.1|111|11 CISCO



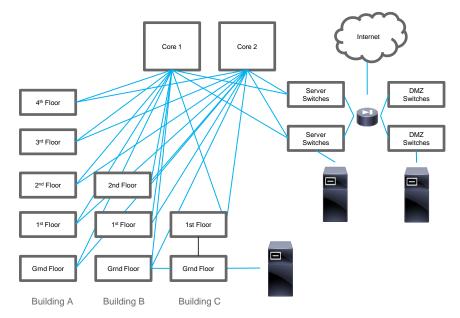
Your Time Is Now

Application Centric Infrastructure Fundamentals

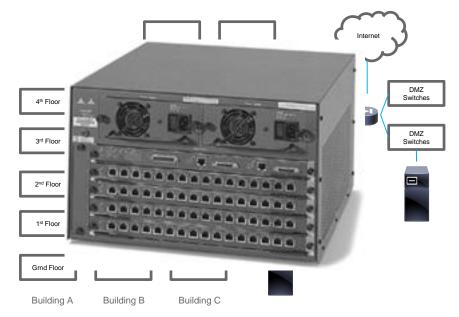
Nicholas Gorse – System Engineer BRKACI-2000



- 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...



- 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...



- 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...



Ciscolive

- 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...



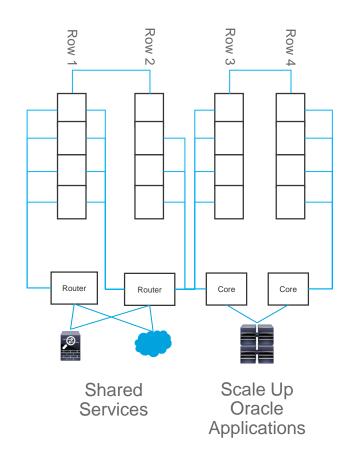
Ciscolive

- 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...



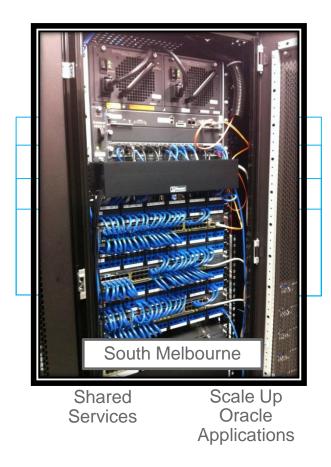
Ciscolive

- 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...



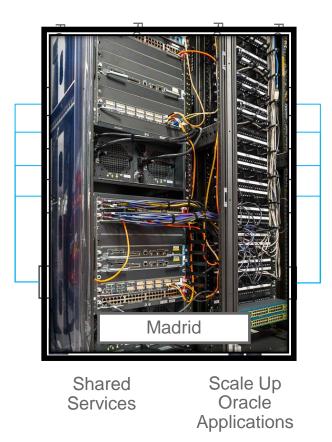


- Then I worked for a company that hosted a large Oracle applications for multiple customers
- Provided Hosting Services for customer infrastructure, including access to shared services like Internet and Firewall
- · Had different size locations around the world...



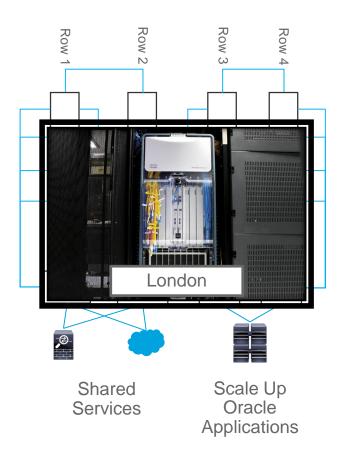
Ciscolive

- 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...



Ciscolive:

- 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...





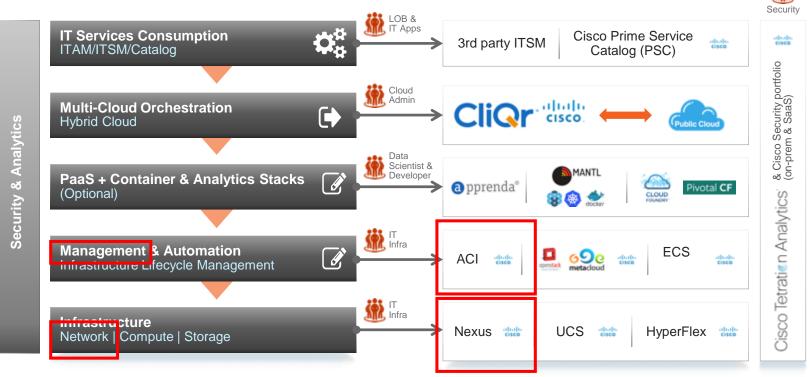
What I Learnt From Those Networks

- 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

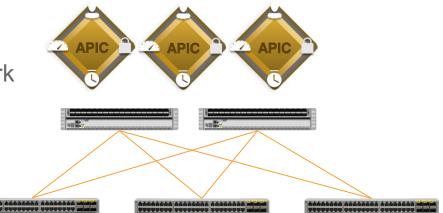


System Building Blocks



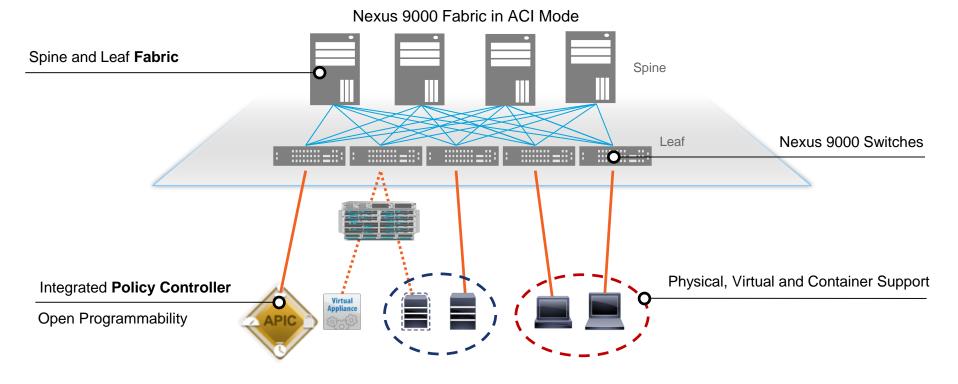
Application Centric Infrastructure

- · 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



Ciscolive!

A Controller for the Network



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

	ngorse — ssh r1 — ttys001
priv Oxed@ber	Raa269497s13s72dcab46s9s70 locslizadkou
rmon endu Ove	ngorse — ssh r1 — ttys001
rmon mon	Anno 100 (2010) 100
rmon rmon pri	w. SvadShanSha760407-12-72dcab46-0-79 Joch16radkav
rmon rmon	🖲 😑 🏠 🏠 ngorse — ssh r1 — ttys001
vlan rmon rmon na vlan rmon vlan vlan rmon na na vlan vlan vlan vlan vlan	priv %xxd8be38a569407a12a33dceb45a9279 localizedkey rmon event 1 log trap public description FATAL(1) owner PMON@FATAL rmon event 2 log trap public description CRITICAL(2) owner PMON@FATAL rmon event 3 log trap public description ERROR(3) owner PMON@FATAR rmon event 4 log trap public description MARING(4) owner PMON@FATAR rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
vlan na na	vlan 1,16-18,28-29,31,56,90,230,900-901,3090,3099
na vian vian	vlan 31
vlar vlar	name lab33
na na	vlan 56 name ptan
vrf vlan vlan na na	vlan 90 name outer
inte vrf vlan	name inter
inte inte vrf	vian 901 name translated
ip inte inte	vrf context management
inte ip inte	interface Vlan1
SH inte in	Interface Vlan17
dinte SM	no shutdown
fe inte SH	ip address 10.67.17.33/24
inte 👬	interface port-channel100 switchport access vian 17
SW SH SH	switchport trunk allowed vlan 17
sw fe	interface port-channel101
inte	switchport mode fex-fabric fex associate 101
_	interface port-channel103 switchport mode fex-fabric





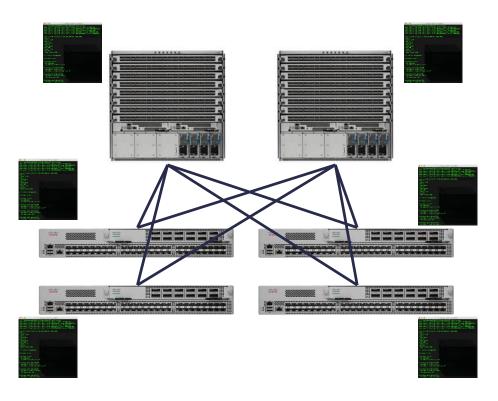




How Traditional Networks are Managed

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, ...

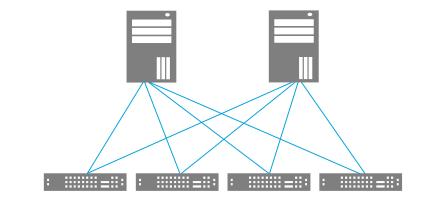


Cisco ACI solves the problem ...



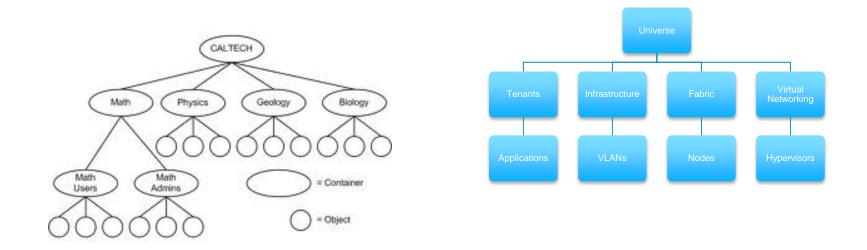
Interfaces, protocols, TCAM, etc ... all represented in an object model, and ALL accessible through an Controller Cluster called Application Programmable Infrastructure Controller (APIC)

System														kovence Icome,
ystem Health	Loone Loone soon		66					i		t Count Acked Fault	s By Dor		legated Fau	15
					-				Fact D	net:	Δ	A	0	
30									SYSTE	M WIDE	14	78	221	,
score									Acces		13	з	2	_
S 25									Extern	al	0	14	0	
									Frame	eak	0	39	1	
0									intre		1	15	36	
	6.00 18.00	20:00 23	2.00 12. Feb Time	02:00 04	ico osise	05:00	10.00	12:00		ement	0	a	0	
1.1			an l					1	Securi		0	0	10	
(<u> </u>	16.00	20:00	12. Feb		05:20	88:00		12.00	Tenant		0	,	172	
Name	POD D		Турк			Health Score			- Fast L	Acked Feat	Δ	A High De	iegeted Feu	109
e name ef 1	1		iyos iso/			58			Fact L	oveit	≙	A	0	
r10	1		lee/			80			Comm	unicati	13	12	2	
13	1		kef			68			Contg		0	8	174	
:14	1		loaf			98			Enviro	Internation	1	a	3	
ne1	1		spine			80			Operat	tional	0	58	42	
ine2	1		spine			80			Con	troller S	tatus			
									- ID	Neme	P	Admin Stete	Operational Status	n H S
enants With Health	≤ 99					99			1	apic 1	10.0.0.1	in Servi	Aveilable	B
rte .			Handth						2	apic2	10.0.0.2	In Servi	Avellable	R
DNTIV-default			99						3	apic3	10.0.0.3	In Servi_	Available	Ð
qr			66											
icc			99											
mmen			97											
630			- 99											
			99											





APIC Object Model is a Database



Common Operational Properties - AD, LDAP, ...

System Management, Change Management, System Integrity, Correlation

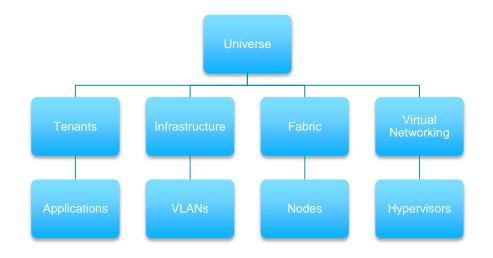


APIC Object Model

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

havgetar J	Ness	
(intere) (1)	Gering Stand Alexa	
Doos A/D Falanci		
PURE .	How to intersect with your Class ACI Fabric	~
ACI Fabric	This interface rate you easily configure and monitor value ACI ("ables from your vCohere any intervent."	manna and a second
Application Profile		
a hit we high	Francises, you are able to formulate your application metwork requirements in an interview	
P Trainmeng		and a state of the
al Astern	reven adverting a pile pound order and and a set	All the second
M Annah	Experi ba	
Dame Demethra		
W LAT Service	67 voted	A THE AND A THE AND
	per perio	25 6
		No. Anter Anter State State State State
	Dank Taste	Diplans Nativer
	& Create a new Tenent	Application Centric Infrastructure (ACI)
	Create a new Application Profile	
	II Creats a new Endpoint Group	
	- Green a new snappint Group	

VShpere Client

Neuron Rather Advention & 💩								
1 mar (i) 🕢	# Geo.	lever Corrents 🔛 Erits	lara .					
United (0) (0) Carted Directory Representation Strengthment (1) (1) - Strengthment (1) (1) (1) - Carted Directory Representation (1) (1) (1) - Carted Directory Representation (1) (1) (1) (1) - Carted Directory Representation (1) <t< th=""><th></th><th>E tree monitoria and an annual and an annual and an annual and an annual annual</th><th>E Aust</th><th>i fanting</th><th>H-harped (map) (map) (map) (map) (map) (map) (map) (map) (map) (map) (map) (map)</th><th>Basers</th><th>B Rapiner grup</th><th>Bankan (</th></t<>		E tree monitoria and an annual and an annual and an annual and an annual	E Aust	i fanting	H-harped (map) (map) (map) (map) (map) (map) (map) (map) (map) (map) (map) (map)	Basers	B Rapiner grup	Bankan (
					(angl)			
		TMRC SOCIET			(HEARING)			

ServiceNow



VRealise

(Notes)									35	
_										 Construction of the local sectors of the local sect
e		2							-	
-										_
_	inter ten 1	1000	Cox Martin		0.000	Adder Allan		Test de		
-	1012						1			
1.471	1997	10000	Low grants	~	10000	100				
24		100.223		-			100			
	144									
	1911									
21.21	w	POR NOT	OV PER I		n Barrar		-			
-										
01										
s										
	2004 6 - 67 (* 24 24 (24) 24 (24)	Loss of annual of annua	Kurrer M In Control (Internation Control (Internatio))))	Interf Interf<	Interf Interf<	Land State State				Intelligence Section

UCS Director



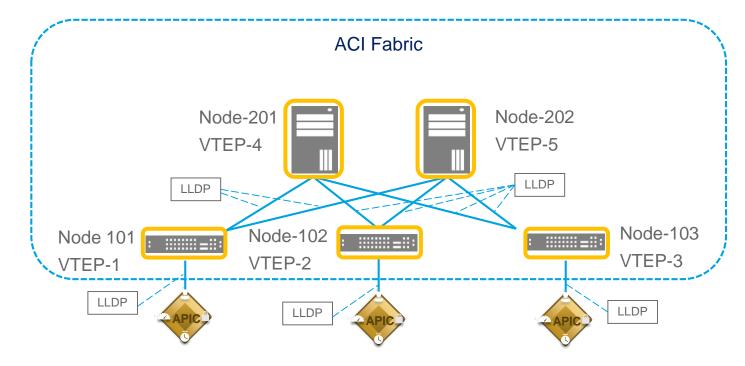
Openstack

Service Management Part	• v		0	wingschiltrates som
AL 1994	aci			
UNITED AND AND AND A	PATRILICS. MERCHANNER	TRUBAL AND HERE . HEREALT . TRUBAL AND HE	MARTINETON CONTRACT	
An Account		COLUM	005998	p
A.	101	01.04	801	
·	• • • • • • • • • • • • • • • • • • • •	• FNF		
THERE IN CASE AND ADDRESS	VADINE (~) NEWNIK	NEXT NOW		
🚊 we account	- CREWALL	000 Million State State State State	<u>.</u>	
ø «	ф сознания	292 286 2 254 34		
	and a subscription of the	THE SECRET PARTY & LIVES AND ALL REPORT OF A DE	_	
		Pro facilitati (Pro facilitati ing		

Windows Azure Pack



Booting the Network (Zero Touch Deployment)



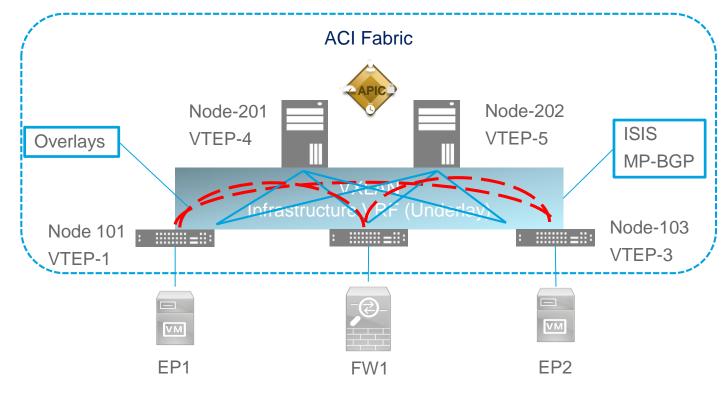
Ciscolive;

How we connect things



BRKACI-2000 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 3

How Endpoints Connect



Ciscolive;

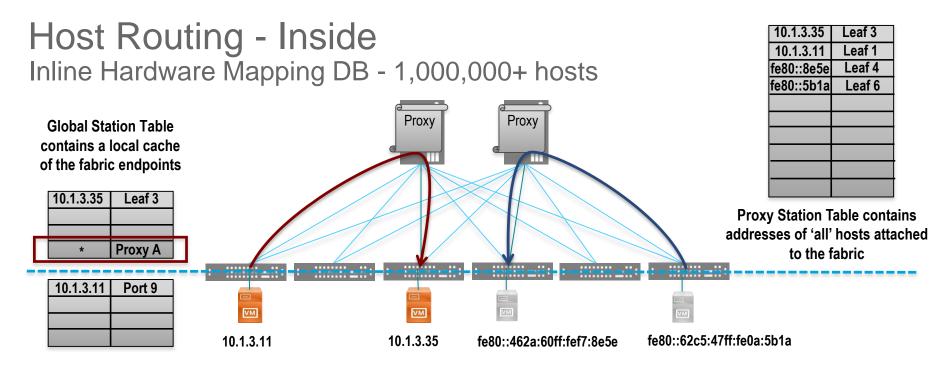
Agenda

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

Forwarding Packets



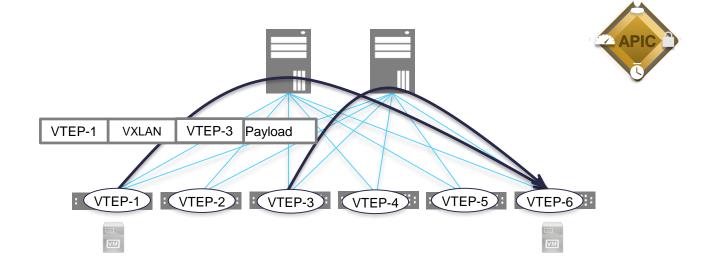
BRKACI-2000 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 3



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

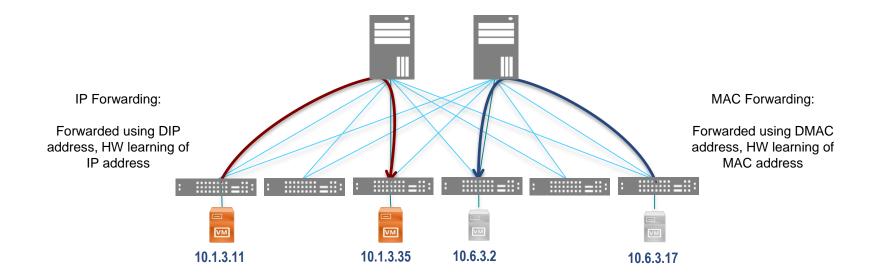
Ciscolive

ACI Fabric – Integrated Overlay Decoupled Identity, Location & Policy



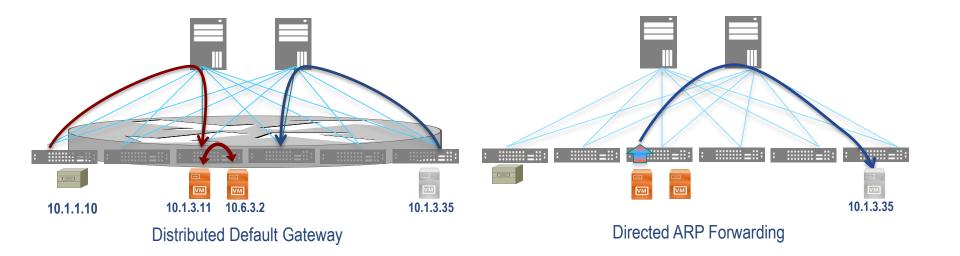
Cisco

Location Independent Forwarding Layer 2 and Layer 3





Location Independent Forwarding Layer 2 and Layer 3

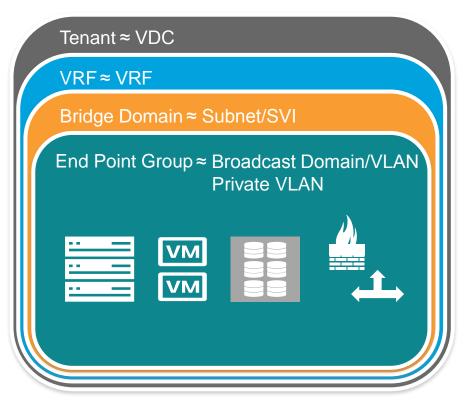




Logical Network Design







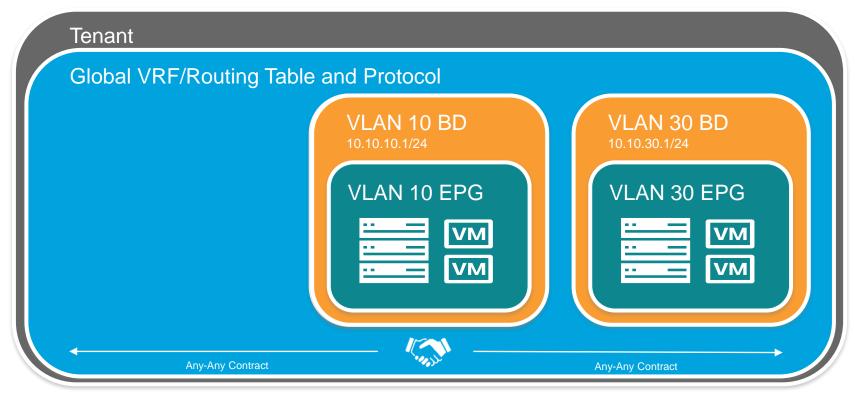


L2 External EPG≈ 802.1q Trunk

L3 External EPG≈ L3 Routed Link

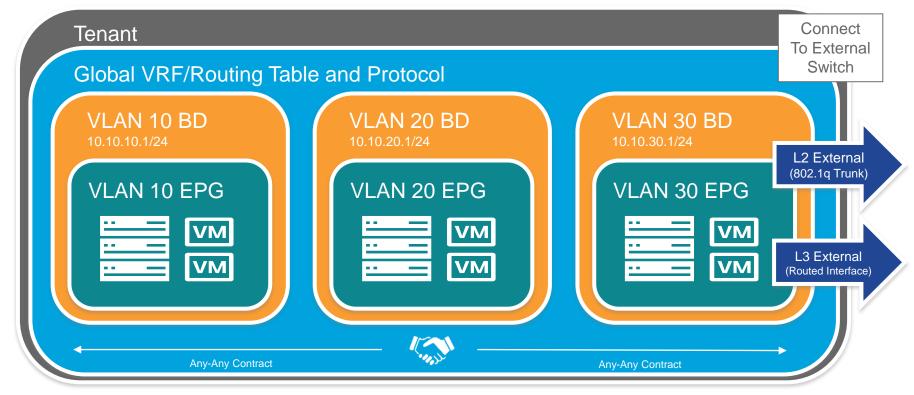
Cisco

The Policy Model – Network Centric Configuration



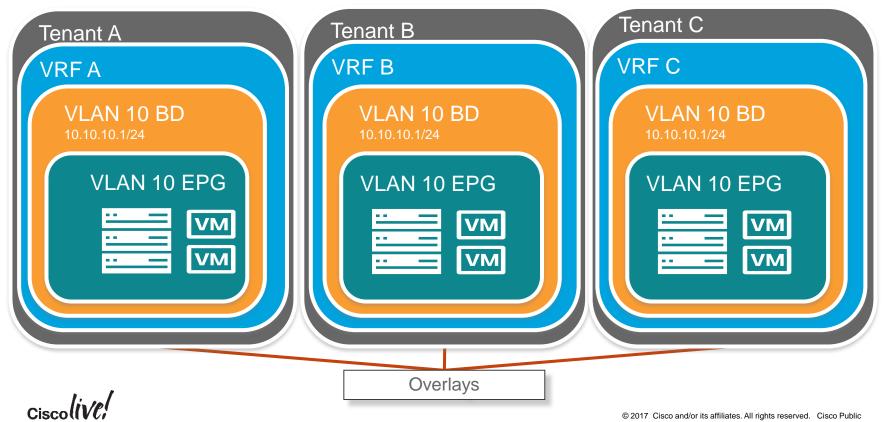
Cisco

The Policy Model – Network Centric Configuration



Cisco

The Policy Model – Flexibility in Design

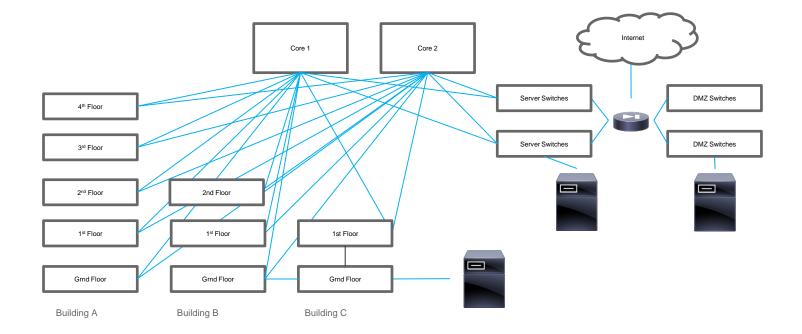


Example



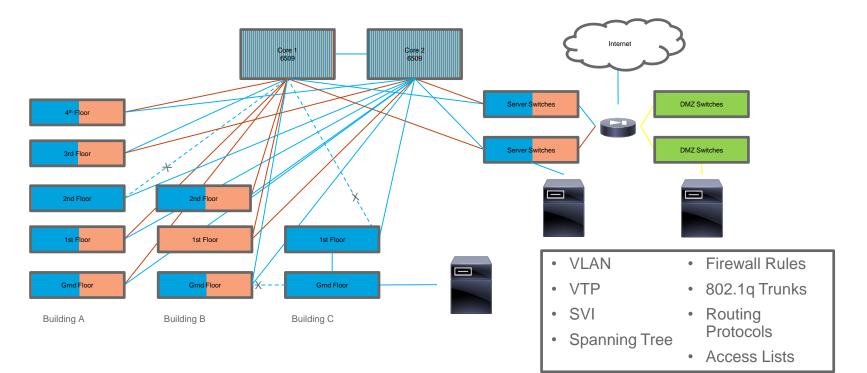
BRKACI-2000 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 4

Physical Network Design



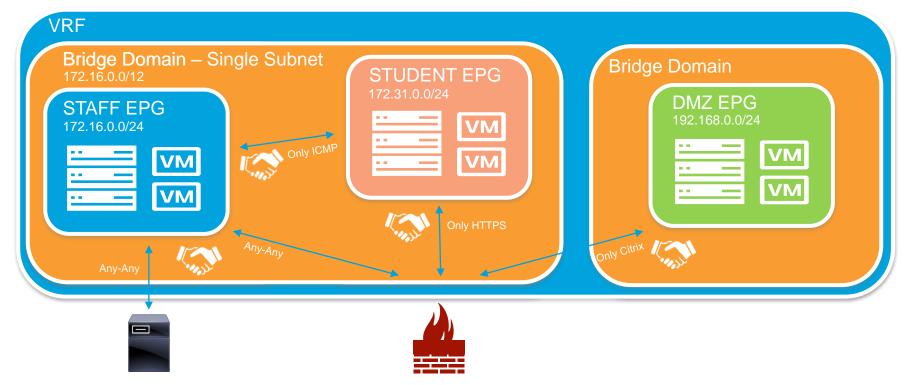
Ciscolive,

Logical Network Design



Ciscolive,

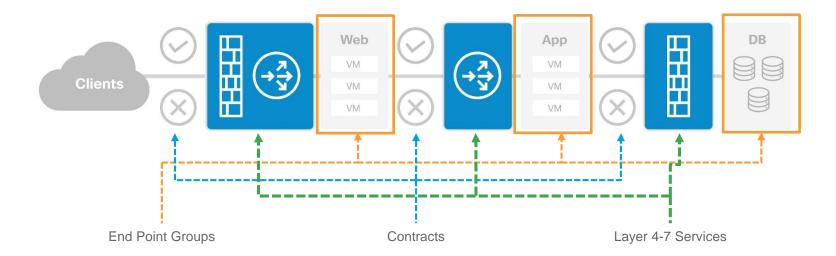
The Policy Model – My First Network in ACI



Ciscolive!

Sample Application Profiles

Student Management System

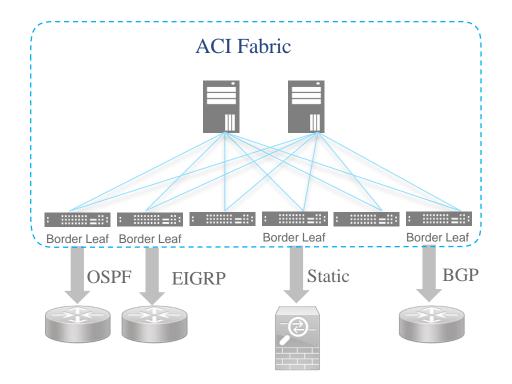




L2/L3 Out

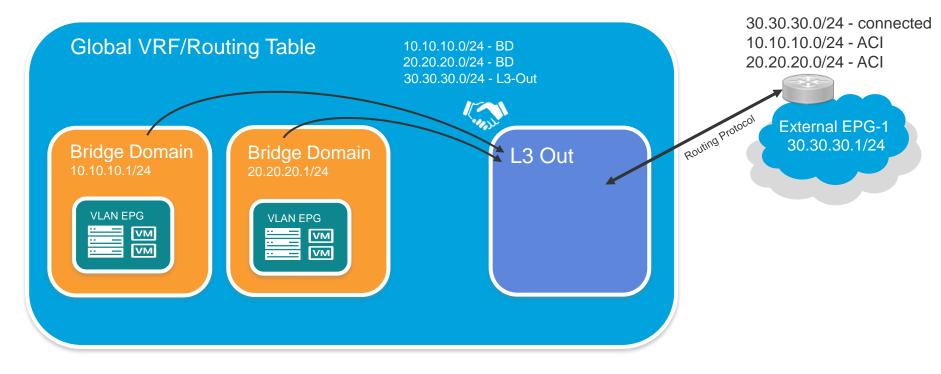


External Routing

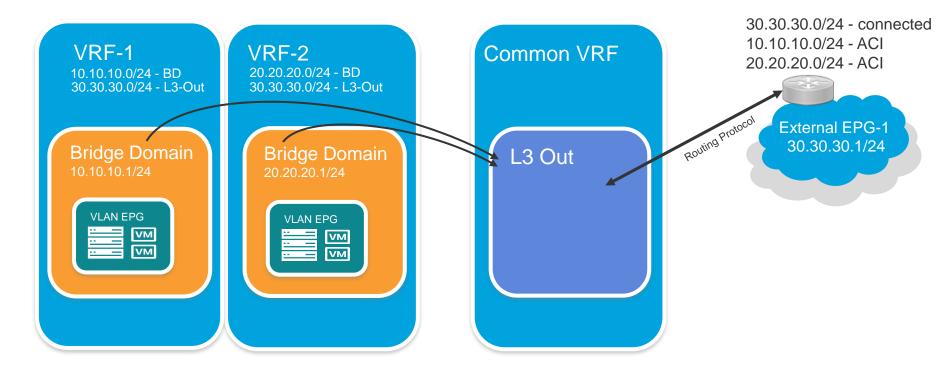


Ciscolive!

Routing Process



Flexibility in Routing



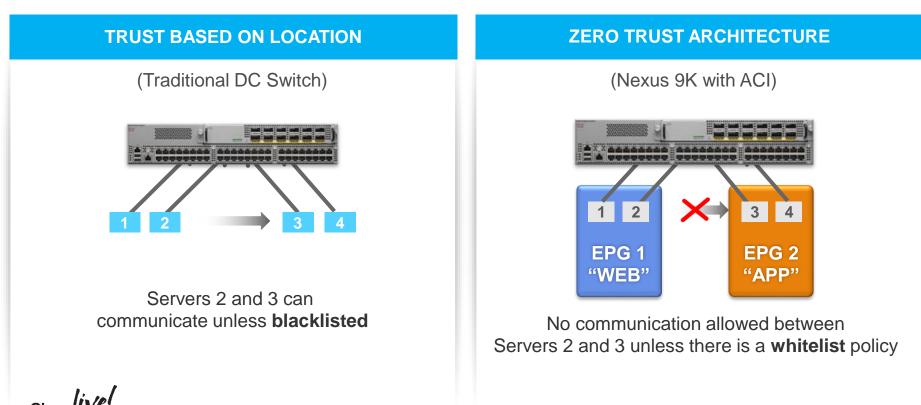
Ciscolive,

Segmentation

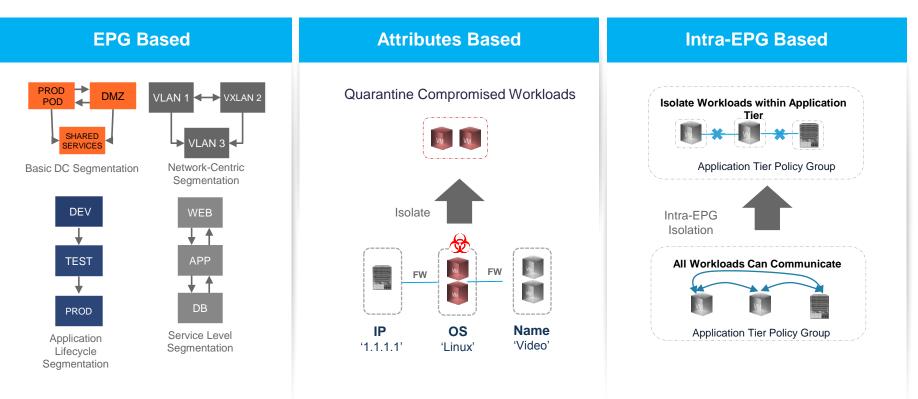


BRKACI-2000 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 5

ACI Whitelist Policy supports "Zero Trust" Model



ACI Delivers Hypervisor-Agnostic Microsegmentation





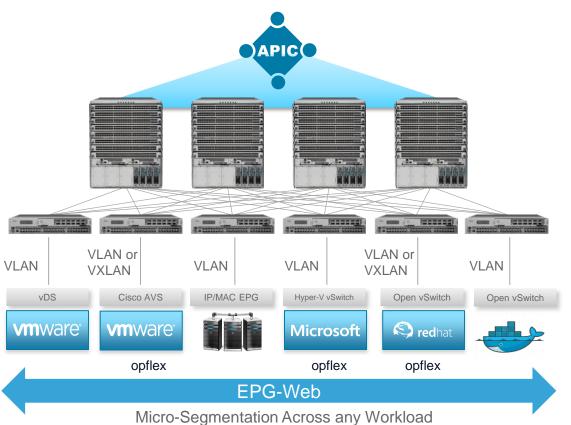
Micro-Segmentation with ACI

2 Capabilities:

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

Attributes	Туре
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

Ciscolive!



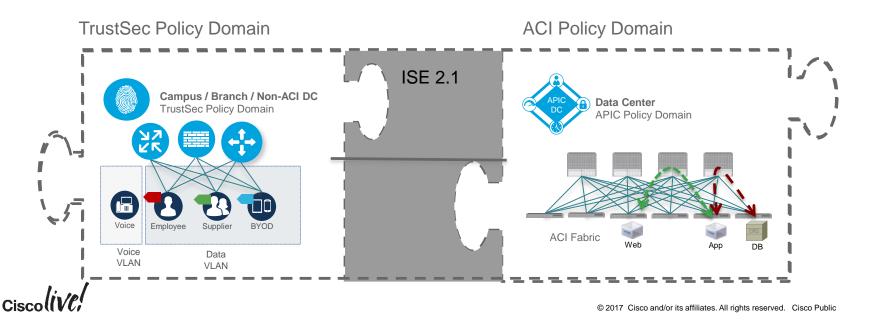
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



ISE Dynamically provisions TrustSec Security Groups in ACI Fabric



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



Security Groups



TrustSec Groups represented as External EPGs



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

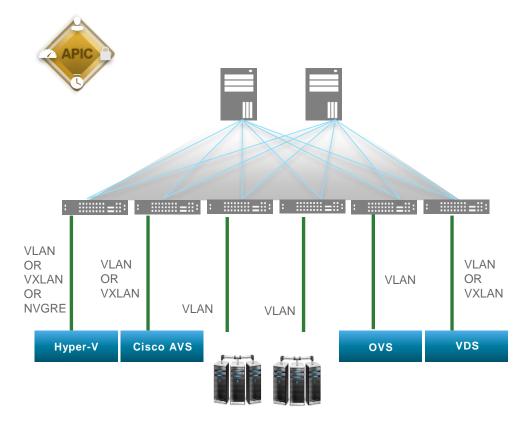
Agenda

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

Control of Hypervisor Networking

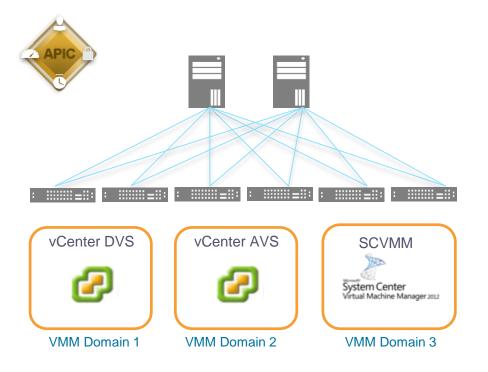


ACI – Any Application, Any Hypervisor



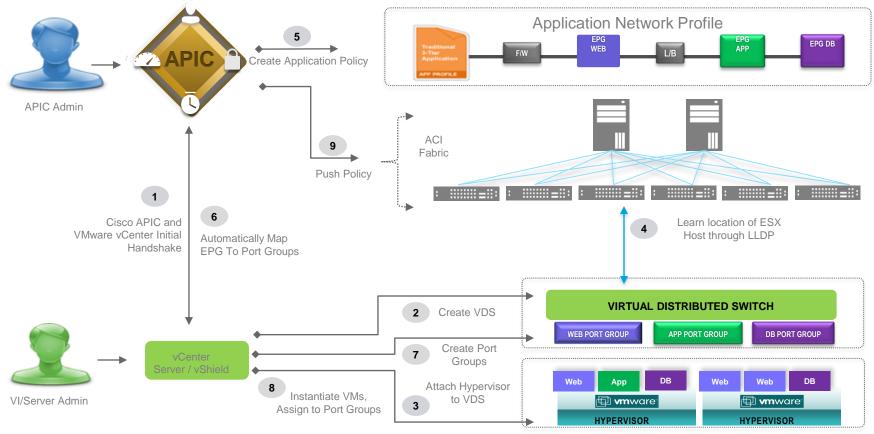


Hypervisor Integration with ACI

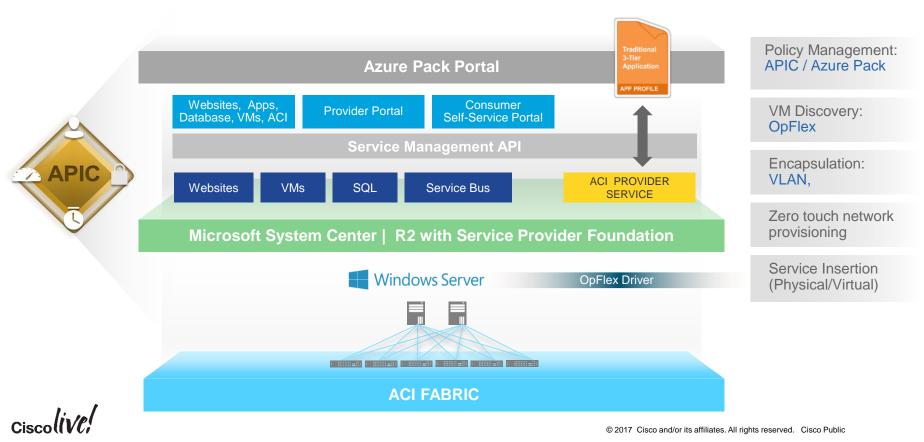




ACI Hypervisor Integration – VMware DVS/vShield



Cisco ACI – Microsoft Integration Microsoft System Center/Azure Pack



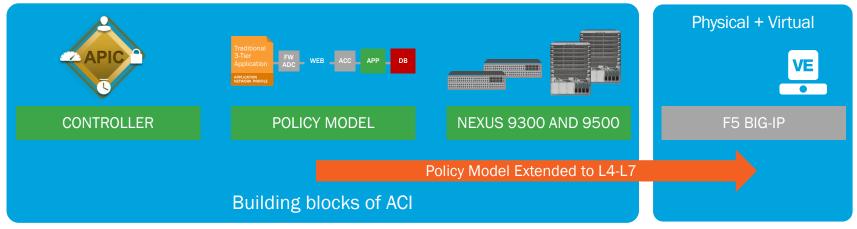
Control of Layer 4/7 Services



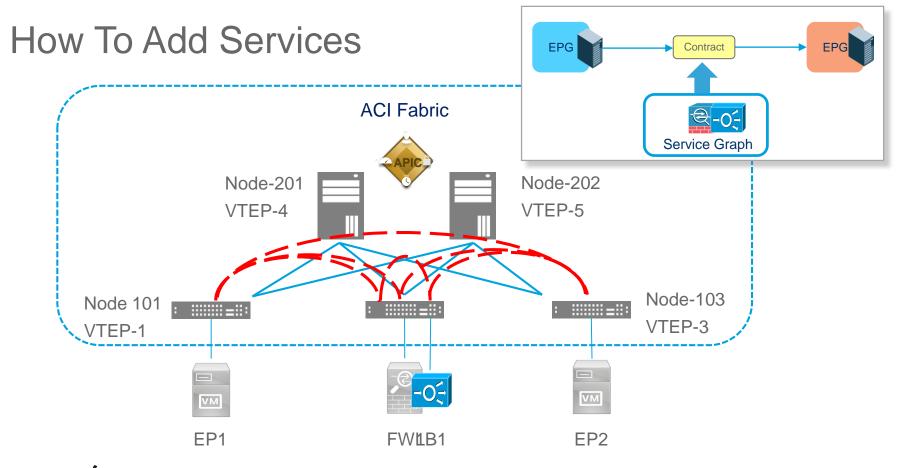
Cisco ACI Service Insertion

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

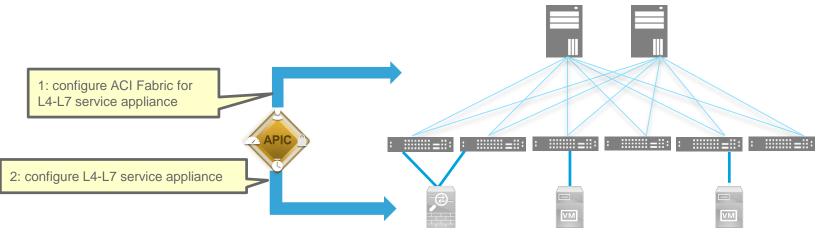


Ciscolive!

Service Graph Overview

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

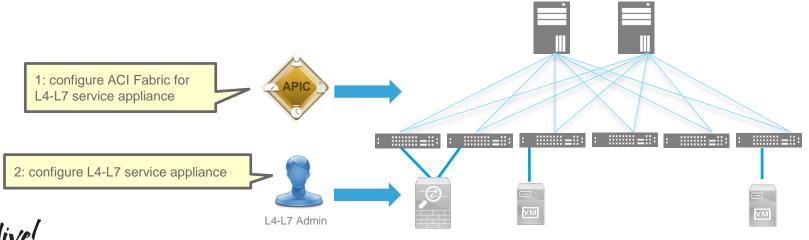
- 1. Network automation: Allocate the fabric resources(VLANs) for the service and program fabric
- 2. L4-L7 configuration automation: Configure L4-L7 service appliance.



Unmanaged mode

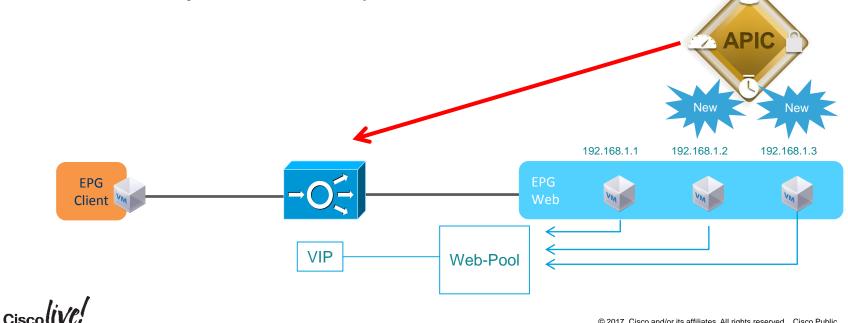
Network only switching feature adds the flexibility for customer to **use only network automation for service appliance.** The configuration of the L4-L7 device is left to be done by customer.

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

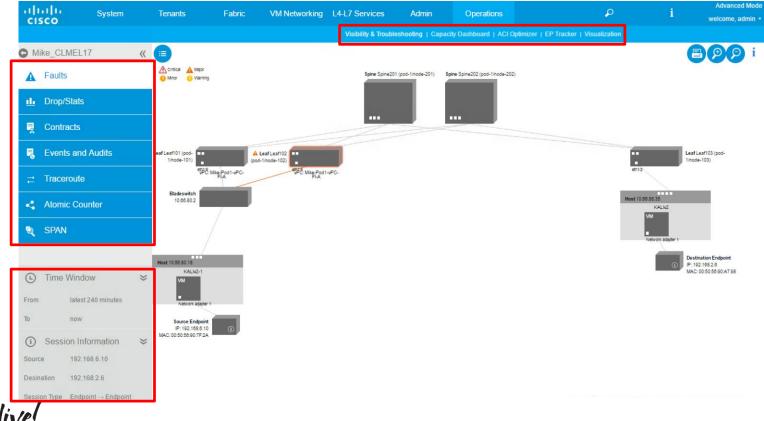


Visibility and Automation



ACI - Troubleshooting and Operation Tools

Cisco



ACI Developers

0000

Introducing the Cisco App Center

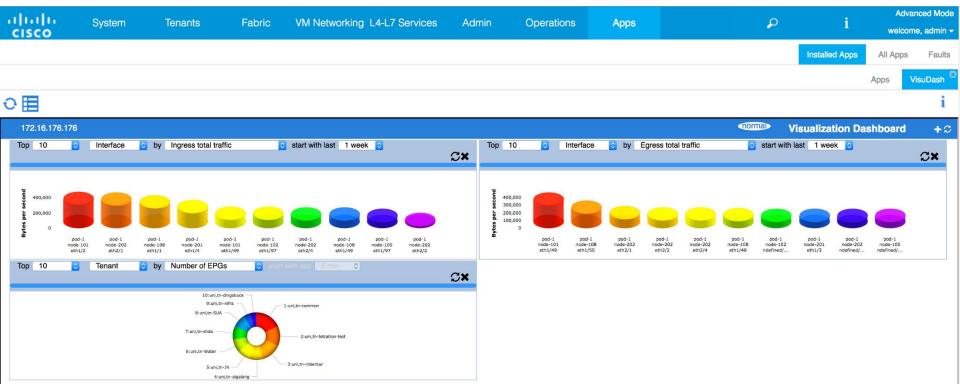
Software Defined Networking (SDN) is enabling organizations to accelerate application deployment, dramatically reducing IT costs through policy-enabled workflow automation. Explore the Cisco App Center and select from a wide range of SDN applications that allow you better align your network with your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

Browse apps

Featured Apps

Contract Viewer		InfobloxSync	Infobiox 📚	ServiceNowCon	Service <mark>now</mark>
Cisco ★★★★★	🛨 Download	Cisco ★★★★★	🛨 Download	Cisco ****	🛨 Download
VisuDash	1				

VisuDash



Ciscolive,

Contract Viewer

Cisco



Public 82

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



ıılıılıı cısco



7-10 March 2017 · Melbourne, Australia