Document Generated: 11/05/2026

Learning Style: Virtual Classroom

Technology: Microsoft

Difficulty: Intermediate

Course Duration: 3 Days

Designing and Implementing Microsoft Azure Networking Solutions (AZ-700T00)



About this Course:

This course teaches Network Engineers how to design, implement, and maintain Azure networking solutions. This course covers the process of designing, implementing, and managing core Azure networking infrastructure, Hybrid Networking connections, load balancing traffic, network routing, private access to Azure services, network security and monitoring. Learn how to design and

implement a secure, reliable, network infrastructure in Azure and how to establish hybrid connectivity, routing, private access to Azure services, and monitoring in Azure.

Course Objectives:

- Design, implement and manage hybrid network connections
- Design and implement core Azure networking infrastructure
- Design and implement routing and load balancing in Azure
- Secure and monitor networks
- Design and implement private access to Azure Services

Audience:

This course is for Network Engineers looking to specialize in Azure networking solutions. An Azure Network engineer designs and implements core Azure networking infrastructure, hybrid networking connections, load balance traffic, network routing, private access to Azure services, network security and monitoring. The azure network engineer will manage networking solutions for optimal performance, resiliency, scale, and security.

Prerequisites:

- Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding of network configurations, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding of software defined networking.
- Understanding hybrid network connectivity methods, such as VPN.
- Understanding resilience and disaster recovery, including high availability and restore operations.

Course Outline:

Module 1: Introduction to Azure Virtual Networks

In this module you will learn how to design and implement fundamental Azure Networking resources such as virtual networks, public and private IPs, DNS, virtual network peering, routing, and Azure Virtual NAT.

Lessons

- Explore Azure Virtual Networks

- Configure public IP services
- Design name resolution for your Virtual Network
- Enable Cross-VNet connectivity with peering
- Implement virtual network traffic routing
- Configure internet access with Azure Virtual NAT

Lab : Exercise: design and implement a Virtual Network in Azure

Lab : Exercise: configure DNS settings in Azure

Lab : Exercise: connect two Azure Virtual Networks using global virtual network peering

After completing this module, students will be able to:

- Implement virtual networks
- Configure public IP services
- Configure private and public DNS zones
- Design and implement cross-VNET connectivity
- Implement virtual network routing
- Design and implement an Azure Virtual Network NAT

Module 2: Design and Implement Hybrid Networking

In this module you will learn how to design and implement hybrid networking solutions such as Site-to-Site VPN connections, Point-to-Site VPN connections, Azure Virtual WAN and Virtual WAN hubs.

Lessons

- Design and implement Azure VPN Gateway
- Connect networks with Site-to-site VPN connections
- Connect devices to networks with Point-to-site VPN connections
- Connect remote resources by using Azure Virtual WANs
- Create a network virtual appliance (NVA) in a virtual hub

Lab : Exercise: create a Virtual WAN by using Azure Portal

Lab : Exercise: create and configure a virtual network gateway

After completing this module, students will be able to:

- Design and implement a site-to-site VPN connection
- Design and implement a point-to-site VPN connection
- Design and implement Azure Virtual WAN Resources

Module 3: Design and implement Azure ExpressRoute

In this module you will learn how to design and implement Azure ExpressRoute, ExpressRoute Global Reach, ExpressRoute FastPath and ExpressRoute Peering

options.

Lessons

- Explore Azure ExpressRoute
- Design an ExpressRoute deployment
- Configure peering for an ExpressRoute deployment
- Connect an ExpressRoute circuit to a VNet
- Connect geographically dispersed networks with ExpressRoute global reach
- Improve data path performance between networks with ExpressRoute FastPath
- Troubleshoot ExpressRoute connection issues

Lab : Exercise: configure an ExpressRoute gateway

Lab : Exercise: provision an ExpressRoute circuit

After completing this module, students will be able to:

- Design and implement Expressroute
- Design and implement Expressroute Direct
- Design and implement Expressroute FastPath

Module 4: load balancing non-HTTP(S) traffic in Azure

In this module you will learn how to design and implement load balancing solutions for non-HTTP(S) traffic in Azure with Azure Load balancer and Traffic Manager.

Lessons

- Explore load balancing
- Design and implement Azure load balancer using the Azure portal
- Explore Azure Traffic Manager

Lab : Exercise: create a Traffic Manager profile using the Azure portal

Lab : Exercise: create and configure an Azure load balancer

After completing this module, students will be able to:

- Design and implement Azure Laod Balancers
- Design and implement Azure Traffic Manager

Module 5: Load balancing HTTP(S) traffic in Azure

In this module you will learn how to design and implement load balancing solutions for HTTP(S) traffic in Azure with Azure Application gateway and Azure Front Door.

Lessons

- Design Azure application gateway
- Configure Azure application gateway
- Design and configure Azure front door

Lab : Exercise: deploy Azure application gateway

Lab : Exercise: create a front door for a highly available web application

After completing this module, students will be able to:

- Design and implement Azure Application Gateway
- Implement Azure Front Door

Module 6: Design and implement network security

In this module you will learn to design and imponent network security solutions such as Azure DDoS, Azure Firewalls, Network Security Groups, and Web Application Firewall.

Lessons

- Secure your virtual networks in the Azure portal
- Deploy Azure DDoS Protection by using the Azure portal
- Deploy Network Security Groups by using the Azure portal
- Design and implement Azure Firewall
- Working with Azure Firewall Manager
- Implement a Web Application Firewall on Azure Front Door

Lab : Exercise: deploy and configure Azure Firewall using the Azure portal

Lab : Exercise: secure your virtual hub using Azure Firewall Manager

Lab : Exercise: configure DDoS Protection on a virtual network using the Azure portal

After completing this module, students will be able to:

- Configure and monitor an Azure DDoS protection plan
- implement and manage Azure Firewall
- Implement network security groups
- Implement a web application firewall (WAF) on Azure Front Door

Module 7: Design and implement private access to Azure Services

In this module you will learn to design and implement private access to Azure Services with Azure Private Link, and virtual network service endpoints.

Lessons

- Define Private Link Service and private endpoint

- Explain virtual network service endpoints
- Integrate Private Link with DNS
- Integrate your App Service with Azure virtual networks

Lab : Exercise: create an Azure private endpoint using Azure PowerShell

Lab : Exercise: restrict network access to PaaS resources with virtual network service endpoints

After completing this module, students will be able to:

- Define the difference between Private Link Service and private endpoints
- Design and configure private endpoints
- Explain virtual network service endpoints
- Design and configure access to service endpoints
- Integrate Private Link with DNS
- Integrate your App Service with Azure virtual networks

Module 8: Design and implement network monitoring

In this module you will learn to design and implement network monitoring solutions such as Azure Monitor and Network watcher.

Lessons

- Monitor your networks with Azure Monitor
- Monitor your networks with Azure Network Watcher

Lab : Exercise: Monitor a load balancer resource by using Azure Monitor

After completing this module, students will be able to:

- Configure network health alerts and logging by using Azure Monitor
- Create and configure a Connection Monitor instance
- Configure and use Traffic Analytics
- Configure NSG flow logs
- Enable and configure diagnostic logging
- Configure Azure Network Watcher

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:



- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges