Windows Server Assignment: **Windows Networking Services**

1. Discuss the role of Windows Firewall in Windows Server and how to configure it.

Ans: Windows Firewall in Windows Server protects the system by filtering incoming and outgoing network traffic based on defined security rules. It helps block unauthorized access and allows permitted communication to and from the server.

Role of Windows Firewall in Windows Server

1. **Traffic Filtering:** Controls network traffic based on IP address, port, and protocol.
2. **Protection:** Prevents unauthorized users and malware from accessing network resources.
3. **Application Control:** Allows or blocks programs based on predefined or custom rules.
4. **Integration:** Works with IPsec for secure data transmission and authentication.
5. **Profile-based Rules:** Supports Domain, Private, and Public profiles for different network environments.
6. **Centralized Management:** Can be managed through Group Policy, PowerShell, or Windows Admin Center.

Steps to Configure

1. **Open Windows Firewall:**
    - Go to **Control Panel → System and Security → Windows Defender Firewall**.
2. **Check Firewall Status:**
    - Select **"Turn Windows Defender Firewall on or off"** to enable or disable it for Domain, Private, and Public networks.
3. **Allow an App or Feature:**
    - Click **"Allow an app or feature through Windows Defender Firewall."**
    - Select the application (e.g., File and Printer Sharing, Remote Desktop).
    - Check the appropriate network types and click **OK**.
4. **Create Inbound/Outbound Rules:**
    - Go to **Advanced Settings → Windows Defender Firewall with Advanced Security**.
    - Choose **Inbound Rules → New Rule**.
    - Select **Port**, **Program**, or **Custom**.
    - Define protocol (TCP/UDP), port number, and action (Allow/Block).
    - Apply the rule to the desired profiles and give it a name.

5. **Verify Configuration:**
    - Use the command:
    - netsh advfirewall show allprofiles
    - To check active rules:

Get-NetFirewallRule | Where-Object {$_.Enabled -eq "True"}

2. What is Network Address Translation (NAT) in Windows Server, and how do you configure it?

Ans: Network Address Translation (NAT)** in Windows Server allows multiple internal (private) network devices to access external (public) networks using a single public IP address. It hides internal IPs, conserves public IPs, and enhances network security.

Role of NAT

1. **IP Address Conservation:** Converts private IPs to a single public IP for internet access.
2. **Security:** Masks internal network structure from external users.
3. **Routing Support:** Enables communication between internal and external networks.
4. **Traffic Management:** Controls how traffic is translated and forwarded.

Types of NAT

1. **Static NAT:** One-to-one mapping between private and public IPs.
2. **Dynamic NAT:** Maps private IPs to available public IPs dynamically.
3. **PAT (Port Address Translation):** Many private IPs share one public IP using different ports (most common in Windows Server).

Steps to Configure NAT in Windows Server (Using Routing and Remote Access – RRAS)

1. Install RRAS Role

- Open **Server Manager → Manage → Add Roles and Features**.
- Select **Remote Access → Routing**.
- Complete the installation.

2. Configure NAT

- Open **Routing and Remote Access** console (rrasmgmt.msc).
- Right-click the server name → select **Configure and Enable Routing and Remote Access**.
- Choose **Network Address Translation (NAT)** setup option.

- Select the network interface connected to the internet (public).
- Mark it as **Public interface connected to the Internet**.
- Check **Enable NAT on this interface**.
- Select the private/internal network interface and mark it as **Private interface connected to private network**.

3. Start the Service

- After configuration, right-click the server in RRAS and click **Start**.

4. Explain the concept of Dynamic Host Configuration Protocol (DHCP) and how to configure it in Windows Server 2016.

Ans:

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and related network settings to client devices on a network. It reduces manual configuration errors and simplifies IP management.

Concept of DHCP

DHCP operates on a **client-server model**. The **DHCP Server** dynamically allocates IP addresses and network configuration parameters to **DHCP Clients**.

Key Functions

1. **Automatic IP Assignment:** Allocates IPs from a predefined range (scope).
2. **Centralized Management:** Manages all IP configurations from one server.
3. **Lease Duration:** Assigns temporary IPs for a specific time (lease).
4. **Prevents Conflicts:** Ensures no two devices get the same IP.
5. **Provides Additional Info:** Such as DNS server, default gateway, subnet mask, etc.

DHCP Process (DORA)

1. **Discover:** Client broadcasts a DHCP Discover message.
2. **Offer:** DHCP Server offers an available IP.
3. **Request:** Client requests the offered IP.
4. **Acknowledge:** Server confirms and allocates the IP lease.

Steps to Configure DHCP in Windows Server 2016

1. Install DHCP Role

- Open **Server Manager → Manage → Add Roles and Features**.

- Choose **Role-based or feature-based installation**.
- Select **DHCP Server** → Install.
- After installation, click **Complete DHCP configuration** in Server Manager.
- Authorize the server in Active Directory (if domain-joined).

2. Open DHCP Management Console

- Go to **Tools → DHCP** in Server Manager.

3. Create a New Scope

1. Right-click **IPv4 → New Scope**.
2. Enter:
    - **Name:** e.g., *Office LAN*
    - **IP Range:** e.g., *192.168.1.10 – 192.168.1.200*
    - **Subnet Mask:** *255.255.255.0*
    - **Exclusions (optional):** IPs reserved for printers, servers, etc.
    - **Lease Duration:** e.g., *8 days*
3. Add **Router (Gateway)**, **DNS Server**, and **WINS Server** if needed.
4. Activate the scope.

4. Authorize and Start DHCP Service

- Right-click the server in DHCP console → **Authorize**.

4.Describe the process of configuring DNS (Domain Name System) in Windows Server.

Ans:

To configure DNS in Windows Server so that the domain **kishan.com** resolves to **10.0.0.1**, you must install the DNS role, create a forward lookup zone for kishan.com, and add an A record mapping the name to the IP.

Steps to Configure DNS for kishan.com → 10.0.0.1

1. Install the DNS Role

1. Open **Server Manager → Manage → Add Roles and Features**.
2. Select **Role-based or feature-based installation**.
3. Choose your server and check **DNS Server**.
4. Click **Install**.

5. After installation, open **Tools → DNS**.

2. Create a Forward Lookup Zone

1. In **DNS Manager**, expand your server name.
2. Right-click **Forward Lookup Zones → New Zone**.
3. Select **Primary Zone** → click **Next**.
4. Choose **Store the zone in Active Directory** (if applicable).
5. Enter **kishan.com** as the **Zone Name**.
6. Choose **Allow only secure dynamic updates** (recommended for AD).
7. Finish the wizard.

This zone will handle all DNS records for the kishan.com domain.

3. Add an A Record

1. Under **Forward Lookup Zones → kishan.com**, right-click → **New Host (A or AAAA)**.
2. Leave the **Name** field blank to represent the root of kishan.com.
3. In **IP address**, enter **10.0.0.1**.
4. Click **Add Host**.
5. (Optional) Add a record for www.kishan.com pointing to the same IP if you want browser access via "www".

5. Verify the Configuration

6. What is Server Manager, and how do you use it to manage servers in Windows Server?

Ans: **Server Manager** in Windows Server is a centralized management console that allows administrators to configure, monitor, and manage local and remote servers from a single interface.

Purpose of Server Manager

1. **Centralized Management:** Manage multiple servers without logging into each.
2. **Role and Feature Management:** Install, configure, or remove server roles and features.
3. **Performance Monitoring:** View alerts, performance data, and events.

4. **Remote Administration:** Add and manage remote servers in the same domain or trusted domains.
5. **Simplified Setup:** Provides post-deployment configuration wizards.

Key Features

- **Dashboard:** Overview of roles, features, and server health.
- **Local Server Tab:** View and configure system properties (e.g., computer name, network, updates).
- **All Servers Tab:** Consolidates management of multiple servers.
- **Role-Based Views:** Manage services like DNS, DHCP, and File Services directly.
- **Event Viewer Integration:** Displays recent events and alerts.

Steps to Use Server Manager

1. Open Server Manager

- Automatically opens at login, or open manually via:
- Start → Server Manager

2. Add Roles and Features

1. Click **Manage → Add Roles and Features**.
2. Choose **Role-based or feature-based installation**.
3. Select the target server.
4. Choose roles such as **DNS**, **DHCP**, **File Server**, etc.
5. Complete installation through the wizard.

3. Add Remote Servers

1. Click **Manage → Add Servers**.
2. Search by **Active Directory**, **DNS**, or **IP address**.
3. Add selected servers to the **Server Manager pool** for remote management.

4. Manage Server Roles

- Select a server from the list.
- Expand its role (e.g., DNS, File Services).
- Perform actions like starting/stopping services or opening management consoles.

5. Monitor Server Health

- View performance data, events, and alerts under each server tile.

- Filter by severity to focus on critical issues.

6. Discuss the role of Remote Desktop Services (RDS) in Windows Server 2016 or 2019 and how to configure it.

Ans: **Remote Desktop Services (RDS)** in Windows Server 2016/2019 allows users to access desktops and applications hosted on a server from any device. It supports centralized management, remote app delivery, and secure multi-user access.

Role of Remote Desktop Services (RDS)

1. **Remote Access:** Lets multiple users log in to a server remotely via Remote Desktop Protocol (RDP).
2. **Centralized Application Hosting:** Users can run applications installed on the server without installing them locally.
3. **Resource Optimization:** Reduces client hardware requirements; processing happens on the server.
4. **Security:** Uses encryption and access policies to secure sessions.
5. **Scalability:** Supports multiple concurrent sessions and can be expanded using additional session hosts.
6. **Management:** Integrates with Active Directory and Group Policy for user control.

Key RDS Components

1. **RD Session Host (RDSH):** Hosts Windows apps and desktops for users.
2. **RD Licensing:** Manages and issues Remote Desktop Client Access Licenses (CALs).
3. **RD Connection Broker:** Balances sessions between servers and reconnects users to existing sessions.
4. **RD Web Access:** Provides a web-based portal for users to access applications.
5. **RD Gateway:** Allows secure remote connections over HTTPS (internet access).

Steps to Configure RDS in Windows Server 2016/2019

1. Install RDS Role

1. Open **Server Manager → Manage → Add Roles and Features**.
2. Choose **Role-based or feature-based installation**.
3. Under **Server Roles**, check **Remote Desktop Services**.

4. Expand and select:
    - **Remote Desktop Licensing**
    - **Remote Desktop Session Host**
    - (Optional) **Remote Desktop Web Access**
5. Complete installation and restart if required.

2. Configure RD Licensing

1. In **Server Manager → Tools → Remote Desktop Licensing Manager**.
2. Right-click your server → **Activate Server**.
3. Use **Automatic connection** or **Web browser** activation.
4. Install purchased **RDS CALs** using the wizard.

3. Enable Remote Desktop Access

1. Go to **Server Manager → Local Server**.
2. Click **Remote Desktop: Disabled → Enable Remote Desktop**.
3. Allow connections from any version of RDP or only secure ones.

4. Configure User Access

1. Right-click **This PC → Properties → Remote settings**.
2. Under **Remote Desktop**, click **Select Users**.
3. Add users or groups allowed to connect.

5. Connect from a Client Device

On a Windows client:

1. Open **Remote Desktop Connection (mstsc.exe)**.
2. Enter the server's IP or hostname (e.g., 10.0.0.1 or kishan.com).
3. Log in with valid credentials.