MATICMIND®

MAKES IT EASY

Cisco ACI Training Course - TIM

DAY2 – Tenant & Fabric Access Configuration

November 2020

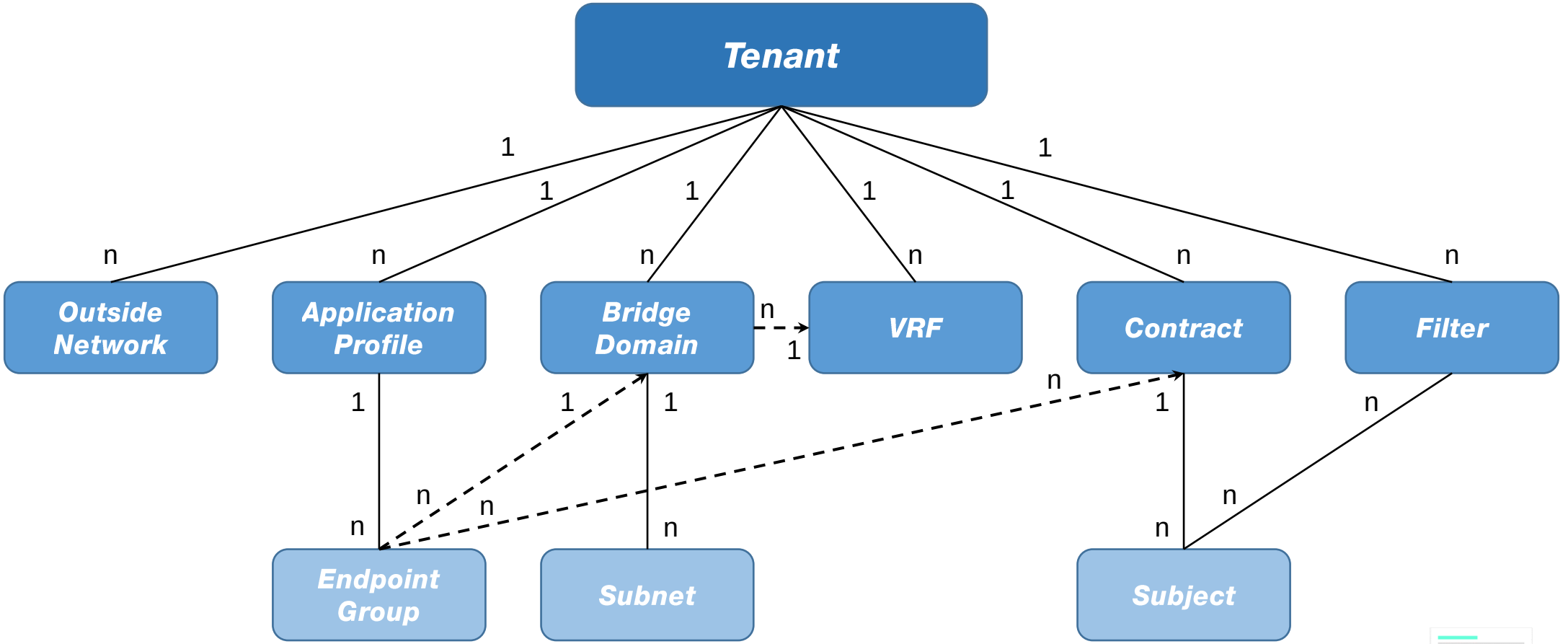
AGENDA DAY2

1. Tenant Configuration
    1. PART I
        1. What is a Tenant in Cisco ACI?
        2. VRF & Bridge Domain (BD)
        3. Hands-On LAB2
        4. Application Profile (AP)
        5. EndPoint Group
        6. Hands-On LAB3
    2. PART II
        1. Contracts
        2. Contract Subjects
        3. Contract Components
        4. Contract Directions
        5. Hands-On LAB4
    3. PART III
        1. Outside Networks (L2Out – L3Out)
        2. L3Out Evolution
        3. Hands-On LAB5

AGENDA DAY2

2. Fabric Access
    1. VPC Domains
    2. Switch Profiles
    3. Interface Policies & IPGs
    4. Leaf Interface Profiles
        1. Leaf Interface Profile & Switch Profile Association
    5. DEMO LAB6
    6. FEX & Connection to Leaves
        1. FEX Profiles & Association to Switch Profile
    7. Physical Domain & VLAN Pool
    8. Attachable Access Entity Profile
    9. EPG Deployment
        1. DEMO LAB 7

Tenant Configuration

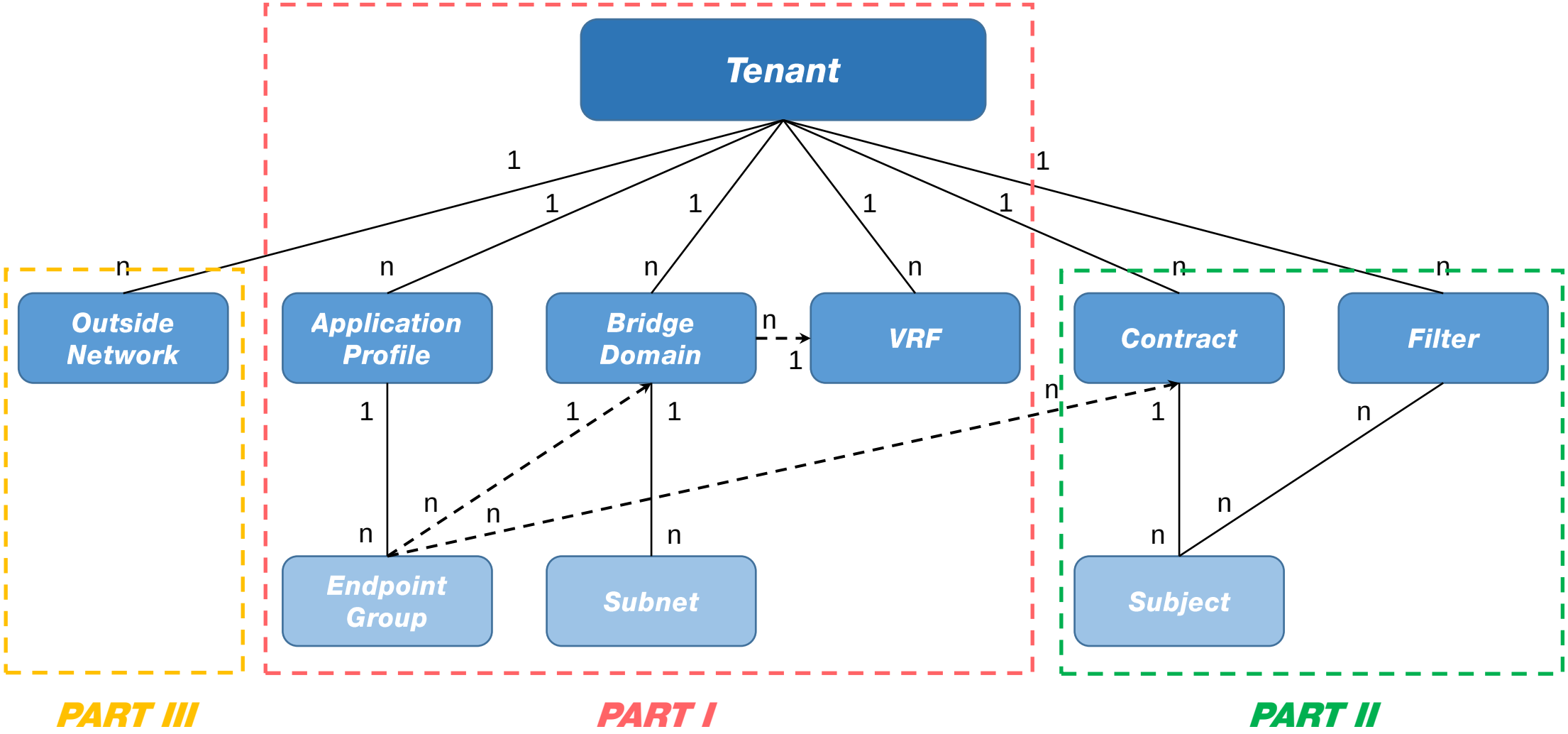


Legend

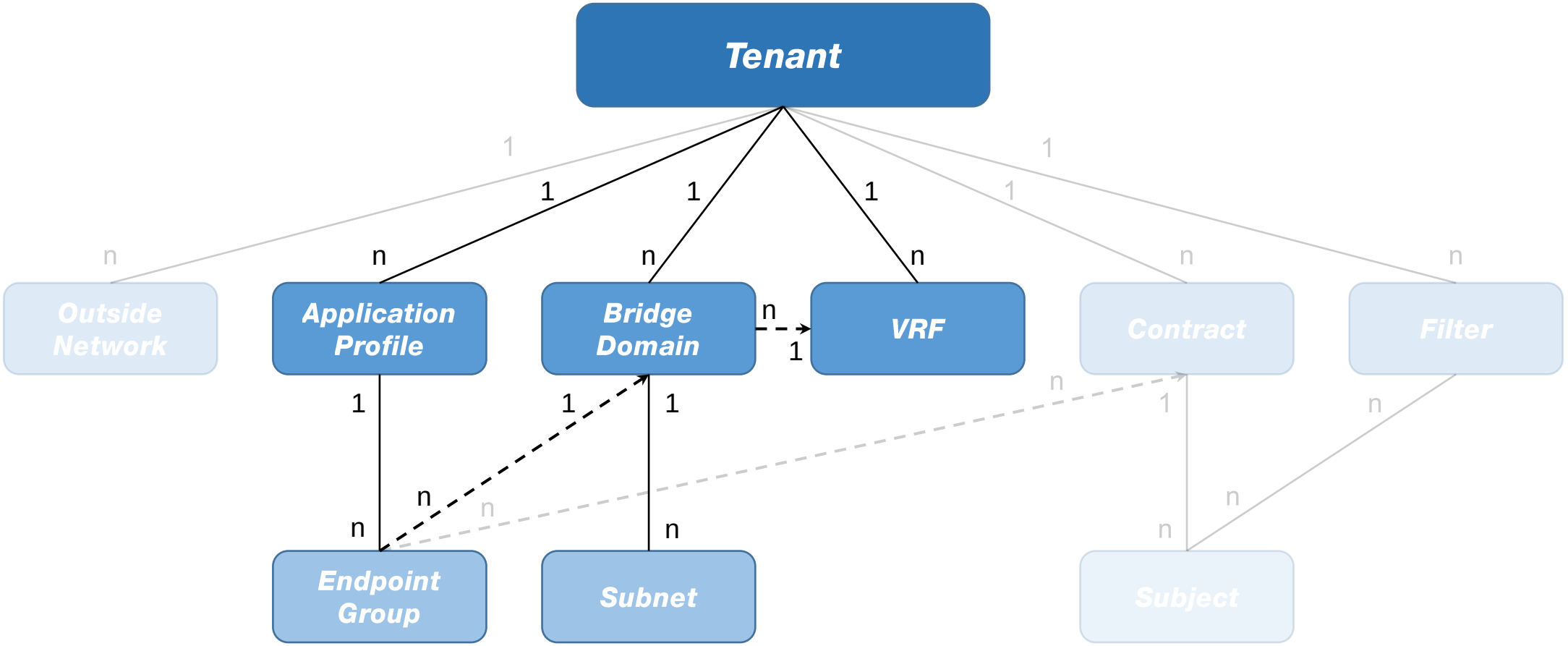
- Solid line: indicates that an object contains the one below.
- Dotted line: indicates a relationship.

Cisco Guide

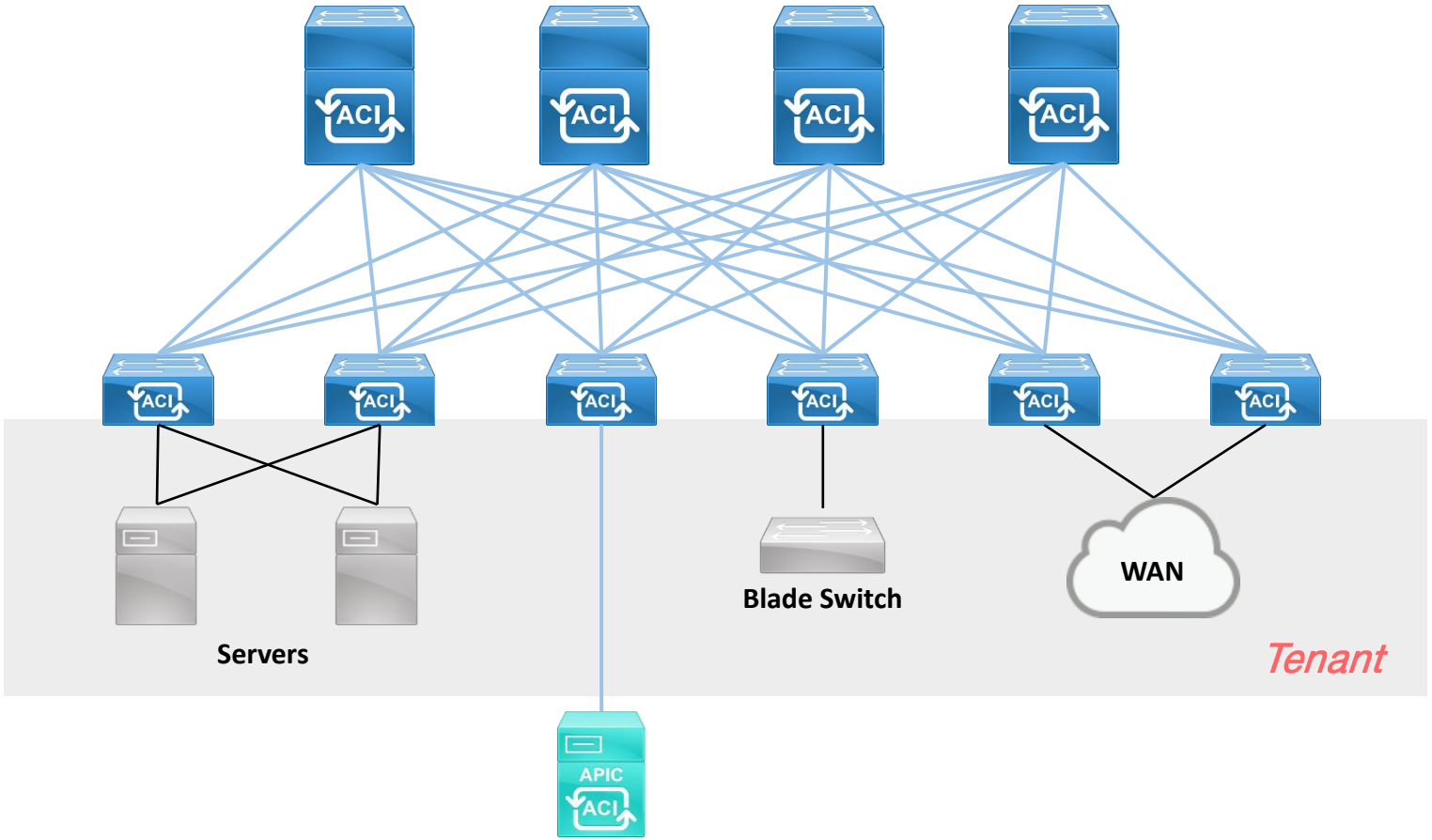
Cisco ACI - Tenant Configuration



Tenant Configuration – PART I



What is a Tenant in Cisco ACI?



A **TENANT** is a logical container for application policies that enable an administrator to exercise domain-based access control.

Examples of tenants are:

- A customer in a service provider setting,
- An organization or domain in an enterprise setting,
- A convenient grouping of policies.

What is a Tenant in Cisco ACI?

User Tenant

User tenants are **defined by the administrator**. They contain policies that govern the operation of resources such as applications, databases, web servers, network-attached storage, virtual machines, …

Common Tenant

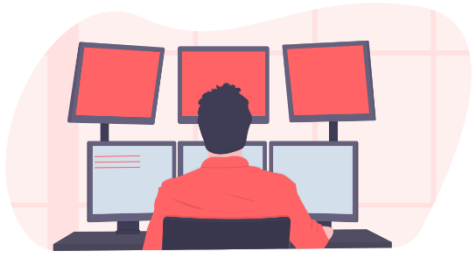
The common tenant is **provided by the system** but can be configured by the fabric administrator. It contains policies that *govern the operation of resources accessible to all tenants*, such as firewalls, load balancers, Layer 4 to Layer 7 services, IDS appliances, …

Infrastructure Tenant

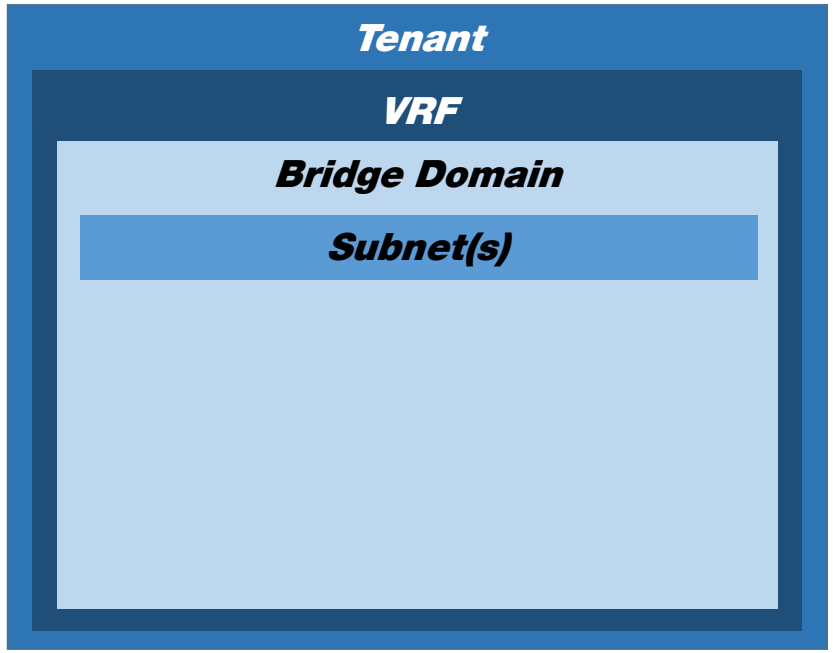
The infrastructure tenant is **provided by the system** but can be configured by the fabric administrator. It contains policies that *govern the operation of infrastructure resources* such as the fabric VXLAN overlay.

Management Tenant

The management tenant is **provided by the system** but can be configured by the fabric administrator. It contains policies that *govern the operation of fabric management functions* used for in-band and out-of-band configuration of fabric nodes. The management tenant contains a private out-of-bound address space for the APIC/fabric internal communications that is outside the fabric data path that provides access through the management port of the switches.



VRF & Bridge Domain (BD)



VRF

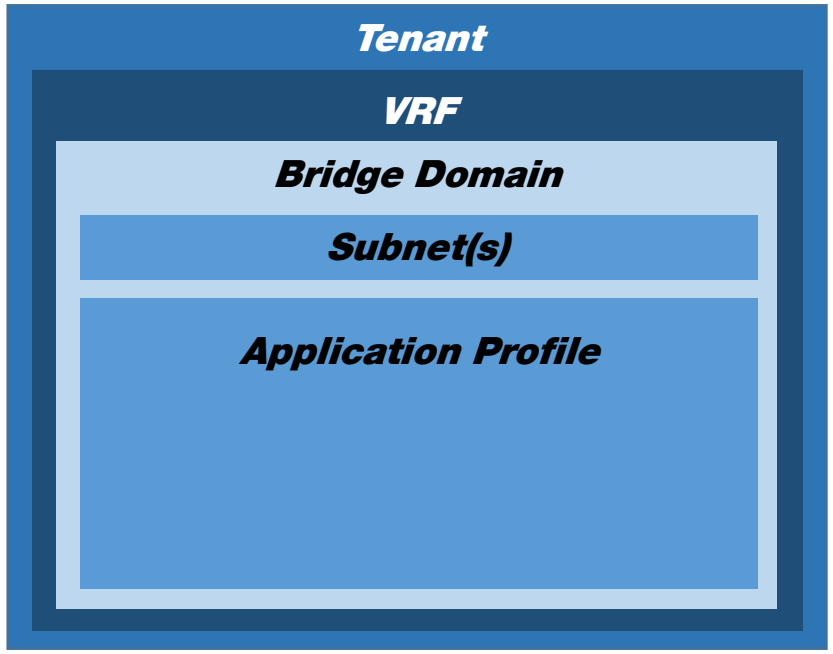
A Virtual Routing and Forwarding (VRF) is a representation of a private Layer3 name space and is a unit of isolation in the Cisco ACI environment. Each tenant can have one or more VRF. Because VRFs use separate forwarding instances, IP addressing can be duplicated in separate VRFs for multitenancy.

Bridge Domain

Bridge domains are containers for IP subnets and can be used to define a Layer2 boundary. Bridge domains are overlays that are contained within the VRF. These bridge domains are, in fact, virtual VXLANs. VXLANS allow a device on subnet A to communicate directly with a device on subnet B (VXLAN Bridging). You can even allow the device on subnet A to communicate directly with the device on subnet D in a different VXLAN (VXLAN Routing). The devices that are communicating are not required to be on the same subnet.

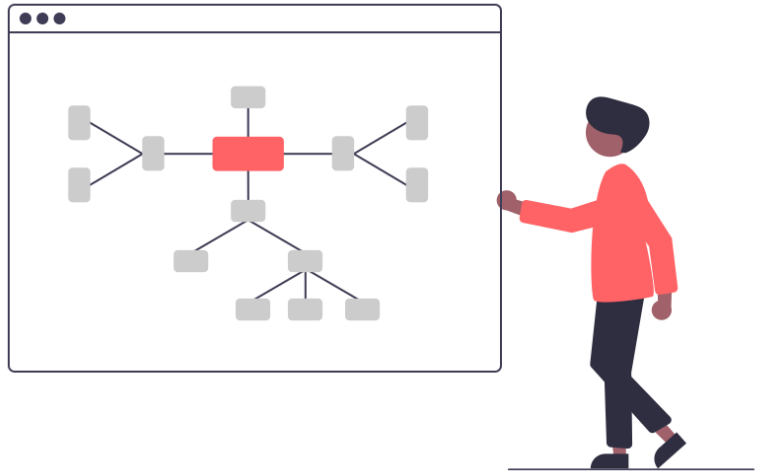
HANDS-ON LAB 2

Application Profiles (AP)

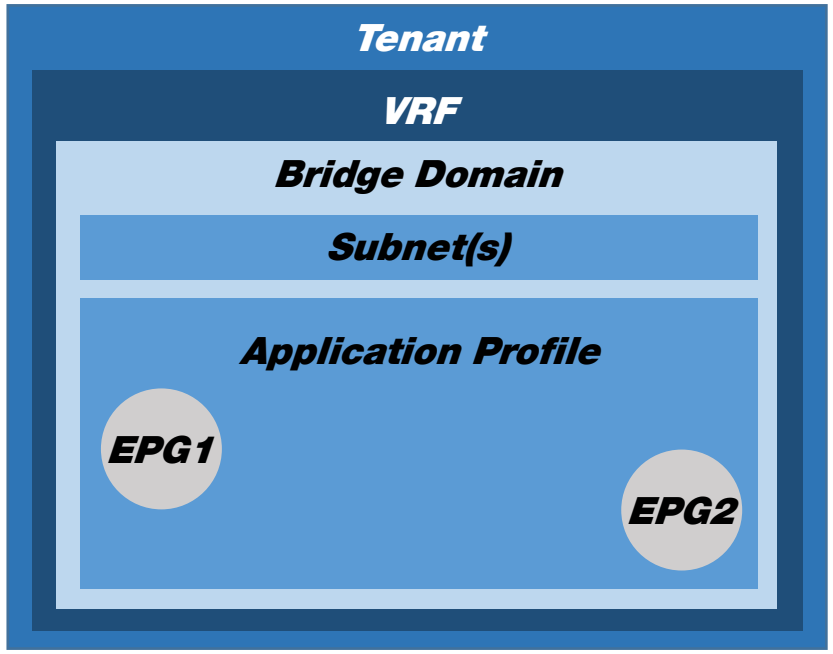


Application Profile

An application profile defines the policies, services and relationships between endpoint groups (EPGs). Modern applications contain multiple components (web server, database server, access to outside resources,…). The application profile contains as many EPGs as necessary that are logically related to provide the capabilities of an application.



EndPoint Group (EPG)



EPG

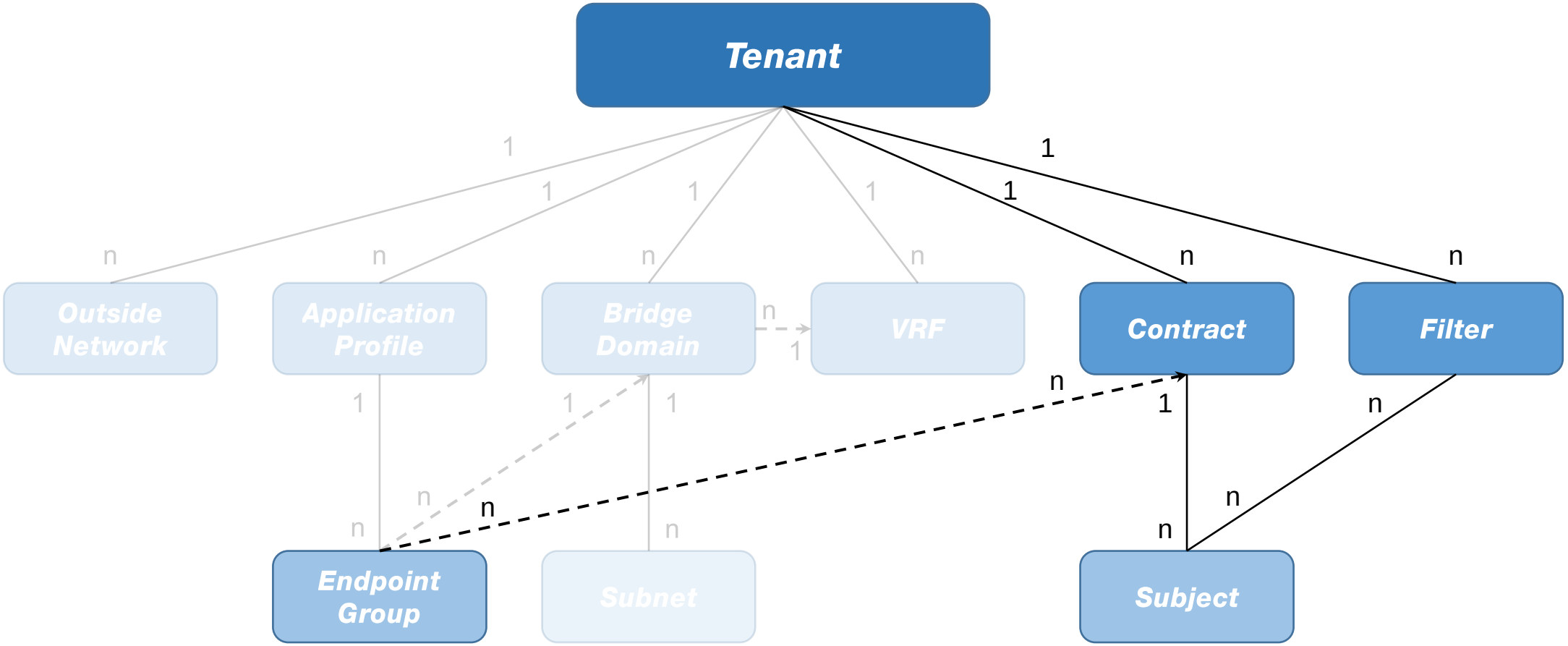
Endpoint groups are groupings of applications or application components that are independent of other network constructs. In other words, an EPG is a container for endpoints with similar policies. Notice that endpoints may be physical or virtual entities.

Examples of EPGs are:

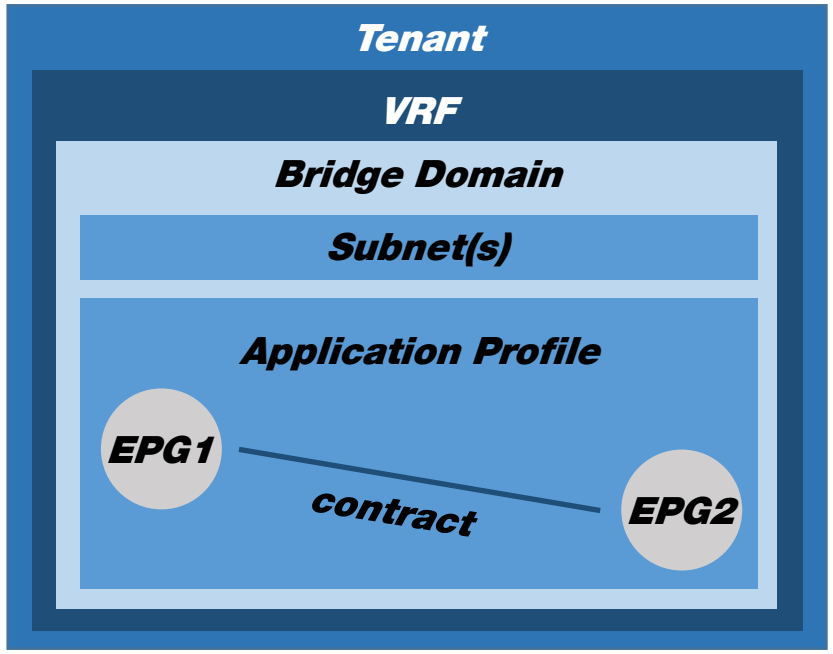
- Application EPGs
- Layer 2 external network EPGs
- Layer 3 external network EPGs

Hands-on LAB 3

Tenant Configuration – PART II



Contracts

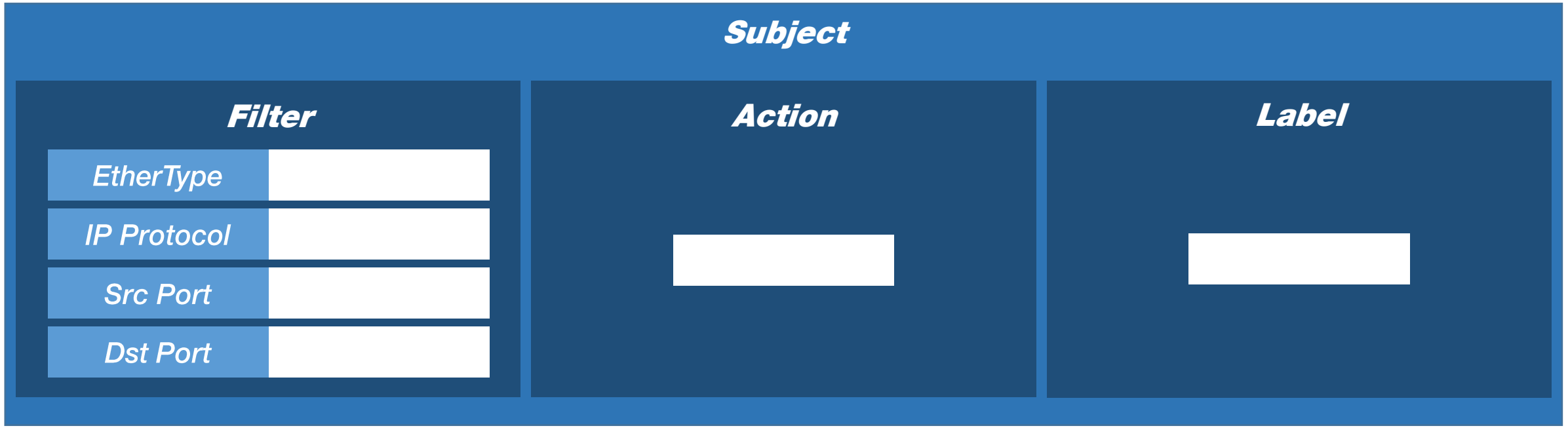


Contract

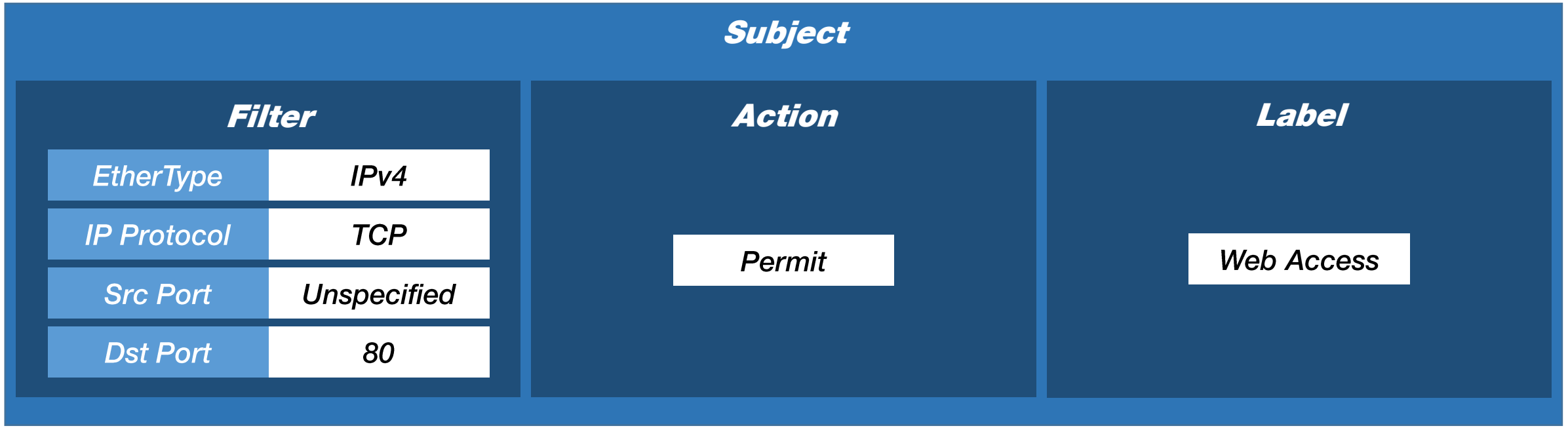
A contract defines communication between EPGs, specifying what is permitted, action to take and so on. An administrator uses a contract to select the type(s) of traffic that can pass between EPGs, including the protocols and ports allowed. Contracts contains logical subcomponents:

- Subjects
- Filters
- Actions
- Labels

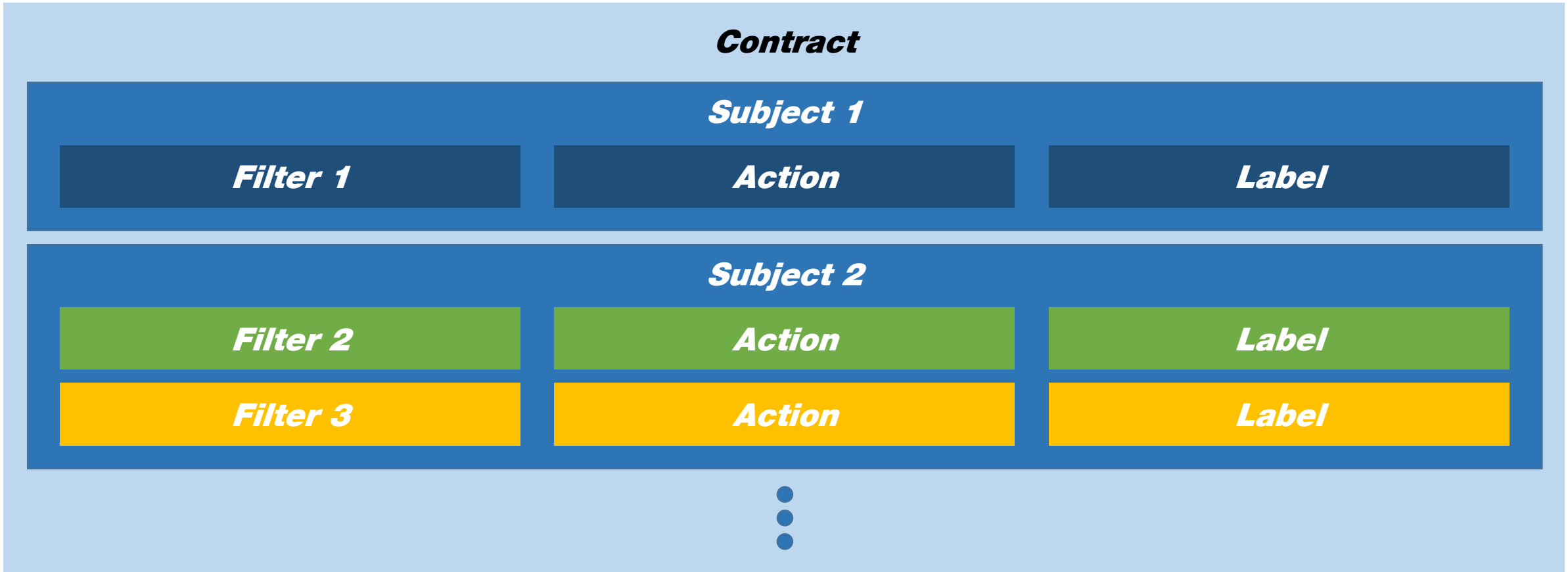
Contract Subject



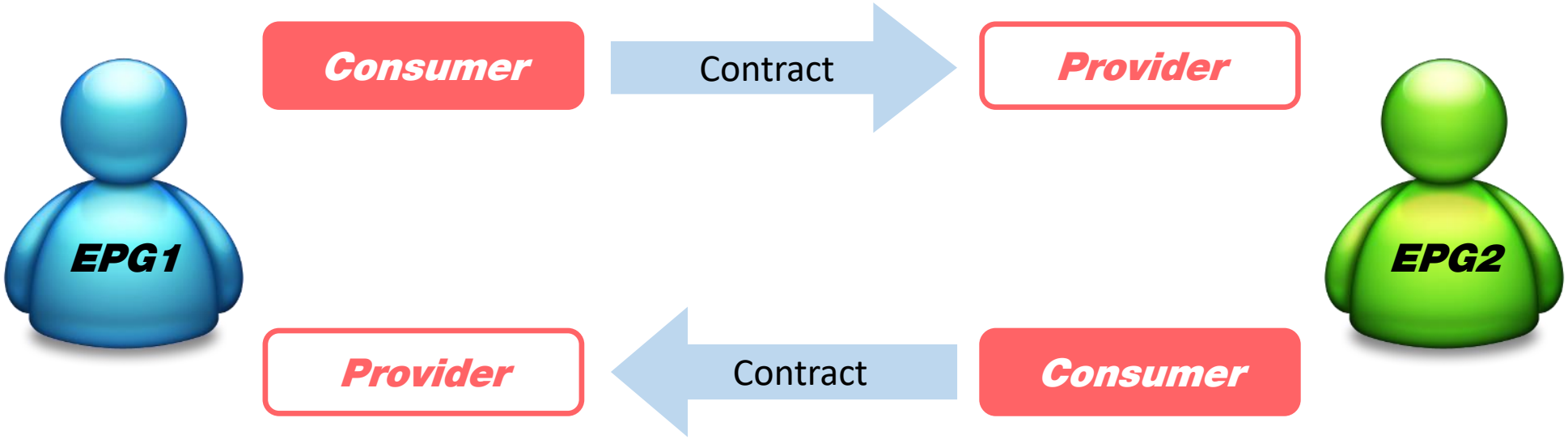
Contract Subject



Contract Components

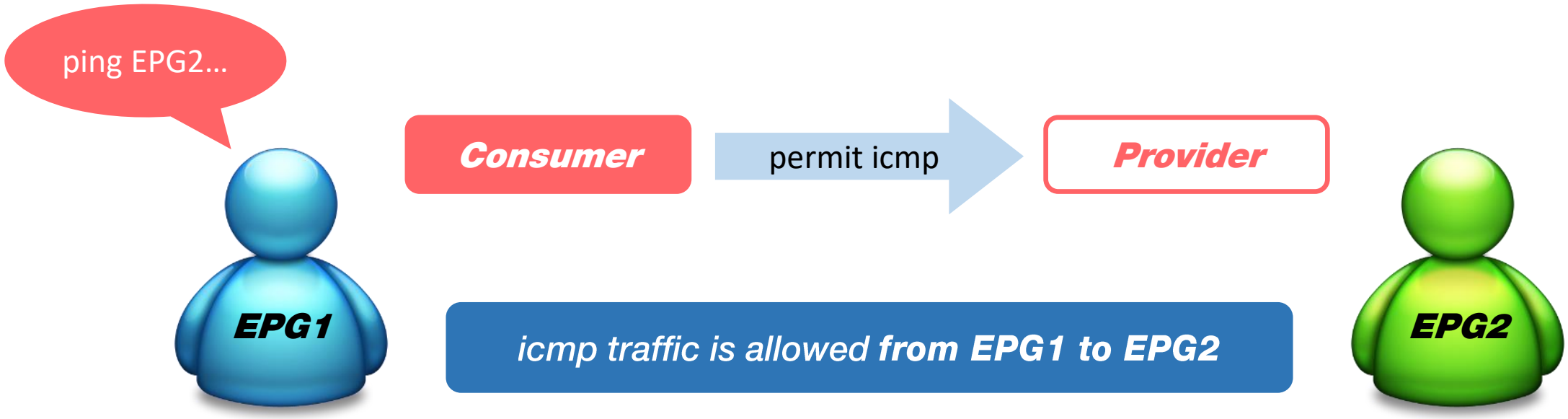


Contract Directions



Contract Directions

Example: permit icmp



Contract Directions

Example: permit icmp

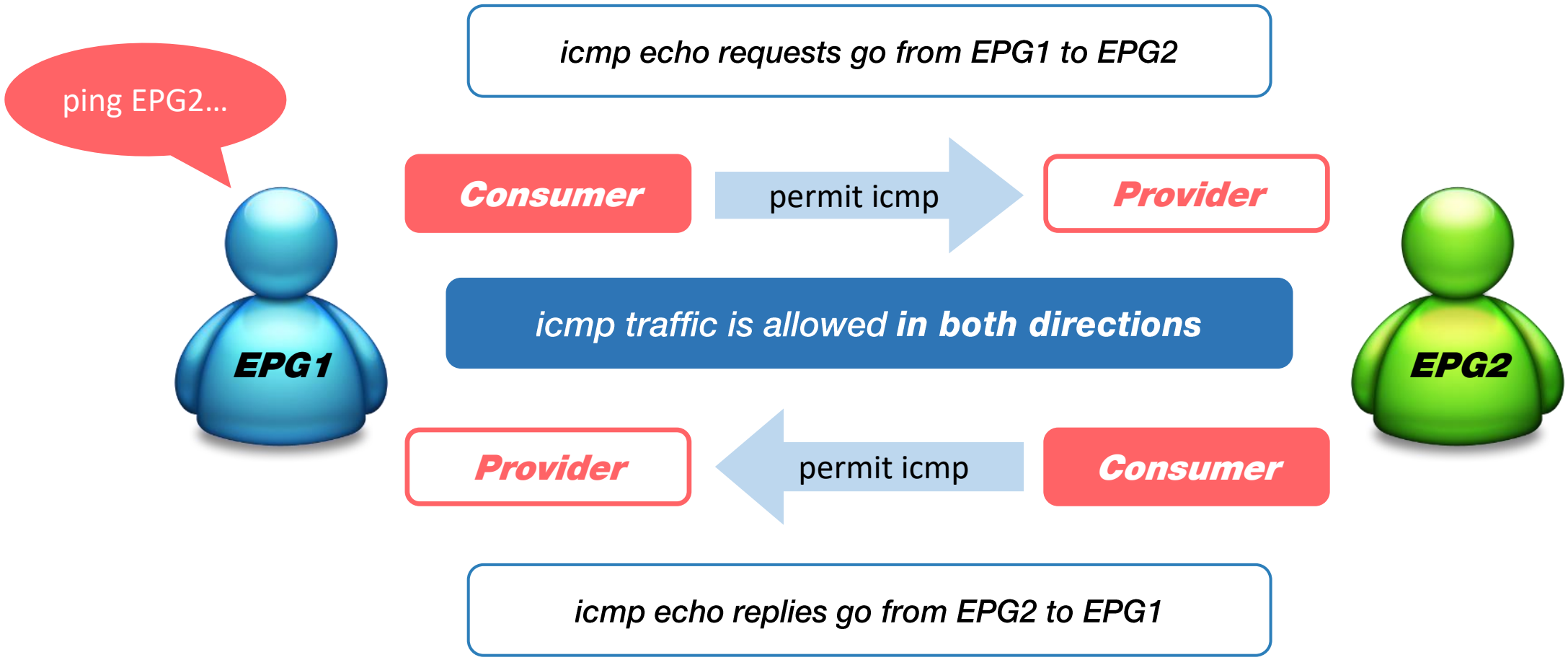
*icmp traffic is allowed **from EPG2 to EPG1***

icmp echo requests go from EPG2 to EPG1

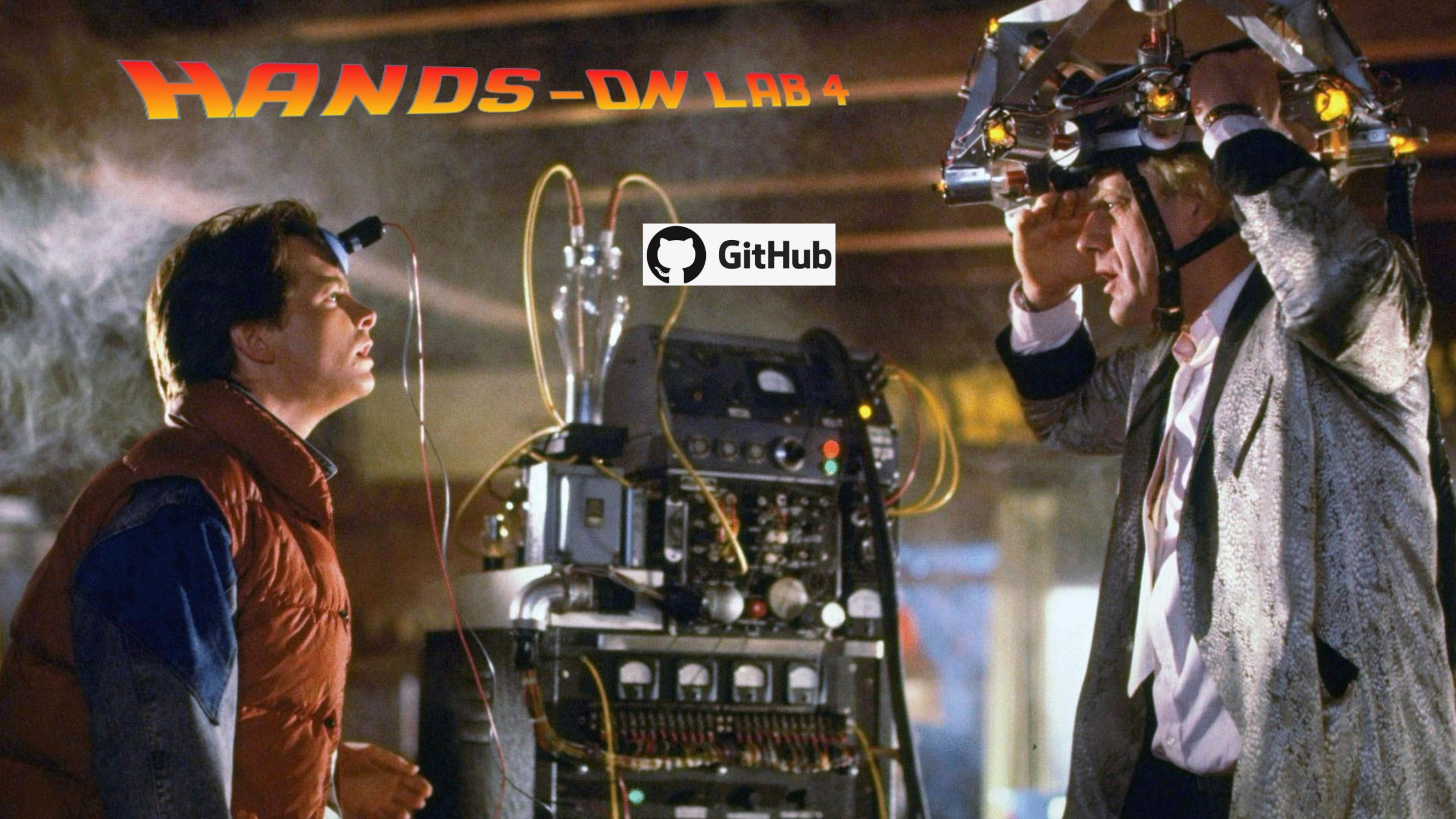
icmp echo replies from EPG1 to EPG2 are blocked

Provider ← permit icmp ← **Consumer**

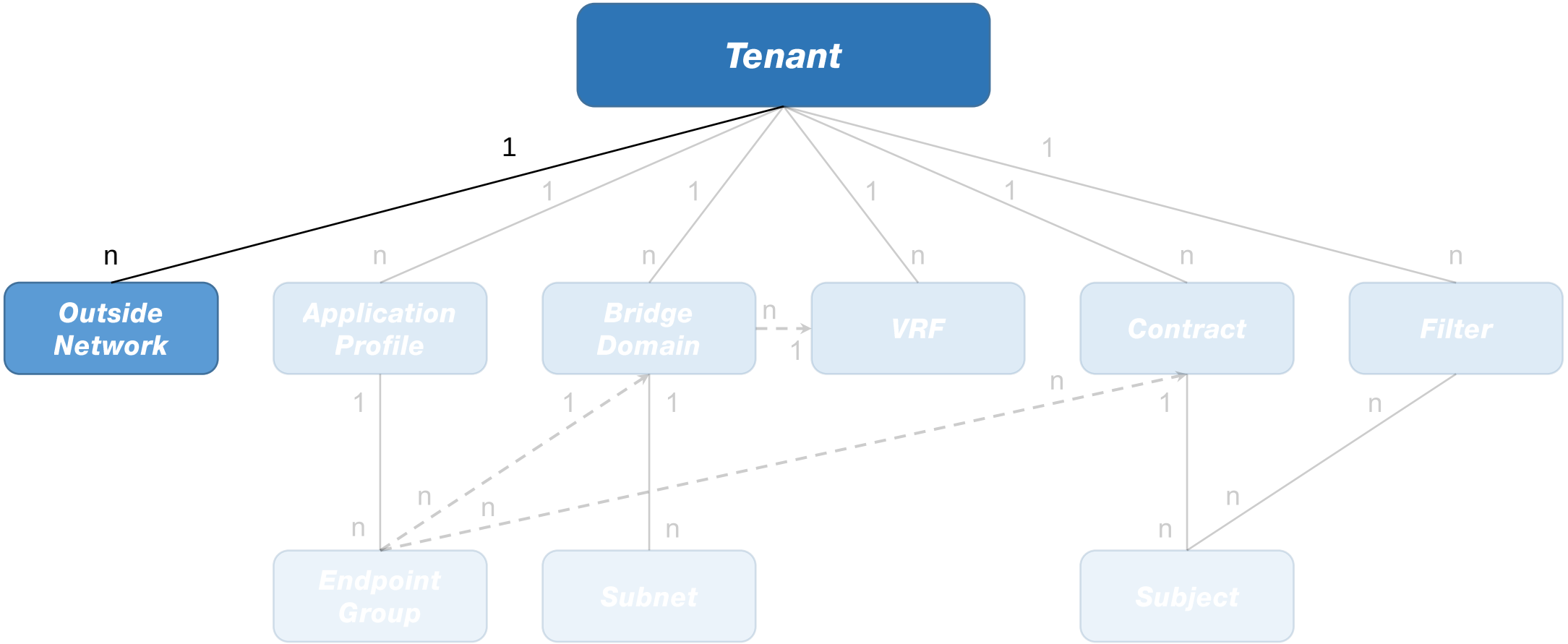
Contract Directions



HANDS-ON LAB 4



Tenant Configuration – PART III



Outside Network (L2Out - L3Out)

L2Out

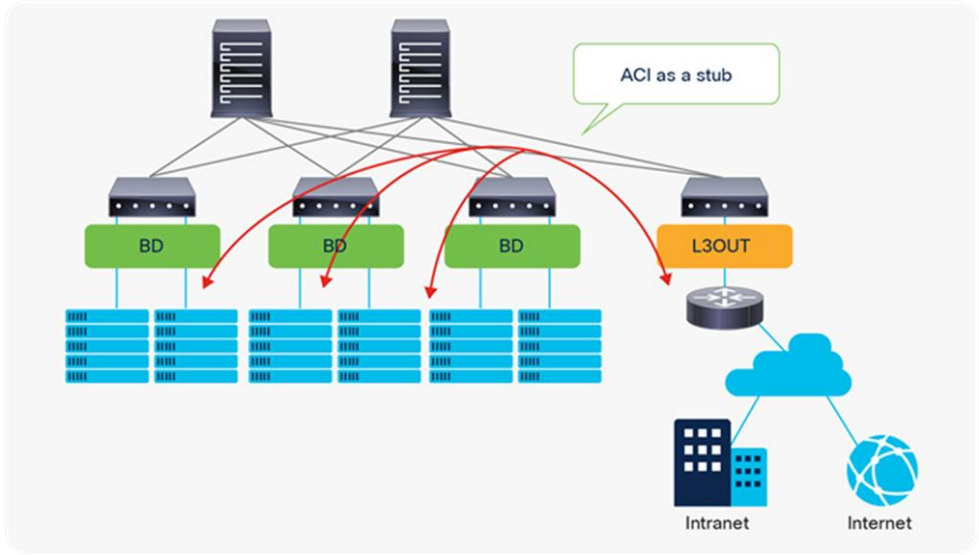
Provides L2 Extension from fabric to outside networks:
Usually associated with a bridge domain and it is designed to extend the whole bridge domain (not an individual EPG under bridge domain) to the outside network.

L3Out

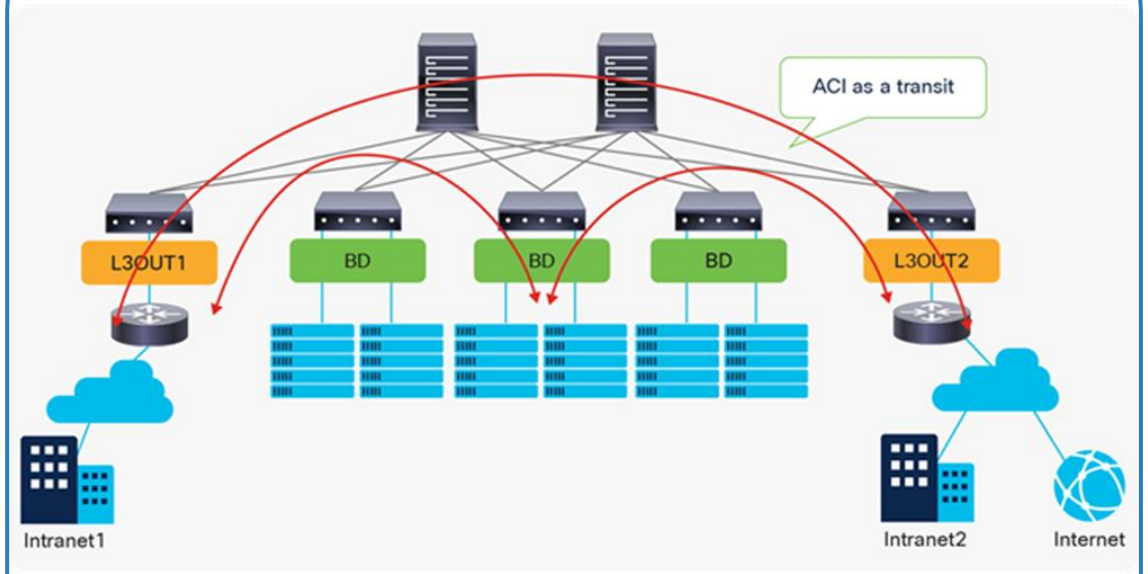
Set of configurations that define connectivity from ACI to external networks, via routing protocols or static route, allowing servers connected to the Fabric to reach outside destinations.

Outside Network: L3Out Evolution

L3Out Before



L3Out After



Outside Network: L3Out Evolution

L3Out Key Functions

1. Learn external routes via routing protocols (or static routes)
2. Distribute learned external routes (or static routes) to other leaf switches
3. Advertise ACI internal routes (BD subnets) to outside ACI
4. Advertise learned external routes to other L3Outs (Transit Routing)
5. Allow traffic to arrive from or be sent to external networks via L3Out by using a contract

Outside Network: L3Out Evolution

L3Out Basic Component

- **VRF**

This is the VRF on which the L3Out and its routing protocol are deployed.

- **External routed domain**

This is the domain to allow the L3Out to use a set of interfaces and VLANs. (NOTE: Different pool from the Fabric Vlan Pool

- **Routing protocol**

Routing protocol that is deployed with the L3Out on the node and interface specified by the Logical Node/Interface Profile. Cisco ACI allows only one routing protocol per L3Out with one exception. BGP and OSPF can be configured in the same L3Out as an exception in order to be able to use OSPF as the IGP for BGP.

Outside Network: L3Out Evolution

L3Out Basic Configuration Procedure

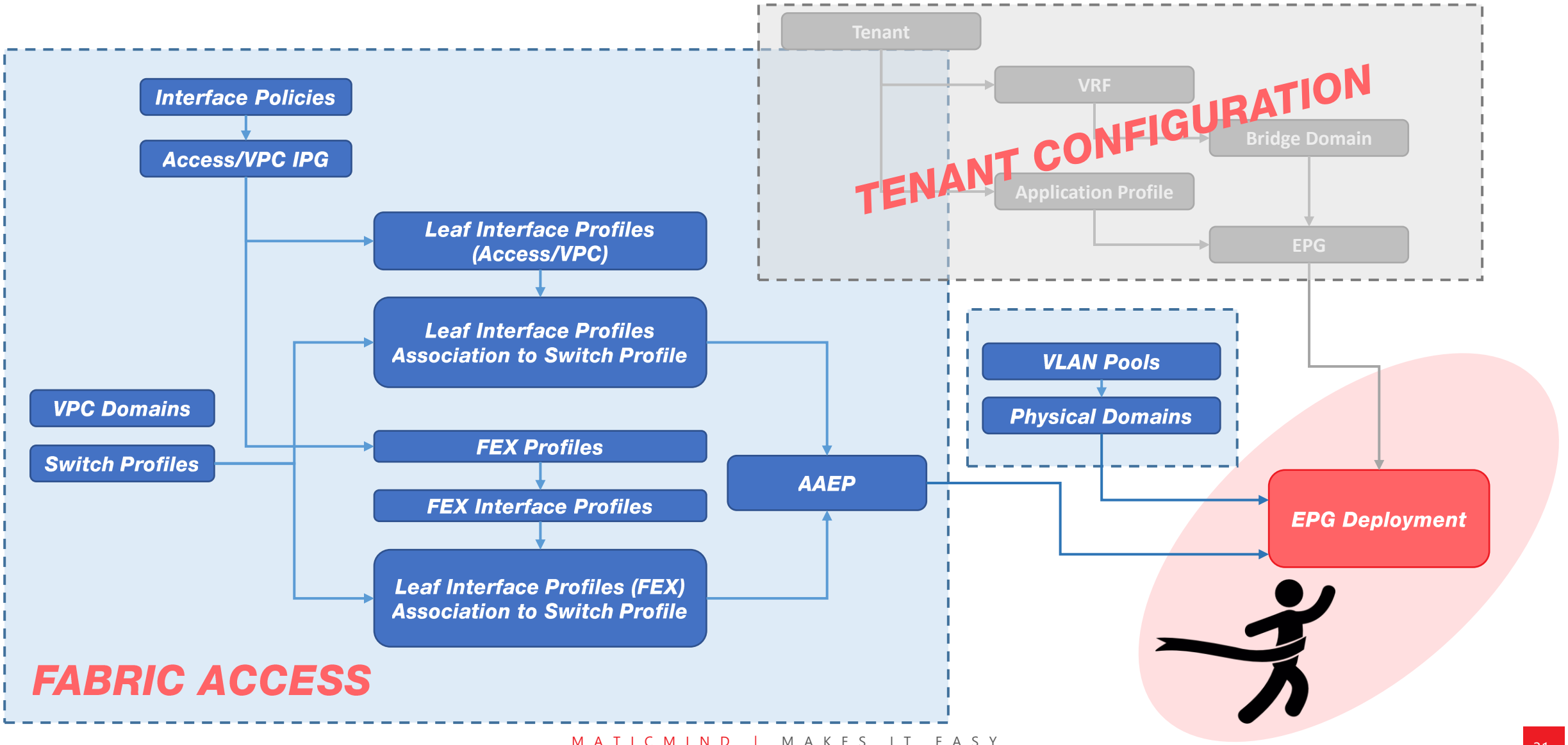
1. On the menu bar, click **Tenants**.
2. On the submenu bar, click *<Tenant_name>*.
3. In the Navigation pane, expand *<Tenant_name>* **-> Networking -> L3Outs**.
4. Right-Click on **L3Outs** and select **Create L3Out**.

--- *IDENTITY TAB* ---

1. In the **Create L3Out** dialog box, fill the **Name** field with *<L3OUT_Name>.*
2. From the drop-down menu **VRF** select *<VRF_Name>.*
3. From the drop-down menu **L3 Domain** select ***Create L3 Domain***.
4. In the **Create L3 Domain** dialog box, fill the **Name** field with *<L3Domain_name>*
5. From the drop-down menu **Associate Attachable Entity Profile** select *<AAEP_name>*
6. From the drop-down menu **VLAN Pool** select ***Create VLAN Pool***
7. In the **Create VLAN Pool** dialog-box, fill the **Name** field with *<Vlan_POOL_Name>*
8. In the **Allocation Mode** field, select **Static Allocation**
9. Choose **Static Allocation** for the **Allocation Mode**.
10. Click on "**+**" button next to **Encap Blocks** field.
11. Fill the two empty forms in the **Range** field with values required (repeat if not consecutive vlans).
12. Click the **OK** button.
13. In the **Create VLAN Pool** dialog box, click the **Submit** button.
14. In the **Create Physical Domain** dialog box, click the **Submit** button.


DEMO LAB 5

Fabric Access



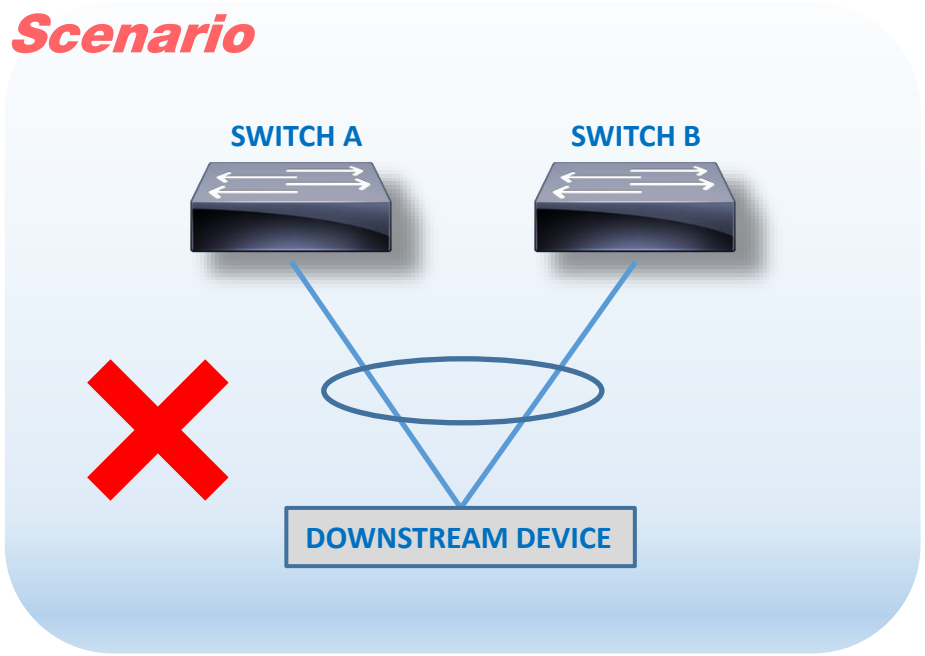
VPC Domains

What is a VPC?

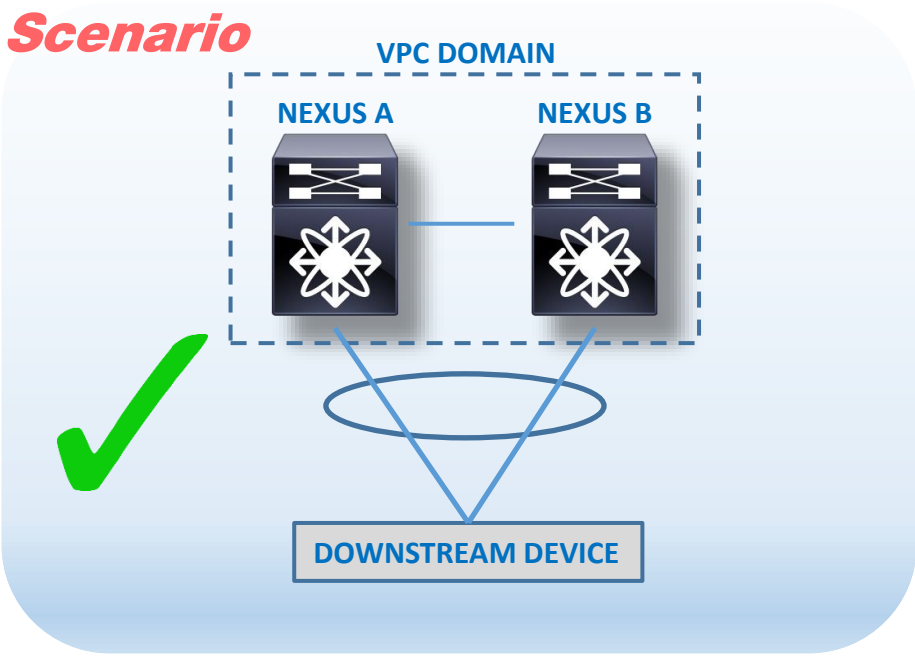
Virtual PortChannels (vPCs) allow links that are physically connected to two different Cisco® switches to appear to a third downstream device to be coming from a single device and as part of a single PortChannel. The third device can be a switch, a server, or any other networking device that supports IEEE 802.3ad PortChannels.

Cisco NX-OS Software vPCs and Cisco Catalyst® Virtual Switching Systems (VSS) are similar technologies. For Cisco EtherChannel technology, the term “multichassis EtherChannel” (MCEC) refers to either technology interchangeably.

IOS Scenario

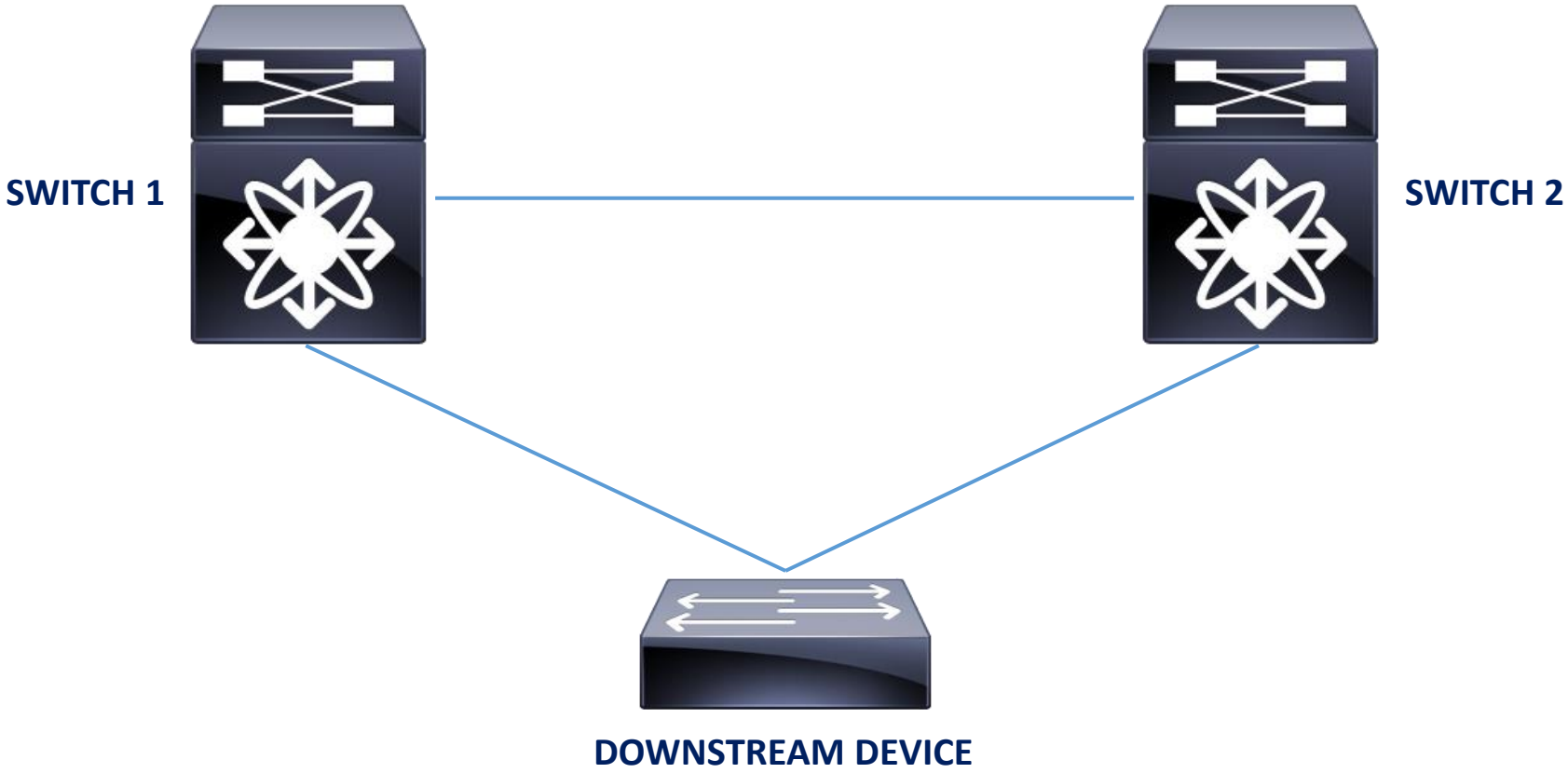


NX-OS Scenario



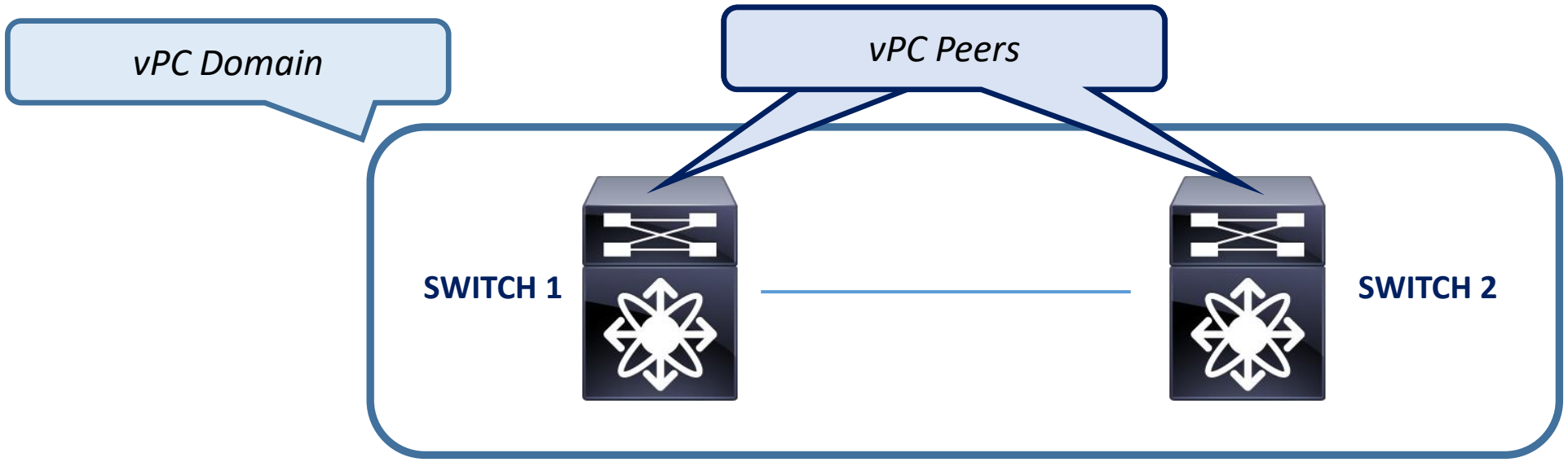
VPC Domains

Basics & Terminology



VPC Domains

Basics & Terminology

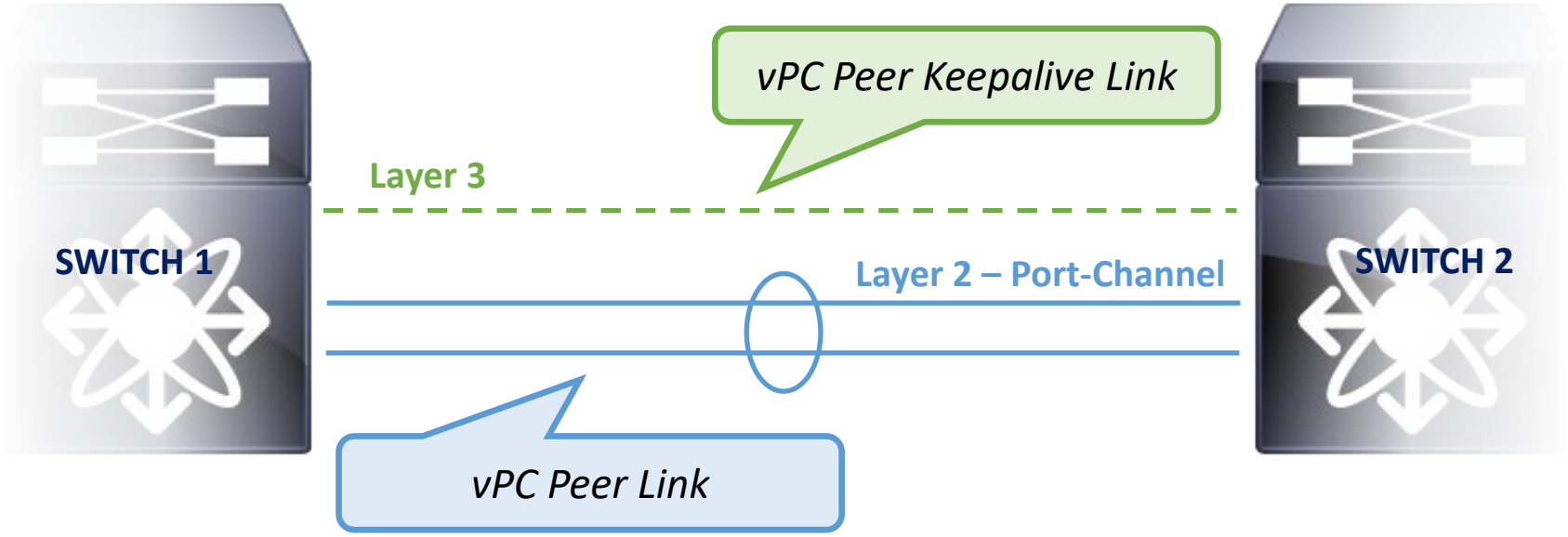


vPC Peers: the two Cisco Nexus switches combined to build a vPC architecture are referred to as vPC peers. *This pair of switches acts as a single logical switch*, which enables other devices to connect to the two chassis using vPC.

vPC Domain: This is a pair of vPC peer switches combined using vPC configuration. A vPC domain is created using two vPC peer devices that are connected using a vPC peer keepalive link and a vPC peer link. A numerical domain ID is assigned to the vPC domain. *A peer switch can join only one vPC domain.*

VPC Domains

Basics & Terminology

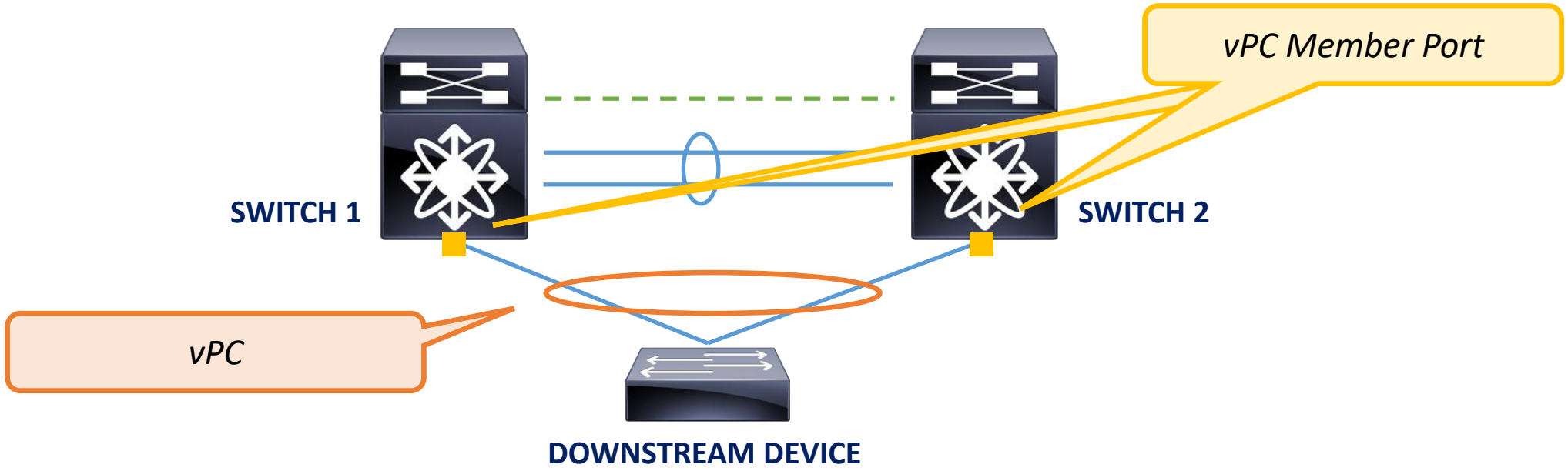


vPC Peer Link: this is a link between two vPC peers to *synchronize state*. The vPC peer link is the most important connectivity element in the vPC system. vPC peer link *must* be built using at least two physical 10G interfaces bundled in port channel configuration.

vPC Peer Keepalive Link: This is a Layer 3 communication path between vPC peer switches. The peer keepalive link is used to monitor the status of the vPC peer when the vPC peer link goes down. *Peer keepalive is used as a secondary test to make sure that the remote peer switch is operating properly*. The vPC peer keepalive link is not used for any data or synchronization traffic; it only sends IP packets to make sure that the originating switch is operating and running vPC.

VPC Domains

Basics & Terminology



vPC: This is a *Layer 2 port channel that spans the two vPC peer switches*. The device on the other end of vPC sees the vPC peer switches as a single logical switch. There is no need for this device to support vPC itself. It connects to the vPC peer switches using a regular port channel. This device can be configured to use LACP (preferred) or a static port channel configuration.

vPC Member Port: This port is a member of a virtual port channel on the vPC peer switch.

VPC Domains

Configuration Snippets

SWITCH 1

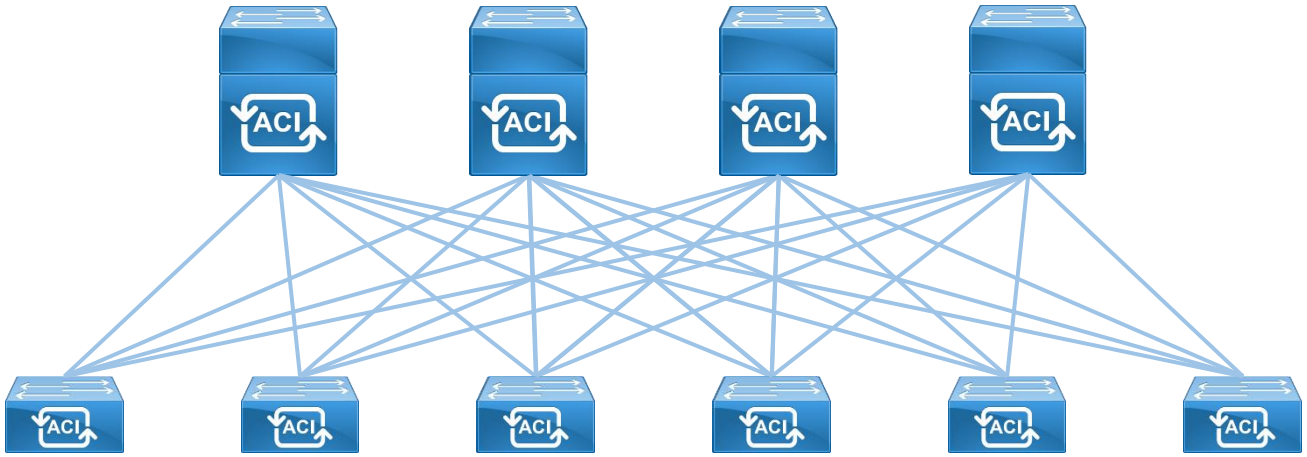
```
feature lacp
feature vpc
!
vrf context keepalive-link
!
vpc domain 34
  peer-switch
  peer-keepalive destination 10.1.2.2 source 10.1.2.1 vrf
keepalive-link
!
interface port-channel1
  description *** vPC Peer Link ***
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link
!
interface Ethernet1/4
  description *** vPC Peer Keepalive Link ***
  no switchport
  vrf member keepalive-link
  ip address 10.1.2.1/30
  no shutdown
!
interface Ethernet1/5
  description *** vPC Peer Link ***
  switchport mode trunk
  channel-group 1 mode active
!
interface Ethernet1/6
  description *** vPC Peer Link ***
  switchport mode trunk
  channel-group 1 mode active
```

SWITCH 2

```
feature lacp
feature vpc
!
vrf context keepalive-link
!
vpc domain 34
  peer-switch
  peer-keepalive destination 10.1.2.1 source 10.1.2.2 vrf
keepalive-link
!
interface port-channel1
  description *** vPC Peer Link ***
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link
!
interface Ethernet1/4
  description *** vPC Peer Keepalive Link ***
  no switchport
  vrf member keepalive-link
  ip address 10.1.2.2/30
  no shutdown
!
interface Ethernet1/5
  description *** vPC Peer Link ***
  switchport mode trunk
  channel-group 1 mode active
!
interface Ethernet1/6
  description *** vPC Peer Link ***
  switchport mode trunk
  channel-group 1 mode active
```

VPC Domains

In ACI Fabric



VPC Domains

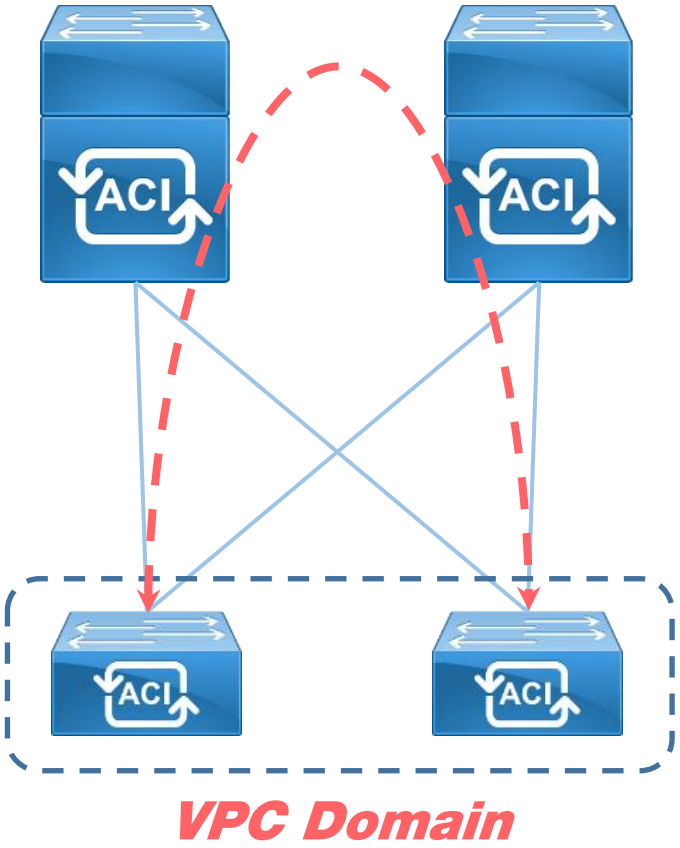
In ACI Fabric

Leaf-Spine Topology

No Horizontal Links

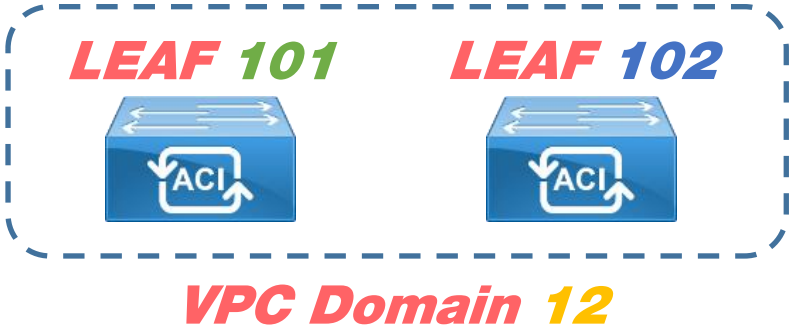
No VPC Peer-Keepalive Link!
No VPC Peer-Link!

Synchronization and peer link communications go through the fabric.



VPC Domains

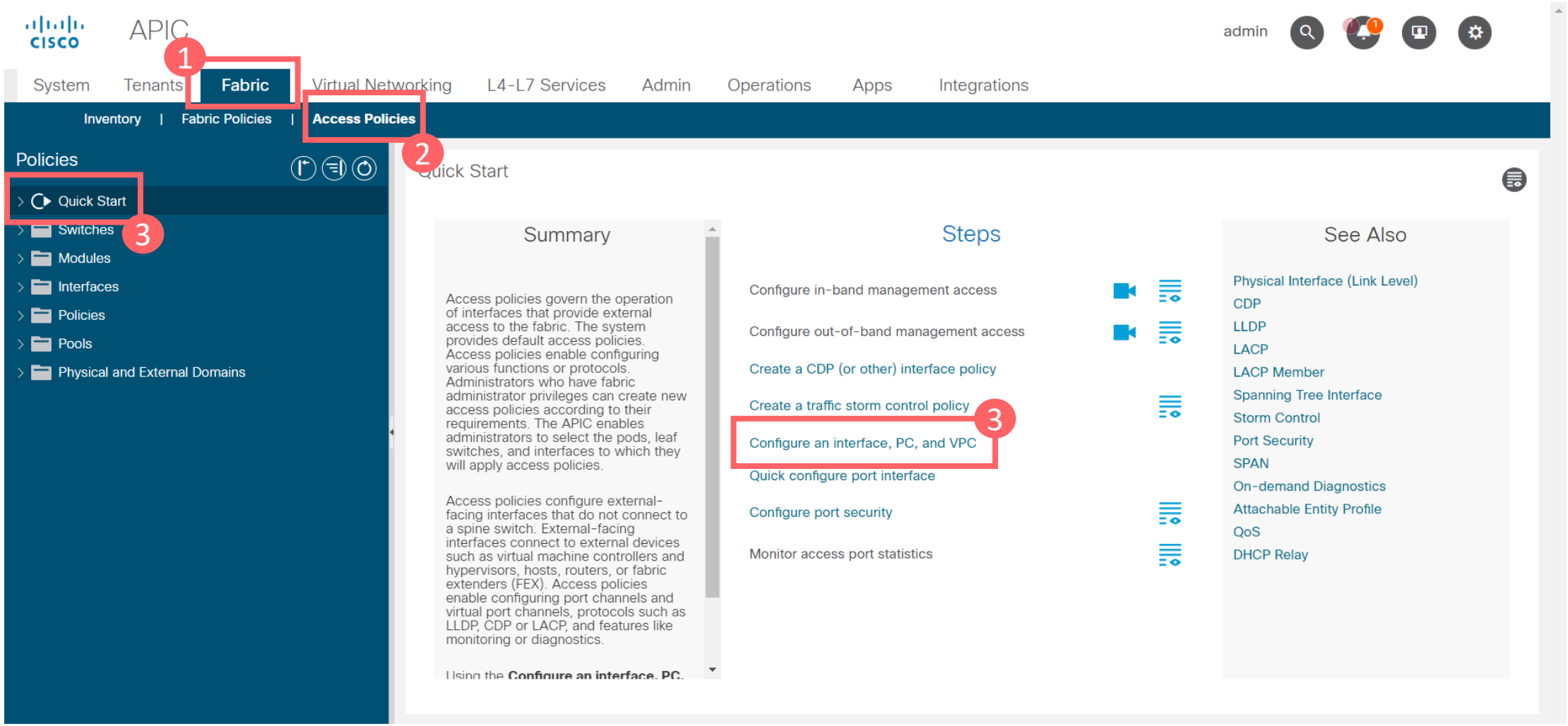
Configuration Procedure



1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. On the Quick Start Menu click on **Configure an interface, PC, and VPC**.
4. On the **VPC Switch Pairs** panel, select the '**+**' button to add a VPC Domain.
5. In the **VPC Domain ID** form type *12*.
6. From the drop-down menu **Switch 1**, select *101*.
7. From the drop-down menu **Switch 2**, select *102*.
8. Click the **Save** button.
9. Click the **Submit** button.

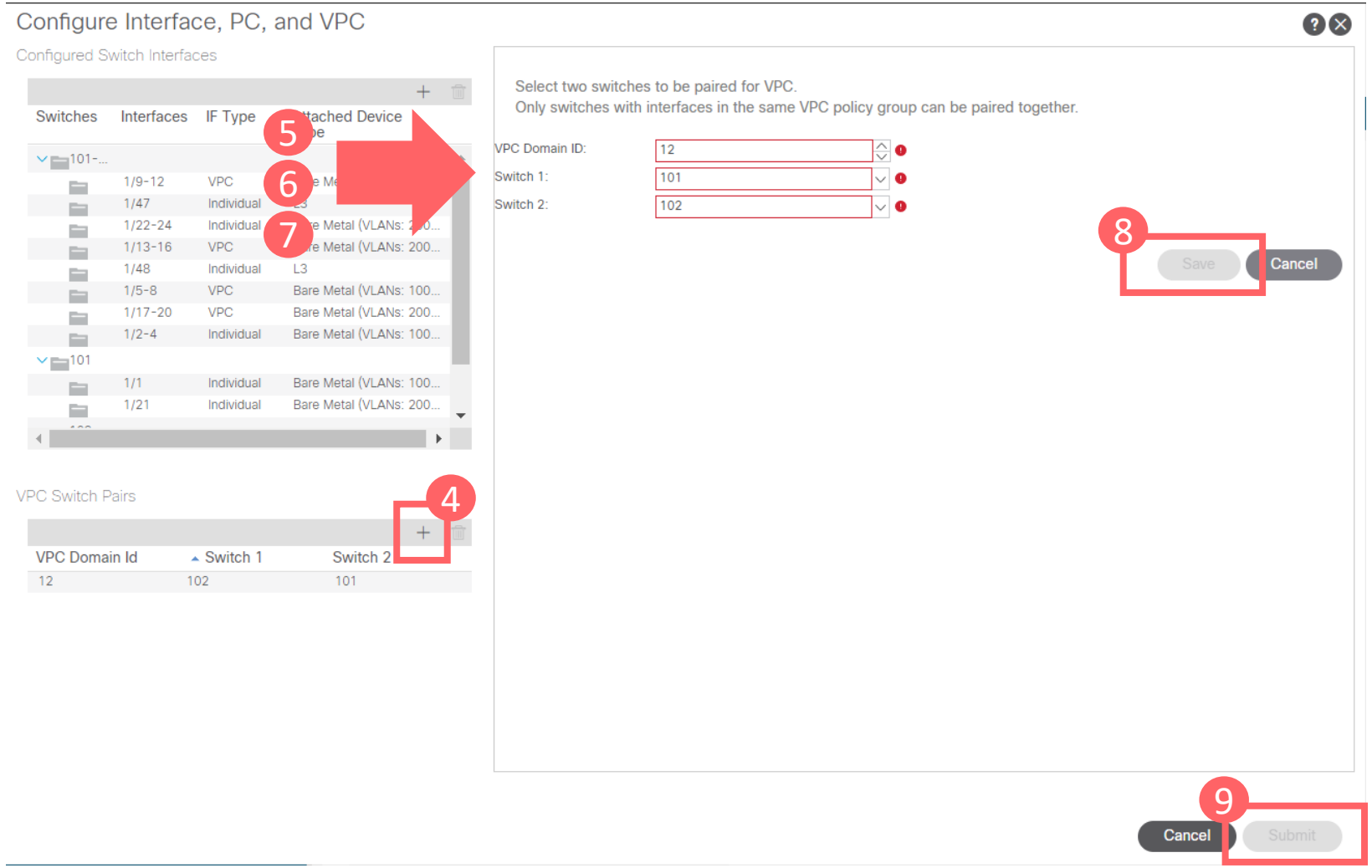
VPC Domains

Configuration Procedure

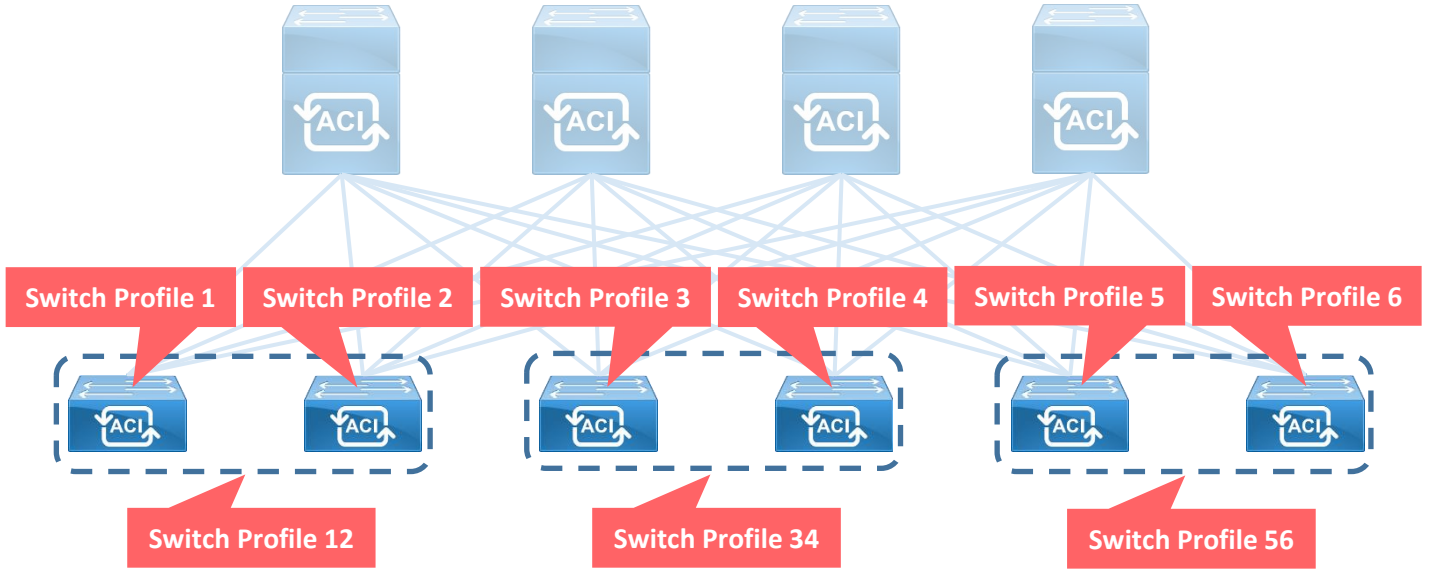


VPC Domains

Configuration Procedure



Switch Profiles



Switch Profile

Defines the specific switch to apply the Interface Profiles.

Best Practice

1 Switch Profile per Leaf Switch + 1 Switch Profile per VPC pair.

Switch Profiles

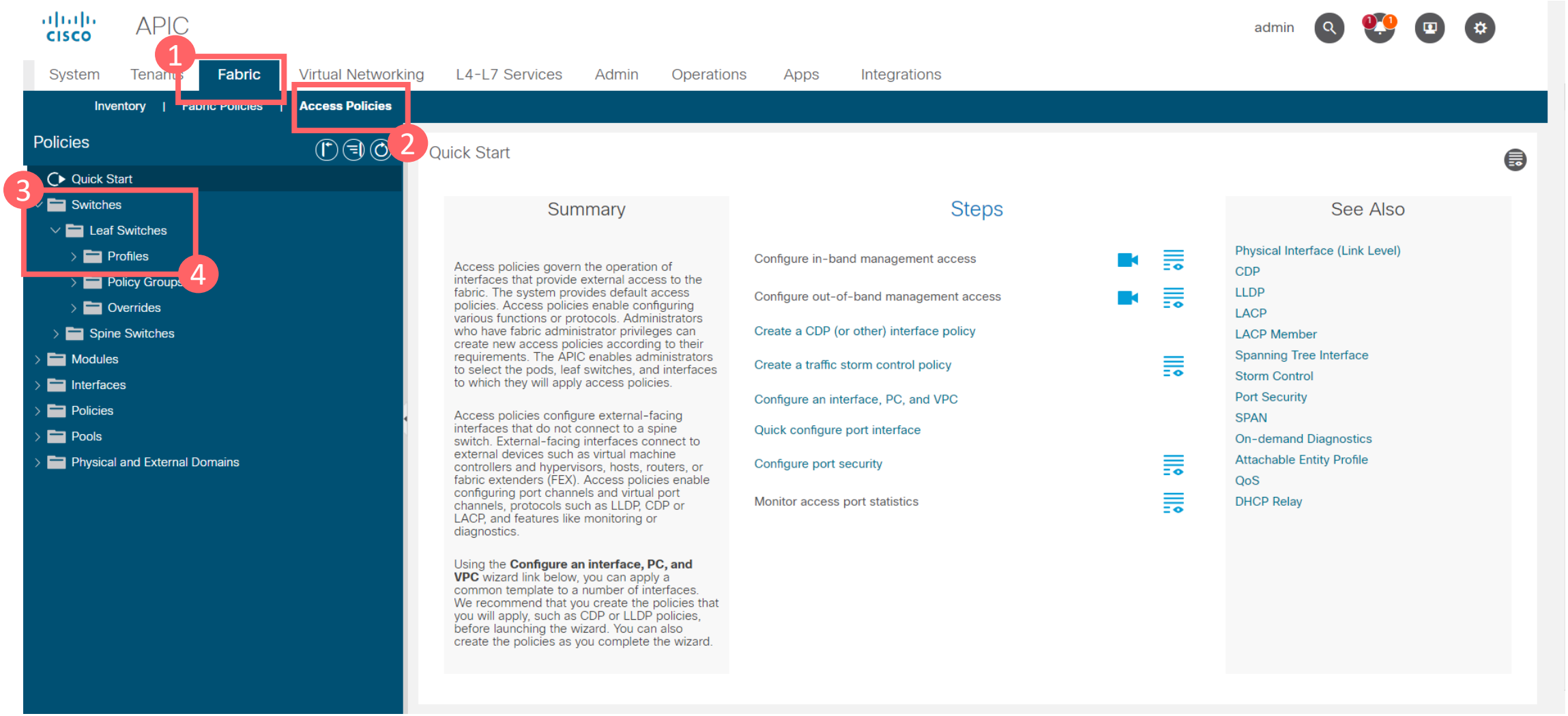
Configuration Procedure

LEAF 101

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Switches>Leaf Switches>Profiles**.
4. Right-click on **Profiles** and choose **Create Profile**.
5. In the **Create Leaf Profiles** dialog box, fill the **Name** field with *SP-101*
6. In the **Leaf Selectors** section, click the "**+**" button:
   a. Fill the **Name** field with *101*
   b. From the drop-down menu **Blocks**, select the leaf with ID = 101
   c. Click the **Update** button.
7. Click the **Next** button.
8. Click the **Submit** button.

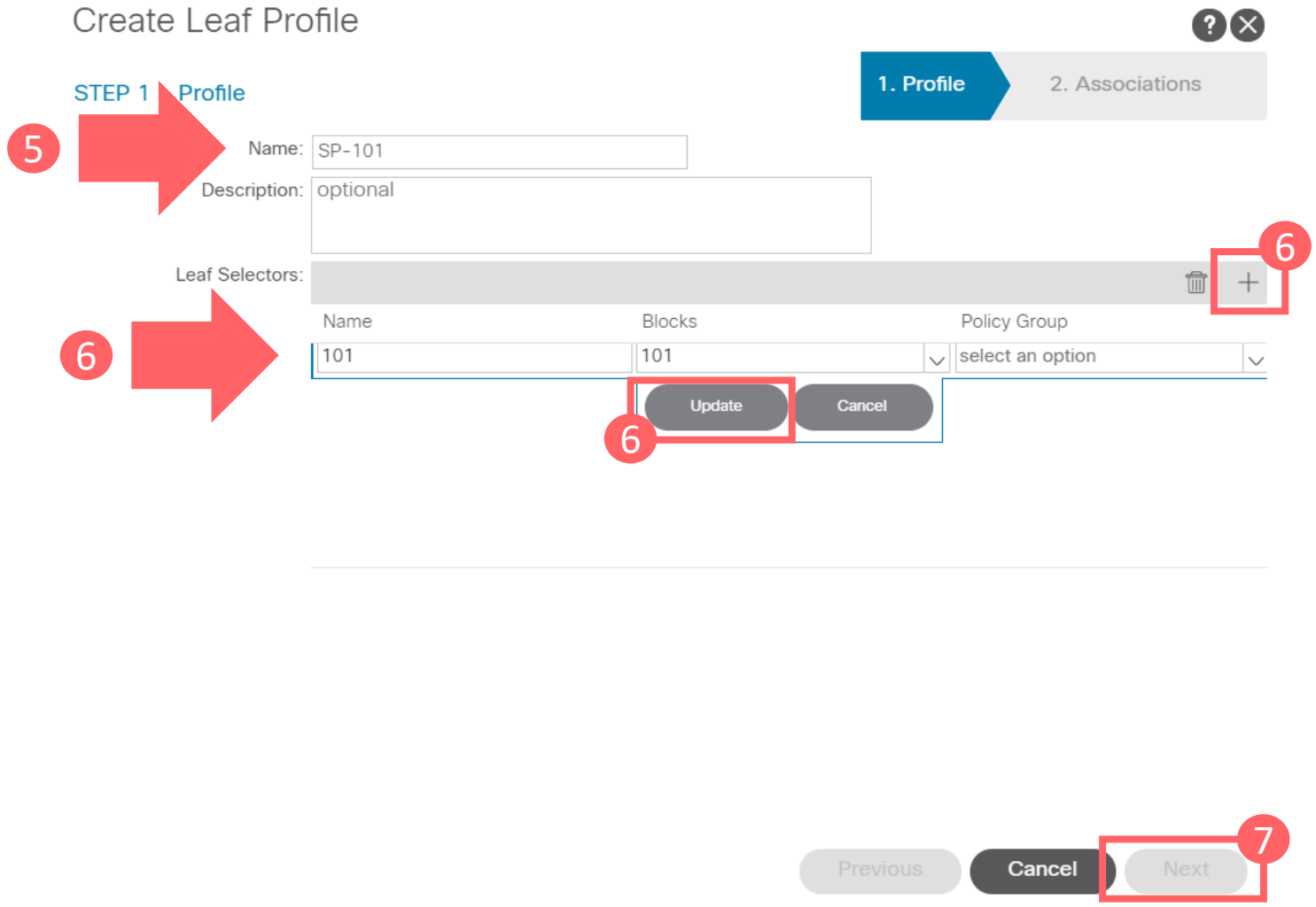
Switch Profiles

Configuration Procedure



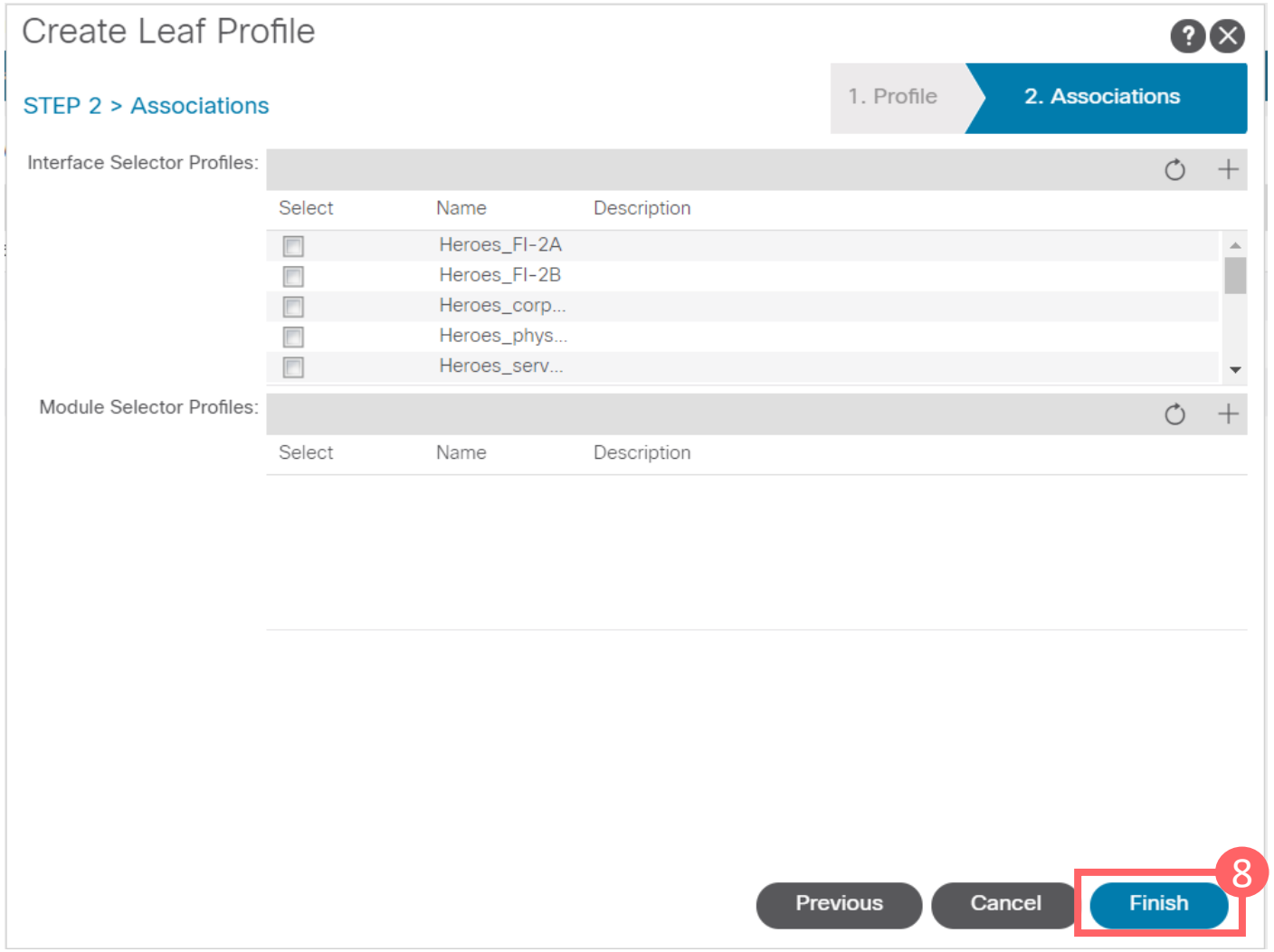
Switch Profiles

Configuration Procedure



Switch Profiles

Configuration Procedure



Interface Policies & Interface Policy Group

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- Spanning Tree Interface
- MCP

Interface Policy Group (IPG)

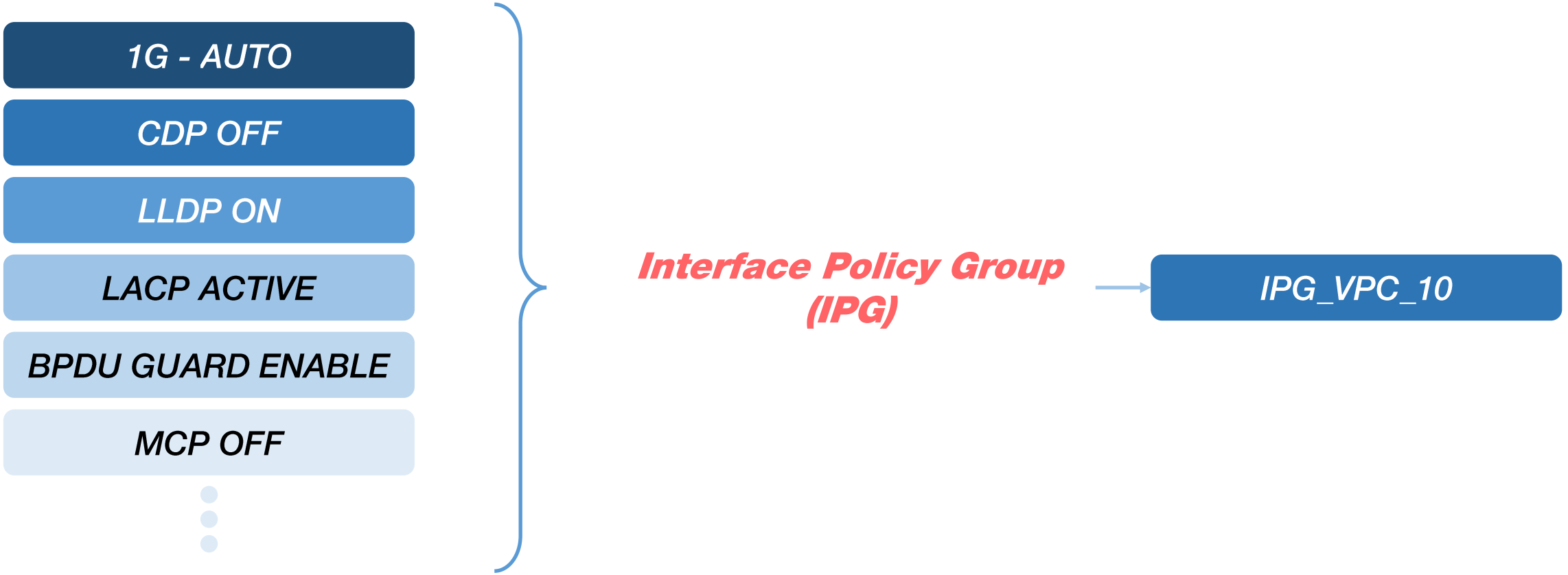
- Access Port
- vPC
- Port Channel

Constraint

1 VPC IPG per Port-Channel (either virtual or standard)

Interface Policies & Interface Policy Group

Example



Interface Policies & Interface Policy Group

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- Spanning Tree Interface
- MCP

```
--- Interface speed = 100Mbps policy ---
```

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies** and then **Interface**.
4. Right-click **Link Level** and choose **Create Link Level Policy**.
5. In the **Create Link Level Policy** dialog box, fill the **Name** field with *AUTO_SPEED_100M*.
6. Choose **On** for the **Auto Negotiation** field (default).
7. Click on the drop-down menu **Speed** and choose **100Mbps**.
8. Click the **Submit** button.

```
--- Interface speed = 1Gbps policy ---
```

9. Repeat steps from 1. to 4.
10. In the **Create Link Level Policy** dialog box, fill the **Name** field with *AUTO_SPEED_1G*.
11. Choose **On** for the **Auto Negotiation** field (default).
12. Click on the drop-down menu **Speed** and choose **1Gbps**.
13. Click the **Submit** button.

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- Spanning Tree Interface
- MCP

```
--- Interface speed = 10Gbps policy ---
```

14. Repeat steps from 1. to 4.
15. In the **Create Link Level Policy** dialog box, fill the **Name** field with *AUTO_SPEED_10G*.
16. Choose **On** for the **Auto Negotiation** field (default).
17. Click on the drop-down menu **Speed** and choose **10Gbps**.
18. Click the **Submit** button.

```
--- Interface speed = AUTO NEGOTIATION---
```

19. Repeat steps from 1. to 4.
20. In the **Create Link Level Policy** dialog box, fill the **Name** field with *AUTO_NEGOTIATION*.
21. Choose **On** for the **Auto Negotiation** field (default).
22. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- Spanning Tree Interface
- MCP

```
--- CDP Enabled ---
```

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies** and then **Interface**.
4. Right-click **CDP Interface** and choose **Create CDP Interface Policy**.
5. In the **Create CDP Interface Policy** dialog box, fill the **Name** field with *CDP_ON*.
6. Choose **Enabled** for the **Admin State** field (default).
7. Click the **Submit** button.

```
--- CDP Disabled ---
```

8. Repeat steps from 1. to 4.
9. In the **Create CDP Interface Policy** dialog box, fill the **Name** field with *CDP_OFF*.
10. Choose **Disabled** for the **Admin State** field.
11. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

Interface Policies

- Link Level
- CDP
- **LLDP**
- Port Channel
- Spanning Tree Interface
- MCP

```
--- LLDP Enabled ---
```

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies** and then **Interface**.
4. Right-click **LLDP Interface** and choose **Create LLDP Interface Policy**.
5. In the **Create LLDP Interface Policy** dialog box, fill the **Name** field with *LLDP_ON*.
6. Choose **Enabled** for the **Receive State** field (default).
7. Choose **Enabled** for the **Transmit State** field (default).
8. Click the **Submit** button.

```
--- LLDP Disabled ---
```

9. Repeat steps from 1. to 4.
10. In the **Create LLDP Interface Policy** dialog box, fill the **Name** field with *LLDP_OFF*.
11. Choose **Disabled** for the **Receive State** field.
12. Choose **Disabled** for the **Transmit State** field.
13. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- **Port Channel**
- Spanning Tree Interface
- MCP

```
--- LACP ACTIVE ---
```

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies** and then **Interface**.
4. Right-click **Port-Channel** and choose **Create Port Channel Policy**.
5. In the **Create Port Channel Policy** dialog box, fill the **Name** field with *LACP_ACTIVE*.
6. Choose **LACP Active** for the **Mode** field.
7. Click the **Submit** button.

```
--- LACP PASSIVE ---
```

8. Repeat steps from 1. to 4.
9. In the **Create Port Channel Policy** dialog box, fill the **Name** field with *LACP_PASSIVE*.
10. Choose **LACP Passive** for the **Mode** field.
11. Click the **Submit** button.

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- **Port Channel**
- Spanning Tree Interface
- MCP

```
--- MODE ON ---
```

12. Repeat steps from 1. to 4.
13. In the **Create Port Channel Policy** dialog box, fill the **Name** field with *MODE_ON*.
14. Choose **Static Channel – Mode On** for the **Mode** field.
15. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- **Spanning Tree Interface**
- MCP

--- BPDU FILTER ENABLED ---

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies** and then **Interface**.
4. Right-click **Spanning Tree Interface** and choose **Create Spanning Tree Interface Policy**.
5. In the **Create Spanning Tree Interface Policy** dialog box, fill the **Name** field with *BPDU_FILTER_ENABLED*.
6. Check **BPDU filter enabled** box for the **Interface controls** field.
7. Click the **Submit** button.

--- BPDU GUARD ENABLED ---

8. Repeat steps from 1. to 4.
9. In the **Create Spanning Tree Interface Policy** dialog box, fill the **Name** field with *BPDU_GUARD_ENABLED*.
10. Check **BPDU Guard enabled** box for the **Interface controls** field.
11. Click the **Submit** button.

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- Spanning Tree Interface
- MCP

```
--- BPDU FILTER AND GUARD ENABLED ---
```

12. Repeat steps from 1. to 4.
13. In the **Create Spanning Tree Interface Policy** dialog box, fill the **Name** field with *BPDU_FILTER_AND_GUARD_ENABLED*.
14. Check **BPDU filter enabled** box for the **Interface controls** field.
15. Check **BPDU Guard enabled** box for the **Interface controls** field.
16. Click the **Submit** button.

```
--- BPDU TRANSPARENT ---
```

17. Repeat steps from 1. to 4.
18. In the **Create Spanning Tree Interface Policy** dialog box, fill the **Name** field with *BPDU_TRANSPARENT*.
19. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- Spanning Tree Interface
- MCP

```
--- MCP INSTANCE GLOBALLY ENABLED ---
```

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies** and then **Global**.
4. Click **MCP Instance Policy default**.
5. Choose **Enabled** for the **Admin State** field.
6. Check **Enable MCP PDU per VLAN** box.
7. Fill the **Key** field with the password *matic_mind*.
8. Fill the **Confirm Key** field with the same password used in previous step.
9. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

Interface Policies

- Link Level
- CDP
- LLDP
- Port Channel
- Spanning Tree Interface
- **MCP**

--- MCP ENABLED ---

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies** and then **Interface**.
4. Right-click **MCP Interface** and choose **Create Mis-cabling Protocol Interface Policy**.
5. In the **Create Mis-cabling Protocol Interface Policy** dialog box, fill the **Name** field with *MCP_ON*.
6. Choose **Enabled** for the **Admin State** field (default).
7. Click the **Submit** button.

--- MCP DISABLED ---

8. Repeat steps from 1. to 4.
9. In the **Create Mis-cabling Protocol Interface Policy** dialog box, fill the **Name** field with *MCP_OFF*.
10. Choose **Disabled** for the **Admin State** field.
11. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

IPG

- Access Port
- vPC
- Port Channel

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Interfaces>Leaf Interfaces>Policy Groups>Leaf Access Port**.
4. Right-click **Leaf Access Port** and choose **Create Leaf Access Port Policy Group**.
5. In the **Create Leaf Access Port Policy Group** dialog box, fill the **Name** field with *IPG-ACCESS-AUTO-INFRA*.
6. Choose AUTO_*NEGOTIATION* for the **Link Level Policy** field.
7. Choose *CDP_ON* for the **CDP Policy** field.
8. Choose *MCP*_ON for the **MCP Policy** field.
9. Choose *LLDP_ON* for the **LLDP Policy** field.
10. Choose *BPDU_TRANSPARENT* for the **STP Interface Policy** field.
11. Click the **Submit** button.

Interface Policies & Interface Policy Group

Configuration Procedure

IPG

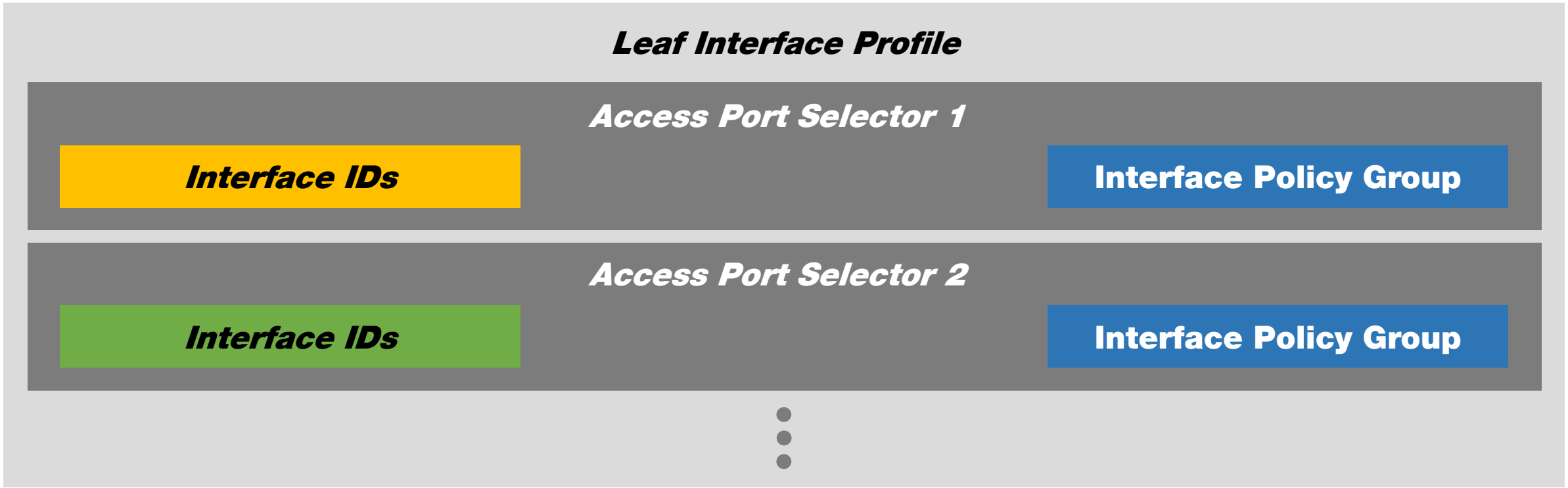
Access Port

vPC

Port Channel

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Interfaces>Leaf Interfaces>Policy Groups>VPC Interface**.
4. Right-click **VPC Interface** and choose **Create VPC Interface Policy Group**.
5. In the **Create VPC Interface Policy Group** dialog box, fill the **Name** field with *IPG-VPC-AUTO-INFRA*.
6. Choose AUTO_*NEGOTIATION* for the **Link Level Policy** field.
7. Choose *CDP_ON* for the **CDP Policy** field.
8. Choose *MCP*_ON for the **MCP Policy** field.
9. Choose *LLDP_ON* for the **LLDP Policy** field.
10. Choose *BPDU_TRANSPARENT* for the **STP Interface Policy** field.
11. Choose *VLAN_SCOPE_LOCAL* for the **L2 Interface Policy** field.
12. Choose *LACP_ACTIVE* for the **Port Channel Policy** field.
13. Click the **Submit** button.

Leaf Interface Profiles

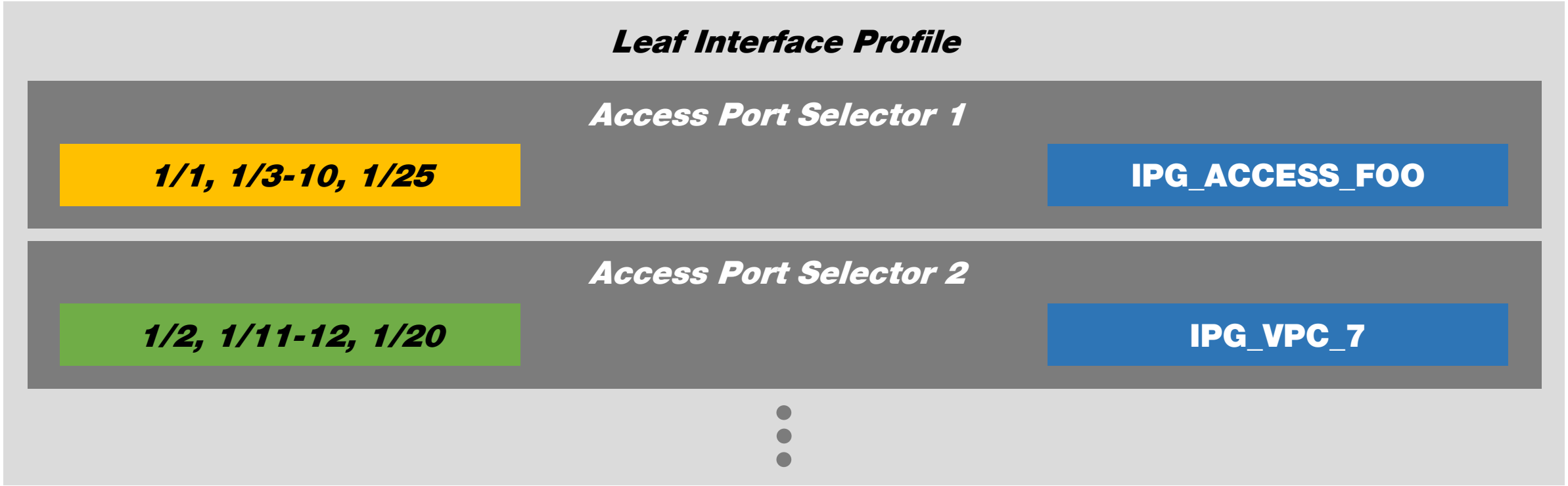


Leaf Interface Profile

The Interface Profile is used to apply policies to physical interfaces.

Leaf Interface Profiles

Example



Leaf Interface Profile

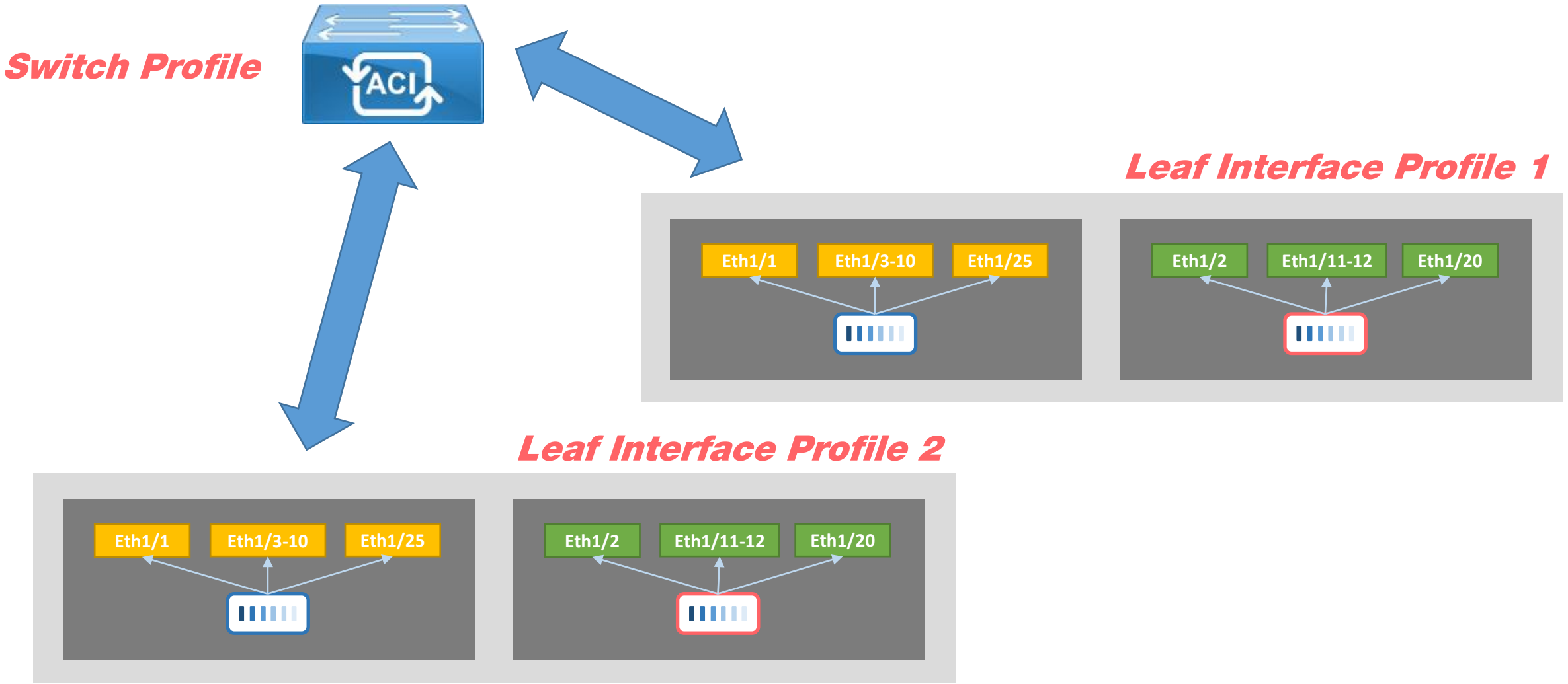
The Interface Profile is used to apply policies to physical interfaces.

Leaf Interface Profiles

Configuration Procedure

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Interfaces>Leaf Interfaces>Profiles**.
4. Right-click **Profiles** and choose **Create Leaf Interface Profile**.
5. In the **Create Leaf Interface Profile** dialog box, fill the **Name** field with *L101-ACCESS-PORTS*
6. Click on "**+**" button in the **Interface Selectors** field.
7. In the **Create Access Port Selector** dialog box, fill the **Name** field with PS-L101-ACCESS-10G-INFRA.
8. Fill the **Interface IDs** with *1/1, 1/2*.
9. From the drop-down menu **Interface Policy Group** select the Interface Policy Group *IPG-ACCESS-1G-INFRA*.
10. Click the **Ok** button.
11. Click the **Submit** button.

Leaf Interface Profile to Switch Profile Association



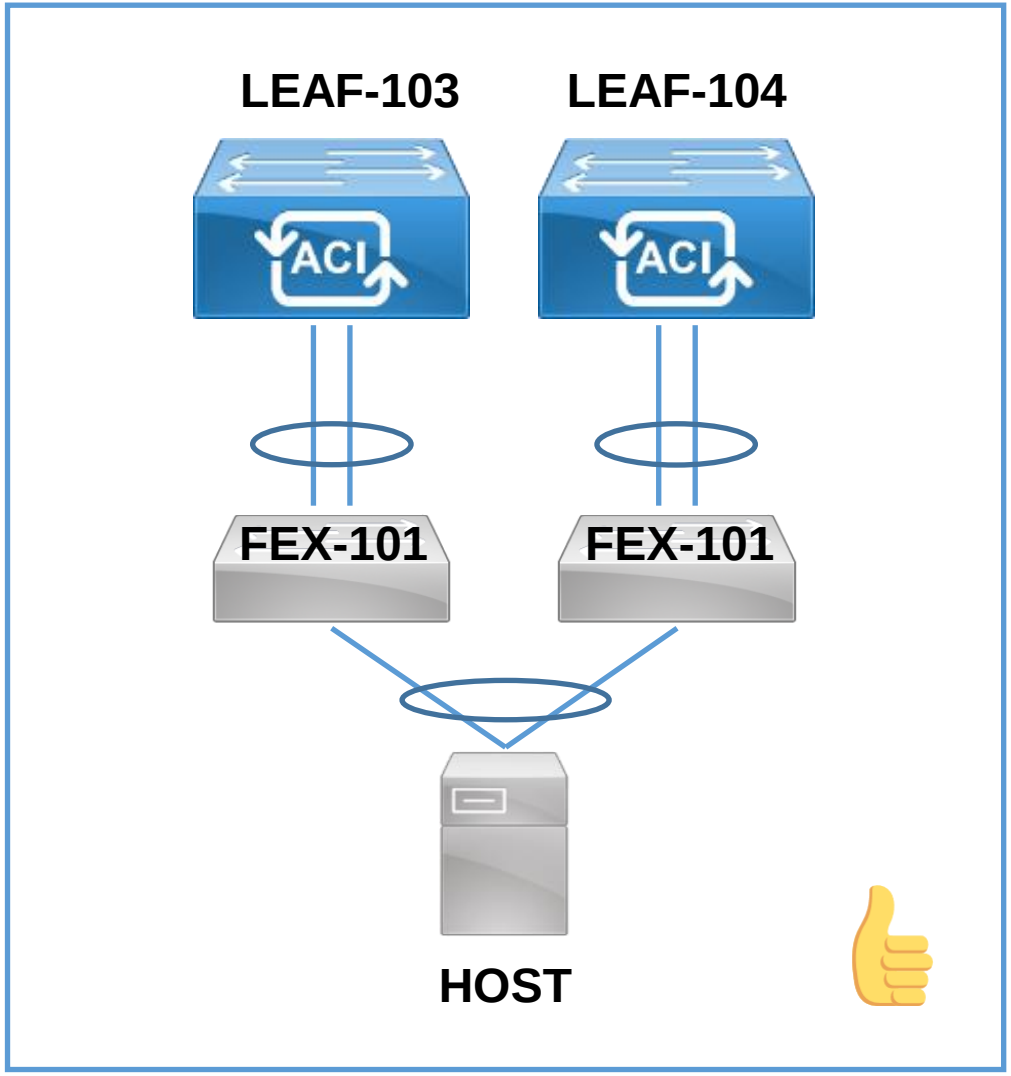
Leaf Interface Profile to Switch Profile Association

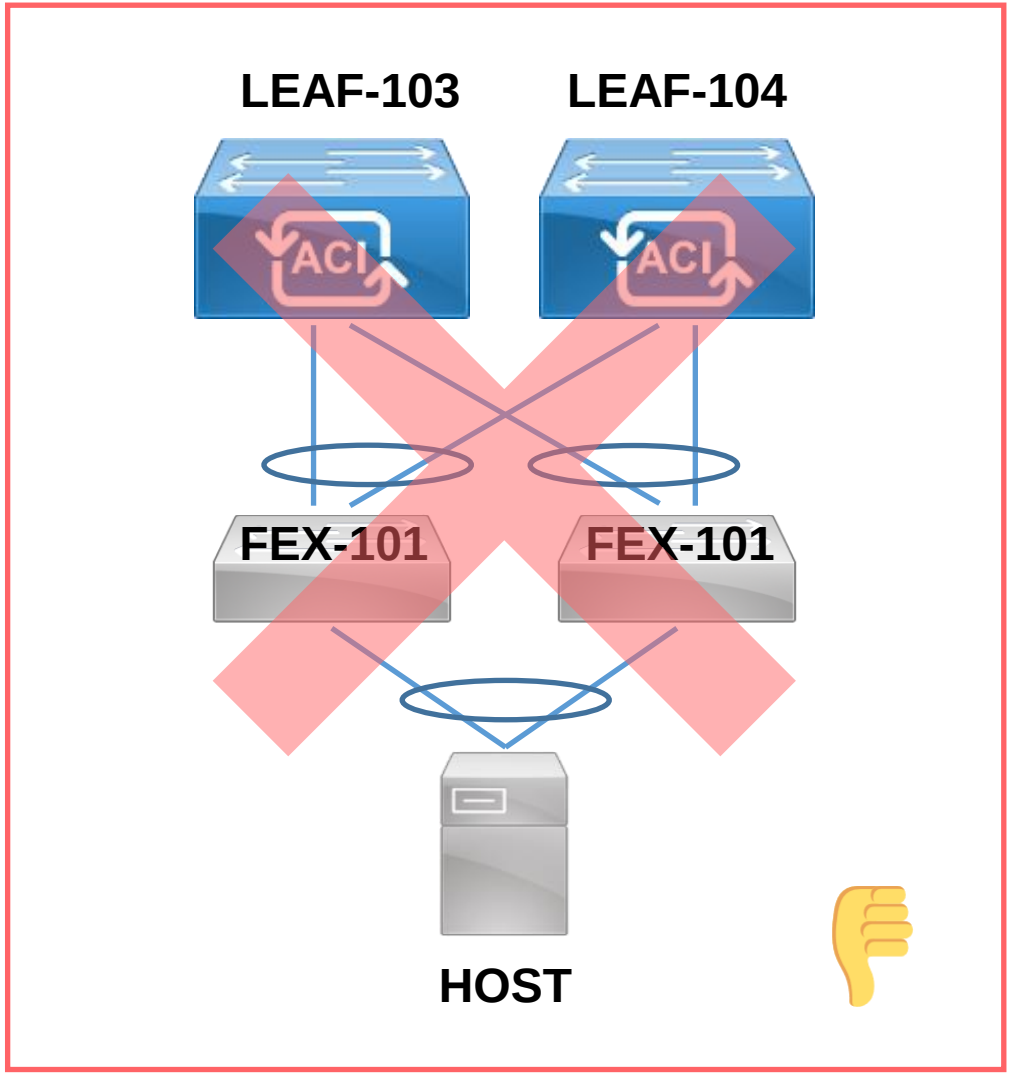
Configuration Procedure

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Switches>Leaf Switches>Profiles**.
4. Select the Leaf Profile *SP-101*
5. Click on "**+**" button in the **Associated Interface Selector Profiles** field.
6. In the **Create Interface Profile** dialog box, select from the drop-down menu **Interface Select Profile** the Leaf Interface Profile *L101-ACCESS-PORTS*.

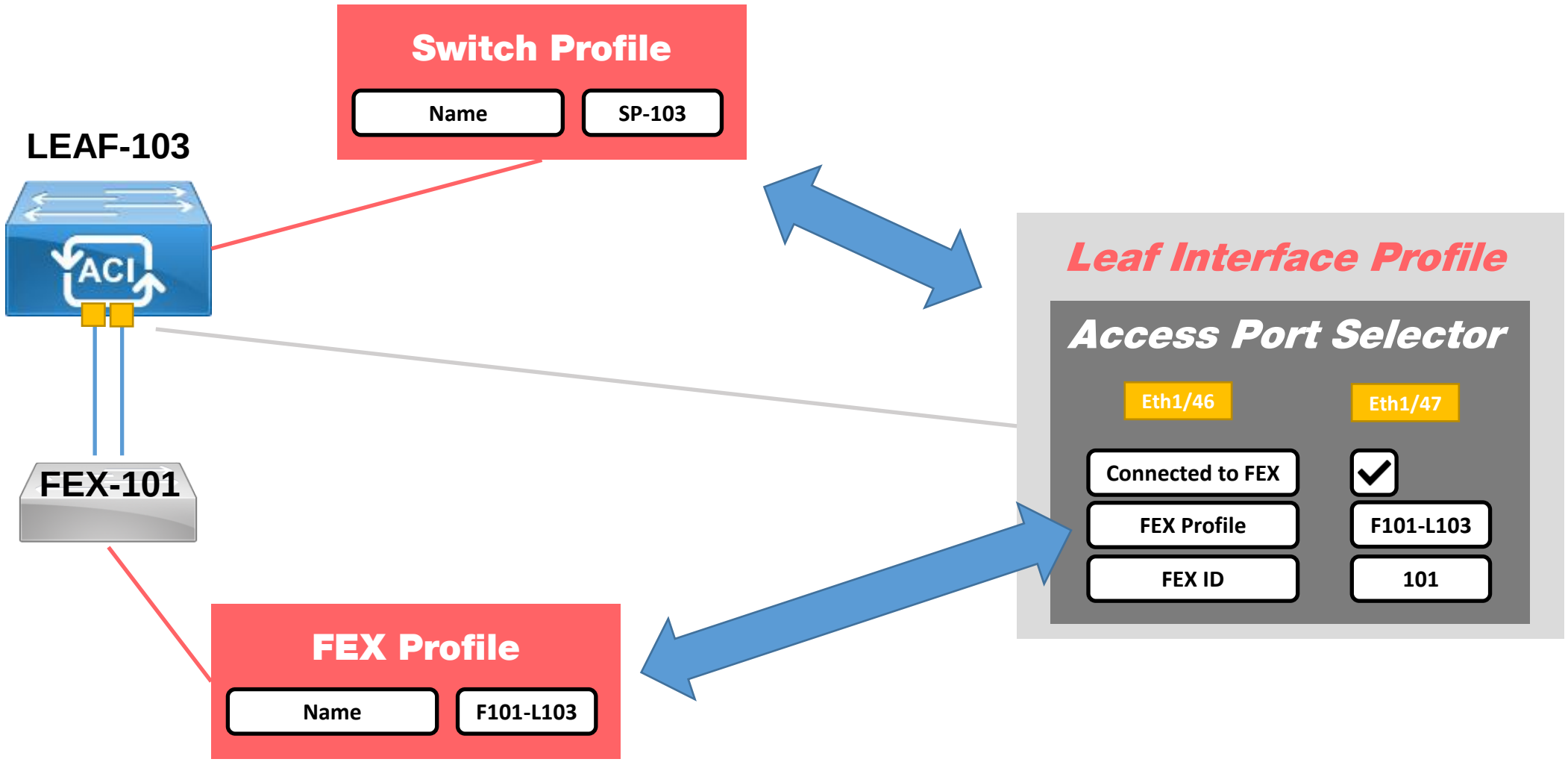

DEMO LAB 6

FEX & Connections to Leaves



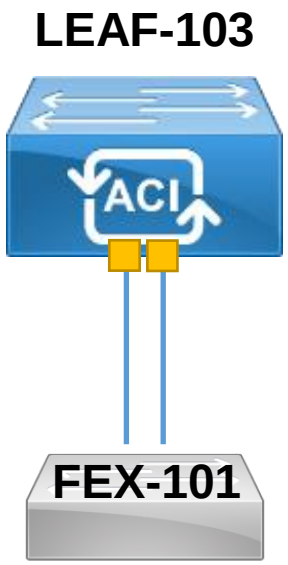


FEX Profiles & Association to Switch Profile



FEX Profiles & Association to Switch Profile

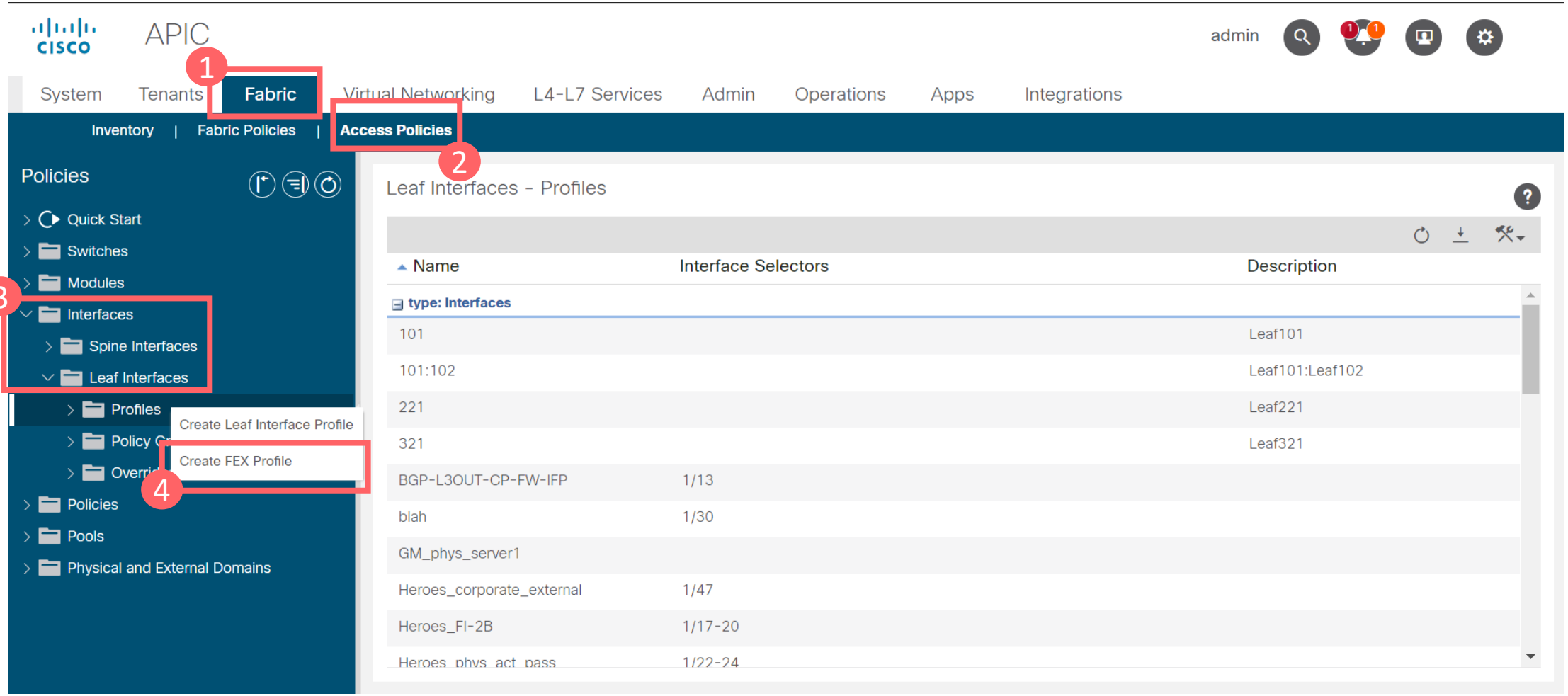
Configuration Procedure



1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Interfaces>Leaf Interfaces**.
4. Right-click on **Profiles** and choose **Create FEX Profile**.
5. In the **Create FEX Profile** dialog box, fill the **Name** field with *FEX101-LEAF103.*
6. Click the **Submit** button.
7. In the Navigation pane, expand **Interfaces>Leaf Interfaces**.
8. Right-click on **Profiles** and choose **Create Leaf Interface Profile**.
9. In the **Create Leaf Interface Profile** dialog box, fill the **Name** field with *L103-FEX-PORTS*
10. In the **Interface Selectors** section, click the "**+**" button:
11. In the **Create Access Port Selector** dialog box, fill the **Name** field with *FEX-101-UPLINK-PORTS*
12. Fill the **Interface IDs** field with *Eth1/47-48*.
13. Check box **Connected To Fex.**
14. From the drop-down menu **FEX Profile**, select previously created Profile *FEX101-LEAF103*.
15. Fill the **FEX ID** field with *101*.
16. Click the **Ok** button.
17. Click the **Submit** button.
18. Associate created Leaf Interface Profile *L103-FEX-PORTS* to the switch profiles *SP-103.*

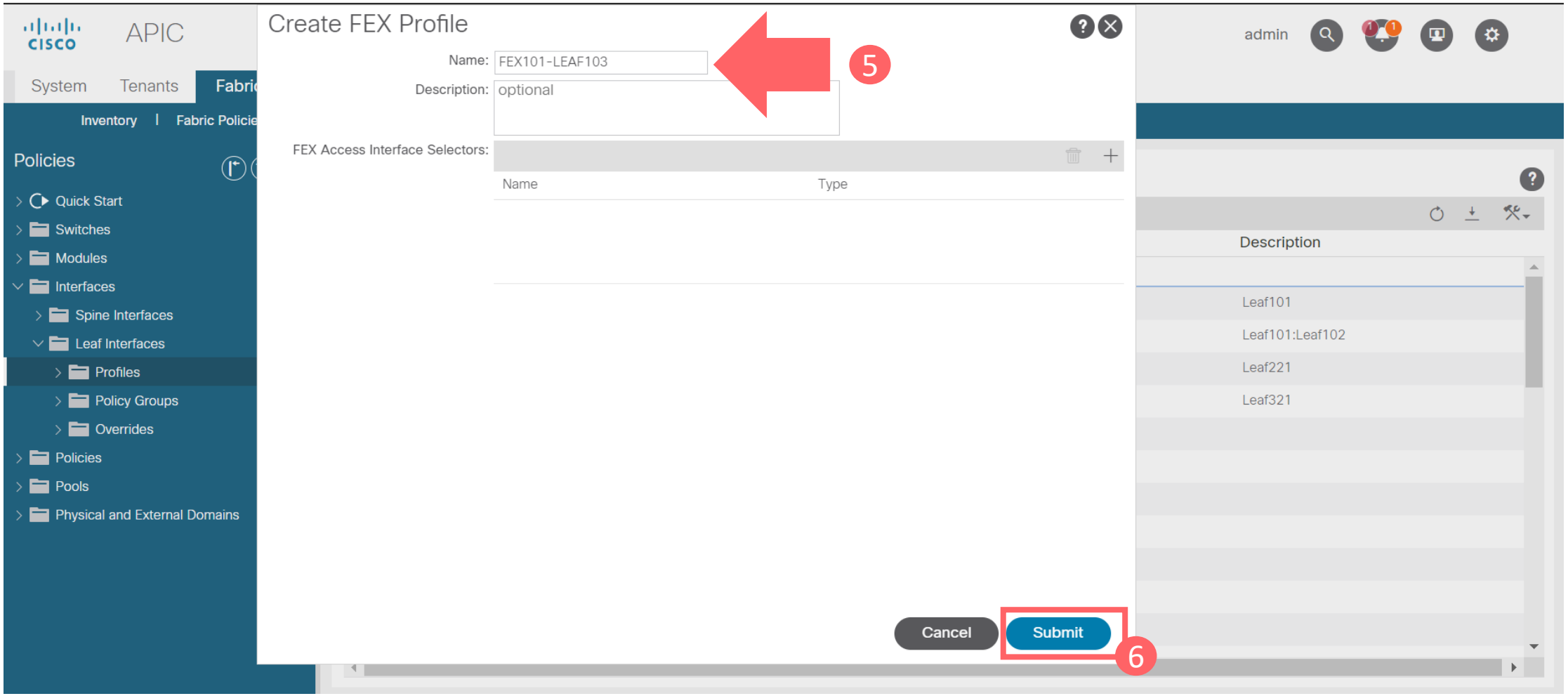
FEX Profiles & Association to Switch Profile

Configuration Procedure



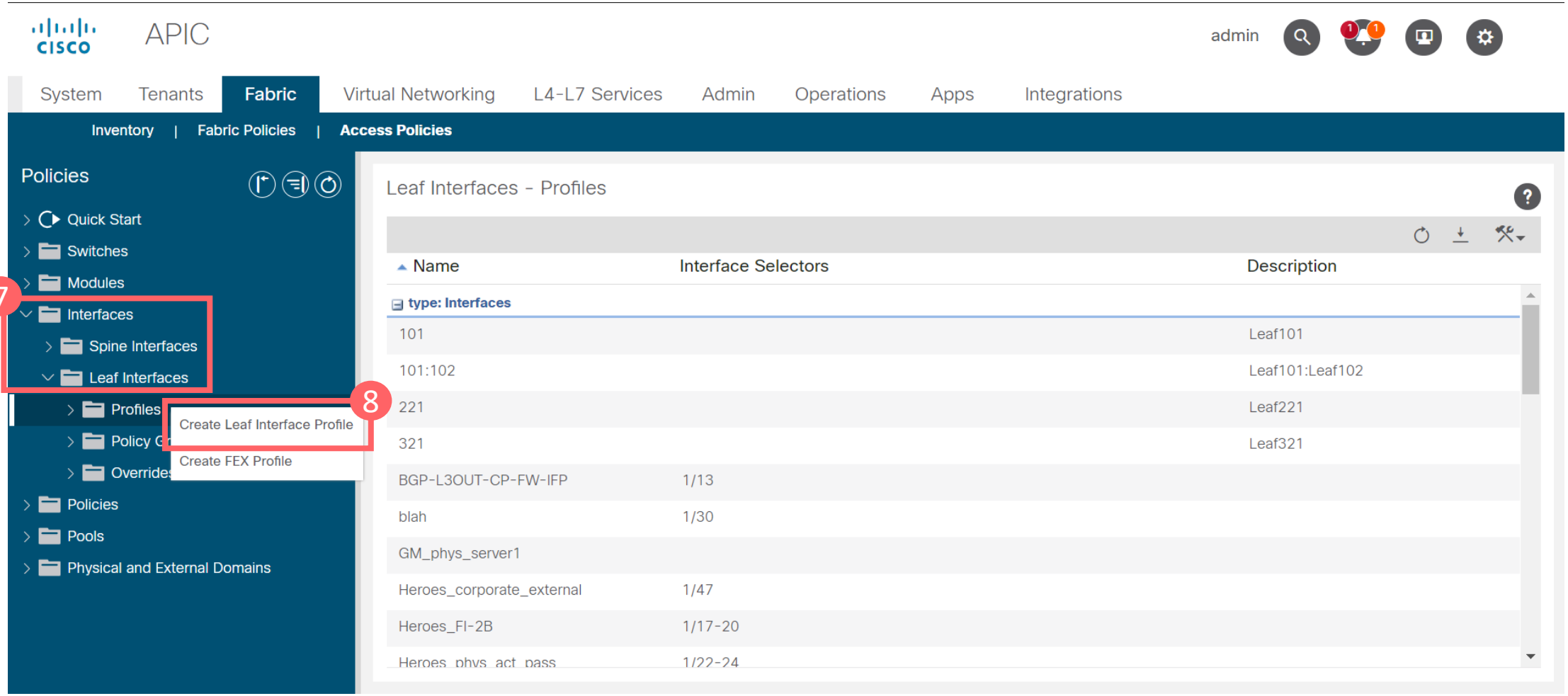
FEX Profiles & Association to Switch Profile

Configuration Procedure



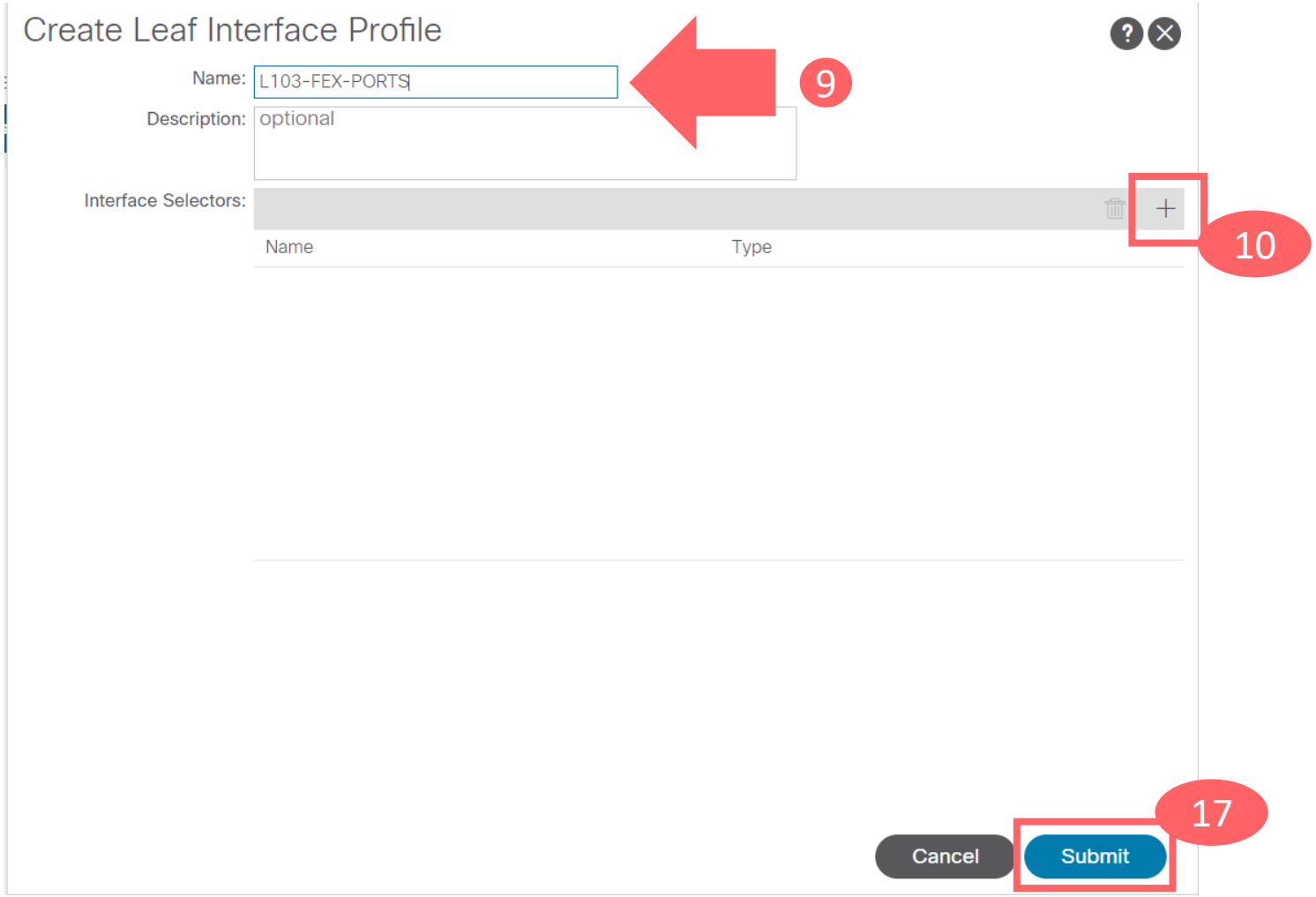
FEX Profiles & Association to Switch Profile

Configuration Procedure



FEX Profiles & Association to Switch Profile

Configuration Procedure

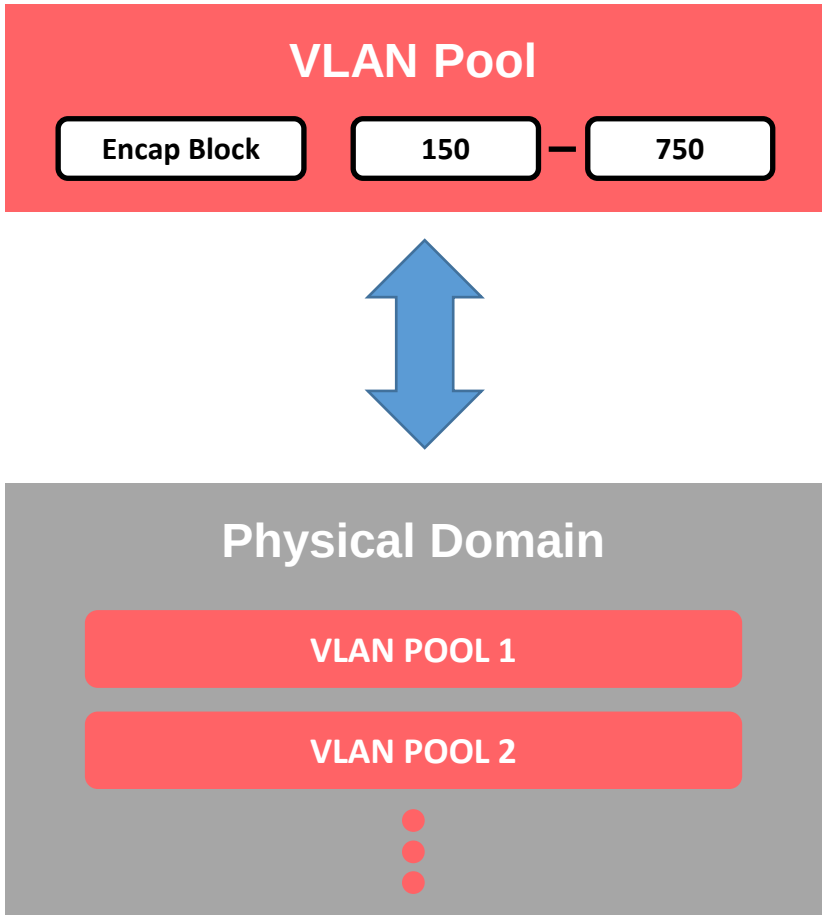


FEX Profiles & Association to Switch Profile

Configuration Procedure

18 DEMO LAB 6

Physical Domain & VLAN Pool



VLAN Pool

Range of VLANs that can be applied to a switch or an interface.

Physical Domain

Defines the «scope» of the VLANs defined in the VLAN Pools associated with the Physical Domain.

Best Practices

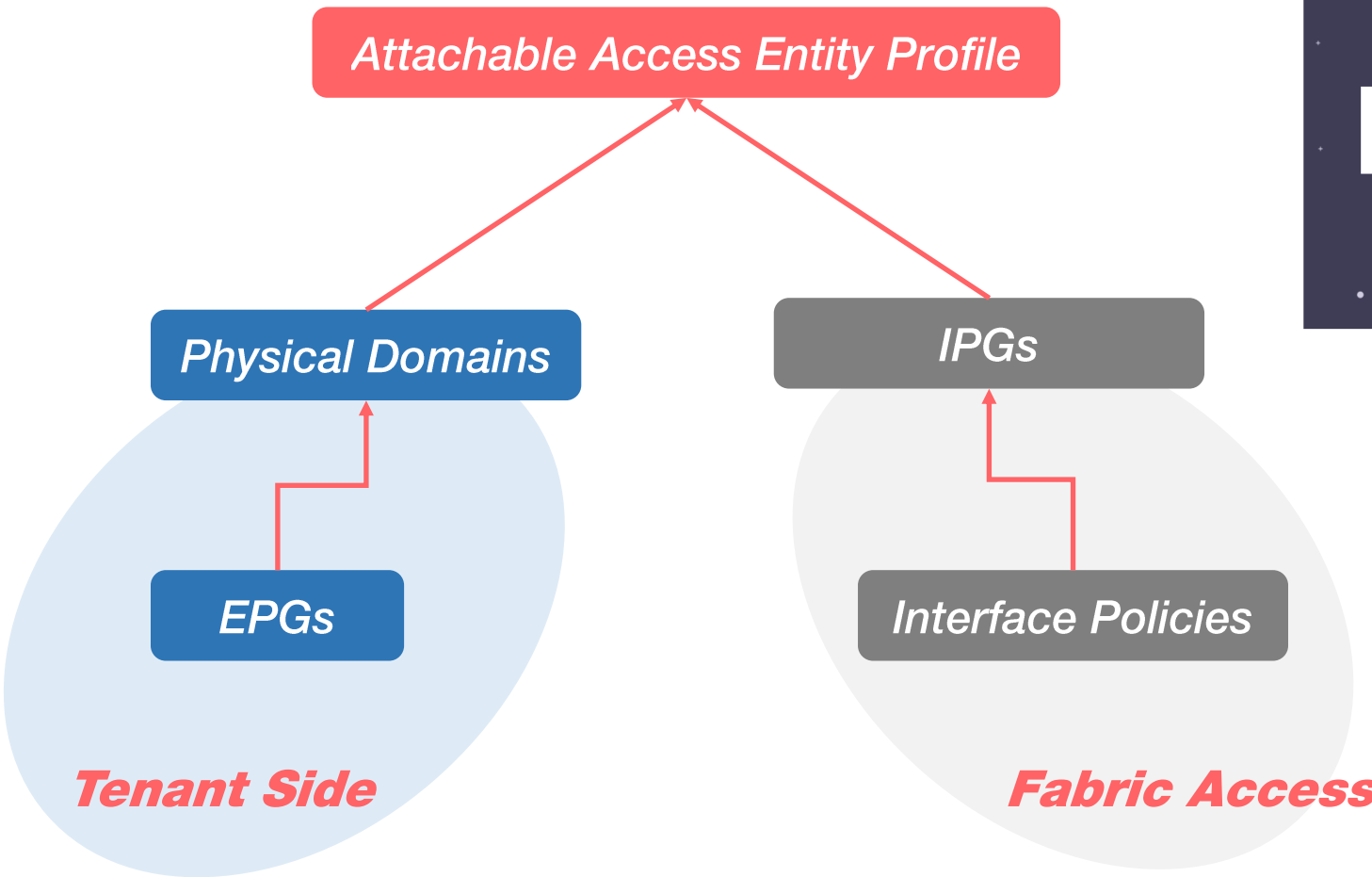
One physical domain per tenant for bare metal servers.

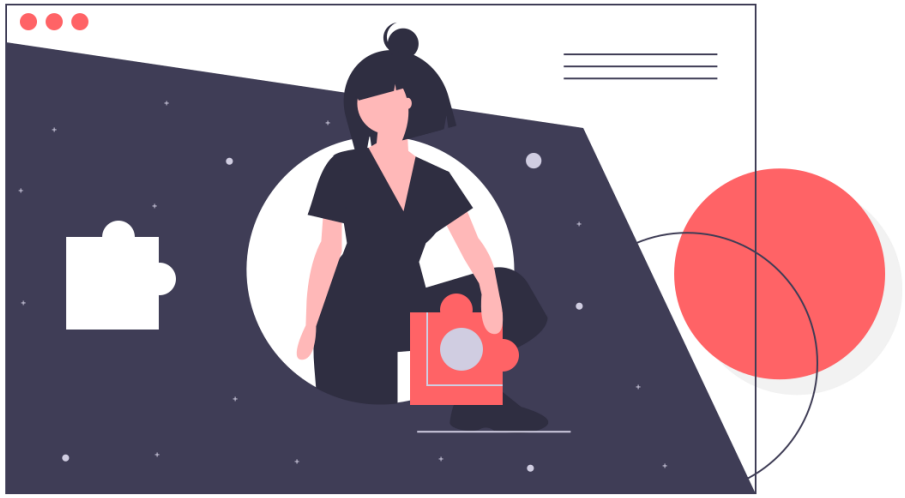
Physical Domain & VLAN Pool

Configuration Procedure

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Physical and External Domains.**
4. Right-click **Physical Domains** and choose **Create Physical Domain**.
5. In the **Create Physical Domain** dialog box, fill the **Name** field with *MM-PHYS-DOMAIN*.
    1. From the drop-down menu **VLAN Pool** select **Create VLAN Pool**
        1. In the **Create VLAN Pool** dialog box, fill the **Name** field with *MM-VPOOL*.
        2. In the **Allocation Mode** field, select **Static Allocation**.
        3. In the **Encap Blocks** section, click on the "**+**" button.
            1. In the **Create Ranges** dialog box, fill the **Range** field with *1000* and *1500*.
            2. Click the **OK** button.
        4. Click the **Submit** button.
6. Click the **Submit** button.

Attachable Access Entity Profile (AAEP)



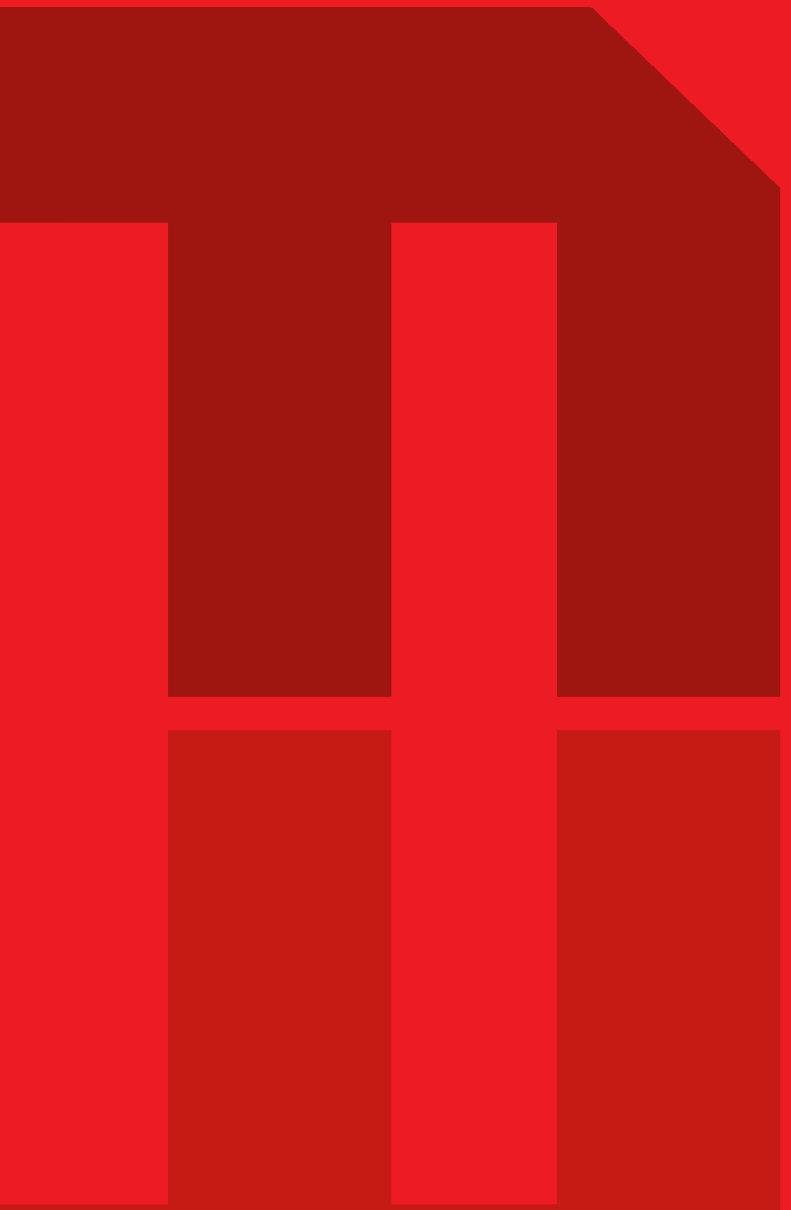


Attachable Access Entity Profile (AAEP)

Configuration Procedure

1. On the menu bar, click **Fabric**.
2. On the submenu bar, click **Access Policies**.
3. In the Navigation pane, expand **Policies>Global>Attachable Access Entity Profiles**.
4. Right-click **Attachable Access Entity Profiles** and choose **Create Attachable Access Entity Profile**.
5. In the **Create Attachable Access Entity Profile** dialog box, fill the **Name** field with *AAEP-MM*.
6. Add one Domain:
   a. Click the "**+**" button next to **Domains (VMM, Physical or External) To Be Associated To Interfaces** section.
   b. From the drop-down menu in **Domain Profile** field, choose *MM-PHYS-DOMAIN* physical domain previously created.
   c. Click the **Update** button.
7. Click the **Next** button.
8. In the **Association To Interfaces** menu, select the interfaces to be associated to this AAEP:
   a. click on the interface policy group *IPG-ACCESS-10G-HOST* and select **All** in the **Select Interfaces** column.
   b. repeat previous step to associate all the IPGs to this AAEP
9. Click the **Finish** button.


DEMO LAB 7



DATA CENTER COLLABORATION NETWORK APPLICATIONS SECURITY

www.maticmind.it