Module 6 : (Network Security, Maintenance and Troubleshooting Procedures)

Topic : A SOHO Networks

1) A Small Office Home Office (SOHO) network refers to a type of a local area or LAN network connection designed for a small business.
2) Small Office Home Office. (SOHO)
3) SOHO networks can be a small wired ethernet LAN or a combination of wired and wireless computers.
4) Virtually all peer-to-peer home networking issues can be broken down into just three categories:

- No Internet access.
- No local network browsing.
- No network-resources access.

5) It typically involves a small number of employees, usually ranging from 1 to10.
6) While home networks shifted to predominantly Wi-Fi configurations years ago, SOHO routers continue to feature wired ethernet.

Topic : NAT & PAT

1) Nat is a way to map multiple private addresses inside a local network to a public ip address before transferring the information into the internet.
2) Pat is an extension of network address translation (NAT) that permits multiple devices on a LAN to be mapped to a single public ip address to conserve ip address.
3) The primary distinction is that NAT is used to map public IP addresses to

private IP addresses in a one-to-one or many-to-one relationship. On the other hand, PAT is a sort of NAT in which numerous private IP addresses (many-to-one) are mapped into a single public IP address via ports.

4) NAT works by having a firewall act as an intermediary for traffic entering and leaving the protected network.
5) Network Address Translation (NAT) is a process that enables one, unique ip address to represent an entire group of computers.
6) The main difference between dynamic NAT and static NAT is that static NAT allows a remote host to initiate a connection to a translated host if an access list exists that allows it, while dynamic NAT does not.
7) Network Address Translation. (NAT)

8) Port Address Translation. (PAT)

Topic : Authentication and Access Control

1) A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it.
2) Two types of Acl
- Standard Acl
- Extended Acl
3) Acls are a set of rules for regulating network traffic and minimizing network threats.
4) Extended access list is generally applied close to the source but not always.
5) A wildcard mask is similar to a subnet mask in that it uses the ANDing process

to identify which bits in an IPv4 address to match.

6) Access lists are applied either inbound(packets received on an interface, before routing), or outbound (packets leaving an interface, after routing).

Topic : WAN Technologies

1) Fiber-optic communication is a method of transmitting information from one place to another by spending pulses of infrared or visible light through an optical fiber.

2) A leased line is an allocated circuit between two points of communication.

3) Circuit switching is a method of implementing a telecommunications network in which two network nodes establish a dedicated communications

channel (circuit) through the network before the nodes may communicate.

4) Circuit switching is a method of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

5) A leased line contract guarantees businesses uninterruptible download and upload speeds, unlike broadband that competes for internet speed and bandwidth with other users.

6) Leased Line Connection Price at Rs 90000/mbps.

7) POTS line is voice -grade, dial up, while leased line is better quality, always on. POTS line is voice - grade , dial up ,

while leased line is better quality , always on.

8) Packet switching is the transfer of small pieces of data across various networks.

9) Circuit switching is a connection-oriented network technique (much like transmission control protocol or TCP), while packet switching is a connectionless network switching method.

10) From the Windows start button, type appwiz.cpl and choose open. Click Turn Windows features on or off. Scroll down and choose Internet Information Services, leave all of the defaults

selected but ensure the below options are enabled.

Topic : Communication Technologies Cloud and Virtualization

1) Virtualization is technology that you can use to create virtual representations of servers, storage, networks, and other physical machines.
2) Two types of virtualization in cloud

- Internal
- Externel

3) Two types of virtualization

- Storage virtualization
- Network virtualization

4) Virtualization software creates an abstraction layer over computer hardware that allows the hardware elements of a single computer—processors, memory, storage, and more— to be divided into multiple virtual computers, commonly called virtual machines (VMs).

5) Difference between cloud and virtualization

- While cloud computing is a model that enables users to access a shared pool of resources conveniently.
- Virtualization creates simulated versions of a machine's software or hardware components.

6) Virtualization gives you premium-level data security without the cost of physical firewalls.

Topic : Monitoring Tools

1) They help track various performance metrics like traffic, bandwidth utilization, availability, packet loss and much more.
2) A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
3) A core switch is the primary switch in a network, built to transfer data fast.

4) Client-server networks are computer networks that employ a dedicated computer to store data, manage/provide resources, and control user access (server).

5) Network management is the sum total of applications, tools and processes used to provision, operate, maintain, administer and secure network infrastructure.

6) The Event Viewer is a tool in Windows that displays detailed information about significant events on your computer.

Topic : Network Security, Network Vulnerabilities

1) A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach.
2) Types of network security attacks

- Man in the middle attack
- SQL injection
- Ransomware
- Phishing
- Denial of service attack
- Botnet
- Insider threat
- Computer worm

3) A computer virus is a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself.

4) Difference between virus and antivirus

- A virus is a computer program that can replicate itself and infect your computer.
- Antivirus software is used to prevent, detect, and remove malware like computer viruses, worms, spyware, Trojan horses, adware, and spyware.

5) Network security by accidentally accessing a file system without approval, reading confidential information on their monitor without

being aware of who is watching, and not verifying intruders in disguise.

6) Vulnerability assessments often employ automated testing tools such as network security scanners, showing the results in a vulnerability assessment report.

7) Principles of network security

- Confidentiality
- Integrity
- Authentication
- Availability
- Principle of least privilege
- Access control
- Malware
- Network security
- Complete meditation

8) Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic.

9) Go to the Control Panel and click "System and Security."

- Click on "Windows Firewall" and then click on "Advanced Settings."
- In the left pane, click on "Inbound Rules" or "Outbound Rules," depending on the type of traffic you want to allow.

10) Tap Settings to open the Settings menu.

- Tap Date & Time.
- Check that the correct Date, Time and Time Zone are selected.