Nexus Validation Test
Phase 2

Contents

1. Introduction

Cisco Nexus line of Data-center product hardware and software releases must pass Cisco's comprehensive quality assurance process, which includes a multistage approach comprising extensive unit test, feature test, and system-level test. Each successive stage in the process adds increasingly higher levels of complexity in a multidimensional mix of features and topology.

Nexus Validation Test (NVT) has been established as an additional quality assurance stage in order to leverage customer feedback and requirements into the product development cycle. NVT will validate and publish guidelines for deploying NX-OS switching and UCS solutions for datacenter networks.

This document describes the NVT topologies, hardware & software configurations, test procedures and findings. Addendums to this document will be published when NVT completes any future test cycles using the same test topology and procedures.

2. NVT Topology Design Overview

2.1 Network Logical Topology Design Overview

The topologies and test cases validate highly-available data-center networks in order to provide unified fabric and computing services. This is achieved by using Nexus line of switches and UCS B-series servers with features such as vPC and FabricPath.

2.1.1 Description of the Test Network

The following figure illustrates the test network topology, consisting of two datacenter sites interconnected through a public IP cloud. The first data center site is built around Nexus 7000 with Sup 1 and the second data center is built with Sup 2E.

Within each datacenter site the network is split into two halves:

- Nexus 7000 with vPC to Nexus 5000 for access
- Nexus 7000 with FabricPath with Nexus 5000

While the majority of test cases focus on integrated solutions using Nexus switching and UCS products, modular Catalyst switches are also included for interoperability between NX-OS and IOS.

Figure 1 DC1 Topology

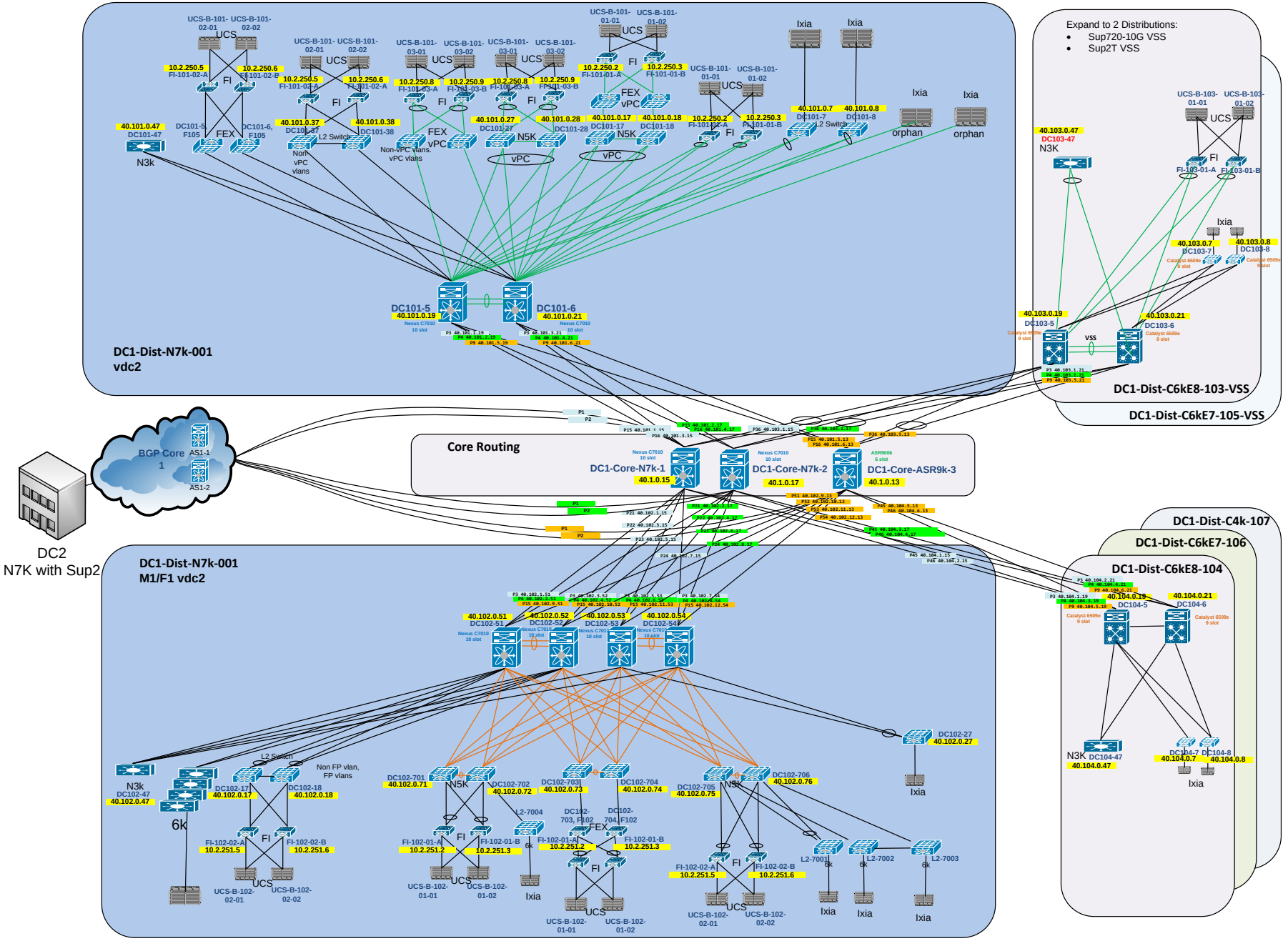
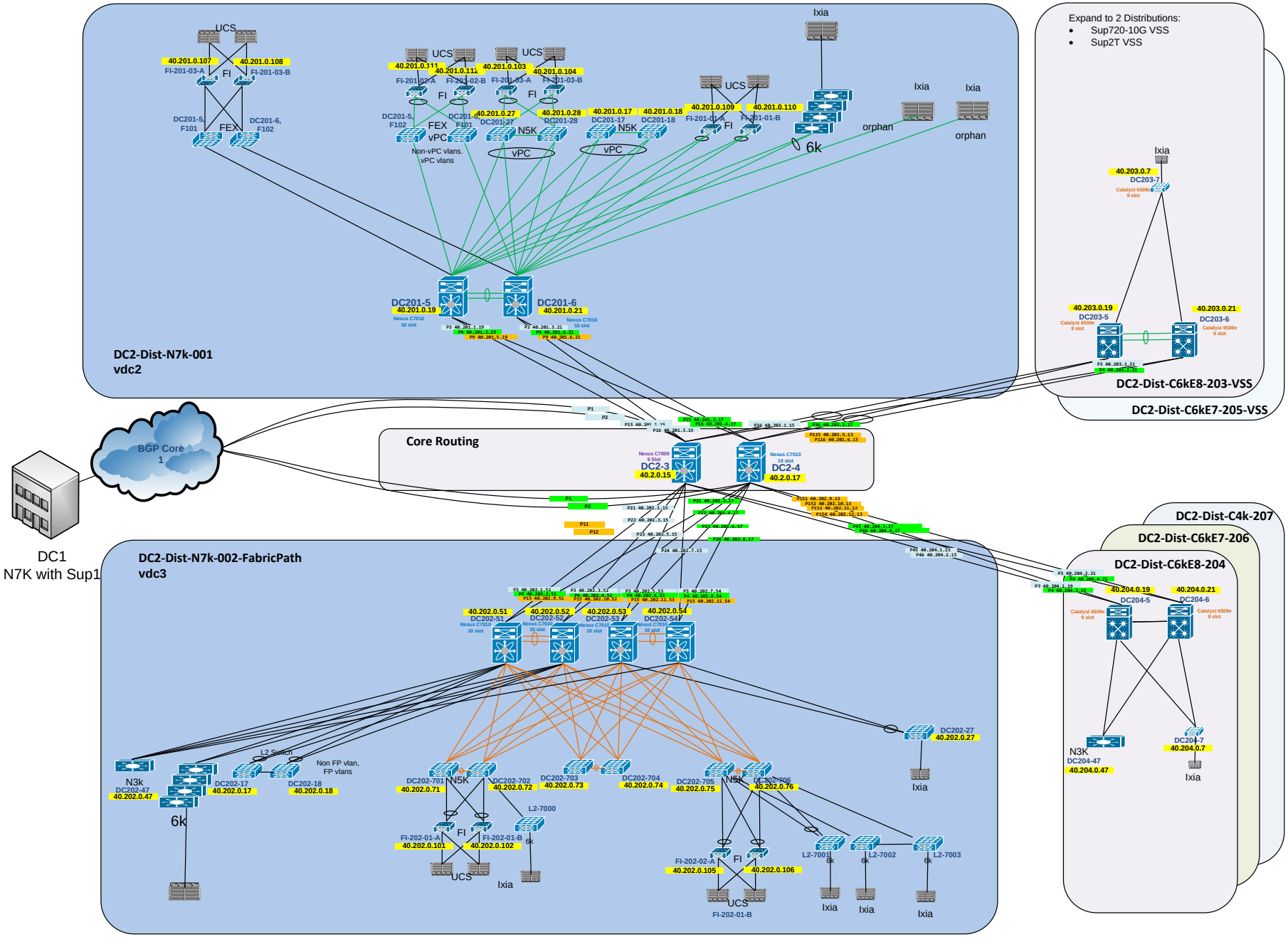


Figure 2 DC2 Topology



2.1.1.1 Core Routing

The core layer provides routing and high bandwidth connectivity between the aggregation-access blocks. The core layer of each datacenter in the test network is implemented using each of the following two platform types to ensure feature parity and interoperability:

- Cisco Nexus 7000 Series Switch
- Cisco ASR 9000

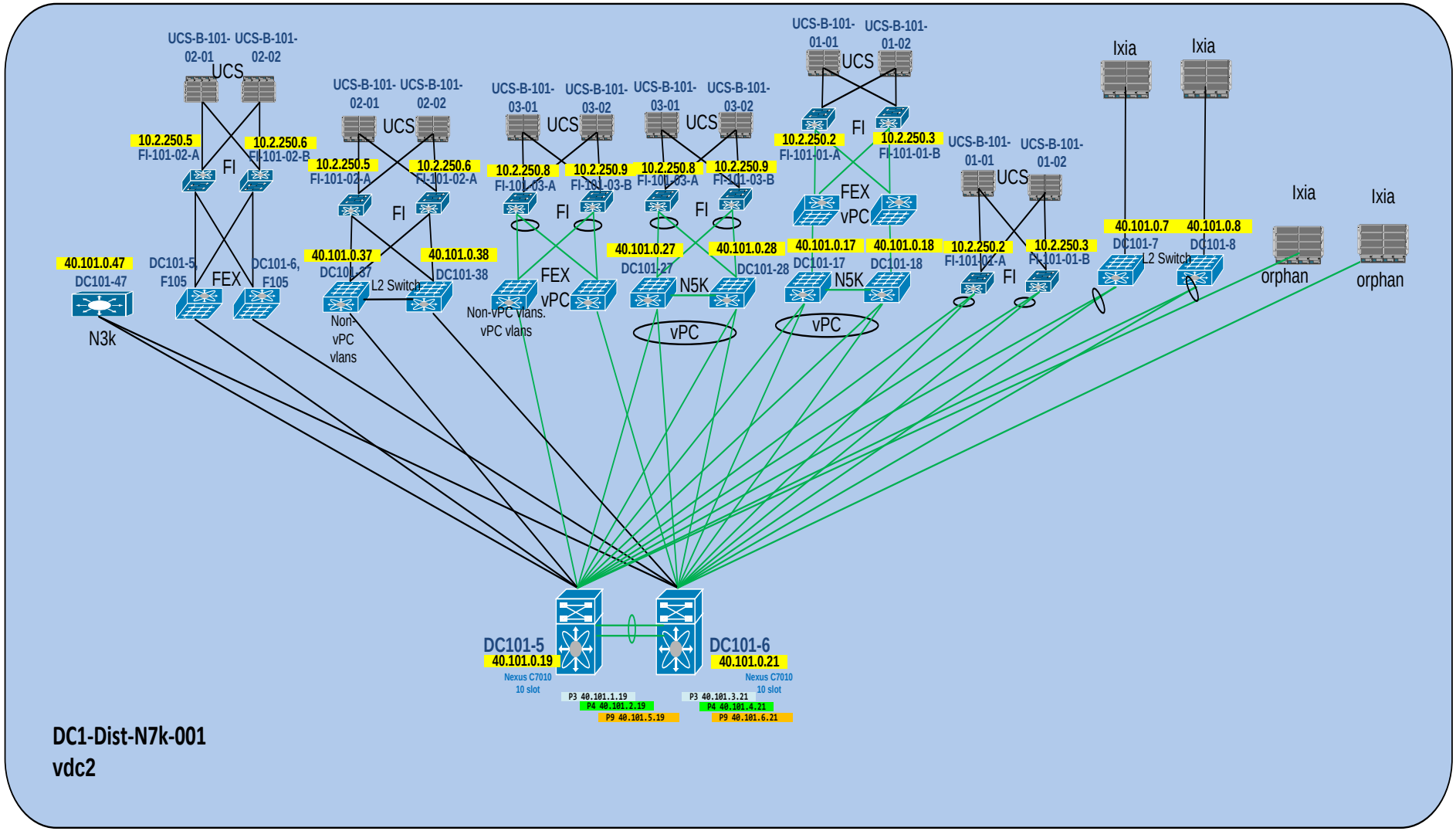
2.1.1.2 Aggregation-Access Blocks

The aggregation-access blocks provide connectivity and policy services for locally attached servers/hosts. These blocks are implemented as follows:

- Block 1: Cisco Nexus 7000 Series Switch with virtual port channel (vPC)
- Block 2: Cisco Nexus 7000 Series Switch with FabricPath (FP)
- Blocks for interoperability with Catalyst platforms

2.1.1.2.1 Block 1: Cisco Nexus 7000 Series Switch with virtual port channel (vPC)

Figure 3 Nexus 7000 vPC Topology



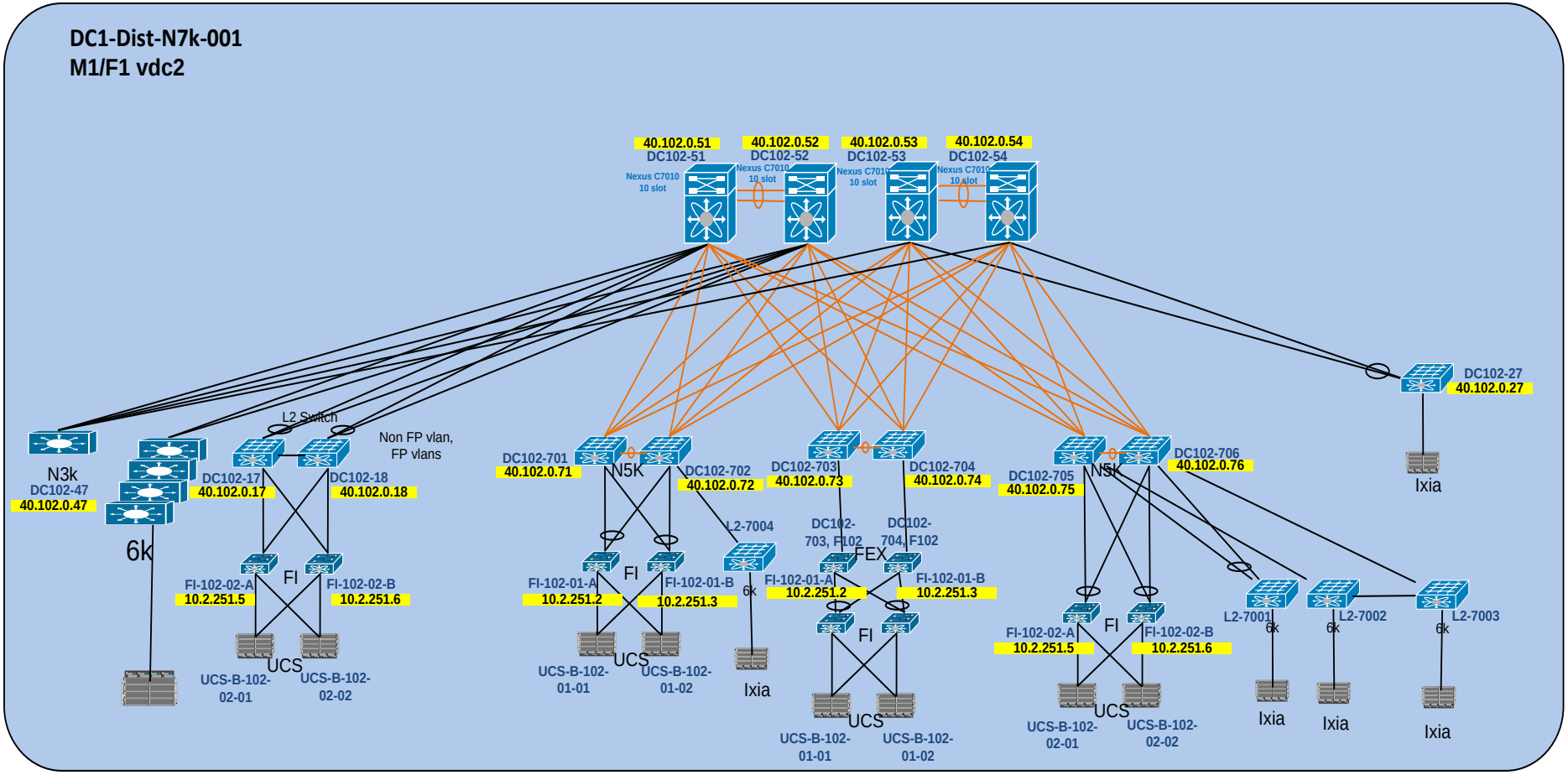
In this block the Nexus 7000 switches are used in vPC configuration on the aggregation level. The following types of Top of Rack devices are deployed:

- ToR FEX vPC: Fabric Extenders are directly attached to Nexus 7000 parent switches as well as the Nexus 5000 parent switches. The host ports are configured as vPC member ports.
- ToR Layer 2 Switch: Layer 2 switches are directly connected to the Nexus 7000 with vPC
- ToR N5k vPC: A pair of Nexus 5000 switches is connected in a dual-sided vPC formation to the Nexus 7000 switches.

UCS B-series chassis are attached to UCS Fabric Interconnect (FI) clusters. The UCS FI clusters are directly connected to the Nexus 7000 switches as well as to the ToRs mentioned above, as shown in Figure 3.

2.1.1.2.2 Block 2: Cisco Nexus 7000 Series Switch with FabricPath (FP)

Figure 4 Nexus 7000 FabricPath Topology



In this block the Nexus 7000 switches are used to form the spine layer for FabricPath. Nexus 5000 switches are deployed as the leaf layer. The following types of Top of Rack devices are deployed:

- ToR N5k FEX vPC+: Fabric Extenders are directly attached to Nexus 5000 parent switches on the FabricPath leaf. The host ports are configured as vPC+ member ports.
- ToR Layer 2 Switch: Layer 2 switches are directly connected to the Nexus 5000 switches on the Fabricpath Leaf.
- ToR Layer 2 Switch vPC+: Layer 2 switches are directly connected to the Nexus 7000 vPC+ on the Fabricpath Spine as well as the Nexus 5000 vPC+ on the FabricPath leaf.
- ToR N3k Layer 3: The Nexus 3000 is deployed as a layer 3 access device. The Nexus 3000 are connected to the spine layer with routed links.

UCS B-series chassis are attached to UCS Fabric Interconnect (FI) clusters. The UCS FI clusters are directly connected to the Nexus 5000 leaf switches as well as some of the ToRs mentioned above, as shown in Figure 4.

2.1.1.2.3 Blocks for interoperability with Catalyst platforms

Blocks 3 to 7 are used to test interoperability of the Catalyst platform switches with the Nexus line of switches

- Block 3: Cisco Catalyst 6500 Series Switch Supervisor Engine 2T VSS
- Block 4: Cisco Catalyst 6500 Series Switch Supervisor Engine 2T
- Block 5: Cisco Catalyst 6500 Series Switch Supervisor Engine 720-10G VSS
- Block 6: Cisco Catalyst 6500 Series Switch Supervisor Engine 720
- Block 7: Cisco Catalyst 4500 Series Switch

UCS B-series chassis are attached to UCS Fabric Interconnect (FI) clusters. The UCS FI clusters are directly connected to Block 3 and Block 6.

The aggregation layer of each datacenter is identical in design to the others to ensure that each of the core platforms interoperates well with all major Cisco modular switching products. The common design allows for the comparison of feature behavior, performance, and scale among the major Cisco modular switching products operating at the aggregation layers.

2.1.2 Test Network Configuration

The following configurations are applied to the test network:

- Common System control, management and accounting: Common system features like SSH, TACACS+, Syslog, SNMP, NTP, SPAN, DNS, NDE are configured.
- BGP: eBGP is configured between the core switches and the public cloud.

- OSPF: OSPF is the IGP running across the network. Each aggregation-access block is configured as a unique area with the core switches playing the role of the ABR.
- PIM-ASM: PIM-Any Source Multicast/PIM-sparse mode is deployed across the network to support multicast. Each aggregation-access block is configured with the RP for the locally sourced groups.
- MSDP Anycast RP: MSDP is deployed to exchange source information between Anycast RPs.
- vPC: vPC technology is deployed in the aggregation-access blocks DC1-Dist-N7k-101 and DC2-Dist-N7k-201 as shown in Figure 1, Figure 2. In addition, dual-sided vPC is configured between the Nexus 7000 and Nexus 5000 switches.
- FP: FabricPath is deployed in the aggregation blocks DC1-Dist-N7k-102 and DC2-Dist-N7k-202. The spine layer is comprised of Nexus 7000 switches and the leaf switches are deployed using Nexus 5000 switches.
- Vlan trunking: VLAN trunking is used in the aggregation-access blocks to maintain segregation and security.
- STP: Rapid Spanning tree protocol is used to prevent layer 2 loops in the aggregation-access blocks. The spanning tree root is placed on the aggregation level. Root guard is configured on the aggregation level to enforce root placement. BPDU Filter, BPDU guard and Portfast edge are configured on the access ports towards hosts.
- HSRP: HSRP is used as the first hop gateway protocol for hosts.
- FEX: Multiple types Fabric Extenders are deployed on Nexus 7000 and Nexus 5000 parent switches.
- IGMP: IGMP is used by hosts to join multicast groups of interest. IGMP snooping is enabled on all switches in the aggregation-access blocks to prevent flooding of multicast data traffic.
- LACP: LACP is used for link aggregation to form port-channels across the network.
- UDLD: UDLD aggressive mode is configured across the network to detect and prevent unidirectional links.
- DHCP relay: DHCP relay is enabled on the aggregation layer to provide IP address services to hypervisors and VMs running on UCS systems.
- End-Host Mode: All of the FI clusters are configured to run in End-Host Mode in order to prevent loops within the topology.
- VM-FEX: VM-FEX has been deployed to provide a direct connection for all of the virtual machine’s network interfaces to the UCS Fabric Interconnect.

2.2 Hardware and Software Overview

2.2.1 Network Hardware and Software version Details

DC 1:

Platform	Model No.	NVT 2.1	NVT 2.2	NVT 2.3
N7K	N7K-SUP1	6.1.3	5.2.9	6.1.4
N5K	N5K-C5548UP-SUP	5.2.1.N1.3	5.2.1.N1.3	5.2.1.N1.3
N3K	N3K-C3048TP-1GE-SUP	5.0.3.U5.1b	5.0.3.U5.1b	5.0.3.U5.1b
ASR9K	A9K-RSP-4G	4.2.3	4.2.3	4.2.3
C6K	VS-SUP2T-10G	150-1.SY3	150-1.SY3	150-1.SY3
	VS-S720-10G	122-33.SXJ4	122-33.SXJ4	122-33.SXJ4
	WS-SUP720	122-33.SXJ4	122-33.SXJ4	122-33.SXJ4
	WS-SUP32-GE	122-33.SXJ	122-33.SXJ	122-33.SXJ
C4K	WS-X45-SUP7-E	03.03.02.SG.151-1.SG2	03.03.02.SG.151-1.SG2	03.03.02.SG.151-1.SG2
	WS-C4948	150-2.SG6-6.9	150-2.SG6-6.9	150-2.SG6-6.9
UCS	UCS-5108	N/A	N/A	N/A
	UCS-B200-M2	N/A	N/A	2.1(1a)B
	UCS-B22-M3	N/A	N/A	2.1(1a)B
	UCS-2208XP-IOM	N/A	N/A	2.1(1a)A
	UCS-6248UP-FI	N/A	N/A	2.1(1a)A
	UCS-6296UP-FI	N/A	N/A	2.1(1a)A
	UCS-M81KR-VIC	N/A	N/A	2.1(1a)B
	UCS-VIC-1280	N/A	N/A	2.1(1a)B

DC 2:

Platform	Model No.	NVT 2.3
N7K	N7K-SUP2E	6.1.4
N5K	N5K-C5548P -SUP	5.2.1.N1.3
	N5K-C5548UP-SUP	5.2.1.N1.4
N3K	N3K-C3548P-10G-SUP	5.0.3.A1.2
C6K	VS-SUP2T-10G	150-1.SY3
	VS-S720-10G	122-33.SXJ4
	WS-SUP720	122-33.SXJ4

C4K	WS-X45-SUP7-E	03.03.02.SG.151-1.SG2
	WS-C4948	150-2.SG6-6.9

2.2.2 Nexus 7000 Line Cards and Fabric Extenders (FEX)

The following line cards are used on the Nexus 7000 devices:

- N7K-M108X2-12L
- N7K-M132XP-12L
- N7K-F132XP-15
- N7K-F248XP-25
- N7K-F248XP-25E

The following types of FEX are utilized in the network:

- N2K-C2224TP-1GE
- N2K-C2248TP-E-1GE
- N2K-C2248TP-1GE
- N2K-C2232PP-10GE

2.2.3 Unified Computing System (UCS) Physical

2.2.3.1 Unified Computing System (UCS) Hardware

The hardware used in the NVT UCS setup contains the following:

- Cisco UCS 6248UP 48-Port Fabric Interconnect
- Cisco UCS 6296UP 96-Port Fabric Interconnect
- UCS 5108 Blade Server Chassis
- UCS 2208XP Fabric Extender (IOM)
- Cisco B200 M2 Blade Server
- Cisco B22 M3 Blade Server
- Cisco M81KR Virtual Interface Card
- Cisco Virtual Interface Card (VIC) 1280

2.2.3.2 Unified Computing System (UCS) Upstream Switch Connectivity

	Fabric Interconnect		**Blade**		**Mezzanine**		**Chassis/ IOM**
DC1	**Cisco UCS 6248UP**	**Cisco UCS 6296UP**	**Cisco B200 M2**	**Cisco B22 M3**	**Cisco UCS VIC 1280**	**Cisco UCS M81KR**	**UCS 5108/ UCS-IOM-2208XP**
N7k vpc (M1) (101-01) DC101-5/6		X		X	X		X

		X	X			X	X
		X		X	X		X
N7k vpc (F1) (101-01) DC101-5/6		X	X			X	X
N7k Fex (101-02) DC101-5/6,F105 (N2K-C2232PP-10GE)		X	X			X	X
N7k Fex vpc (101-03) DC101-5/6,F104 (N2K-C2232PP-10GE)	X		X			X	X
N5k vpc (101-03) DC101-27/28	X		X			X	X
		X		X	X		X
N5k Fex vpc (101-01) DC101-17/18 (N2K-C2224TP-1GE)		X	X			X	X
N5k fabricpath (102-01) DC102-701/702	X	X		X	X		X
	X	X	X			X	X
N5k fabricpath Fex (102-01) DC102-703-704 (N2K-C2232PP-10GE)		X	X			X	X
Cat6k Earl 8 VSS (103-01) DC103-VSS (WS-X6904-40G)	X			X	X		X
Cat6k Earl 7 standalone (106-01) DC106 (WS-X6708-10GE WS-X6704-10GE)	X			X	X		X
L2 Switch 4849 (101-02) DC101-37/38		X	X			X	X
L2 Switch 6509 (102-02) DC102-17/18	X			X		X	X

3. NVT Network Implementation and Configuration

3.1 Configuration of Platform specific features

3.1.1 Licensing

Feature-based licenses enable specific feature sets for the physical device. Any feature not included in a license package is bundled with the Cisco NX-OS software.

License usage on Nexus 7000 in NVT

```
N7K# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                Count
--------------------------------------------------------------------------------
```

```
MPLS_PKG                     Yes   -   In use Never       -
STORAGE-ENT                  No    -   Unused             -
VDC_LICENSES                 No    0   Unused             Grace 119D 23H
ENTERPRISE_PKG               No    -   Unused             -
FCOE-N7K-F132XP              No    0   Unused             -
FCOE-N7K-F248XP              No    0   Unused             -
ENHANCED_LAYER2_PKG          Yes   -   Unused Never       -
SCALABLE_SERVICES_PKG        Yes   -   In use Never       -
TRANSPORT_SERVICES_PKG       Yes   -   In use Never       -
LAN_ADVANCED_SERVICES_PKG    Yes   -   In use Never       -
LAN_ENTERPRISE_SERVICES_PKG  Yes   -   In use Never       -
--------------------------------------------------------------------------------
```

List of Nexus 7000 features activated by licenses used in the NVT testbed

Feature License	Product ID	Features
Enterprise Services Package LAN_ENTERPRISE_SERVICES_PKG	N7K-LAN1K9	• Open Shortest Path First (OSPF) Protocol • Border Gateway Protocol (BGP) • Intermediate System-to-Intermediate System (IS-IS) Protocol (Layer 3 only) • Protocol Independent Multicast (PIM) which includes sparse mode, bidirectional mode, and source-specific mode (SSM) • Multicast Source Discovery Protocol (MSDP) • Policy-Based Routing • Generic routing encapsulation (GRE) tunnel • Enhanced Interior Gateway Routing Protocol (EIGRP)
Advanced Services Package LAN_ADVANCED_SERVICES_PKG	N7K-ADV1K9	Virtual device contexts (VDCs)
VDC Licenses VDC_PKG	N7K-VDC1K9	Increments four VDC licenses that allow the Cisco Nexus 7000 Series Supervisor 2 Enhanced module to support eight VDCs
Scalable Services Package SCALABLE_SERVICES_PKG	N7K-C7004-XL N7K-C7009-XL N7K-C7010-XL N7K-C7018-XL	A single license per system enables all XL-capable I/O modules to operate in XL mode. The license increases the performance of the following features: IPv4 routes IPv6 routes ACL entries
Enhanced Layer 2 Package ENHANCED_LAYER2_PKG	N7K-EL21K9	FabricPath support on the F Series module

License usage on Nexus 5000 in NVT

```
DC202-701# sh license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                Count
--------------------------------------------------------------------------------
FCOE_NPV_PKG                  No    -   Unused             -
```

```
FM_SERVER_PKG                 No    -   Unused             -
ENTERPRISE_PKG                No    -   Unused             -
FC_FEATURES_PKG               No    -   Unused             -
VMFEX_FEATURE_PKG             No    -   Unused             -
ENHANCED_LAYER2_PKG           Yes   -   In use Never       -
LAN_BASE_SERVICES_PKG         Yes   -   In use Never       -
LAN_ENTERPRISE_SERVICES_PKG   No    -   Unused             -
--------------------------------------------------------------------------------
```

List of Nexus 5000 features activated by licenses used in the NVT testbed

Feature License	Product ID	Features
FabricPath Services Package ENHANCED_LAYER2_PKG	N5548-EL2-SSK9 N5596-EL2-SSK9	FabricPath

3.1.2 Common Configs

3.1.2.1 SSH and TACACS+

SSH is enabled in NVT to provide connectivity for network device management. Authentication is provided through TACACS+.

Configuration:

```
feature tacacs+

tacacs-server key 7 "fewhg123"
ip tacacs source-interface loopback0
tacacs-server host 172.28.92.17 key 7 "fewhg123"
aaa group server tacacs+ AAA-Servers
    server 172.28.92.17
    use-vrf management
```

3.1.2.2 CDP and LLDP

CDP is pervasively used on the NVT testbed for inter-device discovery. LLDP is used where CDP is not supported on links to UCS.

3.1.2.3 Syslog

Syslog is used to record all network events on the NVT test bed. Whenever possible, NVT uses a separate management VRF for syslog.

Configuration:

```
logging server 172.28.92.10 7 use-vrf management facility local6
```

3.1.2.4 SNMP

SNMP is used for system monitoring in NVT. Scripts are used to poll the systems asynchronously during the course of all NVT test execution.

Configuration:

```
snmp-server user admin vdc-admin auth md5 0xc2e0f2d24f608fd0cdf3c536652f6353 priv
0xc2e0f2d24f608fd0cdf3c536652f6353 localizedkey
snmp-server user interop vdc-admin auth md5 0xc2e0f2d24f608fd0cdf3c536652f6353 priv
0xc2e0f2d24f608fd0cdf3c536652f6353 localizedkey
```

```
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server community private group vdc-admin
snmp-server community interop group vdc-operator
snmp-server community cisco group vdc-admin
snmp-server community public group vdc-operator
```

3.1.2.5 NTP

NTP is used to sync the clocks on all NVT devices to provide consistent timestamps on all network logs and events.

Configuration:

```
ntp distribute
ntp server 172.28.92.1
ntp commit
```

3.1.2.6 SPAN

SPAN has been enabled on NVT switches to provide packet captures to assist in network debugging.

Configuration:

```
monitor session 1
  source interface port-channel4 rx
  source interface port-channel501 both
  destination interface Ethernet9/41
  destination interface Ethernet9/42
  no shut
```

3.1.2.7 DNS

DNS has been enabled to provide name lookup in NVT network.

Configuration:

```
ip domain-lookup
ip domain-name interop.cisco.com
ip domain-list cisco.com
ip domain-list interop.cisco.com
ip name-server 172.28.92.9 172.28.92.10
```

3.1.2.8 NDE

NetFlow data export is used to identify packet flows for both ingress and egress IP packets and provide statistics based on these packet flows.

Configuration:

```
feature netflow

flow exporter export-out
  destination 172.28.92.112
  transport udp 9991
  source loopback0
  version 9
flow exporter export-out1
```

```
  transport udp 9995
  version 5
flow record my-flow-record
  description custom-flow-record
  match ipv4 source address
  match ipv4 destination address
  match transport destination-port
  collect counter bytes
  collect counter packets
flow monitor my-flow-monitor
  record my-flow-record
  exporter export-out

interface port-channel1
  ip flow monitor my-flow-monitor input

interface port-channel2
  ip flow monitor my-flow-monitor input
```

3.1.2.9 UDLD

UDLD is used to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a device detects a unidirectional link, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can cause a variety of problems, including spanning tree topology loops.

Configuration:

```
feature udld

udld aggressive
```

3.1.2.10 DHCP Relay

DHCP relay is enabled on the aggregation layer to provide IP address services to hypervisors and VMs running on UCS systems.

Configuration:

```
feature dhcp

service dhcp
ip dhcp relay

interface Vlan11
  ip dhcp relay address 94.253.253.2
  ip dhcp relay address 94.1.1.2
```

3.1.3 Out-of-Band Management Network

NVT makes use of out-of-band method to manage the chassis in the network to separate management traffic from production traffic. Specifically, NVT makes use of the mgmt0 ports on the Nexus devices on a separate management vrf.

Configuration:

```
interface mgmt0
  vrf member management
  ip address 10.2.101.21/16
```

3.1.4 CoPP

CoPP is used to control the rate at which packets are allowed to reach the switch CPU.

When the switch comes up first time, there are multiple CoPP configuration templates that are presented: *strict, moderate, lenient, dense*. NVT has chosen the *lenient* template.

NVT phase 1 testing recommended a custom CoPP class that should be added to the chosen CoPP template to enhance PIM source registration performance. For Nexus 7000 6.2.x release a new built-in filter has been added for the same purpose. This addition is highlighted below.

```
class-map type control-plane match-any copp-system-p-class-normal
  match access-group name copp-system-p-acl-mac-dot1x
  match exception multicast directly-connected-sources
  match protocol arp
```

Configuration on Nexus 7000 for release 6.2.x:

```
copp profile lenient
```

Default lenient CoPP on Nexus 7000 for software release 6.2.x as used in NVT

```
policy-map type control-plane copp-system-p-policy-lenient
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 375 ms conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 375 ms conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 680 kbps bc 375 ms conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 680 kbps bc 375 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1500 kbps bc 375 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1800 kbps bc 750 ms conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 375 ms conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 360 kbps bc 375 ms conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1500 ms conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit
  class copp-system-p-class-undesirable
```

```
    set cos 0
    police cir 32 kbps bc 375 ms conform drop violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1060 kbps bc 1500 ms conform transmit violate drop
  class copp-system-p-class-l2-default
    police cir 100 kbps bc 375 ms conform transmit violate drop
  class class-default
    set cos 0
    police cir 100 kbps bc 250 ms conform transmit violate drop
```

Configuration of CoPP on Nexus 7000 software release 6.1.x/5.2.x as used in NVT

```
! In order to update the CoPP configuration on the Nexus 7000, enter the following command to create a
copy of the default configuration:

copp copy profile lenient prefix test

! Enter the following commands to apply the copy to the control plane interface:

control-plane
  service-policy input test-copp-policy-lenient
hardware rate-limiter layer-3 multicast directly-connected disable
ip access-list multicast-source-data
  10 deny ip any 224.0.0.0/24
  20 deny ip any 224.0.1.0/24
  30 permit ip any 224.0.0.0/4
class-map type control-plane match-any multicast-source-data
  match access-group name multicast-source-data


policy-map type control-plane test-copp-policy-lenient
  class test-copp-class-critical
    set cos 7
    police cir 39600 kbps bc 375 ms conform transmit violate drop
  class test-copp-class-important
    set cos 6
    police cir 1060 kbps bc 1500 ms conform transmit violate drop
  class test-copp-class-management
    set cos 2
    police cir 10000 kbps bc 375 ms conform transmit violate drop
  class test-copp-class-normal
    set cos 1
    police cir 680 kbps bc 375 ms conform transmit violate drop
  class test-copp-class-normal-dhcp
    set cos 1
    police cir 680 kbps bc 375 ms conform transmit violate drop
  class test-copp-class-normal-dhcp-relay-response
    set cos 1
    police cir 900 kbps bc 750 ms conform transmit violate drop
  class test-copp-class-redirect
    set cos 1
    police cir 280 kbps bc 375 ms conform transmit violate drop
  class test-copp-class-exception
    set cos 1
    police cir 360 kbps bc 375 ms conform transmit violate drop
  class test-copp-class-monitoring
    set cos 1
    police cir 130 kbps bc 1500 ms conform transmit violate drop
  class test-copp-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit
  class test-copp-class-undesirable
    set cos 0
    police cir 32 kbps bc 375 ms conform drop violate drop
  class test-copp-class-l2-default
    police cir 100 kbps bc 375 ms conform transmit violate drop
  class multicast-source-data
    police cir 1000 kbps bc 250 ms conform transmit violate drop
```

```
  class class-default
    set cos 0
    police cir 100 kbps bc 250 ms conform transmit violate drop
```

Default CoPP on Nexus 5000 as used in NVT

```
DC202-706# show policy-map type control-plane name copp-system-policy-default

  policy-map type control-plane copp-system-policy-default
    class copp-system-class-igmp
      police cir 1024 kbps bc 65535 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-icmp-echo
      police cir 64 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-mcast-miss
      police cir 256 kbps bc 3200000 bytes
    class copp-system-class-excp-ip-frag
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-same-if
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-ttl
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-default
      police cir 512 kbps bc 6400000 bytes
```

Default CoPP on Nexus 3000 as used in NVT

```
dc102-47# sh policy-map type control-plane expand name copp-system-policy

  policy-map type control-plane copp-system-policy
    class copp-s-selfIp
      police pps 500
    class copp-s-default
      police pps 400
    class copp-s-l2switched
      police pps 200
    class copp-s-ping
      police pps 100
    class copp-s-l3destmiss
      police pps 100
    class copp-s-glean
      police pps 500
    class copp-s-l3mtufail
      police pps 100
    class copp-s-ttl1
      police pps 100
    class copp-s-ipmcmiss
      police pps 400
    class copp-s-l3slowpath
      police pps 100
    class copp-s-dhcpreq
      police pps 300
    class copp-s-dhcpresp
      police pps 300
    class copp-s-dai
      police pps 300
    class copp-s-igmp
      police pps 400
    class copp-s-routingProto2
      police pps 1300
    class copp-s-v6routingProto2
      police pps 1300
    class copp-s-eigrp
      police pps 200
    class copp-s-pimreg
      police pps 200
    class copp-s-pimautorp
      police pps 200
    class copp-s-routingProto1
      police pps 1000
    class copp-s-arp
      police pps 200
    class copp-s-ptp
      police pps 1000
    class copp-s-bfd
      police pps 350
    class copp-s-bpdu
      police pps 12000
    class copp-icmp
      police pps 200
    class copp-telnet
      police pps 500
    class copp-ssh
      police pps 500
    class copp-snmp
      police pps 500
    class copp-ntp
      police pps 100
    class copp-tacacsradius
      police pps 400
    class copp-stftp
      police pps 400
```

3.1.5 Rate Limiters

Rate limiters are an additional set of features on Nexus 7000 to prevent undesirable packets from overwhelming the CPU on the supervisor module.

Default values:

```
dc2-3# show hardware rate-limiter

Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters


Module: 3
  R-L Class           Config           Allowed         Dropped            Total
 +------------------+--------+--------------+--------------+-----------------+
  L3 mtu                  500             436              0               436
  L3 ttl                  500          171234         14981787          15153021
  L3 control            10000               0              0                 0
  L3 glean                100             823           6036              6859
  L3 mcast dirconn    Disable
  L3 mcast loc-grp       3000               0              0                 0
  L3 mcast rpf-leak       500             165              0               165
  L2 storm-ctrl       Disable
  access-list-log         100               0              0                 0
  copy                  30000        16351350              0          16351350
  receive               30000         9922819              0           9922819
  L2 port-sec             500               0              0                 0
  L2 mcast-snoop        10000               0              0                 0
  L2 vpc-low             4000               0              0                 0
  L2 l2pt                 500               0              0                 0
  f1 rl-1                4500                              0
  f1 rl-2                1000                              0
  f1 rl-3                1000                              0
  f1 rl-4                 100                              0
  f1 rl-5                1500                              0
  L2 vpc-peer-gw          5000               0              0                 0
  L2 lisp-map-cache       5000               0              0                 0
  L2 dpss                  100               0              0                 0
  L3 glean-fast            100               0              0                 0
```

3.1.6 VDCs and Resource Allocation

VDCs on the Nexus 7000 are used in the NVT testbed to partition a single physical device into multiple logical devices that provide fault isolation, management isolation, address allocation isolation, service differentiation domains, and adaptive resource management.

```
DC6# show vdc

Switchwide mode is m1 f1 m1xl f2 m2xl f2e

vdc_id  vdc_name                        state              mac                type        lc
------  --------                        -----              ----------         ---------   ------
1       DC6                             active             00:23:ac:64:bb:c1  Ethernet    m1 f1 m1xl m2xl
2       DC101-6                         active             00:23:ac:64:bb:c2  Ethernet    m1 f1 m1xl m2xl
3       DC102-52                        active             00:23:ac:64:bb:c3  Ethernet    m1 f1 m1xl m2xl
4       DC102-54                        active             00:23:ac:64:bb:c4  Ethernet    m1 f1 m1xl m2xl
```

Resource allocation for VDC's is done from the main VDC based on the requirements. The configuration used in the NVT testbed is as shown below.

The following command can be used to help estimate the VDC resource allocation:

```
N7k# show routing memory estimate routes 68000 nex 2
Shared memory estimates:
  Current max     16 MB;  13743 routes with 16 nhs
          in-use   7 MB;  23290 routes with  2 nhs (average)
  Configured max  16 MB;  13743 routes with 16 nhs
  Estimate        17 MB;  68000 routes with  2 nhs
```

Configuration:

```
vdc DC6-sup2 id 1
  cpu-share 5
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 96 maximum 96
  limit-resource u6route-mem minimum 24 maximum 24
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
vdc DC201-6 id 2
  limit-resource module-type f2 f2e
  allow feature-set fabricpath
  allow feature-set fex
  allow feature-set mpls
  cpu-share 5
  allocate interface Ethernet1/1-16
  allocate interface Ethernet2/1-16
  allocate interface Ethernet3/1-16
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
vdc DC202-52 id 3
  limit-resource module-type f2 f2e
  allow feature-set fabricpath
  allow feature-set fex
  allow feature-set mpls
  cpu-share 5
  allocate interface Ethernet1/17-32
  allocate interface Ethernet2/17-32
  allocate interface Ethernet3/17-32
  allocate interface Ethernet9/1-48
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
```

```
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
vdc DC202-54 id 4
  limit-resource module-type f2 f2e
  allow feature-set fabricpath
  allow feature-set fex
  allow feature-set mpls
  cpu-share 5
  allocate interface Ethernet1/33-48
  allocate interface Ethernet2/33-48
  allocate interface Ethernet3/33-48
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
```

3.2 Image Upgrade and Downgrade

NVT makes use of ISSU/D to upgrade/downgrade software images whenever possible.

On the Nexus 7000, to check if the process will be disruptive or non-perform *show install all impact system <system_image_name> kickstart <kickstart_image_name>.*

```
DC3-3a# show install all impact system bootflash:n7000-s2-dk9.6.1.2.bin kickstart  n7000-s2-
kickstart.6.1.2.bin
Installer will perform impact only check. Please wait.

Verifying image bootflash:/n7000-s2-kickstart.6.1.2.bin for boot variable "kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/n7000-s2-dk9.6.1.2.bin for boot variable "system".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Extracting "lc1n7k" version from image bootflash:/n7000-s2-dk9.6.1.2.bin.
[####################] 100% -- SUCCESS

Extracting "bios" version from image bootflash:/n7000-s2-dk9.6.1.2.bin.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/n7000-s2-dk9.6.1.2.bin.
[####################] 100% -- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/n7000-s2-kickstart.6.1.2.bin.
[####################] 100% -- SUCCESS


"Running-config contains configuration that is incompatible with the new image (strict incompatibility).
 Please run 'show incompatibility-all system <image>' command to find out which feature needs to be
disabled.".
Pre-upgrade check failed. Return code 0x40930029 (Current running-config is not supported by new image).
```

Running the command *show incompatibility-all system <image-name>* will show the incompatible configuration and the necessary steps needed achieve non-disruptive upgrade/downgrade.

```
DC3-3a# show incompatibility-all system bootflash:n7000-s2-dk9.6.1.2.bin

Checking incompatible configuration(s) for vdc 'DC3-3a':
------------------------------------------------------
The following configurations on active are incompatible with  the system image
1) Service : confcheck , Capability : CAP_FEATURE_ISSD_PRE621_DENIED
Description : ISSD from current image is not supported.
Capability requirement : STRICT
Enable/Disable command : There is no workaround. If ISSD is required, please
configure the boot variables and reload the switch(disruptive).

2) Service : ipqosmgr , Capability : CAP_FEATURE_IPQOS_DCE_TEMPLATE_8E_4Q4Q
Description : The DCE-QoS template 8e-4q4q exists.
Capability requirement : STRICT
Enable/Disable command : Detach template of type 8e-4q4q from all the interfaces and system qos. Remove
DCE-QoS template 8e-4q4q using the command " clear qos policies 8e-4q4q" from default-vdc at the exec mode


Checking dynamic incompatibilities for vdc 'DC3-3a':
----------------------------------------------------
No incompatible configurations

Checking incompatible configuration(s) for vdc 'DC3-3':
------------------------------------------------------
The following configurations on active are incompatible with  the system image
1) Service : confcheck , Capability : CAP_FEATURE_ISSD_PRE621_DENIED
Description : ISSD from current image is not supported.
Capability requirement : STRICT
Enable/Disable command : There is no workaround. If ISSD is required, please
configure the boot variables and reload the switch(disruptive).

2) Service : ipqosmgr , Capability : CAP_FEATURE_IPQOS_DCE_TEMPLATE_8E_4Q4Q
Description : The DCE-QoS template 8e-4q4q exists.
Capability requirement : STRICT
Enable/Disable command : Detach template of type 8e-4q4q from all the interfaces and system qos. Remove
DCE-QoS template 8e-4q4q using the command " clear qos policies 8e-4q4q" from default-vdc at the exec mode


Checking dynamic incompatibilities for vdc 'DC3-3':
----------------------------------------------------
No incompatible configurations

Checking incompatible configuration(s) for vdc 'DC3-1':
------------------------------------------------------
The following configurations on active are incompatible with  the system image
1) Service : confcheck , Capability : CAP_FEATURE_ISSD_PRE621_DENIED
Description : ISSD from current image is not supported.
Capability requirement : STRICT
Enable/Disable command : There is no workaround. If ISSD is required, please
configure the boot variables and reload the switch(disruptive).

2) Service : ipqosmgr , Capability : CAP_FEATURE_IPQOS_DCE_TEMPLATE_8E_4Q4Q
Description : The DCE-QoS template 8e-4q4q exists.
```

```
Capability requirement : STRICT
Enable/Disable command : Detach template of type 8e-4q4q from all the interfaces and system qos. Remove
DCE-QoS template 8e-4q4q using the command " clear qos policies 8e-4q4q" from default-vdc at the exec mode


Checking dynamic incompatibilities for vdc 'DC3-1':
------------------------------------------------
No incompatible configurations
```

The following caveats apply to ISSU/D:

- When performing a software release upgrade or downgrade without ISSU in a system with FEX, the host interface configurations on the FEX will be lost after the reload to activate the new image. An extra step is required to reapply the configuration after the FEX module is fully online (CSCuh58086). A future FEX pre-provisioning feature will take care of this issue (CSCuh57942).
- When performing ISSU process with OTV configuration, the following error was encountered: *Conversion function failed for service "otv" (error-id 0xFFFFFFFF)*
  With OTV configured, ISSU will be disruptive and requires shutting down the overlay interface. An enhancement request has been filed to place a configuration compatibility check and throw a message to disallow the procedure until the overlay interface is shutdown (CSCug73006).

3.3 Routing Design Overview

3.3.1 Unicast Routing Design

3.3.1.1 BGP Routing Design

From edge/core switches to public cloud, NVT has enabled eBGP to establish peering between data center autonomous systems and public cloud autonomous systems to exchange routing updates. BGP policy has been applied to the eBGP peering configuration to control route updates between peers.

NVT has configured route maps to filter the redistribution of OSPF routes from the DC1 and DC2 into BGP. The filters are configured based on IP prefix matching.

NSF is a high availability feature on modular switches running NX-OS or IOS with a redundant supervisor. On the Nexus 7000, data packets are forwarded by the hardware forwarding engines on the linecards. These engines are programmed with information learned from the routing control plane running on the supervisors. If the active supervisor were to fail, the forwarding tables on the linecards are preserved. All interface states are also preserved while the standby supervisor takes over active control of the system. This high availability system prevents any drop in traffic during the failure of the active control plane.

BGP Graceful restart is a BGP feature that prevents disruption to the control and data plane. It allows for the graceful recovery of BGP sessions after a peer has failed. When combined with the NSF feature, any GR capable peers connected to a switch going through supervisor switchover will continue to forward traffic seamlessly.

Nonstop forwarding (NSF) and graceful restart (GR) for BGP are enabled by default on NX-OS. SSO/NSF and graceful restart must be explicitly enabled for the system and for BGP, respectively, for catalyst 6500 and 4500 running IOS.

NVT BGP configuration:

```
feature bgp
router bgp 200
  router-id 40.2.0.15
  graceful-restart stalepath-time 360
  log-neighbor-changes
  address-family ipv4 unicast
    redistribute direct route-map CONN
    redistribute ospf 2 route-map CONN
    maximum-paths 8
    maximum-paths ibgp 8
  neighbor 40.90.201.11 remote-as 100090
    address-family ipv4 unicast
      prefix-list NO_SELF in
  neighbor 40.90.203.13 remote-as 100090
    address-family ipv4 unicast
      prefix-list NO_SELF in
```

3.3.1.2 OSPF Routing Design

OSPF has been chosen as the IGP routing protocol for both NVT DC1 and DC2. OSPF has been deployed from Core to Aggregation to L3 Access in NVT data center.

NVT DC1 and DC2 core switches are configured as backbone Area 0. Each aggregation-access block is configured as a different non-backbone area. The multi-area design reduces computational work for OSPF routers during a topology change.

NVT OSPF configuration:

```
feature ospf
router ospf 2
  router-id 40.2.0.15
  redistribute bgp 200 route-map BGPCORE-TO-DC2
  log-adjacency-changes
  timers throttle spf 100 200 5000
  timers throttle lsa 50 100 300
  auto-cost reference-bandwidth 1000000

interface loopback0
  ip router ospf 2 area 0.0.0.0

interface loopback1
  ip router ospf 2 area 0.0.0.0

interface port-channel15
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 a667d47acc18ea6b
  ip ospf network point-to-point
  ip router ospf 2 area 0.0.0.201
```

3.3.1.2.1 OSPF Router-ID

Each switch in the OSPF routing domain is identified by a Router ID. NVT has configured a loopback interface IP address as OSPF Router-ID for each switch in DC1 and DC2 to identify each OSPF instance. If there is no OSPF Router-ID, NX-OS will choose the available loopback IP address as OSPF Router-ID and if there is no loopback address available, NX-OS will choose the highest interface IP address as OSPF Router-ID. If the interface IP address is used as the OSPF Router-ID, it will cause routing re-convergence when that interface goes down.

Router-ID is configured per OSPF process instance. NVT testing only creates one instance per VDC.

To verify the OSPF router-id:

```
dc2-3# sh ip ospf

 Routing Process 2 with ID 40.2.0.15 VRF default
 Routing Process Instance Number 1

DC201-5# sh ip ospf nei
 OSPF Process ID 2 VRF default
 Total number of neighbors: 7
 Neighbor ID     Pri State            Up Time  Address         Interface
 40.2.0.15         1 FULL/ -          03:32:21 40.201.1.15     Po3
```

3.3.1.2.2 OSPF Reference Bandwidth

The default OSPF Auto-Cost reference bandwidth for calculating OSPF metric is 40Gbps for NX-OS and 100Mbps for IOS. The reference bandwidth should be configured to be the same across the entire network; NVT has configured 100Gpbs as the reference bandwidth.

To verify OSPF reference-bandwidth, using the command:

```
dc2-3# sh ip ospf
 Routing Process 2 with ID 40.2.0.15 VRF default
 Routing Process Instance Number 1
 Stateful High Availability enabled
 Graceful-restart is configured
   Grace period: 60 state: Inactive
   Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an area border and autonomous system boundary.
 Redistributing External Routes from bgp-200
 Administrative distance 110
 Reference Bandwidth is 1000000 Mbps
```

3.3.1.2.3 OSPF Network Type

NVT has configured point-to-point OSPF Network Type on all interfaces between the core and aggregation switches. It removes the OSPF designated router and backup designated router (DR/BDR) election and reduces the OSPF neighbor adjacency negotiation process.

To verify OSPF point-to-point OSPF Network:

```
dc2-3# sh ip ospf interface P15
 port-channel15 is up, line protocol is up
    IP address 40.201.1.15/24, Process ID 2 VRF default, area 0.0.0.201
    Enabled by interface configuration
    State P2P, Network type P2P, cost 50
    BFD is enabled
    Index 1, Transmit delay 1 sec
    1 Neighbors, flooding to 1, adjacent with 1
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello timer due in 00:00:00
    Message-digest authentication, using key id 1
    Number of opaque link LSAs: 0, checksum sum 0

dc2-3# sh ip ospf neighbors
 OSPF Process ID 2 VRF default
 Total number of neighbors: 13
 Neighbor ID     Pri State            Up Time  Address         Interface
 40.201.0.19       1 FULL/ -          03:28:34 40.201.1.19     Po15
 40.201.0.21       1 FULL/ -          03:56:40 40.201.2.21     Po16
```

3.3.1.2.4 OSPF Authentication

Cisco NX-OS supports two authentication methods, simple password authentication and MD5 authentication digest. Authentication can be configured for an OSPFv2 area or per interface.

NVT has configured MD5 authentication for each interface.

To verify OSPF authentication

```
dc2-3# show ip ospf interface p15
 port-channel15 is up, line protocol is up
    IP address 40.201.1.15/24, Process ID 2 VRF default, area 0.0.0.201
```

```
    Enabled by interface configuration
    State P2P, Network type P2P, cost 50
    BFD is enabled
    Index 1, Transmit delay 1 sec
    1 Neighbors, flooding to 1, adjacent with 1
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello timer due in 00:00:01
    Message-digest authentication, using key id 1
    Number of opaque link LSAs: 0, checksum sum 0
```

3.3.1.2.5 Route Redistribution

Route redistribution is configured on Core/Edge switches for both DC1 and DC2 to learn routes from BGP. Route maps are used to control which external routes are redistributed. NVT has configured IP prefix-list to filter IP addresses.

3.3.1.2.6 OSPF High Availability and Graceful Restart

Cisco provides multilevel high-availability architecture for OSPF: Non Stop Routing (NSR) and Graceful Restart (GR) with NSF.

With NSR, OSPF preserves the running state of the protocol data and sessions in persistent memory. If the OSPF application fails or needs to be restarted for any reason, it will restart from the preserved state to ensure that there's no disruption seen by any of its OSPF peers. The internal applications that manage the routing table and hardware forwarding tables will also not experience any failure, allowing for non-disruptive OSPF process restarts.

OSPF GR and NSF allow for non-disruptive failure of the supervisor on Cisco modular switches. On the Nexus 7000, the hardware routing engines are programed per linecard. On active supervisor failure, the forwarding tables on the linecards are preserved while the standby supervisor takes over active control of the system. There's no disruption to packet forwarding during this process. GR prevents OSPF peers from restarting during a supervisor failure; thus, preserving their packet forwarding states. The combination of OSPF GR and SSO/NSF allows the entire network to continue operating seamlessly during a supervisor failure.

OSPF NSR and graceful restart are enabled by default on NX-OS. SSO/NSF and graceful restart must be explicitly enabled for the system and for OSPF, respectively, for catalyst 6500 and 4500 running IOS.

To Verify OSPF graceful restart:

```
dc2-3# sh ip ospf
 Routing Process 2 with ID 40.2.0.15 VRF default
 Routing Process Instance Number 1
 Stateful High Availability enabled
 Graceful-restart is configured
   Grace period: 60 state: Inactive
   Last graceful restart exit status: None
```

3.3.1.2.7 Passive Interfaces

All servers/hosts facing SVIs (Switched Virtual Interfaces) are configured as OSPF passive interfaces. This is to ensure that server farm subnets are advertised into OSPF, while preventing the formation of unnecessary OSPF adjacencies through the access layer.

To verify OSPF passive interface:

```
DC201-5# sh ip ospf interface vlan 12
 Vlan12 is up, line protocol is up
    IP address 201.12.0.19/16, Process ID 2 VRF default, area 0.0.0.201
    Enabled by interface configuration
    State DR, Network type BROADCAST, cost 1000
    Index 9, Passive interface
```

3.3.1.2.8 OSPF Timers and Optimization

NVT has kept the OSPF hello/hold timers at their default values. This allows other resilience features such as SSO/NSF to provide high availability. BFD should be used for networks where fast peer failure detection is desired. NVT has left all OSPF hello/hold timers as default for DC1 and DC2.

To verify OSPF timers and optimization:

```
dc2-3# sh ip ospf

 Routing Process 2 with ID 40.2.0.15 VRF default
 Routing Process Instance Number 1
 Stateful High Availability enabled
 Graceful-restart is configured
   Grace period: 60 state: Inactive
   Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an area border and autonomous system boundary.
 Redistributing External Routes from
   bgp-200
 Administrative distance 110
 Reference Bandwidth is 1000000 Mbps
 SPF throttling delay time of 100.000 msecs,
   SPF throttling hold time of 200.000 msecs,
   SPF throttling maximum wait time of 5000.000 msecs
 LSA throttling start time of 50.000 msecs,
   LSA throttling hold interval of 100.000 msecs,
   LSA throttling maximum wait time of 300.000 msecs
 Minimum LSA arrival 1000.000 msec
 LSA group pacing timer 10 secs
 Maximum paths to destination 8
 Number of external LSAs 74, checksum sum 0x26b5ec
 Number of opaque AS LSAs 0, checksum sum 0
 Number of areas is 8, 8 normal, 0 stub, 0 nssa
 Number of active areas is 8, 8 normal, 0 stub, 0 nssa
 Install discard route for summarized external routes.
 Install discard route for summarized internal routes.
 BFD is enabled
   Area BACKBONE(0.0.0.0) (Inactive)
        Area has existed for 1w5d
        Interfaces in this area: 3 Active interfaces: 3
        Passive interfaces: 0  Loopback interfaces: 2
        No authentication available
        SPF calculation has run 2404 times
         Last SPF ran for 0.000257s
        Area ranges are
        Number of LSAs: 460, checksum sum 0xe018d2
   Area (0.0.0.201)
```

```
        Area has existed for 1w5d
        Interfaces in this area: 2 Active interfaces: 2
        Passive interfaces: 0  Loopback interfaces: 0
        No authentication available
        SPF calculation has run 2404 times
         Last SPF ran for 0.001564s
        Area ranges are
        Number of LSAs: 790, checksum sum 0x17ed452

dc2-3# sh ip ospf interface port-channel 15
 port-channel15 is up, line protocol is up
    IP address 40.201.1.15/24, Process ID 2 VRF default, area 0.0.0.201
    Enabled by interface configuration
    State P2P, Network type P2P, cost 50
    BFD is enabled
    Index 1, Transmit delay 1 sec
    1 Neighbors, flooding to 1, adjacent with 1
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello timer due in 00:00:07
      ACK timer due in 00:00:00
    Message-digest authentication, using key id 1
    Number of opaque link LSAs: 0, checksum sum 0
```

3.3.1.3 Unicast Forwarding Verification

On NX-OS platforms, routing is performed using hardware forwarding engines. The following sequence of commands illustrates verification of the programming of a host on a directly connected subnet on the Nexus 7000.

This switch is the authoritative router for a directly connected subnet on vlan 11: 10.11.0.0/16.

```
DC101-6# show running-config interface vlan 11

!Command: show running-config interface Vlan11
!Time: Fri Aug 30 16:03:24 2013

version 6.1(4a)

interface Vlan11
  ip access-group data_center_v4 in
  ipv6 traffic-filter data_center_v6 in
  no ip redirects
  ip address 101.11.0.21/16
  ip address 101.111.0.21/16 secondary
  ipv6 address 2001:1:101:11::21/64
  ip router ospf 1 area 0.0.0.101
  ip pim sparse-mode
  hsrp version 2
  hsrp 1
    authentication md5 key-string cisco
    preempt delay minimum 120
    priority 200
    ip 101.11.0.1
  hsrp 2
    authentication md5 key-string cisco
    preempt delay minimum 120
    priority 200
    ip 101.111.0.1
  hsrp 101 ipv6
    authentication md5 key-string cisco
    preempt delay minimum 120
    priority 200
    ip 2001:1:101:11::1
  ip dhcp relay address 94.253.253.2
  ip dhcp relay address 94.1.1.2
```

```
   no shutdown
```

The host 101.11.7.1 has been learned via ARP on this subnet.

```
DC101-6# show ip arp 101.11.7.1

Flags: * - Adjacencies learnt on non-active FHRP router
       + - Adjacencies synced via CFSoE
       # - Adjacencies Throttled for Glean
       D - Static Adjacencies attached to down interface

IP ARP Table
Total number of entries: 1
Address         Age       MAC Address     Interface
101.11.7.1      00:04:45  0065.0b07.0100  Vlan11
```

On NX-OS, “show ip route” will also show directly connected host as /32 routes.

```
DC101-6# sh ip route 101.11.7.1

IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

101.11.7.1/32, ubest/mbest: 1/0, attached
    *via 101.11.7.1, Vlan11, [250/0], 00:02:43, am
```

Directly connected host entries are programed as adjacencies for programming in the FIB table.

```
DC101-6# sh ip adjacency 101.11.7.1

Flags: # - Adjacencies Throttled for Glean
       G - Adjacencies of vPC peer with G/W bit

IP Adjacency Table for VRF default
Total number of entries: 1
Address         MAC Address     Pref Source     Interface
101.11.7.1      0065.0b07.0100  50   arp        Vlan11
```

Find the PO interface on which this mac address is learnt

```
DC101-6# sh mac address-table address 0065.0b07.0100
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
* 11       0065.0b07.0100    dynamic   0          F    F  Po7
```

Display PO7 member interface with module information

```
DC101-6# sh port-channel summary | in Po7
7     Po7(SU)     Eth      LACP      Eth8/1(P)
```

Display adjacency index for this route in hardware table

```
DC101-6# sh system internal forwarding ip route 101.11.7.1 module 8
Routes for table default/base

----+---------------------+----------+----------+------+-----------
Dev | Prefix              | PfxIndex | AdjIndex | LIFB | LIF
----+---------------------+----------+----------+------+-----------
 1    101.11.7.1/32          0x4202    0x4300f       0   0x7b
```

Display DMAC entry programmed in adjacency table

```
DC101-6# sh system internal forwarding adjacency module 8 entry 0x4300f  detail
 Device: 1   Index: 0x4300f   DMAC: 0065.0b07.0100 SMAC: 0023.ac64.bbc2
            LIF: 0x7b (Vlan11) DI: 0x0     ccc: 4   L2_FWD: NO  RDT: NO
            packets: 0   bytes: 549755813888zone enforce: 0
```

Display allocated bridge-domain matches in the hardware table

```
DC101-6# sh vlan internal bd-info vlan-to-bd 11

VDC Id  Vlan Id  BD Id
------  -------  -------
2        11       123
```

Display LTL entry for this mac address associated with bridge-domain

```
DC101-6# sh hardware mac address-table 8 vlan 11
FE | Valid| PI|  BD  |      MAC       |  Index| Stat| SW  | Modi| Age| Tmr| GM| Sec| TR| NT| RM| RMA| Cap| Fld|Always
   |      |   |      |                |       |  ic |     | fied|Byte| Sel|   | ure| AP| FY|   |    |TURE|    | Learn
---+------+---+------+----------------+-------+-----+-----+-----+----+----+---+----+---+---+---+----+----+----+------
0    1     1   123   0065.0b07.0100  0x00a2b   0   0x003   0    247   1    0    0   0   0   0    0    0    0    0
```

Display DMAC sent to LTL index for PO7

```
DC101-6# sh system internal pixm info ltl 0x00a2b

PC_TYPE    PORT    LTL      RES_ID       LTL_FLAG      CB_FLAG      MEMB_CNT
------------------------------------------------------------------------------
Normal     Po7     0x0a2b    0x16000006   0x00000000    0x00000002   1
```

3.3.2 Multicast Routing Design with PIM-ASM

Multicast routing has been enabled across the entire NVT network on DC1 and DC2. On NX-OS, multicast routing is enabled by default, while it needs to be explicitly enabled on IOS.

NVT multicast configuration:

```
feature pim
ip pim rp-address 40.2.50.1 group-list 230.2.0.0/16
ip pim rp-address 40.2.50.1 group-list 239.1.1.1/32
ip pim send-rp-announce loopback1 group-list 230.201.0.0/16
ip pim send-rp-discovery loopback1
ip pim ssm range 232.0.0.0/8
ip pim auto-rp forward listen
ip pim pre-build-spt
```

```
interface loopback1
  ip address 40.201.51.1/32
  ip router ospf 2 area 0.0.0.201
  ip pim sparse-mode
```

```
feature msdp
ip msdp originator-id loopback0
ip msdp peer 40.201.0.19 connect-source loopback0

interface loopback0
  ip address 40.201.0.21/32
  ip router ospf 2 area 0.0.0.201
  ip pim sparse-mode
```

3.3.2.1 PIM-ASM Rendezvous Point

The NVT topology relies heavily on vPC and as such PIM Sparse mode has been configured as the protocol of choice for multicast routing. NX-OS does not support PIM SSM and PIM Bidir operating over vPC.

3.3.2.1.1 Auto-RP

The NVT testbed is designed to have an RP for each POD in DC1 and DC2 data centers to support the groups sourced from that particular POD. Each RP is configured on the aggregation switches for a given POD. NVT makes use of Auto-RP to automate distribution of RP information in the network.

To verify PIM RP:

```
DC201-6# sh ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP RPA: 40.207.51.1, uptime: 22:40:53, expires: 00:02:38
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None
RP: 40.2.50.1, (0), uptime: 22:50:21, expires: 00:02:38 (A),
  priority: 0, RP-source: 40.207.51.1 (A), (local), group ranges:
      239.1.1.1/32   230.2.0.0/16
RP: 40.201.51.1*, (0), uptime: 22:48:58, expires: 00:02:38,
  priority: 0, RP-source: 40.207.51.1 (A), group ranges:
      230.201.0.0/16

DC201-6# sh ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
232.0.0.0/8        SSM       -                -
230.2.0.0/16       ASM       40.2.50.1        -
230.201.0.0/16     ASM       40.201.51.1      -
239.1.1.1/32       ASM       40.2.50.1        -
```

3.3.2.1.1.1 Auto-RP Forward Listen

NVT has enabled the Auto-RP listening and forwarding feature so that the Auto-RP mechanism can dynamically inform routers in the PIM domain of the group-to-RP mapping. By default, listening or forwarding of Auto-RP messages is not enabled on NX-OS.

3.3.2.1.2 Static RP

The NVT network is configured with a backup RP on the core routers for all groups in the network. This RP is statically configured on all routers in the network. Auto-RP takes precedence over static RP.

To verify PIM RP:

```
DC201-6# sh ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP RPA: 40.207.51.1, uptime: 22:40:53, expires: 00:02:38
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None
RP: 40.2.50.1, (0), uptime: 22:50:21, expires: 00:02:38 (A),
  priority: 0, RP-source: 40.207.51.1 (A), (local), group ranges:
      239.1.1.1/32   230.2.0.0/16
RP: 40.201.51.1*, (0), uptime: 22:48:58, expires: 00:02:38,
  priority: 0, RP-source: 40.207.51.1 (A), group ranges:
      230.201.0.0/16

DC201-6# sh ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
232.0.0.0/8        SSM       -                -
230.2.0.0/16       ASM       40.2.50.1        -
230.201.0.0/16     ASM       40.201.51.1      -
239.1.1.1/32       ASM       40.2.50.1        -
```

3.3.2.1.3 Anycast RP with MSDP

NVT has configured Anycast RP with MSDP within each POD at the aggregation layer. NVT has also configured Anycast RP with MSDP among the core switches.

NVT Anycast RP and MSDP configuration:

```
N7K aggregation 1:

!Anycast RP configuration
ip pim send-rp-announce loopback1 group-list
230.201.0.0/16
ip pim send-rp-discovery loopback1
interface loopback1
  ip address 40.201.51.1/32
  ip router ospf 2 area 0.0.0.201
  ip pim sparse-mode

! MSDP configuration
ip msdp originator-id loopback0
ip msdp peer 40.201.0.21 connect-source loopback0
interface loopback0
  ip address 40.201.0.19/32
  ip router ospf 2 area 0.0.0.201
  ip pim sparse-mode
```

```
N7K aggregation 2:

!Anycast RP configuration
ip pim send-rp-announce loopback1 group-list
230.201.0.0/16
ip pim send-rp-discovery loopback1
interface loopback1
  ip address 40.201.51.1/32
  ip router ospf 2 area 0.0.0.201
  ip pim sparse-mode

! MSDP configuration
ip msdp originator-id loopback0
ip msdp peer 40.201.0.19 connect-source loopback0
interface loopback0
  ip address 40.201.0.21/32
  ip router ospf 2 area 0.0.0.201
  ip pim sparse-mode
```

To verify MSDP peer and SA_Cache:

```
DC201-5# sh ip msdp sa-cache
MSDP SA Route Cache for VRF "default" - 100 entries
Source          Group           RP              ASN         Uptime
201.11.7.1      230.201.0.1     40.201.0.21     0           16:23:37
```

```
201.11.7.2      230.201.0.1      40.201.0.21      0           16:12:19
201.11.7.3      230.201.0.1      40.201.0.21      0           16:23:37
201.11.7.4      230.201.0.1      40.201.0.21      0           16:12:19
201.11.7.5      230.201.0.1      40.201.0.21      0           16:23:37
201.11.7.6      230.201.0.1      40.201.0.21      0           16:12:19

DC201-5# sh ip msdp sum
MSDP Peer Status Summary for VRF "default"
Local ASN: 0, originator-id: 40.201.0.19

Number of configured peers:  1
Number of established peers: 1
Number of shutdown peers:    0

Peer            Peer        Connection      Uptime/   Last msg  (S,G)s
Address         ASN         State           Downtime  Received  Received
40.201.0.21     0           Established     17:34:46  00:00:35  100
```

3.3.2.2 PIM spt-threshold

NVT has enabled *ip pim spt-threshold infinity* on the last hop non-vPC PIM routers to decrease the multicast entries hardware usage across the network. Nexus 7000 vPC does not support PIM spt-threshold configuration.

3.3.2.3 Multicast Multipath

Cisco NX-OS Multicast multipath is enabled by default and the load sharing selection algorithm is based on the source and group addresses. On Cisco IOS Multicast multipath is disabled by default. When multipath is enabled on Cisco IOS, the default load sharing selection algorithm is source-based. The algorithm on IOS can be configured to match the behavior on NX-OS with the command *"ip multicast multipath s-g-hash basic".*

NVT has enabled multicast multipath across the whole network on all applicable platforms.

3.3.3 Multicast Forwarding Verification

The following sequence of commands illustrates the verification of the Cisco NX-OS multicast L2 and L3 forwarding.

Displays a specific multicast route 230.101.0.1 with incoming interface information

```
DC6-DC101-6# show ip mroute 230.102.0.1
IP Multicast Routing Table for VRF "default"

(*, 230.102.0.1/32), uptime: 00:21:33, igmp ip pim
  Incoming interface: port-channel4, RPF nbr: 40.101.4.17
  Outgoing interface list: (count: 20)
    Vlan2010, uptime: 00:21:28, igmp
    Vlan2004, uptime: 00:21:28, igmp
    Vlan17, uptime: 00:21:28, igmp
    Vlan16, uptime: 00:21:28, igmp
    Vlan15, uptime: 00:21:28, igmp
    Vlan14, uptime: 00:21:28, igmp
    Vlan2009, uptime: 00:21:33, igmp
    Vlan2008, uptime: 00:21:33, igmp
```

```
    Vlan2007, uptime: 00:21:33, igmp
    Vlan2006, uptime: 00:21:33, igmp
    Vlan2005, uptime: 00:21:33, igmp
    Vlan2003, uptime: 00:21:33, igmp
    Vlan2002, uptime: 00:21:33, igmp
    Vlan2001, uptime: 00:21:33, igmp
    Vlan20, uptime: 00:21:33, igmp
    Vlan19, uptime: 00:21:33, igmp
    Vlan18, uptime: 00:21:33, igmp
    Vlan13, uptime: 00:21:33, igmp
    Vlan12, uptime: 00:21:33, igmp
    Vlan11, uptime: 00:21:33, igmp

(102.11.17.1/32, 230.102.0.1/32), uptime: 00:08:48, ip mrib pim
  Incoming interface: port-channel4, RPF nbr: 40.101.4.17
  Outgoing interface list: (count: 20)
    Vlan2010, uptime: 00:08:48, mrib
    Vlan2009, uptime: 00:08:48, mrib
    Vlan2008, uptime: 00:08:48, mrib
    Vlan2007, uptime: 00:08:48, mrib
    Vlan2006, uptime: 00:08:48, mrib
    Vlan2005, uptime: 00:08:48, mrib
    Vlan2004, uptime: 00:08:48, mrib
    Vlan2003, uptime: 00:08:48, mrib
    Vlan2002, uptime: 00:08:48, mrib
    Vlan2001, uptime: 00:08:48, mrib
    Vlan20, uptime: 00:08:48, mrib
    Vlan19, uptime: 00:08:48, mrib
    Vlan18, uptime: 00:08:48, mrib
    Vlan17, uptime: 00:08:48, mrib
    Vlan16, uptime: 00:08:48, mrib
    Vlan15, uptime: 00:08:48, mrib
    Vlan14, uptime: 00:08:48, mrib
    Vlan13, uptime: 00:08:48, mrib
    Vlan12, uptime: 00:08:48, mrib
    Vlan11, uptime: 00:08:48, mrib
```

Display DR information for that interface Vlan11

```
DC101-6# sh ip pim interface brief
PIM Interface Status for VRF "default"
Interface            IP Address      PIM DR Address  Neighbor  Border
                                                     Count     Interface
Vlan11               101.11.0.21     101.11.0.21     1         no
Vlan2001             101.201.0.21    101.201.0.21    1         no
port-channel3        40.101.2.21     40.101.2.21     1         no
port-channel4        40.101.4.21     40.101.4.21     1         no
port-channel9        40.101.6.21     0.0.0.0         0         no
loopback0            40.101.0.21     40.101.0.21     0         no
loopback1            40.101.51.1     40.101.51.1     0         no
```

Displays mroute RPF interface and forwarding counters in L3 hardware table

```
DC6-DC101-6# sh forwarding multicast route group 230.102.0.1 source 102.11.17.1

slot  1
=======


  (102.11.17.1/32, 230.102.0.1/32), RPF Interface: port-channel4, flags:
    Received Packets: 13820 Bytes: 1326720
    Number of Outgoing Interfaces: 20
    Outgoing Interface List Index: 6
      Vlan11 Outgoing Packets:35186683 Bytes:3377921568
      Vlan12 Outgoing Packets:26230679 Bytes:2518145184
      Vlan13 Outgoing Packets:26230679 Bytes:2518145184
```

```
      Vlan14 Outgoing Packets:26230679 Bytes:2518145184
      Vlan15 Outgoing Packets:26230679 Bytes:2518145184
      Vlan16 Outgoing Packets:26230679 Bytes:2518145184
      Vlan17 Outgoing Packets:26230679 Bytes:2518145184
      Vlan18 Outgoing Packets:26230679 Bytes:2518145184
      Vlan19 Outgoing Packets:26230679 Bytes:2518145184
      Vlan20 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2001 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2002 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2003 Outgoing Packets:39346009 Bytes:3777216864
      Vlan2004 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2005 Outgoing Packets:39346028 Bytes:3777218688
      Vlan2006 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2007 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2008 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2009 Outgoing Packets:26230679 Bytes:2518145184
      Vlan2010 Outgoing Packets:26230679 Bytes:2518145184
```

Displays the multicast routing table with packet counts and bit rates for all Sources

```
DC6-DC101-6# sh ip mroute 230.102.0.1 summary
IP Multicast Routing Table for VRF "default"

Total number of routes: 1018
Total number of (*,G) routes: 17
Total number of (S,G) routes: 1000
Total number of (*,G-prefix) routes: 1
Group count: 17, rough average sources per group: 58.8

Group: 230.102.0.1/32, Source count: 400
Source          packets      bytes          aps   pps       bit-rate     oifs
(*,G)           65428        5363312        81    0         0.000   bps  20
102.11.17.1     14727        1207606        81    20        13.186  kbps 20
102.11.17.2     14629        1199578        82    20        13.186  kbps 20
102.11.17.3     14689        1204482        81    20        13.186  kbps 20
```

Display IGMP Snooping groups information for that group

```
DC101-6# sh ip igmp snooping groups 230.102.0.1 vlan 11
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan  Group Address      Ver  Type  Port list
11    230.102.0.1        v2   D     Po7 Po8
```

Displays detected multicast routers for that Vlan

```
DC101-6# sh ip igmp snooping mrouter vlan 11

Type: S - Static, D - Dynamic, V - vPC Peer Link
      I - Internal, F - Fabricpath core port
      U - User Configured
Vlan  Router-port   Type      Uptime      Expires
11    Vlan11        I         02:04:10    never
11    Po5           SVD       01:38:00    00:04:54
```

Displays IGMP Snooping querier information for that Vlan

```
DC101-6# sh ip igmp snooping querier vlan 11
Vlan  IP Address       Version   Expires     Port
11    101.11.0.19      v2        00:03:51    port-channel5
```

Display L2 MFDM software entries for that group/vlan 11

```
DC6-DC101-6# sh forwarding distribution ip igmp snooping vlan 11 group 230.102.0.1
Vlan: 11, Group: 230.102.0.1, Source: 0.0.0.0
  Outgoing Interface List Index: 76
  Reference Count: 12
  Platform Index: 0x7fc7
  Number of Outgoing Interfaces: 4
    port-channel5
    port-channel7
    port-channel8
    Replicator1/2/5

Vlan: 11, Aggregated Group: 230.102.0.1, Source: 0.0.0.0
  Outgoing Interface List Index: 82
  Reference Count: 120
  Platform Index: 0x7fc1
  Number of Outgoing Interfaces: 3
    port-channel5
    port-channel7
    port-channel8
```

Display L2 hardware entry for that group/vlan

```
DC6-DC101-6# sh system internal ip igmp snooping vlan 11 group 230.102.0.1 module 8

VDC: 2
Lookup Mode : IP

Vlan   Group           Source          Epoch   RID   DTL      hwptr     Ref#    GS Entry#
11    230.102.0.1                      1       76    0x7fc7   0x4a3f    1       0
```

Display DTL sent to LTL index for PO7

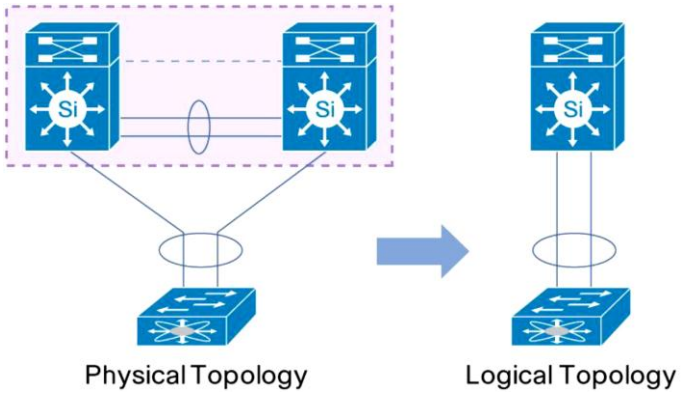
```
DC6-DC101-6# sh system internal pixm info ltl 0x7fc7
MCAST LTLs allocated for VDC:2
==========================================
LTL    IFIDX/RID   LTL_FLAG CB_FLAG
0x7fc7 0x0000004c 0x00     0x0002

mi  | v4_fpoe | v5_fpoe | clp_v4_l2 | clp_v5_l2 | clp20_v4_l3 | clp_cr_v4_l3 | flag | proxy_if_index
0xd | 0xb     | 0x0     | 0x7       | 0x0       | 0x0         | 0x47         | 0x0  | repl1/2/5

Member info
------------------
IFIDX           LTL
---------------------------------
Po8                0x0a2d
Po7                0x0a2b
Po5                0x0a29
```

3.4 Layer-2/ Layer-3 Aggregation/Access Layer Network Design Overview

3.4.1 vPC

A virtual port channel (vPC) allows links that are physically connected to two different Cisco NX-OS switches to appear as a single port channel to a third device. The third device can be a switch, server, or any other networking device that supports link aggregation technology.

Figure 5 Creating a Single Logical Node through vPC (virtual Port Channel) Technology



Typical vPC peers configuration

```
N7K 1:
feature vpc

! vpc domain config
vpc domain 95
  peer-switch
  role priority 200
  peer-keepalive destination 1.1.1.2 source 1.1.1.1
vrf vpc-keepalive
  track 10
  auto-recovery
  ip arp synchronize

! vpc peer-link config
interface port-channel6N7K-2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1-100,2001-
2010,3001-3010,3951-3960
  spanning-tree port type network
  vpc peer-link
! vpc peer-link member config
interface Ethernet1/4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1-100,2001-
2010,3001-3010,3951-3960
  channel-group 6 mode active
  no shutdown

! vpc peer-keepalive config
interface Ethernet1/1
  vrf member vpc-keepalive
  ip address 1.1.1.1/24
  no shutdown

! vpc member port-channel config
interface port-channel7
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,11-20,2001-
2010,3001-3010
  vpc 7
! vpc member port config
interface Ethernet8/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,11-20,2001-
```

```
N7K 1:
feature vpc

! vpc domain config
vpc domain 95
  peer-switch
  role priority 200
  peer-keepalive destination 1.1.1.1 source 1.1.1.2
vrf vpc-keepalive
  track 10
  auto-recovery
  ip arp synchronize

! vpc peer-link config
interface port-channel5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1-100,2001-
2010,3001-3010,3951-3960
  spanning-tree port type network
  vpc peer-link
! vpc peer-link member config
interface Ethernet1/4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1-100,2001-
2010,3001-3010,3951-3960
  channel-group 5 mode active
  no shutdown

! vpc peer-keepalive config
interface Ethernet1/1
  vrf member vpc-keepalive
  ip address 1.1.1.2/24
  no shutdown

! vpc member port-channel config
interface port-channel7
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,11-20,2001-
2010,3001-3010
  vpc 7
! vpc member port config
interface Ethernet8/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,11-20,2001-
```

```
2010,3001-3010
  channel-group 7 mode active
  no shutdown

!vpc object tracking
!! uplinks
track 1 interface port-channel3 line-protocol
track 2 interface port-channel4 line-protocol
!!vpc peer-link
track 3 interface port-channel6 line-protocol
track 10 list boolean or
  object 1
  object 2
  object 3

! PIM prebuild SPT(only for non F2 mode)
ip pim pre-build-spt
```

```
2010,3001-3010
  channel-group 7 mode active
  no shutdown

!vpc object tracking
!! uplinks
track 1 interface port-channel3 line-protocol
track 2 interface port-channel4 line-protocol
!!vpc peer-link
track 3 interface port-channel5 line-protocol
track 10 list boolean or
  object 1
  object 2
  object 3

! PIM prebuild SPT(only for non F2 mode)
ip pim pre-build-spt
```

Display vPC status:

```
N7K-2# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 95
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 108
Track object                      : 10
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po5    up     1-100,2001-2010,3001-3010,3951-3960

vPC status
----------------------------------------------------------------------
id   Port      Status Consistency Reason                Active vlans
--   ----      ------ ----------- ------                ------------
7    Po7       up     success     success                  1,11-20,200
                                                         1-2010,3001
                                                         -3010
8    Po8       up     success     success                  1,11-20,200
                                                         1-2010,3001
```

3.4.1.1 LACP

NVT makes use of LACP mode active for all link aggregation.

Display port-channels and link aggregation protocol information:

```
N7K-2# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
```

```
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
3     Po3(RU)     Eth      LACP      Eth1/3(P)    Eth1/5(P)
4     Po4(RU)     Eth      LACP      Eth1/2(P)    Eth1/6(P)
5     Po5(SU)     Eth      LACP      Eth1/4(P)    Eth1/7(P)
7     Po7(SU)     Eth      LACP      Eth8/1(P)
8     Po8(SU)     Eth      LACP      Eth8/2(P)
DC6-DC101-6# show lacp interface ethernet 8/1
Interface Ethernet8/1 is up
  Channel group is 7 port channel is Po7
  PDUs sent: 2381
  PDUs rcvd: 2577
  Markers sent: 0
  Markers rcvd: 0
  Marker response sent: 0
  Marker response rcvd: 0
  Unknown packets rcvd: 0
  Illegal packets rcvd: 0
Lag Id: [ [(7f9b, 0-23-4-ee-be-5f, 8007, 0, 0), (8000, 0-1b-90-25-44-0, 6, 0, 0)] ]
Operational as aggregated link since Tue Aug 13 12:15:43 2013

Local Port: Eth8/1   MAC Address= 0-23-ac-64-bb-c2
  System Identifier=0x8000,  Port Identifier=0x8000,0x801
  Operational key=32775
  LACP_Activity=passive
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
  Partner information refresh timeout=Long Timeout (90s)
Actor Admin State=60
Actor Oper State=60
Neighbor: 0x103
  MAC Address= 0-1b-90-25-44-0
  System Identifier=0x8000,  Port Identifier=0x8000,0x103
  Operational key=6
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
Partner Admin State=61
Partner Oper State=61
Aggregate or Individual(True=1)= 1
```

3.4.1.2 VLAN Trunking

NVT makes use of VLAN trunking in the aggregation-access blocks to provide security and segregation. Cisco devices make use of some vlans for internal use. These vlans must not be used externally by the network.

Display vlan information for Nexus 7000:

```
N7K-2# show vlan internal usage

VLANs                   DESCRIPTION
--------------------    -----------------
3968-4031               Multicast
4032-4035,4048-4059     Online Diagnostic
```

```
4036-4039,4060-4087     ERSPAN
4042                    Satellite
4040                    Fabric scale
3968-4095               Current
N7K-2# show vlan id 11

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
11   VLAN0011                         active    Po5, Po7, Po8, Po17, Po27, Po71
                                                Po72, Po73, Po74, Po77, Po78
                                                Po201, Po221, Po401, Po421
                                                Po441, Po501, Po521, Eth1/4
                                                Eth1/7, Eth8/1, Eth8/2, Eth8/16
                                                Eth8/18, Eth8/29, Eth8/30
                                                Eth9/42, Eth10/31, Eth102/1/1
                                                Eth102/1/21, Eth102/1/41
                                                Eth104/1/25, Eth104/1/26
                                                Eth104/1/27, Eth104/1/28
                                                Eth104/1/29, Eth104/1/30
                                                Eth104/1/31, Eth104/1/32

VLAN Type         Vlan-mode
---- -----        ----------
11   enet         CE

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  -----------------------------------------
```

Display vlan information for Nexus 5000:

```
DC202-701# sh vlan internal usage

VLANs                   DESCRIPTION
--------------------    -----------------
3968-4031               Multicast
4032-4035               Online Diagnostic
4036-4039               ERSPAN
4042                    Satellite
3968-4047,4094          Current
```

Display vlan information for Nexus 3000:

```
DC202-47# sh vlan internal usage

VLAN        DESCRIPTION
---------   ----------------------------------------------------------
3968-4031   Multicast
4032        Online diagnostics vlan1
4033        Online diagnostics vlan2
4034        Online diagnostics vlan3
4035        Online diagnostics vlan4
4036-4047   Reserved
4094        Reserved
```

3.4.1.3 Spanning Tree

vPC technology helps build a loop free topology by leveraging port-channels from access devices to the vPC domain. A port-channel is seen as a logical link from the spanning tree's standpoint, so a vPC

domain with vPC-attached access devices forms a star topology at L2 (there are no STP blocked ports in this type of topology). In this case, STP is used as a fail-safe mechanism to protect against any network loops caused by human error (like plugging a loopback cable across the 2 vPC peer device).

NVT makes use of Rapid-PVST which is the default spanning tree protocol on NX-OS. For networks with larger logical port counts, MST is recommended.

Display spanning tree information:

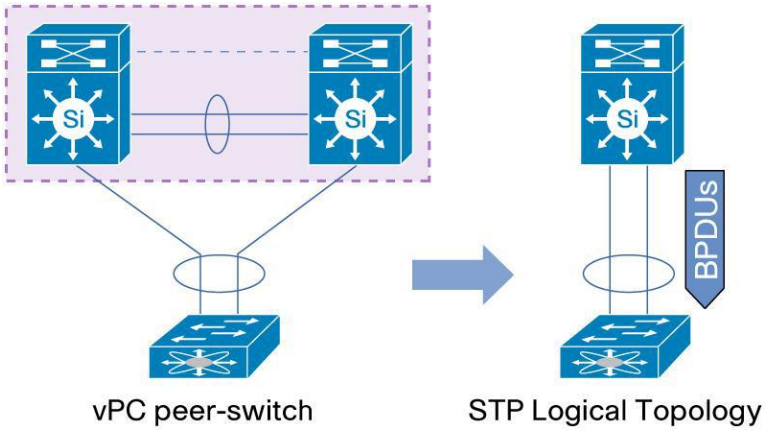
```
N7K-2# show spanning-tree vlan 11

VLAN0011
  Spanning tree enabled protocol rstp
  Root ID    Priority    24587
             Address     0023.04ee.be5f
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24587  (priority 24576 sys-id-ext 11)
             Address     0023.04ee.be5f
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po5              Desg FWD 1000      128.4100 (vPC peer-link) Network P2p
Po7              Desg FWD 200       128.4102 (vPC) P2p
Po8              Desg FWD 200       128.4103 (vPC) P2p
Po17             Desg FWD 200       128.4112 (vPC) P2p
Po71             Desg FWD 200       128.4166 (vPC) Edge P2p
Po77             Desg FWD 200       128.4172 (vPC) Edge P2p
Po78             Desg FWD 200       128.4173 (vPC) Edge P2p
Eth102/1/1       Desg FWD 20000     128.4197 Edge P2p
Eth102/1/21      Desg FWD 20000     128.4197 Edge P2p
Eth102/1/41      Desg FWD 20000     128.4197 Edge P2p

N7K-2# show spanning-tree summary totals
Switch is in rapid-pvst mode
Root bridge for: VLAN0001-VLAN0006, VLAN0009-VLAN0100, VLAN2001-VLAN2010
  VLAN3001-VLAN3010, VLAN3951-VLAN3960
Port Type Default                        is disable
Edge Port [PortFast] BPDU Guard Default  is disabled
Edge Port [PortFast] BPDU Filter Default is disabled
Bridge Assurance                         is enabled
Loopguard Default                        is disabled
Pathcost method used                     is long
vPC peer-switch                          is enabled (operational)
STP-Lite                                 is enabled

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
130 vlans                   0         0        0        488        488
```

3.4.1.3.1 vPC Peer-Switch Feature

The vPC Peer-Switch feature allows a pair of vPC peer devices to appear as a single Spanning Tree Protocol root in the Layer 2 topology (they have the same bridge ID). vPC peer-switch must be configured on both vPC peer devices to become operational.

This feature simplifies Spanning Tree Protocol configuration by configuring vPC VLANs on both peer devices with the same Spanning Tree Protocol priority. A vPC Peer-Switch eliminates the need to map the Spanning Tree Protocol root to the vPC primary peer device.

Figure 6 vPC Peer-switch



3.4.1.4 Configuration Parameters Consistency

After the vPC feature is enabled and the vPC peer-link on both peer devices is configured, Cisco Fabric Services messages provide a copy of the local vPC peer device configuration to the remote vPC peer device. The systems then determine whether any of the crucial configuration parameters differ on the two devices.

When a Type 1 inconsistency check is detected, the following actions are taken:

- For global configuration type 1 inconsistency check, all vPC member ports are set to down state.
- For vPC interface configuration type 1 inconsistency check, the misconfigured vPC is set to down state.

When a Type 2 inconsistency check is detected, the following actions are taken:

- For global configuration type 2 inconsistency check, all vPC member ports remain in up state and vPC systems trigger protective actions.
- For vPC interface configuration type 2 inconsistency check, the misconfigured vPC remains in up state. However, depending on the discrepancy type, vPC systems will trigger protective actions. The most typical misconfiguration deals with the allowed VLANs in the vPC interface trunking configuration. In this case, vPC systems will disable the vPC interface VLANs that do not match on both sides.

Display vPC consistency parameters:

```
N7K-2# show vpc consistency-parameters global

    Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
STP Mode                    1     Rapid-PVST             Rapid-PVST
```

```
STP Disabled                1     None                    None
STP MST Region Name         1     ""                      ""
STP MST Region Revision     1     0                       0
STP MST Region Instance to  1
 VLAN Mapping
STP Loopguard               1     Disabled                Disabled
STP Bridge Assurance        1     Enabled                 Enabled
STP Port Type, Edge         1     Normal, Disabled,       Normal, Disabled,
BPDUFilter, Edge BPDUGuard        Disabled                Disabled
STP MST Simulate PVST       1     Enabled                 Enabled
Interface-vlan admin up     2     1,10-20,2001-2010,3951  1,10-20,2001-2010,3951
                                  -3960                   -3960
Interface-vlan routing      2     1,10-20,2001-2010,3951  1,10-20,30,75,2001-201
capability                        -3960                   0,3951-3960
VTP domain                  2     interop                 interop
VTP version                 2     1                       1
VTP mode                    2     Server                  Server
VTP password                2
VTP pruning status          2     Disabled                Disabled
Allowed VLANs               -     1-100,2001-2010,3001-3  1-100,2001-2010,3001-3
                                  010,3951-3960           010,3951-3960
Local suspended VLANs       -     -                       -
N7K-2# show vpc consistency-parameters interface port-channel 7

    Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name                        Type  Local Value             Peer Value
-------------               ----  ---------------------- -----------------------
lag-id                      1     [(7f9b,                 [(7f9b,
                                  0-23-4-ee-be-5f, 8007,  0-23-4-ee-be-5f, 8007,
                                   0, 0), (8000,           0, 0), (8000,
                                  0-1b-90-25-44-0, 6, 0,  0-1b-90-25-44-0, 6, 0,
                                   0)]                     0)]
mode                        1     passive                 passive
STP Port Type               1     Default                 Default
STP Port Guard              1     Default                 Default
STP MST Simulate PVST       1     Default                 Default
Native Vlan                 1     1                       1
Port Mode                   1     trunk                   trunk
MTU                         1     1500                    1500
Duplex                      1     full                    full
Speed                       1     10 Gb/s                 10 Gb/s
Admin port mode             1     trunk                   trunk
Interface type              1     port-channel            port-channel
LACP Mode                   1     on                      on
vPC card type               1     Earl8                   Earl8
Allowed VLANs               -     1,10-20,2001-2010,3001  1,11-20,2001-2010,3001
                                  -3010                   -3010
Local suspended VLANs       -     10                      -
```

3.4.1.5 vPC in mixed chassis mode (M1/F1 ports in same system or VDC)

Mixed chassis mode is a system where both M1 ports and F1 ports are used simultaneously.

M1 Series line cards provide scalable Layer 2 and Layer 3 capabilities. F1 Series line cards provide high-density cost-effective Layer 2 10-Gigabit Ethernet connectivity. Interoperability between M1 and F1 ports is provided by L3 internal proxy routing where M1 ports are used for L3 proxy when traffic entering a F1 port needs to be routed (L3 traffic for inter VLAN routing or traffic going outside of data center). M1 line cards typically host the interface VLAN (i.e SVI - Switch Virtual Interface) on behalf of F1 line cards.

A vPC system in mixed chassis mode with peer-link on F1 ports present the following characteristics:

- The total number of MAC addresses supported is 16K (capacity of one forwarding engine [i.e switch on chip] on the F1 series line card)
- M1 ports are used only for L3 uplinks
- F1 ports are used for vPC member ports (can use M1 ports as well if needed)
- Need to use the *peer-gateway exclude-vlan <VLAN list>* knob to exclude VLANs that belong to backup routing path (this command only applies to a vPC system in mixed chassis mode with vPC peer-link on F1)

NVT makes use of M1 ports for the vPC peer-link and F1 ports for the vPC member ports. A vPC system in mixed chassis mode with the peer-link on M1 ports presents the following characteristics:

- The total number of MAC addresses supported is 128K (capacity of forwarding engine on the M1 series line card)
- M1 ports are used for L3 uplinks and vPC peer-link
- F1 ports are used for vPC member ports (can use M1 ports as well if needed). Non-overlapping assignment of vlans on the F1 card SoC's ensures the best use of mac address table space.
- There is no need to use the *peer-gateway exclude-vlan <VLAN list>* knob

Display layer 3 proxy details:

```
N7K-2# show hardware proxy layer-3 detail

Global Information:
        Layer-2 only Modules: Count: 1, Slot: 7
        Layer-3 Modules supporting proxy layer-3: Count: 4, Slot: 1,8-10

        Replication Rebalance Mode:             Manual
        Number of proxy layer-3 forwarders:     22
        Number of proxy layer-3 replicators:    14

Forwarder Interfaces                    Status     Reason
------------------------------------------------------------------------------
Eth1/1                                  up         SUCCESS
Eth1/2                                  up         SUCCESS
Eth1/3                                  up         SUCCESS
Eth1/4                                  up         SUCCESS
Eth1/5                                  up         SUCCESS
Eth1/6                                  up         SUCCESS
Eth1/7                                  up         SUCCESS
Eth8/1, Eth8/3, Eth8/5, Eth8/7          up         SUCCESS
Eth8/2, Eth8/4, Eth8/6, Eth8/8          up         SUCCESS
Eth8/10, Eth8/12, Eth8/14, Eth8/16      up         SUCCESS
Eth8/17, Eth8/19, Eth8/21, Eth8/23      up         SUCCESS
Eth8/18, Eth8/20, Eth8/22, Eth8/24      up         SUCCESS
Eth8/25, Eth8/27, Eth8/29, Eth8/31      up         SUCCESS
Eth8/26, Eth8/28, Eth8/30, Eth8/32      up         SUCCESS
Eth9/41-44                              up         SUCCESS
Eth10/1, Eth10/3, Eth10/5, Eth10/7      up         SUCCESS
Eth10/2, Eth10/4, Eth10/6, Eth10/8      up         SUCCESS
Eth10/9, Eth10/11, Eth10/13, Eth10/15   up         SUCCESS
Eth10/10, Eth10/12, Eth10/14, Eth10/16  up         SUCCESS
Eth10/17, Eth10/19, Eth10/21, Eth10/23  up         SUCCESS
Eth10/18, Eth10/20, Eth10/22, Eth10/24  up         SUCCESS
Eth10/25, Eth10/27, Eth10/29, Eth10/31  up         SUCCESS

RE = Replication Engine
Replicator Interfaces (RE instance)     #Interface-Vlan   Interface-Vlan
------------------------------------------------------------------------------
Eth1/1-2 (0)                            4                 1,10-12
```

```
Eth1/3-4 (1)                            3               13-15
Eth1/5-6 (2)                            3               16-18
Eth1/7-8 (3)                            3               19-20,2001
Eth8/1, Eth8/3, Eth8/5, Eth8/7, Eth8/9, 3               2002-2004
Eth8/11, Eth8/13, Eth8/15 (3)
Eth8/2, Eth8/4, Eth8/6, Eth8/8, Eth8/10, 3              2005-2007
 Eth8/12, Eth8/14, Eth8/16 (0)
Eth8/17, Eth8/19, Eth8/21, Eth8/23,     3               2008-2010
Eth8/25, Eth8/27, Eth8/29, Eth8/31 (2)
Eth8/18, Eth8/20, Eth8/22, Eth8/24,     3               2950-2952
Eth8/26, Eth8/28, Eth8/30, Eth8/32 (1)
Eth9/1-24 (0)                           3               2953-2955
Eth9/25-48 (1)                          3               2956-2958
Eth10/1, Eth10/3, Eth10/5, Eth10/7,     3               2959-2960,3951
Eth10/9, Eth10/11, Eth10/13, Eth10/15
(3)
Eth10/2, Eth10/4, Eth10/6, Eth10/8,     3               3952-3954
Eth10/10, Eth10/12, Eth10/14, Eth10/16
(0)
Eth10/17, Eth10/19, Eth10/21, Eth10/23, 3               3955-3957
Eth10/25, Eth10/27, Eth10/29, Eth10/31
(2)
Eth10/18, Eth10/20, Eth10/22, Eth10/24, 3               3958-3960
Eth10/26, Eth10/28, Eth10/30, Eth10/32
(1)
```

3.4.1.6 vPC Role Priority

There are two defined vPC roles: primary and secondary. The vPC role defines which of the two vPC peer devices processes Bridge Protocol Data Units (BPDUs) and responds to Address Resolution Protocol (ARP).

In case of a tie (same role priority value defined on both peer devices), the lowest system MAC will dictate the primary peer device.

Display vpc role, system-mac, system-priority:

```
N7K-2# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : primary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:5f
vPC system-priority             : 32667
vPC local system-mac            : 00:23:ac:64:bb:c2
vPC local role-priority         : 110
```

3.4.1.7 vPC Peer-Link

The vPC peer-link is a standard 802.1Q trunk that performs the following actions:

- Carry vPC and non-vPC VLANs.
- Carry Cisco Fabric Services messages that are tagged with CoS=4 for reliable communication.
- Carry flooded traffic between the vPC peer devices.
- Carry STP BPDUs, HSRP hello messages, and IGMP updates.

When the vPC peer-link fails and the vPC peer-keepalive link is still up, the vPC secondary peer device performs the following operations:

- Suspends its vPC member ports
- Shuts down the SVI associated to the vPC VLAN

Display vPC peer-link information:

```
N7K-2# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 95
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 108
Track object                      : 10
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po5    up     1-100,2001-2010,3001-3010,3951-3960

vPC status
----------------------------------------------------------------------
id   Port      Status Consistency Reason                Active vlans
--   ----      ------ ----------- ------                ------------
7    Po7       up     success     success                  1,11-20,200
                                                         1-2010,3001
                                                         -3010
8    Po8       up     success     success                  1,11-20,200
                                                         1-2010,3001
```

3.4.1.8 vPC Peer-keepalive Link

The vPC peer-keepalive link is a Layer 3 link that joins one vPC peer device to the other vPC peer device and carries a periodic heartbeat between those devices. It is used at the boot up of the vPC systems to guarantee that both peer devices are up before forming the vPC domain. It is also used when the vPC peer-link fails, in which case, the vPC peer-keepalive link is leveraged to detect split brain scenario (both vPC peer devices are active-active).

Default values for VPC peer-keepalive links:

Timer	Default value
Keepalive interval	1 seconds
Keepalive hold timeout (on vPC peer-link loss)	3 seconds
Keepalive timeout	5 seconds

When building a vPC peer-keepalive link, use the following in descending order of preference:

1. Dedicated link(s) (1-Gigabit Ethernet port is enough) configured as L3. A port-channel with 2 X 1G port is preferred.
2. Mgmt0 interface (along with management traffic)
3. As a last resort, route the peer-keepalive link over the Layer 3 infrastructure.

NVT makes use of the 1st option.

Display vpc peer-keepalive information:

```
N7K-2# show vpc peer-keepalive

vPC keep-alive status             : peer is alive
--Peer is alive for              : (5775) seconds, (700) msec
--Send status                    : Success
--Last send at                   : 2013.08.14 12:19:21 112 ms
--Sent on interface              : Eth1/1
--Receive status                 : Success
--Last receive at                : 2013.08.14 12:19:21 113 ms
--Received on interface          : Eth1/1
--Last update from peer          : (0) seconds, (709) msec

vPC Keep-alive parameters
--Destination                    : 1.1.1.1
--Keepalive interval             : 1000 msec
--Keepalive timeout              : 5 seconds
--Keepalive hold timeout         : 3 seconds
--Keepalive vrf                  : vpc-keepalive
--Keepalive udp port             : 3200
--Keepalive tos                  : 192
```

3.4.1.9 vPC Member Link

As suggested by the name, a vPC member port is a port-channel member of a vPC. A port-channel defined as a vPC member port always contains the keywords *vpc <vpc id>.*

A vPC only supports Layer 2 port-channels. The port-channel can be configured in access or trunk switchport mode. Any VLAN allowed on the vPC member port is by definition called a vPC VLAN. Whenever a vPC VLAN is defined on a vPC member port, it must also be defined on the vPC peer-link. Not defining a vPC VLAN on the vPC peer-link will cause the VLAN to be suspended.

The configuration of the vPC member port must match on both the vPC peer devices. If there is an inconsistency, a VLAN or the entire port channel may be suspended (depending on type-1 or type-2 consistency check for the vPC member port). For instance, an MTU mismatch will suspend the vPC member port.

Display vPC member port-channel information:

```
N7K-2# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 95
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 108
Track object                      : 10
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)
```

```
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po5    up     1-100,2001-2010,3001-3010,3951-3960

vPC status
----------------------------------------------------------------------
id   Port      Status Consistency Reason                Active vlans
--   ----      ------ ----------- ------                ------------
7    Po7       up     success     success                  1,11-20,200
                                                         1-2010,3001
                                                         -3010
8    Po8       up     success     success                  1,11-20,200
                                                         1-2010,3001
N7K-2# show vpc consistency-parameters interface port-channel 7

    Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
lag-id                      1     [(7f9b,                [(7f9b,
                                  0-23-4-ee-be-5f, 8007, 0-23-4-ee-be-5f, 8007,
                                   0, 0), (8000,          0, 0), (8000,
                                  0-1b-90-25-44-0, 6, 0, 0-1b-90-25-44-0, 6, 0,
                                   0)]                    0)]
mode                        1     passive                passive
STP Port Type               1     Default                Default
STP Port Guard              1     Default                Default
STP MST Simulate PVST       1     Default                Default
Native Vlan                 1     1                      1
Port Mode                   1     trunk                  trunk
MTU                         1     1500                   1500
Duplex                      1     full                   full
Speed                       1     10 Gb/s                10 Gb/s
Admin port mode             1     trunk                  trunk
Interface type              1     port-channel           port-channel
LACP Mode                   1     on                     on
vPC card type               1     Earl8                  Earl8
Allowed VLANs               -     1,10-20,2001-2010,3001 1,11-20,2001-2010,3001
                                  -3010                  -3010
Local suspended VLANs       -     10                     -
```

3.4.1.10 vPC ARP Synchronization

The vPC ARP Sync feature improves the convergence time for Layer 3 flows (North to South traffic). When the vPC peer-link fails and subsequently recovers, vPC ARP Sync performs an ARP bulk synchronization over Cisco Fabric Services (CFS) from the vPC primary peer device to the vPC secondary peer device.

Displays vPC ARP sync information:

```
N7K-2# show ip arp sync-entries

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Address         Age       MAC Address     Interface
101.39.59.101   00:01:22  0050.5601.0009  Vlan3959
101.39.59.102   00:01:22  0050.5601.0109  Vlan3959
101.39.59.103   00:01:22  0050.5601.0209  Vlan3959
101.39.59.104   00:01:22  0050.5601.0309  Vlan3959
```

3.4.1.11 vPC Delay Restore

After a vPC peer device reloads and comes back up, the routing protocol needs time to reconverge. The recovering vPCs leg may black-hole routed traffic from the access to the core until the Layer 3 connectivity is reestablished.

The vPC Delay Restore feature delays the vPCs leg bringup on the recovering vPC peer device. vPC Delay Restore allows for Layer 3 routing protocols to converge before allowing any traffic on the vPC leg. The result is a more graceful restoration and zero packet loss during the recovery phase (traffic still gets diverted to the alive vPC peer device).

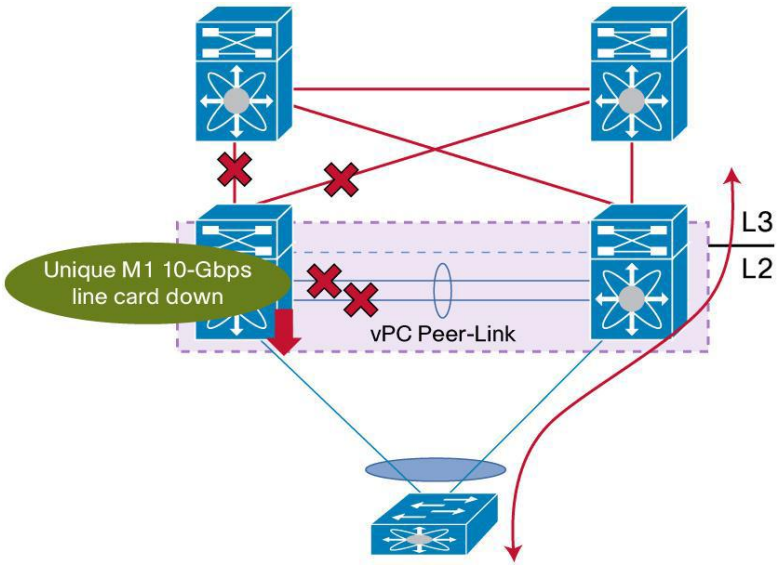
This feature is enabled by default with a vPC restoration default timer of 30 seconds, which NVT maintains in the testbed.

3.4.1.12 vPC Object-Tracking

A vPC deployment with a single Cisco Nexus 7000 Series M132XP-12 module or M108XP-12 module, where the L3 core uplinks and vPC peer-link interfaces are localized on the same module, is vulnerable to access layer isolation if the 10-Gbps module fails on the primary vPC (vPC member ports are defined on both 1-Gbps line cards and on 10-Gbps line card).

In this scenario, the vPC Object Tracking feature shuts down vPC member ports on the peer device where M1 10-Gbps is damaged (irrespective of vPC role primary or secondary). This triggered action allows traffic flows (southbound and northbound) to go through the other peer device where the M1 10-Gbps line card is up.

Figure 7 vPC Object Tracking Feature – Behavior when vPC peer-link fails



The vPC Object Tracking feature suspends the vPCs on the impaired device so that traffic can be diverted over the remaining vPC peer.

To use vPC object tracking, track both Peer-link interfaces and L3 core interfaces as a list of Boolean objects. Note that the Boolean AND operation is not supported with vPC object tracking. The vPC object tracking configuration must be applied on both vPC peer devices.

Sample Configuration:

```
! Track the vpc peer link
track 1 interface port-channel5 line-protocol
! Track the uplinks to the core
track 2 interface port-channel3 line-protocol
track 3 interface port-channel4 line-protocol
! Combine all tracked objects into one.
! "OR" means if ALL objects are down, this object will go down
! ==> we have lost all connectivity to the L3 core and the peer link
track 10 list boolean OR
  object 1
  object 2
  object 3
! If object 10 goes down on the primary vPC peer,
! system will switch over to other vPC peer and disable all local vPCs
vpc domain 95
  track 10
```

Display tracked object status:

```
N7K-2# show track 10
Track 10
  List  Boolean or
  Boolean or is UP
  4 changes, last change 1d00h
  Track List Members:
    object 3 UP
    object 2 UP
    object 1 UP
  Tracked by:
    vPCM Domain 95
```

3.4.1.13 vPC Auto-Recovery

vPC auto-recovery feature was designed to address 2 enhancements to vPC.

- to provide a backup mechanism in case of vPC peer-link failure followed by vPC primary peer device failure (vPC auto-recovery feature).
- to handle a specific case where both vPC peer devices reload but only one comes back to life (vPC auto-recovery reload-delay feature).

Helpful commands for vPC Object tracking

Show vpc brief	Displays Auto-recovery status

Configuration check:

```
N7K-2# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 95
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
```

```
vPC role                          : primary
Number of vPCs configured         : 108
Track object                      : 10
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
--------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po5    up     1-100,2001-2010,3001-3010,3951-3960
```

3.4.1.14 HSRP Active/Active with vPC

HSRP in the context of vPC has been improved from a functional and implementation standpoint to take full benefits of the L2 dual-active peer devices nature offered by vPC technology. HSRP operates in active-active mode from data plane standpoint, as opposed to classical active/standby implementation with STP based network. No additional configuration is required. As soon as vPC domain is configured and interface VLAN with associated HSRP group is activated, HSRP will behave by default in active/active mode (on data plane side).
From a control plane standpoint, active-standby mode still applies for HSRP in context of vPC; the active HSRP instance responds to ARP request. ARP response will contain the HSRP vMAC which is the same on both vPC peer devices. The standby HSRP vPC peer device just relays the ARP request to active HSRP/VRRP peer device through vPC peer-link.

Sample Configuration:

```
! N7K-1:
interface Vlan11
  no ip redirects
  ip address 101.11.0.21/16
  hsrp version 2
  hsrp 1
    authentication md5 key-string cisco
    preempt delay minimum 120
    priority 200
    ip 101.11.0.1
  no shutdown

! N7K-2:
interface Vlan11
  no ip redirects
  ip address 101.11.0.19/16
  hsrp version 2
  hsrp 1
    authentication md5 key-string cisco
    preempt delay minimum 120
    ip 101.11.0.1
  no shutdown
```

Helpful commands for HSRP active/active with vPC

Show hsrp brief	Displays hsrp status
Show mac address-table vlan <vlan id>	Displays mac addresses including HSRP vMAC; check for G-flag on vMAC for active/active HSRP

Configuration check:

```
N7K-2# show hsrp brief
*:IPv6 group   #:group belongs to a bundle
                    P indicates configured to preempt.
                    |
 Interface   Grp  Prio P State    Active addr      Standby addr     Group addr
  Vlan1       1    200  P Active   local            101.0.1.19       101.0.1.1       (conf)
  Vlan10      1    200  P Active   local            101.10.0.19      101.10.0.1      (conf)
  Vlan10      2    200  P Active   local            101.10.0.19      101.110.0.1     (conf)
  Vlan11      1    200  P Active   local            101.11.0.19      101.11.0.1      (conf)
N7K-2# show mac address-table vlan 11
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G 11       0000.0c9f.f001    static       -       F    F  sup-eth1(R)
G 11       0000.0c9f.f002    static       -       F    F  sup-eth1(R)
```

3.4.1.15 PIM pre-build-spt with vPC

PIM Pre-build SPT on non-forwarder attracts multicast traffic by triggering upstream PIM J/Ps (Join/Prune) without setting any interface in the OIF (Outgoing Interface) list. Multicast traffic is then always pulled to the non-active forwarder and finally dropped due to no OIFs.

The immediate effect of enabling PIM Pre-build SPT is to improve the convergence time upon active forwarder failure (1 to 3 seconds of convergence time). The other vPC peer device (which is the non-active forwarder) does not need to create any new upstream multicast state and can quickly transition to the active forwarder role by properly programming the OIF (Outgoing Interface) list.
The impact of enabling PIM prebuild SPT is the consumption of bandwidth and replication capacity on the primary and secondary data path (i.e. on vPC primary and secondary peer devices) in steady state.

In the vPC implementation in F2-mode, because of a hardware limitation, the PIM dual DR mode is disabled. In this case (with F2 mode), even if the **ip pim pre-build-spt** command is configured, there is no value added because the corresponding (S,G) route is not created in the first place.

As shown below, on the non-forwarder/secondary the (S,G) is created with no OIFs.

On non-forwarder

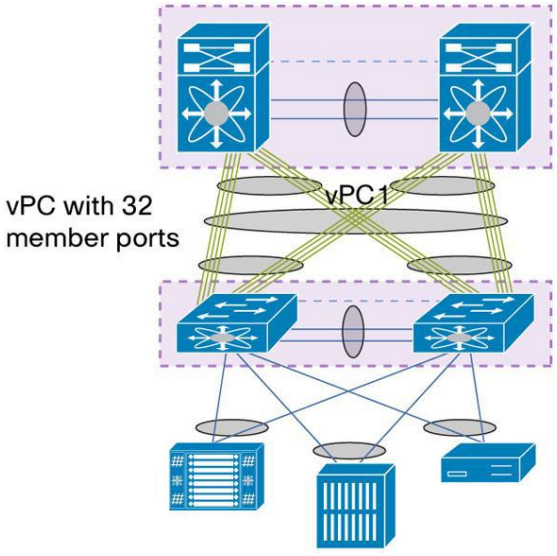
```
DC5-DC101-5# sh ip mrout 230.102.0.1
IP Multicast Routing Table for VRF "default"

(*, 230.102.0.1/32), uptime: 00:24:01, igmp ip pim
  Incoming interface: port-channel3, RPF nbr: 40.101.1.15
  Outgoing interface list: (count: 20)
    Vlan20, uptime: 00:22:39, igmp
    Vlan14, uptime: 00:22:43, igmp
    Vlan16, uptime: 00:22:45, igmp
    Vlan12, uptime: 00:22:56, igmp
    Vlan18, uptime: 00:22:58, igmp
    Vlan15, uptime: 00:22:58, igmp
    Vlan17, uptime: 00:22:58, igmp
    Vlan11, uptime: 00:22:58, igmp
    Vlan13, uptime: 00:22:58, igmp
    Vlan19, uptime: 00:23:00, igmp
```

```
    Vlan2010, uptime: 00:23:54, igmp
    Vlan2006, uptime: 00:23:54, igmp
    Vlan2001, uptime: 00:23:54, igmp
    Vlan2008, uptime: 00:23:57, igmp
    Vlan2009, uptime: 00:23:57, igmp
    Vlan2003, uptime: 00:23:57, igmp
    Vlan2007, uptime: 00:23:57, igmp
    Vlan2002, uptime: 00:23:58, igmp
    Vlan2004, uptime: 00:24:00, igmp
    Vlan2005, uptime: 00:24:01, igmp

(102.11.17.1/32, 230.102.0.1/32), uptime: 00:24:01, ip pim
  Incoming interface: port-channel4, RPF nbr: 40.101.3.17
  Outgoing interface list: (count: 0)


DC5-DC101-5# sh ip pim intern vpc rp
PIM vPC RPF-Source Cache for Context "default" - Chassis Role Secondary


Source: 102.11.17.1
  Pref/Metric: 110/1100
  Source role: secondary
  Forwarding state: Tie (not forwarding)
```

3.4.1.16 Double-Sided vPC Topology

A double-sided vPC topology superposes two layers of vPC domain and the bundle between vPC domain 1 and vPC domain 2 is by itself a vPC. The vPC domain at the bottom is used for active/active connectivity from end-point devices to the network access layer. The vPC domain at the top is used for active/active FHRP in the L2/L3 boundary aggregation layer.

Figure 8 Double-Sided vPC Topology



Benefits of double-sided vPC over single-sided vPC topology are listed below:

- Enables a larger Layer 2 domain.

- Provides a highly resilient architecture. In double-sided vPC, two access switches are connected to two aggregation switches whereas in single-sided vPC, one access switch is connected to two aggregation switches.
- Provides more bandwidth from the access to aggregation layer. Using a Cisco Nexus F1 or F2 Series modules line card for vPC and Cisco Nexus 5000 Series Switches with Release 4.1(3)N1(1a) or later, a vPC with 32 active member ports (that is, 320 Gbps) can be instantiated.

3.4.2 FabricPath

NVT fabricpath topology is designed to have four Spines using Nexus 7000 at the aggregation layer. There are six Nexus 5000 leaf switches on access layer that are connected to all four spines. The FabricPath feature is only supported on the F Series modules on the Nexus 7000. In DC1, spine switches consist of Nexus 7000 with sup 1 and F1/M1 linecards, and while in DC2, spine switches consist of Nexus 7000 with sup2e and F2 linecards.

Because of the multiple forwarding engines (FEs) on the F Series modules, the port pairs and port sets in the table below must be configured to be in the same VDC.

Nexus 7000 F Series Modules Port Pairs and Port Sets	
Port Pairs for F1 Modules	**Port Sets for F2 Modules**
Ports 1 and 2	Ports 1, 2, 3, 4
Ports 3 and 4	Ports 5, 6, 7, 8
Ports 5 and 6	Ports 9, 10, 11, 12
Ports 7 and 8	Ports 13, 14, 15, 16
Ports 9 and 10	Ports 17, 18, 19, 20
Ports 11 and 12	Ports 21, 22, 23, 24
Ports 13 and 14	Ports 25, 26, 27, 28
Ports 15 and 16	Ports 29, 30, 31, 32
Ports 17 and 18	Ports 33, 34, 35, 36
Ports 19 and 20	Ports 37, 38, 39, 40
Ports 21 and 22	Ports 41, 42, 43, 44
Ports 23 and 24	Ports 45, 46, 47, 48
Ports 25 and 26	
Ports 27 and 28	
Ports 29 and 30	
Ports 31 and 32	

NVT FabricPath configuration is as the following:

```
feature-set fabricpath

logging level fabricpath isis 5

vlan 1,11-20,2001-2010,3001-3010
  mode fabricpath
fabricpath switch-id 251
logging level fabricpath switch-id 5
vpc domain 211
  fabricpath switch-id 1001
  fabricpath multicast load-balance


interface port-channel52
  switchport mode fabricpath
  fabricpath isis metric 200

interface port-channel701
  switchport mode fabricpath

interface port-channel702
  switchport mode fabricpath

interface port-channel703
  switchport mode fabricpath

interface port-channel704
  switchport mode fabricpath

interface port-channel705
  switchport mode fabricpath

interface port-channel706
  switchport mode fabricpath

fabricpath domain default
  root-priority 109
fabricpath load-balance unicast include-vlan
fabricpath load-balance multicast rotate-amount 0x3 include-vlan
```

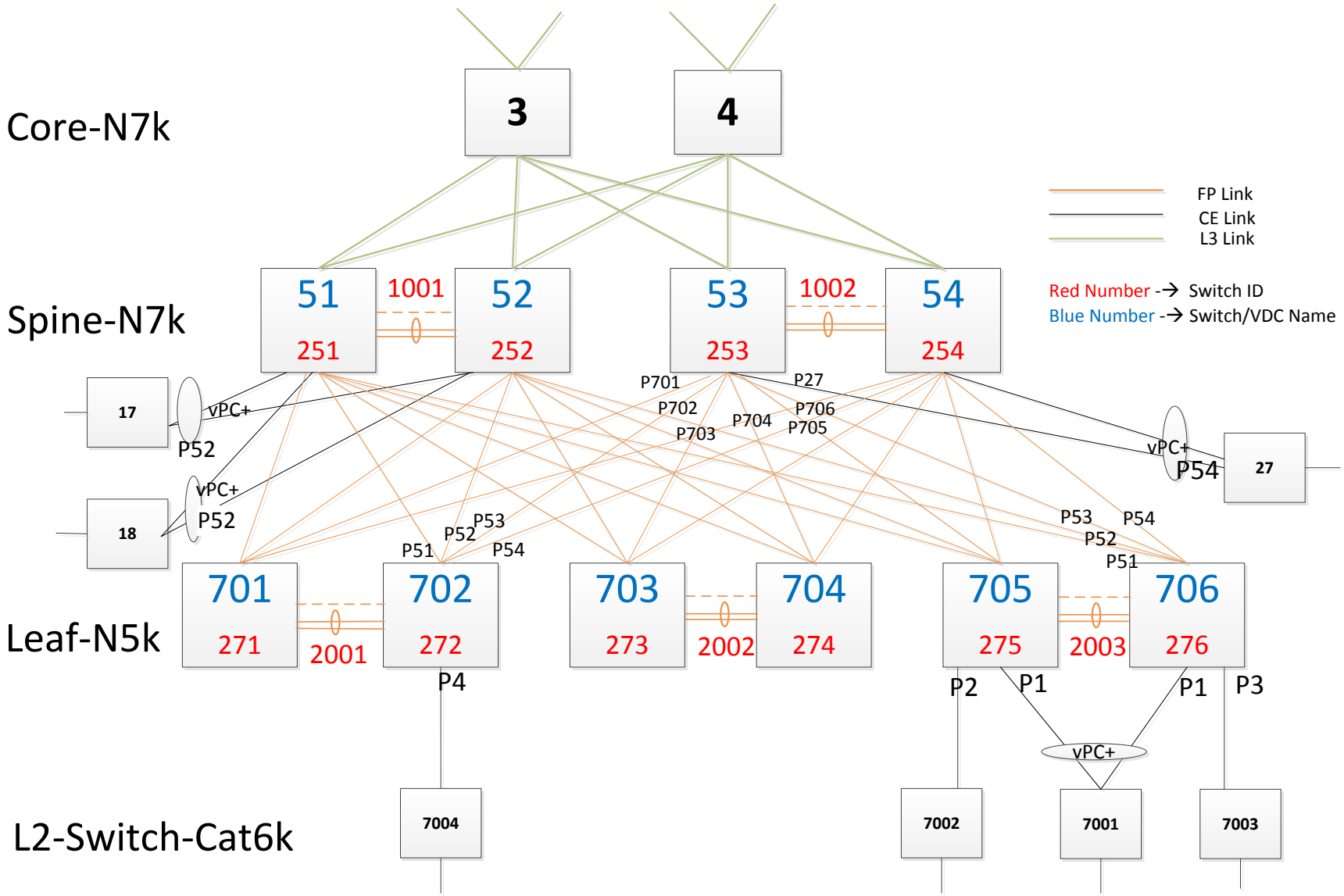
3.4.2.1 FabricPath Switch-IDs

Cisco FabricPath can assign switch IDs to all the devices in the network automatically; however, it is convenient to use a meaningful numbering scheme. During network troubleshooting, having a distinct numbering scheme allows for faster and easier switch role identification.

NVT has assigned switch IDs using the following scheme in the FabricPath domain network:

- The devices in the spine have been assigned a three-digit ID related to spine VDC naming: 251 or 252
- The devices at the leaf have been assigned a three-digit ID related to leaf device naming: 701 or 702
- The virtual switch for the domain has a four-digit ID: 1001 or 1002

Figure 9 NVT FabricPath POD Logical Topology



To verify the FabricPath switch ID:

```
DC202-51# sh fabricpath switch-id local
Switch-Id: 251
System-Id: 0026.980c.c0c3

DC202-51# sh fabricpath switch-id
                      FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
        '[E]' - local Emulated Switch-id
        '[A]' - local Anycast Switch-id
Total Switch-ids: 20
================================================================================
    SWITCH-ID      SYSTEM-ID       FLAGS         STATE    STATIC  EMULATED/
                                                                   ANYCAST
--------------+----------------+------------+-----------+--------------------
*   251         0026.980c.c0c3    Primary     Confirmed Yes     No
    252         f866.f207.2543    Primary     Confirmed Yes     No
    253         0026.980c.c0c4    Primary     Confirmed Yes     No
    254         f866.f207.2544    Primary     Confirmed Yes     No
    271         547f.eef7.dafc    Primary     Confirmed Yes     No
    272         547f.eef7.d97c    Primary     Confirmed Yes     No
    273         547f.eef7.e3fc    Primary     Confirmed Yes     No
    274         547f.eebb.bd3c    Primary     Confirmed Yes     No
    275         547f.eef7.debc    Primary     Confirmed Yes     No
    276         547f.eede.927c    Primary     Confirmed Yes     No
[E] 1001         0026.980c.c0c3    Primary     Confirmed No      Yes
    1001        f866.f207.2543    Primary     Confirmed No      Yes
    1002         0026.980c.c0c4    Primary     Confirmed No      Yes
    1002        f866.f207.2544    Primary     Confirmed No      Yes
    2001          547f.eef7.d97c    Primary     Confirmed No      Yes
    2001        547f.eef7.dafc    Primary     Confirmed No      Yes
    2002        547f.eebb.bd3c    Primary     Confirmed No      Yes
    2002          547f.eef7.e3fc    Primary     Confirmed No      Yes
    2003        547f.eede.927c    Primary     Confirmed No      Yes
    2003        547f.eef7.debc    Primary     Confirmed No      Yes
```

3.4.2.2 FabricPath VLANs

Cisco FabricPath VLANs should be consistently defined on all the Cisco FabricPath switches in a particular FabricPath topology.

To verify the FabricPath VLANs:

```
DC202-54# sh fabricpath isis vlan-range
Fabricpath IS-IS domain: default
MT-0
Vlans configured:
1, 11-20, 2001-2010, 3001-3010, 4040
```

3.4.2.3 FabricPath Core Port

The configuration of a FabricPath core port is performed with the command *switchport mode fabricpath.* The FabricPath core port exchanges topology info through L2 ISIS adjacency and forwarding based on the Switch ID Table.

To verify the FabricPath interface:

```
DC202-54# sh fabricpath isis interface port-channel 701
Fabricpath IS-IS domain: default
Interface: port-channel701
  Status: protocol-up/link-up/admin-up
  Index: 0x0002, Local Circuit ID: 0x01, Circuit Type: L1
  No authentication type set
  Authentication check is not specified
  Extended Local Circuit ID: 0x160002BC, P2P Circuit ID: 0000.0000.0000.00
  Retx interval: 5, Retx throttle interval: 66 ms
  LSP interval: 33 ms, MTU: 1500
  P2P Adjs: 1, AdjsUp: 1, Priority 64
  Hello Interval: 10, Multi: 3, Next IIH: 00:00:01
  Level   Adjs   AdjsUp  Metric   CSNP  Next CSNP  Last LSP ID
  1          1        1      20     60  00:00:46   ffff.ffff.ffff.ff-ff
  Topologies enabled:
    Level Topology Metric  MetricConfig Forwarding
    0     0        4000    no           UP
    1     0        20      no           UP

DC202-54# sh fabricpath isis interface brief
Fabricpath IS-IS domain: default
Interface    Type  Idx State        Circuit   MTU  Metric  Priority  Adjs/AdjsUp
--------------------------------------------------------------------------------
port-channel53 P2P   1     Up/Ready   0x01/L1   1500 200     64          1/1
port-channel701 P2P   2     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel702 P2P   3     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel703 P2P   4     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel704 P2P   5     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel705 P2P   6     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel706 P2P   7     Up/Ready   0x01/L1   1500 20      64          1/1
```

3.4.2.4 FabricPath Metric

Cisco FabricPath ISIS calculates the preferred path to any switch-id based on the metric to any given destination. The metric is as follows:

- 1-Gbps Ethernet links have a cost of 400
- 10-Gigabit Ethernet links have a cost of 40
- 20-Gbps have a cost of 20

NVT has set a higher ISIS metric on vPC peer links between spine switches to prevent traffic from flowing through the vPC peer links.

To verify the FabricPath ISIS metric, use the following commands:

```
DC202-54# sh fabricpath isis interface brief
Fabricpath IS-IS domain: default
Interface    Type  Idx State        Circuit   MTU  Metric  Priority  Adjs/AdjsUp
--------------------------------------------------------------------------------
port-channel53 P2P   1     Up/Ready   0x01/L1   1500 200     64          1/1
port-channel701 P2P   2     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel702 P2P   3     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel703 P2P   4     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel704 P2P   5     Up/Ready   0x01/L1   1500 20      64          1/1
port-channel705 P2P   6     Up/Ready   0x01/L1   1500 20      64          1/1
```

```
port-channel706 P2P    7      Up/Ready    0x01/L1    1500 20       64          1/1
```

3.4.2.5 Root for FabricPath Multi-destination Trees

In FabricPath multicast traffic, broadcast and flooded traffic is forwarded along a Multi-destination tree. FabricPath allows for multiple Multi-destination trees in order to achieve traffic load balancing for Multi-destination frames.

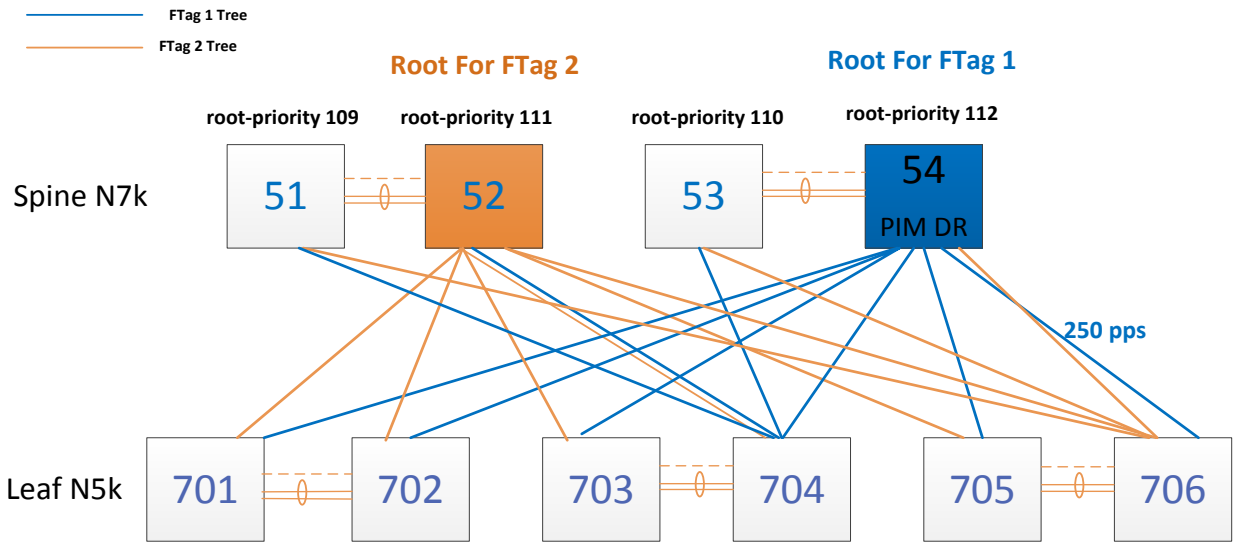
Two multi-destination trees are defined in Cisco FabricPath network by default, and Multi-destination traffic is mapped to either of those trees for load-balancing purposes. The root of those multi-destination trees in the network should be explicitly set so as to provide an optimal topology.

Cisco FabricPath Intermediate Switch-to-Intermediate Switch (IS-IS) Protocol elects the switch with the highest configured root priority as the root for Multi-destination tree 1. The switch with the second-highest root priority becomes the root for Multi-destination tree 2. If there is no root priority configured, the other two parameters will be compared, system ID and switch ID, with higher values being better in all cases.

NVT has set the roots of the two multi-destination trees at two spine switches, one from each pair of vPC+ switches. If either of those switches fails, a replacement root would be elected out of the all FabricPath domain switches. This backup root should be configured in advance so that the system falls back to a predetermined topology in a failure scenario.

The following picture shows the NVT FabricPath Root design for the multi-destination trees. Spine 54 has highest root priority and is selected as root of FTag 1 and Spine 52 has second highest root priority and is selected as root of FTag 2.

Figure 10 NVT FabricPath Root design for the multi-destination trees



FTag trees are used as follows:
• FTag1 tree is used for unknown unicast, broadcast, and multicast.
• FTag2 tree is used only for multicast traffic.

To verify FabricPath multi-destination tree root:

```
DC202-54# sh fabricpath isis topology sum
FabricPath IS-IS Topology Summary
Fabricpath IS-IS domain: default
MT-0
  Configured interfaces:  port-channel53  port-channel701  port-channel702
  port-channel703  port-channel704  port-channel705  port-channel706
 Max number of trees: 2  Number of trees supported: 2
    Tree id: 1, ftag: 1, root system: f866.f207.2544, 254
    Tree id: 2, ftag: 2 [transit-traffic-only], root system: f866.f207.2543, 252
Ftag Proxy Root: f866.f207.2544
```

To verify which multicast FTag tree is used in N7K:

```
DC202-54# sh fabricpath load-balance multicast ftag-selected flow-type l3 src-ip 202.11.27.1 dst-ip
230.202.0.1 vlan 12 module 2
128b Hash Key generated : 00 6d 00 00 00 00 00 00 32 82 c6 c0 40 00 00 00
0x6c
    FTAG SELECTED IS : 2 (HASH 108)

DC202-53# sh fabricpath load-balance multicast ftag-selected flow-type l3 src-ip 202.11.27.1 dst-ip
230.202.0.1 vlan 11 module 2
128b Hash Key generated : 00 32 82 c6 c0 40 00 00 00 00 6c 00 00 00 00 00
0x49
    FTAG SELECTED IS : 1 (HASH 73)
```

To verify which multicast FTag tree is used in N5K:

```
DC202-706# sh fabricpath load-balance multicast ftag-selected vlan 12 macg 0100.5e4d.0002

 If the traffic is received on a non-vPC port:
 Ftag selected : 2

 If the traffic is received on a vPC port:
 Ftag selected : 1
=====================================

 Vlan : 12 (int_vlan : 16)
 Macg : 0100.5e4d.0002

 Hash-key : 0x00100000 00000000
 Hash-val : 143
Num_trees : 2
```

3.4.2.6 vPC+ for FabricPath

NVT testbed is designed to have 2 pairs of vPC+ peers on the fabricpath spine and 3 pairs of vPC+ peers on the fabricpath leaf. The vPC+ peer-link must be configured as a fabricpath core link.

NVT FabricPath vPC+ configuration is as the following:

```
N7K aggregation VDC 5:

!vPC+ configuration
feature vpc
vpc domain 211
  peer-switch
  peer-keepalive destination 1.1.1.2 source 1.1.1.1
vrf vpc-keepalive
  delay restore 120
  dual-active exclude interface-vlan 1,11-20,2001-
2010
  track 10
  auto-recovery
  fabricpath switch-id 300
  fabricpath multicast load-balance
  ip arp synchronize


!vPC+ member configuration
interface port-channel17
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,11-20,2001-
2010,3001-3010
  medium p2p
  vpc 17

!vPC+ peer link configuration
interface port-channel52
  switchport
  switchport mode fabricpath
  spanning-tree port type network
  medium p2p
  vpc peer-link
  fabricpath isis metric 200

!vPC+ peer keepalive configuration
interface Ethernet1/19
  vrf member vpc-keepalive
  ip address 1.1.1.1/24
  no shutdown
```

```
N7K aggregation VDC 6:

!vPC+ configuration
feature vpc
vpc domain 211
  peer-switch
  role priority 110
  peer-keepalive destination 1.1.1.1 source 1.1.1.2
vrf vpc-keepalive
  delay restore 120
  dual-active exclude interface-vlan 1,11-20,2001-
2010
  track 10
  auto-recovery
  fabricpath switch-id 300
  fabricpath multicast load-balance
  ip arp synchronize

!vPC+ member configuration
interface port-channel17
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,11-20,2001-
2010,3001-3010
  medium p2p
  vpc 17

!vPC+ peer link configuration
interface port-channel51
  switchport
  switchport mode fabricpath
  spanning-tree port type network
  medium p2p
  vpc peer-link
  fabricpath isis metric 200

!vPC+ peer keepalive configuration
interface Ethernet1/19
  vrf member vpc-keepalive
  ip address 1.1.1.2/24
  no shutdown
```

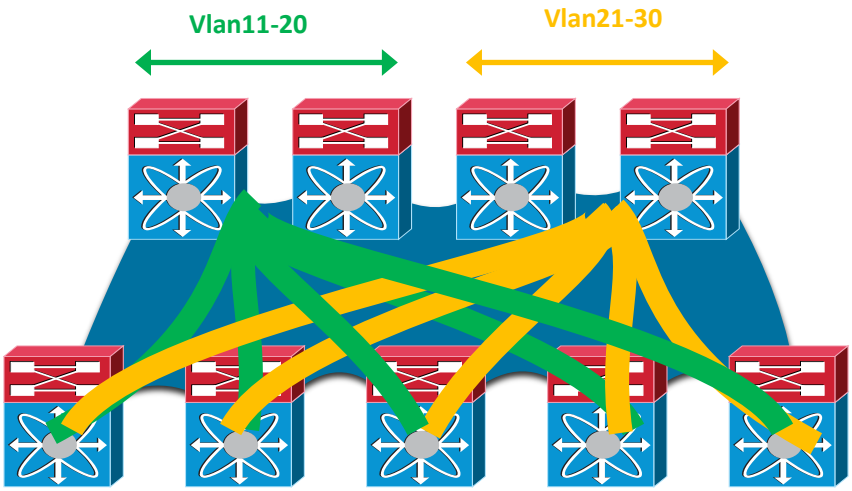
To verify the vPC+:

```
DC202-51# sh vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 211
vPC+ switch id                    : 300
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
vPC fabricpath status             : peer is reachable through fabricpath
```

```
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 2
Track object                      : 10
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : 1,11-20,2001-2010
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)
Fabricpath load balancing         : Enabled
Port Channel Limit                : limit to 244

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po52   up     1,11-20,2001-2010,3001-3010

vPC status
----------------------------------------------------------------------------
id   Port      Status Consistency Reason           Active vlans  vPC+ Attribute
--   ----      ------ ----------- ------           ------------  --------------
17   Po17      up     success     success          1,11-20,2001- DF: Partial,
                                                   2010,3001-301  FP MAC:
                                                   0             300.11.65535
```

3.4.2.6.1 HSRP Active/Active with vPC+

Figure 11 HSRP Active/Active with vPC+



NVT has split HSRP for VLANs among four spines with half the VLANs running HSRP between the first pair of spines only and the other half running HSRP between the other pair of spines only.

NVT spine HSRP configuration is as the below. Two HSRP groups with authentication and priority are configured for each Vlan.

```
interface Vlan11
  no shutdown
  no ip redirects
  ip address 202.11.0.51/16
  ip address 202.111.0.51/16 secondary
  ipv6 address 2001:1:202:11::51/64
  ip router ospf 2 area 0.0.0.202
  ip pim sparse-mode
  hsrp version 2
  hsrp 1
    authentication md5 key-string cisco
    preempt delay minimum 120
    priority 200
    ip 202.11.0.1
  hsrp 2
    authentication md5 key-string cisco
    preempt delay minimum 120
    priority 200
    ip 202.111.0.1
```

To verify HSRP peers and virtual mac address on Nexus 7000 spine:

```
DC202-51# sh hsrp interface vlan 11
Vlan11 - Group 1 (HSRP-V2) (IPv4)
  Local state is Active, priority 200 (Cfged 200), may preempt
    Forwarding threshold(for vPC), lower: 1 upper: 200
  Preemption Delay (Seconds) Minimum:120
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.523000 sec(s)
  Virtual IP address is 202.11.0.1 (Cfged)
  Active router is local
  Standby router is 202.11.0.52 , priority 100 expires in 10.362000 sec(s)
  Authentication MD5, key-string "cisco"
  Virtual mac address is 0000.0c9f.f001 (Default MAC)
  2 state changes, last state change 01:43:32
  IP redundancy name is hsrp-Vlan11-1 (default)

Vlan11 - Group 2 (HSRP-V2) (IPv4)
  Local state is Active, priority 200 (Cfged 200), may preempt
    Forwarding threshold(for vPC), lower: 1 upper: 200
  Preemption Delay (Seconds) Minimum:120
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.523000 sec(s)
  Virtual IP address is 202.111.0.1 (Cfged)
  Active router is local
  Standby router is 202.11.0.52 , priority 100 expires in 9.933000 sec(s)
  Authentication MD5, key-string "cisco"
  Virtual mac address is 0000.0c9f.f002 (Default MAC)
  2 state changes, last state change 01:43:32
  IP redundancy name is hsrp-Vlan11-2 (default)

DC202-51# sh hsrp bri
                    P indicates configured to preempt.
                    |
Interface   Grp Prio P State    Active addr      Standby addr     Group addr
Vlan11      1   200  P Active   local            202.11.0.52      202.11.0.1      (conf)
Vlan11      2   200  P Active   local            202.11.0.52      202.111.0.1     (conf)

DC202-51# sh mac address-table vlan 11
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
```

```
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G 11       0000.0c9f.f001    static       -       F    F  sup-eth1(R)
G 11       0000.0c9f.f002    static       -       F    F  sup-eth1(R)
```

To verify HSRP virtual mac on Nexus 5000 edge switches mac table:

```
N5k-705# sh mac address-table vlan 11
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
* 11       0000.0c9f.f001    dynamic   0          F    F  300.0.65535
* 11       0000.0c9f.f002    dynamic   0          F    F  300.0.65535
```

3.4.2.6.2 vPC+ Dual-Active Exclude

As a result of declaring the link that connects the spines as a vPC peer-link, the default behavior of vPC applies, whereby, if the peer-link goes down, the SVIs on the vPC secondary device are shut down.

In the context of FabricPath designs, this behavior is not beneficial, because the FabricPath links are still available, and there's no good reason to shut down the SVIs on the secondary. It is thus recommended to configure *dual-active exclude* for all the vPC+ vlans.

To verify dual-active exclude Vlan:

```
DC202-51# sh vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 211
vPC+ switch id                    : 300
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
vPC fabricpath status             : peer is reachable through fabricpath
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 2
Track object                      : 10
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : 1,11-20,2001-2010
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)
Fabricpath load balancing         : Enabled
Port Channel Limit                : limit to 244

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po52   up     1,11-20,2001-2010,3001-3010
```

```
vPC status
----------------------------------------------------------------------------
id   Port      Status Consistency Reason           Active vlans  vPC+ Attribute
--   ----      ------ ----------- ------           ------------  --------------
17   Po17      up     success     success          1,11-20,2001- DF: Partial,
                                                   2010,3001-301  FP MAC:
                                                   0             300.11.65535
```

3.4.2.7 FabricPath Region as Spanning Tree Root of the Network

On all the Cisco FabricPath switches that have Classic Ethernet ports, configure the same root priority using the *spanning-tree pseudo-information* command shown below. Make sure that this root priority is the best (lowest) in the network so that the Cisco FabricPath region is the root of the spanning tree. If the Classic Ethernet edge ports receive a superior Bridge Protocol Data Unit (BPDU), those ports will be blocked from forwarding traffic. Also, those Classic Ethernet edge ports connecting to the same Layer 2 domain that is not a Cisco FabricPath domain, should be configured with the spanning-tree domain number. This approach will allow proper BPDU Propagation through the Cisco FabricPath network and help ensure a loop-free environment within that Layer 2 domain.

```
Dc202-54(config)# spanning-tree pseudo-information
Dc202-54(config-pseudo)# vlan 11-20 root priority 4096
```

3.4.2.8 Routed Multicast in FabricPath vPC+

PIM is enabled on Nexus 7000 four spine VDCs FabricPath VLAN under SVI. It follows the same rules as in all other non-FabricPath PODs. NVT has defined all 4 spines as an auto-RP with anycast RP/MSDP configured. From an operational perspective, it is advisable to align the PIM designated router (DR) priority with the HSRP primary.

3.4.2.9 FabricPath Load-balancing And Verification

In Nexus 7000 F2 VDC, to modify default unicast/multicast load-balancing, the port-channel load-balancing has to be changed first, followed by the unicast/multicast load-balancing change.

3.4.2.9.1 FabricPath Unicast Load-balancing And Verification

Cisco NX-OS FabricPath unicast Layer 2 equal cost multipath is on by default.

The default FabricPath unicast load balancing mechanism on the Nexus 7000 with F1/M1 line cards and the Nexus 5000 uses Layer 2/Layer 3/Layer 4 source and destination addresses and VLAN with symmetric hashing, while on the Nexus 7000 with F2 line cards, the default FabricPath unicast load balancing uses Layer 3/Layer 4 source and destination addresses without the VLAN included. To avoid hash polarization, each Cisco FabricPath switch automatically rotates the hash string by a number of bytes based on the system MAC address.

NVT has changed Nexus 7000 spine FabricPath unicast balancing mechanism by the following command and kept the Nexus 5000 FabricPath unicast load-balance as default.

F2 VDC	F1/M1 VDC
! Change port-channel load-balance on main VDC DC5-sup2(config)# fabricpath load-balance source-destination	! Change FabricPath load-balance on F1/M1VDC DC102-52(config)# fabricpath load-balance source-destination
! Change FabricPath load-balance unicast on spine F2 VDC DC202-51(config)# fabricpath load-balance unicast rotate-amount 0xb include-vlan	! Change FabricPath load-balance unicast on spine F1/M1 VDC DC102-52(config)# fabricpath load-balance unicast layer3 include-vlan
! Verify Nexus 7000 spine FabricPath load-balance after modify DC202-51(config)# sh fabricpath load-balance ECMP load-balancing configuration: L3/L4 Preference: Mixed Rotate amount: 11 bytes Use VLAN: TRUE Ftag load-balancing configuration: Rotate amount: 3 bytes Use VLAN: TRUE	! Verify Nexus 7000 spine FabricPath load-balance after modify DC102-52(config)# sh fabricpath load-balance ECMP load-balancing configuration: L3/L4 Preference: L3 Hash Control: Source-Destination Rotate amount: 14 bytes Use VLAN: TRUE Ftag load-balancing configuration: Hash Control: Source-Destination Rotate amount: 14 bytes Use VLAN: TRUE

In the NVT FabricPath network topology there are four equal cost paths from one leaf switch to any other leaf switch, except its vPC+ peer.

To verify the FabricPath unicast ECMP path and load-balancing in leaf switch Nexus 5000, use the following commands.

Display information about all FabricPath topology interfaces

```
DC202-705# sh fabricpath topology interface
Interface           Topo-Description                Topo-ID    Topo-IF-State
------------------- ------------------------------- ---------- -------------
port-channel51      0                               0              Up
port-channel52      0                               0              Up
port-channel53      0                               0              Up
port-channel54      0                               0              Up
port-channel706     0                               0              Up
```

Display all FabricPath IS-IS adjacency information

```
DC202-705# sh fabricpath isis adjacency
Fabricpath IS-IS domain: default Fabricpath IS-IS adjacency database:
System ID       SNPA            Level  State  Hold Time  Interface
DC202-51        N/A             1      UP     00:00:30   port-channel51
DC202-52        N/A             1      UP     00:00:32   port-channel52
DC202-53        N/A             1      UP     00:00:23   port-channel53
DC202-54        N/A             1      UP     00:00:23   port-channel54
DC202-706       N/A             1      UP     00:00:24   port-channel706
```

Display the FabricPath Layer 2 IS-IS routing table for unicast routes

```
N5k-705# sh fabricpath isis route
```

```
Fabricpath IS-IS domain: default MT-0
Topology 0, Tree 0, Swid routing table
251, L1
 via port-channel51, metric 20
252, L1
 via port-channel52, metric 20
253, L1
 via port-channel53, metric 20
254, L1
 via port-channel54, metric 20
271, L1
 via port-channel51, metric 40
 via port-channel53, metric 40
 via port-channel52, metric 40
 via port-channel54, metric 40
272, L1
 via port-channel51, metric 40
 via port-channel53, metric 40
 via port-channel52, metric 40
 via port-channel54, metric 40
273, L1
 via port-channel51, metric 40
 via port-channel53, metric 40
 via port-channel52, metric 40
 via port-channel54, metric 40
274, L1
 via port-channel51, metric 40
 via port-channel53, metric 40
 via port-channel52, metric 40
 via port-channel54, metric 40
276, L1
 via port-channel706, metric 20
1001, L1
 via port-channel51, metric 20
 via port-channel52, metric 20
1002, L1
 via port-channel53, metric 20
 via port-channel54, metric 20
2001, L1
 via port-channel51, metric 40
 via port-channel53, metric 40
 via port-channel52, metric 40
 via port-channel54, metric 40
2002, L1
 via port-channel51, metric 40
 via port-channel53, metric 40
 via port-channel52, metric 40
 via port-channel54, metric 40
706, L1
 via port-channel706, metric 20
```

Display unicast routes to switch-ID 271

```
N5k-705# sh l2 route switchid 271
FabricPath Unicast Route Table
'a/b/c' denotes ftag/switch-id/subswitch-id
'[x/y]' denotes [admin distance/metric]
ftag 0 is local ftag
subswitch-id 0 is default subswitch-id


FabricPath Unicast Route Table for Topology-Default

1/271/0, number of next-hops: 4
        via Po51, [115/40], 0 day/s 12:18:25, isis_fabricpath-default
        via Po52, [115/40], 0 day/s 04:00:31, isis_fabricpath-default
```

```
        via Po53, [115/40], 0 day/s 10:54:47, isis_fabricpath-default
        via Po54, [115/40], 0 day/s 03:59:12, isis_fabricpath-default
```

Display FabricPath unicast Ftag information

```
DC202-705# sh fabricpath topology ftag unicast
Topo-Description          Topo-ID    Graph-ID  Ftag
------------------------- ---------- --------- ---------
0                         0          1         1
```

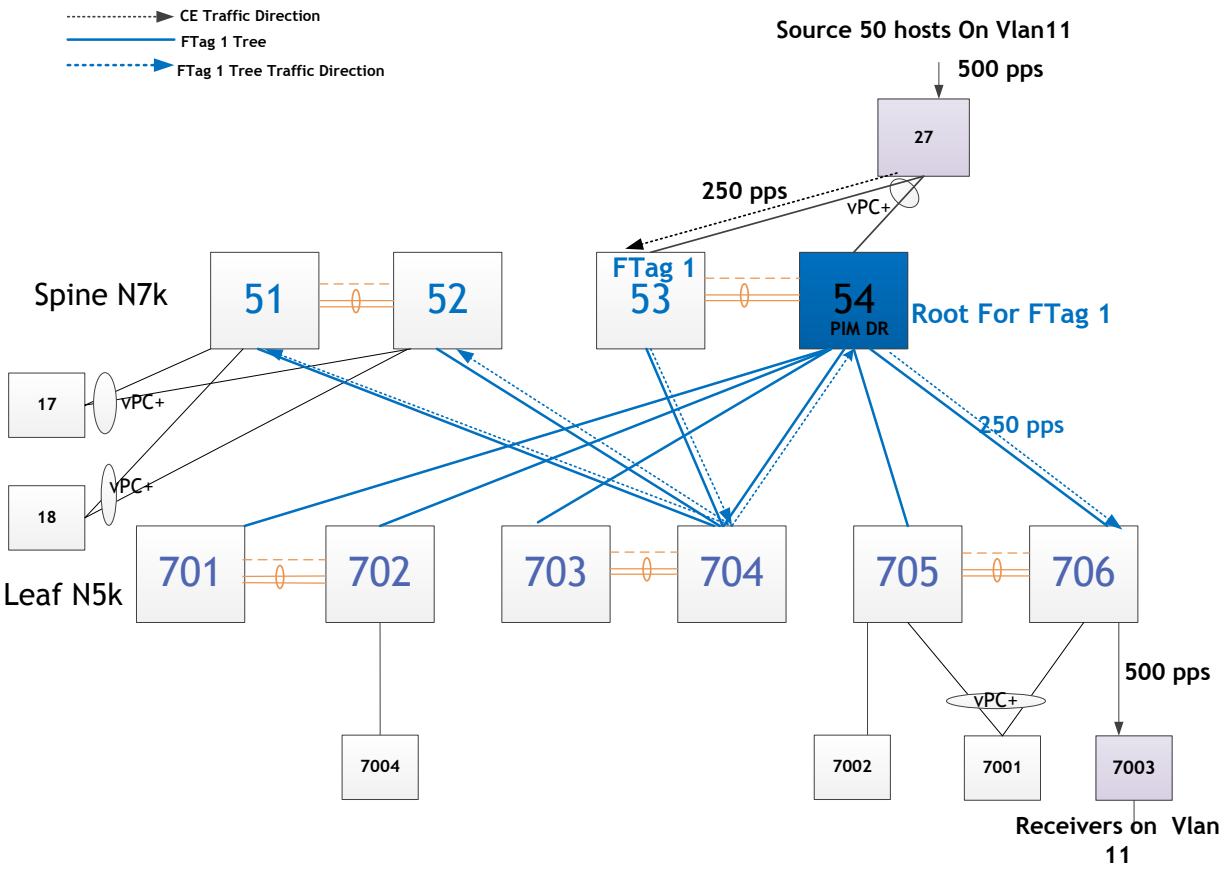
Display which path the FabricPath unicast load-balancing utilizes for a given flow

```
DC202-705# sh fabricpath load-balance unicast forwarding-path ftag 1 switchid 271 dst-ip 201.11.7.1
Missing params will be substituted by 0's.

crc8_hash: 28
This flow selects interface Po51

DC202-705# sh fabricpath load-balance unicast forwarding-path ftag 1 switchid 271 dst-ip 201.11.7.2

Missing params will be substituted by 0's.

crc8_hash: 42
This flow selects interface Po53
```

3.4.2.9.2 FabricPath Multicast Load-balancing And Verification

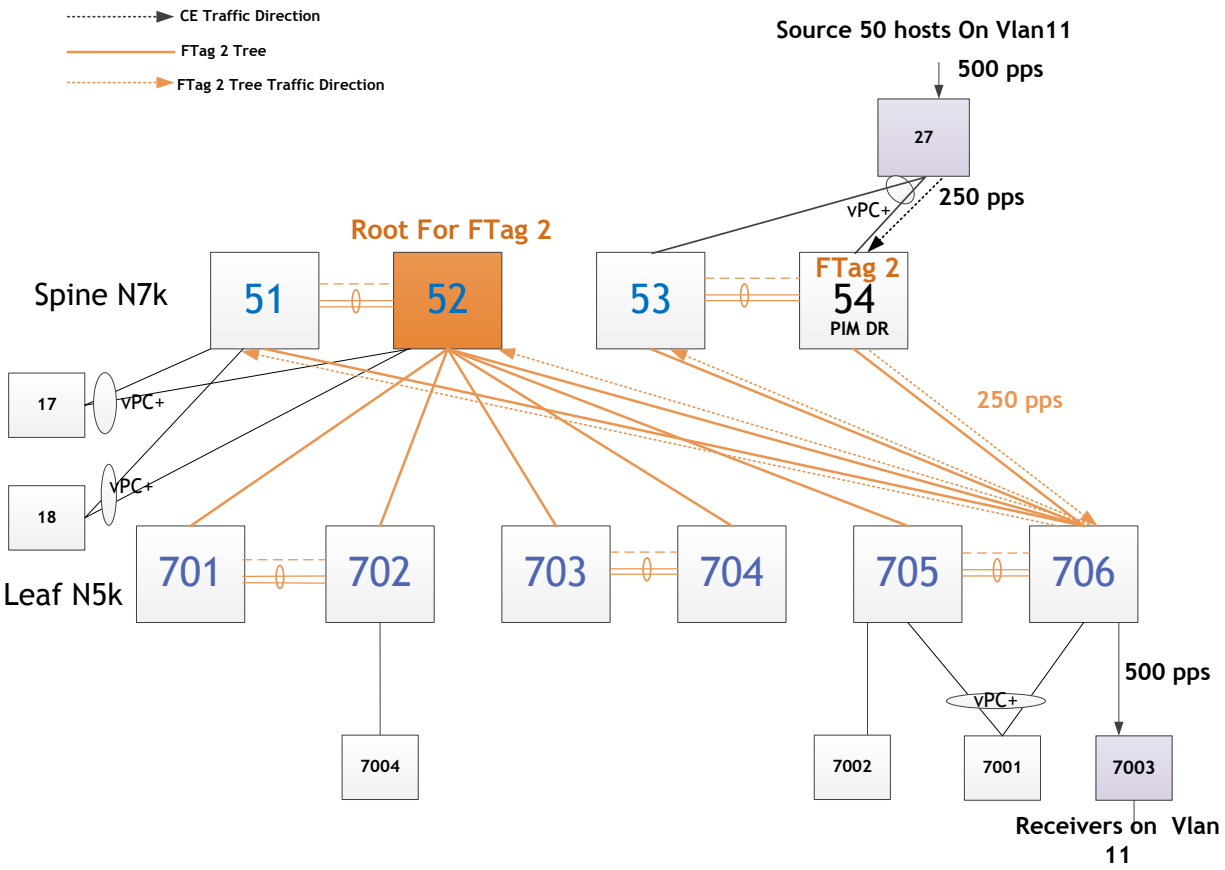
In the NVT FabricPath topology excerpt shown below, the multicast traffic source is located on the L2 switch 27 and the receiver is located on the L2 switch 7003. Multicast traffic that reaches the spine 53 selects FTag 1 and uses tree 1 to forward the multicast data to the receiver which is attached to leaf switch 706. Note that the multicast traffic is also forwarded to all other spines because of PIM neighborship.

Figure 12 FabricPath Ftag 1 Multi-destination Tree



The Multicast traffic that reaches the spine 54 selects FTag 2 and uses tree 2 to forward the multicast data to the receiver which is attached to leaf switch 706. Note that this multicast traffic is also forwarded to all other spines because of PIM neighborship.

Figure 13 FabricPath Ftag 2 Multi-destination Tree



The hashing to either multi-destination tree is platform-dependent and the hash function is per flow. The default multicast load balancing mechanism for Nexus 7000 F1 VDC uses a symmetric hash input combining both Layer 3 (source and destination IP addresses) and Layer 4 (source and destination TCP and UDP port numbers, if present) information, as well as the VLAN ID; while in Nexus 7000 F2 VDC it does not include the VLAN ID. The default multicast load balancing mechanism for the Nexus 5000 uses symmetric hash with Layer 2/Layer 3/Layer 4 source and destination addresses as well as VLAN ID.

NVT has changed Nexus 7000 F2 VDC multicast load balancing mechanism to include Vlan while leaving Nexus 7000 F1/M1 VDC and Nexus 5000 as default.

```
DC202-51(config)#  fabricpath load-balance multicast rotate-amount 0x3 include-vlan

N7k-51(config)# sh run fabricpath  | in "multicast"
fabricpath load-balance multicast rotate-amount 0x3 include-vlan

N7k-51(config)# sh fabricpath load-balance
ECMP load-balancing configuration:
L3/L4 Preference: Mixed
Rotate amount: 11 bytes
Use VLAN: TRUE
```

```
Ftag load-balancing configuration:
Rotate amount: 3 bytes
Use VLAN: TRUE
```

To verify the FabricPath multicast load-balancing path for a given multicast group in Nexus 7000, use the following commands.

Display the IP multicast routes for vlan 11, group 230.202.0.1

```
DC202-54# sh fabricpath isis ip mroute vlan 11 group 230.202.0.1
Fabricpath IS-IS domain: default
Fabricpath IS-IS IPv4 Multicast Group database
VLAN 11: (*, 230.202.0.1)
  Outgoing interface list: (count: 6)
    SWID: 0xfb (251)
    SWID: 0xfc (252)
    SWID: 0xfd (253)
    SWID: 0x110 (272)
    SWID: 0x113 (275)
    SWID: 0x114 (276)
```

Display FabricPath multicast routes for vlan 11

```
DC202-54# sh fabricpath mroute vlan 11

(vlan/11, 0.0.0.0, 224.0.1.39), uptime: 19:21:48, isis igmp
 Outgoing interface list: (count: 4)
  Interface Vlan11, [SVI] uptime: 19:20:25, igmp
  Switch-id 251, uptime: 16:16:00, isis
  Switch-id 252, uptime: 19:20:23, isis
  Switch-id 253, uptime: 16:15:06, isis

(vlan/11, 0.0.0.0, 224.0.1.40), uptime: 19:21:48, isis igmp
 Outgoing interface list: (count: 4)
  Interface Vlan11, [SVI] uptime: 19:20:25, igmp
  Switch-id 251, uptime: 16:16:07, isis
  Switch-id 252, uptime: 19:20:23, isis
  Switch-id 253, uptime: 16:15:06, isis

(vlan/11, 0.0.0.0, 230.202.0.1), uptime: 16:00:05, isis igmp
 Outgoing interface list: (count: 7)
  Interface port-channel27, uptime: 16:00:04, igmp
  Switch-id 251, uptime: 16:00:04, isis
  Switch-id 252, uptime: 16:00:04, isis
  Switch-id 253, uptime: 16:00:04, isis
  Switch-id 272, uptime: 16:00:04, isis
  Switch-id 275, uptime: 16:00:05, isis
  Switch-id 276, uptime: 16:00:05, isis

 (vlan/11, *, *), Flood, uptime: 19:21:48, isis
 Outgoing interface list: (count: 9)
  Switch-id 251, uptime: 16:16:16, isis
  Switch-id 252, uptime: 19:21:48, isis
  Switch-id 253, uptime: 16:15:16, isis
  Switch-id 271, uptime: 19:21:48, isis
```

```
  Switch-id 272, uptime: 19:21:48, isis
  Switch-id 273, uptime: 19:21:48, isis
  Switch-id 274, uptime: 19:21:48, isis
  Switch-id 275, uptime: 19:21:48, isis
  Switch-id 276, uptime: 19:21:48, isis

(vlan/11, *, *), Router ports (OMF), uptime: 19:21:48, isis igmp
 Outgoing interface list: (count: 5)
  Interface Vlan11, [SVI] uptime: 19:21:48, igmp
  Interface port-channel53, uptime: 19:21:48, igmp
  Switch-id 251, uptime: 16:16:14, isis
  Switch-id 252, uptime: 19:21:48, isis
  Switch-id 253, uptime: 16:15:16, isis

Found total 5 route(s)
```

Display FabricPath topology FTag information

```
DC202-54# sh fabricpath topology ftag multicast
Topo-Description          Topo-ID    Graph-ID  Ftag
------------------------- ---------- --------- ---------
0                         0          1         1
0                         0          2         2
DC202-54# sh fabricpath topology ftag active
Topo-Description          Topo-ID    Graph-ID  Ftag
------------------------- ---------- --------- ---------
0                         0          2         2
```

Display FabricPath multicast load-balancing information

```
DC202-54# sh fabricpath load-balance multicast ftag-selected flow-type l3 src-ip 202.11.27.1 dst-ip
230.202.0.1 vlan 12 module 2
128b Hash Key generated : 40 39 00 00 00 00 00 00 32 82 c6 c0 79 b2 80 00
0x8c
    FTAG SELECTED IS : 2 (HASH 140)
```

Display FabricPath multicast route for vlan 11, ftag 2

```
DC202-54# sh fabricpath mroute vlan 11 ftag 2

(ftag/2, vlan/11, 0.0.0.0, 224.0.1.39), uptime: 19:25:55, isis igmp
 Outgoing interface list: (count: 4)
  Interface Vlan11, [SVI] uptime: 19:24:32, igmp
  Interface port-channel706,   Switch-id 251, uptime: 16:20:24, isis
  Interface port-channel706,   Switch-id 252, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 253, uptime: 16:19:23, isis

(ftag/2, vlan/11, 0.0.0.0, 224.0.1.40), uptime: 19:25:55, isis igmp
 Outgoing interface list: (count: 4)
  Interface Vlan11, [SVI] uptime: 19:24:32, igmp
  Interface port-channel706,   Switch-id 251, uptime: 16:20:24, isis
  Interface port-channel706,   Switch-id 252, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 253, uptime: 16:19:23, isis

 (ftag/2, vlan/11, 0.0.0.0, 230.202.0.1), uptime: 16:04:12, isis igmp
 Outgoing interface list: (count: 7)
  Interface port-channel27, uptime: 16:04:11, igmp
```

```
  Interface port-channel706,   Switch-id 251, uptime: 16:20:24, isis
  Interface port-channel706,   Switch-id 252, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 253, uptime: 16:19:23, isis
  Interface port-channel706,   Switch-id 272, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 275, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 276, uptime: 19:25:55, isis

 (ftag/2, vlan/11, *, *), Flood, uptime: 19:25:55, isis
 Outgoing interface list: (count: 9)
  Interface port-channel706,   Switch-id 251, uptime: 16:20:24, isis
  Interface port-channel706,   Switch-id 252, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 253, uptime: 16:19:23, isis
  Interface port-channel706,   Switch-id 271, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 272, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 273, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 274, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 275, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 276, uptime: 19:25:55, isis

(ftag/2, vlan/11, *, *), Router ports (OMF), uptime: 19:25:55, isis igmp
 Outgoing interface list: (count: 5)
  Interface Vlan11, [SVI] uptime: 19:25:55, igmp
  Interface port-channel53, uptime: 19:25:55, igmp
  Interface port-channel706,   Switch-id 251, uptime: 16:20:24, isis
  Interface port-channel706,   Switch-id 252, uptime: 19:25:55, isis
  Interface port-channel706,   Switch-id 253, uptime: 16:19:23, isis

Found total 5 route(s)
```

To verify the traffic path for a given multicast group in Nexus 5000 leaf switch, use the following commands.

Display the IP multicast routes for vlan 11, group 230.202.0.1

```
DC202-706# sh fabricpath isis ip mroute vlan 11 group 230.202.0.1
Fabricpath IS-IS domain: default
Fabricpath IS-IS IPv4 Multicast Group database
VLAN 11: (*, 230.202.0.1)
  Outgoing interface list: (count: 6)
    SWID: 0xfb (251)
    SWID: 0xfc (252)
    SWID: 0xfd (253)
    SWID: 0xfe (254)
    SWID: 0x110 (272)
    SWID: 0x113 (275)
```

Display FabricPath multicast routes for vlan 11

```
DC202-706# sh fabricpath mroute vlan 11

(vlan/11, 0.0.0.0, 224.0.1.39), uptime: 6d21h, isis
 Outgoing interface list: (count: 4)
  Switch-id 251, uptime: 16:54:03, isis
  Switch-id 252, uptime: 19:58:27, isis
  Switch-id 253, uptime: 16:53:09, isis
  Switch-id 254, uptime: 19:58:27, isis

(vlan/11, 0.0.0.0, 224.0.1.40), uptime: 6d21h, isis
```

```
 Outgoing interface list: (count: 4)
  Switch-id 251, uptime: 16:54:10, isis
  Switch-id 252, uptime: 19:58:27, isis
  Switch-id 253, uptime: 16:53:09, isis
  Switch-id 254, uptime: 19:58:27, isis

(vlan/11, 0.0.0.0, 230.202.0.1), uptime: 16:38:09, isis igmp
 Outgoing interface list: (count: 8)
  Switch-id 251, uptime: 16:38:07, isis
  Switch-id 252, uptime: 16:38:07, isis
  Switch-id 253, uptime: 16:38:07, isis
  Switch-id 254, uptime: 16:38:07, isis
  Switch-id 272, uptime: 16:38:07, isis
  Switch-id 275, uptime: 16:38:08, isis
  Interface port-channel1, uptime: 16:38:09, igmp
  Interface port-channel3, uptime: 16:38:08, igmp

 (vlan/11, *, *), Flood, uptime: 7w6d, isis
 Outgoing interface list: (count: 9)
  Switch-id 251, uptime: 16:54:19, isis
  Switch-id 252, uptime: 21:14:55, isis
  Switch-id 253, uptime: 16:53:20, isis
  Switch-id 254, uptime: 21:13:45, isis
  Switch-id 271, uptime: 4w2d, isis
  Switch-id 272, uptime: 7w6d, isis
  Switch-id 273, uptime: 7w6d, isis
  Switch-id 274, uptime: 7w6d, isis
  Switch-id 275, uptime: 7w6d, isis

(vlan/11, *, *), Router ports (OMF), uptime: 7w6d, isis
 Outgoing interface list: (count: 4)
  Switch-id 251, uptime: 16:54:17, isis
  Switch-id 252, uptime: 21:14:55, isis
  Switch-id 253, uptime: 16:53:20, isis
  Switch-id 254, uptime: 21:13:43, isis

Found total 5 route(s)
```

Display FabricPath topology FTag information

```
DC202-706# sh fabricpath topology ftag multicast
Topo-Description          Topo-ID    Graph-ID  Ftag
------------------------- ---------- --------- ---------
0                         0          1         1
0                         0          2         2
DC202-706# sh fabricpath topology ftag active
Topo-Description          Topo-ID    Graph-ID  Ftag
------------------------- ---------- --------- ---------
0                         0          1         1
```

Display FabricPath multicast load-balancing information

```
DC202-706# sh fabricpath load-balance multicast ftag-selected vlan 11 macg 0100.5e4d.0001

 If the traffic is received on a non-vPC port:
 Ftag selected : 1

 If the traffic is received on a vPC port:
 Ftag selected : 1

=====================================

 Vlan : 11 (int_vlan : 15)
 Macg : 0100.5e4d.0001

 Hash-key : 0x000f0000 00000000
 Hash-val : 34
 Num_trees : 2
```

```
=====================================
```

Display FabricPath multicast route for a vlan 11, ftag 1

```
DC202-706# sh fabricpath mroute vlan 11 ftag 1


(ftag/1, vlan/11, 0.0.0.0, 224.0.1.39), uptime: 6d21h, isis
 Outgoing interface list: (count: 4)
  Interface port-channel54, uptime: 17:02:31, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 17:01:30, isis
  Interface port-channel54, uptime: 21:21:33, isis

(ftag/1, vlan/11, 0.0.0.0, 224.0.1.40), uptime: 6d21h, isis
 Outgoing interface list: (count: 4)
  Interface port-channel54, uptime: 17:02:31, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 17:01:30, isis
  Interface port-channel54, uptime: 21:21:33, isis

(ftag/1, vlan/11, 0.0.0.0, 230.202.0.1), uptime: 16:46:22, isis igmp
 Outgoing interface list: (count: 8)
  Interface port-channel54, uptime: 17:02:31, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 17:01:30, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel1, uptime: 16:46:22, igmp
  Interface port-channel3, uptime: 16:46:20, igmp

 (ftag/1, vlan/11, *, *), Flood, uptime: 7w6d, isis
 Outgoing interface list: (count: 9)
  Interface port-channel54, uptime: 17:02:31, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 17:01:30, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 21:21:33, isis

(ftag/1, vlan/11, *, *), Router ports (OMF), uptime: 7w6d, isis
 Outgoing interface list: (count: 4)
  Interface port-channel54, uptime: 17:02:31, isis
  Interface port-channel54, uptime: 21:21:33, isis
  Interface port-channel54, uptime: 17:01:30, isis
  Interface port-channel54, uptime: 21:21:33, isis

Found total 5 route(s)
```

3.4.3 Fabric Extenders (FEX)

The **Fabric Extender** integrates with its parent switch, which is a Cisco Nexus Series device, to allow automatic provisioning and configuration taken from the settings on the parent device.

The **Fabric Interface** is an uplink port that is designated for connection from the Fabric Extender to its parent switch. A fabric interface cannot be used for any other purpose. It must be directly connected to the parent switch. Multiple fabric interfaces can be combined together to form a **port-channel fabric**

interface. Beginning with Cisco NX-OS Release 6.1(3), you can configure a minimum number of links for the FEX fabric port channel so that when a certain number of FEX fabric port-channel member ports go down, the host-facing interfaces of the FEX are suspended.

The **host interfaces** are Ethernet host interfaces for connection to a server or host system.

```
feature-set fex

fex 101
  pinning max-links 1
  description FEX0101

! Port-channel fabric interface
interface port-channel101
  switchport
  switchport mode fex-fabric
  fex associate 101
  port-channel min-links 2

interface Ethernet10/1
  switchport
  switchport mode fex-fabric
  fex associate 101
  channel-group 101
  no shutdown

! Port-channel host interface
interface port-channel201
  switchport
  switchport access vlan 11
  spanning-tree port type edge
  spanning-tree bpdufilter enable
  flowcontrol send on
  vpc 201

interface Ethernet101/1/1
  switchport
  switchport access vlan 11
  logging event port link-status
  channel-group 201 mode active
  no shutdown
```

Display the fabric extenders attached to the system

```
DC6-DC101-6# show fex
  FEX         FEX           FEX                 FEX
Number    Description      State            Model            Serial
------------------------------------------------------------------------
101        FEX0101               Online     N2K-C2224TP-1GE   SSI15480E4B
103        FEX0103               Online     N2K-C2248TP-1GE   SSI161509VH
104        FEX0104               Online    N2K-C2232PP-10GE   SSI160700MV
105        FEX0105               Online    N2K-C2232PP-10GE   SSI16070CM8
```

Since the FEX host interfaces are supposed to be connected directly to hosts, certain defaults should be noted as shown below. Also, **cdp** is **not** supported on the Fabric Extenders connected to a Nexus 7000 parent switch.

```
DC6-DC101-6# show run int e101/1/1 all
interface Ethernet101/1/1
  no description
```

```
  lacp port-priority 32768
  lacp rate normal
  lldp transmit
  lldp receive
  switchport
  switchport mode access
  no switchport dot1q ethertype
  switchport access vlan 11
  switchport trunk native vlan 1
  switchport trunk allowed vlan 1-4094
  spanning-tree port-priority 128
  spanning-tree cost auto
  spanning-tree link-type auto
  spanning-tree port type edge
  spanning-tree bpduguard enable
  no spanning-tree bpdufilter
  speed auto
  duplex auto
  flowcontrol receive off
  flowcontrol send on
  link debounce time 100
  no beacon
  delay 1
  snmp trap link-status
  logging event port link-status
  logging event port trunk-status default
  medium broadcast
  channel-group 201 mode active
    lacp suspend-individual
  no ip dhcp snooping trust
  no ip dhcp snooping limit rate
  no ip arp inspection trust
  ip arp inspection limit rate 15 burst interval 5
  no ip verify source dhcp-snooping-vlan
  no shutdown
```

3.5 Unified Computing System (UCS) Overview

Cisco Unified Computing System (UCS) combines computing, networking, management, virtualization and storage access into a single integrated architecture.

3.5.1 UCS Management & Monitoring

Cisco Unified Computing System Manager (UCSM) is the management system for all components in a Cisco UCS domain and runs on the fabric interconnect (FI). Any of the interfaces available with this management service can be used to access, configure, administer and monitor the network and blade resources for all chassis connected to the Fabric Interconnect (FI).

Cisco UCS Manager includes the following user interfaces that can be used to manage a Cisco UCS domain:

- Cisco UCS Manager GUI
- Cisco UCS Manager CLI

NVT has provisioned out-of-band (OOB) networks for network infrastructure and virtual machine management.

3.5.1.1 Image Upgrade

NVT has configured NTP and time zones to ensure that the clocks on all UCS infrastructure and chassis components are synchronized.

The following issues may be encountered if the clocks are not synchronized:

- IOM may freeze during image upgrade (CSCuh25709/CSCuh25841/CSCuh87431).
  - To be addressed as part of feature enhancement: CSCtg28246 - *System / Fabric A&B Clock Set and Synchronization*.
  - Workaround: Manually OIR the failed IOM
- The upgrade procedure continuously retries step "Deploy Poll Activate Of Local FI" during the firmware install process (CSCui13535).
  - Workaround: Manually issue the install firmware command again with the 'Force' option enabled.

3.5.1.2 Syslogs

NVT has configured syslog to report to a centralized server.

Verification of Syslogs through the UCSM CLI

```
UCS-FI-106-01-A# scope monitoring
UCS-FI-106-01-A /monitoring # show syslog

console
    state: Enabled
    level: Alerts

monitor
    state: Enabled
    level: Information

file
    state: Enabled
    level: Information
    name:  UCS-FI-106-01
    size:  4194304

remote destinations
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
    Server 1 172.28.92.10         Enabled  Information   Local6
    Server 2 none                 Disabled Critical      Local7
    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Enabled
    events: Enabled


UCS-FI-106-01-A /monitoring #
```

3.5.2 UCS Blade Management

In order to provision blade servers, service profiles need to be defined using policies and resource pools.

3.5.2.1 Service Profiles & Blade Policies

Service profiles must be created in order to provision compute services on the blade servers. All service profiles are configured with two static vNICs: vNIC0 for management and vNIC1 for data-plane traffic. Service profiles are made up of a set of policies and address pools, including the following:

- **Local Disk Policy** – NVT has configured RAID 1 when local disks are present. Any modifications to the disk policy may result in data loss.
- **BIOS Policy** – NVT has configured the BIOS policy enabling Virtualization Technology (VT) and Intel Directed IO for higher performance on the virtual machines deployed on the blade servers. These are required in order to leverage the performance advantage of VM-FEX.
- **Maintenance Policy** – NVT has configured the "UserACK" policy option instead of "Immediate". When this option is selected, the blade server is not immediately rebooted when changes to the service profile are made. Instead, the service profile will show the pending changes in its status field, and will wait for the administrator to manually acknowledge the changes to reboot the blade server.
- **Dynamic vNIC Connection Policy** – NVT has allocated 50 dynamic vNICs per blade server. Each of these dynamic vNIC connection policies has been configured with a "VMWarePassThru" adapter policy for performance and the "Protected" option to enable failover.
- **MAC Address Pools** – NVT has configured MAC Address Pools as part of the Service Profiles in order to provide addresses to the hypervisor or bare metal OS on the blade server.

Service profile templates facilitate the reuse and rapid-deployment of service profiles. There are two types of templates supported:

- **Initial template** – Service profiles created from an initial template inherit all the properties of the template. After the creation of a service profile from the template, any changes to the template no longer affect the replicated service profiles.
- **Updating templates** – Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

NVT makes use of Updating templates in order to quickly propagate service profile changes to facilitate test configurations.

3.5.3 UCS Uplink Port Infrastructure

Any port on the Fabric Interconnect can be configured as either an uplink port or a server port. NVT makes use of End-Host Mode on the uplink ports.

Verification of End-Host mode through the UCSM CLI

```
UCS-FI-106-01-A# scope eth-uplink
UCS-FI-106-01-A /eth-uplink # show detail

Ethernet Uplink:
    Mode: End Host
    MAC Table Aging Time (dd:hh:mm:ss): Mode Default
    VLAN Port Count Optimization: Disabled
```

```
    Current Task:
UCS-FI-106-01-A /eth-uplink #
```

In End-Host mode, a single uplink port/port channel on each FI is chosen to be the receiver for broadcast, multicast and unknown-unicast traffic on all VLANs. This port is called the G-pinned port and is selected by the system.

Verification of the G-pinned port in UCSM CLI

```
UCS-FI-106-01-A(nxos)# show platform software enm internal info vlandb id 11

vlan_id 11
-------------
Designated receiver: Po71
Membership:
Po71
UCS-FI-106-01-A(nxos)#
```

3.5.3.1 Uplink Port-Channels

Cisco UCS uses Link Aggregation Control Protocol (LACP) to bundle the uplink ports into a port channel. In order to maximize throughput from the FIs while also guaranteeing both high-availability and load-sharing to the upstream switches, NVT has configured up to eight ports per uplink port-channel.

NVT uses static pinning to assign VM data traffic to specific uplink port-channels. This configuration is done using LAN Pin Groups.

Verification of LAN Pin Groups through the UCSM CLI

```
UCS-FI-106-01-A# scope eth-uplink
UCS-FI-106-01-A /eth-uplink # show pin-group expand

Ethernet Pin Group:
    Name: DC106-5-6

    Ethernet Pin Target:
        Fabric Endpoint
        ------ --------
        A      fabric/lan/A/pc-71
        B      fabric/lan/B/pc-72

    Name: Management

    Ethernet Pin Target:
        Fabric Endpoint
        ------ --------
        A      fabric/lan/A/phys-slot-1-port-32
        B      fabric/lan/B/phys-slot-1-port-32
UCS-FI-106-01-A /eth-uplink #
```

3.5.3.2 VLAN Configuration

NVT has configured *common*/*global* VLANs that span across both Fabric Interconnects in a cluster. Note that VLANs with IDs from 3968 to 4043 and 4094 are reserved and cannot be created for data traffic.

Display Reserved VLANs on the FIs

```
UCS-FI-106-01-A(nxos)# show vlan internal usage

VLAN        DESCRIPTION
---------   ----------------------------------------------------------
3968-4031   Multicast
4032        Online diagnostics vlan1
4033        Online diagnostics vlan2
4034        Online diagnostics vlan3
4035        Online diagnostics vlan4
4036-4043   Reserved
4094        Reserved

UCS-FI-106-01-A(nxos)#
```

Verification of VLANs through the UCSM CLI

```
UCS-FI-106-01-A(nxos)# show vlan id 11

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
11   VLAN0011                         active    Po71

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------



UCS-FI-106-01-A(nxos)#
```

3.5.3.2.1 VLAN Groups

NVT configured an out-of-band management domain on separate VLAN groups for all deployed FIs and VMs. VLANs 2 & 3 are associated for management network interfaces. VLANs 11-20 & 2001-2010 are associated with data plane network interfaces.

Verification of VLAN Groups through the UCSM CLI

```
UCS-FI-106-01-A# scope eth-uplink
UCS-FI-106-01-A /eth-uplink # show vlan-group

    Network Group:

    Name                 Size   Native VLAN Name     Native VLAN
    -------------------- ------ -------------------- -----------
    Data_Uplink          20

    Management_Uplink    2      vlan2                fabric/lan/net-vlan2
UCS-FI-106-01-A /eth-uplink #
```

3.5.4 UCS Server Port Infrastructure

In order to obtain maximum throughput from the IOMs, NVT has utilized eight connections from the FI to the IOM. All links from an individual IOM must connect to the same FI because intercrossed connections are not supported.

3.5.4.1 Chassis Discovery Policy with Port Channels

NVT has configured the minimum number of links needed to discover the chassis and set the Link Grouping Preference to Port Channel.

3.5.5 UCS Distributed Virtual Switches (DVS)

NVT has enabled VM-FEX and all inter-VLAN traffic is forwarded by the FI to the upstream gateway switch for routing.

NVT has configured DirectPath I/O to increase performance from the VMs through the hypervisor.

Distributed virtual switches created by UCSM cannot span across multiple FI clusters. The UCSM running on a FI cluster can only create and manage distributed virtual switches within that cluster (CSCuh38886).

3.5.5.1 Port Profiles

NVT has configured port profiles for each *common*/*global* VLAN so that all VM interfaces can be logically separated by VLAN ID.

Verification of Port Profiles through the UCSM CLI

```
UCS-FI-106-01-A(nxos)# show port-profile brief
------------------------------------------------------------
Port                Profile  Conf   Eval   Assigned  Child
Profile              State   Items  Items  Intfs     Profs
------------------------------------------------------------
UCS_Vlan11          1        8      8      0         0
UCS_Vlan12          1        8      8      0         0
UCS_Vlan13          1        8      8      0         0
UCS_Vlan14          1        8      8      0         0
UCS_Vlan15          1        8      8      0         0
UCS_Vlan16          1        8      8      0         0
UCS_Vlan17          1        8      8      0         0
UCS_Vlan18          1        8      8      0         0
UCS_Vlan19          1        8      8      0         0
UCS_Vlan3           1        7      7      0         0
ucsm_internal_rackserver_portprofile 1        3      3      0         0
UCS-FI-106-01-A(nxos)#
```

4. NVT Test Methodology

4.1 Host/Server Configuration

4.1.1 Traffic Generator Configuration

Unicast Hosts configuration:

- Block 1: Nexus 7000 vPC block consists of [20vlans x 120hosts] spread across layer 2 ToR devices and FEX.

- Block 2: Nexus 7000/5000 FabricPath Block consists of [20vlans x 350hosts] spread across layer 2 devices attached to the leaf and spine of the fabricpath network.
- Blocks 3-7: These blocks consist of [20vlans x 100hosts] in each block.

Each host in the network sends traffic to all other hosts to form a fully meshed traffic configuration.

Multicast Source Configuration:

- Block 1: Nexus 7000 vPC block consists of 100hosts spread across layer 2 ToR devices sourcing multicast traffic for groups with local RP.
- Block 2: Nexus 7000/5000 FabricPath Block consists of 350hosts spread across layer 2 devices attached to the leaf and spine of the fabricpath network sourcing multicast traffic for groups with local RP.
- Blocks 3-7: These blocks consist of 100hosts in each block sourcing multicast traffic for groups with local RP.

Multicast Receiver Configuration:

- Block 1: Nexus 7000 vPC block consists of [20vlans x 2hosts] spread across layer 2 ToR devices and FEX joining all multicast groups sourced in the network.
- Block 2: Nexus 7000/5000 FabricPath Block consists of [20vlans x 7host] spread across layer 2 devices attached to the leaf and spine of the fabricpath network joining all multicast groups sourced in the network.
- Blocks 3-7: These blocks consist of [20vlans x 2hosts] in each block joining all multicast groups sourced in the network.

4.1.2 UCSM Test Methodology

All NVT UCS test cases have been verified and debugged leveraging the following UCSM tools and capabilities:

- Fault Summary Area
- Finite State Machine (FSM)
- Statistics Collection Policies

4.1.3 Provisioning of Virtual Machines (VMs)

- Each blade is configured with a VMWare ESXi 5.1 hypervisor deploying 5 VMs with 10 network adapters each:
    - The first network adapter is always utilized for Out-of-Band (OOB) management running in VM-FEX in Emulated Mode.
    - The remaining network adapters are configured for distinct VLAN data-plane traffic with VM-FEX in VMDirectPath Mode. All inter-VLAN traffic is forwarded by a single designated network adapter.
- Upon bootup, each VM's network interface obtains its particular interface information from the DHCP server based upon its assigned MAC address.
- Both stateful and stateless traffic are sent and received by each VM's network interfaces; all traffic is sent and received across and within FI clusters.

4.1.4 VMware® vMotion™

VMware® vMotion™ was performed within the FI cluster traversing the vPC+ connections while running in VM-FEX mode. As part of the testing, active traffic was sent and received by the virtual machines being migrated.

4.2 Test Cycle

The test cycle consists of the following steps:

1. Network configuration and verification
2. Software and firmware upgrade and downgrade
3. Trigger network disruptions
4. Stress platform control-plane
5. Check for CPU usage anomalies and Memory leaks

4.3 Network Disruption Test Cases

The following sections describe the test disruptions and the verification criteria:

- System Level
- Core Layer
- Spine Layer
- Leaf Layer

System Level

Disruption	**Verification**
Image upgrade and rollback with ISSU	Hitless upgrade/rollback for all configured features with parallel enhancement

Core Layer

Disruption	**Verification**
Router Link Failure/Recovery between Core and Edge	• IGP and PIM reconvergence (control-plane & data plane)
Member of Port-channel Failure/Recovery between Core and Edge	• Traffic load-sharing for port-channels • LACP interoperability • Unidirectional Link Detection (UDLD)
Clear IGP Neighbors/Process at Core	Stress test for control-plane recovery
Clear IPv4 Unicast Routes at Core	Stress test for control-plane recovery
Clear IPv4 Multicast Routes at Core	Stress test for control-plane recovery
Core Switch System Failure/Recovery	• IGP and PIM reconvergence (control-plane & data plane) • PIM Rendezvous Point redundancy & Back-up verification

	• VDC failure does not impact other VDCs
Core Switch Power Redundancy	Partial Power loss causes no impact to control/data plane
Core Switch Supervisor High-Availability	• NSF, GR, in-chassis and on peers • NSF interoperability
Core Switch Fabric High-Availability	Fabric module failure causes no impact to control/data plane
Line Card OIR at Core Switch	• Hitless operation for non-affected ports • Traffic load-sharing for distributed port-channels • IGP and PIM reconvergence (control-plane & data plane) • LACP interoperability for distributed port-channels • Unidirectional Link Detection (UDLD)

Aggregation Layer

Disruption	**Verification**
Router Link Failure/Recovery between Aggregation and Core	• IGP and PIM reconvergence (control-plane & data plane)
Member of Port-channel Failure/Recovery between Aggregation and Core	• Traffic load-sharing for port-channels • LACP interoperability • Unidirectional Link Detection (UDLD)
Layer 2 Trunk Link Failure/Recovery between Aggregation and Access	• STP reconvergence • IGMP reprogramming with snooping • MAC address re-learning • Security ACL & FNF reprogramming • No FHRP impact • No ARP/ND impact • vPC functionality
FabricPath Core Link Failure/Recovery	• MAC address re-learning • No FHRP impact • No ARP/ND impact • FabricPath Functionality • vPC+ functionality
Member of Port-channel Failure/Recovery between Aggregation and Access	• Traffic load-sharing for port-channels • LACP interoperability • Unidirectional Link Detection (UDLD)
Clear IGP Neighbors/Process at Aggregation	Stress test for control-plane recovery
Clear IPv4 Unicast Routes at Aggregation	Stress test for control-plane recovery
Clear IPv4 Multicast Routes at Aggregation	Stress test for control-plane recovery
Aggregation Switch System Failure/Recovery	• STP reconvergence

	• IGP and PIM reconvergence (control-plane & data plane) • PIM Rendezvous Point redundancy & Back-up verification • PIM DR/BDR functionality • IGMP Snooping & Querier functionality • VDC failure does not impact other VDCs • Security ACL & FNF reprogramming • FHRP redundancy • MAC address learning • ARP/ND re-learning • vPC/vPC+ functionality • FabricPath functionality
Aggregation Switch Power Redundancy	Partial Power loss causes no impact to control/data plane
Aggregation Switch Supervisor High-Availability	• NSF, GR, in-chassis and on peers • NSF and GR interoperability • No impact to vPC peering status
Aggregation Switch Fabric High-Availability	Fabric module failure causes no impact to control/data plane
Line Card OIR at Aggregation Switch	• Hitless operation for non-affected ports • Traffic load-sharing for distributed port-channels • IGP and PIM reconvergence (control-plane & data plane) • LACP interoperability for distributed port-channels • Unidirectional Link Detection (UDLD)
vPC/vPC+ peer-link/keep-alive Failure/Recovery	vPC functionality and peering status
vPC/vPC+ Leg Failure/Recovery	• No impact to STP overlay • IGMP reprogramming with snooping • MAC address re-learning • Security ACL & FNF reprogramming • No FHRP impact • No ARP/ND impact
vPC/vPC+ Leg member Failure/Recovery	• Traffic load-sharing for port-channels • LACP interoperability • Unidirectional Link Detection (UDLD)

Access/ToR Layer

Disruption	**Verification**
Access/ToR Switch System Failure/Recovery	• STP reconvergence • IGMP snooping reprogramming

	• MAC address re-learning • No impact to other vPC/vPC+ • FabricPath functionality

Access/End-host Layer

Disruption	**Verification**
Member of Port-channel Failure/Recovery between FI and upstream switches	• Verify FI uplink static pinning works as expected • Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities • MAC address learning • LACP interoperability • Verify DHCP functionalities
Port-channel Failure/Recovery between FI and upstream switches	• Verify FI uplink static pinning works as expected • Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities • MAC address learning • LACP interoperability • Verify DHCP functionalities
Port-channel Failure/Recovery between FI and IOM	• Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities • MAC address learning
Cluster Link Failure/Recovery between FIs	• Traffic load-sharing for link members • Traffic load-sharing within the FI cluster • Recovery of system functionalities
Member of Cluster Link Failure/Recovery between FIs	• Traffic load-sharing for link members • Traffic load-sharing within the FI cluster • Recovery of system functionalities
Fabric Interconnect System Failure/Recovery	• Traffic load-sharing within the FI cluster • Recovery of system functionalities • MAC address learning • vPC functionality/FabricPath functionality • LACP interoperability
Blade OIR	• Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities
NIC Bonding	• Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities • MAC address learning

Service Profile Operations	• Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities
Software Upgrade/Downgrade	• Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities
VMware® vMotion™	• Traffic load-sharing for port-channels • Traffic load-sharing within the FI cluster • Recovery of system functionalities • MAC address learning • Verify DHCP functionalities

Sample Test Case

Sample Test Case	
Title	Link failure between aggregation and core layers
Description	Verify network control and data plane recovery after link flap
Test Setup	• Reference topology • Reference network configuration setup test case • Reference test plan for control and data plane setup matrices
Procedure	**1.** Fail one of the links between the aggregation and core layers. **2.** Recover the above link. **3.** Repeat the same test at least 5 iterations to ensure consistent behavior for the devices and network. **4.** Repeat the above procedures for the other links between the aggregation and core layers.
Pass/Fail Criteria	• During the link failure, traffic should drop in proportion to the number of links and paths affected, and the traffic should be able to reconverge within the expected time. • Ensure that the unicast and multicast routing protocols have detected peer failure in order to start network reconvergence within the expected time. • Verify the convergence pattern is as expected. • Verify the CPU usage pattern is as expected. • Verify the memory usage is as expected. • Verify the route tables for both unicast and multicast routing are updated correctly on all switches in the network. Ensure that only affected switches show change in the forwarding tables. • Verify the hardware forwarding entries, line card programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast routing are updated correctly on all switches in the network. • Verify Layer 2 forwarding tables on aggregation and access switches. They should not be affected by this failure.

4.4 Automation

A test script suite is used to perform failure executions and to perform data collection. Automated testing ensures the reliability and repeatability of test runs. The test scripts can be broken down into several key components: initialization, failure execution and data collection.

4.4.1 Initialization

Initialization prepares the device under test for failure execution. The script connects to the device and retrieves running image version, neighbor information (via CDP), port-channel information and inventory (i.e. linecards, supervisor types). Where applicable, the script also checks for redundancy state and ensures switch is HA ready.

4.4.2 Failure Execution

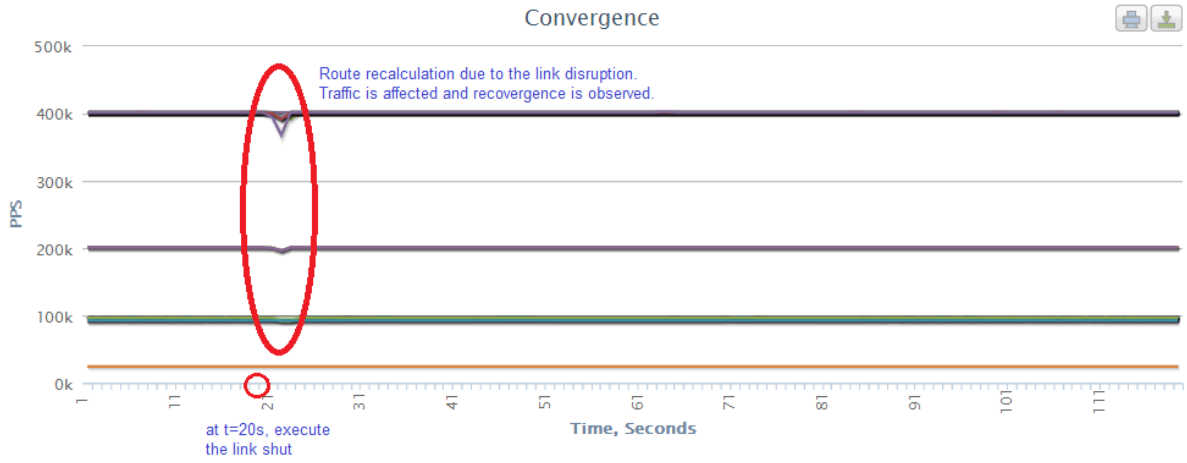
A deterministic approach to test execution is accomplished by predefining the test duration, configuring the point in time for failure execution and providing the capability to repeat test cases using a configuration file. If tests are executed with the same set of configuration files, the sequence of failures, the timing of the failure execution and the duration of test monitor will not be changed, and this notion provides the repeatability factor. If an issue was found with a script, the success of the reproducibility of the bug will be drastically increased and can be reproduced by re-running the script with the same configuration conditions. The following is a list of failure triggers supported by automation today:

- Switchover
- ISSU/D
- VDC reload
- Link Shut
- Link No Shut
- Module Insertion
- Module Removal
- Xbar Removal
- Xbar Insertion
- Clear OSPF process
- Clear BGP process
- Clear Ip Routes
- Clear Ip Mroutes
- Clear PIM neighbors
- Reload

4.4.3 Data Collection

The data collection tool will connect to the Ixia IxNetwork application via IxTclNetwork API's to collect traffic statistics related data. In particular, flow statistics which include per flow statistics information of frames delta, transmit rate and receive rate are collected for every test run. Once collected, the results are analyzed in either a graphical format, or for sub-second packet losses, in a raw data format, to calculate the packet loss duration.

Figure 14 Sample link disruption convergence graph



In addition, specific modules are being developed to address well known problem areas for the use in regression testing. For example, there have been issues in the past with startup and running configuration mismatching or configuration lost after supervisor switchover or during the ISSU process. To check for such issues, a configuration checkpoint has been developed to verify startup and running configuration before and after a switchover failure.

5. NVT Findings/Conclusion/Recommendations

5.1 Caveats for NVT 2.1-2.3

CSCuc51372
Symptom: ISIS routing adjacencies flap on SSO
Conditions: This symptom may be seen when SSO is performed on a switch with ISIS adjacencies.
Workaround: Decrease adjacencies or Increase hold time.
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 6.2(2)
Applicable Releases: 6.1(3) 5.2(9) 6.1(4)

CSCud84214
Symptom: SSO causes "%DIAG_PORT_LB-2-PROC_INIT_FAILURE". Data traffic drop may be observed. UDLD may cause ports to go to error-disabled state.
Conditions: This symptom is seen on performing an SSO.
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 6.1(3)
Applicable Releases: None

CSCud88581
Symptom: Remote peer's ports are in UDLD err-disabled after SSO
Conditions: This symptom is seen on performing an SSO.
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 6.1(3)
Applicable Releases: None

CSCud98846
Symptom: Initial egress PIM join may be dropped after Port-channel member add.
Conditions: This symptom maybe be observed if the member of a port-channel flaps.
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(3) 5.2(9) 6.1(4)

CSCty72738
Symptom: No incompatibility message shown for more than 4 ospf instances in 6.1 while performing ISSD
Conditions: This symptom is seen if a downgrade is to be performed from a release that supports more than 4 instances of OSPF to one that does not. The output of "show incompatibility-all system" does not warn about this incompatibility.

Workaround: None
Severity: Enhancement
Platform Seen: Nexus 7000
Resolved Releases: 6.1(3) 6.2(2)
Applicable Releases: None

CSCue46961
Symptom: Tunnel interface descriptions tails in the config
Conditions: When the description on a tunnel is configured, it shows up as the last line on the config.
interface Tunnel2003
 no ip redirects
 ip address 40.3.13.13/24
 ip pim sparse-mode
 tunnel source loopback0
 tunnel destination 40.2.0.15
 description GRE tunnel to DC2-3
Workaround: None
Severity: Cosmetic
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(3)

CSCue49116
Symptom: No syslog notification on the main vdc when a vdc with 'feature tunnel' is converted to an F2 only vdc
Conditions: When a vdc with 'feature tunnel' configuration is changed to an F2 only vdc a syslog message is shown in that particular vdc. This message is not shown on the main vdc.
%TUNNEL-2-TM_F2_ONLY_VDC: Tunnel feature is not supported in F2 only VDC
Workaround: None
Severity: Moderate
Platform Seen: Nexus 7000
Resolved Releases: 6.2(2)
Applicable Releases: 6.1(3) 6.1(4)

CSCue51163
Symptom: Service ""snmpd"" crash is seen when invoking "show running-config" command while performing MIB walk
%SYSMGR-2-SERVICE_CRASHED: Service ""snmpd"" (PID 4280) hasn't caught signal
Conditions: This symptom is seen when the "show running-config" command is invoked parallel with MIB walk.
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 6.1(4)
Applicable Releases: 6.1(3)

CSCue55841
Symptom: RSA key changes after reloading a switch with a different image release
Conditions: This symptom is seen while performing a non-ISSU image change on a system.
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(3) 5.2(9) 6.1(4)

CSCue56741
Symptom: vPC member ports are error disabled on the neighbor switch due to “LACP multiple neigbors detected” after SSO on Nexus 7000 vPC system.
Conditions: This symptom is seen after an SSO on the Nexus 7000 vPC switch.
Workaround: None. Flap the affected ports on the neighbor switch to recover.
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(3) 6.1(4)

CSCue29303
Symptom: Switchport trunk commands prevent FabricPath from working
Conditions: Fabric Path will not work if "switchport trunk allowed vlan" command is present in interface configs.
Workaround: Do not use “switchport trunk allowed vlan” command on fabricpath core ports
Severity: Moderate
Platform Seen: Nexus 7000
Resolved Releases: 6.1(4) 5.2(9) 6.2(2)
Applicable Releases: 6.1(3)

CSCuf52081
Symptom: ISSU fails with error "SRG collection error" due to M132XP failure
Conditions: This symptom may be seen when an ISSU is performed with M132XP line card present in the chassis
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 5.2(9)

CSCuf86556
Symptom: Suspending VDC causes crash in l2fm process
Conditions: This symptom is seen while suspending a VDC
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 6.1(4) 6.2(2)

Applicable Releases: None

CSCug04958
Symptom: MAC address is not programmed on the forwarding engine after ISSU causing traffic blackhole.
Conditions: This symptom is seen after an ISSU is performed.
Workaround: None
Severity: Moderate
Platform Seen: Nexus 7000
Resolved Releases: 6.1(3) 6.1(4) 6.2(2)
Applicable Releases: 5.2(9)

CSCug05324
Symptom: FEX times out during ISSU and FEX uplinks are in "SDP timeout/SFP Mismatch" state.
Conditions: This symptom may be seen while performing an ISSU with Fabric Extenders present in the chassis
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 5.2(9) 6.2(2)
Applicable Releases: None

CSCug40990
Symptom: Unsuspending VDC causes crash with "%SYSMGR-2-SERVICE_CRASHED: Service "spm" (PID 16976) hasn't caught signal 11 (core will be saved)."
Conditions: This symptom occurs while unsuspending a VDC.
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 6.1(4) 6.2(2)
Applicable Releases: None

CSCug41055
Symptom: Unsuspending VDC causes crash with "%SYSMGR-2-SERVICE_CRASHED: Service "msdp" (PID 26636) hasn't caught signal 11 (core will be saved)."
Conditions: This symptom occurs while unsuspending a VDC.
Workaround: None
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: 6.2(2)
Applicable Releases: 6.1(4)

CSCug41477
Symptom: Memory leak on FEX reload in fex process at libutils and libveobc
Conditions: This symptom occurs after reloading a Fabric Extender
Workaround: None
Severity: Moderate

Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(4)

CSCug66005
Symptom: Output of "show spanning-tree" on Secondary vPC Peer shows interface as Forwarding even though it is shut.
Conditions: This symptom is seen on the secondary vpc peer after shutting a vPC leg and invoking the "show spanning-tree" command
Workaround: None
Severity: Minor
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(4)

CSCug66377
Symptom: When vPC tracking object is down the following message is seen: "VPC-2-TRACK_INTFS_DOWN: In domain 112, vPC tracked interfaces down, suspending all vPCs and keep-alive"
Conditions: This symptom is seen when the vPC object goes down
Workaround: The keep-alive is only suspended for 20sec; this behavior needs to be reflected in the syslog message.
Severity: Moderate
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(4)

CSCug67069
Symptom: M1 module bringup causes duplicate multicast packets
Conditions: This symptom is seen when an M1 module with routed uplinks, vPC peer-link and vPC keepalive link is brought up.
Workaround: None.
Severity: Severe
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(4)

CSCug93314
Symptom: vPC is not suspended even with Type-1 inconsistency.
Conditions: This is seen when port channel mode is active on one vPC peer and passive on the other.
Workaround: None.
Severity: Moderate
Platform Seen: Nexus 7000
Resolved Releases: None
Applicable Releases: 6.1(4)

CSCuh07028

Symptom: vPC object tracking suspends vPC member ports twice when the object goes down and comes back up.
Conditions: This symptom is seen when a vPC object consisting of the uplinks and the vPC peer-link goes down and comes back up. The vPC member ports are correctly suspended when the object goes down. But, when the uplinks are brought up the object comes back up and the vPC member ports are erroneously suspended again.
Workaround: None.
Severity: Moderate
Platform Seen: Nexus 7000
Resolved Releases: 6.2(2)
Applicable Releases: 6.1(4)

CSCuh10527
Symptom: "Copy complete" message is not seen after copying a saved config to the running-config on a Nexus 3000
Conditions: This symptom is seen after a saved config is copied onto the running-config
Workaround: None
Severity: Cosmetic
Platform Seen: Nexus 3000
Resolved Releases: None
Applicable Releases: 5.0(3)U5(1)

CSCuh62160
Symptom: Fabricpath configuration could be lost after reload (non-ISSU downgrade) from 6.0.2N2.0.141 to 5.2.1N1.4 on the Nexus 5000
Conditions: This symptom is seen after a non-ISSU downgrade is performed from 6.0.2N2.0.141 to 5.2.1N1.4 on the Nexus 5000.
Workaround: "The following steps should be performed for the downgrade:
1) Change Boot up variables
2) Copy run start; this saves the boot variable changes.
3) Copy run bootflash:Config.cfg; so ASCII replay can be done in step 6.
4) Write erase; this will clear the PSS.
5) Reload the switch.
6) After the switch boots up copy bootflash:Config.cfg run; this will do the ASCII replay.
7) Copy run start; this will save the configuration to startup."
Severity: Severe
Platform Seen: Nexus 5000
Resolved Releases: None
Applicable Releases: 5.2(1)N1(4)

CSCui20256
Symptom: On the ASR 9000 the RPF entries could be Null for some (S,G) multicast routes with no Accept interfaces, this causes data traffic for those (S,G) to be blackholed.
Conditions: This symptom could occur when PIM topology change causes new (S,G) entries to be created on the switch.
Workaround: None
Severity: Moderate

Platform Seen: ASR 9000
Resolved Releases: None
Applicable Releases: 04.02.03.BASE

CSCui25751
Symptom: Due to versioning restrictions, UCSM registration to UCS Central might fail.
Conditions: This symptom can occur when there is a version mismatch between UCS Manager and UCS Central.
Workaround: None. Ensure that the UCSM and UCS Central versions are compatible to establish proper communication.
Severity: Severe
Platform seen: UCS
Resolved releases: None
Applicable releases: UCSM 2.1(1a) and UCS Central 1.1

CSCuh87431
Symptom: IOM can remain stuck while firmware upgrade is in progress with the following message displayed: *[FSM:FAILED]: update backup image of IOM*
Conditions: This symptom can occur while performing an infrastructure firmware upgrade.
Workaround: None. Failed IOM has to be manually OIRed to recover.
Severity: Severe
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh25841
Symptom: During an infrastructure firmware upgrade, the IOM may become unresponsive.
Conditions: This symptom can occur while performing an infrastructure firmware upgrade.
Workaround: None. Failed IOM has to be manually OIRed to recover.
Severity: Severe
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh34052
Symptom: VM-FEX port profile may take a long time (>2 hrs) to disassociate VM.
Conditions: This symptom may occur while disassociating a port profile from a VM.
Workaround: Set the lifecycle policy to a lower setting.
Severity: Severe
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCui46259

Symptom: UCSM User Configuration Guide 2.1 refers to an incorrect step when modifying the Local Disk Configuration Policy.
Conditions: This symptom is an incorrect reference located within the UCSM User Configuration Guide 2.1
Workaround: Refer to the "Storage" tab within the UCSM Working pane.
Severity: Severe
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh49861
Symptom: **`ifdown`** and **`ifup`** of a VM's interface may lead to the MAC and VIF entries becoming out of sync on the NX-OS CLI and UCSM GUI.
Conditions: This symptom may occur when **`ifdown`** and **`ifup`** are executed within a VM.
Workaround: None. Power cycle the Fabric Interconnect to re-establish MAC synchronization between the NX-OS CLI and UCSM GUI.
Severity: Severe
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh47788
Symptom: The deletion of a DVS object from UCSM can fail if the object is also shared with other instances of UCSM.
Conditions: This symptom may occur when a DVS is deleted from UCSM.
Workaround: None. Configuring DVS objects that are not shared between multiple instances of UCSM will avoid this issue.
Severity: Moderate
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh81950
Symptom: After an OIR is performed on a single HDD in a UCS B-series blade server, a Transient Disk Inoperable fault is displayed although the disk is still operational.
Conditions: This symptom may be seen after performing an OIR of a single HDD in a UCS B-series blade server.
Workaround: None.
Severity: Moderate
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh25799
Symptom: Upon completion of infrastructure firmware upgrades, UCSM may display multiple running versions.
Conditions: This symptom may be seen after performing an infrastructure firmware upgrade.

Workaround: None.
Severity: Moderate
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh36965
Symptom: OIR of a UCS B-series blade server will display the warning message in the Fault Summary with the following message displayed: *ERR-IBMC-fru-retrieval-error Message: Could not get Fru from 7f060201*.
Conditions: This symptom may be seen after performing an OIR of a UCS B-series blade server.
Workaround: None. The warning message will clear automatically.
Severity: Minor
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCui13535
Symptom: Lack of clock synchronization between IOMs may lead to an endless loop during the firmware upgrade process with the following message displayed: *Infrastructure Upgrade FSM: Stuck at "Deploy Poll Activate Of Local FI"*
Conditions: This symptom may be seen when performing an infrastructure firmware upgrade while the clocks on the FI are not synchronized.
Workaround: Ensure that NTP is enabled on UCSM in order to synchronize the clocks on the FI.
Severity: Enhancement
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

CSCuh25709
Symptom: Lack of clock synchronization between IOMs might lead to an IOM failure while performing a firmware upgrade.
Conditions: This symptom may be seen when performing an infrastructure firmware upgrade while the clocks on the FI are not synchronized.
Workaround: Ensure that NTP is enabled on UCSM in order to synchronize the clocks on the FI.
Severity: Enhancement
Platform seen: UCS
Resolved releases: None
Applicable releases: 2.1(1a)

References:
Cisco NX-OS Licensing Guide
Nexus 7000 Install and Upgrade Guides
Nexus 7000 Configuration Guides
Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide

Design Considerations for Classical Ethernet Integration of the Cisco Nexus 7000 M1 and F1 Modules
Cisco FabricPath Best Practices
Cisco FabricPath Design Guide: Using FabricPath with an Aggregation and Access Topology
Data Center Access Design with Cisco Nexus 5000 Series Switches and 2000 Series Fabric Extenders and Virtual PortChannels
Cisco UCS Manager Configuration Common Practices and Quick-Start Guide
Cisco VM-FEX Best Practices for VMware ESX Environment Deployment Guide
Virtual Machine Mobility with VMware VMotion and Cisco Data Center Interconnect Technologies
UCS Command References
UCS Install and Upgrade Guides
UCS Configuration and Firmware Management Guides

6. Test Results

				NVT 2.3		NVT 2.2		NVT 2.1	
Heading		**Test Case**	**Pass/Fail Verification**	**Status**	**Bugs**	**Status**	**Bugs**	**Status**	**Bugs**
1. DC1 Setup		**DC1 Setup**							
1.1. Common Configuration		Common Configuration for all switches	Verify SSH works through the management network on a dedicated vrf Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers Verify NTP and Time Zone : ntp.interop.cisco.com Verify Syslog to syslog.interop.cisco.com Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10 Verify DNS search list: interop.cisco.com, cisco.com Verify CDP neighbors Verify SNMP agent (read community): public + interop; (private community): private + cisco Verify UDLD neighbors and UDLD aggressive mode Verify LACP for link aggregation Verify BFD peering for all possible clients with default protocol timers for the clients on all relevant interfaces. Verify SSO/NSF and GR Verify CoPP function Verify SPAN ensuring cross-module SPAN. Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV) Verify DHCP IP helper and primary/backup server	pass		pass		pass	CSCue51163
1.2. Edge/Core to Public Network Setup									
1.2.1. DC1-Core-N7k-1		Setup interfaces from DC1-Core-N7k-1 to Public network [AS1-1,AS1-2]	BGP: Verify Ipv4 eBGP peering between DC1-Core-n7k-1 and AS1-1,AS1-2. Verify eBGP multipath. PIM: Verify PIM peering. Redistribute: Verify routes are redistributed according to configured policies. Acl: Verify ACL policies are properly programmed in hardware and are functioning as expected.	pass		pass		pass	CSCue46961

1.2.2. DC1-Core-N7k-2		Setup interfaces from DC1-Core-N7k-2 to Public network [AS1-1,AS1-2]	BGP: Verify IPv4/IPv6 eBGP peering between DC1-Core-n7k-2 and AS1-1,AS1-2. Verify eBGP multipath. PIM: Verify PIM peering. Redistribute: Verify routes are redistributed according to configured policies. Acl: Verify ACL policies are properly programmed in hardware and are functioning as expected.	pass		pass		pass	CSCue46961
1.2.3. DC1-Core-ASR9k-3		Setup interfaces from DC1-Core-ASR9k-3 to Public network [AS1-1,AS1-2]	BGP: Verify IPv4/IPv6 eBGP peering between DC1-Core-ASR9k-3 and AS1-1,AS1-2. Verify eBGP multipath. PIM: Verify PIM peering. Redistribute: Verify routes are redistributed according to configured policies.	pass		pass		pass	
1.3. Core to Distribution Setup									
1.3.1. DC1-Core-N7k-1		Setup interfaces from DC1-Core-N7k-1 to Distribution blocks	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache	pass		pass		pass	CSCue04898
1.3.2. DC1-Core-N7k-2		Setup interfaces from DC1-Core-N7k-2 to Distribution blocks	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache	pass		pass		pass	CSCue04898
1.3.3. DC1-Core-ASR9k-3		Setup interfaces from DC1-Core-ASR9k-3 to Distribution blocks	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache	pass		pass		pass	
1.4. Distribution to Core Setup									
1.4.1. DC1-Dist-N7k-101		Setup interfaces from Distribution N7k to the core switches	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering.	pass		pass		pass	CSCue04898
1.4.2. DC1-Dist-N7k-102		Setup interfaces from Distribution N7k to the core switches	OSPF: Verify OSPFv2/OSPFv3 peering.	pass		pass		pass	CSCue04898

			PIM: Verify PIM peering.						
1.4.3. Distribution Interop									
1.4.3.1. DC1-Dist-C6kE8-103-VSS		Setup interfaces from Distribution C6kE8 VSS to the core switches	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering.	pass		pass		pass	
1.4.3.2. DC1-Dist-C6kE8-104		Setup interfaces from Distribution C6kE8 to the core switches	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering.	pass		pass		pass	
1.4.3.3. DC1-Dist-C6kE7-105-VSS		Setup interfaces from Distribution C6kE7 VSS to the core switches	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering.	pass		pass		pass	
1.4.3.4. DC1-Dist-C6kE7-106		Setup interfaces from Distribution C6kE7 to the core switches	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering.	pass		pass		pass	
1.4.3.5. DC1-Dist-C4k-107		Setup interfaces from Distribution C4k to the core switches	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering.	pass		pass		pass	
1.5. Distribution to ToR Setup									
1.5.1. DC1-Dist-N7k-101		Setup interfaces from Distribution N7k to the ToR	vPC: Verify vPC peer-gateway, vPC peer-switch, vPC Object tracking, vPC auto recovery. Verify vPC peer status, vPC priority and consistency parameters. Check MAC/ARP/igmp snooping synchronization. OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache IGMP/MLD Snooping: Verify IGMP/MLD Snooping HSRP: Verify HSRP Ipv4/IPv6 peering between s5 and s6. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. STP: Verify RSTP parameters and port status. ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines.	pass	CSCug93314	pass		pass	

			ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.						
1.5.1.1. ToR FEX vPC		Setup interface from DC1-Dist-N7k-101 to ToR FEX vPC	Verify FEX association with configured port-channels and that the FEX devices are up.	pass	CSCug41477	pass		pass	
1.5.1.2. ToR Layer 2 Switch		Setup interface from DC1-Dist-N7k-101 to ToR Layer 2 Switch	Verify spanning tree status on all vlans.	pass		pass		pass	
1.5.1.3. ToR N5k vPC		Setup interface from DC1-Dist-N7k-101 to ToR N5k vPC	Verify vPC status and consistency parameters. Verify spanning tree status on all vlans.	pass		pass		pass	
1.5.1.4. ToR UCS Fabric Interconnect vPC		Setup interface from DC1-Dist-N7k-101 to ToR Fabric Interconnect vPC	Verify vPC status and consistency parameters						
1.5.2. DC1-Dist-N7k-102		Setup interfaces from Distribution N7k to the ToR	FabricPath: Verify FabricPath route and mac-table are built as expected. Verify IS-IS database. Verify multi-destination trees for unknown unicast, broadcast and multicast with root configured on the spine switches. Verify fabricpath load-balance works as expected OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache IGMP/MLD Snooping: Verify IGMP/MLD Snooping HSRP: Verify HSRP Ipv4/IPv6 peering between s51 & s52; s53 & s54. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch with G flag. STP: Verify RSTP parameters and port status. ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.	pass		pass		pass	
1.5.2.1. ToR FEX		Setup interface from distribution DC1-Dist-N7k-102 to ToR FEX	Verify FEX association with configured port-channels and that the FEX devices are up.	pass		pass		pass	
1.5.2.2. ToR Layer 2 Switch		Setup interface from DC1-Dist-N7k-102 to ToR L2 Switch	Verify spanning tree status on all vlans.	pass		pass		pass	

1.5.2.3. ToR N5k FabricPath		Setup interface from DC1-Dist-N7k-102 to ToR N5k FabricPath	Verify FabricPath route and mac-table are built as expected. Verify the unknown unicast, broadcast and multicast multi-destination trees are built as expected. Verify fabricpath load-balance works as expected Verify IS-IS database, topology and route distribution.	pass		pass		pass	
1.5.2.4. ToR UCS Fabric Interconnect vPC+		Setup interface from DC1-Dist-N7k-102 to ToR Fabric interconnect vPC+	Verify vPC+ status and consistency parameters.						
1.5.2.5. ToR Layer 2 Switch vPC+		Setup interface from DC1-Dist-N7k-102 to ToR L2 Switch vPC+	Verify vPC+ status and consistency parameters.	pass		pass		pass	
1.5.2.6. ToR N3k Layer 3		Setup interface from DC1-Dist-N7k-102 to ToR N3k Layer 3	Verify OSPF/OSPFv3 peering. Verify PIM peering.	pass		pass		pass	
1.5.3. Distribution Interop									
1.5.3.1. DC1-Dist-C6kE8-103-VSS		Setup interfaces from Distribution DC1-Dist-C6kE8-103-VSS to the ToR	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. VSS: Verify VSS active/standby roles and VSL/MEC status. Verify Fast-redirect optimization IGMP/MLD Snooping: Verify IGMP/MLD Snooping HSRP: Verify HSRP configuration. STP: Verify RSTP parameters and port status. ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.	pass		pass		pass	
1.5.3.1.1. ToR Layer 2 Switch		Setup interface from DC1-Dist-C6kE8-103-VSS to ToR L2 Switch	Verify spanning tree status on all vlans.	pass		pass		pass	
1.5.3.1.2. ToR UCS Fabric Interconnect		Setup interface from DC1-Dist-C6kE8-103-VSS to ToR Fabric Interconnect	Verify spanning tree status on all vlans.						
1.5.3.2. DC1-Dist-C6kE8-104		Setup interfaces from Distribution C6k to the ToR	OSPF: Verify OSPFv2/OSPFv3 peering.	pass		pass		pass	

			PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache IGMP/MLD Snooping: Verify IGMP/MLD Snooping HSRP: Verify HSRP peering between s5 and s6. STP: Verify RSTP parameters and port status. ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.						
1.5.3.2.1. ToR Layer 2 Switch		Setup interface from DC1-Dist-C6kE8-104 to ToR L2 Switch	Verify spanning tree status on all vlans.	pass		pass		pass	
1.5.3.2.2. ToR UCS Fabric Interconnect MEC		Setup interface from DC1-Dist-C6k-006-VSS to ToR Fabric Interconnect	Verify spanning tree status on all vlans.						
1.5.3.2.3. ToR N5k MEC		Setup interface from DC1-Dist-C6kE8-104 to ToR N5k MEC	Verify spanning tree status on all vlans.	pass		pass		pass	
1.5.3.2.4. ToR N3k Layer 3		Setup interface from DC1-Dist-C6kE8-104 to ToR N3k Layer 3	Verify OSPF/OSPFv3. Verify PIM peering.	pass		pass		pass	
1.5.3.3. DC1-Dist-C6kE7-105-VSS		Setup interfaces from Distribution C6k to the ToR	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. VSS: Verify VSS active/standby roles and VSL/MEC status. Verify Fast-redirect optimization IGMP/MLD Snooping: Verify IGMP/MLD Snooping HSRP: Verify HSRP configuration. STP: Verify RSTP parameters and port status. ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.	pass		pass		pass	
1.5.3.3.1. ToR Layer 2 Switch		Setup interface from DC1-Dist-C6kE7-105-VSS to ToR L2 Switch	Verify spanning tree status on all vlans.	pass		pass		pass	

1.5.3.3.2. ToR UCS Fabric Interconnect		Setup interface from DC1-Dist-C6kE7-105-VSS to ToR Fabric Interconnect	Verify spanning tree status on all vlans.						
1.5.3.4. DC1-Dist-C6kE7-106		Setup interfaces from Distribution C6k to the ToR	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache IGMP/MLD Snooping: Verify IGMP/MLD Snooping HSRP: Verify HSRP peering between s5 and s6. STP: Verify RSTP parameters and port status. ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.	pass		pass		pass	
1.5.3.4.1. ToR Layer 2 Switch		Setup interface from DC1-Dist-C6kE8-008-VSS to ToR L2 Switch	Verify spanning tree status on all vlans.	pass		pass		pass	
1.5.3.4.2. ToR UCS Fabric Interconnect MEC		Setup interface from DC1-Dist-C6kE7-106 to ToR Fabric Interconnect	Verify spanning tree status on all vlans.						
1.5.3.4.3. ToR N5k MEC		Setup interface from DC1-Dist-C6kE7-106 to ToR N5k MEC	Verify spanning tree status on all vlans.	pass		pass		pass	
1.5.3.5. DC1-Dist-C4k-107		Setup interfaces from Distribution C4k to the ToR	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. MSDP: Verify MSDP peering and SA-cache IGMP/MLD Snooping: Verify IGMP/MLD Snooping HSRP: Verify HSRP peering between s5 and s6. STP: Verify RSTP parameters and port status. ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.	pass		pass		pass	
1.5.3.5.1. ToR UCS Fabric Interconnect		Setup interface from DC1-Dist-C4k-107 to ToR Fabric Interconnect	Verify spanning tree status on all vlans.						

1.6. ToR to Distribution Setup									
1.6.1. ToR Layer 2 Switch vPC									
1.6.1.1. DC1-Dist-N7k-101		Setup vPC interface from ToR Layer 2 Switch to DC1-Dist-N7k-101	STP: Verify RSTP parameters and port status. IGMP/MLD Snooping: Verify IGMP/MLD Snooping	pass		pass		pass	
1.6.2. ToR Layer 2 Switch vPC+									
1.6.2.1. DC1-Dist-N7k-102		Setup interfaces from ToR Layer 2 Switch vPC+ to the DC1-Dist-N7k-102	IGMP/MLD Snooping: Verify IGMP/MLD Snooping STP: Verify RSTP parameters and port status.	pass		pass		pass	
1.6.3. ToR N3k Layer 3									
1.6.3.1. DC1-Dist-N7k-102		Setup interface from ToR N3k Layer 3 to DC1-Dist-N7k-102	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. IGMP/MLD Snooping: Verify IGMP/MLD Snooping ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.	pass	CSCuh10527	pass	CSCuh10527	pass	CSCuh10527
1.6.3.2. DC1-Dist-C6kE8-104		Setup interface from ToR N3k Layer 3 to DC1-Dist-C6kE8-104	OSPF: Verify OSPFv2/OSPFv3 peering. PIM: Verify PIM peering. IGMP/MLD Snooping: Verify IGMP/MLD Snooping ARP & MAC : Verify ARP and MAC addresses are properly learnt across all the forwarding engines. ACL: Verify that all the policies are properly programmed in hardware. DHCP Relay Agent: Verify DHCP relay functionality.	pass	CSCuh10527	pass	CSCuh10527	pass	CSCuh10527
1.6.4. ToR N5k vPC									
1.6.4.1. DC1-Dist-N7k-101		Setup interface from ToR N5k vPC Switch to DC1-Dist-N7k-101	vPC: Verify vPC peer status and consistency parameters. Check MAC/ARP/igmp snooping synchronization.	pass		pass		pass	

			IGMP/MLD Snooping: Verify IGMP/MLD Snooping STP: Verify RSTP parameters and port status. VACL, PACL: Verify that all the policies are properly programmed in hardware.						
1.6.5. ToR N5k FabricPath									
1.6.5.1. DC1-Dist-N7k-102		Setup interfaces from ToR N5k FabricPath to the DC1-Dist-N7k-102	FabricPath: Verify FabricPath route and mac-table are built as expected. Verify IS-IS database. Verify multi-destination trees for unknown unicast, broadcast and multicast. Verify fabricpath load-balance works as expected HSRP: Verify HSRP MAC address is programmed in the mac table IGMP/MLD Snooping: Verify IGMP/MLD Snooping STP: Verify RSTP parameters and port status. VACL, PACL: Verify that all the policies are properly programmed in hardware.	pass		pass		pass	
1.7. ToR to Hosts Setup									
1.7.1. FEX									
1.7.1.1. End Host		Setup interface from FEX to End Host (traffic generator)	Verify spanning tree status (edge) on all vlans for the host ports. Verify mac table is populated correctly. Verify IGMP/MLD snooping.	pass		pass		pass	
1.7.1.2. End Host vPC		Setup interface from FEX to End Host vPC (traffic generator)	Verify spanning tree status (edge) on all vlans for the host ports. Verify mac table is populated correctly. Verify IGMP/MLD snooping.	pass		pass		pass	
1.7.1.3. UCS Fabric Interconnect		Setup interface from FEX to UCS Fabric Interconnect	Verify spanning tree status (edge) on all vlans for the host ports. Verify mac table is populated correctly. Verify IGMP/MLD snooping.						
1.7.1.4. UCS Fabric Interconnect vPC		Setup interface from FEX to UCS Fabric Interconnect vPC	Verify spanning tree status (edge) on all vlans for the host ports. Verify mac table is populated correctly. Verify IGMP/MLD snooping.						

1.7.1.5. UCS Fabric Interconnect vPC+		Setup interface from FEX to UCS Fabric Interconnect vPC+	Verify spanning tree status (edge) on all vlans for the host ports. Verify mac table is populated correctly. Verify IGMP/MLD snooping.						
1.7.2. ToR Layer 2 Switch									
1.7.2.1. End Host		Setup interface from ToR Layer 2 Switch to End Host (traffic generator)	Verify spanning tree status (edge) on all vlans for the host ports. Verify mac table is populated correctly. Verify IGMP/MLD snooping.	pass		pass		pass	
1.7.2.2. UCS Fabric Interconnect		Setup interface from ToR Layer 2 Switch to UCS Fabric Interconnect	Verify spanning tree status (edge) on all vlans for the host ports. Verify mac table is populated correctly. Verify IGMP/MLD snooping.						
1.7.3. ToR N3k Layer 3									
1.7.3.1. End Host		Setup interface from ToR N3k Layer 3 Switch to End Host (traffic generator)	Verify spanning tree status on all vlans. Verify mac table is populated correctly. Verify IGMP/MLD snooping.	pass		pass		pass	
1.7.4. ToR N5k vPC									
1.7.4.1. FEX vPC		Setup interface from ToR N5k FEX to End Host vPC (traffic generator)	Verify spanning tree status on all vlans. Verify mac table is populated correctly. Verify IGMP/MLD snooping.	pass		pass		pass	
1.7.4.1. UCS Fabric Interconnect vPC		Setup interface from ToR N5k vPC to UCS Fabric Interconnect vPC	Verify spanning tree status on all vlans. Verify mac table is populated correctly. Verify IGMP/MLD snooping.						
1.7.5. ToR N5k Fabricpath Leaf									
1.7.5.1. UCS Fabric Interconnect vPC+		Setup interface from ToR N5k FP to UCS Fabric	Verify spanning tree status on all vlans.						

		Interconnect vPC+	Verify mac table is populated correctly. Verify IGMP/MLD snooping.						
1.7.5.4. ToR L2 switch		Setup interface from ToR N5k FP to ToR L2 switch	Verify spanning tree status on all vlans. Verify mac table is populated correctly. Verify IGMP/MLD snooping.	pass		pass		pass	
1.7.5.5. ToR L2 switch vPC+		Setup interface from ToR N5k FP to ToR L2 switch vPC+	Verify spanning tree status on all vlans. Verify mac table is populated correctly. Verify IGMP/MLD snooping.	pass		pass		pass	
1.8. UCS Setup									
1.8.1. Fabric Interconnect									
1.8.1.1. DC1-Dist-N7k-101									
1.8.1.1.1. UCS to N7K FEX	1.8.1.1.1.1	Setup for UCS 6296UP FI to FEX	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards FEX. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and pinning.	pass					
1.8.1.1.2. UCS to N7K VPC	1.8.1.1.2.1	Setup for UCS 6296UP FI to FEX	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards ToR FEX. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.1.1.3. UCS to Layer 2 Switch	1.8.1.1.3.1	Setup for UCS 6296UP FI to Layer 2 Switch	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards layer 2 switch. Verify static pinning on the FI uplinks.	pass					

			Verify IOM to FI connectivity and pinning.						
1.8.1.1.4. UCS to N5k VPC	1.8.1.1.4.1	Setup for UCS 6248UP FI to N5k VPC	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards N5k VPC. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.1.1.5. UCS to N7K FEX VPC	1.8.1.1.5.1	Setup for UCS 6248UP FI to N7K FEX VPC	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards N7k VPC. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.1.1.6. UCS to N5K FEX VPC	1.8.1.1.6.1	Setup for UCS 6296UP FI to N5K FEX VPC	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards N7k VPC. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.1.2. DC1-Dist-N7k-102									
1.8.1.2.2. UCS to Layer 2 Switch	1.8.1.2.2.1	Setup for UCS 6248UP FI to Layer 2 Switch	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards the layer 2 switch. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.1.2.3. UCS to N5K FabricPath VPC+	1.8.1.2.3.1	Setup for UCS 6248UP/6296UP FI to N5k VPC+	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards N5k VPC+. Verify static pinning on the FI uplinks.	pass					

			Verify IOM to FI connectivity and port-channel mode.						
1.8.1.2.4. UCS to N5K FEX FabricPath VPC+	1.8.1.2.4.1	Setup for UCS 6296UP FI to N5k FEX VPC+	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards N5k VPC+. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.1.3. DC1-Dist-C6kE8-103-VSS									
1.8.1.3.1. UCS to C6kE8 VSS	1.8.1.3.1.1	Setup for UCS 6248UP FI to C6kE8 VSS	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards C6k. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.1.6. DC1-Dist-C6kE7-106 Standalone									
1.8.1.6.1. UCS to C6kE7 Standalone	1.8.1.6.1.1	Setup for UCS 6248UP FI to C6kE7 Standalone	Verify the two FI's are in a cluster. Verify FI end host mode configuration. Verify uplink port-channels towards C6k. Verify static pinning on the FI uplinks. Verify IOM to FI connectivity and port-channel mode.	pass					
1.8.2. UCS Setup									
1.8.2.1 UCSM Initial Configuration	1.8.2.1.1	Setup network parameters for the FI cluster.	Verify that the primary FI's System Name, Admin Password, Management IP Address, Management IP Netmask, Default Gateway, DNS Server IP, and Domain Name are all properly configured. Verify that the secondary FI is configured to be in a cluster. Verify that the FI cluster is reachable. Verify successful user authentication.	pass					
1.8.2.2. Hypervisor Installation	1.8.2.2.1	Setup ESXi 5.1 for server virtualization	Verify the ESXi 5.1 software installation on the B2xx Mx blade. Verify server's IP address can be pinged.	pass					

			Verify the configured VM's are up and running. Verify the distributed virtual switch is functional. Verify successful installation of operating systems. Verify traffic can be generated by the servers.						
1.8.2.3 VM Provisioning	1.8.2.3.1	Configure 5 virtual machines with 10 virtual network adapters [per each ESXi host].	Verify through the VM's CLI that the virtual network interfaces are up and associated to a vNIC on UCSM. Verify through the VM's CLI and vCenter 5.1, that the proper MAC addresses are associated to each of the VM's virtual network interfaces. Verify through the VM's CLI and vCenter 5.1, that the proper IP addresses are associated to each of the VM's virtual network interfaces via DHCP. Verify that the VMs are able to be accessed through SSH/Telnet. Verify that the VMs are reachable through the management interface. Verify that the VMs in the same subnet are reachable with one another.	pass					
1.8.2.4. VM-FEX Installation	1.8.2.4.1 1.8.2.4.2	Setup VM-FEX Create datacenter in UCSM under VM tab	Verify through UCSM and vCenter that VM-FEX port profiles are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters via DHCP. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass pass					

	1.8.2.4.3	Create folder under datacenter in UCSM	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass					
	1.8.2.4.4	Create distributed virtual switch under folder in UCSM.	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass					
1.8.2.4. Nexus 1000V Installation (Pod 106)	1.8.2.4.1	Setup Nexus 1000V	Verify that the Nexus 1000V is installed following the Java Installer procedure. Verify the network configurations for control, packet and management ports are configured with the proper vlans. Verify the configured VEMs and VSMs are up and running.	pass not verified					

			Verify that the VSMs are properly configured in cluster-mode. Verify the n1kv distributed virtual switch is functional. Verify successful installation of operating systems. Verify traffic can be generated by the servers. Verify through UCSM and vCenter that all port profiles are properly mapped to the network adapters in standard performance mode.							
	1.8.2.4.2	Configure uplink port profile on the Nexus 1000V	Verify that vCenter executes the command properly and that it is reflecting the proper operation. Using the NXOS CLI, Verify that the operation is properly updated during the entire process. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify the configured VEMs and VSMs are up and running. Verify that the VSMs are properly configured in cluster-mode. Verify through UCSM and vCenter that all port profiles are properly mapped to the network adapters in standard performance mode. Fault monitoring verification on vCenter and NXOS CLI. Verify the expected behavior is properly executed following the best practice and user guide.	pass						
	1.8.2.4.3	Configure server-side port profiles on the Nexus 1000V	Verify that vCenter executes the command properly and that it is reflecting the proper operation. Using the NXOS CLI, Verify that the operation is properly updated during the entire process. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify the configured VEMs and VSMs are up and running. Verify that the VSMs are properly configured in cluster-mode. Verify through UCSM and vCenter that all port profiles are properly mapped to the network adapters in standard performance mode. Fault monitoring verification on vCenter and NXOS CLI. Verify the expected behavior is properly executed following the best practice and user guide.	pass						
	1.8.2.4.4	Configure ESXi hosts to use the Cisco Nexus 1000V in vCenter 5.1	Verify that vCenter executes the command properly and that it is reflecting the proper operation.	pass						

	1.8.2.4.5	Associate ESXi hosts to use the Cisco Nexus 1000V in vCenter 5.1	Using the NXOS CLI, Verify that the operation is properly updated during the entire process. Verify that the configured VEMs and VSMs are up and running. Verify that the VSMs are properly configured in cluster-mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify through UCSM and vCenter that all port profiles are properly mapped to the network adapters in standard performance mode. Fault monitoring verification on vCenter and NXOS CLI. Verify the expected behavior is properly executed following the best practice and user guide. Verify that vCenter executes the command properly and that it is reflecting the proper operation. Using the NXOS CLI, Verify that the operation is properly updated during the entire process. Verify that the configured VEMs and VSMs are up and running. Verify that the VSMs are properly configured in cluster-mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify through UCSM and vCenter that all port profiles are properly mapped to the network adapters in standard performance mode. Fault monitoring verification on vCenter and NXOS CLI. Verify the expected behavior is properly executed following the best practice and user guide.	pass					
2. Network Disruptions Test Cases		**Network Disruptions Test Cases** Common checks for all network disruptions	Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases. Verify that all unicast/multicast traffic convergence is comparable to previous releases. Verify UCS end host mode on FI and VM-FEX functionality.						
2. Network Disruptions Test Cases		**Network Disruptions Test Cases** Common checks for all network disruptions	Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases. Verify that all unicast/multicast traffic convergence is comparable to previous releases. Verify UCS end host mode on FI and VM-FEX functionality.						

2.1. L2 Link Failure/Recovery	2.1.1	L2 Port-channel Failure/Recovery between Distribution and ToR devices	Verify STP port states after link disruption are in the expected forwarding mode. Verify that the STP root does not change. Verify HSRP peers status does not change. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify the L2 forwarding table should remove entries of the affected link at the access switch and re-learnt correctly on the alternative link. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the aggregation switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding. Verify that the L2 forwarding entries on all switches for nodes connected to the access layer are associated with the corresponding STP forwarding ports. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify IGMP/MLD snooping entries are deleted for the affected link at the access switch and re-learnt correctly on the alternative link after query from the IGMP snooping router. Verify that IGMP/MLD membership is not affected on the routers. Verify ACL TCAM is programmed correctly to share for ACL's and features that allow for sharing and verify ACL's are not sharing when not expected. Verify SPAN is mirroring packets correctly. DHCP relay configured on the aggregation switches should remain unaffected. Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, HSRP services, ARP, proxy arp and IGMP. Verify that IPv6 global HSRP is functional. Verify that packets only traverse the fabric for known unicast/multicast destinations and flood through the fabric for unknown unicast, multicast when IGMP snooping is disabled, and broadcast. All unicast and multicast traffic should re-converge with	pass		pass		pass	

			minimal packet loss. Verify traffic destined for CoPP classes is policed as expected.							
	2.1.2	L2 port-channel member failure/recovery between Distribution and ToR devices	Verify port-channel load balancing and rbh assignment Verify that IGMP/MLD membership is not affected. The maximum traffic loss for member failure multicast will be proportionate to number of members failed Multicast DR should not change. Verify that there is no protocol flapping.	pass		pass		pass		
	2.1.3	vPC leg failure/recovery between Distribution and ToR devices	The maximum traffic disruption for unicast will be half for both upstream and downstream traffic. The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC leg is shut. Multicast forwarder should not change. Verify that there is no protocol flapping. The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC leg member is shut (assuming there are 2 members on each vPC leg). Multicast forwarder should not change. Verify that there is no protocol flapping. Verify port-channel load balancing and rbh assignment. Verify that IGMP/MLD membership is not affected.	pass	CSCug66005	pass	CSCug66005	pass	CSCug66005	
	2.1.5	vPC peer-link failure/recovery between Distribution vPC peer switches	Verify that the operational secondary vPC peer will bring down the vPC member ports. Verify that secondary peer will suspend the vpc vlan svi's. Verify that on recovery, the original states will be re-established.	pass		pass		pass		
	2.1.6	vPC Peer-keepalive failure/recovery between Distribution vPC peer switches	There is no expected effects, both vPC peers continue to synchronize MAC address tables, IGMP entries, no traffic disruptions.	pass		pass		pass		

			Verify that on recovery, the original states will be re-established.							
	2.1.7	vPC peer-link and keep-alive failure between Distribution vPC peer switches	If the keep-alive fails first followed by vPC peer link, then both vPC peers will become active. Verify dual-active scenario is encountered and with the peer-switch feature enabled, ensure the downstream device does not detect any spanning-tree misconfigurations.	pass		pass		pass		
			If the vPC peer-link fails first followed by the keep-alive link, the secondary should keep it's vPC member ports suspended.							
	2.1.8	vPC peer-link and keep-alive recovery from Dual-active between Distribution vPC peer switches	If keep-alive is recovered first, the active/secondary switch is determined by the role priority and the secondary switch will suspend vPC member ports and vpc svi's.	pass		pass		pass		
			If vpc peer link is recovered first followed by keep alive, the active/secondary switch is determined by the role priority and the system resumes.							
	2.2.2	L3 Port-channel Failure/Recovery between Core and Distribution Layers[Interop between N7K, ASR9k, C6K, C4k]	Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.	pass	CSCuh07028 CSCug66377	pass	CSCug66377	pass	CSCug66377	
			Verify the L2 forwarding table should remove entries of the affected link. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly. Verify OTV traffic reconverges and optimize OSPF as needed. Verify SNMP traps are sent to SNMP collector. All unicast and multicast traffic should re-converge with proportionate packet loss. Verify traffic destined for CoPP classes is policed as expected. Verify OSPF interface status for the affected links. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency.. Verify OSPF multi-path load-balancing. Verify HW and SW entries are properly programmed and synchronized. Verify PIM neighbor status.							

			Verify PIM both multipath and non-multipath functionalities. Verify AutoRP mapping. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized. On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings. Verify PIM source register and register stop. Verify BFD peer detection and client notifications.							
	2.2.3	L3 Port-channel Failure/Recovery between Distribution to ToR N3k Layer 3 [Interop between N7K & N3K; C6K &N3k]	Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify the L2 forwarding table should remove entries of the affected link. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly. All unicast and multicast traffic should re-converge with proportionate packet loss. Verify traffic destined for CoPP classes is policed as expected. Verify OSPF interface status for the affected links. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency.. Verify OSPF multi-path load-balancing. Verify HW and SW entries are properly programmed and synchronized. Verify PIM neighbor status. Verify PIM both multipath and non-multipath functionalities. Verify AutoRP mapping. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency.	pass		pass		pass		

	2.2.4	L3 port-channel member failure/recovery	Verify multicast HW and SW entries are properly programmed and synchronized. On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings. Verify PIM source register and register stop. Verify BFD peer detection and client notifications. Verify port-channel load balancing and rbh assignment Verify traffic switches to high Bandwidth port-channels for both unicast and multicast when member failure and traffic will switch back when member recovers. Verify LACP rebundle for port-channel after member recover. The traffic should be able to re-converge within acceptable time. Verify the convergence pattern is as expected. Verify the route tables for both unicast and multicast are updated correctly. Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.	fail	CSCud98846	fail	CSCud98846	fail	CSCud98846
2.3. Clear OSPF Neighbors/Process/Routes	2.3	Clear OSPF Neighbors/Process/Routes	All unicast and multicast traffic should re-converge. Verify OSPF IPv4/IPv6 neighbors will restart and come back correctly. Verify that the hardware entries are properly removed and re-installed during the neighbor/process flapping. Verify that CDP/LLDP does not lose peer information. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly. Verify traffic destined for CoPP classes is policed as expected. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency. Verify OSPF multi-path load-balancing. Verify HW and SW entries are properly programmed and synchronized.	pass		pass		pass	

			Verify multicast HW and SW entries are properly programmed and synchronized. Verify BFD peer detection and client notifications. Verify the route tables for both unicast and multicast are updated correctly. Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
2.4. Clear IPv4/IPv6 Multicast Routes	2.4	Clear IPv4/IPv6 Multicast Routes	All multicast traffic should re-converge. Verify periodic PIM joins are received and sent upstream after clearing. Verify that the multicast hardware entries are properly removed and re-installed during the mroute flaps Verify that CDP/LLDP does not lose peer information. Verify that no flooding happens after traffic convergence. Verify PIM neighbor status. Verify PIM both multipath and non-multipath functionalities. Verify AutoRP mapping. On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings. Verify PIM source register and register stop. Verify IGMP/MLD snooping entries are deleted and re-learnt correctly after query from the IGMP snooping router. Verify SPAN is mirroring packets correctly. Verify traffic destined for CoPP classes is policed as expected. Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.	pass		pass		pass	
2.5. Reload and Power Cycle Switch	2.5.1	Reload and Power Cycle Edge/Core Switch	Verify BGP neighbors status and authentication. Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings. Verify BGP multi-path load-balancing. Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes. Verify the conditional injection of the default route from BGP into the IGP. Verify BGP recursive lookup scenario.	fail	CSCuh25560 CSCug34987 CSCue55841	pass	CSCug34987 CSCue55841	pass	CSCug34987 CSCue55841

	2.5.2	Reload and Power Cycle Distribution Switch	Verify BGP reconvergence (control-plane & data-plane). Verify OSPF interface status for the affected links. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency.. Verify OSPF multi-path load-balancing. Verify HW and SW entries are properly programmed and synchronized. Verify PIM neighbor status. Verify PIM both multipath and non-multipath functionalities. Verify AutoRP mapping and boundaries. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized. Verify STP port states during and after reload. Verify HSRP peers status during and after reload. Verify CDP/LLDP status during reload on the peers and after reload on the peers and DUT. Verify the L2 forwarding table should remove entries of the affected link at the neighbor switch. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the aggregation switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding after reload. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify IGMP/MLD snooping entries are deleted for the affected links at the access switches and re-learnt correctly on the	pass	CSCug44378 CSCug34987 CSCue55841	pass	CSCug34987 CSCue55841	pass	CSCug34987 CSCue55841

			alternative links after query from the IGMP snooping router. Verify ACL/QoS TCAM is programmed correctly to share for ACL's and features that allow for sharing and verify ACL's are not sharing when not expected. Verify SPAN is mirroring packets correctly. All unicast and multicast traffic should re-converge. Verify traffic destined for CoPP classes is policed as expected. Verify OSPF interface status for the affected links. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency.. Verify OSPF multi-path load-balancing. Verify HW and SW entries are properly programmed and synchronized. Verify PIM neighbor status. Verify PIM both multipath and non-multipath functionalities. Verify AutoRP mapping and boundaries. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized. On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings. Verify PIM source register and register stop. Verify GRE Tunnel re-route due to transport disruption. Verify MTU fragmentation and reassembling at tunnel edge. Verify BFD peer detection and client notifications. The maximum traffic disruption for unicast will be half for both upstream and downstream traffic. The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC peer switch reload. Verify vPC peer status (role, peer link, keepalive link and consistency parameters)						

	2.5.3	vPC peer switch VDC reload	The maximum traffic disruption for unicast will be half for both upstream and downstream traffic. The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC peer switch reload. Verify vPC peer status (role, peer link, keepalive link and consistency parameters)	fail	CSCug41055 CSCug40990 CSCuf86556	pass		pass	
2.6. Supervisor and Fabric HA	2.6.1	Supervisor HA on the edge/core layer	Compare startup/running configuration on Active Sup and Standby Sup before and after SSO. Verify BGP neighbors status and authentication. Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings. Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes. Verify the conditional injection of the default route from BGP into the IGP. Verify BGP recursive lookup scenario. Verify BGP reconvergence (control-plane & data-plane). Verify OSPF interface status. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency.. Verify HW and SW entries are properly programmed and synchronized after SSO. Verify PIM neighbor status. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized after SSO. Verify BFD peer should not flap during and after SSO. No traffic loss is expected.	pass	CSCug95795 CSCuc51372	pass	CSCug95795 CSCuc51372	pass	CSCug95795 CSCuc51372
	2.6.2	Supervisor HA on the Distribution layer	Compare startup/running configuration on Active Sup and Standby Sup before and after SSO. Verify STP port states during and after SSO.	pass	CSCug95795	pass	CSCug95795 CSCud88581	pass	CSCug95795 CSCue56741 CSCud88581 CSCud84214 CSCue56741

			Verify HSRP peers status during and after SSO. Verify CDP/LLDP status after SSO. Verify ARP tables remain unaffected Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the aggregation switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding after SSO. Verify IGMP snooping entries remain unaffected. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly during and after SSO. Verify traffic destined for CoPP classes is policed as expected. Verify OSPF interface status. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency.. Verify HW and SW entries are properly programmed and synchronized after SSO. Verify PIM neighbor status. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized after SSO. Verify BFD peer should not flap during and after SSO. Verify vPC peer status (role, peer link, keepalive link and consistency parameters) before and after SSO No traffic loss is expected.							
	2.6.3	Fabric Failover on the Edge/Core and	Verify there is no impact to data plane and control plane on Fabric failover with no oversubscription	pass		pass		pass		

		Distribution Layers							
2.7. Line Card OIR and Reset	2.7.1	L3 port-channel member failure/recovery, on OIR/reset line card	Verify hitless operation for non-affected ports Verify traffic load-balancing for distributed port-channels before and after OIR/reset Verify BGP/ IGP/ PIM reconvergence (control-plane & data plane) Verfiy BFD peer detection and client notifications Verify LACP interoperability for distributed port-channels Verify that CDP/LLDP does not lose peer information for non-affected line card. Verify that CDP/LLDP peer is removed for disrupted line cards. Verify the L2 forwarding table should be re-learnt correctly after OIR/reset. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly. All unicast and multicast traffic should re-converge with minimal packet loss. Verify traffic destined for CoPP classes is policed as expected.	pass		pass		pass	
	2.7.2	L2 port-channel member failure/recovery, on OIR/reset line card	Verify port-channel load balancing and rbh assignment Verify LACP interoperability for distributed port-channels Verify STP port states after OIR/reset are in the expected forwarding mode. Verify HSRP peers status after OIR/reset. Verify HSRP MAC in ARP table. Verify IGMP/MLD snooping entries are deleted for the links of affected line card and re-learnt correctly on the alternative link after query from the IGMP snooping router. Verify that IGMP/MLD membership is not affected. Verify the L2 forwarding table should be re-learnt correctly after OIR/reset. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.	pass		pass		pass	

			Verify SPAN is mirroring packets correctly. The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic. Multicast DR should not change. Verify that there is no protocol flapping.							
	2.7.3	vPC leg failure/recovery, on OIR/reset line card	The maximum traffic disruption for unicast will be half for both upstream and downstream traffic. The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC leg is shut. Multicast forwarder should not change. Verify that there is no protocol flapping.	pass		pass		pass		
	2.7.4	vPC leg member failure/recovery on OIR/reset line card	The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic. The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC leg member is shut (assuming there are 2 members on each vPC leg). Multicast forwarder should not change. Verify that there is no protocol flapping. Verify port-channel load balancing and rbh assignment. Verify that IGMP/MLD membership is not affected.	pass		pass		pass		
	2.7.5	vPC peer-link failure/recovery on OIR/reset line card	Verify that the operational secondary vPC peer will bring down the vPC member ports. Verify that secondary peer will suspend the vpc vlan svi's. Verify that on recovery, the original states will be re-established.	pass		pass		pass		
	2.7.6	vPC Peer-keepalive failure/recovery on OIR/reset line card	There are no expected effects, both vPC peers continue to synchronize MAC address tables, IGMP entries, no traffic disruptions. Verify that on recovery, the original states will be re-established.	pass		pass		pass		
	2.7.7	vPC peer-link and peer-keepalive failure on OIR/reset line card	If the keep-alive fails first followed by vPC peer link, then both vPC peers will become active. Verify dual-active scenario is encountered and with the peer-switch feature enabled, ensure the downstream device does not detect any spanning-tree misconfigurations.	pass		pass		pass		

	2.7.8	vPC peer-link and peer-keepalive recovery on OIR/reset line card	If the vPC peer-link fails first followed by the keep-alive link, the secondary should keep it's vPC member ports suspended. If keep-alive is recovered first, the active/secondary switch is determined by the role priority and the secondary switch will suspend vPC member ports and vpc svi's. If vpc peer link is recovered first followed by keep alive, the active/secondary switch is determined by the role priority and the system resumes.	pass w/e	CSCug66334 CSCug67069	pass w/e	CSCug66334 CSCug67069	pass w/e	CSCug66334 CSCug67069
2.8. ISSU/ISSD	2.8.1	ISSU/ISSD	Verify if ISSU image compatibility for non-disruptive upgrade/downgrade Verify ISSU/ISSD happens as expected. OSPF graceful restart, PIM triggered Joins should work as expected. Compare startup/running configuration on Active Sup and Standby Sup before and after ISSU/ISSD. Verify STP port states during and after ISSU/ISSD. Verify HSRP peers status during and after ISSU/ISSD. Verify CDP/LLDP status after ISSU/ISSD. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the distribution switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding after ISSU/ISSD. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly during and after ISSU/ISSD. Verify traffic destined for CoPP classes is policed as expected. Verify BGP neighbors status and authentication. Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings. Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes. Verify the conditional injection of the default route from BGP into the IGP. Verify BGP recursive lookup scenario.	pass		fail	CSCug05324 CSCug04958 CSCuf52081	pass	

			Verify BGP reconvergence for control-plane. Verify OSPF interface status. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency. Verify HW and SW entries are properly programmed and synchronized after ISSU/ISSD. Verify PIM neighbor status. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized after ISSU/ISSD. Verify BFD peer should not flap during and after ISSU/ISSD. No traffic loss is expected. If ISSU is disruptive, verify that all unicast/multicast traffic reconverges. DHCP relay configured on the spine switches should remain unaffected after each change. Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, HSRP services, ARP, proxy ARP and IGMP after each change. All unicast and multicast traffic should re-converge with expected packet loss. Verify that all unicast/multicast traffic convergence.						
2.10.FabricPath – Network disruptions									
2.10.1. FabricPath – Link Failure/Recovery	2.10.1.1	FabricPath - Core Link Failure/Recovery	Verify FabricPath route and mac-table are built as expected. Verify IS-IS database, topology and route distribution. Verify multi-destination trees for unknown unicast, broadcast and multicast. Verify fabricpath load-balance works as expected. Verify HSRP peers status does not change. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.	pass		pass			

			Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the aggregation switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify IGMP/MLD snooping entries are deleted for the affected link and re-learnt correctly on the alternative link after query from the IGMP snooping router. Verify that IGMP/MLD membership is not affected on the routers. Verify SPAN is mirroring packets correctly. DHCP relay configured on the aggregation switches should remain unaffected. Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, HSRP services, ARP, proxy arp and IGMP. Verify that IPv6 global HSRP is functional. Verify that packets only traverse the fabric for known unicast/multicast destinations and flood through the fabric for unknown unicast, multicast when IGMP snooping is disabled, and broadcast. All unicast and multicast traffic should re-converge with minimal packet loss. Verify traffic destined for CoPP classes is policed as expected.							
	2.10.1.2	Fabricpath - Core Link member failure/recovery	Verify port-channel load balancing and RBH assignment. Verify IS-IS database, topology and route distribution for metric change. Verify that IGMP/MLD membership is not affected. Verify that IGMP snooping entries change based on multi-destination tree topology change. The maximum traffic disruption for unicast/multicast should be in sub-second range for both upstream and downstream traffic. Multicast DR should not change. Verify that there is no protocol flapping.	pass		pass				
	2.10.1.3	Fabricpath - vPC+ leg failure/recovery	The maximum traffic disruption for unicast will be half for both upstream and downstream traffic or no loss.	pass		pass				

			The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC+ leg is shut. Multicast forwarder should not change. Verify that there is no protocol flapping. The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC+ leg member is shut (assuming there are 2 members on each vPC+ leg). Multicast forwarder should not change. Verify that there is no protocol flapping. Verify port-channel load balancing and rbh assignment. Verify that IGMP/MLD membership is not affected.						
	2.10.1.5	Fabricpath - vPC+ peer-link failure/recovery (spine/leaf)	Verify that the operational secondary vPC+ peer will bring down the vPC+ member ports. Verify that secondary peer will not suspend the vPC+ vlan SVI's if "*dual-active exclude vlans*" is configured Verify on recovery that the operational secondary vPC+ peer will bring up the vPC+ member ports after the configured "*delay restore*" timer	pass		pass			
	2.10.1.6	Fabricpath - vPC+ Peer-keepalive failure/recovery	There are no expected effects; both vPC+ peers continue to synchronize MAC address tables, IGMP entries, no traffic disruptions.	pass		pass			
	2.10.1.7	Fabricpath - vPC+ peer-link and Peer-keepalive failure/recovery	When the keep-alive fails first followed by vPC+ peer link, the peers should continue to see each other through fabricpath network. The effect should be same as just peer-link failure. The recovery should be same as the peer-link recovery.	pass		pass			
2.10.2. FabricPath – Reload	2.10.2.1	FabricPath - Spine Node failure/recovery	Verify Fabricpath multi-destination trees reconverge after root change on node failure. Verify FabricPath route and mac-table are built as expected. Verify IS-IS database, topology and route distribution. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the distribution switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding.	pass		pass			

	2.10.2.2	FabricPath - Leaf Node failure/recovery	Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines on the other spine routers Verify IGMP/MLD snooping entries are deleted for the affected link at the access switch and re-learnt correctly on the alternative link after query from the IGMP snooping router. Verify that IGMP/MLD membership is not affected on the other spine routers. Verify SPAN is mirroring packets correctly. DHCP relay configured on the aggregation switches should remain unaffected. Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, HSRP services, ARP, proxy arp and IGMP. All unicast and multicast traffic should re-converge with minimal packet loss. Verify traffic destined for CoPP classes is policed as expected. Verify that the MAC table, FP ISIS route table, ARP table, IP routing table, IGMP membership table, IGMP snooping table, Multicast routing table return to original state on recovery Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines on recovery Verify Fabricpath multi-destination trees reconverge after leaf node failure. Verify FabricPath route and mac-table are built as expected. Verify IS-IS database, topology and route distribution. Verify HSRP peers status does not change when CE or leaf switches are reloaded. Verify IGMP/MLD snooping entries are deleted for the affected link at the access switch and re-learnt correctly on the alternative link after query from the IGMP snooping router. Verify that IGMP/MLD membership is not affected on the spine routers. Verify that the MAC table, FP ISIS route table, IGMP snooping table return to original state on recovery Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines on recovery	pass w/e		pass w/e			
2.10.3. FabricPath – Supervisor and Fabric HA	2.10.3.1	FabricPath – Supervisor HA on the spine nodes	Verify FabricPath route and mac-table are built as expected. Verify IS-IS database, topology and route distribution. Verify multi-destination trees for unknown unicast, broadcast and multicast. Verify fabricpath load-balance works as expected.	pass		pass			

			Compare startup/running configuration on Active Sup and Standby Sup before and after SSO. Verify STP port states during and after SSO. Verify HSRP peers status during and after SSO. Verify CDP/LLDP status after SSO. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the aggregation switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding after SSO. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly during and after SSO. Verify SNMP traps are sent to SNMP collector. Verify OSPF interface status. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency.. Verify HW and SW entries are properly programmed and synchronized after SSO. Verify PIM neighbor status. Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized after SSO. Verify BFD peer should not flap during and after SSO. Verify vPC+ peer status (role, peer link, keepalive link and consistency parameters) before and after SSO No traffic loss is expected.							
	2.10.3.2	FabricPath - Fabric	Verify there is no impact to data plane and control plane on	pass		pass				

		Failover on spine nodes	Fabric failover with no oversubscription						
2.10.4. FabricPath – Line card OIR and Reset	2.10.4.1	FabricPath – Line card OIR and Reset on spine nodes	Verify FabricPath route and mac-table are built as expected. Verify IS-IS database, topology and route distribution. Verify multi-destination trees for unknown unicast, broadcast and multicast. Verify fabricpath load-balance works as expected. Verify hitless operation for non-affected ports Verify traffic load-balancing for distributed port-channels before and after OIR/reset Verfiy BFD peer detection and client notifications Verify LACP interoperability for distributed port-channels Verify STP port states after OIR/reset are in the expected forwarding mode. Verify HSRP peers status after OIR/reset. Verify that CDP/LLDP does not lose peer information for non-affected line card. Verify that CDP/LLDP peer is removed for disrupted line cards. Verify the L2 forwarding table should be re-learnt correctly after OIR/reset. Verify HSRP MAC in ARP table. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify IGMP/MLD snooping entries are deleted for the links of affected line card and re-learnt correctly on the alternative link after query from the IGMP snooping router. Verify SPAN is mirroring packets correctly. All unicast and multicast traffic should re-converge with minimal packet loss. Verify traffic destined for CoPP classes is policed as expected.	pass		pass			
	2.10.4.2	FabricPath – FP core port-channel member failure/recovery, on OIR/reset line card	Verify port-channel load balancing and rbh assignment Verify that IGMP/MLD membership is not affected. The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic.	pass		pass			

			Multicast DR should not change. Verify that there is no protocol flapping.						
	2.10.4.3	FabricPath – vPC+ leg failure/recovery on OIR/reset line card	The maximum traffic disruption for unicast will be half for both upstream and downstream traffic. The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC+ leg is shut. Multicast forwarder should not change. Verify that there is no protocol flapping.	pass		pass			
	2.10.4.4	FabricPath – vPC+ leg member failure/recovery on OIR/reset line card	The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic. The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC+ leg member is shut (assuming there are 2 members on each vPC+ leg). Multicast forwarder should not change. Verify that there is no protocol flapping. Verify port-channel load balancing and rbh assignment. Verify that IGMP/MLD membership is not affected.	pass		pass			
	2.10.4.5	FabricPath – vPC+ peer-link failure/recovery on OIR/reset line card	Verify that the operational secondary vPC+ peer will bring down the vPC+ member ports. Verify that secondary peer will not suspend the vPC+ vlan SVI's if "*dual-active exclude vlans*" is configured Verify on recovery that the operational secondary vPC+ peer will bring up the vPC+ member ports after the configured "*delay restore*" timer	pass		pass			
	2.10.4.6	FabricPath – vPC+ Peer-keepalive failure/recovery on OIR/reset line card	There are no expected effects; both vPC+ peers continue to synchronize MAC address tables, IGMP entries, no traffic disruptions.	pass		pass			
	2.10.4.7	Fabricpath - vPC+ peer-link and Peer-keepalive failure/recovery on OIR/reset line card	When the keep-alive fails first followed by vPC+ peer link, the peers should continue to see each other through fabricpath network. The effect should be same as just peer-link failure. The recovery should be same as the peer-link recovery.	pass		pass			
2.10.5. FabricPath – ISSU/ISSD	2.10.5.1	FabricPath – ISSU/ISSD	Verify if ISSU image compatibility for non-disruptive upgrade/downgrade	pass		fail	CSCug04958		

			Verify ISSU/ISSD happens as expected. OSPF graceful restart, PIM triggered Joins should work as expected. Compare startup/running configuration on Active Sup and Standby Sup before and after ISSU/ISSD. Verify FabricPath route and mac-table are built as expected. Verify IS-IS database, topology and route distribution. Verify multi-destination trees for unknown unicast, broadcast and multicast. Verify fabricpath load-balance works as expected. Verify STP port states during and after ISSU/ISSD. Verify HSRP peers status during and after ISSU/ISSD. Verify CDP/LLDP status after ISSU/ISSD. Verify HSRP MAC in ARP table. Verify HSRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch. Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers. On the aggregation switches, verify that the ARP are programmed as adjacencies for L3 next hop forwarding after ISSU/ISSD. Verify that no flooding happens after traffic convergence. Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines. Verify SPAN is mirroring packets correctly during and after ISSU/ISSD. All unicast and multicast traffic should re-converge. Verify traffic destined for CoPP classes is policed as expected. Verify OSPF interface status. Verify OSPF neighbor changes and authentication. Verify OSPF DB/Topology consistency. Verify OSPF routes and forwarding table consistency. Verify HW and SW entries are properly programmed and synchronized after ISSU/ISSD. Verify PIM neighbor status.							

			Verify static RP mapping as the backup of auto RP. Verify MSDP neighbors and SA cache consistency. Verify multicast HW and SW entries are properly programmed and synchronized after ISSU/ISSD. Verify BFD peer should not flap during and after ISSU/ISSD. No traffic loss is expected. If ISSU is disruptive, verify that all unicast/multicast traffic reconverges.						
2.10.7. FabricPath – Configuration Change	2.10.7.1	Perform FP Vlan add and delete	Verify FabricPath route and mac-table are built as expected. Verify that no flooding happens after traffic convergence after each change. Verify the L2/L3 forwarding entries are synchronized among the hardwre forwarding engines after each change. Verify IGMP/MLD snooping entries are properly relearned on the affected FP switches after each change. DHCP relay configured on the spine switches should remain unaffected after each change. Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, HSRP services, ARP, proxy ARP and IGMP after each change. Verify that packets only traverse the fabric for known unicast/multicast destinations and flood through the fabric for unknown unicast, multicast when IGMP snooping is disabled, and broadcast on all the affected FP switches. All unicast and multicast traffic should re-converge with minimal packet loss. Monitor all unicast/multicast traffic convergence.	pass	CSCue62989	pass	CSCue62989		
2.12.UCS – Disruptions									
2.12.1. UCS – Link Failure/Recovery	2.12.1.1	UCS - Link Failure/Recovery Between FI and N7K: VPC	Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify VM does not lose network connectivity. Measure traffic convergence for each disruption	pass					
	2.12.1.2	FI Uplink port-channel member failure/recovery: 101-01 n7k vpc	Verify traffic recovery within the expected time frame.	pass					

			Verify that rehashing is performed according to the port-channel protocol (LACP) deployed. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works with no impact. Verify there is no mac address learning on FI uplink. Verify MAC learning on FI server links is not impacted.							
	2.12.1.3	FI Uplink port-channel failure/recovery: 101-01 n7k vpc	Verify traffic should switch to other FI and re-converge with expected packet loss. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected. Verify GARP is sent by other FI after fabric switchover. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify there is no mac address learning on FI uplink. Verify mac learning on other FI server links.	pass not verified							
	2.12.1.4	FI to IOM port-channel member failure/recovery: 101-01 n7k vpc	Verify traffic recovery within the expected time frame. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works with no impact. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links is not impacted.	pass							
	2.12.1.5	FI to IOM port-channel failure/recovery:	Verify traffic recovery within the expected time frame. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected. Verify GARP is sent by other FI after fabric switchover. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify there is no mac address learning on FI uplink. Verify mac learning on other FI server links.	pass not verified							
	2.12.1.6	FI cluster link member failure/recovery: 101-01 n7k vpc	Verify traffic should have no impact. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works with no impact. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches.	pass							

	2.12.1.7	FI to FI isolation/recovery: 101-01 n7k vpc	Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links is not impacted. Verify traffic should re-converge after FI cluster link recovery. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after FI cluster link recovery. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify there is no mac address learning on FI uplink after FI cluster link recovery. Verify mac learning on other FI server links after FI cluster link recovery.	pass					
2.12.2. UCS – Fabric Interconnect Reload and Power Cycle	2.12.2.1	UCS – Fabric Interconnect Reload and Power Cycle: 101-01 n7k vpc	Verify traffic recovery within the expected time frame. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected. Verify GARP is sent by other FI after fabric switchover. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify that traffic flows accordingly through the uplink switches following the VPC model. Verify there is no mac address learning on other FI uplink. Verify mac learning on other FI server links. Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify VM does not lose network connectivity. Measure traffic convergence for each disruption	pass not verified not verified					
2.12.3. UCS – IOM OIR	2.12.3.1	UCS – IOM OIR	Verify traffic recovery within the expected time frame. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected. Verify GARP is sent by other FI after fabric switchover. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved.	pass not verified					

			Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify there is no mac address learning on other FI uplink. Verify mac learning on other FI server links. Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify VM does not lose network connectivity.	not verified						
2.12.4. UCS – Blade OIR	2.12.4.1	UCS – Blade OIR	Verify FI uplink static pinning works as expected. Verify unicast and multicast traffic should re-converge after blade recovery. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify mac learning on FI server links after blade recovery. Verify when blade is re-inserted that hypervisor and VMs are restored.	pass						
	2.12.4.2	Perform live blade OIR (same slot, same chassis)	Remove live blade and re-insert into the same slot within the same chassis. Verify when blade is re-inserted that hypervisor and vm are properly restored. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected.	pass						

			Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass w/exep	CSCuh36965					
	2.12.4.3	Perform live blade OIR (different slot, same chassis)	Remove live blade and decomission from slot. Then re-insert the blade into a different slot within the same chassis, and associate the service profile to the blade. Verify when blade is re-inserted that hypervisor and vm are properly restored. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass pass w/exep	 CSCuh36965					
	2.12.4.4	Perform maintenance blade oir (different slot, different chassis)	Gracefully shutdown VMs and blade. Dissassociate service profile from blade. Remove the blade and accept notifications. Insert the blade into a different slot in a different chassis, and associate the service profile to the blade. Verify when blade is re-inserted that hypervisor and vm are properly restored.	pass						

			Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery. Fault monitoring verification on both UCSM and vCenter.	pass w/exep	CSCuh36965				
	2.12.4.5	Perform a blade swap (B200 with B22) for a blade upgrade	Verify the expected behavior is properly following the best practice and user guide. Verify when blade is re-inserted that hypervisor and vm are properly restored. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the same HDDs are retained throughout the process. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery. Fault monitoring verification on both UCSM and vCenter.	pass					

			Verify the expected behavior is properly following the best practice and user guide.							
	2.12.4.6	In a B-Series chassis perform a blade upgrade/downgrade (B22/B200)	Verify when blade is re-inserted that hypervisor and vm are properly restored. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the same HDDs are retained throughout the process. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery. Fault monitoring verification on both UCSM and vCenter.	pass						
			Verify the expected behavior is properly following the best practice and user guide.							
	2.12.4.7	In a B-Series chassis perform a complete blade upgrade/downgrade (B22/B200)	Verify when blade is re-inserted that hypervisor and vm are properly restored. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning	pass						

			works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide. Verify that the HDD OIR in a RAID 1 Mirrored system does not impact the VMs.						
2.12.6. UCS – FI image and IOM Firmware Upgrade	2.12.6.1	UCS – FI image and IOM Firmware Upgrade	Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify traffic should re-converge after IOM firmware upgraded. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after IOM firmware upgraded. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after IOM firmware upgraded. Verify that no flooding happens after traffic convergence after IOM firmware upgraded. Verify that IGMP snooping is working as expected after IOM firmware upgraded. Verify VM network connectivity is restored.	fail	CSCui13535 CSCuh87431 CSCuh25841 CSCuh25799 CSCuh25709				
2.12.7. UCS – Blade adapter Firmware upgrade	2.12.7.1	UCS – Blade adapter Firmware upgrade	Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify traffic should re-converge after blade adapter firmware upgraded. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade adapter firmware upgraded. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify there is no mac address learning on FI uplink.	fail	CSCui13535 CSCuh87431 CSCuh25841 CSCuh25799 CSCuh25709				

			Verify mac learning on FI server links after blade adapter firmware upgraded. Verify that no flooding happens after traffic convergence after blade adapter firmware upgraded. Verify that IGMP snooping is working as expected after blade adapter firmware upgraded. Verify VM network connectivity is restored.						
2.12.8. UCS – Blade BIOS upgrade	2.12.8.1	UCS – Blade BIOS upgrade	Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify traffic should re-converge after blade BIOS upgraded. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade BIOS upgraded. Verify proper MAC address learning on both fabric interconnects and Nexus 7000 switches. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade BIOS upgraded. Verify that no flooding happens after traffic convergence after blade BIOS upgraded. Verify that IGMP snooping is working as expected after blade BIOS upgraded. Verify VM network connectivity is restored.	fail	CSCui13535 CSCuh87431 CSCuh25841 CSCuh25799 CSCuh25709				
2.12.9. UCS – VMotion for Blade Maintenance	2.12.9.1	Migrate live VM across different blades, same chassis, same FI pair (VM-FEX)	Verify that the VM's vNICs and port profiles are still associated and configured properly before and after the migration through monitoring the CLI. Verify that the MAC address of the migrated VM is learned on the destined Fabric Interconnect and the corresponding upstream switch throughout the migration. Verify that the VMs within the testbed remain pingable between one another during and after the migration. Verify that the VM's network interfaces remain pingable from our management network before and after the migration. Verify that the VM is still reachable through an SSH, or Telnet session. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode.	pass					

			Verify that no faults are raised on either UCSM or vCenter during the operation. Verify that the VM migration is properly executed while following the best practices and user guide.							
	2.12.9.2	Migrate live VM across different blades, different chassis, same FI pair (VM-FEX)	Verify that the VM's vNICs and port profiles are still associated and configured properly before and after the migration through monitoring the CLI. Verify that the MAC address of the migrated VM is learned on the destined Fabric Interconnect and the corresponding upstream switch throughout the migration. Verify that the VMs within the testbed remain pingable between one another during and after the migration. Verify that the VM's network interfaces remain pingable from our management network before and after the migration. Verify that the VM is still reachable through an SSH, or Telnet session. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that no faults are raised on either UCSM or vCenter during the operation. Verify that the VM migration is properly executed while following the best practices and user guide.	pass						
	2.12.9.3	Migrate live VM across different blades, same chassis, same FI pair (VMWare vDS)	Verify that the VM's vNICs and port profiles are still associated and configured properly before and after the migration through monitoring the CLI. Verify that the MAC address of the migrated VM is learned on the destined Fabric Interconnect and the corresponding upstream switch throughout the migration. Verify that the VMs within the testbed remain pingable between one another during and after the migration. Verify that the VM's network interfaces remain pingable from our management network before and after the migration. Verify that the VM is still reachable through an SSH, or Telnet session. Verify that no faults are raised on either UCSM or vCenter during the operation. Verify that the VM migration is properly executed while following the best practices and user guide.	pass						
	2.12.9.4	Migrate live VM across different blades, different	Verify that the VM's vNICs and port profiles are still associated and configured properly before and after the migration through	pass						

		chassis, same FI pair (VMWare vDS)	monitoring the CLI. Verify that the MAC address of the migrated VM is learned on the destined Fabric Interconnect and the corresponding upstream switch throughout the migration. Verify that the VMs within the testbed remain pingable between one another during and after the migration. Verify that the VM's network interfaces remain pingable from our management network before and after the migration. Verify that the VM is still reachable through an SSH, or Telnet session. Verify that no faults are raised on either UCSM or vCenter during the operation. Verify that the VM migration is properly executed while following the best practices and user guide.						
	2.12.9.5	Migrate live VM across different blades, different chassis, different FI pair (VMWare vDS)	Verify that the VM's vNICs and port profiles are still associated and configured properly before and after the migration through monitoring the CLI. Verify that the MAC address of the migrated VM is learned on the destined Fabric Interconnect and the corresponding upstream switch throughout the migration. Verify that the VMs within the testbed remain pingable between one another during and after the migration. Verify that the VM's network interfaces remain pingable from our management network before and after the migration. Verify that the VM is still reachable through an SSH, or Telnet session. Verify that no faults are raised on either UCSM or vCenter during the operation. Verify that the VM migration is properly executed while following the best practices and user guide.	pass					
2.12.10. UCS – NIC Bonding	2.12.10.1	Configure Active / Standby nic bonding	Modify ifcfg-eth8 configuration file Modify ifcfg-eth9 configuration file Create ifcfg-bond0 configuration file Create Modprobe.conf file for mode1 active/standby nics Verify that the bonding is successful Perform an ifdown on eth8 which is the active nic Verify standby nic eth9 becomes active after failover. Perform an ifup on eth8 and verify it becomes standby Verify ping and ssh sessions are all active	pass					

			Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify there is no mac address learning on FI uplink.							
	2.12.10.2	Configure Adaptive Load Balancing nic bonding	Modify ifcfg-eth8 configuration file Modify ifcfg-eth9 configuration file Create ifcfg-bond0 configuration file Create Modprobe.conf file for mode6 (ALB) nics Verify that the bonding is successful Perform an ifdown on eth8 Verify traffic continues without loss as secondary nic continues to forward traffic. Perform ifup on eth8 and verify traffic continues to load balance between links. Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify there is no mac address learning on FI uplink. Verify ping and ssh sessions are all active	fail	CSCuh49861					
	2.12.10.3	Perform FI Failover from Fi-A to Fi-B	login to FI CLI and enter local-mgmt and preform reload on FI-A verify that the FI recovers and there are no critical error messages verify that the vifs failover to FI-B and traffic resumes verify that the vifs resume on FI-A and traffic resumes Verify ping and ssh sessions are all active Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify there is no mac address learning on FI uplink.	pass						
	2.12.10.4	Perform Network uplink failover	Shut the network uplink portchannel on the FI	pass						

			Verify that enm pinning fails verify that the vifs failover to FI-B and traffic resumes No-Shut the network uplink portchannel on the FI verify that the vifs resume on FI-A and traffic resumes Verify ping and ssh sessions are all active Verify FI uplink static pinning works as expected. Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link. Verify there is no mac address learning on FI uplink.						
2.12.11. UCS – Port Profile Tests	2.12.11.1	Remove a port profile in UCSM	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass					
	2.12.11.2	Toggle port profile's I/O Performance mode	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode.	pass					

			Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter.							
	2.12.11.3	Create a profile client in UCSM	Verify the expected behavior is properly following the best practice and user guide. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI.	pass						
			Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter.							
	2.12.11.4	Associate a port profile to a VM	Verify the expected behavior is properly following the best practice and user guide. Verify vCenter executes the command properly and that UCSM is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI.	pass						
			Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter.							

			Verify the expected behavior is properly following the best practice and user guide.							
	2.12.11.5	Remove associated port profile and profile client in UCSM	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter.	pass						
			Verify the expected behavior is properly following the best practice and user guide.							
	2.12.11.6	Unassociate port profile from a VM	Verify vCenter executes the command properly and that UCSM is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter.	pass						
			Verify the expected behavior is properly following the best practice and user guide.							
	2.12.11.7	Remove unassociated port profile and profile client in UCSM	Verify UCSM executes the command properly and that vCenter is reflecting the operation.	pass /w exep	CSCuh34052					

			Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter.							
	2.12.11.8	Modify port profile and LAN pin group in UCSM	Verify the expected behavior is properly following the best practice and user guide. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter.	pass						
	2.12.11.9	Create duplicate port profile in UCSM	Verify the expected behavior is properly following the best practice and user guide. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved.	pass						

			Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.						
2.12.12. UCS – VM-FEX Tests	2.12.12.1	Create duplicate associated distributed virtual switch (VM-FEX) from the same FI cluster in UCSM	Verify UCSM detects and reflects the proper duplication error. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the data plane interfaces are configured in VMDirectPath mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass					
	2.12.12.2	Associate/Sync distributed virtual switch to ESXi hosts in vCenter	Verify vCenter executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved.	pass					

			Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.							
	2.12.12.3	Remove associated distributed virtual switch in UCSM	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass						
	2.12.12.4	Create duplicate associated distributed virtual switch from a different FI cluster in UCSM	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode.	pass /w exep	CSCuh38886					

	2.12.12.5	Remove duplicate associated distributed virtual switch from different FI-pair in UCSM	Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI and vCenter GUI. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass						
2.12.13. UCS – Server Clustering Tests	2.12.13.1	Convert pod to cluster setting in vCenter 5.1	Verify vSphere GUI executes the command properly and that it is reflecting the proper operation. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that vCenter 5.1 acknowledges the creation of the cluster and its components. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected	pass						

			VMs is preserved throughout the entire process. Fault monitoring verification on vCenter.							
	2.12.13.2	Configure and associate a shared datastore for cluster High Availability in vCenter 5.1	Verify the expected behavior is properly following the best practice and user guide. Verify vSphere GUI executes the command properly and that it is reflecting the proper operation. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that vCenter 5.1 acknowledges the creation of the cluster and its components. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on vCenter.	pass						
	2.12.13.3	Enable VM Monitoring within the High Availability cluster	Verify the expected behavior is properly following the best practice and user guide. Verify vSphere GUI executes the command properly and that it is reflecting the proper operation. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify that vCenter 5.1 acknowledges the creation of the cluster and its components. Verify through UCSM and vCenter that VM-FEX port profiles for all necessary data plane traffic are properly mapped to the network adapters in VMDirectPath (High-Performance) mode. Verify through UCSM and vCenter that VM-FEX port profiles for management plane traffic are properly mapped to the network adapters in standard performance mode.	pass						

			Fault monitoring verification on vCenter. Verify the expected behavior is properly following the best practice and user guide.						
2.12.14. UCS – Service Profile Testing	2.12.14.1	From UCSM GUI perform server shutdown for a scheduled maintenance.	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass					
	2.12.14.2	From UCSM GUI perform boot server to recover after a schedule maintenance	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass /w exep	CSCuh52416				
	2.12.14.3	From UCSM GUI perform a blade reset to simulate a blade failure	Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass					
	2.12.14.4	From UCSM GUI perform a server profile (SP) rename	Verify UCSM executes the command properly and that vCenter is reflecting the operation.	pass					

		for management purposes								
	2.12.14.5	From UCSM GUI perform a server profile (SP) clone for management purposes	Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide. Verify UCSM executes the command properly and that vCenter is reflecting the operation.	pass						
	2.12.14.6	From UCSM GUI perform a server profile (SP) template creation for portability and usability purposes	Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide. Verify UCSM executes the command properly and that vCenter is reflecting the operation.	pass /w exep						

	2.12.14.7	From UCSM GUI perform service profile (SP) dis-association for a blade maintanance	Verify when blade is re-inserted that hypervisor and vm are properly restored. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery. Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.	pass						
	2.12.14.8	From UCSM GUI perform a bind to a template for the reprovisioning of a newly inserted blade	Verify when blade is re-inserted that hypervisor and vm are properly restored. Verify UCSM executes the command properly and that vCenter is reflecting the operation. Verify syncing between UCSM GUI, vCenter GUI and KVM consoles. Using the CLI, verify that the vNICs, MAC, and IP addresses are properly associated on all of the VMs' network adapters. Verify that the reachability of all the affected interfaces is properly restored after each disruption and the network convergence is achieved. Verify that the reachability of all the interfaces of non-affected VMs is preserved throughout the entire process. Verify FI uplink static pinning works as expected. Verify RPF check/ Déjà vu check/ Broadcast traffic pinning works as expected after blade recovery. Verify there is no mac address learning on FI uplink. Verify mac learning on FI server links after blade recovery.	pass						

			Fault monitoring verification on both UCSM and vCenter. Verify the expected behavior is properly following the best practice and user guide.						