A Nightmare on Kube Street: Slicing Kubernetes Networks like Freddy Krueger

Surya Seetharaman
Principal Software Engineer @ Red Hat
OVN-Kubernetes project maintainer
@tssurya

Dave Tucker
Architect @ Red Hat
OVN-Kubernetes contributor
@dave-tucker

What are VPCs?

It’s a container… for networks.

Grouping of network configuration into a single logical construct

Administrative Boundary to allow for self-service

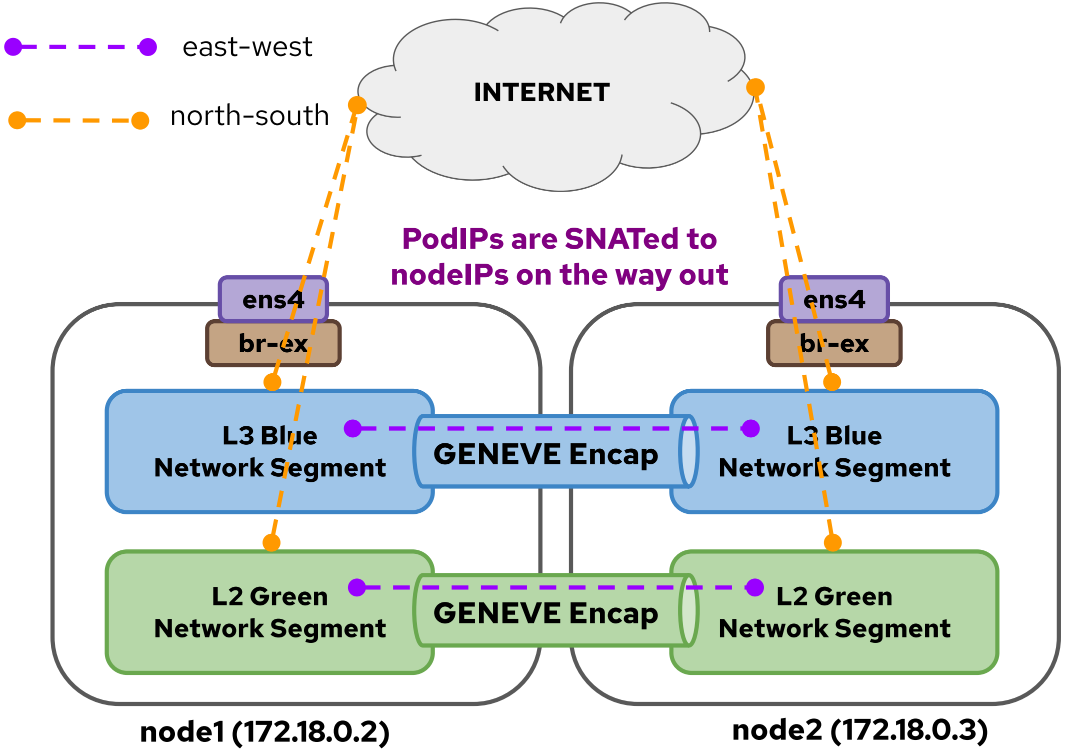
AI was used to generate this image

VPC Concepts

AWS	Azure	Google Cloud	VMware	OpenStack	OVN-K8s
VPC	VNet	VPC	VPC	Network	???
Subnet	Subnet	Subnet	Subnet	Subnet	UDN
Security Groups	Network Security Groups	Firewall Rules	Distributed Firewall	Security Groups	Network Policy
Route Table	Route Table	Routes	T0/T1 Gateways	Router	???
Internet Gateway	N/A - Public IP only	Implicit	T0 Gateway	External Network	Implicit
NAT Gateway	NAT Gateway	Cloud NAT	T0 Gateway	Router	EgressIP
VPN Connection	VPN Gateway	Cloud VPN	???	VPNaaS	???

How do we achieve this in OVN-Kubernetes using OVN and OVS?

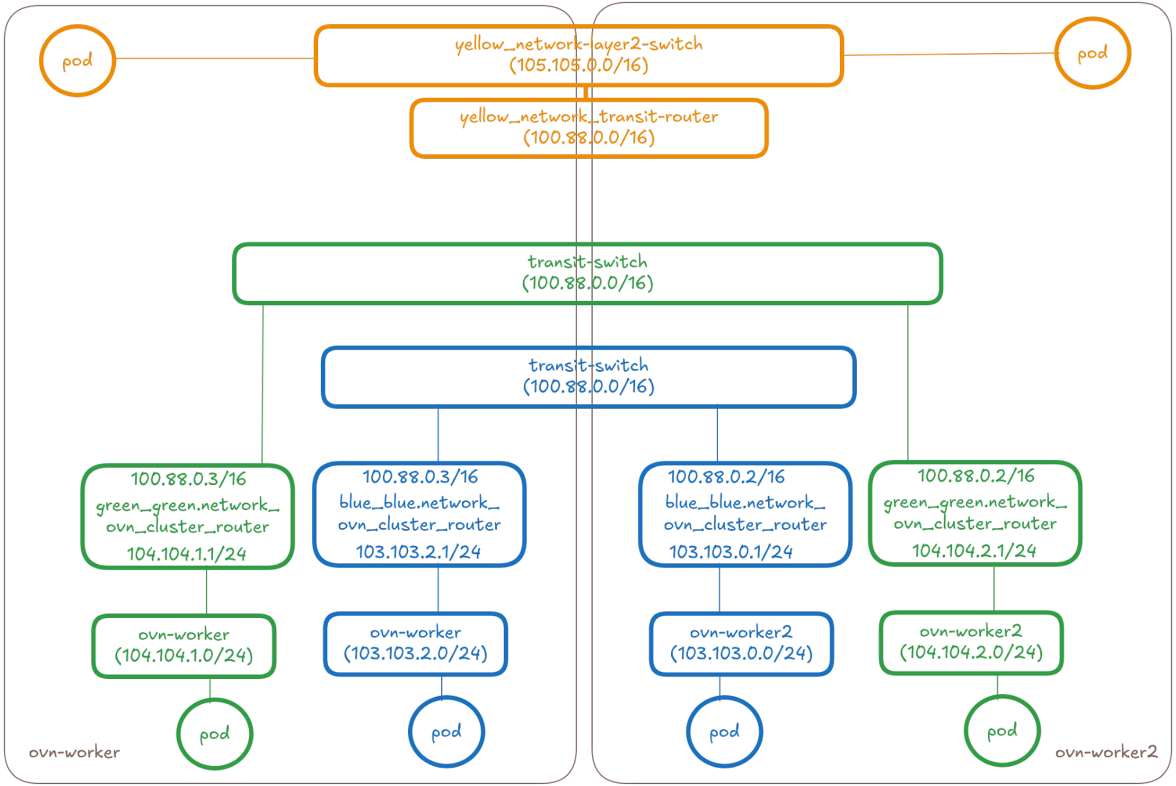
User Defined Networks == Subnet(s)?



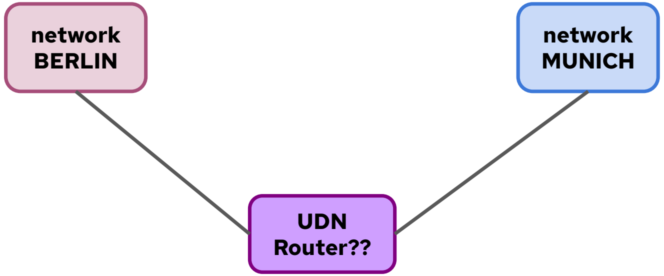
PodIPs are SNATed to nodeIPs on the way out

```yaml
apiVersion: k8s.ovn.org/v1
kind: UserDefinedNetwork
metadata:
 name: blue-network
 namespace: blue
 labels:
   name: blue
   purpose: german-network
spec:
 topology: Layer3
 layer3:
   role: Primary
   subnets:
   - cidr: 103.103.0.0/16
     hostSubnet: 24
```

User Defined Networks (OVN Layer)

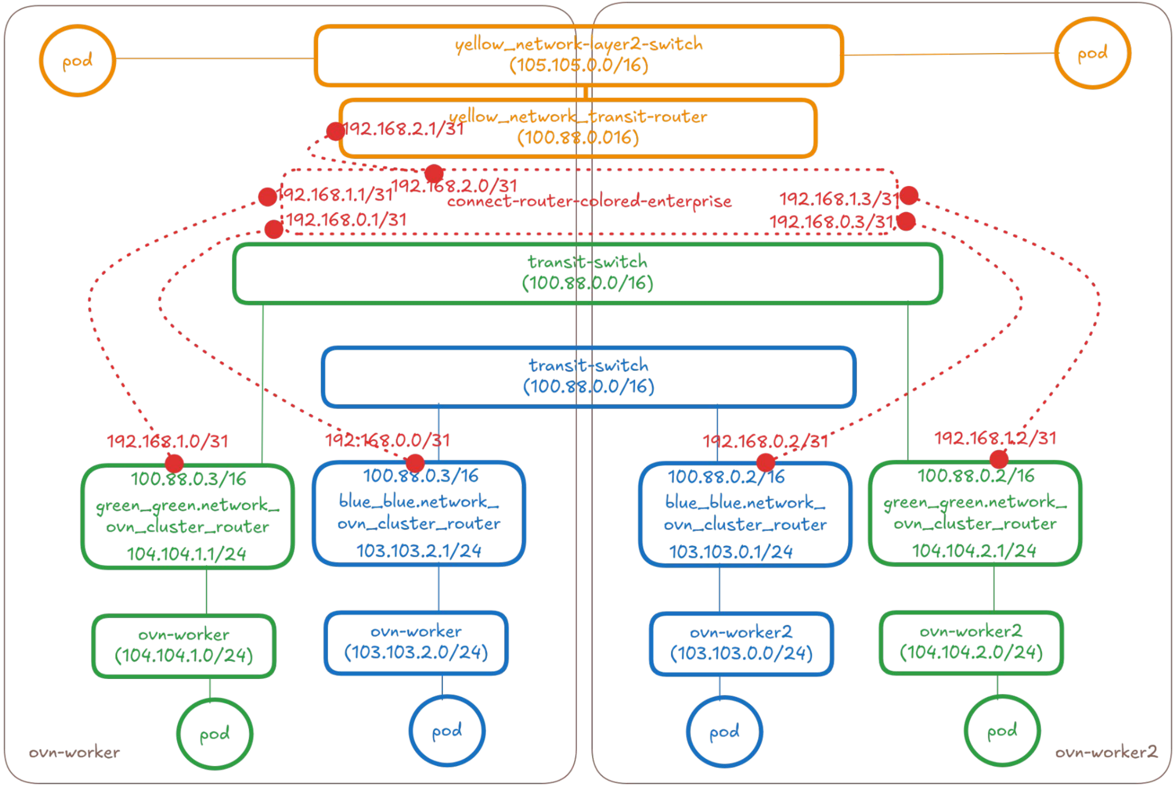


Cluster Network Connect = Group of connected Subnets



```yaml
apiVersion: k8s.ovn.org/v1
kind: ClusterNetworkConnect
metadata:
  name: colored-enterprise
spec:
  networkSelectors: # can match on UDNs and/or CUDNs
    - networkSelectionType: ClusterUserDefinedNetworks
      clusterUserDefinedNetworkSelector:
        networkSelector:
          matchExpressions:
          - key: purpose  # Match on actual label
            operator: In
            values:
            - german-network
    - networkSelectionType: PrimaryUserDefinedNetworks
      primaryUserDefinedNetworkSelector:
        namespaceSelector:
          matchExpressions:
          - key: kubernetes.io/metadata.name
            operator: In
            values:
            - blue
  connectSubnets: # can have at most 1 CIDR for each family type
    - cidr: 192.168.0.0/16
      networkPrefix: 24
    - cidr: fd01::/64
      networkPrefix: 100
  connectivity:
    - PodNetwork
    - ClusterIPServiceNetwork
```

Cluster Network Connect (OVN Layer)



Conclusion

- We have more features building on top of UDNs:
  - RouteAdvertisements (BGP) - advertise and receive networks
  - EVPN - extend your network isolation all the way to your provider networks
  - Support for connecting to cloud constructs

- OVN and OVS being the core stack helps with innovation
  - Flexible plug and play network types