**N+ - Network security, Maintenance and Troubleshooting procedures**

**Module – 2**

**• What is SOHO network?**

**Ans.** A Small Office Home Office (SOHO) network refers to a type of local area or LAN network connection designed for small businesses. SOHO networks can be a small wired Ethernet LAN or a combination of wired and wireless computer. It typically involves a small number of employees, usually ranging from 1 to 10.

OR

* SOHO stands for “Small Office/Home Office.” A SOHO network refers to a small-scale computer network typically designed for use in home office or a small business setting.

**• What is NAT?**

**Ans.** NAT stands for Network address translation. It’s a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet.

OR

* It’s like a translator for your home network, allowing multiple devices to share a single public IP address when accessing the internet.

**• What is PAT?**

**Ans.** PAT stand for Port Address translation. It’s a type of Network Address Translation (NAT) that not only translates private IP address to a single public IP but also keeps track of different connection using unique port number. It helps multiple devices on a local network share a single public IP address.

**• Different between NAT & PAT?**

**Ans.**

|  |  |
| --- | --- |
| **NAT** | **PAT** |
| NAT stands for Network Address Translation. | PAT stands for Port Address Translation. |
| NAT can be considered PAT’s superset. | PAT is a dynamic NAT. |
| NAT uses IPv4 address. | PAT also uses IPv4 address but with port number. |
| NAT Private IP addresses are translated into the public IP address. | PAT, Private IP address are translated into the public IP address via port number. |

**• What Is ACL?**

**Ans.** A network access control list is made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusiveclub. Only those on the list are allowed in the doors.

**• What Are Different Types of ACL? What Is Wildcard Mask?**

**Ans.** ACL stands for Access Control List, and there are two main types:

1. Standard ACL: Filters traffic based on source IP address only.
2. Extended ACL: Filter traffic based on source and destination IP address, as well as other parameters like protocols and port numbers.

* A **Wildcard Mask** is used in conjunction with ACLs to specify which bits in an IP address should be checked. It is a binary mask where 0 means “must match” and 1 means “don’t care.”

Wildcard masks help define ranges of IP address for ACL rules.

**• Explain Circuit switching.**

**Ans.** Circuit switching is a type of network configuration in which a physical path is obtained and dedicated to a single connection between two endpoint in the network for the duration of a dedicated connection. Ordinary voice phone service uses circuit switching.

**• What is difference between leased line and broadband?**

**Ans.**

|  |  |
| --- | --- |
| **Leased Line** | **Broadband** |
| Quicker connection speeds. | Slower connection speeds. |
| Symmetrical download and upload speeds. | Asymmetrical download and upload speeds. |
| Service Level Agreements as standard. | Typically, no Service Level Agreements. |
| More expensive. | Cheaper. |

**• Difference between a POTS line and a leased line?**

**Ans.**

**POTS (Plain Old Telephone Service) Line:**

Use: Primarily designed for traditional voice communication.

Nature: Analog in nature and mainly used for basic telephone services.

Availability: Widely available and commonly used in residential areas.

Bandwidth: Relatively low bandwidth, suitable for voice but not high-s peed data transmission.

Dedication: Typically shared with other users in a local area.

**Leased Line:**

Use: Intended for high-speed data communication, private networks, or dedicated internet access.

Nature: Can be analog or digital, with digital leased lines (like T1 or E1) offering higher data rates.

Availability: Typically used by businesses and organizations that require dedicated and reliable connections.

Bandwidth: Offers higher bandwidth compared to POTS lines, making it suitable for data-intensive applications.

Dedication: Fully dedicated to the subscriber, providing a constant and private connection.

**• Practice on printer sharing.**

**Ans.**

**Connect the Printer:** Physically connect the printer to a computer within the network.

**Enable Printer Sharing:** On the computer to which the printer is connected, enable printer sharing in the printer settings.

**Configure Network Settings:** Ensure that all computers are on the same network (Wi-Fi or Ethernet).

**Find the Shared Printer:** On other computers, navigate to printer settings and select "Add a printer" or "Network printer."

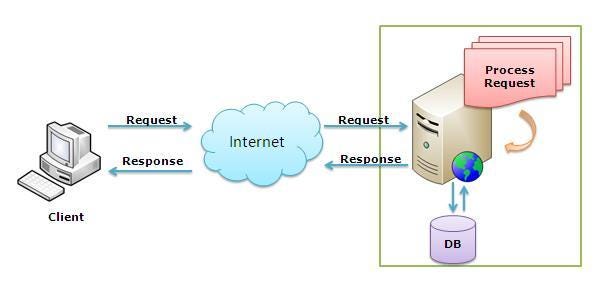
**Select Shared Printer:** Choose the shared printer from the list of available printers on the network.

**Install Printer Drivers:** If prompted, install the necessary printer drivers on the computer accessing the shared printer.

**Test Printing:** Print a test page from the computer that added the shared printer to confirm proper setup.

**• Use of IIS.**

**Ans. Internet Information Services**, also know as IIS, is Microsoft web server that runs on Windows operating system and is used to exchange static and dynamic web content with internet users. IIS can be used to host, deploy, and manage web application using technologies such as ASP.NET and PHP.



**• Create FTP server**

**Ans.** Setting up an FTP (File Transfer Protocol) server involves a few steps.

1. **Install FTP Server Software:**

Choose and install FTP server software on the computer that will host the FTP server. Popular options include FileZilla Server, vsftpd (for Linux), or Core FTP Server (for Windows).

1. **Configure FTP Server:**

Open the FTP server software and configure settings such as server address, port, and user access permissions. Set up user accounts if required.

1. **Port Forwarding (if applicable):**

If the FTP server is behind a router, configure port forwarding to allow external access. Forward port 21 (default FTP control port) to the internal IP address of the computer hosting the FTP server.

1. **Firewall Configuration:**

Adjust the firewall settings to permit traffic on the configured FTP port. This ensures that the FTP server can communicate with external devices.

1. **Test the FTP Server:**

Verify the setup by connecting to the FTP server using an FTP client. Use the server's IP address, port number, and appropriate credentials.

1. **Transfer Files:**

Once connected, you can upload and download files to and from the FTP server using the FTP client.

**• What is the difference between cloud and virtualization?**

**Ans.**

|  |  |
| --- | --- |
| **Cloud** | **Virtualization** |
| Cloud is used to provide pools and automated resources that can be accessed on-demand. | While it is used to make various simulated environments through physical hardware system. |
| Cloud computing setup is tedious, complicated. | Virtualization setup is simple as compared to cloud computing. |
| Cloud computing is high scalable. | Virtualization is low scalable compared to cloud computing. |
| Cloud computing is Very flexible. | Virtualization is less flexible than cloud computing. |
| In cloud computing, the workload is stateless. | In virtualization, the work is stateful. |

**• Why are network monitoring tools used?**

**Ans.** Network Monitoring tools collect data from the network devices present in the environment through network protocols and keep the network immune to any threats. They help track various performance metrics like traffic, bandwidth utilization, availability, packet loss and much more.

**• What is ping?**

**Ans.** A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allow a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration. The acronym was contrived to match the submariners’ term for the sound of a returned sonar pulse.

OR

* Ping is a network utility that checks the connection and responsiveness between two devices, often used to test if a host (like a website or server) is reachable and how long it takes to get a response.

**• What is traceroute?**

**Ans.** Traceroute is a network diagnostic tool that traces and displays the route that data packets take from one computer to another over a network. It helps identify the path and any delays between the source and destination.

OR

* Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between.

**• What is nslookup?**

**Ans.** Nslookup (from “name server lookup”) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records.

OR

* Nslookup is a command-line tool used to query and retrieve domain name system (DNS) information, such as IP addresses associated with domain names or domain names associated with IP address.

**• Explain core switches.**

**Ans.** Core switches are like traffic hubs in a network. They efficiently manage and direct data between different parts of a network, ensuring fast and reliable fast and reliable communication. Think of them as the central coordinators that handle the main flow of data, connecting various devices and subnetworks within an organization’s infrastructure.

OR

* A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to a wide area network (WAN) or the Internet – they provide the final aggregation point for the network and allow multiple aggregation modules to work together.

**• What is network management?**

**Ans.** Network management systems collect real-time data from network elements, such as switches, routers, and access point, as well as from endpoint devices, such as mobile phones, laptop, and desktops.

**• Explain Event Viewer.**

**Ans.** The Event Viewer is a tool in Windows that displays detailed information about significant events on your computer. Examples of these are programs that don't start as expected, or automatically downloaded updates. Event Viewer is especially useful for troubleshooting Windows and application errors.

**• Practice "parental control" or "family safety" option in control pane What are network vulnerabilities?**

**Ans.** Parental control or family safety options in the Control Panel allow parents to monitor and control their children's computer activities. These features enable setting restrictions on website access, controlling app usage, and managing screen time to ensure a safer and more controlled online environment for children.

* Network vulnerabilities refer to weaknesses in a computer network that could be exploited by unauthorized users or malicious software. These weaknesses may include outdated software, misconfigured settings, or insecure network protocols, making the network susceptible to unauthorized access, data breaches, or other cyber threats. Regular updates, strong passwords, and security configurations help mitigate network vulnerabilities.

**• What are the types of network security attacks?**

**Ans.**

1. **Malware:** Malicious software, such as viruses, worms, and ransomware, designed to damage or disrupt computer systems.
2. **Phishing:** Deceptive attempts to acquire sensitive information by pretending to be a trustworthy entity, often through email or fake websites.
3. **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** Overloading a network or website with traffic to make it unavailable to users.
4. **Man-in-the-Middle (MitM):** Intercepting and potentially altering communication between two parties without their knowledge.
5. **SQL Injection:** Exploiting vulnerabilities in web applications to manipulate or access a database by injecting malicious SQL code.
6. **Cross-Site Scripting (XSS):** Injecting malicious scripts into websites that are then viewed by other users, compromising their data or session information.
7. **Zero-Day Exploits:** Attacks that target unknown vulnerabilities in software or hardware before developers can provide a fix or patch.
8. **Password Attacks:** Attempts to gain unauthorized access by exploiting weak passwords through methods like brute force attacks or password cracking.
9. **Social Engineering:** Manipulating individuals into divulging confidential information or performing actions that may compromise security.
10. **Eavesdropping:** Unauthorized interception of network communication to gather sensitive information.
11. **Insider Threats:** Malicious actions or data breaches initiated by individuals within an organization, either intentionally or unintentionally.