Module 6. Network security, Maintenance and Troubleshooting procedures

Topic: A SOHO Networks

• Beginner Question

1.What is SOHO network?

Ans. A SOHO network is a small-scale network used individuals or small businesses at home or in a small office. it connects devices like computers and printers for sharing resources and accessing the internet.

2.What does SOHO mean networking?

Ans. Soho in networking refers to a small office or home office network, where devices are connected for sharing resources and accessing the internet.

• Intermediate Question

1.How does a SOHO network work?

Ans. A Small Office/Home Office (SOHO) network connects devices like computers and printers at home or in a small office, allowing them to share information and resources through a common router or wireless access point.

2.Issues with SOHO Networking?

Ans. some common issues with SOHO networking include slow internet speeds, connectivity problems, and difficulty in setting up and managing the network.

• Advance Question

1.How Small is the “S” in SOHO?

Ans. in the term SOHO the s stands for small indicating that it refers to a network setup for small offices or hone offices.

2.SOHO Routers vs. Home Routers? Ans. **SOHO Routers: 1. SOHO** (Small Office/Home Office) routers are designed to cater to the networking needs of both small offices and home offices. **2.SOHO routers** ..are suitable for scenarios where there is a mix of work-related and personal networking requirements

**1.Home routers..** are typically designed for residential use and are focused on providing essential networking functions for household devices. **2.Home routers..** are often more user-friendly and easier to set up, targeting users who may not have advanced networking knowledge.

Topic: NAT & PAT

• Beginner Question

1.What is NAT?

Ans. It is a technique used in networking to translate private IP addresses to public IP addresses, allowing devices on a local network to communicate with the internet.

2.What is PAT?

Ans. PAT is a type of Network Address Translation (NAT) that maps multiple private IP addresses to a single public IP address using different ports to uniquely identify each internal device on a network

3.Different between NAT & PAT?

Ans. NAT - assigns a single public IP address to each private IP address within a network, allowing devices on a local network to communicate with the internet.

PAT- uses a single public IP address but distinguishes between devices by assigning unique port numbers to each connection, enabling multiple devices to share the same public IP.

• Intermediate Question

1.However, Will Nat work?

Ans. NAT will work effectively in allowing devices on a private network to communicate with the internet using a shared public IP address. It is a commonly used technique in networking.

2. Explain NAT?

Ans. NAT stands for Network Address Translation. It is a technique used in networking to translate private IP addresses to public IP addresses, allowing devices on a local network to communicate with the internet. It helps conserve ip addresses and adds an extra layer of security.

• Advance Question

1.What is different between Static & Dynamic NAT?

Ans. **static NAT** • one-to-one address mapping. • fixed in time.

**dynamic NAT** • based on used requirement and session flow. • binding used and re used.

2. NAT stand for?

Ans. NAT stands for Network Address Translation, a technique used in computer networking to map private IP addresses to a single public IP address for internet communication.

3. PAT stand for?

Ans. PAT stands for Port Address Translation, a type of Network Address Translation (NAT) that uses unique port numbers to manage multiple private IP addresses sharing a single public IP address.

Topic: Authentication and Access Control

• Beginner Question

1.What Is ACL?

Ans. ACL stands for access control list, which is a set rules used to control network traffic.

2.What Are Different Types of ACL?

Ans. 1. Standard ACLs:- These filter traffic based on the source IP address. 2. Extended ACLs:-These filter traffic based on source and destination IP addresses, protocols, and ports. 3. Named ACLs:- Similar to extended ACLs, but they are given a name for easier management. 4. Reflexive ACLs:- These dynamically allow inbound traffic based on outbound traffic initiated from within the network.

• Intermediate Question

1.Explain Standard Access List?

Ans. A Standard Access List is a type of access control list (ACL) in networking that filters traffic based on source IP addresses, allowing or denying access to specific network resources.

2.Explain Extended Access List?

Ans. An Extended Access List is a type of access control list (ACL) in networking that filters traffic based on various criteria, including source and destination IP addresses, port numbers, and protocols, offering more granular control over network traffic compared to Standard Access Lists.

• Advance Question

1.What Is Wildcard Mask?

Ans. the wildcard mask is the inverse of the subnet mask. It helps define which parts of an address can vary.

2. In Which Directions We Can Apply an Access List?

Ans. you can apply an access list in two directions. Inbound and out bound. Inbound applies to incoming traffic, while outbound applies to outbound traffic.

Topic: WAN Technologies

• Beginner Question

1.Fiber-optic communication

Ans. fiber-optic communication is a technology that uses light to transmit data over long distances.

2.What is Leased Line

Ans. A leased line is a dedicated, always-on telecommunications line that provides a constant, high-bandwidth connection between two points, typically used for private data or internet access.

3.Explain Circuit switching

Ans. Circuit switching is a communication method that establishes a dedicated physical path between two devices for the duration of a conversation, ensuring a continuous connection without sharing resources with other users.

• Intermediate Question

1.Explain Packet Switching

Ans. packet switching is a way of sending data in small packet over a network, like breaking a message into smaller parts and sending them separately

2. What is difference between leased line and broadband?

Ans. A leased line is a dedicated, private connection between two locations, providing a reliable and secure connection. Broadband, on the other hand, is a shared internet connection that is available to multiple users and offers higher speeds but may have varying levels of reliability and security. So, a leased line is like having your own exclusive highway, while broadband is like sharing a highway with others.

3. How much is a 100mb Leased Line?

Ans. A 100MB leased line is a point-to-point symmetric data connection that offers a connection speed of 100Mbit/s. Cost Comparison.

• Advance Question

1.Difference between a POTS line and a leased line?

Ans. A POTS line, also known as a Plain Old Telephone Service line, is a traditional analog phone line used for voice communication So. a POTS line is like a regular phone line, while a leased line is like a dedicated highway for data.

2.What is the process of packet switching?

Ans. Packet switching is a digital communication method that breaks data into packets, which are individually routed based on destination addresses, optimizing network efficiency and enabling simultaneous transmission of multiple data streams.

3.Difference between circuit switching and packet switching?

Ans. Circuit switching establishes a dedicated communication path, while packet switching breaks data into packets that travel independently across the network.

4. Practice on printer sharing

Ans. Done

5.Use of IIS [ Via "add and remove" feature from control panel. "appwiz.cpl" command] Topic: Communication technologies Cloud and Virtualization.

Ans. a "add and remove" feature from the control panel, accessed via the "appwiz.cpl" command, can be used to uninstall or modify installed components, including Internet Information Services (IIS), which is crucial for web hosting and server management in the context of communication technologies, cloud, and virtualization.

• Beginner Question

1.What is virtualization?

Ans. Virtualization is the process of creating a virtual version of something, like a computer or server, to run multiple operating systems or applications on a single physical machine. It's like having multiple virtual machines within one physical machine.

2. What are two types of virtualization in cloud?

Ans. Two types of virtualization in the cloud are server virtualization, which creates virtual servers on a physical host, and network virtualization, which abstracts network resources to create virtual networks.

• Intermediate Question

1.What are the two types of virtualization?

Ans. 1. Server Virtualization. 2.Network Virtualization.

**2.** What is VMware virtualization technology?

Ans. VMware virtualization technology is a suite of products that enables the creation and management of virtualized computing environments, allowing multiple operating systems to run on a single physical server.

• Advance Question

1.What is the difference between cloud and virtualization?

Ans. Cloud refers to the delivery of computing resources and services over the internet, while virtualization is the process o creating virtual versions of physical resources.

2. What are the benefits of implementing virtualization in cloud computing?

Ans. Implementing virtualization in cloud computing enhances resource efficiency, scalability, and flexibility by creating virtual instances of computing components, optimizing utilization and facilitating dynamic allocation of resources.

Topic: Monitoring Tools

• Beginner Question

1.Why are network monitoring tools used?

Ans. Network monitoring tools are used to monitor and analyze network traffic, detect issues, and ensure optimal network performance and security.

2. Explain firewalls

Ans. firewalls are like security guards that protect your computer or network form unwanted intruders.

• Intermediate Question

1.Explain core switches

Ans. Core switches are high-capacity networking devices that efficiently manage and direct data traffic within the core or backbone of a computer network

2. Explain client systems

Ans. Client systems are end-user devices, such as computers or mobile devices, that interact with and request services from servers in a network.

• Advance Question

1.What is network management?

Ans. Network management involves the administration and monitoring of computer networks to ensure their efficient operation, performance, and security.

2.Explain Event Viewer

Ans. Event Viewer is a Windows tool that logs system and application events, helping users and administrators troubleshoot issues and monitor the performance of a computer.

Top of Form

Top of Form

3. Parentice "parental control" or "family safety" option in control panel Topic: Network Security, Network vulnerabilities

Ans. The "Parental Control" or "Family Safety" option in the control panel falls under the broader topic of Network Security, specifically addressing measures to control and monitor access to online content for family safety, particularly protecting children from inappropriate or harmful online material.

• Beginner Question

1.What are network vulnerabilities?

Ans. Network vulnerabilities are weaknesses or flaws in a computer network's security that could be exploited by attackers to compromise the confidentiality, integrity, or availability of information.

2.What are the types of network security attacks?

Ans. Malware Attacks, Denial-of-Service (DoS) Attacks, Man-in-the-Middle (MitM) Attacks, Phishing Attacks, SQL Injection Attacks, Cross-Site Scripting (XSS) Attacks, Password Attacks, DNS Spoofing, Zero-Day Exploits, Eavesdropping Attacks

• Intermediate Question

1.What is virus in network security?

Ans. A virus in network security is malicious software that attaches itself to legitimate programs or files, spreading across a network and potentially causing harm by executing unwanted actions.

2. What is the difference between virus and antivirus?

ans. **virus-** • A virus is malicious software designed to replicate itself and spread to other computers or files, causing harm to the system. • Viruses aim to compromise the integrity of a system, steal data, or disrupt normal operations.

**Antivirus-** • Antivirus is protective software designed to detect, prevent, and remove viruses and other malicious software from a computer or network. • Antivirus programs aim to safeguard systems by identifying and neutralizing malicious software, preventing its execution and ensuring the security of the system.

• Advance Question

1.Who is vulnerable in network security?

Ans. Users, devices, and systems can be vulnerable in network security, subject to exploitation through various attacks due to weaknesses in software, configurations, or human factors

2. How do you assess vulnerability?

Ans. Vulnerability assessment involves systematically identifying, quantifying, and prioritizing weaknesses in a system's security, typically through scanning tools and methodologies.

3. What are the principles of network security?

Ans. Principles of network security include confidentiality, integrity, availability, authentication, and non-repudiation, forming the foundation for safeguarding information and systems.

4. What is a firewall to use for?

Ans. A firewall is used to monitor and control incoming and outgoing network traffic, acting as a barrier between a private internal network and the public internet to enhance security.

5. configure advanced firewall setting?

Ans. To configure advanced firewall settings, access the firewall management interface and customize rules, permissions, and security parameters based on specific network requirements and threat prevention strategies.

6. configure "date and time" OPTI ?

Ans. To configure "date and time" settings, access the operating system's control panel or settings menu, locate the "Date and Time" options, and adjust preferences, including time zone, format, and synchronization settings.