Introduction to ACI

Chris Merkel
Solutions Engineer - DC Architecture
CCIE 17841

BRKDCN-1601

Cisco Webex App

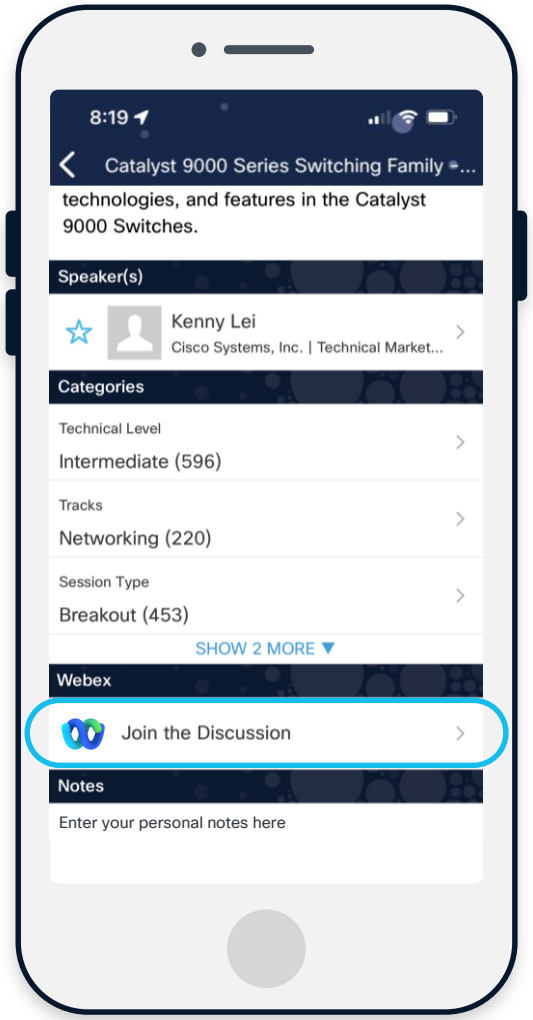
Questions?

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 June 13, 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKDCN-1601**

Agenda

01 Fabric Basics

02 Policy Model

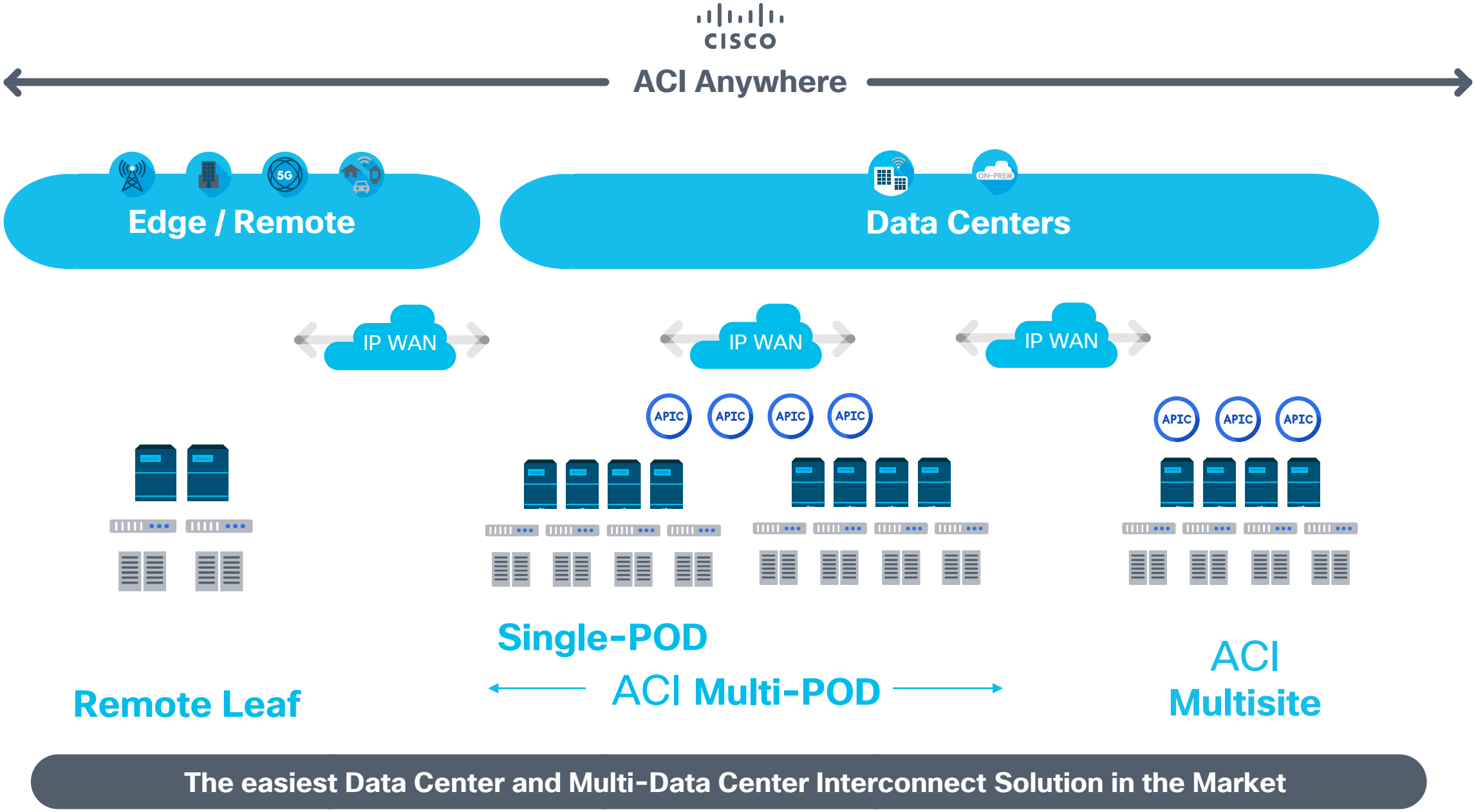
03 Architectural Deployments

04 Day 2 and beyond

05 Conclusion

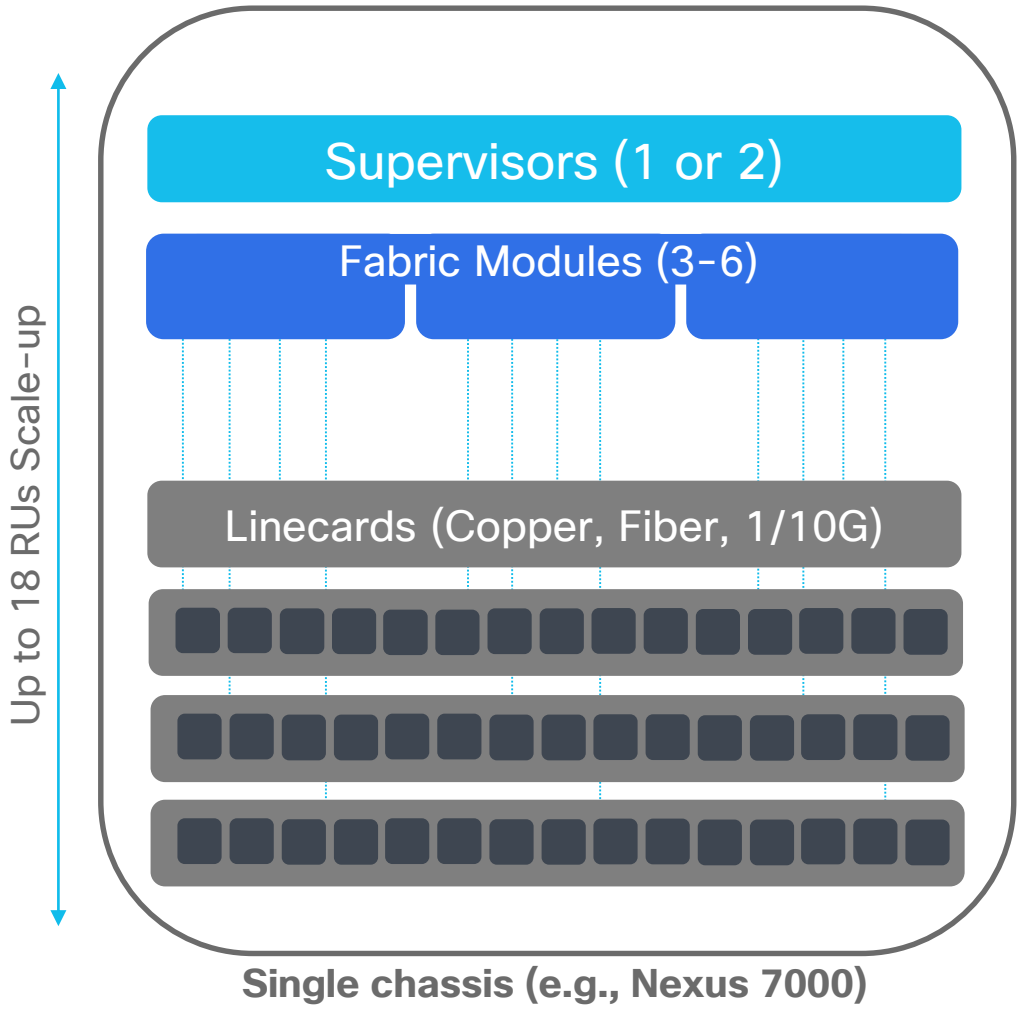
Fabric Basics

ACI : One Network, any location



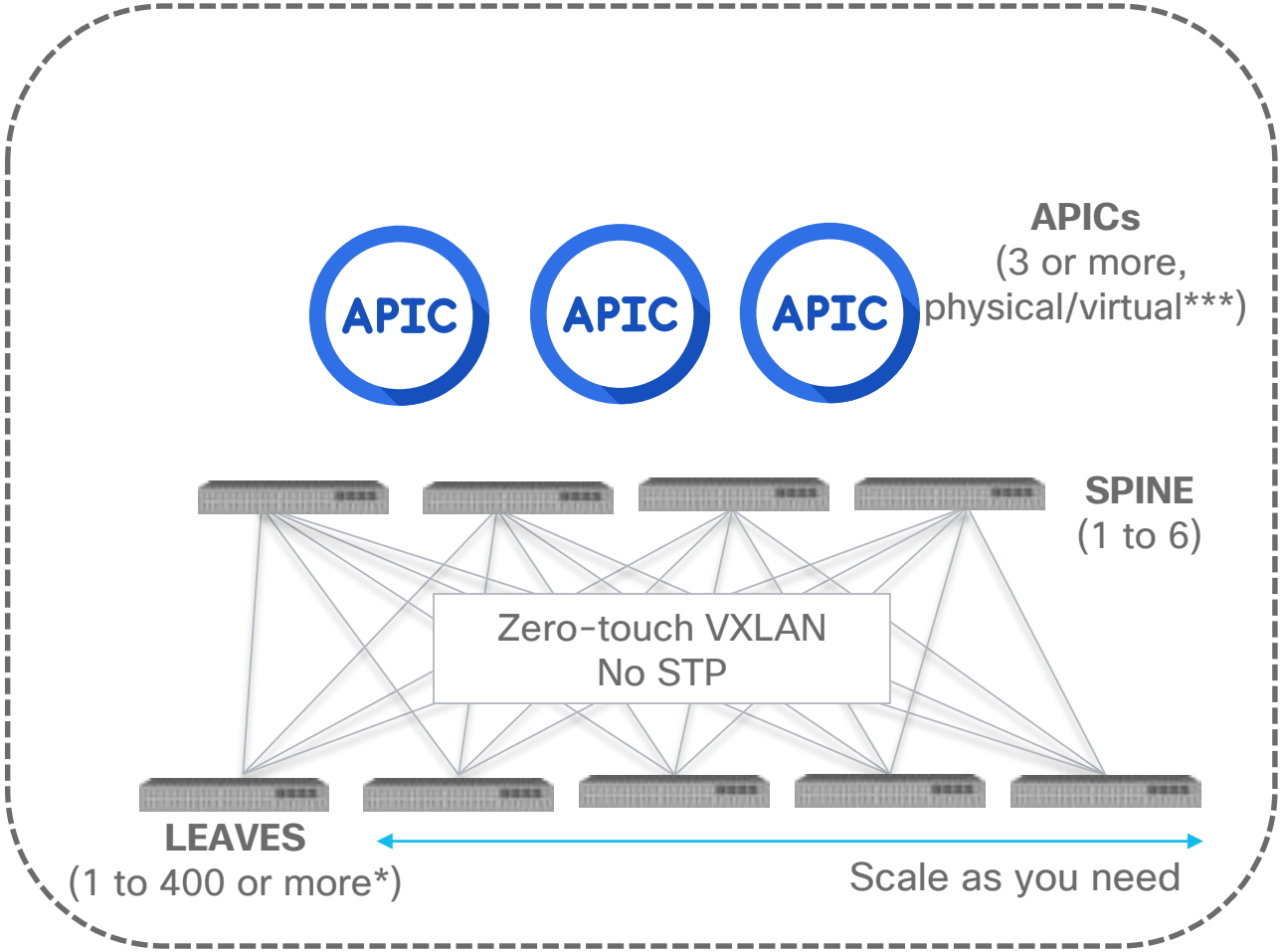
The easiest Data Center and Multi-Data Center Interconnect Solution in the Market

The DC network before
Classic modular switching



Single chassis (e.g., Nexus 7000)

The DC network NOW
ACI



Single VXLAN Network**
Evolution from Nexus 5000 and Nexus 7000

* 500+ Leaves with MultiPod/Multi-Site
** Other topologies available (e.g.,3-tier, etc)
*** Requires ACI 6.1 for full flexibility

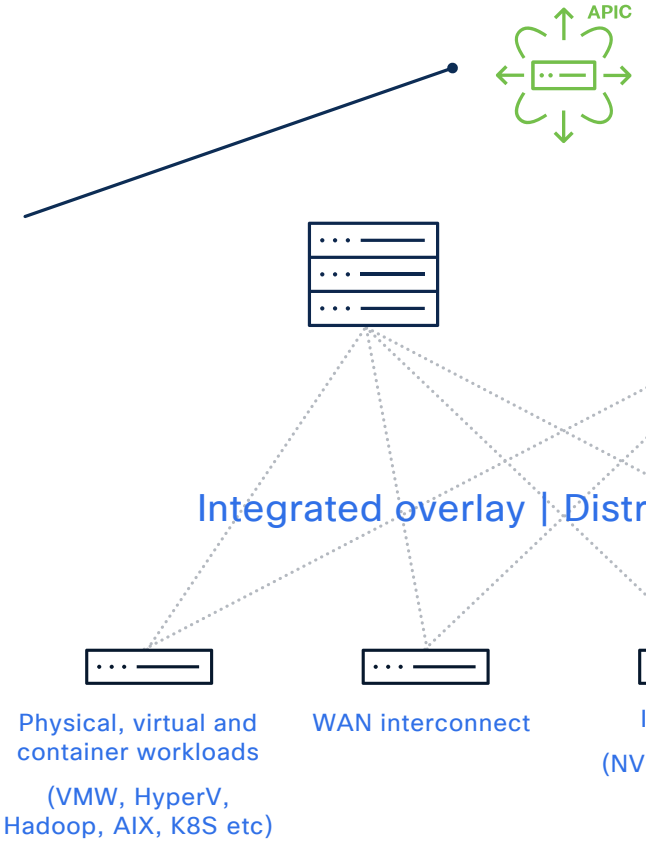
Application Centric Infrastructure building blocks

Built on Cisco Nexus 9000

Cisco APIC (3 or more)

Centralized policy model, network automation

Single open API for entire system – (Terraform, Ansible, Python, Etc)



Flexible: Modular and fixed spine options

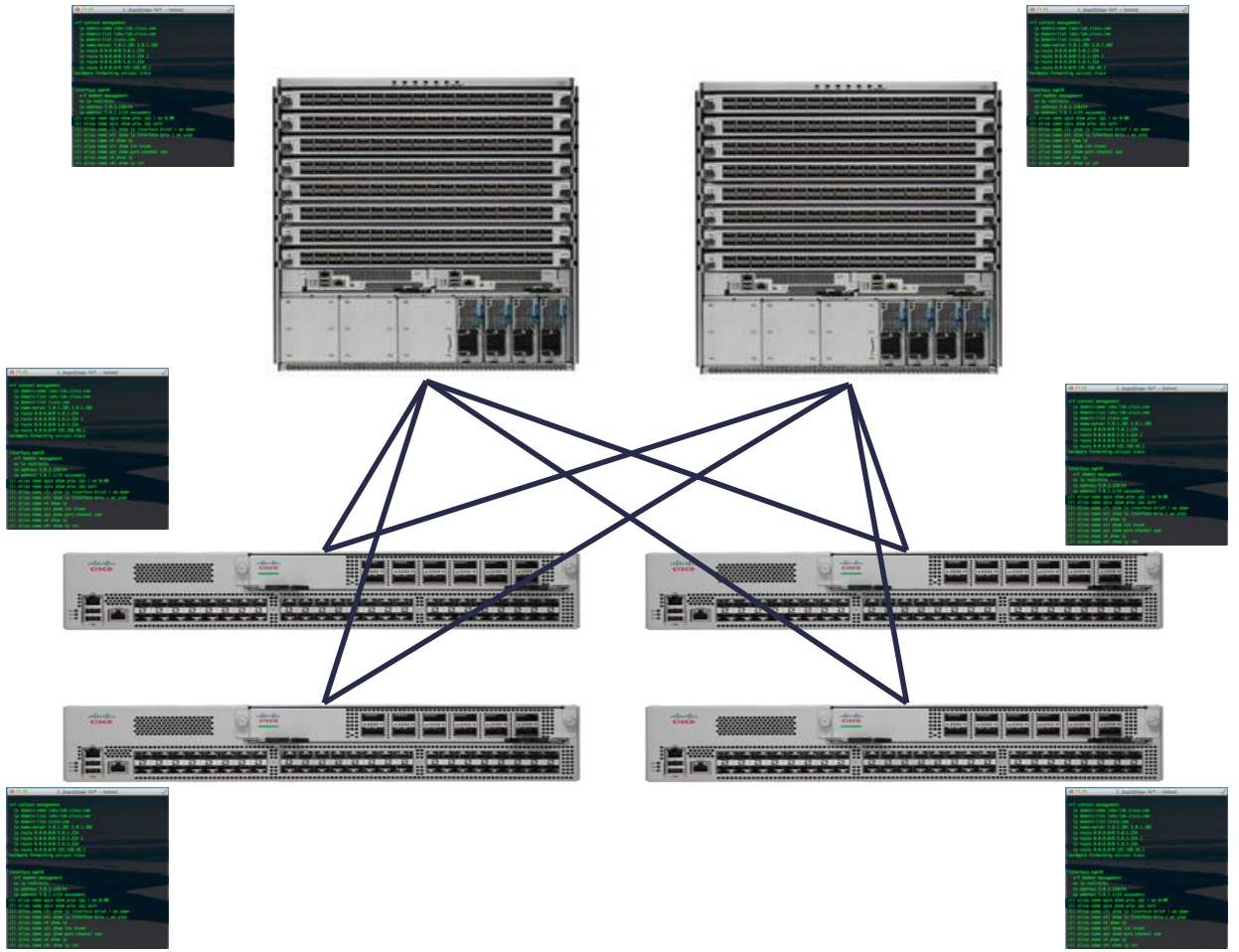
Non-blocking 40/100/400G fabric, CLOS fabric

Built-in distributed stateless firewall, multi-tenant security

Price | Performance | Port density | Programmability | Power efficiency

All nodes are managed and operated independently, and the actual topology dictates a lot of configuration

- **Device basics**: AAA, syslog, SNMP, PoAP, hash seed, default routing protocol bandwidth ...
- **Interface and/or Interface Pairs**: UDLD, BFD, MTU, interface route metric, channel hashing, Queuing, LACP, ...
- **Fabric and hardware specific design**: HW Tables, ...
- **Switch Pair/Group**: HSRP/VRRP, VLANs, vPC, STP, HSRP sync with vPC, Routing peering, Routing Policies, ...
- **Application specific**: ACL, PBR, static routes, QoS, ...
- **Fabric wide**: MST, VRF, VLAN, queuing, CAM/MAC & ARP timers, COPP, route protocol defaults



ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

BEFORE

- Nexus 9000 VTEP-1 configuration:

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 second
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

SSH to every switch, Assign IP Address, Enable Telnet/SSH, Add users on every switch/Create ACLs (optional)

(Times **X** Switches & **Y** VNIs)

ACI: How difficult was it to bring up?

What tasks & configuration did ACI just saved me from doing manually on every switch

BEFORE

- Nexus 9000 VTEP-1 configuration:

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 second
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

```
switch-vtep-1(config)# feature nv overlay
switch-vtep-1(config)# feature vn-segment-vlan-based

switch-vtep-1(config)# feature ospf
switch-vtep-1(config)# feature pim
switch-vtep-1(config)# router ospf 1
switch-vtep-1(config-router)# router-id 200.200.200.1
switch-vtep-1(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4
switch-vtep-1(config)# interface loopback0
switch-vtep-1(config-if)# ip address 200.200.200.1/32
switch-vtep-1(config-if)# ip address 100.100.100.1/32 secondary
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode
switch-vtep-1(config)# interface e2/1
switch-vtep-1(config-if)# ip address 20.1.1.1/30
switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
switch-vtep-1(config-if)# ip pim sparse-mode

switch-vtep-1(config)# interface port-channel 10
switch-vtep-1(config-if)# vpc 10
switch-vtep-1(config-if)# switchport
switch-vtep-1(config-if)# switchport mode access
switch-vtep-1(config-if)# switchport access vlan 10
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# interface e1/1
switch-vtep-1(config-if)# channel-group 10 mode active
switch-vtep-1(config-if)# no shutdown

switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0

switch-vtep-1(config-if)# member vni 10000 mcast-group 230.1.1.1
switch-vtep-1(config)# vlan 10
switch-vtep-1(config-vlan)# vn-segment 10000
switch-vtep-1(config-vlan)# exit
```

SSH to every switch, Assign IP Address, Enable Telnet/SSH, Add users on every switch/Create ACLs (optional)

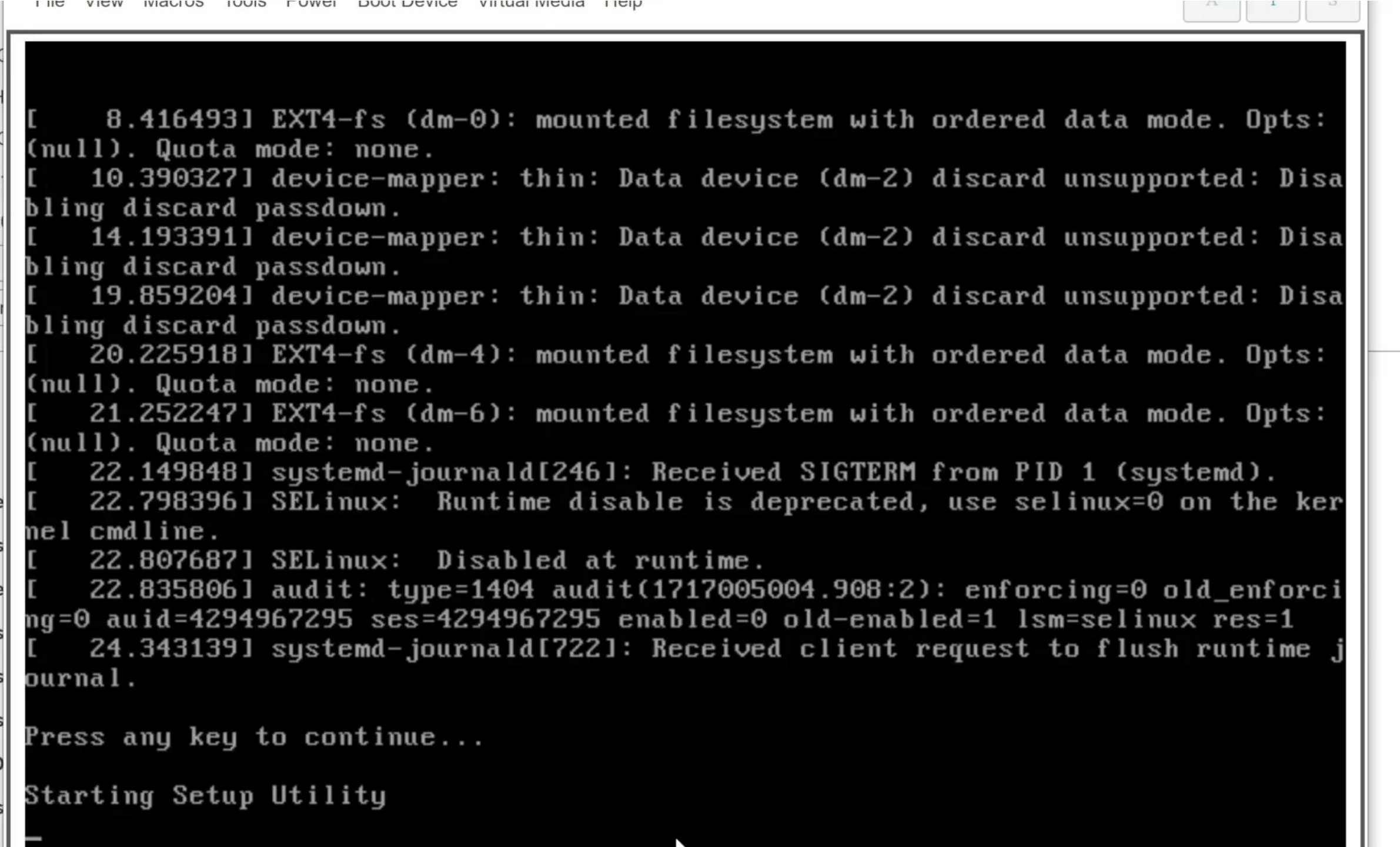
(Times **X** Switches & **Y** VNIs)

NOW

- External to Internal Route redistribution & Control Plane (MP-BGP, QoS, etc)
- Multicast (BD GIPo Addressing)
- Overlay Network (VXLAN)
- Underlay Routed Network (IS-IS)
- Switch management & Best Practices

ACI Automated tasks
From HOURS to seconds!

Demo!


File View Macros Tools Power Boot Device Virtual Media Help
[8.416493] EXT4-fs (dm-0): mounted filesystem with ordered data mode. Opts: (null). Quota mode: none.
[10.390327] device-mapper: thin: Data device (dm-2) discard unsupported: Disabling discard passdown.
[14.193391] device-mapper: thin: Data device (dm-2) discard unsupported: Disabling discard passdown.
[19.859204] device-mapper: thin: Data device (dm-2) discard unsupported: Disabling discard passdown.
[20.225918] EXT4-fs (dm-4): mounted filesystem with ordered data mode. Opts: (null). Quota mode: none.
[21.252247] EXT4-fs (dm-6): mounted filesystem with ordered data mode. Opts: (null). Quota mode: none.
[22.149848] systemd-journald[246]: Received SIGTERM from PID 1 (systemd).
[22.798396] SELinux: Runtime disable is deprecated, use selinux=0 on the kernel cmdline.
[22.807687] SELinux: Disabled at runtime.
[22.835806] audit: type=1404 audit(1717005004.908:2): enforcing=0 old_enforcing=0 auid=4294967295 ses=4294967295 enabled=0 old-enabled=1 lsm=selinux res=1
[24.343139] systemd-journald[722]: Received client request to flush runtime journal.
Press any key to continue...
Starting Setup Utility

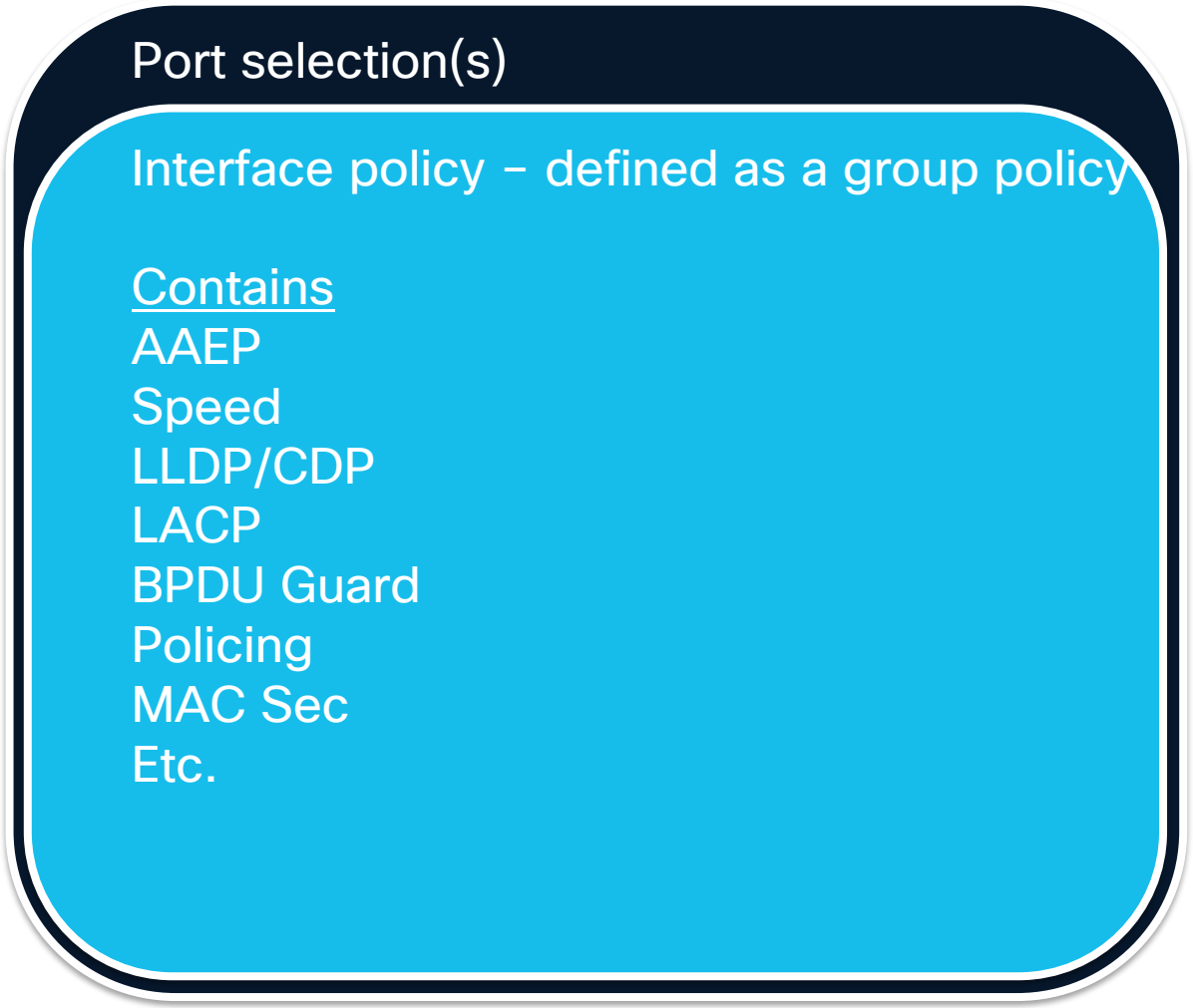
ACI Policy Model Simplified

The ACI Policy Model

Physical

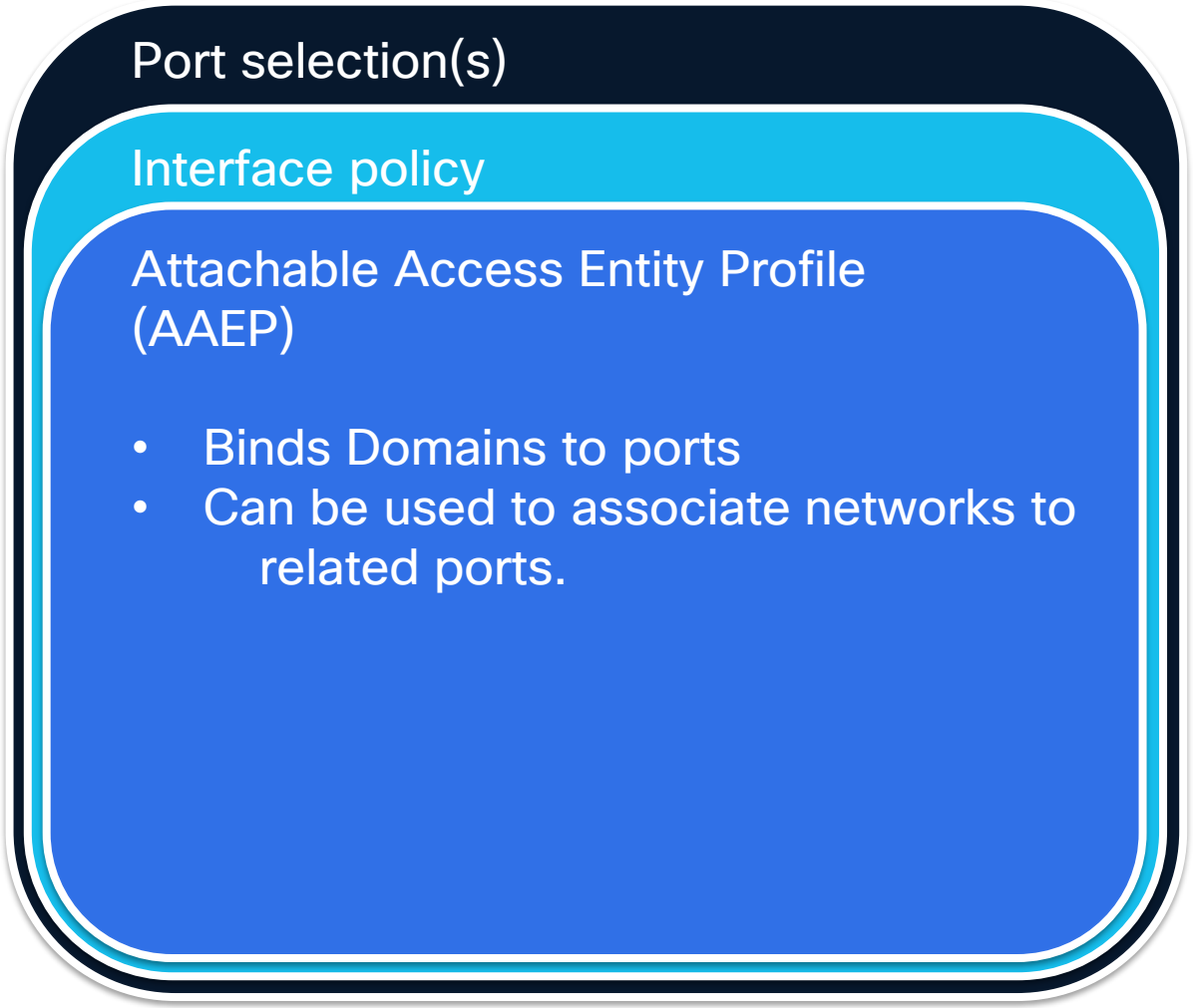
The ACI Policy Model

Physical



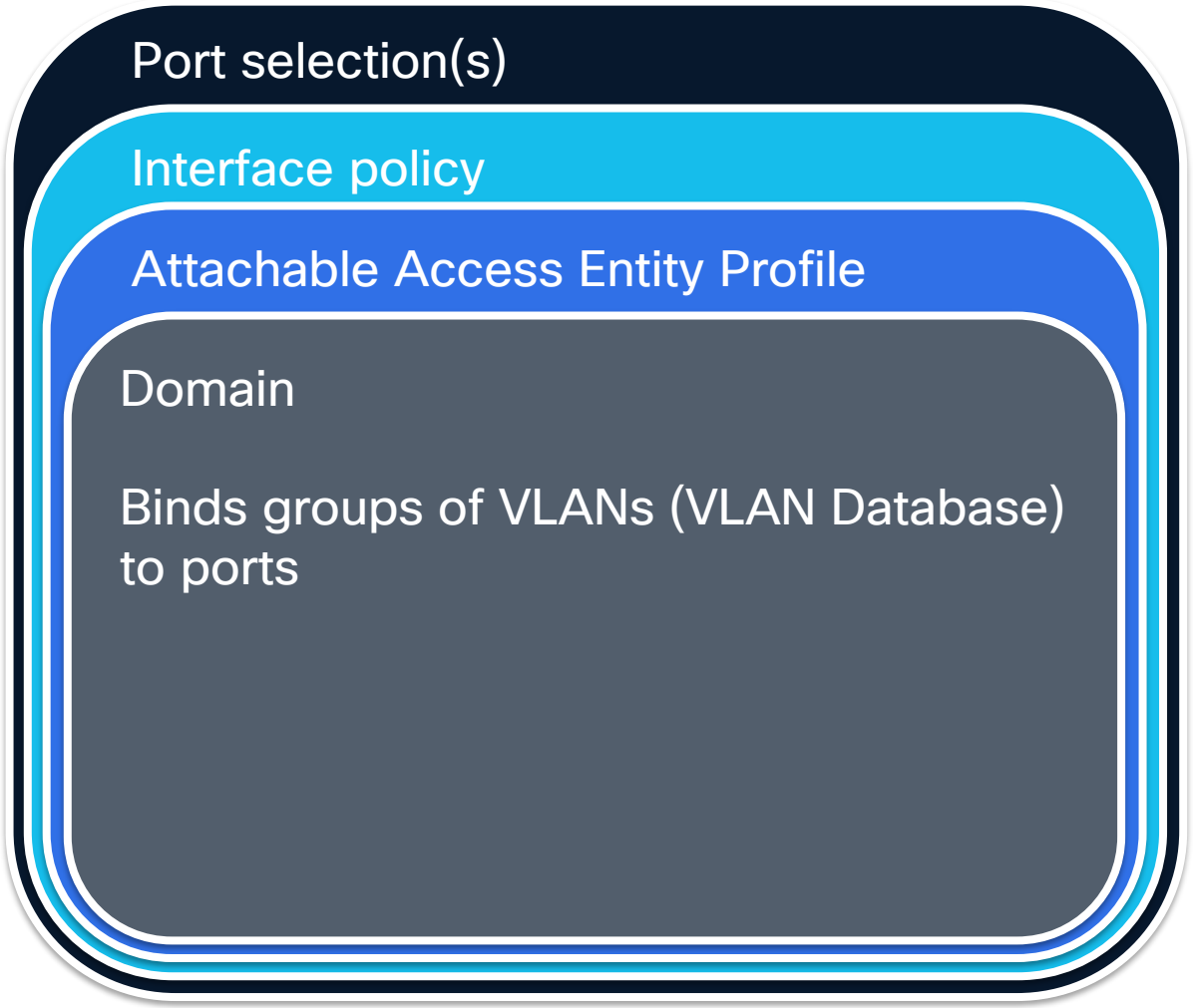
The ACI Policy Model

Physical

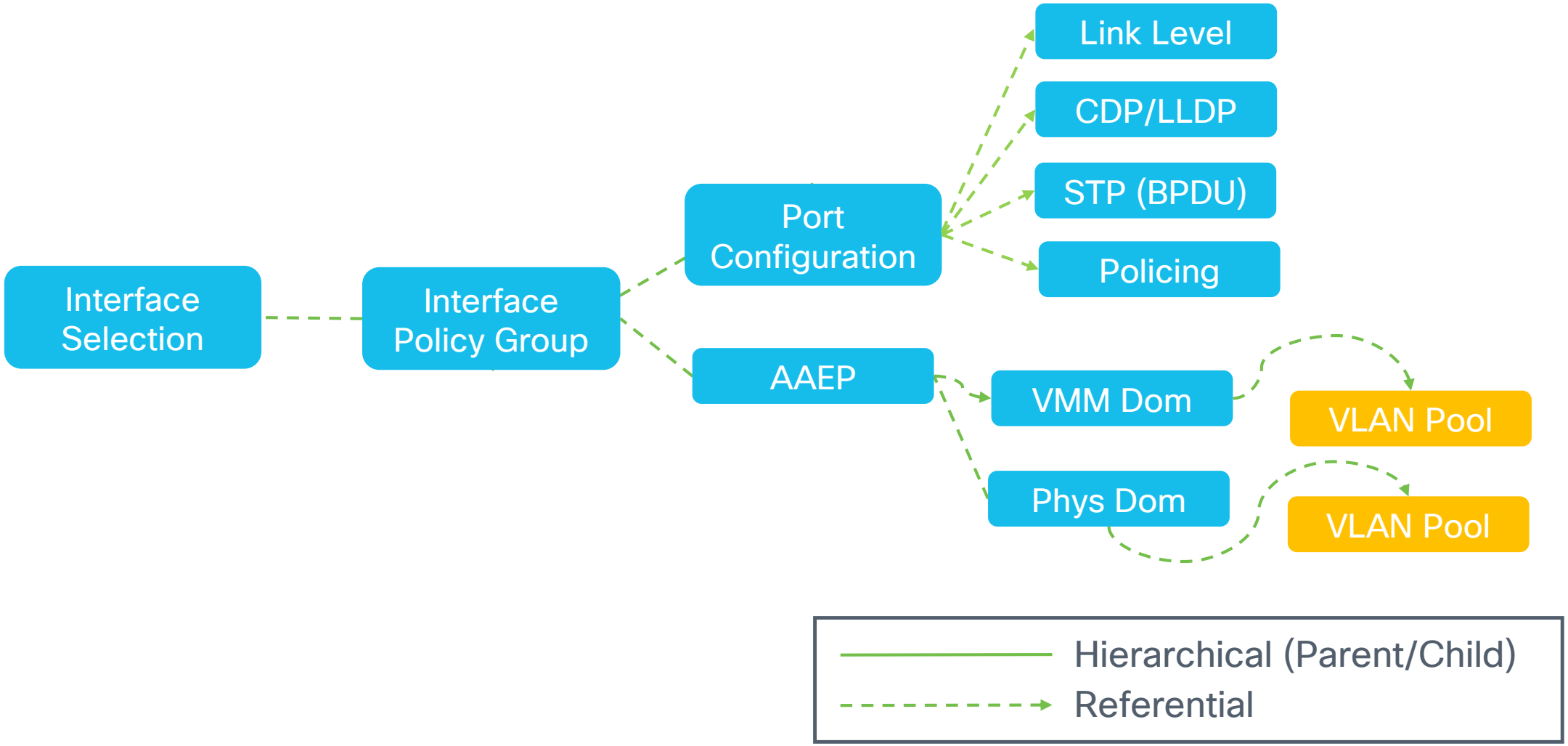


The ACI Policy Model

Physical



Access Policies Object Model



Demo!

Policies

- Quick Start
- Interface Configuration
- Switch Configuration
- Switches
- Modules
- Interfaces
- Policies
- Physical and External Domains
- Pools

Interface Configuration

Refresh

This table uses a new configuration method. If you prefer the old one, do not use this table or we can help you migrate. Show More

Summary

Configured State

Admin Up 22

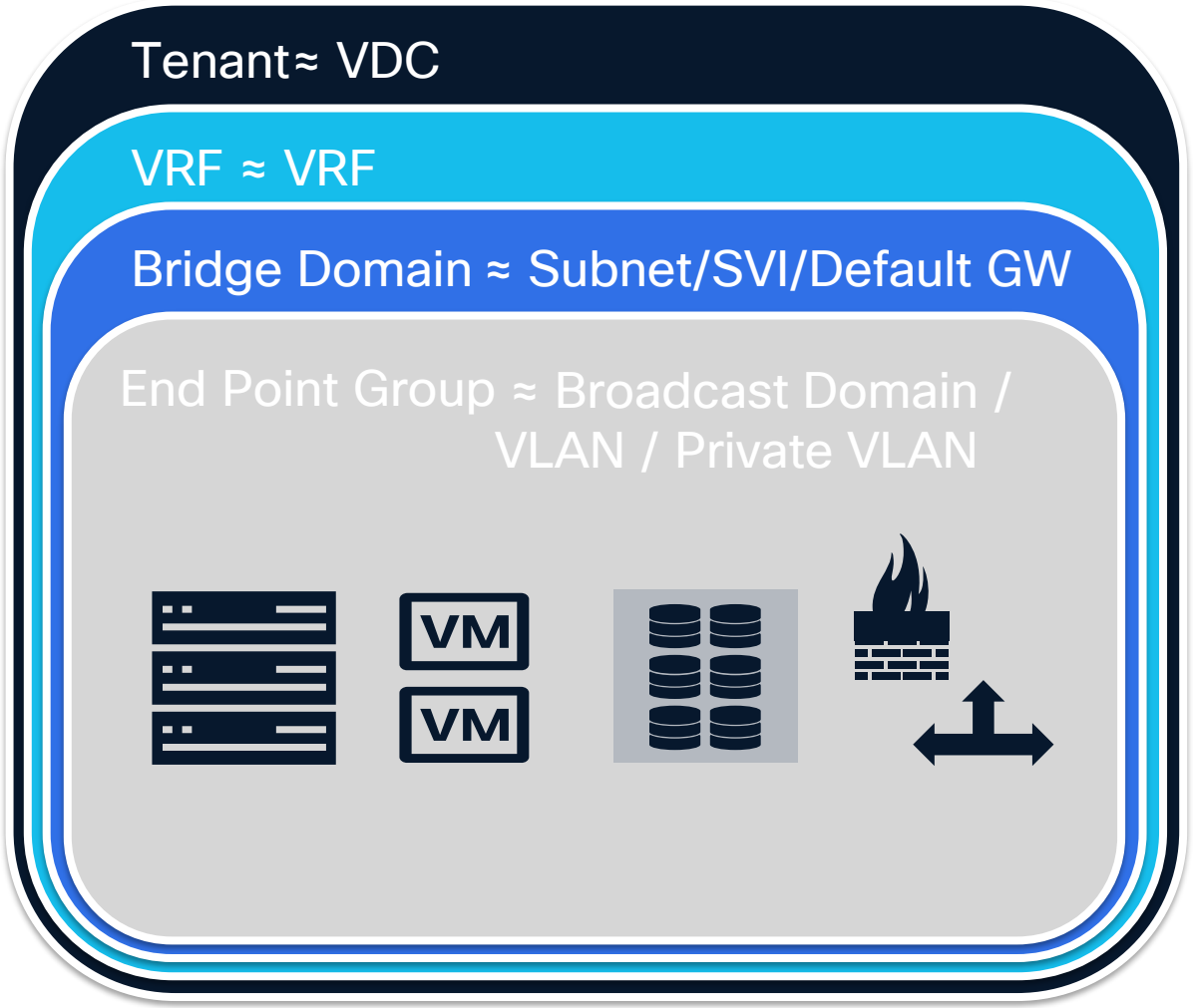
Filter by attributes

Actions

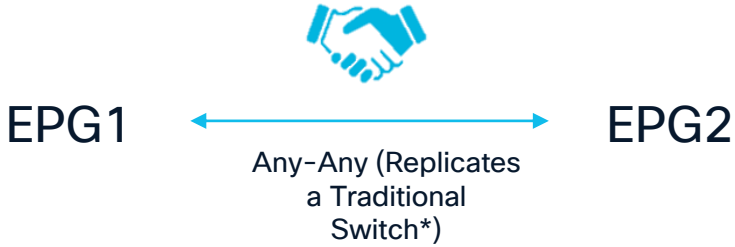
Node	Interface	Port Type	Admin State	Port Mode	Policy Group	Description	Port Direction
101 1	eth1/12	Access Leaf	Enabled	Individual	Rack-ESX Used by 4 int	-	Default
101 1	eth1/33	Access Leaf	Enabled	Individual	nfv-esxi Used by 4 int	-	Default
101 1	eth1/34	Access Leaf	Enabled	Individual	nfv-esxi Used by 4 int	-	Default

The ACI Policy Model

Logical



More Contracts ≈Intelligent Access Lists

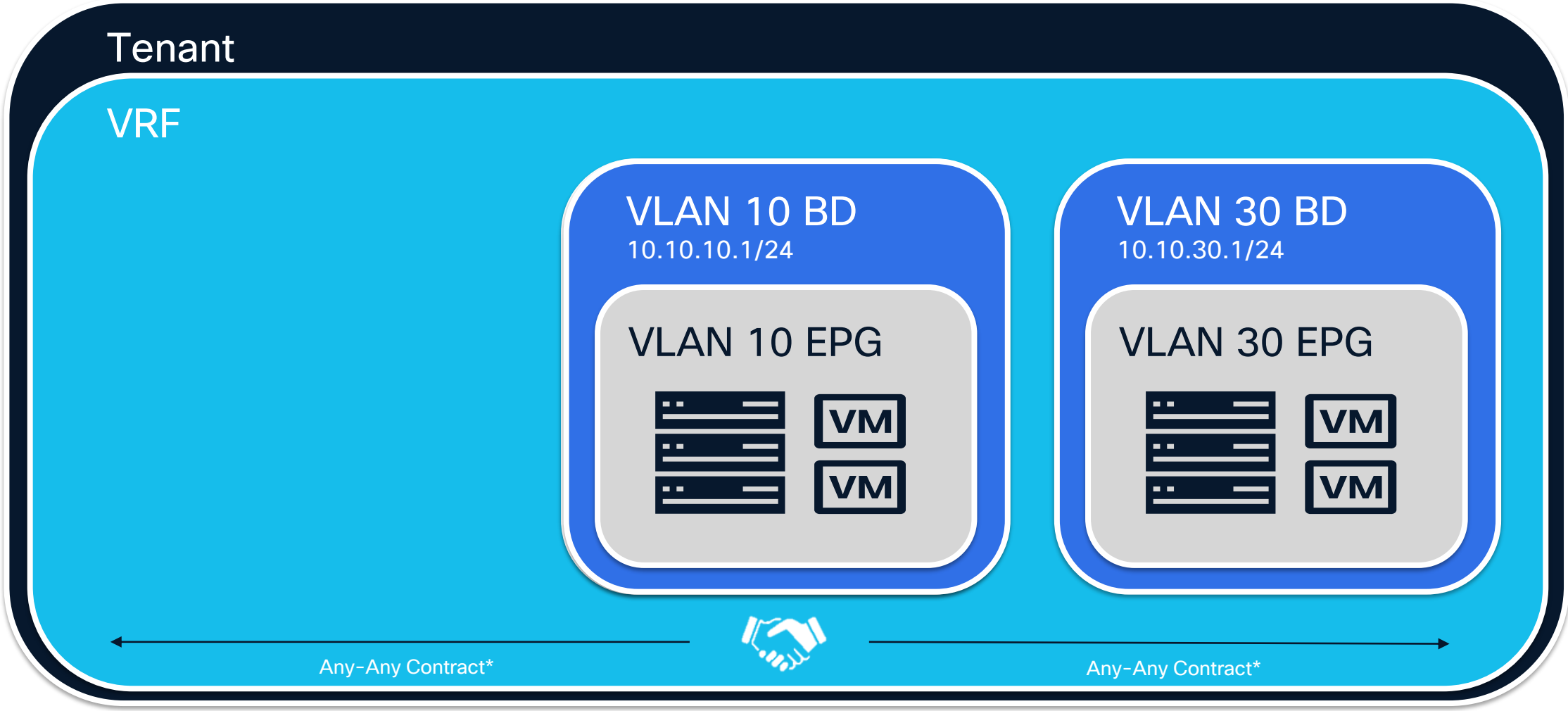


L2 External EPG≈ 802.1q Trunk

L3 External EPG ≈ L3 Path(s) exiting ACI with traffic control capabilities

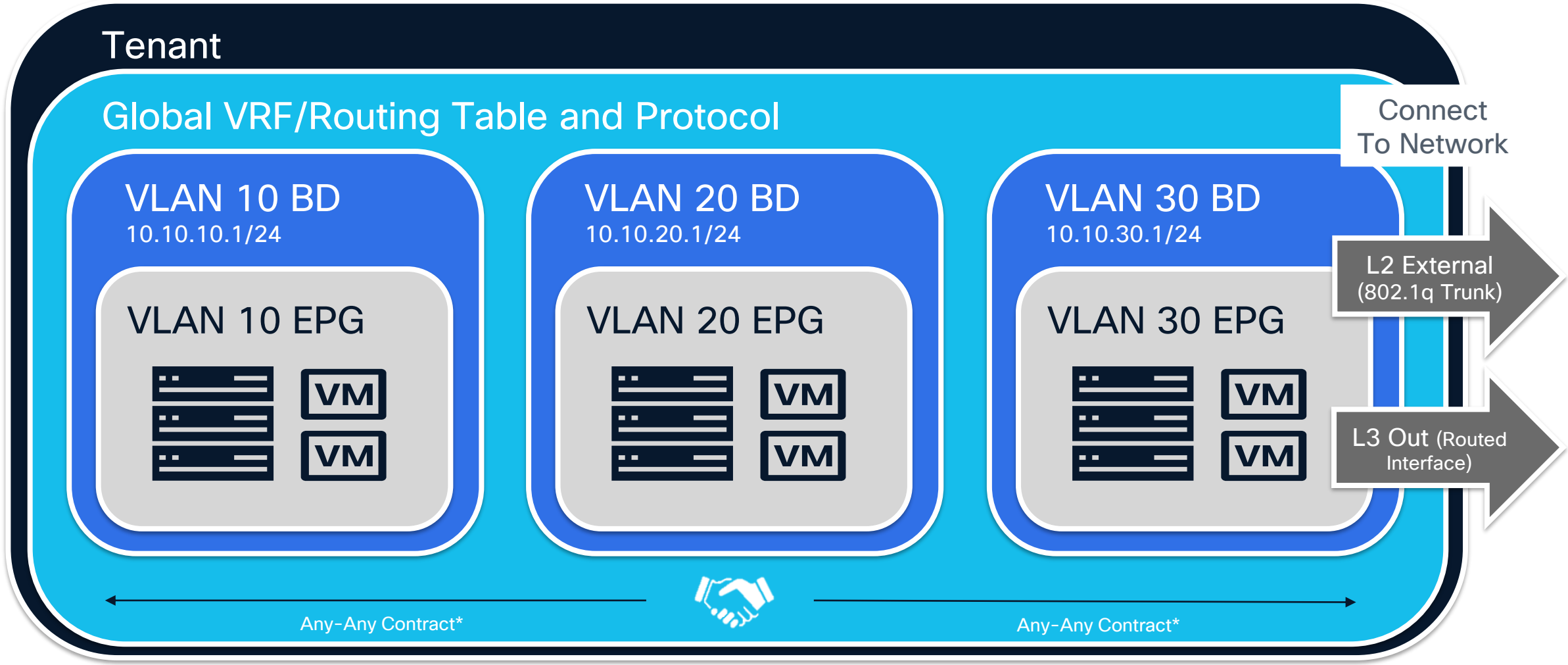
* Preferred group or vzAny Contract achieves the same outcome

The ACI Policy Model – Starting off with ACI



* Preferred group or vzAny Contract achieves the same outcome

The ACI Policy Model – Starting off with ACI



* Preferred group or vzAny Contract achieves the same outcome

Demo!

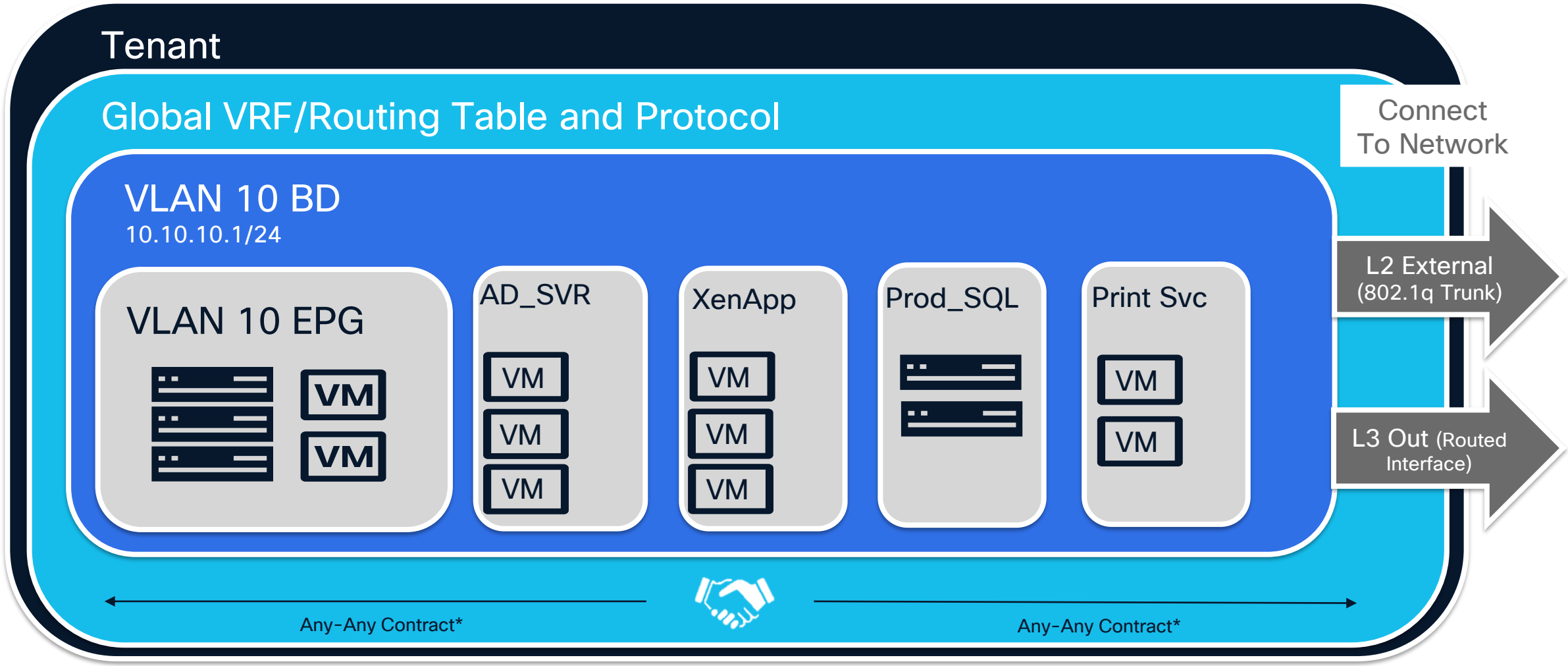
System | Tenants | Fabric | Virtual Networking | Admin | Operations | Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | ESG-Test | prod

All Tenants

Name	Alias	Description	Bridge Domains	VRFs	EPGs	Health Score
ansible Ansible		Ansible testing -davis	0	1	0	Healthy
common NDO			2	4	1	Healthy
ECU-CLT			20	1	21	Healthy
ECU-RTP			20	1	20	Healthy
ESG-Test			1	1	1	Healthy
infra			2	2	2	Healthy
kd_tn		kedieter tenant for demo purp...	5	2	7	Healthy
kedieter			3	1	1	Healthy
mgmt			2	4	1	Healthy
ndi-demo NDO		ND Insights Demo Tenant	3	1	9	Healthy
ndo-green NDO		Greenfield NDO Demo Tenant	9	1	9	Healthy
NIQTenant01 NDO			0	0	0	Healthy
NIQtenant01 NDO			0	0	0	Healthy
NIQTenantDemo NDO			0	0	0	Healthy
pbr-test NDO			1	1	3	Healthy
prod			1	1	3	Healthy

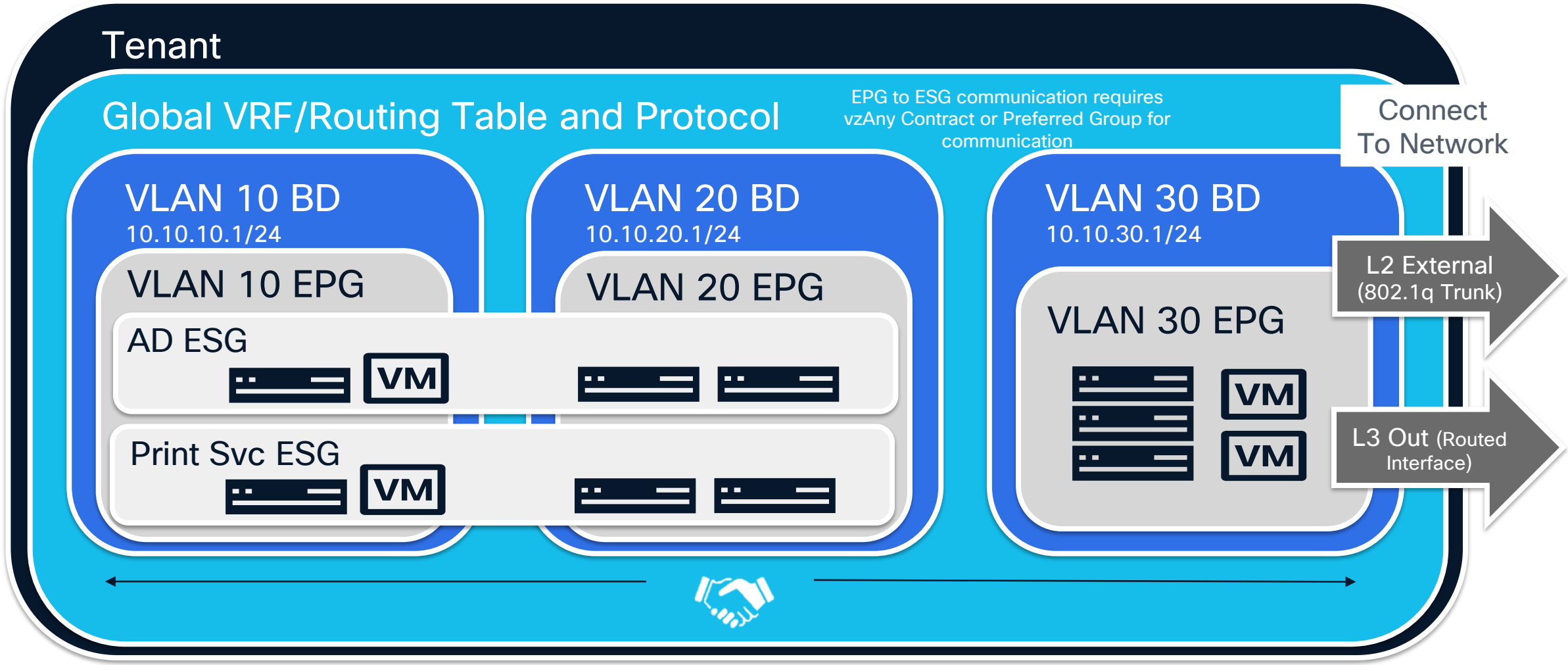
The ACI Policy Model – Extending the configuration
Endpoint Groups



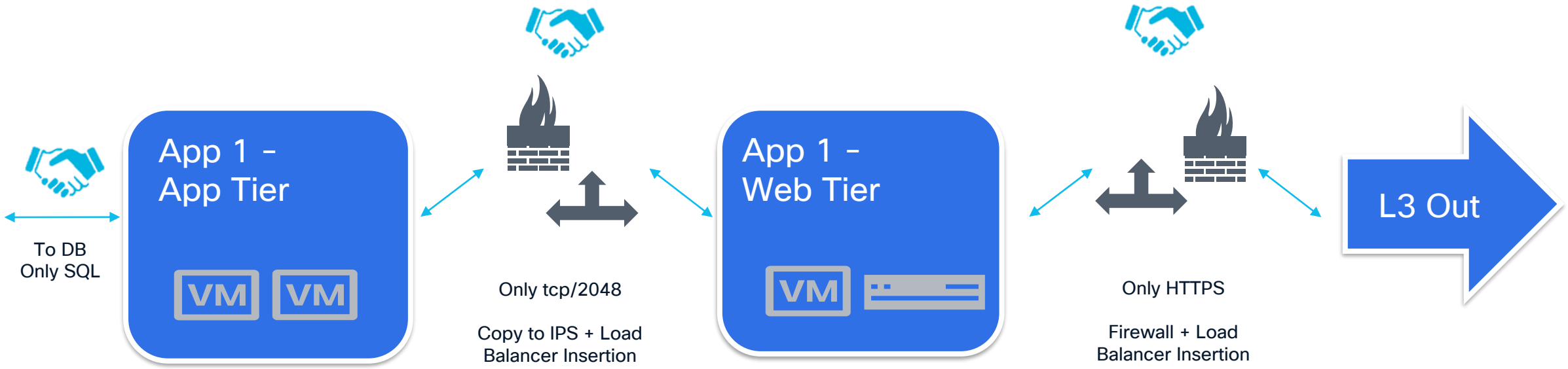
* Preferred group or vzAny Contract achieves the same outcome

The ACI Policy Model – Extending the configuration

Endpoint Security Groups (ESG) - ACI 5.0 and greater



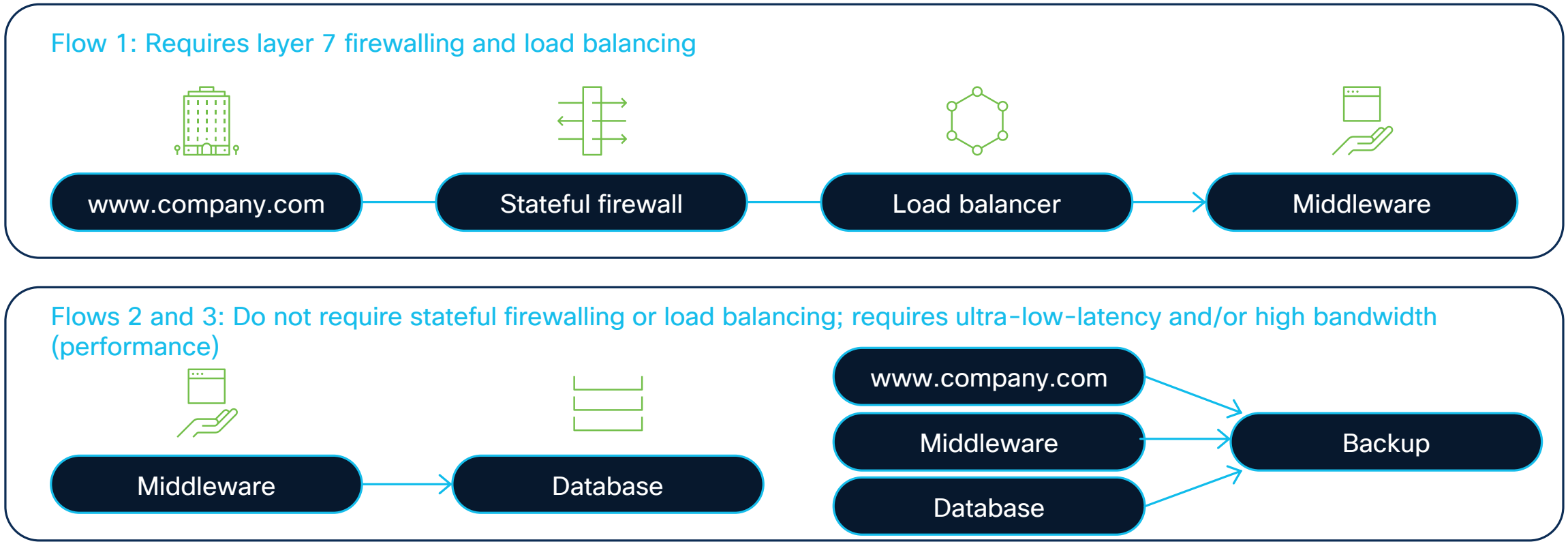
Advancing the ACI Configuration



Policy Based Redirect with Service Graphs

Cisco ACI application aware service chaining

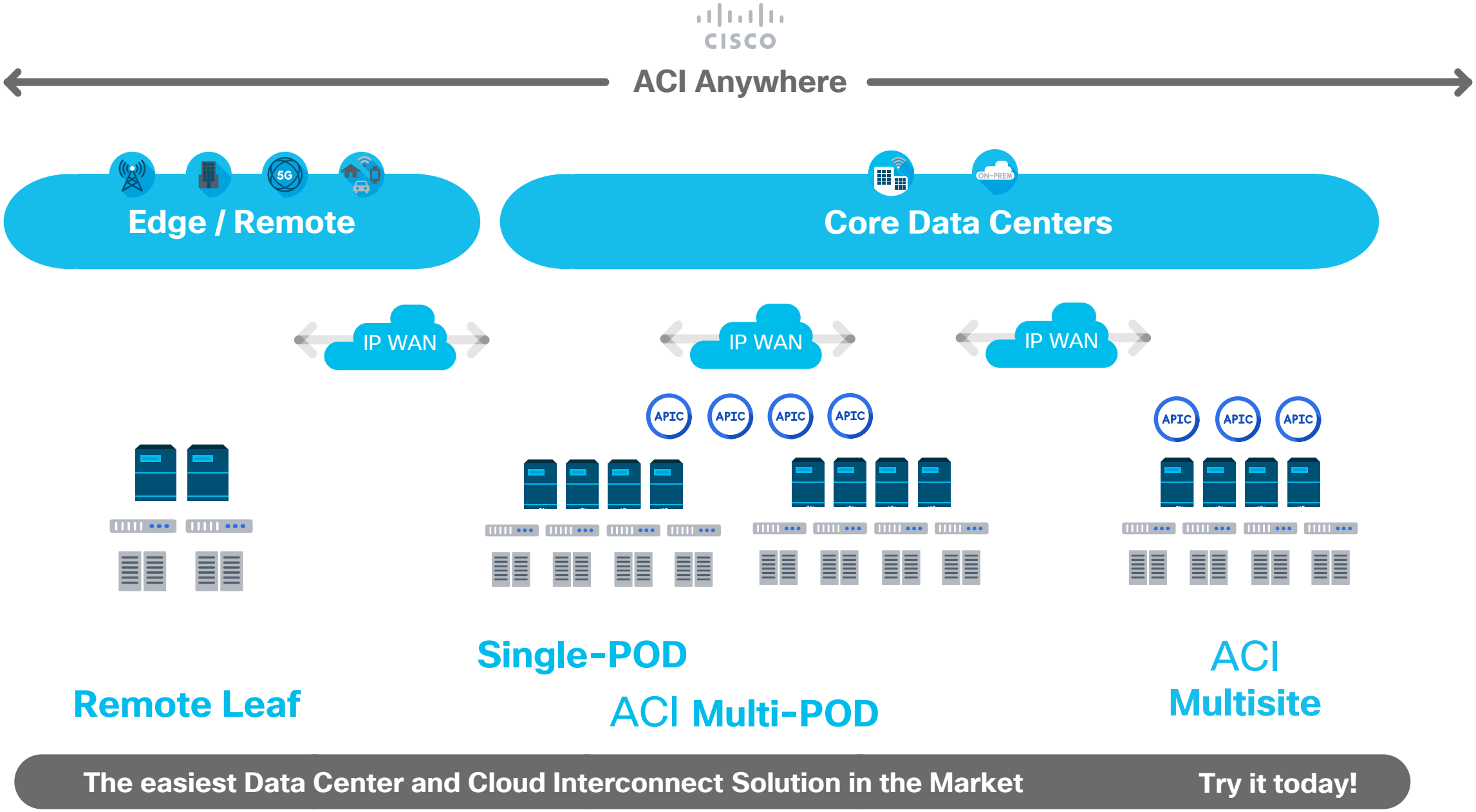
Different forwarding treatment for different flows in a multi-tiered web application



Benefits

- Redirect specific flows based on business requirements
- Offload traffic from expensive firewalls and load balancers
- Decouple appliance placement from routing table
- Forward traffic based on compliance and performance

ACI Deployment Options

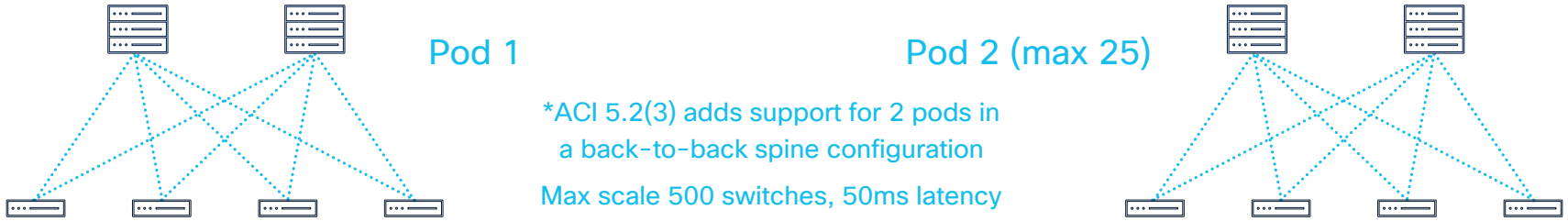


Cisco ACI multi-pod

Create on-prem availability zones with multiple fabrics, evolution of stretched fabric

Inter-pod IP network

w/ PIM BiDir support*



Pod 1

Pod 2 (max 25)

*ACI 5.2(3) adds support for 2 pods in a back-to-back spine configuration

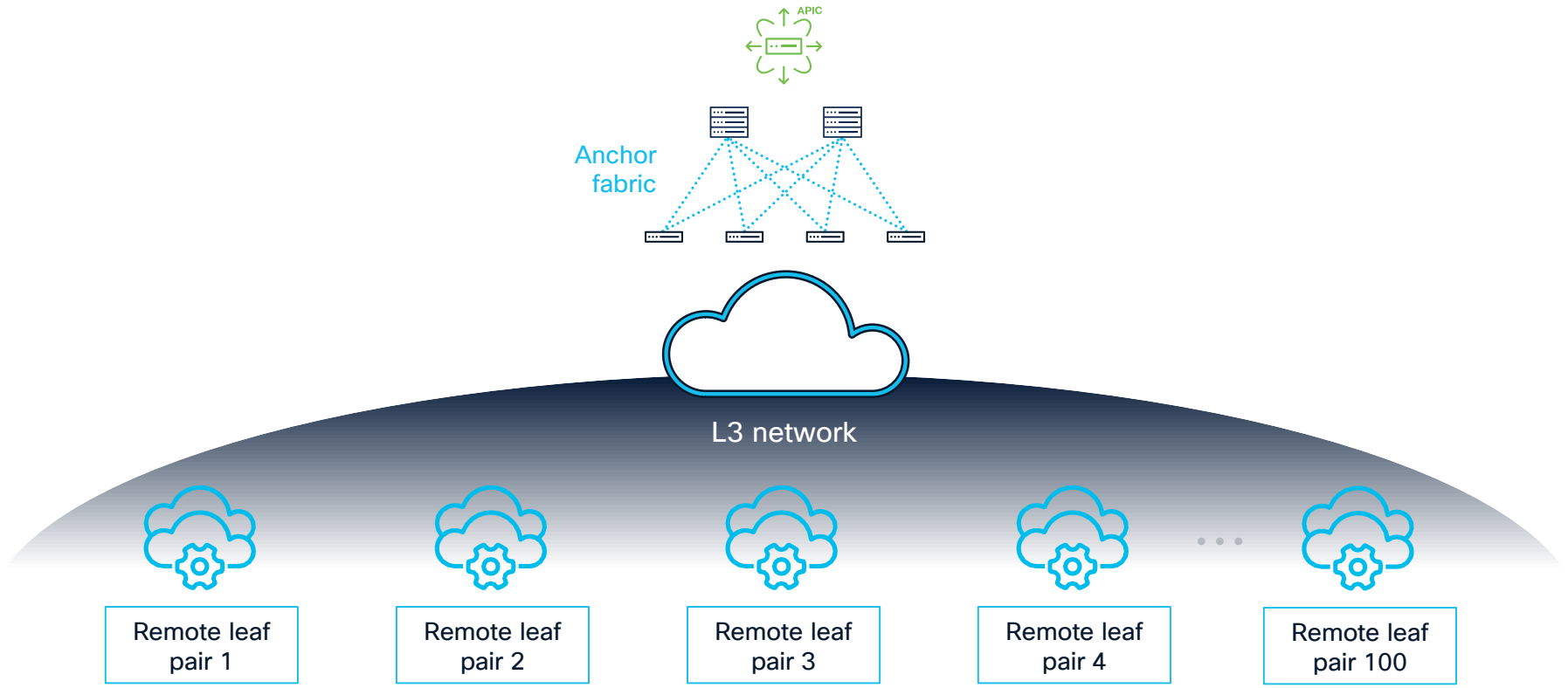
Max scale 500 switches, 50ms latency

Benefits

- Disaster recovery
- Active-active load balancing
- Deploy highly available applications
- Extend VM and container mobility domains

Cisco ACI: Remote leaf

Enable low-touch remote application deployments with the power of Cisco ACI

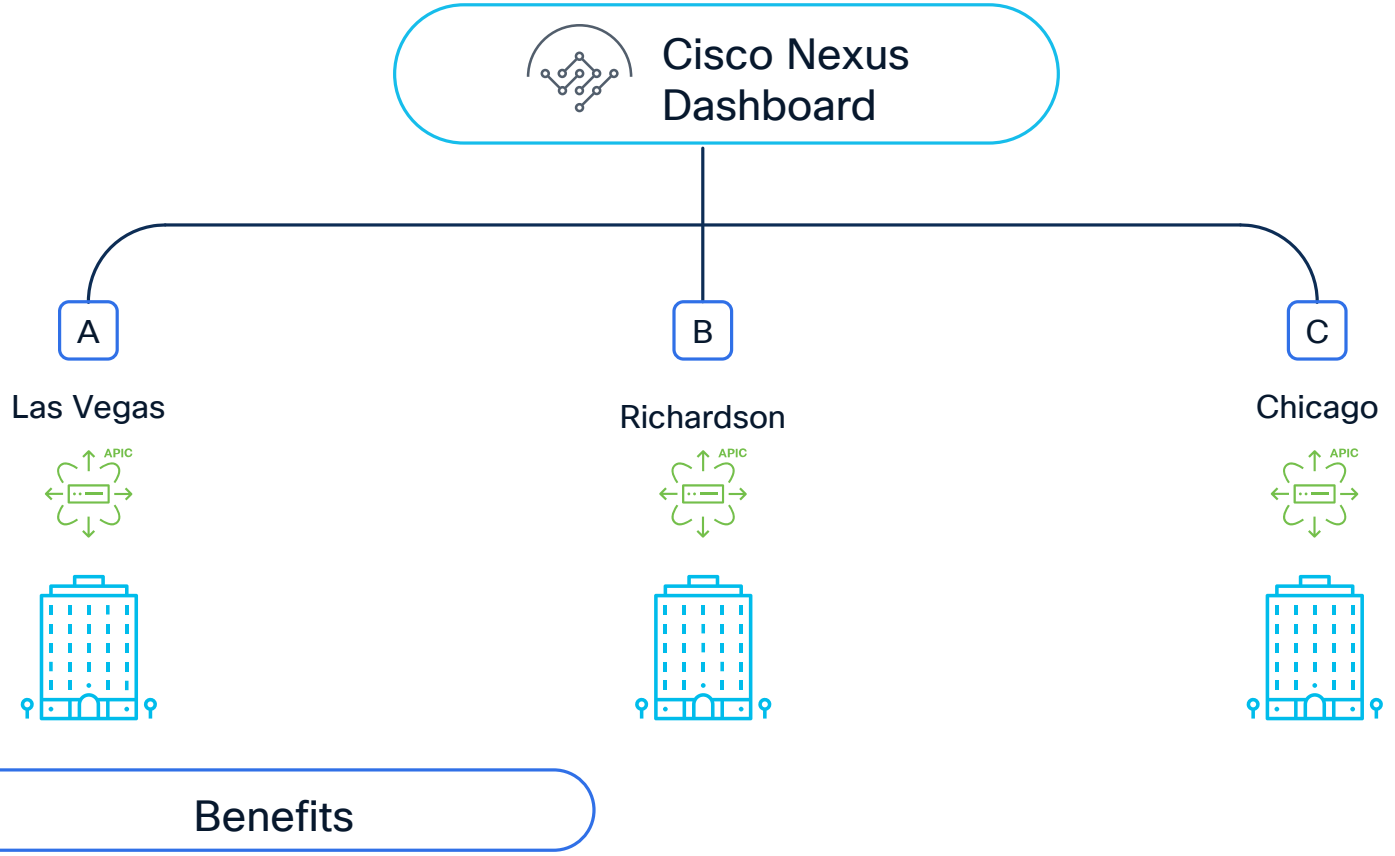


Benefits

- Single management plane for core fabric and remote leaf (RL)
- Up to 200 RLs per fabric
- DC Migration / OTV replacement
- End-to-end security using Cisco ACI's segmentation model

Cisco ACI multi-site

Create fault tolerant regions in geographically distributed on-prem data centers



Benefits

Deploy applications based on geo-performance

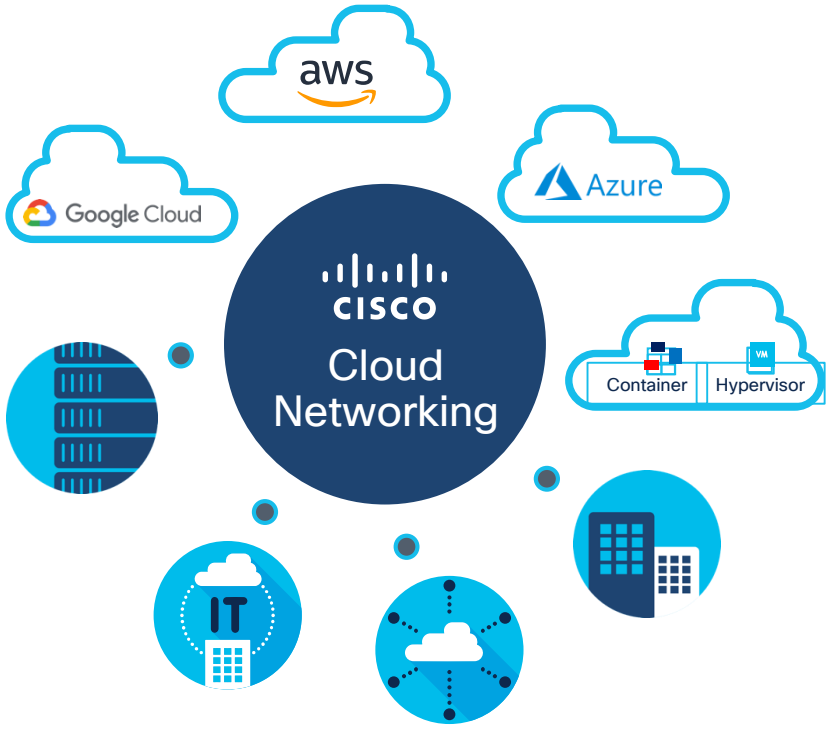
Geo-compliance and data privacy

Limit blast radius to a single application geography

Unify Cisco ACI policy geographically

ACI Day 2 and Beyond – Making ACI Hum

Cloud Networking: Challenges



Connectivity and management

Workloads are increasingly distributed and diverse. Complex to connect workloads across multiple public cloud providers, data centers and edge locations.

Visibility and automation

Troubleshooting challenges due to more decentralized architectures with different environments.

Zero trust and security

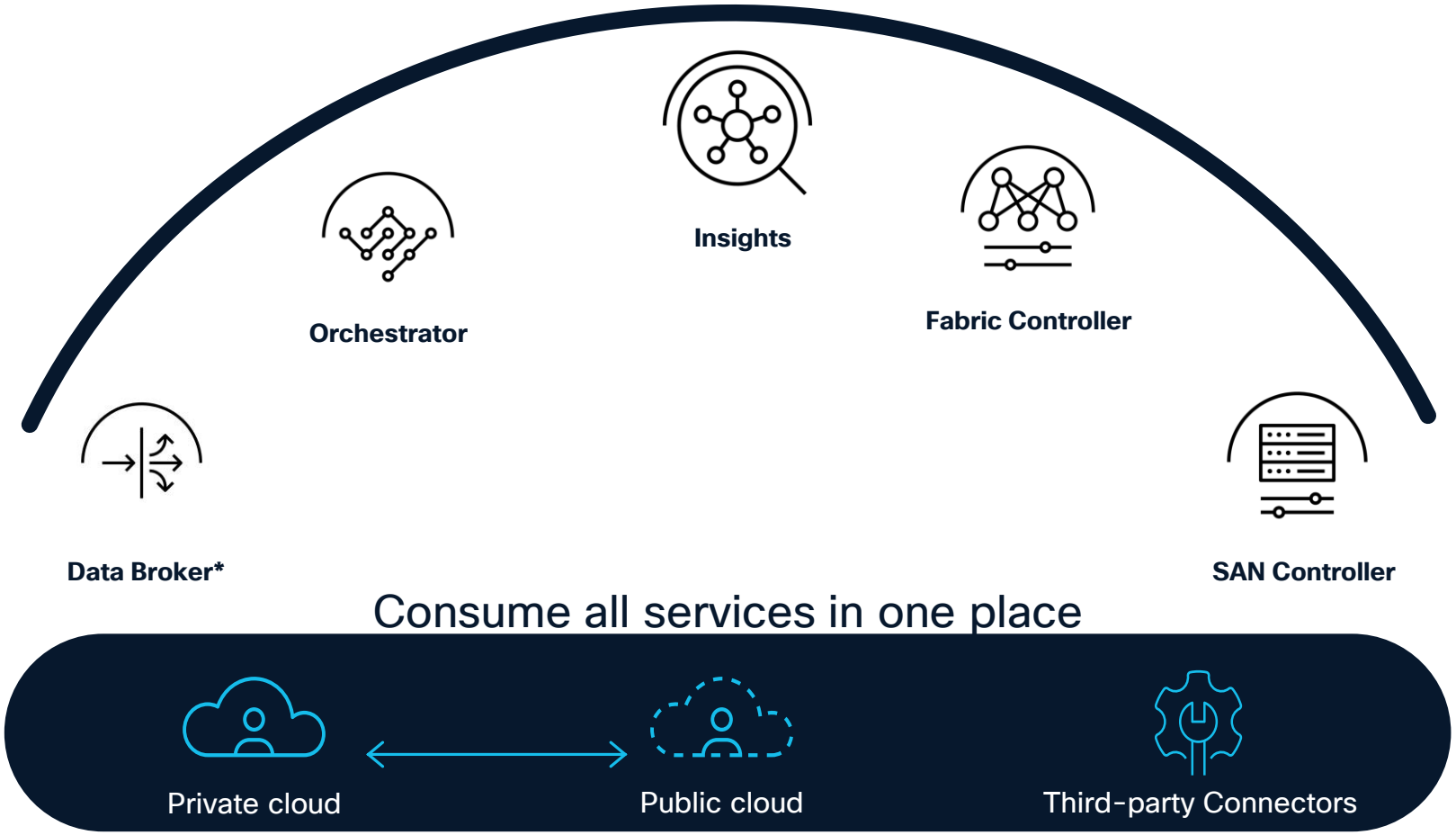
Workload migration and mobility of users imposes significant challenges to enforce right security policies across different environments.

Need for homogenous experience across heterogenous cloud environments

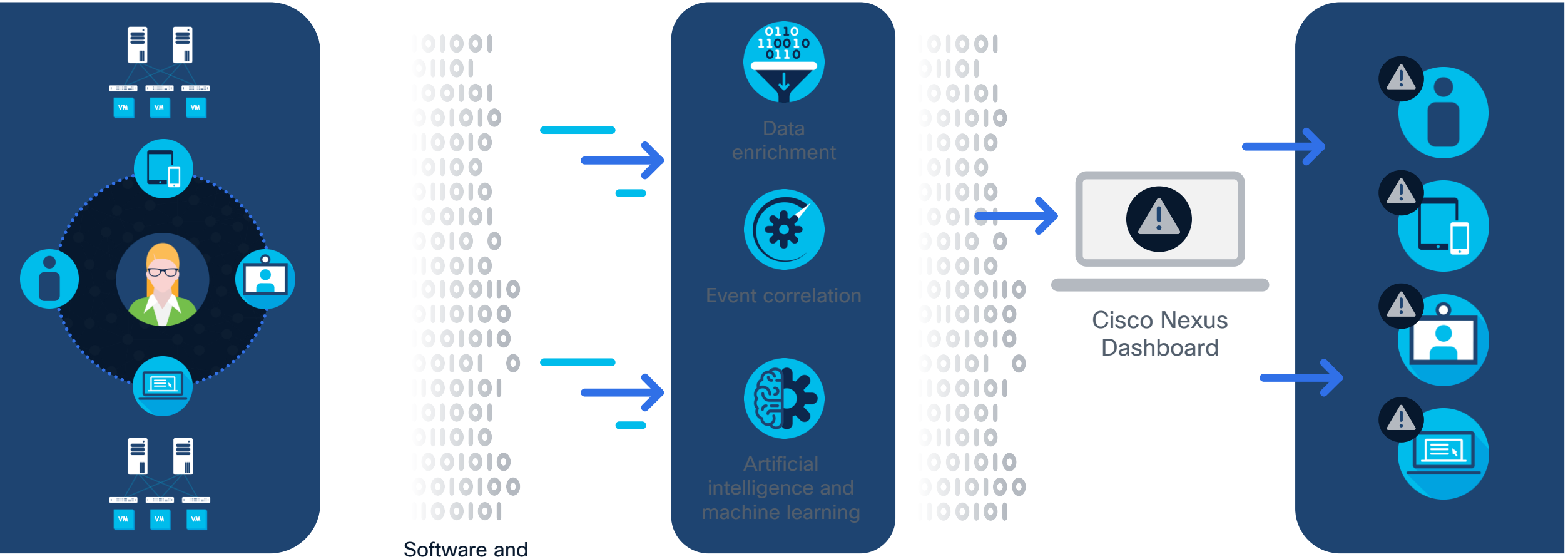
Powering automation
Unified agile platform

Cisco Nexus Dashboard

Simple to automate, simple to consume



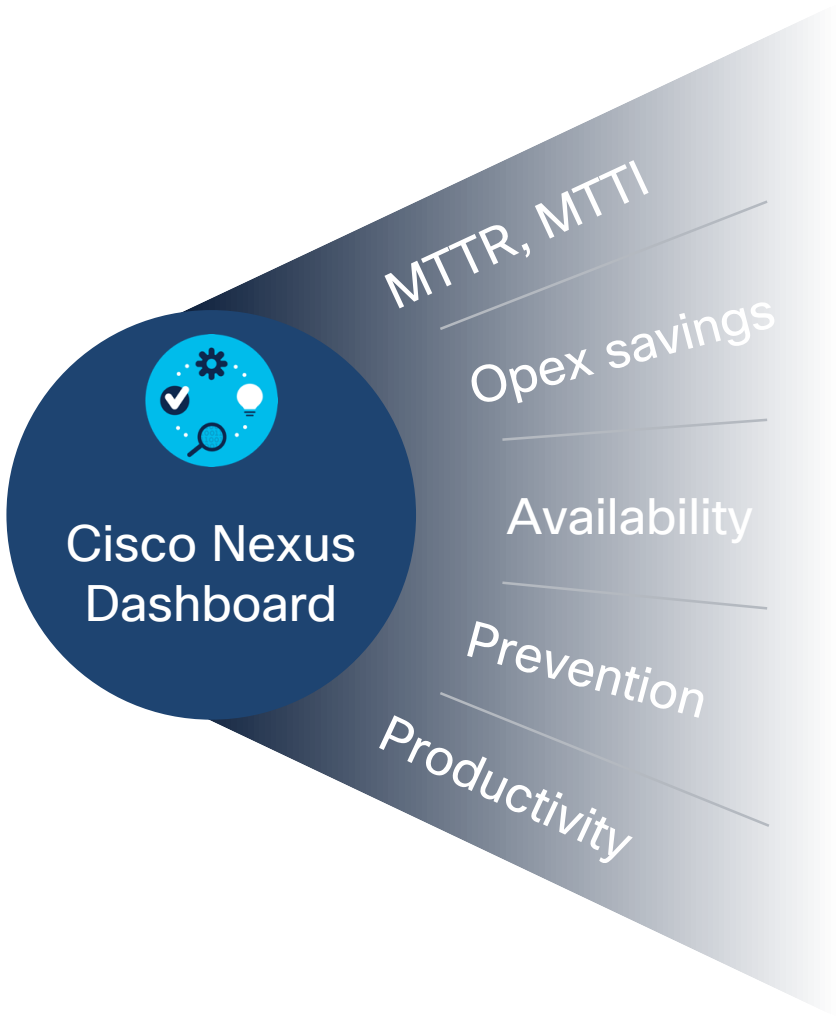
Intelligent operations powered by telemetry



Software and hardware telemetry – from switches and APIC

Cisco Nexus Dashboard

Use cases



- Identify, locate, root cause, remediate
- Upgrade impact advisories
- Error detection, latency, packet drops
- Control plane issue
- Mitigate
- Prevent outages
- Automated alerts
- Explorer
- Hardening checks
- Software hardware recommendations
- Pre-change analysis*
- Compliance alerts
- PSIRT notices
- EoS/EoL notices
- End-to-end workflows
- Guided remediation
- TAC assist
- Topology checker

Key Takeaways

Consistent SDN enabled network policy across all the switches within a fabric

The Multi-site architecture allows the same network policy to be applied across multiple fabrics using Nexus Dashboard as a central manager

Nexus Dashboard enables proactive day 2 operations for ACI to give a better understanding of how the applications interact with network

Complete Your Session Evaluations

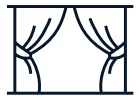
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

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

Contact me at: chmerkel@cisco.com – email and Webex

Thank you

cisco Live !


CISCO