

**Hardware Networking**

**Networking with Windows Server**

**SUBMITTED TO**

**KAMLESH SHUKLA SIR**

**SUBMITTED BY**

**MANAV BANDHANIA**

**1. Role of Windows Firewall in Windows Server and How to Configure It**

Windows Firewall in Windows Server is a security feature that helps protect the server from unauthorized access and cyber threats. It filters incoming and outgoing traffic based on predefined security rules, preventing malicious activities while allowing necessary communication.

**Role of Windows Firewall in Windows Server:**

* **Traffic Filtering:** Blocks or allows network traffic based on rules.
* **Enhanced Security:** Protects against unauthorized access, malware, and cyber threats.
* **Integration with Group Policy:** Enables centralized management of firewall settings.
* **Logging and Monitoring:** Keeps records of blocked or allowed traffic for analysis.
* **Application-Specific Rules:** Allows or denies traffic for specific applications.

**How to Configure Windows Firewall in Windows Server:**

1. **Open Windows Firewall:**
   * Press **Win + R**, type wf.msc, and press **Enter**.
2. **Create New Inbound or Outbound Rules:**
   * Click on **Inbound Rules** (for incoming traffic) or **Outbound Rules** (for outgoing traffic).
   * Select **New Rule...** on the right panel.
3. **Choose Rule Type:**
   * Select **Port, Program, Predefined, or Custom** based on requirement.
4. **Define Rule Conditions:**
   * Specify **protocols and ports** or the specific application to allow or block.
5. **Set Action:**
   * Choose **Allow the connection** or **Block the connection**.
6. **Apply Rule to Network Profiles:**
   * Select **Domain, Private, or Public** networks based on your security needs.
7. **Name the Rule and Finish:**
   * Give a meaningful name and click **Finish** to apply.

**2. Network Address Translation (NAT) in Windows Server and How to Configure It**

**Network Address Translation (NAT)** allows multiple devices on a private network to share a single public IP address to access external networks, typically the internet. NAT acts as an intermediary between private and public networks, enhancing security and reducing the need for multiple public IPs.

**Types of NAT:**

* **Static NAT:** Maps a single private IP to a single public IP.
* **Dynamic NAT:** Maps private IPs to public IPs dynamically from a pool.
* **PAT (Port Address Translation):** Maps multiple private IPs to a single public IP using different ports.

**How to Configure NAT in Windows Server:**

1. **Install Remote Access Role:**
   * Open **Server Manager** → Click **Manage** → Select **Add Roles and Features**.
   * Choose **Remote Access** and install **Routing and Remote Access (RRAS)**.
2. **Enable and Configure RRAS:**
   * Open **RRAS Console** (rrasmgmt.msc).
   * Right-click on the server name → Click **Configure and Enable Routing and Remote Access**.
   * Choose **NAT (Network Address Translation)**.
3. **Configure NAT Interface:**
   * Select the interface that connects to the internet and enable NAT.
   * Add an internal network interface for local devices.
4. **Enable NAT Services:**
   * Expand **IPv4** → Right-click **NAT** → Click **New Interface**.
   * Select the external (internet-facing) interface and enable NAT.
5. **Apply and Restart RRAS:**
   * Save the settings and restart **Routing and Remote Access Service**.

**3. Dynamic Host Configuration Protocol (DHCP) and How to Configure It in Windows Server 2016**

**Dynamic Host Configuration Protocol (DHCP)** automatically assigns IP addresses and other network configurations (subnet mask, default gateway, DNS) to devices on a network.

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

1. **Install DHCP Role:**
   * Open **Server Manager** → Click **Manage** → Select **Add Roles and Features**.
   * Choose **DHCP Server** and complete the installation.
2. **Authorize the DHCP Server:**
   * Open **DHCP Console (dhcpmgmt.msc)**.
   * Right-click the server → Click **Authorize**.
3. **Create a New DHCP Scope:**
   * Expand **IPv4** → Right-click **New Scope**.
   * Define **Scope Name**, **IP Range**, **Subnet Mask**, and **Exclusion Range**.
4. **Set Lease Duration:**
   * Choose how long a client can use an assigned IP before renewal.
5. **Configure Additional Options:**
   * Add **Default Gateway**, **DNS Servers**, and **WINS Servers**.
6. **Activate the Scope:**
   * Right-click the new scope and select **Activate**.

**4. Configuring DNS (Domain Name System) in Windows Server**

**DNS (Domain Name System)** resolves human-readable domain names (e.g., google.com) to IP addresses.

**How to Configure DNS in Windows Server:**

1. **Install the DNS Role:**
   * Open **Server Manager** → **Add Roles and Features** → Select **DNS Server**.
2. **Open DNS Manager (dnsmgmt.msc)**
3. **Create a New Forward Lookup Zone:**
   * Right-click **Forward Lookup Zones** → Select **New Zone**.
   * Choose **Primary Zone**, **Secondary Zone**, or **Stub Zone**.
   * Assign a **Zone Name** (e.g., example.com).
4. **Create Host (A) Records:**
   * Inside the zone, right-click → Select **New Host (A or AAAA)**.
   * Enter the hostname and corresponding IP.
5. **Configure Reverse Lookup Zone (Optional):**
   * Right-click **Reverse Lookup Zones** → **New Zone** → Configure as needed.
6. **Restart DNS Service:**
   * Use services.msc to restart the **DNS Server service**.

**5. Server Manager and Its Role in Managing Windows Server**

**Server Manager** is a centralized tool for managing Windows Servers. It helps administrators monitor performance, configure roles, and troubleshoot issues.

**Functions of Server Manager:**

* **Role and Feature Management** – Install and remove Windows roles.
* **Server Performance Monitoring** – View real-time performance data.
* **Event Logs and Alerts** – Detect errors and security warnings.
* **Remote Server Management** – Manage multiple servers from a single interface.

**How to Use Server Manager:**

1. **Launch Server Manager** (open servermanager.exe).
2. **Add Servers to Manage:**
   * Click **Manage** → **Add Servers** → Select from **Active Directory or IP address**.
3. **Install Server Roles:**
   * Click **Manage** → **Add Roles and Features** → Follow the installation wizard.
4. **Monitor System Health:**
   * Use the **Dashboard** to check alerts, events, and performance issues.

**6. Role of Remote Desktop Services (RDS) in Windows Server 2016/2019 and How to Configure It**

**Remote Desktop Services (RDS)** allows users to remotely access Windows-based applications and desktops hosted on a server.

**How to Configure RDS in Windows Server:**

1. **Install RDS Role:**
   * Open **Server Manager** → **Add Roles and Features**.
   * Select **Remote Desktop Services Installation**.
2. **Deploy RDS Components:**
   * Choose **Standard or Quick Start Deployment**.
   * Install **Remote Desktop Session Host, Connection Broker, and Web Access**.
3. **Configure Remote Desktop Licensing:**
   * Open **RD Licensing Manager** → Activate a license server.
4. **Create and Publish RemoteApps:**
   * Use **RemoteApp Manager** to configure applications.
5. **Allow Remote Connections:**
   * Open **System Properties (sysdm.cpl)** → Enable **Remote Desktop**.
6. **Test the Remote Desktop Connection:**
   * Use **Remote Desktop Connection (mstsc)** to connect.