
cisco
Cisco live!
7-10 March 2017 · Melbourne, Australia
Your Time Is Now

Application Centric Infrastructure Fundamentals

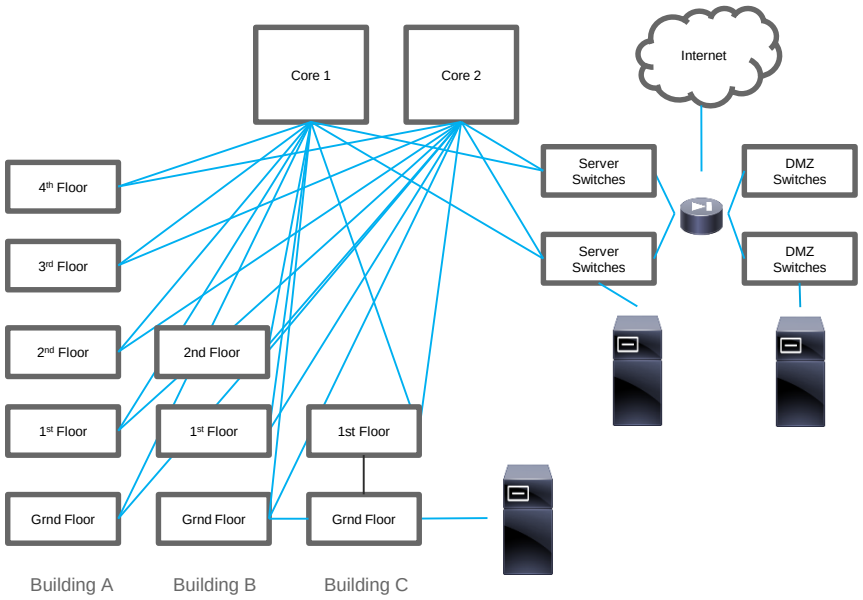
Nicholas Gorse – System Engineer

BRKACI-2000

Cisco live!

About Me

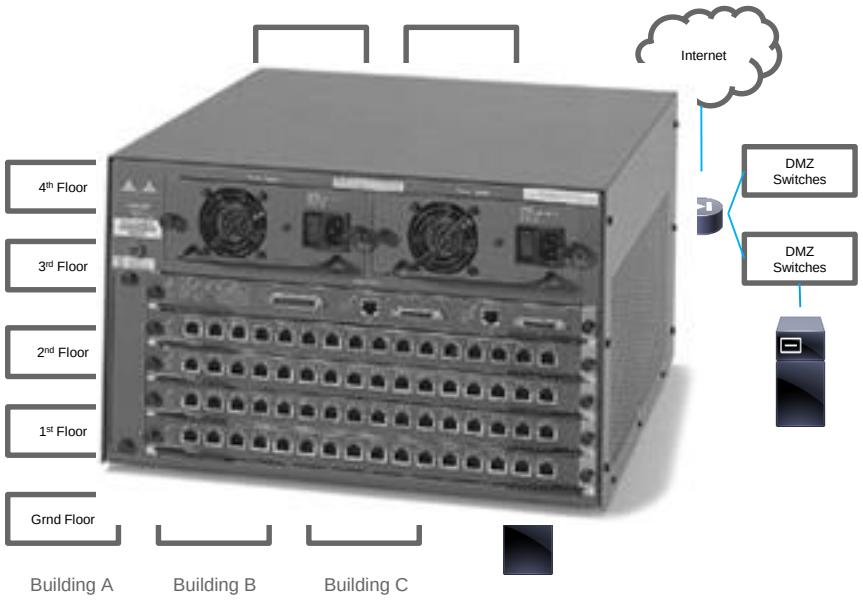
- Been at Cisco since 2014
- System Engineer specialising in Data Centre
- Started in Networking (on Novell) in 1997
- The first network I worked on was for Higher Education here in Melbourne that looked like…



This Design was constrained by the connections to the buildings and make sure Students weren't on the Staff Network

About Me

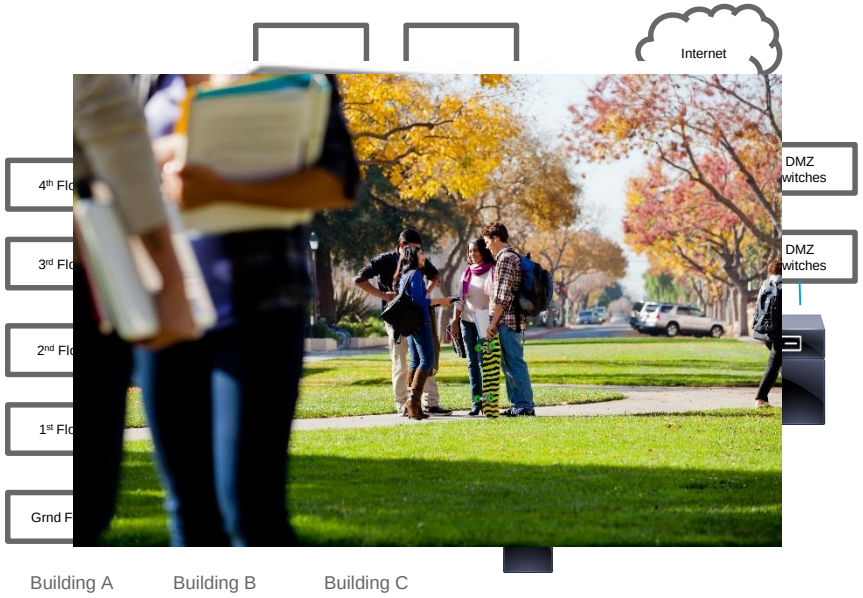
- Been at Cisco since 2014
- System Engineer specialising in Data Centre
- Started in Networking (on Novell) in 1997
- The first network I worked on was for Higher Education here in Melbourne that looked like…



This Design was constrained by the connections to the buildings and make sure Students weren't on the Staff Network

About Me

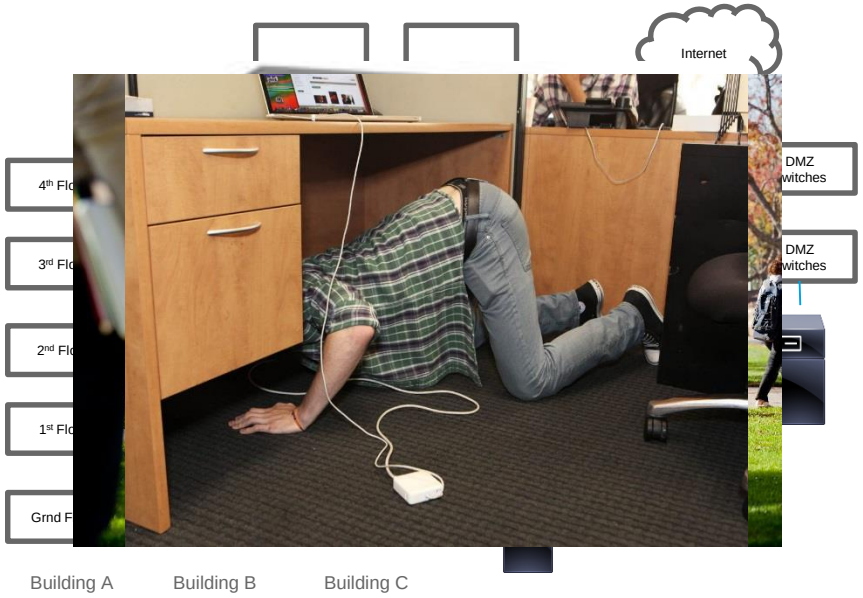
- Been at Cisco since 2014
- System Engineer specialising in Data Centre
- Started in Networking (on Novell) in 1997
- The first network I worked on was for Higher Education here in Melbourne that looked like…



This Design was constrained by the connections to the buildings and make sure Students weren't on the Staff Network

About Me

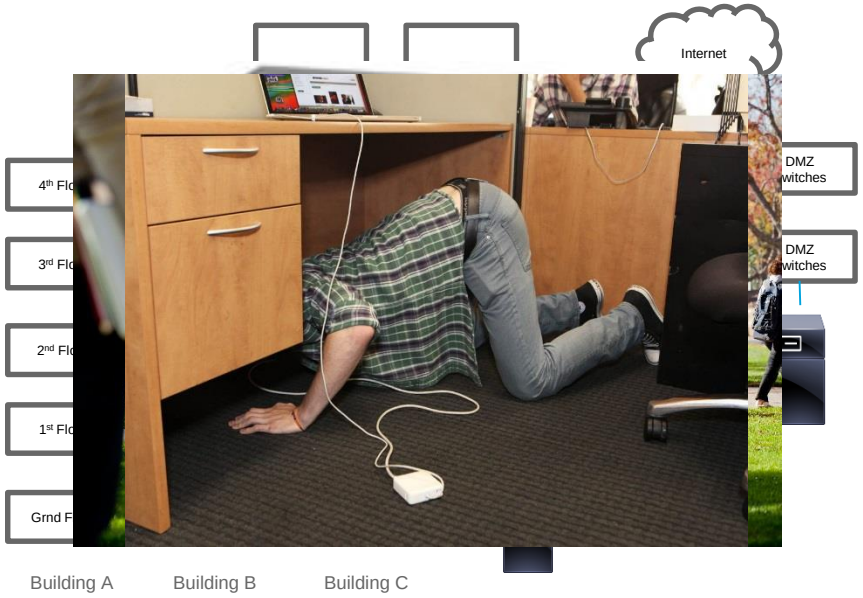
- Been at Cisco since 2014
- System Engineer specialising in Data Centre
- Started in Networking (on Novell) in 1997
- The first network I worked on was for Higher Education here in Melbourne that looked like…



This Design was constrained by the connections to the buildings and make sure Students weren't on the Staff Network

About Me

- Been at Cisco since 2014
- System Engineer specialising in Data Centre
- Started in Networking (on Novell) in 1997
- The first network I worked on was for Higher Education here in Melbourne that looked like…

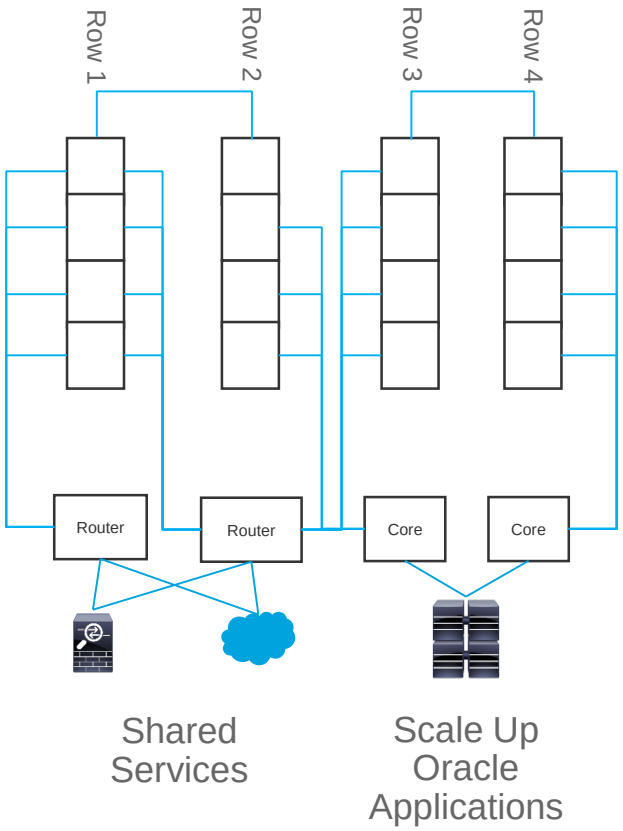


This Design was constrained by the connections to the buildings and make sure Students weren't on the Staff Network

About Me cont…

- Then I worked for a company that hosted a large Oracle applications for multiple customers
- Provided Hosting Services for customer infrastructure, including access to shared services like Internet and Firewall
- Had different size locations around the world…

This Design was constrained by the process of creating customer networks and isolating traffic while providing access to the hosted applications



About Me cont…

- Then I worked for a company that hosted a large Oracle applications for multiple customers
- Provided Hosting Services for customer infrastructure, including access to shared services like Internet and Firewall
- Had different size locations around the world…

This Design was constrained by the process of creating customer networks and isolating traffic while providing access to the hosted applications

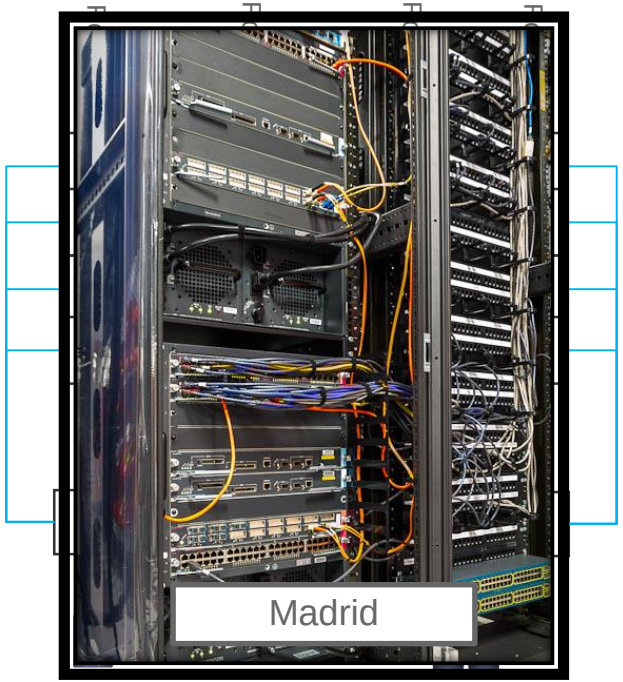
Shared Services

Scale Up Oracle Applications

About Me cont…

- Then I worked for a company that hosted a large Oracle applications for multiple customers
- Provided Hosting Services for customer infrastructure, including access to shared services like Internet and Firewall
- Had different size locations around the world…

This Design was constrained by the process of creating customer networks and isolating traffic while providing access to the hosted applications



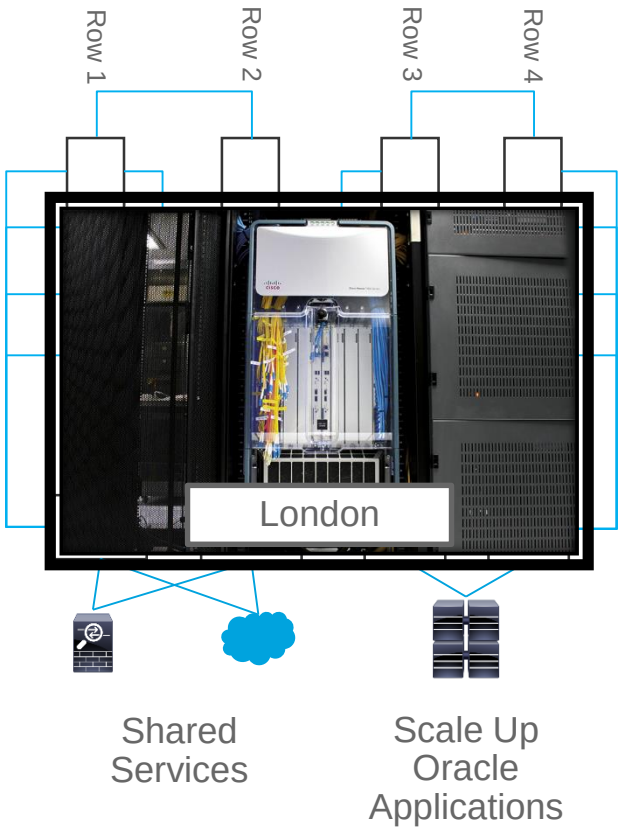
Shared Services

Scale Up Oracle Applications

About Me cont…

- Then I worked for a company that hosted a large Oracle applications for multiple customers
- Provided Hosting Services for customer infrastructure, including access to shared services like Internet and Firewall
- Had different size locations around the world…

This Design was constrained by the process of creating customer networks and isolating traffic while providing access to the hosted applications



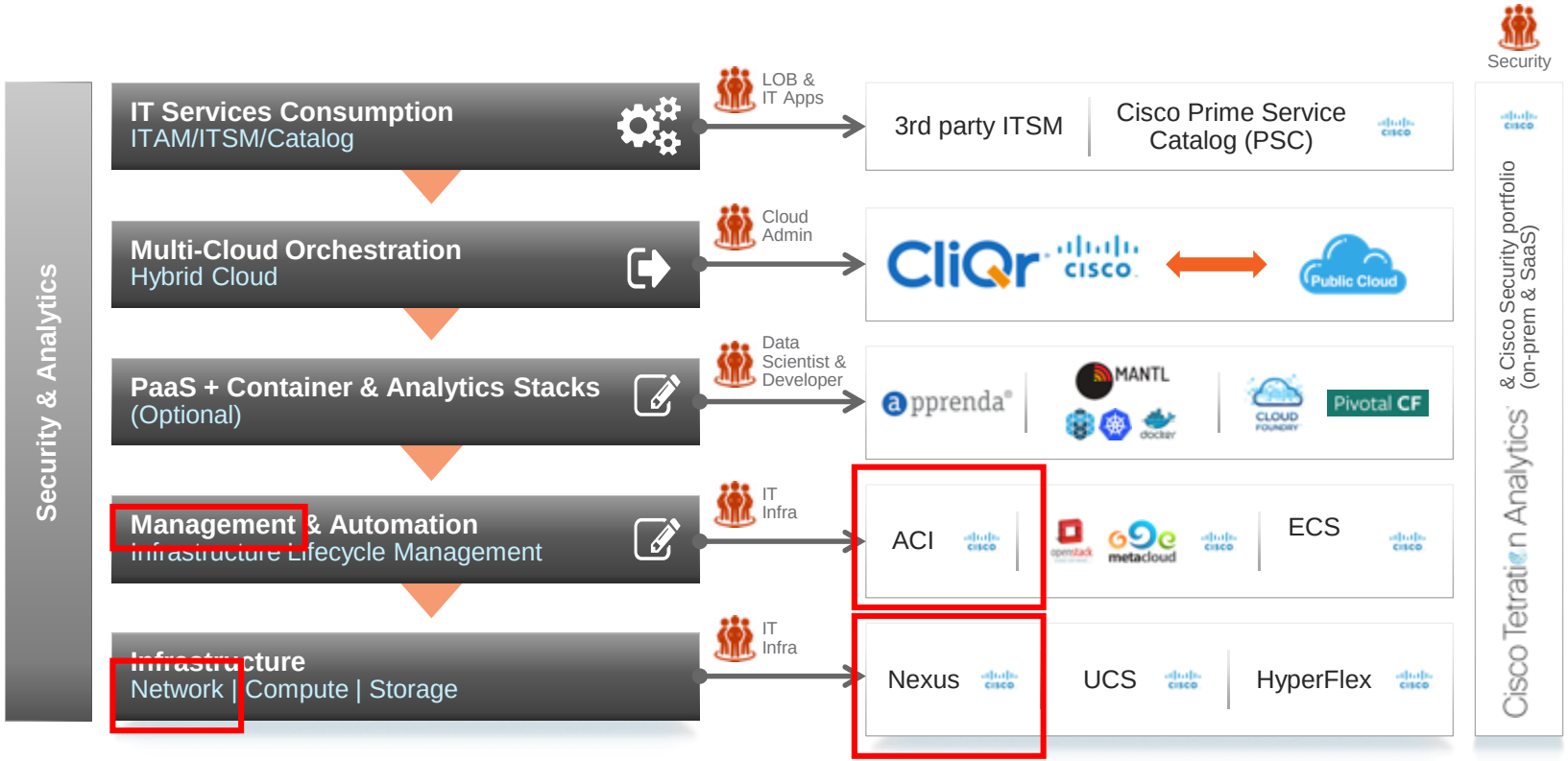
What I Learnt From Those Networks

1. The physical network constraints invariably dictate the design
2. Networks state exist device per device
3. Simplicity/Complexity of Operation dictated by Design
4. That I Wish I had Cisco Application Centric Infrastructure

Agenda

- Introduction
- System Building Blocks
- Forwarding Packets
- More Than Switching
- Wrap Up

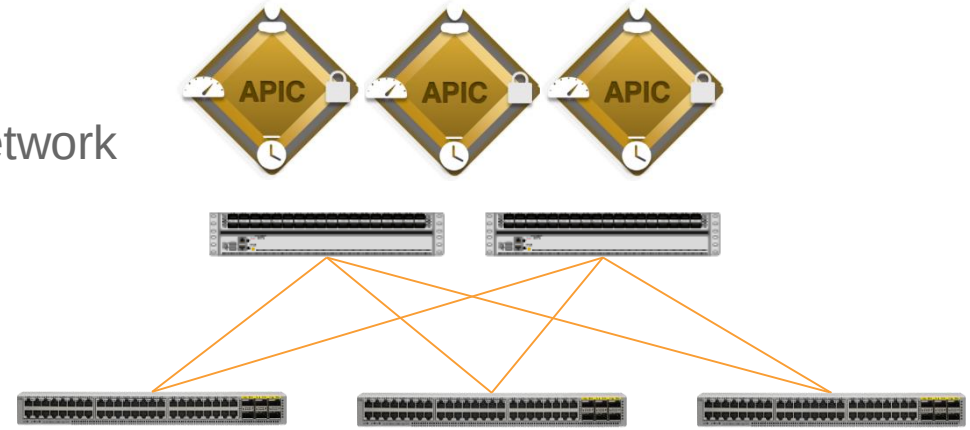
Cisco ASAP Reference Architecture Stack



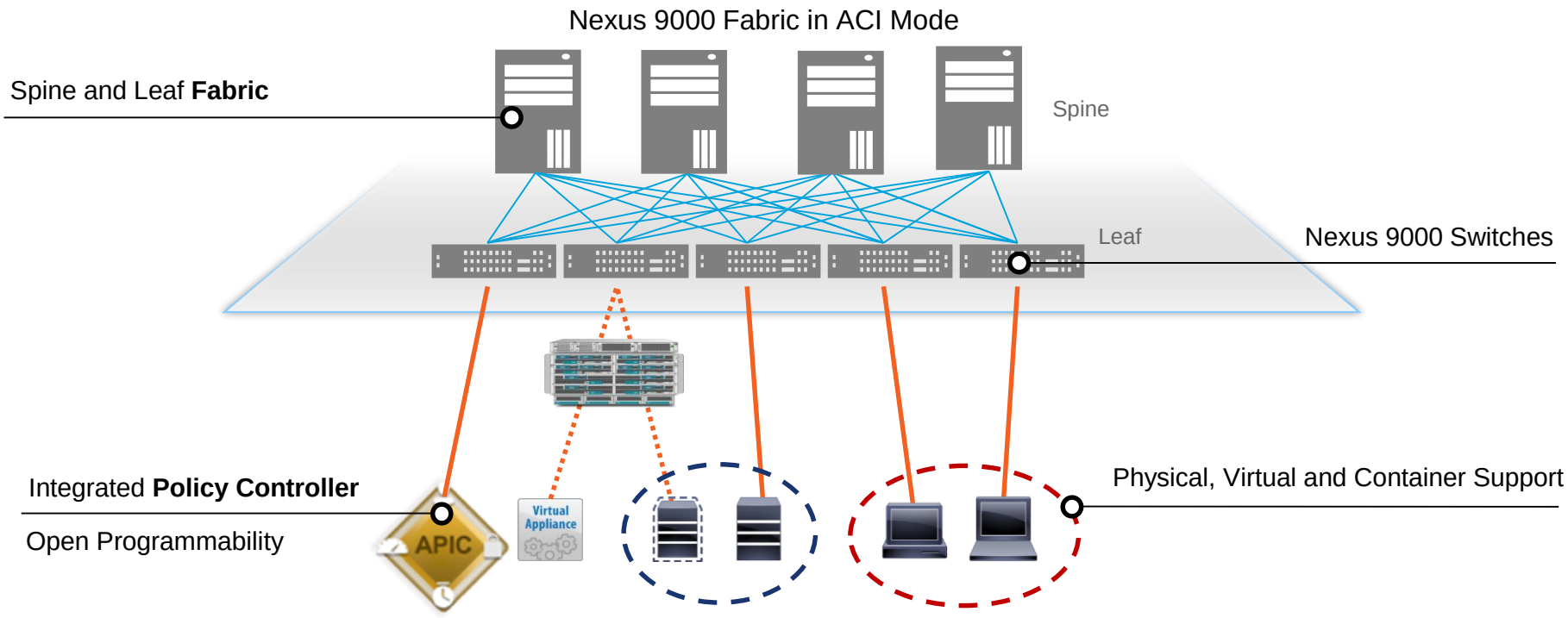
System Building Blocks

Application Centric Infrastructure

- Is a network fabric for datacenters.
  - Leaf/Spine Topology
- Uses VXLAN and Tunnel Endpoints as an underlay, this is completely automated
- All configuration is done from a controller and is pushed to the network switches

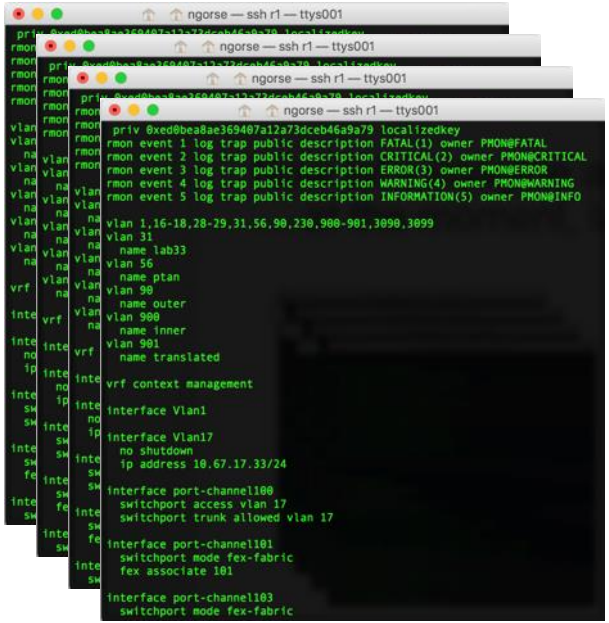


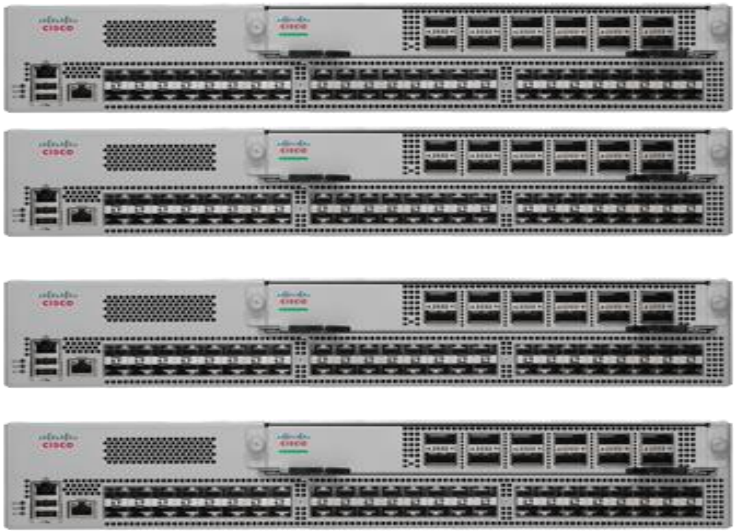
ACI Nomenclature



A Controller for the Network

Now let’s imagine a network switch …
… at the moment, largely configured on the CLI

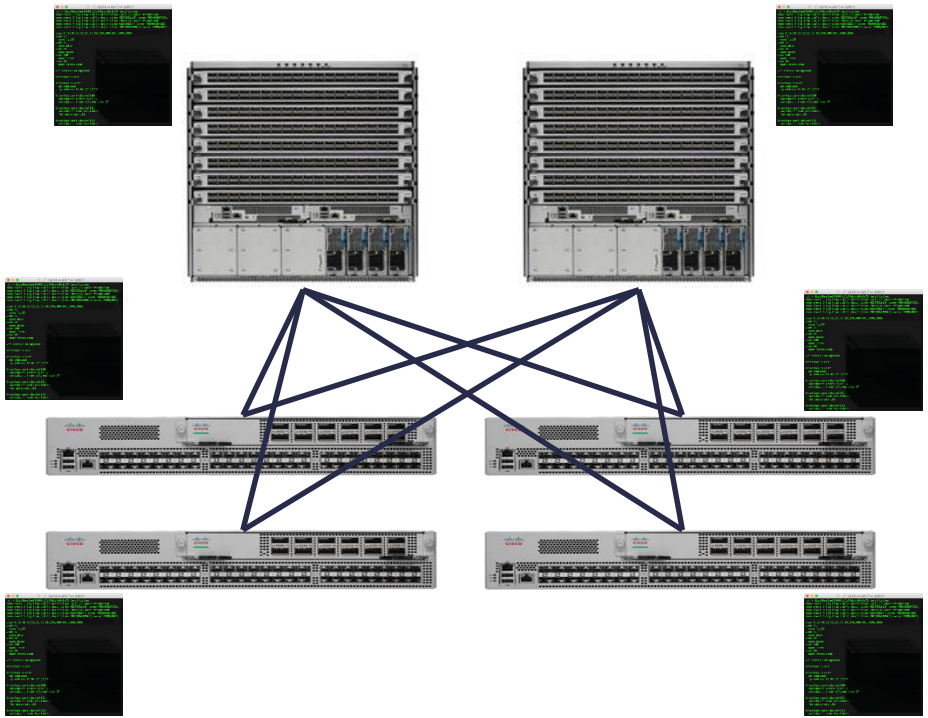




How Traditional Networks are Managed

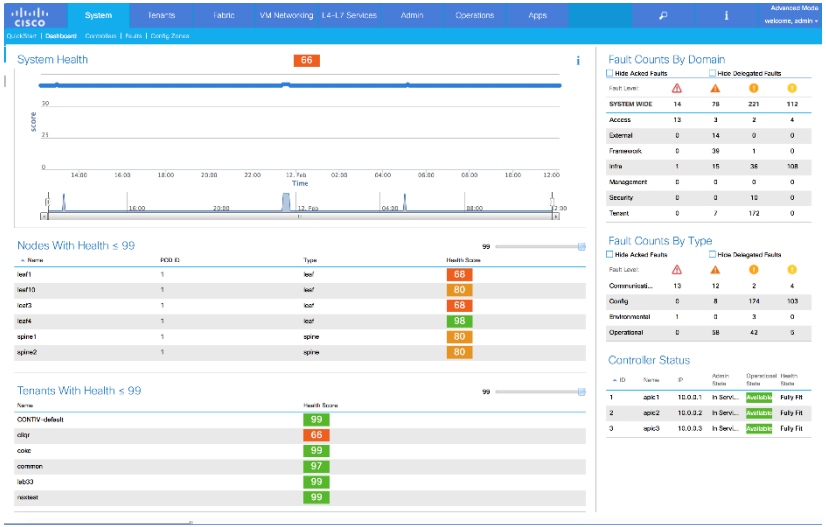
All nodes are managed and operated independently, and the actual topology dictates a lot of configuration

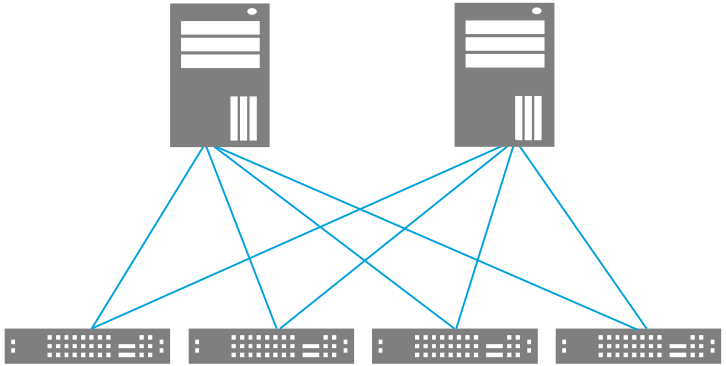
- Device basics: AAA, syslog, SNMP, PoAP, hash seed, default routing protocol bandwidth …
- Interface and/or Interface Pairs: UDLD, BFD, MTU, interface route metric, channel hashing, Queuing, LACP, …
- Fabric and hardware specific design: HW Tables, TCAM, …
- Switch Pair/Group: HSRP/VRRP, VLANs, vPC, STP, HSRP sync with vPC, Routing peering, Routing Policies, …
- Application specific: ACL, PBR, static routes, QoS, ...



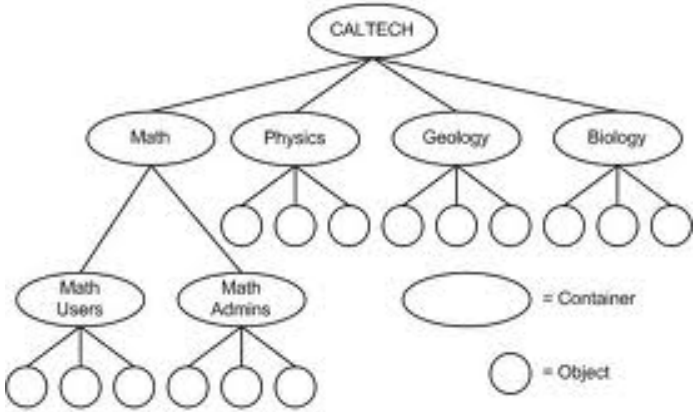
Cisco ACI solves the problem …

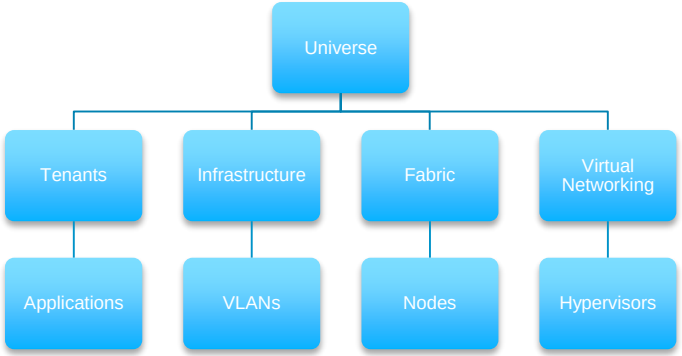
Interfaces, protocols, TCAM, etc … all represented in an object model, and ALL accessible through an Controller Cluster called Application Programmable Infrastructure Controller (APIC)





APIC Object Model is a Database





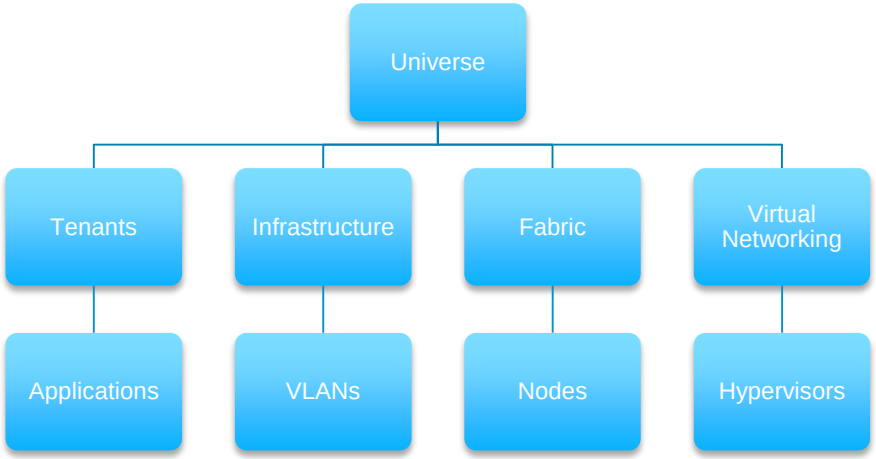
Common Operational Properties - AD, LDAP, …

System Management, Change Management, System Integrity, Correlation

APIC Object Model

Contains a modeled representation of everything

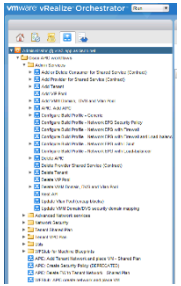
- Network constructs
- Application constructs
- Management constructs
- Services constructs
- Virtualization constructs



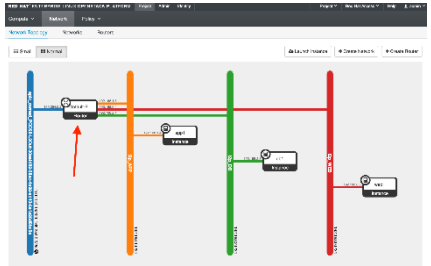
Manipulating objects changes configuration on the fabric

What Can Control the Controller

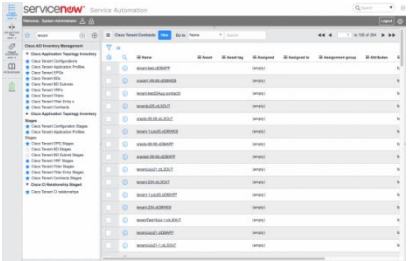
VShpere Client



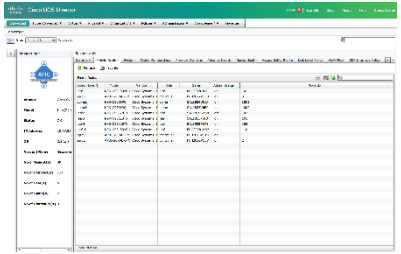
VRealise



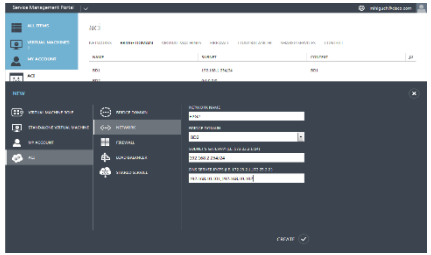
Openstack



ServiceNow

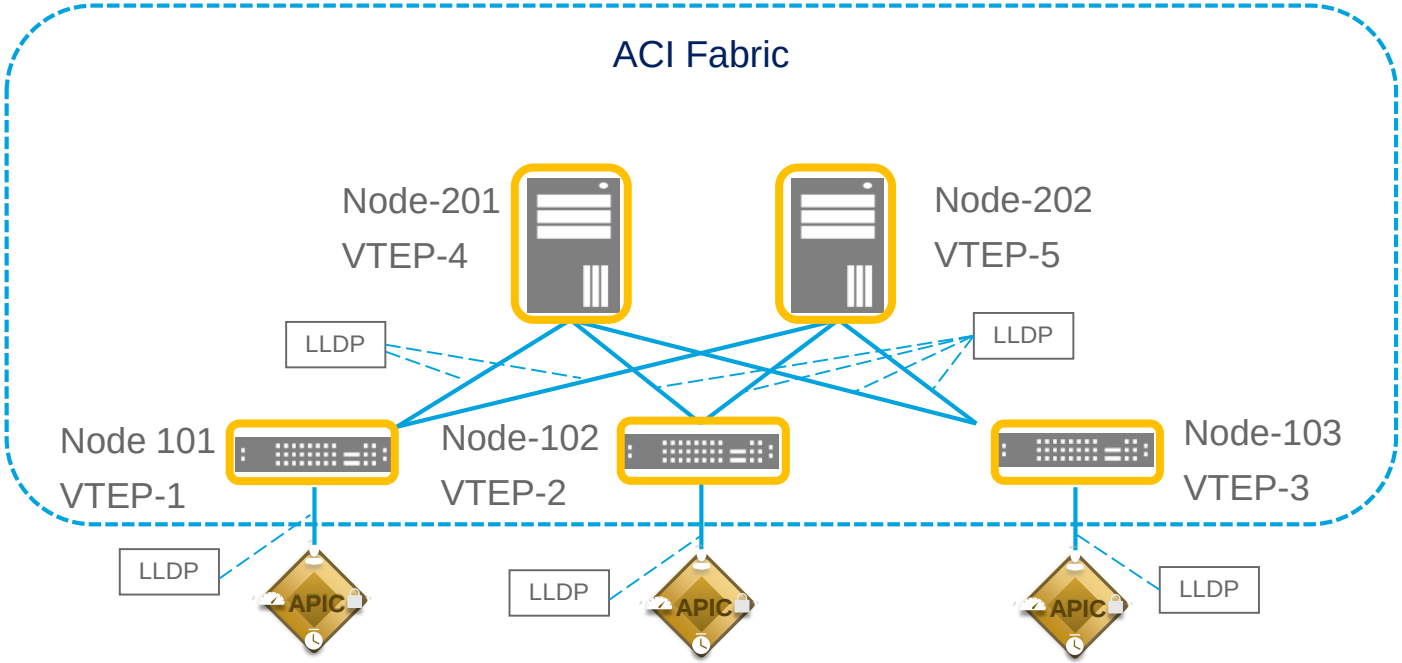


UCS Director



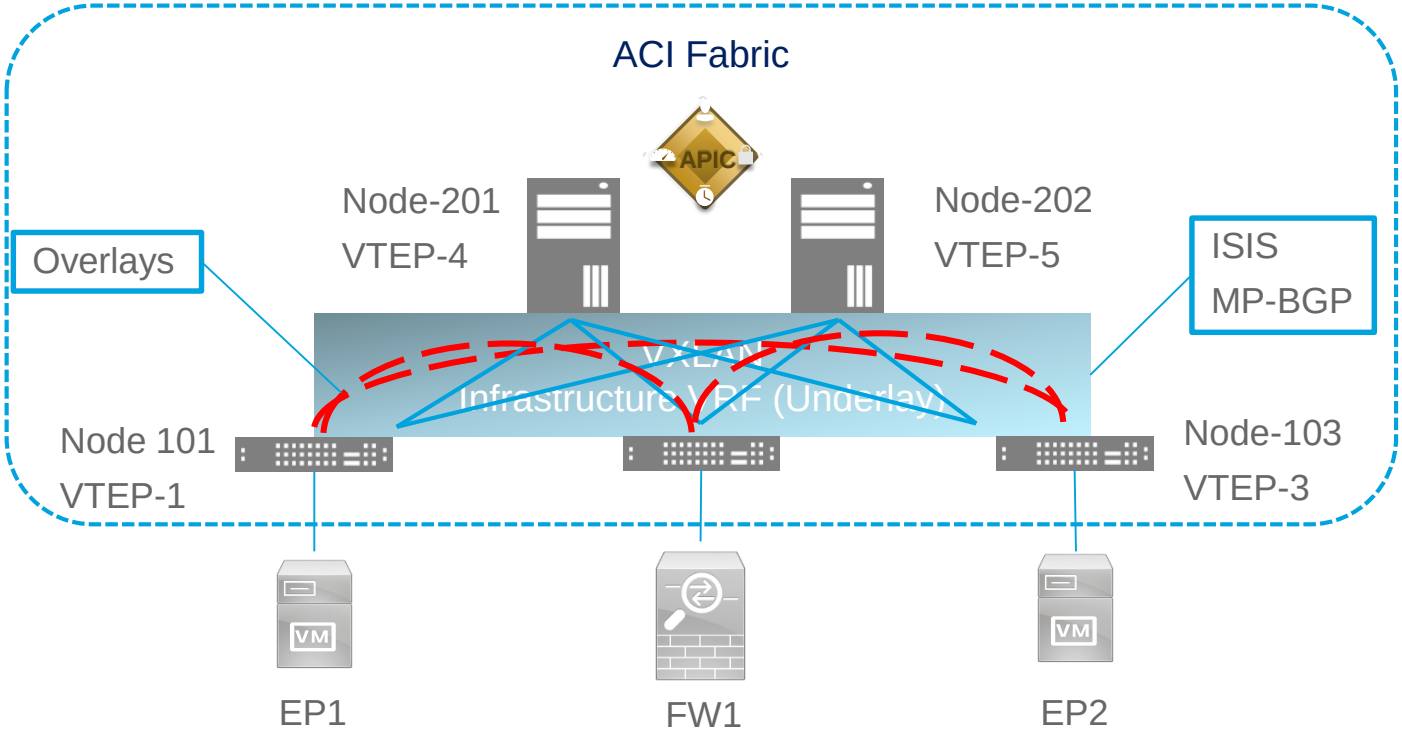
Windows Azure Pack

Booting the Network (Zero Touch Deployment)



How we connect things

How Endpoints Connect



Agenda

- Introduction
- System Building Blocks
- Forwarding Packets
- More Than Switching
- Wrap Up

Forwarding Packets

Host Routing - Inside

Inline Hardware Mapping DB - 1,000,000+ hosts

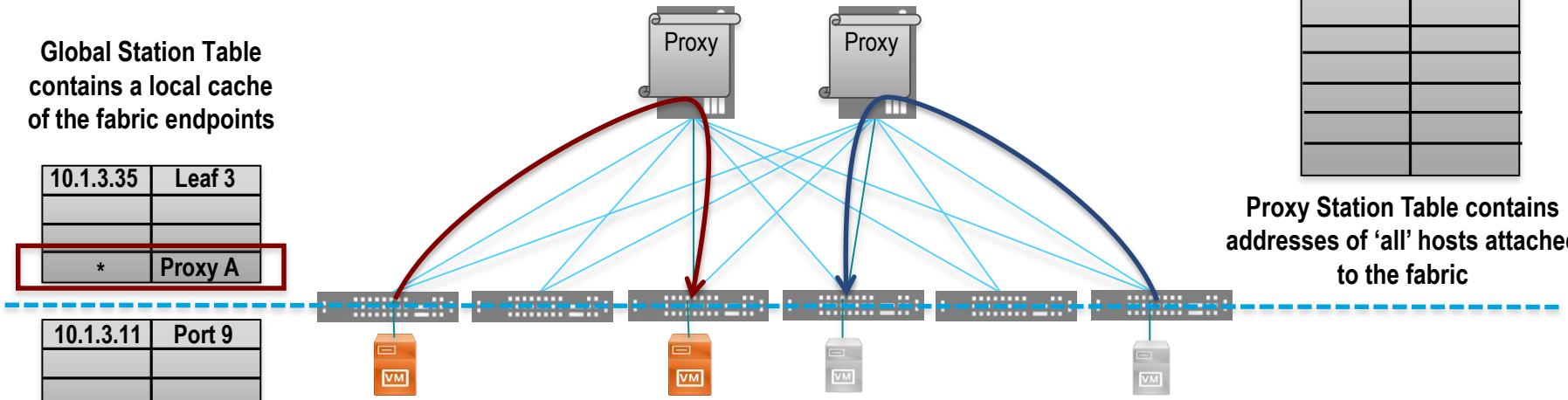
10.1.3.35	Leaf 3
10.1.3.11	Leaf 1
fe80::8e5e	Leaf 4
fe80::5b1a	Leaf 6

Proxy Station Table contains addresses of 'all' hosts attached to the fabric

Global Station Table contains a local cache of the fabric endpoints

10.1.3.35	Leaf 3
*	Proxy A

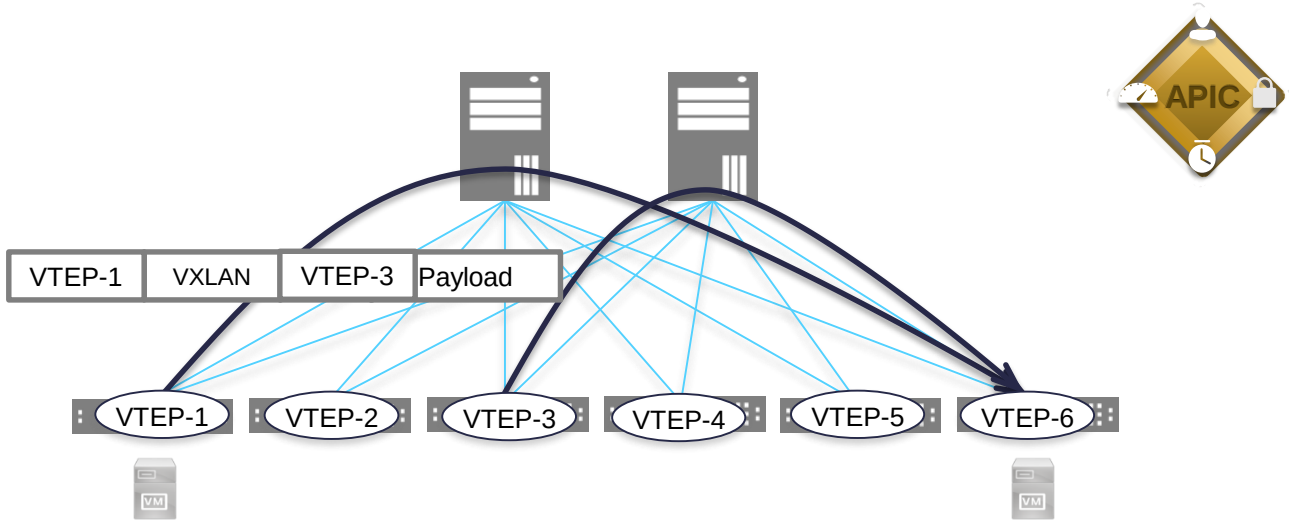
10.1.3.11	Port 9



Local Station Table contains addresses of 'all' hosts attached directly to the Leaf

ACI Fabric – Integrated Overlay

Decoupled Identity, Location & Policy

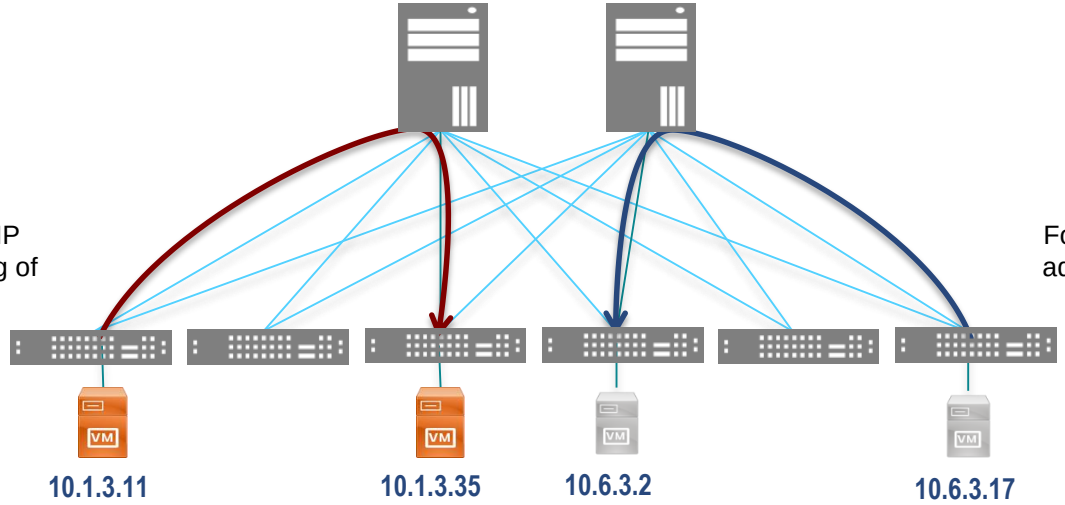


Location Independent Forwarding

Layer 2 and Layer 3

IP Forwarding:

Forwarded using DIP address, HW learning of IP address

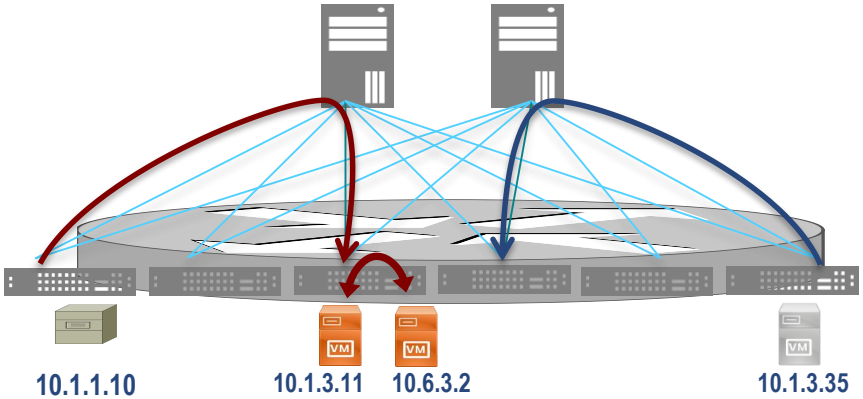


MAC Forwarding:

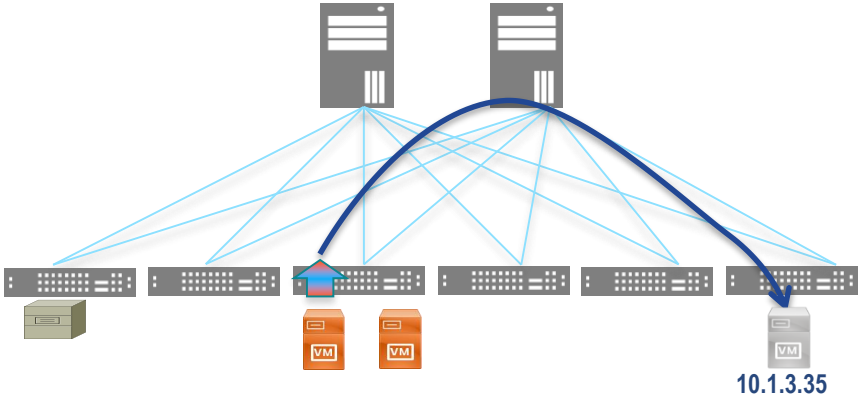
Forwarded using DMAC address, HW learning of MAC address

Location Independent Forwarding

Layer 2 and Layer 3



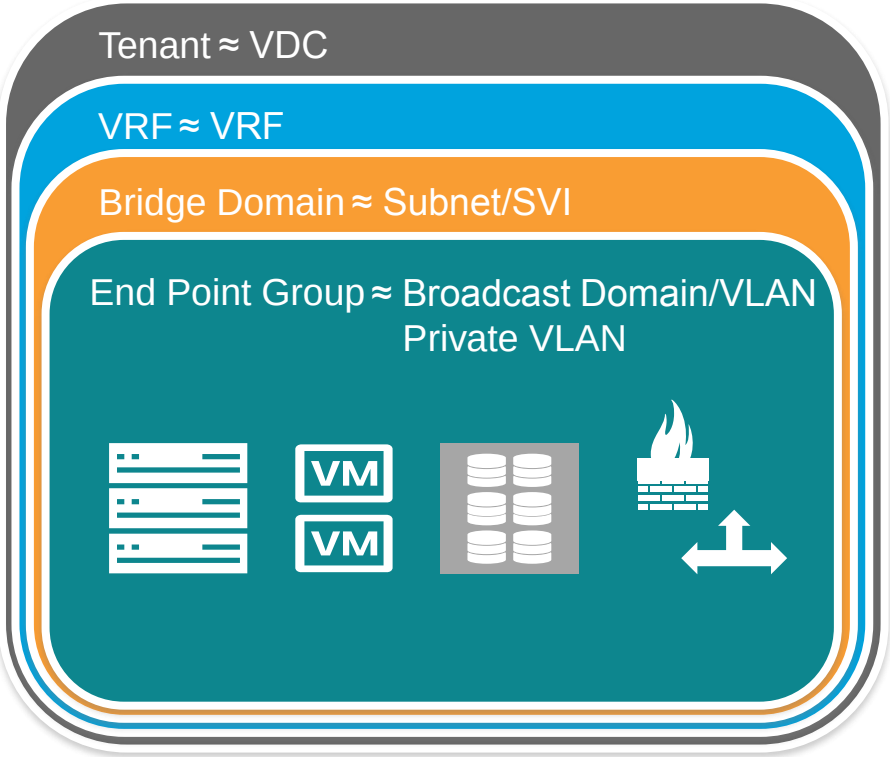
Distributed Default Gateway



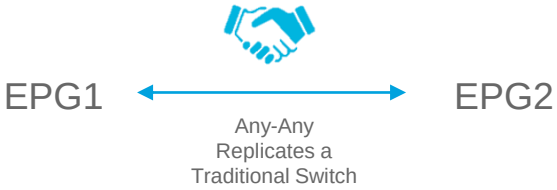
Directed ARP Forwarding

Logical Network Design

The Policy Model



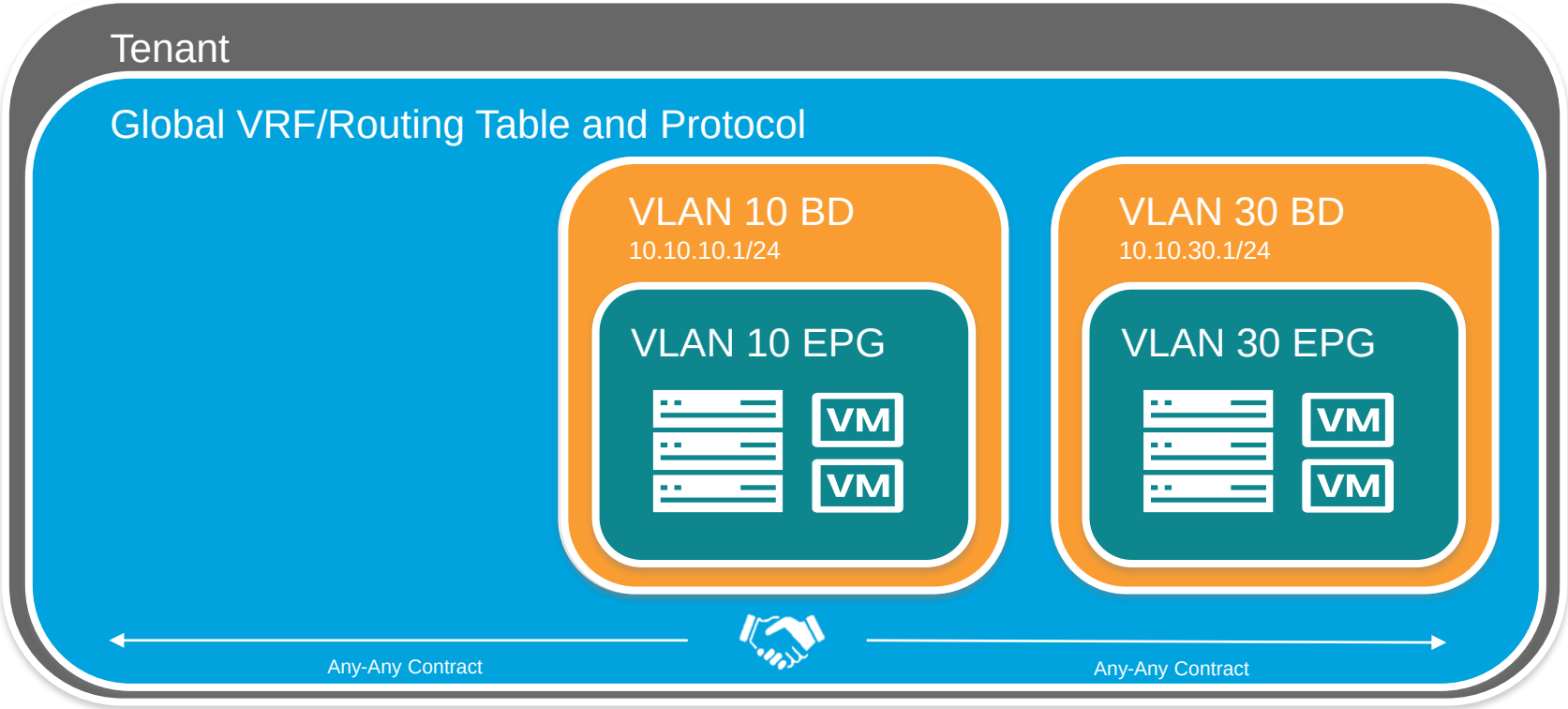
Contracts ≈ Access Lists



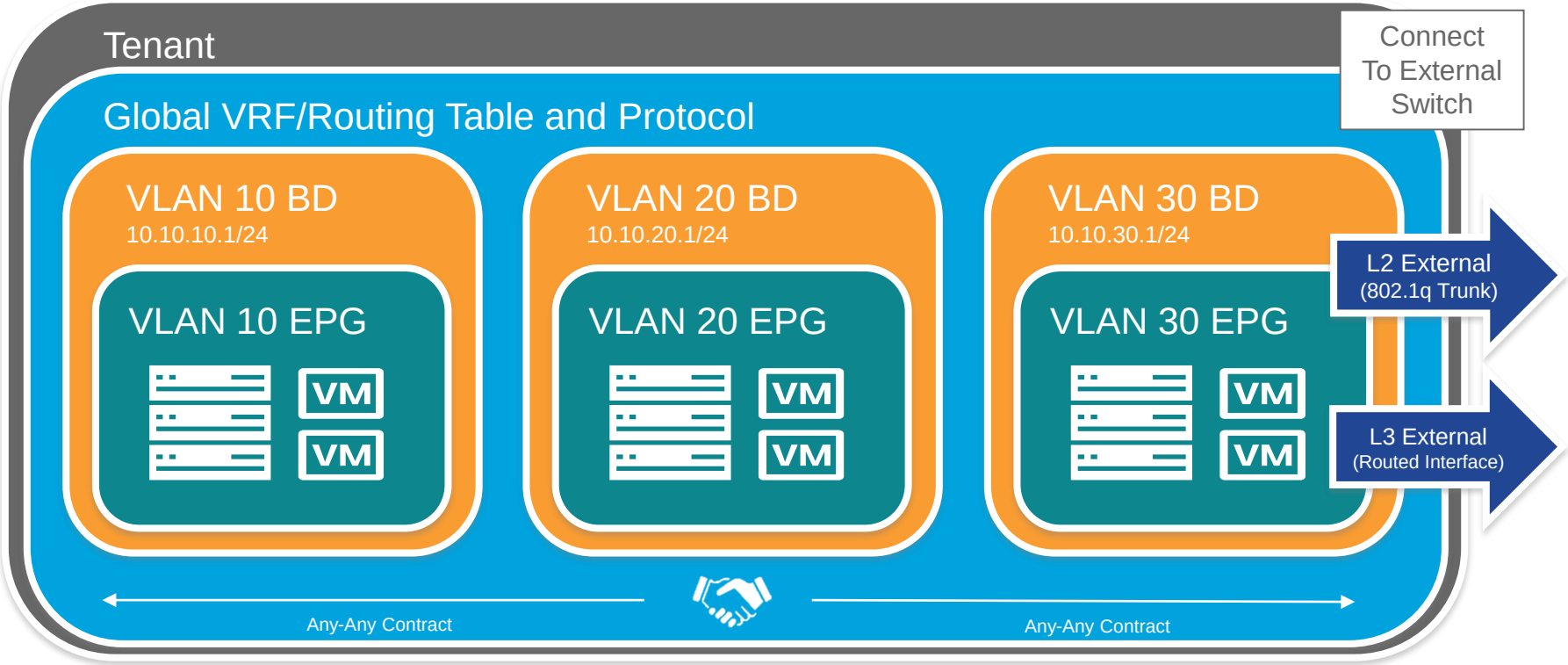
L2 External EPG ≈ 802.1q Trunk

L3 External EPG ≈ L3 Routed Link

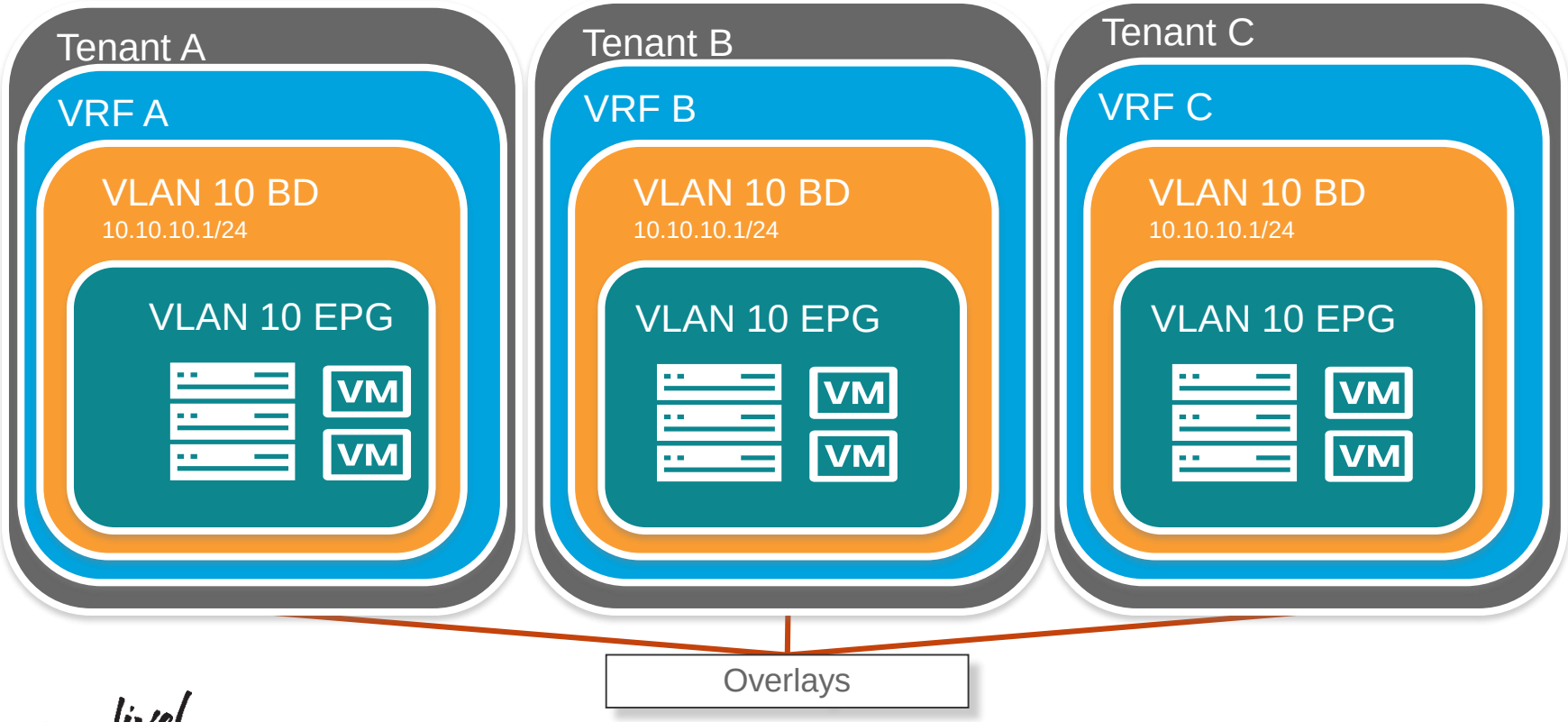
The Policy Model – Network Centric Configuration



The Policy Model – Network Centric Configuration

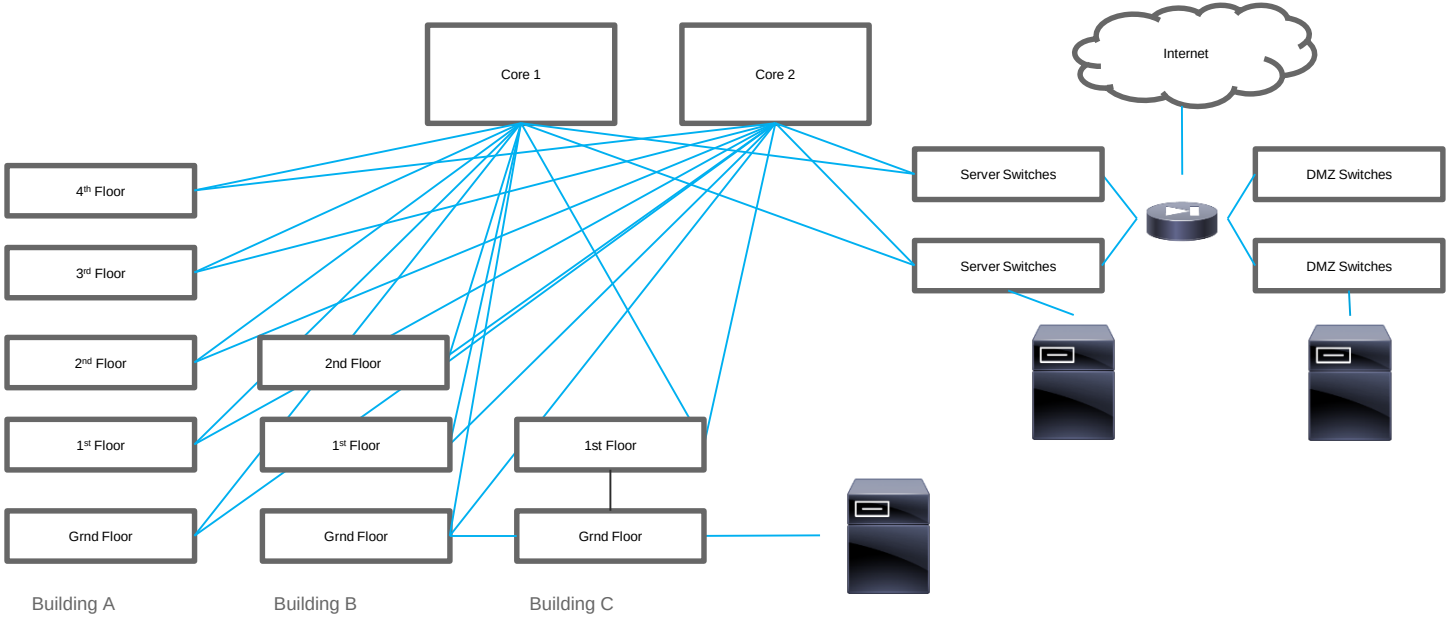


The Policy Model – Flexibility in Design

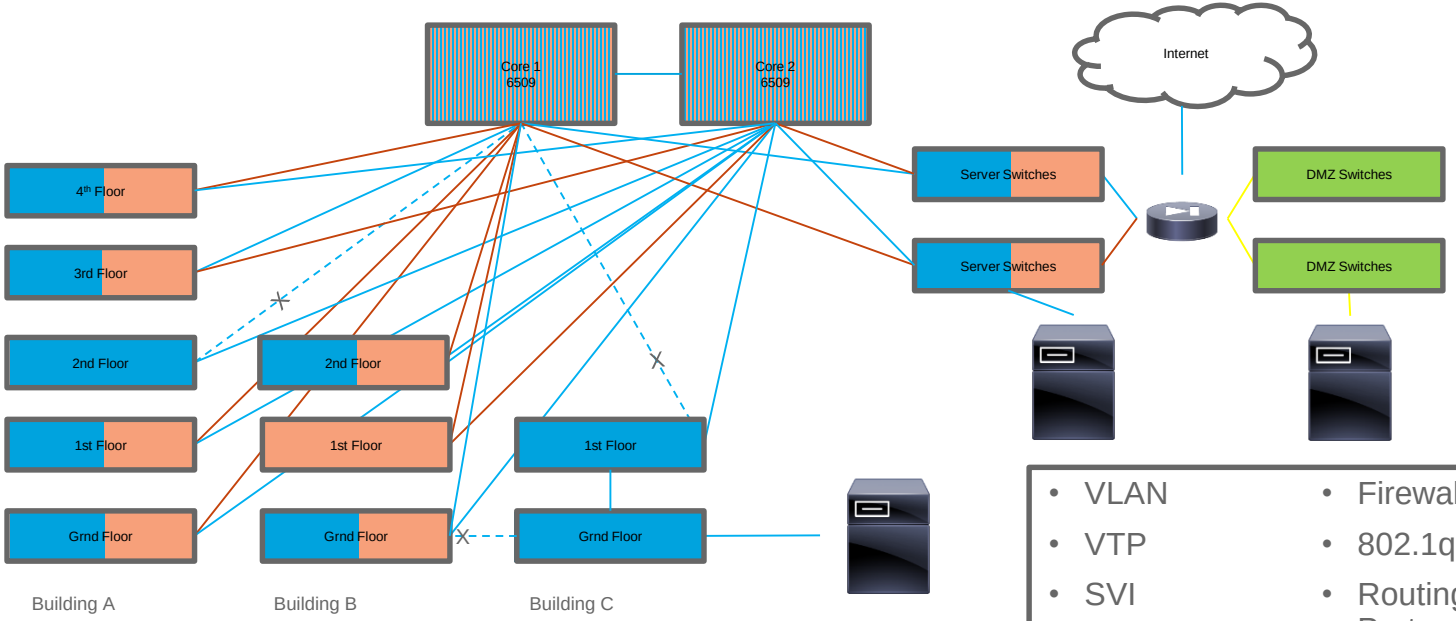


Example

Physical Network Design

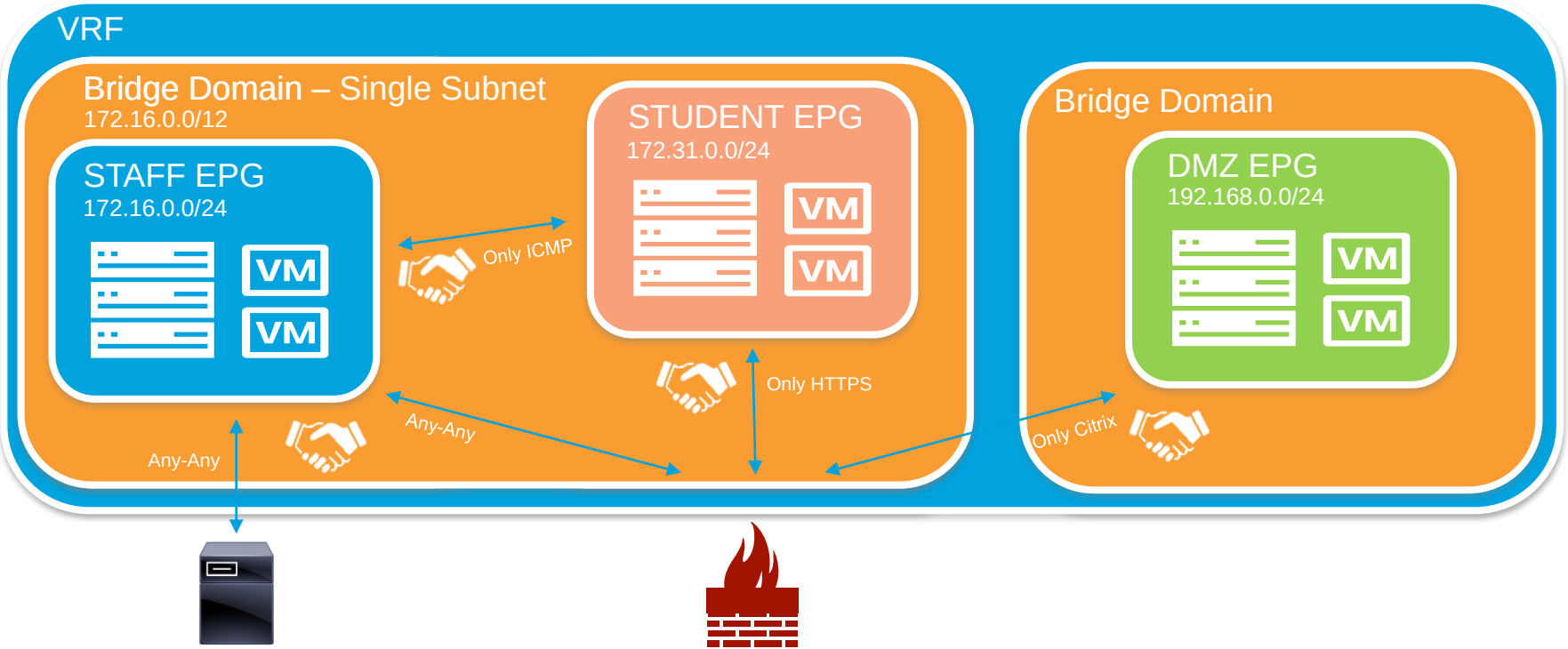


Logical Network Design



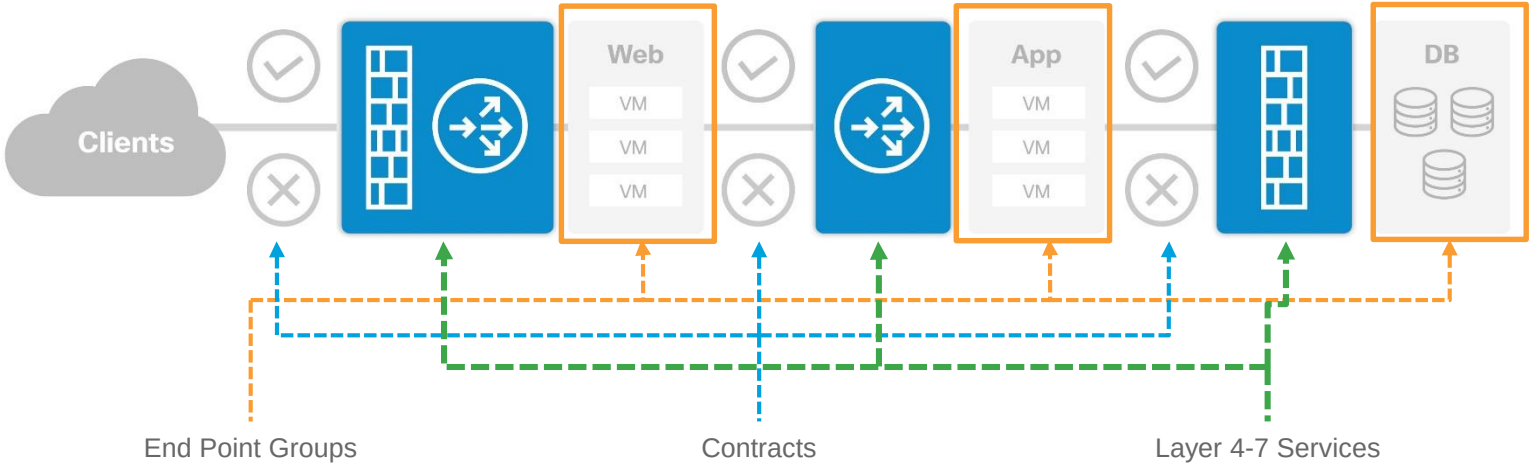
- VLAN
- VTP
- SVI
- Spanning Tree
- Firewall Rules
- 802.1q Trunks
- Routing Protocols
- Access Lists

The Policy Model – My First Network in ACI



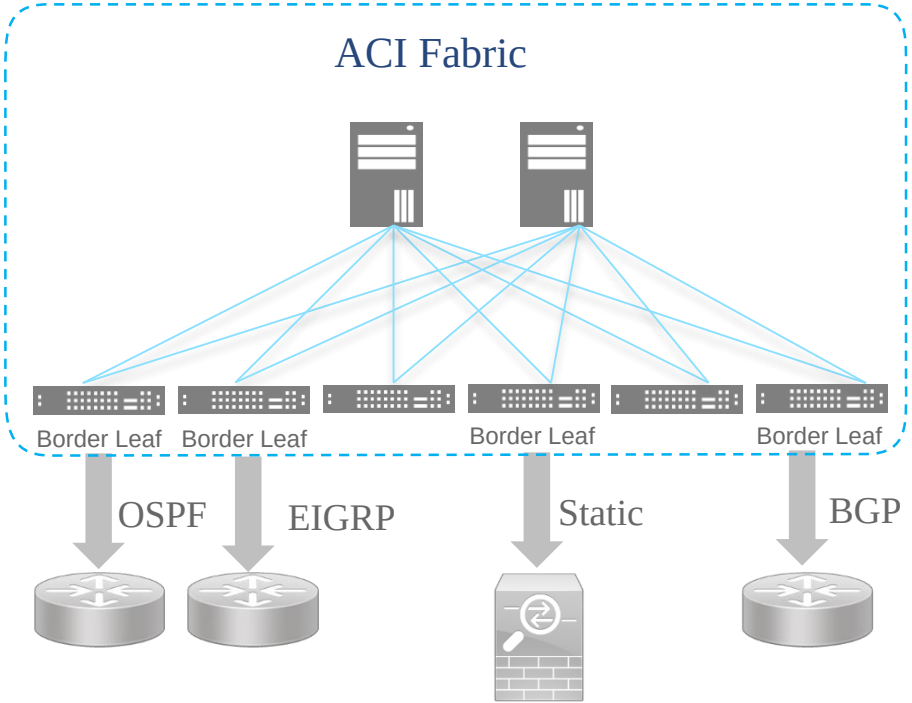
Sample Application Profiles

Student Management System

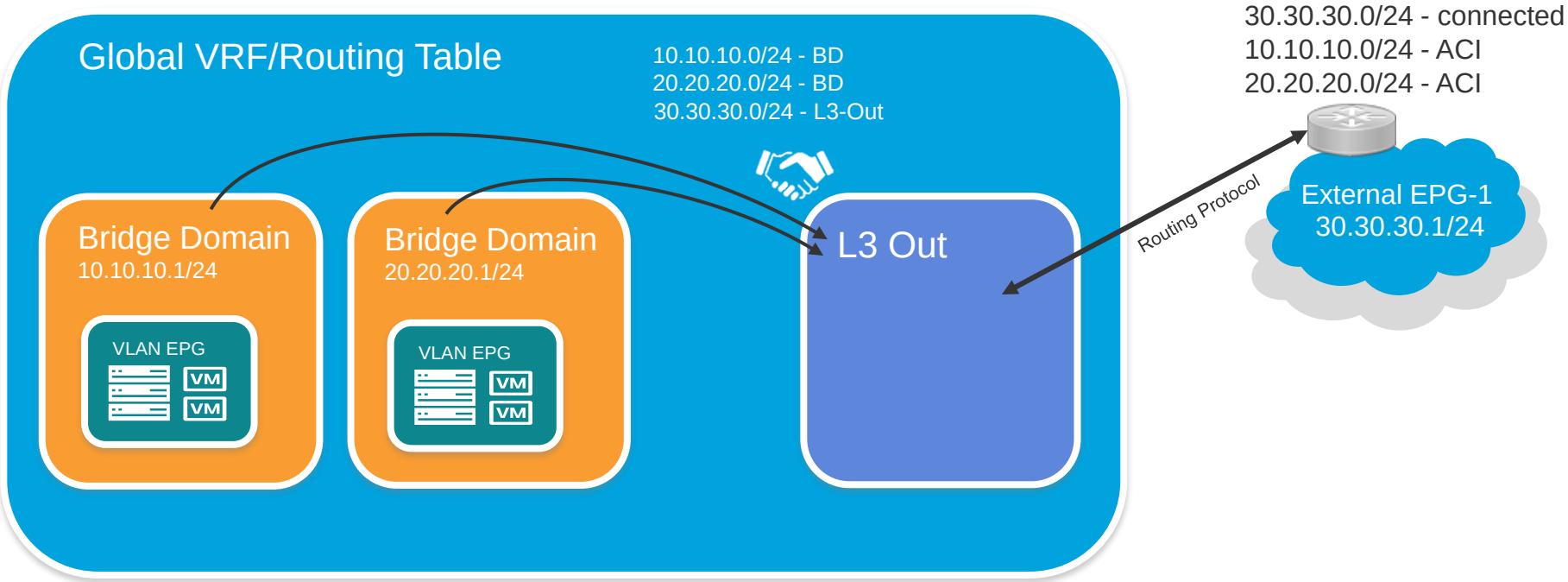


L2/L3 Out

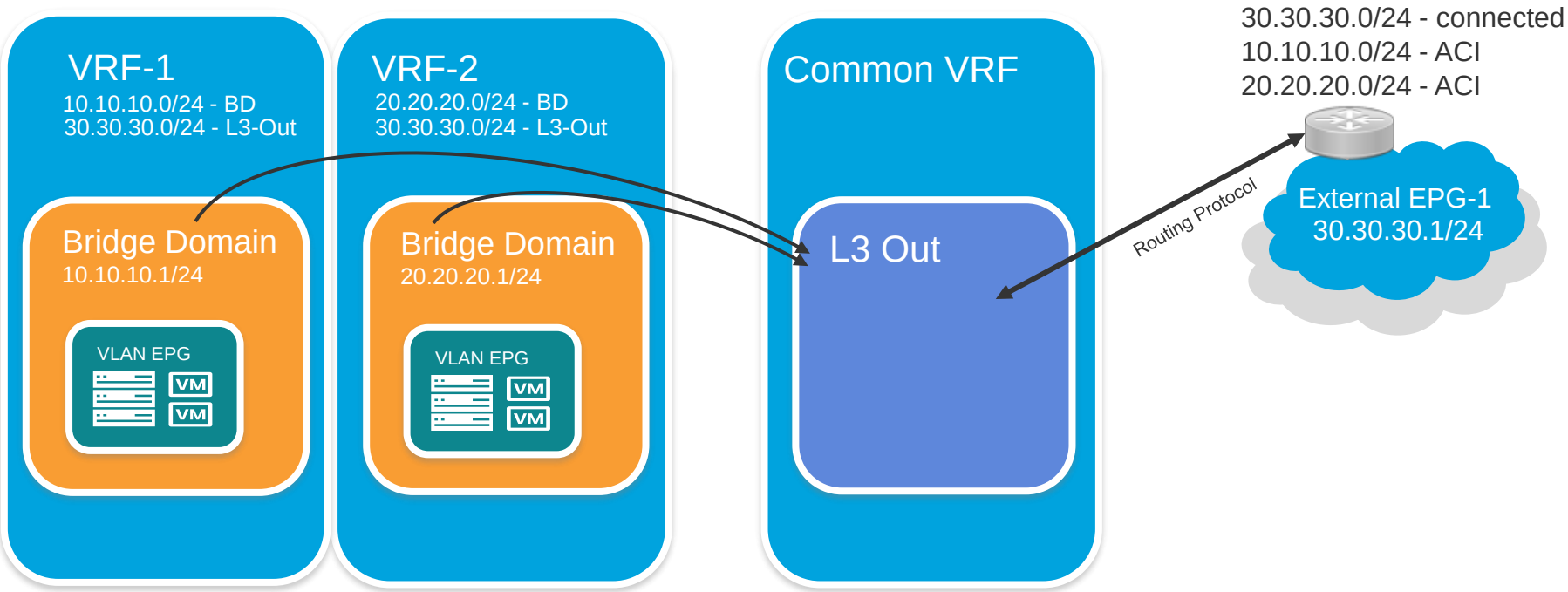
External Routing



Routing Process



Flexibility in Routing

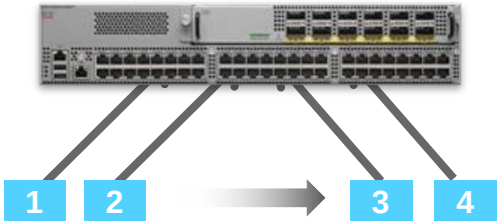


Segmentation

ACI Whitelist Policy supports “Zero Trust” Model

TRUST BASED ON LOCATION

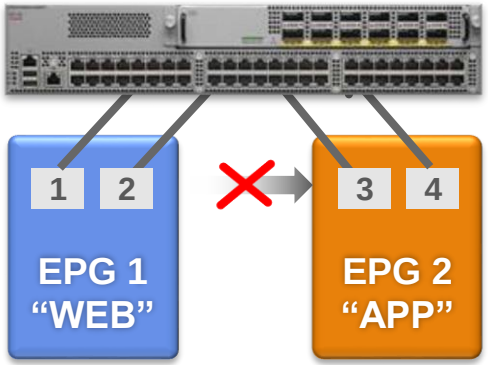
(Traditional DC Switch)



Servers 2 and 3 can communicate unless **blacklisted**

ZERO TRUST ARCHITECTURE

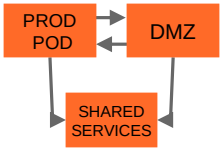
(Nexus 9K with ACI)



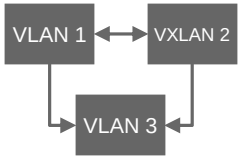
No communication allowed between Servers 2 and 3 unless there is a **whitelist** policy

ACI Delivers Hypervisor-Agnostic Microsegmentation

EPG Based

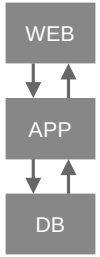


Basic DC Segmentation



Network-Centric Segmentation

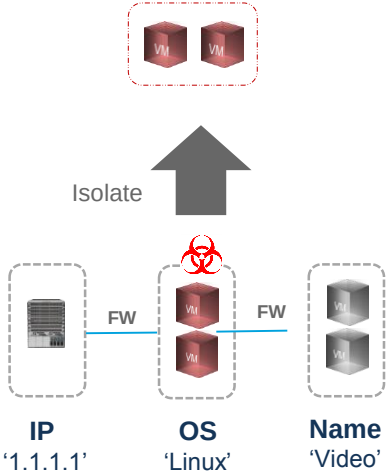
Application Lifecycle Segmentation



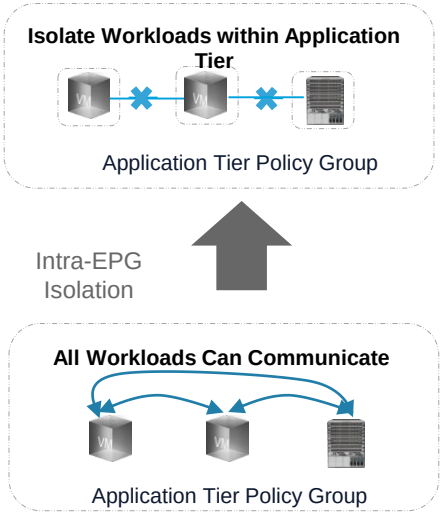
Service Level Segmentation

Attributes Based

Quarantine Compromised Workloads



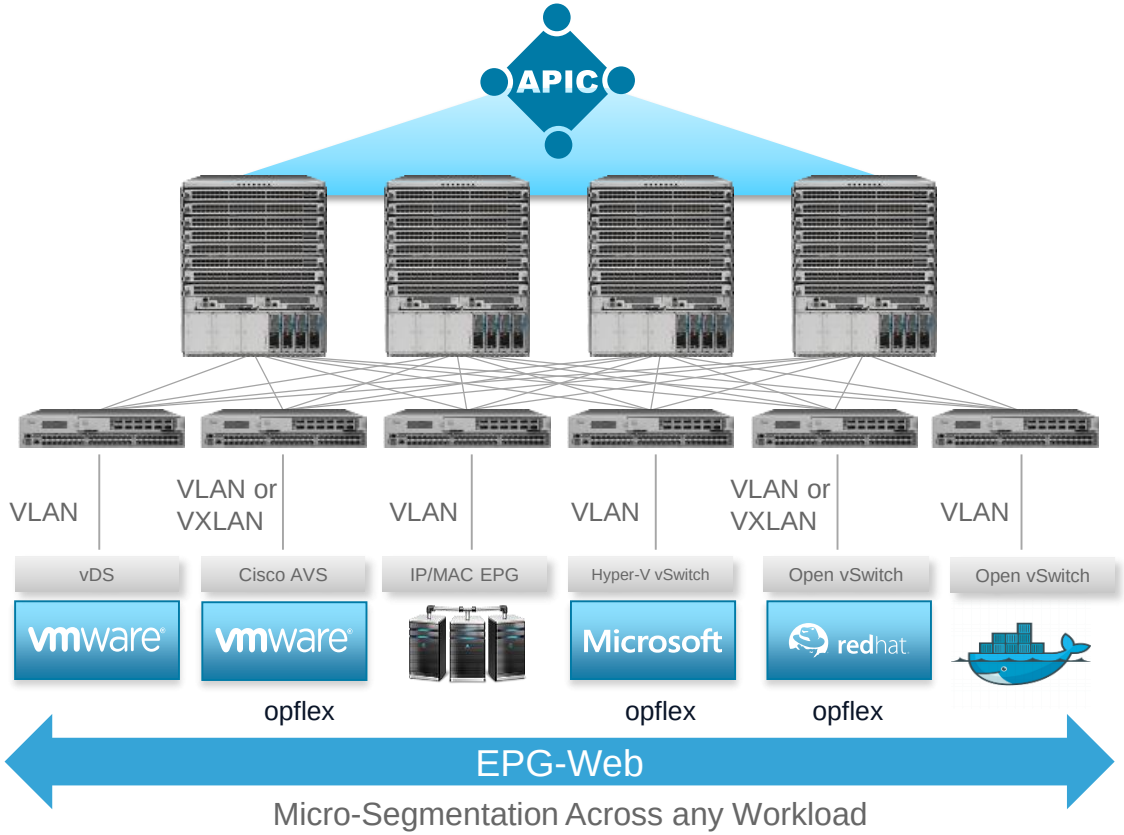
Intra-EPG Based



Micro-Segmentation with ACI

2 Capabilities:
1. Intra-EPG Isolation
2. Micro-Segmentation

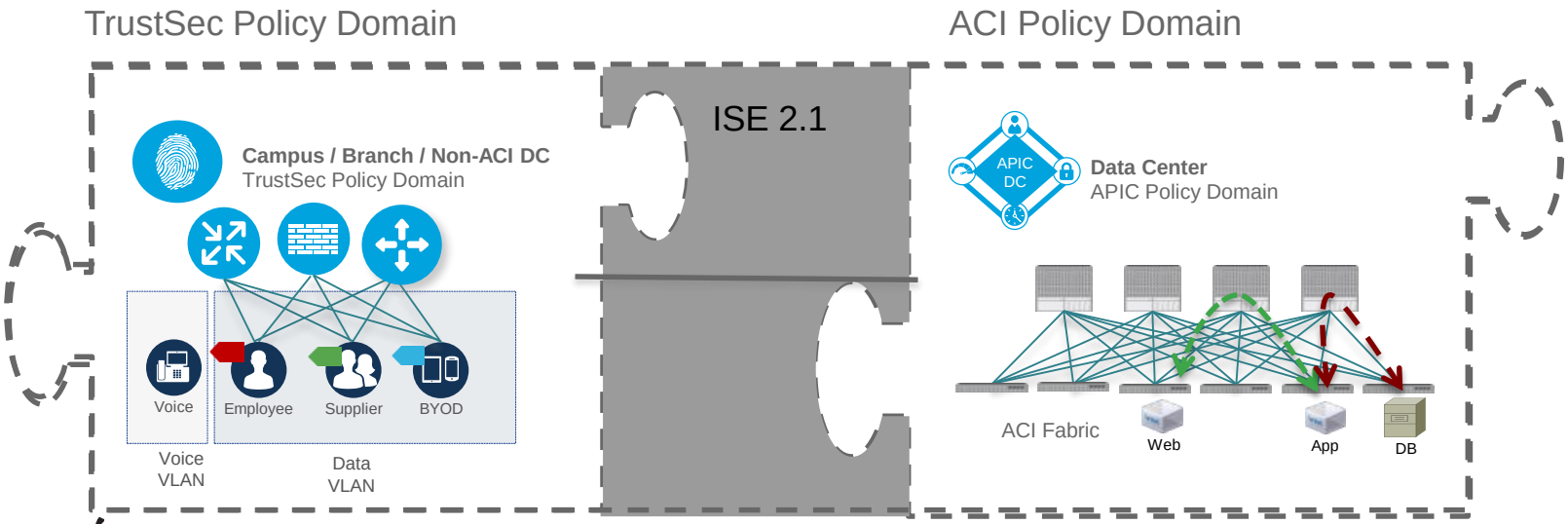
Attributes	Type
MAC Address Filter	Network
IP Address Filter	Network
VNic Dn (vNIC domain name)	VM
VM Identifier	VM
VM Name	VM
Hypervisor Identifier	VM
VMM Domain	VM
Datacenter	VM
Custom Attribute (VMWare AVS/vDS only)	VM
Operating System	VM



Security/Campus Network Integration

Enabling Group-Based Policies across the Enterprise

- Cohesive security policy
- Simplified security management
- End-to-End segmentation



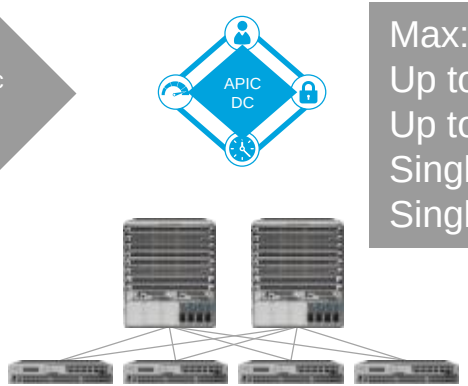
Delivering user/device/security context to ACI

TrustSec

Security Groups

ISE Dynamically provisions TrustSec Security Groups in ACI Fabric

ACI



Max: 250 Security Groups
Up to 4000/32 mappings (gen1)
Up to 10K/32 mappings (gen2) (-EX)
Single Tenant
Single L3Out

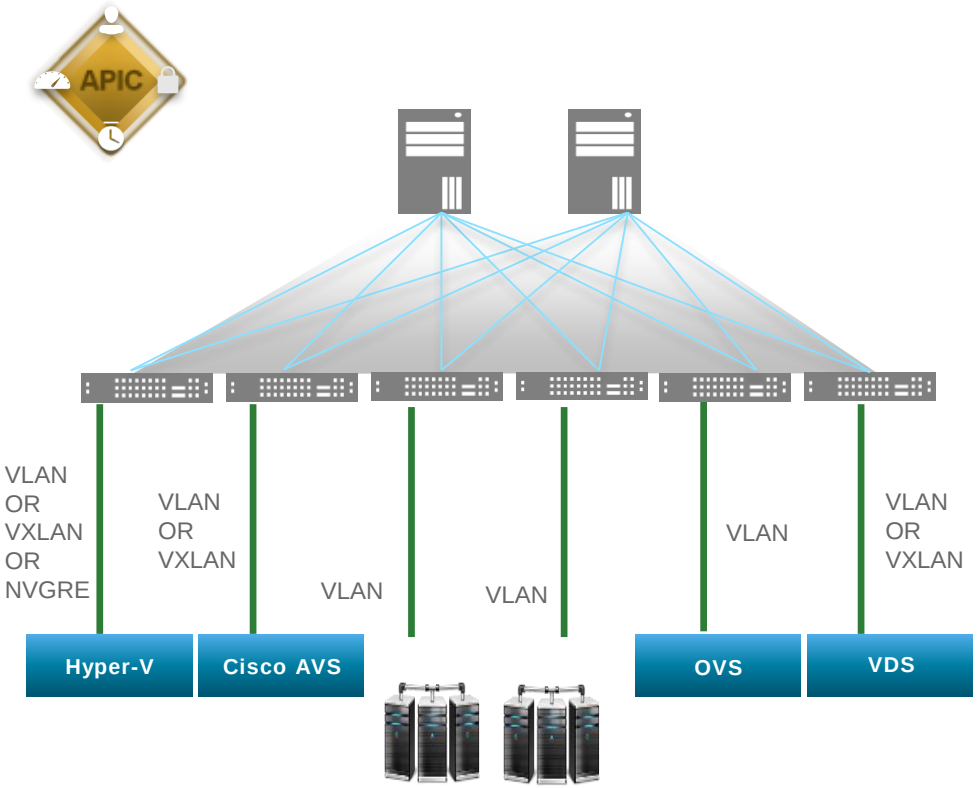
TrustSec Groups represented as External EPGs

Agenda

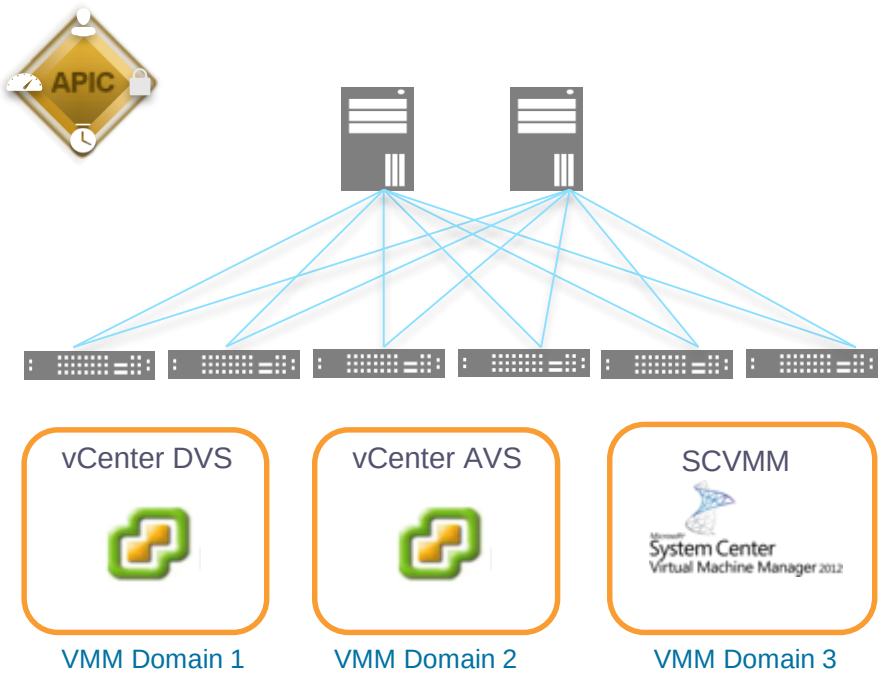
- Introduction
- System Building Blocks
- Forwarding Packets
- More Than Switching
- Wrap Up

Control of Hypervisor Networking

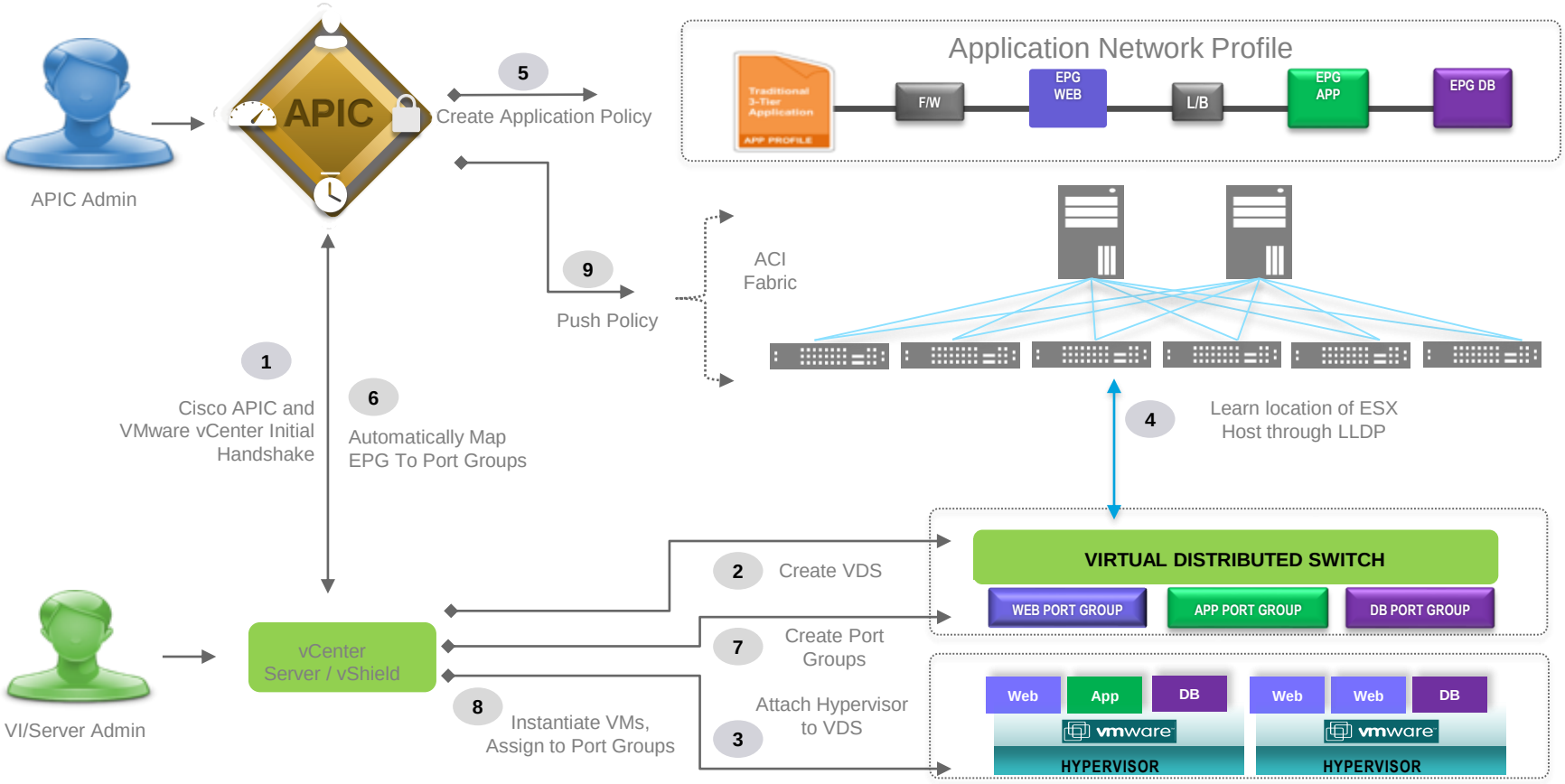
ACI – Any Application, Any Hypervisor



Hypervisor Integration with ACI

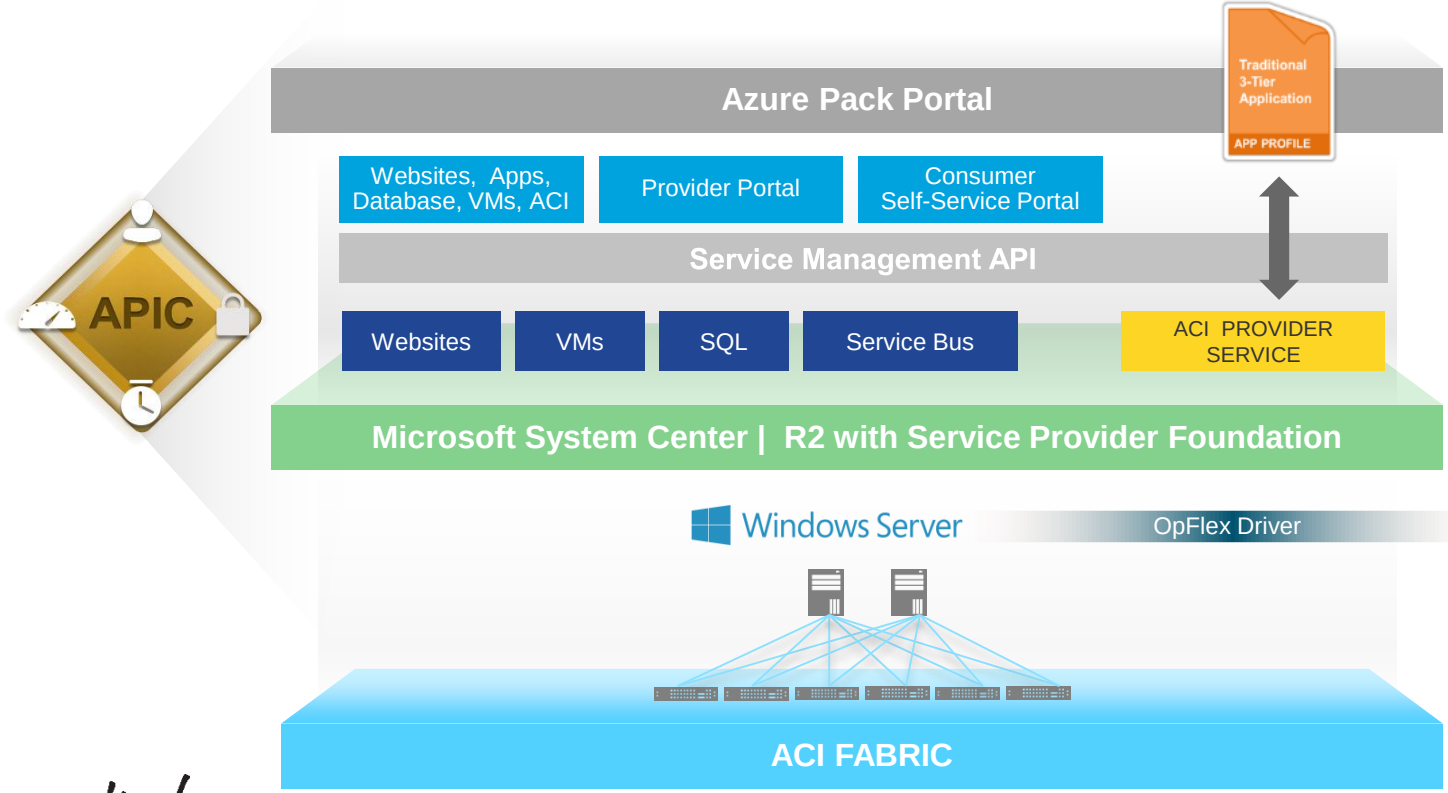


ACI Hypervisor Integration – VMware DVS/vShield



Cisco ACI – Microsoft Integration

Microsoft System Center/Azure Pack



Policy Management:
APIC / Azure Pack

VM Discovery:
OpFlex

Encapsulation:
VLAN,

Zero touch network provisioning

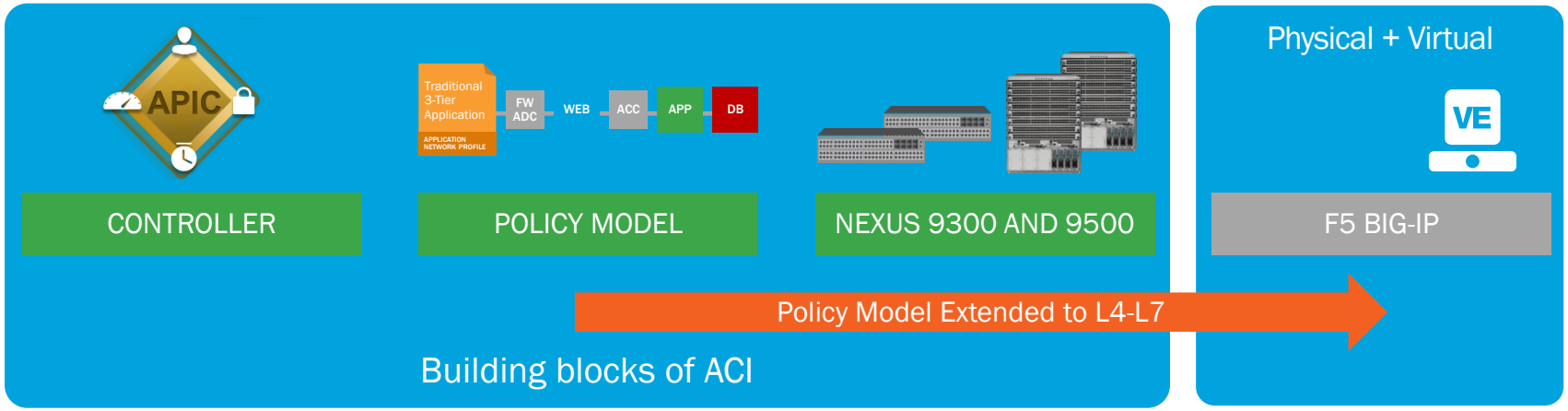
Service Insertion (Physical/Virtual)

Control of Layer 4/7 Services

Cisco ACI Service Insertion

Extending ACI Policy Model to L4-L7 Services

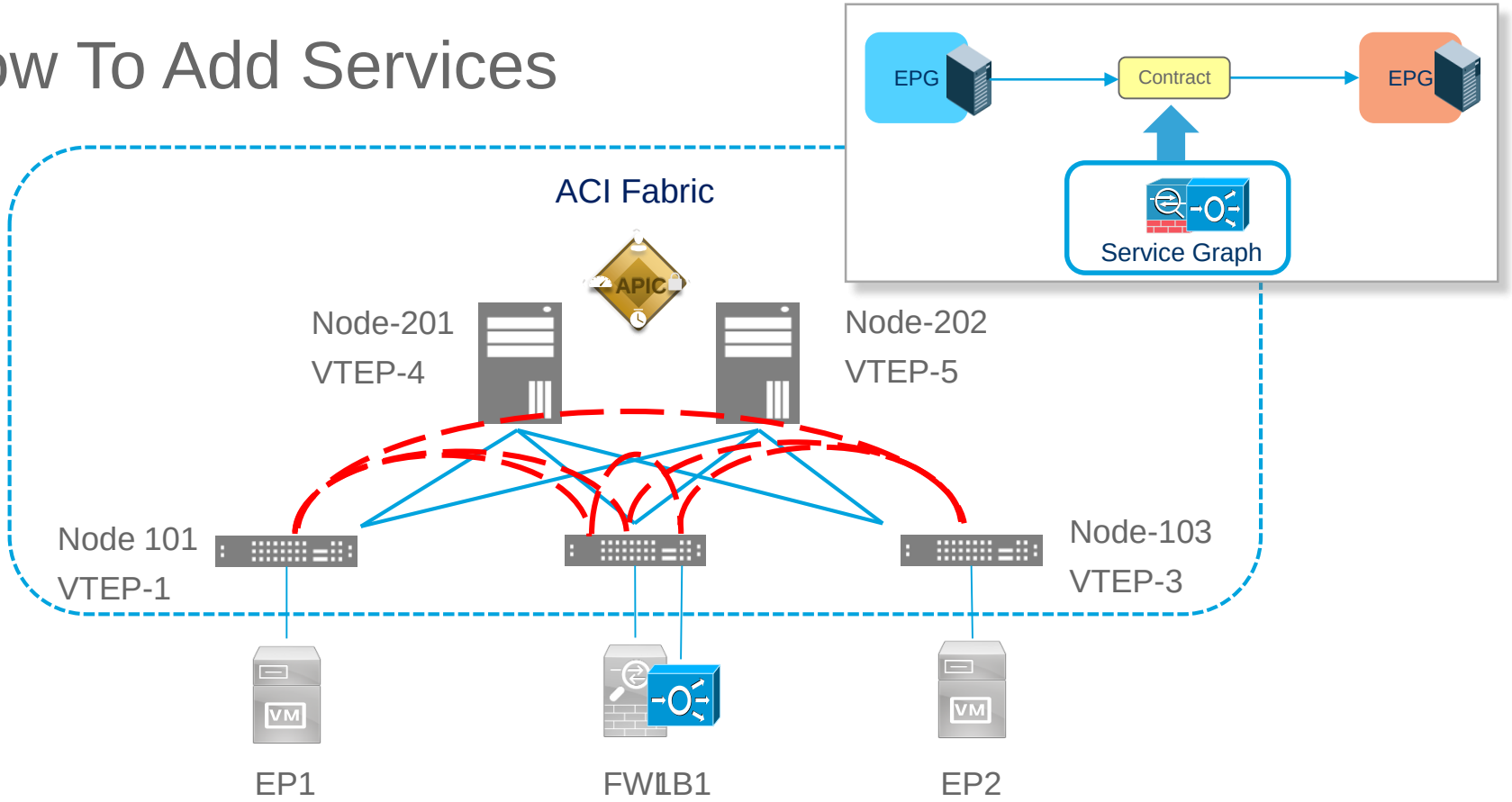
Application Centric Infrastructure Building Blocks



Application: 3 tier application (WEB-APP-DB) ➔ This may use ADC, FW services

Policy model: Define QOS, Security, Network, L4-L7 etc. to be applied to EPG

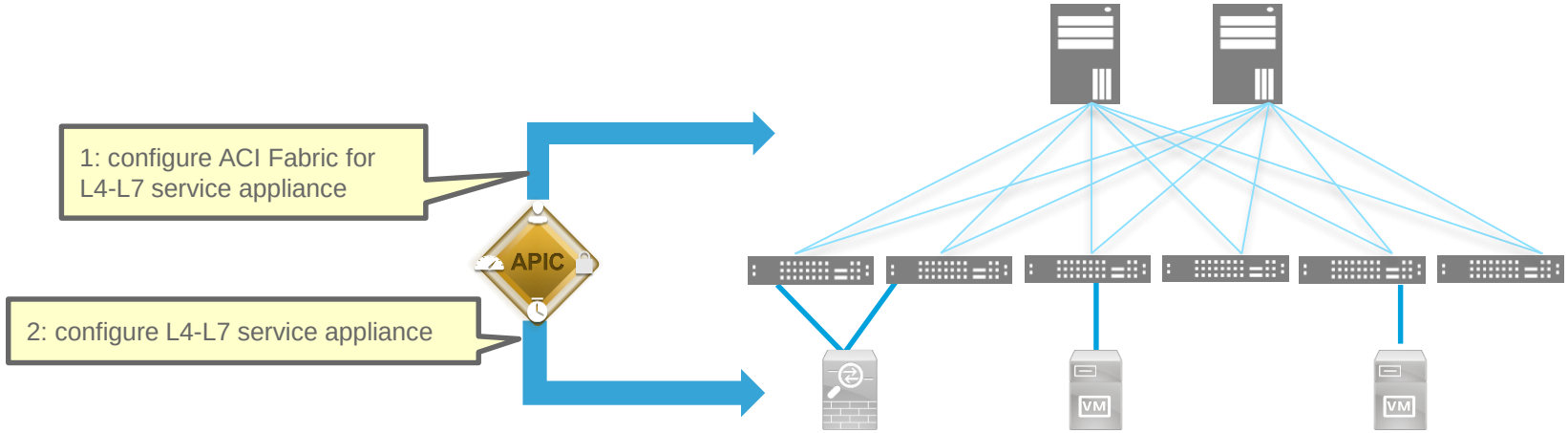
How To Add Services



Service Graph Overview

Service Graph feature enables us to insert one of more services between two EPGs.

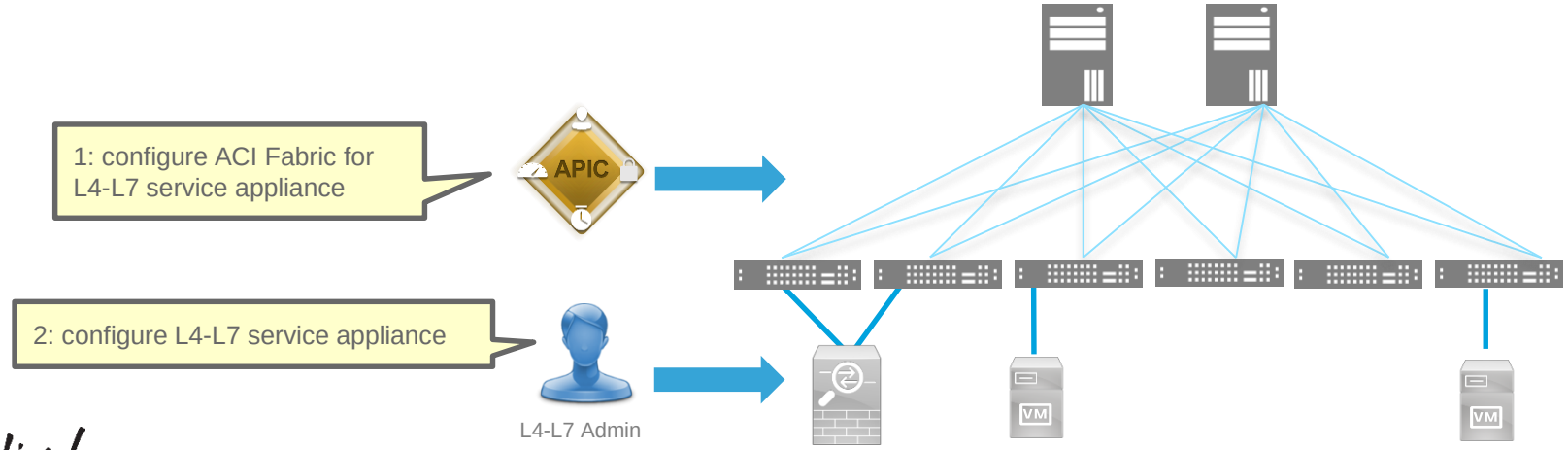
1. Network automation: Allocate the fabric resources(VLANs) for the service and program fabric
2. L4-L7 configuration automation: Configure L4-L7 service appliance.



Unmanaged mode

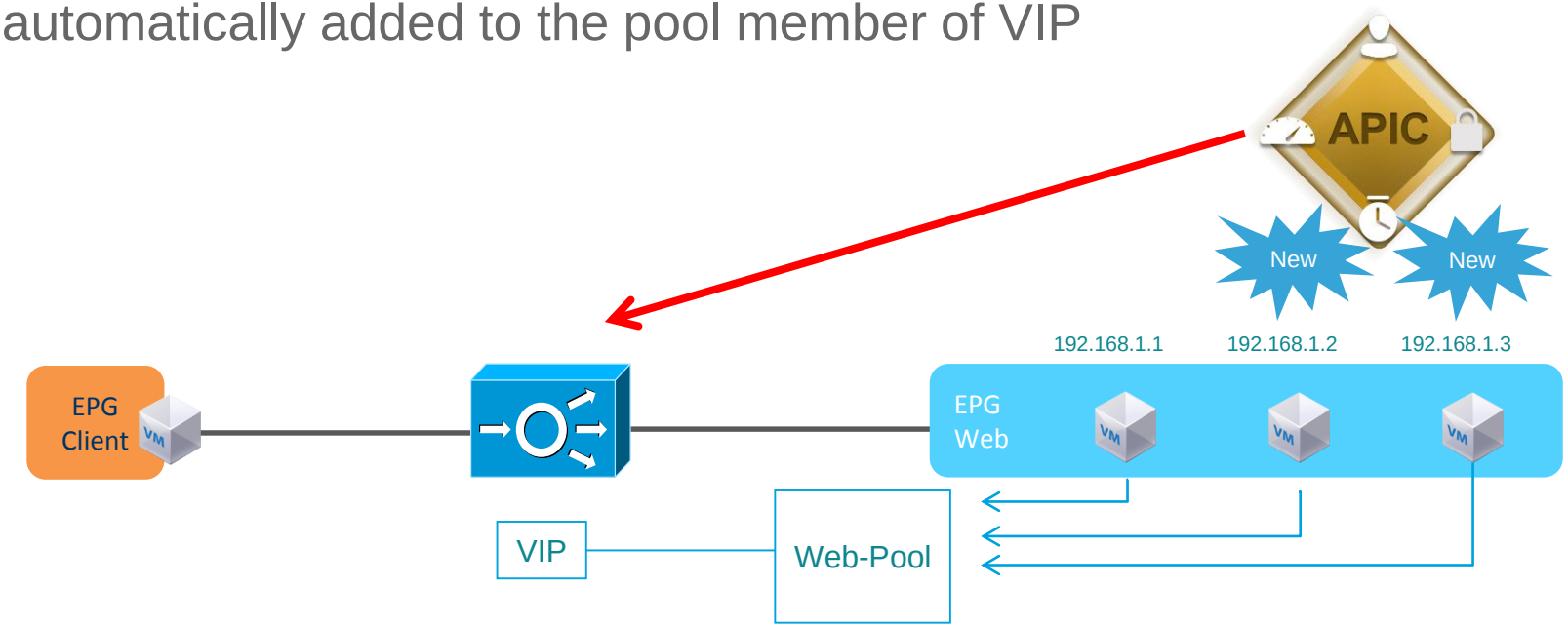
Network only switching feature adds the flexibility for customer to **use only network automation for service appliance.** The configuration of the L4-L7 device is left to be done by customer.

Customer can keep current L4-L7 device config administration.



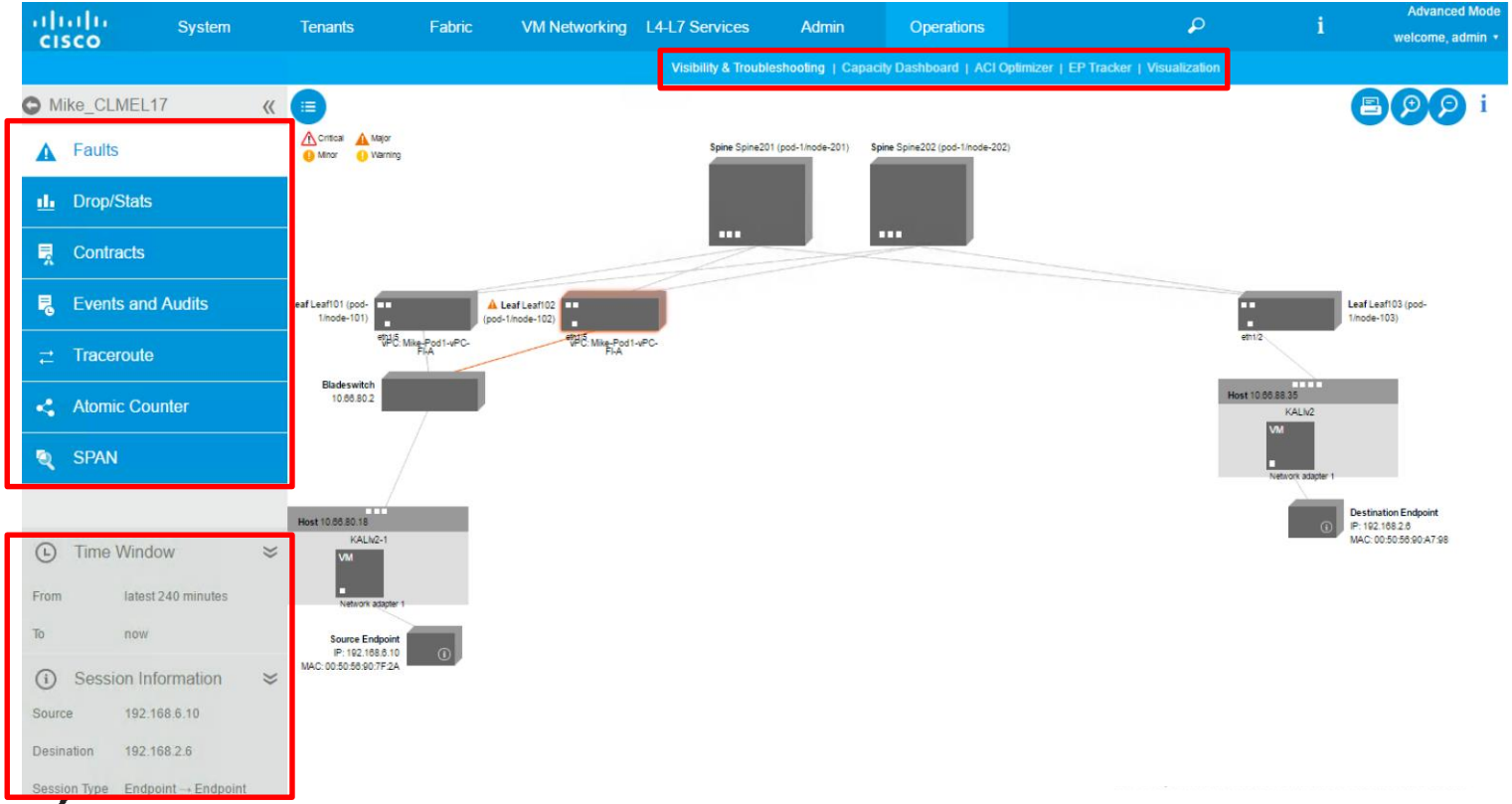
Dynamic Attach Endpoint

- APIC dynamically detect new endpoint, then the endpoint is automatically added to the pool member of VIP



Visibility and Automation

ACI - Troubleshooting and Operation Tools



Cisco ACI App Center

ACI Developers

Search for apps...

Introducing the Cisco App Center

Software Defined Networking (SDN) is enabling organizations to accelerate application deployment, dramatically reducing IT costs through policy-enabled workflow automation. Explore the Cisco App Center and select from a wide range of SDN applications that allow you better align your network with your business needs.

Browse apps

Featured Apps

Contract Viewer

Cisco

★★★★★

Download

InfobloxSync

Cisco

★★★★★

Download

ServiceNowCon...

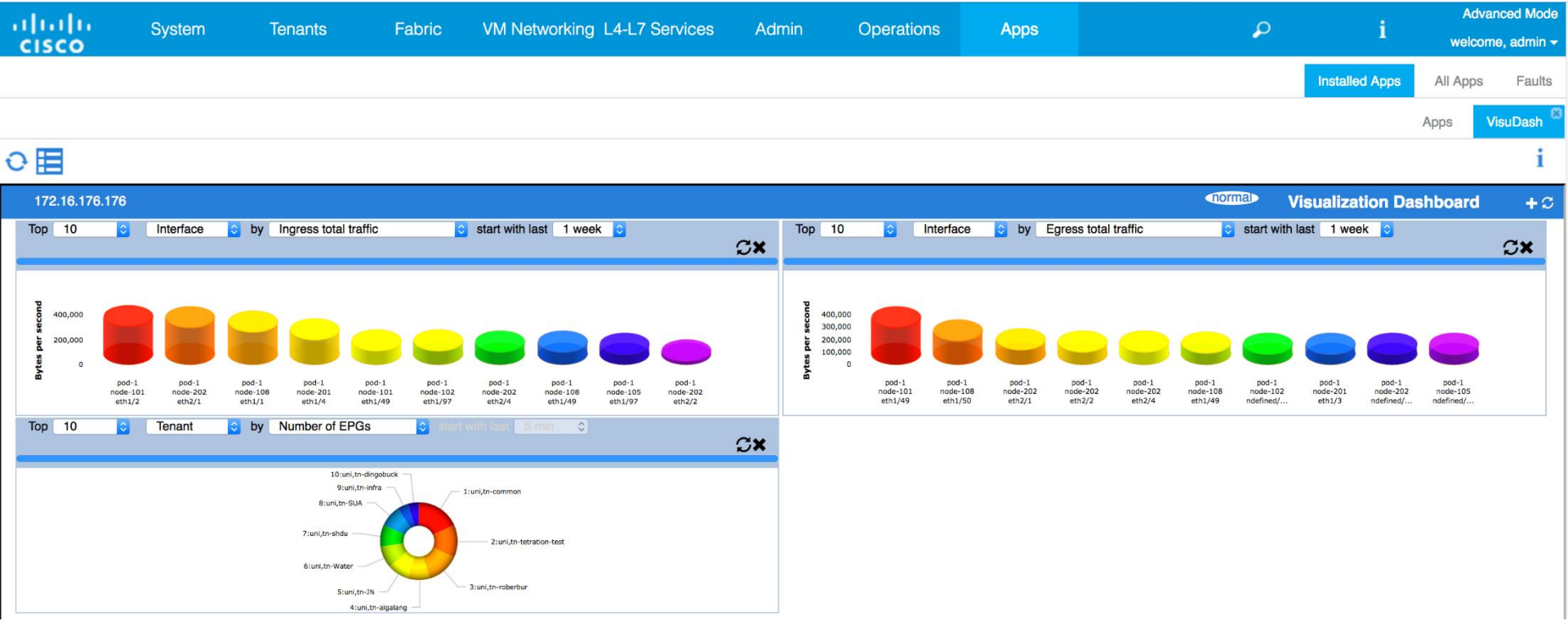
Cisco

★★★★★

Download

VisuDash

VisuDash



Contract Viewer

Wrap Up

What’s Change about my Networks with ACI

1. The physical network is decoupled from the logical design
2. Networks state exist as a system
3. Simplicity of Operation is consistent and decouple from the forwarding complexity

Q & A

Please Join the Session at Cisco Live

Tuesday 7th March at 4pm

Room 210

- For more session on ACI please Visit

http://www.ciscolive.com/anz/learn/sessions/session-catalog/?search=aci&showEnrolled=false

Thank you

cisco

Cisco live!

7–10 March 2017 · Melbourne, Australia