CISCO

You make **possible**

Your First Seven Days Of ACI

Joseph Ristaino – Technical Leader, DCBU ACI Escalation
Carlo Schmidt – Technical Leader – ACI Solution Support

BRKACI-1001

Agenda

- Day 1: Why ACI?
- Day 2: Infrastructure and Policies
- Day 3: Forwarding Overview
- Day 4: Network Centric Migrations
- Day 5: Multi Location Deployments
- Day 6: Troubleshooting Tools
- Day 7: Additional Resources

Cisco Webex Teams

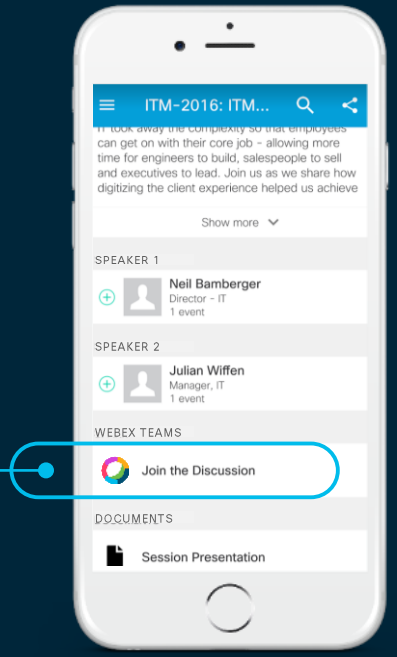
Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 16, 2019.



cs.co/ciscolivebot#BRKACI-1001

Acronyms/Definitions

Reference Slide Icon ➔

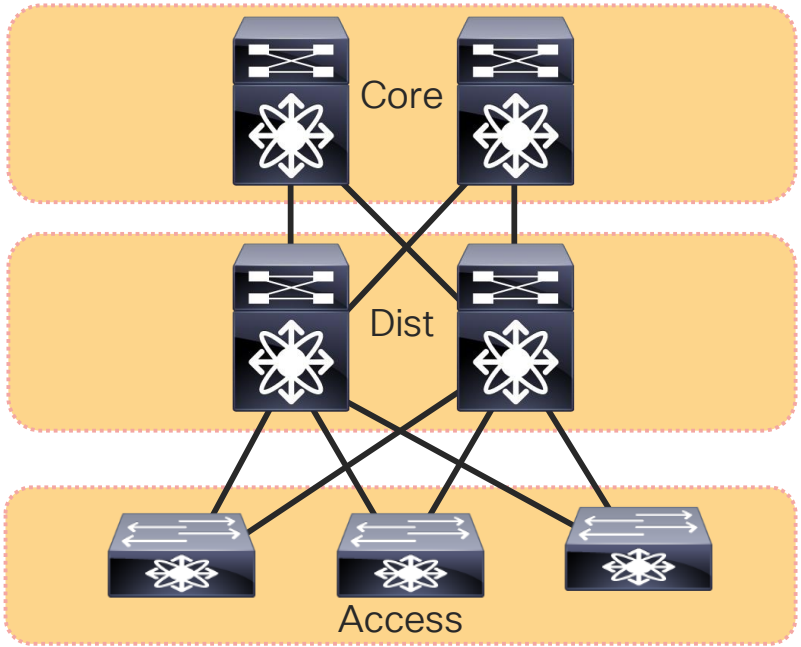
Acronyms	Definitions	Acronyms	Definitions
ACI	Application Centric Infrastructure	SVI	Switch Virtual Interface
ACL	Access Control List	VIC	Virtual Interface Card
API	Application Programming Interface	VNID	Virtual Network Identifier
APIC	Application Policy Infrastructure Controller	VPC	Virtual Port-Channel
BD	Bridge Domain	VRF	Virtual Routing and Forwarding
COOP	Council of Oracle Protocol	VTEP	VXLAN Tunnel Endpoint
ECMP	Equal Cost Multi Pathing	VXLAN	Virtual Extensible LAN
EP	Endpoint		
EPG	Endpoint Group		
KVM	Keyboard, Video, and Mouse		
MP-BGP	Multi Protocol BGP		
pcTag	Policy Control Tag		

Day 1: Why ACI?

You make networking **possible**

Why ACI?

Challenges of Today



Management

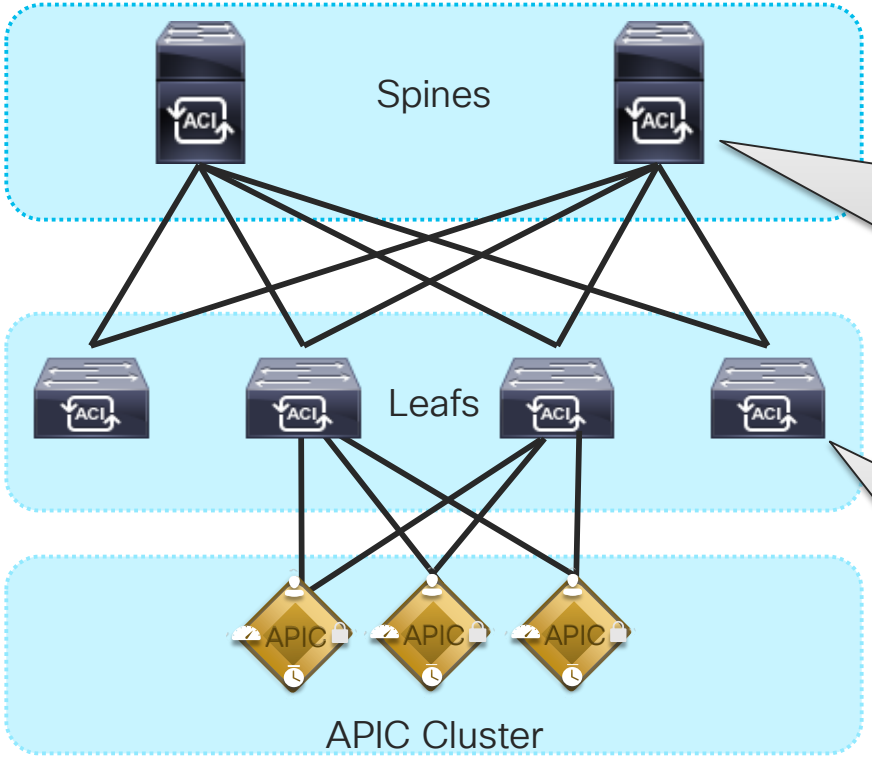
- CLI to every Device
- Manual Configuration – Takes Time
- Coordination between Network and Server Team
- Harder as we scale!

Functionality

- Static Configuration
- Allow all Traffic by Default
- Spanning Tree to Prevent Loops

Why ACI?

ACI Overview



Application Centric Infrastructure

Software Defined Networking built on Nexus 9000

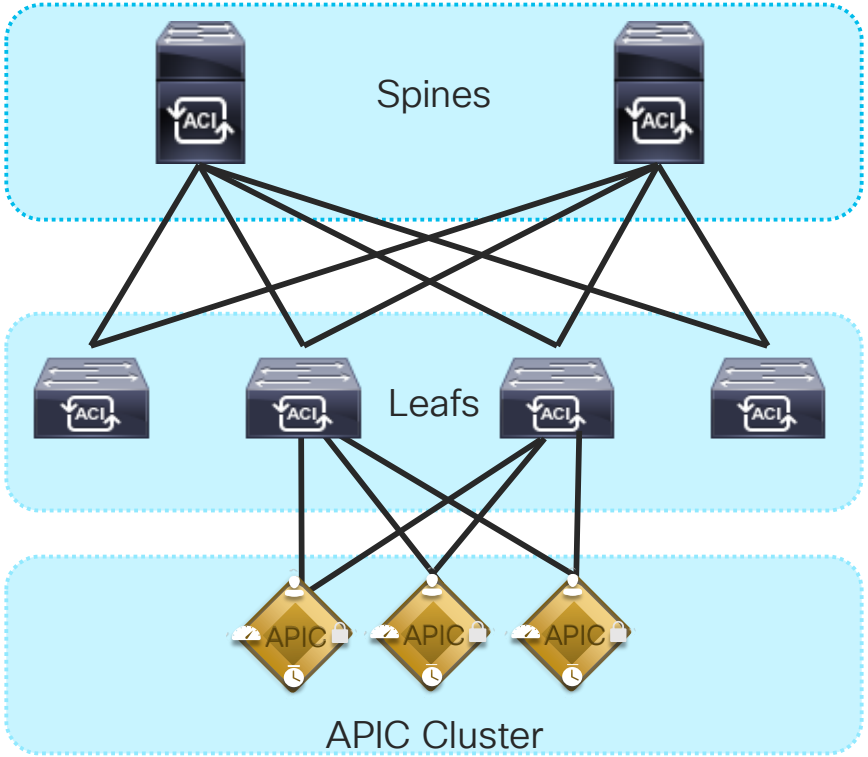
Control Plane is Decoupled From the Data Plane

```
Spine1# show module
Mod  Ports  Module-Type                          Model           Status
---  -----  ----------------------------------- --------------- ------
2    32     32p 40/100G Ethernet Module          N9K-X9732C-EX     ok
22   0      Fabric Module                        N9K-C9504-FM-E    ok
23   0      Fabric Module                        N9K-C9504-FM-E    ok
24   0      Fabric Module                        N9K-C9504-FM-E    ok
26   0      Fabric Module                        N9K-C9504-FM-E    ok
27   0      Supervisor Module                    N9K-SUP-A       Active
28   0      Supervisor Module                    N9K-SUP-A       Standby
```

```
Leaf4# show module


Mod  Ports  Module-Type                          Model             Status
---  -----  ----------------------------------- ------------------ ------
----
1    54     48x10/25G+6x40/100G Switch          N9K-C93180YC-EX     ok
```

What is ACI?

ACI Overview



Management

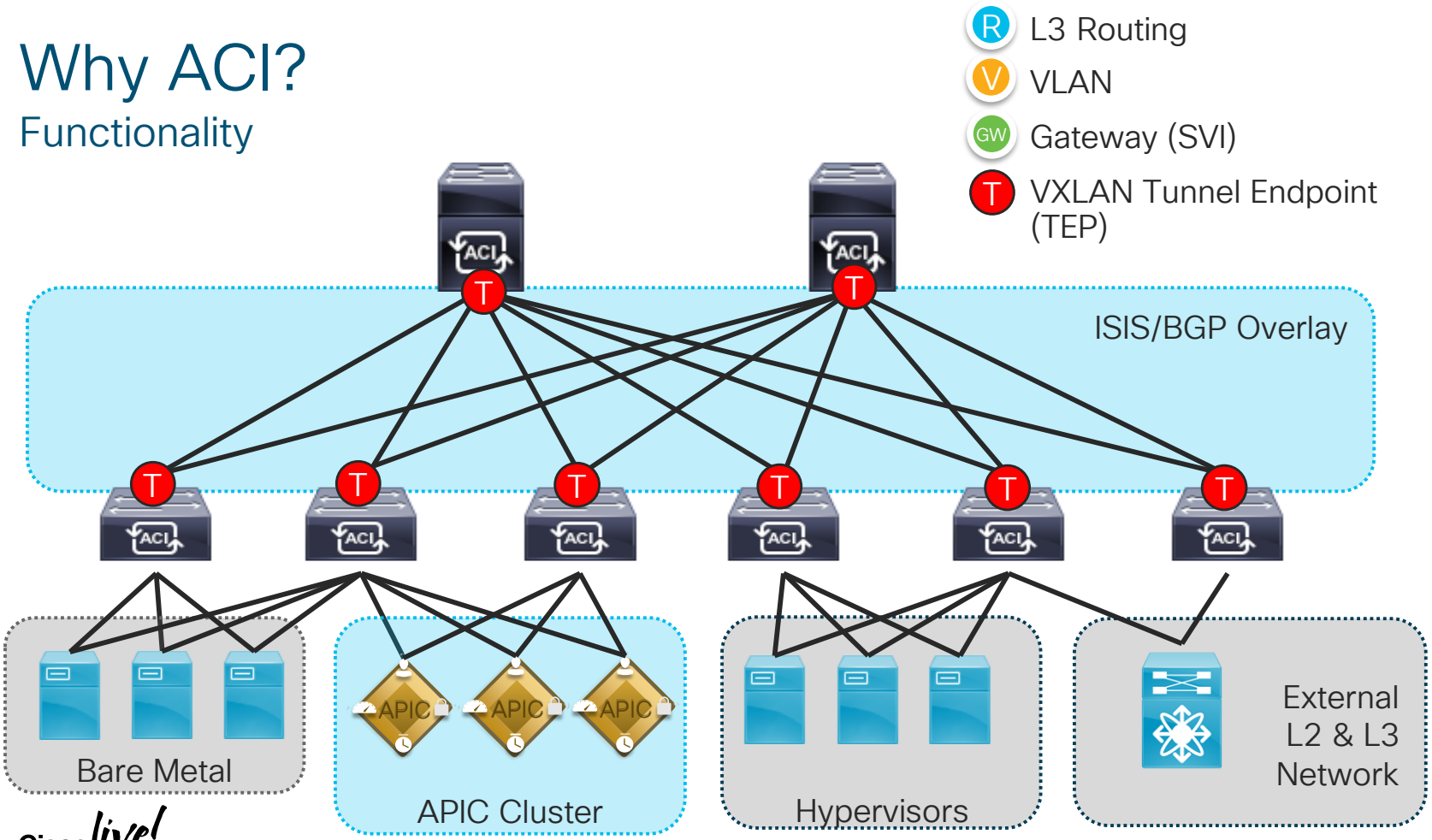
- Fabric is managed by APIC
- All configuration exposed via API
- Switches join fabric in a few clicks!

Functionality

- No spanning Tree – ECMP Routing
- Dynamic Configuration
- Whitelist Model (customizable)

Why ACI?

Functionality



Why ACI?

Functionality

A layer 3 network running ISIS is configured automatically by your APIC cluster to provide a routed underlay network between leafs and spines – **user does not have to understand and build underlay**

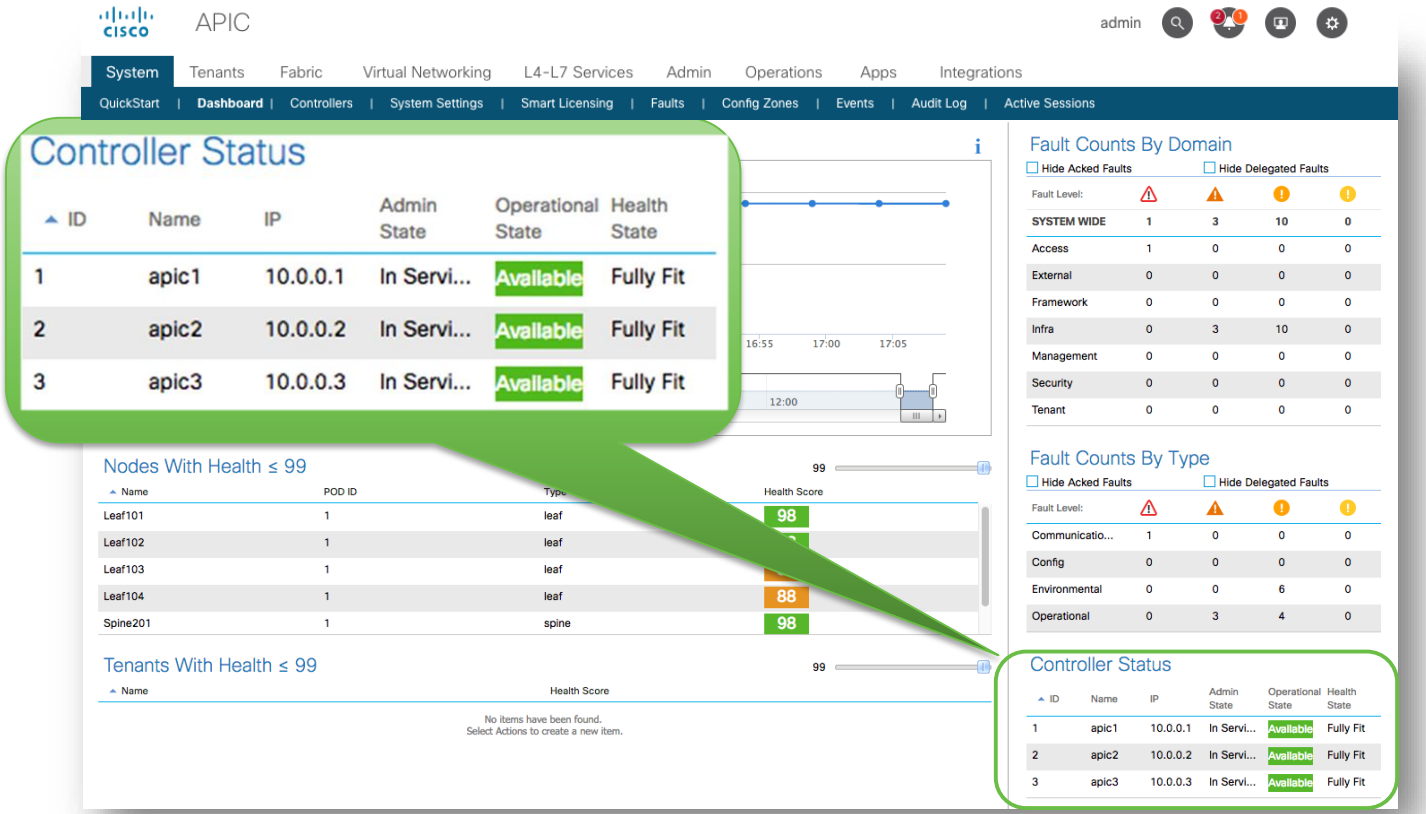
A overlay network is built using a enhanced version of VXLAN to allow layer 2 switching across the fabric as well as per VRF routing across the fabric – **user does not have to understand how to build overlay**

VXLAN VNIDs are used to separate layer 2 switching as well as layer 3 routing

Why ACI?

Management Overview

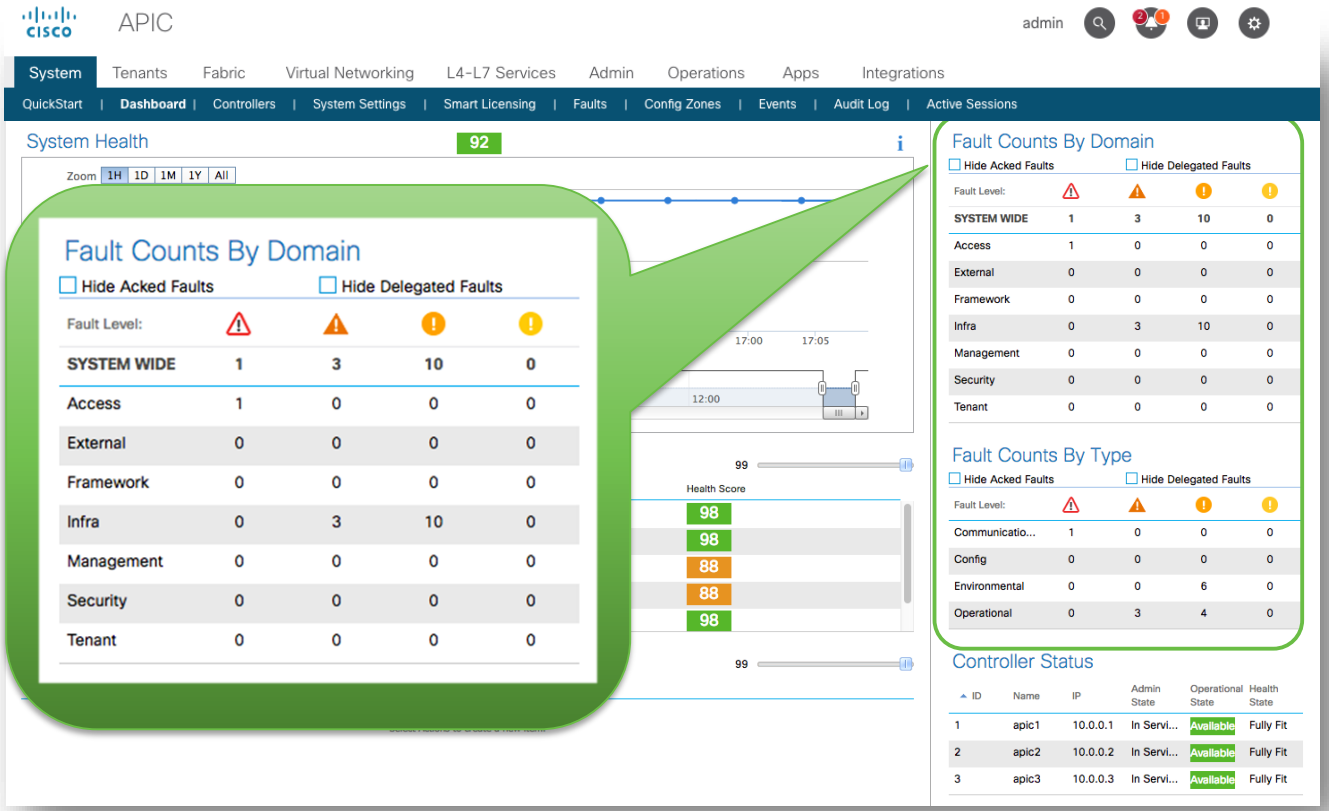
- GUI gives full visibility into the entire system
- Controller status shows state of the APIC Cluster.
- “Fully Fit” means all APIC’s are in sync and communicating



Why ACI?

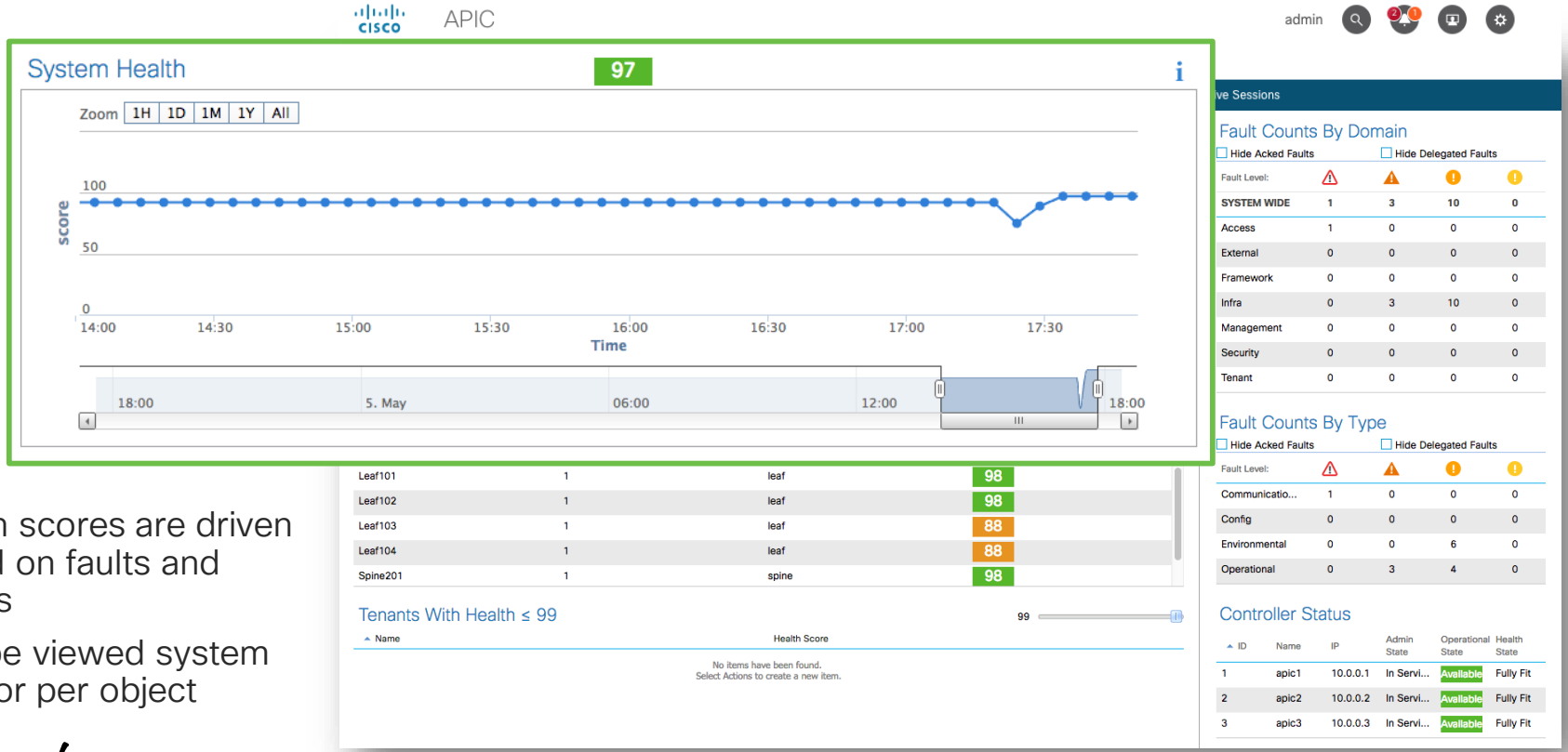
Management Overview

- Faults are raised for various reasons to warn user of issues in the environment.
- Faults are classified based on severity of the error



Why ACI?

Management Overview

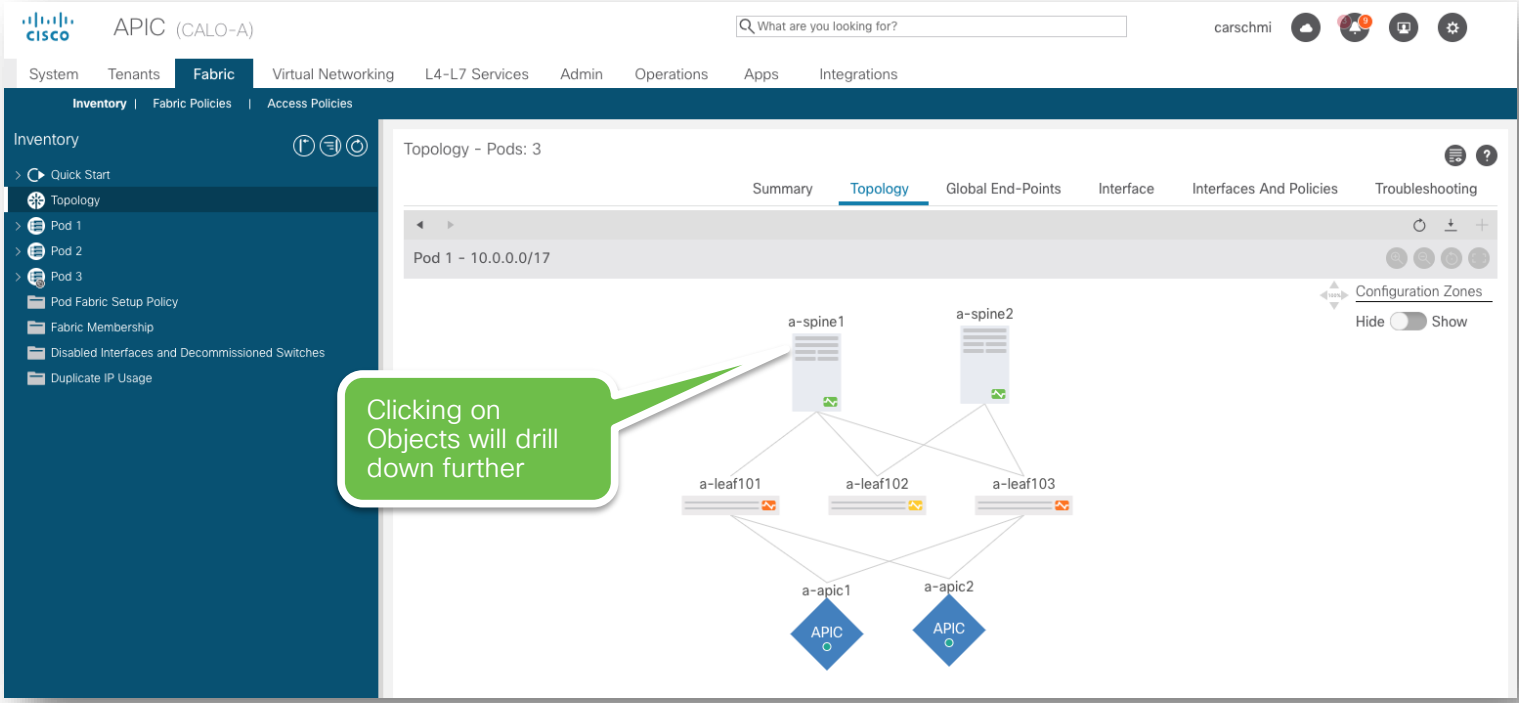


- Health scores are driven based on faults and events
- Can be viewed system wide or per object

Why ACI?

Management Overview

- Fabric Inventory and Topology are centrally managed.



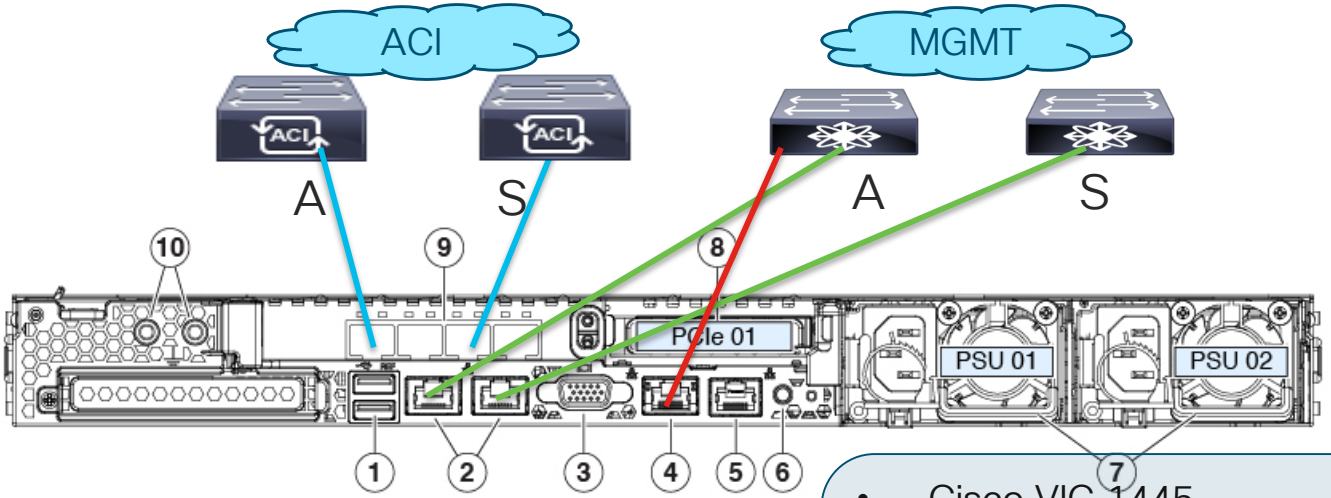
Day 2: Infrastructure and Policies

You make networking **possible**

Cisco live!

Infrastructure and Policies

APIC Components



UCS C220

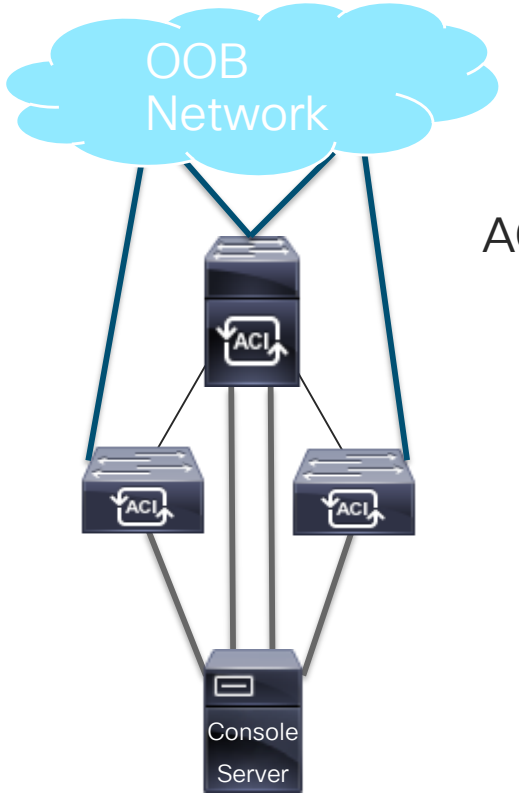
- Cisco VIC 1445
- Two 10Gb port for connections to ACI Switches
- Console Port
- 1Gb Copper Ethernet port for CIMC
- Two 1Gb Copper Ethernet Ports for OOB MGMT

A – Active

S – Standby

Infrastructure and Policies

Best Practice



ACI Spine Switches

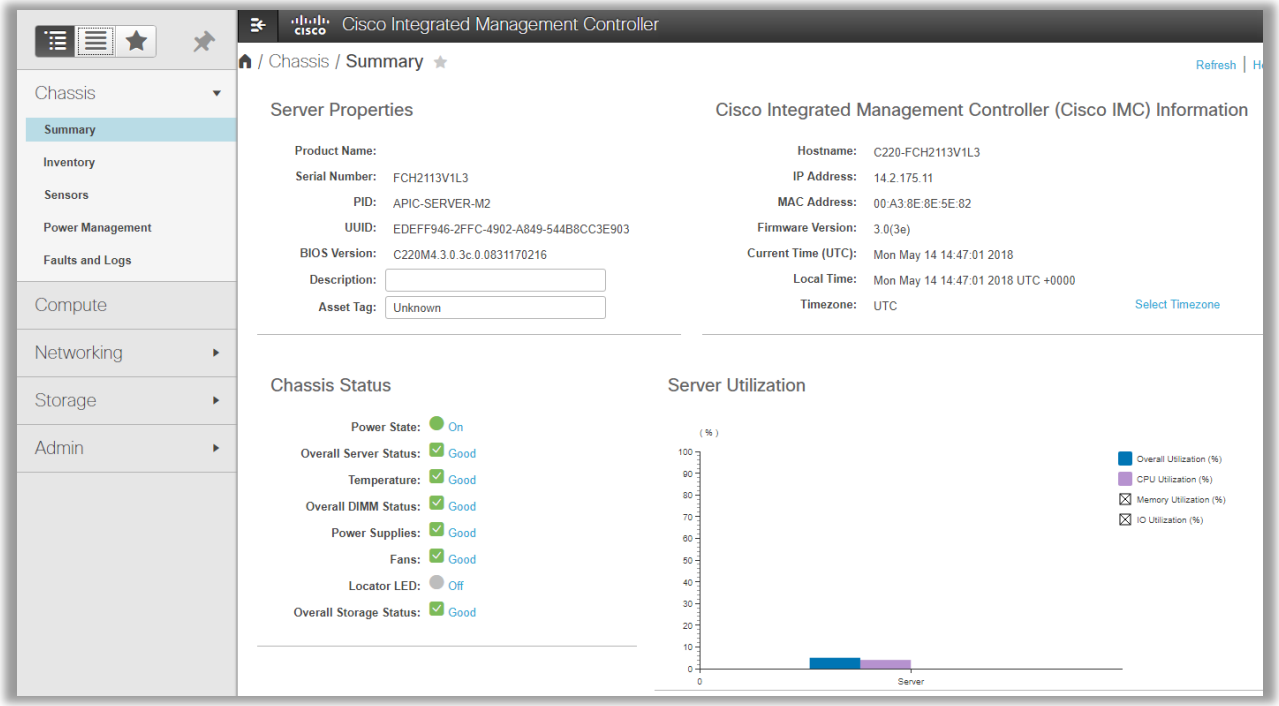
- 1 OOB MGMT per SUP
- 1 Console per SUP
- 40/100 Gb connections to Leafs

ACI Leaf Switches

- 1 OOB MGMT
- 1 Console
- 40/100 Gb connections to Spines

Infrastructure and Services

CIMC



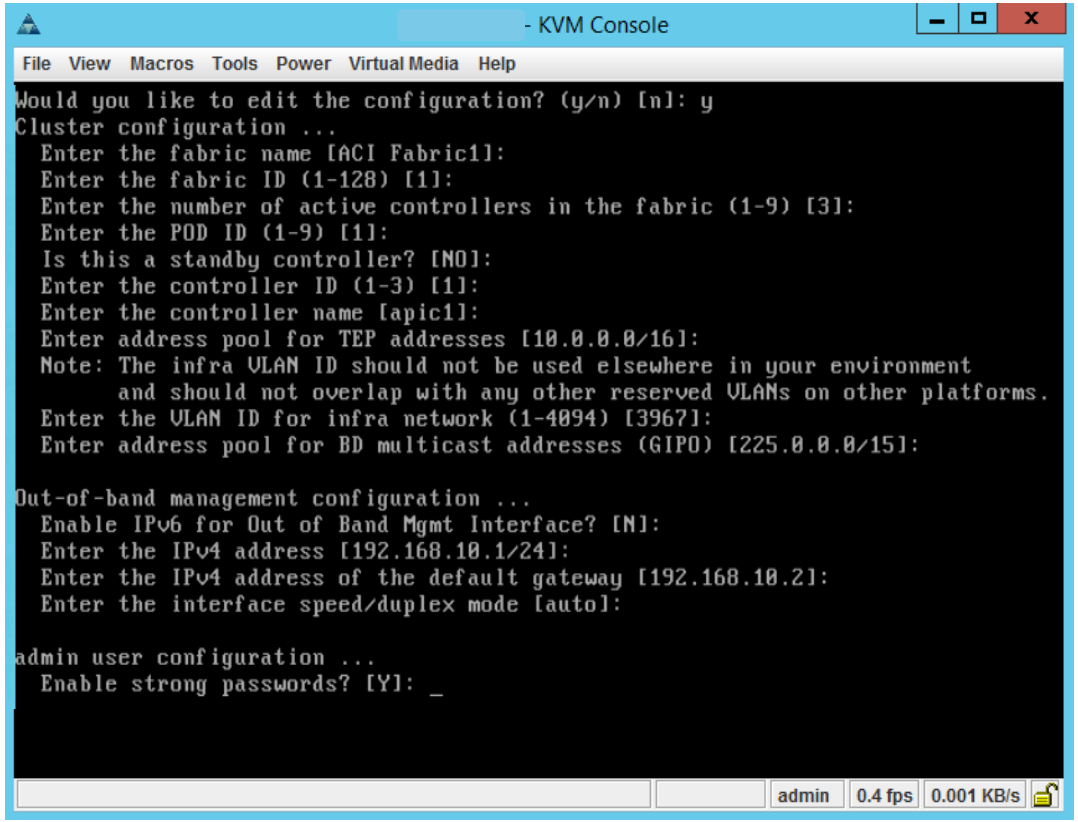
Use for APIC Hardware Diagnostics and Remote Access

Use to install the APIC Software

Infrastructure and Services

CIMC

- CIMC KVM Provides Remote Access
- Equivalent of Console



Infrastructure and Services

Required Addressing

```
Would you like to edit the configuration? (y/n) [n]: y
Cluster configuration ...
  Enter the fabric name [ACI Fabric1]:
  Enter the fabric ID (1-128) [1]:
  Enter the number of active controllers in the fabric (1-9) [3]:
  Enter the POD ID (1-9) [1]:
  Is this a standby controller? [NO]:
  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]:
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (1-4094) [3967]:
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]:
  Enter the IPv4 address [192.168.10.1/24]:
  Enter the IPv4 address of the default gateway [192.168.10.2]:
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]: _
```

1. Infra Subnet
2. Infra VLAN
3. BD Multicast Range
4. OOB Network IP's (CIMC included)

NOTE: Infrastructure subnet and BD MCAST is used internally for APICs and Switches!

Management - Required Addressing

Planning

Requirements	Notes	
Fabric Name	Has to be consistent on all APICs	Fabric1
Fabric ID	Set to 1 (Default)	1
TEP Pool	Recommended a /19 network. APIC will assign IPs from this pool to Leafs, Spines and other Fabric specific services. Avoid IP space which APIC might have to communicate with. E.g.: vCenter or other integrated services	10.0.0.0/16
GIPO Pool	Multicast network for flooding inside ACI. Not exposed to external network unless using Multipod	225.0.0.0/15
Infra VLAN	VLAN will be reserved for internal ACI communication. Cannot be deployed toward user servers	3967
APIC OOB IP	1 IP per APIC, has to be out of band. Inband can be configured later.	
Switch Management IP	1 IP per switch, can have inband, out of band or both.	

Checklist

- ✓ CIMC
- ❑ Management
- ❑ NTP
- ❑ AAA
- ❑ Backups

You make security **possible**

Infrastructure and Services

APIC Management

https://apic1/

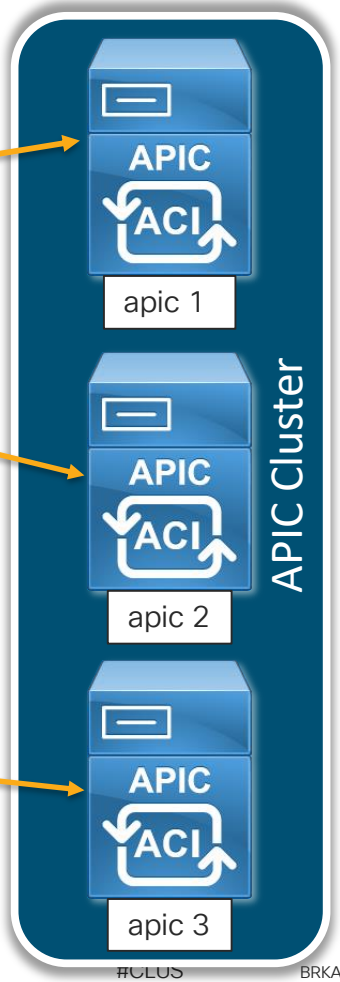
Web Browser

REST API

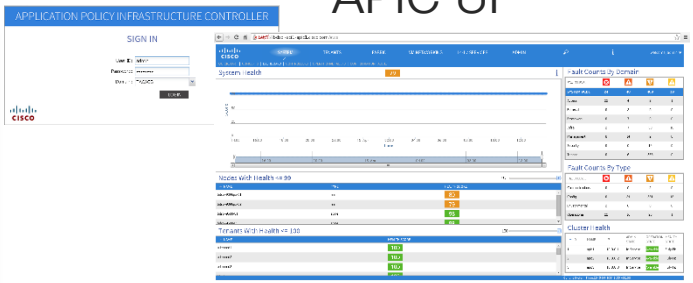
https://apic2/api/

ssh apic3 –l admin

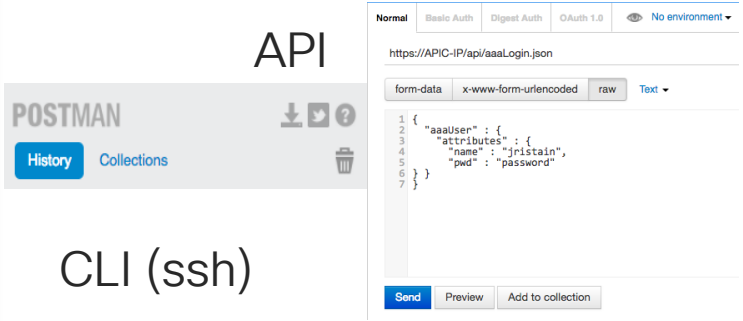
SSH



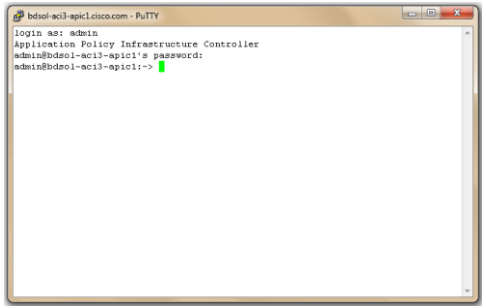
APIC UI



API

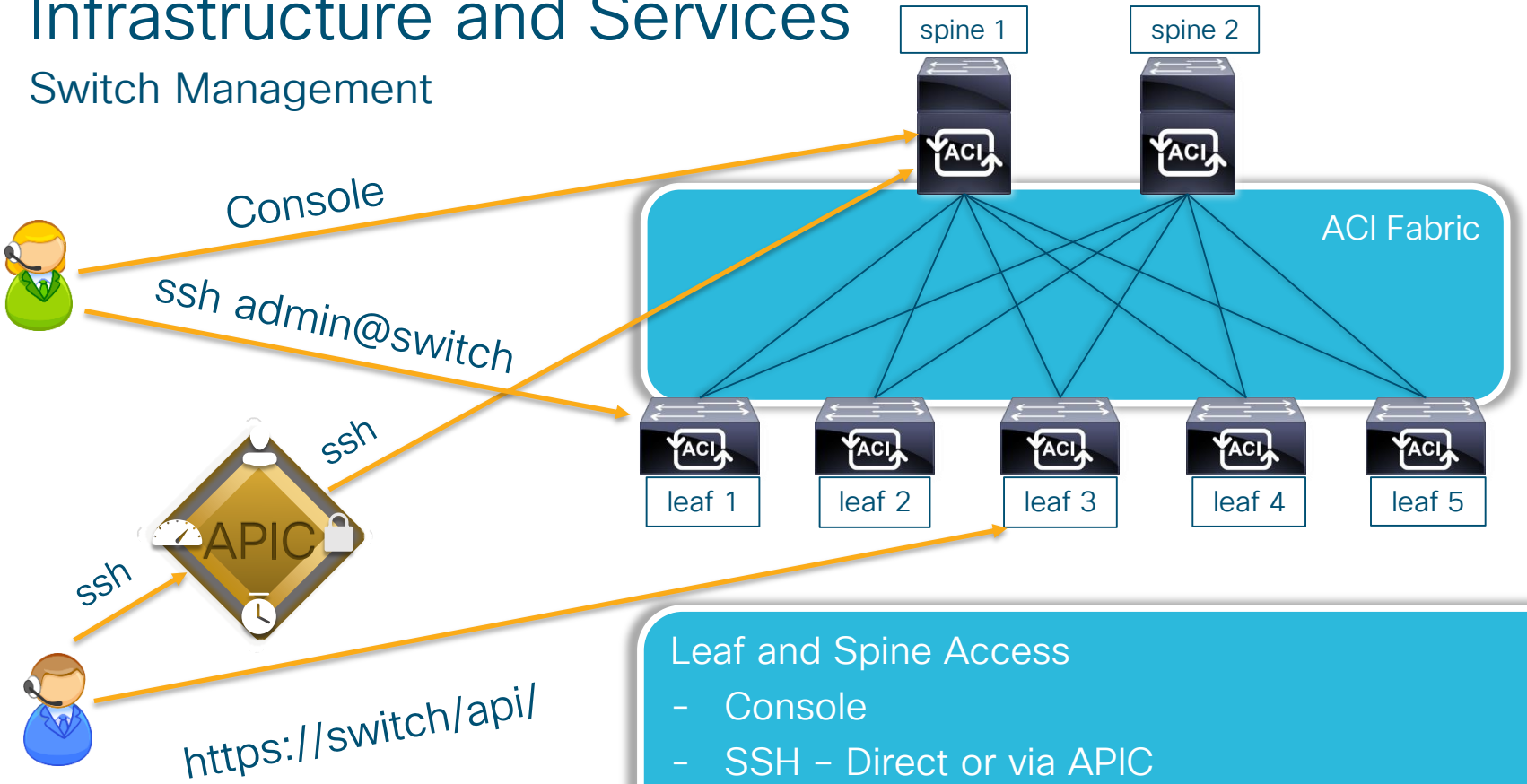


CLI (ssh)



Infrastructure and Services

Switch Management



Leaf and Spine Access

- Console
- SSH – Direct or via APIC
- REST API

Checklist

- ✓ CIMC
- ✓ Management
- ❑ NTP
- ❑ AAA
- ❑ Backups

You make security **possible**

Infrastructure and Services

NTP & PTP

- APIC's send time in control plane messaging
- Certificates
- Tech Supports ☺
- Atomic Counters!

- If Fabric is Gen 2 or newer (EX/FX), Spine can act as a PTP master as well
- Allows user to measure latency between EndPoints and leafs

Checklist

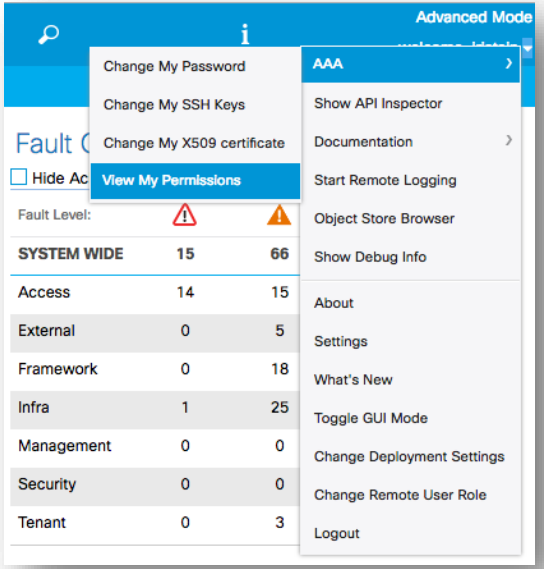
- ✓ CIMC
- ✓ Management
- ✓ NTP
- ❑ AAA
- ❑ Backups

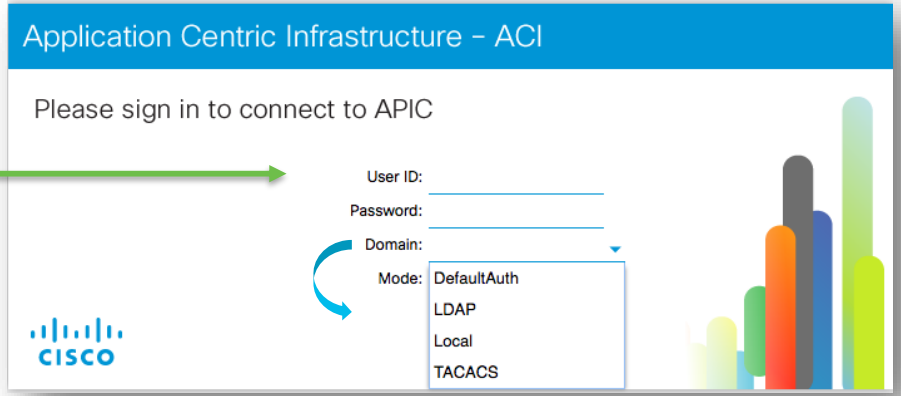
You make security **possible**

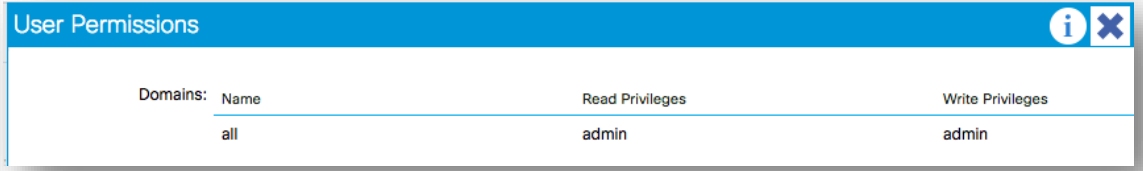
Infrastructure and Services

AAA

Allows users to authenticate with certain privilege levels



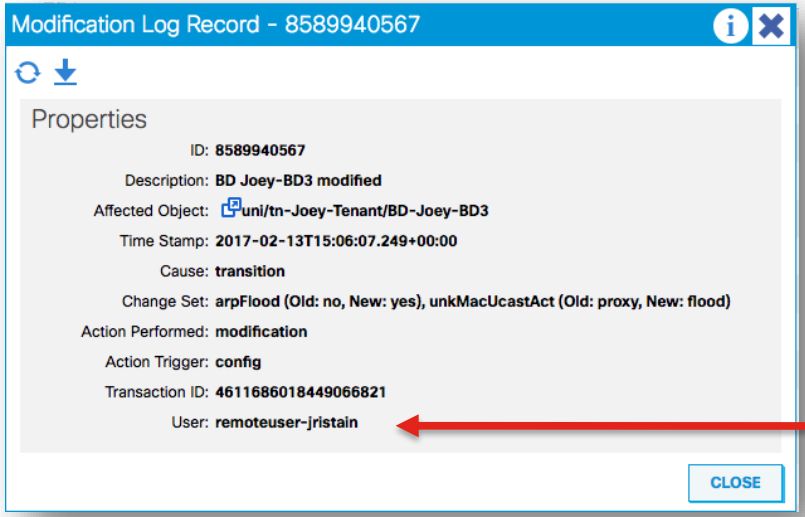




Infrastructure and Services

AAA

"Oh no! We lost connectivity to servers on February 12th at 3pm EST!?"




```
jristain@apic1:~> moquery -c aaaModLR | grep -C 12 "2017-02-13T15"
<snip>
# aaa.ModLR
id            : 8589940567
affected      : uni/tn-Joey-Tenant/BD-Joey-BD3
cause         : transition
changeSet     : arpFlood (Old: no, New: yes), unkMacUcastAct (Old: proxy, New: flood)
childAction   :
clientTag     :
code          : E4206171
created       : 2017-02-13T15:06:07.249+00:00
descr         : BD Joey-BD3 modified
dn            : subj-[uni/tn-Joey-Tenant/BD-Joey-BD3]/mod-8589940567
ind           : modification
modTs         : never
rn            : mod-8589940567
sessionId     :  Ld0sxAcCRfmb2Qb+W+XbUg==
severity      : info
status        :
trig          : config
txId          : 4611686018449066821
user          : remoteuser-jristain
```

Logs changes per user!!

Checklist

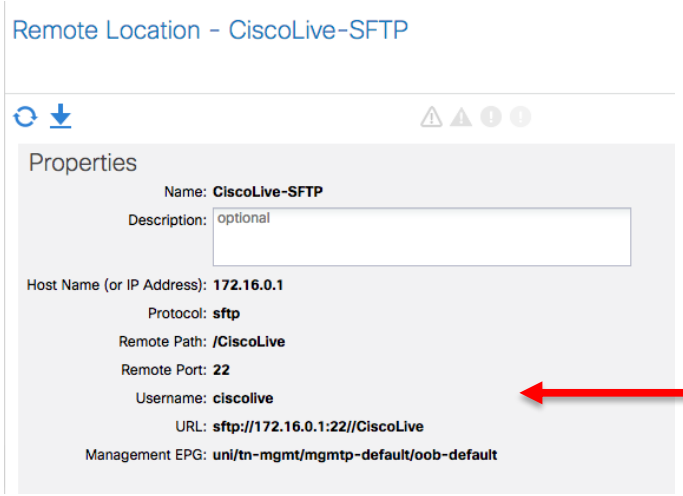
- ✓ CIMC
- ✓ Management
- ✓ NTP
- ✓ AAA
- ❑ Backups

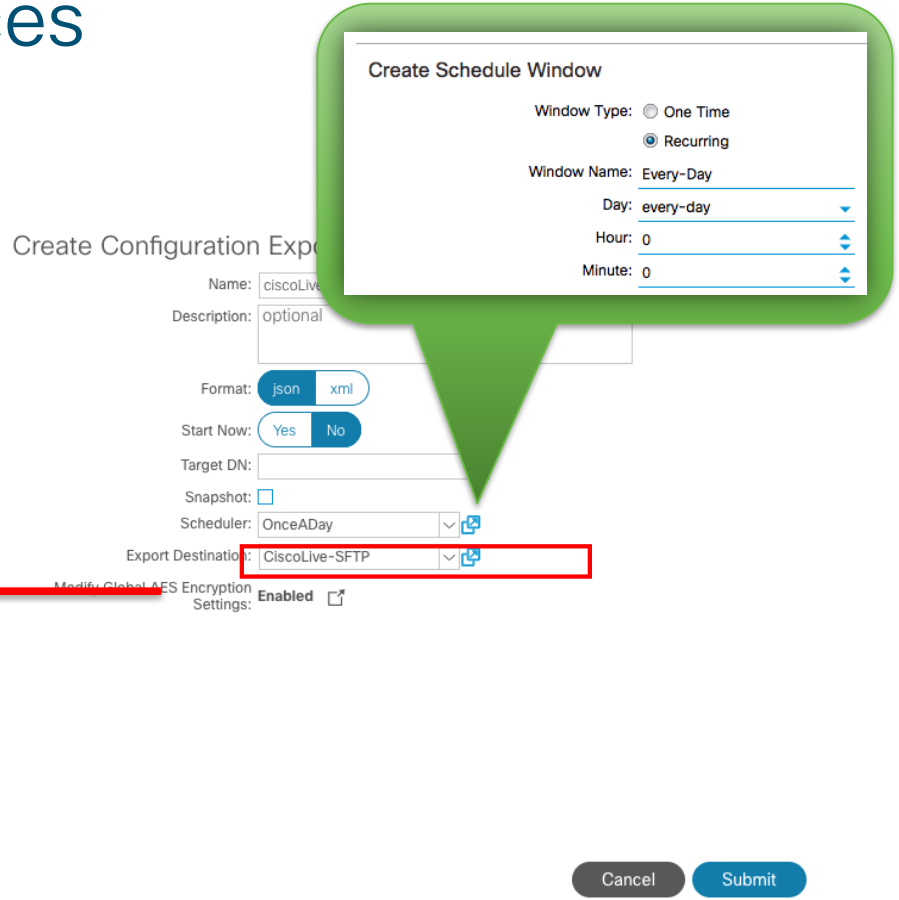
You make security **possible**

Infrastructure and Services

Backups – Configuration Export

- JSON/XML export of the current fabric configuration
- Can set on a scheduler
- Exports to a Remote Location (FTP/SCP/SFTP) – DISASTER RECOVERY





Infrastructure and Services

Backups - Snapshots

Creates a Config Backup that is stored on the APIC by default

Run on a Per Fabric or Tenant Basis

System | Tenants | Fabric | Virtual Networking | L4-L7 Services | Admin | Operations | Apps | Integrations

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

Config Rollbacks for: Tenant

Snapshots	File Name	Description	File Size (bytes)
2019-01-02 1...	ce2_defaultOneTime-2019-01-0...		54885
2019-05-11 1...	ce2_DailyAutoBackup-2019-05-1...		61945
2019-05-12 0...	ce2_DailyAutoBackup-2019-05-1...		61771
2019-05-12 0...	ce2_DailyAutoBackup-2019-05-1...		61632

Actions

Rollback
Select any one snapshot on left to start.

Take a snapshot
Location: APIC
Description: optional
Create a snapshot now

Import export file to snapshot
Click icon on top

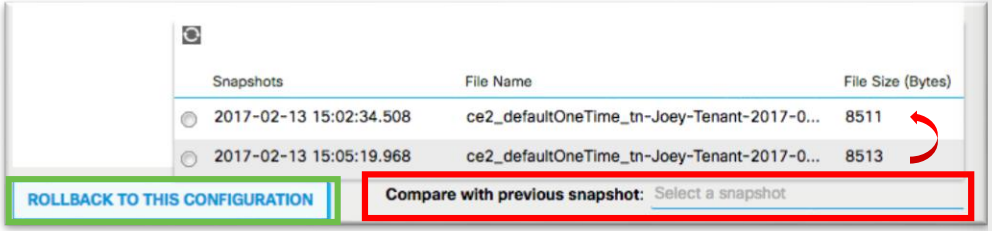
Modify import/export security settings
Click icon on top

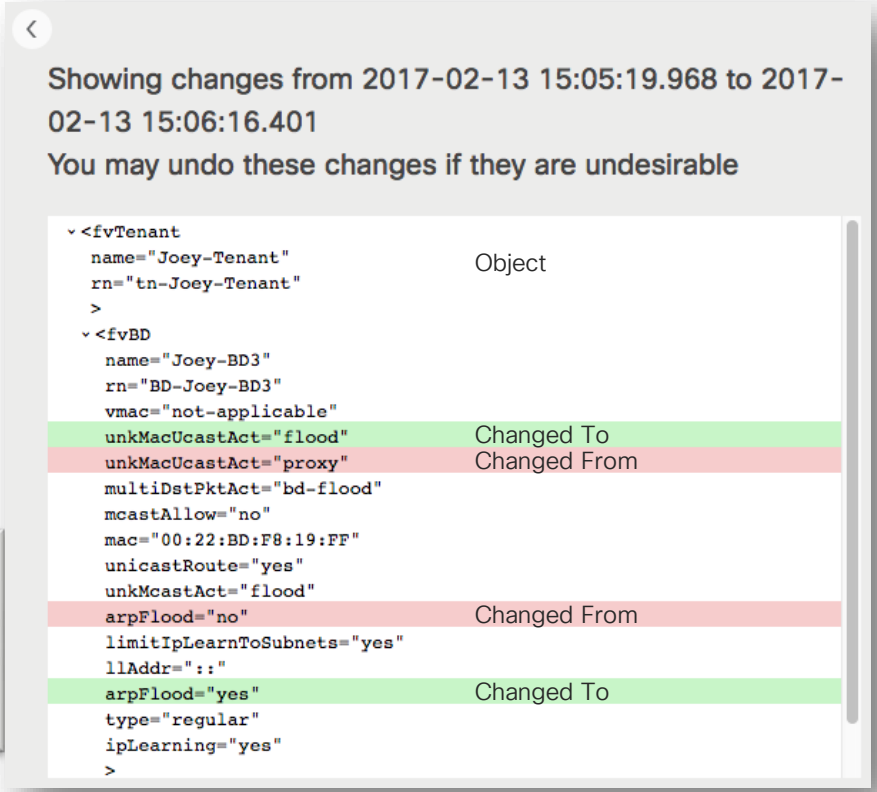
Create recurring snapshots
Click icon on top

Infrastructure and Services

Backups - Snapshots

- Rollback feature allows config rollback between 2 snapshots
- Can also compare differences between a previous SS





Infrastructure and Services

CIMC, NTP, AAA, and Backup Planning

Requirements	Notes	
CIMC IP per APIC	Unique IP address used for IP KVM built into APIC. Must use dedicated port	
NTP Server	NTP Server which all nodes inside fabric will use	
User Management	TACAS/ RBAC or RADIUS Server for accounting. Custom local user account can be used too	
Scheduled backup	Multicast network for flooding inside ACI. Not exposed to external network unless using Multipod	
Backup Server	Server outside of ACI Fabric running FTP, SFTP or SCP Server	

Checklist

- ✓ CIMC
- ✓ Management
- ✓ NTP
- ✓ AAA
- ✓ Backups

You make security **possible**

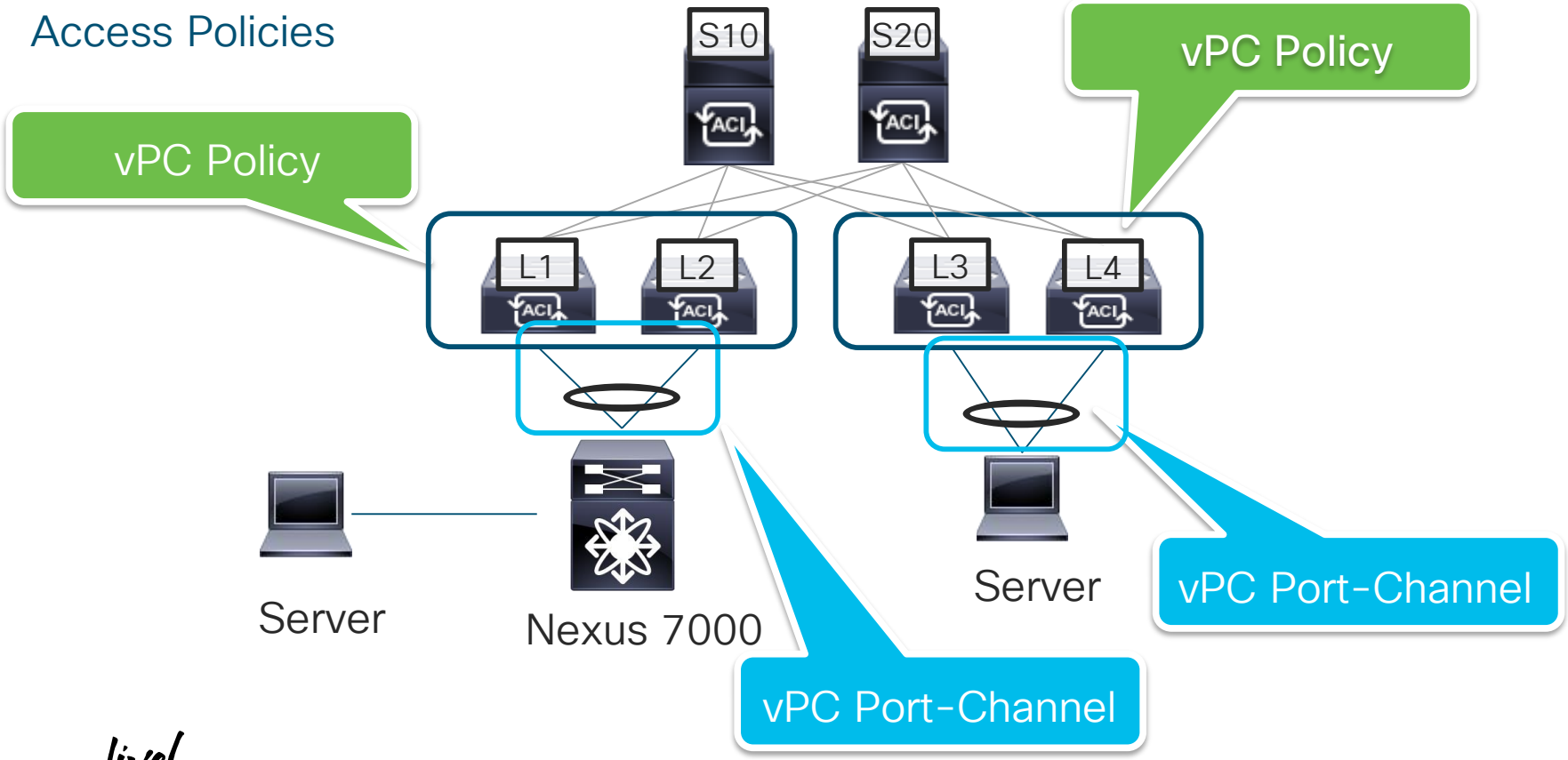
Fabric and Tenant Policies

You make the power of data **possible**

Cisco live!

Fabric and Tenant Policies

Access Policies



Fabric and Tenant Policies

Access Policies

Access policies refer to the configuration that is applied for physical and virtual (hypervisors/VMs) devices attached to the fabric.

Broken into a few major areas:

Global Policy

- Pools
- Domains
- Attachable Access Entity Profiles

Switch Policy

- Policies
- Policy Groups
- Profiles

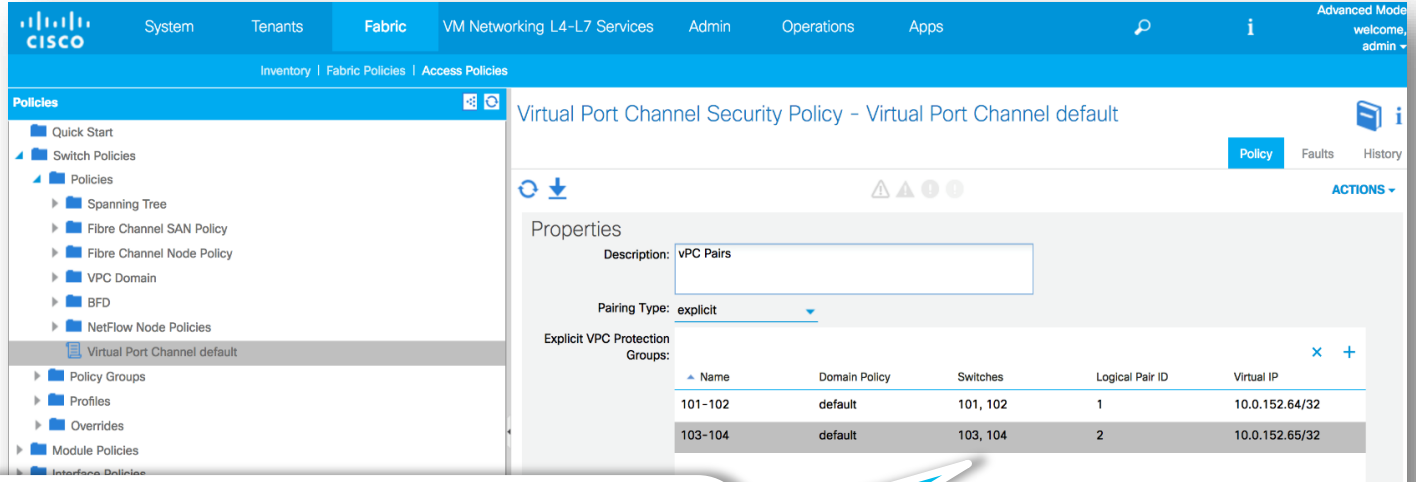
Interface Policy

- Policies
- Policy Groups
- Profiles

Fabric and Tenant Policies

vPC Domain Policy

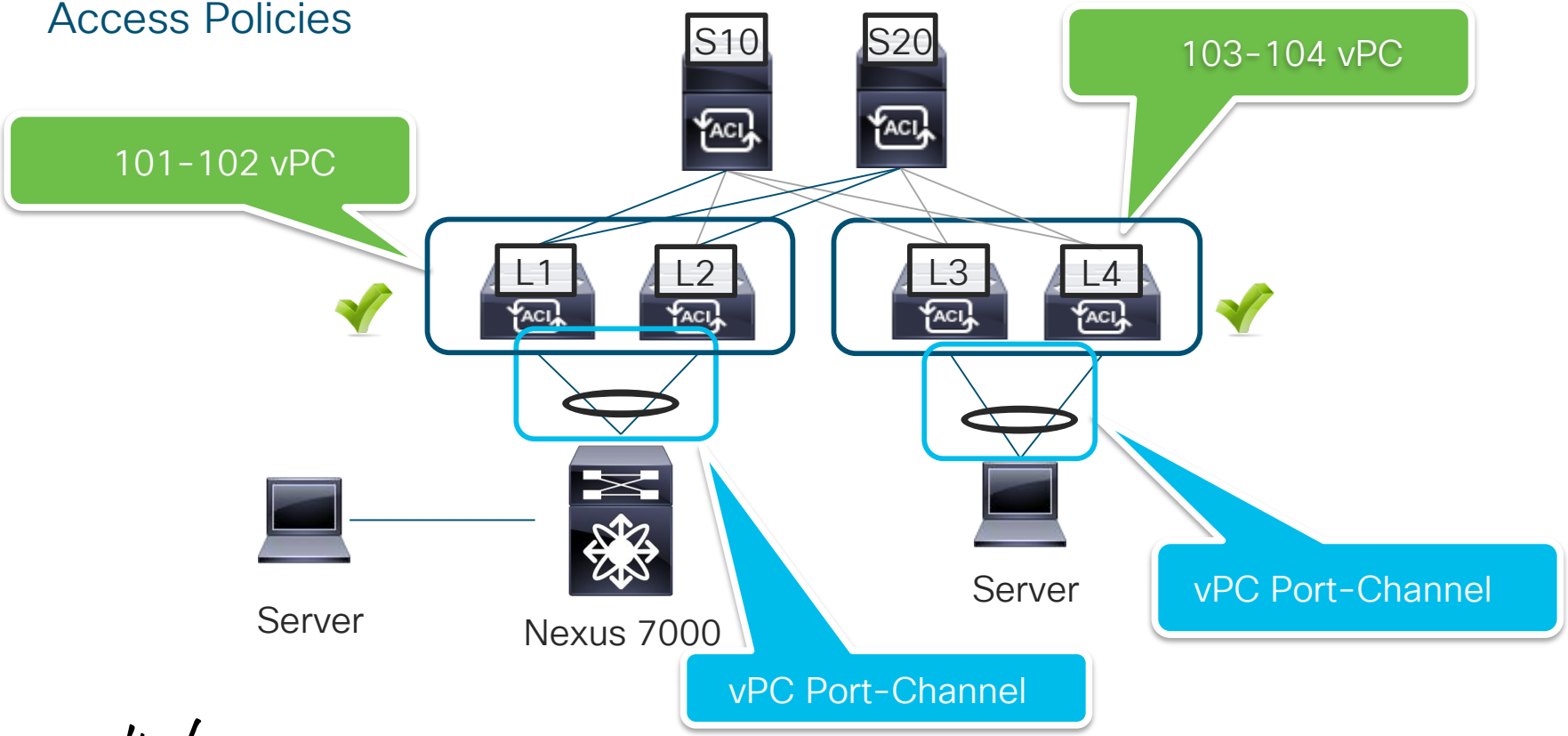
- No Peer-Link
- No Peer-Keepalive
- Uses Fabric Links for Communication



Switches	Logical Pair ID	Virtual IP
101, 102	1	10.0.152.64/32
103, 104	2	10.0.152.65/32

Fabric and Tenant Policies

Access Policies

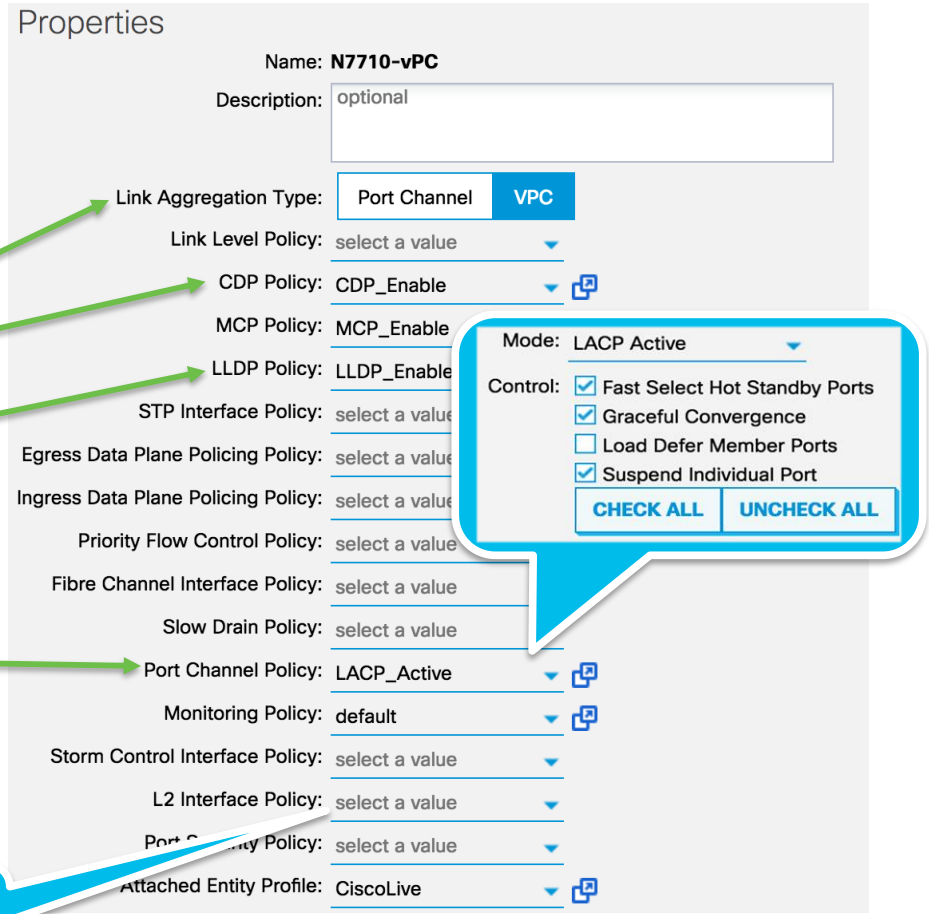


Fabric and Tenant Policies

Port-Channels

Legacy NXOS Config

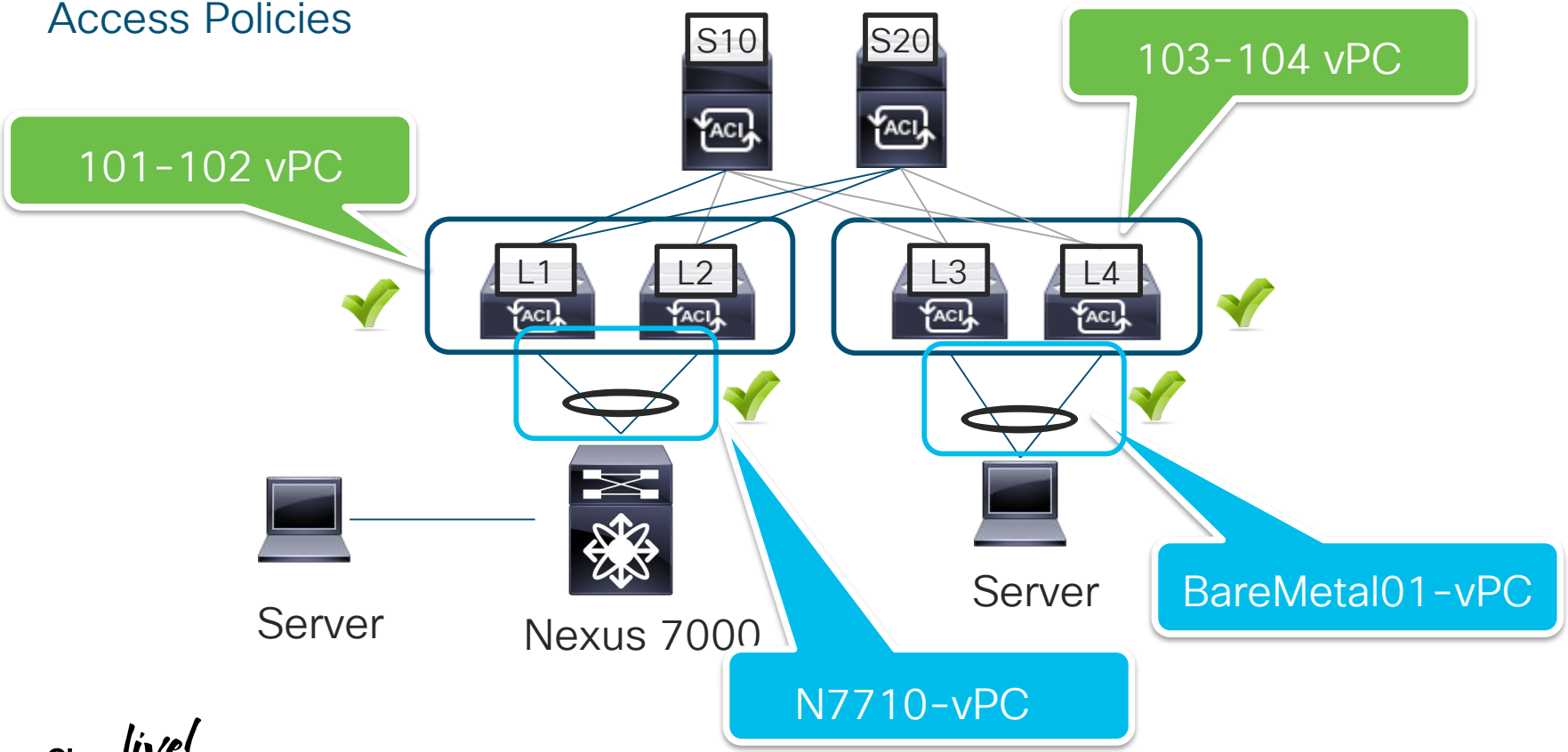
```
Nexus7710# show run int po 10

interface port-channel10
  switchport mode trunk
  vpc 10

Nexus7710# show run interface Ethernet1/10

interface Ethernet1/10
 speed 10000
 lldp transmit
 lldp receive
 channel-group 10 mode active
```



Unspecified fields use default values

Fabric and Tenant Policies

Access Policies



AEP

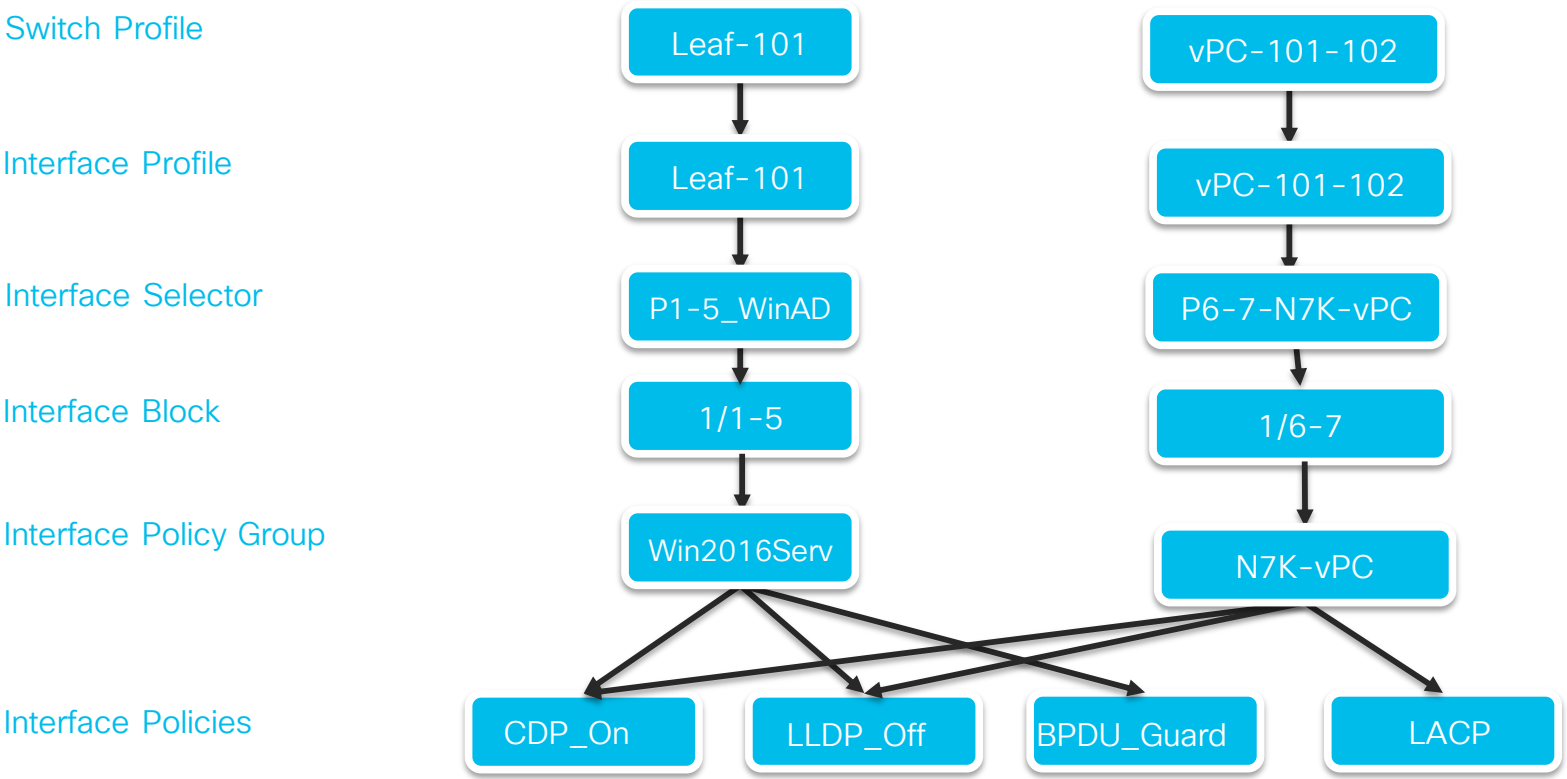
The AEP is used to associate a domain to one or more interface policy groups. In most deployments it is recommended to use a single AEP if VMM integration is not being used. If the ACI Fabric will be integrated with n VMM domains, use 1 + n to determine how many AEPs are needed

The Domain is used to specify what type of path (vlan) can be deployed on a interface. If a AEP does not contain a “External Routed Domain”, the interface can not be used to deploy a L3Out.

In Most deployments a single VLAN pool can be used with 1 Physical Domain and 1 External Routed Domain.

Relationship View

Access Policies Workflow Example



Management - Required Addressing

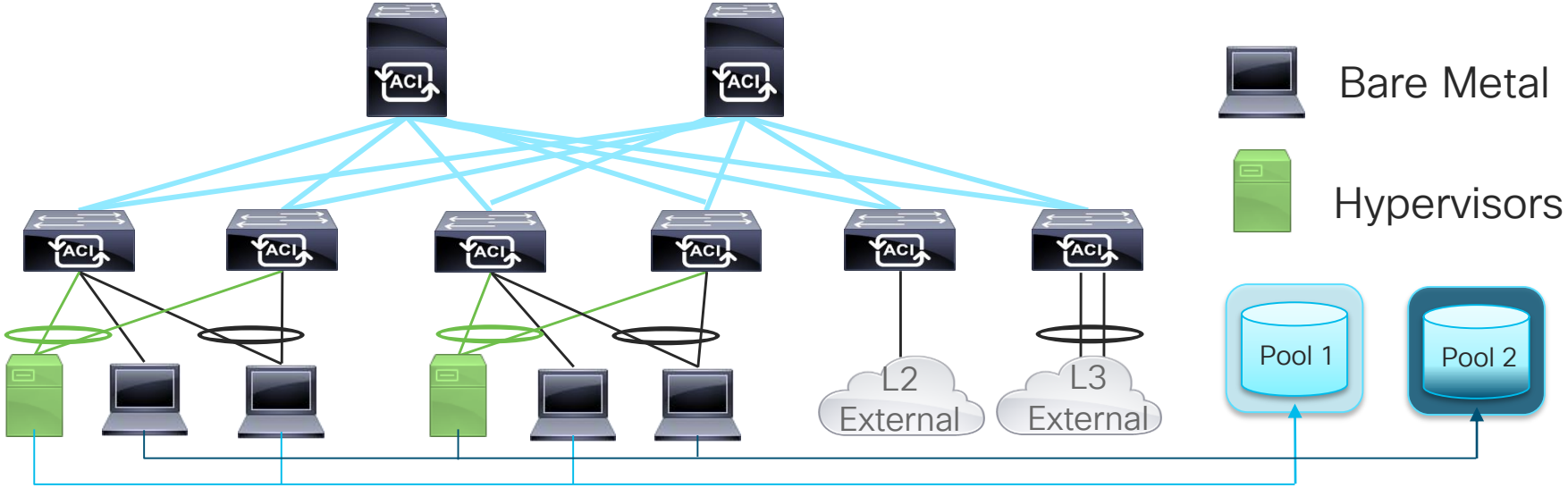
Planning

Requirements	Notes	Example
AEP	1 AEP for all Policy groups. Map all domains to this Policy group	Prod_AEP
Domain	1 Physical Domain, 1 External Routed Domain	phys L3Out
VLAN Pool	1 VLAN pool for all statically deployed vlans. 1 VLAN pool for Dynamically deployed VLANs. These pools should not overlap.	Static_VLANs VMM_Domain
Switch Profile	1 Profile per switch for Orphan Ports, 1 Profile per vPC Domain (Containing both switches)	vPC-101-102, Leaf101, Leaf102
Interface Profile	Create a 1 to 1 mapping to switch Profile	vPC-101-102, Leaf101, Leaf102
Interface Selector	Name after Server, Include Port ID.	P11-N7710-vPC
Policy Group	1 Policy Group per Port-Channel/ vPC. Policy Groups can be reused for access ports. Assign AEP to Policy Group	N7710-vPC

Access Policies

What is the goal? What are we trying to accomplish?

1) Provide consistent configurations across the whole fabric.
2) A simplified and well organized configuration, where policy is defined once and re-used.
3) Define what policies are allowed to be deployed on leafs/ports
4) Restrict Resource deployment in a multi-tenant environment.



Access Policies

Access policies refer to the configuration that is applied for physical and virtual (hypervisors/VMs) devices attached to the fabric.

Broken into a few major areas:

Switch Policy
- Policies
- Policy Groups
- Profiles

Interface Policy
- Policies
- Policy Groups
- Profiles

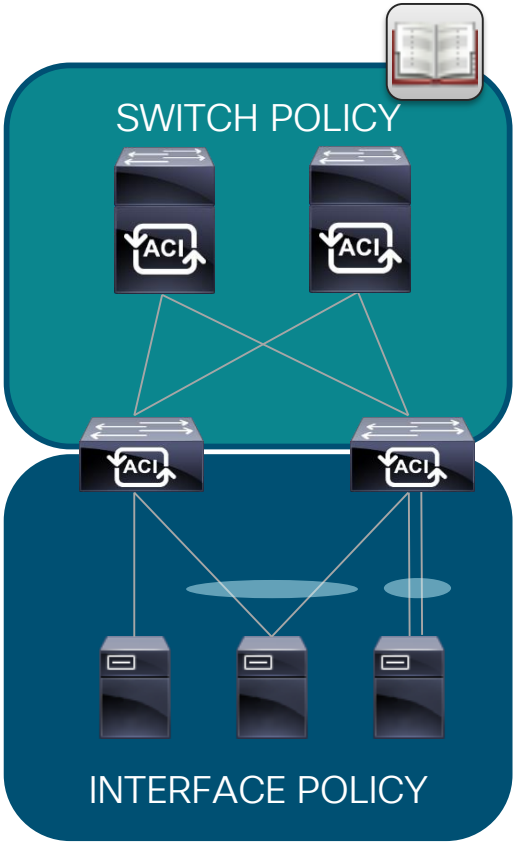
Global Policy
- Pools
- Domains
- Attachable Access Entity Profiles

Access Policies

Policies define protocol / feature configurations

Policy Groups select which policies should be applied

Profiles associate policy groups to switches or interfaces, through the use of selectors



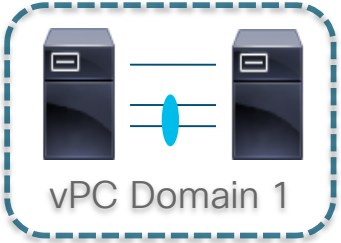
Switch Policy Types:

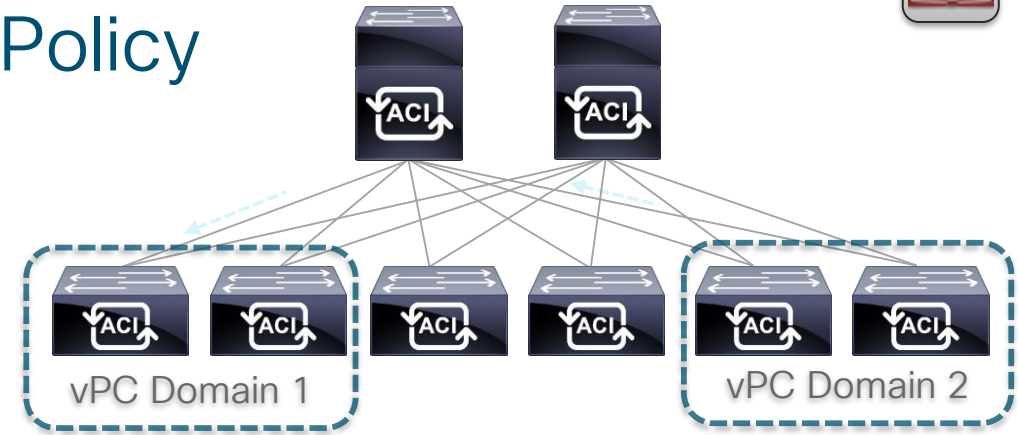
- VPC Domain
- Spanning-tree (MST)
- BFD
- Fibre-channel SAN/Node

Interface Policy Types:

- Link-level
- CDP
- LLDP
- Port-channel / LAG
- Port-channel member
- Spanning-tree
- Storm Control
- Data plane policing
- MCP
- L2 (Vlan local / global)
- Firewall

vPC Protection Group Policy





Classical vPC Domain configuration

Required configuration of domain, peer-link, and peer-keepalive link on both devices in domain

```
vpc domain 1
  peer-keepalive destination 172.168.1.2 /
    source 172.168.1.1 vrf vpc-keepalive
  peer-gateway
  ip arp synchronize

interface port-channel 20
  vpc peer-link
```

ACI vPC Domain configuration

Specify the Domain ID and the two Leaf switch IDs that form the domain pair

VPC Protection Group

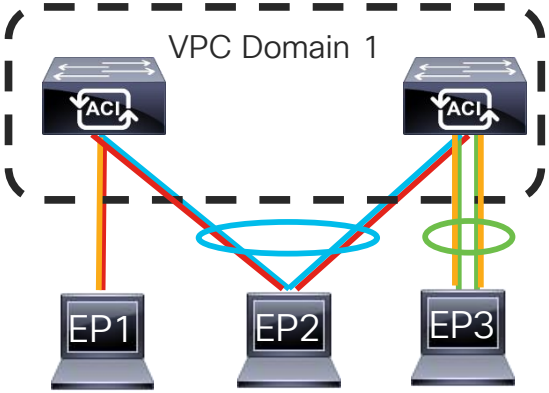
Name: vPC-Domain100
ID: 100
Switch1: 101
Switch2: 102

Interface Policies

Used to define a particular policy for a given interface level function. The intention of Interface Policies is that they are defined once and re-used among interfaces that need like policies.

Examples:

- LLDP On/Off
- CDP On/Off
- Port-Channel
  - LACP
  - Mode On
- Storm Control
- MACsec



Interface Policy Groups

Used to specify which interface policies to be applied to a particular interface type.

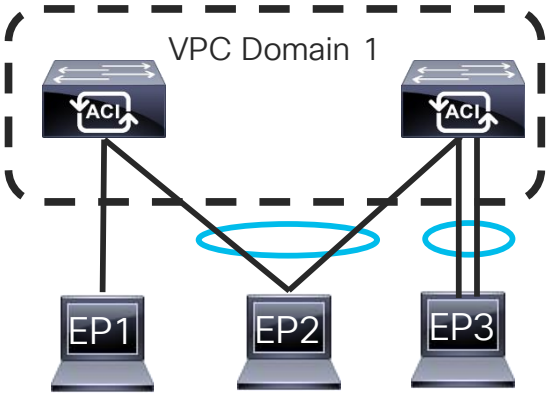
It also associates an AEP (which defines which domains are allowed on the interface).

Types:

Access port (EP1)

Access Bundle Groups

- Virtual Port-channel (EP2)
- Port-channel (EP3)



Note: Separate policy groups should be created for each port-channel (standard or VPC) that you need to configure. All interfaces on leaf that are associated with a particular access bundle group reside in same channel.

Global Policy

Pools (Vlan / VXLAN)

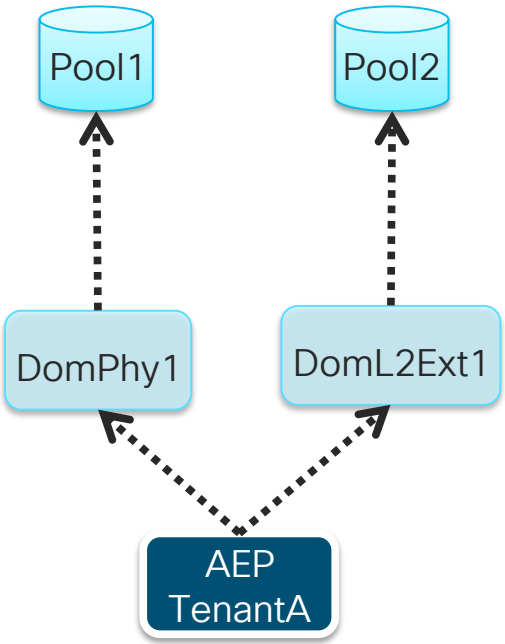
A resource pool of encapsulations that can be allocated within the fabric.

Domains (Physical / VMM / External Bridged / External Routed)

Administrative domain which selects a vlan/vxlan pool for allocation of encaps within the domain

Attachable Access Entity Profiles (AEP)

Selects one or more domains and is referenced/applied by interface policy groups.



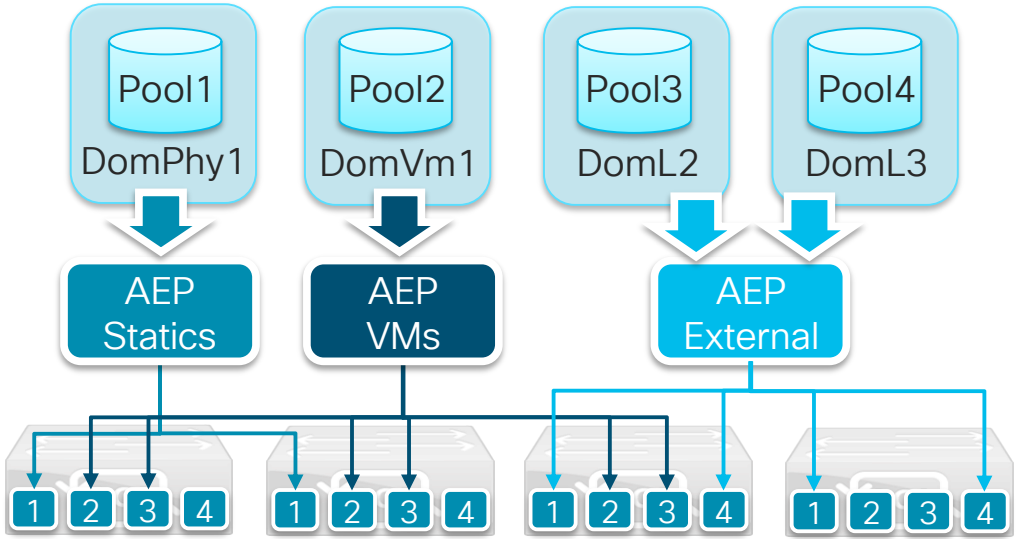
Global Policy – Attachable Entity Profiles

Configuration:

- Create a VLAN/VXLAN **pool** with a range of encapsulations
- Create a **domain** (physical, l2/l3 external, or VMM) and associate **pool**
- Associate **domain** to **AEP**
- Associate **interface policy group** to **AEP** *switch/interface selectors will apply the config through the interface policy group assign to specific ports*

What have we accomplished?

- Specified what domains and corresponding pools are allowed per interface in the fabric!



Port-Channel Policies

Classical vPC Domain configuration

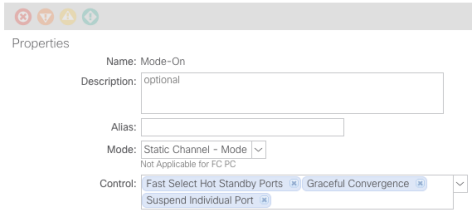
Required configuration of domain, peer-link, and peer-keepalive link on both devices in domain

```
interface Ethernet1/5-6
  lacp port-priority 32768
  lacp rate normal
  channel-group 10 mode on

interface Ethernet1/10-11
  lacp port-priority 32768
  lacp rate fast
  channel-group 20 mode active
```

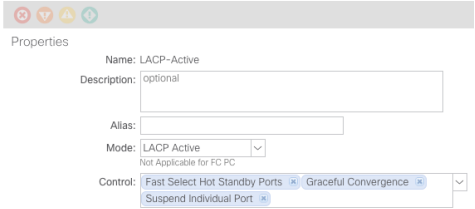
ACI Port-Channel Policies

Specify mode, minimum / maximum links, and related protocol options (relating to LACP)

Port Channel Policy - Mode-On



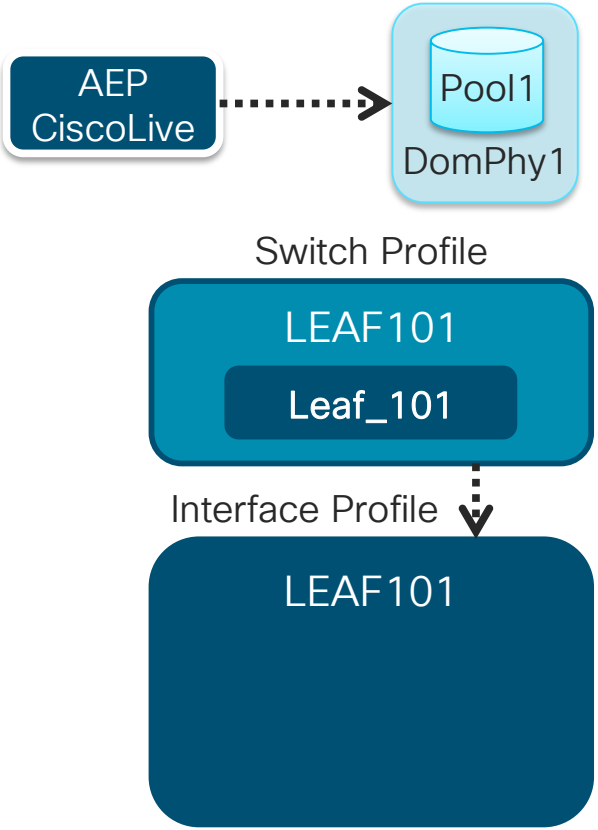
Port Channel Policy - LACP-Active

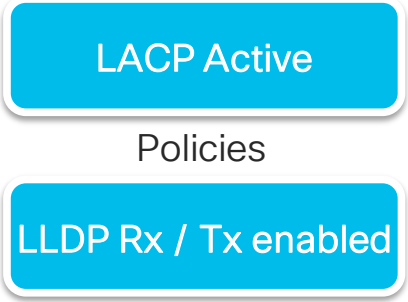


Access Policy Example

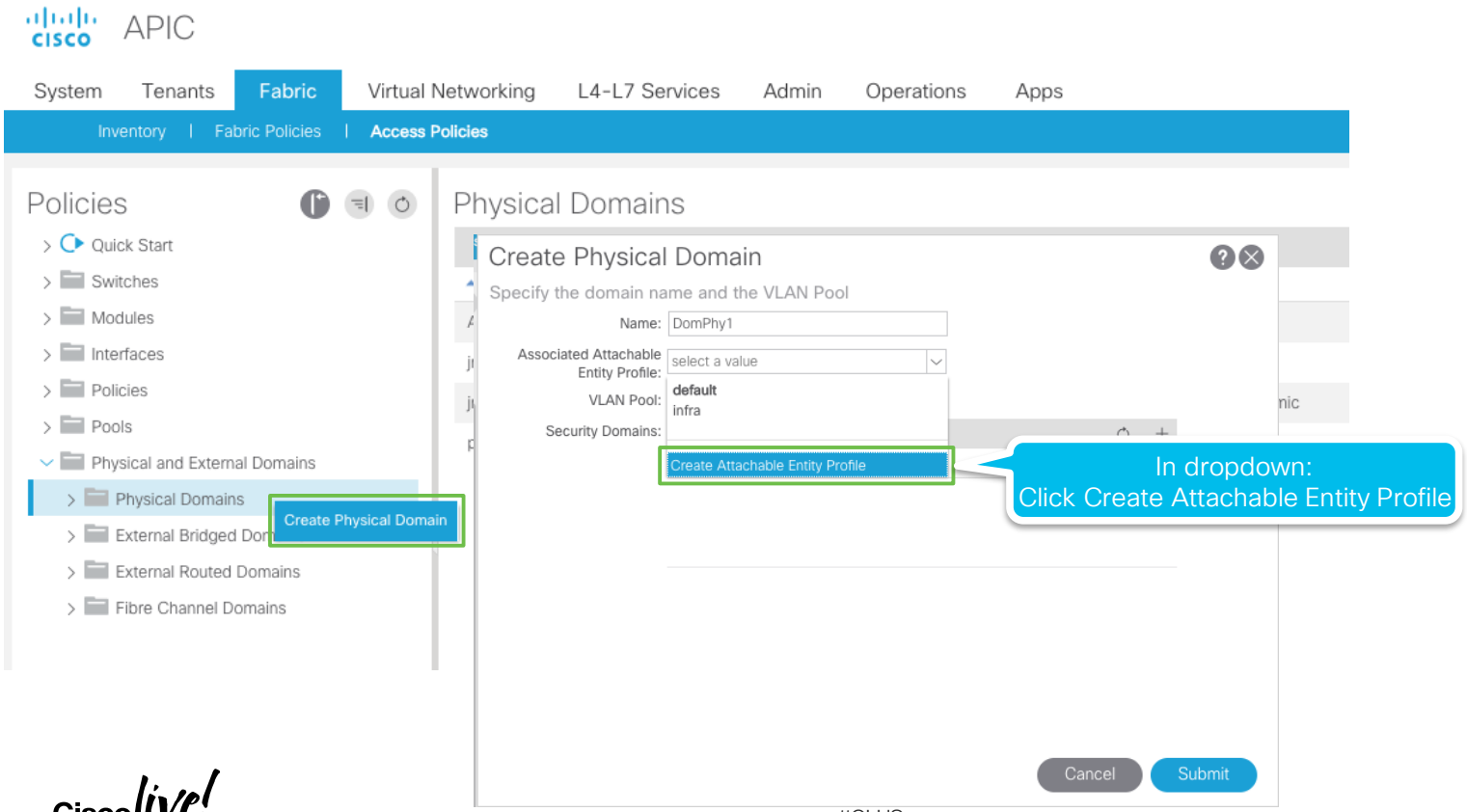
General Configuration (reused for many interfaces):

1) Configure a physical domain and vlan pool
2) Create an AEP and associate physical domain
3) Create switch/interfaces profiles for leaf (LEAF101)
   - very easy to apply configurations if you create a switch/interface profile for each leaf and one for each VPC domain pair
4) Configure Interface policies (LACP / LLDP)

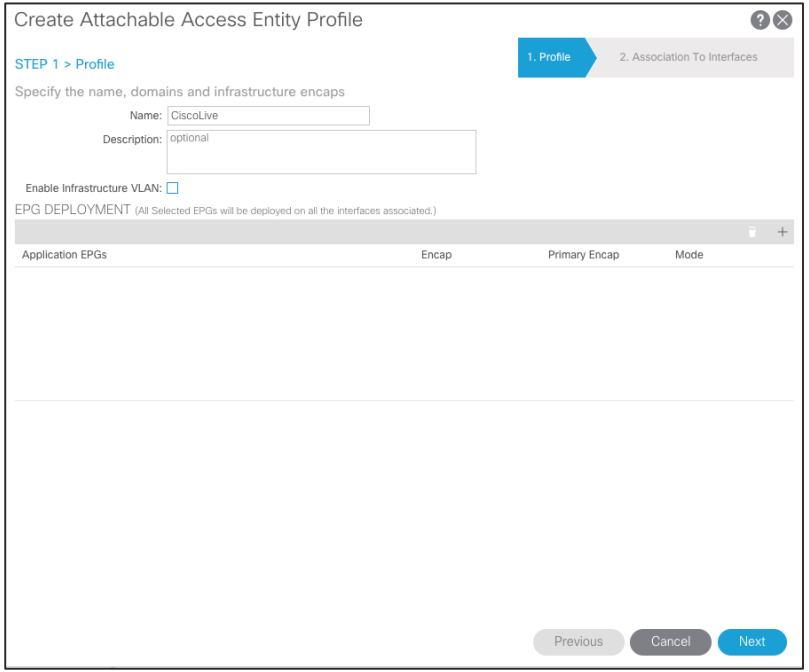


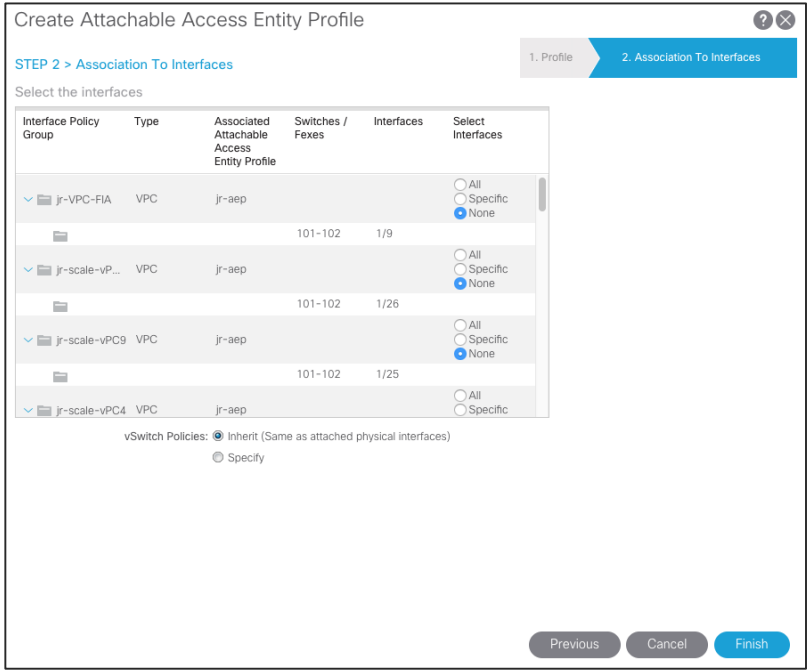


Creating Physical Domain / AEP / Vlan Pool

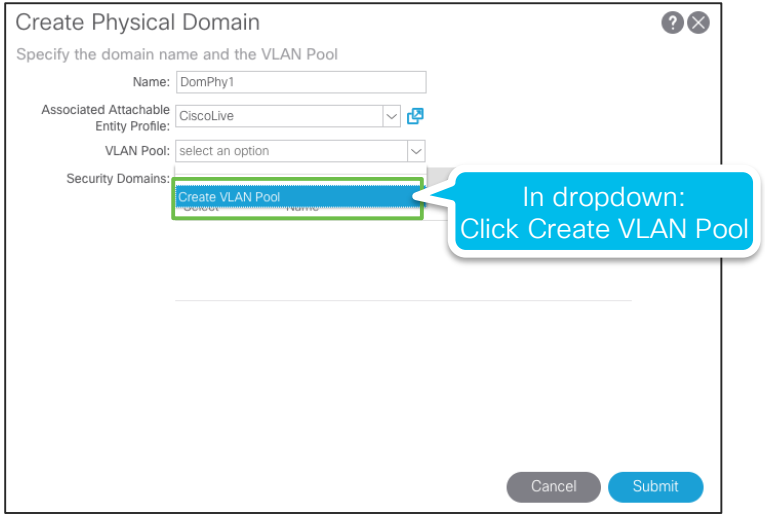


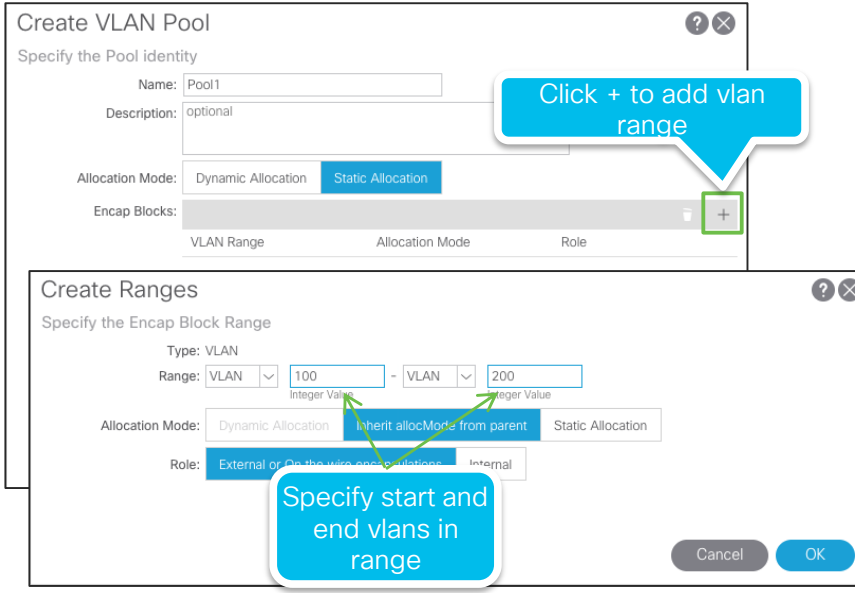
Creating Physical Domain / AEP / Vlan Pool



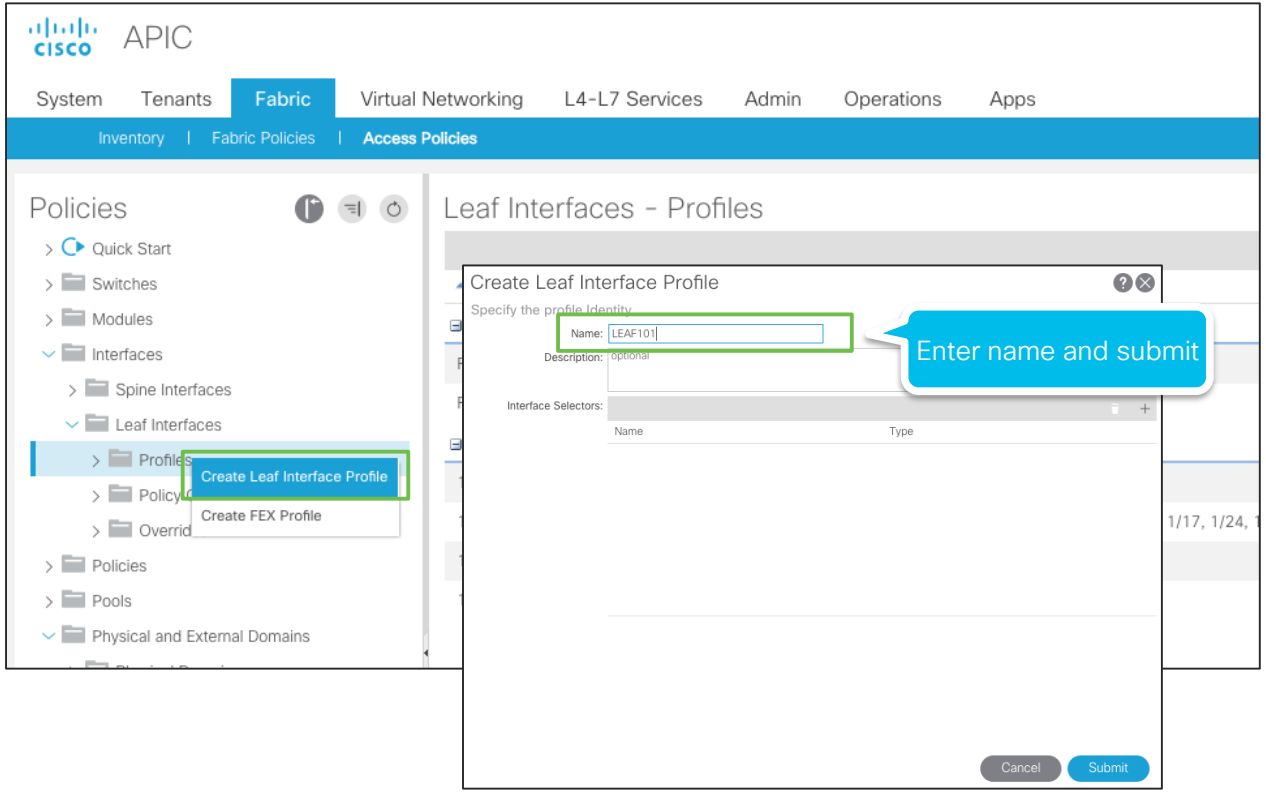


Creating Physical Domain / AEP / Vlan Pool

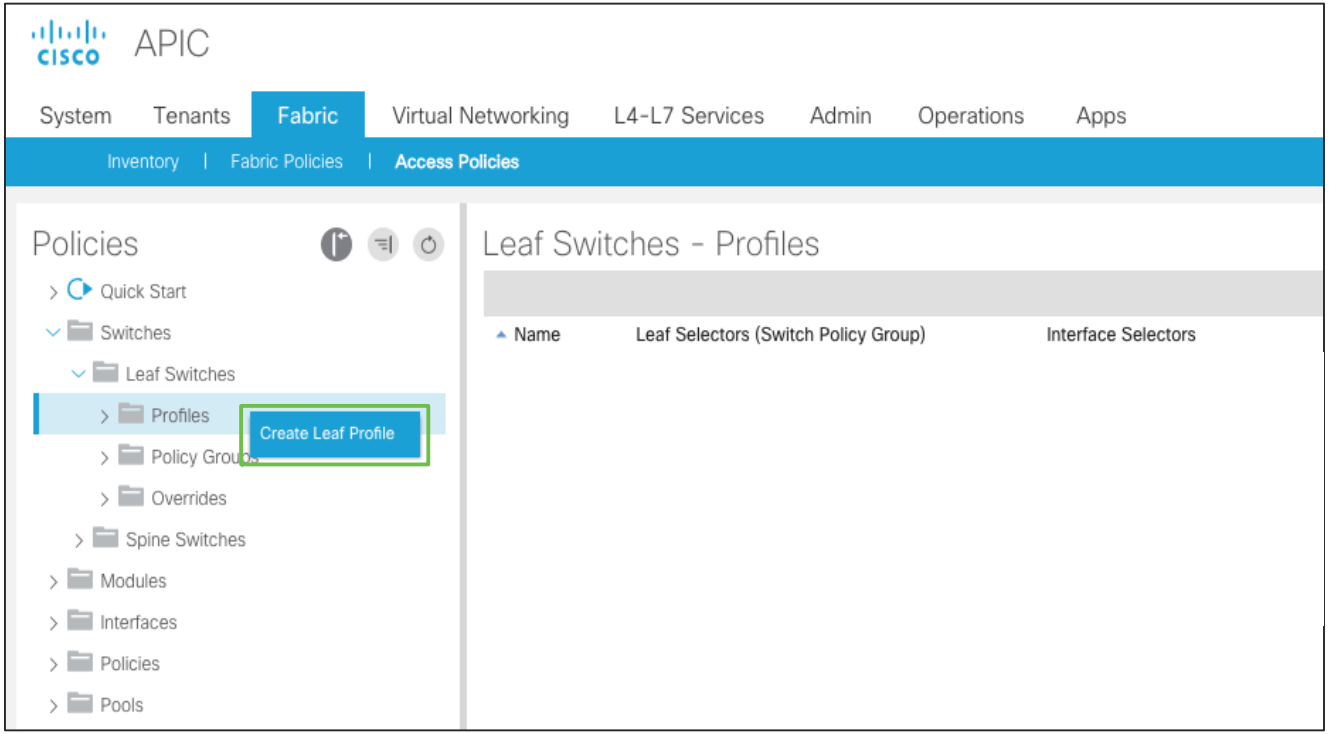




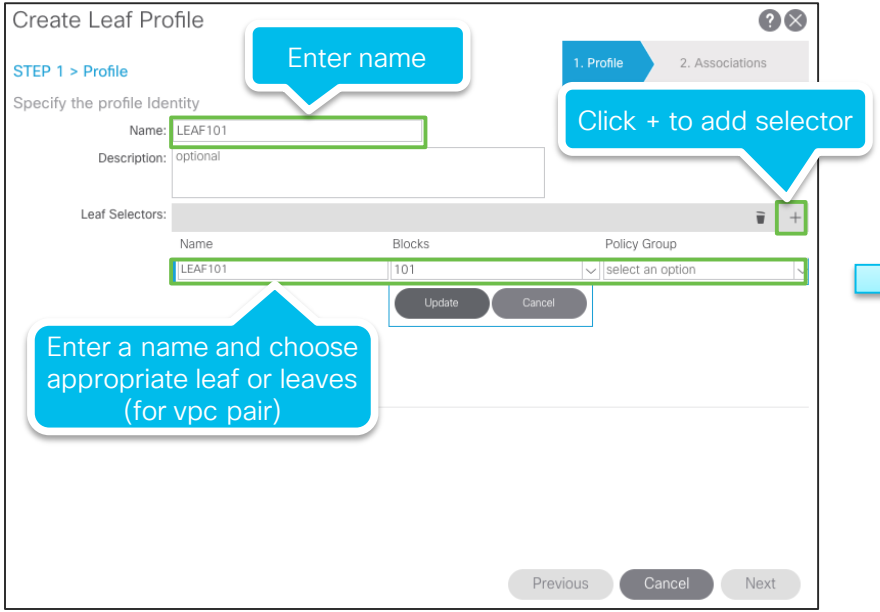
Create Interface Profile for each leaf / VPC domain

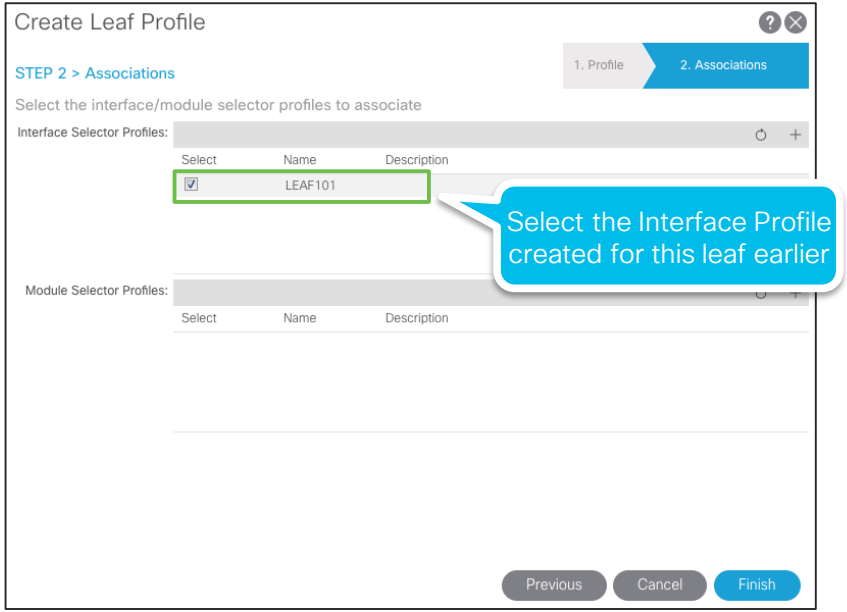


Create Switch Profile for each leaf / VPC domain



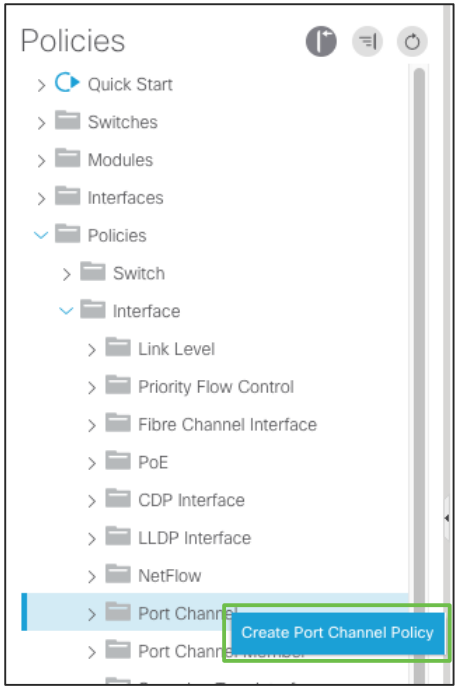
Create Switch Profile for each leaf / VPC domain

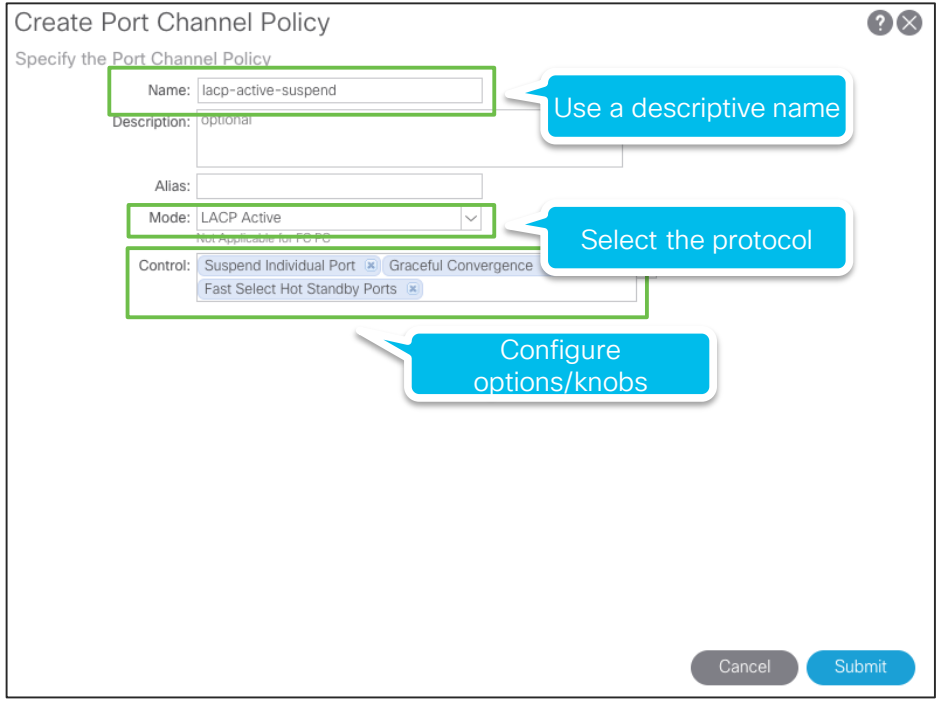




Create common protocol configurations

Example demonstrates a common lacp port-channel policy

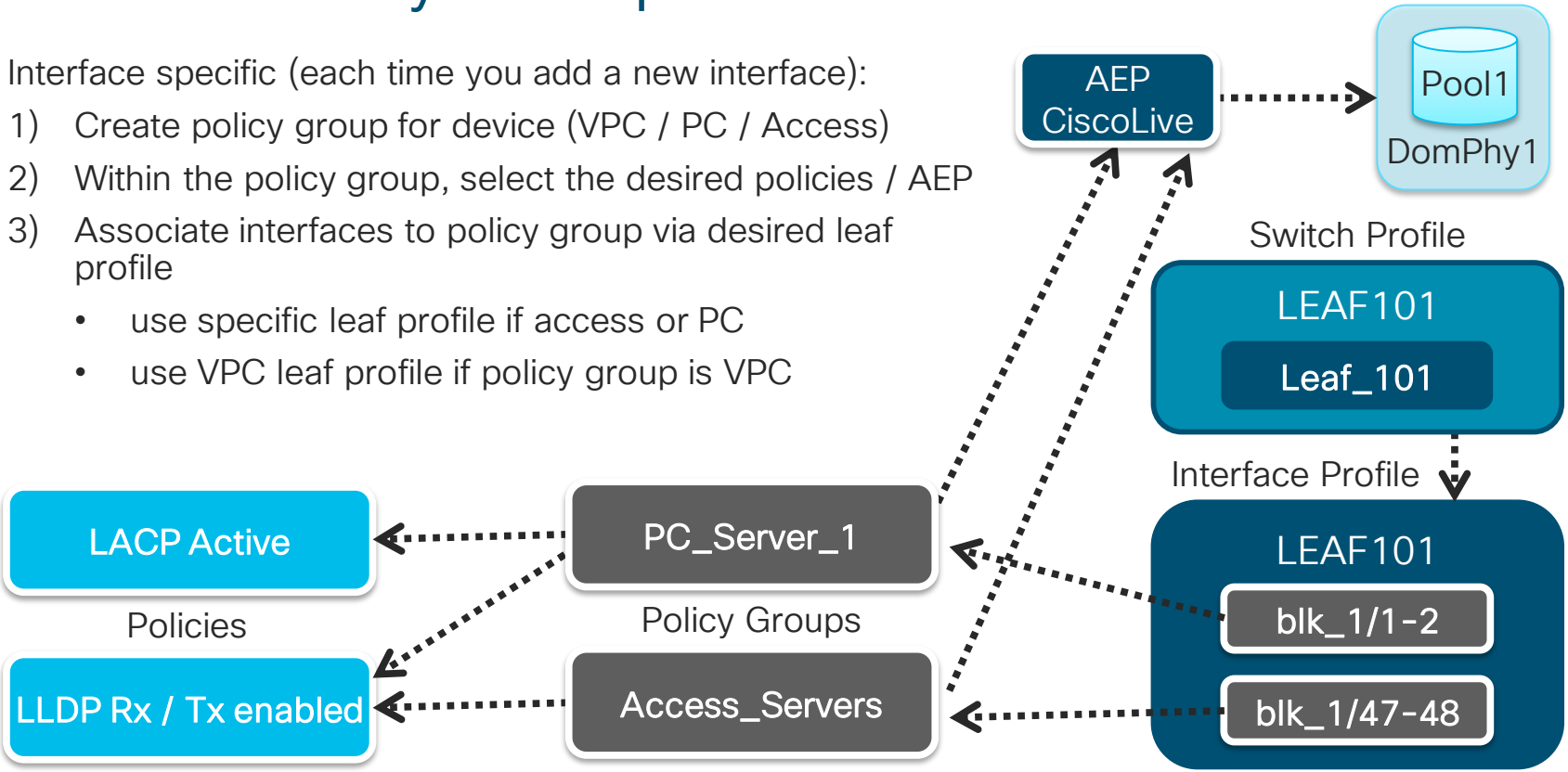




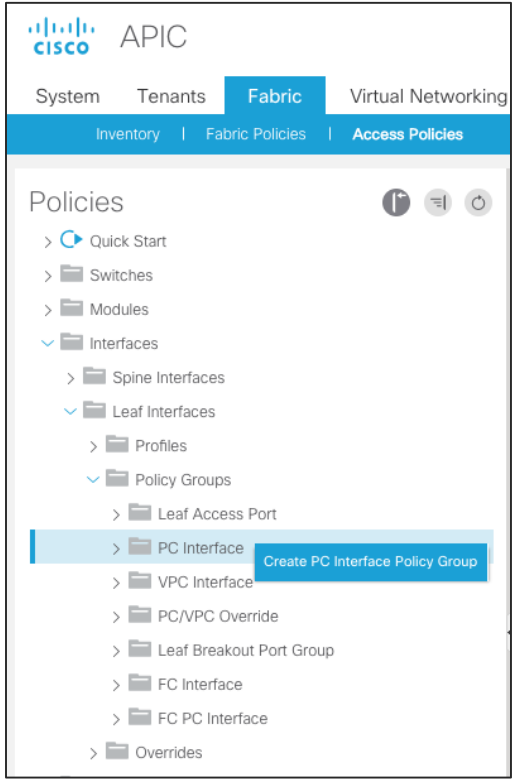
Access Policy Example

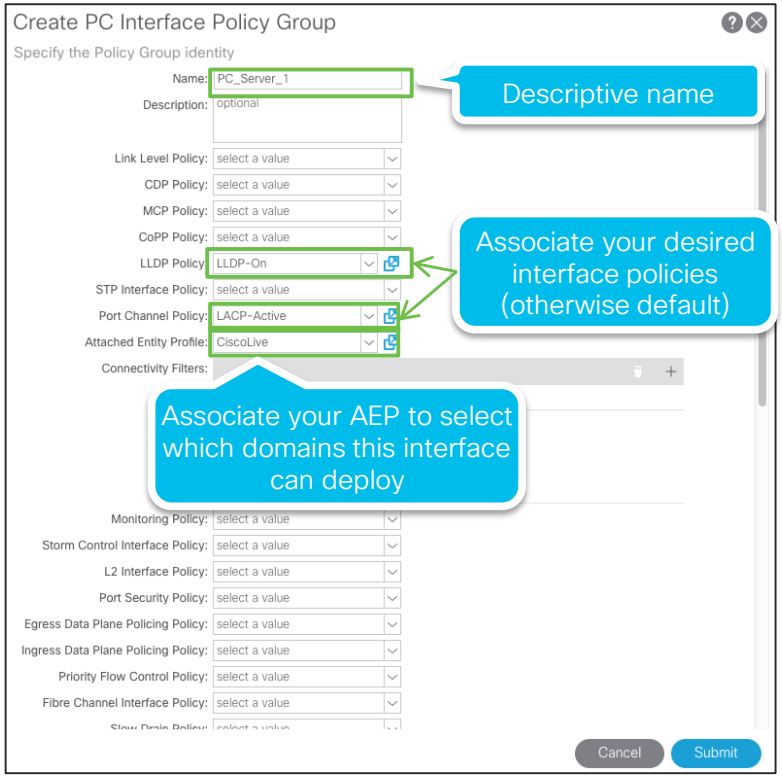
Interface specific (each time you add a new interface):

1) Create policy group for device (VPC / PC / Access)
2) Within the policy group, select the desired policies / AEP
3) Associate interfaces to policy group via desired leaf profile
   - use specific leaf profile if access or PC
   - use VPC leaf profile if policy group is VPC



Create policy groups

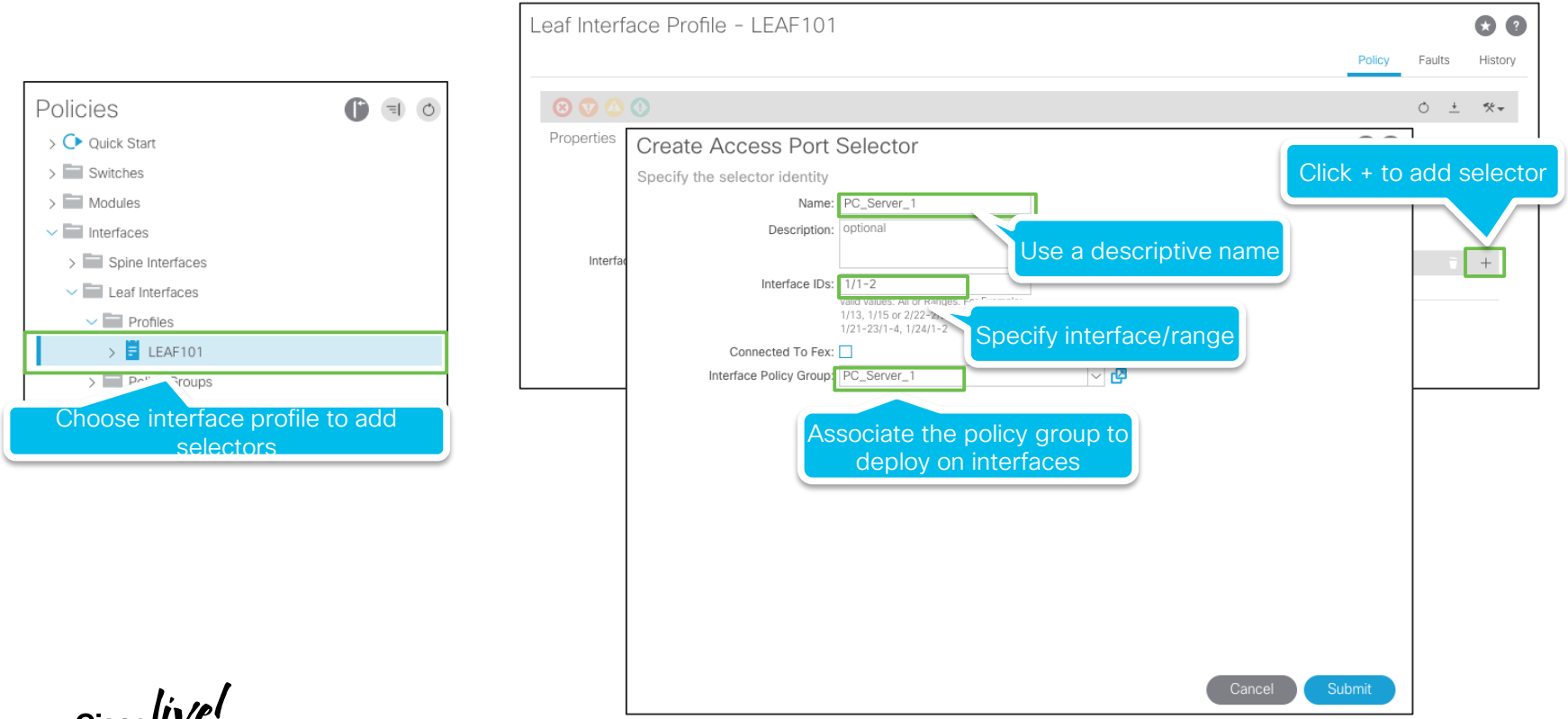




Note:

A separate policy group should be created for each PC/VPC that you will deploy

Create interface selectors / associate policy group



Example policy scheme

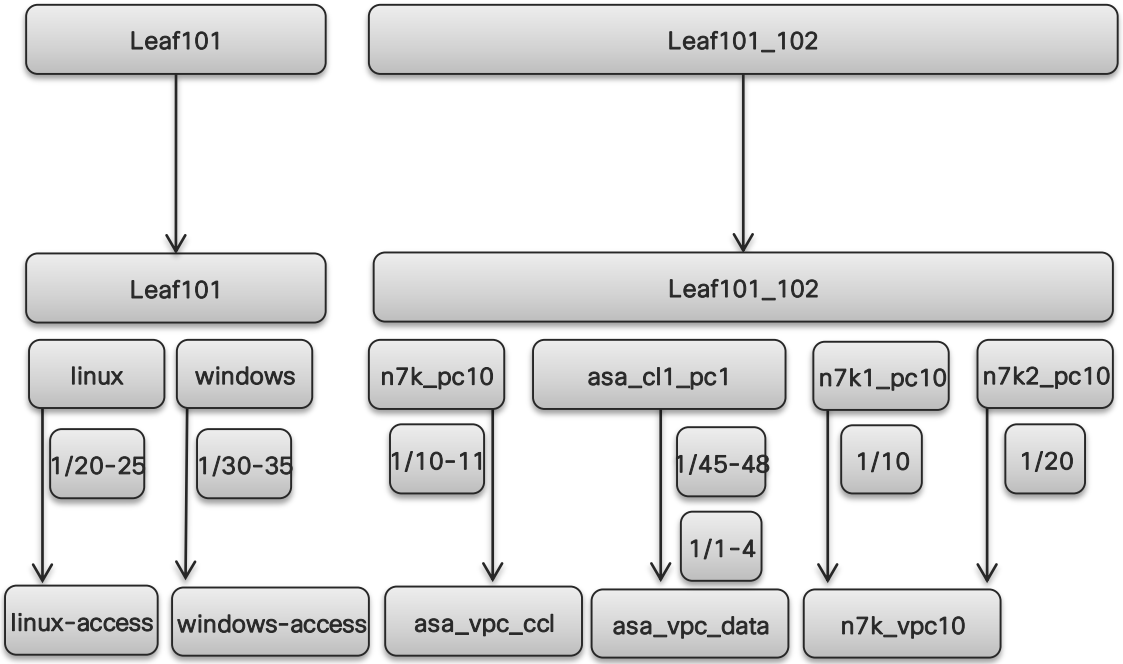
Switch Profile

Interface Profile

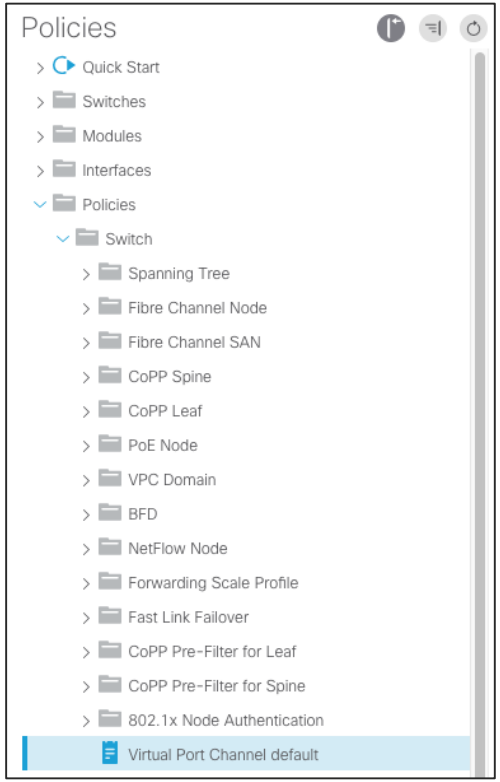
Interface Selector

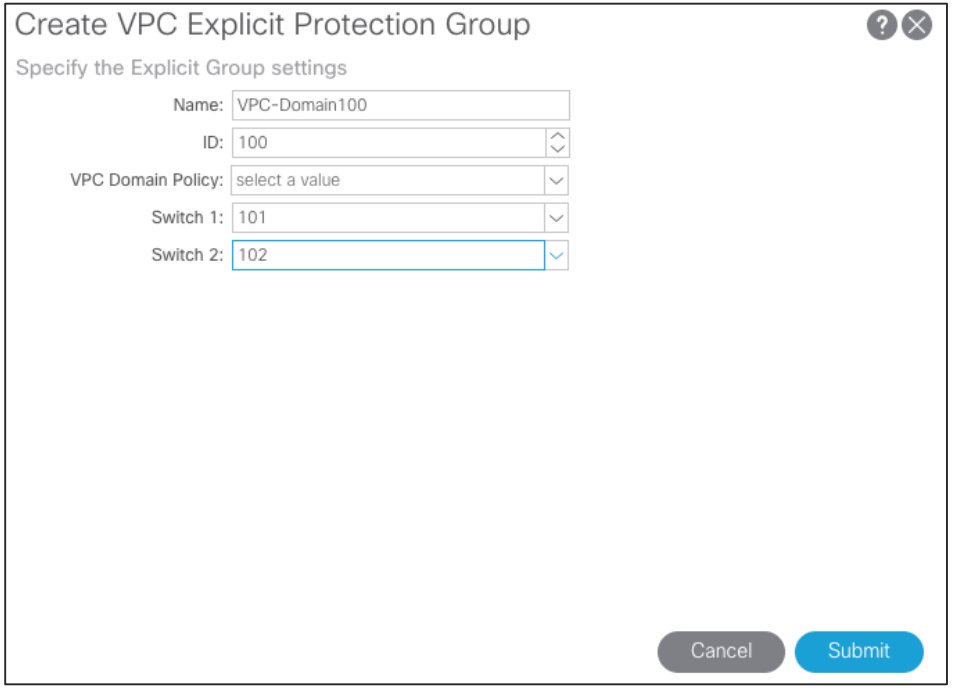
Interface Block

Interface Policy Group



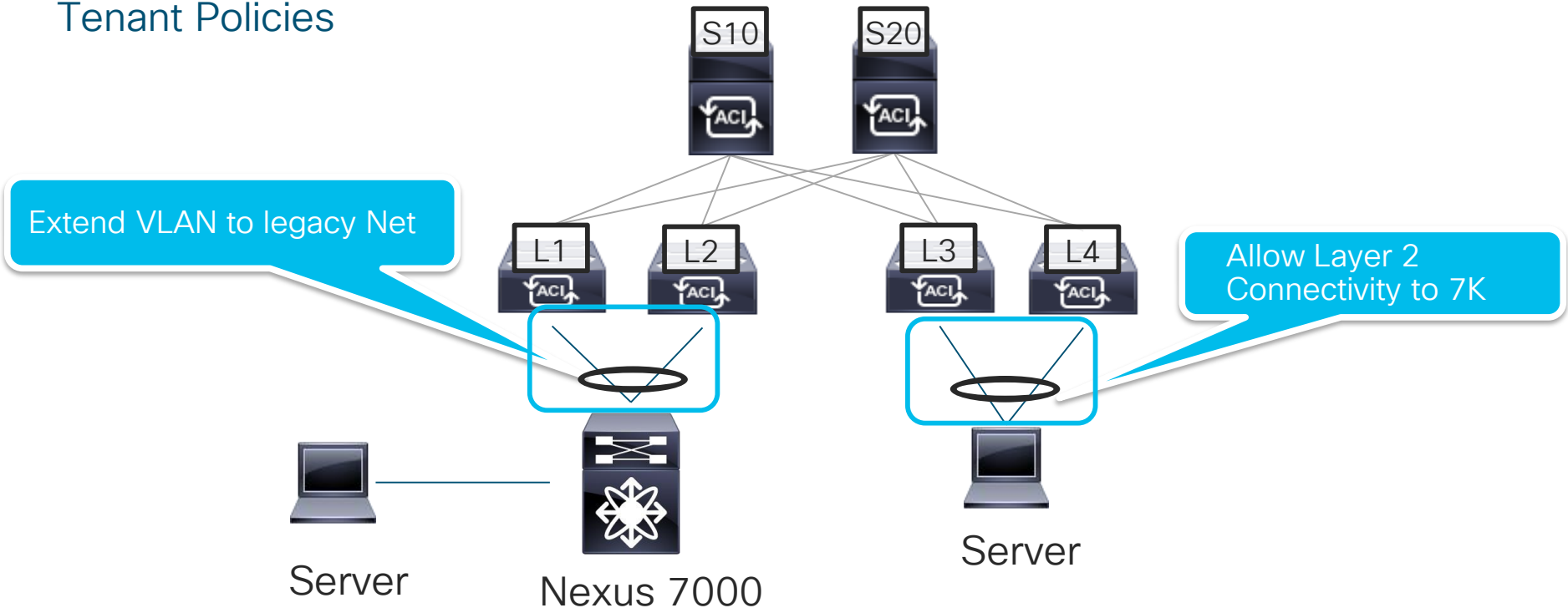
VPC Protection Group (example configuration)





Fabric and Tenant Policies

Tenant Policies



Fabric and Tenant Policies

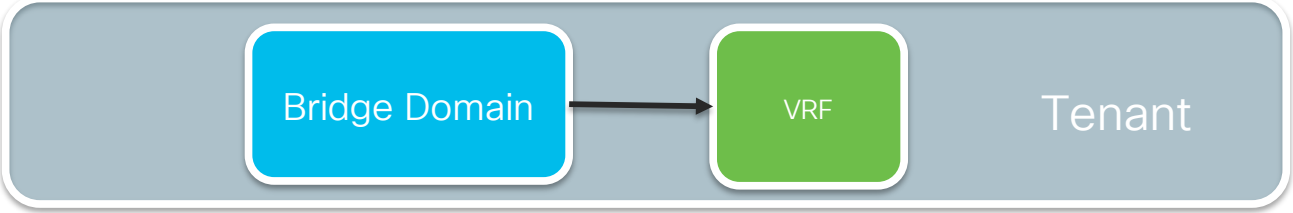
Tenant Policies – Key concepts

Tenants are a Logical Grouping containing Policies. Resources in the **Common Tenant** can be used in **User Tenants**

VRFs are used to separate routing tables inside the ACI Fabric. 1 or more VRFs can be used.

Bridge Domains define your Broadcast/ Flood domain

- Unique VXLAN VNID is used per Bridge Domain
- Configure ARP Optimization and L2 Unknown Unicast Proxy
- Subnet (SVI) can be defined under the BD and is mapped to a single VRF



Fabric and Tenant Policies

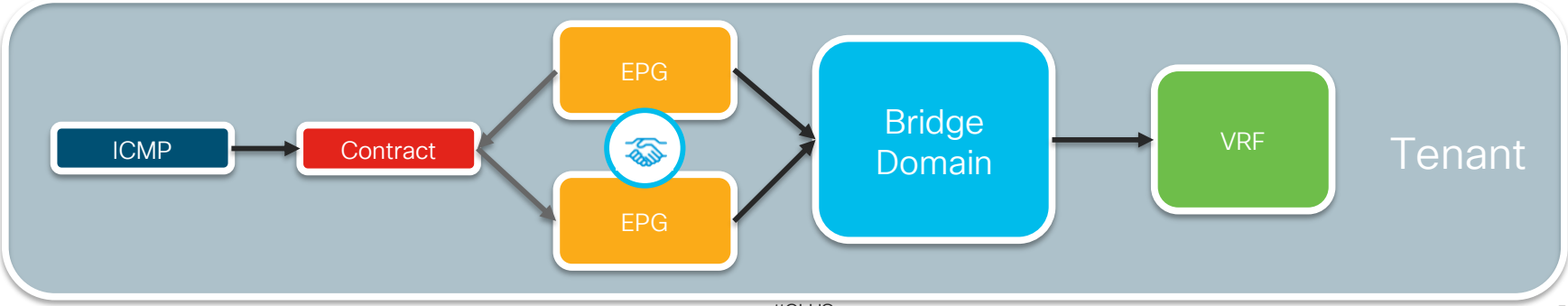
Tenant Policies – Key concepts one EPG to another

EPGs defines a collation of policy assigned to a group of devices

- Contracts, QoS, SPAN requirements
- L4-L7 policies (PBR, Load balancing, Firewalls)
- EPG is most commonly determined by ingress VLAN & Port

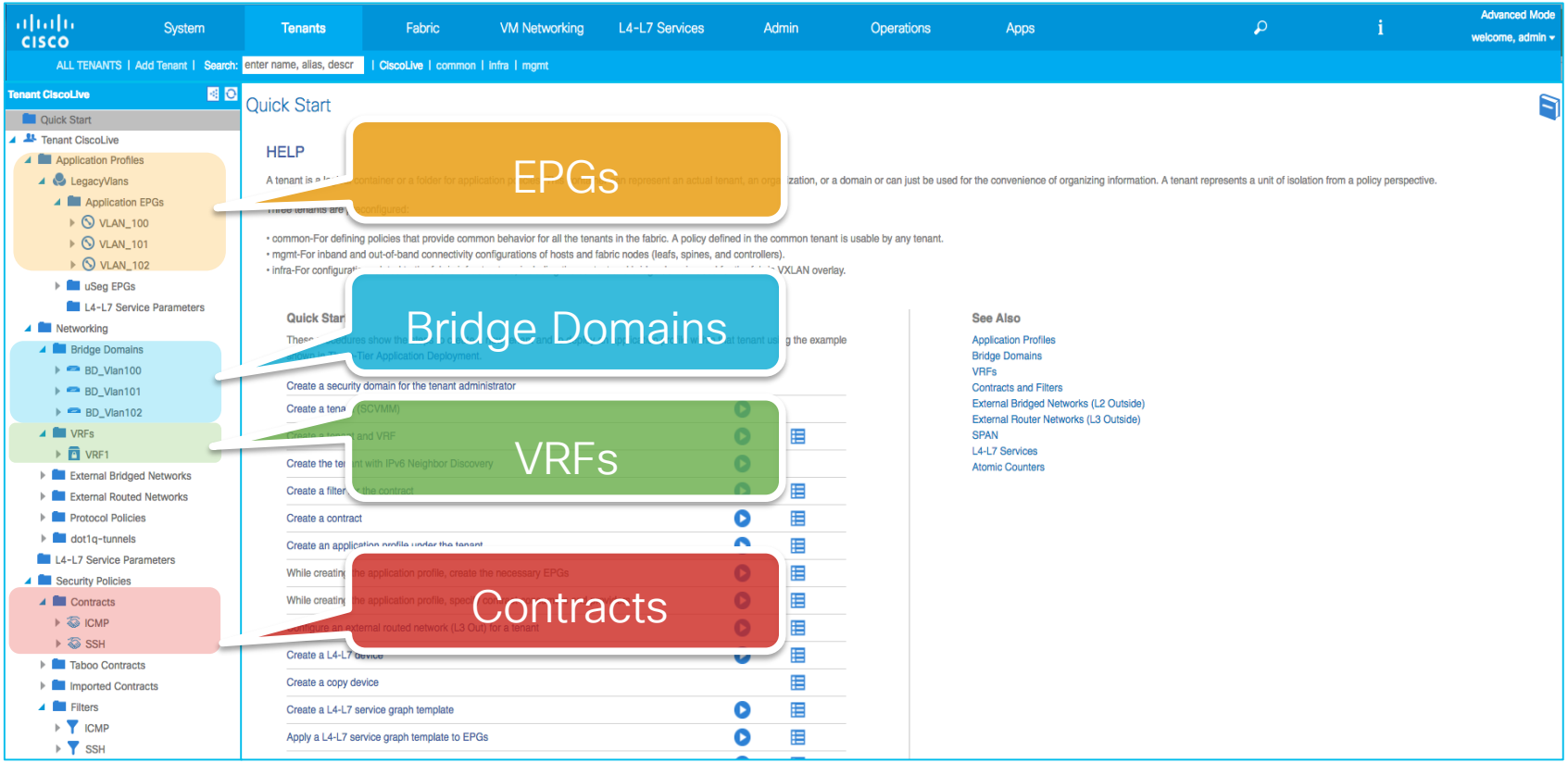
Contracts are a collection of filters which allow traffic to pass between EPGs

- Contacts are similar to access-lists. Consumer is Source, Provider is Destination
- Filters contain a list of protocols and ports



Fabric and Tenant Policies

Tenant View



Fabric and Tenant Policies

Deploying a VRF

Create VRF

STEP 1 > VRF

Specify Tenant VRF

Name: VRF2

Alias:

Description: optional

Policy Control Enforcement Preference: Enforced | Unenforced

Policy Control Enforcement Direction: Egress | Ingress

End Point Retention Policy: select a value

This policy only applies to remote L3 entries

Monitoring Policy: select a value

DNS Labels:

enter names separated by comma

Route Tag Policy: select a value

Create A Bridge Domain: ☑

Configure BGP Policies: ☐

Configure OSPF Policies: ☐

Configure EIGRP Policies: ☐

Change the VRF from a White-List model to an "Allow All" Model

Fabric and Tenant Policies

Deploying a Bridge Domain

STEP 1 > Main

1. Main | 2. L3 Configurations

Specify Bridge Domain for the VRF

Name: BD_VLAN100

Alias:

Description: optional

Type: fc | regular

VRF: CiscoLive/VRF1

Forwarding: Optimize

End Point Retention Policy: default

This policy only applies to local L2 L3 and remote L3 entries

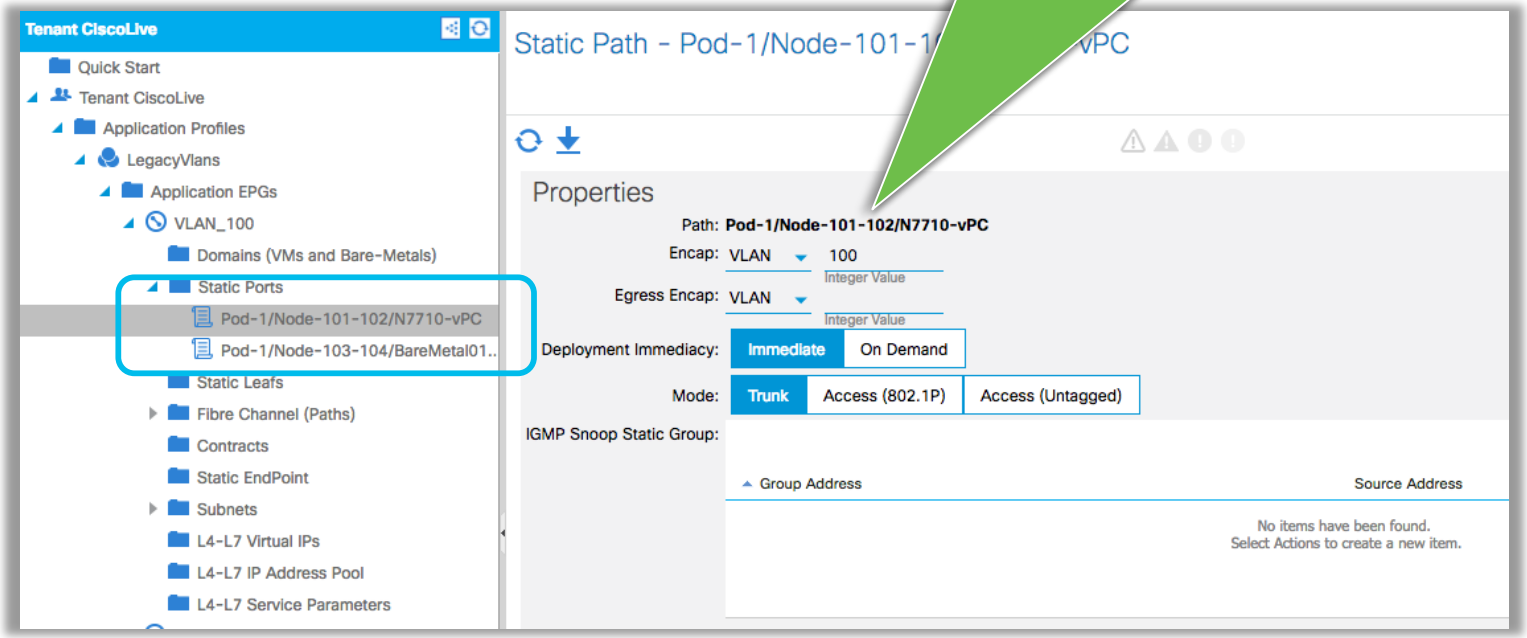
IGMP Snoop Policy: default

Associate Bridge Domain to VRF

Fabric and Tenant Policies

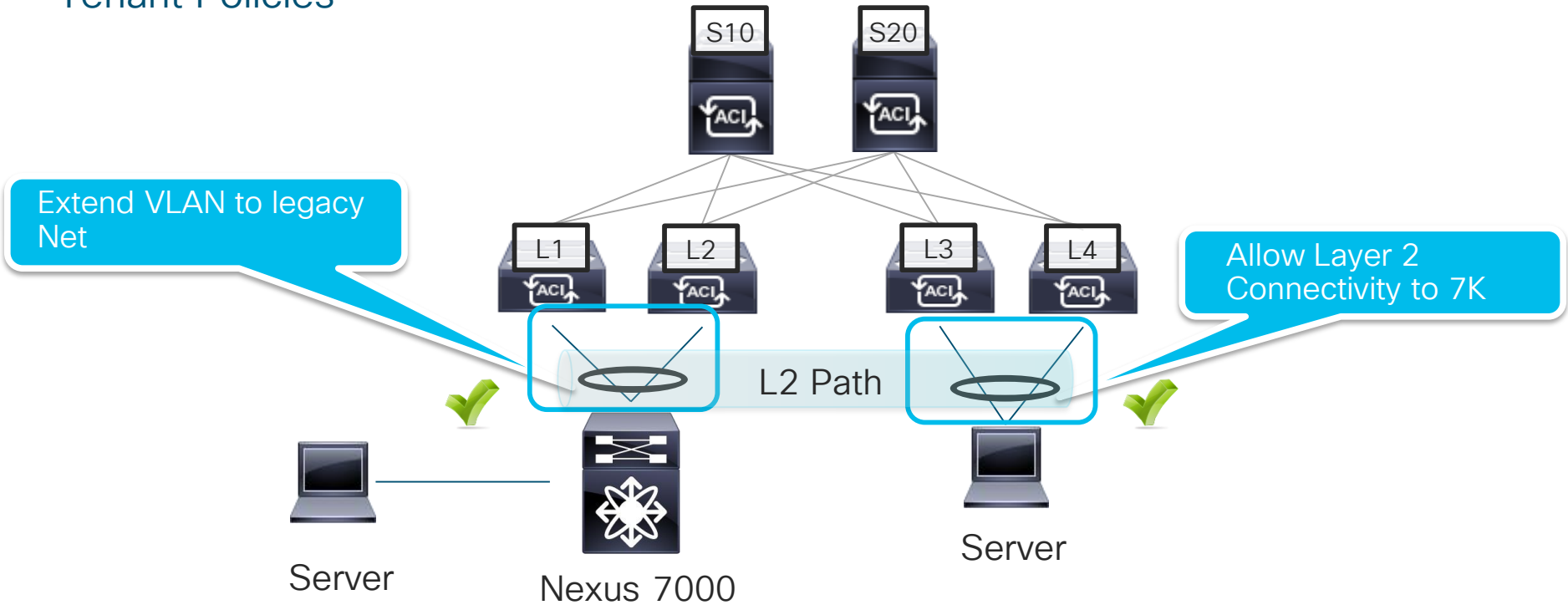
Deploying an EndPoint Group

```
N7710# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
N7710(config)# interface port-channel 1
N7710(config-if)# switchport trunk allowed vlan add 100
```



Fabric and Tenant Policies

Tenant Policies



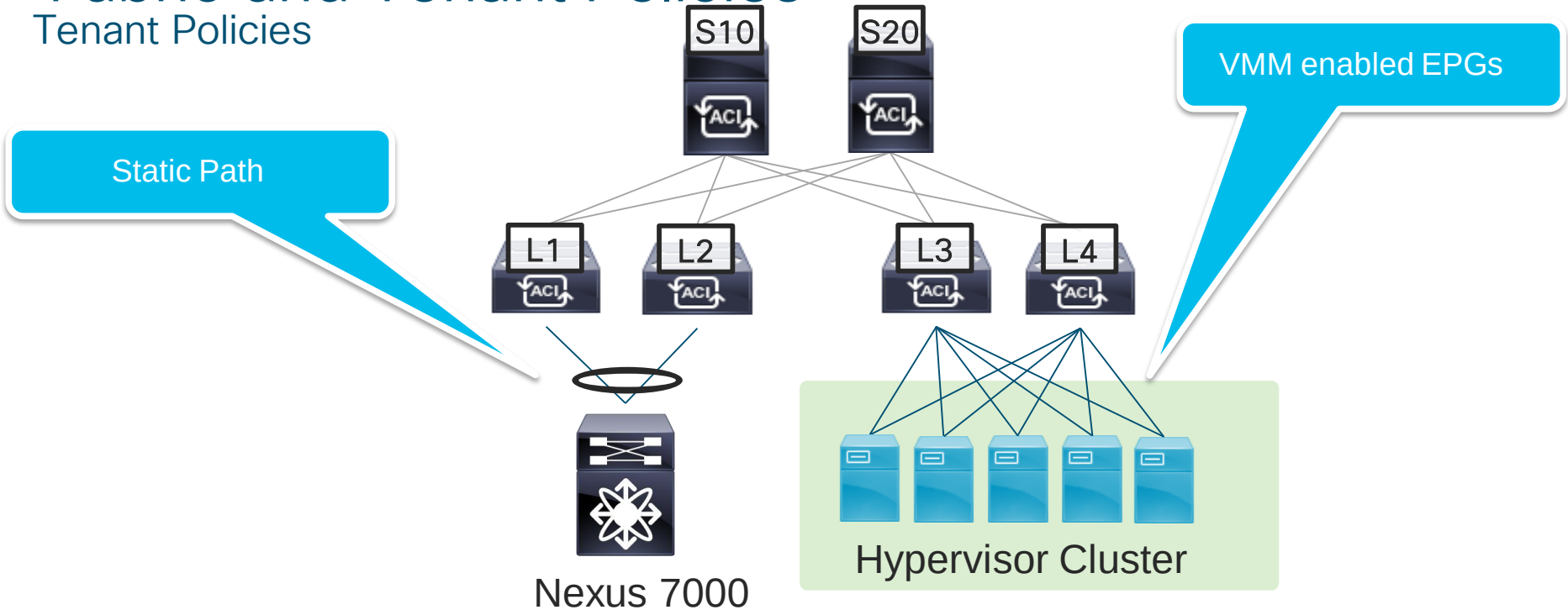
Fabric and Tenant Policies

Planning

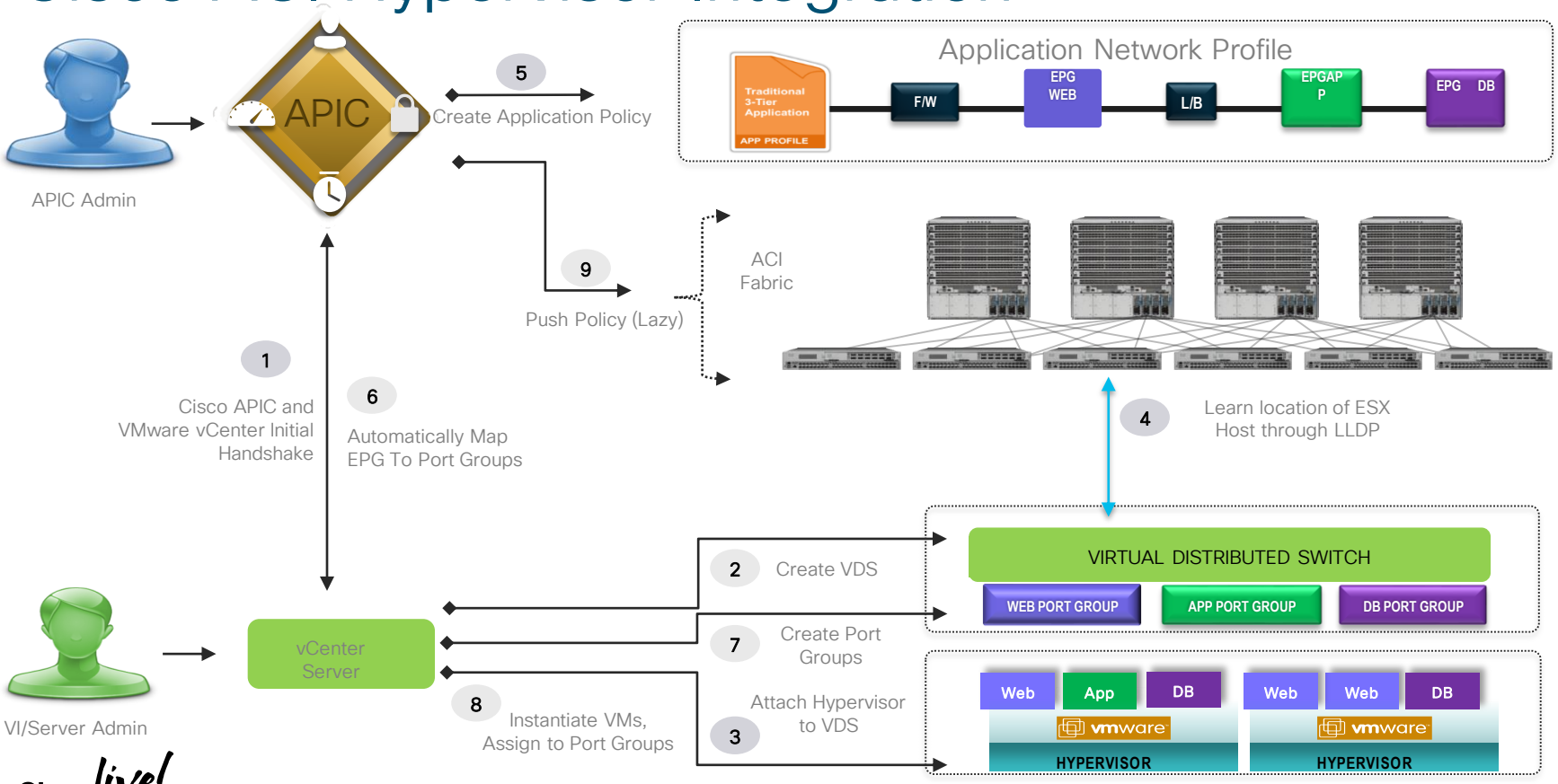
Requirements	Notes	Example
Tenant	1 Tenant can be used company. Tenants can also separate functions of a business. NOTE: Shorter names are easier when using CLI	Prod/Dev
VRF	1 or more VRFs per Tenant	PROD-MAIN DEV-TEST,DEV-PROD
Bridge Domain	Recommended to have 1 BD per Legacy VLAN. For Network Centric Migrations, 1 BD should be used for each EPG.	VLAN_100,VLAN_101 BD_vMotion
Application Profile	Logical Container for EPGs. 1 AP is sufficient in most installations. NOTE: This is strictly a management entity. No policies are defined on this object.	Prod-AP
EndPoint Group	Ports/VLANs (static path bindings) are added to EPGs to define what Endpoints get defined in what EPGs. QOS/Contracts, etc are added to EPGs. For Network Centric Migrations, 1 EPG should be used for each Legacy VLAN.	VLAN_100 VLAN_101 vMotion
Contracts	Contracts can be re-used across multiple EPGs. If we compare this to an ACL, the Consumer is the Source, and the Provider is the Destination.	Web
Filters	Add Required Ports and Protocols to allow communication. Only what is specified in the filter → contract will be allowed between EPGs providing and consuming that contract.	SRC: Any, DST:80 SRC: Any, DST:443

Fabric and Tenant Policies

Tenant Policies

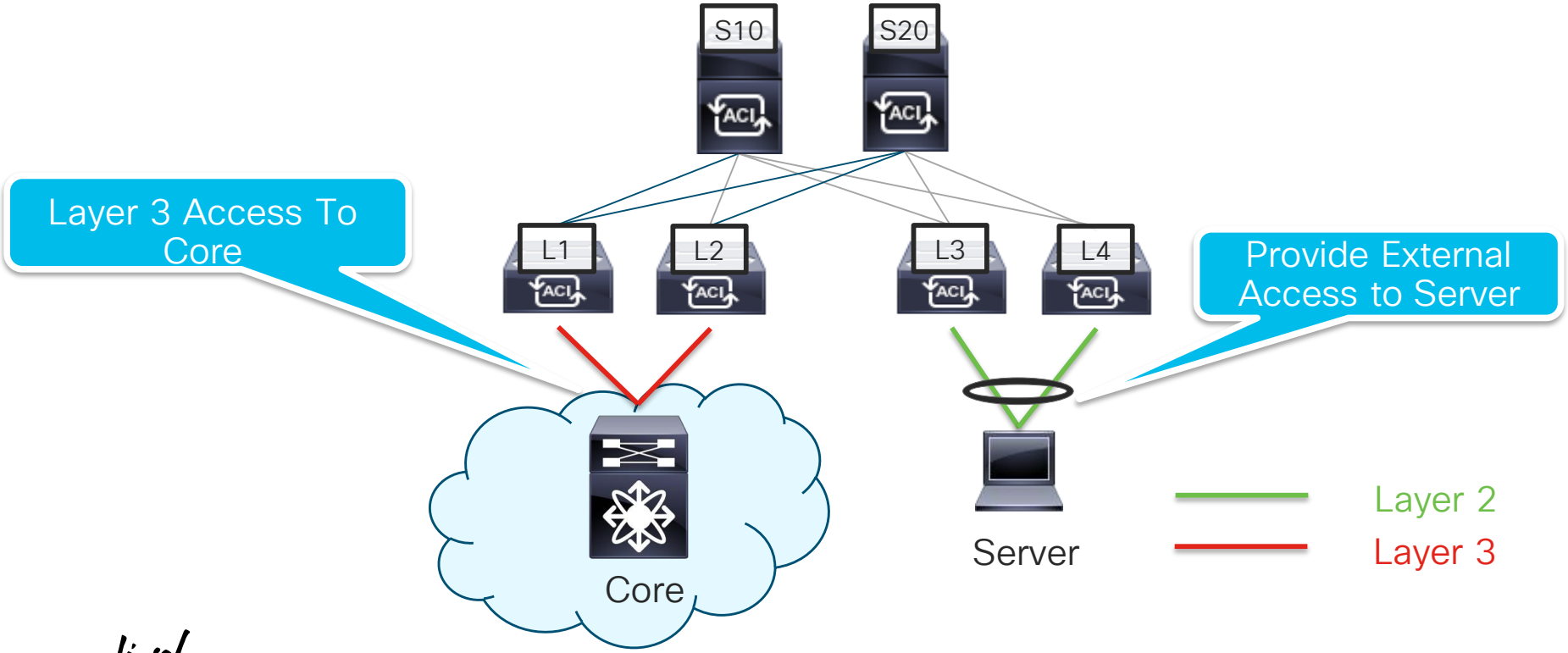


Cisco ACI Hypervisor Integration



Fabric and Tenant Policies

Layer 3 Connectivity



Basic Connectivity

Layer3 Out: L3Out-1
VRF: VRF-V1
Layer-3 Domain: DomL3

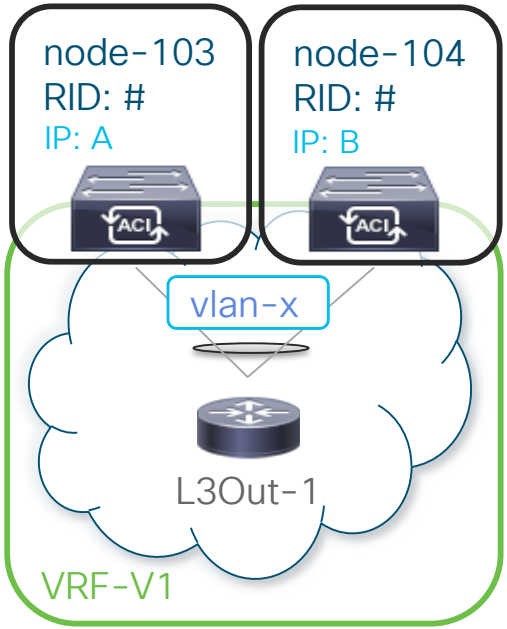
Logical Node Profile: node-103-104

node: node-103
Router-ID: #

node: node-104
Router-ID: #

Logical Interface Profile: ipv4-lif

path: topology/pod-1/...vpcX
type: ext-svi, encap: vlan-x
IP-A, IP-B, MTU, MAC

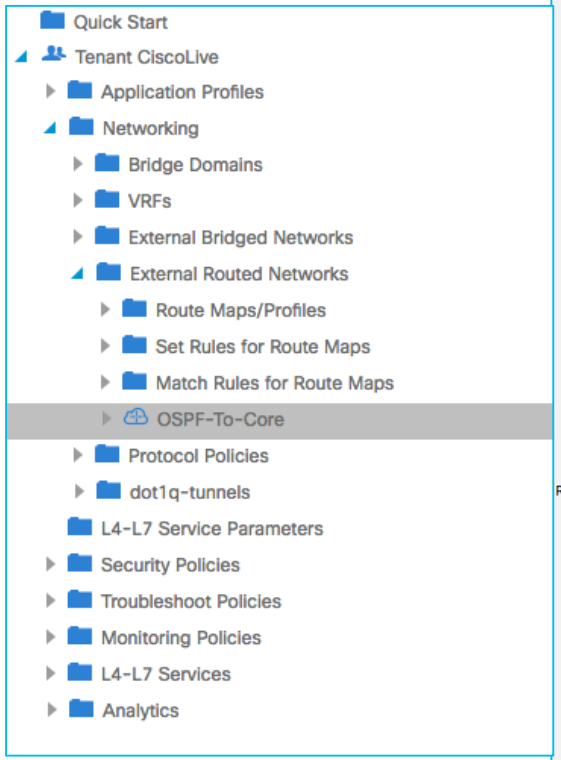


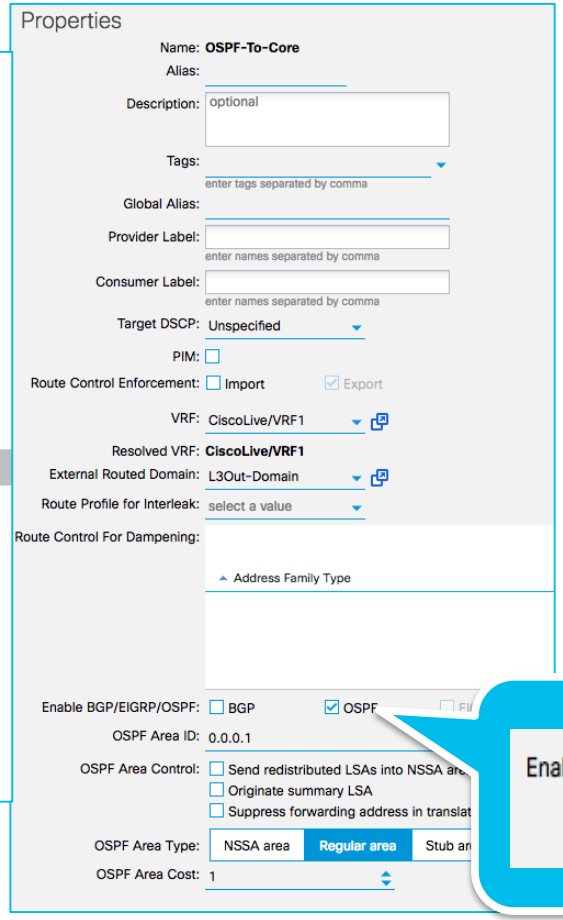
Create the L3Out

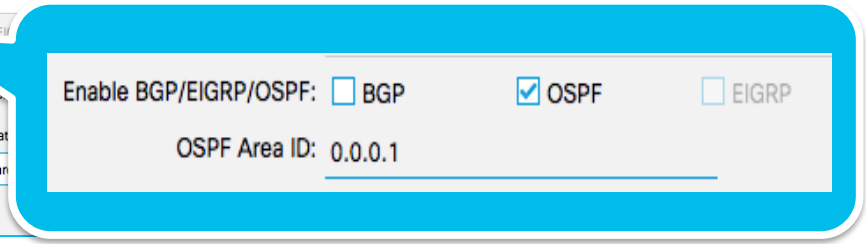
- Associate VRF and L3 Domain
- Create Logical Node Profile and associate fabric nodes to the L3Out.
- Create Logical Interface Profile
- Specify Path attributes containing physical interface, encapsulation, and IPs

Fabric and Tenant Policies

Creating a Layer 3 Out





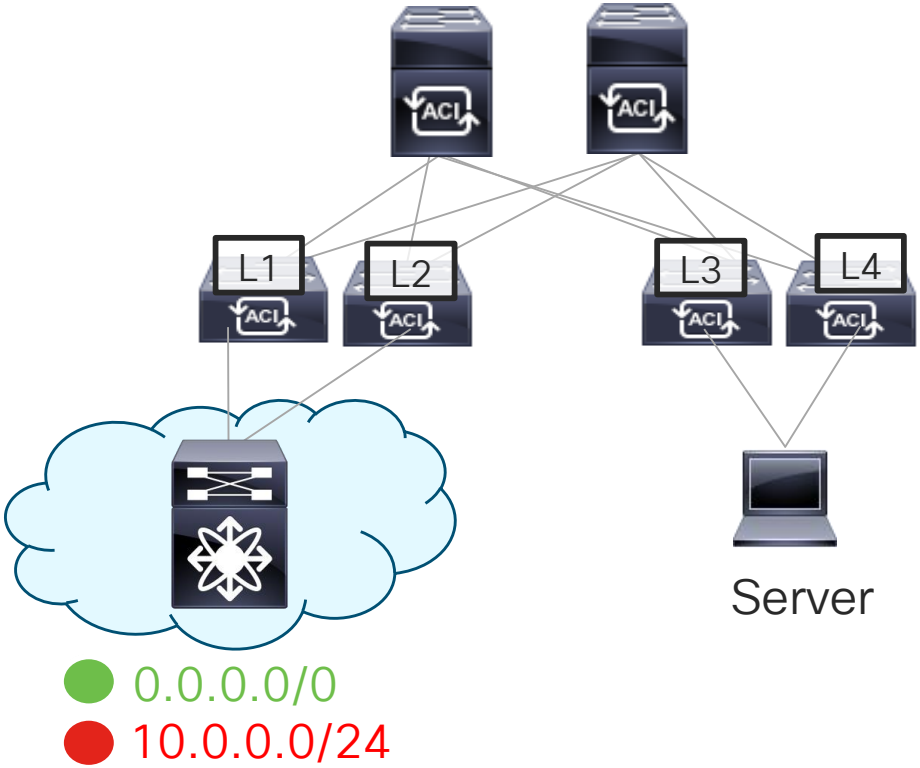


- External Routed Networks allow us to peer with external routers
- Dynamic Protocols
  - EIGRP
  - OSPF
  - BGP
- Static Routing

Fabric and Tenant Policies

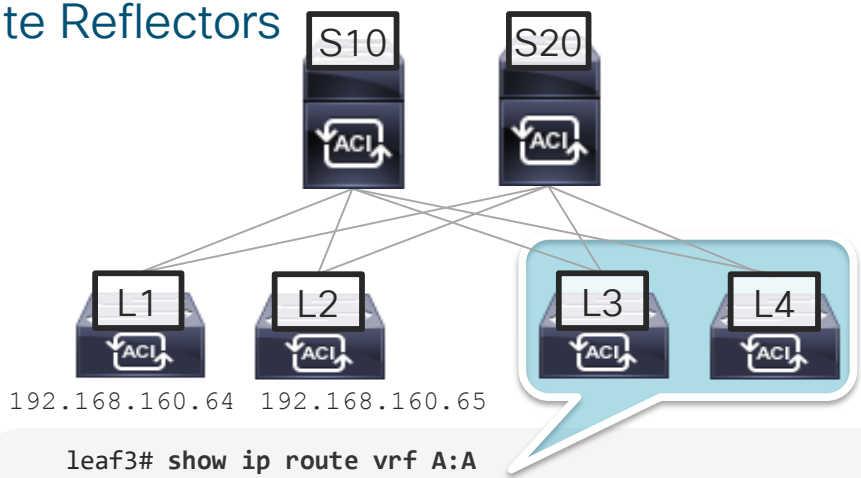
Route Reflectors

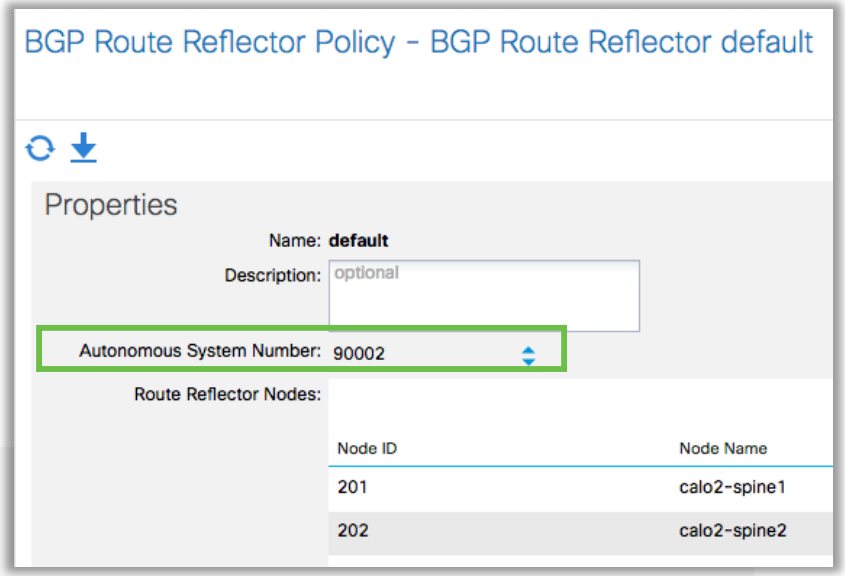
- Fabric nodes communicate using MP-BGP.
- BGP advertises routes from Border Leaf to Compute Leafs.
- Runs in overlay-1 VRF



Fabric and Tenant Policies

Route Reflectors






```
leaf3# show ip route vrf A:A
IP Route Table for VRF "A:A"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

0.0.0.0/0, ubest/mbest: 1/0
    *via 192.168.160.64%overlay-1, [200/1], 03w21d, bgp-90002, internal, tag 90002
    *via 192.168.160.65%overlay-1, [200/1], 03w21d, bgp-90002, internal, tag 90002
10.0.0.0/24, ubest/mbest: 1/0
    *via 192.168.160.64%overlay-1, [200/1], 03w21d, bgp-90002, internal, tag 90002
    *via 192.168.160.65%overlay-1, [200/1], 03w21d, bgp-90002, internal, tag 90002
```

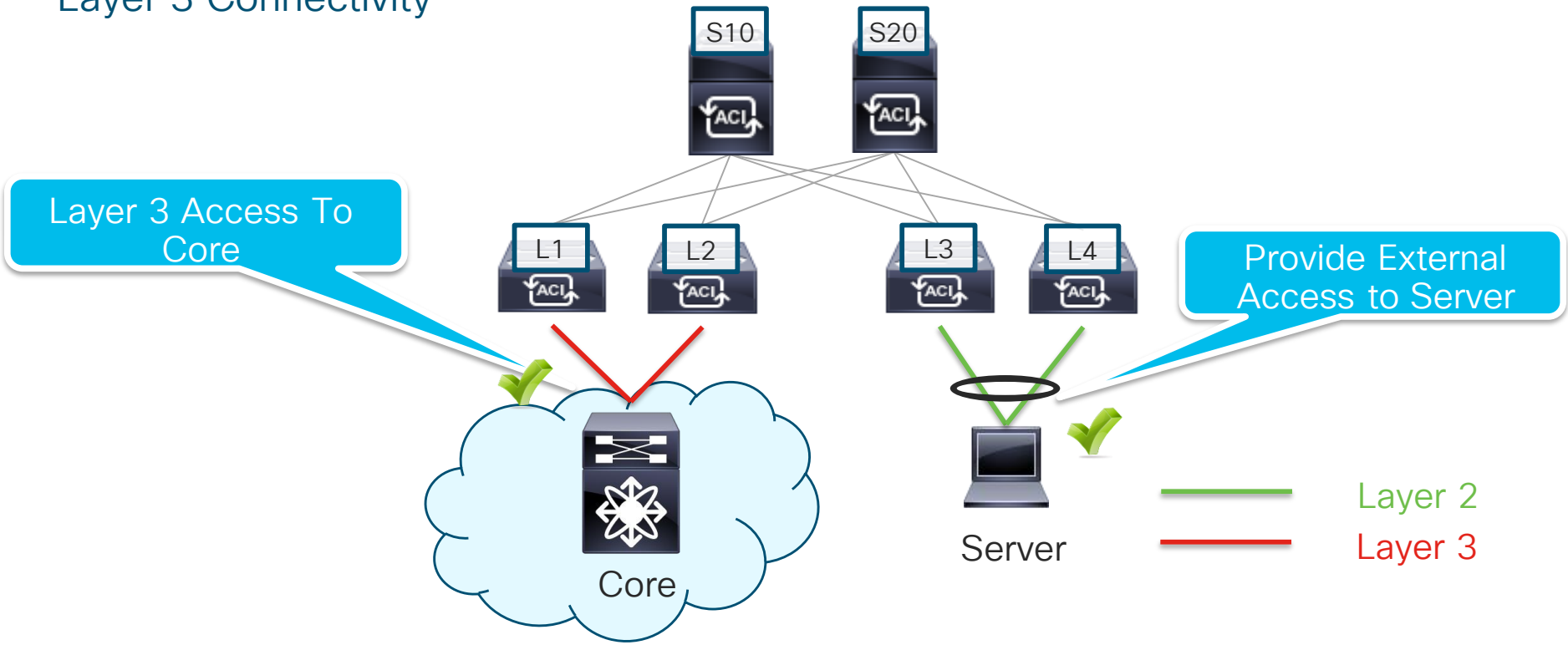
Fabric and Tenant Policies

Planning

Requirements	Notes	Example
BGP Route Reflector	Use an AS Number not already in your environment. The AS number is only exposed to the external network when peering BGP with devices. Private AS number can be used. NOTE: CHANGING THE AS NUMBER IS DISRUPTIVE!	65000
External Routed Network	This is your Layer 3 Object. It contains the entire Layer 3 path configuration.	L3out-To-Core
Node Profile	Defines which nodes are part of the Layer 3 out Domain. Here is where you define your Router ID's and Static Routes.	Leaf101, Leaf102 Leaf101-102
Logical Interface Profile	Defines which interfaces are used for peering. Support Types are Routed Interfaces, Routes Sub-Interfaces, and SVIs. This is also where you define the IP/MTU/VLAN is SVI or Sub-Interface.	Port10 vPC-To-Core
Networks (External EPG)	This is where you define the external subnets you want to apply policy to. You do this by listing the subnets and applying contracts. NOTE: multiple all 0's subnets should not be configured in the same VRF.	Ext_EPG → 0.0.0.0/0 subnet

Fabric and Tenant Policies

Layer 3 Connectivity



Day 3: Forwarding Overview

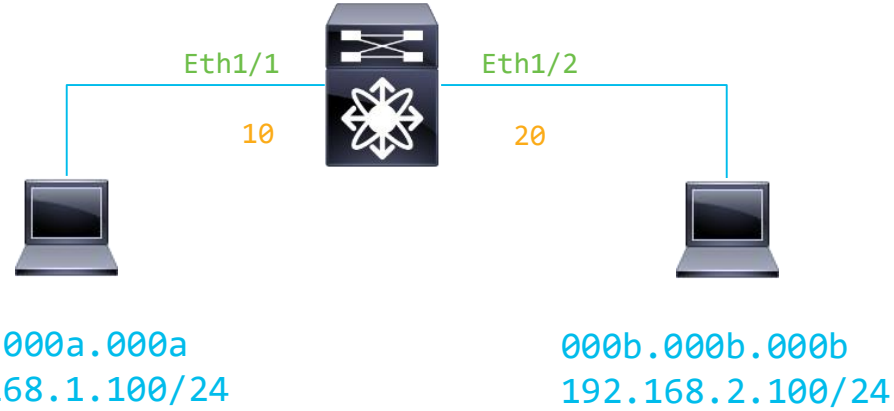
You make networking **possible**

What is an Endpoint?

Traditional Endpoint

L2 – MAC Table
- MAC Address
- VLAN
- Interface

L3 – ARP Table
- IP / MAC
- Interface
- VRF



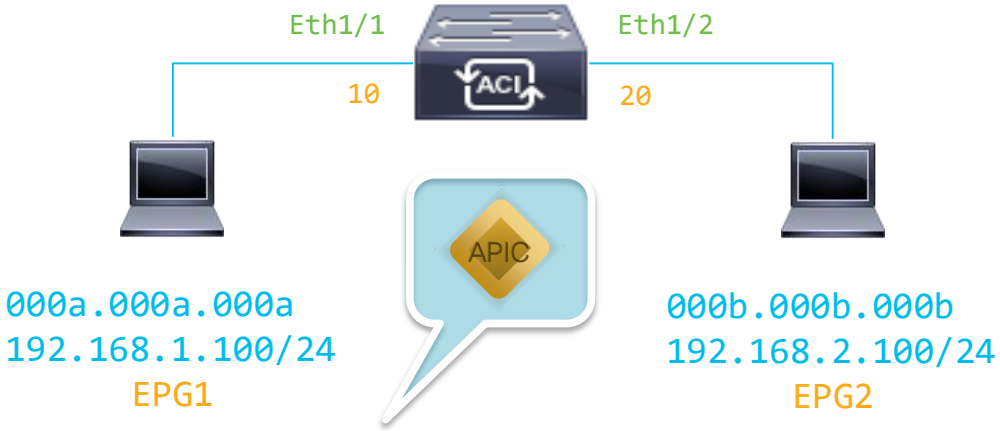

```
N5K# show ip arp vrf default | grep 000a
192.168.1.1      00:00:01 000a.000a.000a  Vlan10
N5K# show mac address-table | grep 000a
10       000a.000a.000a     dynamic    0    Eth1/1
```

```
N5K# show ip arp vrf default | grep 000b
192.168.2.1      00:00:01 000b.000b.000b  Vlan20
N5K# show mac address-table | grep 000b
20       000b.000b.000b     dynamic    0    Eth1/2
```

What is an Endpoint?

ACI Endpoint

- MAC or MAC/IP → IP is /32 or /128 Route
- VLAN → EPG (pcTag)
- Interface
- VRF
- Flags → Local, vPC, static, etc.

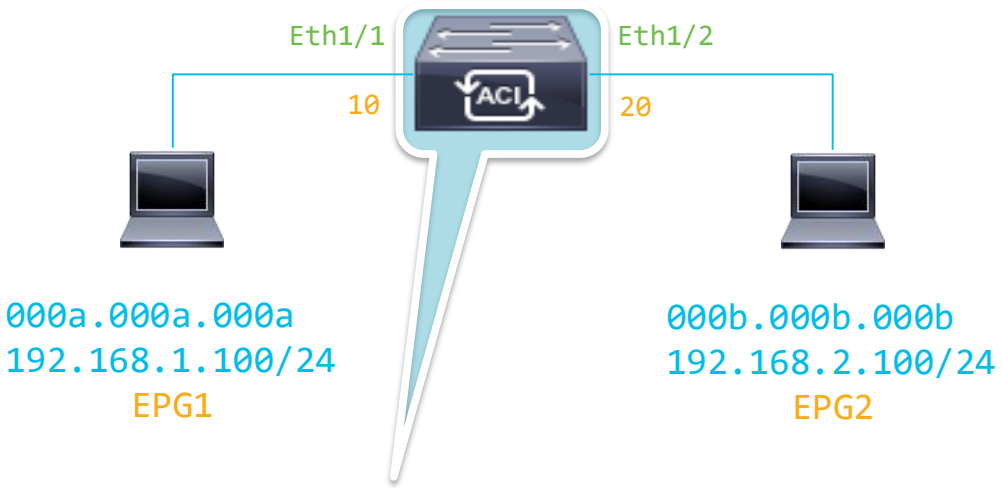



```
apic1# show endpoints ip 192.168.1.100
Dynamic Endpoints:
Tenant      : CL
Application : CL
AEPg        : EPG1


 End Point MAC      IP Address                                  Node        Interface                        Encap
 -----------------  ------------------------------------------  ----------  -------------------------------  ---------------
 00:0A:00:0A:00:0A  192.168.1.100                               101         eth1/1                           vlan-10
```

What is an Endpoint?

ACI Endpoint

- MAC or MAC/IP → IP is /32 or /128 Route
- VLAN → EPG (pcTag)
- Interface
- VRF
- Flags → Local, vPC, static, etc.

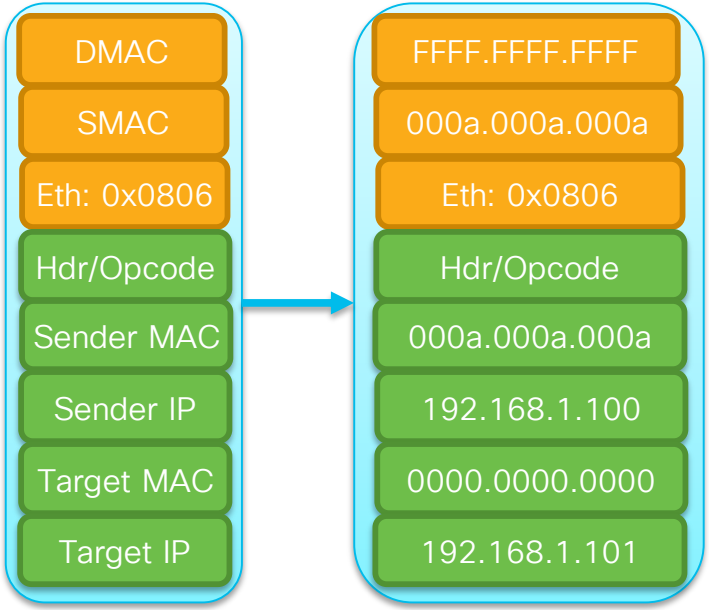



```
Leaf1# show endpoint mac 000a.000a.000a detail
Legend:
 s - arp              O - peer-attached    a - local-aged       S - static
 V - vpc-attached     p - peer-aged        M - span             L - local
 B - bounce           H - vtep
+-----------------------------------+---------------+-----------------+--------------+-------------+----------------+
      VLAN/                          Encap           MAC Address       MAC Info/       Interface   Endpoint Group
      Domain                         VLAN            IP Address        IP Info                     Info
+-----------------------------------+---------------+-----------------+--------------+-------------+----------------+
16                                   vlan-10         000a.000a.000a    L               eth1/1       CL:CL:EPG1
CL:17                                vlan-10         192.168.1.100     L               eth1/1
```

Endpoint Learning - ARP

ACI Leafs learn via ARP!

ARP Request



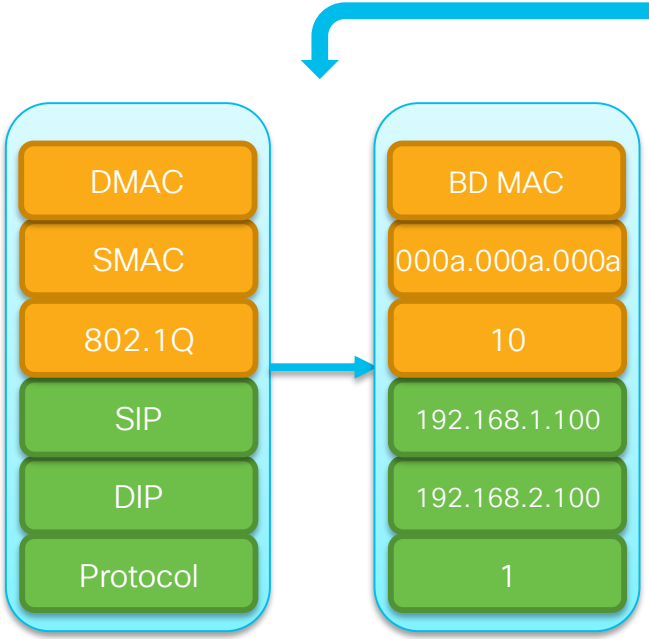
000a.000a.000a
192.168.1.100/24
EPG1

000b.000b.000b
192.168.1.101/24
EPG1

Frame	Unicast Routing?	EP Contents
ARP	No	MAC (Sender MAC)
ARP	Yes	MAC (Sender MAC), IP (Sender-IP)

Endpoint Learning- Routed Packets

Routed Packet triggers an EP Learn



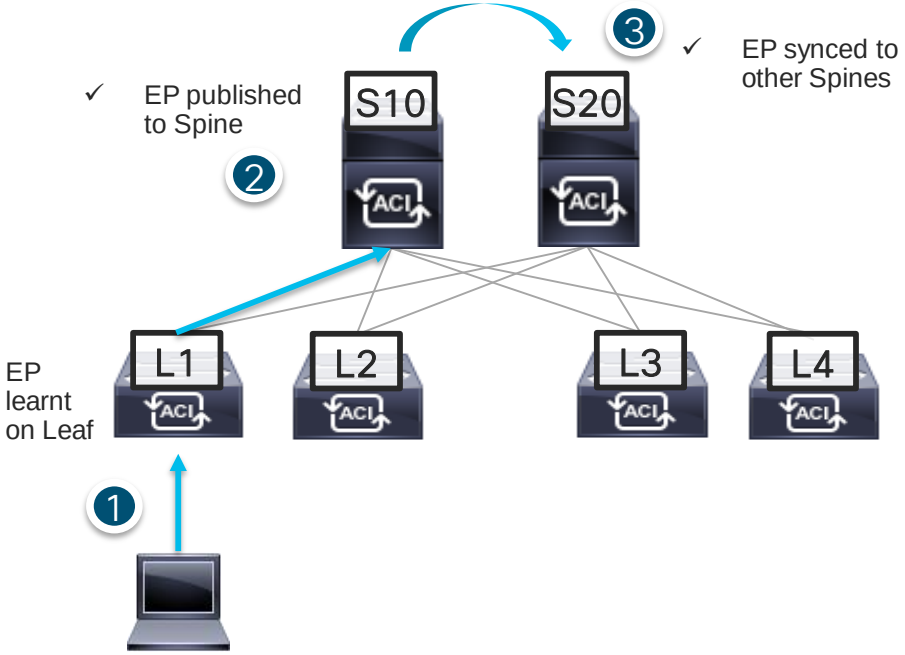
000a.000a.000a
192.168.1.100/24
EPG1

000b.000b.000b
192.168.2.100/24
EPG2

Frame	Unicast Routing	EP Contents
IPV4/6	Yes	MAC (L2 SRC MAC), IP (SRC IP)

Proxy Routing

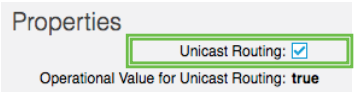
- Leafs report EP's to spine once Learnt
- Spines maintain a database of all Endpoints Learnt in the Fabric, and on what Leaf(s) they exist.
- Used for "Hardware Proxy" BD Mode.

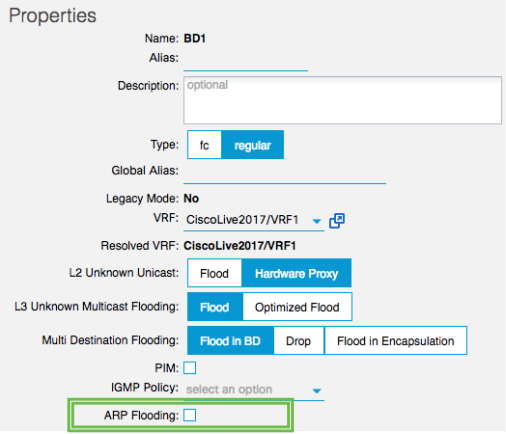


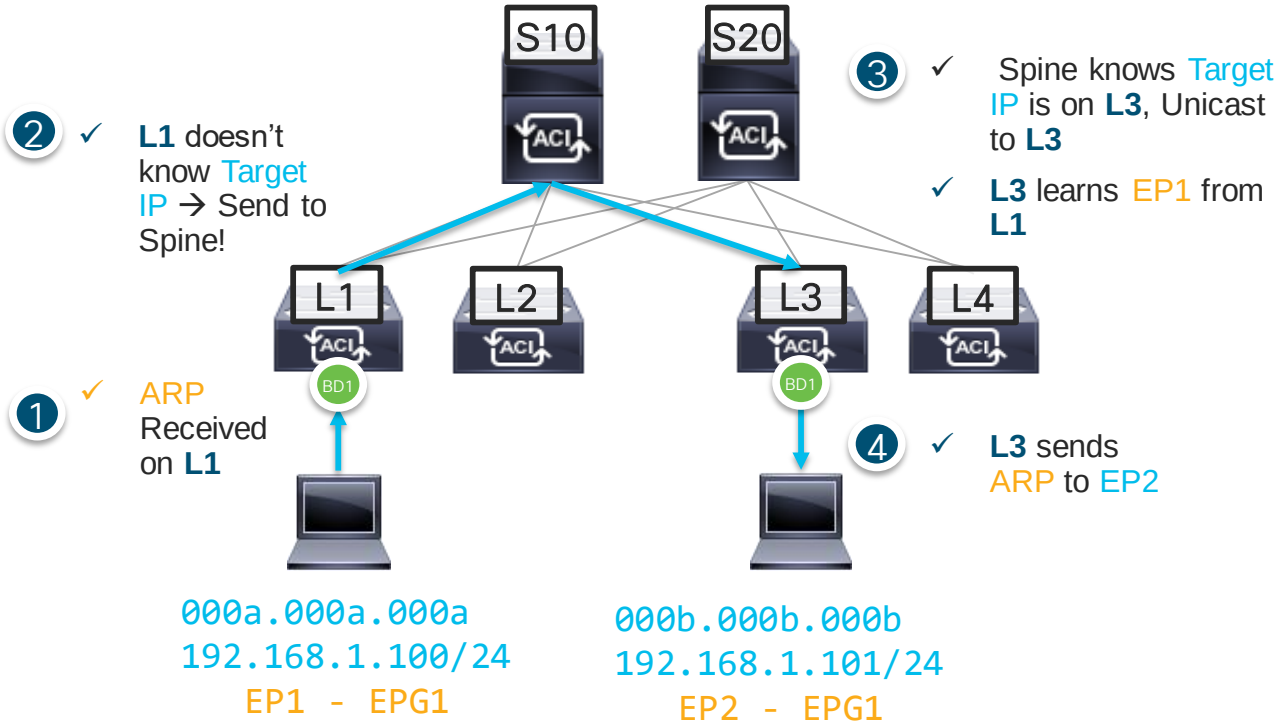
ARP Optimization – Unicast Routing

EP1 ARP's for EP2

- ACI can Unicast ARP to avoid unnecessary Flood traffic. → Requires Unicast Routing on BD



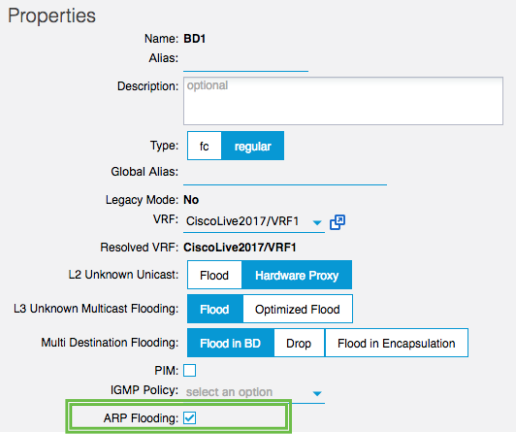


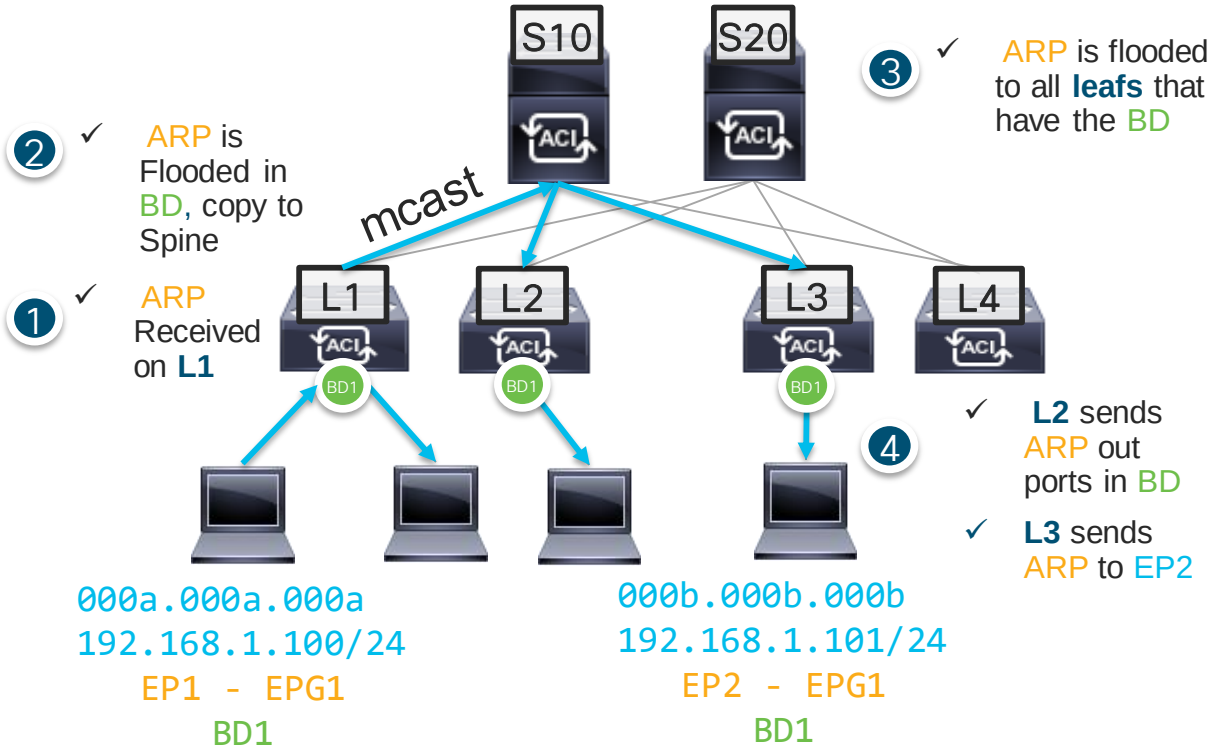


ARP Flooding

EP1 ARP's for EP2

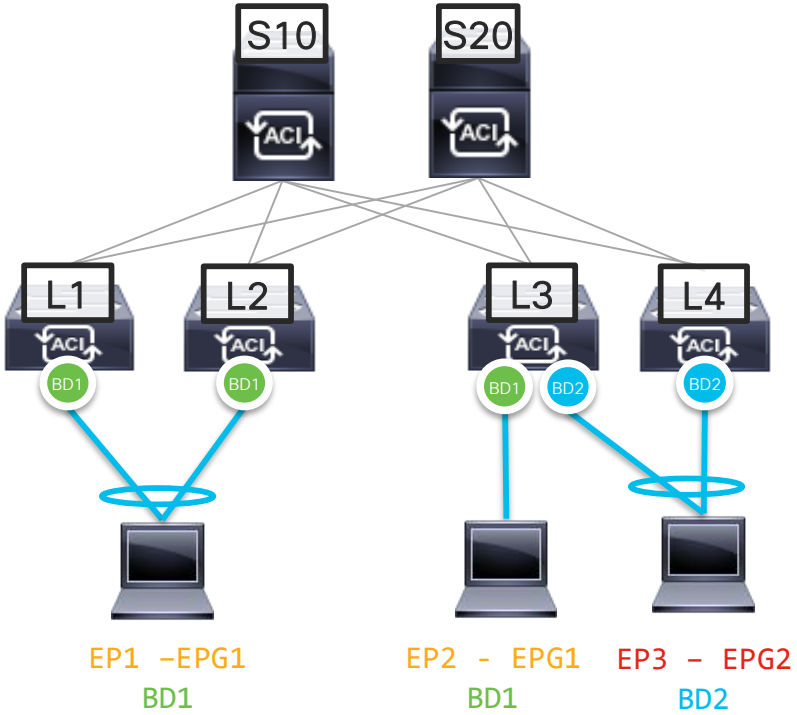
- Behavior is the same as Traditional Switches
- ARP is flooded using BD Multicast Group to all Leafs that have the BD





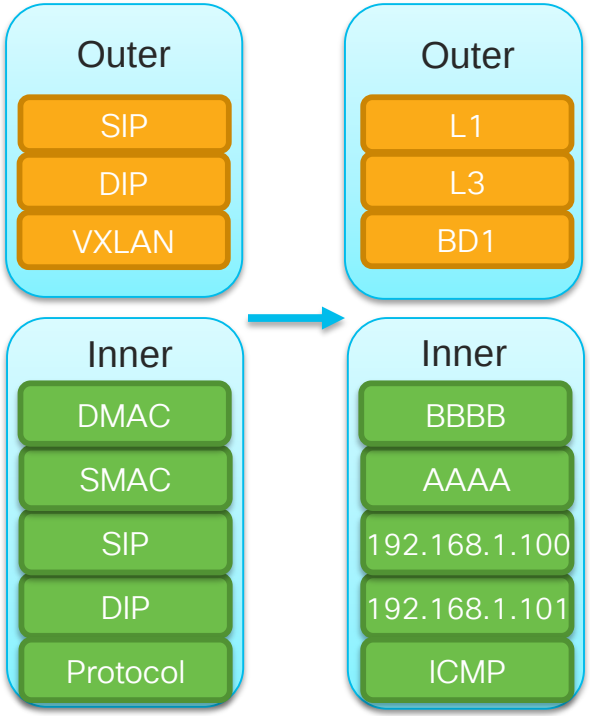
Anycast Gateway

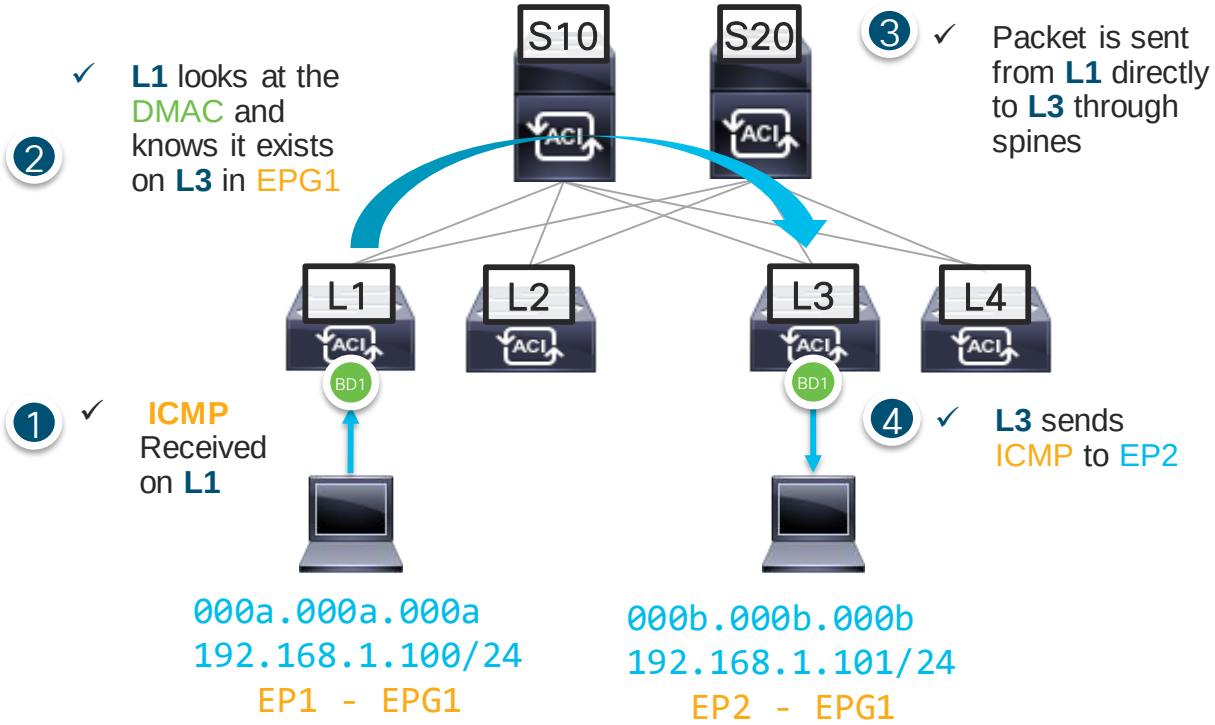
- Gateway IP is programmed on all leafs that need it
- Deterministic Traffic Flow to Gateway
- Consistent Latency across all Devices Towards Gateway



Known Unicast – Layer 2

EP1 pings EP2



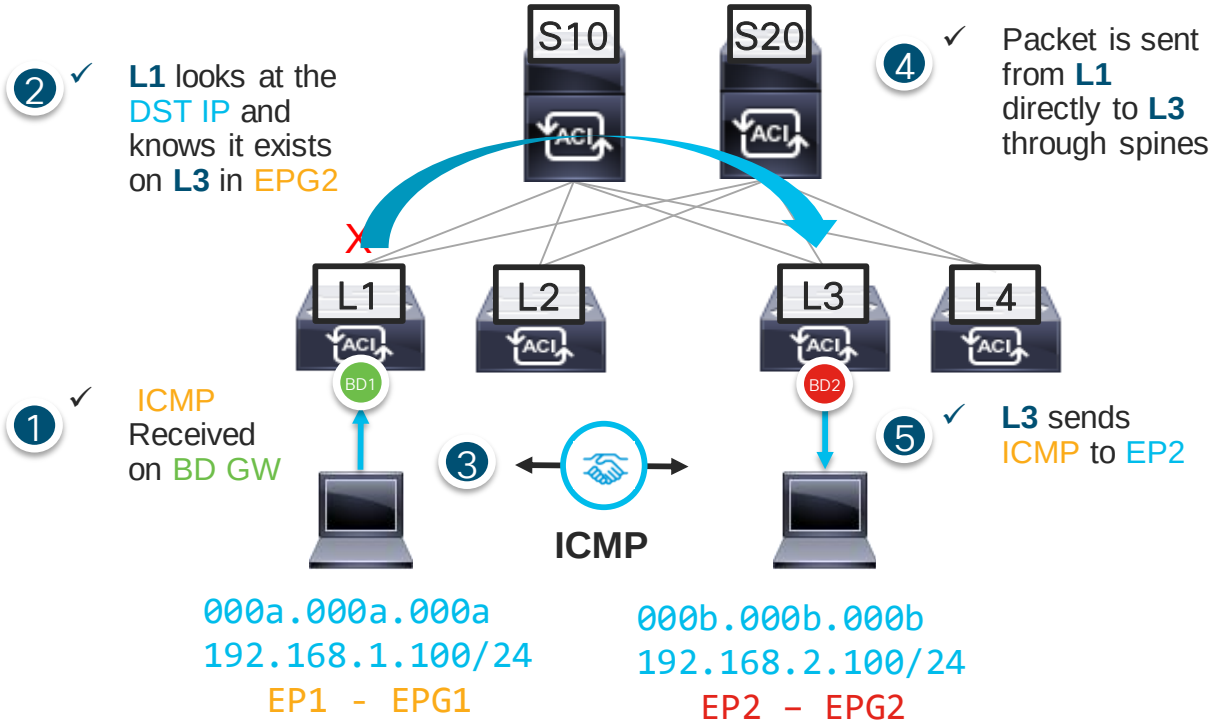


Known Unicast – Layer 3

EP1 pings EP2

Subnet under BD acts as GW

If traffic is destined to the GW MAC, we do an IP Lookup in the VRF



Agenda

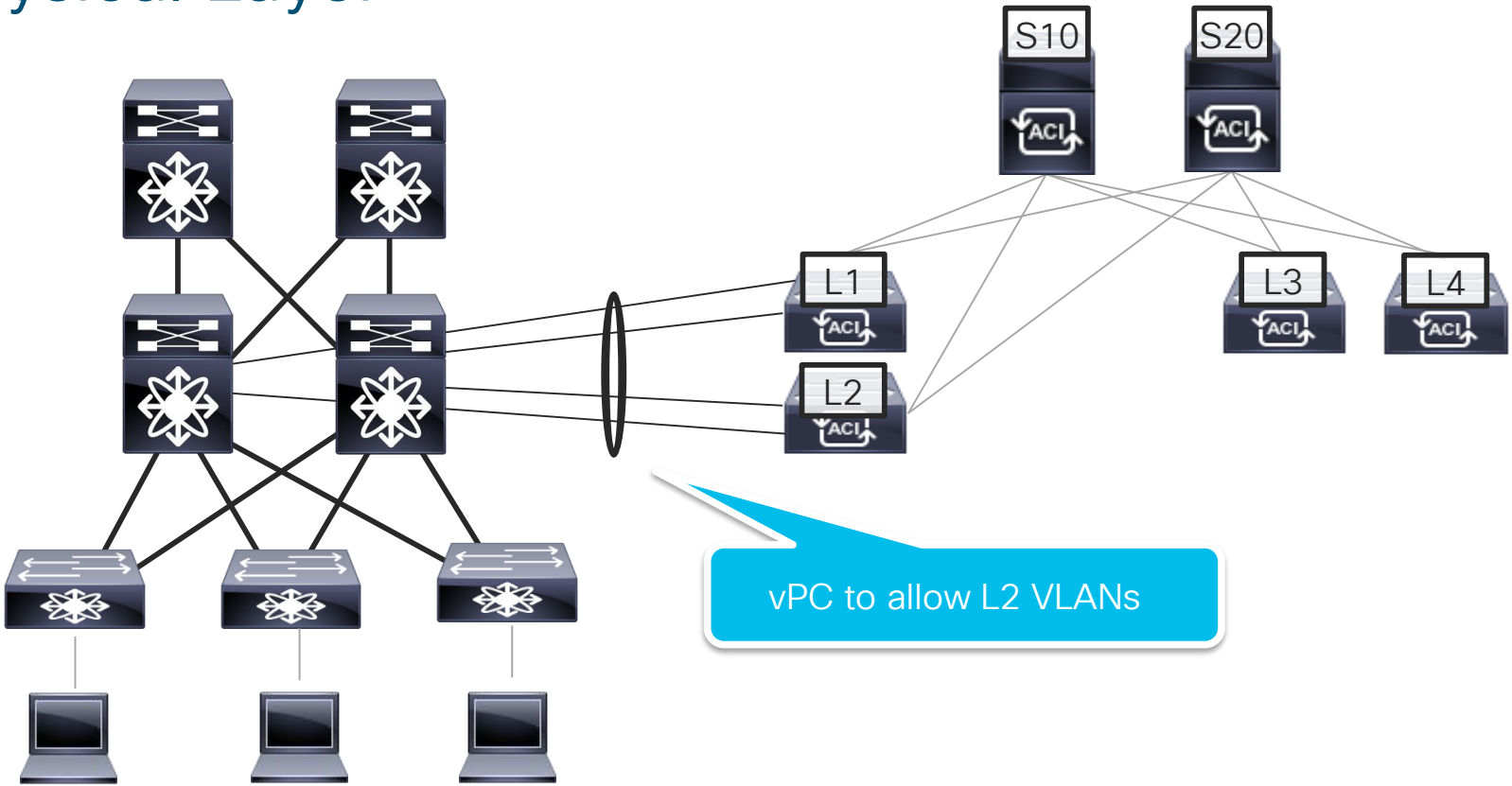
- Day 1: Why ACI?
- Day 2: Infrastructure and Policies
- Day 3: Forwarding Overview
- Day 4: Network Centric Migrations
- Day 5: Multi Location Deployments
- Day 6: Troubleshooting Tools
- Day 7: Additional Resources

Day 4:
Network Centric Migrations

You make networking **possible**

Cisco live!

Physical Layer



Checklist

- ✓ Physical Layer ☺
- ❑ Layer 2
- ❑ Layer 3

You make security **possible**

Network Centric Design

L2 Migration Recommendations

Each Legacy VLAN requires a unique Bridge Domain

Settings: Unicast Routing Disabled

Unknown L2 Flooding

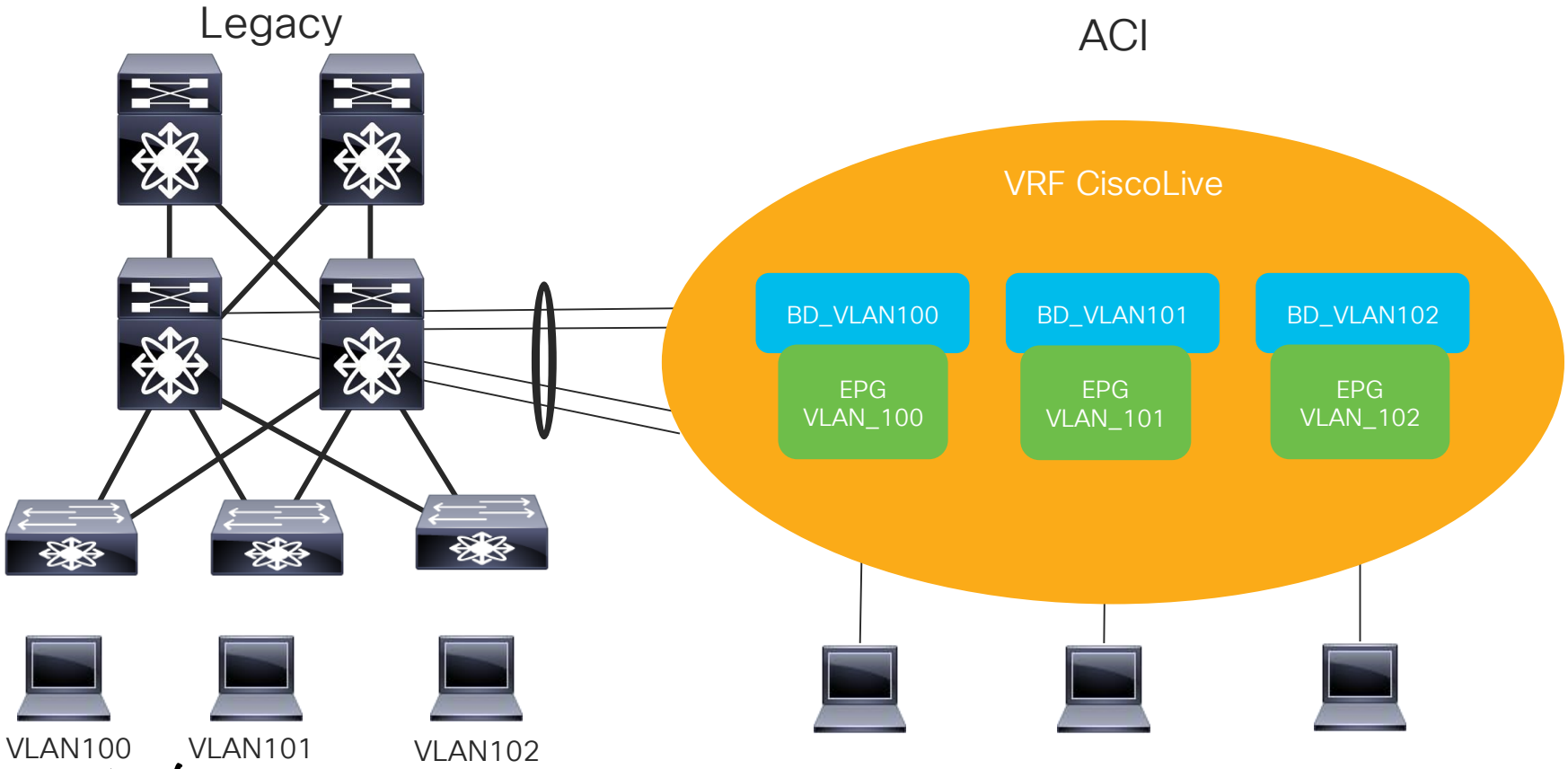
ARP Flooding

Each Legacy VLAN has a unique EPG

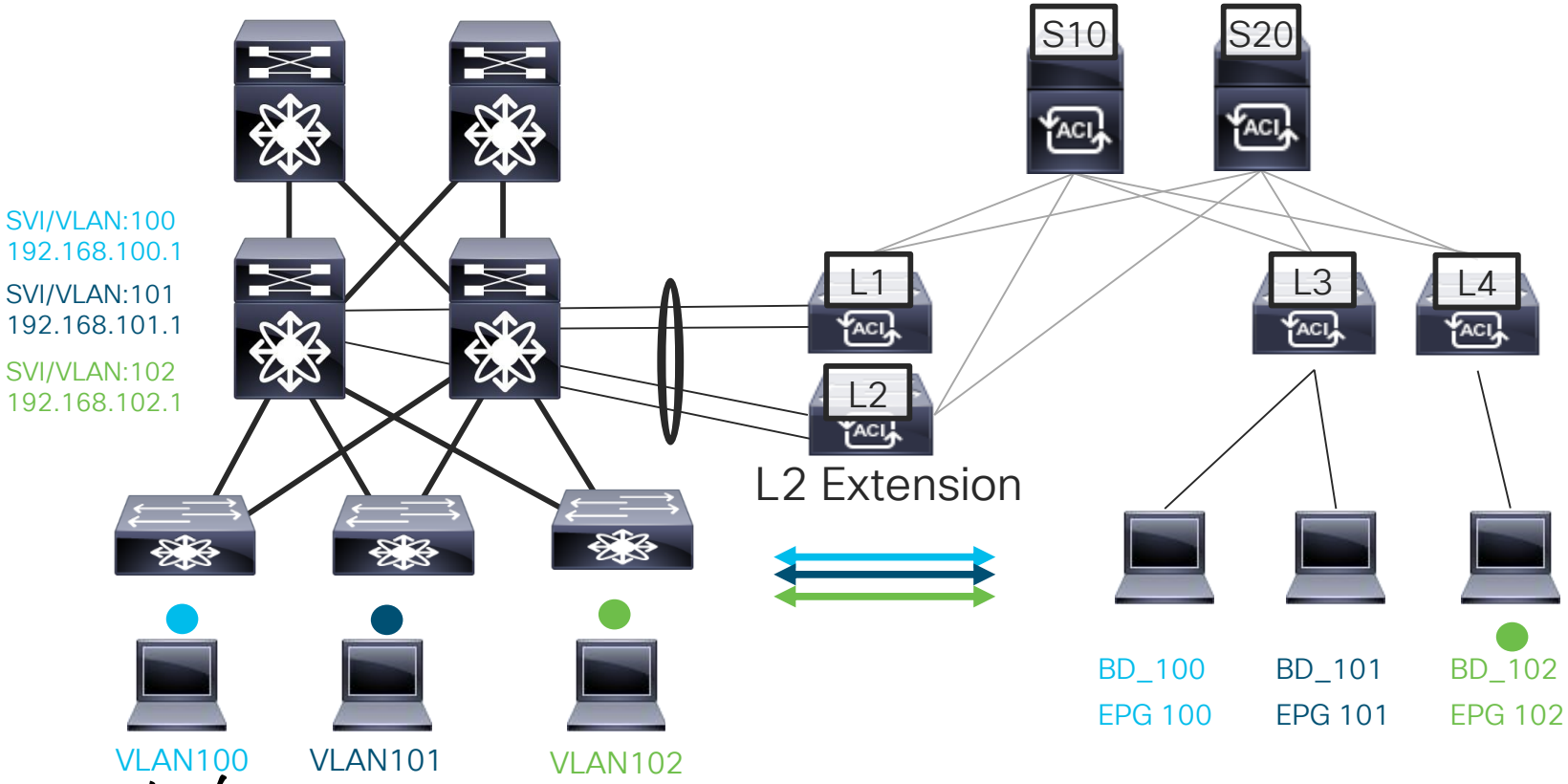
What have we Accomplished?

Each Legacy VLAN maps to a unique Bridge Domain

Conceptual View



Conceptual View



Spanning-tree in ACI

- ACI Fabric does not run Spanning-tree
  - BPDUs are flooded in ‘EPG VNID’ (use same VLAN pool for all ports deploying legacy VLANs)
  - ACI Fabric does snoop BPDUs and will flush Endpoints (Mac & IP) when TCNs are received
  - Learning is disabled when excessive BPDUs are received
- External Spanning-tree devices should be configured with “spanning-tree link-type shared”
- Use “show mcp internal info vlan *encap_vlan*” to see TCNs

```
Leaf101# show mcp internal info vlan 100
-----------------------------------------------
               PI VLAN: 13 Up
            Encap VLAN: 100
       PVRSTP TC Count: 11
         RSTP TC Count: 0
Last TC flush at Mon May  1 19:32:22 2017
 on Tunnel13
```

Verification

APIC GUI shows connected Endpoints (MAC and or IP) per EPG and Path

E.g.: 5C:83:8F:69:BB:C9 (N7K) connected via Nodes-101-102/N7710-vPC

MAC	Learning Source	Interface	Encap
5C:83:8F:69:BB:C9	learned	Pod-1/Node-101-102/N7710-vPC (learned)	vlan-100

- CiscoLive
  - Application Profiles
    - CiscoLive
      - Application EPGs (1000)
        - VLAN2000
      - uSeg EPGs
    - LegacyVlans
      - Application EPGs
        - Vlan100
          - Domains (VMs and Bare-Metals)
          - EPG Members
          - Static Ports
            - Pod-1/Node-101-102/N7710-vPC
            - Pod-1/Node-103-104/BareMetal01-vPC

Client End-Points | Configured Access Policies | Contracts | Controller End-Points | Learned End-Points

End Poi...	C	IP	Learning Source	Hosting Server	Reporting Controlle Name	Interface	Multicast Address	Encap
EP-5C:83:8F:69:BB:01	5C:83... BB:01	---	learned	---	---	Pod-1/Node-101-102/N7710-vPC (lear...	---	vlan-100
EP-5C:83:8F:69:BB:C9	5C:83:8F:69:BB:C9	---	learned	---	---	Pod-1/Node-101-102/N7710-vPC (lear...	---	vlan-100
EP-5C:83:8F:69:BB:C1	5C:83:8F:69:BB:C1	---	learned	---	---	Pod-1/Node-103-104/BareMetal01-vPC...	---	vlan-100

Checklist

- ✓ Physical Layer ☺
- ✓ Layer 2
- ❑ Layer 3

You make security **possible**

Network Centric Design

L3 Migration Requirements

Configure "Layer 3 Out" to create a routed connection to legacy network

- Routed Interface
- Routed subinterface
- Switched Virtual Interface (SVI)

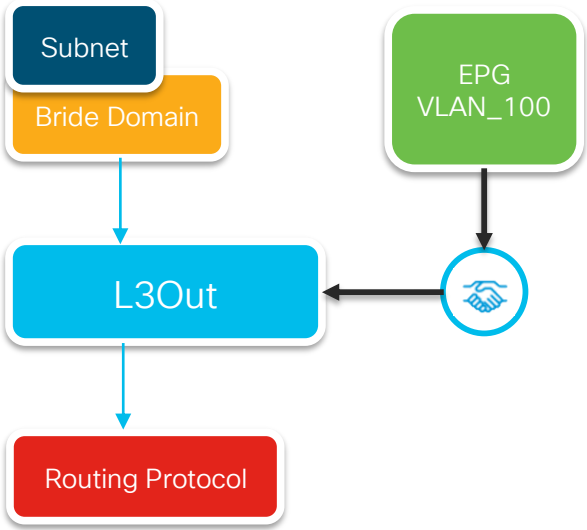
Bridge Domain with "Unicast Routing" enabled

- Subnet defined on BD
- L3Out associated with BD

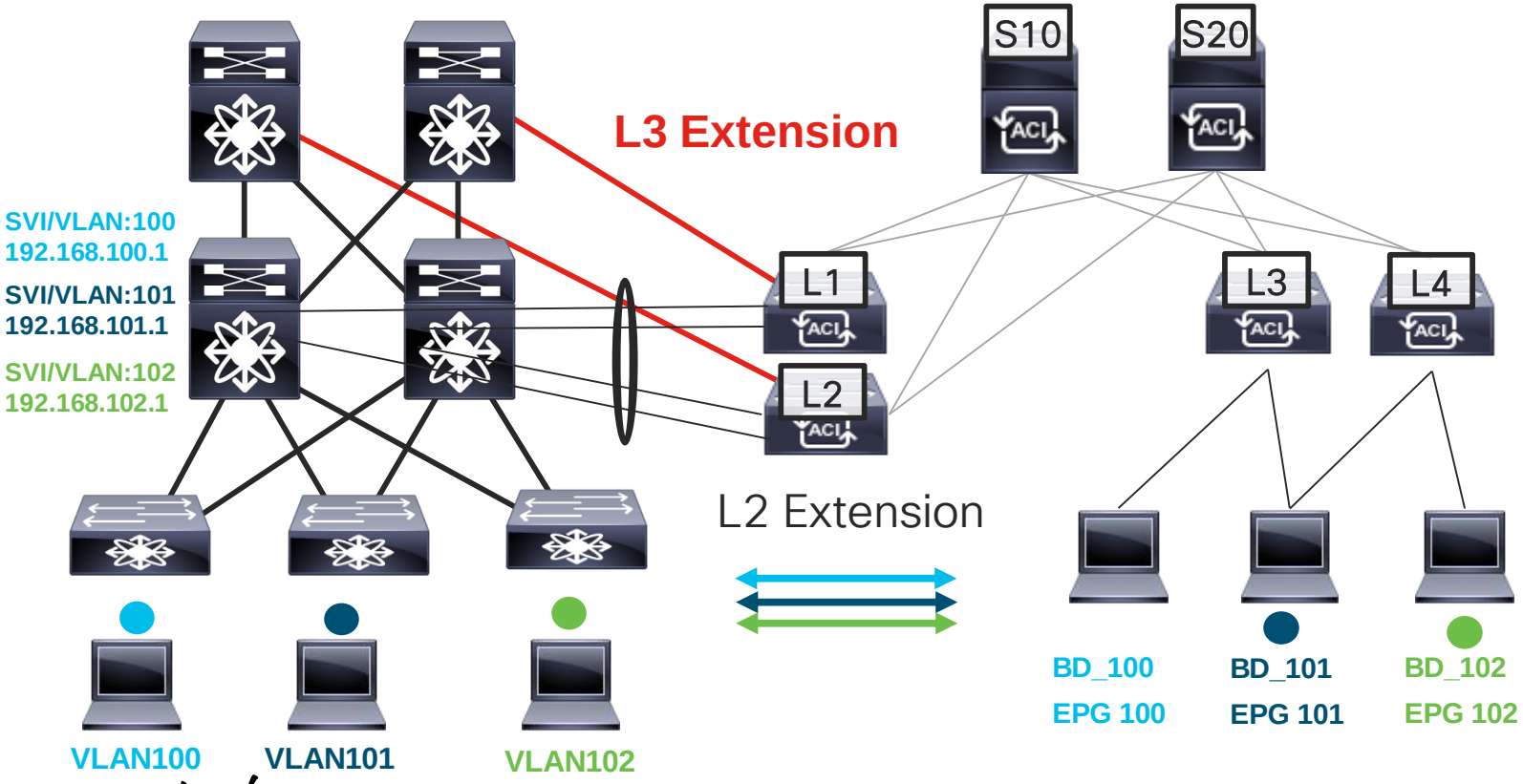
EPG has contract to L3Out Network

Dynamic Routing

- OSPF/ EIGRP/ BGP/ Static

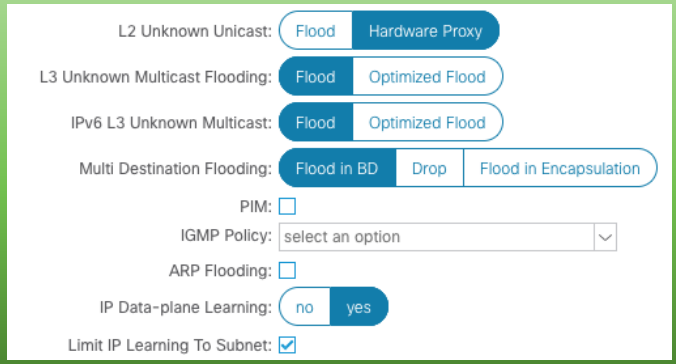


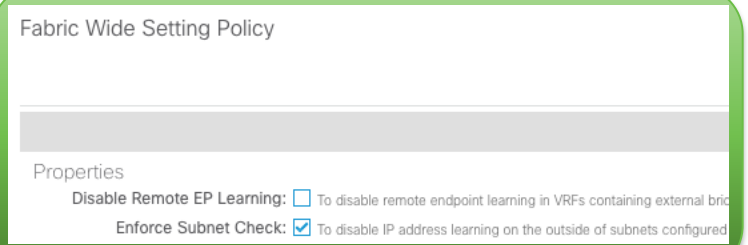
Conceptual View



L3 Migration Considerations

1) Disable External GW!
2) Bridge Domain Settings
   - Unicast routing Enabled – Minor Service Impact
   - L2 Unknown Unicast H/W Proxy – Service Impact
   - ARP Flooding Optimized - In conjunction with L2 Unknown Unicast
   - Limit IP learning to Subnet
     - Off Subnet Learns are cleared
     - Learning is disabled for 2 minutes
3) Global Settings
   - Enforce Subnet Check - adds prefix check to all BD's

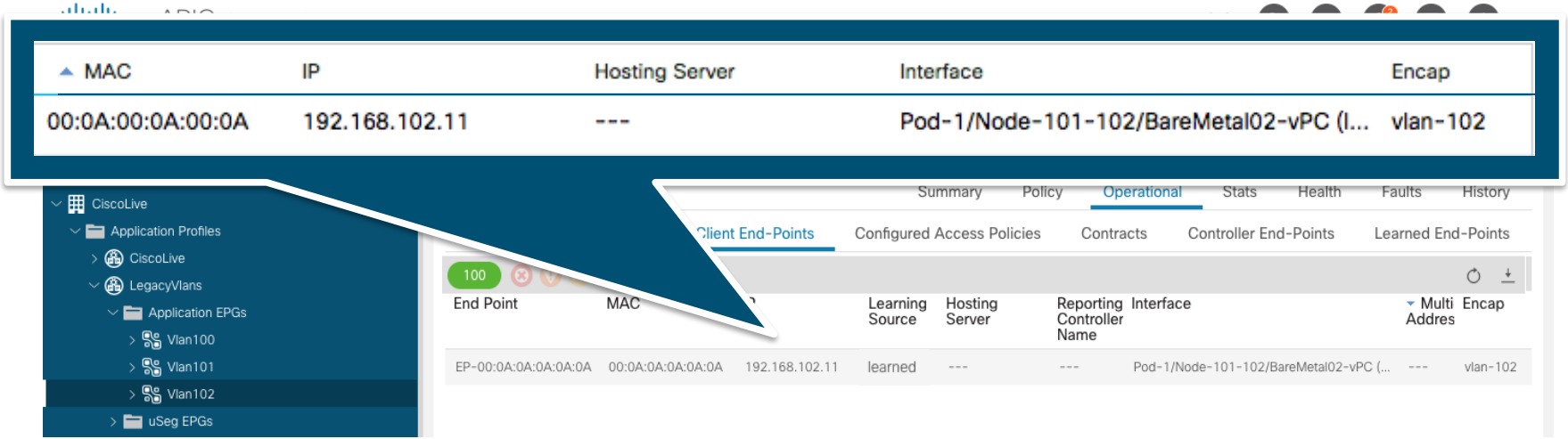




Verification

APIC GUI now shows IP information since UC Routing is enabled on BD

E.g.: 192.168.102.11 connected via Nodes-101-102/BareMetal02-vPC

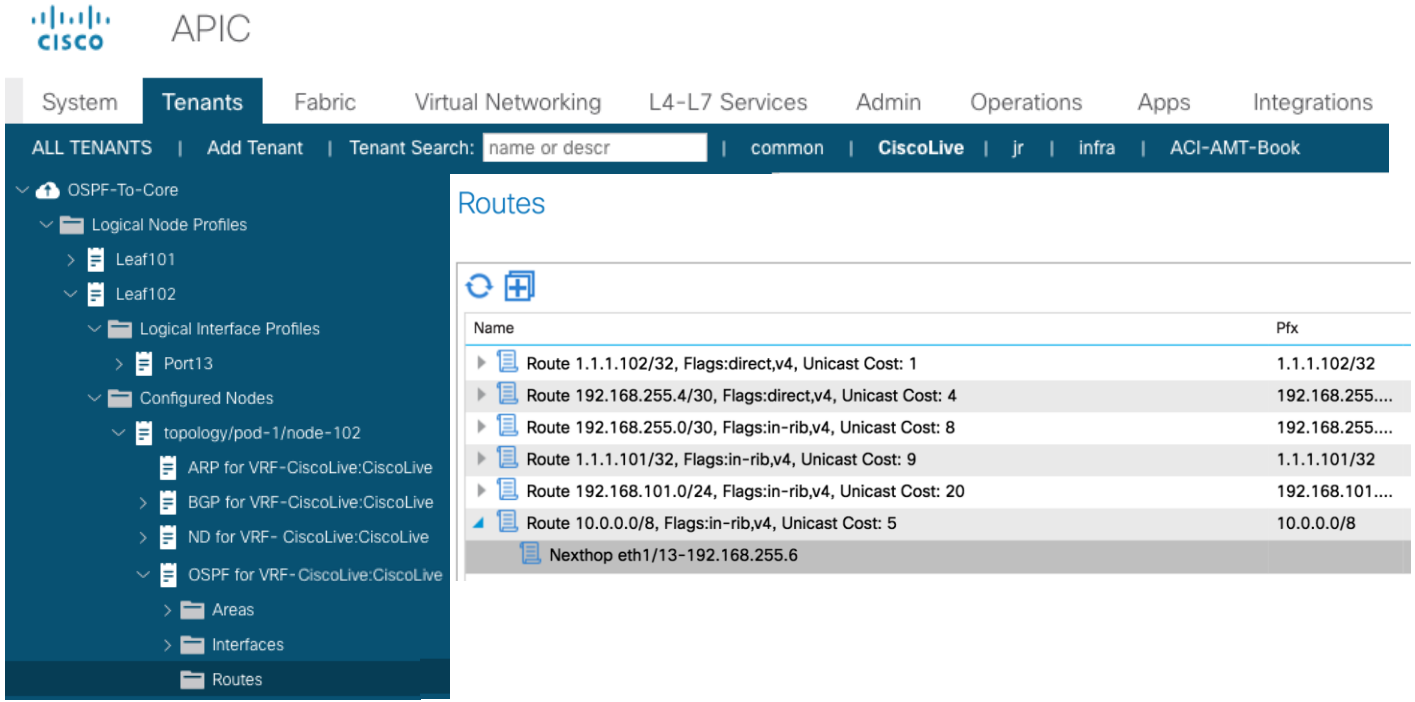


Recommended Content! – ACI Endpoint Learning White Paper

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739989.html

Verification

GUI



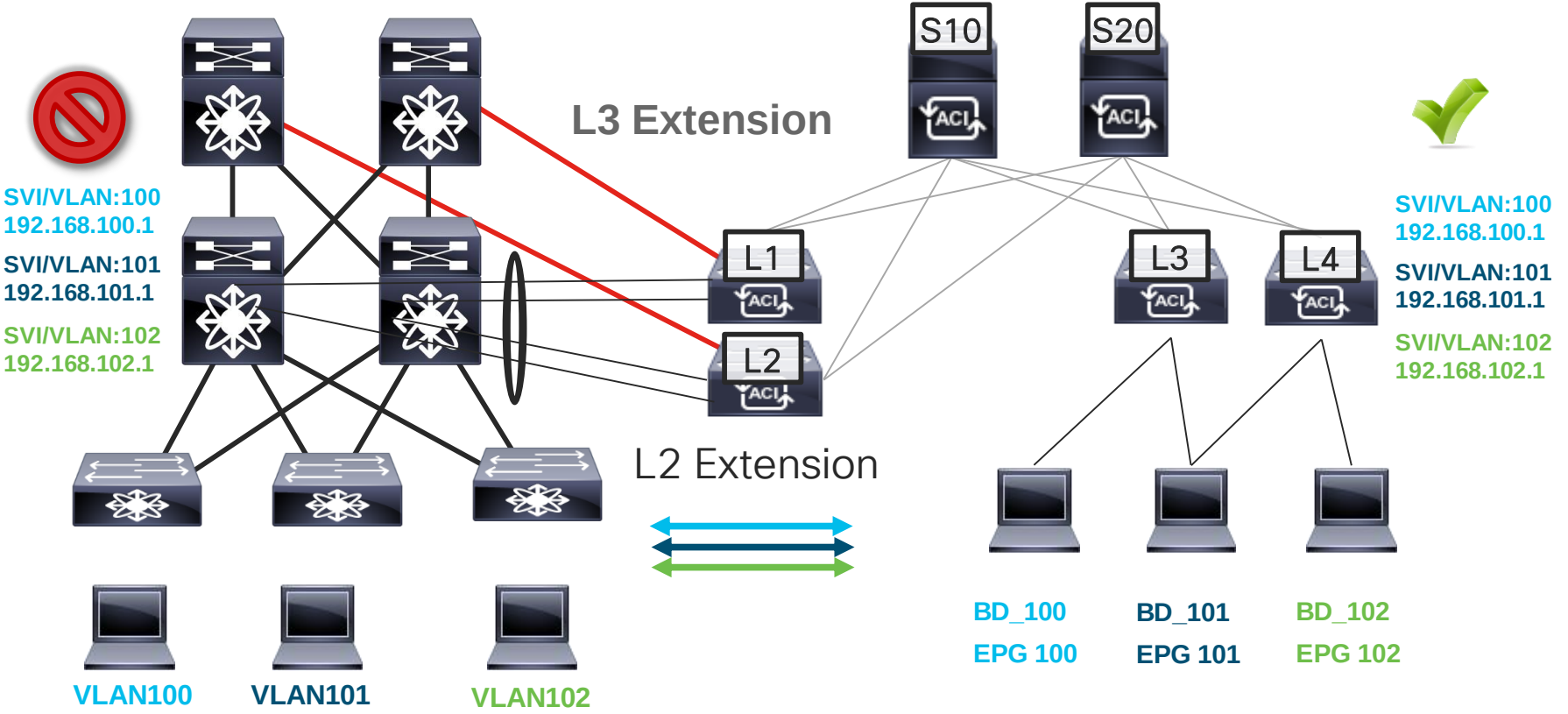
Verification

SSH

```
Leaf101# show ip ospf neighbors vrf CiscoLive:CiscoLive
 OSPF Process ID default VRF CiscoLive:VRF1
 Total number of neighbors: 1
 Neighbor ID     Pri State            Up Time  Address         Interface
 192.168.255.255   1 FULL/BDR         02:27:05 192.168.255.2   Eth1/13


Leaf101# show ip route 10.0.0.0/8 vrf CiscoLive:CiscoLive
IP Route Table for VRF "CiscoLive:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>


10.0.0.0/8, ubest/mbest: 1/0
    *via 192.168.255.2, eth1/13, [110/5], 01:45:34, ospf-default
```

Common Pitfalls

Old Gateway still Active!



Common Pitfalls

Windows Dynamic Load Balancing

Problem:

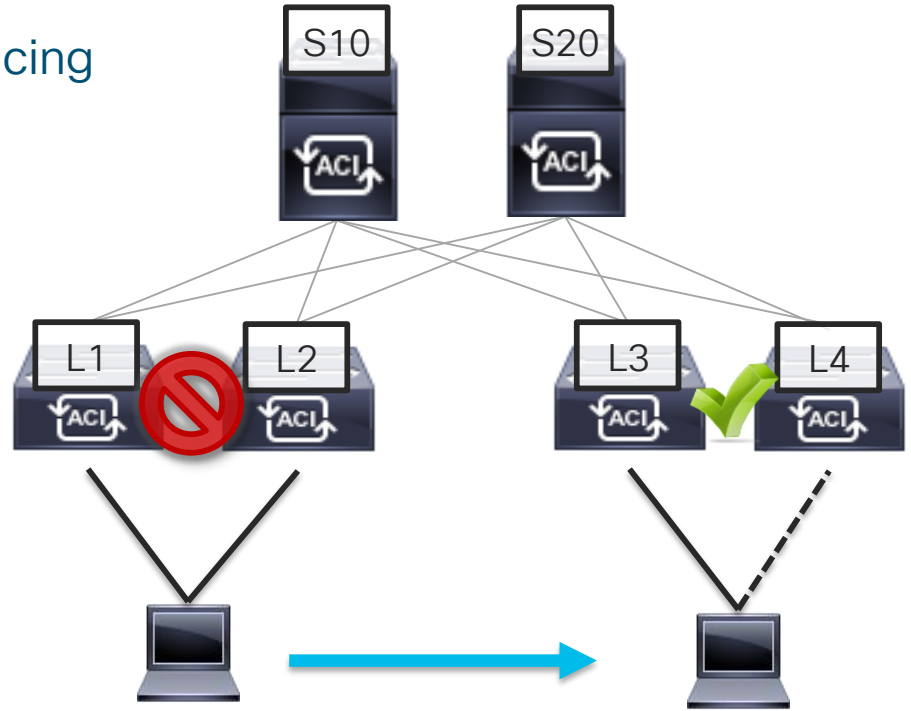
Traffic is Sourced with the same IP but from both NIC's using different MACs

ACI Fabric sees frequent IP Move between MAC's when Routing is Enabled!

Solution:

1) Use "Hyper-V Port" to force single MAC to IP Communication

2) Disable IP Learning on the VRF



Checklist

- ✓ Physical Layer ☺
- ✓ Layer 2
- ✓ Layer 3

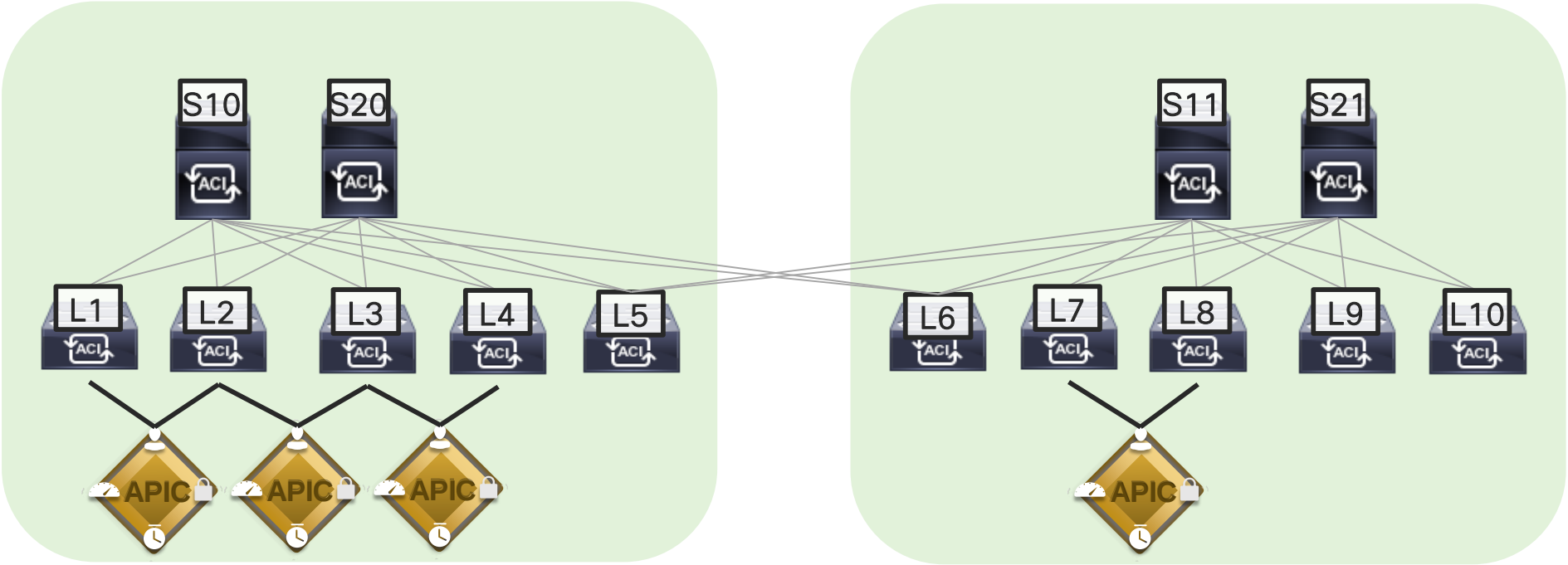
You make security **possible**

Day 5: Multi-Location Deployment Options

You make networking **possible**

Cisco live!

Stretched Fabric



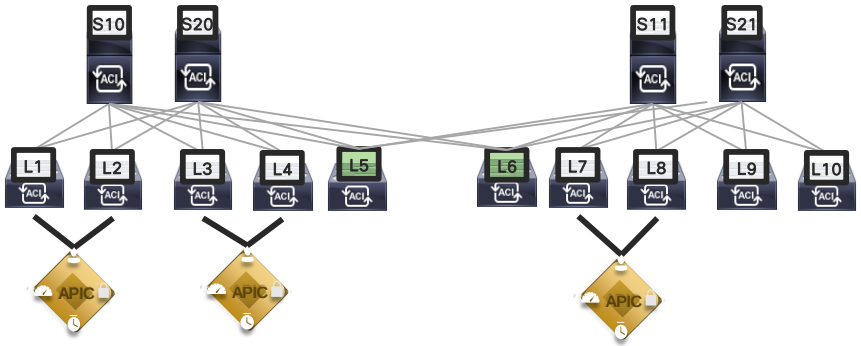
Stretched Fabric

Advantages

- All one Fabric
- No Additional Routed Infrastructure
- Simple Provisioning – If cabling is in place

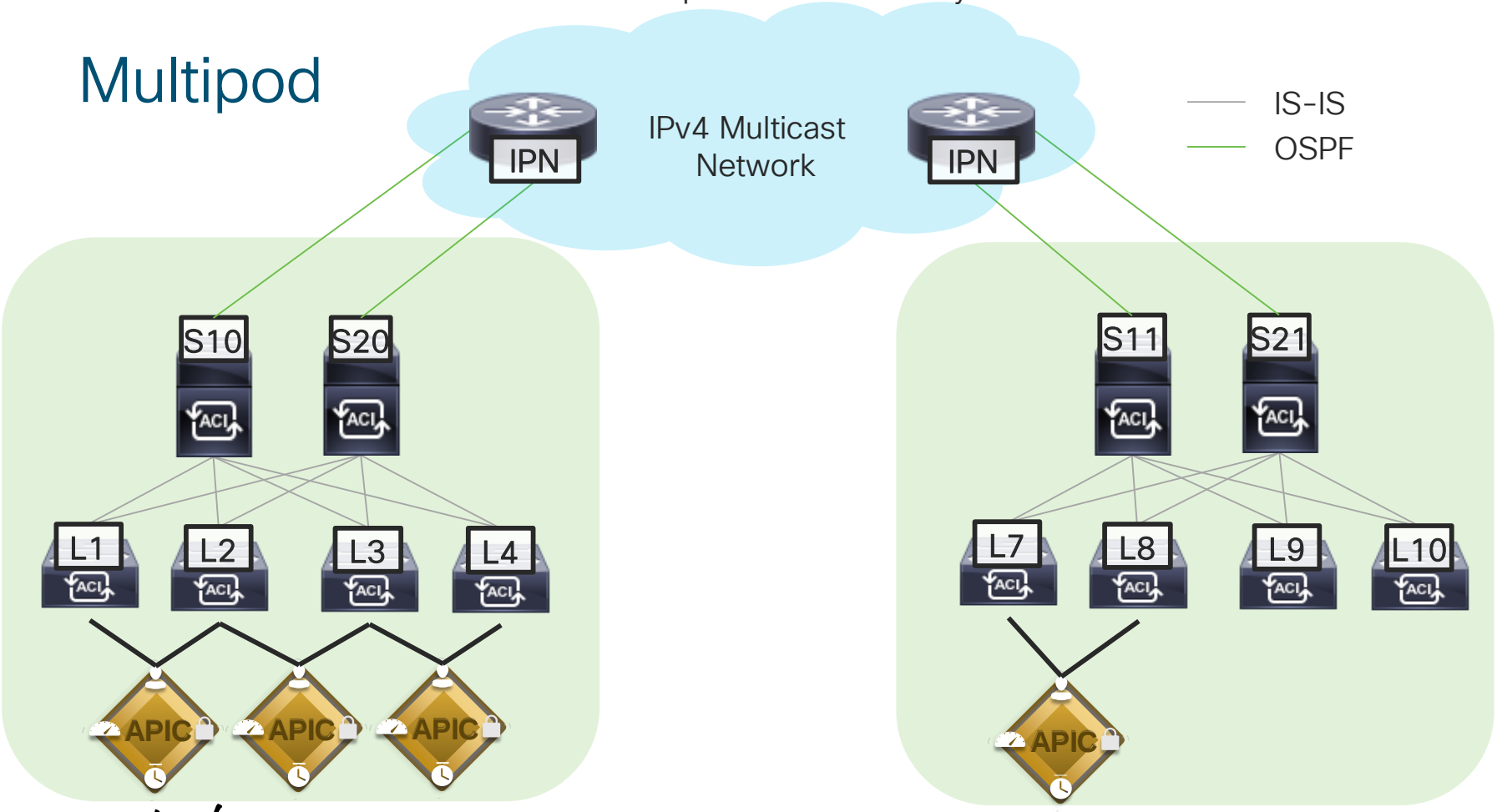
Limitations

- Single APIC Failure Domain
- L1 Connectivity between Transit Leafs and spines (dark fiber)
- Same Control Plane Instance Across Sites



IPN MTU Requirements: 9150 Bytes

Multipod



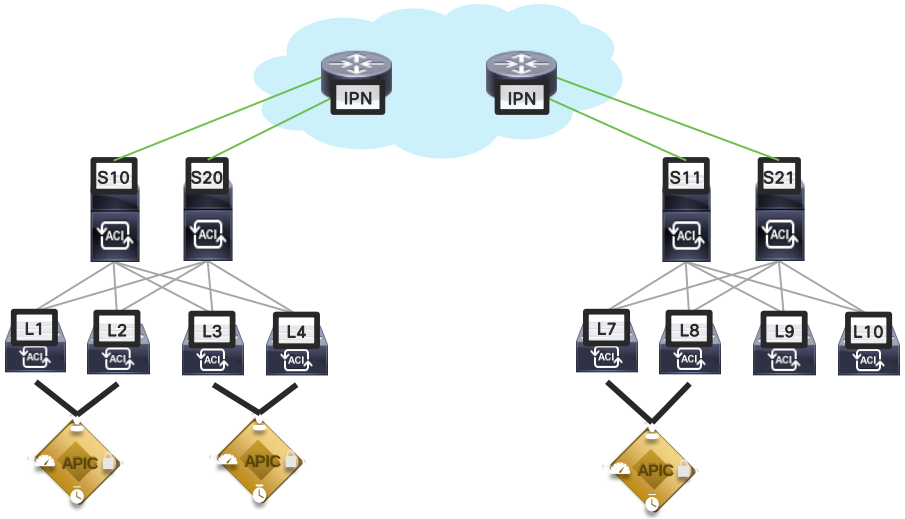
Multipod

Advantages

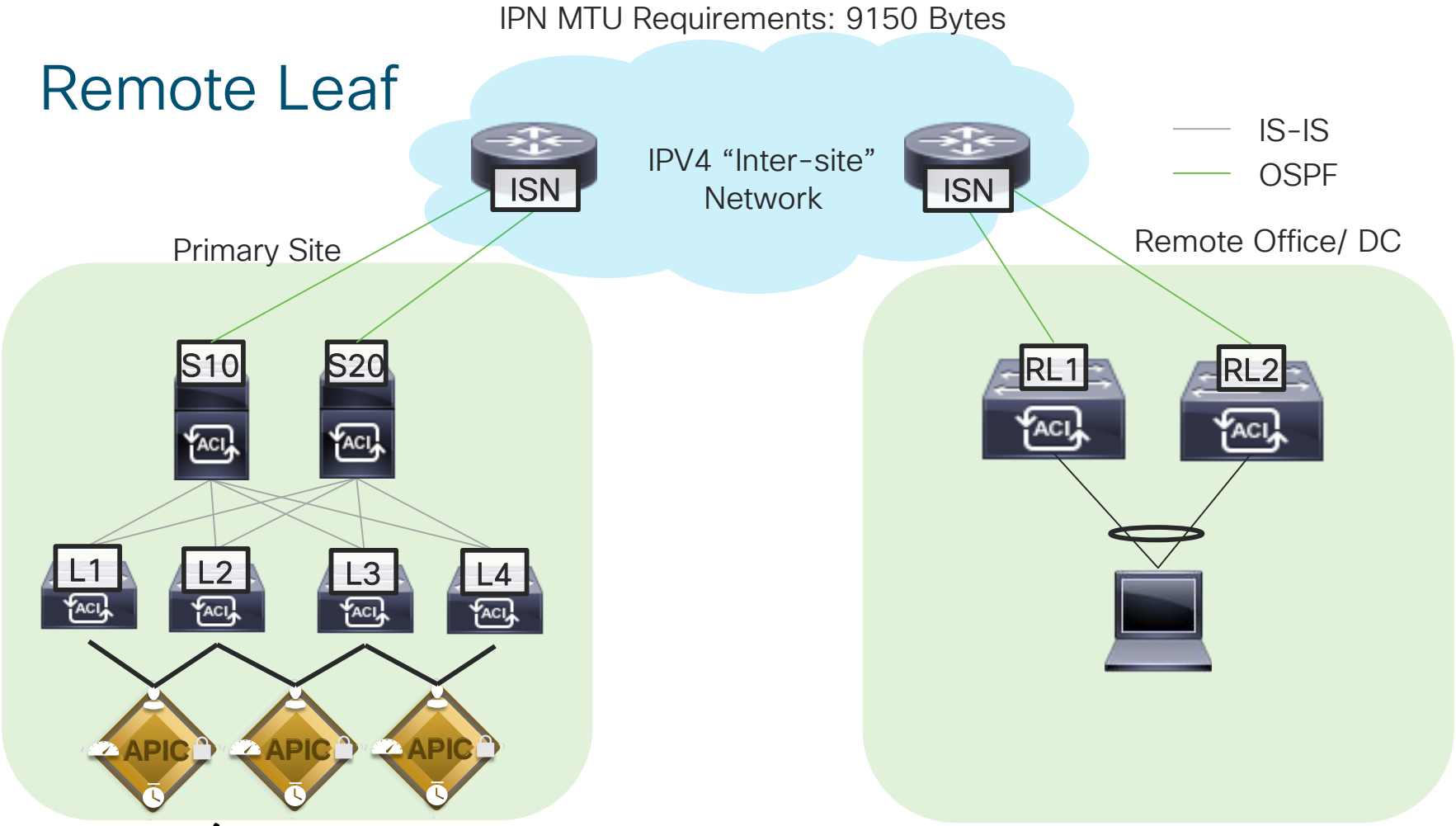
- All one Fabric
- Policy Stretched across sites
- Separate Control Plane Instances per site
- Increases Leaf Scale to 400

Limitations

- Single APIC Failure Domain
- Need dedicated Routing Devices as Inter-Pod Network (IPN) Routers.
- Requires PIM BI-Dir to route BUM traffic between sites.
- 50ms max latency between pods



Remote Leaf



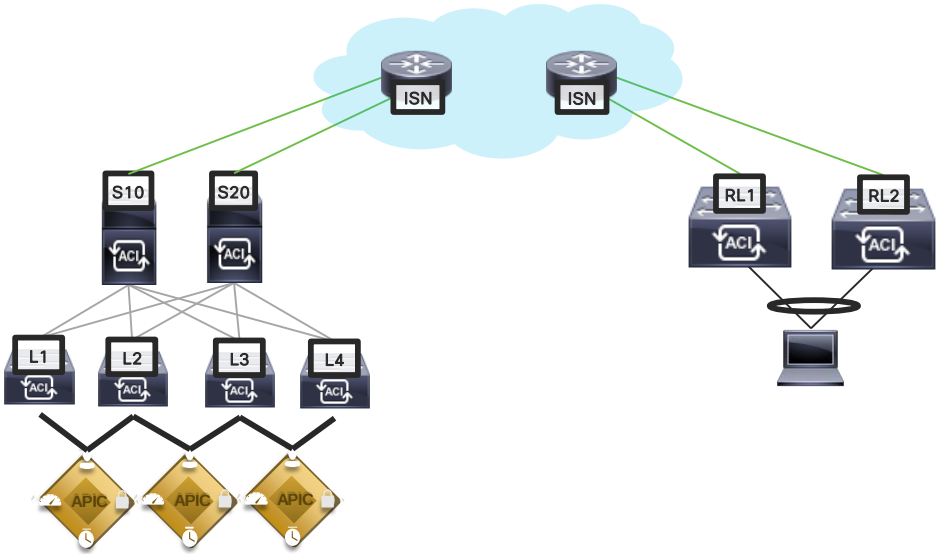
Remote Leaf

Advantages

- All one Fabric
- Easy Addition of small site to existing APIC
- Spines not required in Remote Site.
- Connects to existing routing infrastructure
    - No Multicast required

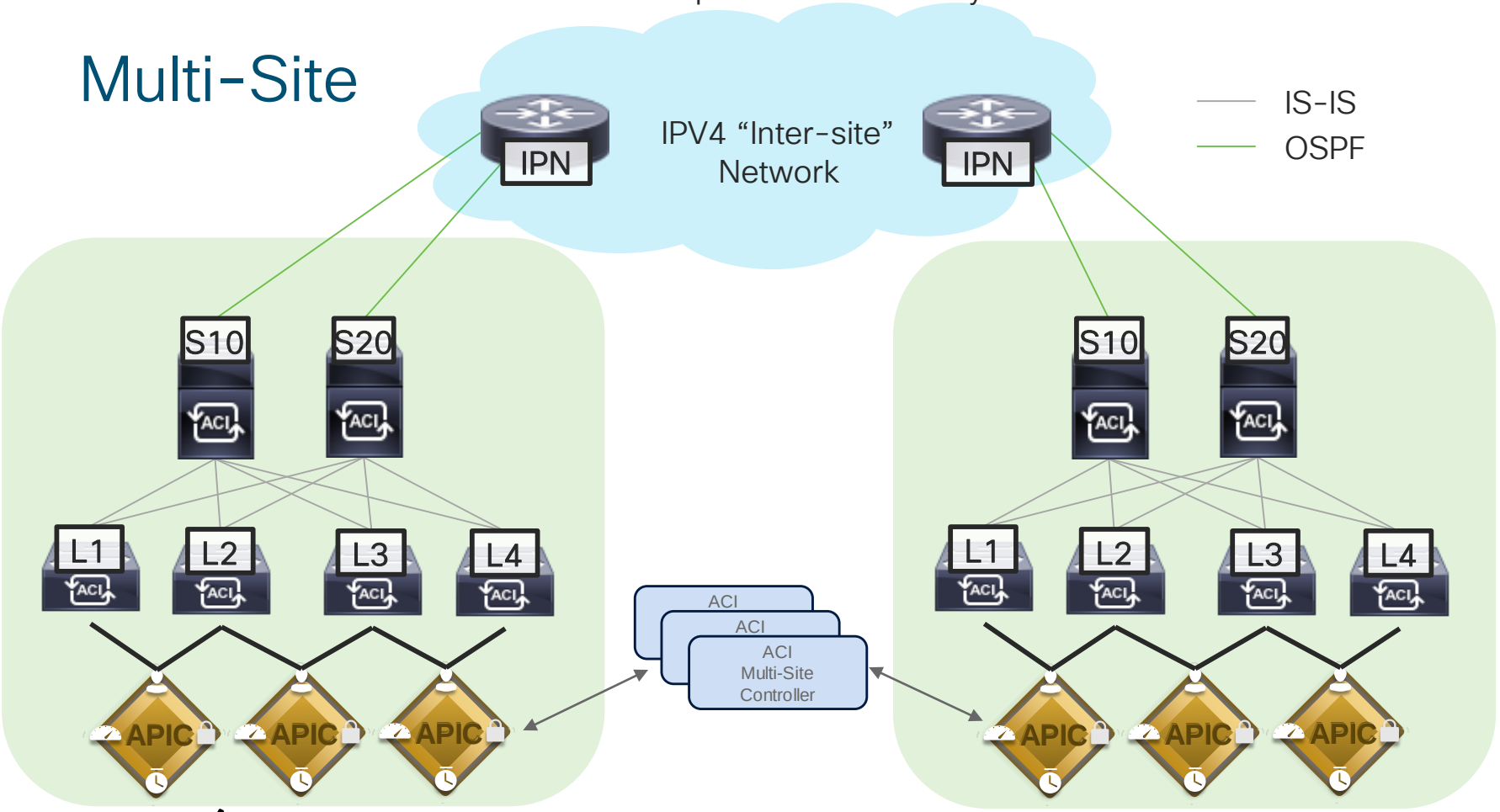
Limitations

- All traffic goes to “main” site before other sites.
- 140ms Latency Restriction
- Port Count



IPN MTU Requirements: 9150 Bytes

Multi-Site



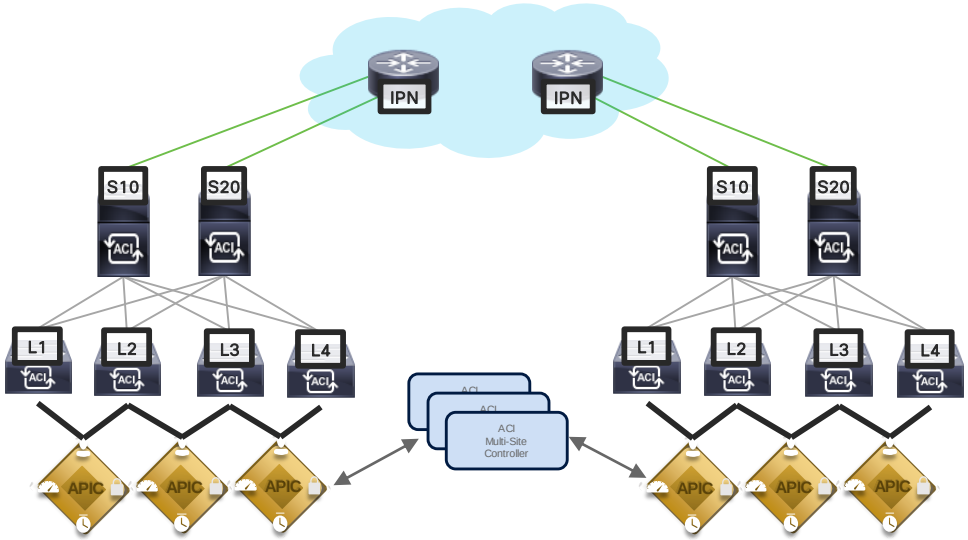
Multi-Site

Advantages

- Two Independent Fabrics (APIC Clusters)
- Policy is synchronized using Multi-Site Controller
- Connects to existing routing infrastructure
  - No Multicast required

Limitations

- 500ms – 1s latency for OOB MSC → APIC connectivity
- Not all Site Specific Config can be done from MSC



Day 6: Troubleshooting Tools

You make networking **possible**

Faults

Fault Properties

General | Troubleshooting | History

Explanation: The object refers to an object that was not found.
Recommended Action: Make sure that referenced object exists and the name is spelled correctly in the relation object.

Audit Logs | Events

Audit log 1 minutes before the fault

Time Stamp	ID	User	Action	Affected Object	Description
2019-05-09T13:13:51.337-04:00	4295108047	carschmi	deletion	uni/tn-CiscoLive/BD-VLAN_100/rsmldsn	RsMldsn deleted
2019-05-09T13:13:51.337-04:00	4295108048	carschmi	deletion	uni/tn-CiscoLive/BD-VLAN_100/rsigmpsn	RsIgmpsn deleted
2019-05-09T13:13:51.337-04:00	4295108049	carschmi	deletion	uni/tn-CiscoLive/BD-VLAN_100/rsctx	RsCtx deleted
2019-05-09T13:13:51.336-04:00	4295108050	carschmi	deletion	uni/tn-CiscoLive/BD-VLAN_100/rsbdToEpRet	RsBdToEpRet deleted
2019-05-09T13:13:51.336-04:00	4295108051	carschmi	deletion	uni/tn-CiscoLive/BD-VLAN_100/rsBDToNdP	RsBDToNdP deleted
2019-05-09T13:13:51.336-04:00	4295108052	carschmi	deletion	uni/tn-CiscoLive/BD-VLAN_100	BD VLAN_100 deleted
2019-05-09T13:13:44.179-04:00	4295108046	carschmi	modification	uni/tn-CiscoLive/ap-LegacyVlans/epg-VLAN_100/rsbd	RsBd modified

EPG - VLAN_100

Summary | Policy | Operational | Stats | Health | Faults | History

Faults | Fault Counts Stats

100

Severity	Acked	Cause	Creation Time	Affected Object	Description	Code	Last Transition	Lifecycle
		configuration-failed	2019-05-09T13:13:5...	uni/tn-CiscoLive/ap-LegacyVlans/epg-VLAN_100	Configuration failed for EPG VLAN_100 due to BD Not present	F05...	2019-05-09T13:13:5...	Soaking
		resolution-failed	2019-05-09T13:13:5...	uni/tn-CiscoLive/ap-LegacyVlans/epg-VLAN_100/rsbd	Failed to form relation to MO BD-VLAN_100 of class fvBD in context	F09...	2019-05-09T13:13:5...	Raised

EP Tracker

"We had a problem at 14:21!!!"

Attach/Detach events are logged for each EP

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations | Apps

192.168.102.11

Learned At	Tenant	Application	EPG
101-102, vPC: BareMetal02-vPC	CiscoLive	LegacyVlans	VLAN_102

192.168.102.11 SEARCH

Learned At	Tenant	Application	EPG	IP
101-102, vPC: BareMetal02-vPC	CiscoLive	LegacyVlans	VLAN_102	192.168.102.11

State Transitions

Date	IP	MAC	EPG	Action	Node	Interface	Encap
2017/05/03 14:27:39	192.168.102.11	00:0A:00:0A:00:0A	CiscoLive/LegacyVlans/...	detached	Pod-1/Node-103-104	BareMetal01-vPC	vlan-102
2017/05/03 14:22:59	192.168.102.11	00:0A:00:0A:00:0A	CiscoLive/LegacyVlans/...	attached	Pod-1/Node-103-104	BareMetal01-vPC	vlan-102
2017/05/03 14:22:11	192.168.102.11	00:0A:00:0A:00:0A	CiscoLive/LegacyVlans/...	detached	Pod-1/Node-103-104	BareMetal01-vPC	vlan-102
2017/05/03 14:21:51	192.168.102.11	00:0A:00:0A:00:0A	CiscoLive/LegacyVlans/...	attached	Pod-1/Node-103-104	BareMetal01-vPC	vlan-102
2017/05/03 14:21:31	192.168.102.11	00:0A:00:0A:00:0A	CiscoLive/LegacyVlans/...	detached	Pod-1/Node-103-104	BareMetal01-vPC	vlan-102
2017/05/03 14:21:22	192.168.102.11	00:0A:00:0A:00:0A	CiscoLive/...	attached	Pod-1/Node-101-102	BareMetal02-vPC	vlan-102
2017/05/03 14:21:11	192.168.102.11	00:0A:00:0A:00:0A	Cis...	attached	Pod-1/Node-103-104	BareMetal01-vPC	vlan-102

Page 1 Of 1 | Objects Per Page: 15 | Displaying Objects 1 - 7 Of 7

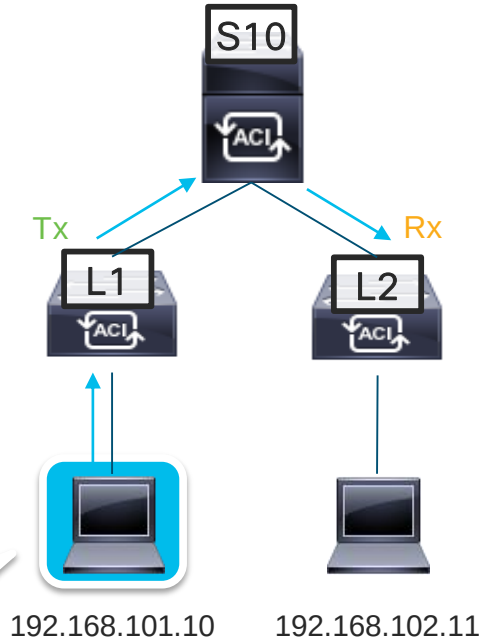
detached	Pod-1/Node-103-104	BareMetal01-vPC
attached	Pod-1/Node-101-102	BareMetal02-vPC
attached	Pod-1/Node-103-104	BareMetal01-vPC

IP Was Moving???

Atomic Counters

- Used to measure packet loss in Overlay
- Logs packet count between EP's on different Leafs
- Specific Filter can be set
- Requires NTP!

Leaf	Direction	Filter	Packet Count
L1	Tx	ICMP	500
L2	Rx	ICMP	500



Ping -c 500 192.168.102.11

Atomic Counters

EP-to-EP CiscoLive-ACP

Policy | Operational | Faults | History

Properties

Name: **CiscoLive-ACP**

Description: optional

Administrative State: Disabled | **Enabled**

Source IP:

IP	State
CiscoLive/LegacyVlans/5C:83:8F:B0:76:C1/192.168.101.10	formed

Destination IP:

IP	State
CiscoLive/LegacyVlans/00:0A:00:0A:00:0A/192.168.102.11	formed

Filters:

Name	Protocol	Source Port	Destination Port	Description
SSH	tcp	Unspecified	22	Source Any, Dest 22

Atomic Counters

EP-to-EP CiscoLive-ACP

Policy | **Operational** | Faults | History

Traffic

Source	Destination	Last Collection (30 Seconds)			Tot			
		Transmit Pkt	Admitted Pkt	Dropped Pkt	Transmit Pkt	Admitted Pkt	Dropped Pkt	Excess Pkt
uni/tn-CiscoLive/ap-Legacy...	uni/tn-CiscoLive/ap-LegacyVlans/epg-...	3926	3926	0	81658	81658	0	0

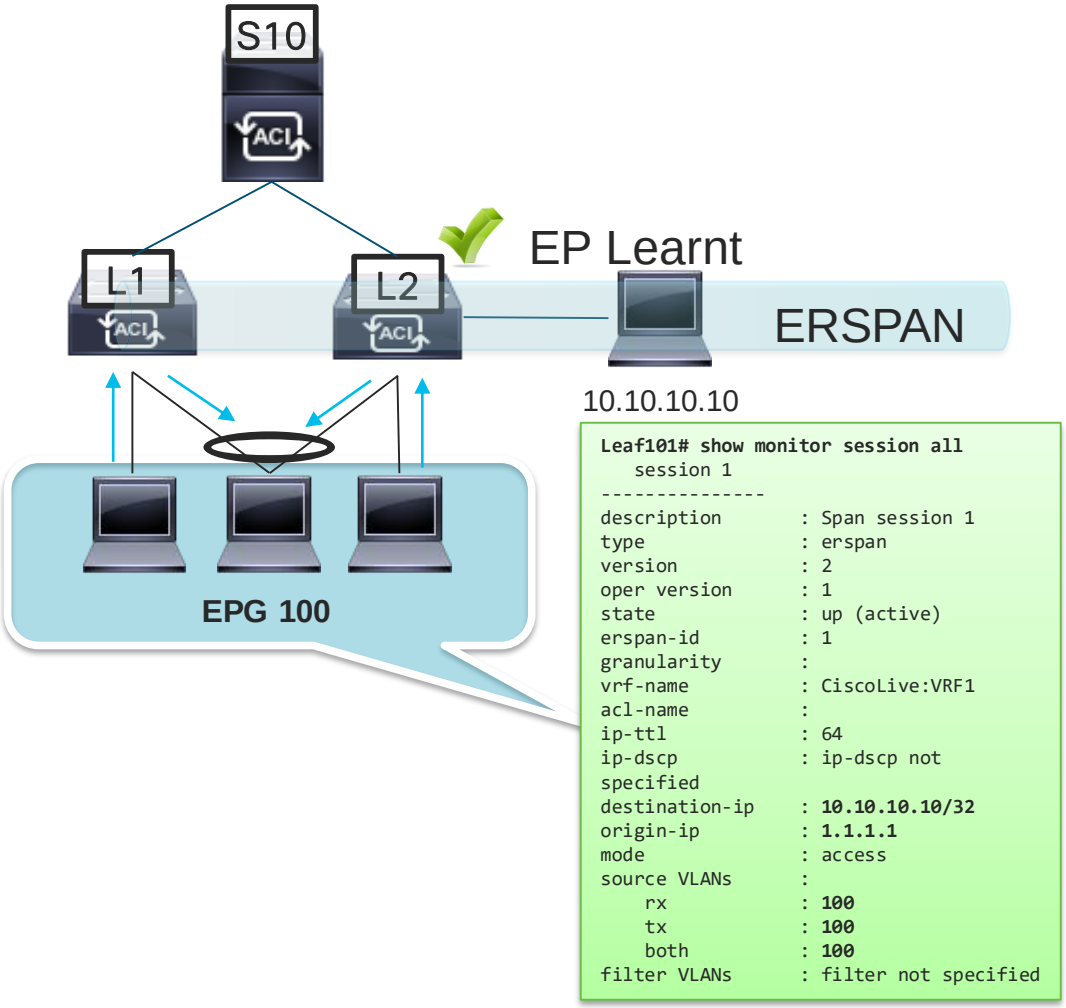
Dropped Pkt	Transmit Pkt	Admitted Pkt
0	81658	81658

NO Packet Loss In Overlay

SPAN

- ACI allows for SPAN of Entire EPG
- ERSPAN Destination must be an IP EP Learnt in ACI
- EP Can run Wireshark or Tshark

SPAN Source	SPAN Destination
EPG	ERSPAN
Port	ERPSAN/Local Port



Troubleshooting Wizard - Faults

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations | Apps

Advanced Mode
welcome, admin

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker | Visualization

CiscoLive-TSW

- Faults
- Drop/Stats
- Contracts
- Events and Audits
- Traceroute
- Atomic Counter
- SPAN

Critical | Major | Minor | Warning

Shows Faults in the Path

Spine Spine201 (pod-1/node-201)
Spine Spine202 (pod-1/node-202)

Leaf Leaf103 (pod-1/node-103)
eth1/15 vPC: BareMetal01-vPC

Leaf Leaf104 (pod-1/node-104)
eth1/15 vPC: BareMetal01-vPC

Leaf Leaf101 (pod-1/node-101)
eth1/14 vPC: BareMetal02-vPC

Leaf Leaf102 (pod-1/node-102)
eth1/14 vPC: BareMetal02-vPC

Source Endpoint
IP: 192.168.101.10
MAC: 5C:83:8F:B0:76:C1

Destination Endpoint
IP: 192.168.102.11
MAC: 00:0A:00:0A:00:0A

Time Window

From	latest 240 minutes
To	now

Session Information

Source	192.168.101.10
Desination	192.168.102.11
Session Type	Endpoint → Endpoint

Current System Time:2017-05-04T18:02 UTC+00:00

Troubleshooting Wizard – Drop Stats

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations | Apps

Advanced Mode
welcome, admin

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker | Visualization

CiscoLive-TSW

- Faults
- Drop/Stats
- Contracts
- Events and Audits
- Traceroute
- Atomic Counter
- SPAN

No stats available | No drop | Packets dropped

Spine Spine201 (pod-1/node-201)
Spine Spine202 (pod-1/node-202)

Leaf Leaf103 (pod-1/node-103)
eth1/15
vPC: BareMetal-vPC

Leaf Leaf104 (pod-1/node-104)
eth1/15
vPC: BareMetal01-vPC

Leaf Leaf101 (pod-1/node-101)
eth1/14
vPC: BareMetal02-vPC

Leaf Leaf102 (pod-1/node-102)
eth1/14
vPC: BareMetal02-vPC

Source Endpoint
IP: 192.168.101.10
MAC: 5C:83:8F:B0:76:C1

Destination Endpoint
IP: 192.168.102.11
MAC: 00:0A:00:0A:00:0A

Time Window

From	latest 240 minutes
To	now

Session Information

Source	192.168.101.10
Desination	192.168.102.11
Session Type	Endpoint → Endpoint

Shows Drops on Every Hop.
Green Arrows portray no Drops

NOTE: Some Drops are expected.
Look for Drops like “Buffer” and “Error”!

Recommended Content! – Understanding Drop Faults in ACI

http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/application-policy-infrastructure-controller-apic/210539-Explanations-of-Packet-Drop-Faults-in-AC.html

Troubleshooting Wizard - Contracts

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations | Apps

Advanced Mode
welcome, admin

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker | Visualization

CiscoLive-TSW

- Faults
- Drop/Stats
- Contracts
- Events and Audits
- Traceroute
- Atomic Counter
- SPAN

Shows Contracts for Flows

Spine Spine201 (pod-1/node-201)
Spine Spine202 (pod-1/node-202)

Leaf Leaf103 (pod-1/node-103)
Leaf Leaf104 (pod-1/node-104)
Leaf Leaf101 (pod-1/node-101)
Leaf Leaf102 (pod-1/node-102)

eth1/15 vPC: BareMetal01-vPC
eth1/15 vPC: BareMetal01-vPC
eth1/14 vPC: BareMetal02-vPC
eth1/14 vPC: BareMetal02-vPC

Source Endpoint
IP: 192.168.101.10
MAC: 5C:83:8F:B0:76:C1

Destination Endpoint
IP: 192.168.102.11
MAC: 00:0A:00:0A:00:0A

Implicit Deny

Allow SSH

Source Endpoint → Destination Endpoint

Filter ID: implicit — BD (CiscoLive/BD_Vlan102)

Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
					permit	node-101 node-102 node-103 node-104	0 0 5 0

Filter ID: implicit — Context Implicit (CiscoLive/VRF1)

Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
					deny,log	node-101 node-102 node-103 node-104	17 7 104 1

Destination Endpoint → Source Endpoint

Filter ID: IP — from VLAN_102 to VLAN_101

Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
	icmp				permit	node-101 node-102 node-103 node-104	2357258 0 0 56

Filter ID: SSH (rev) — from VLAN_102 to VLAN_101

Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
	ip:tcp	22 - 22			permit	node-101 node-102 node-103 node-104	368841 0 0 0

Filter ID: implicit — BD Allow (CiscoLive/BD_Vlan101)

Time Window
From latest 240 minutes
To now

Session Information
Source 192.168.101.10
Desination 192.168.102.11
Session Type Endpoint → Endpoint

Troubleshooting Wizard – Atomic Counters

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations | Apps

Advanced Mode
welcome, admin

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker | Visualization

CiscoLive-TSW

- Faults
- Drop/Stats
- Contracts
- Events and Audits
- Traceroute
- Atomic Counter
- SPAN

Atomic Counter

Press Play to start running 00:06:35

Spine Spine201 (pod-1/node-201)
Spine Spine202 (pod-1/node-202)

Leaf Leaf103 (pod-1/node-103)
Leaf Leaf104 (pod-1/node-104)
Leaf Leaf101 (pod-1/node-101)
Leaf Leaf102 (pod-1/node-102)

eth1/15 vPC: BareMetal01-vPC
eth1/15 vPC: BareMetal01-vPC
eth1/14 vPC: BareMetal02-vPC
eth1/14 vPC: BareMetal02-vPC

Source Endpoint
IP: 192.168.101.10
MAC: 5C:83:8F:B0:76:C1

Destination Endpoint
IP: 192.168.102.11
MAC: 00:0A:00:0A:00:0A

No Drops!

Source Endpoint ↔ Destination Endpoint

Source Endpoint → Destination Endpoint

Current				Cumulative			
Tx	Rx	Drop	Excess	Tx	Rx	Drop	Excess
1000	1000	0	0	20169	20169	0	0

Destination Endpoint → Source Endpoint

Current				Cumulative			
Tx	Rx	Drop	Excess	Tx	Rx	Drop	Excess
1000	1000	0	0	40055	40055	0	0

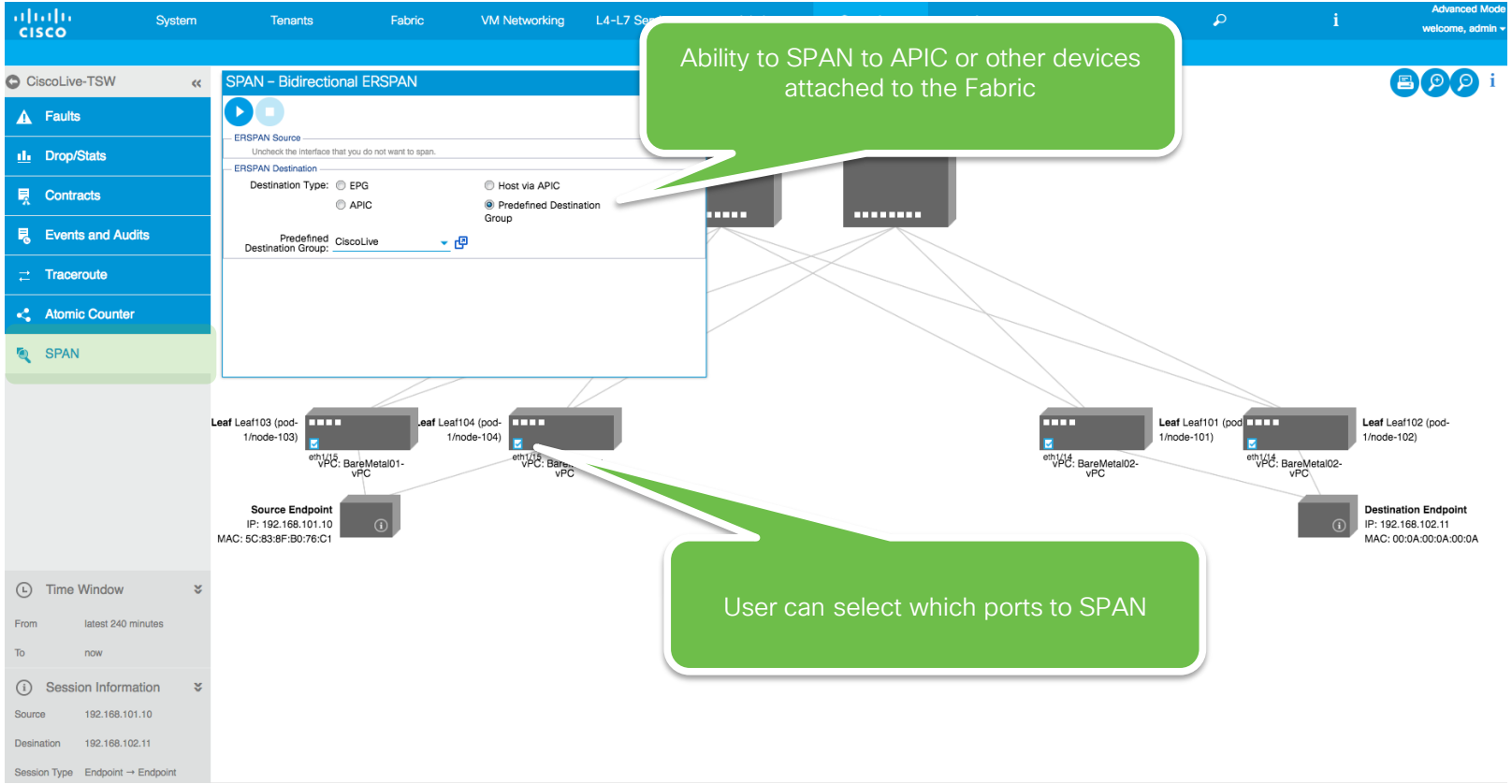
Time Window

From latest 240 minutes
To now

Session Information

Source 192.168.101.10
Desination 192.168.102.11
Session Type Endpoint → Endpoint

Troubleshooting Wizard – SPAN



Capacity Dashboard

APIC

carschmi

System | Tenants | Fabric | Virtual Networking | L4-L7 Services | Admin | Operations | Apps | Integrations

Visibility & Troubleshooting | **Capacity Dashboard** | EP Tracker | Visualization

Capacity Dashboard

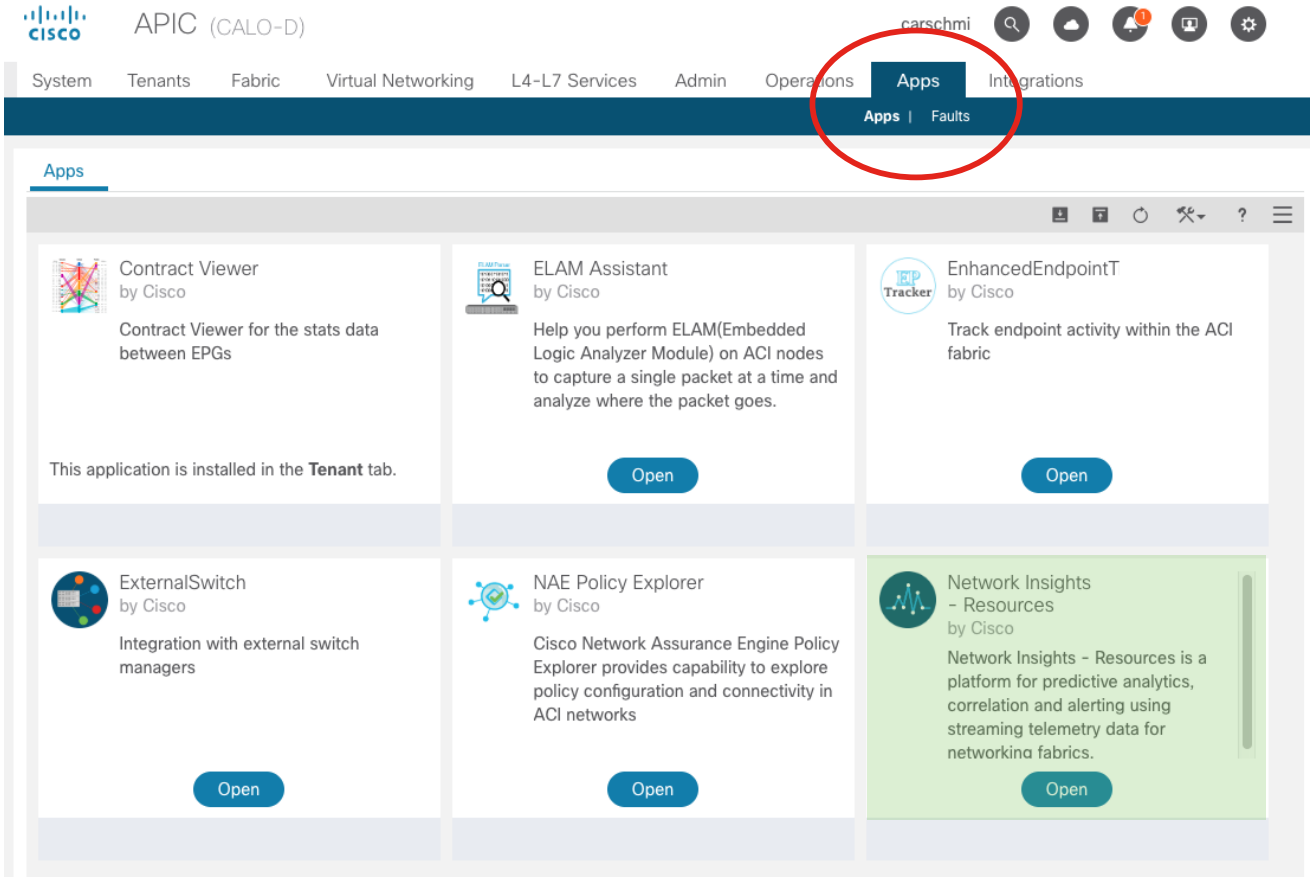
VLAN Capacity is Full!

Fabric Capacity | Leaf Capacity

Switch	VRF	BD	EPG	Mac (learned)	IPv4 (learned)	IPv6 (learned)	Multicast	Policy CAM	VLAN	LPM
pod-1/node-101 N9K-C93180YC-EX Configure Profile	1% 12 of 800	57% 2015 of 3500	50% 2014 of 3960	<1% 19 of 24576 Local: 18 Remote: 1	<1% 11 of 24576 Local: 11 Remote: 0	<1% 1 of 12288 Local: 1 Remote: 0	<1% 1 of 8192	3% Rules: 2078 of 65536 0% Labels: 0	100% 3993 of 3960	0% of 20480
pod-1/node-102 N9K-C93180YC-EX Configure Profile	1% 12 of 800	57% 2016 of 3500	50% 2015 of 3960	<1% 23 of 24576 Local: 23 Remote: 0	<1% 13 of 24576 Local: 13 Remote: 0	<1% 1 of 12288 Local: 1 Remote: 0	<1% 1 of 8192	3% Rules: 2077 of 65536 0% Labels: 0	101% 4001 of 3960	0% of 20480
pod-1/node-103 N9K-C9396PX Scale Profile Not Supported	1% 7 of 400	<1% 9 of 3500	<1% 9 of 3960	<1% Local: 7 of 12288 <1% Remote: 1 of 12288	<1% Local: 5 of 12288 0% Remote: 0 of 12288	<1% Local: 1 of 8192 0% Remote: 0 of 8192	0% 0 of 8192	2% 93 of 4096	<1% 34 of 3960	0%

Capacity Dashboard panel displays your usage by range and percentage.
Use this to plan your fabric Scale.

App Center



Network Insights - Resources

Apps | Network Insights - Resources

Network Insights - Resources

- Dashboard
- System
  - Resource Utilization
  - Environmental
- Operations
  - Flow Analytics
  - Event Analytics

Time Range: May 21st 2019, 4:59 PM - May 21st 2019, 5:14 PM

Time Window allows for filtering of data

Event Analytics Dashboard

Event Analytics by time

Faults (50)
Events (29)
Audit Logs (1)

05 PM 05:01 05:02 05:03 05:04 05:05 05:09 05:10 05:11 05:12 05:13 05:14

Audits/Events/Faults are displayed for the given time window

Audit Logs by Actions

118 Total

0 DELETION
118 CREATION
0 MODIFICATION

Events by Severity

16849 Total

32 CRITICAL
0 MAJOR
0 MINOR
16817 OTHER

Faults by Severity

524 Total

0 CRITICAL
59 MAJOR
48 MINOR
417 OTHER

Network Insights - Resources

Apps | Network Insights - Resources

Network Insights - Resources

Dashboard

Event Analytics

Time Range: May 21st 2019, 4:59 PM - May 21st 2019, 5:14 PM

Browse Audit Logs, Events & Faults

Filters: Description contains VLAN

View by: Type

Audit Logs by Actions: 20 Total; 0 DELETION; 20 CREATION; 0 MODIFICATION

Events by Severity: 0 Total; 0 CRITICAL; 0 MAJOR

Faults by Severity: 0 Total; 0 CRITICAL; 0 MAJOR

20 Total Audit Logs, Events & Faults

Creation Time	Type	Severity/Action	Node	Affected Object	Description
May 21 2019 05:14:03pm	Audit Logs	Creation	calo-d-apic1	uni/tn-CiscoLive/BD-VLAN2007	BD VLAN2007 created
May 21 2019 05:14:03pm	Audit Logs	Creation	calo-d-apic1	uni/tn-CiscoLive/ap-CiscoLive/epg-VLAN2005	AEPg VLAN2005 created
May 21 2019 05:14:03pm	Audit Logs	Creation	calo-d-apic1	uni/tn-CiscoLive/ap-CiscoLive/epg-VLAN2003	AEPg VLAN2003 created

Only Audit Entries Are Present
No Events or Faults!

Filters can be set to focus on specific entries

Now only objects with “VLAN” in the Description are shown

Network Insights - Resources

Apps | Network Insights - Resources

Audit Log Details - **4211945**

General | Timeline

General Information

USER NAME	ACTION	AFFECTED OBJECT	EVENT CODE	EVENT TYPE	CREATED
remoteuser-carschmi	creation	uni/tn-CiscoLive/BD-VLAN2051	4211945	AuditLog	May 29 2019 02:16:11pm

Diagnostics

DESCRIPTION
BD VLAN2051 created

Come On Carlo... Again? How many times do I have to tell you to submit a change control request!

Network Insights - Resources

Apps | Network Insights - Resources

Network Insights - Resources

Time Range: May 21st 2019, 2:27 PM - May 21st 2019, 2:42 PM

- Dashboard
- System
  - Resource Utilization
  - Environmental
- Operations
  - Flow Analytics
  - Event Analytics

Dashboard

Total Controllers: 3

Total Nodes: spines, leaves

Anomaly Detection Helps Identify Changes in Real Time

Anomalies by Type

2 Total

1 FLOW ANALYTICS

0 UTILIZATION

1 ENVIRONMENTAL

2 Total

0 CRITICAL

0 MAJOR

0 MINOR

2 OTHER

Network Insights - Resources

Apps | Network Insights - Resources

Network Insights - Resources

- Dashboard
- System
  - Resource Utilization
  - Environmental
- Operations
  - Flow Analytics
  - Event Analytics

Time Range: May 21st 2019, 2:27 PM - May 21st 2019, 2:42 PM

Browse Anomalies

Filters: Category == **Flow Analytics**

Anomalies By: Type

1 Total

1 FLOW ANALYTICS | 0 UTILIZATION | 0 ENVIRONMENTAL

Top 2 nodes contributing to Anomalies

Node	Anomaly Score
d-leaf104	
d-leaf101	

Flow Analytics Can Analyze Broken Traffic Flows and alert via Anomaly

1 Total Anomalies

Start Time	End Time	Severity	Resource Type	Nodes	Description
May 21 2019 02:39:26pm	May 21 2019 02:43:59pm	Info	flow	d-leaf101	Packet drop is detected due to Policy Drop.

Network Insights - Resources

Details about Affected Endpoints are reported

Apps | Network Insights - Resources

Flow Details

General Information

SOURCE			DESTINATION		
ADDRESS	PORT	EPG	ADDRESS	PORT	EPG
192.168.4.40	0	e4	192.168.3.11	0	e3

View More

If drop, Node which is dropping and reason can be easily identified!

Path Summary

No Contract!

May 21 2019, 2:39 PM

Policy Drop

Source → d-leaf101 → Destination

192.168.4.40
Port: 0
e4

d-leaf101
po2 unknown

192.168.3.11
Port: 0
e3

ELAM Assistant App

Apps | ELAM Assistant

ELAM Assistant

Capture a packet with ELAM (Embedded Logic Analyzer Module)

- Capture (Perform ELAM)
- node-101 (d-leaf101)
- node-102 (d-leaf102)
- node-103 (d-leaf103)
- node-104 (d-leaf104)
- node-201 (d-spine201)
- node-202 (d-spine202)
- Unsupported Nodes

ELAM PARAMETERS | Quick Add | Add Node

Name your capture: *(optional)*

Status	Node	Direction	Source I/F	Parameters	
Set	node-101	from frontport	any	src ip	192.168.4.40
				dst ip	192.168.3.11
Report Ready	node-102	from frontport	any	src ip	192.168.4.40
				dst ip	192.168.3.11

VxLAN (outer) header

Set ELAM(s) | Check Trigger

(report name:)

Select a report.

Report is generated if packet enters the switch with matching criteria

Set packet parameters to match on

ELAM Assistant App

Provides Detailed Information about the packet that was triggered

Captured Packet Information

Basic Information	
Device Type	LEAF
Packet Direction	ingress (front panel port -> leaf)
Inconming I/F	eth1/13

Packet Forwarding Information

Forward Result	
Destination Type	To a local port
Destination Logical Port	Eth1/32
Destination Physical Port	packet dropped
Sent to SUP/CPU instead	yes
SUP Redirect Reason (SUP code)	ISTACK_SUP_CODE_ACL_LOG

Packet is Dropped

Drop	
Drop Code	SECURITY_GROUP_DENY

No Contract!

L2 Header	
Destination MAC	0022.BDF8.19FF
Source MAC	8C60.4F08.0241
Access Encap VLAN	740
CoS	0

L3 Header	
L3 Type	IPv4
Destination IP	192.168.3.11
Source IP	192.168.4.40
IP Protocol	0x1 (ICMP)
DSCP	0
TTL	255
Don't Fragment Bit	0x0 (not set)
IP Checksum	0xBD96
IP Packet Length	84 (IP header(28 bytes) + IP payload)

Enhanced Endpoint Tracker

Troubleshooting Endpoint Moves

Provides Historical Data of All Endpoints, including # of moves

Search MAC or IP for this fabric. I.e., 00:50:56:01:BB:12, 10.1.1.101, or 2001:a:b::65

Moves

Time	Type	Address	Event Count	VRF/BD
May 09 2019 - 14:20:44	mac	90:E2:BA:29:F8:C9	145	uni/tn-insbulab/BD-internetConnectedBD
May 09 2019 - 14:19:59	ipv4	172.23.136.172	58	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:19:44	mac	00:50:56:67:D8:93	59	uni/tn-insbulab/BD-192
May 09 2019 - 14:19:39	mac	00:50:56:63:88:49	58	uni/tn-insbulab/BD-192
May 09 2019 - 14:18:37	ipv4	172.31.141.245	5	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:14:57	ipv4	172.31.140.115	32	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:14:32	ipv4	172.31.142.39	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:13:43	ipv4	172.23.139.233	17	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:12:53	ipv4	172.23.136.237	27	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:12:01	ipv4	172.23.136.154	28	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:11:54	ipv4	172.23.138.99	7	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:11:16	ipv4	172.31.140.89	36	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 14:09:33	ipv4	172.31.128.168	3	uni/tn-insbulab/ctx-labvrf

Enhanced Endpoint Tracker

Troubleshooting Endpoint Moves

Search MAC or IP for this fabric. I.e., 00:50:56:01:BB:12, 10.1.1.101, or 2001:a:b::65

mac 90:E2:BA:29:F8:C9

Fabric **insbu** BD **uni/tn-insbulab/BD-internetConnectedBD** EPG **uni/tn-insbulab/ap-base/epg-lab**

Local on **pod-1** node **1004** interface **eth1/44** encap **vlan-900**

Remotely learned on **1** node.

145 Moves 0 Rapid events 0 OffSubnet events 0 Stale events 0 Clear events

Actions

History Detailed Move Rapid OffSubnet Stale Cleared

Time	Local Node	Status	Interface	Encap	pcTAG	EPG
May 09 2019 - 14:20:44	1004	created	eth1/44	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:20:44	1010	created	eth1/37	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:20:44	1004	created	eth1/44	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:20:44	1010	created	eth1/37	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:20:44	1004	created	eth1/44	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:19:48	1010	created	eth1/37	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:19:40	1004	created	eth1/44	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:18:48	1010	created	eth1/37	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:18:42	1004	created	eth1/44	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab
May 09 2019 - 14:18:38	1010	created	eth1/37	vlan-900	16387	uni/tn-insbulab/ap-base/epg-lab

Provides Exact Location of Endpoint

Node and Interface Move history allows for easy issue isolation

Enhanced Endpoint Tracker

Troubleshooting Off Subnet Endpoints

Any Endpoint which is off subnet is flagged. Unexpected for Network Centric Deployment!

Search MAC or IP for this fabric. I.e., 00:50:56:01:BB:12, 10.1.1.101, or 2001:a:b::65

These are historical records. The endpoint may no longer be offsubnet.

OffSubnet Endpoints

Time	Type	Address	Affected Node	Event Count	VRF/BD
May 09 2019 - 13:12:49	ipv4	10.193.239.113	1007	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.193.31.149	1009	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.23.236.93	1009	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.193.12.220	1009	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.193.10.244	1010	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	172.31.162.135	1010	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.30.219.84	1010	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.23.239.37	1009	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	64.100.48.246	1009	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.30.11.70	1005	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.122.143.19	1010	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	172.27.193.213	1009	1	uni/tn-insbulab/ctx-labvrf
May 09 2019 - 13:12:49	ipv4	10.193.250.87	1009	1	uni/tn-insbulab/ctx-labvrf

Enhanced Endpoint Tracker

Troubleshooting Off Subnet Endpoints

Search MAC or IP for this fabric. I.e., 00:50:56:01:BB:12, 10.1.1.101, or 2001:a:b::65

ipv4 10.193.239.113

offsubnet Nodes 1007

Fabric **insbu** VRF **uni/tn-insbulab/ctx-labvrf** EPG **-**

Not local on any node.

Remotely learned on **1** node.

Actions

0 Moves 0 Rapid events 1 OffSubnet events 0 Stale events 0 Clear events

History Detailed Move Rapid OffSubnet Stale Cleared

Time	Affected Node	Interface	Encap	Remote Node	EPG
May 09 2019 - 13:12:49	1007	tunnel6	-	(1101,1102)	uni/tn-insbulab/ap-base/epg-lab

1 total

Day 7: Additional Resources

You make networking **possible**

Support Forums

TAC Engineers are Subscribed

Easy Portal to Post Non Impacting Questions or Concerns

Has Documentation written by CSE's and Technical Leaders

Application Centric Infrastructure

Join the ACI conversation. Jump into this space for access to peers and industry experts. You'll find the latest updates, helpful resources, and assistance when you need it.

Labels

ACI App Center (7) | ACI Multi-Site (8) | ACI Power Tool (3) | ACI Virtual Edge (AVE) (1) | ACI Virtual Pod (2) | APIC (48) | Cisco ACI (1,622) | Other ACI Topics (11) | Other ACI TopicsCisco ACI (8) | Software Defined Networks (31)

‹ Previous 1 2 3 ... 113 Next ›

	Replies	Helpful Votes	Views
How to downgrade the ACI-Mode OS. by pine78 on 05-21-2019 06:34 PM · Latest post on 05-22-2019 06:35 AM by stcorry Cisco ACI	1 REPLY	0	70 VIEWS
Cisco ACI contracts by MedRT on 05-22-2019 02:33 AM Cisco ACI	0 REPLIES	0	47 VIEWS

https://supportforums.cisco.com/t5/application-centric/bd-p/12206936-discussions-aci

Facebook Group

Many Customers and Cisco Employees

Great Real World Deployment Advice

Great way to meet others working with ACI

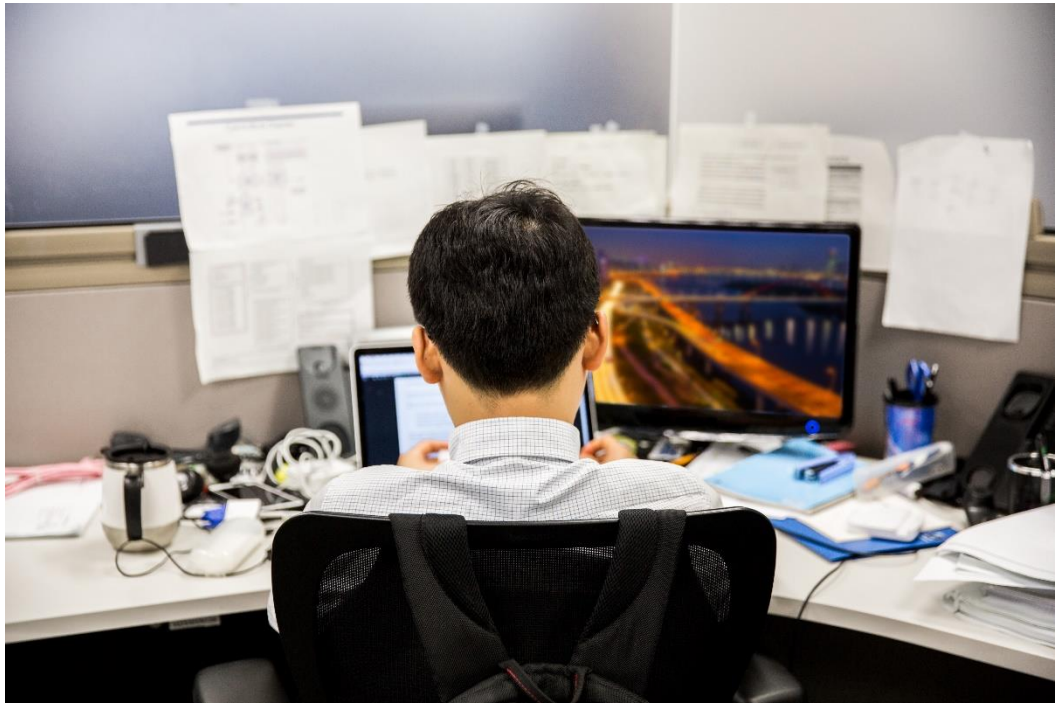
Solutions Support

One TAC team to support all aspects of ACI

Engineers are familiar with 3rd party products like VMWare

Case does not get handed off when it is a Switching vs. Routing issue.

ACI Team takes ownership



Complete your online session evaluation

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live water bottle.
- All surveys can be taken in the Cisco Live Mobile App or by logging in to the Session Catalog on ciscolive.cisco.com/us.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.cisco.com.

Continue your education

Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**