NetworkLife
Another packet in the network....

Cisco ACI — L3Out (Layer 3 Out)

Layer 3 Outside (L3out) for Routed Connectivity to External Networks

In a Cisco ACI fabric, the bridge domain is not meant for the connectivity of routing devices, and this is why you cannot configure static or dynamic routes directly on a bridge domain.
You need to use a specific construct for routing configurations: the L3Out.

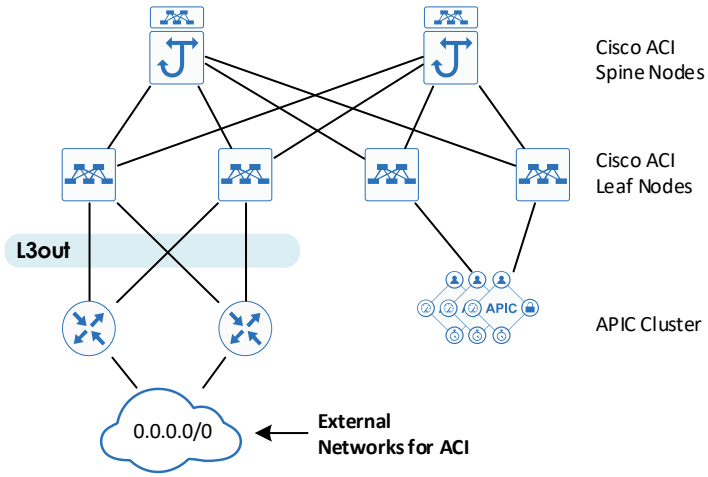
Localisation : Tenant > Networking > External Routed Domains

A L3Out policy is used to configure interfaces, protocols, and protocol parameters necessary to provide IP connectivity to external routing devices.

Part of the L3Out configuration involves also defining an **external network** (also known as an external EPG) for the purpose of access-list filtering.

The external network is used to define which subnets are potentially accessible through the Layer 3 routed connection.

As part of the L3Out configuration, these subnets should be defined as external networks. Alternatively, an external network could be defined as 0.0.0.0/0 to cover all possible destinations, but in case of multiple L3Outs, you should use more specific subnets in the external network definition.

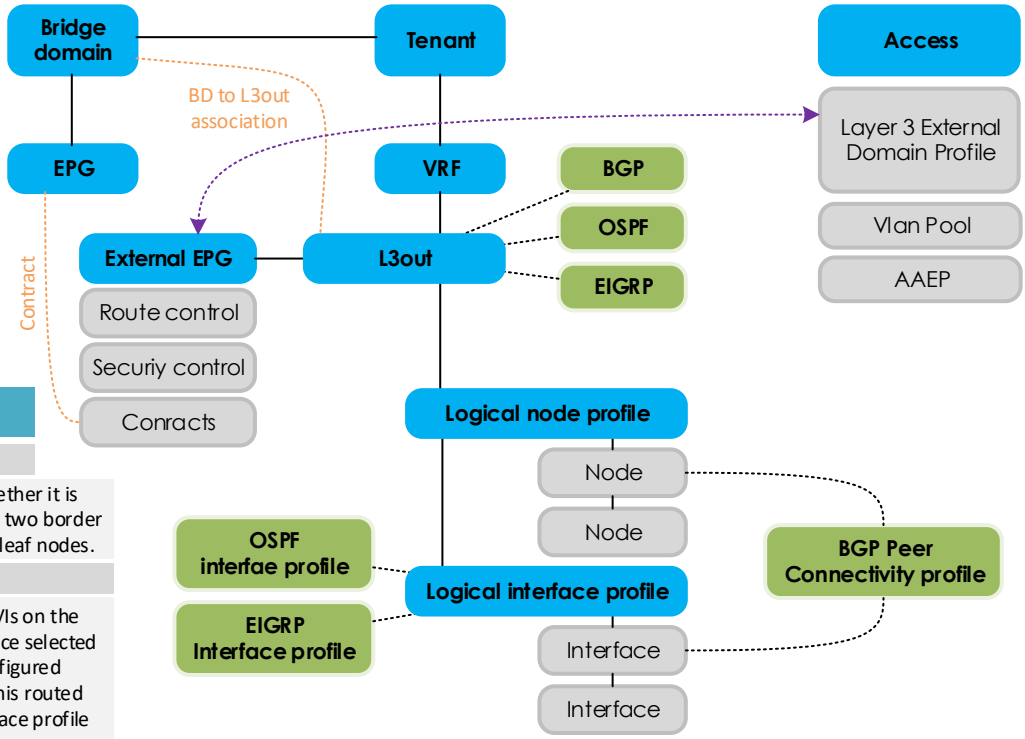


L3out objects relationships

Routed connectivity to external networks is enabled by associating a fabric access **external routed domain** with a tenant Layer 3 **external instance profile** (l3extInstP or external EPG) of a **Layer 3 external outside network** (l3extOut), in the hierarchy in the side diagram:

A **Layer 3 external outside network** (l3extOut object) includes the routing protocol options (BGP, OSPF, EIGRP, static) and the switch-specific and interface-specific configurations.

The **External EPG** exposes the external network to tenant EPGs through a contract.



Definitions

Logical node profile

This is the leafwide VRF routing configuration, whether it is dynamic or static routing. For example, if you have two border leaf nodes, the logical node profile consists of two leaf nodes.

Logical interface profile

This is the configuration of Layer 3 interfaces or SVIs on the leaf defined by the logical node profile. The interface selected by the logical interface profile must have been configured with a routed domain in the fabric access policy. This routed domain may also include VLANs if the logical interface profile defines SVIs.

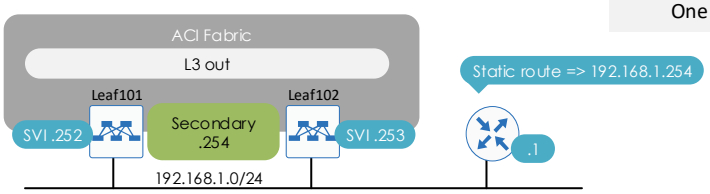
External network and EPG

This is the configuration object that classifies traffic from the outside into a security zone.

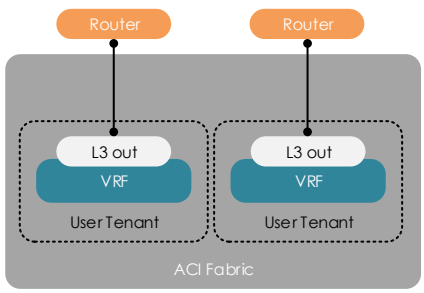
Gateway Resiliency (static routing)

Some design scenarios require gateway resiliency on L3Out. For L3Outs configured with static routing, Cisco ACI provides multiple options for a resilient next hop:

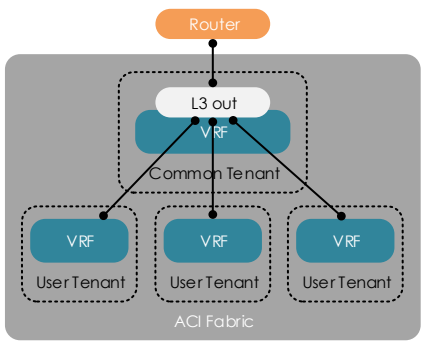
Secondary IP	This option is available on routed interfaces, subinterfaces, and SVIs, but is used mostly with SVIs.
HSRP	This option is available on routed interfaces and on subinterfaces (not on SVIs). It is used primarily in conjunction with an external switch.



L3out Design



One L3out object per User Tenant



One L3out object inside the Common Tenant
Every user Tenant are associated to it (*simplify and scale the configuration*).

This is called « shared services ».
Example of config in page 3.

Author: Benoit GONCALVES – 2020 – ACI 4.2

NetworkLife
Another packet in the network....

Cisco ACI — L3Out (Layer 3 Out)

Tenant Tab

1 Configure Tenant & VRF
Localisation : Tenants > Add Tenant
Localisation : Tenants > Networking > VRF

Tenant: **ACME**
VRF: **Networklife**

2 Configure the Bridge Domain
Localisation : Tenant > Networking > Bridge Domain

Name: **Standalone.BD**
Clic on « **Advertise Host Routes** » to enable advertisement to all deployed border leaf switches.
VRF: attach it to the VRF created at previous step.
Subnet: **10.0.0.1/24 + « Advertise Externally »**

3 Configure the AP & EPG
Localisation : Tenant > Application Profiles

Name of AP: **Standalone.AP**
Name of EPG: **Standalone.EPG**
BD: **Standalone.BD**

4 Configure the L3out
Localisation : Tenant > Networking > External Routed Networks

Right click and choose create L3out
Name: **WAN-L3out**
VRF: **Networklife**
External Routed Domain: **WAN-L3out.RoutedDomain**

- If you need dynamic routing, tick the BGP, OSPF or EIGRP. For this example, we will configure static routing.

5 Configure Node Profile
Localisation : Tenant > Networking > External Routed Networks

- Inside the **L3out** object > **Policy** > **Node Profiles**, Click « **+** »
Name : **ACINodeProfile**
- Nodes, click « **+** », select the ID of the leaf 1**02** and configure the **Router ID** IP address
- Set the **static route 0.0.0.0/0** with the external router IP as a next-hop.

6 Configure Logical Interface Profiles
Localisation : Tenant > Networking > External Routed Networks > Logical Node Profiles > ACINodeProfile > Logical Interface Profiles

Name: **Leaf102-IntProf**
- Configure the **local IP** in the same subnet as the external router, you can use Routed sub-interfaces, Routed interfaces or SVI.
- Choose the **Port 1/1** previously created and encapulation **vlan-10**.

7 Configure External Networks (EPG)
Localisation : Tenant > Networking > External Routed Networks > Networks

Name: **WAN-ExtNet**
Subnets: **0.0.0.0/0**

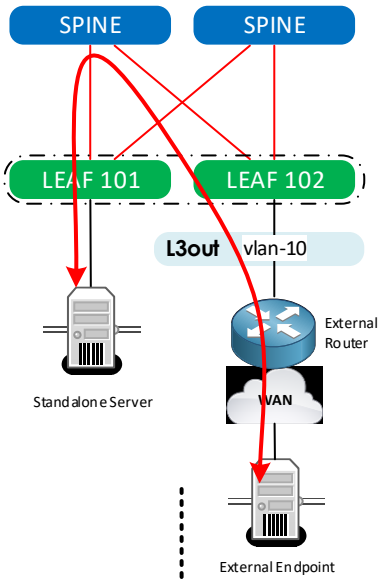
8 Attach the BD to the L3out
Localisation : Tenant > Networking > Bridge Domain

- Go to the Bridge domain which need to access the L3out
- Click on **Policy** > **L3 Configuration**
- Into L3out, click « **+** » and add the object **WAN-L3out**

9 Create Contract and attach it to the EPGs
*Localisation : **Tenant** > Contract > Standard*

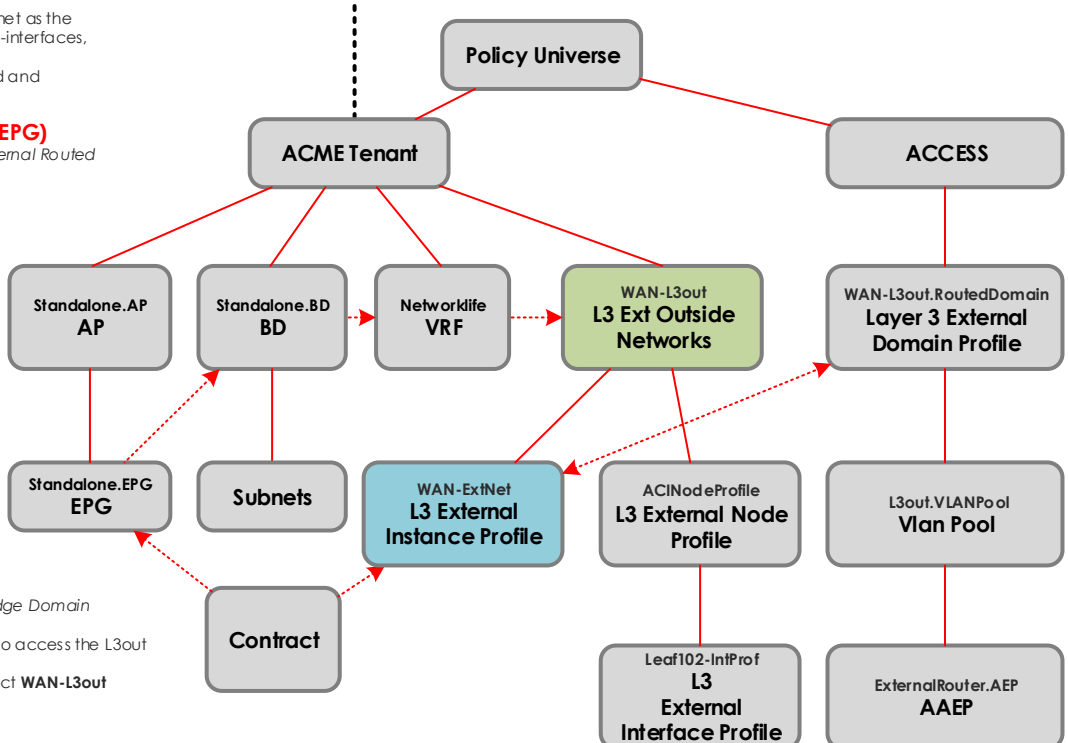
- Create a standard contract, with a filter allowing IP any.
- Configure the External EPG **WAN-ExtNet** as *Provider*
- Configure the **vZany** (EPG Collection for VRF) as *Consumer* (one application for all BDs)

Configuration Steps



Don't forget to attach your L3out to each BD.

Don't forget the contract.



Fabric Tab

1 Configure VLAN Pool
Localisation : Fabric > Access Policies > Pools > Vlan

Name **L3out.VLANPool**
Vlan: **10**

2 Configure External Routed Domain
Localisation : Fabric > Access Policies > Physical and External Domains > External Domains

Name: **WAN-L3out.RoutedDomain**
Vlan Pool: **L3out.VLANPool**

3 Configure AEP
Localisation : Fabric > Access Policies > Policies > Global > Attachable Access Entity Profiles

Name: **ExternalRouter.AEP**
Domain: **WAN-L3out.RoutedDomain**

4 Configure Interface Policies
Localisation : Fabric > Access Policies > Policies > Interface
Reuse previously created objects

5 Configure Interface Policy Groups
Localisation : Fabric > Access Policies > Interface > Leaf Interface > Policy Groups > Access Port

Name: **ExternalRouter.APPG**
Link: **1G-Auto**
STP: STP-BPDU-Guard-on
STP: STP-BPDU-Filter-on
PFC: PFC-auto
LACP: LACP-active
AAEP: **ExternalRouter.AEP**

6 Configure Interface Profiles
Localisation : Fabric > Access Policies > Interface > Leaf Interface > Profiles

Name: **Leaf101-LeafProf**
- Access Port Selector: **Eth1.01**
- Access Block Port: **1/1**
- Interface Policy Group: **StandaloneServer.APPG**

Name: **Leaf102-LeafProf**
- Access Port Selector: **Eth1.01**
- Access Block Port: **1/1**
- Interface Policy Group: **ExternalRouter.APPG**

Author: Benoit GONCALVES – 2020 – ACI 4.2

NetworkLife
Another packet in the network....

Cisco ACI — L3Out (Layer 3 Out)

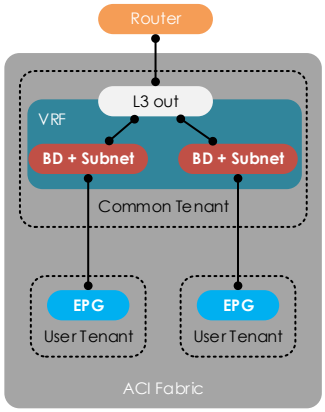
Configuration Steps

Shared L3out with multiple Tenants

3 validated designs are possible for « shared services »:

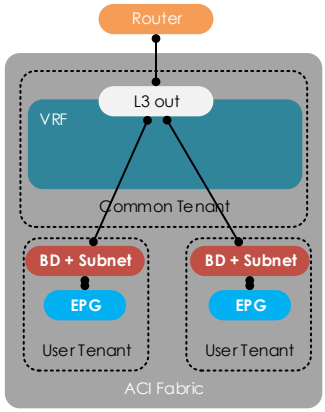
Option 1 - BD in Common Tenant

- **Shared L3 out** for the fabric with static/dynamic routing in Tenant Common.
- All Endpoint groups (**EPGs**) are configured in respective **user Tenant(s)**
- Bridge Domains (**BDs**), subnets, and **VRFs** are all configured in the **Tenant common**.



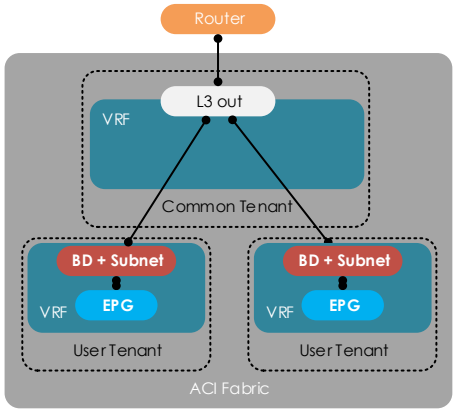
Option 2 - BD in User tenant

- **Shared L3** out for the fabric with static/dynamic routing in Tenant Common.
- All Endpoint groups (**EPGs**), Bridge Domains (**BDs**), and subnets are configured within the customer's respective **user Tenant(s)**
- The **VRF** is configured in the **Tenant common** where the L3out is configured.



Option 3 - Inter-VRF Leaking with Shared L3out

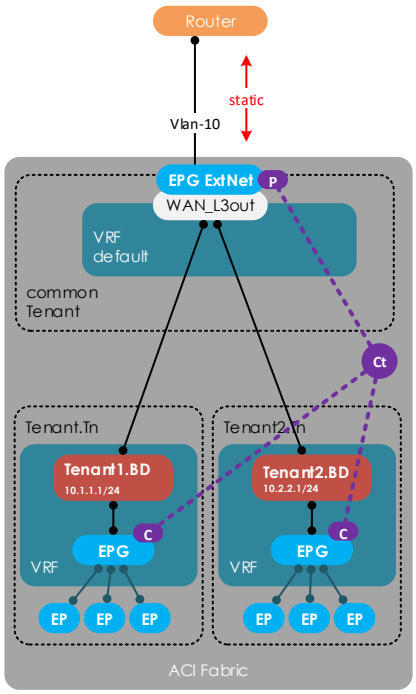
- **Shared L3out** for the fabric with static/dynamic routing in Tenant Common.
- All Endpoint groups (**EPGs**), Bridge Domains (**BDs**), subnets and **VRFs** are configured within the customer's respective **user Tenant(s)**
- **Only L3out** is configured in the **common tenant**.



HowTo Configure Option 3 - Inter-VRF Leaking with Shared L3out

Make sure the IP subnets in user tenants do not overlap, this design requires them to be shared between VRFs.

In this example, we reuse the physical topology of the page 2 (L3out on leaf 102), but the logical configuration is changing.



User Tenants

1 Configure the Tenant **Tenant1.Tn** / Configure the VRF **Tenant1.VRF**

2 Configure the **Bridge Domain**

Localisation : Tenant Tenant1.Tn > Networking > Bridge Domains > YourBD > L3 Configurations

Name: **Tenant1.BD** — Tenant1.BD 10.1.1.1/24

On L3 configuration, enable unicast routing and create the subnet 10.1.1.1/24 with the following options:
- **Advertise Externally** - to advertise these gateway subnets out to Shared L3Out to the internet
- **Shared between VRFs** - To leak the subnets to the common tenant.

NOTE – Do not associate L3out listed on the BD; when we use an Inter-vrf Shared L3out, we do not need to associate the user Tenant BDs with the L3out in Tenant Common.

3 Configure the **AP & EPG**

Localisation : Tenant > Application Profiles

Name of AP: **Standalone.AP**
Name of EPG: **Standalone.EPG**
BD: **Tenant1.BD**

1 Configure the Tenant **Tenant2.Tn** / Configure the VRF **Tenant2.VRF**

2 Configure the **Bridge Domain**

Localisation : Tenant Tenant2.Tn > Networking > Bridge Domains > YourBD > L3 Configurations

Name: **Tenant2.BD** — Tenant2.BD 10.2.2.1/24

On L3 configuration, enable unicast routing and create the subnet 10.2.2.1/24 with the following options:
- **Advertise Externally** - to advertise these gateway subnets out to Shared L3Out to the internet
- **Shared between VRFs** - To leak the subnets to the common tenant.

NOTE – Do not associate L3out listed on the BD; when we use an Inter-vrf Shared L3out, we do not need to associate the user Tenant BDs with the L3out in Tenant Common.

3 Configure the **AP & EPG**

Localisation : Tenant > Application Profiles

Name of AP: **Standalone.AP**
Name of EPG: **Standalone.EPG**
BD: **Tenant2.BD**

Common Tenant

Moving into common tenant

4 Configure the **L3out**

Localisation : Tenant > Networking > External Routed Networks

5 Configure **Node Profile**

Localisation : Tenant > Networking > External Routed Networks

6 Configure **Logical Interface Profiles**

Localisation : Tenant > Networking > External Routed Networks > Logical Node Profiles > ACINodeProfile > Logical Interface Profiles

8 Create **Contract** and attach it to the **EPGs**

*Localisation : **Tenant Common** > Contract > Standard*

- Create a standard contract, with a **Global scope** and a filter allowing IP any.
- Configure the External EPG **WAN-ExtNet** as *Provider* (P)
- Configure the **vZany** as *Consumer* (C) *on Tenant1.VRF and Tenant2.VRF.*

7 Configure **External Networks (EPG)**

Localisation : Tenant > Networking > External Routed Networks > Networks

Name: **WAN-ExtNet** — EPG ExtNet
Subnets: **0.0.0.0/0**

Tick the following options:

- **External Subnets for the External EPG** – allow this subnet in the external EPG

- **Shared Route Control Subnet** – if this network is learned from the outside through this VRF, it can be leaked to the othe§l

- **Shared Security Import Subnet** – sets the classifier for the subnets in the VRF where the routes are advertised. Shared security-import subnets are used with shared L3Out configuration, not used for routing control. This setting configures an ACL in the VRF that is consuming the shared L3Out.

Author: Benoit GONCALVES – 2020 – ACI 4.2