The bridge to possible

Introduction to ACI

BRKDCN-1601

Chris Merkel, DC TSA – CCIE 17841

cisco Live!

#CiscoLive

Cisco Webex App

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

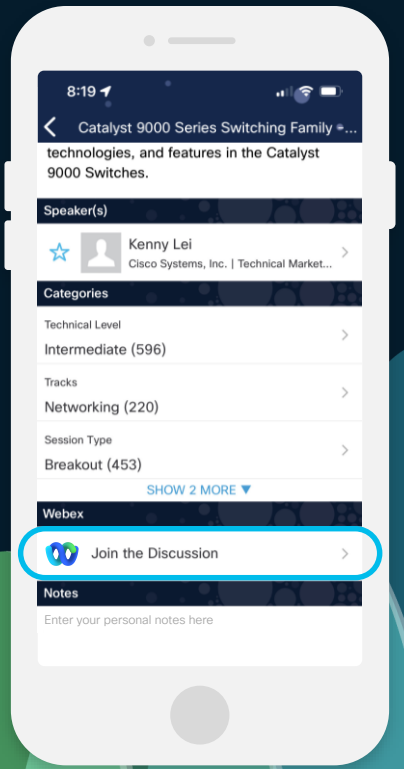
Questions?

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

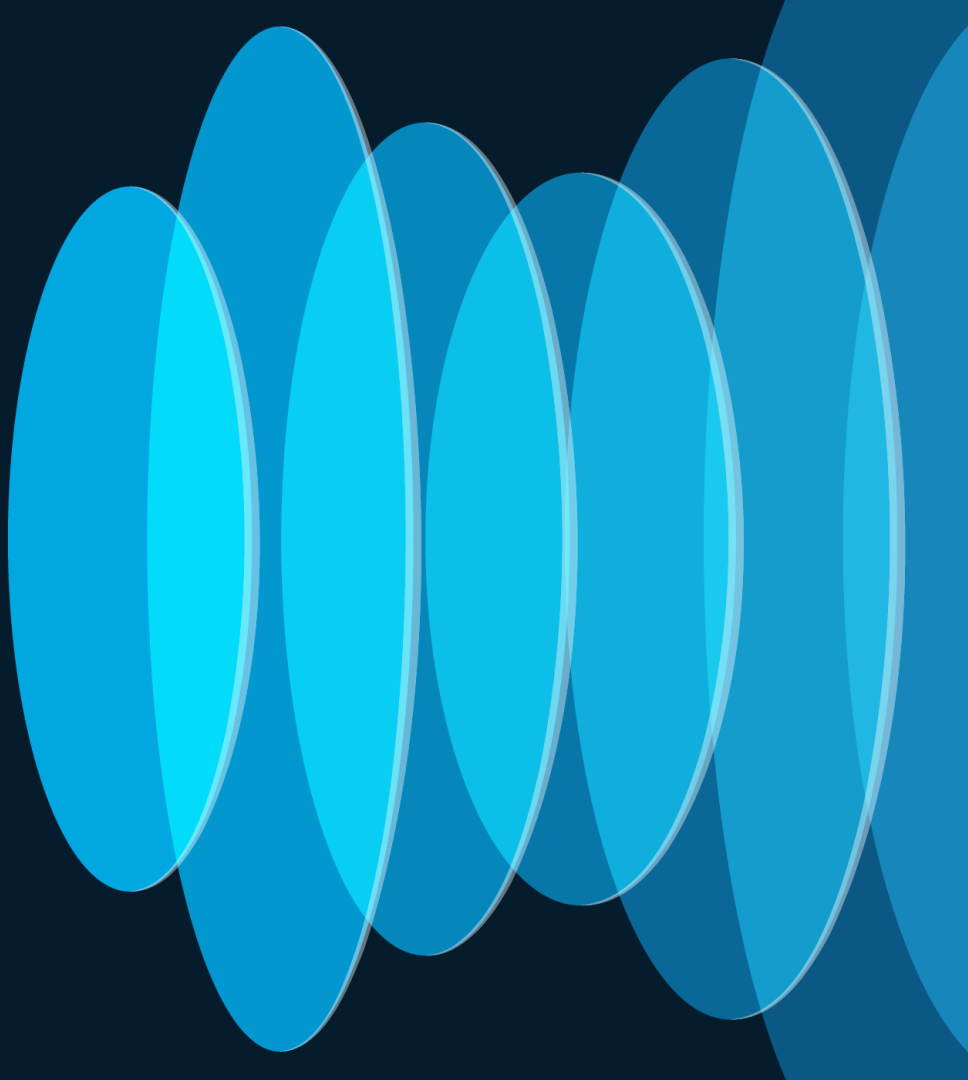
Webex spaces will be moderated by the speaker until June 7, 2024.



Agenda

- Fabric Basics
- Policy Model
- Architectural Deployments
- Day 2 and beyond
- Conclusion

Fabric Basics



ACI: One Network, any location

What is Cisco ACI?

An application centric model- networking framework

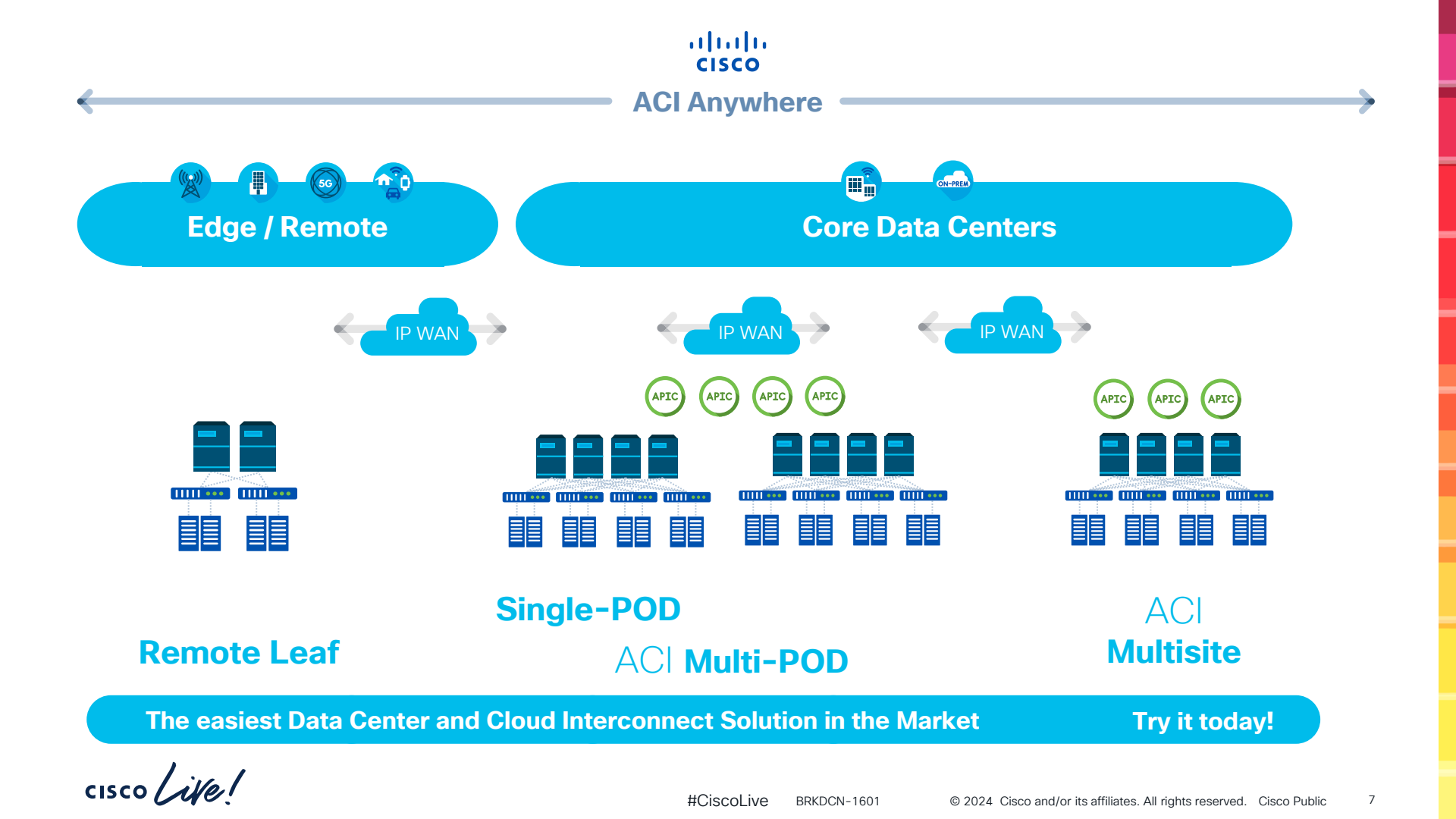
Software-defined network that takes a systems approach to deliver best-in-class automation through integration of hardware, software, physical and virtual elements

Policy-model (application basic components)

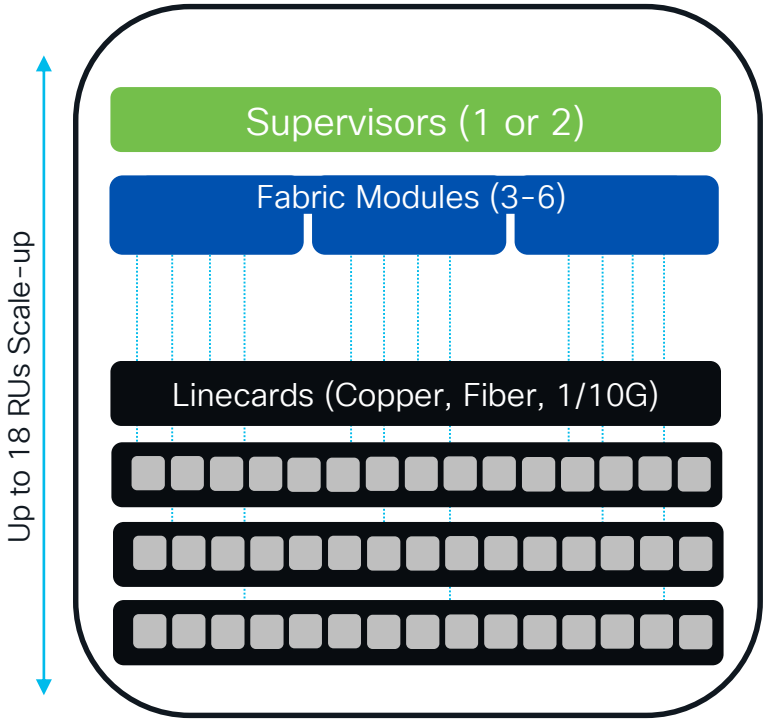
Application Policy Infrastructure Controller (APIC)

Fabric (Cisco Nexus 9000)

The unified point of automation and management for the Cisco ACI fabric, policy enforcement and health monitoring for physical, virtual and cloud infrastructures

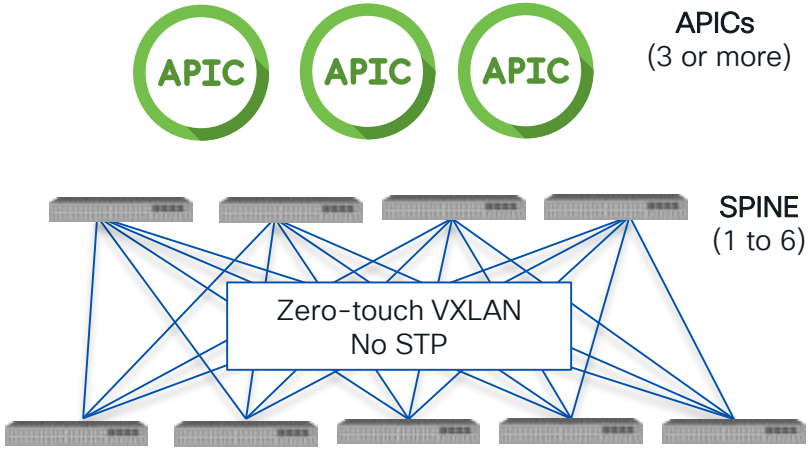


The DC network before
Classic modular switching



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)

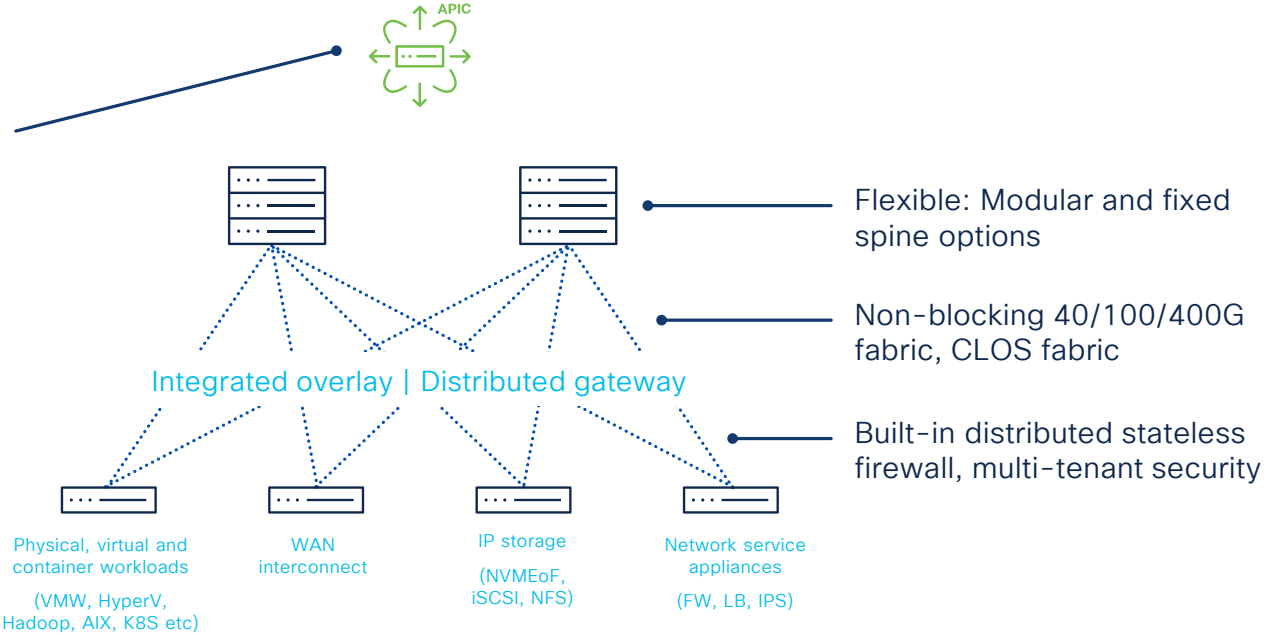
Application Centric Infrastructure building blocks

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

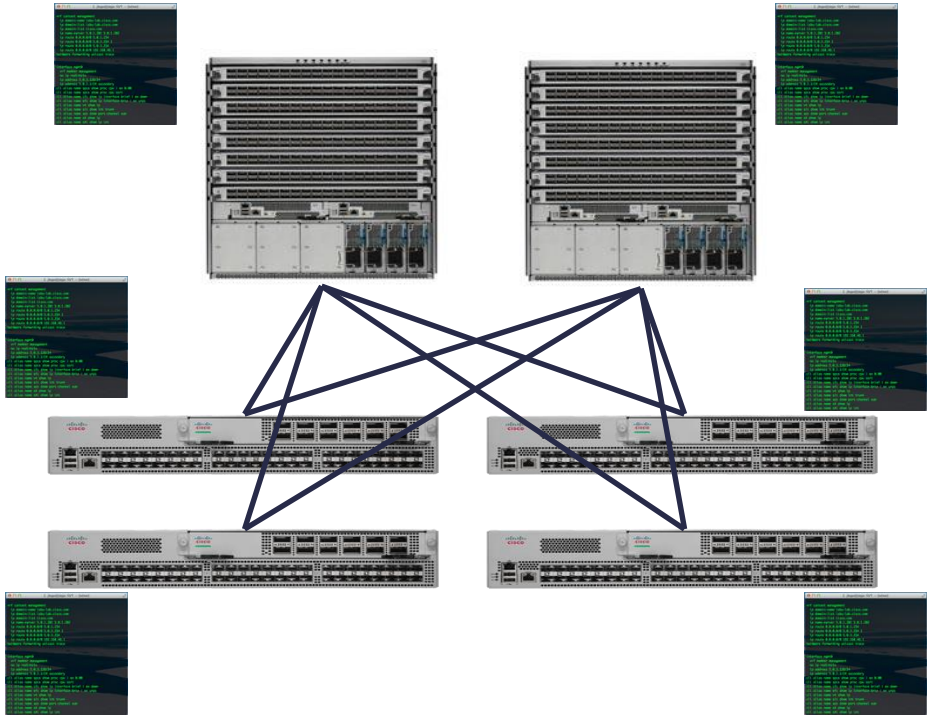
Non-blocking 40/100/400G fabric, CLOS fabric

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

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

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)

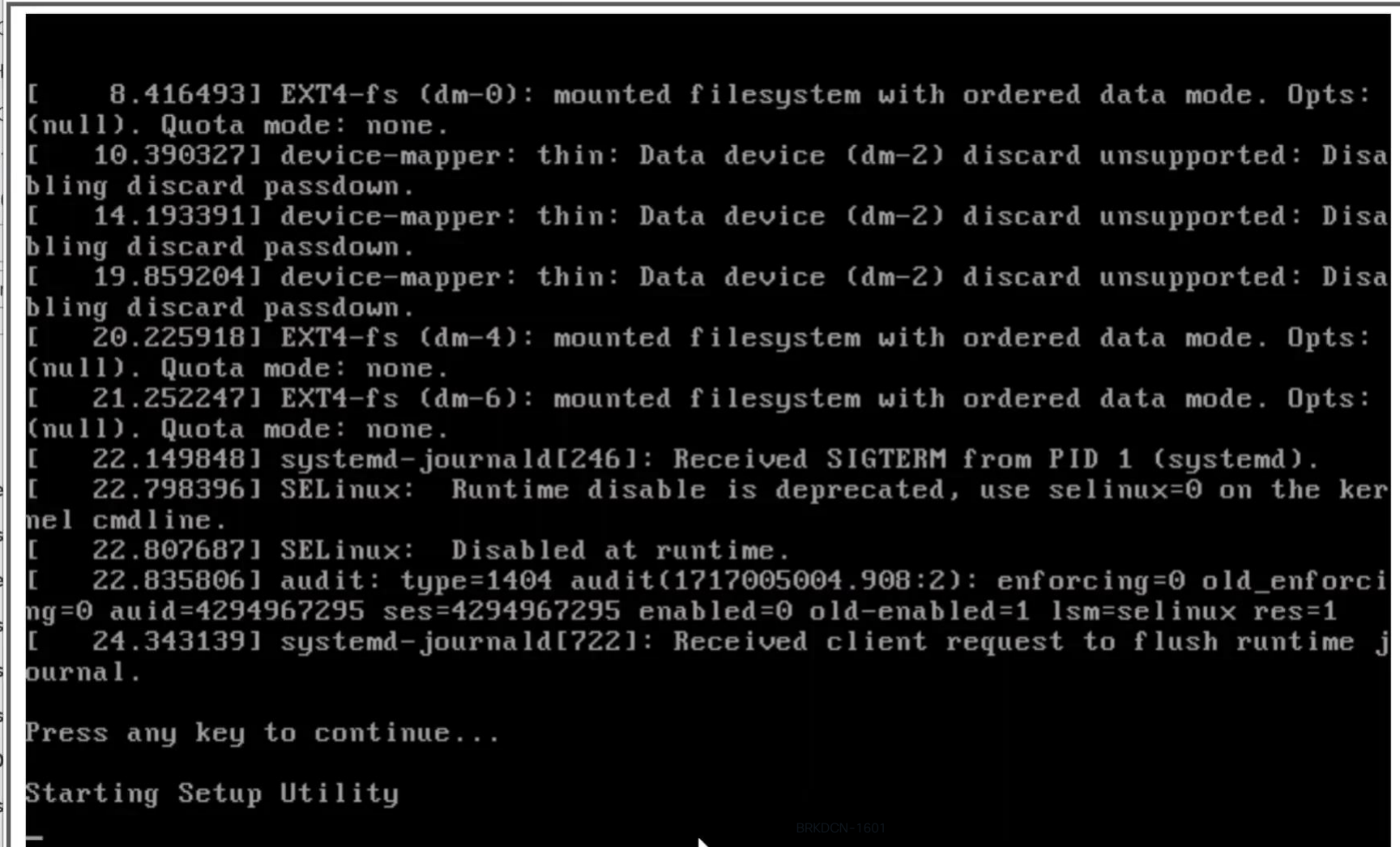
(Times X Switches & Y VNIs)

NOW

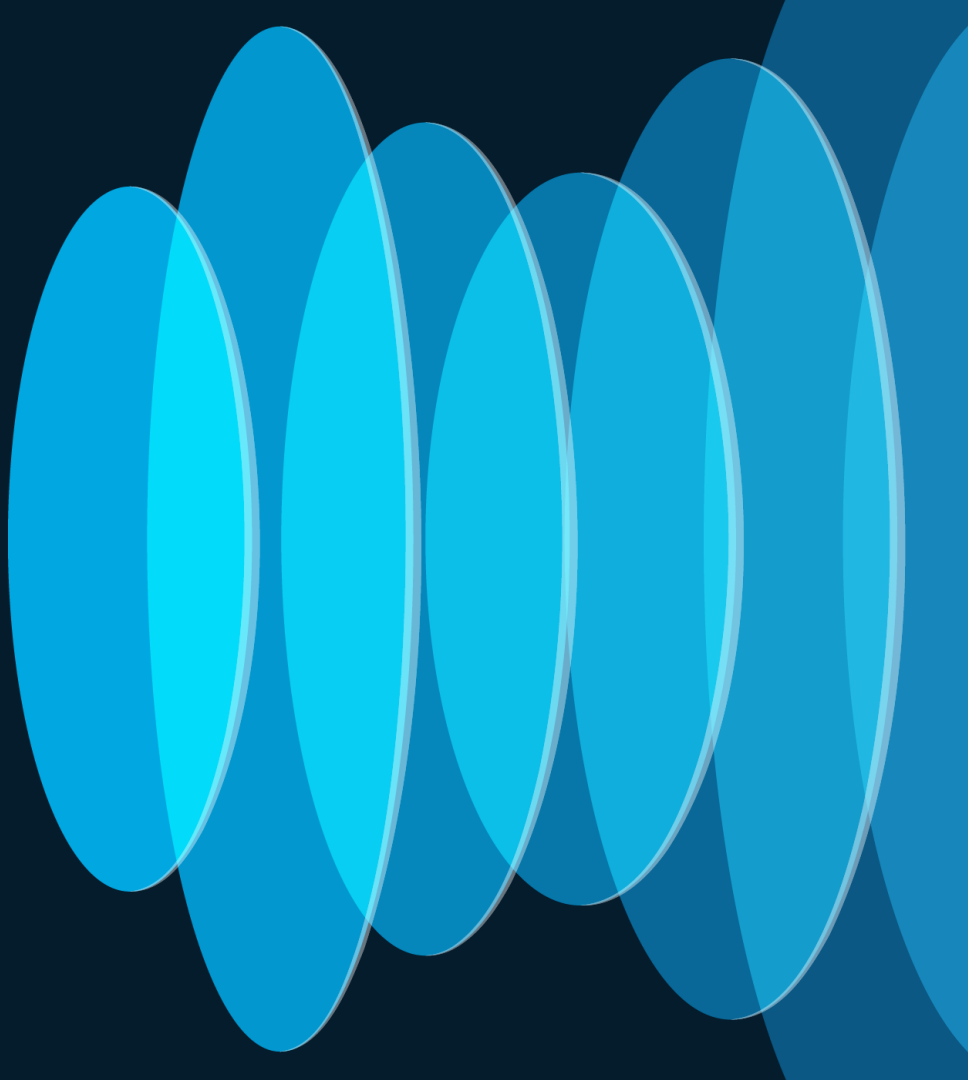
- External to Internal Route redistribution & Control Plane (MP-BGP, QoS, etc)
- Multicast (BD GIPo Addressing)
- Overlay Network (VXLAN)
- Underlay Routed Network (IS-IS)
- Switch management & Best Practices

ACI Automated tasks
From HOURS to seconds!

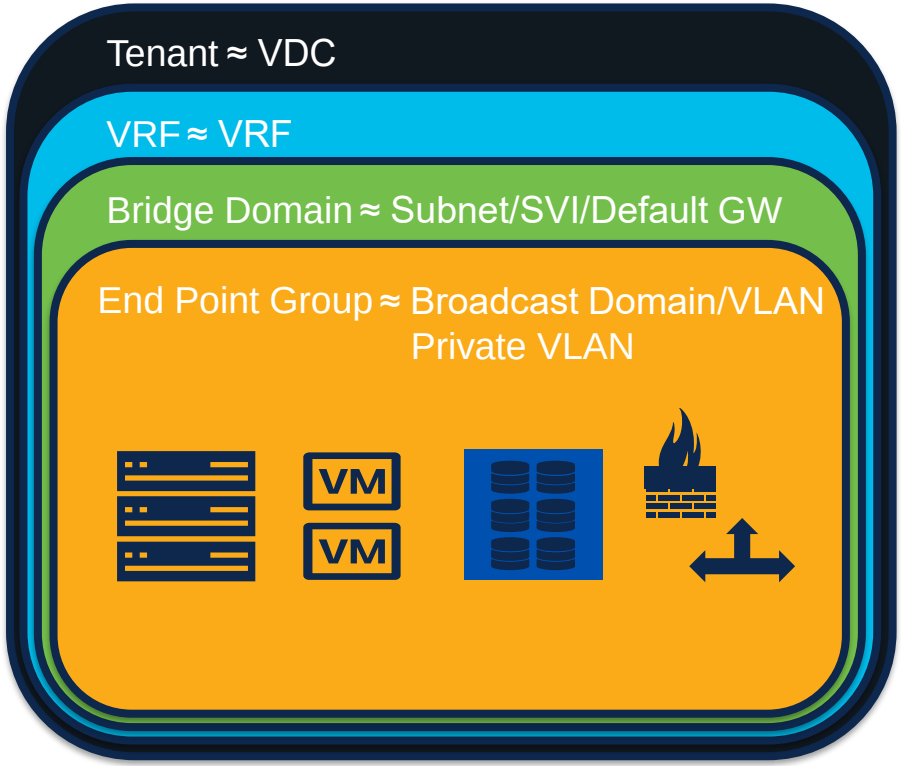
Demo!


[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



Contracts ≈ More Intelligent Access Lists

EPG1 ⟷ EPG2

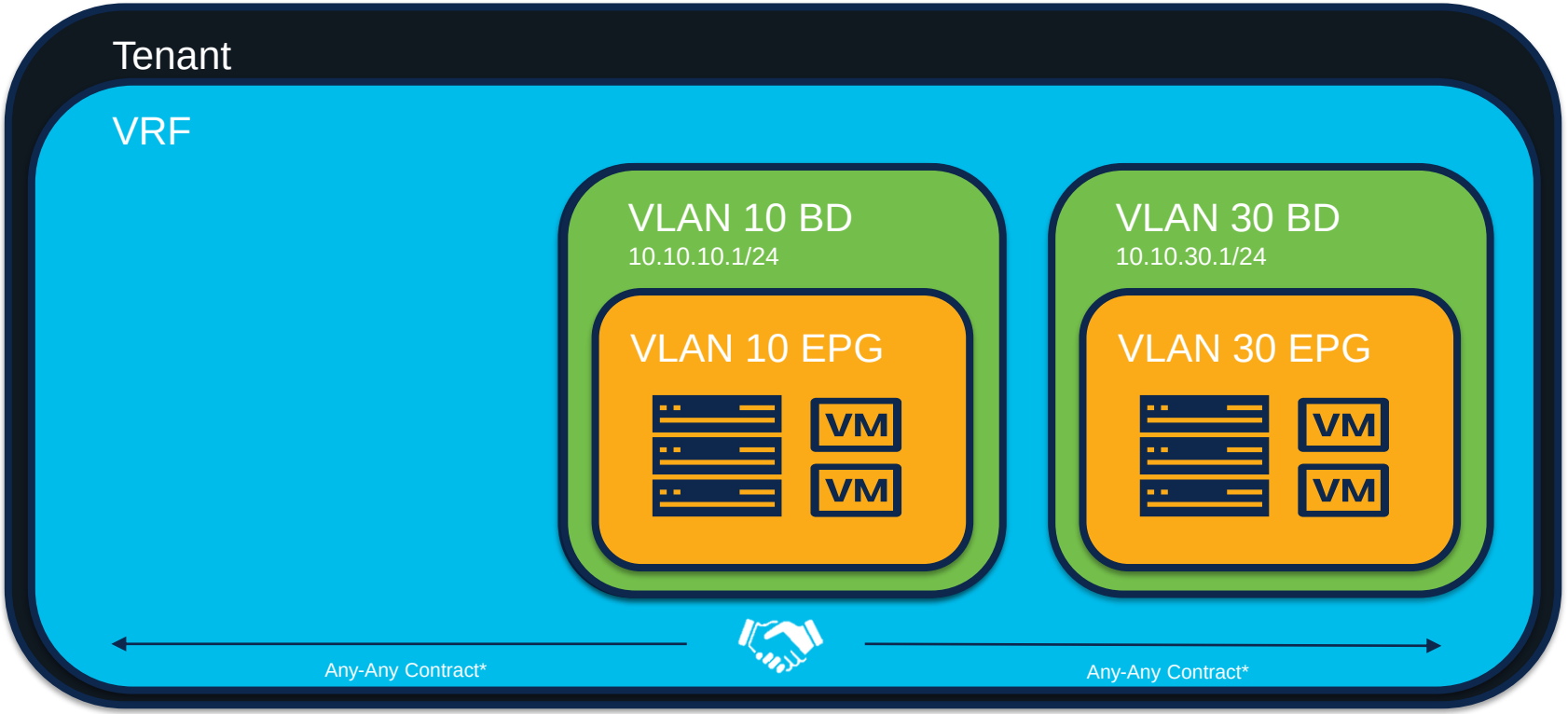
Any-Any (Replicates a Traditional Switch*)

L2 External EPG≈ 802.1q Trunk

L3 External EPG≈ L3 Routed Link

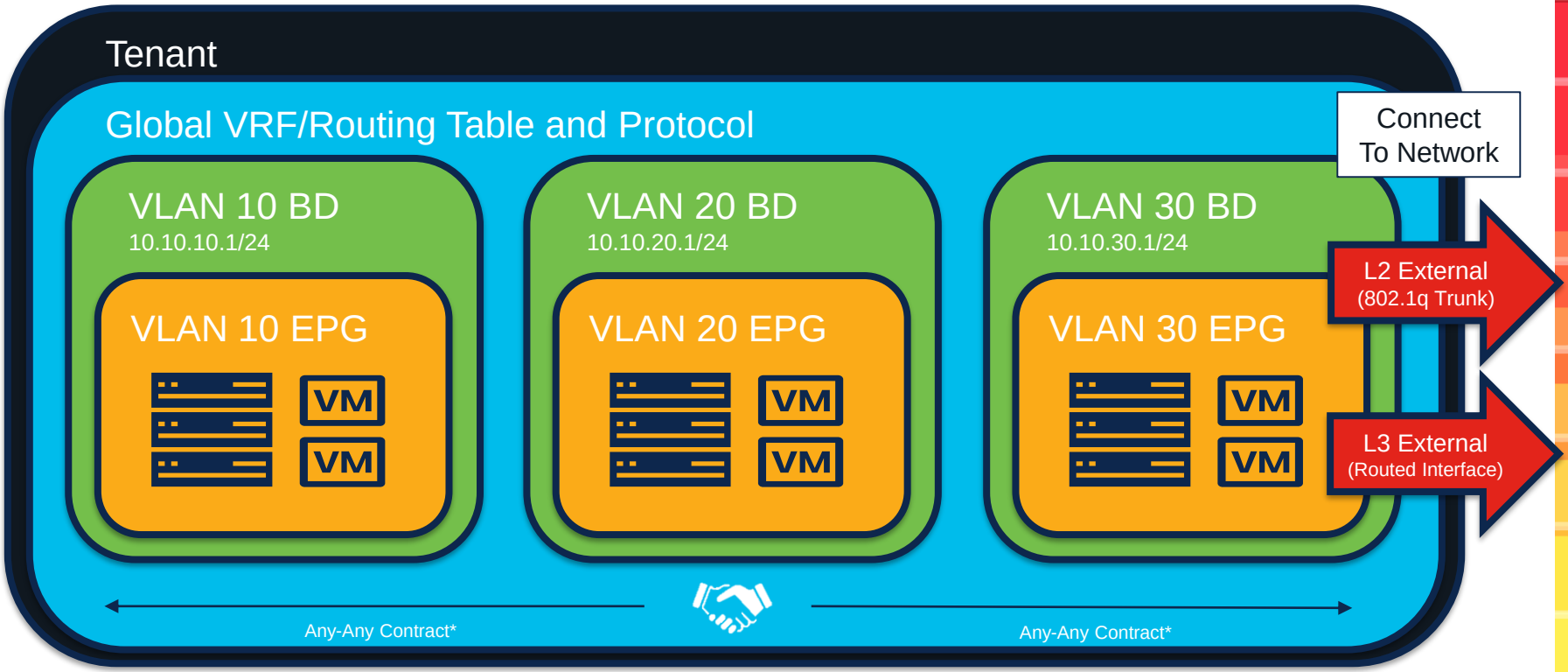
* Preferred group or vzAny Contract achieves the same outcome

The ACI Policy Model – Starting off with ACI



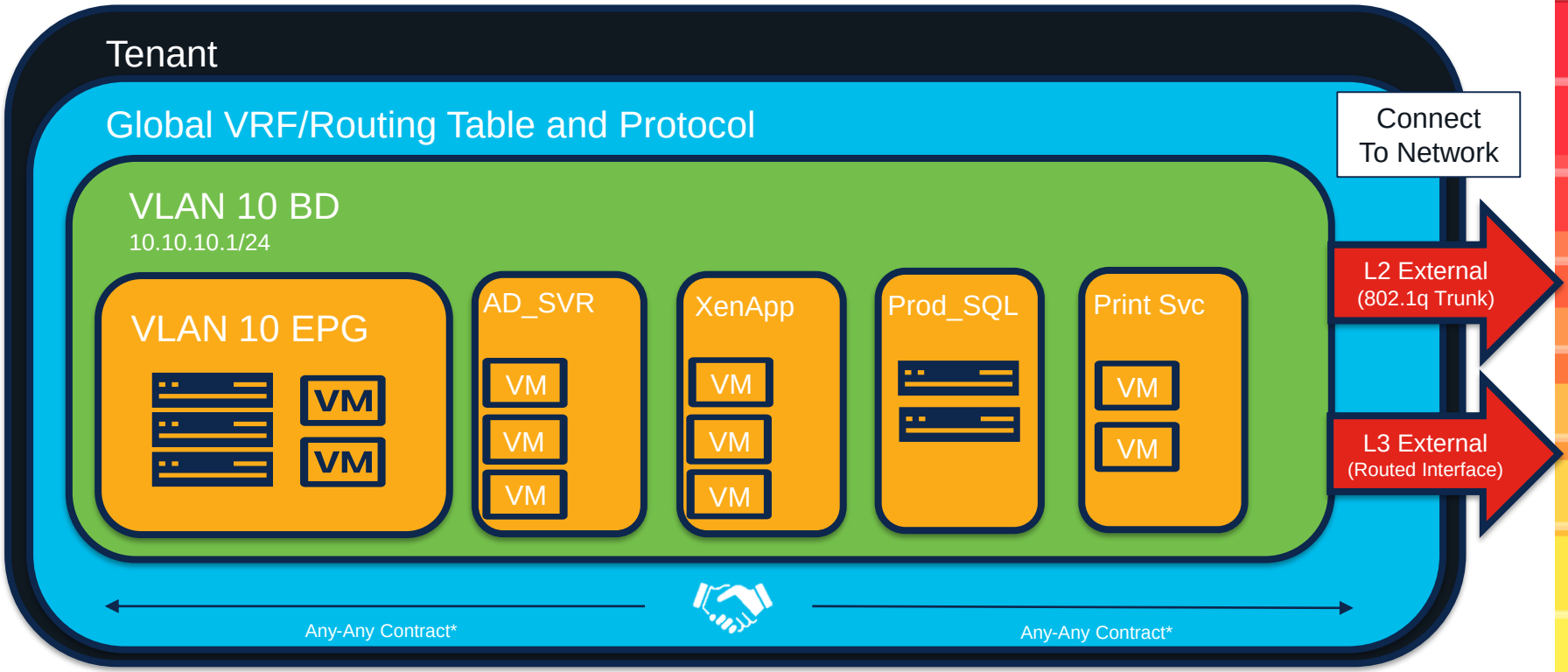
* Preferred group or vzAny Contract achieves the same outcome

The ACI Policy Model – Starting off with ACI



* Preferred group or vzAny Contract achieves the same outcome

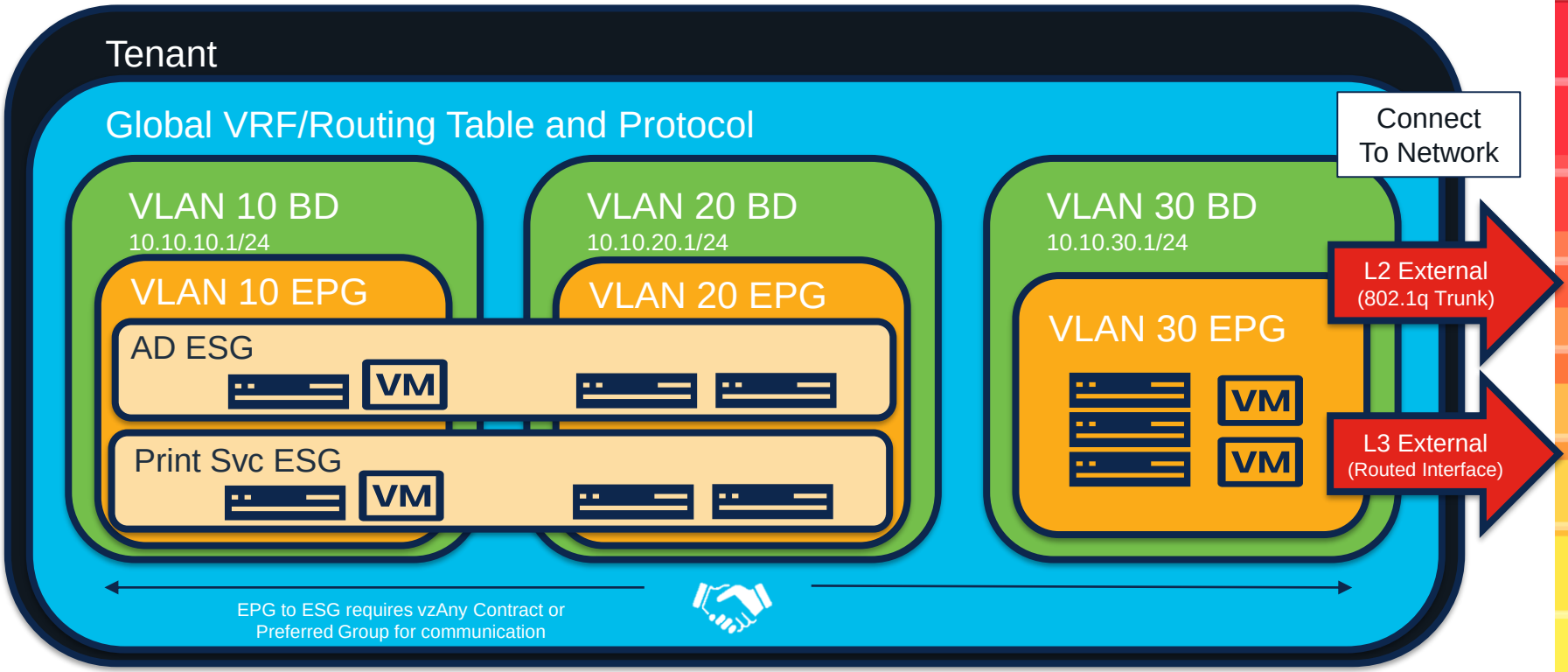
The ACI Policy Model – Extending the configuration
Endpoint Groups



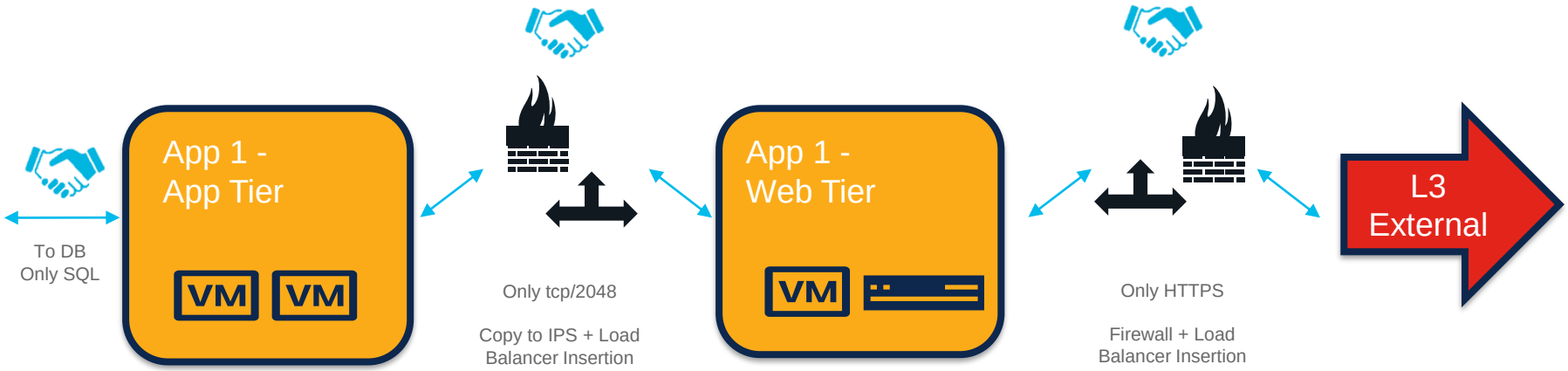
* Preferred group or vzAny Contract achieves the same outcome

The ACI Policy Model – Extending the configuration

Endpoint Security Groups (ESG) - ACI 5.0 and greater



Advancing the ACI Configuration

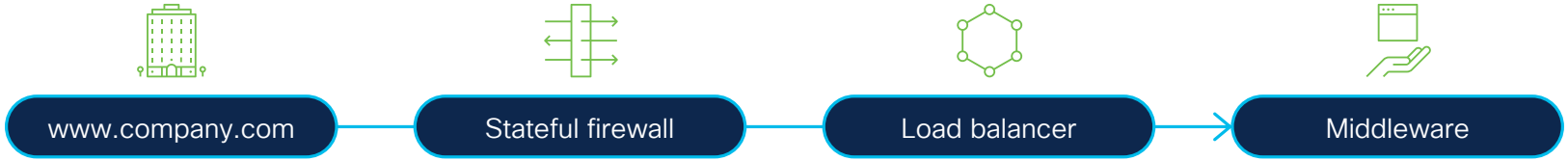


Policy Based Redirect with Service Graphs

Cisco ACI application aware service chaining

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

Flow 1: Requires layer 7 firewalling and load balancing

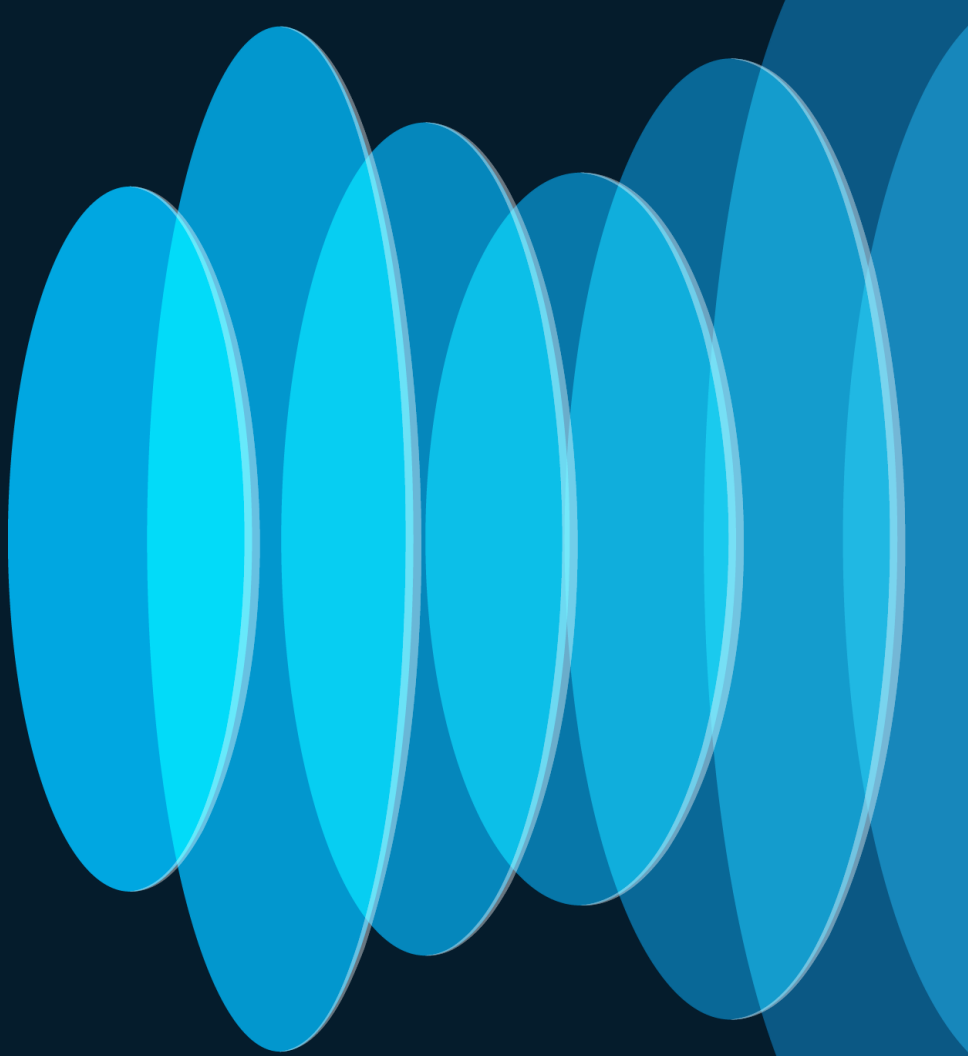


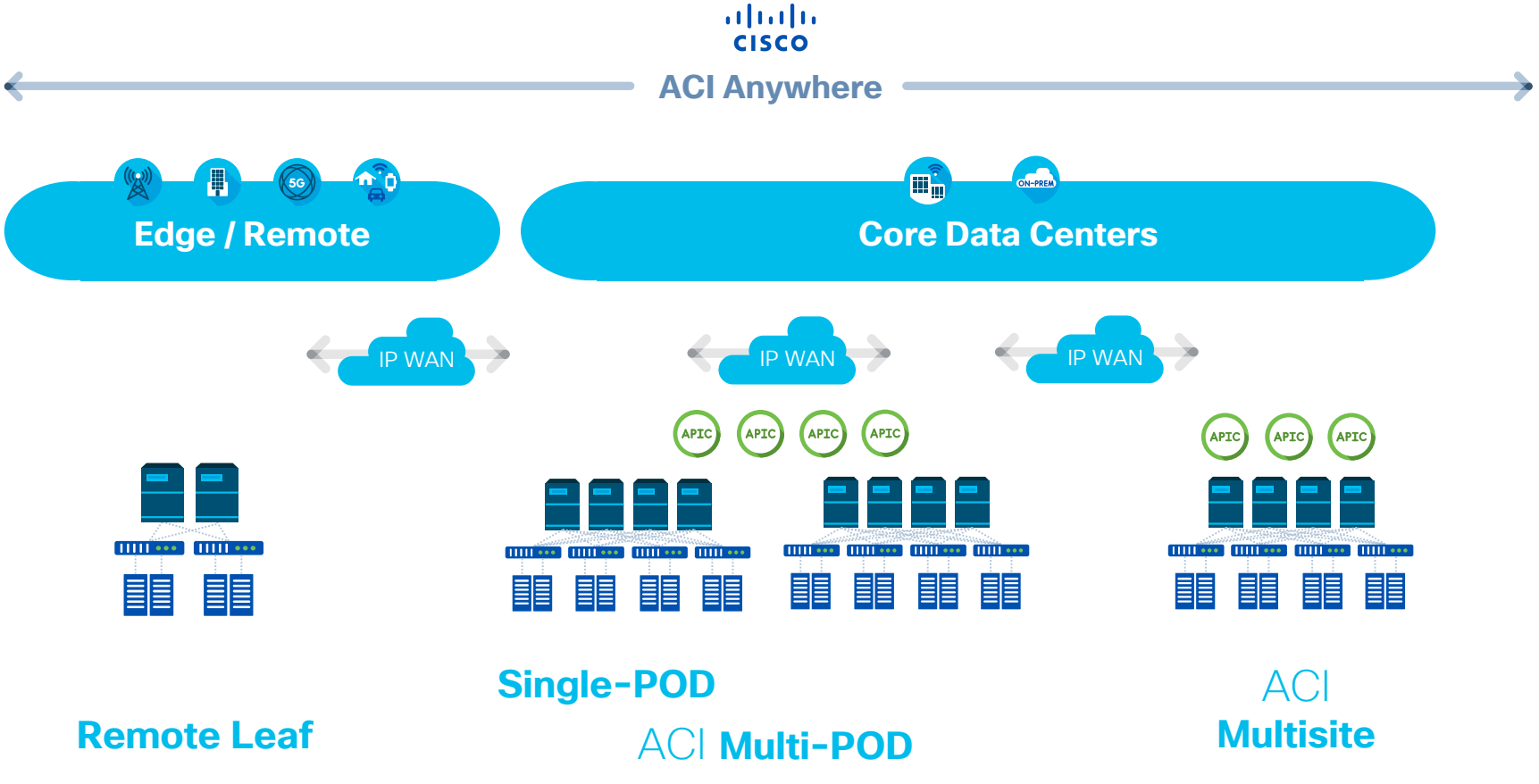
Flows 2 and 3: Do not require stateful firewalling or load balancing; requires ultra-low-latency and/or high bandwidth (performance)

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

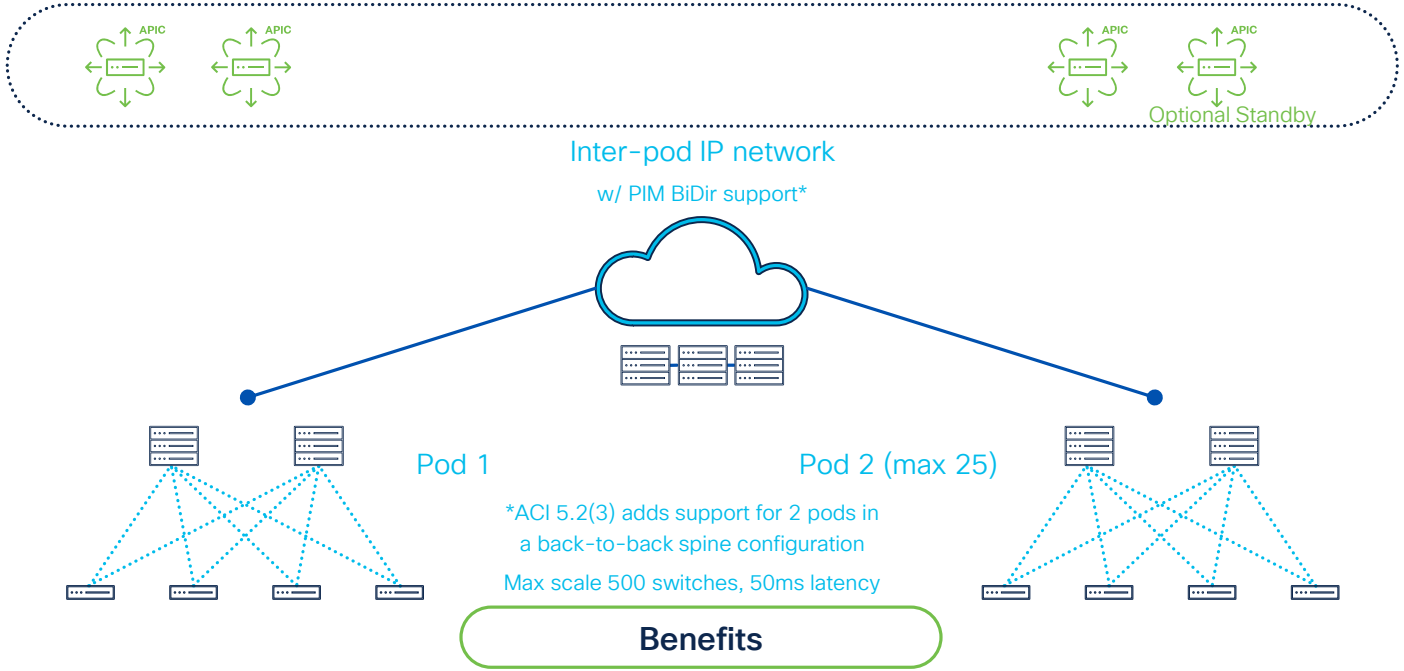
ACI Deployment Options





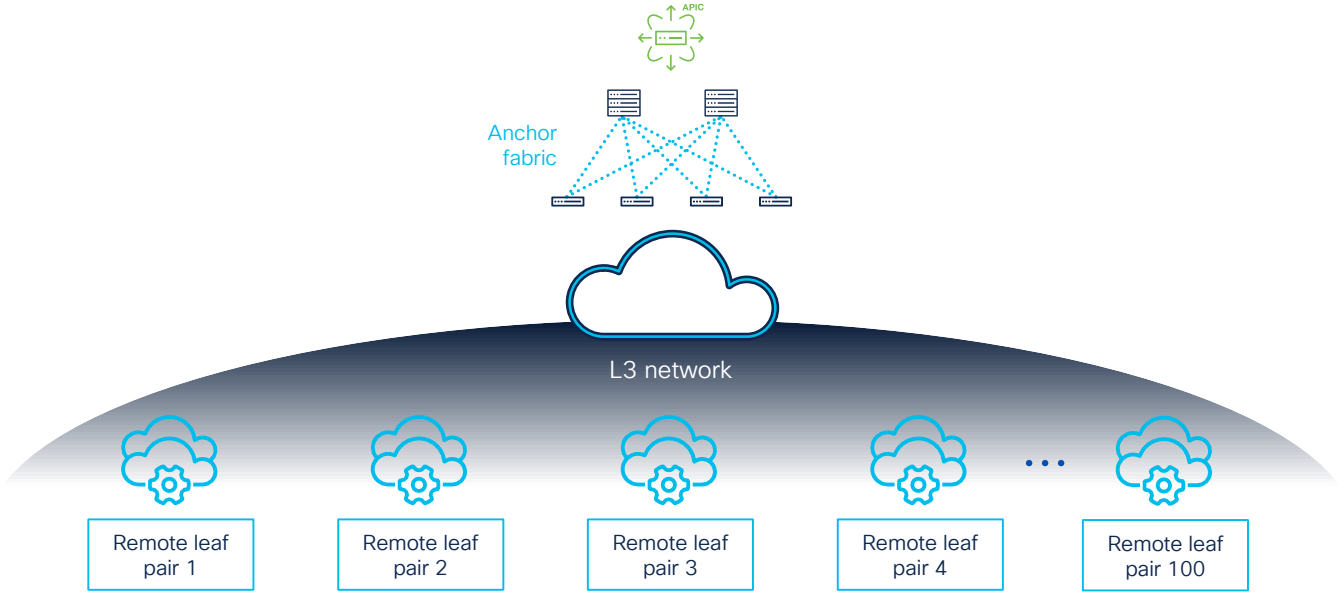
Cisco ACI multi-pod

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



Cisco ACI: Remote leaf

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

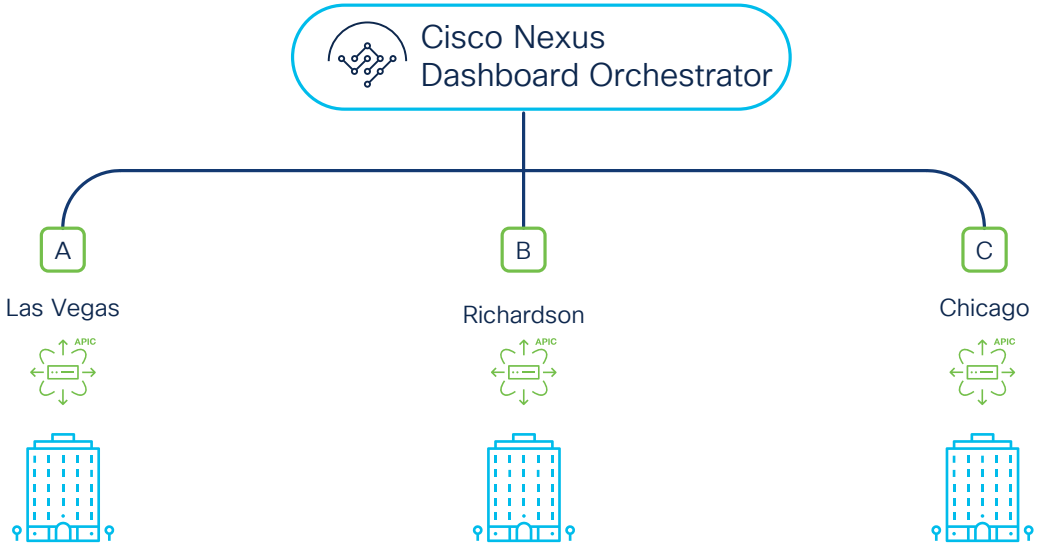


Benefits

- Single management plane for core fabric and remote leaf (RL)
- Up to 200 RLs per site
- 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

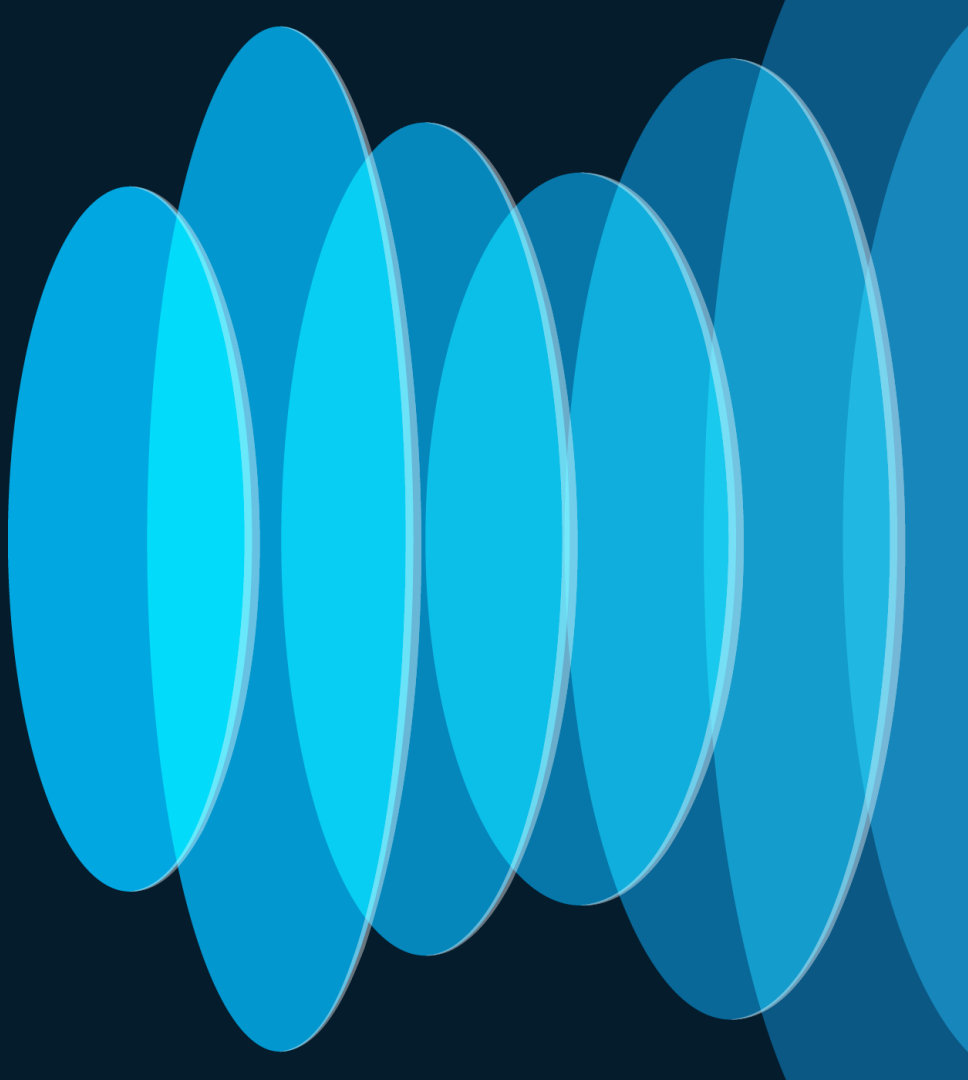
Deploy applications based on geo-performance

Geo-compliance and data privacy

Limit blast radius to a single application geography

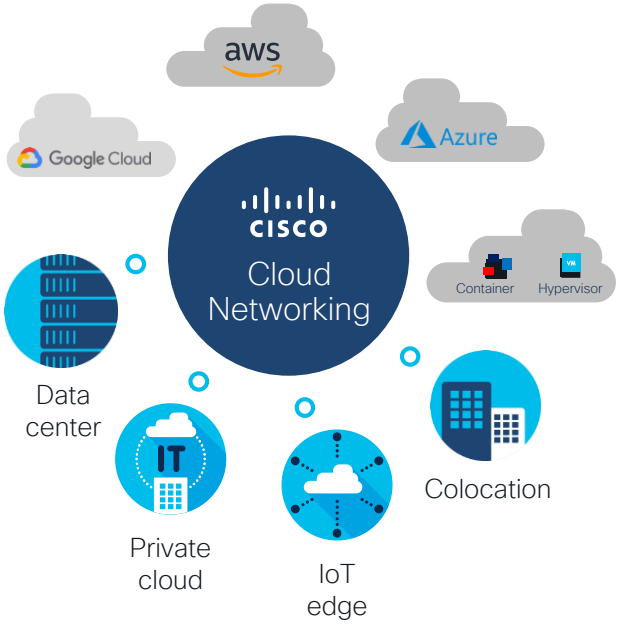
Unify Cisco ACI policy geographically

ACI Day 2 and Beyond – Making ACI Hum



cisco Live!

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.

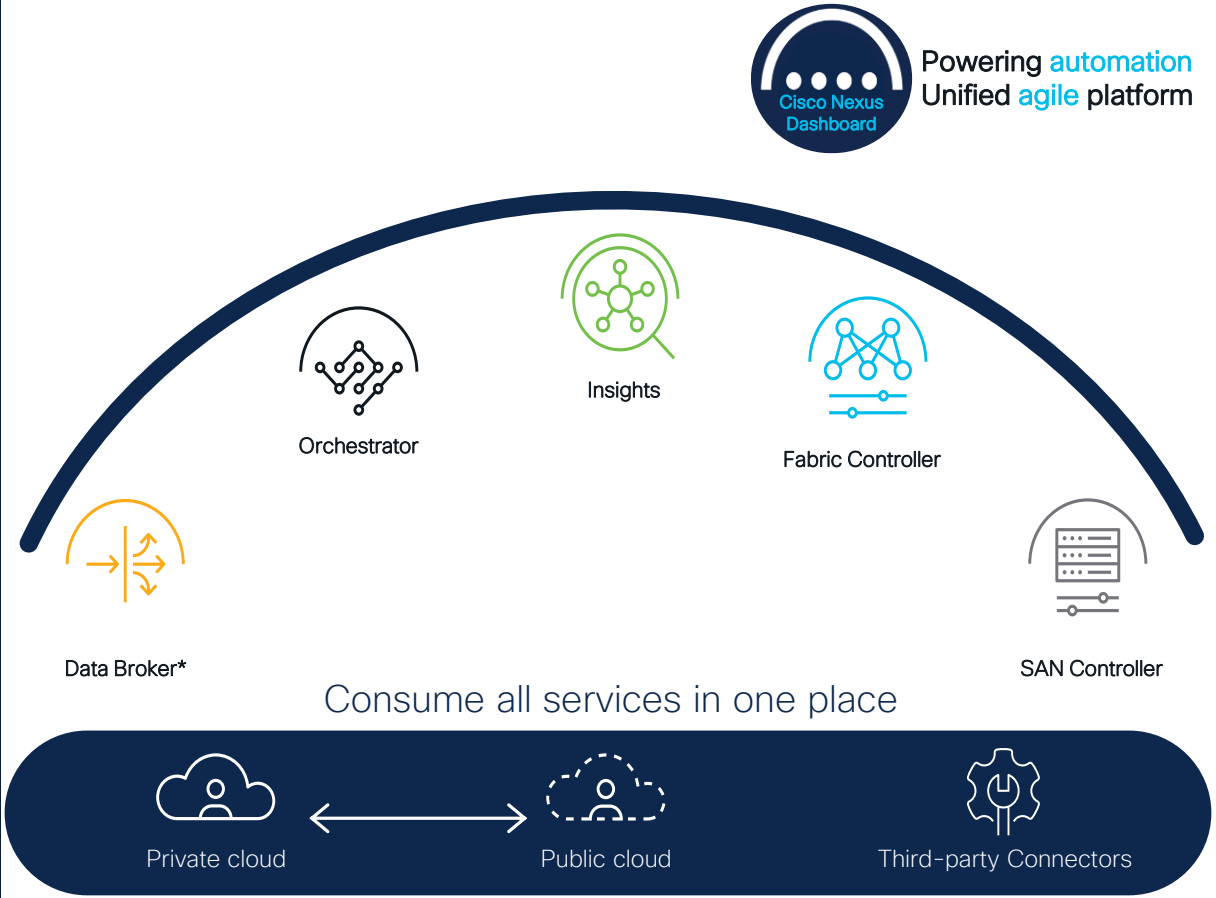
Zero trust and security

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

Cisco Nexus Dashboard

Simple to automate, simple to consume



* Roadmap

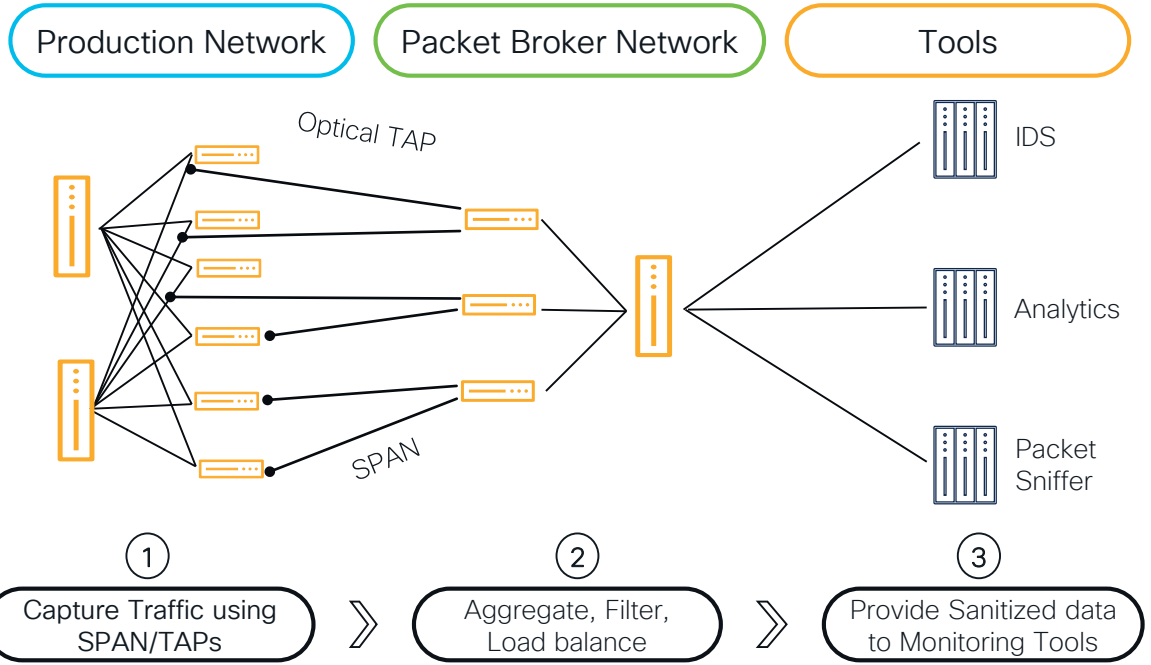
SPAN and Tap Aggregation

Production Network Types

Cisco NX-OS fabrics

Cisco ACI fabrics

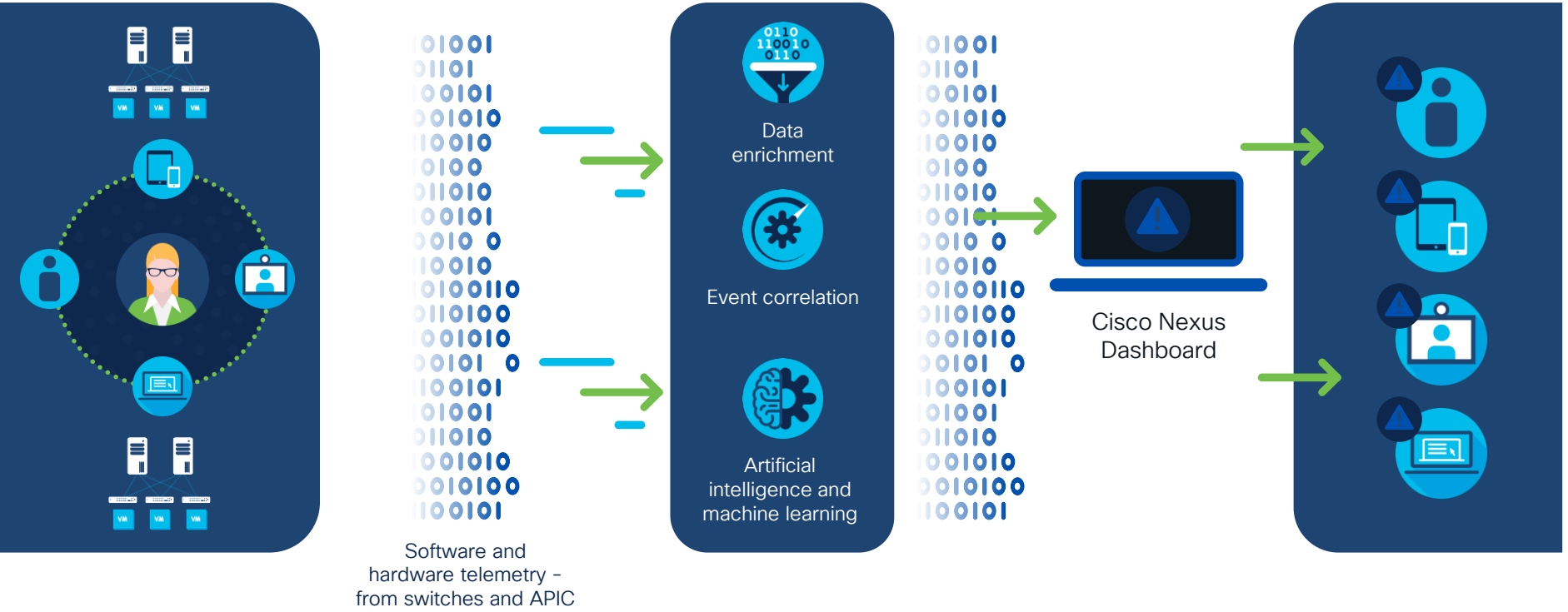
Cisco Enterprise networks



Benefits

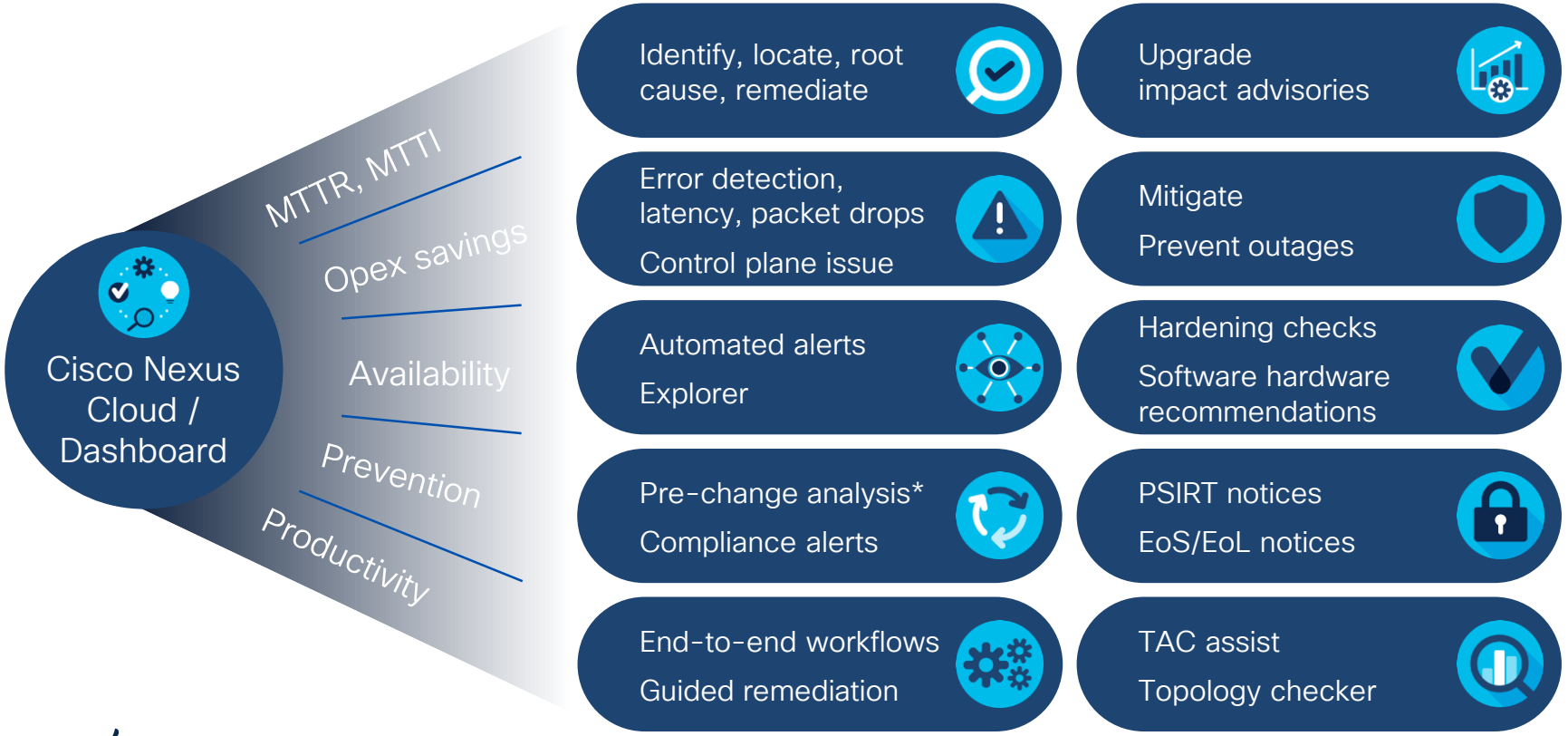
Nexus switch functions as packet broker	Cost effective	Turnkey automation with NDDB Controller	Supports Tap Aggregation and inline redirection

Intelligent operations powered by telemetry



Cisco Nexus Dashboard

Use cases and benefits



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 any number of fabrics
- 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 2025.

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

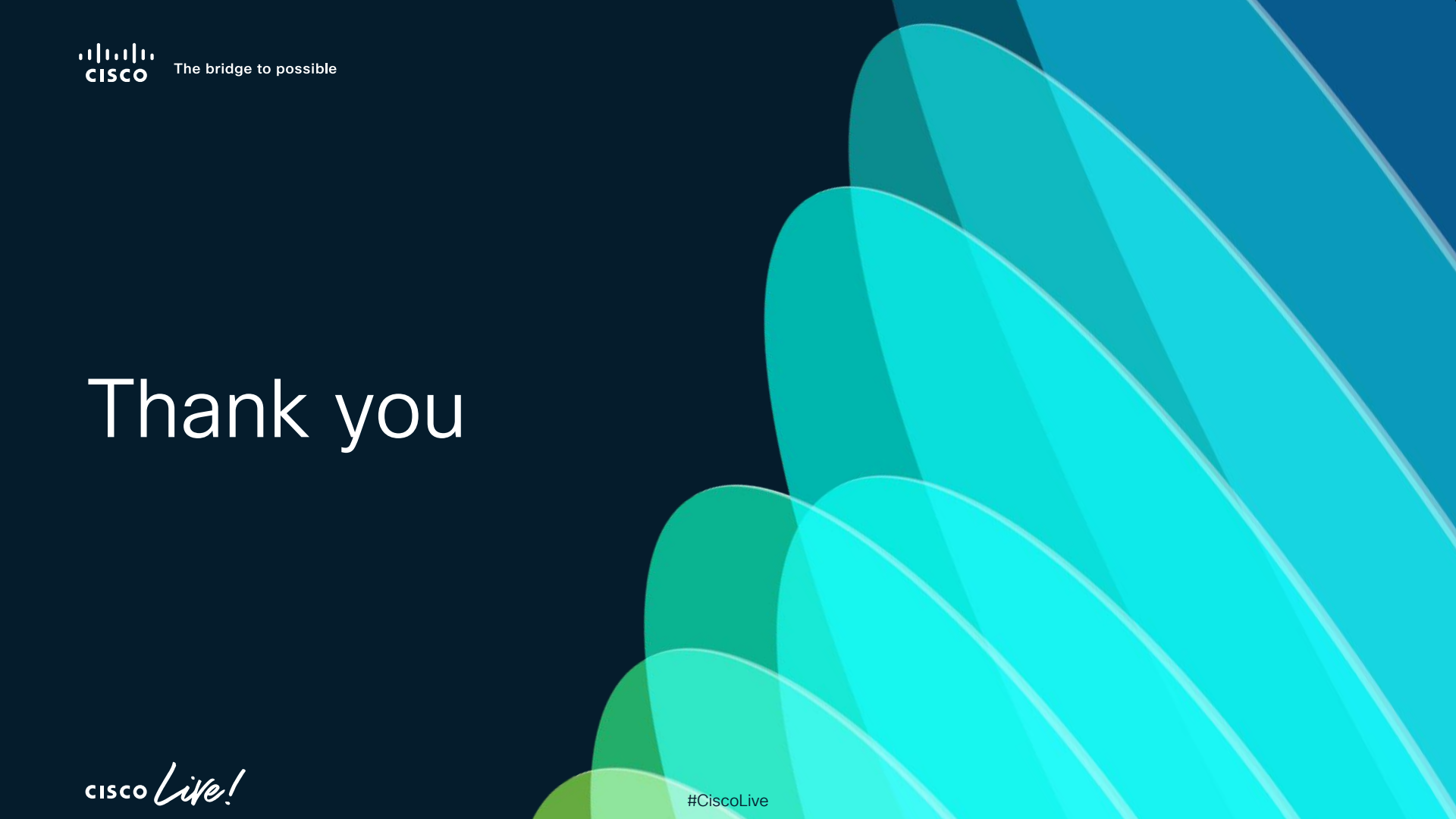
Level up and earn **exclusive prizes!**

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


The bridge to possible
Thank you
cisco Live!
#CiscoLive