The bridge to possible

Data Center Maintenance and Migration Best Practices

Arvind Durai, Director Solutions Integration
Anis Edavalath, Technical Leader Engineering

BRKDCN-2612

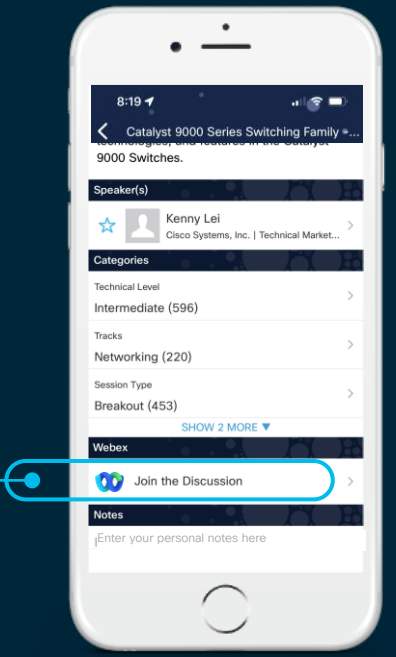
Cisco Webex app

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2612

Webex spaces will be moderated by the speaker until June 17, 2022.

Arvind Durai

- 22 years with Cisco Advanced Services
- Has worked with 100+ customers in enterprise architecture, technology designs and operational simplification
- 14 years of Active Cisco live presenter
- Co-authored five Cisco Press Books
    - Cisco Firewall Services Module, Virtual Routing in the Cloud, TCL Scripting for Cisco IOS and IP Multicast vol1 & 2
- CCIE R/S and Security #7016

Anis Edavalath

- 10 years with Cisco Advanced Services
- 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

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
  - Migration – Features and Tools (controllers)
  - Migration Methodolgy

Agenda

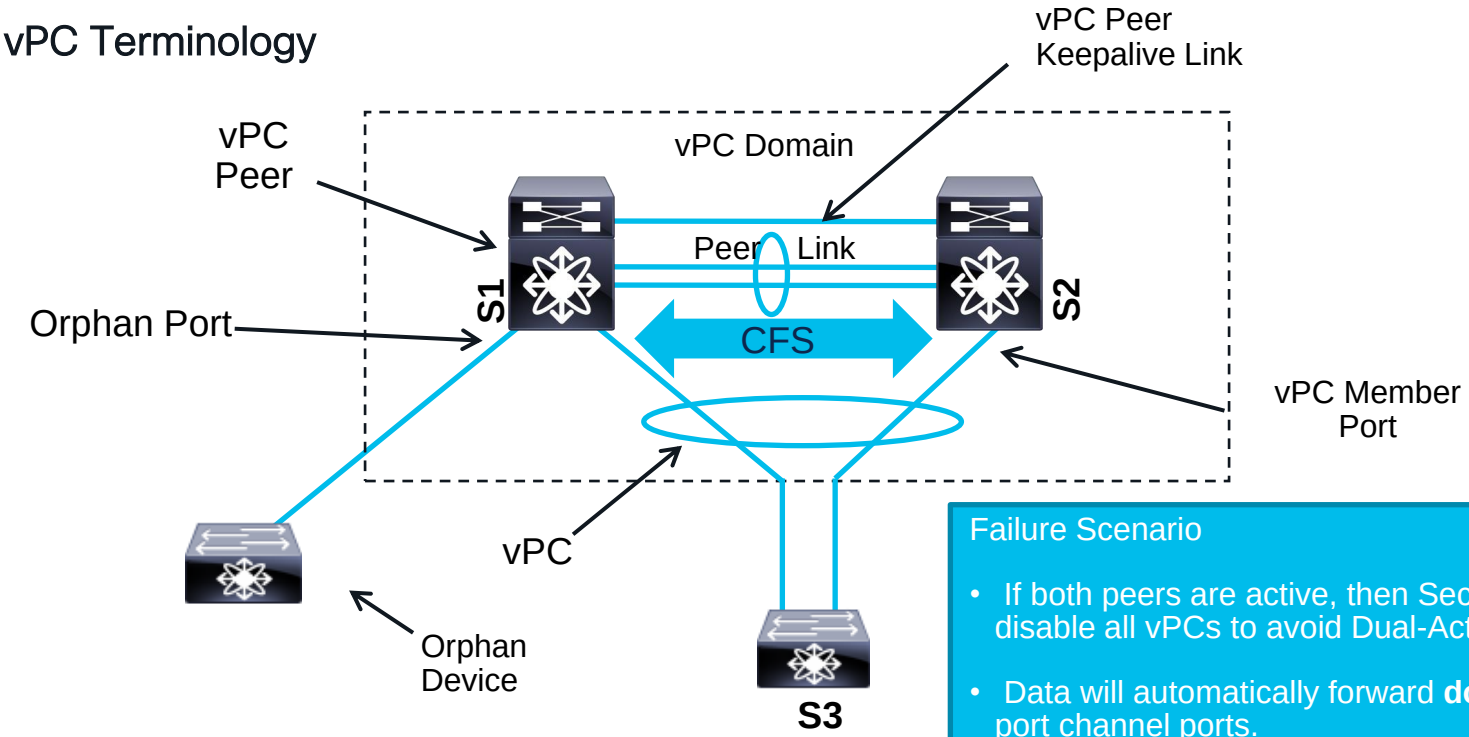
- Baseline
  - VPC, VxLAN & ACI Refresher
  - Change Management best practices
- Features and Tools
  - Graceful insertion and removal
  - Fabric controllers and Nexus
- Migration Methodology
  - Five key Use cases
- Change Window Best Practices

DC Baseline Refresher

vPC Feature Overview

For Your Reference

vPC Terminology

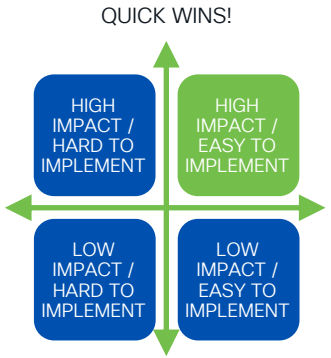


Failure Scenario

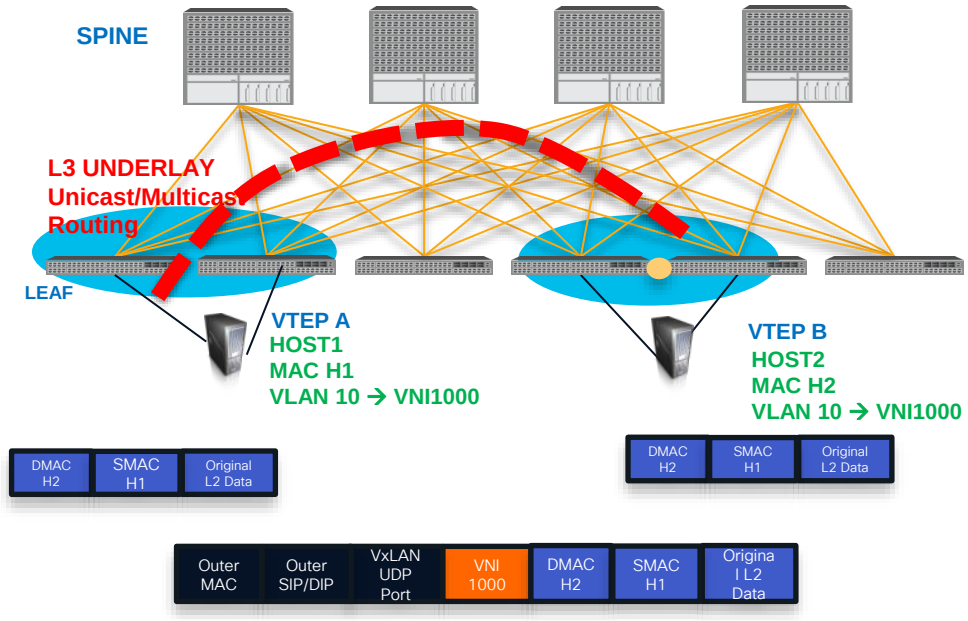
- If both peers are active, then Secondary vPC peer will disable all vPCs to avoid Dual-Active.
- Data will automatically forward **down** remaining active port channel ports.
- Loss of in-flight packets will depend on deployment of vPC best practice.

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.



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

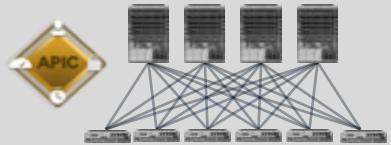
- No need of Spanning Tree (blocks paths)
- Utilize L3 underlay network (ECMP, Link Agg,…)

Multi-Tenant with virtualization

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

SDN ‘with’ FCAPS ‘and’ Automation

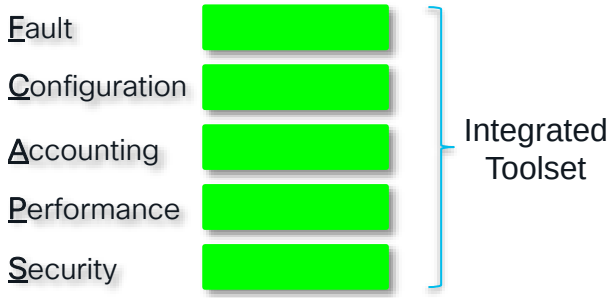
Application Centric Infrastructure



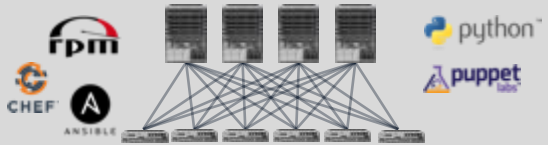
Turnkey integrated solution with security, centralized management, compliance and scale

Automated application centric-policy model with embedded security

Broad and deep ecosystem



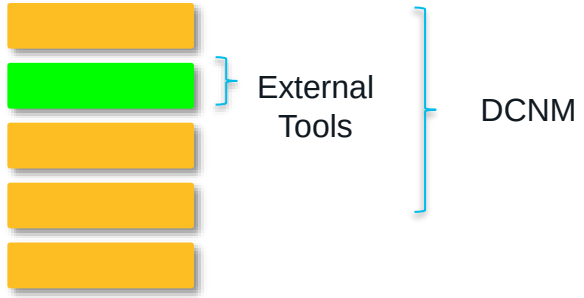
Programmable EVPN Fabric



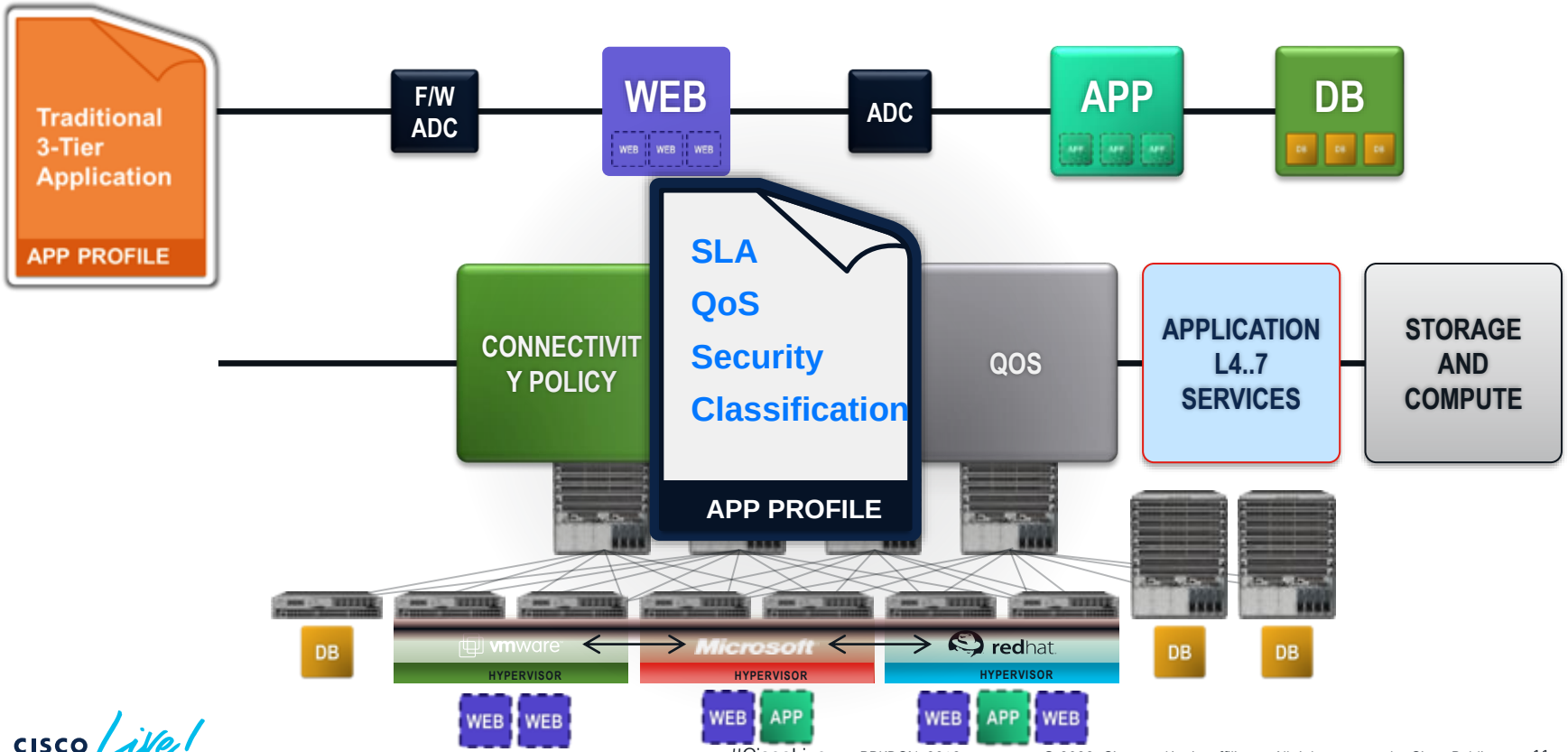
Modern NX-OS with enhanced NX-APIs

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

Custom Script based Operations and Workflows



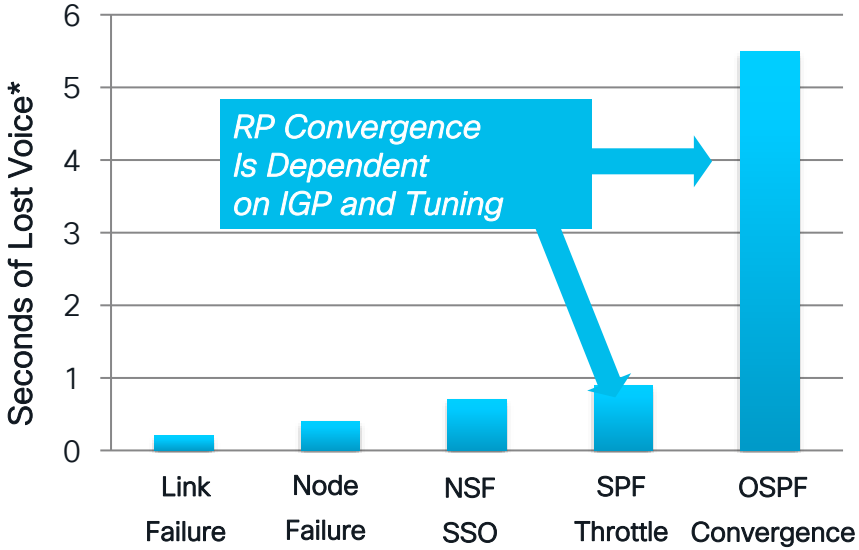
Application Network Profiles (ANP) & ACI: how it works?



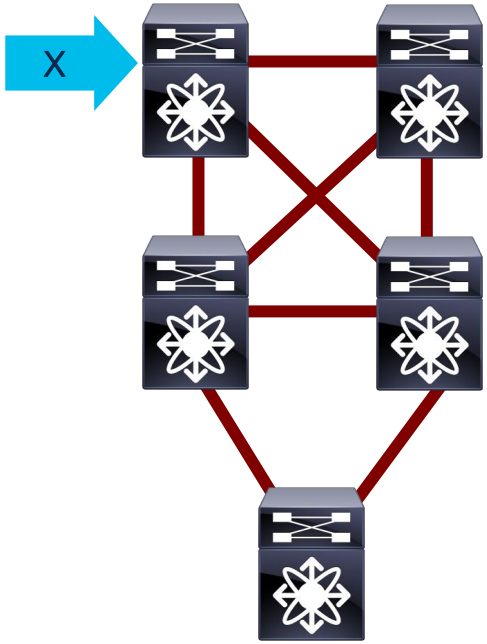
Standalone Chassis Redundant Core

Failure or Change at the Core

- Redundant topologies with equal cost paths provide sub-second convergence.
- NSF/SSO provides superior availability in environments with non-redundant paths.



* Route scale dependent.



Best practices:
- Layer 3
- Layer 2
- Hardware

- Enable BFD for all OSPF neighbor links
- Adjust OSPF spf-throttling timers with:

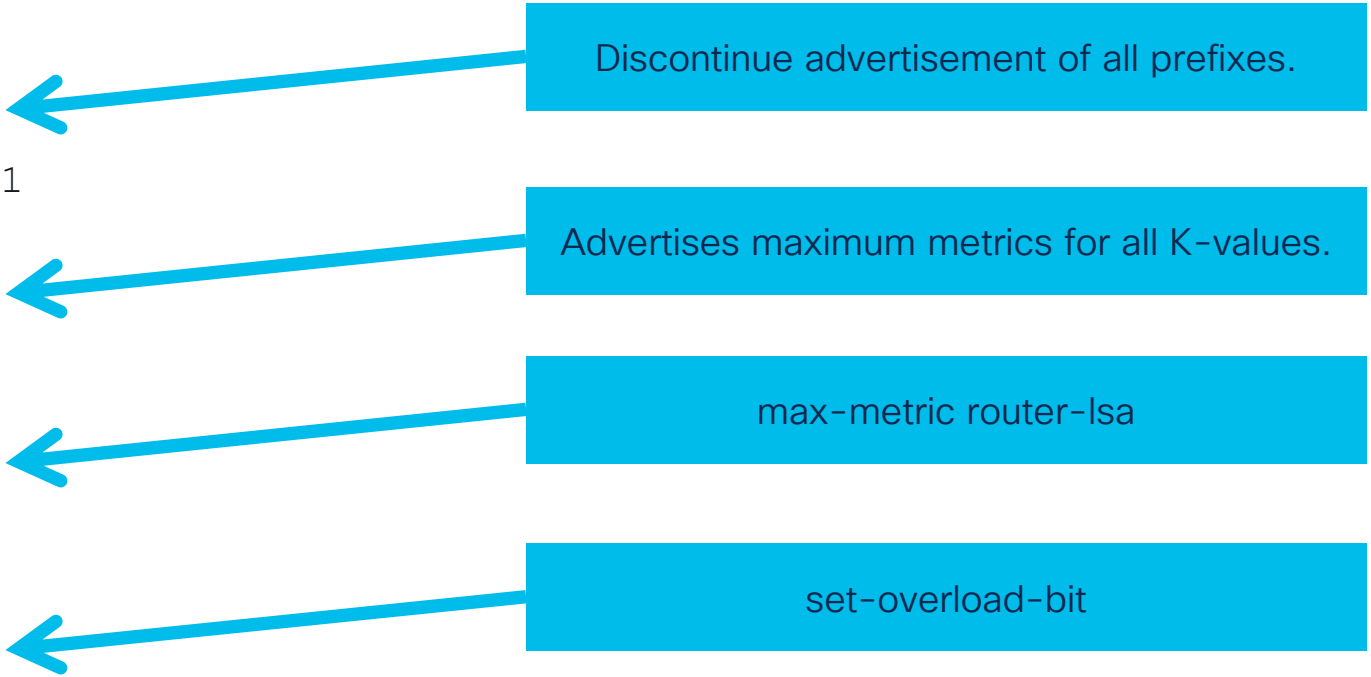
```
timers throttle spf
timers throttle lsa
timers lsa arrival
```

NX-OS Graceful Insertion and Removal

cisco Live!

Nexus Graceful Removal

```
router bgp 33
   isolate
 router eigrp 1
   isolate
 router ospf 1
   isolate
 router isis 1
   isolate
```



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.

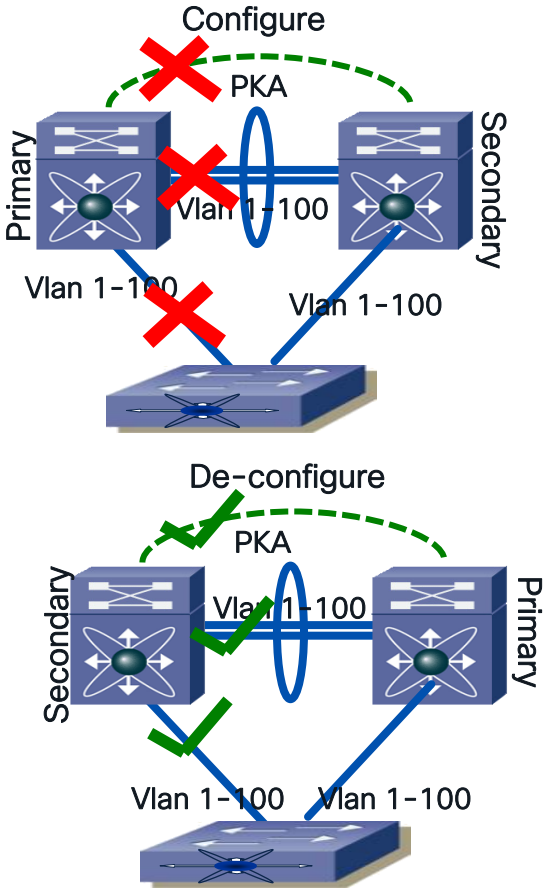
```
N9372(config)# no system
mode maintenance
Following configuration
will be applied:
  router bgp 33
    no isolate
  router eigrp 1
    no isolate
  router ospf 1
    no isolate
  router isis 1
    no isolate
```

VPC Shutdown Feature

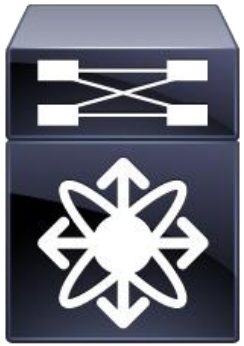
This feature allows customer to manually “isolate” a switch from vPC domain. This is a vPC configuration option.

Pre-VPC Shutdown	VPC Shutdown Behavior

• No “shutdown” command.
• Manual Shutdown Required
  • Down vPCs
  • Down Peer Link
  • vPC Members
  • Etc.
	• 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...

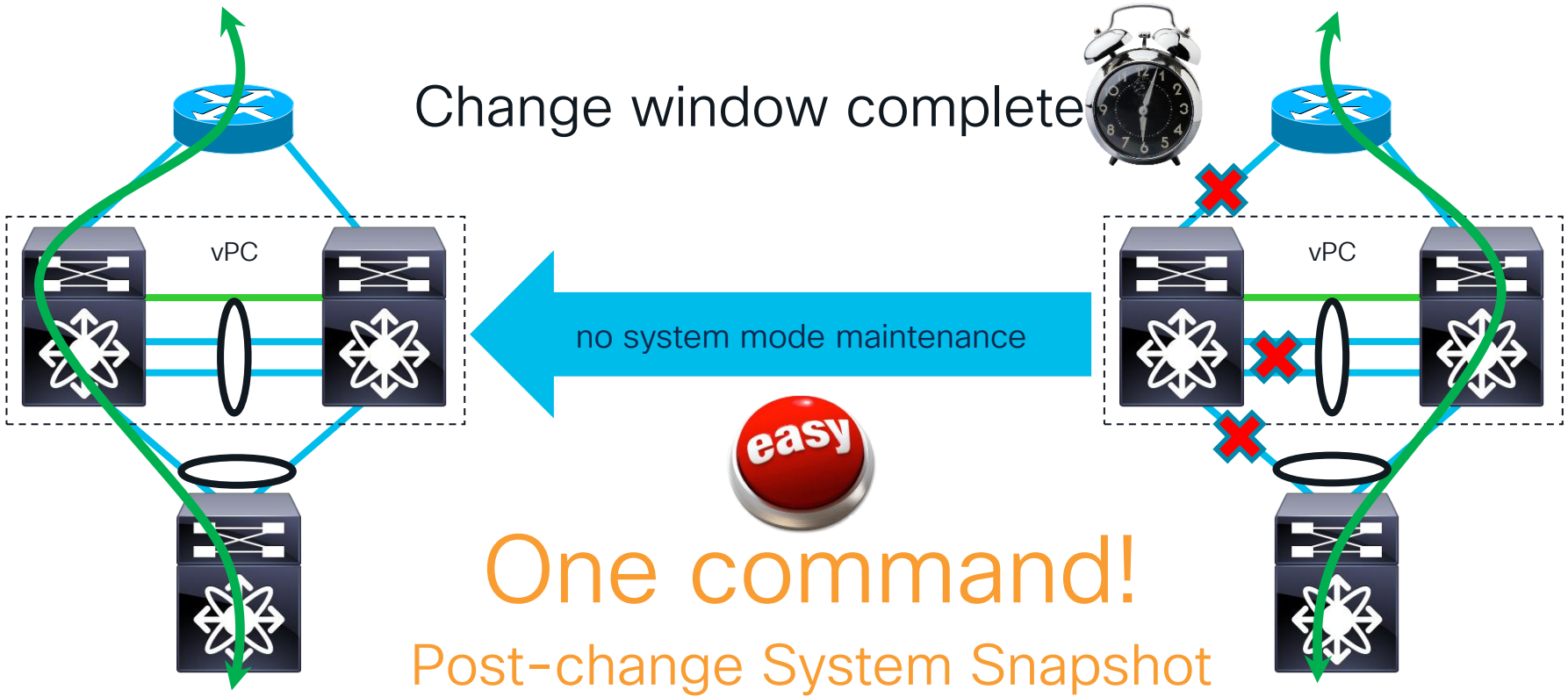
Graceful Insertion and Removal

Change window begins.

One command!

Pre-change System Snapshot

Graceful Insertion and Removal



One command!

Post-change System Snapshot

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
• Generated by default • Parses configuration to determine changes going into and out of GIR • Changes based on base protocol configuration settings. • Use: Maintenance Windows	• 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

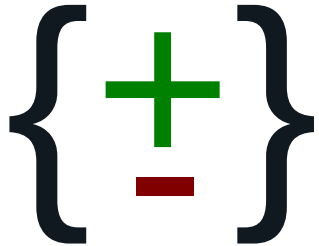
```
Nexus# sh snapshots compare before_maintenance after_maintenance
================================================================================
Feature Tag           before_maintenance           after_maintenance
================================================================================

[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**
<...>
```

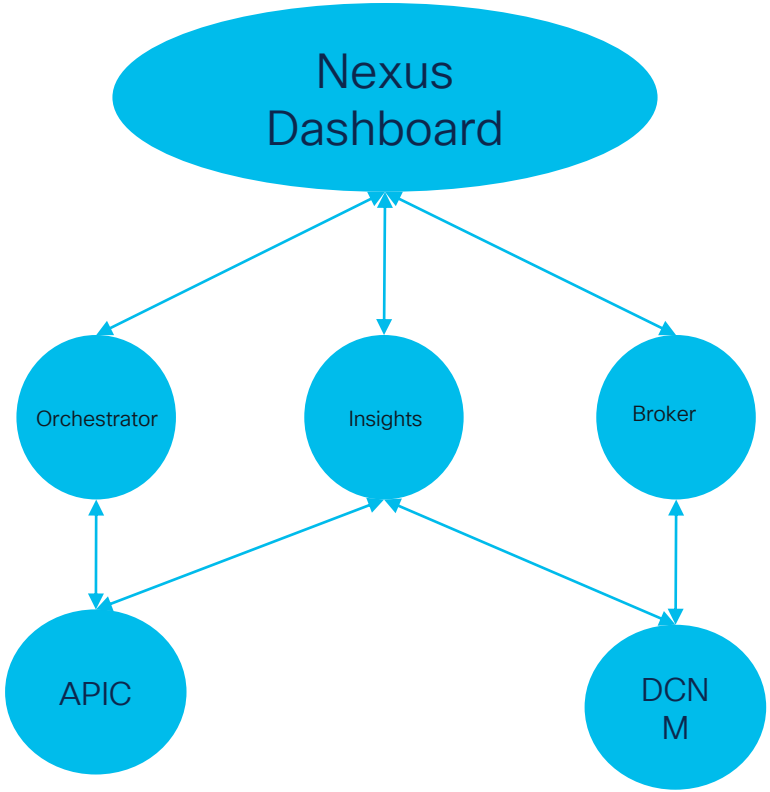
```
switch# show snapshots compare snapshot1 snapshot2 ipv4routes
metric                snapshot1    snapshot2     changed
# of routes           33           3             *
# of adjacencies      10           4             *

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)
```



Data center Fabric controllers

Unified Datacenter Controller views



#1 Benchmarking

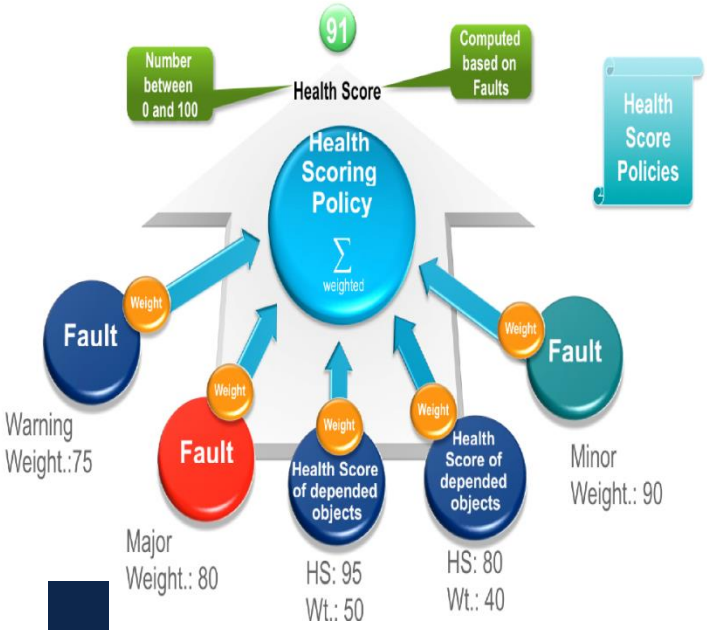
#2 Upgrade planning

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

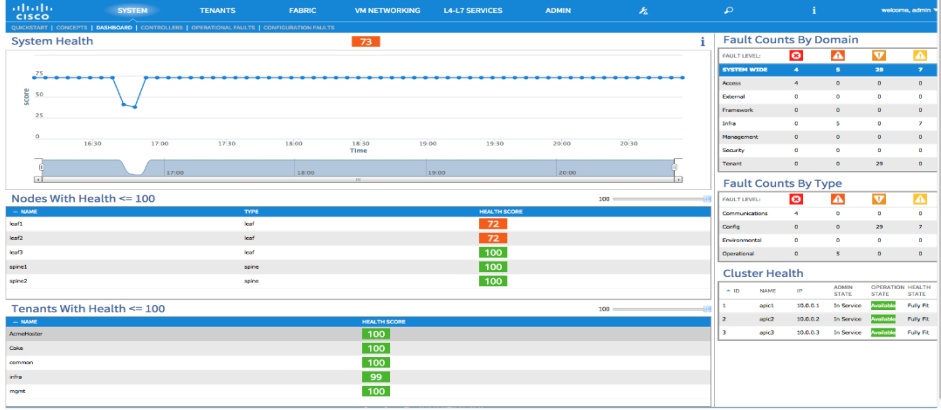
#3 Pre and Post Change window baselining

Moving forward DCNM can be application in Nexus Dashboard as an Application called Nexus Dashboard Fabric Controller

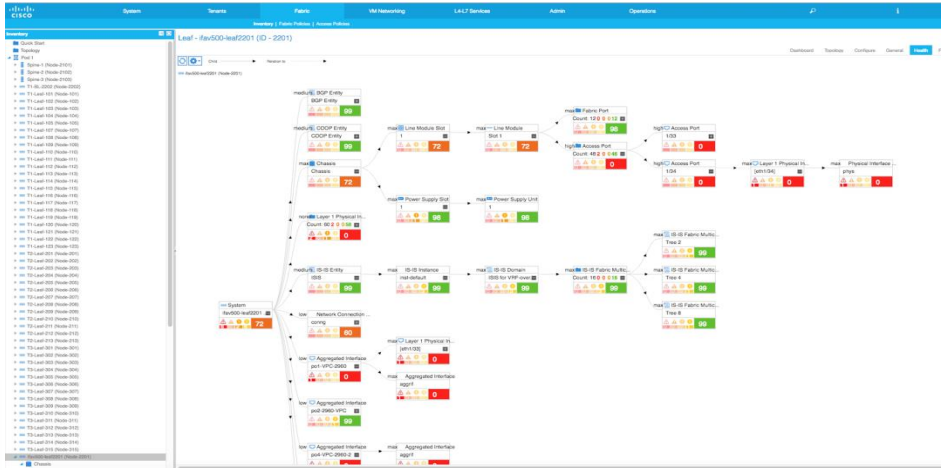
Health Score



Aggregated View



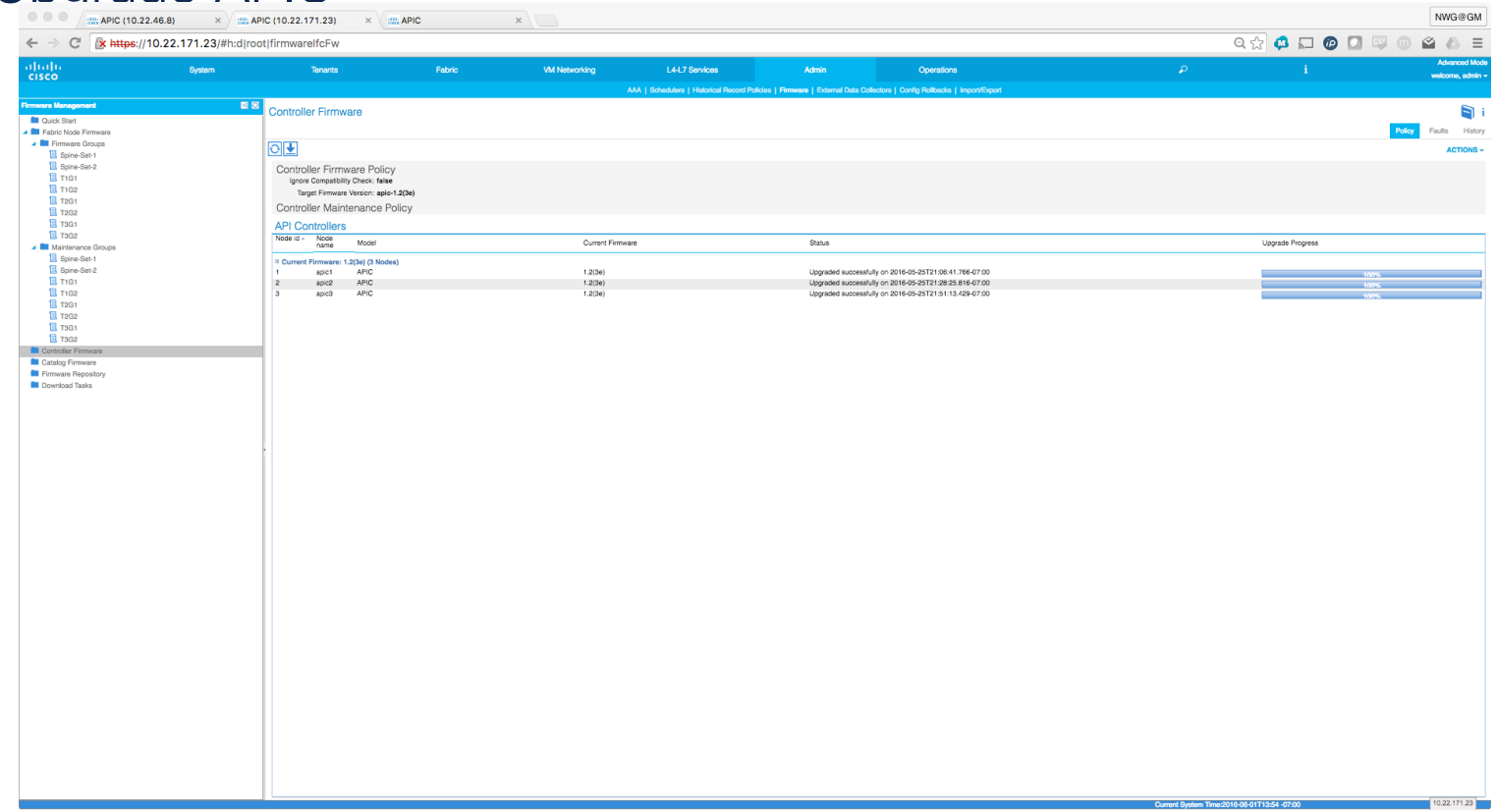
Fabric Topology View



Aggregation of system-wide health, including pod health scores, tenant health scores, system fault counts domain and type and the APIC cluster health state.

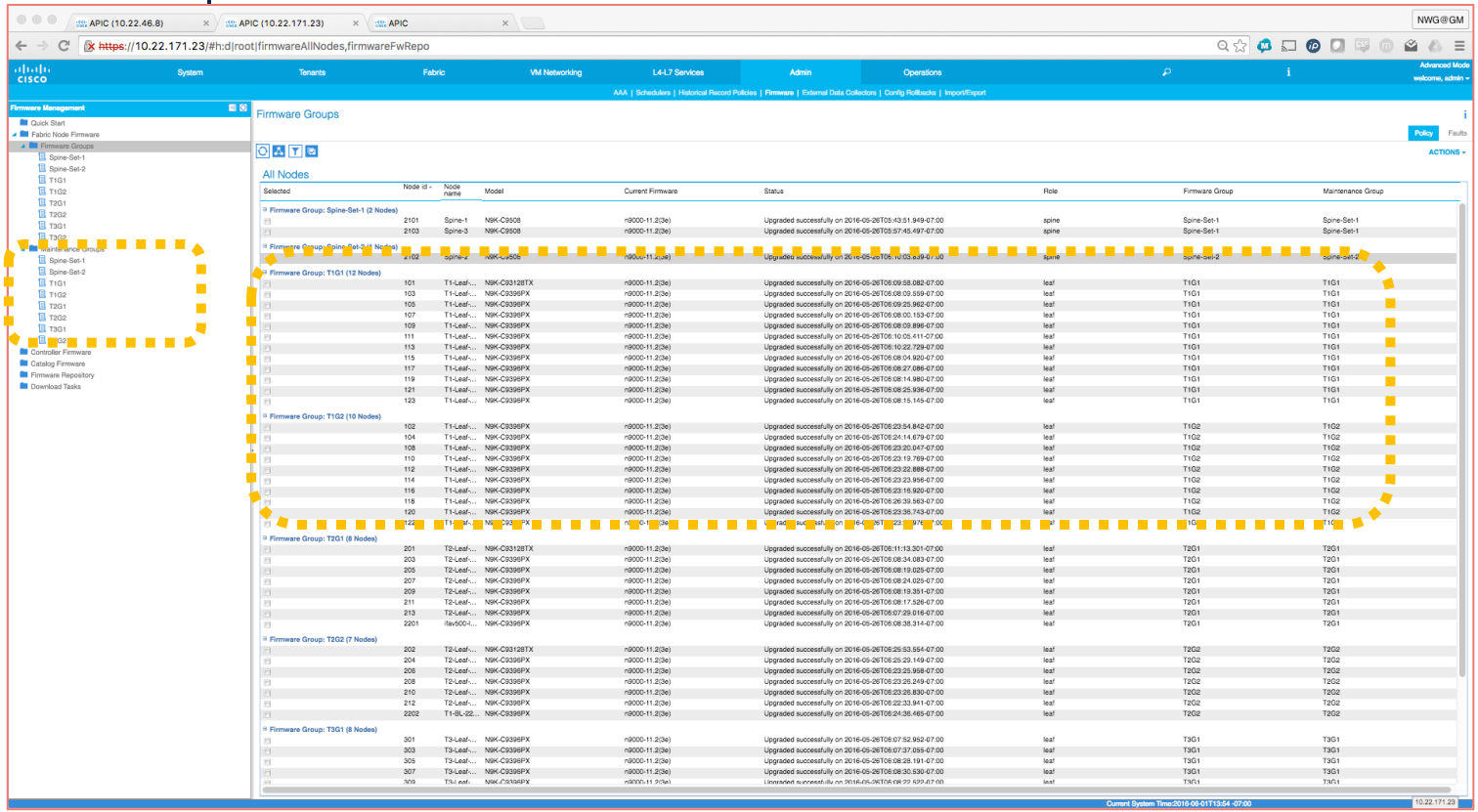
Maintenance Upgrade #1

Upgrade APIC

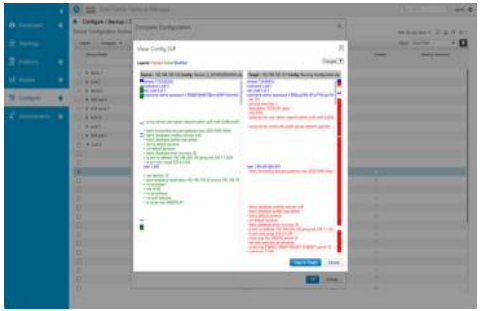


Maintenance Upgrade #2

Create Groups



Upgrade Using DCNM

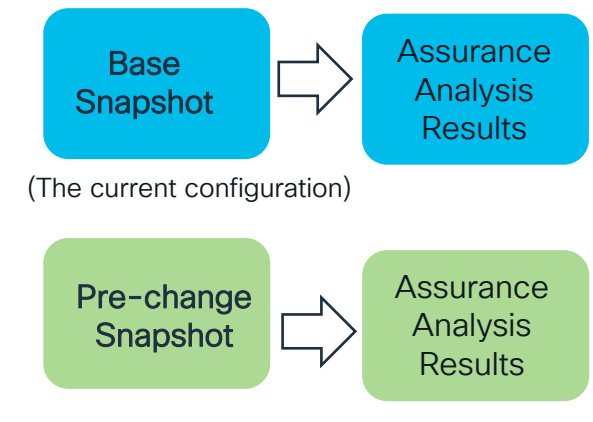


DCNM: Image, Config, Patch, GIR

DCNM will need to have this methodology planned manually in the template

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

Migration Best Practices

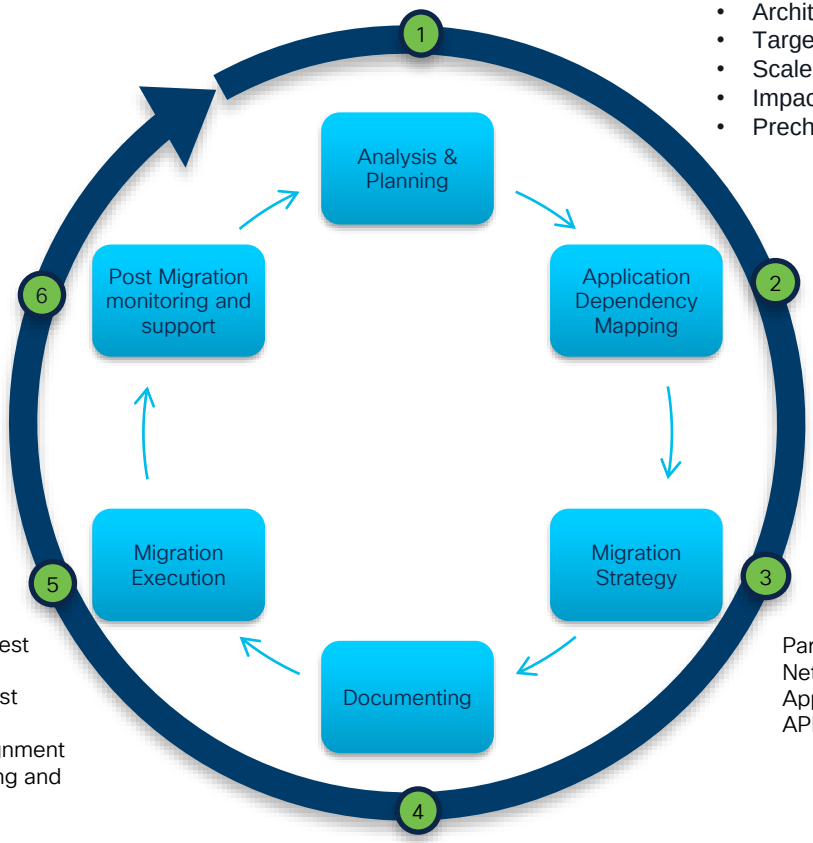
Datacenter Migration – Strategy and Approach

Source Architecture

Spanning Tree	Fabric Path
Vxlan	ACI

Destination Architecture

Vxlan
ACI



- 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

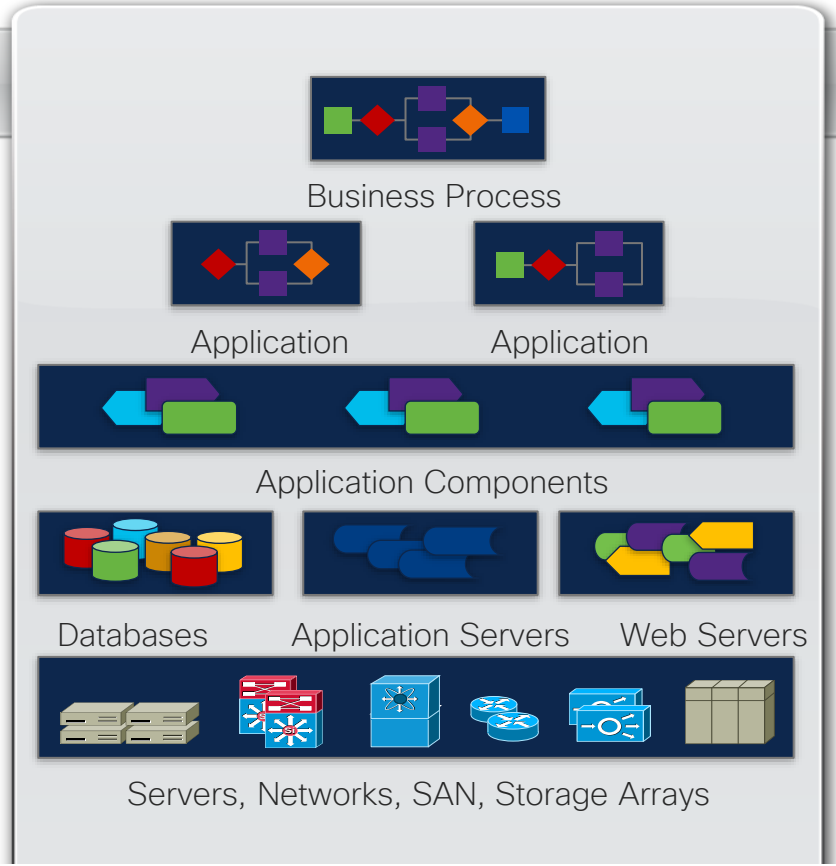
- Change Management Best practices
- SW and HW Platform best practices
- Go – No Go strategy alignment
- Validations before , during and after migration
- Reporting

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

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

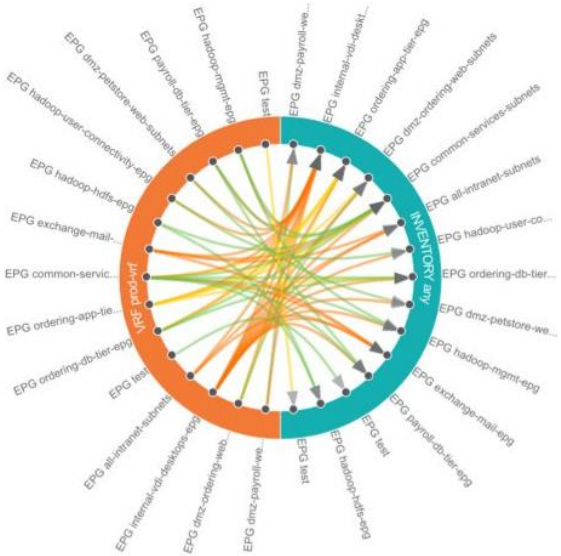


Datacenter Migration Scenarios and Considerations

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

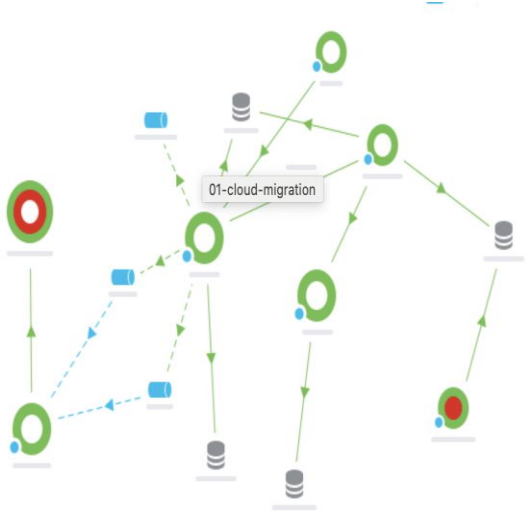
Visibility Considerations and Best Practices for Migration

Application dependency Mapping



Application Dependency Mapping

Application flow Map



Application Flow Mapping

1. Selecting Application for Migration

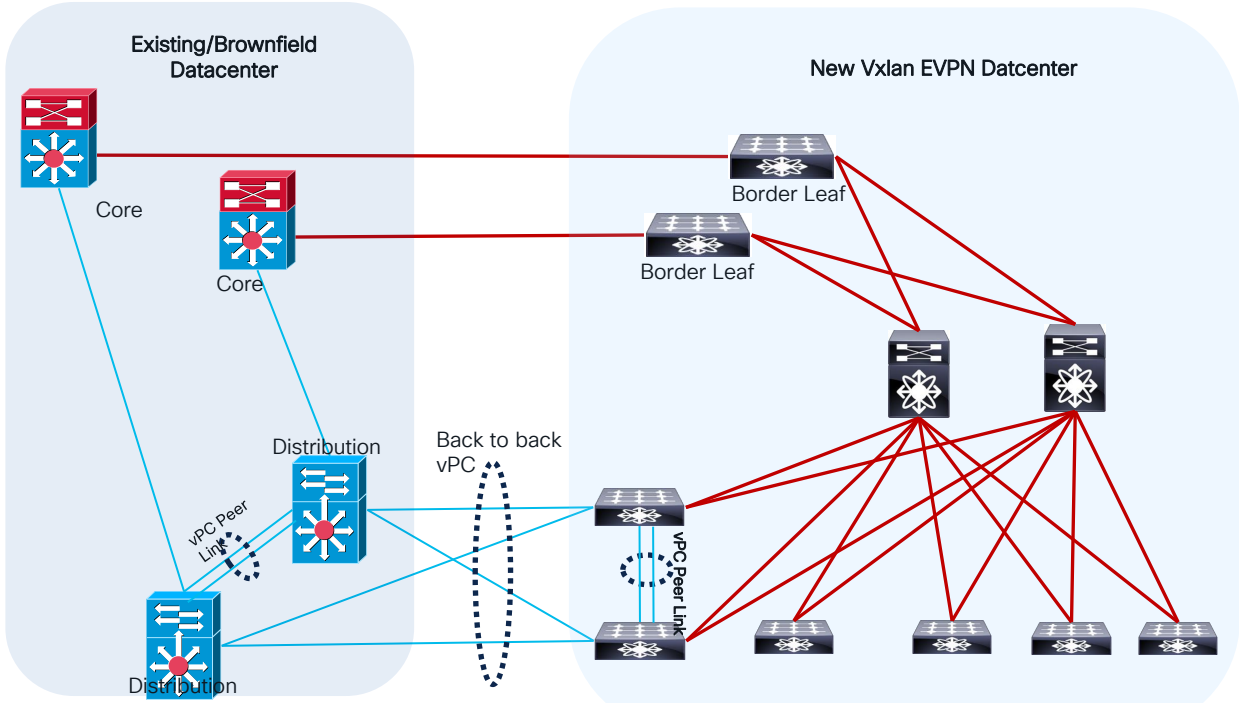
2. benchmark digital experience

3. review the following during Migrations
   a) Application performance monitoring
   b) Latency considerations
   c) Avoiding Suboptimal routing conditions

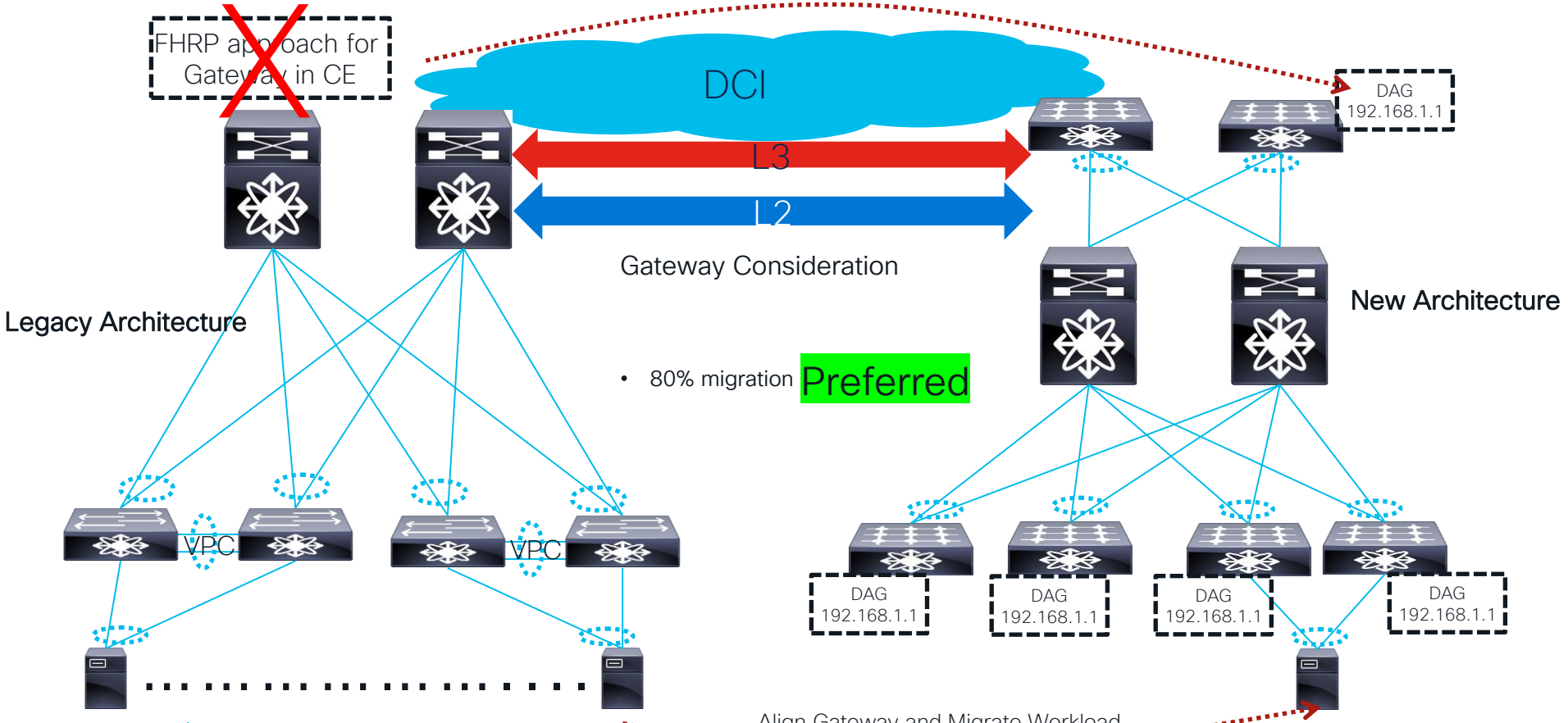
4. Application Performance Monitoring After the migration

Network Considerations for Datacenter Migration

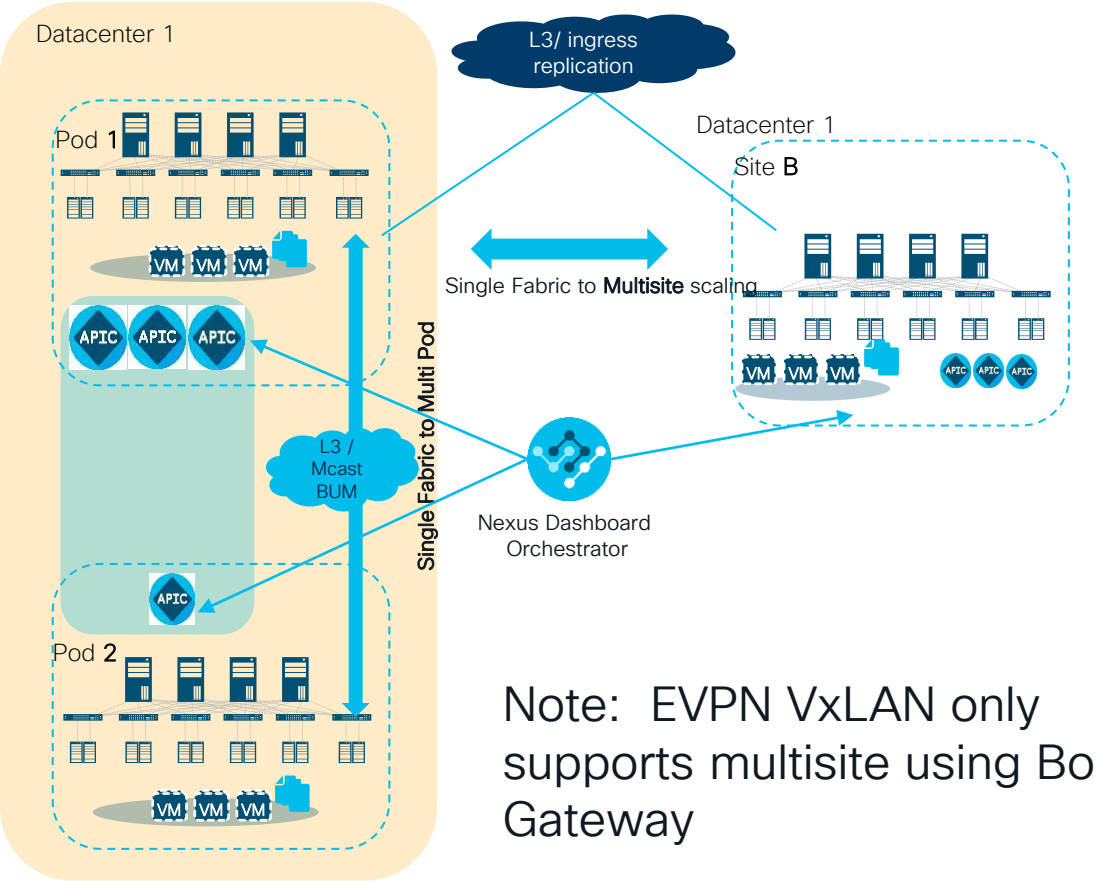
1	Migration Planning	Build a parallel vxlan fabric Establish L2 connection between legacy and new vxlan fabric Establish Dedicated L3 interconnect Between 2 fabrics
2	Layer 2 Considerati on	Dedicated Leaf for L2 Connection using double sided VPC STP Root bridge placement in the fabric
3	Layer 3 Considerati on	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



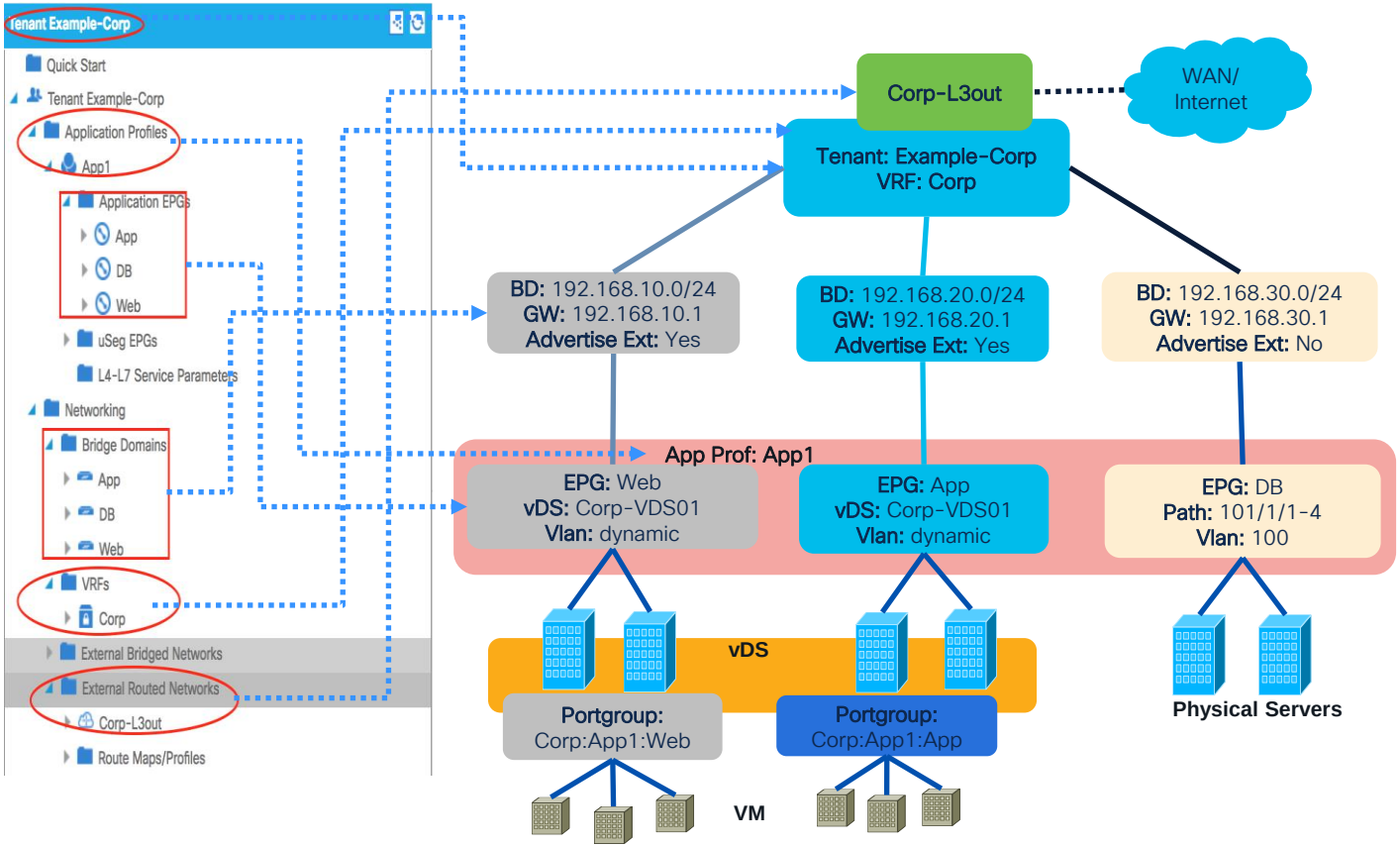
1. Scale Consideration in Data Center 1; options –
   - Multi Pod – same mgmt domain
   - Multi site – separate mgmt. domain
2. Multi-Pod Consideration
   - Extension of APIC cluster- no new policy consideration
   - Special emphasis on the underlay BUM (Mcast support)
3. Multi-site consideration for 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

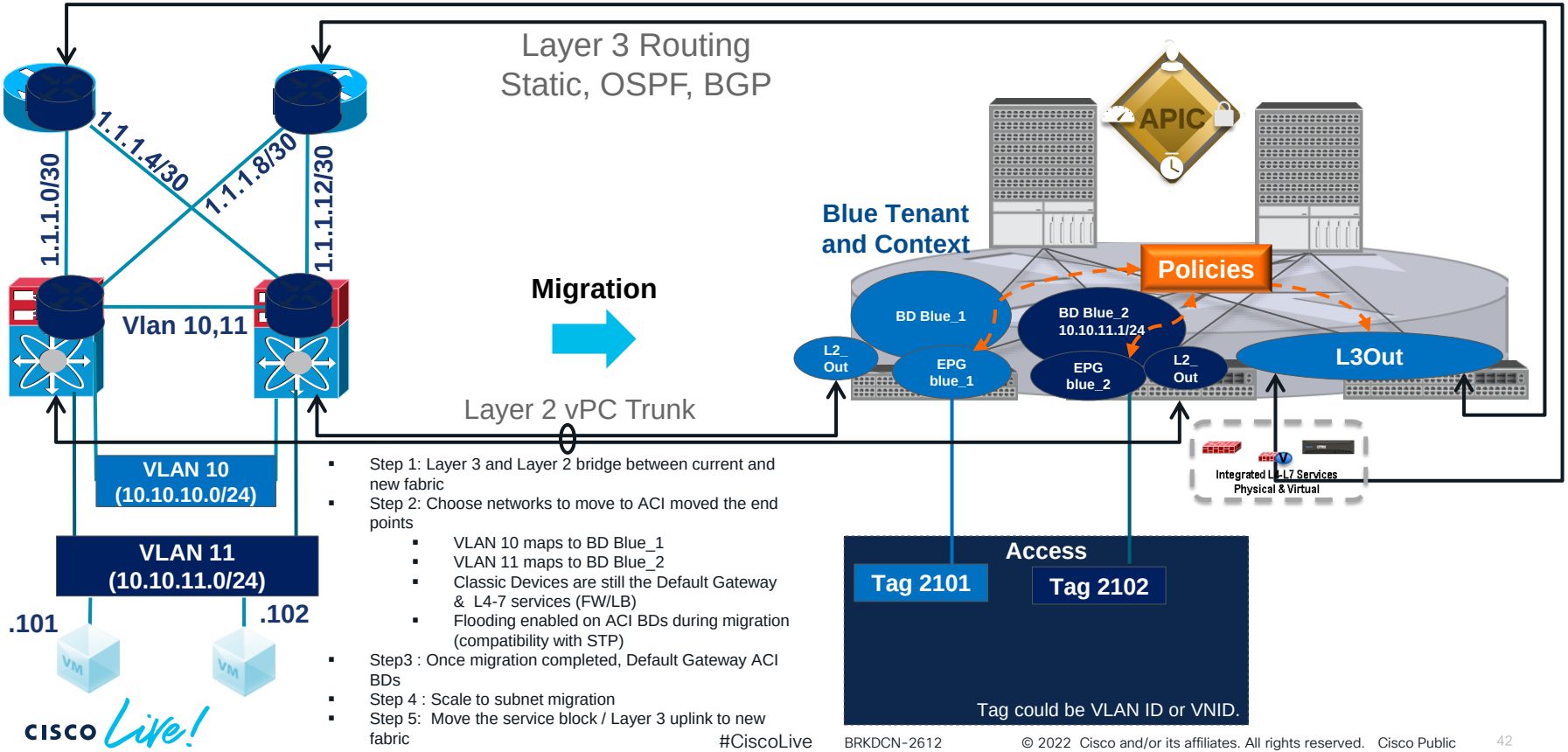
ACI Network Centric Deployment

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



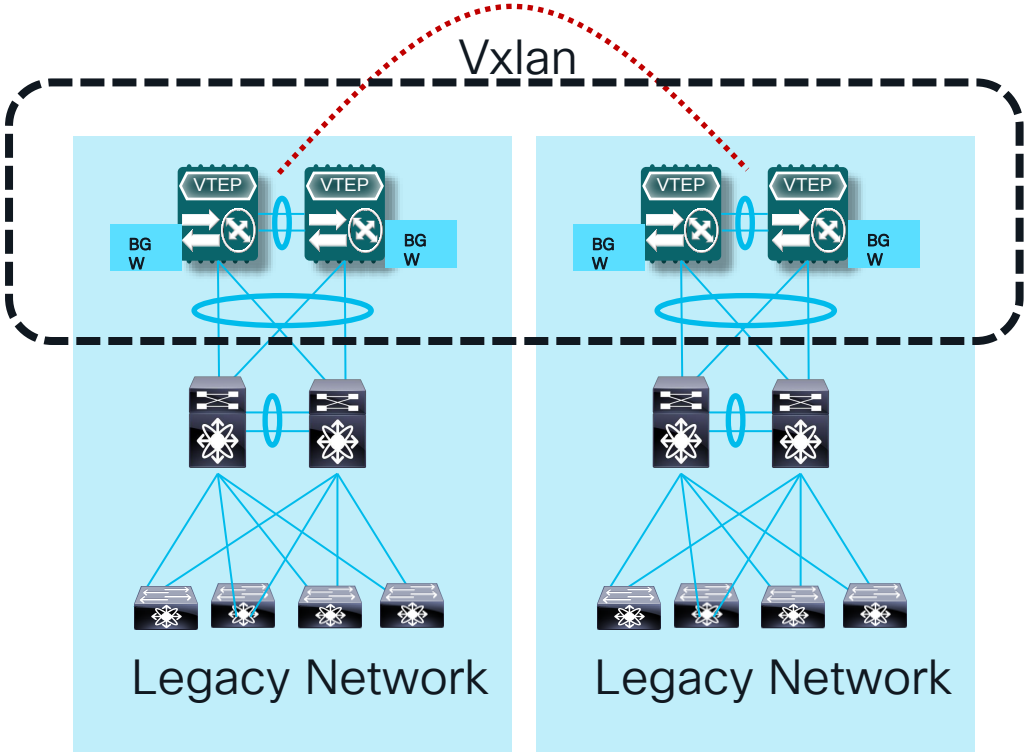
ACI Migration Example



- Step 1: Layer 3 and Layer 2 bridge between current and new fabric
- Step 2: Choose networks to move to ACI moved the end points
  - VLAN 10 maps to BD Blue_1
  - VLAN 11 maps to BD Blue_2
  - Classic Devices are still the Default Gateway & L4-7 services (FW/LB)
  - Flooding enabled on ACI BDs during migration (compatibility with STP)
- Step3 : Once migration completed, Default Gateway ACI BDs
- Step 4 : Scale to subnet migration
- Step 5: Move the service block / Layer 3 uplink to new fabric

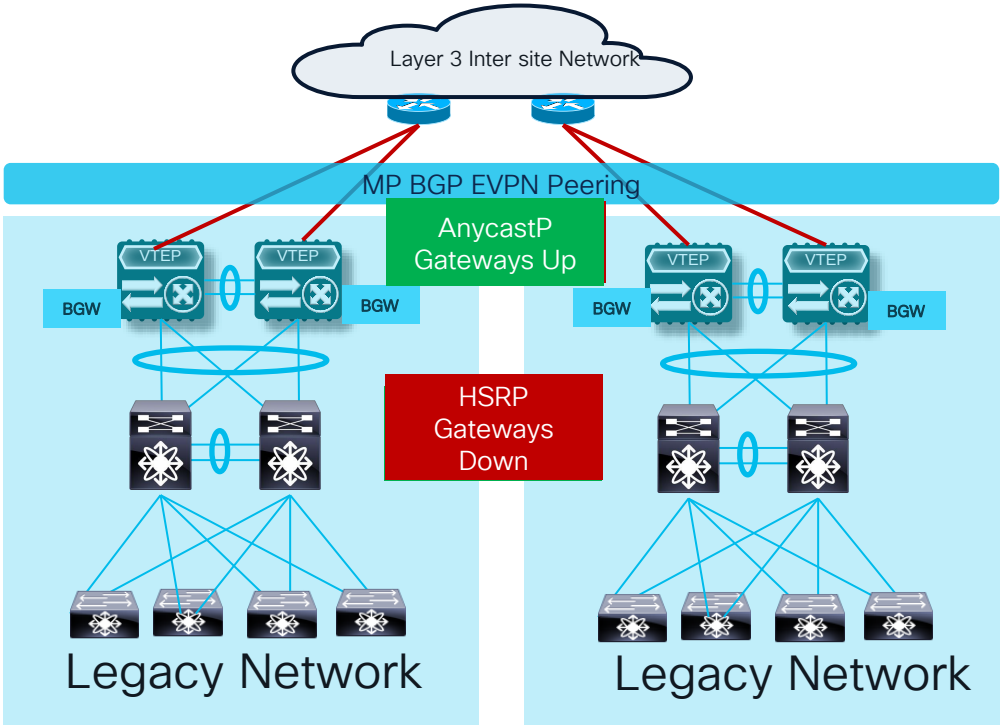
Network Interconnectivity using VXLAN EVPN Border Gateway

- 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
- Key technical features
  - Fault Containment: BGW provides EVPN Multicast Storm Control
  - Transport Agnostic - Vxlan tunnel built over any IP connectivity
  - Multihoming and Multipath Load sharing



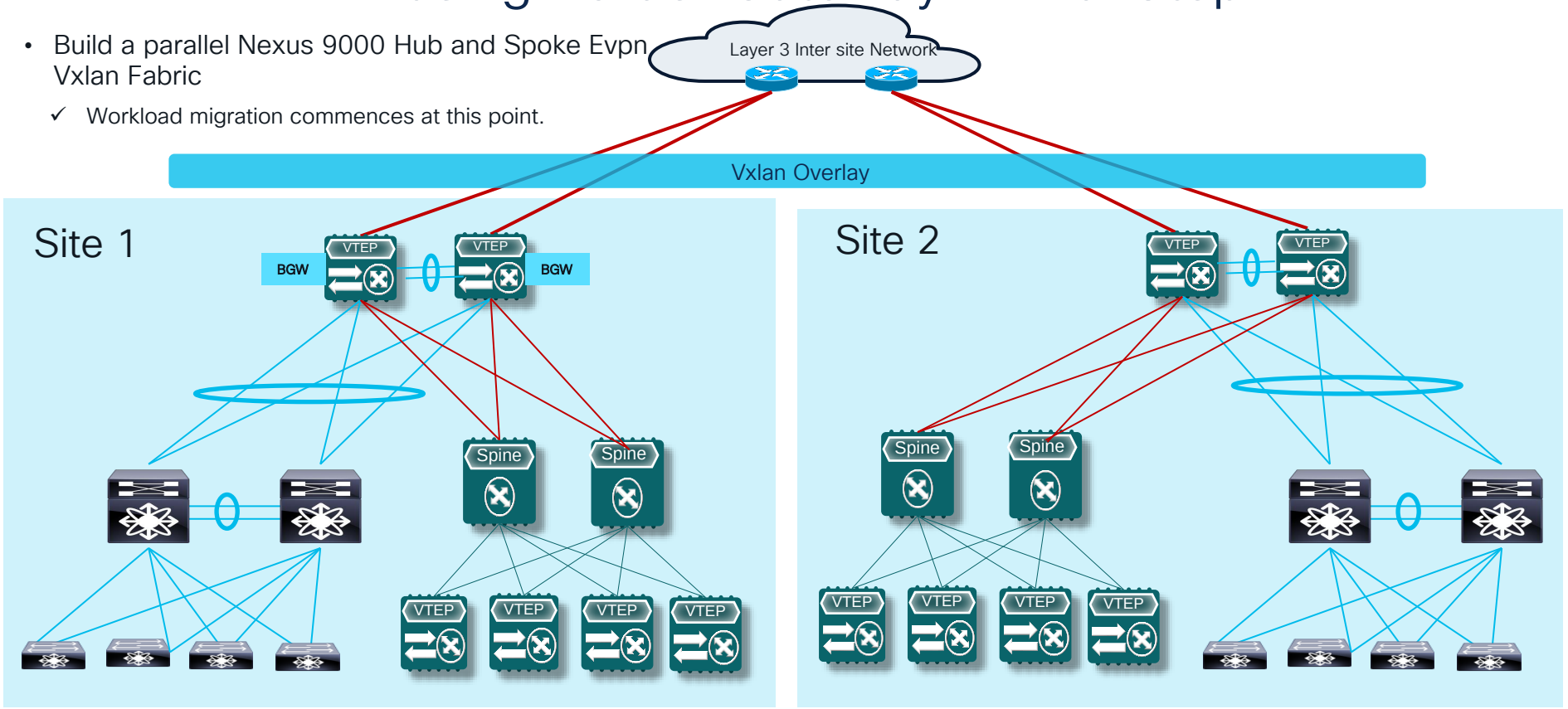
Legacy Network to VXLAN EVPN Migration using Border Gateway

- 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
- Bringh up vPC BGW Underlay network
  - ✓ Route opeering 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 nides 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.

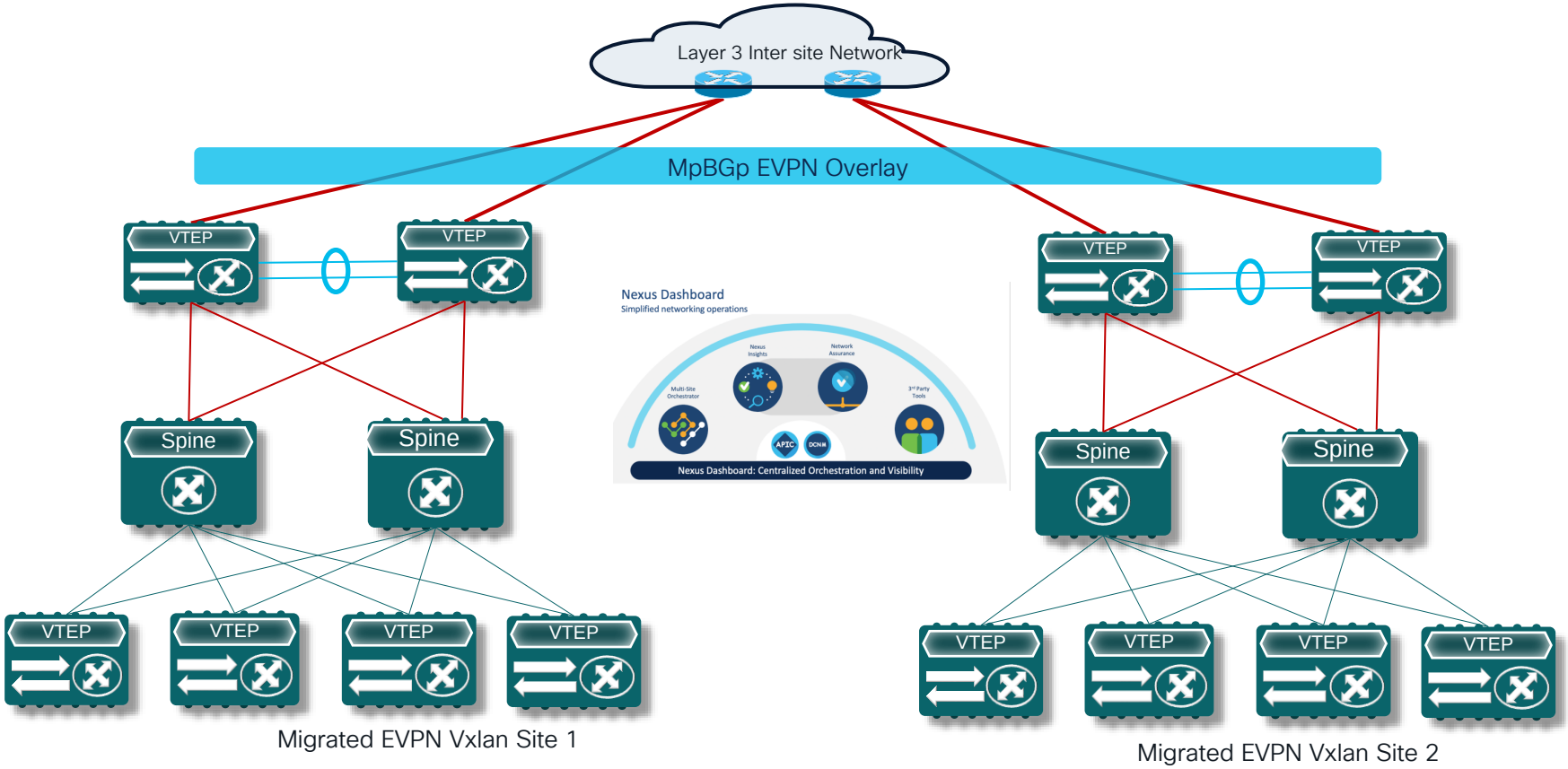


Transition Legacy Network to VXLAN EVPN using Border Gateway – Final Step

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



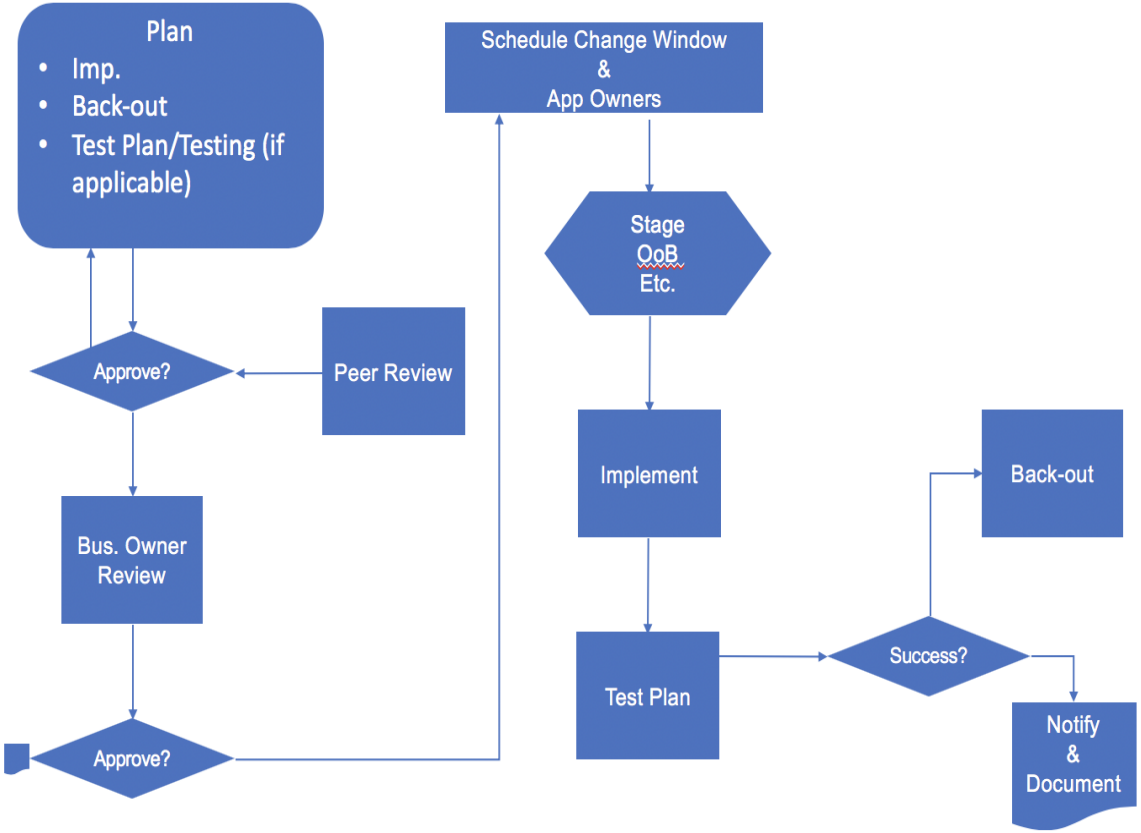
Legacy Network to VXLAN EVPN Migration using Border Gateway



Change Management

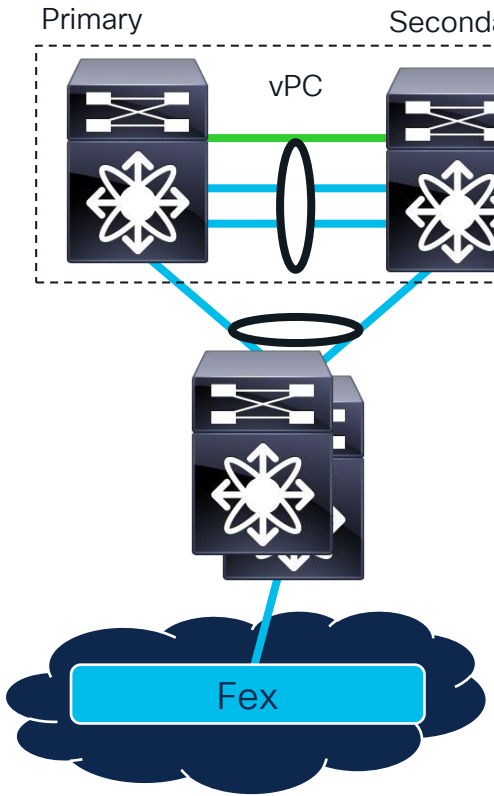
Maintenance Windows – Golden Rules

- 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

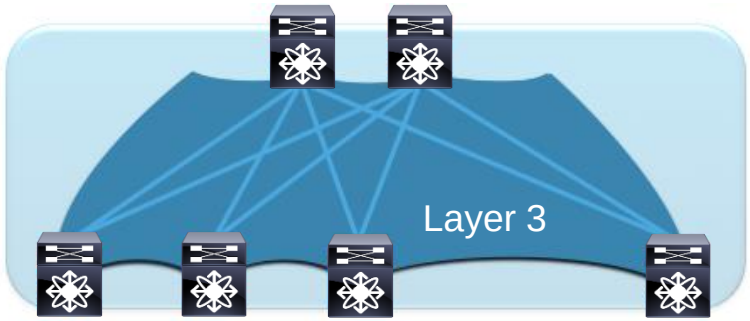
1. Layer 2 Isolation
   - VPC
2. Interface Isolation
   1. Fex-fabric (include/exclude)
   2. Dual-attached FEX Procedure * Recommended

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

Summary

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**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN