

AZURE CNI OPTIONS

OVERLAY vs NODE SUBNET vs POD SUBNET

Choose the right networking model for AKS



WHY IT MATTERS?



Networking affects scalability, security, IP management, performance and cost.



AKS offers 3 main Azure CNI models.



Each fits different architectures and use cases.

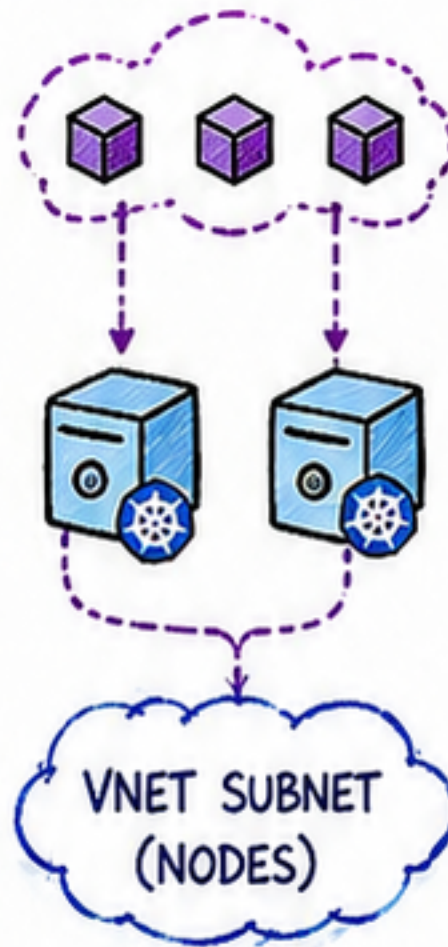


Choose based on connectivity and IP constraints.

THE 3 AZURE CNI MODELS

1

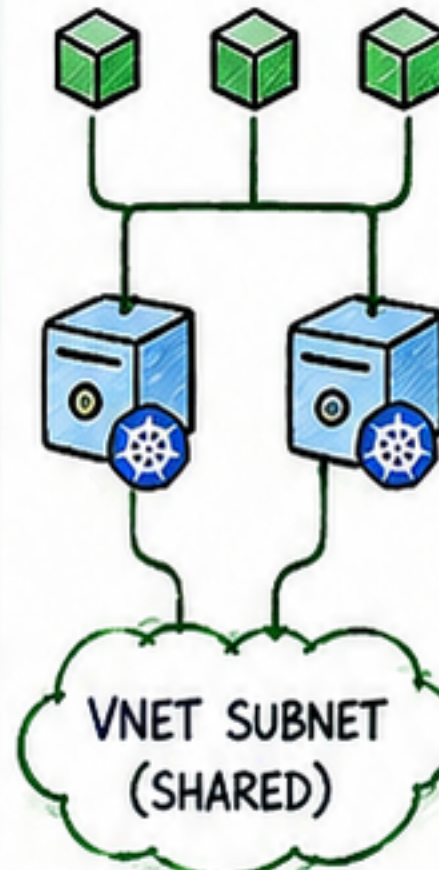
OVERLAY (Azure CNI Overlay)



Pods get IPs from a logical overlay / private pod CIDR, nodes get VNet subnet IPs.

2

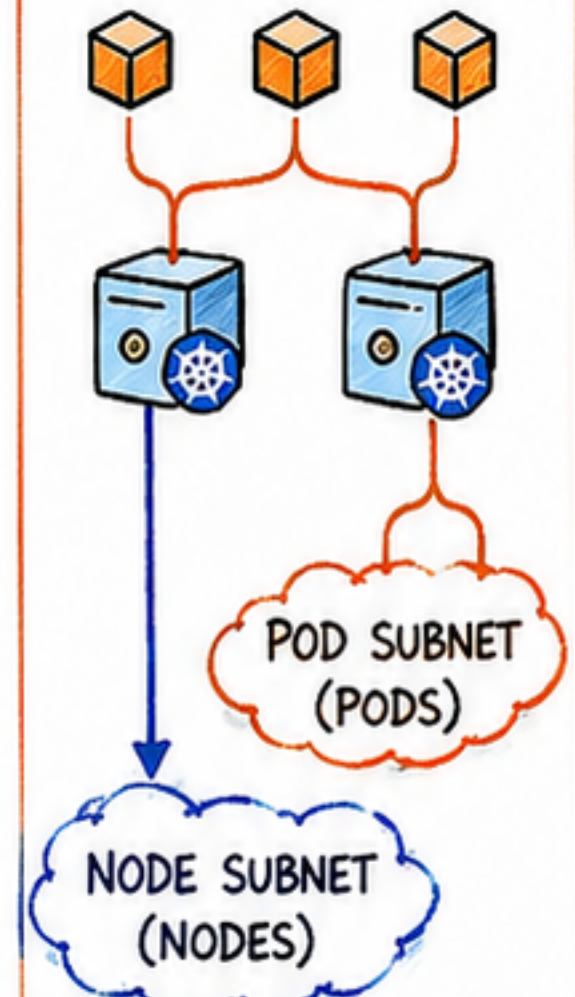
NODE SUBNET (Azure CNI)



Pods get IPs from the same subnet as nodes; legacy flat model.

3

POD SUBNET (Azure CNI with Pod Subnet)



Pods get IPs from a dedicated pod subnet; nodes use a separate node subnet.

KEY TAKEAWAY



No single option is best for all. Understand trade-offs and pick what fits your workload and network design.



Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.



AKS NETWORKING BUILDING BLOCKS



VNET

Isolated virtual network in Azure for your AKS cluster.



SUBNETS

IP ranges carved out of the VNet for nodes and other resources.



NODES

VMs in the node subnet that run your pods.



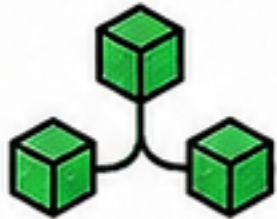
PODS

Workloads (containers) with their own IPs.



CNI PLUGIN

Manages IP allocation & networking for nodes and pods.



SERVICES

Stable virtual IPs that expose applications.

AKS NETWORK & IP FLOW



VNET

10.0.0.0/16



SUBNET (NODES)

10.0.1.0/24

NODE-1

10.0.1.4



NODE-2

10.0.1.5



PODS (ON NODE-1)



10.244.1.2



10.244.1.3

PODS (ON NODE-2)



10.244.2.2



10.244.2.3



SERVICE

10.0.1.100
(ClusterIP)

IN SIMPLE TERMS



The CNI plugin gives IPs to nodes (from the node subnet) and pods (from pod CIDR range), sets up networking, and makes sure everything can communicate securely.



OPTION 1: OVERLAY

Azure CNI Overlay



vighnesh-
notes

vighneshnaik.com

linkedin.com/in/
vighneshnaik6



HOW IT WORKS



Pods get IPs from a logical overlay / private pod CIDR.



Only nodes get IP addresses from the VNet subnet.



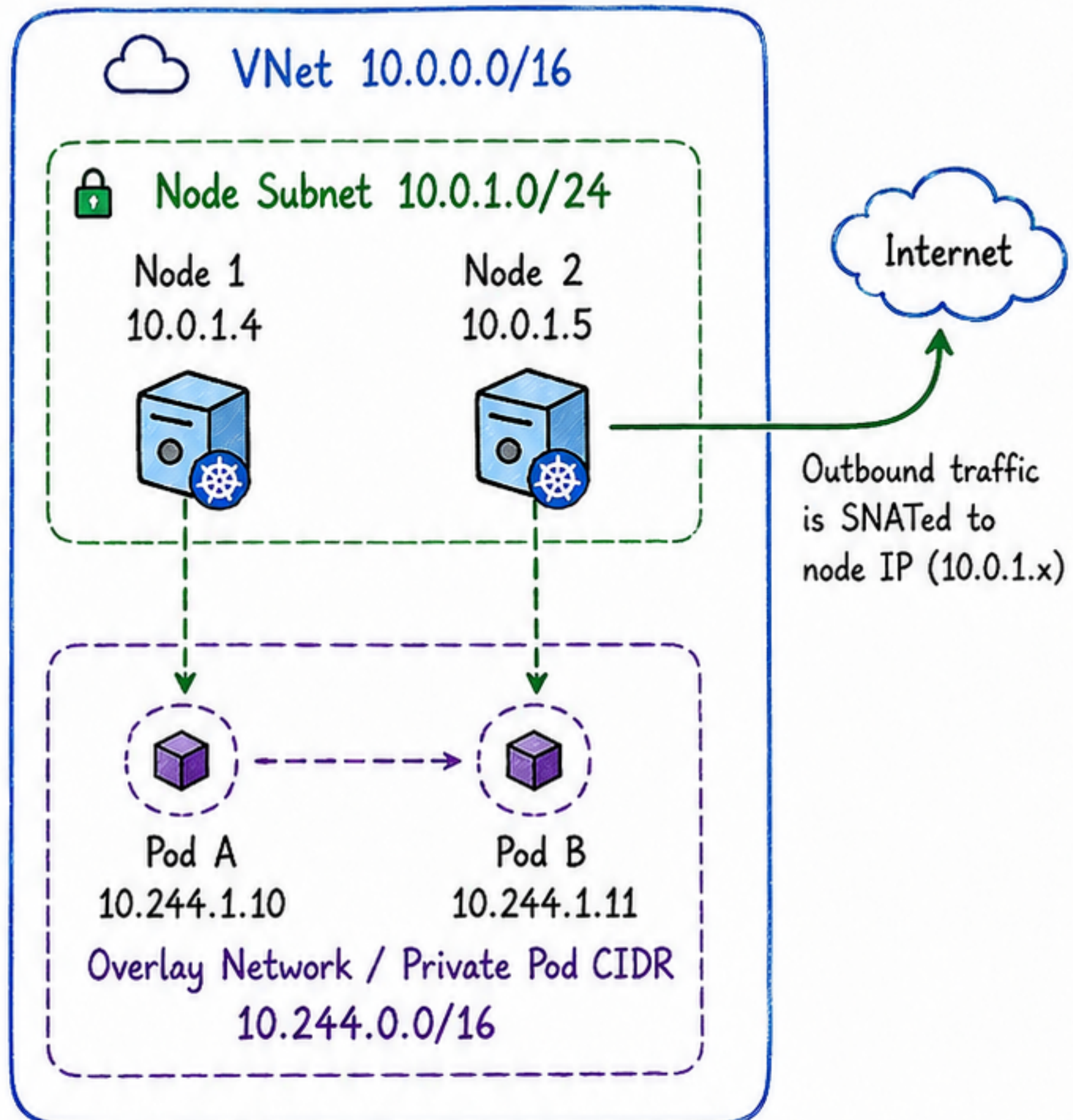
Traffic between pods stays in the overlay network.



Outbound traffic from pods is SNATed to the node IP.



Simplifies IP management and enables large scale.



- ✓ Pods get IPs from a logical overlay / private pod CIDR
- ✓ Only nodes use real IPs from the VNet subnet
- ✓ Pod-to-pod traffic stays inside the overlay network

- ✓ Outbound traffic is SNATed to the node IP
- ✓ VNet IPs are conserved for nodes only

PROS

- ✓ Conserves VNet IP space
- ✓ Easy scaling to thousands of pods
- ✓ Good for IP-constrained environments

CONS

- ✗ No direct external access to pod IPs
- ✗ Must use Service or ingress for access
- ✗ Plan CIDR overlap carefully

BEST FIT FOR

- ★ Limited VNet IP space
- ★ Large clusters
- ★ Most pod communication stays internal

OPTION 2: NODE SUBNET

Azure CNI • Legacy Flat Model



**vighnesh-
notes**

vighneshnaik.com

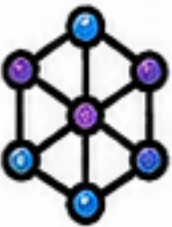
linkedin.com/in/vighneshnaik6



HOW IT WORKS



Pods get IPs from the same subnet as nodes.



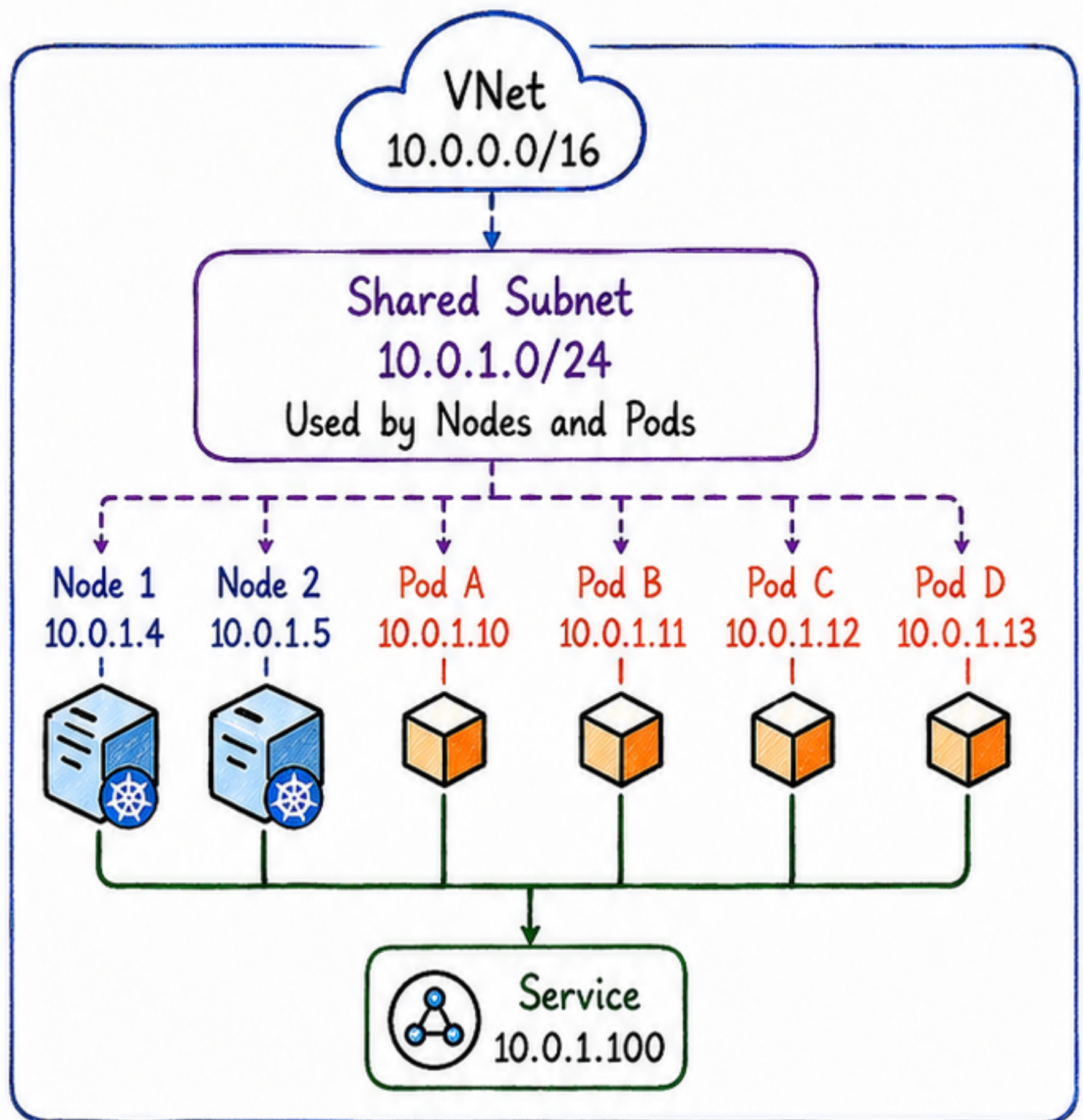
Flat networking (no separate pod subnet).



Direct routing within the VNet.



Each node reserves pod capacity in this subnet.



BEST FIT FOR



- Existing legacy AKS clusters
- Compatibility-driven environments
- Teams already operating this model



PROS

- ✓ Simple concept.
- ✓ Direct pod reachability in flat network.
- ✓ Familiar model for many teams.

CONS

- ⚠ Consumes more VNet IPs.
- ⚠ Harder IP management.
- ⚠ Subnet exhaustion risk.
- ⚠ Treated as legacy for new designs.



Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.



OPTION 3: POD SUBNET

Azure CNI with Pod Subnet

**vighnesh-
notes**

vighneshnaik.com

linkedin.com/in/vighneshnaik6

HOW IT WORKS



Pods get IPs from a dedicated pod subnet.



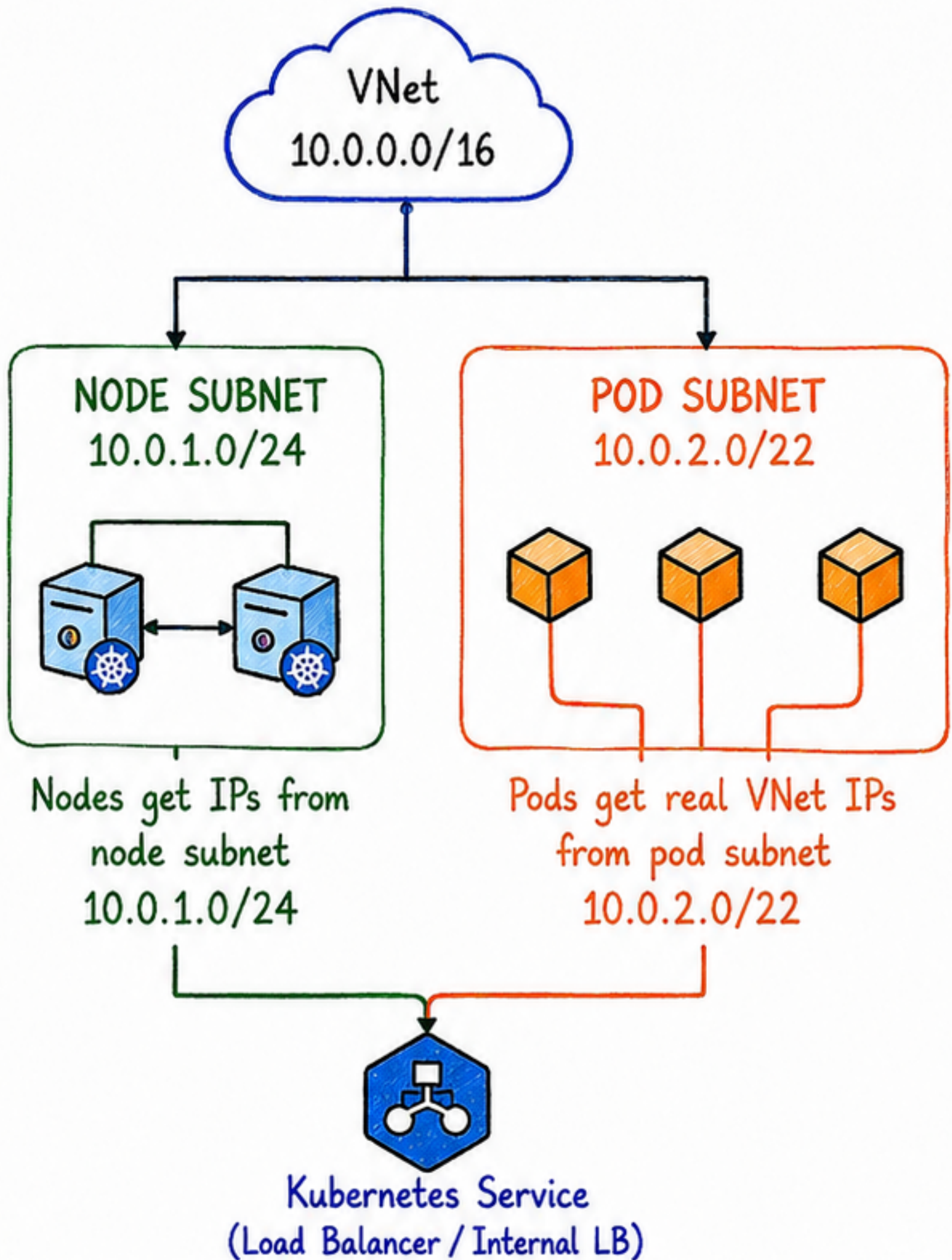
Nodes use a separate node subnet.



Flat networking – no overlays.



Direct routing within the VNet.



BEST FIT FOR



Enterprise or regulated environments.



Advanced network policies.



Direct pod reachability needs.



Strong separation between nodes and pods.



PROS

- ✓ Direct pod connectivity.
- ✓ Separate pod policy control.
- ✓ Strong network isolation.



CONS

- ✓ Uses more IPs than overlay.
- ✓ More address planning.
- ✓ Can be more complex.

RECOMMENDED OPTION

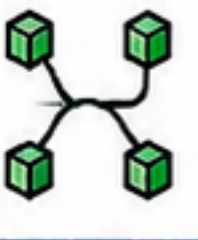


Choose Pod Subnet (Azure CNI with Pod Subnet) when your workloads need direct reachability, strong isolation, and flat networking.

COMPARISON AT A GLANCE

Overlay vs Pod Subnet vs Node Subnet


vighnesh-notes
vighneshnaik.com
linkedin.com/in/vighneshnaik6

ASPECT	OVERLAY (Azure CNI Overlay)	POD SUBNET (Azure CNI with Pod Subnet)	NODE SUBNET (Azure CNI)
 Pod IP source	Private pod CIDR (overlay / tunneled)	Dedicated pod subnet	Shared node subnet
 Network type	Overlay (tunneled)	Flat network (L3 routing)	Flat network (Legacy)
 Direct external pod reachability	No (Not reachable directly)	Yes (Reachable directly via pod subnet)	Yes (Direct flat connectivity)
 VNet IP consumption	Low (Uses only node subnet IPs)	Medium to High (Consumes IPs for all pods)	Highest (Each node IP is also a pod IP)
 Scalability	Very good (Scales to very large clusters)	High (Scales well with enough IPs)	Legacy (Limited by node subnet IPs)
 Complexity	Medium (Overlay setup & troubleshooting)	Medium (Subnet & routing management)	Low (Simple but legacy model)
 Performance	Good (Slight overlay overhead)	Very good (Native routing)	Good (Native routing)
 Best fit	Modern clusters needing IP conservation & high scale	Clusters needing direct pod reachability with subnet separation	Legacy workloads & flat network requirements

KEY TAKEAWAY



- 1 Overlay is best for IP conservation and massive scale.
- 2 Pod Subnet is best for direct pod connectivity with clear subnet separation.
- 3 Node Subnet is mainly for legacy scenarios.



Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.



BEST PRACTICES & CONSIDERATIONS



vighnesh-
notes

vighneshnaik.com

linkedin.com/in/vighneshnaik6

Make the right CNI choice. Build it right. Keep it simple!



BEST PRACTICES



Plan IP address space early.



Test in non-production.



Monitor subnet utilization.



Choose model based on workload needs.



Document routing and connectivity.



MIGRATION NOTES

- Moving between models usually requires new clusters or node pools.
- Validate DNS, ingress, egress, and connectivity.
- Plan rollback.



THINGS TO CONSIDER



IP availability in your region & quotas.



Network policies and organizational rules.



NSGs & UDRs impact traffic flow.



Egress design (NAT Gateway, Firewall, Private Endpoints).



Compliance & security requirements.



Future scale & growth expectations.

TIP



Right CNI choice today saves cost, time and complexity tomorrow!



Keep It Simple. Design for Scale. Secure by Design. Cost Optimized.

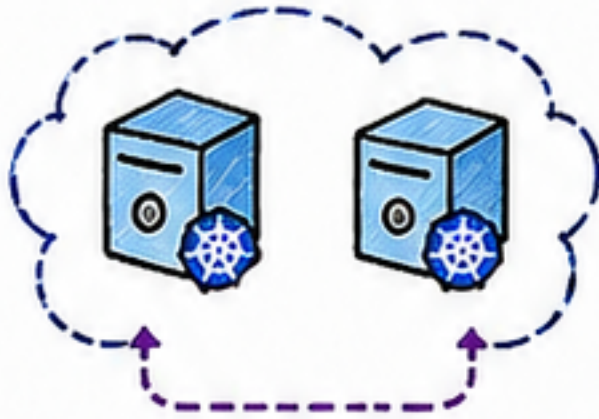




QUICK DECISION GUIDE

Choose the right AKS networking model

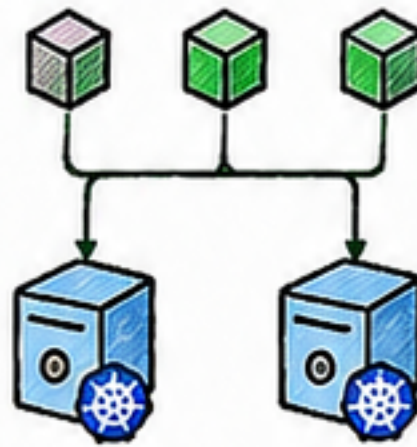
1



CHOOSE OVERLAY IF...

- VNet IP space is limited
- most pod traffic stays internal
- direct external pod IP access is not needed
- you want simple IP management

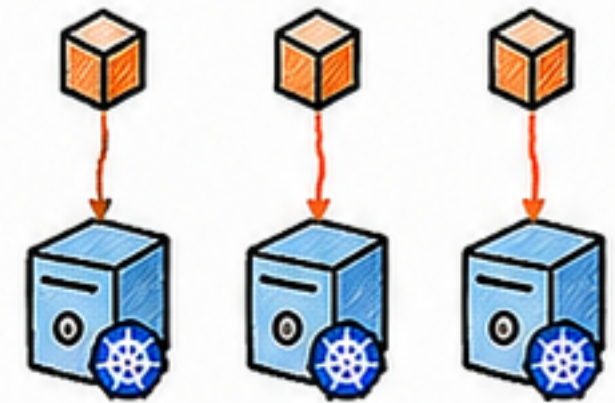
2



CHOOSE NODE SUBNET IF...

- you must support an existing legacy pattern
- compatibility requires the shared-subnet model
- you understand the higher IP consumption
- ⚠️ **NOT** the default recommended option

3



CHOOSE POD SUBNET IF...

- you need direct pod reachability
- want strict separation between pods and nodes
- have enough IP address space
- need stronger subnet-level policy control



Understand. Plan. Choose Right.

Match the model to your IP strategy and connectivity needs.

