Cisco Dynamic Fabric Automation Migration Guide

First Published: January 31, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-31503-01

© 2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface v

- Audience v
- Document Organization v
- Document Conventions vi
- Related Documentation for Cisco DFA vii
- Documentation Feedback viii
- Obtaining Documentation and Submitting a Service Request viii

CHAPTER 1

Information About Cisco DFA 1

- Terminology 2
- Cisco Dynamic Fabric Automation Overview 3
- Fabric Management 3
  - Cisco Prime Data Center Network Manager 4
- Optimized Networking 4
  - Frame Encapsulation 5
- Cisco DFA Services Support 5
- OpenStack for Cisco DFA 7

CHAPTER 2

Migration Overview 9

- Prerequisites 9
- Existing FabricPath Topology 10
- Cisco Dynamic Fabric Automation Topology 11
- Traffic Flow Before and After Migration 14

CHAPTER 3

Migration Steps 23

- Step 1: Upgrade the Spine Switch software 23
- Step 2: Upgrade the Border Leaf Software 24

Step 3: Add Cisco DFA-related Configuration to the First Border Leaf Pair 25

Step 4: Upgrade the Second Border Leaf Pair 26

Step 5: Add Cisco DFA-related Configuration to the Second Border Leaf Pair 26

Step 6: Upgrade the FabricPath Leaf Pair 27

Step 7: Add Cisco DFA Configuration to Layer 2 Leaves 27

Step 8: Upgrade and Configure All Remaining Leaf Switches 28

Step 9: Remove HSRP Configurations on Border Leaf Pairs 29

CHAPTER 4 Migration Configuration 31

Configuring the BGP Route Reflector on a Spine 31

Configuring the Virtual Network Identifier Range 35

Configuring SVIs and HSRPs on Border Leafs 36

Configuring Border Leaves for DFA 39

Configuring a Host-facing Interface 45

Adding a Tenant (VRF) Instance on a Leaf 47

Adding a Host-facing Tenant Interface (Vlan) 49

Removing HSRP Configuration on all Border Leaves 51

Preface

The Preface contains the following sections:

- Audience, page v
- Document Organization, page v
- Document Conventions, page vi
- Related Documentation for Cisco DFA, page vii
- Documentation Feedback, page viii
- Obtaining Documentation and Submitting a Service Request, page viii

Audience

This publication is for experienced network administrators who configure and maintain Cisco Dynamic Fabric Automation.

Document Organization

This document is organized into the following chapters:

Chapter	Description
"Information About Cisco DFA"	Provides an overview of Cisco Dynamic Fabric Automation (DFA) and descriptions of the Cisco DFA building blocks.
"Deploying Cisco DFA"	Provides information about how to prepare for and deploy Cisco DFA, including compatibility and licensing information.
"Configuration Examples for Cisco DFA"	Provides examples of basic Cisco DCNM templates for configuring spine and leaf devices.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation for Cisco DFA

The Cisco Dynamic Fabric Automation documentation is at the following URL: http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns945/dynamic_fabric_automation.html#~Products .

The Cisco Nexus 6000 Series documentation is at the following URL: http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html.

The Cisco Nexus 7000 Series documentation is at the following URL: http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html.

The Cisco Nexus 1000V Switch for VMware vSphere documentation is at the following URL: http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html. The documentation therein includes the following guides for Cisco DFA. Additional information pertaining to troubleshooting can be located in the Cisco Nexus 1000V documentation for Cisco NX-OS Release 4.2(1)SV2(2.2).

- *Cisco Nexus 1000V DFA Configuration Guide, Release 4.2(1)SV2(2.2)*
- *Cisco Nexus 1000V VDP Configuration Guide, Release 4.2(1)SV2(2.2)*

The Cisco Prime Data Center Network Manager (DCNM) documentation is at the following URL: http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html. The Cisco Prime DCNM documentation for Cisco DFA includes but is not limited to the following guides:

- *Cisco DCNM 7.0 OVA Installation Guide.*
- *Cisco DCNM 7.0 Fundamentals Guide*
- *Cisco DCNM DFA REST 7.0 API Guide*

The Cisco Prime Network Services Controller (NSC) documentation is at the following URL: http://www.cisco.com/en/US/products/ps13213/tsd_products_support_series_home.html.

The OpenStack for Cisco DFA install documentation includes the following guide and documents:

- *Open Source Used In OpenStack for Cisco DFA 1.0* at the following URL: http://preview.cisco.com/en/US/docs/switches/datacenter/dfa/openstack/opensource/OpenStack_for_Cisco_DFA_1.0_Open_Source_Documentation.pdf
- *OpenStack for Cisco DFA Install Guide Using Cisco OpenStack Installer* at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/dfa/openstack/install/guide/os-dfa-coi.pdf
- *OpenStack for Cisco DFA Install Guide for Using Pre-built OpenStack for Cisco DFA Images* at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/dfa/openstack/install/guide/preblt-image.pdf

- *Quick Guide to Clonezilla* at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/dfa/openstack/install/guide/clonezilla-image-restore.pdf

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to one of the following:

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

CHAPTER 1

Information About Cisco DFA

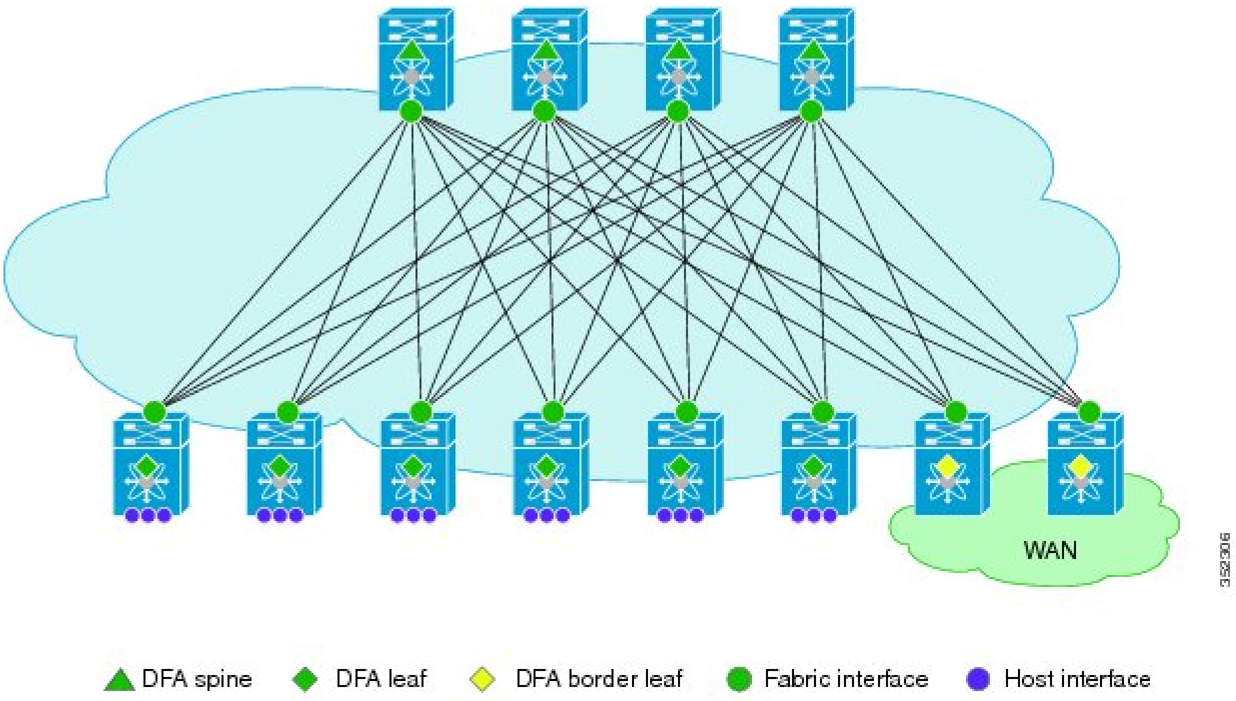
This chapter includes the following sections:

- Terminology, page 2
- Cisco Dynamic Fabric Automation Overview, page 3
- Fabric Management, page 3
- Optimized Networking, page 4
- Cisco DFA Services Support, page 5
- OpenStack for Cisco DFA, page 7

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.

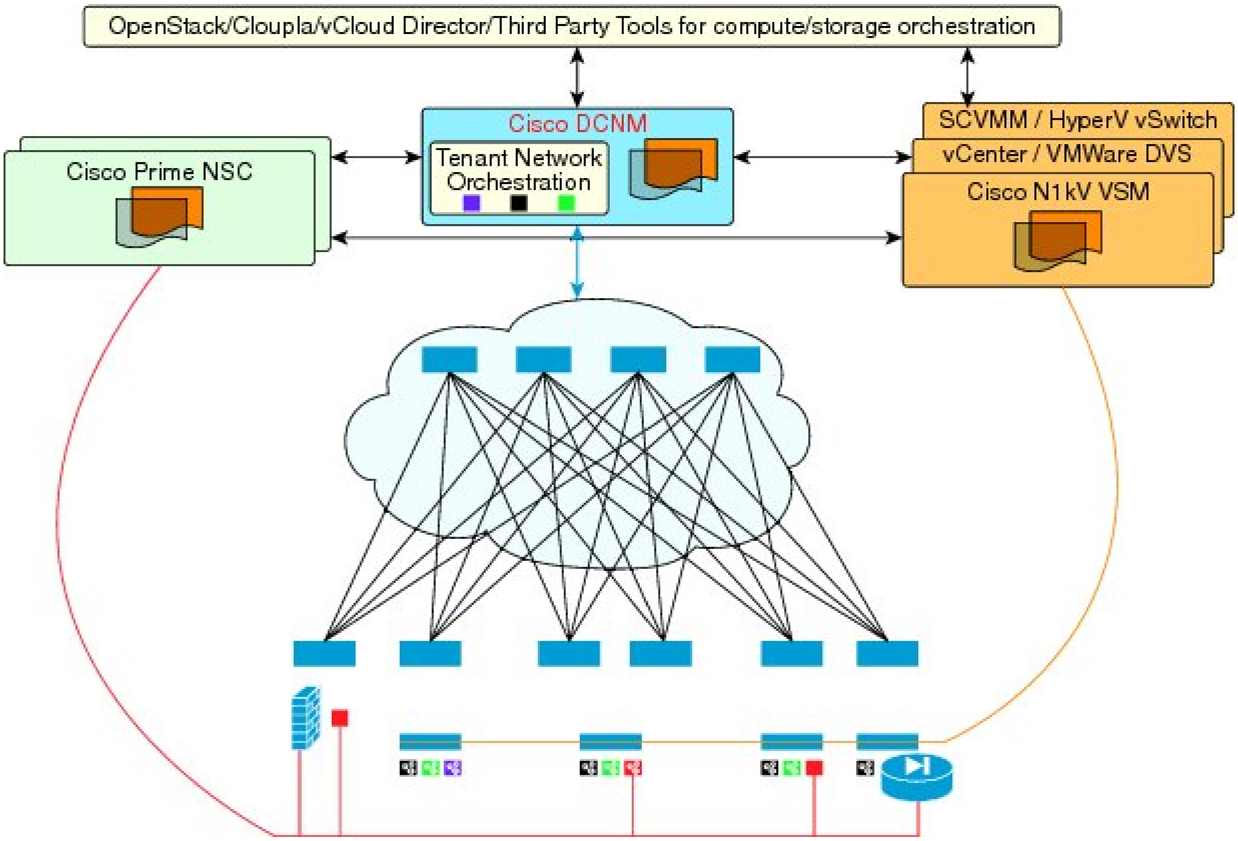
The Cisco DFA enhanced forwarding improves Cisco FabricPath FE by optimizing the conversational learning from Layer 2 to the Layer 3. In addition to the enhanced control and data plane for unicast and multicast forwarding, Cisco DFA reduces the Layer 2 failure domain by having the Layer2/Layer 3 demarcation 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


OpenStack/Cloupla/vCloud Director/Third Party Tools for compute/storage orchestration
Cisco DCNM
Tenant Network Orchestration
Cisco Prime NSC
SCVMM / HyperV vSwitch
vCenter / VMWare DVS
Cisco N1kV VSM
352307

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).

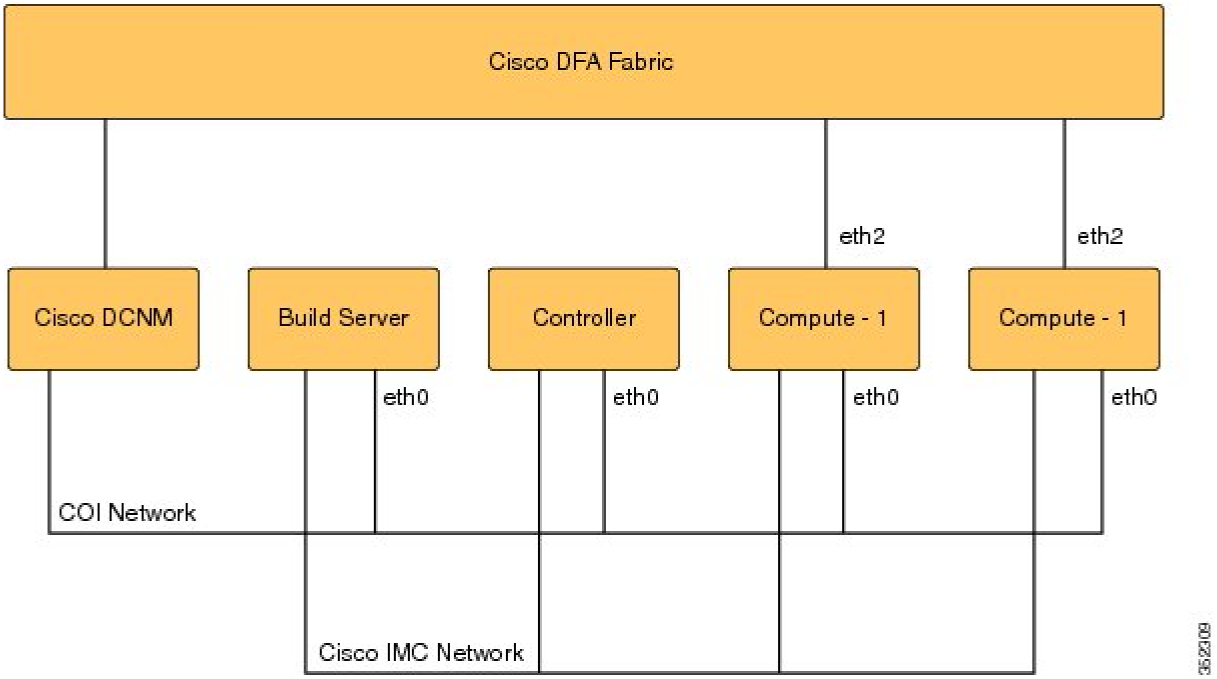
The OpenStack for Cisco DFA software is included in the Cisco OpenStack Installer with its Grizzly-based release for this initial Cisco Dynamic Fabric Automation (DFA) release. OpenStack for Cisco DFA provides orchestration of the cloud that is enabled by Cisco DFA.

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.

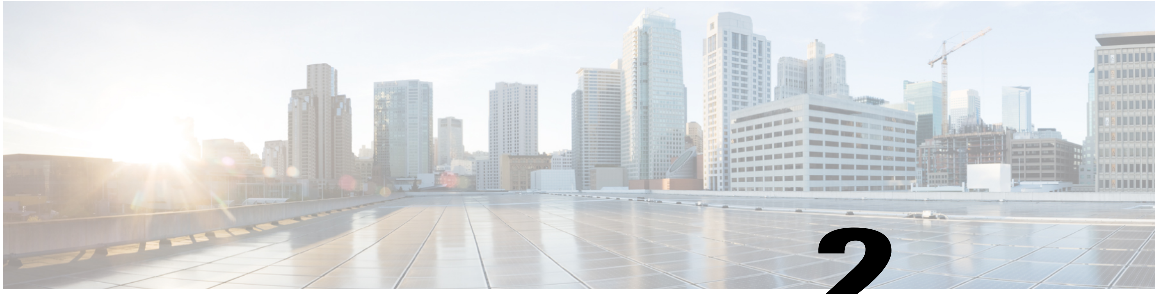
Figure 3: OpenStack for Cisco DFA Topology



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.



CHAPTER 2

Migration Overview

This chapter contains the following sections:

- Prerequisites, page 9
- Existing FabricPath Topology, page 10
- Cisco Dynamic Fabric Automation Topology, page 11
- Traffic Flow Before and After Migration, page 14

Prerequisites

To prepare for migration to the Cisco Dynamic Fabric Automation (DFA) solution, you must meet the following prerequisites.

- Install and configure Cisco Data Center Network Manager 7.0
  - Perform tasks specified in the DCNM 7.0 OVA Installation Guide
  - Perform tasks specified in the DCNM 7.0 Fundamentals Guide
- FabricPath on Spine-Leaf Topology
  - Nexus 7000 spine switches with NX-OS 6.2.(2) images
  - Nexus 6000 border leaf switches with NX-OS 6.02.N2 images
  - Nexus 6000 leaf switches with NX-OS 6.02.N2 images

    Note All non-Nexus 6000 boxes must be physically replaced with Nexus 6000 boxes with NX-OS 7.0(0)N1(1).

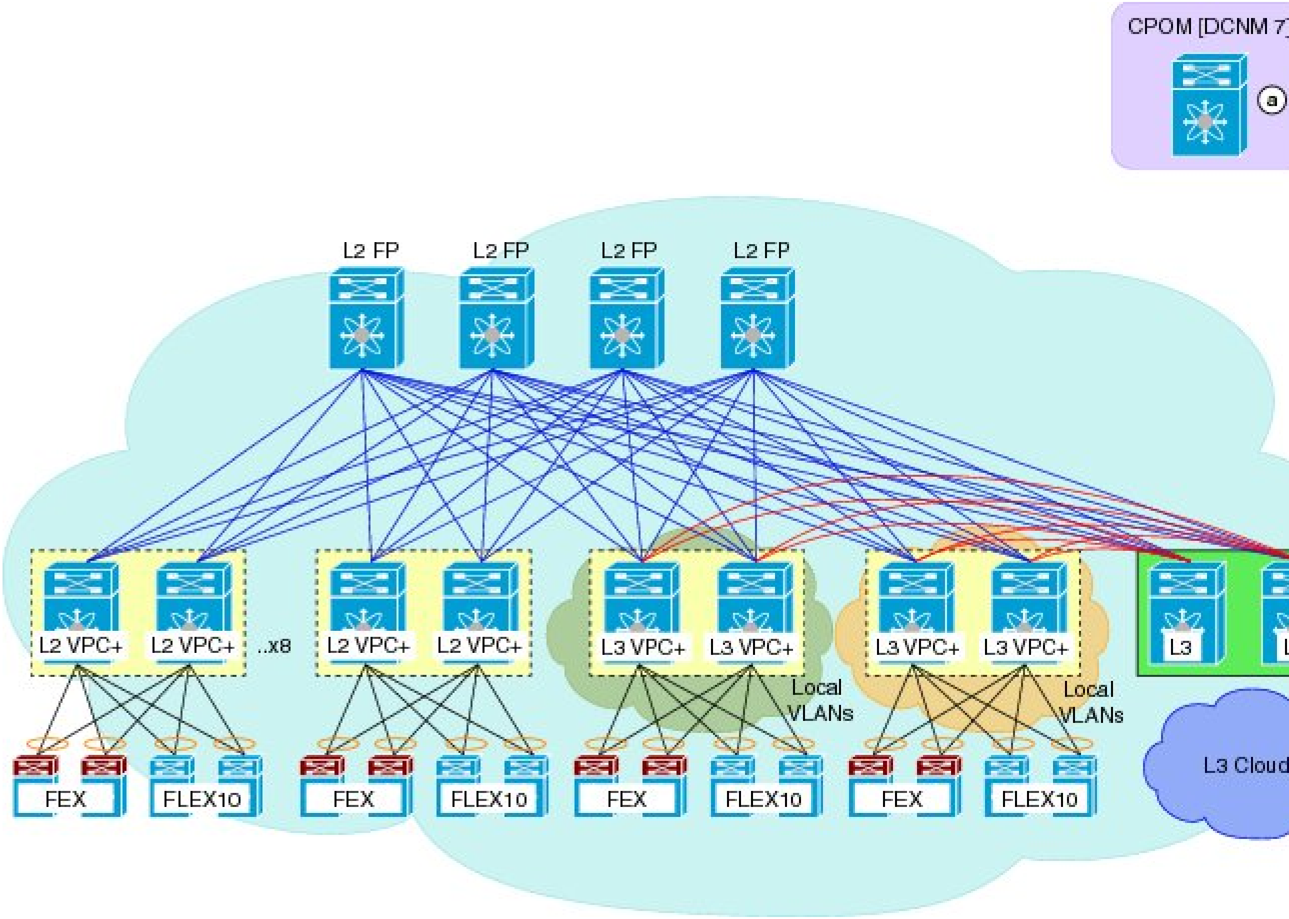
  - Nexus 1000v Series virtual switches at the virtual machine access layer

Existing FabricPath Topology

The existing FabricPath topolgy from which you are migrating includes:

- An access layer with FabricPath-enabled VPCpath peers (VPC+)
- Layer 3 aggregation layer-only connection to Spine layers
- Two peers of Layer 3 boxes
- Switched Virtual Interfaces (SVI) on only one set of VPC+ peers
- HSRP running in local Layer 3 VLANS

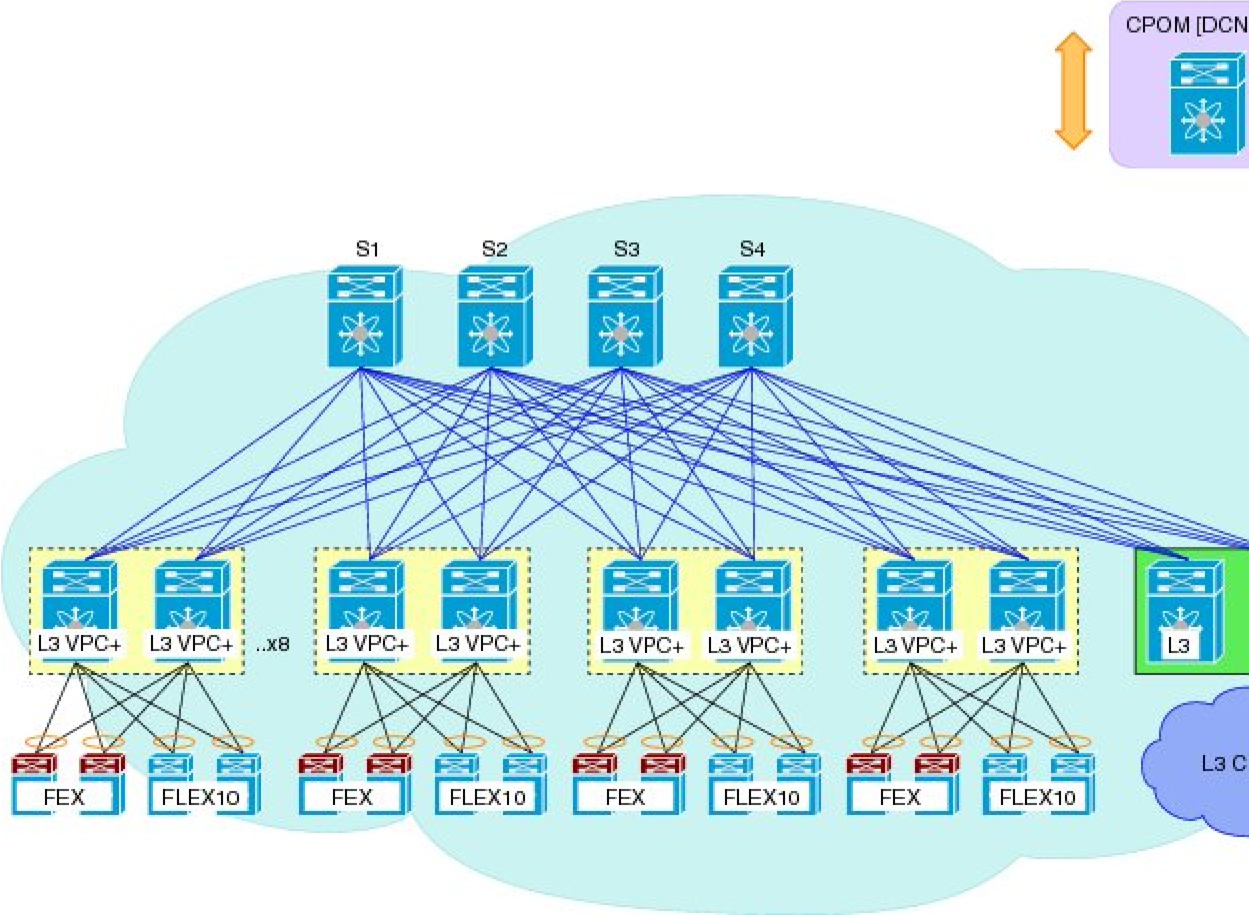
Figure 4: Figure: Pre-migration Fabric Topology



Cisco Dynamic Fabric Automation Topology

An illustration of the Cisco Dynamic Fabric Automation (DFA) topology is shown in the following figure.

Figure 5: Cisco DFA topology



You can structure your Cisco Dynamic Fabric Automation (DFA) topology with two distinct fabrics:

- Fabric with a mix of Nexus 5000 and Nexus 6000 leaves

- Fabric with only Nexus 6000 leaves

Figure 6: DFA Fabric with a mix of Nexus 5000 and Nexus 6000 leaves

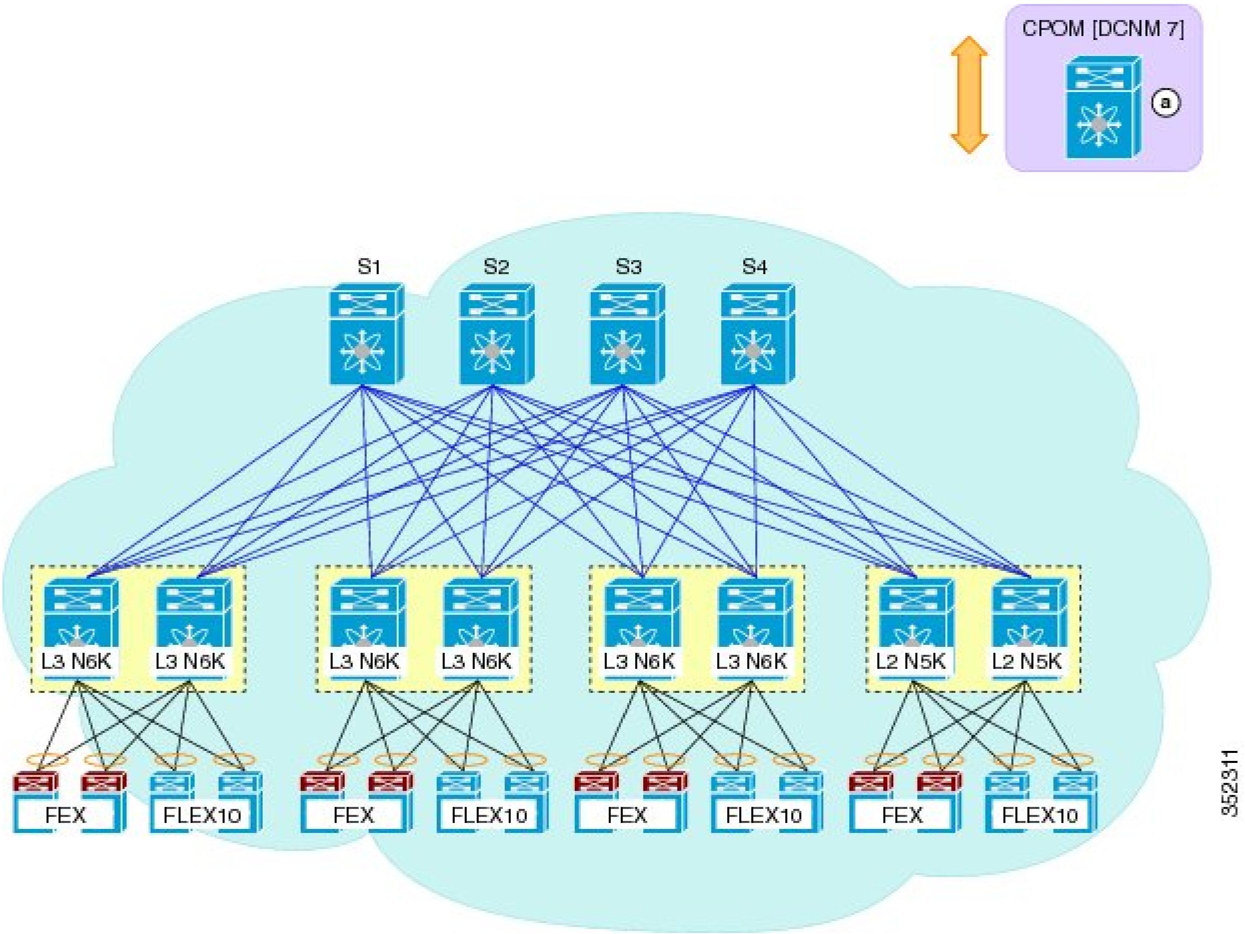
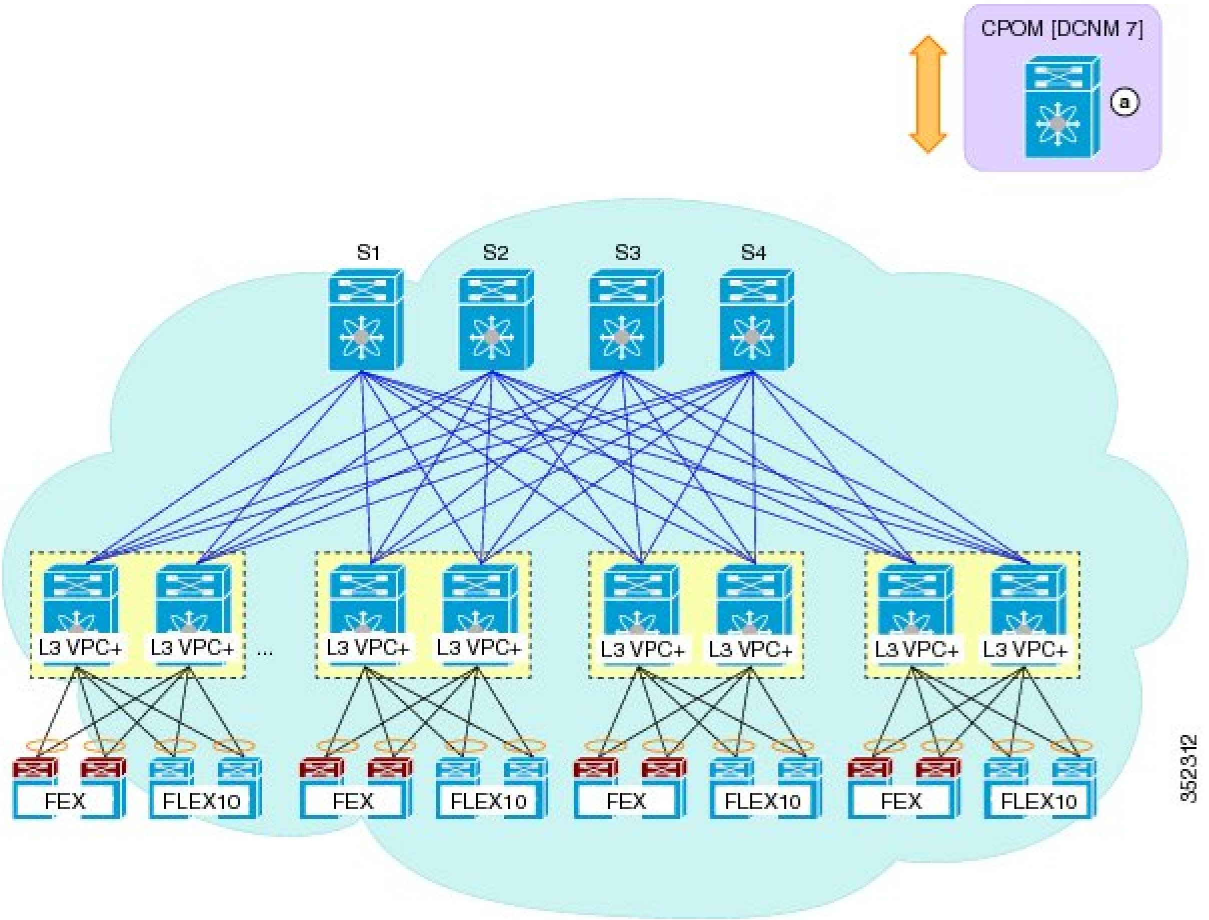


Figure 7: DFA Fabric with only Nexus 6000 leaves



The Cisco DFA fabric with both Nexus 5000 and 6000 leaves includes the following:

- Nexus 5000 remains as Layer 2
- Spine switches that can forward both 1q and 2q traffic, encapsulated in a FabricPath header
- VLAN/SVI distinctions:
    - On a Nexus 5000, the VLAN/SVI is non-Segment ID-enabled across all Cisco DFA leaves running anycast gateway mode on Nexus 6000 leaves. Border leaf runs HSRP/VRRP as well as anycast gateway
    - On a Nexus 6000, the VLAN/SVI is Segment ID-enabled. The forwarding mode can be either proxy or anycast gateway.
    - Multicast will continue to run in the legacy multicast mode. Cisco DFA multicast should not be turned on.

The DFA fabric with only Nexus 6000 leaves includes the following:

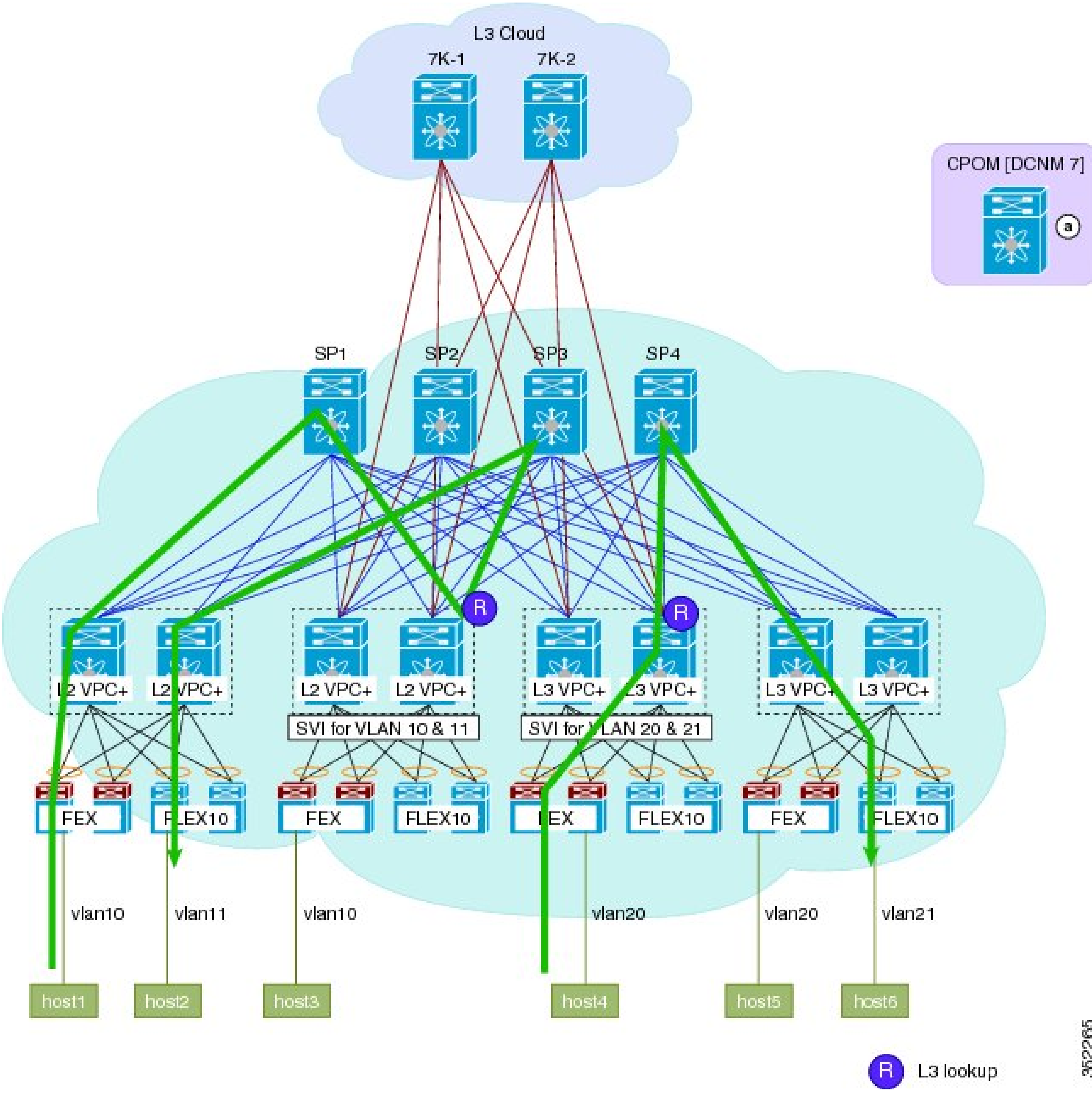
- Nexus 6000 leaves running either Anycast Gateway mode or Proxy Gateway mode
- Spine switches that can forward both 1q and 2q traffic, encapsulated in a FabricPath header
- VLANS that can be Segment ID-enabled

Traffic Flow Before and After Migration

As a result of changes to the topology and configuration of switches, traffic flow is optimized after the migration. Differences in traffic flow are shown in the following set of figures:

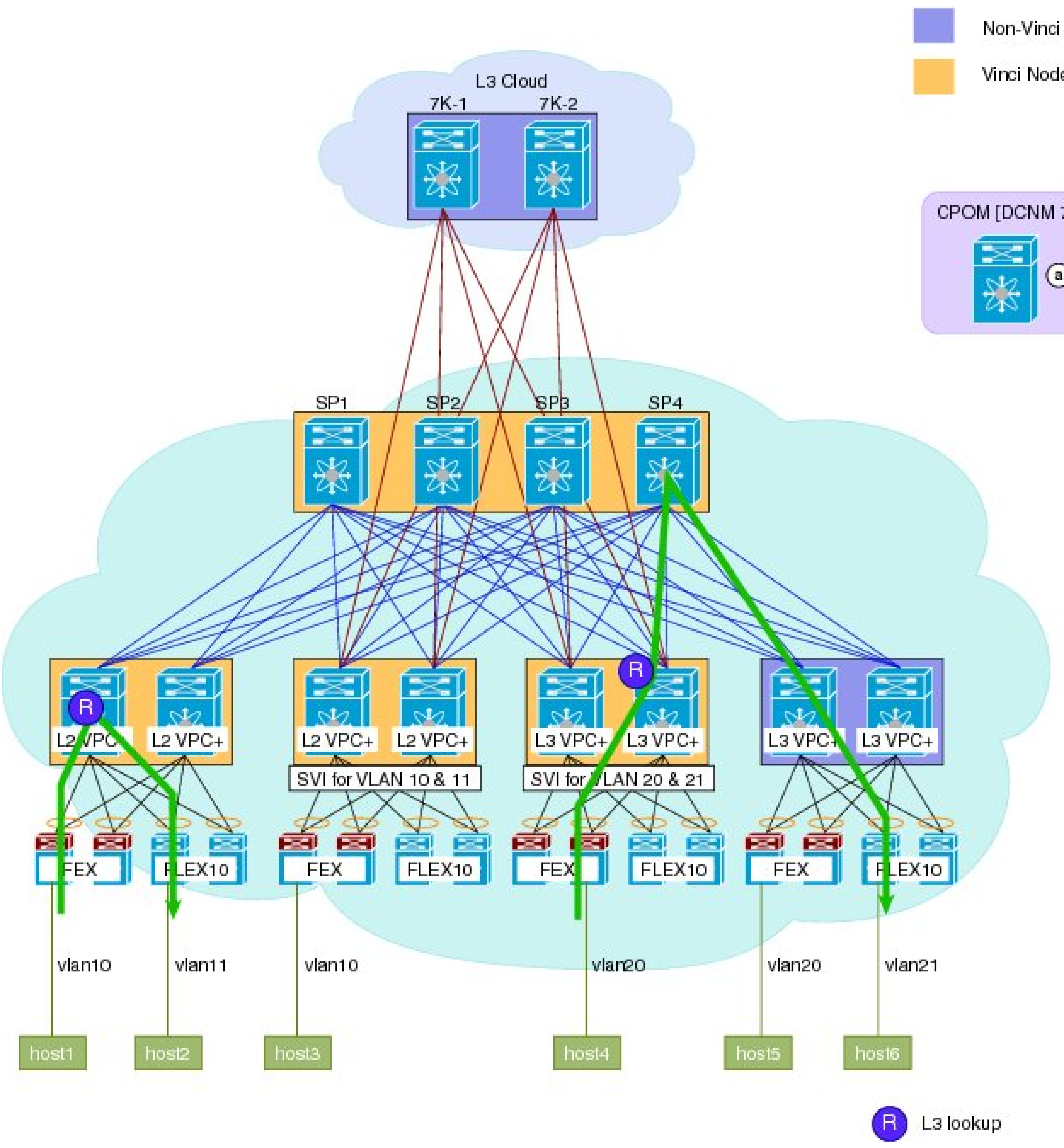
Prior to migration, Inter-VLAN traffic from Host 1 on VLan10 goes through single Layer 3 hops up through the spine to get to host 2 on Vlan11.

Figure 8: Figure: pre-migration inter-vlan single hop



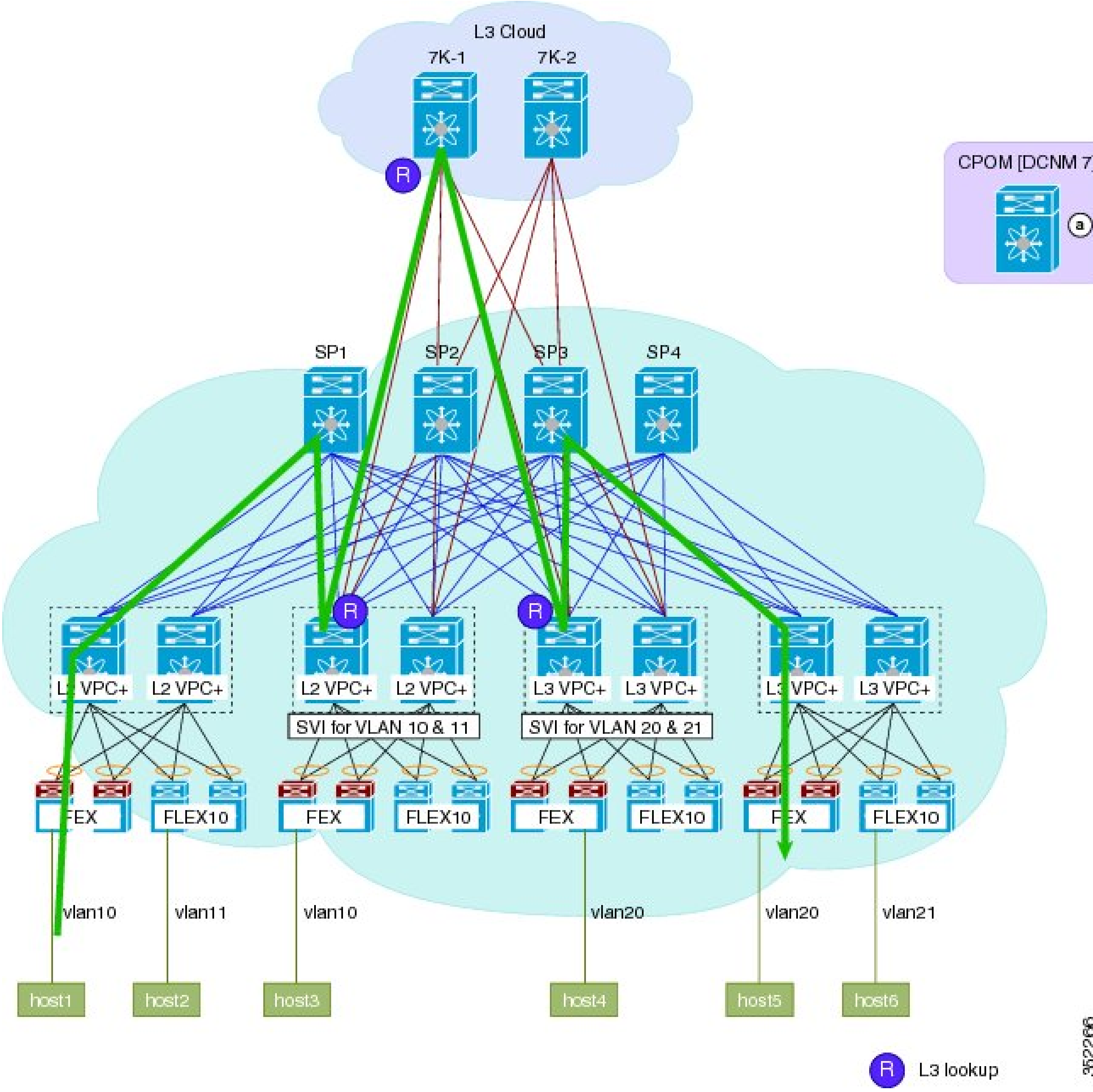
After migration to the Cisco DFA fabric, inter-Vlan traffic from Host 1 on Vlan 10 takes a single hop through a single leaf node, where a Layer 3 lookup is performed and traffic is routed to host 2 on Vlan 11. Border Leafs start to respond to address resolution protocol (ARP) with anycast gateway media access control (MAC).

Figure 9: Figure: post-migration inter-vlan single hop



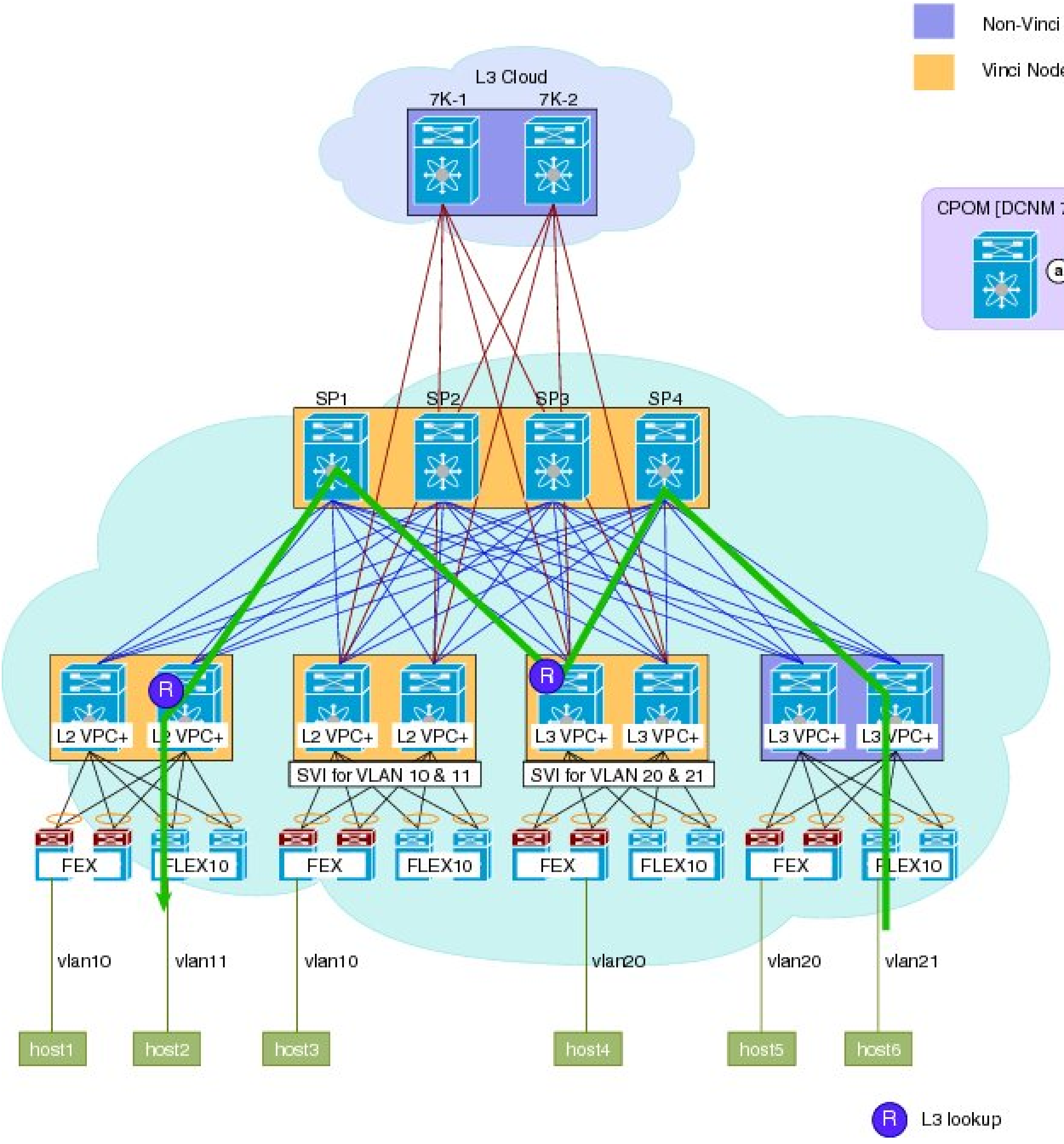
Prior to migration, traffic going from host1 on vlan10 to host 5 on vlan20 takes multiple Layer 3 hops up to the Nexus 7000 Layer 3 and a series of Layer 3 lookups.

Figure 10: Figure: inter-vlan trafic multiple l3 hops x



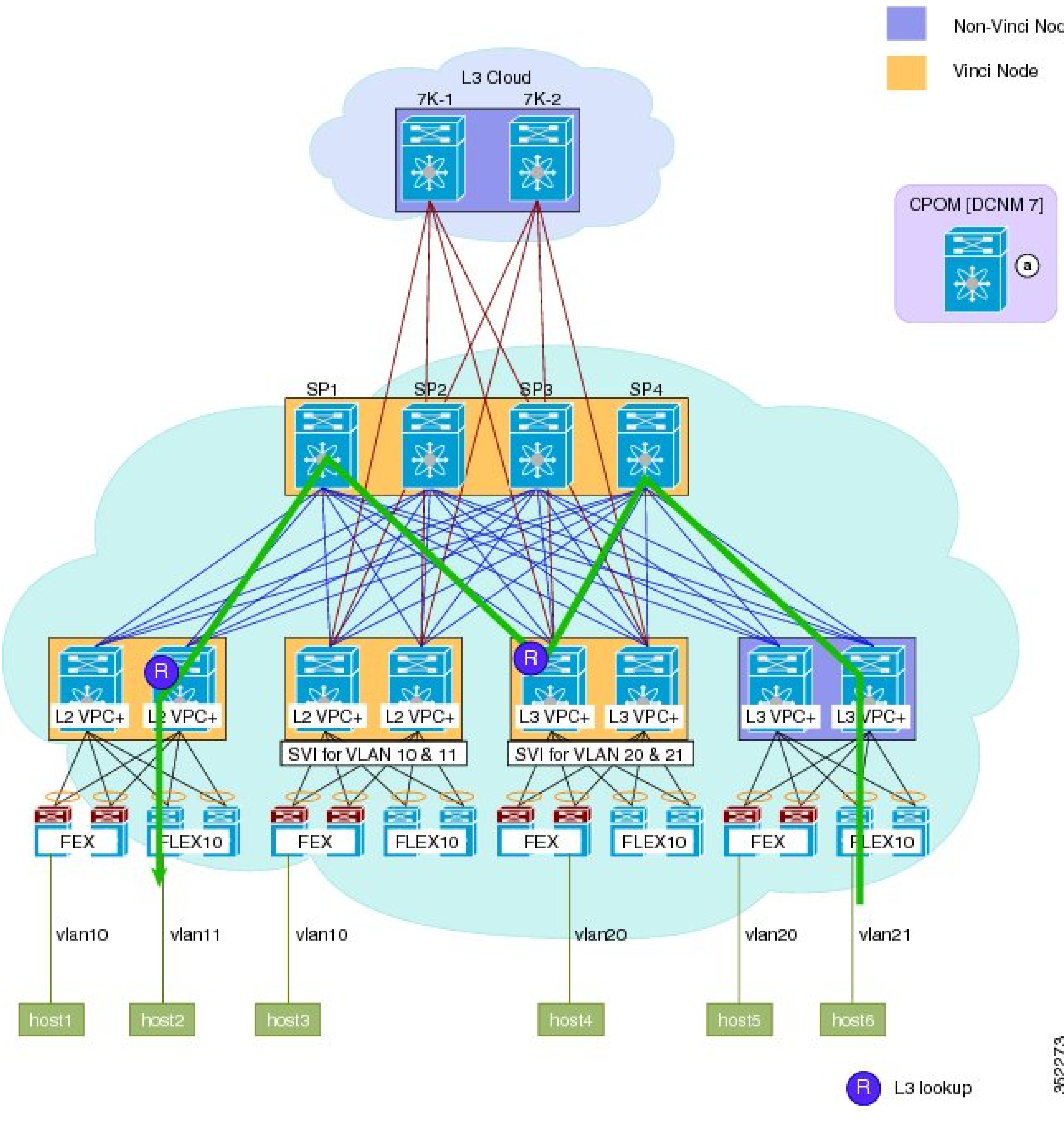
After migration, unicast traffic going from host 1 on vlan 10 to host 4 on vlan 20 takes fewer Layer 3 lookups at the leaf-level, and direct forwarding occurs between border leaf pairs through the spine without going to the Nexus 7000.

Figure 11: Figure: post-migration Unicast traffic flow



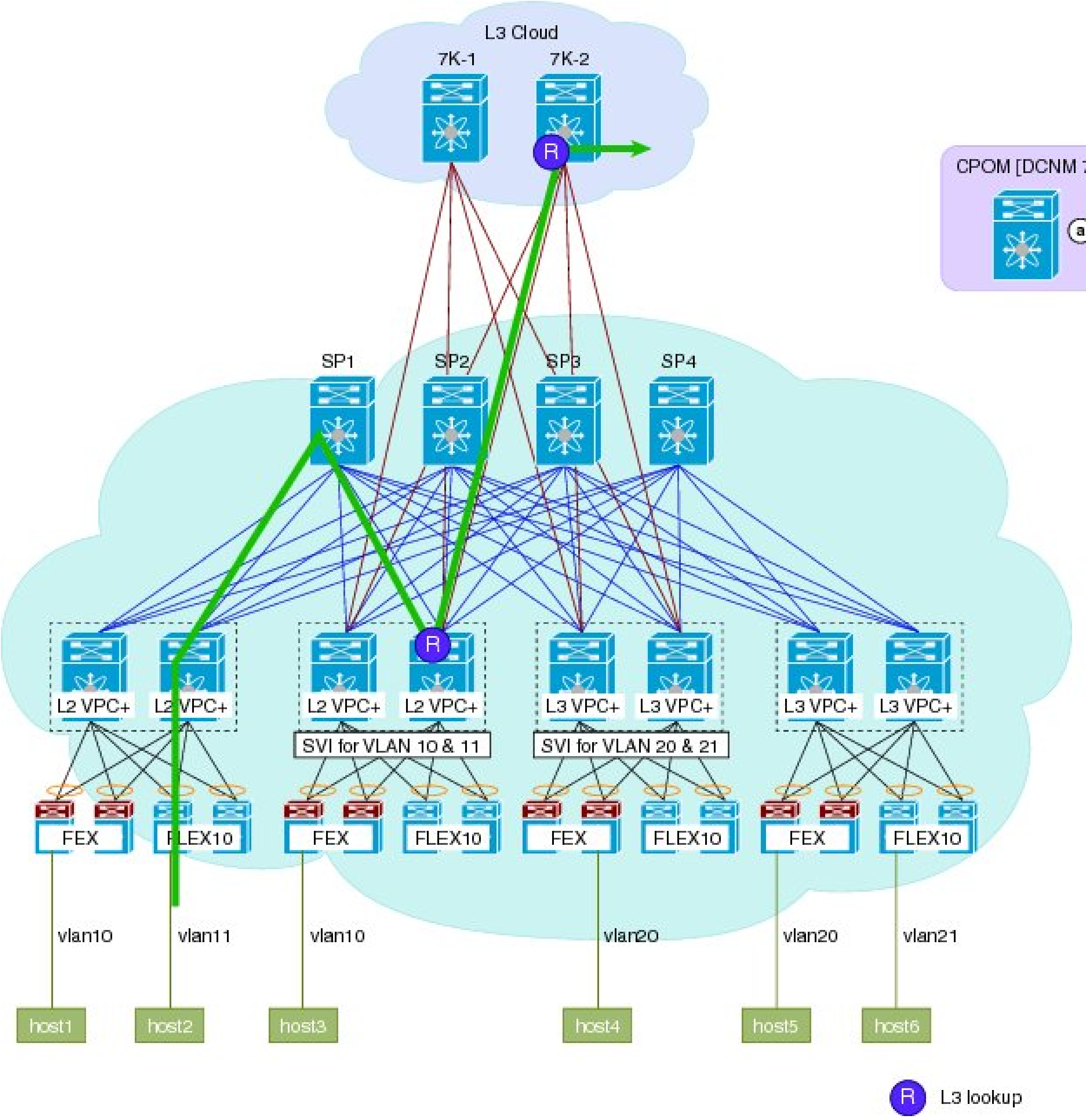
Another illustration of post-migration unicast traffic flow.

Figure 12: Figure: post-migration unicast traffic flow



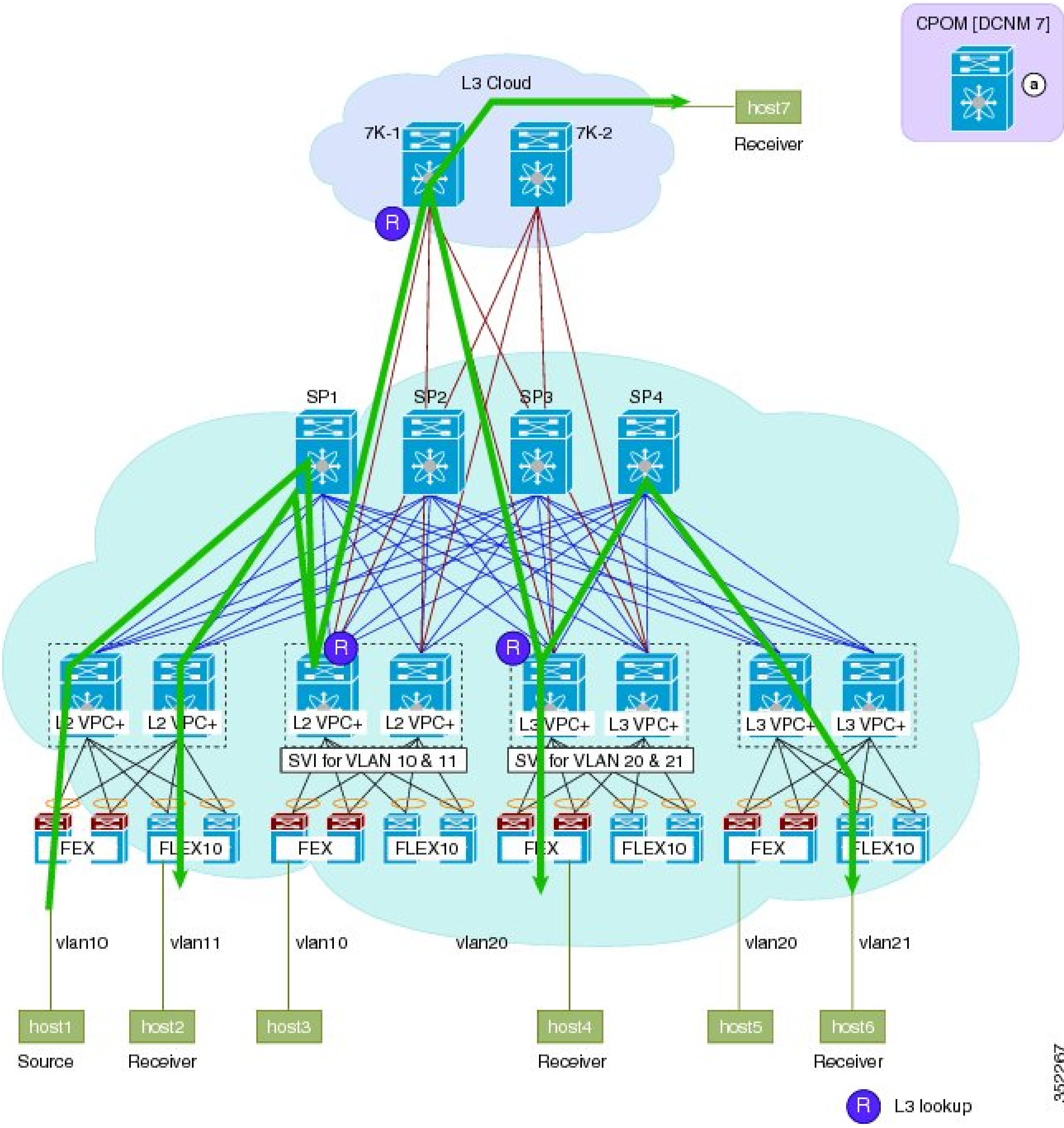
North-South traffic remains unchanged after the migration and requires two Layer 3 lookups before reaching the Layer 3 cloud

Figure 13: Figure: North South Traffic Flow



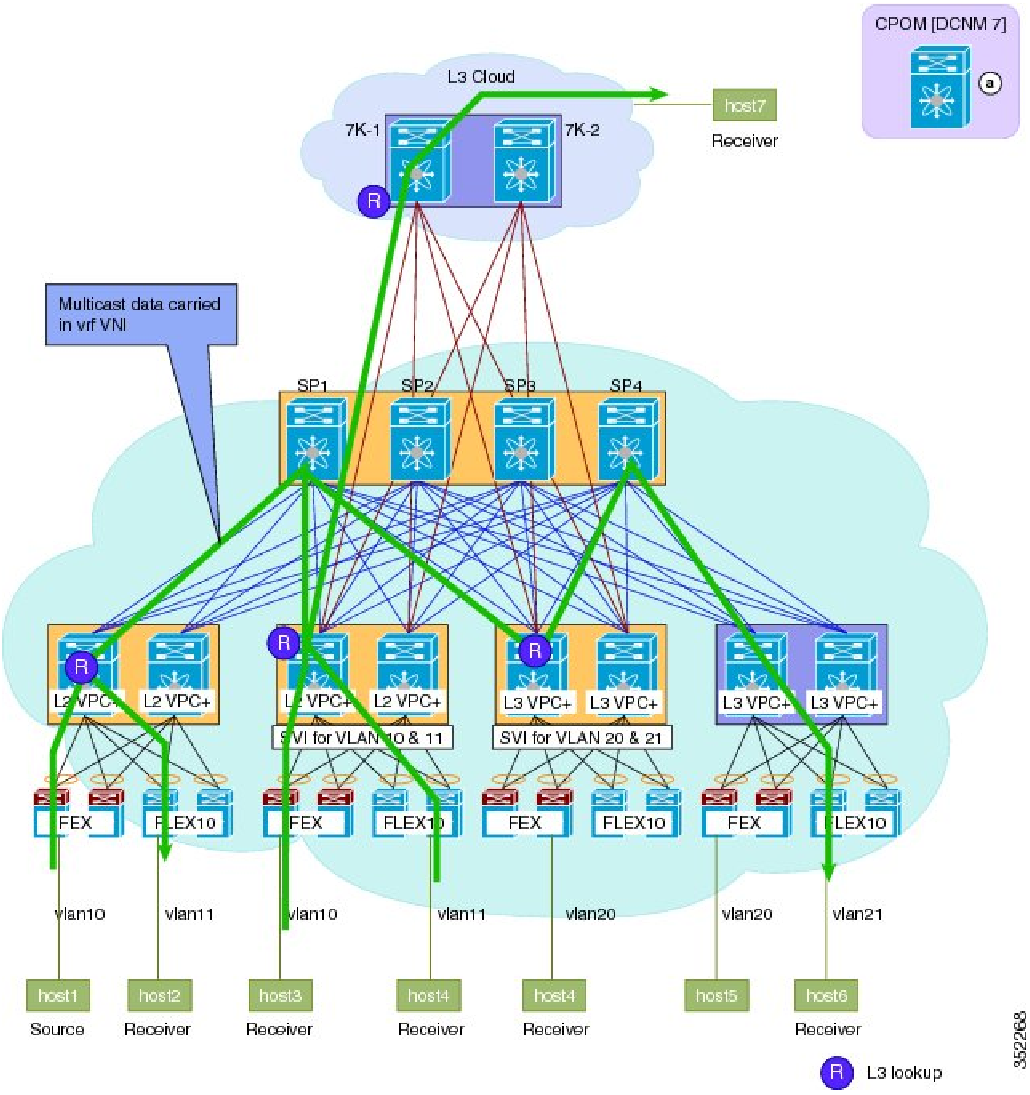
PIM-SM and multicast replication behavior is the same as a non-FabricPath topology. Layer 2 multicast forwarding follows a pruned FabricPath tree. Internet Group Management Protocol (IGMP) is propagated to all FabricPath nodes via Intermediate-system to intermediate-system (ISIS).

Figure 14: Figure: Pre-migration Multicast Traffic Flow



IF there is a Nexus 5000 in the topology, legacy multicast will continue to run.

Figure 15: Figure: post-migration multicast traffic flow



CHAPTER 3

Migration Steps

This chapter contains the following sections:

- Step 1: Upgrade the Spine Switch software, page 23
- Step 2: Upgrade the Border Leaf Software, page 24
- Step 3: Add Cisco DFA-related Configuration to the First Border Leaf Pair, page 25
- Step 4: Upgrade the Second Border Leaf Pair, page 26
- Step 5: Add Cisco DFA-related Configuration to the Second Border Leaf Pair, page 26
- Step 6: Upgrade the FabricPath Leaf Pair, page 27
- Step 7: Add Cisco DFA Configuration to Layer 2 Leaves, page 27
- Step 8: Upgrade and Configure All Remaining Leaf Switches, page 28
- Step 9: Remove HSRP Configurations on Border Leaf Pairs, page 29

Step 1: Upgrade the Spine Switch software

The first step of the migration is to upgrade all spine switch software.

Before You Begin

The following pre-requisites must be met for upgrading Nexus 6000 spine switch software

- Nexus 6000 series switch must be running on Cisco NX-OS version 6.2.(2) software release
- Border leaf nodes must be DFA hardware-capable Nexus 6000 nodes running Cisco NX-OS version 6.0.2.N2

Note If you have anything other than a Nexus 6000 series switch, you must physically replace the switch with the version 7.0.(0)N1(1) image; the configuration remains the same as the previous image.

Step 1 On the Nexus 6000 series spine switches, perform a non-disruptive in-service software upgrade (ISSU) upgrade to Cisco NX-OS version 7.0(0)N1(1).
See Refer to the Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade, Release 6.0 for instructions on performing the ISSU upgrade.

No impact to traffic should occur as a result of the ISSU upgrade.

Step 2 Add Cisco Dynamic Fabric Automation-specific configuration on the spine.
For specific configuration, commands, and samples for the spine, see Migration Configuration, on page 31.

The VNI and border gateway protocol (BGP) will be configured.

What to Do Next

Proceed to Step 2: Upgrading the first pair of border leaves in the topology.

Step 2: Upgrade the Border Leaf Software

In this procedure, you will perform a disruptive in-service software upgrade (ISSU) for the first border leaf pair.

Step 1 Upgrade the first border leaf node from Cisco NX-OS Release 6.0.(2)N2 to Cisco NX-OS Release 7.0.(0)N1(1) using an ISSU disruptive upgrade procedure.Refer to the Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade, Release 6.0 for information on performing an ISSU upgrade.

Step 2 Make sure that the first border leaf comes up fully and becomes operational again, without any unforeseen issues impacting ISSU procedure.

Step 3 Make sure traffic streams are already running intra-vlan, inter-vlan, across PoDs, and that north-bound traffic all remains unaffected.

Step 4 Repeat steps 1-3 for the second border leaf node in the pair.

Although the disruptive upgrade has some effect on traffic, there is no change in the traffic flow.

What to Do Next

Configure the border leaf pair with Cisco Dynamic Fabric Automation-specific configuration.

Step 3: Add Cisco DFA-related Configuration to the First Border Leaf Pair

In this procedure, you will manually configure the first pair of border leafs in the network.

Note For specific configuration commands and examples, see Migration Configuration, on page 31.

Before You Begin

Make sure you have upgraded the border leaf software, as described in Step 2.

Step 1 On the first border leaf switch:

a) Configure an additional hot standby router protocol (HSRP) per virtual local area network (VLAN) with the anycast gateway MAC address with an unused IP adddress.
b) Configure the iBGP router reflector
c) Configure anycast gateway MAC
d) Add a vrf-tenant-profile and configure the virtual network identifier (VNI) under the virtual router
e) Enable traditional forwarding on the switch virtual interfaces (SVIs)
f) Advertise host routes to the BGP route reflector

Step 2 Repeat step 1 a-f for the second border leaf switch in the pair.

There should be no change to the traffic flow after you have configured the border leaf pair.

What to Do Next

Upgrade the software for the second pair of border leaves.

Step 4: Upgrade the Second Border Leaf Pair

In this procedure, you will perform a disruptive in-service software upgrade (ISSU) for the second border leaf pair.

Step 1 Upgrade the second border leaf node in the pair from Cisco NX-OS Release 6.0.(2)N2 to Cisco NX-OS Release 7.0.(0)N1(1) using an ISSU disruptive upgrade procedure.Refer to the Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade, Release 6.0 for information on the ISSU upgrade.

Step 2 Make sure that the border leaf comes up fully and becomes operational again, without any unforeseen issues impacting the ISSU procedure.

Step 3 Make sure traffic streams are already running intra-vlan, inter-vlan, across PoDs, and that north-bound traffic all remains unaffected.

Step 4 Repeat steps 1-3 for the second border leaf node in the pair.

Although the disruptive upgrade has some effect on traffic, there is no change in the traffic flow.

What to Do Next

Configure the border leaf pair with Cisco Dynamic Fabric Automation-specific configuration

Step 5: Add Cisco DFA-related Configuration to the Second Border Leaf Pair

In this procedure, you will manually configure the second pair of border leafs in the network.

Note For specific configuration commands and examples, see Migration Configuration, on page 31.

Before You Begin

Make sure you have upgraded the border leaf software, as described in Step 4.

Step 1 On the first border leaf switch in the pair:

a) Configure an additional hot standby router protocol (HSRP) per virtual local area network (VLAN) with the anycast gateway MAC address with an unused IP address.
b) Configure the iBGP router reflector
c) Configure the anycast-gateway MAC address
d) Add a vrf-tenant-profile and configure the virtual network identifier (VNI) under the virtual router
e) Create switch virtual interfaces (SVIs), if they are not present.
f) Enable anycast-gateway on the SVIs.
g) Enable traditional forwarding on the switch virtual interfaces (SVIs)

h) Advertise host routes to the BGP route reflector

Step 2 Repeat step 1 a-h for the second border leaf switch in the pair.

After you configure the second border leaf pair, the following changes occur:

- All border leafs start to respond to address resolution protocol (ARP) with anycast-gateway MAC addresses.
- Direct forwarding occurs between the border leaf pairs, without going through the Nexus 7000.

The unicast traffic flow and North-South traffic remains unchanged.

What to Do Next

Upgrade the software for FabricPath leaf pair.

Step 6: Upgrade the FabricPath Leaf Pair

In this procedure, you will perform an in-service software upgrade (ISSU) for the FabricPath leaf pair.

Step 1 Upgrade the leaf node from Cisco NX-OS Release 6.0.(2)N2 to Cisco NX-OS Release 7.0.(0)N1(1) using an ISSU upgrade procedure.Refer to the Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade, Release 6.0 for information on performing an ISSU upgrade.

Step 2 Make sure that the first leaf comes up fully and becomes operational again, without any unforeseen issues impacting ISSU procedure.

Step 3 Make sure traffic streams are already running intra-vlan, inter-vlan, across PoDs, and that north-bound traffic all remains unaffected.

Step 4 Repeat steps 1-3 for the second border leaf node in the pair.

There is no change in the traffic flow.

What to Do Next

Configure the border leaf pair with Cisco Dynamic Fabric Automation-specific configuration.

Step 7: Add Cisco DFA Configuration to Layer 2 Leaves

In this procedure, you will configure the FabricPath leafs in the network.

Note For specific configuration commands and examples, see Migration Configuration, on page 31.

Before You Begin

Prior to configuring the Fabric Path leaf, you should have upgraded the software.

Step 1 On the first switch in the pair:

a) Install a L3 license.
b) Enable Cisco DFA.
c) Add the iBGP router reflector client.
d) Add the segment ID and VRF.
e) Add a vrf-tenant-profile and configure the virtual network identifier (VNI) under the virtual router.
f) Create switch virtual interfaces (SVIs) for all VLANs.
g) Enable anycast-gateway for all VLANs.
h) Advertise host routes to the BGP route reflector.
i) Start handling gateway functionality for local hosts.

Step 2 Repeat step 1 a-i for the second border leaf switch in the pair.

If you are migrating a fabric that includes both Nexus 5000 and Nexus 6000 switches:

- Migration is completed if you have upgraded all Nexus 6000 software and enabled Cisco DFA forwarding.
- HSRP/VRRP will remain as long as there are Nexus 5000 leaves in the network.
- In Nexus 5000-involved VLANs and SVIs: VLANs are global, non-segment-id-enabled, and the forwarding mode can be either proxy or anycast gateway.
- In upgraded and configured Nexus 6000-involved VLANs and SVIs: Can be segment-id enabled, and the forwarding mode can be either proxy or anycast gateway.
- Multicast will continue run in the legacy multicast mode. Cisco DFA multicast should not be enabled.

What to Do Next

If you are migrating a fabric that includes both Nexus 5000 and Nexus 6000 switches, the migration is completed if you have upgraded all Nexus 6000 software and enabled Cisco DFA forwarding.

Step 8: Upgrade and Configure All Remaining Leaf Switches

You should perform this procedure on all of the remaining leaf switches in the network. Refer to Steps 6 and 7 for additional information.

Note For specific configuration commands and examples, see Migration Configuration, on page 31.

Step 1 Upgrade the software on all of the remaining leaf switches.

Step 2 Add Cisco DFA-related configuration on all of the remaining leaf switches.

Step 3 Enable anycast-gateway on leaf switches for all VLANs.

What to Do Next

Remove HSRP Configurations on border leaf pairs.

Step 9: Remove HSRP Configurations on Border Leaf Pairs

During the migration, some hosts learn the anycast gateway MAC address as its MAC address for the default gateway. Some hosts will learn the HSRP VMAC as the MAC for the default gateway. We recommend that you wait a couple of hours to make sure that the HSRP VMAC is aged out on all hosts.

Note For specific configuration commands and examples, see Migration Configuration, on page 31.

Before You Begin

You should have completed migration on all leaf switches.

Step 1 Remove HSRP configuration on each border leaf switch.

Step 2 Change the SVI IP address to the VIP.

After you have removed HSRP configurations, migration is complete.

- You can move to Cisco DFA multicast, if preferred. There is no VPC on border leaf connector to external multicast routers.
- SVIs can be switched to proxy forwarding mode, if preferred.
- New VLANs can be segment-id enabled.
- In the all-Nexus 6000 topology, you can move to Cisco DFA multicast, if preferred.

Note Multicast traffic disruption will occur during the move to Cisco DFA multicast. Also, the border leaf that connects to external multicast routers cannot run VPC.

CHAPTER 4

Migration Configuration

This chapter contains the following sections:

- Configuring the BGP Route Reflector on a Spine, page 31
- Configuring the Virtual Network Identifier Range, page 35
- Configuring SVIs and HSRPs on Border Leafs , page 36
- Configuring Border Leaves for DFA , page 39
- Configuring a Host-facing Interface, page 45
- Adding a Tenant (VRF) Instance on a Leaf, page 47
- Adding a Host-facing Tenant Interface (Vlan), page 49
- Removing HSRP Configuration on all Border Leaves, page 51

Configuring the BGP Route Reflector on a Spine

In this procedure, you will add the Cisco Dynamic Fabric Automation-specific BGP configuration on the spine and identify the BGP route reflector.

Before You Begin

Before configuring the Border Gateway Protocol (BGP), you should have upgraded the spine switch software.

SUMMARY STEPS

1. **configure terminal**
2. switch (config) # **feature bgp**
3. switch (config) # **router bgp** *bgp-as*
4. switch (config-router) # **address-family ipv4 unicast**
5. switch (config-router) # **maximum-paths** [**ibgp**]
6. switch (config-router-af) # **additional-paths send**
7. switch (config-router-af) # **additional-paths selection route-map** *All-paths*
8. switch (config-router) # **address-family ipv6 unicast**
9. switch (config-router) # **maximum-paths** [**ibgp**]
10. switch (config-router-af) # **additional-paths send**
11. switch (config-router-af) # **additional-paths selection route-map**
12. switch (config-router) # **address-family vpnv4 unicast**
13. switch (config-router-af) # **additional-paths send**
14. switch (config-router-af) # **additional-paths receive**
15. switch (config-router-af) # **additional-paths selection route-map**
16. switch (config-router) # **address-family vpnv6 unicast**
17. switch (config-router-af) # **additional-paths send**
18. switch (config-router-af) # **additional-paths receive**
19. switch (config-router-af) # **additional-paths selection route-map**
20. switch (config-router) # **neighbor** {*ip-addr* | *ip-prefixlength* | *ipv6-addr* | *ipv6-prefixlength* } [**remote-as** {*as-num* [,*as-num*]}
21. switch (config-router-neighbor) # **address-family ipv4 unicast**
22. switch (config-router-neighbor-af) # **send-community**
23. switch (config-router-neighbor-af) # **send-community** [**extended**]
24. **[route-reflector-client]**
25. switch (config-router-neighbor) # **address-family ipv6 unicast**
26. switch (config-router-neighbor-af) # **send-community** [**extended**]
27. **[route-reflector-client]**
28. switch (config-router-neighbor) # **address-family vpnv4 unicast**
29. switch (config-router-neighbor-af) # **send-community** [**extended**]
30. **[route-reflector-client]**
31. switch (config-router-neighbor-af) # **capability additional-paths receive**
32. switch (config-router-neighbor)**address-family-vpnv6 unicast**
33. switch (config-router-neighbor-af) # **send-community** [**extended**]
34. **[route-reflector-client]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters configuration mode
Step 2	switch (config) # **feature bgp**	Enables the Border Gateway Protocol (BGP). You must enable the BGP feature before you can configure BGP
Step 3	switch (config) # **router bgp** *bgp-as*	Configures a Border Gateway Protocol process for an interface. The as-number is the number of an autonomous system that identifies the router to other BGP routers and tags that the routing information passed along. The AS number can be a 16-bit integer or a 32-bit integer in the form of a higher 16-bit decimal number and a lower 16-bit decimal number in xx.xx format
Step 4	switch (config-router) # **address-family ipv4 unicast**	Enters the address family mode and configures submode commands for the Border Gateway Protocol (BGP)
Step 5	switch (config-router) # **maximum-paths** [**ibgp**]	Controls the maximum number of parallel routes that the Border Gateway Protocol (BGP) can support.
Step 6	switch (config-router-af) # **additional-paths send**	Configures the capability of sending additional paths to and from the BGP peers.
Step 7	switch (config-router-af) # **additional-paths selection route-map** *All-paths*	.
Step 8	switch (config-router) # **address-family ipv6 unicast**	Enter the address family mode and configures submode commands for the BGP.
Step 9	switch (config-router) # **maximum-paths** [**ibgp**]	Controls the maximum number of parallel routes that the BGP can support
Step 10	switch (config-router-af) # **additional-paths send**	Configures the capability of sending additional paths to and from the BGP peers.
Step 11	switch (config-router-af) # **additional-paths selection route-map**	.
Step 12	switch (config-router) # **address-family vpnv4 unicast**	Enters the address family mode and configures submode commands for the Border Gateway Protocol (BGP)
Step 13	switch (config-router-af) # **additional-paths send**	Configures the capability of sending additional paths to and from the BGP peers.
Step 14	switch (config-router-af) # **additional-paths receive**	Configures the capability of receiving additional paths to and from the BGP peers
Step 15	switch (config-router-af) # **additional-paths selection route-map**	.
Step 16	switch (config-router) # **address-family vpnv6 unicast**	Enters the address family mode and configures submode commands for the Border Gateway Protocol (BGP)
Step 17	switch (config-router-af) # **additional-paths send**	Configures the capability of sending additional paths to and from the BGP peers.

	Command or Action	Purpose
Step 18	switch (config-router-af) # **additional-paths receive**	Configures the capability of receiving additional paths to and from the BGP peers
Step 19	switch (config-router-af) # **additional-paths selection route-map**	.
Step 20	switch (config-router) # **neighbor** {*ip-addr* | *ip-prefixlength* | *ipv6-addr* | *ipv6-prefixlength* } [**remote-as** {*as-num* [,*as-num*]}	Configures a BGP neighbor (router, vrf) and enters neighbor configuration mode.
Step 21	switch (config-router-neighbor) # **address-family ipv4 unicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode to configure submode commands for the BGP.
Step 22	switch (config-router-neighbor-af) # **send-community**	Sends a BGP community attribute to a peer.
Step 23	switch (config-router-neighbor-af) # **send-community** [**extended**]	Sends a BGP community attribute to a peer
Step 24	**[route-reflector-client]**	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
Step 25	switch (config-router-neighbor) # **address-family ipv6 unicast**	Enters the address family mode configure submode commands for the BGP.
Step 26	switch (config-router-neighbor-af) # **send-community** [**extended**]	Sends a BGP community attribute to a peer
Step 27	**[route-reflector-client]**	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
Step 28	switch (config-router-neighbor) # **address-family vpnv4 unicast**	Enters the address family mode configure submode commands for the BGP.
Step 29	switch (config-router-neighbor-af) # **send-community** [**extended**]	Sends a BGP community attribute to a peer
Step 30	**[route-reflector-client]**	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
Step 31	switch (config-router-neighbor-af) # **capability additional-paths receive**	Configures BGP to advertise the capability of sending and receiving additional paths to and from the BGP peers.
Step 32	switch (config-router-neighbor)**address-family-vpnv6 unicast**	Enters the address family mode configure submode commands for the BGP.
Step 33	switch (config-router-neighbor-af) # **send-community** [**extended**]	.
Step 34	**[route-reflector-client]**	Configures the router as a BGP route reflector and configures the specified neighbor as its client.

The following example shows a configuration of the BGP route reflector on the spine.

```
switch # configure terminal
switch (config) # feature bgp
switch (config) # router bgp 1.1
 switch (config-router) # router-id 1.1.1.4
 switch (config-router) # address-family ipv4 unicast
  switch (config-router-af) # redistribute hmm route-map AM
  switch (config-router) # maximum-paths ibgp 2
  switch (config-router-af) # additional-paths send
  switch (config-router-af) # additional-paths selection route-map ALL-PATHS
 switch (config-router) # address-family ipv6 unicast
  switch (config-router-af) # maximum-paths ibgp 2
  switch (config-router-af) # additional-paths send
  switch (config-router-af) # additional-paths selection route-map ALL-PATHS
 switch (config-router) # address-family vpnv4 unicast
  switch (config-router-af) # additional-paths send
  switch (config-router-af) # additional-paths receive
  switch (config-router-af) # additional-paths selection route-map ALL-PATHS
 switch (config-router) # address-family vpnv6 unicast
  switch (config-router-af) # additional-paths send
  switch (config-router-af) # additional-paths receive
  switch (config-router-af) # additional-paths selection route-map ALL-PATHS
 switch (config-router) # neighbor 1.1.1.1 remote-as 1.1<--- Route-Reflector Spine IP=1.1.1.1

  switch (config-router-neighbor) # address-family ipv4 unicast
  switch (config-router-neighbor-af) # send-community
   switch (config-router-neighbor-af) # send-community extended
   switch (config-router-neighbor-af) # route-reflector-client
  switch (config-router-neighbor) # address-family ipv6 unicast
   switch (config-router-neighbor-af) # send-community extended
   switch (config-router-neighbor-af) # route-reflector-client
  switch (config-router-neighbor) # address-family vpnv4 unicast
   switch (config-router-neighbor-af) # send-community extended
   switch (config-router-neighbor-af) # route-reflector-client
  switch (config-router-neighbor) # address-family vpnv6 unicast
   switch (config-router-neighbor-af) # send-community extended
   switch (config-router-neighbor-af) # route-reflector-client
```

Configuring the Virtual Network Identifier Range

In this procedure, you will configure the virtual network (VN) segment id of the virtual LAN (VLAN).

Before You Begin

Before the configuring the segment-id, you should have upgraded the spine switch software.

SUMMARY STEPS

1. switch (config) # **install feature-set fabricpath**
2. switch (config) # **feature-set fabricpath**
3. Device (config) # **feature vn-segment-vlan-based**
4. switch (config) # **vni** [*vn-id* | [-*vni-id*]]
5. switch (config-vlan) # **vn-segment** *segment-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch (config) # **install feature-set fabricpath**	Install FabricPath feature set on the switch.
Step 2	switch (config) # **feature-set fabricpath**	Enables the FabricPath feature set on the switch
Step 3	Device (config) # **feature vn-segment-vlan-based**	Enables virtual LAN (VLAN) based virtual network (VN) segment feature on a device when used in global configuration mode. Can be enabled only if the feature-set fabricpath is enabled on the device.
Step 4	switch (config) # **vni** [*vn-id* | [-*vni-id*]]	Configures a virtual network identifier range
Step 5	switch (config-vlan) # **vn-segment** *segment-id*	Configures the virtual network segment id of the virtual LAN (VLAN).

In this example, you configure the segment id 4099.

```
switch (config)# install feature-set fabricpath
switch (config)# feature-set fabricpath
switch (config)# feature vn-segment-vlan-based
switch (config)# vni 300001-3000010
```

What to Do Next

Upgrade the first border leaf pair.

Configuring SVIs and HSRPs on Border Leafs

In this procedure, you will:

- Enable TF fabric forwarding on switched virtual interfaces (SVIs) without vn-segment involvement on both border leaf devices and the same for non-default VRF VLANs
- Enable Hot Standby Routing Protocol (HSRP) VIPs on the border leaf

Before You Begin

Prior to this procedure, you should have upgraded the border leaf software.

SUMMARY STEPS

1. switch (config) # **feature hsrp**
2. switch (config) # **interface** *type-number*
3. switch (config-if) # **no shutdown**
4. switch (config-if) # **no ip redirects**
5. switch (config-if) # **ip address** *ip-address-mask*
6. switch (config-if) # **ipv6 address** {*addr* | [**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*] | **use-link-local-only** }
7. switch (config-if) # **ip router ospf area** *instance-tag* **area** *area-id* [**secondaries none**]
8. switch (config-if) # **fabric forwarding anycast-gateway-mac** *mac-address*
9. switch (config-if) # **hrsp version 2**
10. switch (config-if-hsrp) # **hsrp** *group-number* [**ip4** | **ipv6**]
11. switch (config-if-hsrp) #**preempt** [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync** | *sync-delay*}]
12. switch (config-if-hsrp) # **priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]
13. switch (config-if-hsrp) # **ip** [**autoconfig** | *ip-address* [**secondary**]]
14. switch (config-if-) # **hsrp** *group-number* [**ip4** | **ipv6**]
15. switch (config-if-hsrp) # **mac-address** *mac-address*
16. switch (config-if-hsrp) # **preempt** [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync** | *sync-delay*}]
17. switch (config-if-hsrp) # **priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]
18. switch (config-if-hsrp) # **ip** [**autoconfig** |*ip-address* [**secondary**]]
19. switch (config-if-) # **hsrp** *group-number* [**ip4** |**ipv6**]
20. switch (config-if-hsrp) # **mac-address** *mac-address*
21. switch (config-if-hsrp) # **preempt** [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync**|*sync-delay*}]
22. switch (config-if-hsrp) # **priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]
23. switch (config-if-hsrp) # **ip** [**autoconfig** | *ip-address* [**secondary**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch (config) # **feature hsrp**	Enters Hot Standby Router Protocol (HSRP) configuration mode and enables HSRP.
Step 2	switch (config) # **interface** *type-number*	Specifies an interface type and number.
Step 3	switch (config-if) # **no shutdown**	Disables the shutdown function on an instance of the BGP.
Step 4	switch (config-if) # **no ip redirects**	
Step 5	switch (config-if) # **ip address** *ip-address-mask*	Specifies a primary IP address for an interface.
Step 6	switch (config-if) # **ipv6 address** {*addr*	[**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*]	**use-link-local-only** }	Configures an IPv6 address on an interface.

	Command or Action	Purpose
Step 7	switch (config-if) # **ip router ospf area** *instance-tag* **area** *area-id* [**secondaries none**]	Specifies the Open Shortest Path First (OSPF) instance and area for an interface.
Step 8	switch (config-if) # **fabric forwarding anycast-gateway-mac** *mac-address*	Specifics the MAC address of the server-facing ports across all leaf nodes. The anycast gateway MAC address is used per interface, therefore it is replicated across all the switch virtual interfaces (SVI) that are supporting proxy gateway or anycast gateway.
Step 9	switch (config-if) # **hrsp version 2**	Configures the Hot Standby Redundancy Protocol (HSRP) version 2.
Step 10	switch (config-if-hsrp) # **hsrp** *group-number* [**ip4** | **ipv6**]	Enters HSRP configuration mode and creates an HSRP group.
Step 11	switch (config-if-hsrp) #**preempt** [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync** | *sync-delay*}]	Configures a preemption delay.
Step 12	switch (config-if-hsrp) # **priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]	Sets the priority level within an HSRP group.
Step 13	switch (config-if-hsrp) # **ip** [**autoconfig** | *ip-address* [**secondary**]]	Assigns a virtual address to an HSRP group.
Step 14	switch (config-if-) # **hsrp** *group-number* [**ip4** | **ipv6**]	Enters HSRP configuration mode and creates an HSRP group.
Step 15	switch (config-if-hsrp) # **mac-address** *mac-address*	Configures a static MAC address for a Layer 3 interface.
Step 16	switch (config-if-hsrp) # **preempt** [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync** | *sync-delay*}]	Configures a preemption delay.
Step 17	switch (config-if-hsrp) # **priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]	Sets the priority level within an HSRP group.
Step 18	switch (config-if-hsrp) # **ip** [**autoconfig** |*ip-address* [**secondary**]]	Assigns a virtual address to an HSRP group.
Step 19	switch (config-if-) # **hsrp** *group-number* [**ip4** |**ipv6**]	Enters HSRP configuration mode and creates an HSRP group.
Step 20	switch (config-if-hsrp) # **mac-address** *mac-address*	Configures a static MAC address for a Layer 3 interface.
Step 21	switch (config-if-hsrp) # **preempt** [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync**|*sync-delay*}]	Configures a preemption delay.
Step 22	switch (config-if-hsrp) # **priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]	Sets the priority level within an HSRP group.

	Command or Action	Purpose
Step 23	switch (config-if-hsrp) # **ip** [**autoconfig** | *ip-address* [**secondary**]]	Assigns a virtual address to an HSRP group.

The following example configures the SVI interfaces for default/non-default VRFs, as well associated HSRP and dummy HSRP groups with anycast Gateway MAC addresses.

```
switch (config) # feature hsrp
switch (config) # interface Vlan20
switch (config-if) # no shutdown
switch (config-if) #  no ip redirects
switch (config-if) # ip address 20.1.1.104/24
switch (config-if) # ipv6 address 20:1::104/64
switch (config-if) # ip router ospf 1 area 0.0.0.
switch (config-if) # fabric forwarding mode anycast gateway
switch (config-if) # hsrp version 2
switch (config-if) # hrsp 20
switch (config-if-hsrp) # preempt
switch (config-if-hsrp) # priority 110
switch (config-if-hsrp) # ip 20.1.1.100
switch (config-if) # hsrp 20 ipv6
switch (config-if-hsrp) # preempt
switch (config-if-hsrp) # priority 110
switch (config-if-hsrp) # ip 20.1.1.100
switch (config-if) # hsrp 50
switch (config-if-hsrp) # mac-address DEAD.0000.DEAF
switch (config-if-hsrp) # preempt
switch (config-if-hsrp) # priority 110
switch (config-if-hsrp) # ip 20.1.1.200
switch (config-if) # hsrp 50 ipv6
switch (config-if-hsrp) # mac-address DEAD.0000.DEAF
switch (config-if-hsrp) # preempt
switch (config-if-hsrp) # priority 110
switch (config-if-hsrp) # ip 20.1.1.200
```

Configuring Border Leaves for DFA

Use the following commands to configure an upgraded border leaf.

Before You Begin

Prior to configuring the border leaf, you should have upgraded the border leaf software.

SUMMARY STEPS

1. switch # **configure terminal**
2. switch (config)# **install feature-set fabricpath**
3. switch (config) # **install feature-set fabric**
4. **feature-set fabricpath**
5. switch (config) #**feature-set fabric**
6. switch (config) #**feature fabric** *forwarding*
7. switch (config) #**feature bgp**
8. switch (config) #**feature isis**
9. switch (config) # **feature fabric multicast**
10. switch (config) #**feature vn-segment-vlan-based**
11. switch (config) #**system fabric reserved-vlans** *vlan-id range*
12. switch (config)#**system fabric core-vlans** *vlan-id -subrange*
13. switch (config) #**fabric forwarding identifier** *id*
14. switch (config) #**fabric forwarding anycast-gateway-mac** *mac-address*
15. switch (config) #**fabric forwarding switch-role** [**border**] {**leaf | spine**}
16. switch (config) #**fabricpath domain default**
17. switch (config) #**ip multicast fabric-forwarding**
18. switch (config) #**vlan** *fabric-control-vland-id*
19. switch (config--vlan) #**mode fabricpath**
20. switch (config) #**interface Vlan** *fabric-control-vlan-number*
21. switch (config-if) #**no shutdown**
22. switch (config-if) #**ip address** *ip-address-mask*
23. switch (config-if) #**fabric forwarding** *control-segment*
24. switch (config) #**route-map** *map-tag*
25. switch (config-route-map) #**set path-selection all advertise**
26. switch (config-s) #**ip access-list** *access-list-name*
27. switch (config-s-acl)#**permit ip** *source destination*
28. switch (config) #**ipv6 access-list** *access-list-name*
29. switch (config-acl) #*sequence-number***permit** *protocol*
30. switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]
31. switch (config-route-map) #**match interface** {*interface-type number* [,*interface-type number...*]}
32. switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]
33. switch (config-route-map) #**match ip address** *prefix-list name [prefix-list name..] access-list-name*
34. switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]
35. switch (config-route-map) #**match interface** *{interface-type number[,interface-type number...]}*
36. switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]
37. switch (config-route-map) #**match ip address** *prefix-list name [prefix-list name..] access-list-name*
38. Device (config) #**router bgp** *as-number*
39. Device (config-router) #**address-family ipv4 unicast**

40. Device (config-router-af) #**redistribute hmm route-map** *map-name*
41. switch (config-router-af) #**maximum-paths [ibgp]** *number-paths*
42. switch (config-router-af) #**additional-paths receive**
43. switch (config-router) #**address-family ipv6 unicast**
44. switch (config-router-af) #**redistribute hmm route-map** *map-name*
45. switch (config-router-af) #**maximum-path [ibgp]** *number-paths*
46. switch (config-router-af) #**additional-paths-receive**
47. switch (config) #**address-family vpnv4 unicast**
48. switch (config-router-af) #**additional-paths receive**
49. switch (config-router) #**address-family vpnv6 unicast**
50. switch (config-router-af) #**additional-paths receive**
51. switch (config-router) #**neighbor** {*ip-addr* |*ip-prefixlentgth*} [**remote-as** {*as-num* [,*as-num*] |**route-map** *map name*}
52. switch (config-router-neighbor) #**address-family ipv4 unicast**
53. switch (config-router-neighbor-af) #**send community** *text*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch # **configure terminal**	Enters global configuration mode.
Step 2	switch (config)# **install feature-set fabricpath**	Install FabricPath feature set on the switch.
Step 3	switch (config) # **install feature-set fabric**	
Step 4	**feature-set fabricpath**	
Step 5	switch (config) #**feature-set fabric**	
Step 6	switch (config) #**feature fabric** *forwarding*	Enables the Host Mobility Manager (HMM) and release specific HMM configuration commands.
Step 7	switch (config) #**feature bgp**	Enables the Border Gateway Protocol (BGP). You must enable the BGP feature before you can configure BGP.
Step 8	switch (config) #**feature isis**	Enables intermediate-system-to-intermediate-system (ISIS) for FabricPath core.
Step 9	switch (config) # **feature fabric multicast**	Enables multicast feature.
Step 10	switch (config) #**feature vn-segment-vlan-based**	Enables virtual LAN (VLAN) based virtual network (VN) segment feature on a device when used in global configuration mode. Can be enabled only if the feature-set fabricpath is enabled on the device.
Step 11	switch (config) #**system fabric reserved-vlans** *vlan-id range*	Pre-allocates a range of regular Vlans to be used by the fabric.

	Command or Action	Purpose
Step 12	switch (config)#**system fabric core-vlans** *vlan-id -subrange*	Defines a range of Vlans from within the reserved-vlans to be used as a fabric-control-vlan and tenant bridge-domain-vlans.
Step 13	switch (config) #**fabric forwarding identifier** *id*	Specifies a fabric forwarding identifier.
Step 14	switch (config) #**fabric forwarding anycast-gateway-mac** *mac-address*	Specifies the MAC address of the server-facing ports across all leaf nodes. The anycast gateway MAC address is used per interface, so it is replicated across all the switch virtual interfaces (SVI) that are supporting proxy gateway or anycast gateway.
Step 15	switch (config) #**fabric forwarding switch-role** [**border**] {**leaf** | **spine**}	Defines the switch role. Leaf adds tenant (vrf) functionality; border leaf adds the ability to connect with routers.
Step 16	switch (config) #**fabricpath domain default**	Enters the global FabricPath Layer 2 ISIS configuration mode.
Step 17	switch (config) #**ip multicast fabric-forwarding**	Enables DFA multicast operation in passive mode. Enables PIM passive mode over the fabric, as well as on the host-facing interfaces (without the need for "ip pim sparse-mode" on a leaf. On a border leaf, PIM on the host-facing interfaces is disabled by default.
Step 18	switch (config) #**vlan** *fabric-control-vland-id*	Specifies the VLAN IDs of the allowed FabrichPath VLANs in the anycast bundle.
Step 19	switch (config--vlan) #**mode fabricpath**	Enables the VLAN as a FabricPath VLAN.
Step 20	switch (config) #**interface Vlan** *fabric-control-vlan-number*	Creates the corresponding layer 3 Vlan interface.
Step 21	switch (config-if) #**no shutdown**	Disables the shutdown function on an instance of the BGP.
Step 22	switch (config-if) #**ip address** *ip-address-mask*	Configures the IP address to be used as BGP endpoints.
Step 23	switch (config-if) #**fabric forwarding** *control-segment*	Specifies this interface to be the DFA control-segment. There must only be one interface of this type.
Step 24	switch (config) #**route-map** *map-tag*	Specifies a route map by identifying route map name (map-tag). Maximum size is 63 characters. This mame should be the same as when configuring the BGP additional-paths.
Step 25	switch (config-route-map) #**set path-selection all advertise**	Sets path selection criteria for Border Gateway Protocol (BGP).
Step 26	switch (config-s) #**ip access-list** *access-list-name*	Defines an IP4 access list access control list (ACL) in order to enable filtering for packets.
Step 27	switch (config-s-acl)#**permit ip** *source destination*	Creates an access control list (ACL) rule that permits traffic matching its conditions. The source destination identifies the source network address and the destination network address.
Step 28	switch (config) #**ipv6 access-list** *access-list-name*	Creates an IPv6 access control list (ACL) or enters IP access list configuration mode for a specific ACL.

	Command or Action	Purpose
Step 29	switch (config-acl) #*sequence-number***permit** *protocol*	Configures a permit rule in an IPv6 ACL.
Step 30	switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]	Pre-defines a route-map for redistribution HMM host ruotes. Name should be kept the same as in the BGP **redistribute-hmm route map** command.
Step 31	switch (config-route-map) #**match interface** {*interface-type number* [,*interface-type number...*]}	Matches an interface in a route map. Use match interface command to provide a list of interfaces to match a route against. Route next-hop addresses that are reached by one of these interfaces result in a match for the route map.
Step 32	switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]	Specifies a route map by identifying route map name (map-tag). Maximum size is 63 characters.
Step 33	switch (config-route-map) #**match ip address** *prefix-list name [prefix-list name..] access-list-name*	Distributes routes that have a destination IPv6 network number address that is permitted by a standard access list, an expanded list, or a prefix list, or to perform policy routing on packets.
Step 34	switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]	Specifies a route map by identifying route map name (map-tag). Maximum size is 63 characters.
Step 35	switch (config-route-map) #**match interface** *{interface-type number[,interface-type number...]}*	Matches an interface in a route map. Use match interface command to provide a list of interfaces to match a route against. Route next-hop addresses that are reached by one of these interfaces result in a match for the route map.
Step 36	switch (config) #**route-map** *map-tag* [**deny** | **permit**] [*sequence-number*]	Specifies a route map by identifying route map name (map-tag). Maximum size is 63 characters.
Step 37	switch (config-route-map) #**match ip address** *prefix-list name [prefix-list name..] access-list-name*	Distributes routes that have a destination IPv6 network number address that is permitted by a standard access list, an expanded list, or a prefix list, or to perform policy routing on packets.
Step 38	Device (config) #**router bgp** *as-number*	Configures a Border Gateway Protocol process for an interface. The as-number is the number of an autonomous system that identifies the router to other BGP routers and tags that the routing information passed along. The AS number can be a 16-bit integer or a 32-bit integer in the form of a higher 16-bit decimal number and a lower 16-bit decimal number in xx.xx format.
Step 39	Device (config-router) #**address-family ipv4 unicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode and configures submode commands for the Border Gateway Protocol (BGP).
Step 40	Device (config-router-af) #**redistribute hmm route-map** *map-name*	Enables redistribution of IPv4 and IPv6 Host Mobility Manager (HMM) routes through specific route maps.
Step 41	switch (config-router-af) #**maximum-paths [ibgp]** *number-paths*	Controls the maximum number of parallel routes that the Border Gateway Protocol (BGP) can support.

	Command or Action	Purpose
Step 42	switch (config-router-af) #**additional-paths receive**	Configures the capability of receiving additional paths to and from the BGP peers.
Step 43	switch (config-router) #**address-family ipv6 unicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode and configure submode commands for the Border Gateway Protocol (BGP).
Step 44	switch (config-router-af) #**redistribute hmm route-map** *map-name*	Enables redistribution of IPv4 and IPv6 Host Mobility Manager (HMM) routes through specific route maps.
Step 45	switch (config-router-af) #**maximum-path [ibgp]** *number-paths*	Controls the maximum number of parallel routes that the BGP can support.
Step 46	switch (config-router-af) #**additional-paths-receive**	Configures the capability of receiving additional paths to and from the BGP peers.
Step 47	switch (config) #**address-family vpnv4 unicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode and configure submode commands for the Border Gateway Protocol (BGP).
Step 48	switch (config-router-af) #**additional-paths receive**	Configures the capability of receiving additional paths to and from the BGP peers.
Step 49	switch (config-router) #**address-family vpnv6 unicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode and configure submode commands for the Border Gateway Protocol (BGP).
Step 50	switch (config-router-af) #**additional-paths receive**	Configures the capability of receiving additional paths to and from the BGP peers.
Step 51	switch (config-router) #**neighbor** {*ip-addr* |*ip-prefixlentgth*} [**remote-as** {*as-num* [,*as-num*] |**route-map** *map name*}	Configures a BGP neighbor (router, vrf) and enters neighbor configuration mode.
Step 52	switch (config-router-neighbor) #**address-family ipv4 unicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode to configure submode commands for the BGP.
Step 53	switch (config-router-neighbor-af) #**send community** *text*	Sends a message to the active user session. Text string can be up to 80 alphanumeric characters and is case-sensitive.

The follow example shows the core configuration for a border leaf.

```
N6K4#
!
switch (config)# install feature-set fabricpath
switch (config)# install feature-set fabric
switch (config)# feature-set fabricpath
switch (config)# feature fabric forwarding
switch (config)# feature bgp
switch (config)# feature isis
switch (config)# feature fabric multicast
switch (config)# feature interface-vlan
switch (config)# feature vn-segment-vlan-based

switch (config)# system fabric dynamic-vlans 20-21, 201-202, 1001-1010
switch (config)# system fabric core-vlans 1001-1002
switch (config)# fabric forwarding identifier 100
switch (config)# fabric forwarding anycast-gateway-mac.DEAD.0000.DEAF
switch (config)# fabric forwarding switch-role leaf
switch (config)# fabricpath domain default
switch (config)# ip multicast fabric-forwarding

switch (config)# vlan 1001-1010
switch (config-vlan)# mode fabricpath

switch (config) # interface Vlan1
 switch (config-if) # no shutdown
 switch (config-if) # ip address 1.1.1.4/24
 switch (config-if) # fabric forwarding control-segment

switch (config) # route-map ALL-PATHS permit 10
switch (config-route-map) # set path-selection all advertise

switch (config-s)# ip access-list HOSTS
switch (config-s-acl)# 10 permit ip any any
switch (config-s)# ipv6 access-list hosts-v6
switch (config-s-acl)# 10 permit ipv6 any any

switch (config) # route-map AM deny 10
switch (config-route-map) # match interface Vlan1
switch (config) # route-map AM permit 20
switch (config-route-map) # match ip address HOSTS
switch (config) # route-map hosts-v6 permit 20
switch (config-route-map) # match ipv6 address hosts-v6

switch (config) # router bgp 1.1
 switch (config-router) # address-family ipv4 unicast
  switch (config-router-af) # redistribute hmm route-map AM
  switch (config-router-af) # maximum-paths ibgp 2
  switch (config-router-af) # additional-paths receive
  switch (config-router-af) # additional-paths selection route-map ALL PATHS
 switch (config-router) # address-family ipv6 unicast
  switch (config-router-af) # redistribute hmm route-map hosts-v6
  switch (config-router-af) # maximum-paths ibgp 2
  switch (config-router-af) # additional-paths receive
  switch (config-router-af) # addtional-path seelction route-map ALL PATHS
 switch (config-router) # address-family vpnv4 unicast
  switch (config-router-af) # additional-paths receive
 switch (config-router) # address-family vpnv6 unicast
  switch (config-router-af) # additional-paths receive
 switch (config-router) # neighbor 1.1.1.1 remote-as 1.1
  switch (config-router-neighbor) # address-family ipv4 unicast
   switch (config-router-neighbor-af) # send-community both


N6K4#
```

Configuring a Host-facing Interface

In this procedure, you will:

- Allocate a new VLAN ID and an unused virtual network identifier (VNI) and tie them together
- Create the corresponding layer 3 VLAN interface and put it into the VRF
- Configure the appropriate fabric forwarding mode

SUMMARY STEPS

1. switch (config) # **vlan** *vland-ids*
2. switch (config--vlan) # **mode fabricpath**
3. switch (config-vlan) # **vn-segment** *vni*
4. switch (config-vlan) # **interface** *type-number*
5. switch (config-vlan-if) # **ip address** *p-address-mask*
6. switch (config-vlan-if) # **[ip pim sparse-mode]**
7. switch (config-vlan-if) # **fabric forwarding anycast-gateway-mac** *mac-address*
8. switch (config-vlan-if) # **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch (config) # **vlan** *vland-ids*	Specifies the VLAN IDs of the allowed FabrichPath VLANs in the anycast bundle
Step 2	switch (config--vlan) # **mode fabricpath**	Enables the VLAN as a FabricPath VLAN.
Step 3	switch (config-vlan) # **vn-segment** *vni*	Configures the virtual network (VN) segment id of the VLAN.
Step 4	switch (config-vlan) # **interface** *type-number*	Specifies an interface type and number
Step 5	switch (config-vlan-if) # **ip address** *p-address-mask*	Specifies a primary IP address for an interface
Step 6	switch (config-vlan-if) # **[ip pim sparse-mode]**	
Step 7	switch (config-vlan-if) # **fabric forwarding anycast-gateway-mac** *mac-address*	Specifies the MAC address of the server-facing ports across all leaf nodes. The anycast gateway MAC address is used per interface, so it is replicated across all the switch virtual interfaces (SVI) that are supporting proxy gateway or anycast gateway.
Step 8	switch (config-vlan-if) # **no shutdown**	Disables the shutdown function on an instance of the BGP

The following example adds a host-facing tenant interface (Vlan).

```
switch (config-)# vlan 1001-1010
 switch (config-vlan)# mode fabricpath
 switch (config-vlan)# vn-segment
switch (config-vlan) # interface Vlan1
  switch (config-vlan-if) # ip address 1.1.1.4/24
  switch (config-vlan-if) # [ip pim sparse-model]
 switch (config-vlan-if) # fabric forwarding anycast-gateway-mac DEAD.0000.DEAF
 switch (config-vlan-if) # no shutdown
```

Adding a Tenant (VRF) Instance on a Leaf

In this procedure, you will:

- Configure a profile named "vrf-tenant-profile"
- Allocate a VLAN
- Create a VRF instance
- Configure the route distinguisher and route targets
- Tie the vni/segment ID to the VRF
- Create an L3 VLAN and configure it with the same IP address/mask as the fabric control VLAN interface to map the BGP endpoint and the VRF BD Vlan

SUMMARY STEPS

1. switch # **configure profile** *vrf-tenant-profile*
2. switch # **configure terminal**
3. switch (config-profile) # **apply profile** *vrf-tenant-profile*
4. switch (config-profile) # **vlan** *vland-ids*
5. switch (config--profile-vlan) # **mode fabricpath**
6. switch (config-profile-vlan) # **vn-segment** *vni*
7. switch (config-profile) # **vrf context** *name*
8. switch (config-profile-vrf) # **rd** *route-distinguisher*
9. switch (config-profile-vrf) # **address-family-ipv4 unicast**
10. switch (config-profile-vrf--af) # **route-target import** *route-target-ext-community*
11. switch (config-profile-vrf-af) # **route-target export** *route-target-ext-community*
12. switch (config-profile-vrf) # **vni** [*vni-id* | [-*vni-id*]]
13. switch (config-profile-vrf) # **interface** *type-number*
14. switch (config-profile-if-vrf) # **vrf member** *name*
15. switch (config-profile-if-vrf) # **ip address** *ip-address-mask*
16. switch (config-profile-if-vrf) # **no shutdown**
17. switch (config-profile-if) # **router bgp** *as-number*
18. switch (config-profile-if) # **vrf** *name*
19. switch (config-profile-if-vrf) # **address-family ipv4 multicast**
20. switch (config-profile-if-vrf) # **address-family ipv4 multicast**
21. switch (config-profile-if-vrf-af) # **redistribute hmm route-map** *map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch # **configure profile** *vrf-tenant-profile*	Configures profile and enters configuration profile mode to configure profile parameters.
Step 2	switch # **configure terminal**	Enters global configuration mode.
Step 3	switch (config-profile) # **apply profile** *vrf-tenant-profile*	Applies a configuration profile to configure hosts.
Step 4	switch (config-profile) # **vlan** *vland-ids*	Specifies the VLAN IDs of the allowed FabricPath VLANs in the anycast bundle
Step 5	switch (config--profile-vlan) # **mode fabricpath**	Enables the VLAN as a FabricPath VLAN.
Step 6	switch (config-profile-vlan) # **vn-segment** *vni*	Configures the virtual network (VN) segment id of the VLAN.
Step 7	switch (config-profile) # **vrf context** *name*	Creates a virtual routing and forwarding instances (VRF) and enters VRF configuration mode. The name of the VRF can be any case-sensitive, alphanumeric string up to 32 characters.
Step 8	switch (config-profile-vrf) # **rd** *route-distinguisher*	Creates routing and forwarding tables
Step 9	switch (config-profile-vrf) # **address-family-ipv4 unicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode and configures submode commands for the Border Gateway Protocol (BGP)
Step 10	switch (config-profile-vrf--af) # **route-target import** *route-target-ext-community*	Creates a route-target extended community for a virtual routing and forwarding (VRF) instance
Step 11	switch (config-profile-vrf-af) # **route-target export** *route-target-ext-community*	Creates a route-target extended community for a virtual routing and forwarding (VRF) instance
Step 12	switch (config-profile-vrf) # **vni** [*vni-id* | [-*vni-id*]]	Configures the virtual network identifier (VNI) in global configuration mode. **Note** You can specify a single ID or a range. For example, 4099, 5000-5005
Step 13	switch (config-profile-vrf) # **interface** *type-number*	Specifies an interface type and number
Step 14	switch (config-profile-if-vrf) # **vrf member** *name*	Creates a VPN routing and forwarding instance (VRF) or enters the VRF configuration mode to configure submode commands for the Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS)
Step 15	switch (config-profile-if-vrf) # **ip address** *ip-address-mask*	Specifies a primary IP address for an interface
Step 16	switch (config-profile-if-vrf) # **no shutdown**	Disables the shutdown function on an instance of the BGP
Step 17	switch (config-profile-if) # **router bgp** *as-number*	Configures a Border Gateway Protocol process for an interface. The as-number is the number of an autonomous system that identifies the

	Command or Action	Purpose
		router to other BGP routers and tags that the routing information passed along. The AS number can be a 16-bit integer or a 32-bit integer in the form of a higher 16-bit decimal number and a lower 16-bit decimal number in xx.xx format
Step 18	switch (config-profile-if) # **vrf** *name*	Creates a VPN routing and forwarding instance (VRF) or enters the VRF configuration mode to configure submode commands for the Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS)
Step 19	switch (config-profile-if-vrf) # **address-family ipv4 multicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode and configures submode commands for the Border Gateway Protocol (BGP)
Step 20	switch (config-profile-if-vrf) # **address-family ipv4 multicast**	Enters the address family mode or a virtual routing and forwarding (VRF) address-family mode and configures submode commands for the Border Gateway Protocol (BGP)
Step 21	switch (config-profile-if-vrf-af) # **redistribute hmm route-map** *map-name*	Enables redistribution of IPv4 Host Mobility Manager (HMM) routes through specific route maps

The following example configures the profile name and the adds the tenant vrf profile and associated parameters

```
switch # configure profile vrf-tenant-profile
switch # configure terminal
switch (config-profile)) # apply profile vrf-tenant-profile
switch (config-profile)# vlan 1001-1010
 switch (config-profile-vlan)# mode fabricpath
 switch (config-profile-vlan)# vn-segment
switch (config-profile) # vrf context VRF2
switch (config-profile-vrf) # rd auto
 switch (config-profile-vrf) # address-family ipv4 unicast
  switch (config-profile-vrf-af) #  route-target import 7000:1
  switch (config-profile-vrf-af) #  route-target export 7000:1
switch (config-profile-vrf) # vni 7000
 switch (config-profile-vrf) # interface Vlan1
 switch (config-profile-if-vrf) # vrf VRF2
  switch (config-profile-if-vrf) # ip address 1.1.1.4/24
 switch (config-profile-if-vrf) # no shutdown
switch (config-profile-if) # router bgp 1.1
switch (config-profile-if) # vrf VRF2
  switch (config-profile-if-vrf) # address-family ipv4 multicast
  switch (config-profile-if-vrf) # address-family ipv4 unicast
   switch (config-profile-if-vrf-af) # redistribute hmm route-map AM
```

Adding a Host-facing Tenant Interface (Vlan)

When you add a host-facing tenant interface (Vlan), you:

- Allocate a new Vlan ID and an unused vni and tie them together
- Create the corresponding layer 3 interface, put it into the VRF

- Configure the appropriate fabric forwarding mode

SUMMARY STEPS

1. switch (config) # **vlan** *vland-ids*
2. switch (config--vlan) # **mode fabricpath**
3. switch (config-vlan) # **vn-segment** *vni*
4. switch (config-vlan) # **interface** *type-number*
5. switch (config-vlan-if) # **vrf member** *name*
6. switch (config-vlan-if-vrf) # **ip address** *ip-address-mask*
7. switch (config-vlan-if-vrf) # [**ip pim sparse-mode**]
8. Device (config-vlan-if-vrf) # **fabric forwarding anycast-gateway-mac** *mac-address*
9. switch (config-vlan-if-vrf) # **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch (config) # **vlan** *vland-ids*	Specifies the VLAN IDs of the allowed FabrichPath VLANs in the anycast bundle
Step 2	switch (config--vlan) # **mode fabricpath**	Enables the VLAN as a FabricPath VLAN.
Step 3	switch (config-vlan) # **vn-segment** *vni*	Configures the virtual network (VN) segment id of the VLAN.
Step 4	switch (config-vlan) # **interface** *type-number*	Specifies an interface type and number
Step 5	switch (config-vlan-if) # **vrf member** *name*	Creates a VPN routing and forwarding instance (VRF) or enters the VRF configuration mode to configure submode commands for the Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS)
Step 6	switch (config-vlan-if-vrf) # **ip address** *ip-address-mask*	Specifies a primary IP address for an interface
Step 7	switch (config-vlan-if-vrf) # [**ip pim sparse-mode**]	
Step 8	Device (config-vlan-if-vrf) # **fabric forwarding anycast-gateway-mac** *mac-address*	Specifies the MAC address of the server-facing ports across all leaf nodes. The anycast gateway MAC address is used per interface, so it is replicated across all the switch virtual interfaces (SVI) that are supporting proxy gateway or anycast gateway.
Step 9	switch (config-vlan-if-vrf) # **no shutdown**	Disables the shutdown function on an instance of the BGP

The following adds a host-facing tenant interface (Vlan).

```
switch (config-)# vlan 1001-1010
 switch (config-vlan)# mode fabricpath
switch (config-vlan)# vn-segment
switch (config-vlan) # interface Vlan1
switch (config-vlan-if) # vrf VRF2
 switch (config-vlan-if-vrf) # ip address 1.1.1.4/24
 switch (config-vlan-if-vrf) # [ip pim sparse-model]
switch (config-vlan-if-vrf) # fabric forwarding anycast-gateway-mac DEAD.0000.DEAF
switch (config-vlan-if-vrf) # no shutdown
```

Removing HSRP Configuration on all Border Leaves

During the migration, some hosts will start learning the Anycast Gateway IP/MAC and will start using it. HSRP is required until the last leaf pair is upgraded to DFA configuration.

Note HSRP/VRRP is required as long as there is a Nexus 5000 leaf in the network topology.

In this procedure, you will remove the HSRP configuration on border leaves after you migrated all of the switches.

SUMMARY STEPS

1. switch (config-if-hsrp) # **show running-config interface** *type-number*
2. switch (config-if-hsrp) # **no hsrp** *group-number*
3. switch (config) # **show interface** *type-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch (config-if-hsrp) # **show running-config interface** *type-number*	Shows interface for the VLAN.
Step 2	switch (config-if-hsrp) # **no hsrp** *group-number*	Disables HRSP.
Step 3	switch (config) # **show interface** *type-number*	Shows an interface type and number.

The following example shows how to remove the HSRP configuration on a border leaf.

```
switch (config-if-hsrp) # show running-config interface vlan80

!Command: show running-config interface Vlan80
!Time: Thu Jan 30 05:00:58 2014

version 7.0(0)N1(1)
interface Vlan80
ip address 80.0.0.31/8
hsrp version 2
hsrp 10
 mac-address 2020.0000.00AA
 preempt
 priority 101
 ip 80.0.0.1
hsrp 180
 preempt
 priority 101
 ip 80.1.1.1
switch (config-if-hsrp) # interface vlan 80
switch (config-if-hsrp) # no hsrp 10
switch (configif-hsrp) # show running interface vlan 80

!Command: show running-config interface Vlan80
!Time: Thu Jan 30 05:01:26 2014

version 7.0(0)N1(1)

interface Vlan80
  no shutdown
  ip address 80.0.0.31/8
  hsrp version 2
  hsrp 180
    preempt
    priority 101
    ip 80.1.1.1

switch (config-if-hsrp) # interface vlan 80
switch (config-if-hsrp) # no hsrp 180
switch (configif-hsrp) # show running interface vlan 80

!Command: show running-config interface Vlan80
!Time: Thu Jan 30 05:01:35 2014

version 7.0(0)N1(1)

interface Vlan80
  no shutdown
  ip address 80.0.0.31/8
  hsrp version 2

switch (config-if-hsrp) # interface vlan 80
switch (config-if-hsrp) # no hsrp version 2
```