

Nexus One: An Architecture for Your Cisco Datacenter of Tomorrow

CISCO Live !

Max Ardica
Distinguished TME



Session ID: BRKDCN-2602

Cisco Webex App

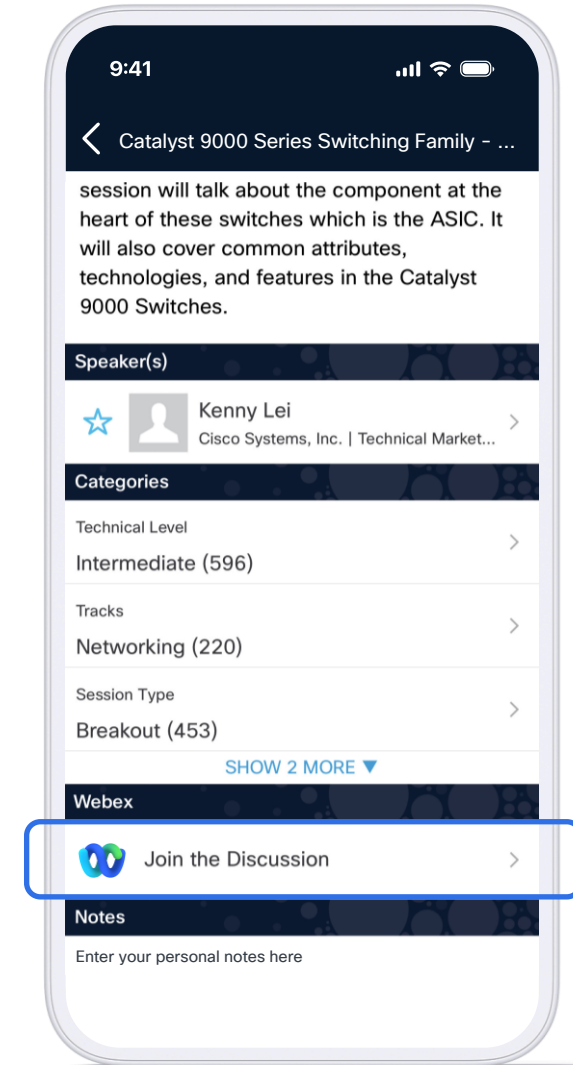
Questions?

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

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://cislive.ciscoevents.com/cislivebot/#BRKDCN-2602>

Agenda

01 DC Design Evolution

- From a Single Fabric to a Distributed Architecture

02 Cisco Distributed DC Architectures

03 Nexus One Architecture

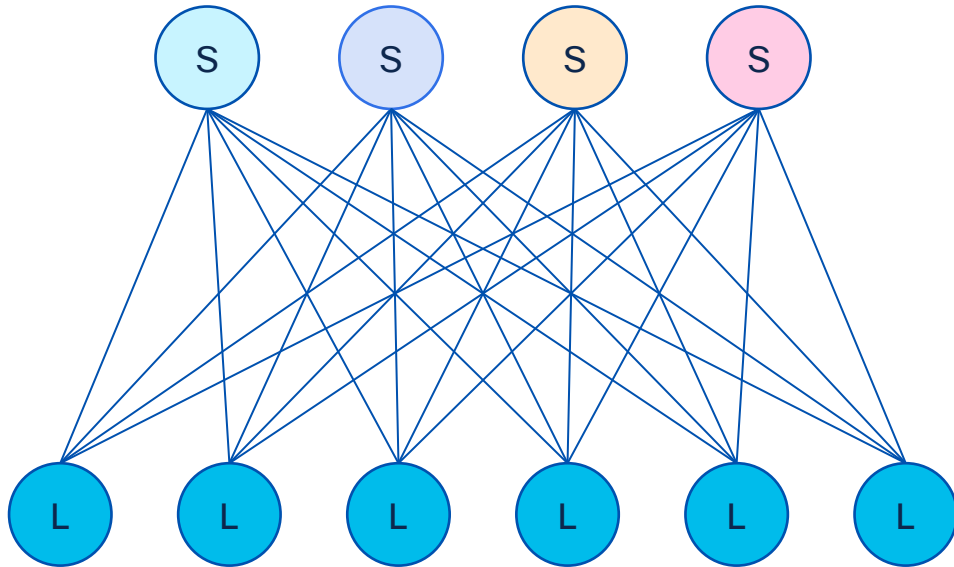
- Group Policy Option (GPO)
- ACI BGWs
- Unified Nexus Dashboard



DC Design Evolution

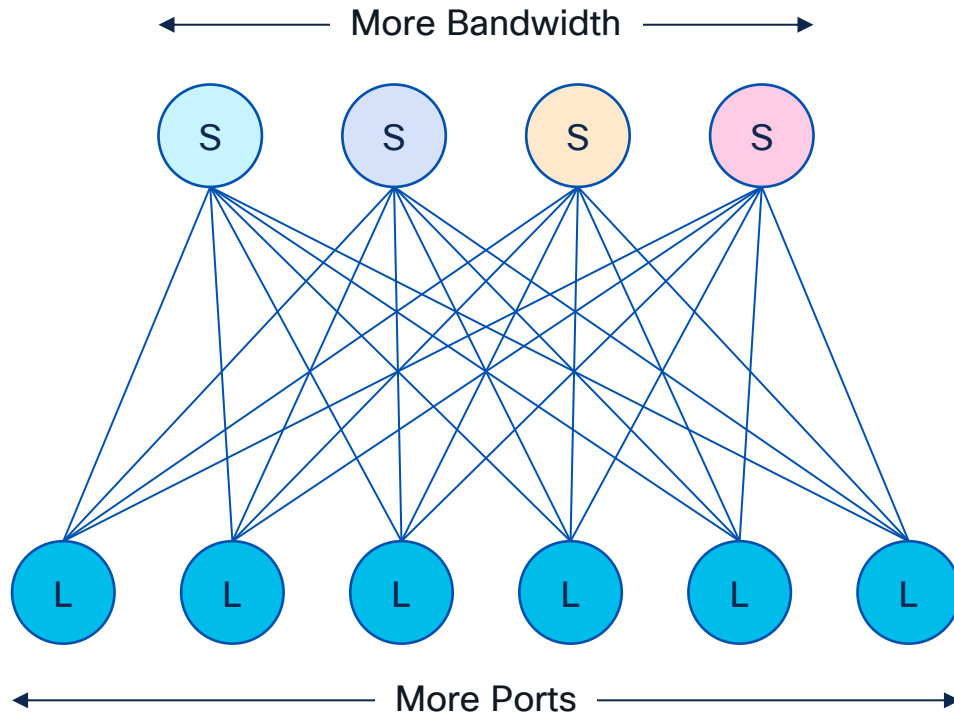
From a Single Fabric to a Distributed Architecture

Leaf and Spine Topology



- A Leaf and Spine Topology
- Variations or Names of the same:
 - Fat Tree
 - Folded Clos
 - 3 Stage Clos
 - 2 Tier Network

Leaf and Spine Topology



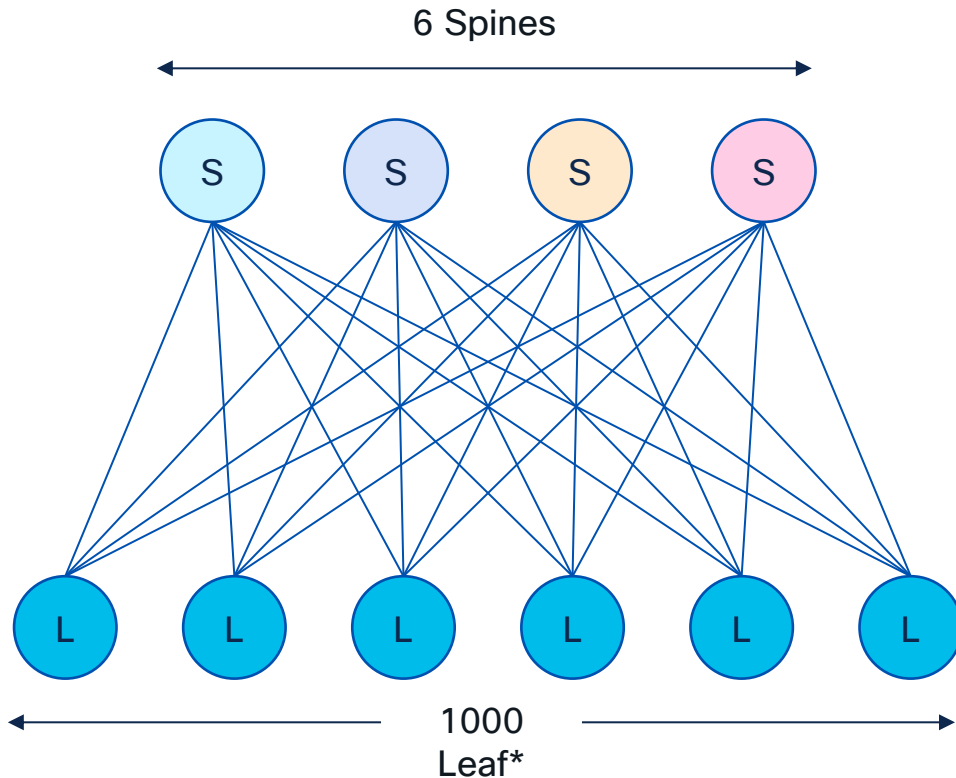
- A Scale Out Architecture
 - More Leaf = More Ports
 - More Spine = More Bandwidth

How large should I build a
leaf-spine fabric topology?



Data Center Design Evolution

Various Considerations to Reduce the Fabric's Size



*Supported in an NX-OS VXLAN EVPN fabric

- What is my Failure Domain?
- What is my Change Domain?
- What is my Overall Scale?
- What is my Fabric Solution Scale?
- What is my Fabric SLA?
- What is my Maximum Downtime?

What Have we Learned from the Cloud Titans?

Building Scalable Data Center Networks

#1

Simplicity is Key
Simple Design Principals

#2

Scale as you Go
Scale is Never Finite

#3

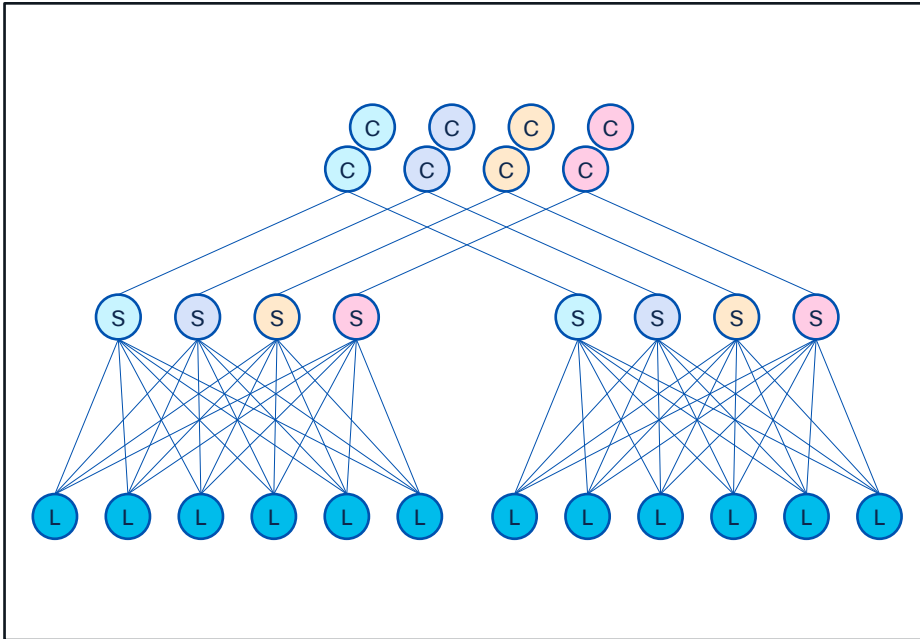
Fail but Fail Fast
Reduce Brown-Out Exposure

#4

Redundant and Repeatable
Risk is Never an Option

Design Evolution

Building a Distributed Architecture



3 Tier Leaf-Spine-Core (or Super-Spine)

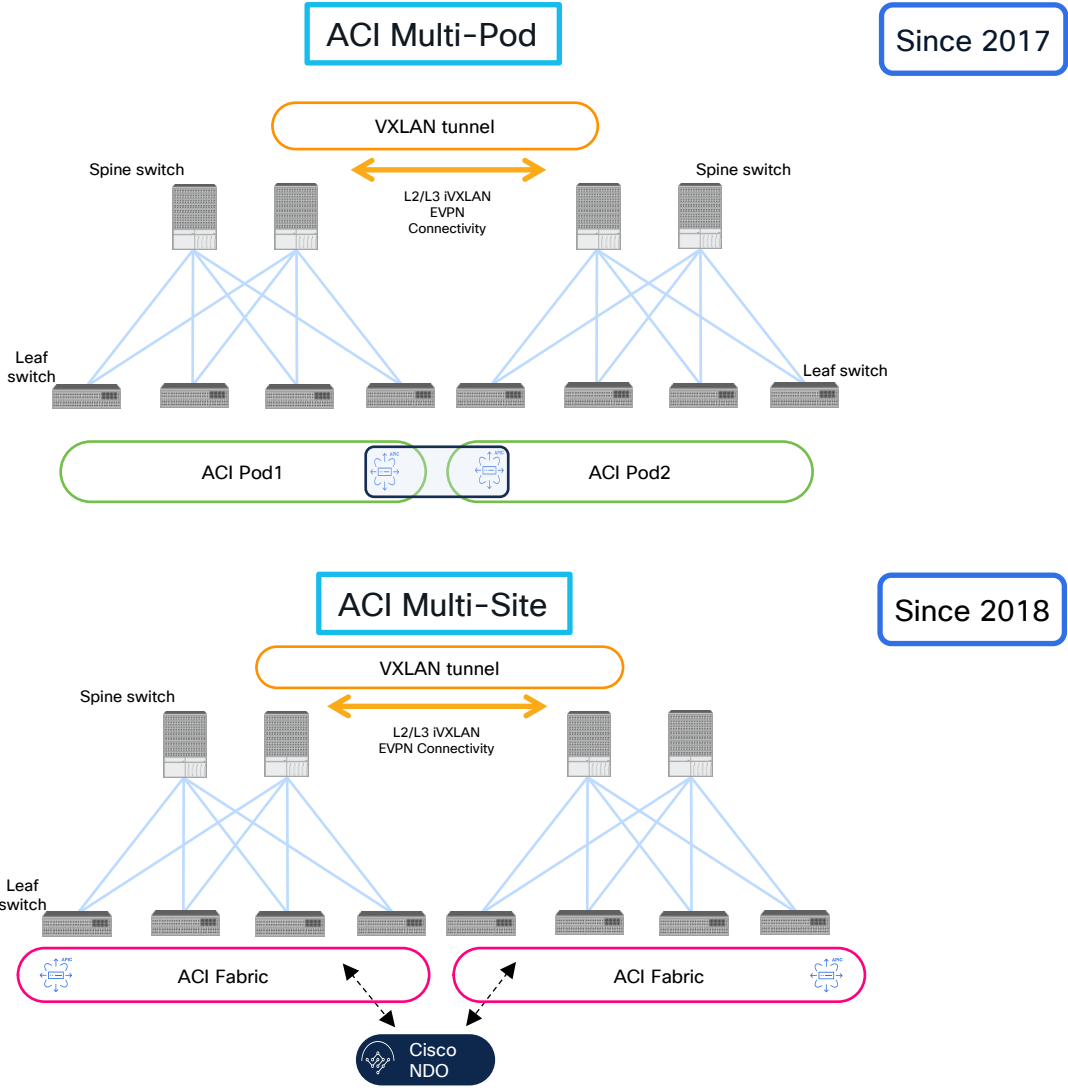
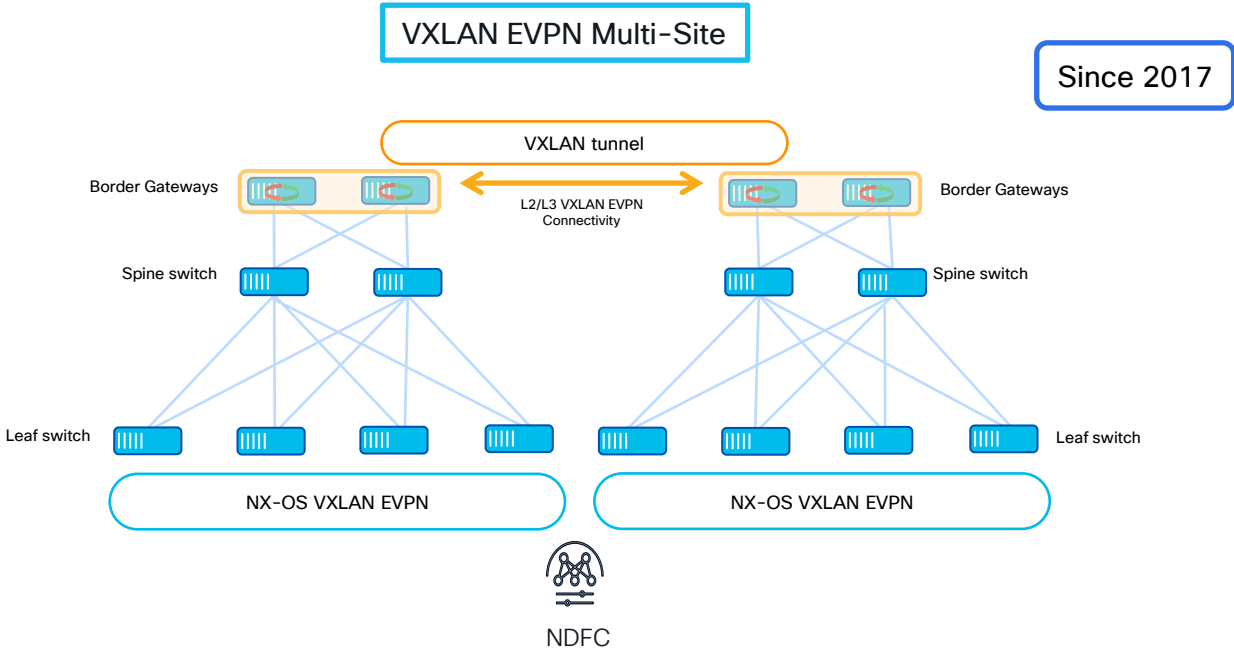
- Increasing Scale-Out in all Tiers
- Reducing Complexity
- Simple Design Principles
- Increasing the “Finite Scale”
- Scale as You Go
- Disaggregated Redundancy
- Flexible Link and Bandwidth Distribution
- Favor the use of non modular platforms in every tier

For More Information on Multi-Tier Fabric Deployments refer to BRKDCN-2999 from Cisco Live San Diego 2025:
<https://www.ciscolive.com/on-demand/on-demand-library.html?search=marina%20ferreira#/session/1750271892264001zRcH>

Cisco Distributed DC Architectures

Building Distributed DC Architectures

Homogeneous Options

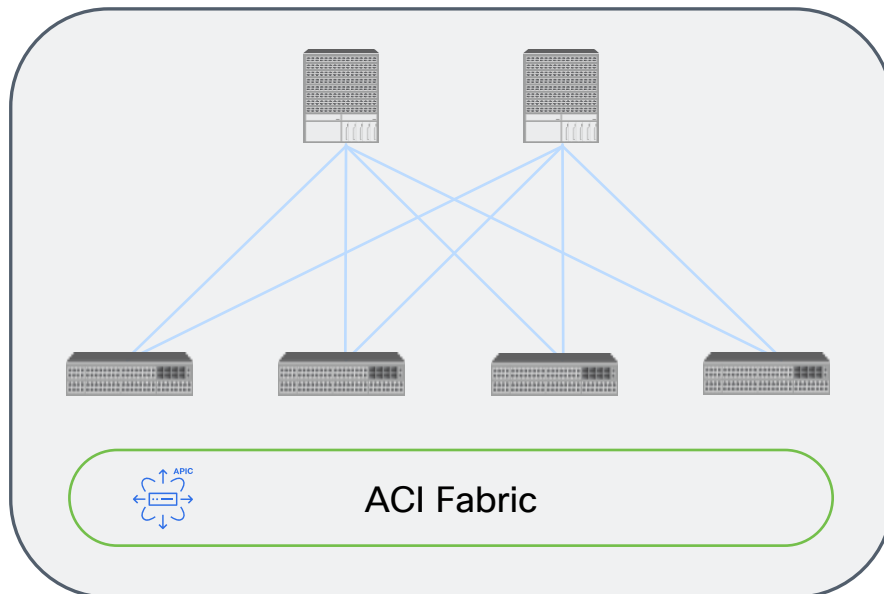
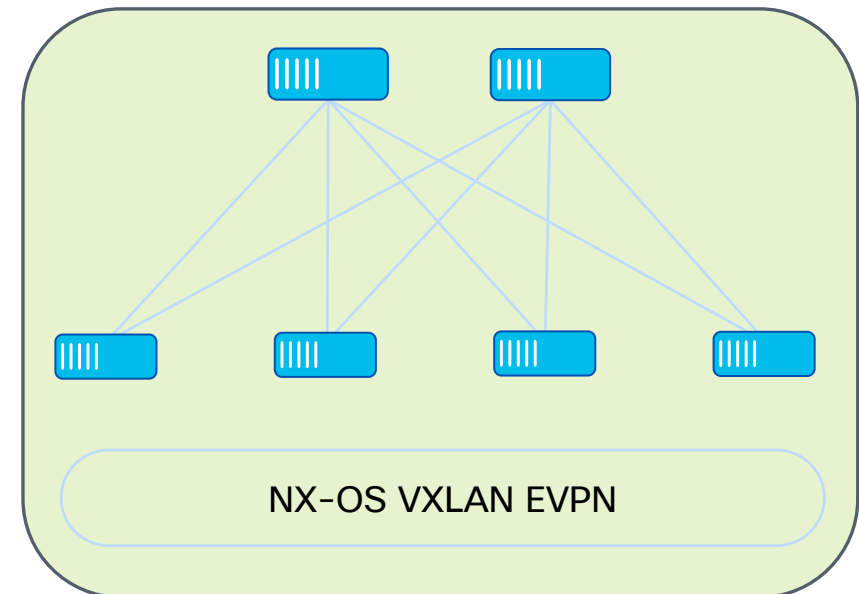


Introducing Cisco Nexus One Architecture

Cisco Nexus One Architecture

Cisco ACI and Cisco NX-OS Fabrics

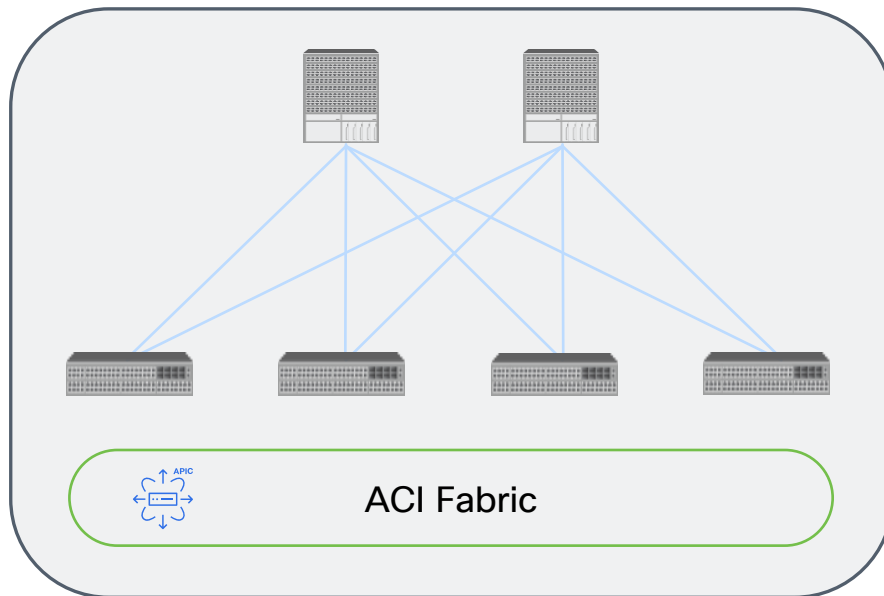
Customers can choose one or more Cisco technologies for their DC network



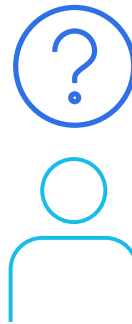
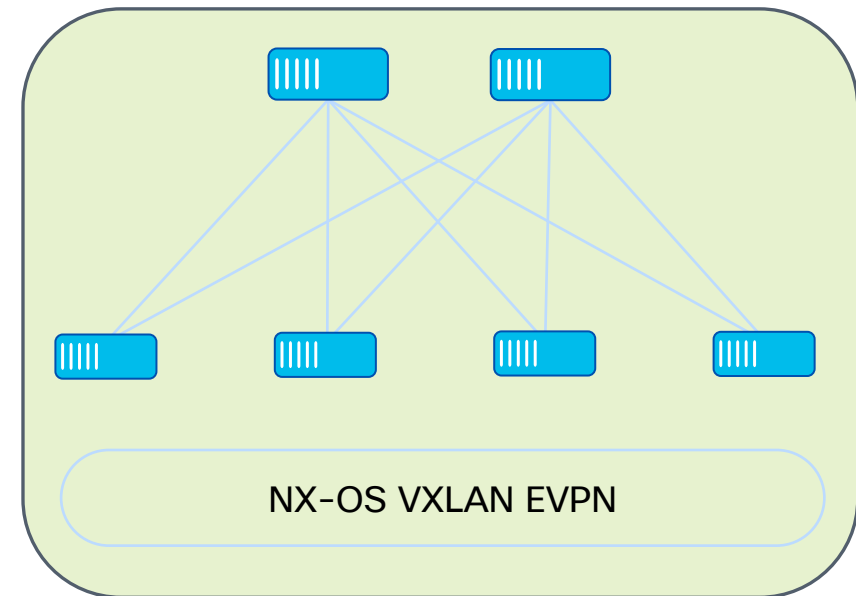
Cisco Nexus One Architecture

The Challenges with Interconnecting Heterogeneous Fabrics

Customers can choose one or more Cisco technologies for their DC network



DCI?
VRF/BD Stretch?
VM Mobility?
Security?
Management?



What is Cisco Nexus One Fabric Experience?

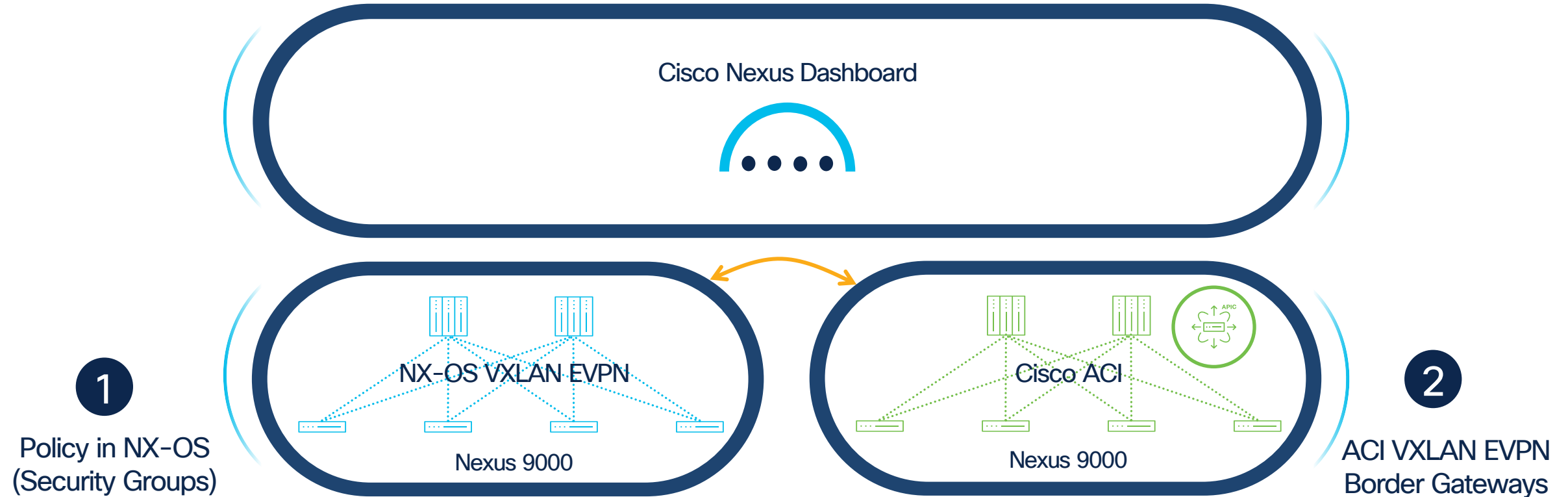
Open Networking Fabric Experience

Evolve multiple DCN fabrics into a **single user experience** to deliver consistent use cases

Nexus One Architecture

Functional Components

3 Cisco Nexus Dashboard as single point of control and operations



Different fabric architectures

Same outcome with common experience

VXLAN GPO

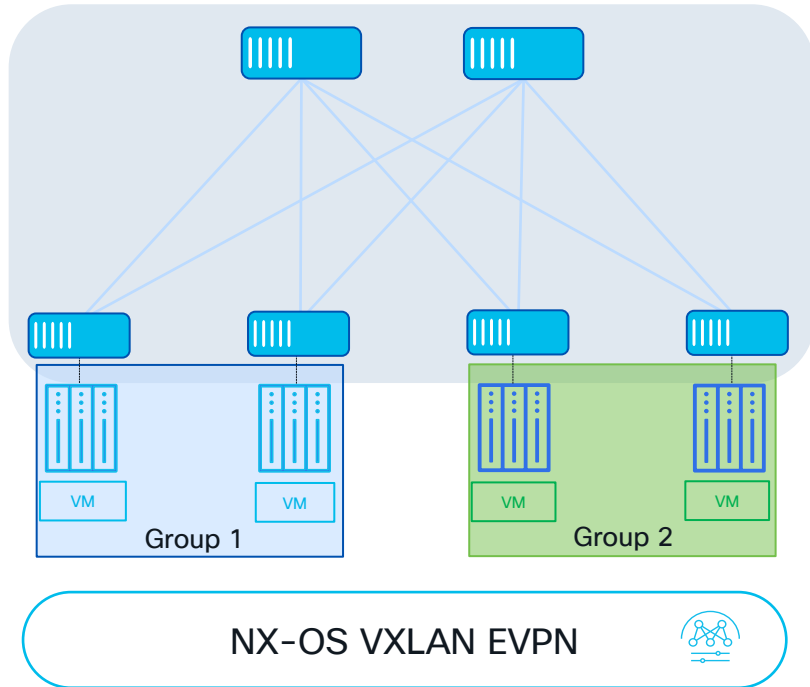
For More Information on VXLAN GPO:

BRKDCN-2609: Automating Micro-Segmentation and Deploying Layer 4-7 Services in VXLAN
EVPN Fabrics using Group Policy Option (GPO) and Nexus Dashboard

Thursday November 13th at 10.30 am

For Additional Information on VXLAN GPO please refer to BRKDCN-2633 from Cisco Live San Diego 2025:
<https://www.ciscolive.com/on-demand/on-demand-library.html?search=ardica#/session/1750271884651001zqS7>

VXLAN GPO with NX-OS



VXLAN GPO with NX-OS

- Group Policy Object carried in standard VXLAN header
- BGP Extended Community to advertise policy information on EVPN control plane advertisements
- Decoupling network connectivity and security

Grouping

- Classify endpoints to create security groups
- Based on IP, VLAN, VM attributes, etc. across VRFs

Policy enforcement

- Create contracts/SGACLs between Endpoint Security Groups (ESGs*)
- Possible actions: permit, deny, redirect (service chaining)

Automation

- Automate using [Nexus Dashboard \(ND\)](#) or [Open APIs](#)

Benefits

Segment East-West traffic

Flexible security isolation

Reduce attack surface

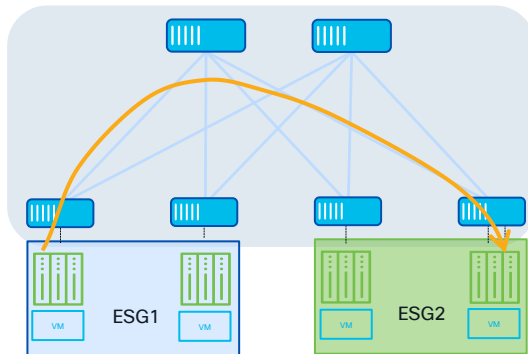
Automate your way

VXLAN GPO with NX-OS

Creation of Security Zones and Service Chaining

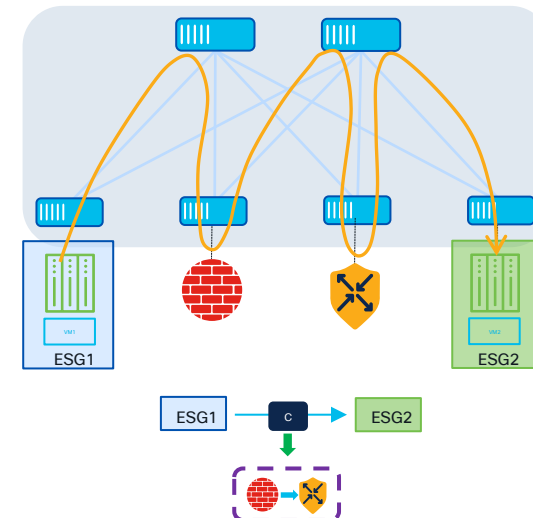
Creation of Security Zones

- VXLAN GPO allows to define policies for enforcing security policies (SGACLs) between endpoint security groups (ESGs)
- SGACLs are a simpler, more flexible and more scalable policy enforcement mechanism compared to traditional ACLs
- Provides better control over the flow of network traffic (both east-west and north-south)



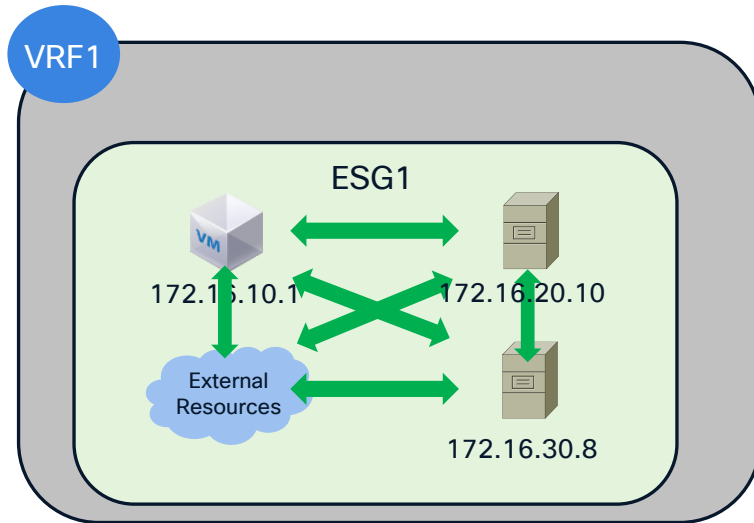
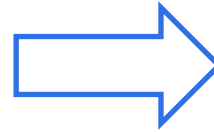
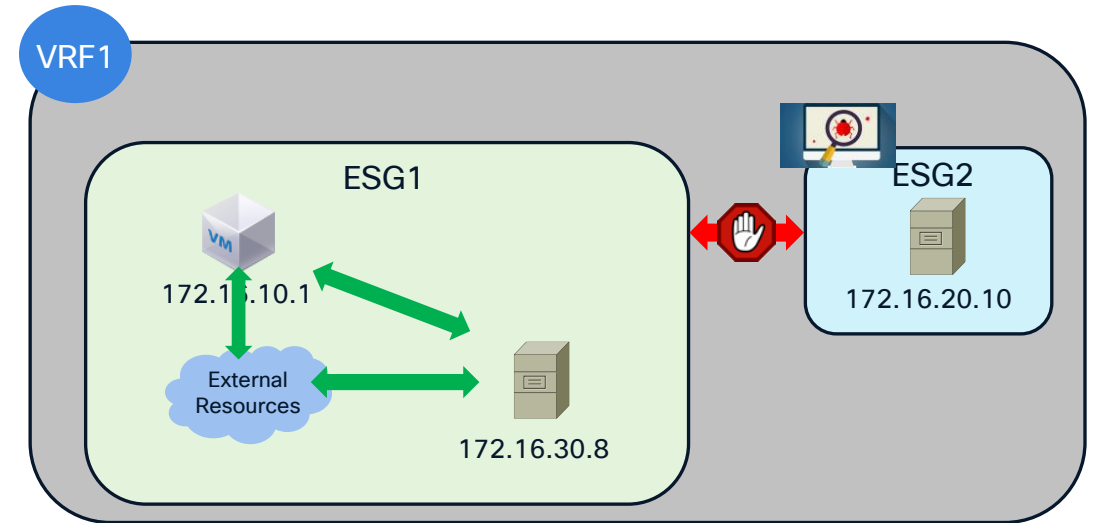
Service Chaining

- VXLAN GPO can be used to insert network services into a packet flow based on specific policy criteria
- Service chaining steers flows through the appropriate network services functions (such as firewalls, load balancers, or intrusion detection systems)



VXLAN GPO with NX-OS

Use Case - VRF as a Security Zone

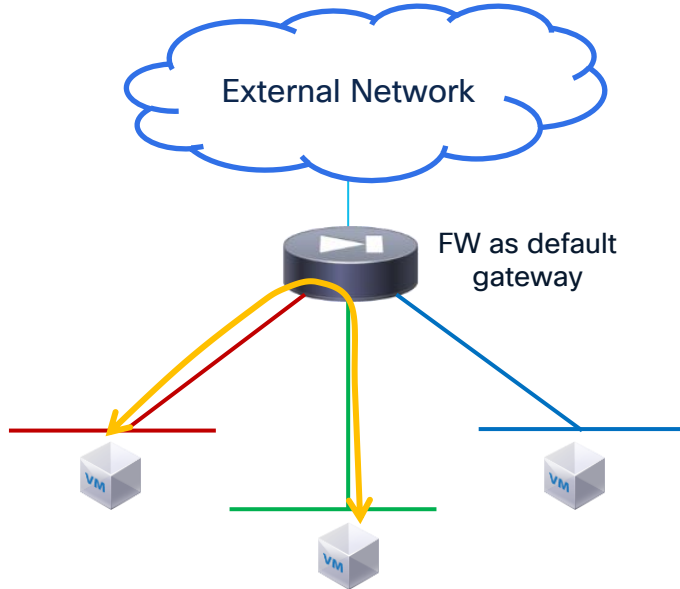
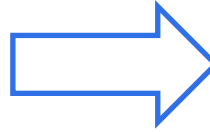


- Creation of a single security group to classify endpoints connected to all the networks (internal and external) part of the same VRF
- Provides intra-VRF open connectivity

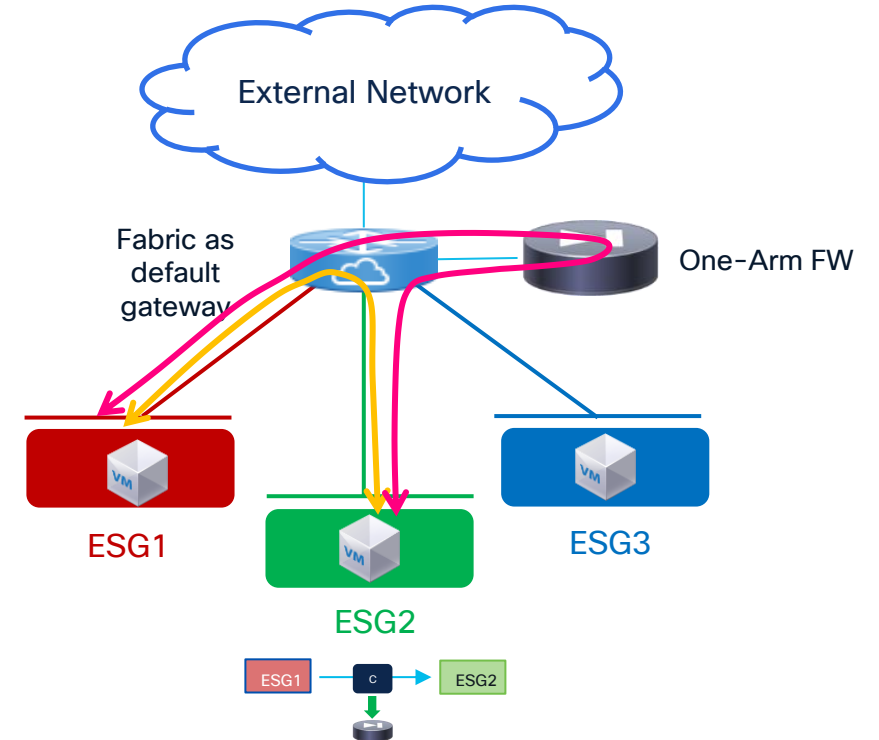
- Easy way to segment out specific endpoints that needs to get isolated (for example because they got compromised)

VXLAN GPO with NX-OS

Use Case - Subnet as a Security Zone



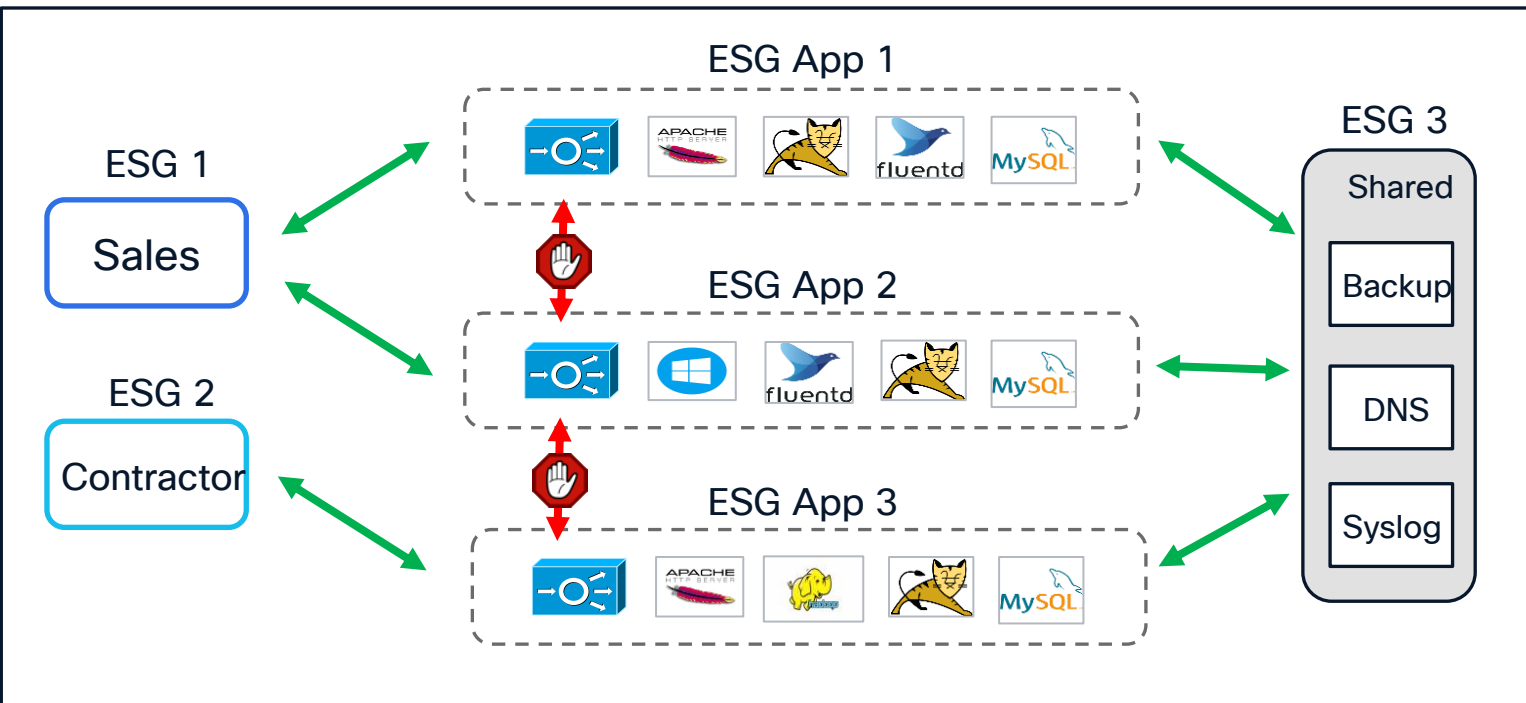
- Traditional design requires the deployment of a firewall as default gateway
- All inter-subnet flows are forced through the firewall, which may become a bottleneck



- Moving the default gateway function on the fabric
- Defining a separate ESG per subnet
- Redirect selective inter-subnet traffic flows only through the firewall, enforce policy or simply route at the fabric level for the rest of the flows

VXLAN GPO with NX-OS

Use Case - Application as a Security Zone

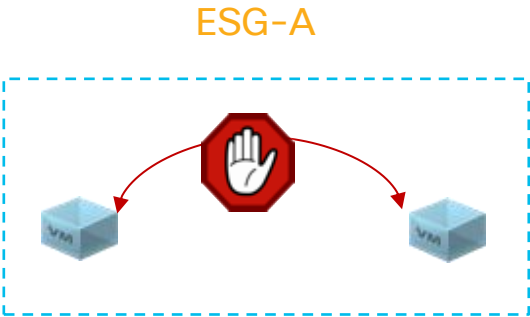


- Application as a security zone
- Does not require to know how the various components of the same application interact with each other
- Control communication between users and app, app to app and app to shared services

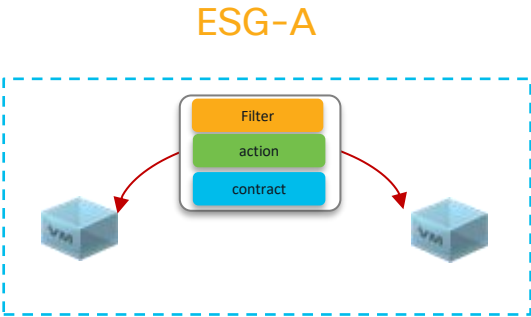
VXLAN GPO with NX-OS

Upcoming Use Cases*

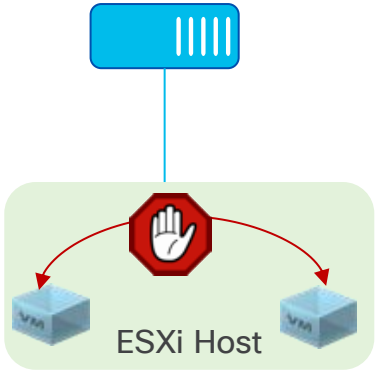
Intra-group Isolation



Intra-group Contract



Policy enforcement between endpoints connected to a common southbound Layer 2 switch (physical or virtual)



VXLAN GPO with NX-OS

Cisco GPO Control Plane Functionalities

Data Plane (draft-smith-vxlan-group-policy)

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 25, 2019

M. Smith
Cisco Systems, Inc.
L. Kreeger
Arrcus, Inc.
October 22, 2018

VXLAN Group Policy Option
draft-smith-vxlan-group-policy-05

Abstract

This document defines a backward compatible extension to Virtual eXtensible Local Area Network (VXLAN) that allows a Tenant System Interface (TSI) Group Identifier to be carried for the purposes of policy enforcement.



Control Plane (draft-wlin-bess-group-policy-id-extended-community)

bess
Internet-Draft
Intended status: Standards Track
Expires: 22 April 2024

W. Lin
Juniper Networks
J. Drake
Individual
D. Rao
Cisco Systems
20 October 2023

Group Policy ID BGP Extended Community
draft-wlin-bess-group-policy-id-extended-community-03

Abstract

Group Based Policy can be used to achieve micro or macro segmentation of user traffic. For Group Based Policy, a Group Policy ID, also known as Group Policy Tag, is used to represent a logical group that shares the same policy and access privilege. This specification defines a new BGP extended community that can be used to propagate Group Policy ID through a BGP route advertisement in the control plane. This is to facilitate policy enforcement at the ingress node when the optimization of network bandwidth is desired.

Data Plane and Control Plane (draft-lrssi-bess-evpn-group-policy)

BESS WorkGroup
Internet-Draft
Intended status: Standards Track
Expires: 5 September 2024

W. Lin
Juniper
D. Rao
A. Sajassi
M. Smith
Cisco
L. Kreeger
Arrcus
4 March 2024

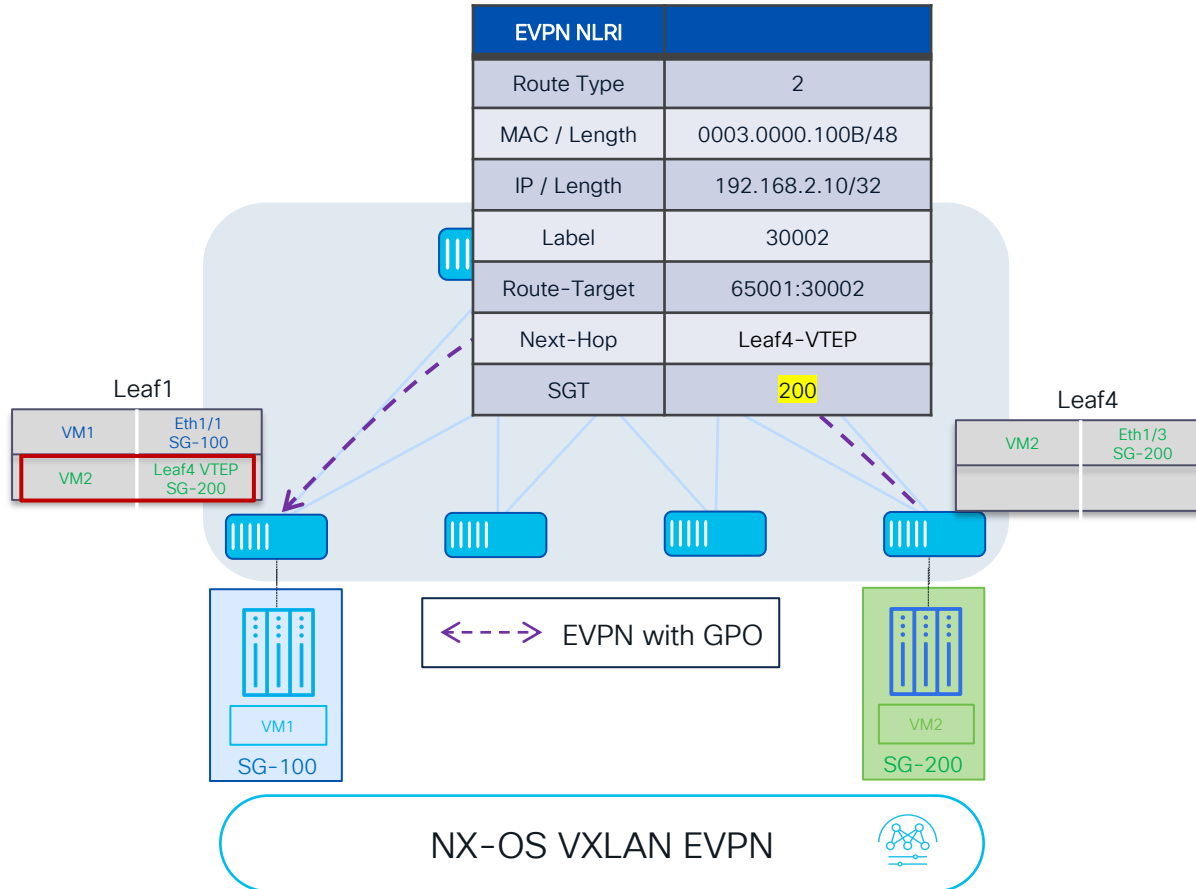
EVPN Group Policy
draft-lrssi-bess-evpn-group-policy-00

Abstract

Group Based Policy can be used to achieve micro or macro segmentation of user traffic. For Group Based Policy, a Group Policy ID, also known as Group Policy Tag, is used to represent a logical group that shares the same policy and access privilege. This document defines a backward compatible extension to Virtual eXtensible Local Area Network (VXLAN) that allows a Group Policy ID to be carried for the purposes of policy enforcement at the egress Network Virtualization Edge (NVE). It also defines a new BGP Extended Community that can be used to propagate Group Policy ID through a BGP route advertisement in the control plane. This is to facilitate policy enforcement at the ingress NVE when feasible.

VXLAN GPO with NX-OS

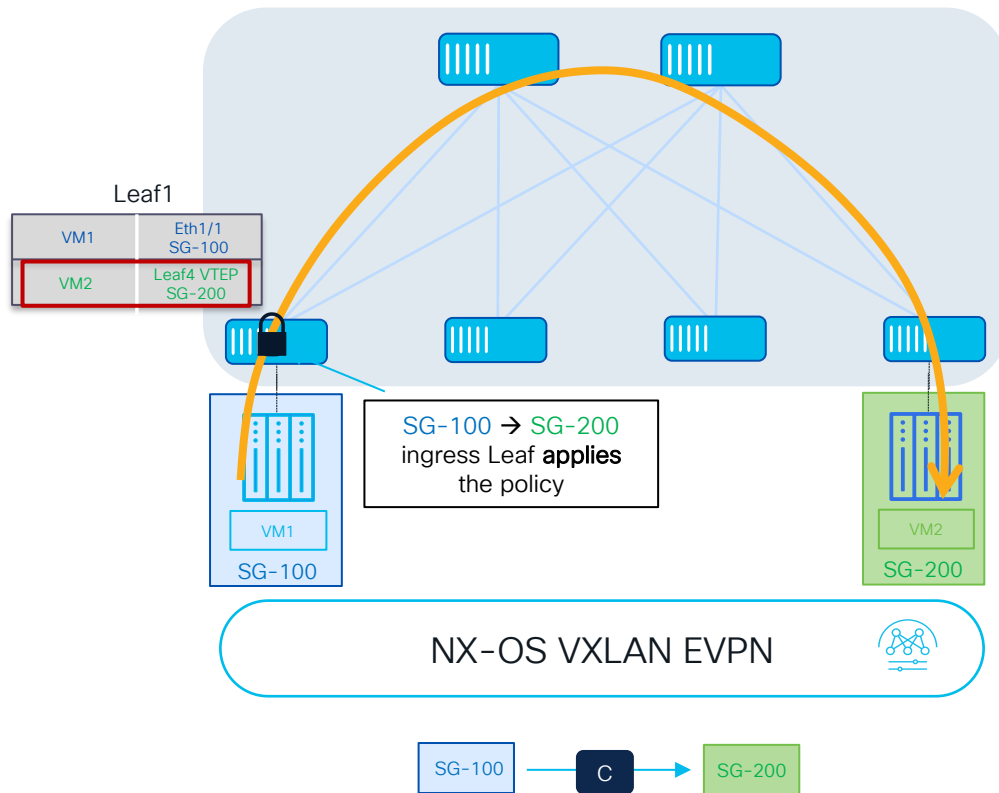
Use of MP-BGP EVPN for Exchanging Security Tags



- Use of MP-BGP EVPN control plane to propagate endpoints connectivity and policy information inside the fabric
- The SGT information is propagated as a BGP extended community (Group Policy ID Extended Community)

VXLAN GPO with NX-OS

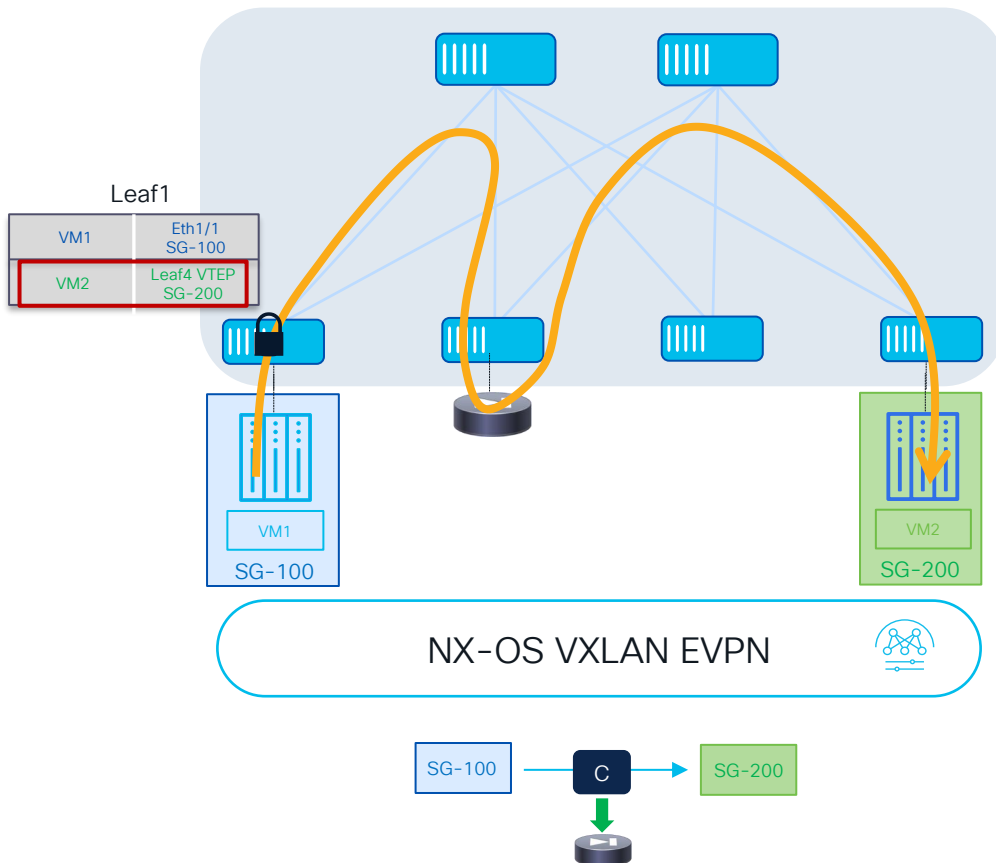
Enforcing Policy on the Ingress Leaf



- Facilitate the optimal enforcement of policy on the ingress leaf node (for both directions)
- Security Group Access Control Lists (SGACLs/contracts) enforced between groups

VXLAN GPO with NX-OS

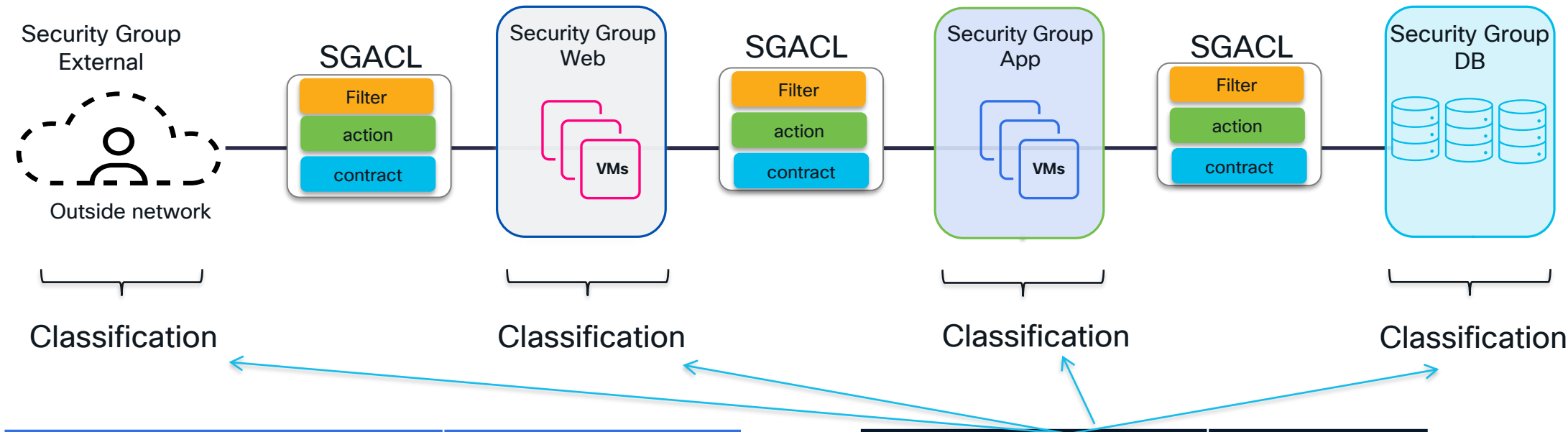
Traffic Steering with Policy Based Redirection



- Policy Based Redirection capabilities to steer through one or more service devices (firewall, load balancers, etc.) traffic flows between different security groups
- Redirection to a Firewall service function with NX-OS 10.4(3)F
- Other use cases, including redirection to service-chains supported from NX-OS 10.5(2) release

VXLAN GPO with NX-OS

Classification Criteria and SGACL Actions



SGACL Action	NX-OS Version
Permit, Permit + Log	10.4(3)
Deny, Deny + Log	10.4(3)
Redirect (FW service only)	10.4(3)
Redirect (SLB, Service-Chain)	10.5(2)

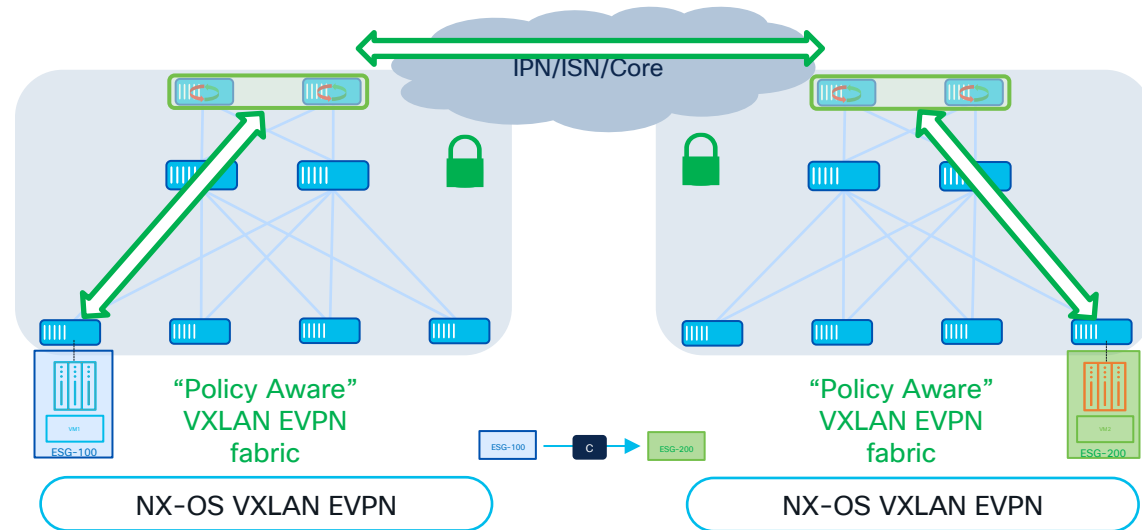
Security Group Attributes	NX-OS Version
IP Prefix (internal & external)	10.4(3)
VLAN	10.4(3)
Port + VLAN	10.5(1)
VM Tags/Attributes	Roadmap

Classification is done assigning a fabric-wide unique tag (valid range: 16-65535)

VXLAN GPO with NX-OS

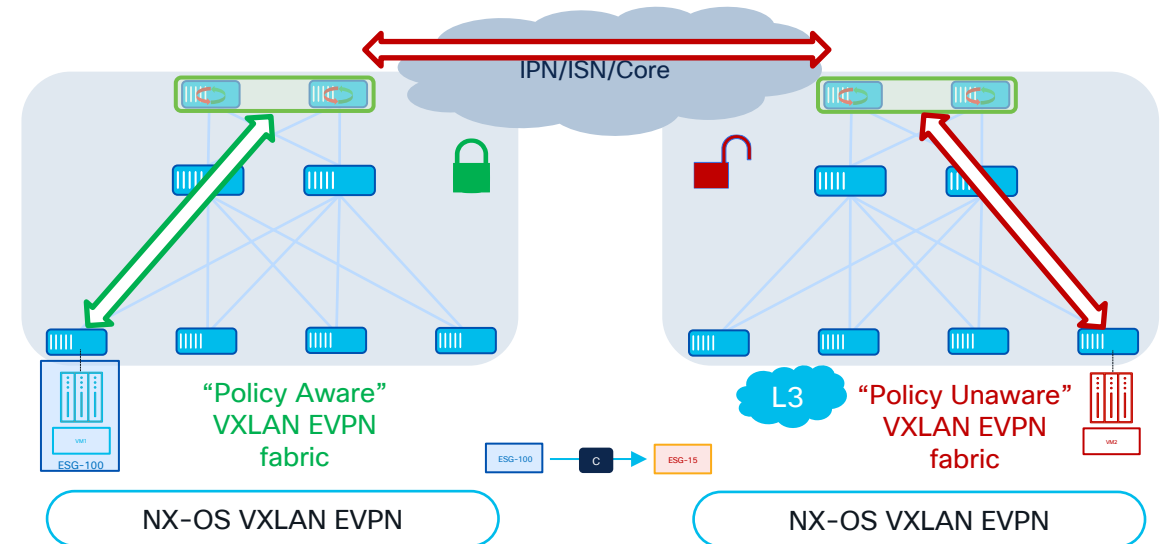
Multi-Site Support

Policy-Aware to Policy-Aware



- Creation of an end-to-end policy domain
- The defined security policy is consistently and optimally applied independently from the specific location of the endpoints

Policy-Aware to Policy-Unaware



- Resources connected to "Policy Unaware" fabrics are automatically classified as part of ESG 15 (reserved value) in "Policy Aware" fabrics
- Allows to define a coarse security policy

ACI Border Gateways (BGWs)

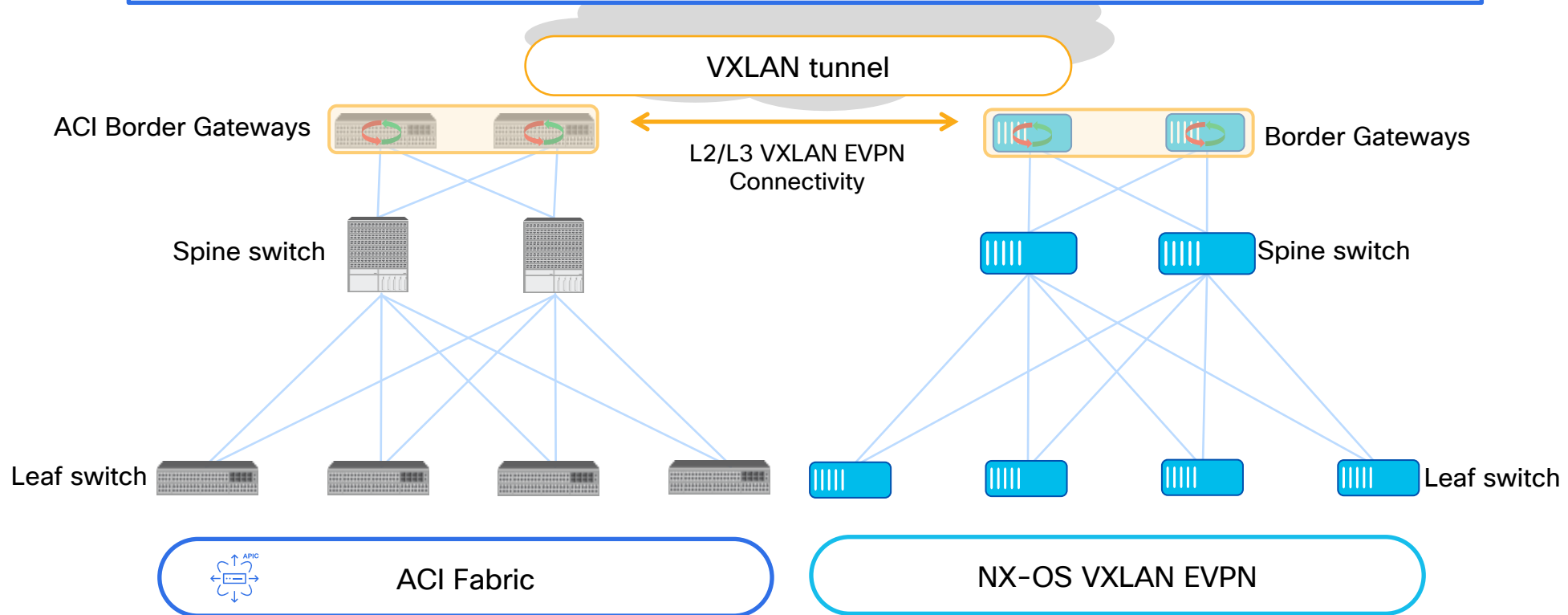
For More Information on ACI BGWs please refer to BRKDCN-2634 from Cisco Live San Diego 2025:
<https://www.ciscolive.com/on-demand/on-demand-library.html?search=ardica#/session/1750271884651001zqS7>

Heterogeneous Fabrics

ACI 6.1(x)

Introducing ACI Border Gateways

“Opening Up” L2/L3 Connectivity between ACI and VXLAN EVPN Fabrics



ACI Border Gateway

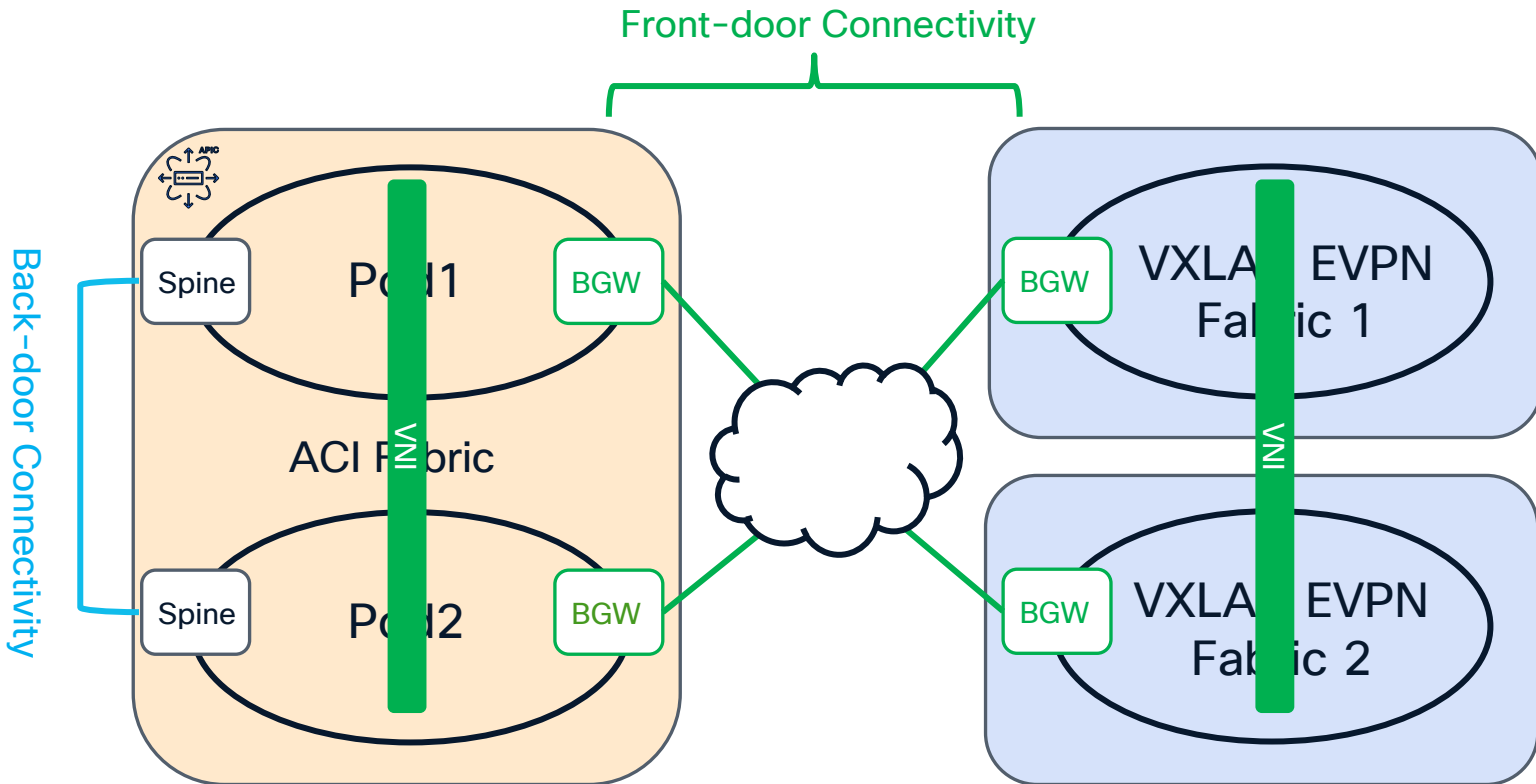
Deployment Considerations and Current Restrictions

- Hardware support for ACI BGWs: Nexus 9000 FX and above
 - Requires 32 GB of memory (or more) on the BGW switches
- Software support for ACI BGWs
 - ACI 6.1(5)M or later (recommended)
- Dedicated leaf nodes for Border Gateway functionality
 - Coexistence with Border Leaf functions (Tenant L3Outs) planned for a future release
 - In an ACI Multi-Pod fabric, local BGW instances must be deployed in each Pod
- IGMP snooping and L3 Multicast traffic (TRM) not supported across domains
 - L2 Multicast and intra-subnet IP Multicast traffic forwarded as BUM
- Support symmetric and asymmetric namespaces across ACI and NX-OS domains

Supported Topologies

ACI 6.1(1)

Single ACI Fabric (Multi-Pod) Support

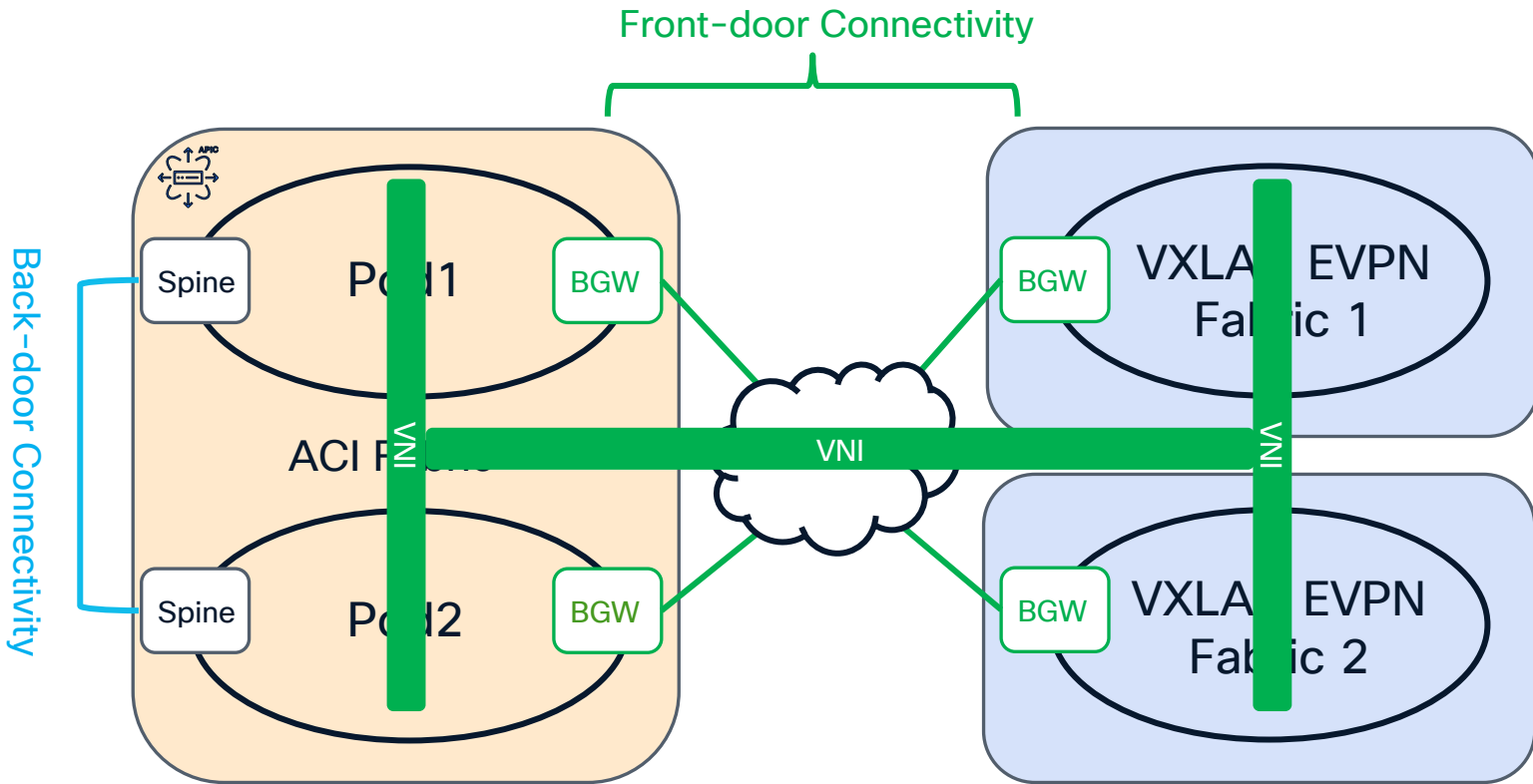


- Between ACI Pods
 - iVXLAN through spines via the IPN (same as before)
 - Not through BGWs
 - BGWs must be present in each Pod
- Between VXLAN EVPN Fabrics
 - VXLAN through BGWs

Supported Topologies

ACI 6.1(1)

Single ACI Fabric (Multi-Pod) Support

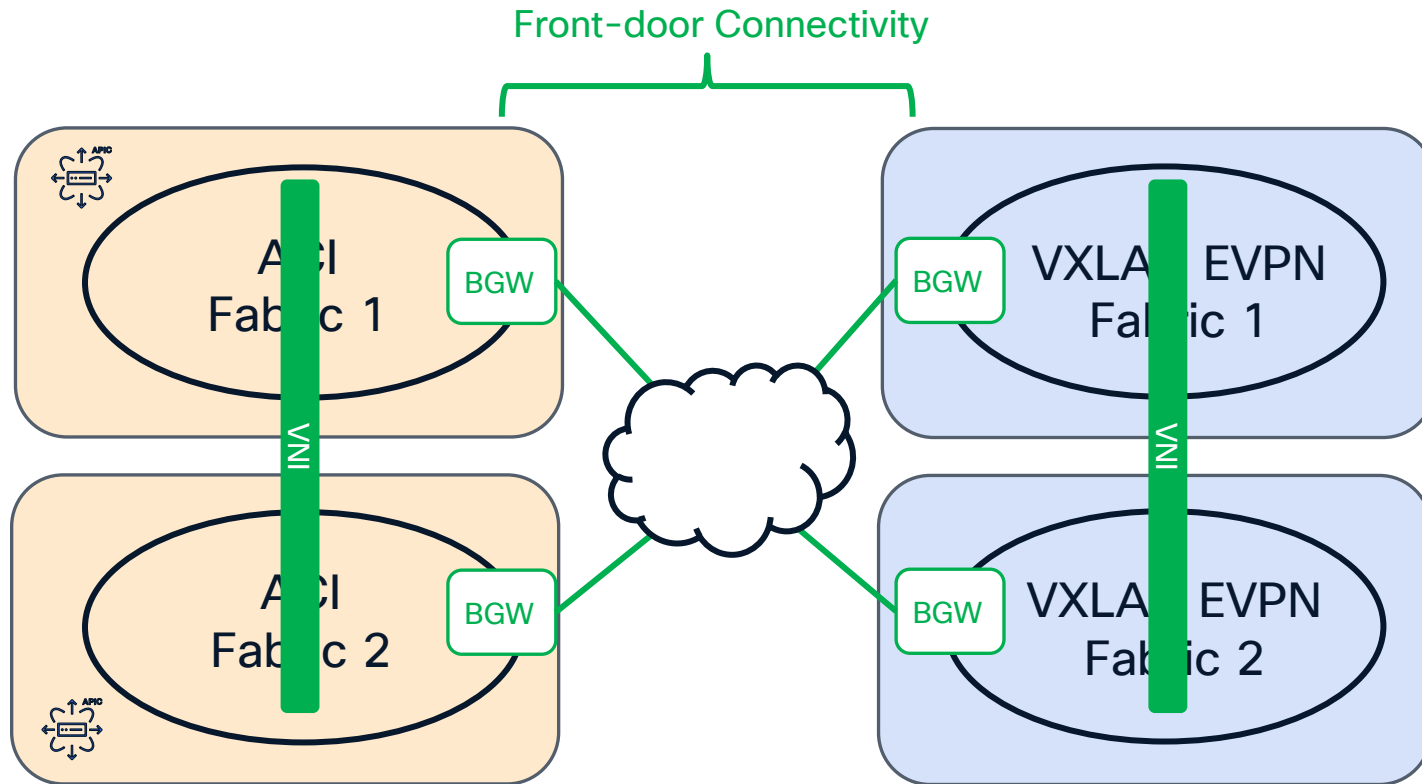


- Between ACI Pods
 - iVXLAN through spines via the IPN (same as before)
 - Not through BGWs
 - BGWs must be present in each Pod
- Between VXLAN EVPN Fabrics
 - VXLAN through BGWs
- Between ACI and VXLAN EVPN Domains
 - VXLAN through BGWs
 - One BGW across Pods is elected as Designated Forwarder (DF) for each stretched BD (L2VNI)

Supported Topologies

ACI 6.1(5)

Independent ACI Fabrics Connecting to the VXLAN EVPN Domain

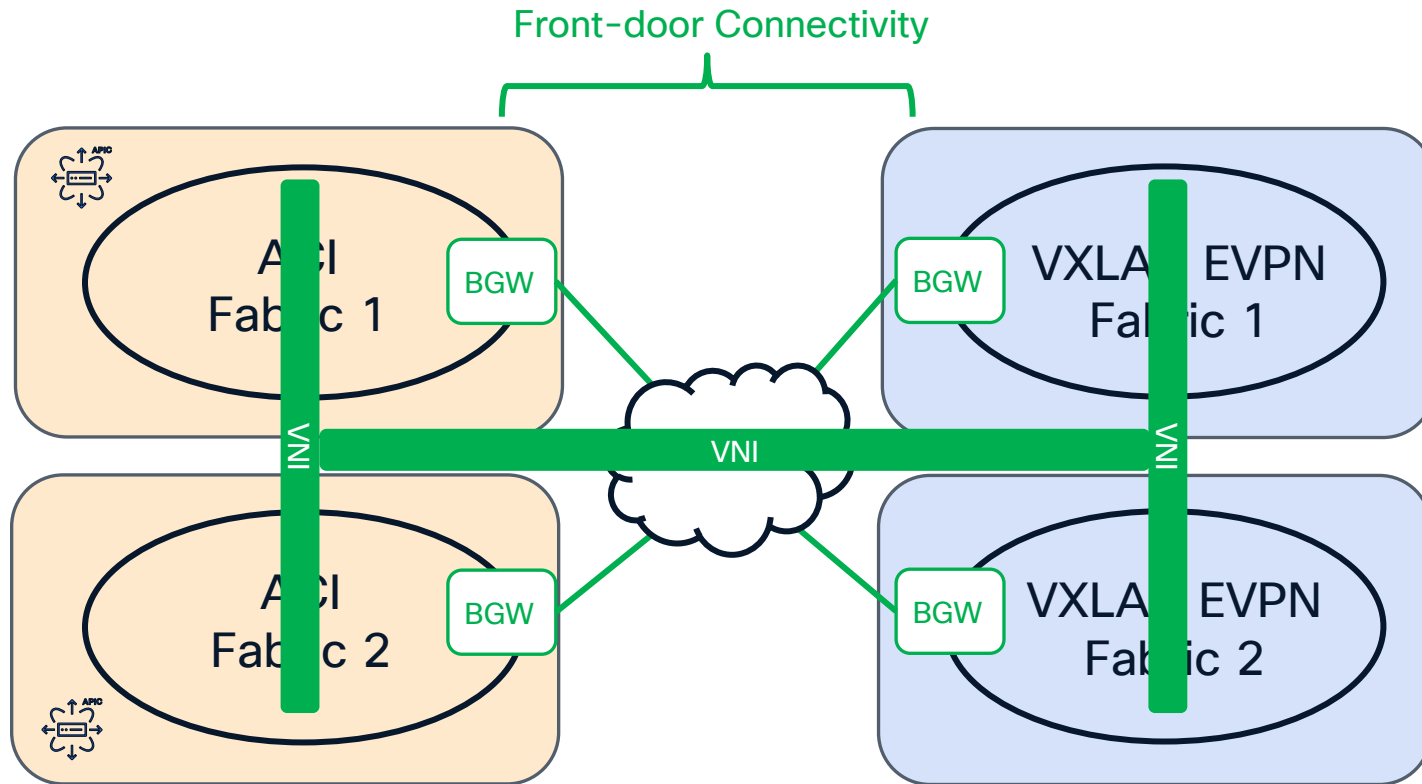


- Between ACI Fabrics
 - VXLAN through BGWs
- Between VXLAN EVPN Fabrics
 - VXLAN through BGWs

Supported Topologies

ACI 6.1(5)

Independent ACI Fabrics Connecting to the VXLAN EVPN Domain

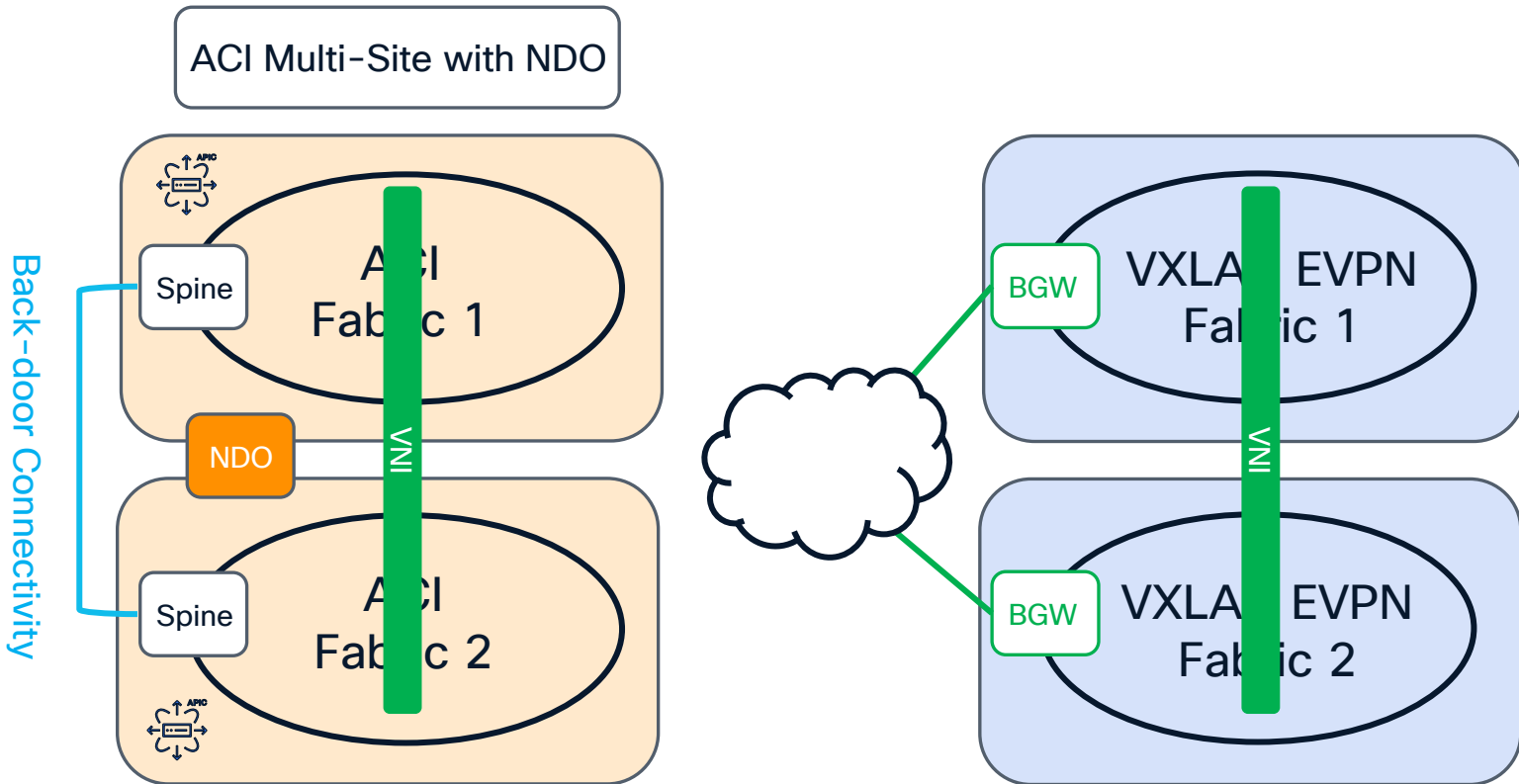


- Between ACI Fabrics
 - VXLAN through BGWs
- Between VXLAN EVPN Fabrics
 - VXLAN through BGWs
- Between ACI and VXLAN EVPN Domains
 - VXLAN through BGWs

ACI Multi-Site with NDO and VXLAN EVPN Domain

Future

Coexistence Use Case

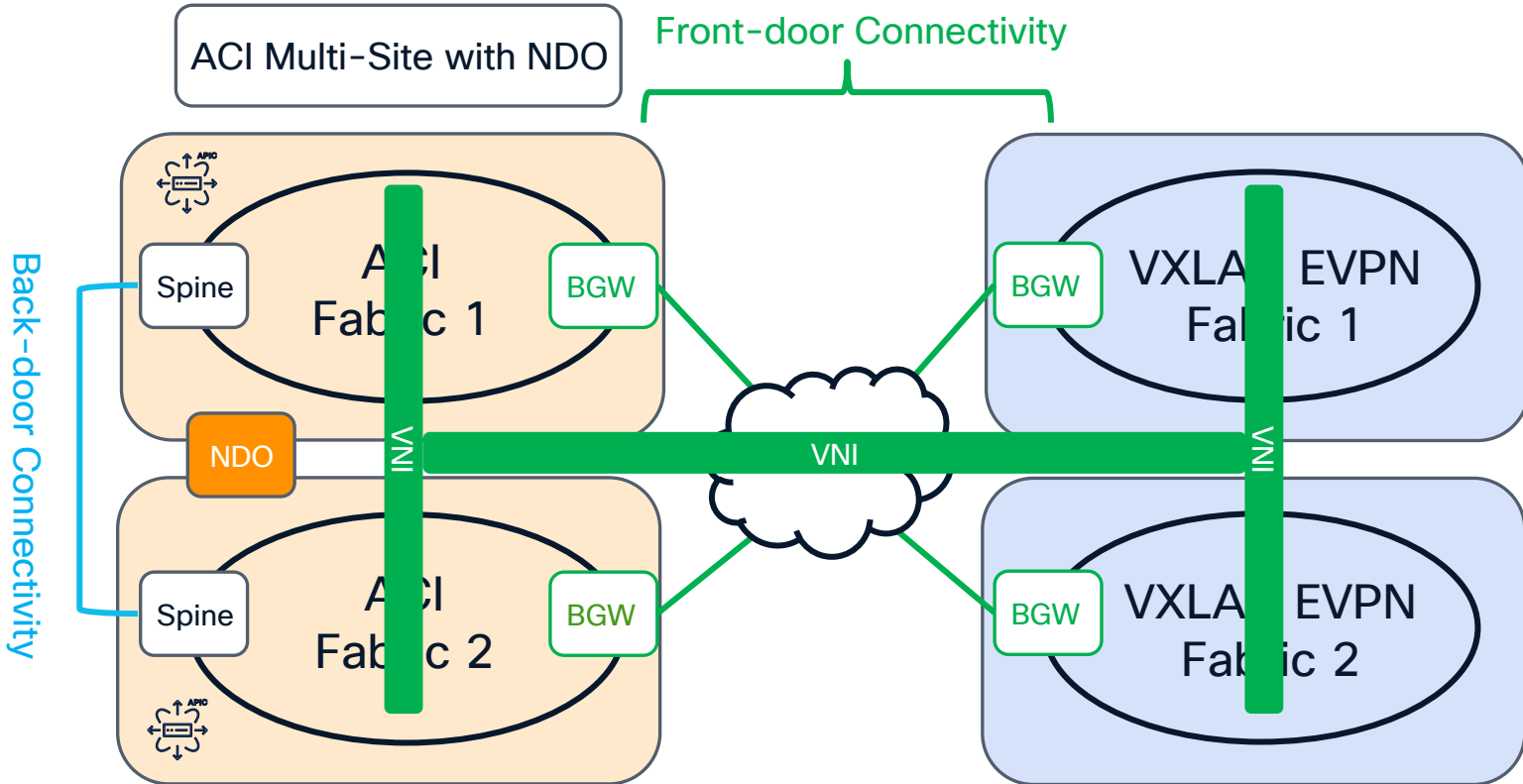


- Existing connection through the spines continue to provide ACI-to-ACI L2/L3 extension and policy
- Use of ACI BGWs only for connecting to the VXLAN EVPN domain
- **Requirement:** ACI BGWs must be deployed in each ACI fabric (i.e. no inter-fabric transit support for communication to the VXLAN EVPN domain)

ACI Multi-Site with NDO and VXLAN EVPN Domain

Future

Coexistence Use Case

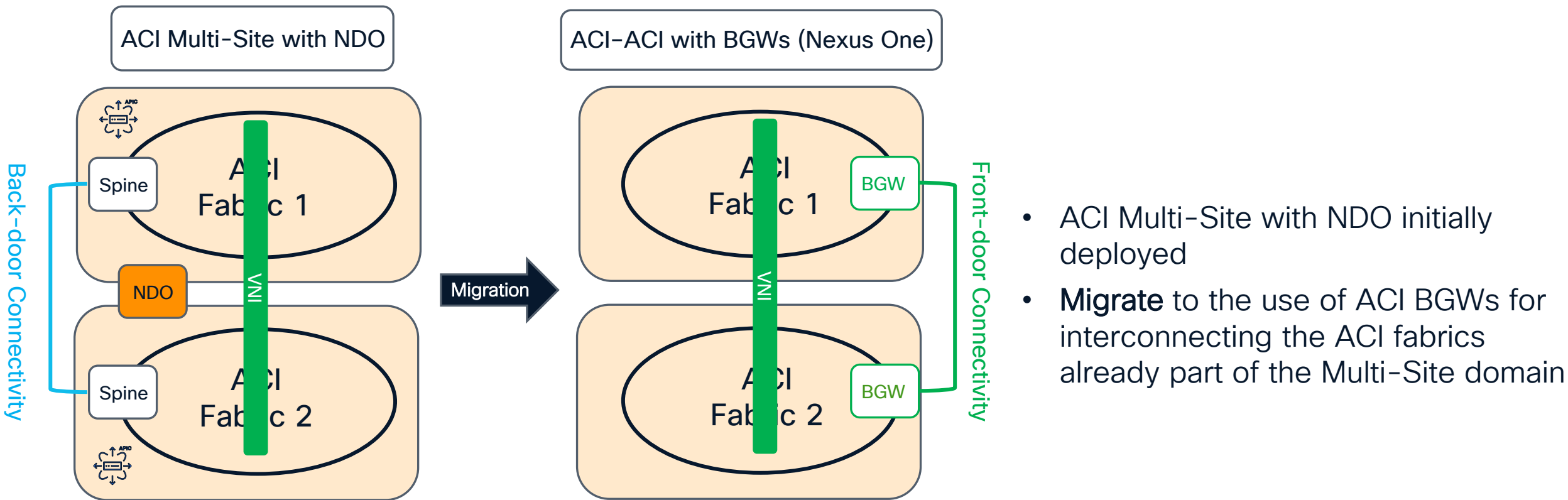


- Existing connection through the spines continue to provide ACI-to-ACI L2/L3 extension and policy
- Use of ACI BGWs only for connecting to the VXLAN EVPN domain
- **Requirement:** ACI BGWs must be deployed in each ACI fabric (i.e. no inter-fabric transit support for communication to the VXLAN EVPN domain)

ACI Multi-Site with NDO and VXLAN EVPN Domain

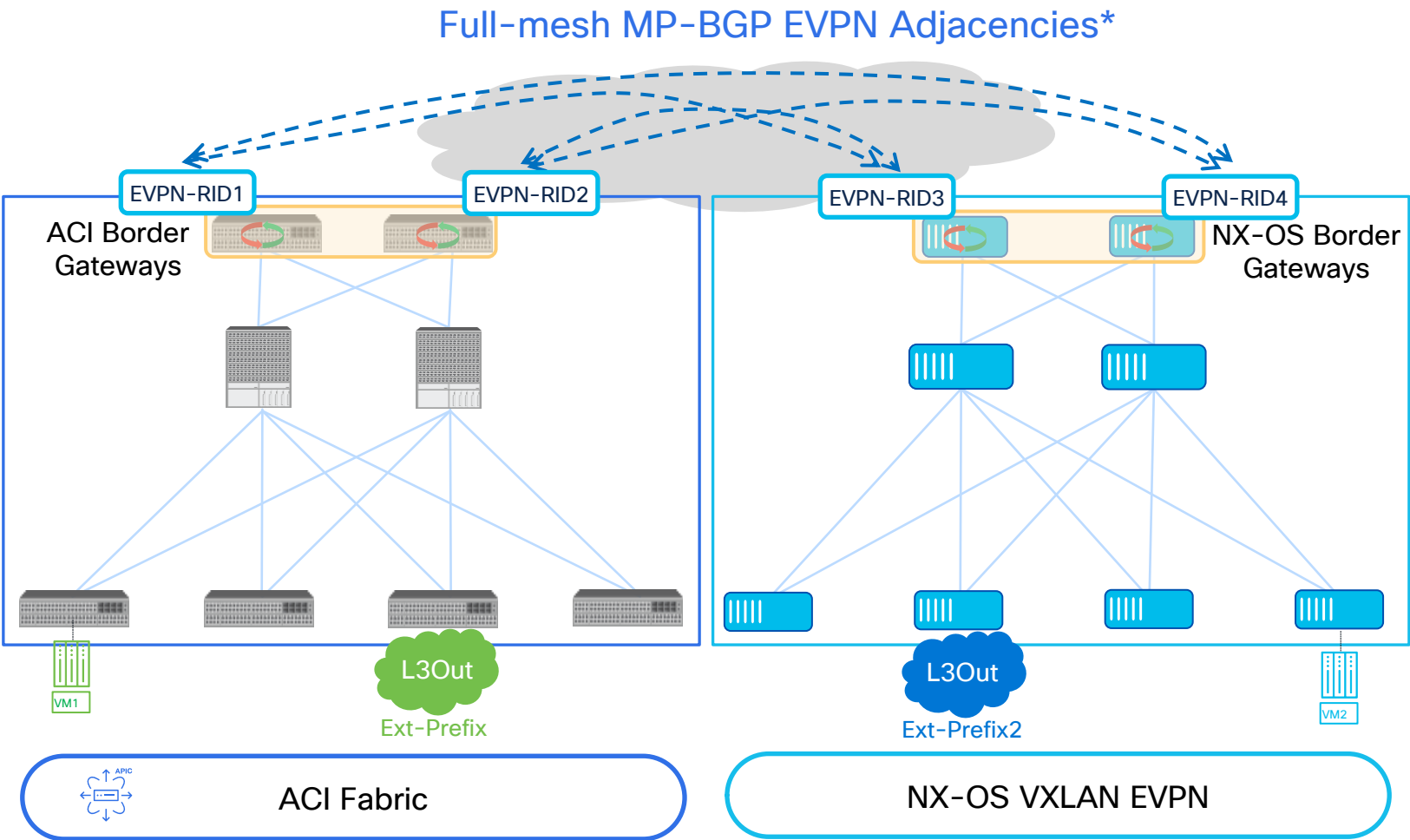
Future

Migration Use Case



ACI Border Gateways

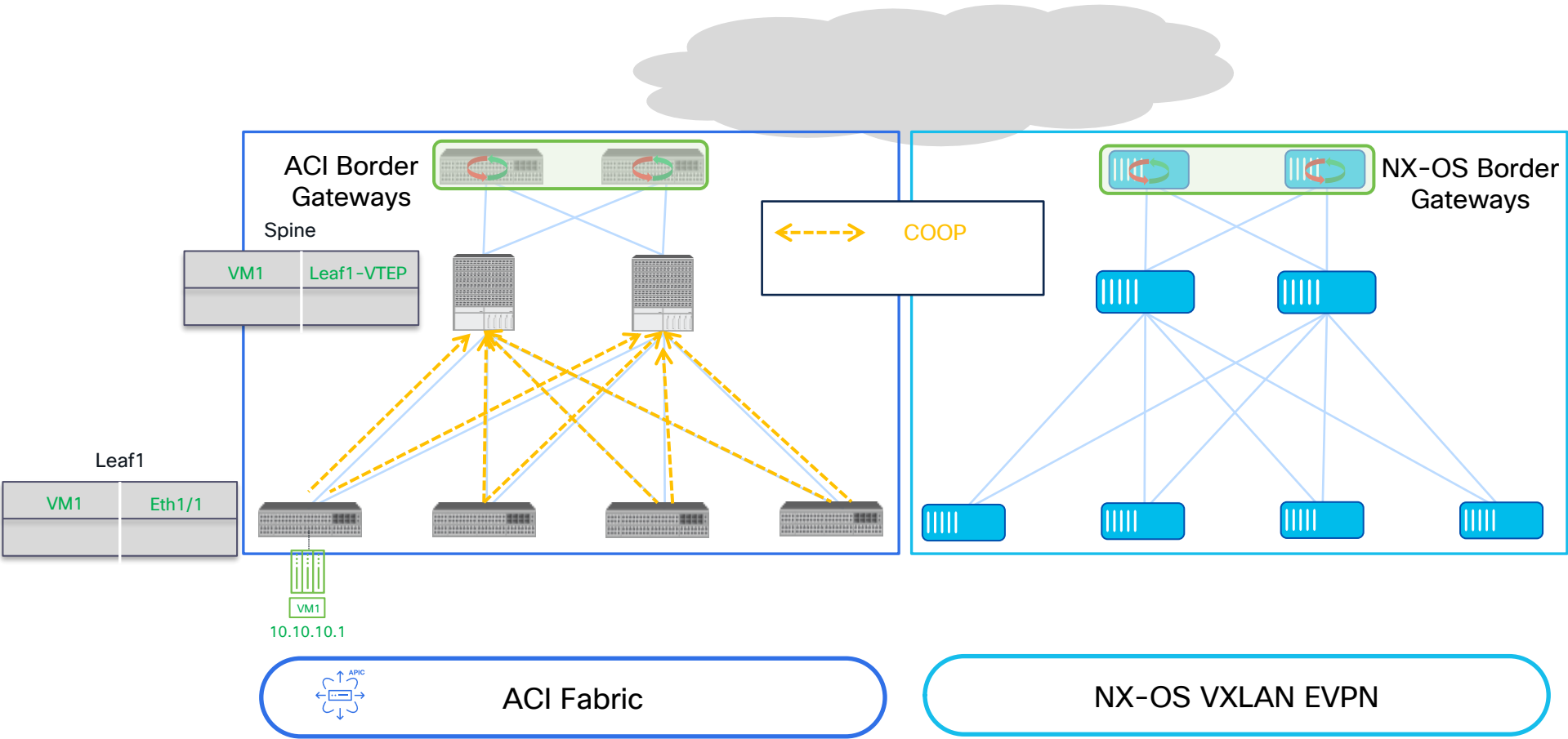
Overlay EVPN Connectivity across Domains



*No current Route-Server support

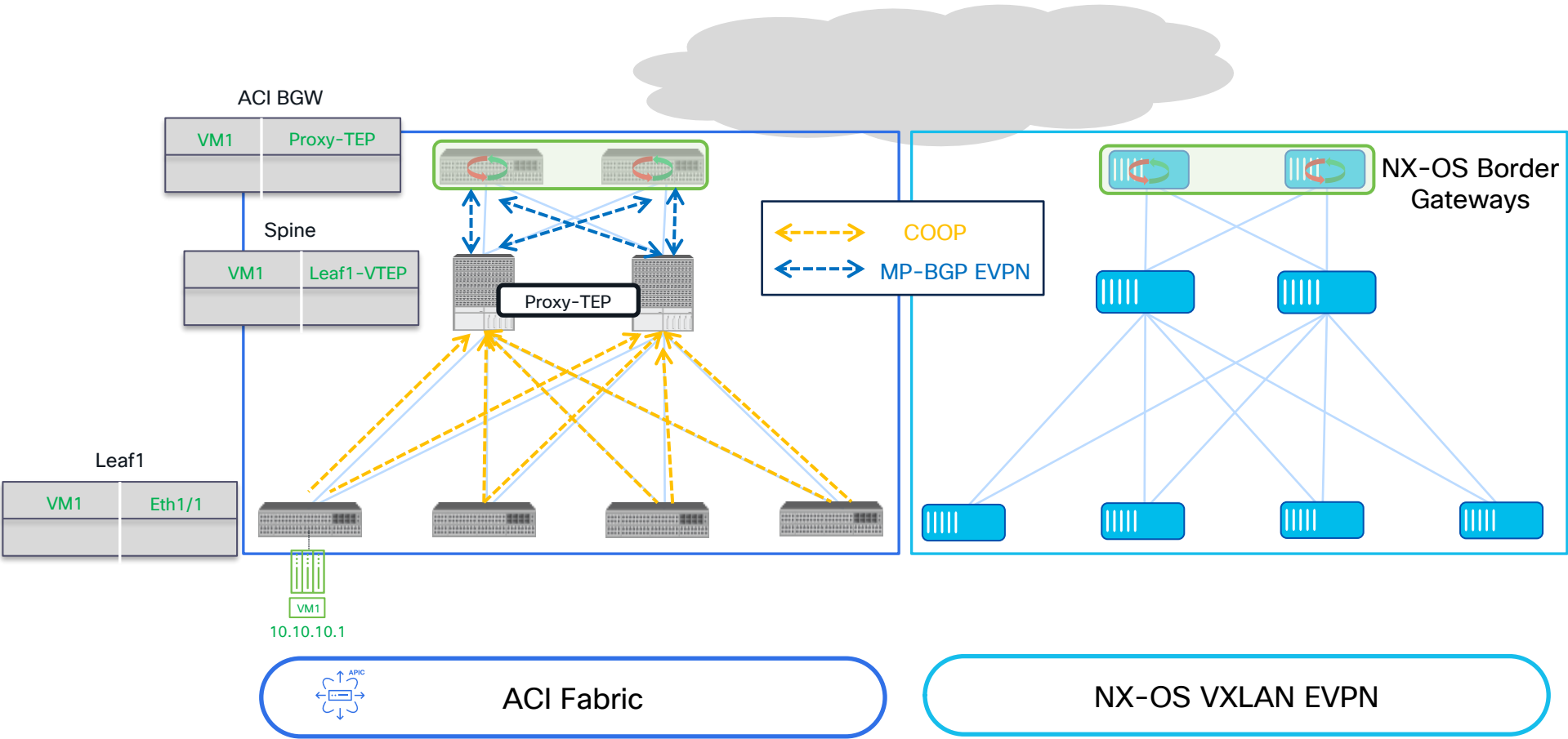
ACI Border Gateways

Control-Plane Overview



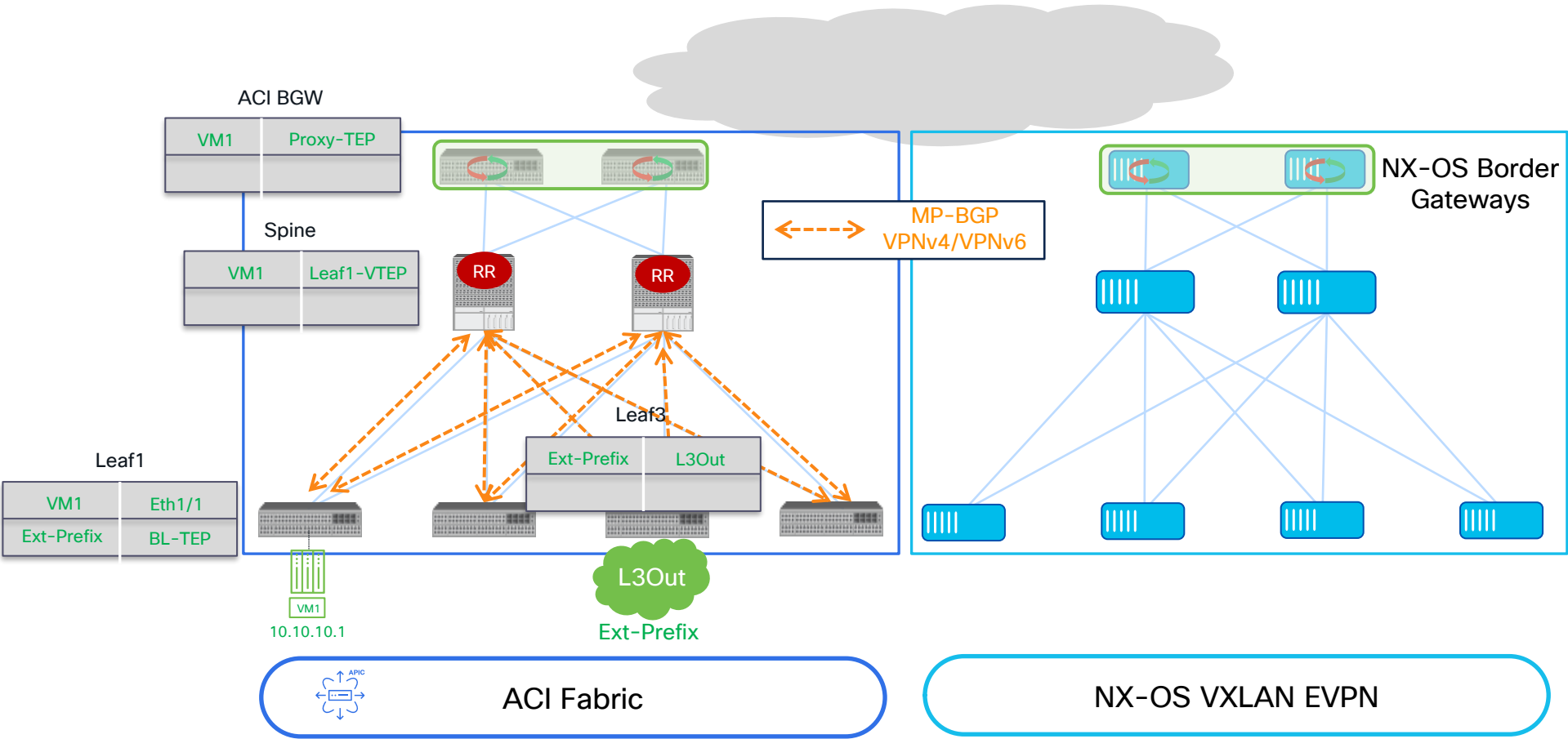
ACI Border Gateways

Control-Plane Overview



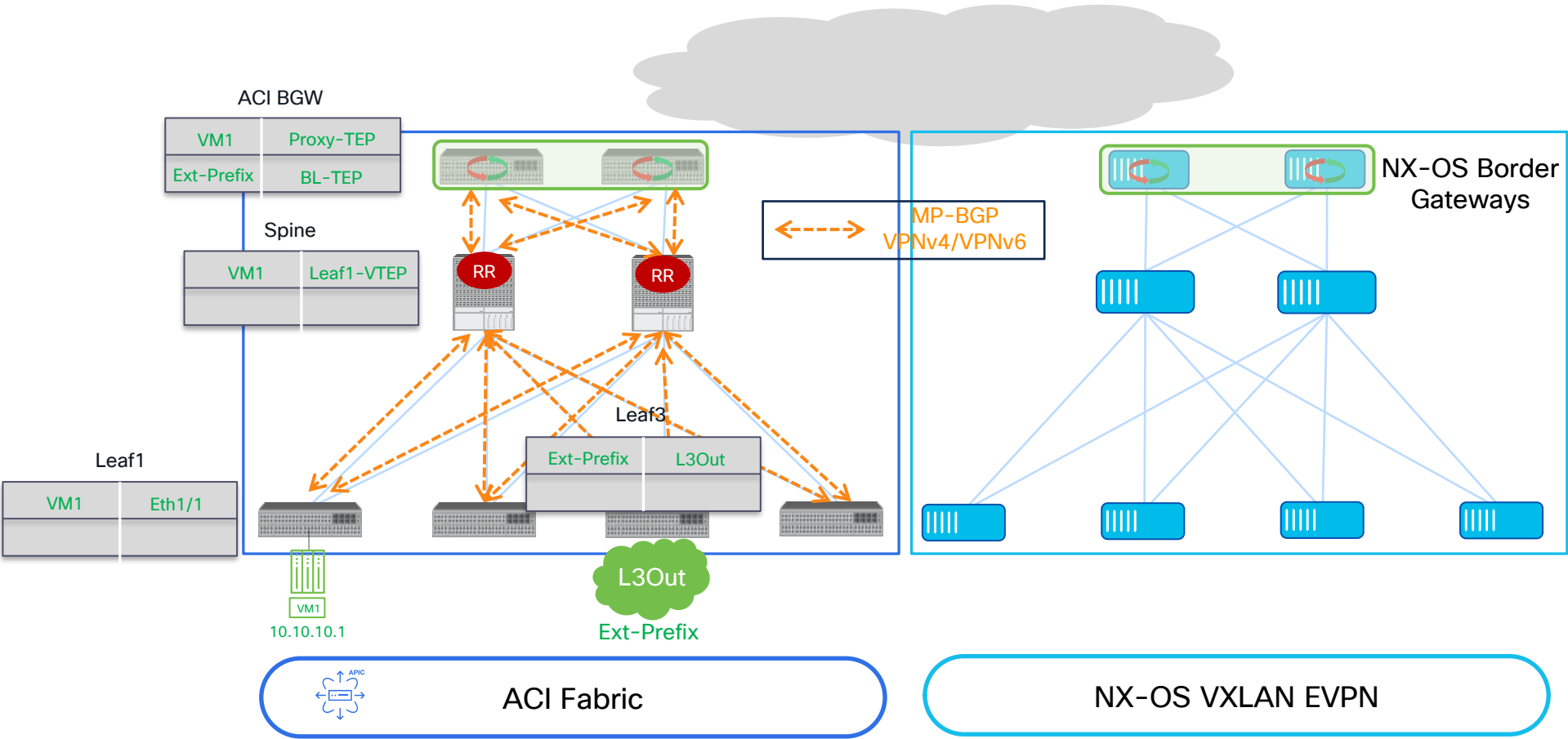
ACI Border Gateways

Control-Plane Overview



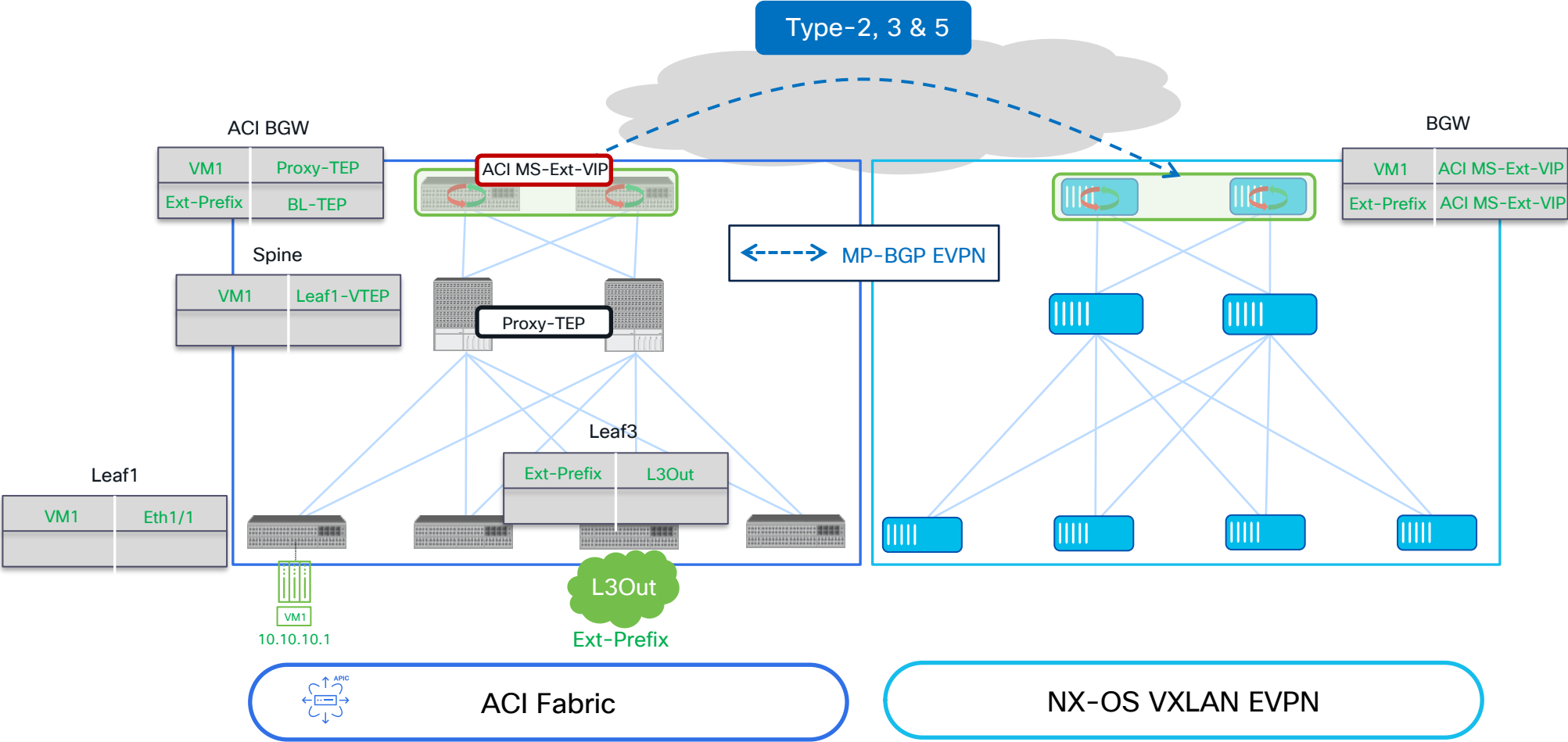
ACI Border Gateways

Control-Plane Overview



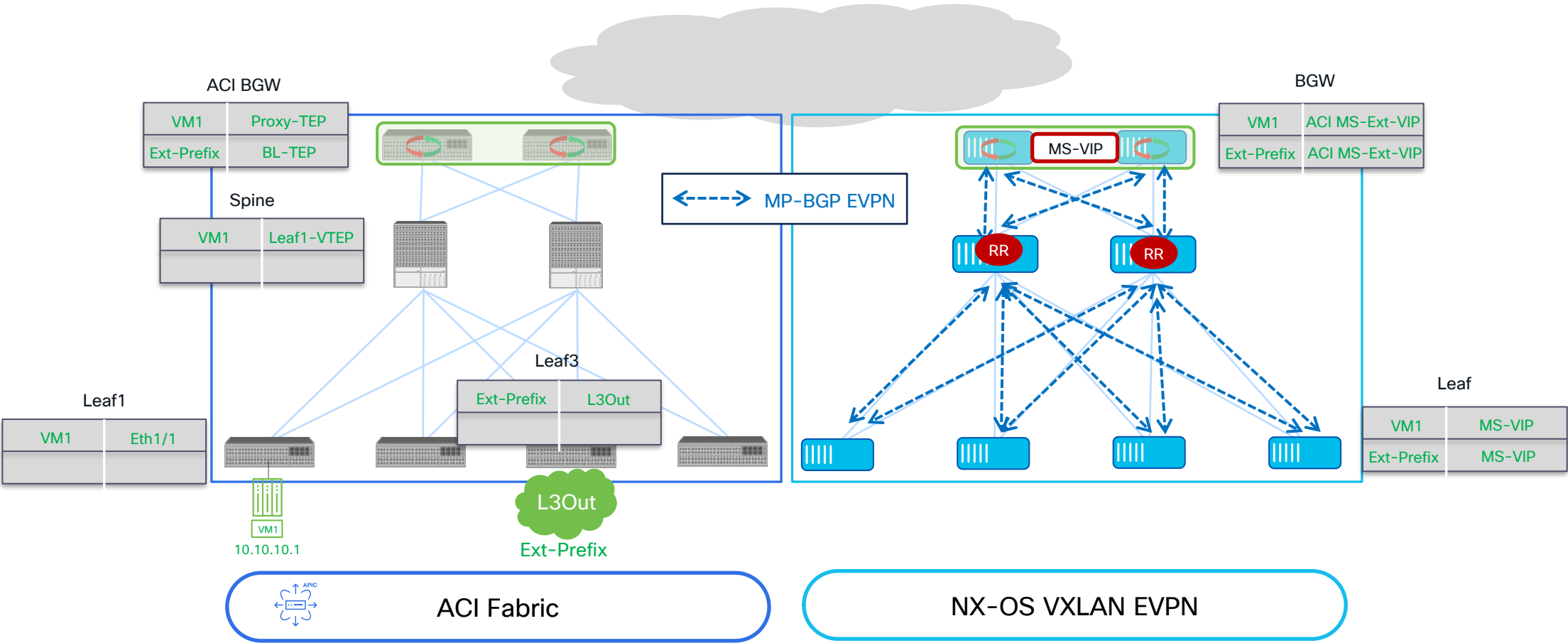
ACI Border Gateways

Control-Plane Overview



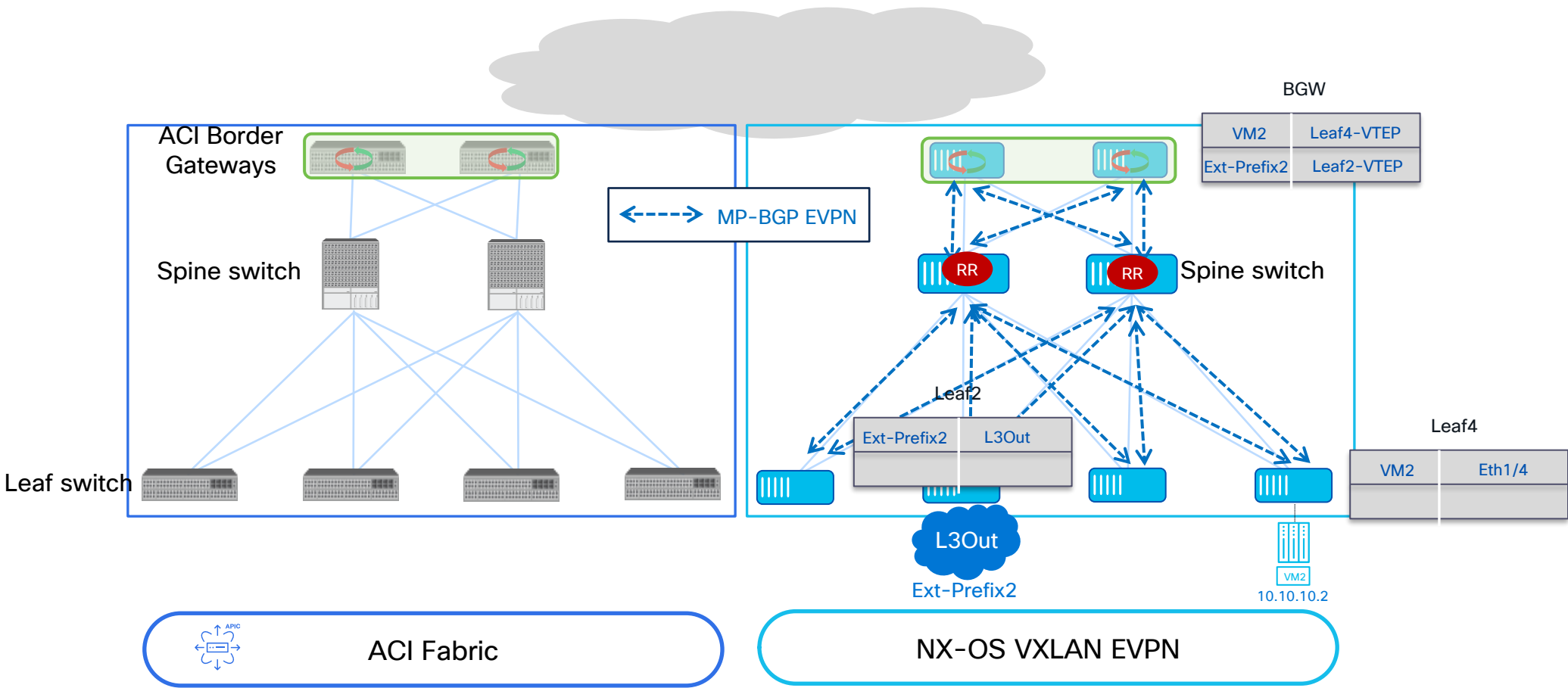
ACI Border Gateways

Control-Plane Overview



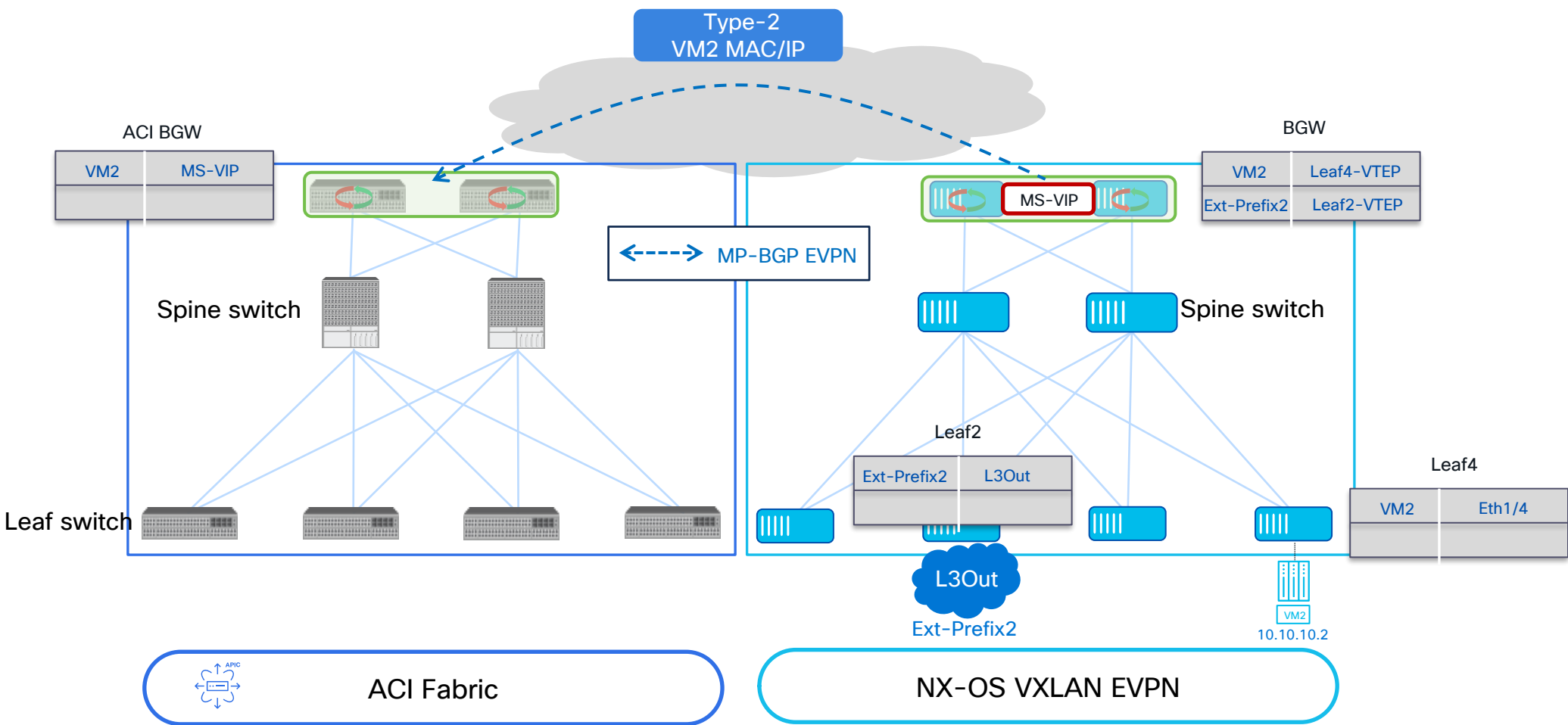
ACI Border Gateways

Control-Plane Overview



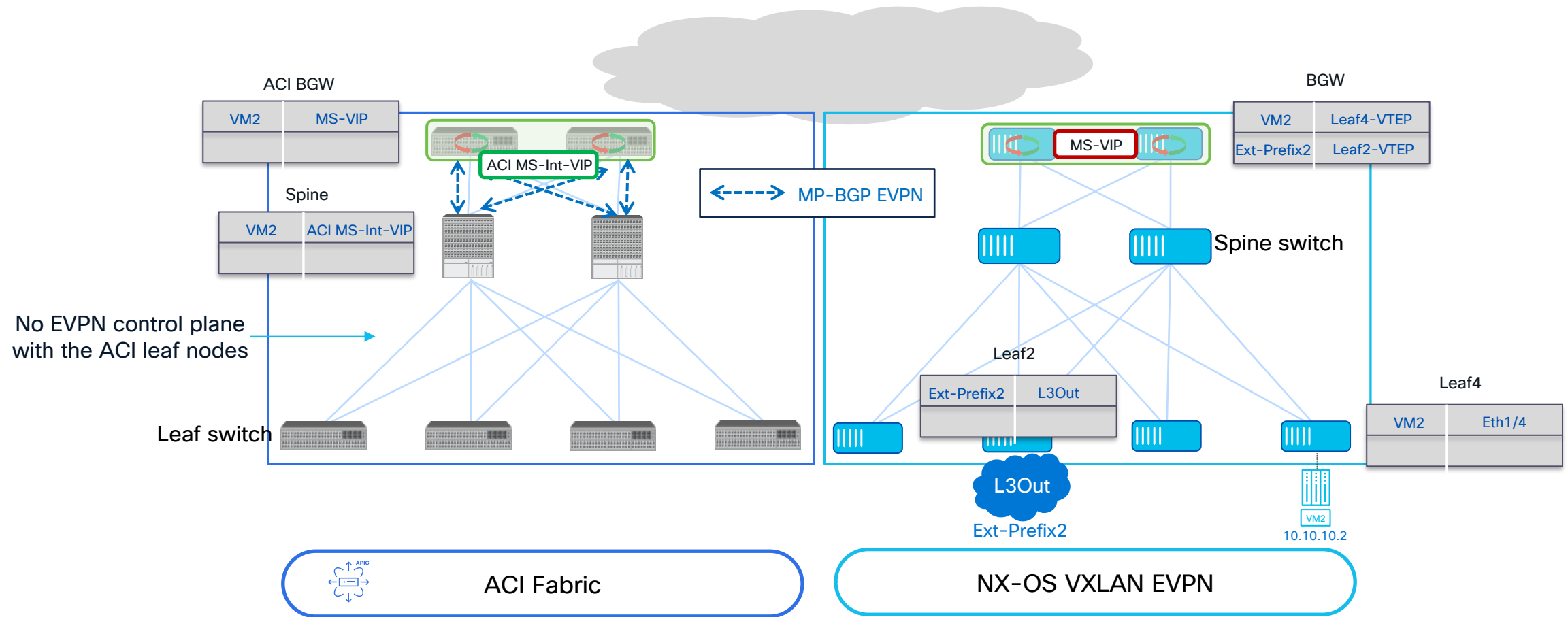
ACI Border Gateways

Control-Plane Overview



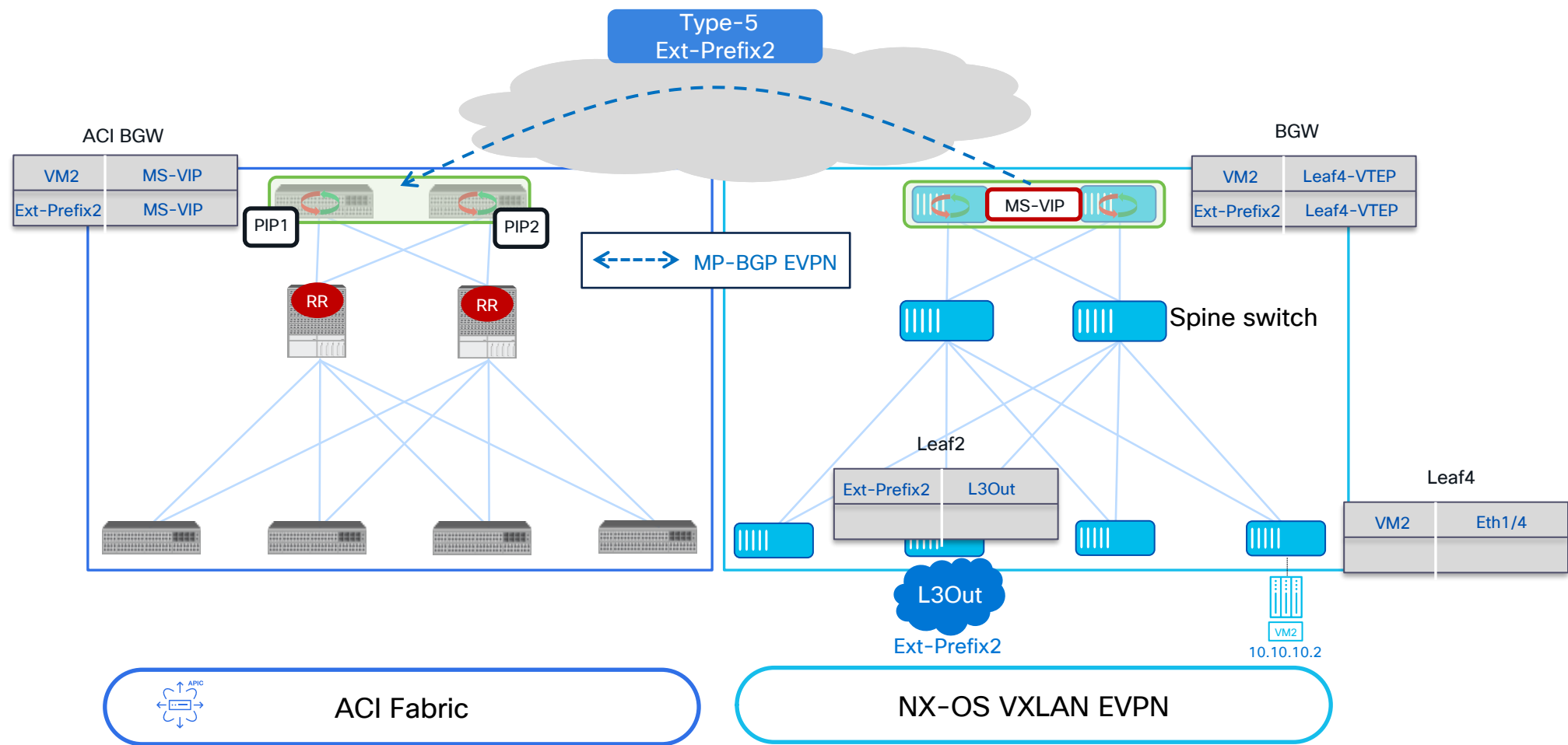
ACI Border Gateways

Control-Plane Overview



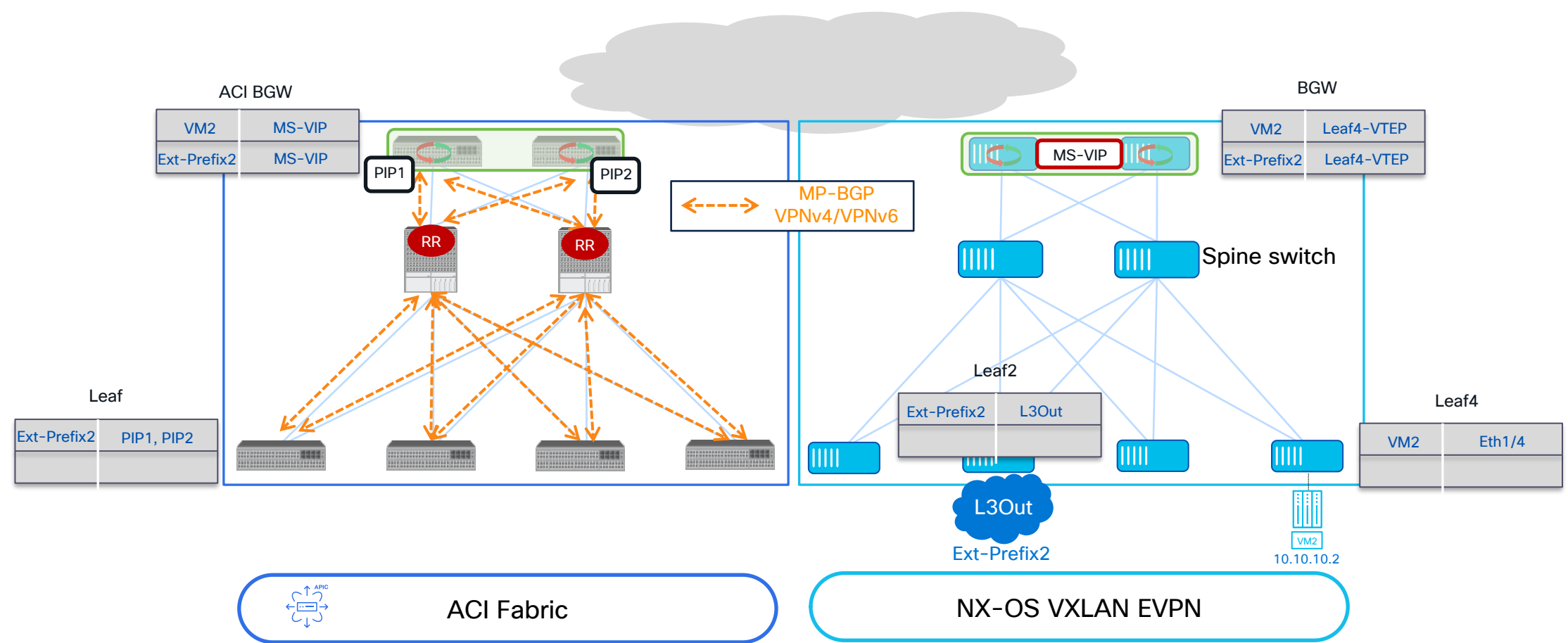
ACI Border Gateways

Control-Plane Overview



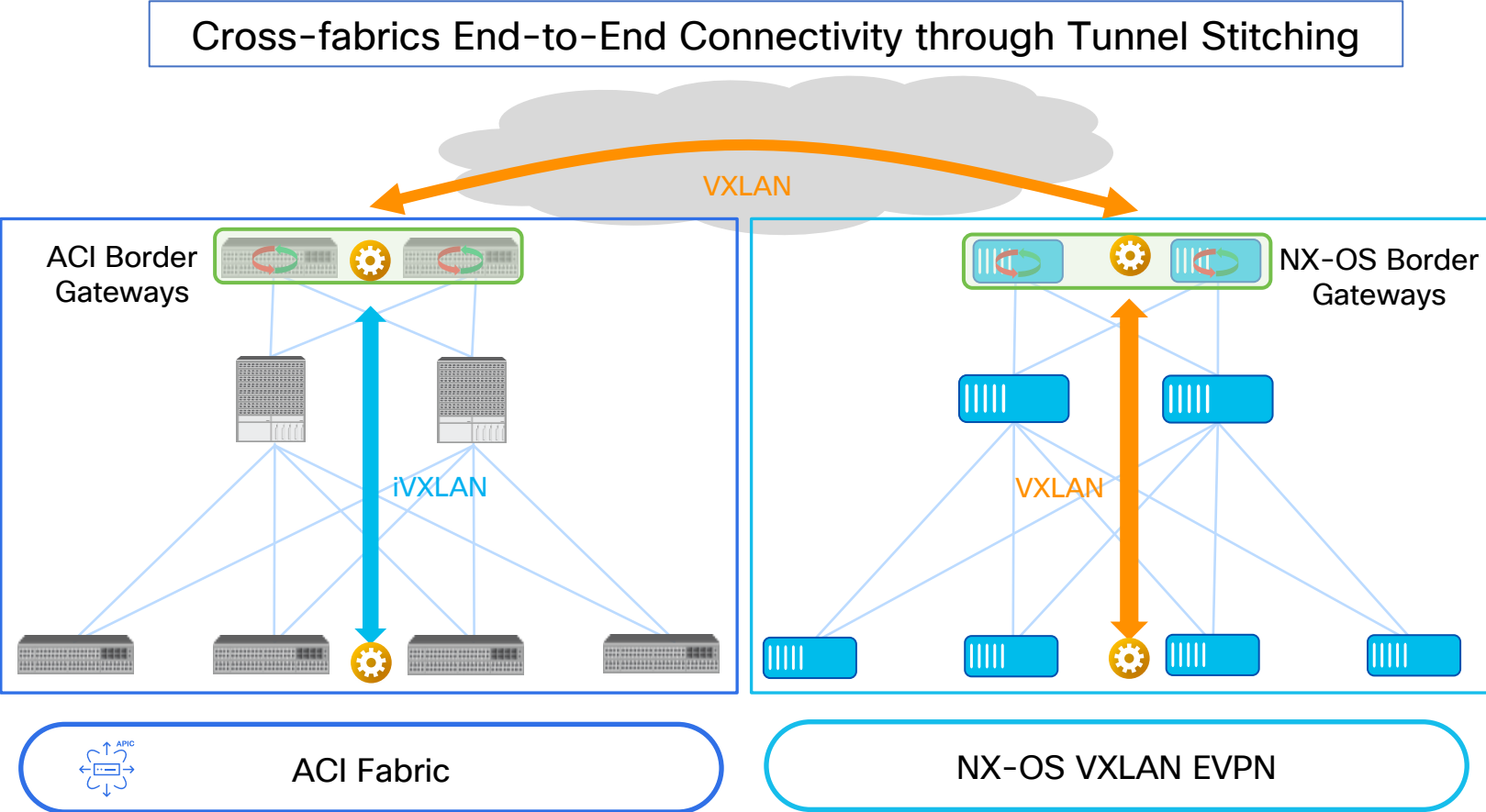
ACI Border Gateways

Control-Plane Overview



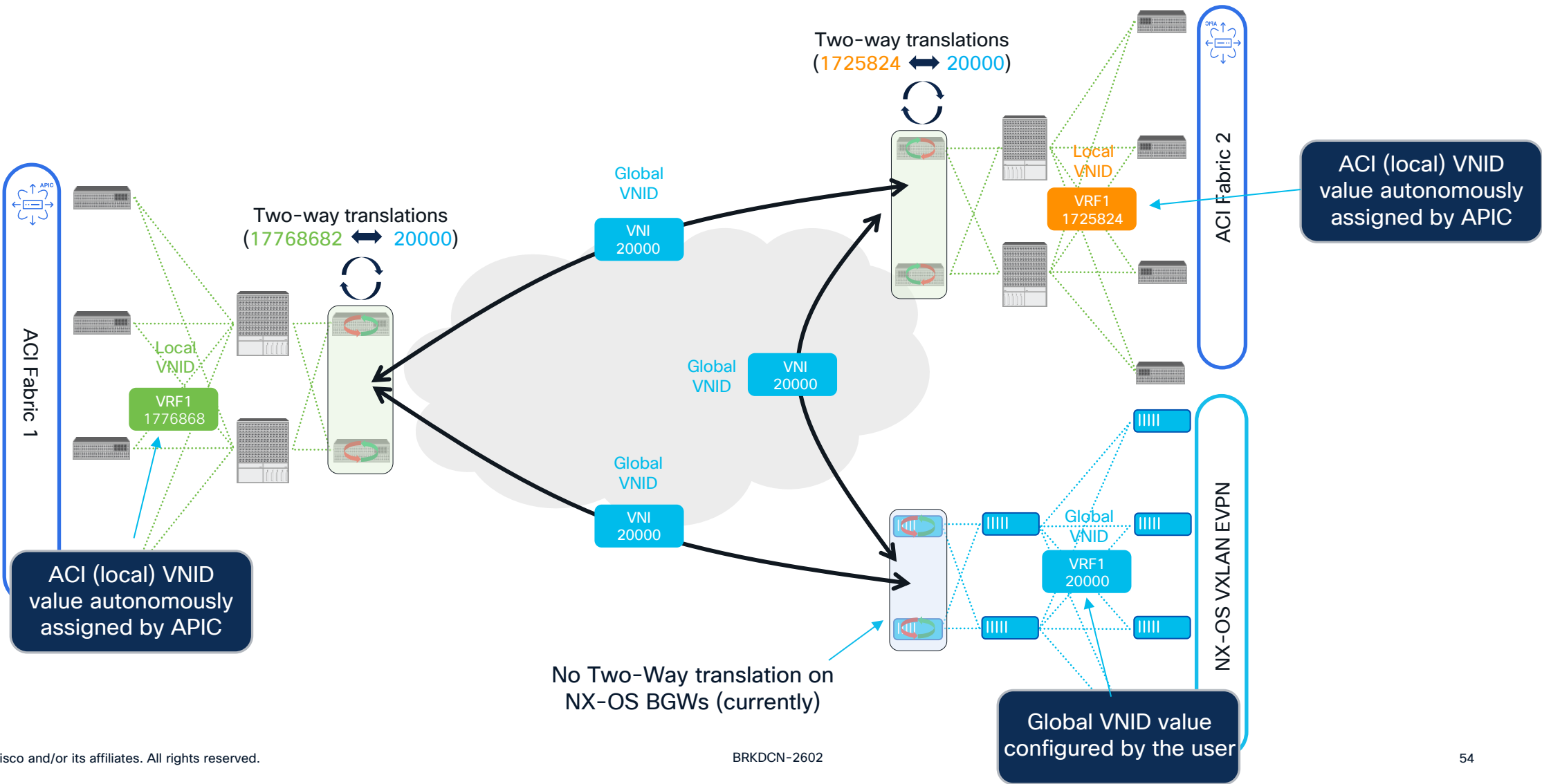
ACI Border Gateways

Data-Plane Overview



ACI Border Gateways

Two-Way Translation Function on ACI BGWs



NX-OS GPO + ACI BGWs

**End-to-End Policy Domain between
Heterogeneous Fabrics**

Pre-Requisite

Migrating EPGs to ESGs on ACI Fabrics for the VRFs that are Stretched to Remote Fabrics

Cisco will provide a Python script to facilitate the uplifting of EPGs to ESGs

- Initially, can be run directly on the APIC CLI or outside the APIC
- In a second phase, the plan is to provide UI support (on Nexus Dashboard)
- The procedure consists of three main steps:

Dry-Run

Analyze an APIC snapshot and provides a plan for mapping EPGs to ESGs

Conversion

Creates and provisions to APIC the new ESG configuration, including route-leaking (when needed)

Cleanup

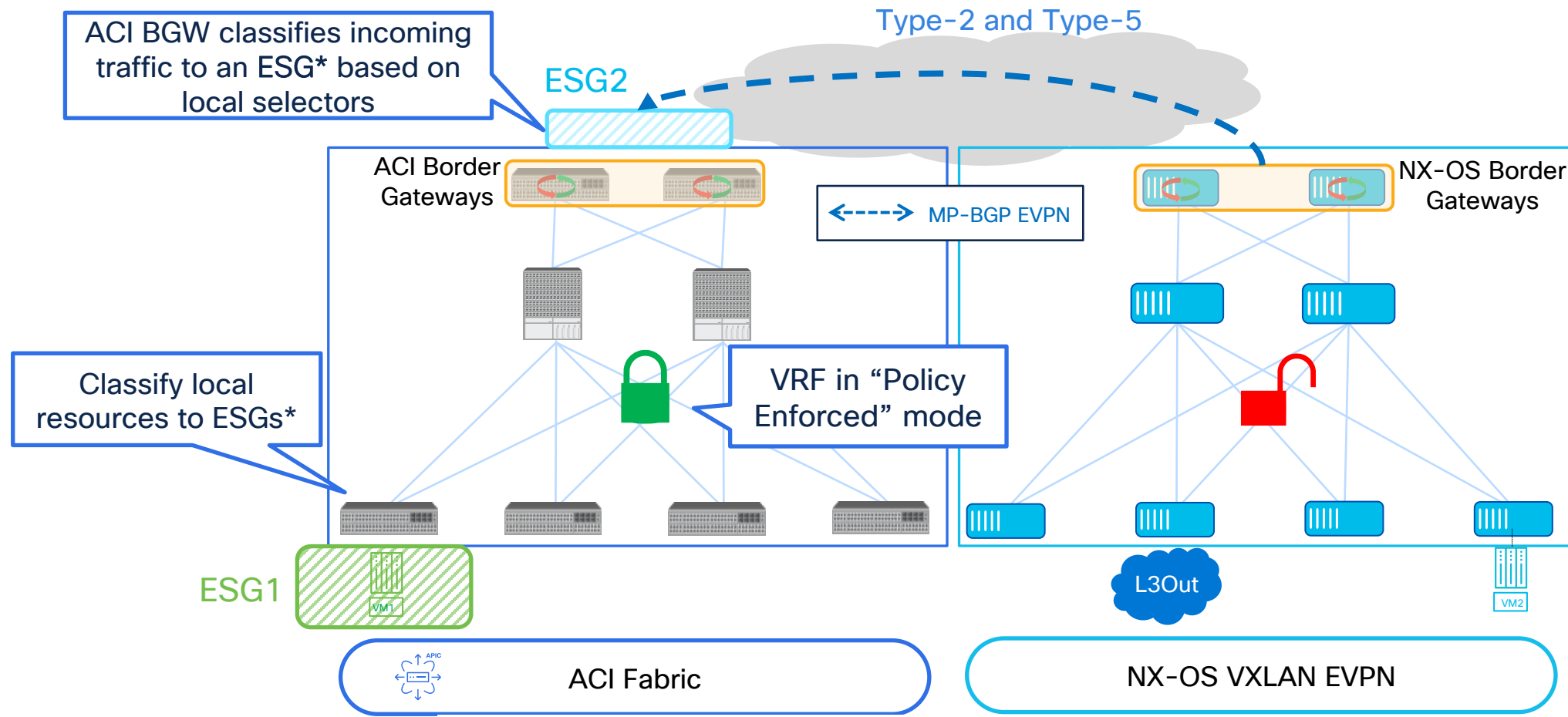
Removes the old contracts consumed/provided by the EPGs and any EPG config required for route-leaking

Use Case 1

Cisco ACI to Policy Unaware VXLAN EVPN

Cisco ACI to Policy Unaware VXLAN EVPN

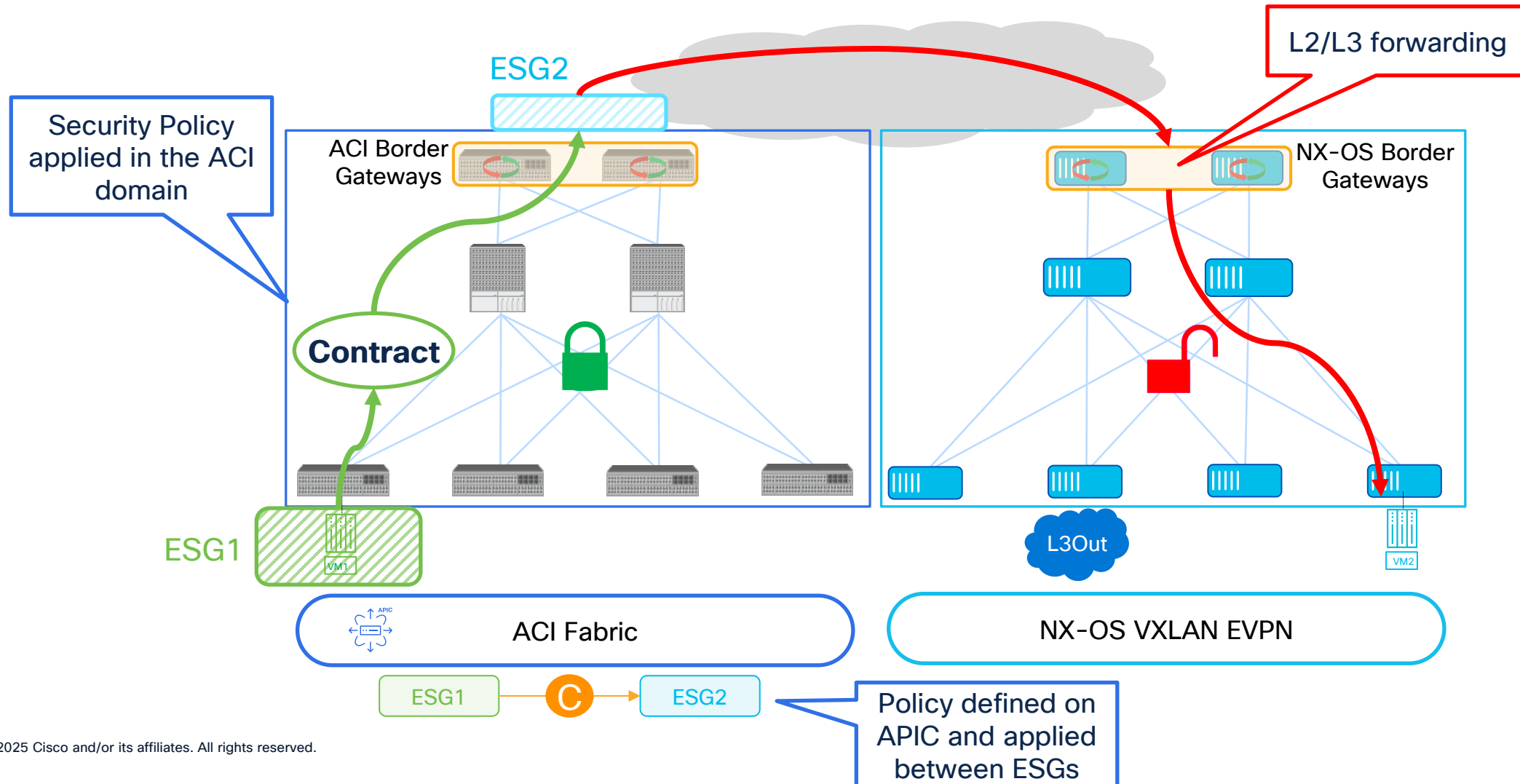
Classification and Enforcement only on Cisco ACI



*Nexus ONE mandates the use of Endpoint Security Groups (ESGs) in ACI for classification and enforcement. EPG to ESG migration procedure ("uplifting") should be performed upfront.

Cisco ACI to Policy Unaware VXLAN EVPN

Classification and Enforcement only on Cisco ACI

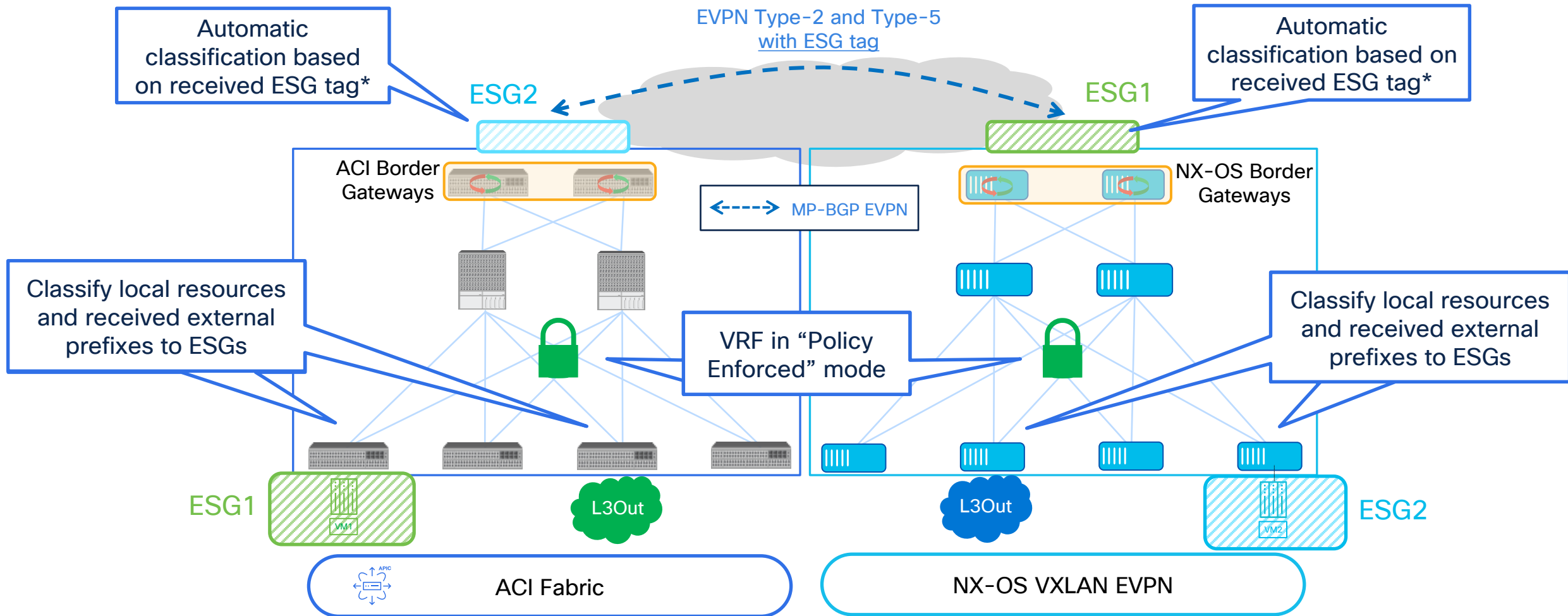


Use Case 2

Cisco ACI to Policy Aware VXLAN EVPN

Cisco ACI to Policy Aware VXLAN EVPN

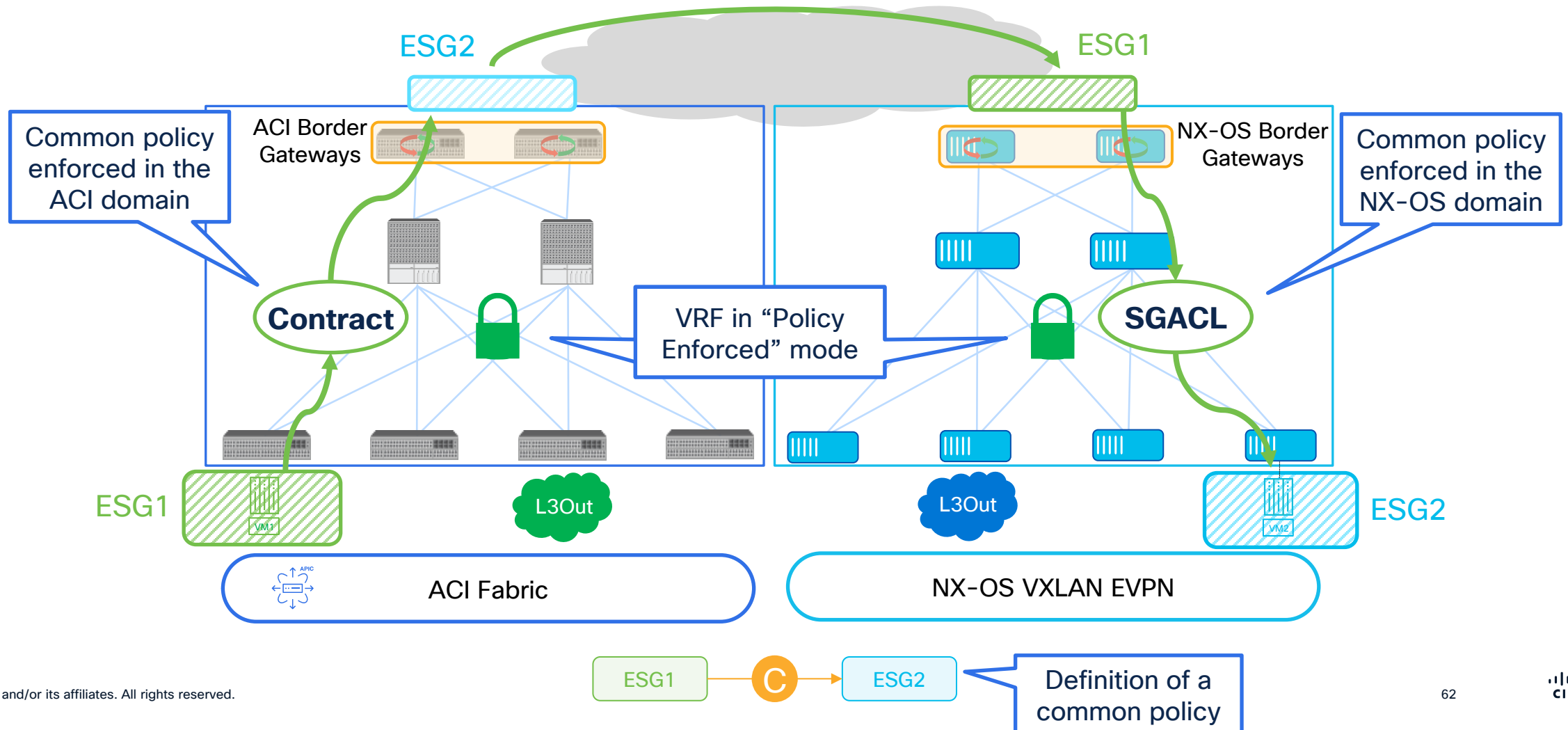
Classification and Enforcement in both Domains



*Tag normalization performed on the ACI BGWs

Cisco ACI to Policy Aware VXLAN EVPN

Classification and Enforcement in both Domains

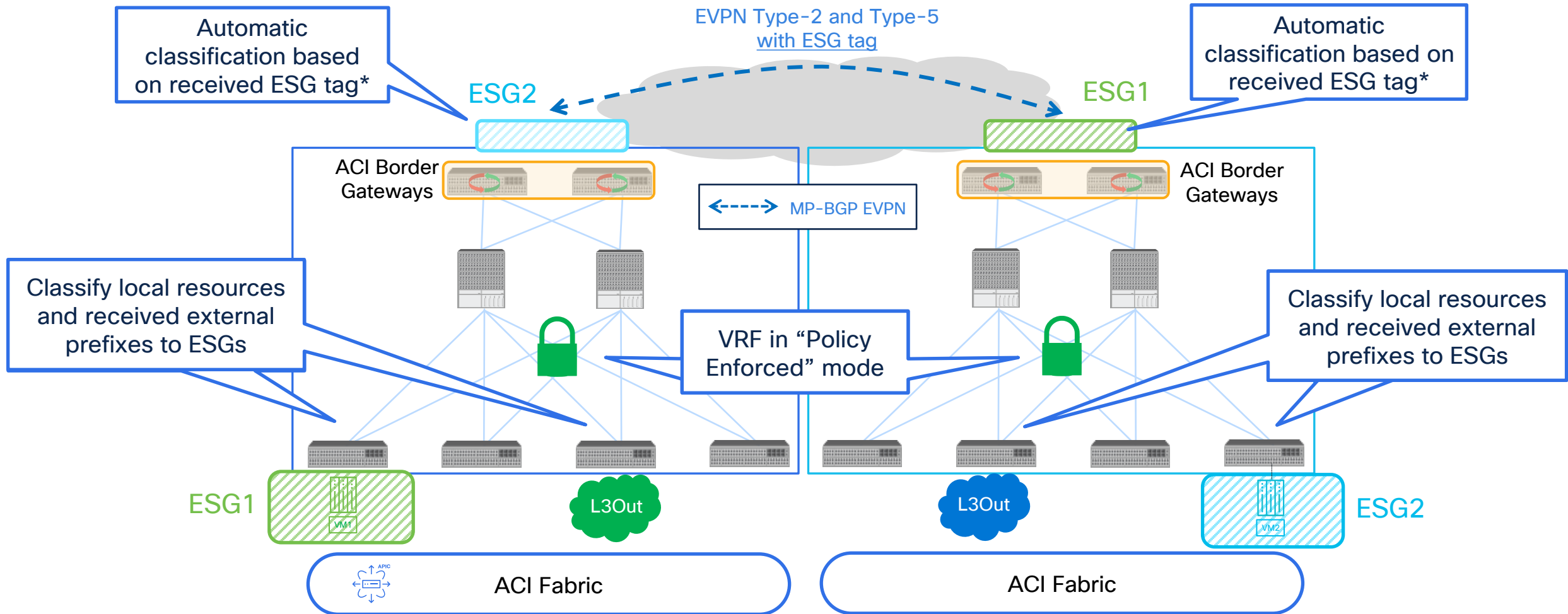


Use Case 3

Cisco ACI to Cisco ACI

Cisco ACI to Cisco ACI

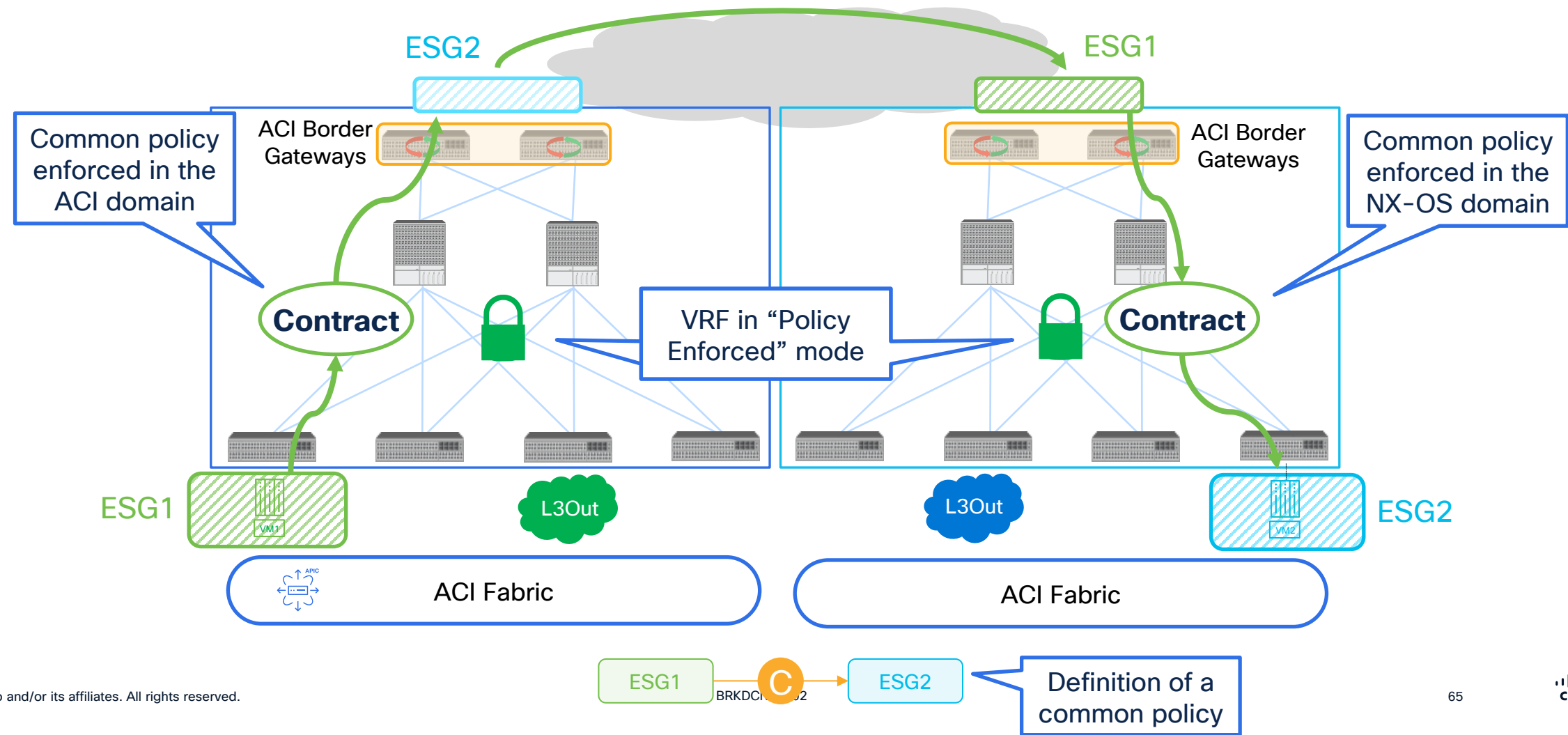
Classification and Enforcement in both Fabrics



*Tag normalization performed on the ACI BGWs

Cisco ACI to Cisco ACI

Classification and Enforcement in both Fabrics



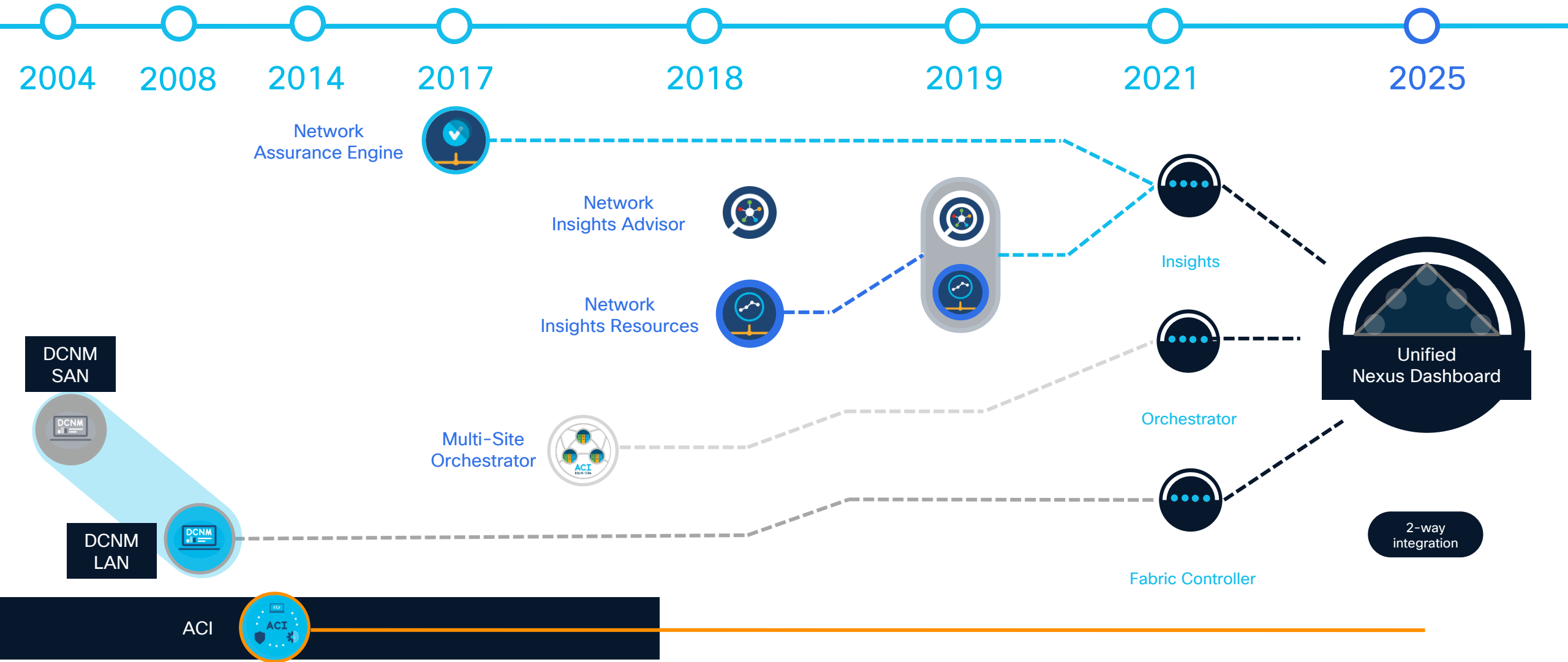
Unified Nexus Dashboard

For More Information on Unified Nexus Dashboard please refer to PSODCN-1009 from Cisco Live San Diego:
<https://www.ciscolive.com/on-demand/on-demand-library.html?search=PSODCN-1009#/session/1750271880376001z7Ob>

We Have Embarked on a Journey

Towards Simplification and Unification

 Products have evolved through the years with microservices-based architectures & other enhancements



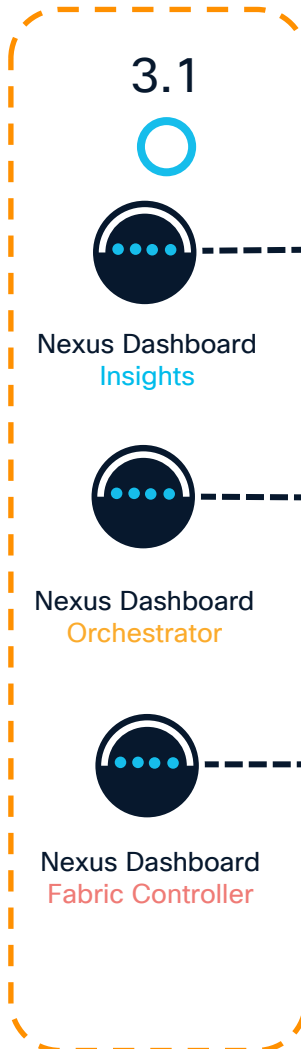
Nexus Dashboard – Unified What?

A Journey of Combining Six Products into One

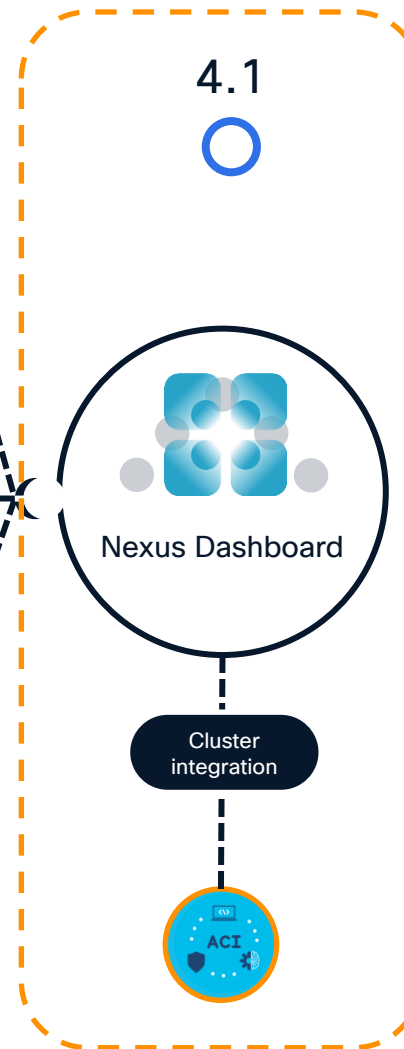
Unified Image

- Single Image Installation
- All Services pre-installed (NDO/NDI/NDFC)
- Service versions bound to ND version

Unified Image



Unified Product



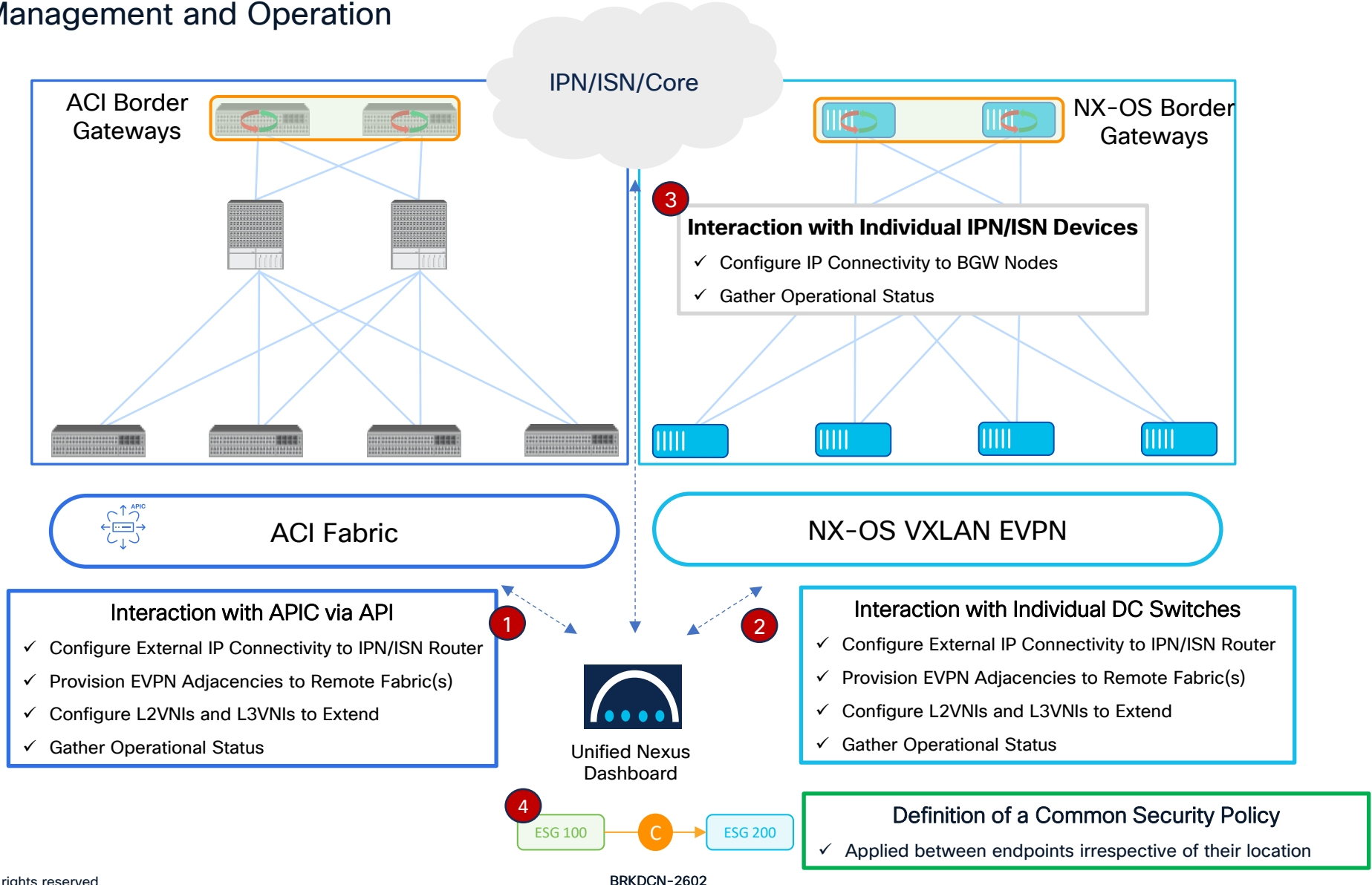
Unified Product

- Single Image Installation
- Services merged into base OS
- Originally separate services have now become ND Capabilities: [Automation](#), [Orchestration](#), [Telemetry](#)

Unified Nexus Dashboard

ND 4.2

Single Point of Management and Operation



ND 4.2

Nexus Dashboard

Q

🔔

?

|

admin

vND-184

Home

Manage

Analyze

Admin

Fabrics

Fabrics

Fabric groups

Refresh

Filter by attributes

Actions

Name	Type	Anomaly level	Advisory level	License tier	ASN	Connectivity status	Fabric group	Features
 ACI-Fabric01	ACI	 Critical	 Not Applicable	Premier	65529	 Up	N/A	-
 External_Fabric	External and Inter-Fabric Connectivity	 Major	 Not Applicable	Premier	65530	 Up	N/A	-
 fab1	Data Center VXLAN EVPN - IBGP	 Not Applicable	 Not Applicable	Essentials	65531	 Up	N/A	-

3 items found

Rows per page101

Unified Nexus Dashboard

Creation of a New Fabric Group

ND-SYS-1

Home

Manage

Analyze

Admin

Fabrics

Fabrics

Fabric groups

Refresh

Fabric Groups

Create a group of fabrics with common attributes for visualization purposes and simpler management.

Filter

☐	Group name	Member fabrics	Type	
☐	MSD Fabric Group	Anchorage, Melbourne	VXLAN	
☐	IPFM Fabric Group	San Jose, San Francisco	IPFM	
☐	Classic Fabric Group	Asheville, North Carolina	Classic	

Rows per page 10 < 1 2 ... 10 >

Creation of a new Fabric Group

Unified Nexus Dashboard

Selecting an Heterogenous Fabric Group

ND-SYS-1

Home

Manage

Analyze

Admin

← Back

Create Fabric Group

1 Settings

2 Advanced fabric group settings

3 Summary

Settings

Name *

ACI-NX Unified Fabric Group

Type *

VXLAN

VXLAN Group can contain individual VXLAN, External, Enhanced Classic LAN/ACI fabrics, and Campus VXLAN EVPN fabrics. This type of group allows shared deployments for VXLAN overlays (Networks and VRFs) and fabric interconnectivity.

Classic

Classic Group can contain Enhanced Classic LAN/Classic-LAN/External fabrics. This group allows for a combined visualization at a topology level. No group level deployments are available in this fabric group.

IPFM

IPFM Group can contain individual PFM/IPFM-Classic/Classic-LAN fabrics. This type of group allows shared host and flow definitions.

Fabric group type

VXLAN

VXLAN

This fabric group enables interconnection of Data Center VXLAN EVPN fabrics, Campus VXLAN EVPN fabrics, and external fabrics through VXLAN EVPN Multi-Site.

VXLAN-ACI

This fabric group enables interconnection of ACI and VXLAN EVPN fabrics via border gateways.

Cancel

Next

Creation of a heterogeneous Fabric Group

Unified Nexus Dashboard

Add Member Fabrics to the Fabric Group

ND-SYS-1

Home

Manage

Analyze

Admin

← Fabrics

ACI-NX Unified Fabric Group

OverviewInventoryConnectivitySegmentation and securityConfiguration policiesAnomaliesHistory

Anomaly level Critical

4 total critical anomalies, out of which 2 occurred in the last week



Edit Image

General

Group name
ACI-NX Unified Fabric Group

Type
VXLAN

Tags

+ Add

Config-sync status

In-Sync

Interfaces

PhysicalAll

150 total

Up (90)

Down (50)

Admin down (1)

Security and segmentation

Tenants
12

VRFs
12

Security groups
5

Networks
8

Recent Activity

Fabric San Jose was removed from MSD-1

2 minutes ago

Fabric Melbourne was added to MSD-1

2 minutes ago

MSD-1 was edited by admin

2 minutes ago

View all activity

Inventory

2 Fabrics

5 Switches

2 VPC domains

2 Other devices

Connectivity

L3 neighbors
3

Interfabric
3

Refresh

Actions

Add member fabric

Recalculate and deploy

Add the different fabric types to the Fabric Group

Unified Nexus Dashboard

Provision underlay connectivity (BGWs and ISN devices) and EVPN Adjacencies between BGWs

vND-184

Home

Manage

Analyze

Admin

Nexus Dashboard

admin

Refresh

View in topology

Actions

Edit fabric group settings

Add child fabric

Recalculate and deploy

Configuration

Maintenance

Overview

Inventory

Connectivity

Segmentation and security

Configuration policies

Anomalies

History

Child Fabrics

Switches

VPC pairs

Other devices

Filter by attributes

Name	Type	Anomaly level	Advisory level	License tier	ASN	Connectivity status	Software version	Security group status
ACI-Fabric01	ACI	Critical	Not Applicable	Premier	65529	Up	10.5(3)	Disabled
External_Fabric	External and Inter-Fabric Connectivity	Major	Not Applicable	Premier	65530	Up	7.0(3)I4(2)9.3(1)	-
fab1	Data Center VXLAN EVPN - iBGP	Not Applicable	Not Applicable	Essentials	65531	Up		-

Run “Recalculate and Deploy” to provision:

➤ Underlay adjacencies between BGWs and ISN devices

➤ Overlay MP-GP EVPN adjacencies between BGWs

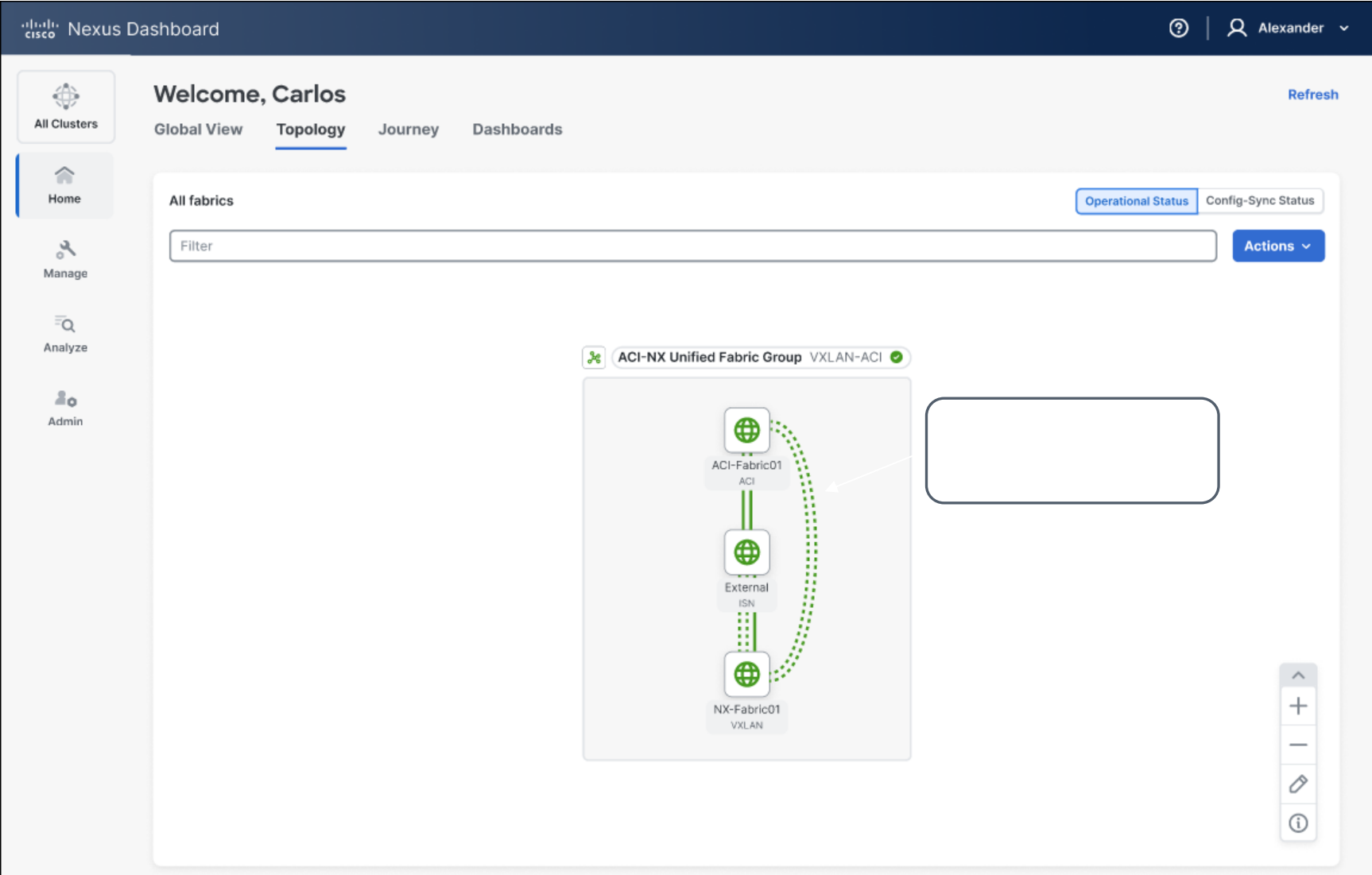
© 2025 Cisco and/or its affiliates. All rights reserved.

BRKDCN-2602

76

Unified Nexus Dashboard

Topology View



Unified Nexus Dashboard

Create Networks (or VRFs)

ND-SYS-1

Home

Manage

Analyze

Admin

← Fabrics

ACI-NX Unified Fabric Group

Refresh

Actions

Overview

Inventory

Connectivity

Segmentation and security

Configuration policies

Anomalies

History

Networks

VRFs

Security groups

Security contracts

Security associations

Protocol definitions

L4-L7 services

Tenants

Filter

Actions

☐	Name	Tenant	VRF	IP prefix	Config-sync
☐	Net-100001	tenant1	vrf-1	6.6.6.6	Deployed
☐	Net-100002	tenant1	vrf-1	6.6.6.6	Deployed

Create network

Edit

Configure fabric stretch

Multi-attach

Multi-detach

Deploy

Delete

Rows per page

10

<

1

2

...

10

>

Unified Nexus Dashboard

Deploy the Overlay Configuration

ND-SYS-1

Home

Manage

Analyze

Admin

← Back

Deploy Configuration

Recalculate and deploy configuration for ACI-NX Unified Fabric Group

1

Config preview

2

Deploy progress

Filter

Resync all

Tenant name	Fabric name	Switch name	IP address	Role	Fabric status	Pending config	Diff
Tenant-1	ACI-Fabric01	—	—	—	✖ Out of sync	4000	+200 -20
▼ Tenant-1	VXLAN-Fabric1						
		Spine1	5.5.5.5	Spine	✖ Out of sync	61	+40 -60
		Spine1	5.5.5.5	Spine	✖ Out of sync	61	+40 -60
▼ Tenant-1	VXLAN-Fabric2						
		Spine1	5.5.5.5	Spine	✖ Out of sync	61	+40 -60

Cancel

Deploy all

Conclusions

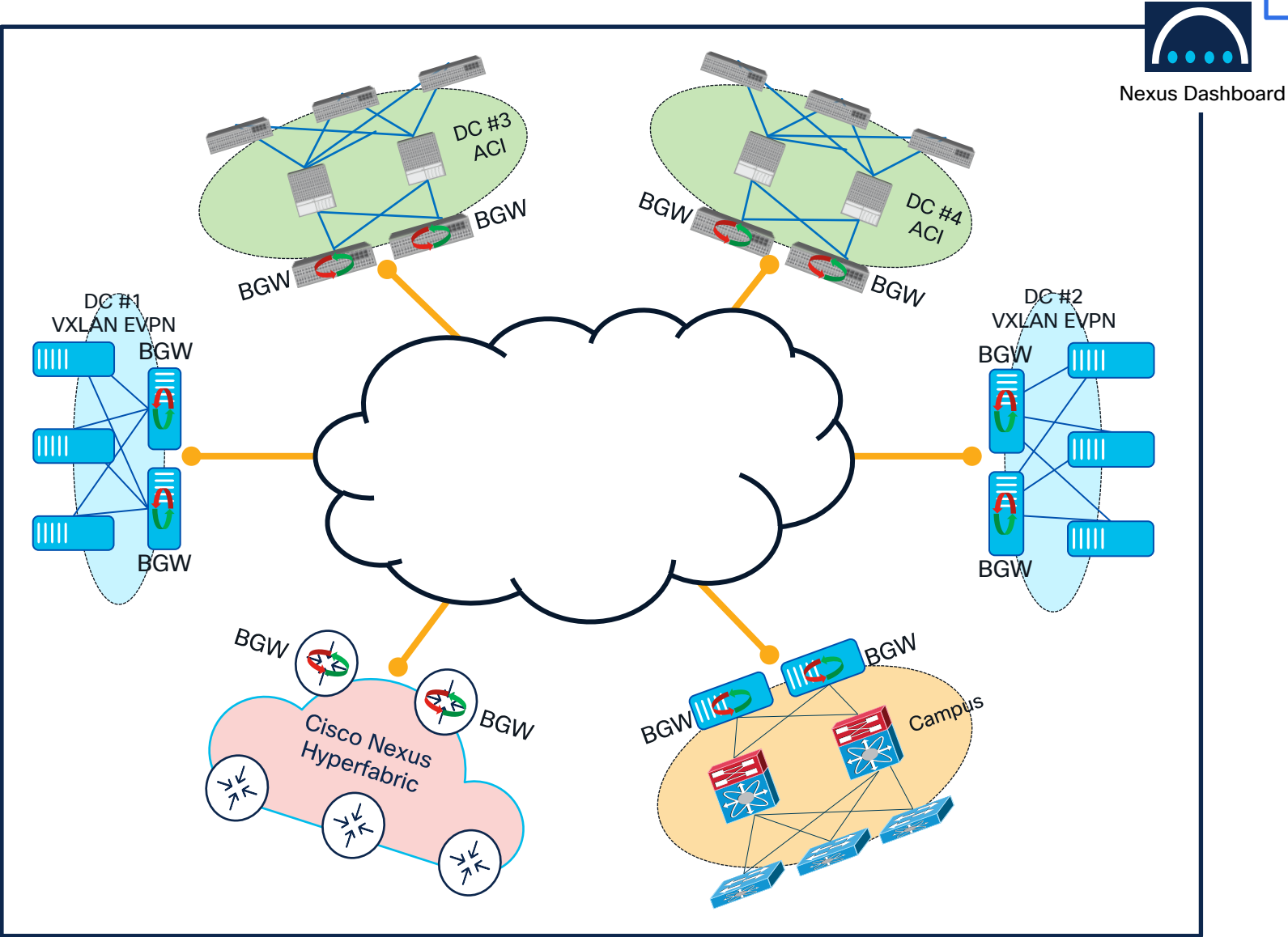
Conclusions

- Building distributed infrastructures is key to the deployment of resilient and scalable designs
- Cisco Nexus One Architecture aims to seamlessly interconnect and operate a mix of heterogeneous fabrics (ACI and VXLAN EVPN)
- The three main functional components of Cisco Nexus One are:
 1. BGW function for ACI fabrics
 2. Security policies in VXLAN EVPN fabrics (GPO)
 3. Introduction of centralized management and operation platforms for heterogeneous fabric on Nexus Dashboard

Nexus ONE Future Evolution

Strategic Vision

For More Information on Cisco Nexus Hyperfabric please refer to [BRKDCN-2944](#)



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

