

INTUITIVE

Cisco *live!*

5-8 March 2019 • Melbourne, Australia

#CLMEL



Introduction to ACI

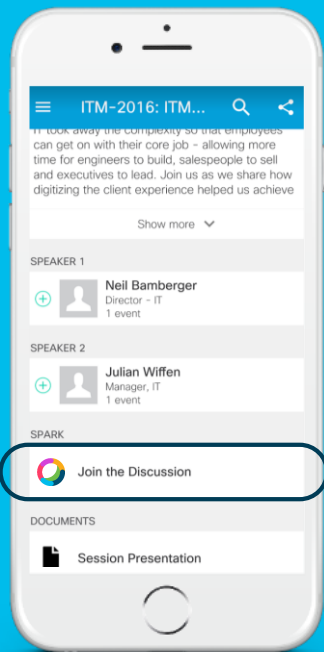
Richard Watson, DC Systems Engineer
BRKACI-1000



#CLMEL



INTUITIVE



cs.co/ciscolivebot#BRKACI-1000

Cisco *live!*

Cisco Webex Teams



Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

- 1 Open the Cisco Events Mobile App
- 2 Find your desired session in the “Session Scheduler”
- 3 Click “Join the Discussion”
- 4 Install Webex Teams or go directly to the team space
- 5 Enter messages/questions in the team space



hey.

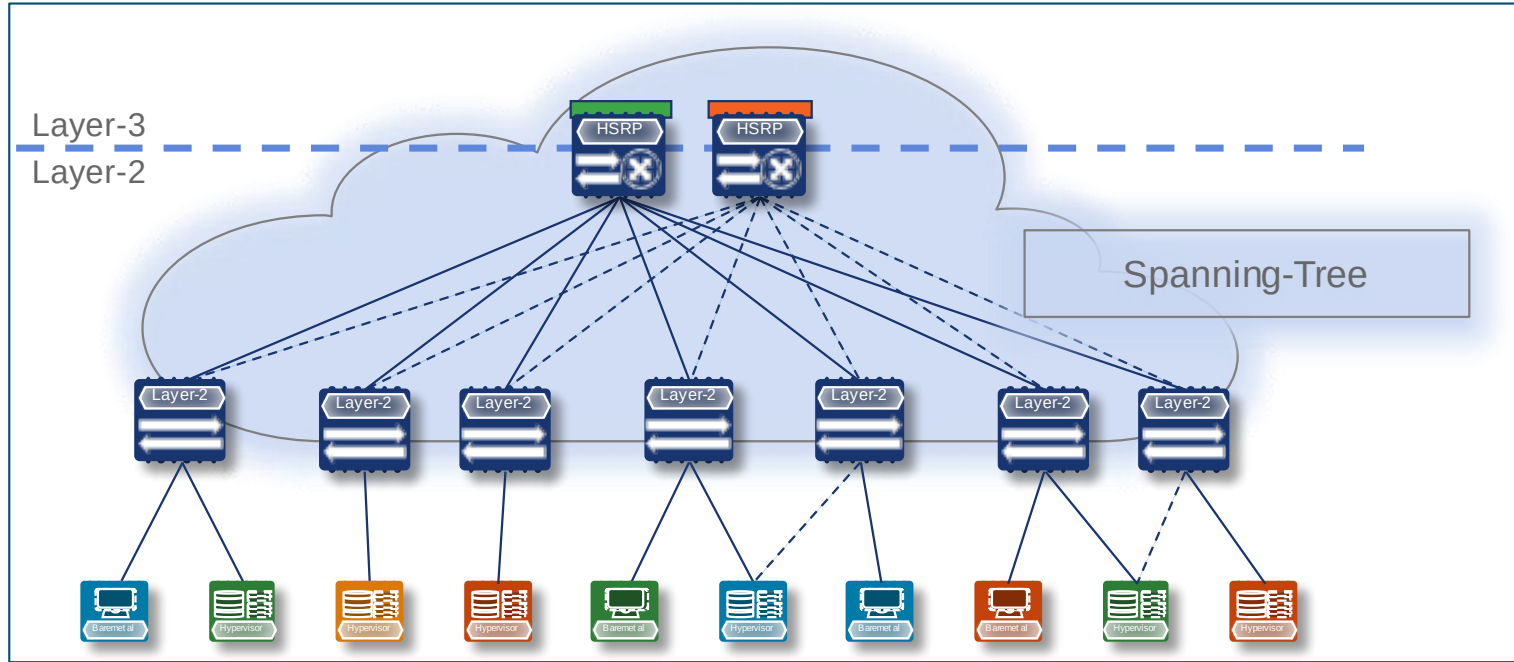


Agenda

- Introduction
- **Evolution of Data Centre Networking & Management**
- What is ACI?
- ACI Anywhere
- Making the most of ACI
- Where to go next

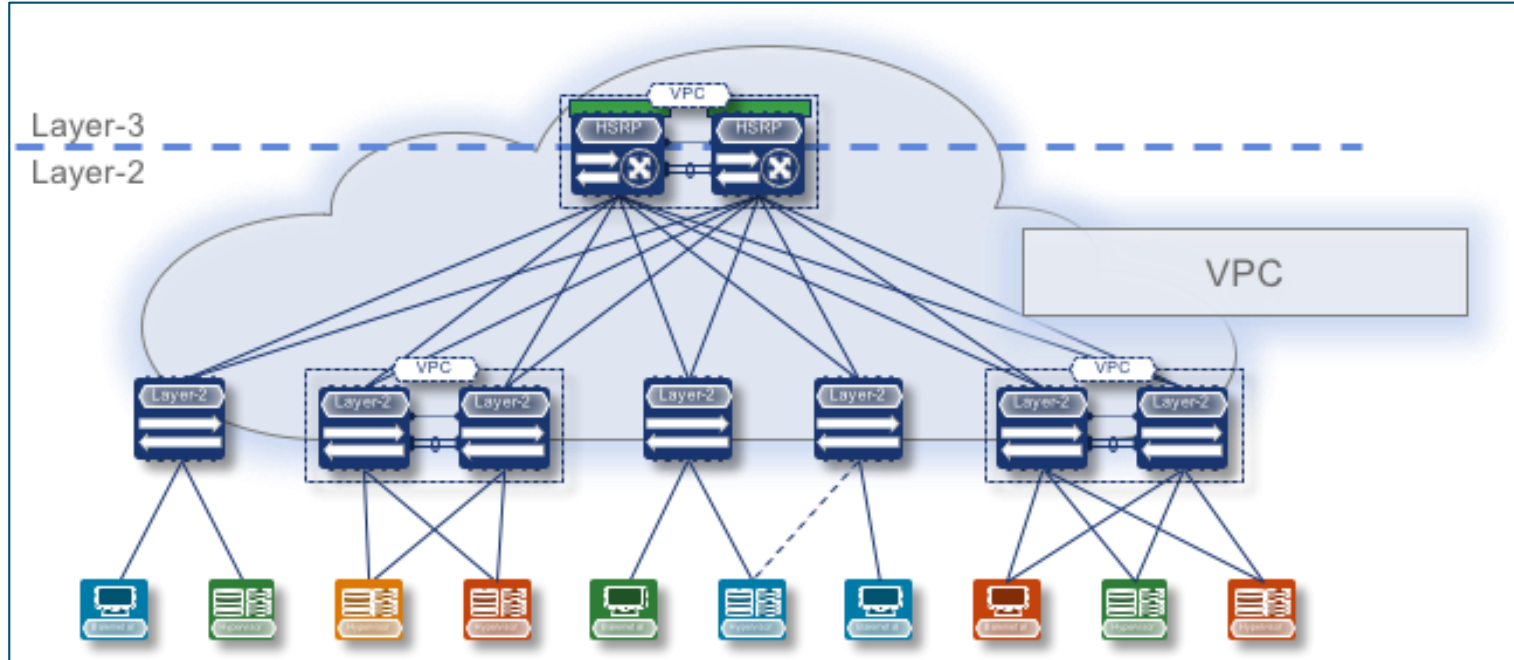
DC Network Evolution

Spanning Tree



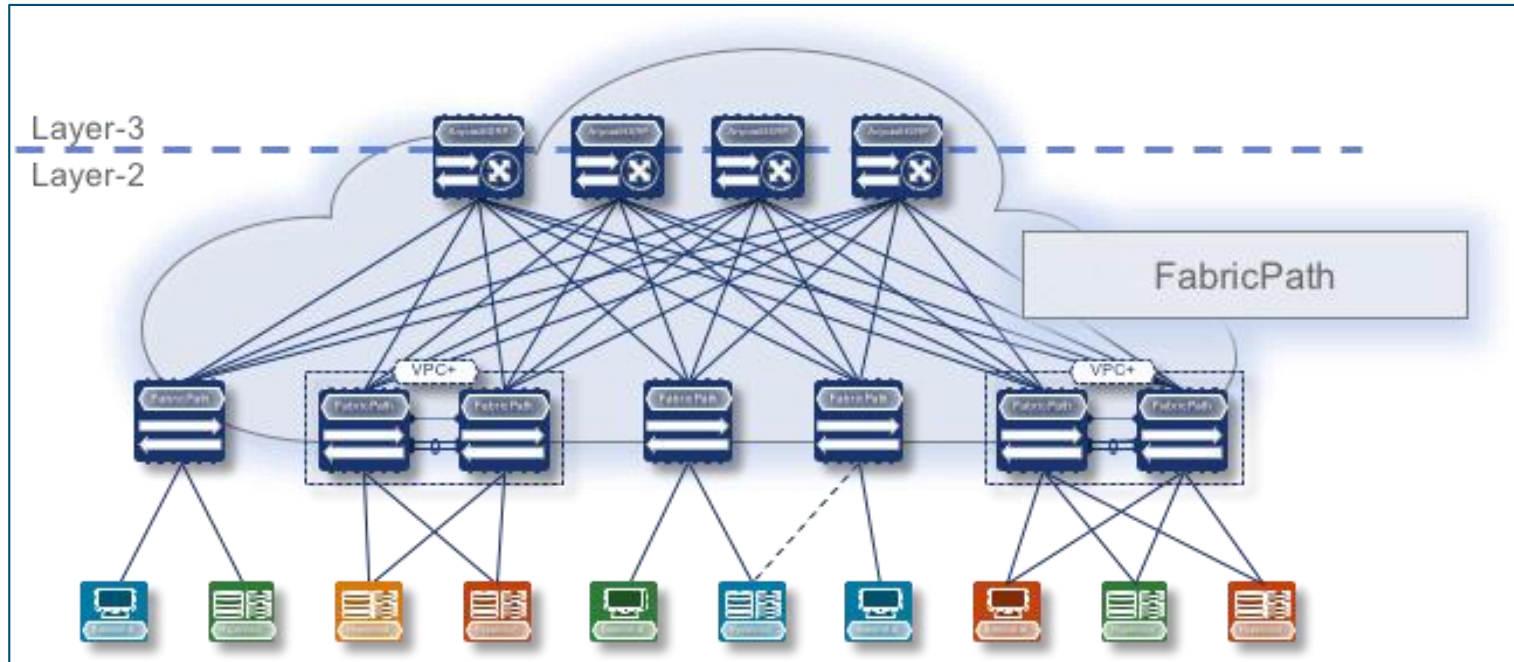
DC Network Evolution

Simplified Spanning Tree with vPCs



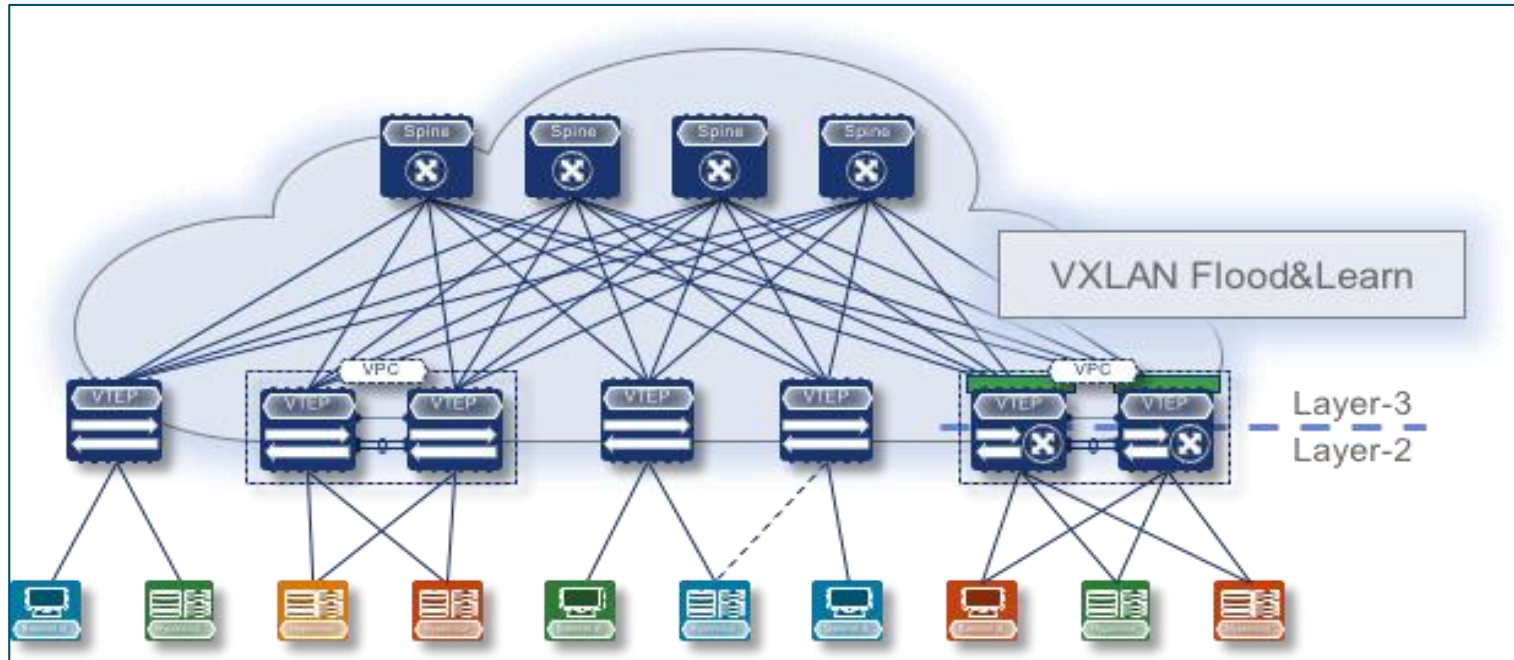
DC Network Evolution

Replace Spanning Tree with FabricPath (MAC-in-MAC Encapsulation)



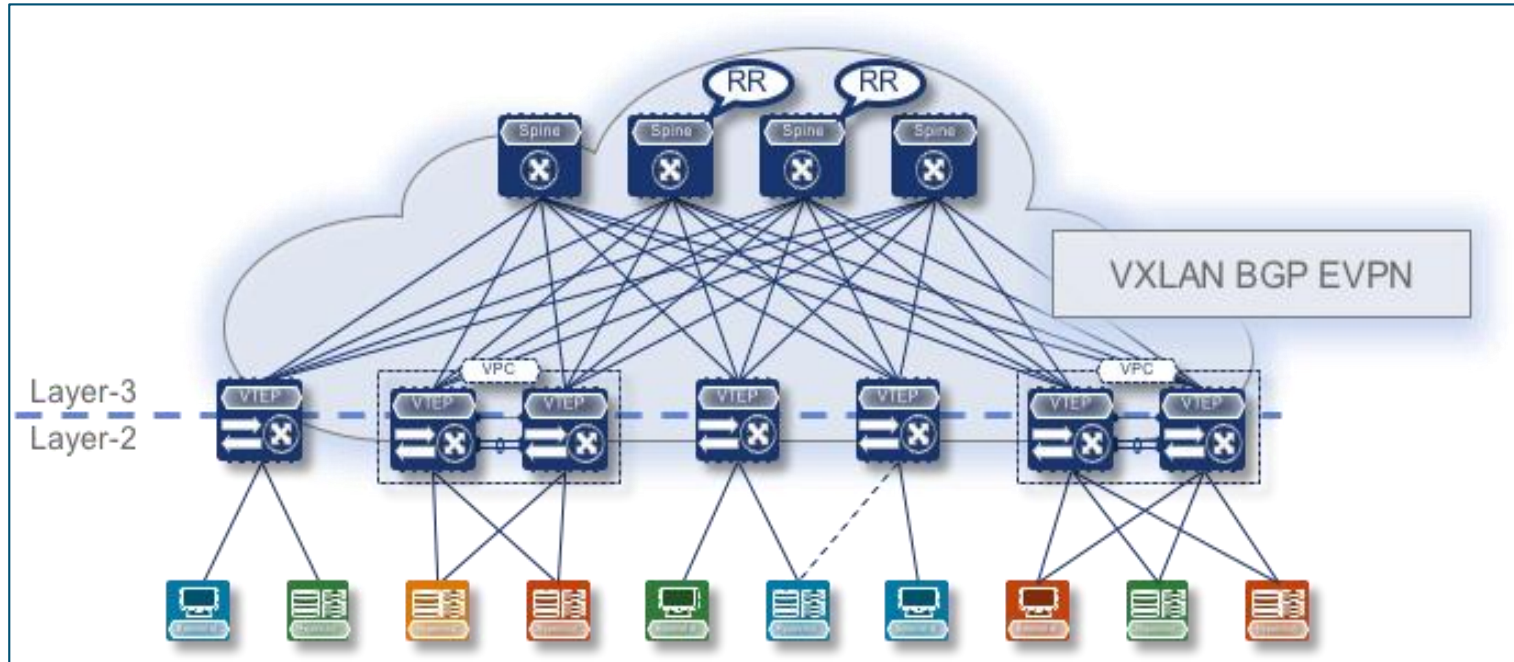
DC Network Evolution

Replace Spanning Tree with VXLAN (MAC-in-IP Encapsulation)

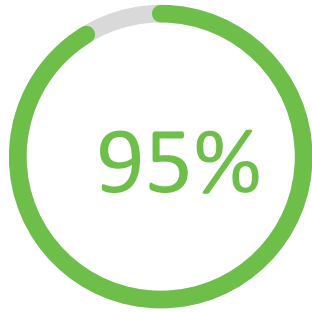


DC Network Evolution

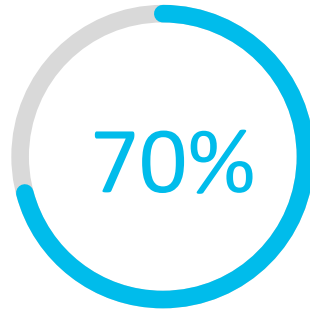
Improved VXLAN Performance with BGP Control Plane (EVPN)



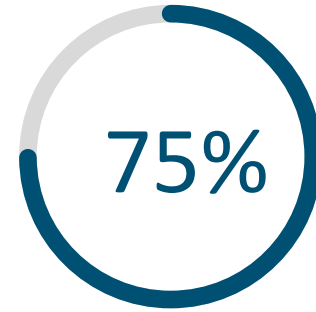
Current operating models aren't working



Network Changes
Performed Manually



Policy Violations
Due to Human Error



OpEx Spent on Network Changes
and Troubleshooting

US\$60B

Spent on Network Operations Labour and Tools

Source: McKinsey study conducted for Cisco in 2016

22% of all network outages are caused by human error



core-router#debug ip packet

Traditional Automation

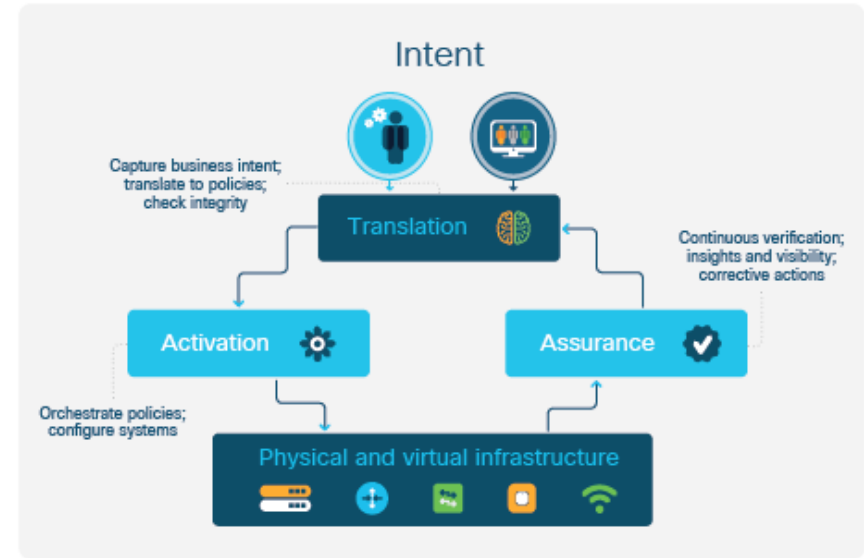
Software Defined Networking

- SDN is about providing a mechanism to automatically configure the network as a whole.
- Still deals with traditional networking constructs, Interfaces, VLANs, VRFs etc.
- Typically focused at automating “Day 2” tasks
 - *Add a VLAN to these interfaces on these switches*
 - *Add a route to this VRF*
- **Still a gap between the business requirements of the network and how those requirements are implemented and verified**
 - **Leaves room to misinterpret and misconfigure**
- ***Ideally need a network that is defined by the original Intent***

Intent-Based Networking

Intelligent Automation & Assurance

- Builds on traditional SDN capabilities
 - Activation
- Starts with Business Requirements (i.e. the intent) and **translates** into device-specific configuration (i.e. policies)
- Uses the policies to generate device-specific configuration that is then programmed (**activation**) though API
- Feedback loop (**assurance**) to ensure that the intent has been realised
 - Continuously checked
- **What is the Intent of the Application?**
 - Who the users, How they access the app, What Other services are required?



Networking comparison

	SOFTWARE-DEFINED	INTENT-BASED
TRANSLATION		
Input intent		●
Translate to policy		●
Check integrity		●
ACTIVATION		
Orchestrate policies	●	●
Automate network configurations	●	●
ASSURANCE		
Visibility	CENTRALIZED (DOMAIN)	CENTRALIZED (WITH BROADER CONTEXT)
Insights (context + policy)		●
Continuous verification		●
Corrective actions		●

Automation – Do what works for you...

Do-It-Yourself / B.Y.O Automation

- Standard NXOS Open API
- NetConf / Yang Models
- Large Ecosystem of partners
- Extensible for homegrown tools with LXC and Docker containers
- ..But takes time to setup & manage



Cisco *live!*

Off-the-Shelf / Prebuilt Platform

- Single vendor simplicity
 - From build to ongoing support
- Integrated Intent Based Networking
 - Translation, Activation, Assurance
- Intent-based Policy based management



Partners



Automated



IT Policy

Application Centric Infrastructure

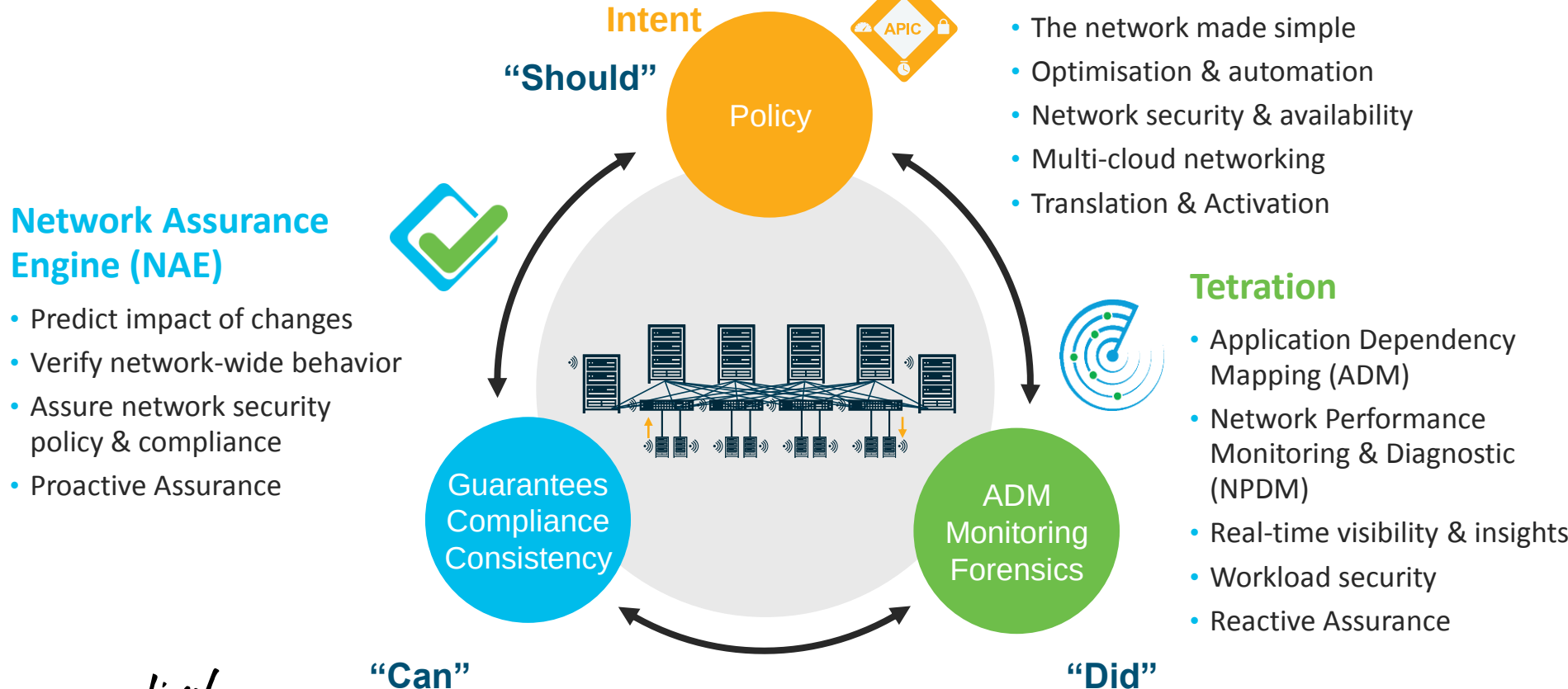
*Pre-built, Best Practice-based, Platform for
Intent-based DC Networking Automation*



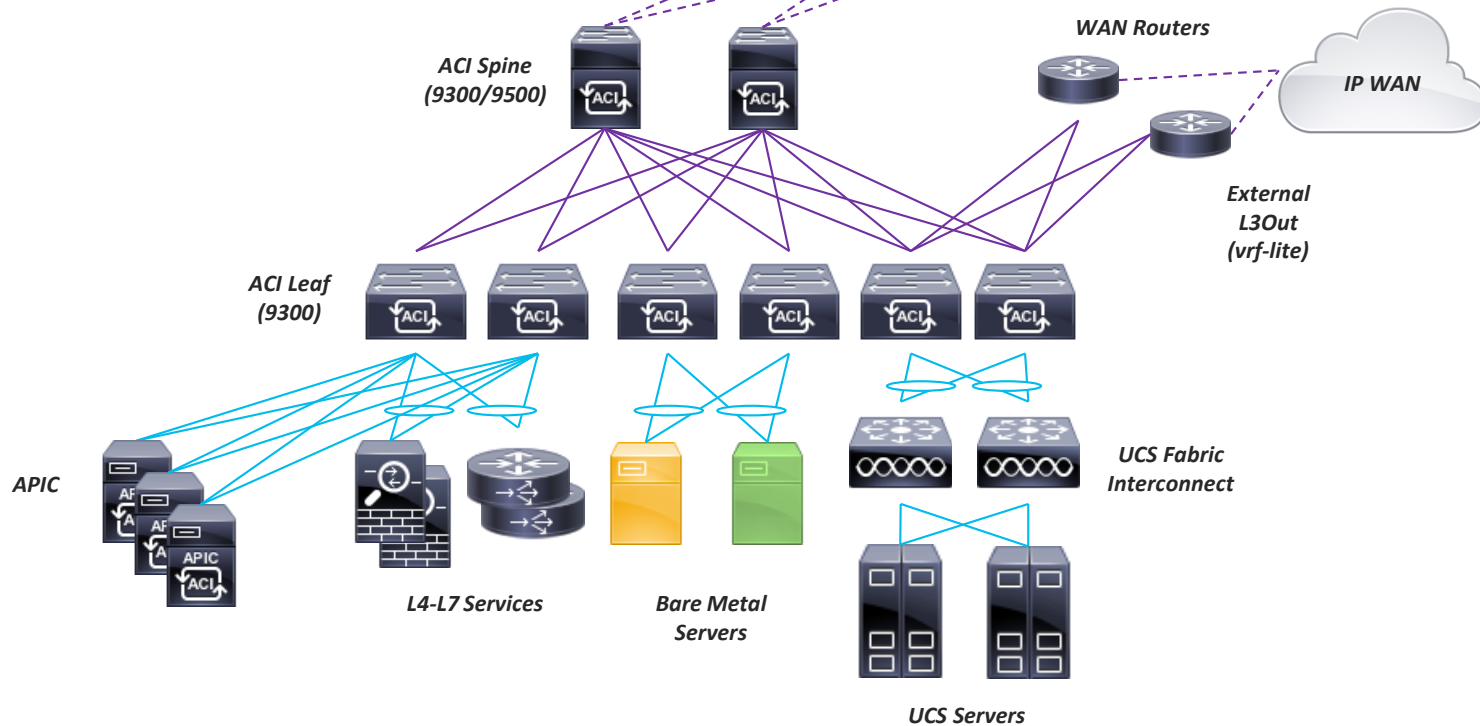
Agenda

- Introduction
- Evolution of Data Centre Networking & Management
- **What is ACI?**
- ACI Anywhere
- Making the most of ACI
- Where to go next

Intent-Based Data Centre

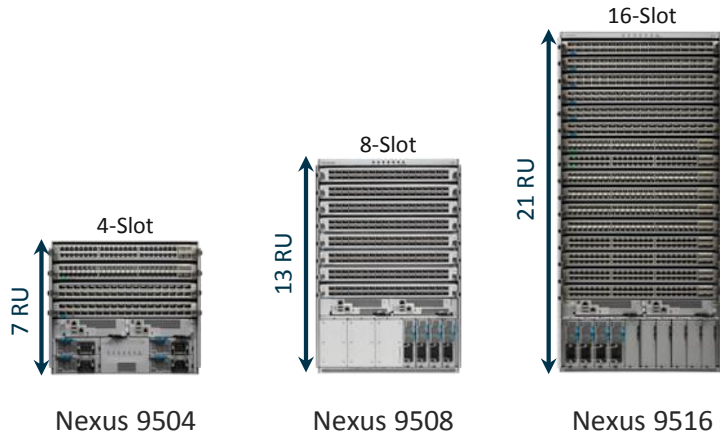


ACI Fabric Physical Overview



Cisco Nexus 9500 Cloud Scale Modular Portfolio

Cisco Nexus® 9500 Chassis



	ACI	MACSec	CloudSec	Capacity
 X9736C-FX 36p 100G	✓	✓	✓ Ports 29 - 36	3.6Tbps (5 FM NX-OS)
 X9732C-EX 32p 100G	✓			3.2Tbps
400G QSFP-DD* <small>* CY19 Roadmap</small>	✓			6.4Tbps

EX & FX line cards can be mixed in the same chassis with FM-E or FM-E2 fabric modules

Cisco Nexus 9300 Fixed CloudScale 1/10/25G Switches

Nexus 9300 FX2

96p 1/10GT + 12p 100G QSFP28

Nexus 93216TC-FX2



Q2 CY19

Q2 CY19

96p 25G SFP + 12p 100G QSFP28

Nexus 93360YC-FX2



48p 25G SFP + 12p 100G QSFP

Nexus 93240YC-FX2



48p 1/10GT + 6p 100G QSFP28

Nexus 93108TC-FX



48p 25G SFP + 6p 40/100G QSFP

Nexus 93180YC-FX



48p 100M/1GT + 4p 25G SFP

+ 2p 100G QSFP28

Nexus 9348GC-FXP



Nexus 9300 FX

48p 1/10GT + 6p 100G QSFP28

Nexus 93108TC-EX



48p 25G SFP + 6p 100G QSFP28

Nexus 93180YC-EX



Nexus 9300 EX

Cisco Nexus 9300 CloudScale 40/100/400G Switches

Nexus 9300 400G Leaf/Spine

16p 40/100/400G

Nexus 9316D-GX

*CY19



28p 40/100G QSFP & 8p 40/100/400G

Nexus 93600CD-GX

*CY19



Nexus 9300 40/100G Spine

64p 40/100G QSFP

Nexus 9364C



32p 40/100G QSFP

Nexus 9332C



Nexus 9300 40/100G Leaf

32p QSFP

32p 40/50G | 24p 40G + 6p 100G | 28p 40G + 4p 100G | 18p 100G

Nexus 93180LC-EX



36p 40/100G QSFP 28

Nexus 9336C-FX2



Legend

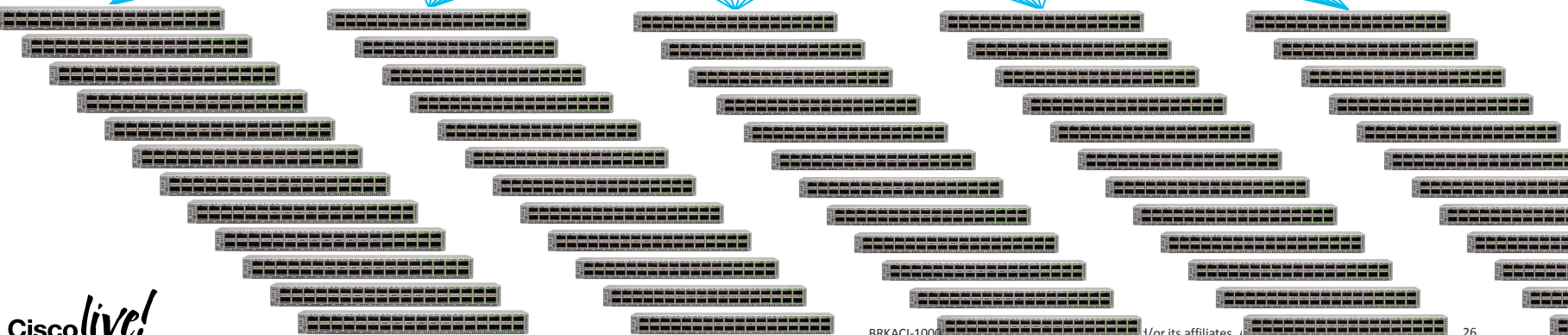
ACI Leaf/Spine & NX-OS

ACI Spine & NX-OS

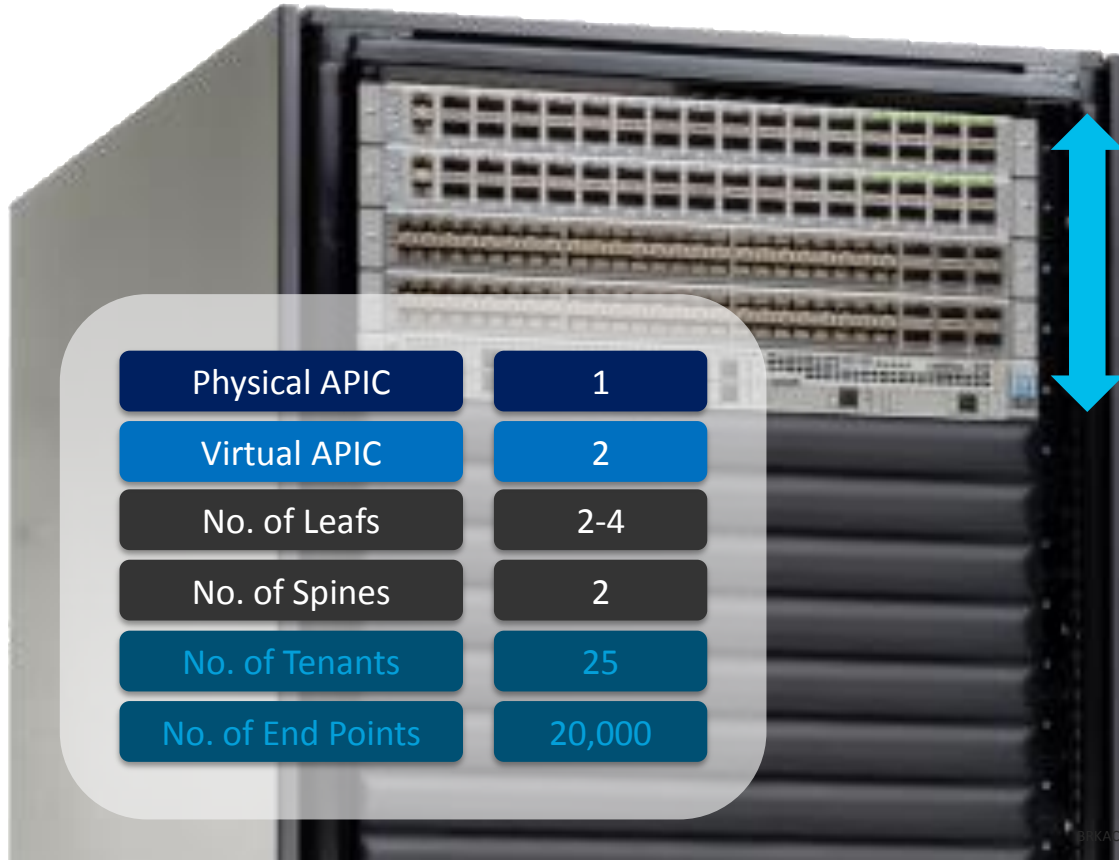
ACI Leaf & NX-OS

- 6 ACI Spines
- Up to 16 x 16p 400G LCs
- 6.4Tb per LC
- >100Tb per Spine

- Up to 200 x Access Leaf Switches
- Each 28 x 100G Access
- >400Tb Access Bandwidth!
- 326 RU of Space!!



ACI Mini – Maximum features, Minimum size



5 RU

- Full ACI Platform
 - 2 x Nexus 9332C
 - 2 x Nexus 93180YC
 - 1 x APIC-M3 Controller Server

Physical APIC

1

Virtual APIC

2

No. of Leafs

2-4

No. of Spines

2

No. of Tenants

25

No. of End Points

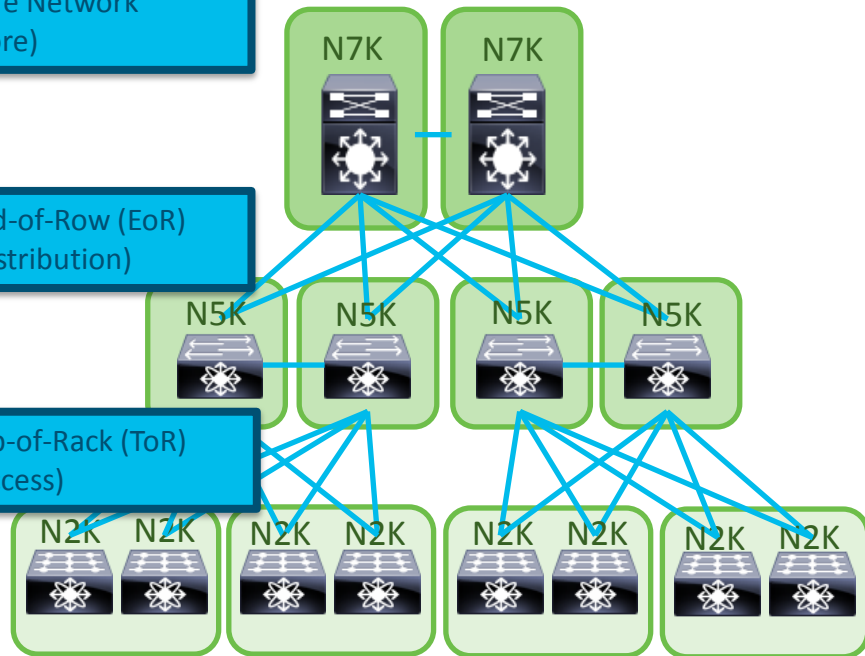
20,000

Typical 3-Tier DC Cabling

Core Network
(Core)

End-of-Row (EoR)
(Distribution)

Top-of-Rack (ToR)
(Access)



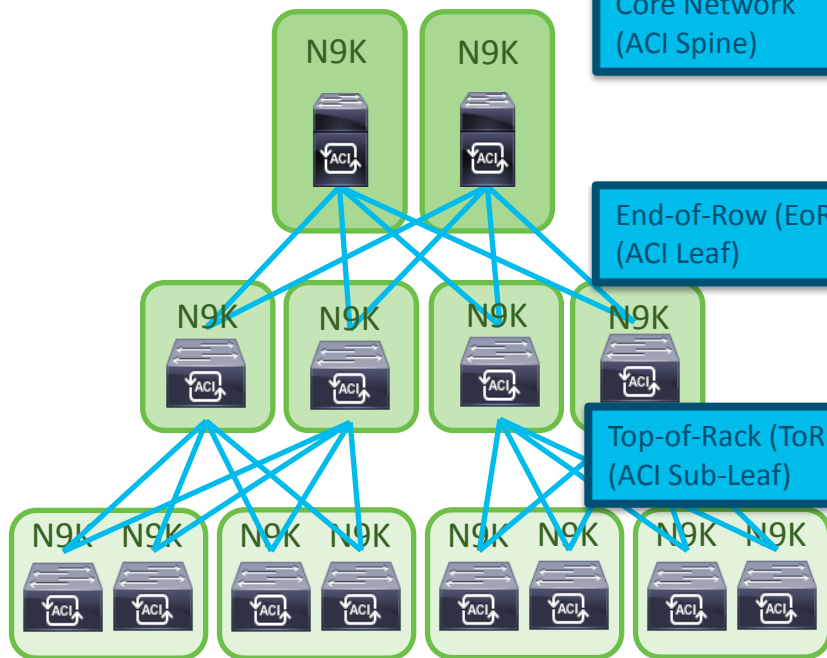
10G MMF

ACI Multi-Tier (New)

Core Network
(ACI Spine)

End-of-Row (EoR)
(ACI Leaf)

Top-of-Rack (ToR)
(ACI Sub-Leaf)

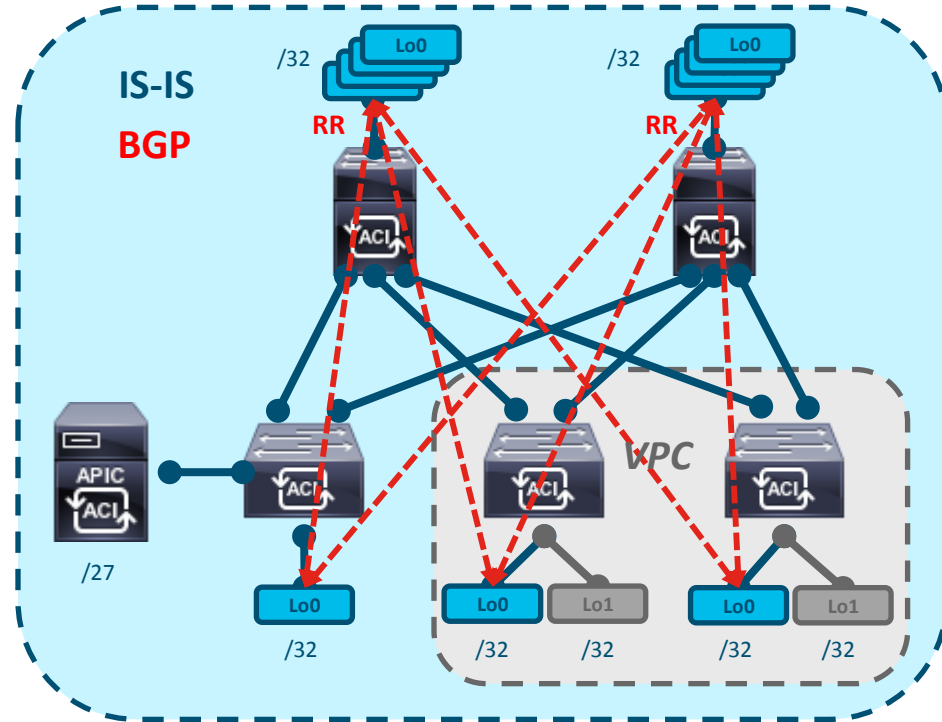


40/100G BiDi

Network Underlay

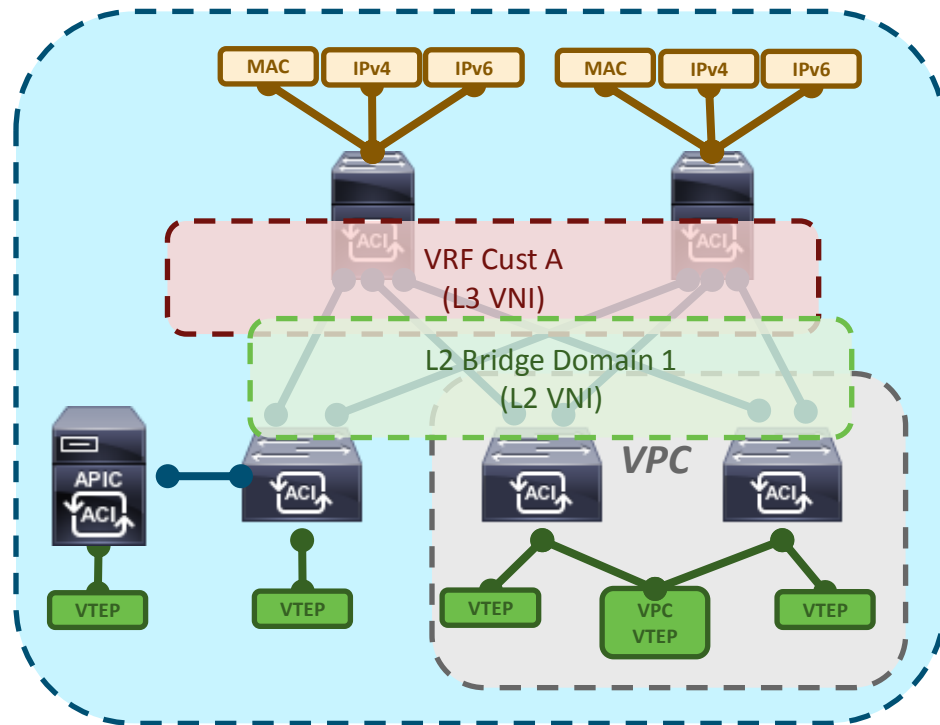
Routing between Leaf & Spines Switches

- Routed Interfaces between Leaf & Spines
 - APIC assigns IP Addresses Automatically
 - Jumbo+ MTUs (9366)
- vPC without Peer Link!
- Loopbacks (/32) for VTEP & BGP
 - VXLAN Tunnel Endpoint for Leaf and Spines
 - 2nd Anycast VTEP Loopback for vPC Switches
 - Spines have additional Anycast IP Proxy VTEP Loopbacks
- IS-IS and PIM are used as the routing protocol
- MP-BGP between leaf & selected spines
 - Spines as Route Reflectors



VXLAN with In-band Flow-level Metadata

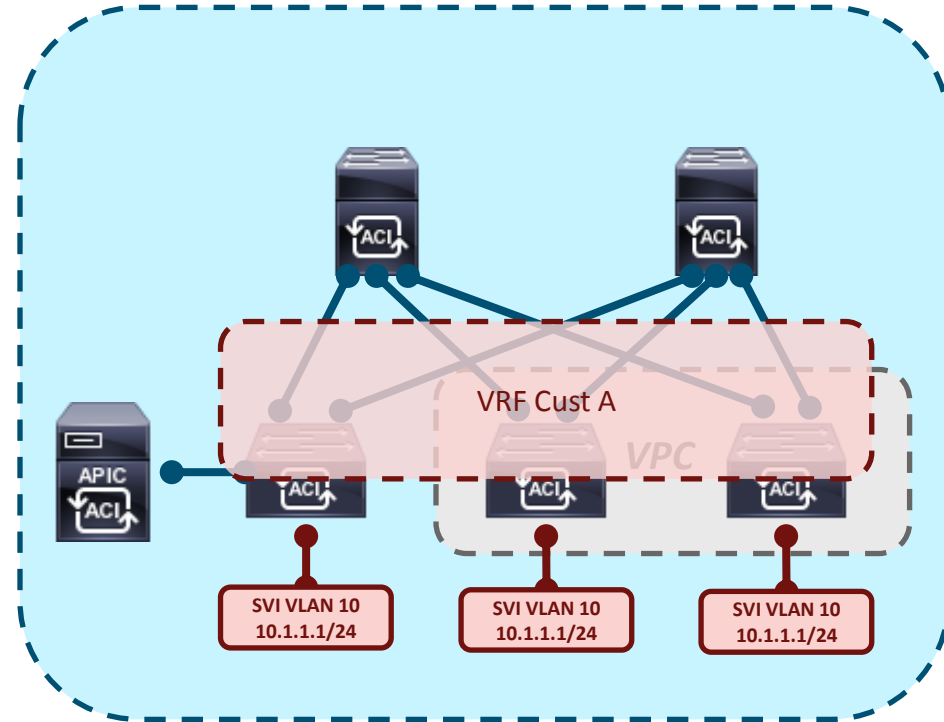
- VXLAN-GPE (Generic Protocol Extension)
 - Carries “Class ID” defining flows’ details
- VXLAN Virtual Network Identifiers
 - Separate VNIs for L2 & L3 traffic
- ALL external traffic carried in Overlay
 - Both Bridged & Routed Traffic in VXLAN VNI
 - Routed L3 Multicast supported!
- Mapping Database of IP/MAC to VTEP
 - Council of Oracles Protocol (COOP)
 - Spine know where ALL hosts are
 - Unknown destination traffic sent to Spine HW proxy VTEP (MAC, IPv4/v6)



Integrated VXLAN Overlay

Pervasive L3 Gateway at Top of Rack

- L3 SVI IP address created on each relevant ToR
 - No Endpoints on switch, no SVI
- Same IP address, Same MAC address
- If routed to GW MAC, ToR will answer and use local VRF's L3 route table
- No HSRP, No vPC Peer Gateway
- External routes learnt via MP-BGP



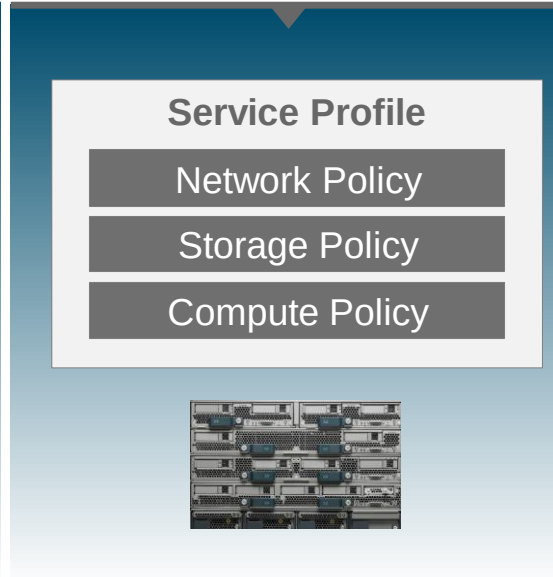
SIM Cards and Application Profiles

Logical Abstraction of Identity and Configuration

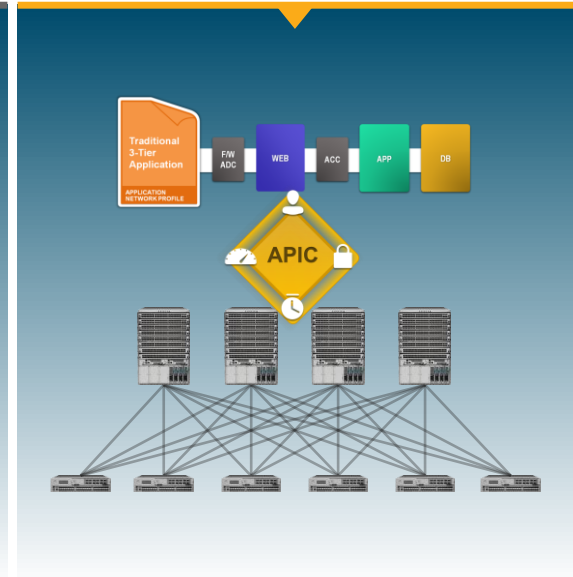
SIM Card Identity for a Phone



Service Profile Identity for Compute



Application Profile Identity for the Network



Fabric Access Policies

Interface Policies & Profiles

Link Level Policy - default

Properties

Name: default
Description: optional

Alias:

Auto Negotiation: off **on**

Speed: inherit

Link debounce interval (msec): 100

Forwarding Error Correction: CL74-FC-FEC CL91-RS-FEC disable-FEC **inherit**

LLDP Interface Policy - default

Properties

Name: default
Description: optional

Alias:

Receive State: Disabled **Enabled**

Transmit State: Disabled **Enabled**

Port Channel Policy - default

Properties

Name: default
Description: optional

Alias:

Mode: Static Channel - Mode On

Control: LACP Active **Static Channel - Static On** **Gracful Convergence**

LACP Passive

MAC Pinning

MAC Pinning-Physical-RIC-load

E1/1

E1/2

Link Level Policy

LLDP Policy

Port Channel Policy

Interface Policy Group

Name: ESXi Uplink Policy

Type: Virtual Port Channel

Policies:

Interface Group Profile

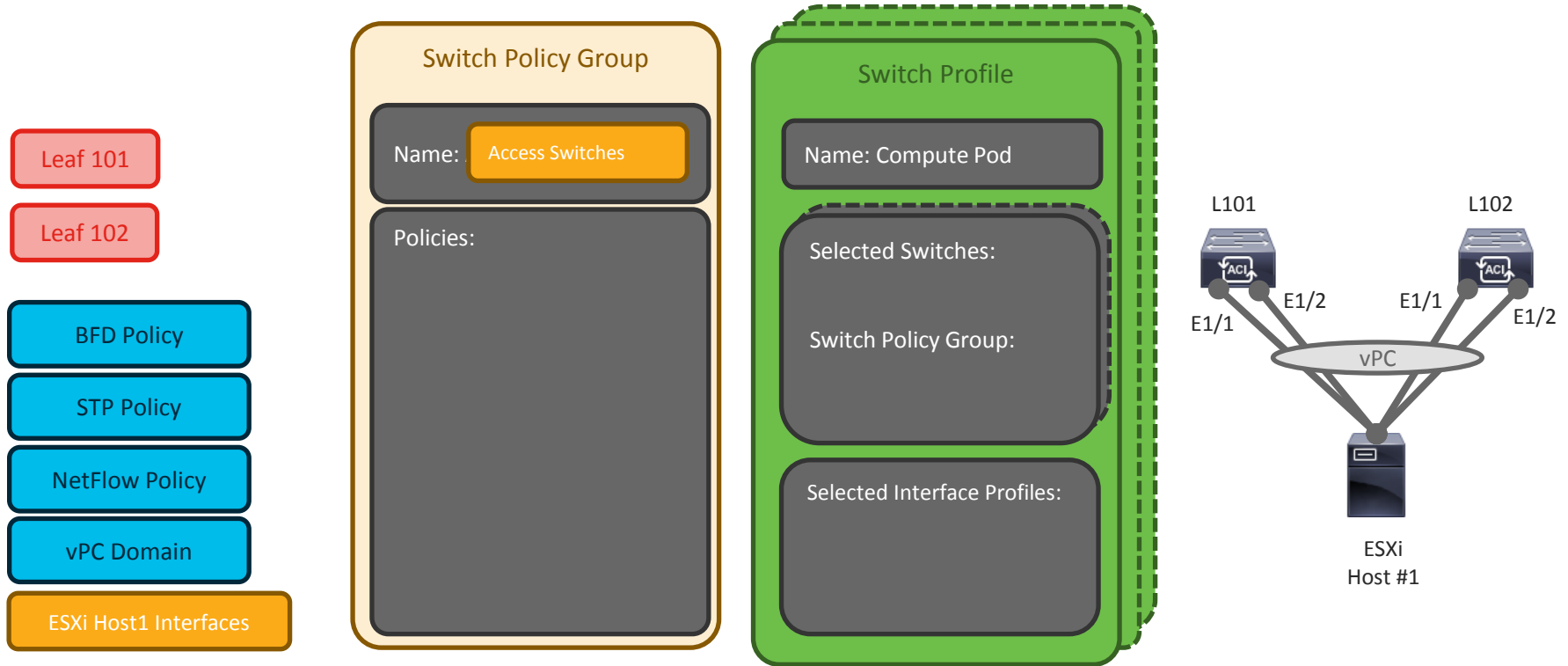
Name: ESXi Host1 Interfaces

Selected Interfaces:

Interface Policy Group:

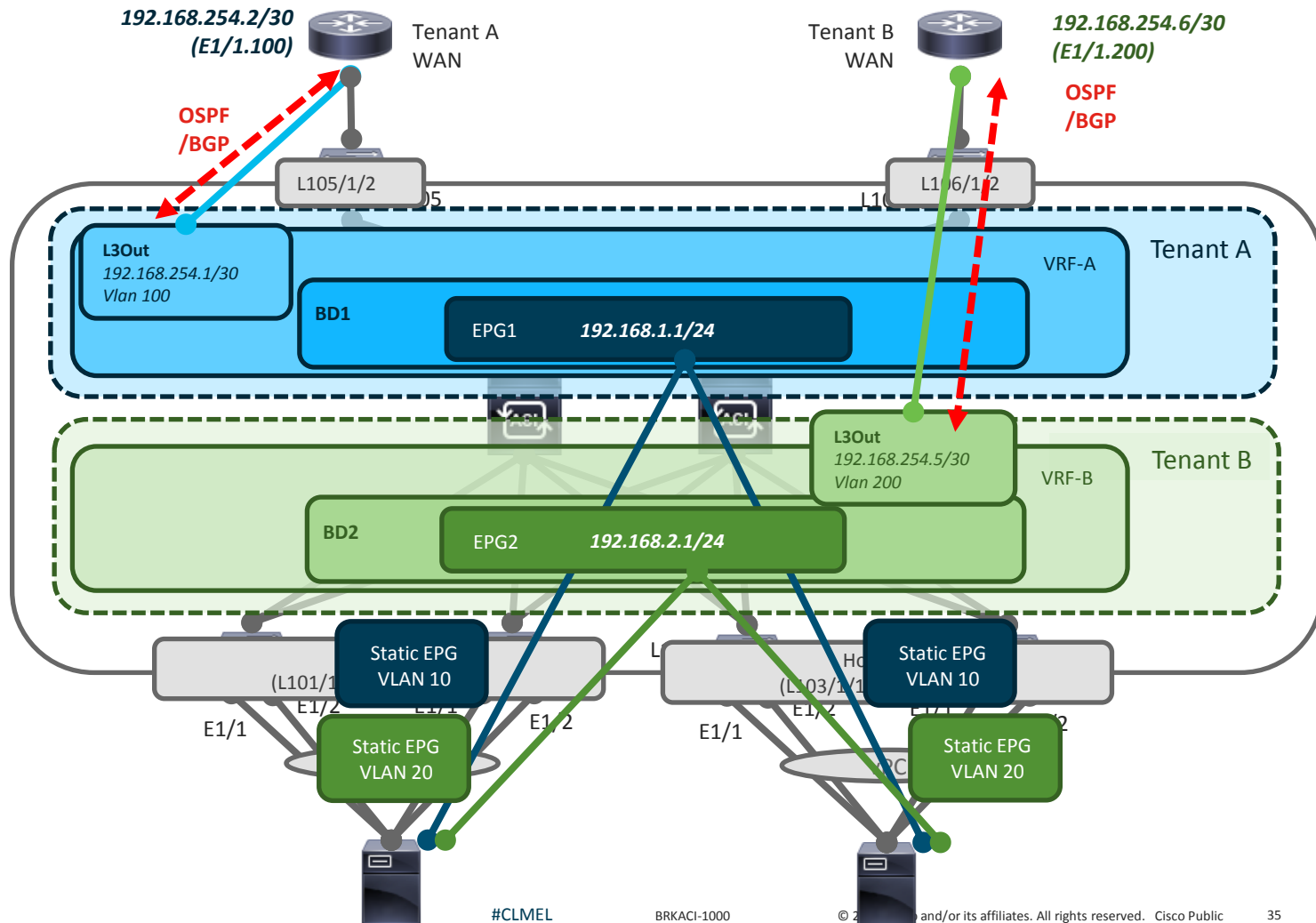
Fabric Access Policies

Switch Policies & Profiles



Tenant Policy Model

ACI FABRIC



End Point Groups

Collection of Servers that Provide or Consume a Common Service

Static EPGs

- Simple mapping of ingress VLAN ID to an EPG
- i.e. All MAC/IPs learnt on Port X join EPG A
- VLAN IDs can be different per switch or interface

Static EPG Members

Static Epg Members

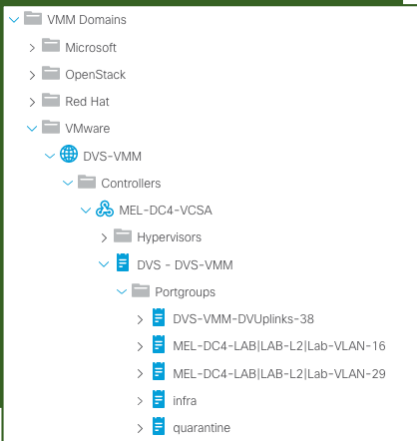
node-101-[eth1/17]-[vlan-102]

node-101-[eth1/18]-[vlan-102]

Dynamic EPGs

- Virtual Machine Manager (VMM) Domains
 - VMware, Hyper-V, RHEL, Kubernetes
- Mapping of vDS Port Group (VMware) to EPG
 - i.e. All MAC/IPs from VMs on PG X join EPG B
- ***ACI can automate creating dPG and assign dynamic VLAN from host(s) to ACI Leaf***
- Very simple to operate

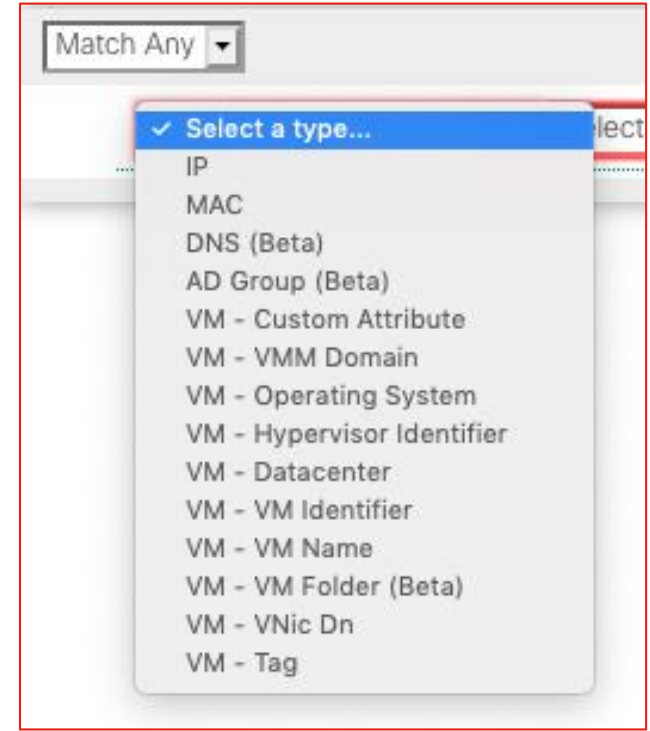
***EPGs are
fundamental to
ACI Security!***



End Point Groups – Micro-Segmentation

Micro-Segmentation EPGs

- Sub-IP Network or VLAN Segmentation
- Works across VM, Bare Metal, Containers, Cloud etc
- Use a combination of attributes to create micro-segmentation EPGs
 - IP/MAC
 - DNS
 - AD Group
 - VM Operating System
 - VM Custom Attributes
 - VM Tags



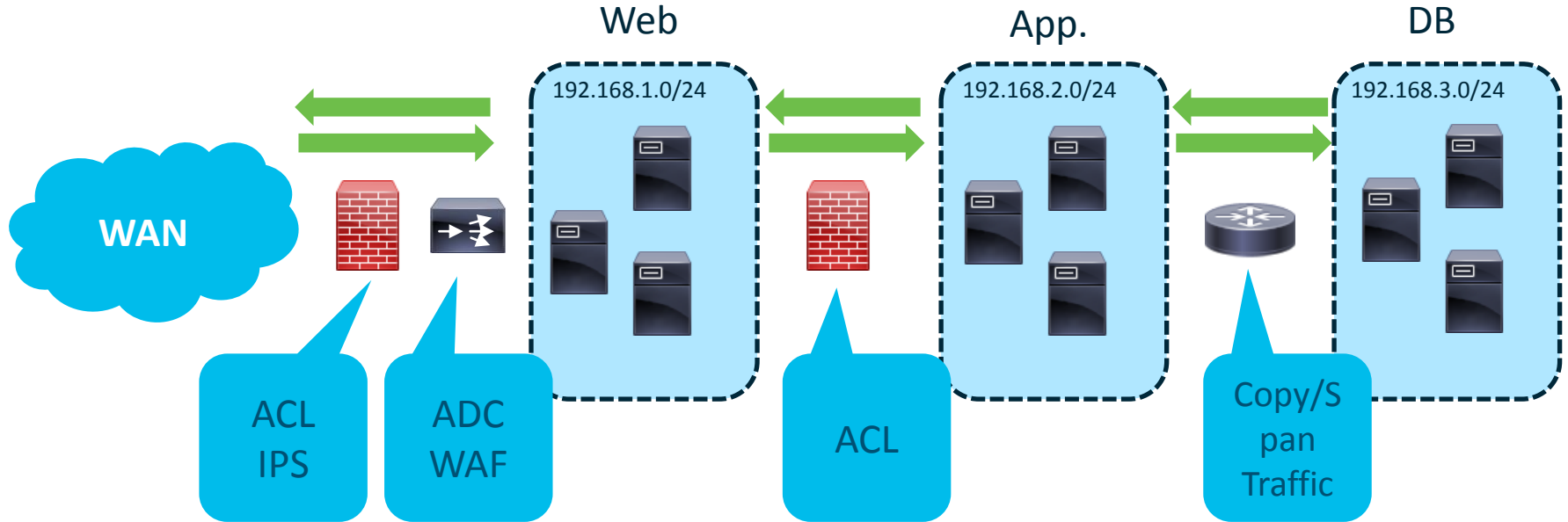
End Point Groups - External

- IP networks used to identify source and destination traffic flows
 - *outside the ACI fabric*
- Only have IP addresses to work with!
- Think of network objects used in an ACL
- Associated with an External (L3Out) Domain
- Not necessarily the same as a learnt dynamic or static route

External EPG Networks				
Name	QoS Class	Description	Target DSCP	Subnet
Corporate_LAN	Unspecified		Unspecified	10.0.0.0/8
Branch_Offices	Unspecified		Unspecified	192.168.0.0/16
Internet	Unspecified		Unspecified	0.0.0.0/0

Application Profiles (AP)

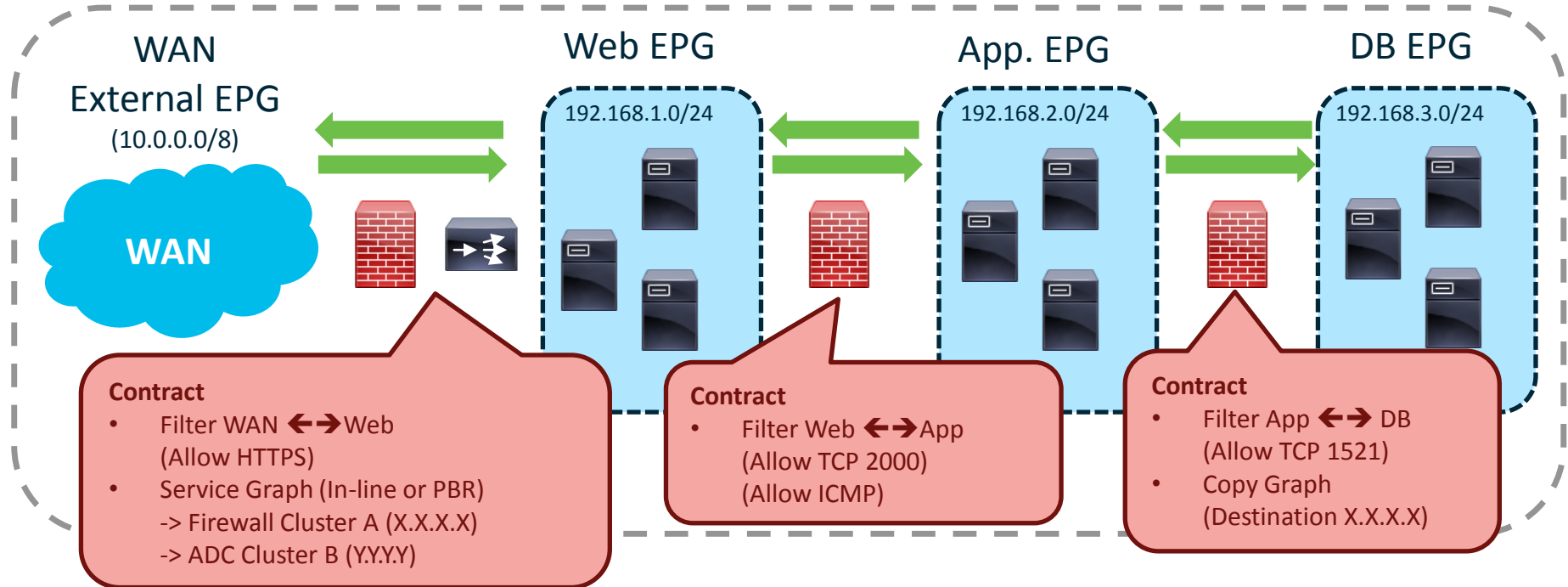
Typical 3-tier Application – Common Policies



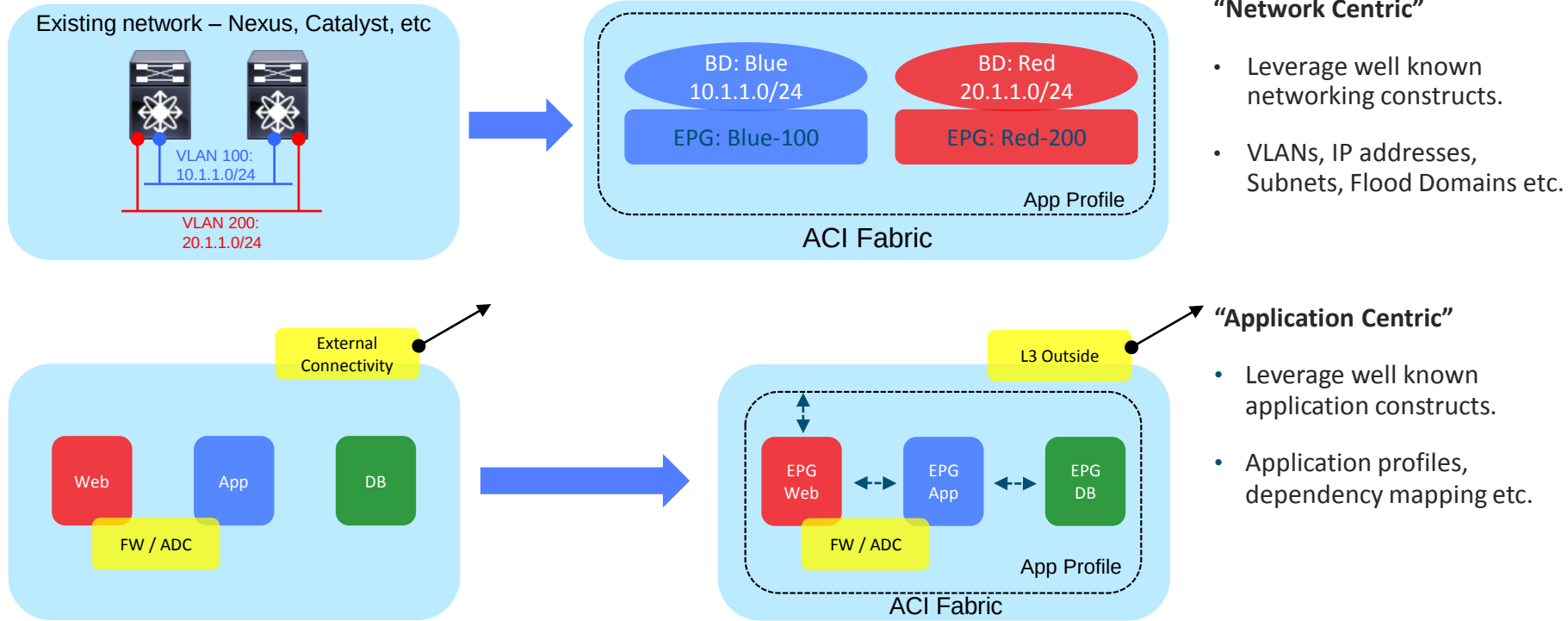
Application Profiles (AP)

Abstracted logical construct of an “Application” and associated policies

Application Profile



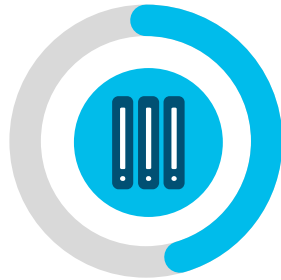
ACI Fabric – Two Deployment Models



You can mix both network centric and application centric -> typical customer transition path!

76% of the Security Team's Time is Spent on Security in the Data Centre

Percentage of Security Team's Time



47%

Servers



29%

Customer Data

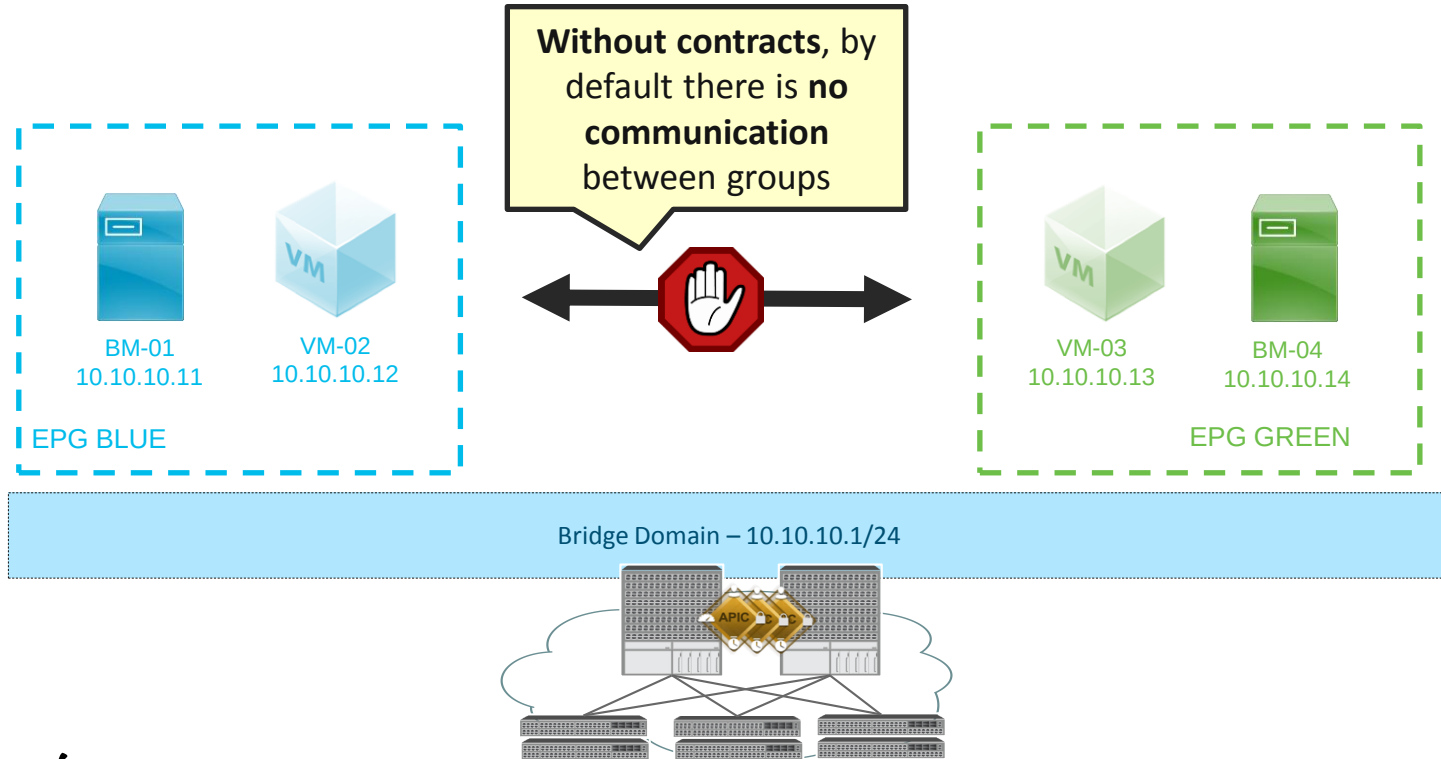


24%

Endpoints

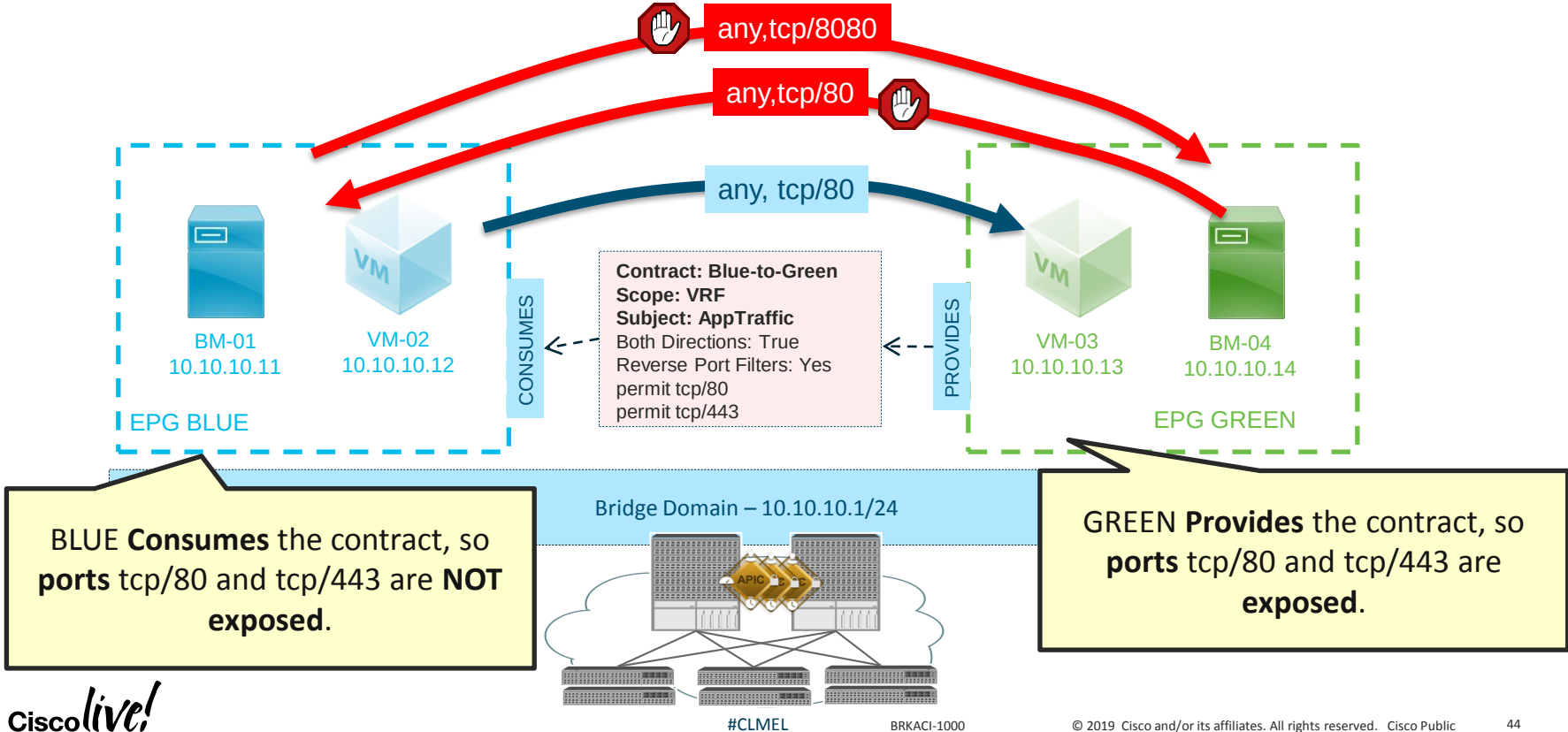
Zero-Trust Default Security

White List Model: No Contract, No Communication



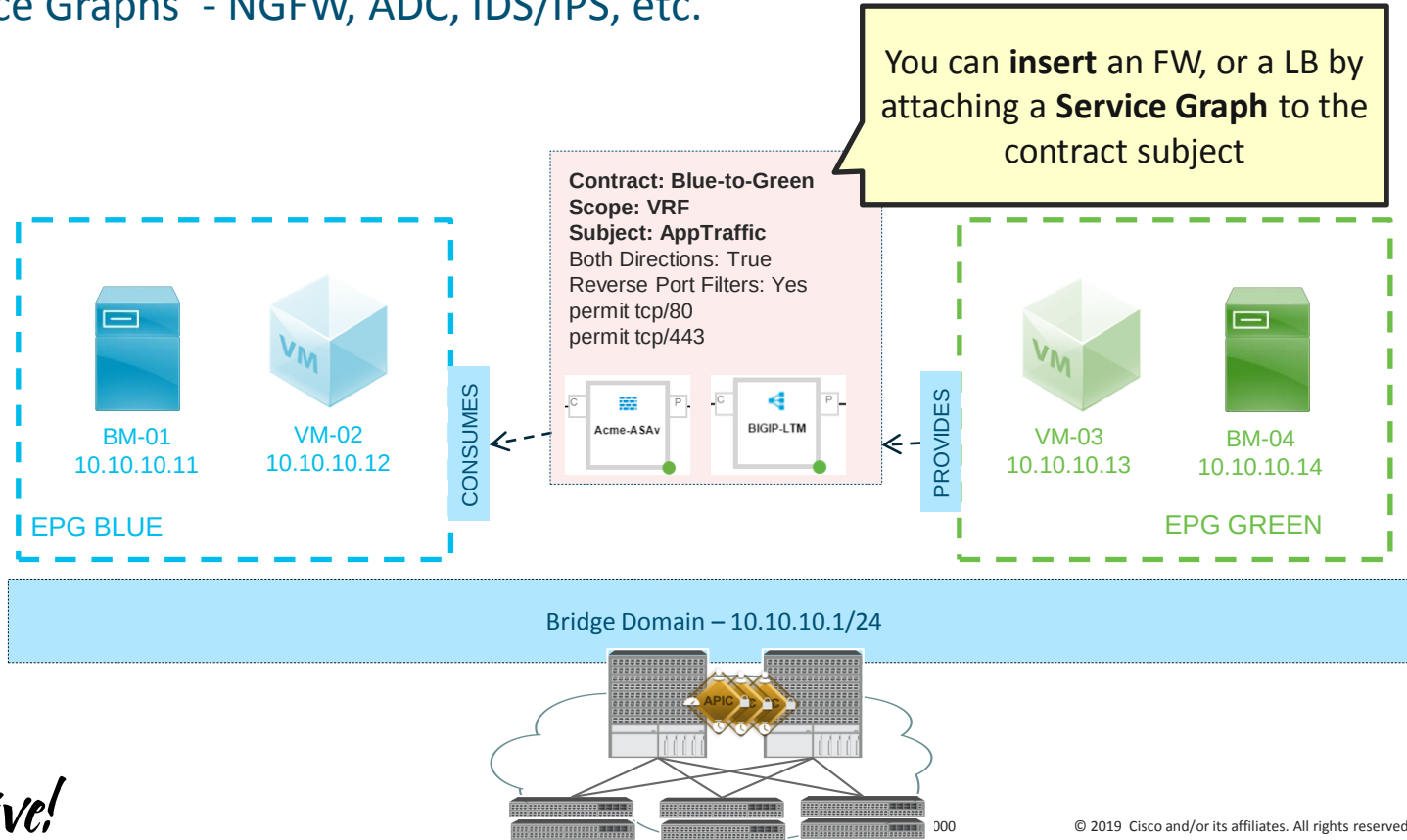
Contracts Enforce Communication Intent

White List Model: Contract Determines Communication



Contracts Redirect Traffic to L4-7 Services

Service Graphs - NGFW, ADC, IDS/IPS, etc.



Trusted External EPGs

- By default – have to manually create External EPGs
- Can use ISE (Identity Services Engine) to bridge common data between Enterprise and Data Centre
- Group information shared between ISE and APIC
 - Authenticated, trusted user groups dynamically synchronised to ACI
 - ACI sends dynamic EPG membership back to ISE as groups



For Policy Export go to [Administration > System > Backup & Restore >](#)

	 Add	 Import	 Export	 Delete	 Push
Icon	Name	SGT (Dec / Hex)			
☐	 Auditors	20/0014			
☐	 Billing_Systems	29/001D			
☐	 BYOD	15/000F			
☐	 Contractors	5/0005			
☐	 CUCM_Servers	6/0006			
☐	 Developers	8/0008			
☐	 Dev_Svs	12/000C			
☐	 Doctors	41/0029			
☐	 Edu_Adm	19/0013			
☐	 Edu_Portal	21/0015			
☐	 Employees	4/0004			
☐	 Environmental	31/001F			
☐	 Extranet_Partnet	16/0010			
☐	 Facilities	33/0021			
☐	 Faculty_Svr	24/0018			
☐	 Guests	9/0009			
☐	 Internet	40/0028			
☐	 IoT_Devices	42/002A			
☐	 IT	34/0022			
☐	 Med_Portal	26/001A			
☐	 Med_Techs	22/0016			



The screenshot displays the Cisco ISE (Identity Services Engine) web interface. The top navigation bar includes 'SYSTEM', 'TENANTS', and 'FABRIC'. Below this, a search bar is present with the text 'enter name'. The main content area is titled 'Tenants' and shows a hierarchical tree on the left. The tree is expanded to show 'L3_ROUTE_NEW' > 'L3_Route' > 'Logical Node Profiles' > 'Networks'. A list of 14 networks is shown, each with a plus icon and a name ending in 'SGT'. The right pane shows the 'Networks' configuration page with a 'NAME' field.

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Icon	Name	SGT (Dec / Hex)	Description
☐	 ACI_Development_Svr_EPG	10003/2713	Learned from APIC.
☐	 ACI_HIPAA_Svr_EPG	10004/2714	Learned from APIC.
☐	 ACI_Medical_Records_EPG	10005/2715	Learned from APIC.
☐	 ACI_PCI_Svr_EPG	10002/2712	Learned from APIC.
☐	 ACI_Production_Svr_EPG	10001/2711	Learned from APIC.

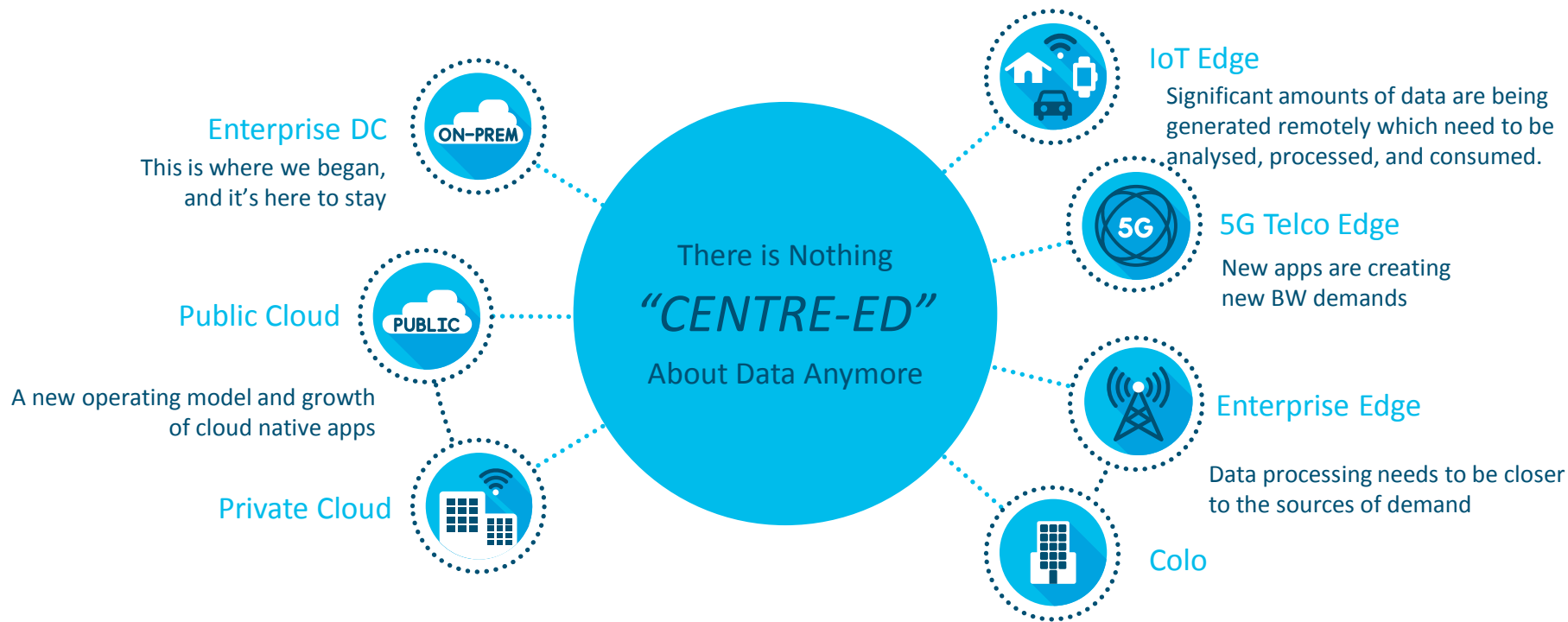


The screenshot shows the Cisco SD-WAN GUI interface. At the top, there is a navigation bar with the Cisco logo and two tabs: "System" and "Tenants". Below the navigation bar, there is a search bar with the text "ALL TENANTS | Add Tenant | Search: enter name, desc". The main content area is titled "Tenant pod41" and contains a tree view of configuration elements. The tree view shows the following structure:

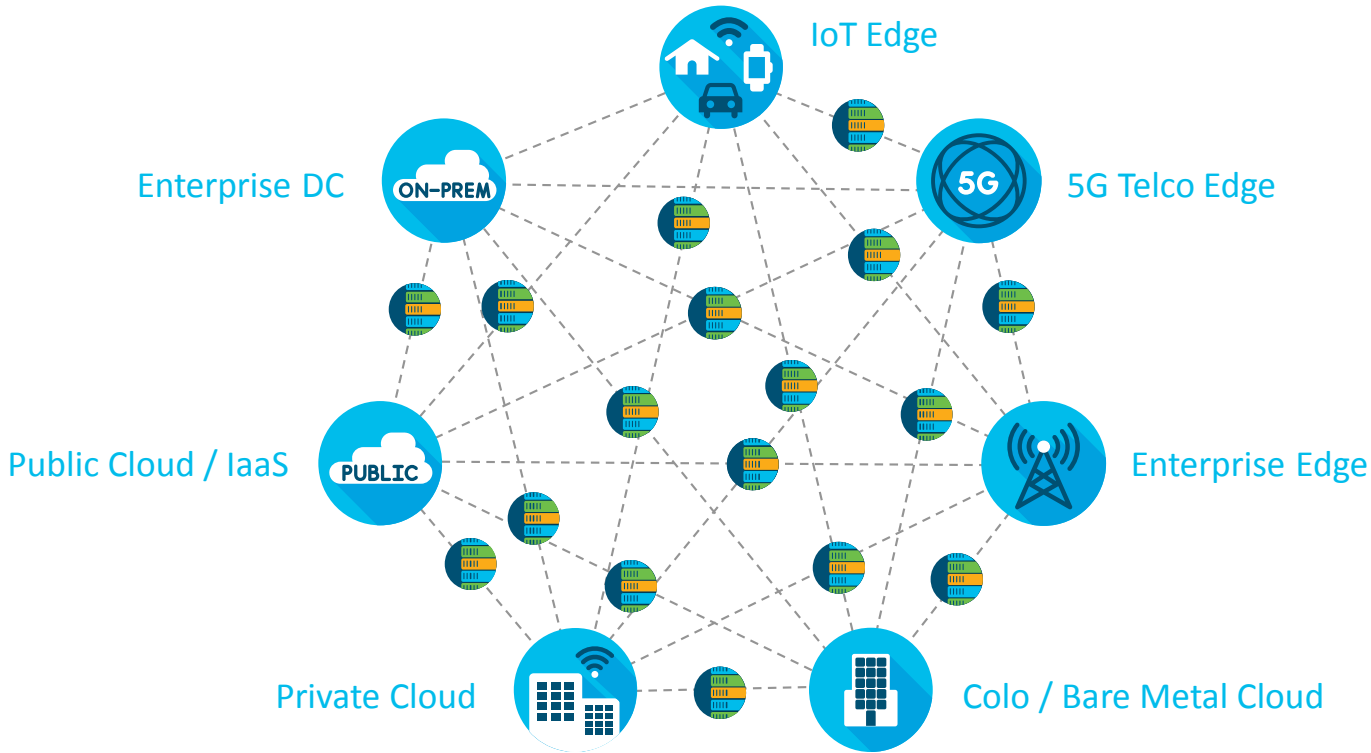
- Quick Start
- Tenant pod41
 - Application Profiles
 - ACI
 - Application EPGs
 - EPG Development_Svr
 - EPG HIPAA_Svr
 - EPG Medical_Records
 - EPG PCI_Svr
 - EPG Production_Svr

Agenda

- Introduction
- Evolution of Data Centre Networking & Management
- What is ACI?
- **ACI Anywhere**
- Making the most of ACI
- Where to go next



The DC Needs to go Anywhere the Data is

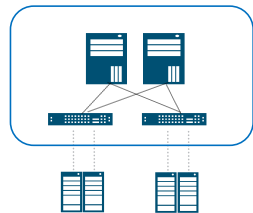


Cisco ACI Anywhere

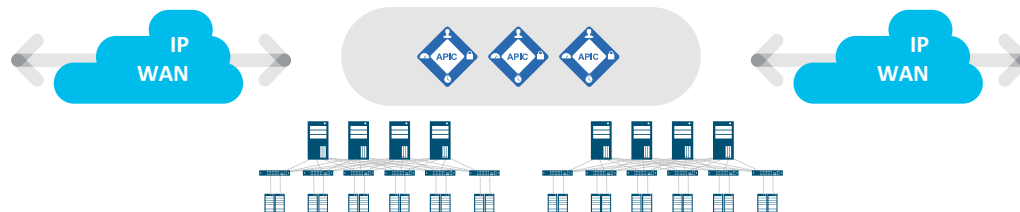
Any Workload, Any Location, Any Cloud

ACI Anywhere

Remote Leaf / Virtual ACI



Multi-Pod / Multi-Site ACI



Cloud ACI



Remote Location

On Premise

Public Cloud

Security Everywhere



Analytics Everywhere



Policy Everywhere



Cisco *live!*

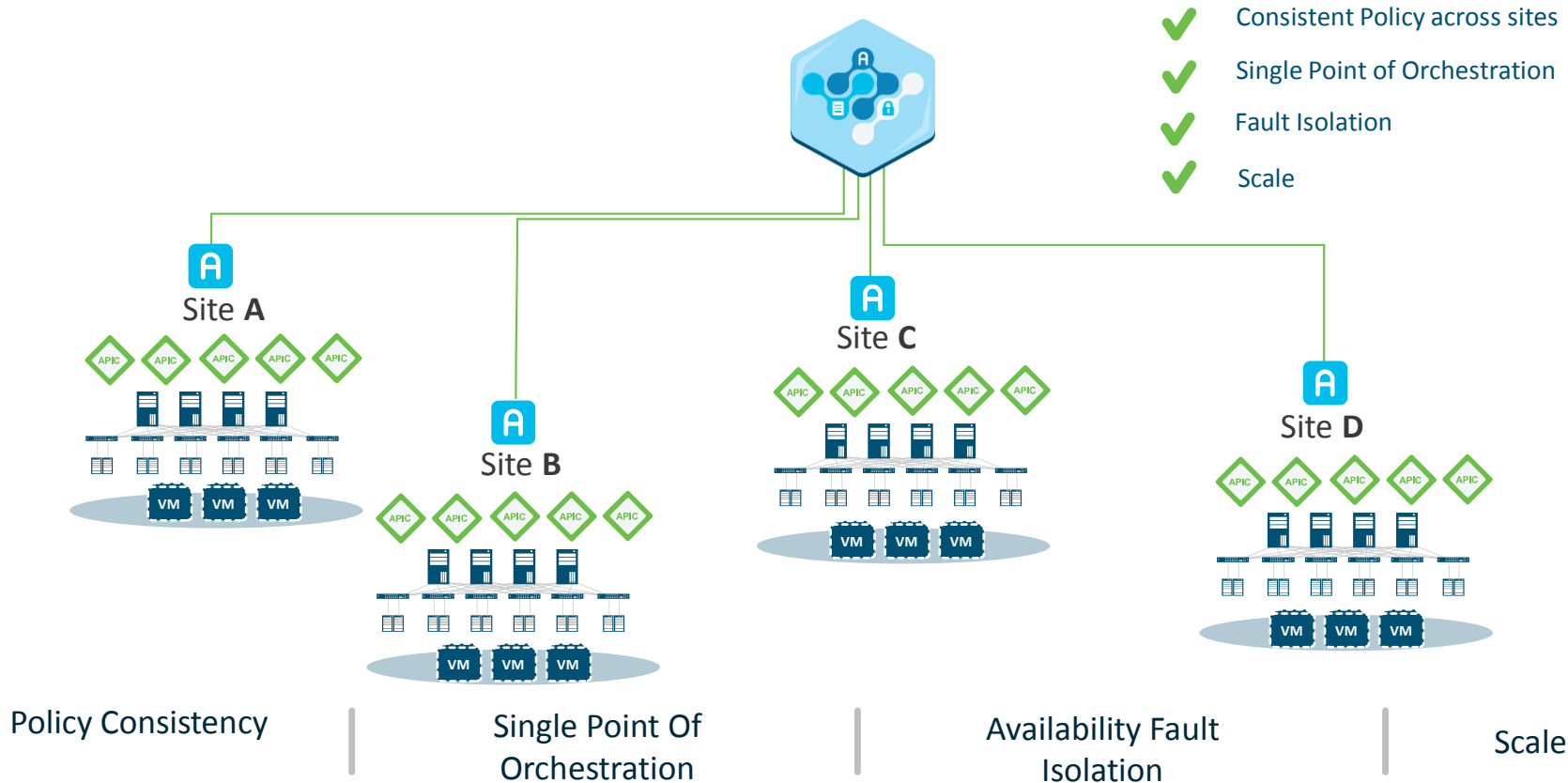


- 50ms Latency
- IP Multicast (PIM BiDir),
- OSPF,
- DHCP Relay

ACI Multi-Site

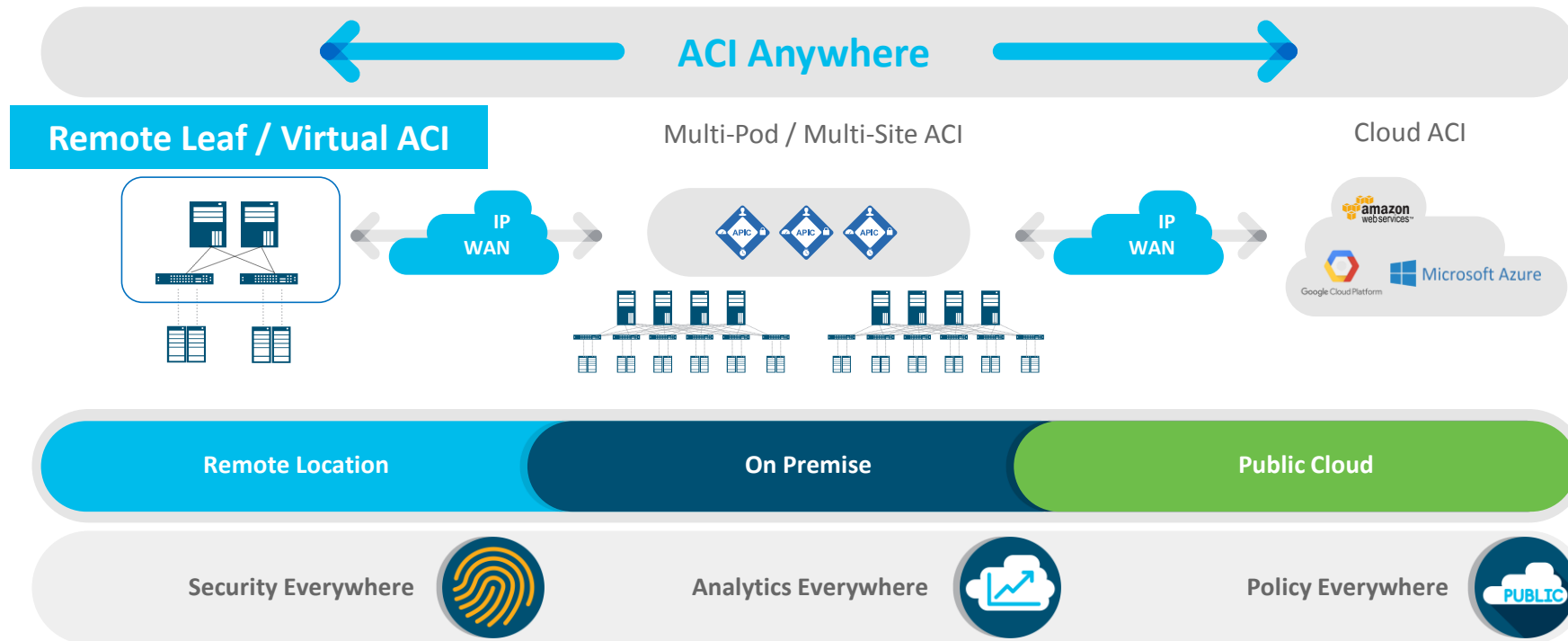
Shipping Since ACI 3.0

Multi-Site Orchestrator

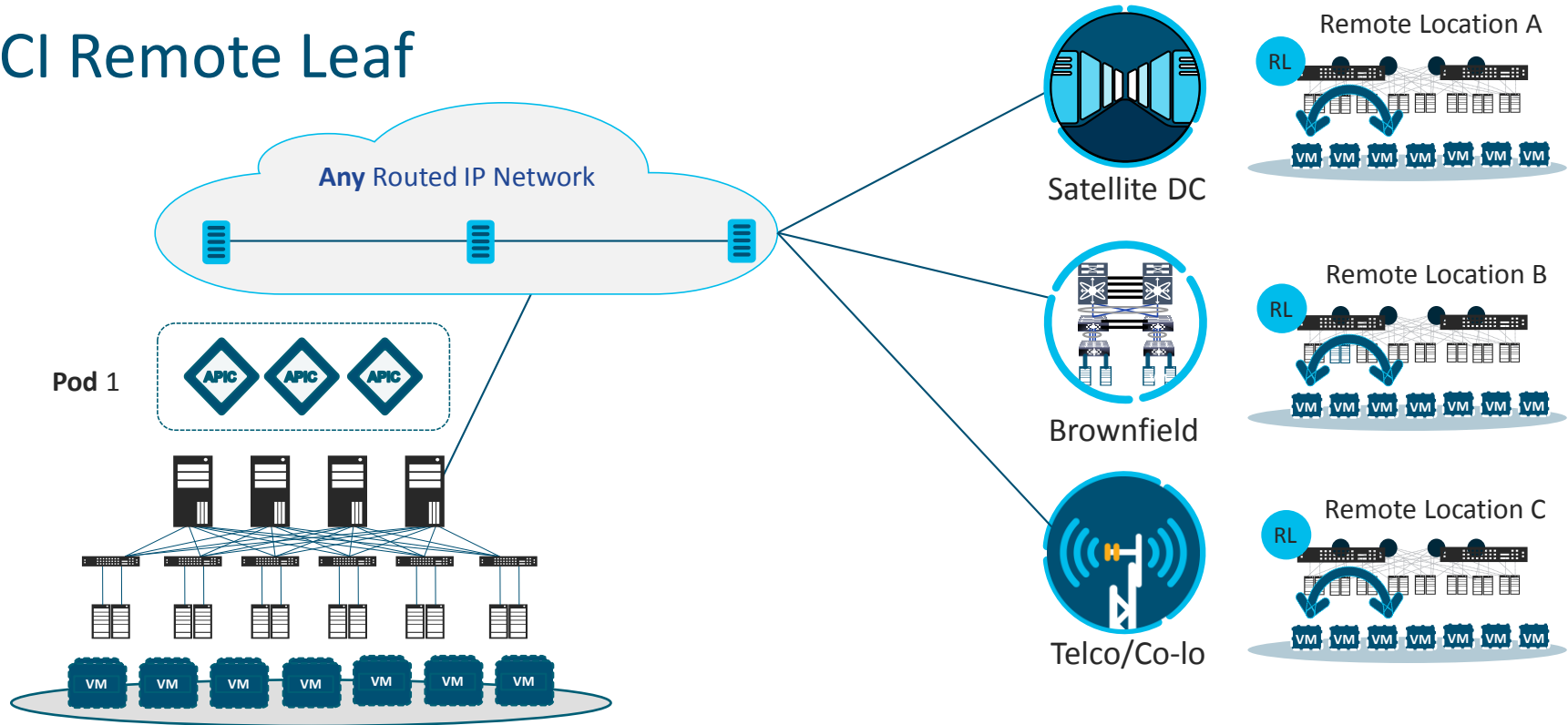


Cisco ACI Anywhere

Any Workload, Any Location, Any Cloud



ACI Remote Leaf



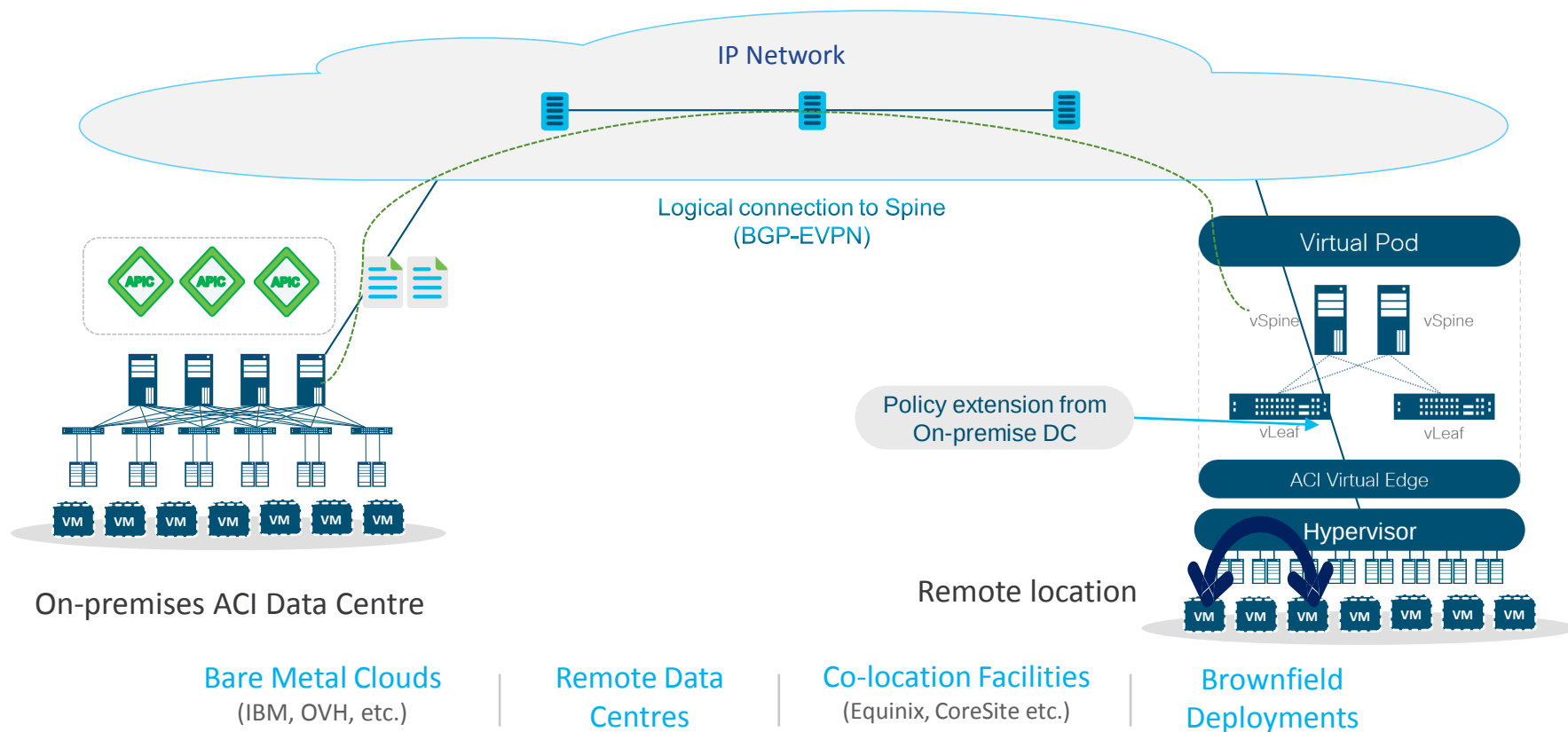
Zero Touch Auto Discovery of
Remote Leaf

≤ 300 ms RTT, 100M+ BW
Up to **20** Remote Locations

Single central management
Automated **L2 VXLAN extension**

Cisco Virtual ACI (Virtual Pod)

Extend ACI to Bare Metal Clouds and Remote Data Centres

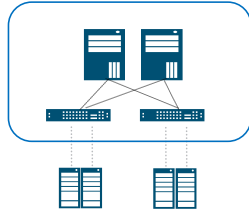


Cisco ACI Anywhere

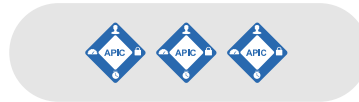
Any Workload, Any Location, Any Cloud

ACI Anywhere

Remote Leaf / Virtual ACI



Multi-Pod / Multi-Site ACI



Cloud ACI



Remote Location

On Premise

Public Cloud

Security Everywhere



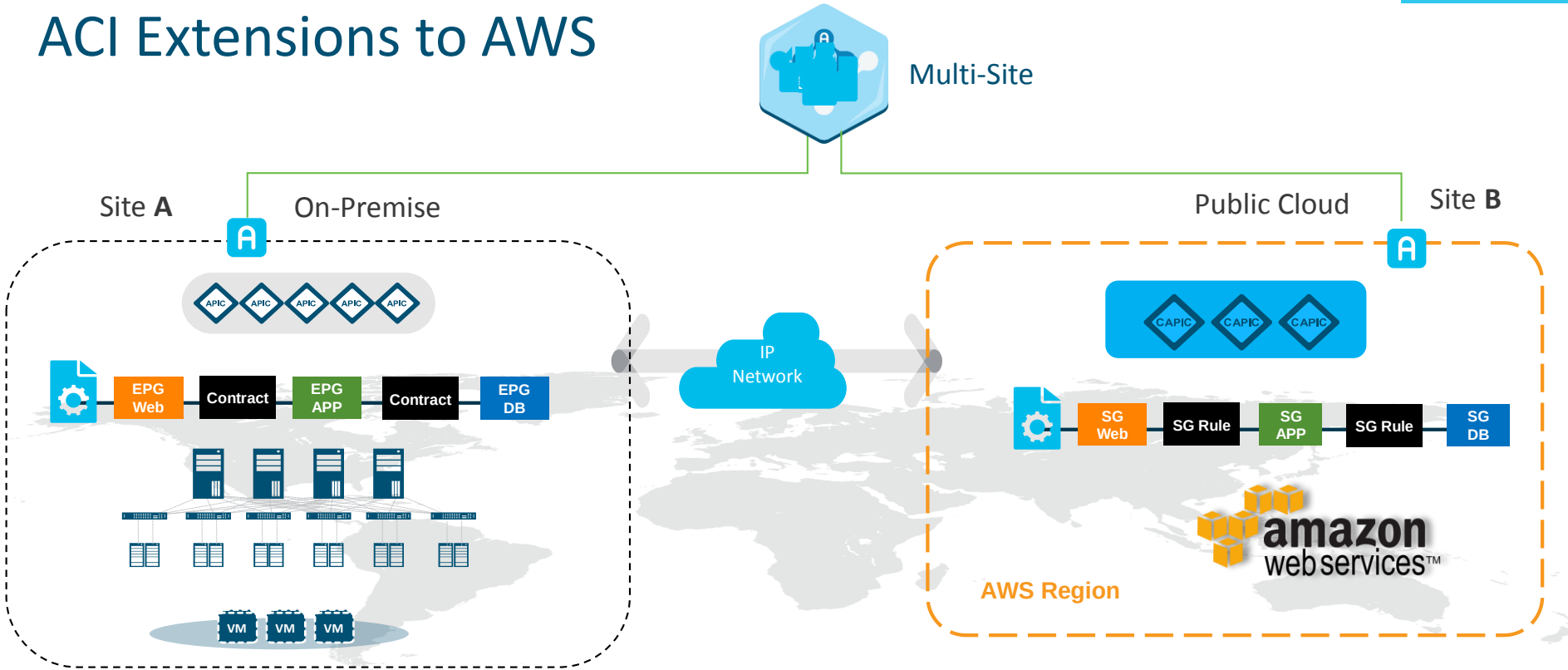
Analytics Everywhere



Policy Everywhere



ACI Extensions to AWS



Common
Governance

Discovery
& Visibility

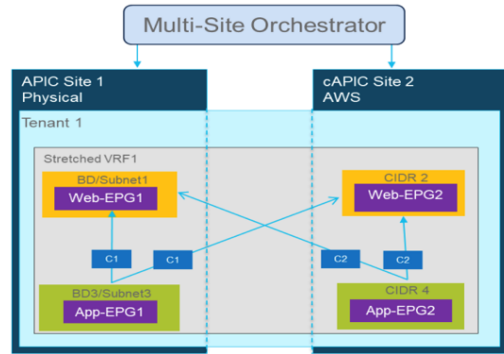
Policy
Translation

Monitoring &
Troubleshooting

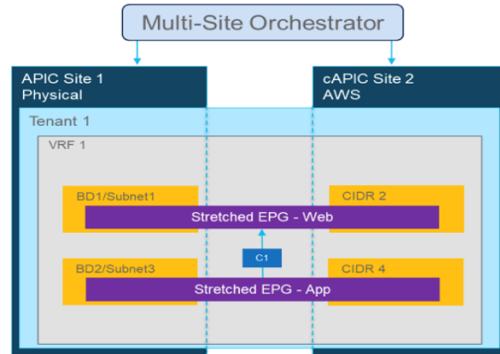
Single Point
Of Orchestration

Operational
Consistency

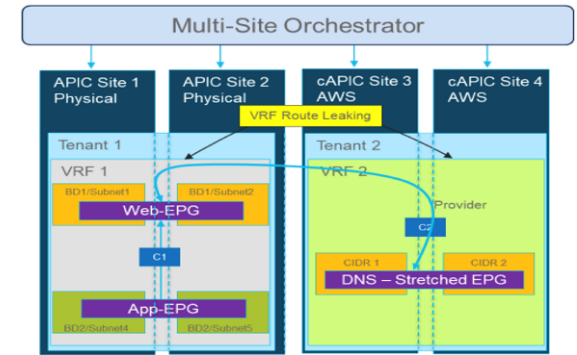
Example Use Cases



Tenant Stretching



Cloud Bursting



Shared Services

Note: Extending a L2 broadcast domain between on-premises and the cloud is not possible. Cloud vendors typically do not run broadcast or multicast and never face unknown unicast situations.

Agenda

- Introduction
- Evolution of Data Centre Networking & Management
- What is ACI?
- ACI Anywhere
- **Making the most of ACI**
- Where to go next

Furthering the reach with ACI integrations

Observability and Analysis



Automation



ADC



Container & VM Management



Public Cloud



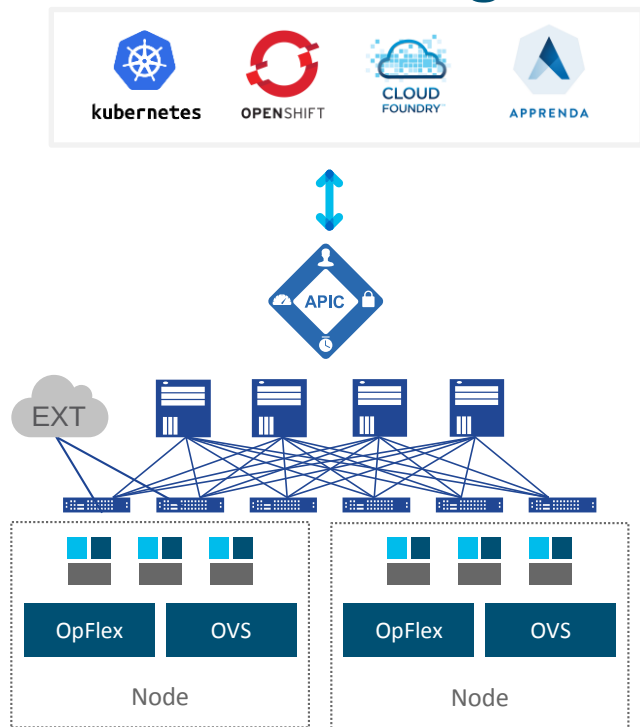
ITSM



Security



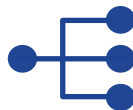
Cisco ACI Integration with Containers / PaaS



Key Benefits



Unified networking: Containers, VMs, and bare-metal



Micro-services load balancing integrated in fabric for HA / performance

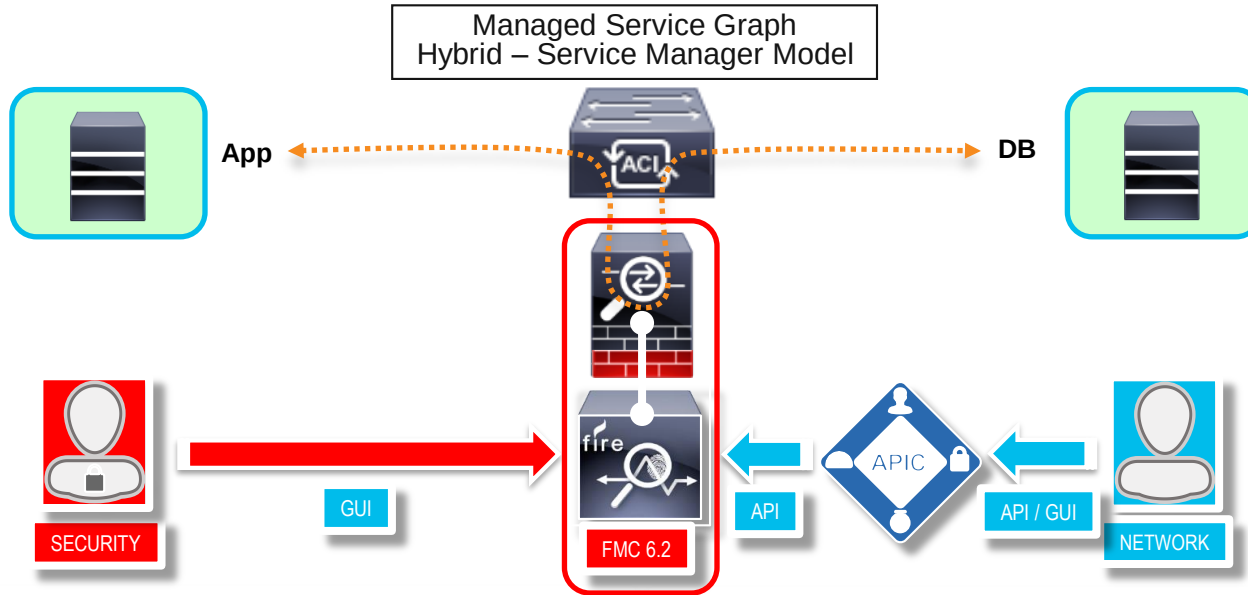


Secure multi-tenancy and seamless integration of Kubernetes network policies and ACI policies



Visibility: Live statistics in APIC per container and health metrics

Firepower (FTD) Integration with ACI



Security Admin

Pre-defines a security policy rule in FMC for use in the ACI fabric:

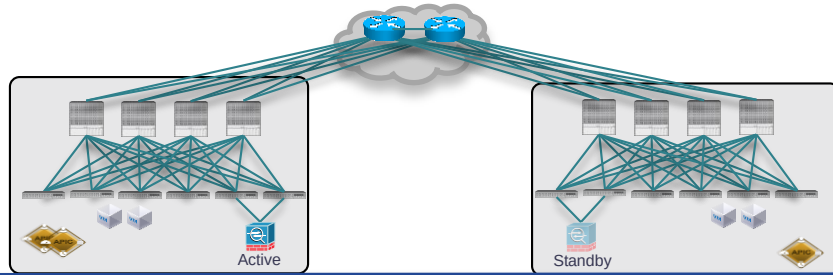
- ✓ Defines initial criteria for allowed Protocols and can update later
- ✓ Attaches appropriate threat policies (Malware, NGIPS)
- ✓ Adds URL Filtering, Geo-location, Threat Grid sandboxing, etc.
- Access Control Policy Rule is dedicated per service graph

Network Admin

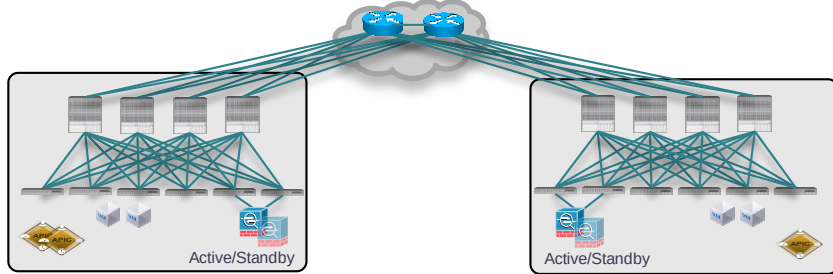
Uses APIC to attach FTD to ACI fabric and EPG traffic to a policy by:

- ✓ Creating Interfaces and matching VLANs for traffic to arrive to FTD
- ✓ Defining mode of operation: Routed, Transparent FW, NGIPS
- ✓ Creating Security Zones and attaching to pre-defined security policy
- FTD device package programs Fabric Insertion features from APIC

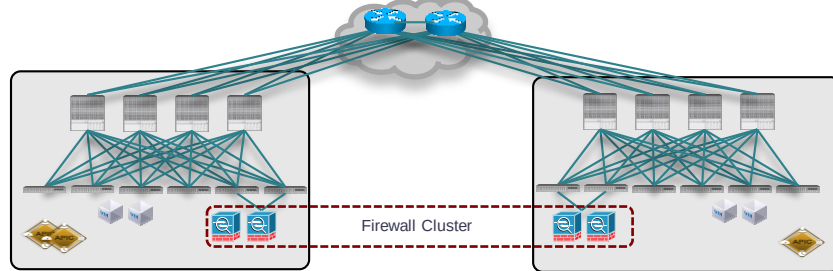
ACI Multi-Pod and Network Services



- Active and Standby pair deployed across Pods
- No issues with asymmetric flows but causes traffic hair-pinning across the IPN

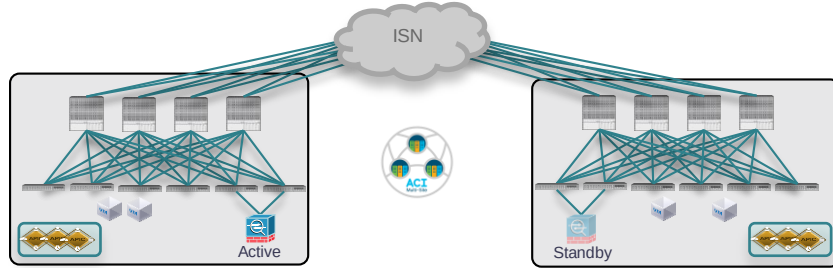


- Independent Active/Standby pair deployed in each Pod
- Only for perimeter FW use case assuming proper solution is adopted to keep symmetric ingress/egress traffic flows

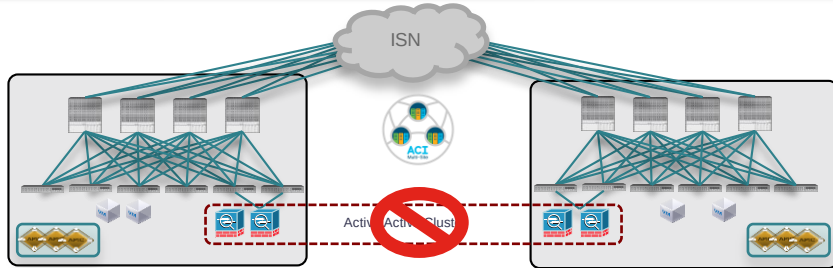


- FW cluster (ASA/FTD) deployed across Pods
- Supported from ACI 3.2
- Allows for stateful active/active DC failovers

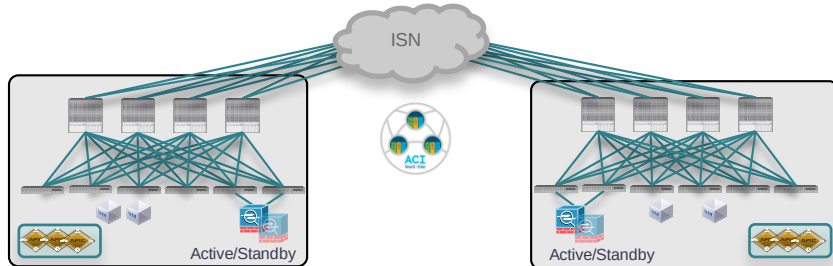
ACI Multi-Site and Network Services



- Active and Standby pair deployed across Pods
- Currently supported only if the FW is in L2 mode or in L3 mode but acting as default gateway for the endpoints
- Useful for Active/Standby DC Scenarios



- Active/Active FW cluster deployed across Sites
- **Not currently supported – Probably a bad idea anyway!**



- Most common deployment model for ACI Multi-Site
- Independent L4-7 services per DC, Better fault separation

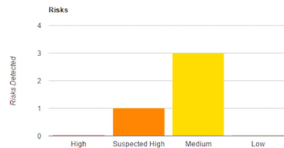
ACI App Centre (<https://aciappcenter.cisco.com>)

Programmable Infrastructure: Open APIs for Value Added Applications

AlgoSec

Security Rating: 77

PCI Compliance Score: 60



Get Your Fabric A Score On Security And Compliance.

Path Analysis

Connectivity and Compliance

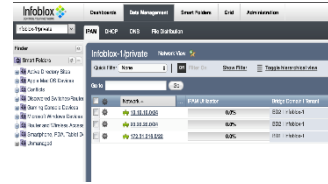
Splunk



Gain real time visibility centrally across your ACI deployments

Splunk Connector for Centralised Monitoring

Infoblox



Sync Configuration Between ACI & Infoblox Appliance

Simplify IP Address Management

ServiceNow



Push ACI Logical Topology Constructs To Service Now

Automated Service Management

ECOSYSTEM

Cisco *live!*

splunk>

puppet labs

servicenow

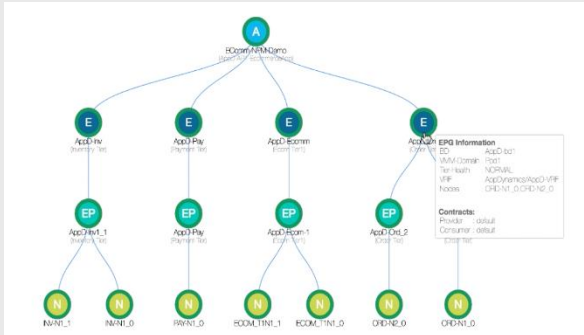
Infoblox

Sample Apps

Cisco ACI and AppDynamics (AppIQ)

Enhanced Visibility & Monitoring

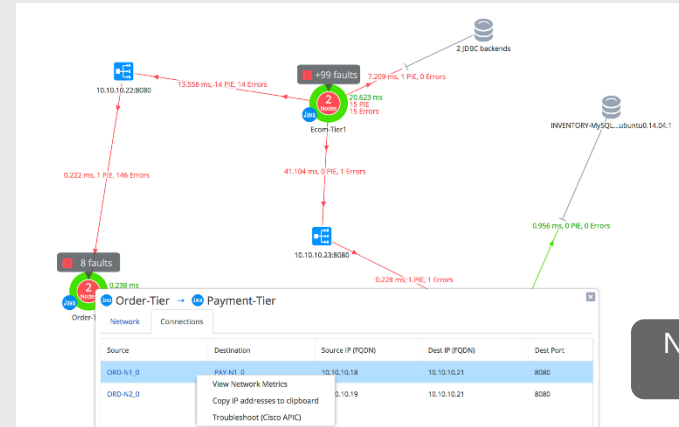
- Automated correlation of application services with ACI constructs
- Contextual overlay of services rendered by the application, business transactions, health and metrics on ACI constructs
- Augmented Application Flow Map on objects in ACI



App on ACI
App Center

Troubleshooting

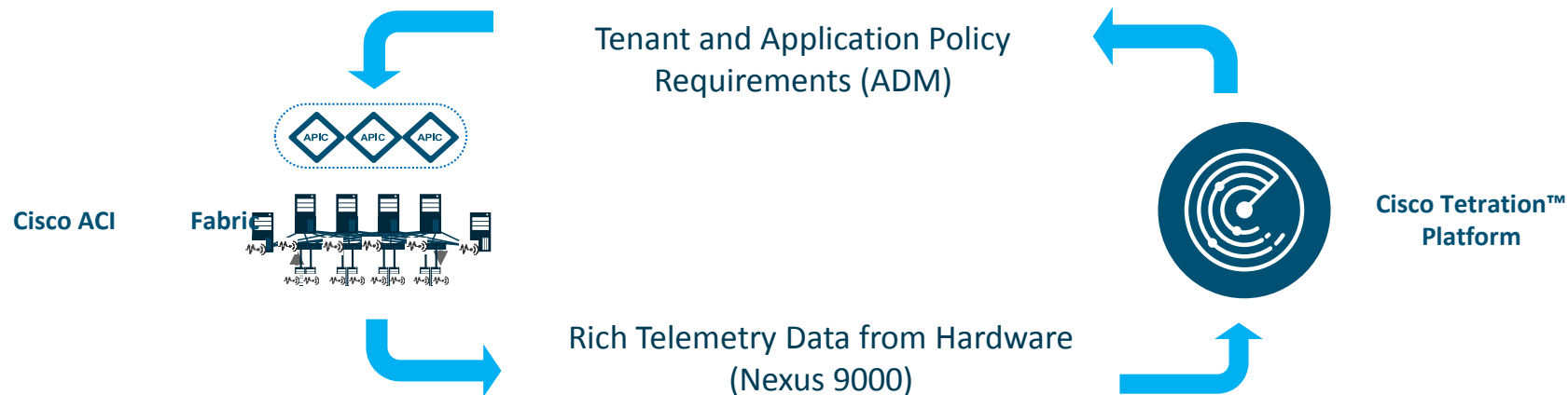
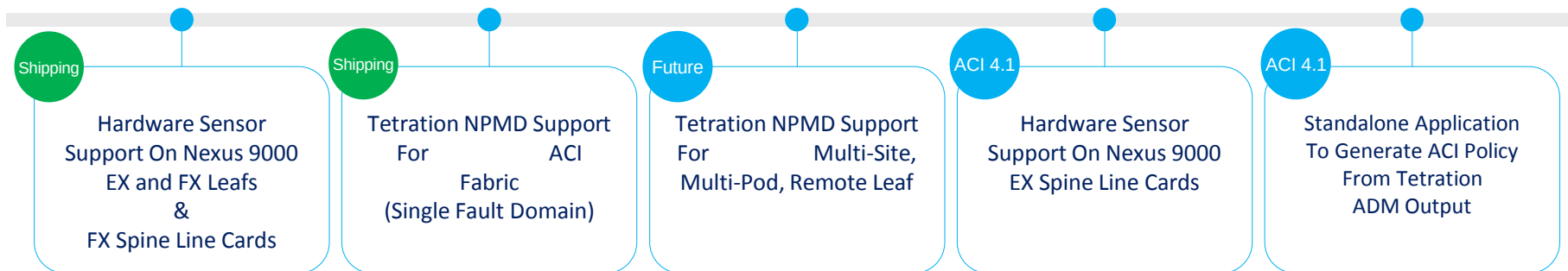
- Faster MTTR with context aware cross launch and report generation from Appdynamics to APIC
- ACI fault and health aware creation of Application Baseline on Appdynamics



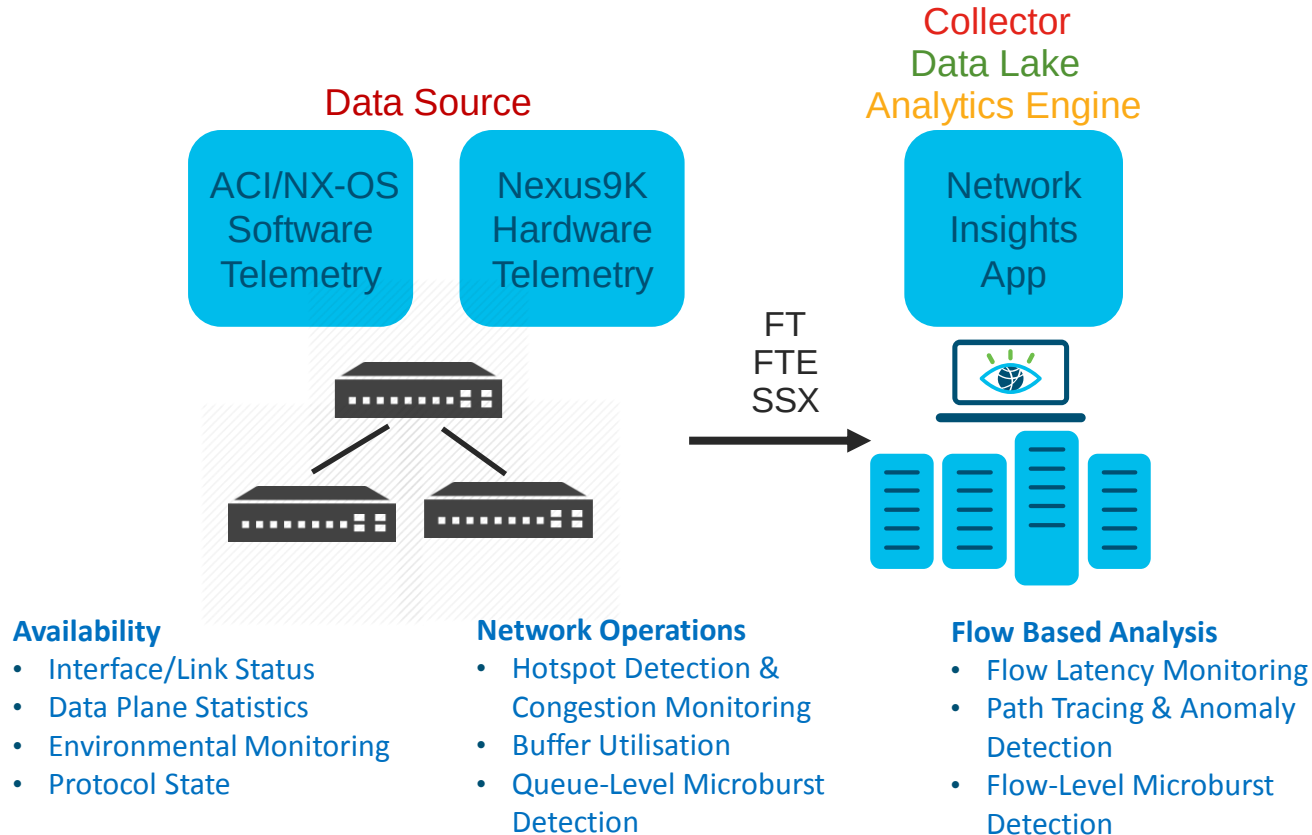
Native support
in AppD

ACI: Tetration Integration

Capture Intent & Translate To ACI Policy



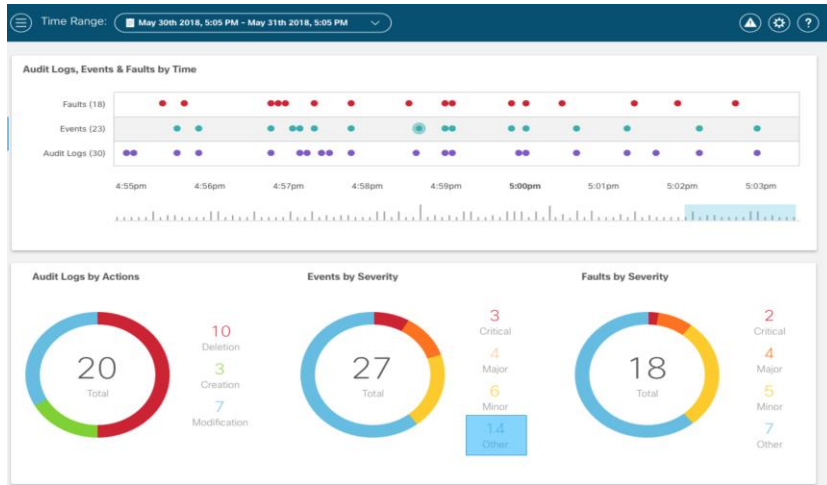
ACI: Telemetry with Network Insights App



ACI: Network Insights - Resources

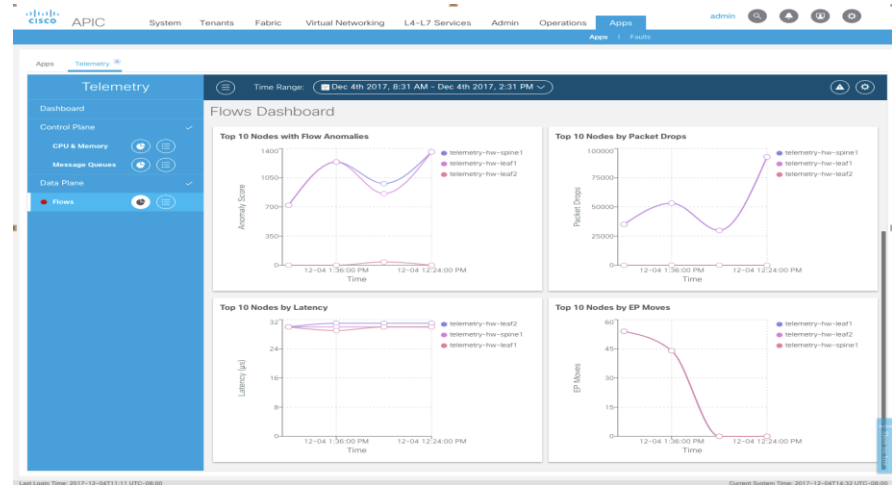
Understand What's Running In Your Network

Event Analytics Dashboard



Displays Faults, Events, And Audit Logs In A Time Series Fashion.

Flow Analytics Dashboard



Displays Key Indicators Of Infrastructure Data Plane Health In A Time Series Fashion.

ACI: Network Insights - Advisor

Analyse and Advise

- Advisories**

- Software/Hardware Recommendations

- Notices**

- EOL/EOS Field Notices

- Anomalies**

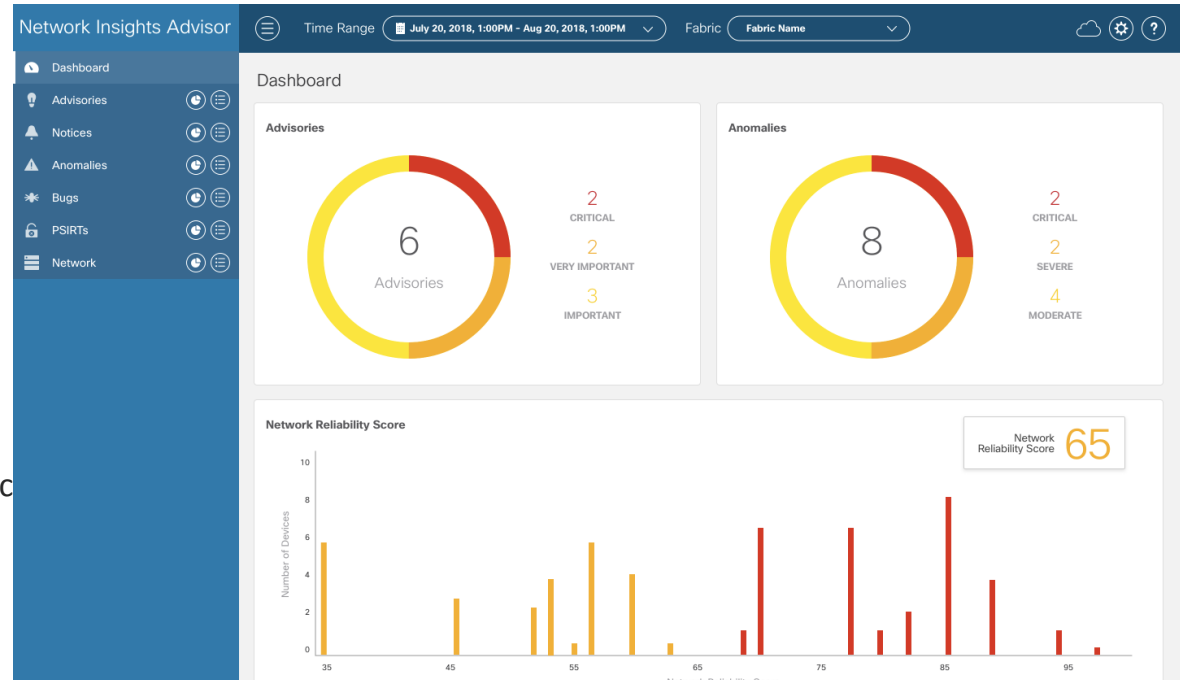
- Known Bugs/PSIRTs
- Config anomalies

- Compliance**

- Version Scale Limits/Hardening Checks

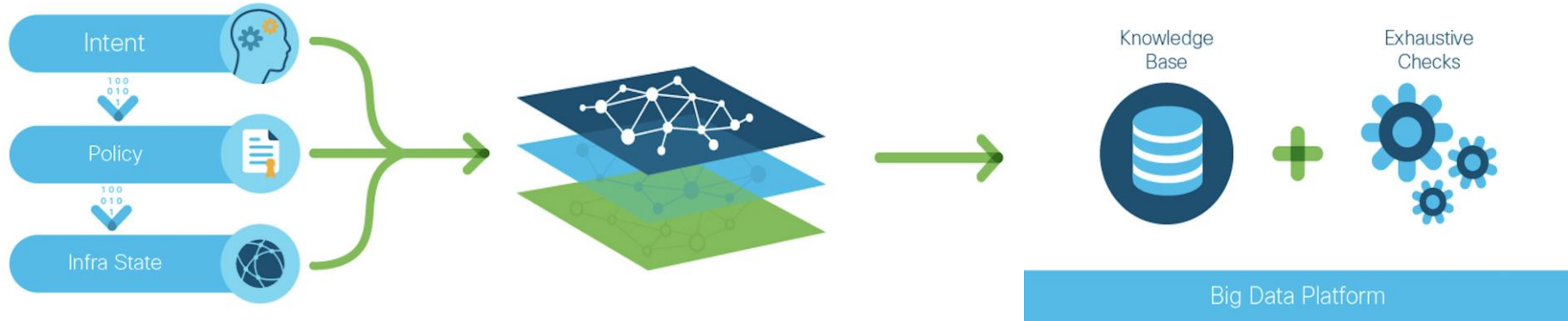
- Diagnostics**

- Forwarding State Check
- Loops Detection



Cisco Network Assurance Engine

Proactive Assurance



Data Collection

Capture DC Wide Intent, Policy, Control/State across Forwarding & Security

Formal Modeling of Network

Precise Mathematical Models that codify Cisco's 30+ Years of Networking and Cross Customer Domain Knowledge

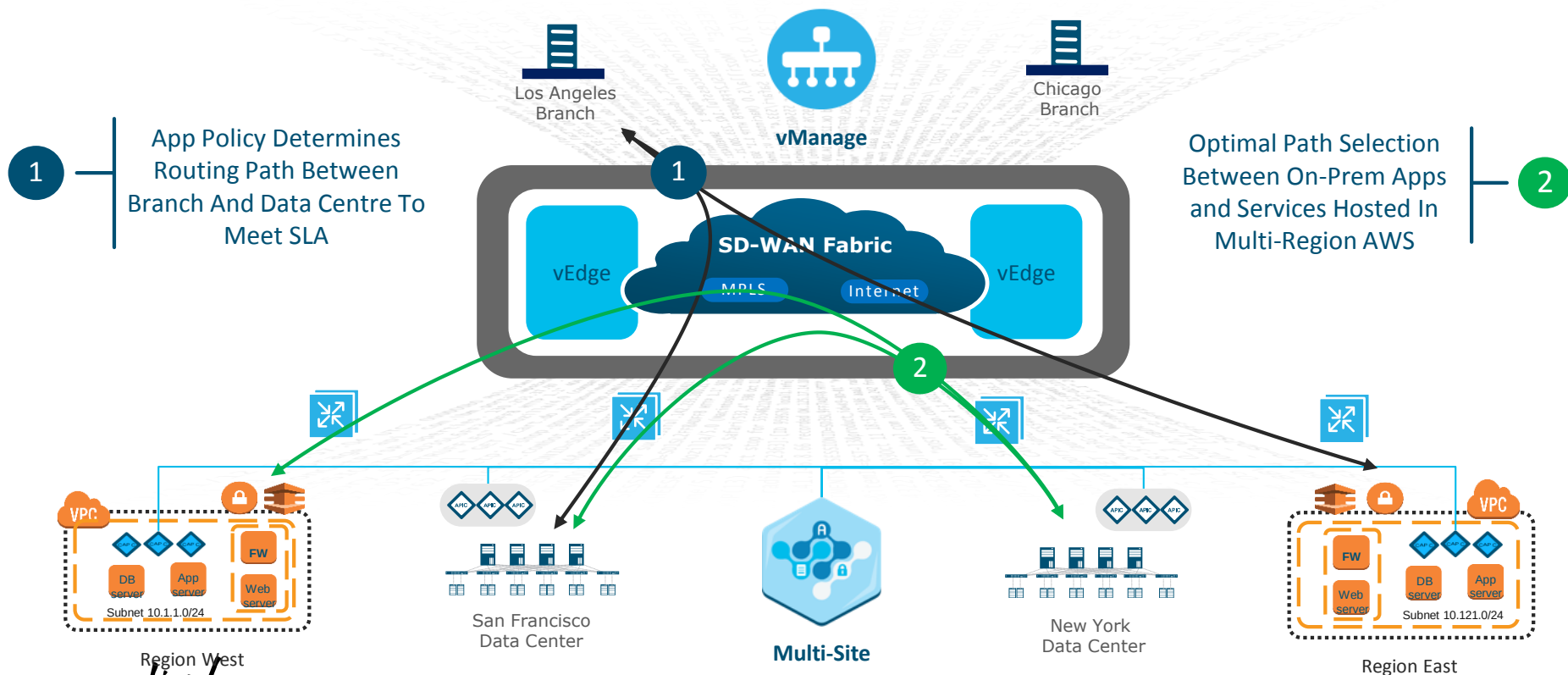
Continuous Analysis

Models verify that **Network operates per Intent** and accurately tell what is wrong, where, why, impact and how to fix

Reasoning you do after the fact, the Engine does before the fact, continuously, network wide

ACI: SD WAN (Viptela) Integration

Extend Operational Domain And Policy To Branch & Public Cloud



Automation Beyond the Fabric

- Comprehensive APIC REST API and Python SDK
 - Exposes the logical, abstracted, tenant policy model
- Integrate ACI with 3rd party automation tools
 - Ansible, Chef, Puppet etc.
- Private Cloud Automation Plugins
 - vRealise, AzurePack, OpenStack, UCS Director



Agenda

- Introduction
- Evolution of Data Centre Networking & Management
- What is ACI?
- ACI Anywhere
- Making the most of ACI
- **Where to go next**

Cisco Intent-Based Networking



Software-Defined **Campus**
Access (SDA)
Catalyst 9000



ACI
The network
made **simple**

Software-Defined
Data Centre Networking (SDN)
Nexus 9000



viptela



Software-Defined
WAN (SD-WAN)

ACI – Leading Intent-Based DC Networking



Improving Agility, Better Automation

Better Orchestration, Integration with DC Infrastructure

Maintaining Uptime In Data Centre Networks

“The percentage of manual data centre networking operational activities will fall below 50% by 2021, down from 80% today”

Gartner Magic Quadrant 2018

Gartner Magic Quadrant - 2018

Ciscolive!

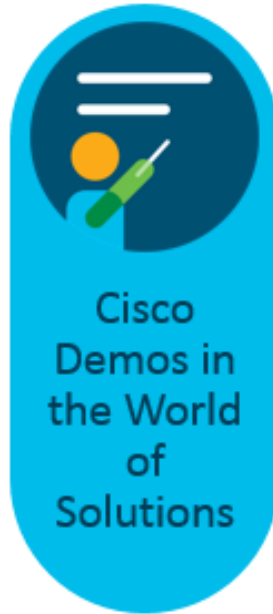
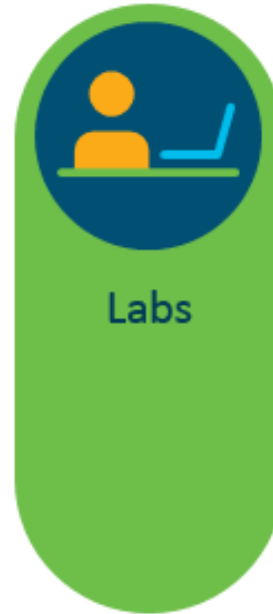
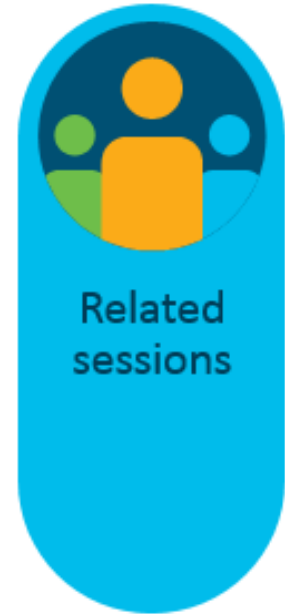


Q & A



INTUITIVE

Continue your education



Like to learn more?

Session ID	Title	Day	Time
BRKACI-1001	Your First 7 Days of ACI	Tuesday	2:15PM
BRKACI-2001	Integration and Interoperation of Existing Nexus Networks into an ACI Architecture	Wednesday	8:30AM
BRKACI-2004	How to Setup an ACI Fabric from Scratch	Wednesday	12:50PM
BRKACI-2102	ACI Troubleshooting	Wednesday	2:30PM
BRKACI-3128	Extending Your Data Centre Policies into the Cloud with Cisco ACI Anywhere	Thursday	8:30AM
BRKACI-3545	Mastering ACI Forwarding Behaviour – A Day in the Life of a Packet	Thursday	12:50PM
BRKACI-2506	How to Easily Integrate Security/L4-L7 Services into ACI	Thursday	2:30PM
BRKACI-2505	Deploying Kubernetes in the Enterprise with Cisco ACI	Thursday	4:30PM
BRKACI-2125	ACI Multi-Site Architecture and Deployment	Friday	8:00AM
BRKACI-2770	Automating ACI	Friday	9:40AM

Like to learn more?

Session ID	Title	Day	Time
TECACI-2540	How to manage and build your DC Fabric DevOps style (4 Hours)	Tuesday	9:00AM
TECACI-1132	Migrating Your Network Centric ACI Deployment to Application Centric (4 Hours)	Tuesday	2:00PM

Session ID	Session Title	Day	Start	End
DEVNET-2000	Network Programmability with Cisco ACI	Wednesday	12:00PM	12:45PM
DEVWKS-2001	Mastering ACI Programmability and Automating Common DC Tasks	Thursday	1:00PM	1:45PM

Complete Your Online Session Evaluation

- Give us your feedback and receive a complimentary **Cisco Live 2019 Power Bank** after completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Melbourne Mobile App.
- Don't forget: Cisco Live sessions will be available for viewing on demand after the event at:

<https://ciscolive.cisco.com/on-demand-library/>





Thank you



#CLMEL



INTUITIVE



INTUITIVE