



# ACI OVERVIEW

(DCACIO v4.0)

# Agenda

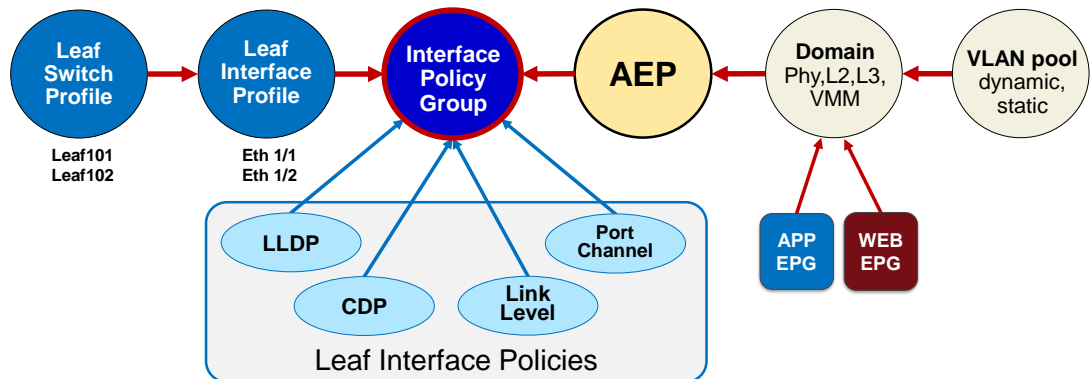
- Configuration Review
- Lab Topology
- Discovery Lab 1 - Tenants
- Discovery Lab 2 - VMM Integration
- Discovery Lab 3 - Layer-2 Out
- Discovery Lab 4 - Layer-3 Out
- Contract Deny (Taboo) Logging
- Lesson Exercise Create Taboo Contract



# Configuration Review

(DCACIO v4.0)

## ACI Access Policy Workflow



### Create Access Policies in preparation for tenant policy

- Set up interfaces, port-channels, vPC, LLDP / CDP, VLAN pools, etc..

© 2019 Cisco and/or its affiliates. All rights reserved.

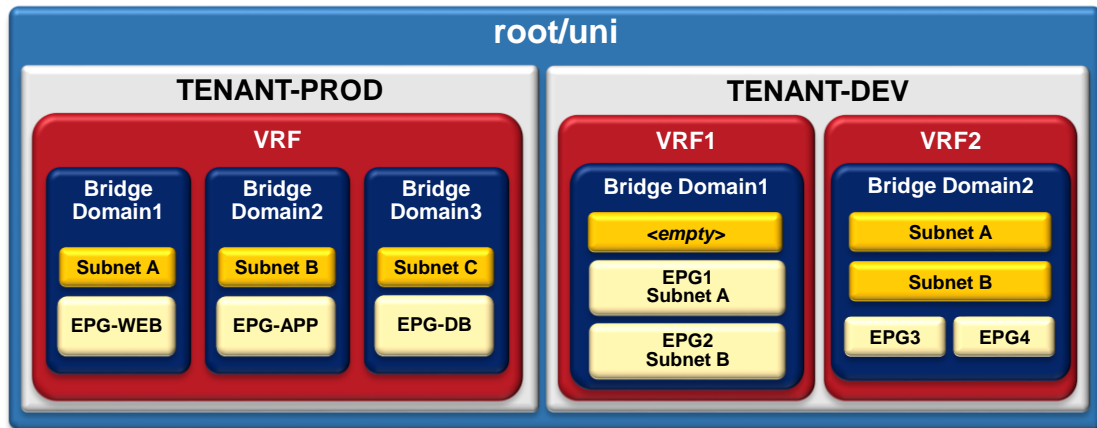
4

**Policy-based Configuration of Access Ports** – The infrastructure administrator configures ports in the fabric for speed, Link Aggregation Control Protocol (LACP) mode, LLDP and Cisco Discovery Protocol, etc.

In Cisco ACI, the configuration of physical ports is designed to be extremely simple for both small- and large-scale data centers. The underlying philosophy of Cisco ACI is that the infrastructure administrator categorizes servers based on their requirements: virtualized servers with hypervisor A connected at a Gigabit Ethernet, nonvirtualized servers running OS A connected at 10 Gigabit Ethernet, etc.

Cisco ACI provides a way to keep this level of abstraction when defining the connection of the servers to the fabric. The infrastructure administrator prepares a template of configurations for servers connected with active-standby teaming, PortChannels, and VPCs and bundles all the settings for the ports into a policy group. The administrator then creates objects that select interfaces of the fabric in ranges that share the same policy-group configuration.

## Logical Model Overview



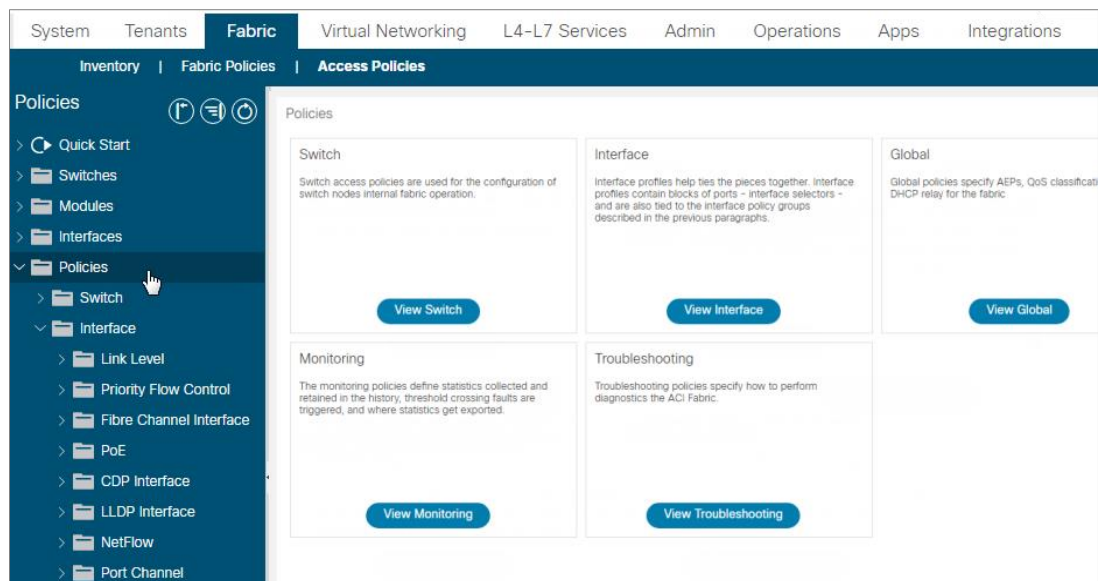
VRF and subnets are independent between tenants

© 2019 Cisco and/or its affiliates. All rights reserved.

5

**Logical Constructs** – The policy model manages the entire fabric, including the infrastructure, authentication, security, services, applications, and diagnostics. Logical constructs in the policy model define how the fabric meets the needs of any of the functions of the fabric. The diagram is an illustration of the logical model hierarchy. The top of the ACI logical model is represented by the 'root' (or universe). The next hierarchical separation is the Tenant. Each tenant will have at least one or more VRF. Forwarding constructs are separated from connectivity constructs – security & location separate them out.

# Configuring Fabric Access Policies



© 2019 Cisco and/or its affiliates. All rights reserved.

6

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 (FEXs). Access policies enable an administrator to configure port channels and virtual port channels, protocols such as LLDP, CDP, or LACP, and features such as monitoring or diagnostics. Sample XML policies for switch interfaces, port channels, virtual port channels, and change interface speeds are provided in *Cisco APIC Rest API Configuration Guide*.

**Note** While tenant network policies are configured separately from fabric access policies, tenant policies are not activated unless the underlying access policies they depend on are in place.

To apply a configuration across a potentially large number of switches, an administrator defines switch profiles that associate interface configurations in a single policy group. In this way, large numbers of interfaces across the fabric can be configured at once. Switch profiles can contain symmetric configurations for multiple switches or unique special purpose configurations. The following figure shows the process for configuring access to the ACI fabric.

# Configuring Interface Policy Groups

The screenshot displays the Cisco APIC GUI for configuring interface policy groups. The left sidebar shows a tree view with 'VPC Interface' and 'Leaf Breakout Port Group' selected. The main area displays two tables: 'Policy Groups - VPC Interface' and 'Policy Groups - Leaf Breakout Port Group'. A modal window titled 'Create Leaf Breakout Port Group' is open, showing fields for Name, Description, and Breakout Map.

**Policy Groups - VPC Interface**

Name	Link Aggregation Type	Link Level Policy	CDP Policy	Port Channel Policy	LLDP Policy	Attached Entity Profile
Shared-vPC-to-FI-A	vpc	10Gbps	CDP-enabl...	LACP-active	LLDP-disabled	Shared-UCS-AAEP
Shared-vPC-to-FI-B	vpc	10Gbps	CDP-enabl...	LACP-active	LLDP-disabled	Shared-UCS-AAEP

**Policy Groups - Leaf Breakout Port Group**

Name	Breakout Map
Breakout-10g-4x	10g-4x
Breakout-25g-4x	25g-4x

**Create Leaf Breakout Port Group**

Name: Breakout-25g-4x

Description: optional

Breakout Map: 10g-4x 25g-4x none

© 2019 Cisco and/or its affiliates. All rights reserved.

7

## Port Channel and Virtual Port Channel Access

Access policies enable an administrator to configure port channels and virtual port channels. Sample XML policies for switch interfaces, port channels, virtual port channels, and change interface speeds are provided in *Cisco APIC Rest API Configuration Guide*.

## Configuration of Dynamic Breakout Ports

Breakout cables are suitable for very short links and offer a cost effective way to connect within racks and across adjacent racks.

Breakout enables a 40 Gigabit (Gb) port to be split into four independent and logical 10Gb ports or a 100Gb port to be split into four independent and logical 25Gb ports. Before you configure breakout ports, connect a 40Gb port to four 10Gb ports or a 100Gb port to four 25Gb ports with one of the following cables:

Cisco QSFP-4SFP10G

Cisco QSFP-4SFP25G

The 40Gb to 10Gb dynamic breakout feature is supported on the access facing ports of the following switches:

N9K-C9332PQ

N9K-C93180LC-EX

N9K-C9336C-FX

The 100Gb to 25Gb breakout feature is supported on the access facing ports of the following switches: N9K-C93180LC-EX

N9K-C9336C-FX2

Observe the following guidelines and restrictions:

In general, breakouts and port profiles (ports changed from uplink to downlink) are not supported on the same port.

Fast Link Failover policies are not supported on the same port with the dynamic breakout feature.

Breakout subports can be used in the same way other port types in the policy model are used.

When a port is enabled for dynamic breakout, other policies (except monitoring policies) on the parent port are no longer valid.

When a port is enabled for dynamic breakout, other EPG deployments on the parent port are no longer valid.

A breakout sub-port can not be further broken out using a breakout policy group.



## Fabric Access Policies Configuration Example

Connected device	Interface Policy Grp	AEP	Domains	VLAN Pools	VLAN Range
UCS-FIA	UCSA-VPC	ESX-AEP	ESX-Dom	ESX-Vlans	
UCS-FIB	UCSB-VPC			Dynamic range:	1,3,49-51,88
ESX Host Server1	ESX-IPG			Static range:	90-94
ESX Host Server2					
HyperV Host Server1	HyperV-IPG	HyperV-AEP	HyperV-Dom	HyperV-Vlans	
HyperV Host Server2				Dynamic range:	100-110
				Static range:	150,161
LNx Server1	LNx-IPG	LNx-AEP	LNx-Phydom	LNx-Vlans	200
LNx Server2					
SLB1	SLB1-VPC	SLB-AEP	SLB-Phydom	SLB-Vlans	1000-1001
SLB2	SLB2-VPC				
5K-1 legacy	5K1-VPC	5K-AEP	5K-Phydom	5K-Vlans	300,315,322
5K-2 legacy	5K2-VPC				341,356
iSCSI SAN ctrl1	iSCSI1-PC	iSCSI-AEP	iSCSI-Phydom	iSCSI-Vlans	1002-1003
iSCSI SAN ctrl2	iSCSI2-PC				
7K-L3out	7K-L3	7K-L3-AEP	7K-L3-Dom	7K-L3out-Vlans	1010-1011
Firewall	FW-L3	FW-L3-AEP	FW-L3-Dom	FWL3-Vlan	1020-1021
WAN router	WAN-L3	WAN-L3-AEP	WAN-L3-Dom	WAN-L3out-Vlan	1030-1031
Multi-Pod IPN	MPOD-IPG	MPOD-AEP	MPOD-Dom	MPOD-Vlan4	4

© 2019 Cisco and/or its affiliates. All rights reserved.

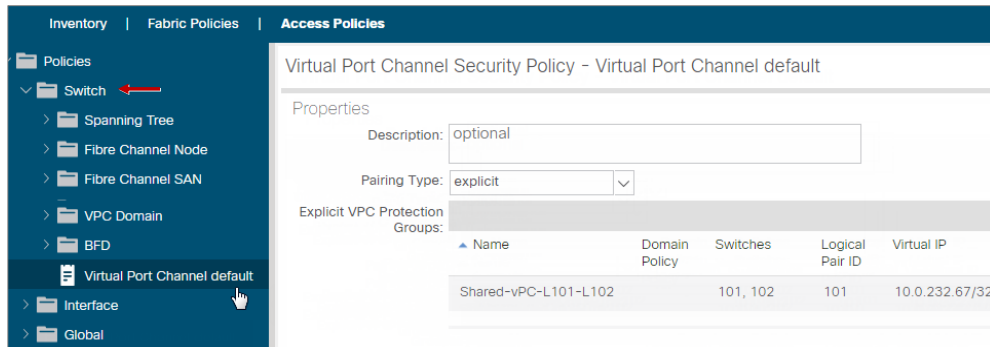
8

Best practice(s) for Fabric Access Policies are to separate distinct workloads from each other in the policy model. Although this can get very complex at scale it has been discovered that separating common workloads (eg Bare Metal, Hypervisor, L2, L3, SLB/FW) into separate constructs within the policy model greatly enhances the logical flow of provisioning components. It also lessens policy density and can protect from pre-mature policy deletions affecting downstream policy dependencies.

# VPC Explicit Protection Group

Divide leaf switches into Logical VPC pairs

- Leaves belong to only one VPC Domain



© 2019 Cisco and/or its affiliates. All rights reserved.

9

**Pre-provisioning VPC Logical Pairs for each Leaf pair** – As part of the initial configuration, you can divide the leaf switches into VPC pairs by creating a VPC Explicit protection group. You should pair the leaf switches in the same way as you paired them in the switch profiles: that is, you could create vpcdomain1, vpcdomain2, etc., where vpcdomain1 selects leaf switches 101 and 102, vpcdomain2 selects leaf switches 103 and 104, etc..

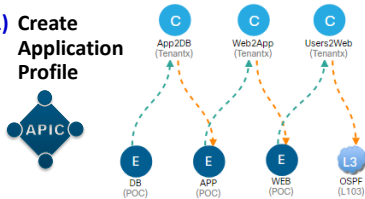
The infrastructure administrator is responsible for the following operations:

- Creating the VPC Explicit Protection Group
- Associating the correct AEP with the policy group

The tenant administrator is responsible for associating the EPG with the path that includes the VPC

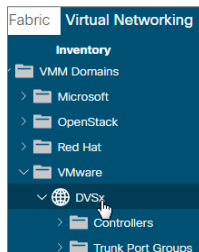
# VMM Integration Work Flow

## 1) Create Application Profile



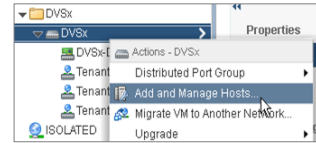
## 2) Create VMM Domain

- APIC creates DVS in vCenter



## 3) vCenter: add ESXi hosts to DVS

- Add and Manage Hosts

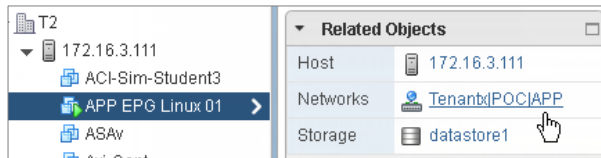


## 4) In Tenant associate EPGs to VMM Domain

- APIC creates Port Groups in vCenter



## 5) vCenter: assign port group to virtual machines – Edit Settings



© 2019 Cisco and/or its affiliates. All rights reserved.

10

Cisco ACI virtual machine (VM) networking supports hypervisors from multiple vendors. It provides the hypervisors programmable and automated access to high-performance scalable virtualized data center infrastructure.

Programmability and automation are critical features of scalable data center virtualization infrastructure. The Cisco ACI open REST API enables virtual machine integration with and orchestration of the policy model-based Cisco ACI fabric. Cisco ACI VM networking enables consistent enforcement of policies across both virtual and physical workloads managed by hypervisors from multiple vendors. Attachable entity profiles easily enable VM mobility and placement of workloads anywhere in the Cisco ACI fabric. The Cisco Application Policy Infrastructure Controller (APIC) provides centralized troubleshooting, application health score, and virtualization monitoring. Cisco ACI multi-hypervisor VM automation reduces or eliminates manual configuration and manual errors. This enables virtualized data centers to support large numbers of VMs reliably and cost effectively.

## EPG Policy Resolution and Deployment Immediacy

Whenever an EPG associates to a VMM domain, the administrator can choose the resolution and deployment preferences to specify when a policy should be pushed into leaf switches.

### Resolution Immediacy

**Pre-provision**—Specifies that a policy (for example, VLAN, VXLAN binding, contracts, or filters) is downloaded to a leaf switch even before a VM controller is attached to the virtual switch (for example, VMware VDS). This pre-provisions the configuration on the switch.

This helps the situation where management traffic for hypervisors/VM controllers are also using the virtual switch associated to APIC VMM domain (VMM switch).

Deploying a VMM policy such as VLAN on ACI leaf switch requires APIC to collect CDP/LLDP information from both hypervisors via VM controller and ACI leaf switch.

However if VM Controller is supposed to use the same VMM policy (VMM switch) to communicate with its hypervisors or even APIC, the CDP/LLDP information for hypervisors can never be collected because the policy required for VM controller/hypervisor management traffic is not deployed yet.

When using pre-provision immediacy, policy is downloaded to ACI leaf switch regardless of CDP/LLDP neighborship. Even without a hypervisor host connected to the VMM switch.

**Immediate**—Specifies that EPG policies (including contracts and filters) are downloaded to the associated leaf switch software upon ESXi host attachment to a DVS. LLDP or OpFlex permissions are used to resolve the VM controller to leaf node attachments.

The policy will be downloaded to leaf when you add host to the VMM switch. CDP/LLDP neighborship from host to leaf is required.

**On Demand**—Specifies that a policy (for example, VLAN, VXLAN bindings, contracts, or filters) is pushed to the leaf node only when an ESXi host is attached to a DVS and a VM is placed in the port group (EPG).

The policy will be downloaded to leaf when host is added to VMM switch and virtual machine needs to be placed into port group (EPG). CDP/LLDP neighborship from host to leaf is required.

With both immediate and on demand, if host and leaf lose LLDP/CDP neighborship the policies are removed.

### Deployment Immediacy

Once the policies are downloaded to the leaf software, deployment immediacy can specify when the policy is pushed into the hardware policy content-addressable memory (CAM).

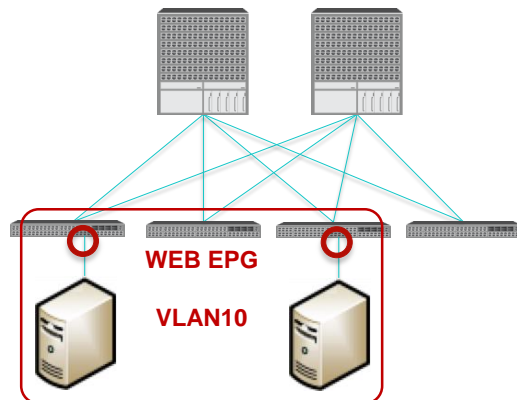
**Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as the policy is downloaded in the leaf software.

**On demand**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

## Layer 2 – Extend EPG out of ACI Fabric

Also known as the **baremetal** or **Static EPG Mapping** method

- VLANs used between a server and a leaf have local significance (per port or per switch)
- Manually assign interface to a VLAN which in turn is mapped to an EPG
- **Extends an EPG beyond ACI fabric**
  - No contract within EPG
- BPDU is always flooded within EPG



© 2019 Cisco and/or its affiliates. All rights reserved.

11

**Extend the EPG Out of the ACI Fabric** – The user can extend an EPG beyond an ACI leaf by statically assigning a leaf port (along with a VLAN ID) to an EPG. After doing so, all the traffic received on this leaf port with the configured VLAN ID will be mapped to the EPG and the configured policy for this EPG will be enforced. The endpoints need not be directly connected to the ACI leaf port. They can be behind a layer 2 network as long as the VLAN associated with the EPG is enabled within the layer 2 network that connects the remote endpoint to the ACI fabric.

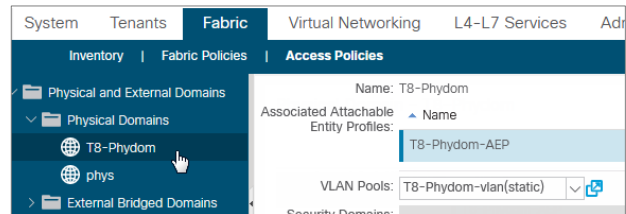
**Use of VLANs as a Segmentation Mechanism** – In Cisco ACI the VLANs used between a server and a leaf have local significance and they are used exclusively to segment traffic coming from the servers. Cisco ACI has been designed so that when using virtualized workloads you don't have to enter VLAN numbers manually per each port-group. Whenever possible one should leverage the dynamic negotiation of VLANs between the virtualized server and the Cisco ACI fabric.

The illustration shows how a virtualized server tags traffic with a VLAN (or a VxLAN) and sends it to the leaf. The tenant configuration defines the VLAN or VxLAN that belongs to the EPG.

## Extend EPG Work Flow

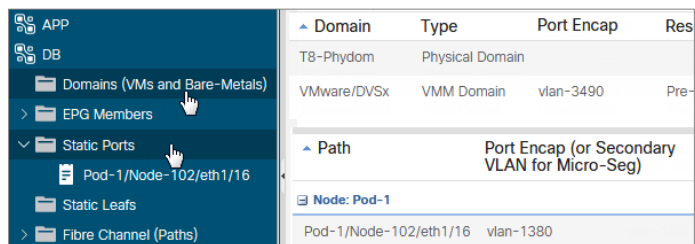
### Create Fabric Access Policies

- Create Physical Domain & VLAN pool
- Map Domain to AEP
- Create Leaf Interface Policy Group and associate to AEP and Interface Selector in Leaf Profile



### Tenant configuration

- Associate EPG with Physical Domain
- Assign Static Port(s) & VLAN encap to EPG



© 2019 Cisco and/or its affiliates. All rights reserved.

12

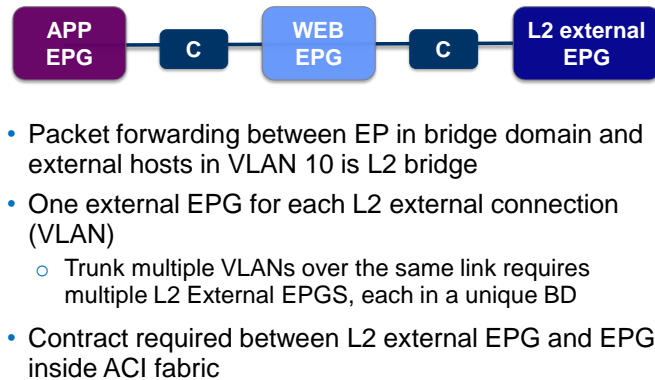
### Extend the EPG Out of the ACI Fabric

The user can extend an EPG beyond an ACI leaf by statically assigning a leaf port (along with a VLAN ID) to an EPG. After doing so, all the traffic received on this leaf port with the configured VLAN ID will be mapped to the EPG and the configured policy for this EPG will be enforced. The endpoints need not be directly connected to the ACI leaf port. They can be behind a layer 2 network as long as the VLAN associated with the EPG is enabled within the layer 2 network that connects the remote endpoint to the ACI fabric.

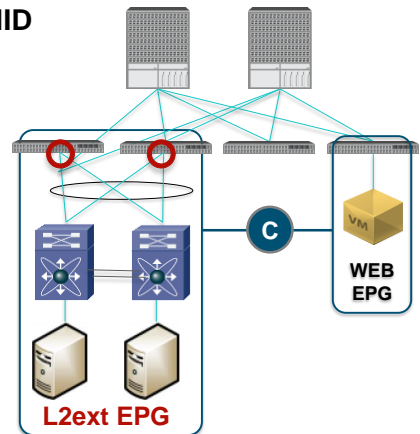
- To statically assign port to an EPG, go to menu Tenants-Application Profiles-EPG-Static Binding (Paths).
- Click the Action menu on the right side to start to assign port to an EPG. The Figure provides an example that assigns interface eth1/10 from the leaf node 103 along with VLAN 1320 to EPG DB.

# Extend L2 Bridge Domain

## Extend bridge domain to an external VLAN or VNID



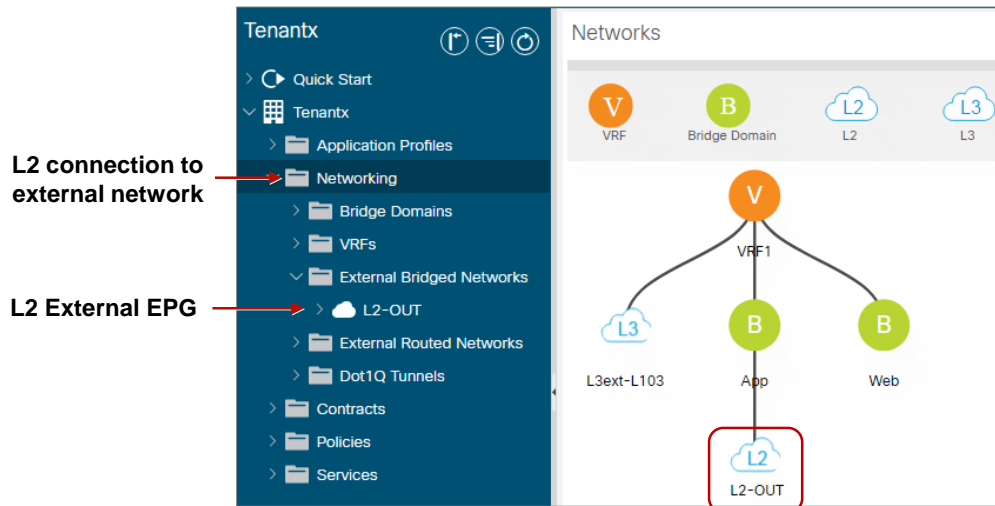
- Packet forwarding between EP in bridge domain and external hosts in VLAN 10 is L2 bridge
- One external EPG for each L2 external connection (VLAN)
  - Trunk multiple VLANs over the same link requires multiple L2 External EPGs, each in a unique BD
- Contract required between L2 external EPG and EPG inside ACI fabric



Since every EPG lives under a Bridge Domain, the second option is to extend the Bridge Domain itself outside ACI; not the EPG. This requires creating an EPG for the L2 external network. In the example, Bridge Domain 'BD-1' is extended to the layer-2 switch with VLAN tag 500. A contract required between the external EPG and the internal EPG (WEB EPG in the illustration). In the example, this effectively is taking VLAN 500 in Leaf 6 and bridging it to Leaf-4 with policy enforcement.

If there is a requirement for trunking multiple VLANs over the link, you must create multiple L2 External EPGs and associate each one to a unique Bridge Domain for each VLAN.

## L2 External Connection in Tenant Networking View



Here we view any configured External EPGs. All this is under just one Tenant – Tenant2 in the diagram.

Navigation within the GUI:

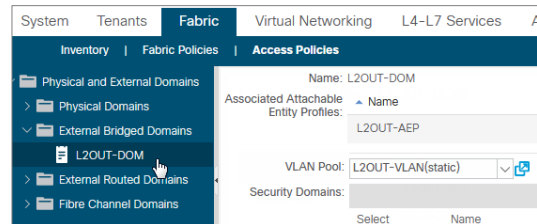
- Select respective Tenant > expand Networking
- For L2, expand External Bridged Networks > then expand L2Out
- Private Networks is where you configure the L3



## L2 Work Flow: Extend BD (Legacy NW Connection)

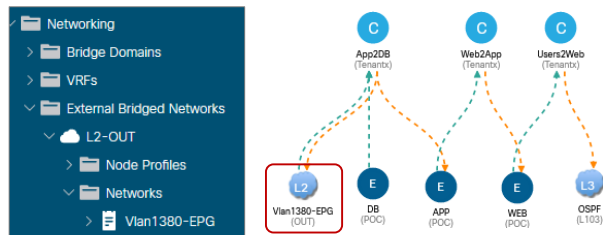
### Create Fabric Access Policies

- Create Layer2 Bridged Domain & VLAN pool
- Map Domain to AEP
- Create Leaf Interface Policy Group and associate to AEP and Interface Selector in Leaf Profile



### Tenant configuration tasks

- Create a Bridged Outside (L2Out)
- Assign port(s) & VLAN encap to Bridged Outside
- Create an External L2EPG (Networks)
- Associate L2EPG with External Bridged Domain
- Create/Assign Contract for External L2EPG



© 2019 Cisco and/or its affiliates. All rights reserved.

15

### Extend the Bridge Domain Out of the ACI Fabric

Another way to extend the layer 2 domain beyond the ACI fabric is to create layer 2 outside connections. On the APIC GUI it is under menu Tenant > Networking > External Bridged Networks (Figure 53). A layer 2 outside connection is associated with a bridge domain and it is designed to extend the whole bridge domain (not an individual EPG under bridge domain) to the outside network.

In Figure 53, we create a layer 2 outside connection for a bridge domain called “bd1”. There are two EPGs (EPG APP and EPG WEB) under this bridge domain. The layer 2 outside connection extends the bridge domain to the Cisco Nexus switch and the hosts attached to the switch. The layer 2 outside connection configuration specifies that the bridge domain “bd1” is extended to the network connected to the border leaf on the far right. All the traffic for the “bd1” carries the VLAN tag 500 when it leaves the ACI fabric. For the traffic entering the ACI fabric, the border leaf assigns all traffic with VLAN 500 to an external EPG. The traffic flows between the external EPG and other EPGs in the ACI fabric are enforced with the configured contract. The bottom portion of Figure 53 illustrates the policy model with the layer 2 outside connection. Although the diagram only shows the contract between an external EPG with one inside EPG, there is no limitation about how many inside EPGs can talk to an

external EPG. It is all driven by the policy configuration.

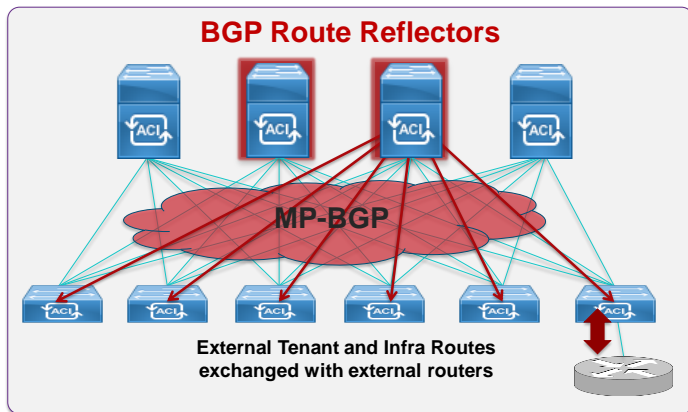
As shown in Figure 53, the layer 2 outside connection for a given bridge domain effectively extends the bridge domain beyond the ACI fabric. The endpoints in the outside network share all the characters and configurations for the bridge domain, such as the IP subnet assigned to the bridge domain and the default gateway. The endpoints in the outside network are also in the same flooding domain as the rest of the endpoints under the same bridge domain. Obviously, the ACI fabric can't control the flooding behavior for the outside network. In other words, even when a user disables the flooding of some unknown unicast under the bridge domain (which has been extended to the outside layer 2 network), the flooding of the unknown unicast still occurs on the outside network.

The ACI border leaf that connects to the outside layer 2 network learns the endpoint information. The learning behavior is the same as one explained in the section, "Extend EPG Out of the ACI Fabric."

On the surface, the layer 2 outside connection is similar to the way of extending an EPG by statically assigning a port plus VLAN tagging to an EPG. There are big differences between these two. Figure 52 explains the difference between these two methods by looking at the placement of outside endpoints and the policy model.

## ACI Layer 3 – Route Distribution

- Fabric leverages **MP-BGP** for distributing external routes to leaf switches
- BGP Peering between **Route Reflectors** and leaves located in spine
- Route Redistribution between internal BGP and 'outside' occurs on **border leaves**



© 2019 Cisco and/or its affiliates. All rights reserved.

16

All of Spines can be **Route Reflectors**. A route reflector (RR) is a network routing component; an alternative to the logical full-mesh requirement of internal BGP (IBGP). Route reflectors act as a focal point for IBGP sessions. The purpose of the RR is concentration. Multiple BGP routers can peer with a central point, the RR, rather than peer with every other router in a full mesh. All the other IBGP routers become route reflector clients.

In ACI, all Leaves will establish a neighbor (client) relationship with the route reflector(s). As each Spine can be configured as a route reflector, configure at least two for fault-tolerance.

**Multiprotocol BGP (MP-BGP)** is an extension to BGP that enables BGP to carry routing information for multiple network layers and address families. MP-BGP can carry the unicast routes used for multicast routing separately from the routes used for unicast IP forwarding. Even though the external router may be iBGP, the ACI fabric is still doing a re-distribution internal from the Leaf into MP-BGP. The Router could be OSPF or static route; supported at FCS.

**Ethernet VPN (EVPN)** allows Multiprotocol Label Switching (MPLS) networks to provide multipoint Layer 2 VPN (L2VPN) services. In EVPN, the customer MAC addresses are learned in the data plane over links connecting customer devices (CE) to the provider edge (PE) devices. The MAC addresses are then distributed over the

Multiprotocol Label Switching (MPLS) core network using Border Gateway Protocol (BGP) with an MPLS label identifying the service instance. A single MPLS label per EVPN instance is sufficient as long as the receiving PE device performs a MAC lookup in the disposition path. Receiving PE devices inject these routable MAC addresses into their Layer 2 routing information base (RIB) and forwarding information base (FIB) along with their associated adjacencies.

EVPN defines a BGP Network Layer Reachability Information (NLRI) that advertises different route types and route attributes. The EVPN NLRI is carried in BGP using BGP multiprotocol extensions with an Address Family Identifier (AFI) and a Subsequent Address Family Identifier (SAFI). BGP drops unsupported route types and does not propagate them to neighbors.

# ACI Layer 3 – BGP Route Reflector Configuration

System | System Settings | **BGP Route Reflector**

BGP Route Reflector Policy - BGP Route Reflector

Properties

Name: default

Description: RR Spine nodes

Autonomous System Number: 1

Route Reflector Nodes:

Node ID	Node Name	Description
103	Spine103	
104	Spine104	

© 2019 Cisco and/or its affiliates. All rights reserved.

17

To configure **Route Reflectors** in the ACI GUI, navigate: Fabric | Fabric Policies | Pod Policies | Policies

- Select BGP Route Reflector default
- Click Route Reflector Nodes [+] to launch Create Route Reflector Node Policy dialog
- In the dialog, select the Spine node(s) from the drop-down menu
- Click Submit.

Once the BGP Route Reflector default policy has been configured, the **Pod Policy Group** is then configured to use the **BGP Route Reflector default** policy (not illustrated).



**Figure 25. Adding a Layer 3 Border Leaf**

3. **Add layer 3 interfaces for this border leaf.** Click the “+” sign under “OSPF Interface Profiles”. Figure 26 provides an example of how to add two layer 3 sub-interfaces (sub-interface for eth1/39 and eth1/40 with dot1q tag 1000) on border leaf node 102 to connect to the two Nexus 3000s. Specify the MTU to be 1500. Leave the OSPF policy empty for the time being.

**Figure 26. Adding Two Layer 3 Sub-Interfaces**

4. Repeat steps 2 and 3 to add node 103 as a border leaf node for “L3OUT-1”. Add two sub-interfaces (eth1/39 and eth1/40 with dot1q tag 1000) for the border leaf node.

5. Click ‘Next’ to start to configure the external EPG. The ACI fabric maps external layer 3 endpoints to the external EPG by using the IP prefix and mask. One or more external EPGs can be supported for each layer 3 outside connection, depending on whether the user wants to apply a different policy for different groups of external endpoints. In this example we treat all outside endpoints equally and create only one external EPG. The ACI policy model requires an external EPG and the contract between the external EPGs and inside EPGs. Without this, all connectivity to outside will be blocked, even if external routes are learned properly. This is part of the security model of ACI (Figure 27).

**Figure 27. Configuring the External EPG**

6. **Configure a contract between the external and internal EPG.** In this example, we specify “WEB\_contract” as consumed contract for external EPG “L3EPG” (steps to configure this contract is skipped here). Click “Finish” in the previous step and go to menu **TenantàTenant PepsiàNetworkingàExternal Routed NetworksàL3OUT-1àNetworksàL3EPG**. Click “+” under the section of “Consumed Contracts” to add “WEB\_contract” as the consumed contract (Figure 28).

**Figure 28. Configuring a Contract for External EPG**

Next go to menu **Application ProfilesàApplication1àApplication EPGsàWEB EPG** and add the same contract, “WEB\_contract”, as the provided contract for WEB EPG. Once the consumer-provider relationship is established, check the application profile; it should look like Figure 29 on the APIC GUI. It states that communication between WEB EPG and L3EPG is regulated by policy “WEB\_contract”. Note that without a contract all communications between EPGs are blocked, including the communication with external EPGs.

**Figure 29. Contract Relationship with L3 External EPG**

7. **Create OSPF interface policy** by going to menu **TenantàNetworkingàProtocol PoliciesàOSPF Interface** (Figure 30).

**Figure 30. Creating the OSPF Interface Policy**

8. **Associate the OSPF interface policy with the sub-interfaces** on the two border leaf switches by going to menu **External Routed NetworksàLogical Node ProfilesàLogical Interface Profiles** (Figure 31). You will need to repeat this step for both border leaf switches.

**Figure 31.** Associating the OSPF Interface Policy with Sub-Interfaces

**9. Configure the policy for OSPF protocol parameters and associate it with private networks** (Figure 32). This is equivalent to configuring OSPF parameters under the VRF of “router ospf”.

Create the OSPF policy by going to menu **TenantàNetworkingàProtocol PoliciesàOSPF Timers**.

**Figure 32.** OSPF Protocol Parameters Policy Configuration

Associate the policy with private network CTX1 for this tenant by going to menu **TenantàNetworkingàPrivate Networks** (Figure 33).

**Figure 33.** Associating Configured OSPF Protocol Policy with Private Network

**10. Associate the layer 3 outside connection with bridge domain “BD1”** for this tenant (Figure 34). Repeat this step if there are multiple bridge domains for the tenant.

**Figure 34.** Associating Layer 3 Outside Connection with Bridge Domain

Under bridge domain “BD1” there are three subnets; two of them should be configured as public subnets (Figure 35). With this association, these two public subnets will be advertised to external routers by OSPF.

**Figure 35.** Subnet Scope of Bridge Domain

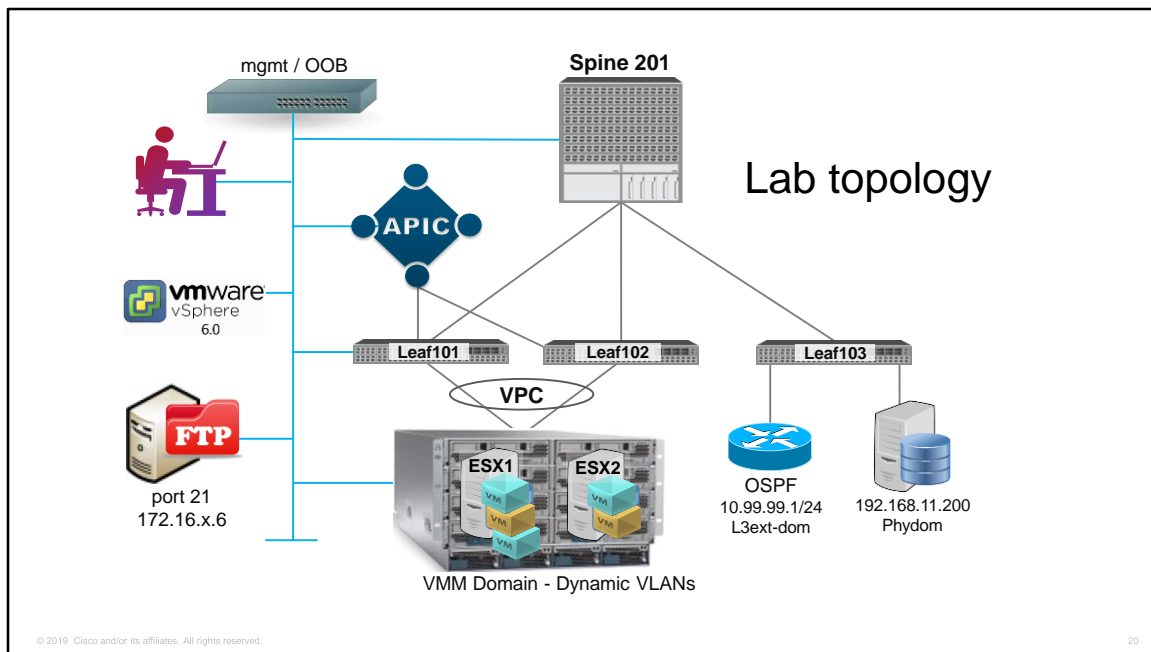
With above steps the Layer 3 outside connection configuration on APIC GUI is complete. If required by design, you have the option to configure policy to set the tag value for the tenant routes. Follow the steps explained in the section, “Tag Tenant Routes Using OSPF Route Policy.” Users must configure a BGP AS number and route reflector as explained in the section, “Route Distribution within the ACI Fabric.” Otherwise, the external routes won’t be propagated to non-border leaf switches.





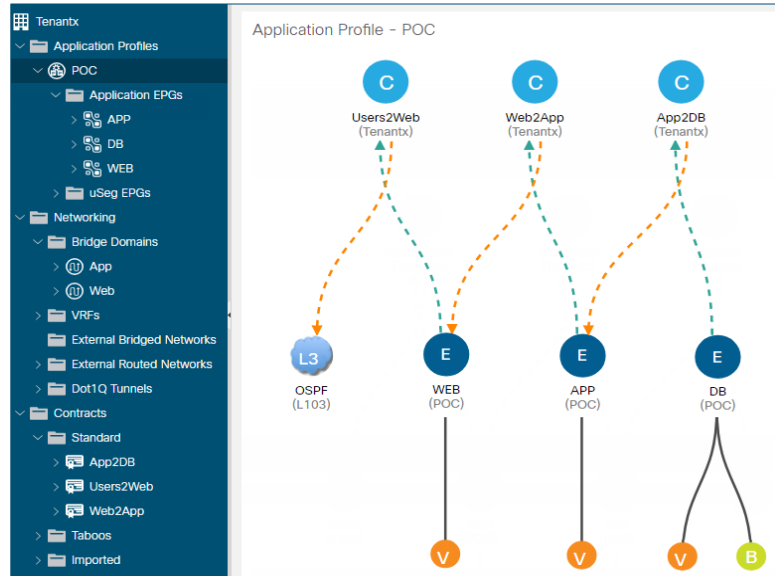
# Lab Topology

(DCACIO v4.0)



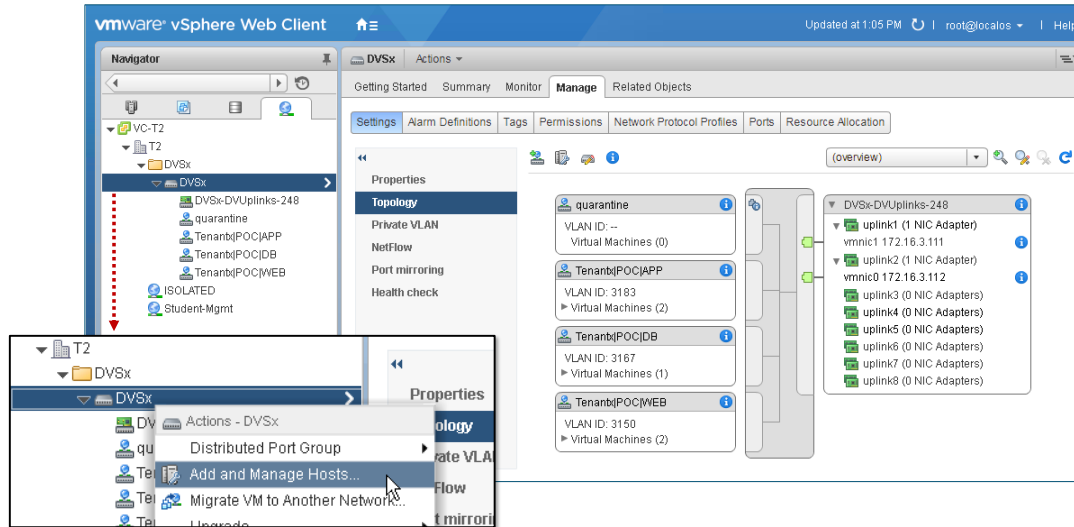
ACI device topology used in this course.

# Tenant configuration

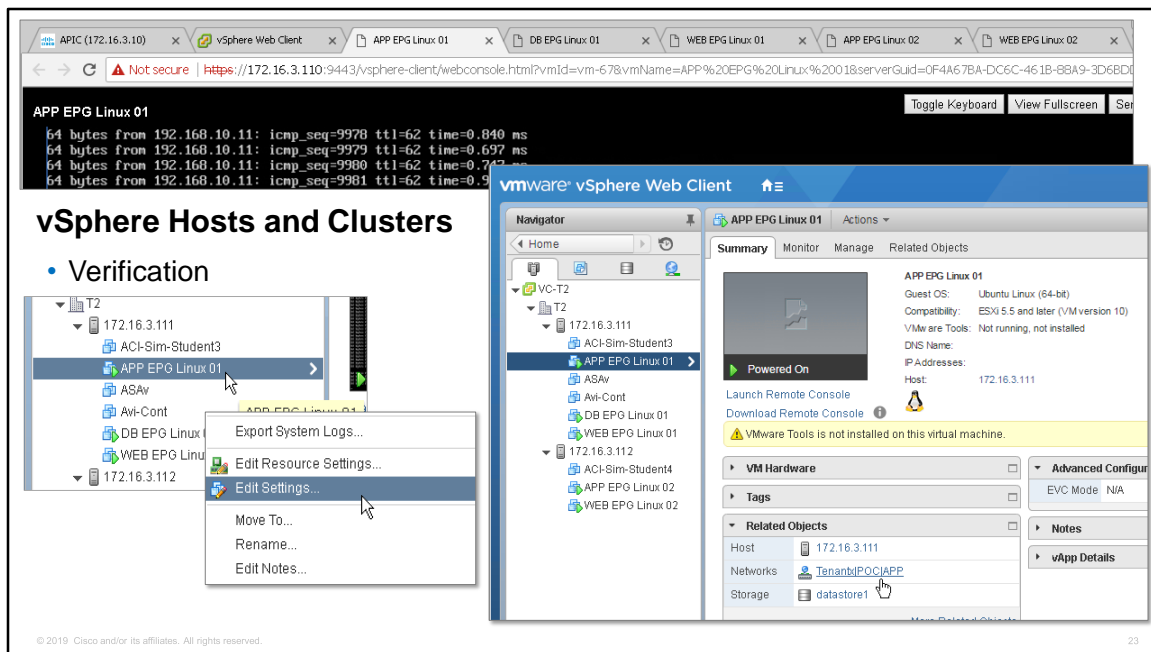


Final Tenant application profile state after for completing labs 1-4.

## vSphere Networking View



vSphere networking view in vCenter.

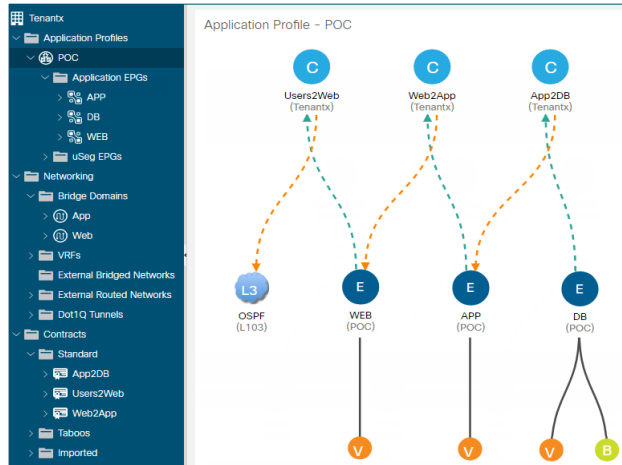


Verify ACI connectivity through Hosts and Clusters in vCenter.

# DCACIO Labs: Create Base Configuration

## Discovery Labs:

- Lab01 Tenant Creation
- Lab02 vCenter Integration
- Lab03 External Layer2
- Lab04 External Layer3 OSPF



Each Tenant will complete the listed Labs to create the baseline configuration to be used for the remaining course lessons and troubleshooting labs.

## VM Ping Scenario

### **Launch all virtual machine consoles**

- Invoke and leave running the following pings

App-server1 → Web-server2 192.168.10.12

DB-server1 → App-server2 192.168.11.12

Web-server1 → L3ext OSPF 10.99.99.1

App-server2 → Physical DB 192.168.11.200

Web-server2 → App-server2 192.168.11.12

© 2019 Cisco and/or its affiliates. All rights reserved.

25

Each Tenant will launch the consoles for each 'virtual-machine endpoint' and invoke the listed ping scenario.

App-server1 > Web-server2 192.168.10.12

DB-server1 > App-server2 192.168.11.12

Web-server1 > L3ext OSPF 10.99.99.1

App-server2 > Physical DB 192.168.11.200

Web-server2 > App-server2 192.168.11.12



# Contract Deny (Taboo) Logging

(DCACIO v4.0)



## Contract Deny (Taboo) Logging Configuration

Policies

System Messages Policy – Policy for system syslog messages

Properties

**Fabric | Fabric Policies | Policies | Monitoring | Common Policy | Syslog Message Policies**

- Select **Policy for system syslog messages**

Facility	Severity
auth	alerts
authpriv	alerts
cron	alerts
daemon	errors
default	information
ftp	alerts
kern	emergencies
local0	critical
local1	warnings
local2	debugging
local3	information
local4	errors
	notifications

**Instructor Demo:**  
Set default to information

© 2019 Cisco and/or its affiliates. All rights reserved. 27

### Contract Deny (Taboo) Logging Configuration

While the normal processes for ensuring security still apply, the ACI policy model aids in assuring the integrity of whatever security practices are employed. In the ACI policy model approach, all communications must conform to these conditions:

- Communication is allowed only based on contracts, which are managed objects in the model. If there is no contract, inter-EPG communication is disabled by default.
- No direct access to the hardware; all interaction is managed through the policy model.

Taboo contracts can be used to deny specific traffic that is otherwise allowed by contracts. The traffic to be dropped matches a pattern (such as, any EPG, a specific EPG, or traffic matching a filter). Taboo rules are unidirectional, denying any matching traffic coming toward an EPG that provides the contract.

With Cisco APIC Release 3.2(x) and switches with names that end in EX or FX, you can alternatively use a subject Deny action or Contract or Subject Exception in a standard contract to block traffic with specified patterns.

Taboo contracts allow employing a black-list designation applied to a given APG. Before configuring taboo contracts, the infra-administrator must the Policy for system syslog messages 'default' parameter to 'information' (illustrated).

### **About ACL Contract Permit and Deny Logs**

To log and/or monitor the traffic flow for a contract rule, you can enable and view the logging of packets or flows that were allowed to be sent because of contract permit rules or the logging of packets or flows that were dropped because of:

- Taboo contract deny rules
- Deny actions in contract subjects
- Contract or subject exceptions
- ACL contract permit and deny logging in the ACI fabric is only supported on Nexus 9000 Series switches with names that end in EX or FX, and all later models. For example, N9K-C93180LC-EX or N9K-C9336C-FX.
- Using log directive on filters in management contracts is not supported. Setting the log directive will cause zoning-rule deployment failure.

For information on standard and taboo contracts and subjects, see Cisco Application Centric Infrastructure Fundamentals and Cisco APIC Basic Configuration Guide.

### **EPG Data Included in ACL Permit and Deny Log Output**

Up to Cisco APIC, Release 3.2(1), the ACL permit and deny logs did not identify the EPGs associated with the contracts being logged. In release 3.2(1) the source EPG and destination EPG are added to the output of ACL permit and deny logs. ACL permit and deny logs include the relevant EPGs with the following limitations:

- Depending on the position of the EPG in the network, EPG data may not be available for the logs.
- When configuration changes occur, log data may be out of date. In steady state, log data is accurate.

The most accurate EPG data in the permit and deny logs results when the logs are focussed on:

- Flows from EPG to EPG, where the ingress policy is installed at the ingress TOR and the egress policy is installed at the egress TOR.
- Flows from EPG to L3Out, where one policy is applied on the border leaf TOR and the other policy is applied on a non-BL TOR.

EPGs in the log output are not supported for uSeg EPGs or for EPGs used in shared services (including shared L3Outs).

# Create Taboo Contract

The screenshot illustrates the process of creating a Taboo Contract in a network configuration tool. It shows three main components:

- Navigation Pane:** A tree view on the left with categories like Contracts, App-Contract, DB-Contract, Web-Contract, Taboo Contracts, Imported Contracts, and Filters. A 'Create Taboo Contract' button is visible next to the Taboo Contracts category.
- Create Taboo Contract Dialog:** A modal window titled 'Create Taboo Contract' with the subtitle 'Specify Identity Of Taboo'. It contains fields for 'Name' (set to 'ICMP-deny'), 'Description' (set to 'Deny ping'), and a 'Subjects' section with a table header 'Name' and 'Description'. A red box highlights a '+' button next to the Subjects field.
- Create Taboo Contract Subject Dialog:** A modal window titled 'Create Taboo Contract Subject' with the subtitle 'Specify Identity Of Subject'. It contains fields for 'Name' (set to 'icmp') and 'Description' (set to 'common/icmp'). It also has a 'Filters' section with a table header 'Name' and 'Directives', showing 'common/icmp' and 'none'. 'UPDATE' and 'CANCEL' buttons are at the bottom.
- Taboo Contract - ICMP-deny Configuration Page:** A configuration page titled 'Taboo Contract - ICMP-deny' with a 'Properties' section. It shows 'Name: ICMP-deny' and 'Description: Deny ping'. Below is a 'Subjects' table with columns 'Name', 'Filters', and 'Description'. The table contains one row: 'icmp', 'icmp', 'common/icmp'. A red box labeled 'Verify' is placed over the table.

## Create a taboo contract

1. On the menu bar, choose **Tenants > ALL TENANTS**.
2. In the Work pane, choose the **Tenant\_Name**.
3. In the Navigation pane choose **Tenant\_Name > Security Policies > Taboo Contracts**.
4. In the Work pane, choose **Action > Create Taboo Contract**.
5. In the **Create Taboo Contract** dialog box, perform the following actions:
  - Enter a Taboo Contract **Name**.
  - Click **+** to next to the **Subject** field to add a Taboo Subject.
    - Enter a Filter **Name**.
    - Choose **Directives**.
6. Click **Update**.
7. Click **OK**.
8. Click **Submit**.

## Add Taboo Contract

The screenshot illustrates the steps to add a Taboo Contract in the Cisco SD-WAN GUI. On the left, the 'Contracts' option is selected in the navigation pane, and 'Add Taboo Contract' is highlighted. The top right pane shows the 'Add Taboo Contract' dialog box, where 'Tn34/ICMP-deny' is selected from the dropdown menu. The bottom right pane shows the 'Contracts' table, which lists existing contracts and the newly added one.

Tenant Name	Contract Name	Contract Type	Provided / Consumed
<b>Contract Type: Contract</b>			
Tn34	App-Contract	Contract	Consumed
Tn34	Web-Contract	Contract	Provided
<b>Contract Type: Taboo</b>			
Tn34	ICMP-deny	Taboo	Both

© 2019 Cisco and/or its affiliates. All rights reserved.

29

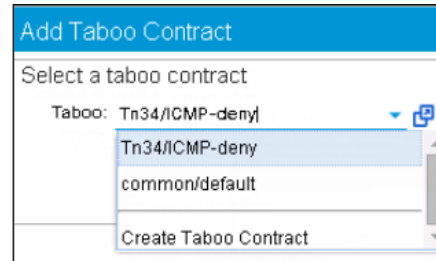
### Apply a taboo contract

1. On the menu bar, choose **Tenants > ALL TENANTS**.
2. In the Work pane, choose the **Tenant\_Name**.
3. In the Navigation pane choose **Tenant\_Name > Security Policies > Taboo Contracts > Taboo\_Contract\_Name**.
4. In the Work pane, choose **policy**.
  - Click **+** to next to the **Subject** field.
  - In the **Create Taboo Contract Subject** dialog box, perform the following actions:
    - Enter a Taboo Contract Subject **Name**.
    - Click **+** in the **Filter Chain** field.
      - Enter a **Filter Name**.
      - Choose **Directives**.
5. Click **Submit**.

## Lesson exercise: Create Taboo Contract

1. Verify Contract Deny Logging Configured
2. Launch ping from both Web and App servers (VMs)
3. Create/add Taboo contract
4. Verify ping has failed
5. Remove Taboo contract
6. Verify successful ping

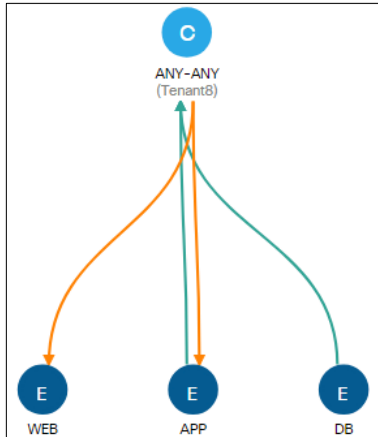
**You will view the Deny Log in a later exercise**



Exercise – Create and apply a Taboo contract

# Contract Exception

Contracts are enhanced in APIC Release 3.2(1) to enable denying a subset of contract providers or consumers from participating in the contract



**What if . . . we do not want **WEB** to talk to **DB**?**

- Exception uses **provider regex** and **consumer regex** to define the exceptions, and checks for matching providers and consumers
- When a pair of EPGs matches an exception, they cannot consume the corresponding contract or contract subject
- Exceptions can be configured under a contract, or under specific subject(s)
- There can be multiple exceptions under a contract or contract subject

© 2019 Cisco and/or its affiliates. All rights reserved.

31

## Configuring Contract or Subject Exceptions for Contracts

In Cisco APIC Release 3.2(1), contracts between EPGs are enhanced to enable denying a subset of contract providers or consumers from participating in the contract. Inter-EPG contracts and Intra-EPG contracts are supported with this feature.

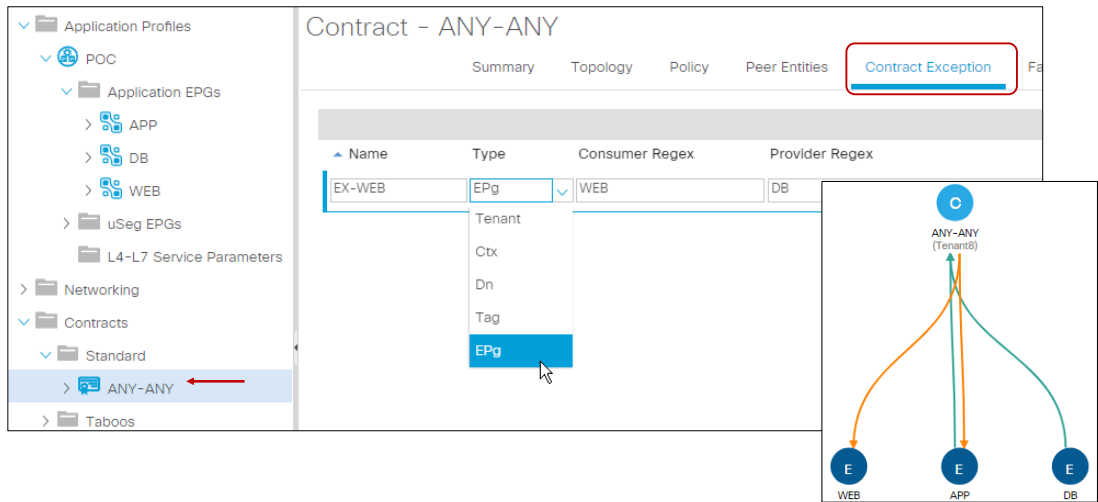
You can enable a provider EPG to communicate with all consumer EPGs except those that match criteria configured in a subject or contract exception. For example, if you want to enable an EPG to provide services to all EPGs for a tenant, except a subset, you can enable those EPGs to be excluded. To configure this, you create an exception in the contract or one of the subjects in the contract. The subset is then denied access to providing or consuming the contract.

Labels, counters, and permit and deny logs are supported with contracts and subject exceptions.

To apply an exception to all subjects in a contract, add the exception to the contract. To apply an exception only to a single subject in the contract, add the exception to the subject.

When adding filters to subjects, you can set the action of the filter (to permit or deny objects that match the filter criteria). Also for Deny filters, you can set the priority of the filter. Permit filters always have the default priority. Marking the subject-to-filter relation to deny automatically applies to each pair of EPGs where there is a match for the subject. Contracts and subjects can include multiple subject-to-filter relationships that can be independently set to permit or deny the objects that match the filters.

# Configuring Contract Exceptions



Contract - ANY-ANY

Summary Topology Policy Peer Entities **Contract Exception**

Name	Type	Consumer Regex	Provider Regex
EX-WEB	EPg	WEB	DB

Diagram illustrating the contract exception configuration:

- Consumer: ANY-ANY (Tenant)
- Endpoints: WEB, APP, DB
- Connections: The consumer is connected to all three endpoints (WEB, APP, DB).

Go to Contract Exception and add the type of object to add to the exception.



# Filter Options

## Create Contract Subject

Specify Identity Of Subject

Alias:

Description: optional

Target DSCP: Unspecified

Apply Both Directions: ☒

Reverse Filter Ports: ☒

## Filter Chain

L4-L7 Service Graph: select an option

QoS Priority:

Name	Directives	Action	Priority
TenantS/Prod-Filter	Enable Policy Compression	Deny	highest priority
	none	Permit	default level
	log	Deny	lowest priority
	Enable Policy Compression		highest priority
			medium priority

APIC Release 3.2(1) allows new filter options:

### Directives:

- **Log**—permit and deny logging
- **Enable Policy Compression**—contract data storage optimization
- **None**—disables contract logging or Enable Policy Compression

**Action:** Permit / Deny for Subject Filters

**Priority:** for traffic matching the filter criteria

### NOTE:

- Some features, such as statistics, will be unavailable while Policy Compression is active
- Filters containing prio, qos and markDscp are not considered for compression

## Filters Options

A filter is a group of filter entries that are aimed to filter traffic. Each filter entry is a rule that allows or denies traffic that is classified based on TCP/IP header fields, such as Layer 3 protocol type or Layer 4 ports. The filter is defined on the contract that is associated with an endpoint group. This can be either incoming toward an endpoint group, outgoing away from an endpoint group, or both. A subject is an entity that connects the filter to the contract, thereby affecting the traffic between endpoint groups that are provided and consumed by this contract.

## Filter Entry Configuration Parameters

When configuring a filter, the following options can be defined:

- **Name**—The name of a filter entry.
- **EtherType**—The EtherType of the filter entry. The EtherTypes are:
  - **ARP**
  - **FCOE**
  - **IP**
  - **MAC Security**
  - **MPLS Unicast**
  - **Trill**

- **Unspecified**

**ARP Flag**—The Address Resolution Protocol flag for a filter entry. The filter entry is a combination of network traffic classification properties.

**IP Protocol**—The IP protocol for a filter entry. The filter entry is a combination of network traffic classification properties.

**Match Only Fragments**—Match only packet fragments. When enabled, the rule applies to any IP fragment with an offset that is greater than 0 (all IP fragments except the first). When disabled, the rule will not apply to IP fragments with an offset greater than 0 because TCP/UDP port information can only be checked in initial fragments.

**Port Ranges (Source, Destination)**—The port fields for the source and destination. You can define a single port by specifying the same value in the **From** and **To** fields, or you can define a range of ports from 0 to 65535 by specifying different values in the **From** and **To** fields. Instead of specifying a number, you can instead choose one of the following server types to use the pre-defined port of that type:

- **HTTPS**
- **SMTP**
- **HTTP**
- **FTP-Data**
- **Unspecified**
- **DNS**
- **POP3**
- **RTSP**

The default is **Unspecified**.

- **TCP Session Rules**—The TCP session rules for a filter entry. The filter entry is a combination of network traffic classification properties.

