

Examining Cisco ACI Building Blocks and VMM Domains



Sean Douglas

DATA CENTER ENGINEER

@ocdlearning



Overview



Examine Cisco ACI building blocks

- Tenants, VRFs, Bridge Domains

Examine virtual switches, VMM domains, contracts

Demonstrate how to use APIC to create

- VMM domains, tenants, application profiles and contracts



Tenants, VRF, Bridge Domain, EPG



Tenant-Based Components



At the top level, the Cisco APIC policy model is built on a series one or more tenants.



Logical container or a folder for application policies. Tenants allow us to separate network infrastructure administration.



Tenants can be used to draw boundaries between different organizations that use the same infrastructure.



Tenants can contain objects that define the tenant policies such as application profiles and EPGs.



Tenants

Customer, business unit, policy group

Reuse IP space

Tenants only see inside their space

Shared services between tenants

Preconfigured tenants:

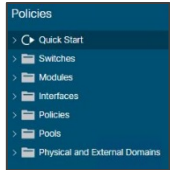
- Common
- Infra
- Mgmt



ACI Tenants



Tenants can be isolated from one another or can share resources.



Primary elements are filters, contracts, outside networks, bridge domains, VRF instances, and application profiles that contain EPGs.



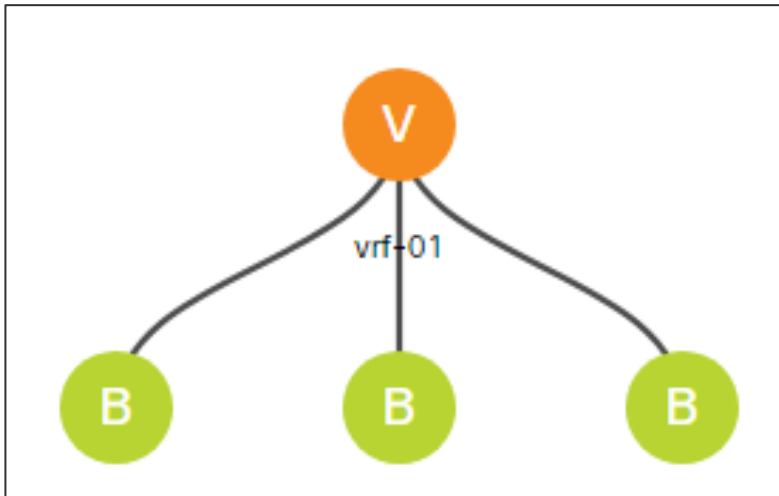
Entities in the tenant inherit its policies. VRFs are also known as contexts; each VRF can be associated with multiple bridge domains.



The ACI fabric supports IPv4, IPv6, and dual-stack configurations for tenant networking



ACI Components



VRFs are like private layer 3 networks. Each tenant can have one or more VRFs

Bridge domains are like layer 2 forwarding domains and must be linked to a VRF

EPG is like a VLAN. Logical group of hosts or servers that perform similar functions. Must be associated to a bridge domain



Cisco ACI Building Blocks



VDC

Tenant



Cisco ACI Building Blocks



The diagram illustrates the relationship between a VRF and its Virtual Routing Table. A large orange rectangle represents the VRF, and a smaller blue rectangle inside it represents the Virtual Routing Table.

**Virtual Routing
Table**

VRF



Cisco ACI Building Blocks



Bridge Domain



Cisco ACI Building Blocks



Application Profile



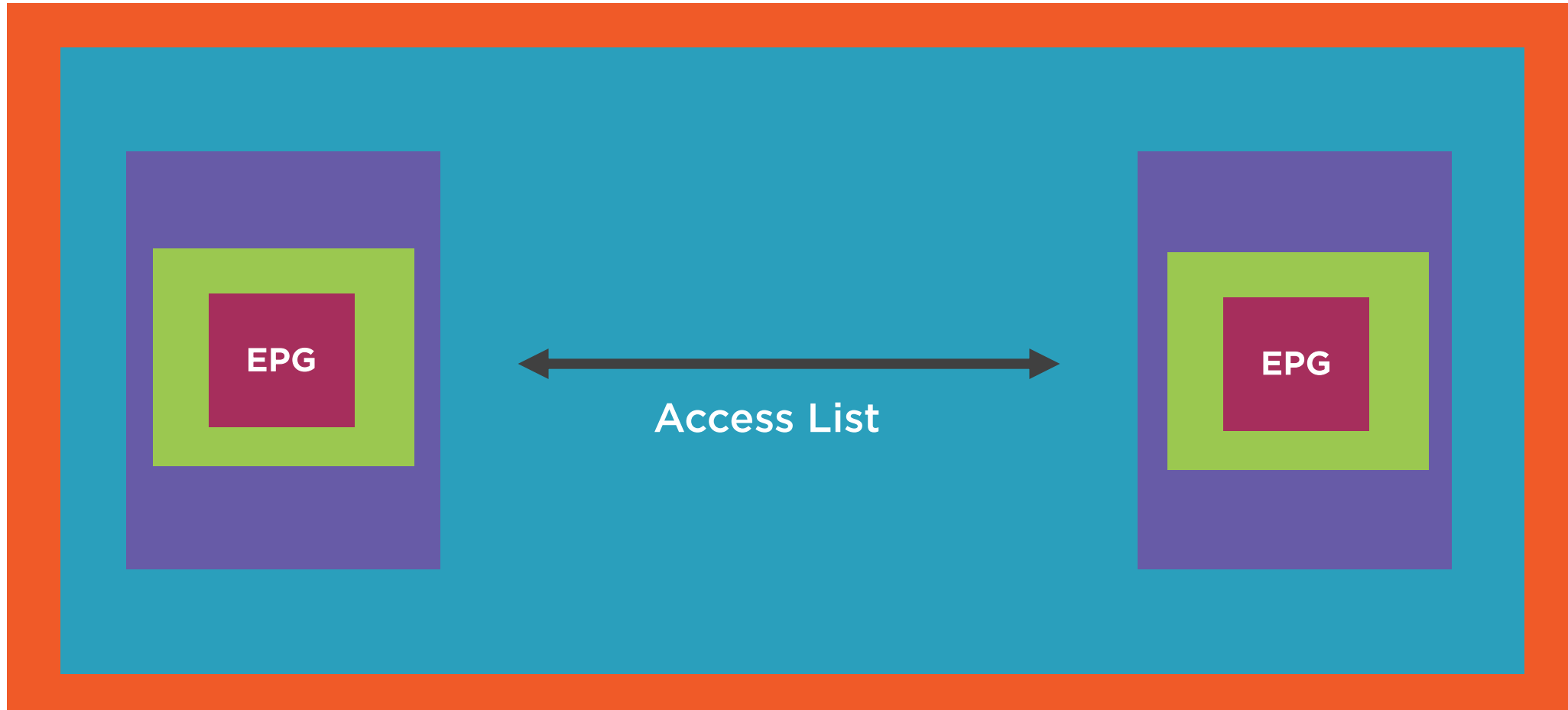
Cisco ACI Building Blocks



EPG



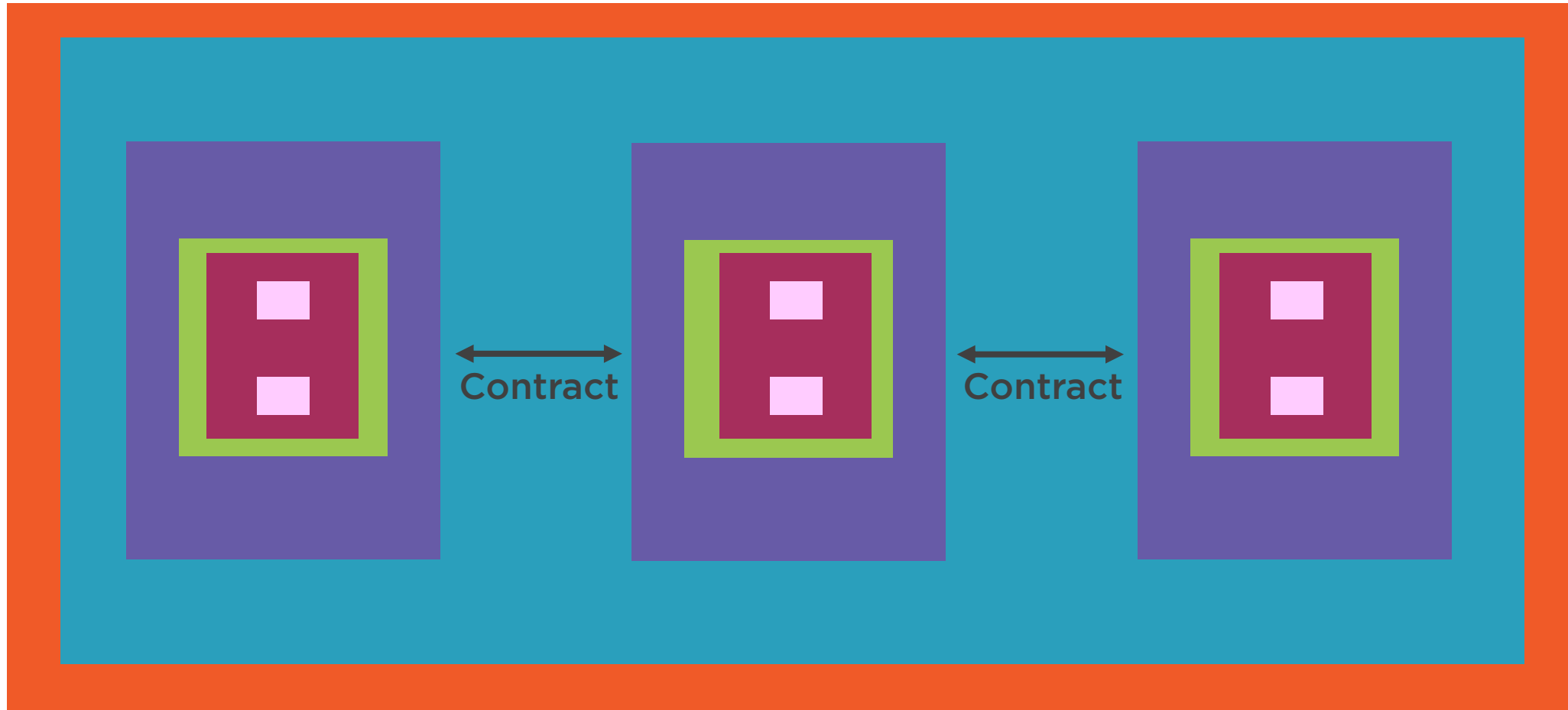
Cisco ACI Building Blocks



Contract



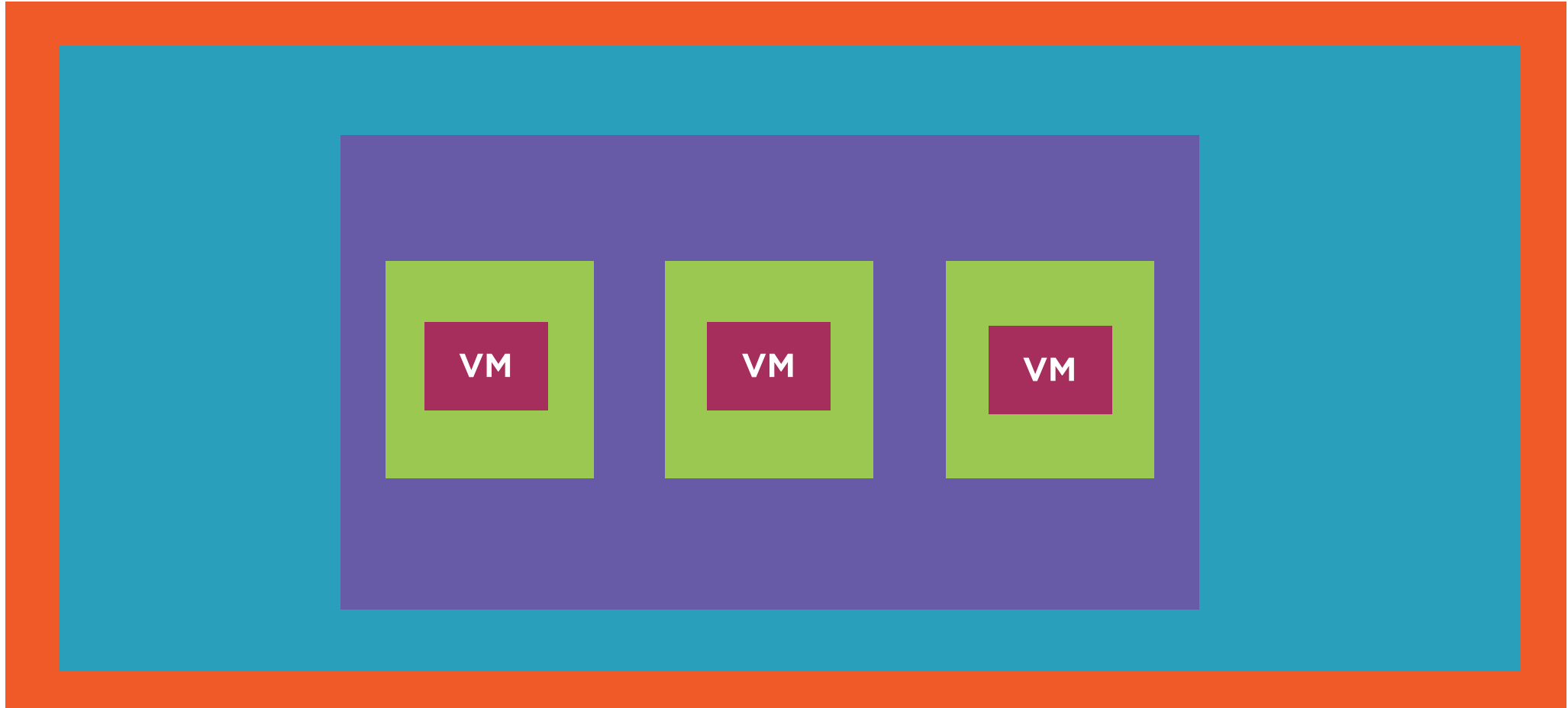
Cisco ACI Fabric



Endpoints



Cisco ACI Fabric



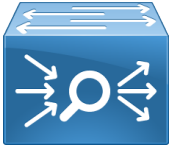
Cisco ACI Endpoints and Endpoint Groups



Endpoint Groups



EPGs are used to create logical groupings of hosts or servers that perform similar functions within the fabric



Each created EPG can have its own monitoring and QoS policy, and it must be associated with a bridge domain



An EPG is a child object of the application profile, and an application profile can contain multiple EPGs



Policies apply to EPGs, never to individual endpoints. Endpoints inside an EPG can communicate with each other



Endpoint Groups

Create Application EPG

STEP 1 > Identity

Name:

Alias:

Description:

Tags:
enter tags separated by comma

Contract Exception Tag:

QoS class:

Custom QoS:

Data-Plane Policer:

Intra EPG Isolation: ☒ Enforced ☐ Unenforced

Preferred Group Member: ☒ Exclude ☐ Include

Flood in Encapsulation: ☒ Disabled ☐ Enabled

Bridge Domain:

Monitoring Policy:

FHS Trust Control Policy:

Shutdown EPG: ☐

Associate to VM Domain Profiles: ☐

Statically Link with Leaves/Paths: ☐

EPG Contract Master:

Application EPGs

Communication between EPGs controlled by contracts

We can extend a single subnet across several EPGs

Each EPG is identified by a VLAN or VXLAN

Set of endpoints that require similar policy



Endpoints



Endpoints are devices that are connected to the network—either directly or indirectly



Endpoints have an address (identity), a location, attributes, and can be either virtual or physical



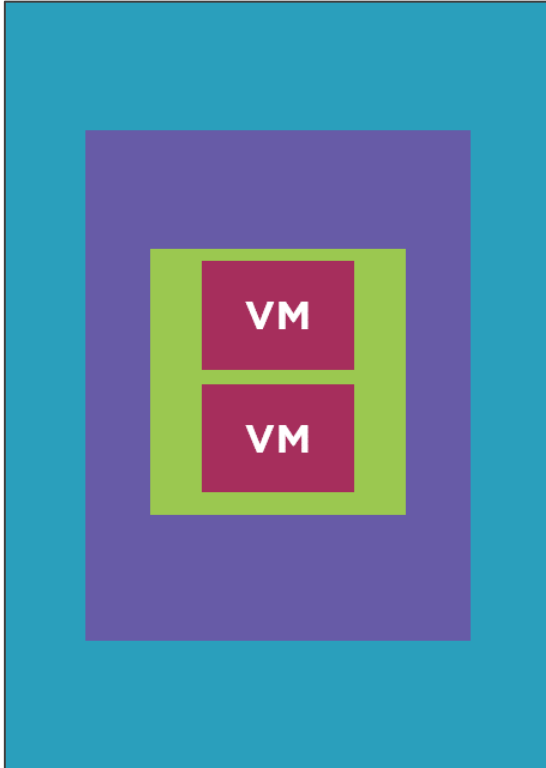
Each endpoint has a path, an encapsulation, and a deployment immediacy mode associated with it



An endpoint is a child object of the EPG and an EPG construct can contain multiple endpoints



Endpoints



Virtualized servers

Bare-metal servers

Mainframes

IP storage devices

Switches and routers

Firewall, IPS

Application Profile



A container that holds EPGs that are logically related to one another



EPGs can communicate with other EPGs in the same application profile and with EPGs in other application profiles



Within an application profile, you may group servers in EPGs depending on the use of common policies



Application profiles provide a mechanism to understand groups of servers as a single application



Demo



Demonstrate how to use Cisco APIC to create a tenant and configure:

- VRF
- Bridge Domain
- Subnet
- EPG
- Application Profile
- Contracts



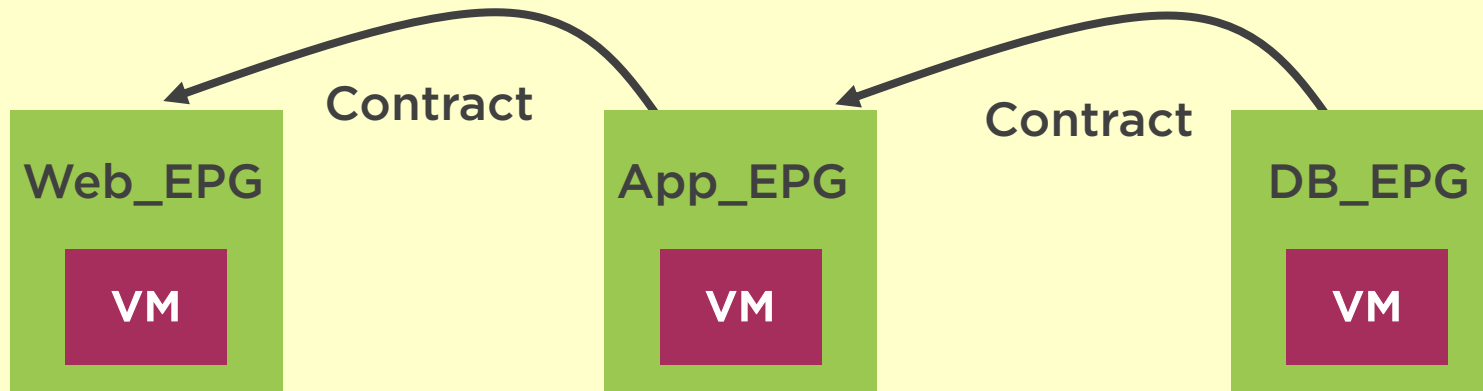
Implement Cisco ACI Tenant Policies

Tenant - Marketing

VRF - Sales

Bridge Domain - Sales

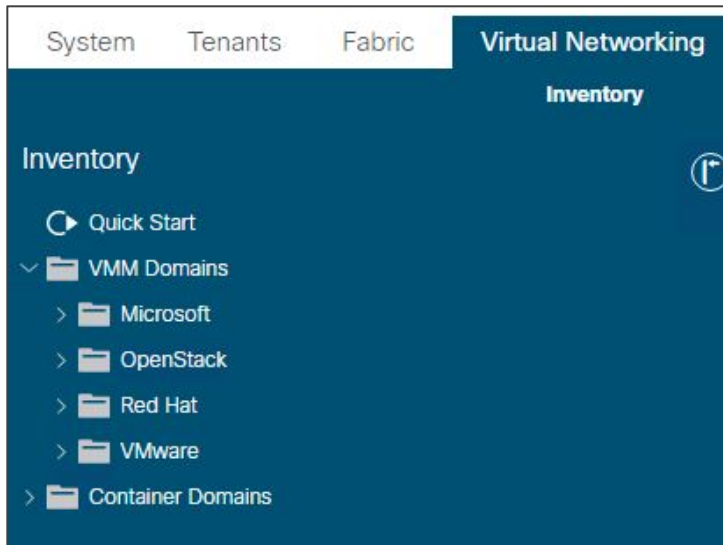
Application Profile - eCommerce



Virtual Switches and VMM Domains



Virtual Switches



ACI can be integrated into virtual deployments and deliver:

- Simplicity
- Scalability
- Security

ACI works with a variety of different hypervisors

- Programmable and automated access
- Policy-based management
- VMM domains to manage VM controllers



Virtual Switches

Software component that enables communication among VMs running on a hypervisor

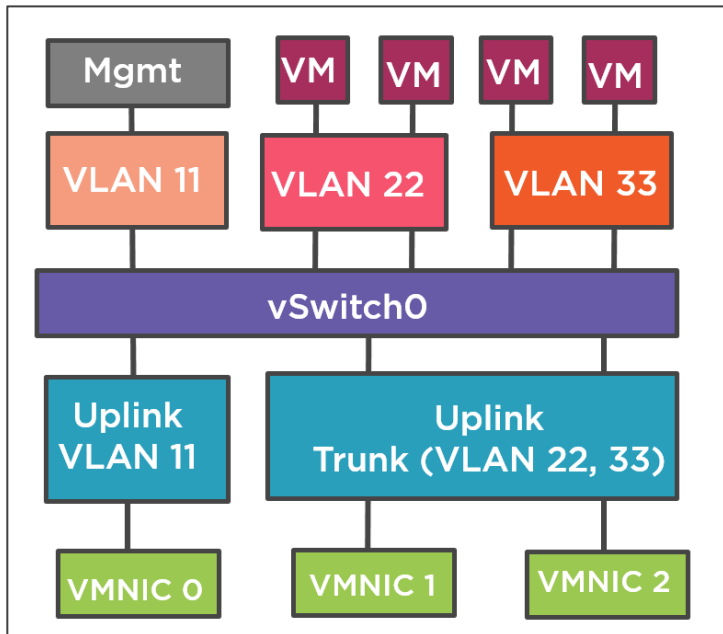
Provide a link between the VM environment and Cisco ACI

ACI integrates with multiple hypervisor solutions:

- VMware
- Microsoft
- KVM



vSwitches



vSwitches are Layer 2 devices

vSwitch switches traffic between VMs on the same host

Other traffic is forwarded to the uplink port

vSwitches support trunking, port channels, CDP



VMware Standard Switch



In VMware environment, most components of the network are virtualized, except for the NIC that's in the host



Physical NICs often act as uplink ports in the vSwitches that are created on the VMware hypervisor level



A VMware vSwitch is a virtual component that performs network switching between the VMs on a host and the external network



A vSwitch can have up to 32 network ports assigned to it. Bandwidth and reliability increase with the number of assigned ports



VMware vSphere Distributed Switch



Eliminates the configuration of individual virtual switches and enables centralized provisioning, administration, and monitoring



The VDS requires a VMware vCenter server or appliance



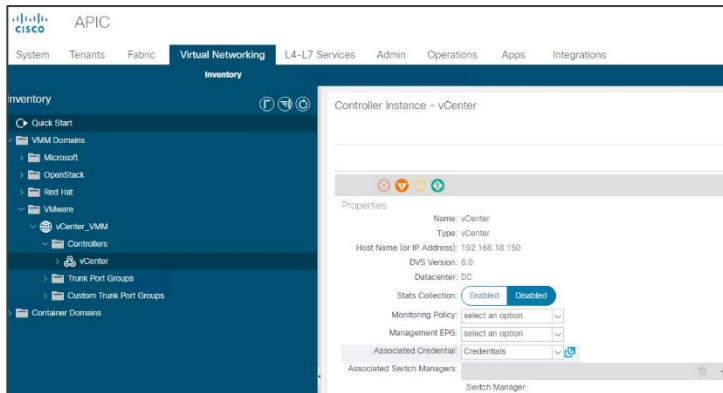
Standard vSwitch managed individually on the host where it was created; VDS is managed globally across all hosts as a single switch



Can be provisioned and managed by APIC. Spans multiple ESX hosts in a data center



Cisco ACI VMM Domains



Contain one or more of the same type of VM controllers and credentials

Allow the APIC to interact with the VM controller

Integration with ACI

- Push policies to the VM controller
- Create port groups and other elements
- Listen and respond to controller events



VMM Domain Components

VMM profile groups VM controllers with similar requirements

VMM profile contains:

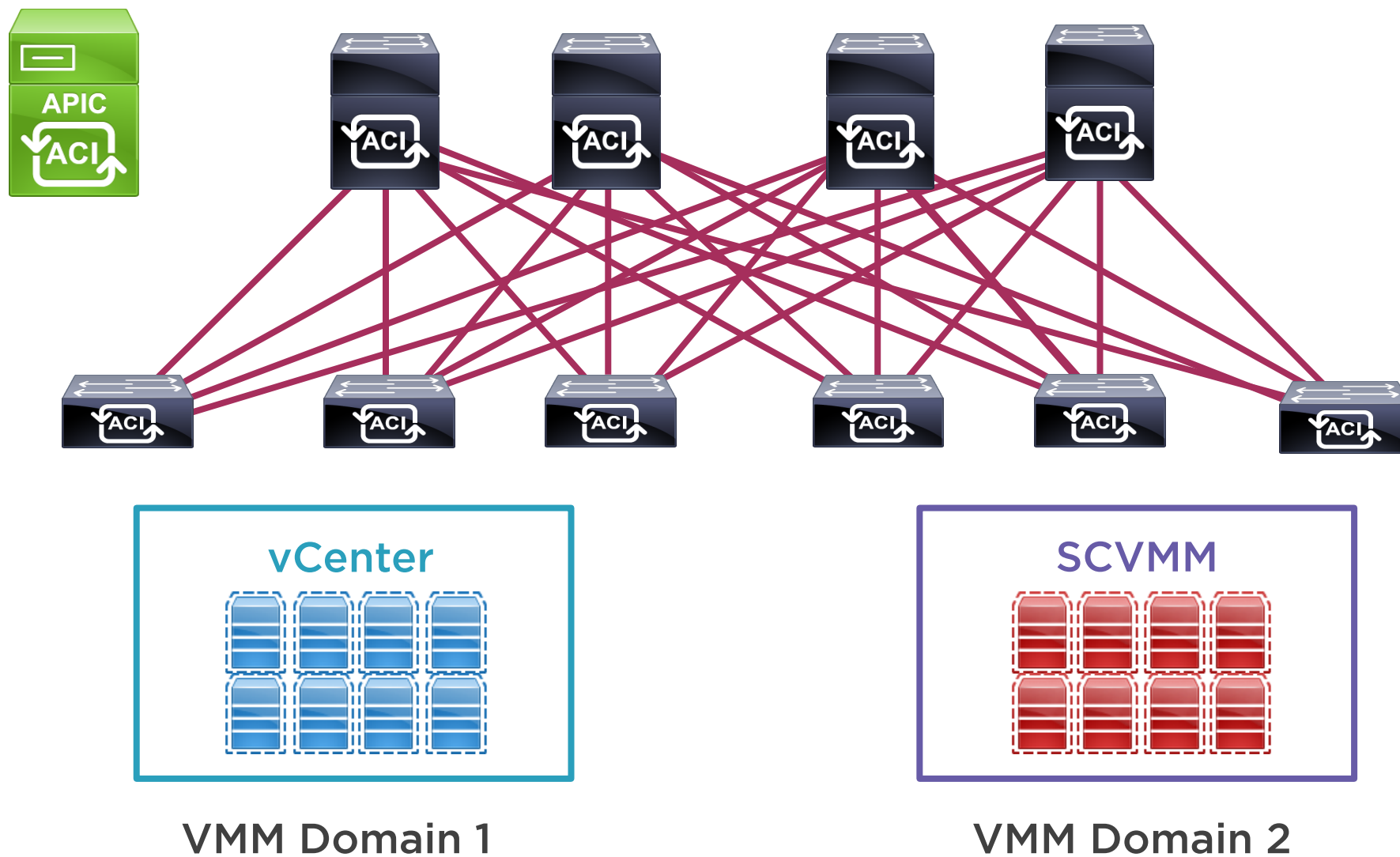
- Controller
- Controller username/password

VMM profile is associated with:

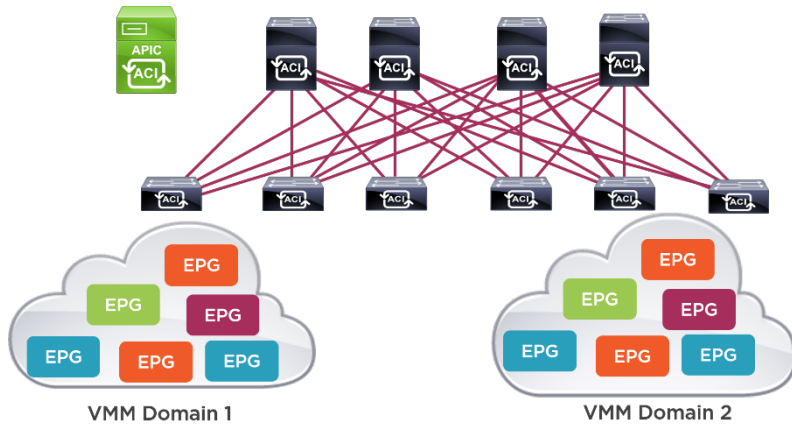
- EPG
- AEP
- VLAN pool



APIC VMM Domains



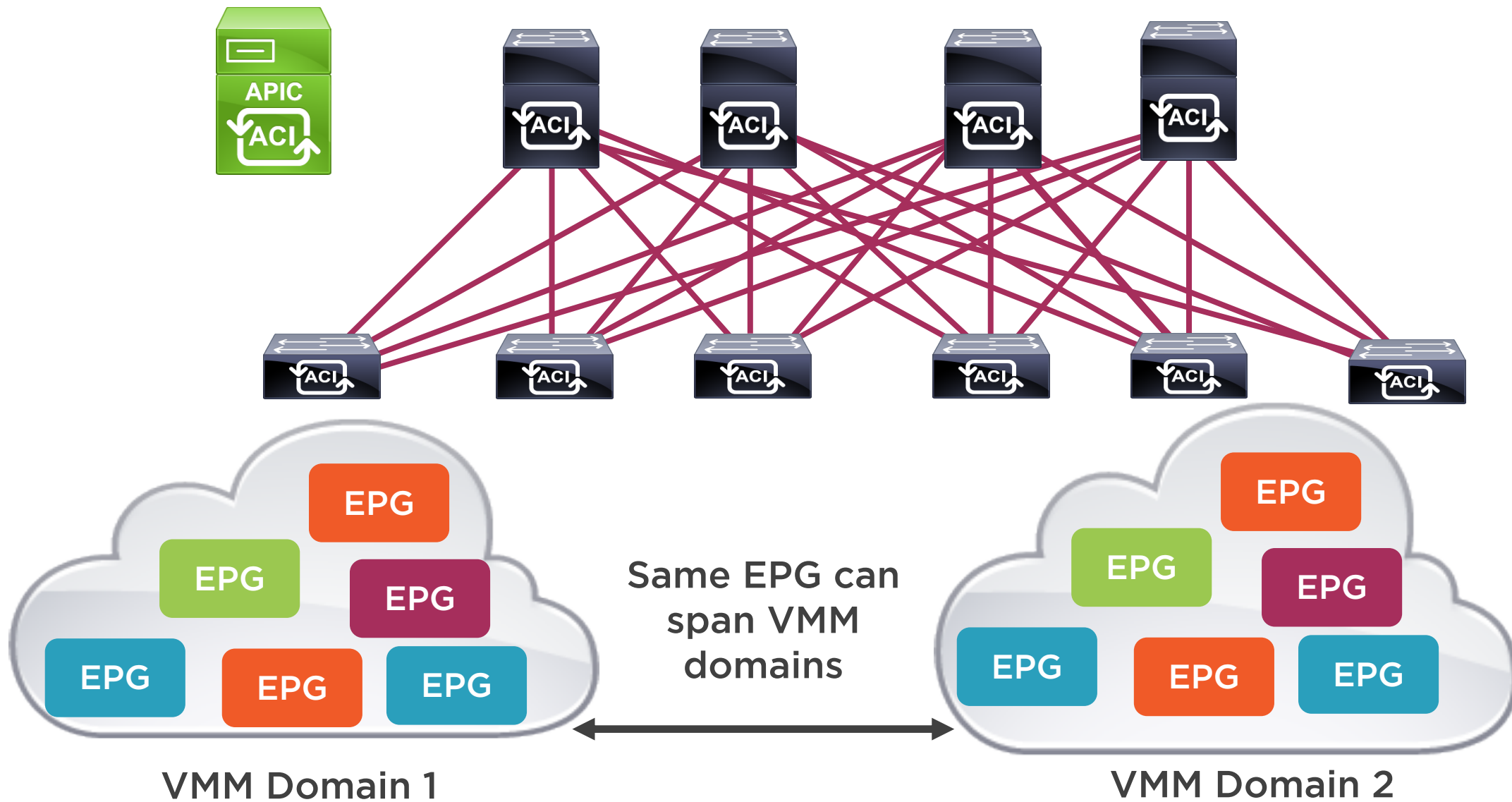
VMM Domain EPG



- EPGs are associated with VMM domain
- APIC pushes port groups for each EPG
- VMM administrator associates VMs with EPGs
- An EPG can span multiple domains
- Up to 5000 EPGs per VMM domain



APIC VMM Domains



Contracts

Configure Contract

EPG Information

Configure an Intra-EPG Contract: ☐

Consumer EPG / External Network: Globomantics/MyApp/epg-App_21

Provider EPG / Internal Network: Globomantics/MyApp/epg-DB_22

Contract Information

Contract Type: **New Contract** | Select Existing Contract

Contract Name: DB_App

No Filter (Allow All Traffic): ☒

Filter Entries:

ARP Flag	IP Protocol	Match Only Fragments	Stateful	Source Port / Range		Destination Port / Range		TCP Session Rules
				From	To	From	To	
	tcp	False	False	3306	3306	3306	3306	Unspecified

Contracts give ACI admin ability to control traffic flow within EPGs

One EPG provides the services it wants to offer, and another EPG consumes them

Assigned scope of Global, Tenant, VRF, or Application Profile to limit accessibility

Not need for endpoints within the same EPG



Demo



Demonstrate how to use Cisco APIC to create a VMM domain and tenant, as well as:

- VRF
- Bridge Domain
- Application Profile
- EPGs
- Contracts



Summary



Examine Cisco ACI tenants and their components

- Demonstrate how to use Cisco APIC to implement tenant policies

Examine virtual switches, VMM domains, and endpoint group functions

- Demonstrate how to use APIC to integrate Cisco ACI with VMware