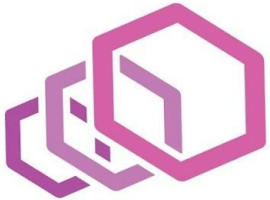


Envoy at Square

Michael Puncel and Snow Pettersen

Who are we?

- Michael Puncel
  - Software Engineer on Traffic team for ~1 year
  - Before that I worked on our deployment system called P2 (https://github.com/square/p2)
- Snow Pettersen
  - Software Engineer on Traffic team for ~1 ½ years

Agenda

- Motivation
- Infrastructure Overview
- Design
  - Control Plane
  - Facilitating Migration
  - Security
  - Traffic Shaping
- Where we are & what's next

Motivation

- Simplify client/server libraries
- Distribute load balancing responsibilities
- Abstract infrastructure from app code
- Increase agility of infrastructure changes

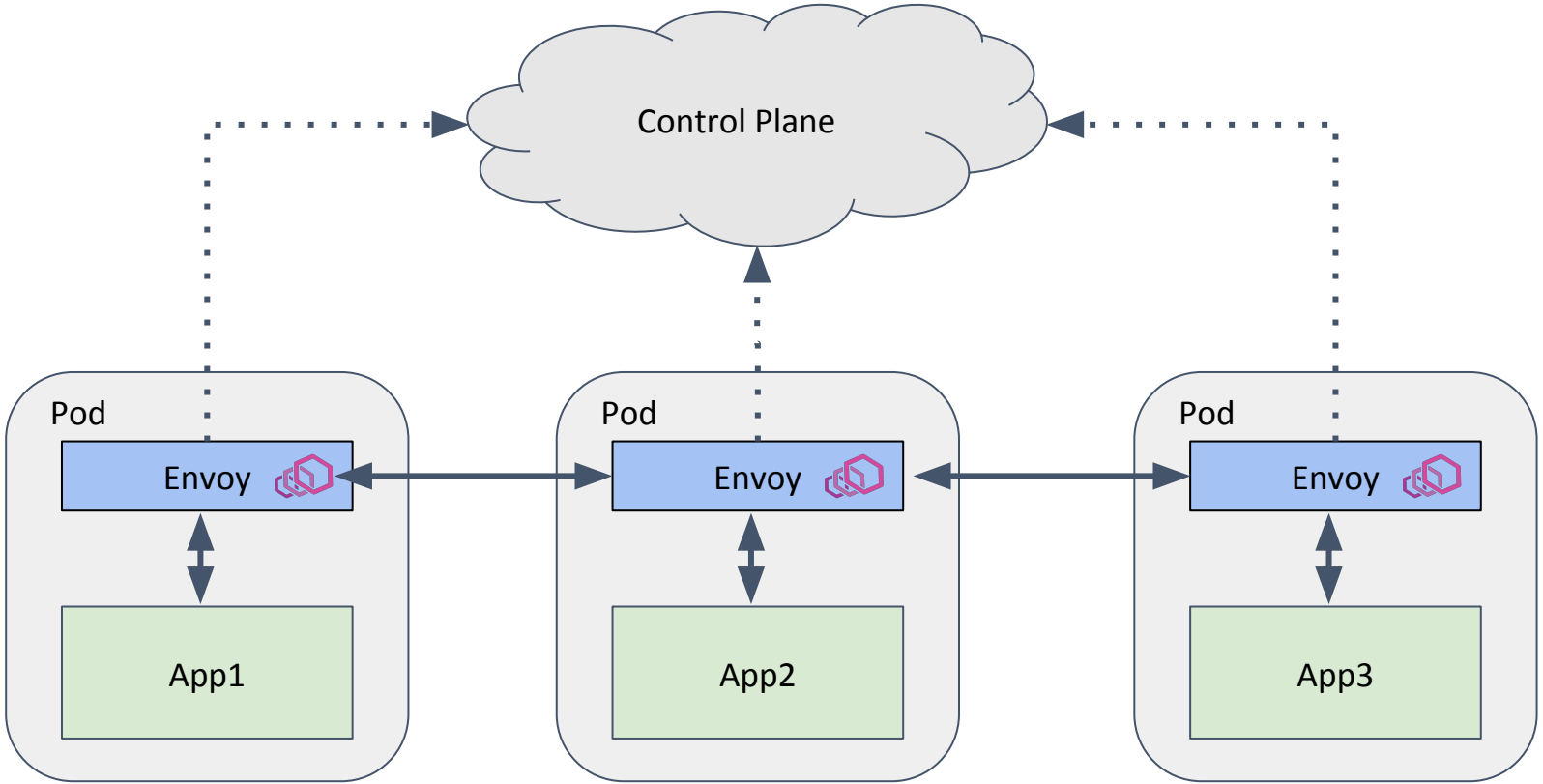
Infrastructure Overview

- Primary bare-metal on-prem, some cloud as well
- Kubernetes-like deployment system
- Multi-tenant hosts with no network namespacing
- mTLS between applications
- Centos 6/7

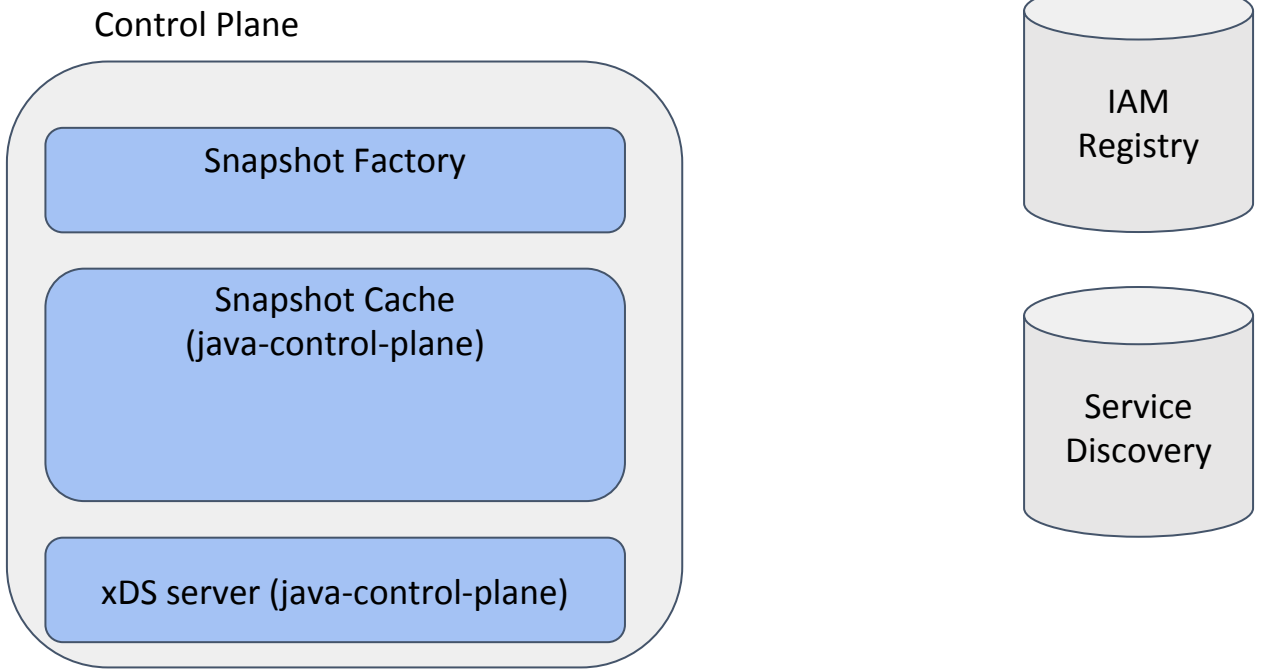
Design

Control Plane Design

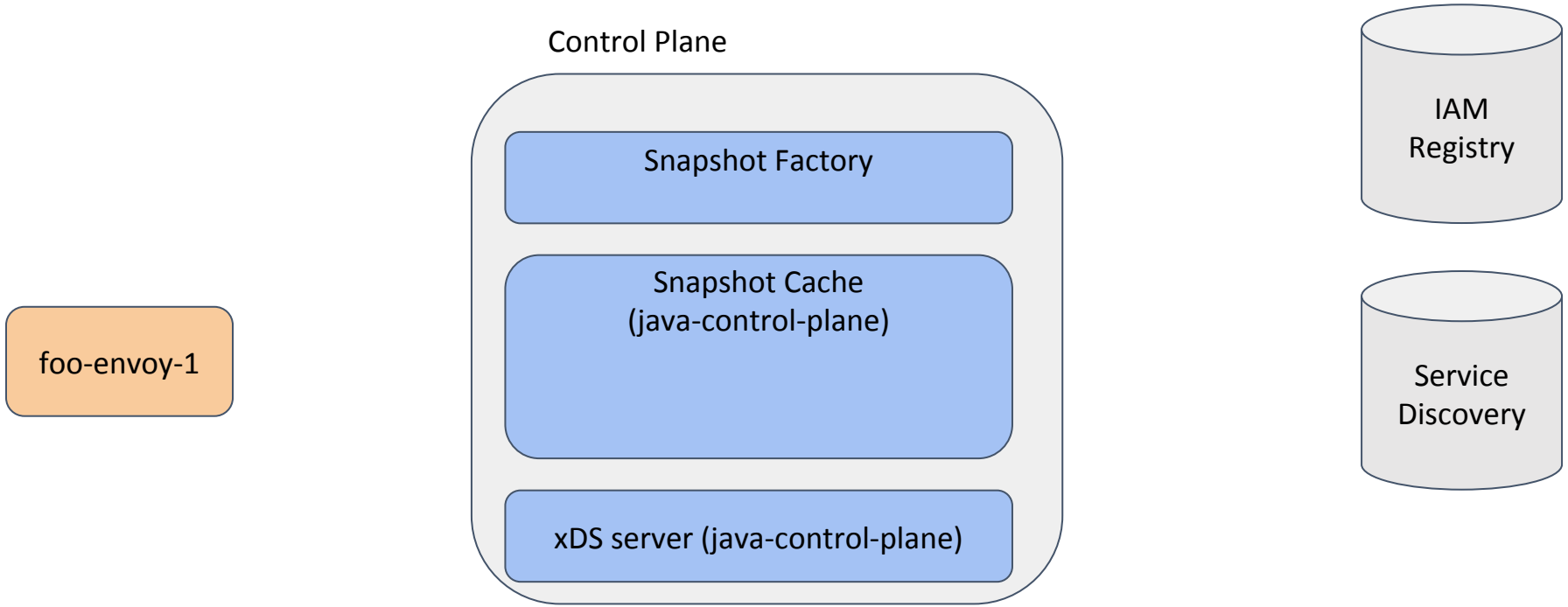
envoycon



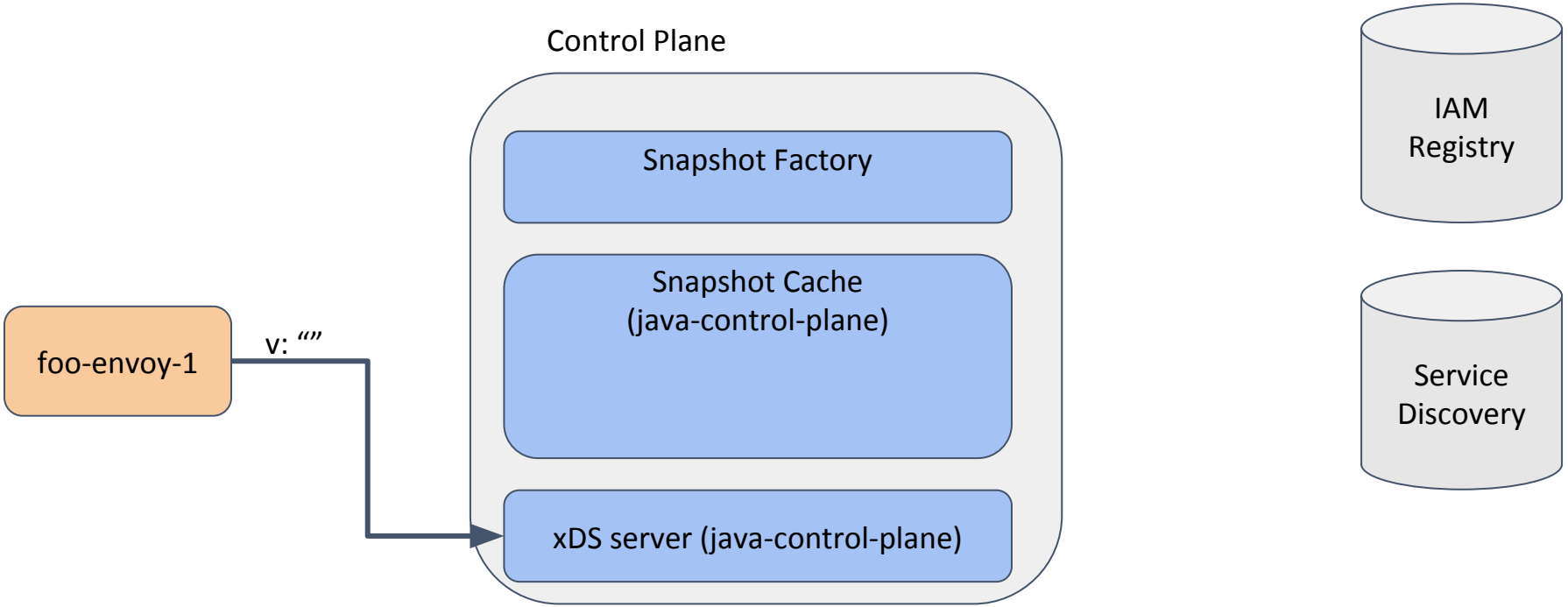
Control Plane Design



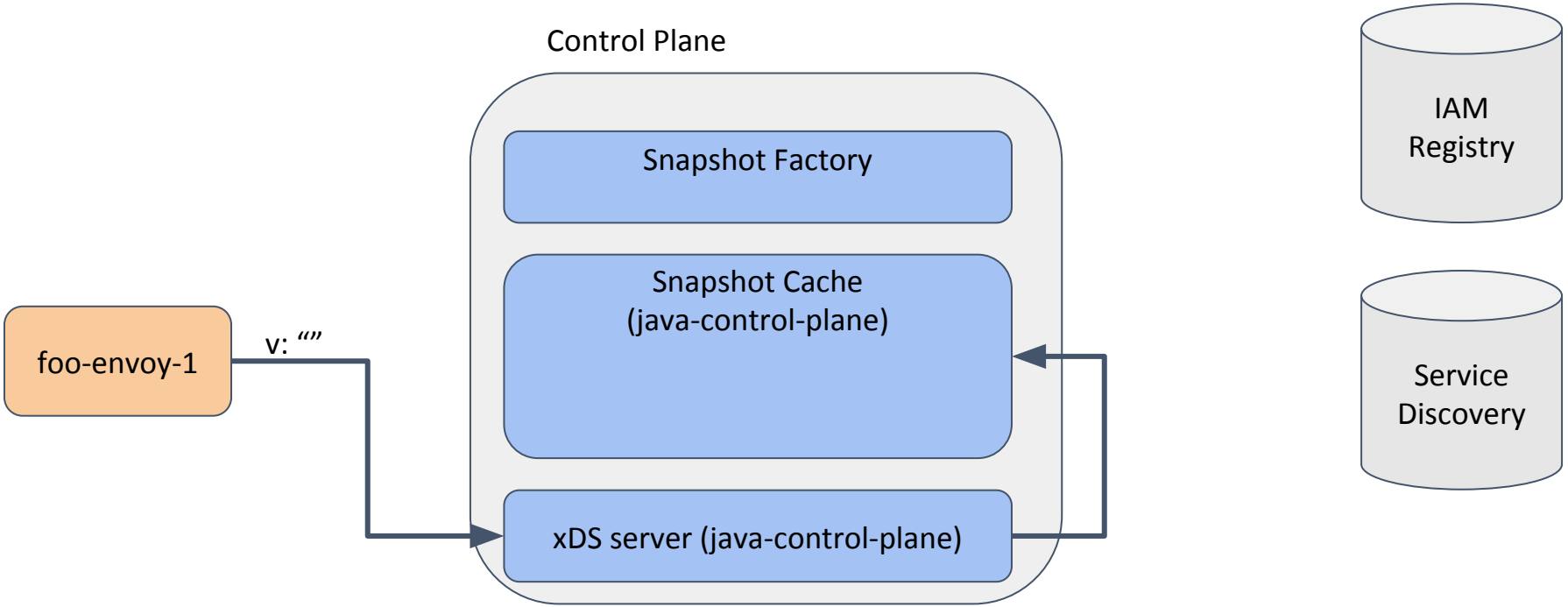
Control Plane Design



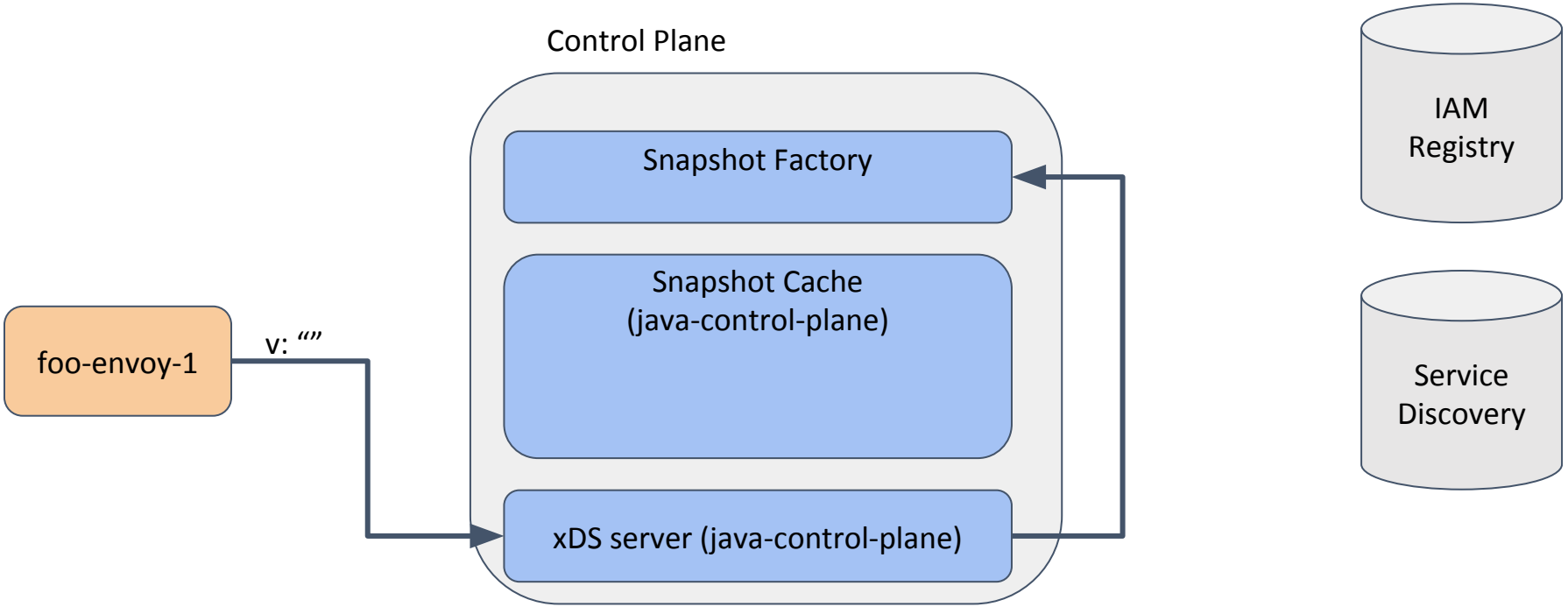
Control Plane Design



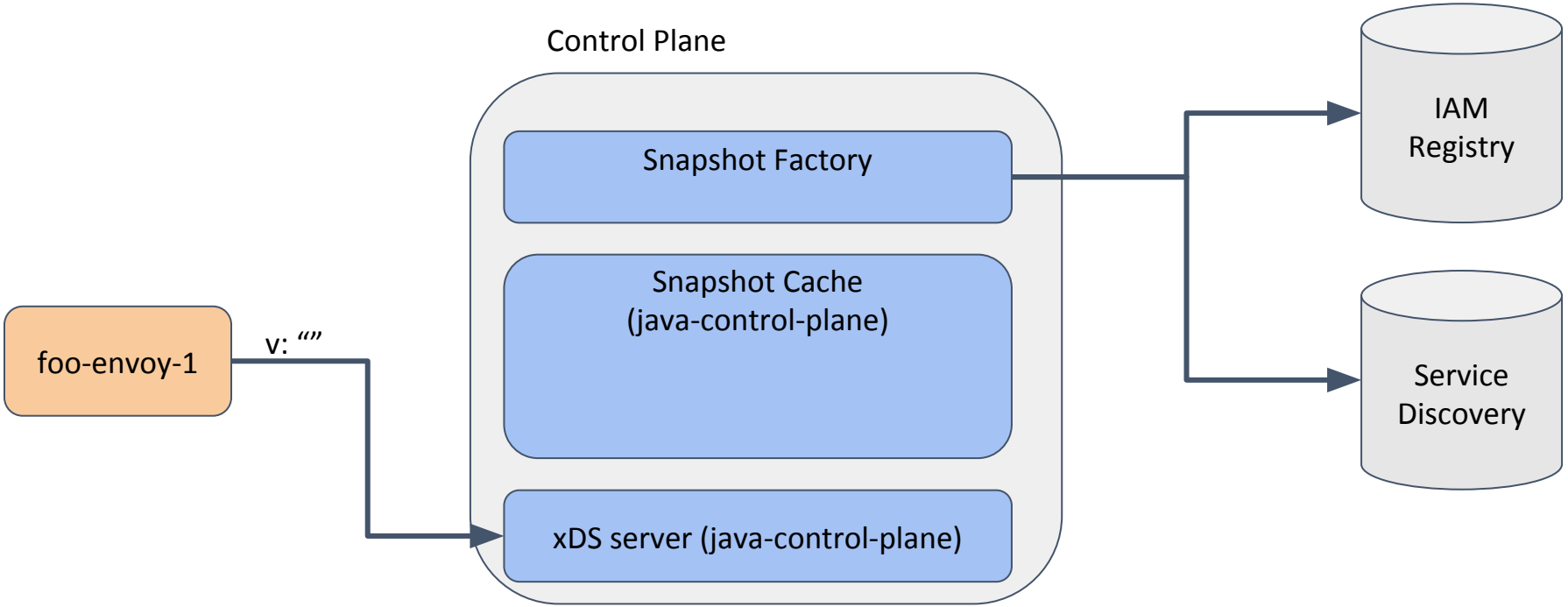
Control Plane Design



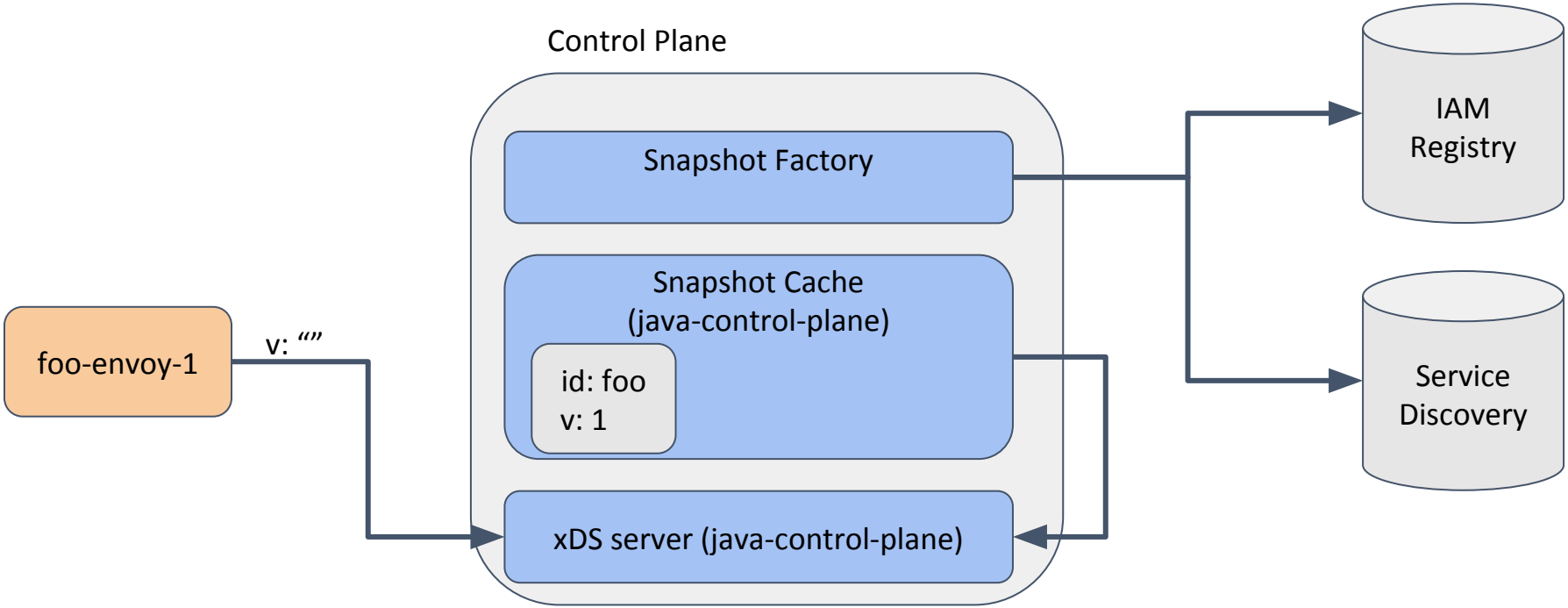
Control Plane Design



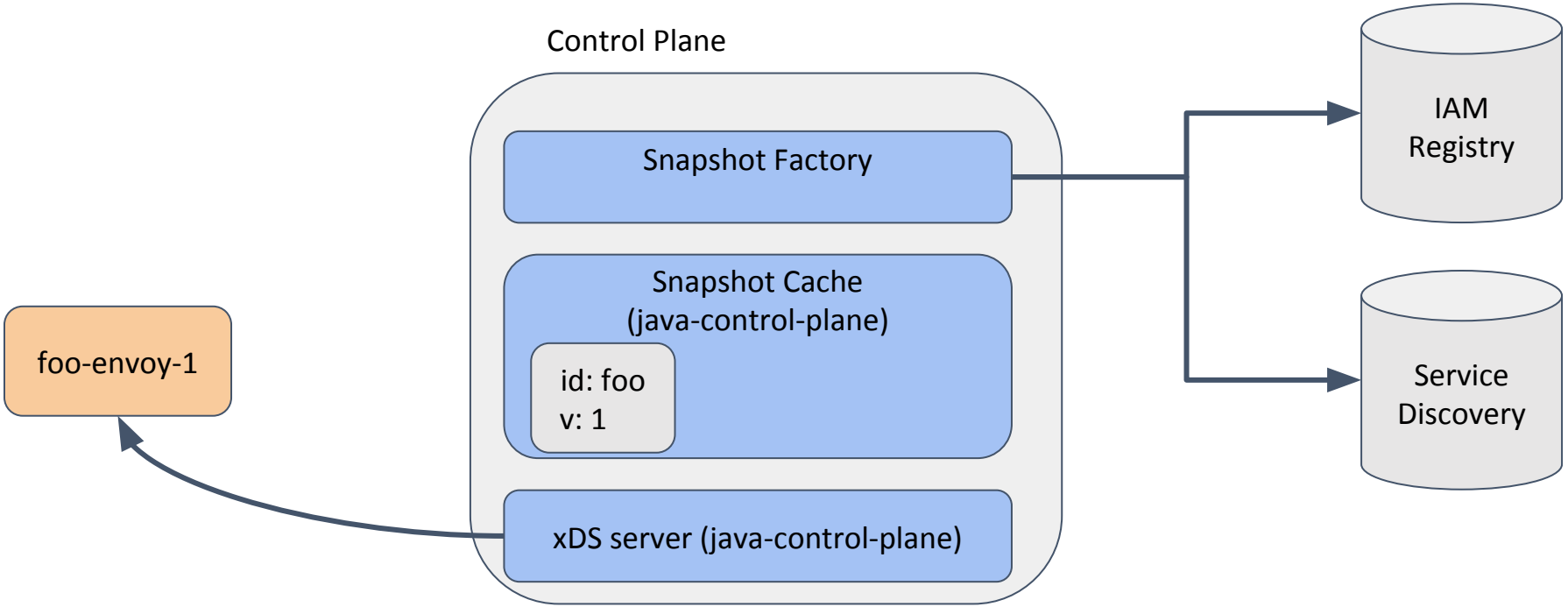
Control Plane Design



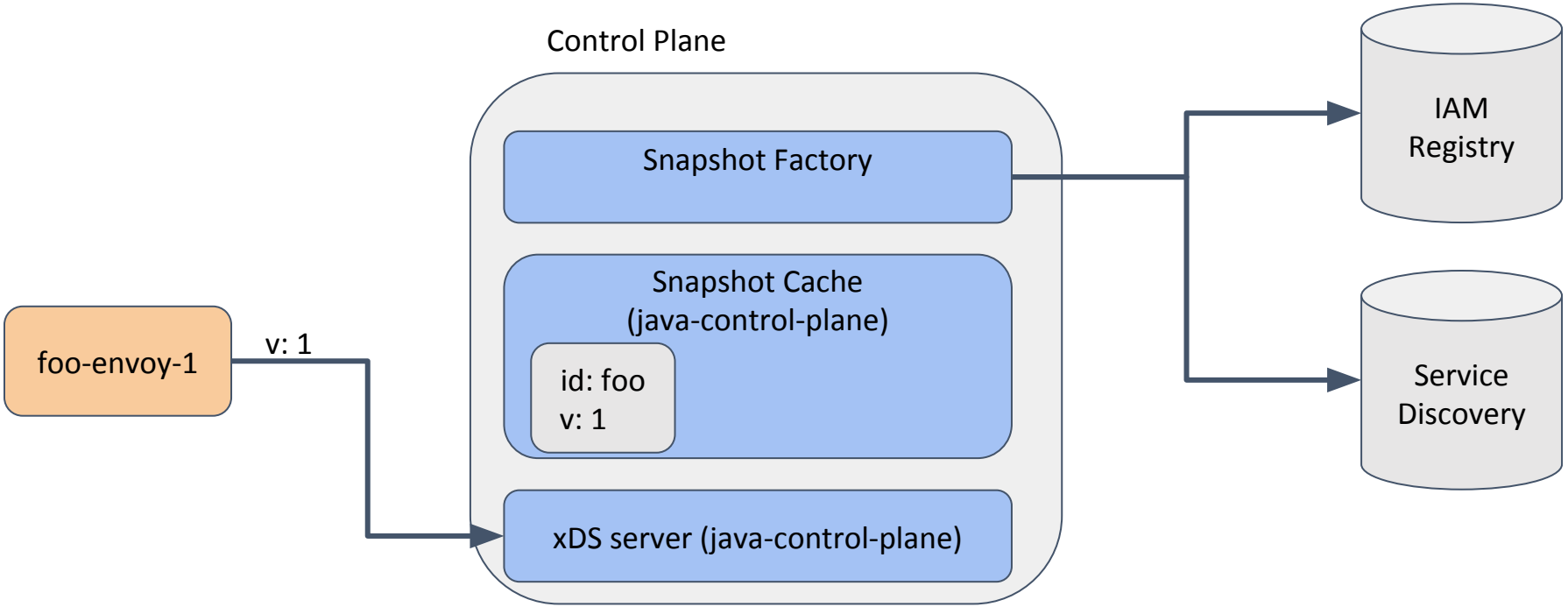
Control Plane Design



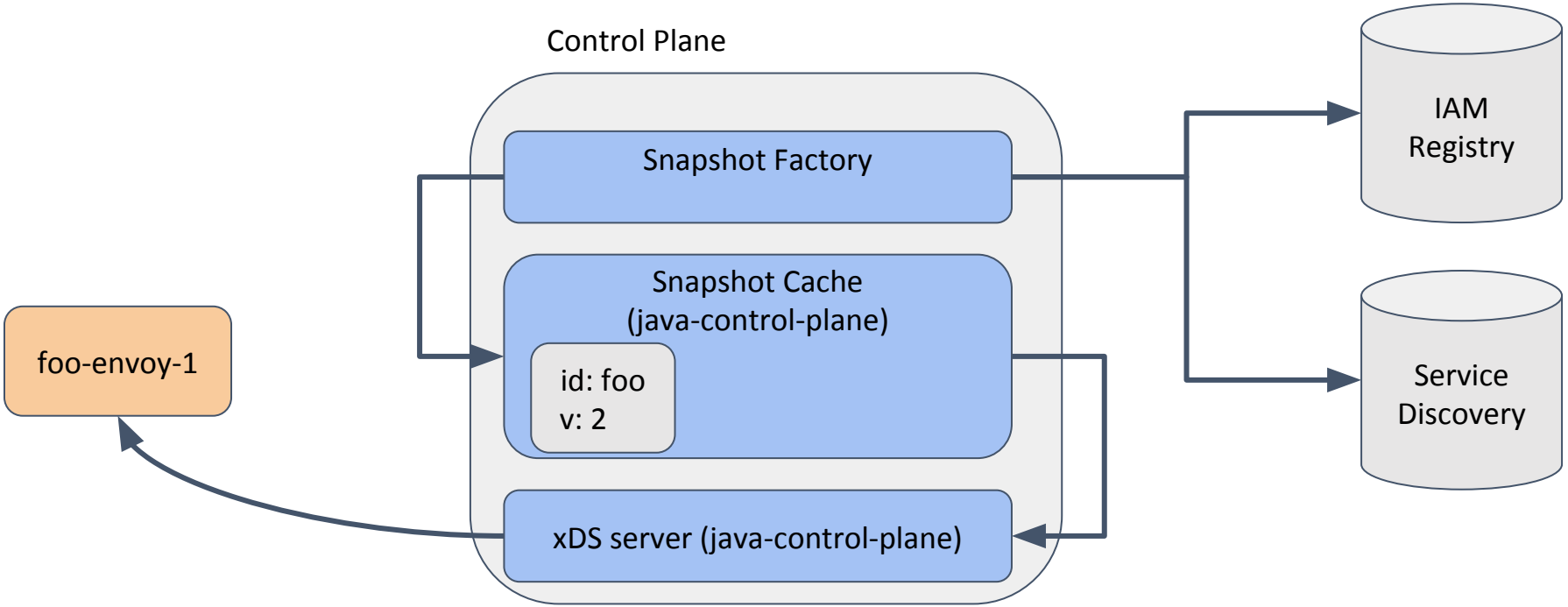
Control Plane Design



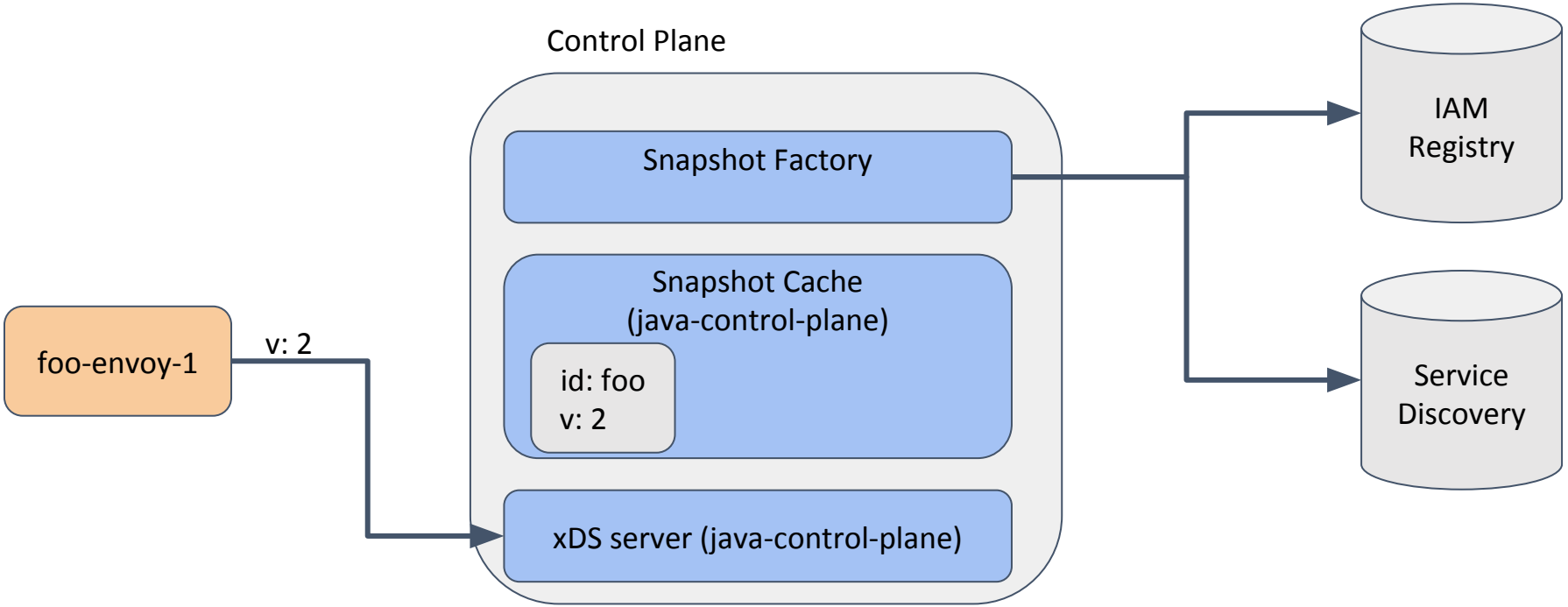
Control Plane Design



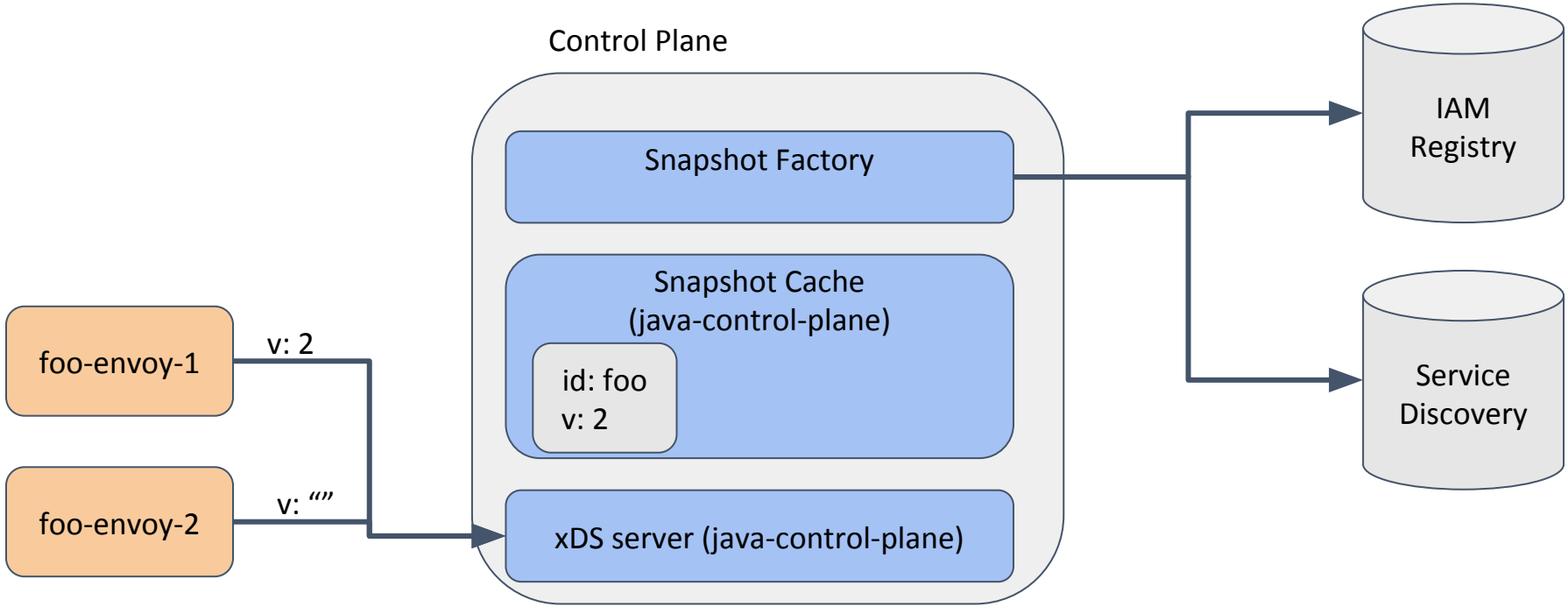
Control Plane Design



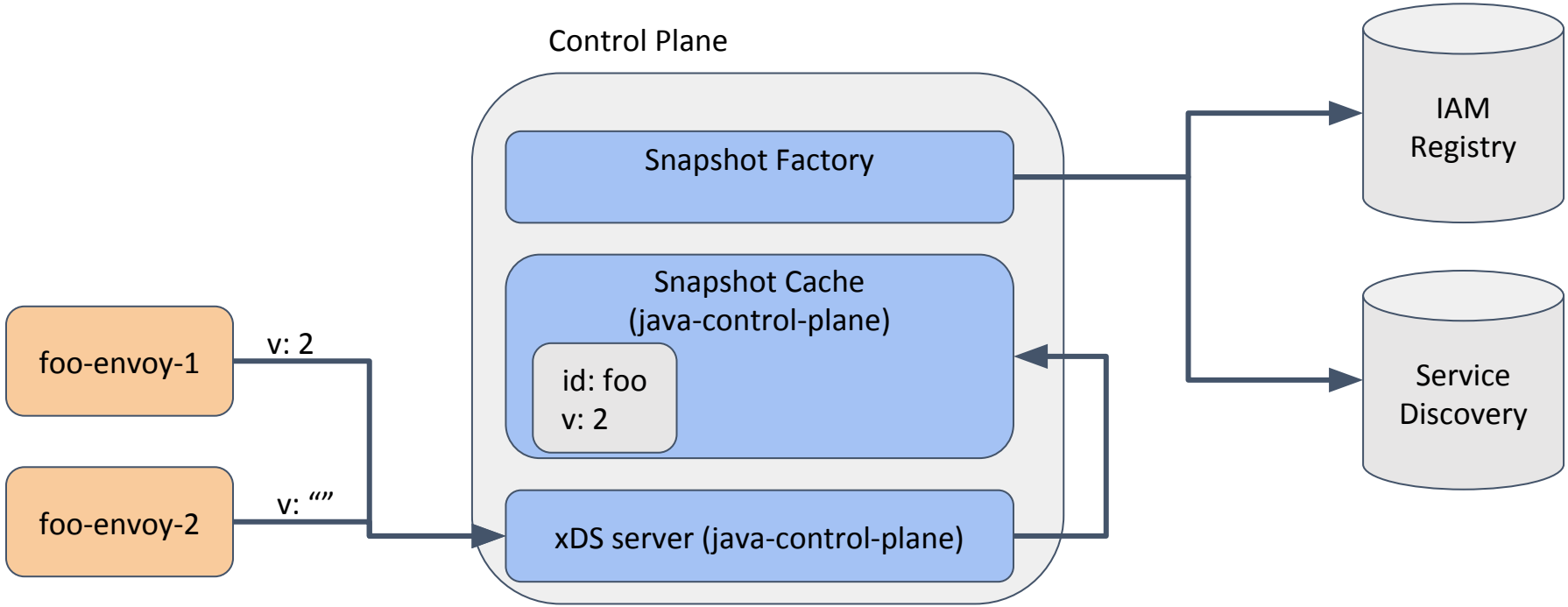
Control Plane Design



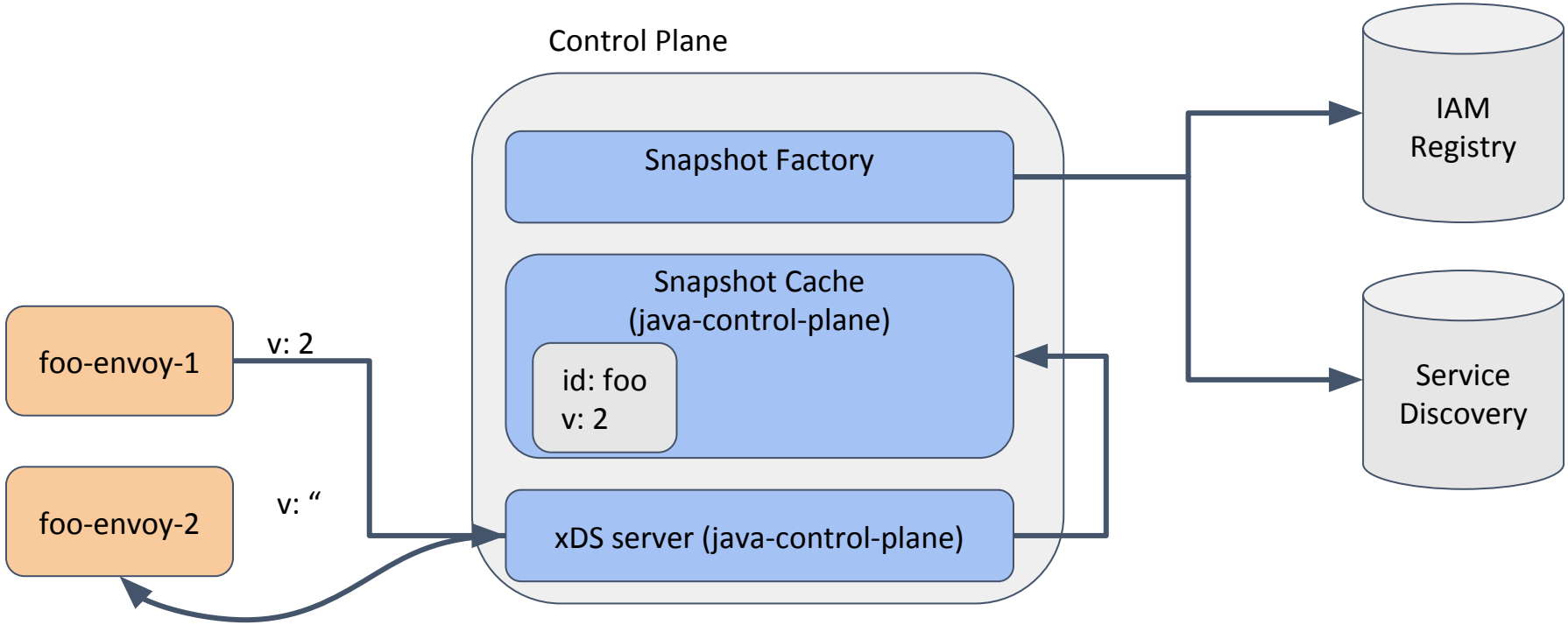
Control Plane Design



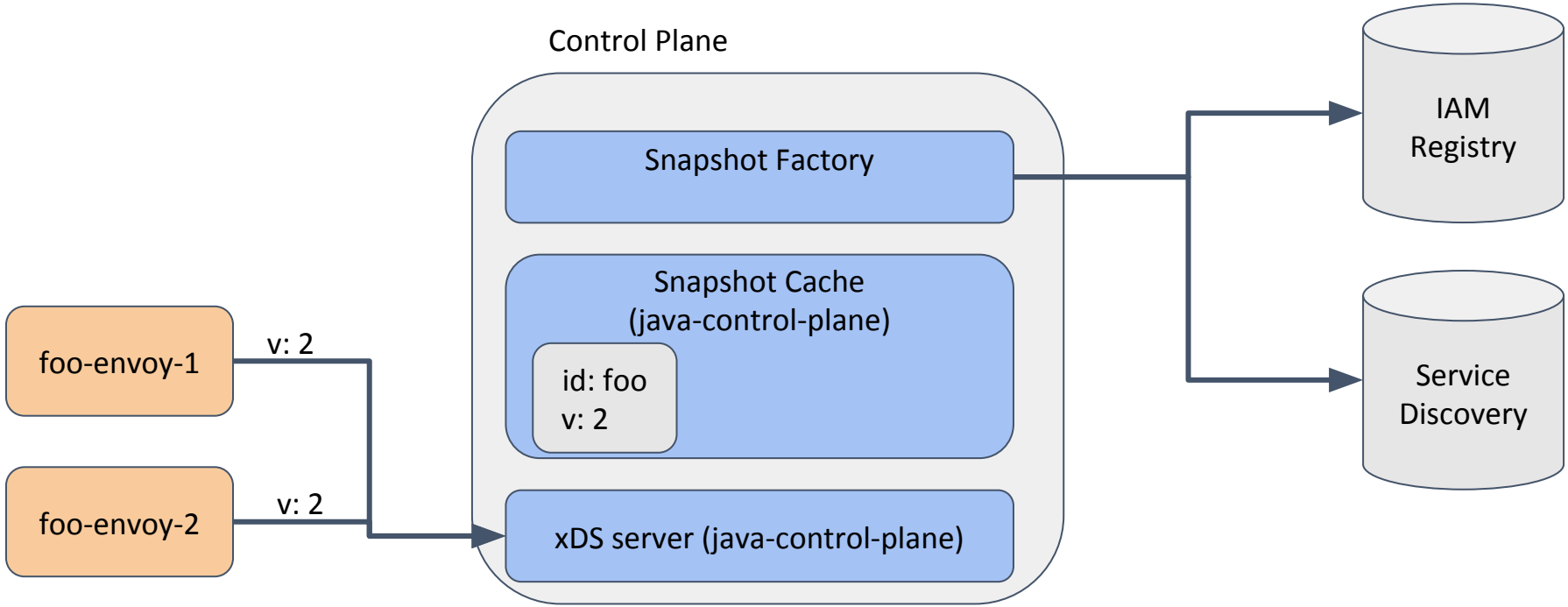
Control Plane Design



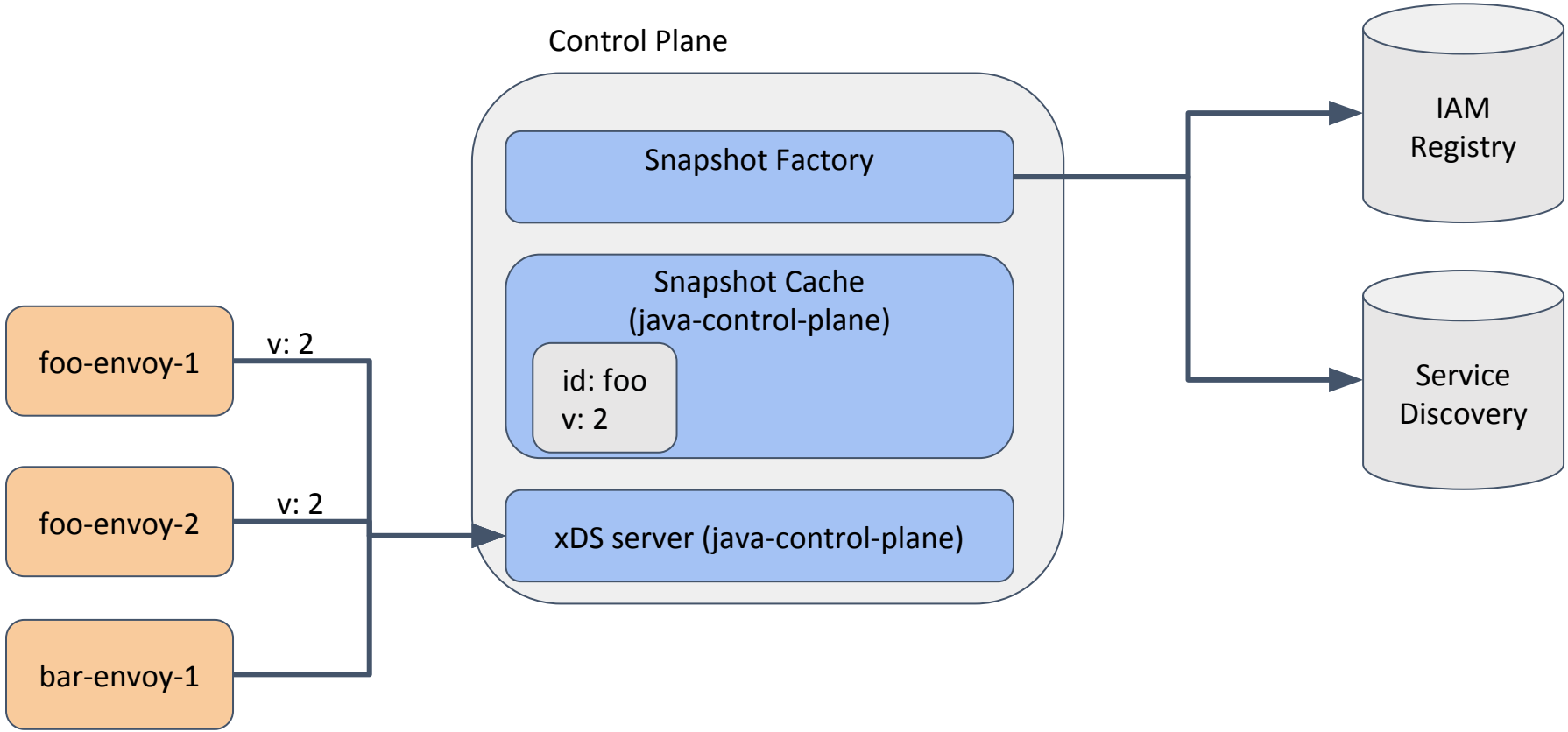
Control Plane Design



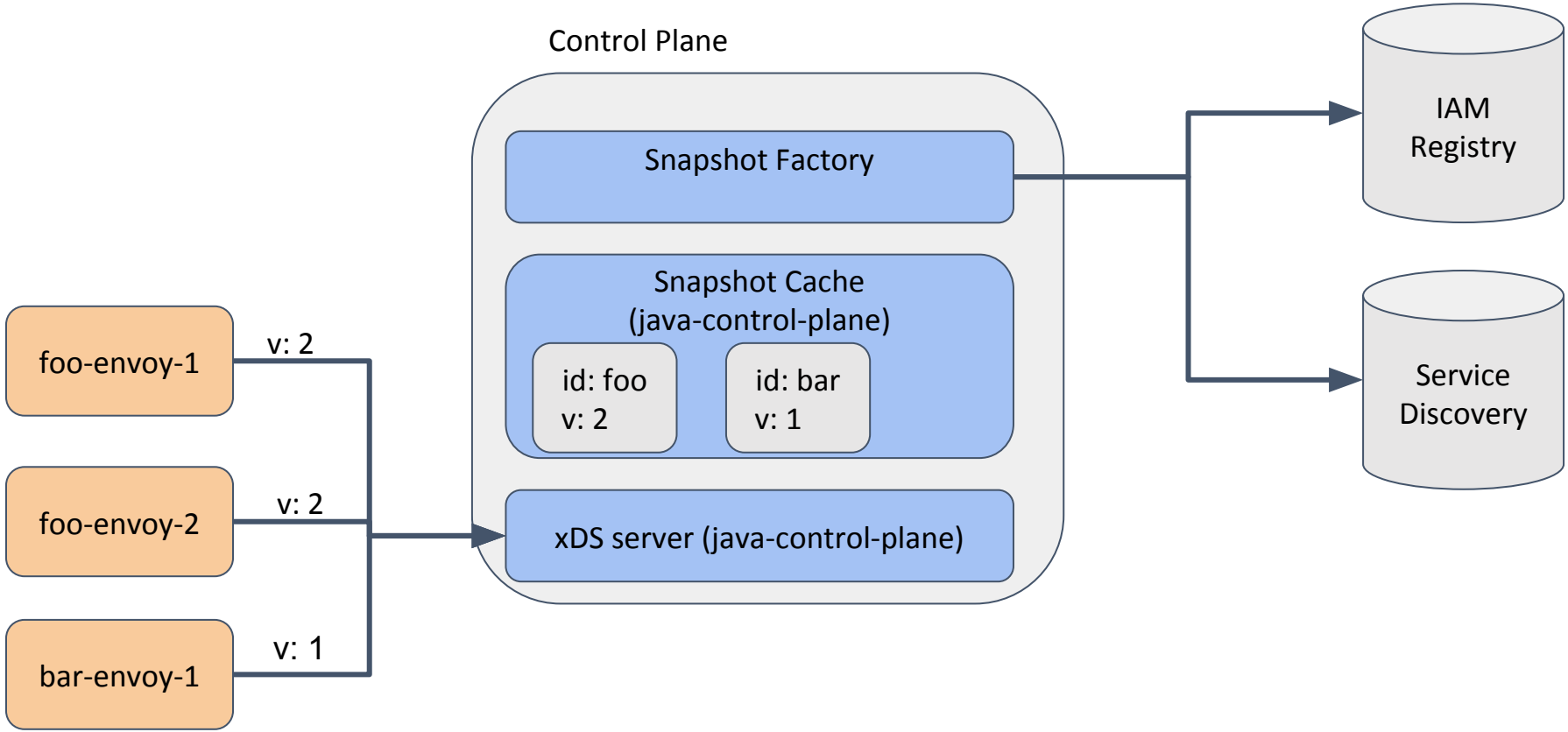
Control Plane Design



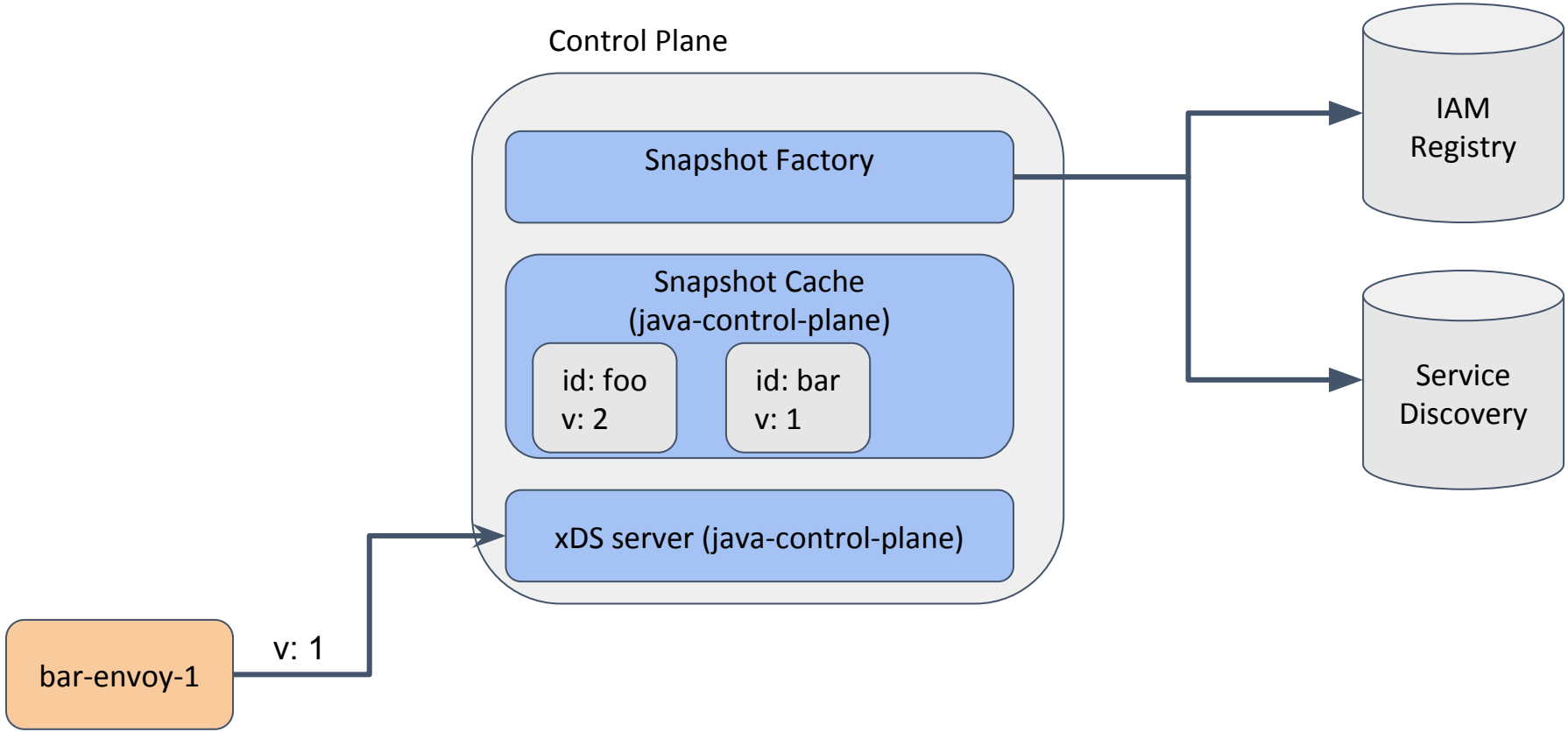
Control Plane Design



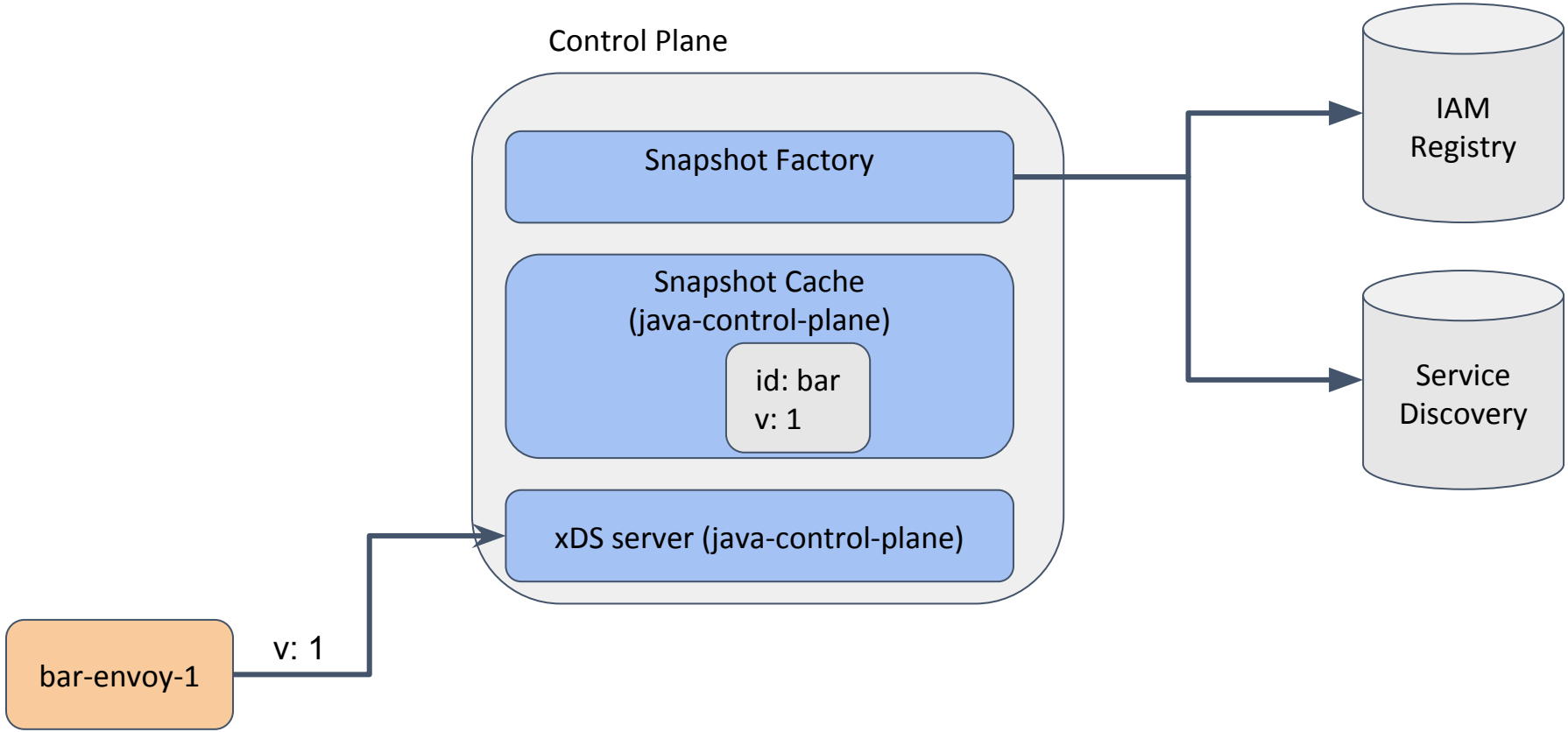
Control Plane Design



Control Plane Design

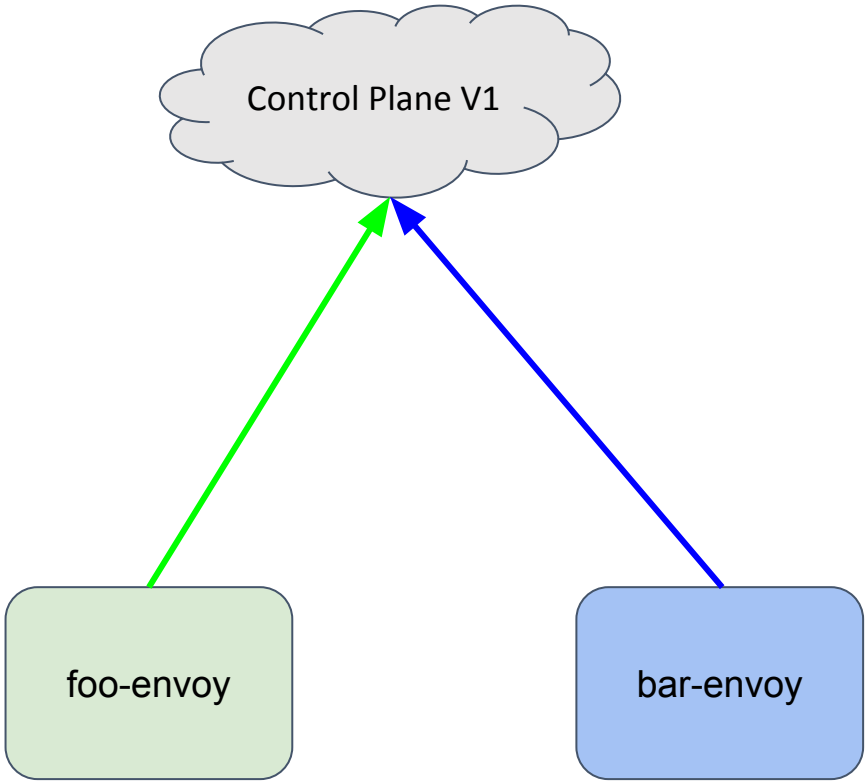


Control Plane Design

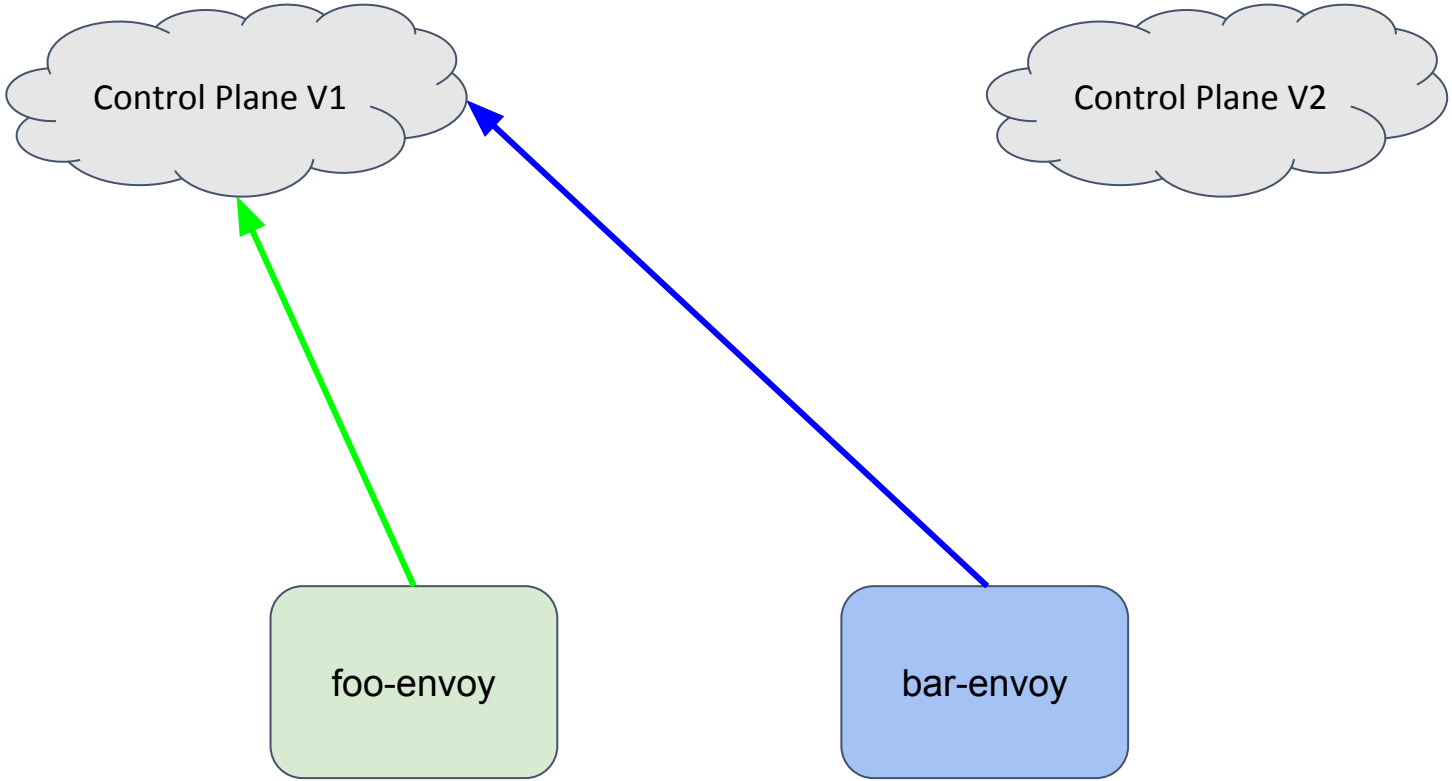


Control Plane Design

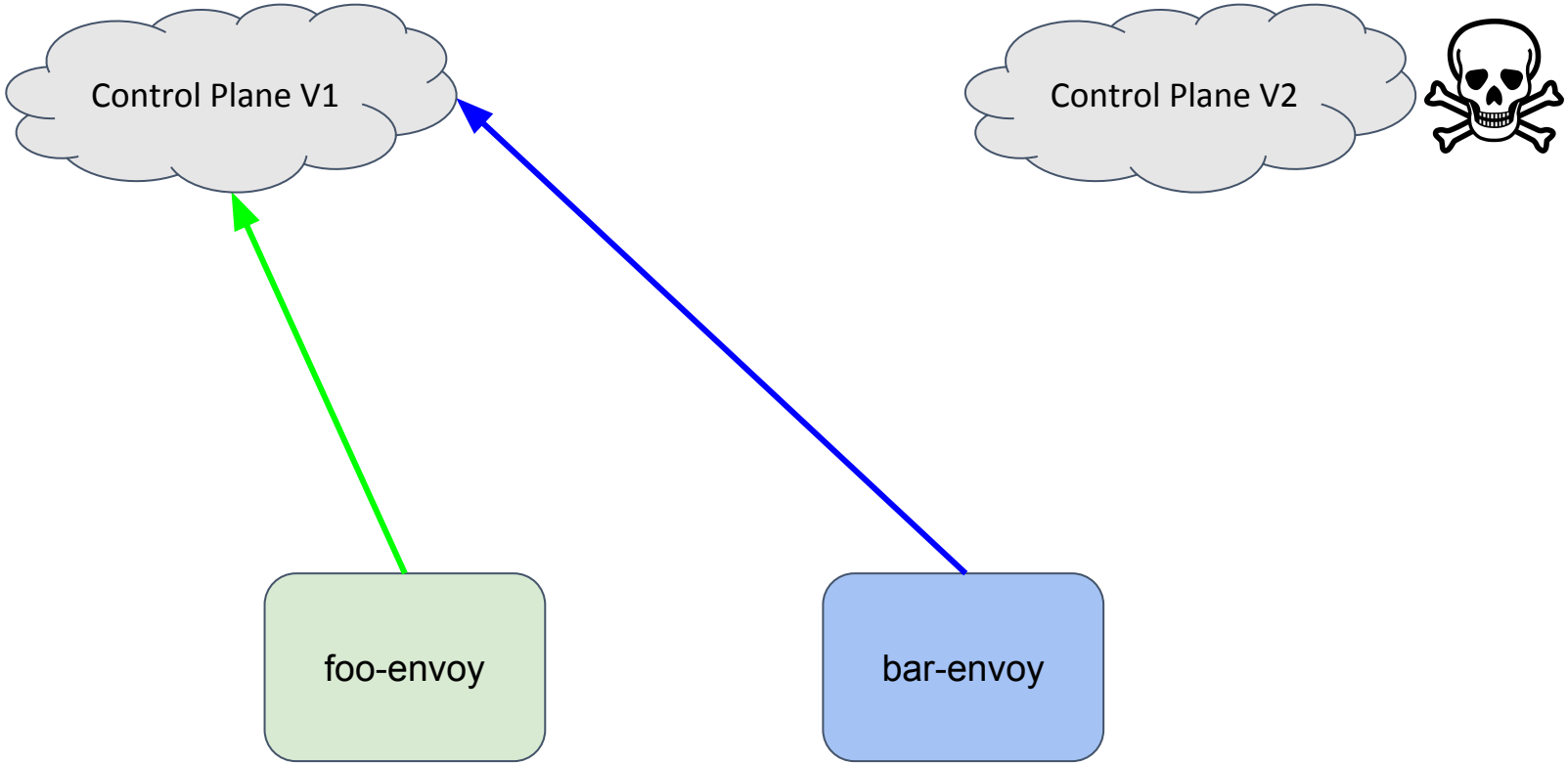
envoycon



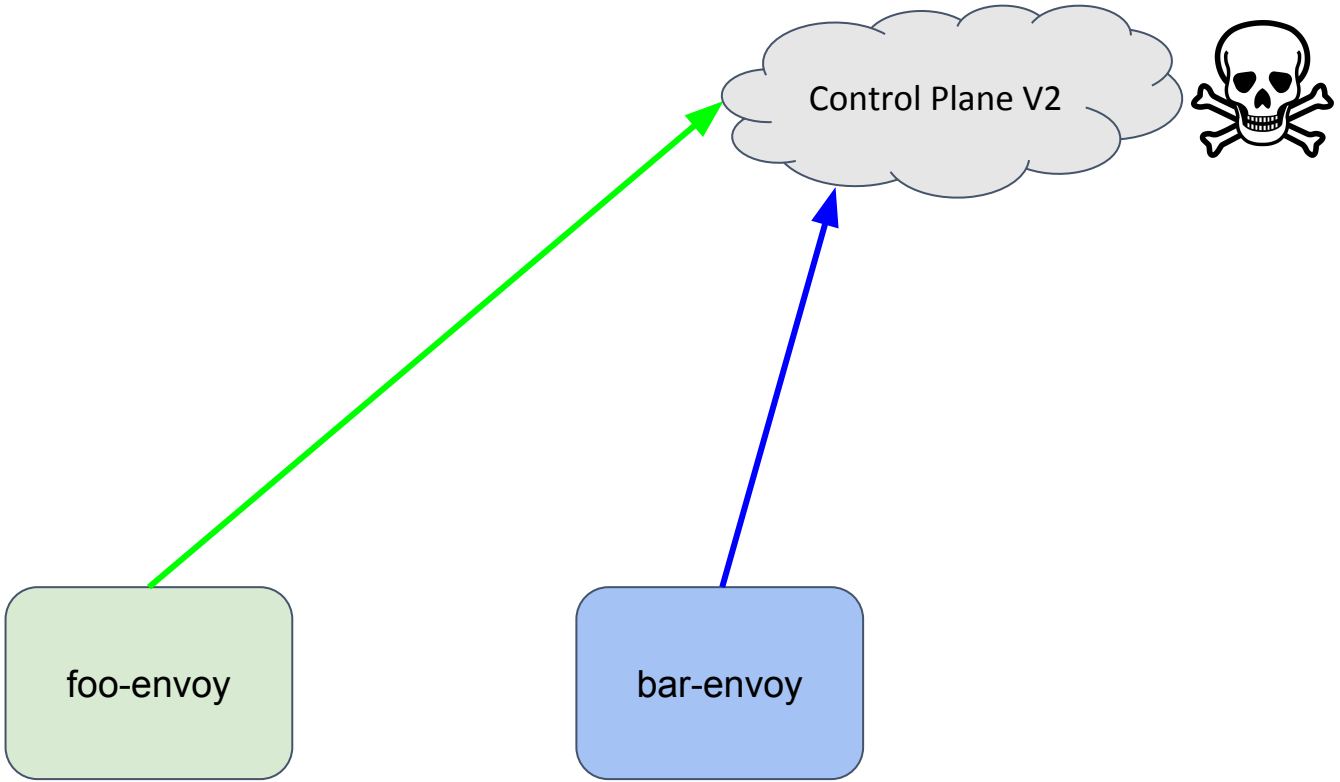
Control Plane Design



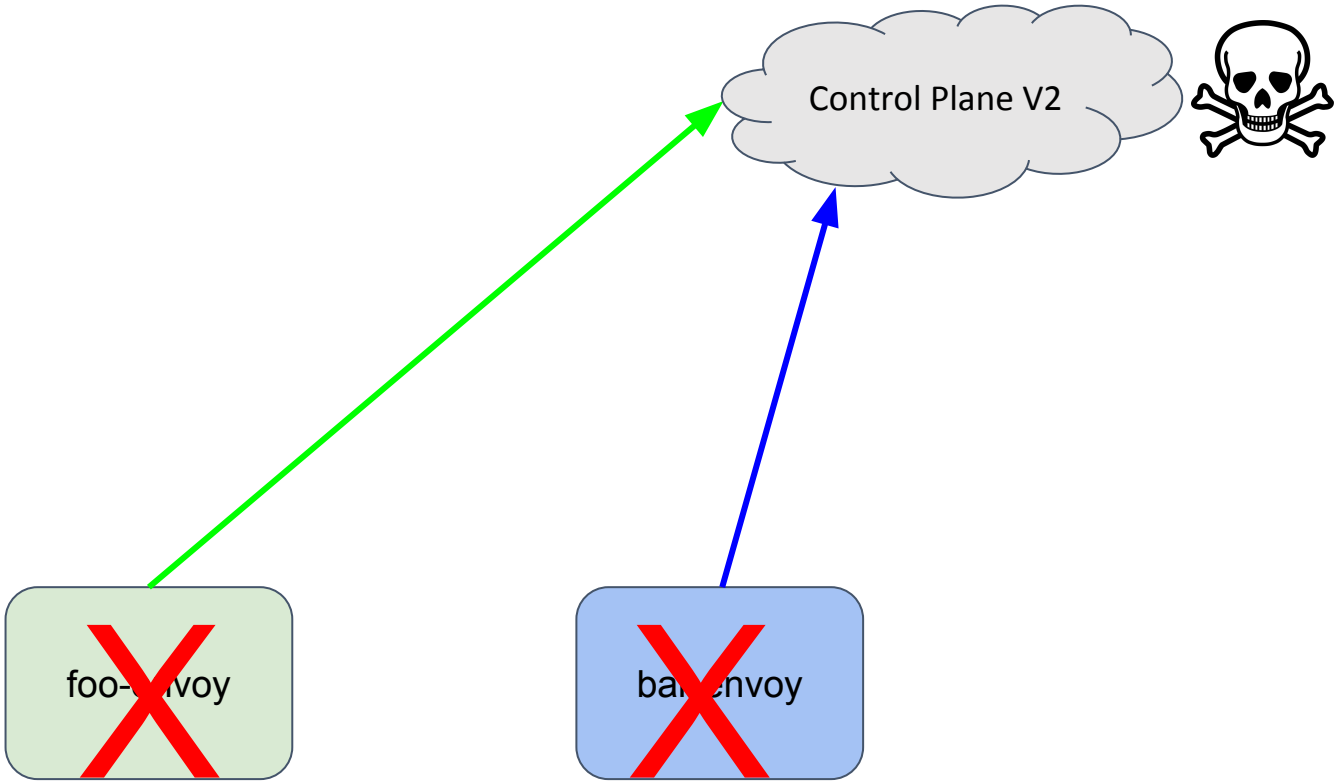
Control Plane Design



Control Plane Design

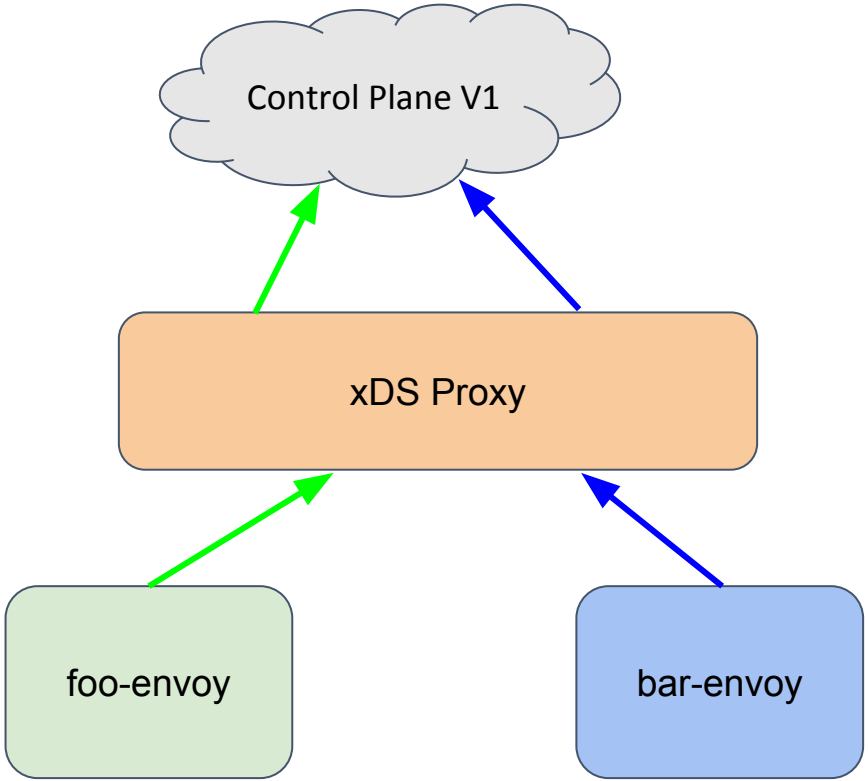


Control Plane Design

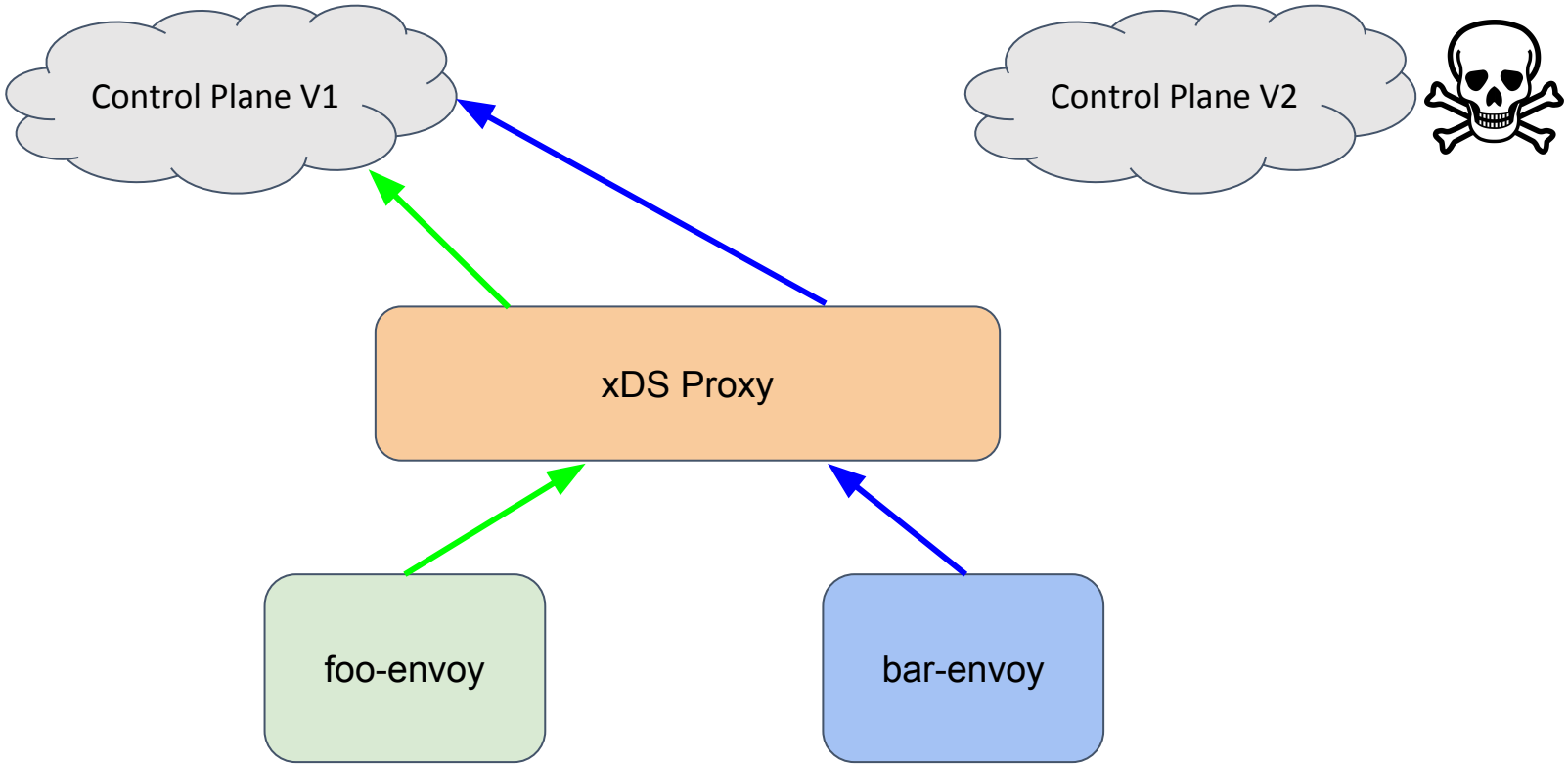


Control Plane Design

envoycon

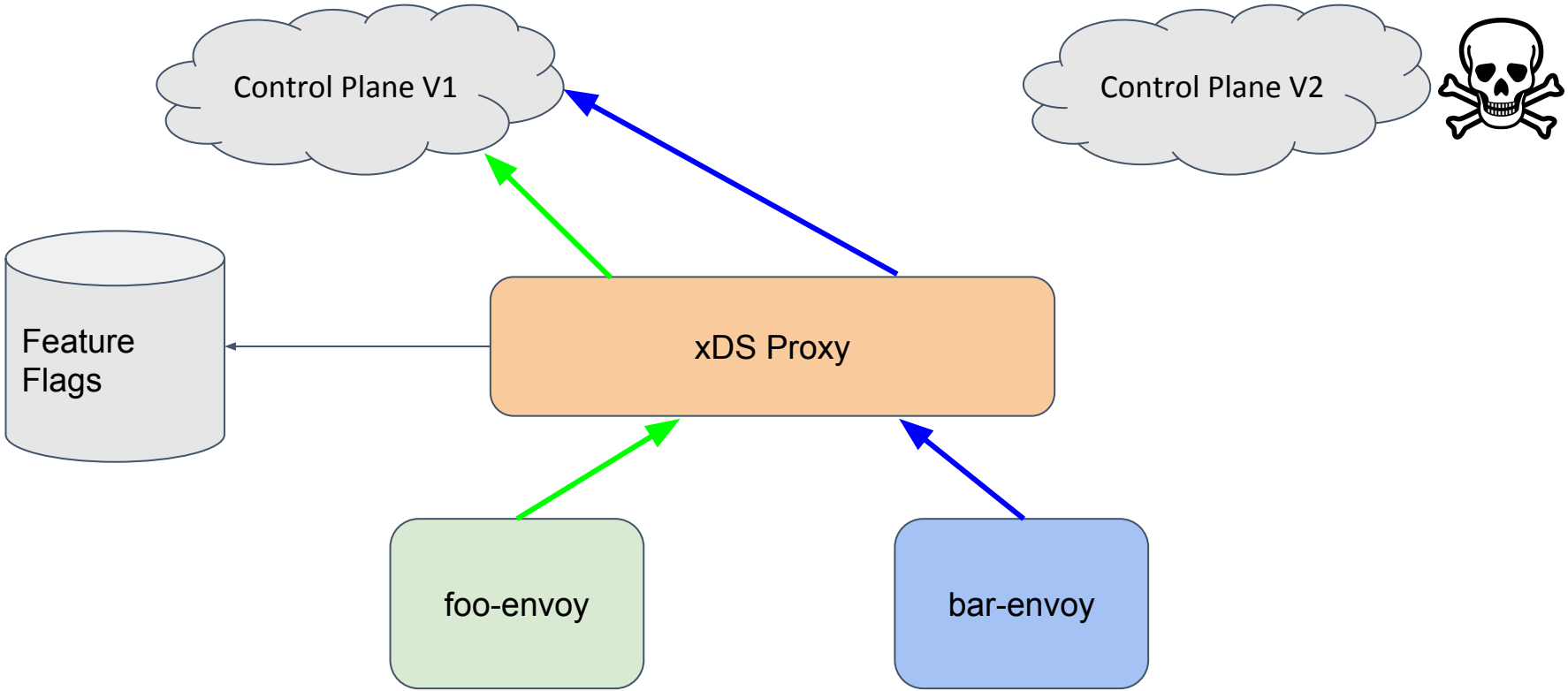


Control Plane Design

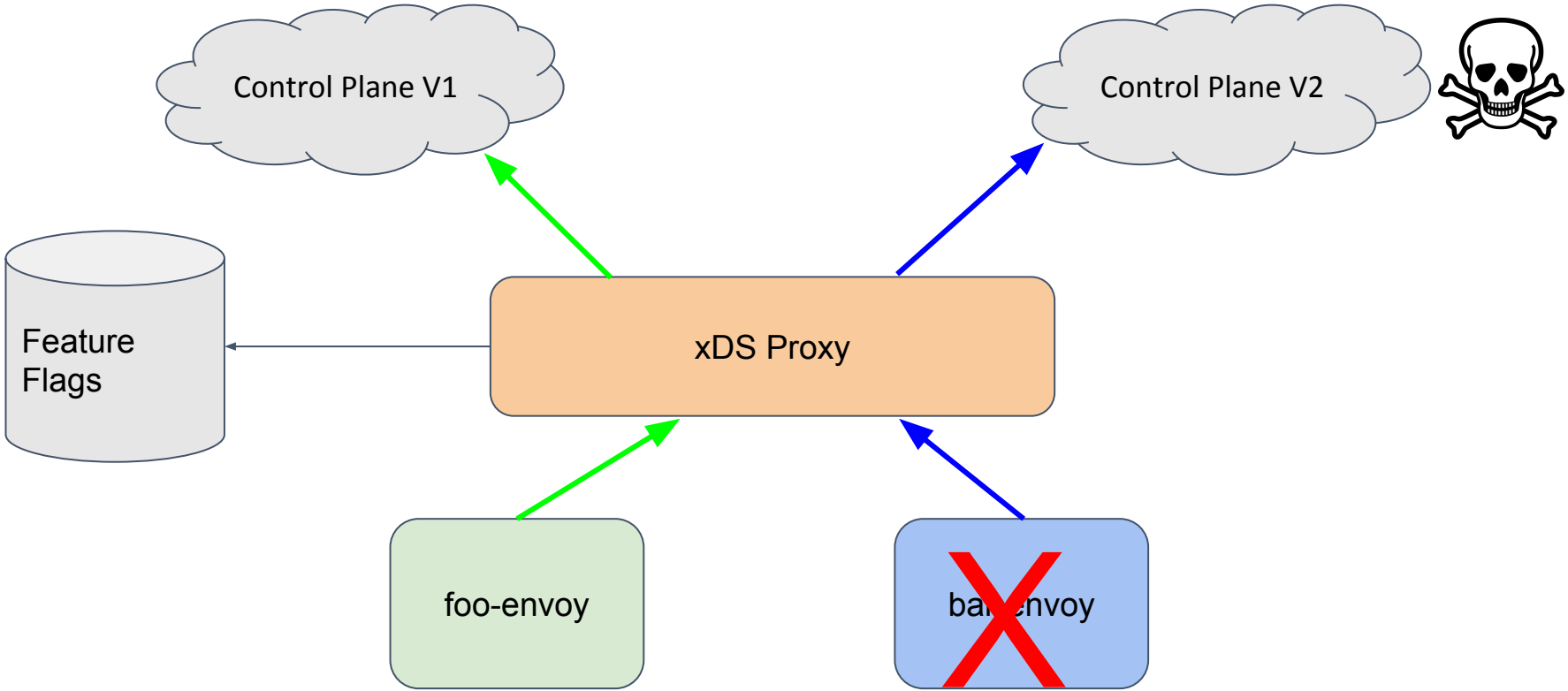


Control Plane Design

envoycon

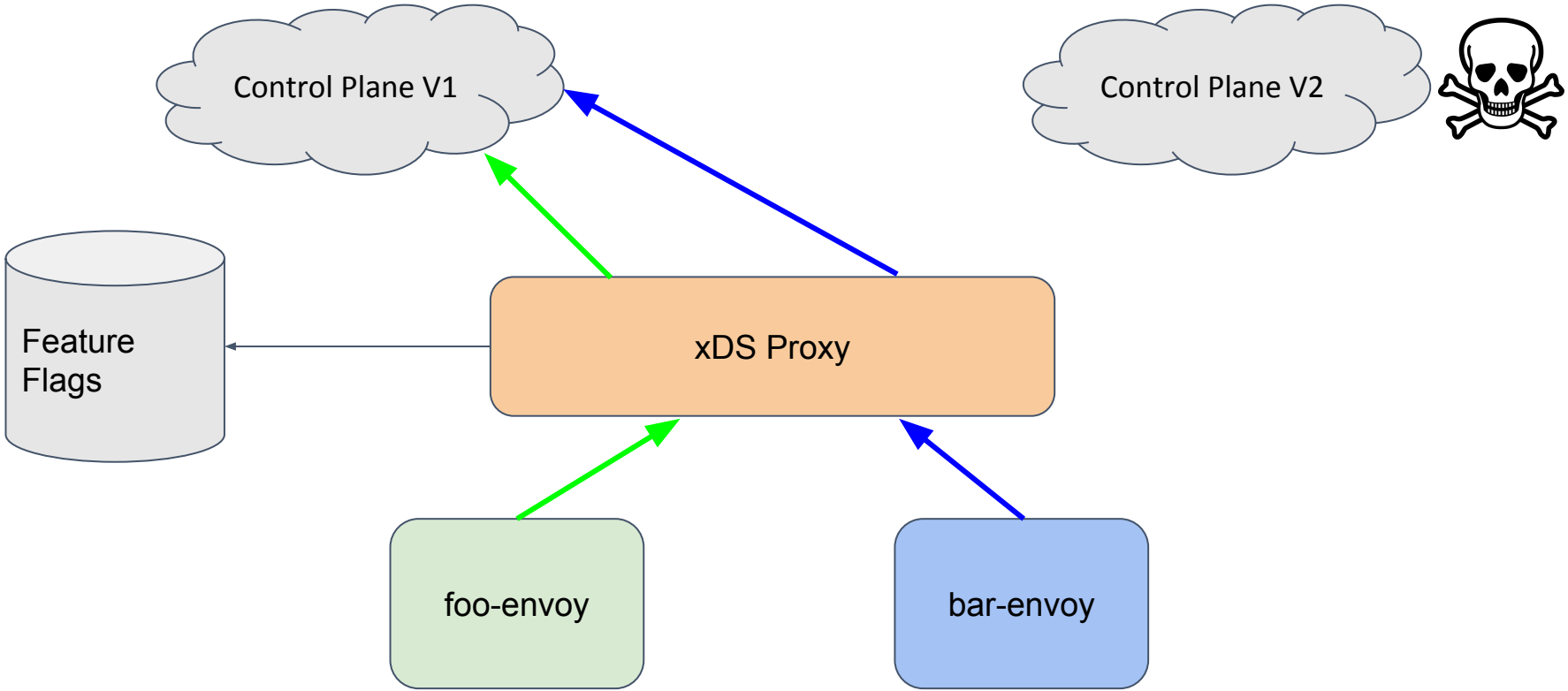


Control Plane Design

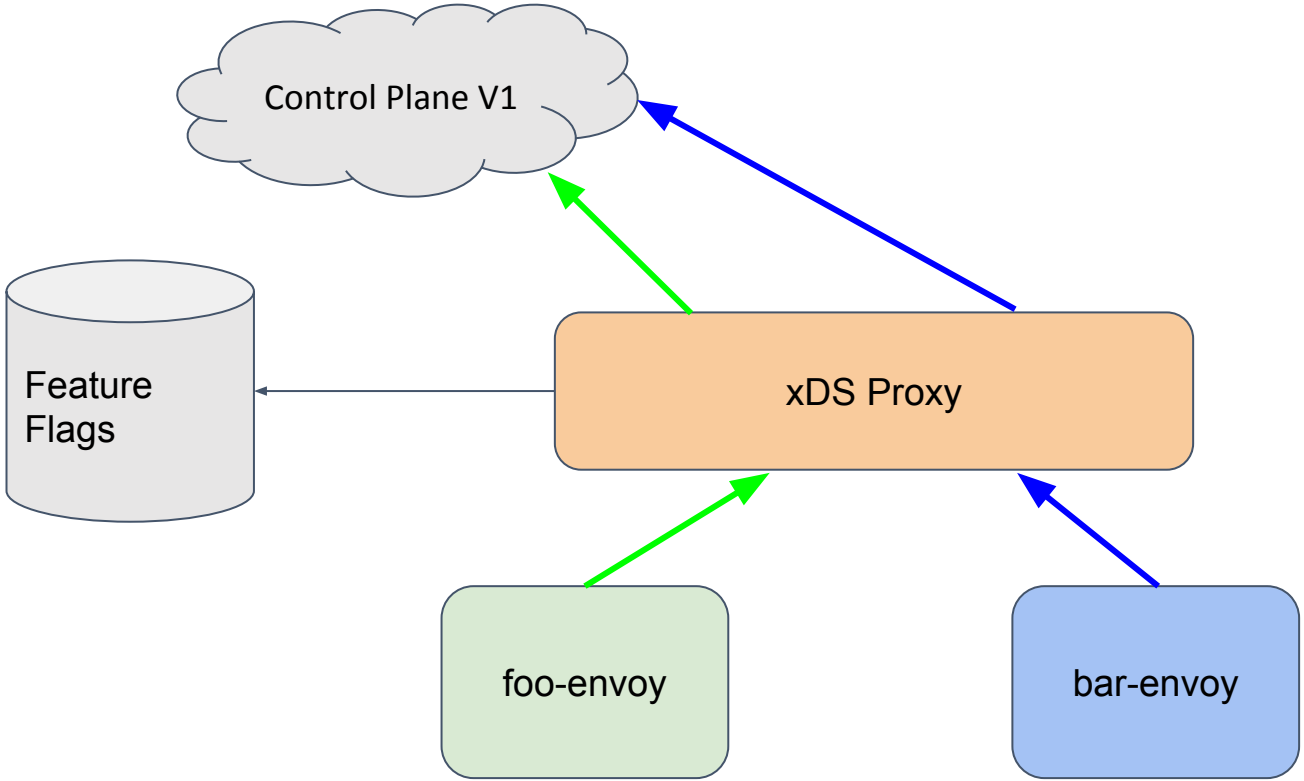


Control Plane Design

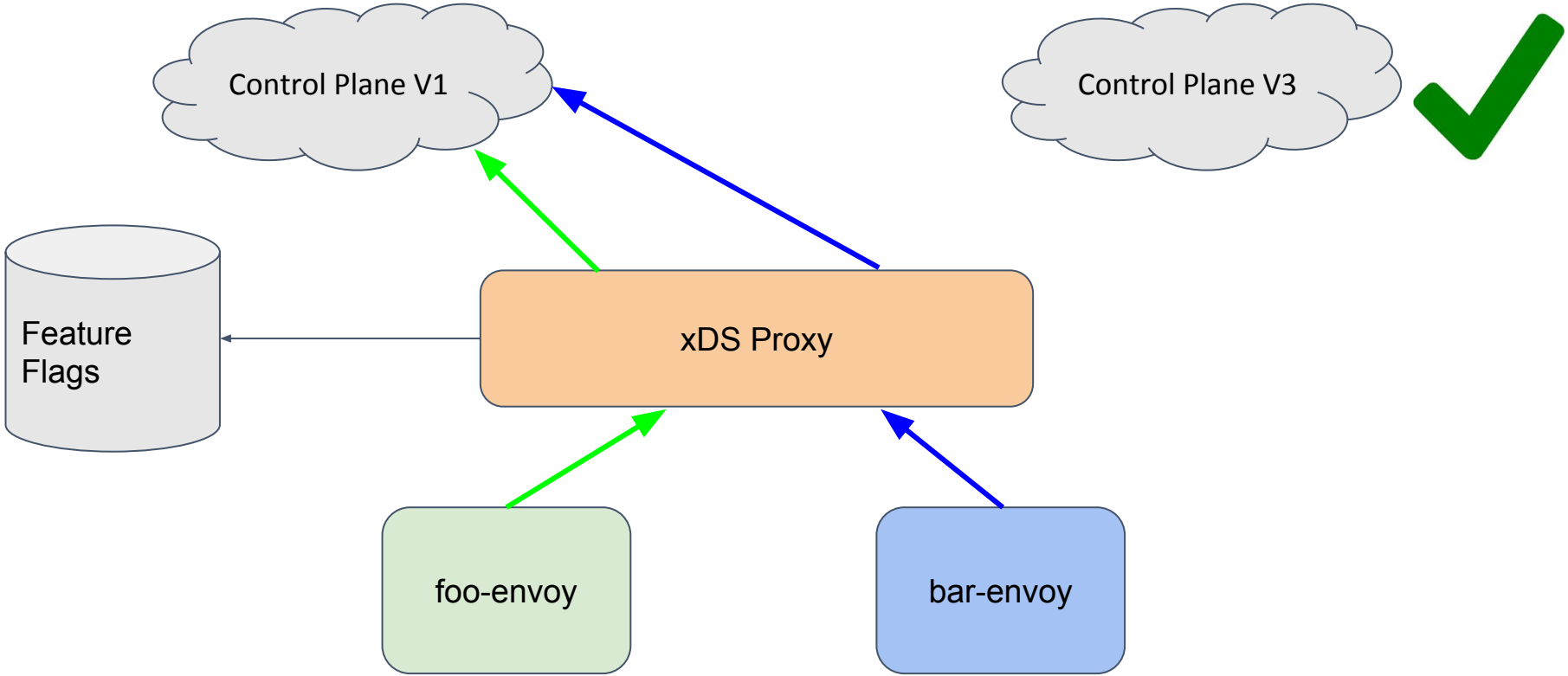
envoycon



Control Plane Design

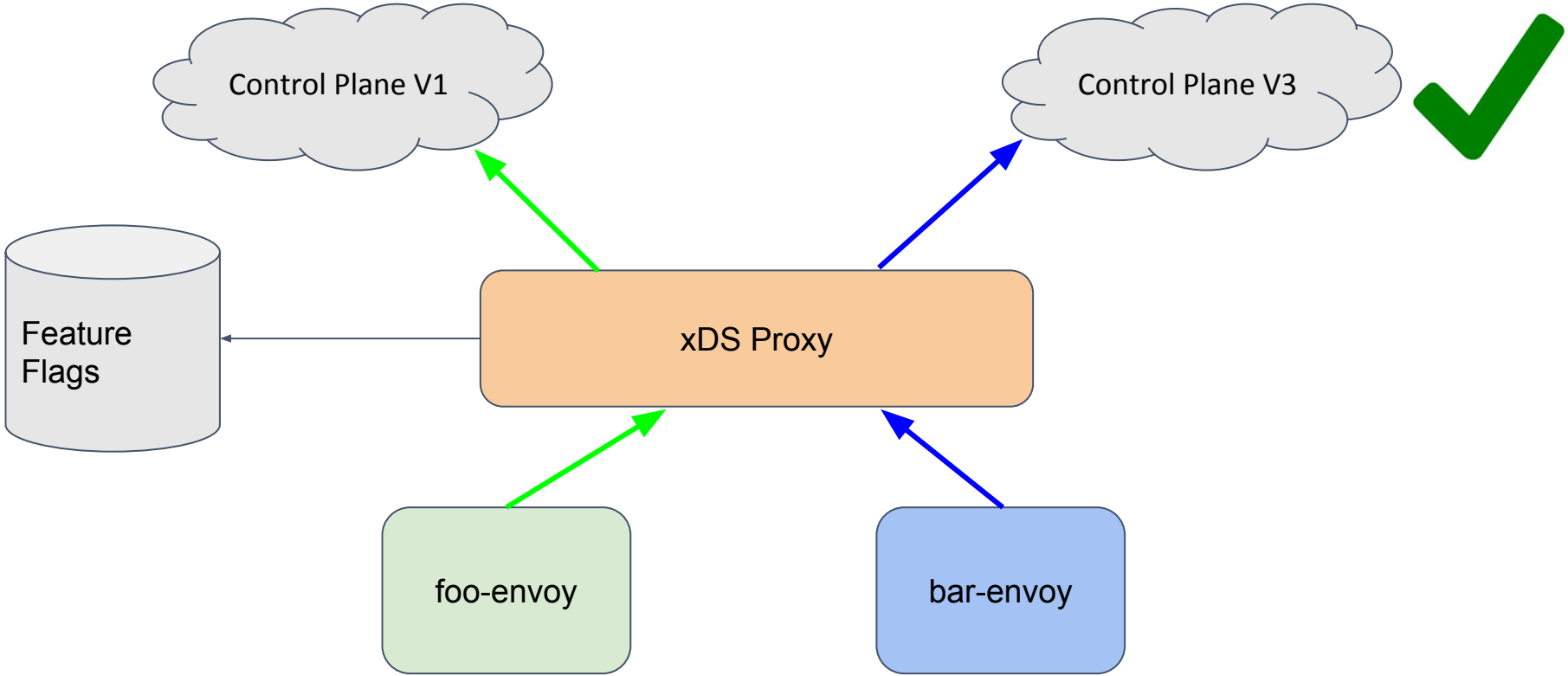


Control Plane Design



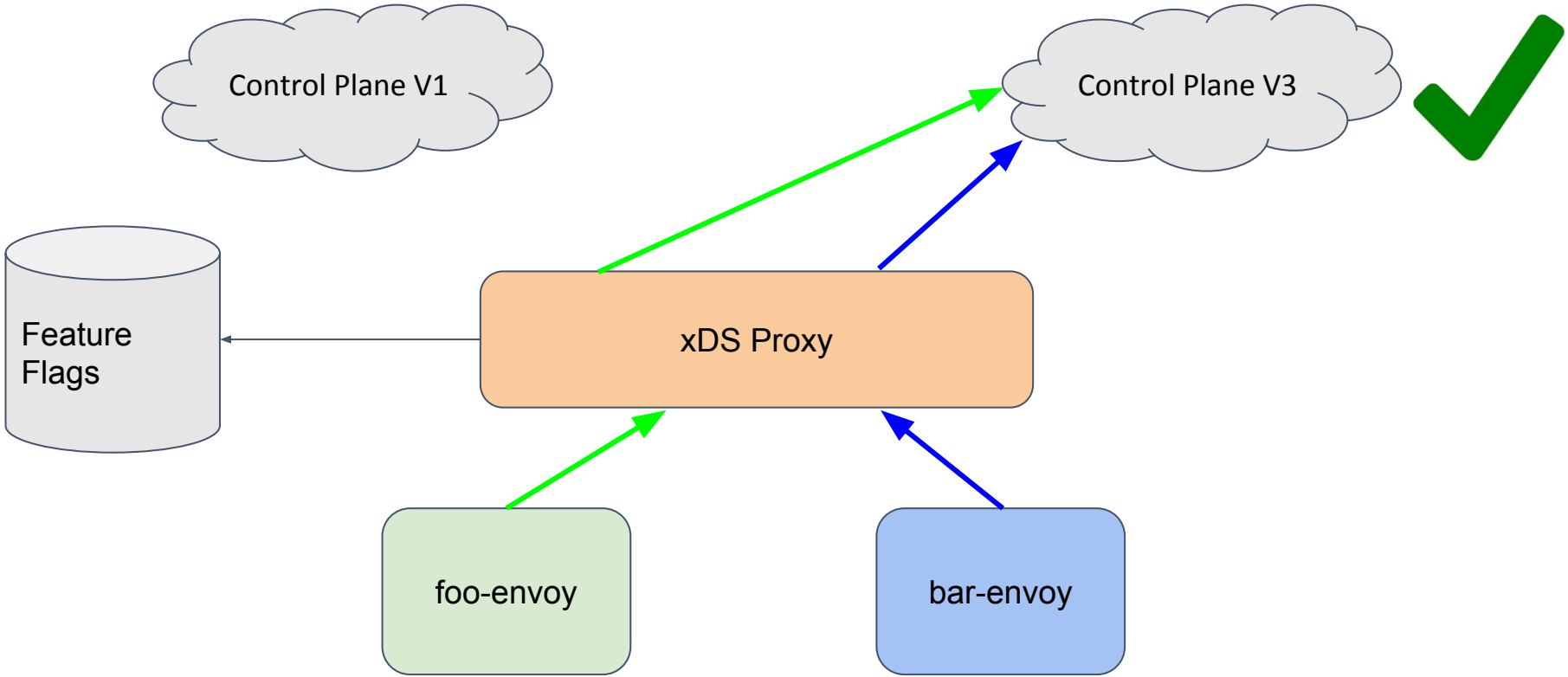
Control Plane Design

envoycon



Control Plane Design

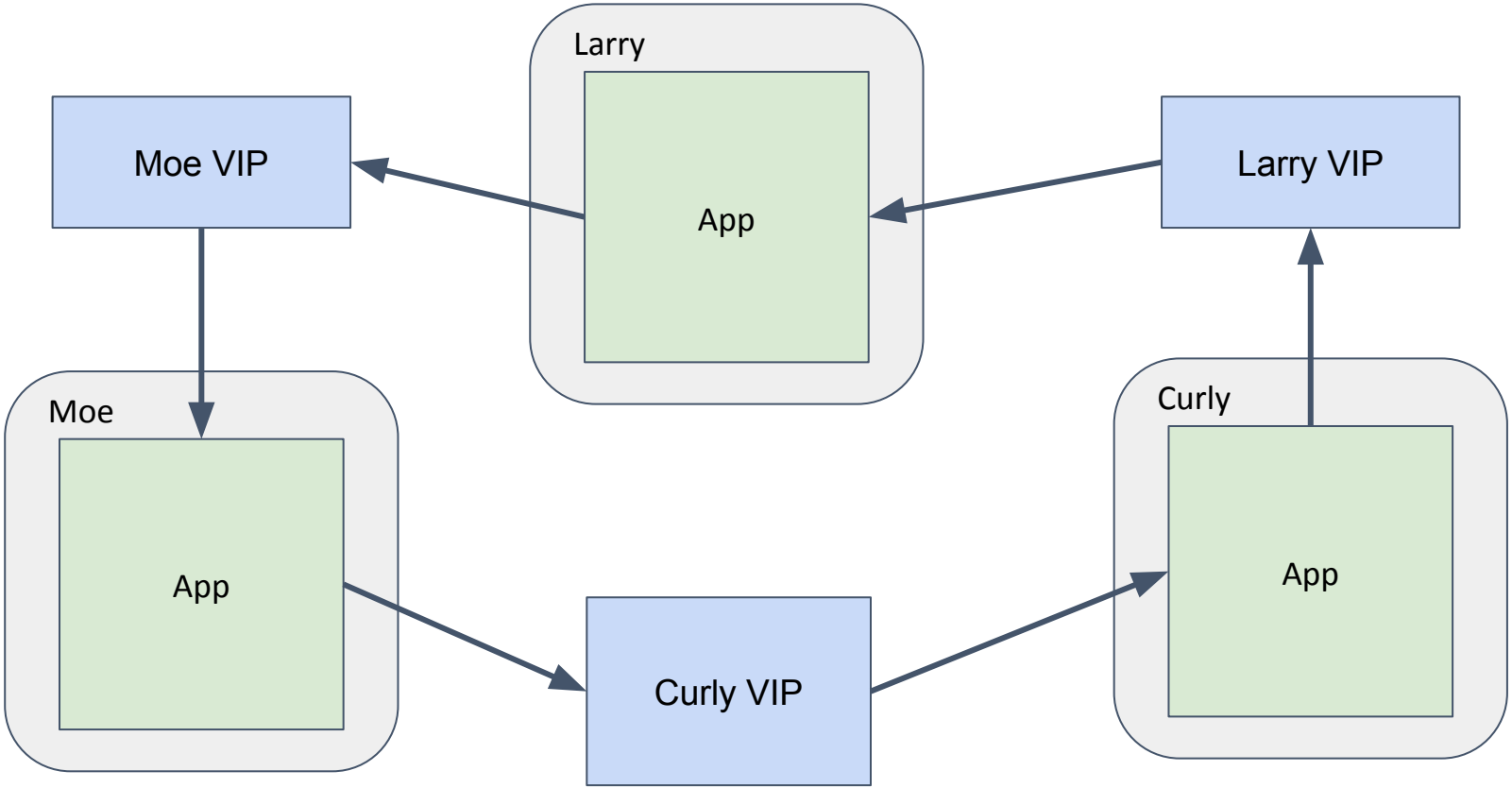
envoycon



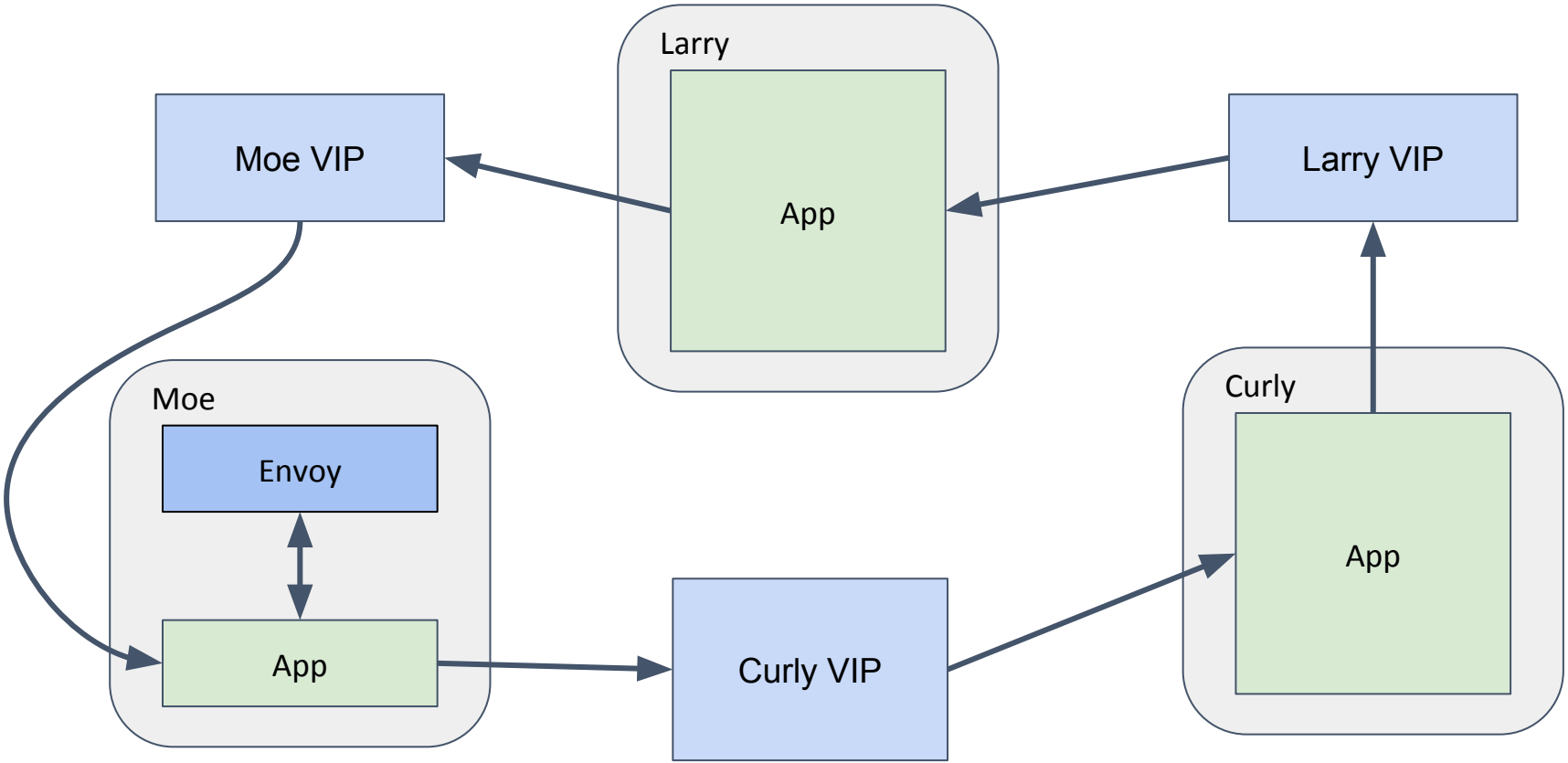
Facilitating Migration

- Automatic sidecar deploy: “traffic-cli add-envoy”
- Provide client/server libraries in major languages
- Simplest possible clients, just send a particular host header to “egress” unix socket
- Preserve legacy service discovery and traffic shaping
- “vip to mesh” feature flag

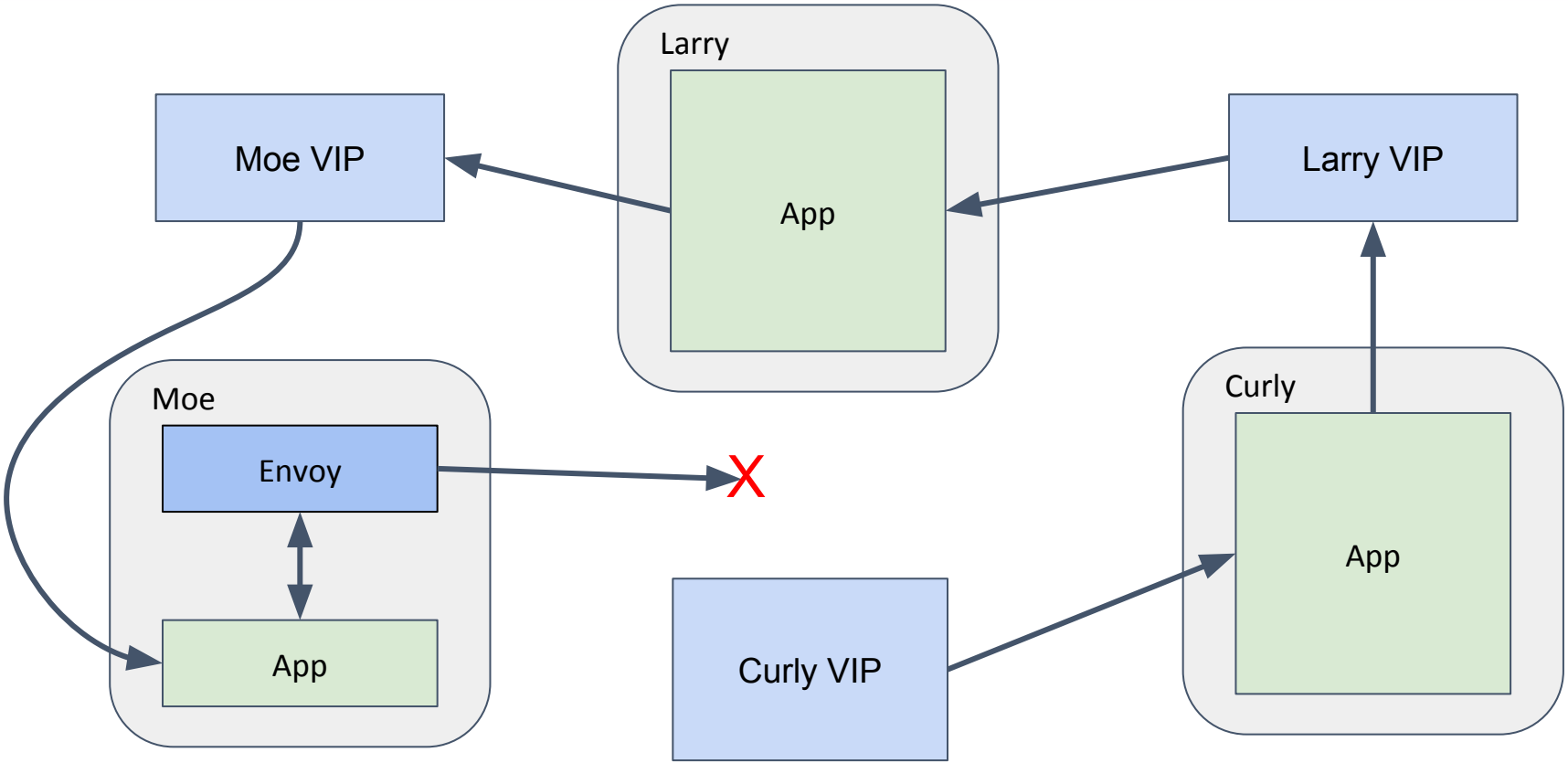
Vip-to-Mesh Feature Flag



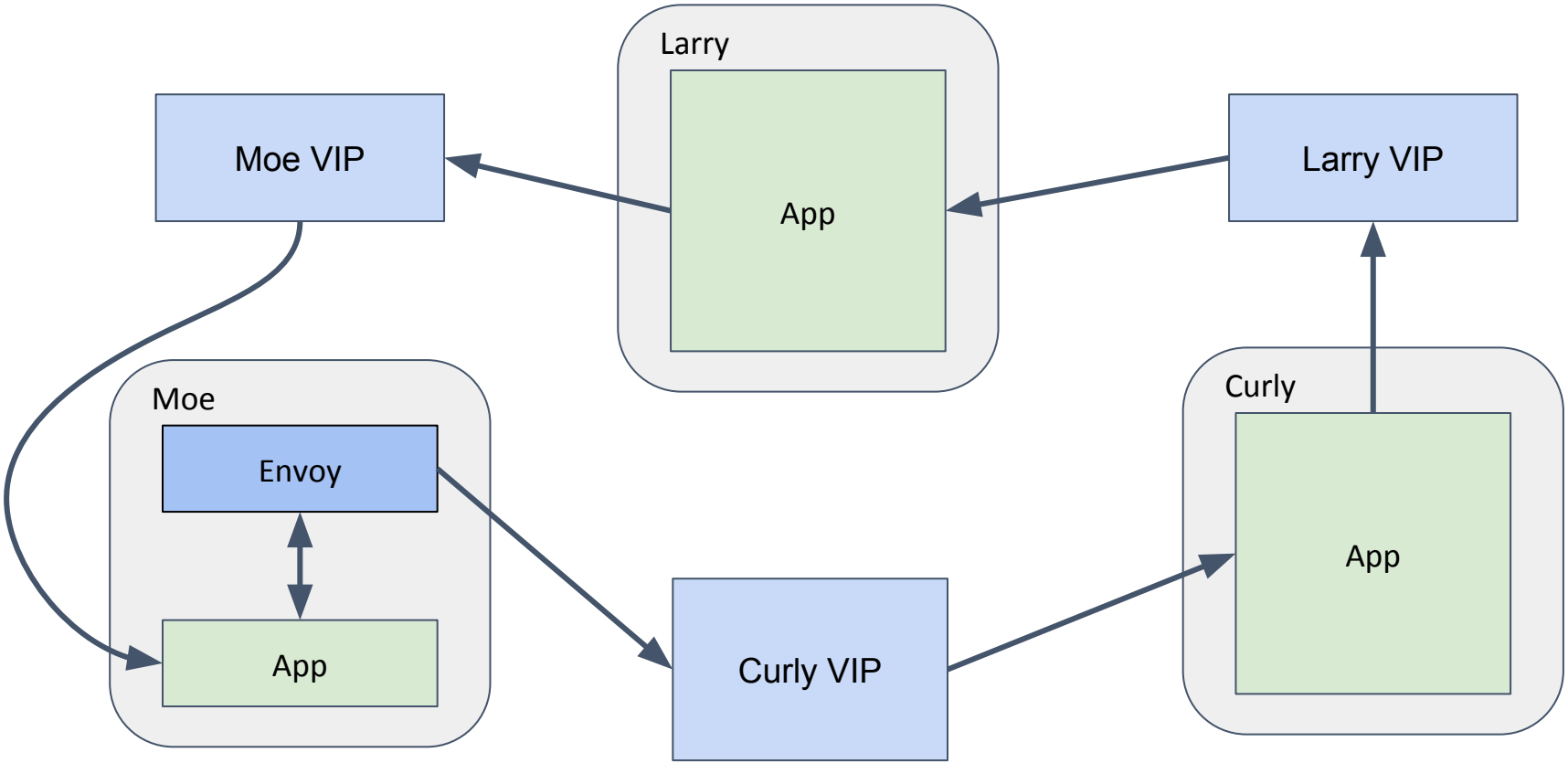
Vip-to-Mesh Feature Flag



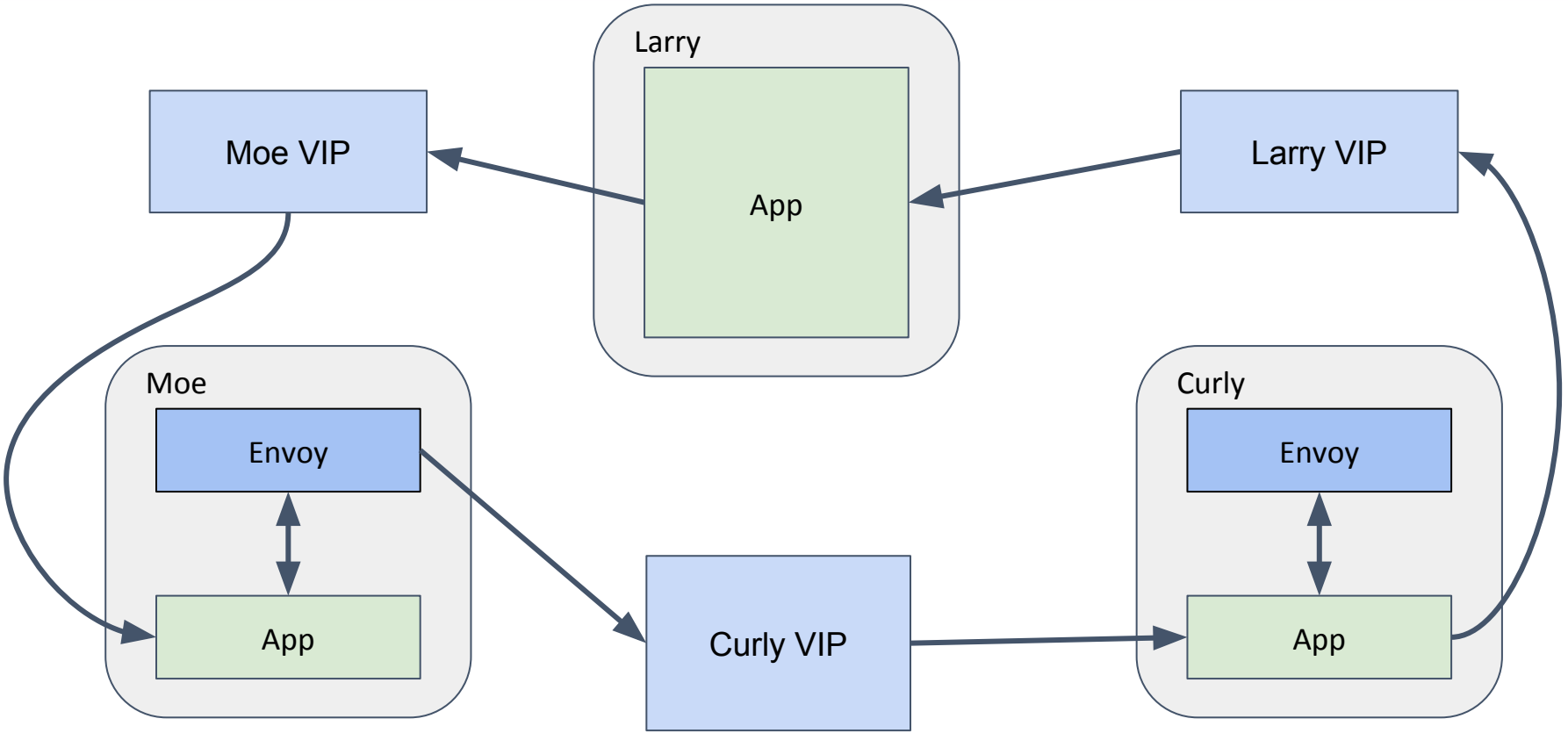
Vip-to-Mesh Feature Flag



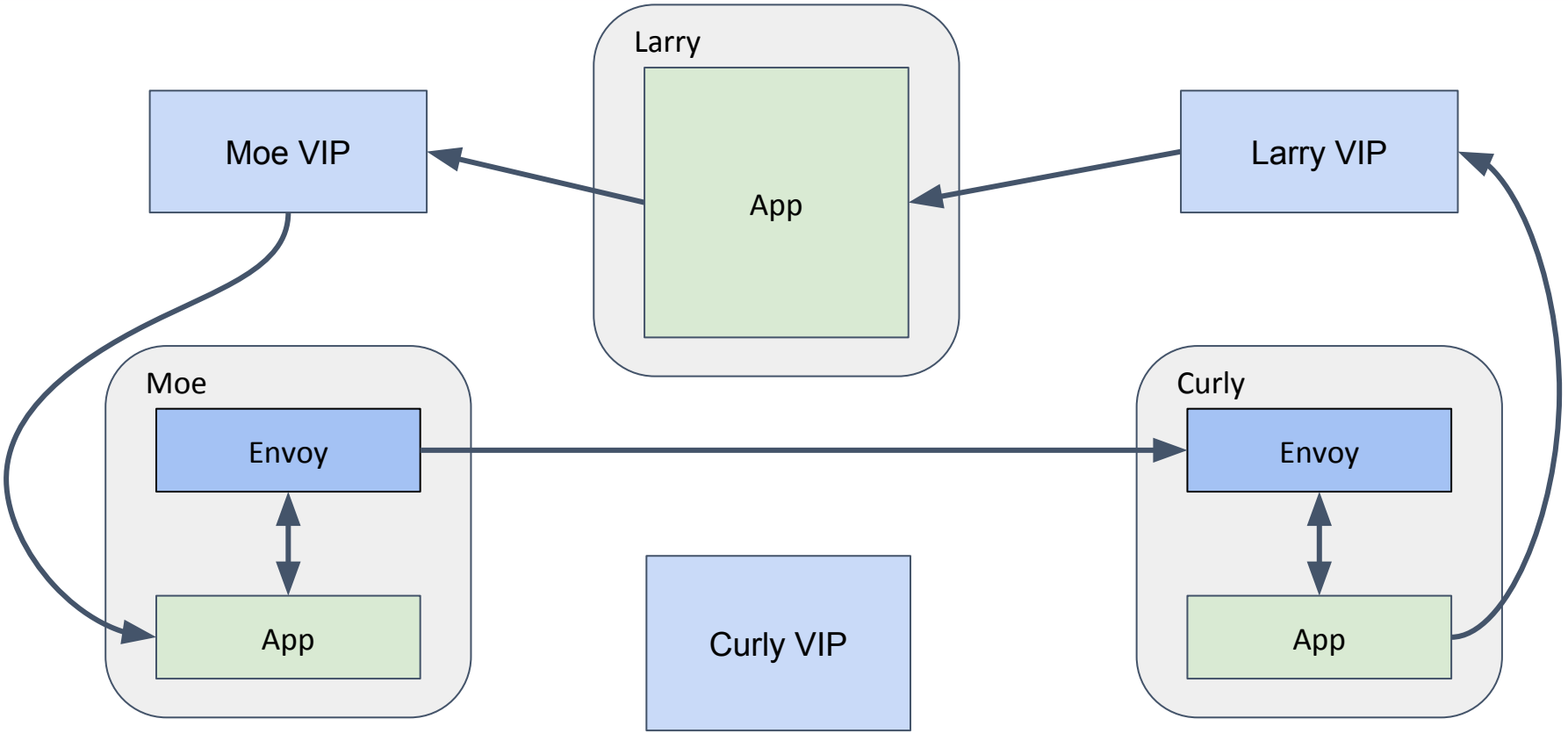
Vip-to-Mesh Feature Flag



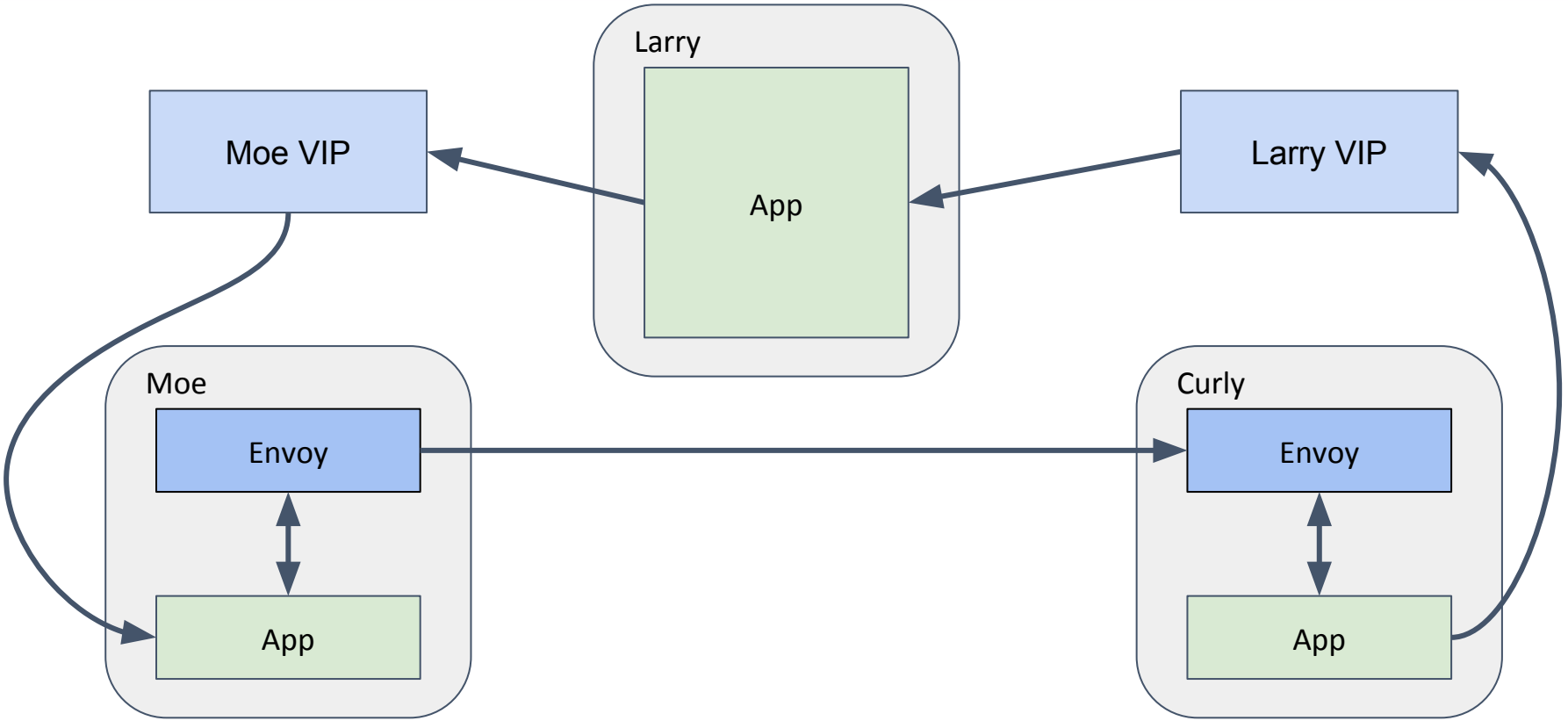
Vip-to-Mesh Feature Flag



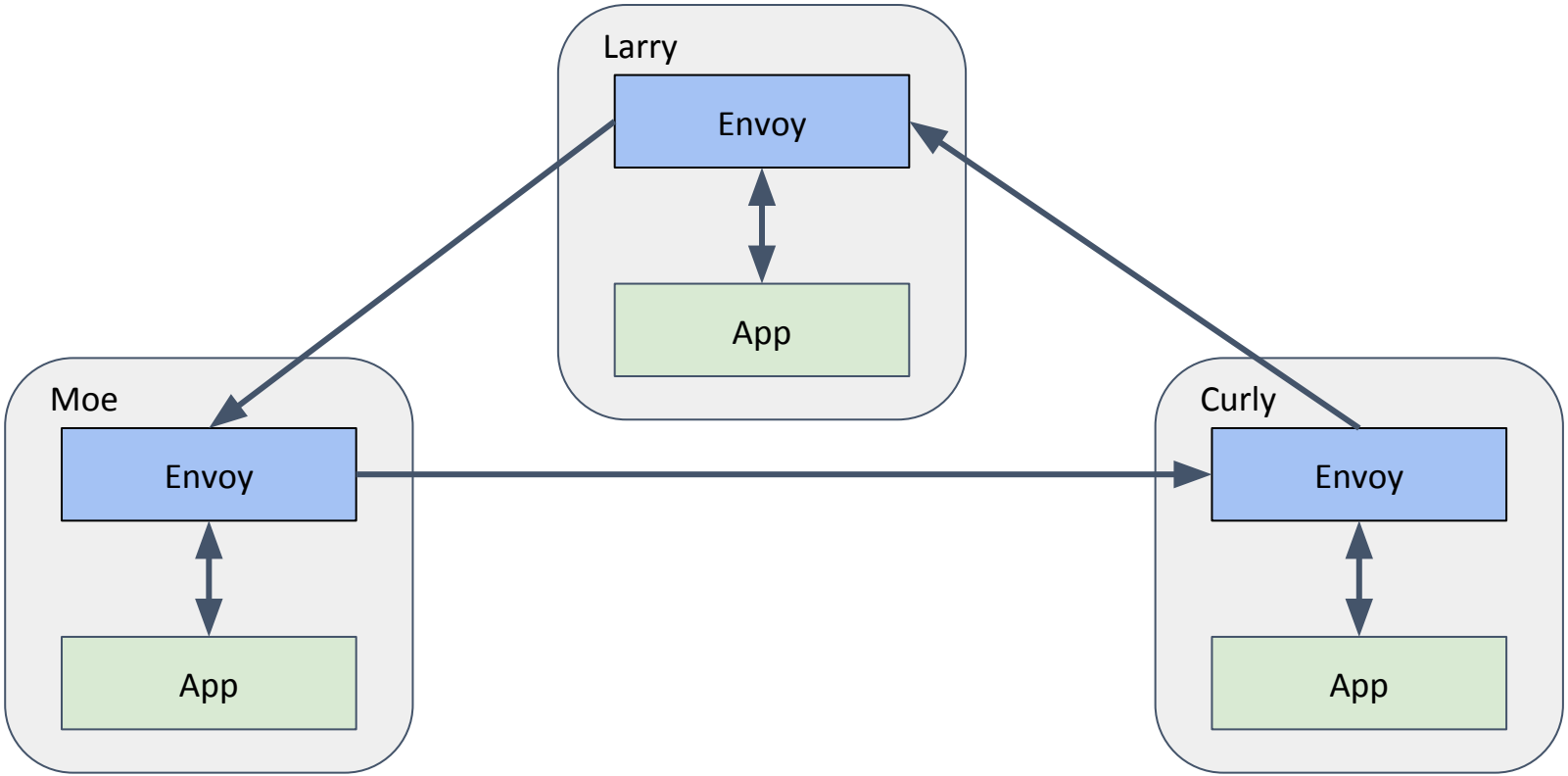
Vip-to-Mesh Feature Flag



Vip-to-Mesh Feature Flag



Vip-to-Mesh Feature Flag



Client/Sidecar Contract

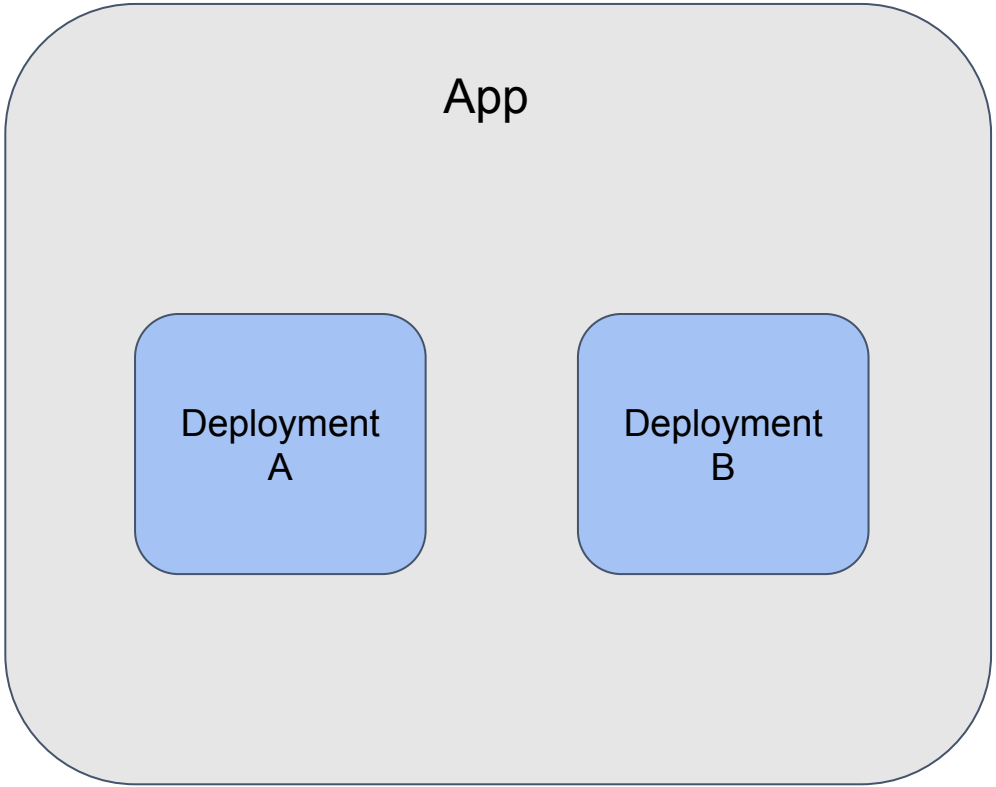
- Send requests to sidecar on unix socket at $ENVOY_EGRESS_SOCKET workaround for not having network namespaces
- Format host header as “[production|staging].{app}.square”
- Developer only needs to know the name of the app they’re talking to and staging/production

Offloading TLS to Proxy

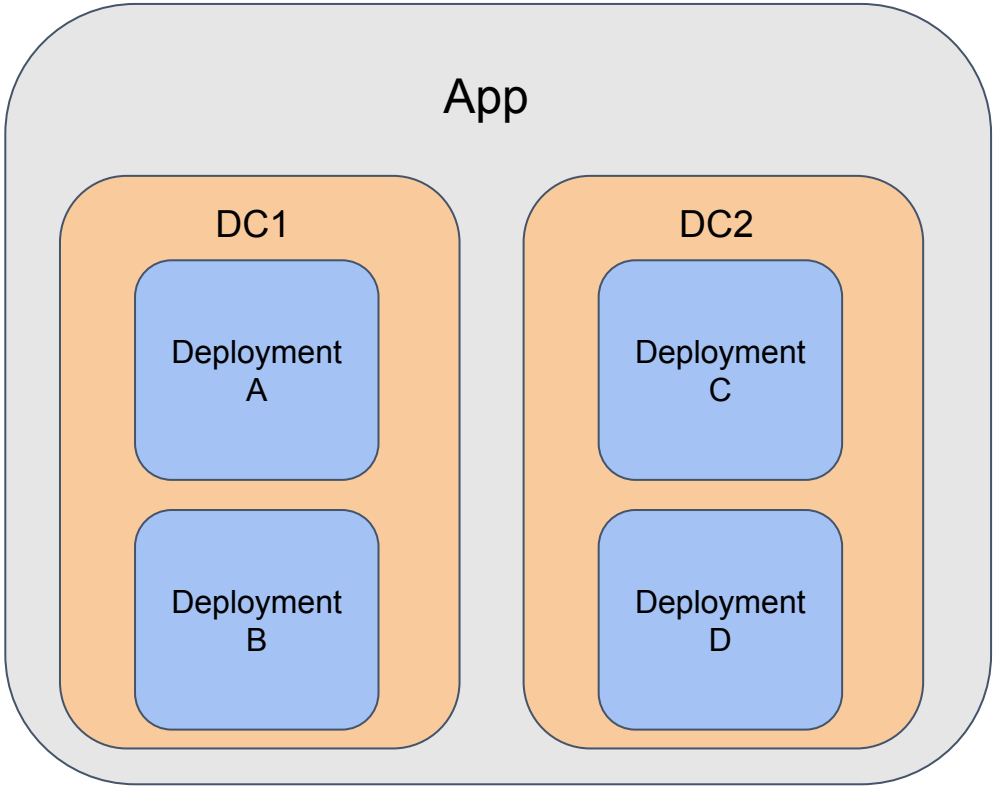
- Take advantage of L7 Envoy features
- Enforce mTLS on both ends of every connection
- Use unix sockets with file permissions
  - Secure traffic from sniffing without requiring TLS in application
- Pass client cert details in HTTP header to support legacy access control

Traffic Shaping

Service Discovery Model

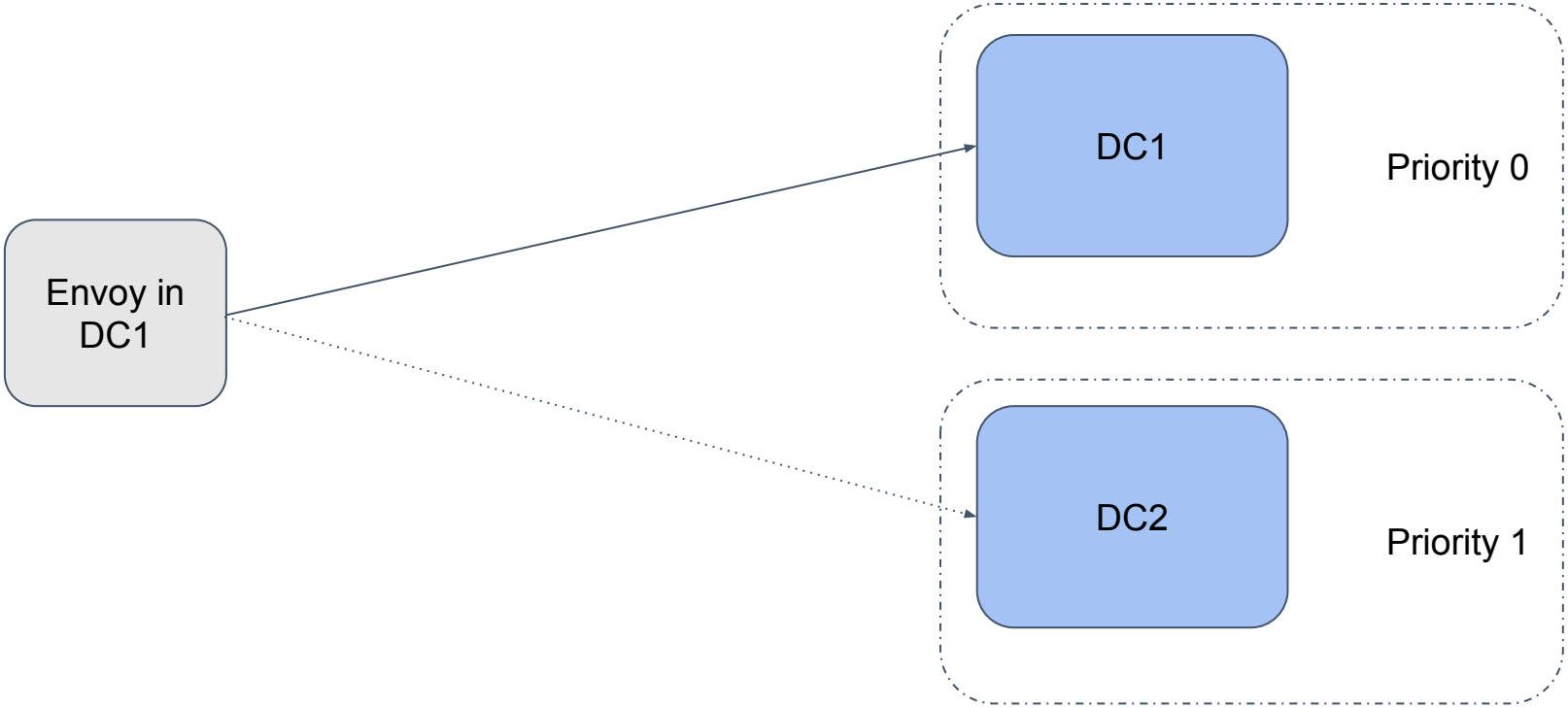


Service Discovery Model

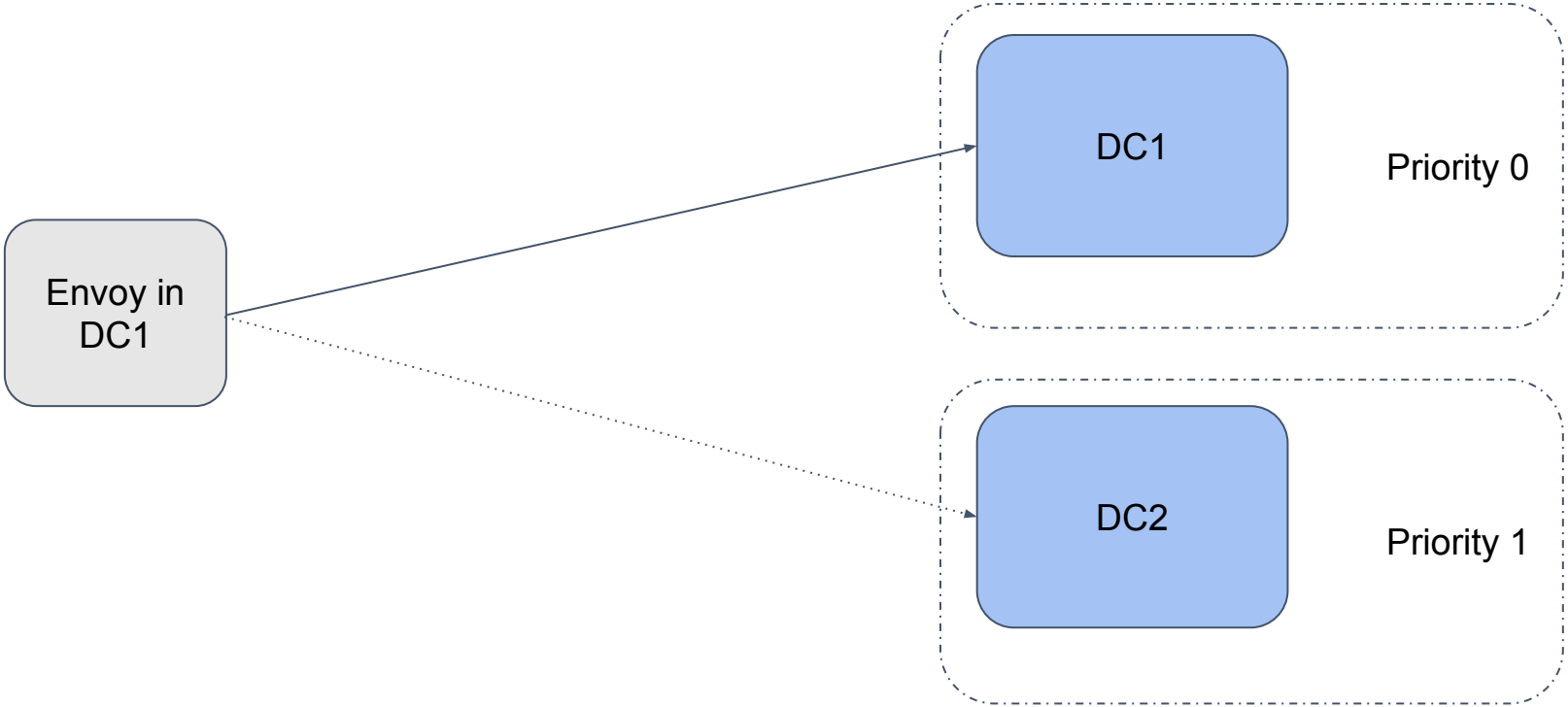


Datacenter Priority Routing

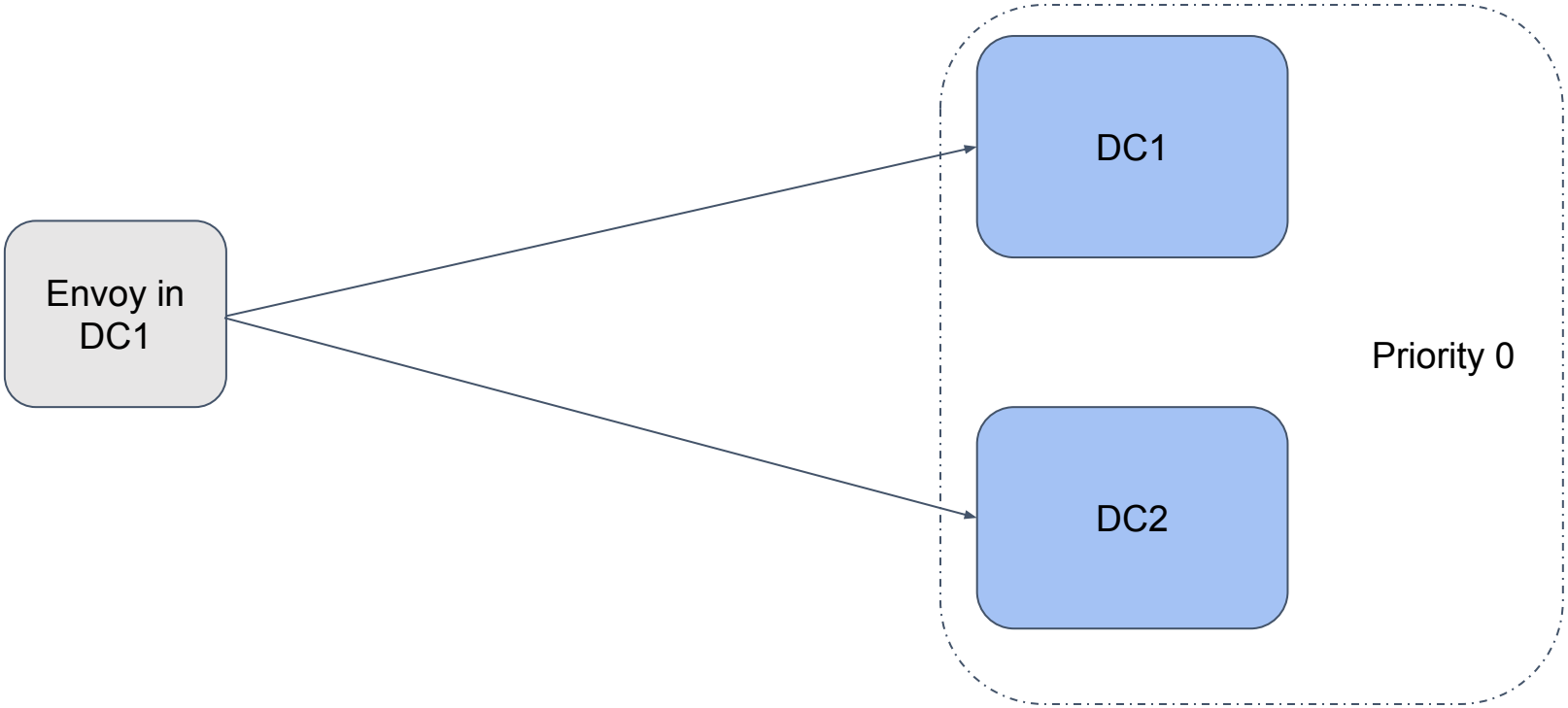
Datacenter Priority Routing



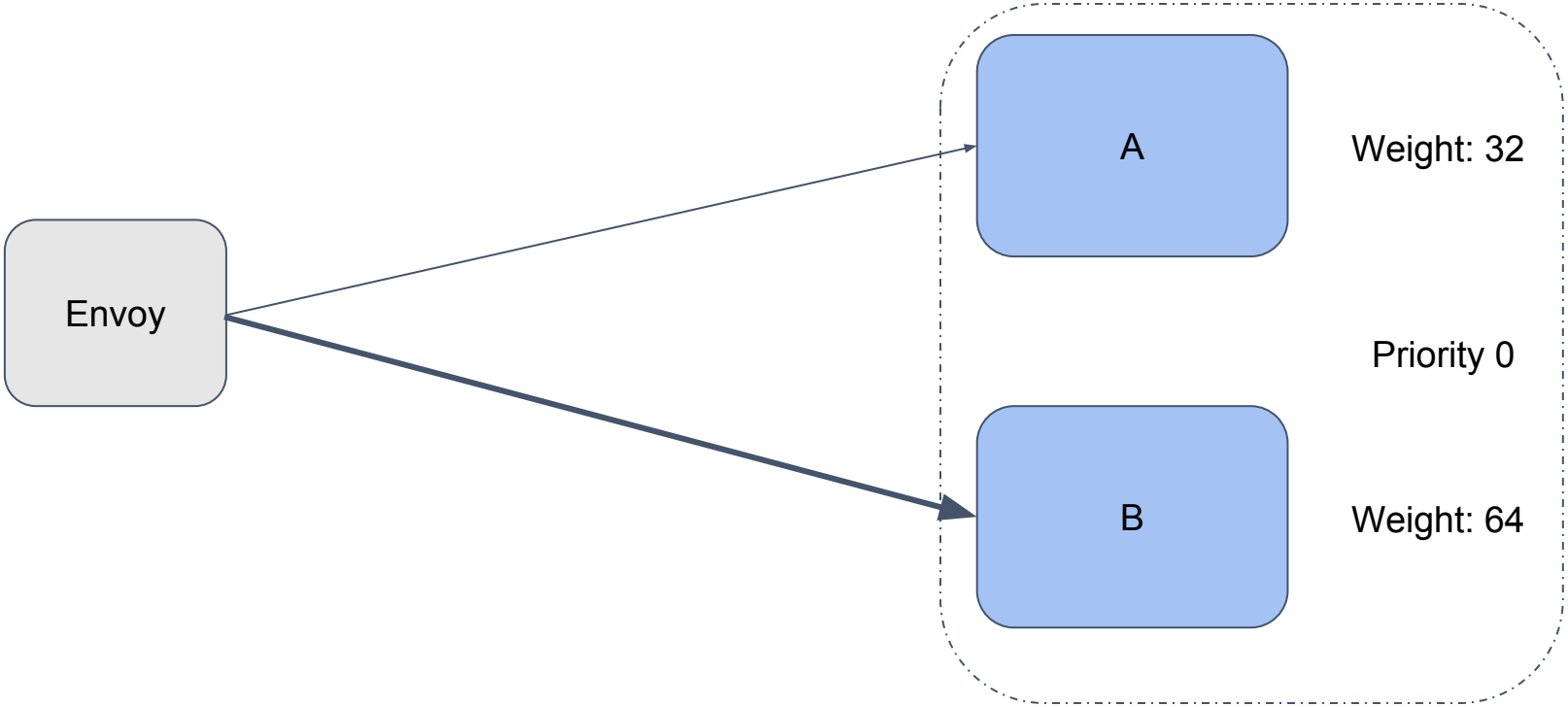
Virtual Datacenters



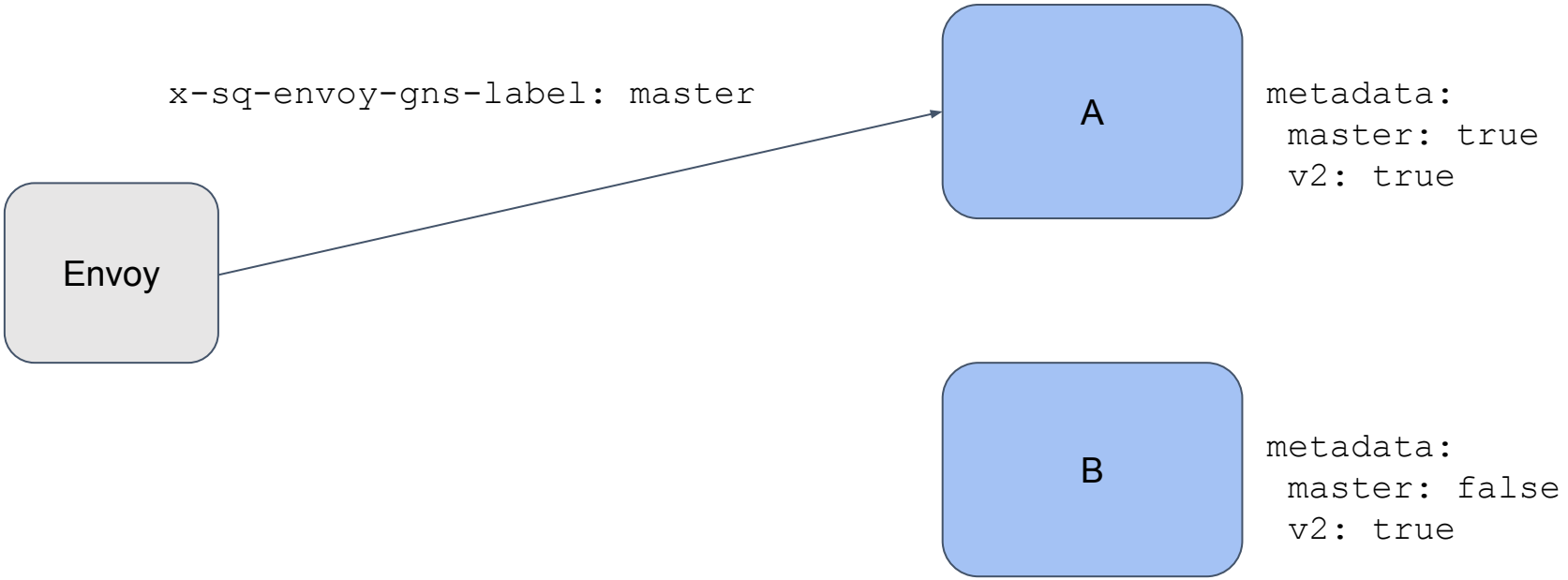
Virtual Datacenters



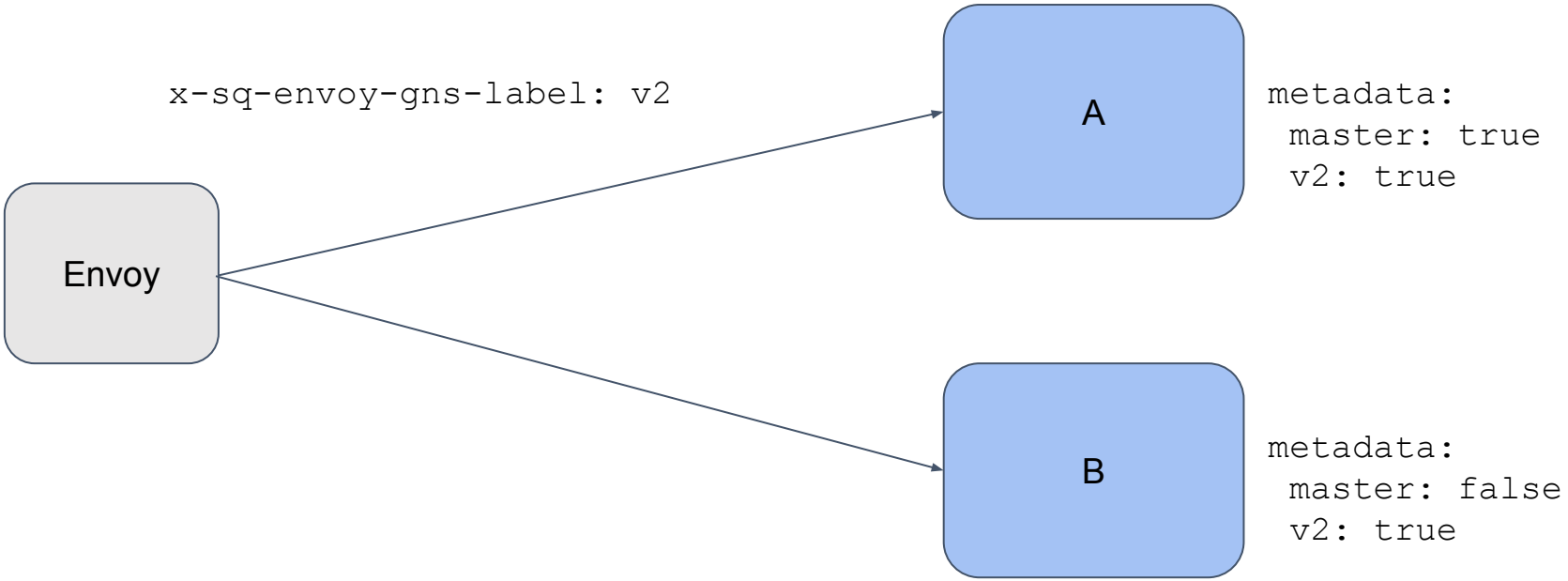
Locality Weighting



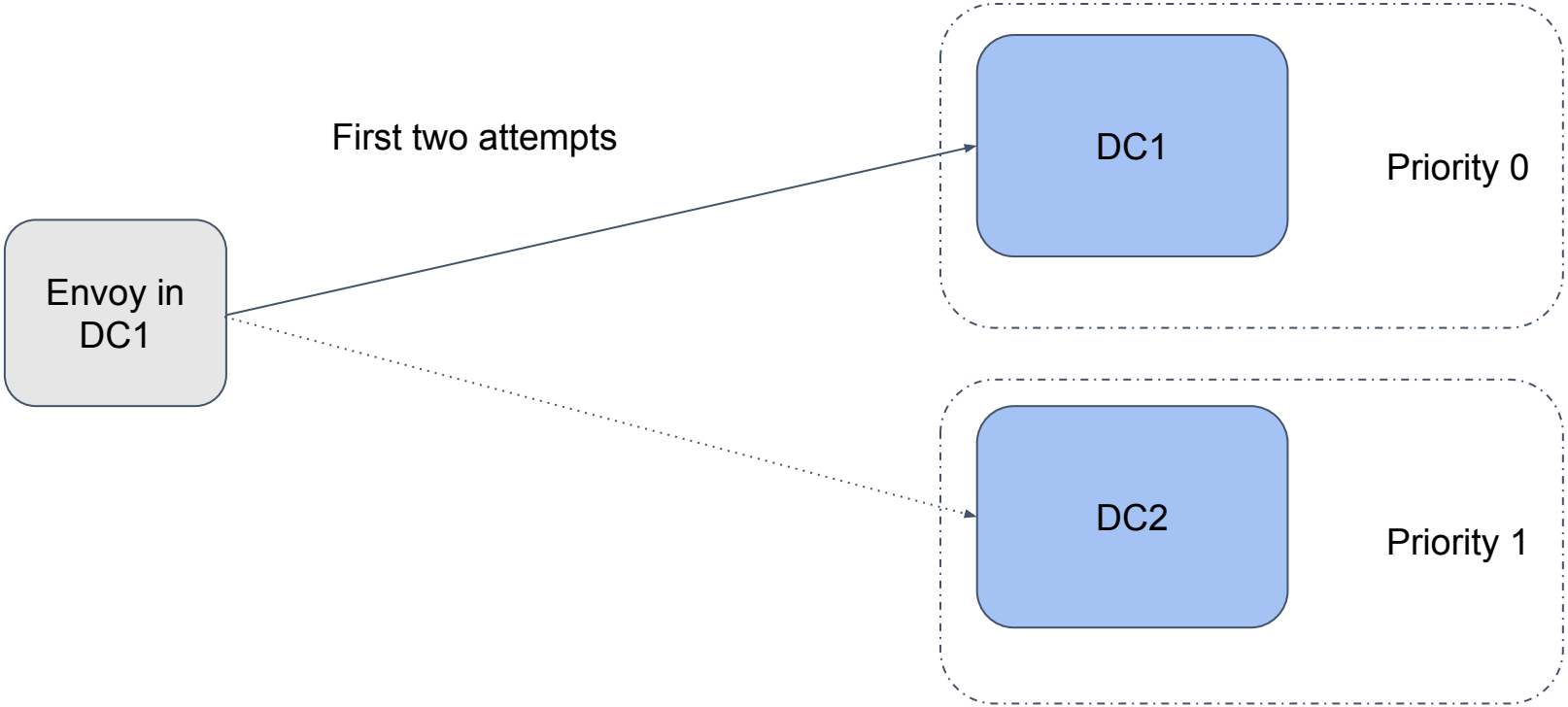
Cluster Targeting



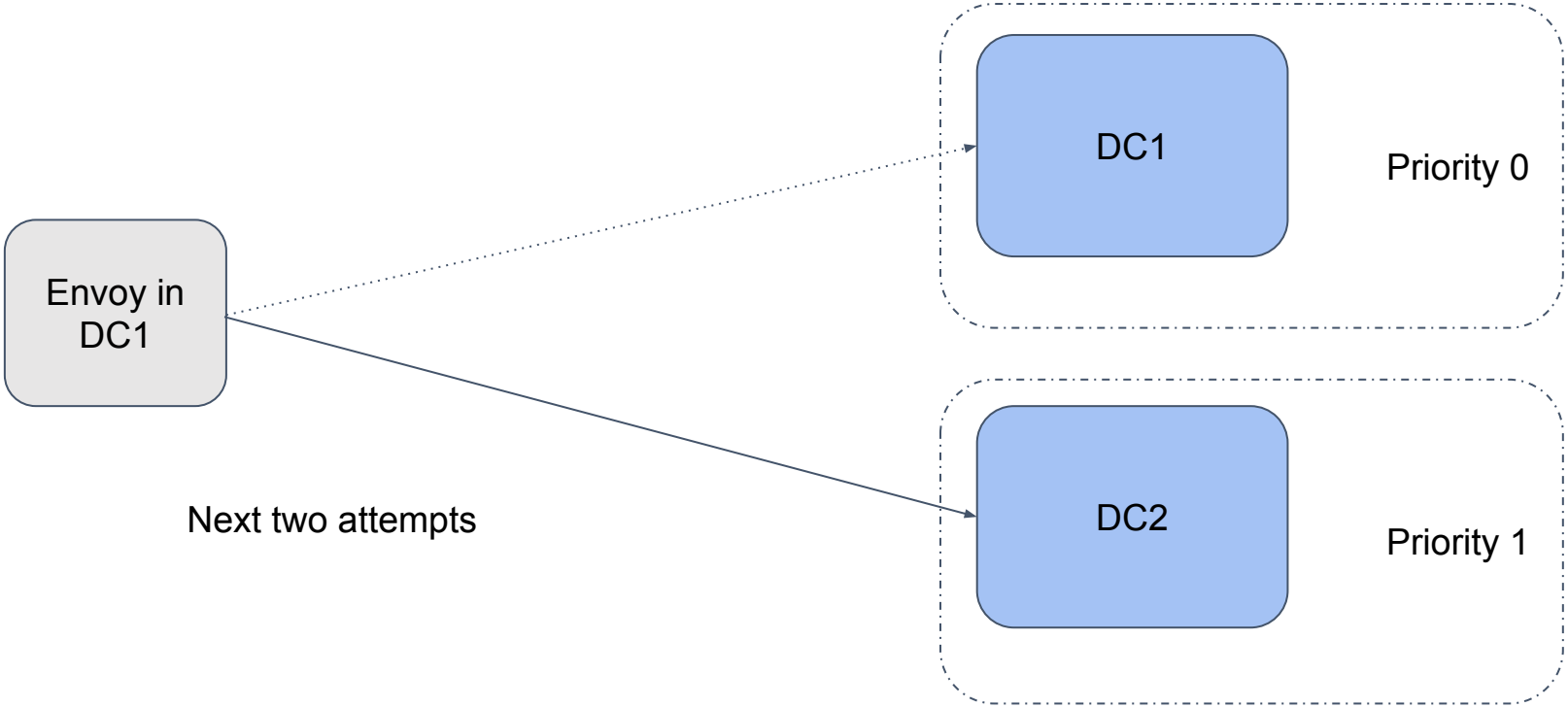
Cluster Targeting



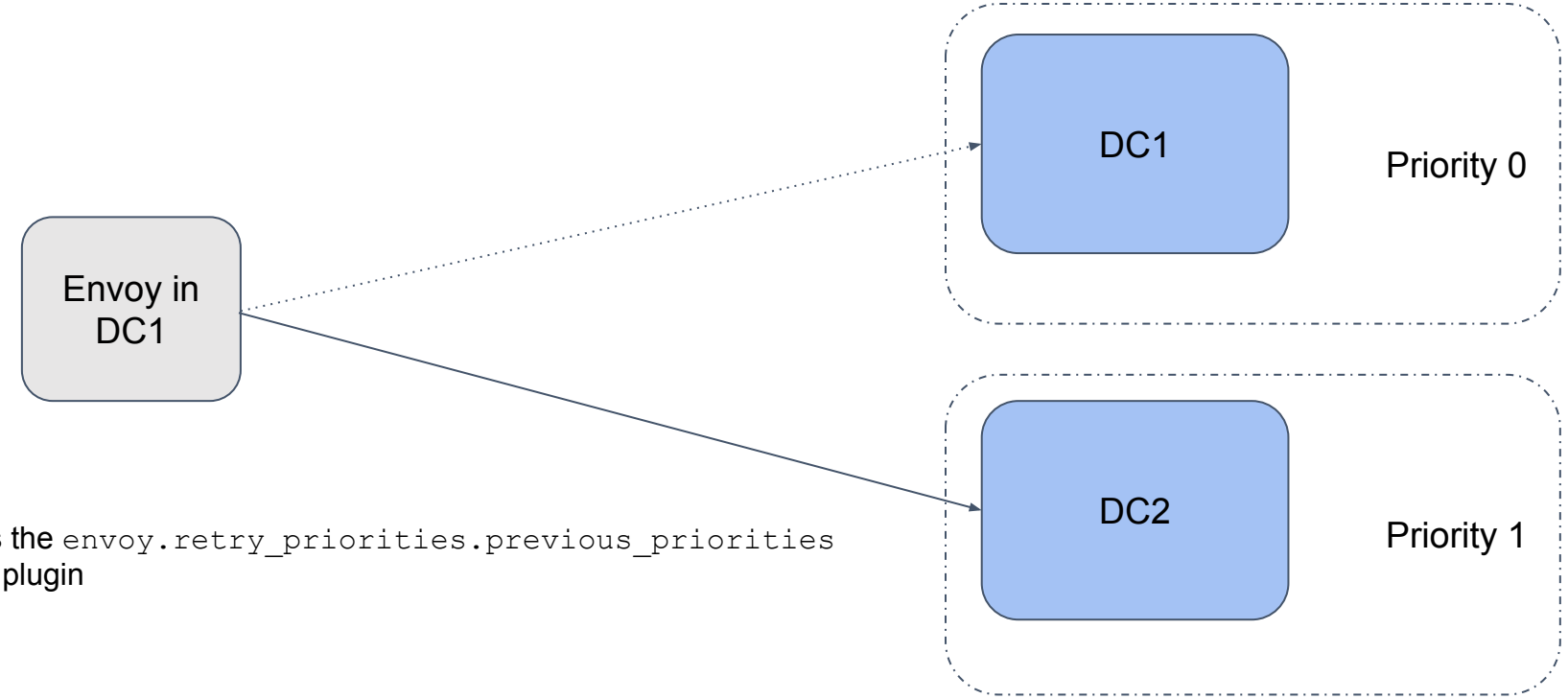
Cross-Datacenter Retries



Cross-Datacenter Retries



Cross-Datacenter Retries



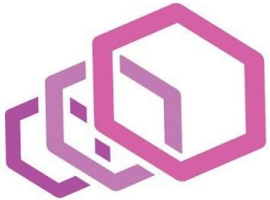
Uses the `envoy.retry_priorities.previous_priorities` retry plugin

Where are we now?

- Feature parity with legacy system
- Envoy partially rolled out
- 2000 Envoy instances deployed across 120 services
- Both on-prem and cloud

What's next?

- Finish migration
- Migrate to Kubernetes
- SPIFFE integration
- L7 Access Control
- Replace edge proxy
- Replace forward proxy



Thanks!

mpuncel@squareup.com / @mpuncel

snowp@squareup.com / @snowypeas