# Module 6.

# Network security, Maintenance and Troubleshooting procedures

# Topic: A SOHO Networks

1. What is SOHO network?

A: SOHO network means a network used in small office or home office.

2. What does SOHO mean networking?

A: SOHO – Small Office Home Office

1. How does a SOHO network work?

A: SOHO network connects devices like computers and printers for communication and resource sharing.

2. Issues with Soho Networking?

A: limited scalability, security, and bandwidth, wireless interference, reliability concerns, basic management features, single point of failure .

1. How Small is the “S” in SOHO?

A: SOHO is for limited devices in small local network.

2. SOHO Routers vs. Home Routers?

A: SOHO routers are for small offices with extra features. Home routers are simpler, designed for residential use.

# Topic: NAT & PAT

1. What is NAT?A: NAT is a way for many devices at home or in an office to share one internet address, keeping things private and saving addresses.

2. What is PAT?A: PAT lets multiple devices at home or in an office share one internet address by using different port numbers for each device.

3. Different between NAT & PAT?

A: NAT allows multiple devices to share a single public IP address. PAT is a specific type of NAT that assigns unique port numbers to each device, enabling them to share the same public IP address more effectively.

1. However, Will Nat work?A: NAT works by allowing multiple devices in a local network to share a single public IP address for accessing the internet, providing a layer of security and conserving public IP addresses.

1. What is different between Static & Dynamic NAT?A: Static NAT has a fixed one-to-one mapping of private to public IP addresses. Dynamic NAT assigns private addresses to a pool of public addresses, with mappings changing based on demand.

2. NAT stand for?A: Network Address Translation

3. PAT stand for?A: Port Address Translation

# Topic: Authentication and Access Control

1. What Is ACL?

A: ACL stands for Access Control List. It is a set of rules that decides what network traffic is allowed or denied based on specified conditions, helping control access and secure networks.

2. What Are Different Types of ACL?

A: Standard ACLs, Extended ACLs

1. Explain Standard Access List?A: Standard Access List regulates network access based only on source IP addresses, often used in routers to permit or deny traffic.

2. Explain Extended Access List?

A: Extended Access List controls network access based on source/destination IP, port numbers, and protocols.

1. What Is Wildcard Mask?

A: wildcard mask is a pattern used in networking to match multiple IP addresses with a single rule, indicating which parts of the address should be considered for matching by using 0s and 1s.

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

A: Inbound and Outbound

# Topic: WAN Technologies

1. Fiber-optic communicationA: Fiber-optic communication: Fast data transmission using light pulses in thin glass strands. High bandwidth, low signal loss, and immune to interference. Components: transmitter, optical fiber, amplifiers, receiver.

2. What is Leased Line ?

A: Leased line is a dedicated, not-shared communication line rented by a customer for reliable and guaranteed high-speed connections between two points, commonly used for private networks and internet access.

3. Explain Circuit switchingA: Circuit switching is Dedicated path for entire conversation, common in traditional telephony, fixed resources allocated.

1. Explain Packet Switching.

A: Packet switching sends data in small pieces over the network, reassembling them at the destination.

2. What is difference between leased line and broadband?A: Leased lines offer dedicated and consistent connections at a higher cost, ideal for businesses. Broadband provides shared and more affordable connections, commonly used by individuals and smaller businesses.

1. Difference between a POTS line and a leased line?A: POTS lines are for basic voice communication, typically for homes and small businesses. Leased lines are for data communication, providing higher capacity for business applications and networking.

2. What is the process of packet switching?

A: Packet switching breaks data into small packets, sends them independently to the destination, and reassembles them there. Efficient and adaptable, it's the basis of internet communication.

3. Difference between circuit switching and packet switching?

A: Circuit switching is a dedicated line for the entire conversation; fixed resources. Packet switching sends data in small packets, sharing resources dynamically; flexible and efficient.

# Topic: Communication technologies Cloud and Virtualization

1. What is virtualization?A: Virtualization creates virtual versions of physical computing resources, optimizing efficiency and flexibility in managing IT infrastructure.

2. What are two types of virtualizations in cloud?A: Server virtualization and network virtualization are two types of virtualizations in the cloud.

1. What is VMware virtualization technology?

A: VMware is a company specializing in virtualization technology, allowing multiple operating systems and applications to run on a single server or network.

1. What is the difference between cloud and virtualization?

A: Virtualization is creating virtual instances of computing resources, while the cloud is accessing shared resources over the internet as a service.

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

A: Virtualization in cloud computing provides better resource use, scalability, flexibility, cost savings, and simplified management.

# Topic: Monitoring Tools

1. Why are network monitoring tools used?

A: Network monitoring tools are used to observe and manage network performance, identify issues, and optimize efficiency.

2. Explain firewalls

A: Firewall is a security barrier and it monitors and controls network traffic, and protects against unauthorized access and cyber threats.

1. Explain core switches

A: Core switches serve as the backbone of a network, efficiently managing high-volume data traffic between different sections, crucial for large-scale networks.

2. Explain client switches

A: Client switches are devices that connect individual devices, like computers or printers, to a local network.

1. What is network management?

A: Network management is the administration and optimization of computer networks to ensure efficient operation.

2. Explain Event Viewer

A: Event Viewer is a Windows tool for viewing and troubleshooting system events and notifications.

# Topic: Network Security, Network vulnerabilities

1. What are network vulnerabilities?A: Network vulnerabilities are weaknesses that, if exploited, can lead to unauthorized access, data breaches, or service disruptions.

2. What are the types of network security attacks?A: Network security attacks include malware, phishing, denial of service (DoS), man-in-the-middle (MitM), SQL injection, cross-site scripting (XSS), social engineering, password attacks, and DNS spoofing.

1. What is virus in network security?

A: Network security virus is harmful software that attaches to legitimate programs, spreading and infecting systems by executing malicious code.

2. What is the difference between virus and antivirus?

A: A virus is malicious software that infects and harms computer systems, while antivirus is protective software designed to detect, prevent, and remove viruses from systems.

1. Who is vulnerable in network security?

A: Everyone connected to a network can be vulnerable in network security, including individuals, businesses, and organizations.

2. How do you assess vulnerability?

A: Vulnerability assessment involves identifying and evaluating security weaknesses in a system.

3. What are the principles of network security?

A: Network security principles include confidentiality, integrity, availability, authentication, authorization, non-repudiation, defense-in-depth, least privilege, security by design, and continuous monitoring.

4. What is a firewall to use for?

A: Firewall is used to control and monitor network traffic, safeguarding against unauthorized access and cyber threats.