Module 6. Network security, Maintenance and Troubleshooting procedures

Topic: A SOHO Networks

- Beginner Question

1. What is SOHO network?

ANS: A SOHO (small office home office) network is a small scale network used in home and small businesses.

2. What does SOHO mean networking?

ANS:SOHO stands for small office home office in network

- Intermediate Question

1. How does a SOHO network work?

ANS:A SOHO network work by connecting devices within a small office or home office to share resource like file printer internet access often using router.

2. Issues with Soho Networking?

ANS:Limited bandwidth, security vulnerabilities and potential challenges in managing network configuration for non technical user

- Advance Question

1. How small is the "S" in SOHO?

ANS: Small scale setup

2. SOHO Routers vs. Home Routers?

ANS

Feature	SOHO Router	Home Router
Purpose	Designed for small offices or home offices	Primarily intended for residential home use
Performance	Generally offers higher performance and features	Typically more basic in terms of performance and features
Network Size	Suitable for a small network with multiple users	Ideal for smaller networks with fewer users
Security Features	Enhanced security features, often with business-level security options	Basic security features for home use
VPN Support	Commonly includes VPN support for secure remote access	May have basic VPN support, often for consumer-grade use
Number of Ports	Typically comes with more LAN ports and additional features	Usually has a smaller number of ports for basic home use
Wireless Standards	Supports the latest wireless standards and technologies	May support basic wireless standards like Wi-Fi 5 (802.11ac)

Topic: NAT & PAT

- Beginner Question

1. What is NAT?

ANS: Network address translation is a method that enables multiple devices in a local network to share a single public ip address for internet communication.

2. What is PAT?

ANS: Port address translation. It is a variation of network address translation that maps multiple private ip address to single public ip address using different port. PAT help manage and conserve public ip address in a more efficient way

3. Different between NAT & PAT?

ANS:

function	NAT	PAT
Approach	In NAT translation of private IP address happens to public IP address	In PAT translation of private IP address happens to public IP address via ports
link	NAT is superset of PAT	PAT is subset of NAT it is a form of dynamic NAT
Ip address scheme	IPv4	IPv4 with port numbers
type	Static Dynamic Overloading /IP masqerading	Static Overloaded PAT

• Intermediate Question

1. However, Will Nat work?

ANS : NAT can temporarily work to enable multiple devices in a private network to share a single public ip address for internet access.

2. Explain NAT?

ANS:

Approach	In NAT translation of private IP address happens to public IP address
link	NAT is superset of PAT
Ip address scheme	IPv4
type	Static Dynamic Overloading /IP masqerading

• Advance Question

1. What is different between Static & Dynamic NAT?

ANS:

Static NAT	Dynamic NAT
One to one address mapping	Based on usage requirements and session flow
Fixed in time	Binding used and reused

2. NAT stand for?

ANS: Network address translation

3. PAT stand for?

ANS: Port address translation

Topic: Authentication and Access Control

• Beginner Question

1. What Is Acl?

ANS:Access control list a set of rule that defines what action are allows or denied on a particular resource such as files direction or network devices

2. What Are Different Types of Acl?

- Discretionary Access control list(DACL)
- System access control list(SACL)
- Standard Access List(ACL)
- Extended Access list (ECL)

• Intermediate Question

1. Explain Standard Access List?

ANS:ACL is list of rule applied to a router interface that filter traffic based on source ip address .it control access based on the source address of the packet making decision primarily on the sender ip address

2. Explain Extended Access List?

ANS: ECL is set of rules applied o router or firewalls that traffic based on various criteria including source and destination ip address, protocol, and port numbers. It offer more granual control compared to standard ACLs

• Advance Question

1. What Is Wildcard Mask?

ANS: A wildcard mask is numerical value used in conjunction with ACLs to specify which portions of ip address should be ignored when matching. It help define the rang of addresses affected by the ACL rule

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

- Inbound
- outbound

Topic: WAN Technologies

• Beginner Question

1. Fiber-optic communication

ANS: Fiber optic communication uses light pulses to transmit data through thin, flexible glass or plastic fiber, enable high speed, long distance communication with minimal signal loss

2. What is Leased Line?

ANS:A leased line is a dedicated ,fixed bandwidth communication link between two point, providing exclusive and consistent connectivity for businesses or organization.

3. Explain Circuit switching

ANS: Circuit switching is a communication method where a dedicated physical connection or circuit is established between two devices for the entire duration of their conversation, ensuring a constant link during communication session.

• Intermediate Question

1. Explain Packet Switching

ANS: Packet switching is a communication method where data is broken into packets each travelling independently across a network to reach its destination .this enable efficient use of network resources and supports flexible, shared communication paths

2. What is difference between leased line and broadband?

ANS:

Leased line	Broadband
Leased line connection have identical connection speeds upstream and downstream	Broadband connection usually have different speed
The bandwidth is reserved 24/7 band if customer not using it nobody else is	Throughput may be reduced at times when lots of other customer are trying to actively use their connection
Leased lines tend to have less data transmission delay latency	Lower data transmission because of low bandwidth higher latency and jitter
The router by which your data travels to your ISP may differ for leased line and broadband	Customer don't have control over data router

3. How much is a 100mb Leased Line?

ANS: The cost of a 100MB leased line can vary depending on several factors, including the location, service provider, and specific requirements of the customer. Leased line pricing is typically influenced by factors such as the length of the leased line, the level of service (symmetric or asymmetric), and any additional features or service level agreements (SLAs) that may be included.

• Advance Question

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

ANS:

Feature	POTS line	leased line
purpose	Voice calls	Data or voice communication
Dedication	Shared with other	Exclusive use
Bandwidth	Low	High
Reliability	Susceptible to interence	More reliable
Cost	Relatively low	Higher ,especially for bandwidth
Installation Time	Quick and easy	Longer
Use cases	Residential, small businesses	Larger enterprises ,data heavy application

2. What is the process of packet switching?

ANS: Packet switching is a method of data transmission where messages are broken into small packet each with its destination address. These packets travel independently across the network, taking different router and are reassembled at the destination. This approach improved efficiency and robustness compared to circuit switching as it allows for shared network resources and adaptability to varying traffic conditions.

3. Difference between circuit switching and packet switching?

ANS:

circuit switching	packet switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth wastage	No bandwidth wastage
No store and forward transmission	Supports store and forward transmission

4. Practice on printer sharing

ANS:DONE

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

ANS:DONE

Topic: Communication technologies Cloud and Virtualization

• Beginner Question

1. What is virtualization?

ANS: virtualization is the process of creating a virtual version of something such as a computer hardware platform operating system, storage device or network resources. This allows multiple instances of these resources to run independently on a signal physical machine optimizing resource utilization and enhancing flexibility in IT environments

2. What are two types of virtualization in cloud?

- Network virtualization
- Storage virtualization

• Intermediate Question

1. What are the two types virtualization ?

- Server virtualization

- Desktop virtualization

2. What is VMware virtualization technology?

ANS: it allows multiple operating systems and application to run on single physical machine simultaneously optimizing resource utilization and enhancing flexibility.

• Advance Question

1. What is the difference between cloud and virtualization?

ANS:

function	Cloud	virtualization
Serves as	A methodology that pools and automates virtual resources for on demand use	A technology that create multiple simulated environment form a single hardware system
configuration	Template based	Imaged based
Service type	laaS	saaS
lifespan	Short term	Long term
type	Public and private	Hardware and application
tenancy	Multiple tenants	Single tenant
scalability	high	limited

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

- Increased resource
- Utilization
- Cost efficiency
- Scalability
- Managing application

Topic: Monitoring Tools

• Beginner Question

1. Why are network monitoring tools used?

ANS: network monitoring tools used to track and analyze network performance, detect and troubleshoot issues, ensure optimal resource utilization and enhance overall network security

2. Explain firewalls

ANS: A firewall is a security barrier that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It helps protect a network by filtering and blocking unauthorized access while allowing legitimate communication

• Intermediate Question

1. Explain core switches

ANS:A core switches is a high capacity network switch that server as the central hub in network connecting multiple distribution switches and facilitating efficient data flow within a large scale network infrastructure

2. Explain client systems

ANS:A client system refers to a computer or device that interact with and request services or resource form a server within a network typically in a client server architecture

• Advance Question

1. What is network management?

   ANS: network management involves overseeing the operation, performance and security of functioning. It includes task such as monitoring, configuring and troubleshooting devices to maintain a reliable and efficient network

2. Explain Event Viewer

ANS: event viewer is a windows tool that logs and display system events, errors and warning. it help user and administrators identify issues monitor system activates and troubleshoot problem on a windows computer

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

Topic: Network Security, Network vulnerabilities

• Beginner Question

What are are network vulnerabilities?

ANS: network vulnerabilities are weakness in a computer network security like software flaws or misconfiguration that can be exploited by attackers to compromise the network's integrity confidentiality or availability

3. What are the types of network security attacks?

- Malware
- Phishing
- Denial of service and distributed
- Man in the middle attack
- SQL injection
- Cross sit scripting
- Brute force attack
- Zero day exploits
- Social engineering

• Intermediate Question

1. What is virus in network security?

ANS: A computer virus is a type of malicious software or malware that spreads between computer and cusses damage to data and software

2. What is the difference between virus and antivirus?

ANS:

Aspect	virus	antivirus
nature	Malicious software	Protective software
purpose	Causes harm, replicates	Detect prevent and remove
action	Spreads to other attacker	Scans identifies and quarantines
creation	Create by attacker	Developed by cyber security experts
goal	Exploits vulnerabilities	Protects against vulnerabilities
effect	Damages files or system	Safeguards files and system
functionality	destructive	defensive

• Advance Question

1. Who is vulnerable in network security?

ANS: users, administrators and developers

2. How do you assess vulnerability?

ANS: vulnerability assess involve system scanning and analyzing computer system network or application to identify potential weakness or flaws. Automated tools and manual techniques are used to evaluate the security posture and discover vulnerability allowing organization to prioritize and address potential risk

3. What are the principles of network security?

- Confidentiality
- Integrity
- Availability
- Authentication
- Authentication
- Accountability
- Non repudiation
- Least privilege
- Risk management
- Defense in depth

4. What is a firewall to use for?

- Network security
- Access control
- Packet filtering
- VPN security
- Logging and monitoring
- Protection against malware
- Load balancing
- Application layer security

5. configure advanced firewall setting?

:Done

6. configure "date and time" opt

:Done