Assignment : Windows Server

**Submitted By :- Purv Patel**

**Module 13: Networking with Windows Server**

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

> Windows Firewall in Windows Server: Role & Configuration

Role of Windows Firewall

Windows Firewall secures Windows Server by controlling network traffic, preventing unauthorized access, and blocking malicious activity. It filters inbound and outbound traffic based on rules, protecting the server across different network profiles (Domain, Private, Public).

Configuration Steps

1. Open Windows Firewall

Go to Server Manager → Tools → Windows Defender Firewall with Advanced Security

Or run wf.msc

2. Configure Firewall Rules

Inbound Rules: Control incoming traffic

Outbound Rules: Control outgoing traffic

Define rules based on ports, programs, or protocols

3. Enable/Disable Firewall

Open Windows Defender Firewall → Click Turn Windows Defender Firewall on or off

4. Allow an App Through Firewall

Go to Allow an app through Windows Defender Firewall → Choose app & network profile

5. Manage via PowerShell

Check status: Get-NetFirewallProfile

Enable Firewall: Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True

Allow Port 80:

New-NetFirewallRule -DisplayName "Allow HTTP" -Direction Inbound -Protocol TCP -LocalPort 80 -Action Allow

Reset Firewall to Default

GUI: Restore Defaults in Firewall settings

PowerShell: netsh advfirewall reset

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

> Network Address Translation (NAT) in Windows Server:-

NAT allows multiple devices on a private network to access external networks (e.g., the internet) using a single public IP. It helps with internet sharing, IP conservation, and security.

How to Configure NAT

1. Install Remote Access Role

Go to Server Manager → Add Roles and Features

Select Remote Access → Routing → Install

2. Enable NAT in Routing and Remote Access (RRAS)

Open Routing and Remote Access

Right-click server → Configure and Enable Routing and Remote Access

Choose NAT → Select public network interface → Finish

3. Configure NAT Interfaces

Add Public Interface → Enable NAT

Add Private Interface → Connect to internal network

4. Enable Port Forwarding (Optional)

In NAT Properties, add port forwarding rules for internal services

PowerShell Commands for NAT

Install NAT Role

Install-WindowsFeature -Name Routing -IncludeManagementTools

Create NAT Rule

New-NetNat -Name "NATNetwork" -InternalIPInterfaceAddressPrefix "192.168.1.0/24"

View NAT Configuration

Get-NetNat

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

> **Dynamic Host Configuration Protocol (DHCP) in Windows Server 2016**

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that **automates IP address assignment** to devices on a network. Instead of manually configuring IP settings, DHCP dynamically provides devices with:

**IP Addresses**

**Subnet Masks**

**Default Gateways**

**DNS Server Addresses**

**Benefits of DHCP**

✅ **Automates IP Assignment** – Reduces manual configuration errors  
✅ **Efficient IP Management** – Prevents IP conflicts  
✅ **Centralized Control** – Manages IP leases from a single server  
✅ **Scalability** – Ideal for large networks

**How to Configure DHCP in Windows Server 2016**

**1. Install the DHCP Server Role**

Open **Server Manager** → Click **Manage** → **Add Roles and Features**

Select **Role-based or feature-based installation** → Click **Next**

Choose the **server** → Click **Next**

Select **DHCP Server** → Click **Next** → Click **Install**

After installation, click **Complete DHCP Configuration**

Authorize the DHCP server (if part of an Active Directory domain)

**2. Configure a DHCP Scope**

A **scope** defines a range of IP addresses for client devices.

Open **DHCP Manager** (dhcpmgmt.msc)

Expand the **server name** → Right-click **IPv4** → **New Scope**

Click **Next** → Enter a **Scope Name**

Define the **IP address range** (e.g., 192.168.1.100 – 192.168.1.200)

Enter **Subnet Mask** (e.g., 255.255.255.0)

**Exclude IPs** (optional) to prevent assigning certain addresses

Set the **Lease Duration** (default: 8 days)

Configure DHCP Options:

**Default Gateway** (e.g., 192.168.1.1)

**DNS Server** (e.g., 8.8.8.8)

**WINS Server** (if applicable)

Activate the **Scope**

**3. Authorize and Start DHCP Service**

If the server is part of **Active Directory**, DHCP must be **authorized**:

Open **DHCP Manager** → Right-click the server → **Authorize**

Start the **DHCP Service**:

Restart-Service dhcpserver

**4. Verify DHCP Functionality**

On a client PC, open **Command Prompt** and type:

ipconfig /release

ipconfig /renew

The client should receive an IP from the DHCP server

**Managing DHCP via PowerShell**

**Install DHCP Role**

Install-WindowsFeature -Name DHCP -IncludeManagementTools

**Add a DHCP Scope**

Add-DhcpServerv4Scope -Name "OfficeLAN" -StartRange 192.168.1.100 -EndRange 192.168.1.200 -SubnetMask 255.255.255.0 -State Active

**Set Default Gateway Option**

Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -OptionId 3 -Value 192.168.1.1

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

> **Configuring DNS in Windows Server (Short Guide)**

**What is DNS?**

DNS (Domain Name System) converts **domain names** (e.g., example.com) into **IP addresses** (e.g., 192.168.1.1), enabling efficient network communication.

**Steps to Configure DNS**

**1. Install the DNS Server Role**

Open **Server Manager** → **Add Roles and Features**

Select **DNS Server** → **Install**

Open **DNS Manager** (dnsmgmt.msc)

**2. Create a Forward Lookup Zone** (Resolves domain names to IPs)

Open **DNS Manager** → Right-click **Forward Lookup Zones** → **New Zone**

Select **Primary Zone** → Enter the **domain name** (e.g., example.com)

Enable **Dynamic Updates** → **Finish**

**3. Create a Reverse Lookup Zone (Optional)** (Resolves IPs to domain names)

Right-click **Reverse Lookup Zones** → **New Zone**

Enter the **network ID** (e.g., 192.168.1) → Enable **Dynamic Updates**

**4. Add DNS Records**

**A Record (Host)**: Maps a hostname to an IP

Right-click zone → **New Host (A)** → Enter **hostname** & **IP**

**CNAME (Alias) Record**: Maps an alias to an existing domain

**5. Configure Forwarders (Optional, for external queries)**

Right-click **DNS Server** → **Properties** → **Forwarders**

Add **Google DNS (8.8.8.8)** or ISP DNS

**6. Test DNS Configuration**

**Check DNS resolution:** nslookup example.com

**Flush DNS cache (if needed):** ipconfig /flushdns

**PowerShell Commands for DNS**

**Install DNS Role:**

Install-WindowsFeature -Name DNS -IncludeManagementTools

**Create a Forward Lookup Zone:**

Add-DnsServerPrimaryZone -Name "example.com" -ZoneFile "example.com.dns"

**Add an A Record:**

Add-DnsServerResourceRecordA -ZoneName "example.com" -Name "www" -IPv4Address "192.168.1.10"

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

## > **What is Server Manager in Windows Server?**

### **Overview**

Server Manager is a centralized **management console** in Windows Server that allows administrators to **install roles and features, monitor system performance, and manage multiple servers** remotely.

### **Key Functions of Server Manager**

✅ **Manage Local & Remote Servers** – Add and control multiple servers  
✅ **Install & Configure Roles/Features** – Deploy services like **DHCP, DNS, AD DS**  
✅ **Monitor Server Performance** – View logs, alerts, and events  
✅ **Simplified Administration** – Single dashboard for multiple servers

## **How to Use Server Manager**

### **1. Open Server Manager**

* Click **Start** → **Server Manager**
* Or run servermanager.exe

### **2. Add and Manage Remote Servers**

* Click **Manage** → **Add Servers**
* Select servers by **Active Directory, DNS, or IP Address**

### **3. Install Roles and Features**

* Click **Manage** → **Add Roles and Features**
* Choose **Role-based or Feature-based installation**
* Select the **server** and install services like **DNS, DHCP, IIS**

### **4. Monitor Server Health**

* View **Dashboard** for alerts and event logs
* Click **Local Server** to check status, updates, and firewall settings

### **5. Manage Services & Performance**

* Click **Tools** → Open management consoles (e.g., Event Viewer, Task Scheduler)
* Check **Performance Monitor** for CPU, memory, and network usage

## **Managing Server Manager via PowerShell**

* **Install a Role (e.g., DHCP)**
* Install-WindowsFeature -Name DHCP -IncludeManagementTools
* **List Installed Roles & Features**
* Get-WindowsFeature
* **Check Server Health**
* Get-EventLog -LogName System -Newest 10

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

## > **Remote Desktop Services (RDS) in Windows Server 2016/2019**

### **What is RDS?**

Remote Desktop Services (RDS) allows users to remotely access applications, desktops, and resources hosted on a Windows Server. It enables centralized application management and secure remote access for users.

### **Key Components of RDS**

✅ **Remote Desktop Session Host (RDSH)** – Hosts remote applications and desktops  
✅ **Remote Desktop Connection Broker (RDCB)** – Manages user sessions  
✅ **Remote Desktop Gateway (RDG)** – Allows secure access over the internet  
✅ **Remote Desktop Licensing (RDL)** – Manages RDS client access licenses (CALs)  
✅ **Remote Desktop Web Access (RDWA)** – Provides a web portal for remote access

## **How to Configure RDS in Windows Server 2016/2019**

### **1. Install the RDS Role**

1. Open **Server Manager** → Click **Manage** → **Add Roles and Features**
2. Choose **Remote Desktop Services Installation** → Click **Next**
3. Select **Standard Deployment** → Choose the **server**
4. Select **Roles to Install** (e.g., RDSH, RDCB, RDWA) → Click **Next**
5. Confirm installation and wait for completion

### **2. Configure RDS Deployment**

1. In **Server Manager**, go to **Remote Desktop Services**
2. Click **Overview** → Select **Add RD Licensing**
3. Right-click **RD Connection Broker** → Configure high availability (if needed)
4. Assign **RDS Licensing Mode** (Per User/Per Device)

### **3. Publish RemoteApps (Optional)**

1. Open **Server Manager** → Go to **Remote Desktop Services**
2. Click **Collections** → **Create Session Collection**
3. Add **RemoteApps** to allow users to access applications remotely

### **4. Configure RD Gateway (Optional, for Internet Access)**

1. Open **RD Gateway Manager** → Create a new **Gateway Server**
2. Configure SSL certificates for **secure remote access**

### **5. Test RDS Configuration**

* Use **Remote Desktop Connection (mstsc.exe)** to connect
* Open a web browser and access **RD Web Access** (https://server-name/RDWeb)

## **Managing RDS via PowerShell**

* **Install RDS Role**
* Install-WindowsFeature -Name RDS-RD-Server -IncludeManagementTools
* **Set RDS Licensing Mode**
* Set-RDLicenseConfiguration -Mode PerUser -LicenseServer "RDS-Server"
* **Publish RemoteApps**
* New-RDRemoteApp -CollectionName "RemoteApps" -DisplayName "Notepad" -FilePath "C:\Windows\System32\notepad.exe"