

CISCO *Live!*

Let's go

Please read

This presentation template uses the CiscoSans TT ExtraLight font. If the text in these two columns does not match, please take a moment to install the font. Otherwise, your presentation will not display correctly.

Please download the fonts from Brand Exchange [here](#). The font can also be found in the zipped folder. Double-click the font file and click “Install” in the window that appears.

This presentation template uses the CiscoSans TT ExtraLight font. If the text in these two columns does not match, please take a moment to install the font. Otherwise, your presentation will not display correctly.

Please download the fonts from Brand Exchange [here](#). The font can also be found in the zipped folder. Double-click the font file and click “Install” in the window that appears.



The bridge to possible

Data Center Operations Maintenance and Migration Best Practices

Anis Edavalath
Principal Architect , Cisco CX

Anis Edavalath



- 11 years with Cisco Customer Experience (CX)
- Focused in Strategizing and implementing Digital Transformation including Security , Observability and Hybrid Cloud
- Enterprise Campus and Datacenter across different verticals
- Worked 10 years with BU engineering groups in Security , switching, datacenter and Network Management products
- Design and deployment of Next Gen Data center architecture enterprise and cloud customers
- AS team lead for ACI, VxLAN, Tetration, SDA (uniform policy)
- Worked with major telecom vendors and Cloud providers prior to Cisco
- CCIE Datacenter # 48152

Contributor: Arvind Durai - Director , Cisco Cx

Support: Carlos Campos Torres - Director Product management,
Cisco

Course Objective and Goal

- To help Data Center operations and engineering staff understand the change management best practice to maintain a datacenter environment or migrate a legacy environment to next gen Cisco Nexus data center network deployment.

- Attendees should leave the session with a firm understanding of
 - Baseline - Fabric best practices
 - Operational Best Practices
 - Features and Tools used to manage DC fabric
 - Migration - Features and Tools (controllers)
 - Migration Methodology

Agenda

CISCO *Live!*

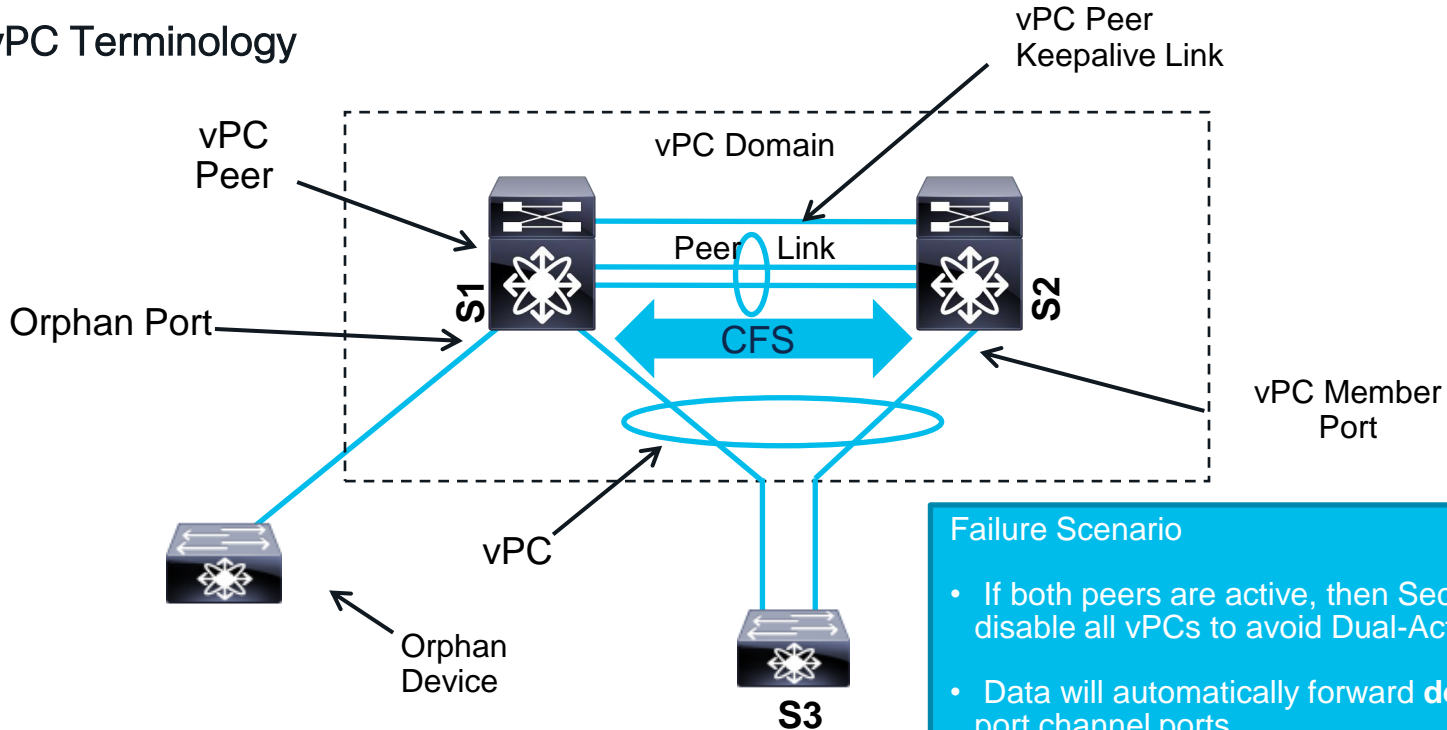
- Baseline
 - VPC, VxLAN & ACI Refresher
 - Change Management best practices
- Features and Tools
 - Graceful insertion and removal
 - Fabric controllers and Nexus
- Migration Methodology
 - Five key Use cases
- Change Window Best Practices

DC Baseline Refresher

vPC Feature Overview



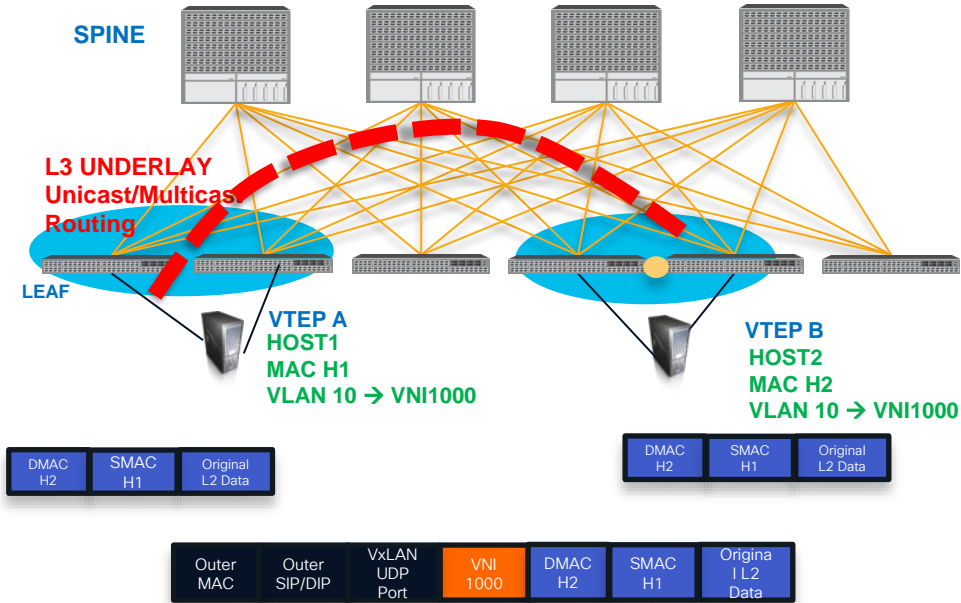
vPC Terminology



Failure Scenario

- If both peers are active, then Secondary vPC peer will disable all vPCs to avoid Dual-Active.
- Data will automatically forward **down** remaining active port channel ports.
- Loss of in-flight packets will depend on deployment of vPC best practice.

VXLAN Overview



VTEP A or VTEP B in deployment will be a pair, and this pair will provide host redundancy for Layer 2 via VPC.

VPC is still NEEDED and VTEP will represent the VPC pair!

Layer 2 overlay on top of your Layer 3 underlay

- Each VXLAN Segment is identified by a unique 24-bit segment ID called a **VXLAN Network Identifier (VNI)**
- Only hosts on the same VNI are allowed to communicate with each other
- Original L2 packet is encapsulated with VXLAN header in a **UDP->IP->Ethernet**

Overcome 4094 VLAN Scale Limitation

- VLANs use a 10-bit VLAN ID

Better utilization of available network paths

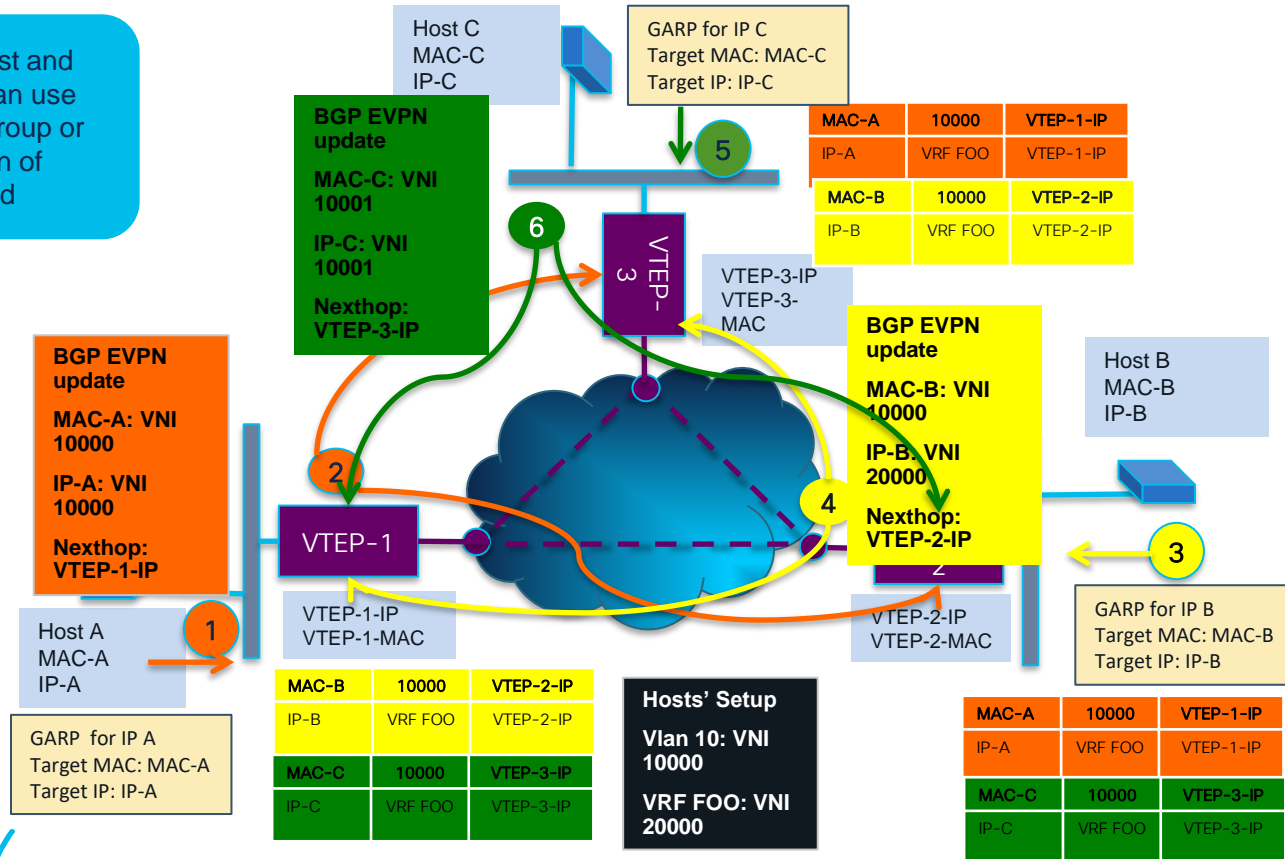
- No need of Spanning Tree (blocks paths)
- Utilize L3 underlay network (ECMP, Link Agg,...)

Multi-Tenant with virtualization

- Isolation of network traffic by a tenant and reusability of networking taxonomy for tenancy

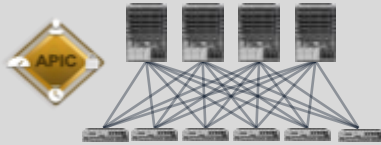
VxLAN Refresher With BGP EVPN Address Learning

Broadcast, Unicast and Multicast traffic can use either Multicast group or Ingress replication of traffic- not covered



SDN 'with' FCAPS 'and' Automation

Application Centric Infrastructure



Turnkey integrated solution with security, centralized management, compliance and scale

Automated application centric-policy model with embedded security

Broad and deep ecosystem

Fault

Configuration

Accounting

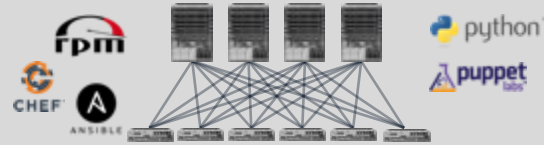
Performance

Security



Integrated
Toolset

Programmable EVPN Fabric



Modern NX-OS with enhanced NX-APIs

DevOps toolset used for Network Management
(Puppet, Chef, Ansible etc.)

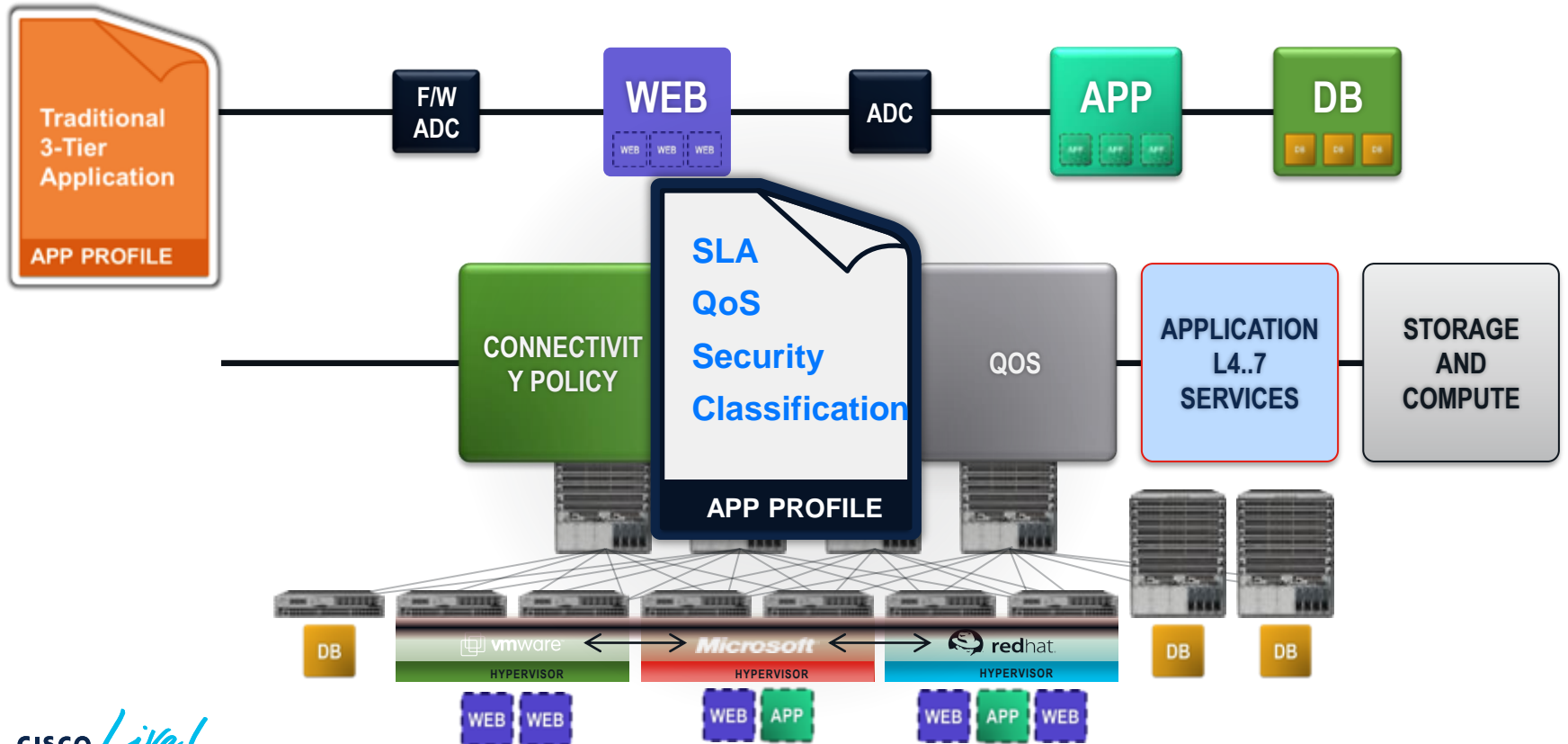
Custom Script based Operations and Workflows



External
Tools

NDFC

Application Network Profiles (ANP) & ACI: how it works?

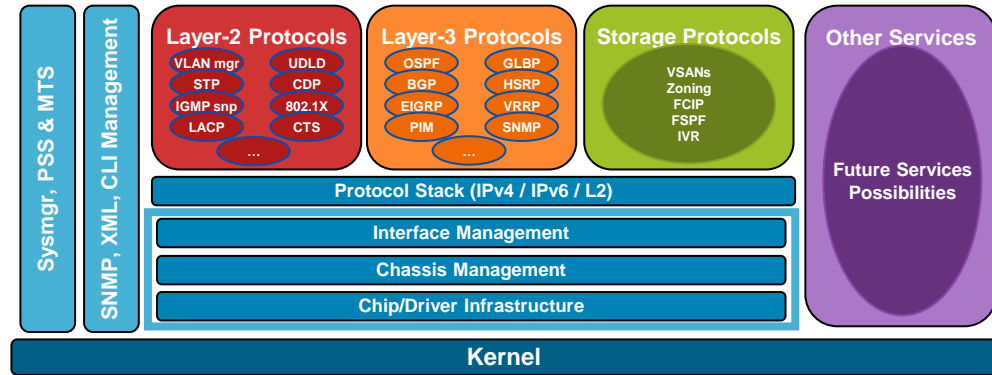


Operational Best Practices

NX-OS High Availability

Process Modularity

- Independent memory-protected restart-able processes
- Service Restart-ability
 - Stateful Restart with Persistent Storage Service (PSS)
 - Checkpoints states to PSS
 - Recover states from PSS upon restart.
 - Stateful Restart with Graceful Restart
 - Recover states based on information from other services and/or network.
 - Mainly Routing Protocols
 - Stateless Restart
 - Fresh start, no trace of former instantiation.

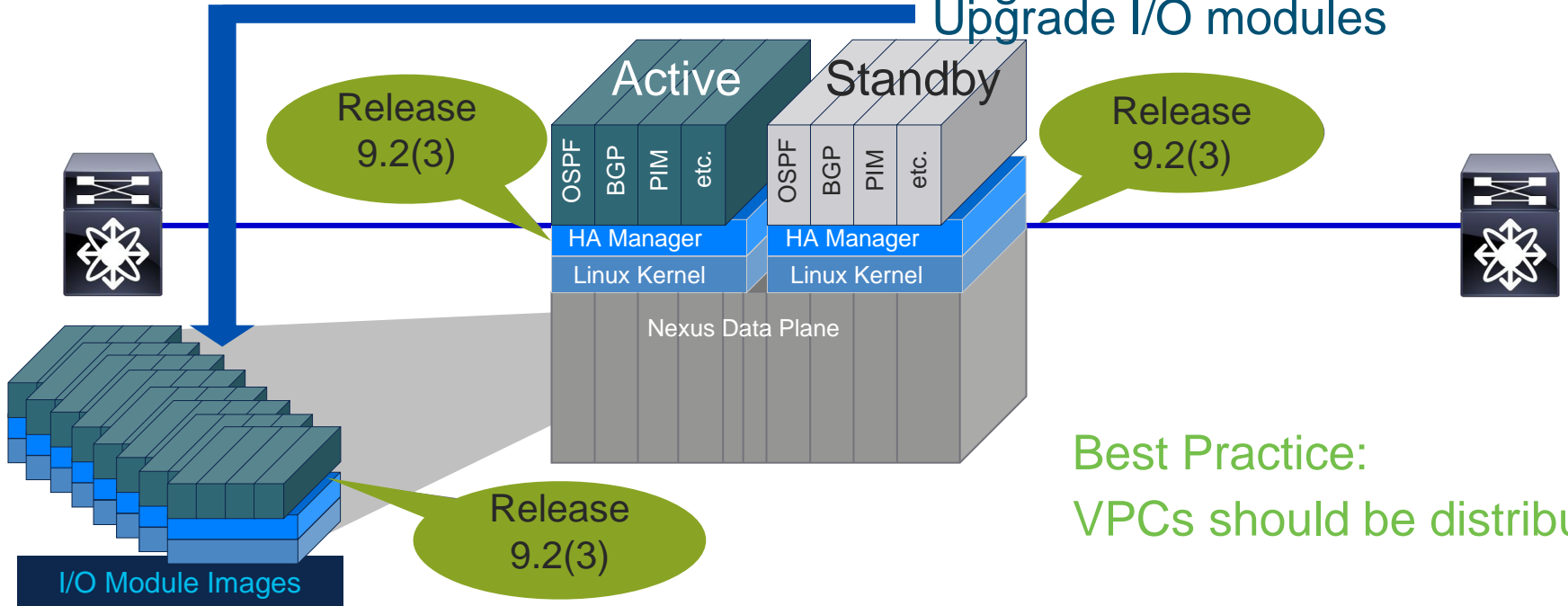


In-Service Software Upgrade

```
Nexus# install all nxos bootflash:nxos.9.2.3.bin
```

Upgrade and reboot
Initiate stateful failover

Upgrade and reboot
Upgrade I/O modules

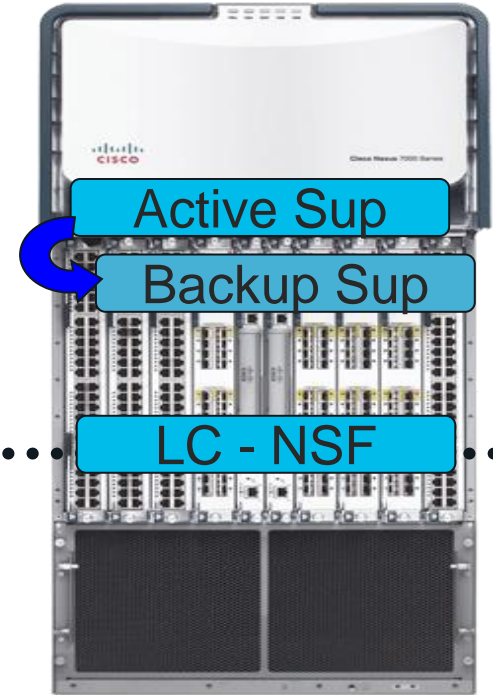


Best Practice:
VPCs should be distributed.

NX-OS High Availability

Supervisor Switchover


- Stateful Switchover (SSO)
 - Active-backup supervisors synchronized at all times
- Routing Protocols: → PSS Stateful Restart
 - NSF Graceful Restart failover
- Other components: → PSS Stateful Restart
- Triggers:
 - HA Policy Initiated – e.g. 3 component crashes → SSO
 - User Initiated – system switchover
 - ISSU initiated SSO



Defect Impact

TAC: You've encountered defect CSCxy12345.
It's operationally impacting and, I'm sorry to say,
there's no workaround. You'll need to **upgrade**.

Belay my last.
We have a SMU
for that.

You: Fine. Let's just get it fixed.
Bill, start up a war room.
 John, get our AS NCE on the phone.
Sally, schedule testers in two hours.
Where's my \$#@! coffee?

What?
Gesundheit.

Sally: You know how Richard gets when we call him at 2 AM...

Software Patching in NX-OS

Who's familiar with Software Maintenance Updates (SMU)?

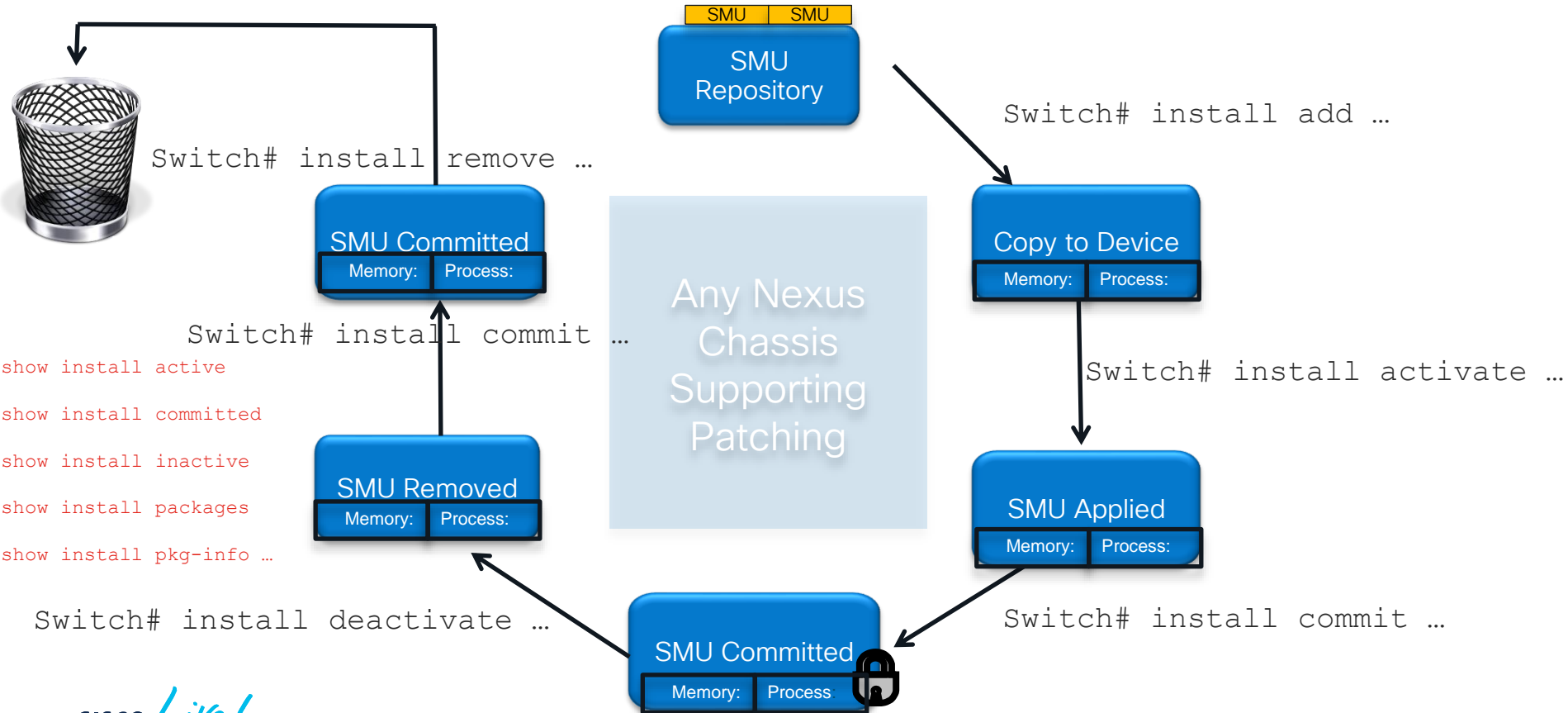
Overview

- Software Patching is Platform Independent
- Available on Nexus 9000 (6.1(2)I2)
- FCS NX-OS 7.2 (5/6/7k)
- Fully supported with ISSU

Benefits

- Reduce time to resolution in your network.
- SMUs in NX-OS build upon years of experience in IOS XR.
- Simplify customer operations for defect resolution and code qualification.
- Better utilize the software HA capabilities of NX-OS.
- Provide a common cross-platform experience (N9K/N7K/N6K/N5K).

SMU Lifecycle - CLI



Patching Highlights



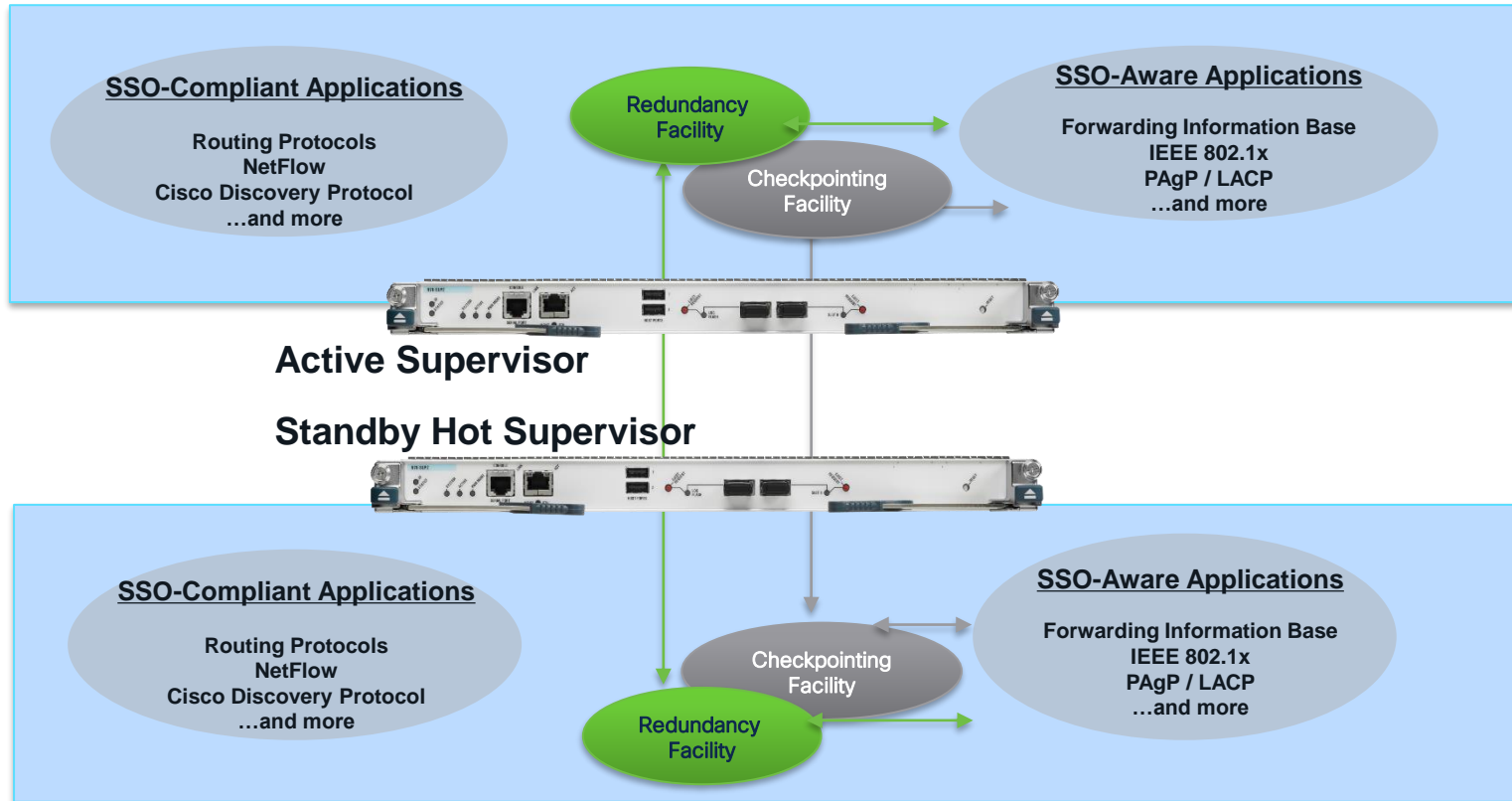
SMU Types

- Restart: Restarts affected process
 - Process restarted in all VDCs where running.
- ISSU SMU:
 - Dual Sup -> ISSU
 - Single Sup -> Reload

- Patching is for operationally impacting bugs without a **workaround**.
 - **Cannot patch to next release.**
- Patching is done in default/admin VDC and applies to all VDCs.
 - **Patching is not available per-VDC.**
- ISSU will work with all, or a subset of patches applied.
 - **You don't need to apply all patches.**
- Some SMUs may only have a single fix, others may have multiple packaged.

Stateful Switchover Mode

SSO-Aware and SSO-Compliant Applications



Routing Protocol Redundancy With NSF (Graceful Restart)

Active Supervisor Engine Slot 1

EIGRP RIB		OSPF RIB		ARP Table	
Prefix	Next Hop	Prefix	Next Hop	IP	MAC
10.0.0.0	10.1.1.1	192.168.0	192.168.0.1	10.1.1.1	aabbcc:ddee32
10.1.0.0	10.1.1.1	192.168.55.0	192.168.55.1	10.1.1.2	adbb32:d34e43
10.20.0.0	10.1.1.1	192.168.32.0	192.168.32.1	10.20.1.1	aa25cc:ddeee8

Standby Supervisor Engine Slot 2

EIGRP RIB		OSPF RIB		ARP Table	
Prefix	Next Hop	Prefix	Next Hop	IP	MAC
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	-

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddeee8

SSO
Redundancy Facility



Checkpoint Facility

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddeee8



Routing Protocol Redundancy With NSF (Graceful Restart)

Supervisor Engine Slot 1

EIGRP RIB		OSPF RIB		ARP Table	
Prefix	Next Hop	Prefix	Next Hop	IP	MAC
10.0.0.0	10.1.1.1			10.1.1.1	aabbcc:ddee32
10.1.0.0	10.1.1.1			10.1.1.2	adbb32:d34e43
10.20.0.0	10.1.1.1			10.20.1.1	aa25cc:ddee8

Standby Supervisor Engine Slot 2

EIGRP RIB		OSPF RIB		ARP Table	
Prefix	Next Hop	Prefix	Next Hop	IP	MAC
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	-

SSO
Redundancy Facility

Checkpoint Facility

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddee8

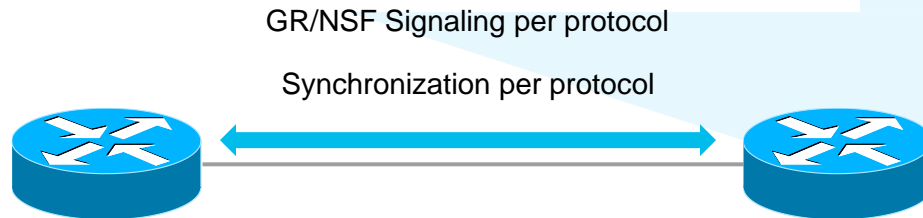


Routing Protocol Redundancy With NSF (Graceful Restart)

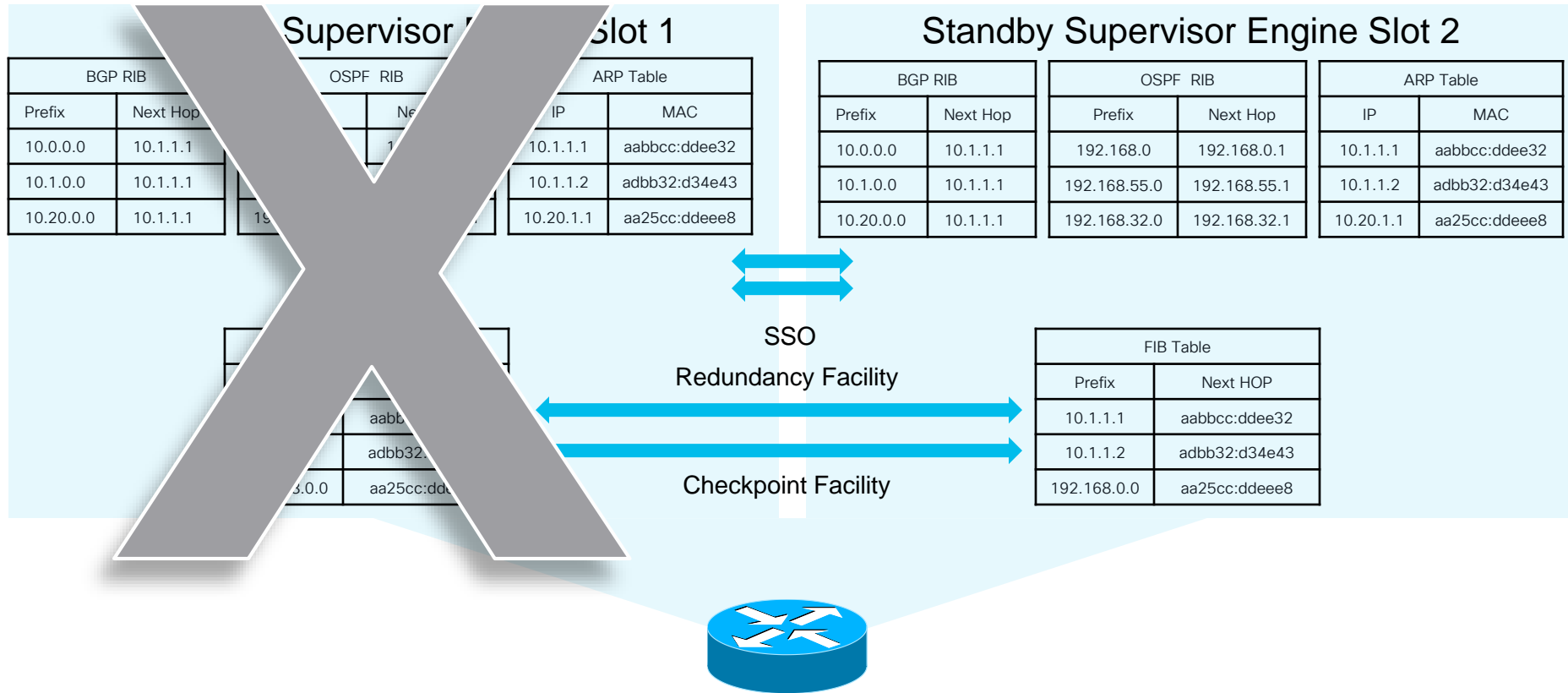
Standby Supervisor Engine Slot 2

EIGRP RIB		OSPF RIB		ARP Table	
Prefix	Next Hop	Prefix	Next Hop	IP	MAC
10.0.0.0	10.1.1.1	192.168.0	192.168.0.1	10.1.1.1	aabbcc:ddee32
10.1.0.0	10.1.1.1	192.168.55.0	192.168.55.1	10.1.1.2	adbb32:d34e43
10.20.0.0	10.1.1.1	192.168.32.0	192.168.32.1	10.20.1.1	aa25cc:ddee8

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddee8



Routing Protocol Redundancy With NSR (Stateful Restart)



Routing Protocol Redundancy With NSR (Stateful Restart)

Standby Supervisor Engine Slot 2

BGP RIB		OSPF RIB		ARP Table	
Prefix	Next Hop	Prefix	Next Hop	IP	MAC
10.0.0.0	10.1.1.1	192.168.0	192.168.0.1	10.1.1.1	aabbcc:ddee32
10.1.0.0	10.1.1.1	192.168.55.0	192.168.55.1	10.1.1.2	adbb32:d34e43
10.20.0.0	10.1.1.1	192.168.32.0	192.168.32.1	10.20.1.1	aa25cc:ddeee8

FIB Table	
Prefix	Next HOP
10.1.1.1	aabbcc:ddee32
10.1.1.2	adbb32:d34e43
192.168.0.0	aa25cc:ddeee8

No additional signaling required to maintain topology



vPC Best Practice

- **vPC Domain ID's**
 - ✓ Use a unique vPC domain ID within a contiguous L2 domain to avoid MAC overlap.
- **vPC Peer Link**
 - ✓ Should be point-to-point connection & dedicated links.
- **vPC Peer Keepalive Link**
 - ✓ Dedicate a control plane in a dual-supervisor environment. Use a management switch.
- **vPC peer-gateway**
 - ✓ Acts as active gateway for frames addressed to peer switch. Avoid Peer Link forwarding.
- Use **vPC peer-switch**
 - ✓ Optimizes BPDU processing, single logical L2 entity
- **Distribute port-channel member interfaces** across line cards within the same chassis.
- Create a **map for oversubscription** aligned to current and future demand.
 - ✓ Deployment practice – 20:1 at access and 2:1 at Core.

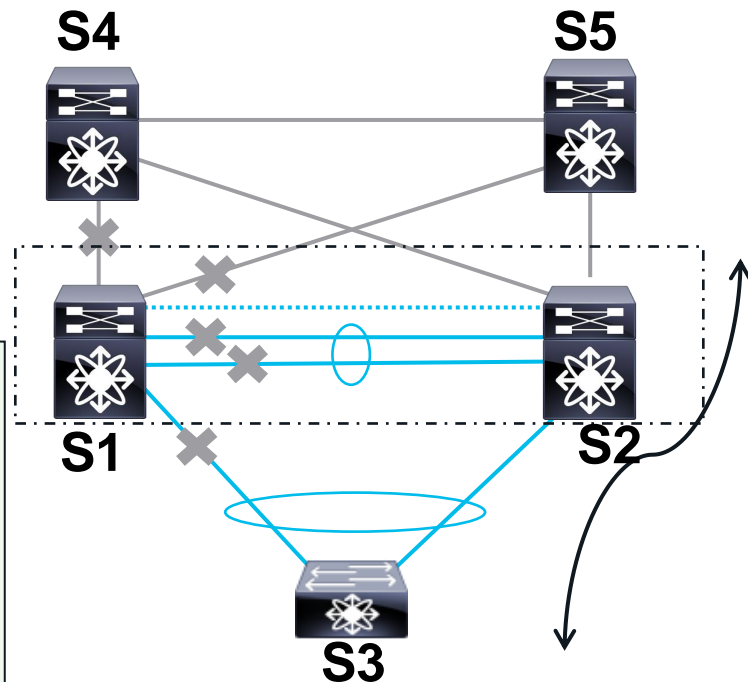
vPC Configuration Best Practices

- vPC object tracking, tracks both peer-link and uplinks in a list of Boolean OR
- Object Tracking triggered when the track object goes down
- Suspends the vPCs on the impaired device.
- Traffic forwarded over the remaining vPC peer.

```
! Track the vpc peer link
track 1 interface port-channel11 line-protocol
! Track the uplinks
track 2 interface Ethernet1/1 line-protocol
track 3 interface Ethernet1/2 line-protocol

! Combine all tracked objects into one.
! "OR" means if ALL objects are down, this object will go down
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 1
track 10
```



Vxlan Considerations and Best Practices

- Use the Nexus Dashboard NDFC App for Vxlan configuration and management
- Vxlan EVPN preferred over Flood and learn
- Design Hierarchical Vxlan fabric to accommodate the scale out
- Ingress replication , Underlay multicast for BUM traffic handling
- Summarize external routes on border leaf or Advertise default routes on a per tenant basis
- Advertise only the LPM prefix routes of internal public layer 3 subnets out of border leaf switches
- Include all local loopbacks in underlay routing to make troubleshooting easy
- Same Vlan Per L2 VNI and consistent naming for vlan VNI pair

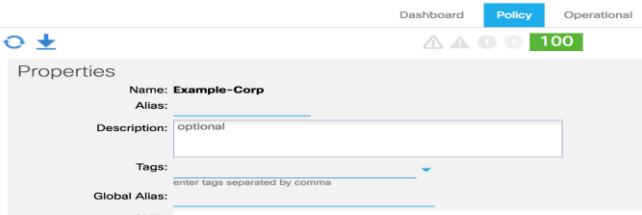
Operational Best Practices

MO Naming Convention

- Develop and plan the MO(Managed Objects) Naming Convention according to Organizations best Practice

Tags and Aliases

- Workaround to Rename Objects
 - Objects can be grouped to make query easier
 - Tags/Aliases have no functional impact- Where as Labels have
- Tenant - Example-Corp

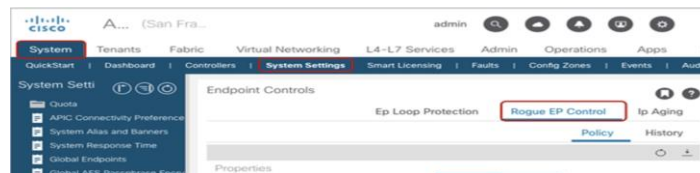


AAA Fallback to Local Auth

- Fallback domain should be set to local to avoid lockout

Loop Mitigation Settings

- Enable MCP (Miscabling Protocol) per vlan
 - To find out and disable loops caused by misbehaving external L2
- Rogue EP Control preferred over Endpoint loop protection



BD Level Configuration

- Do Not enable Unicast routing when gateway is not BD SVI
- Limit IP Learning to Subnet
- L2 Unknown unicast set to Flood
- ARP Flooding enabled

Fabric Wide Configuration

- IP Aging Policy
- Disable Remote EP Learning - On Border Leaf
- Enforce Subnet Check

NX-OS Graceful Insertion and Removal

Nexus Graceful Removal

```
router bgp 33
```

```
  isolate
```

Discontinue advertisement of all prefixes.

```
router eigrp 1
```

```
  isolate
```

Advertises maximum metrics for all K-values.

```
router ospf 1
```

```
  isolate
```

max-metric router-lsa

```
router isis 1
```

```
  isolate
```

set-overload-bit

Nexus feature

Graceful Insertion

- Move the switch from Maintenance mode to Normal mode.
- Control plane maintained throughout isolation of the switch.
- Protocols advertise routes only after it is installed in hardware.

```
N9372(config)# no system
mode maintenance
```

Following configuration
will be applied:

```
router bgp 33
```

```
no isolate
```

```
router eigrp 1
```

```
no isolate
```

```
router ospf 1
```

```
no isolate
```

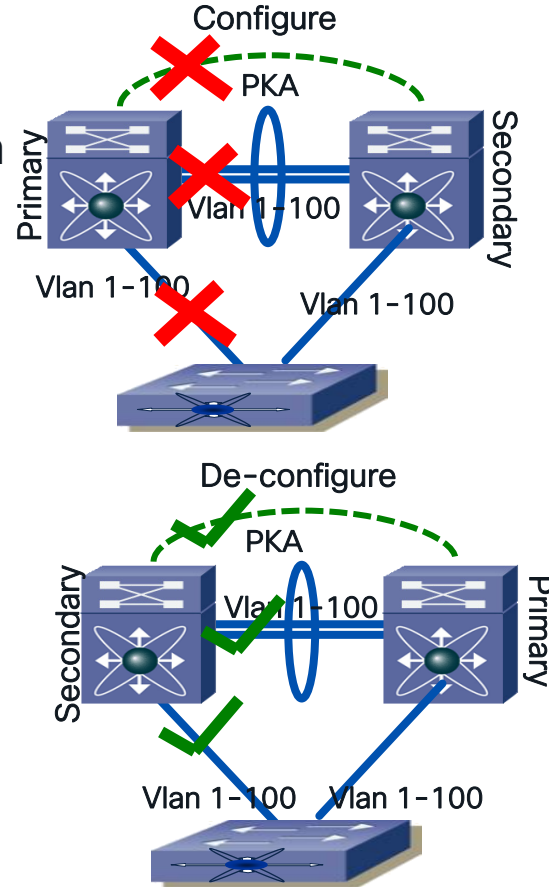
```
router isis 1
```

```
no isolate
```

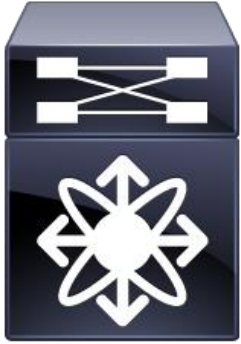
VPC Shutdown Feature

This feature allows customer to manually “isolate” a switch from vPC domain. This is a vPC configuration option.

Pre-VPC Shutdown	VPC Shutdown Behavior
<ul style="list-style-type: none">• No “shutdown” command.• Manual Shutdown Required<ul style="list-style-type: none">• Down vPCs• Down Peer Link• vPC Members• Etc.	<ul style="list-style-type: none">• Local switch isolated from remote.• Cannot exit shutdown without manual intervention.• When exiting, PKA, PL, and vPCs will be re-initialized; vPC domain brought to normal state.



Graceful Insertion and Removal



```
feature ospf
```

```
feature vpc
```

Isolate for
Change Window

OSPF:
max-metric router-lsa

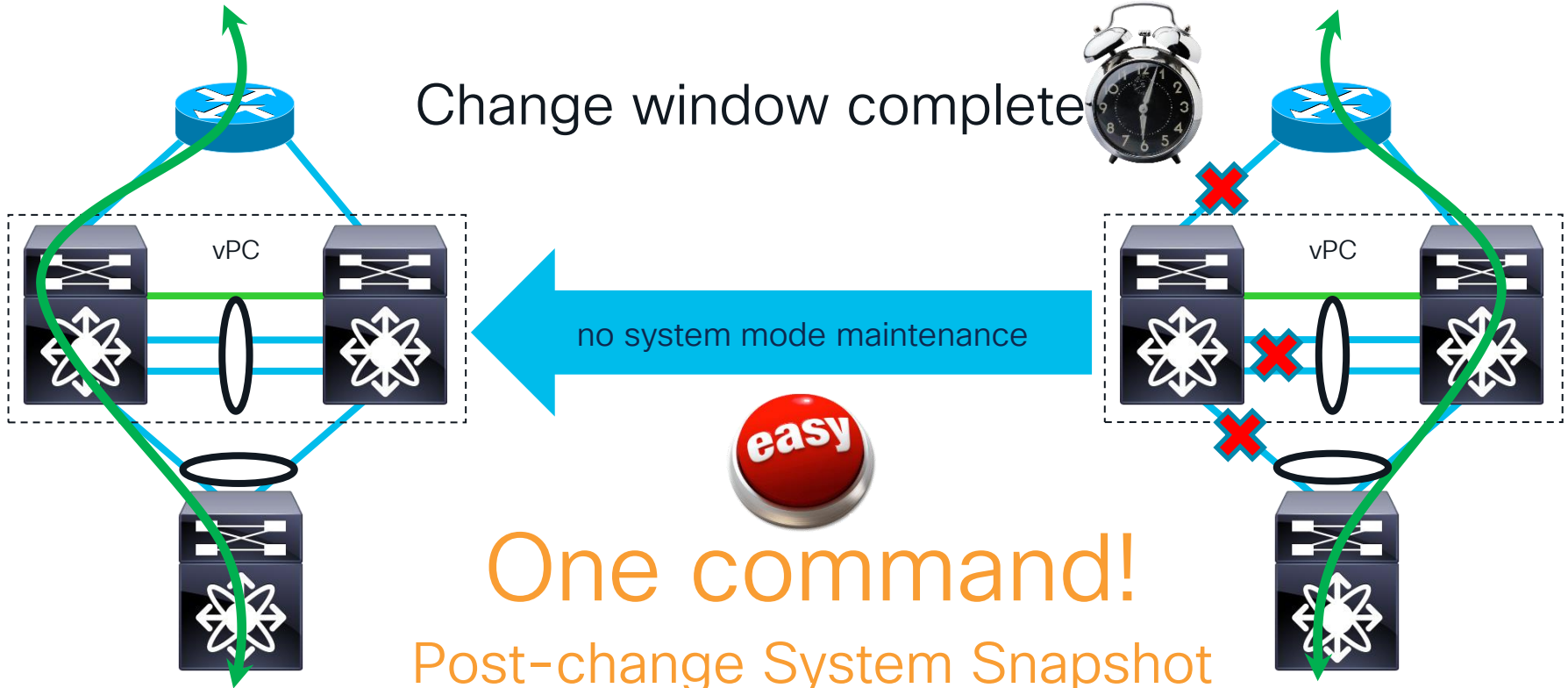
VPC:
shutdown

Scripting takes time.
It'd be nice to
automate this...

Graceful Insertion and Removal



Graceful Insertion and Removal



Configuration Profiles

- Maintenance-mode profile is applied when entering GIR mode,
- Normal-mode profile is applied when GIR mode is exited.

Automatic Profiles	Manual Profiles
<ul style="list-style-type: none">• Generated by default• Parses configuration to determine changes going into and out of GIR• Changes based on base protocol configuration settings. • Use: Maintenance Windows	<ul style="list-style-type: none">• User created profile for maintenance-mode and normal-mode• Flexible selection of protocols for isolation • Use: maintenance windows and isolation during troubleshooting using preconfigured scripts.

Enabling Graceful Insertion and Removal Automatic Profile Generation

```
N7K-1-Core# show system mode
System Mode : Normal
N7K-1-Core# config
Enter configuration commands, one per line.  End with
CNTL/Z.
N7K-1-Core(config)# system mode maintenance

BGP is not enabled, nothing to be done

EIGRP is not enabled, nothing to be done

OSPF is up..... will be shutdown
  OSPF TAG = 100, VRF = default
    config terminal
    router ospf 100
    shutdown
    end

OSPFv3 is not enabled, nothing to be done

ISIS is not enabled, nothing to be done

vPC is not enabled, nothing to be done

Interfaces will be shutdown
Do you want to continue (y/n)? [n] y
```

```
Generating maintenance-mode profile
Progressing.....Done.

System mode operation completed successfully

N7K-1-Core# show system mode
System Mode : Maintenance
N7K-1-Core#
```

Enabling Graceful Insertion and Removal Custom Profile Generation

```
config-profile maintenance-mode type admin
router bgp 65001
  isolate
  sleep instance 1 10
router ospf 100
  isolate
  sleep instance 3 20
vpc domain 20
  shutdown
system interface shutdown exclude fex-fabric
```

```
config-profile normal-mode type admin
router bgp 65001
  no isolate
  sleep instance 1 10
router ospf 100
  no isolate
  sleep instance 3 20
vpc domain 20
  no shutdown
no system interface shutdown
```

- By default, GIR Mode will automatically generate profiles.
- CLI to disable automatic profile generation: dont-generate-profile
- If you enter GIR mode with automatic profile, it will overwrite your custom profile.

Graceful Insertion and Removal Mode for Unplanned Outages

system mode maintenance on-reload reset-reason *reason*

HW_ERROR-Hardware error,

SVC_FAILURE-Critical service failure,

KERN_FAILURE-Kernel panic,

WDOG_TIMEOUT-Watchdog timeout,

FATAL_ERROR-Fatal error,

MANUAL_RELOAD---Manual reload,

MATCH_ANY-Any of the above reasons,

ANY_OTHER-Any reload reason not specified above.

Nexus GIR Snapshots

- Used before and after a GIR mode to compare pre/post change operation.
- Snapshots are automatically generated when entering GIR mode.

```
switch# snapshot create snap1 For testing  
Executing show interface... Done  
Executing show bgp sessions vrf all... Done  
Executing show ip eigrp topology summary... Done  
Executing show vpc... Done  
Executing show ip ospf vrf all... Done  
Feature 'ospfv3' not enabled, skipping...  
Snapshot 'snap1' created  
Switch#
```

Nexus GIR Snapshots Comparison

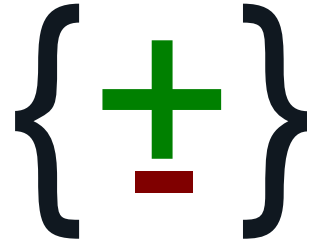
```
Nexus# sh snapshots compare before_maintenance after_maintenance
=====
Feature Tag          before_maintenance      after_maintenance
=====
```

```
[bgp]
```

```
-----
[neighbor-id:100.120.1.221]
connectionsdropped 2          **3**
lastflap             P1DT21H5M12S             **P1DT21H25M47S**
lastread            P1DT21H25M12S             **PT0S**
lastwrite           P1DT21H25M14S             **PT0S**
state                Established                **Idle**
localport            52737                      **0**
remoteport          179                        **0**
notificationssent   2                          **3**
<...>
```

```
switch# show snapshots compare snapshot1 snapshot2 ipv4routes
metric              snapshot1  snapshot2  *  changed
# of routes          33         3          *
# of adjacencies    10         4          *
```

```
Prefix              Changed Attribute
-----
23.0.0.0/8          not in snapshot2
10.10.10.1/32       not in snapshot2
21.1.2.3/8          adjacency index has changed from 29 (snapshot1) to 38
                    (snapshot2)
```



Tools to Manage DC

- Controller (APIC / NDFC)
- Nexus Insights

New Topology

- Dynamic Arrangement
- Multi-Fabric/Overlay
- Arrange by Tier
 - Core, Ag, Access Leaf, Spine etc..
- Metadata Tags
- Show FEX links
- Device Pop-Over
- Side-By Side View

The screenshot displays the Cisco Data Center Network Manager interface. On the left is a navigation sidebar with options: Dashboard, Topology, Inventory, Monitor, Configure, and Administration. The main area shows a network topology with nodes labeled Fab2-N9K-Leaf-1, Fab2-N9K-Leaf-2, and Fab2-N9K-Leaf-3. On the right, two side-by-side pop-over windows are shown for Fab2-N9K-Leaf-4 and Fab2-N9K-Leaf-6. Each window displays a summary of device information and health metrics.

Device	IP Address	Serial Number	WWN	CPU	Memory
Fab2-N9K-Leaf-4	192.168.100.124	SAL1909A89Z	SAL1909A89Z	25%	34%
Fab2-N9K-Leaf-6	192.168.100.126	SAL1833YM5U	SAL1833YM5U	17%	28%

Health Summary for both devices:

- 68% overall health
- 1/8 Modules in warning
- 57/64 Switch ports in warning
- 1/0 Events marked in warning or higher

Tags: sample, sample2

System Tags: feature:BGP

Buttons: Beacon, Show more details

Side-By-Side Views

Capacity Dashboard

View the Capacity of Data Center Fabric -ACI

Capacity Dashboard

Endpoints 1
136 of 18000(<1%)

Bridge Domains
493 of 15000(3%)

L3 Contexts
57 of 3000(1%)

Endpoint Groups
522 of 15000(3%)

L4/L7 Devices
6 of 1200(<1%)

L4/L7 Graphs
10 of 600(1%)

Usage Overview 2

Switch	VRF	BD	EPG	Mac (learned)	IPv4 (learned)	IPv6 (learned)	Multicast	Policy CAM	VLAN
node-101	<1% 4 of 500	3% 128 of 3500	3% 128 of 3500	<1% 45 of 12288	<1% 45 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 36 of 4096	7% 275 of 3500
node-102	<1% 4 of 500	3% 127 of 3500	3% 129 of 3500	<1% 65 of 12288	<1% 46 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 36 of 4096	7% 275 of 3500
node-103	<1% 4 of 500	3% 127 of 3500	3% 127 of 3500	<1% 46 of 12288	<1% 46 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 36 of 4096	7% 273 of 3500
node-104	<1% 4 of 500	3% 127 of 3500	3% 127 of 3500	<1% 44 of 12288	<1% 45 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 36 of 4096	7% 273 of 3500
node-105	<1% 4 of 500	3% 127 of 3500	3% 127 of 3500	<1% 44 of 12288	<1% 45 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 36 of 4096	7% 273 of 3500
node-107	<1% 4 of 500	3% 127 of 3500	3% 127 of 3500	<1% 44 of 12288	<1% 45 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 36 of 4096	7% 273 of 3500
node-108	<1% 4 of 500	3% 127 of 3500	3% 127 of 3500	<1% 44 of 12288	<1% 45 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 36 of 4096	7% 273 of 3500

Troubleshoot a Flow

Use Inbuilt Visibility Engine

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer

This tool provides:

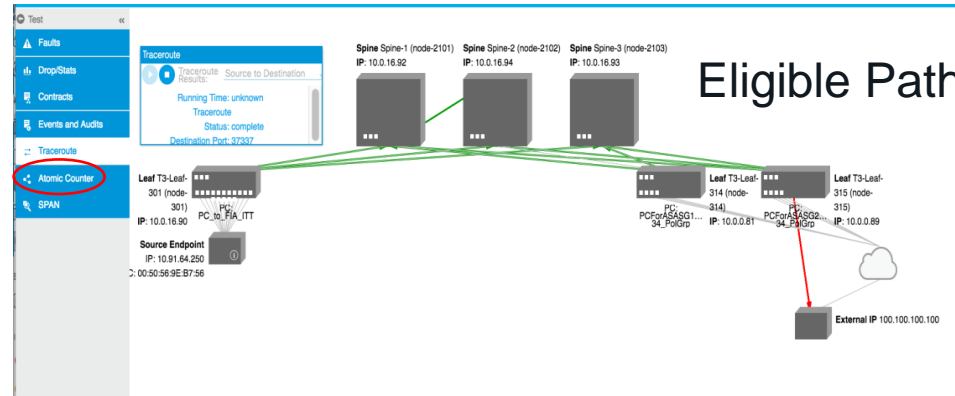
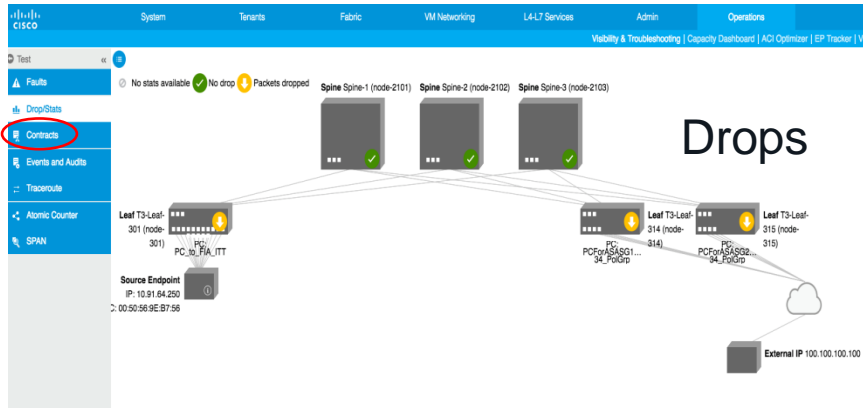
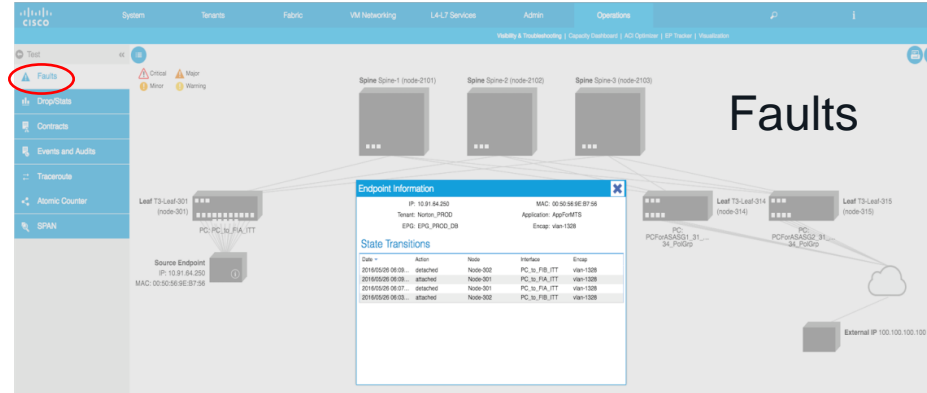
1. Location of the specified end points in the fabric and displays the traffic path including any L4-L7 devices. Along the path between these end points, statistics, contracts, faults, events, and audit logs are displayed in scope.
 2. Optional triggering of traceroute, and atomic counters for troubleshooting these end points. These debugging steps create and delete corresponding debugging policies as needed.
- In interactive mode, you can navigate through these capabilities step by step. In report generation mode, both 1 and 2 are executed automatically for offline analysis.

Session Name: **Test** Description: **Test**

Source: **10.91.64.250** External IP: **100.100.100.100** Destination: **100.100.100.100** External IP

Example: 00:50:56:BD:2E:6C, 10.0.0.1 or 2002:50:22:0:50::1

Time Window: Latest Minutes: **240** To: now Use fixed time



Troubleshoot a Flow

Use Inbuilt Visibility Engine

Fabric Security Policies

The screenshot displays the configuration for Fabric Security Policies in the Cisco NCS600M GUI. The left sidebar has 'Contracts' highlighted. The main area shows two policy configurations:

- Source Endpoint -> External IP:**

Filter ID	Default	Hit	Priority	Match	Hit
1	deny	0	1	any	0
2	allow	0	2	any	0
- External IP -> Source Endpoint:**

Filter ID	Default	Hit	Priority	Match	Hit
1	deny	0	1	any	0
2	allow	0	2	any	0

Network diagrams show Spine 3 (node-2108) and Leaf 73-Leaf 315 (node-2115) connected to a Source Endpoint (IP: 10.81.84.250, MAC: 00:50:56:9E:87:56) and an External IP (100.100.100.100).

Real Time Traffic Capture

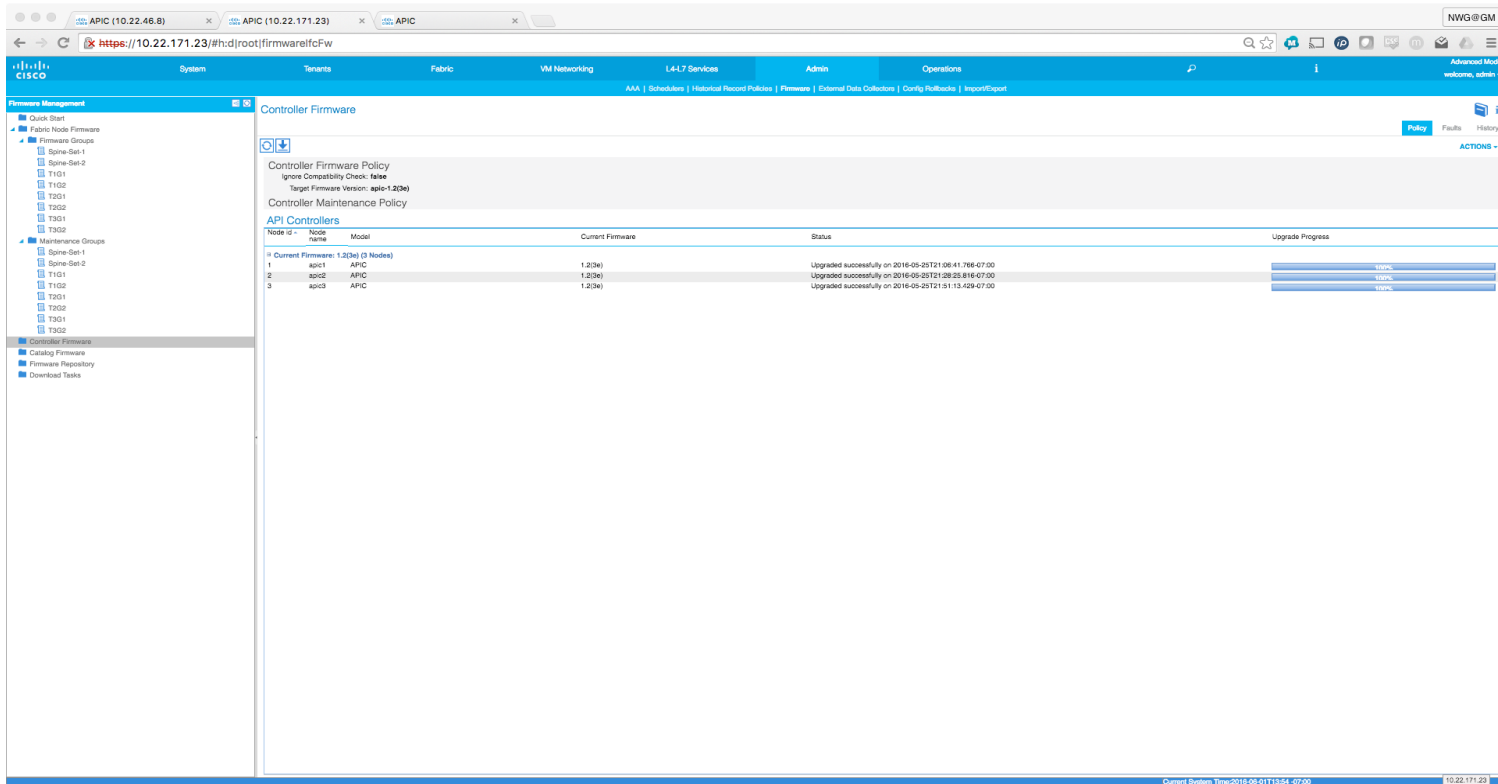
The screenshot displays the SPAN configuration in the Cisco NCS600M GUI. The left sidebar has 'SPAN' highlighted. The main area shows the configuration for a Bidirectional ERSPAN:

- SPAN - Bidirectional ERSPAN:**
 - ERSPAN Source: 10.81.84.250, MAC: 00:50:56:9E:87:56
 - ERSPAN Destination: 100.100.100.100

Network diagrams show Spine 1-3 (nodes 2101-2103) and Leaf 73-Leaf 301 (node-2101) connected to a Source Endpoint (IP: 10.81.84.250, MAC: 00:50:56:9E:87:56) and an External IP (100.100.100.100). The SPAN configuration is applied to the traffic between the Source Endpoint and the External IP.

Maintenance Upgrade #1

Upgrade APIC



The screenshot shows the Cisco Prime Infrastructure web interface. The left sidebar displays the navigation tree with 'Controller Firmware' selected. The main content area shows the 'Controller Firmware' configuration page. It includes sections for 'Controller Firmware Policy' and 'Controller Maintenance Policy'. Below these is a table titled 'API Controllers' showing the upgrade progress for three nodes.

Node ID	Node name	Model	Current Firmware	Status	Upgrade Progress
Current Firmware: 1.2(3a) (3 Nodes)					
1	apic1	APIC	1.2(3a)	Upgraded successfully on 2016-05-25T21:08:41.768-07:00	100%
2	apic2	APIC	1.2(3a)	Upgraded successfully on 2016-05-25T21:28:25.616-07:00	100%
3	apic3	APIC	1.2(3a)	Upgraded successfully on 2016-05-25T21:51:13.429-07:00	100%

Maintenance Upgrade #2

Create Groups

The screenshot shows the Cisco Prime Network Manager interface for configuring firmware groups. The left sidebar shows a tree view with 'Firmware Groups' selected. The main area displays a table of nodes grouped by their firmware groups. A yellow dashed box highlights the 'Firmware Groups' section in the tree and the corresponding rows in the table.

Selected	Node id	Node name	Model	Current Firmware	Status	Role	Firmware Group	Maintenance Group
+ Firmware Group: Spine-Set-1 (2 Nodes)								
	2101	Spine-1	NK-C9508	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:43:31.849-07:00	spine	Spine-Set-1	Spine-Set-1
	2102	Spine-2	NK-C9508	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:43:46.7-07:00	spine	Spine-Set-1	Spine-Set-1
+ Firmware Group: Spine-Set-2 (1 Nodes)								
	2102	Spine-2	NK-C9508	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:10:03.839-07:00	spine	Spine-Set-2	Spine-Set-2
+ Firmware Group: T1G1 (12 Nodes)								
	101	T1-Leaf...	NK-C9128TX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:09:58.082-07:00	leaf	T1G1	T1G1
	103	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:09.589-07:00	leaf	T1G1	T1G1
	105	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:09:25.988-07:00	leaf	T1G1	T1G1
	107	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:00.183-07:00	leaf	T1G1	T1G1
	109	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:03.886-07:00	leaf	T1G1	T1G1
	111	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:10:20.411-07:00	leaf	T1G1	T1G1
	113	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:10:23.729-07:00	leaf	T1G1	T1G1
	115	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:54.820-07:00	leaf	T1G1	T1G1
	117	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:27.086-07:00	leaf	T1G1	T1G1
	119	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:14.960-07:00	leaf	T1G1	T1G1
	121	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:25.988-07:00	leaf	T1G1	T1G1
	123	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:15.145-07:00	leaf	T1G1	T1G1
+ Firmware Group: T1G2 (10 Nodes)								
	102	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:54.842-07:00	leaf	T1G2	T1G2
	104	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:24:14.679-07:00	leaf	T1G2	T1G2
	108	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:04.7-07:00	leaf	T1G2	T1G2
	110	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:19.709-07:00	leaf	T1G2	T1G2
	112	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:22.888-07:00	leaf	T1G2	T1G2
	114	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:39.67-07:00	leaf	T1G2	T1G2
	116	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:18.920-07:00	leaf	T1G2	T1G2
	118	T1-Leaf...	NK-C9128TX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:13.810-07:00	leaf	T1G2	T1G2
	120	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:36.13-07:00	leaf	T1G2	T1G2
	122	T1-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:22.876-07:00	leaf	T1G2	T1G2
+ Firmware Group: T2G1 (8 Nodes)								
	201	T2-Leaf...	NK-C9128TX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:11:13.201-07:00	leaf	T2G1	T2G1
	203	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:07.67-07:00	leaf	T2G1	T2G1
	205	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:19.025-07:00	leaf	T2G1	T2G1
	207	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:24.029-07:00	leaf	T2G1	T2G1
	209	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:31.621-07:00	leaf	T2G1	T2G1
	211	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:17.526-07:00	leaf	T2G1	T2G1
	213	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:07:29.616-07:00	leaf	T2G1	T2G1
	2201	Sw001...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:31.4-07:00	leaf	T2G1	T2G1
+ Firmware Group: T2G2 (7 Nodes)								
	202	T2-Leaf...	NK-C9128TX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:26:53.654-07:00	leaf	T2G2	T2G2
	204	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:19.07-07:00	leaf	T2G2	T2G2
	206	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:25.988-07:00	leaf	T2G2	T2G2
	208	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:28.269-07:00	leaf	T2G2	T2G2
	210	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:28.088-07:00	leaf	T2G2	T2G2
	212	T2-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:23:34.1-07:00	leaf	T2G2	T2G2
	2202	T1-BL-02...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:24:38.485-07:00	leaf	T2G2	T2G2
+ Firmware Group: T3G1 (8 Nodes)								
	301	T3-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:07:52.862-07:00	leaf	T3G1	T3G1
	303	T3-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:07:37.055-07:00	leaf	T3G1	T3G1
	305	T3-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:28.191-07:00	leaf	T3G1	T3G1
	307	T3-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:30.330-07:00	leaf	T3G1	T3G1
	309	T3-Leaf...	NK-C939FPX	#9000-11.2(36)	Upgraded successfully on 2016-05-26T05:08:29.429-07:00	leaf	T3G1	T3G1

Troubleshoot a Flow

Use Inbuilt Visibility Engine

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer

This tool provides:

1. Location of the specified end points in the fabric and displays the traffic path including any L4-L7 devices. Along the path between these end points, statistics, contracts, faults, events, and audit logs are displayed in scope.
 2. Optional triggering of traceroute, and atomic counters for troubleshooting these end points. These debugging steps create and delete corresponding debugging policies as needed.
- In interactive mode, you can navigate through these capabilities step by step. In report generation mode, both 1 and 2 are executed automatically for offline analysis.

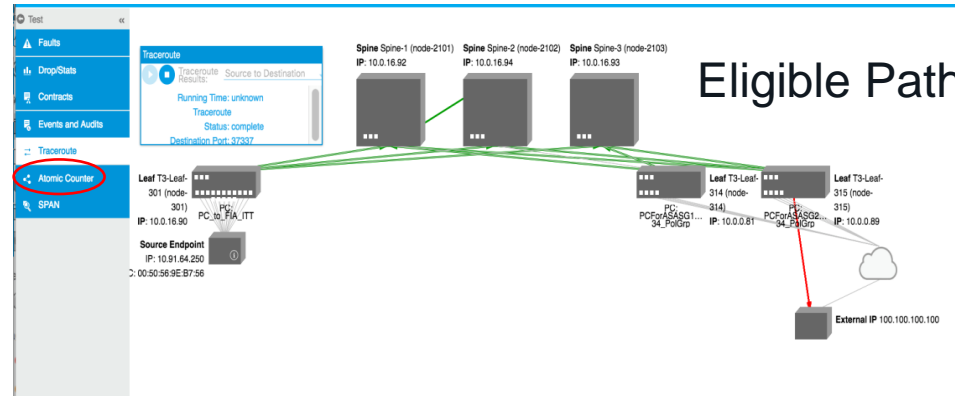
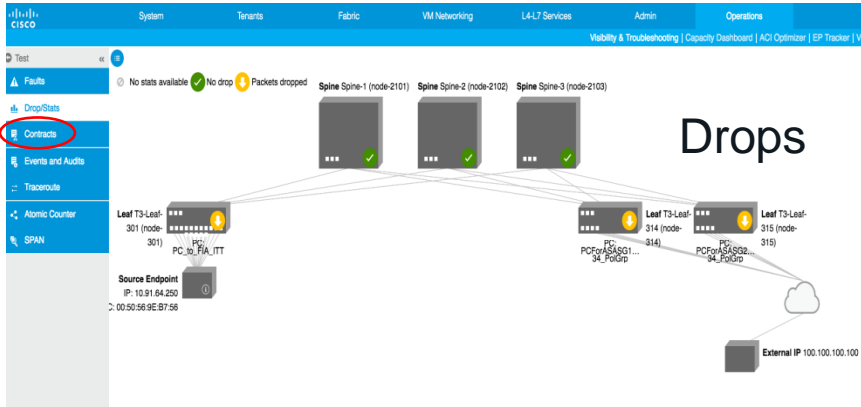
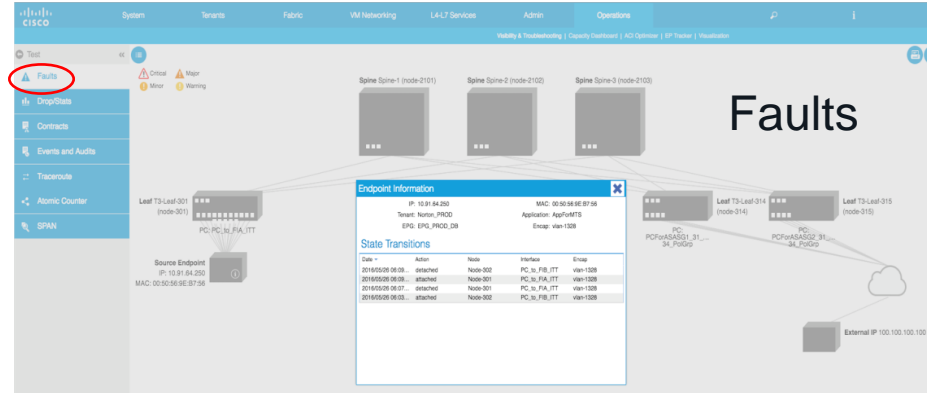
Session Name: **Test** Description: **Test**

Source: **10.91.64.250** External IP: **100.100.100.100** Destination: **100.100.100.100**

External IP: **100.100.100.100** External IP: **100.100.100.100**

Example: 00:50:56:BD:2E:6C, 10.0.0.1 or 2002:50:22:0:50::1

Time Window: Latest Minutes: **240** To: now Use fixed time



Cisco Nexus Dashboard Fabric Controller

Part of Nexus Dashboard

Simple to automate, simple to consume



With Nexus Dashboard
Fabric Controller
(NDFC)



1. Single plane to build and manage multisite fabrics
2. NDFC is an application that you can invoke in single installation for SAN and for the fabric
3. IPAM integration for VXLAN EVPN fabrics
4. Micro Services Scaled mode – active/ active, increased scale for managed/monitored objects
5. Manages IOS-XE and IOS-XR platforms
6. Granular RBAC applicable to Multisite fabric management

New Topology

Side-By-Side Views

- Dynamic Arrangement
- Multi-Fabric/Overlay
- Arrange by Tier
 - Core, Ag, Access Leaf, Spine etc..
- Metadata Tags
- Show FEX links
- Device Pop-Over
- Side-By Side View

The screenshot displays the Cisco Nexus Dashboard interface. On the left is a navigation menu with sections like Fabric Controller, LAN, and Settings. The main area shows a network topology for 'Fabric: RTP-VXLAN-FABRIC' with a hierarchical view of devices including rtp-leaf-1 through rtp-leaf-4. A 'View' panel on the left allows switching between 'Operation' and 'Configuration' views and shows a legend for device health status (Healthy, Warning, Minor, Major, Critical, NA). On the right, a 'Switch' pop-over for 'rtp-leaf-4' is shown, indicating a 'HEALTHY' status. It includes an 'Alerts' table, 'General Info' (Switch Name, IP Address, Serial Number, Role, Border, Model, Version, vPC Domain Id), 'Maintenance Mode Status' (Normal, Connectivity OK), 'Uptime' (306 days, 12 hours, 3 minutes), and 'Inventory' (7 Modules, 0 FEX).

CRITICAL	MAJOR	MINOR	WARNING
0	0	0	0

Switch Name	IP Address	Serial Number
rtp-leaf-4	198.18.133.104	FDO25080L5J

Role	Group
Border	RTP-VXLAN-FABRIC

Model	Version	vPC Domain Id
N9K-C93180YC-FX3	10.1(2)	0

Maintenance Mode	Connectivity Status
Normal	OK

Inventory
7 Modules
0 FEX

New Topology

Side-By-Side Views

- Dynamic Arrangement
- Multi-Fabric/Overlay
- Arrange by Tier
 - Core, Ag, Access Leaf, Spine etc..
- Metadata Tags
- Show FEX links
- Device Pop-Over
- Side-By Side View

The screenshot displays the Cisco Nexus Dashboard Fabric Controller interface. The main view shows a network topology with various components: DCI, NET, VRF, WAN, BL11, BL12, BGW11, BGW12, SPINE11, SPINE12, LEAF11, and LEAF12. A side-by-side view of the SPINE12 device is shown on the right, displaying its general information, alarms, and performance metrics.

General Info

Switch Name	IP Address	Serial Number
SPINE12	10.201.43.12	FDC0341515GT

Alarms (1)

Severity	Count	Warning
critical	0	
major	0	
minor	1	
warning	0	

Performance Metrics

Metric	Value
CPU Utilization	12%
Memory	37%

Capacity Dashboard

View the Capacity of non ACI Fabric

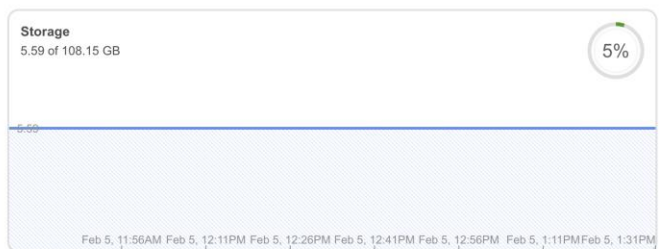
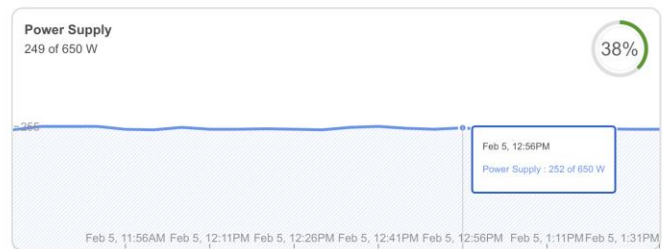
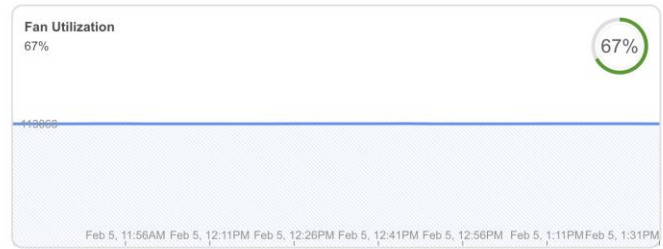
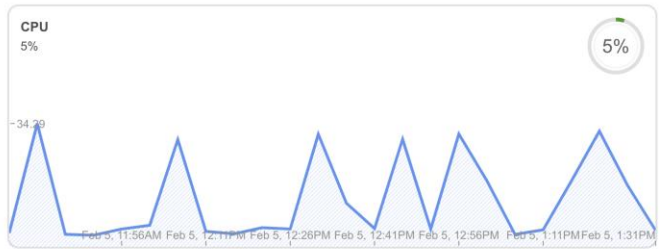
cisco Nexus Dashboard

- Overview
- Operate
- Analyze
- Configure
- Admin

Explore

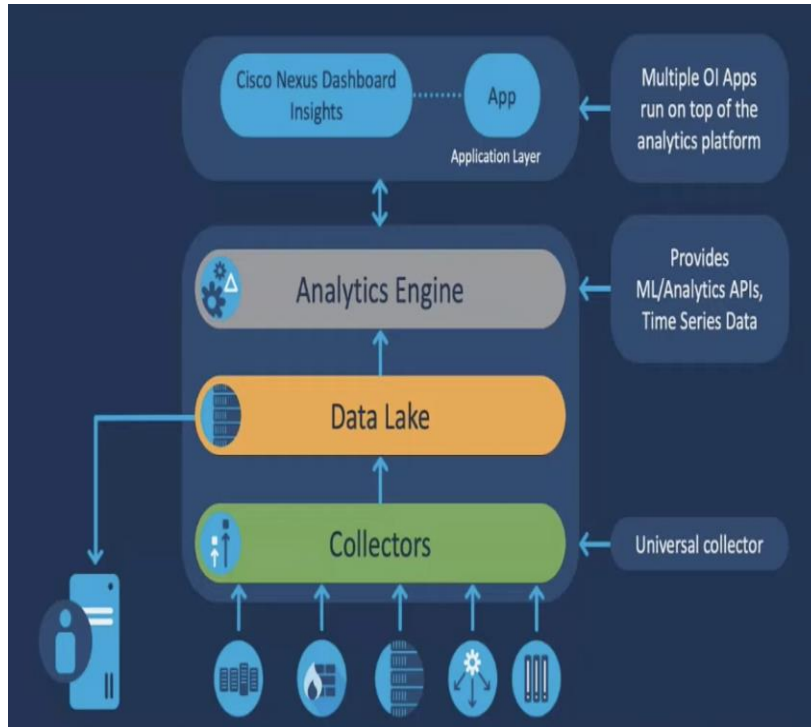
Bookmarks

Hardware Resources for rtp-leaf-4 Current



Nexus Dashboard

Efficient Operations at the DC (AIOps)- Nexus Dashboard



Ingest Anything

A common data model for applications and infrastructure that unifies data across domains

Query Anything

Search using a Unified Query Layer across our AIOps data platform

Visualize Anything

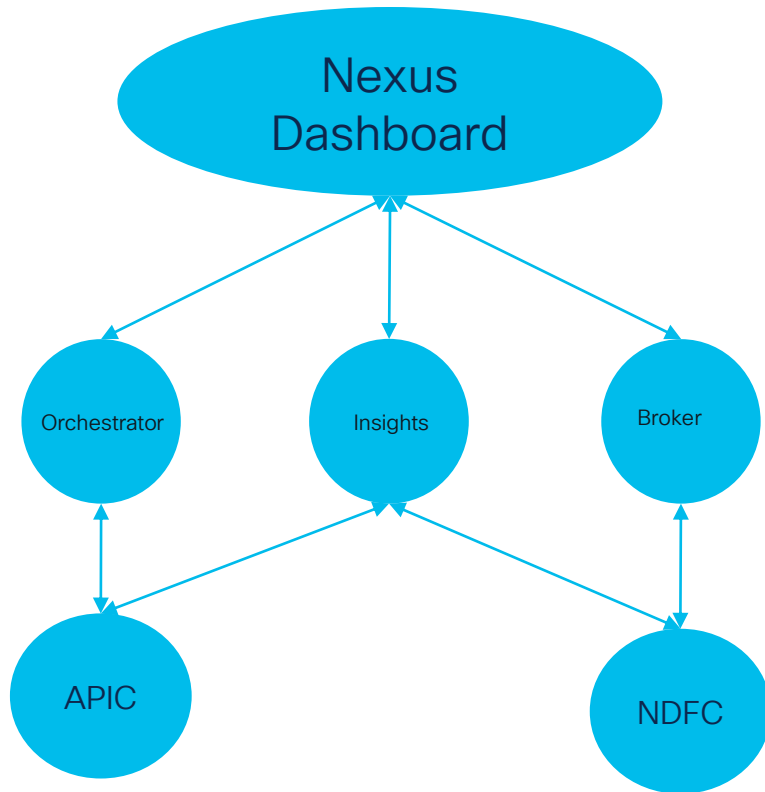
See your apps and infra through a new set of lenses with Hypergraph and Dash Studio

Alert Anything

Harnessing the power of the new AIOps data platform for more sophisticated health rules

Note: Application insights using AppD integration with nexus insight upgrade is not covered in this session

Unified Datacenter Controller views



#1 Benchmarking

#2 Upgrade planning

- Day 0 , Day 1 and Day 2
- Software Image management
- Migrations

#3 Pre and Post Change window baselining

Verify Fabric Communication & relationship

The screenshot displays the Cisco Nexus Dashboard interface for fabric communication verification. The browser address bar shows the URL: ase1.svpod.dc-05.com/appcenter/cisco/nexus-insights/ui/#/overview/globalView. The main navigation menu on the left includes Overview, Operate, Analyze, Configure, Admin, and Explore (highlighted with a yellow box). The Explore section is active, showing a search query: "Can VRF:uni/tn-config_compliance_in/ctx-main_vrf talk to any". The Query Results section displays a path from Source (EPG main_vrf) to Destination (EPG any) with a green arrow and a checkmark, indicating "Can talk". Below this, the "Which entities can talk?" section features a circular network diagram showing connections between various EPGs and VRFs. A filter panel on the right is also highlighted with a yellow box, showing options for View (EPGs, Prefixes), Type (Objects, Tenants, VRFs), and Health Status (Healthy, Unhealthy).

Explore

Connectivity for Site dcloud-sjc on Jan 31st 2024, 11:29 PM

Can VRF:uni/tn-config_compliance_in/ctx-main_vrf talk to any

Query Results

Can source talk to destination?

Source: EPG main_vrf

Destination: EPG any

Can talk

Which entities can talk?

View: EPGs, Prefixes

Type: Objects, Tenants, VRFs

Health Status: Healthy , Unhealthy

Advanced Filter

Analyse the Anomalies

Anomalies

Overview
Operate
Analyze
Configure
Admin
Explore
Bookmarks

Online Sites
Anomalies
Advisories
Analysis Hub

Grouped Active Now

Filter

Anomaly Level

- Critical 109
- Major 11
- Other 98

Category

- Compliance 104
- Connectivity 12
- Capacity

Title

- SLA Compliance Violated
- Configuration Compliance Violated**
- Log Permit Policy Violation
- External Routed Network EPG Has No Contract In Enforced VRF
- Contract Has No Providers
- AppD Netlink Baseline

Configuration Compliance Violated

Filter

What's Wrong?	Anomaly Level	Site	Detection Time	Status
EPG DatabaseServices is not...	Critical	dcloud-sjc	Jan 12 2024 09:30:17.000 AM	Active
EPG ccp_tn1_svc_ccp_nginx-...	Critical	dcloud-sjc	Jan 31 2024 03:30:31.000 PM Recent	Active
EPG CommonPolicies is not...	Critical	dcloud-sjc	Jan 12 2024 09:30:17.000 AM	Active
EPG ccp_tn1_svc_istio-system_ist...	Critical	dcloud-sjc	Jan 31 2024 03:30:31.000 PM Recent	Active
EPG db_cache_epg is not configur...	Critical	dcloud-sjc	Jan 12 2024 09:30:17.000 AM	Active
EPG BalanceServices is not...	Critical	dcloud-sjc	Jan 12 2024 09:30:17.000 AM	Active
EPG Inbound is not configured...	Critical	dcloud-sjc	Jan 12 2024 09:30:17.000 AM	Active
EPG WireServices is not configure...	Critical	dcloud-sjc	Jan 12 2024 09:30:17.000 AM	Active

Analyse the Anomalies

What's the impact?

The attributes of the specified object do not match those in the configuration compliance requirement.

Requirement	Object Type	Object Name	Scope
test sj	EPG	DatabaseServices	common

How do I fix it?

Recommended Solution Failing Condition (1/1)

To fix this anomaly, ensure the expected and the configured values match for all attributes. When making configuration changes, always adhere to best practices around maintenance windows as some changes might be disruptive.

Analysis Hub – The one stop shop for operations



Nexus Dashboard

Insights ▾



Overview

Operate

Analyze

Configure

Admin

Explore

Bookmarks

Analyze > Analysis Hub

Analysis Hub

Analyze and troubleshoot your network with advanced analytics tools optimized for you to gain valuable insights into the performance and health of your network.



Compliance

Monitor your fabric's compliance with custom anomaly rules



Conformance

Keep track of your hardware and software life cycles



Policy CAM

Monitor your network's policies



Connectivity

Analyze flows from one endpoint to another



Log Collector

Collect and analyze logs from you devices



Sustainability

Explore your site's energy usage, cost, and emissions



Delta Analysis

Compare configurations and differences in your site(s) between two points in time



Pre-Change

View the potential impact of configuration changes

Network Compliances Use Cases

Network Compliances

Regulatory Compliance

EPGs in SecureVRF_PCI tenant must be segmented

Business Requirements

EPGs in VDI tenant must always talk to DHCP service in tenant common

IT Governance Operational

- Golden Configuration
- Naming Convention

Creating Network Compliances Use Cases

Configure > Alerts and Rules > Create Compliance Rule

Create Compliance Rule

Basic Information

Settings

Communication Rule Type
Communication
This type will allow you to create a SLA, Segmentation, or Traffic Restriction rule.

Configuration
This type will allow you to create a configuration or naming rule.

Communication Type*

Must Talk To
 Must Not Talk To
 May Talk To

From Objects [View Selected Objects](#)

Object Type*
EPG

Matching Criteria
+ Add Criteria

From Objects Criteria is required.

To Objects [View Selected Objects](#)

Object Type*
EPG

Matching Criteria

Cancel All changes saved

Back Next

Compliance Rule allow_common

Actions ×

General

Name
allow_common

Description
-

Site(s)
dcloud-sjc

State
Enabled

Settings

Compliance Requirement Type
Communication

Communication Type
Must Talk To

From objects
Includes EPGs that in Tenant DN Equal to tn-common

To objects
Includes EPGs that in Tenant DN Equal to tn-common

Traffic Selector Ether Type
IP

Traffic Selector Protocol Type
ALL

View Compliance Analysis Status – Analysis hub

Compliance is a top-level option in the Analysis Hub.

On the Compliance page, the summary of the compliance analysis of the site is shown for the selected time window.

Compliance Summary

Violations by Severity

- Critical: 103
- Warning: 1
- Info: 0

Non-Compliant Resources

- Tenant: 3/64
- Application Profile: 8/97
- Endpoint Groups: 33/320

Rule Violations

Name	Description	Rule Type	Enforcement Status
HTTP	-	Configuration	Enabled
allow_common	-	Communication	Enabled
PREFIX_EPG	-	Configuration	Enabled
ComplianceRule	-	Configuration	Not Inherited
ALLOW_TRAFFIC	-	Communication	Enabled

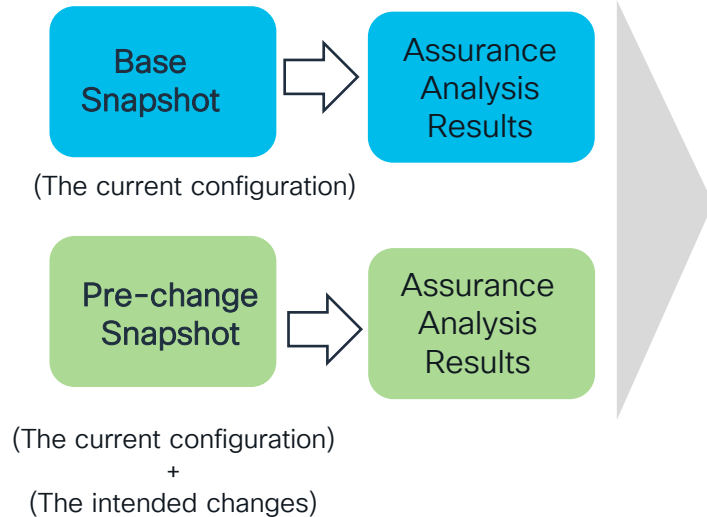
Anomalies from Violations Ungrouped

Filter

What's Wrong?	Level	Category	Detection Time	Status
EPG DatabaseServices is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG auth_egg is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG app_egg is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG WireServices is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG BalanceServices is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG SessionTracking is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG log_egg is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG db_cache_egg is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG db_egg is not configured according to compliance rule test sj	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active
EPG ops is not configured according to compliance rule PREFIX_EPG	Critical	Configuration	Feb-01 2024 01:29:58.000 AM Recent	Active

Pre-Change Analysis using Nexus Dashboard

Analyzes and Reveals the impacts of intended configuration changes.

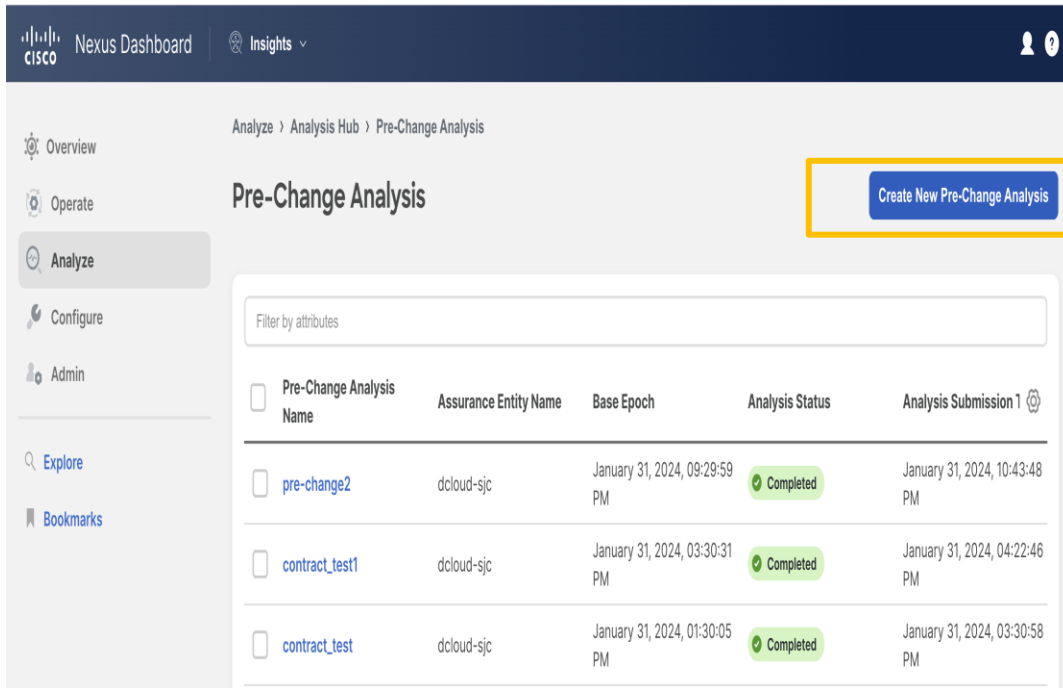


- ✓ Pre Change Analysis – Reveals the impact of the changes.
- ✓ Operations can also have custom snapshots

Other features: Anomaly detection and correlation (software, config or hardware), Upgrade pre-check and post-check across multiple fabrics, data plane dependency mapping and micro burst detection

Create and Run a Pre-Change Analysis

Pre-Change Analysis is within the “Analysis Hub” Option in the Analyze panel. Users can create, edit, clone or delete a pre-change analysis.



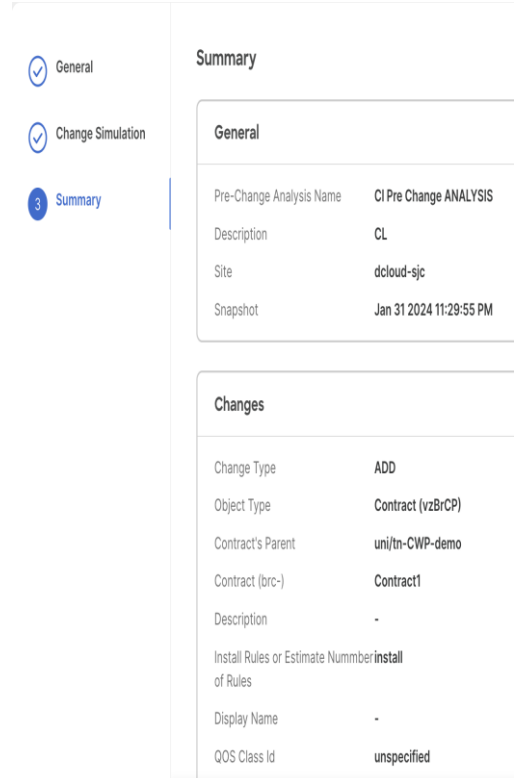
Nexus Dashboard Insights

Analyze > Analysis Hub > Pre-Change Analysis

Pre-Change Analysis

Filter by attributes

<input type="checkbox"/>	Pre-Change Analysis Name	Assurance Entity Name	Base Epoch	Analysis Status	Analysis Submission 1
<input type="checkbox"/>	pre-change2	dcloud-sjc	January 31, 2024, 09:29:59 PM	Completed	January 31, 2024, 10:43:48 PM
<input type="checkbox"/>	contract_test1	dcloud-sjc	January 31, 2024, 03:30:31 PM	Completed	January 31, 2024, 04:22:46 PM
<input type="checkbox"/>	contract_test	dcloud-sjc	January 31, 2024, 01:30:05 PM	Completed	January 31, 2024, 03:30:58 PM



- General
- Change Simulation
- Summary

Summary

General

Pre-Change Analysis Name	CI Pre Change ANALYSIS
Description	CL
Site	dcloud-sjc
Snapshot	Jan 31 2024 11:29:55 PM

Changes

Change Type	ADD
Object Type	Contract (vzBrCP)
Contract's Parent	uni/tn-CWP-demo
Contract (brc-)	Contract1
Description	-
Install Rules or Estimate Number of Rules	install
Display Name	-
QOS Class Id	unspecified

Upgrade Assist

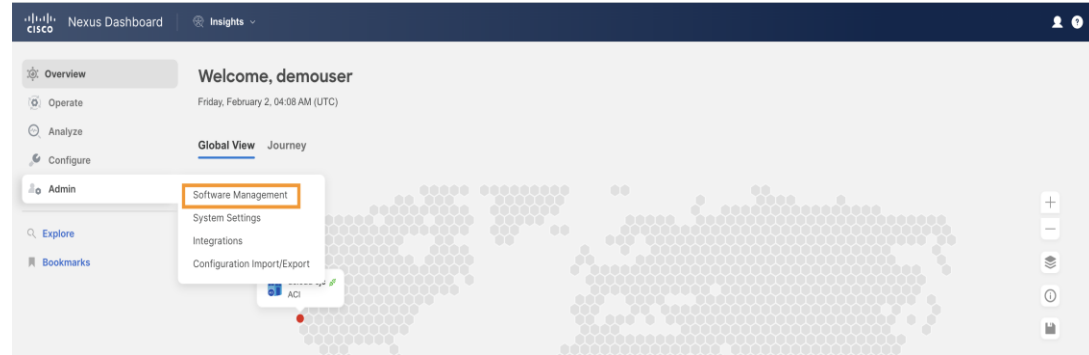
Overview Upgrade Assist

- The upgrade assist feature helps to identify
 - What issues are affecting nodes with the current software versions running on them
 - What issues will no longer be seen post software upgrade
- This is done based off of metadata and affects both ACI and NDFC



How to do an upgrade analysis

- To start an upgrade analysis, select Admin -> Software management



- Start a New Analysis





How to do an upgrade analysis

Create a New software management Job

Admin > Software Management

Create new Software Management job

The screenshot shows a web interface for creating a new software management job. On the left, there is a vertical navigation menu with three items: '1 General Information' (highlighted with a blue circle), '2 Site Firmware', and '3 Node Firmware'. The main content area is titled 'Create new Software Management job' and contains the following elements:

- A 'Name*' field with the text 'Pre_Upgrade' entered. A callout bubble points to this field with the text '1. Name of the Upgrade analysis'.
- A 'Site*' field containing a selection box. The selected item is 'dcloud-sjc' with an APIC logo to its left. A callout bubble points to this selection box with the text '2. Select The Site'.
- A 'Next' button in the bottom right corner. A callout bubble points to this button with the text '3. Click Next'.
- A 'Cancel' button and a back arrow icon in the bottom left corner.



How to do an upgrade analysis

Select the Site Firmware and Move to Next Step

Admin > Software Management

Create new Software Management job

General Information

2 Site Firmware

3 Node Firmware

FW 6.0(3e)(F) Recommended

2024-02-02

[Release Notes](#)

Cancel

Skip this step

Next



How to do an upgrade analysis

Select the Node Firmware and Click Select Nodes to select the switches to be upgraded

Admin > Software Management

Create new Software Management job

- General Information
- Site Firmware
- 3 Node Firmware**

1. Select The Node Firmware

2. Select the nodes

3. Create the Job

Node	Anomaly Score	Model	Type	Serial	Firmware
sjc-apic1	Critical	APIC-SERVER-M3	Controller	WMP2452004M	6.0(3e)
sjc-apic2	Critical	APIC-SERVER-M3	Controller	WMP2452004N	6.0(3e)
sjc-apic3	Critical	APIC-SERVER-M3	Controller	WMP2452004Q	6.0(3e)

10 Rows Page 1

Cancel Back Create Job



How to do an upgrade analysis

Node Selection

The screenshot shows a 'Select Nodes to Update' dialog box. At the top, there is a search bar with the text 'Search'. Below it, a list of nodes is displayed, each with a checked checkbox and a green status icon. The nodes are:

- qa-leaf1leaf
- qa-leaf2leaf
- qa-spine1spine

At the bottom right of the dialog, there is a blue 'Add' button. In the background, a 'Select Nodes' button is visible on the right side of the interface.



How to do an upgrade analysis

Viewing the Upgrade Analysis Results


Admin > Software Management

Software Management

Software Management Jobs ⊙ Current ▼ Refresh New Analysis

Filter

Job Status

 Running 1 Complete 1

Status	Name	Site	Node Target Firmware	Devices	Start Time	End Time	⚙
🔄 Analysis In Progress	Pre_Upgrade	dcloud-sjc		sjc-apic1 , sjc-apic2 , sjc-apic3	Feb 02 2024 04:32:27.160 AM	-	
✅ Analysis Complete	pre_upgrade	dcloud-sjc		sjc-apic1 , sjc-apic2 , sjc-apic3	Jan 31 2024 04:29:43.859 PM	Jan 31 2024 04:45:10.560 PM	

10 ▼ Rows Page 1 of 1 ⏪ 1-2 of 2 ⏩



How to do an upgrade analysis

Viewing the Upgrade Analysis Details

Admin > Software Management > pre_upgrade > Update Analysis

Overview Pre-Update Analysis Post-Update Delta Analysis

Update Summary

Status: 🕒 0 Controllers of 3 Updated

Nodes by Firmware: 6.0(3e) 3

Target Software: [6.0\(3e\)\(F\)](#)

Analysis Last Run: Jan 31 2024 04:30:40.154 PM

3 Controllers

Current: FW 6.0(3e)

Target: FW 6.0(3e)(F)

Controllers

Node	Model	Type	Serial	Starting Firmware
sjc-apic3	APIC-SERVER-M3	controller	WMP2452004Q	6.0(3e)
sjc-apic2	APIC-SERVER-M3	controller	WMP2452004N	6.0(3e)
sjc-apic1	APIC-SERVER-M3	controller	WMP2452004M	6.0(3e)



How to do an upgrade analysis

Viewing the Upgrade Analysis Details

Admin > Software Management > pre_upgrade > Update Analysis

Overview Pre-Update Analysis Post-Update Delta Analysis

Update Summary

Status: 0 Controllers of 3 Updated

Nodes by Firmware: 6.0(3e) 3

Target Software: 6.0(3e)(F)

Analysis Last Run: Jan 31 2024 04:30:40.154 PM

3 Controllers

Current: 6.0(3e)

Target: 6.0(3e)(F)

Controllers

Node	Model	Type	Serial	Starting Firmware
sjc-apic3	APIC-SERVER-M3	controller	WMP2452004Q	6.0(3e)
sjc-apic2	APIC-SERVER-M3	controller	WMP2452004N	6.0(3e)
sjc-apic1	APIC-SERVER-M3	controller	WMP2452004M	6.0(3e)



How to do an upgrade analysis

Pre Update Analysis

Admin > Software Management > pre_upgrade > Update Analysis

Overview **Pre-Update Analysis** Post-Update Delta Analysis

Rerun Analysis

Pre-Update Summary

Status: 0 Controllers of 3 Updated

Validation Results: 38 (Passed 34, Failed 4)

POTENTIAL AFFECTED OBJECTS: 0 (Applications 0)

FORECASTED CLEARED ALERTS: 0 (Anomalies 0, Advisories 0)

POTENTIAL RELEASE DEFECTS: 0 (Bugs 0, PSIRTs 0)

Analysis Last Ran: Jan 31 2024 04:30:40.154 PM

Validation Results

- Devices active check: No Issues found
- APIC Cluster Status: No Issues found
- APIC Disk Space: No Issues found
- Switch Bootflash Usage: Following nodes do not have space in the bootflash folder to download the image: Spine2
- APIC SSD Health: No Issues found

Anomaly Forecast

Critical	Major	Minor	Warning
0	0	0	10
Total	Total	Total	Total
0	0	0	10

Advisory Forecast

Critical	Major	Minor	Warning
0	0	0	0
Total	Total	Total	Total
0	0	0	0



How to do an upgrade analysis

Run delta analysis After the actual upgrade is completed

Overview Pre-Update Analysis **Post-Update Delta Analysis** Run Analysis

Post-Update Summary

Status: 3 Nodes of 3 Updated Analysis Last Ran: **Mar 29 2023 10:34:48.331 PM**

General

Mar 29 2023 06:01:52.913 PM (Earlier) Mar 29 2023 10:34:48.331 PM (Later) **0d 4hr 32m 55s** (Time Range)

Health Delta Policy Delta Operational Delta

Anomaly Count

- Critical**: Earlier 3, Later 7, Overlap 3
- Major**: Earlier 2, Later 2, Overlap 2
- Minor**: Earlier 0, Later 0, Overlap 0
- Warning**: Earlier 7, Later 7, Overlap 7
- Info**: Earlier 0, Later 0, Overlap 0
- Total**: Earlier 12, Later 16, Overlap 12

Health Delta by Resources Only Show Mismatch

Resources	Total		Unhealthy		Total Unhealthy Earlier	Total Unhealthy Later	Total Unhealthy Both	No Issues	
	Earlier	Later	Earlier	Later				Earlier	Later
VRFs	10	10	2	5	2	5	2	8	5

10 Rows Page 1 of 1



How to do an upgrade analysis

The areas checked for during pre-upgrade analysis for 'ACI are listed' below

1	Critical faults	No Critical Faults from System -> Faults
2	OOB management IP	Ensure static OOB Management IP is configured
3	vPC nodes	Configure vPC for the listed leaf nodes to avoid traffic loss during the reboot of leaf nodes.
4	Route reflectors	Configure vPC for the listed leaf nodes to avoid traffic loss during the reboot of leaf nodes.
5	NTP status	Configure NTP to avoid any issues in DB sync between nodes, SSL certificate check, etc.
6	Infra VLAN id	Check if configured infra VLAN ID are same across nodes
7	Fabric Recovery Enabled	Check if Fabric Recovery is in progress
8	CIMC compatibility	Check if running recommended CIMC version
9	Version compatibility	Check version is compatible or multi-hop upgrade is needed
10	Target firmware check	Check if image is copied and available in device
11	SNMPv3 auth compatibility	Check SNMPv3 authorization and/or privacy
12	Remote leaf compatibility	Check if remote leaf is not supported in the target version.
13	Multi-Tier compatibility	Check if Remote leaf is not supported in the target version
14	Bootflash storage	Check for space in bootflash folder to download image
15	Spine redundancy	Check if each pod upgrades spine nodes with at least two separate groups to avoid traffic loss. Spines should not be in maintenance group.
16	Hardware compatibility	Check if hardware is compatible with version
17	Maintenance groups	Check if maintenance groups were created in pre 4.0 release
18	APIC Cluster Status	Check if APIC Cluster status is fully fit for all APIC nodes



How to do an upgrade analysis

The areas checked for during pre-upgrade analysis for NXOS are listed below

#	Validation Step	Description
1	validate po summary	Check if all port-channel members are in (P) state
2	validate vpcs	Check if vpc status is "up"
3	validate vpc role	Check if local vPC role is secondary
4	validate sticky bit	Check if local switch vPC sticky bit is False
5	validate hsrp state	Check if "hsrp mgo state" is Active/Standby
6	validate mods	Check if module in ok/active/standby state and diag pass
7	validate ospf	Check if OSPF is in FULL FULL/DR state
8	validate bgp	Check if BGP session is in Up State
9	validate free space	Check if bootflash on active/standby supervisor is greater than threshold
10	validate logging nvram	Check for Severity 1, 2 or 3 messages
11	validate logging log	Check for Severity 1, 2 or 3 messages
12	validate mod exceptions	Check for non-user initiated resets
13	validate redundancy	Check if redundancy status is "Active with HA standby" for EOR
14	validate reset reason	Check if module was reset due to reasons other than those initiated by user
15	validate system reset reason	Check if module was reset due to reasons other than those initiated by user
16	validate diag module	Checks if previously initiated diag had shown failure
17	validate flash ramdisk	Check if all filesystems are equal to or below integer percentage
18	validate console mgmt	Check if console register bits are RTS DTR DSR
19	validate environment	Check if all modules are in ok state and backup power present
20	validate arp table	Check if certain number of ARP'S are in INCOMPLETE
21	validate cores	Check if core files are present
22	validate device connectivity	Check if we are able to reach the device with PolicyGateway/NDFC/SIM

Migration Best Practices

Datacenter Migration – Strategy and Approach

Source Architecture

Spanning Tree	Fabric Path
Vxlan	ACI

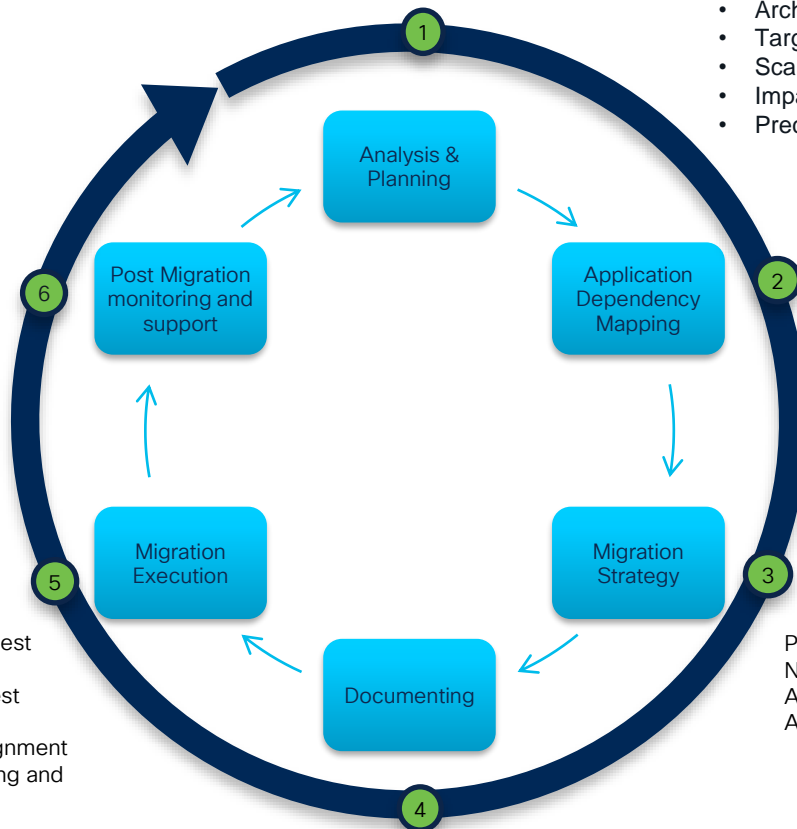


Destination Architecture

Vxlan
ACI

- APM monitoring
- Issue resolution and SLA
- Detailed Health analysis

- Change Management Best practices
- SW and HW Platform best practices
- Go – No Go strategy alignment
- Validations before , during and after migration
- Reporting



- Architecture Governance
- Target Architecture definition
- Scale Considerations
- Impact Analysis
- Prechecks and Validations

- Nexus Dashboard or Cisco Secure Workload (flow metrics or ADM)
- Open-Source automation
- Business Process
- Server to port Mapping
- Automated policy generation

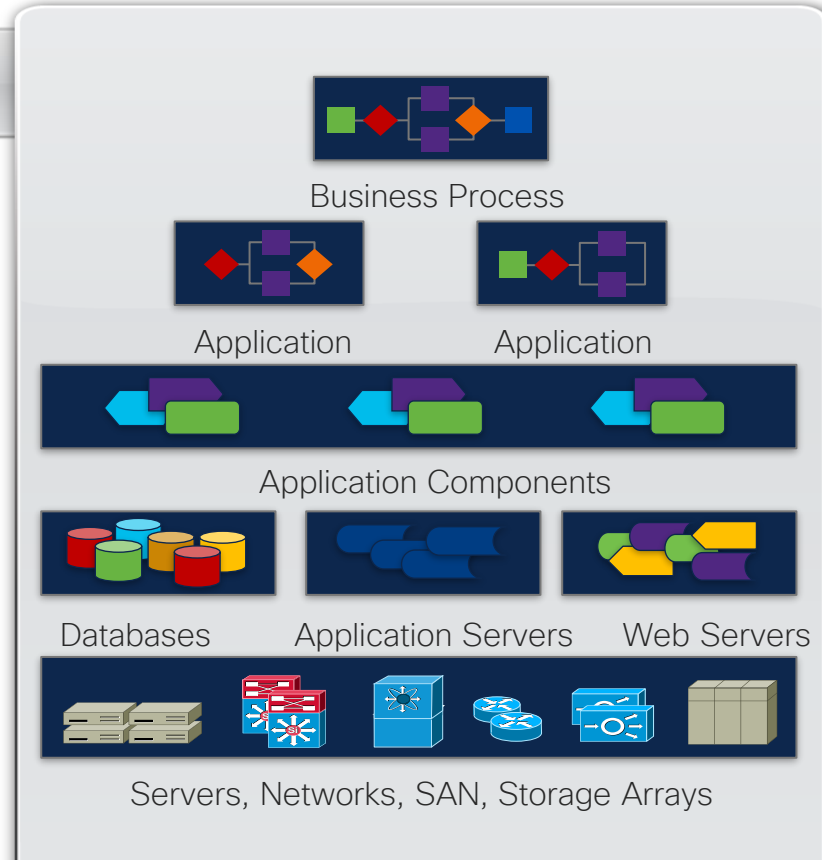
Parallel Vs Hybrid
Network Centric migration
Application based migration
APM during Migration

Runbook, Validation , Rollback

Discover Hidden Interdependencies

Discovery

- **What do I need to migrate?**
 - Understand installed asset base (applications, server, storage, network)
 - Understand interdependencies
- **Understand business and operational constraints**
 - Core business processes
 - Operational processes
 - Application criticality (prioritize)
 - Current DR capability
 - Available downtime window for migration
- **Understand facilities requirements and constraints**
 - Power, cooling and rack space
 - Regulatory compliance constraints



Datacenter Migration Scenarios and Considerations

- Application workload visibility options
- Baseline connectivity Considerations
- Gateway Considerations
- Site Based considerations – for scalability
- Constructs based considerations

Network Considerations for Datacenter Migration

1 Migration Planning Build a parallel vxlan fabric

Establish L2 connection between legacy and new vxlan fabric

Establish Dedicated L3 interconnect Between 2 fabrics

2 Layer 2 Consideration

Dedicated Leaf for L2 Connection using double sided VPC

STP Root bridge placement in the fabric

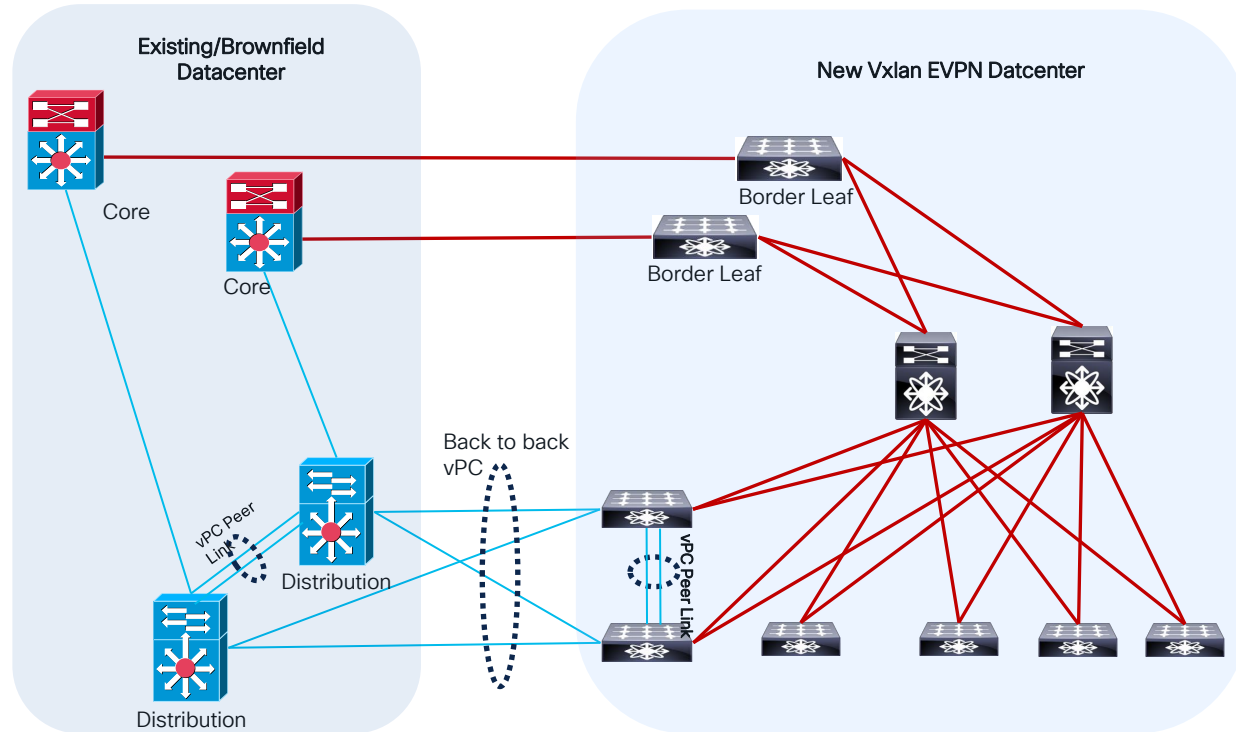
3 Layer 3 Consideration

Non VPC Border Leaf switches for existing Connections to the core

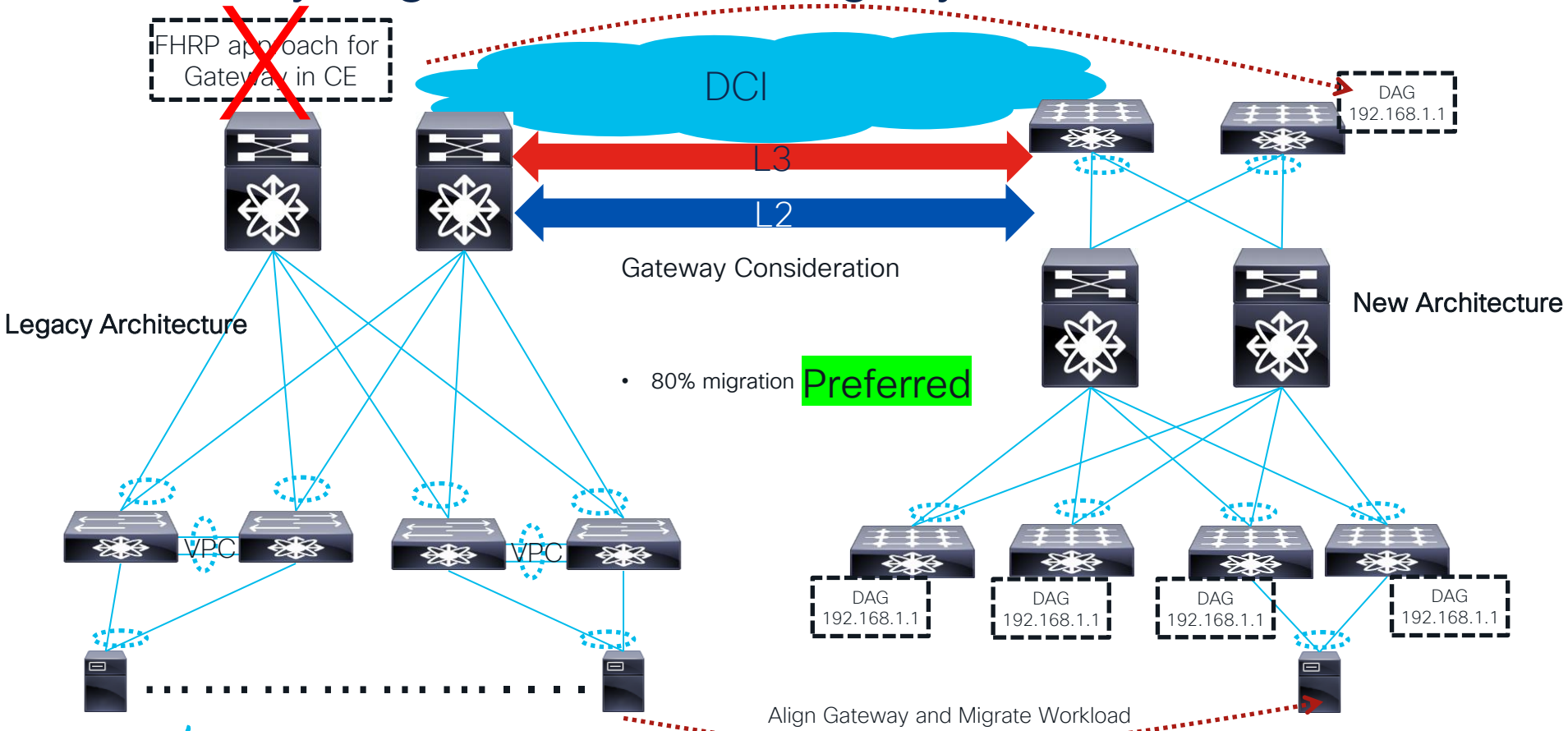
No summarization on border routers during Migration

4 Overlapping Vlans

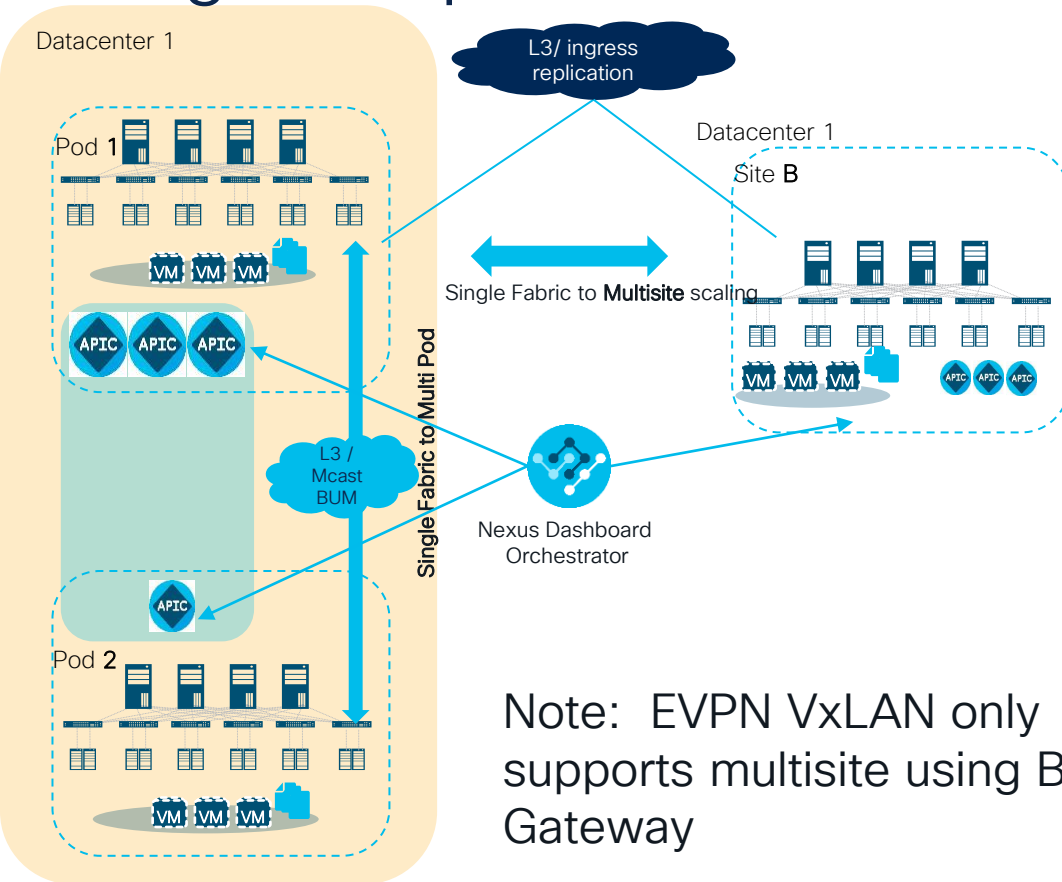
Vlan translation on the Migration Leaf



Gateway Migrations from Legacy to EVPN environment



Migration practices for Scaling out – use case with ACI



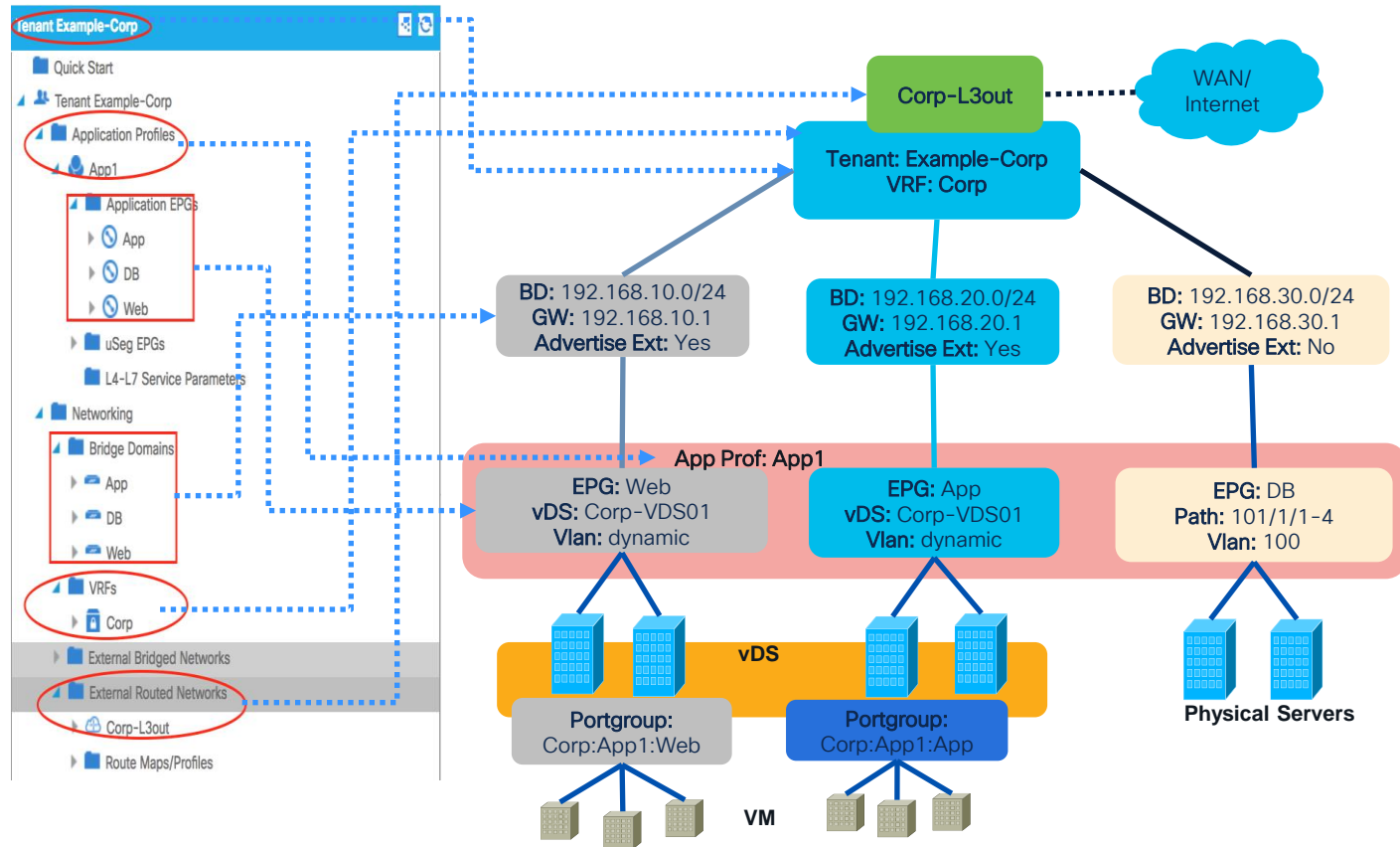
1. Scale Consideration in Data Center 1; options –
 - Multi Pod – same mgmt domain
 - Multi site – separate mgmt. domain
2. Multi-Pod Consideration
 - Extension of APIC cluster- no new policy consideration
 - Special emphasis on the underlay BUM (Mcast support)
3. Multi-site consideration for policy –
 - Creating new policies Vs importing existing policies
 - Hardware consideration and service block localization for multisite
 - Controller based redundancy for multisite

Note: EVPN VxLAN only supports multisite using Border Gateway

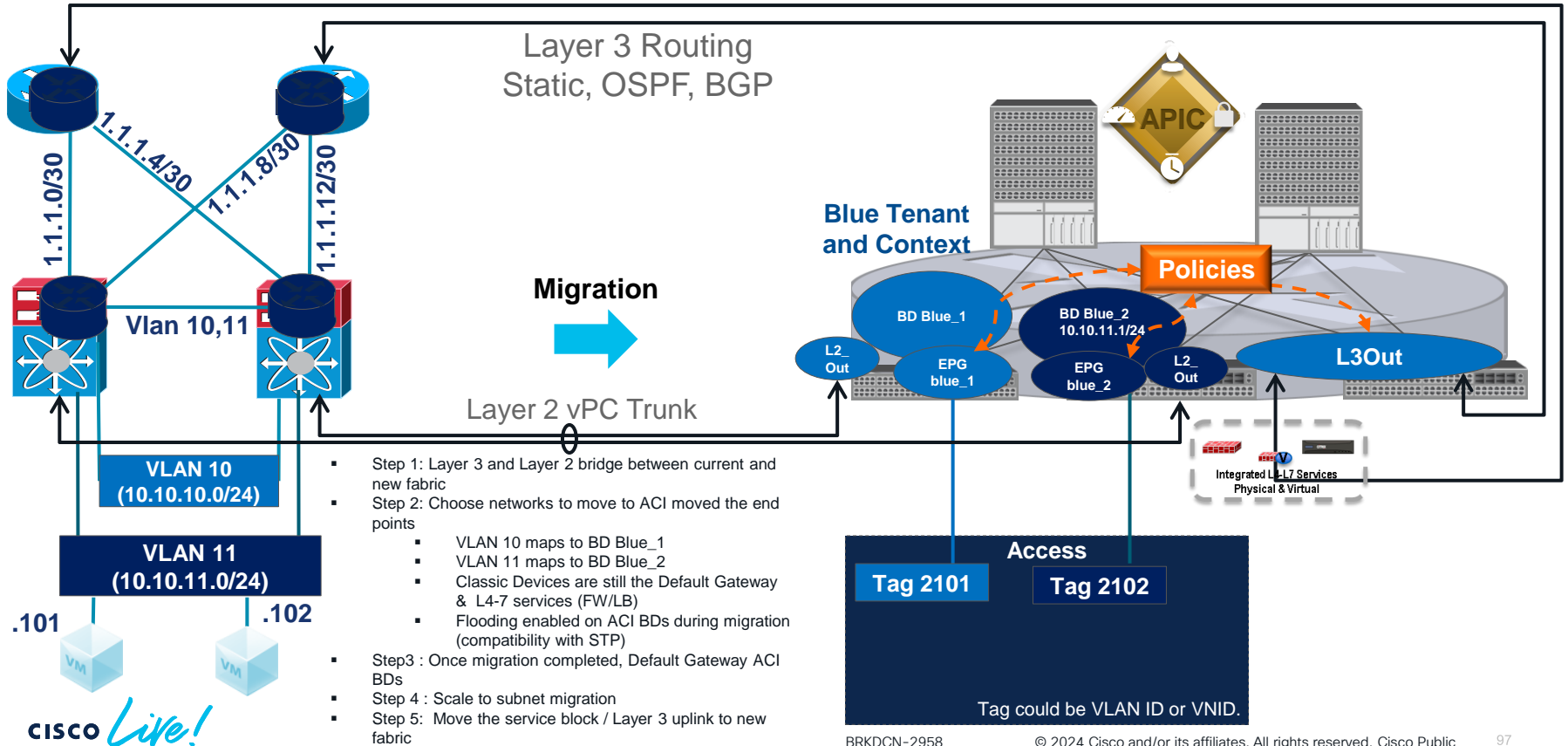
ACI Network Centric Deployment

Network configuration

- VRF CORP vrf configuration
- Interface VLAN 100 (192.168.10.0/24), VIP 192.168.10.1, VRF corp
- Trunk the switch ports with respective vlans
- VMware port Group Assignment
- Routing Configuration for subnets

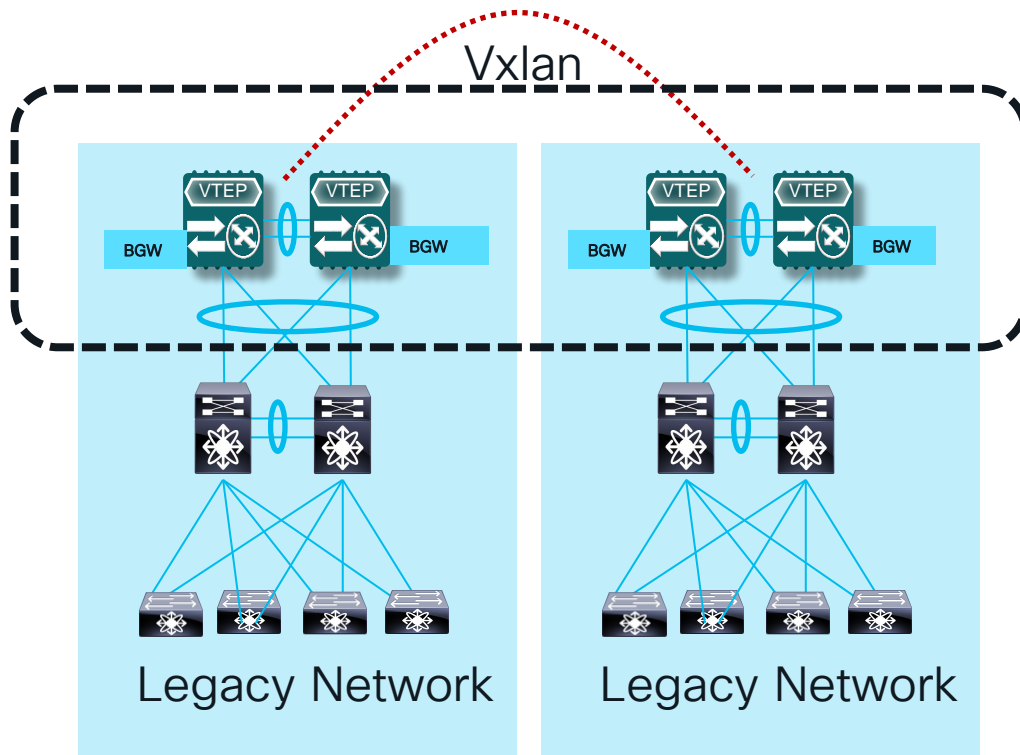


ACI Migration Example



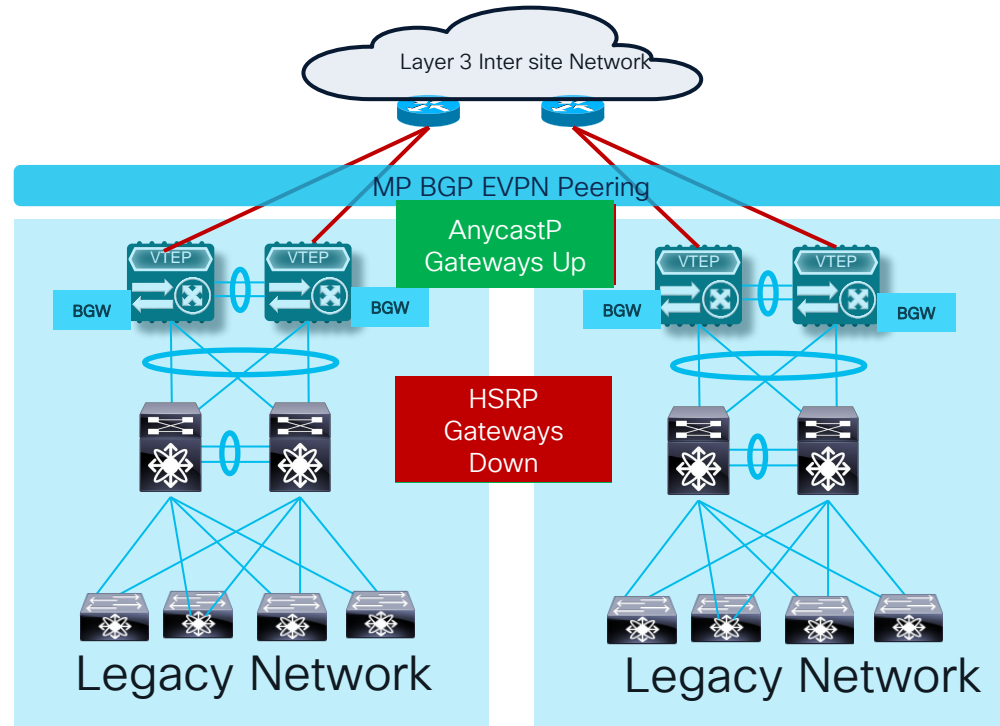
Network Interconnectivity using VXLAN EVPN Border Gateway

- Border Gateway (BGW) provides interconnectivity and translation between multiple Vxlan Sites
- vPC Border Gateway is positioned as replacement for traditional DCI
- Benefits:
 - ✓ Connects to layer 2 domains or 2 domains to EVPN fabric with fault isolation
 - ✓ Simple to deploy compare to old DCI technology and uses EVPN concept
 - ✓ Supports endpoints connected to BGW – cost effective for smaller fabrics Vx Dedicated anycast BGW
- Architectural Benefits
 - Control Plane and Data plane
 - Integrated L2/L3 Extension
 - Fault Containment: BGW provides EVPN Multicast Storm Control
 - Transport Agnostic - Vxlan tunnel built over any IP connectivity
 - Multihoming and Multipath Load sharing



Legacy Network to VXLAN EVPN Migration using Border Gateway

- Introduce a pair of BGW to Legacy sites
 - ✓ Back to back vPC provide multipath connectivity
 - ✓ No STP loops as Double sided vpc provides a single link
- Bring up vPC BGW Underlay network
 - ✓ Route peering between BGW and first Hop layer 3 devices in the intersite network.
 - ✓ eBGP is recommended as the Underlay protocol
- Configure vPC BGW overlay network
 - ✓ MP-BGP as the overlay Control Plane between BGW nodes in two sites.
 - ✓ Full mesh eBGP or route servers in external network depending on size of network
- Configure L2 extension across sites
 - ✓ Should be point-to-point connection & dedicated links.
- Migrate HSRP Gateway on Distribution to Anycast Gateway on BGW
 - ✓ Should be point-to-point connection & dedicated links.

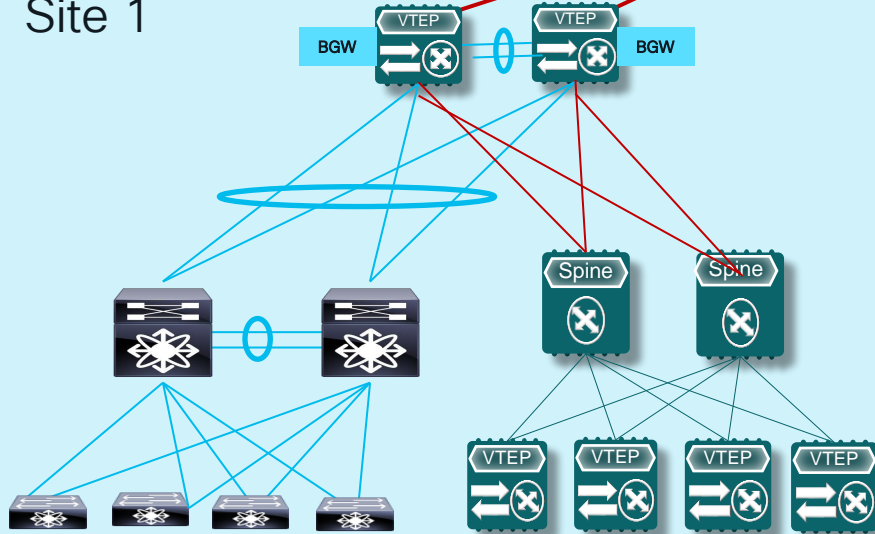


Transition Legacy Network to VXLAN EVPN using Border Gateway – Final Step

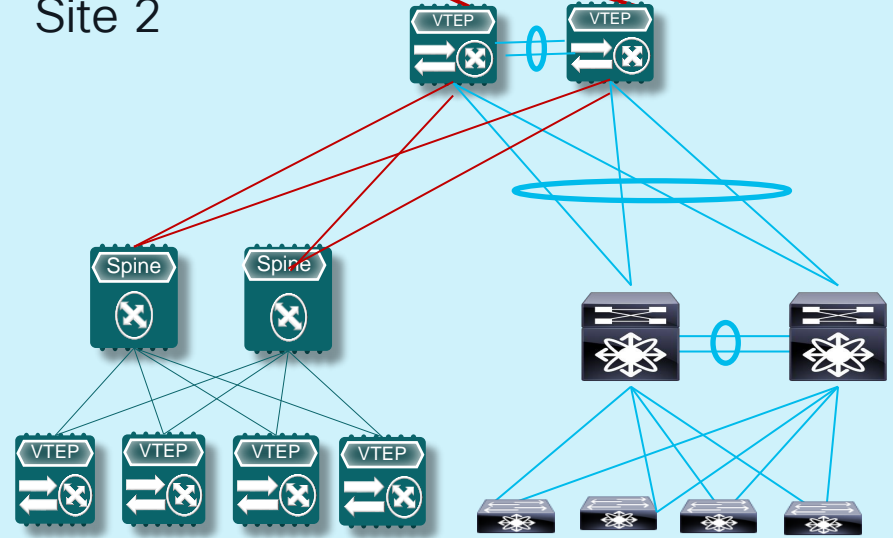
- Build a parallel Nexus 9000 Hub and Spoke Evpn Vxlan Fabric
- ✓ Workload migration commences at this point.



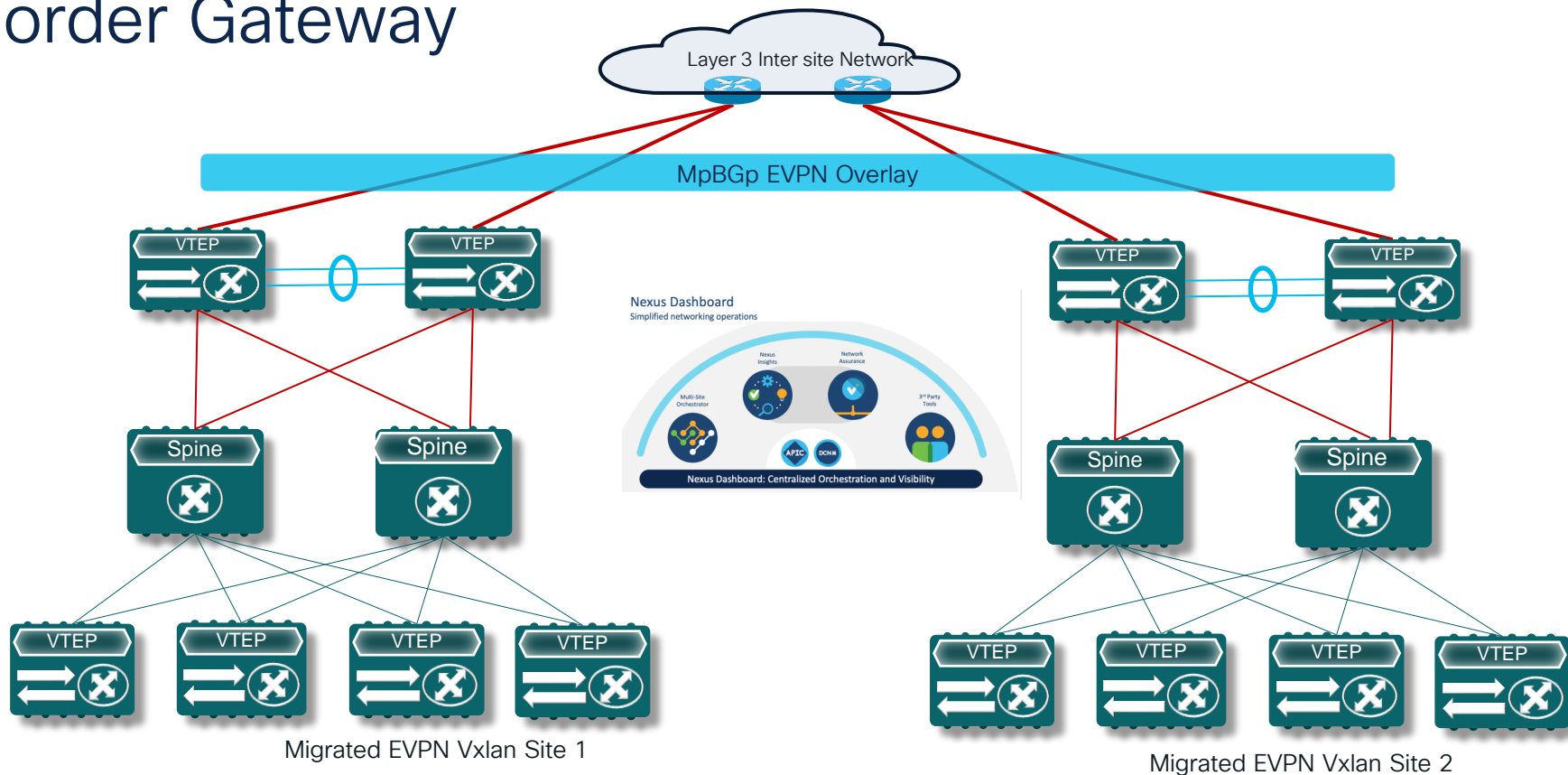
Site 1



Site 2



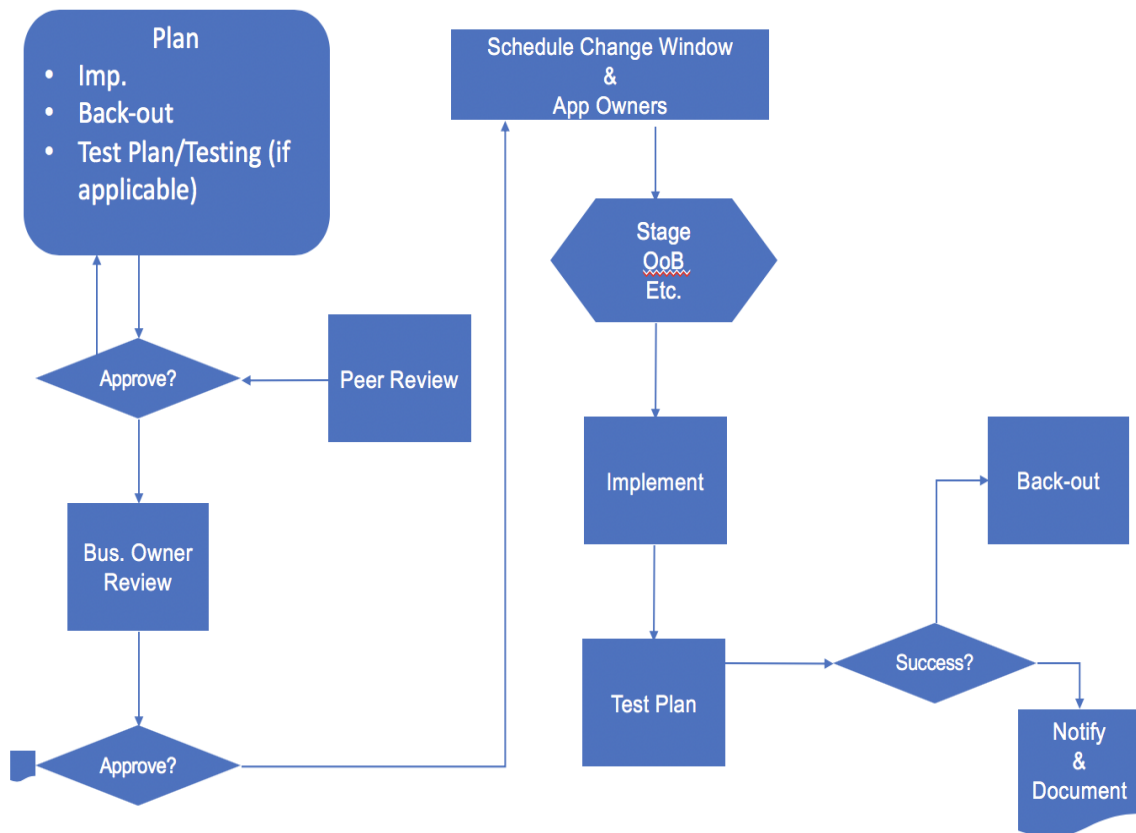
Legacy Network to VXLAN EVPN Migration using Border Gateway



Change Management

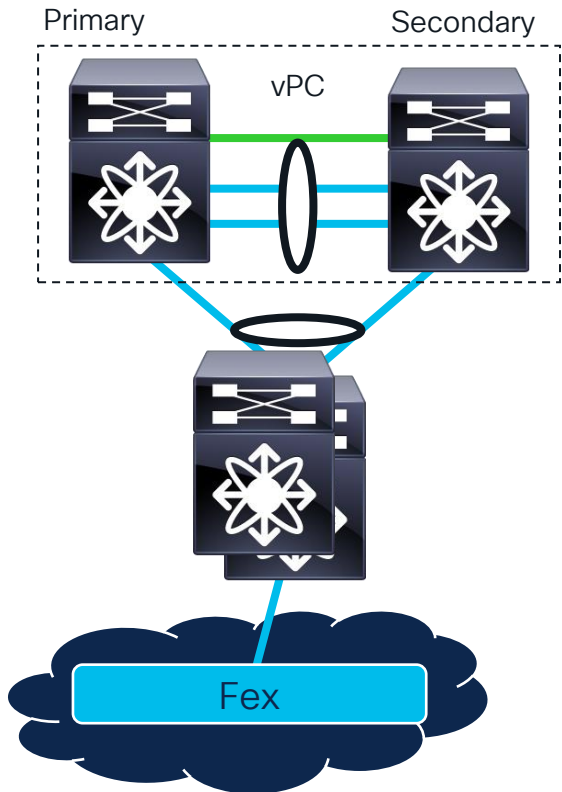
Maintenance Windows – Golden Rules

- Change Review Board
- Schedule when environment will be least impacted.
- Software Staging
- Verify out of band.
- Test! After *and* before.



Traditional vPC Environment Change

Change Best Practice and Window



Core Isolation

1. Graceful L3 Protocol Isolation
2. Layer 2 Isolation
 - VPC
3. Interface Isolation

Using GIR Mode Steps 1-3 could be achieved prescriptively.

Access Isolation

1. Layer 2 Isolation
 - VPC
2. Interface Isolation
 1. Fex-fabric (include/exclude)
 2. Dual-attached FEX Procedure * Recommended

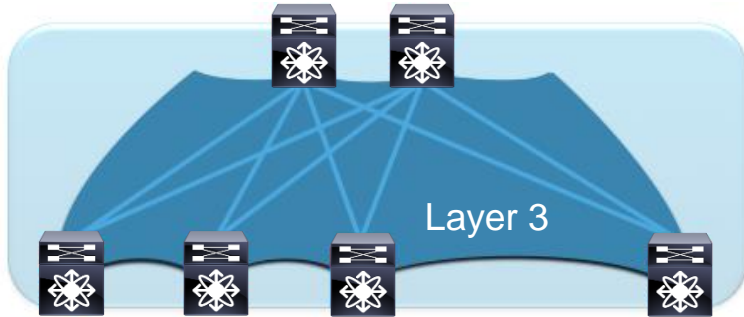
Using GIR Mode Steps 1-2 could be achieved prescriptively.

NOTE: Maintenance mode consideration should be based on Fex-fabric connectivity.

If change window is for software upgrade or spot fix, consider ISSU or SMU feasibility.

L3 Environment

Change Best Practice and Window



Core Isolation

1. Graceful L3 Protocol Isolation
2. Interface Isolation

Using GIR Mode Steps 1-2 could be achieved prescriptively.

Access Isolation

1. L3 Protocol isolation
2. Layer 2 Isolation
 - vPC
3. Interface Isolation
 1. Fex-fabric (include/exclude)
 2. Dual-attached FEX Procedure * Recommended

Using GIR Mode, prescriptive isolation is possible.

If change window is for software upgrade or spot fix, consider ISSU or SMU feasibility.

Summary

Putting it all Together

- What to use? GIR Mode? Patching? ISSU? All of them?

Option \ Situation	Critical Bug Fix & PSIRT	Hardware Upgrade	New Features
ISSU	✓	✗	✓
GIR + Cold Boot	✓	✗	✓
GIR + Disruptive Installer	✓	✗	✓
SMU Restart	✓	✗	✗
GIR + SMU ISSU	✓	✗	✗
GIR	✗	✓	✗

Datacenter Operations –key take ways

- Understand the features and relations to best practices
- Utilize Software hardware best practice in deployment of the Data center
- Change Management features
 - Isolation (GIR)
- Tools used to manage DC environment
 - Day 0,1,2 use controllers based on automation
 - Assurance to manage DC use Nexus Insights

Datacenter Migrations –key take ways

1. Verify environment conforms to data center networking best practices, and leverage DC controllers
2. Isolate Node to minimize the disruption - leverage features like GIR for change window planning
3. Leverage the Migration methodology and use cases to customize your transformation

Technical session surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



The bridge to possible

Thank you

CISCO *Live!*

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white center on the right side.

CISCO *Live!*

Let's go