The following figure provides an overview of the ACI policy model logical constructs.

The following is an outline of the main components in ACI Tenant. The details of each group will be explained in following order:

Logical Policy Grouping

Tenant

Application Profile

Network Grouping

Virtual Routing and Forwarding

Unique Layer 3 forwarding domain

Relation to application profile(s) with their policies

Bridge domain

Layer 3 functions

Subnet, default gateway

Bridge domain = broadcast domain

L3Out

Security Grouping

Endpoint Group

Named groups of related endpoints, for example, finance

Static or dynamic membership

Contracts

The rules that govern the interactions of EPGs

Contracts determine how applications use the network

Terms & Conditions Privacy Statement Cookie Policy EULA Trademarks Release Notes Keyboard Shortcuts

At the top level, the Cisco APIC policy model is built on a series of one or more tenants. A tenant is a logical container for application policies that enable an administrator to exercise domain-based access control. The fabric can contain multiple tenants. A tenant represents a unit of isolation from a policy perspective, but it does not represent a VRF. Tenants can represent a customer in a service provider setting, an organization or domain in an enterprise setting, or just a convenient grouping of policies.

The main features of a tenant are:

Can represent a customer, business unit, or group.

Provides a separate profile space.

Tenants only see inside their space.

Shared services can be defined between tenants.

Three tenants are preconfigured in the system by default, and cannot be deleted:

Common: A special tenant that provides services that are common to other tenants in the Cisco ACI fabric. Global reuse is a core principle in the common tenant. Examples of common services include Domain Name System (DNS), DHCP, and Active Directory.

Infra: The infrastructure tenant that is used for all internal fabric communications, such as tunnels and policy deployment, including switch-to-switch (leaf, spine, Cisco Application Virtual Switch [AVS], or Cisco Application Virtual Edge [AVE]) and switch-to-APIC. The infra-tenant does not get exposed to other tenants. It has its own VRF and bridge domains. Fabric discovery, image management, and DHCP for fabric functions are all handled within the infra-tenant. Users do not need to manually configure components in this tenant with a few exceptions such as when configuring ACI multi-pod infra.

Mgmt: 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. The management tenant enables discovery and automation of communications with virtual machine controllers.

User tenants are defined by the administrator according to the needs of users. They contain policies that govern the operation of resources such as applications, databases, web servers, network-attached storage, virtual machines, and so on.

Terms & Conditions Privacy Statement Cookie Policy EULA Trademarks Release Notes Keyboard Shortcuts
A VRF (Virtual Route Forwarding) is the largest network component in a tenant, which provides an IP address spaces and Layer 3 forwarding domain just like a normal router. Each tenant has its own VRF(s) and all tenant components such as endpoints can only belong to a VRF within the same tenant except for tenant common.

Characteristics of VRFs are:

Layer 3 Forwarding Domain

One or more per Tenant

Closed within each Tenant (except for tenant common)

Hence, even though ACI introduced application point of view when defining the network infrastructure fabric, VRF is still one of the most important components to design the ACI tenant and network infra.

For example, if multiple tenants are created per organization or department even though there is no need to allocate a dedicated VRF for each organization, users will need to configure VRF route leaking unnecessarily to everywhere across organizations for them to talk to each other, which is obviously not a scalable design. In a such scenario, it is recommended to have all organizations that share a same IP address space (VRF)

under a single tenant and its VRF. Then, logically group them with Application Profiles if needed. An alternative would be to define a VRF in tenant common, which is a special tenant with resources such as VRF to be shared across multiple tenants. The details on tenant common usage is covered in the Cisco Application-Centric Infrastructure Advanced (DCACIA) course.

VRF also provides an option "Policy Control Enforcement" to turn off the allow list security model that is enforced with EPG and contract. By default it's enforced and no communication between EPGs is allowed without a contract rule. Once it's unenforced, no contract rules will be applied, and any endpoints can talk to anyone as long as there is Layer 2 or Layer 3 reachability.

Policy enforcement within a VRF:

Terms & Conditions Privacy Statement Cookie Policy