**N+ - Network Fundamentals And Building Networks**

 What is SOHO network?

SOHO stands for "Small Office/Home Office." A SOHO network is a network used by small businesses or home offices. It typically involves basic networking setups, such as a few computers, printers, and shared internet access. SOHO networks often rely on wireless routers, switches, and basic firewalls for security and connection.

 What is NAT?

NAT stands for **Network Address Translation**. It is a method used in networking where private IP addresses on an internal network are mapped to a single public IP address or a few public addresses. This is primarily used in routers and firewalls to allow multiple devices on a local network to access the internet using one public IP address.

 What is PAT?

PAT stands for **Port Address Translation**, a specific type of NAT. It allows multiple devices on a local network to share a single public IP address by differentiating the connections using port numbers. This is commonly used to manage internet access for a large number of devices.

 Different between NAT & PAT?

* **NAT**: Translates private IP addresses into a public IP address.
* **PAT**: A type of NAT that allows multiple devices to share a single public IP address by distinguishing the connections using different port numbers.

In summary, while NAT focuses on translating IP addresses, PAT is more about distinguishing traffic based on ports, often enabling more devices to share the same IP address.

 What Is Acl?

**ACL (Access Control List)** is a set of rules used to filter network traffic. ACLs are used in routers and firewalls to control which users or systems can access resources on a network. ACLs specify which IP addresses, ports, or protocols are allowed or denied from accessing certain network resources.

 What Are Different Types of Acl? What Is Wildcard Mask?

There are mainly two types of ACLs:

* **Standard ACL**: Filters traffic based only on the source IP address.
* **Extended ACL**: Filters traffic based on source IP, destination IP, ports, and protocols.

A **Wildcard Mask** is used in networking, especially with ACLs, to specify the range of IP addresses. It is the inverse of a subnet mask and defines which bits in an IP address should be matched and which should be ignored.

 Explain Circuit switching

**Circuit Switching** is a communication method where a dedicated communication path is established between two devices for the duration of the communication. This is used in traditional telephone networks where a direct path is established and maintained for the entire call.

 What is difference between leased line and broadband?

**Leased Line**: A dedicated, fixed-bandwidth, and always-on connection that provides a private line between two locations, typically used by businesses.

**Broadband**: A high-speed internet connection that is typically shared by multiple users. It is often less expensive than a leased line and may be subject to bandwidth limitations or slowdowns during peak usage.

 Difference between a POTS line and a leased line?

**POTS (Plain Old Telephone Service)**: A standard telephone line for voice communication, often used for basic residential telephone service.

**Leased Line**: A private line that provides dedicated communication for data or voice and is typically more expensive and reliable than POTS.

 Practice on printer sharing

Printer sharing allows multiple computers to use a single printer. This can be done by connecting the printer to one computer and sharing it over a network, or by using a print server. On Windows, this can be set up by enabling printer sharing in the printer's properties.

 Use of IIS

**IIS (Internet Information Services)** is a web server software developed by Microsoft. It is used to host websites, web applications, and services. IIS supports a variety of protocols like HTTP, HTTPS, FTP, and others.

 Create FTP server ,

To create an FTP server, you can use software like FileZilla Server, or on Windows, IIS can be used to configure FTP services. Here are the basic steps for setting up an FTP server:

* Install FTP server software.
* Set up user accounts and permissions.
* Open necessary ports (usually port 21 for FTP).
* Configure the firewall to allow FTP traffic.

 What is the difference between cloud and virtualization?

**Cloud Computing**: Refers to services and resources that are hosted over the internet, allowing users to access computing power, storage, and applications remotely, often on a pay-per-use basis.

**Virtualization**: Refers to the technology that allows you to create virtual instances of servers, storage, or networking devices. It enables multiple virtual machines to run on a single physical server.

 Why are network monitoring tools used?

Network monitoring tools are used to track and analyze network performance, troubleshoot issues, ensure security, and maintain optimal network operation. These tools can detect problems such as outages, bottlenecks, or security threats.

 What is ping ?

**Ping** is a network diagnostic tool used to test the reachability of a device on a network. It works by sending ICMP Echo Request messages and waiting for a response (ICMP Echo Reply). It's commonly used to check if a device is online and responding.

 What is traceroute ?

**Traceroute** is a diagnostic tool that traces the path that packets take from one device to another across a network. It shows each hop (router or device) that the packets pass through, helping to identify where delays or issues occur.

 What is nslookup?

**Nslookup** (Name Server Lookup) is a tool used to query DNS servers to obtain domain name or IP address information. It helps in troubleshooting DNS issues by resolving domain names into IP addresses and vice versa.

 Explain core switches

**Core Switches** are high-performance switches used in the core layer of a network. They provide high-speed data transfer between different parts of the network and handle large volumes of traffic. Core switches are essential in data centers and enterprise networks.

What is network management?

Network management refers to the process of monitoring, maintaining, and optimizing a network to ensure that it operates efficiently. This includes tasks such as configuring network devices, ensuring network security, monitoring network performance, troubleshooting issues, and managing the network's infrastructure (hardware and software). Network management aims to ensure reliability, performance, and security of the network by using management protocols like SNMP (Simple Network Management Protocol).

 Explain Event Viewer

**Event Viewer** is a Windows tool used to view and analyze event logs on a system. It logs information about system activities, errors, warnings, and other events related to system performance. Event Viewer helps system administrators monitor for issues like hardware failures, security breaches, software errors, and performance degradation. You can filter events by categories such as:

* **Application Logs**: Information about applications running on the system.
* **System Logs**: Information about the operating system's performance.
* **Security Logs**: Events related to user activities and security events like logins and system access.

 Practice "parental control" or "family safety" option in control pane What

are network vulnerabilities?

The **Parental Control** or **Family Safety** feature in Windows allows you to set up restrictions for family members or children using the computer. It helps manage what content can be accessed, when the computer can be used, and limits on online activities. Here's how you can enable and configure it:

* **On Windows 10/11**:
  + Open **Control Panel**.
  + Go to **User Accounts** and click on **Set up Family & other users**.
  + Add a child account and configure the restrictions.
  + You can set time limits, web filtering, and even monitor activity through the **Microsoft Family Safety app**.

**Features include**:

* + Setting limits on screen time.
  + Filtering inappropriate websites.
  + Managing app and game usage.
  + Monitoring activity and getting reports.

**Network vulnerabilities** are weaknesses or flaws in a network's design, implementation, or configuration that can be exploited by attackers to compromise the network. These vulnerabilities can lead to data breaches, unauthorized access, and disruption of services. Some common network vulnerabilities include:

* Weak or default passwords.
* Unpatched software or outdated firmware.
* Insecure network configurations.
* Lack of encryption or weak encryption standards.
* Open ports and unmonitored network traffic.

 What are the types of network security attacks?

Network security attacks can be classified into various types based on their nature and the technique used. Here are some common types:

* **Denial of Service (DoS)**: This type of attack floods a network or server with so much traffic that it becomes unavailable to legitimate users.
  + **Distributed Denial of Service (DDoS)**: A variant where the attack comes from multiple sources, making it harder to block.
* **Man-in-the-Middle (MitM)**: In this type of attack, an attacker intercepts communication between two parties and can alter or steal data without the participants knowing.
* **Phishing**: A form of social engineering where attackers attempt to trick individuals into revealing sensitive information like usernames, passwords, or credit card numbers by pretending to be a trustworthy entity.
* **SQL Injection**: In this attack, malicious SQL code is injected into an application’s database query to manipulate or steal data.
* **Malware**: This refers to any malicious software, including viruses, worms, and ransomware, that can infiltrate and harm a network or system. Malware can cause damage, steal information, or give unauthorized access.
* **Password Attacks**: Attackers try to gain access to accounts by guessing or cracking passwords through methods like brute force, dictionary attacks, or keylogging.
* **Eavesdropping/Sniffing**: Attackers use sniffing tools to capture and intercept network traffic, which may include sensitive data such as login credentials or personal information.
* **Spoofing**: This is when an attacker impersonates another device or user to gain unauthorized access to a network. This can include IP spoofing or email spoofing.
* **Cross-Site Scripting (XSS)**: In this attack, attackers inject malicious scripts into web pages that can be executed on the client side to steal information or compromise the user’s session.