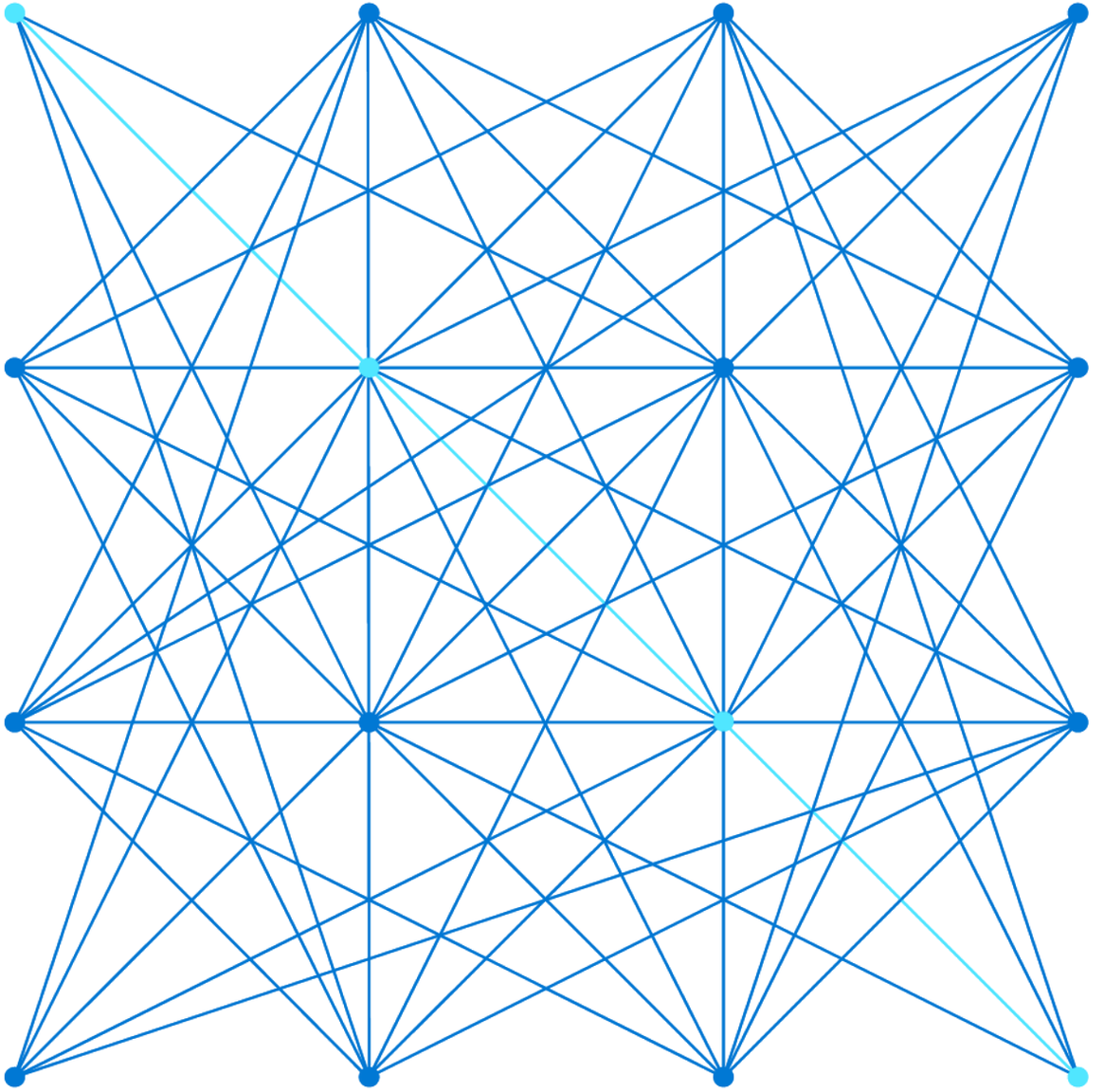
Microsoft Azure

AKS Foundational Training Networking



Microsoft Azure

Conditions & Terms of Use

Microsoft Proprietary and Confidential Information

This training package content is proprietary and confidential, and is intended only for users described in the training materials. Some elements of this document and the content contained herein are subject to change. This document and the content contained herein are for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

This content and information is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or information included in this package is strictly prohibited. Any persons accessing this document, and the content contained herein, are responsible for complying with all applicable copyright laws. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document and the content contained herein. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document, and of the content contained herein, does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft and the Microsoft products and services listed are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft Azure

Contents

Microsoft Azure

Course/Lesson Objectives

At the end of this session, you'll be able to:

1. Recognize the AKS general networking architecture.
2. Distinguish between Azure Network components and Kubernetes components.
3. Explain AKS network troubleshooting.

Microsoft Azure

AKS networking introduction

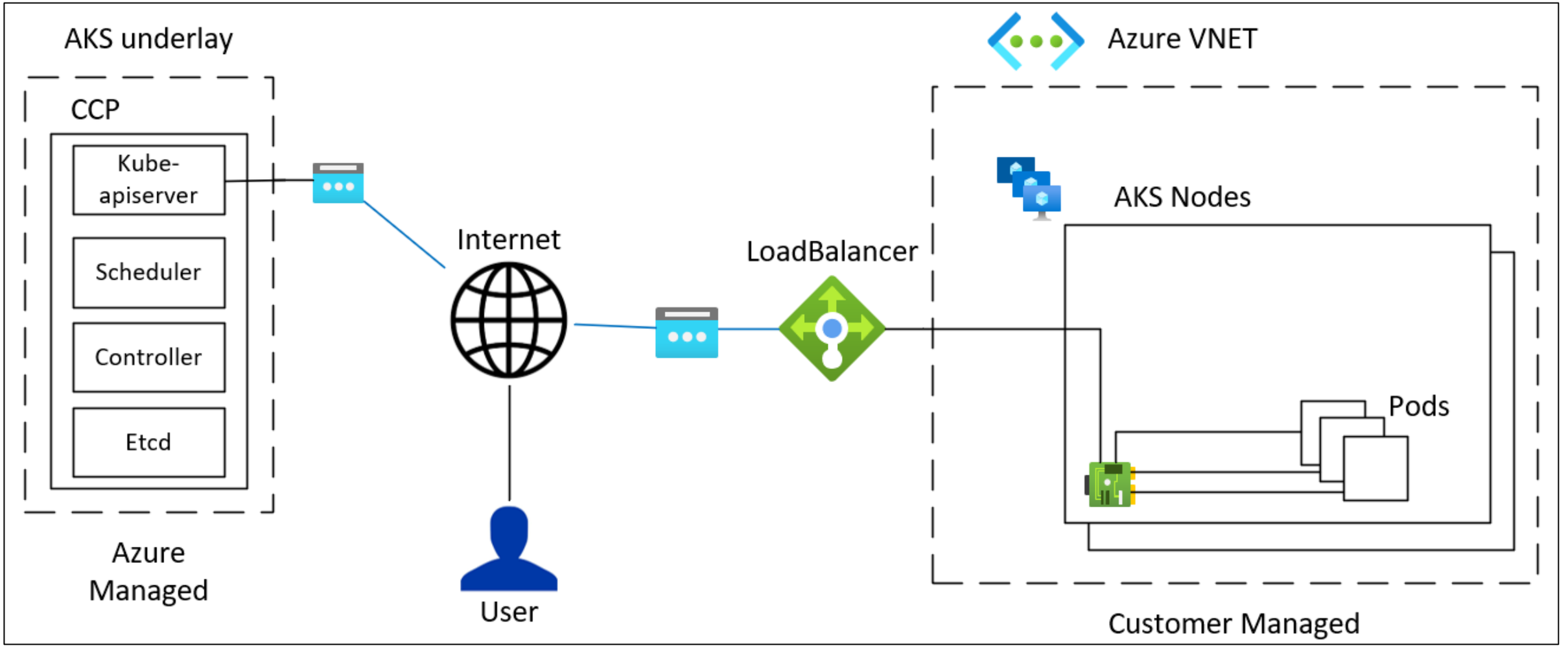
Microsoft Azure

High level overview

- Kubernetes API is exposed with a public IP.
- AKS nodes reach the API through a standard load balancer (LB) dedicated outbound IP.
- CNI (Container Network Interface) provides IPs to pods.
- Pods outbound network address translation (NAT) through nodes and then the LB outbound.

Microsoft Azure

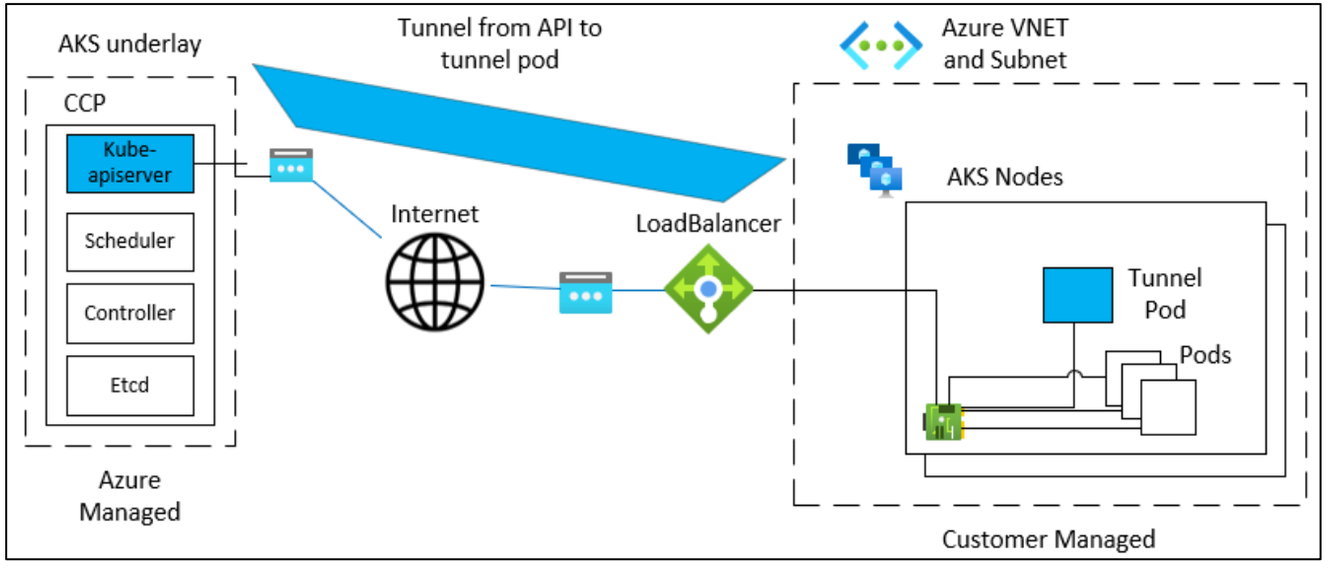
Networking overview



Microsoft Azure

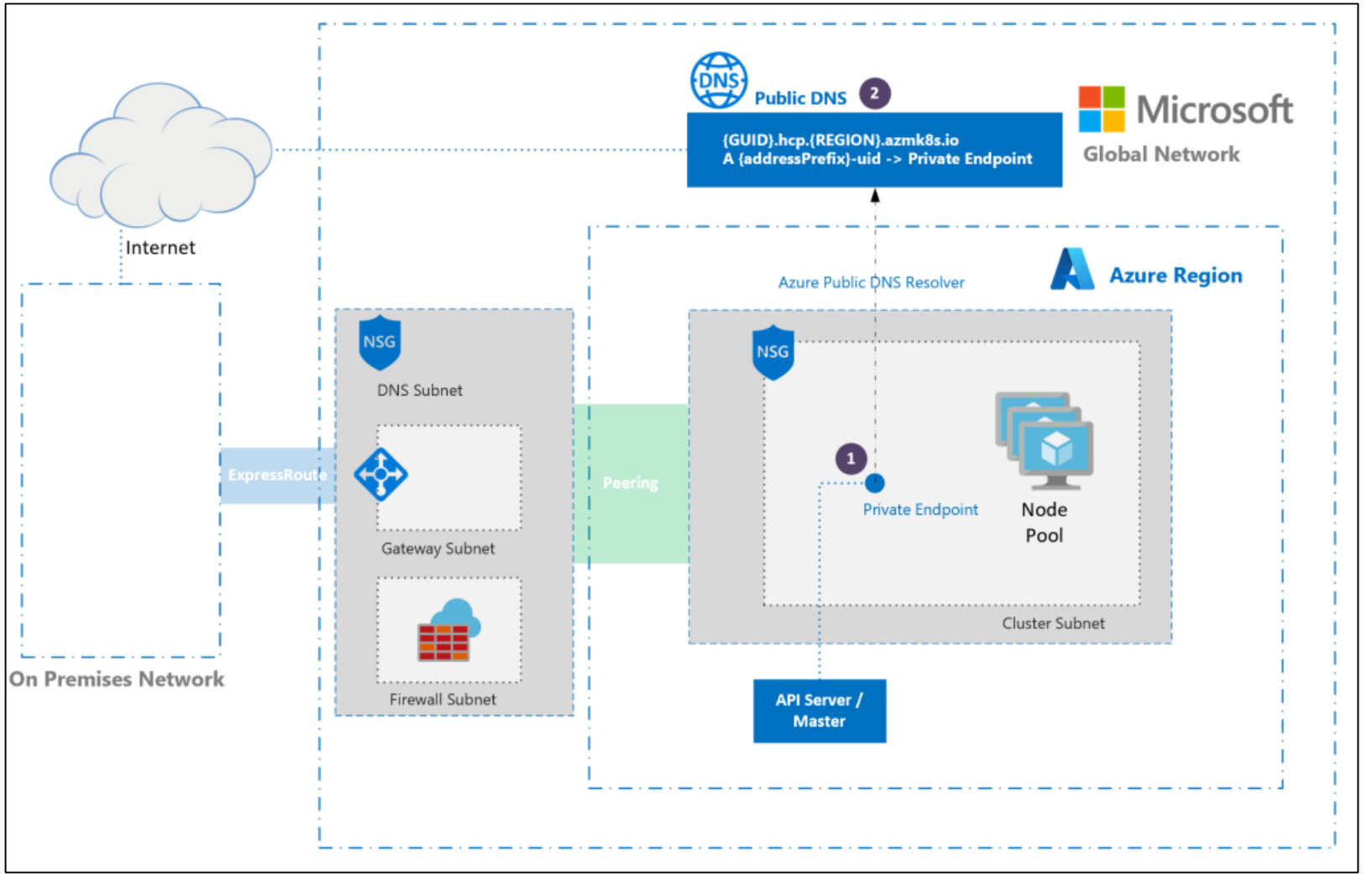
AKS tunnel

- Network path required from API server to the cluster node network for specific operations.
- AKS control plane components are in a separate networks.
- This tunnel consists of a server on the control plane side, and a client on the customer side.



Microsoft Azure

Networking overview for private cluster



Microsoft Azure

AKS CNI options

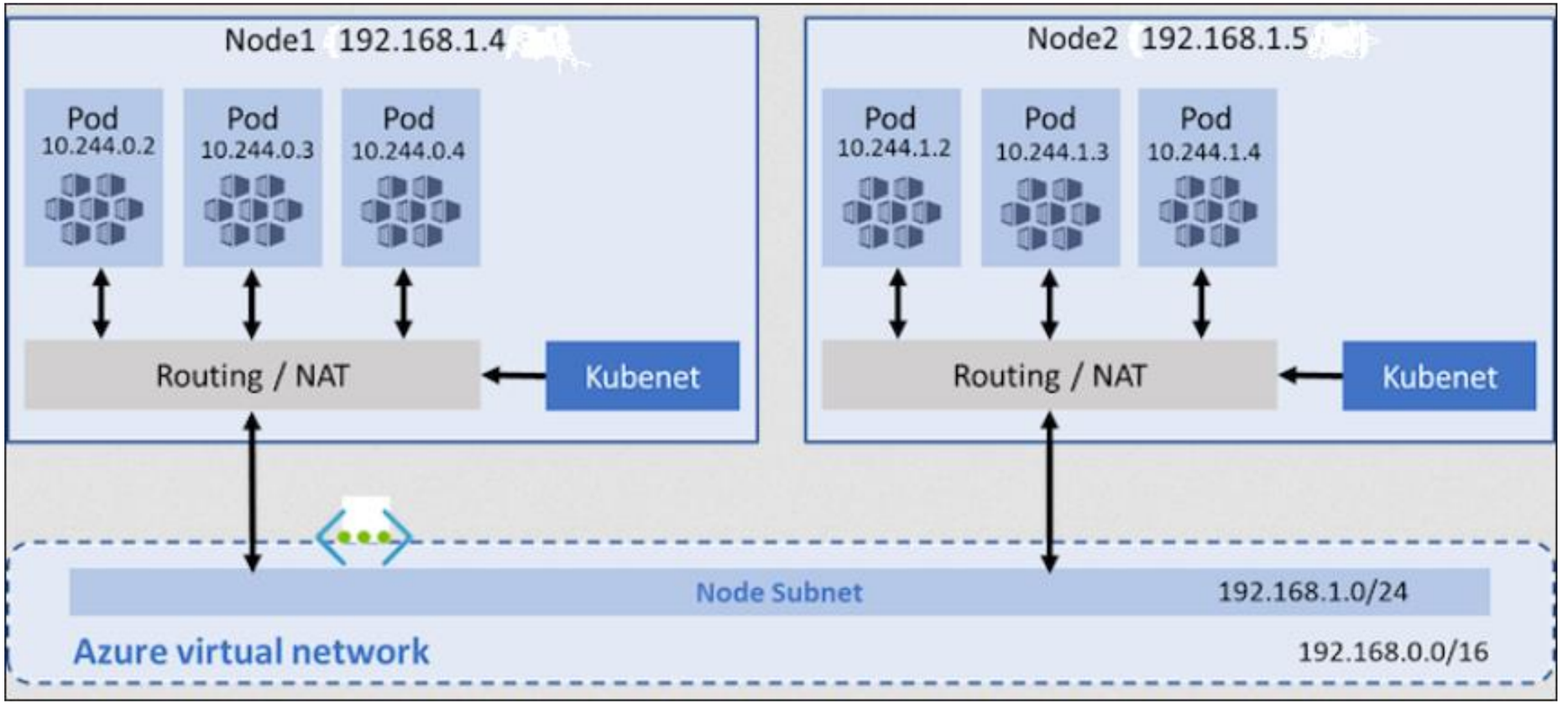
Microsoft Azure

AKS Kubenet

- Default Container Network Interface (CNI).
- Nodes get an IP from an Azure subnet.
- Pods get an IP from a logical address space in the nodes.
- NAT configured for pods to reach Azure virtual network.
- Source IP is translated to the node's primary IP.
- User defined route (UDR) is required on the nodes' subnet.

Microsoft Azure

AKS Kubenet



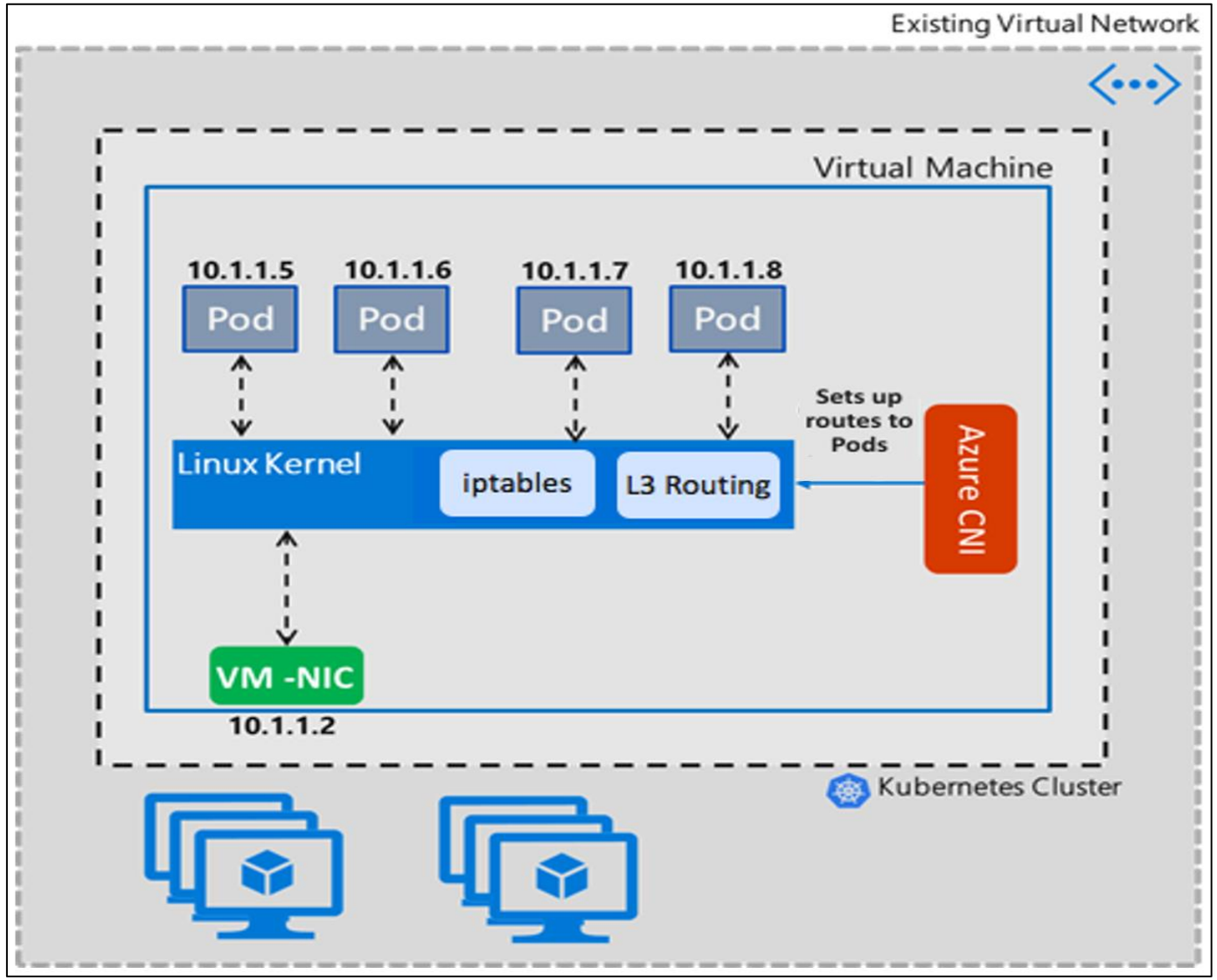
Microsoft Azure

Azure CNI (Advance CNI)

- Nodes and Pods get an IP from the subnet.
- Each node gets 1 + MaxPod IPs assigned.
- Pods traffic going to a different network get NAT through node IP.
- An UDR is not required.

Microsoft Azure

Azure CNI (Advance CNI)



Microsoft Azure

AKS network components

Microsoft Azure

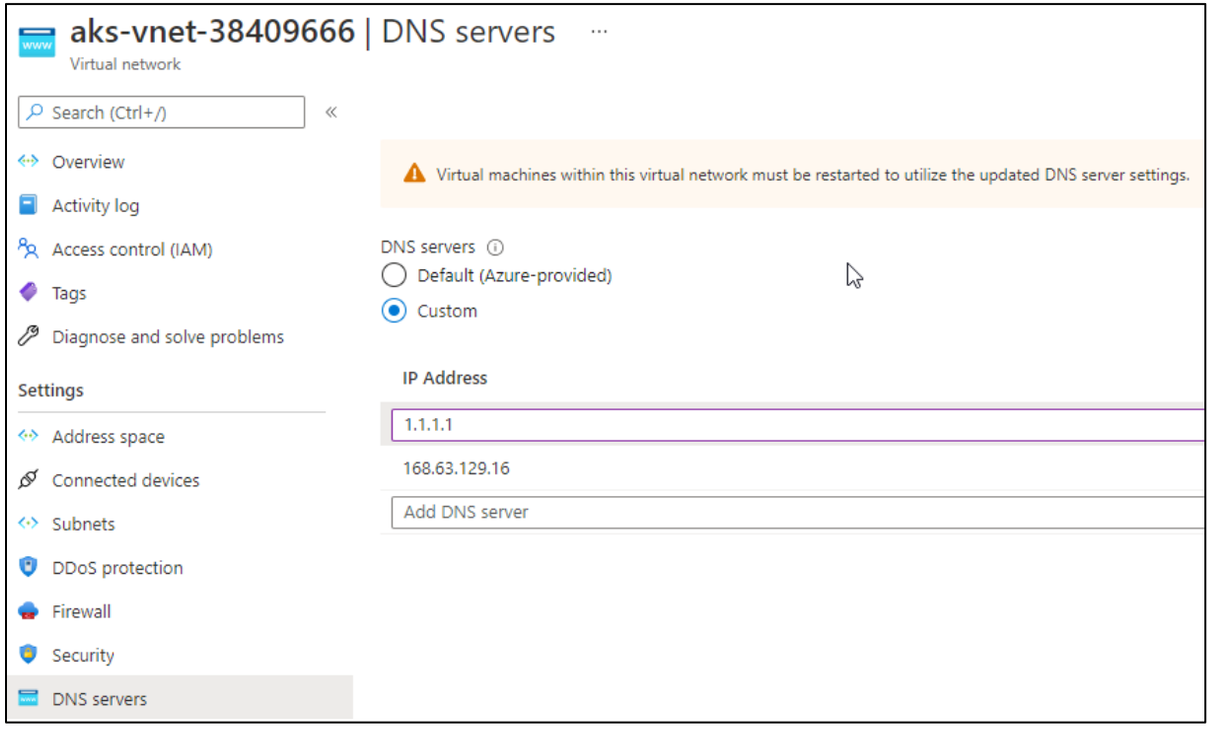
Azure network components

- VNET, Subnet, LB, Network Security Group (NSG), UDR, PublicIP, DNS.
- For Kubenet you can specify an existing UDR.
- AKS nodes requires an NSG.
- Default Azure Domain Name System (DNS) is set on the VNET but can be customized.

Microsoft Azure

Azure network DNS

- Azure VNET default DNS 168.63.129.16.
- Custom DNS servers can be set on the VNET.
- AKS nodes get DNS configured through Dynamic Host Configuration Protocol (DHCP).



Microsoft Azure

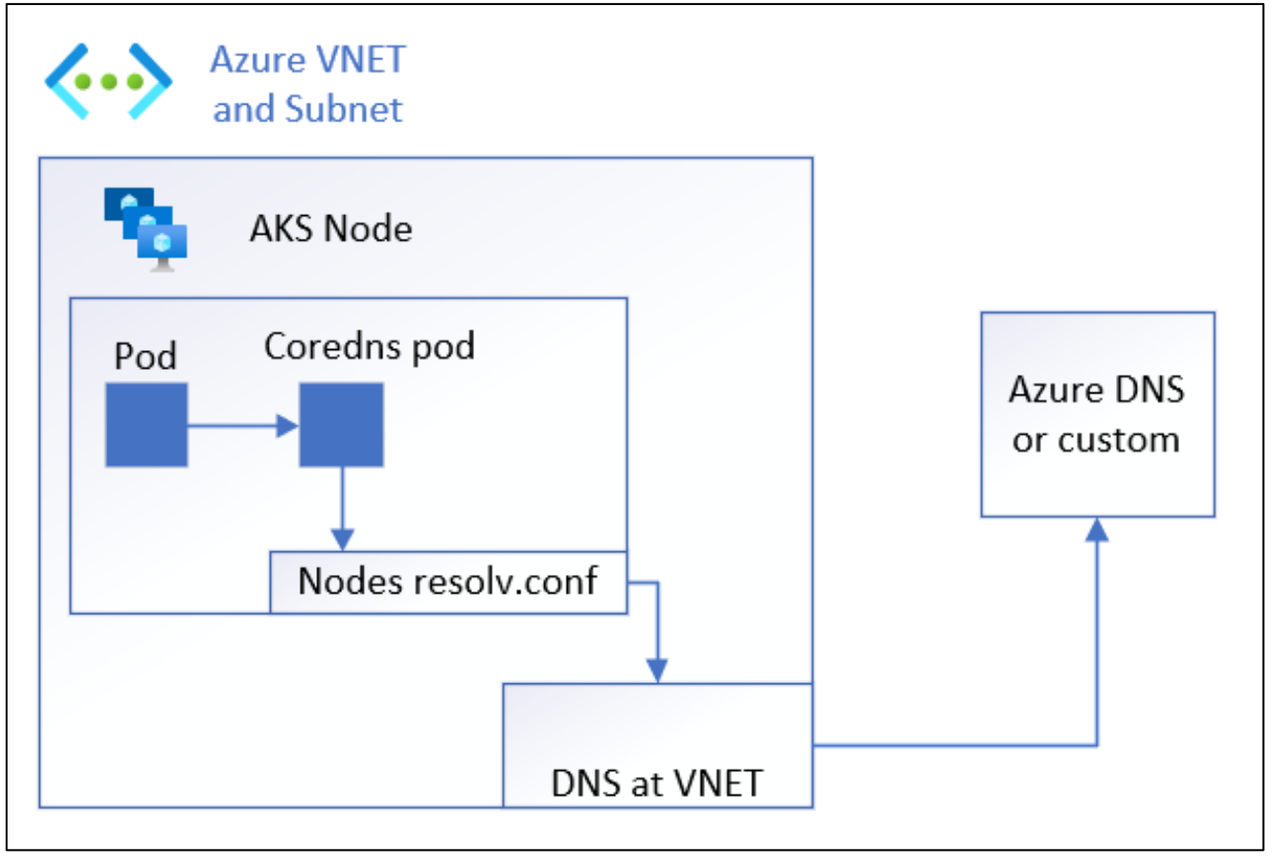
Kubernetes network components

- --service-cidr sets the K8s service CIDR.
- --dns-service-ip sets the kubedns service IP.
- --pod-cidr sets Kubenet pod CIDR
  - Must be large enough to accommodate the number of nodes that you expect. You can't change this address range once the cluster is deployed.
  - This range is used to assign a /24 address space to each node in the cluster.
- --docker-bridge-address lets nodes communicate with the underlying management platform.

Microsoft Azure

AKS Kubernetes DNS service

- AKS includes Coredns service.
- Coredns uses the node /etc/resolv.conf as a forwarder (the DNS on the VNET will be use as forwarders for external records).
- Coredns deployment is controlled by the CCP addon manager.
- Coredns-custom configmap.



Microsoft Azure

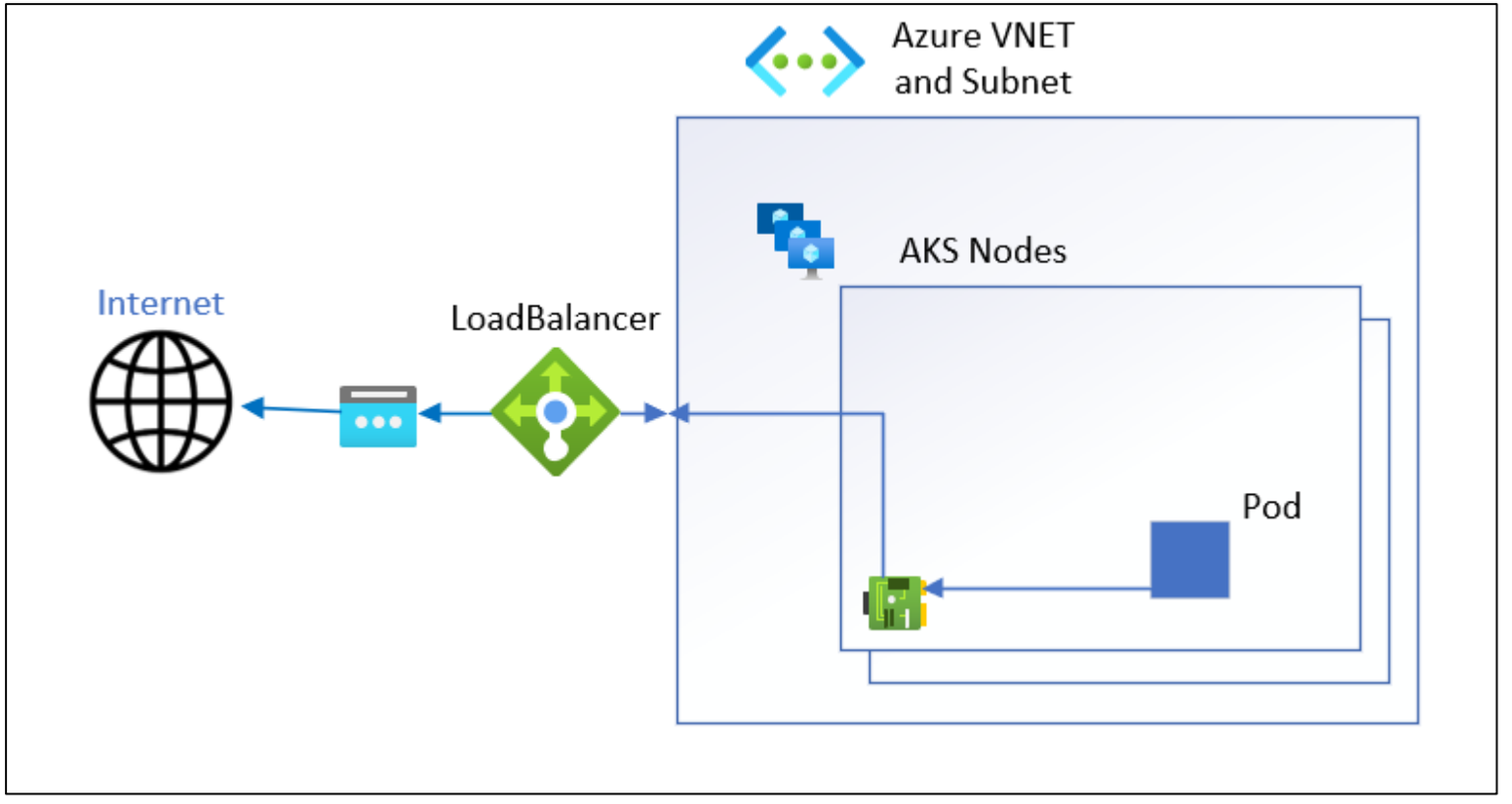
AKS traffic flow

Microsoft Azure

AKS common traffic flows

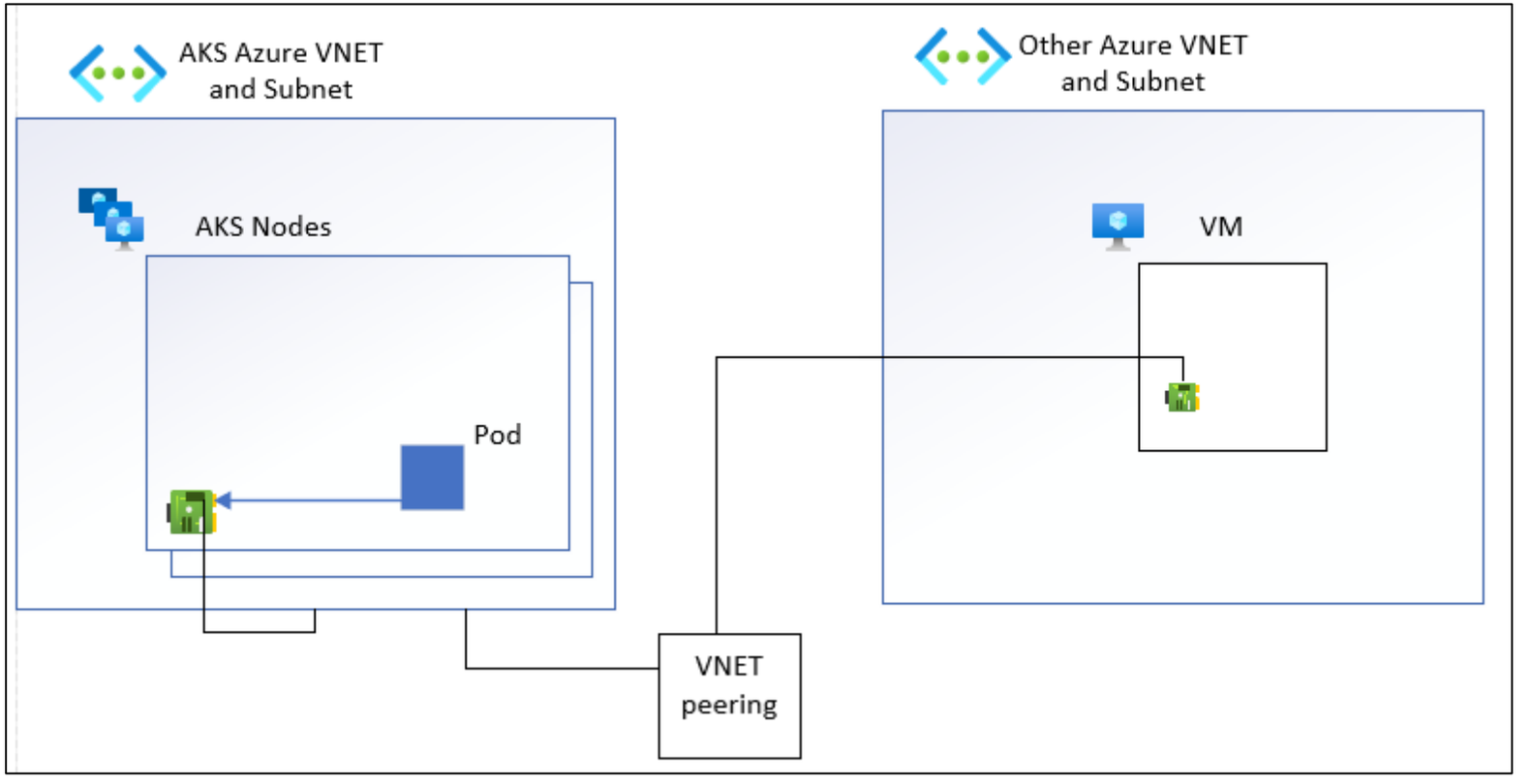
- Outbound from a pod to the Internet.
- Outbound from a pod to another VNET.
- Inbound from the Internet to a pod.
- Inbound from another VNET to a pod.

Outbound from a pod to the internet



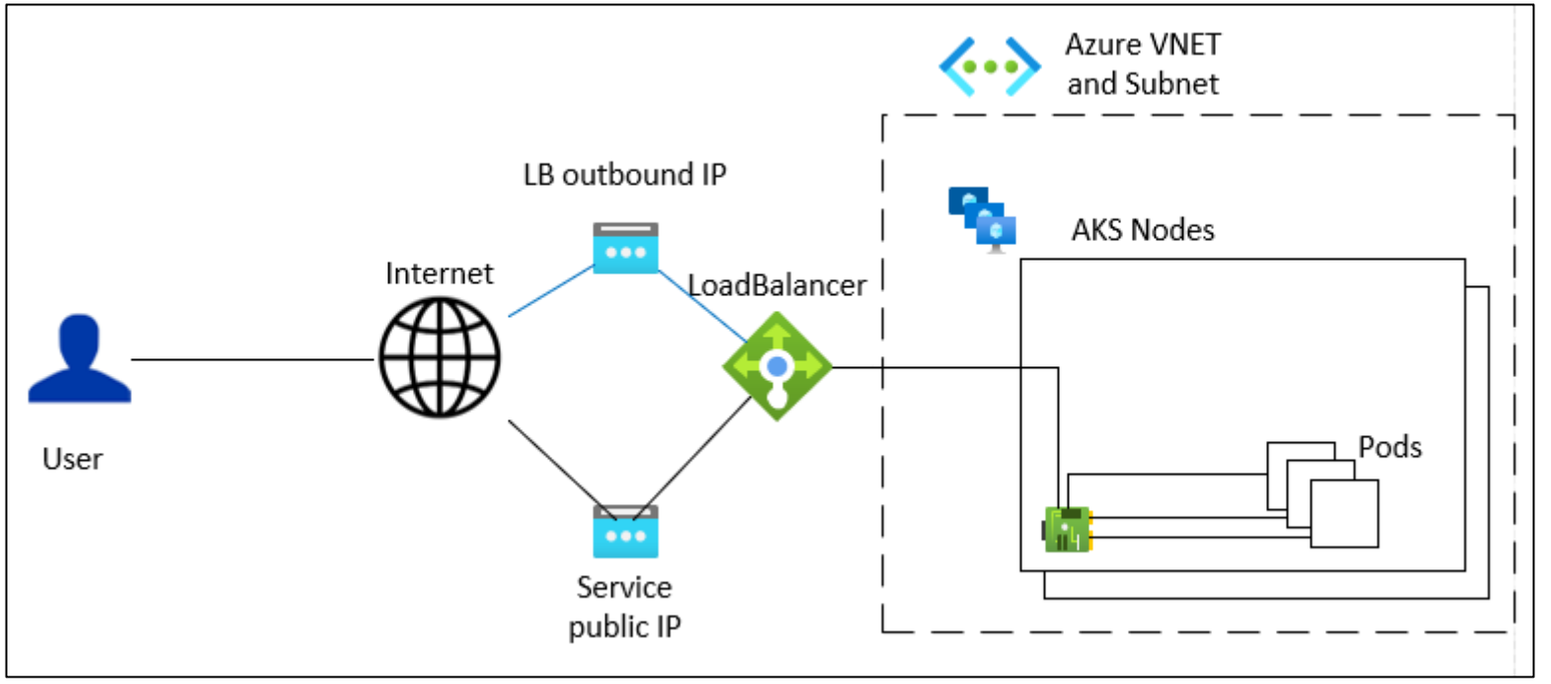
Microsoft Azure

Outbound from a pod to another VNET



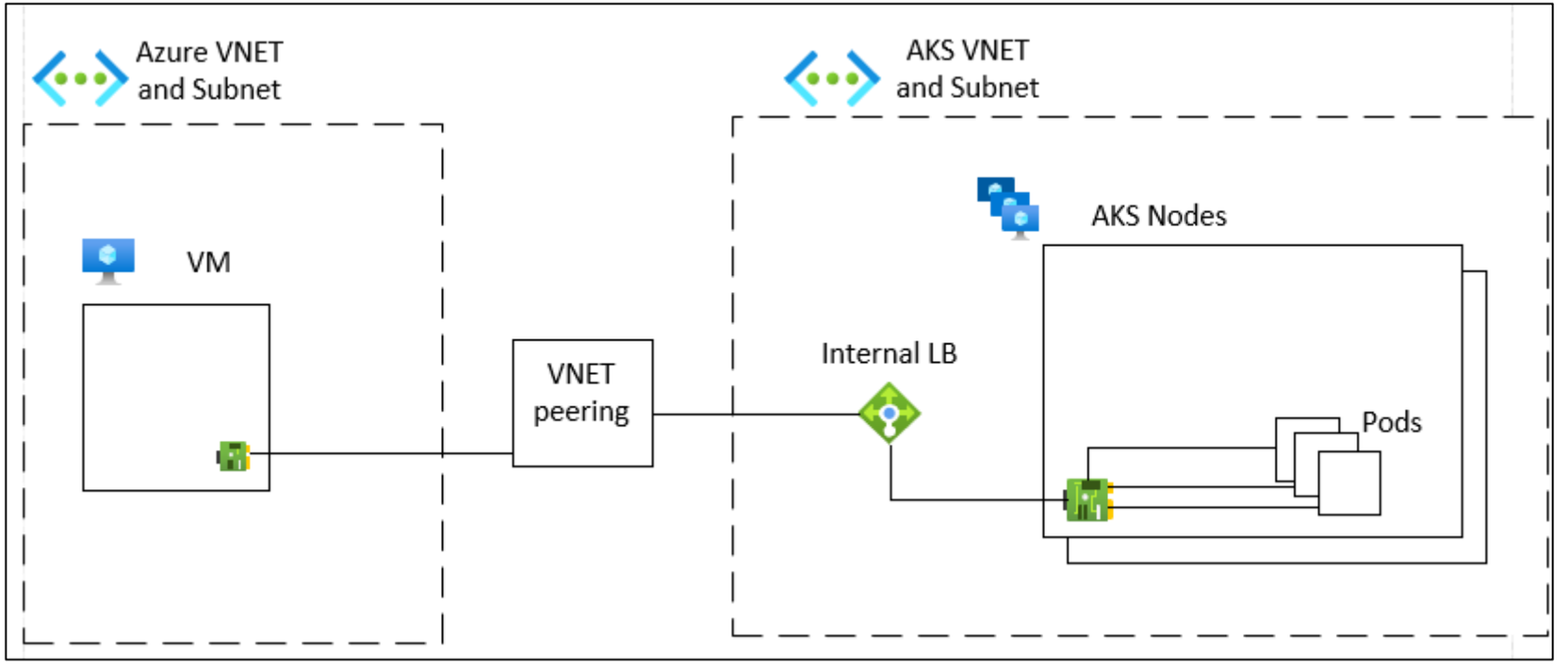
Microsoft Azure

Inbound from the internet to a pod



Microsoft Azure

Inbound from another VNET to a pod

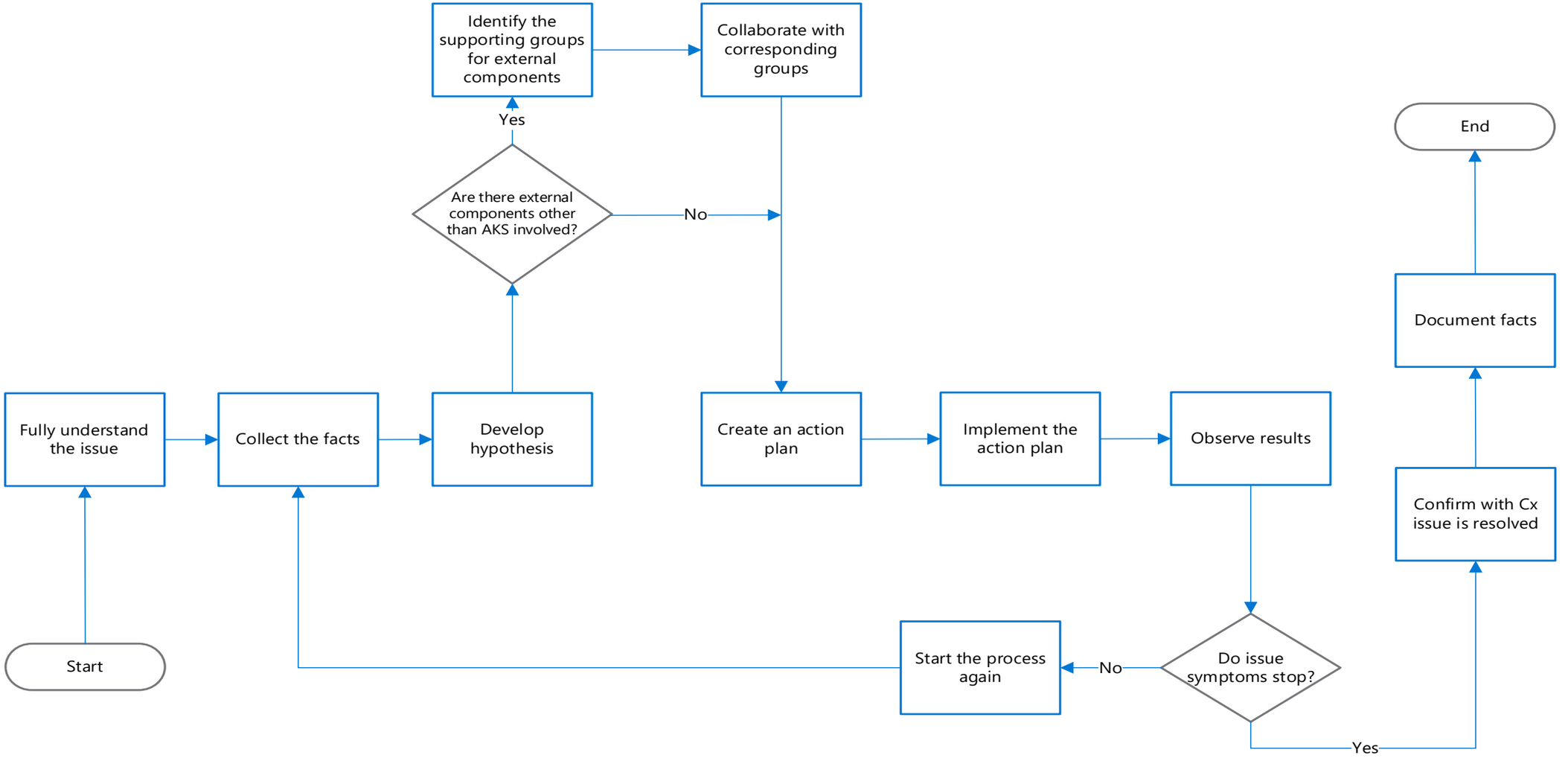


Microsoft Azure

AKS network troubleshooting

Microsoft Azure

AKS general network troubleshooting



Microsoft Azure

Demo: Troubleshooting Pod to Pod Connectivity

Scenario

- Walkthrough for AKS network troubleshooting exercise where pods are not able to reach other pods on different nodes.

Tasks

1. Review AKS cluster with pod-to-pod connectivity issues.
2. Use ASC and Applens to collect general cluster information.
3. Diagnose and resolve the issue.

Duration: 13 minutes.

Microsoft Azure

Course/Lesson summary

During this session, you have gain knowledge about:

1. The AKS general networking architecture.
2. The Azure network components and Kubernetes components.
3. AKS network troubleshooting.

Microsoft Azure

Resources

- Network concepts for applications in Azure Kubernetes Service (AKS)
- Use kubenet networking with your own IP address ranges in Azure Kubernetes Service (AKS)
- Configure Azure CNI networking in Azure Kubernetes Service (AKS)
- Customize CoreDNS with Azure Kubernetes Service
- Control egress traffic for cluster nodes in Azure Kubernetes Service (AKS)
- Name resolution for resources in Azure virtual networks

Microsoft Azure

Thank you.