



Certified Kubernetes Administrator Prep

CNI -- Container Network Interface

CNI

- All pods can communicate with all other pods.
- Each pod has its own IP address
- No need for mapping container ports
- Backward compatible model with VMs:
 - Port allocation
 - Naming
 - Service Discovery
 - Load balancing
 - Application Configuration
 - Migration



Kubernetes Network model

- **Dynamic Port Allocation Problems:**
 - Every application must be configured to know which ports, etc.
 - API services must inject dynamic port numbers into containers
 - Services must be able to find one another or be configured to do so
- **The Kubernetes Way:**
 - All containers can communicate with each other without NAT
 - All nodes can communicate with all containers (& vice versa) without NAT
 - The IP of a container is the same regardless of which container views it
 - K8s applies IP addresses at the pod level
 - “IP-per-Pod” -- Containers in a pod share a single IP address, like processes in a VM



But... How?

CNI -- Container Network Interface

- Must be implemented as an executable invoked by the container management system (in our case, Kubernetes)
- Plugin is responsible for
 - Inserting the network interface into the container network namespace
 - Making necessary changes to the host
 - Assign IP address to the interface
 - Set up routes consistent with IP address management



Kubelet

- Default network plugin
- Default cluster-wide network
- Probes for network plugins on startup



Flannel

- Simple and easy Layer 3 network fabric
- `flanneld` runs on each host (via a DaemonSet)
 - Allocates subnet least to each host
 - Stores network configuration, allocated subnets, other data
 - Packets forwarded using VxLANs



Calico

- Free and Open Source
- Simplified networking model
- Scalable, distributed control plane
- Policy-driven network security
- Uses overlay networks sparingly
- Widely deployed
- Can be run in policy enforcement mode



Others Worth Mentioning

- Cilium
- Contiv
- Contrail
- Multus
- NSX-T
- Nuage Networks VCS
- OpenVSwitch
- OVN
- Romana
- Weave Net
- CNI-Genie



Conclusion

Kubernetes requires its networking model to be implemented by a third-party plugin, called a CNI (Container Network Interface).

Different CNIs feature support for different hardware, software, overlay networks, policies, and features.

Administrators must select a CNI appropriate to their environment.

