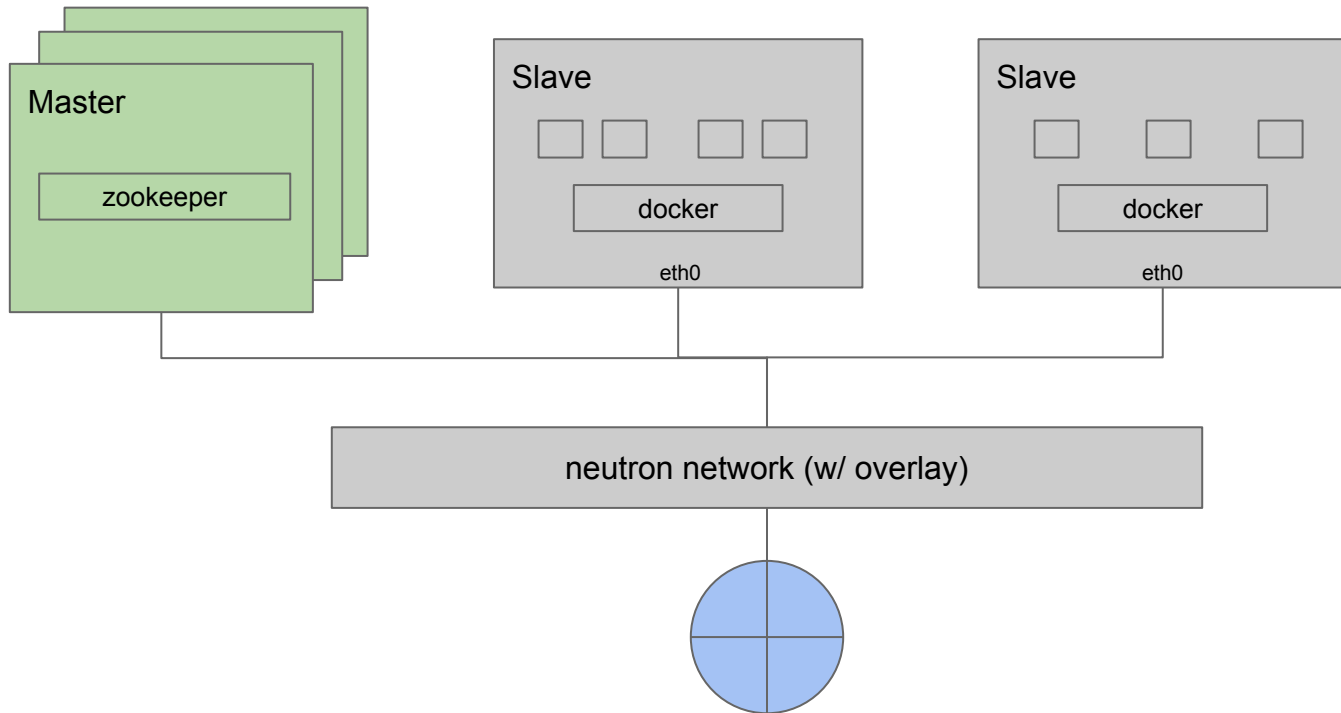


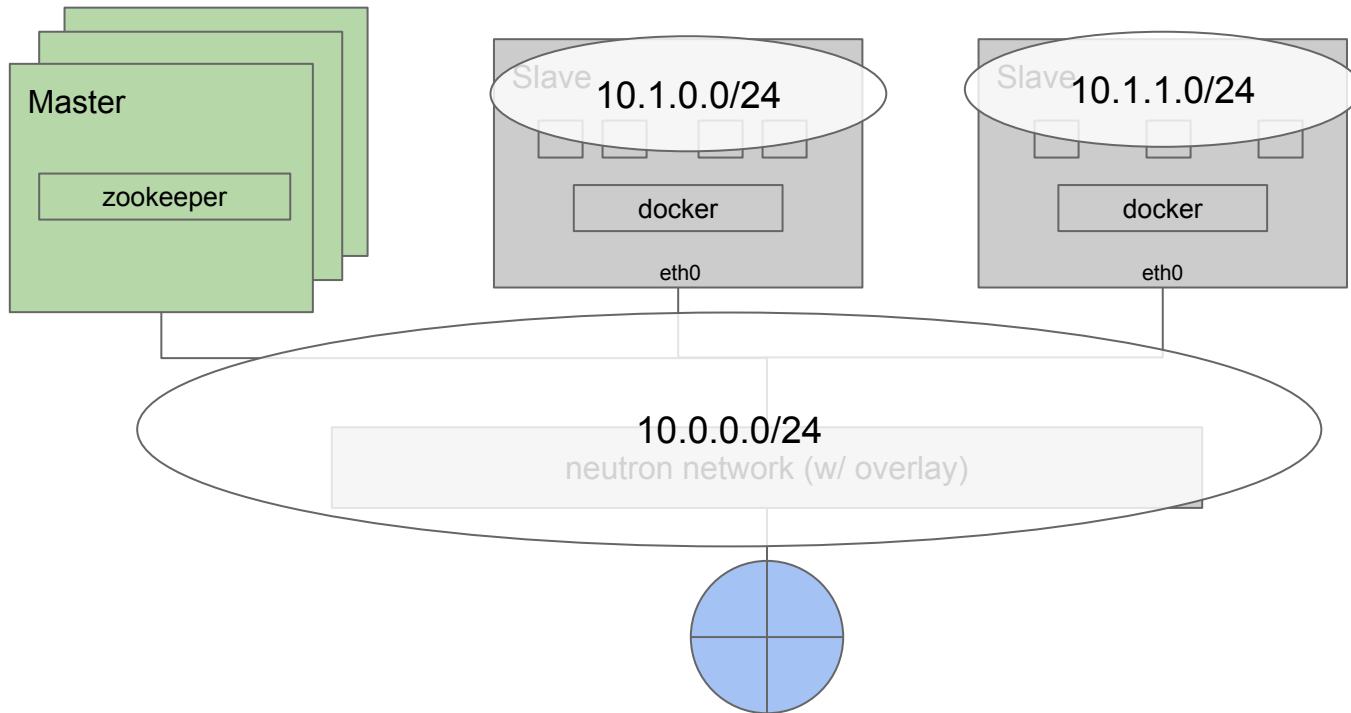
IO Visor for Container Networking

Brenden Blanco

Mesos on Magnum



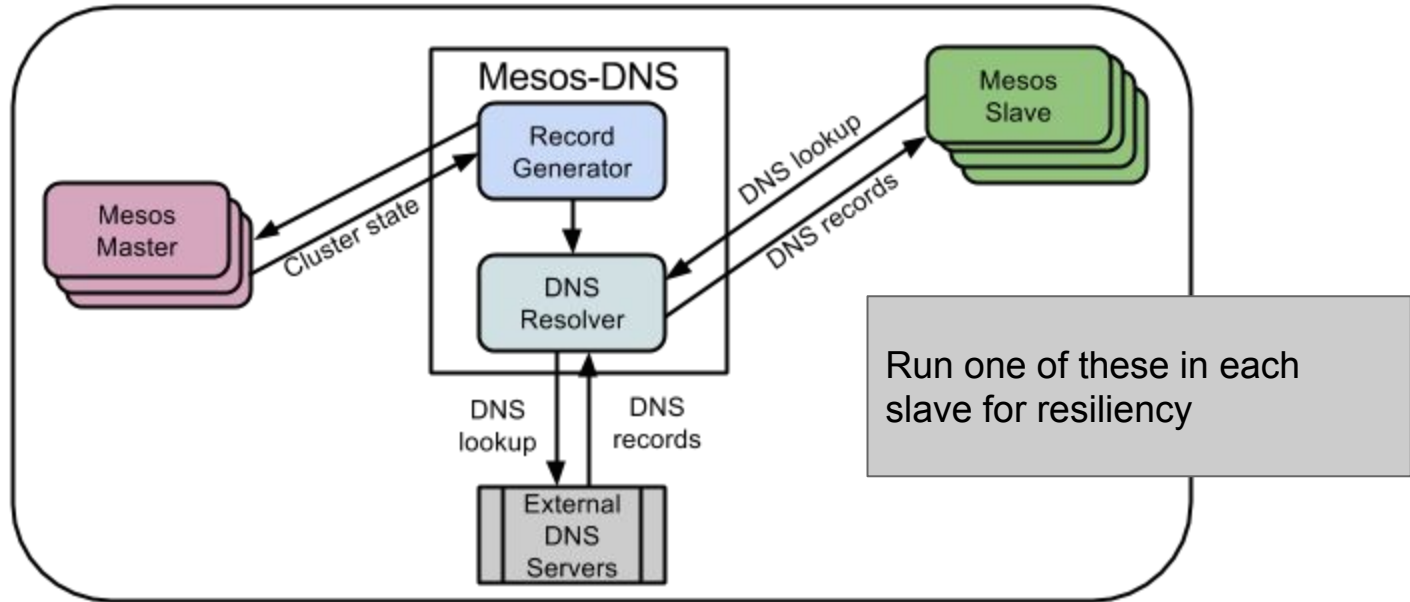
Routed Approach



Routed Container Interfaces

- Create unique routable IP for each container
- Everyone is reachable!
- No nested (docker) NAT
- IPVlan kernel driver for optimal device utilization
 - Note: used by Google for years for their entire fleet of containers

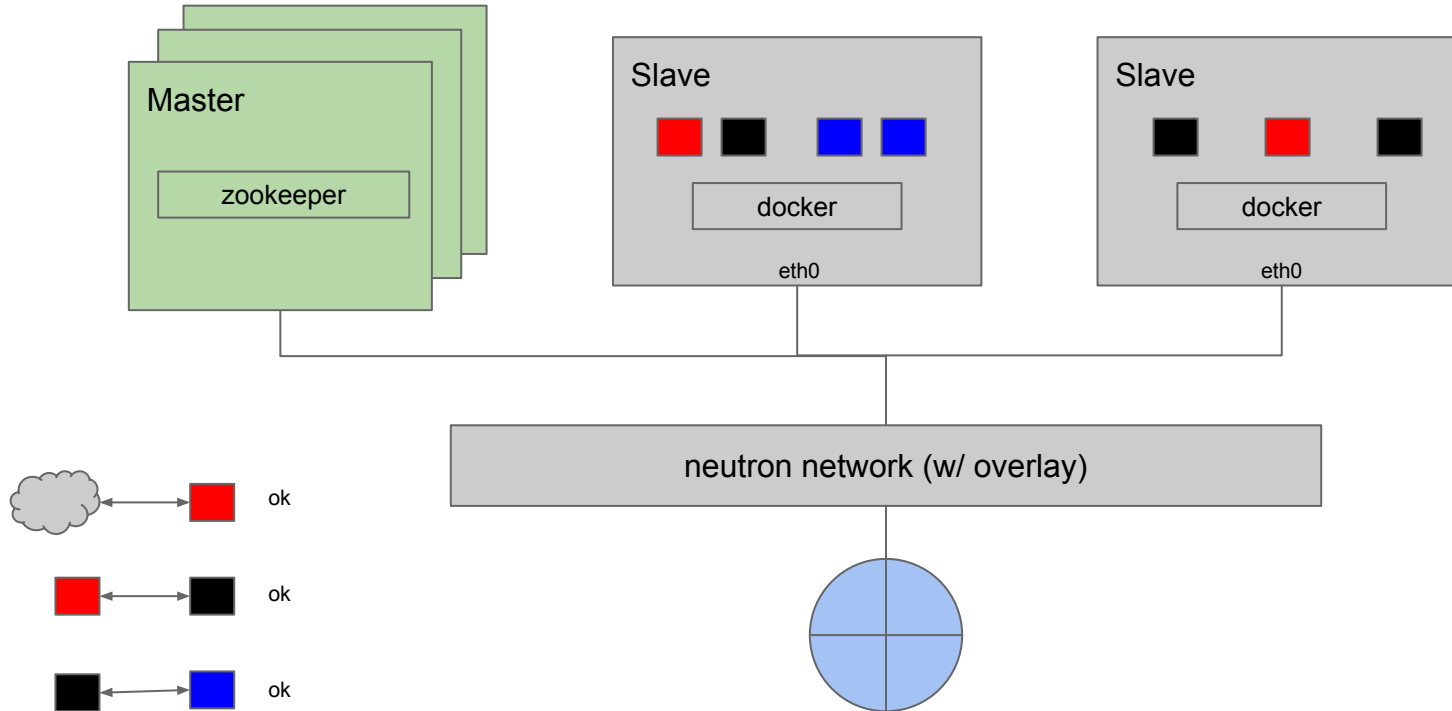
Mesos Service Discovery



Policy Enforcement

- Q: What if I don't want every container to be reachable?
- A: Group Based Policy
 - Specify your policy in the application template
 - Tag containers with a label
 - Enforce policy using IO Visor programs
 - Example: Everyone can talk to Web, Web can talk to DB, everything else denied

Labeled Containers



Parts of IO Module

