Cisco ACI – Basics and Updates

Market Momentum Continues

6,000+
Nexus 9K and ACI Customers Globally

1400+
ACI Customers

50
Ecosystem Partners

NEW Infoblox · VERITAS · n3n · tufin · vARMOUR **ECOSYSTEM**

NetQoS · ca technologies · AVI Networks · CFEngine · Panduit · intel Security · splunk> · radware · NIKSUN · Check Point Software Technologies Ltd. · cloudstack

Microsoft · redhat · IBM · NUTANIX · NETSCOUT · MAPR · A10 Networks · FORTINET · cloudera · puppet labs · One Convergence

VCE · f5 · NetApp · Symantec · bmc · ScienceLogic · EMC² · EMULEX · SOURCEfire · CANONICAL · DATATORRENT

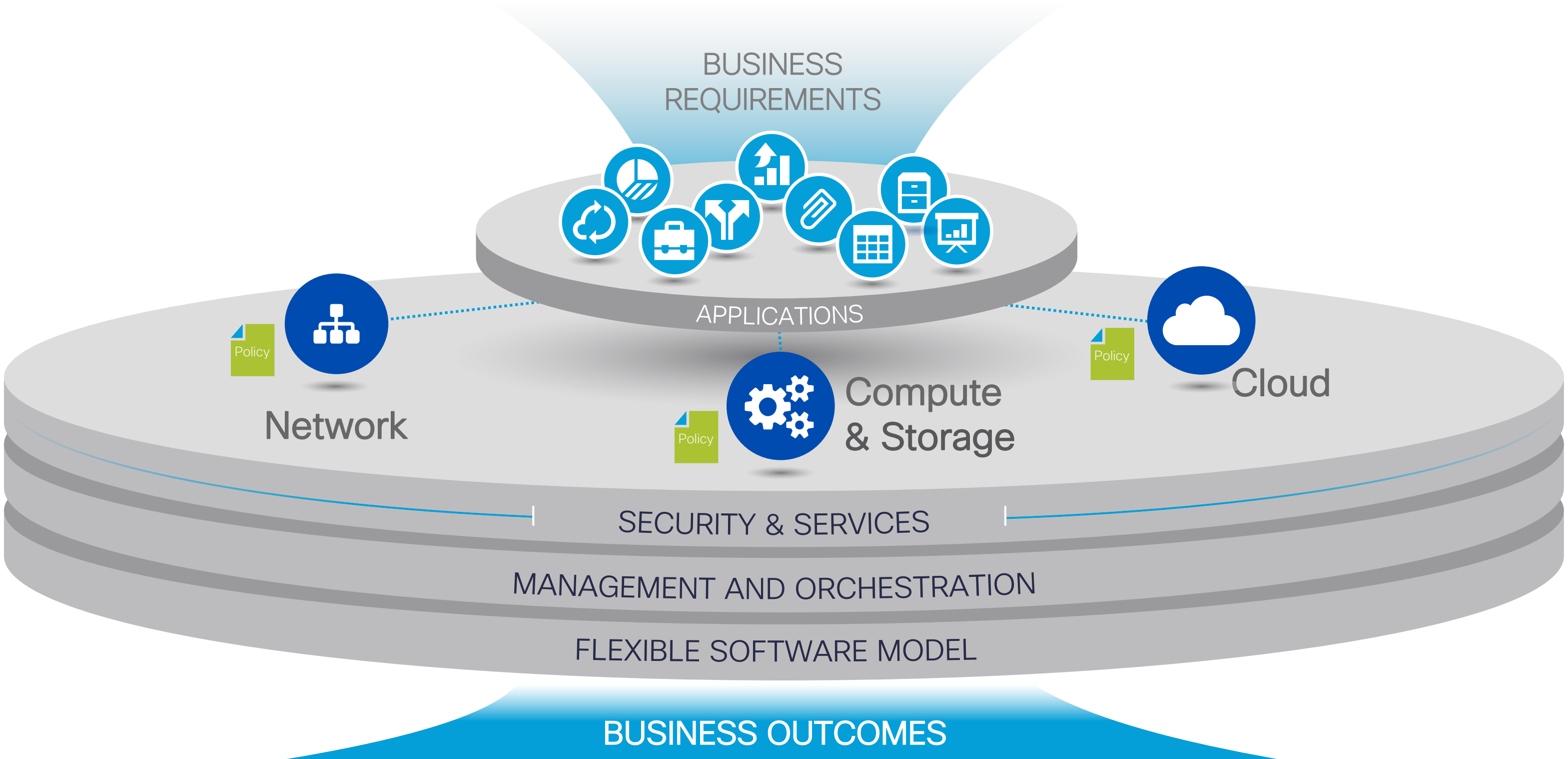
KillerIT · Vnomic Policy Driven Software Defined Everything · Zenoss · apprenda · vmware · openstack · CITRIX · CliQr · SAP · OPSCODE CODE CAN · CATBIRD · python

cisco

Best of INTEROP 2015 Awards

Cisco Data Center Strategy

Defined by **Applications**. Driven by **Policy**. Delivered as a **Service / Solution**



Efficiency	Speed	Digitization

Foundational Switching Platforms for the Next Decade

Nexus 9000

1/10/40/100G

BEST OF SHOW AWARD INTEROP

BEST OF INTEROP

Standalone / ACI Ready

Industry Leading Price/Performance, Port Density:
Fastest 10G/25G/40G/50G/100G Platform

Programmability/ Open APIs: Linux Containers, Python, Power Shell, Puppet, Chef… **Ideal for DevOps!!**

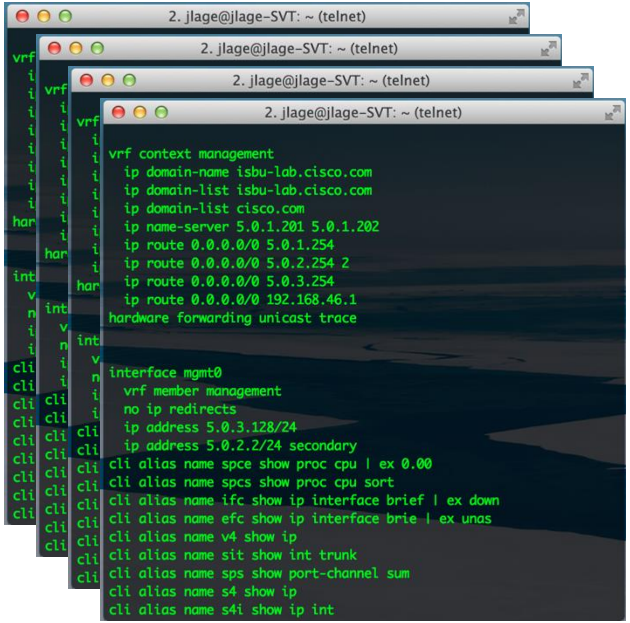
15% Better Power & Cooling–**2.8X** Better Reliability

Innovation Object Model, No Backplane,
No Midplane, Health scores

$ Multi-million Savings 40/100G on Existing Cables using BiDi Optics. **Non disruptive migration to 40G**

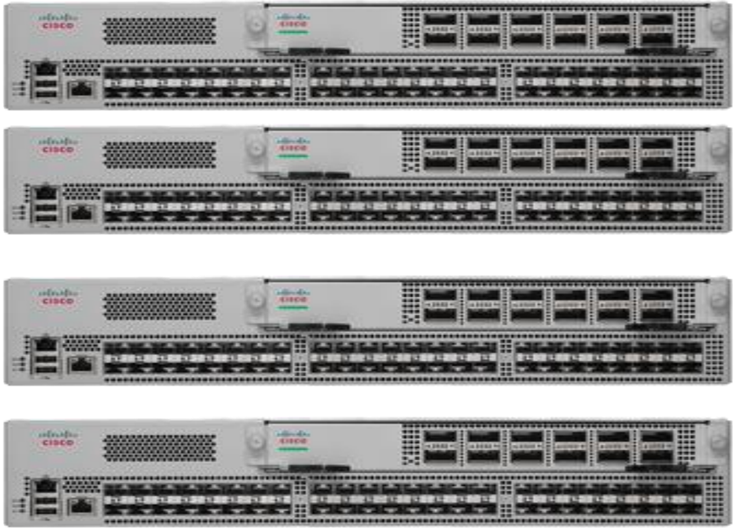
What problem are we solving?

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



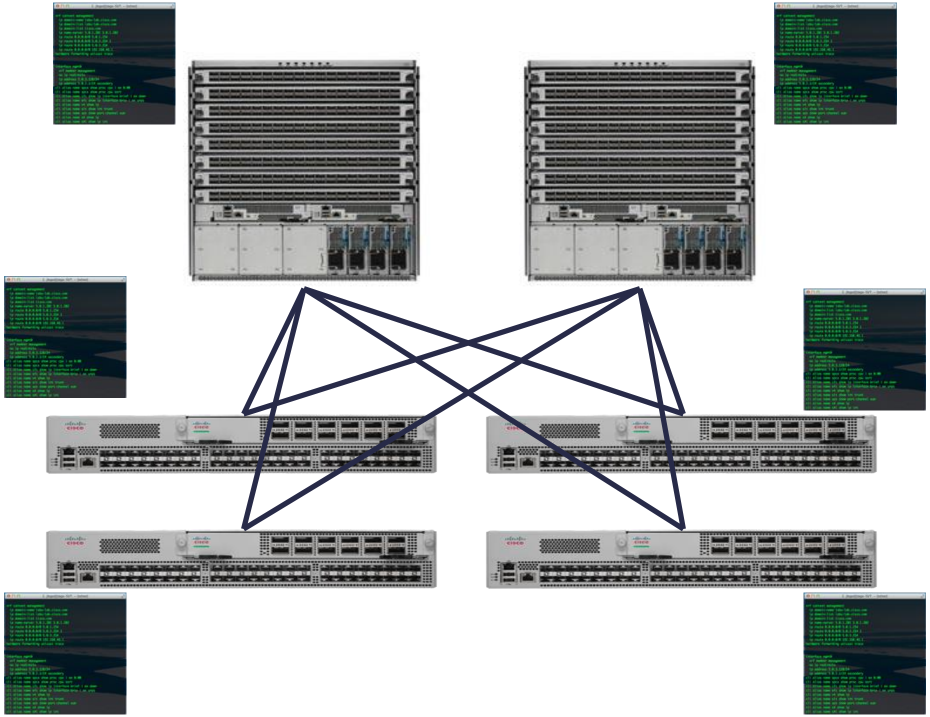
```
vrf context management
  ip domain-name isbu-lab.cisco.com
  ip domain-list isbu-lab.cisco.com
  ip domain-list cisco.com
  ip name-server 5.0.1.201 5.0.1.202
  ip route 0.0.0.0/0 5.0.1.254
  ip route 0.0.0.0/0 5.0.2.254 2
  ip route 0.0.0.0/0 5.0.3.254
  ip route 0.0.0.0/0 192.168.46.1
hardware forwarding unicast trace


interface mgmt0
  vrf member management
  no ip redirects
  ip address 5.0.3.128/24
  ip address 5.0.2.2/24 secondary
cli alias name spce show proc cpu | ex 0.00
cli alias name spcs show proc cpu sort
cli alias name ifc show ip interface brief | ex down
cli alias name efc show ip interface brie | ex unas
cli alias name v4 show ip
cli alias name sit show int trunk
cli alias name sps show port-channel sum
cli alias name s4 show ip
cli alias name s4i show ip int
```



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

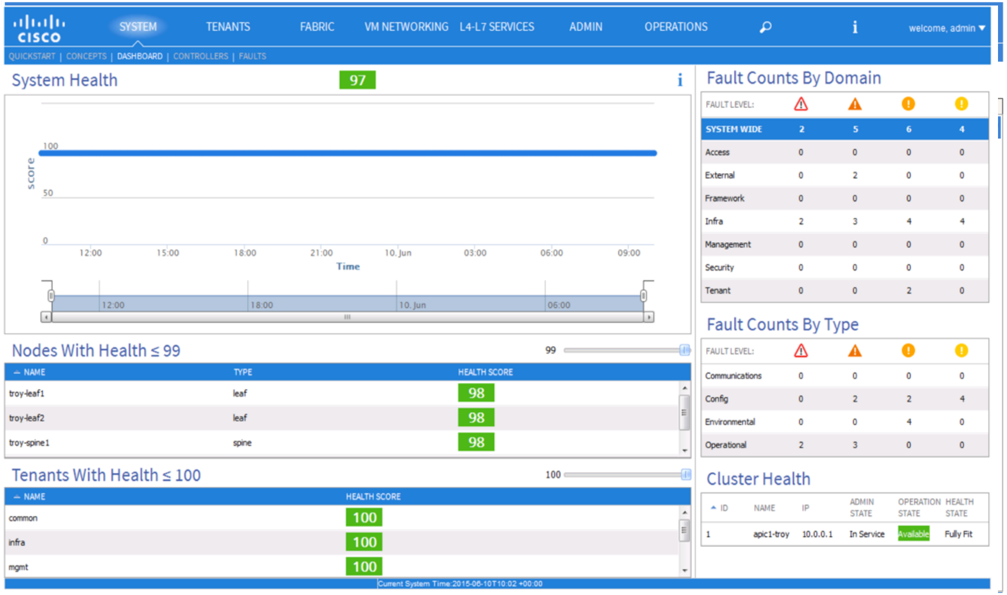
- **Device basics**: AAA, syslog, SNMP, PoAP, hash seed, default routing protocol bandwidth …
- **Interface and/or Interface Pairs**: UDLD, BFD, MTU, interface route metric, channel hashing, Queuing, LACP, …
- **Fabric and hardware specific design**: HW Tables, TCAM, …
- **Switch Pair/Group**: HSRP/VRRP,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



Cisco ACI solves the problem …

APIC

Interfaces, protocols, TCAM, etc … all represented in an object model, and ALL accessible through an XML/JSON API and CLI



System Health 97

Nodes With Health ≤ 99

NAME	TYPE	HEALTH SCORE
troy-leaf1	leaf	98
troy-leaf2	leaf	98
troy-spine1	spine	98

Tenants With Health ≤ 100

NAME	HEALTH SCORE
common	100
infra	100
mgmt	100

Current System Time:2015-06-10T10:02 +00:00

Fault Counts By Domain

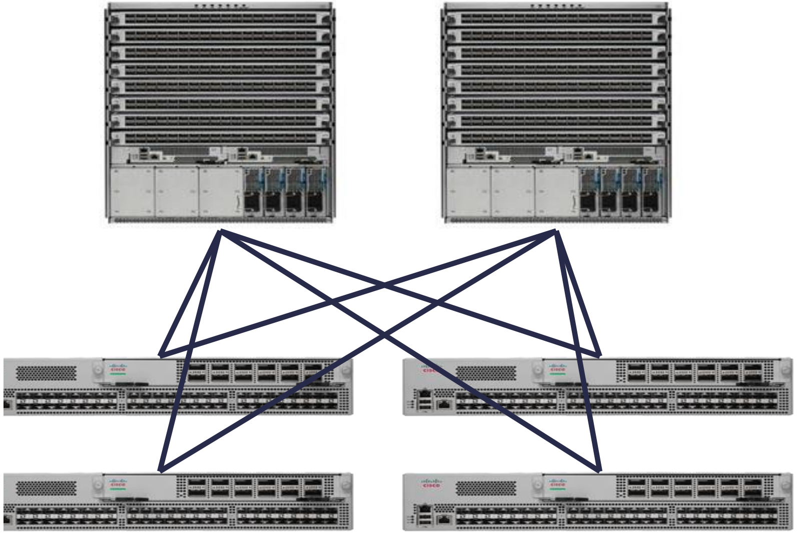
FAULT LEVEL:	⚠	▲	●	●
SYSTEM WIDE	2	5	6	4
Access	0	0	0	0
External	0	2	0	0
Framework	0	0	0	0
Infra	2	3	4	4
Management	0	0	0	0
Security	0	0	0	0
Tenant	0	0	2	0

Fault Counts By Type

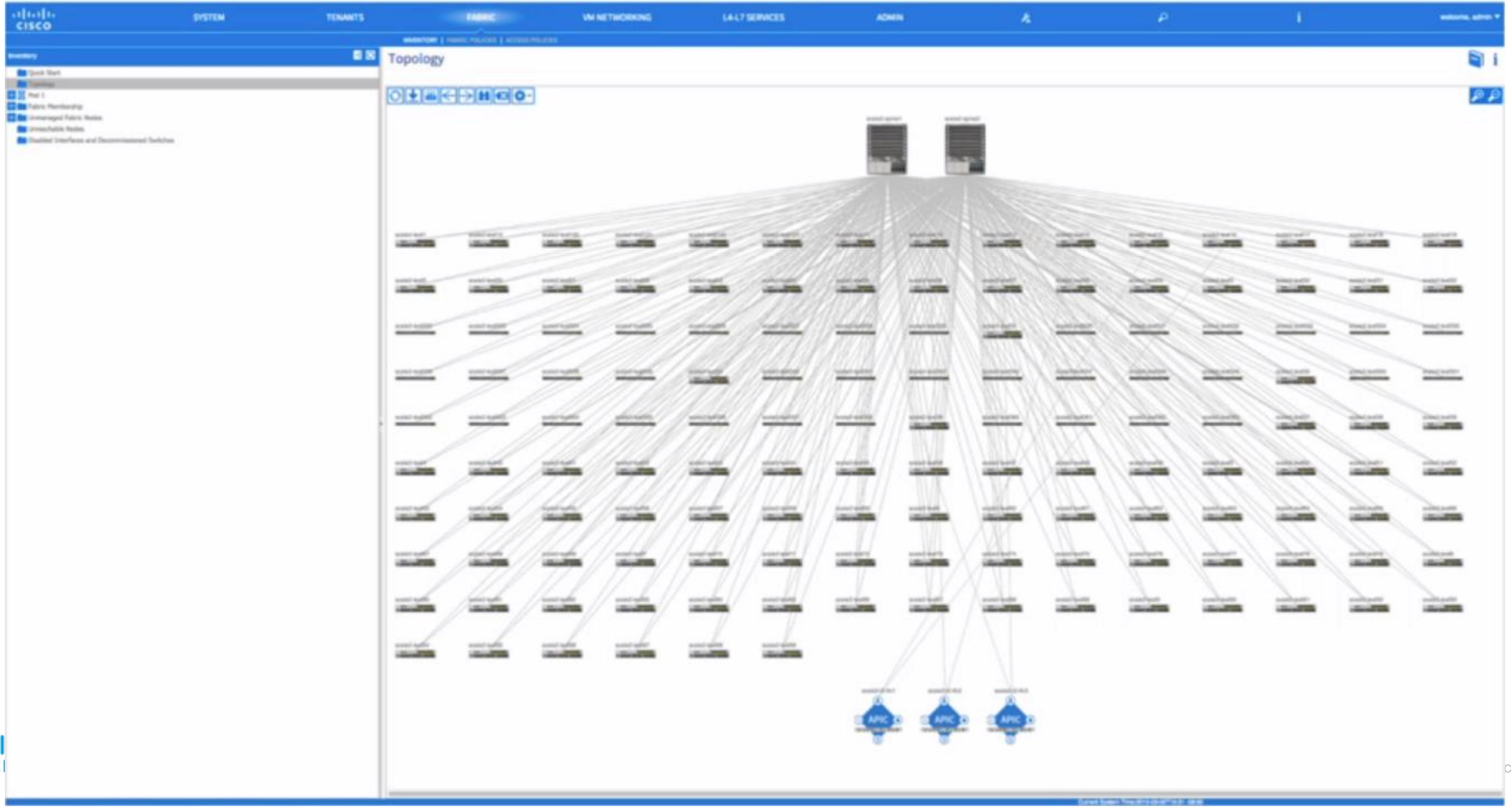
FAULT LEVEL:	⚠	▲	●	●
Communications	0	0	0	0
Config	0	2	2	4
Environmental	0	0	4	0
Operational	2	3	0	0

Cluster Health

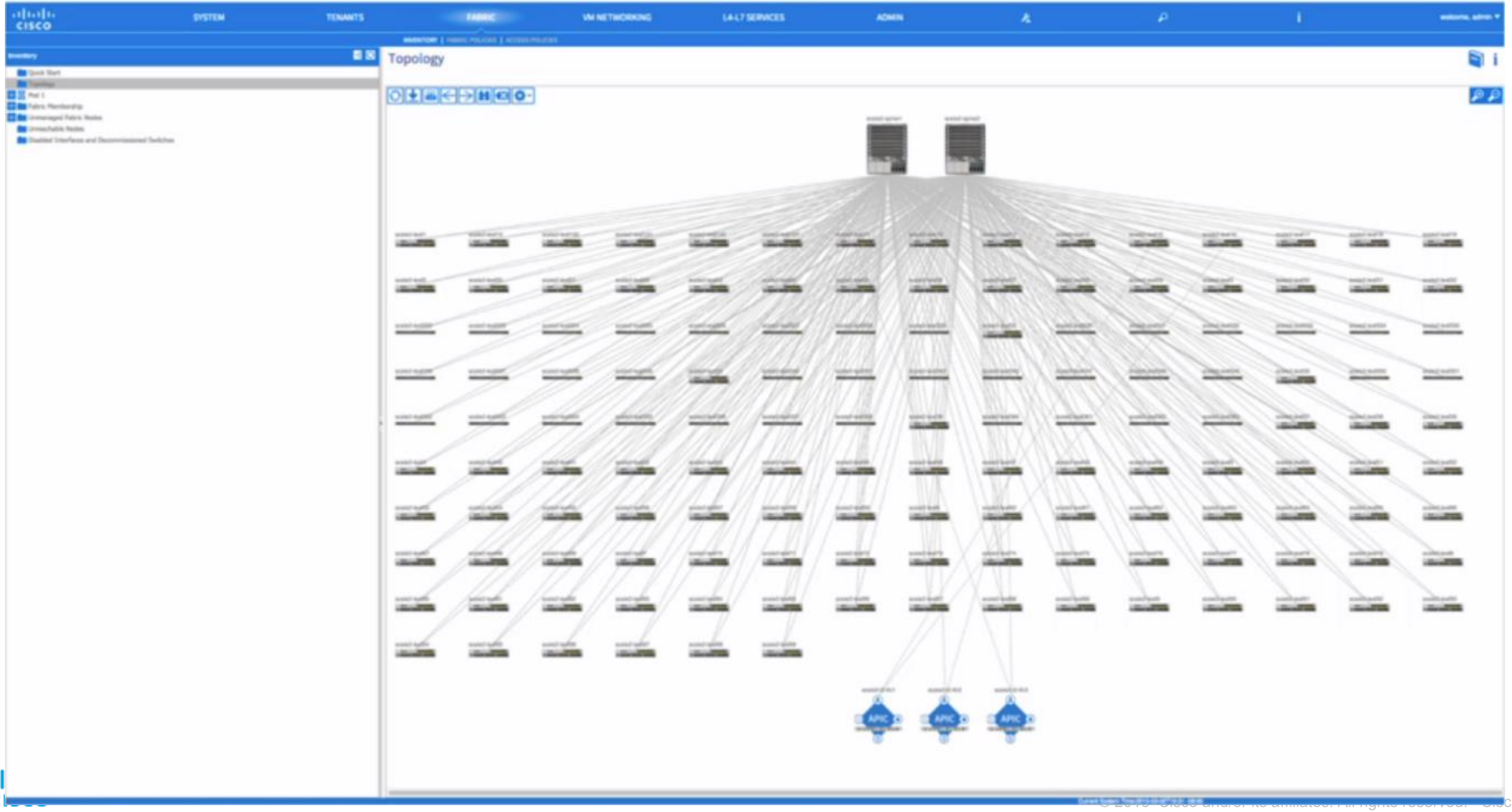
ID	NAME	IP	ADMIN STATE	OPERATION STATE	HEALTH STATE
1	apic1-troy	10.0.0.1	In Service	Available	Fully Fit



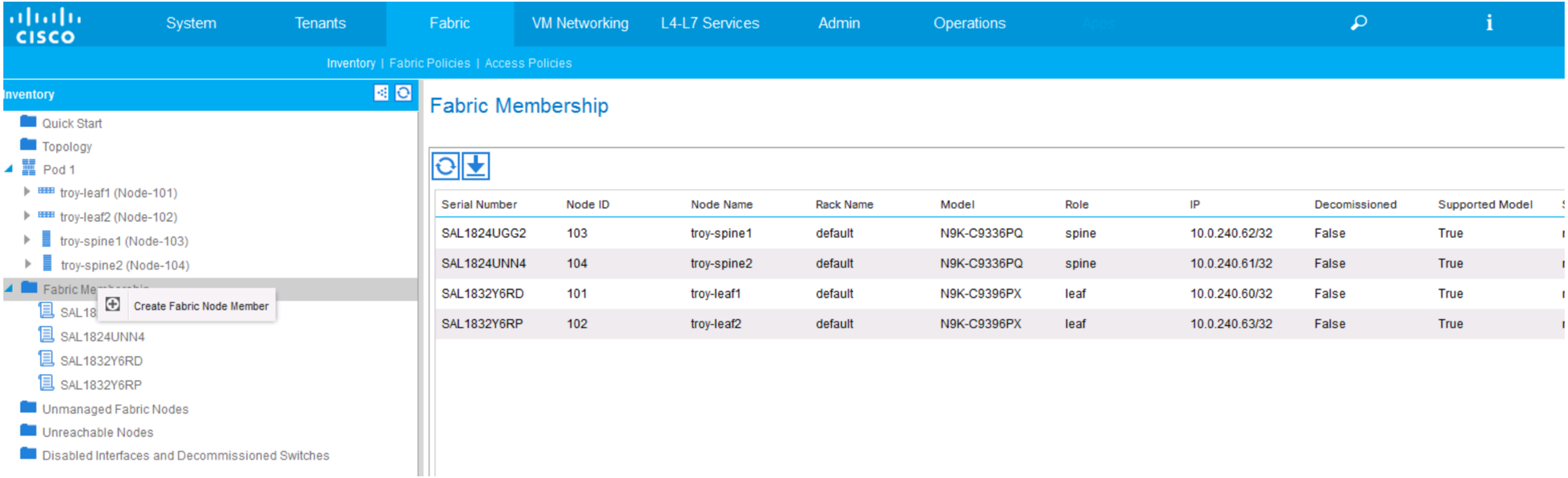
APIC becomes single point of management for the entire fabric … with a policy-based model



… and the fabric acts like a single (virtualized) switch



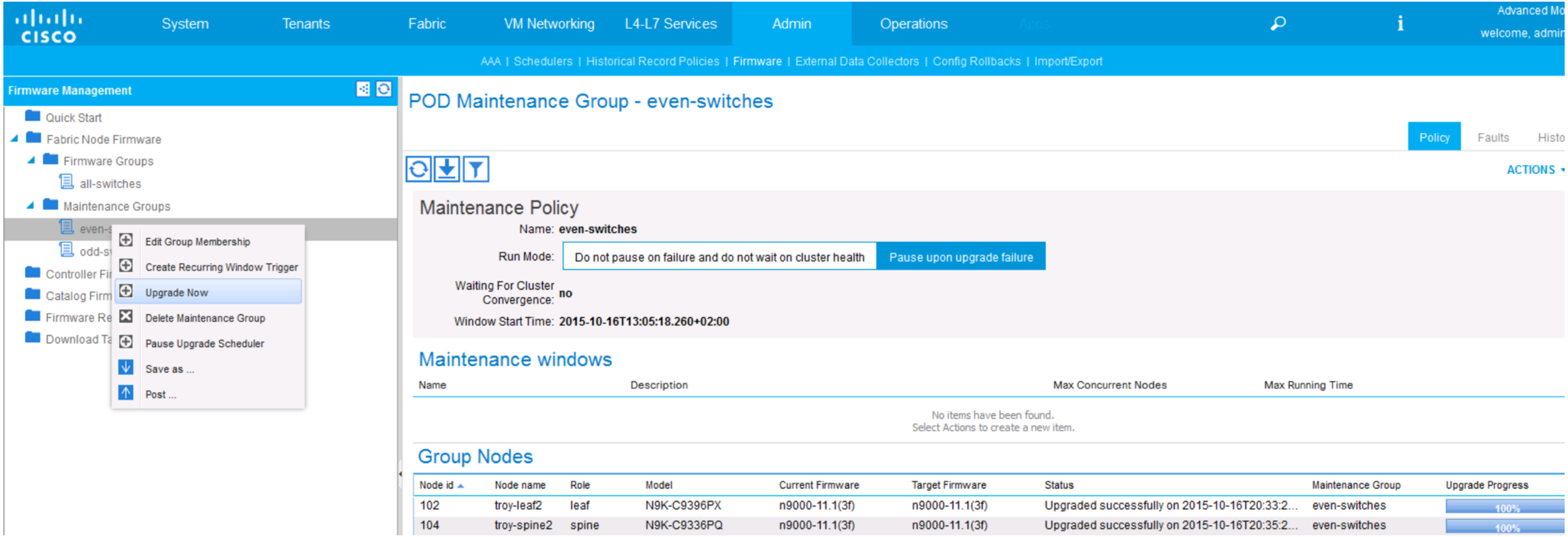
Adding, removing or replacing nodes becomes extremely simple



Fabric Membership

Serial Number	Node ID	Node Name	Rack Name	Model	Role	IP	Decomissioned	Supported Model
SAL1824UGG2	103	troy-spine1	default	N9K-C9336PQ	spine	10.0.240.62/32	False	True
SAL1824UNN4	104	troy-spine2	default	N9K-C9336PQ	spine	10.0.240.61/32	False	True
SAL1832Y6RD	101	troy-leaf1	default	N9K-C9396PX	leaf	10.0.240.60/32	False	True
SAL1832Y6RP	102	troy-leaf2	default	N9K-C9396PX	leaf	10.0.240.63/32	False	True

And so do network upgrades …



POD Maintenance Group - even-switches

Maintenance Policy

Name: **even-switches**

Run Mode: Do not pause on failure and do not wait on cluster health | Pause upgrade failure upon upgrade failure

Waiting For Cluster Convergence: **no**

Window Start Time: **2015-10-16T13:05:18.260+02:00**

Maintenance windows

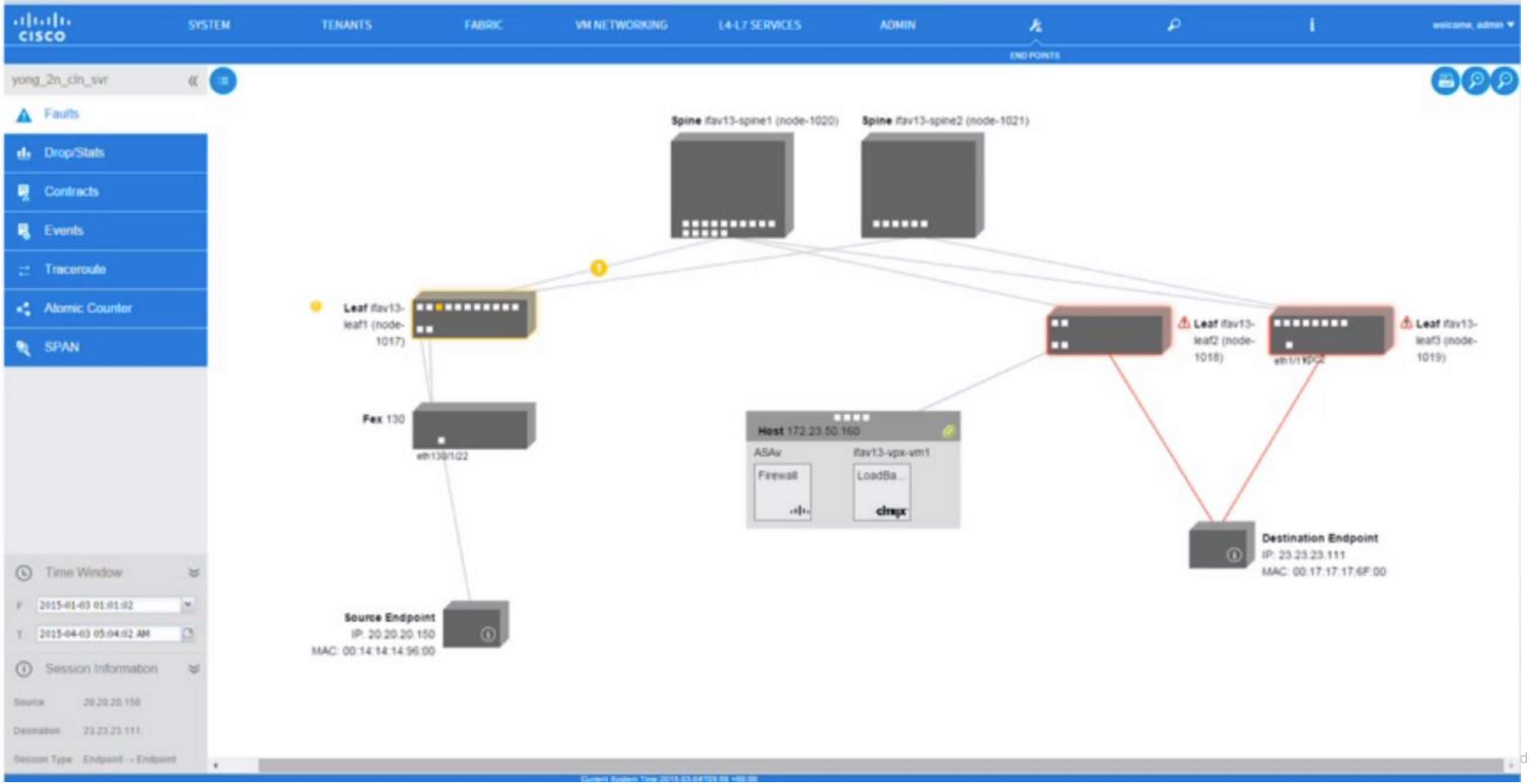
Name	Description	Max Concurrent Nodes	Max Running Time

No items have been found.
Select Actions to create a new item.

Group Nodes

Node id	Node name	Role	Model	Current Firmware	Target Firmware	Status	Maintenance Group	Upgrade Progress
102	troy-leaf2	leaf	N9K-C9396PX	n9000-11.1(3f)	n9000-11.1(3f)	Upgraded successfully on 2015-10-16T20:33:2...	even-switches	100%
104	troy-spine2	spine	N9K-C9336PQ	n9000-11.1(3f)	n9000-11.1(3f)	Upgraded successfully on 2015-10-16T20:35:2...	even-switches	100%

… and you get best troubleshooting with full physical, virtual and services visibility …



Source Endpoint
IP: 20.20.20.150
MAC: 00:14:14:14:96:00

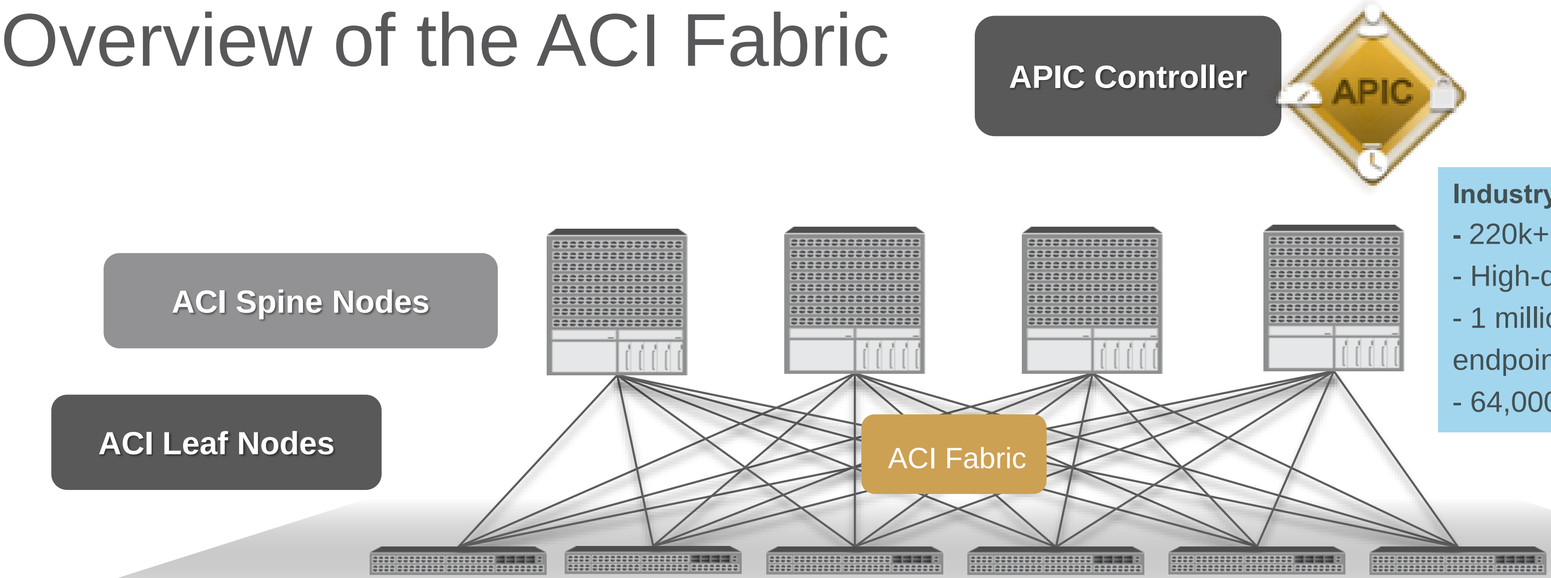
Destination Endpoint
IP: 23.23.23.111
MAC: 00:17:17:17:6F:00

F 2015-01-03 01:01:02
T 2015-04-03 05:04:02 AM

Source 20.20.20.150
Destination 23.23.23.111
Session Type Endpoint → Endpoint

So, the first thing to remember about ACI: it is a programmable physical fabric with a single point of management ...

Overview of the ACI Fabric



Industry's most efficient fabric:
- 220k+ 1/10Gb edge hosts
- High-density 40/100G spine
- 1 million+ IPv4 / IPv6 endpoints
- 64,000+ tenants

ACI Fabric Features -

ACI Spine Layer – Provides bandwidth and redundancy between Leaf Nodes

ACI Leaf Layer – Provides all connectivity outside the fabric - including servers, service devices, other networ

Optimized Traffic Flows – Accommodates new E-W traffic patterns in simple, scalable, non-blocking design

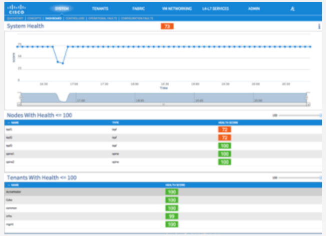
Decoupling of Endpoint Identity – Network policies automatically move with VM/Server/Container

Network Innovations – Dynamic load balancing, dynamic packet prioritization, congestion management

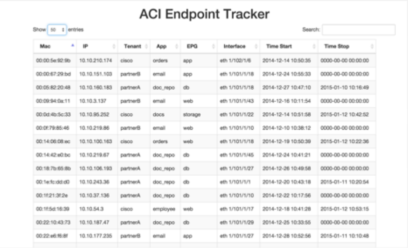
ACI Operational Simplicity

ACI – Day 2 Tools for Simplified Operations

System Health Scores



Endpoint Tracker

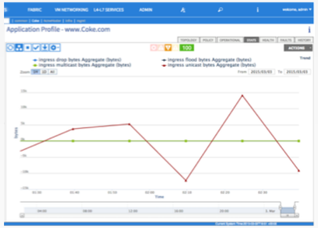


ACI Endpoint Tracker

Show 50 entries   Search:

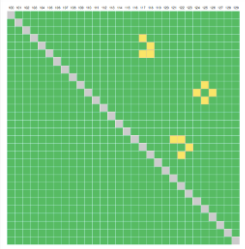
Mac	IP	Tenant	App	EPG	Interface	Time Start	Time Stop
00:00:5e:92:9b	10.10.210.174	cisco	orders	app	eth 1/102/1/6	2014-12-14 10:50:35	0000-00-00 00:00:00
00:00:67:29:bd	10.10.151.103	partnerB	email	app	eth 1/101/1/18	2014-12-24 10:55:33	0000-00-00 00:00:00
00:05:82:20:48	10.10.160.183	partnerA	doc_repo	db	eth 1/101/1/18	2014-12-27 10:47:10	2015-01-10 10:16:49
00:09:94:0a:11	10.10.3.137	partnerB	email	web	eth 1/101/1/43	2014-12-16 10:11:54	0000-00-00 00:00:00
00:0d:4b:5c:33	10.10.95.252	cisco	docs	storage	eth 1/101/1/22	2014-12-14 10:51:58	2015-01-12 10:42:52
00:0f:79:85:46	10.10.219.86	partnerB	email	web	eth 1/101/1/10	2014-12-10 10:38:12	0000-00-00 00:00:00
00:14:06:08:ec	10.10.100.163	cisco	orders	web	eth 1/101/1/18	2014-12-19 10:50:39	2015-01-12 10:22:36
00:14:42:e0:bc	10.10.219.67	partnerA	doc_repo	db	eth 1/101/1/45	2014-12-24 10:41:21	0000-00-00 00:00:00
00:18:7b:65:8b	10.10.106.193	partnerA	doc_repo	db	eth 1/101/1/27	2014-12-26 10:49:58	0000-00-00 00:00:00
00:1e:fc:dd:d0	10.10.243.36	partnerA	doc_repo	db	eth 1/101/1/1	2014-12-20 10:43:18	2015-01-11 10:20:54
00:1f:21:3f:2e	10.10.37.136	partnerA	doc_repo	db	eth 1/101/1/10	2014-12-22 10:17:56	0000-00-00 00:00:00
00:1f:5d:16:39	10.10.54.3	cisco	employee	web	eth 1/101/1/17	2014-12-18 10:41:28	2015-01-12 10:53:15
00:22:10:43:73	10.10.187.47	partnerA	doc_repo	db	eth 1/101/1/29	2014-12-25 10:33:55	0000-00-00 00:00:00
00:22:e6:f6:8f	10.10.177.235	partnerB	email	app	eth 1/101/1/27	2014-12-28 10:52:56	2015-01-11 10:10:48

Statistics Per App

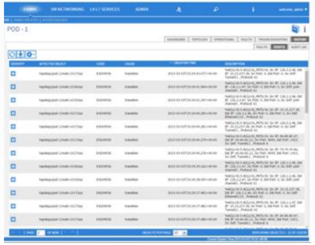


Application Profile - www.Coke.com

Real-time Heat Maps

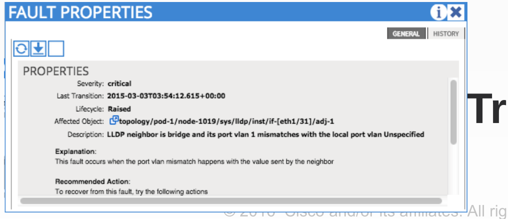


Contract Deny Logs



POD - 1

Endpoint Troubleshooting Wizard



FAULT PROPERTIES

GENERAL | HISTORY

PROPERTIES

Severity: critical

Last Transition: 2015-03-03T03:54:12.615+00:00

Lifecycle: Raised

Affected Object: topology/pod-1/node-1019/sys/lldp/inst/if-[eth1/31]/adj-1

Description: LLDP neighbor is bridge and its port vlan 1 mismatches with the local port vlan Unspecified

Explanation:

This fault occurs when the port vlan mismatch happens with the value sent by the neighbor

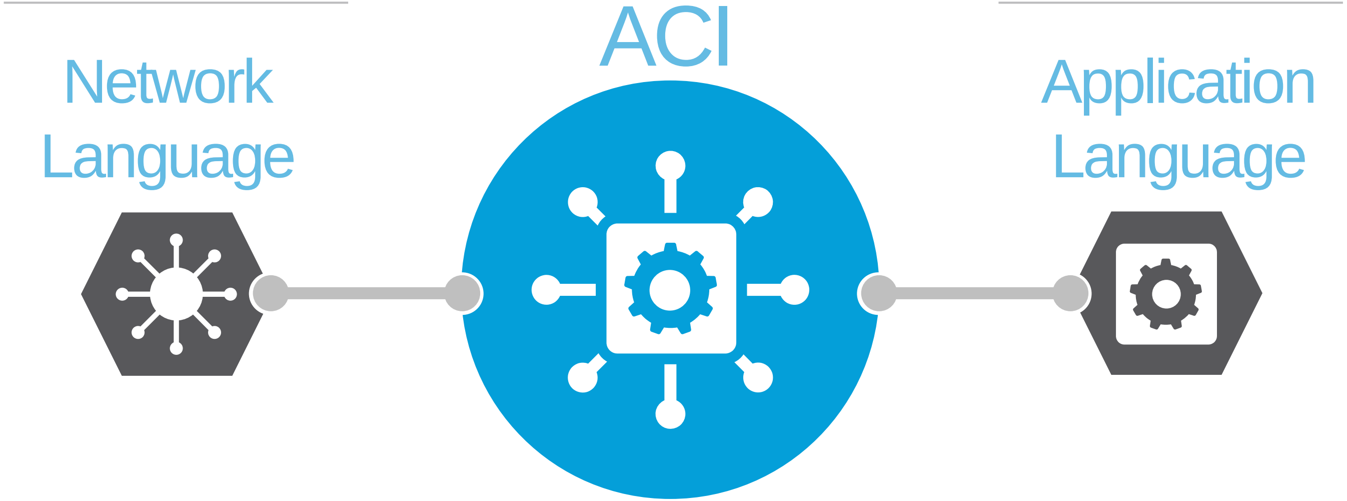
Recommended Action:

To recover from this fault, try the following actions

YORK
LONDON
GENEVA
THE MOMENT YOU PROVE
IT IS NOT THE NETWORK.
imgflip.com

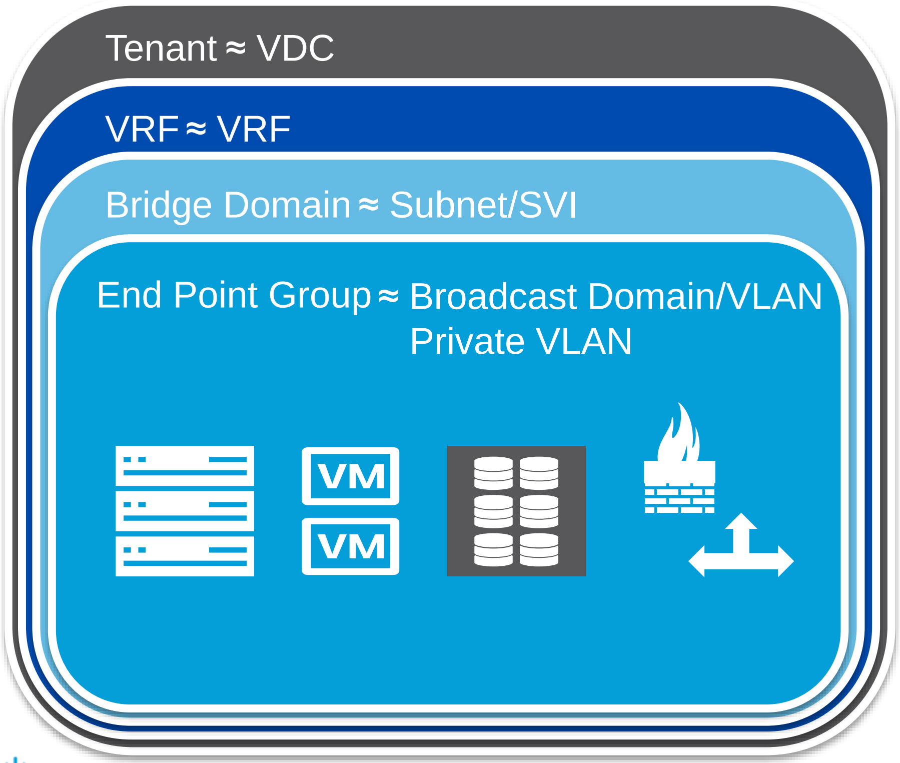
ACI Policy Model

Policy Defined by Application



Push configurations automatically to the entire network

The ACI Policy Model



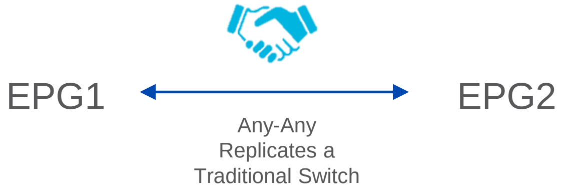
Tenant ≈ VDC

VRF ≈ VRF

Bridge Domain ≈ Subnet/SVI

End Point Group ≈ Broadcast Domain/VLAN
Private VLAN

Contracts ≈ Access Lists

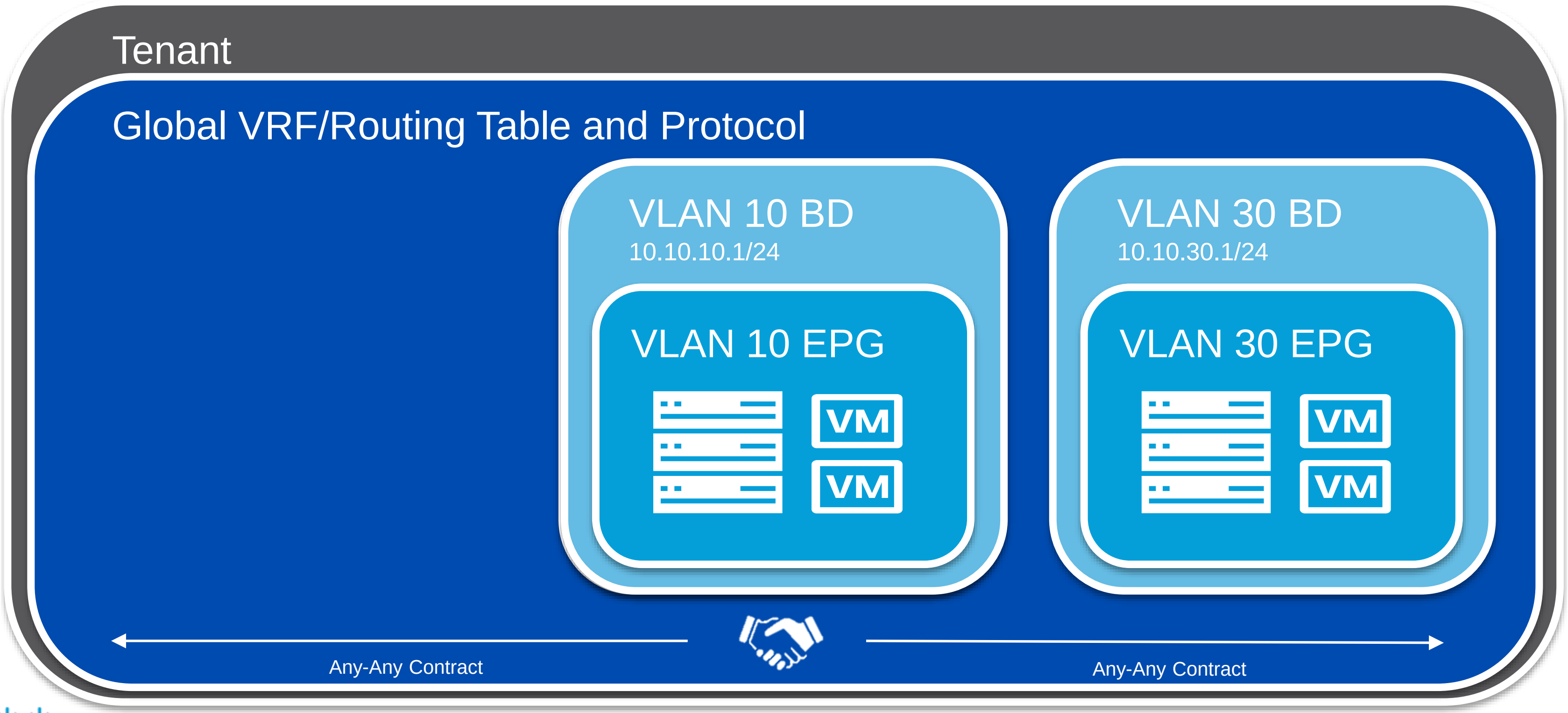


Any-Any
Replicates a
Traditional Switch

L2 External EPG≈ 802.1q Trunk

L3 External EPG≈ L3 Routed Link

The ACI Policy Model – Network Centric Configuration



Tenant

Global VRF/Routing Table and Protocol

VLAN 10 BD
10.10.10.1/24

VLAN 10 EPG

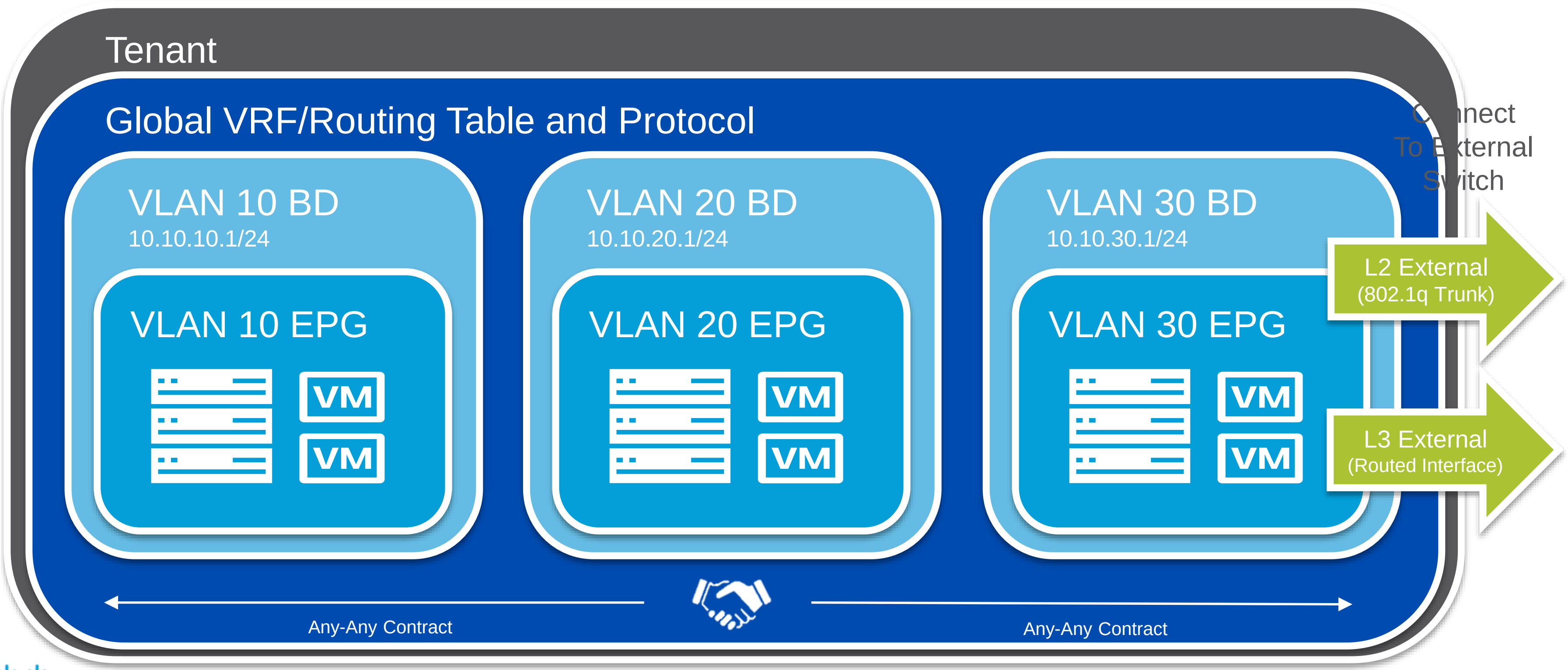
VLAN 30 BD
10.10.30.1/24

VLAN 30 EPG

Any-Any Contract

Any-Any Contract

The ACI Policy Model – Network Centric Configuration



Tenant

Global VRF/Routing Table and Protocol

VLAN 10 BD
10.10.10.1/24

VLAN 10 EPG

VLAN 20 BD
10.10.20.1/24

VLAN 20 EPG

VLAN 30 BD
10.10.30.1/24

VLAN 30 EPG

Connect To External Switch

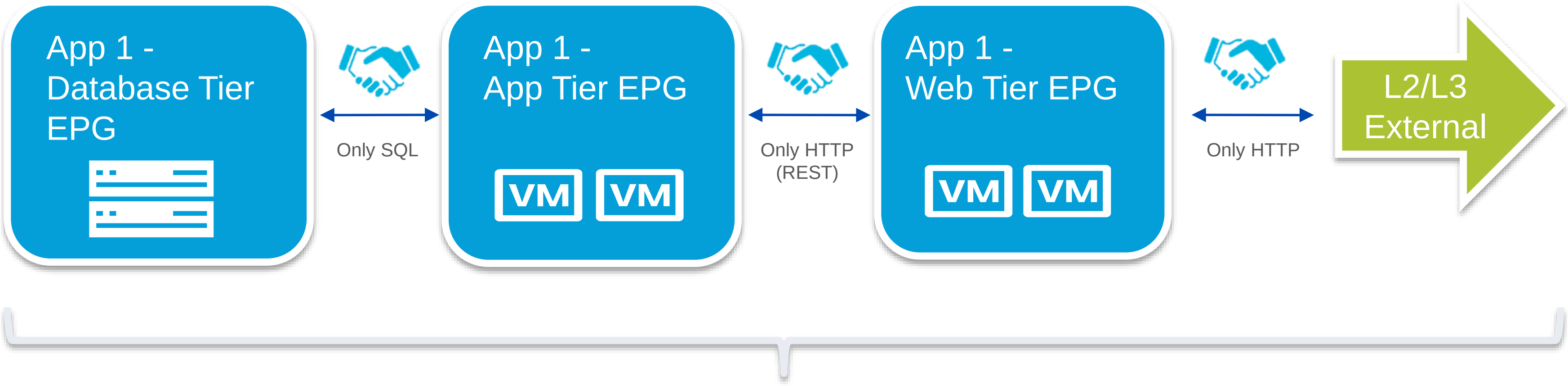
L2 External
(802.1q Trunk)

L3 External
(Routed Interface)

Any-Any Contract

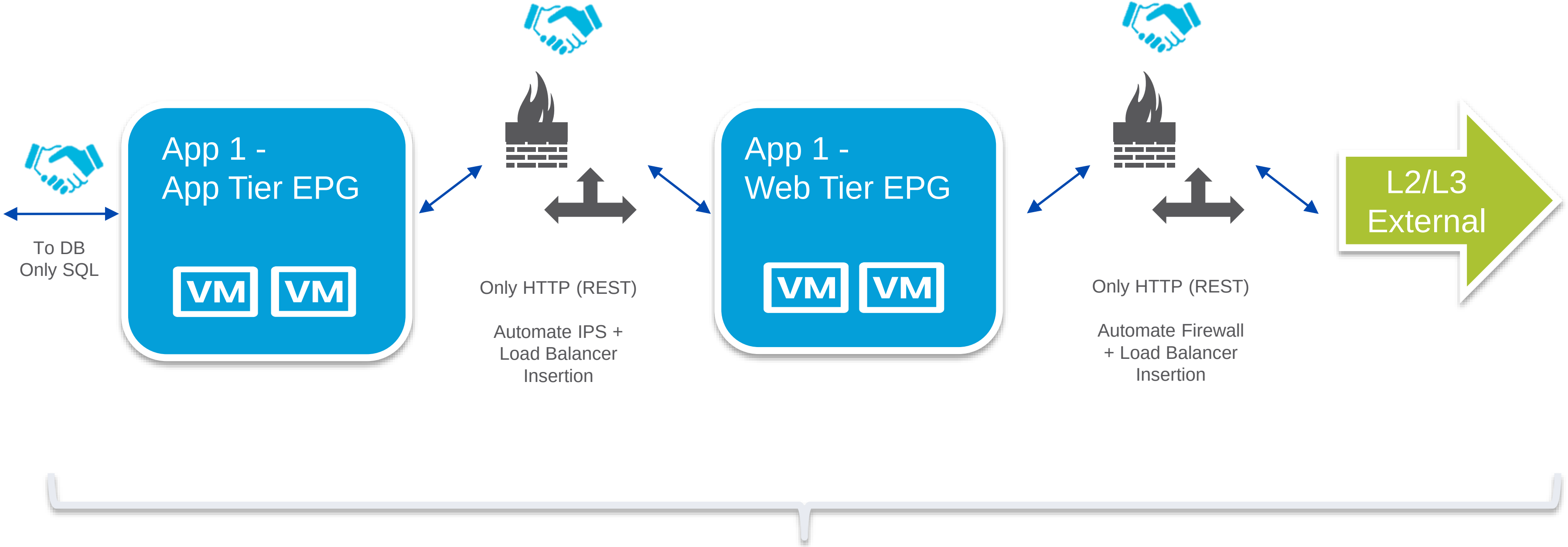
Any-Any Contract

Advanced ACI Policy Model – Micro Segmentation



Application Profile

Advanced ACI Policy Model – Service Insertion



Application Profile with Service Graphs

Software

Cisco ACI 1.2 Release

Infrastructure

- IP-based endpoint group (EPG)
- Shared Layer 3 outside (L3Out) connectivity
- Direct server return
- Common pervasive gateway for IPv4 and secondary IP address for IPv4
- ‘Multi-site Application’ – ACI Toolkit
- Service Insertion and Chaining for Any Layer 4-7 device (no device package)
- Ingress policy enforcement for L3Out scalability
- Class of Service Preservation
- VXLAN support (host to ACI Fabric)
- Static Route with Weights
- TLS 1.2
- Cisco Nexus® 9516 Switch (support for 10 slots)

Virtualization

- VMware vSphere 6.0 support enhancements (vMotion for X-vCenter, X-VDS)
- Micro-segmentation
  - Microsoft Hyper-V
- Cisco® Application Virtual Switch (AVS) for IPv6
- Authentication, authorization, and accounting (AAA) for L4-L7 services
- VMware vRealize integration
- New OpFlex for Open Virtual Switch (OVS)
  - Local policy enforcement
  - Virtual Extensible LAN (VXLAN) support
  - Network Address Translation (NAT) and floating IP address
  - Cisco Application Infrastructure Controller (APIC) GUI integration

Troubleshooting and Operations

- Basic GUI and Advanced GUI modes
- Simple Network Management Protocol (SNMP) support for APIC
- Accurate counter and SNMP MIB support for Layer 3 (L3Out) interface
- Troubleshooting wizard enhancements
- Cisco NX-OS style command-line interface (CLI) on APIC
- Configuration rollback
- Endpoint tracker
- Traffic map

IP-Based EPG

Description

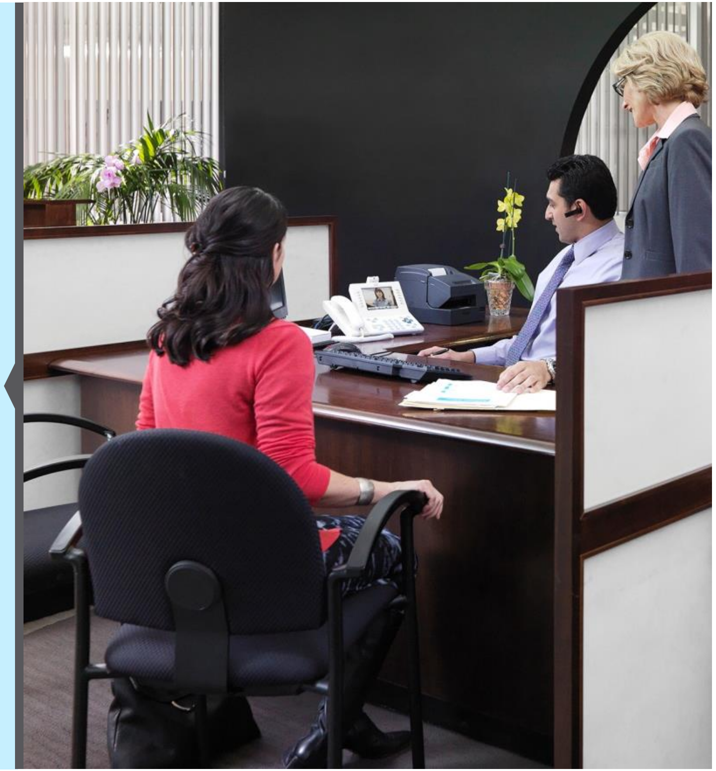
- This feature allows detailed EPG derivation based on the IP address of the endpoint.
- Available for both physical and virtual endpoints.

Use Case

- Directly attached storage filers: Many enterprises use storage filers that expose one MAC address and many different IP addresses, and they want to apply policy per IP prefix. A Cisco 9300 ® E-Series leaf switch or module is required.

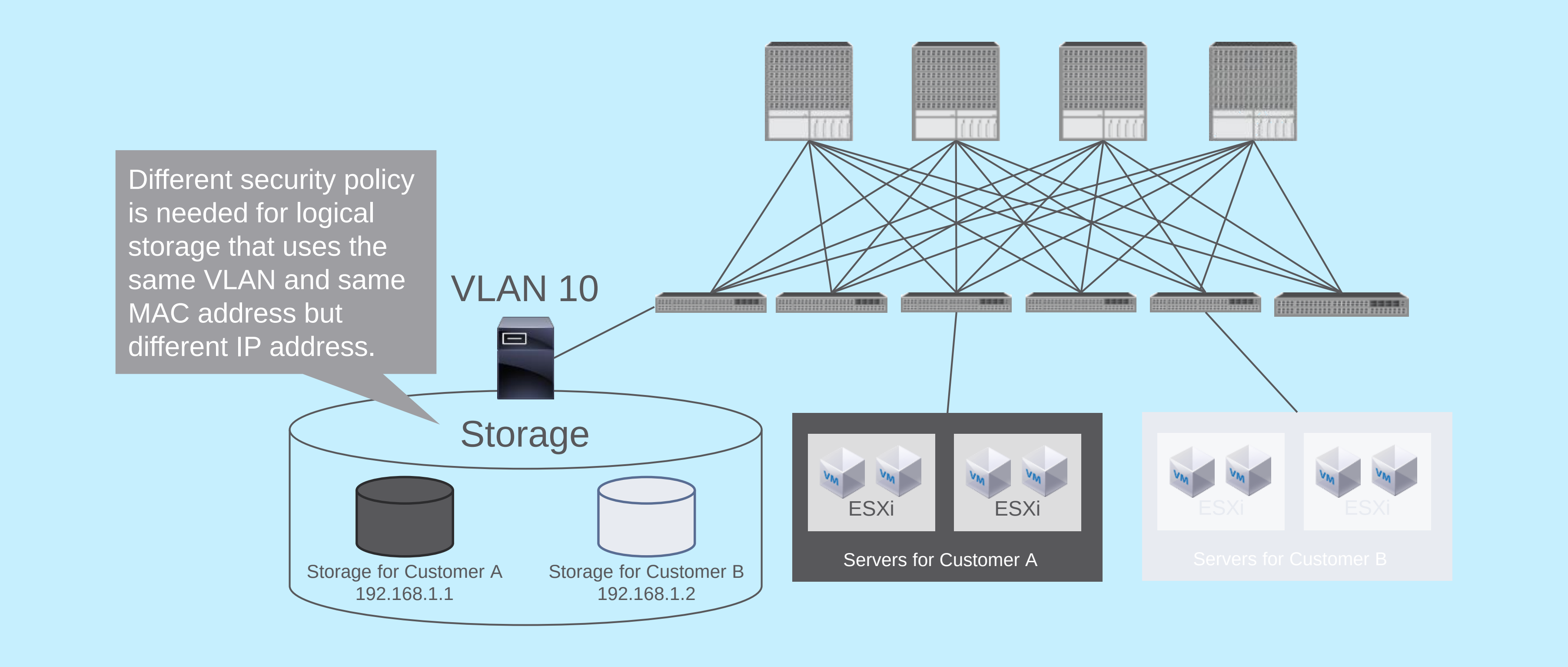
Matching Criteria

- IP address attribute: IP-prefix based
  - The IP address is specified in the Prefix/Subnet format: for example, 1.1.1.0/30.
  - A longest prefix match is performed for the IP address to derive the EPG.
- MAC address attribute (future)
  - The exact and complete MAC address must be specified as a part of this policy.



IP-Based EPG: Use Case 1

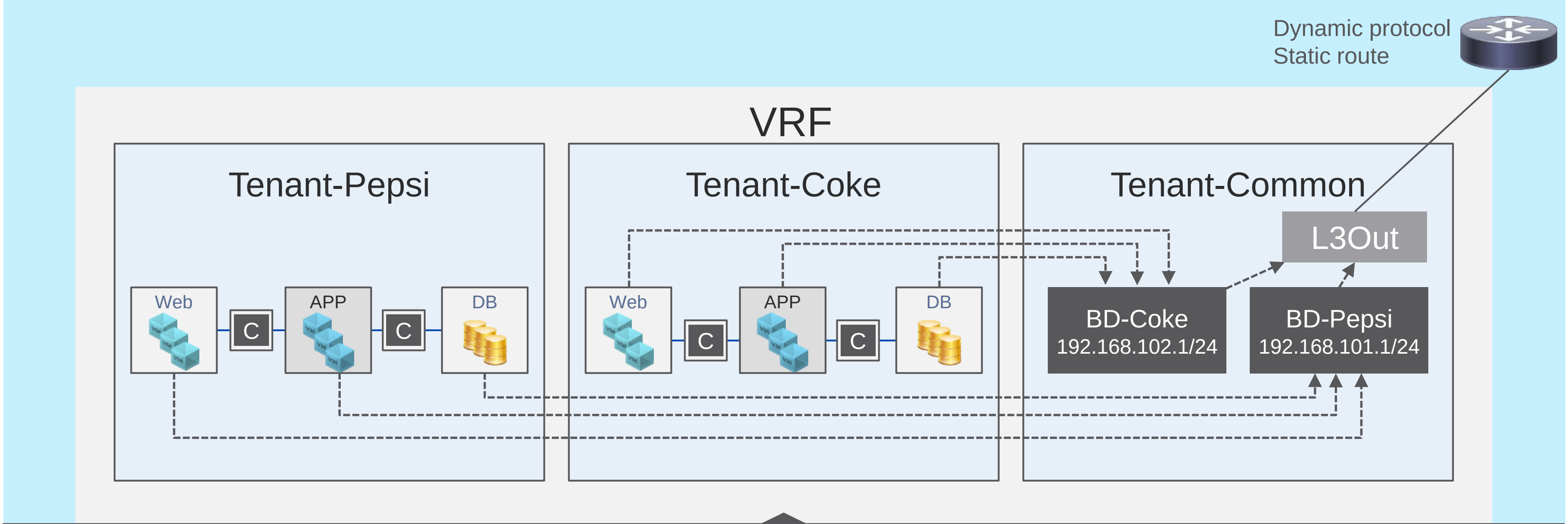
Shared Storage for Each Customer



Different security policy is needed for logical storage that uses the same VLAN and same MAC address but different IP address.

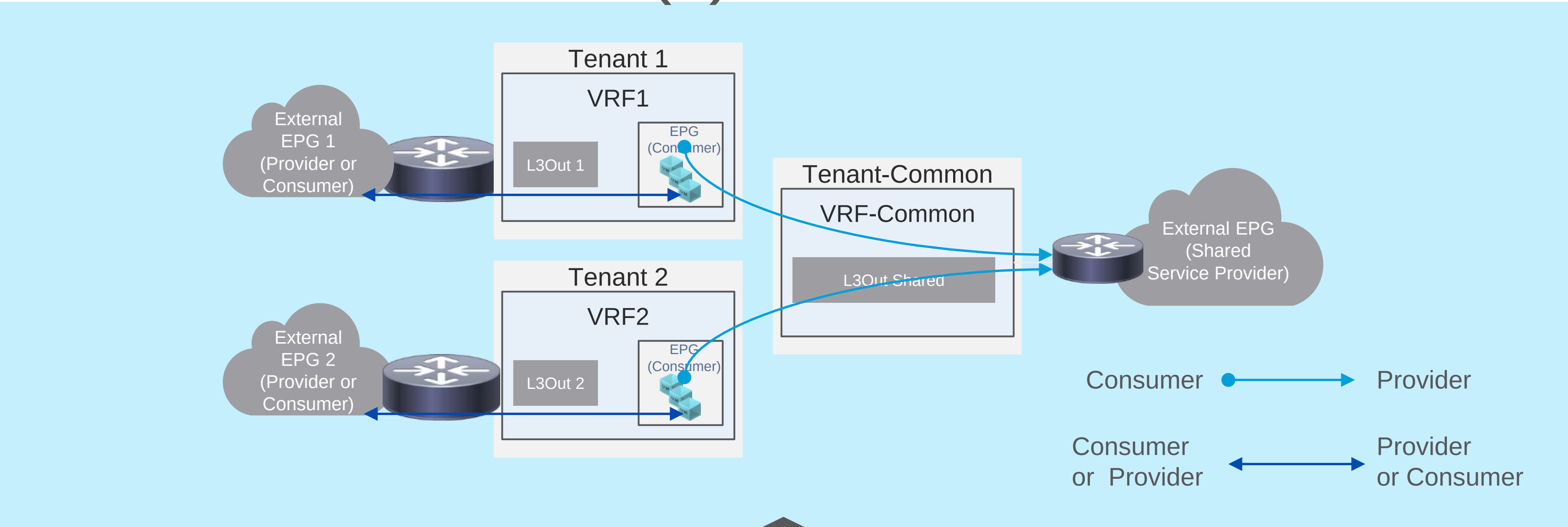
Sharing VRF and L3Out Among Tenants

Bridge Domain, Subnet, and L3Out Under Tenant Common



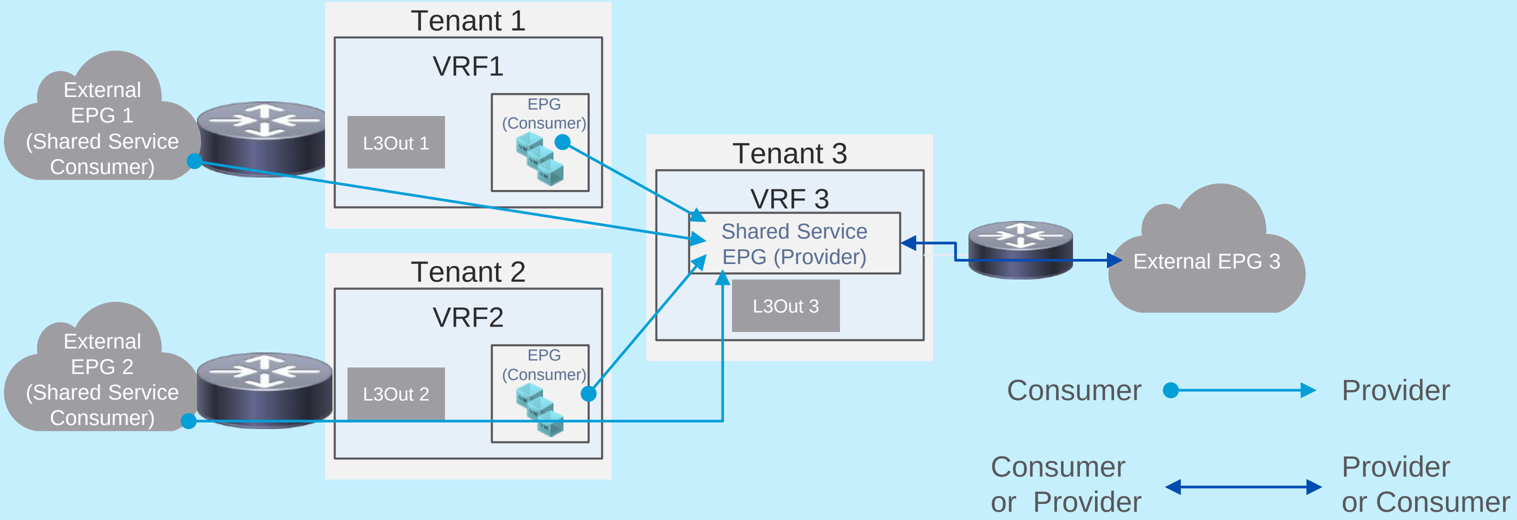
- No overlapping IP addresses among tenants, VRF instances shared among tenants, and traffic isolation through contract
- Bridge domain and subnet and L3Out defined under tenant common
- EPG, contract, and application profile under individual tenants
- Dynamic routing protocol with external routers

Sharing L3Out Across VRF Instances with Cisco ACI 1.2(x)



- Shared service provider is an external EPG.
- Shared service provider can be in any tenants.

Shared Service with L3Out Across VRF Instances



- Shared service provider is tenant EPG.
- External EPGs of different tenant and VRF access to shared services.

Virtualization

VMware vSphere 6.0

- No changes in Cisco® APIC configuration and operations
  - A new VMware DVS Release 6.0 is added to force configuration to DVS to Release 6.
- Support for inter-data center and intra-vCenter
  - Both vCenters should be part of the same single sign-on (SSO) instance.
  - Long-distance vMotion is not verified or supported.
  - Support applies only to DVS, not Cisco Application Virtual Switch.
- For more information, see http://www.vmware.com/files/pdf/vsphere/VMW-WP-vSPHR-Whats-New-6-0-PLTFRM.pdf.
- For a demonstration, see https://ciscosupport.webex.com/ciscosupport/lsr.php?RCID=79b6da87533c4eac85dcedc8eaa5ac85.

Attribute-Based EPG

Description

- This feature allows detailed EPG derivation based on various virtual machine attributes such as virtual machine name, guest OS, MAC address, and IP address.
- Prior to Brazos, this feature was available for virtual endpoints attached with the Cisco® AVS distributed virtual switch (B release). It is not available with VMware DVS. → Available with 1.3 with EX switches!
- Brazos also adds this feature for Cisco ACI™ and Microsoft SCVMM

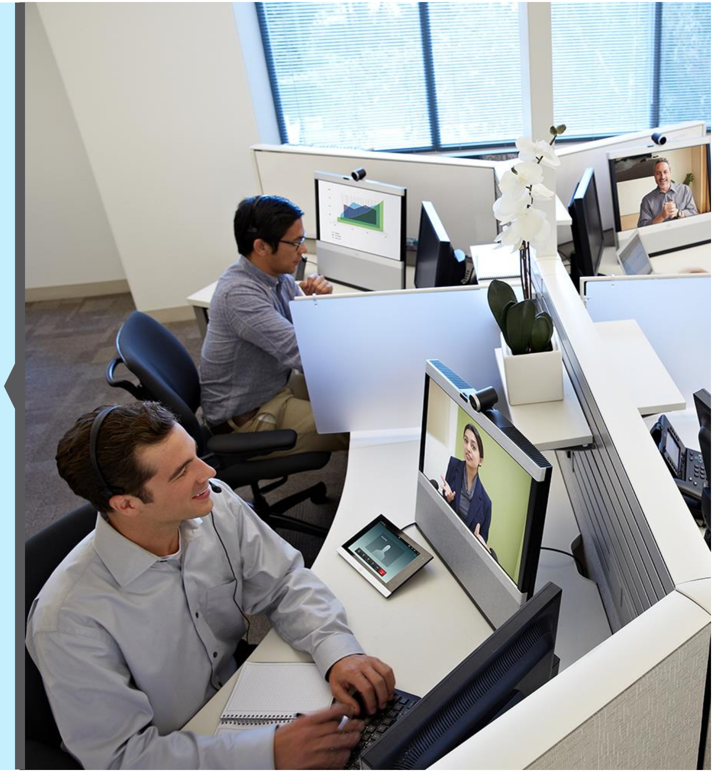
Note: This feature does not provide an intra-EPG security policy.

Use Case

- Isolate malicious virtual machines.
- Create security across zones.

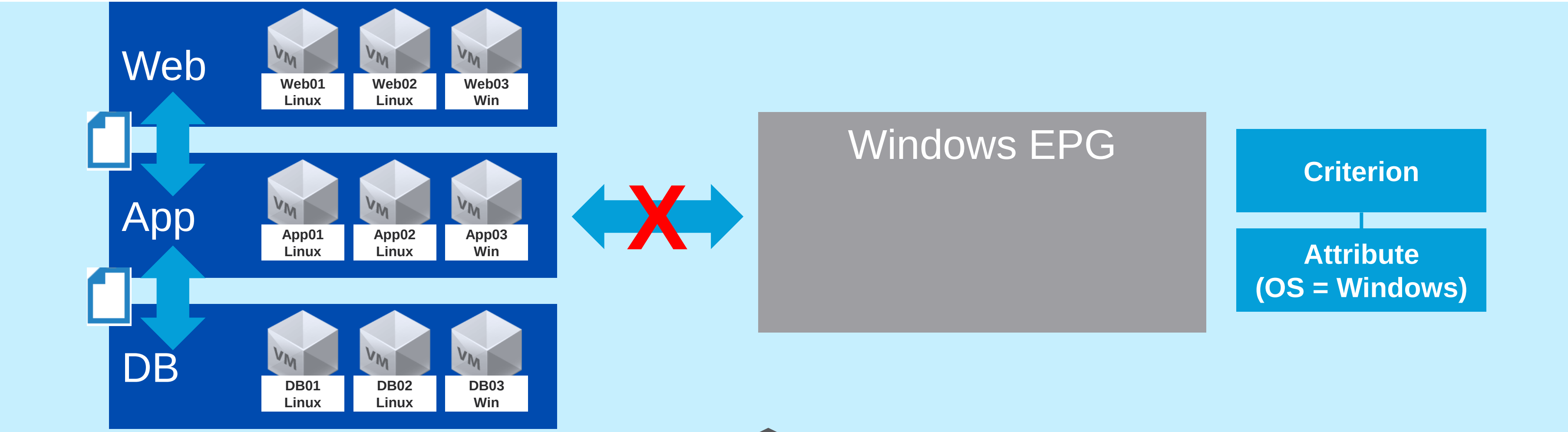
Benefits

- Without changing the port-group association of servers, additional security and segmentation can be provided.



Use Case 1

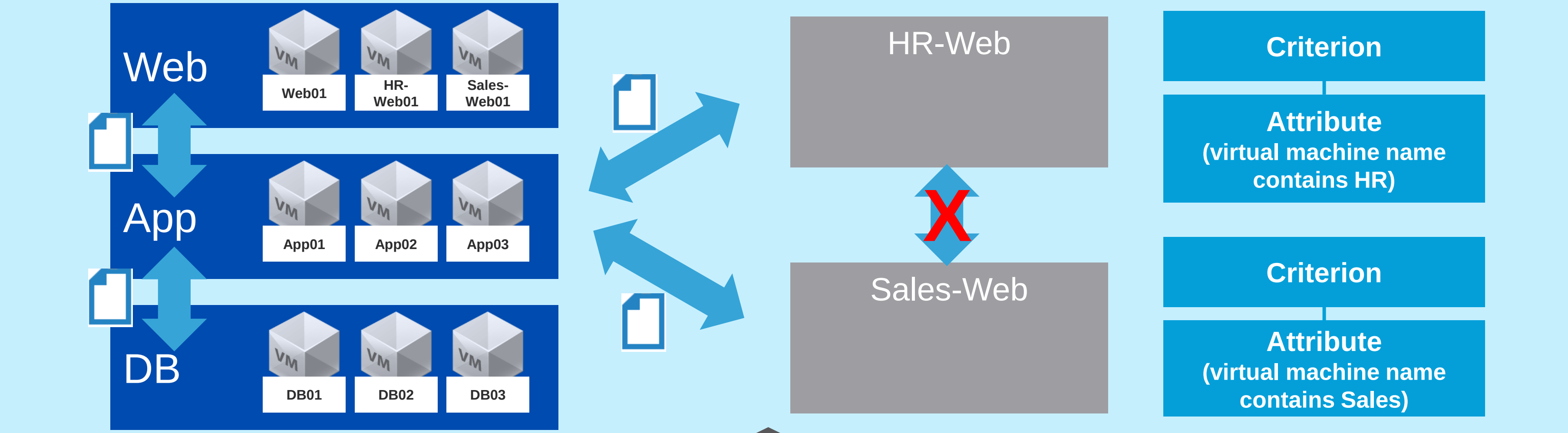
Isolate Malicious Virtual Machines



- Problem: A vulnerability is detected in a particular type of operating system (for example, Microsoft Windows). The network security administrator wants to isolate all Windows virtual machines.
- Solution: Define a security EPG with a criterion such as Operating System = Windows. No contracts are provided or consumed by this EPG. It will stop all inter-EPG communication for the matching virtual machines.
- No virtual machine attachment or detachment or placement in a different port group is needed.

Use Case 2

Security Across Zones



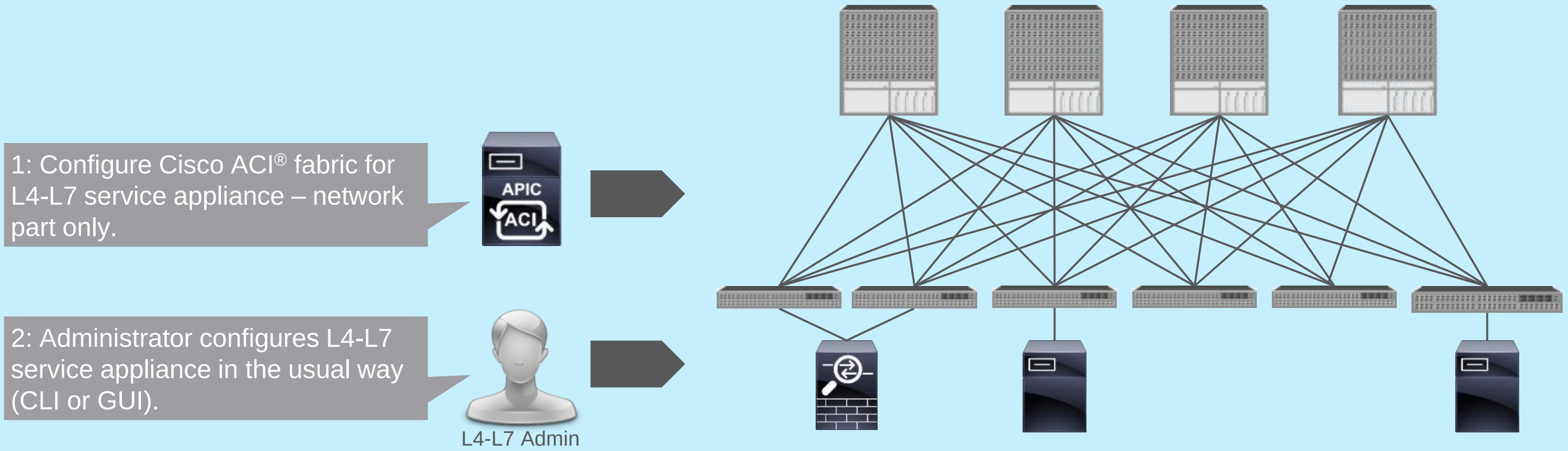
- Problem: Virtual machines belonging to different departments (for example, HR and Sales) or different roles (for example, Production and Testing) are placed in the port group. But isolation across departments is required (for example, HR-Web-VM should not be able to talk to Sales-Web-VM).
- Solution: Define EPGs that match if the virtual machine name contains a matching string (for example, HR or Sales).
- Each attribute-based EPG can have its own security policies.

Service Insertion for Any Layer 4-7 device

(No device package)

Description

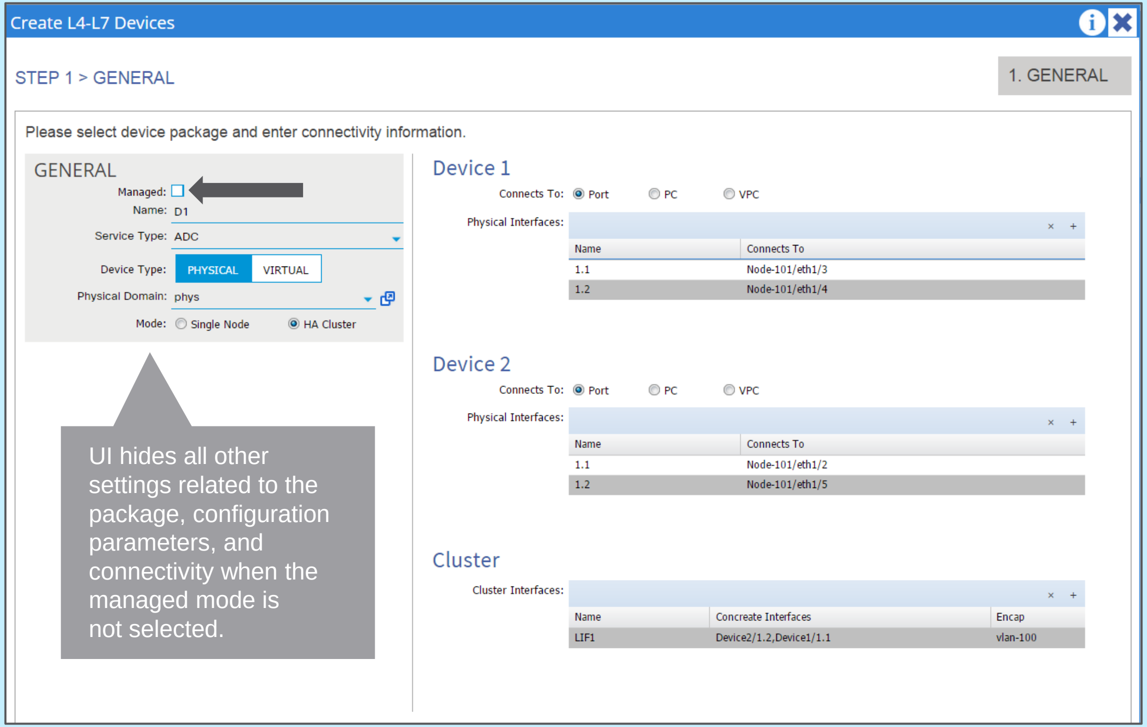
- Unmanaged L4-L7 devices to be used as service node in a service graph between EPGs.
- This approach allows the network team to handle the network automation part for the service devices with Cisco® APIC. However, configuration and management can continue to follow their current model.
- This approach also helps those L4-L7 devices for which a device package is not available.



1: Configure Cisco ACI® fabric for L4-L7 service appliance – network part only.

2: Administrator configures L4-L7 service appliance in the usual way (CLI or GUI).

Service Graph with “Unmanaged” Device



Create L4-L7 Devices

STEP 1 > GENERAL

1. GENERAL

Please select device package and enter connectivity information.

GENERAL

Managed: □

Name: D1

Service Type: ADC

Device Type: [✓ PHYSICAL] VIRTUAL

Physical Domain: phys

Mode: ○ Single Node ● HA Cluster

Device 1

Connects To: ● Port ○ PC ○ VPC

Physical Interfaces:

Name	Connects To
1.1	Node-101/eth1/3
1.2	Node-101/eth1/4

Device 2

Connects To: ● Port ○ PC ○ VPC

Physical Interfaces:

Name	Connects To
1.1	Node-101/eth1/2
1.2	Node-101/eth1/5

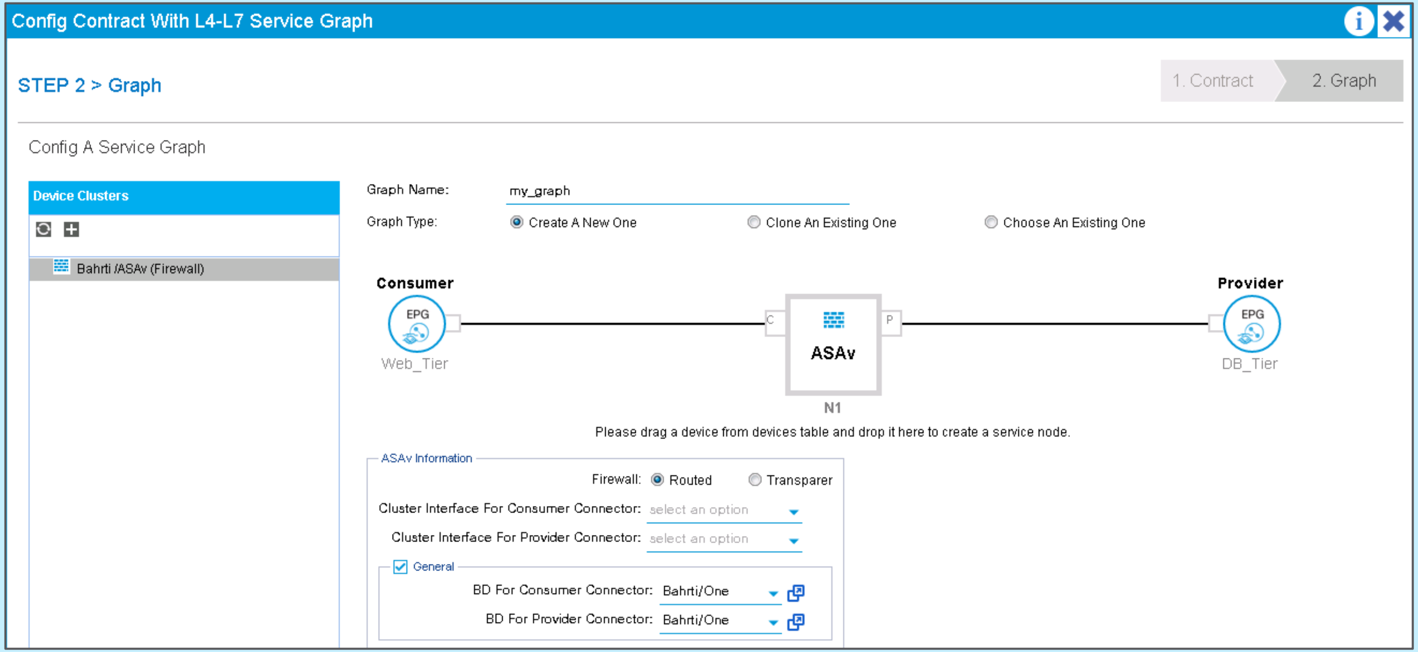
Cluster

Cluster Interfaces:

Name	Concreate Interfaces	Encap
LIF1	Device2/1.2,Device1/1.1	vlan-100

UI hides all other settings related to the package, configuration parameters, and connectivity when the managed mode is not selected.

Simplified L4-L7



Config Contract With L4-L7 Service Graph

STEP 2 > Graph

1. Contract | 2. Graph

Config A Service Graph

Device Clusters

Bahrti /ASAv (Firewall)

Graph Name: my_graph

Graph Type: ● Create A New One ○ Clone An Existing One ○ Choose An Existing One

Please drag a device from devices table and drop it here to create a service node.

ASAv Information

Firewall: ● Routed ○ Transparer

Cluster Interface For Consumer Connector: select an option

Cluster Interface For Provider Connector: select an option

☑ General

BD For Consumer Connector: Bahrti/One

BD For Provider Connector: Bahrti/One

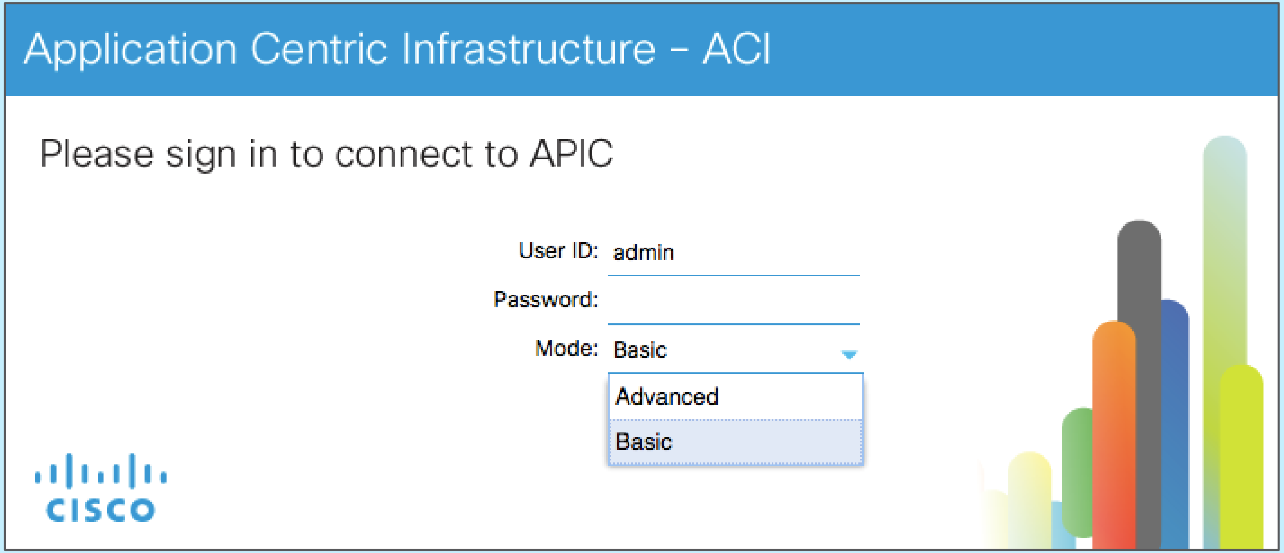
Managed and unmanaged devices can be combined in a single graph.

Troubleshooting and Operations

Basic GUI

Basic GUI

- The Basic GUI mode shows only the most commonly used features and emphasizes ease of use.
- Some features are simply not exposed: L4-L7 integration, advanced routing (L3Out), etc.



Application Centric Infrastructure – ACI

Please sign in to connect to APIC

User ID: admin

Password:

Mode: Basic

Purpose of the Basic GUI

With the Cisco ACI 1.2 release, Release 1.2(x), Cisco ACI™ introduces an alternative user interface to the existing GUI.

The goals of this GUI are as follows:

Reduce the time needed for deployment:

- Shorten the time needed to test Cisco ACI
- Provide ease of use in implementing Cisco ACI

Reduce the need for new learning:

- Provide network engineers with configurations based on current and traditional networking concepts (ACLs, VLANs, subnets, etc.) as much as possible

Switching back and forth between the Advanced and Basic GUIs is not recommended.

Address the markets for specific customers:

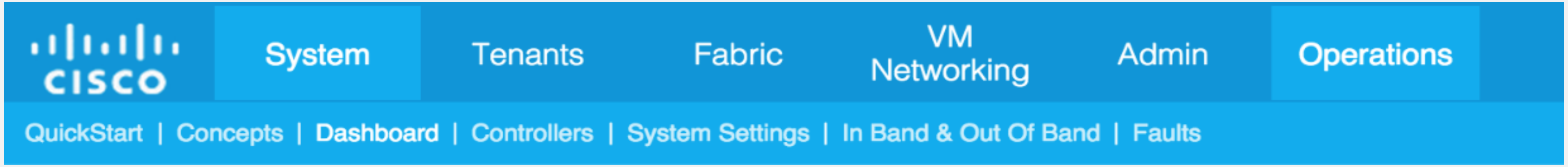
- Provide a tool for commercial customers
- Simplify the most common operations

Main Differences Between Basic and Advanced GUIs

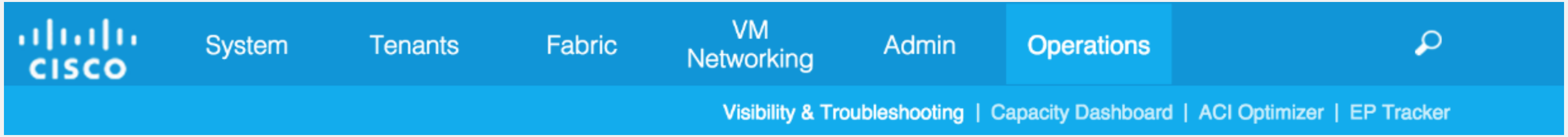
Feature	Basic GUI	Advanced GUI
Port configurations from the topology view	Yes	No
Use of switch and port selectors	No	Yes
Reuse of the same policy	No	Yes
L4-L7 device-package based	No	Yes
L4-L7 network-only stitching	Yes	Yes

Simplified Basic GUI Hierarchy

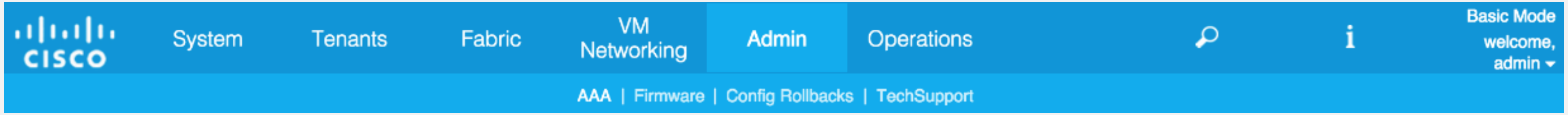
System


System
Tenants
Fabric
VM Networking
Admin
Operations
QuickStart | Concepts | Dashboard | Controllers | System Settings | In Band & Out Of Band | Faults

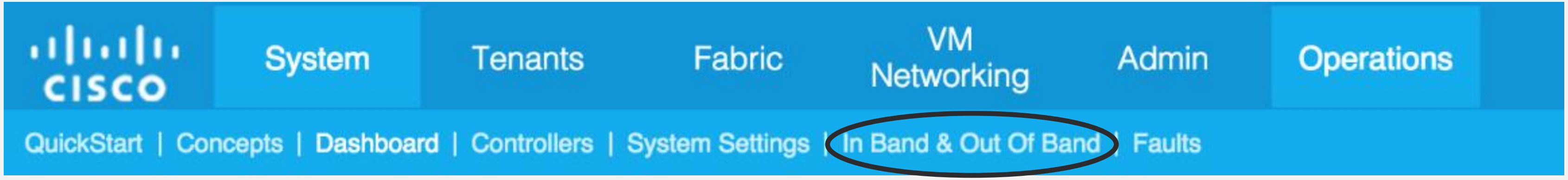
Operations


System
Tenants
Fabric
VM Networking
Admin
Operations
Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker

Administration



Inband and Out of Band

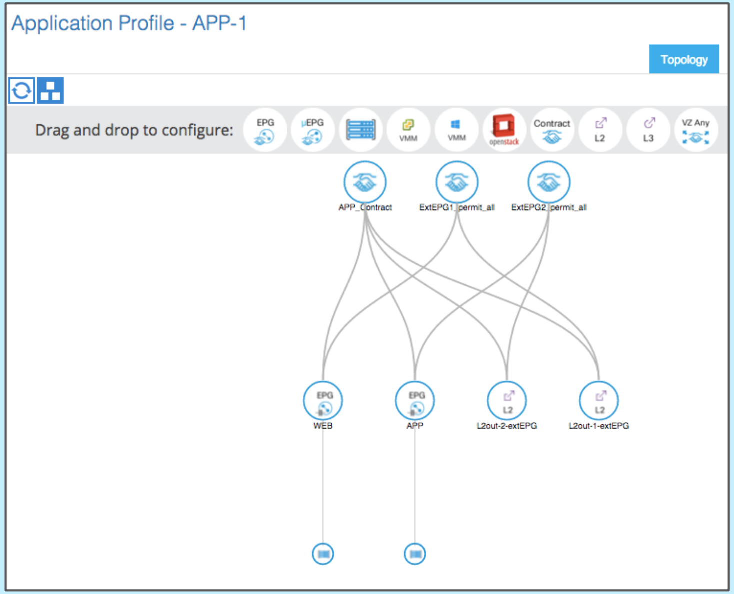

cisco
System
Tenants
Fabric
VM Networking
Admin
Operations
QuickStart | Concepts | Dashboard | Controllers | System Settings | In Band & Out Of Band | Faults

Differences with existing GUI:

- No need to use “Tenant mgmt”
- All in-band and out-of-band management configurations consolidated on a dedicated tab

Drag-and-Drop Configuration

For Both Advanced and Basic GUIs

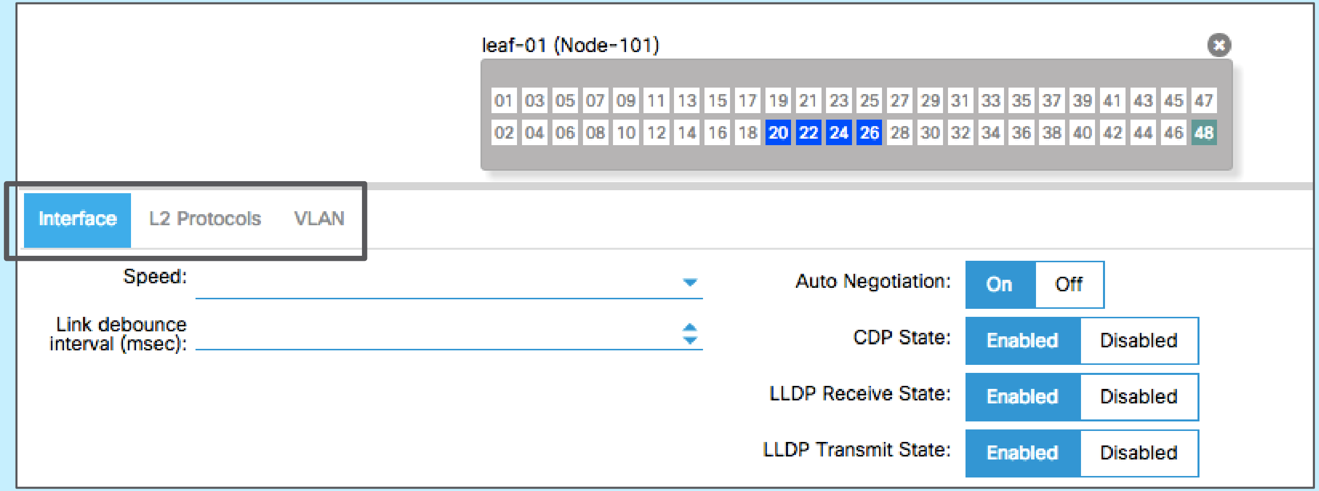


Drag-and-drop configuration is available for the following features:

- EPGs
- Attributed-based EPGs
- Association of EPG with VMM and physical domain
- Contracts
- External EPG for L2Out
- External EPG for L3Out

Simplified Interface Configuration

- One place to configure everything related to interface
- Creation of port channels and virtual port channels (vPCs)
- Interface-level configuration: speed, link debounce, LLDP, and Cisco® Discovery Protocol
- Layer 2 protocol
- VLAN and VMM domain association



leaf-01 (Node-101)

01	03	05	07	09	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
02	04	06	08	10	12	14	16	18	**20**	**22**	**24**	**26**	28	30	32	34	36	38	40	42	44	46	**48**

Interface | L2 Protocols | VLAN

Speed:

Link debounce interval (msec):

Auto Negotiation: [✓ On] Off

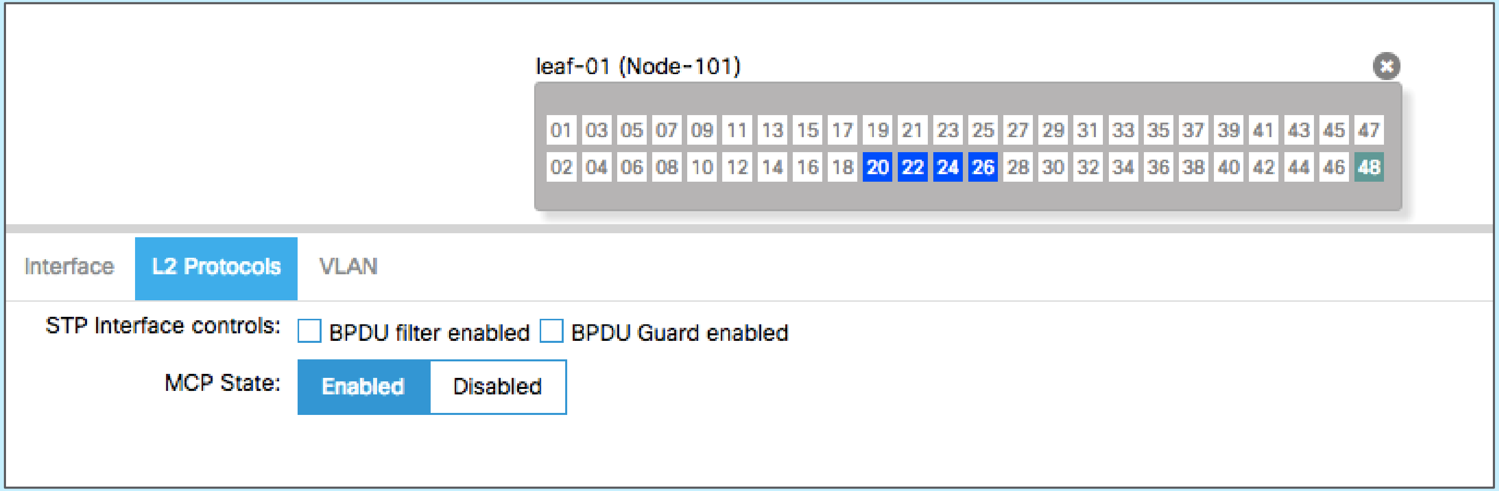
CDP State: [✓ Enabled] Disabled

LLDP Receive State: [✓ Enabled] Disabled

LLDP Transmit State: [✓ Enabled] Disabled

Simplified Interface Configuration

- One place to configure everything related to interface
- Creation of port channels and vPCs
- Interface-level configuration: speed, link debounce, LLDP, and Cisco® Discovery Protocol
- Layer 2 protocol
- VLAN and VMM domain association



leaf-01 (Node-101)

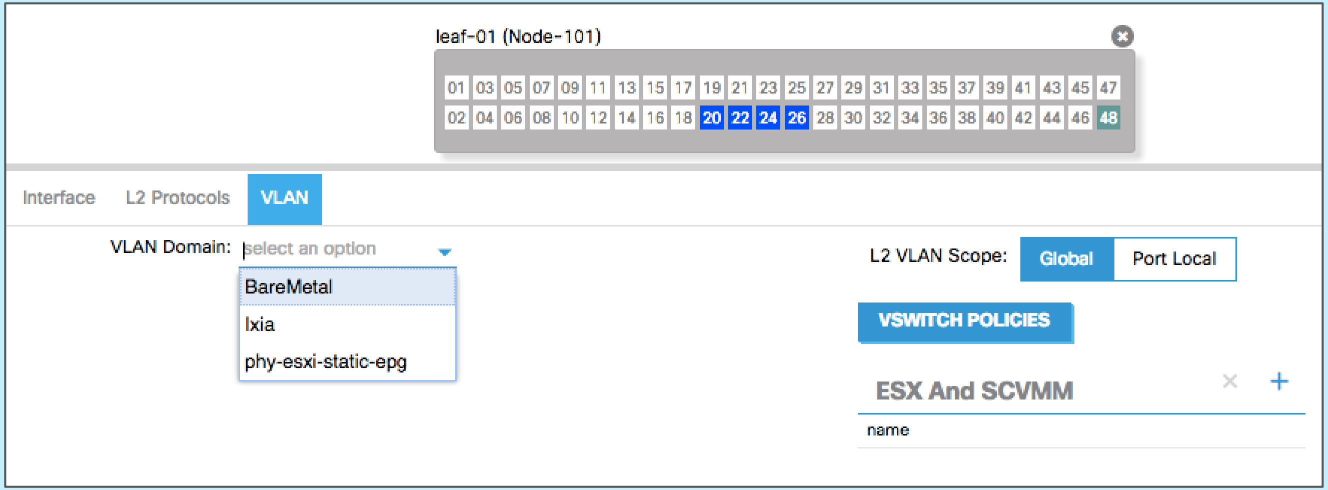
01	03	05	07	09	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
02	04	06	08	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

STP Interface controls: □ BPDU filter enabled □ BPDU Guard enabled

MCP State: [✓ Enabled] Disabled

Simplified Interface Configuration

- One place to configure everything related to interface
- Creation of port channels and vPCs
- Interface-level configuration: speed, link debounce, LLDP, and Cisco® Discovery Protocol
- Layer 2 protocol
- VLAN and VMM domain association



leaf-01 (Node-101)

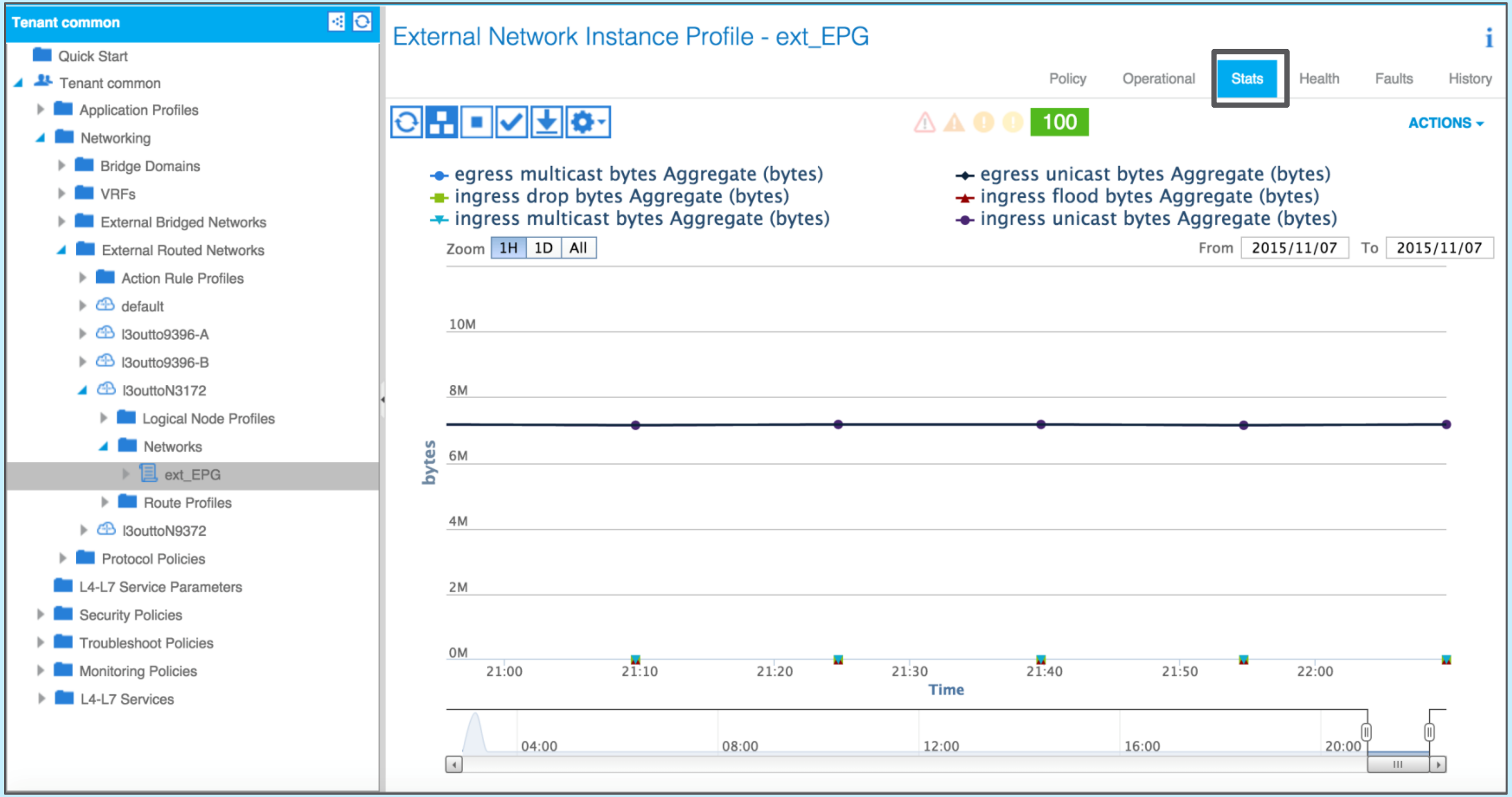
01 03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47
02 04 06 08 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48

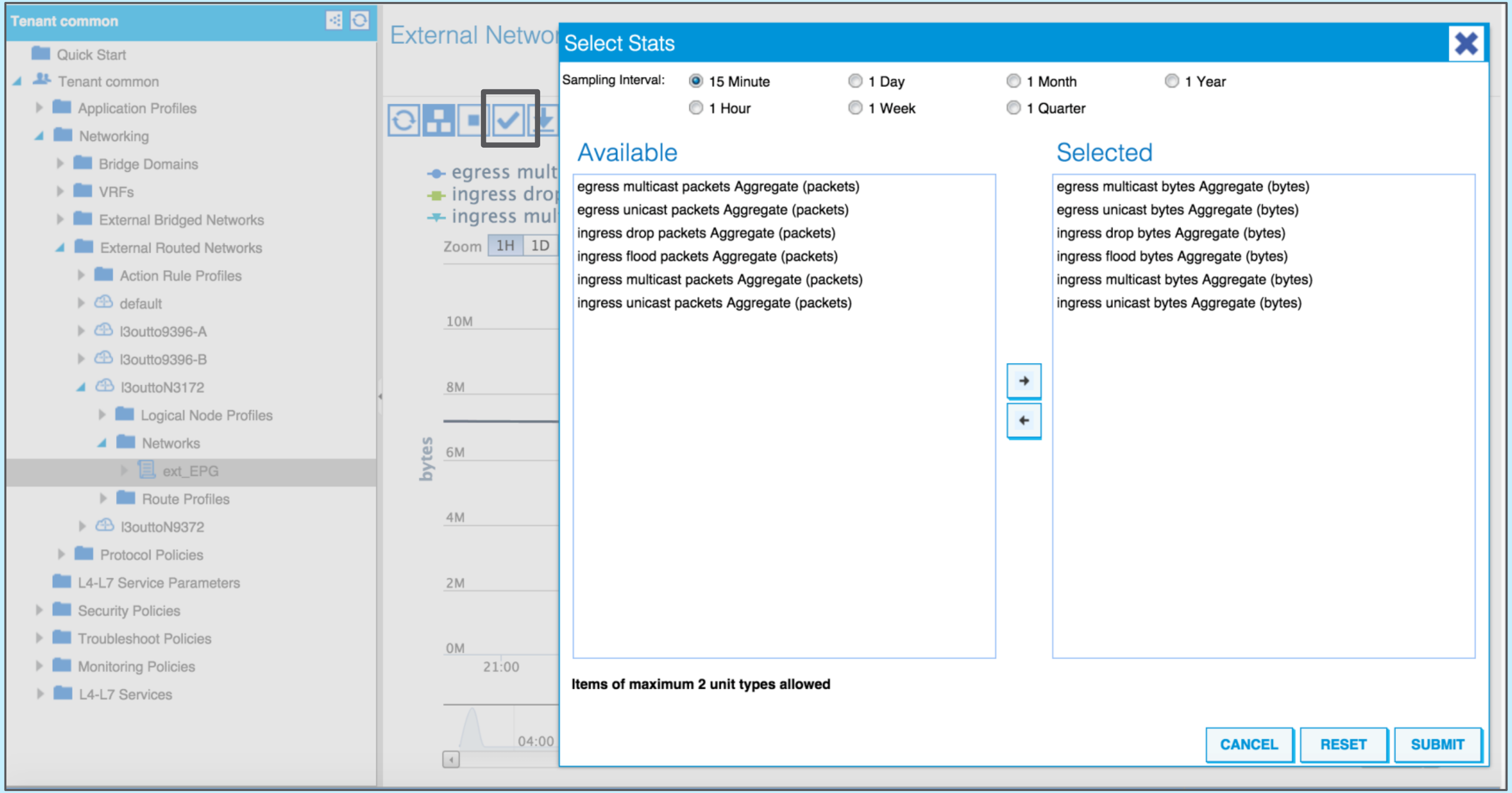
Interface | L2 Protocols | VLAN

VLAN Domain: select an option
- BareMetal
- Ixia
- phy-esxi-static-epg

L2 VLAN Scope: [✓ Global] Port Local

Statistics Through GUI


Tenant common
Quick Start
Tenant common
Application Profiles
Networking
Bridge Domains
VRFs
External Bridged Networks
External Routed Networks
Action Rule Profiles
default
l3outto9396-A
l3outto9396-B
l3outtoN3172
Logical Node Profiles
Networks
ext_EPG
Route Profiles
l3outtoN9372
Protocol Policies
L4-L7 Service Parameters
Security Policies
Troubleshoot Policies
Monitoring Policies
L4-L7 Services
External Network Instance Profile - ext_EPG
Policy
Operational
Stats
Health
Faults
History
100
ACTIONS
egress multicast bytes Aggregate (bytes)
egress unicast bytes Aggregate (bytes)
ingress drop bytes Aggregate (bytes)
ingress flood bytes Aggregate (bytes)
ingress multicast bytes Aggregate (bytes)
ingress unicast bytes Aggregate (bytes)
Zoom
1H
1D
All
From
2015/11/07
To
2015/11/07
10M
8M
6M
4M
2M
0M
bytes
21:00
21:10
21:20
21:30
21:40
21:50
22:00
Time
04:00
08:00
12:00
16:00
20:00



Select Stats

Sampling Interval: ● 15 Minute ○ 1 Day ○ 1 Month ○ 1 Year ○ 1 Hour ○ 1 Week ○ 1 Quarter

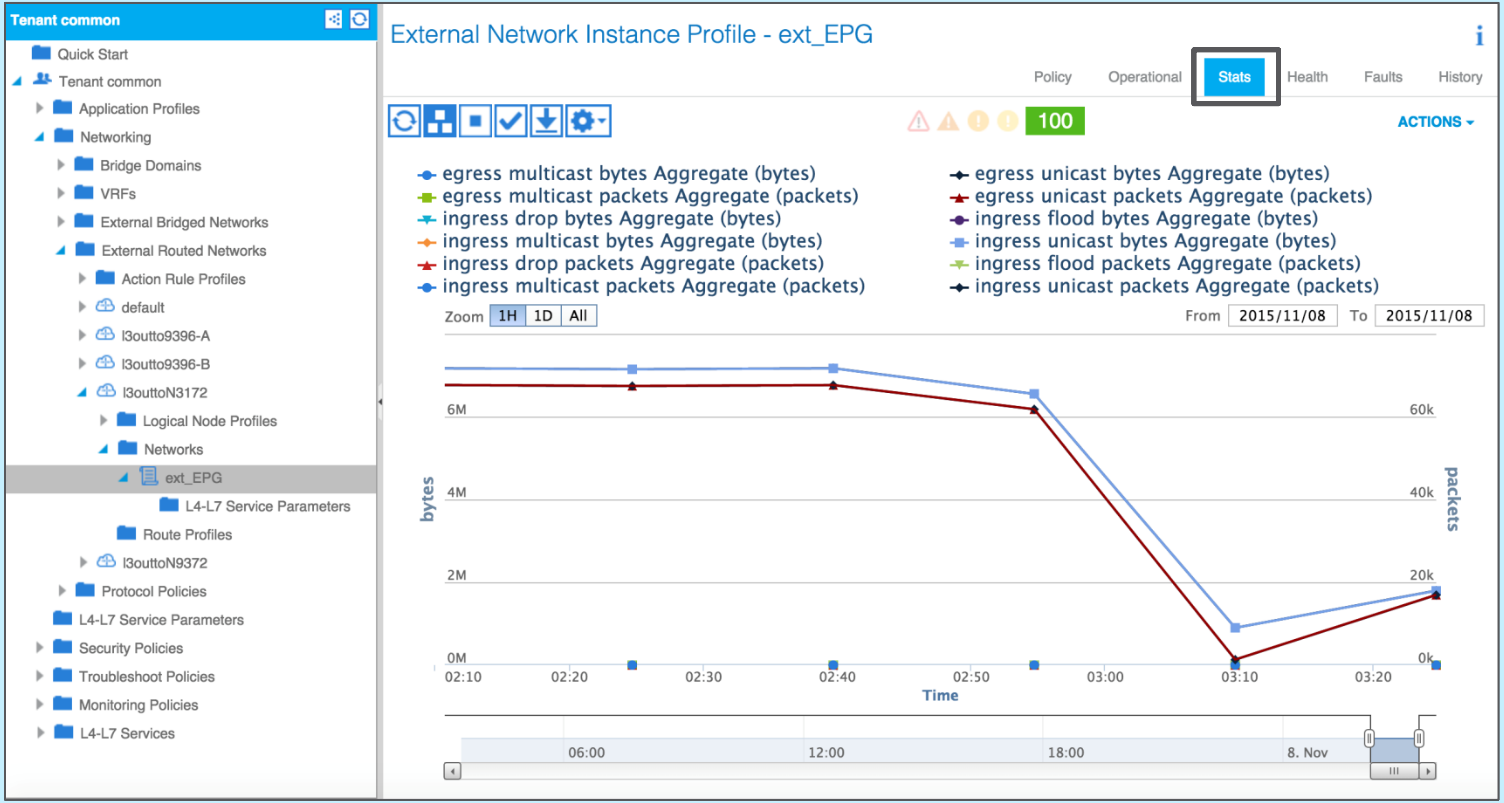
Available

egress multicast packets Aggregate (packets)
egress unicast packets Aggregate (packets)
ingress drop packets Aggregate (packets)
ingress flood packets Aggregate (packets)
ingress multicast packets Aggregate (packets)
ingress unicast packets Aggregate (packets)

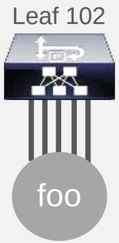
Selected

egress multicast bytes Aggregate (bytes)
egress unicast bytes Aggregate (bytes)
ingress drop bytes Aggregate (bytes)
ingress flood bytes Aggregate (bytes)
ingress multicast bytes Aggregate (bytes)
ingress unicast bytes Aggregate (bytes)

Items of maximum 2 unit types allowed


Tenant common
Quick Start
Tenant common
Application Profiles
Networking
Bridge Domains
VRFs
External Bridged Networks
External Routed Networks
Action Rule Profiles
default
l3outto9396-A
l3outto9396-B
l3outtoN3172
Logical Node Profiles
Networks
ext_EPG
L4-L7 Service Parameters
Route Profiles
l3outtoN9372
Protocol Policies
L4-L7 Service Parameters
Security Policies
Troubleshoot Policies
Monitoring Policies
L4-L7 Services
External Network Instance Profile - ext_EPG
Policy
Operational
Stats
Health
Faults
History
100
ACTIONS
egress multicast bytes Aggregate (bytes)
egress multicast packets Aggregate (packets)
ingress drop bytes Aggregate (bytes)
ingress multicast bytes Aggregate (bytes)
ingress drop packets Aggregate (packets)
ingress multicast packets Aggregate (packets)
egress unicast bytes Aggregate (bytes)
egress unicast packets Aggregate (packets)
ingress flood bytes Aggregate (bytes)
ingress unicast bytes Aggregate (bytes)
ingress flood packets Aggregate (packets)
ingress unicast packets Aggregate (packets)
Zoom 1H 1D All
From 2015/11/08 To 2015/11/08
bytes
6M
4M
2M
0M
packets
60k
40k
20k
0k
02:10
02:20
02:30
02:40
02:50
03:00
03:10
03:20
Time
06:00
12:00
18:00
8. Nov

Cisco NX-OS Style of CLI on Cisco APIC



```
(config)# leaf 102
(config-leaf)# interface port-channel foo
(config-leaf-if)# no shut
```

Configuring port channels

Leaf 101
Leaf 102
Eth 1/1-48
Eth 1/1-48

```
demo-apic1(fabric-exec)# show mac address-table address
---------------------------------------------------------------
 Node leaf101 Output:
 --------------------------------------------------------------
VLAN     MAC Address       Type      age     Secure     Ports
---------+----------------+--------+---------+------+---------+---------+
•  102      4403.a77a.547c    dynamic      -       F    F    po8
---------------------------------------------------------------
```

Searching the MAC address table in leaf switches

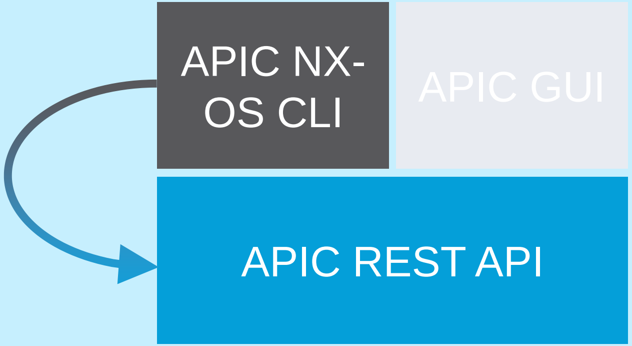
```
demo-apic1# show running-config tenant t1
tenant t1
  vrf context v1
  bridge-domain bd1
    vrf member v1
  exit
```

Showing the configuration for a tenant and leaf

Overview

Cisco® NX-OS style of CLI runs on the Cisco APIC, **not** on the leaf and spine switches.

- The APIC NX-OS style of CLI reuses the **exact** same REST API as used by the GUI.
- The **show version** and **show running** commands are back (you can view the entire running configuration).



Command Output

```
azesulem$ ssh admin@172.31.218.86
Application Policy Infrastructure Controller
admin@172.31.218.86's password:
apic1#
```

```
apic1# show version
 Role                   Id                     Name                         Version
 ----------             ----------        ------------------------          --------------------
 controller             1                      apic1                        1.2(0.245)
 controller             2                      apic2                        1.2(0.245)
 controller             3                      apic3                        1.2(0.245)
 leaf                   101                    leaf1                        n9000-11.2(0.83)
 leaf                   102                    leaf2                        n9000-11.2(0.83)
 leaf                   103                    leaf3                        n9000-11.2(0.83)
 spine                  104                    spine1                       n9000-11.2(0.83)
 spine                  105                    spine2                       n9000-11.2(0.83)
```

Cisco NX-OS Style of CLI on Cisco APIC

- Use CLI with Cisco® NX-OS look and feel to create tenants, VRF instances, and bridge domains.
- Use CLI to enable distributed anycast gateway for the bridge domain.

```
apic1# config terminal
apic1(config)#
apic1(config)# tenant test-tenant-cli
apic1(config-tenant)# vrf context vrf-cli
apic1(config-tenant)# bridge-domain BD-1
apic1(config-tenant-bd)# vrf member vrf-cli
apic1(config-tenant-bd)# unicast routing
apic1(config-tenant-bd)# arp flooding

apic1(config-tenant)# interface bridge-domain BD-1
apic1(config-tenant-interface)# ip address 7.7.7.1/24
```

Cisco NX-OS Style of CLI on Cisco APIC

EPG and Contract

- Create contracts.
- Create EPGs. Associate EPGs with bridge domains and VMM domains. Apply contracts.

```
apic1(config-tenant)# access-list nfs
apic1(config-tenant-acl)# match arp
apic1(config-tenant-acl)# match icmp
apic1(config-tenant-acl)# match tcp dest 111
apic1(config-tenant)# contract NFS_contract
apic1(config-tenant-contract)# subject nfs
apic1(config-tenant-contract-subj)# access-group nfs out
apic1(config-tenant)# application app-1
apic1(config-tenant-app)# epg WEB
apic1(config-tenant-app-epg)# bridge-domain member BD-1
apic1(config-tenant-app-epg)# vmware-domain member DC1
apic1(config-tenant-app-epg)# contract consumer NFS_contract
```

Cisco NX-OS Style of CLI on Cisco APIC

L3Out

- External EPG and route map are under configuration context “tenant.”
- Interface and protocol configurations are under configuration context “leaf.”

```
apic1(config)#leaf 103
apic1(config-leaf)# interface ethernet 1/40.628
apic1(config-leaf-if)# vrf member tenant test-tenant-cli vrf vrf-cli
apic1(config-leaf-if)# ip address 77.77.77.1/30

apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant test-tenant-cli vrf vrf-cli
apic1(config-leaf-ospf-vrf)# area 20 nssa
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit

apic1(config-leaf)# interface ethernet 1/40.628
apic1(config-leaf-if)# ip router ospf default area 20
apic1(config-leaf-if)# mtu 1500
```

Cisco NX-OS Style of CLI on Cisco APIC

Show Commands

- Check fabric, tenant, and related configurations.
- Run **show** command on multiple leaf switches and get results in one window.
- See notes for sample output from CLI.

```
apic1# show running-config tenant

apic1# show endpoints | grep 192.168.1.100
 Tenant2     App1         WEB         00:50:56:94:97:FF  192.168.1.100
102         eth1/11                         vlan-153         not-applicable


apic1# fabric 102-103 show vpc
apic1# fabric 102-103 show system internal epm vlan all
apic1# fabric 102-103 show ip ospf neighbors vrf all
```

Configuration Rollback

You can use configuration rollback to undo the changes made between two snapshots. Objects are processed as follows:

- Deleted managed objects are re-created.
- Created managed objects are deleted.
- Modified managed objects are reverted to their prior state.

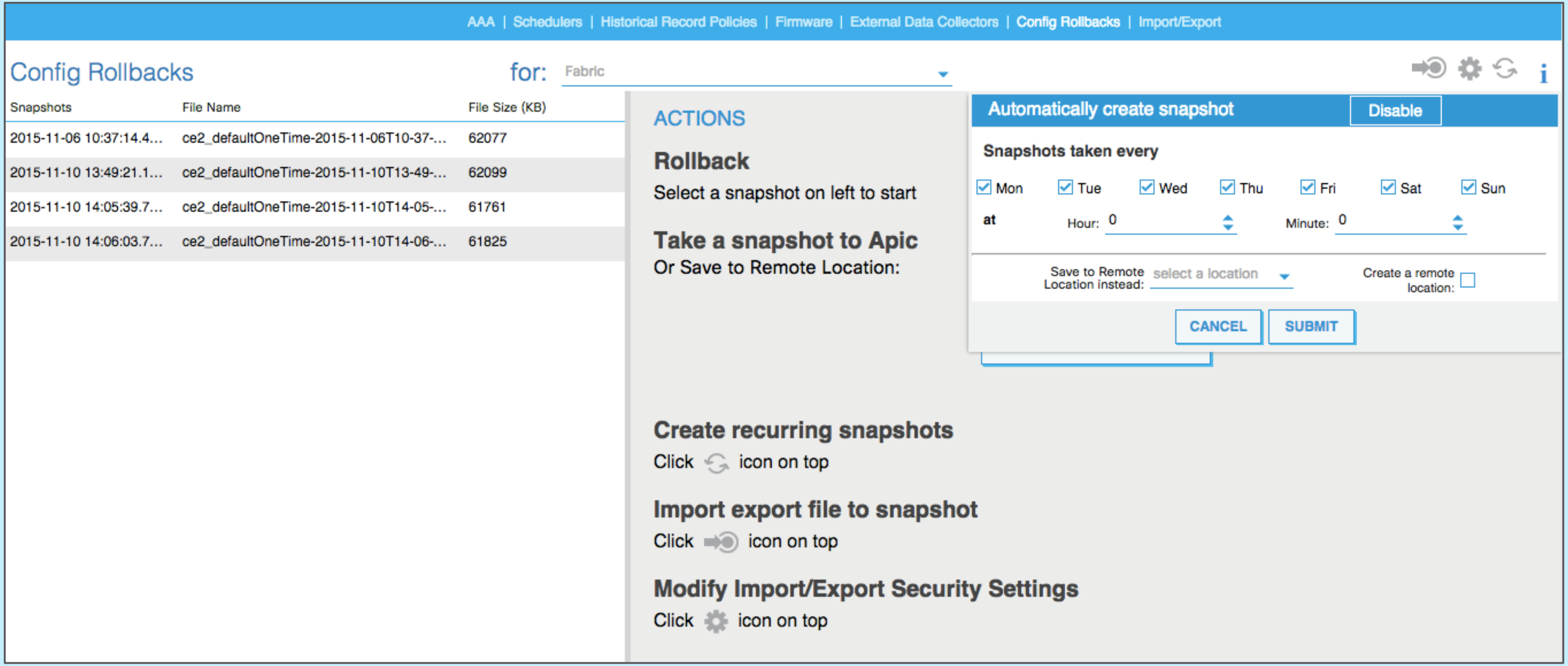
Remote archives are not supported.

Diff Tool

- A special REST API is available that shows the differences between two snapshots:

apichost/mqapi2/snapshots.diff.xml?s1dn=SNAPSHOT_ONE_DN&s2dn=SNAPSHOT_TWO_DN

Configuration Rollback



AAA | Schedulers | Historical Record Policies | Firmware | External Data Collectors | Config Rollbacks | Import/Export

Config Rollbacks for: Fabric

Snapshots	File Name	File Size (KB)
2015-11-06 10:37:14.4...	ce2_defaultOneTime-2015-11-06T10-37-...	62077
2015-11-10 13:49:21.1...	ce2_defaultOneTime-2015-11-10T13-49-...	62099
2015-11-10 14:05:39.7...	ce2_defaultOneTime-2015-11-10T14-05-...	61761
2015-11-10 14:06:03.7...	ce2_defaultOneTime-2015-11-10T14-06-...	61825

ACTIONS

Rollback

Select a snapshot on left to start

Take a snapshot to Apic

Or Save to Remote Location:

Automatically create snapshot Disable

Snapshots taken every

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

at Hour: 0 Minute: 0

Save to Remote Location instead: select a location

Create a remote location: □

CANCEL SUBMIT

Create recurring snapshots

Click ⟳ icon on top

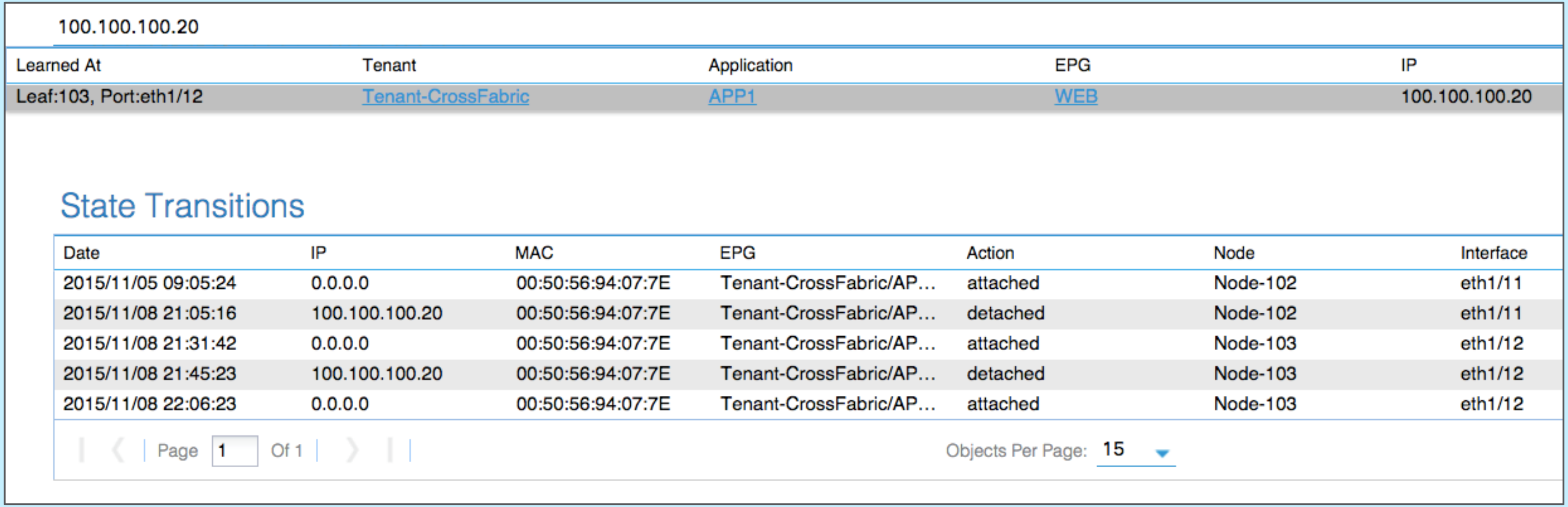
Import export file to snapshot

Click ➔◉ icon on top

Modify Import/Export Security Settings

Click ⚙ icon on top

Endpoint Tracker



100.100.100.20

Learned At	Tenant	Application	EPG	IP
Leaf:103, Port:eth1/12	Tenant-CrossFabric	APP1	WEB	100.100.100.20

State Transitions

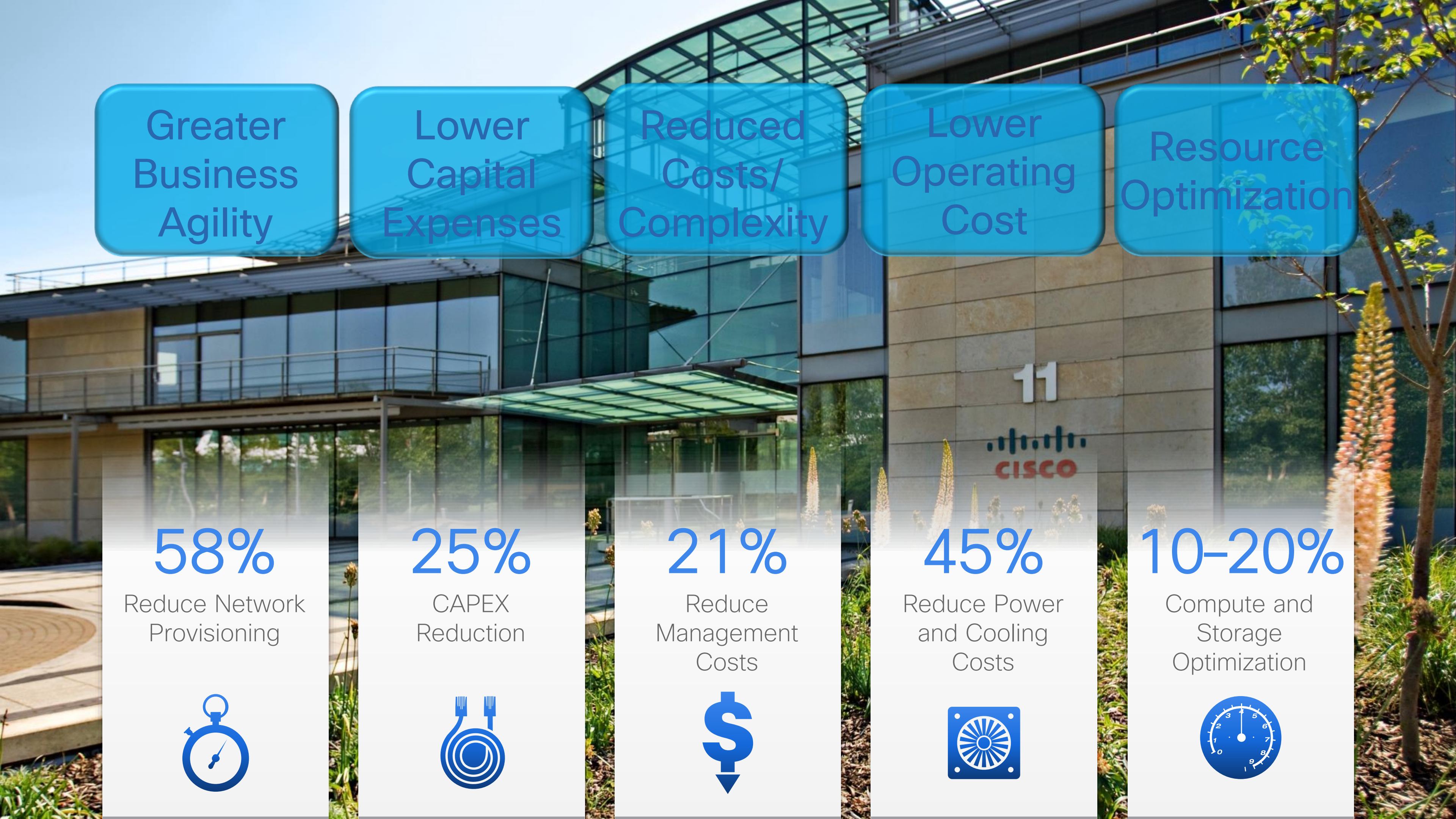
Date	IP	MAC	EPG	Action	Node	Interface
2015/11/05 09:05:24	0.0.0.0	00:50:56:94:07:7E	Tenant-CrossFabric/AP...	attached	Node-102	eth1/11
2015/11/08 21:05:16	100.100.100.20	00:50:56:94:07:7E	Tenant-CrossFabric/AP...	detached	Node-102	eth1/11
2015/11/08 21:31:42	0.0.0.0	00:50:56:94:07:7E	Tenant-CrossFabric/AP...	attached	Node-103	eth1/12
2015/11/08 21:45:23	100.100.100.20	00:50:56:94:07:7E	Tenant-CrossFabric/AP...	detached	Node-103	eth1/12
2015/11/08 22:06:23	0.0.0.0	00:50:56:94:07:7E	Tenant-CrossFabric/AP...	attached	Node-103	eth1/12

Page 1 Of 1

Objects Per Page: 15

Power of
Cisco ACI

- Automation
- Investment Protection
- Open
- Visibility
- Security
- Lowering OPEX and TCO



Greater Business Agility

58%

Reduce Network Provisioning

Lower Capital Expenses

25%

CAPEX Reduction

Reduced Costs/ Complexity

21%

Reduce Management Costs

Lower Operating Cost

45%

Reduce Power and Cooling Costs

Resource Optimization

10–20%

Compute and Storage Optimization

“If you don’t like change, you’re going to like irrelevance even less.”

General Eric Shinseki

Back-up

Brazos M1 Release

Target Q1 CY 2016

Shipping!

Infrastructure

Hardware: 9372TX-E

- 3-site Stretched fabric + RR increase

Routing & Switching

- DSCP marking for traffic based on protocol
- IPv6 Management
- BFD – v4 and v6 for external links
- EIGRPv6 support
- OSPF forward address suppression

Routing & Switching

- BGP knobs (Set Attributes, Dynamic Neighbors, Route Dampening, weight attribute, remove-private-as, Route Aggregation)
- QoS Policing (support on T2)

Security

- Intra-EPG isolation policy for Bare Metal and VMWare vDS

Virtualization, Operations

- Spine L3 In-band connectivity
- SNMP traps for APIC
- AVS Features
  - (1) Stretched Fabric (incl 3-sites)
  - (2) IPv6 Management
  - (3) 96 ports usable per leaf
- Cluster Manager for Services – Sourcefire, PANW, F5
- WAP - IP Pool Manager integration

Openstack

- OpenStack Kilo (Plugin only)
- Installer support (Plugin only) Red Hat, Mirantis

Bronx Release

Target Q2 CY 2016

Execute Committed

Hardware

Nexus 9500 – 100G

- Fabric Module for 8 and 4-slot (E)
- Line cards: 32p 40/100G (EX)

N9K-X9732C-EX

Nexus 9300 TOR

93180YC-EX
(48p 10/25G + 6p 100G)

Software

- IP Based EPG support on N93xx-EX
- Vmware vDS Micro-segmentation on 9300-EX
- Vmware AVS intra-EPG isolation