**TERM-1 N+ Assignment**

**Module 6**

**[Network security, Maintenance and Troubleshooting procedures]**

**BHARGAV DARJI**

**SOHO Networks**

1. What is SOHO network?

Small office/home office networks, or SOHO networks, are made to accommodate home offices' and small businesses' networking requirements.

2. What does SOHO mean networking?

In a small office or home office setting, a network that supports a few people and devices is set up and maintained. This type of networking is known as SOHO networking.

1. How does a SOHO network work?

Through the use of routers, switches, and wireless access points, a SOHO network links several devices (computers, printers, and phones). It enables resource sharing, including file sharing and internet communication, between various devices.

2. Issues with Soho Networking?

- Limited scalability

- Security vulnerabilities

- Limited IT support

- Potential for network congestion

1. How Small is the “S” in SOHO?

The "S" in SOHO typically means fewer than 10 employees or users, often including just a few people working from home or a small office.

1. SOHO Routers vs. Home Routers?

Small business-oriented routers with advanced features like VPN support, improved security, and increased performance are known as SOHO routers.

Home routers: Less sophisticated features and more basic security, ideal for home use. Simplified for ease of use.

**NAT & PAT**

1. What is NAT?

NAT (Network Address Translation) converts private IP addresses to a public IP address for internet access.

1. What is PAT?

PAT (Port Address Translation) is a type of NAT that maps multiple private IP addresses to a single public IP address using different ports.

1. Different between NAT & PAT?

NAT: Maps one private IP to one public IP.

PAT: Maps multiple private IPs to one public IP using different ports.

1. However, Will Nat work?

NAT works by changing the private IP addresses of devices within a local network to a public IP address before data is sent to the internet.

1. Explain NAT?

NAT hides private IP addresses behind a public IP address, allowing multiple devices on a local network to access the internet using one public IP.

1. What is different between Static & Dynamic NAT?

Static NAT: Fixed mapping between a private IP and a public IP.

Dynamic NAT: Dynamic mapping between private IPs and a pool of public IPs.

1. NAT stand for?

Network Address Translation

1. PAT stand for?

Port Address Translation

**Authentication and Access Control**

1. What Is Acl?

An ACL (Access Control List) is a set of rules used to control network traffic and limit access to resources.

1. What Are Different Types of Acl?

Standard ACL

Extended ACL

1. Explain Standard Access List?

A Standard ACL filters network traffic based on the source IP address only.

1. Explain Extended Access List?

An Extended ACL filters network traffic based on both source and destination IP addresses, ports, and protocols.

1. What Is Wildcard Mask?

A Wildcard Mask specifies which bits of an IP address should be matched and which can be ignored in an ACL.

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

Inbound: Traffic entering an interface

Outbound: Traffic leaving an interface

**WAN Technologies**

1.Fiber-optic communication

Fiber-optic communication uses light to transmit data over thin glass or plastic fibers, providing high-speed and long-distance data transfer.

1. What is Leased Line

A leased line is a private, dedicated communication line between two locations, typically used for internet or private network access.

1. Explain Circuit switching

Circuit switching establishes a dedicated communication path between two endpoints for the duration of a connection, like traditional telephone calls.

1. Explain Packet Switching

Packet switching breaks data into packets that are sent independently over the network and reassembled at the destination.

1. What is difference between leased line and broadband?

Leased Line: Dedicated, consistent bandwidth, private connection.

Broadband: Shared connection, variable speeds, public network.

1. How much is a 100mb Leased Line?

The cost of a 100Mb leased line varies by provider and location but typically ranges from $500 to $1,500 per month.

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

POTS Line: Plain Old Telephone Service, analog voice communication.

Leased Line: Dedicated digital communication line for data and voice.

1. What is the process of packet switching?

- Data is divided into packets.

- Packets are sent independently through the network.

- Packets are reassembled at the destination.

3. Difference between circuit switching and packet switching?

Circuit Switching: Dedicated path, continuous connection.

Packet Switching: Data sent in packets, shared network paths.

1. Practice on printer sharing

- Connect the printer to the network.

- Enable printer sharing in the operating system settings.

- Add the shared printer to other devices on the

5. Use of IIS [ Via "add and remove" feature from control panel. "appwiz.cpl" command]

- Open the Control Panel.

- Select "Add or Remove Programs" or "Programs and Features".

- Use the "appwiz.cpl" command.

**Communication technologies Cloud and Virtualization**

1. What is virtualization?

Virtualization is the creation of virtual versions of physical resources like servers, storage, and networks.

1. What are two types of virtualization in cloud?

Server Virtualization

Storage Virtualization

1. What are the two types of virtualization?

Hardware Virtualization

Software Virtualization

1. What is VMware virtualization technology?

VMware virtualization technology provides software for creating and managing virtual machines on physical servers.

1. What is the difference between cloud and virtualization?

Cloud: Delivers scalable, on-demand resources and services over the internet.

Virtualization: Creates multiple simulated environments from one physical hardware system.

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

- Cost Efficiency: Reduced hardware costs.

- Scalability: Easy to scale resources up or down.

- Resource Optimization: Better utilization of resources.

- Flexibility: Easier management and deployment of applications.

**Monitoring Tools**

1. Why are network monitoring tools used?

Network monitoring tools are used to track and analyze network performance, detect issues, and ensure reliable and secure operation.

1. Explain firewalls

Firewalls are security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.

1. Explain core switches

Core switches are high-capacity switches that operate at the core or backbone of a network, handling large amounts of traffic efficiently.

1. Explain client systems

Client systems are end-user devices, such as computers or smartphones, that access and use network resources and services.

1. What is network management?

Network management involves monitoring, maintaining, and optimizing a network's performance, reliability, and security.

1. Explain Event Viewer

Event Viewer is a Windows tool that logs system, security, and application events, helping administrators diagnose and troubleshoot issues

1. Practice "parental control" or "family safety" option in control panel

- Open Control Panel.

- Select "Parental Controls" or "Family Safety".

- Set up restrictions for user accounts to control and monitor children's computer usage.

**Network Security, Network vulnerabilities**

1. What are network vulnerabilities?

Network vulnerabilities are weaknesses in a network that can be exploited by attackers to gain unauthorized access or cause harm.

1. What are the types of network security attacks?

Phishing

Malware

DDoS (Distributed Denial of Service)

Man-in-the-Middle

SQL Injection

1. What is virus in network security?

A virus is a malicious software program that can replicate itself and spread to other devices, causing damage or stealing data.

1. 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.

1. Who is vulnerable in network security?

Any device, user, or system connected to a network can be vulnerable to security threats.

1. How do you assess vulnerability?

- Conducting scans and audits

- Reviewing security policies

- Testing with penetration tools

- Analysing network traffic

3. What are the principles of network security?

Confidentiality: Ensuring data privacy

Integrity: Ensuring data accuracy

Availability: Ensuring reliable access to data

Authentication: Verifying user identity

Authorization: Controlling access to resources

4.What is a firewall to use for?

A firewall is used to monitor and control incoming and outgoing network traffic based on security rules to protect against threats.

5.configure advanced firewall setting?

- Open Control Panel.

- Go to "Windows Defender Firewall".

- Select "Advanced Settings".

- Configure inbound and outbound rules as needed.

1. configure "date and time" option

- Open Control Panel.

- Select "Date and Time".

- Adjust settings for the current date, time, and time zone.