



Cisco *live!*

6-9 March 2018 • Melbourne, Australia

ACI for Network Engineers

Steve Sharman – Technical Solutions Architect

BRKACI-1002

Cisco Spark

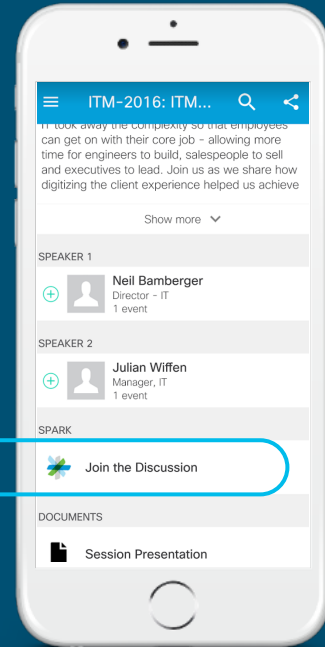


Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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



Abstract

This "Introduction to ACI" session will walk attendees through the design considerations you should undertake when planning the deployment of an ACI network.

Topics covered will be Application Centric Mode vs Network Centric Mode, a deep dive on Bridge Domain configuration and forwarding, a look at firewall integration/migration, VMware integration, and how to get started with automation.

Session objectives

At the end of the session attendees should have a good understanding of how to get an ACI fabric up and running with external connectivity. Plus a working knowledge of how to automate the network configuration from a simple spreadsheet.

Attendees will learn how to verify configuration using both the GUI and the command line.

Before we start, let's get to know each other ...



Agenda

- What is an ACI network?
- Let's build a network...!
- Let's use the network interfaces...!
- Allowing inter EPG communication
- Deep Dive – Bridge Domains
- Deep Dive – EPG Forwarding
- External Connectivity
- Firewall Integration
- VMware integration
- Getting Started with ACI Programming



What is an ACI network?



TYPICAL
3-TIER
APPLICATION

Cisco ACI Policy Model

APPLICATION NETWORK PROFILE



“ACI is all about applications, and I don’t know applications!”

“Are all applications based on three tiers?”

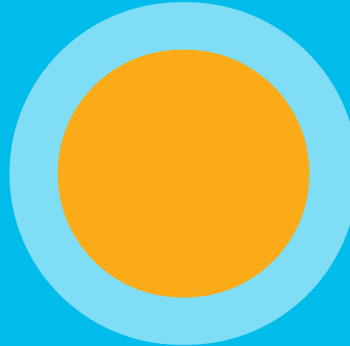


In reality ACI is all about networking and how you deploy applications onto the network

At a very basic level ACI is really just a Spine/Leaf network of Nexus 9k switches with a management platform

The network management platform (APIC) provides you with a single place from which to manage the network

Is ACI an Overlay or Underlay network?



ACI is an automated (VXLAN) overlay network running over an automated (ISIS) underlay network

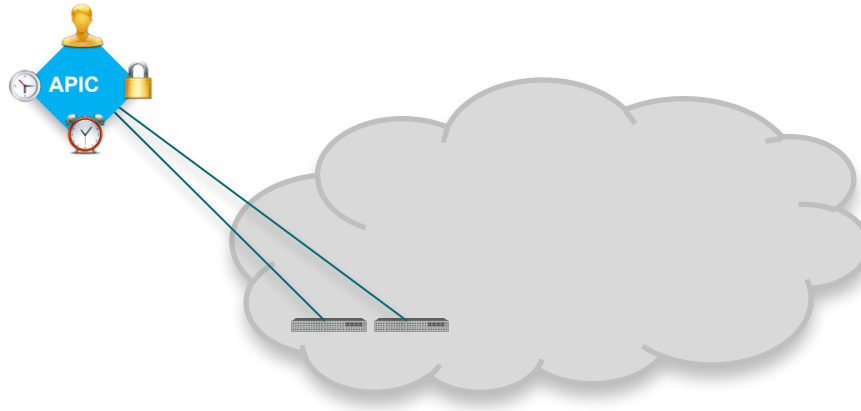
ACI can transport any IP traffic including “Overlay” networks based on VXLAN*, NVGRE* etc.

Let's build a network...!

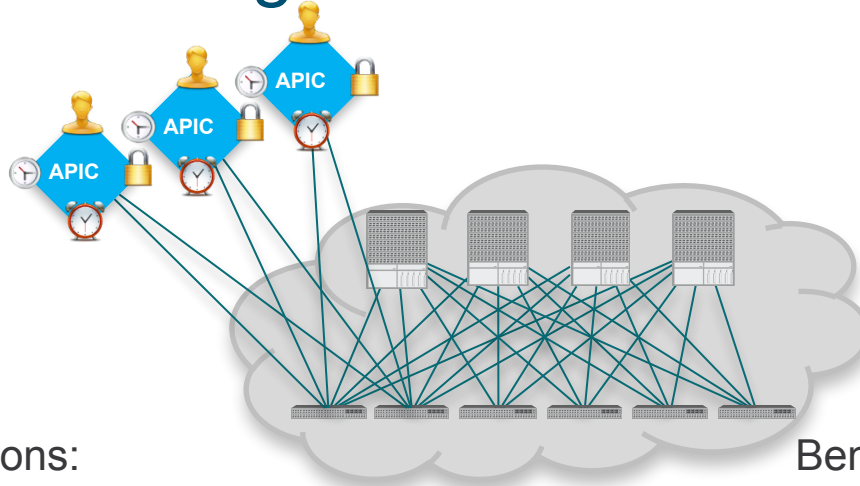
Physically Building the ACI Network



Physically Building the ACI Network



Physically Building the ACI Network



Management options:

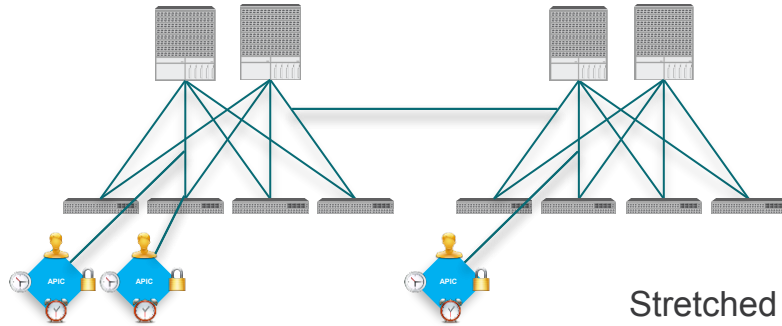
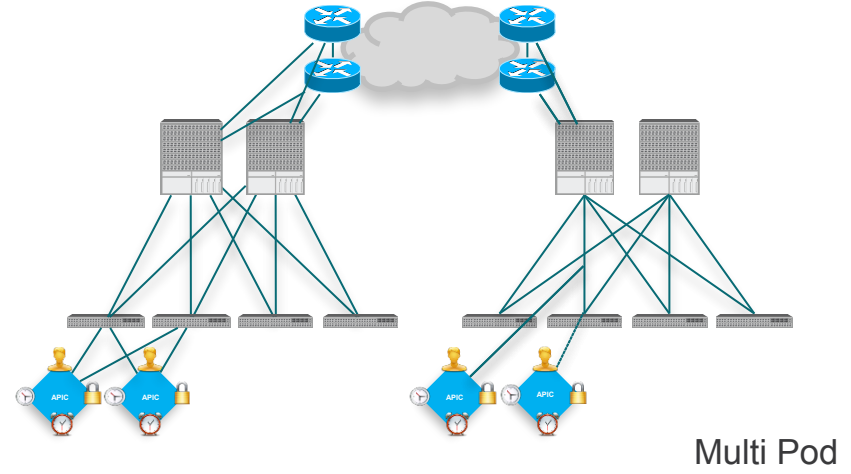
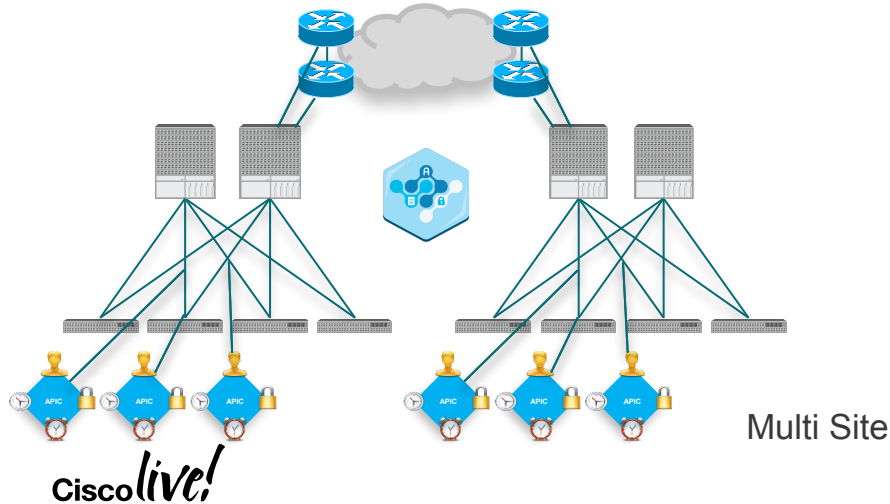
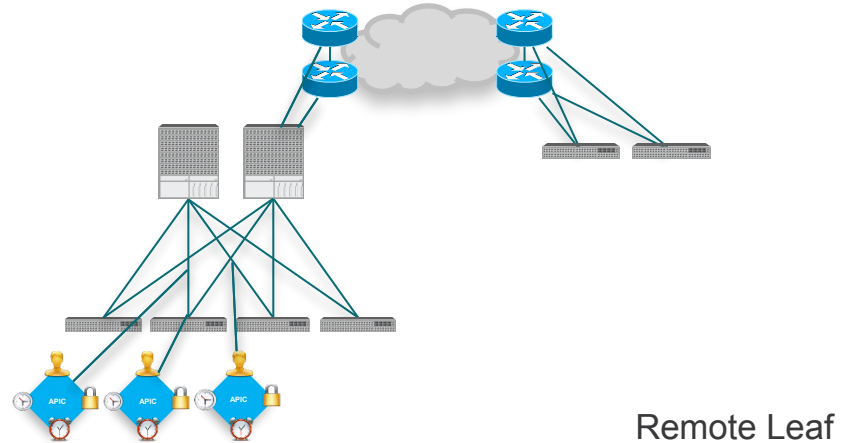
- GUI (basic/advanced)
- CLI
- XML/JSON
- Scripting
- Open API
- Automation

Benefits:

- Distributed, Centralised Management
- Full traffic visibility*
- Self documenting
- Integrated virtual and physical network
- Integrated L4-7 device management
- Policy defined network

* Excludes pre encapsulated/encrypted traffic

Topology options



An ACI network allows organisations to offer automated network services “on demand” through an open REST API

An ACI network provides the underpinning for an automated internal private cloud through a “build and consume” model of providing network services

ACI Consumption Model

Interface Configuration

Fabric | Access Policies

- VLANs
- Domains
- AAEP
- Interface Policies
- Leaf Policy Groups
- Leaf Profiles
- Switch Profiles

Policies



Quick Start

- > Switch Policies
- > Module Policies
- > Interface Policies
- > Global Policies
- > Monitoring Policies
- > Troubleshoot Policies
- > Pools
- > Physical and External Domains

Interface Consumption

Tenants

- Tenants
- VRFs
- Route Leaking
- L2/L3out
- Bridge Domains
- EPGs
- Contracts

Tenant CiscoLive



Quick Start

- > Tenant CiscoLive
 - > Application Profiles
 - > Networking
 - > L4-L7 Service Parameters
 - > DNS Server Groups (Beta)
 - > Security Policies
 - > Troubleshoot Policies
 - > Monitoring Policies
 - > L4-L7 Services
 - > NetFlow

ACI Consumption Model

Interface Configuration

Fabric | Access Policies

- VLANs
- Domains
- AAEP
- Interface Policies
- Leaf Policy Groups
- Leaf Profiles
- Switch Profiles

Policies



Quick Start

- > Switch Policies
- > Module Policies
- > Interface Policies
- > Global Policies
- > Monitoring Policies
- > Troubleshoot Policies
- > Pools
- > Physical and External Domains

Interface Consumption

Tenants

- Tenants
- VRFs
- Route Leaking
- L2/L3out
- Bridge Domains
- EPGs
- Contracts

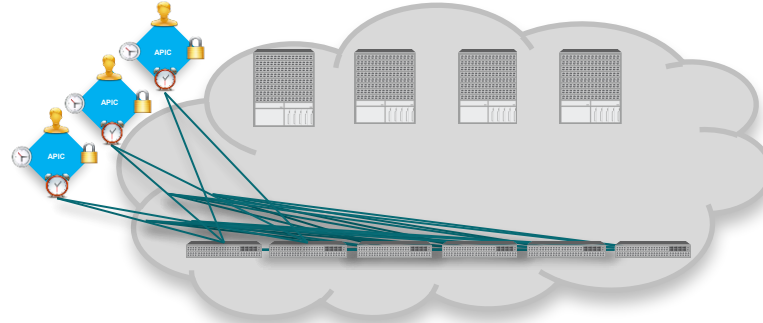
Tenant CiscoLive



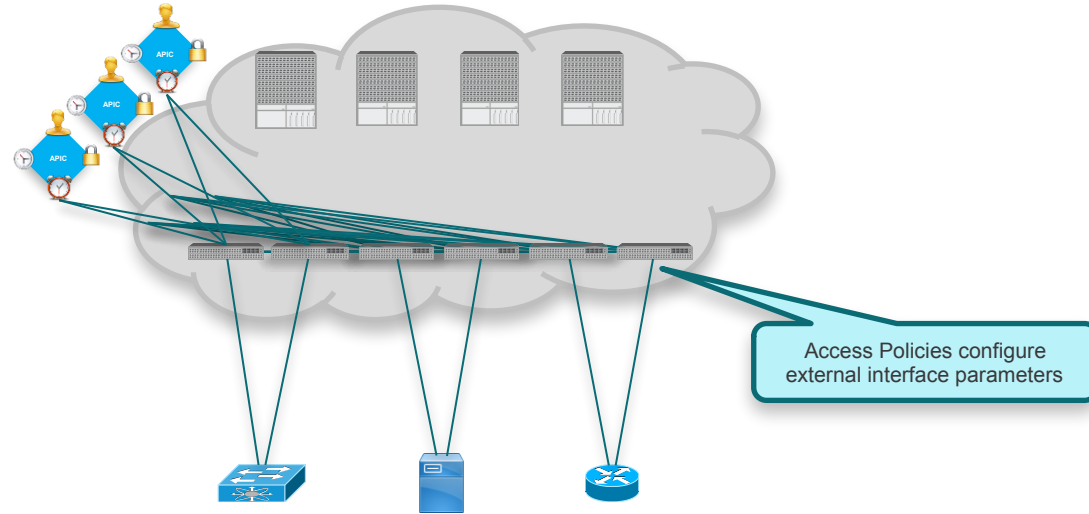
Quick Start

- > Tenant CiscoLive
 - > Application Profiles
 - > Networking
 - > L4-L7 Service Parameters
 - > DNS Server Groups (Beta)
 - > Security Policies
 - > Troubleshoot Policies
 - > Monitoring Policies
 - > L4-L7 Services
 - > NetFlow

Interface Configuration: Fabric | Access Policies



Interface Configuration: Fabric | Access Policies



Interface Configuration: Fabric | Access Policies

The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The top navigation bar includes the Cisco logo, the text 'APIC', and several menu items: System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, Operations, Apps, and Apps. Below this, a secondary navigation bar shows Inventory, Fabric Policies, and Access Policies (also highlighted with a red box). On the left side, a 'Policies' sidebar is visible, containing a 'Quick Start' link and a list of policy categories: Switch Policies, Module Policies, Interface Policies, Global Policies, Monitoring Policies, Troubleshoot Policies, Pools, and Physical and External Domains. The main content area is titled 'Quick Start' and is divided into three columns. The 'Summary' column contains two paragraphs of text explaining the role of access policies. The 'Steps' column lists four tasks: 'Configure in-band management access', 'Configure out-of-band management access', 'Create a CDP (or other) interface policy', 'Create a traffic storm control policy', 'Configure an interface, PC, and VPC', 'Configure port security', and 'Monitor access port statistics'. The 'See Also' column lists various links related to interface configuration, including 'Physical Interface (Link Level)', 'CDP', 'LLDP', 'LACP', 'LACP Member', 'Spanning Tree Interface', 'Storm Control', 'Port Security', 'SPAN', 'On-demand Diagnostics', 'Attachable Entity Profile', 'QoS', and 'DHCP Relay'.

Navigation Path: Fabric > Access Policies

Left Sidebar (Policies):

- Quick Start
- Switch Policies
- Module Policies
- Interface Policies
- Global Policies
- Monitoring Policies
- Troubleshoot Policies
- Pools
- Physical and External Domains

Quick Start Section:

Summary

Access policies govern the operation of interfaces that provide external access to the fabric. The system provides default access policies. Access policies enable configuring various functions or protocols. Administrators who have fabric administrator privileges can create new access policies according to their requirements. The APIC enables administrators to select the pods, leaf switches, and interfaces to which they will apply access policies.

Access policies configure external-facing interfaces that do not connect to a spine switch. External-facing interfaces connect to external devices such as virtual machine controllers and hypervisors, hosts, routers, or fabric extenders (FEX). Access policies enable configuring port channels and virtual port channels, protocols such as LLDP, CDP or LACP, and features like monitoring or diagnostics.

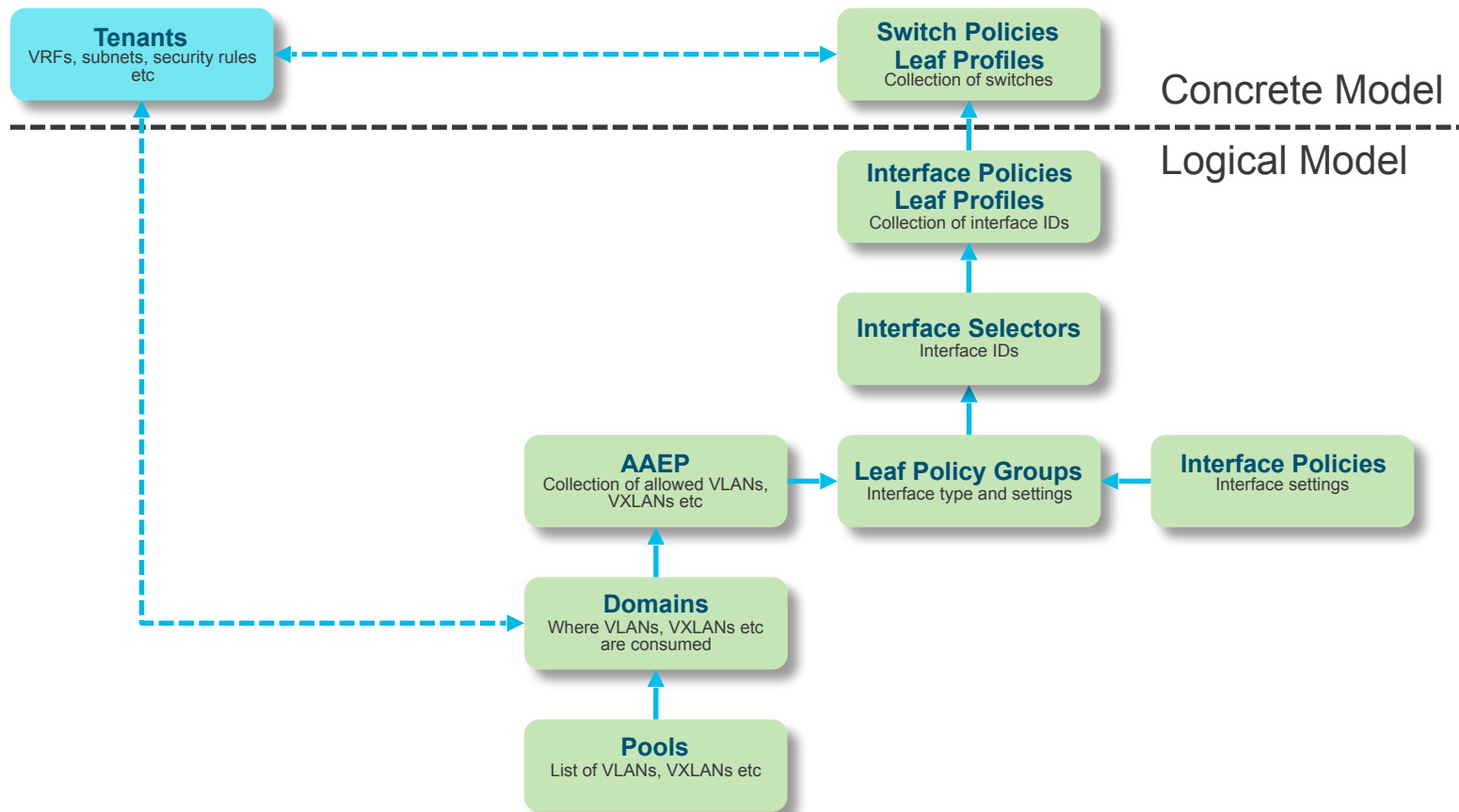
Using the **Configure an interface, PC, and VPC** link below, you can apply a common template to a number of interfaces. We recommend that you create the policies that you will apply, such as CDP or LLDP policies, before launching the wizard. You can also create the policies as you complete the wizard.

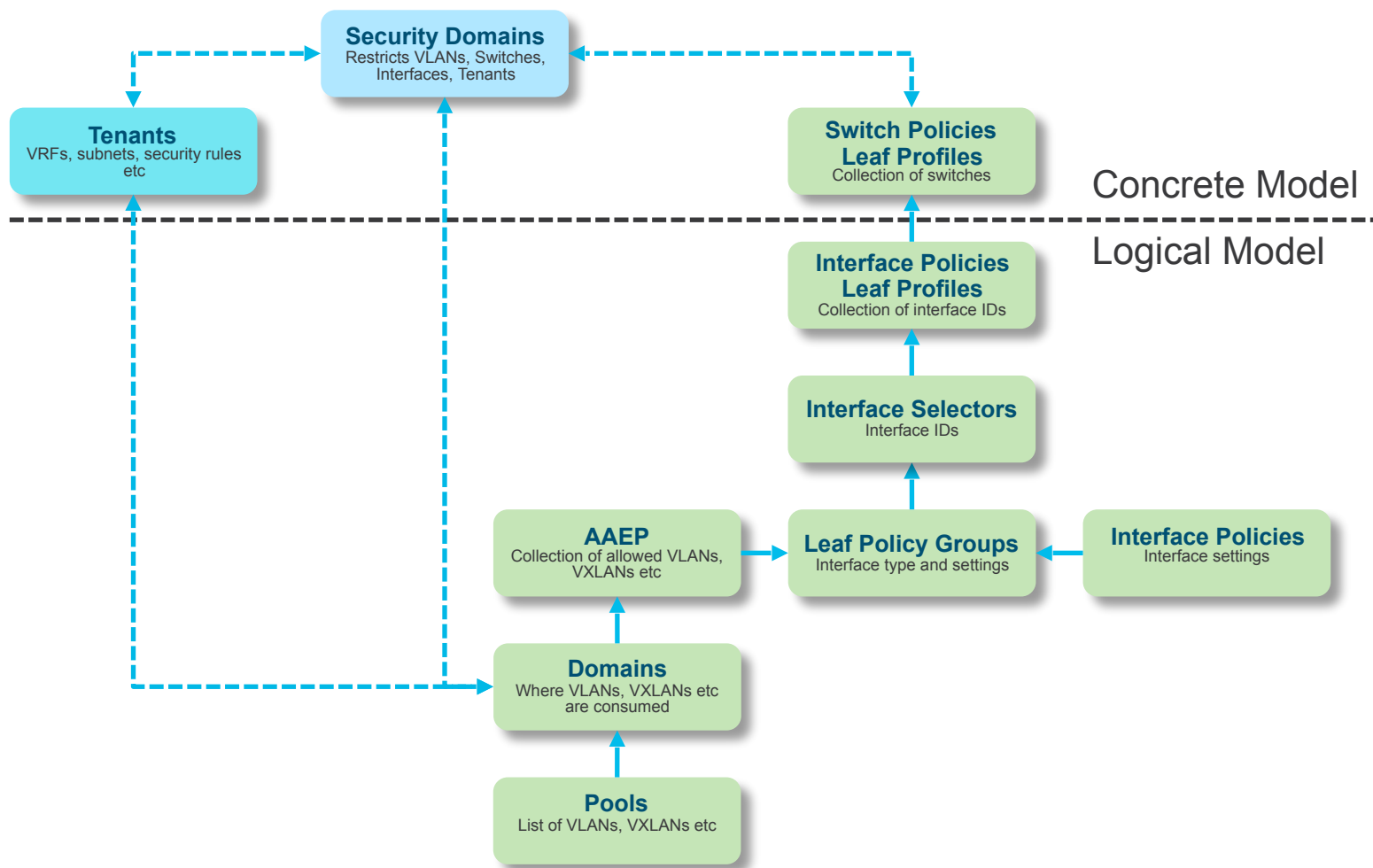
Steps

- Configure in-band management access
- Configure out-of-band management access
- Create a CDP (or other) interface policy
- Create a traffic storm control policy
- Configure an interface, PC, and VPC
- Configure port security
- Monitor access port statistics

See Also

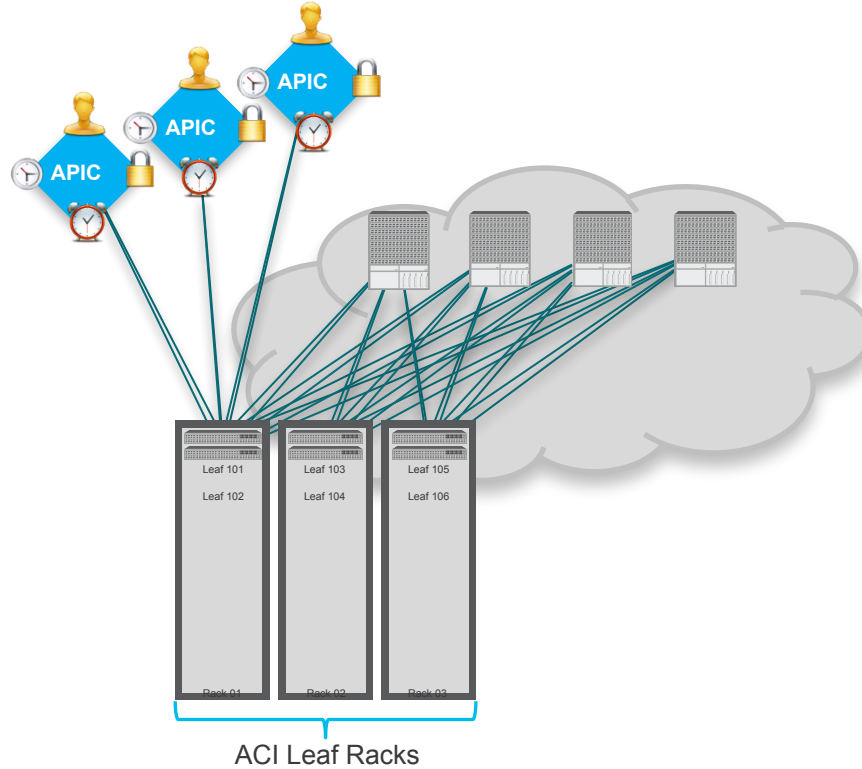
- Physical Interface (Link Level)
- CDP
- LLDP
- LACP
- LACP Member
- Spanning Tree Interface
- Storm Control
- Port Security
- SPAN
- On-demand Diagnostics
- Attachable Entity Profile
- QoS
- DHCP Relay



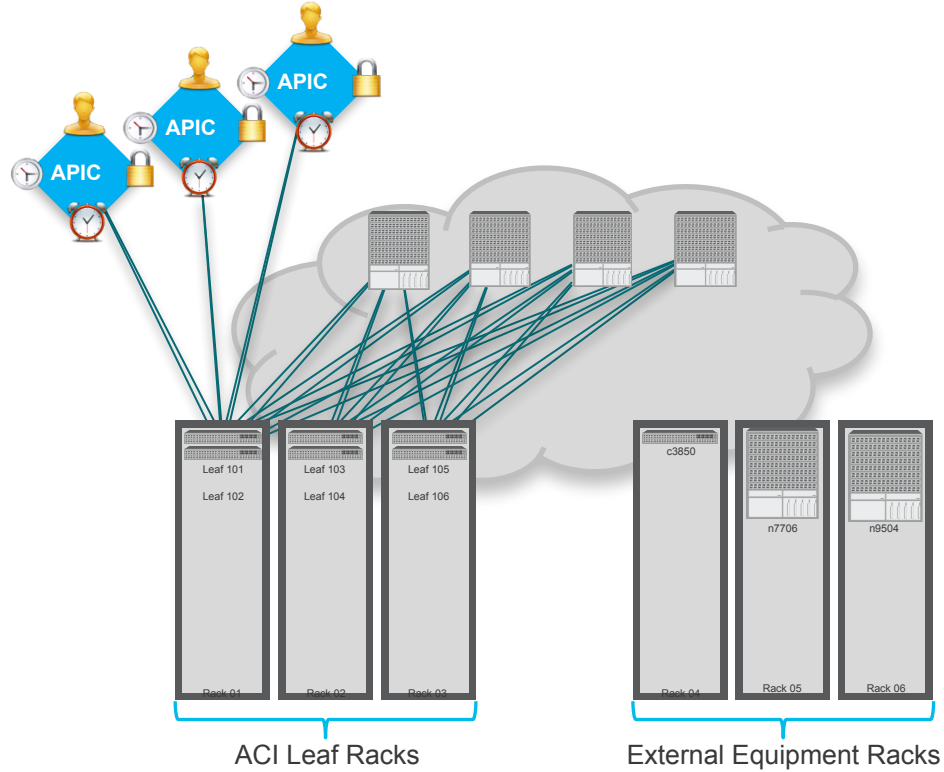


Let's consider a practical example...

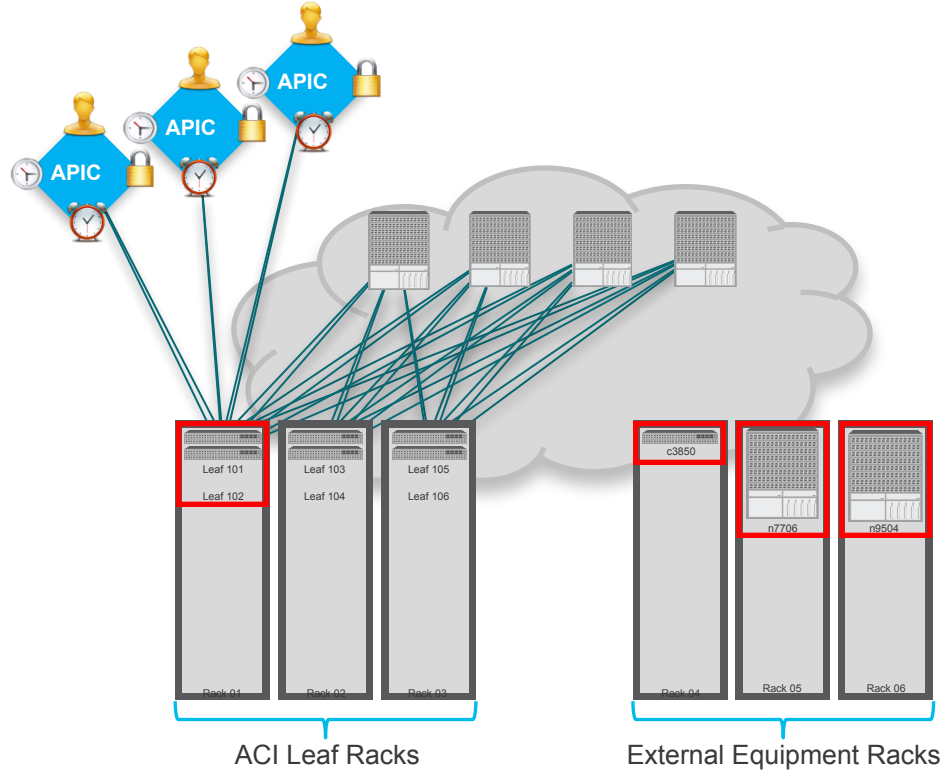
Rack Layout



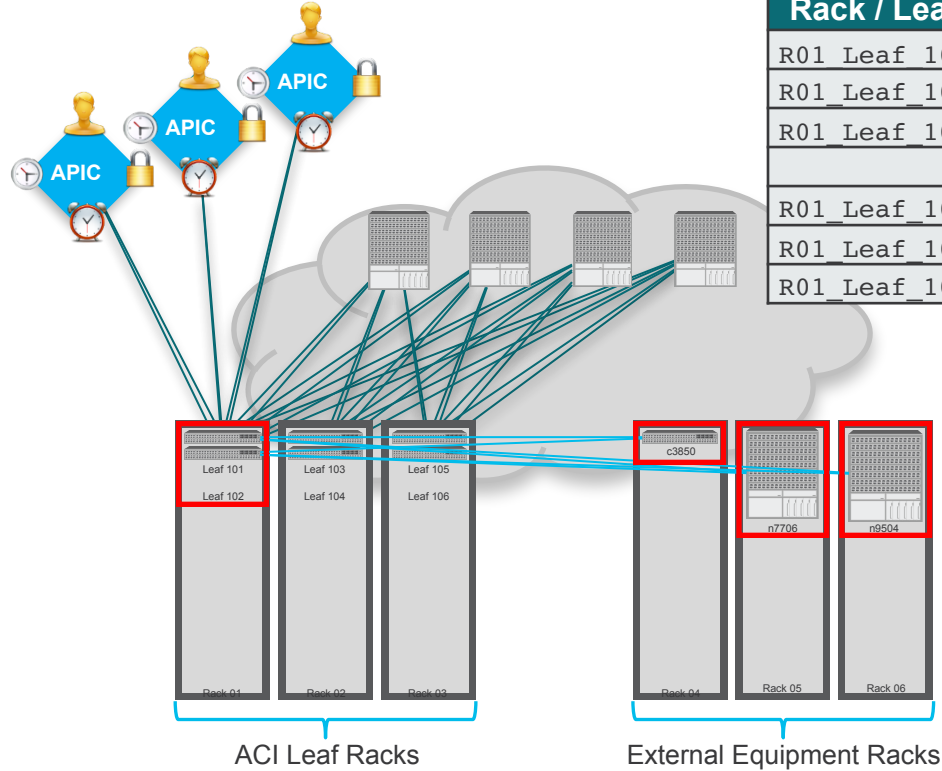
Rack Layout



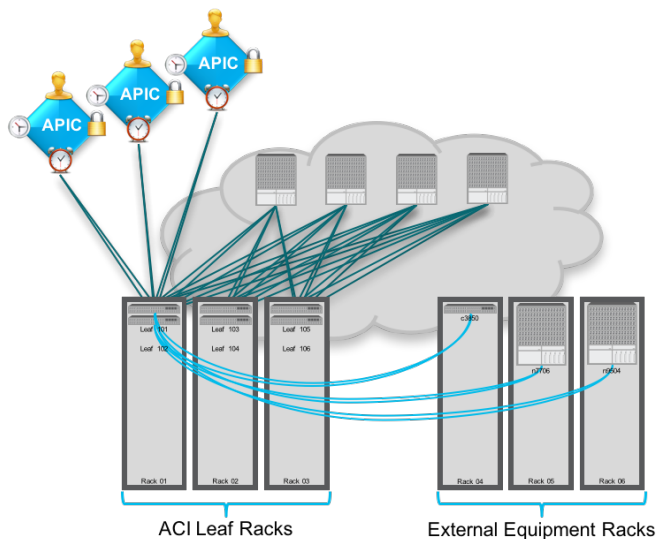
Rack Layout



Rack Layout

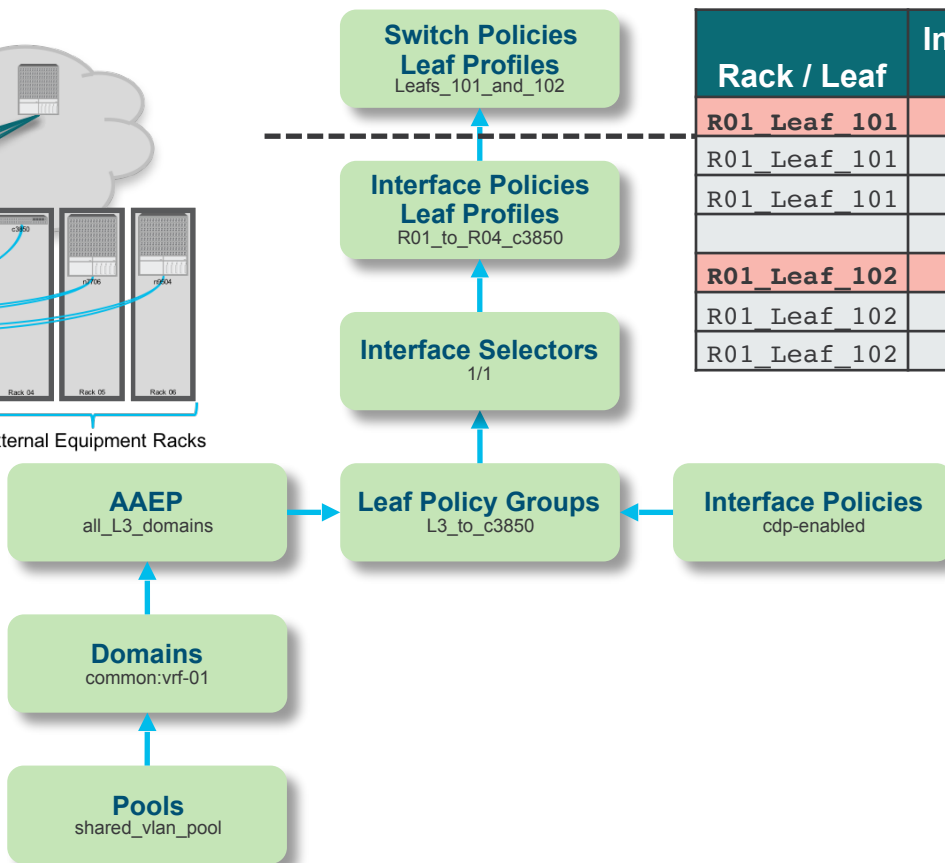


Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

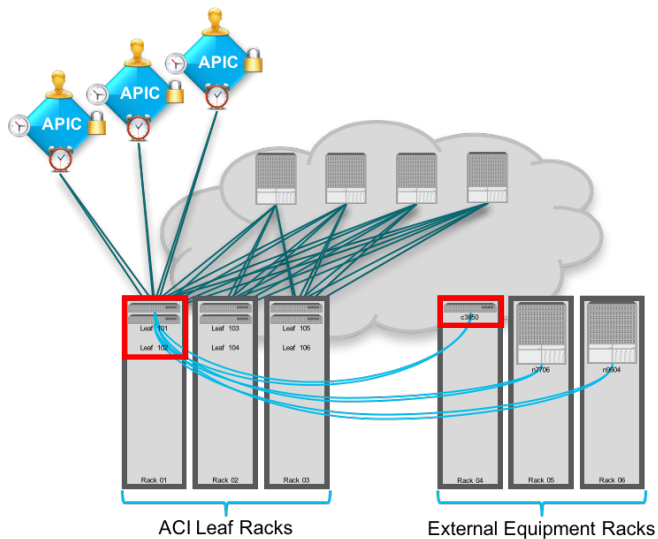


ACI Leaf Racks

External Equipment Racks

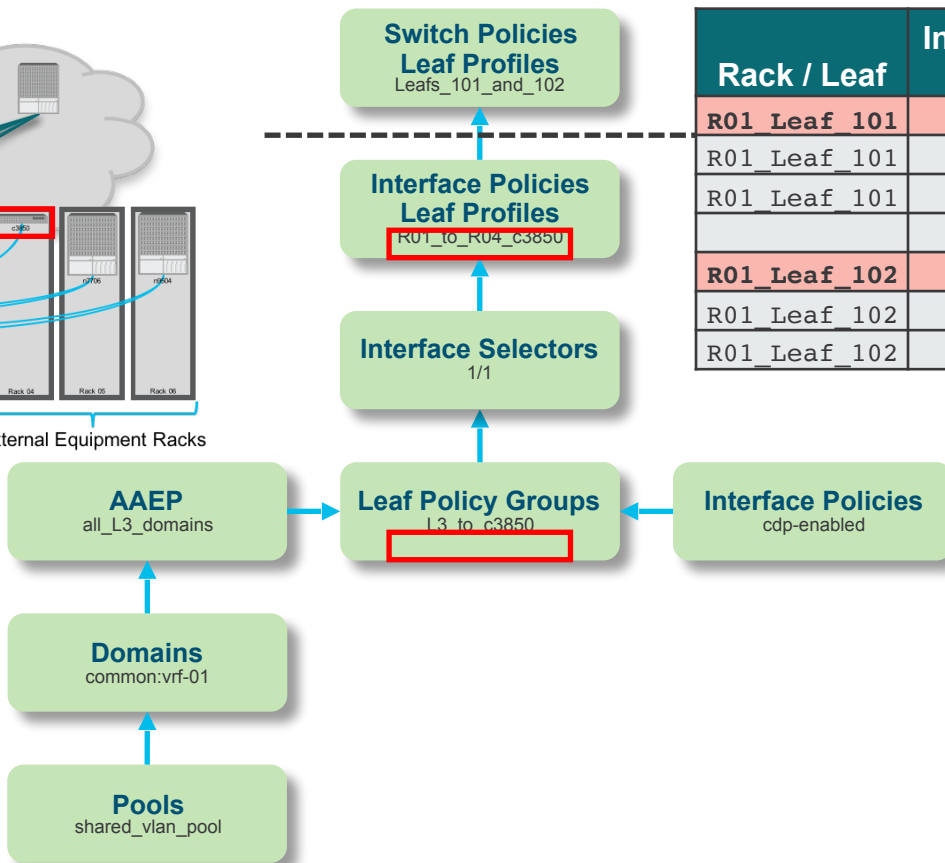


Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

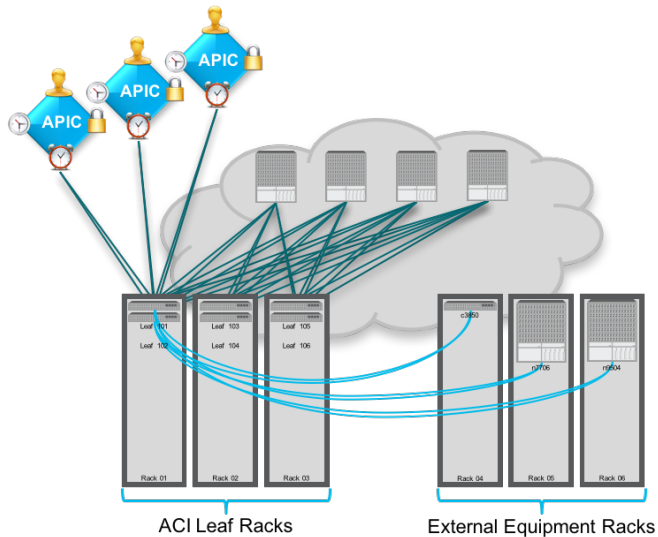


ACI Leaf Racks

External Equipment Racks

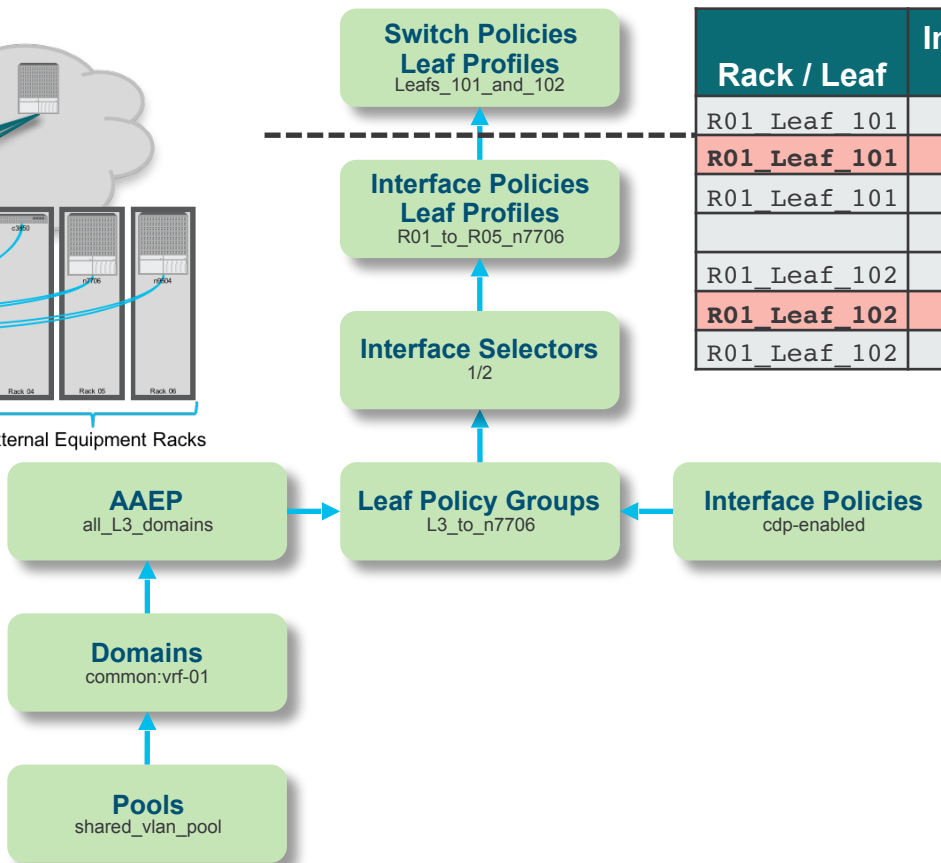


Rack / Leaf	Interface	Rack / Device	Interface
R01 Leaf 101	1/1	R04 c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01 Leaf 102	1/1	R04 c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

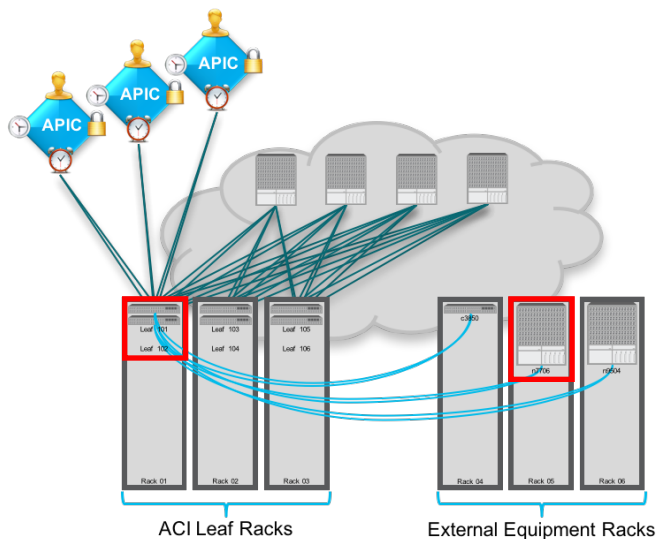


ACI Leaf Racks

External Equipment Racks

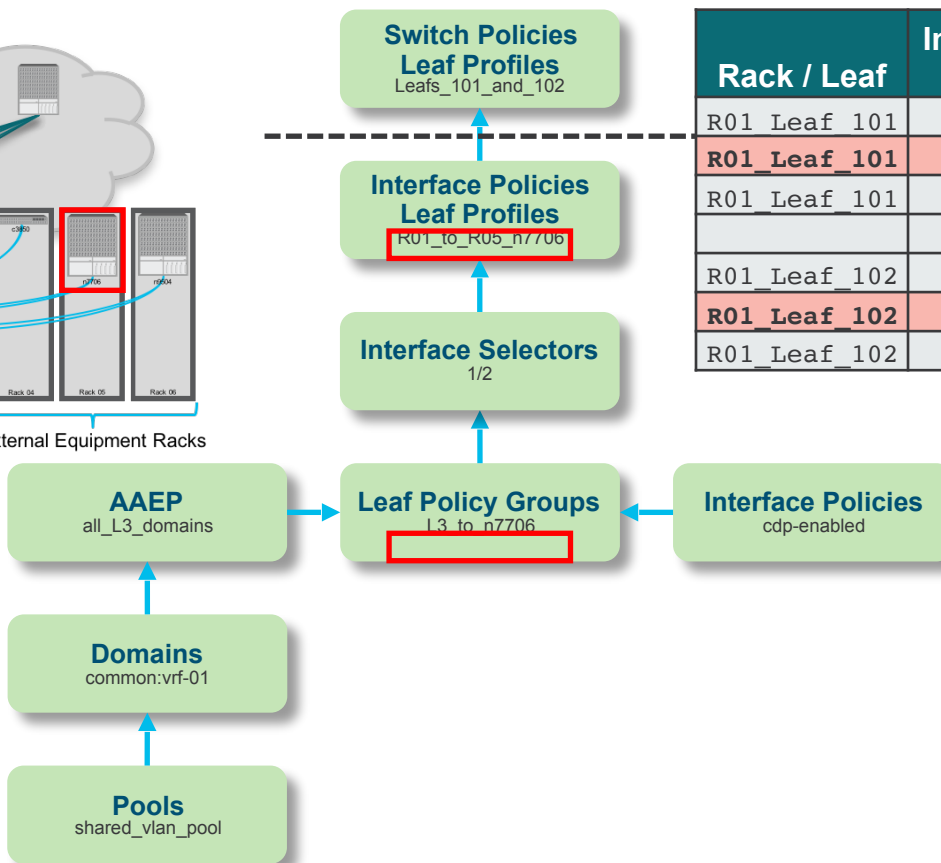


Rack / Leaf	Interface	Rack / Device	Interface
R01 Leaf 101	1/1	R04 c3850	1/1
R01 Leaf 101	1/2	R05 n7706	1/1
R01 Leaf 101	1/3	R06 n9504	1/1
R01 Leaf 102	1/1	R04 c3850	1/2
R01 Leaf 102	1/2	R05 n7706	1/2
R01 Leaf 102	1/3	R06 n9504	1/2

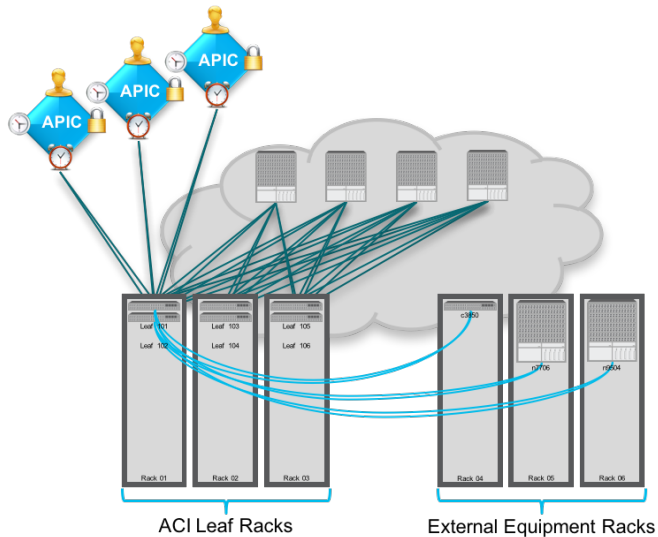


ACI Leaf Racks

External Equipment Racks

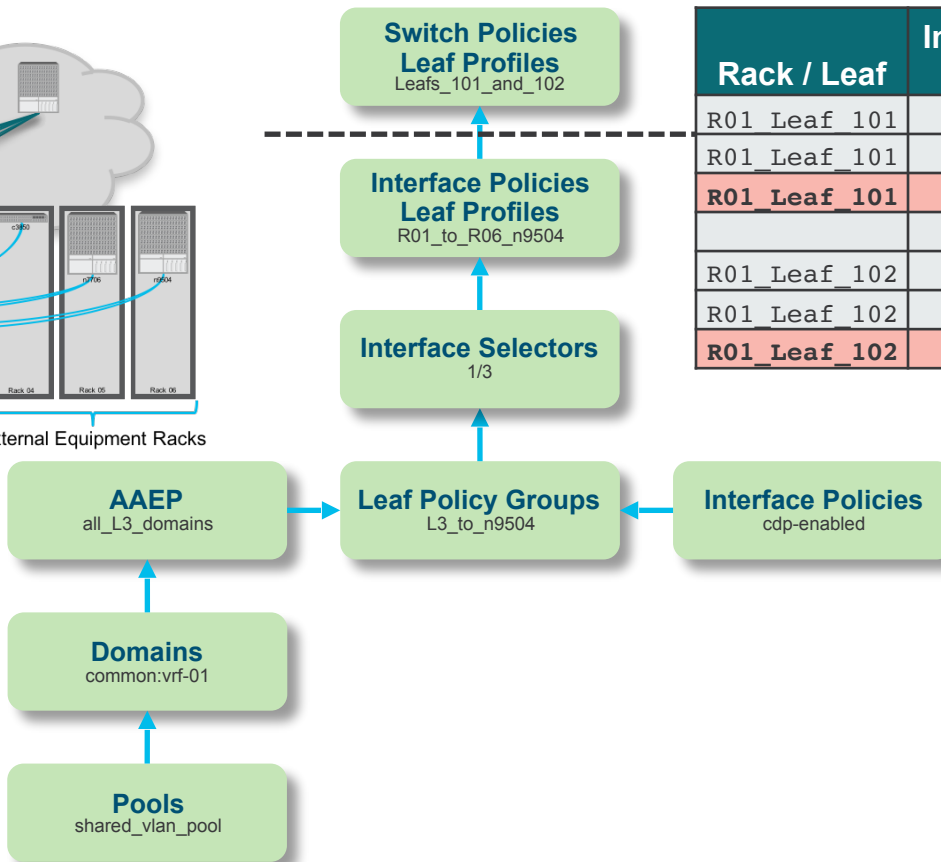


Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

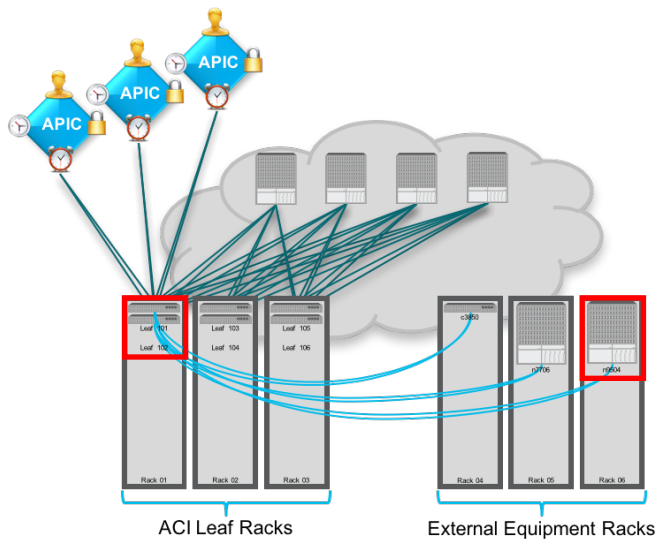


ACI Leaf Racks

External Equipment Racks

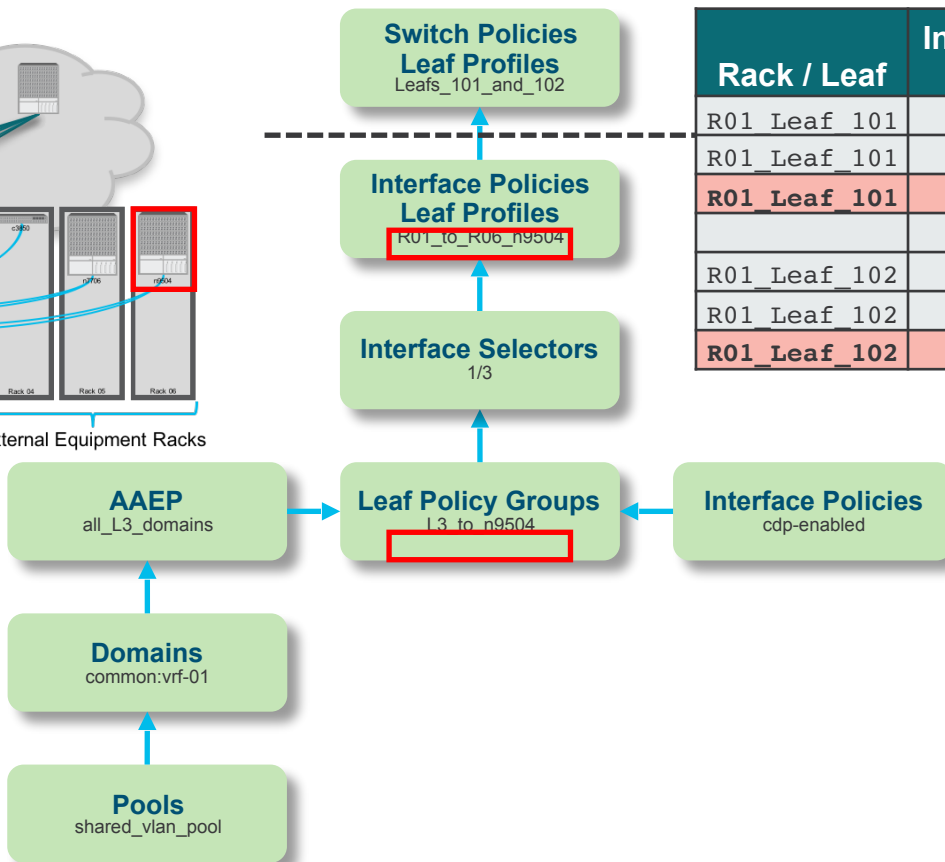


Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

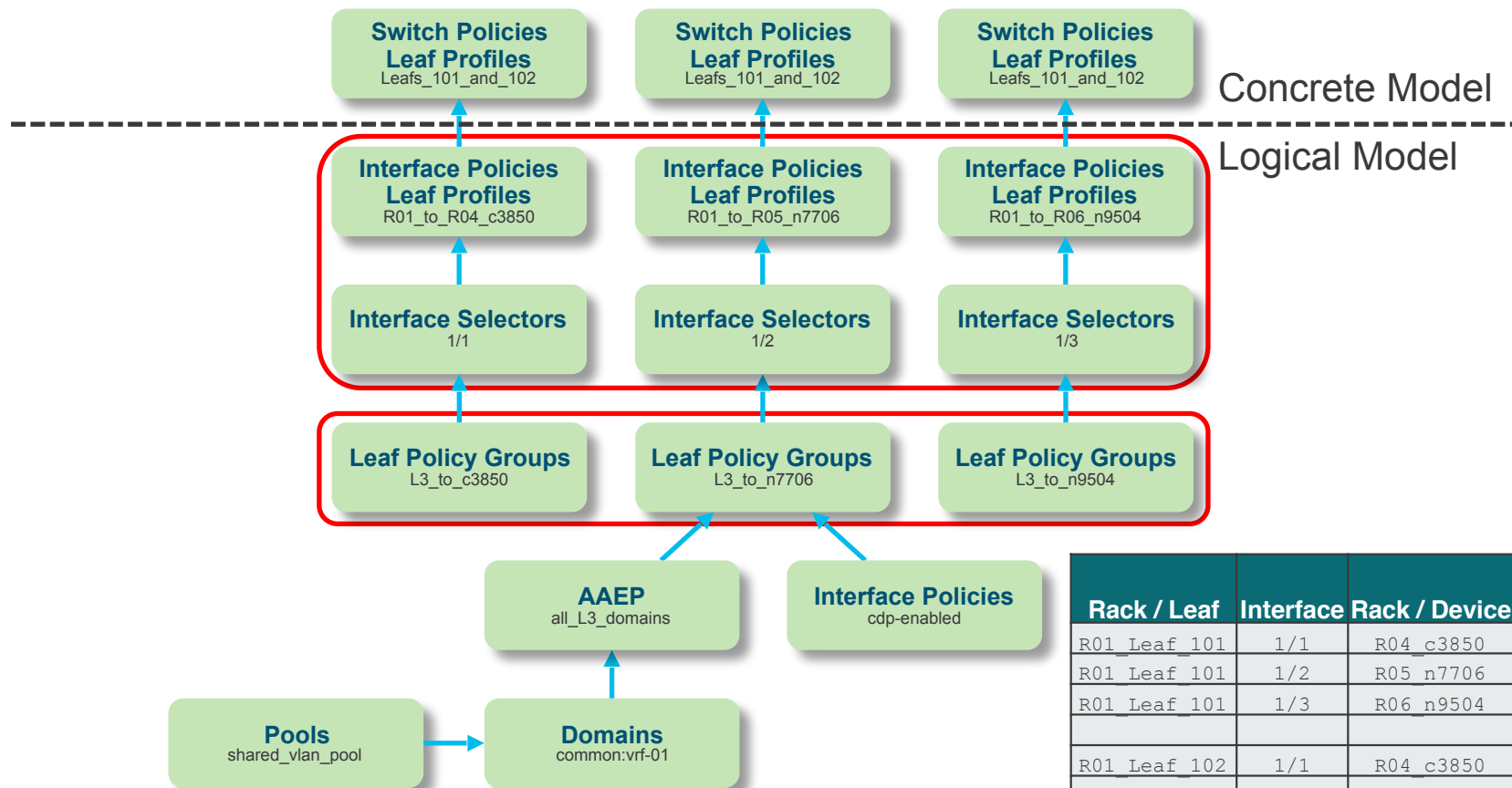


ACI Leaf Racks

External Equipment Racks

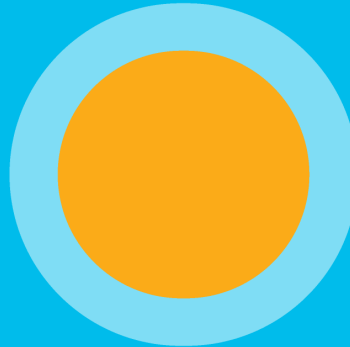


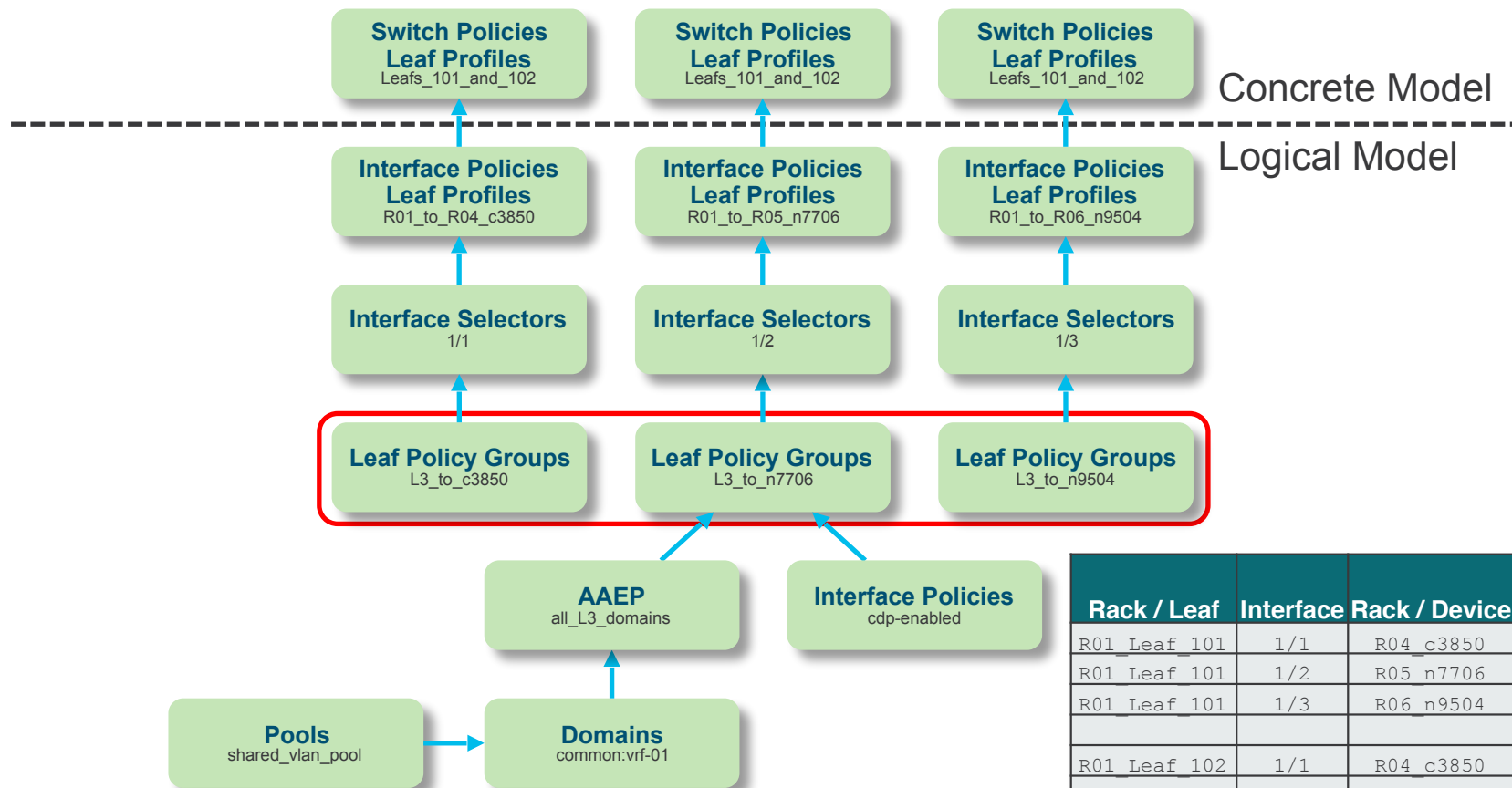
Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2



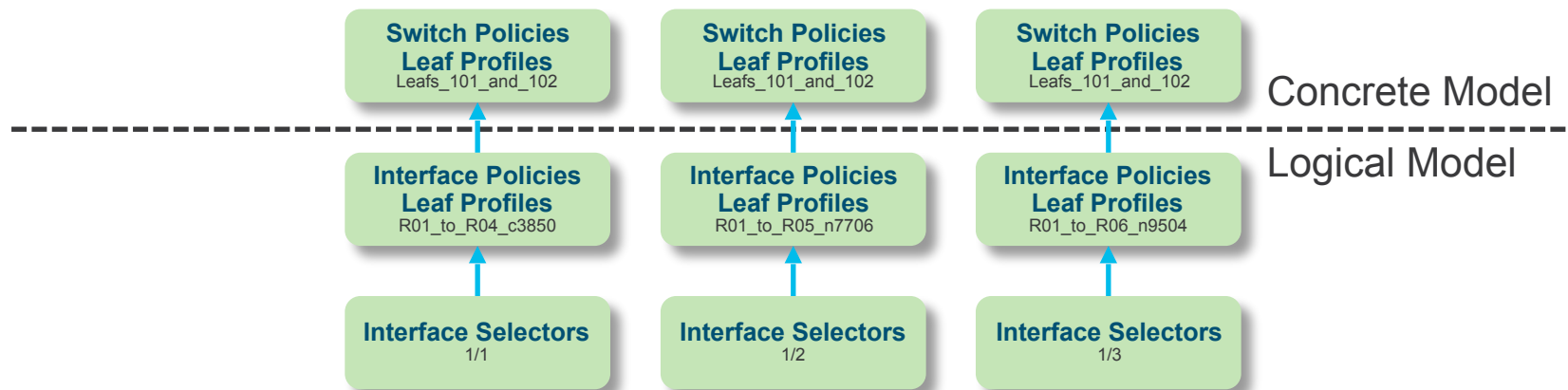
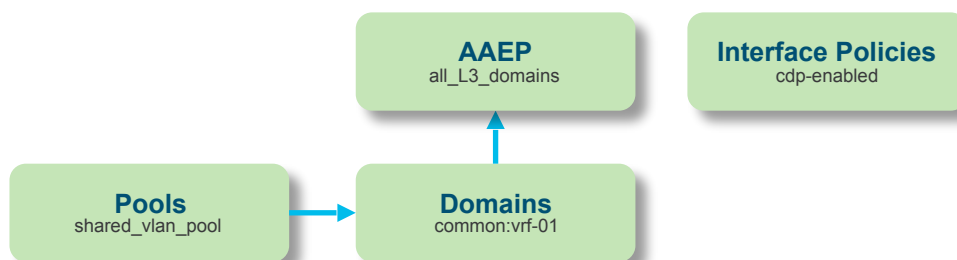
Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

Couldn't we reduce the number of Interface Policy Groups?

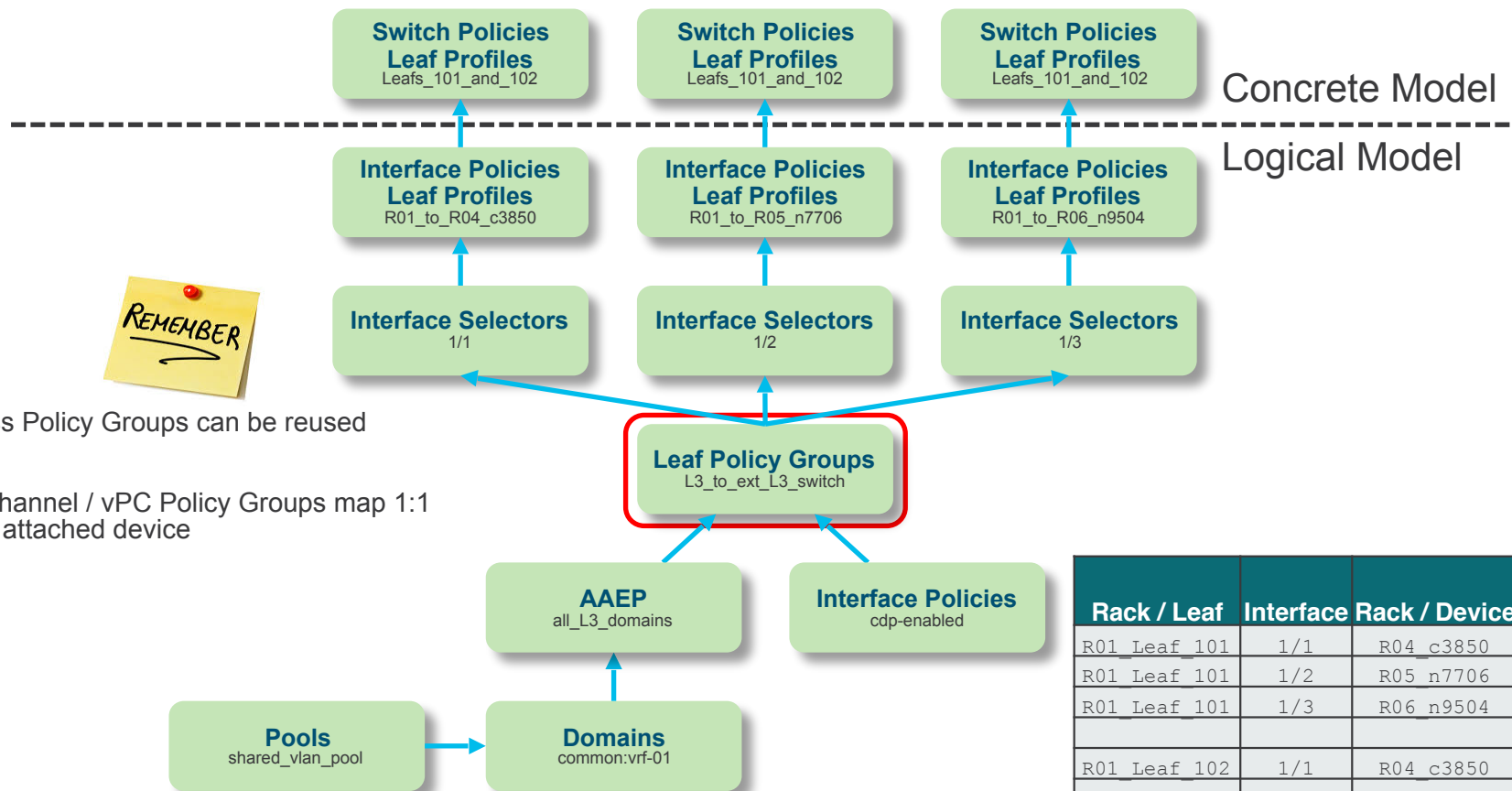




Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2



Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

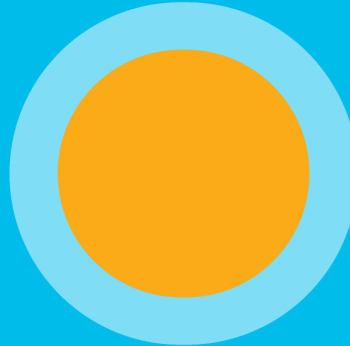


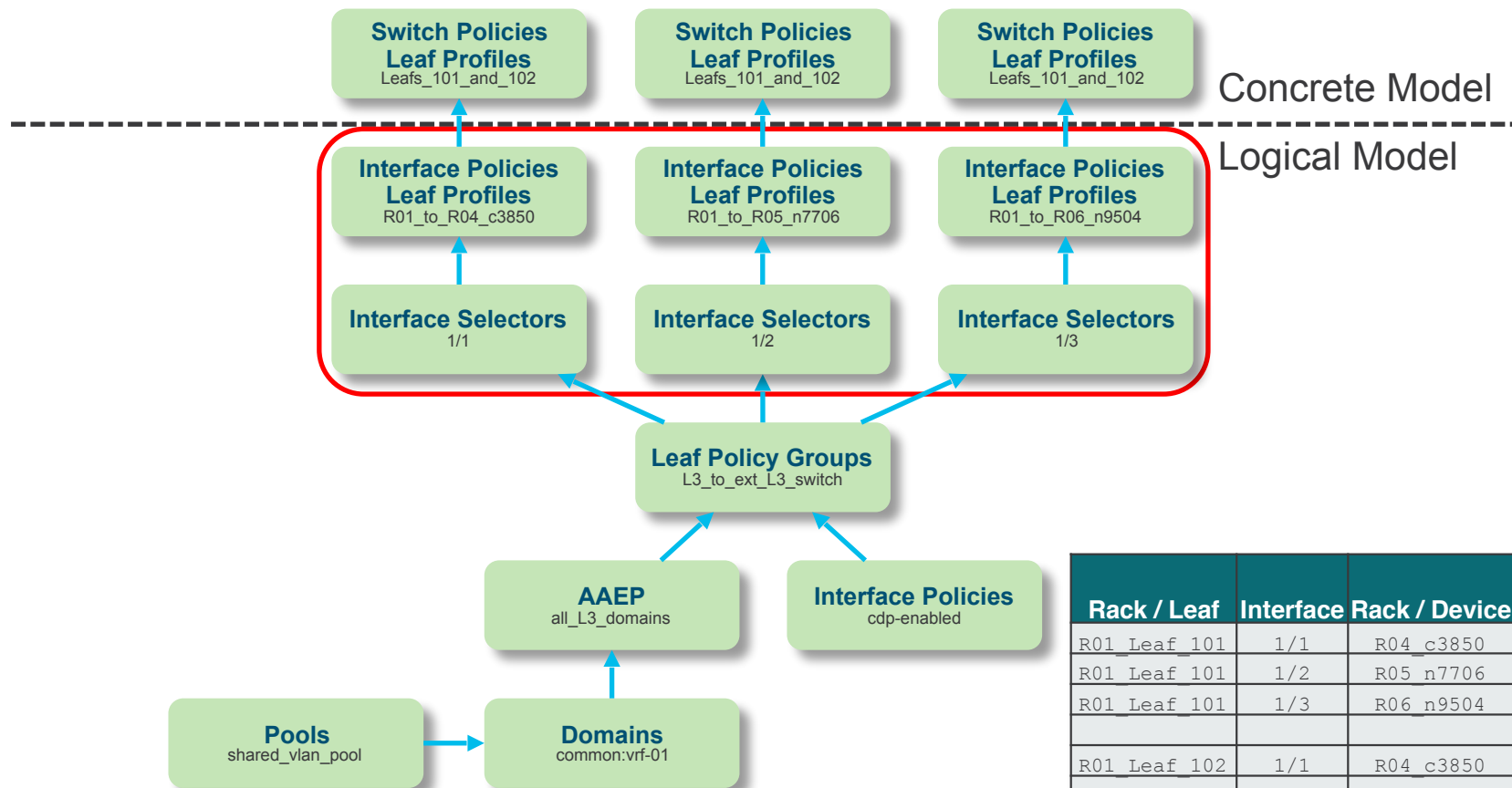
Access Policy Groups can be reused

Port channel / vPC Policy Groups map 1:1 to the attached device

Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

Couldn't we reduce the number of Leaf Profiles?

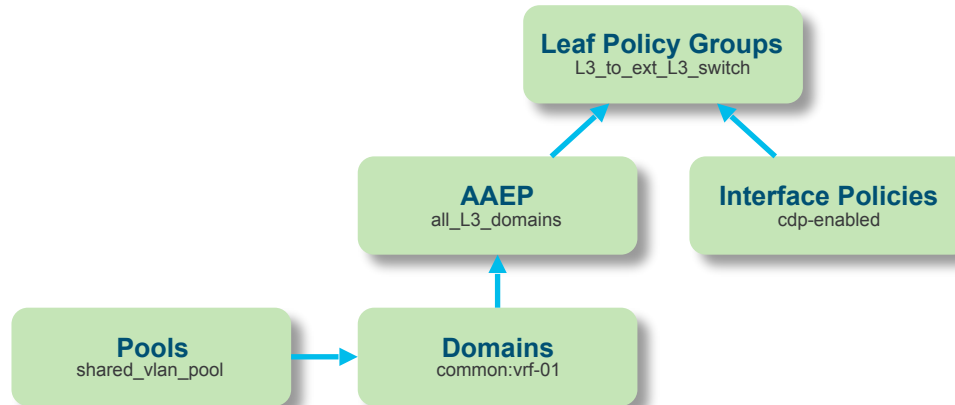




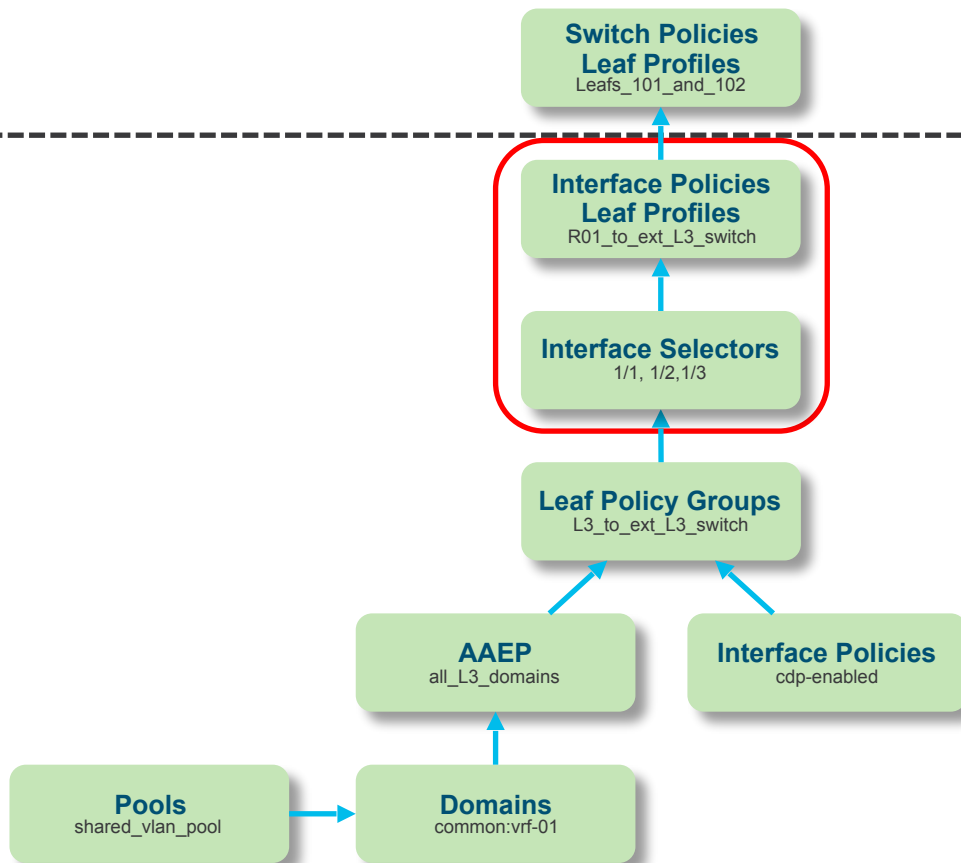
Rack / Leaf	Interface	Rack / Device	Interface
R01 Leaf 101	1/1	R04 c3850	1/1
R01 Leaf 101	1/2	R05 n7706	1/1
R01 Leaf 101	1/3	R06 n9504	1/1
R01 Leaf 102	1/1	R04 c3850	1/2
R01 Leaf 102	1/2	R05 n7706	1/2
R01 Leaf 102	1/3	R06 n9504	1/2

Concrete Model

Logical Model



Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

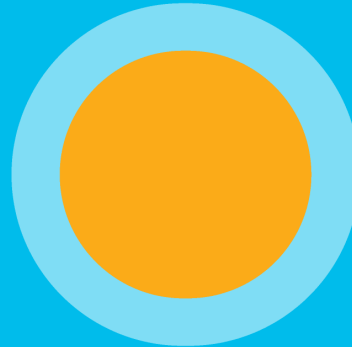


Concrete Model

Logical Model

Rack / Leaf	Interface	Rack / Device	Interface
R01_Leaf_101	1/1	R04_c3850	1/1
R01_Leaf_101	1/2	R05_n7706	1/1
R01_Leaf_101	1/3	R06_n9504	1/1
R01_Leaf_102	1/1	R04_c3850	1/2
R01_Leaf_102	1/2	R05_n7706	1/2
R01_Leaf_102	1/3	R06_n9504	1/2

How should we use Leaf Profiles?



Device Centric Model

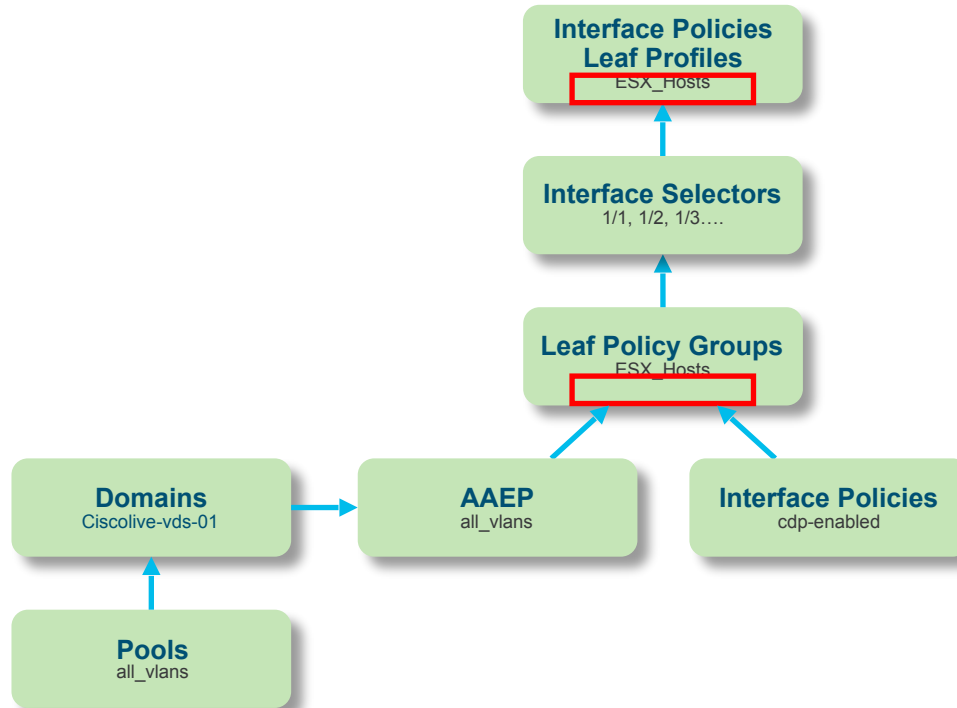
Concrete Model

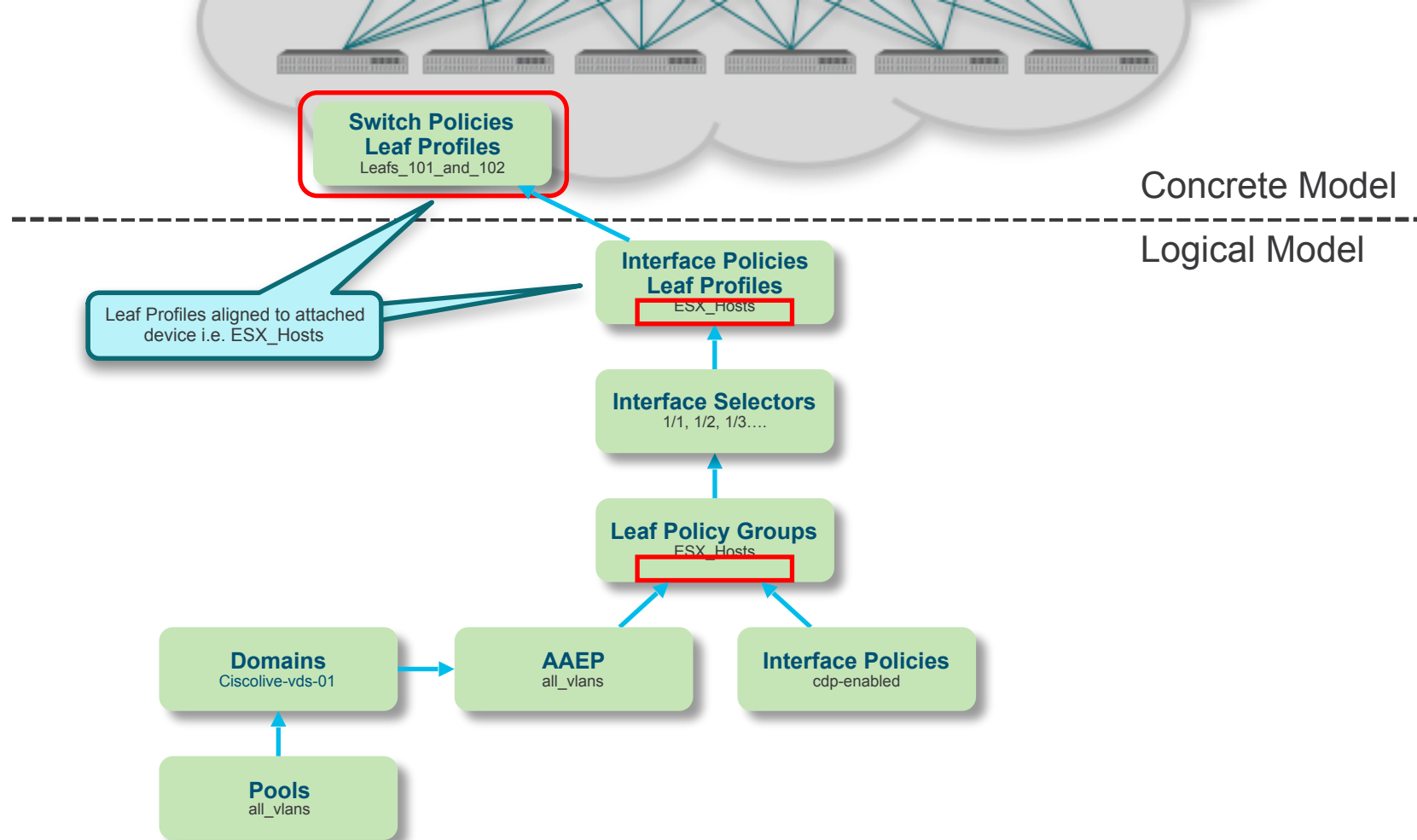
Logical Model

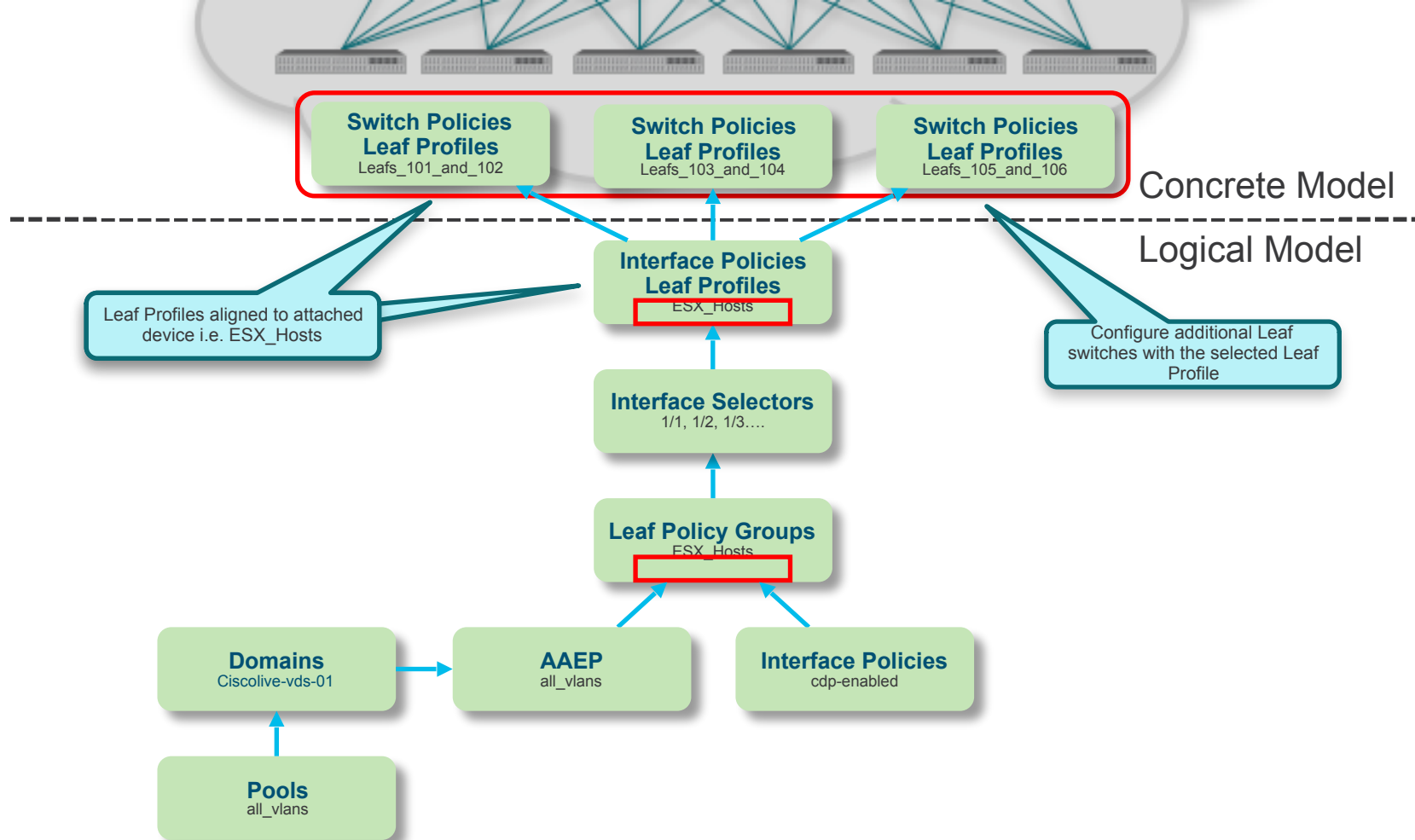
Device Centric Model

Concrete Model

Logical Model

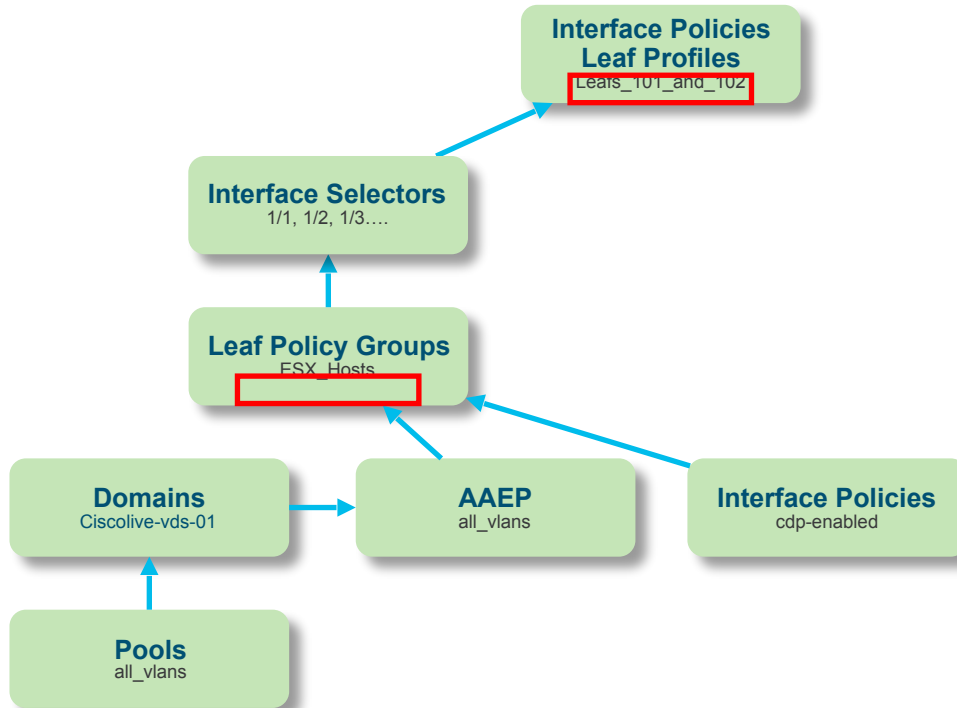


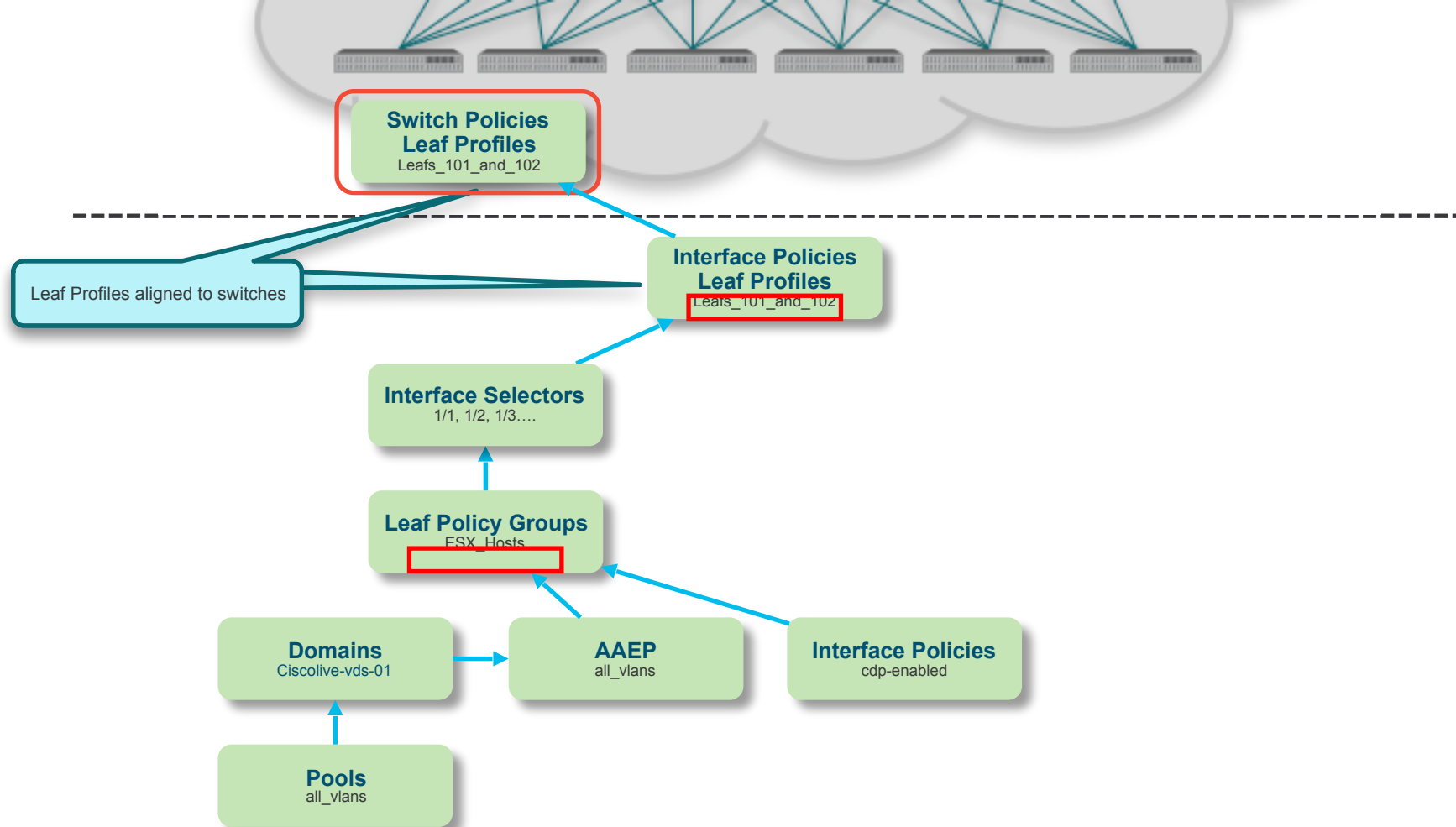


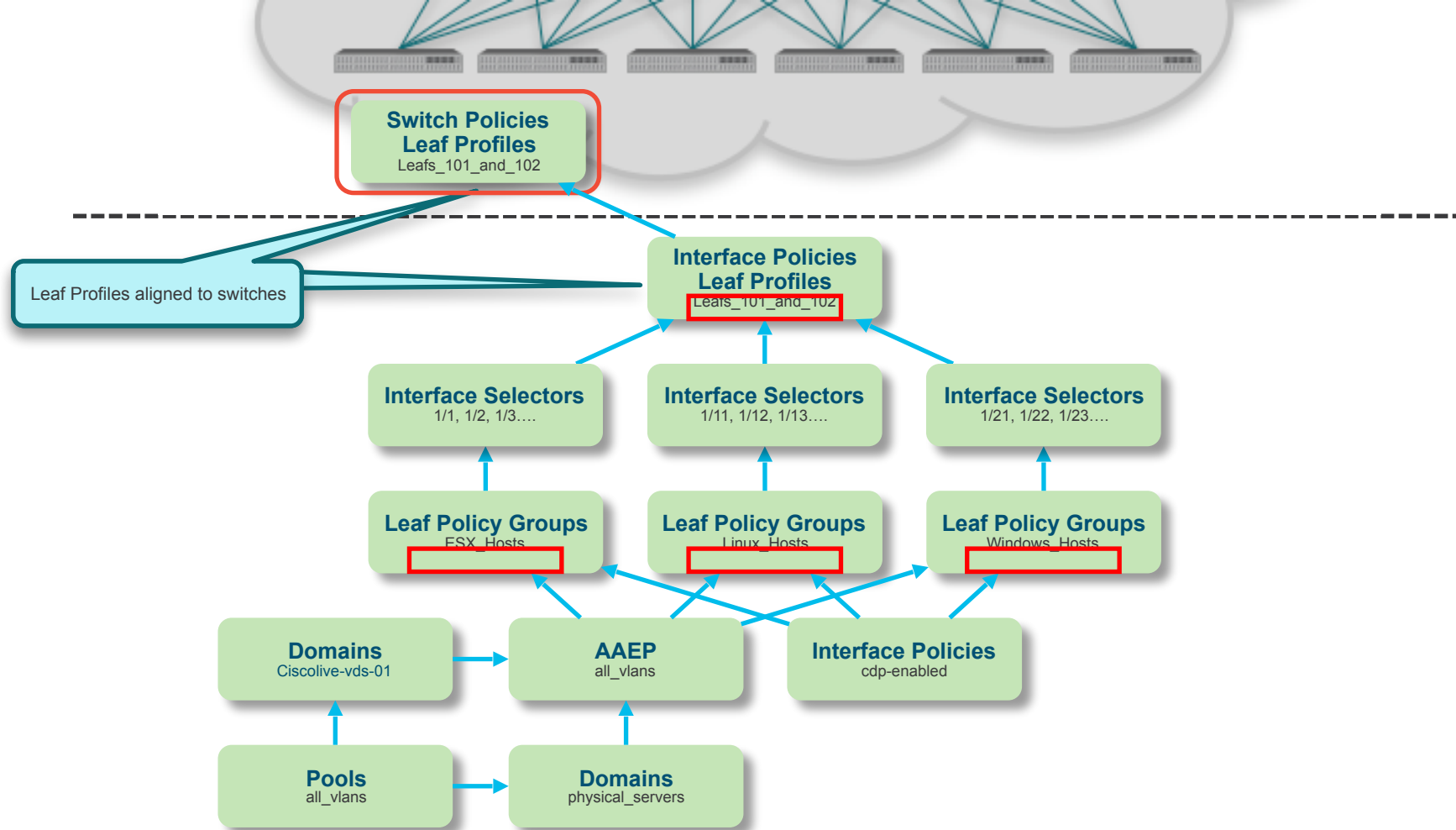


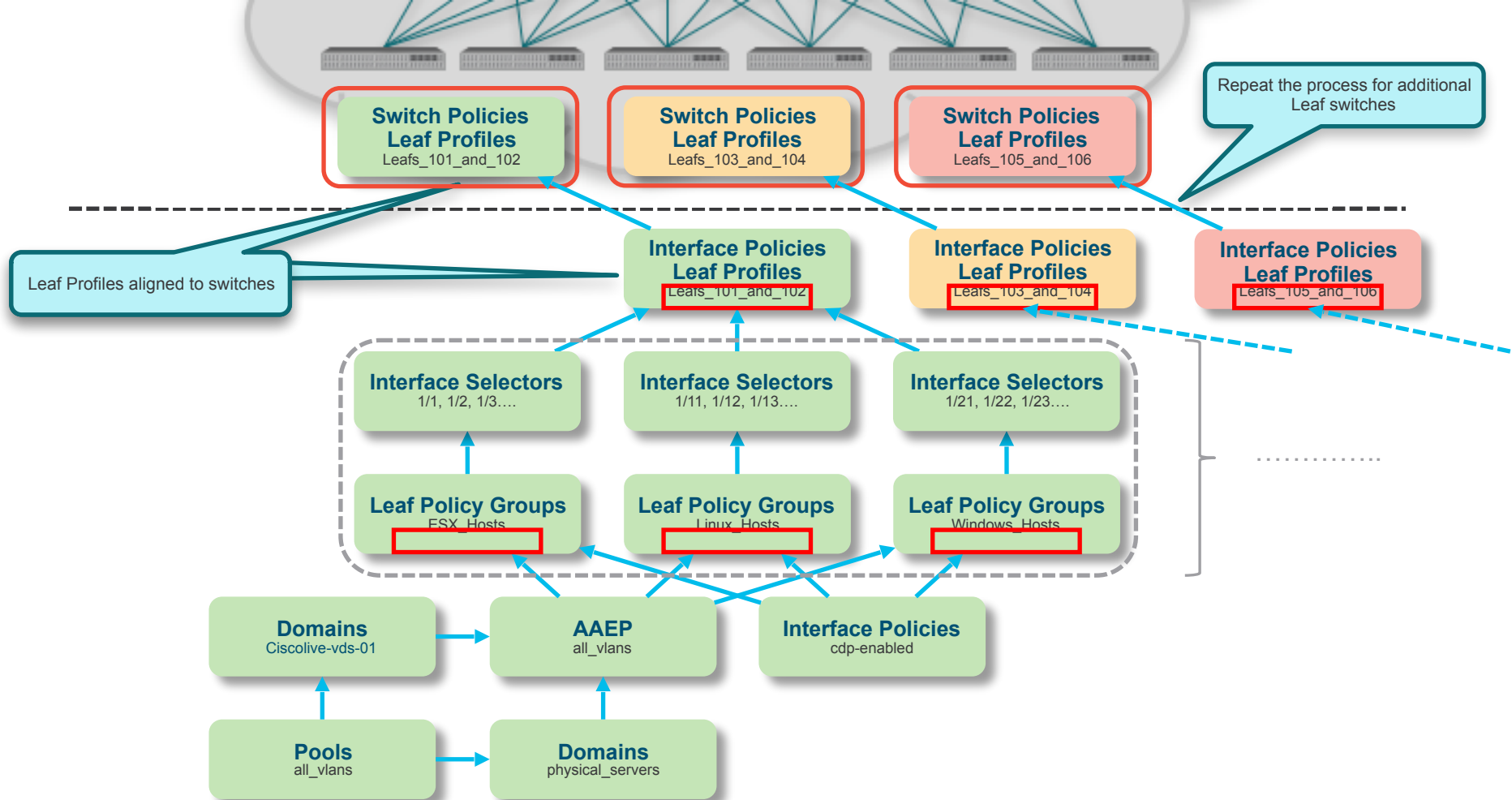
Switch Centric Model

Switch Centric Model









It's not an either/or method, both methods can be used at the same time...



Access Policy Groups can be reused ...
Port channel / vPC Policy Groups create unique port channel IDs

Let's use the network
interfaces....!

ACI Consumption Model

Interface Configuration

Fabric | Access Policies

- VLANs
- Domains
- AAEP
- Interface Policies
- Leaf Policy Groups
- Leaf Profiles
- Switch Profiles

Policies



Quick Start

- > Switch Policies
- > Module Policies
- > Interface Policies
- > Global Policies
- > Monitoring Policies
- > Troubleshoot Policies
- > Pools
- > Physical and External Domains

Interface Consumption

Tenants

- Tenants
- VRFs
- Route Leaking
- L2/L3out
- Bridge Domains
- EPGs
- Contracts

Tenant CiscoLive



Quick Start

- > Tenant CiscoLive
 - > Application Profiles
 - > Networking
 - > L4-L7 Service Parameters
 - > DNS Server Groups (Beta)
 - > Security Policies
 - > Troubleshoot Policies
 - > Monitoring Policies
 - > L4-L7 Services
 - > NetFlow

ACI Consumption Model

Interface Configuration

Fabric | Access Policies

- VLANs
- Domains
- AAEP
- Interface Policies
- Leaf Policy Groups
- Leaf Profiles
- Switch Profiles

Policies



Quick Start

- > Switch Policies
- > Module Policies
- > Interface Policies
- > Global Policies
- > Monitoring Policies
- > Troubleshoot Policies
- > Pools
- > Physical and External Domains

Interface Consumption

Tenants

- Tenants
- VRFs
- Route Leaking
- L2/L3out
- Bridge Domains
- EPGs
- Contracts

Tenant CiscoLive

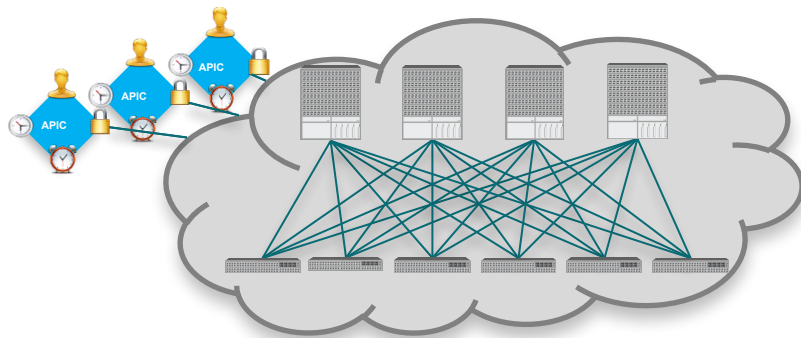


Quick Start

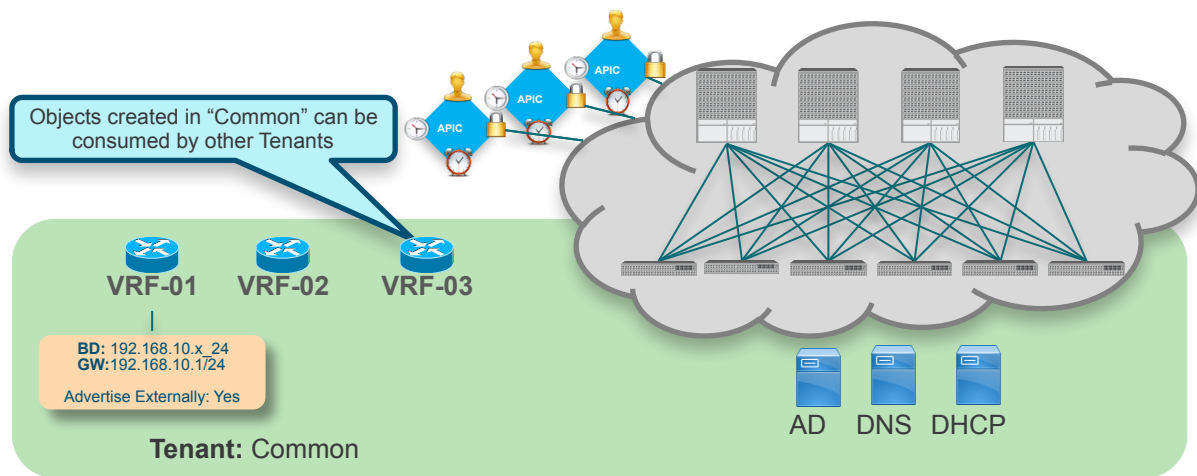
- ✓ Tenant CiscoLive
 - > Application Profiles
 - > Networking
 - L4-L7 Service Parameters
 - > DNS Server Groups (Beta)
 - > Security Policies
 - > Troubleshoot Policies
 - > Monitoring Policies
 - > L4-L7 Services
 - > NetFlow

Tenants

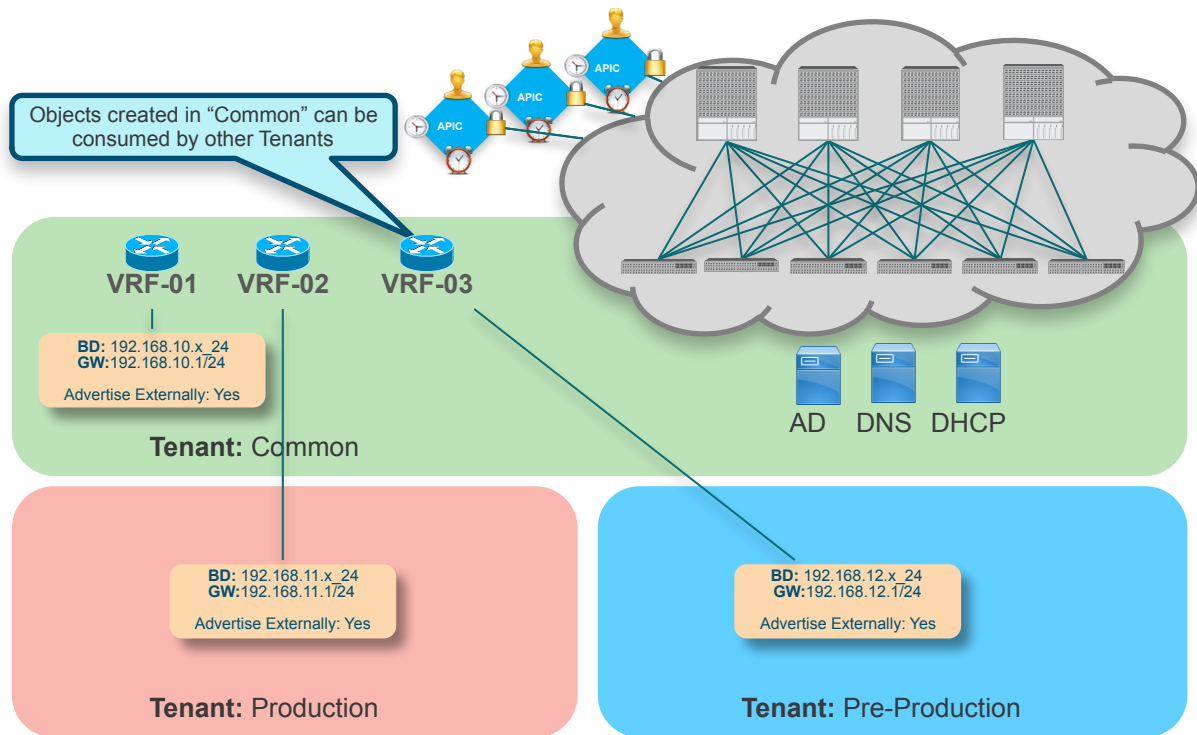
Tenants: Isolated configuration “zones” on common physical infrastructure



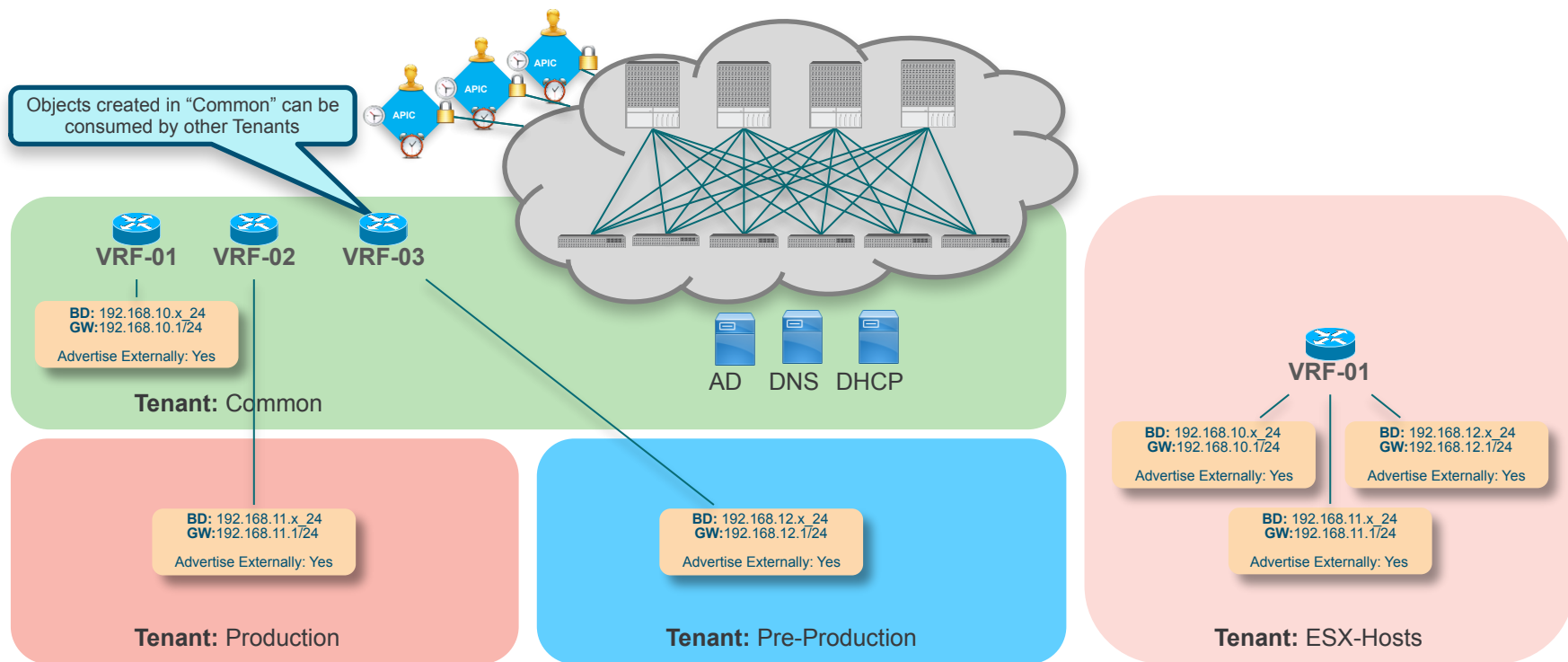
Tenants: Isolated configuration “zones” on common physical infrastructure



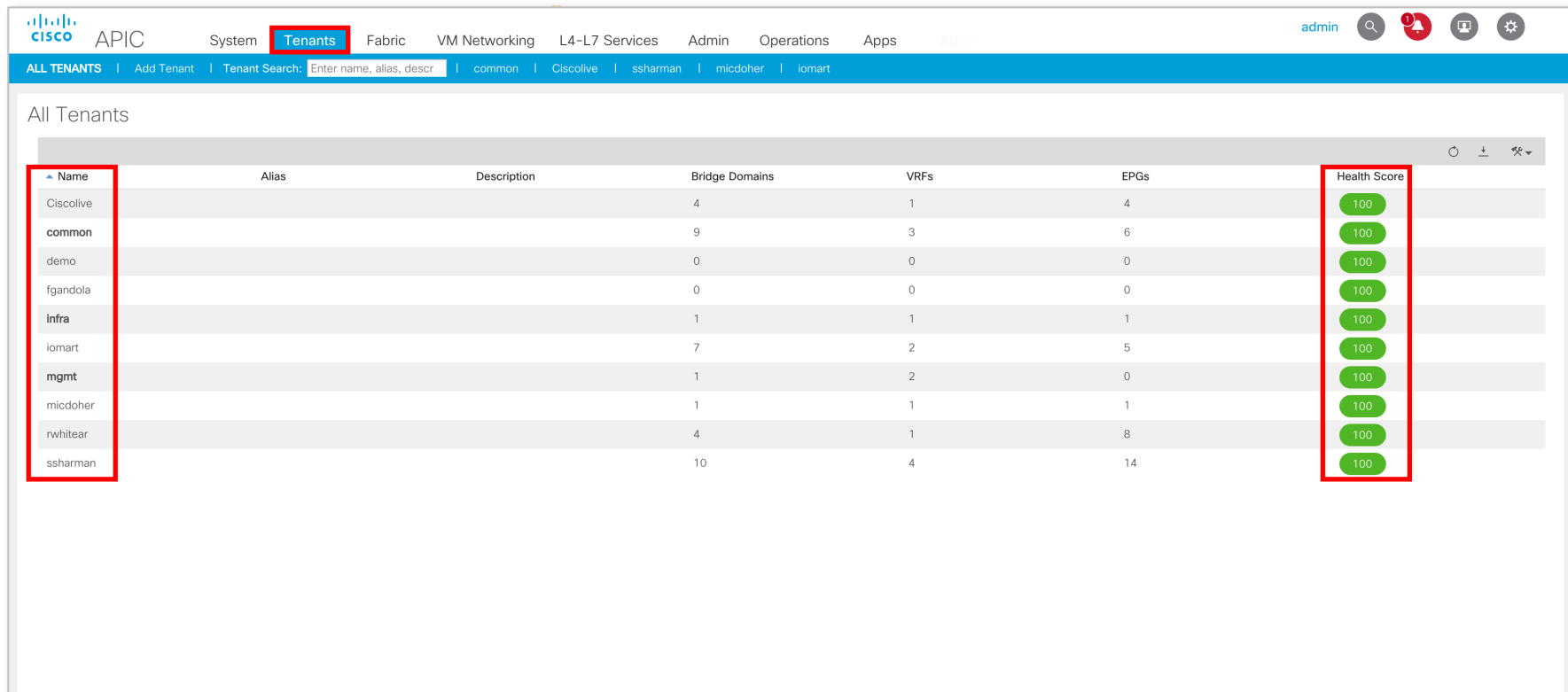
Tenants: Isolated configuration “zones” on common physical infrastructure



Tenants: Isolated configuration “zones” on common physical infrastructure



Tenants: Isolated configuration “zones” on common physical infrastructure



APIC

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

ALL TENANTS | Add Tenant | Tenant Search: Enter name, alias, descr | common | Ciscolive | ssharman | micdoher | iomart

All Tenants

Name	Alias	Description	Bridge Domains	VRFs	EPGs	Health Score
Ciscolive			4	1	4	100
common			9	3	6	100
demo			0	0	0	100
fgandola			0	0	0	100
infra			1	1	1	100
iomart			7	2	5	100
mgmt			1	2	0	100
micdoher			1	1	1	100
rwhitear			4	1	8	100
ssharmar			10	4	14	100

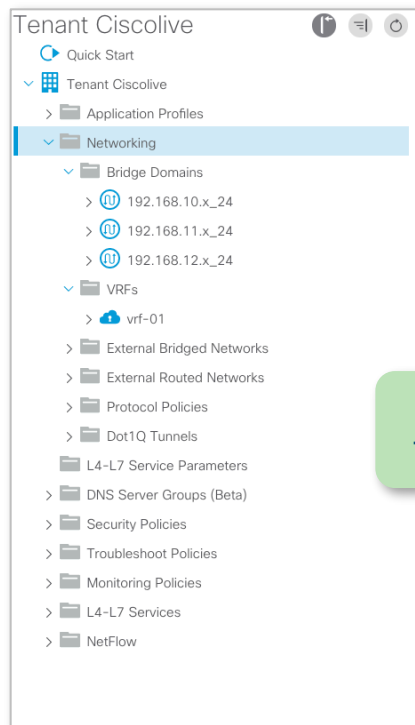
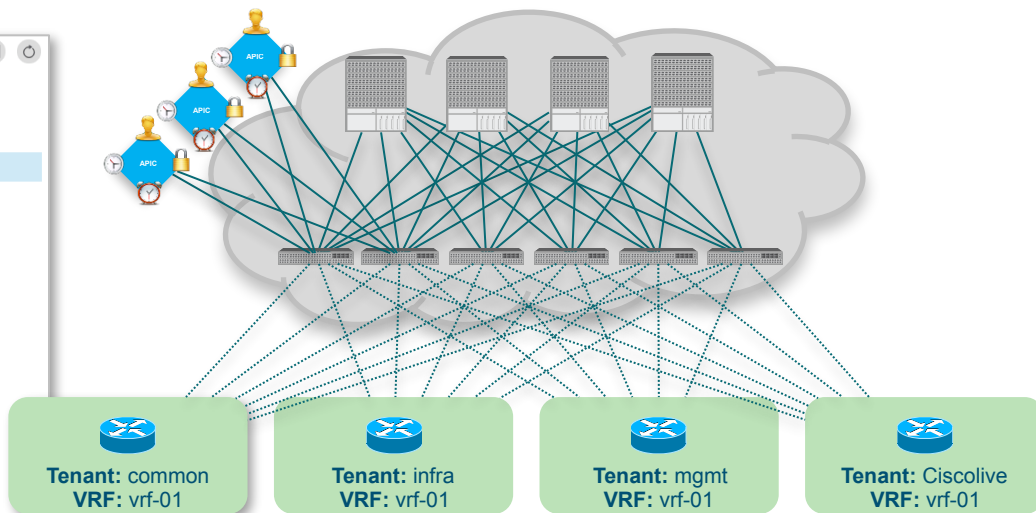
Looking under the covers at Tenants

```
apic1# show running-config tenant Ciscolive
# Command: show running-config tenant Ciscolive
# Time: Tue Jan 30 13:47:50 2018
tenant Ciscolive
  vrf context vrf-01
  exit
  bridge-domain 192.168.10.x_24
  vrf member vrf-01
  exit
  bridge-domain 192.168.11.x_24
  vrf member vrf-01
  exit
  bridge-domain 192.168.12.x_24
  vrf member vrf-01
  exit
  bridge-domain vlan-501
  arp flooding
  l2-unknown-unicast flood
  no unicast routing
  vrf member vrf-01
  exit
```

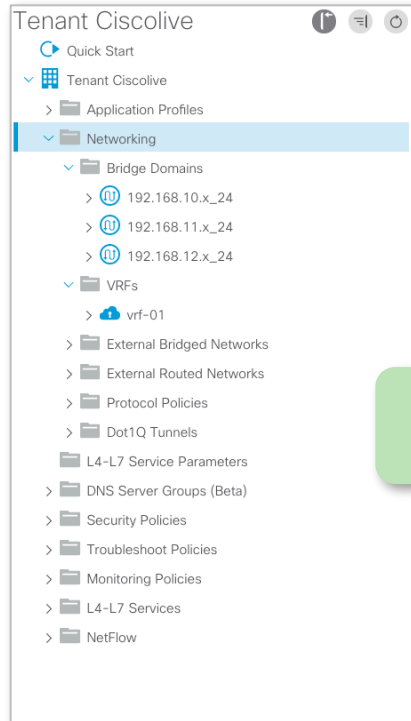
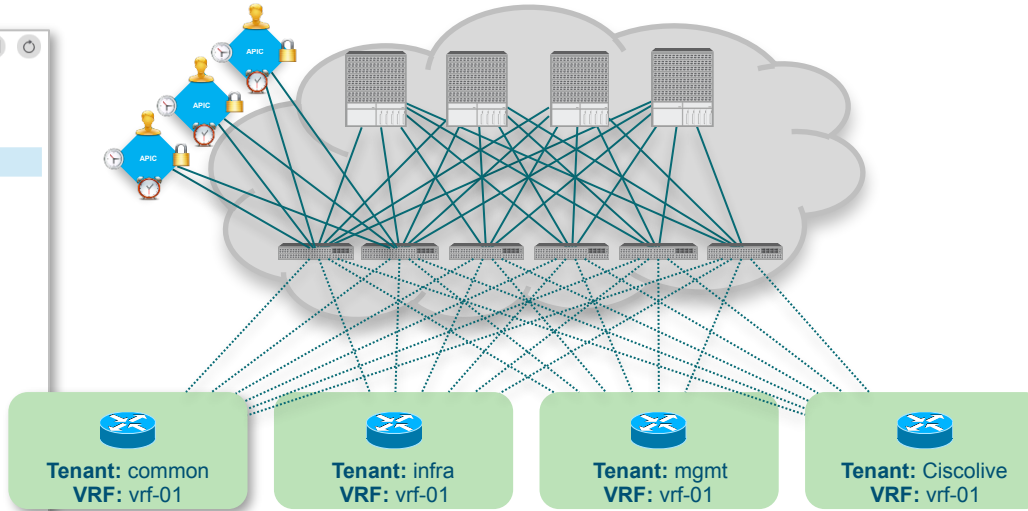
Looking under the covers at Tenants

```
apic1# show running-config tenant Ciscolive
# Command: show running-config tenant Ciscolive
# Time: Tue Jan 30 13:47:50 2018
tenant Ciscolive
  vrf context vrf-01
  exit
  bridge-domain 192.168.10.x_24
  vrf member vrf-01
  exit
  bridge-domain 192.168.11.x_24
  vrf member vrf-01
  exit
  bridge-domain 192.168.12.x_24
  vrf member vrf-01
  exit
  bridge-domain vlan-501
  arp flooding
  l2-unknown-unicast flood
  no unicast routing
  vrf member vrf-01
  exit
```

VRFs



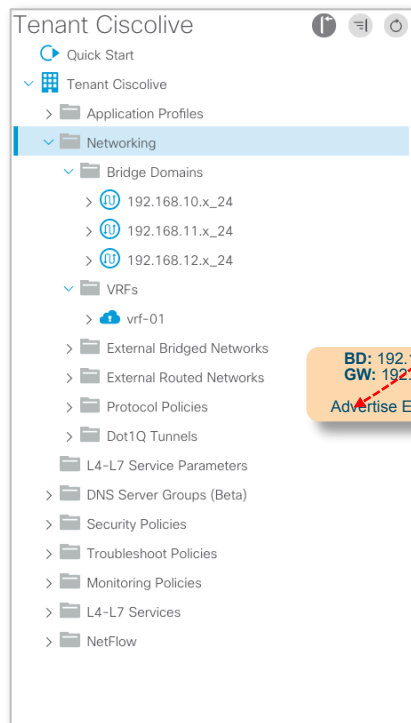
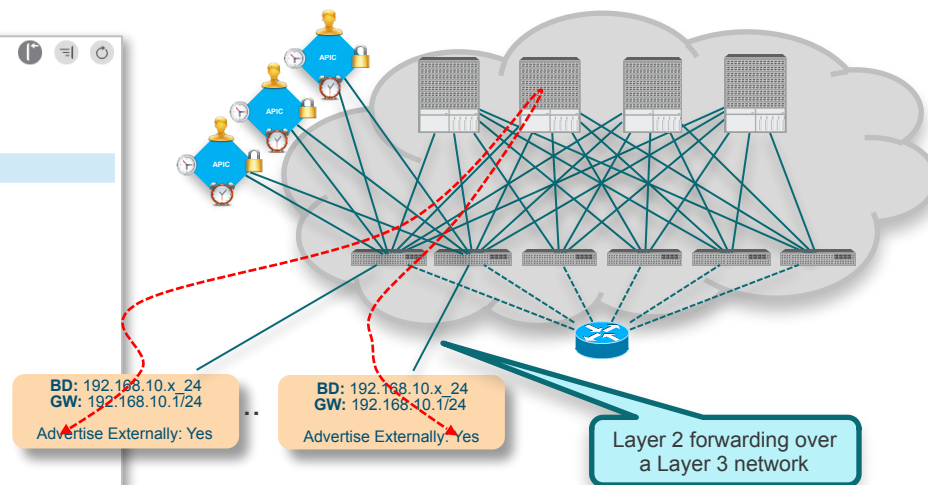
VRFs are configured within a Tenant



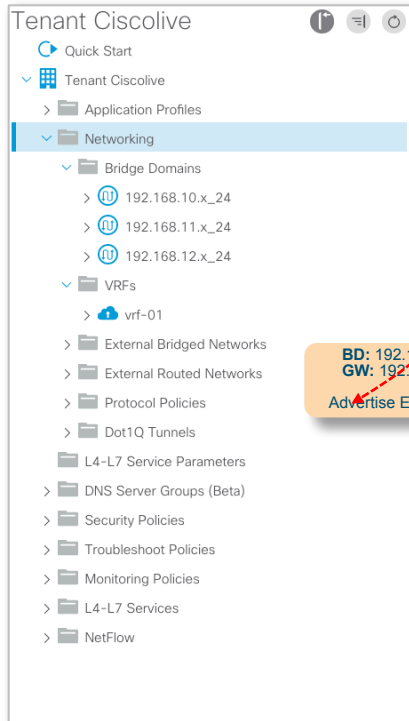
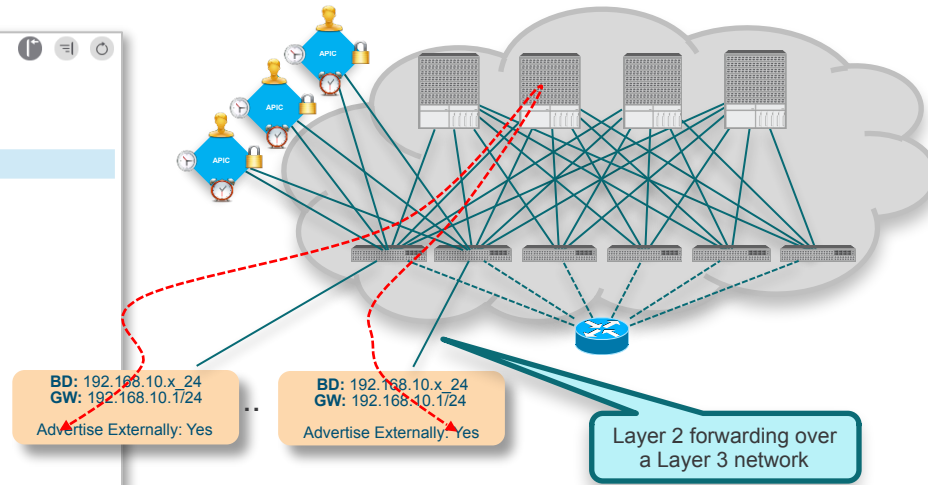
Bridge Domains

A Bridge Domain is a Layer 2 forwarding segment which maps a (locally significant) VLAN on each Leaf switch to a unique VXLAN segment

A Bridge Domain may have one or more associated SVIs



What does this look like...



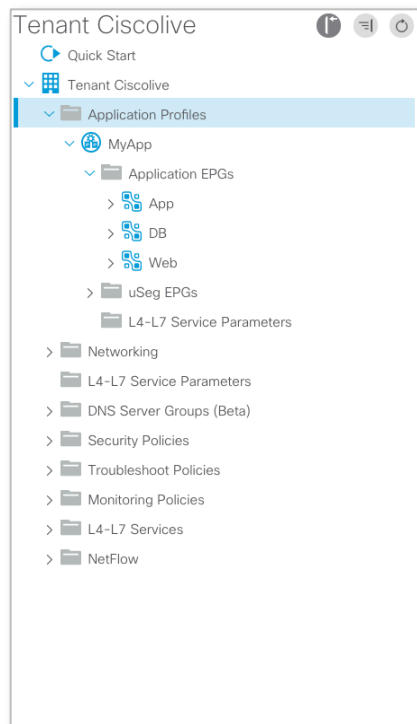
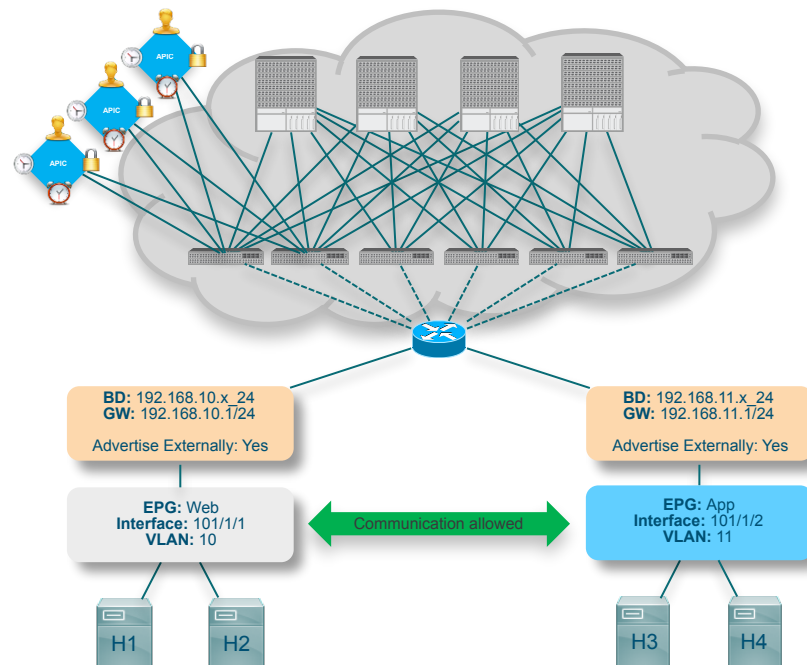
...it looks like a VLAN “over” a VXLAN

Endpoint Groups

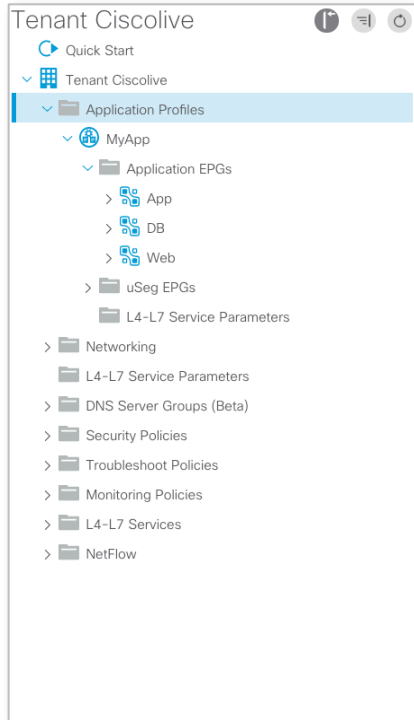
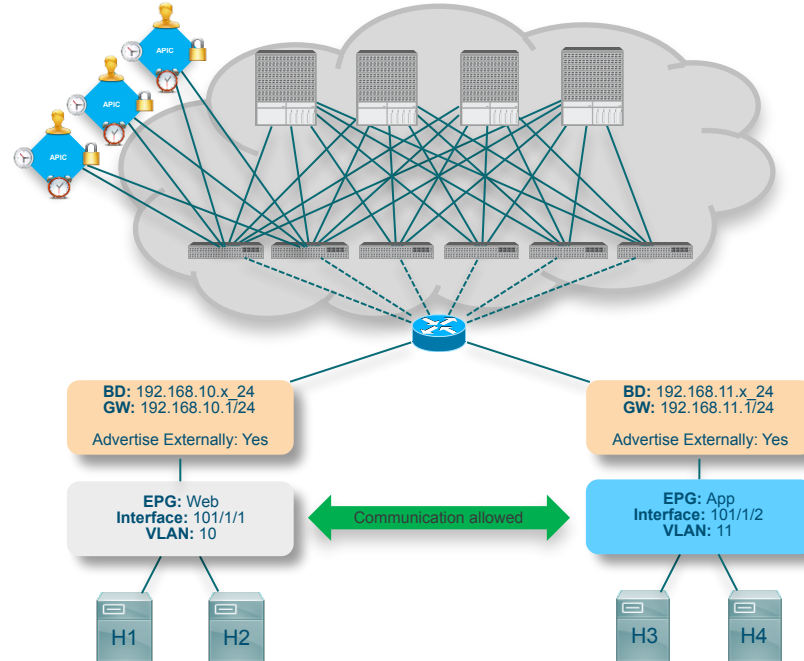
An Endpoint Group is a security “container” for devices that are attached to an ACI fabric. There is a 1:1 mapping between EPGs and Bridge Domains

Devices are mapped into an EPG by considering the incoming switch/interface/vlan, or virtual switch/vlan

Communication within an EPG is permitted (by default), communication between EPGs requires a Contract (ACL)



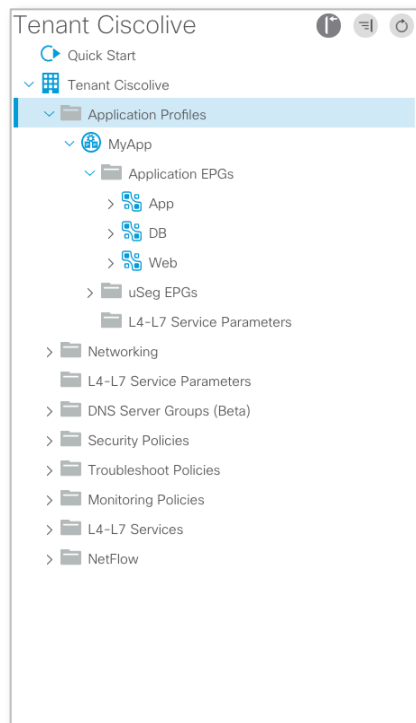
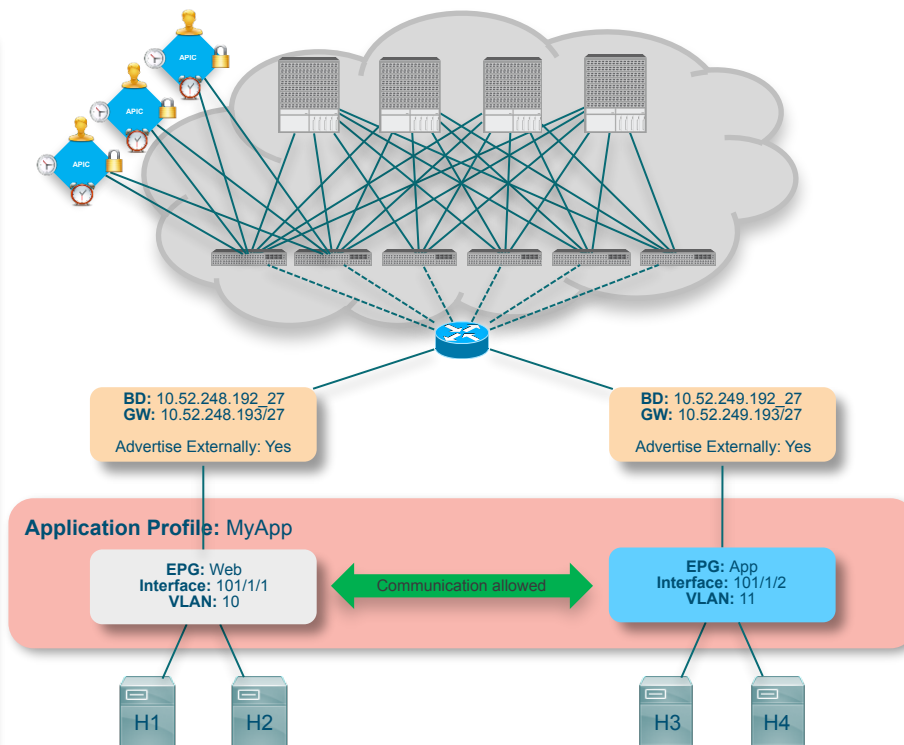
What does this look like...



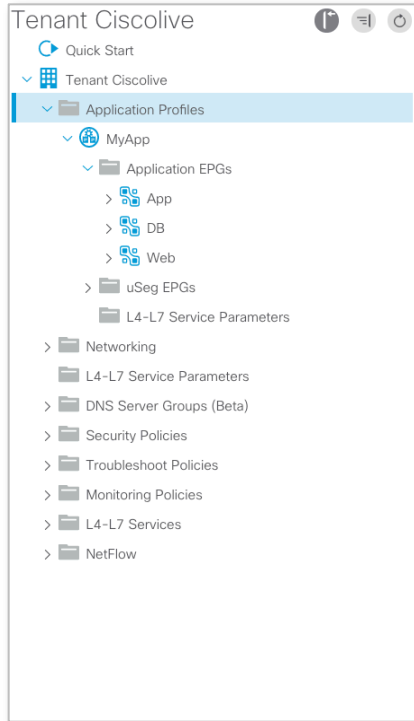
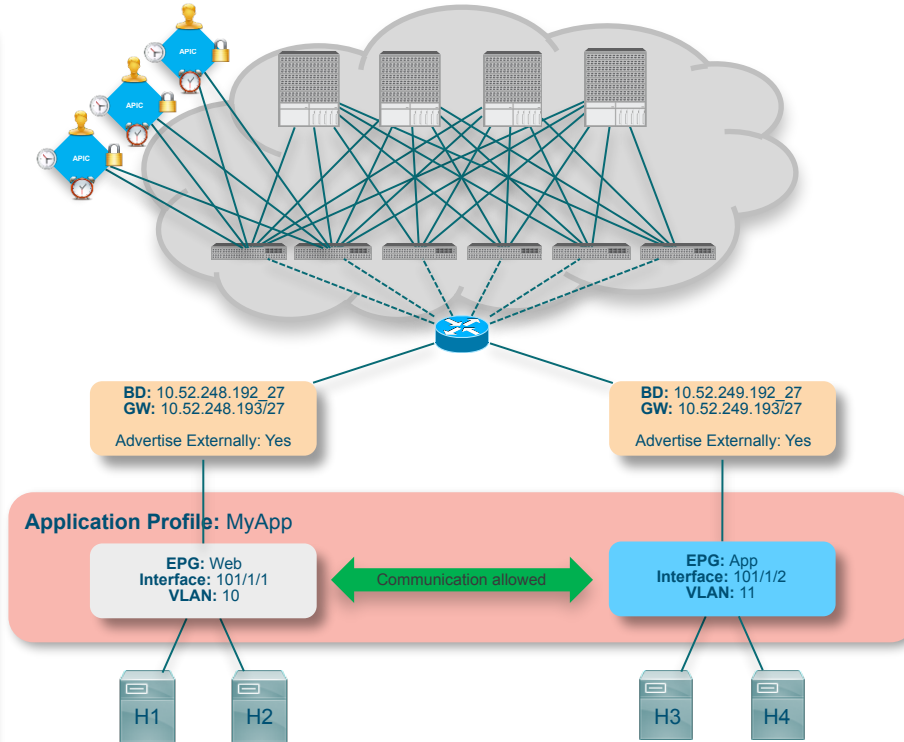
...it looks like VLANs with ACLs

Application Profiles

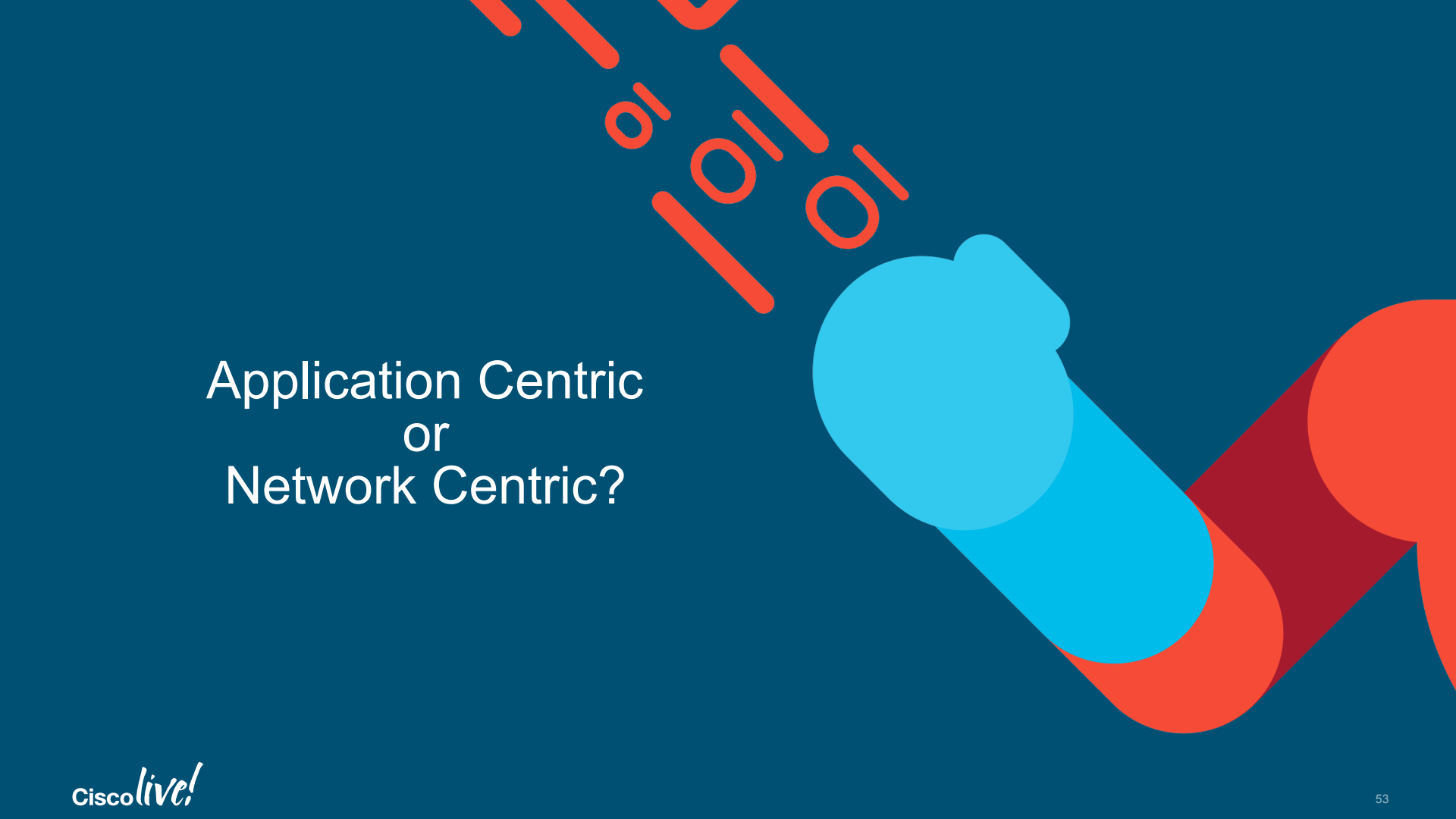
An Application Profile is a collection of EPGs which may or may not represent an Application, e.g. MyExpenses



What does this look like...



...it's a collection of EPGs and Contracts

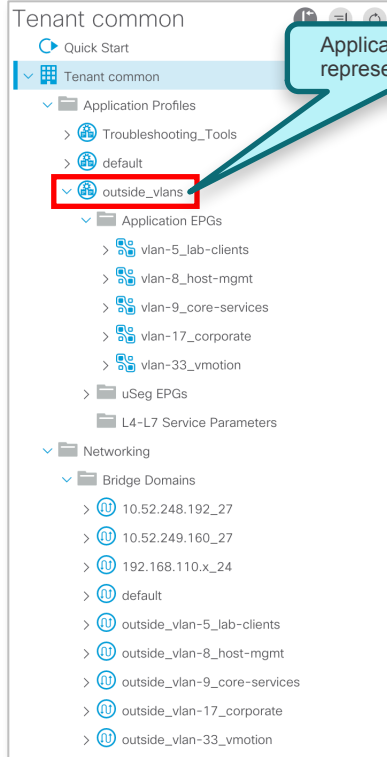
The background is a solid dark blue. In the upper right, there are several red diagonal lines and circles, resembling binary code or data streams. On the right side, there are large, overlapping, rounded shapes in light blue and red. The text is centered on the left side in white.

Application Centric or Network Centric?

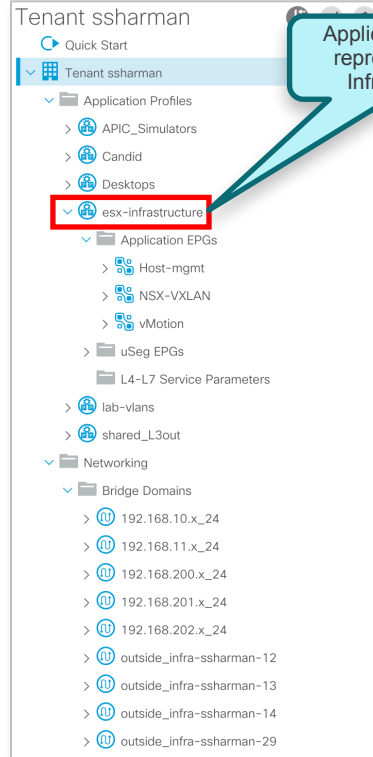


What's in a name?

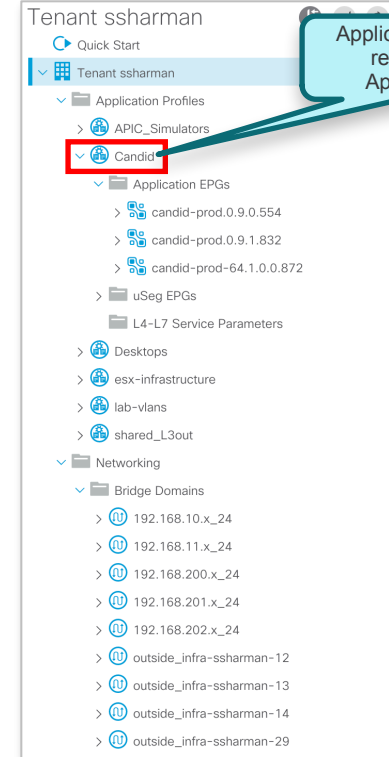
What's in a name?



Application Profile represents VLANs

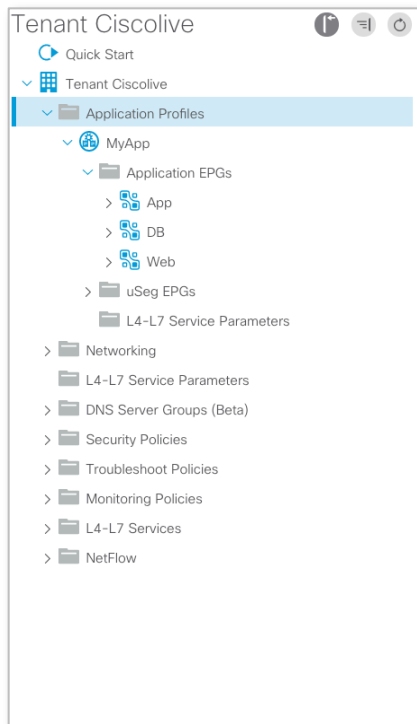
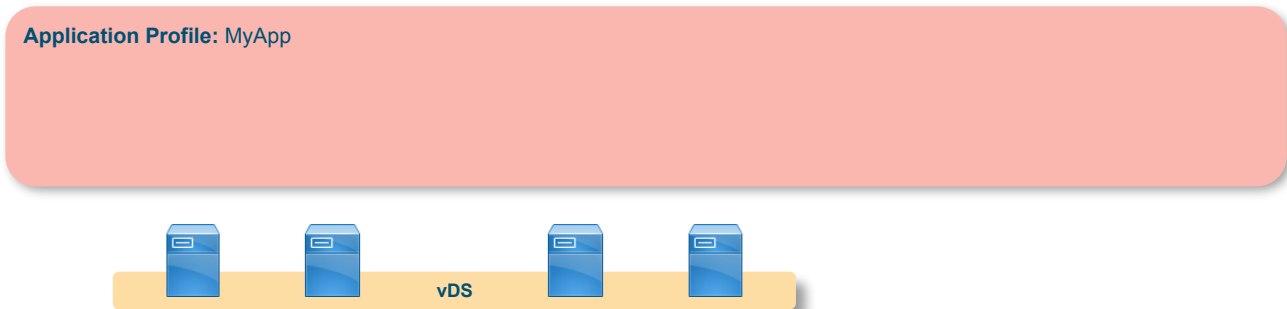


Application Profile represents ESX Infrastructure

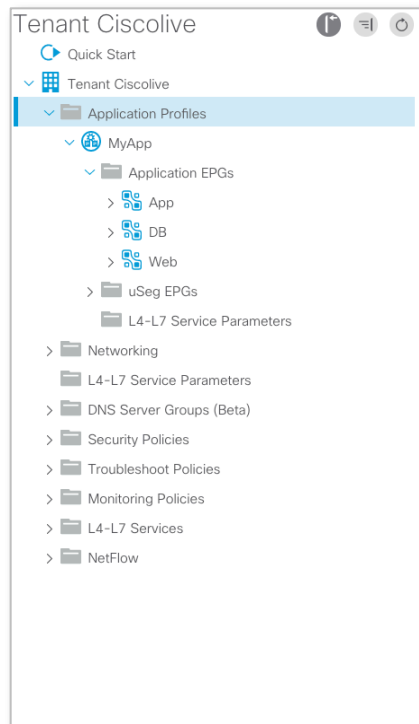
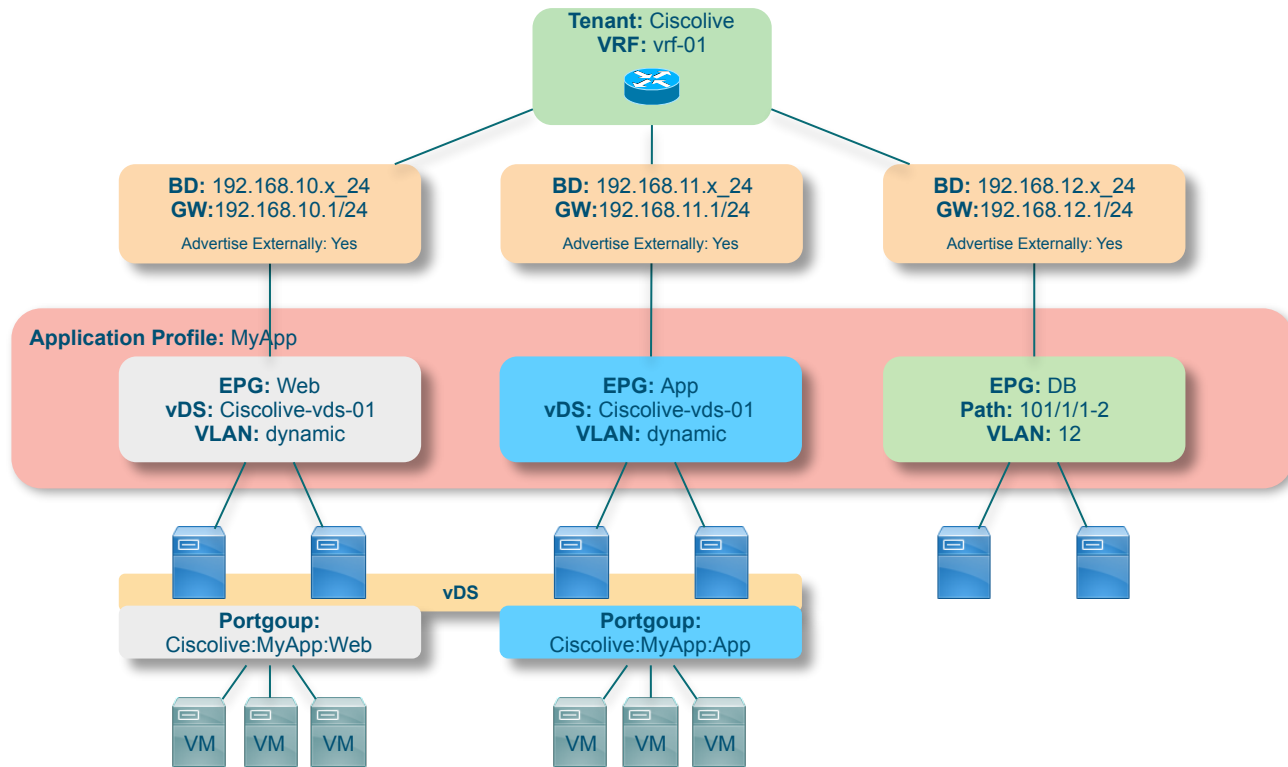


Application Profile represents Applications

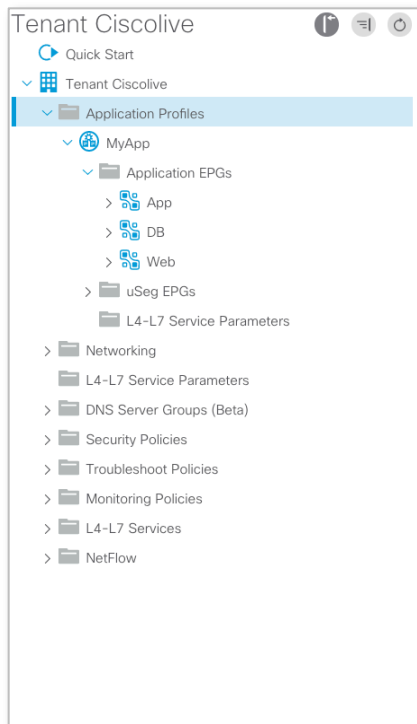
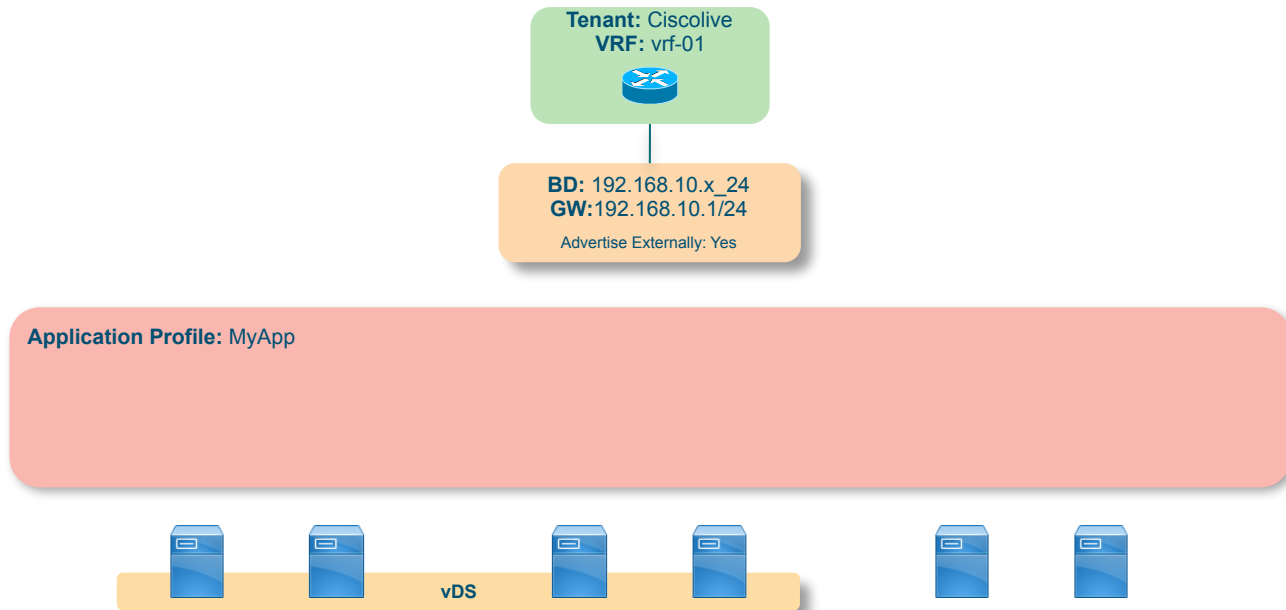
Option 1: Single EPG on a Single BD with a Single Subnet – “standard networking”



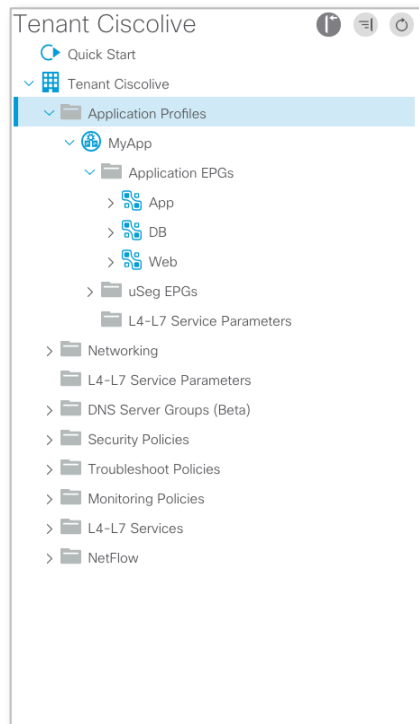
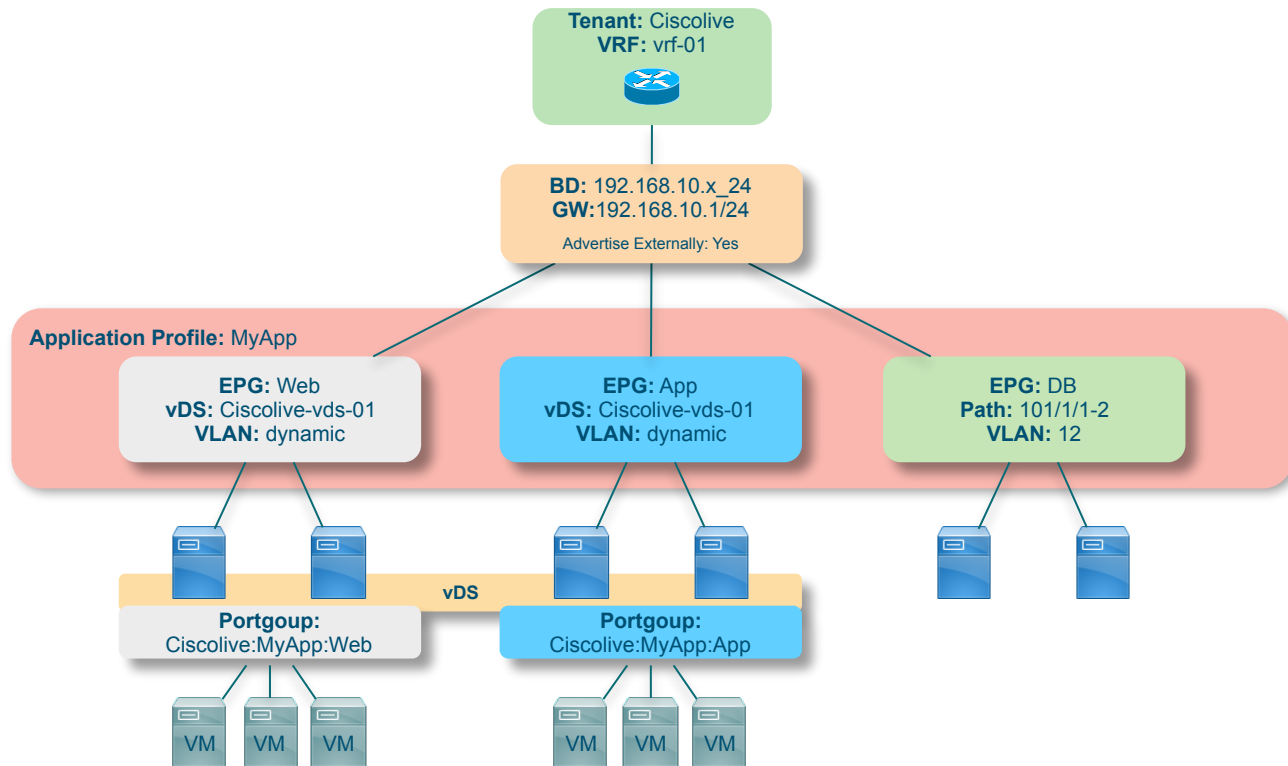
Option 1: Single EPG on a Single BD with a Single Subnet – “standard networking”



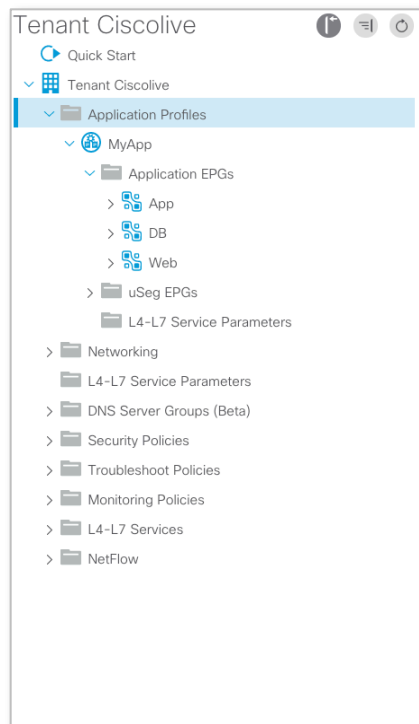
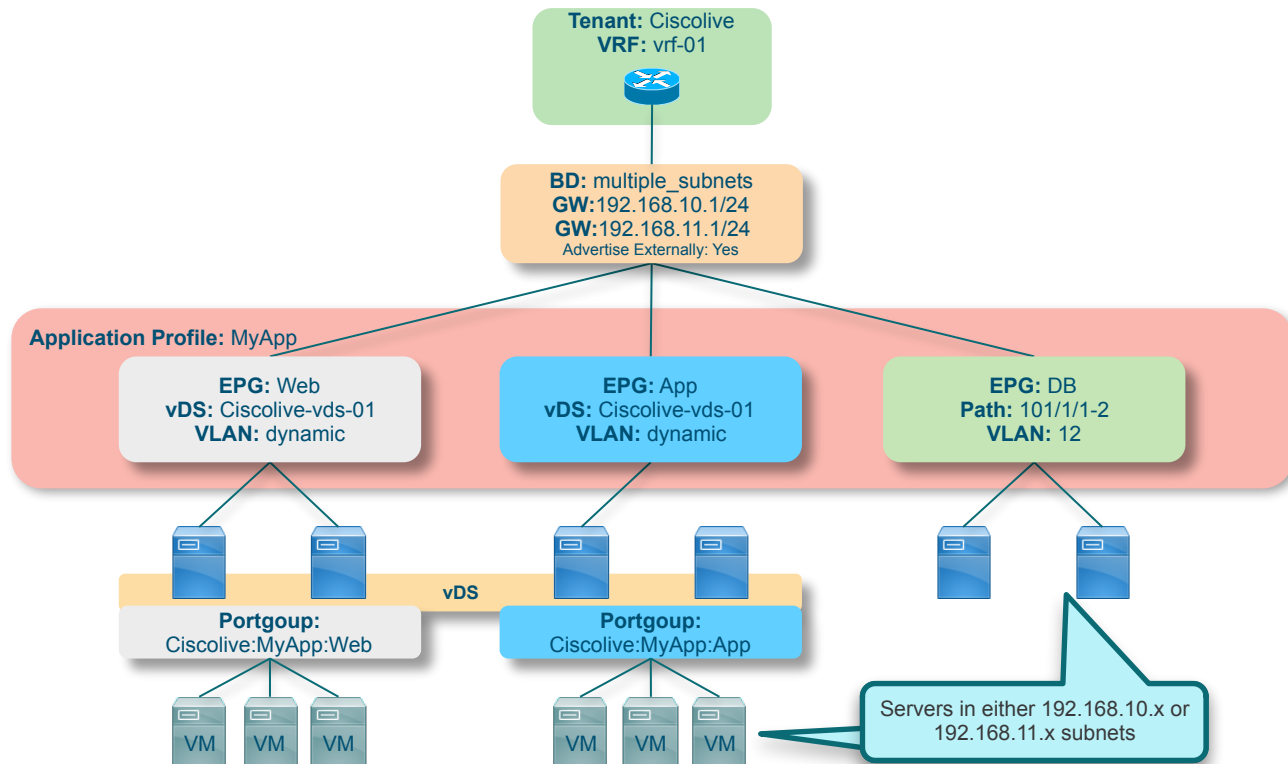
Option 2: Multiple EPGs on a Single BD with a Single Subnet – μ Segmentation in IP space



Option 2: Multiple EPGs on a Single BD with a Single Subnet – μ Segmentation in IP space

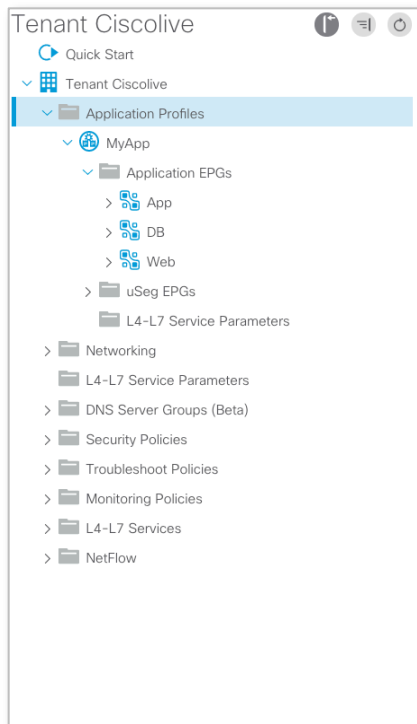
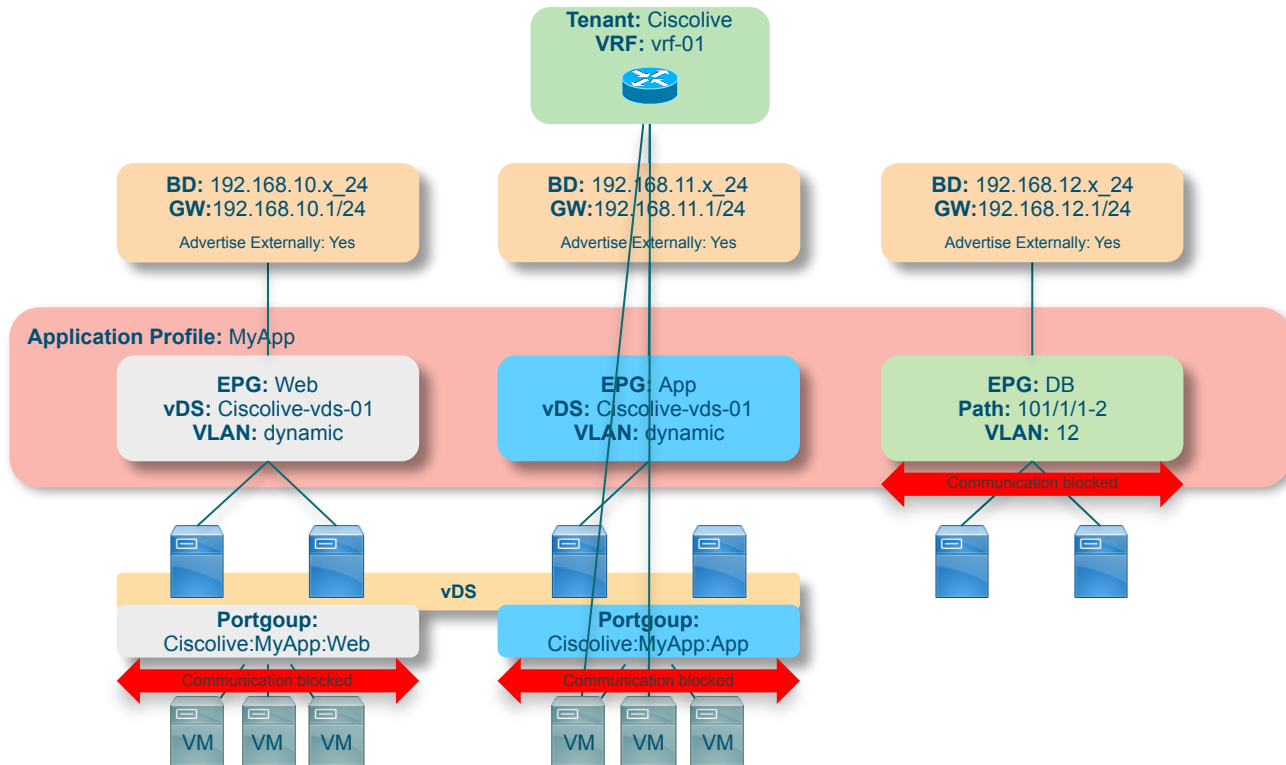


Option 3: Multiple EPGs on a Single BD with Multiple Subnets – IP secondary

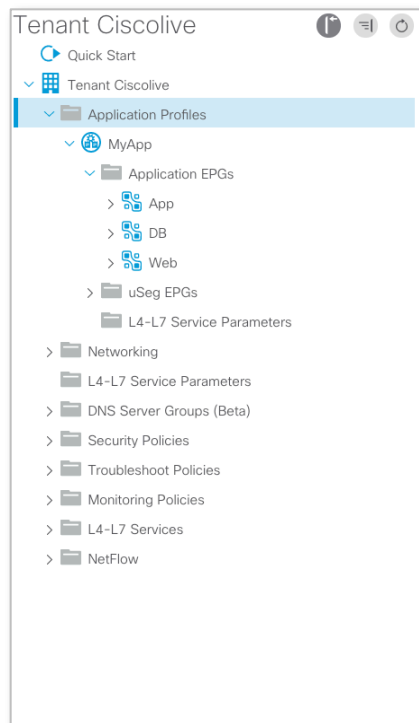
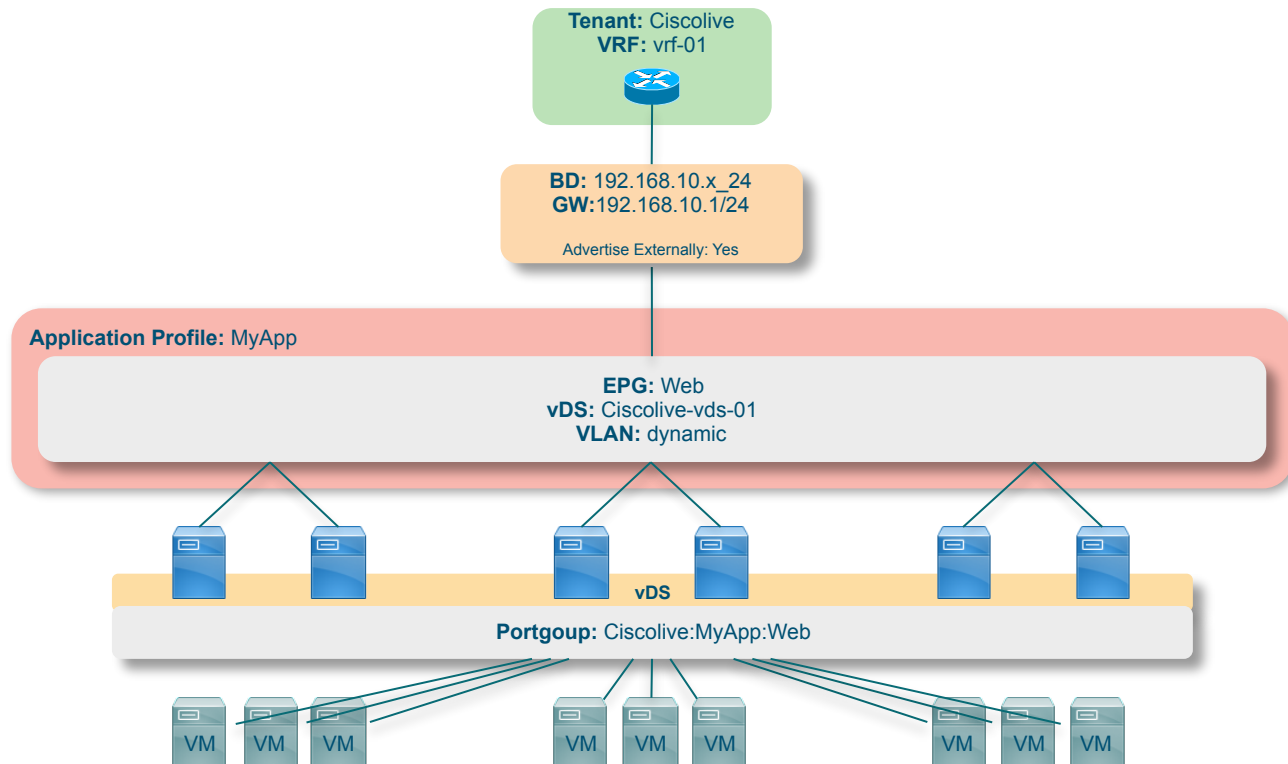


Options 1, 2, and 3 – μSegmentation within an EPG/Port Group

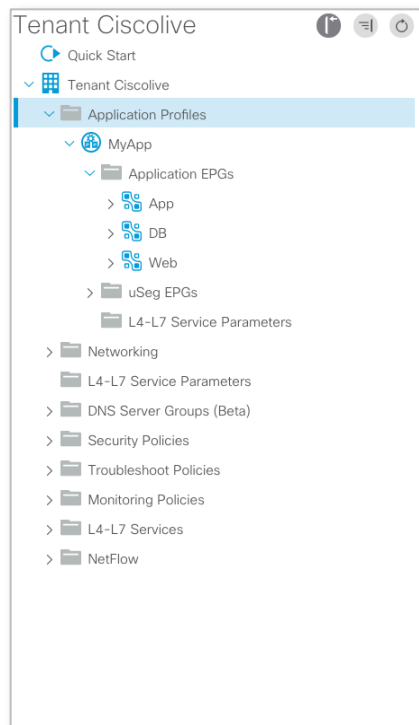
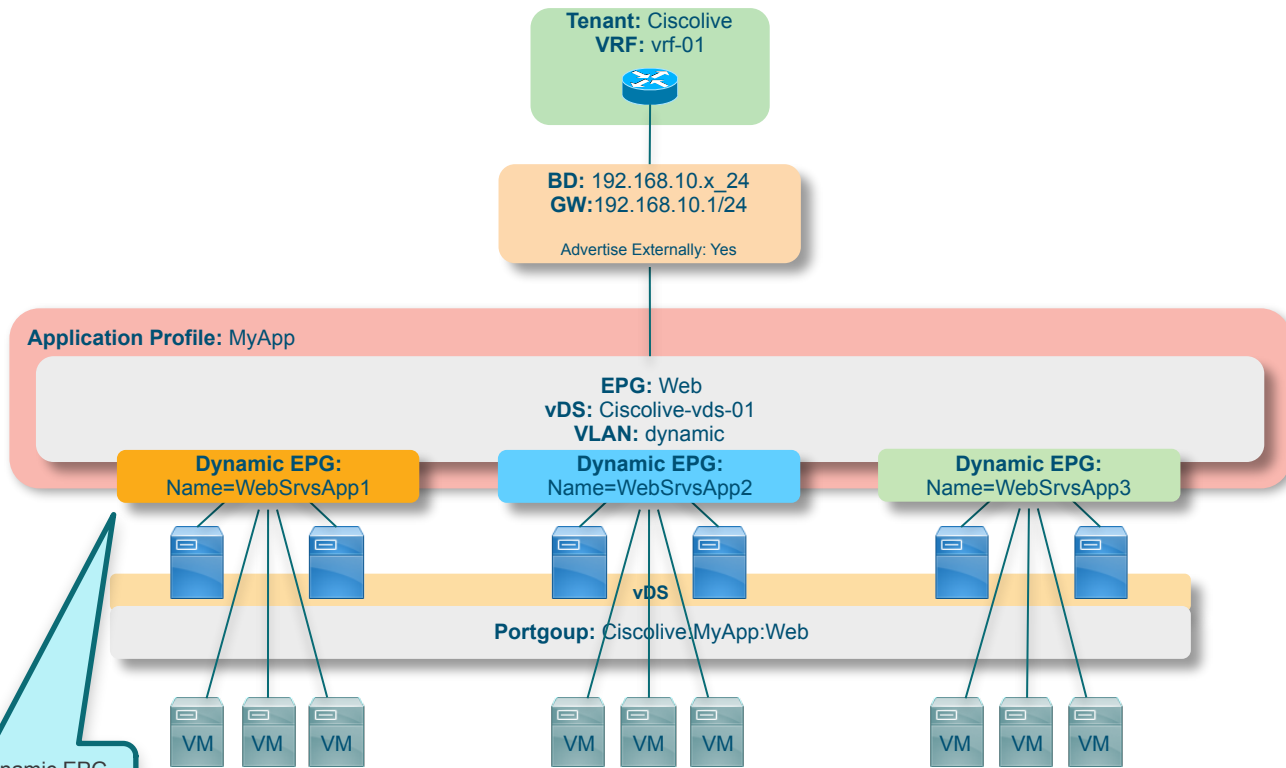
(no East/West traffic flows)



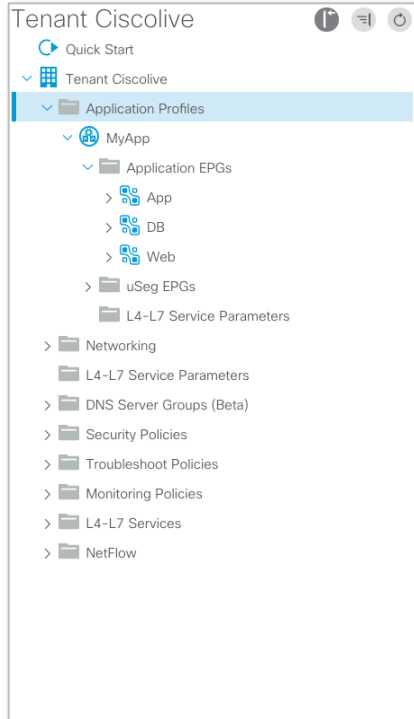
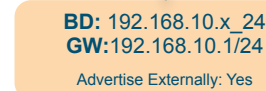
Options 1, 2, and 3 – μSegmentation within an EPG/Port Group based on machine attribute



Options 1, 2, and 3 – μSegmentation within an EPG/Port Group based on machine attribute



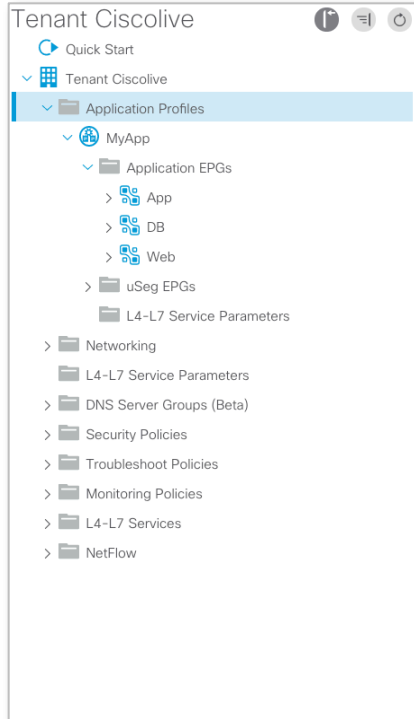
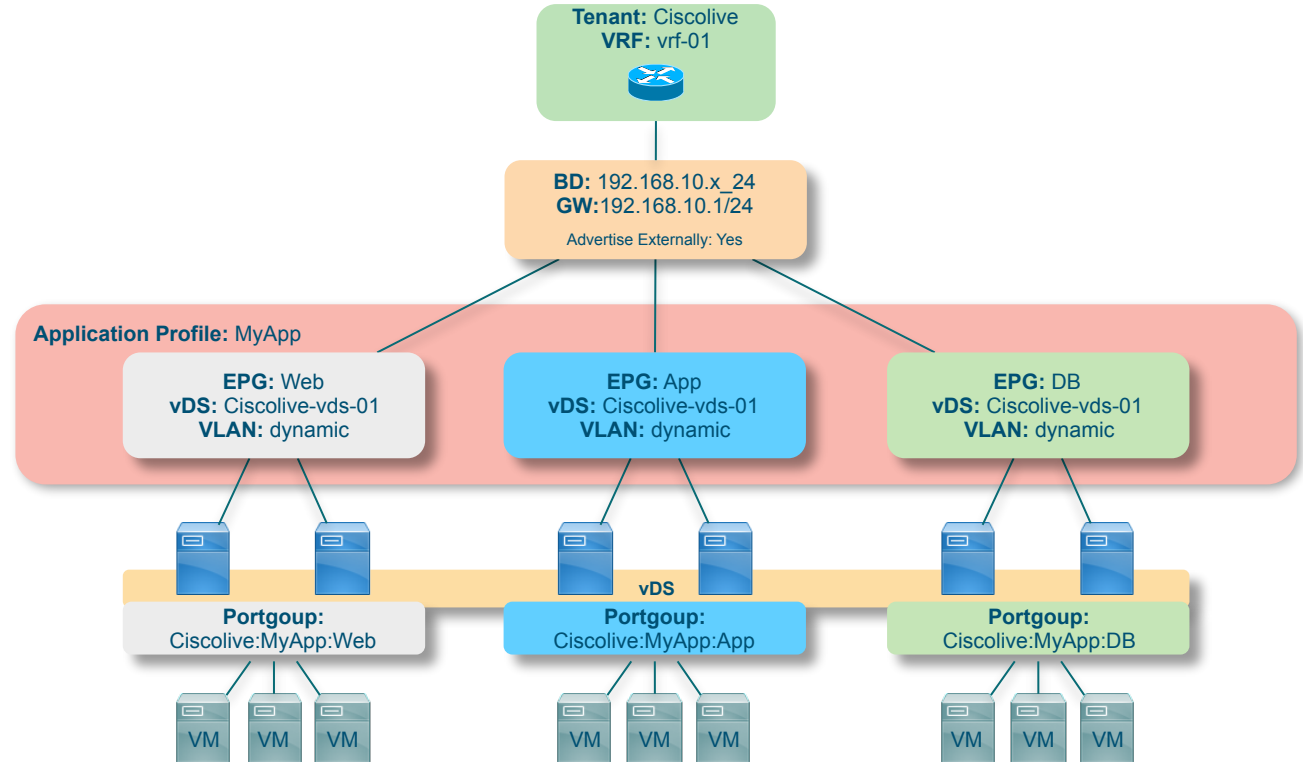
Alternative option: 3x Portgroups



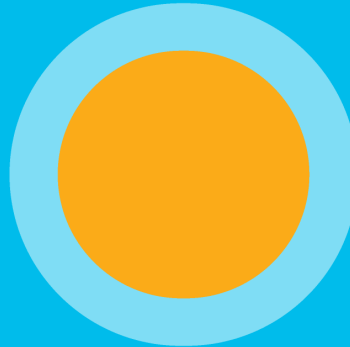
Application Profile: MyApp



Alternative option: 3x Portgroups

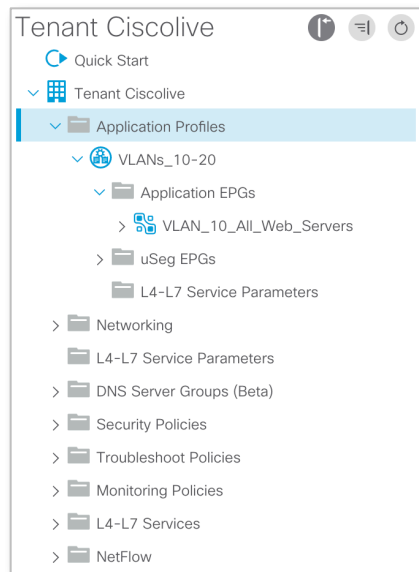
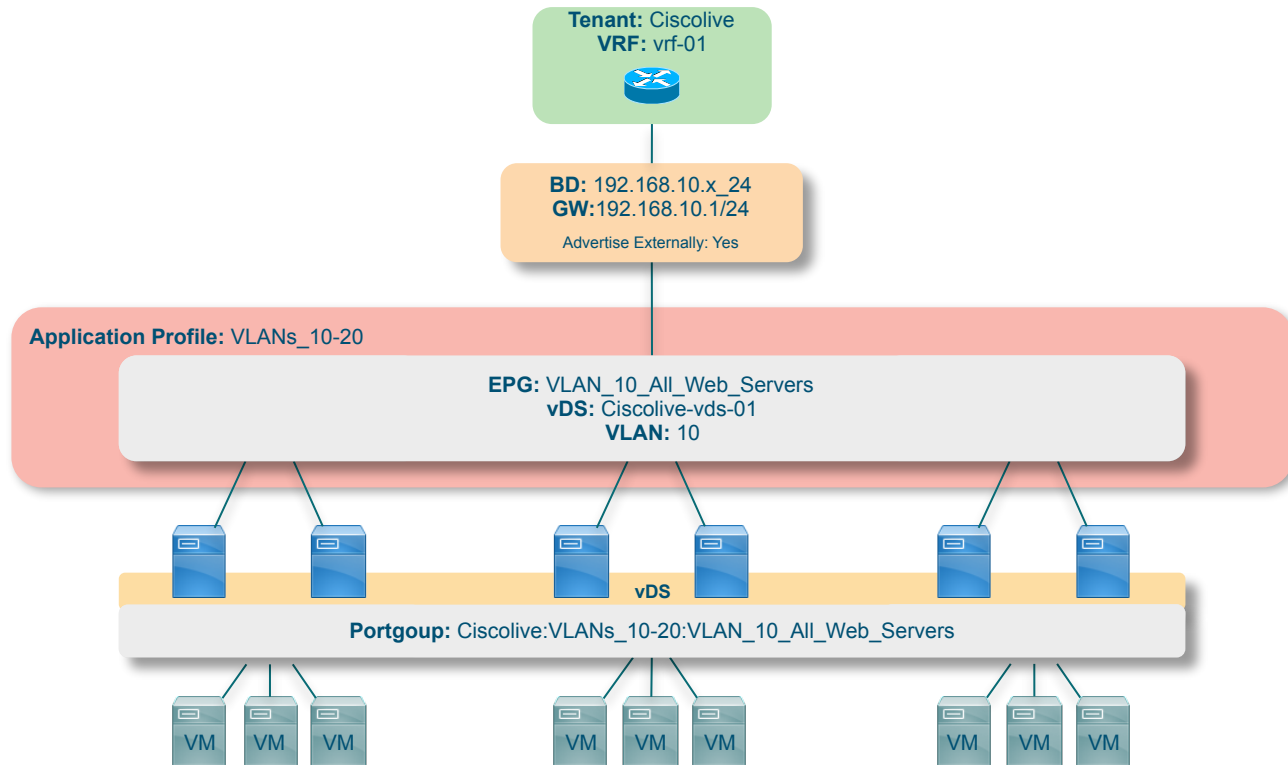


How do I retrofit my network and migrate from “Network Centric” to “Application Centric”...?

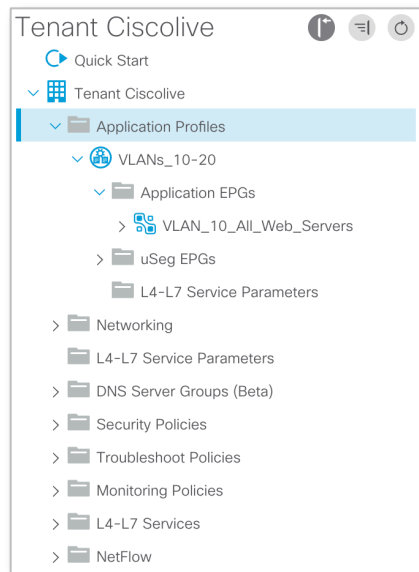
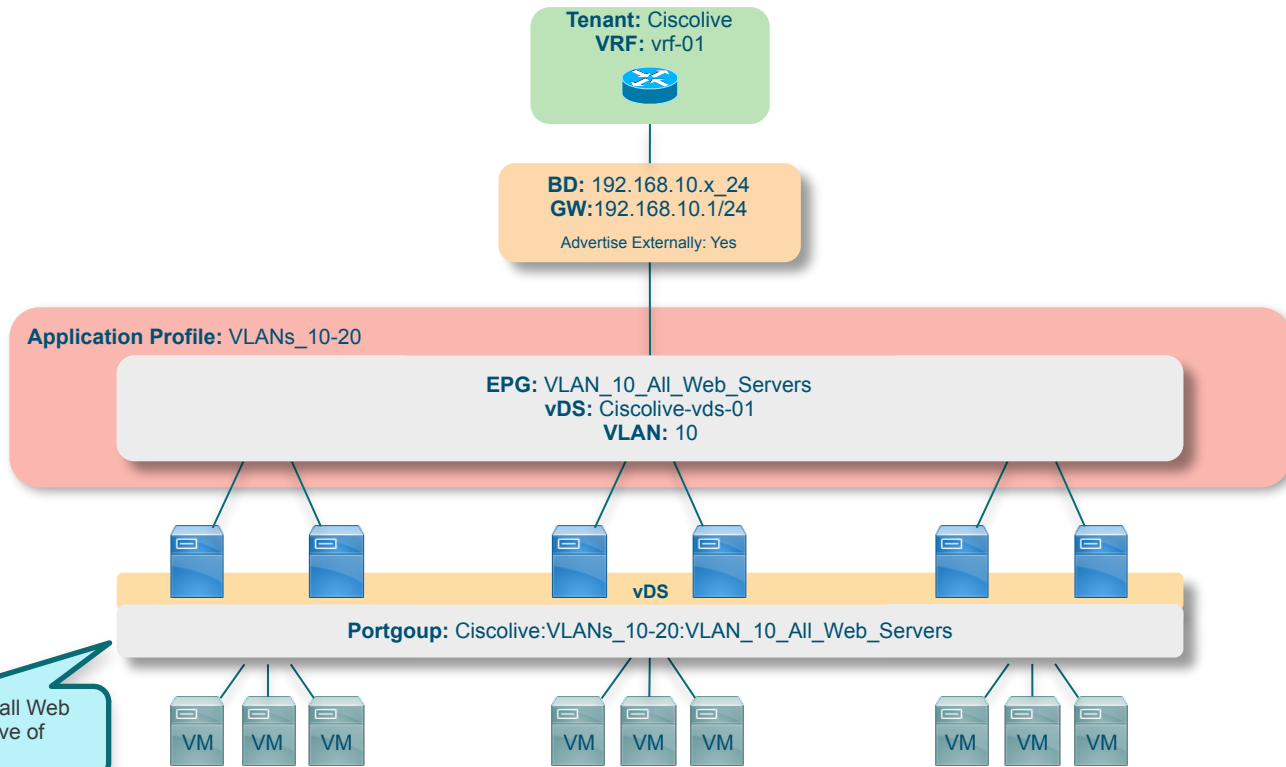


Why change what is already working...?

Network Centric Mode: Single EPG on a Single BD with a Single Subnet – “standard networking”

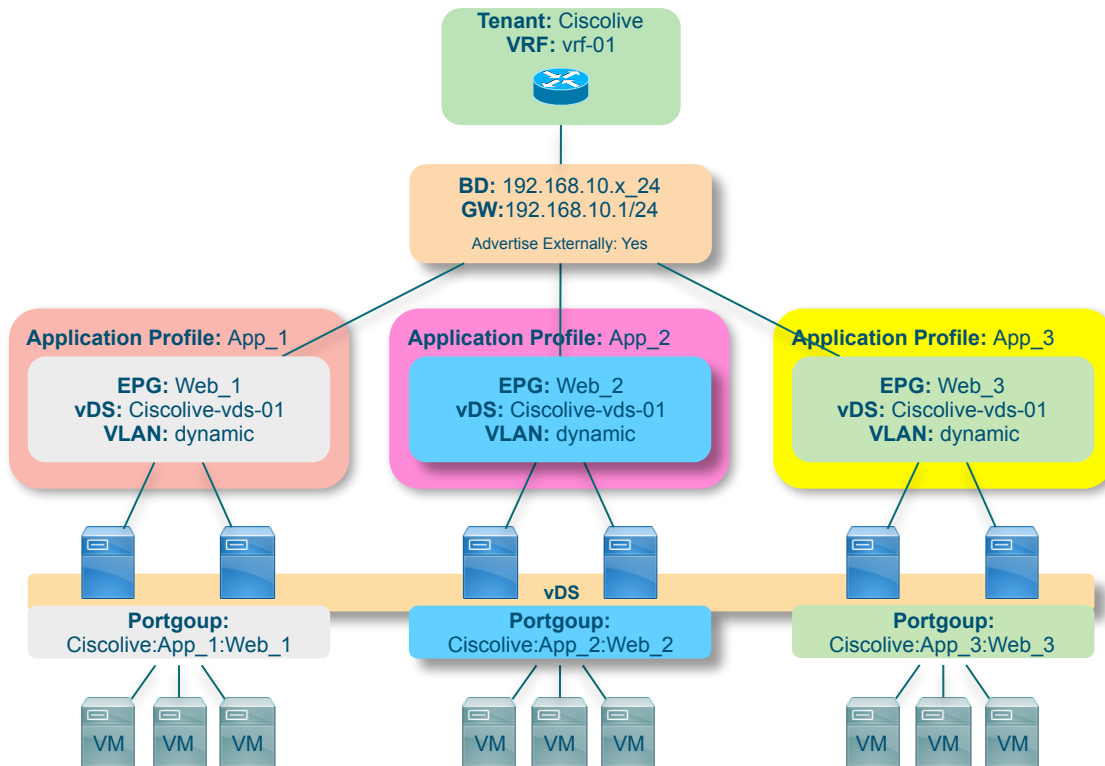


Network Centric Mode: Single EPG on a Single BD with a Single Subnet – “standard networking”

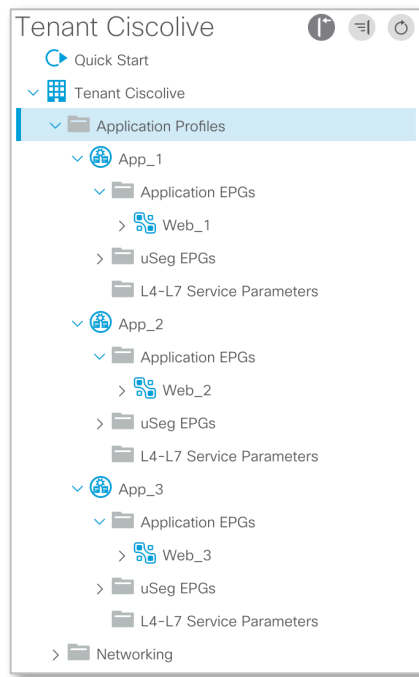
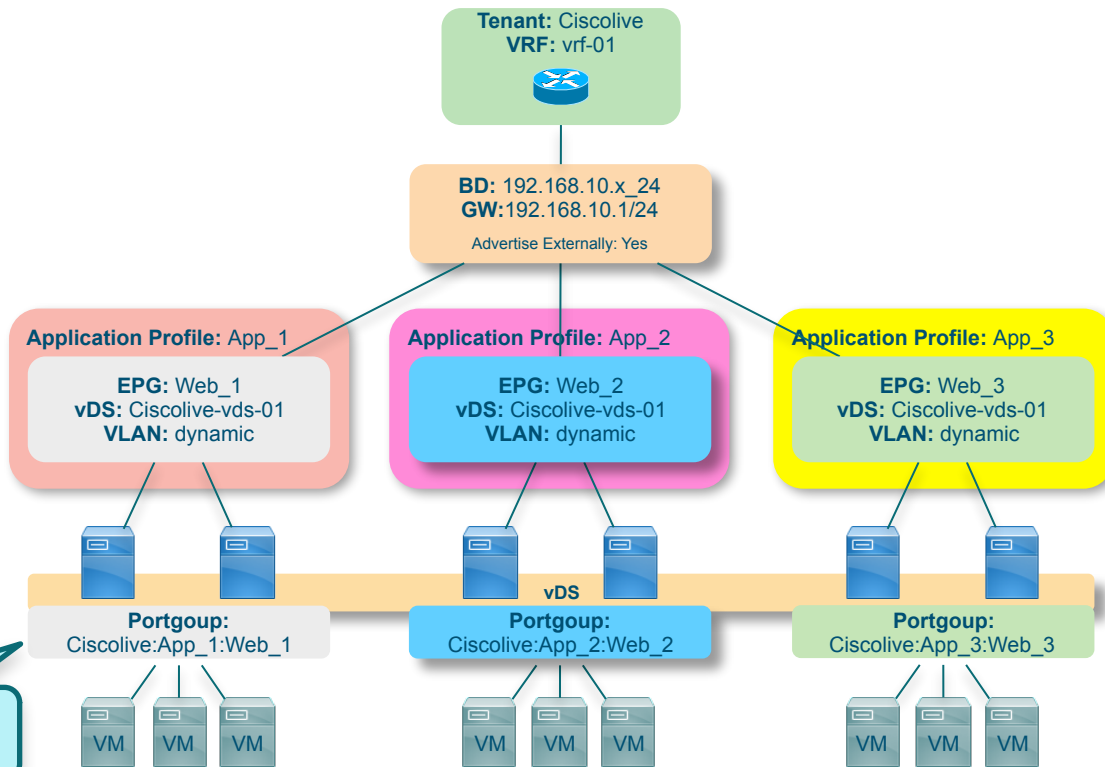


Single portgroup for all Web servers, irrespective of application

Application Centric Mode: Multiple EPGs on a Single BD with a Single Subnet – μ Segmentation in IP space



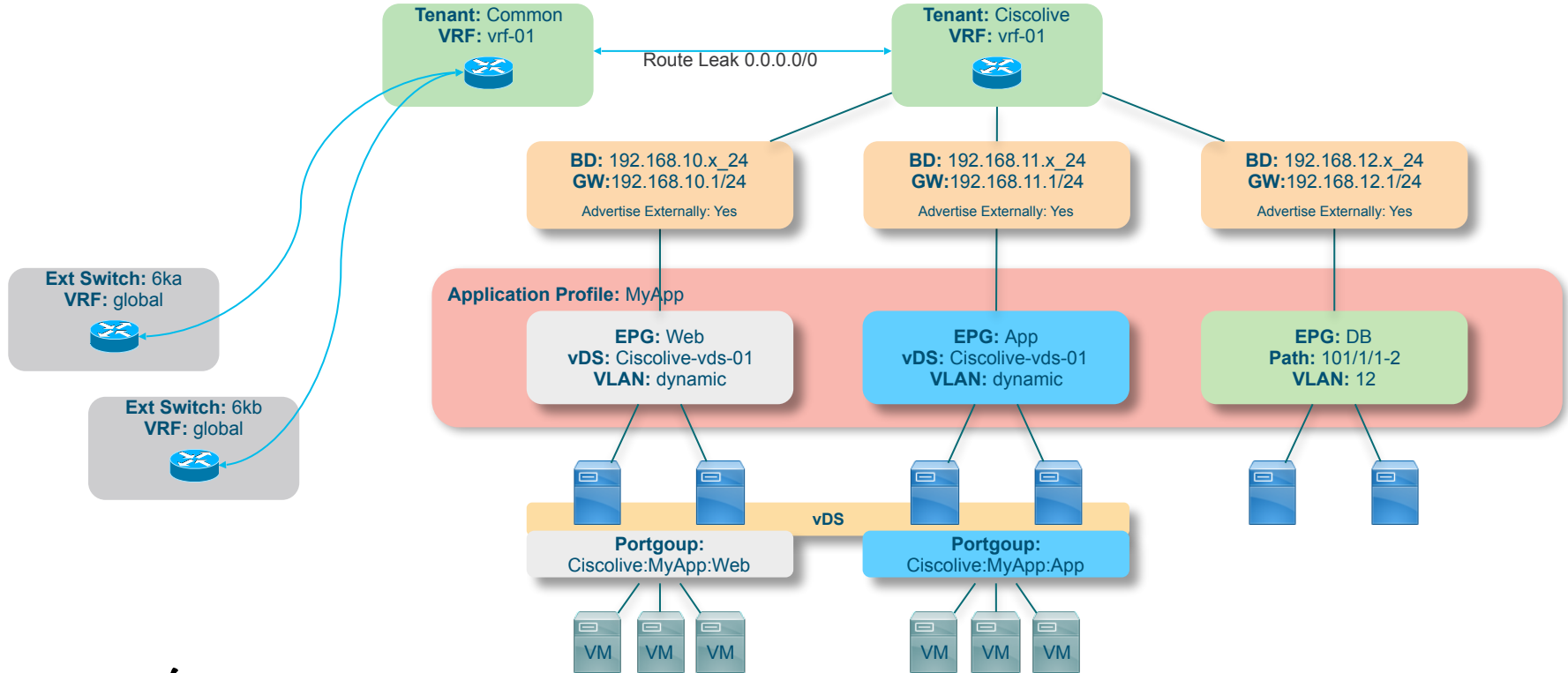
Application Centric Mode: Multiple EPGs on a Single BD with a Single Subnet – μ Segmentation in IP space



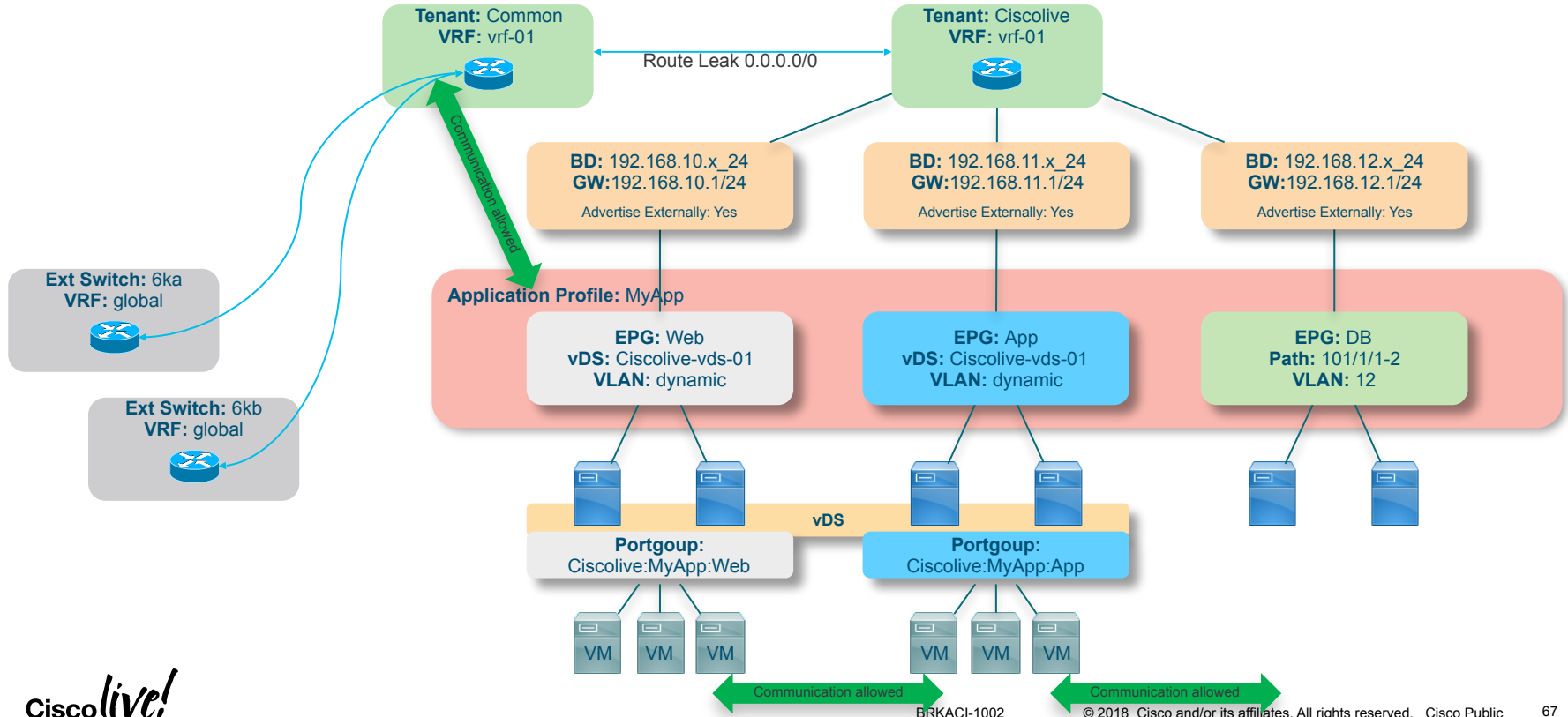
Web servers remapped to Application specific portgroups

How do I allow inter EPG communication?

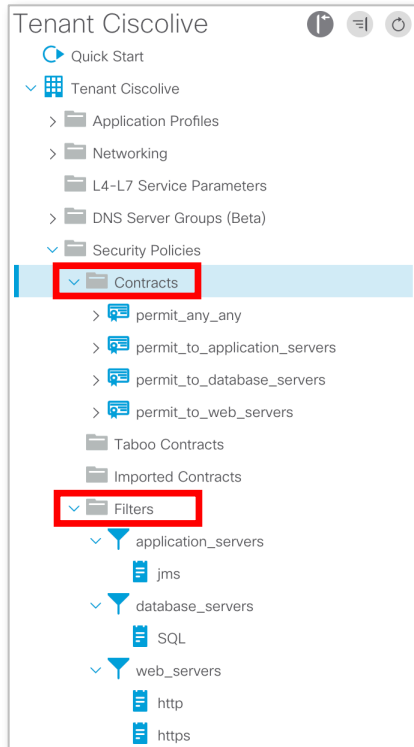
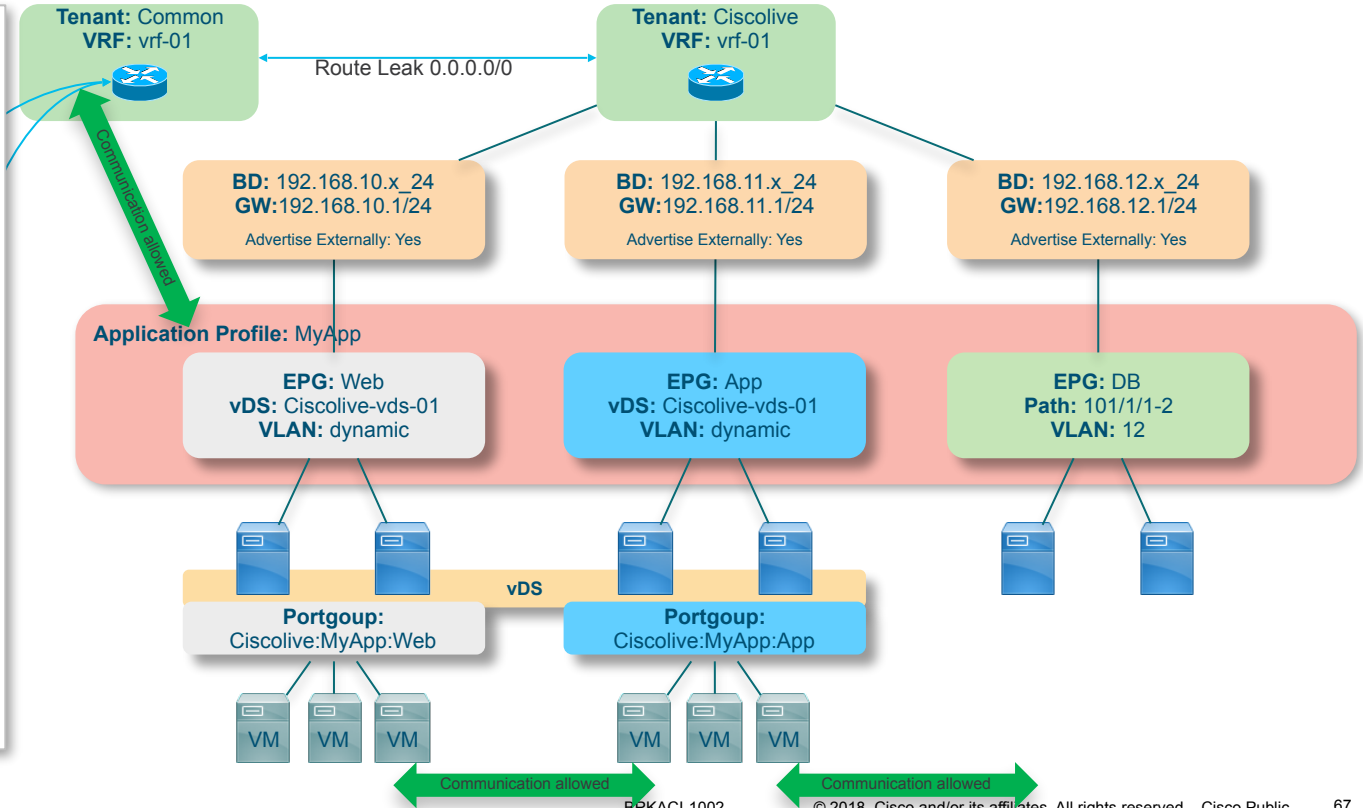
Contracts permit communication



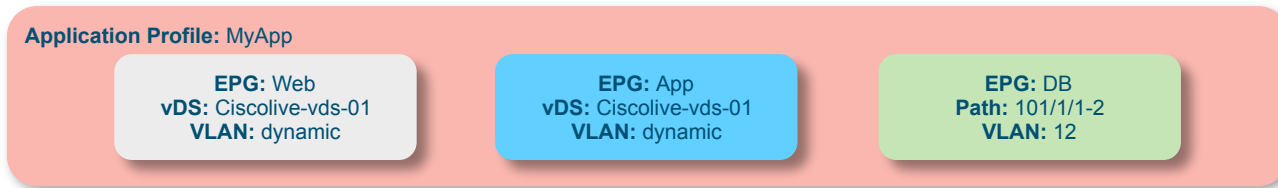
Contracts permit communication



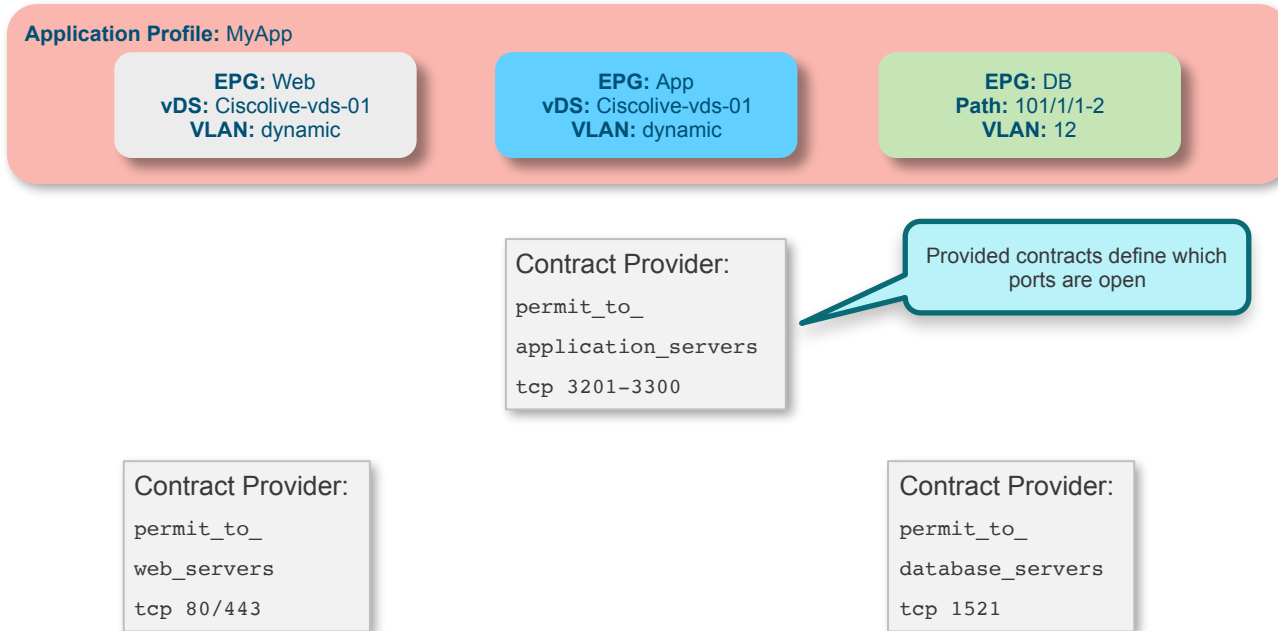
Contracts permit communication



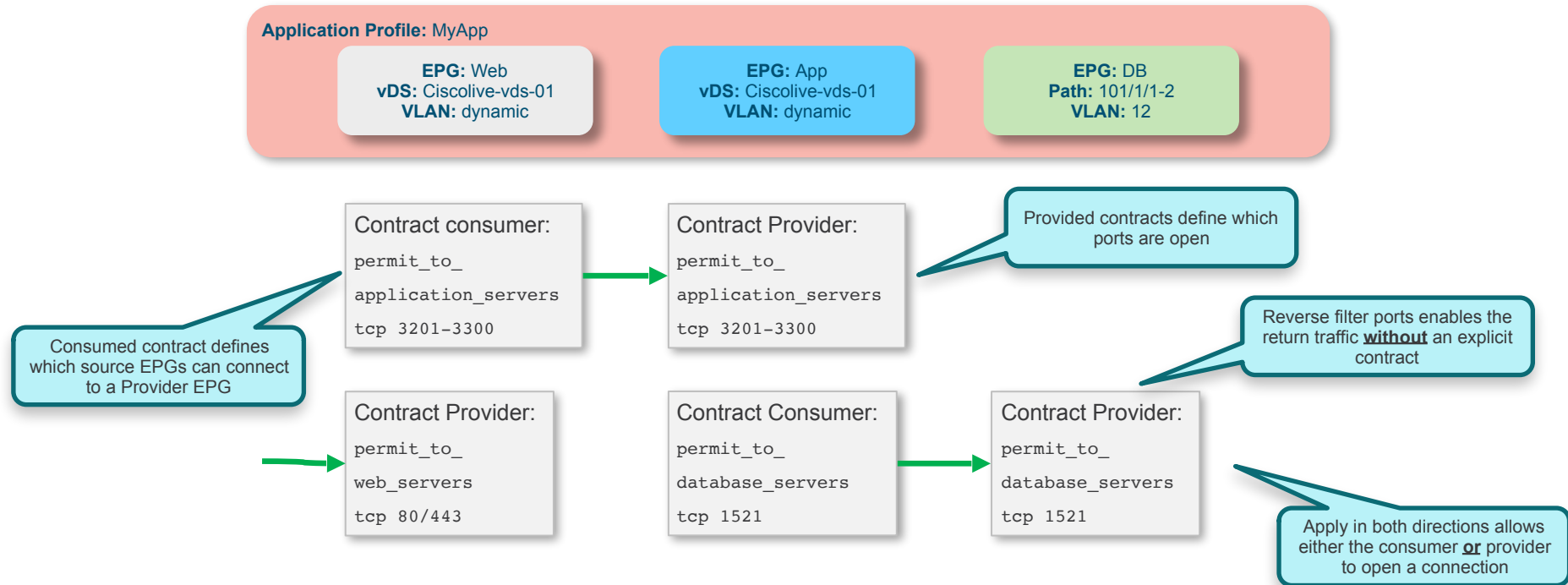
How do I use Contracts?



How do I use Contracts?



How do I use Contracts?



Contract Scope

Contract enforcement is “scoped” at:

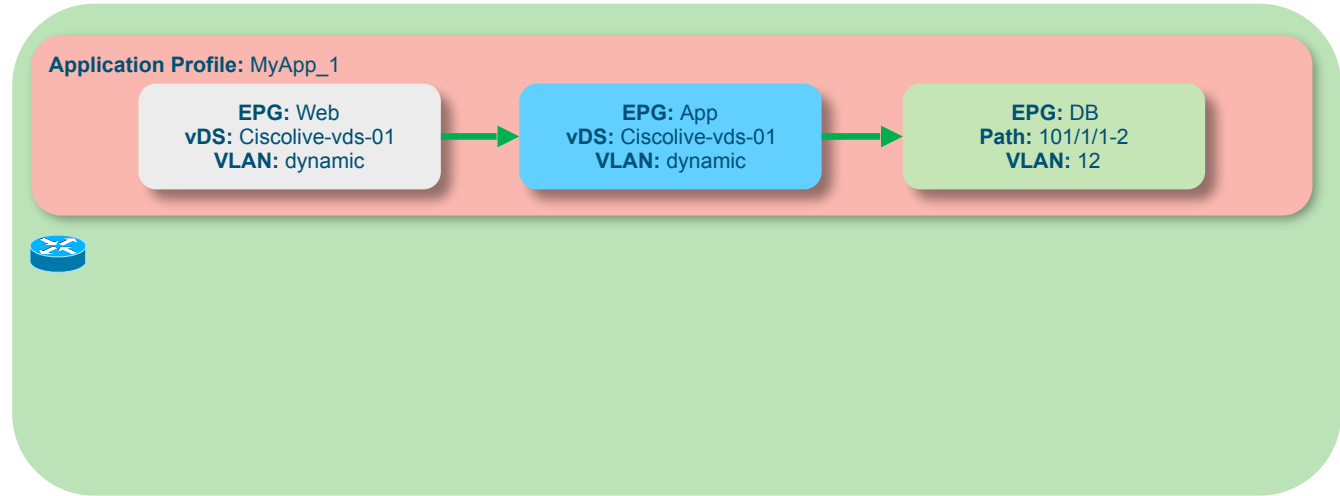
- Global
- Tenant
- VRF
- Application Profile



Contract Scope

Contract enforcement is “scoped” at:

- Global
- Tenant
- VRF
- Application Profile



Contract:
permit_to_
web_servers
tcp 80/443
Scope: Tenant

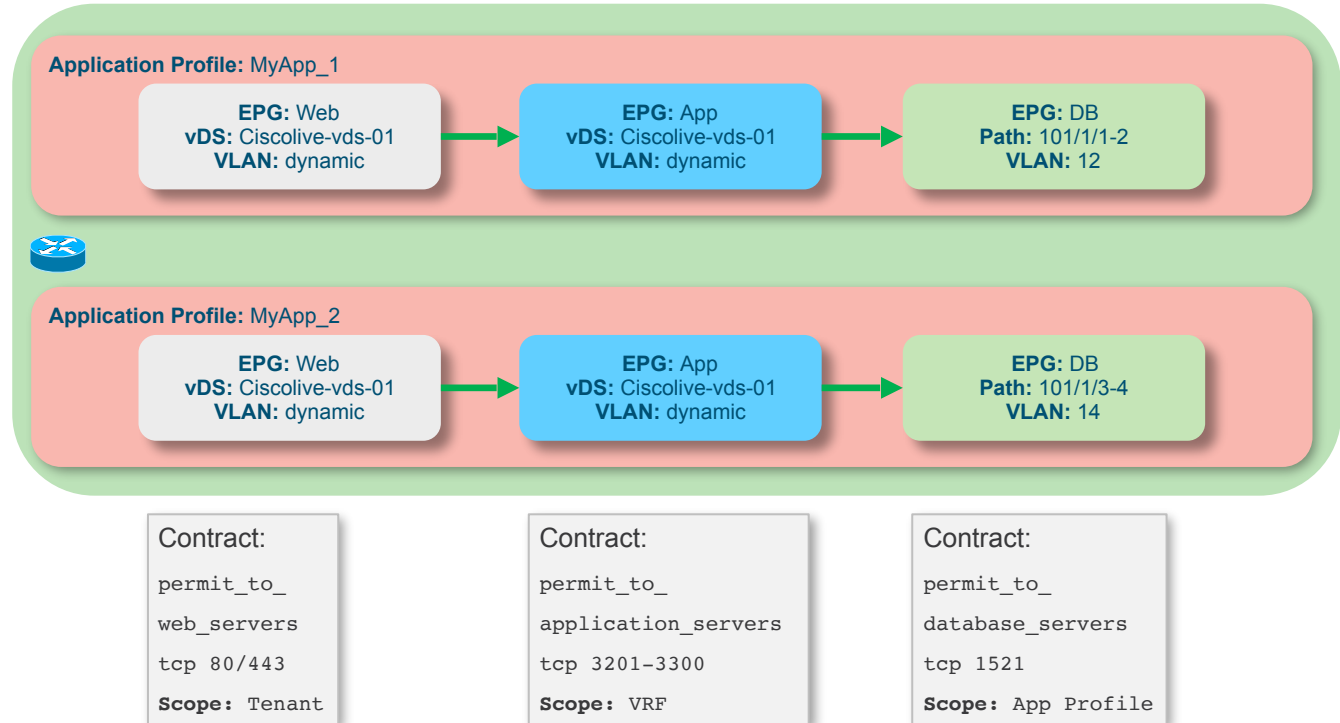
Contract:
permit_to_
application_servers
tcp 3201-3300
Scope: VRF

Contract:
permit_to_
database_servers
tcp 1521
Scope: App Profile

Contract Scope

Contract enforcement is “scoped” at:

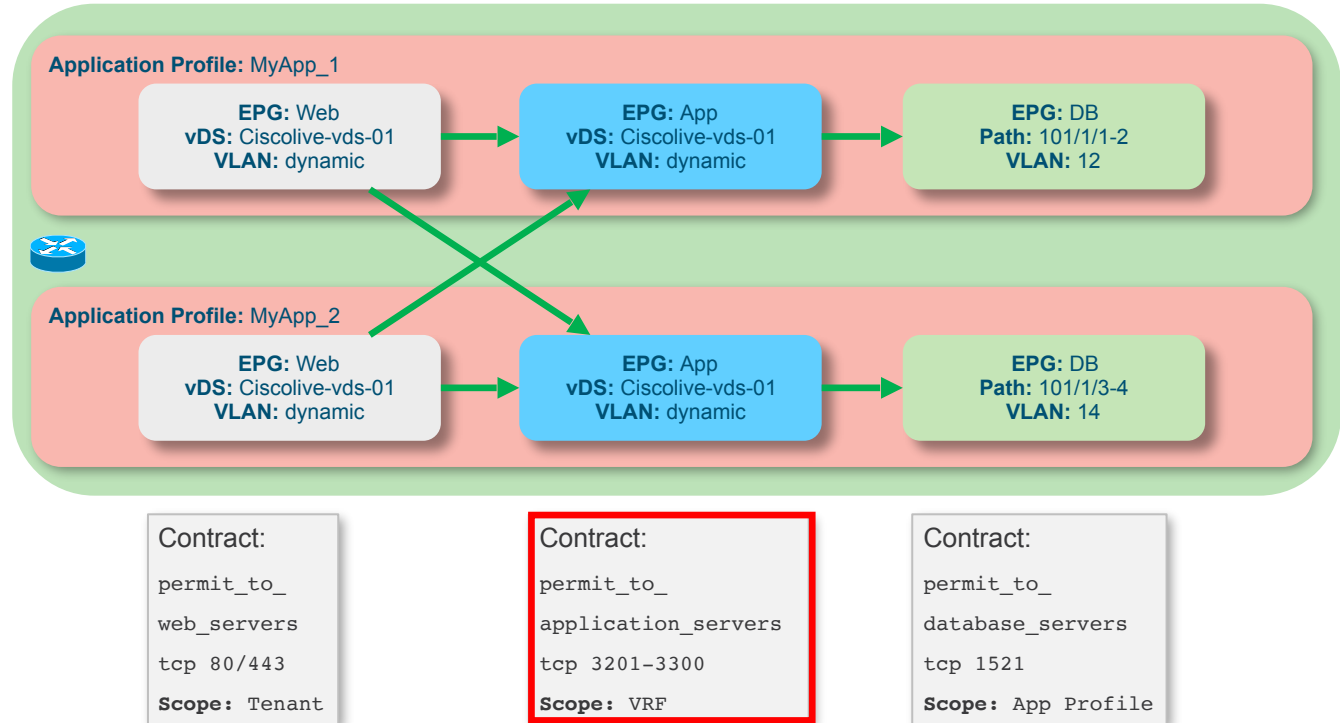
- Global
- Tenant
- VRF
- Application Profile



Contract Scope

Contract enforcement is “scoped” at:

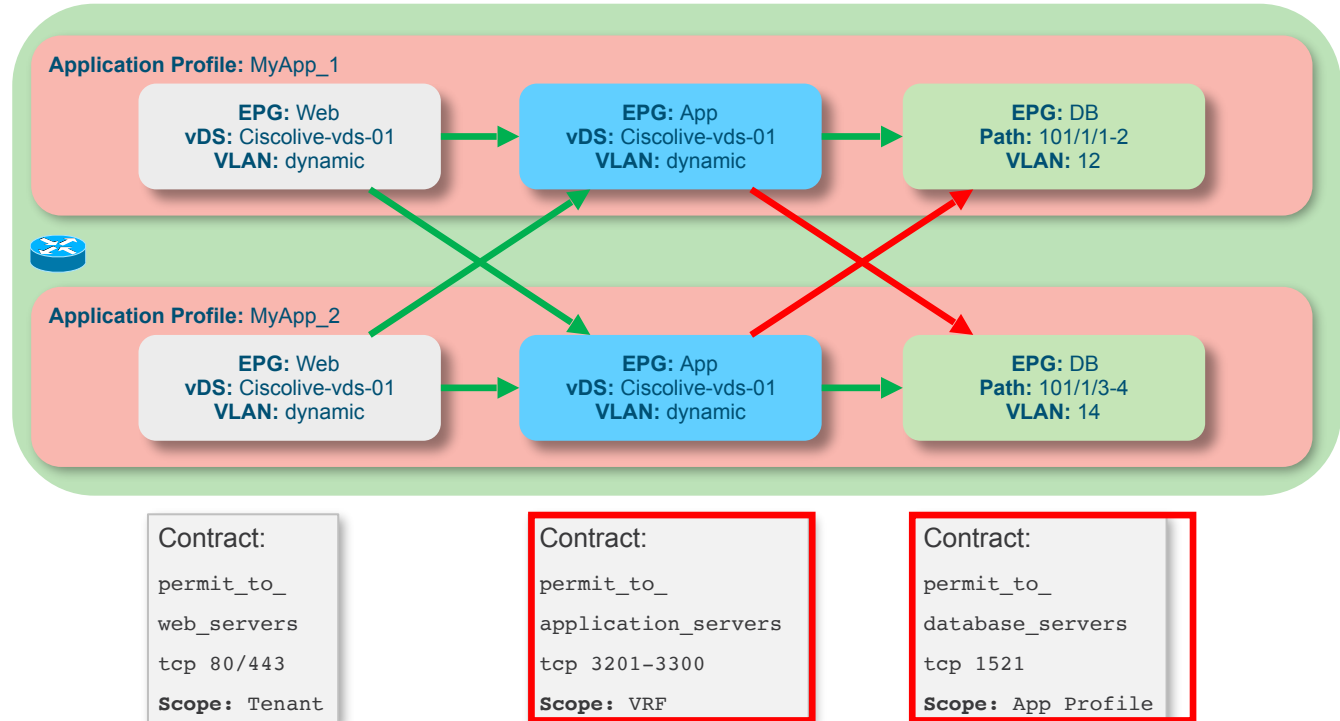
- Global
- Tenant
- VRF
- Application Profile



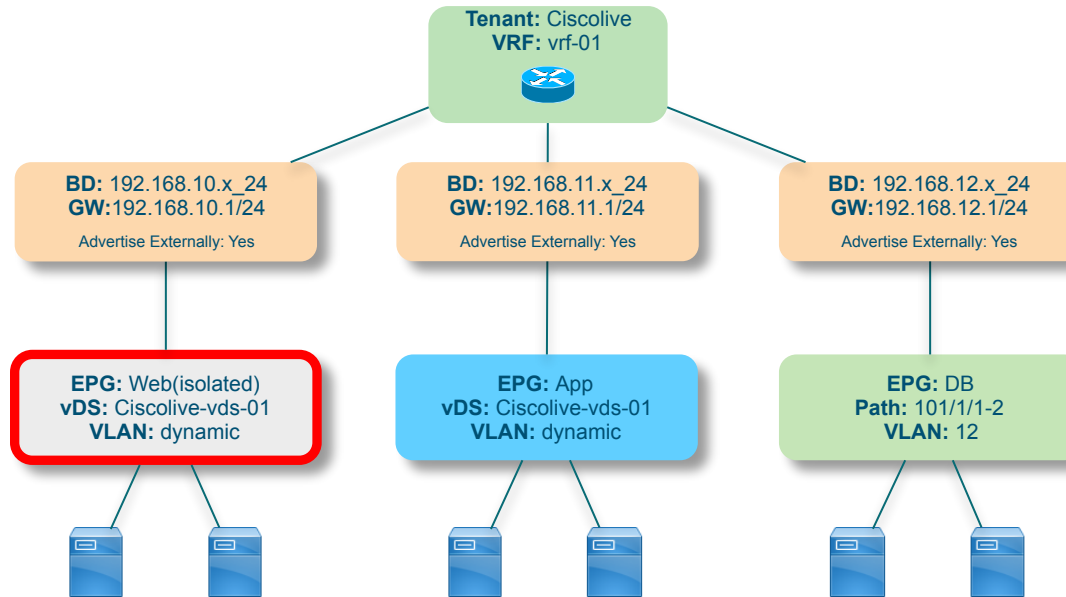
Contract Scope

Contract enforcement is “scoped” at:

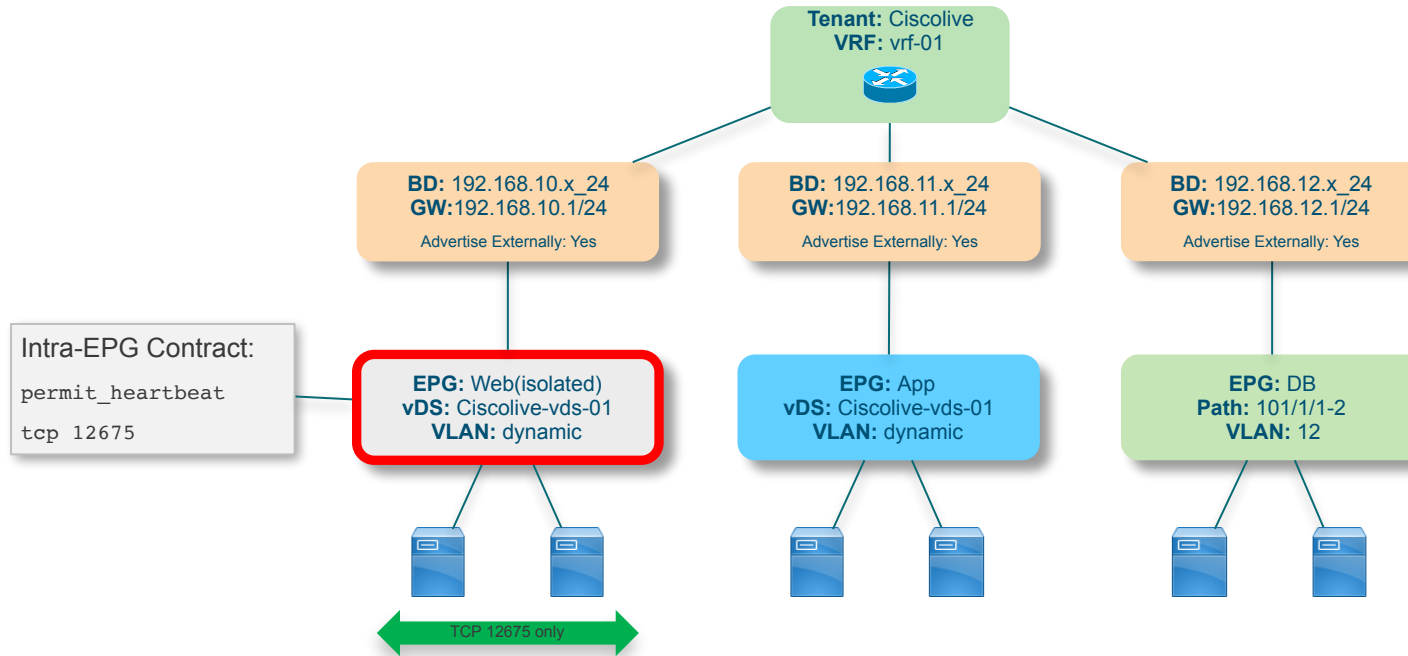
- Global
- Tenant
- VRF
- Application Profile



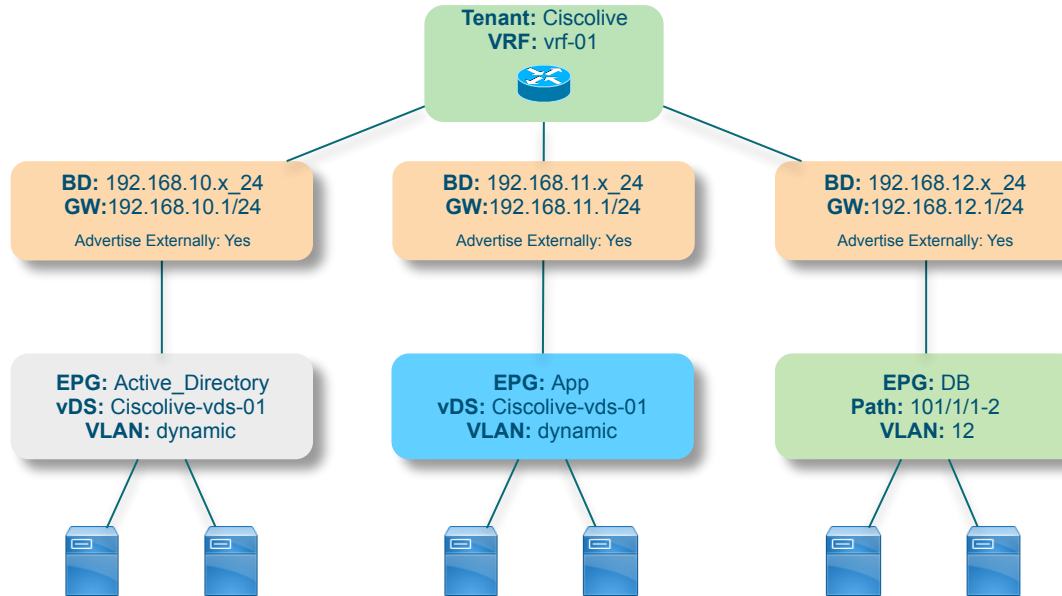
Intra-EPG Contract



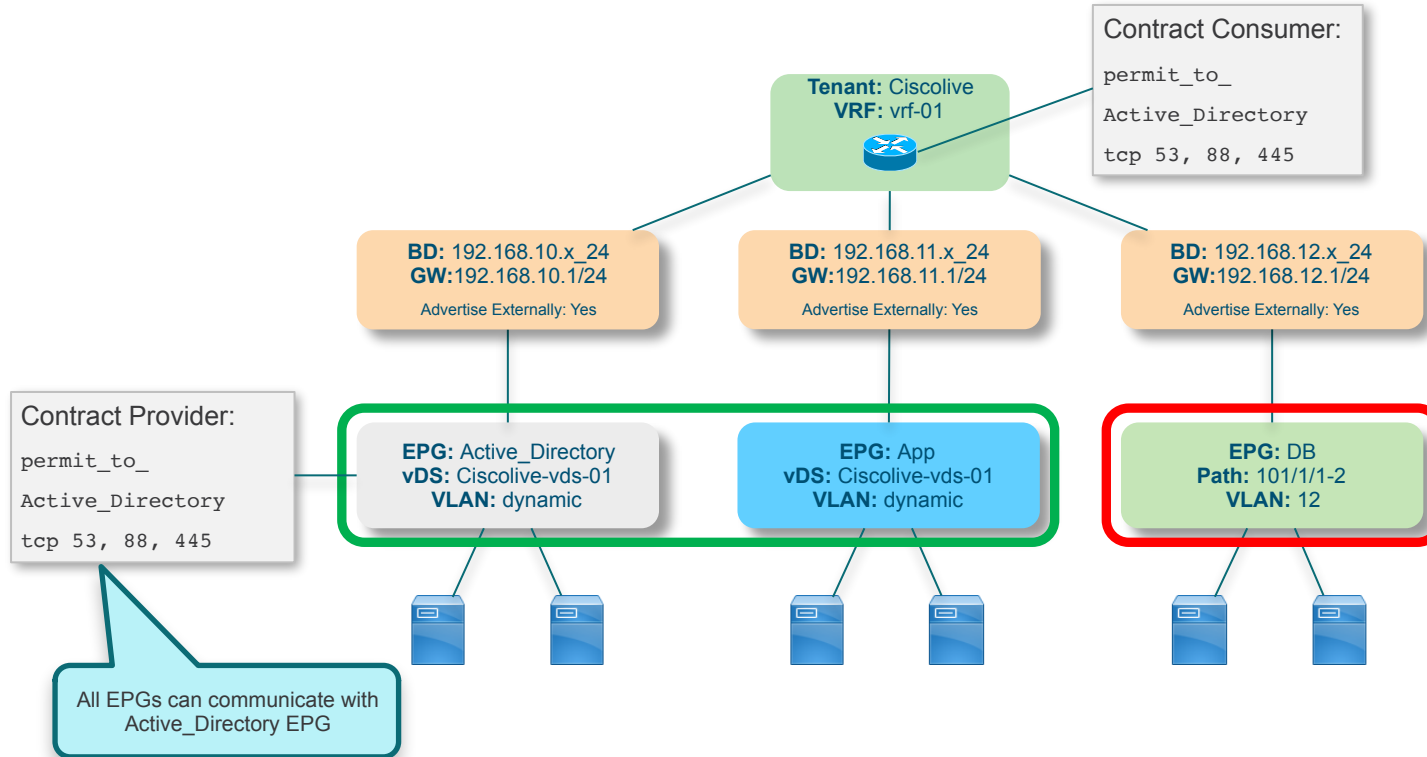
Intra-EPG Contract



Contract Preferred Groups

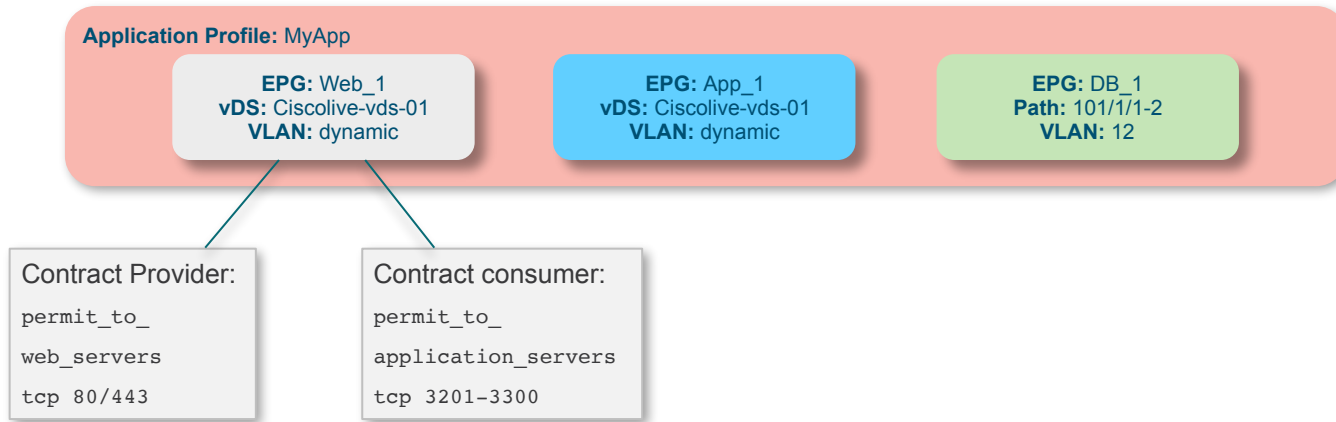


Contract Preferred Groups

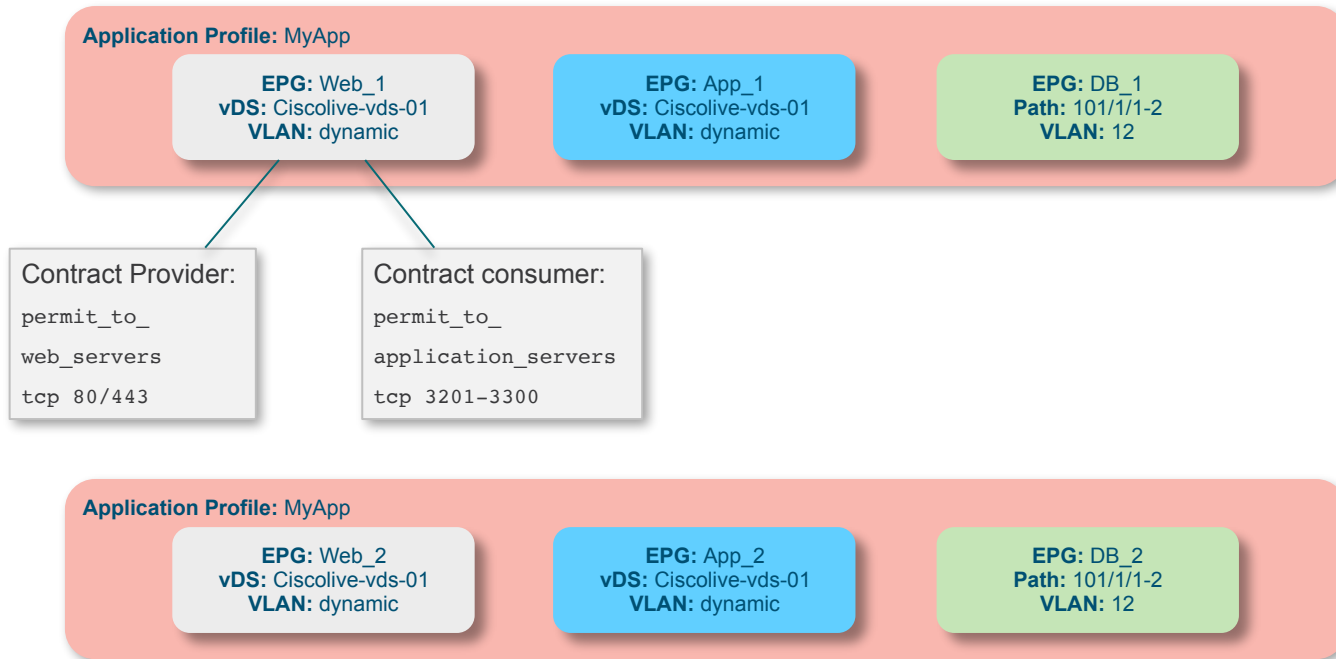


Contracts Inheritance

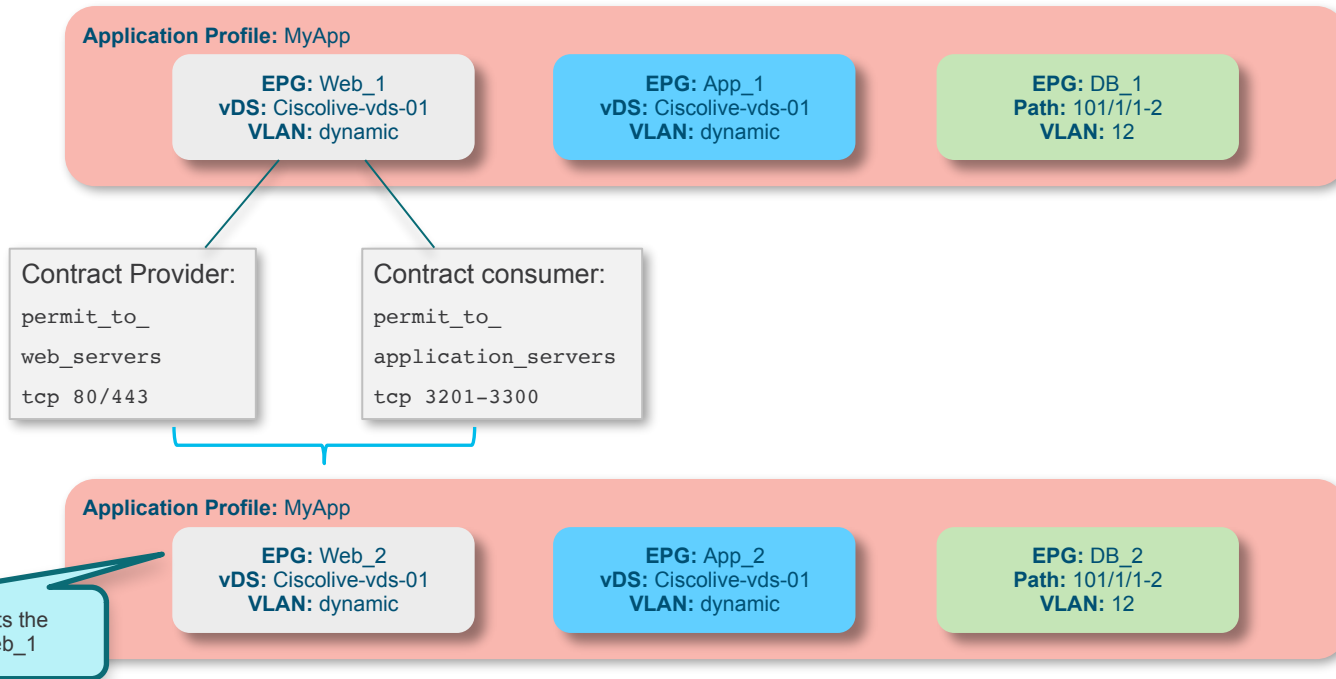
Contracts Inheritance



Contracts Inheritance



Contracts Inheritance



Checking the Provided/Consumed Contracts

```
apic1# show epg
Tenant      Application  AEPg      Consumed Contracts      Provided Contracts      Denied Contracts      Description
-----
Ciscolive   MyApp        App        permit_to_database_servers  permit_to_application_servers
Ciscolive   MyApp        DB          permit_to_database_servers
Ciscolive   MyApp        Web        permit_to_application_servers  permit_to_web_servers
```

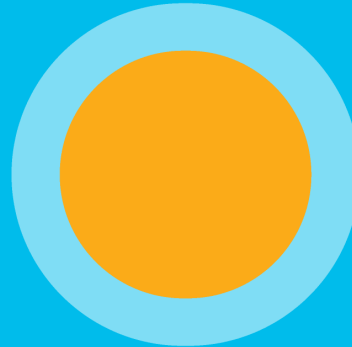
Tenant	Application	AEPg	Consumed Contracts	Provided Contracts	Denied Contracts	Description
Ciscolive	MyApp	App	permit_to_database_servers	permit_to_application_servers		MyApp App
Ciscolive	MyApp	DB		permit_to_database_servers		MyApp DB
Ciscolive	MyApp	Web	permit_to_application_servers	permit_to_web_servers		MyApp Web

Checking the Provided/Consumed Contracts

```
apic1# show epq
```

Tenant	Application	AEPg	Consumed Contracts	Provided Contracts	Denied Contracts	Description
Ciscolive	MyApp	App	permit_to_database_servers	permit_to_application_servers		MyApp App
Ciscolive	MyApp	DB		permit_to_database_servers		MyApp DB
Ciscolive	MyApp	Web	permit_to_application_servers	permit_to_web_servers		MyApp Web

What happens if I don't know the required Filter ports?



Filter discovery

- Ask the Application Owner – it's their application, they will (ok should) know
- Ask the Security Admin for the firewall rules
- Use an “any-any” Filter between EPGs ← Most customers start here
- Install Tetration for Application Dependency Mapping
- Use Wireshark
- Configure “Unenforced” mode on the VRF

Deep Dive – Bridge Domains



Bridge Domain Forwarding Options

Hardware Proxy (default)

- Unknown Unicast sent to Spine Proxy (forward/discarded)
- Removes unknown unicast flooding

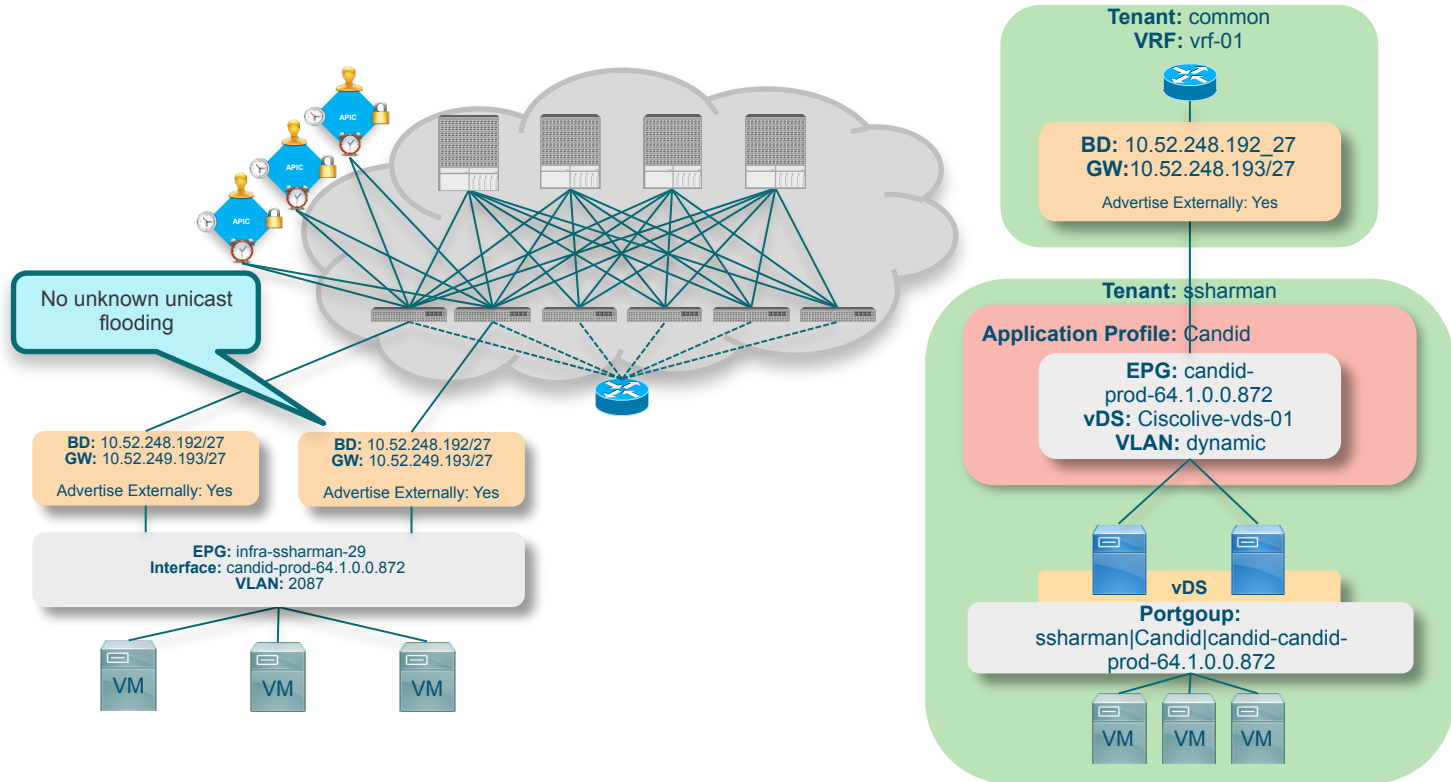
Flood and Learn

- Unknown Unicast flooded over multicast tree and constrained in BD or Encap

Bridge Domain Forwarding – Hardware Proxy (Unicast Routing)

Bridge Domain Forwarding – Hardware Proxy

Bridge Domain Forwarding – Hardware Proxy



Bridge Domain Forwarding – Hardware Proxy

Bridge Domain Forwarding – Hardware Proxy

The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The left sidebar shows the navigation tree with 'Bridge Domains' expanded, and the specific Bridge Domain '10.52.248.192_27' is selected. The main panel shows the configuration for this Bridge Domain, titled 'Bridge Domain - 10.52.248.192_27'. The 'General' tab is active, showing various properties and forwarding options. A red box highlights the 'Resolved VRF: common/vrf-01' section, which includes the following settings:

- L2 Unknown Unicast:** Flood, Hardware Proxy (selected)
- L3 Unknown Multicast Flooding:** Flood, Optimized Flood (selected)
- Multi Destination Flooding:** Flood in BD (selected), Drop, Flood in Encapsulation
- PIM:** ☐
- IGMP Policy:** select an option
- ARP Flooding:** ☐
- Endpoint Dataplane Learning:** ☒
- Limit IP Learning To Subnet:** ☒
- End Point Retention Policy:** select a value
- IGMP Snoop Policy:** select a value

The bottom of the interface includes buttons for 'Show Usage', 'Reset', and 'Submit'.

Bridge Domain Forwarding – Hardware Proxy

The image displays the Cisco APIC interface for configuring a Bridge Domain. The left pane shows the navigation tree with 'Bridge Domains' selected. The main pane shows the configuration for the Bridge Domain 10.52.248.192_27. The 'Properties' section is expanded, showing 'Unicast Routing' checked and 'Hardware Proxy' selected under 'L2 Unknown Unicast'. The 'Subnets' table shows the Gateway Address 10.52.248.193/27 with the scope 'Advertised Externally'.

Bridge Domain - 10.52.248.192_27

Properties

Name: 10.52.248.192_27
Alias:
Description: Corporate address range
Type: fc regular
Global Alias:
Legacy Mode: No
VRF: vrf-01
Resolved VRF: common/vrf-01

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: ☐
Endpoint Dataplane Learning: ☒
Limit IP Learning To Subnet: ☒
End Point Retention Policy: select a value
This policy only applies to local L2, L3, and remote L3 entries
IGMP Snoop Policy: select a value

Subnets

Gateway Address	Scope	Primary IP Address	Virtual IP	Subnet Control
10.52.248.193/27	Advertised Externally	False	False	

Associated L3 Out:

L3 Out
OSPF_to_external_vrf-global

L3 Out for Route Profile: select a value
Route Profile: select value
Link-local IPv6 Address:
ND policy: select a value

Bridge Domain Forwarding – Hardware Proxy

If the destination Mac/IP is not known the packet is sent to the Spine proxy database, where it will be forwarded or discarded

The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. On the left, the 'Tenant common' sidebar shows the navigation tree with 'Bridge Domains' selected. The main area shows the configuration for 'Tenant ssharman' and 'EPG - candid-prod-64.1.0.0.872'. A red box highlights the 'candid-prod-64.1.0.0.872' entry in the 'Candid' list. Another red box highlights the 'Client End-Points' table, which lists learned MAC and IP addresses for the EPG. A callout bubble points to the table with the text 'EPG learns Mac and IP Addresses'.

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
candid-prod-...	00:50:56:99:08:11	10.52.248.203	learned vmm	192.168.10.11	ssharmar-...	10.52.249.5 (vmm) 10.52.249.6 (vmm) Pod-1/Node-101/eth1/22 ...	---	vlan-2087
candid-prod-...	00:50:56:99:B4:7B	10.52.248.204	learned vmm	192.168.10.12	ssharmar-...	10.52.249.5 (vmm) 10.52.249.6 (vmm) Pod-1/Node-101/eth1/21 ...	---	vlan-2087
candid-prod-...	00:50:56:99:EF:B3	10.52.248.202	learned vmm	192.168.10.12	ssharmar-...	10.52.249.5 (vmm) 10.52.249.6 (vmm) Pod-1/Node-101/eth1/21 ...	---	vlan-2087

Endpoint Learning – Flood and Learn with Unicast Routing Enabled

```
apic1# show endpoints vlan 2087
```

Legends:

(P):Primary VLAN

(S):Secondary VLAN

Dynamic Endpoints:

Tenant : ssharman

Application : Candid

AEPg : candid-prod-64.1.0.0.872

End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:50:56:99:08:11	10.52.248.203	101	eth1/22	vlan-2087	not-applicable
00:50:56:99:B4:7B	10.52.248.204	101	eth1/21	vlan-2087	not-applicable
00:50:56:99:EF:B3	10.52.248.202	101	eth1/21	vlan-2087	not-applicable

Total Dynamic Endpoints: 3

Total Static Endpoints: 0

Endpoint Learning – Flood and Learn with Unicast Routing Enabled

```
apic1# show endpoints vlan 2087
```

Legends:

(P):Primary VLAN

(S):Secondary VLAN

Dynamic Endpoints:

Tenant : ssharman

Application : Candid

AEPg : candid-prod-64.1.0.0.872

End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:50:56:99:08:11	10.52.248.203	101	eth1/22	vlan-2087	not-applicable
00:50:56:99:B4:7B	10.52.248.204	101	eth1/21	vlan-2087	not-applicable
00:50:56:99:EF:D3	10.52.248.202	101	eth1/21	vlan-2087	not-applicable

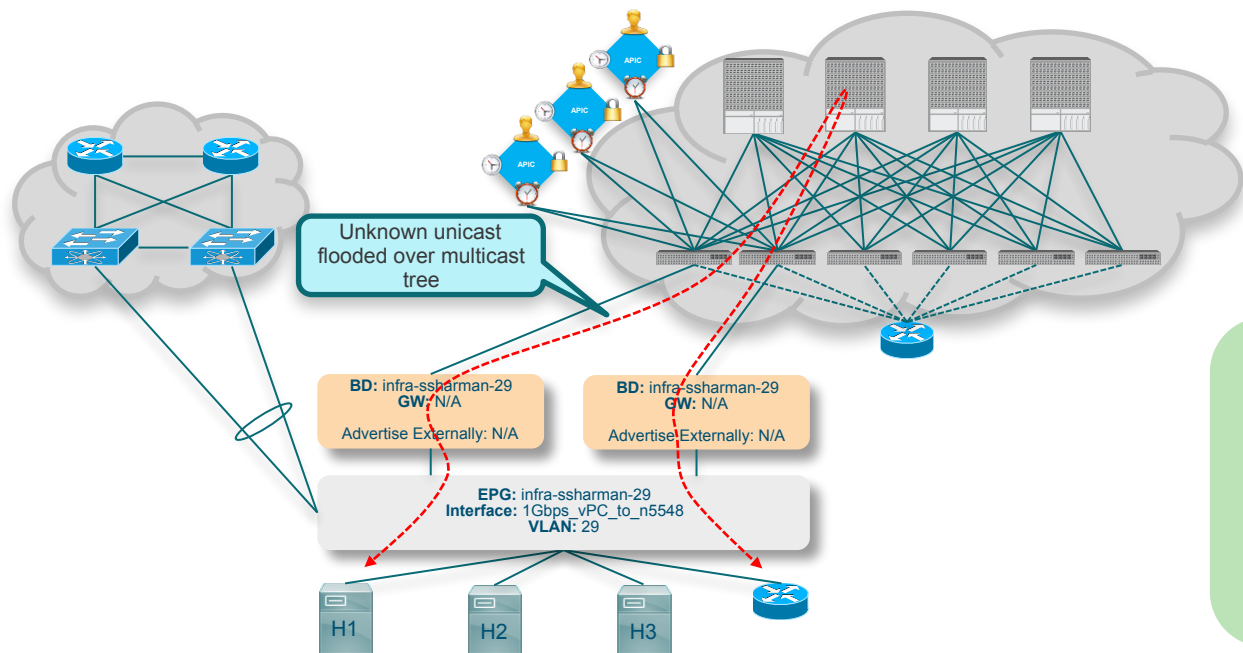
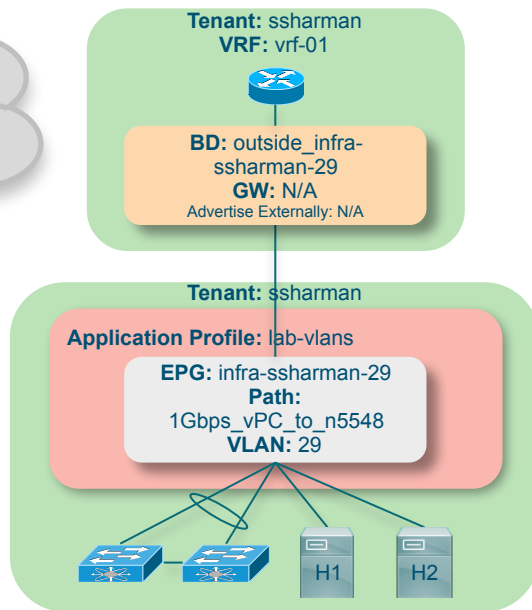
Total Dynamic Endpoints: 3

Total Static Endpoints: 0

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Disabled

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Disabled

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Disabled



Bridge Domain Forwarding – Flood and Learn with Unicast Routing Disabled

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Disabled

Unknown Unicast flooded over multicast tree and constrained in BD or Encap

The screenshot shows the Cisco APIC interface for configuring a Bridge Domain. The left sidebar shows the navigation tree with 'outside_infra-ssharm-29' selected. The main panel displays the configuration for this Bridge Domain, with the 'General' tab active. A red box highlights the 'Resolved VRF' configuration section, which includes the following settings:

- 2 Unknown Unicast: Flood
- 2 Unknown Unicast: Hardware Proxy
- L3 Unknown Unicast Flooding: Flood
- L3 Unknown Unicast Flooding: Optimized Flood
- Multi Destination Flooding: Flood in BD
- Multi Destination Flooding: Drop
- Multi Destination Flooding: Flood in Encapsulation
- PIM: ☐
- IGMP Proxy: select an option
- ARP Flooding: ☒
- Endpoint Dataplane Learning: ☒
- Clear Remote MAC Entries: ☐
- Limit IP Learning To Subnet: ☐
- End Point Retention Policy: select a value

A callout bubble points to the 'ARP Flooding' checkbox with the text: "ARP is always flooded when Hardware Proxy is disabled".

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Disabled

Unknown Unicast flooded over multicast tree and constrained in BD or Encap

The image displays two screenshots of the Cisco APIC interface for configuring a Bridge Domain. The left screenshot shows the 'Properties' tab for Bridge Domain 'outside_infra-ssharmar-29'. A red box highlights the 'ARP Flooding' section, which includes options for 'Flood', 'Drop', and 'Flood in Encapsulation'. A callout points to this section, stating: "ARP is always flooded when Hardware Proxy is disabled". The right screenshot shows the 'L3 Configurations' tab for the same Bridge Domain. A red box highlights the 'Unicast Routing' checkbox, which is currently unchecked. A callout points to this checkbox, stating: "Unicast routing enables/disables the learning of IP addresses for a given BD". Another callout points to the 'ARP Flooding' section on the left, stating: "If Unicast routing is disabled ARP is always flooded".

Unicast routing enables/disables the learning of IP addresses for a given BD

ARP is always flooded when Hardware Proxy is disabled

If Unicast routing is disabled ARP is always flooded

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Disabled

Unknown Unicast flooded over multicast tree and constrained in BD or Encap

The screenshot displays the Cisco APIC GUI. On the left, the 'Tenant ssharman' sidebar shows a tree structure with 'outside_infra-ssharm-29' and 'infra-ssharm-29' highlighted. A callout box points to the 'outside_infra-ssharm-29' entry with the text 'ARP is always Hardware Pr'. The main panel shows the 'EPG - infra-ssharm-29' configuration. The 'Client End-Points' tab is active, displaying a table of learned endpoints. A red box highlights the first five rows of the table, and a callout box points to it with the text 'EPG only learns Mac Addresses'. The table has columns for End Point, MAC, IP, Learning Source, Hosting Server, Reporting Controller Name, Interface, Multicast Address, and Encap. The right sidebar shows 'L3 Configurations' and 'Advanced/Troubleshooting' tabs.

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
EP-00:00:...	00:00:0C:07:AC:1D	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:18:...	00:18:74:E2:15:40	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:1A:...	00:1A:A2:D5:C0:80	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:26:...	00:26:0B:F1:F0:02	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:50:...	00:50:56:86:25:74	---	learned	---	---	Pod-1/Node-102/eth1/21 ...	---	vlan-29

Endpoint Learning – Flood and Learn with Unicast Routing Disabled

```
apic1# show endpoints vlan 29
Legends:
(P):Primary VLAN
(S):Secondary VLAN
Dynamic Endpoints:
Tenant      : ssharman
Application : lab-vlans
AEPg       : infra-ssharman-29
```

End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:00:0C:07:AC:1D	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:18:74:E2:15:40	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:1A:A2:D5:C0:80	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:26:0B:F1:F0:02	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:50:56:86:25:74	---	102	eth1/21	vlan-29	not-applicable

Total Dynamic Endpoints: 5

Total Static Endpoints: 0

Endpoint Learning – Flood and Learn with Unicast Routing Disabled

```
apic1# show endpoints vlan 29
```

Legends:

(P):Primary VLAN

(S):Secondary VLAN

Dynamic Endpoints:

Tenant : ssharman

Application : lab-vlans

AE Pg : infra-ssharman-29

End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:00:0C:07:AC:1D	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:18:74:E2:15:40	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:1A:A2:D5:C0:80	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:26:0B:F1:F0:02	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:50:50:50:23:74	---	102	eth1/21	vlan-29	not-applicable

Total Dynamic Endpoints: 5

Total Static Endpoints: 0

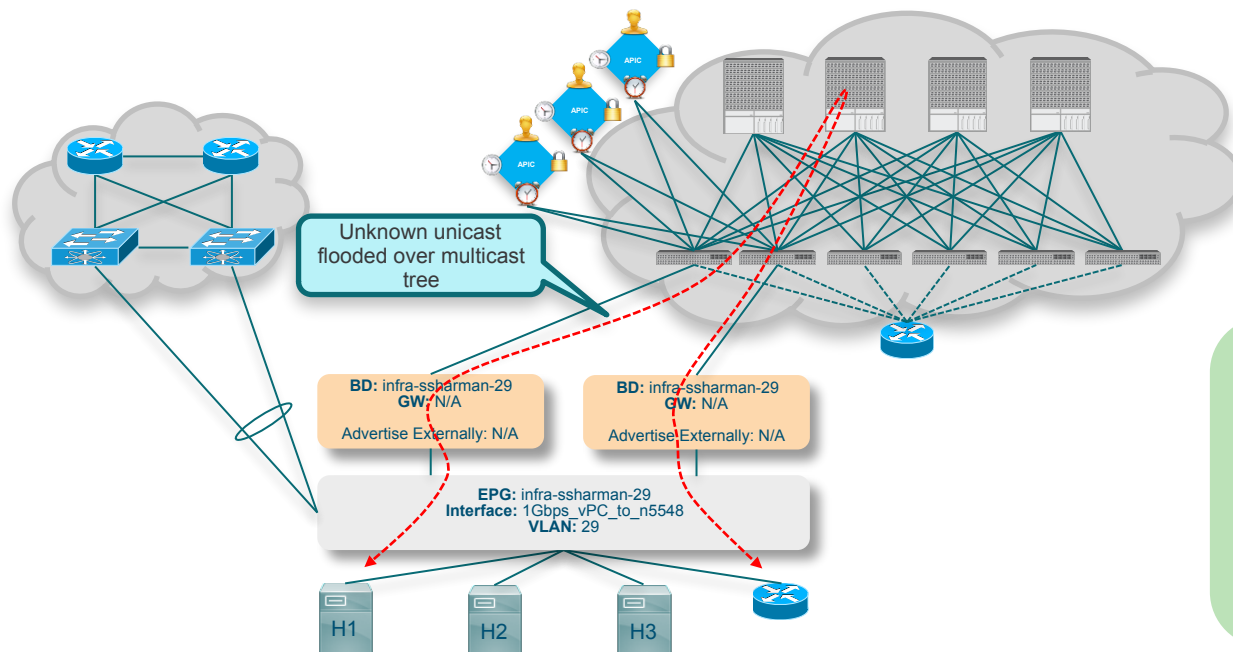
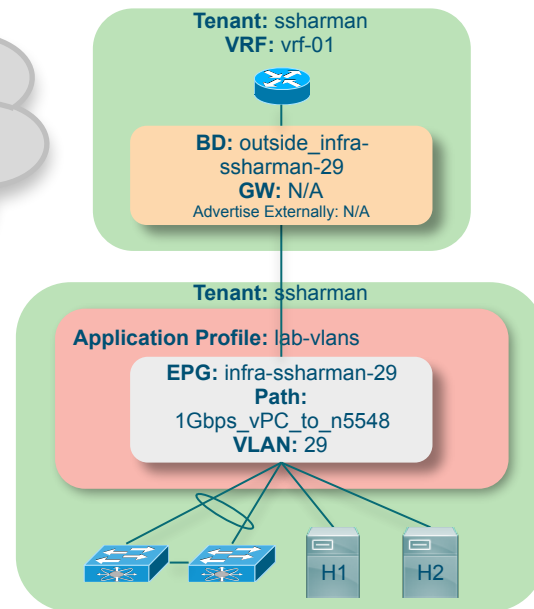


Bridge Domain Forwarding – Flood and Learn with Unicast Routing Enabled

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Enabled



Bridge Domain Forwarding – Flood and Learn with Unicast Routing Enabled



Bridge Domain Forwarding – Flood and Learn with Unicast Routing Enabled



Bridge Domain Forwarding – Flood and Learn with Unicast Routing Enabled



The screenshot displays the Cisco APIC interface for configuring a Bridge Domain. The left sidebar shows the navigation tree with 'outside_infra-ssharmman-29' selected. The main panel shows the configuration for this Bridge Domain, with a red box highlighting the forwarding settings:

- Name:** outside_infra-ssharmman-29
- Alias:** (empty)
- Description:** optional
- Type:** regular
- Global Alias:** (empty)
- Legacy Mode:** No
- VRF:** vrf-01
- Resolved VRF:** ssharmman/vrf-01
- L2 Unknown Unicast:** Flood
- L3 Unknown Multicast Flooding:** Flood
- Multi Destination Flooding:** Flood in BD
- PIM:** (unchecked)
- IGMP Policy:** select an option
- ARP Flooding:** (checked)
- Endpoint Dataplane Learning:** (checked)
- Clear Remote MAC Entries:** (unchecked)
- Limit IP Learning To Subnet:** (unchecked)
- End Point Retention Policy:** select a value

Buttons at the bottom include 'Show Usage', 'Reset', and 'Submit'.

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Enabled



Bridge Domain - outside_infra-ssharmar-29

Properties

Name: outside_infra-ssharmar-29

Alias:

Description: optional

Type: fc regular

Global Alias:

Legacy Mode: No

VRF: vrf-01

Resolved VRF: ssharmar/vrf-01

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: ☒

Endpoint Dataplane Learning: ☒

Clear Remote MAC Entries: ☐

Limit IP Learning To Subnet: ☐

End Point Retention Policy: select a value

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

Unicast Routing: ☒

Operational Value for Unicast Routing: true

Custom MAC Address: 00:22:BD:F8:19:FF

Virtual MAC Address: Not Configured

Subnets:

Gateway Address	Scope	Primary IP Address	Virtual IP	Subnet Control
No items have been found. Select Actions to create a new item.				

EP Move Detection Mode: ☐ GARP based detection

Associated L3 Outs:

L3 Out
No items have been found. Select Actions to create a new item.

L3 Out for Route Profile: select a value

Route Profile: select a value

Link-local IPv6 Address: ::

ND policy: select a value

Show Usage Reset Submit

Bridge Domain Forwarding – Flood and Learn with Unicast Routing Enabled



Unknown Unicast flooded over multicast tree and constrained in BD or Encap

The screenshot displays the Cisco APIC GUI with the following components:

- Left Navigation Panel:** Shows the hierarchy for Tenant `ssharmar` > Bridge Domains > `outside_infra-ssharmar-29`. This item is highlighted with a red box.
- Main Content Area:** Displays the configuration for EPG `infra-ssharmar-29`. The `Client End-Points` tab is active, showing a table of learned endpoints. A red box highlights the first five rows of the table.
- Table Data:**

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
EP-00:00:...	00:00:0C:07:AC:1D	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:18:...	00:18:74:E2:15:40	192.168.29.2	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:1A:...	00:1A:A2:D5:C0:80	192.168.29.3	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:26:...	00:26:0B:F1:F0:02	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-29
EP-00:50:...	00:50:56:86:25:74	192.168.29.10	learned	---	---	Pod-1/Node-102/eth1/21 ...	---	vlan-29

- Callout:** A blue speech bubble points to the table with the text: "EPG learns Mac and IP Addresses".
- Right Panel:** Shows the `L3 Configurations` tab, which is also highlighted with a red box.

Endpoint Learning – Flood and Learn with Unicast Routing Enabled



```
apic1# show endpoints vlan 29
```

Legends:

(P):Primary VLAN

(S):Secondary VLAN

Dynamic Endpoints:

Tenant : ssharman

Application : lab-vlans

AEPg : infra-ssharman-29

End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:00:0C:07:AC:1D	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:18:74:E2:15:40	192.168.29.2	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:1A:A2:D5:C0:80	192.168.29.3	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:26:0B:F1:F0:02	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:50:56:86:25:74	192.168.29.10	102	eth1/21	vlan-29	not-applicable

Total Dynamic Endpoints: 5

Total Static Endpoints: 0

Endpoint Learning – Flood and Learn with Unicast Routing Enabled



```
apic1# show endpoints vlan 29
```

Legends:

(P):Primary VLAN

(S):Secondary VLAN

Dynamic Endpoints:

Tenant : ssharman

Application : lab-vlans

AEPg : infra-ssharman-29

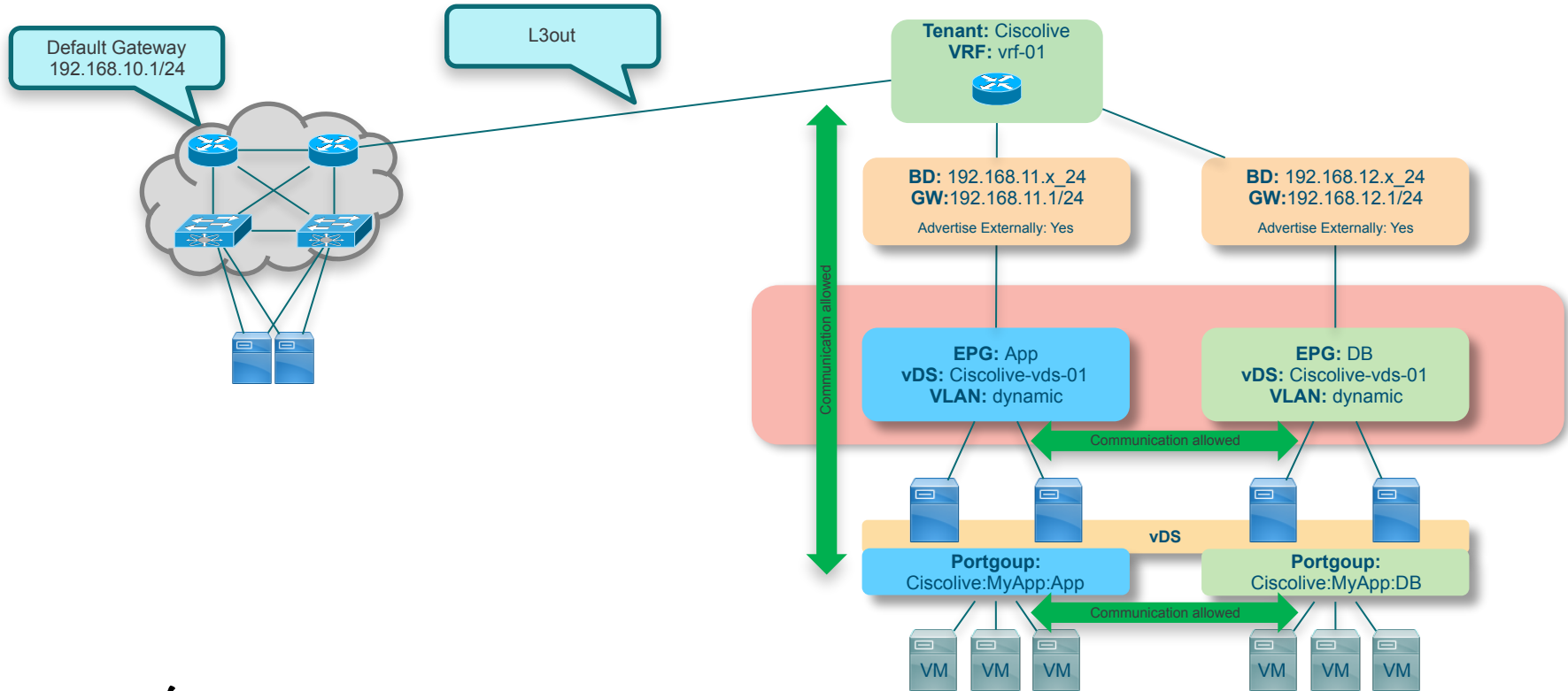
End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:00:0C:07:AC:1D	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:18:74:E2:15:40	192.168.29.2	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:1A:A2:D5:C0:80	192.168.29.3	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:26:0B:F1:F0:02	---	101 102	vpc 1Gbps_vPC_to_n5548	vlan-29	not-applicable
00:50:56:86:25:74	192.168.29.10	102	eth1/21	vlan-29	not-applicable

Total Dynamic Endpoints: 5

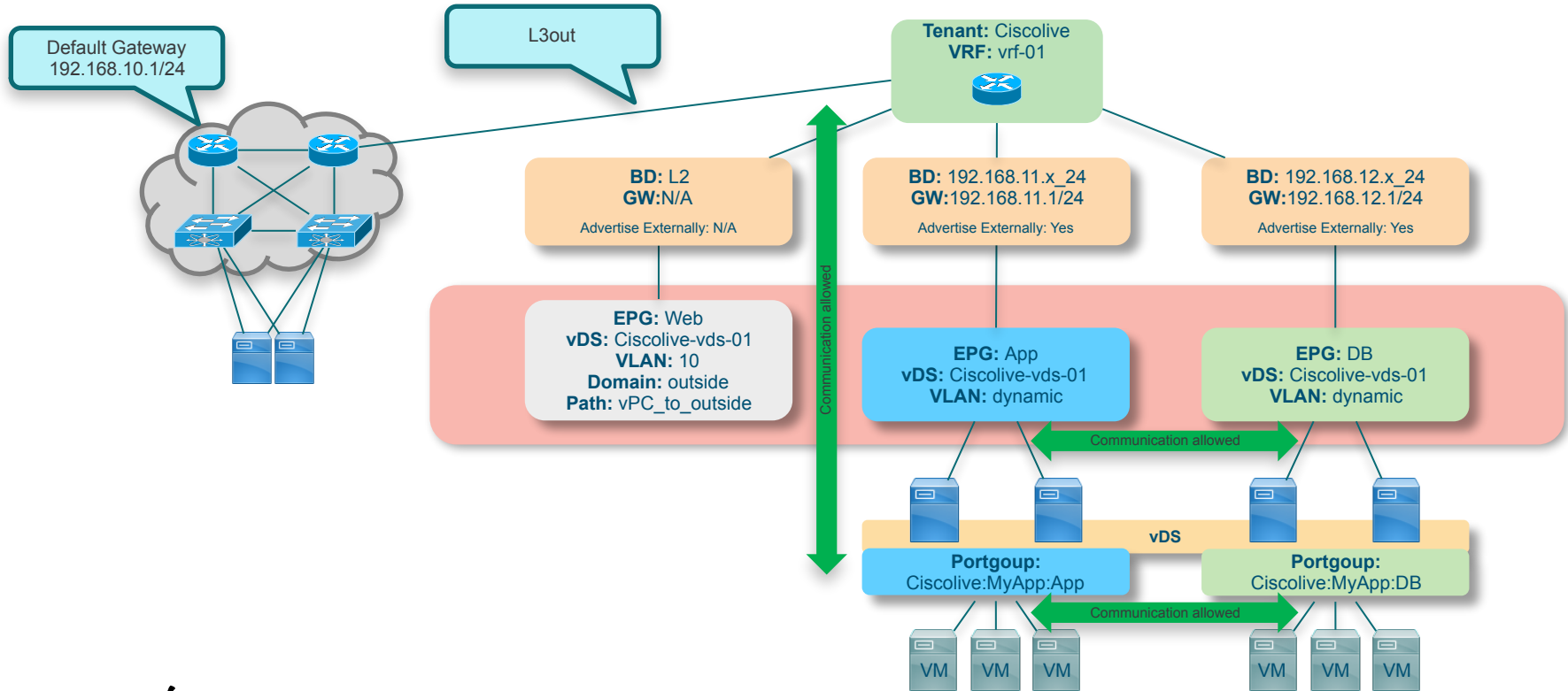
Total Static Endpoints: 0

Why should we be cautious with Unicast Routing Enabled
and no SVI configured...?

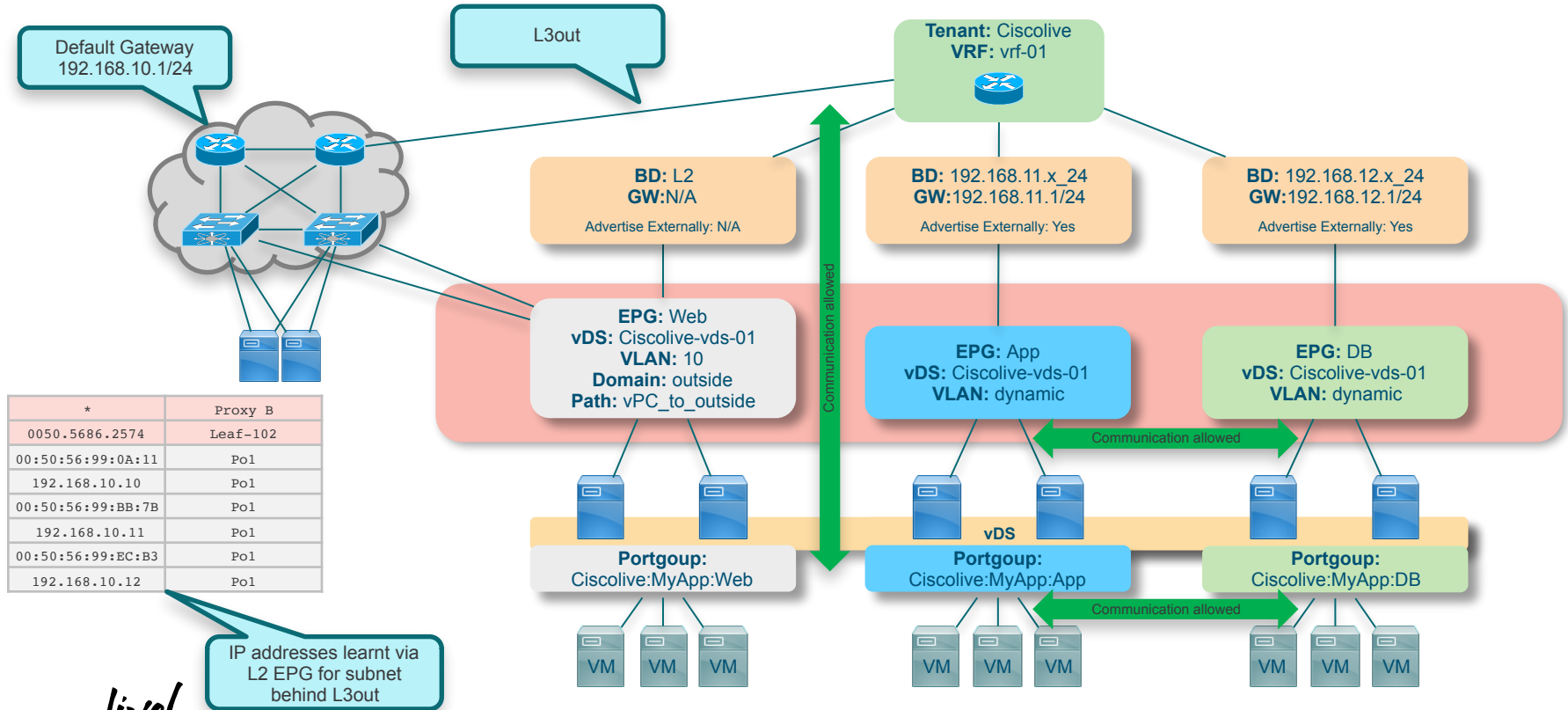
Subnet behind L3out



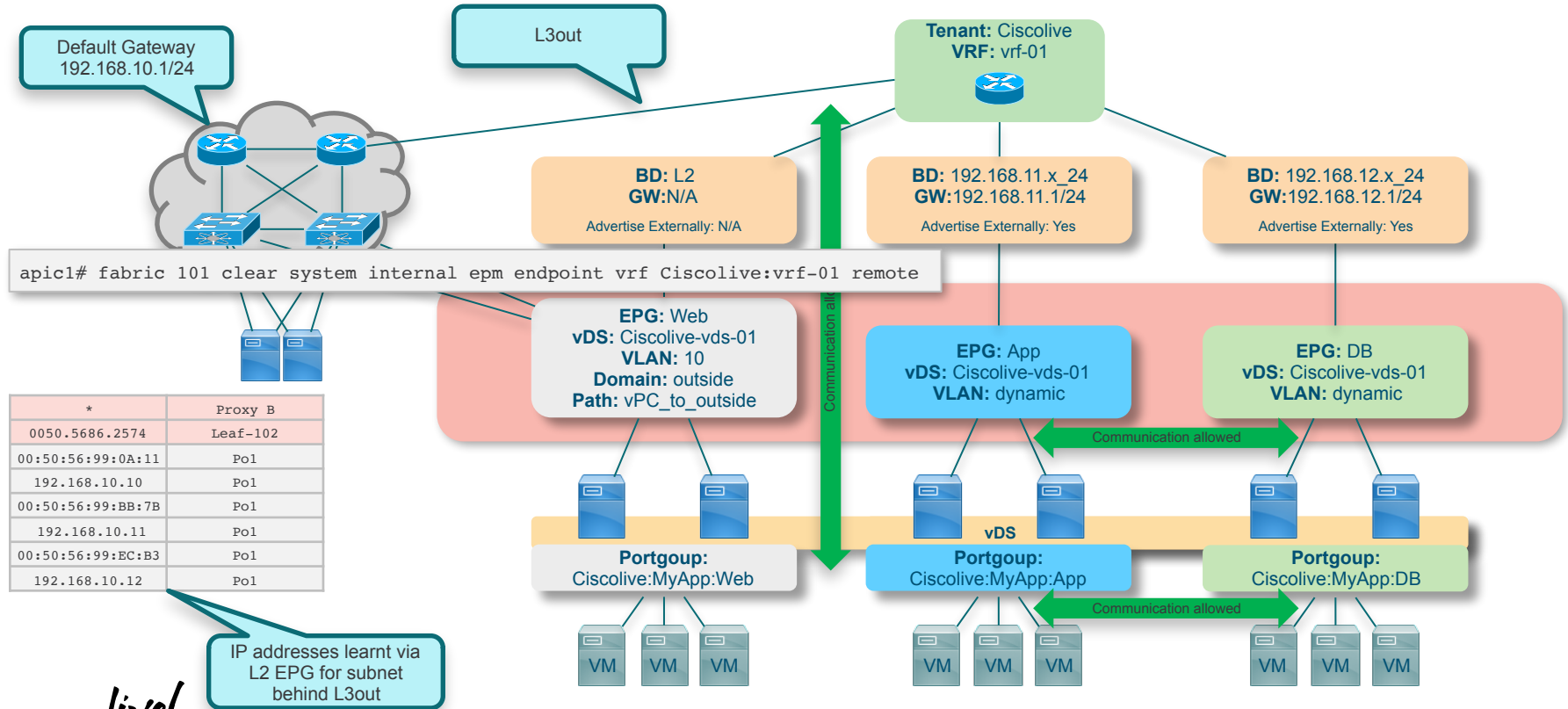
Subnet behind L3out



Subnet behind L3out



Subnet behind L3out



How do we prevent this scenario...?

Enforce Subnet Check on Bridge Domain to prevent IP Learning

The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The left sidebar shows the navigation tree with 'Tenant ssharman' selected, and 'Bridge Domains' expanded. The main content area shows the configuration for 'Bridge Domain - outside_infra-ssharman-29'. The 'Properties' tab is active, showing fields for Name, Alias, Description, Type (set to 'regular'), Global Alias, Legacy Mode (set to 'No'), VRF (set to 'vrf-01'), and Resolved VRF (set to 'ssharman/vrf-01'). The 'L2 Unknown Unicast' policy is set to 'Flood', and 'L3 Unknown Multicast Flooding' is set to 'Flood'. The 'Multi Destination Flooding' policy is set to 'Flood in BD'. The 'PIM' checkbox is unchecked, and the 'IGMP Policy' is set to 'select an option'. The 'ARP Flooding' checkbox is checked, and the 'Endpoint Dataplane Learning' checkbox is checked. The 'Clear Remote MAC Entries' checkbox is unchecked, and the 'Limit IP Learning To Subnet' checkbox is checked. The 'End Point Retention Policy' is set to 'select a value'. The 'Bridge Domain - outside_infra-ssharman-29' configuration is also visible in the background, showing the 'L3 Configurations' tab with 'Unicast Routing' checked and 'Operational Value for Unicast Routing' set to 'true'. The 'Subnets' table is empty, and the 'EP Move Detection Mode' is set to 'GARP based detection'. The 'Associated L3 Outs' table is also empty. The 'L3 Out for Route Profile' is set to 'select a value', the 'Route Profile' is set to 'select a value', the 'Link-local IPv6 Address' is set to '::', and the 'ND policy' is set to 'select a value'. The 'Show Usage', 'Reset', and 'Submit' buttons are visible at the bottom right.

Tenant ssharman

- Quick Start
- Tenant ssharman
 - Application Profiles
 - Networking
 - Bridge Domains
 - 192.168.10.x_24
 - 192.168.11.x_24
 - 192.168.200.x_24
 - 192.168.201.x_24
 - 192.168.202.x_24
 - outside_infra-ssharman-12
 - outside_infra-ssharman-13
 - outside_infra-ssharman-14
 - outside_infra-ssharman-29**
 - VRFs
 - External Bridged Networks
 - External Routed Networks
 - Protocol Policies
 - Dot1Q Tunnels
 - L4-L7 Service Parameters
 - DNS Server Groups (Beta)
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services
 - NetFlow

Bridge Domain - outside_infra-ssharman-29

Properties

Name: outside_infra-ssharman-29

Alias:

Description: optional

Type: fc **regular**

Global Alias:

Legacy Mode: No

VRF: vrf-01

Resolved VRF: ssharman/vrf-01

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: ☒

Endpoint Dataplane Learning: ☒

Clear Remote MAC Entries: ☐

Limit IP Learning To Subnet: ☒

End Point Retention Policy: select a value

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

Bridge Domain - outside_infra-ssharman-29

L3 Configurations

Unicast Routing: ☒

Operational Value for Unicast Routing: true

Custom MAC Address: 00:22:BD:F8:19:FF

Virtual MAC Address: Not Configured

Subnets

Gateway Address	Scope	Primary IP Address	Virtual IP	Subnet Control
No items have been found. Select Actions to create a new item.				

EP Move Detection Mode: ☐ GARP based detection

Associated L3 Outs:

L3 Out
No items have been found. Select Actions to create a new item.

L3 Out for Route Profile: select a value

Route Profile: select a value

Link-local IPv6 Address: ::

ND policy: select a value

Show Usage **Reset** **Submit**

Enforce Subnet Check on Bridge Domain to prevent IP Learning

The screenshot displays the Cisco APIC interface for configuring a Bridge Domain. The left sidebar shows the navigation tree with 'outside_infra-ssharmen-29' selected under Bridge Domains. The main panel shows the configuration for 'Bridge Domain - outside_infra-ssharmen-29'.

Bridge Domain - outside_infra-ssharmen-29

Properties

- Name: outside_infra-ssharmen-29
- Alias: [empty]
- Description: optional
- Type: fc **regular**
- Global Alias: [empty]
- Legacy Mode: No
- VRF: vrf-01
- Resolved VRF: ssharmen/vrf-01
- L2 Unknown Unicast: **Flood** Hardware Proxy
- L3 Unknown Multicast Flooding: **Flood** Optimized Flood
- Multi Destination Flooding: **Flood in BD** Drop Flood in Encapsulation
- PIM: [unchecked]
- IGMP Policy: select an option
- ARP Flooding: [checked]
- Endpoint Dataplane Learning: [checked]
- Clear Remote MAC Entries: [unchecked]
- Limit IP Learning To Subnet: [checked]**
- End Point Retention Policy: select a value

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

Bridge Domain - outside_infra-ssharmen-29

Properties

- Unicast Routing: [checked]**
- Operational Value for Unicast Routing: true
- Custom MAC Address: 00:22:BD:F8:19:FF
- Virtual MAC Address: Not Configured
- Subnets: [empty table]
- EP Move Detection Mode: [unchecked] GARP based detection
- Associated L3 Outs: [empty table]
- L3 Out for Route Profile: select a value
- Route Profile: select a value
- Link-local IPv6 Address: ::
- ND policy: select a value

Show Usage **Reset** **Submit**



Bridge Domain Configuration Recommendations

Generation 1

- Bridge Domain Configuration
 - Limit IP Learning To Subnet
- Fabric Wide Configuration
 - IP Aging Policy (enabled by default)
 - Disable Remote EP Learn (on border leaf)
 - Prerequisite is to set Tenant> Networking> VRFs> Policy Control Enforcement to Ingress on your VRF instances

Generation 2

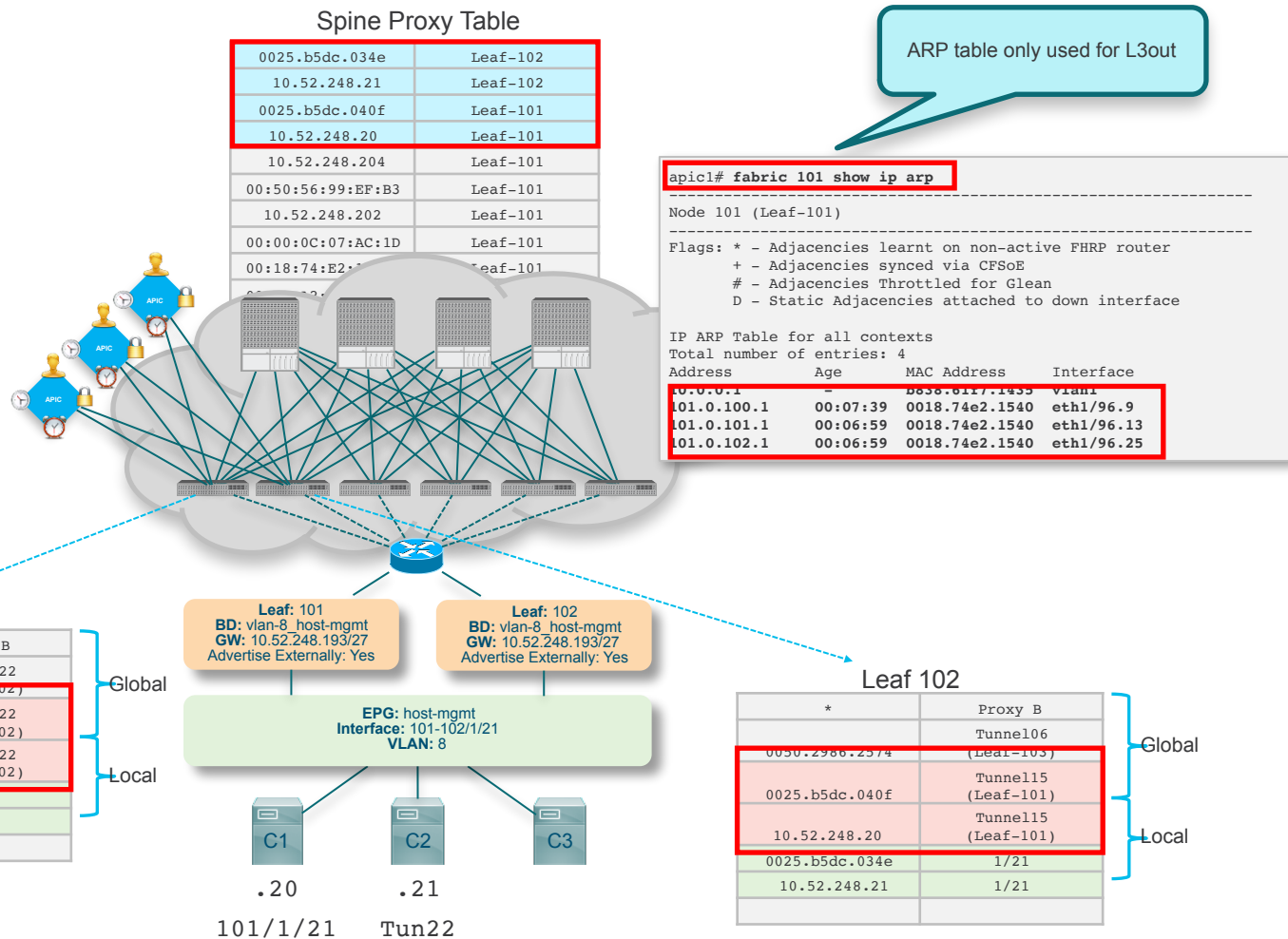
- Fabric Wide Configuration
 - IP Aging Policy (enabled by default)
 - Disable Remote EP Learn (on border leaf)
 - Prerequisite is to set Tenant> Networking> VRFs> Policy Control Enforcement to Ingress on your VRF instances
- Enforce Subnet Check

Mixed Leafs

- Bridge Domain Configuration
 - Limit IP Learning To Subnet
- Fabric Wide Configuration
 - IP Aging Policy (enabled by default)
 - Disable Remote EP Learn (on border leaf)
 - Prerequisite is to set Tenant> Networking> VRFs> Policy Control Enforcement to Ingress on your VRF instances
- Enforce Subnet Check

Deep Dive – EPG Forwarding

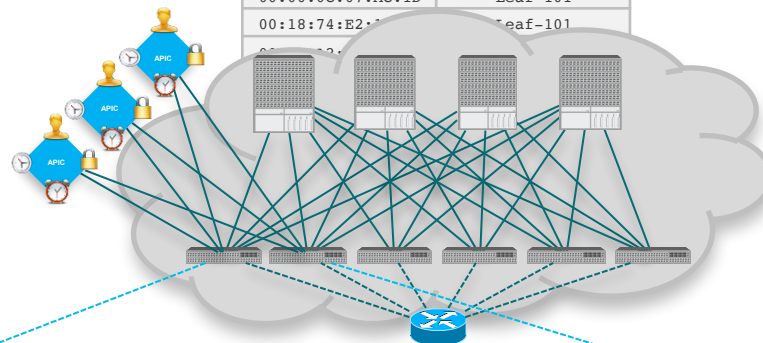
Packet Walk



Packet Walk

Spine Proxy Table

0025.b5dc.034e	Leaf-102
10.52.248.21	Leaf-102
0025.b5dc.040f	Leaf-101
10.52.248.20	Leaf-101
10.52.248.204	Leaf-101
00:50:56:99:EF:B3	Leaf-101
10.52.248.202	Leaf-101
00:00:0C:07:AC:1D	Leaf-101
00:18:74:E2:5A:5A	Leaf-101



IP Payload

1 Packet Sourced from physical server

Leaf 101

*	Proxy B	
	Tunnel22 (Leaf-102)	Global
0050.3680.2574	Tunnel22 (Leaf-102)	Global
0025.b5dc.034e	Tunnel22 (Leaf-102)	Local
10.52.248.21	Tunnel22 (Leaf-102)	Local
0025.b5dc.040f	1/21	
10.52.248.20	1/21	

Leaf: 101
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

Leaf: 102
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

EPG: host-mgmt
Interface: 101-102/1/21
VLAN: 8

C1

C2

C3

.20

.21

101/1/21

Tun22

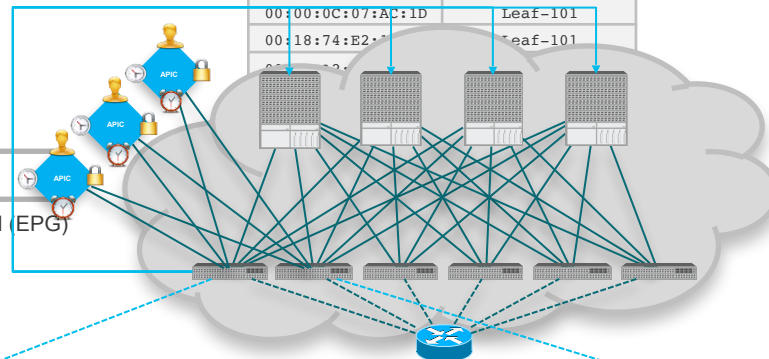
Leaf 102

*	Proxy B	
	Tunnel106 (Leaf-101)	Global
0050.2980.2574	Tunnel115 (Leaf-101)	Global
0025.b5dc.040f	Tunnel115 (Leaf-101)	Local
10.52.248.20	Tunnel115 (Leaf-101)	Local
0025.b5dc.034e	1/21	
10.52.248.21	1/21	

Packet Walk

Spine Proxy Table

0025.b5dc.034e	Leaf-102
10.52.248.21	Leaf-102
0025.b5dc.040f	Leaf-101
10.52.248.20	Leaf-101
10.52.248.204	Leaf-101
00:50:56:99:EF:B3	Leaf-101
10.52.248.202	Leaf-101
00:00:0C:07:AC:1D	Leaf-101
00:18:74:E2:...	Leaf-101



L1 VTEP **VXLAN** **IP** **Payload**

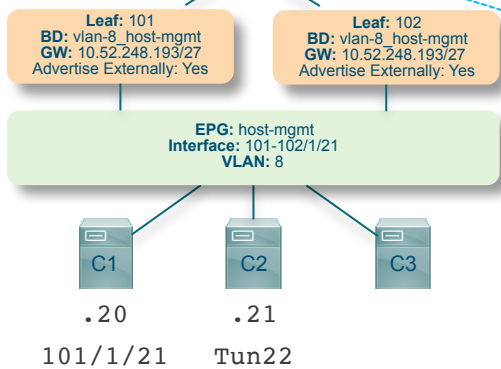
2 Leaf swaps ingress encapsulation with VXLAN ID and performs any required policy functions

IP **Payload**

1 Packet Sourced from physical server

Leaf 101

*	Proxy B	
	Tunnel22	Global
	(Leaf-102)	
0050.3680.2574	Tunnel22	Global
	(Leaf-102)	
0025.b5dc.034e	Tunnel22	Local
	(Leaf-102)	
10.52.248.21		
0025.b5dc.040f	1/21	
10.52.248.20	1/21	



Leaf 102

*	Proxy B	
	Tunnel06	Global
	(Leaf-103)	
0050.2980.2574	Tunnel115	Global
	(Leaf-101)	
0025.b5dc.040f	Tunnel115	Local
	(Leaf-101)	
10.52.248.20		
0025.b5dc.034e	1/21	
10.52.248.21	1/21	

Packet Walk

Spine Proxy Table

0025.b5dc.034e	Leaf-102
10.52.248.21	Leaf-102
0025.b5dc.040f	Leaf-101
10.52.248.20	Leaf-101
10.52.248.204	Leaf-101
00:50:56:99:EF:B3	Leaf-101
10.52.248.202	Leaf-101
00:00:0C:07:AC:1D	Leaf-101
00:18:74:E2:...	Leaf-101

L6 VTEP VXLAN IP Payload

3a If the ingress Leaf has learned the destination IP to egress VTEP binding it will set required destination VTEP address and forward

L1 VTEP VXLAN IP Payload

2 Leaf swaps ingress encapsulation with VXLAN ID and performs any required policy functions

IP Payload

1 Packet Sourced from physical server

Leaf 101

*	Proxy B	
	Tunnel22 (Leaf-102)	Global
0050.2986.2574	Tunnel22 (Leaf-102)	Global
0025.b5dc.034e	Tunnel22 (Leaf-102)	Global
10.52.248.21	Tunnel22 (Leaf-102)	Local
0025.b5dc.040f	1/21	Local
10.52.248.20	1/21	Local

Leaf: 101
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

Leaf: 102
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

EPG: host-mgmt
Interface: 101-102/1/21
VLAN: 8



.20 .21
101/1/21 Tun22

S1 VTEP VXLAN IP Payload

3b If the ingress Leaf has NOT learned the destination IP to egress VTEP binding it will set required destination VTEP to the Spine Proxy VTEP

Leaf 102

*	Proxy B	
	Tunnel106 (Leaf-102)	Global
0050.2986.2574	Tunnel115 (Leaf-101)	Global
0025.b5dc.040f	Tunnel115 (Leaf-101)	Global
10.52.248.20	Tunnel115 (Leaf-101)	Local
0025.b5dc.034e	1/21	Local
10.52.248.21	1/21	Local

Packet Walk

Spine Proxy Table

0025.b5dc.034e	Leaf-102
10.52.248.21	Leaf-102
0025.b5dc.040f	Leaf-101
10.52.248.20	Leaf-101
10.52.248.204	Leaf-101
00:50:56:99:EF:B3	Leaf-101
10.52.248.202	Leaf-101
00:00:0C:07:AC:1D	Leaf-101
00:18:74:E2:...	Leaf-101

L6 VTEP **VXLAN** **IP** **Payload**

3a If the ingress Leaf has learned the destination IP to egress VTEP binding it will set required destination VTEP address and forward

L1 VTEP **VXLAN** **IP** **Payload**

2 Leaf swaps ingress encapsulation with VXLAN ID and performs any required policy functions

IP **Payload**

1 Packet Sourced from physical server

Leaf 101

*	Proxy B	
	Tunnel22 (Leaf-102)	Global
0050.2986.2574	Tunnel22 (Leaf-102)	Global
0025.b5dc.034e	Tunnel22 (Leaf-102)	Local
10.52.248.21	Tunnel22 (Leaf-102)	Local
0025.b5dc.040f	1/21	
10.52.248.20	1/21	

Leaf: 101
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

Leaf: 102
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

EPG: host-mgmt
Interface: 101-102/1/21
VLAN: 8

C1

C2

C3

.20

.21

101/1/21

Tun22

S1 VTEP **VXLAN** **IP** **Payload**

3b If the ingress Leaf has NOT learned the destination IP to egress VTEP binding it will set required destination VTEP to the Spine Proxy VTEP

L6 VTEP **VXLAN** **IP** **Payload**

4 Leaf removes ingress VXLAN (EPG) ID and performs any required policy functions

Leaf 102

*	Proxy B	
	Tunnel106 (Leaf-102)	Global
0050.2986.2574	Tunnel115 (Leaf-101)	Global
0025.b5dc.040f	Tunnel115 (Leaf-101)	Local
10.52.248.20	Tunnel115 (Leaf-101)	Local
0025.b5dc.034e	1/21	
10.52.248.21	1/21	

Packet Walk

Spine Proxy Table

0025.b5dc.034e	Leaf-102
10.52.248.21	Leaf-102
0025.b5dc.040f	Leaf-101
10.52.248.20	Leaf-101
10.52.248.204	Leaf-101
00:50:56:99:EF:B3	Leaf-101
10.52.248.202	Leaf-101
00:00:0C:07:AC:1D	Leaf-101
00:18:74:E2:...	Leaf-101

L6 VTEP **VXLAN** **IP** **Payload**

3a If the ingress Leaf has learned the destination IP to egress VTEP binding it will set required destination VTEP address and forward

L1 VTEP **VXLAN** **IP** **Payload**

2 Leaf swaps ingress encapsulation with VXLAN (EPG) ID and performs any required policy functions

IP **Payload**

1 Packet Sourced from physical server

Leaf 101

*	Proxy B	
0050.2986.2574	Tunnel22 (Leaf-102)	Global
0025.b5dc.034e	Tunnel22 (Leaf-102)	
10.52.248.21	Tunnel22 (Leaf-102)	Local
0025.b5dc.040f	1/21	
10.52.248.20	1/21	

Leaf: 101
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

Leaf: 102
BD: vlan-8 host-mgmt
GW: 10.52.248.193/27
Advertise Externally: Yes

EPG: host-mgmt
Interface: 101-102/1/21
VLAN: 8



.20



.21



101/1/21 Tun22

S1 VTEP **VXLAN** **IP** **Payload**

3b If the ingress Leaf has NOT learned the destination IP to egress VTEP binding it will set required destination VTEP to the Spine Proxy VTEP

L6 VTEP **VXLAN** **IP** **Payload**

4 Leaf removes ingress VXLAN (EPG) ID and performs any required policy functions

IP **Payload**

5 Packet Delivered to physical server

Leaf 102

*	Proxy B	
0050.2986.2574	Tunnel106 (Leaf-102)	Global
0025.b5dc.040f	Tunnel115 (Leaf-101)	
10.52.248.20	Tunnel115 (Leaf-101)	Local
0025.b5dc.034e	1/21	
10.52.248.21	1/21	

The EPG shows the switches where the Mac/IP addresses are learned

The screenshot shows the Cisco APIC interface. The left sidebar displays the navigation tree under 'Tenant common', with 'Application EPGs' expanded and 'vlan-8_host-mgmt' selected. The main content area shows the 'EPG - vlan-8_host-mgmt' page with the 'Operational' tab active. A table lists 15 entries for this EPG, showing details like End Point, MAC, IP, Learning Source, Hosting Server, Reporting Controller Name, Interface, Multicast Address, and Encap. The table indicates that all entries are 'learned' and associated with 'vlan-8'.

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
EP-00:00:...	00:00:0C:07:AC:08	10.52.248.1, 10.52.248.74	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:04:...	00:04:02:F6:1F:13	10.52.248.60	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:14:...	00:14:38:4E:26:E1	10.52.248.12	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:16:...	00:16:35:5B:DD:DA	10.52.248.13	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:18:...	00:18:74:E2:15:40	10.52.248.2	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:1A:...	00:1A:A2:D5:C0:80	10.52.248.3	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:25:...	00:25:B5:01:04:BF	10.52.248.5	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:25:...	00:25:B5:01:04:DF	10.52.248.4	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:25:...	00:25:B5:DC:02:4E	---	learned	---	---	Pod-1/Node-101-eth1/22 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:02:7E	10.52.248.23	learned	---	---	Pod-1/Node-101-eth1/22 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:03:3E	10.52.248.22	learned	---	---	Pod-1/Node-103-eth1/22 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:03:4E	10.52.248.21	learned	---	---	Pod-1/Node-102-eth1/21 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:04:0F	10.52.248.20	learned	---	---	Pod-1/Node-101-eth1/21 ...	---	vlan-8
EP-00:26:...	00:26:0B:F1:F0:02	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:60:...	00:60:16:46:97:DA	10.52.248.59	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8

The EPG shows the switches where the Mac/IP addresses are learned

The screenshot shows the Cisco APIC interface for the 'Tenant common' configuration. The 'EPG - vlan-8_host-mgmt' is selected in the left-hand navigation pane. The 'Operational' tab is active, displaying a table of 'Client End-Points'. The table columns are: End Point, MAC, IP, Learning Source, Hosting Server, Reporting Controller Name, Interface, Multicast Address, and Encap. The table lists 15 entries. The last two entries are highlighted with a red box.

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
EP-00:00:...	00:00:0C:07:AC:08	10.52.248.1, 10.52.248.74	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:04:...	00:04:02:F6:1F:13	10.52.248.60	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:14:...	00:14:38:4E:26:E1	10.52.248.12	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:16:...	00:16:35:5B:DD:DA	10.52.248.13	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:18:...	00:18:74:E2:15:40	10.52.248.2	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:1A:...	00:1A:A2:D5:C0:80	10.52.248.3	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:25:...	00:25:B5:01:04:BF	10.52.248.5	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:25:...	00:25:B5:01:04:DF	10.52.248.4	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:25:...	00:25:B5:DC:02:4E	---	learned	---	---	Pod-1/Node-101-eth1/22 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:02:7E	10.52.248.23	learned	---	---	Pod-1/Node-101-eth1/22 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:03:3E	10.52.248.22	learned	---	---	Pod-1/Node-103-eth1/22 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:03:4E	10.52.248.21	learned	---	---	Pod-1/Node-102-eth1/21 ...	---	vlan-8
EP-00:25:...	00:25:B5:DC:04:0F	10.52.248.20	learned	---	---	Pod-1/Node-101-eth1/21 ...	---	vlan-8
EP-00:26:...	00:26:0B:F1:F0:02	---	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8
EP-00:60:...	00:60:16:46:97:DA	10.52.248.59	learned	---	---	Pod-1/Node-101-102/1G...	---	vlan-8

The EPG shows the switches where the Mac/IP addresses are learned

```
apic1# show endpoints vlan 8
```

Legends:

(P):Primary VLAN

(S):Secondary VLAN

Dynamic Endpoints:

Tenant : common

Application : outside_vlans

AEpg : vlan-8_host-mgmt

End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:25:B5:DC:04:0F	10.52.248.20	101	eth1/21	vlan-8	not-applicable
00:25:B5:DC:03:4E	10.52.248.21	102	eth1/21	vlan-8	not-applicable

The EPG shows the switches where the Mac/IP addresses are learned

```
apic1# show endpoints vlan 8
```

Legends:

(P):Primary VLAN

(S):Secondary VLAN

Dynamic Endpoints:

Tenant : common

Application : outside_vlans

AEPg : vlan-8_host-mgmt

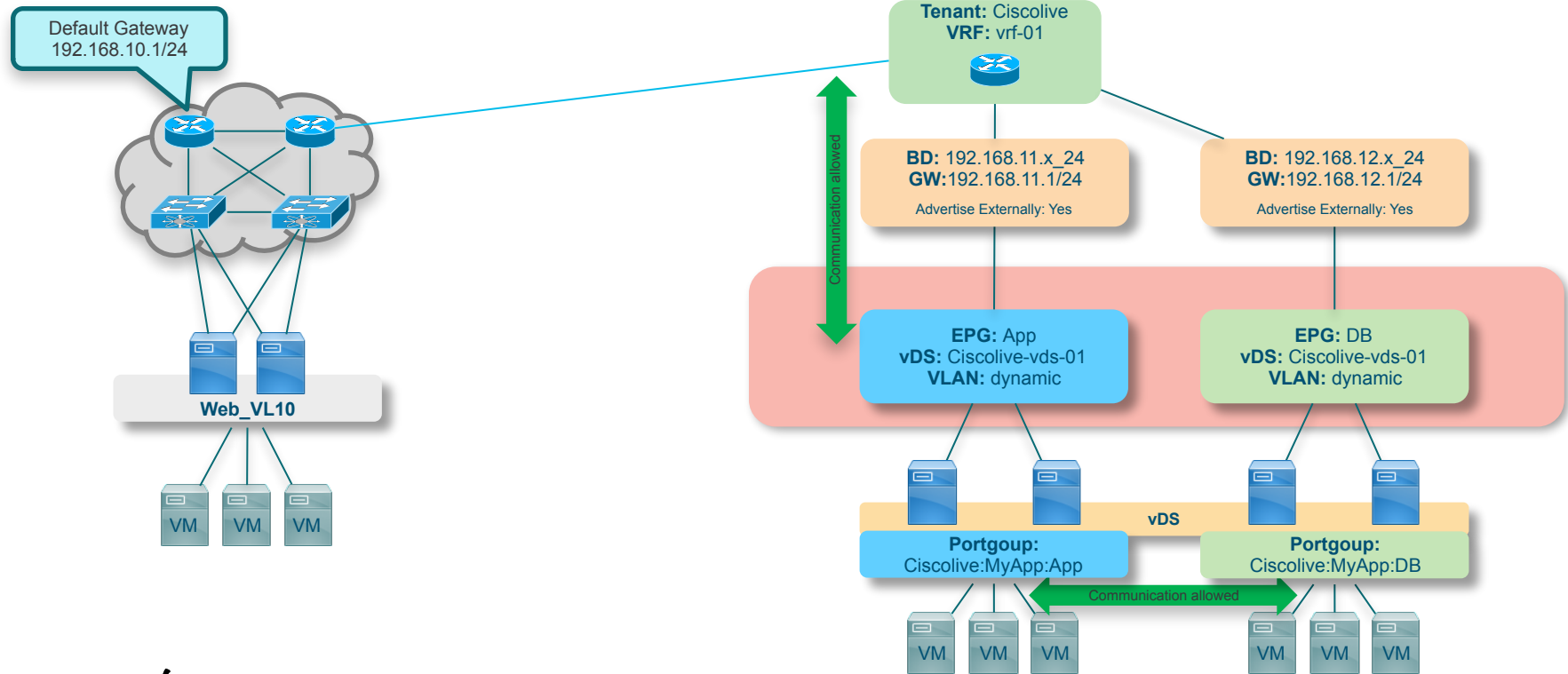
End Point MAC	IP Address	Node	Interface	Encap	Multicast Add
00:25:B5:DC:04:0F	10.52.248.20	101	eth1/21	vlan-8	not-applicable
00:25:B5:DC:03:4E	10.52.248.21	102	eth1/21	vlan-8	not-applicable

External Connectivity

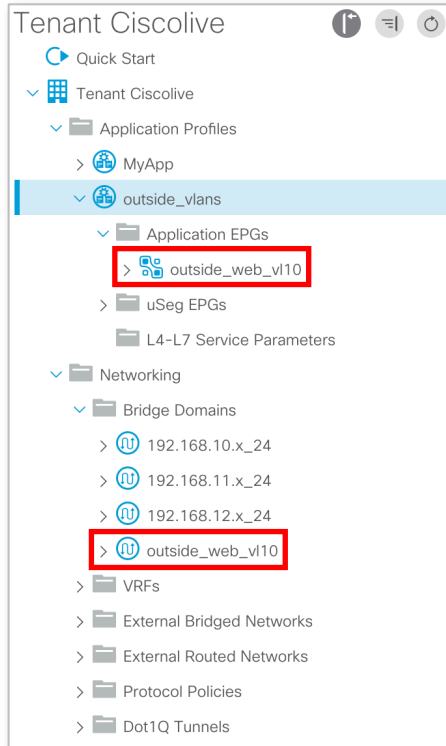
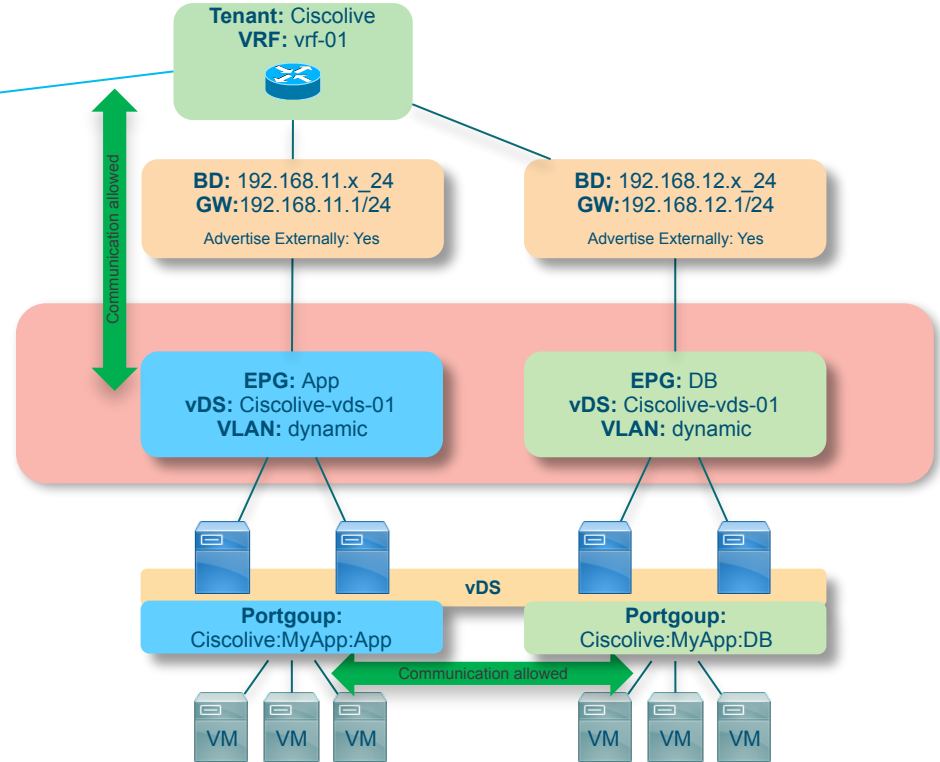
Layer 2 connectivity

1 Bridge Domain = 1 Outside VLAN

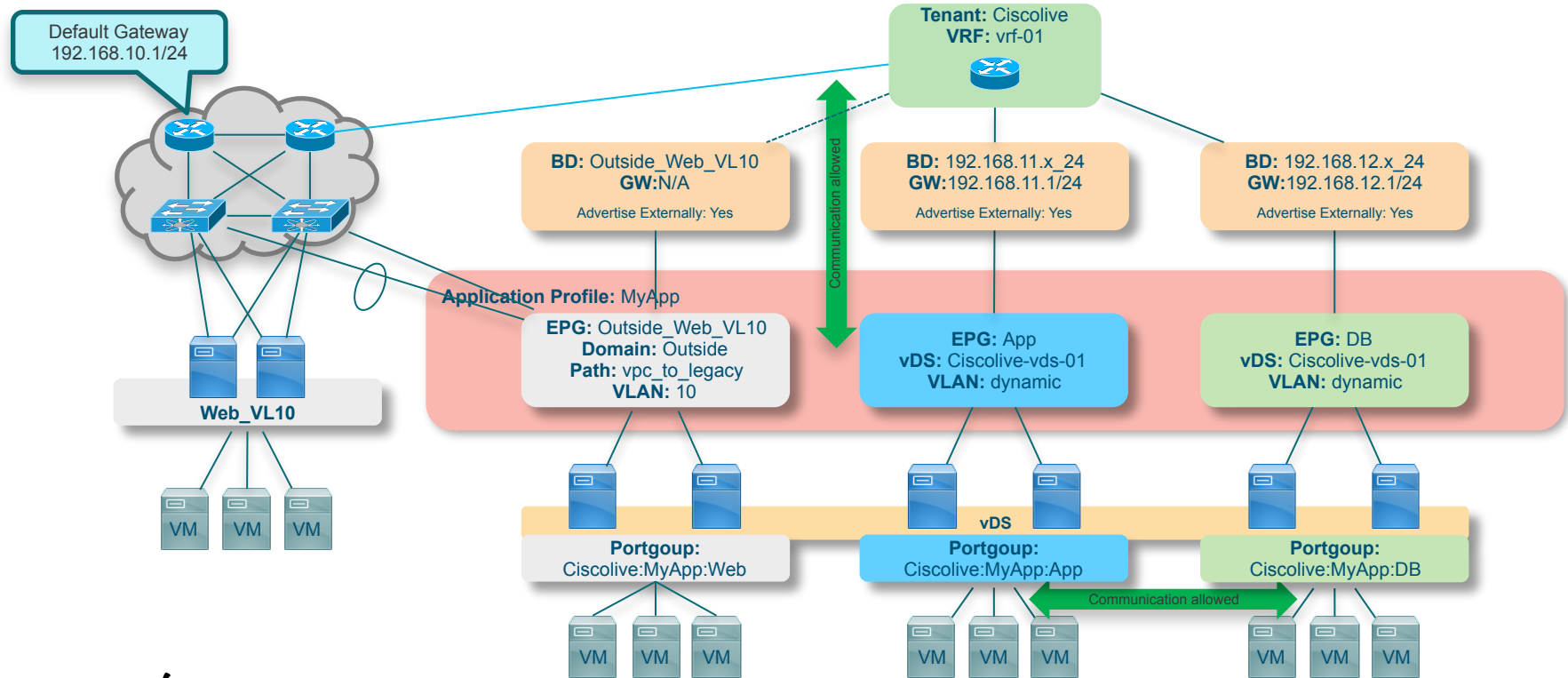
External Layer 2 – Extended EPG



External Layer 2 – Extended EPG



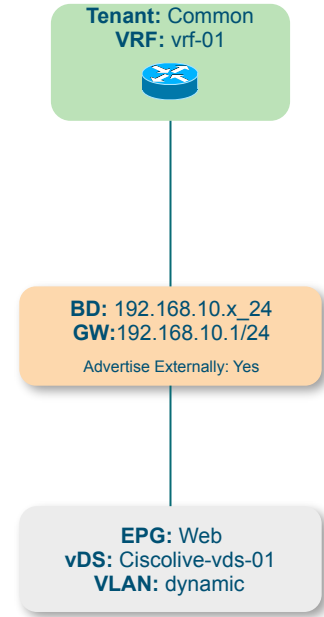
External Layer 2 – Extended EPG



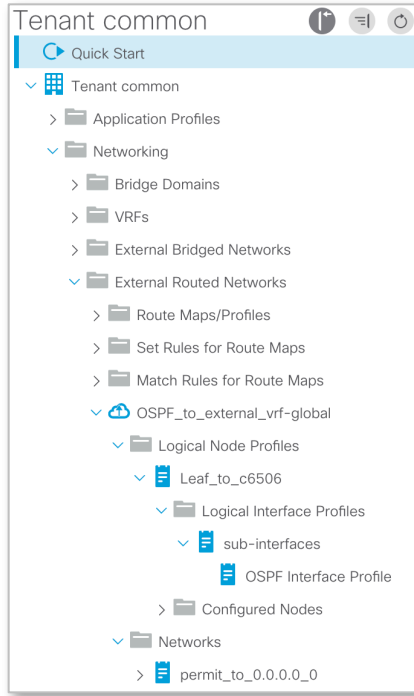
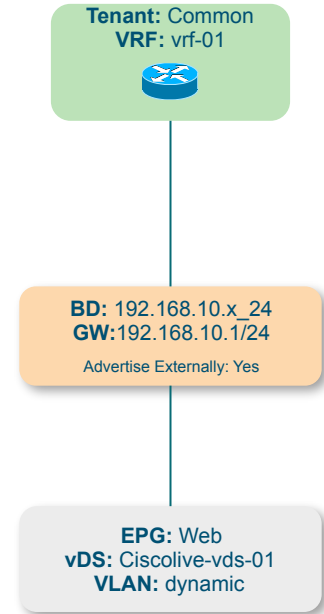
Layer 3 connectivity

L3out's are simply routed interfaces/sub interfaces/SVIs

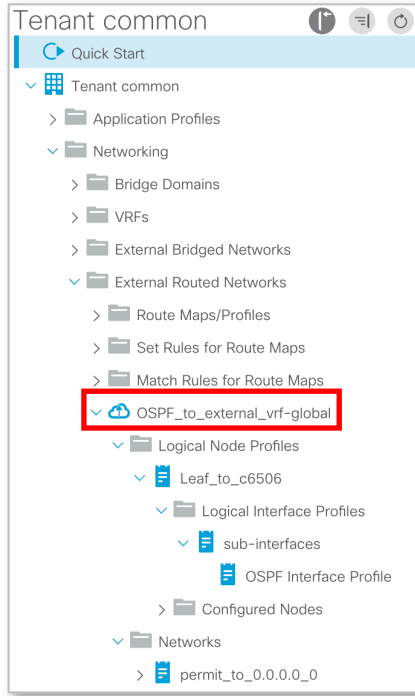
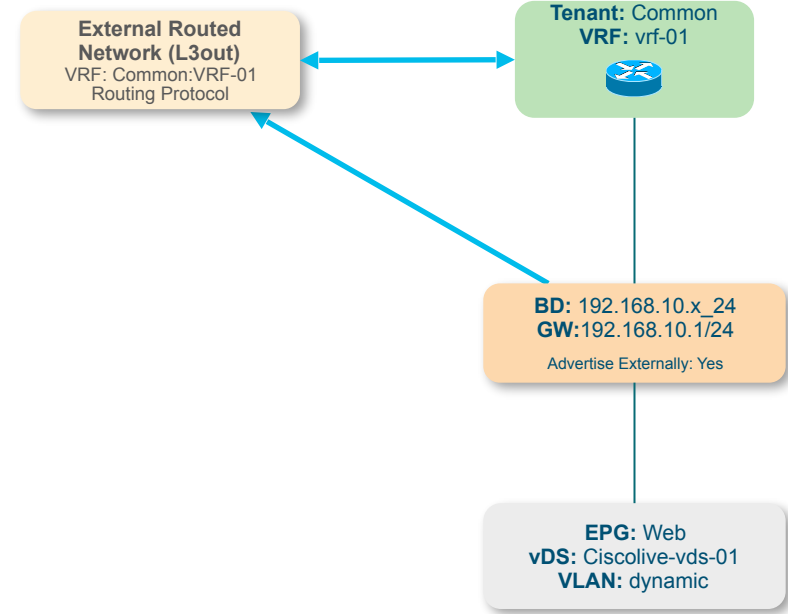
Anatomy of a L3out



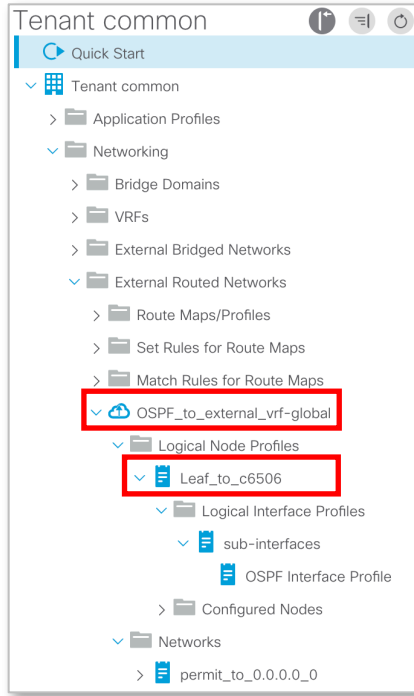
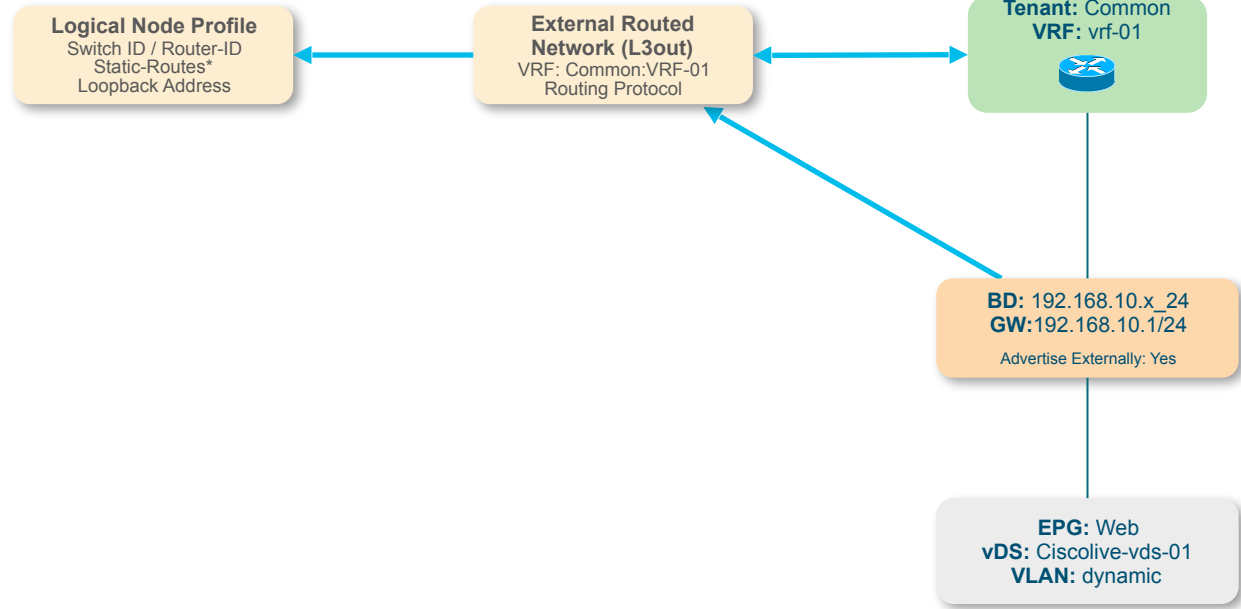
Anatomy of a L3out



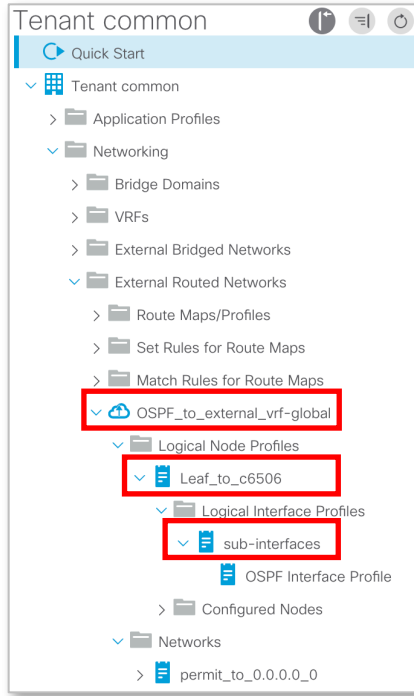
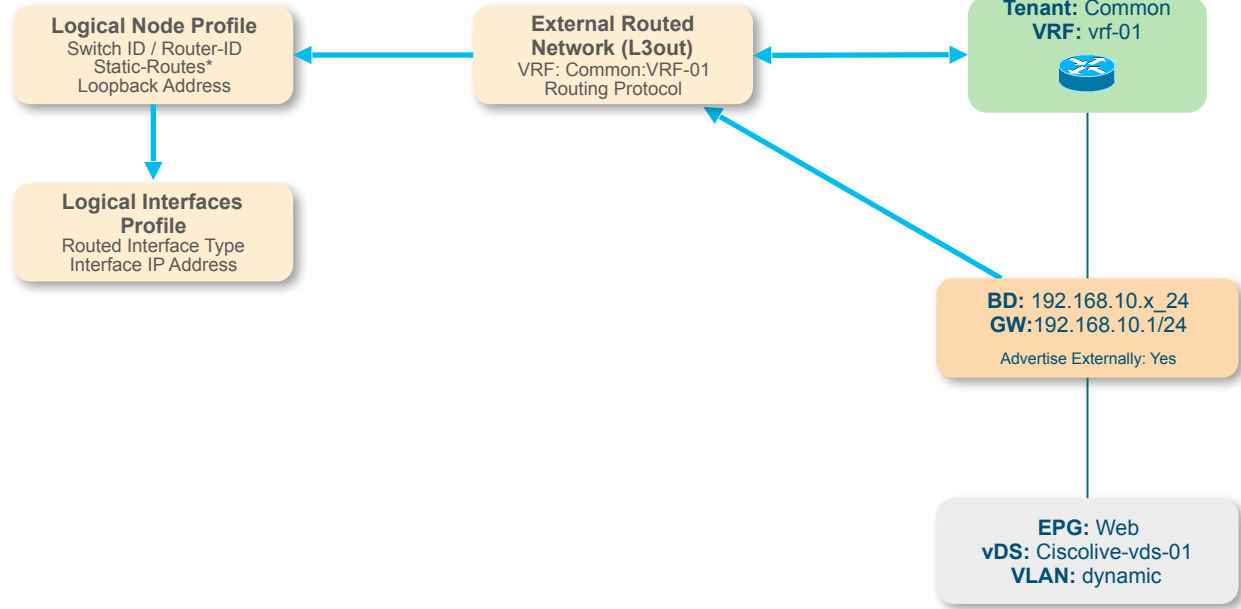
Anatomy of a L3out



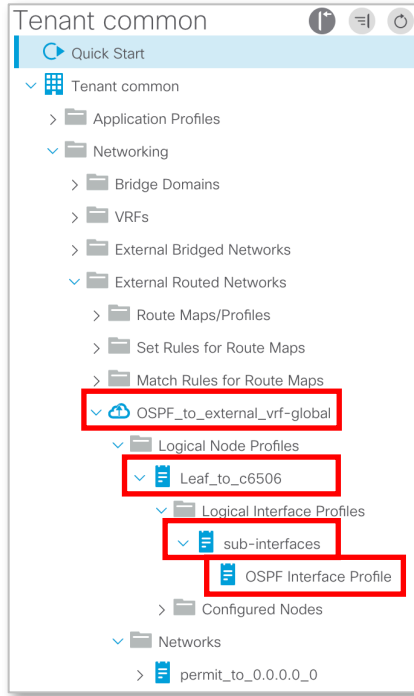
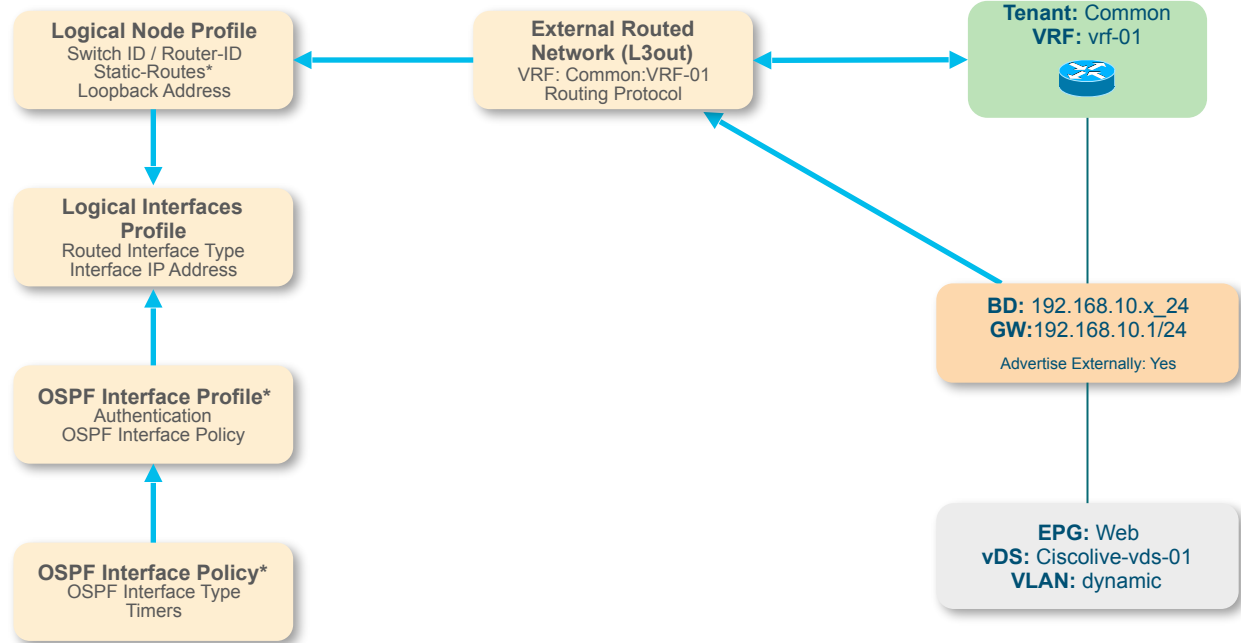
Anatomy of a L3out



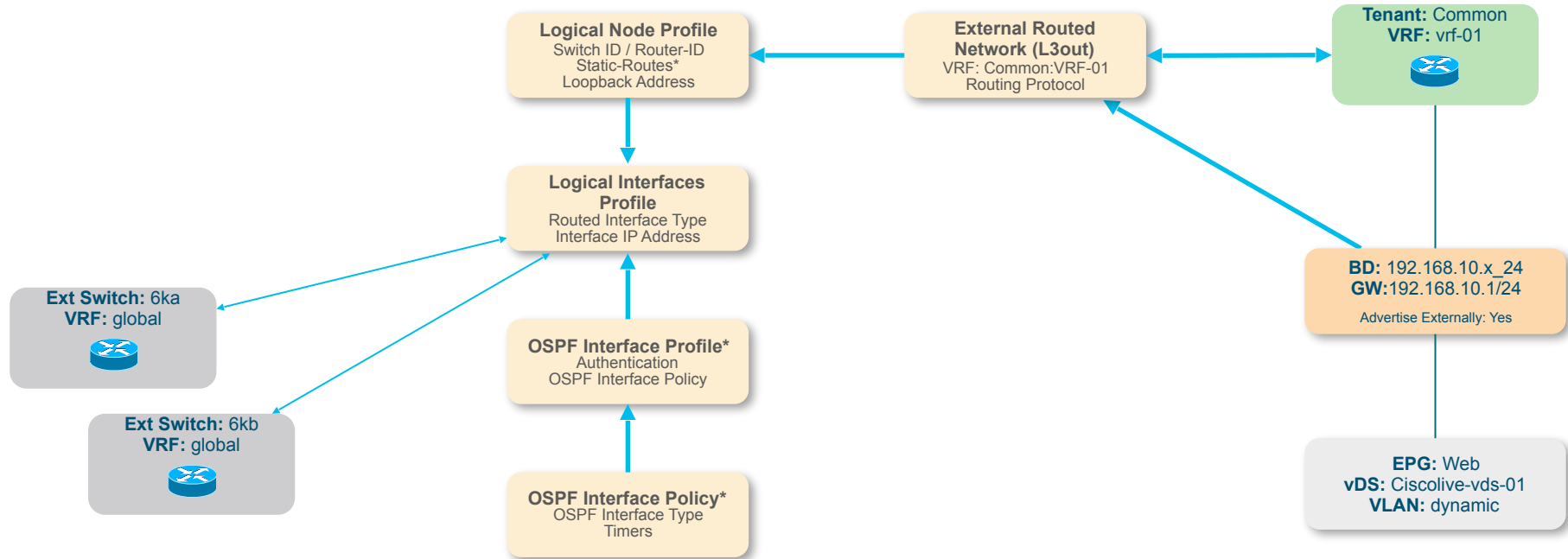
Anatomy of a L3out



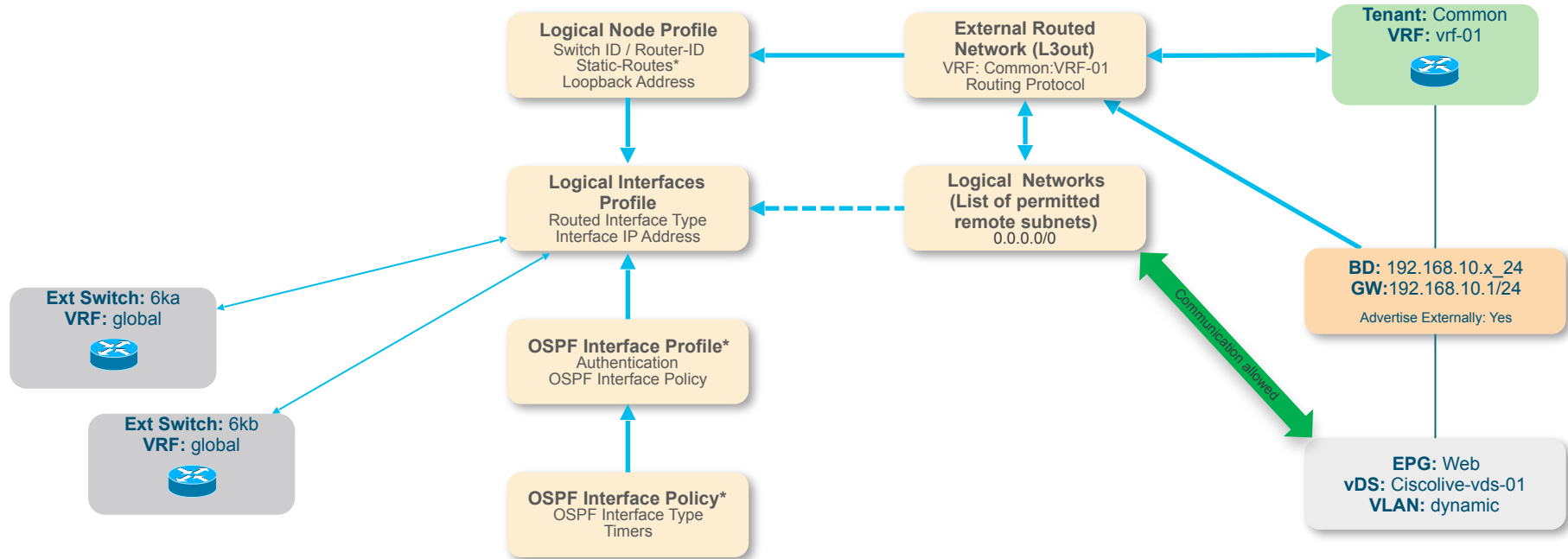
Anatomy of a L3out



Anatomy of a L3out



Anatomy of a L3out



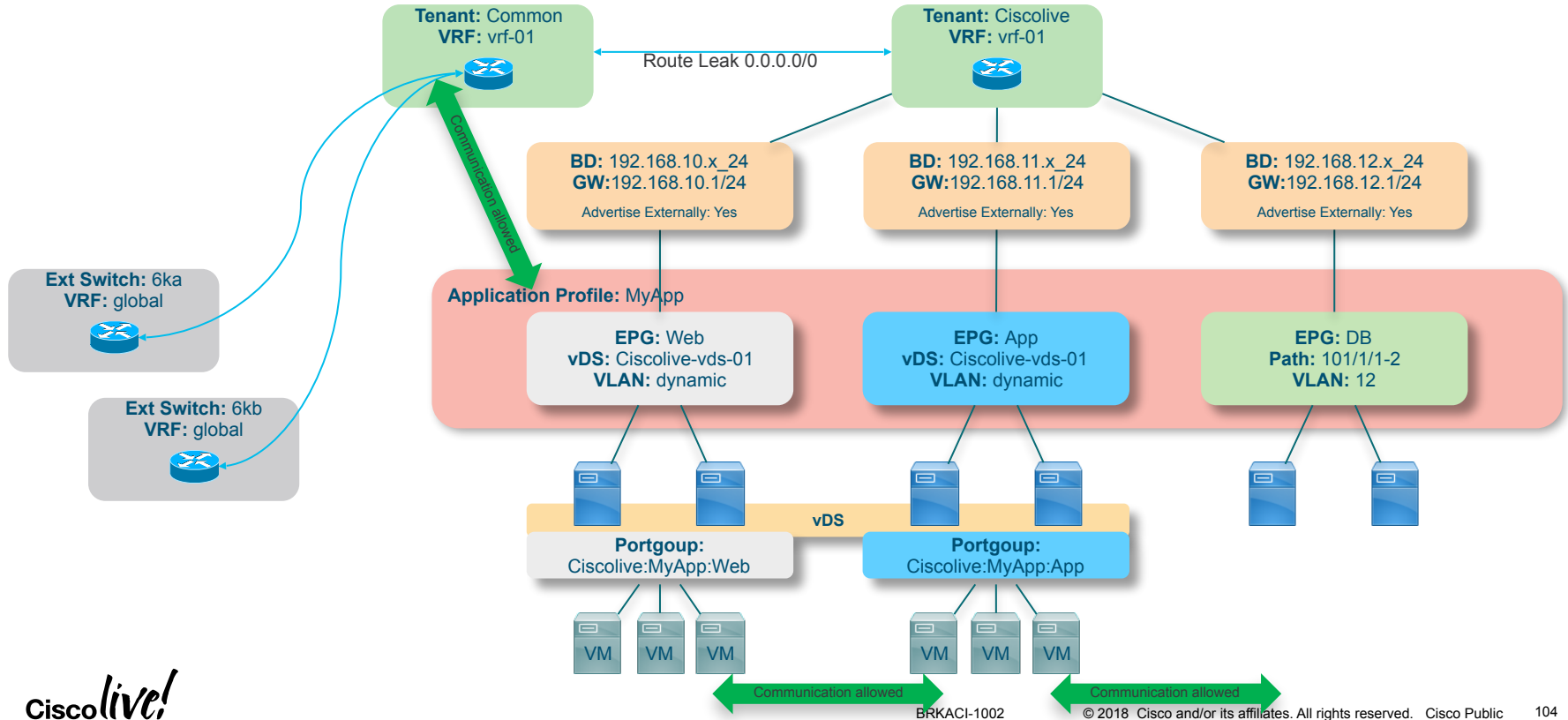
Cisco *live!*



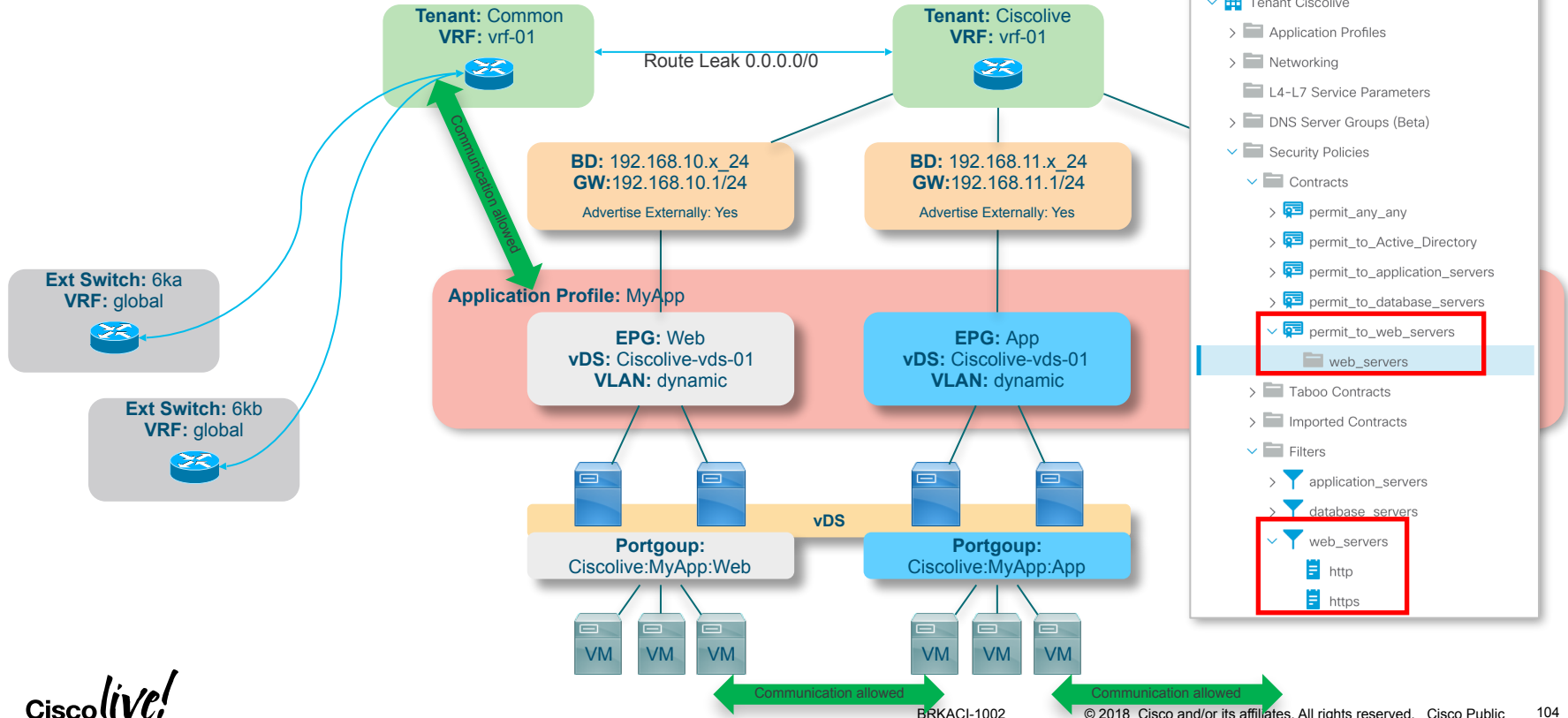
103

scale figures based on Gen2 hardware

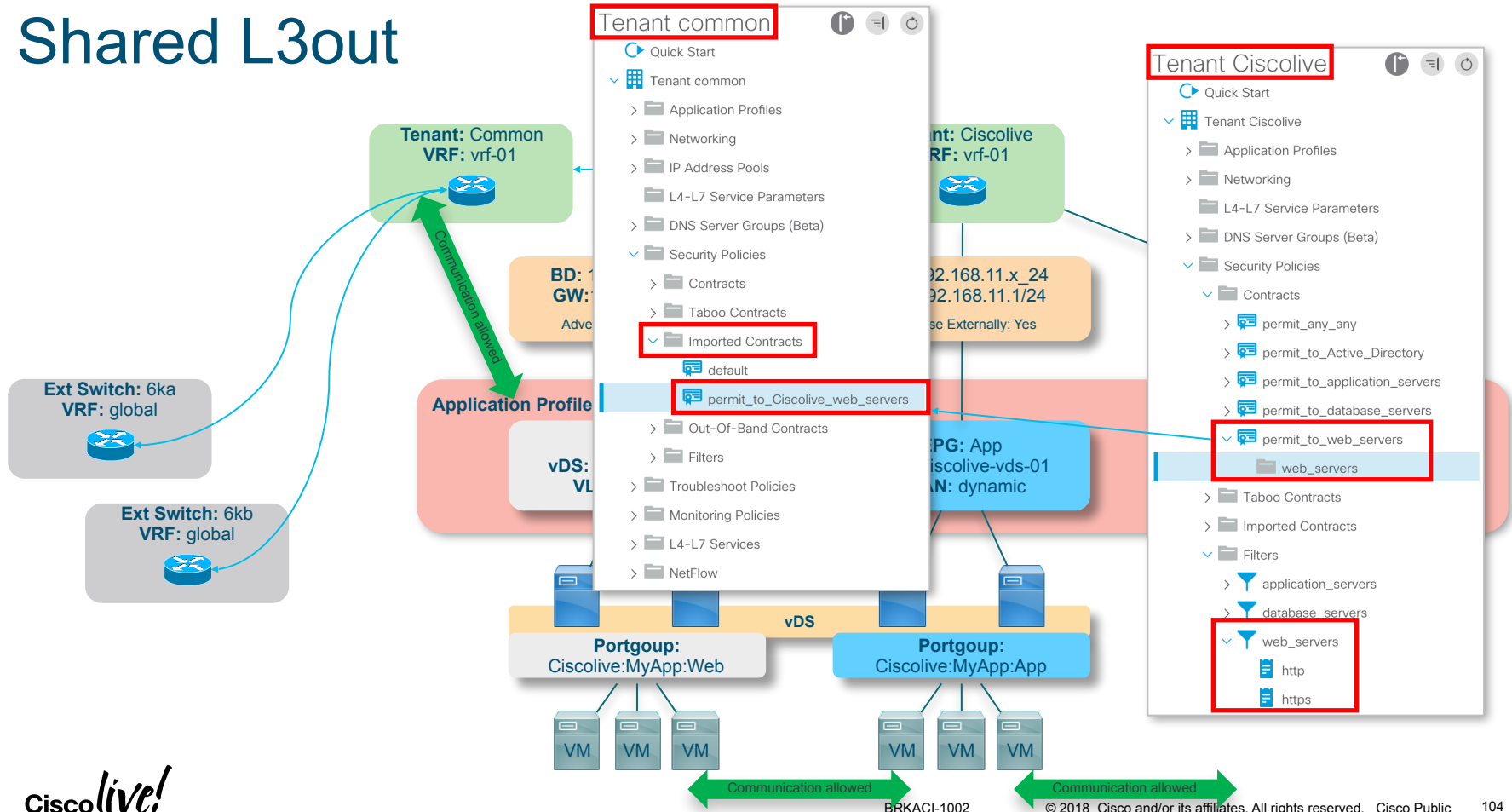
Shared L3out



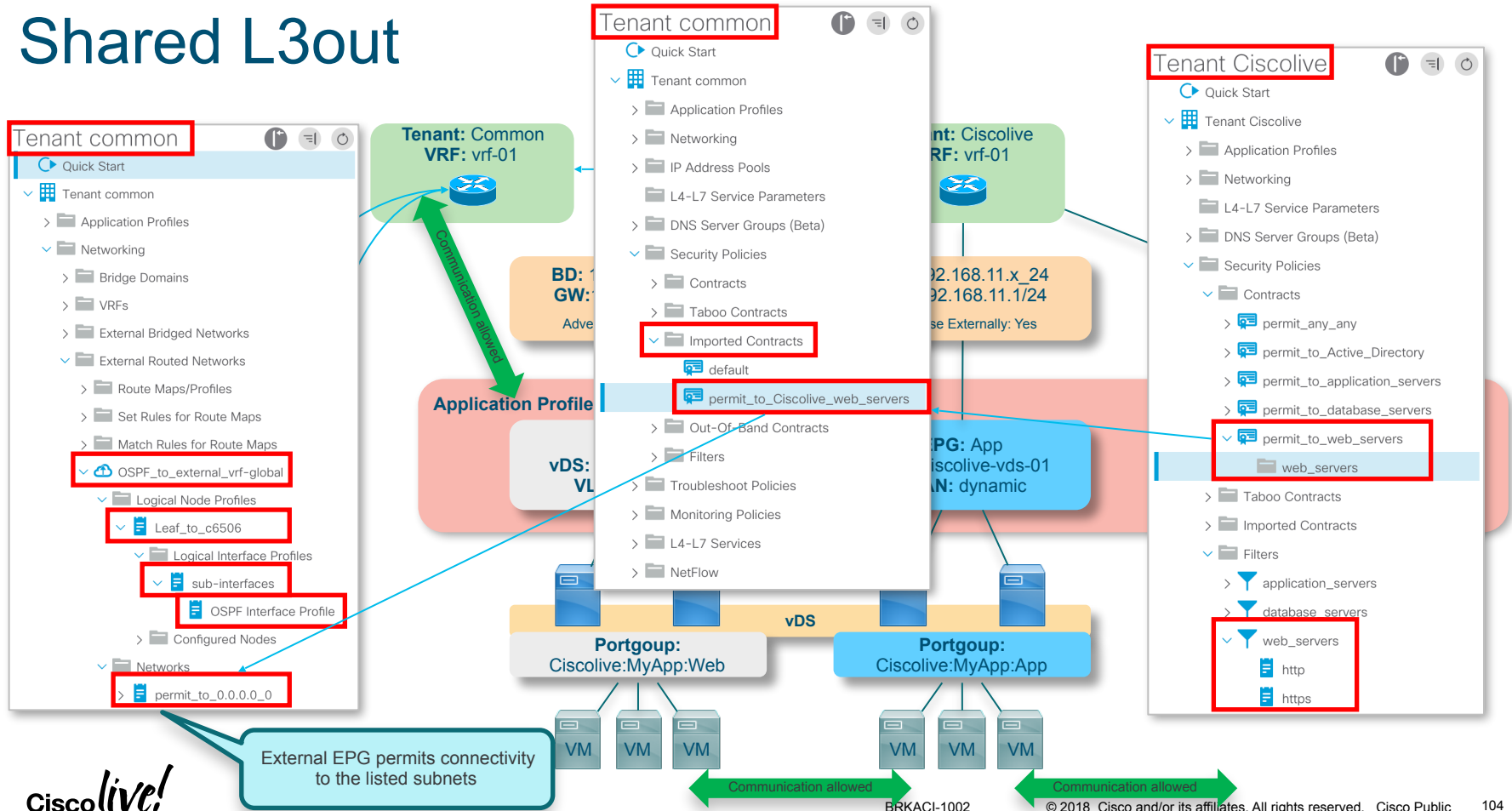
Shared L3out



Shared L3out



Shared L3out



L3out in the Common Tenant

```
apic1# fabric 101-102 show ip interface brief vrf common:vrf-01
-----
Node 101 (Leaf-101)
-----
IP Interface Status for VRF "common:vrf-01"(4)
Interface      Address          Interface Status
eth1/96.9      101.0.100.2/30  protocol-up/link-up/admin-up
vlan12         192.168.110.1/24 protocol-up/link-up/admin-up
vlan54         10.52.248.193/27 protocol-up/link-up/admin-up
lo2            101.1.1.1/32    protocol-up/link-up/admin-up

-----
Node 102 (Leaf-102)
-----
IP Interface Status for VRF "common:vrf-01"(4)
Interface      Address          Interface Status
eth1/96.5      102.0.100.2/30  protocol-up/link-up/admin-up
vlan9          192.168.110.1/24 protocol-up/link-up/admin-up
vlan53         10.52.248.193/27 protocol-up/link-up/admin-up
lo2            102.1.1.1/32    protocol-up/link-up/admin-up

apic1#
```

L3out in the Common Tenant

```
apic1# fabric 101-102 show ip interface brief vrf common:vrf-01
```

```
-----  
Node 101 (Leaf-101)  
-----
```

```
IP Interface Status for VRF "common:vrf-01"(4)
```

Interface	Address	Interface Status
eth1/96.9	101.0.100.2/30	protocol-up/link-up/admin-up
vlan12	192.168.110.1/24	protocol-up/link-up/admin-up
vlan54	10.52.248.193/27	protocol-up/link-up/admin-up
lo2	101.1.1.1/32	protocol-up/link-up/admin-up

Routed sub interface

```
-----  
Node 102 (Leaf-102)  
-----
```

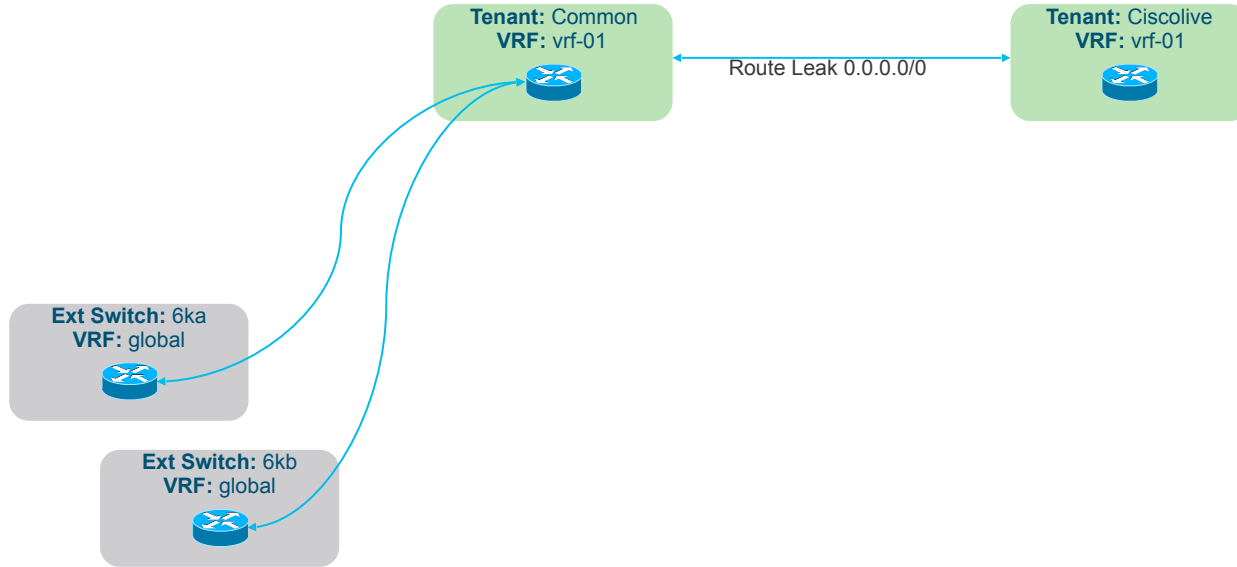
```
IP Interface Status for VRF "common:vrf-01"(4)
```

Interface	Address	Interface Status
eth1/96.5	102.0.100.2/30	protocol-up/link-up/admin-up
vlan9	192.168.110.1/24	protocol-up/link-up/admin-up
vlan53	10.52.248.193/27	protocol-up/link-up/admin-up
lo2	102.1.1.1/32	protocol-up/link-up/admin-up

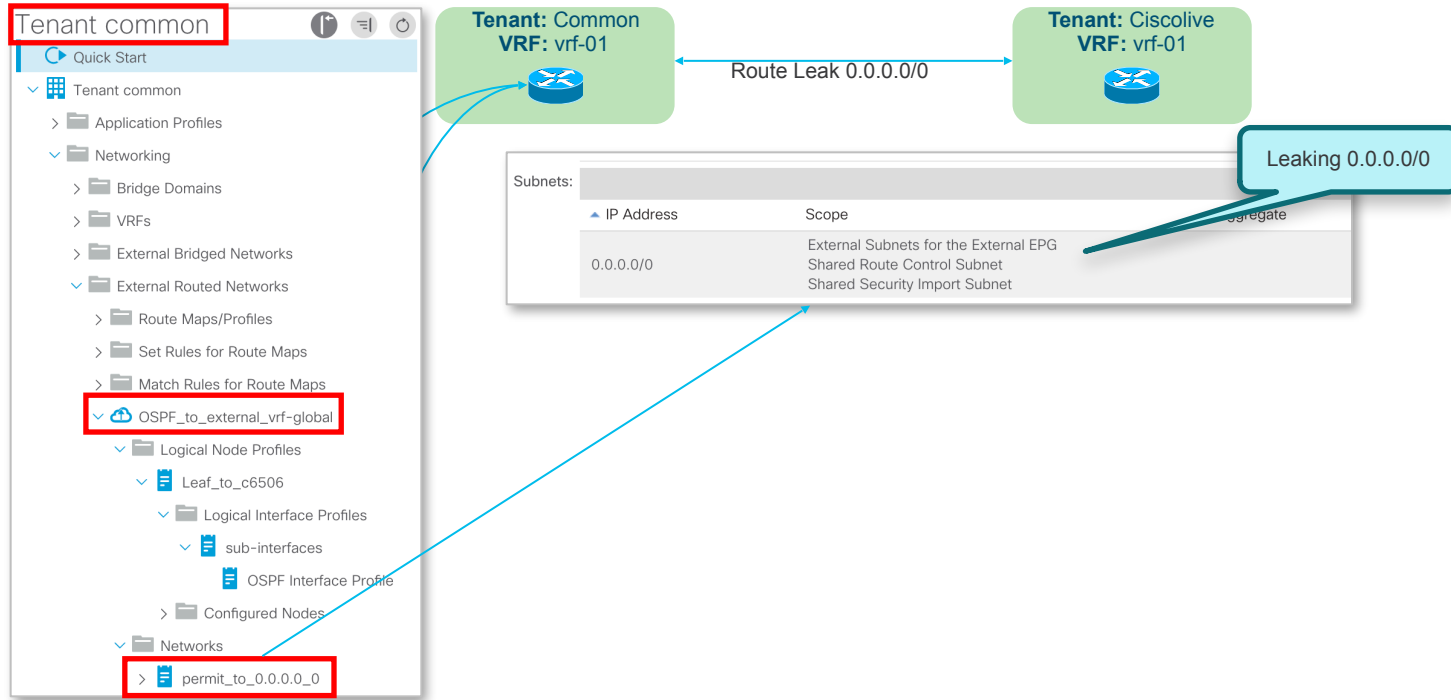
Routed sub interface

```
apic1#
```

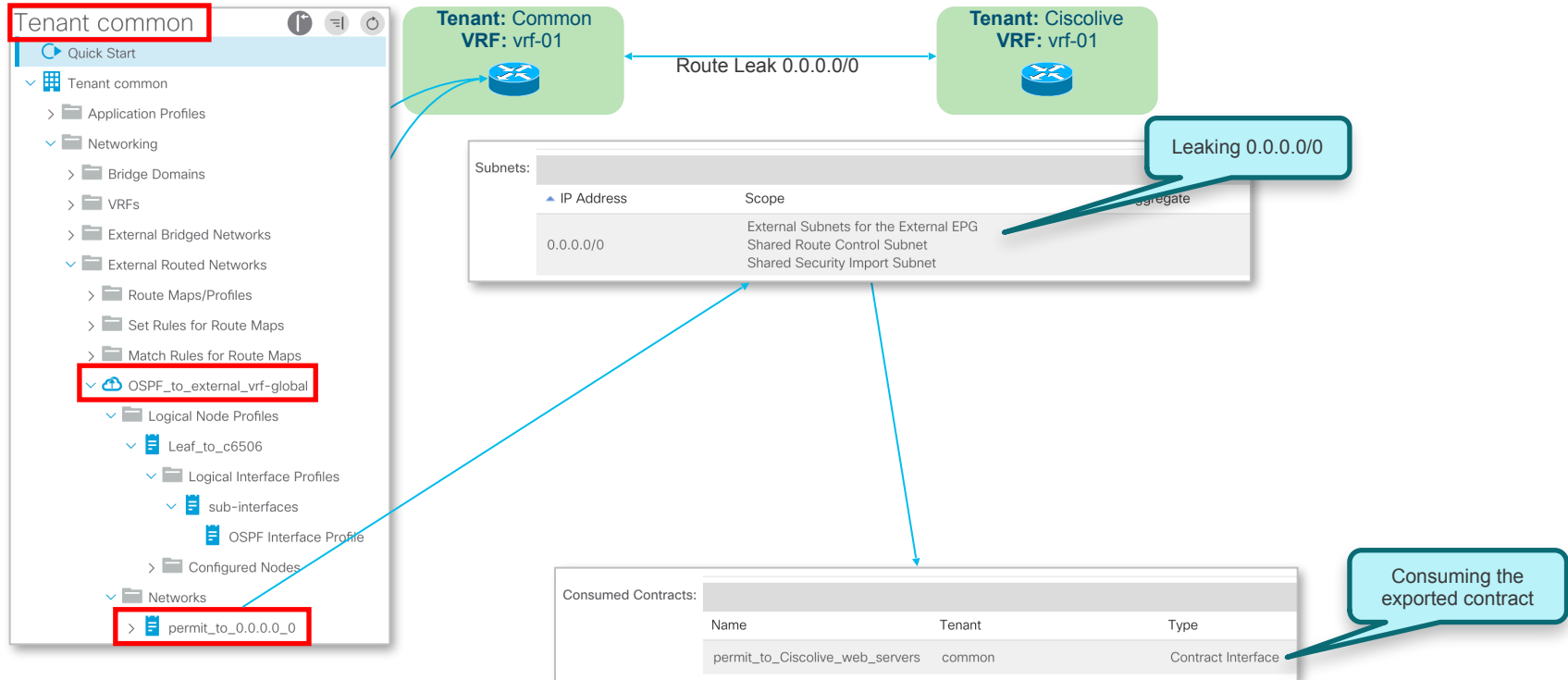
Common Tenant Configuration



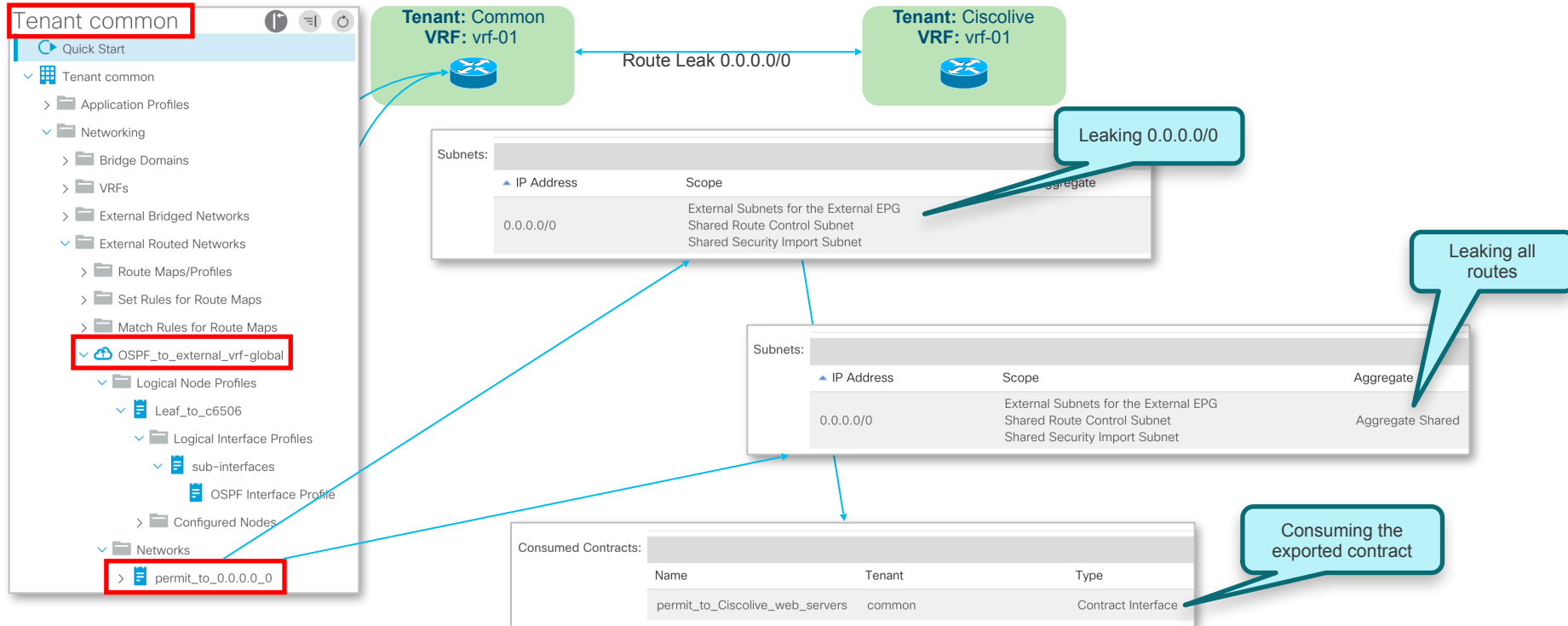
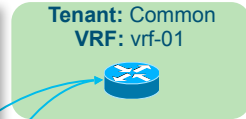
Common Tenant Configuration



Common Tenant Configuration



Common Tenant Configuration



Route Leak 0.0.0.0/0

Subnets:

IP Address	Scope
0.0.0.0/0	External Subnets for the External EPG Shared Route Control Subnet Shared Security Import Subnet

Leaking 0.0.0.0/0

Subnets:

IP Address	Scope	Aggregate
0.0.0.0/0	External Subnets for the External EPG Shared Route Control Subnet Shared Security Import Subnet	Aggregate Shared

Leaking all routes

Consumed Contracts:

Name	Tenant	Type
permit_to_CiscoLive_web_servers	common	Contract Interface

Consuming the exported contract

Default Route in Common Tenant

```
apic1# fabric 101-102 show ip route 0.0.0.0 vrf common:vrf-01
-----
Node 101 (Leaf-101)
-----
IP Route Table for VRF "common:vrf-01"
'*' 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 101.0.100.1, eth1/96.9, [110/1], 5d17h, ospf-default, type-2, tag 1

-----
Node 102 (Leaf-102)
-----
IP Route Table for VRF "common:vrf-01"
'*' 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 102.0.100.1, eth1/96.5, [110/1], 5d17h, ospf-default, type-2, tag 1

apic1#
```

Default Route in Common Tenant

```
apic1# fabric 101-102 show ip route 0.0.0.0 vrf common:vrf-01
```

```
-----  
Node 101 (Leaf-101)  
-----
```

```
IP Route Table for VRF "common:vrf-01"  
'*' 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 101.0.100.1, eth1/96.9, [110/1], 5d17h, ospf-default, type-2, tag 1
```

```
-----  
Node 102 (Leaf-102)  
-----
```

```
IP Route Table for VRF "common:vrf-01"  
'*' 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 102.0.100.1, eth1/96.9, [110/1], 3d17h, ospf-default, type-2, tag 1
```

```
apic1#
```

Default Route in Ciscolive Tenant

```
apic1# fabric 101-102 show ip route 0.0.0.0 vrf Ciscolive:vrf-01
-----
Node 101 (Leaf-101)
-----
IP Route Table for VRF "Ciscolive:vrf-01"
'*' 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 101.0.100.1%common:vrf-01, eth1/96.9, [20/1], 00:16:31, bgp-64512, external, tag 64512

-----
Node 102 (Leaf-102)
-----
IP Route Table for VRF "Ciscolive:vrf-01"
'*' 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 102.0.100.1%common:vrf-01, eth1/96.5, [20/1], 00:16:33, bgp-64512, external, tag 64512

apic1#
```

Default Route in CiscoLive Tenant

```
apic1# fabric 101-102 show ip route 0.0.0.0 vrf Ciscolive:vrf-01
```

```
-----  
Node 101 (Leaf-101)  
-----
```

```
IP Route Table for VRF "Ciscolive:vrf-01"
```

```
'*' 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 101.0.100.1%common:vrf-01, eth1/96.9, [20/1], 00:16:31, bgp-64512, external, tag 64512
```

```
-----  
Node 102 (Leaf-102)  
-----
```

```
IP Route Table for VRF "Ciscolive:vrf-01"
```

```
'*' denotes best ucast next-hop
```

```
'**' denotes best mcast next-hop
```

```
'[x/y]' denotes [preference/metric]
```

```
'%<string>' in via output denotes VRF<string>
```

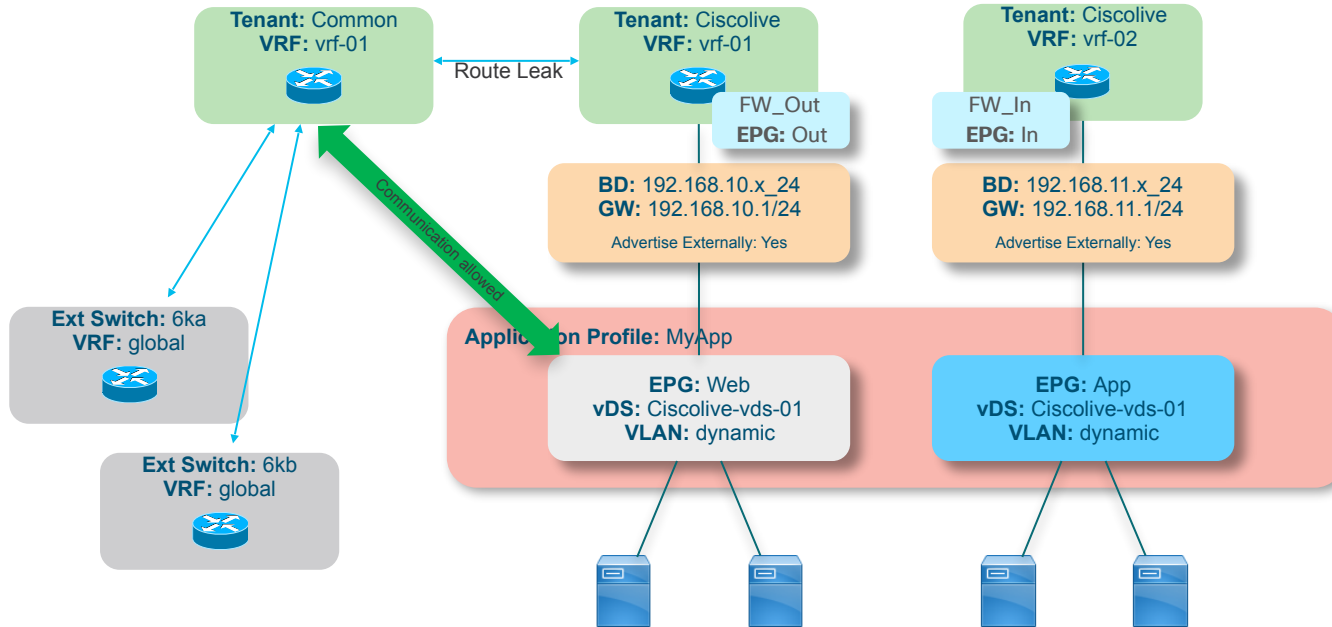
```
0.0.0.0/0, ubest/mbest: 1/0
```

```
*via 102.0.100.1%common:vrf-01, eth1/96.9, [20/1], 00:16:33, bgp-64512, external, tag 64512
```

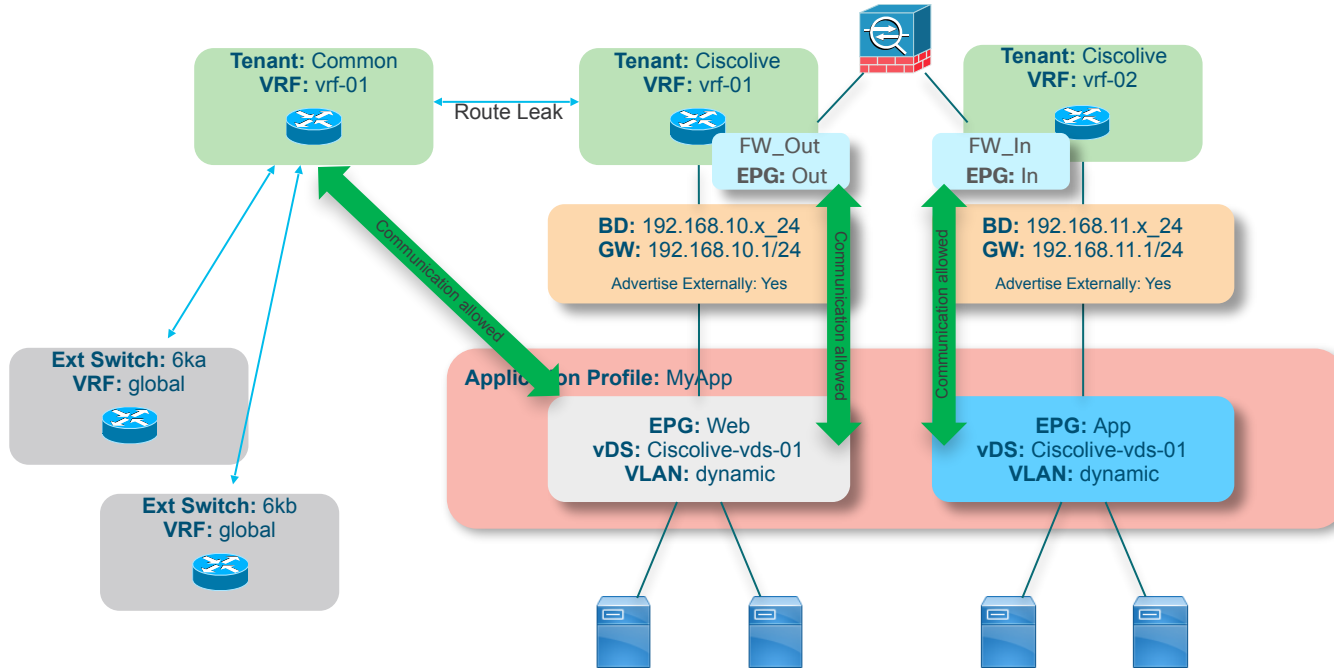
```
apic1#
```

Firewall Integration

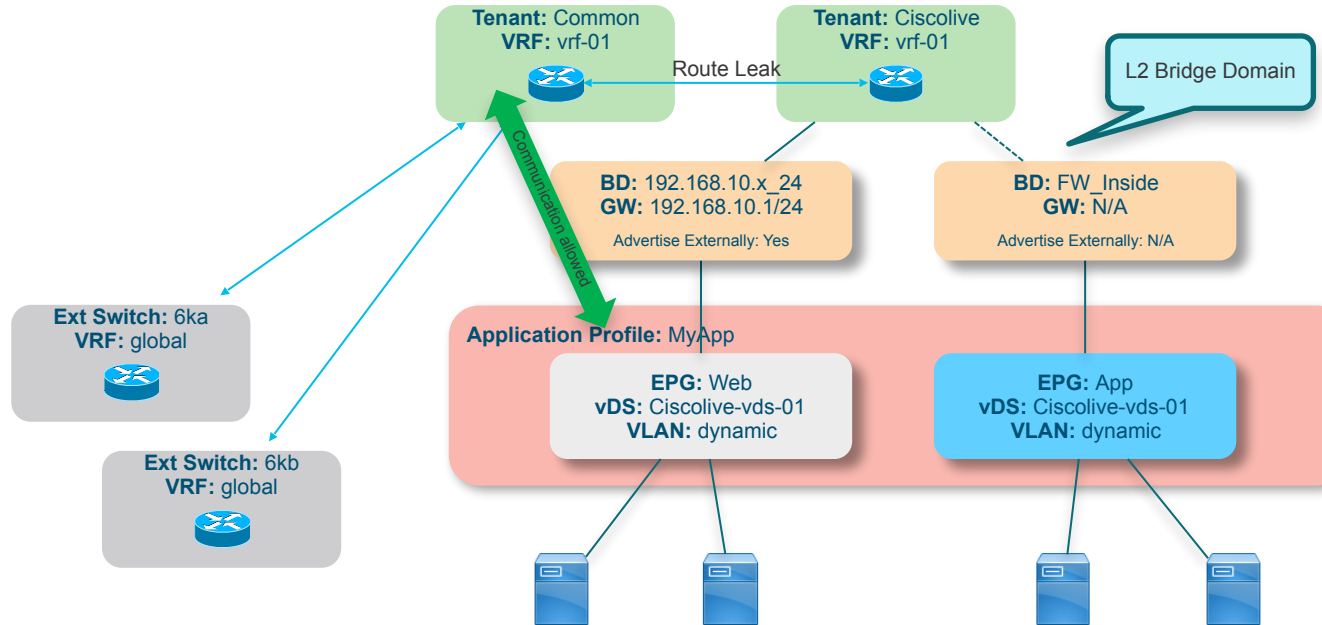
L3out – Route Peering



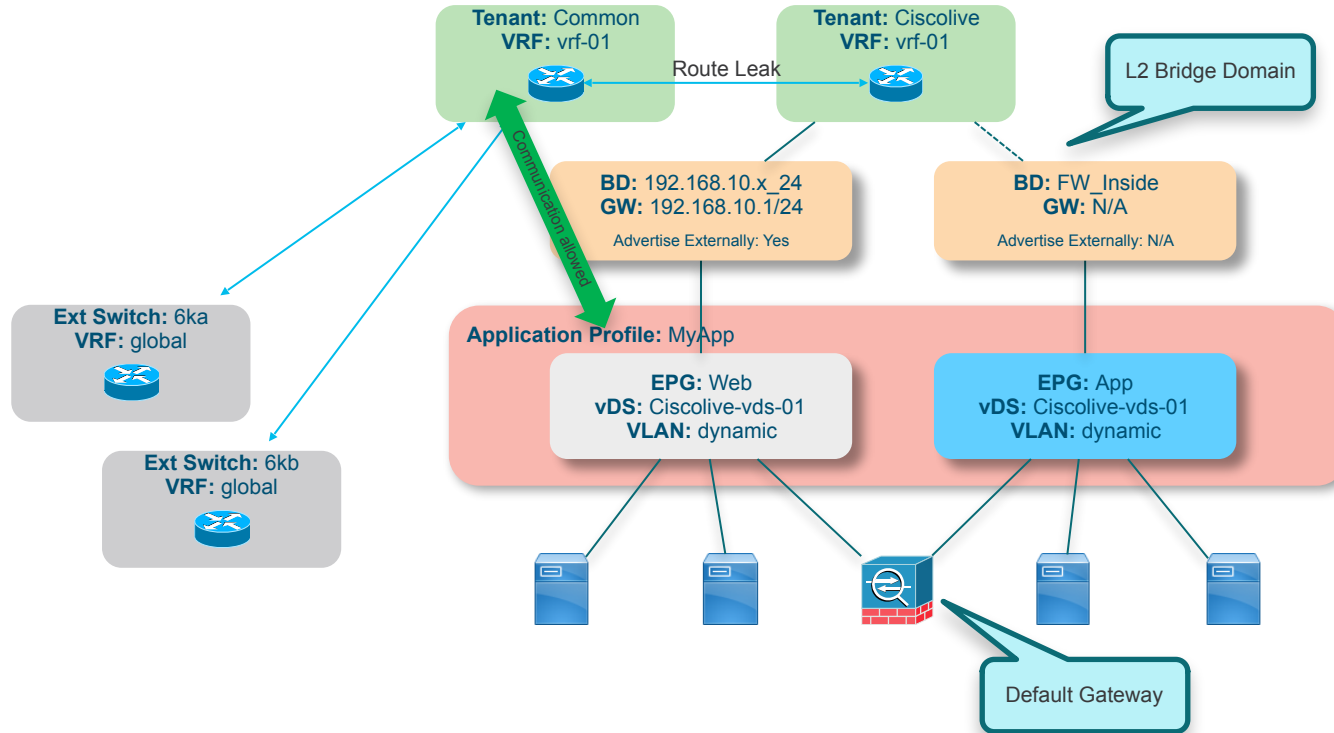
L3out – Route Peering



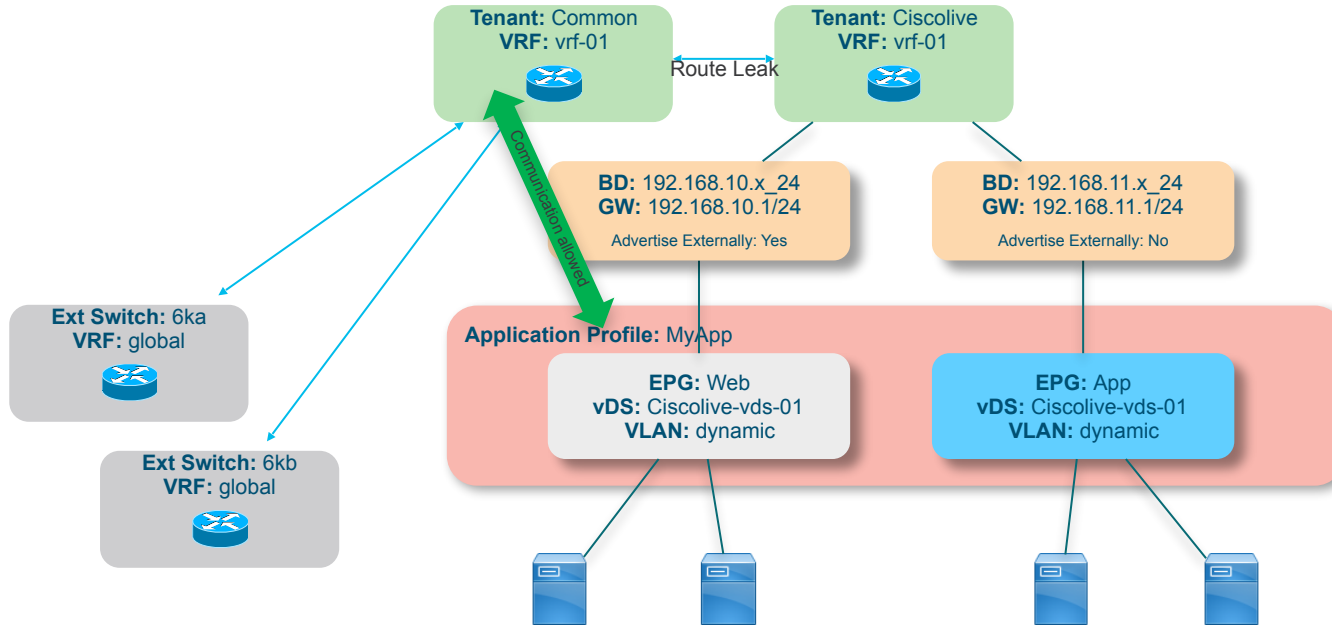
NAT



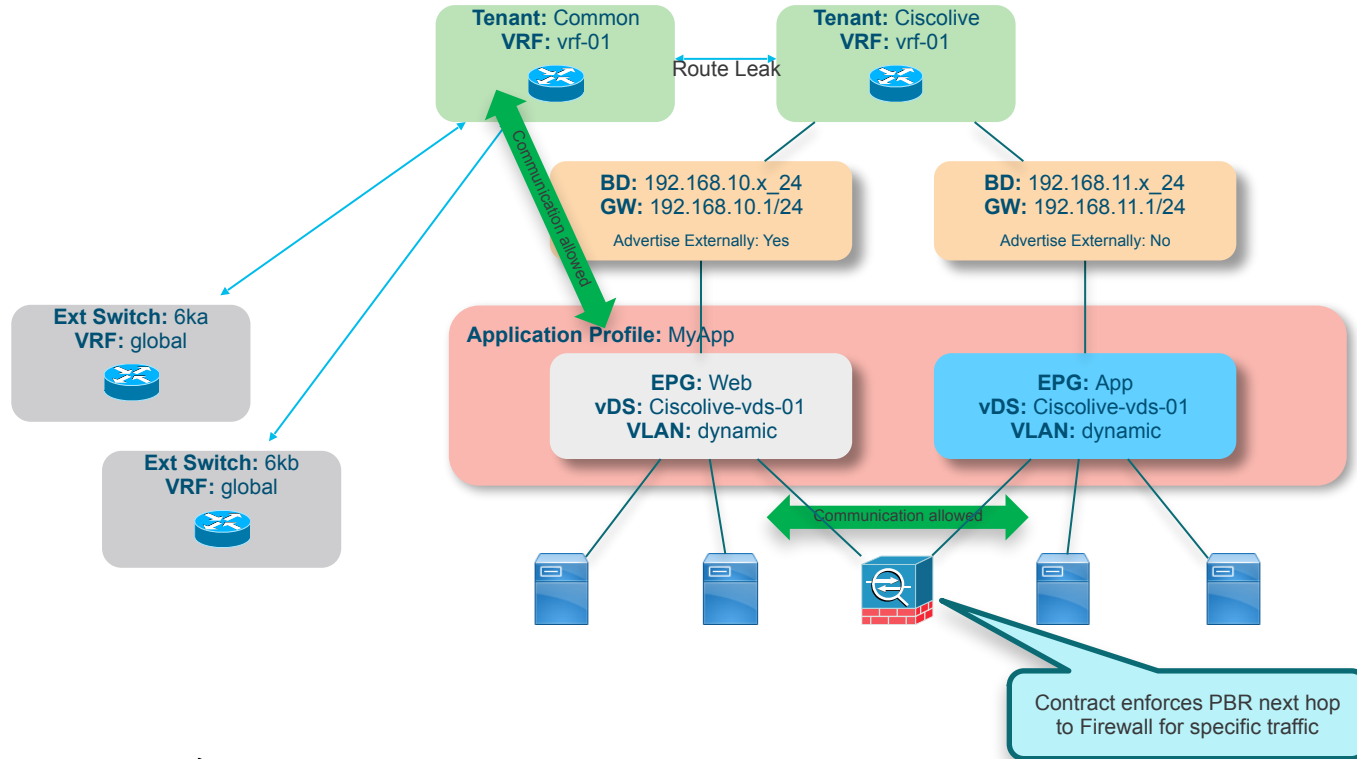
NAT



PBR – Service Graph

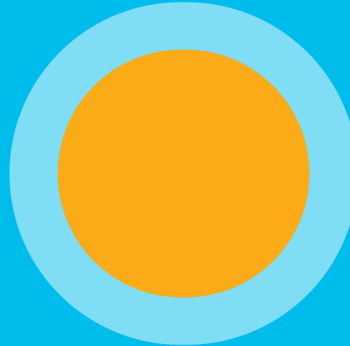


PBR – Service Graph



How does ACI integrate with VMware's virtual switches?

Why should you care about integrating with VMware's Virtual Switches?



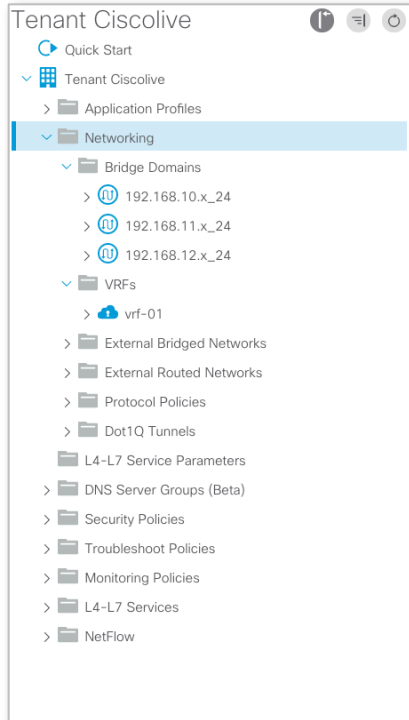
A perceived barrier to timely delivery of new services (from Virtualization Teams) is that it takes too long to provision Network Services i.e. VLANs, Subnets, and L4-7 Devices

Most automation projects start with server/application teams, therefore it makes sense to offer the network as a consumable service

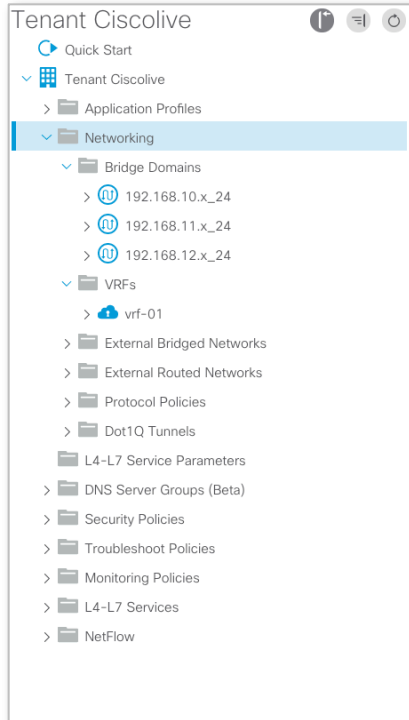
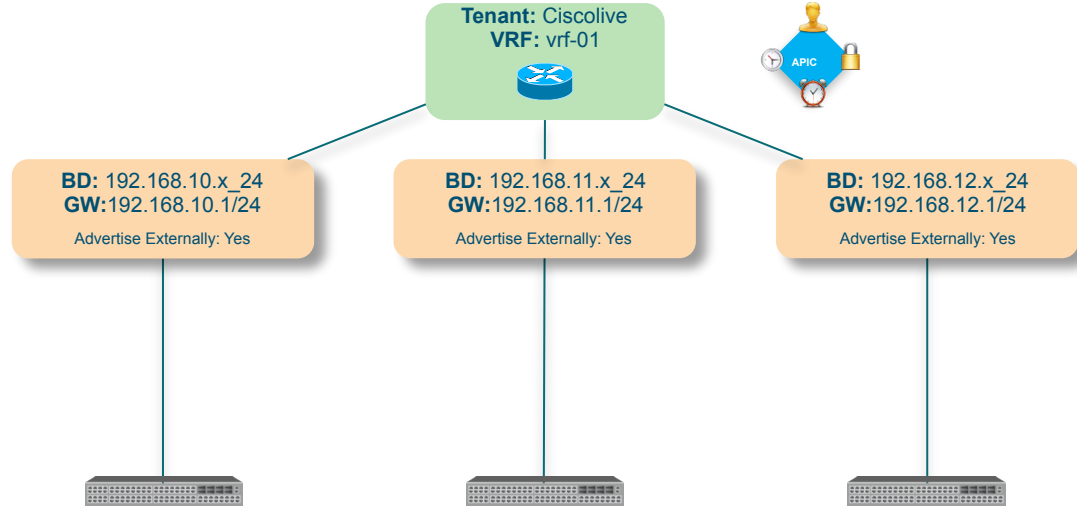
There are four integration options with VMware

1. Independently configure the vSwitch/vDS as you do today
2. Create EPGs on vCenter and map them to an APIC managed vDS to create port groups – requires ACI plugin
3. Create EPGs on APIC and map them to an APIC managed vDS to create port groups
4. Create EPGs on APIC and map them to an AVE to create port groups

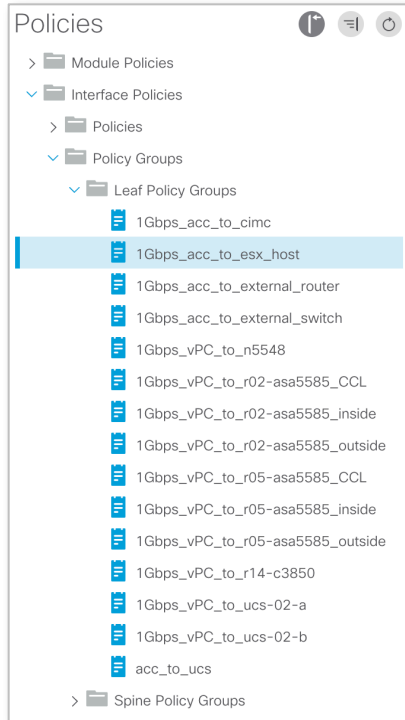
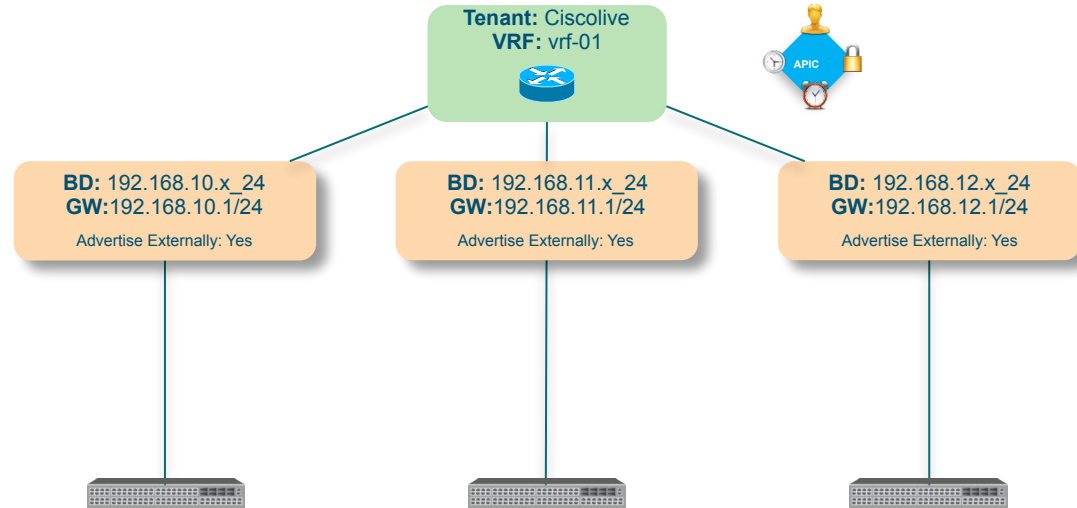
Network Team configures VRFs/subnets



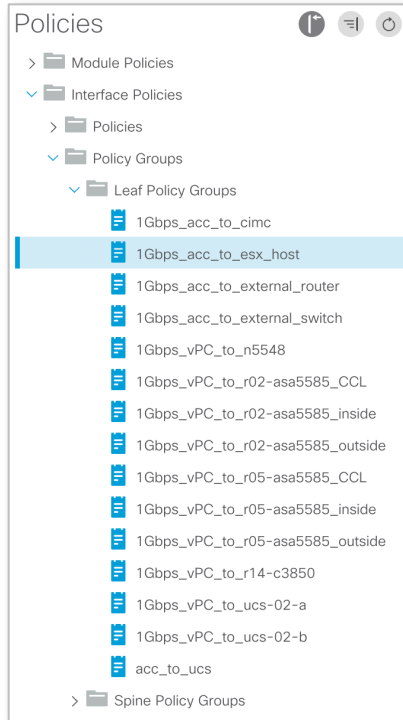
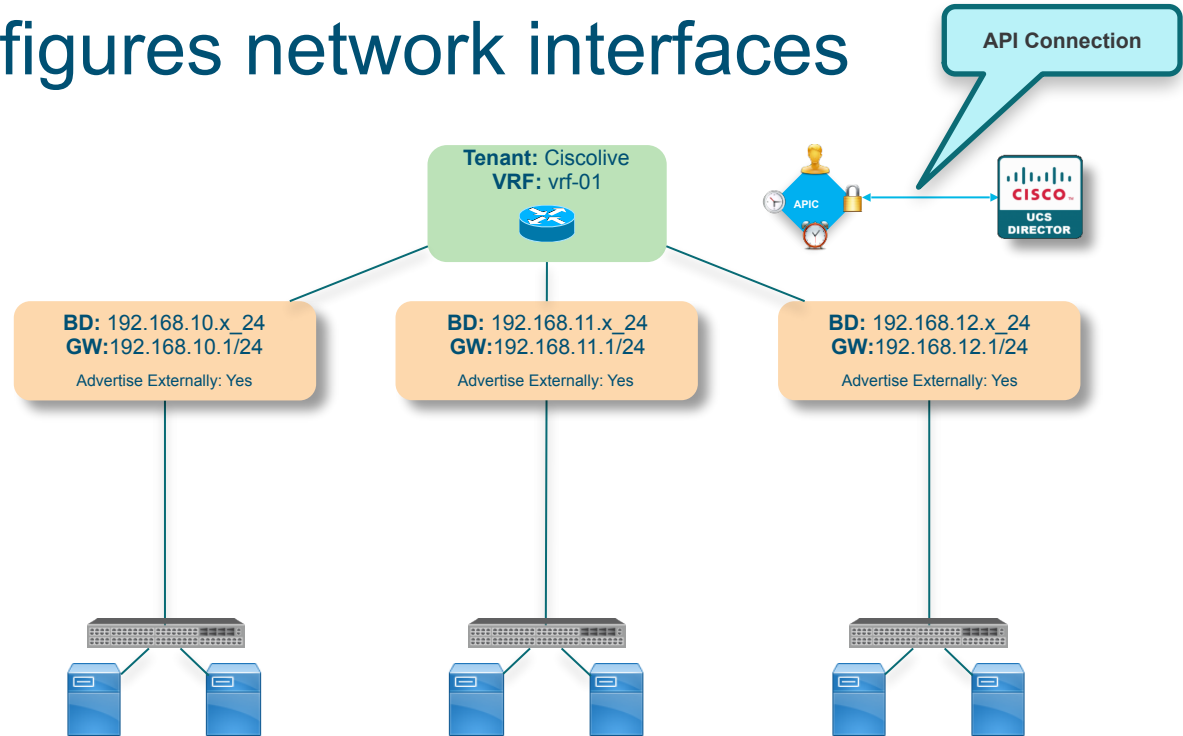
Network Team configures VRFs/subnets



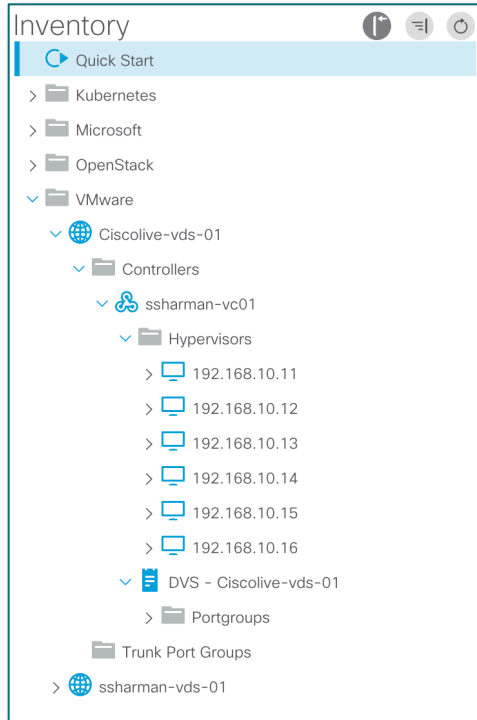
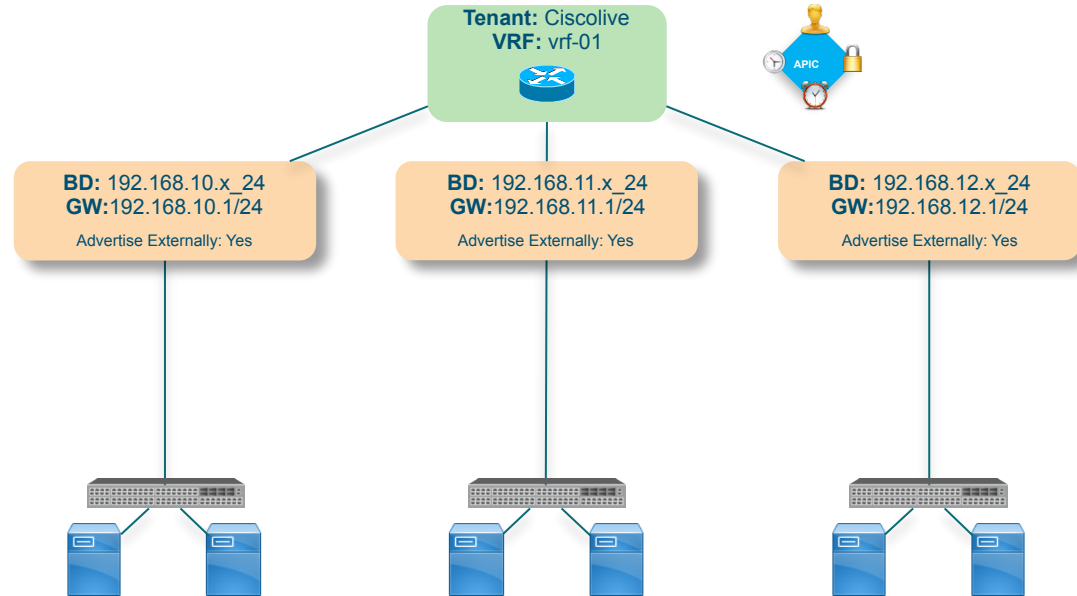
Server Team configures network interfaces



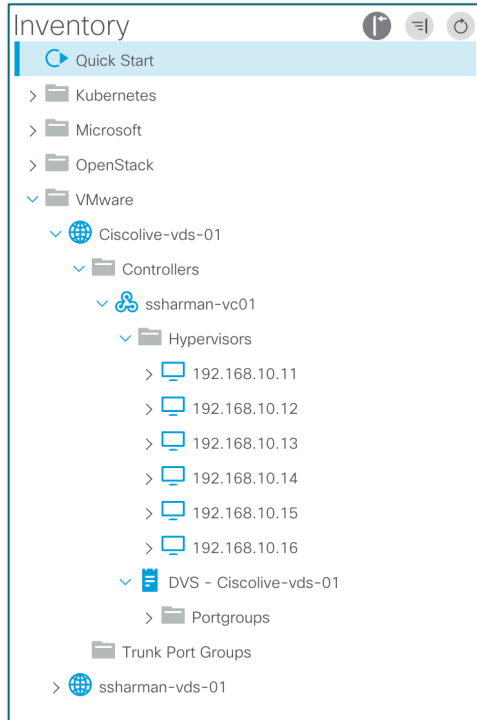
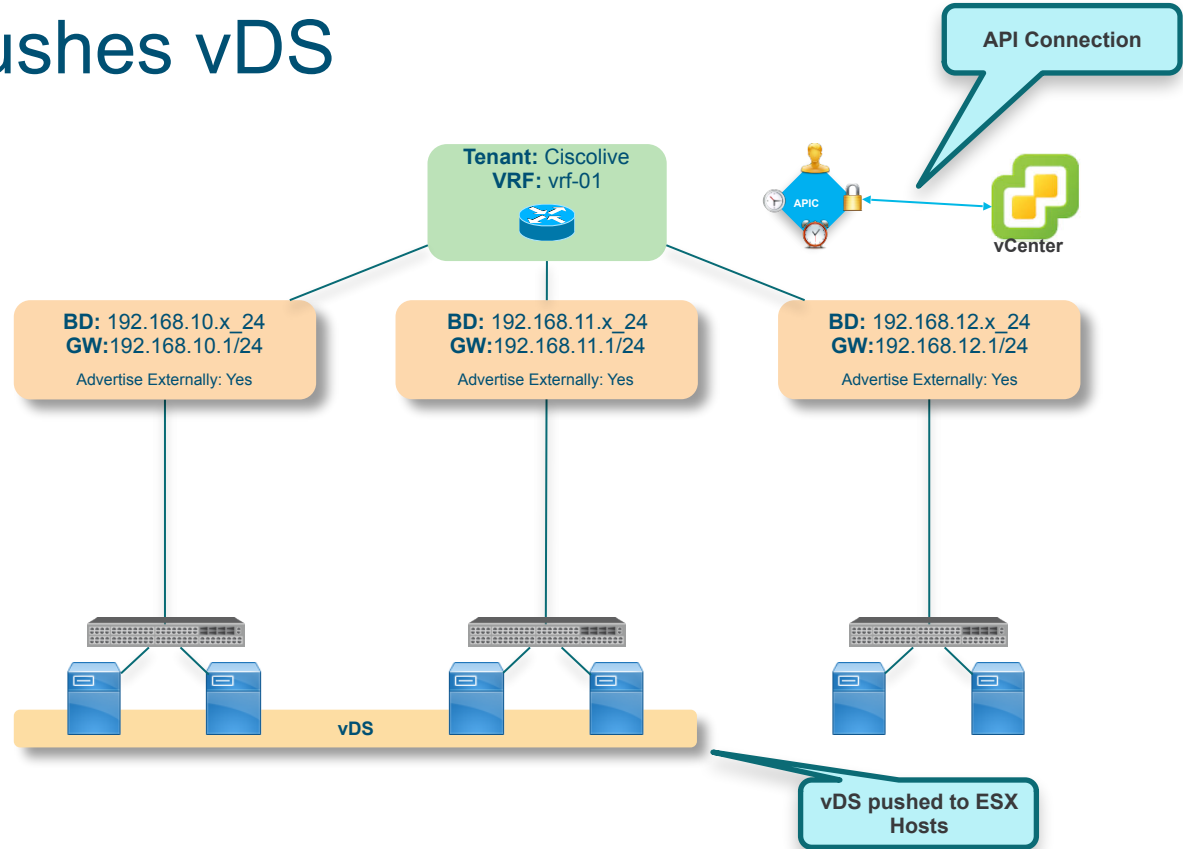
Server Team configures network interfaces



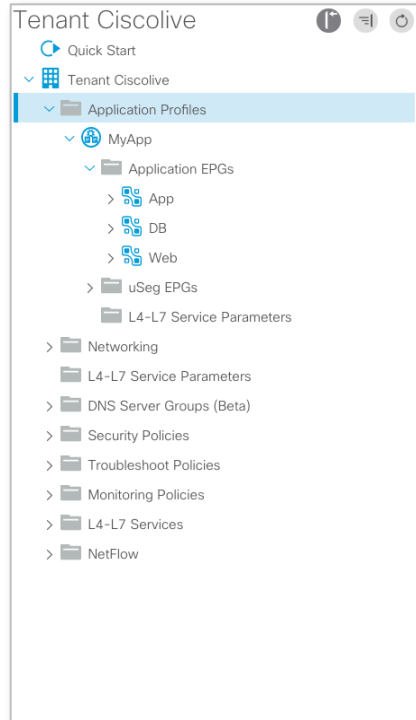
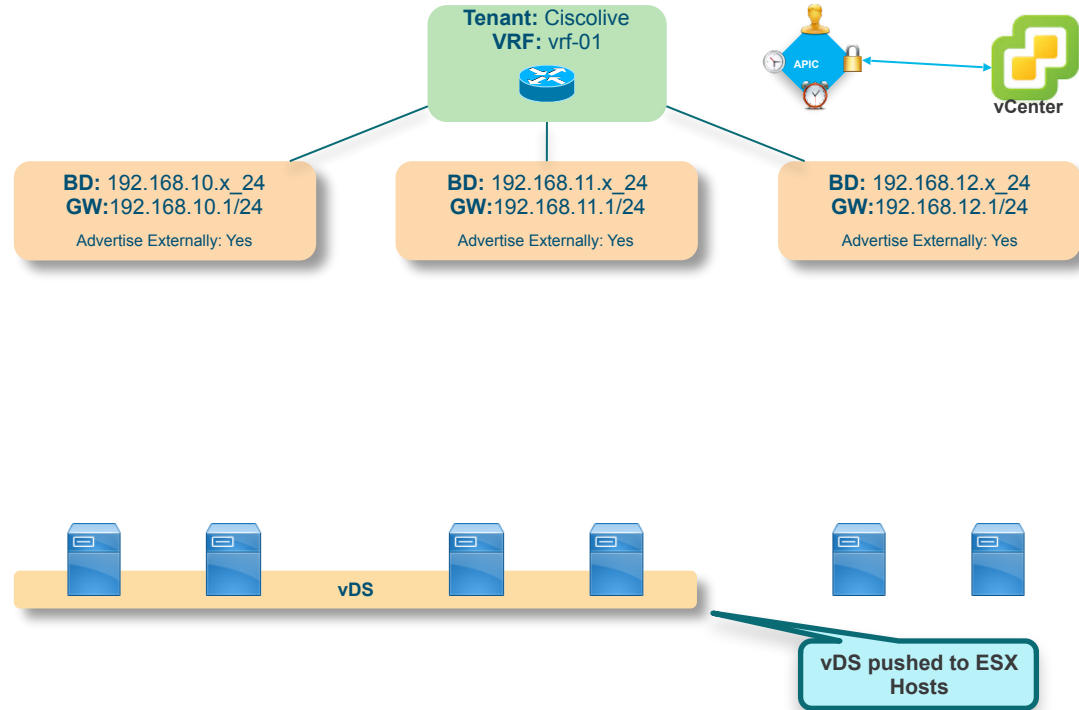
VMware Team pushes vDS



VMware Team pushes vDS



VMware Team pushes portgroups



VMware Team pushes portgroups

Tenant CiscoLive

- Quick Start
- Tenant CiscoLive
 - Application Profiles
 - MyApp
 - Application EPGs
 - App
 - DB
 - Web
 - uSeg EPGs
 - L4-L7 Service Parameters
 - Networking
 - L4-L7 Service Parameters
 - DNS Server Groups (Beta)
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services
 - NetFlow

vmware vSphere Web Client

Updated at 8:11 AM | Administrator@VSPHERE.LOCAL | Help | Search

Navigator

- Back
- Cisco ACI Fabric
 - Home
 - ACI Fabric
 - Application Profile
 - Networking
 - Troubleshooting
 - Cisco AVS
 - Resources
 - Network
 - Security
 - External Connectivity
 - L4-7 Services

Application Profile

Tenant: CiscoLive Application Profile: MyApp

Drag and Drop the different elements below to fully configure your Application Profiles

Create a new Application Profile

Policy Traffic Stats Health Faults Audit Logs Events

Drag and drop to configure:

- Endpoint Group
- uEPG
- L3 External Network
- L2 External Network
- Contract

Reset view Switch to Consumer/Provider view

```
graph LR; A[permit_to_0.0.0.0_0] --> B[permit_to_web_servers]; A --> C[permit_to_application_servers]; A --> D[permit_to_database_servers]; B --> E[Web]; C --> F[App]; D --> G[DB];
```

Recent Objects

Viewed	Created
yVM-02	
yVM-03	
candid-prod-64.1.0.0.872-01	
wireshark-01	

Recent Tasks

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
Check new notifications	ssharmn-vc01.ukt...	Completed	VMware vSphere U...	464 ms	2/7/18, 8:02:01 AM ...	2/7/18, 8:05:33 AM ...	ssharmn-vc01.uktme.cisco.com

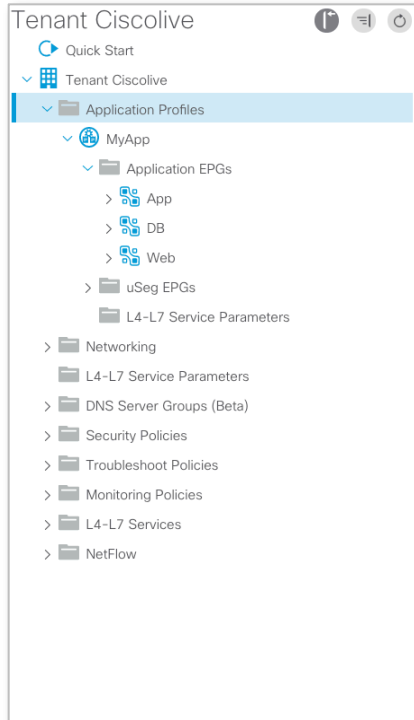
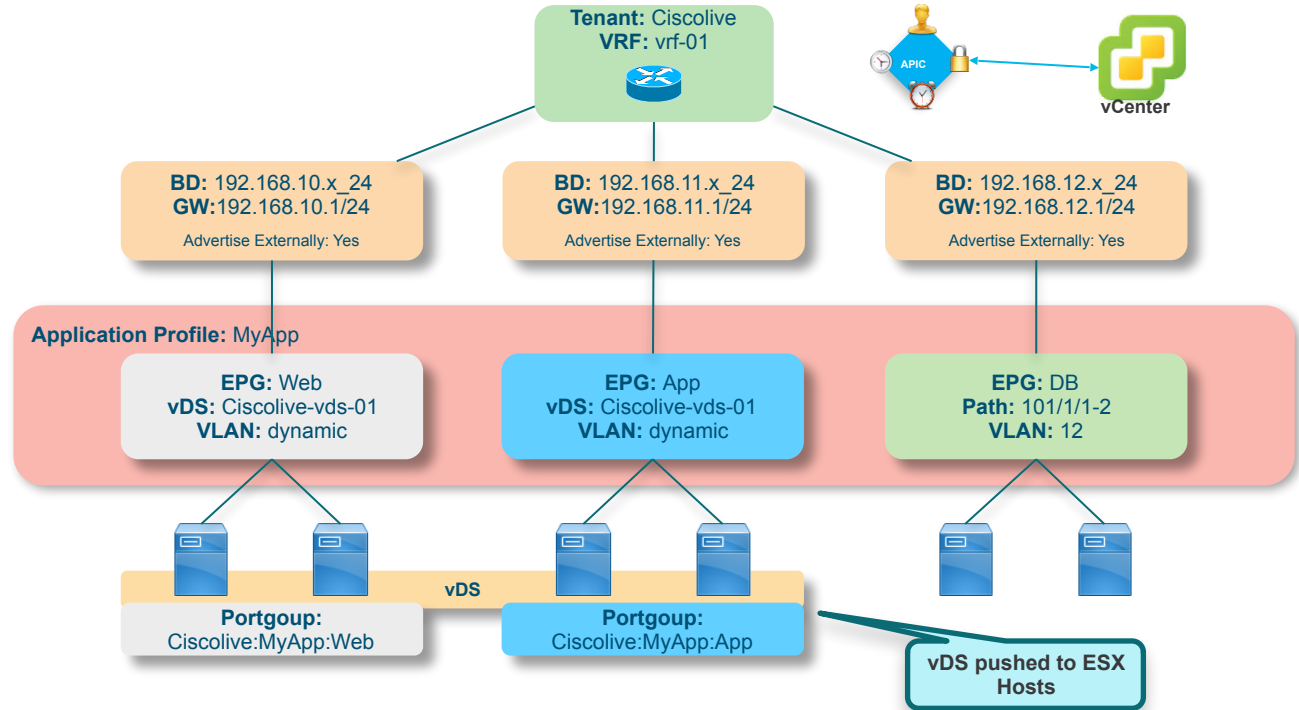
CiscoLive!

BRKACI-1002

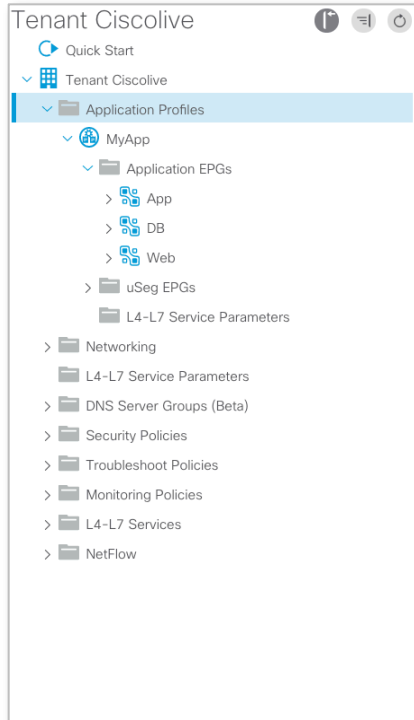
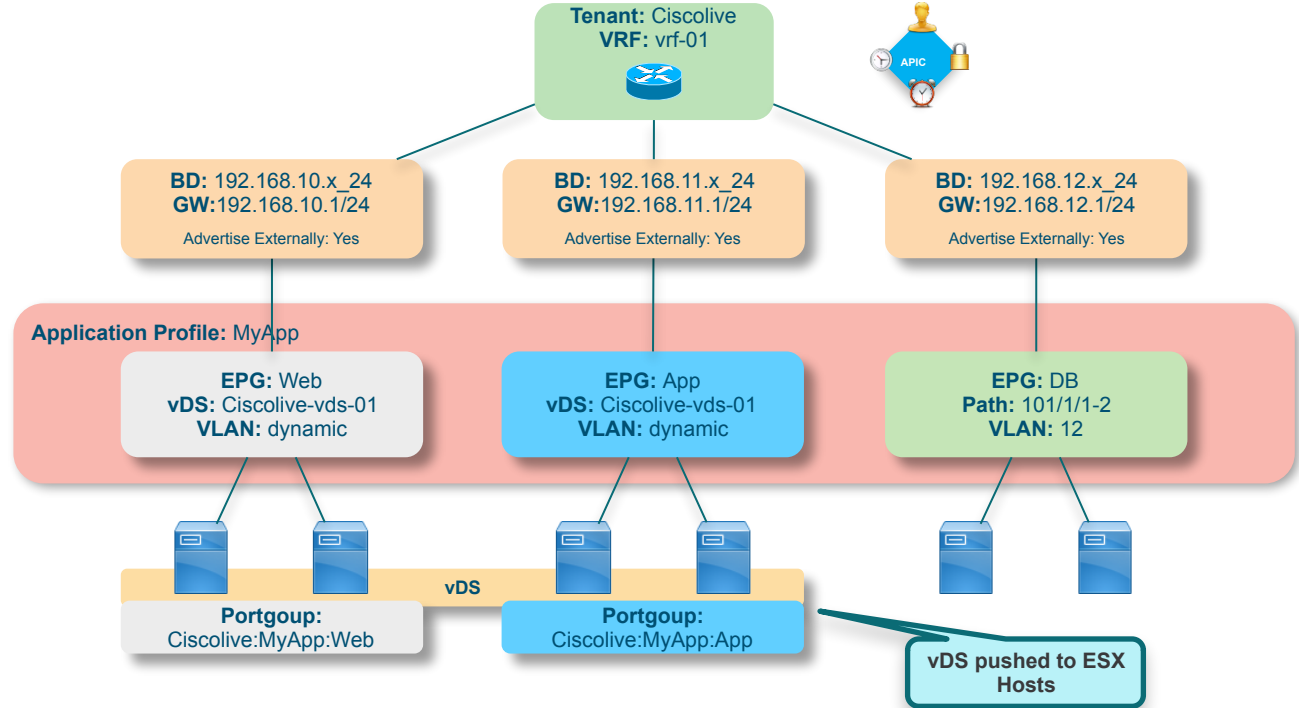
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

120

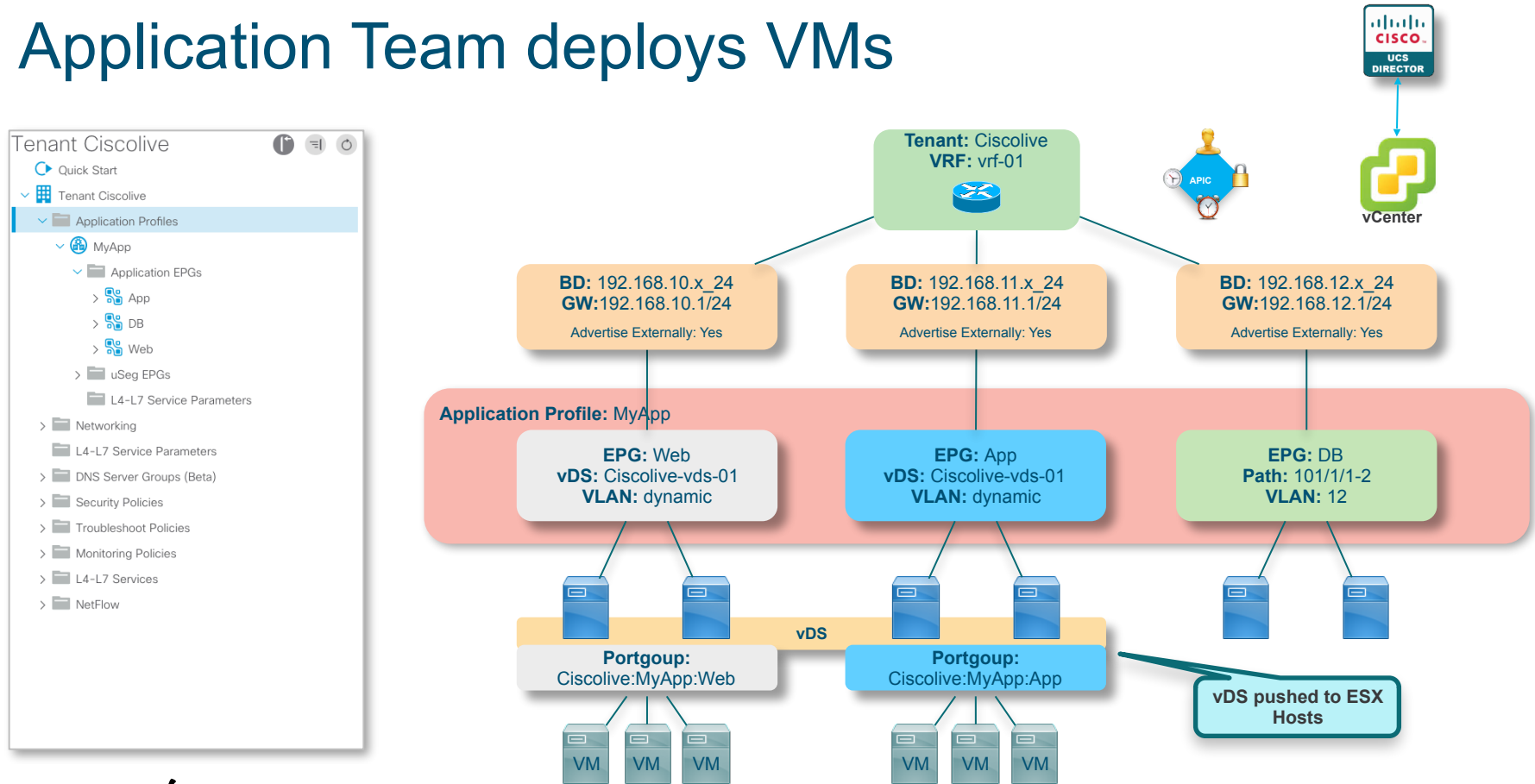
VMware Team pushes portgroups



Application Team deploys VMs



Application Team deploys VMs



There are two ways to interoperate with VMware NSX

Option 1 – NSX for Virtual Machine Security:

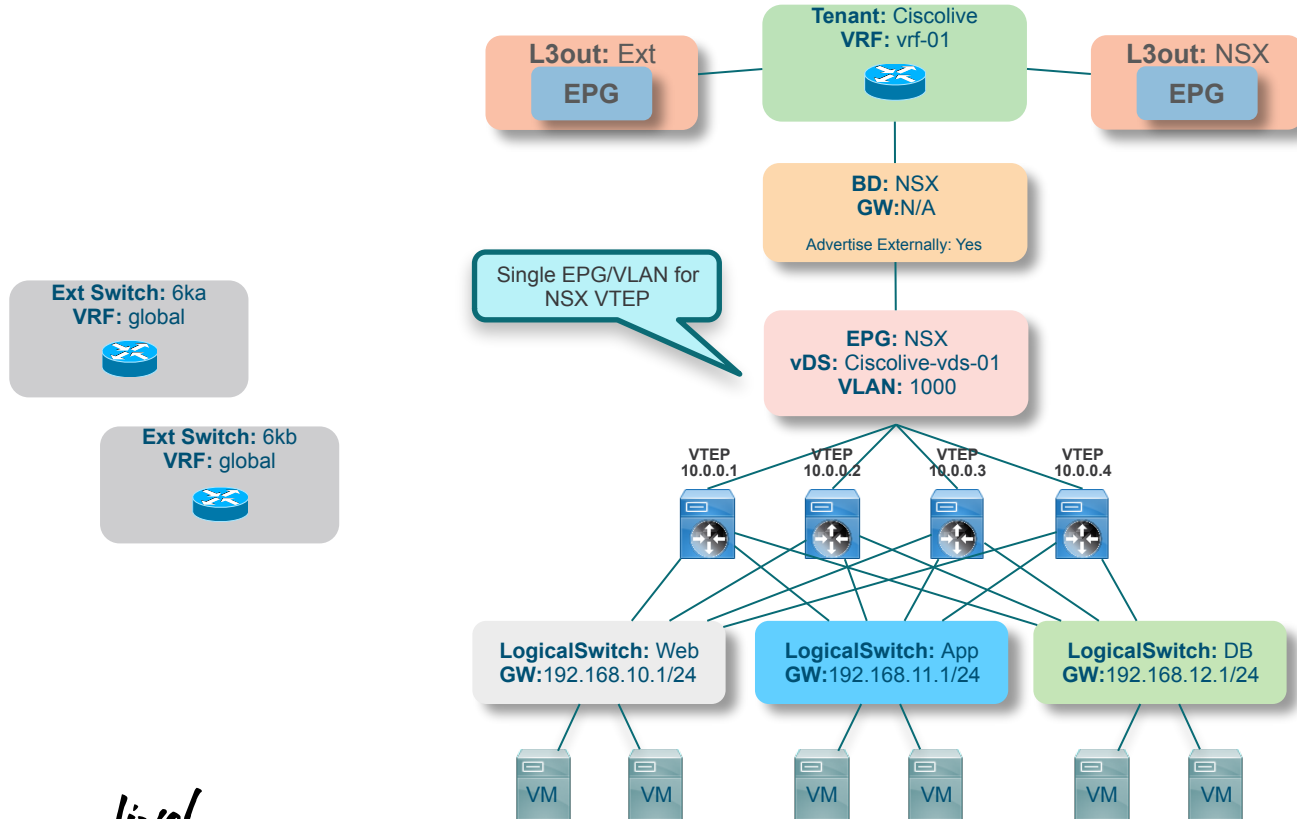
- Uses NSX as a security and services solution (DFW, LB, etc.)
- ACI functions as integrated overlay and underlay
- No requirement for NSX VTEP configuration
- ACI uses VMM Domain programming application dvPortGroups

There are two ways to interoperate with VMware NSX

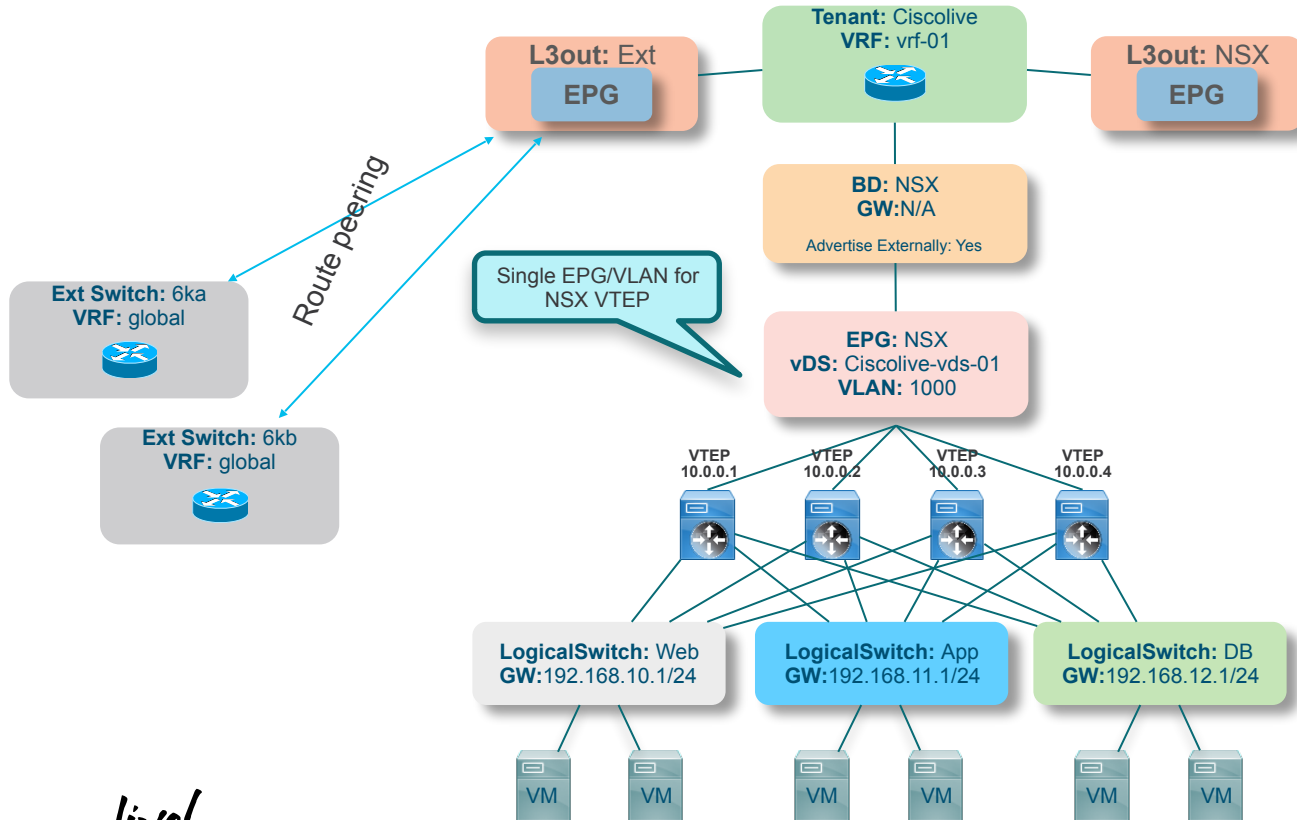
Option 2 – NSX for Networking and Virtual Machine Security:

- ACI functions as an underlay network
- NSX functions as a VXLAN overlay
- Customer follows VMware Design Recommendations
- ACI can use VMM Domain to enhance visibility
- NSX Host to Host VTEP connectivity can use ACI in various VTEP subnet models:
 - Single VTEP Subnet
 - VTEP Subnet per Rack
 - VTEP Subnet per Cluster

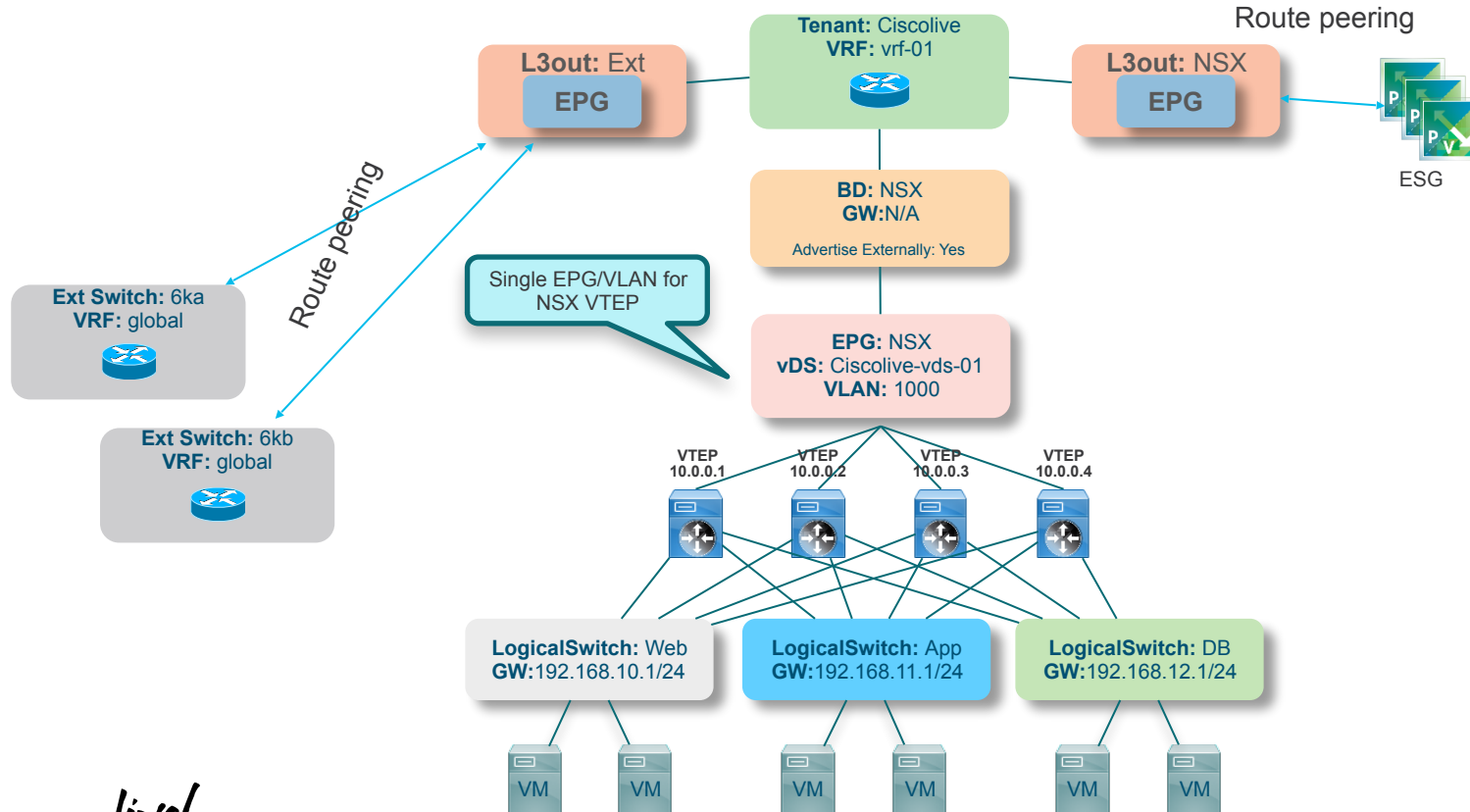
NSX Overlay



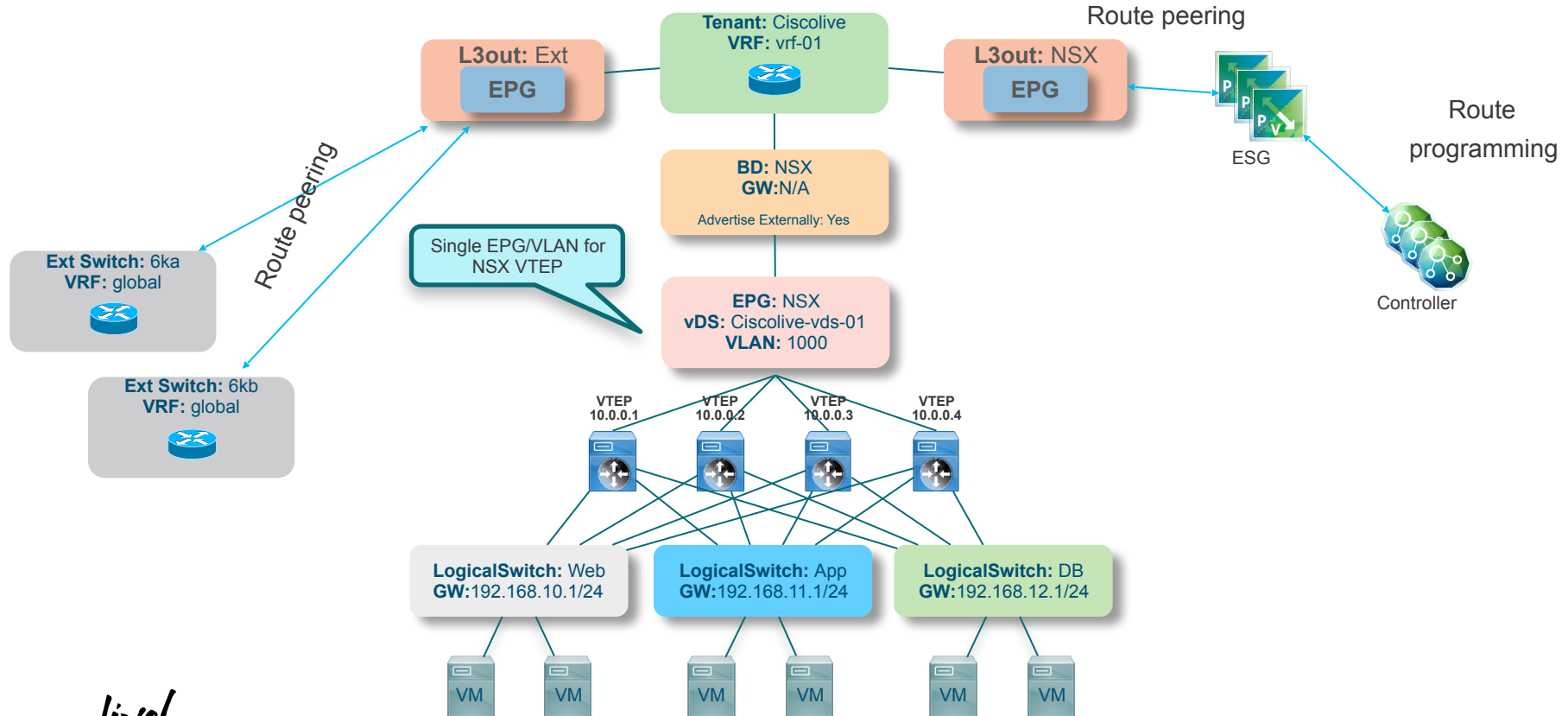
NSX Overlay



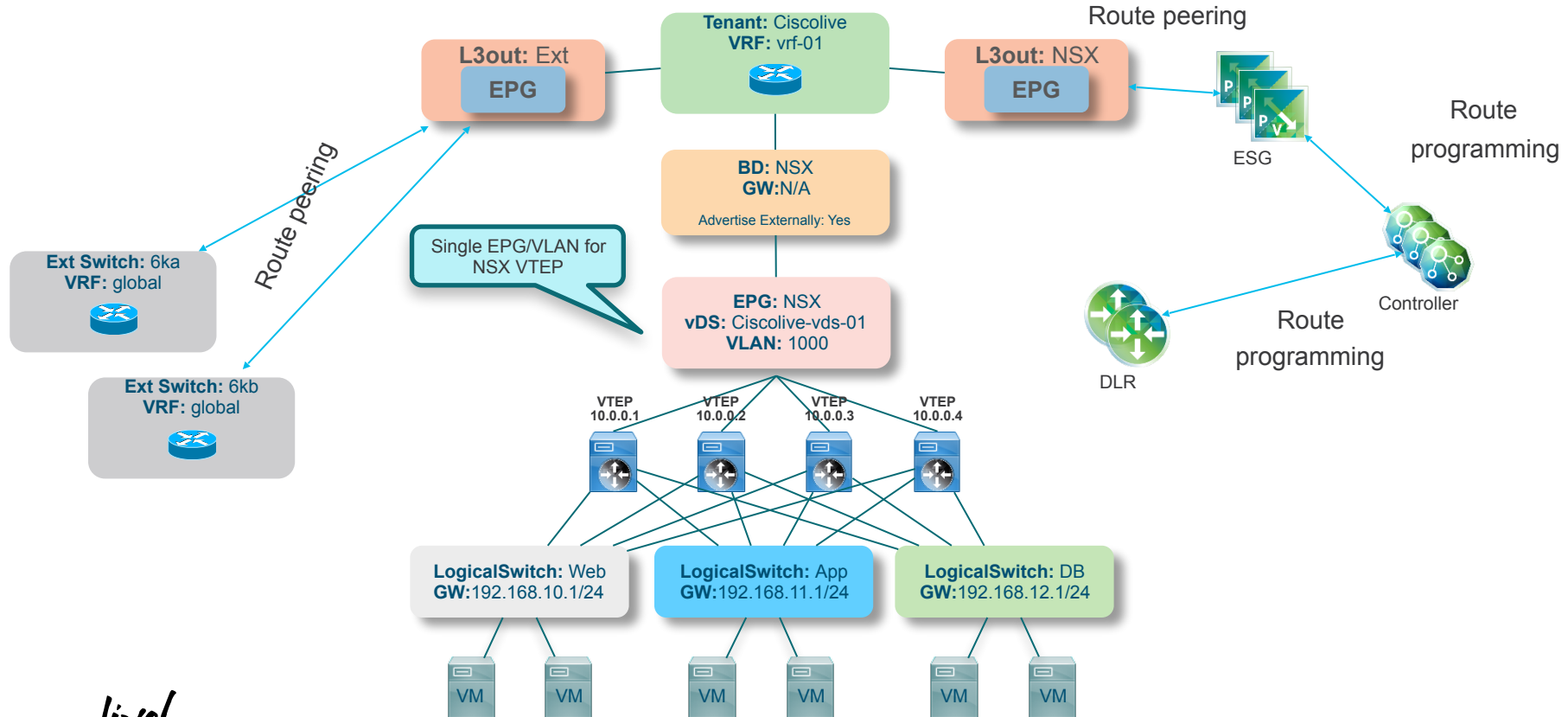
NSX Overlay



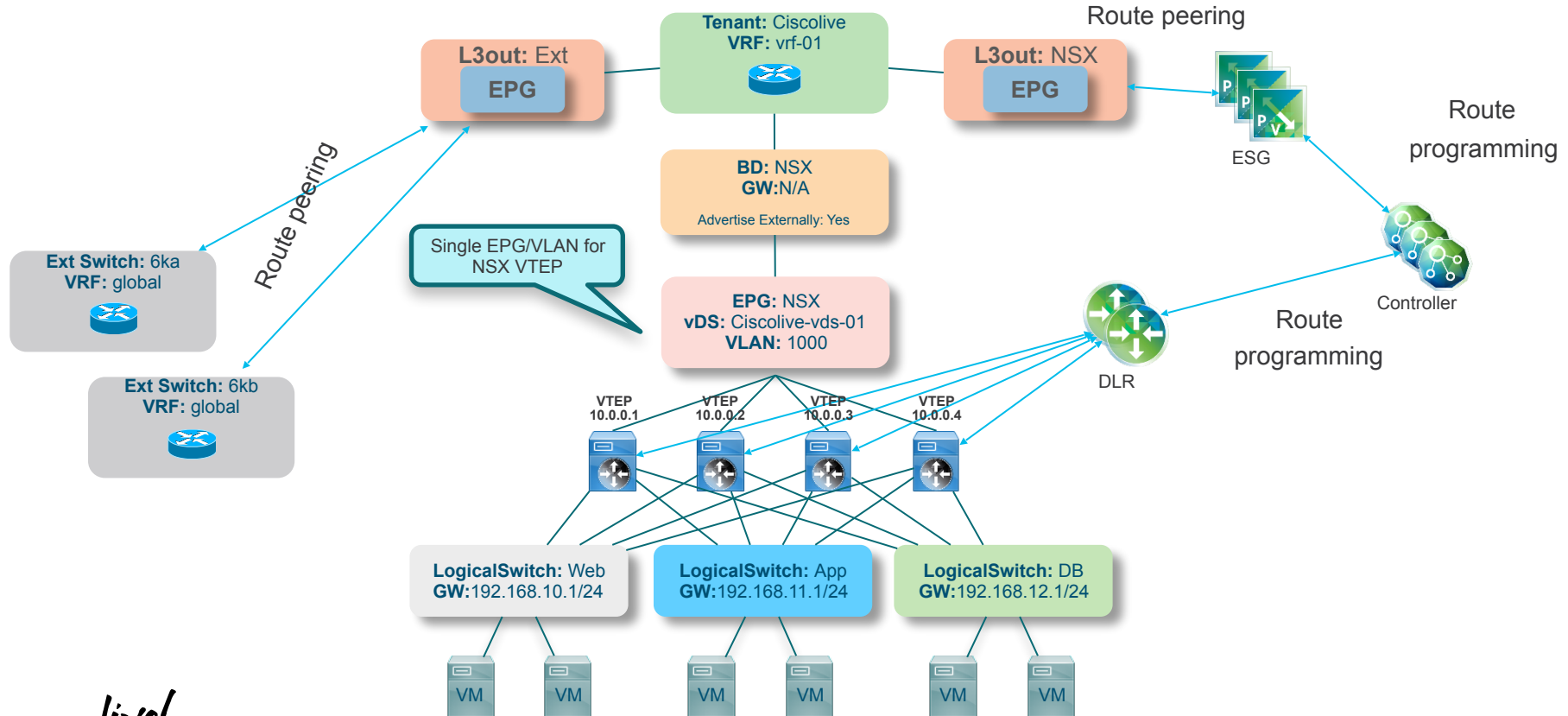
NSX Overlay



NSX Overlay

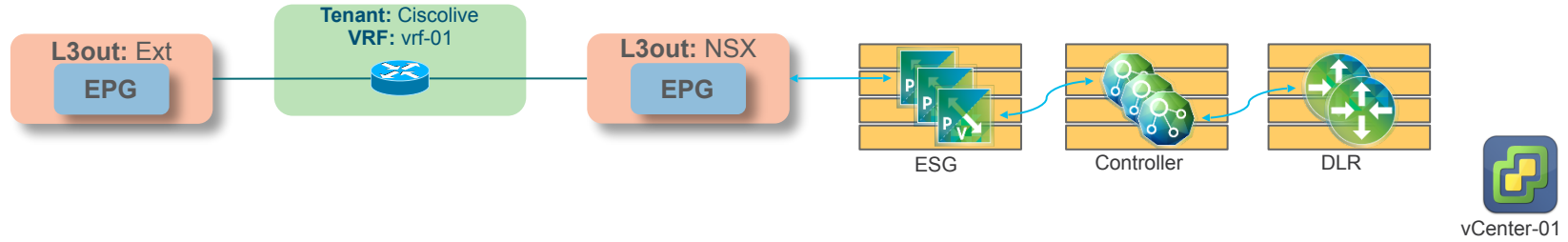


NSX Overlay

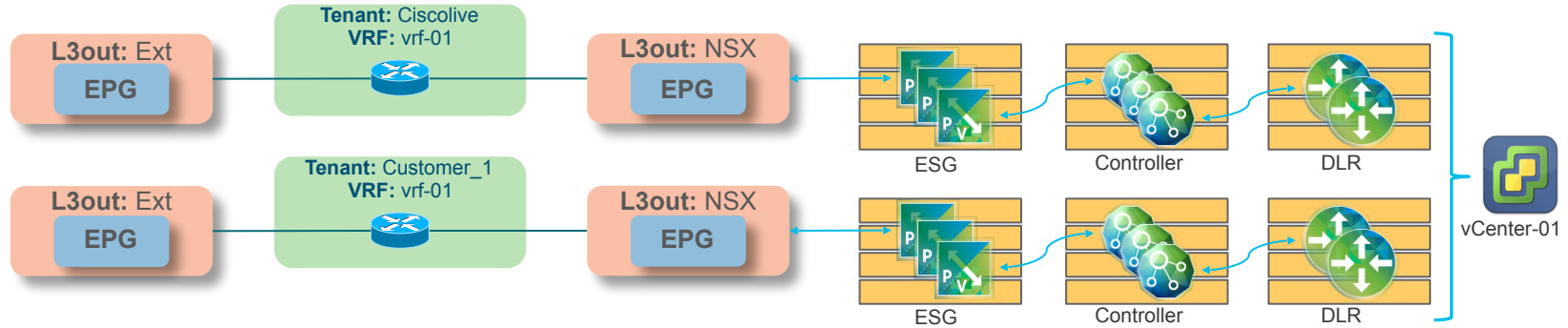


NSX Overlay at scale

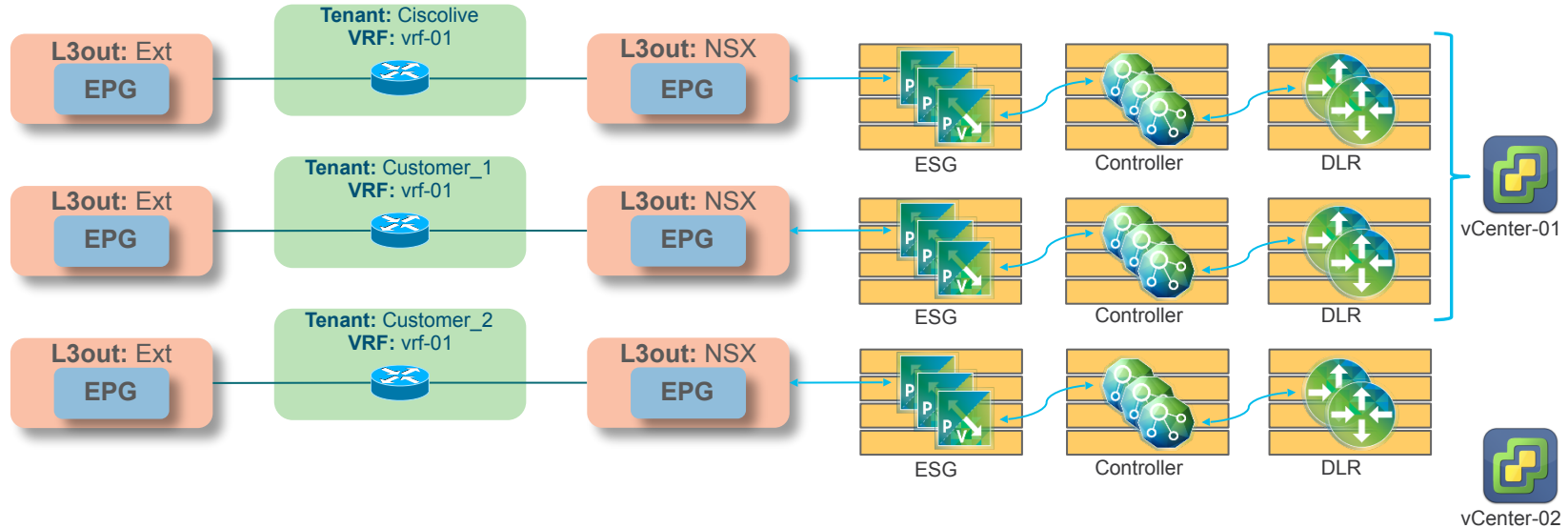
NSX Overlay at scale



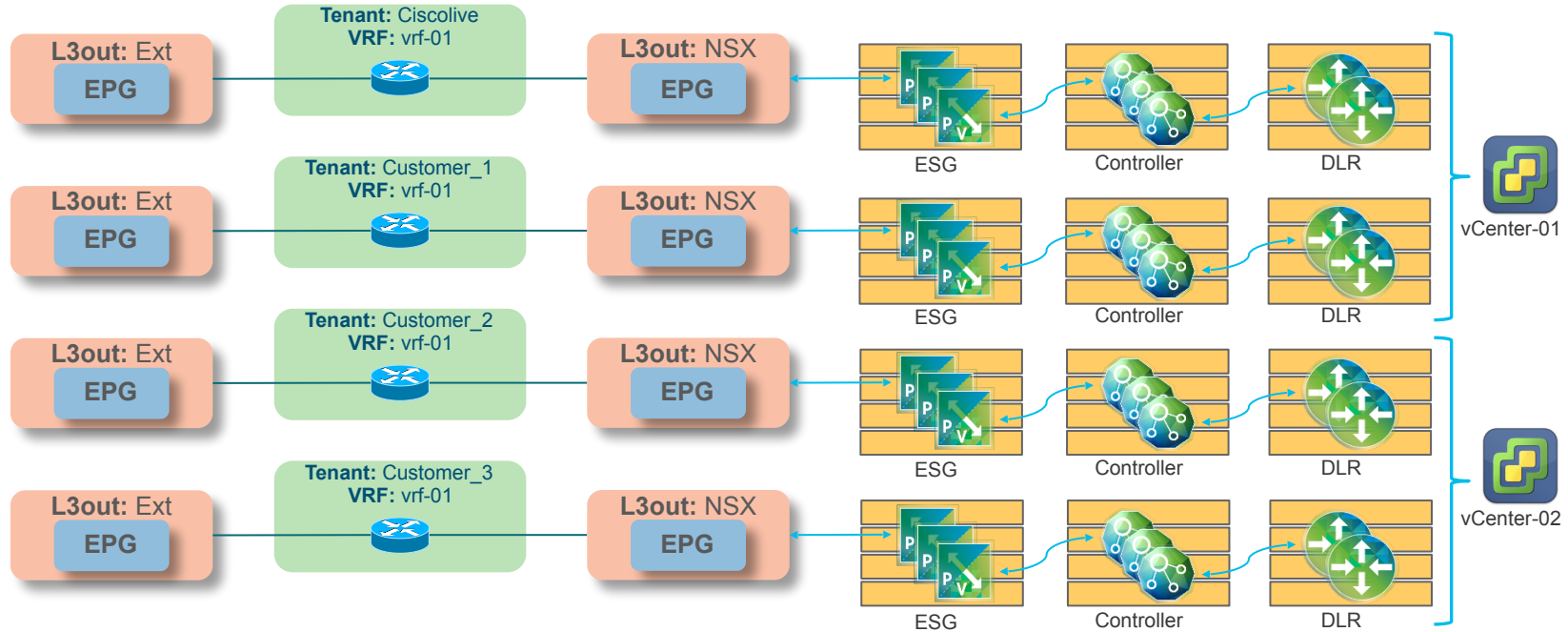
NSX Overlay at scale



NSX Overlay at scale



NSX Overlay at scale

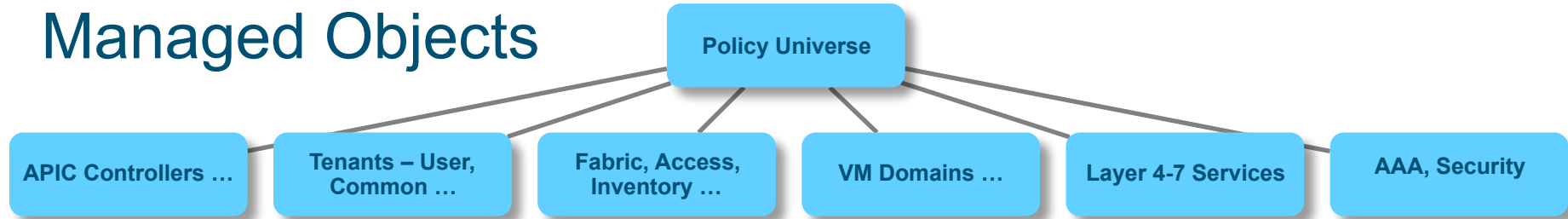


How to get started programming your ACI fabric

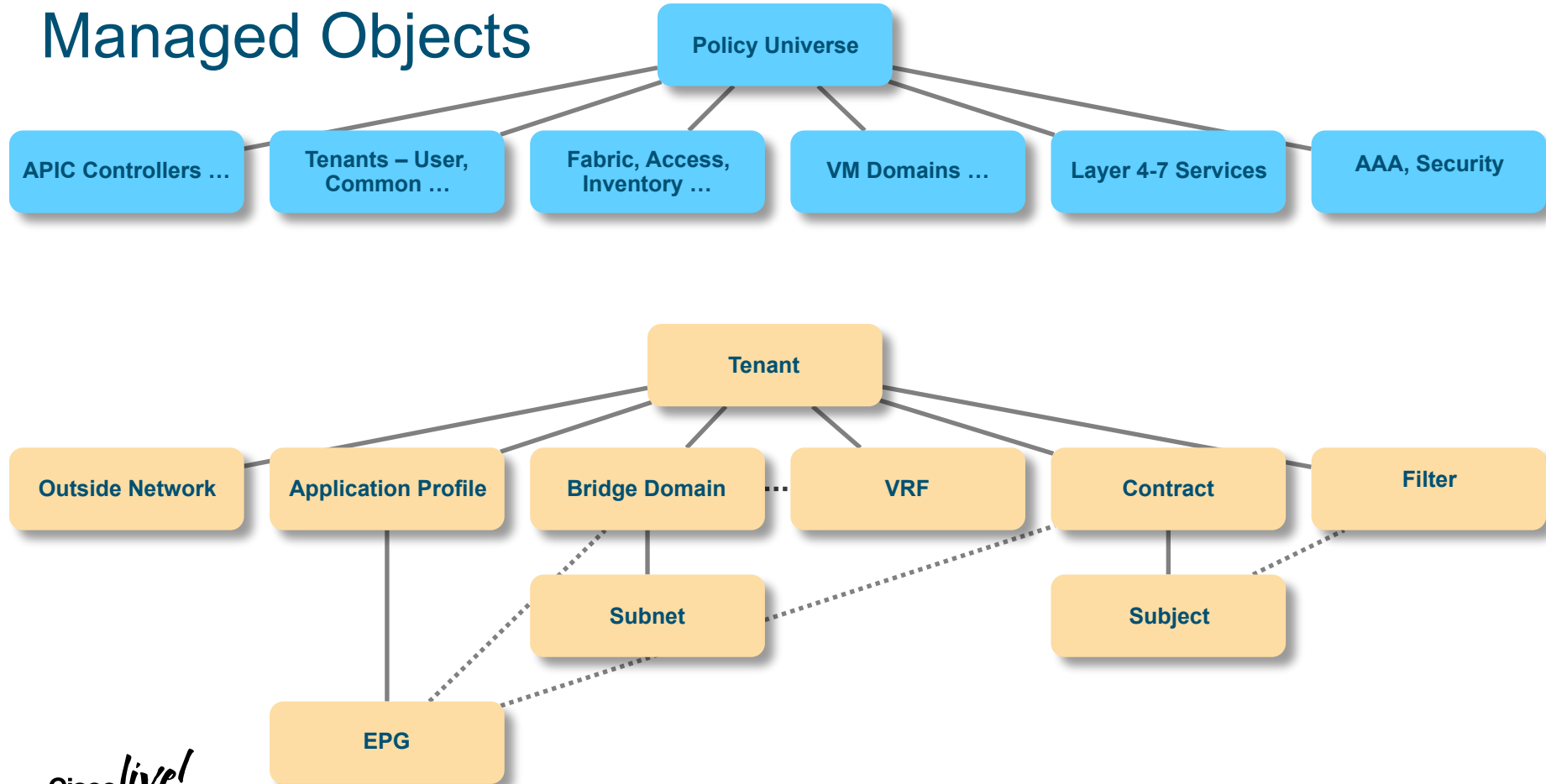
First you need a basic understand of the ACI Policy Model

You've already been learning about the ACI Policy Model
during this presentation

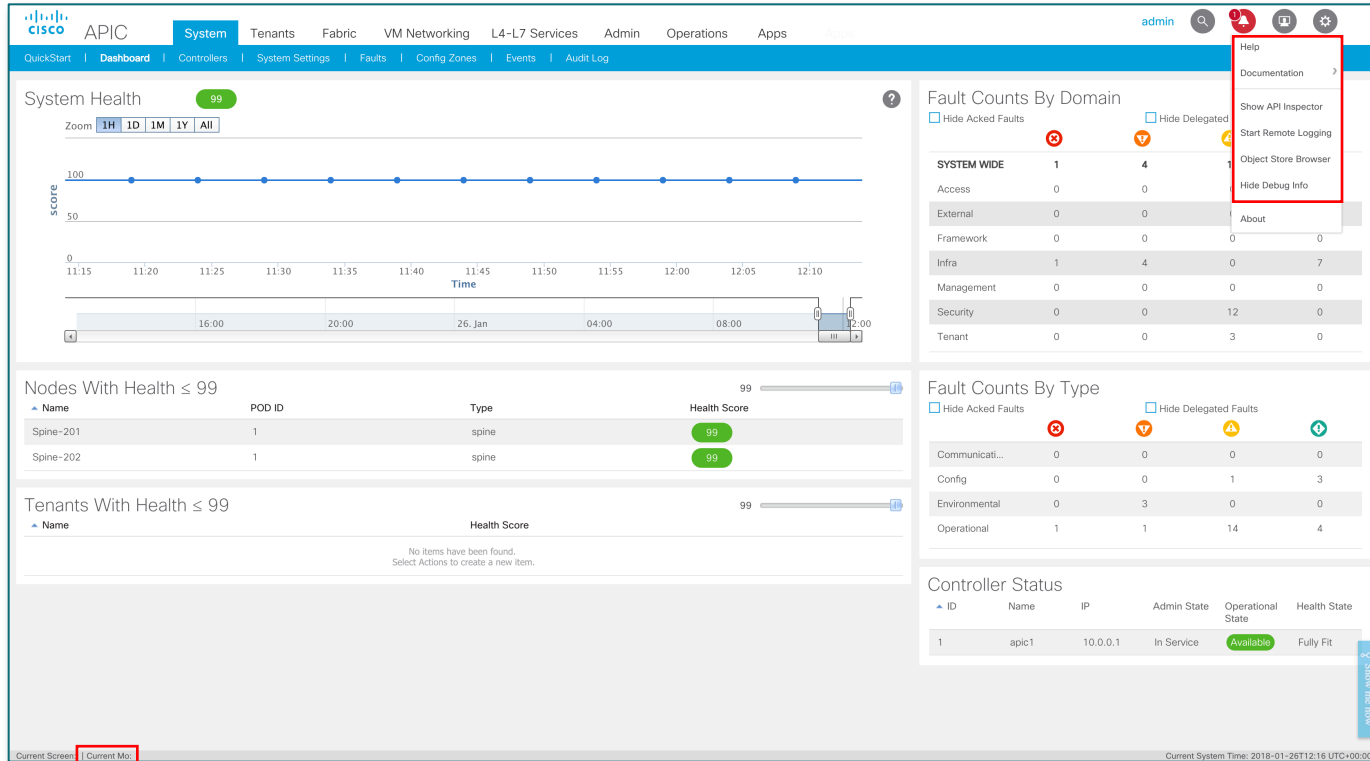
Managed Objects



Managed Objects



https://{{APIC}}/



https://{{APIC}}/doc/html/

CISCO

APIC Management Information Model Reference

?

All Packages

Classes

[aaa:ADomainRef](#) (Reference to Domain Tag for Parent Object)
[aaa:ADomainRefTask](#)
[aaa:AuthProvider](#)
[aaa:ARbacRule](#) (RBAC Rule)
[aaa:ARetP](#) (Record Retention Policy)
[aaa:AppToken](#) (Request webtoken for an App)
[aaa:AppUser](#) (App User)
[aaa:AuthMethod](#)
[aaa:AuthRealm](#) (AAA Authentication)
[aaa:Banner](#)
[aaa:ChangePassword](#) (Change Password Method)
[aaa:ChangeRole](#) (Change Role Method)
[aaa:ChangeSshKey](#) (Change Ssh Key Method)
[aaa:ChangeX509Cert](#) (Change X509 Cert Method)
[aaa:Config](#)
[aaa:ConsoleAuth](#) (Console Authentication Method)
[aaa:CtrlrFipsState](#)
[aaa:CtrlrRetP](#) (Controller Audit Log Retention Policy)
[aaa:DefaultAuth](#) (Default Authentication Method for all Logins)
[aaa:Definition](#)
[aaa:Domain](#) (Security Domain)
[aaa:DomainAuth](#) (Authentication Method for the Domain)
[aaa:DomainRef](#) (Reference to Domain Tag for Parent Object)
[aaa:DomainRolesTuple](#) (Internal RBAC Container)
Type
Events
Faults
FSMs
Tasks
Errors
Syslog Messages

Overview

Diagram

Inheritance

Events

Faults

FSMs

Properties

Summary

Properties Detail

Class aaa:ADomainRef (ABSTRACT)

Class ID:5293
Class Label: Reference to Domain Tag for Parent Object
Encrypted: false - Exportable: true - Persistent: true - Configurable: true - Subject to Quota: Disabled
Write Access: [admin]
Read Access: [aaa, access-connectivity-1, access-connectivity-2, access-connectivity-3, access-connectivity-mgmt, access-connectivity-util, access-equipment, access-protocol-1, access-protocol-2, access-protocol-3, access-protocol-mgmt, access-protocol-ops, access-protocol-util, access-qos, admin, fabric-connectivity-1, fabric-connectivity-2, fabric-connectivity-3, fabric-connectivity-mgmt, fabric-connectivity-util, fabric-equipment, fabric-protocol-1, fabric-protocol-2, fabric-protocol-3, fabric-protocol-mgmt, fabric-protocol-ops, fabric-protocol-util, nw-svc-device, nw-svc-devshare, nw-svc-policy, ops, tenant-connectivity-1, tenant-connectivity-2, tenant-connectivity-3, tenant-connectivity-mgmt, tenant-connectivity-util, tenant-epg, tenant-ext-connectivity-1, tenant-ext-connectivity-2, tenant-ext-connectivity-3, tenant-ext-connectivity-mgmt, tenant-ext-connectivity-util, tenant-ext-protocol-1, tenant-ext-protocol-2, tenant-ext-protocol-3, tenant-ext-protocol-mgmt, tenant-ext-protocol-util, tenant-network-profile, tenant-protocol-1, tenant-protocol-2, tenant-protocol-3, tenant-protocol-mgmt, tenant-protocol-ops, tenant-protocol-util, tenant-qos, tenant-security, vmm-connectivity, vmm-ep, vmm-policy, vmm-protocol-ops, vmm-security]
Creatable/Deletable: derived (see Container Mos for details)
Possible Semantic Scopes: EPG, Infra, Fabric,
Semantic Scope Evaluation Rule: Subclasses
Monitoring Policy Source: Parent
Monitoring Flags: [IsObservable: true, HasStats: false, HasFaults: true, HasHealth: true, HasEventRules: false]

This object is generated and used only by internal processes.

Naming Rules

DN FORMAT:

Diagram

LEGEND

ConcreteModelA

admin-prop
implicit-prop
naming-readonly-prop
oper-prop

aaa

Definition

name : naming Name

explicit relation

Send documentation comments and corrections to apic-docfeed@csco.com | Copyright © 2013–2016 Cisco Systems, Inc. All rights reserved.

Cisco live!

BRKACI-1002

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

130

https://{{APIC}}/visore.html

APIC Object Store Browser (c) 2012-2013 Cisco Systems, Inc.

Filter

Class or DN:

Property: Op: Val1: Val2:

[Display URI of last query](#)

[Display last response](#)

Total objects shown: 6

fabricNode ?	
adSt	on
childAction	
delayedHeartbeat	no
dn	topology/pod-1/node-101 < > [1] [2]
extMngdBy	
fabricSt	active
id	101
lcOwn	local
modTs	2017-12-20T17:01:27.752+00:00
model	N9K-C93128TX
monPolDn	uni/fabric/monfab-default < > [1] [2]
name	Leaf-101
nameAlias	
role	leaf
serial	SAL1816QWEG
status	
uid	0
vendor	Cisco Systems, Inc
version	
fabricNode ?	
adSt	on
childAction	

https://{{APIC}}/visore.html

APIC Object Store Browser

(c) 2012-2013 Cisco Systems, Inc.

Class or DN: Property: Run Query

Display URI

Display last

Total objects

adSt

childAction

delayedHeartbeat

dn

extMngdBy

fabricSt

id

lcOwn

modTs

model

monPolDn

name

nameAlias

role

serial

status

uid

vendor

version

adSt

childAction

Class or DN: Property: Run Query

Filter

fvA

fvAAREpPrerequestorTask

fvAEPg

fvAEPgCont

fvAEPgTask

fvAEPDefTask

fvAREpBootStrap

fvAREpPDomDefDependencyResolver

fvAREpPrerequestorCons

fvAREpPrerequestorCont

fvAREpPUPd

fvARsToRemoteFCTask

fvARsToRemoteTask

fvAccGrpCont

fvAccP

fvAp

fvAppCtxRef

fvAppCtxRefCont

fvAppEpGCons

fvAppEpGPol

fvAppEpGRef

fvAssocBDDefCont

fvAttEntPDepl

fvAttEntityPathAtt

fvAttrDefCont

version

fabricNode

on

2

https://{{APIC}}/visore.html

APIC Object Store Browser

Filter

Class or DN: fvAp

Property: descr Op: contains Val1: Ciscolive Val2:

Run Query

Display URI of last query

Display last response

Display last: Display URI

Total objects: Display last

fvAp		2
childAction		
descr	Ciscolive	
dn	uni/tn-Ciscolive/ap-MyApp	
extMngdBy		
lcOwn	local	
modTs	2018-01-29T10:19:57.297+00:00	
monPolDn	uni/tn-common/monepg-default	
name	MyApp	
nameAlias		
ownerKey		
ownerTag		
prio	unspecified	
status		
uid	15374	

fabriNode

2

adSt on

adSt

childAction

adSt

childAction

delayedHea

dn

extMngdBy

fabriSt

id

lcOwn

modTs

model

monPolDn

name

nameAlias

role

serial

status

uid

vendor

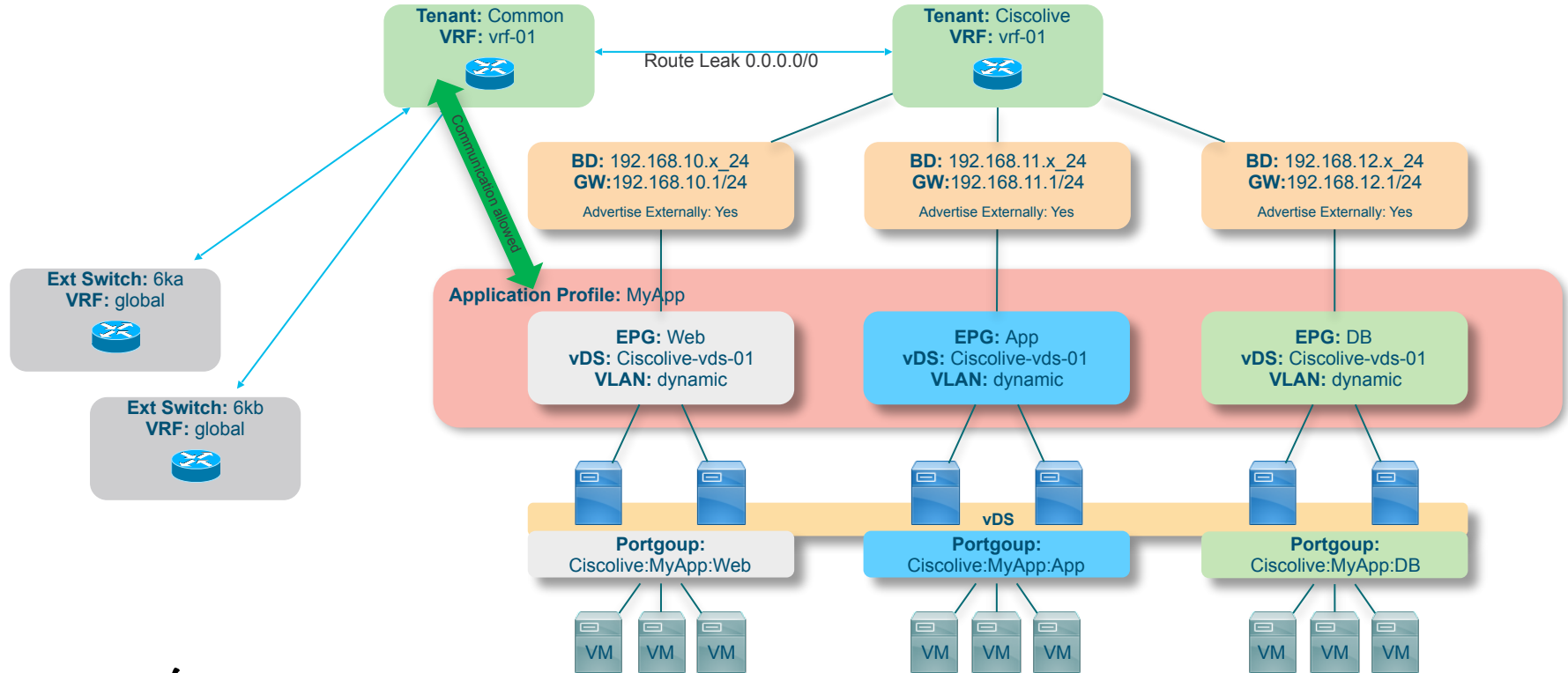
version

adSt

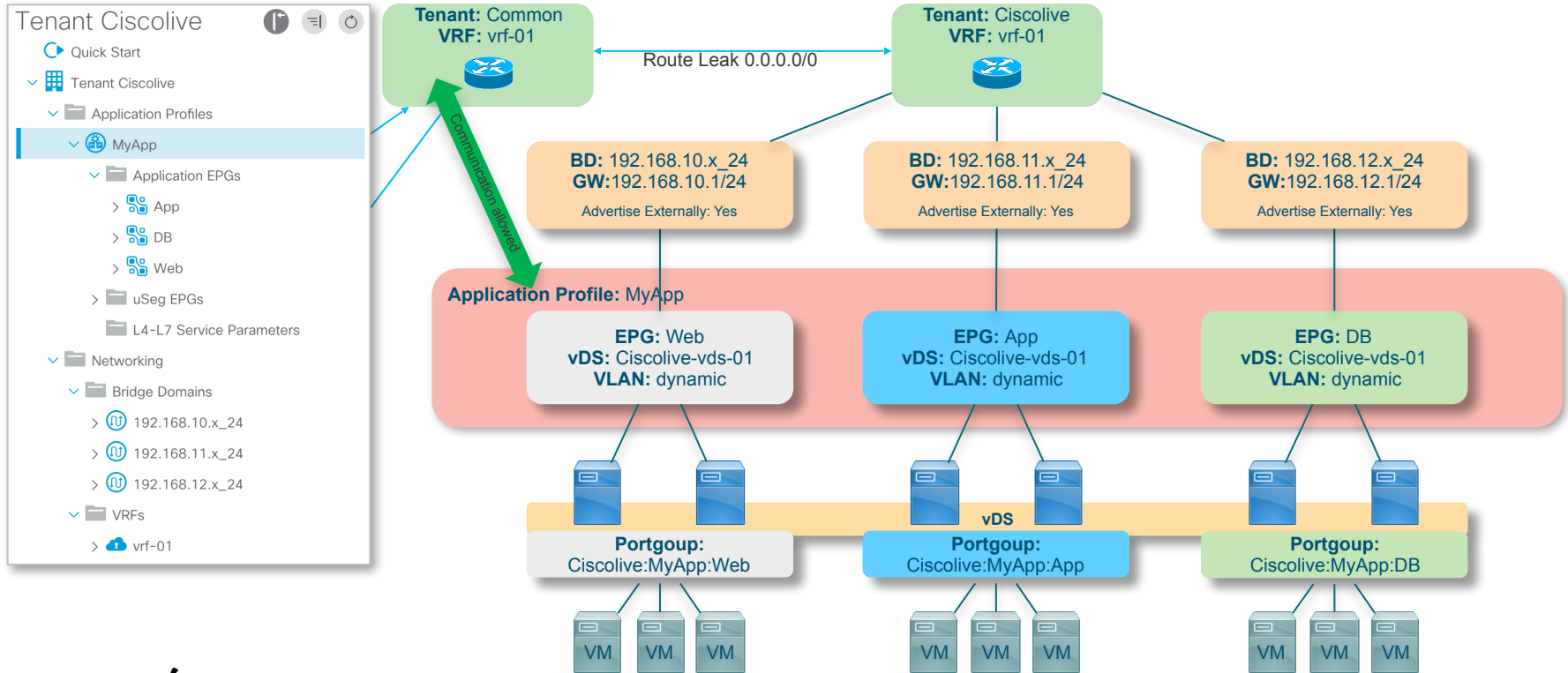
childAction

Using Postman

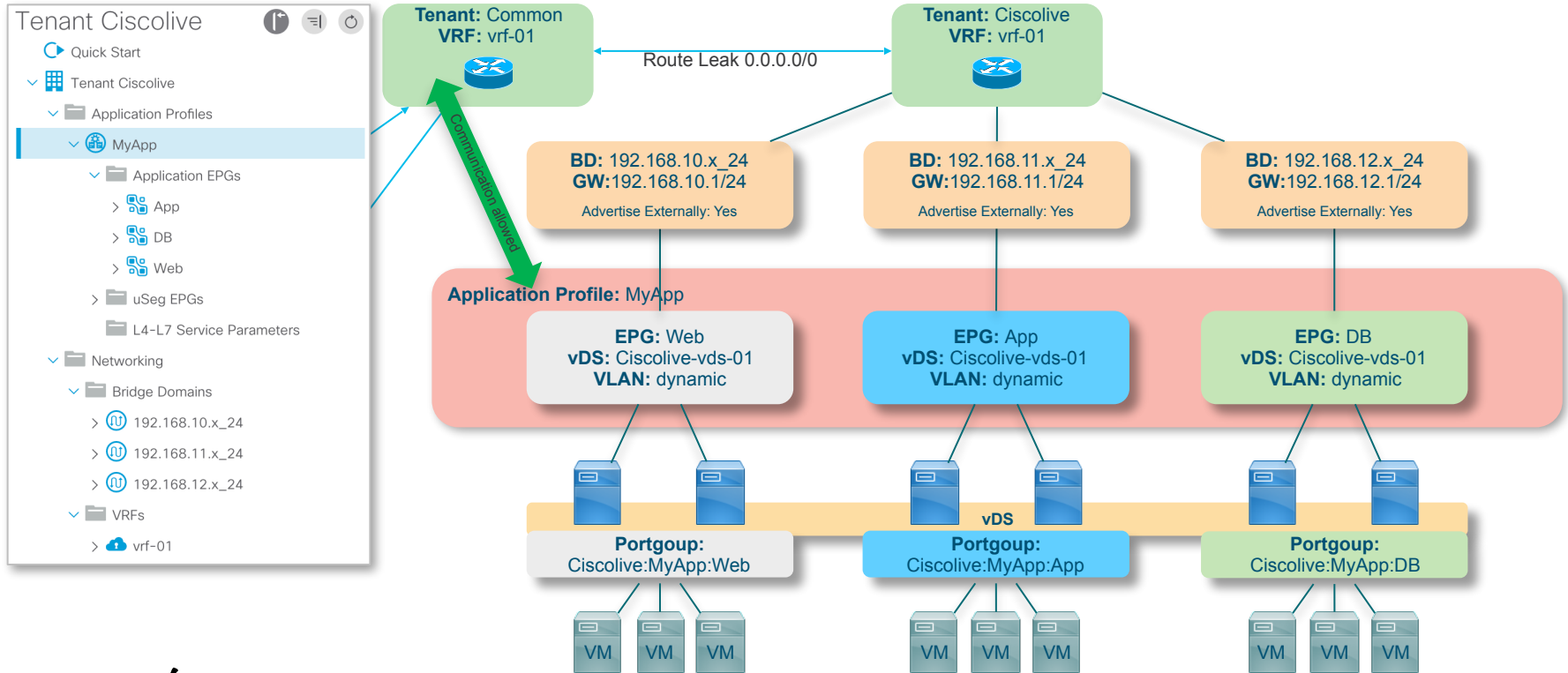
Step 1: Build your required object(s) in the GUI



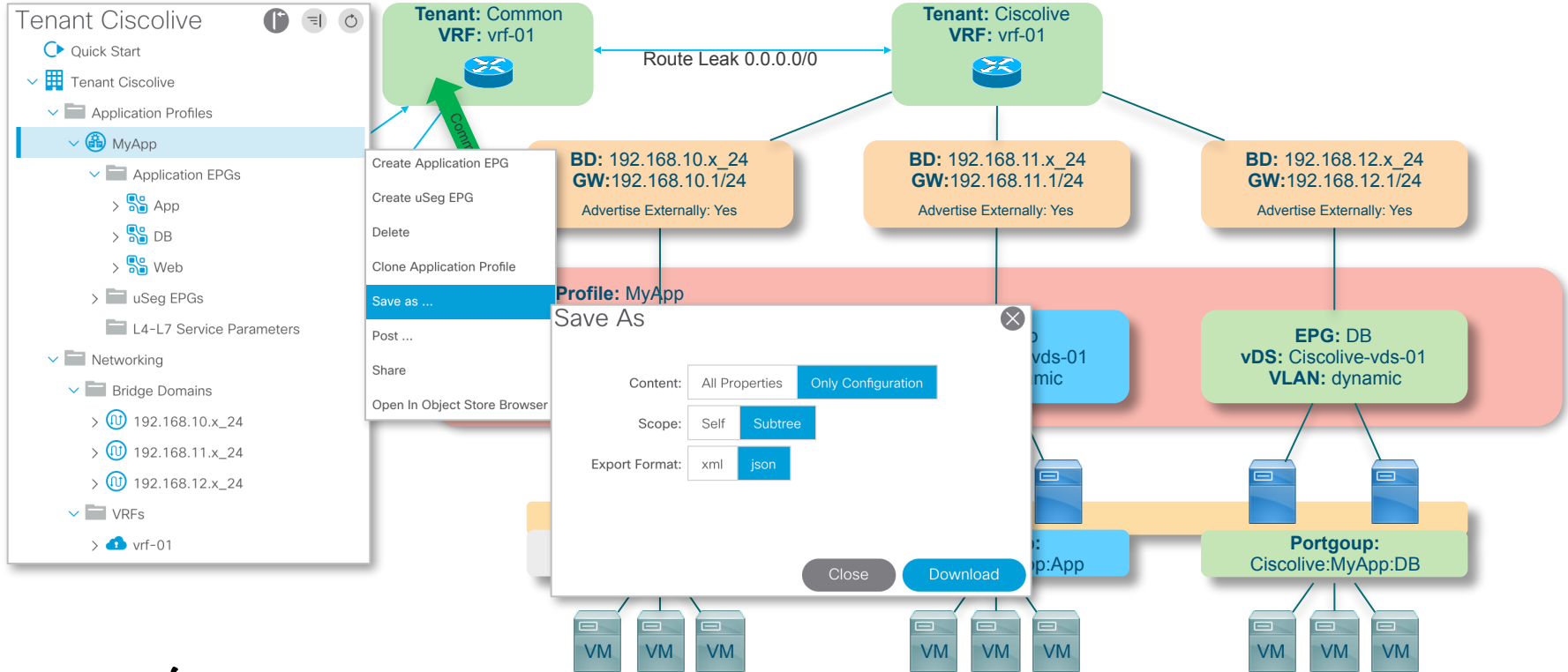
Step 1: Build your required object(s) in the GUI



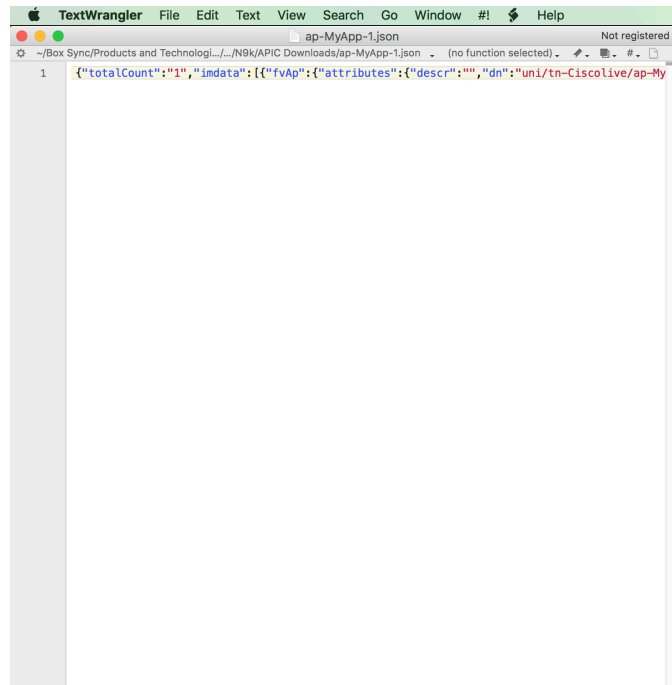
Step 2: Save your configuration



Step 2: Save your configuration

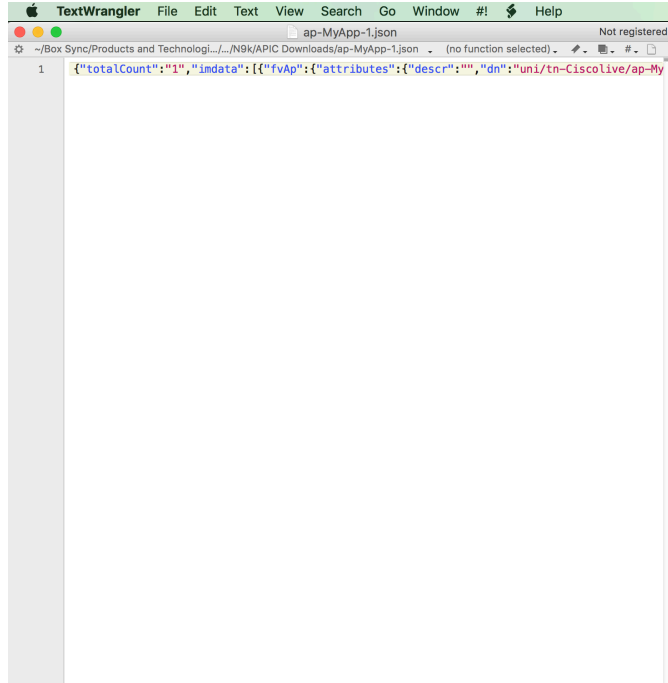
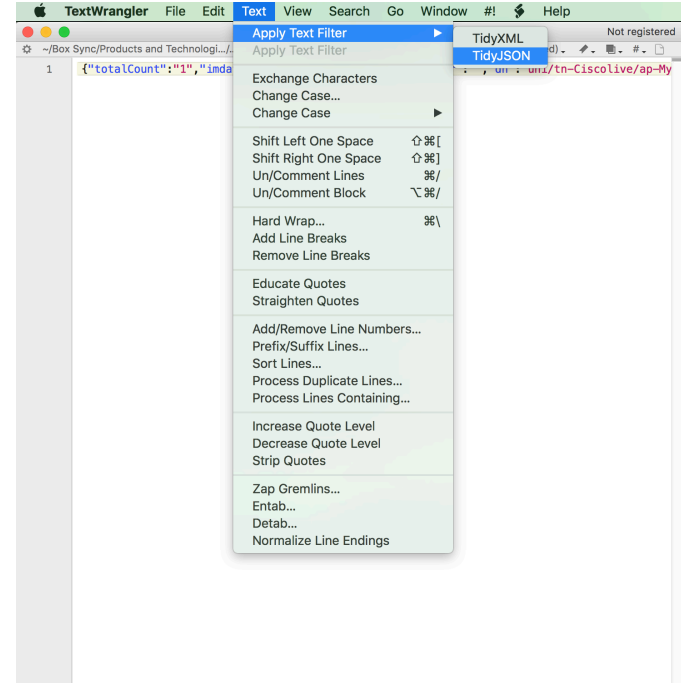


Step 3: Clean up your JSON



```
1 {\"totalCount\": \"1\", \"imdata\": [{\"fvAp\": {\"attributes\": {\"descr\": \"\", \"dn\": \"uni/tn-CiscoLive/ap-My\"}
```

Step 3: Clean up your JSON



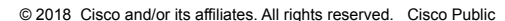
Cisco *live!*

BRKACI-1002

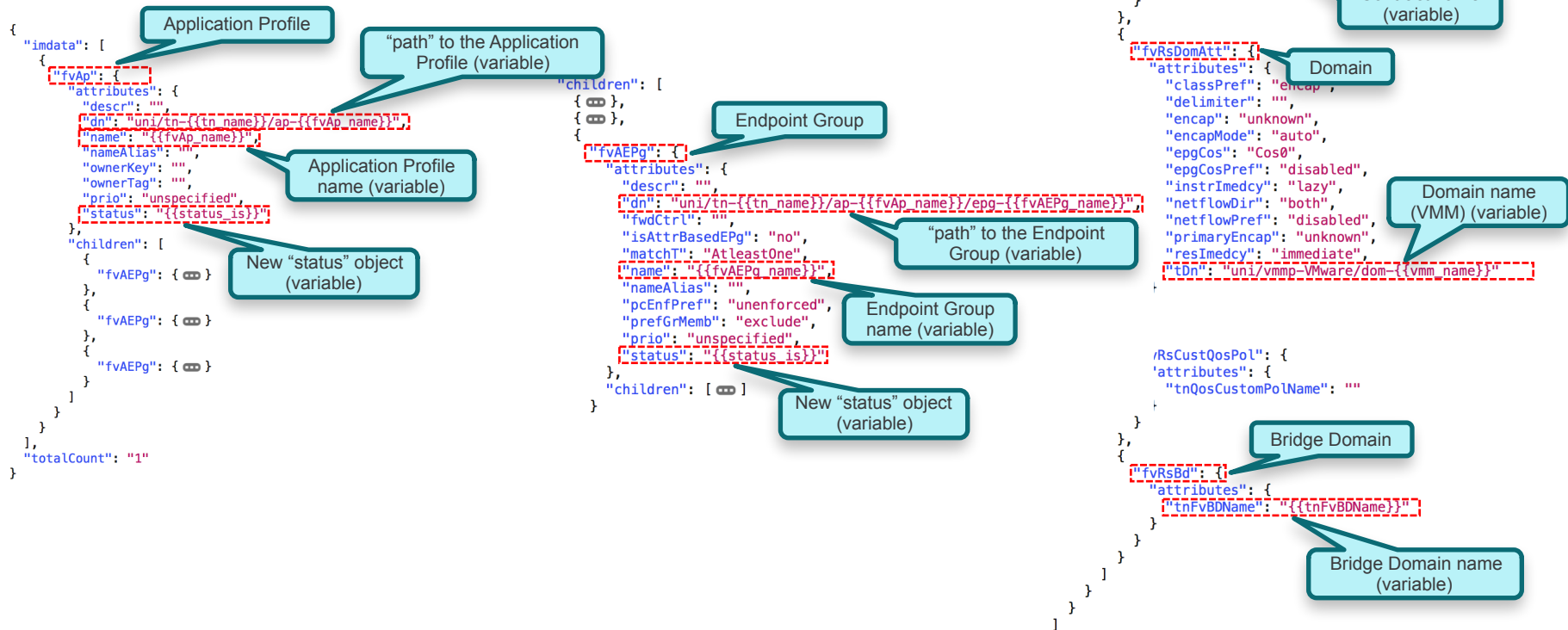
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

135

Cisco *live!*



Step 5: Select parameters to use as variables



Step 6: Create a variable file

```
[
  {
    "tn_name": "Ciscolive",
    "fvAp_name": "MyApp",
    "fvAEPg_name": "Web",
    "provided_contract": "shared_L3out",
    "tnFvBDName": "192.168.10.x_24",
    "vmm_name": "Ciscolive-vds-01",
    "status_is": "created"
  }
]
```

Option: created
Option: created,modified
Option: deleted

tn_name	fvAp_name	fvAEPg_name	provided_contract	tnFvBDName	vmm_name	status_is
Ciscolive	MyApp_1	Web	shared_L3out	192.168.10.x_24	Ciscolive-vds-01	created

Automating ACI with Postman/Runner

Example: Create Multiple Bridge Domains (Subnets)

Automating ACI with Postman/Runner

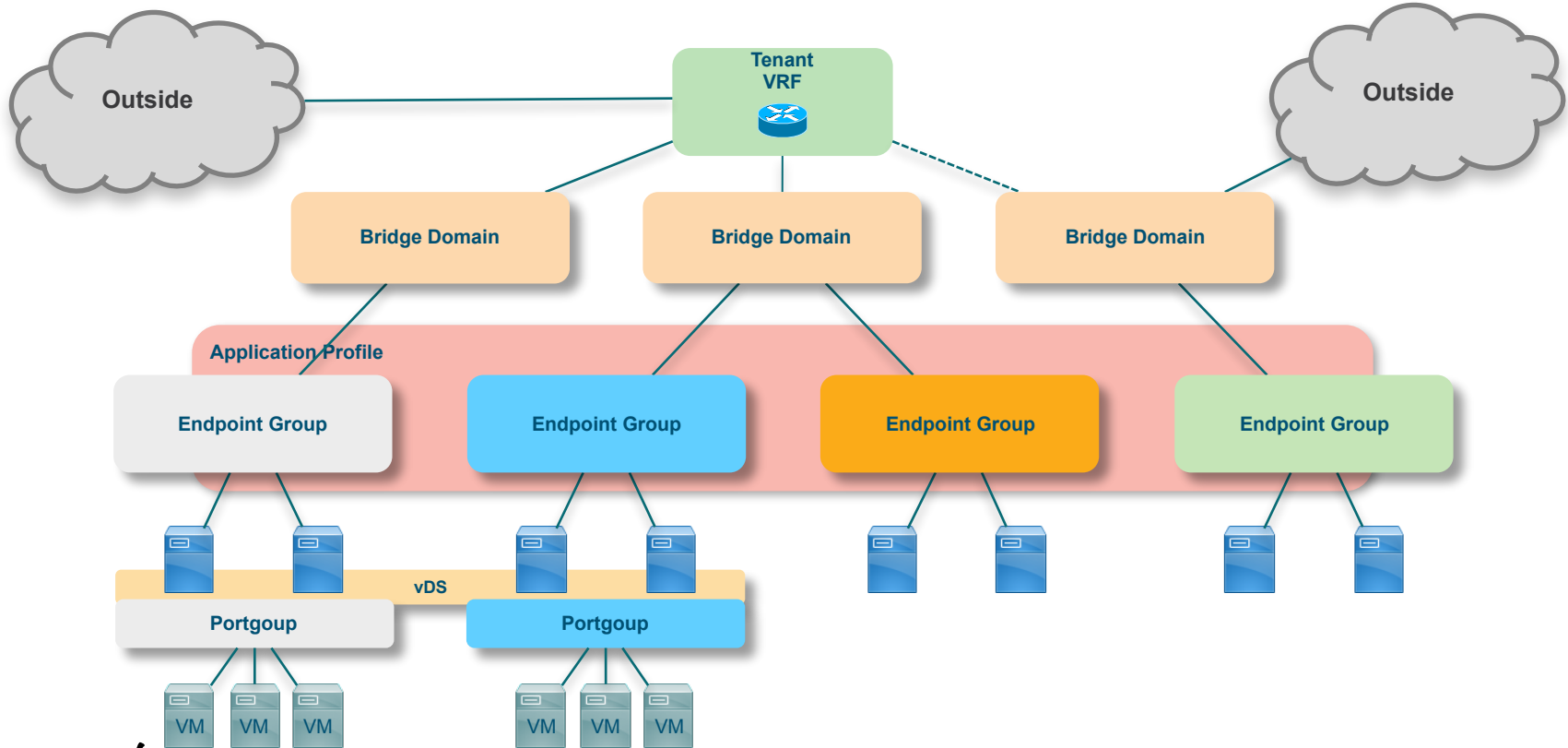
Example: Create Multiple Bridge Domains (Subnets)

Automating ACI with Postman/Runner

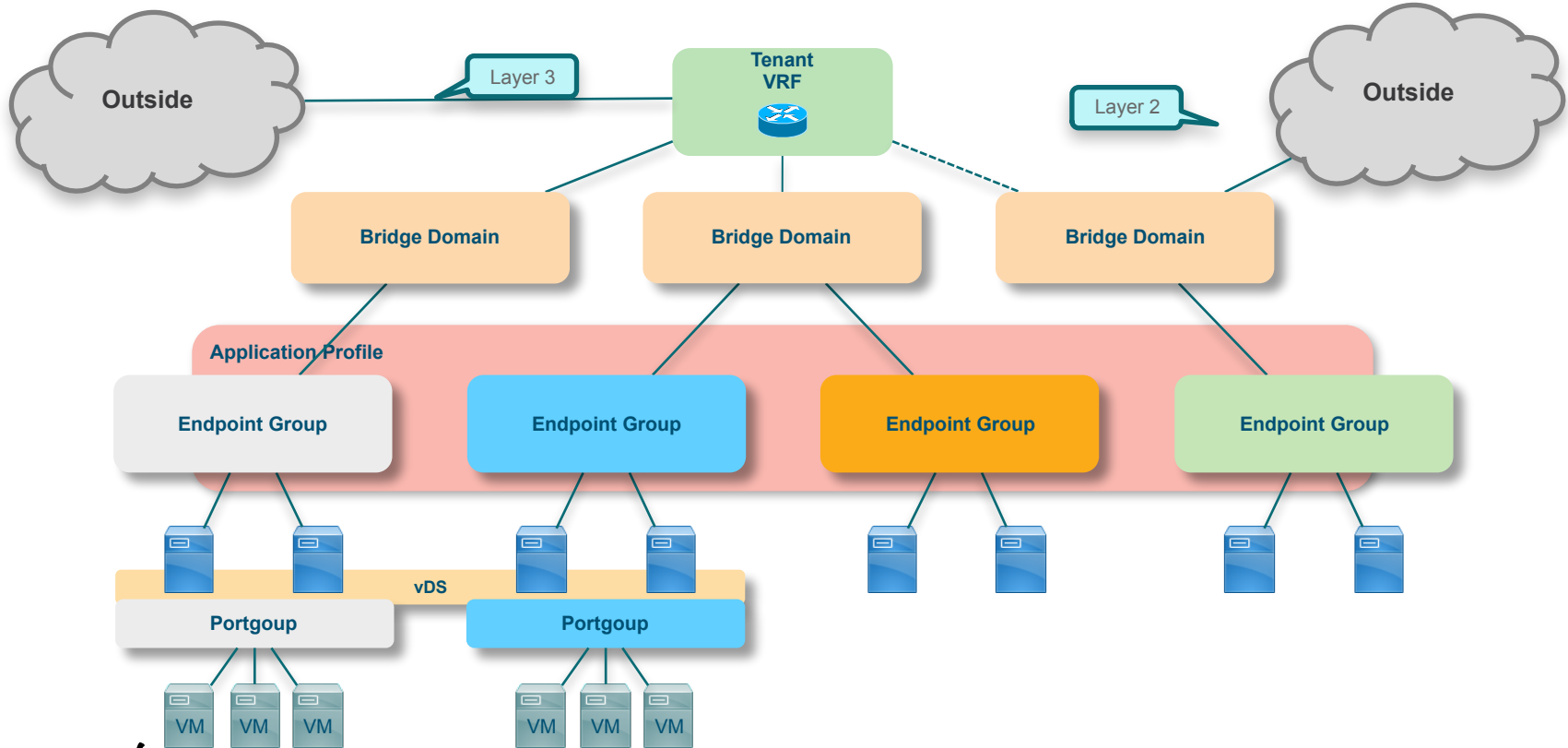
Example: Create Multiple Bridge Domains (Subnets)

Summary

Understand how managed objects are related

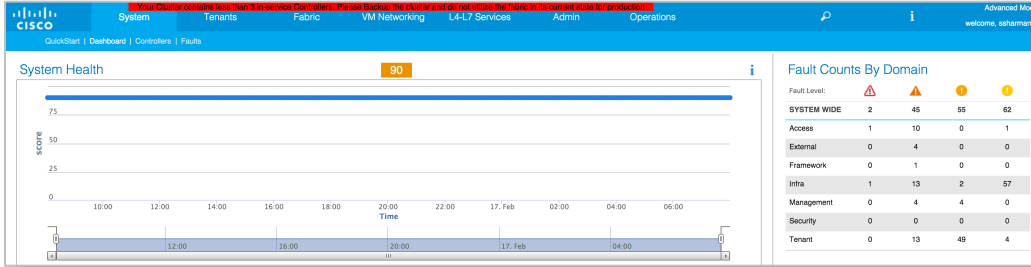


Understand how managed objects are related



Choose Your Management Method(s)

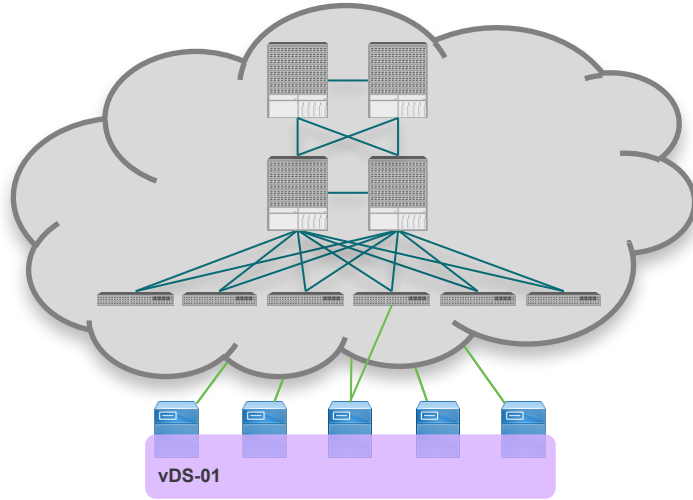
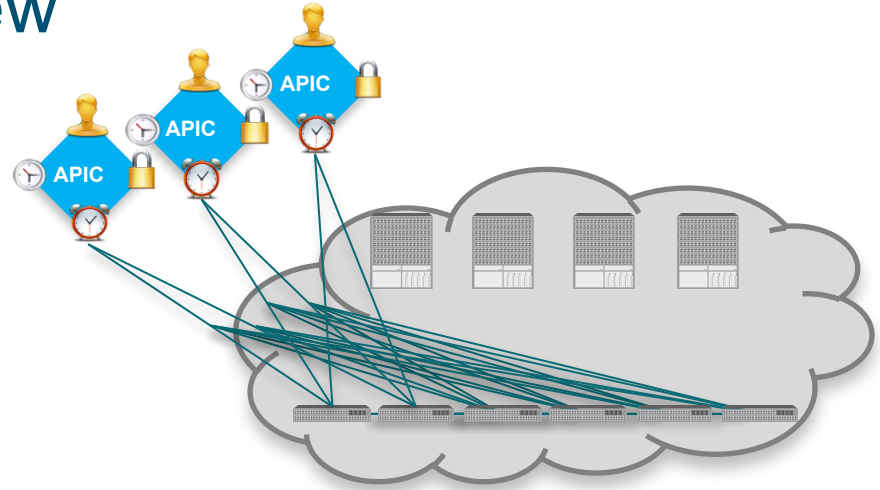
Choose Your Management Method(s)



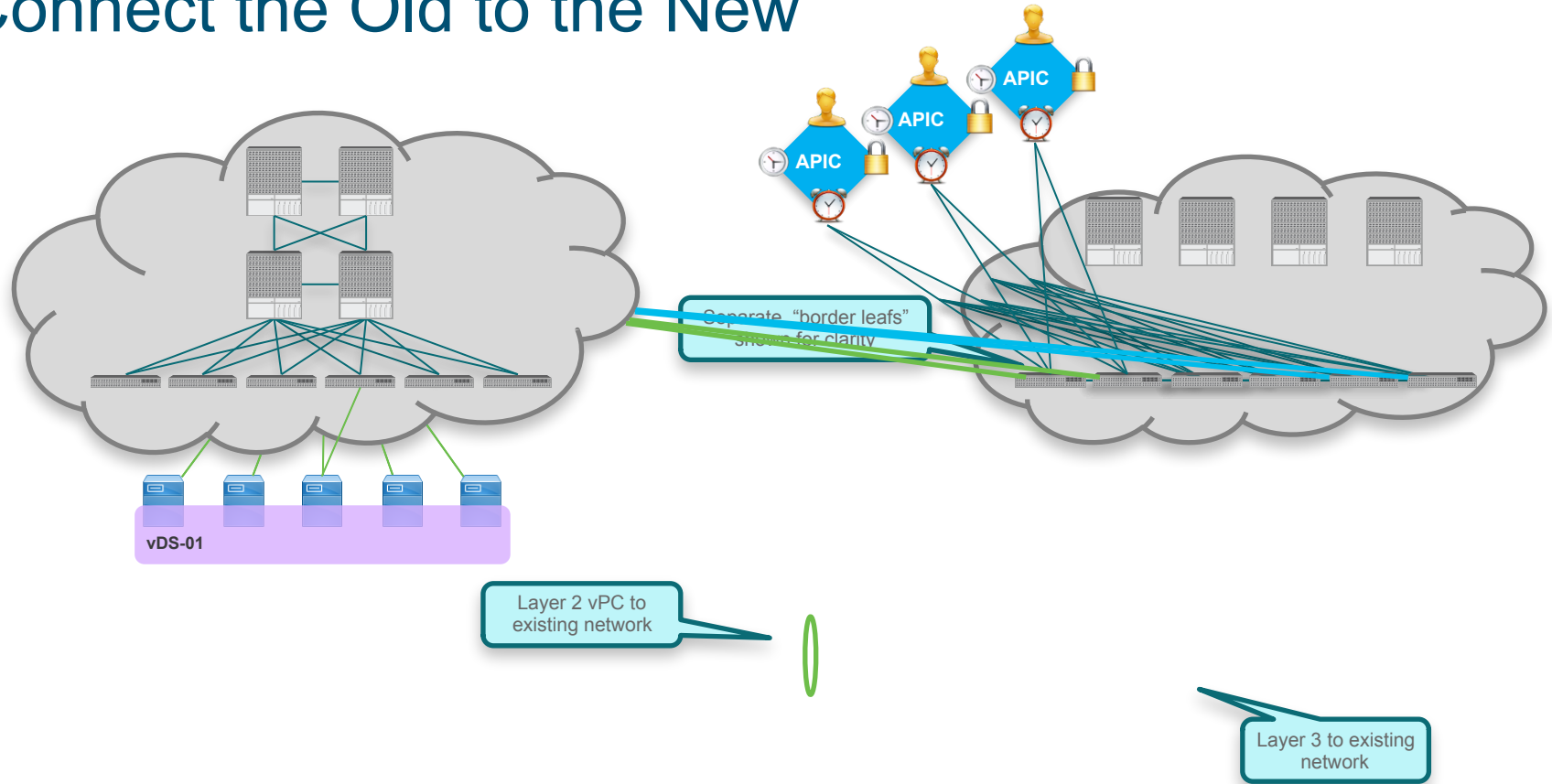
```
1. ssh
Application Policy Infrastructure Controller
admin@apic-01.uktme.cisco.com's password:
apic1#
apic1# configure terminal
apic1(config)# tenant my_new_tenant
apic1(config-tenant)#
```



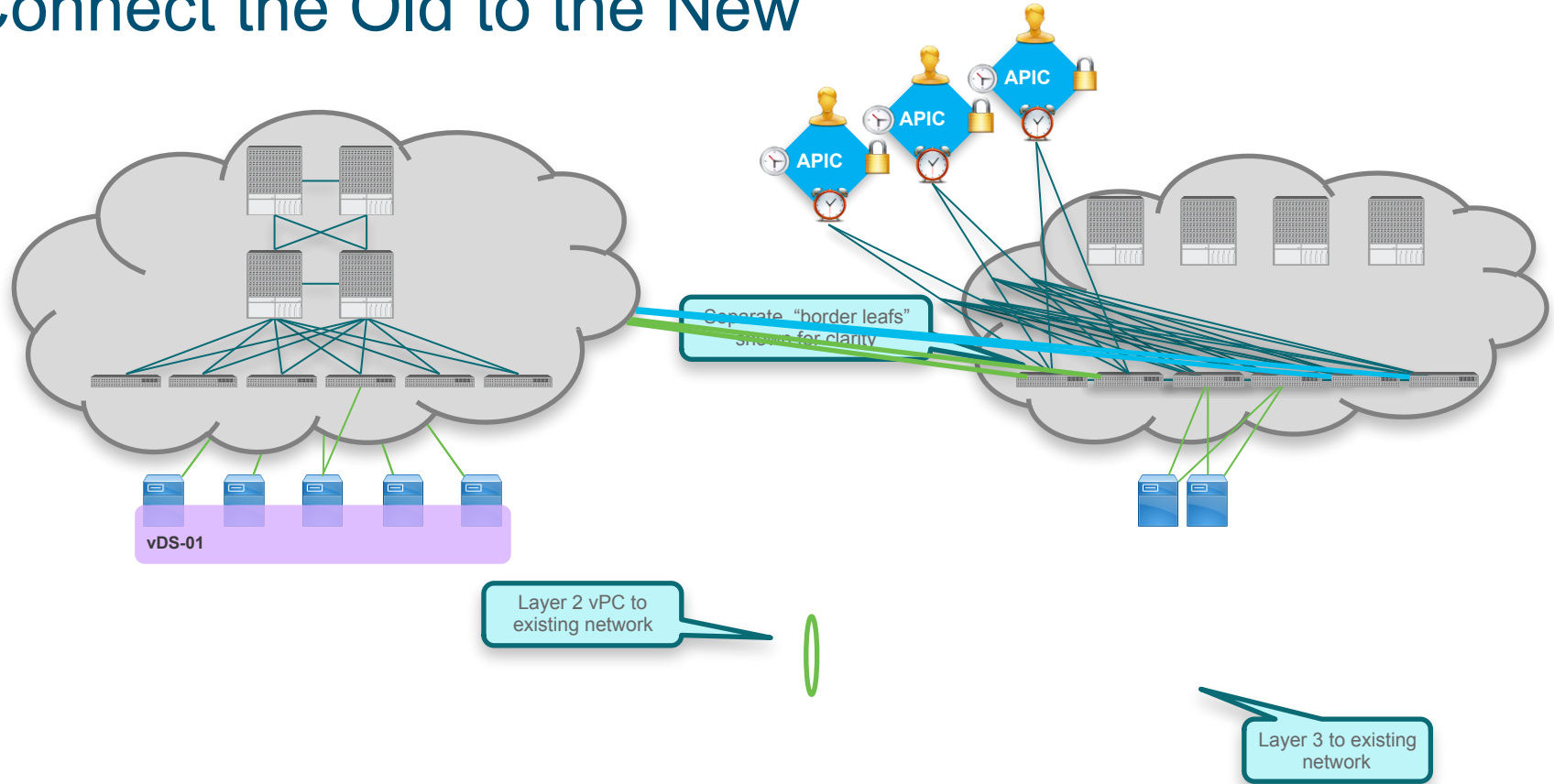
Connect the Old to the New



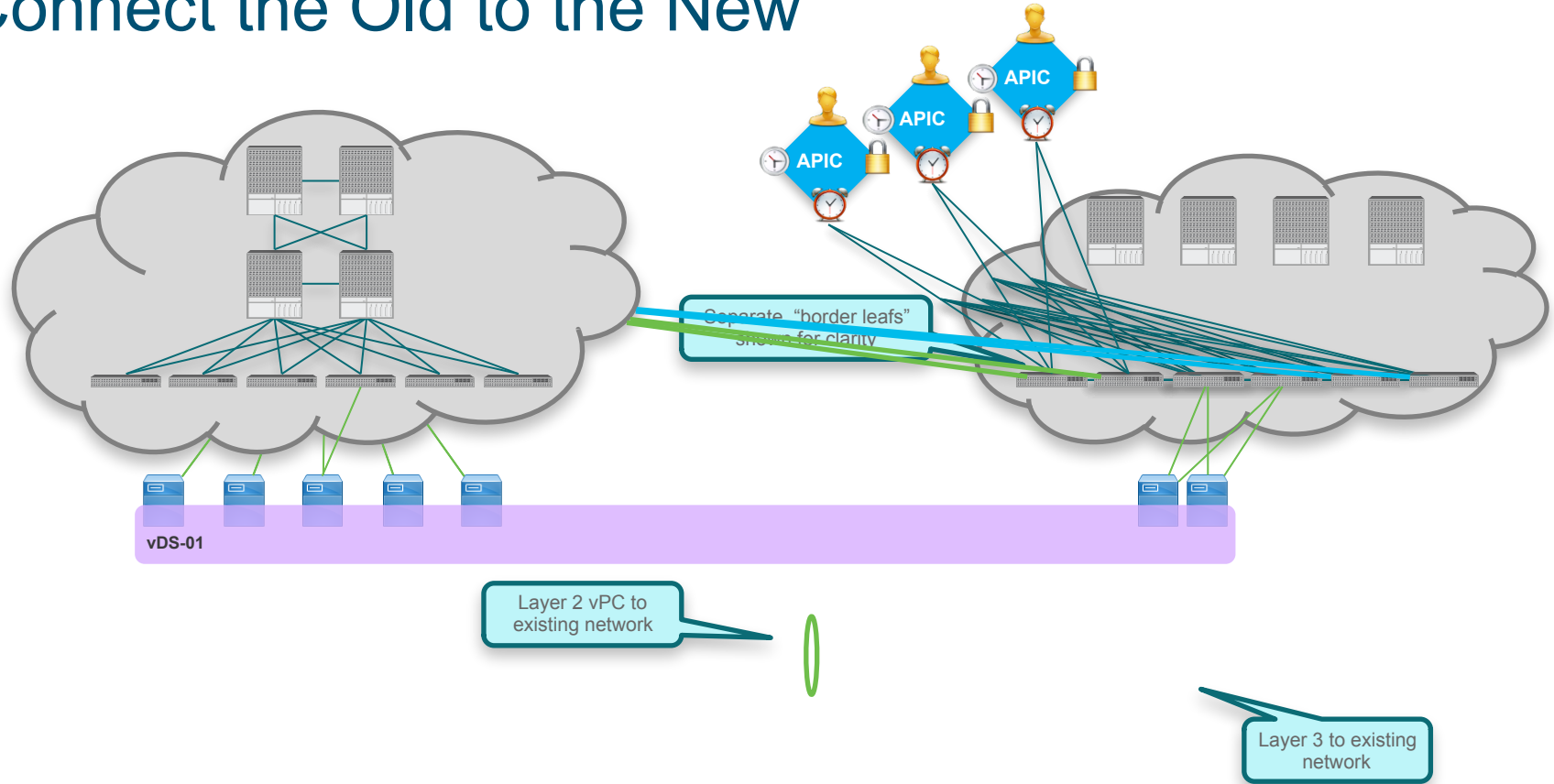
Connect the Old to the New



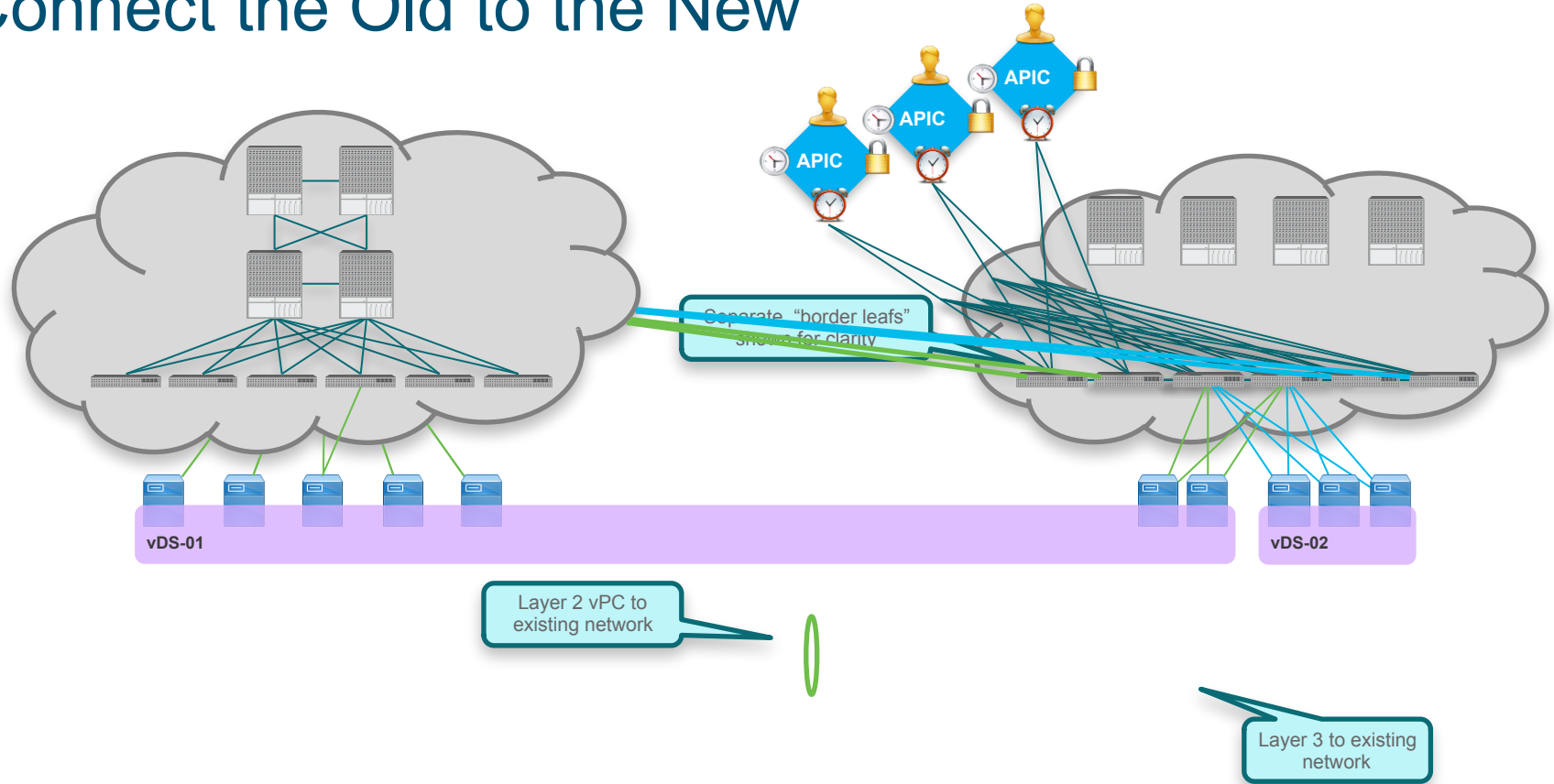
Connect the Old to the New



Connect the Old to the New



Connect the Old to the New



Q & A

Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Global.



Recommended Sessions

- ACI Layer 4-7 Integration – BRKACI-2016
- ACI Multisite Deployment – BRKACI-3502
- ACI Runs Everything – ILTDC-1702
- Cisco Container Networking in ACI mode – LABDC-1605
- How to setup and ACI fabric from scratch – BRKACI-2004
- Integration and Interoperation of Existing Nexus Networks – BRKACI-2001

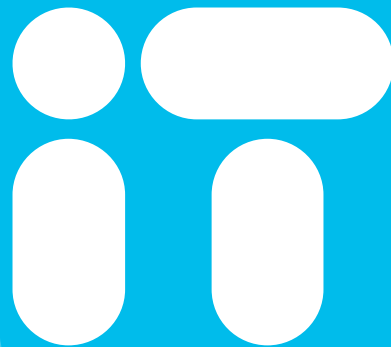




Thank you



You're



Cisco *live!*