



MultiCloud Solutions Anywhere

Any Workload, Any Location, Any Cloud

Nyein Chan Tun

System Engineer, Cisco

Jan 2023



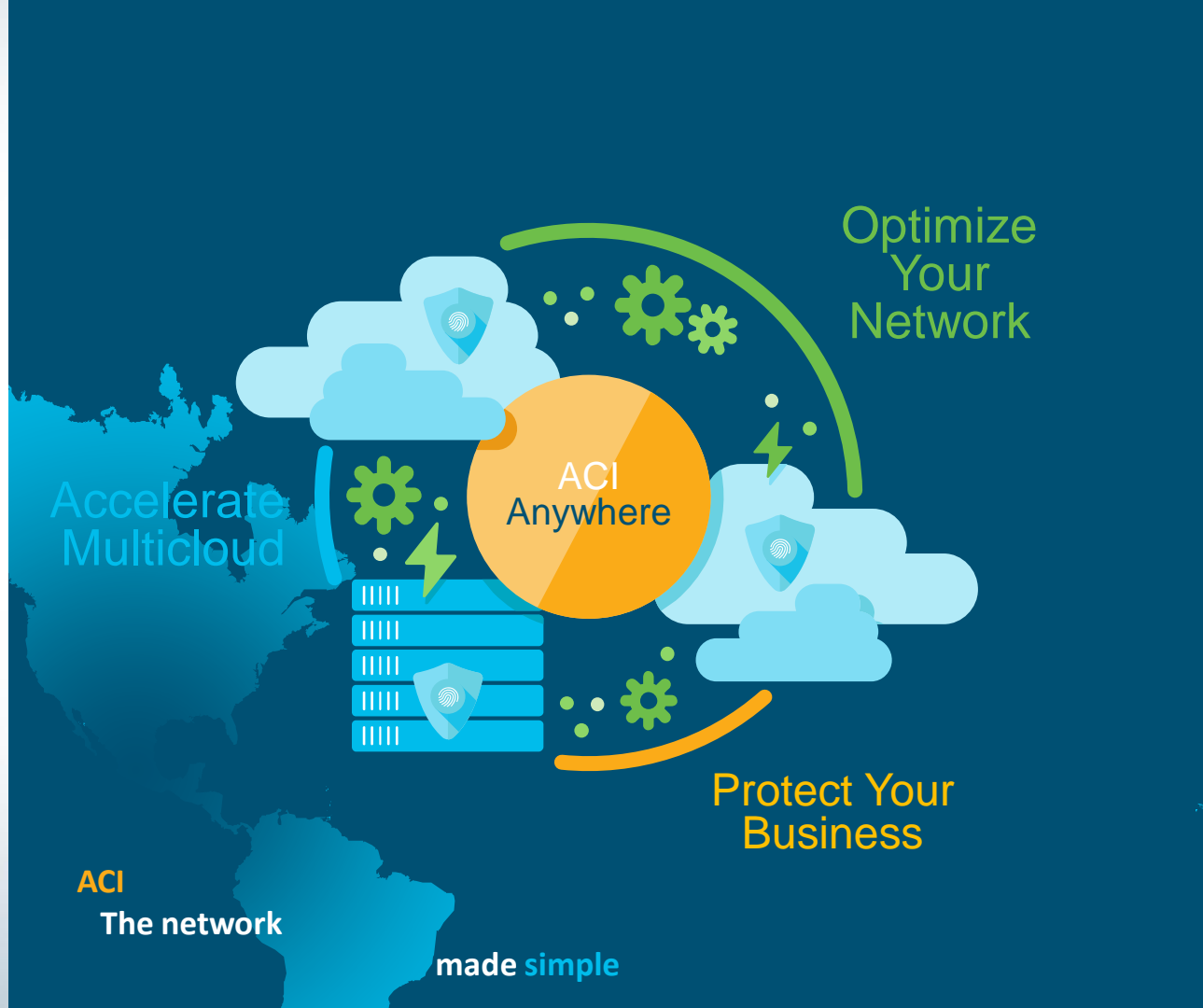
Introduction to ACI (Application Centric Infrastructure)

Cisco ACI

Simpler & better networking for your business

Any DC network: Any Size, Anywhere, Any form

Based on **Nexus 9000** covering any bandwidth (100Mbps – 400Gbps)



Accelerate
Multicloud

ACI
Anywhere

Optimize
Your
Network

Protect Your
Business

ACI
The network

made simple



ACI
The network



Optimize Your Network

- **Single** point of configuration and troubleshooting
- Turnkey network **automation**
- Security / L4-7 **automation**
- **Scale** within/across DCs and geographies
- **Simplify** DC Interconnect
- Seamless integration of **underlay and overlay**



ACI
The network



Protect Your Business

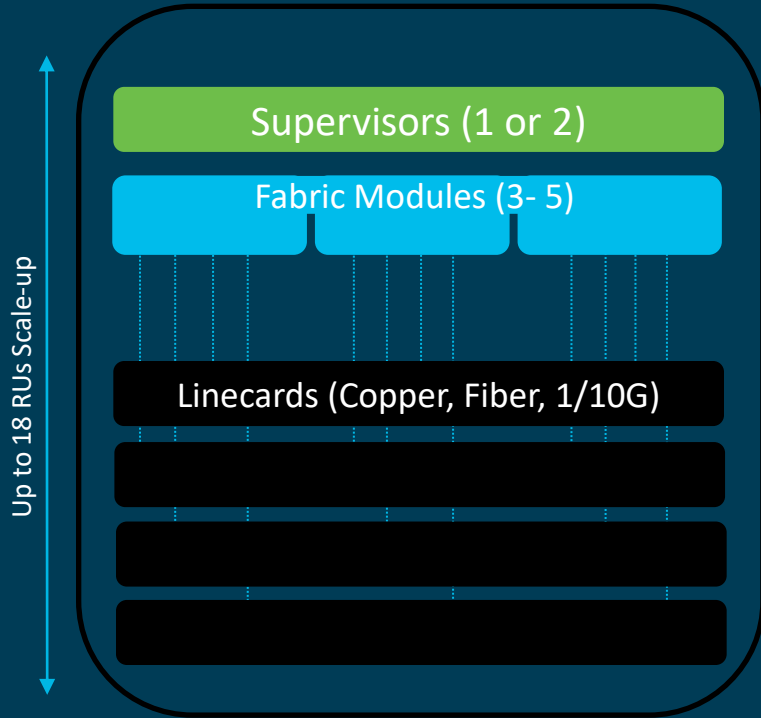
- **Business continuity** and disaster recovery
 - **3-second** rollback
- **Pervasive** security policy
- MacSec/CloudSec **Encryption**
- **Security** at scale with performance
- **Segmentation** for any load (not **just VMWare**)
- **May integrate** to **Tetration Analytics/NAE** for deeper security & assurance



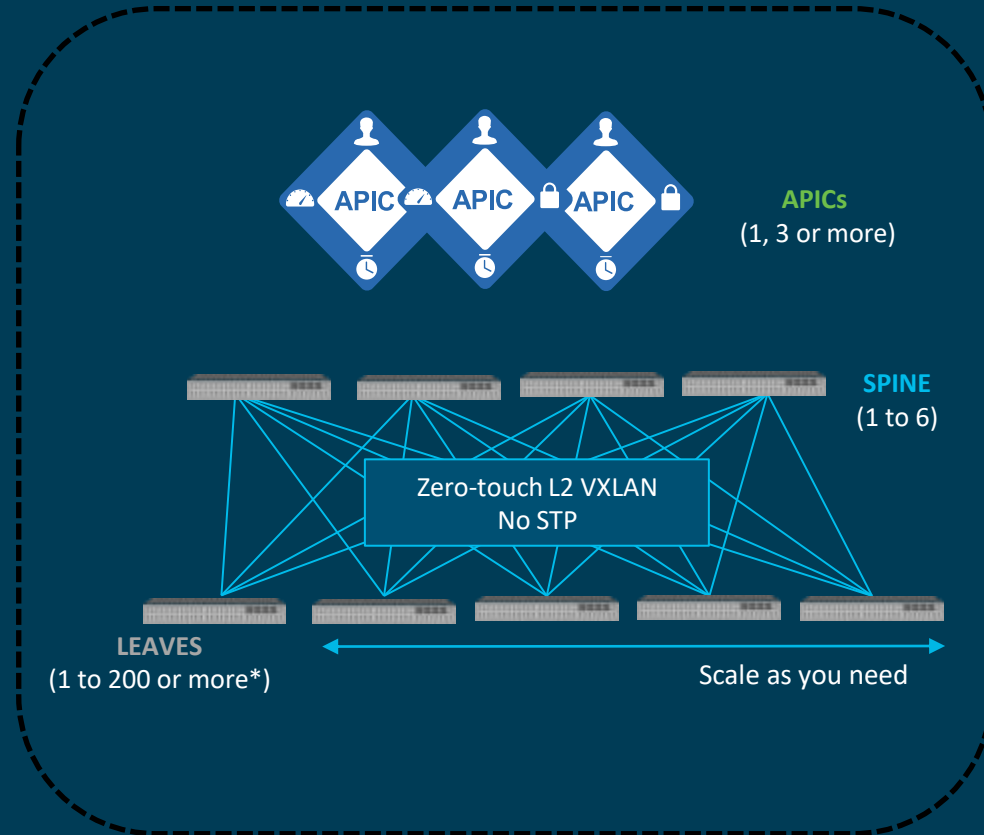
Accelerate Multicloud

- **Single policy and seamless connectivity** across any data center and public cloud
 - **Multiple** Pods, Sites, Clouds, Hypervisors,
 - **Any** workload, **any** location, **any** cloud
- Cloud automation integration through: APIs, vRealize, AzurePack, OpenStack, UCSD, ACI Plugin for VMWare vCenter, Azure Stack, Red Hat Virtualization Manager, Kubernetes Integration, OpenShift Integration, PCF Integration, ServiceNow, SCVMM.

The DC network **before** Classic modular switching



The DC network **NOW** **ACI**



ACI: The elements

APICs

3 Recommended for **Production**
At least 1 **physical** APIC required

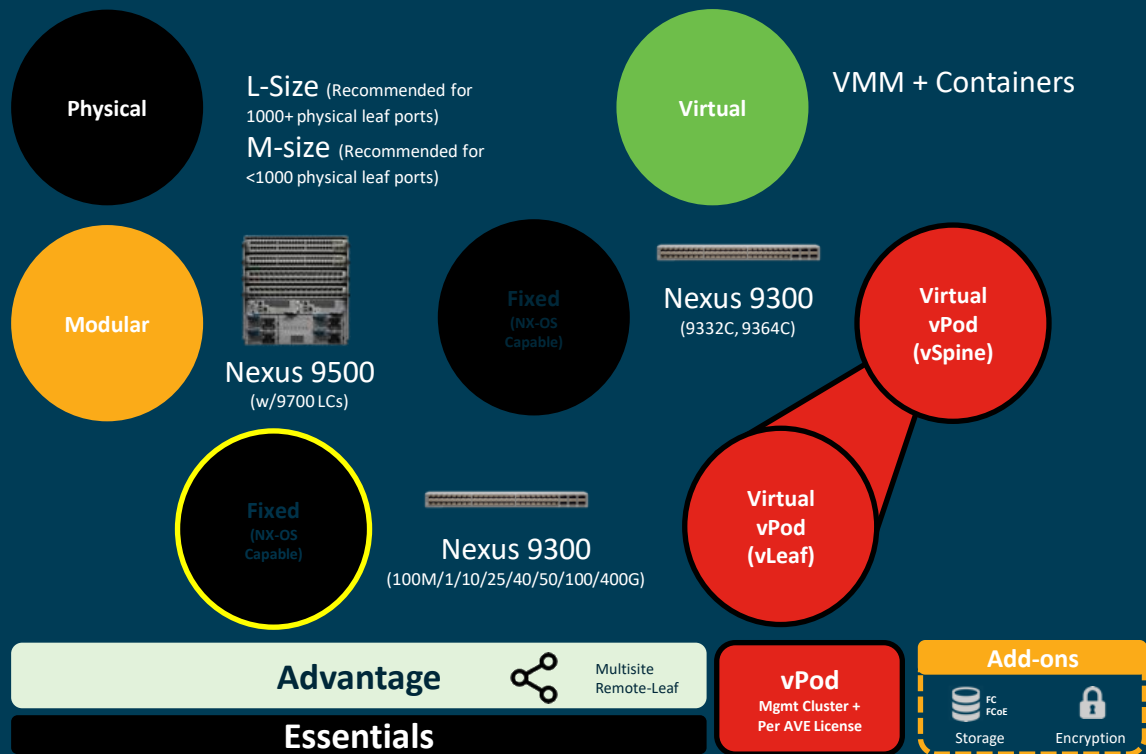
SPINES

LEAVES

Virtual/Container networking integration
included (except vPod mode)

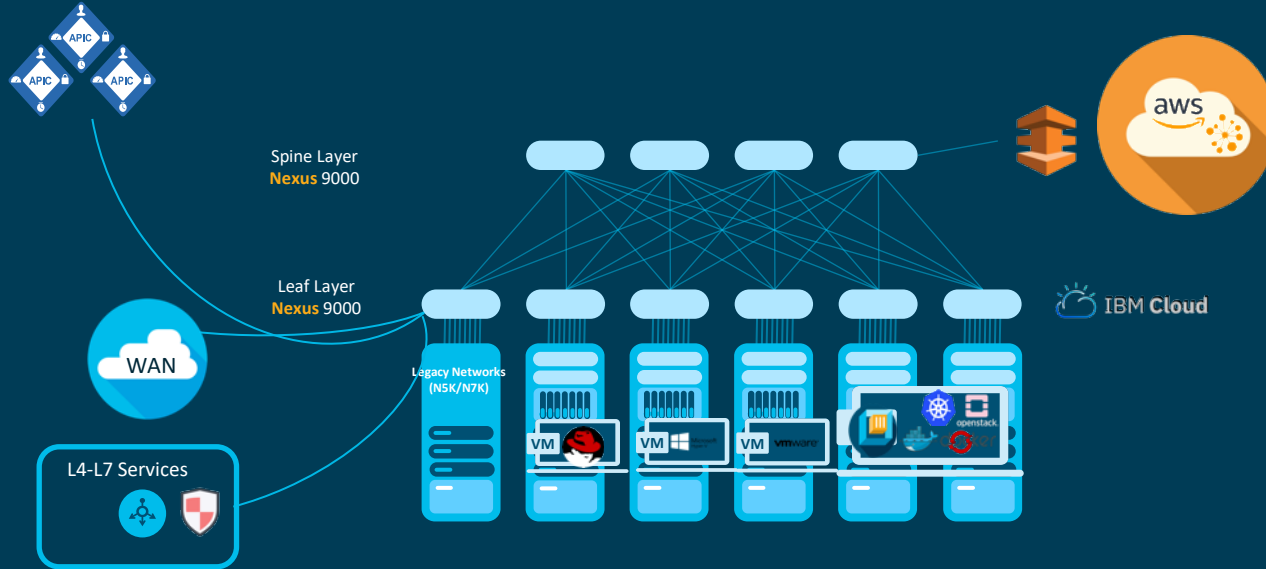
LICENSING

Only applies to **Physical** Leaves
(no licensing on APICs nor Spines)



ACI: Consistent, automated and simpler networking

Single point of management for all your Physical, Virtual, Container-based and Cloud Networking



ACI

The network made simple

Understanding ACI Discovery, Protocols and Automation



Fully Automated

TEP Pool: 192.168.0.0/16
Infra VLAN: 4093

APIC

APIC

APIC

APICs

BGP RR

SPINE NODES

MP-BGP

VXLAN

VTEPs

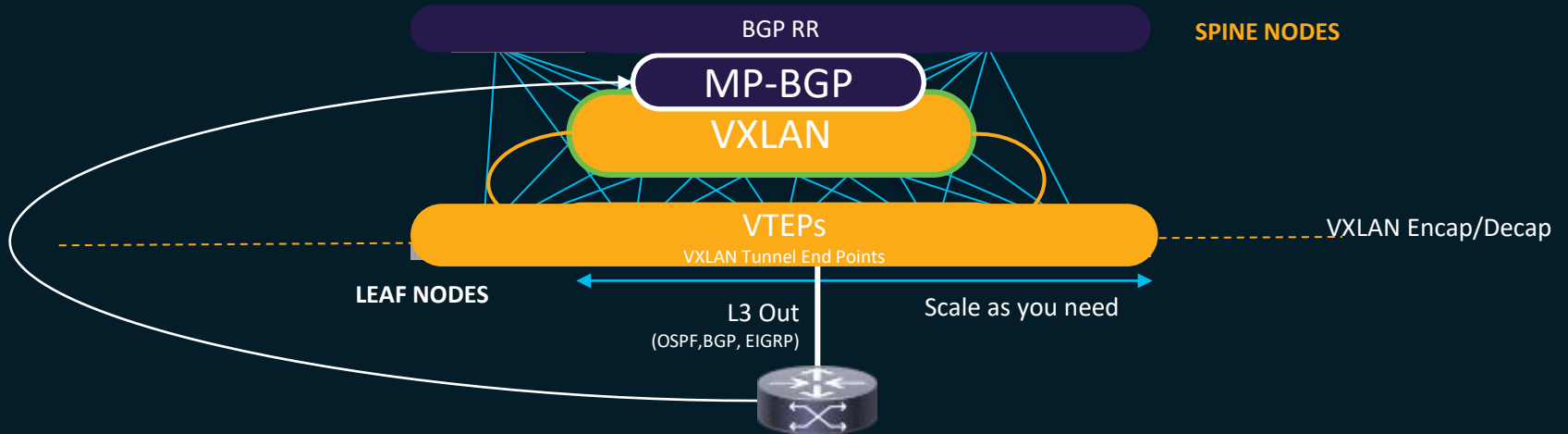
VXLAN Tunnel End Points

VXLAN Encap/Decap

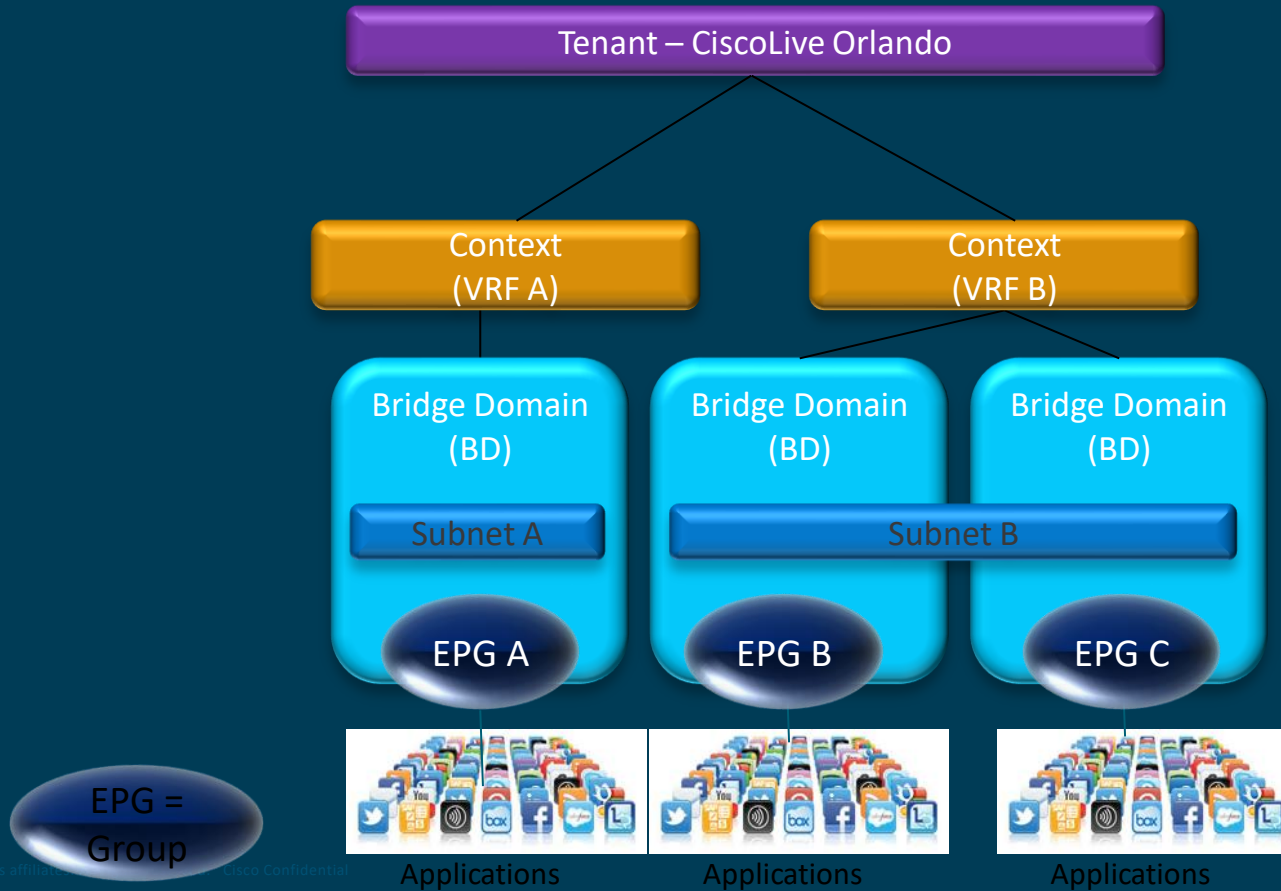
LEAF NODES

L3 Out
(OSPF, BGP, EIGRP)

Scale as you need



ACI Policy Model



ACI Policy Model: EPG To EPG Communication



Zero Trust Security Model

- Need to define a Contract (Policy); - A **contract** is used to specify the interaction between **two EPG(s)**, a provider/consumer pair.
- The goal is to provide a global policy view that focuses on improving automation and scalability.
- You have the option to change the default from white-list to Unenforced VRFs; IP Any Any.

ACI Anywhere

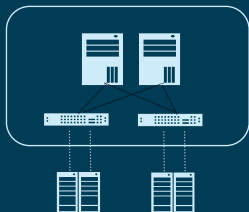
Any Workload, Any Location, Any Cloud



ACI Anywhere



Remote Leaf / Virtual Pod



Multi-Pod / Multi-Site



Multi-Cloud Extensions



Remote Location

On Premises

Public Cloud

Security Everywhere



Analytics Everywhere



Policy Everywhere

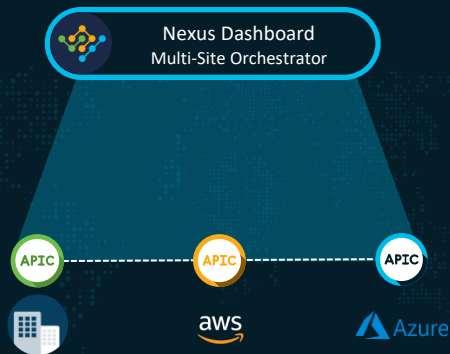


Single Site ACI



Separate management and configuration per site (isolated sites)

Multi-Site ACI



Single management and logical network configuration with automated interconnect

You can run ACI anywhere your business takes you

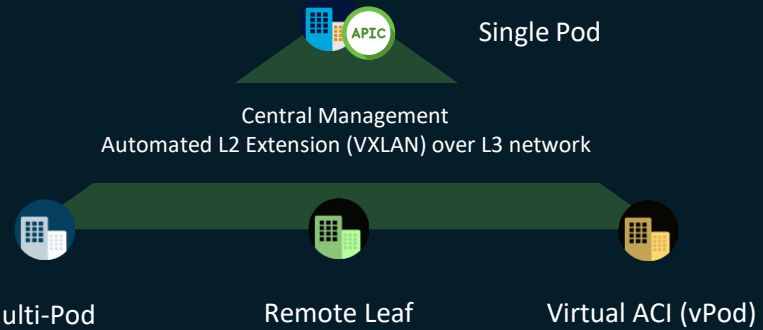
Single Site ACI

On-Premises

Active-Active Data Centers

DC/Pod Interconnect

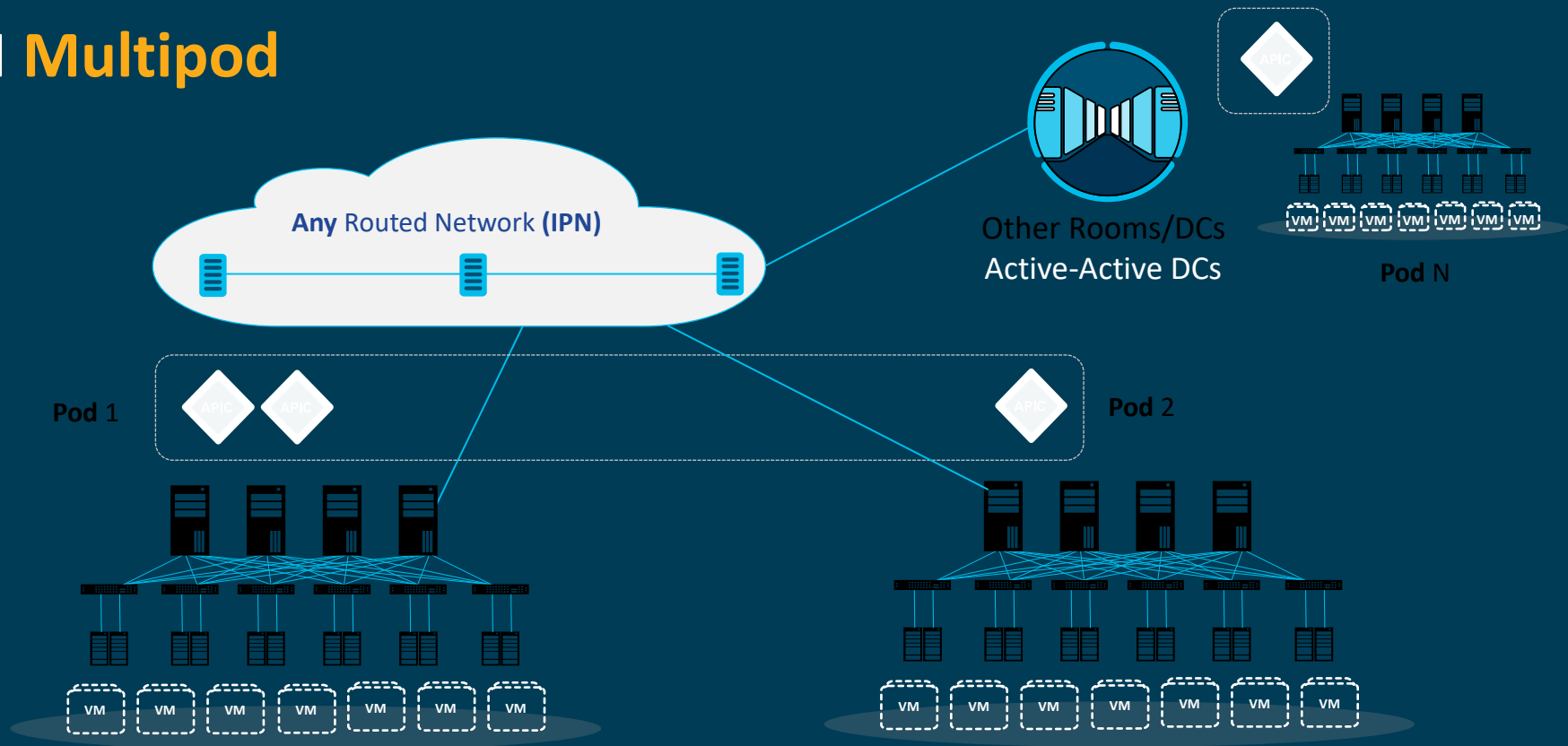
Co-Lo and Regional Data Centers



General L3 network requirements: Payload MTU (add 50+ bytes) & DHCP Relay to APIC

A single on-prem ACI Site can extend to multiple locations

ACI Multipod



Multicast on IPN needed
& **Jumbo Frames** (≤ 1550)

≤ 50 ms RTT Required
Up to **12** Pods, distributed gateway

Single central management (APIC)
Automated **L2 DCI VXLAN extension**

Single Site ACI

On-Premises

ACI Multi-Pod

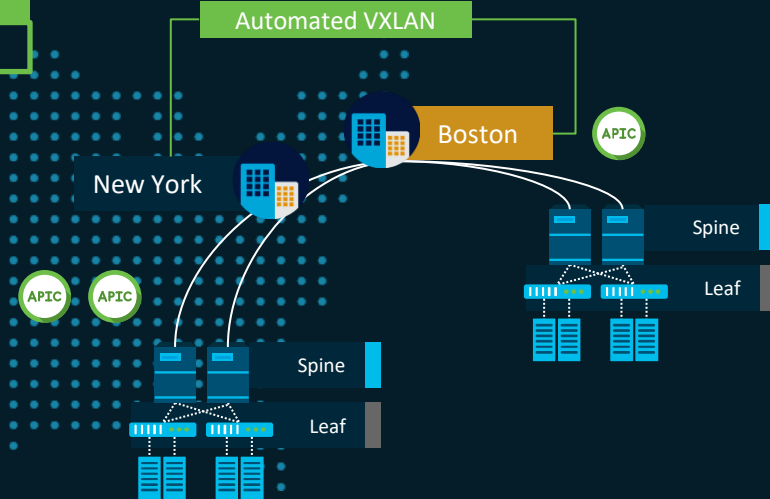
2 Pod Back-to-Back

Active-Active Data Centers

DC/Pod Interconnect

Co-Lo and Regional Data Centers

Automated VXLAN



Common deployments

High-bandwidth

Dark Fiber, NCS, 400G

Extend L2, Active-Active DCs

Requires **ACI 5.2** and later versions

A single on-prem ACI Site can extend to multiple locations

Single Site ACI

On-Premises

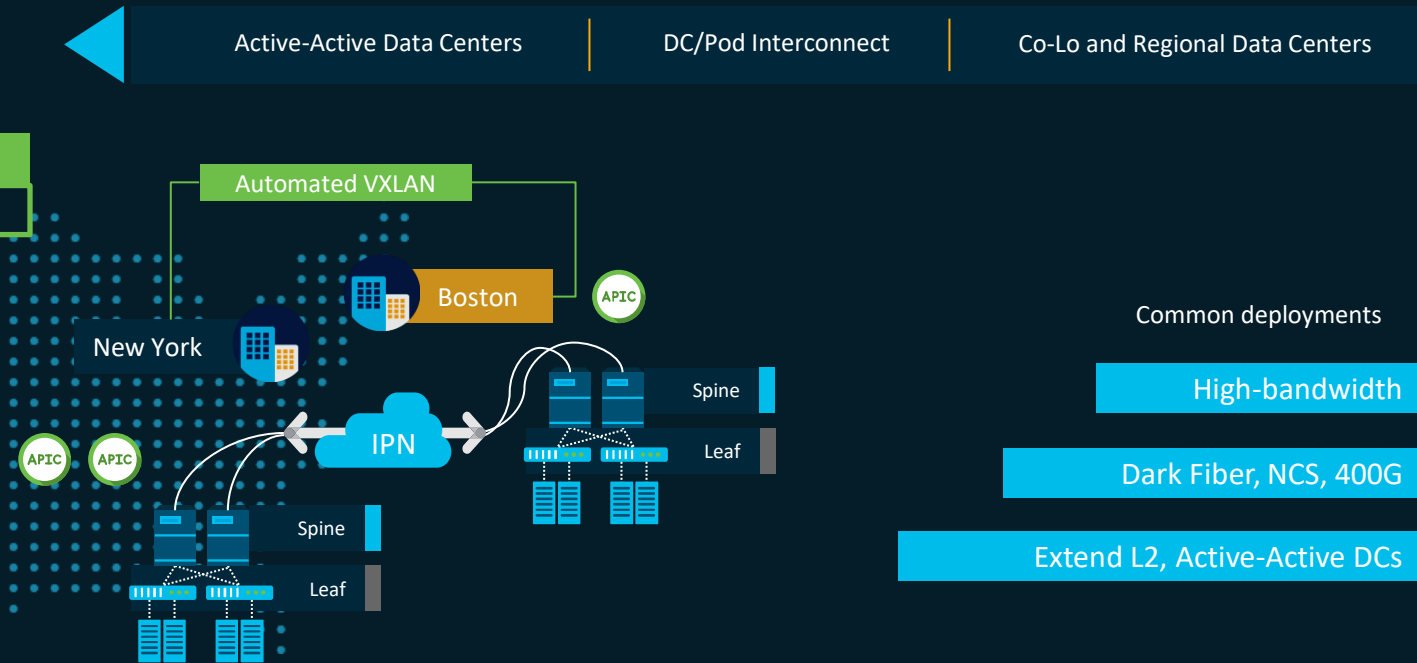
ACI Multi-Pod

3-12 Pods

Requires an Inter-Pod routed Network (IPN) with*:

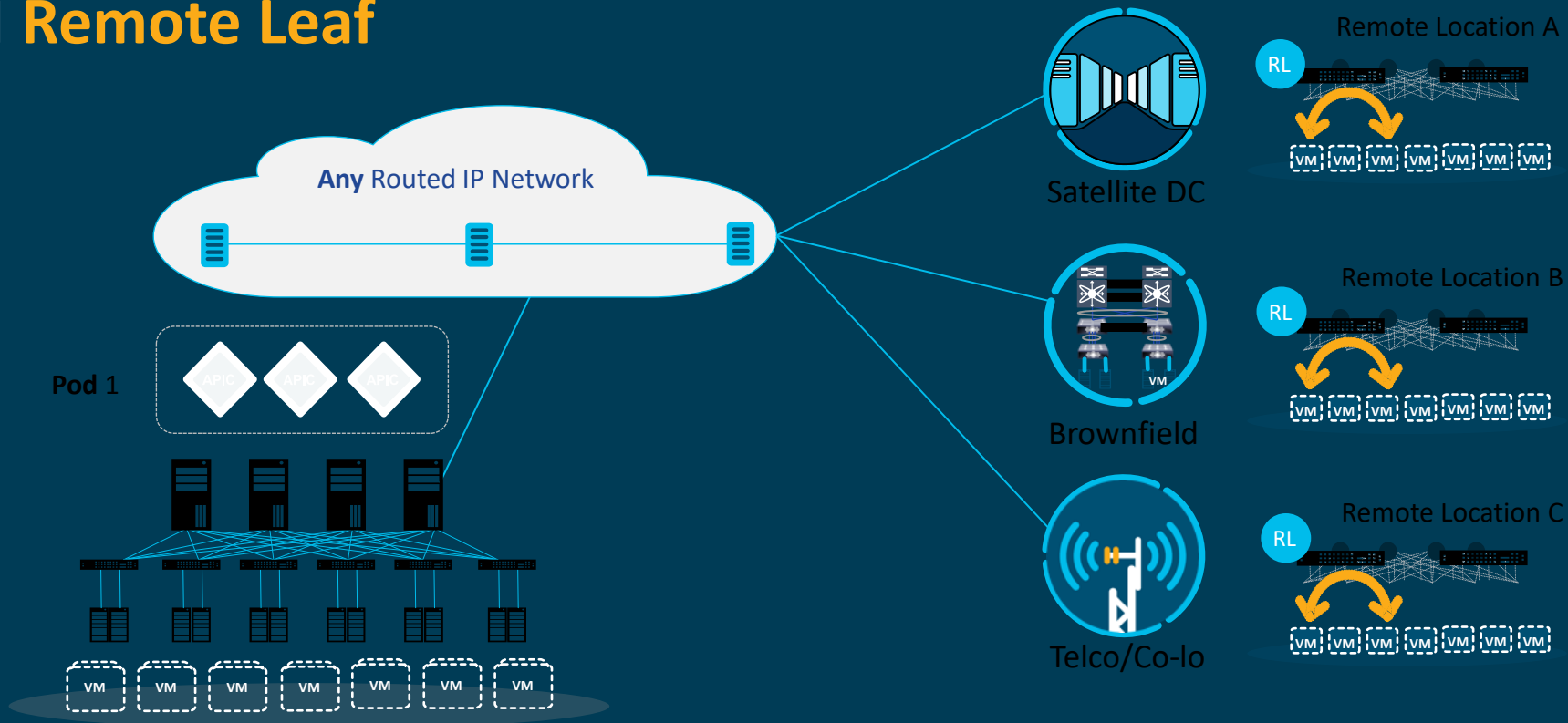
Less than 50 ms in RTT
Multicast support for BUM (PIM-bidir)

Spines on each pod connect to IPN first-hop using OSPF on VLAN 4



A single on-prem ACI Site can extend to multiple locations

ACI Remote Leaf

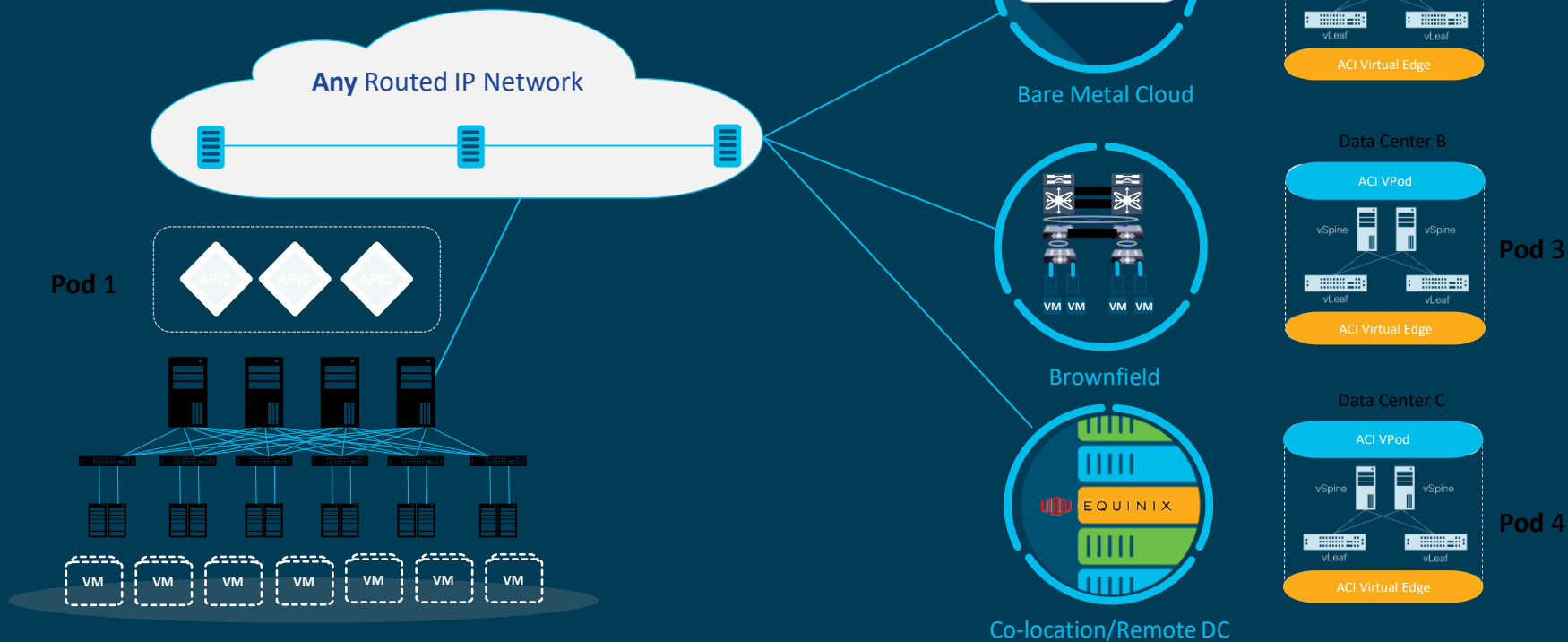


Zero Touch Auto Discovery of Remote Leaf

<= 300 ms RTT Required
Up to **20** Remote Locations

Single central management
Automated **L2 VXLAN extension**

ACI vPod



Virtual Spine/Leaf Functionality
w/**AVE** integration

Up to **64** AVEs per vPod

Single central management
Automated **L2 VXLAN extension**

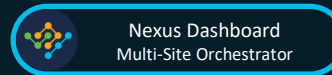
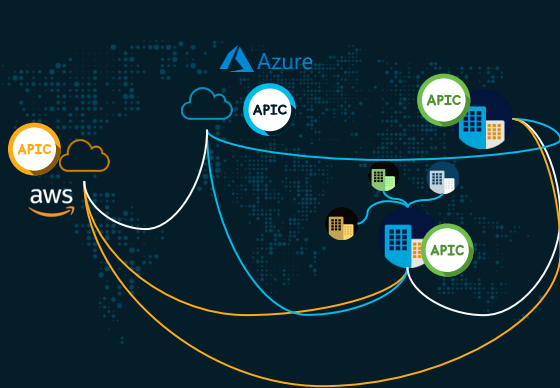
Multi-Site ACI

On-Prem & Cloud

Business continuity/DR/DRaaS

DC/Cloud Interconnect

VM Mobility & Cloud Migration



Central Management
Automated VXLAN and MP-BGP



ACI site(s) (On-prem)



Cloud ACI (AWS)

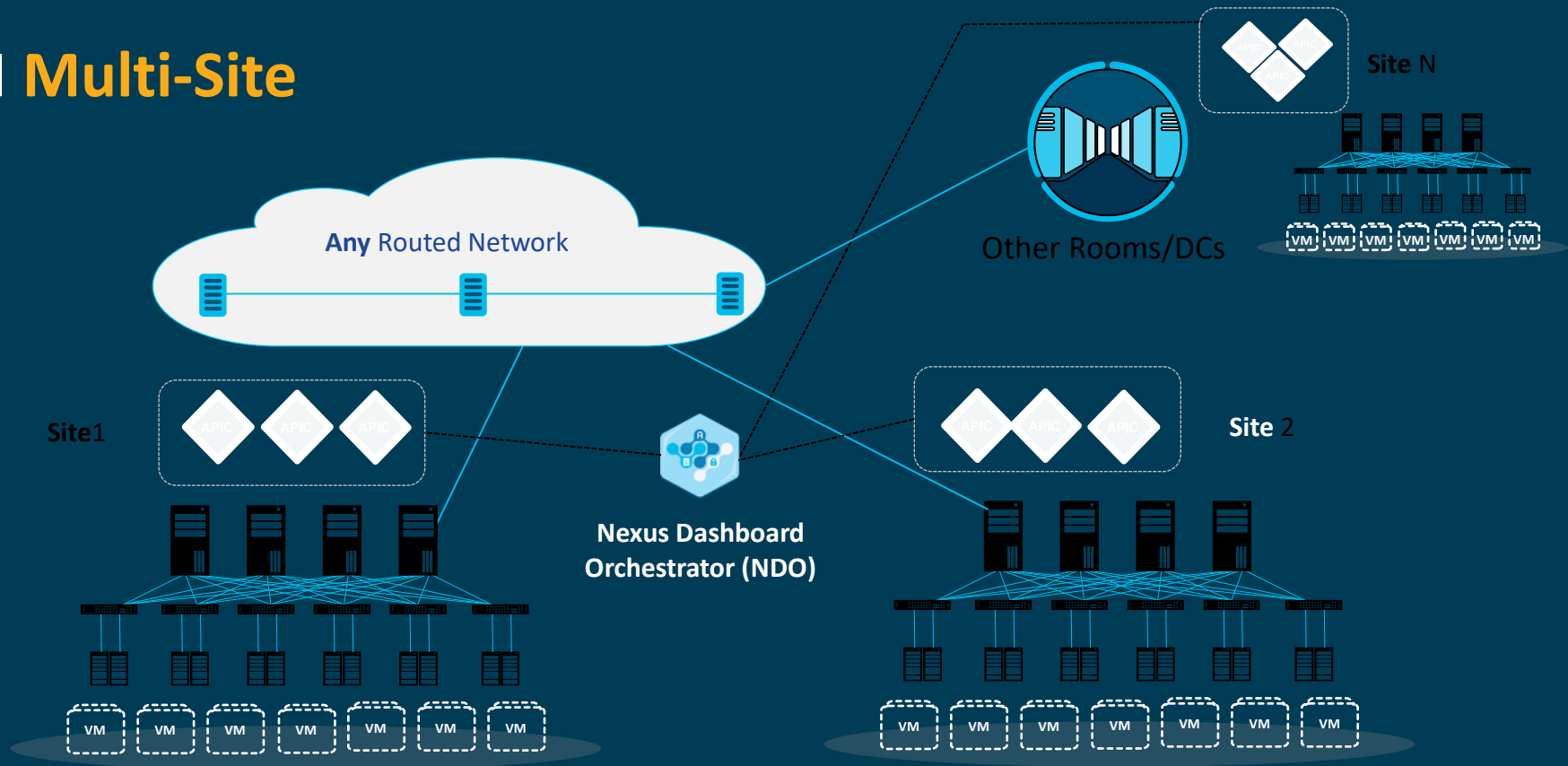


Cloud ACI (Azure)

Routed network requirements: MTU ≥ 1550 and $< 1s$ RTT between APIC & MSO

Automate Cloud and DC Interconnect. Provision **once**, deploy **anywhere**

ACI Multi-Site



No Multicast
Phased Changes (Zones)

<= 1s RTT Required (MSO → APIC)
Up to **12** Sites, distributed gateway

Single central management (MSO)
Automated **L2 DCI VXLAN extension**

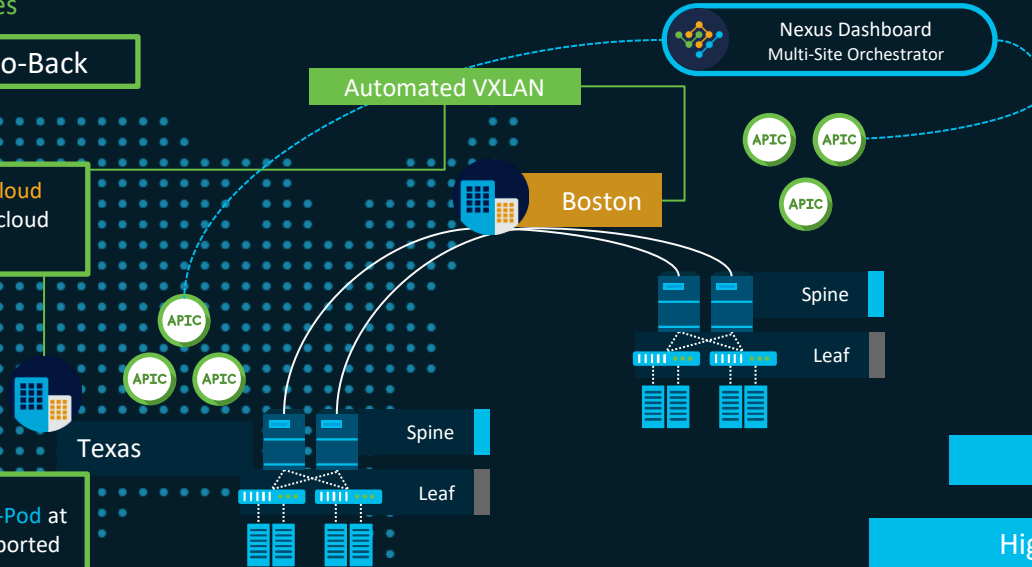
Multi-Site ACI

On-Premises

2 Sites Back-to-Back

An on-prem ACI site is similar to a cloud region while a Pod can be seen as a cloud Availability Zone (AZ)

You can run both Multi-Site and Multi-Pod at the same time. Remote Leaf also supported



Common deployments

DC Migration

DR and Active/Active DCs

Policy centralization, phased changes

High-bandwidth, xDWDM, disperse DCs

Centralize logical networking, automate Data Center Interconnect

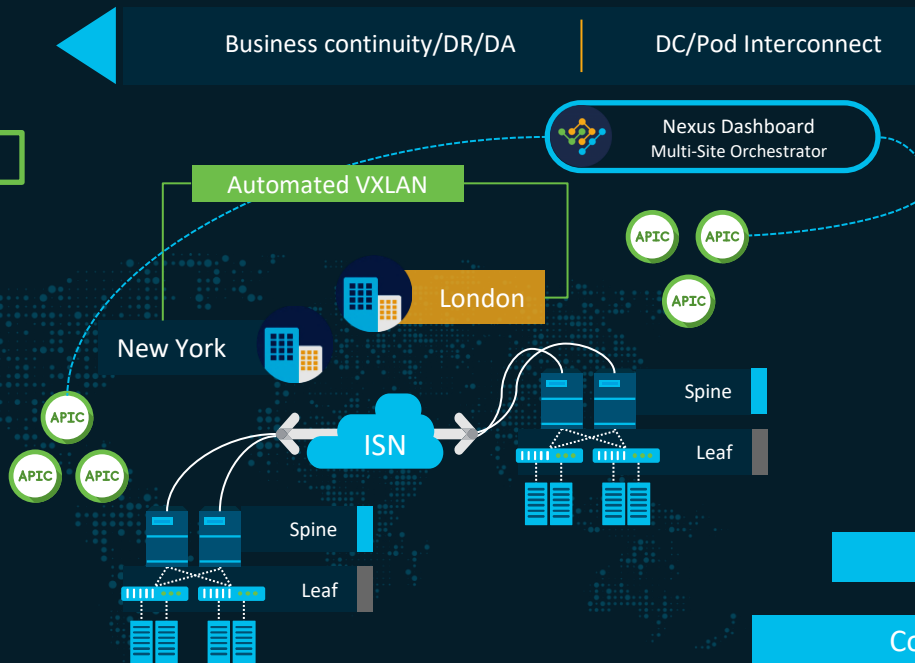
Multi-Site ACI

On-Premises

Up to 12 Sites

Requires an Inter-Site routed Network (ISN) with*:

Spines on each site connect to ISN first-hop using OSPF on VLAN 4



Business continuity/DR/DA

DC/Pod Interconnect

VM Mobility & Migration

Nexus Dashboard
Multi-Site Orchestrator

Automated VXLAN

London

New York

ISN

Spine

Leaf

Spine

Leaf

APIC

APIC

APIC

APIC

APIC

APIC

Common deployments

DC Migration

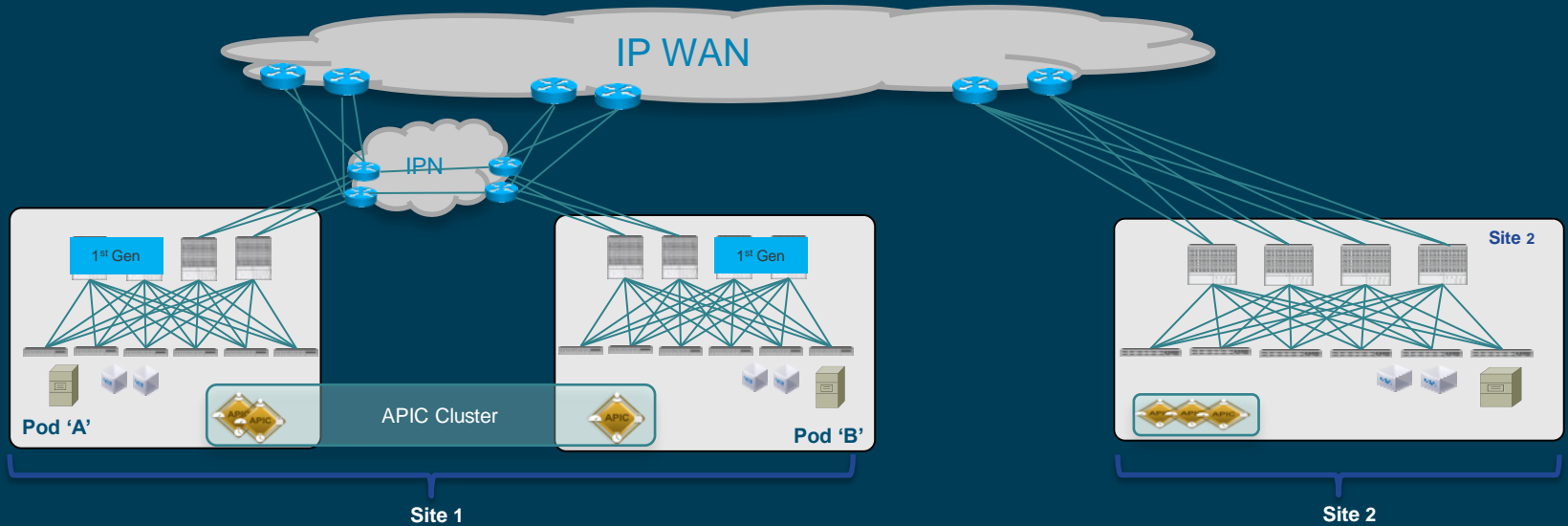
DR and Active/Active DCs

Policy centralization, phased changes

Connect multiple Data Centers globally

Centralize logical networking, automate Data Center Interconnect

ACI Multi-Pod and Multi-Site Connectivity between Pods and Sites



- Only 2nd generation spines must be connected to the external network
 - Need to add 2nd gen spines in each Pod (at least two per Pod) and migrate connections to the IPN from 1st gen spines to 2nd gen spines
- Single 'infra' L3Out and set of uplinks to carry both Multi-Pod and Multi-Site East-West traffic

ACI Multi-Cloud

Multi-Site ACI

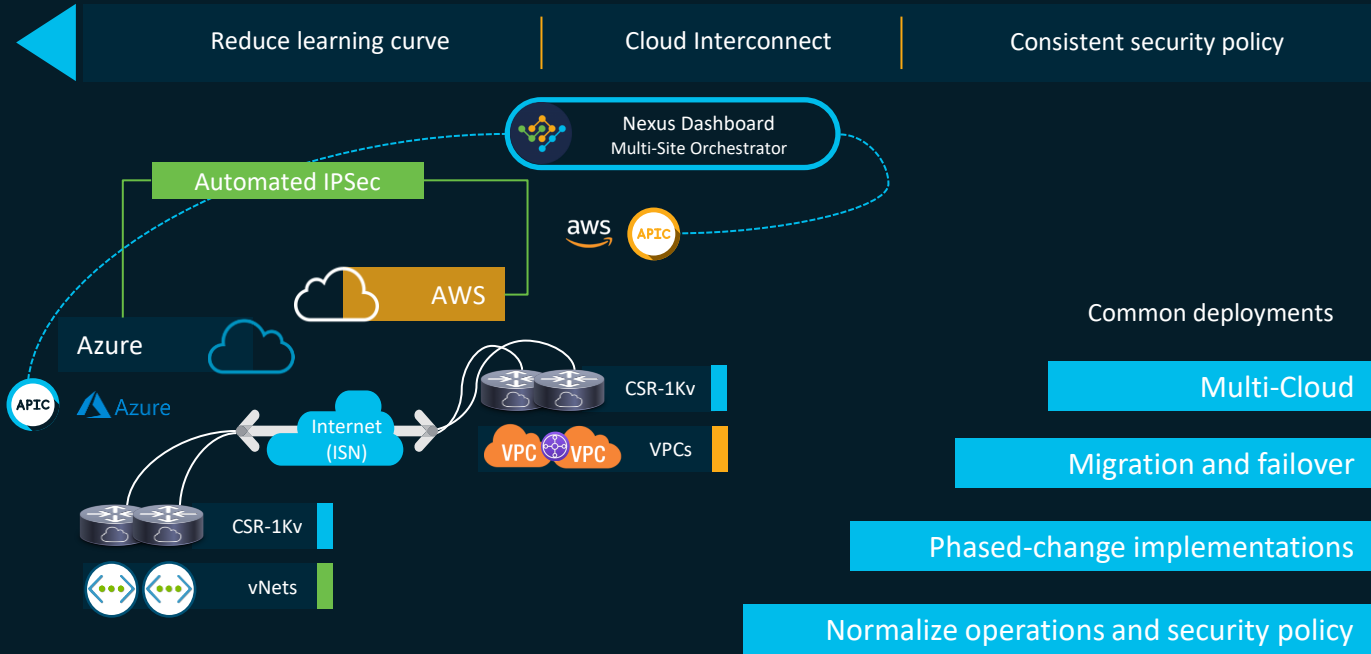
Cloud Only

Up to 12 Sites

Fully automated process

Cisco **CSR-1000v** is deployed and configured **automatically** in Cloud ACI

IPSec, MP-BGP, VXLAN, routes and OSPF configurations are **automated** by Nexus Dashboard **MSO**



Simplify, automate and normalize Multicloud operations

Multi-Site ACI

Hybrid Cloud

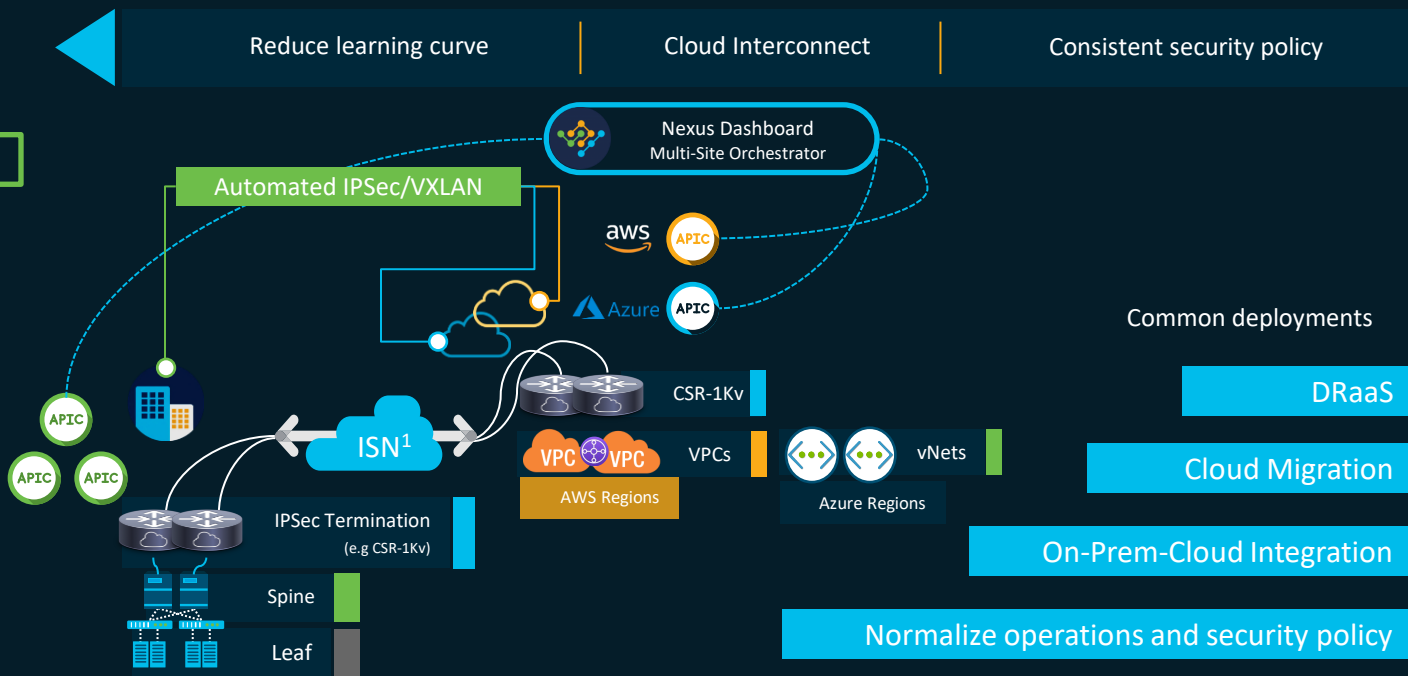
Up to 12 Sites

On-prem requirements and considerations:

Inter-Site Network required¹

IPSec on-prem termination device(s) are required. IPSec Configuration can be downloaded from MSO

MP-BGP, VXLAN, routes and OSPF configurations are automated by MSO



Simplify and accelerate your journey to the cloud

¹ ISN may traverse the Internet or use a dedicated connection (AWS Direct Connect/Express Route)

*In addition to Jumbo Frames (1550+ MTU) and 1 second RTT from Nexus Dashboard MSO to APIC

Automated Multicloud Interconnect



