

**Hardware Networking**

**SUBMITTED TO**

**KAMLESH SHUKLA SIR**

**SUBMITTED BY**

**MANAV BANDHANIA**

## Module 6. Network security, Maintenance and Troubleshooting procedures

### Topic: SOHO Networks

#### Beginner Questions

1. **What is SOHO network?**
   * **SOHO (Small Office/Home Office) Network**:
     + A network designed for small businesses or home offices.
     + Typically includes a few computers, printers, and other devices connected to the internet.
2. **What does SOHO mean in networking?**
   * **SOHO Networking**:
     + Refers to the setup and management of networks in small offices or home offices.
     + Focuses on providing reliable internet access, file sharing, and device connectivity.

#### Intermediate Questions

1. **How does a SOHO network work?**
   * **Components**:
     + **Router**: Connects to the internet and provides network access.
     + **Switch**: Connects multiple devices within the network.
     + **Wireless Access Point**: Provides Wi-Fi connectivity.
     + **Devices**: Computers, printers, smartphones, etc.
   * **Functionality**:
     + Devices communicate through the router and switch.
     + Internet access is shared among all connected devices.
     + File and printer sharing is enabled.
2. **Issues with SOHO Networking?**
   * **Common Issues**:
     + Limited bandwidth.
     + Security vulnerabilities.
     + Interference with wireless signals.
     + Device compatibility problems.

#### Advanced Questions

1. **How Small is the “S” in SOHO?**
   * **Size**:
     + Typically includes 1-10 employees.
     + Limited number of devices (usually less than 20).
2. **SOHO Routers vs. Home Routers?**
   * **SOHO Routers**:
     + Designed for small business environments.
     + More robust security features.
     + Support for VPNs and multiple SSIDs.
   * **Home Routers**:
     + Designed for personal use.
     + Simpler setup and fewer advanced features.
     + Focus on ease of use and basic security.

### Topic: NAT & PAT

#### Beginner Questions

1. **What is NAT?**
   * **NAT (Network Address Translation)**:
     + Translates private IP addresses to a public IP address for internet access.
     + Helps conserve public IP addresses.
2. **What is PAT?**
   * **PAT (Port Address Translation)**:
     + A type of NAT that maps multiple private IP addresses to a single public IP address using different ports.
     + Also known as **NAT Overload**.
3. **Difference between NAT & PAT?**
   * **NAT**:
     + Translates IP addresses.
     + Can map one-to-one or many-to-one.
   * **PAT**:
     + Translates IP addresses and ports.
     + Maps many-to-one using different ports.

#### Intermediate Questions

1. **How does NAT work?**
   * **Functionality**:
     + A router with NAT translates private IP addresses to a public IP address.
     + Keeps track of active connections using a translation table.
     + Ensures that responses from the internet are sent to the correct private IP address.
2. **Explain NAT?**
   * **NAT**:
     + Allows multiple devices on a local network to share a single public IP address.
     + Provides a layer of security by hiding internal IP addresses from the internet.

#### Advanced Questions

1. **What is the difference between Static & Dynamic NAT?**
   * **Static NAT**:
     + Maps a specific private IP address to a specific public IP address.
     + Used for servers that need a consistent public IP address.
   * **Dynamic NAT**:
     + Maps private IP addresses to a pool of public IP addresses.
     + Public IP addresses are assigned dynamically as needed.
2. **NAT stands for?**
   * **NAT**: Network Address Translation.
3. **PAT stands for?**
   * **PAT**: Port Address Translation.

### Topic: Authentication and Access Control

#### Beginner Questions

1. **What is ACL?**
   * **ACL (Access Control List)**:
     + A set of rules that control access to network resources.
     + Specifies which users or devices can access certain resources.
2. **What are different types of ACL?**
   * **Types of ACL**:
     + **Standard ACL**: Filters traffic based on source IP address.
     + **Extended ACL**: Filters traffic based on source and destination IP addresses, ports, and protocols.

#### Intermediate Questions

1. **Explain Standard Access List?**
   * **Standard Access List**:
     + Filters traffic based on the source IP address.
     + Applied close to the destination.
     + Example: access-list 1 permit 192.168.1.0 0.0.0.255.
2. **Explain Extended Access List?**
   * **Extended Access List**:
     + Filters traffic based on source and destination IP addresses, ports, and protocols.
     + Applied close to the source.
     + Example: access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80.

#### Advanced Questions

1. **What is Wildcard Mask?**
   * **Wildcard Mask**:
     + Used in ACLs to specify a range of IP addresses.
     + Inverse of a subnet mask.
     + Example: 0.0.0.255 allows any address in the last octet.
2. **In which directions can we apply an Access List?**
   * **Directions**:
     + **Inbound**: Applied to incoming traffic on an interface.
     + **Outbound**: Applied to outgoing traffic on an interface.

### Topic: WAN Technologies

#### Beginner Questions

1. **Fiber-optic communication**
   * **Fiber-Optic Communication**:
     + Uses light signals to transmit data.
     + High-speed and long-distance communication.
     + Immune to electromagnetic interference.
2. **What is Leased Line?**
   * **Leased Line**:
     + A dedicated, private connection between two locations.
     + Provides consistent bandwidth and reliability.
     + Used for business internet and private networks.
3. **Explain Circuit Switching**
   * **Circuit Switching**:
     + Establishes a dedicated communication path between two devices.
     + Used in traditional telephone networks.
     + Provides a constant connection for the duration of the call.

#### Intermediate Questions

1. **Explain Packet Switching**
   * **Packet Switching**:
     + Data is broken into packets and transmitted over a shared network.
     + Each packet can take a different path to the destination.
     + Used in modern data networks, including the internet.
2. **What is the difference between leased line and broadband?**
   * **Leased Line**:
     + Dedicated connection.
     + Consistent bandwidth.
     + Higher cost.
   * **Broadband**:
     + Shared connection.
     + Variable bandwidth.
     + Lower cost.
3. **How much is a 100mb Leased Line?**
   * **Cost**:
     + The cost of a 100mb leased line varies by location and provider.
     + Typically ranges from $500 to $1,500 per month.

#### Advanced Questions

1. **Difference between a POTS line and a leased line?**
   * **POTS Line**:
     + Plain Old Telephone Service.
     + Analog voice communication.
     + Shared public network.
   * **Leased Line**:
     + Dedicated digital connection.
     + Consistent bandwidth.
     + Private network.
2. **What is the process of packet switching?**
   * **Packet Switching Process**:
     + Data is divided into packets.
     + Packets are routed independently through the network.
     + Packets are reassembled at the destination.
3. **Difference between circuit switching and packet switching?**
   * **Circuit Switching**:
     + Dedicated path.
     + Constant connection.
     + Used in traditional telephony.
   * **Packet Switching**:
     + Shared path.
     + Dynamic routing.
     + Used in data networks.
4. **Practice on Printer Sharing**
   * **Steps**:
     + Connect the printer to the network.
     + Open **Control Panel**.
     + Go to **Devices and Printers**.
     + Right-click the printer and select **Printer properties**.
     + Go to the **Sharing** tab and enable sharing.
5. **Use of IIS (Internet Information Services)**
   * **Steps**:
     + Open **Control Panel**.
     + Go to **Programs and Features**.
     + Click on **Turn Windows features on or off**.
     + Check **Internet Information Services (IIS)** and click **OK**.
     + Configure IIS through the **IIS Manager**.

### Topic: Communication Technologies, Cloud, and Virtualization

#### Beginner Questions

1. **What is virtualization?**
   * **Virtualization**:
     + Creating virtual versions of physical resources (e.g., servers, storage).
     + Allows multiple virtual machines to run on a single physical machine.
2. **What are two types of virtualization in cloud?**
   * **Types of Virtualization**:
     + **Server Virtualization**: Dividing a physical server into multiple virtual servers.
     + **Storage Virtualization**: Pooling physical storage from multiple devices into a single virtual storage device.

#### Intermediate Questions

1. **What are the two types of virtualization?**
   1. **Types of Virtualization**:
      1. **Full Virtualization**: Virtual machines emulate the entire hardware.
      2. **Paravirtualization**: Virtual machines are aware of the hypervisor and interact with it directly.
2. **What is VMware virtualization technology?**
   1. **VMware Virtualization Technology**:
      1. VMware provides software for creating and managing virtual machines (VMs).
      2. Allows multiple VMs to run on a single physical server.
      3. Offers products like VMware vSphere, VMware Workstation, and VMware Fusion.
      4. Enhances resource utilization, simplifies management, and improves scalability.

#### Advanced Questions

1. **What is the difference between cloud and virtualization?**
   * **Virtualization**:
     + Technology that creates virtual versions of physical resources (e.g., servers, storage).
     + Allows multiple virtual machines to run on a single physical machine.
   * **Cloud Computing**:
     + Delivery of computing services (e.g., servers, storage, databases) over the internet.
     + Uses virtualization as a foundational technology.
     + Provides on-demand access to resources, scalability, and pay-as-you-go pricing.
2. **What are the benefits of implementing virtualization in cloud computing?**
   * **Benefits**:
     + **Resource Efficiency**: Maximizes the use of physical hardware.
     + **Scalability**: Easily scale resources up or down based on demand.
     + **Cost Savings**: Reduces hardware and maintenance costs.
     + **Flexibility**: Quickly deploy and manage virtual machines.
     + **Disaster Recovery**: Simplifies backup and recovery processes.

### Topic: Monitoring Tools

#### Beginner Questions

1. **Why are network monitoring tools used?**
   * **Purpose**:
     + Monitor network performance and availability.
     + Detect and diagnose network issues.
     + Ensure network security and compliance.
     + Optimize network resources and performance.
2. **Explain firewalls**
   * **Firewalls**:
     + Security devices that monitor and control incoming and outgoing network traffic.
     + Act as a barrier between trusted and untrusted networks.
     + Can be hardware-based, software-based, or a combination of both.
     + Use rules to allow or block traffic based on security policies.

#### Intermediate Questions

1. **Explain core switches**
   * **Core Switches**:
     + High-capacity switches used in the core layer of a network.
     + Provide fast and reliable data transfer between different parts of the network.
     + Handle large amounts of traffic and support high-speed connections.
     + Essential for backbone connectivity in large networks.
2. **Explain client systems**
   * **Client Systems**:
     + End-user devices that access network resources and services.
     + Examples include desktops, laptops, tablets, and smartphones.
     + Connect to servers and other network devices to perform tasks.
     + Rely on network infrastructure for communication and data exchange.

#### Advanced Questions

1. **What is network management?**
   * **Network Management**:
     + The process of administering, managing, and operating a network.
     + Includes monitoring network performance, troubleshooting issues, and ensuring security.
     + Involves tasks like configuration management, fault management, and performance management.
2. **Explain Event Viewer**
   * **Event Viewer**:
     + A Windows tool that logs system, security, and application events.
     + Helps diagnose and troubleshoot issues by providing detailed event information.
     + Can be accessed through the Control Panel or by typing eventvwr in the Run dialog.
     + Events are categorized into logs such as Application, Security, and System.
3. **Practice “parental control” or “family safety” option in Control Panel**
   * **Steps**:
     + Open **Control Panel**.
     + Go to **User Accounts and Family Safety**.
     + Click on **Family Safety**.
     + Select the user account to apply controls.
     + Configure settings for web filtering, time limits, and app restrictions.

### Topic: Network Security, Network Vulnerabilities

#### Beginner Questions

1. **What are network vulnerabilities?**
   * **Network Vulnerabilities**:
     + Weaknesses or flaws in a network that can be exploited by attackers.
     + Examples include unpatched software, weak passwords, and misconfigured devices.
2. **What are the types of network security attacks?**
   * **Types of Attacks**:
     + **Phishing**: Deceptive emails to steal sensitive information.
     + **Malware**: Malicious software like viruses and ransomware.
     + **DDoS (Distributed Denial of Service)**: Overwhelming a network with traffic.
     + **Man-in-the-Middle**: Intercepting and altering communication between two parties.

#### Intermediate Questions

1. **What is a virus in network security?**
   * **Virus**:
     + Malicious software that attaches itself to legitimate programs.
     + Can replicate and spread to other files and systems.
     + Causes damage by corrupting data, stealing information, or disrupting operations.
2. **What is the difference between virus and antivirus?**
   * **Virus**:
     + Malicious software designed to harm or exploit systems.
   * **Antivirus**:
     + Software designed to detect, prevent, and remove viruses and other malware.
     + Provides real-time protection and regular scans to keep systems secure.

#### Advanced Questions

1. **Who is vulnerable in network security?**
   * **Vulnerable Entities**:
     + Any device or user connected to a network.
     + Includes computers, servers, mobile devices, and IoT devices.
     + Users with weak passwords or outdated software are particularly at risk.
2. **How do you assess vulnerability?**
   * **Vulnerability Assessment**:
     + Conduct regular scans using vulnerability assessment tools.
     + Review and analyze security logs and reports.
     + Perform penetration testing to identify and exploit vulnerabilities.
     + Keep software and systems updated with the latest security patches.
3. **What are the principles of network security?**
   * **Principles**:
     + **Confidentiality**: Ensuring that data is accessible only to authorized users.
     + **Integrity**: Protecting data from unauthorized modification.
     + **Availability**: Ensuring that network services are available when needed.
     + **Authentication**: Verifying the identity of users and devices.
     + **Authorization**: Granting permissions based on user roles and policies.
4. **What is a firewall used for?**
   * **Firewall**:
     + Used to protect a network by controlling incoming and outgoing traffic.
     + Blocks unauthorized access while allowing legitimate communication.
     + Can be configured with rules to filter traffic based on IP addresses, ports, and protocols.
5. **Configure advanced firewall settings**
   * **Steps**:
     + Open **Windows Defender Firewall with Advanced Security**.
     + Click on **Inbound Rules** or **Outbound Rules**.
     + Click **New Rule** to create a custom rule.
     + Choose the rule type (e.g., Program, Port).
     + Specify the conditions and actions for the rule.
     + Click **Finish** to apply the rule.
6. **Configure “date and time” option in Control Panel**
   * **Steps**:
     + Open **Control Panel**.
     + Click on **Date and Time**.
     + Click **Change date and time** to set the correct date and time.
     + Click **Change time zone** to select the appropriate time zone.
     + Click **OK** to save changes.