

Cloud Expert
Duration: 150 Hrs

Network Fundamentals

- 1.1 Explain the role and function of network components
 - 1.1.a Routers
 - 1.1.b L2 and L3 switches
 - 1.1.c Next-generation firewalls and IPS
 - 1.1.d Access points
 - 1.1.e Controllers (Cisco DNA Center and WLC)
 - 1.1.f Endpoints
 - 1.1.g Servers
- 1.2 Describe characteristics of network topology architectures
 - 1.2.a 2 tier
 - 1.2.b 3 tier
 - 1.2.c Spine-leaf
 - 1.2.d WAN
 - 1.2.e Small office/home office (SOHO)
 - 1.2.f On-premises and cloud
- 1.3 Compare physical interface and cabling types
 - 1.3.a Single-mode fiber, multimode fiber, copper
 - 1.3.b Connections (Ethernet shared media and point-to-point)
 - 1.3.c Concepts of PoE
- 1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- 1.5 Compare TCP to UDP
- 1.6 Configure and verify IPv4 addressing and subnetting
- 1.7 Describe the need for private IPv4 addressing
- 1.8 Configure and verify IPv6 addressing and prefix
- 1.9 Compare IPv6 address types
 - 1.9.a Global unicast
 - 1.9.b Unique local
 - 1.9.c Link local
 - 1.9.d Anycast
 - 1.9.e Multicast
 - 1.9.f Modified EUI 64
- 1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
- 1.11 Describe wireless principles
 - 1.11.a Nonoverlapping Wi-Fi channels
 - 1.11.b SSID
 - 1.11.c RF
 - 1.11.d Encryption
- 1.12 Explain virtualization fundamentals (virtual machines)
- 1.13 Describe switching concepts

- 1.13.a MAC learning and aging
- 1.13.b Frame switching
- 1.13.c Frame flooding
- 1.13.d MAC address table

Network Access

- 2.1 Configure and verify VLANs (normal range) spanning multiple switches
 - 2.1.a Access ports (data and voice)
 - 2.1.b Default VLAN
 - 2.1.c Connectivity
- 2.2 Configure and verify interswitch connectivity
 - 2.2.a Trunk ports
 - 2.2.b 802.1Q
 - 2.2.c Native VLAN
- 2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- 2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
- 2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
 - 2.5.a Root port, root bridge (primary/secondary), and other port names
 - 2.5.b Port states (forwarding/blocking)
 - 2.5.c PortFast benefits
- 2.6 Compare Cisco Wireless Architectures and AP modes
- 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- 2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
- 2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

IP Connectivity

- 3.1 Interpret the components of routing table
 - 3.1.a Routing protocol code
 - 3.1.b Prefix
 - 3.1.c Network mask
 - 3.1.d Next hop
 - 3.1.e Administrative distance
 - 3.1.f Metric
 - 3.1.g Gateway of last resort
- 3.2 Determine how a router makes a forwarding decision by default
 - 3.2.a Longest match
 - 3.2.b Administrative distance
 - 3.2.c Routing protocol metric
- 3.3 Configure and verify IPv4 and IPv6 static routing

- 3.3.a Default route
- 3.3.b Network route
- 3.3.c Host route
- 3.3.d Floating static
- 3.4 Configure and verify single area OSPFv2
 - 3.4.a Neighbor adjacencies
 - 3.4.b Point-to-point
 - 3.4.c Broadcast (DR/BDR selection)
 - 3.4.d Router ID
- 3.5 Describe the purpose of first hop redundancy protocol

IP Services

- 4.1 Configure and verify inside source NAT using static and pools
- 4.2 Configure and verify NTP operating in a client and server mode
- 4.3 Explain the role of DHCP and DNS within the network
- 4.4 Explain the function of SNMP in network operations
- 4.5 Describe the use of syslog features including facilities and levels
- 4.6 Configure and verify DHCP client and relay
- 4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
- 4.8 Configure network devices for remote access using SSH
- 4.9 Describe the capabilities and function of TFTP/FTP in the network

Security Fundamentals

- 5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- 5.2 Describe security program elements (user awareness, training, and physical access control)
- 5.3 Configure device access control using local passwords
- 5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- 5.5 Describe remote access and site-to-site VPNs
- 5.6 Configure and verify access control lists
- 5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- 5.8 Differentiate authentication, authorization, and accounting concepts
- 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
- 5.10 Configure WLAN using WPA2 PSK using the GUI

Automation and Programmability

- 6.1 Explain how automation impacts network management
- 6.2 Compare traditional networks with controller-based networking
- 6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric)
 - 6.3.a Separation of control plane and data plane

6.3.b North-bound and south-bound APIs

6.4 Compare traditional campus device management with Cisco DNA Center enabled device management

6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)

6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible

6.7 Interpret JSON encoded data

Windows Server:

- Active Directory Overview
- Users, Group & Computer Account Creation
- Basics of DNS
- Basics of Virtualization
 - Creating VM's
 - Configuring Network for Virtual Machine
- Basics of Storage
- Basics of PowerShell

MS Azure Administrator:

Module 1: Identity

In this module, you will learn how to secure identities with Azure Active Directory, and implement users and groups.

Lessons

- Azure Active Directory
- Users and Groups
- **Lab** : Manage Azure Active Directory Identities

Module 2: Governance and Compliance

In this module, you will learn about managing your subscriptions and accounts, implementing Azure policies, and using Role-Based Access Control.

Lessons

- Subscriptions and Accounts
- Azure Policy
- Role-based Access Control (RBAC)
- **Lab** : Manage Subscriptions and RBAC
- **Lab** : Manage Governance via Azure Policy

Module 3: Azure Administration

In this module, you will learn about the tools an Azure Administrator uses to manage their infrastructure. This includes the Azure Portal, Cloud Shell, Azure PowerShell, CLI, and Resource Manager Templates. This module includes:

Lessons

- Azure Resource Manager
- Azure Portal and Cloud Shell
- Azure PowerShell and CLI
- ARM Templates
- **Lab** : Manage Azure resources by Using the Azure Portal
- **Lab** : Manage Azure resources by Using ARM Templates
- **Lab** : Manage Azure resources by Using Azure PowerShell
- **Lab** : Manage Azure resources by Using Azure CLI

Module 4: Virtual Networking

In this module, you will learn about basic virtual networking concepts like virtual networks and subnetting, IP addressing, network security groups, Azure Firewall, and Azure DNS.

Lessons

- Virtual Networks
- IP Addressing
- Network Security groups
- Azure Firewall
- Azure DNS
- **Lab** : Implement Virtual Networking

Module 5: Intersite Connectivity

In this module, you will learn about intersite connectivity features including VNet Peering, Virtual Network Gateways, and Site-to-Site Connections.

Lessons

- VNet Peering
- VPN Gateway Connections
- ExpressRoute and Virtual WAN
- **Lab** : Implement Intersite Connectivity

Module 6: Network Traffic Management

In this module, you will learn about network traffic strategies including network routing and service endpoints, Azure Load Balancer, Azure Application Gateway, and Traffic Manager.

Lessons

- Network Routing and Endpoints
- Azure Load Balancer
- Azure Application Gateway
- Traffic Manager
- **Lab** : Implement Traffic Management

Module 7: Azure Storage

In this module, you will learn about basic storage features including storage accounts, blob storage, Azure files and File Sync, storage security, and storage tools.

Lessons

- Storage Accounts
- Blob Storage
- Storage Security
- Azure Files and File Sync
- Managing Storage
- **Lab** : Manage Azure storage

Module 8: Azure Virtual Machines

In this module, you will learn about Azure virtual machines including planning, creating, availability and extensions.

Lessons

- Virtual Machine Planning
- Creating Virtual Machines
- Virtual Machine Availability
- Virtual Machine Extensions
- **Lab** : Manage virtual machines

Module 9: Serverless Computing

In this module, you will learn administer serverless computing features like Azure App Service, Azure Container Instances, and Kubernetes.

Lessons

- Azure App Service Plans
- Azure App Service

- Container Services
- Azure Kubernetes Service
- **Lab** : Implement Web Apps
- **Lab** : Implement Azure Container Instances
- **Lab** : Implement Azure Kubernetes Service

Module 10: Data Protection

In this module, you will learn about backing up files and folders, and virtual machine backups.

Lessons

- File and Folder Backups
- Virtual Machine Backups
- **Lab** : Implement Data Protection

Module 11: Monitoring

In this module, you will learn about monitoring your Azure infrastructure including Azure Monitor, alerting, and log analytics.

Lessons

- Azure Monitor
- Azure Alerts
- Log Analytics
- Network Watcher
- **Lab**: Implement Monitoring

MS Azure Security:

Module 1: Identity and Access

Lessons

- Configure Azure Active Directory for Azure workloads and subscriptions
- Configure Azure AD Privileged Identity Management
- Configure security for an Azure subscription

Module 2: Platform Protection

Lessons

- Understand cloud security
- Build a network

- Secure network
- Implement host security
- Implement platform security
- Implement subscription security

Module 3: Security Operations

Lessons

- Configure security services
- Configure security policies by using Azure Security Center
- Manage security alerts
- Respond to and remediate security issues
- Create security baselines

Module 4: Data and applications

Lessons

- Configure security policies to manage data
- Configure security for data infrastructure
- Configure encryption for data at rest
- Understand application security
- Implement security for application lifecycle
- Secure applications
- Configure and manage Azure Key Vault

AWS:

Amazon Web Services (AWS):

- Introduction to the AWS Product
- Amazon Elastic Compute Cloud(EC2)
- Amazon Simple Storage Service (S3)
- Elastic Block Storage (EBS)
- Elastic Load Balancing (ELB)
- Amazon Relational Database Service (RDS)
- Amazon Virtual Private Cloud (VPC)
- Amazon DynamoDB
- Auto Scaling
- Amazon ElastiCache

Elastic Compute Cloud Essentials:

- Introduction to the AWS Management Console
- Regions and Availability Zones - How to choose the right one
- Amazon Machine Images (AMI)
- Setting up security
- Finding the right AMI
- Launching an instance - How to choose the right instance type
- Security via Key Pairs
- Working with the Security Group
- Assigning Elastic IPs
- Logging into the instance

EC2 Instances:

- Deciding between On-demand instances, Spot instances, Reserved instances
- EC2 Reserved Instance Marketplace

Working with AMIs :

- Choosing the right AMI
- Creating your own AMI
- Deciding what goes into an AMI

Elastic Block Store (EBS)

- Creating and deleting volumes
- Attaching and detaching volumes
- Mounting and Unmounting the attached volume
- Creating snapshots

Simple Storage Service (S3)

- Creating and deleting buckets
- Adding objects to buckets
- Getting objects
- Deleting objects

Relational Database Service (RDS):

- Selecting the Engine
- Configuring the Database Engine
- Creating your Database
- Setting up automatic backups
- Authorizing access to the DB via DB Security Groups

Amazon Virtual Private Cloud (VPC)

- Amazon Virtual Private Cloud
- Networking
- Subnets
- Security Group

Cloudwatch :

- Debugging cloud related issues
- Monitoring the AWS Service Health Dashboard
- Monitoring with Cloudwatch
- Getting statistics for a specific EC2 instance
- Getting aggregated statistics
- Metrics for other AWS Services and related namespaces
- Setting up notifications
- Using command-line tools

Elastichache :

- Advantages of ElastiCache
- Understanding various terminologies IAM Best Practices
- Cache Cluster and Cache Node

Other AWS Services :

- Cache Security Groups Elastic Beanstalk
- Cache Parameter Groups Simple Notification Service
- Cache Node Types Simple Email Service (SES)
- Auto-discovery of nodes Simple Queue Service (SQS)