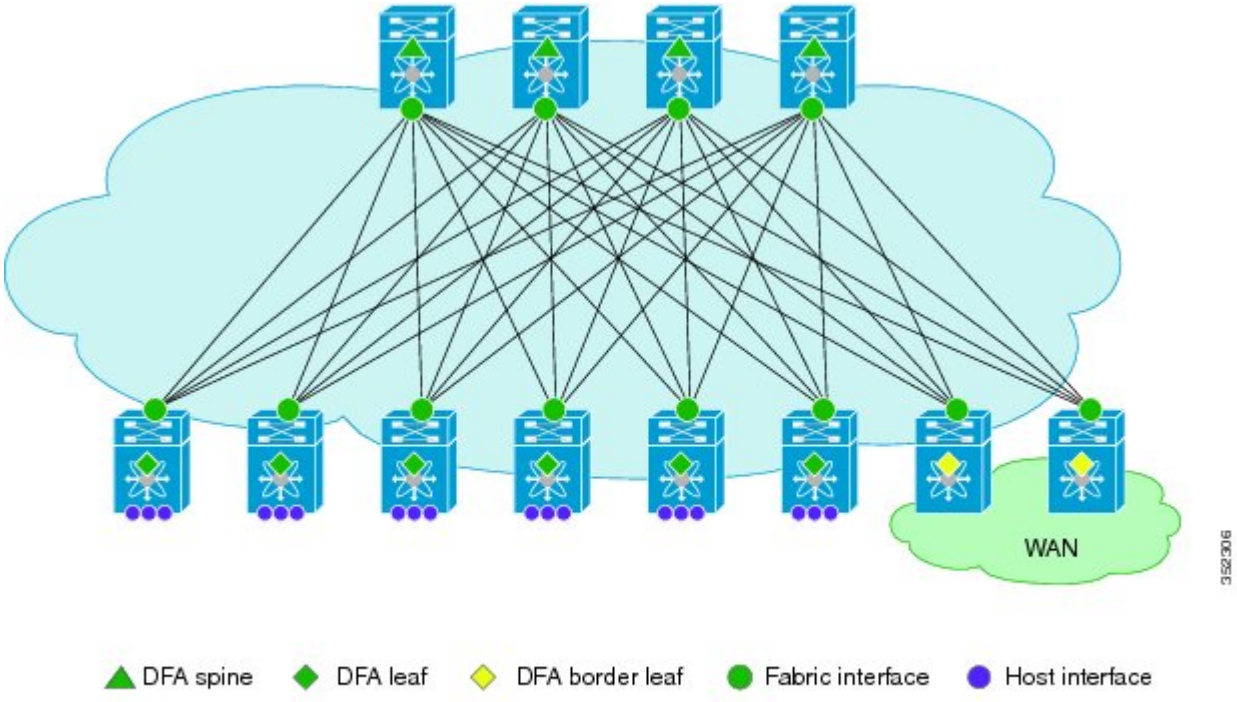
Information About Cisco DFA

This chapter includes the following sections:

Terminology

The following figure illustrates the terms in a Cisco Dynamic Fabric Automation (DFA) deplyment. You should understand these terms and definitions before deploying Cisco Dynamic Fabric Automation (DFA).

Figure 1: Terms Used in a Cisco DFA Deployment



- Cisco DFA fabric--Multistage, switching network in which every connected device is reachable through the same number of hops. The Cisco DFA fabric enables the use of a Scale-Out model for optimized growth.
- Cisco DFA switch--A leaf, border leaf, or spine device.
- Leaf--Switches with ports that are connected to Ethernet devices such as servers (host interfaces) and ports (fabric interfaces) that are connected to the Cisco DFA fabric. Leaf switches forward traffic based on enhanced control-plane functionality of Cisco DFA optimized networking, which requires segment-id based forwarding.
- Border leaf--Switches that primarily connect external network devices or services, such as fire walls and router ports, to a Cisco DFA fabric. Border leaf switches are similar to leaf switches and can perform segment-id based forwarding.
- Spine-- Switches through which all leaf and border leaf switches are connected to each other and to which no end nodes are connected. Spine switches forward traffic based on Cisco DFA optimized networking with enhanced or traditional forwarding.

- Host interface--Leaf-to-server interfaces that receive traffic for connected VLANs to be extended across the Cisco DFA fabric.
- Fabric interface--Ports through which Cisco DFA switches are connected to one another.

Cisco Dynamic Fabric Automation Overview

Cisco Dynamic Fabric Automation (DFA) optimizes data centers through superior integration. The Cisco DFA architecture eliminates the need for overlay networks that can hinder traffic visibility and optimization and reduce scalability when physical server and virtual machine environments are integrated. This simpler, more homogeneous architecture enables zero-touch provisioning and greater orchestration, while delivering more predictable performance and latency for large cloud networks. The following building blocks are the foundation of Cisco DFA:

- Fabric Management--Simplifies workload visibility, optimizes troubleshooting, and automates fabric component configuration.
- Workload Automation--Integrates with automation and orchestration tools through northbound application programming interfaces (APIs) and also provides control for provisioning fabric components by automatically applying templates that leverage southbound APIs and/or standard-based protocols. These automation mechanisms are also extensible to network services.
- Optimized Networking--Uses a simple distributed gateway mechanism to support any subnet, anywhere, concurrently. Existing redundancy models are also utilized to provide N+ redundancy across the entire fabric.
- Virtual Fabrics--Extends the boundaries of segmented environments to different routing and switching instances by using logical fabric isolation and segmentation within the fabric. All of these technologies can be combined to support hosting, cloud, and/or multi-tenancy environments.

Fabric Management

The fabric management network in Cisco Dynamic Fabric Automation (DFA) represents a dedicated out-of-band network that is responsible for bootstrapping and managing the individual networking devices, such as spines, leafs, border leafs, that are controlled by fabric management. The fabric management network is responsible for transporting the protocols required for the different fabric management functions.

Table 1: Functions and Protocols Across the Fabric Management Network

Function	Protocol
Power On Auto provisioning (POAP) for automatically configuring network devices	• Dynamic Host Configuration Protocol (DHCP) • Trivial File Transfer Protocol (TFTP) • Serial Control Protocol (SCP)
Fabric discovery	Simple Network Management Protocol (SNMP)

Function	Protocol
User-to-machine and machine-to-machine communication	Extensible Messaging and Presence Protocol (XMPP)
Automated network provisioning	Lightweight Directory Access Protocol (LDAP)

The management network, also known as the management access, is the Network Administrator-facing interface for accessing fabric management. The management network represents the portion of your network from which a Network Administrator can connect to an Element Manager or a network management station (NMS) and to switches and routers.

The Cisco Data Center Network Manager (DCNM) is a turn-key management system for fabric management, visibility, and an extensible set of functions to more efficiently control the data center fabric. Cisco DCNM combines ease of deployment and use with standards-based control protocols components to provide an extensive level of customization and integration with an operations support system (OSS) network.

Cisco Prime Data Center Network Manager

An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco DCNM OVA includes application functionality that is necessary for Cisco Dynamic Fabric Automation (DFA). The Cisco Prime data Center Network manager (DCNM) as an OVA can be deployed on a VMWare Vsphere infrastructure.

The Cisco Prime Data Center Network Manager (DCNM) provides the following functionality:

- Device auto configuration is the process of bringing up the Cisco DFA fabric by applying preset configuration templates to any device joining the fabric. Auto configuration installs an image or applies the basic configuration.
- Cable-plan consistency checks the physical connectivity of the fabric against a documented cable plan for compliance. The lack of compliance prevents specific links from being active, protecting the fabric from unwanted errors.
- Common point-of-fabric access allows Administrators to interact with the fabric as a single entity (system) to simplify queries and to eliminate switch-by-switch troubleshooting efforts.
- Automated network provisioning provides a new layer of automation integration in which the Data Center fabric-switching infrastructure is automatically provisioned for the physical or virtual workload being instantiated.
- Network, virtual fabric, and host visibility is provided by the management GUI and displays a single set of active network elements belonging to an organization in the fabric.

The Cisco DFA DCNM access network is the network administrator-facing interface for accessing fabric management and for connecting northbound application program interfaces (APIs) to orchestrators.

Optimized Networking

Optimized networking in Cisco Dynamic Fabric Automation (DFA) uses a simple distributed gateway mechanism to support any subnet, anywhere, concurrently.

Frame Encapsulation

Optimized networking in a Cisco Dynamic Fabric Automation (DFA) deployment uses Cisco FabricPath Frame Encapsulation (FE) for efficient forwarding based on a Shortest Path First (SPF) algorithm for unicast and multicast IP Traffic. Host route distribution across the fabric is accomplished using a scalable multi-protocol Border Gateway Protocol (MP-BGP) control plane.

The Cisco DFA enhanced forwarding improves Cisco FabricPath FE by optimizing the conversational learning from Layer 2 to the Layer 3. In addition to the enhanced control and data plane for unicast and multicast forwarding, Cisco DFA reduces the Layer 2 failure domain by having the Layer2/Layer 3 demarcation on the host-connected leaf switch, terminating the host-originated discovery protocols at this layer.

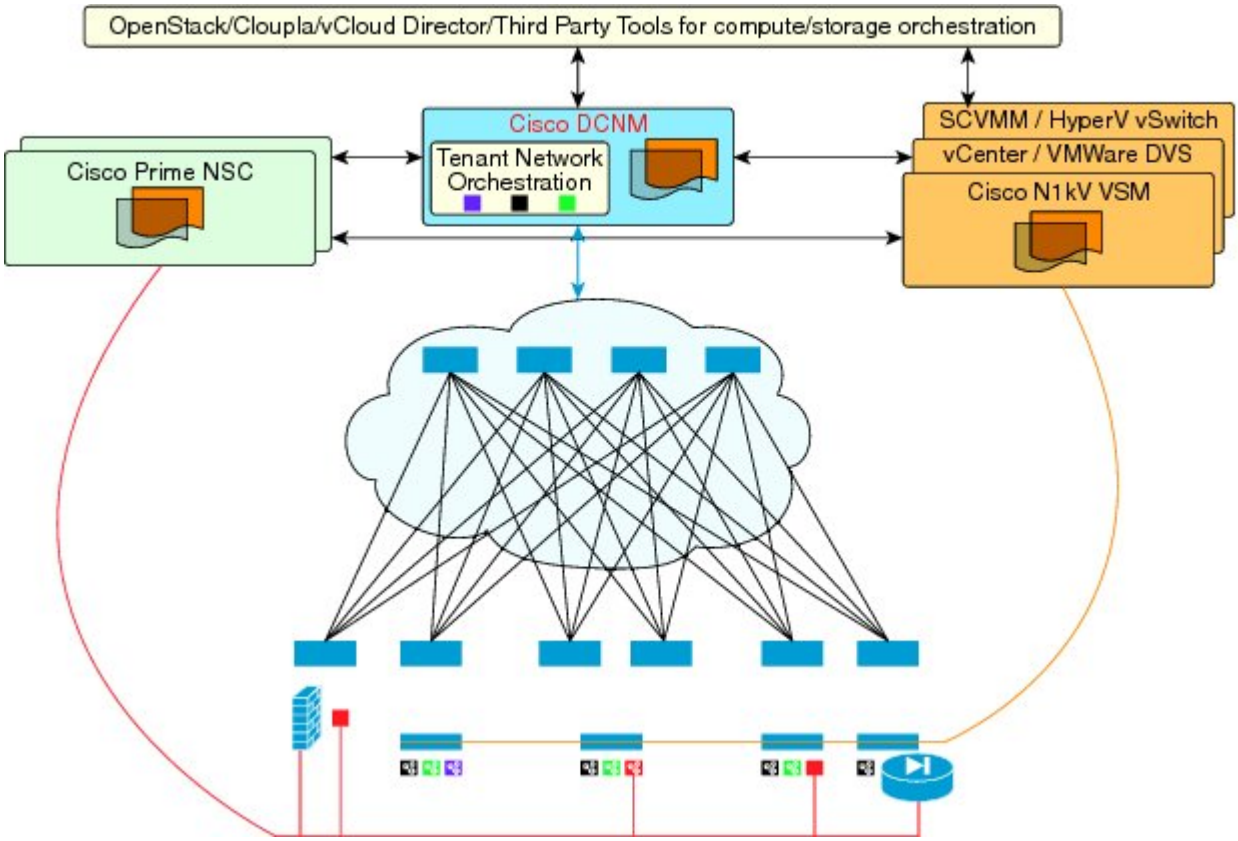
A distributed anycast gateway on all of the Cisco DFA leaf switches for a VLAN improves resilience and enables the fabric to scale to more hosts by keeping a short path for intra and inter VLAN forwarding. Cisco DFA leaf switches that operate as border leaf switches interconnect the Cisco DFA fabric to external networks. Cisco DFA border leaf switches peer with external standard unicast and multicast routing protocols.

Cisco DFA Services Support

Services such as a firewall, load balancer, and virtual private networks (VPNs) are deployed at the aggregation layer in the traditional data center. In a Cisco Dynamic Fabric Automation (DFA) deployment, services nodes

are deployed at regular leaf switches for both east-west and north-south traffic. Services can be physical or virtual services nodes.

Figure 2: Cisco DFA with Services



The Cisco Prime Network Services Controller (NSC) is the services orchestrator for Cisco DFA. The NSC Adapter in the Cisco Data Center Network Manager (DCNM) Open Virtual Appliance (OVA) performs the following functions:

- Provides connectivity between the Cisco Prime DCNM and the Cisco Prime NSC services orchestrator
- Automatically populates the Cisco Prime NSC with the organizations, partitions, and networks that are created in Cisco Prime DCNM
- Populates Cisco Prime DCNM with the services that are stitched through Cisco Prime NSC
- Allows the use of multiple Cisco Prime NSC instances to match the Cisco Prime DCNM scale

In Cisco DFA, configuration profile templates and instantiating the profiles on a leaf switch provides network automation. The templates are extended to support services in Cisco DFA. The profile templates are packaged in Cisco Prime DCNM for the services orchestrator. The table below includes a list of profile templates that are available for Cisco DFA services. It is important that you select the correct profile to orchestrate and automate services in the Cisco DFA fabric.

Table 2: Cisco Templates for Services Support

Service	Network	Routing	Service Profile
Edge Firewall	Host Network	N/A	defaultNetworkIpv4EfEdgeServiceProfile
	Edge Firewall	Static	defaultNetworkIpv4TfEdgeServiceProfile
		Dynamic	serviceNetworkIpv4TfDynamicRoutingProfile
	Tenant External Service Network	Static	defaultExternalNetworkIpv4TfProfile
		Dynamic	externalNetworkIpv4TfDynamicRoutingProfile
Service Node as Router/Default Gateway	Host Network	N/A	defaultNetworkL2Profile

For NSC Adapter installation information, see the *Cisco DCNM 7.0 OVA Installation Guide*.

OpenStack for Cisco DFA

OpenStack creates a human- and machine-accessible service for managing the entire life cycle of the infrastructure and applications within OpenStack clouds. The technology consists of a series of interrelated projects that control pools of processing, storage, and networking resources throughout a data center that can be managed or provisioned through a web-based dashboard, command line tools, or a RESTful application programming interface (API).

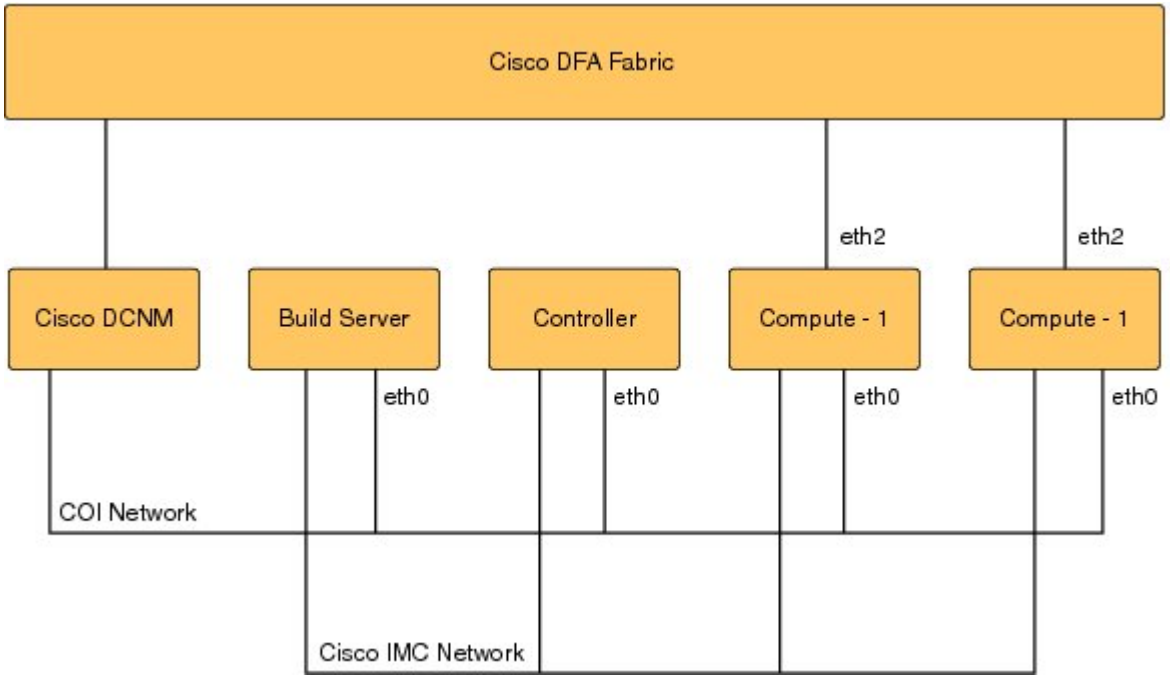
The OpenStack for Cisco DFA software is included in the Cisco OpenStack Installer with its Grizzly-based release for this initial Cisco Dynamic Fabric Automation (DFA) release. OpenStack for Cisco DFA provides orchestration of the cloud that is enabled by Cisco DFA.

A minimum of three Cisco UCS C-series servers, each with a minimum 500.1GB hard disk space, are required for using the pre-installed OpenStack for Cisco DFA. The initial release (1.0) of OpenStack for Cisco DFA is supported only through the web-based dashboard. The role and responsibilities for each Cisco UCS server is described in the following list:

- Build server--One server is a dedicated puppet build server.
- Controller--One server is a dedicated OpenStack controller for performing orchestration.
- Compute--One or more servers provide the hypervisor function for virtual machines (VMs); VMs run in the computes. You can have as many computes as is required and each compute can host multiple VMs.

The following figure illustrates a sample topology for OpenStack for Cisco DFA.

Figure 3: OpenStack for Cisco DFA Topology



Each of the Cisco UCS servers in your implementation must be connected to each other and the Cisco Prime Data Center Network Manager (DCNM) must be connected to the control node. In the sample topology illustrated in the preceding figure, the build server, the controller and the computes are all connected through eth0 on the Cisco OpenStack Installer network (COI in the figure).

All of the Cisco UCS servers in your implementation must be configured with the Cisco Integrated Management Controller (IMC), also called CIMC. All of the Cisco IMC ports on the build server, controller, and computes must be connected to the Cisco IMC network. The Cisco IMC network performs the management functions against each Cisco UCS server.

For information about Open Source used in OpenStack for Cisco DFA 1.0, see the *Open Source used in OpenStack for Cisco DFA 1.0* document.