AZ-700T00
Designing and Implementing Microsoft Azure Networking Solutions

Duration: 3 Days

Course Overview:

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.

Prerequisites:

Successful Azure Network Engineers start this role with experience in enterprise networking, on-premises or cloud infrastructure and network security.

- 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 Objectives:

Upon completing this course, the learner will be able to meet these overall objectives:

- 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.
- Create and Configure a Virtual Network Gateway
- Create a Virtual WAN by Using Azure Portal
- Design and Implement a Site-To-Site and point-to-site VPN Connection
- Design and implement authentication.
- Design and implement Azure Virtual WAN Resources.
- Design and Implement Expressroute, Expressroute Direct, Expressroute FastPath.
- Design and Implement Azure Load Balancers and Azure Traffic Manager.
- Monitor networks with Azure Monitor.
- Use Network Watcher.
- Design and Implement Azure Application Gateway
- Implement Azure Front Door.
- 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.

Who Should Attend:

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.

Course Outline:

Module 1: 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.

- Azure Virtual Networks
- Public IP Services
- Public and Private DNS
- Cross-VNet Connectivity
- Virtual Network Routing
- 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.

- Site-to-Site VPN Connection
- Point-to-Site VP Connections
- Azure Virtual WAN

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.

- ExpressRoute
- ExpressRoute Direct
- ExpressRoute FastPath
- ExpressRoute Peering

Course Outline (Cont.):

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.

- Content Delivery and Load Balancing
- Azure Load Balancer
- Azure Traffic Manager
- Azure Monitor
- Network Watcher

Module 5: Load Balancing HTTP(S) Traffic in Azure

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

- Azure Application Gateway
- Azure Front Door

Module 6: Design and Implement Network Security

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

- Azure DDoS Protection
- Azure Firewall
- Network Security Groups
- Web Application Firewall 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.

- Define Azure Private Link and Private Endpoints
- Design and Configure Private Endpoints
- Integrate Private Link with DNS & On-Premises Clients
- Create, Configure, and Provide Access to Service Endpoints
- Configure VNET Integration for App Service

Lab Outline:

Labs are designed to assure learners a whole practical experience, through the following practical activities:

- Lab 1: Design and Implement a Virtual Network in Azure
- Lab 2: Configure DNS Settings in Azure
- Lab 3: Connect Virtual Networks with Peering
- Lab 4: Create and Configure a Local Gateway
- Lab 5: Create and Configure ExpressRoute
- Lab 6: Create and Configure a Public Load Balancer to Load Balance VMs Using the Azure Portal
- Lab 7: Create a Traffic Manager Profile Using the Azure Portal
- Lab 8: Create, View, and Manage Metric Alerts in Azure Monitor
- Lab 9: Create a Front Door for a Highly Available Web Application Using the Azure Portal
- Lab 10: Create and Configure an Application Gateway
- Lab 11: Create a Virtual Network with DDoS Protection plan
- Lab 12: Deploy and Configure Azure Firewall
- Lab 13: Create a Web Application Firewall Policy on Azure Front Door
- Lab 14: Restrict Network Access to PaaS Resources with Virtual Network Service Endpoints
- Lab 15: Create an Azure Private Endpoint