Module: 13 Networking With Windows Server

1) The Domain Name System (DNS) is a service that translates domain names into IP addresses, allowing users to access websites and other internet resources.
2) A recursive DNS lookup is where one DNS server communicates with several other DNS servers to hunt down an IP address and return it to the client.
3) A forward lookup zone is a part of a Domain Name System (DNS) server that maps host names to IP addresses.
4) A reverse lookup zone is a Domain Name System (DNS) zone that translates IP addresses into domain names.

- The resource type for a reverse lookup zone is Pointer (PTR) records, which contain the IP address in reverse order, followed by the associated domain name.

5) A conditional forwarder is a DNS server that forwards DNS queries for specific domain names to other DNS servers, conditional forwarding is a method for resolving DNS queries for external domains.
6) Primary zones are read-write copies of zone data and hosted by primary DNS servers.

- Secondary zones contain read-only copies of zone data and are used for load balancing and fault tolerance.
- Stub zones contain only resource records for the domain's name servers and are used for faster name resolution.

7) Active Directory-integrated zone is a DNS zone that is stored in an Active Directory database, instead of on a computer.
- They are only available on domain controllers that have the DNS Server role installed.

8) The main authoritative server that generates zone files and handles DNS queries for a domain.
- An authoritative server that receives zone files from the primary server and stores them in a cache. Secondary servers can answer queries for a domain, but they can't modify the zone files.
- A server that performs queries and stores the results, but doesn't use zone files.

9) DNS aging and scavenging is a service that automatically removes stale resource records from a DNS database to maintain a dynamic DNS environment.

10) A mail exchanger record (MX record) is a Domain Name System (DNS) record that directs emails to specific mail servers.

11) A Dynamic Host Configuration Protocol (DHCP) server assigns IP addresses and other network configuration parameters to devices on a network, allowing them to communicate with each other and the internet.
12) The DORA process is a set of four steps that devices go through to obtain an IP address and connect to a network using the Dynamic Host Configuration Protocol (DHCP).
13) The purpose of authorizing the DHCP server is to ensure that only authorized DHCP servers can provide IP addresses to clients on the network.
14) A DHCP Scope is a pool of IP Addresses on a specific subnet that can be leased by the DHCP Server.

- Each subnet can only contain one scope with a continuous range of IP Addresses.
- This means you cannot create a scope ranging from 192.168. 0.1 through 192.168.

15) DHCP reservation, also known as IP reservation or Reserved IP, is a feature that allows a network administrator to assign a specific IP address to a device on a network.
16) A DHCP relay agent is a router or host that forwards DHCP messages between DHCP clients and DHCP servers that are not on the same subnet or local network.

17) The Ipconfig command is a command-line utility that displays and manages a computer's IP address and network settings.

18) IP address management (IPAM) is a method for planning, tracking, and managing IP address space on a network.

19) Dedicated servers offer superior performance, processing power, and storage capacity.

20) To create an access policy

- In Server Manager, click IPAM.
- The IPAM client console appears.
- In the navigation pane.
- Click Access control.
- In the lower navigation pane.
- Right-click Access Policies.
- Then click Add Access Policy.

21) IPAM monitors domain controllers and NPS servers for IP address tracking purposes.

- In addition to monitoring functions, several DHCP server and scope properties can be configured from the IPAM console.
- Zone status monitoring and a limited set of configuration functions are also available for DNS servers.

22) A VPN is a service that encrypts data and masks IP addresses to create a private network connection over the internet.

23) 8 Types of VPN

- **Remote Access VPN**
- **Site to Site VPN**
- **Cloud VPN**
- **Mobile VPN**
- **SSL VPN**
- **PPTP (Point-to-Point Tunneling Protocol) VPN**
- **L2TP (Layer 2 Tunneling Protocol) VPN**
- **OpenVPN**

24) A tunneling protocol is one that encloses in its datagram another complete data packet that uses a different communications protocol.

25) An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities.

26) Routing is the process of selecting a path for data packets to travel from their origin to their destination within or between networks.

- It can apply to any type of network, including the internet, telephone networks, and public transportation.

27) A RADIUS server is a central server that authenticates and authorizes users who access a network remotely.

- It uses the User Datagram Protocol (UDP) and is usually a daemon application that runs on a Windows or UNIX machine.

28) Authentication, authorization and accounting (AAA) is a security framework for controlling and tracking user access within a computer network.

- AAA intelligently controls access to computer resources, enforces policies, audits usage and provides the information necessary to bill for services.

29) It receives authentication requests from RADIUS clients, such as routers, firewalls, or VPNs, verifies the credentials of the user, and returns an authorization decision to the client.

30) RADIUS uses UDP as the transport protocol.

- It uses UDP port 1812 for authentication and UDP port 1813 for accounting.

31) Network Policy Server (NPS) is a Microsoft service that allows users to create and enforce network access policies for their organization.

- NPS is a RADIUS (Remote Authentication Dial-in User Service) server and proxy that can perform the following functions.

32) An IP address is a numerical or alphanumeric code that allows devices to send and receive data over the internet. There are several types of IP addresses.

- IPv4
- IPv6

- Public IP address
- Static IP address
- Dynamic IP address
- Private IP address

33) 5 Class of ip addresses

- Class A
- Class B
- Class C
- Class D
- Class E

34) Public IP address

- A unique IP address that is visible to everyone on the internet. It is assigned by an ISP and is used to connect devices to the internet.
- Private IP address
- An IP address that is used within a private network to connect devices securely to each other. It is assigned to a device by a router within the network.

35) Static IP address

- A manual IP address setting for a computer

- DHCP
- A network management protocol that assigns IP addresses to devices on a network using a centralized server.
- APIPA
- A feature in some operating systems that automatically assigns IP addresses to devices when a DHCP server is unavailable.

36) An IPv6 address is a 128-bit alphanumeric value that identifies a device in an Internet Protocol Version 6 (IPv6) network.

37) The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes, default route, local segment MTU, and other configuration data required to operate in an IPv6 network.

38) Network Address Translation (NAT) is a technique that allows private IP addresses to be translated to public IP addresses before they are sent to the internet.

39) The gateway address can really be any unique address within the subnet itself, but most network

administrators designate the first number of the subnet as the default gateway. Therefore, 192.168. 99.1 would be the default subnet gateway of our source device given the fact that we have a 255.255. 255.0 subnet mask.

40) A loopback address is an internal IP address that routes data packets back to the local system. It's also known as localhost.

41) 3 type of ipv6 address

- Multicast
- Anycast
- Unicast

42) IPv6 Tunneling allows hosts in one private IP network to communicate with hosts in another private IP network by providing a tunnel between two routers across the Internet.

43) A distributed file system (DFS) is a file system that enables clients to access file storage from multiple hosts through a computer network as if the user was accessing local storage.

44) Distributed File System (DFS) Namespace (DFSN) and Distributed File System Replication (DFSR) are

two components of DFS that work together to manage file access and sharing.

45) A folder target is a shared folder's Universal Naming Convention (UNC) path or another namespace that is associated with a folder in a namespace.

46) SDN stands for Software-Defined Networking, a network architecture that uses software to manage and control a network.

47) SCVMM enables you to configure and manage your virtualization host, networking, and storage resources to create and deploy virtual machines and services to private clouds that you have created.