



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

Ciscolive!

June 9-13, 2019 • San Diego, CA

#CLUS



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

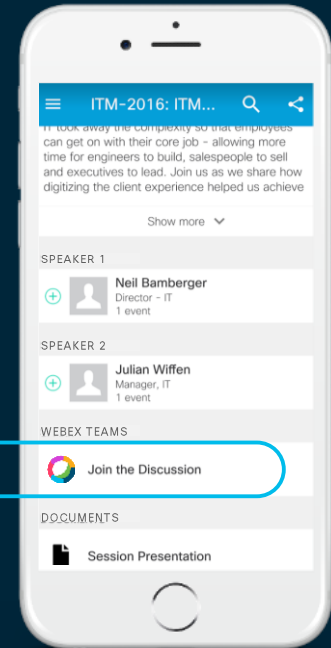
Questions?

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		

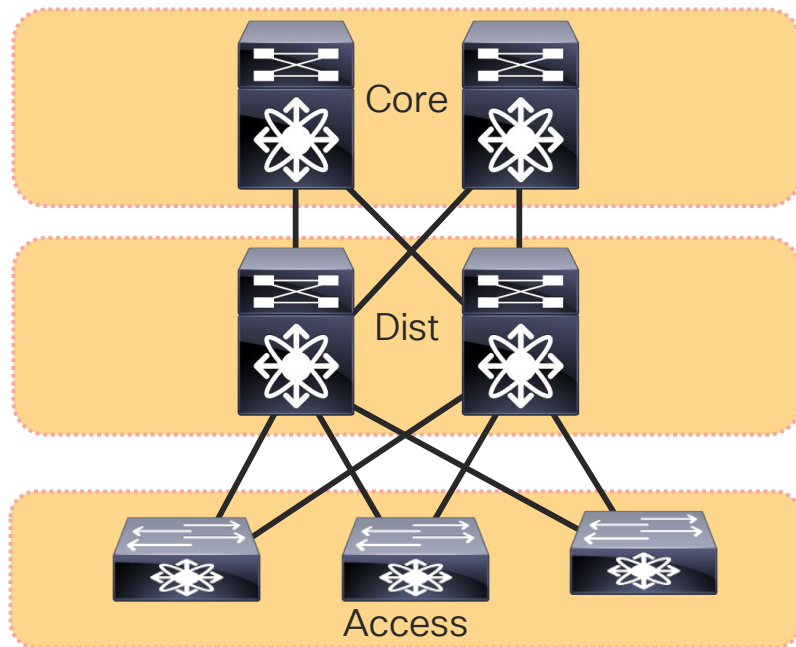
Day 1: Why ACI?



You make networking **possible**

Why ACI?

Challenges of Today



Management

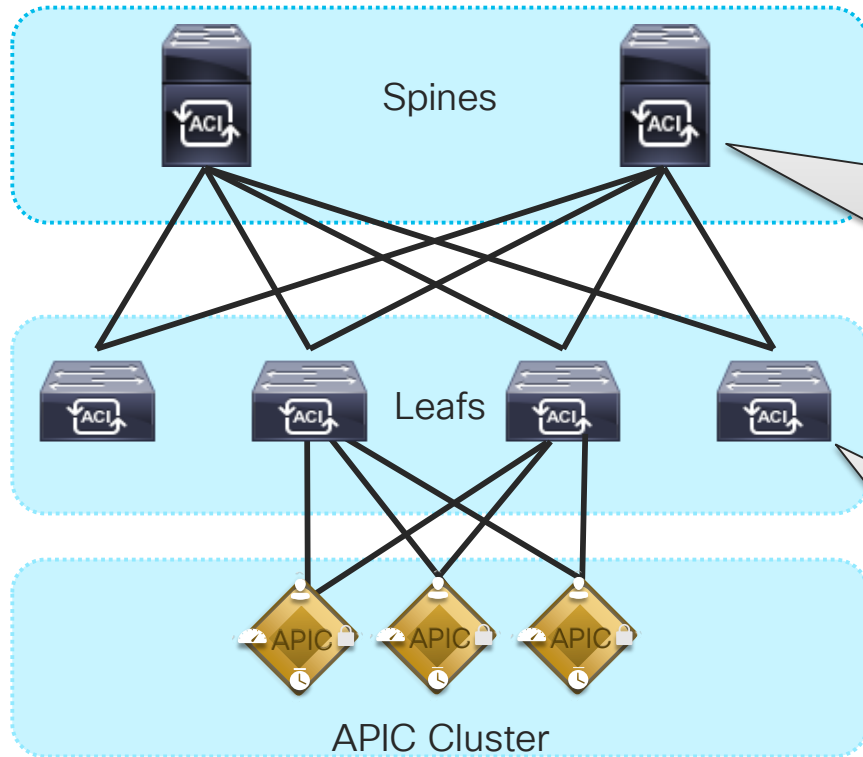
- CLI to every Device
- Manual Configuration – Takes Time
- Coordination between Network and Server Team
- Harder as we scale!

Functionality

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

Why ACI?

ACI Overview



Cisco *live!*

Application Centric Infrastructure

Software Defined Networking built on Nexus 9000

Control Plane is Decoupled From the Data Plane

Spine1# show module

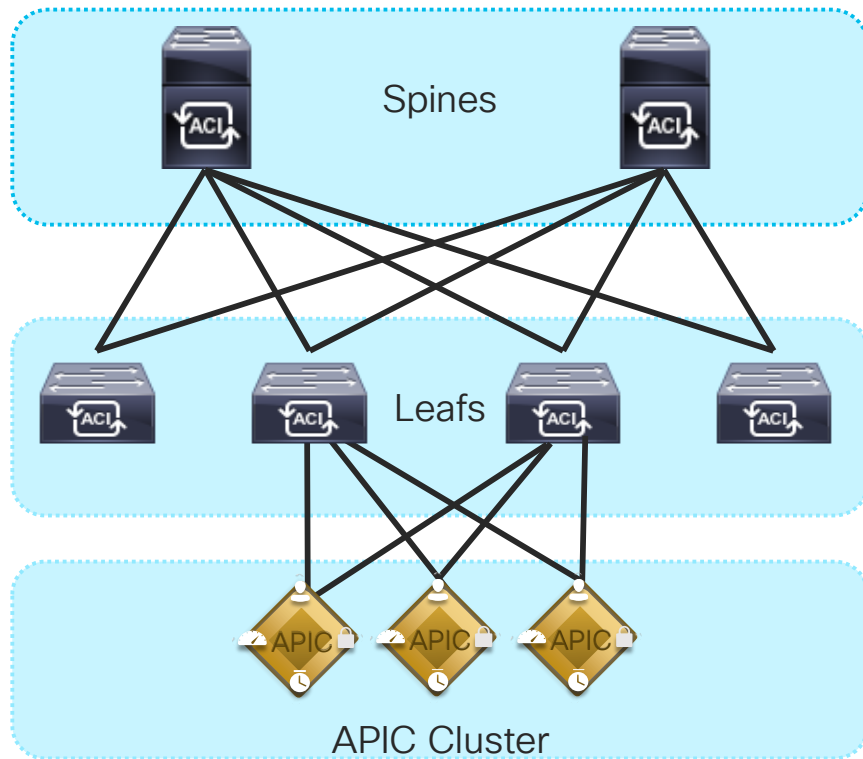
Mod	Ports	Module-Type	Model	Status
2	32	32p 40/100G Ethernet Module	N9K-X9732C-EX	ok
22	0	Fabric Module	N9K-C9504-FM-E	ok
23	0	Fabric Module	N9K-C9504-FM-E	ok
24	0	Fabric Module	N9K-C9504-FM-E	ok
26	0	Fabric Module	N9K-C9504-FM-E	ok
27	0	Supervisor Module	N9K-SUP-A	Active
28	0	Supervisor Module	N9K-SUP-A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



Cisco *live!*

Management

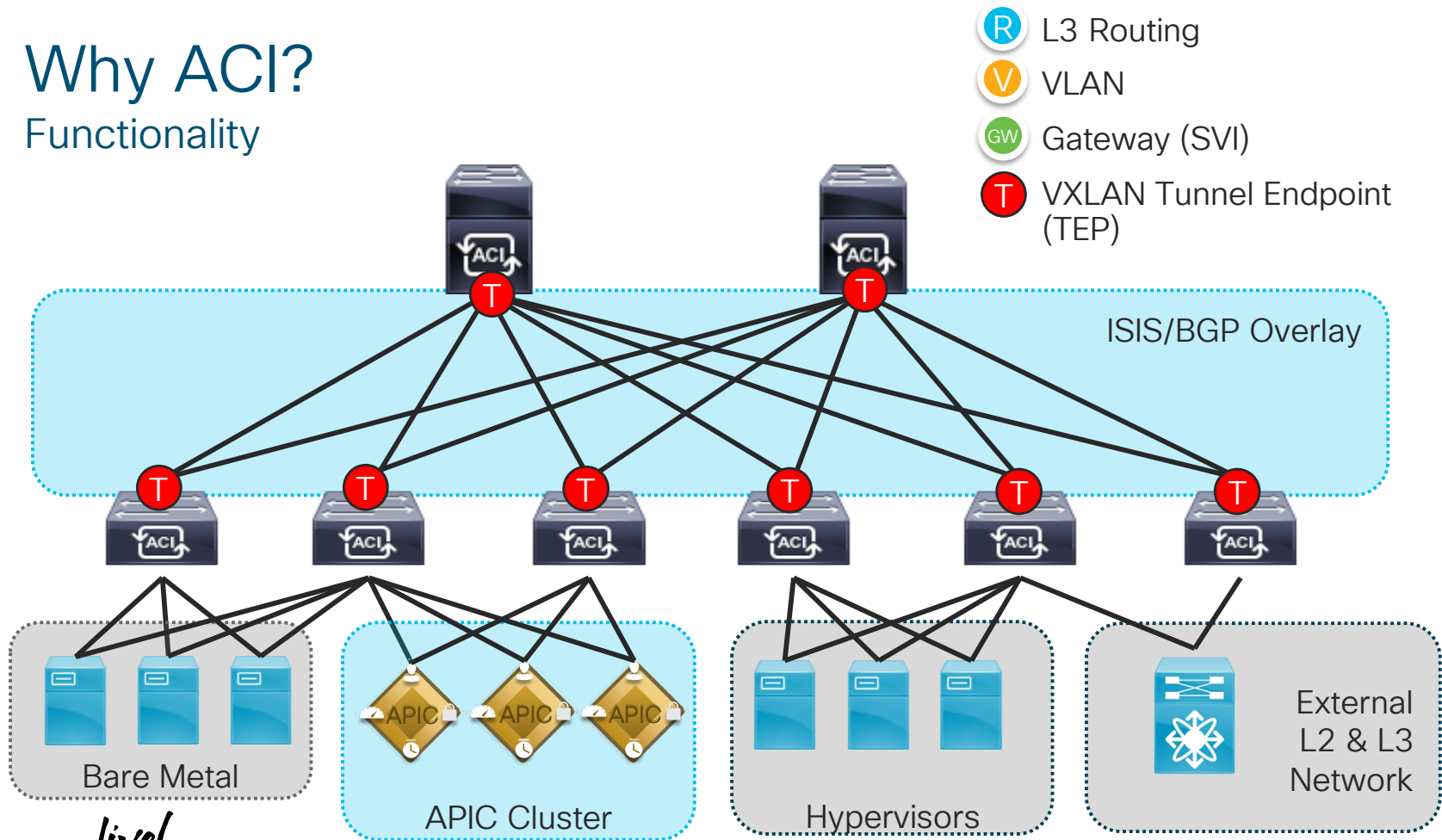
- Fabric is managed by APIC
- All configuration exposed via API
- Switches join fabric in a few clicks!

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 an 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

Controller Status

ID	Name	IP	Admin State	Operational State	Health State
1	apic1	10.0.0.1	In Servi...	Available	Fully Fit
2	apic2	10.0.0.2	In Servi...	Available	Fully Fit
3	apic3	10.0.0.3	In Servi...	Available	Fully Fit

Nodes With Health ≤ 99

Name	POD ID	Type	Health Score
Leaf101	1	leaf	98
Leaf102	1	leaf	98
Leaf103	1	leaf	98
Leaf104	1	leaf	88
Spine201	1	spine	98

Tenants With Health ≤ 99

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

Fault Counts By Domain

☐ Hide Acked Faults ☐ Hide Delegated Faults

Fault Level: △ △ ! !

Domain	1	3	10	0
SYSTEM WIDE	1	3	10	0
Access	1	0	0	0
External	0	0	0	0
Framework	0	0	0	0
Infra	0	3	10	0
Management	0	0	0	0
Security	0	0	0	0
Tenant	0	0	0	0

Fault Counts By Type

☐ Hide Acked Faults ☐ Hide Delegated Faults

Fault Level: △ △ ! !

Type	1	0	0	0
Communication...	1	0	0	0
Config	0	0	0	0
Environmental	0	0	6	0
Operational	0	3	4	0

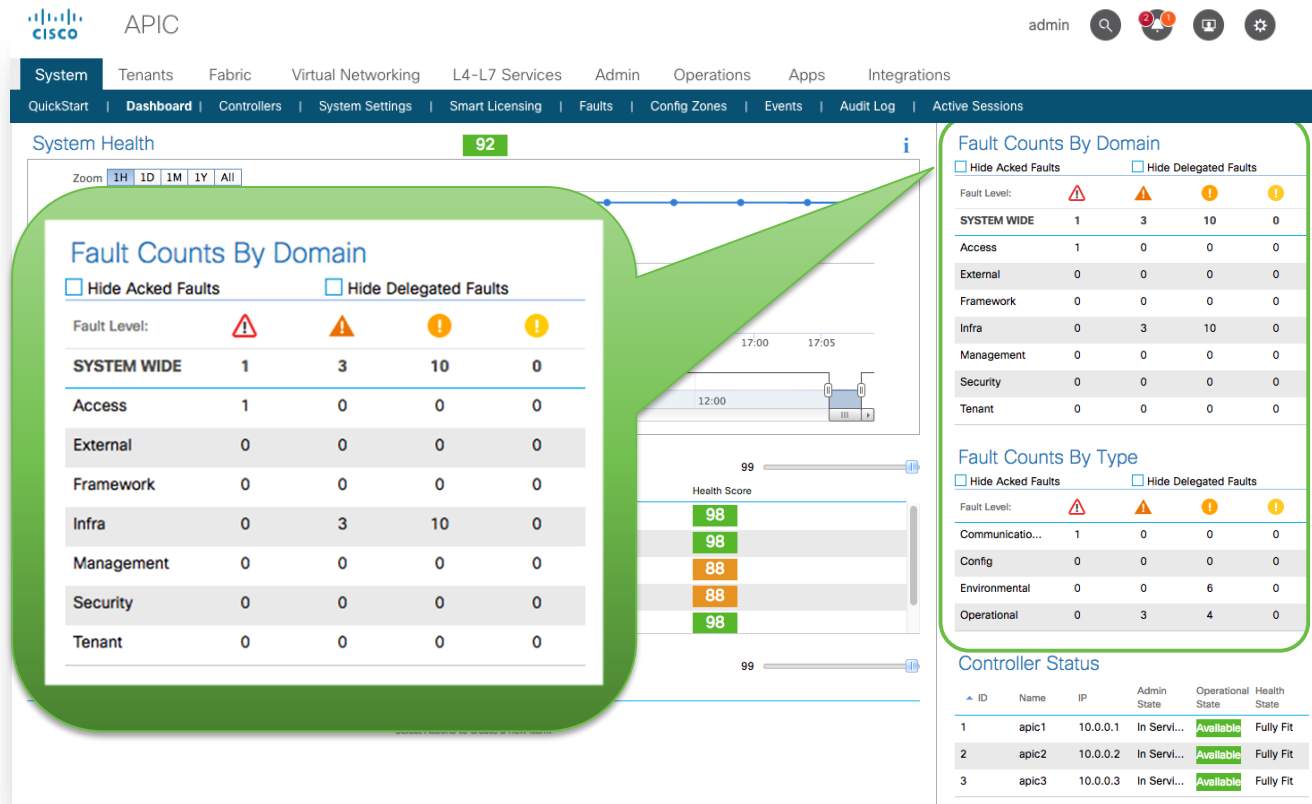
Controller Status

ID	Name	IP	Admin State	Operational State	Health State
1	apic1	10.0.0.1	In Servi...	Available	Fully Fit
2	apic2	10.0.0.2	In Servi...	Available	Fully Fit
3	apic3	10.0.0.3	In Servi...	Available	Fully Fit

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

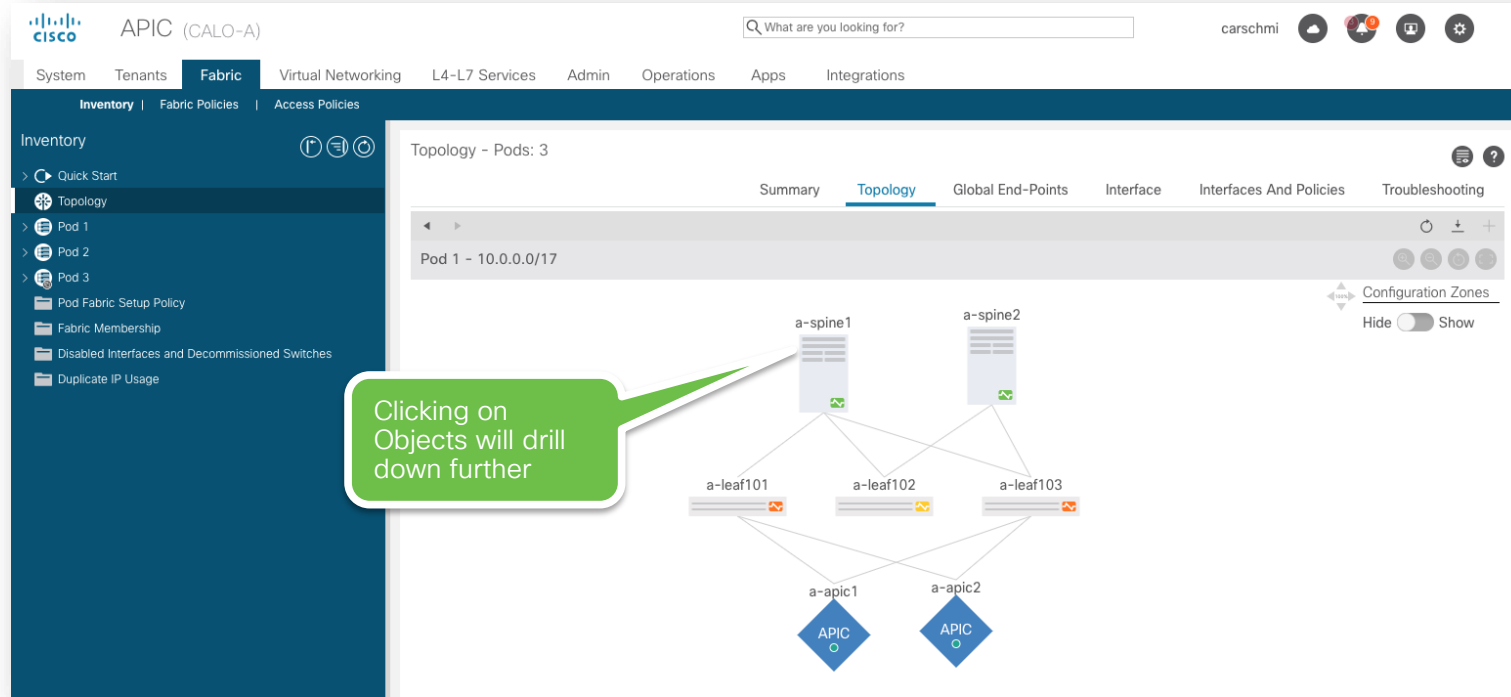
- Health scores are driven based on faults and events
- Can be viewed system wide or per object



Why ACI?

Management Overview

- Fabric Inventory and Topology are centrally managed.



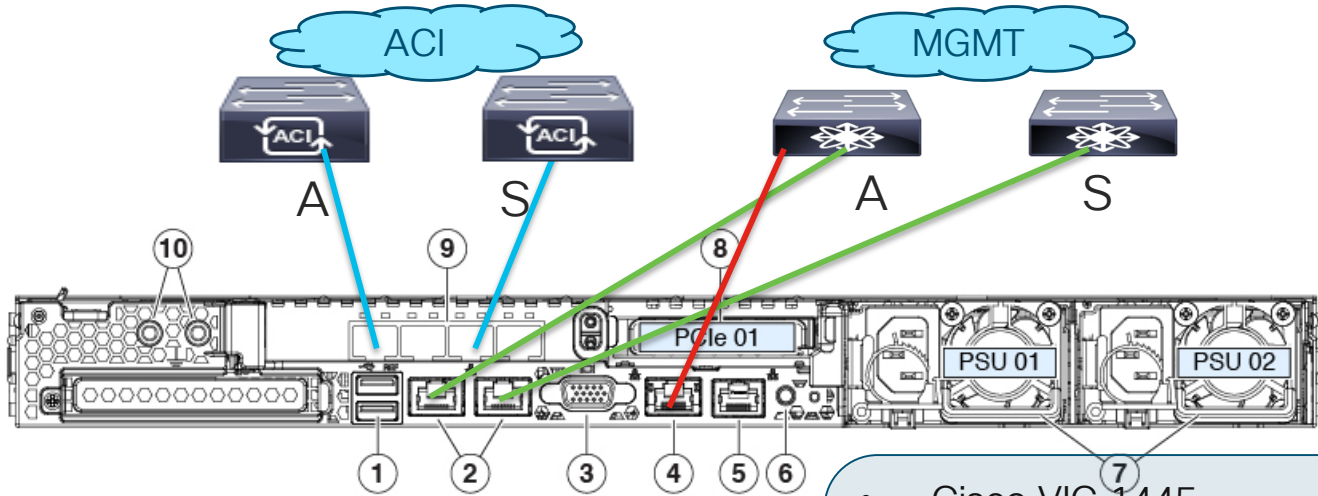
Day 2: Infrastructure and Policies



You make networking **possible**

Infrastructure and Policies

APIC Components



UCS C220

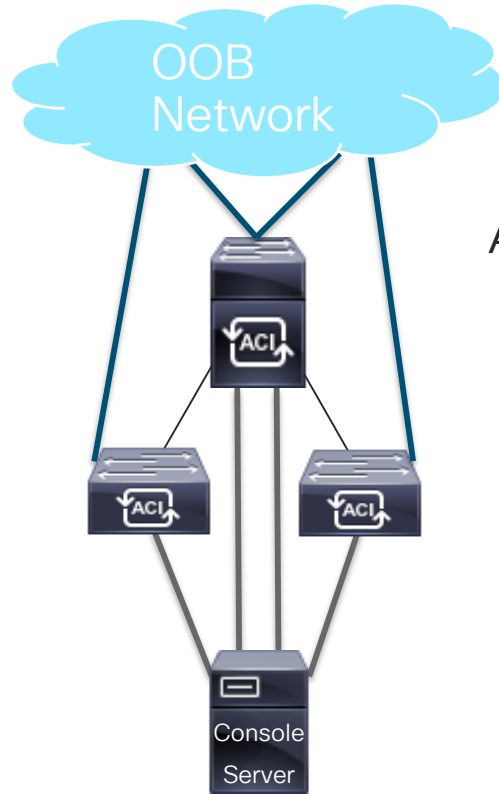
A – Active
S – Standby

- 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



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

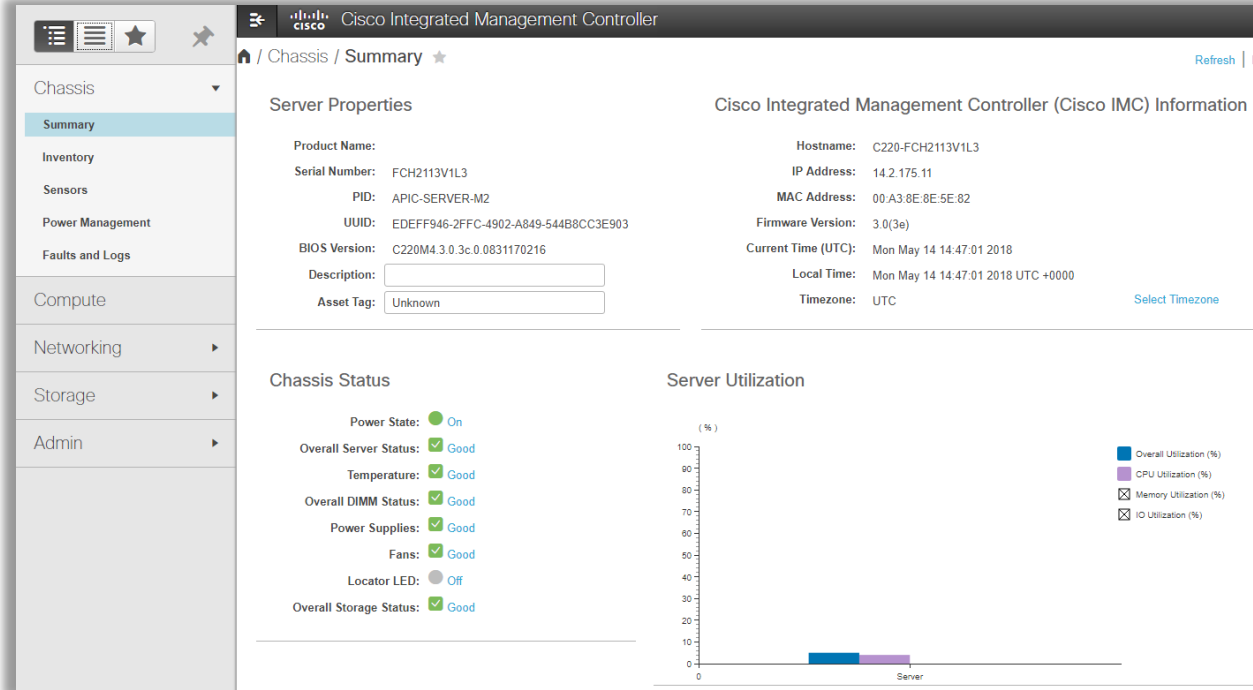
1 Console

40/100 Gb connections to Spines



Infrastructure and Services

CIMC

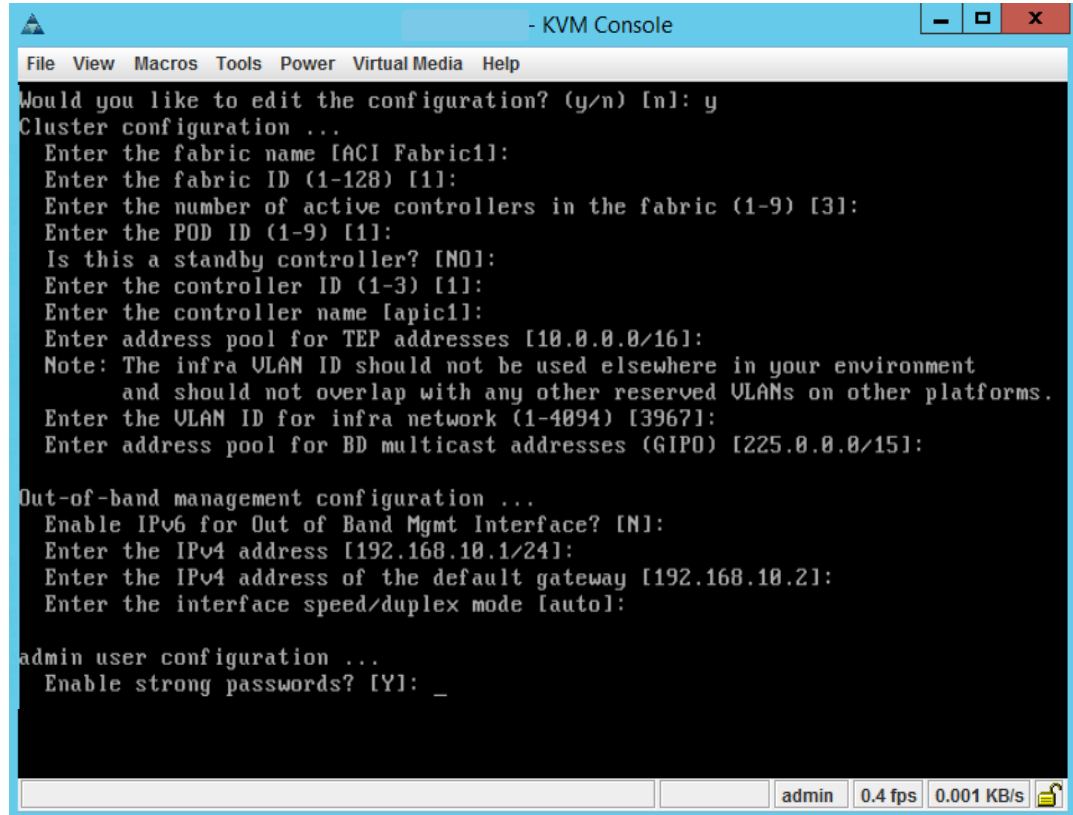
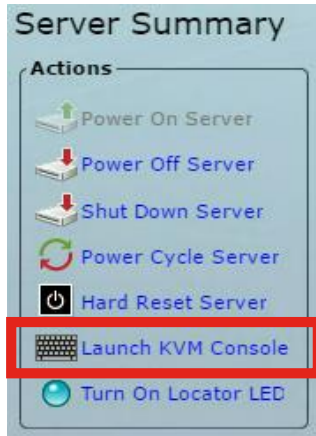


Use for APIC
Hardware
Diagnostics and
Remote Access
Use to install the
APIC Software

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 (GIP0) [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

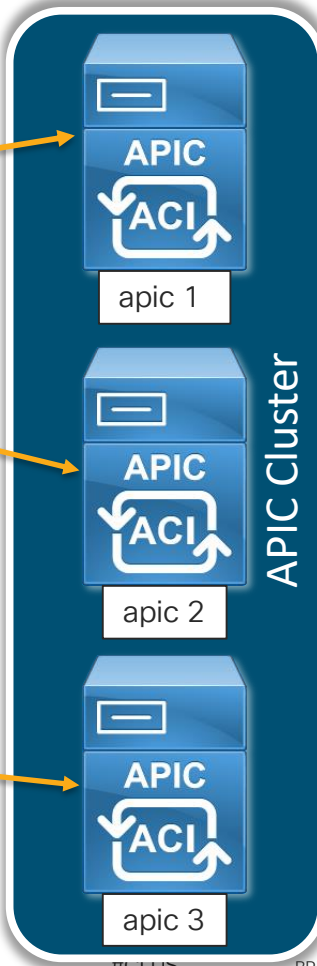


`https://apic1/`
Web Browser

REST API
`https://apic2/api/`



`ssh apic3 -l admin`
SSH



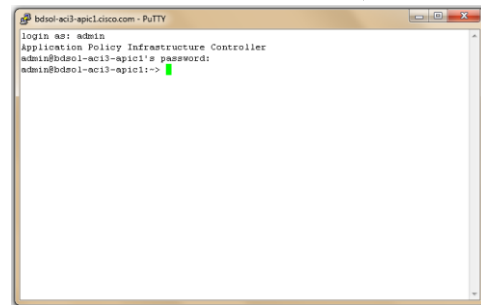
APIC UI



API

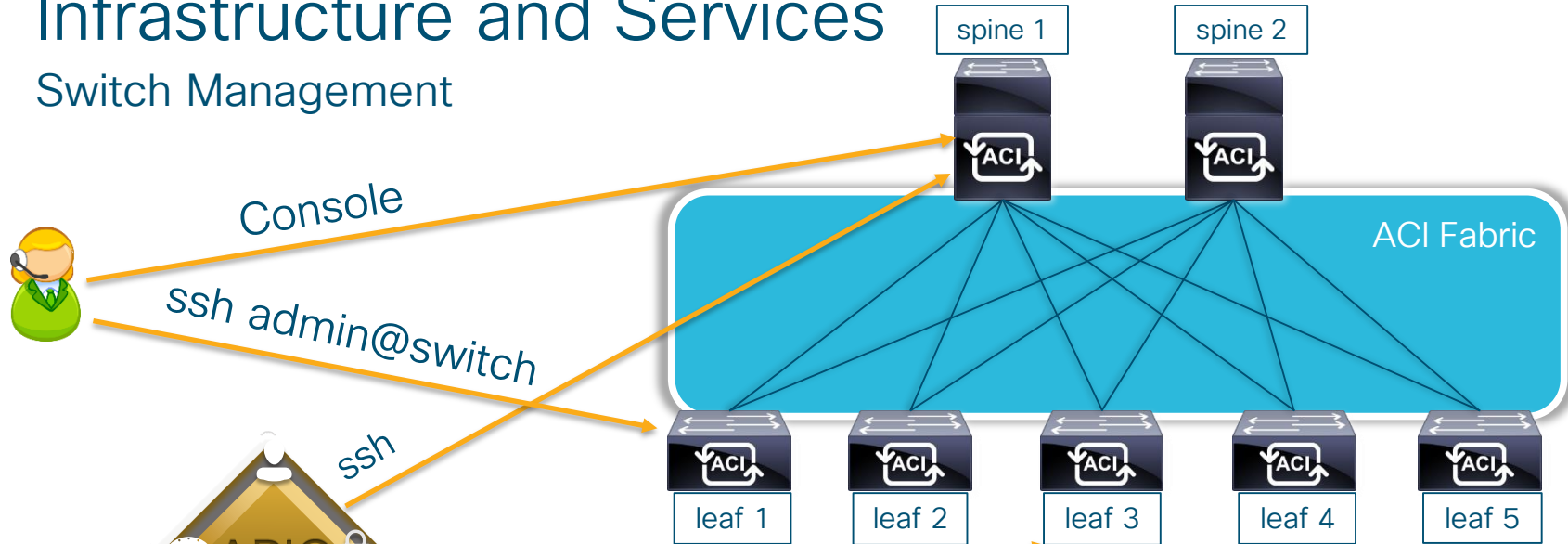


CLI (ssh)



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

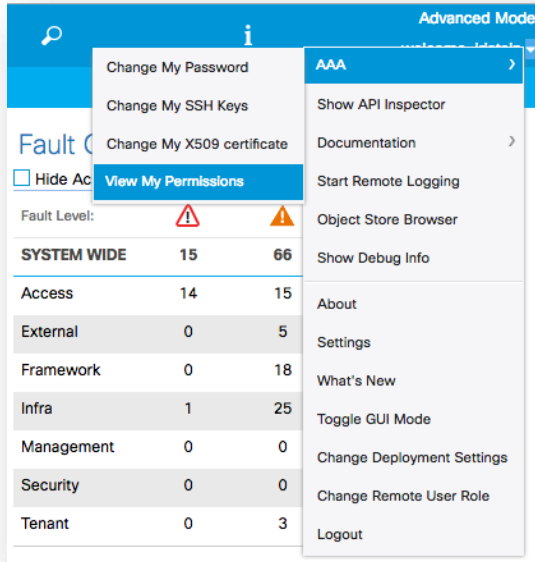


You make security **possible**

Infrastructure and Services

AAA

Allows users to authenticate with certain privilege levels



The screenshot shows the Cisco GUI in 'Advanced Mode'. A user profile icon is in the top left. A dropdown menu is open, showing options like 'Change My Password', 'Change My SSH Keys', 'Change My X509 certificate', and 'View My Permissions' (which is highlighted). To the right of this menu is a sidebar with 'AAA' settings, including 'Show API Inspector', 'Documentation', 'Start Remote Logging', 'Object Store Browser', 'Show Debug Info', 'About', 'Settings', 'What's New', 'Toggle GUI Mode', 'Change Deployment Settings', 'Change Remote User Role', and 'Logout'.



Application Centric Infrastructure - ACI

Please sign in to connect to APIC

User ID: _____

Password: _____

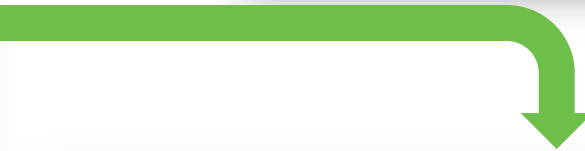
Domain: _____

Mode: DefaultAuth

LDAP

Local

TACACS



User Permissions



Domains:	Name	Read Privileges	Write Privileges
	all	admin	admin

Infrastructure and Services

AAA

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


Modification Log Record - 8589940567

Properties

ID: **8589940567**

Description: **BD Joey-BD3 modified**

Affected Object:  uni/tn-Joey-Tenant/BD-Joey-BD3

Time Stamp: **2017-02-13T15:06:07.249+00:00**

Cause: **transition**

Change Set: **arpFlood (Old: no, New: yes), unkMacUcastAct (Old: proxy, New: flood)**

Action Performed: **modification**

Action Trigger: **config**

Transaction ID: **4611686018449066821**

User: **remoteuser-jristain**

CLOSE

```
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**

Remote Location - CiscoLive-SFTP

Properties

Name: **CiscoLive-SFTP**

Description: optional

Host Name (or IP Address): **172.16.0.1**

Protocol: **sftp**

Remote Path: **/CiscoLive**

Remote Port: **22**

Username: **ciscolive**

URL: **sftp://172.16.0.1:22/CiscoLive**

Management EPG: **uni/tn-mgmt/mgmt-default/oob-default**

Create Configuration Export

Name: ciscoLive

Description: optional

Format: **json** xml

Start Now: **Yes** No

Target DN:

Snapshot: ☐

Scheduler: OnceADay

Export Destination: **CiscoLive-SFTP**

Modify Global AES Encryption Settings: **Enabled**

Create Schedule Window

Window Type: ☐ One Time
☒ Recurring

Window Name: **Every-Day**

Day: **every-day**

Hour: **0**

Minute: **0**

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

The screenshot displays the 'Config Rollbacks' section of the Cisco APIC interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, Apps, and Integrations. The 'Admin' tab is active, and the 'Config Rollbacks' sub-tab is selected. Below the navigation bar, there is a dropdown menu for 'for: Tenant'. The main content area features a table with four columns: Snapshots, File Name, Description, and File Size (bytes). The table lists four snapshots, all with file names starting with 'ce2_DailyAutoBackup-2019-05-1...'. To the right of the table, the 'Actions' section contains several options: 'Rollback' (with a note to select a snapshot), 'Take a snapshot' (with a form for Location and Description, and a 'Create a snapshot now' button), 'Import export file to snapshot' (with a download icon), 'Modify import/export security settings' (with a gear icon), and 'Create recurring snapshots' (with a camera icon).

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:
Description:
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

Snapshots	File Name	File Size (Bytes)
<input type="radio"/> 2017-02-13 15:02:34.508	ce2_defaultOneTime_tn-Joey-Tenant-2017-0...	8511
<input type="radio"/> 2017-02-13 15:05:19.968	ce2_defaultOneTime_tn-Joey-Tenant-2017-0...	8513

ROLLBACK TO THIS CONFIGURATION

Compare with previous snapshot:

<

Showing changes from 2017-02-13 15:05:19.968 to 2017-02-13 15:06:16.401

You may undo these changes if they are undesirable

```
<fvTenant
  name="Joey-Tenant"
  rn="tn-Joey-Tenant"
  >
  <fvBD
    name="Joey-BD3"
    rn="BD-Joey-BD3"
    vmac="not-applicable"
    unkMacUcastAct="flood"
    unkMacUcastAct="proxy"
    multiDstPktAct="bd-flood"
    mcastAllow="no"
    mac="00:22:BD:F8:19:FF"
    unicastRoute="yes"
    unkMcastAct="flood"
    arpFlood="no"
    limitIpLearnToSubnets="yes"
    llAddr="::"
    arpFlood="yes"
    type="regular"
    ipLearning="yes"
  >
```

Object

Changed To

Changed From

Changed From

Changed To



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**

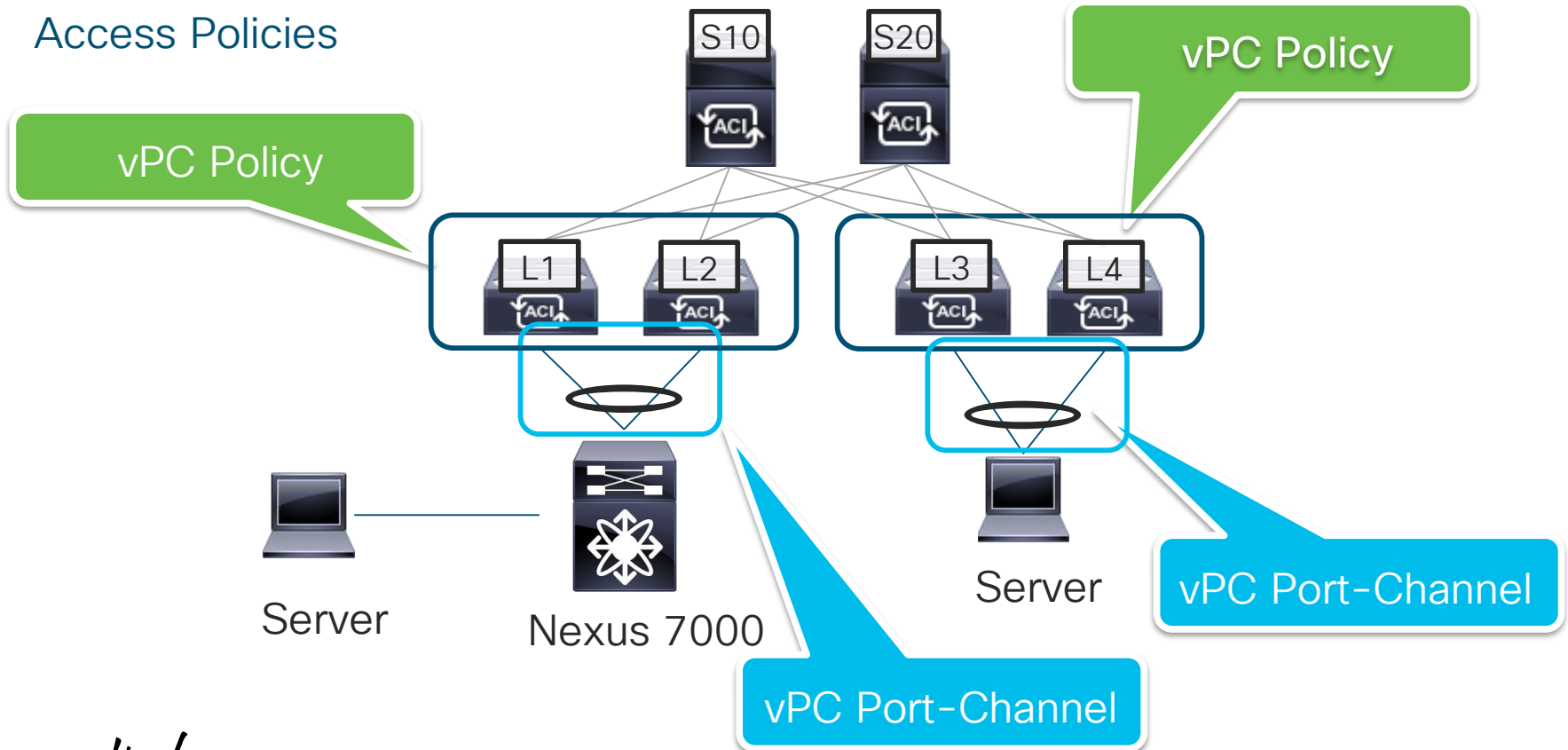
Fabric and Tenant Policies



You make the power of data **possible**

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

The screenshot shows the Cisco vPC configuration interface. The left sidebar displays a tree view of policies, with 'Virtual Port Channel default' selected. The main panel shows the 'Virtual Port Channel Security Policy - Virtual Port Channel default' configuration. The 'Properties' section includes a 'Description' field with the value 'VPC Pairs' and a 'Pairing Type' dropdown set to 'explicit'. Below this, the 'Explicit VPC Protection Groups' table is visible, showing two groups: '101-102' and '103-104', both with a 'Domain Policy' of 'default' and 'Logical Pair ID' of 1 and 2 respectively. The 'Virtual IP' column shows '10.0.152.64/32' and '10.0.152.65/32'.

Name	Domain Policy	Switches	Logical Pair ID	Virtual IP
101-102	default	101, 102	1	10.0.152.64/32
103-104	default	103, 104	2	10.0.152.65/32

Switches

Logical Pair ID

Virtual IP

101, 102

1

10.0.152.64/32

103, 104

2

10.0.152.65/32

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
```

Properties

Name: **N7710-vPC**

Description: optional

Link Aggregation Type: **Port Channel** **VPC**

Link Level Policy: select a value

CDP Policy: CDP_Enable

MCP Policy: MCP_Enable

LLDP Policy: LLDP_Enable

STP Interface Policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Priority Flow Control Policy: select a value

Fibre Channel Interface Policy: select a value

Slow Drain Policy: select a value

Port Channel Policy: **LACP_Active**

Monitoring Policy: default

Storm Control Interface Policy: select a value

L2 Interface Policy: select a value

Port Security Policy: select a value

Attached Entity Profile: CiscoLive

Mode: **LACP Active**

- Control:
- ☒ Fast Select Hot Standby Ports
 - ☒ Graceful Convergence
 - ☐ Load Defer Member Ports
 - ☒ Suspend Individual Port

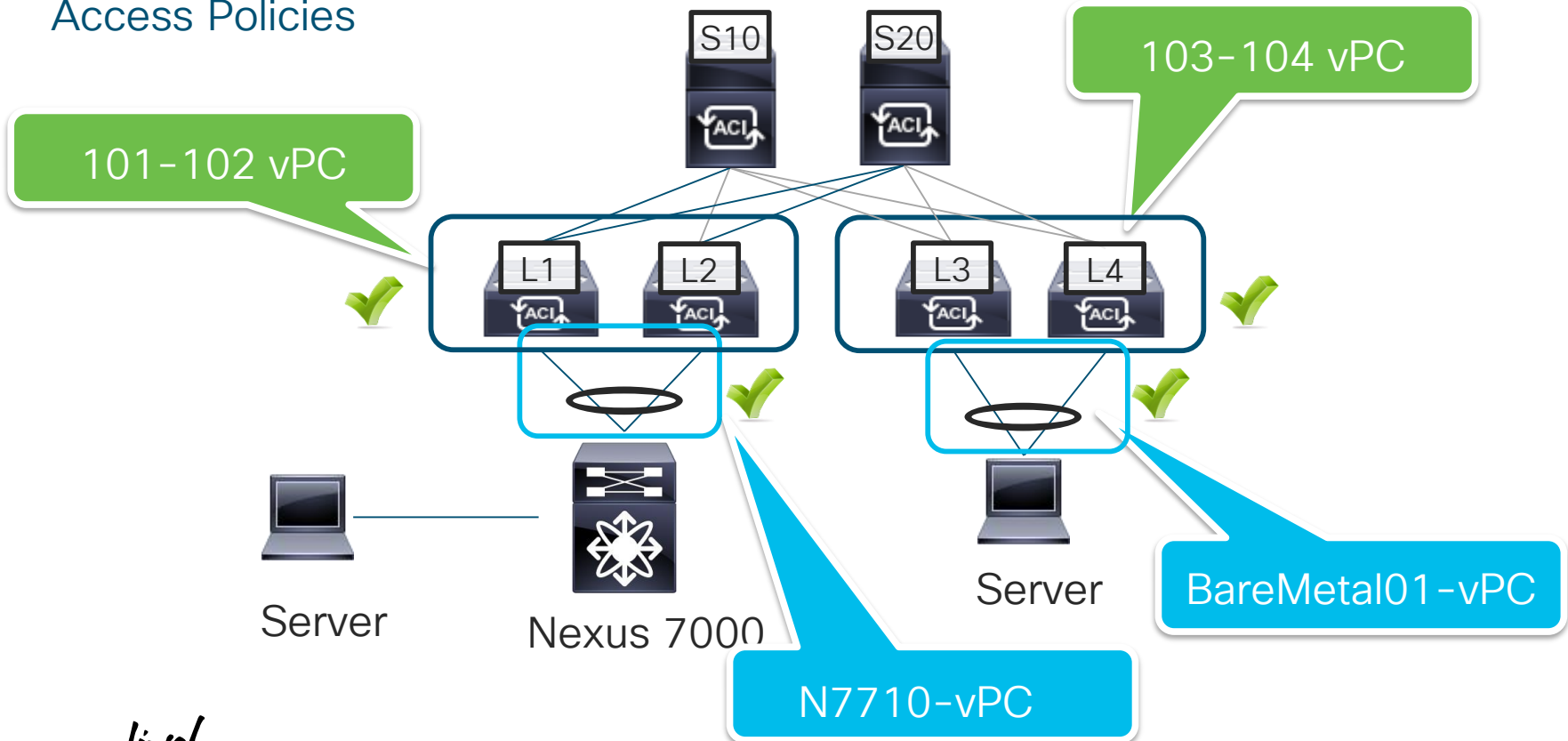
CHECK ALL

UNCHECK ALL

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

Switch Profile

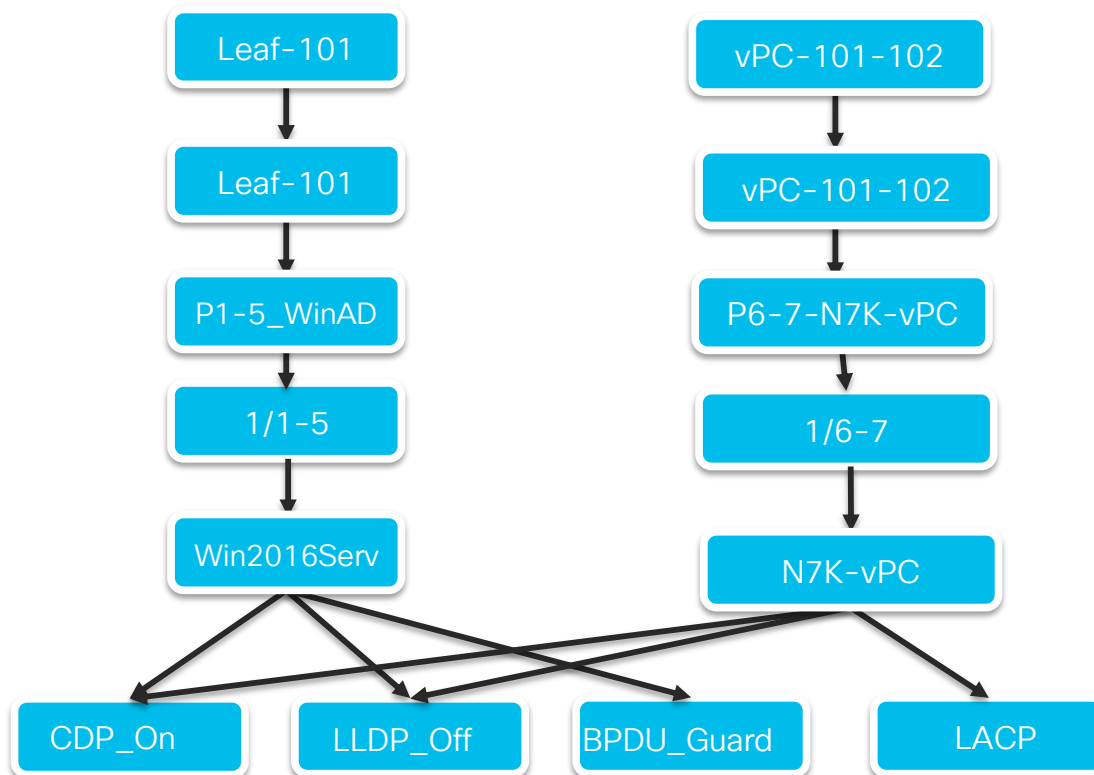
Interface Profile

Interface Selector

Interface Block

Interface Policy Group

Interface Policies





Management - Required Addressing Planning

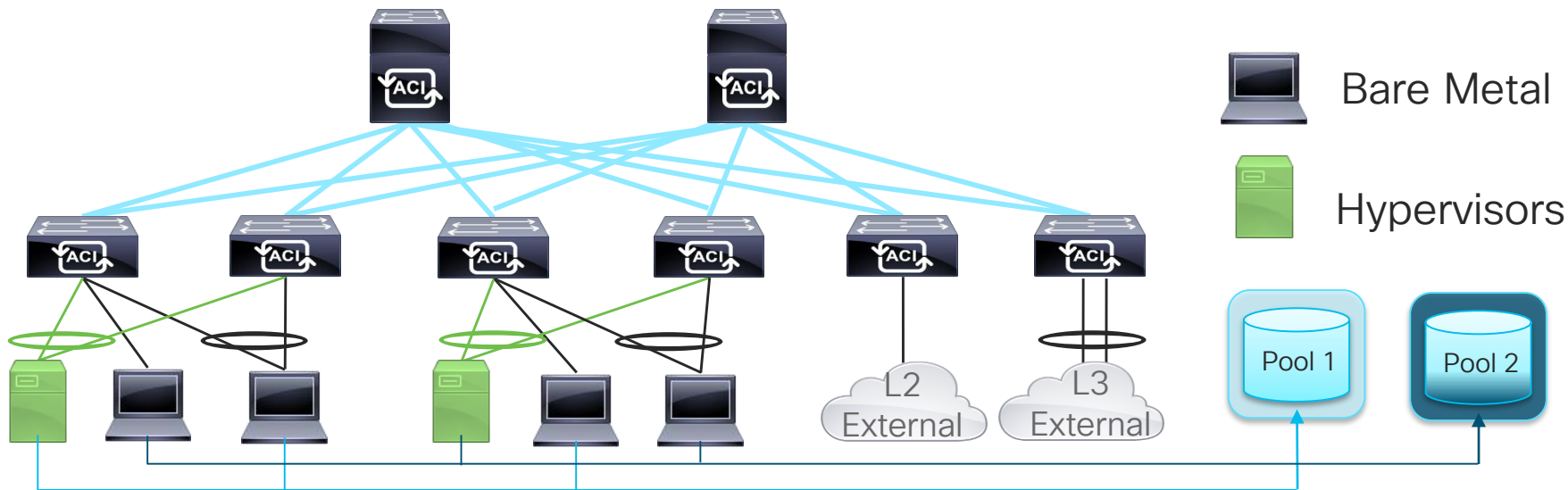
Requirements	Notes	Example
AEP	1 AEP for all Policy groups. Map all domains to this Policy group	Prod_AEP
Domain	1 Physical Domain, 1 External Routed Domain	phys L3Out
VLAN Pool	1 VLAN pool for all statically deployed vlans. 1 VLAN pool for Dynamically deployed VLANs. These pools should not overlap.	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

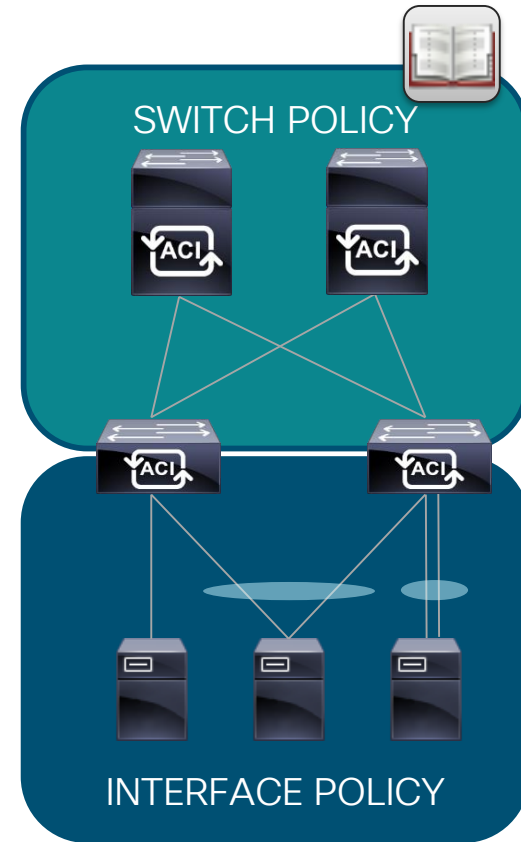
Profiles associate policy groups to switches or interfaces, through the use of selectors

Switch Policy Types:

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

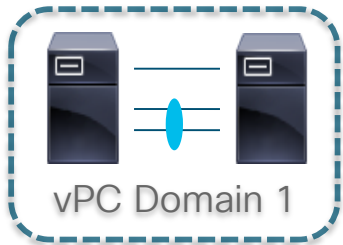
Interface Policy Types:

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





vPC Protection Group Policy

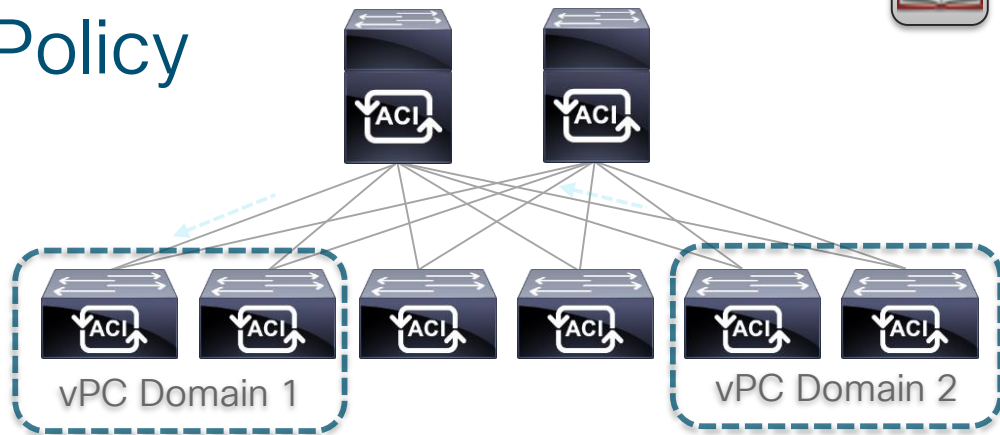


Classical vPC Domain configuration

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

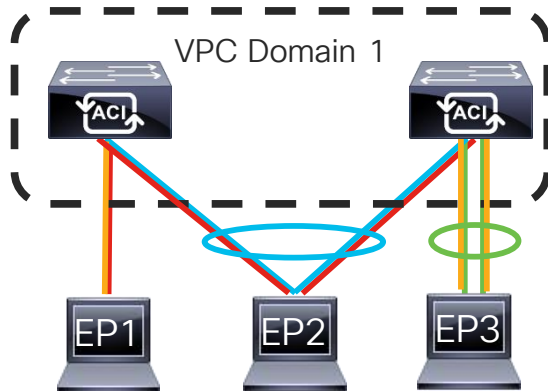


Interface Policies

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

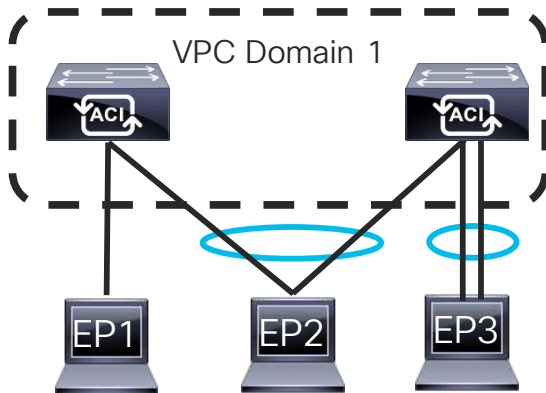
Used to specify which interface policies to be applied to a particular interface type.
It also associates an AEP (which defines which domains are allowed on the interface).

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)

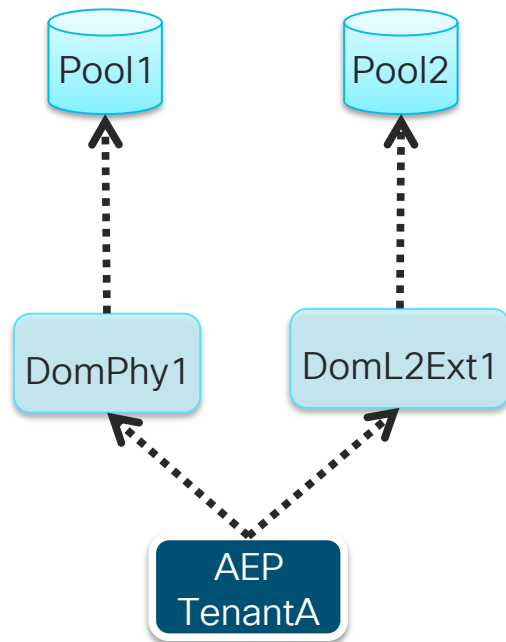
A resource pool of encapsulations that can be allocated within the fabric.

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.





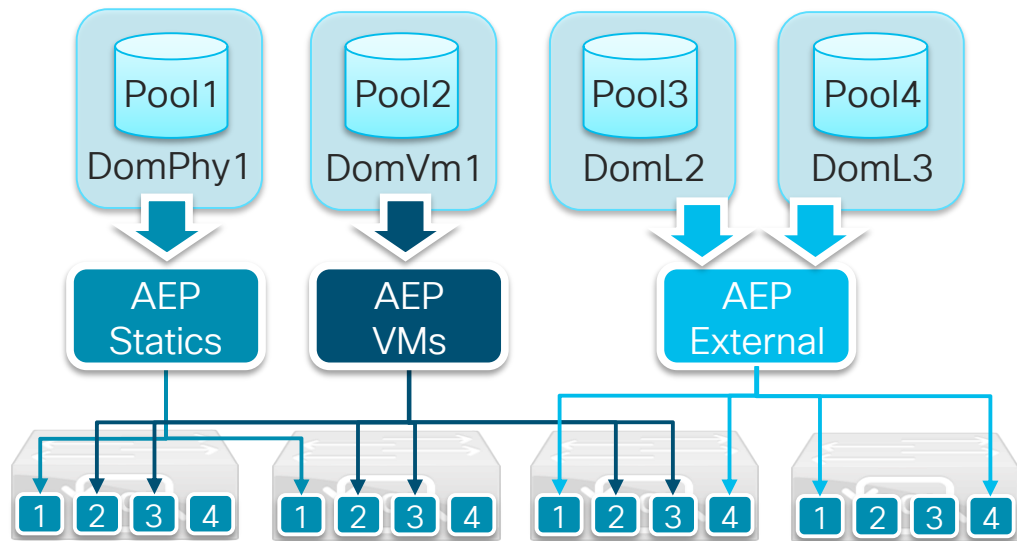
Global Policy - Attachable Entity Profiles

Configuration:

- Create a VLAN/VXLAN **pool** with a range of encapsulations
- Create a **domain** (physical, I2/I3 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

Properties

Name: Mode-On

Description: optional

Alias:

Mode: Static Channel - Mode
Not Applicable for FC PC

Control: Fast Select Hot Standby Ports Graceful Convergence
Suspend Individual Port

Port Channel Policy - LACP-Active

Properties

Name: LACP-Active

Description: optional

Alias:

Mode: LACP Active
Not Applicable for FC PC

Control: Fast Select Hot Standby Ports Graceful Convergence
Suspend Individual Port



Access Policy Example

General Configuration (reused for many interfaces):

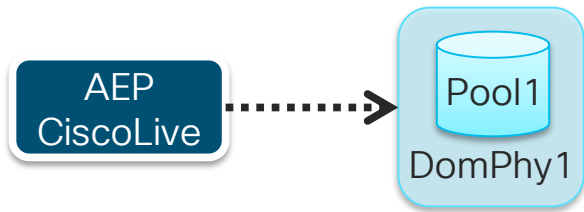
- 1) Configure a physical domain and vlan pool
- 2) Create an AEP and associate physical domain
- 3) Create switch/interfaces profiles for leaf (LEAF101)
 - very easy to apply configurations if you create a switch/interface profile for each leaf and one for each VPC domain pair
- 4) Configure Interface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

LACP Active

Policies

LLDP Rx / Tx enabled

Ciscolive!



Switch Profile

LEAF101

Leaf_101

Interface Profile

LEAF101



Creating Physical Domain / AEP / Vlan Pool



APIC

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

Inventory | Fabric Policies | **Access Policies**

Policies

- > Quick Start
- > Switches
- > Modules
- > Interfaces
- > Policies
- > Pools
- > Physical and External Domains
 - > **Physical Domains**
 - > External Bridged Domains
 - > External Routed Domains
 - > Fibre Channel Domains

Create Physical Domain

Physical Domains

Create Physical Domain

Specify the domain name and the VLAN Pool

Name: DomPhy1
Associated Attachable Entity Profile: select a value
VLAN Pool: default
Security Domains: infra

Create Attachable Entity Profile

In dropdown:
Click Create Attachable Entity Profile

Cancel

Submit

Cisco *live!*



Creating Physical Domain / AEP / Vlan Pool

Create Attachable Access Entity Profile

STEP 1 > Profile

1. Profile2. Association To Interfaces

Specify the name, domains and infrastructure encaps

Name: CiscoLive

Description: optional

Enable Infrastructure VLAN: ☐

EPG DEPLOYMENT (All Selected EPGs will be deployed on all the interfaces associated.)

Application EPGs	Encap	Primary Encap	Mode

Previous

Cancel

Next



Create Attachable Access Entity Profile

STEP 2 > Association To Interfaces

1. Profile2. Association To Interfaces

Select the interfaces

Interface Policy Group	Type	Associated Attachable Access Entity Profile	Switches / Fexes	Interfaces	Select Interfaces
<input checked="" type="checkbox"/> jr-VPC-FIA	VPC	jr-aep			<input type="radio"/> All <input type="radio"/> Specific <input checked="" type="radio"/> None
			101-102	1/9	
<input checked="" type="checkbox"/> jr-scale-vP...	VPC	jr-aep			<input type="radio"/> All <input type="radio"/> Specific <input checked="" type="radio"/> None
			101-102	1/26	
<input checked="" type="checkbox"/> jr-scale-vPC9	VPC	jr-aep			<input type="radio"/> All <input type="radio"/> Specific <input checked="" type="radio"/> None
			101-102	1/25	
<input checked="" type="checkbox"/> jr-scale-vPC4	VPC	jr-aep			<input type="radio"/> All <input type="radio"/> Specific <input checked="" type="radio"/> None

vSwitch Policies: ☒ Inherit (Same as attached physical interfaces)

☐ Specify

Previous

Cancel

Finish



Creating Physical Domain / AEP / Vlan Pool

Create Physical Domain

Specify the domain name and the VLAN Pool

Name: DomPhy1

Associated Attachable Entity Profile: CiscoLive

VLAN Pool: select an option

Security Domains:

Create VLAN Pool

Cancel Submit

In dropdown:
Click Create VLAN Pool



Create VLAN Pool

Specify the Pool identity

Name: Pool1

Description: optional

Allocation Mode: Dynamic Allocation Static Allocation

Encap Blocks:

VLAN Range Allocation Mode Role

Create Ranges

Specify the Encap Block Range

Type: VLAN

Range: VLAN 100 - VLAN 200

Allocation Mode: Dynamic Allocation Inherit allocMode from parent Static Allocation

Role: External or On the network edge Internal

Cancel OK

Click + to add vlan range

Specify start and end vlans in range

Create Interface Profile for each leaf / VPC domain



The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. Below this, a secondary bar shows Inventory, Fabric Policies, and Access Policies. The left sidebar, titled 'Policies', contains a tree view with categories like Quick Start, Switches, Modules, Interfaces, Spine Interfaces, Leaf Interfaces, Profiles, Policy, Override, Policies, Pools, and Physical and External Domains. The 'Leaf Interfaces' section is expanded, and the 'Create Leaf Interface Profile' option is highlighted. A modal dialog box titled 'Create Leaf Interface Profile' is open in the center. It prompts the user to 'Specify the profile identity' with a 'Name' field containing 'LEAF101' and a 'Description' field labeled 'optional'. Below this is an 'Interface Selectors' table with columns for 'Name' and 'Type'. At the bottom of the dialog are 'Cancel' and 'Submit' buttons. A blue callout bubble with the text 'Enter name and submit' points to the 'Name' field.



Create Switch Profile for each leaf / VPC domain

The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The top navigation bar includes tabs for System, Tenants, Fabric (selected), Virtual Networking, L4-L7 Services, Admin, Operations, and Apps. Below this, a secondary bar shows 'Inventory', 'Fabric Policies', and 'Access Policies' (selected).

On the left, the 'Policies' sidebar lists various configuration categories: Quick Start, Switches, Leaf Switches, Profiles (highlighted), Policy Groups, Overrides, Spine Switches, Modules, Interfaces, Policies, and Pools. A 'Create Leaf Profile' button is visible next to the 'Profiles' category.

The main content area is titled 'Leaf Switches - Profiles' and contains a table with the following columns: Name, Leaf Selectors (Switch Policy Group), and Interface Selectors.



Create Switch Profile for each leaf / VPC domain

Create Leaf Profile

STEP 1 > Profile

Specify the profile Identity

Name: LEAF101

Description: optional

Leaf Selectors:

Name	Blocks	Policy Group
LEAF101	101	select an option

Enter name

Click + to add selector

Enter a name and choose appropriate leaf or leaves (for vpc pair)

Update Cancel

Previous Cancel Next



Create Leaf Profile

STEP 2 > Associations

Select the interface/module selector profiles to associate

Interface Selector Profiles:

Select	Name	Description
<input checked="" type="checkbox"/>	LEAF101	

Module Selector Profiles:

Select	Name	Description
--------	------	-------------

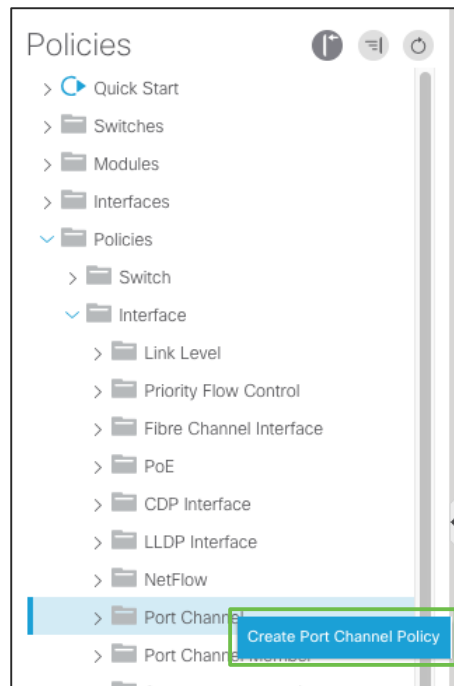
Select the Interface Profile created for this leaf earlier

Previous Cancel Finish



Create common protocol configurations

Example demonstrates a common lacp port-channel policy



Create Port Channel Policy

Specify the Port Channel Policy

Name: Use a descriptive name

Description:

Alias:

Mode: Select the protocol

Control: Configure options/knobs

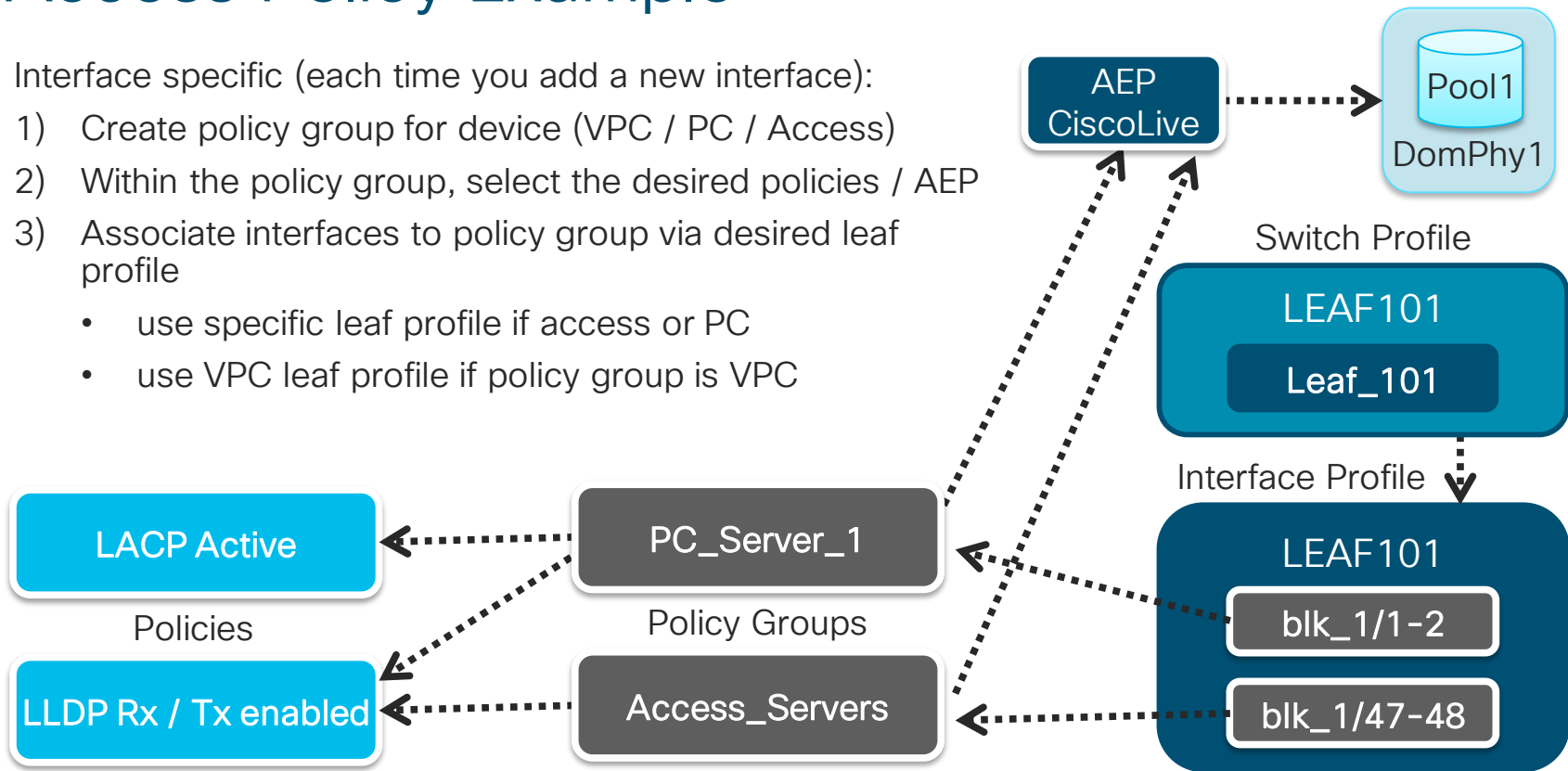
Cancel Submit



Access Policy Example

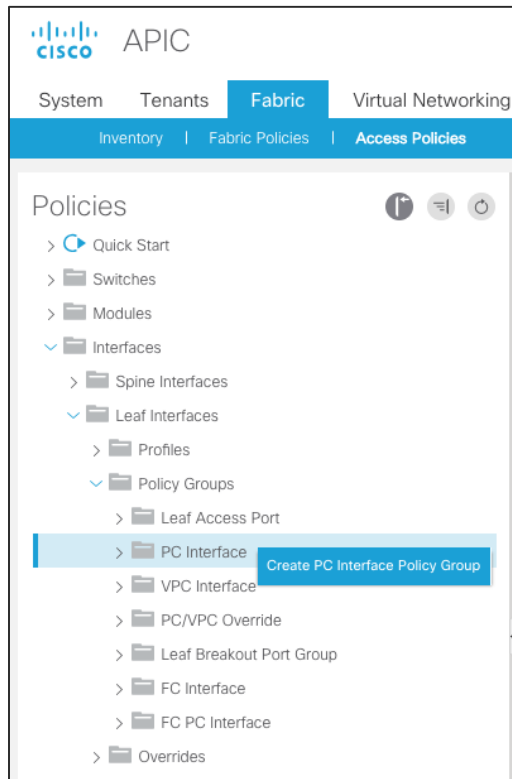
Interface specific (each time you add a new interface):

- 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



Create PC Interface Policy Group

Specify the Policy Group identity

Name: Descriptive name

Description: optional

Link Level Policy:

CDP Policy:

MCP Policy:

CoPP Policy:

LLDP Policy: Associate your desired interface policies (otherwise default)

STP Interface Policy:

Port Channel Policy: Associate your AEP to select which domains this interface can deploy

Attached Entity Profile:

Connectivity Filters:

Monitoring Policy:

Storm Control Interface Policy:

L2 Interface Policy:

Port Security Policy:

Egress Data Plane Policing Policy:

Ingress Data Plane Policing Policy:

Priority Flow Control Policy:

Fibre Channel Interface Policy:

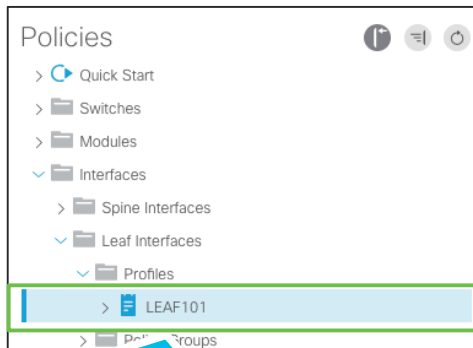
Slow Drain Policy:

Cancel Submit

Note:

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

Create interface selectors / associate policy group



Choose interface profile to add selectors

Leaf Interface Profile - LEAF101

Policy Faults History

Create Access Port Selector

Specify the selector identity

Name: PC_Server_1

Description: optional

Interface IDs: 1/1-2

Valid values: All or Ranges: 1/13, 1/15 or 2/22-23, 1/21-23/1-4, 1/24/1-2

Connected To Fex: ☐

Interface Policy Group: PC_Server_1

Click + to add selector

Use a descriptive name

Specify interface/range

Associate the policy group to deploy on interfaces

Cancel Submit



Example policy scheme

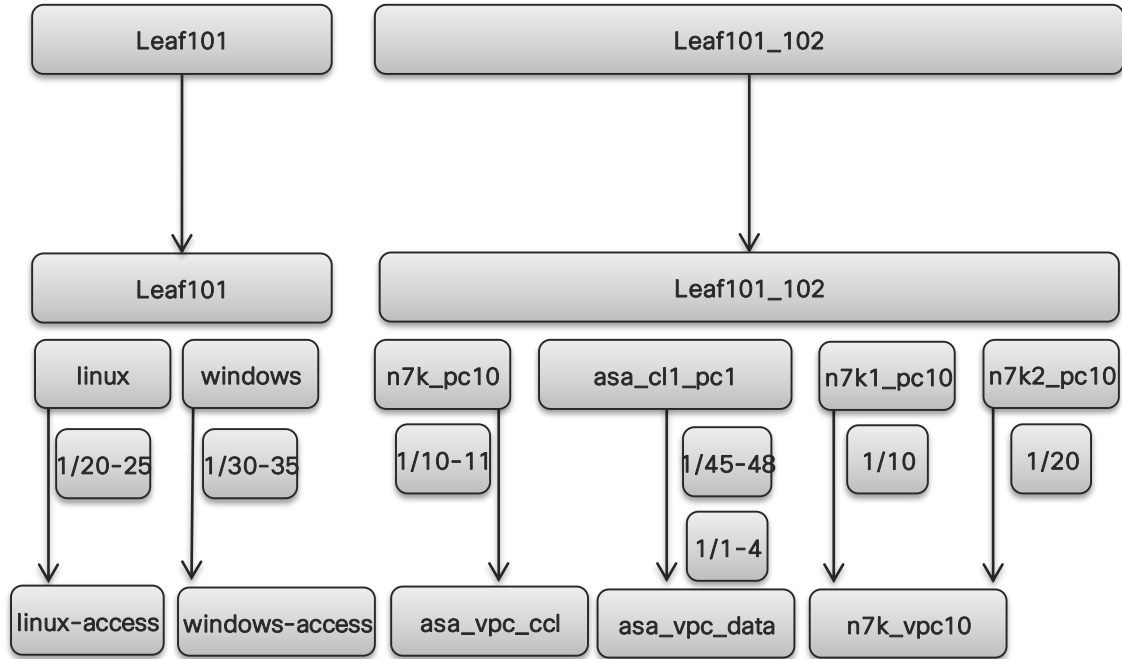
Switch Profile

Interface Profile

Interface Selector

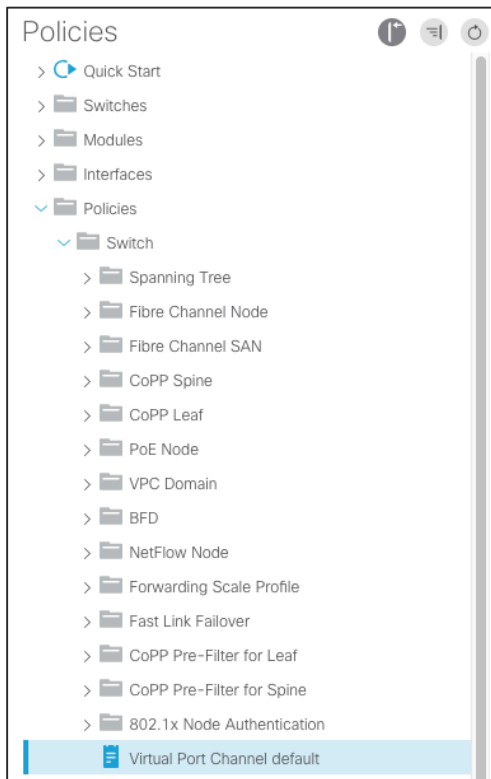
Interface Block

Interface Policy Group





VPC Protection Group (example configuration)



Create VPC Explicit Protection Group

Specify the Explicit Group settings

Name:

ID:

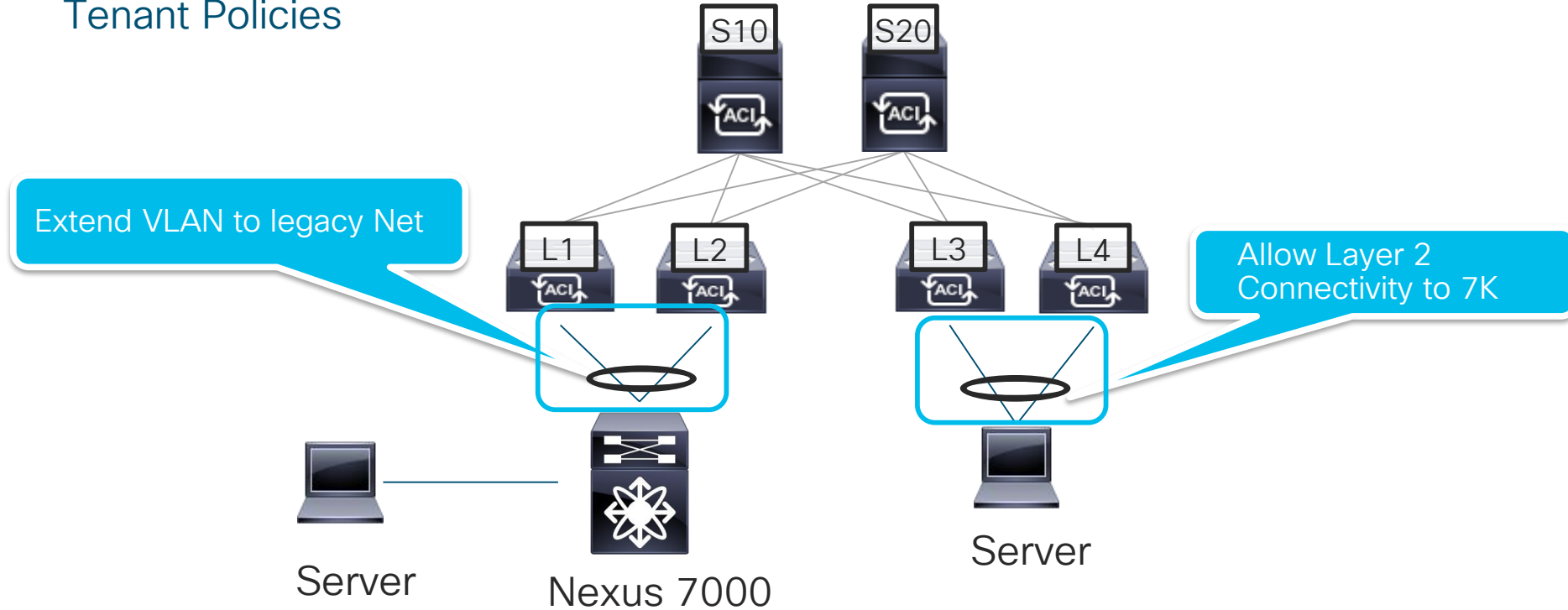
VPC Domain Policy:

Switch 1:

Switch 2:

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**

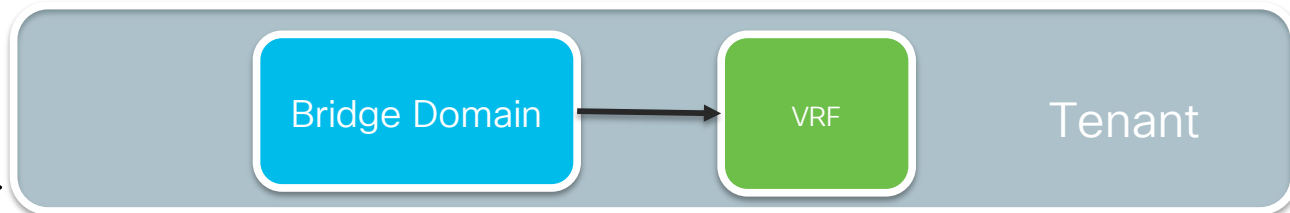
VRFs are used to separate **routing** tables inside the ACI Fabric. 1 or more **VRFs** can be used.

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

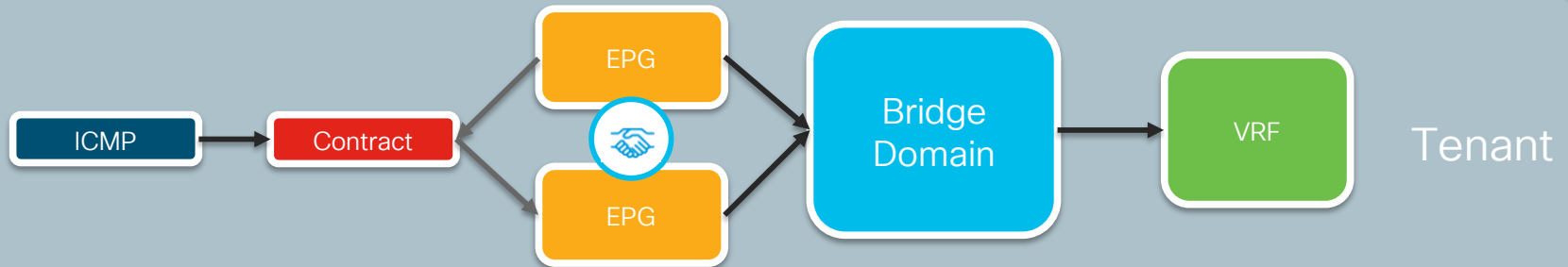
L4-L7 policies (PBR, Load balancing, Firewalls)

EPG is most commonly determined by ingress **VLAN & Port**

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

Contracts 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

The screenshot shows the Cisco Tenant View interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Apps. The 'Tenants' tab is active, showing a search bar and a list of tenants. The left sidebar displays a tree view of the tenant configuration, with categories like Application Profiles, Networking, and Security Policies. Four callout boxes highlight specific features: EPGs (Application Profiles), Bridge Domains (Networking), VRFs (Networking), and Contracts (Security Policies). The main content area shows a 'Quick Start' guide for creating a tenant, with steps like 'Create a security domain for the tenant administrator', 'Create a tenant (SCVMM)', 'Create a tenant and VRF', 'Create the tenant with IPv6 Neighbor Discovery', 'Create a filter for the contract', 'Create a contract', 'Create an application profile for this tenant', 'While creating the application profile, create the necessary EPGs', 'While creating the application profile, specify the necessary VRFs', and 'Create an external routed network (L3 Out) for a tenant'. A 'See Also' section on the right lists related topics like Application Profiles, Bridge Domains, VRFs, Contracts and Filters, External Bridged Networks (L2 Outside), External Router Networks (L3 Outside), SPAN, L4-L7 Services, and Atomic Counters.

EPGs

Bridge Domains

VRFs

Contracts

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:


Alias:


Description:

Type: ☐ ☒

VRF: 

Forwarding: 

End Point Retention Policy: 
This policy only applies to local L2 L3 and remote L3 entries

IGMP Snoop Policy: 

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
```

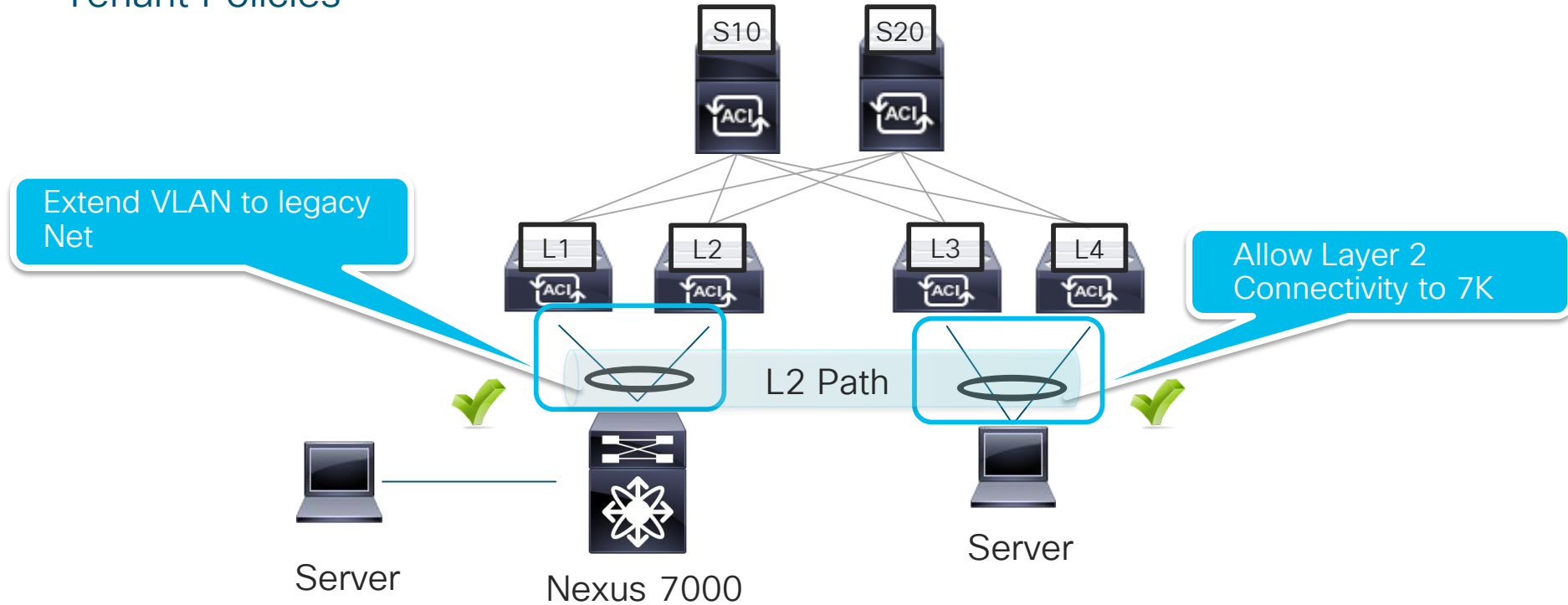
The screenshot displays the Tenant CiscoLive web interface. On the left, a navigation pane shows a tree structure under 'Tenant CiscoLive'. The 'Static Ports' folder is highlighted with a blue box, and within it, the path 'Pod-1/Node-101-102/N7710-vPC' is selected. The main panel on the right is titled 'Static Path - Pod-1/Node-101-102/N7710-vPC'. It shows the 'Properties' section with the following configuration:

- Path: **Pod-1/Node-101-102/N7710-vPC**
- Encap: **VLAN** (dropdown), 100 (Integer Value)
- Egress Encap: **VLAN** (dropdown), (Integer Value)
- Deployment Immediacy: **Immediate** (selected), On Demand
- Mode: **Trunk** (selected), Access (802.1P), Access (Untagged)

Below the properties, there is a section for 'IGMP Snoop Static Group' with a table for 'Group Address' and 'Source Address'. A message at the bottom states: 'No items have been found. Select Actions to create a new item.'

Fabric and Tenant Policies

Tenant Policies



Fabric and Tenant Policies

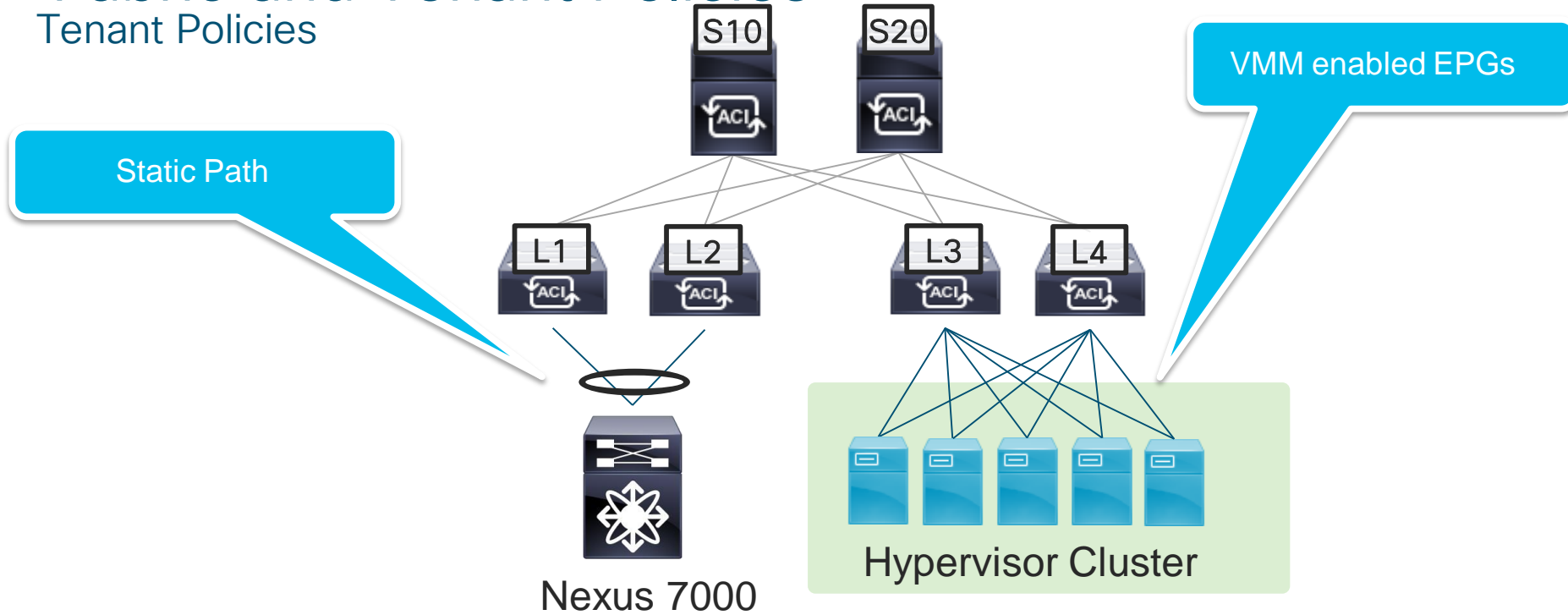
Planning



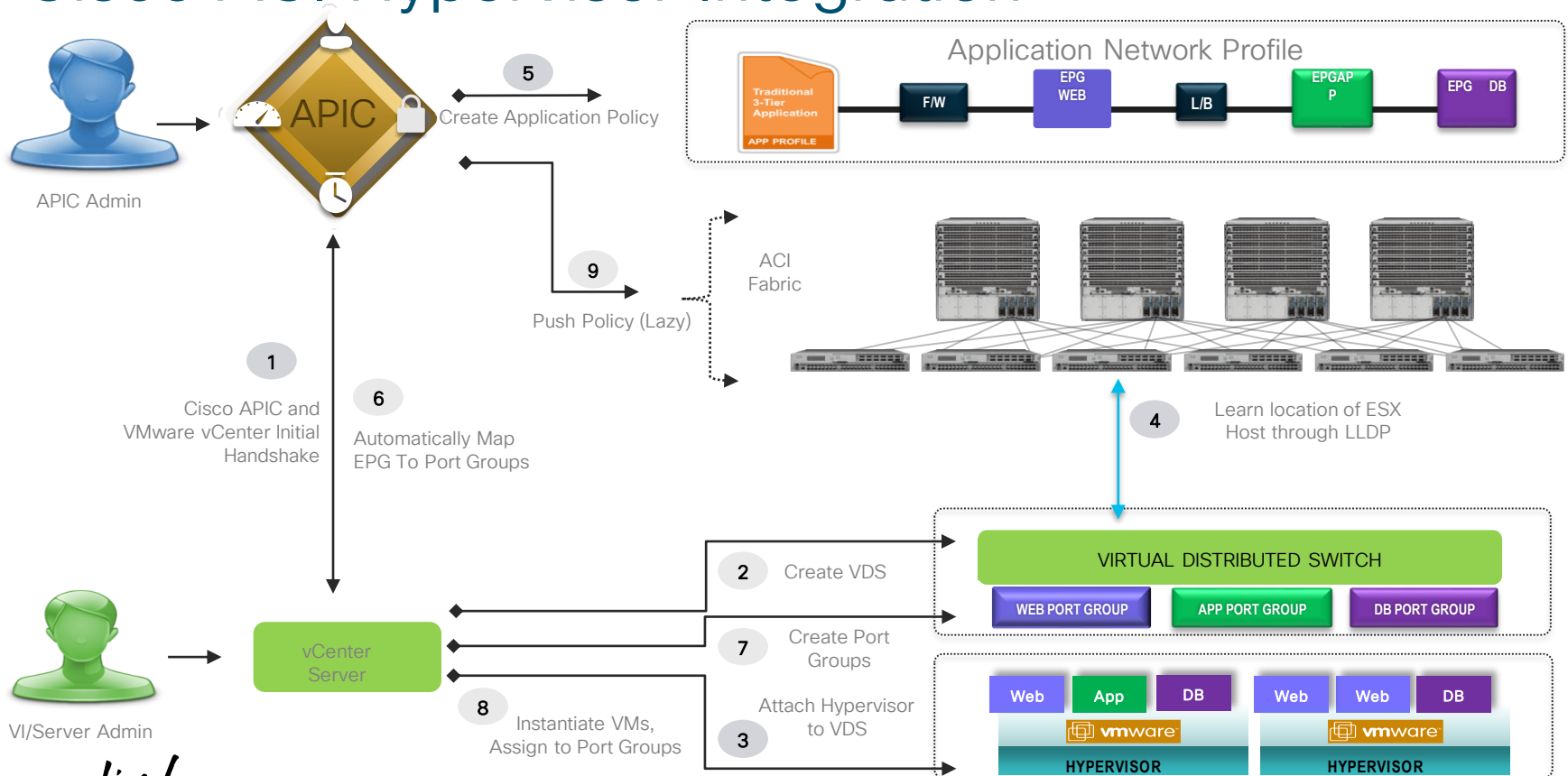
Requirements	Notes	Example
Tenant	1 Tenant can be used company. Tenants can also separate functions of a business. NOTE: Shorter names are easier when using CLI	Prod/Dev
VRF	1 or more VRFs per Tenant	PROD-MAIN DEV-TEST,DEV-PROD
Bridge Domain	Recommended to have 1 BD per Legacy VLAN. For Network Centric 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

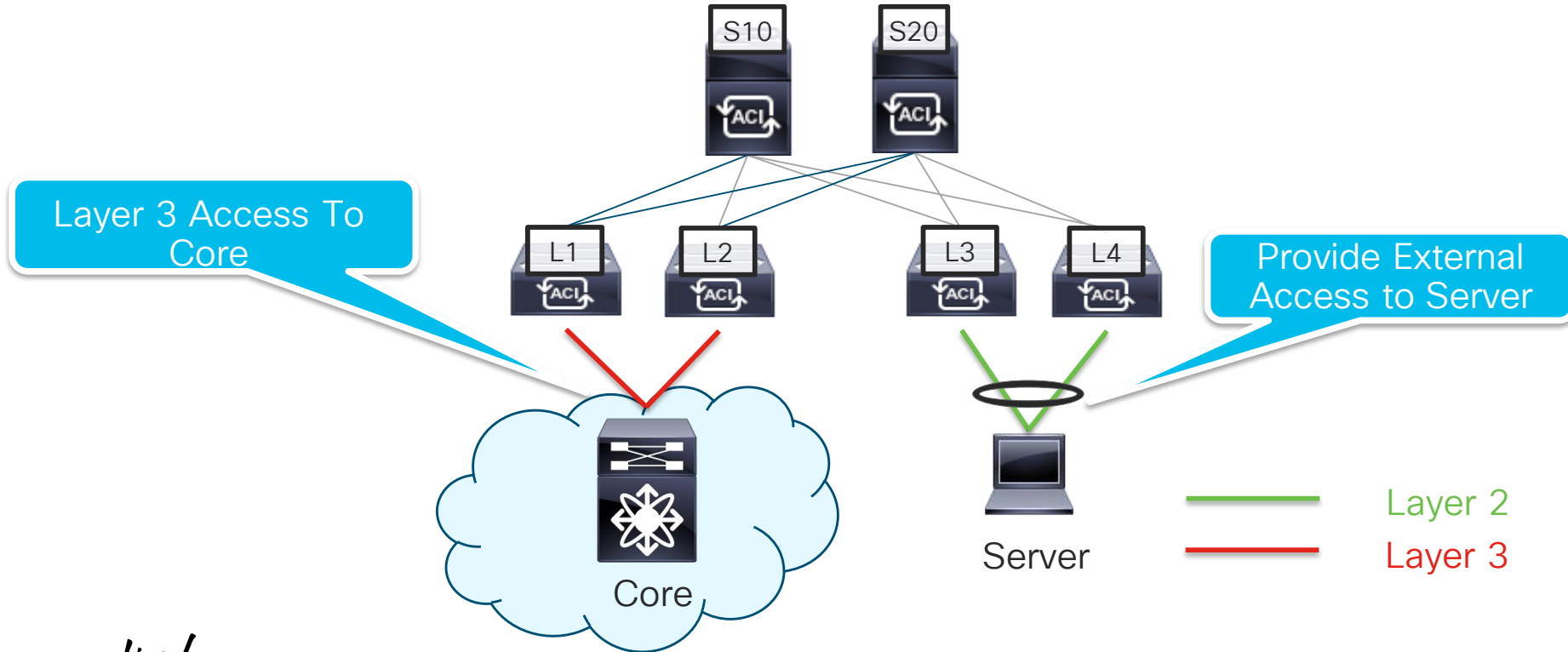


Cisco ACI Hypervisor Integration

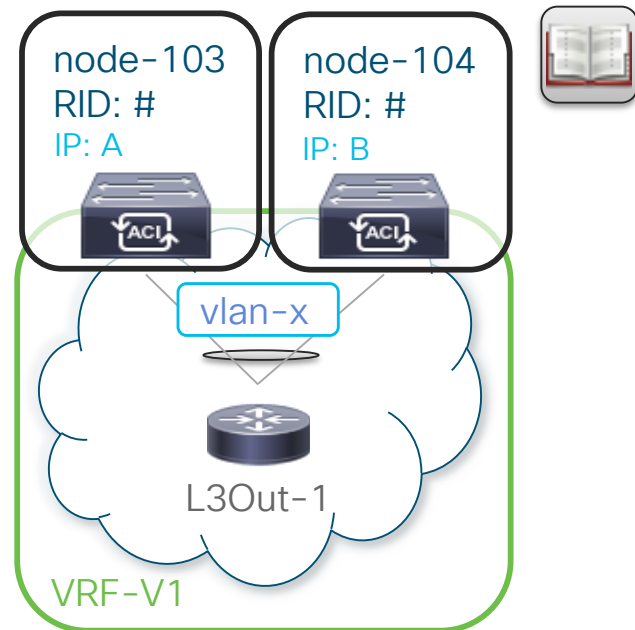
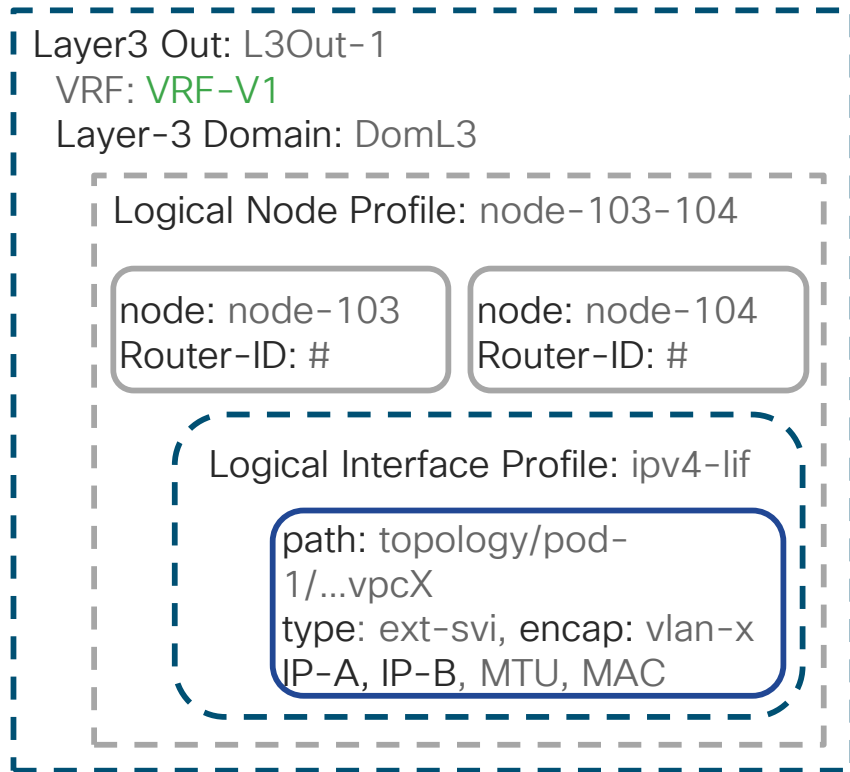


Fabric and Tenant Policies

Layer 3 Connectivity



Basic Connectivity

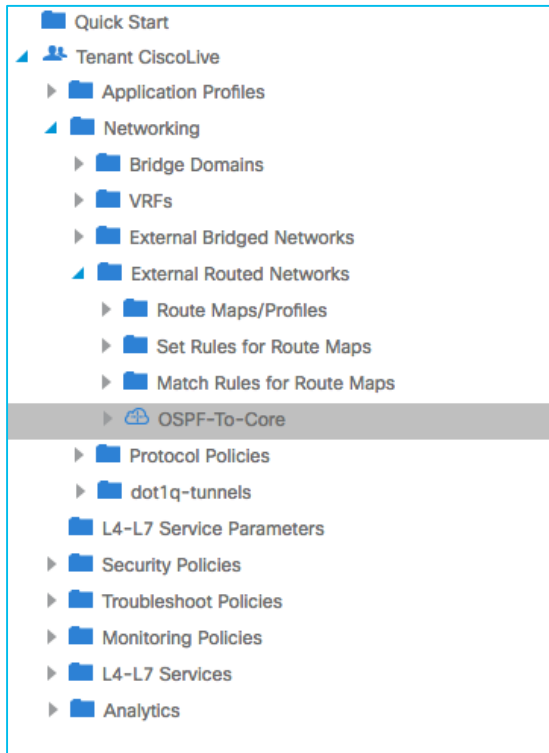


Create the L3Out

- 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



Properties

Name: **OSPF-To-Core**

Alias:

Description:

Tags:

Global Alias:

Provider Label:

Consumer Label:

Target DSCP: **Unspecified**

PIM: ☐

Route Control Enforcement: ☐ Import ☒ Export

VRF: **CiscoLive/VRF1**

Resolved VRF: **CiscoLive/VRF1**

External Routed Domain: **L3Out-Domain**

Route Profile for Interleak:

Route Control For Dampening:

☐ Address Family Type

Enable BGP/EIGRP/OSPF: ☐ BGP ☒ OSPF ☐ EIGRP

OSPF Area ID: **0.0.0.1**

OSPF Area Control: ☐ Send redistributed LSAs into NSSA area ☐ Originate summary LSA ☐ Suppress forwarding address in translation

OSPF Area Type: **NSSA area** **Regular area**

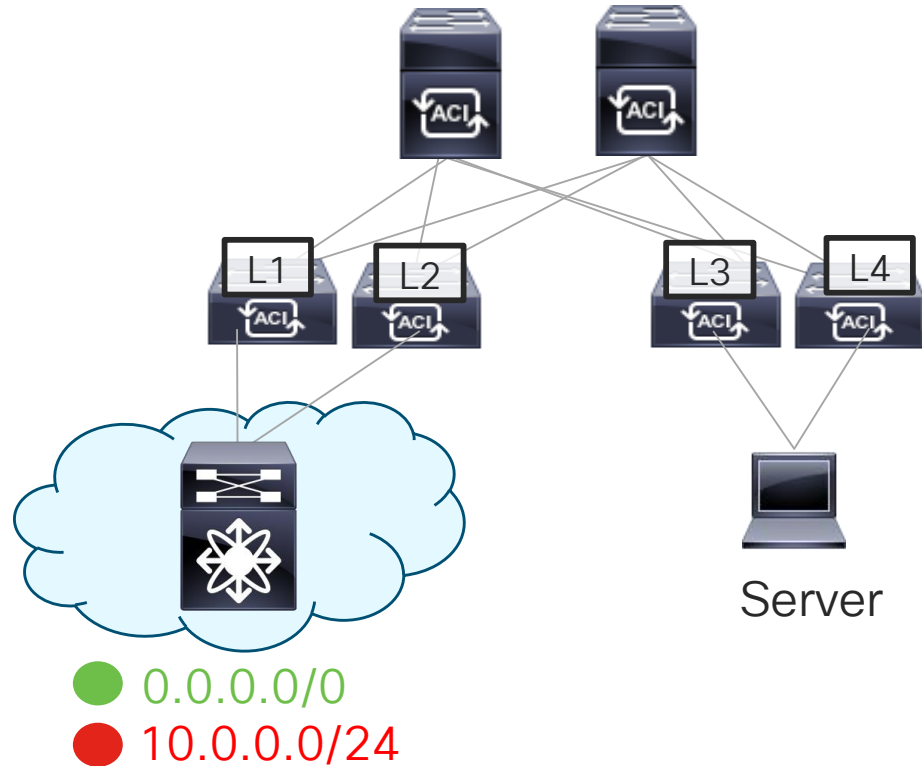
OSPF Area Cost: **1**

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

Fabric and Tenant Policies

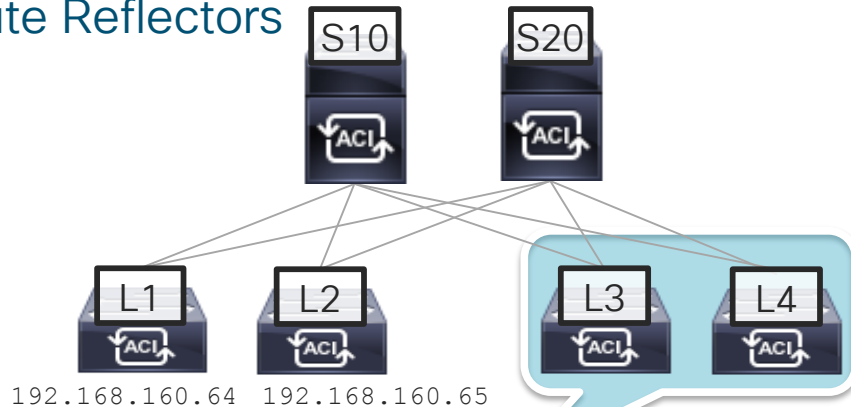
Route Reflectors

- 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
```

BGP Route Reflector Policy - BGP Route Reflector default



Properties

Name: **default**

Description: optional

Autonomous System Number: 90002

Route Reflector Nodes:

Node ID	Node Name
201	calo2-spine1
202	calo2-spine2

Fabric and Tenant Policies

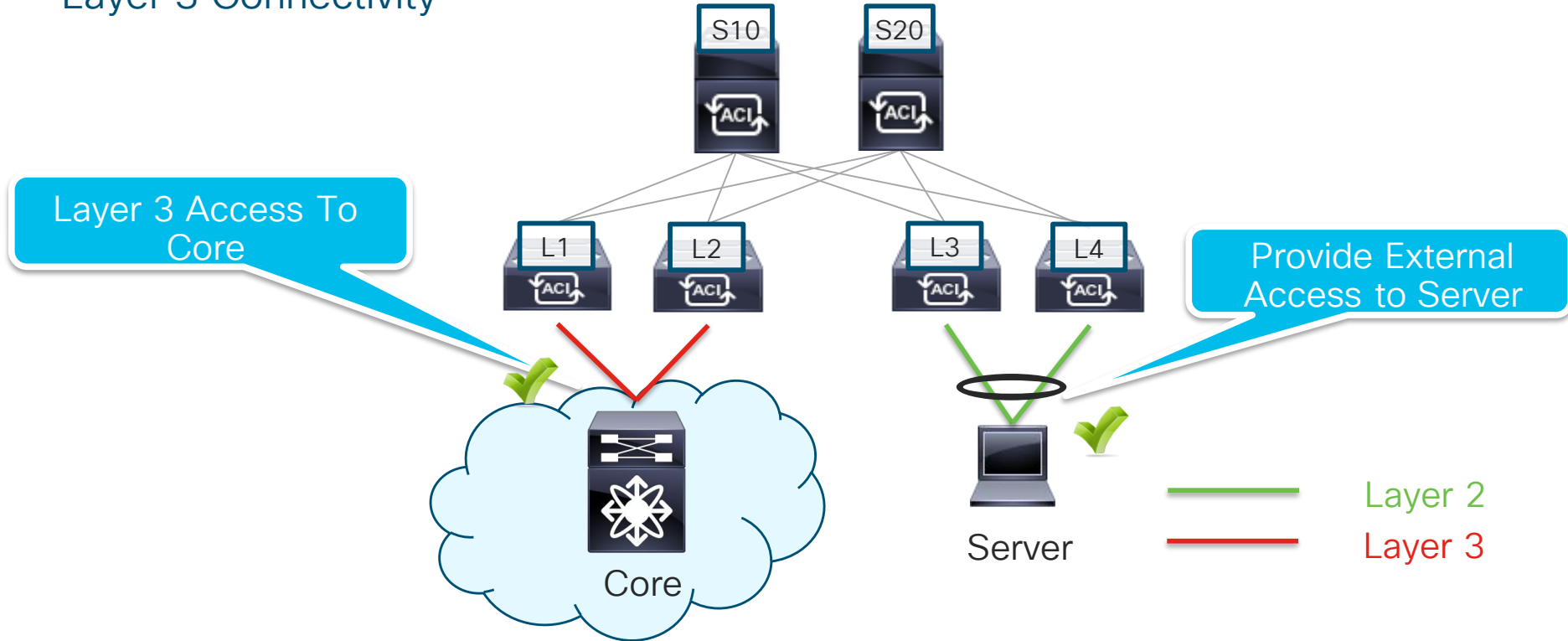
Planning



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?

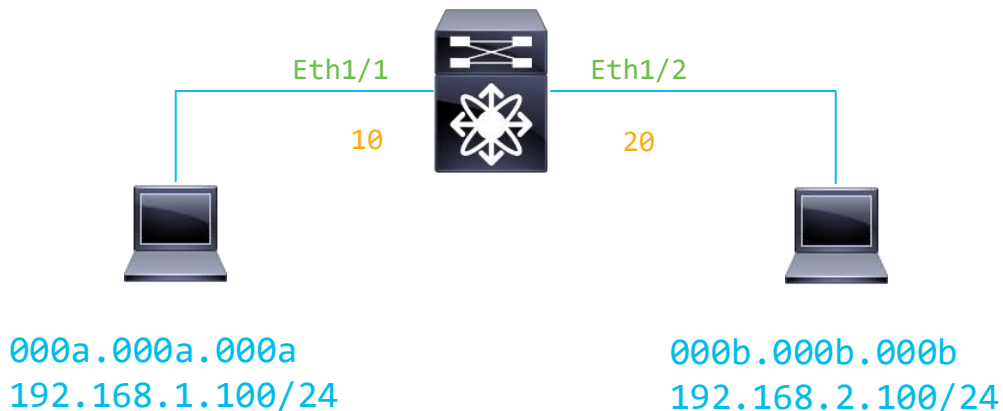
Traditional Endpoint

L2 – MAC Table

- MAC Address
- VLAN
- Interface

L3 – ARP Table

- IP / MAC
- Interface
- VRF



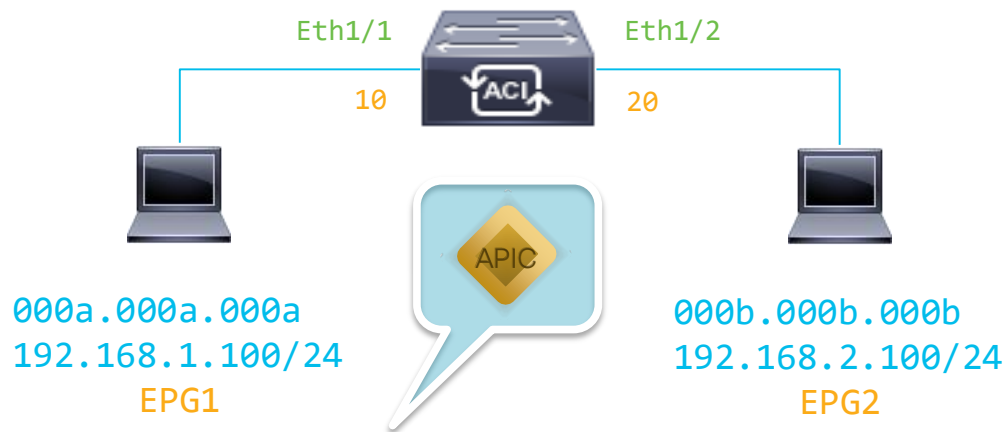
```
N5K# show ip arp vrf default | grep 000a
192.168.1.1    00:00:01 000a.000a.000a  Vlan10
N5K# show mac address-table | grep 000a
10          000a.000a.000a    dynamic  0    Eth1/1
```

```
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:

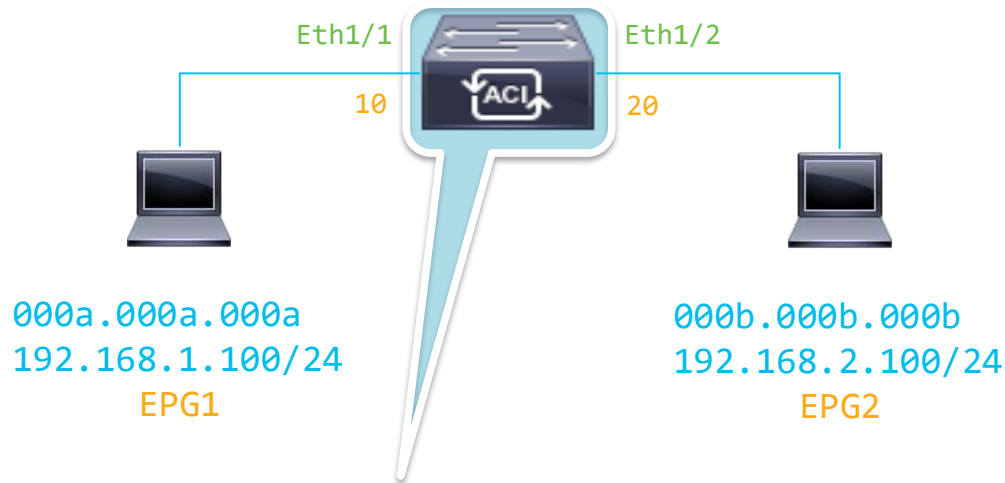
Tenant : CL
Application : CL
AEPg : EPG1

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:

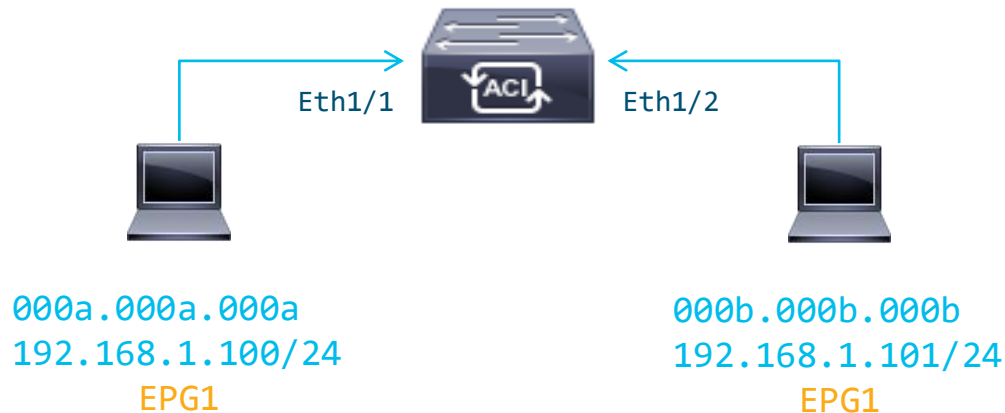
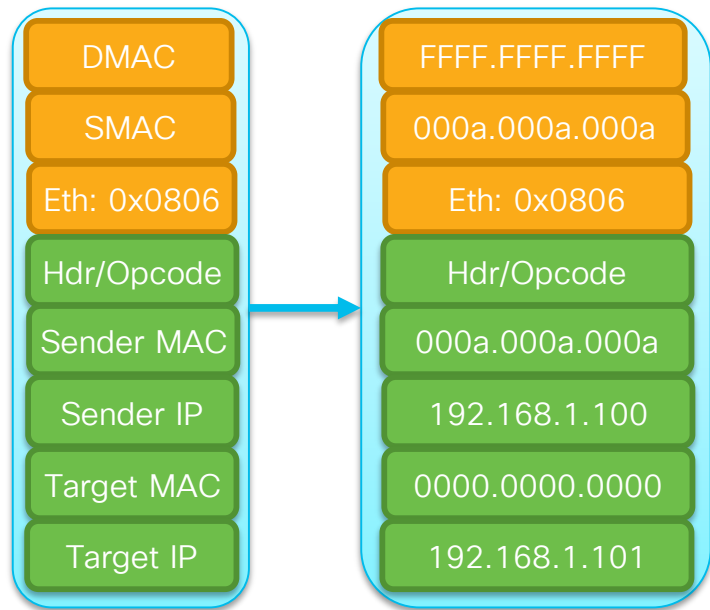
s - arp	O - peer-attached	a - local-aged	S - static
V - vpc-attached	p - peer-aged	M - span	L - local
B - bounce	H - vtep		

VLAN/ Domain	Encap VLAN	MAC Address IP Address	MAC Info/ IP Info	Interface	Endpoint Group 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!

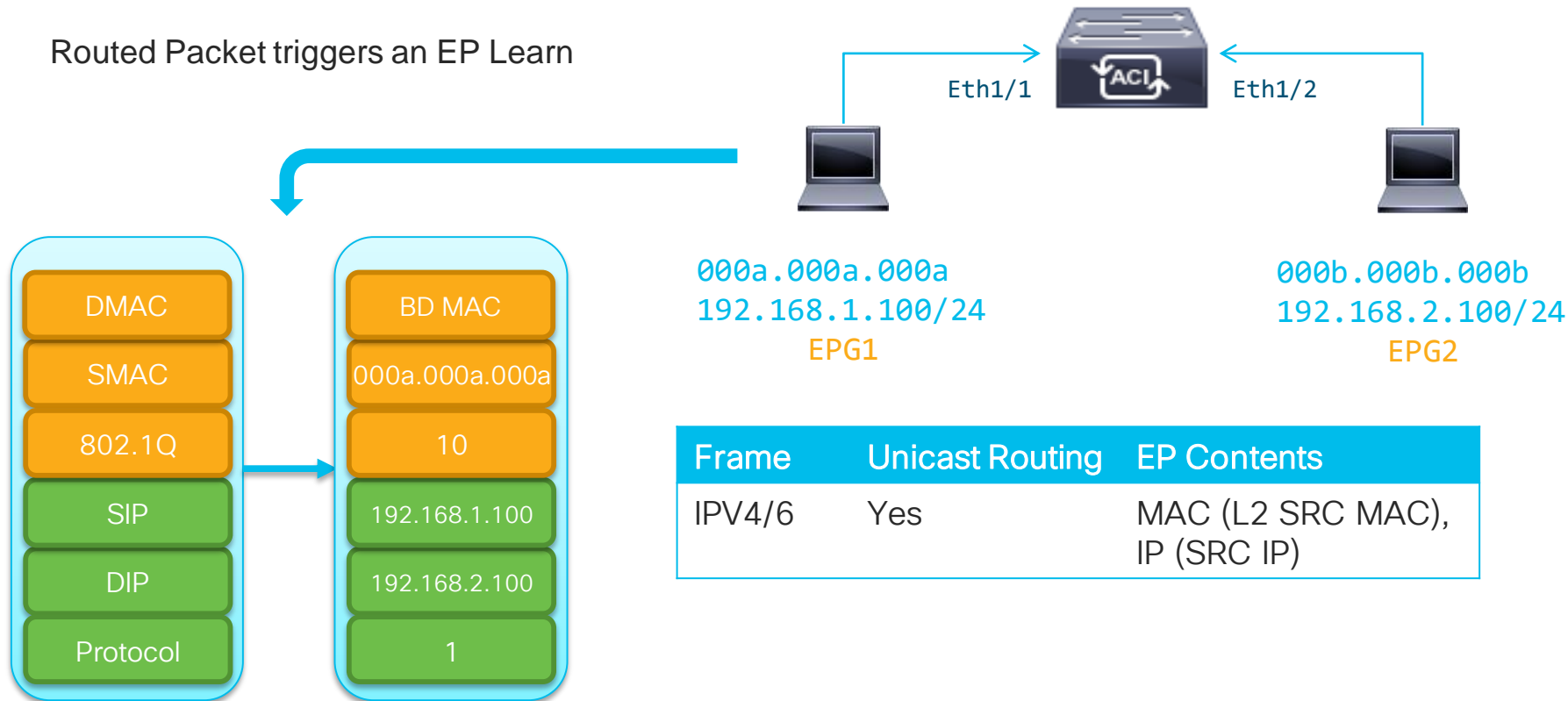
ARP Request



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

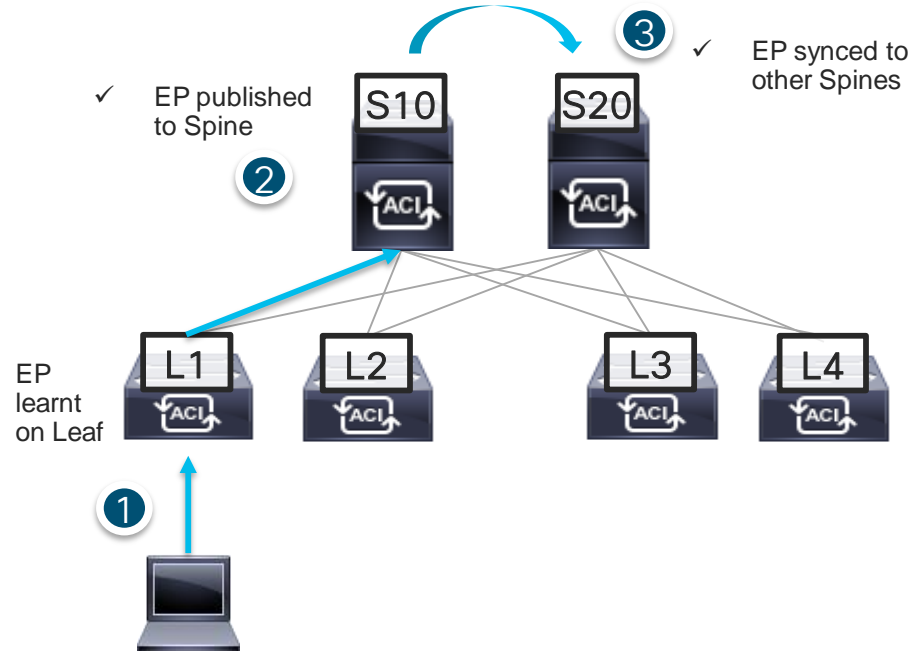
Endpoint Learning- Routed Packets

Routed Packet triggers an EP Learn



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

Properties

Unicast Routing: ☒

Operational Value for Unicast Routing: true

Properties

Name: BD1

Alias:

Description: optional

Type: ☐ regular

Global Alias:

Legacy Mode: No

VRF: CiscoLive2017/VRF1

Resolved VRF: CiscoLive2017/VRF1

L2 Unknown Unicast: ☐ Flood ☒ Hardware Proxy

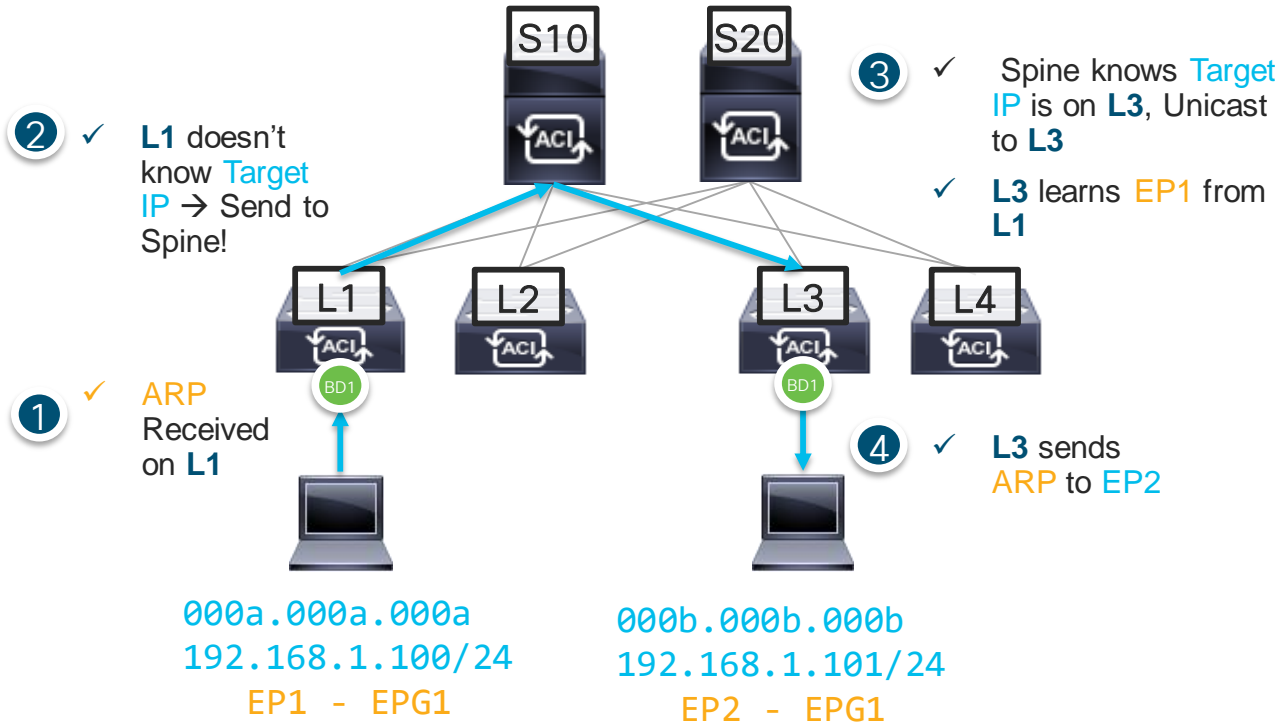
L3 Unknown Multicast Flooding: ☒ Flood ☐ Optimized Flood

Multi Destination Flooding: ☒ Flood in BD ☐ Drop ☐ Flood in Encapsulation

PIM: ☐

IGMP Policy: select an option

ARP Flooding: ☐



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

Properties

Name: **BD1**
Alias:
Description:

Type: **fc** **regular**

Global Alias:

Legacy Mode: **No**
VRF: **CiscoLive2017/VRF1**

Resolved VRF: **CiscoLive2017/VRF1**

L2 Unknown Unicast: **Flood** **Hardware Proxy**

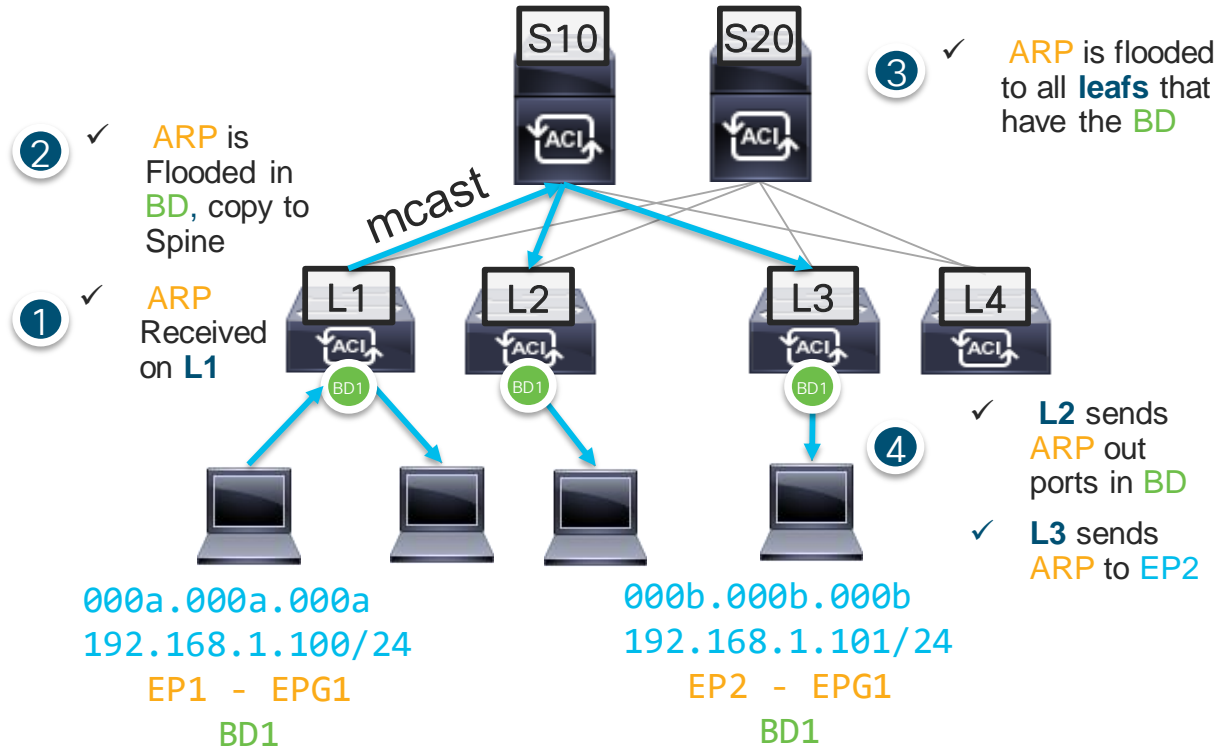
L3 Unknown Multicast Flooding: **Flood** **Optimized Flood**

Multi Destination Flooding: **Flood in BD** **Drop** **Flood in Encapsulation**

PIM: ☐

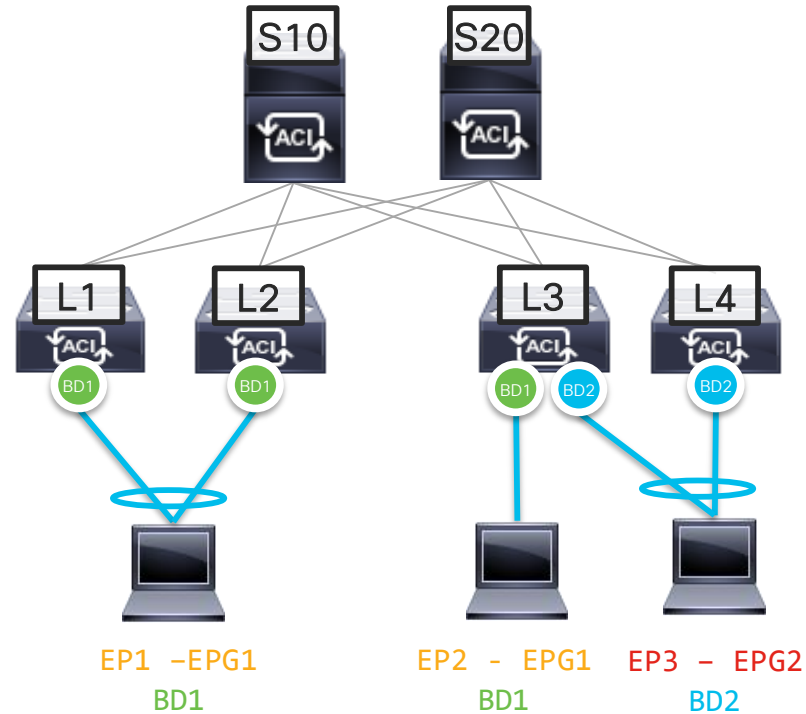
IGMP Policy: **select an option**

ARP Flooding: ☒



Anycast Gateway

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



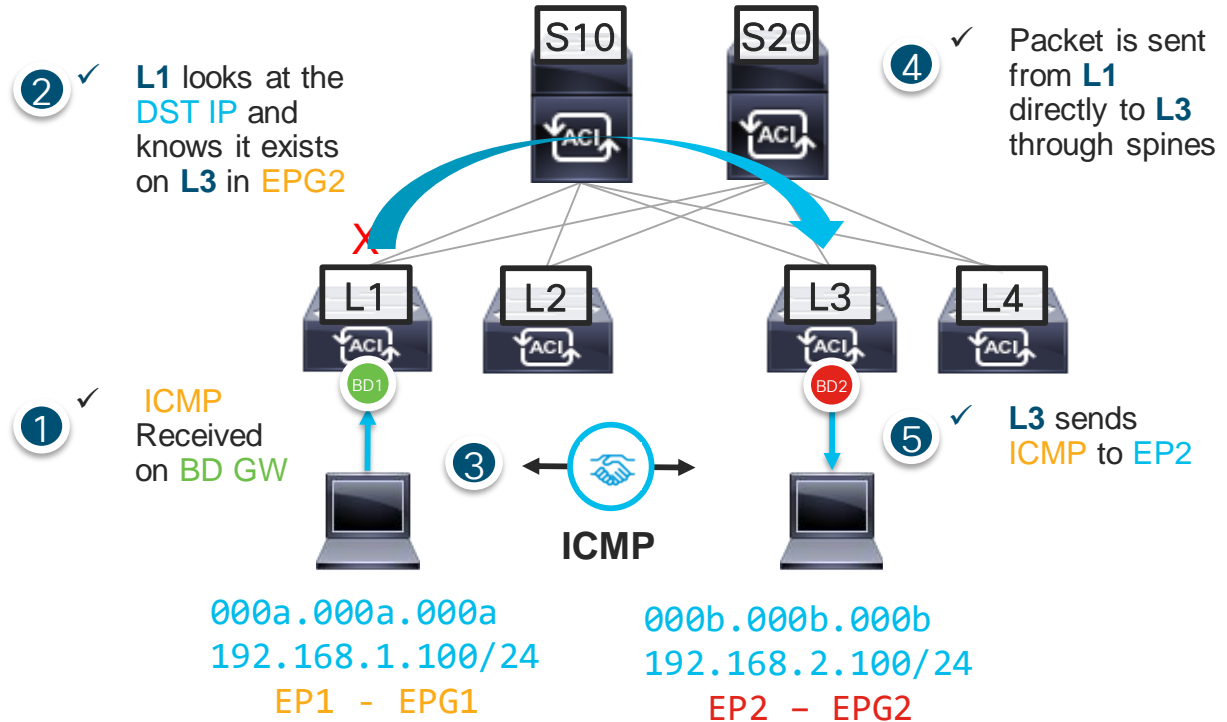
EP1 pings EP2



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

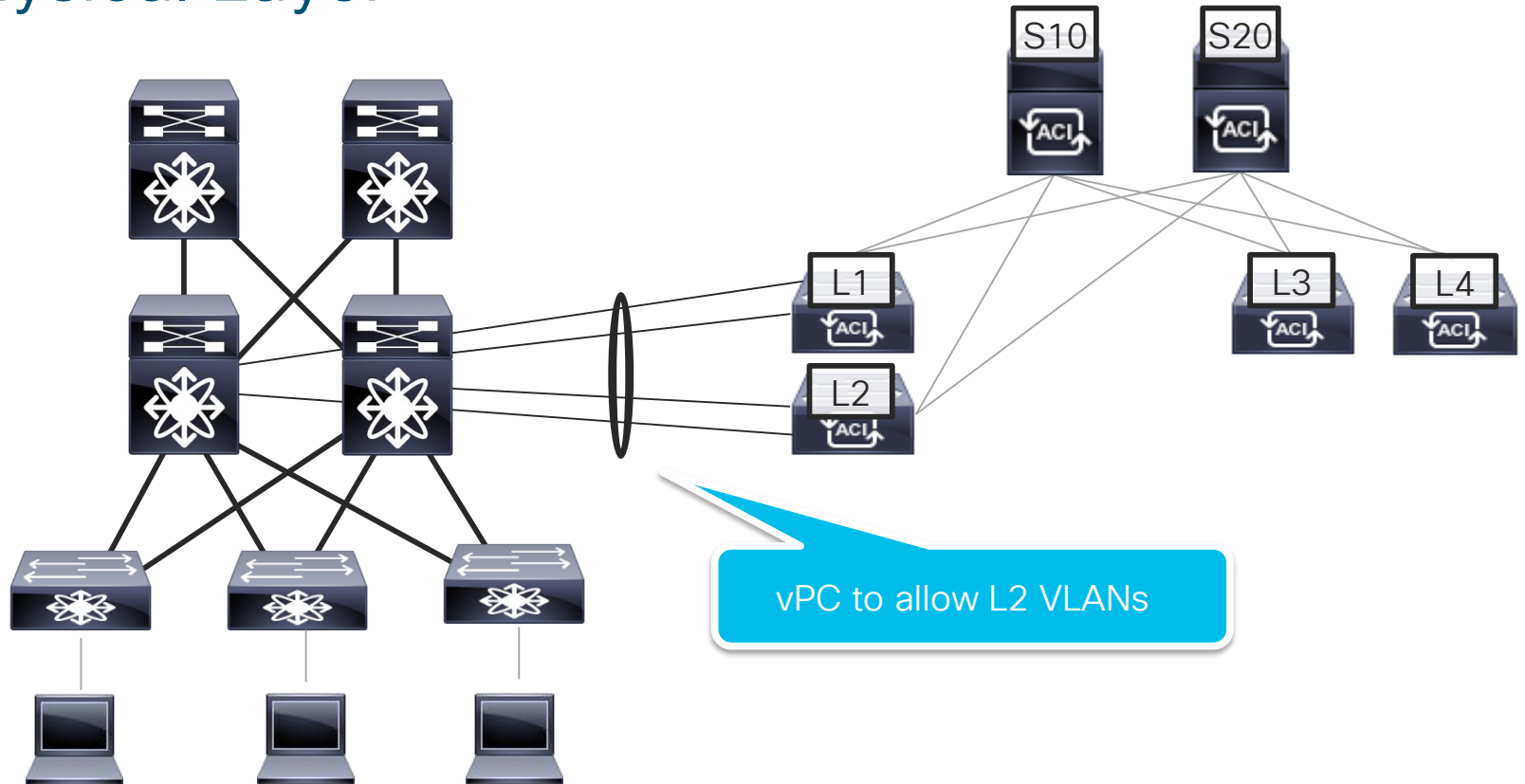
- Day 1: Why ACI?
- Day 2: Infrastructure and Policies
- Day 3: Forwarding Overview
- Day 4: Network Centric Migrations
- Day 5: Multi Location Deployments
- Day 6: Troubleshooting Tools
- Day 7: Additional Resources

Day 4: Network Centric Migrations



You make networking **possible**

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

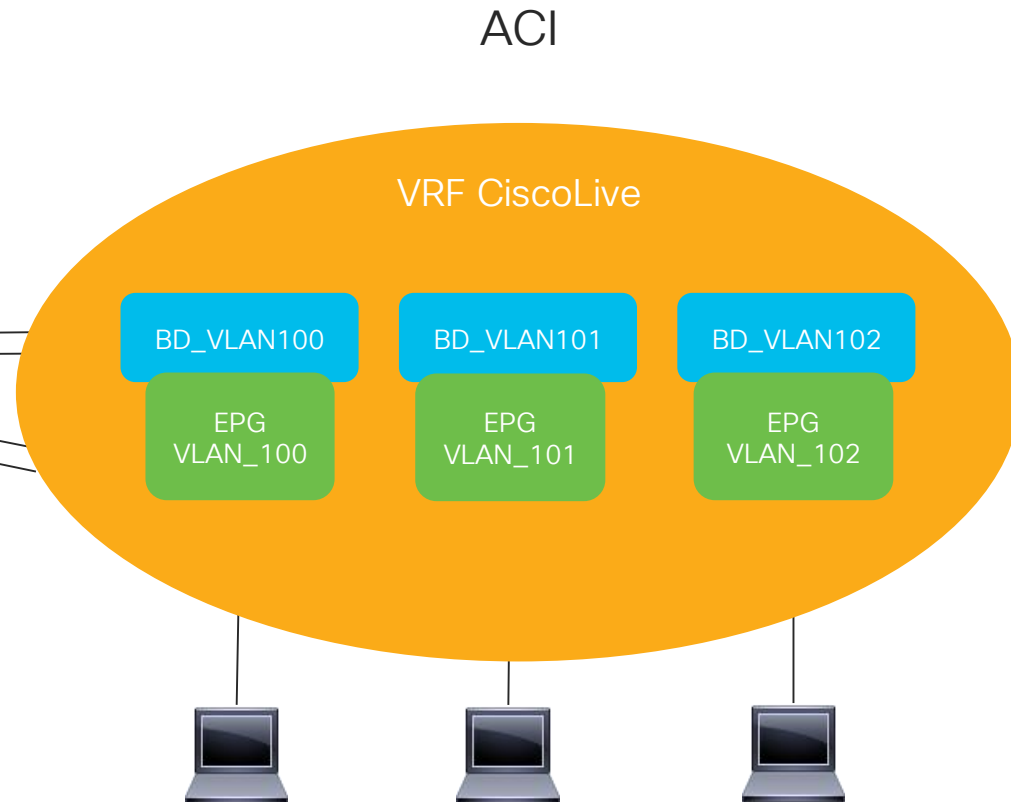
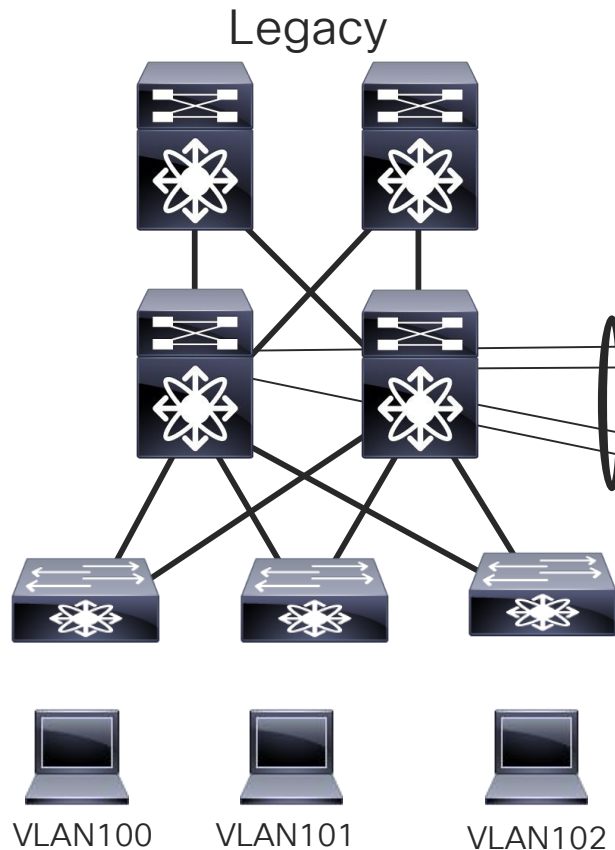
Each Legacy **VLAN** has a unique **EPG**

What have we Accomplished?

Each Legacy **VLAN** maps to a unique **Bridge Domain**

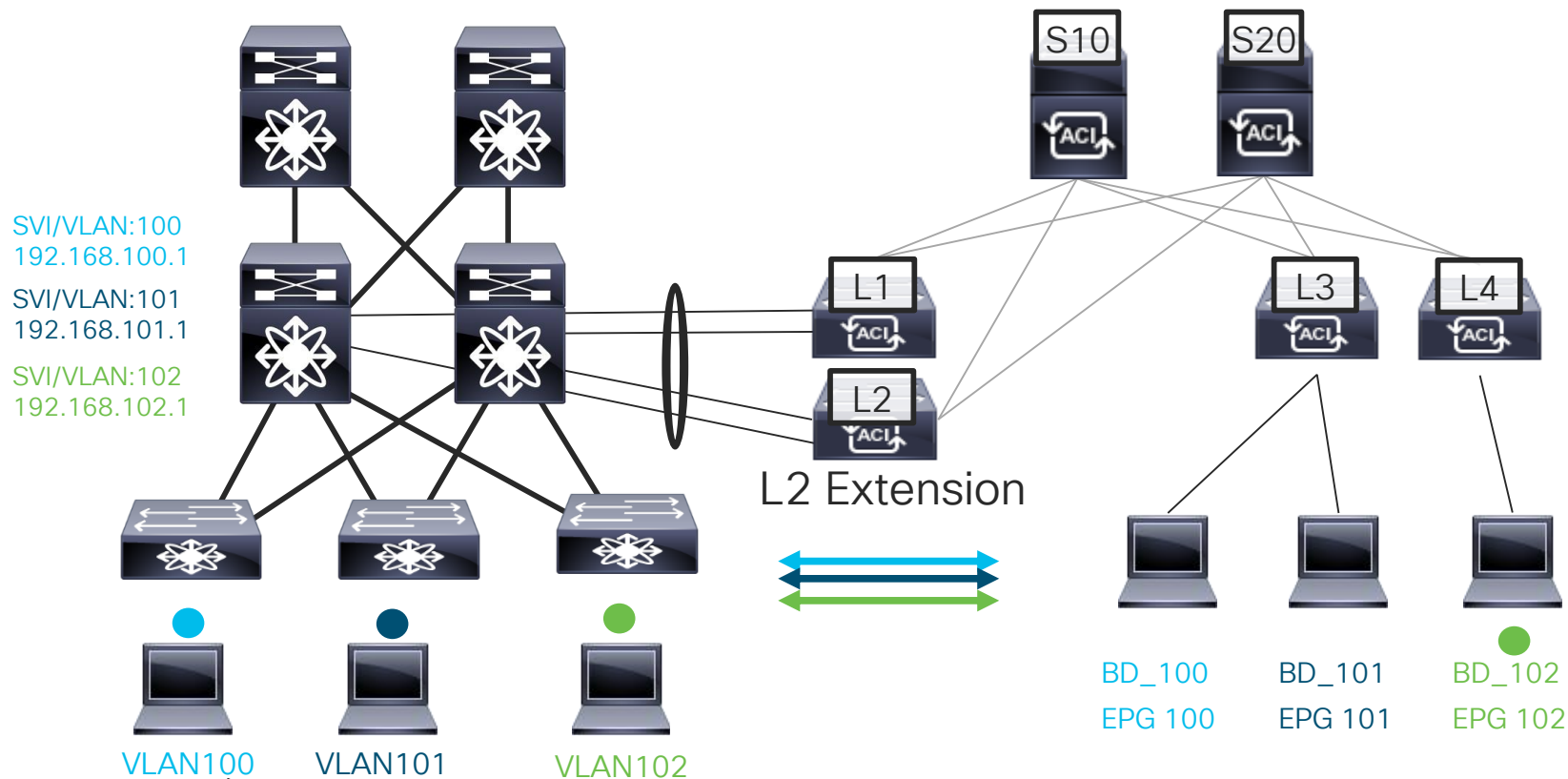


Conceptual View



Ciscolive!

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

The screenshot displays the Cisco APIC GUI interface. On the left, a navigation tree shows the hierarchy: CiscoLive > Application Profiles > CiscoLive > Application EPGs (1000) > VLAN2000 > uSeg EPGs > LegacyVlans > Application EPGs > Vlan100. The 'Vlan100' entry is selected, showing its sub-items: Domains (VMs and Bare-Metals), EPG Members, Static Ports, and two Pod configurations.

The main panel shows the 'Learned End-Points' tab. A callout box highlights a specific entry in the table:

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

The background table in the 'Learned End-Points' tab has the following structure:

End Point	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap	
EP-5C:83:8F:69:BB:01	5C:83:8F:69: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

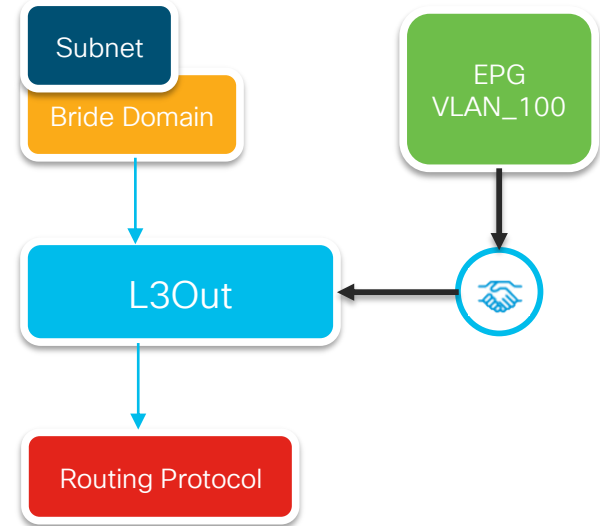
Subnet defined on **BD**

L3Out associated with **BD**

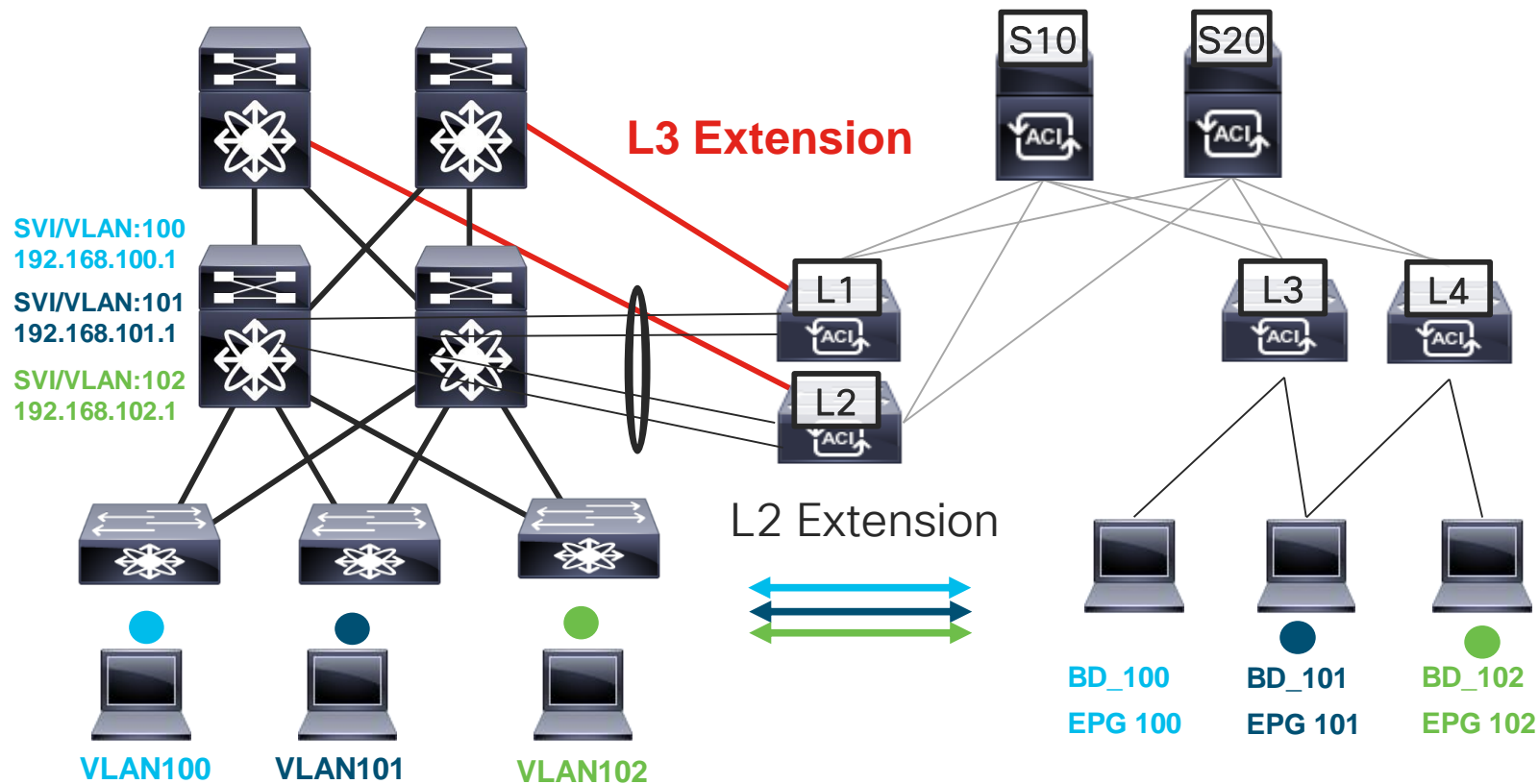
EPG has contract to **L3Out** Network

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

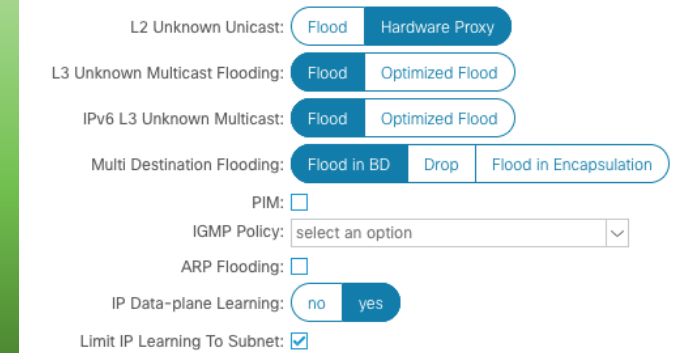
Limit IP learning to Subnet

Off Subnet Learns are cleared

Learning is disabled for 2 minutes

3) Global Settings

Enforce Subnet Check – **adds prefix check to all BD's**



Bridge Domain configuration settings:

- L2 Unknown Unicast: **Flood** | Hardware Proxy
- L3 Unknown Multicast Flooding: **Flood** | Optimized Flood
- IPv6 L3 Unknown Multicast: **Flood** | Optimized Flood
- Multi Destination Flooding: **Flood in BD** | Drop | Flood in Encapsulation
- PIM: ☐
- IGMP Policy: select an option
- ARP Flooding: ☐
- IP Data-plane Learning: **no** | yes
- Limit IP Learning To Subnet: ☒

Fabric Wide Setting Policy

Properties

Disable Remote EP Learning: ☐ To disable remote endpoint learning in VRFs containing external brid

Enforce Subnet Check: ☒ To disable IP address learning on the outside of subnets configured

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

The screenshot displays the APIC GUI interface. On the left, a navigation pane shows a tree structure with 'CiscoLive' at the top, followed by 'Application Profiles', 'CiscoLive', 'LegacyVlans', 'Application EPGs' (containing 'Vlan100', 'Vlan101', and 'Vlan102'), and 'uSeg EPGs'. The main content area is divided into two tabs: 'Operational' (selected) and 'Summary'. The 'Operational' tab contains a table titled 'Client End-Points' with columns: 'End Point', 'MAC', 'Learning Source', 'Hosting Server', 'Reporting Interface', 'Controller Name', 'Multi Encap Address', and 'Encap'. A single row of data is visible, corresponding to the IP 192.168.102.11. A blue arrow points from this row in the table to the 'Operational' tab header.

MAC	IP	Hosting Server	Interface	Encap
00:0A:00:0A:00:0A	192.168.102.11	---	Pod-1/Node-101-102/BareMetal02-vPC (I...	vlan-102

End Point	MAC	Learning Source	Hosting Server	Reporting Interface	Controller Name	Multi Encap Address	Encap
EP-00:0A:0A:0A:0A:0A	00:0A:0A:0A:0A:0A	learned	---	---	Pod-1/Node-101-102/BareMetal02-vPC (...)	---	vlan-102

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



cisco APIC

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

ALL TENANTS | Add Tenant | Tenant Search: | common | CiscoLive | jr | infra | ACI-AMT-Book

▼ OSPF-To-Core

- ▼ Logical Node Profiles
 - > Leaf101
 - ▼ Leaf102
 - ▼ Logical Interface Profiles
 - > Port13
 - ▼ Configured Nodes
 - ▼ topology/pod-1/node-102
 - ARP for VRF-CiscoLive:CiscoLive
 - > BGP for VRF-CiscoLive:CiscoLive
 - > ND for VRF-CiscoLive:CiscoLive
 - ▼ OSPF for VRF-CiscoLive:CiscoLive
 - > Areas
 - > Interfaces
 - Routes

Routes

Name	Pfx
▶ Route 1.1.1.102/32, Flags:direct,v4, Unicast Cost: 1	1.1.1.102/32
▶ Route 192.168.255.4/30, Flags:direct,v4, Unicast Cost: 4	192.168.255....
▶ Route 192.168.255.0/30, Flags:in-rib,v4, Unicast Cost: 8	192.168.255....
▶ Route 1.1.1.101/32, Flags:in-rib,v4, Unicast Cost: 9	1.1.1.101/32
▶ Route 192.168.101.0/24, Flags:in-rib,v4, Unicast Cost: 20	192.168.101....
▶ Route 10.0.0.0/8, Flags:in-rib,v4, Unicast Cost: 5	10.0.0.0/8
Nexthop eth1/13-192.168.255.6	

Verification



SSH



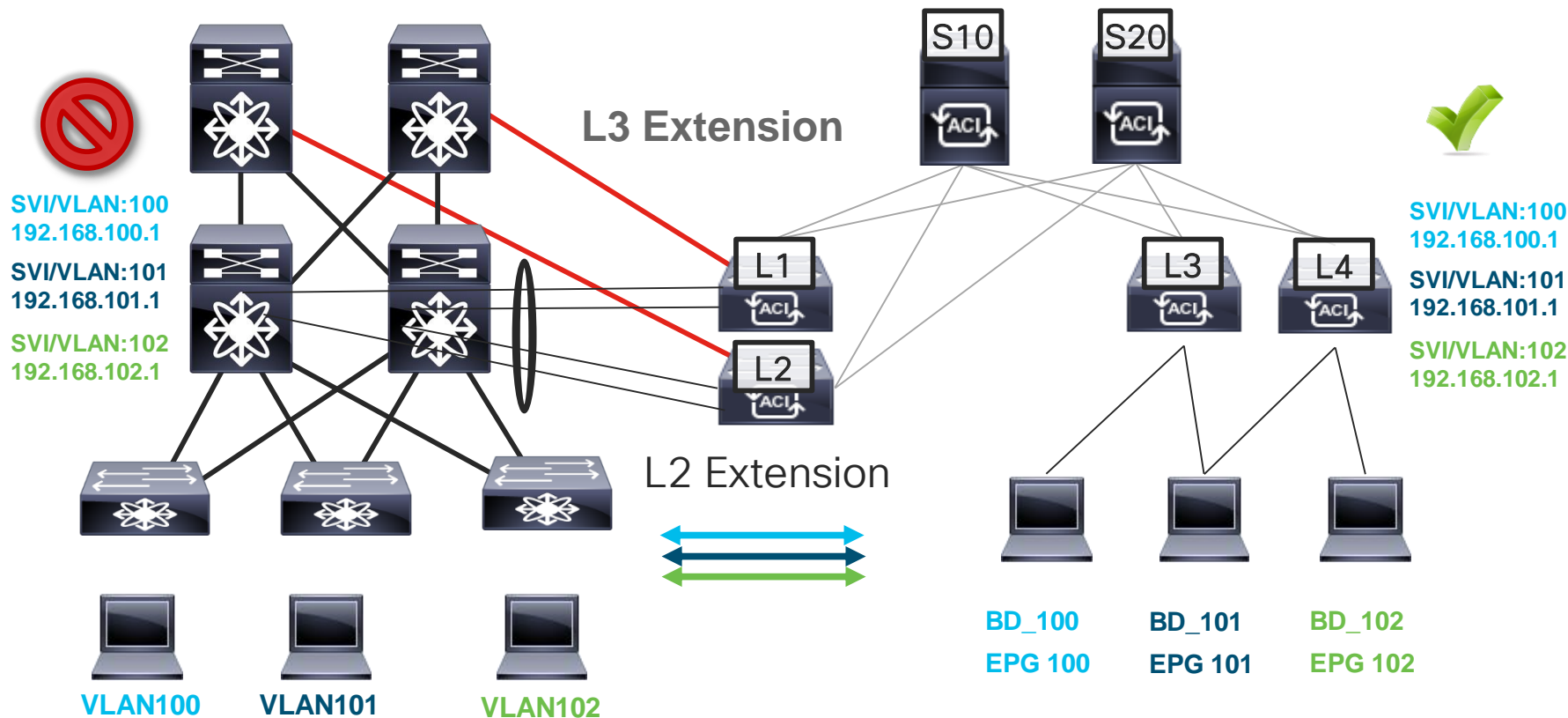
```
Leaf101# show ip ospf neighbors vrf CiscoLive:CiscoLive
OSPF Process ID default VRF CiscoLive:VRF1
Total number of neighbors: 1
Neighbor ID      Pri State                Up Time  Address      Interface
192.168.255.255  1 FULL/BDR             02:27:05 192.168.255.2 Eth1/13
```

```
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

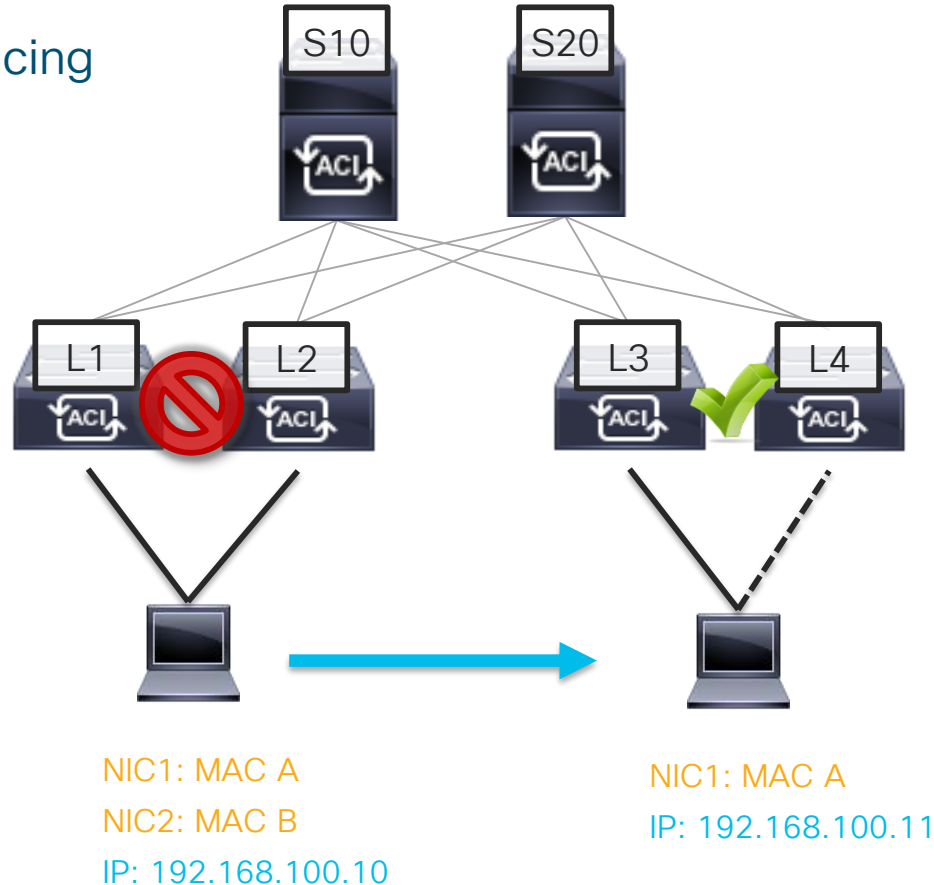
Problem:

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

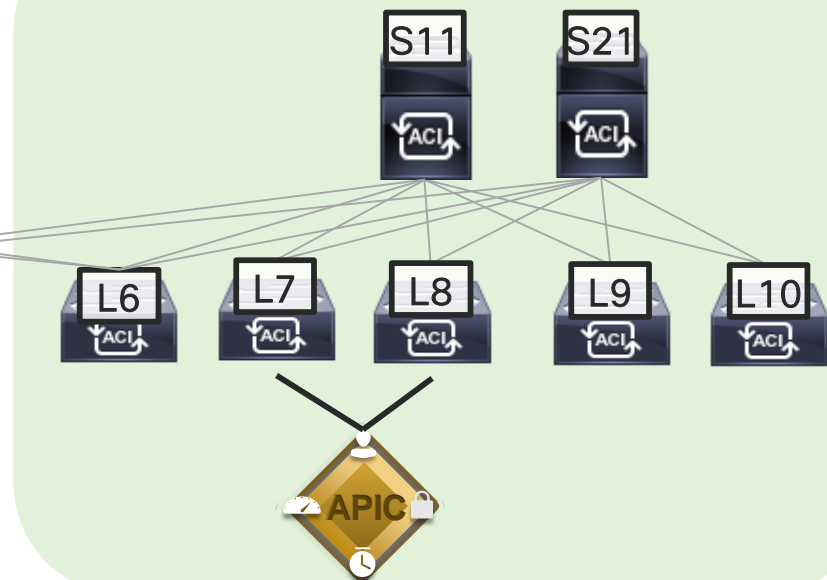
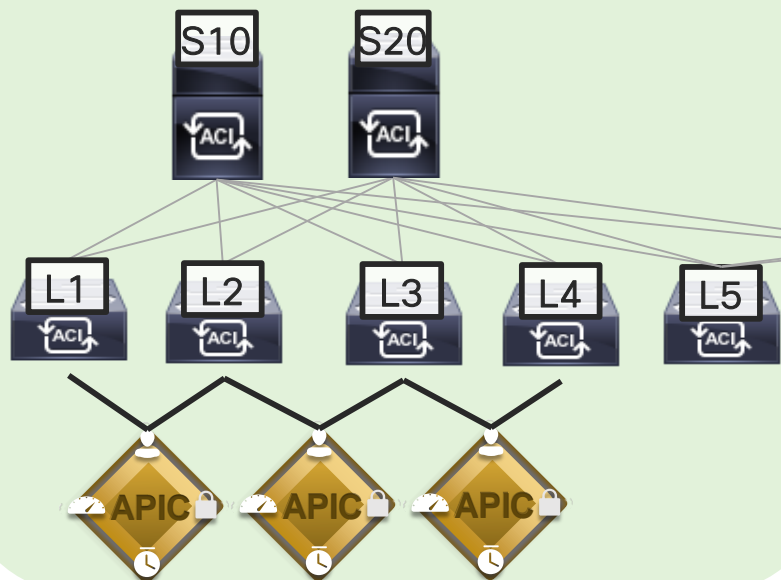


You make networking **possible**



Stretched Fabric

— IS-IS





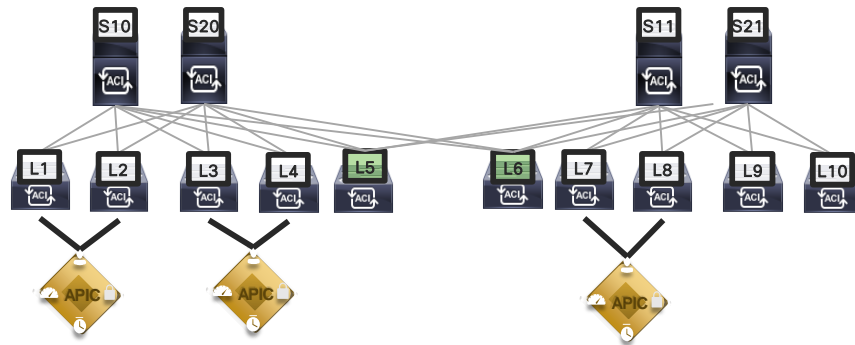
Stretched Fabric

Advantages

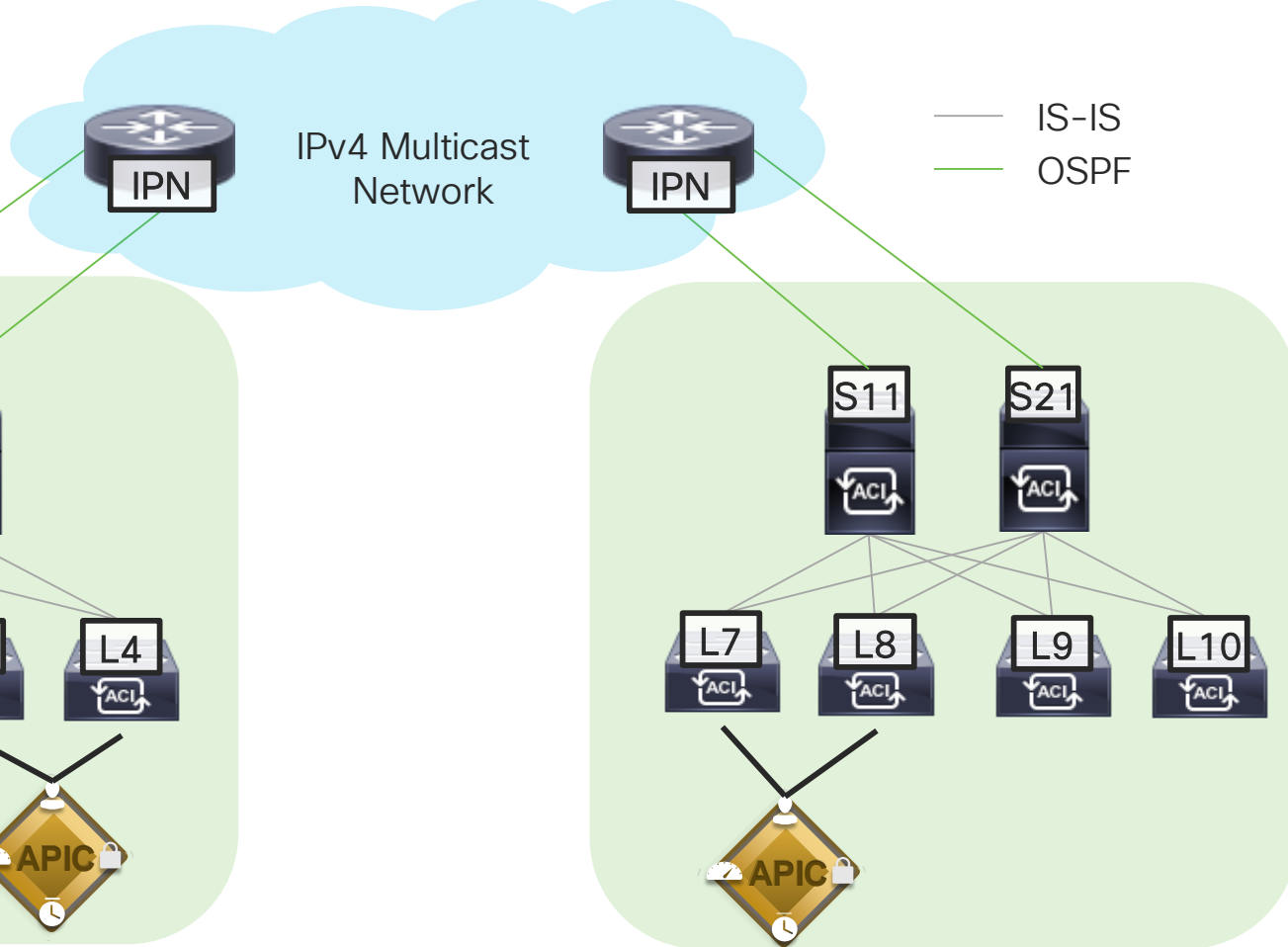
- All one Fabric
- No Additional Routed Infrastructure
- Simple Provisioning – If cabling is in place

Limitations

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



Multipod



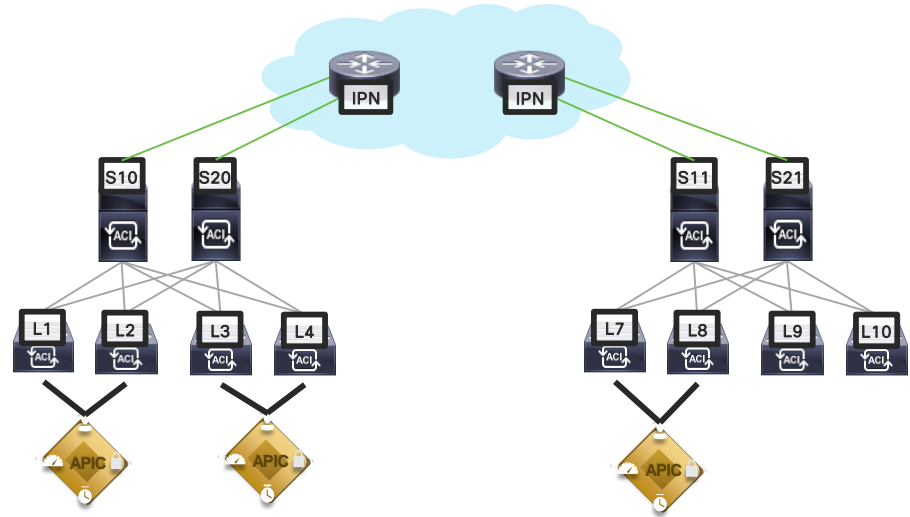
Multipod

Advantages

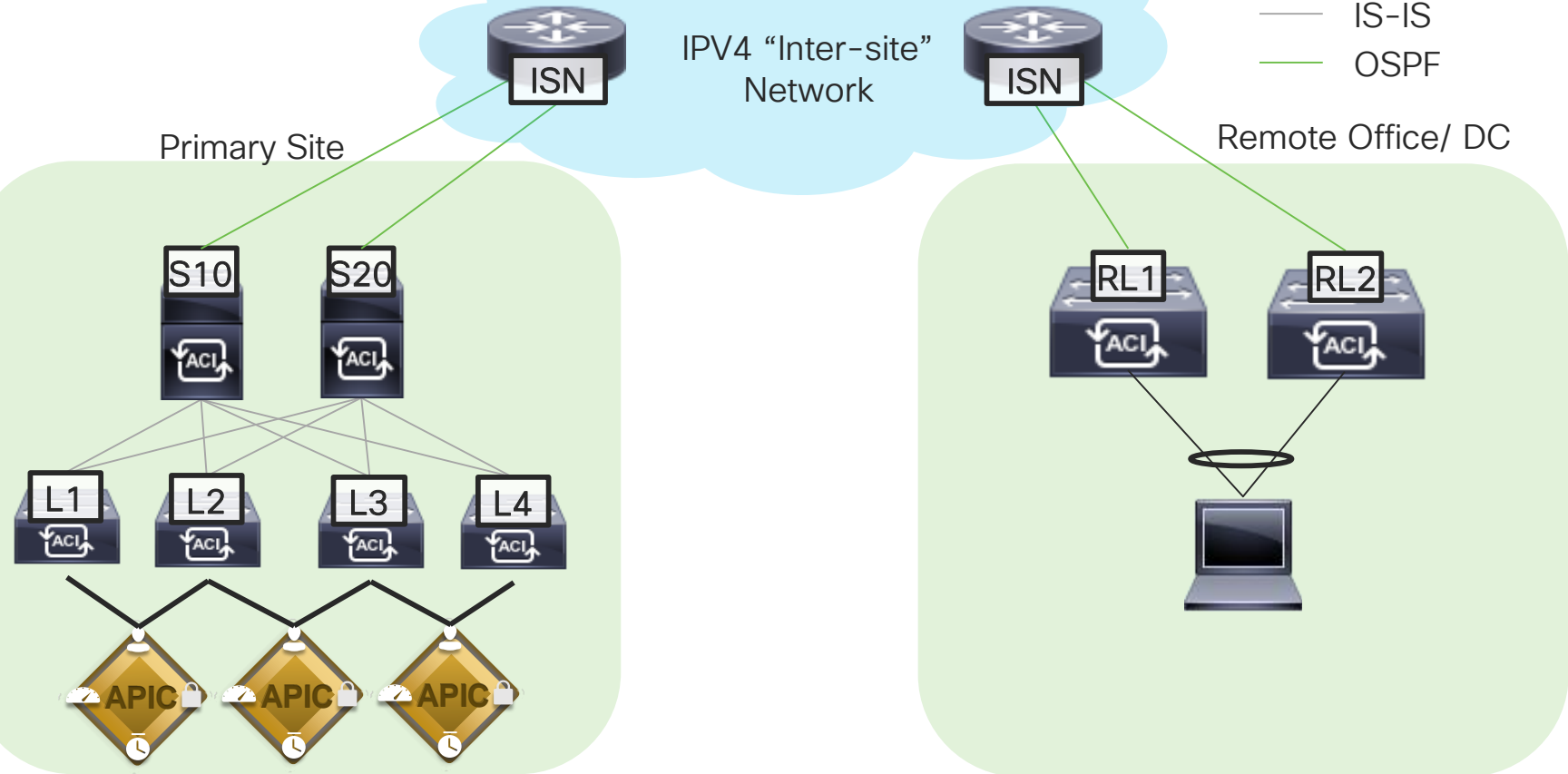
- All one Fabric
- Policy Stretched across sites
- Separate Control Plane Instances per site
- Increases Leaf Scale to 400

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



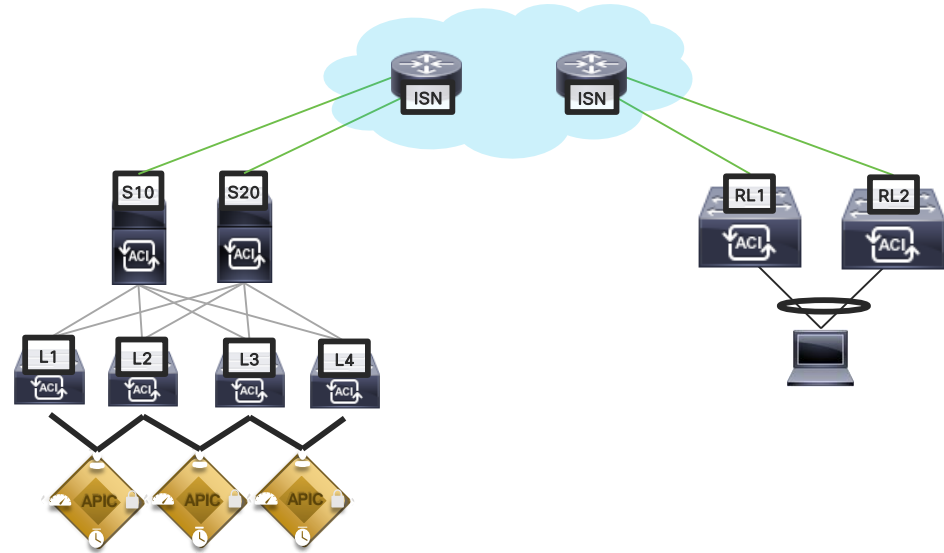
Remote Leaf



Remote Leaf

Advantages

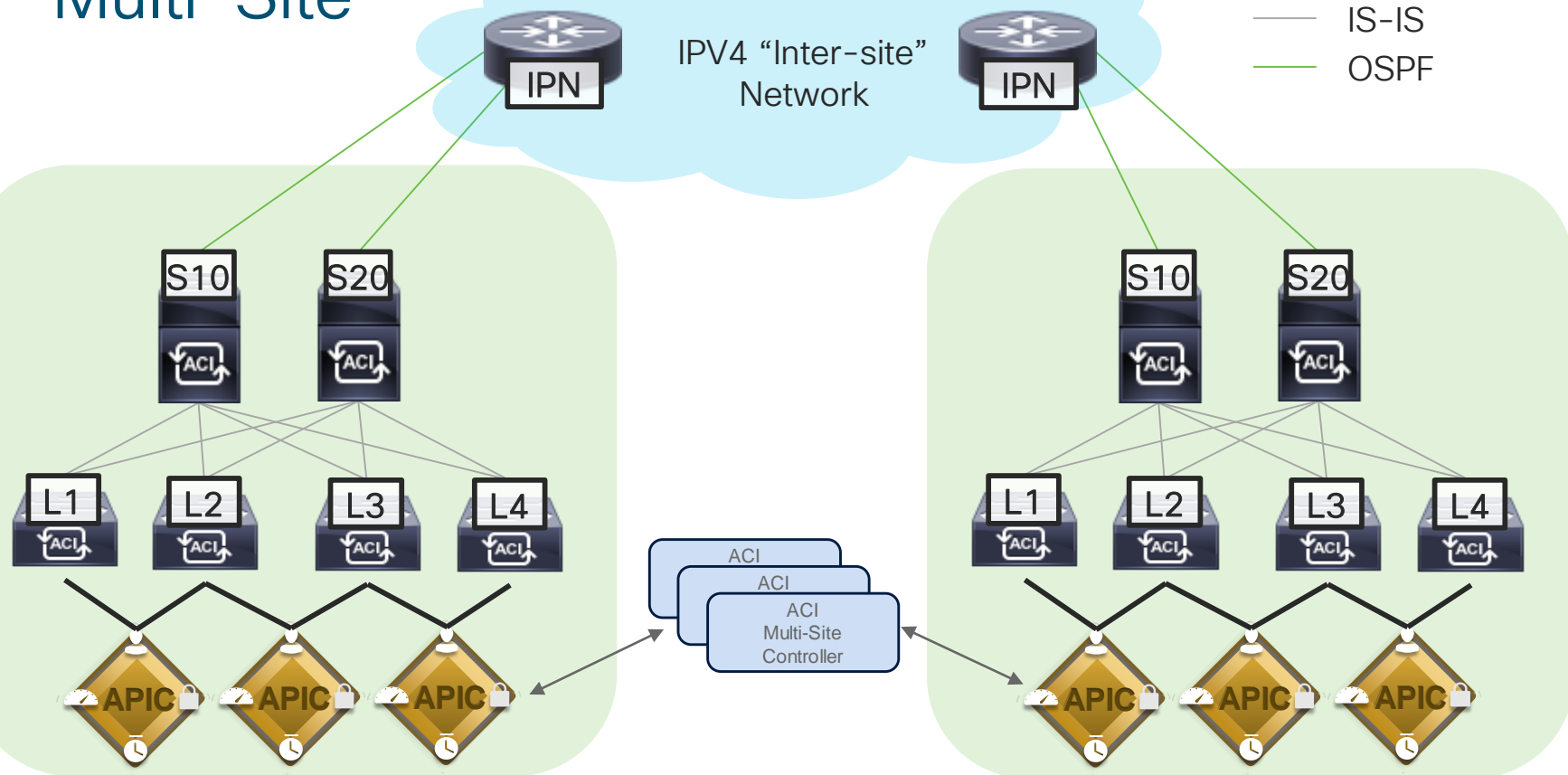
- All one Fabric
- Easy Addition of small site to existing APIC
- Spines not required in Remote Site.
- Connects to existing routing infrastructure
 - No Multicast required



Limitations

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

Multi-Site



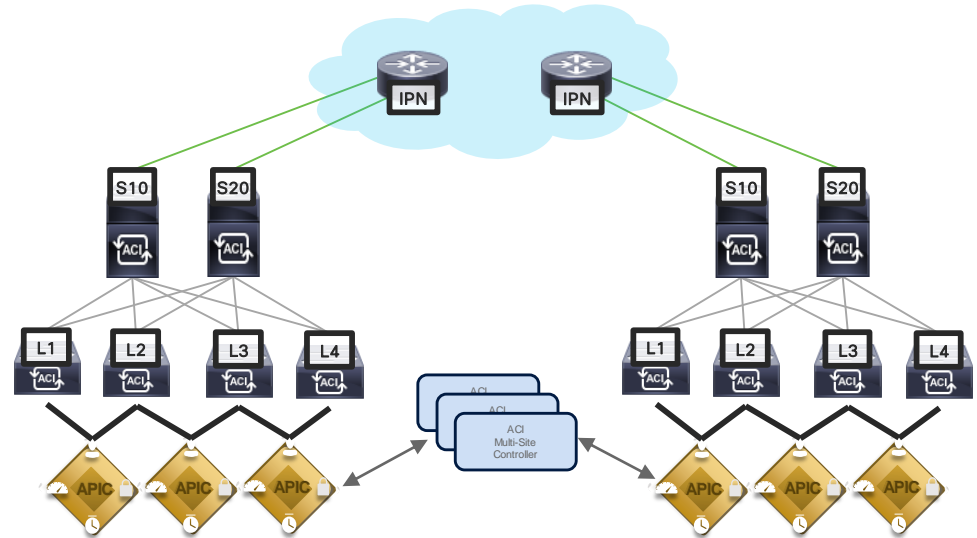
Multi-Site

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/rsmdsn	RsMdsn 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
Warning	<input type="checkbox"/>	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
Info	<input type="checkbox"/>	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

192.168.102.11

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

192.168.102.11

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/LegacyVlans/...	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	CiscoLive/LegacyVlans/...	attached	Pod-1/Node-103-104	BareMetal01-vPC	vlan-102

Page 1 Of 1

Objects Per Page: 15

Displaying Objects 1 - 7 Of 7

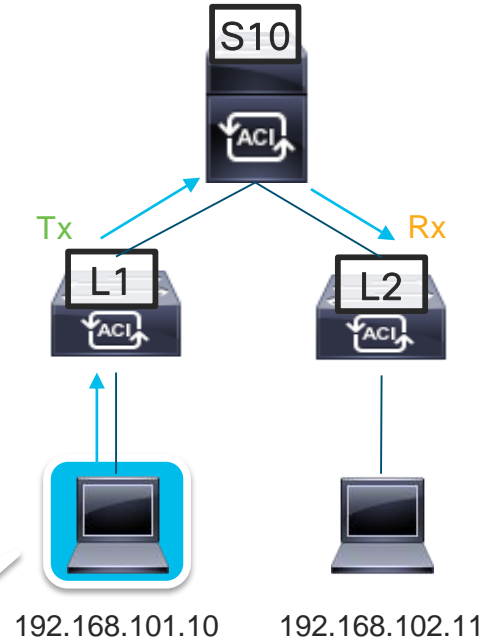
IP Was Moving???

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



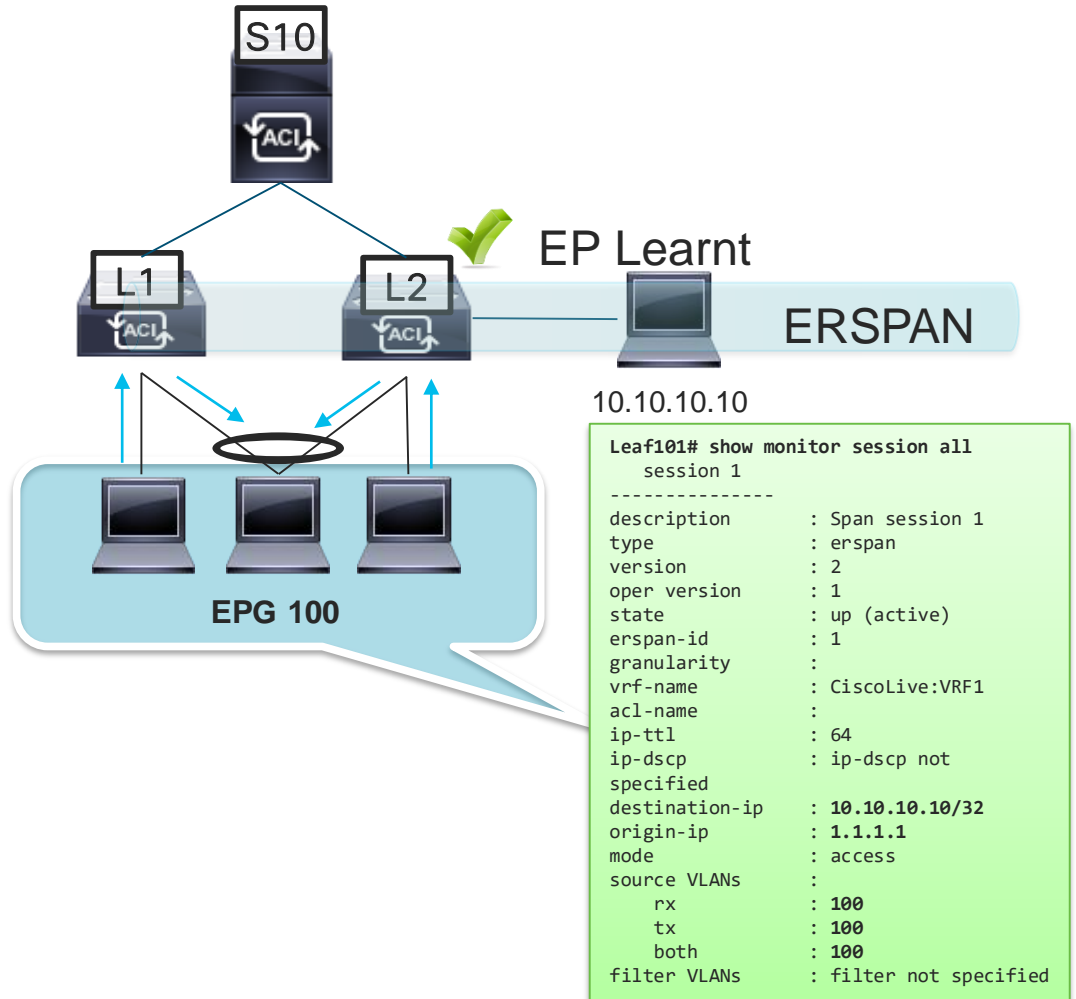
Source	Destination	Last Collection (30 Seconds)			Tot			Excess Pkt
		Transmit Pkt	Admitted Pkt	Dropped Pkt	Transmit Pkt	Admitted Pkt	Dropped Pkt	
uni/tn-CiscoLive/ap-Legacy...	uni/tn-CiscoLive/ap-LegacyVlans/epg-...	3926	3926	0	81658	81658	0	0

NO Packet Loss In Overlay

Dropped Pkt	Transmit Pkt	Admitted Pkt
0	81658	81658

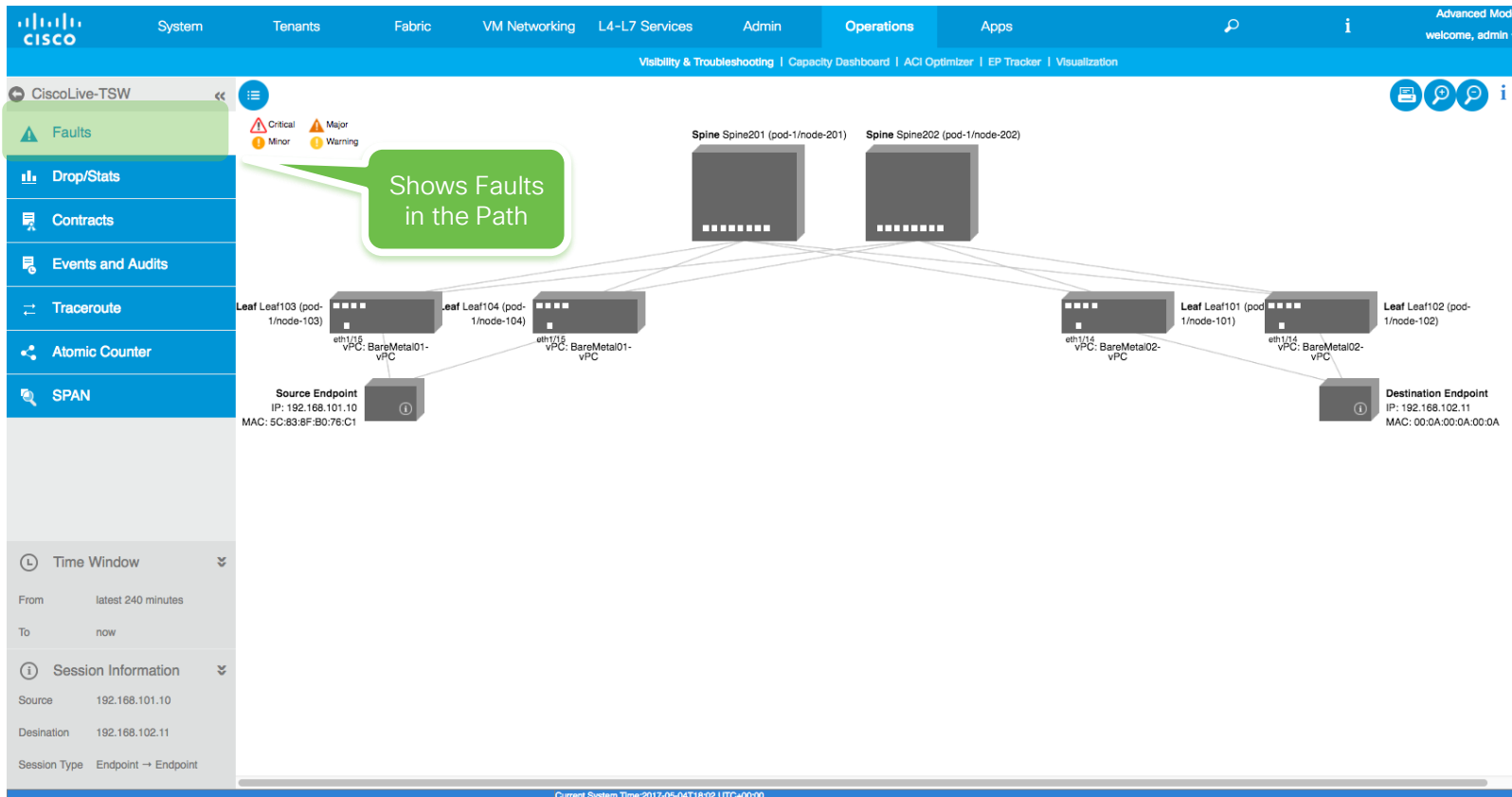
SPAN

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

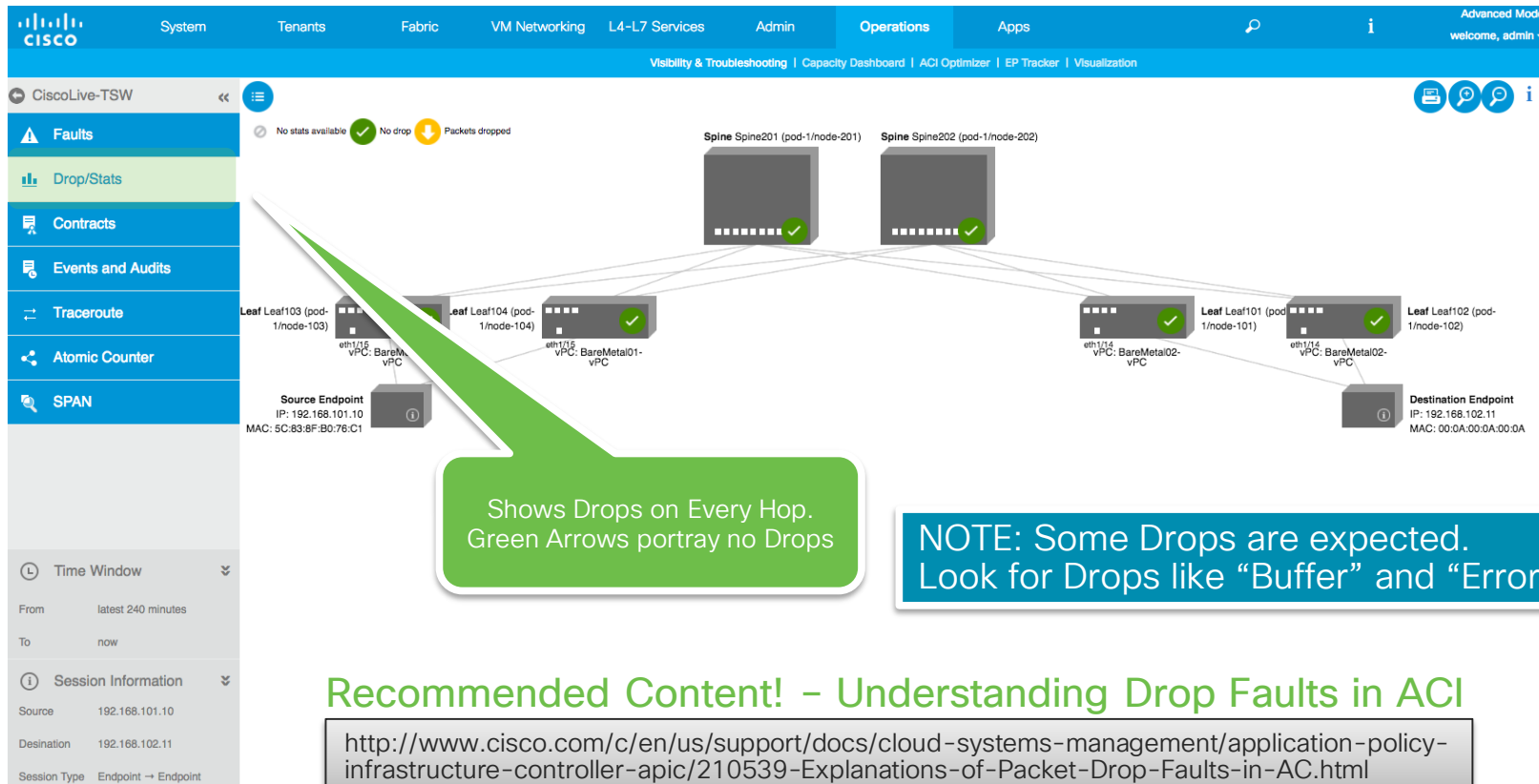


SPAN Source	SPAN Destination
EPG	ERSPAN
Port	ERPSAN/Local Port

Troubleshooting Wizard – Faults



Troubleshooting Wizard – Drop Stats



Troubleshooting Wizard - Contracts



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

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)

Source Endpoint IP: 192.168.101.10 MAC: 5C:83:BF: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	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
Filter ID: Implicit							
1	ip:tcp	22 - 22	22 - 22		deny,log	node-101 node-102 node-103 node-104	17 7 5 0

Context Implicit (CiscoLive/VRFI)

Destination Endpoint → Source Endpoint

Filter ID	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
Filter ID: Implicit							
1	ip:tcp	22 - 22	22 - 22		permit	node-101 node-102 node-103 node-104	2357258 0 0 56

BD Allow (CiscoLive/BD_Vlan101)

Time Window

From latest 240 minutes To now

Session Information

Source 192.168.101.10 Destination 192.168.102.11 Session Type Endpoint → Endpoint

Troubleshooting Wizard – Atomic Counters



CiscoLive-TSW

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

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

Advanced Mode welcome, admin

Failures 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)

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

Destination 192.168.102.11

Session Type Endpoint → Endpoint

Troubleshooting Wizard – SPAN



CiscoLive-TSW

System Tenants Fabric VM Networking L4-L7 Services

Advanced Mode welcome, admin

SPAN - Bidirectional ERSPAN

ERSPAN Source
Uncheck the interface that you do not want to span.

ERSPAN Destination
Destination Type: ☐ EPG ☐ Host via APIC ☒ Predefined Destination Group
Predefined Destination Group: CiscoLive

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

eth1/48 vPC BareMetal01- vPC eth1/48 vPC BareMetal02- vPC eth1/48 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
Destination 192.168.102.11
Session Type Endpoint → Endpoint

Ability to SPAN to APIC or other devices attached to the Fabric

User can select which ports to SPAN

Capacity Dashboard

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	Rules: 2078 of 65536 Labels: 0 of 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	Rules: 2077 of 65536 Labels: 0 of 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% 7 of 12288 Local: Remote: 1 of 12288	<1% 5 of 12288 Local: Remote: 0 of 12288	<1% 1 of 8192 Local: Remote: 0 of 8192	0% 0 of 8192	2% 93 of 4096	<1% 34 of 3960	0%

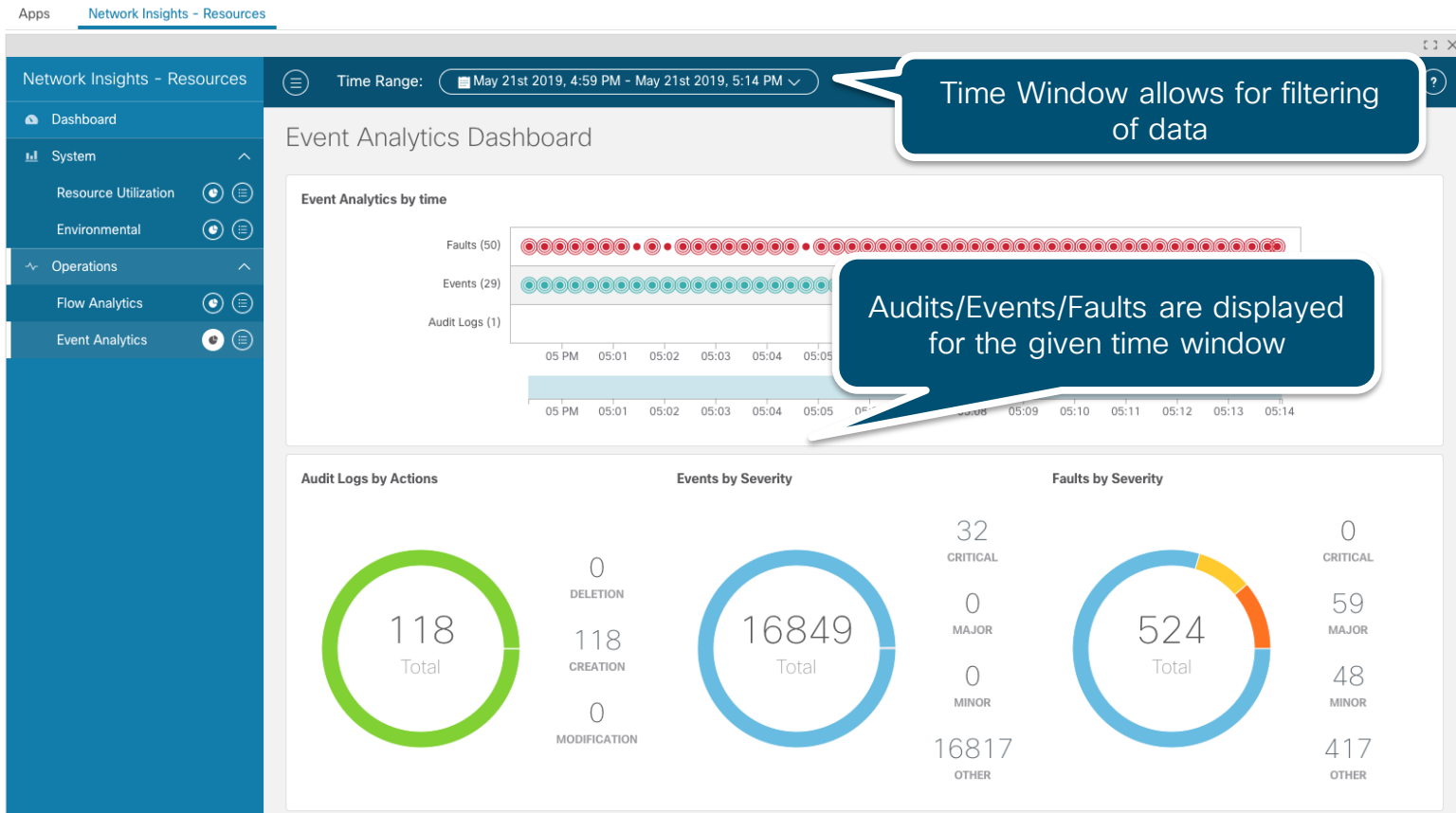
Capacity Dashboard panel displays your usage by range and percentage. Use this to plan your fabric Scale.

App Center

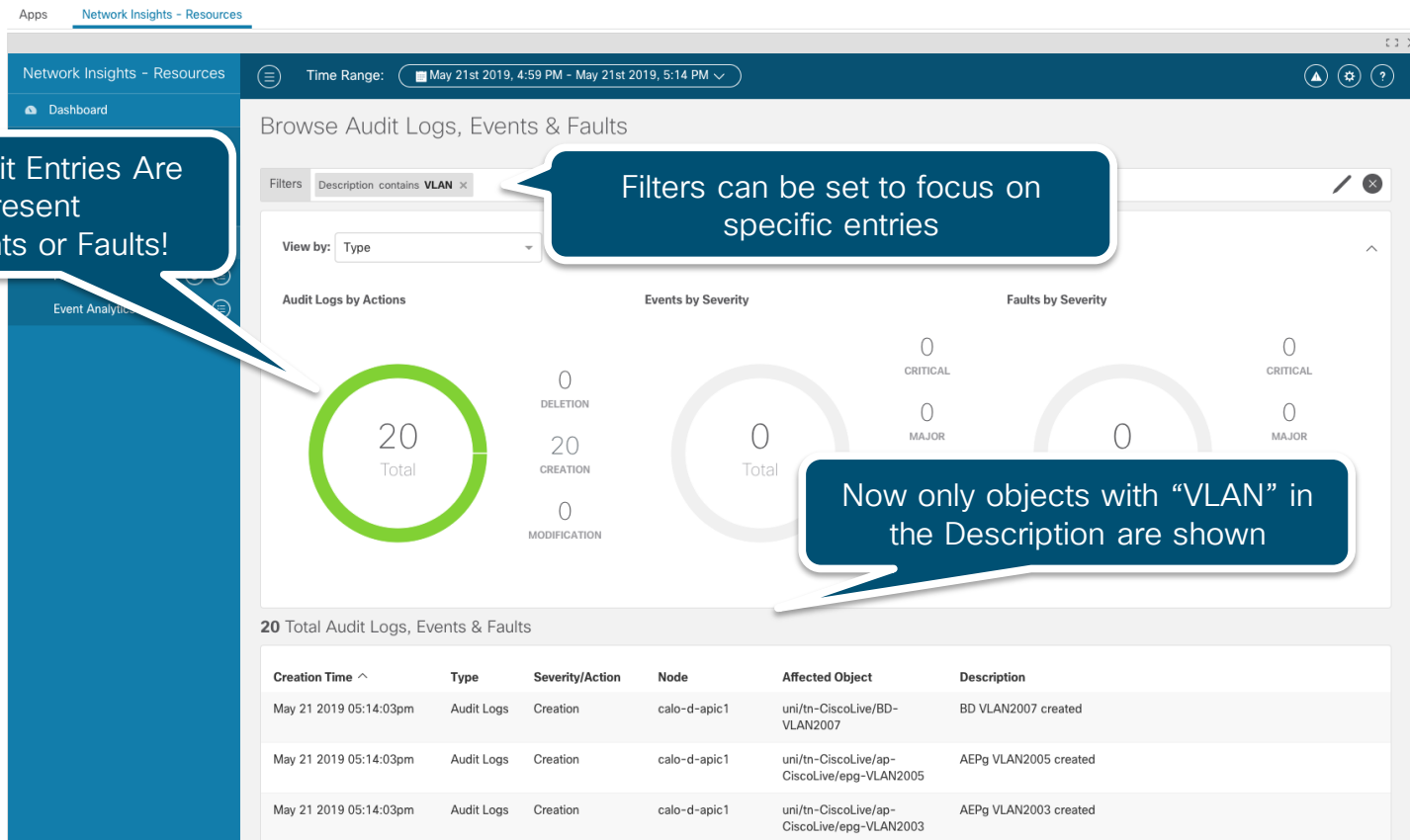
The screenshot shows the Cisco APIC (CALO-D) interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations, **Apps**, and Integrations. The **Apps** tab is highlighted and circled in red. Below the navigation bar, the 'Apps' section displays a grid of application tiles. Each tile includes an icon, the application name, the provider (Cisco), a brief description, and an 'Open' button. The applications shown are Contract Viewer, ELAM Assistant, EnhancedEndpointT, ExternalSwitch, NAE Policy Explorer, and Network Insights - Resources. The Network Insights tile is highlighted with a green background.

Application Name	Provider	Description	Open Button
Contract Viewer	Cisco	Contract Viewer for the stats data between EPGs	Open
ELAM Assistant	Cisco	Help you perform ELAM(Embedded Logic Analyzer Module) on ACI nodes to capture a single packet at a time and analyze where the packet goes.	Open
EnhancedEndpointT	Cisco	Track endpoint activity within the ACI fabric	Open
ExternalSwitch	Cisco	Integration with external switch managers	Open
NAE Policy Explorer	Cisco	Cisco Network Assurance Engine Policy Explorer provides capability to explore policy configuration and connectivity in ACI networks	Open
Network Insights - Resources	Cisco	Network Insights - Resources is a platform for predictive analytics, correlation and alerting using streaming telemetry data for network fabrics.	Open

Network Insights - Resources



Network Insights - Resources



Network Insights - Resources

Apps Network Insights - Resources

Audit Log Details - **4211945**

General Timeline

General Information

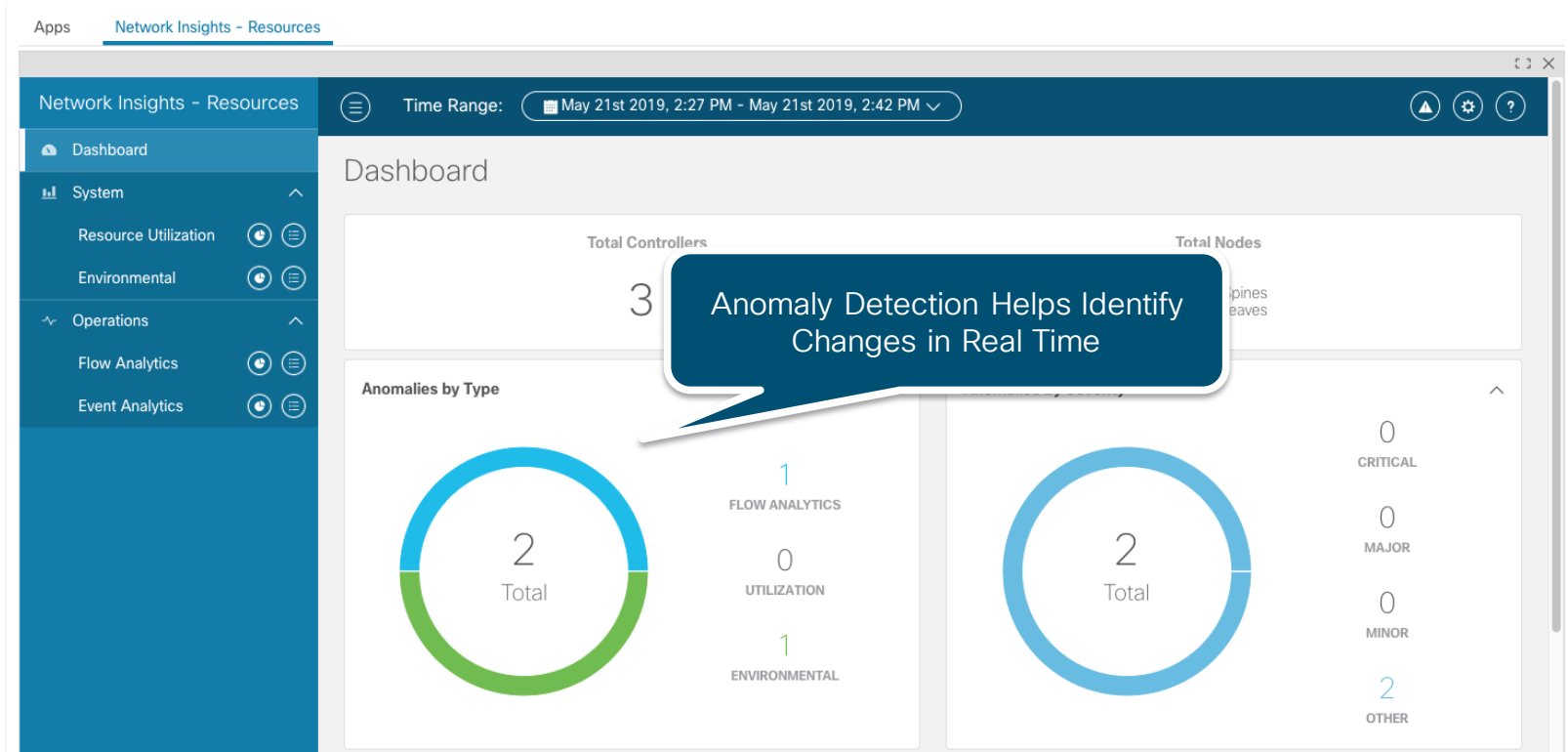
USER NAME	ACTION	AFFECTED OBJECT	EVENT CODE	EVENT TYPE	CREATED
remoteuser-carschmi	creation	uni/tn-CiscoLive/BD-VLAN2051	4211945	AuditLog	May 29 2019 02:16:11pm

Diagnostics

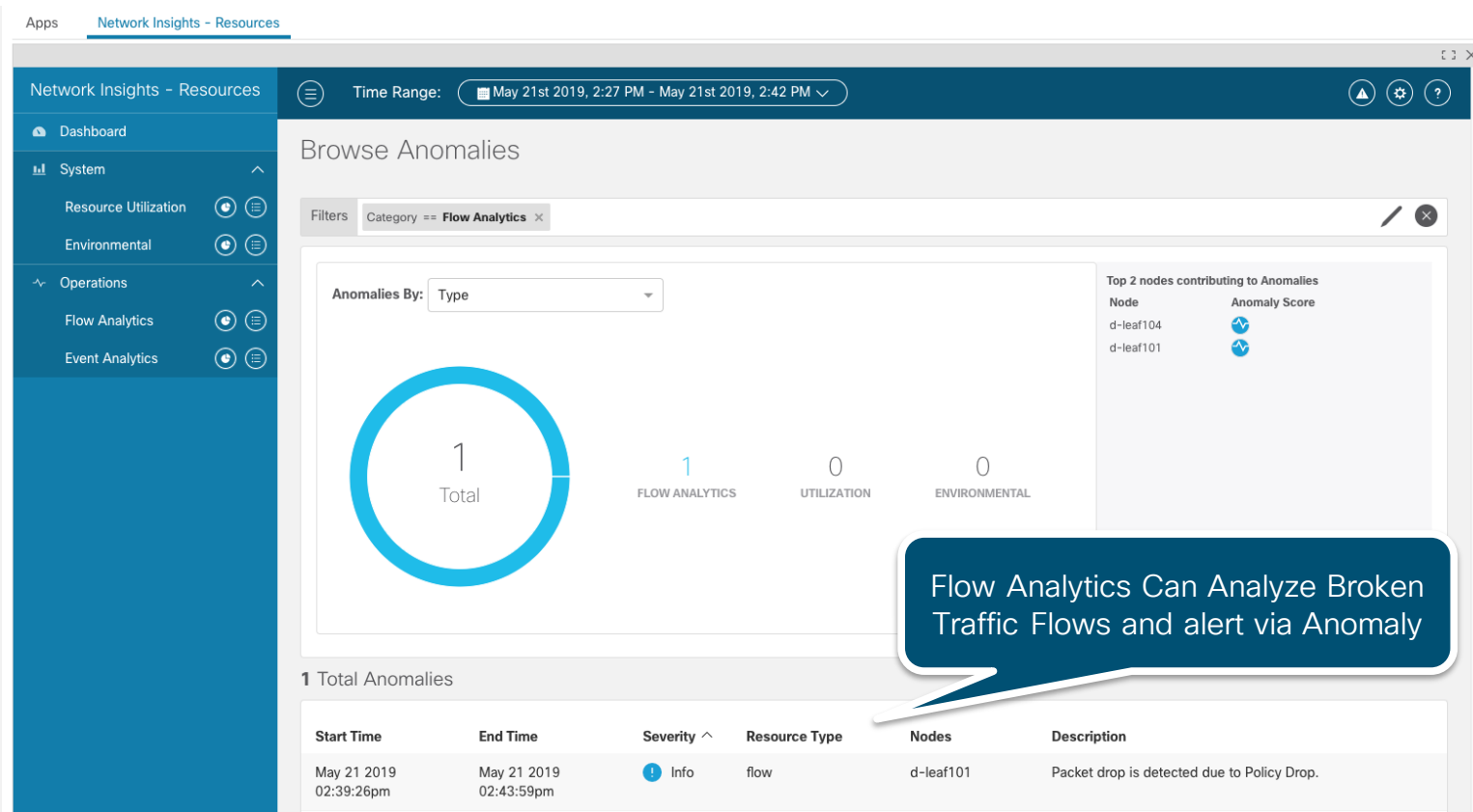
DESCRIPTION
BD VLAN2051 created

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

Network Insights - Resources



Network Insights - Resources



Network Insights - Resources

Apps Network Insights - Resources

Flow Details

Details about Affected Endpoints
are reported

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

May 21 2019, 2:39 PM

Policy Drop

No Contract!

Source

192.168.4.40
Port: 0
e4



d-leaf101
po2 unknown

Destination

192.168.3.11
Port: 0
e3

ELAM Assistant App

The screenshot displays the ELAM Assistant App interface. On the left is a sidebar with a menu including '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)', and 'Unsupported Nodes'. The main panel is titled 'Capture a packet with ELAM (Embedded Logic Analyzer Module)'. It features a 'Name your capture:' field with '(optional)' as a placeholder. Below this is a table with columns: Status, Node, Direction, Source I/F, and Parameters. Two rows are shown: one for 'node-101' with a 'Set' button, and one for 'node-102' with a 'Report Ready' button. Both rows show 'from frontport' for Direction and 'any' for Source I/F. The Parameters column for each row contains 'src ip' (192.168.4.40) and 'dst ip' (192.168.3.11). At the bottom of the main panel are buttons for 'Set ELAM(s)' and 'Check Trigger'. A 'Select a report.' section is visible at the very bottom.

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

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)
Incoming I/F	eth1/13

L2 Header

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

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!

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::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

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

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

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



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. [v](#)

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
REPLIES

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

Cisco ACI User Group

Public Group

Discussion

Members

Events

Photos

Files

Search this group

APIC

Joined

Notifications

Share

Write Post

Add Photo/Video

Add File

More

Write something...

PINNED POST

Robert Burns

February 16

Greetings Group - We are developing a 4-hour Techtorial Session for the upcoming Cisco Live US in June and could use your input. The session will be a Technical Intro to ACI. Looking for comments on what topics you think should be covered for someone that may have little to no experience with ACI. ACI is obviously a beast of a technology, so we're looking for creating the best zero-to-hero type session possible using a combination of presentation & live demos. Any input appreciated!

Daniel Pita and 12 others

12 Comments

Like

Comment

Share

ADD MEMBERS

Enter name or email address...

MEMBERS

1,512 Members

Great Community 😊

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





You make **possible**