classmate

Date

Page

Module-2

Q-1 What is SOHO network?

→ SOHO, or small office and Home office network, is a LAN (local Area network) that connects computers in a home office or remote office to a corporate network or access shared resources. It is ideal for small businesses with a small number of workers, typically ranging from 0 to 10. SOHO networks offer features like easy setup and efficient information sharing with multiple users within the organization.

Q-2 What is NAT?

→ Network Address Translation (NAT) is a service that enables private IP networks to use the internet and cloud. NAT translates private IP addresses in an internal network to a public IP address before packets are sent to an external network.

Q-3 What is PAT?

→ Port Address translation (PAT) is a network address translation (NAT) process that maps a network's private IPv4 addresses to a single public IP address. PAT differs from other NAT methods by using port numbers to map private IP addresses to a public IP address.

Q-4 Difference between NAT and PAT?

→

NAT	PAT
- Network Address Translation.	Port Address Translation.
- In NAT, private IP addresses are translated into the public IP address	In PAT, private IP addresses are translated into the public IP address via port numbers.
- NAT can be considered PAT's superset.	PAT is a dynamic NAT.
- NAT uses IPv4 address	PAT also uses IPv4 address but with port number.
- It have 3 types :- Static, Dynamic NAT and PAT/NAT overloading/IP masquerading.	It also have two types :- Static and overloaded PAT.

Q-5 What is ACL?

→ An Access Control list (ACL) is a set of rules that determines who can access a specific system resource. These lists are installed on routers or switches of users, managing network traffic. Each system resource has a security attribute identifying its ACL, which includes entries for every user. Common privileges include reading, writing, and execution of files. ACLs are also built into network interfaces and operating systems like Linux and Windows. They filter traffic based on source and destination.

Q-6 What are different types of ACL? What is Wildcard Mask?

→ There are two basic types of ACLs:-

1) File System ACLs :- It manages access to files and directories. They give users the instructions that establish user access permissions for the system and their privileges once the system has been accessed.

classmate
Date
Page

2. Networking Acls :- It control network access by defining traffic type and user permissions for network switches and routers, with network administrators predefining these rules, resembling a firewall in function.

⇒ A wildcard is a sequence of numbers that streamlines packet routing inside a proprietary network's subnets. It is also referred to as an inverse mask. The main reason behind this is that unlike a subnet mask on which, binary 1, is equal to a match, and binary 0 is not a match. However, in the wildcard mask, the opposite is true.

Q-7 Explain Circuit switching?

→ Circuit switching is a network configuration where a physical path is reserved for a single connection between two endpoints. It is commonly used in voice phone services, where the reserved circuit is used for a call duration, with fixed bandwidth and data transmission rate. It requires a physical connection between hosts for operation.

Q-8 Difference between leased line and broad band.

→

	Broadband	Leased Line
customer connectivity	Shared connection between customer premises and provider local exchange.	Dedicated connection between customer premises and provider local exchange.
Upload and Download Speed	Asymmetric speed i.e. higher download speed than upload speed.	Symmetric speed i.e. same download speed than upload speed.
Availability & performance SLA	Very less cases where SLA guarantee is provided by service provider.	SLA guarantee is provided by service provider for leased lines.
Performance	Lower than Leased Line	High performance
Bandwidth sharing	Bandwidth is shared across multiple customer.	Bandwidth is dedicated to a customer.
Reliability	Low	High
QoS	Limited or No QoS	Better QoS than Broadband
Cost	Cheaper	Costlier

Q-1 Difference between a POTS line and a Leased line.

→ Purpose and Usage :-

- POTS line are traditional analog telephone lines used primarily for voice communication. They are commonly used for residential phone service and small business.
- Leased lines are dedicated, exclusive connections used for data-intensive applications like office connections, business, etc.

→ Technology :-

- POTS line use analog technology to transmit voice signals.
- Leased line use various technology, including T1/E1 lines (which can carry both voice and data), fiber-optic cables, or other dedicated digital lines

→ Cost :-

- POTS line are generally more affordable and are suitable for basic voice communication needs.
- Leased line tend to be more expensive due to the dedicated and higher bandwidth nature of the service.

Q-10 Practise on printer sharing?

→ Steps :-

1) Connect the printer :-
- Ensure that the printer is connected to the computer that will act as the print server.

2) Enable printer sharing :-
- Right-click on the printer you want to share and select "Printer Properties".
- Navigate to the "Sharing" tab.
- Check the box that says "Share this printer".
- Assign a share name to the printer.

3) Configure permissions :-
- Click on the "Security" tab to set permissions for users who can access the shared printer.
- Add or modify user accounts and set appropriate permissions.
-

4) Access the shared printer :-
- On another computer on the same network, go to "Devices and Bluetooth printer".
- Click on "Add a printer" and select "Add a network, wireless or Bluetooth printer".
- Choose the shared printer from the list.

Q-11. use of IIS?

→ IIS is a window-based microsoft web server that exchanges static and dynamic web content, manages web applications using technologies like Asp.net and PHP, and uses HTTP, SMTP, and FTP protocols.

Outlined below are typical ways to use microsoft IIS server:-

- Website hosting
- Logging
- Request Filtering
- Native Support

Q-12 Create an FTP server.

→

1) Navigate to start > control panel > Administrative Tools > Internet Information Service (IIS) Manager.
2) Once the IIS console is open, expand the local server.
3) Right-click on sites, and click on Add FTP site.
4) In the Add FTP site window, type the FTP server name and the content directory path, and click next. The directory path should be the same as the one we set permissions to allow anonymous access.

Above, we used :- %SystemDrive%\Inetpub\ftproot

5) In the Binding and SSL settings window, type the IP address of the server. check the Start FTP site Automatically option. Choose SSL Based on constraint. Click Next.

6) Now, select Basic for authentication.

7) Click Finish. Now, the FTP site creation is complete.

Q-13 What is the difference between cloud and virtualization?

→ Scope :-

- Virtualization focuses on creating virtual instances of computing resources within a local infrastructure.
- Cloud computing involves delivering a wide range of computing services over the internet, which can include virtualized resources.

→ Deployment :-

- Virtualization is typically implemented within an organization's data center or on-premises infrastructure.

- Cloud computing services can be deployed locally or accessed over the internet from third-party providers.

→ Service Models :-

- Virtualization primarily deals with creating virtual instances of computing resources.
- Cloud computing encompasses a broader range of services, including IaaS, PaaS and SaaS.

Q-14 Why are network monitoring tools used?

→ Networking monitoring tools are used to ensure optimal network performance by tracking metrics such as bandwidth, latency, and security. They aid in early fault detection, troubleshooting, resource utilization optimization, security threat detection, compliance reporting and overall network health management. These tools enable proactive maintenance, capacity planning and cost-effective network management.

Q-15 What is ping?

→ A ping is an Internet program that allows user to verify the existence of a destination IP address and accept requests in computer network administration. It is also used diagnostically to ensure a host computer is operating, and can be used on any operating system with networking capability.

Q-16 What is traceroute?

→ Traceroute is a command - line utility that returns information about the communication route between two nodes on an Internet Protocol (IP) network. The utility sends out User Datagram Protocol (UDP) test packets and tracks their path as they travel from the system where the utility is running - the source - to the destination, which might be a server, router or other device on the network.

Q.7 What is nslookup?

→ Nslookup is the name of a program that lets users enter a host name and find out the corresponding IP address or domain name system (DNS) record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address.

Q.8 Explain Core Switches?

→ A core switch is the primary switch in a network, designed for fast data transfer and reliability. It sits at the top of the network structure, ensuring efficient data circulation across the network.

Key Aspects:-

- Structure
- Designed for efficiency and capacity
- Stability
- Prioritization
- Versability
- Adaptability

Q-19 What is network Management?

→ Network Management involves configuring, monitoring, and managing network performance, and is a platform used by IT and NetOps teams. It incorporates advanced analytics, machine learning, and intelligent automation for continuous optimization. As organizations adopt to a distributed work force, these systems are increasingly deployed in cloud and hosted environments.

Q-20 Explain Event Viewer?

→ Event viewer is a window tool that enables user to manage and monitor system events, errors, warnings, and informational messages, aiding system administrators, support personnel, and advanced users in diagnosing and resolving issues.

The main components and features of Event viewer :-

→ Event Logs:-
Application
Security
Setup
System

→ Views
Custom views
Windows Logs
Applications and services Logs

→ Event Types
Information
Warning
Error
Critical
Audit Success/Failure

→ Filtering and searching
→ Event Details
→ Actions

Event Viewer plays a crucial role in diagnosing system issues, tracking changes, and monitoring security-related events. It provides valuable insights into the health and performance of a Windows system, making it an essential tool for system administrators and advanced users.

Q-21 What are the types of network security attacks?

→ There are various types of attacks on network security :-

- Malware
- Virus
- Worm
- Man-in-the-middle
- Distributed Denial of Service (DDoS)
- Phishing
- IP spoofing
- Bot net
- Trojan horse
- Packet Sniffer

Q-22 Practice "parental control" or "family safety" options in the control panel?

→ Access family safety settings :-

- Open the "Control Panel" on your windows computer.
- Navigate to "User Accounts" and then select "Set up family safety for any user".

2) Create a family safety Account :-

- Sign in with a Microsoft account or create a new one.

- follow the prompts to set up a family group and add family members.

3. Configure family safety settings:-
- Once the family is set up, you can configure various settings for each family member, including web filtering, screen time limits, app and game restrictions, and activity reporting.

4. Web filtering:-
- Choose the appropriate level of web filtering to block inappropriate content.

5. Screen Time limits:-
- Set specific time limits for when each family member can use the computer.

6. App and Game Restrictions:-
- Control access to specific apps and games based on age appropriateness.

7. Activity Reporting:-
- Receive reports on your child's online activity, including websites visited and time spent on the computer.