MATICMIND®

MAKES IT EASY

Cisco ACI Training Course

DAY3 – Advanced Features & Automation

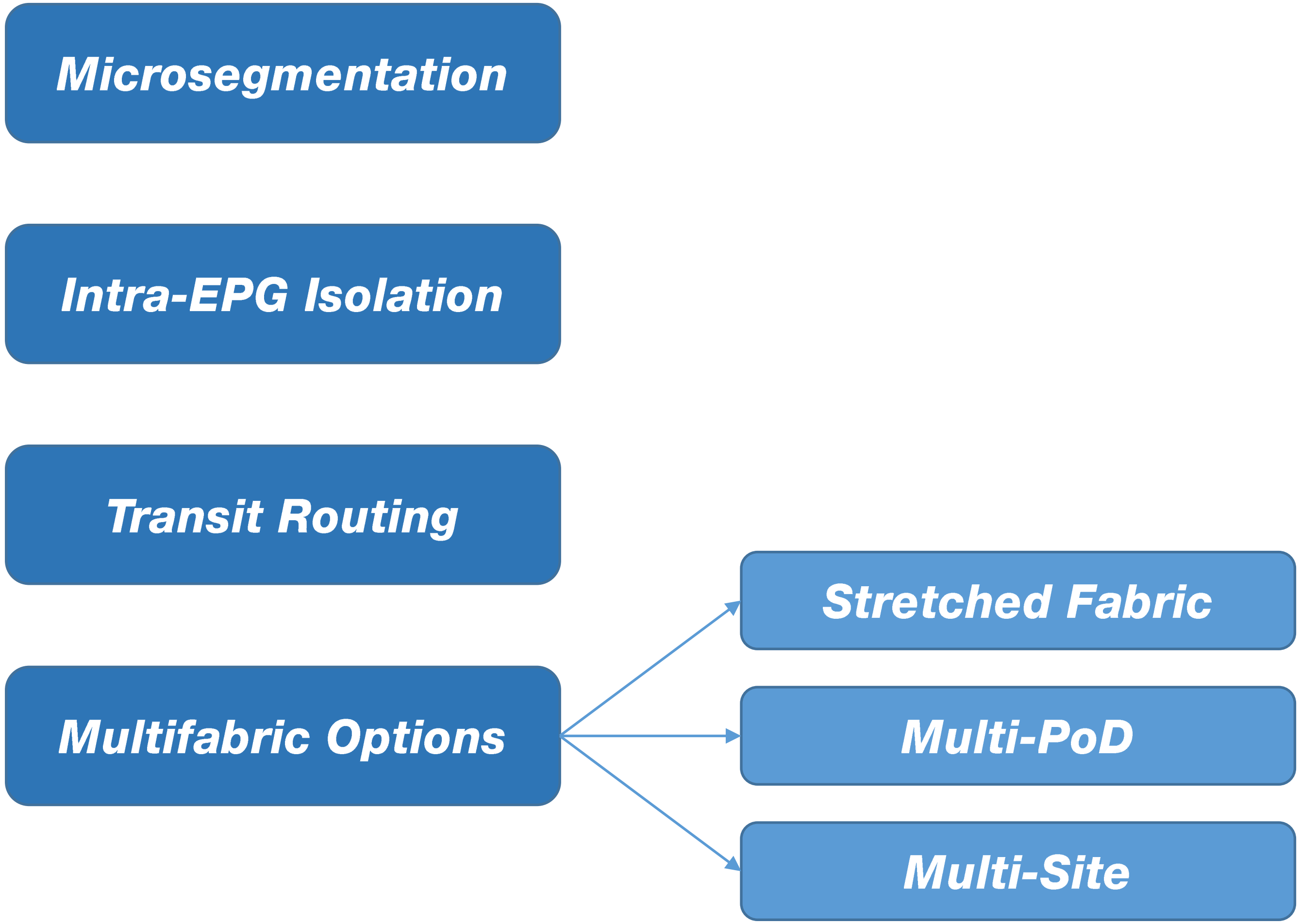
November 2020

AGENDA - DAY 3

1. ACI Advanced Features
    1. Microsegmentation
    2. DEMO LAB8
    3. Intra-EPG Isolation
    4. Transit Routing
    5. Multifabric Options
        1. Stretched Fabric
        2. Multi-Pod
        3. Multi-Site

2. ACI APIs & Automation

ACI Advanced Features



Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

- Stretched Fabric
- Multi-PoD
- Multi-Site

Microsegmentation

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

What is it?

Microsegmentation with the Cisco Application Centric Infrastructure (ACI) provides the ability to automatically assign endpoints to logical security zones called MICRO endpoint groups (uEPGs) based on various network-based or virtual machine (VM)-based attributes.

Microsegmentation polices used by the Cisco AVS, VMware VDS and Microsoft vSwitch are centrally managed by the Cisco Application Policy Infrastructure Controller (APIC) and enforced by the fabric.

Where is it used?

Microsegmentation with Cisco ACI provides support for virtual endpoints attached to the following:

- VMware vSphere Distributed Switch (VDS)
- Cisco Application Virtual Switch (AVS)
- Microsoft vSwitch
- Bare-Metal environments

Microsegmentation

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

uEPGs attributes:

- Network-Based Attributes
  - IP Address
  - MAC
- VM-Based Attributes
  - VMM Domain
  - Operating System
  - Hypervisor Identifier
  - Datacenter
  - VM Identifier
  - VM Name
  - VNic Dn (vNIC domain name)
  - Custom Attribute, and Tag

Microsegmentation

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Methods of Filtering VMs for uSeg EPGs

- Match any attribute
- Match all attributes
- Using simple or block statements
- Overriding existing rules

Microsegmentation

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Configuration Example

1. On the menu bar, click **Tenants**.
2. On the submenu bar, click *<Tenant_Name>*.
3. In the Navigation pane, expand ***<Tenant_Name>* -> Application Profiles -> *<AP_Name>***
4. Right-Click on **uSeg EPGs** and select **Create uSeg EPGs**.
5. In the **Create uSeg EPGs** dialog box
   a. Fill the Name field with *<MicroEPG_Name>.*
   b. From the **Bridge Domain** drop-down menu, select *<BD_Name>*.
   c. Click the **Next** button.
   d. In the **Associated Domain Profile** table, click the "**+**" button.
   e. From the **Domain Profile** drop-down menu, select *<PHYS-DOMAIN_Name>.*
   f. Click **Update**.
   g. Click **Finish**.
6. In the Navigation pane, expand the newly created *<MicroEPG_Name>*
7. Right-Click on **Domains (VMs and Bare-Metal)** and select **Add Physical Domain Association**
8. In the **Physical Domain Profile** drop down menu select *<PHYS-DOMAIN_Name>.*
9. Click on **Submit** button.
10. In the Navigation pane, expand the newly created *< MicroEPG_Name>*
11. Click on uSeg Attributes folder.
12. In the **uSeg Attributes Policy** click the "**+**" button.
    a. Select Type **IP.**
    b. Fill the ip address field with address *<IP_address>*.
13. Repeat steps 12, 12.a and 12.b with other IP addresses if needed.
14. Click on **Submit** button.
15. In the Navigation pane, expand the newly created *<MicroEPG_Name>*.
16. **Right-Click** on the **Satic Leaf** folder and select **Statically Link With Node**.
17. Select the leaf where the microEPG is expected to be.

Click on **Submit** button.

Microsegmentation

- **Microsegmentation**
- *Intra-EPG Isolation*
- *Transit Routing*
- *Multifabric Options*

DEMO LAB 8

Intra-EPG Isolation

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

What is it?

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or uSeg EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from on another within an EPG is desirable.

Where is it used?

- VMware VDS or Microsoft vSwitch
- Enforcement for Cisco AVS
- Enforcement for Cisco ACI Virtual Edge

Intra-EPG Isolation

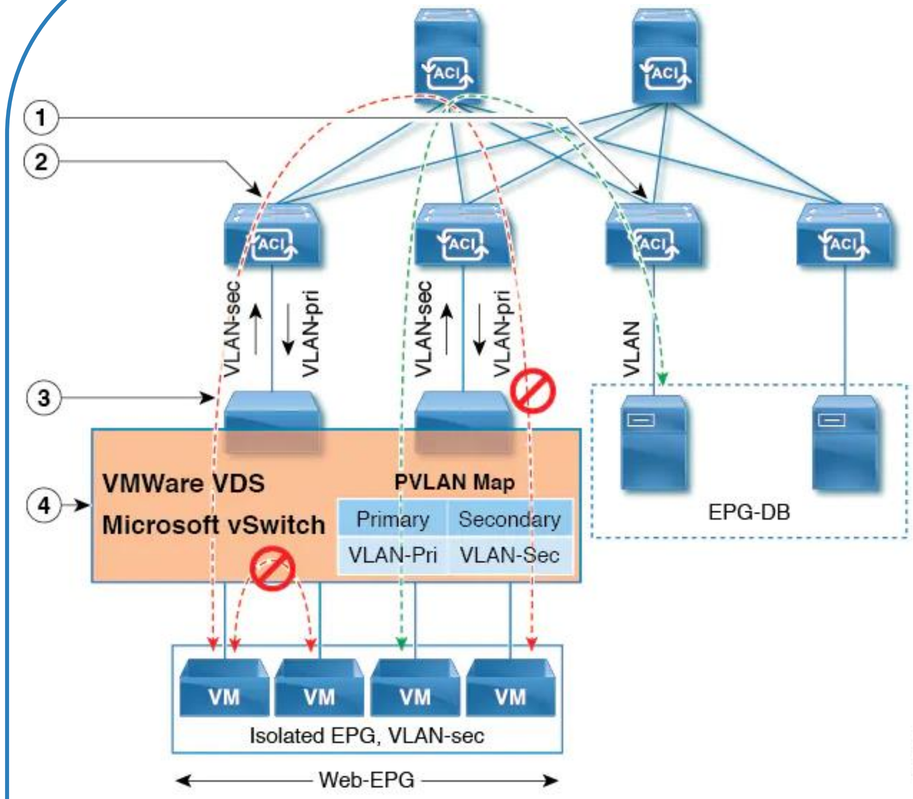
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Example: Intra-EPG Isolation for VMware VDS or Microsoft vSwitch



1.EPG-DB sends VLAN traffic to the Cisco ACI leaf switch. The Cisco ACI egress leaf switch encapsulates traffic with a primary VLAN (PVLAN) tag and forwards it to the Web-EPG endpoint.

2.The VMware VDS or Microsoft vSwitch sends traffic to the Cisco ACI leaf switch using VLAN-sec. The Cisco ACI leaf switch drops all intra-EPG traffic because isolation is enforced for all intra VLAN-sec traffic within the Web-EPG.

3.The VMware VDS or Microsoft vSwitch VLAN-sec uplink to the Cisco ACI Leaf is in isolated trunk mode. The Cisco ACI leaf switch uses VLAN-pri for downlink traffic to the VMware VDS or Microsoft vSwitch.

4.The PVLAN map is configured in the VMware VDS or Microsoft vSwitch and Cisco ACI leaf switches. VM traffic from WEB-EPG is encapsulated in VLAN-sec. The VMware VDS or Microsoft vSwitch denies local intra-WEB EPG VM traffic according to the PVLAN tag. All intra-ESXi host or Microsoft Hyper-V host VM traffic is sent to the Cisco ACI leaf using VLAN-Sec.

Transit Routing

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

What is it?

It's not a FEATURE. It's a design implementation which enables border routers (typically L3Outs) to perform bidirectional redistribution with other routing domains. Unlike the stub routing domains of earlier ACI releases, that block transit redistribution, bidirectional redistribution passes routing information from one routing domain to another. Such redistribution lets the ACI fabric provide full IP connectivity between different routing domains. Doing so can also provide redundant connectivity by enabling backup paths between routing domains.

Where is it used?

- VMware VDS or Microsoft vSwitch
- Enforcement for Cisco AVS
- Enforcement for Cisco ACI Virtual Edge

Transit Routing

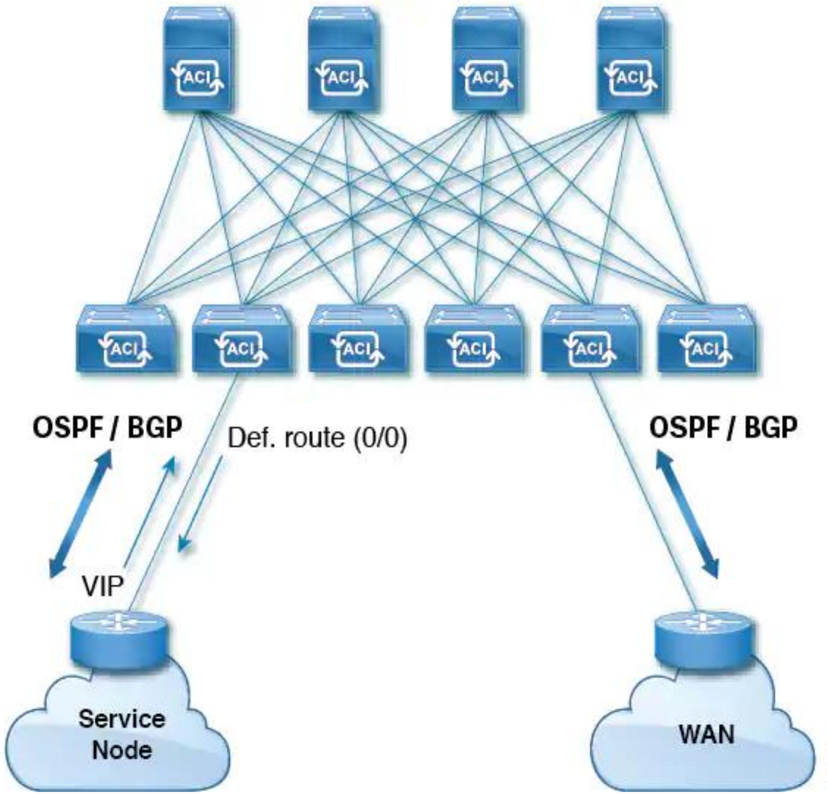
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Example:Transit Routing



1.VIP address is advertised to the Fabric

2.The Fabric Advertise the VIP address to the WAN router for external visibility of the remote VIP.

Transit Routing

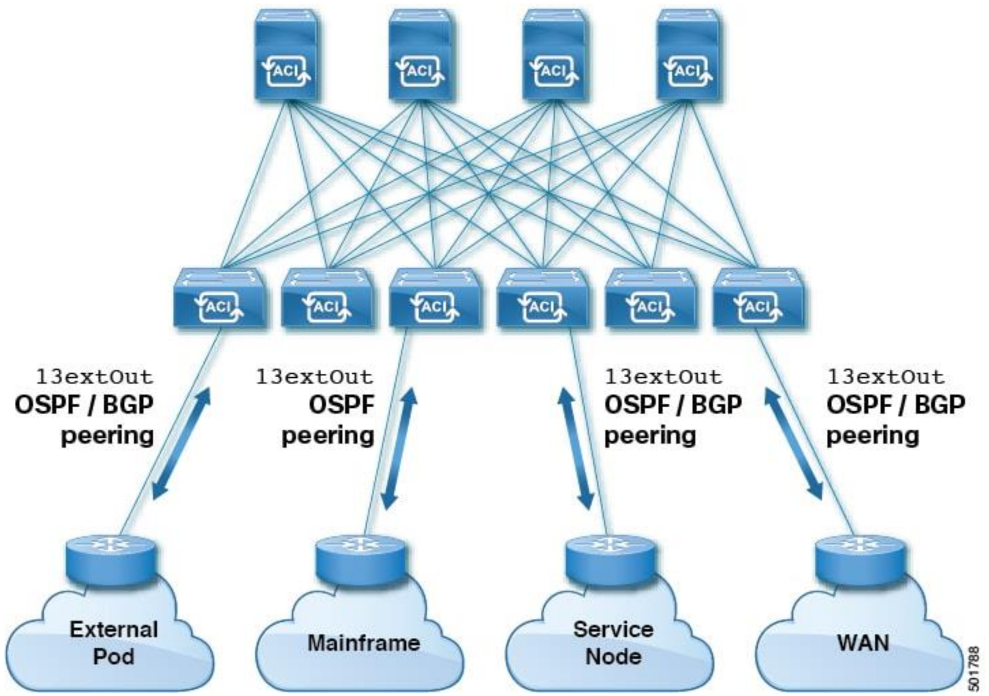
Microsegmentation

Intra-EPG Isolation

Transit Routing

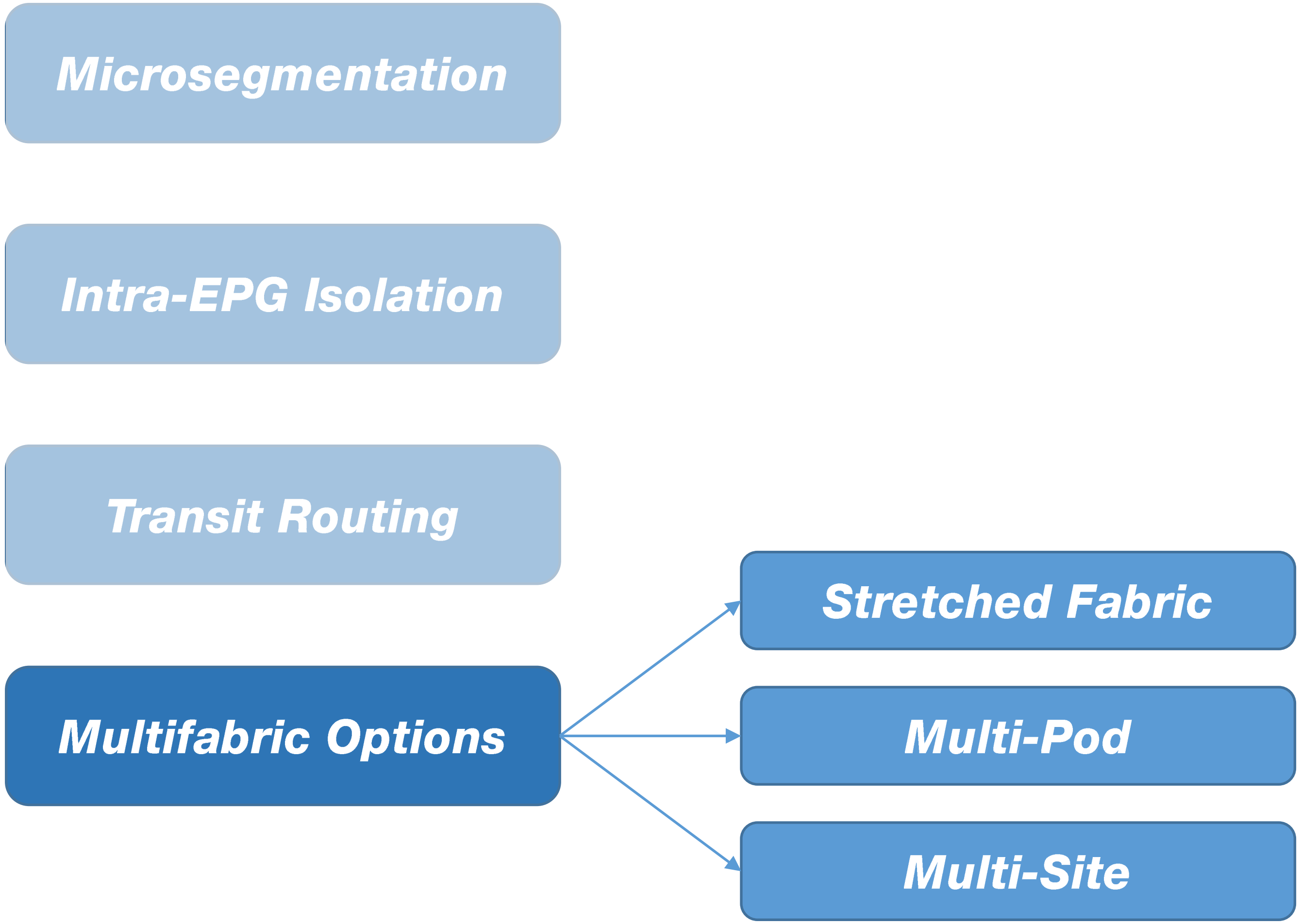
Multifabric Options

Example:Transit Routing



- Not limited to two exit point, depending on the required topology/configuration
- Require planning and caution when redistribuiting routing information

Multifabric Options



Multifabric Options: Stretched Fabric

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

What is it?

Stretched ACI fabric is a partially meshed design that connects ACI leaf and spine switches distributed in multiple locations.

Where is it used?

In multi-site scenarios where full mesh connectivity may be not possible or may be too costly.

Multiple sites, buildings, or rooms can span distances that are not serviceable by enough fiber connections or are too costly to connect each leaf switch to each spine switch across the sites.

Multifabric Options: Stretched Fabric

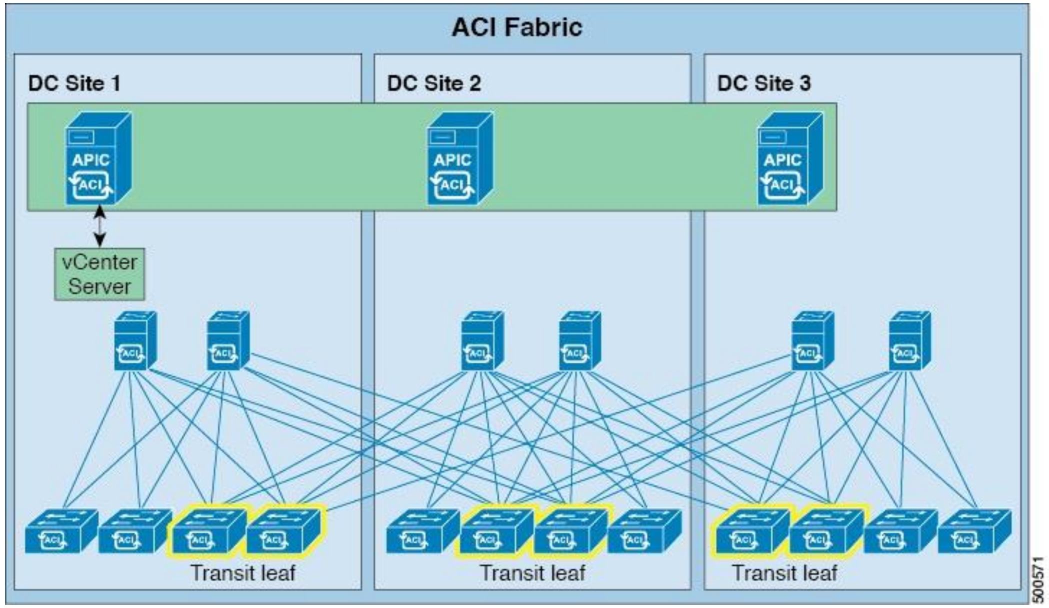
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Example: Stretched Fabric



- Single ACI fabric
- One administration domain and one availability zone
- Live VM migration capability across the sites
- Validated design , on up to three interconnected sites

Multifabric Options: Stretched Fabric

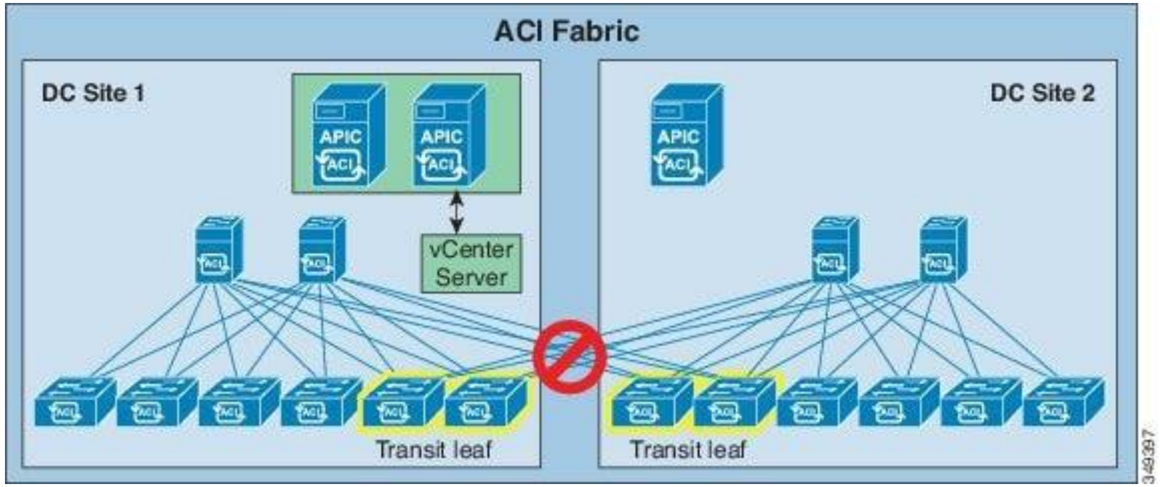
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Fault Example: Stretched Fabric



- The split fabrics continue to operate independently.
- The split fabric site with two APIC controller nodes (site 1) has quorum
- The split fabric site with one APIC controller nodes (site 2) has no quorum (minority)
- Split brain has no impact to the function of the fabric other than controller in site 2 is in the read only mode.

Multifabric Options: Multi-Pod

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

What is it?

Multi-Pod solution is an evolution of the stretched-fabric
A Multi-Pod design consists of a single APIC domain with multiple leaf-and-spine networks (pods) interconnected. As a consequence, a Multi-Pod design is functionally a single fabric (an interconnection of availability zones), but it does not represent a single network failure domain, because each pod runs a separate instance of control-plane protocols.
A layer 3 interpod network (called IPN) is used to provide connection between pods.

Where is it used?

- Used to interconnect separate Data Centers
- Active/Active deployement (Single Fabric)

Multifabric Options: Multi-Pod

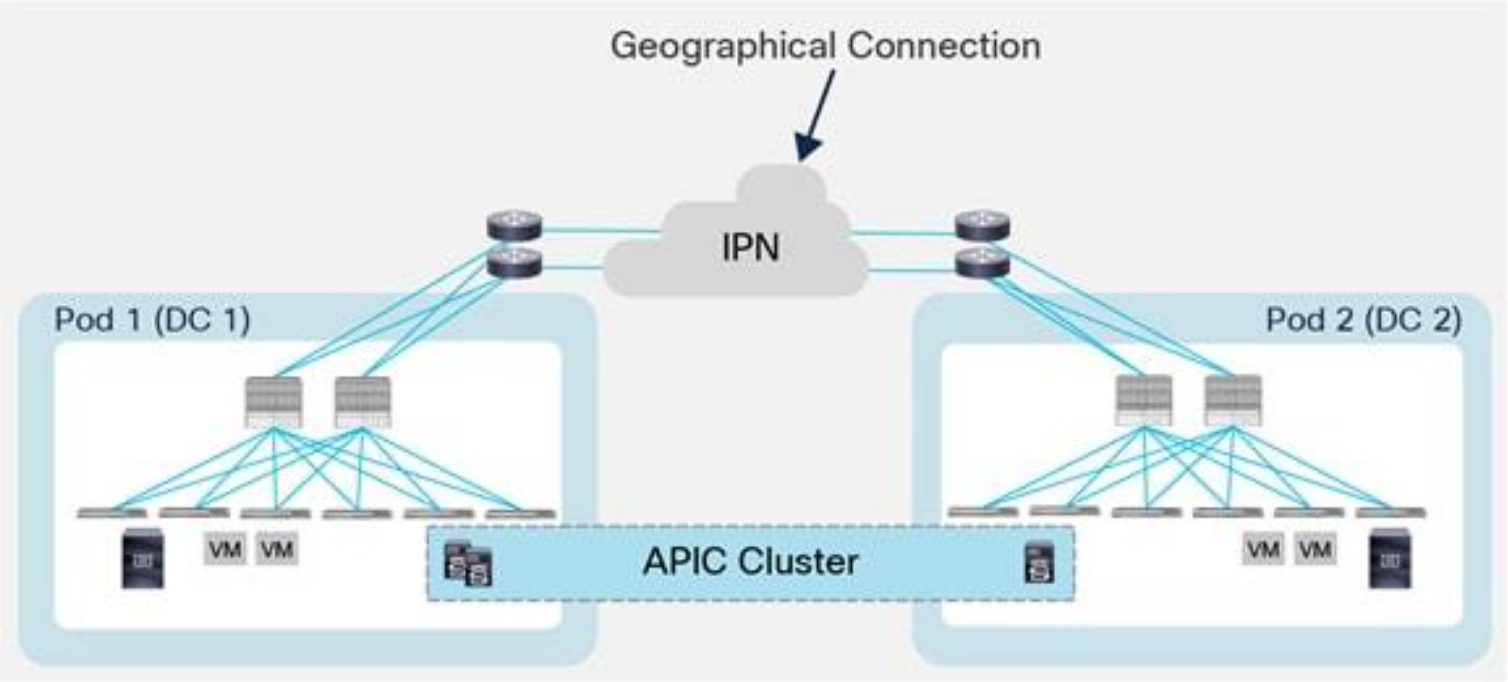
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Common Use



Multifabric Options: Multi-Pod

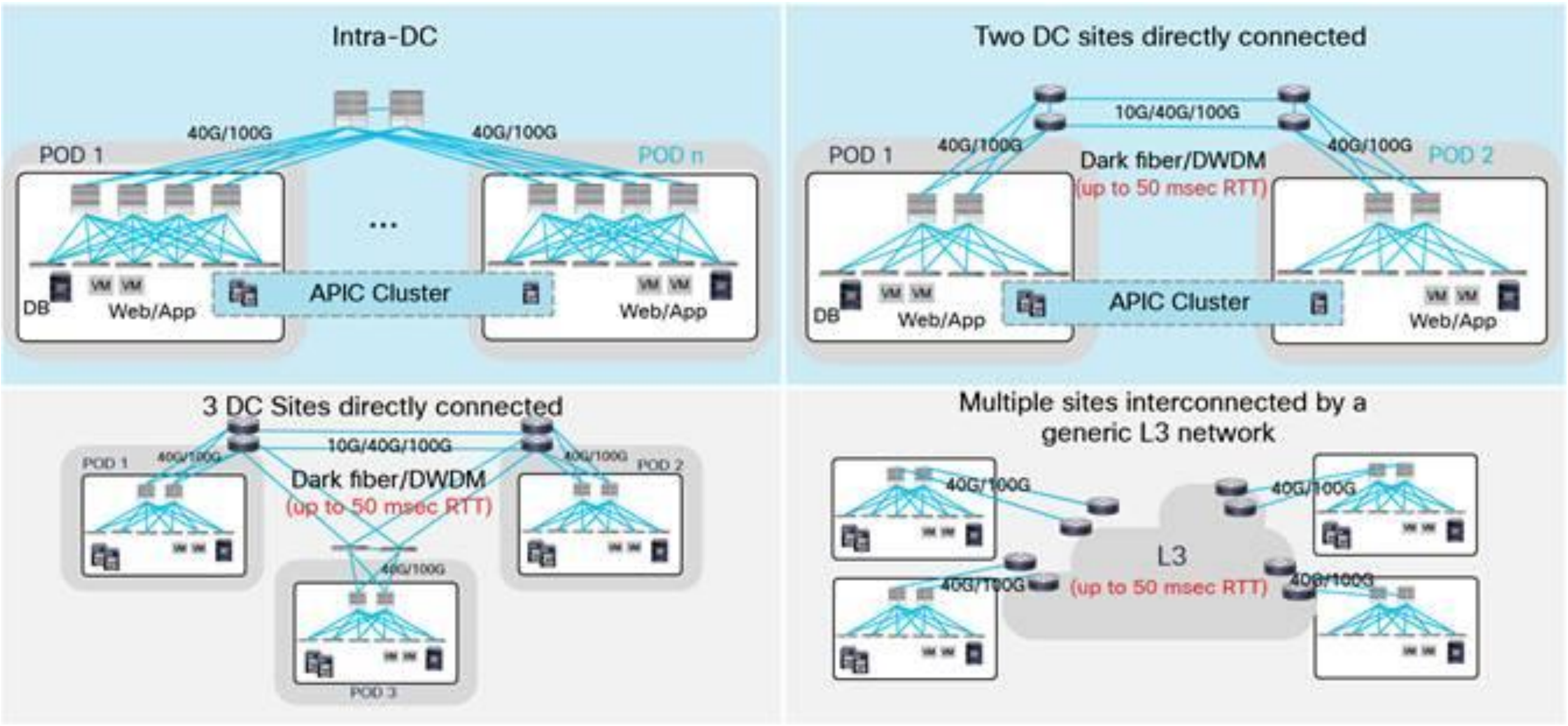
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Supported Design



Multifabric Options: Multi Site

Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

What is it?

A Multi-Site design is the architecture interconnecting multiple APIC cluster domains with their associated pods. A Multi-Site design could also be called a Multi-Fabric design, because it interconnects separate regions (fabrics) each deployed as either a single pod or multiple pods (a Multi-Pod design).

Where is it used?

- To interconnect separate Cisco ACI fabrics
- To address the need of complete isolation across separate cisco ACI Network (against network level failure, configuration/policy definition error propagation)
- To provide connectivity to public cloud resources (AWS, Azure)

Multifabric Options: Multi-Site

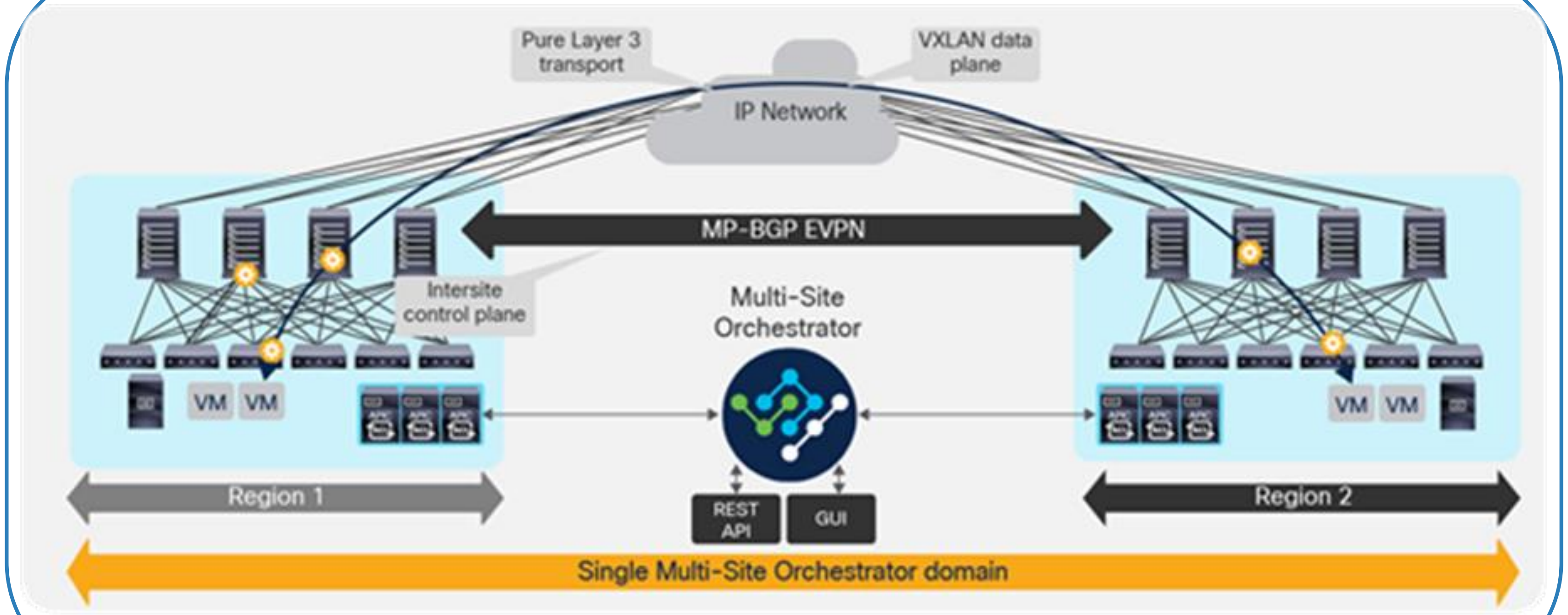
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

Multi-site Aechitecture



Multifabric Options: Recap

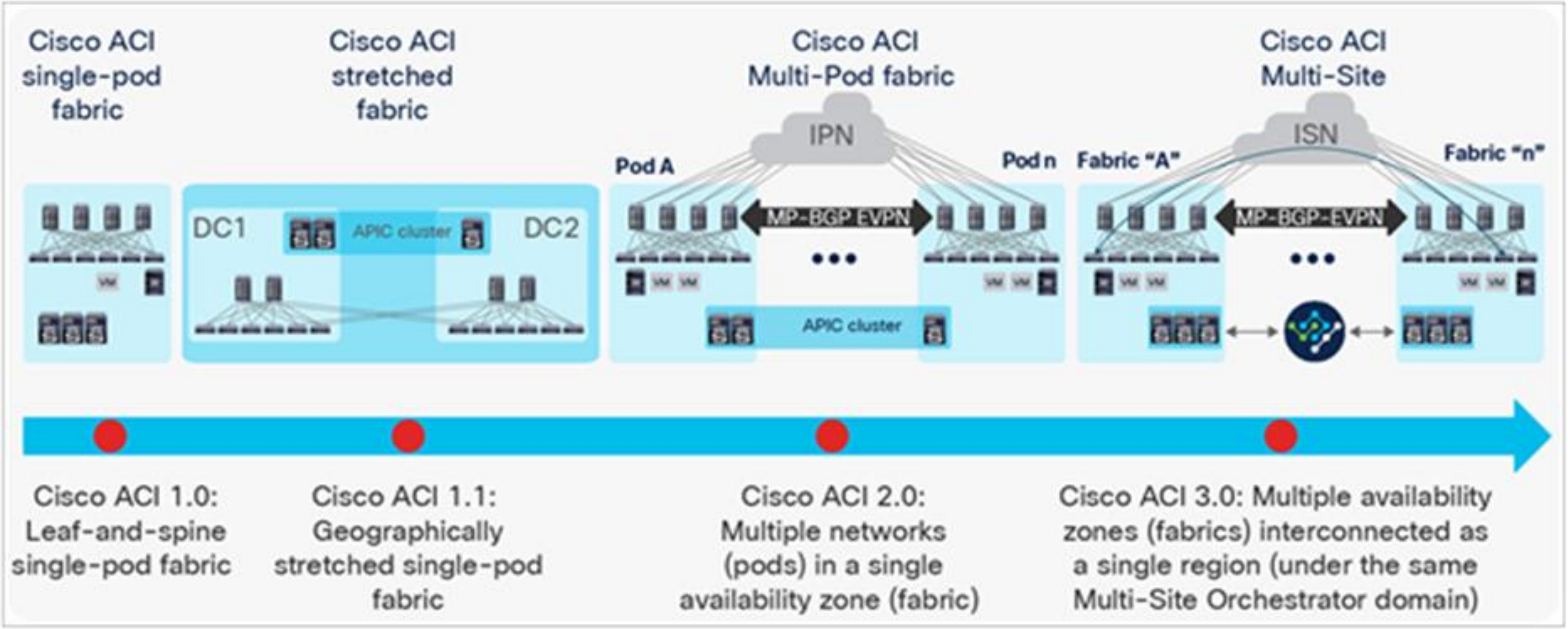
Microsegmentation

Intra-EPG Isolation

Transit Routing

Multifabric Options

ACI Connectivity evolution



Cisco ACI 1.0: Leaf-and-spine single-pod fabric

Cisco ACI 1.1: Geographically stretched single-pod fabric

Cisco ACI 2.0: Multiple networks (pods) in a single availability zone (fabric)

Cisco ACI 3.0: Multiple availability zones (fabrics) interconnected as a single region (under the same Multi-Site Orchestrator domain)

ACI APIs & Automation

POSTMAN

acitoolkit

ANSIBLE

«Say, J.A.R.V.I.S., is it that time?»
*«The **House Party Protocol**, sir?»*
«Correct.»

DEMOLAB9

DATA CENTER COLLABORATION NETWORK APPLICATIONS SECURITY

www.maticmind.it