**Network assignment**

1 What is network?

Two or more computer connected to each other for communication is called network.

2. List Common Network Components.

Desktop, switch, modem, router, server, hub, bridge.

3. Explain application of network.

Communication = email, video, instant message.

Sharing = files, software and data over the network.

Accessing the world wide web and other services.

4. What do you mean by Node?

Every device in a network Is known as node.

5. practice of simple file folder sharing.

1. Create a folder with the files you want to share.
2. Right-click the folder, select "Properties," and then choose the "Sharing" tab.
3. Click "Share" and choose who to share with. Adjust permissions.
4. Click "Share" and send the link or invite to others.
5. They can access and edit the shared folder as permitted.

6 List types of devices.

Switch, router, hub, access point, modem, firewall, bridge, gateway, load balancer, proxy server, network interface card.

7. Explain types of router.

Home Router: Connects multiple devices in a home network.

Wireless Router: Includes Wi-Fi for wireless connections.

Core Router: Used in large networks to manage traffic.

Edge Router: Connects a local network to external networks.

Virtual Router: Runs as software on a computer or server.

8. What is Difference between a LAN, MAN, WAN?

1. LAN (Local Area Network): Covers a small geographic area like a home, office, or campus. It's limited to a few kilometres and provides high data transfer rates.
2. MAN (Metropolitan Area Network): Spans a city or a large campus, covering a larger area than a LAN but smaller than a WAN. It offers moderate data transfer speeds.
3. WAN (Wide Area Network): Extends across large distances, often connecting cities or even countries. WANs provide lower data transfer rates compared to LANs and MANs due to longer distances and various network types involved.

10. Common Network Components

Switch, router, hub, access point, modem, firewall, bridge, gateway, load balancer, proxy server, network interface card.

11. Explain Wide Area Network

A Wide Area Network (WAN) is a network that covers a broad geographical area, often spanning cities, countries, or even continents. It connects multiple Local Area Networks (LANs) and Metropolitan Area Networks (MANs) over long distances.

12. Explain Network Backbone.

A network backbone, often referred to as a "backbone network," is the central infrastructure of a computer network. network backbone include high bandwidth capacity, reliability, and redundancy to minimize network downtime. It typically uses advanced networking equipment such as routers, switches, and Fiber-optic cables to provide fast and reliable data transmission.

13. Explain CAN.

CANs are designed to provide networking infrastructure within a specific area or campus, connecting various buildings, facilities, and departments.

14. Define Physical Network Topologies.

Physical network topologies refer to the physical layout or structure of interconnected devices and cables in a computer network.

15. Network Architecture: Peer-to-Peer.

Peer-to-Peer (P2P) network architecture is a decentralized networking model where every device or node on the network can act as both a client and a server, sharing resources and information directly with other devices.

16. Why we use Network and Devices.

1. Communication, Data Sharing, Access to Information, Collaboration, Resource Sharing, Remote Access, Entertainment, Automation and Control, Business Operation, Education.

17. Explain Switch?

A switch is a network device that operates at the data link layer (Layer 2) of the OSI model. It is primarily used to connect multiple devices within a local area network (LAN).

18. Define list of cables in use of network.

Ethernet Cable, Fiber Optic Cable, Coaxial Cable, Twisted Pair Cable, USB Cable, HDMI Cable, Power over Ethernet (PoE) Cable, Console Cable.

19. Explain Define Access point.

An Access Point (AP) is a networking device that allows wireless devices, such as laptops, smartphones, or tablets, to connect to a wired network, typically via Wi-Fi. APs act as a bridge between wireless clients and the wired LAN, providing a wireless connection to the network.

20. Which types of transmission modes in computer network.

There are three primary transmission modes in computer networks:

1. **Simplex:** Data flows in one direction only, like a one-way street. It's a unidirectional mode where one device is the sender, and the other is the receiver, with no capability to send data in the opposite direction. Examples include television and radio broadcasting.
2. **Half-Duplex:** Data can flow in both directions, but not simultaneously. Devices take turns sending and receiving, like a walkie-talkie, where one person talks, and the other listens, and they switch roles as needed.
3. **Full-Duplex:** Data can flow in both directions simultaneously, like a two-way street. Devices can send and receive data simultaneously, which is common in modern Ethernet networks and telephone conversations.

21. Practice on Remote Desktop connection

Done in lab.

22. Practice on remote assistance.

Done in lab.

23. Explain Repeater and router.

A **Repeater** is a network device used to extend the range of a wireless signal in a Wi-Fi network. It receives wireless signals and retransmits them to cover areas with weak or no signal.

A **Router** is a fundamental networking device that connects multiple networks and directs data between them. In a home or small office, it often serves as the gateway between the local network and the internet.

24. What is multiplexer?

A multiplexer, often abbreviated as "mux," is an electronic device used in digital and analog circuits to combine multiple input signals into a single output signal. It's also referred to as a "data selector".

25. Explain MODEM.

A modem, short for "modulator-demodulator," is a critical networking device that enables digital data to be transmitted over analog communication lines, such as telephone lines or cable systems.

26. Monitor "event viewer".

Event Viewer is a Microsoft Windows application used to view and analyse event logs on a local or remote computer.

27. Explain DHCP Dynamic host configuration protocol.

Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automatically assign IP addresses. It simplifies the management of IP addresses and minimizes configuration errors.

28. Application of DHCP with one example.

One common example of DHCP in action is within a typical home or small office network where multiple devices need to connect to the internet through a router. The router typically functions as a DHCP server.

29. Explain Domain naming Services.

Domain name services used to domain name to ip address or ip to domain name.

30. Application of DNS with one example.

One common example of DNS in action is website access. When you enter a domain name in a web browser, DNS translates that domain name into an IP address, allowing your computer to connect to the corresponding web server.

31. What are the 5 network topologies?

Ring, bus, star, mesh, tree.

32. What is Internet topology?

Internet topology refers to the structure and organization of the interconnected networks that make up the global internet. It describes how various networks, data centers, and routing systems are linked and connected to create the complex and vast network that enables global internet communication.

33. What is protocol.

A protocol is a set of rules and conventions that define how data is transmitted and received in a network or communication system.

34. What is the most common network topology?

The most common network topology used is star topology.

35. Explain star topology in networking?

Star Topology is a type of network configuration in which all devices are connected to a central hub or switch. The central hub acts as a distribution point for data, receiving data from one device and transmitting it to the intended destination device.

36. Explain Hybrid topology.

A Hybrid Topology is a network configuration that combines two or more different types of basic network topologies into a single interconnected network. It's done to leverage the strengths of different topologies and create a more robust and flexible network infrastructure.

37. What is physical and logical topology?

Physical topology refers to the actual physical layout and arrangement of network devices, cables, and connections in a network.

Logical topology, on the other hand, defines how data is transmitted and the path it takes in the network from one device to another, without considering the physical layout.

38. What are the types of logical topology?

There are two types of logical topology bus and ring.

39. What is OSI model explain?

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes and defines the functions of a computer or telecommunications network into seven distinct layers.

40. List of Application layer protocol.

HTTP, HTTPS, DHCP, DNS, FTP, POP3, SMTP, ICMP, TELNET, SNMP.

41. How many types of protocols are there?

There are many types if protocols such as Communication, network, transport, application, security, wireless, routing, VoIP.

42. What is the difference between TCP IP model and OSI model?

The OSI model has seven layers, while the TCP/IP model has four. The OSI model is more comprehensive, covering presentation and session layers, whereas the TCP/IP model is more operationally focused.

43. What is TCP IP networking?

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of networking protocols that form the foundation of the modern internet and most computer networks. It's a set of rules and conventions that govern how data is transmitted, received, and routed across networks.

44. What is a wired Internet connection?

A wired internet connection refers to a network connection that uses physical cables to transmit data between devices and a network infrastructure. This type of connection is also commonly referred to as a "wired network connection.

45. What are the disadvantages of wired networks?

Limited mobility, installation complexity, cost, security concerns, inflexibility.

46. Practice of Team viewer, Any Desk, Google Hangout, Skype, zoom.

Done in lab.

47. Download google chrome.

Done in lab.

48. configure "date and time" opting in control panel.

Done in lab,

49. What is TCP/IP?

TCP/IP stands for Transmission Control Protocol/Internet Protocol. It is a suite of networking protocols that form the foundation of the modern internet and most computer networks.

50. What is the full form of TCP/IP?

Transmission control protocol/ internet protocol.

51. List out the types of IP.

There are mainly two types : ipv4 & ipv6.

52. What is protocol?

A protocol is a set of rules and conventions that define how data is transmitted and received in a network or communication system.

53. DO a practical to set the tcp/ip in network adapter?

Done in lab.

54. Types of cables and connectors?

1. Ethernet Cable, Fiber Optic Cable, Coaxial Cable, Twisted Pair Cable, USB Cable, HDMI Cable.
2. RJ-45, BNC, USB, HDMI, VGA , DVI.

55. Explain twisted pair cable and shielded twisted pair cable.

UTP cables have no additional shielding around the twisted pairs.

STP cables have additional shielding to protect against electromagnetic interference.

56. Which of these cables connect computers to monitors?

VGA, DVI, HDMI are used to connect computers to monitors.

57. How do I connect to a shared printer?

1. Ensure Printer Sharing is Enabled > Share the Printer > Set Permissions > Find the Shared Printer > Add a Printer > Search for the Printer > Select the Shared Printer > Install the Printer Driver > Print a Test Page > Print to the Shared Printer.

58. Which cable that is commonly used to connect a computer to a printer?

USB cables are most widely used to connect to printer.

59. What are the different ports and connectors?

USB , HDMI, SATA, parallel, VGA, DVI, thunderbolt, audio port, ps2 port, firewire port, serial port, coaxial connector, Fiber optic connector,

60. How do I connect my laptop to my printer without cable?

Enable wi-fi on printer > connect laptop > install printer driver > print from your laptop.

61. Application and brief explanation of fiber optic cable and Coaxial cable.

Fiber optic cables use optical fibers to transmit data as light signals. They consist of a core (glass or plastic), which carries the data signals, and a cladding layer to reflect the light back into the core. Used in data center, telecommunication, cable television.

Coaxial cables consist of a central conductor (usually copper) surrounded by insulation, a metallic shield, and an outer insulating layer. Used in networking, cable television, surveillance system.

62. Which of following operates at the 5GHz frequency range?

Devices that operate at the 5GHz frequency range are typically associated with wireless networking, such as Wi-Fi.

63. What frequency does 802.11g use?

The 802.11g Wi-Fi standard operates in the 2.4GHz frequency range.

64.. What standard is compatible with 802.11a?

The 802.11a Wi-Fi standard is compatible with the 802.11g and 802.11n standards.

65. What Is Routing?

Routing is a combination of two process path discover and path selection.

66. How Routing Starts Up?

Routing begins with a routing table. This table contains information about various paths (or routes) in a network. Each route includes details such as network addresses, next-hop destinations, and associated costs or metrics.

67. What Is Hybrid Routing Protocol?

A hybrid routing protocol is a type of routing protocol that combines characteristics of both distance-vector and link-state routing protocols.

68. What Are the Range of Ad Values?

The Ad (administrative distance) values are used in networking to determine the reliability of a routing protocol. Lower administrative distances indicate a more trustworthy or preferred route.

69. What Is an Autonomous System?

An Autonomous System (AS) is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet.

70. Define Static Routing?

Static routing is a network routing method in which network administrators manually configure and maintain a fixed routing table on routers and network devices.

71. Explain Dynamic Routing?

Dynamic routing is a network routing method where routers and network devices use routing protocols to automatically exchange routing information and dynamically update their routing tables based on real-time changes in network conditions.

72. What is VLAN?

A VLAN, which stands for Virtual Local Area Network, is a method used to create separate, logically segmented networks within a physical local area network (LAN).

73. Which two benefits of creating VLANs?

Enhanced Network Security**:** VLANs isolate groups of devices, reducing the risk of unauthorized access and the spread of threats.

Efficient Network Management**:** VLANs simplify network organization based on roles or functions, streamlining management and optimizing performance by reducing broadcast traffic.

74. What is Dynamic VLAN?

Creating a vlan using multiple switch is called dynamic vlan.

75. What is Static VLAN?

Creating vlan in single switch called static vlan.

76. What is VLAN and INTERVLAN?

VLAN (Virtual Local Area Network) is a logical network segmentation for isolating groups of devices, enhancing security and network management. Inter-VLAN routing is the process of enabling communication between different VLANs, allowing data to flow between them, typically facilitated by a router or layer 3 switch.

77. What is trunk port?

Access port convert into trunk port in order to communicate switch to each other.

78. How to delete VLAN information from Switch?

To delete a VLAN, use a command like no vlan [VLAN\_ID].

79. What is SOHO network?

A SOHO network, which stands for "Small Office/Home Office" network, is a type of network commonly found in small offices, home-based businesses, or residential settings.

80. What does SOHO mean networking?

SOHO networking solutions are tailored to the specific needs of a relatively small number of users, providing essential network services such as internet access, file sharing, printing, and email.

81. How does a SOHO network w

ork?

A SOHO network connects devices in small offices or home offices, facilitated by a central router providing internet access via an ISP. This setup allows devices to communicate locally while enabling internet access. It employs a mix of wired and wireless connections, enabling device communication and resource sharing. The router's security features protect the network, and its configuration allows for simple and secure connectivity for small-scale businesses or home-based offices.

82. Issues with Soho Networking?

Addressing these issues typically involves implementing appropriate security measures, considering network upgrades as needed, and ensuring that network equipment and configurations meet the demands of the specific SOHO environment.

83. How Small is the “S” in SOHO?

The "S" in SOHO (Small Office/Home Office) typically refers to very small or micro-scale offices or home-based businesses. While there's no strict definition for the size of the "S," it generally encompasses settings with a limited number of employees, devices, and network needs.

84. SOHO Routers vs. Home Routers?

SOHO routers and home routers serve as the central point for connecting devices to the internet, their target audiences and feature sets differ. SOHO routers are better suited for small businesses or home offices with additional network requirements, while home routers are ideal for basic residential networking.

85. What is NAT?

NAT stands for Network Address Translation. It is a technology used in networking to allow multiple devices within a local network to share a single public IP address when connecting to the internet.

86. What is PAT?

PAT operates by mapping multiple private IP addresses to a single public IP address and using different source port numbers to distinguish traffic from different devices.

87. Different between NAT & PAT?

NAT primarily translates IP addresses, while PAT extends NAT by also translating port numbers, making it more suitable for environments where numerous devices need to access the internet simultaneously while sharing a single public IP address.

88. However, Will Nat work?

NAT helps manage the limited pool of public IP addresses and offers a basic level of network security by hiding the internal network structure from external entities on the internet.

89. What is different between Static & Dynamic NAT?

Static NAT provides a fixed, one-to-one mapping between internal and public IP addresses, while Dynamic NAT allows multiple internal devices to share a pool of public IP addresses, with the specific mapping changing dynamically as devices access the internet.

90. NAT stand for?

Network address translation.

91. PAT stand for?

Port address translation.

92. What Is Acl?

ACL stands for Access Control List. It is a set of rules or conditions used in computer networking and security to control and manage access to network resources

93. What Are Different Types of Acl?

There are mainly two types standard and extended.

94. Explain Standard Access List?

Standard Access Lists are best used in scenarios where basic traffic filtering based on source IP addresses is required without needing to consider the specific destination or traffic type.

95. Explain Extended Access List?

Extended Access Lists are valuable in situations where more advanced and granular traffic filtering is needed. Network administrators use Extended ACLs to define specific rules for permitting or denying traffic based on various factors, such as source and destination IP addresses, port numbers, and protocols.

96. What Is Wildcard Mask?

Wildcard masks are commonly used in access control lists (ACLs) to define rules for permitting or denying traffic based on source or destination IP addresses. They provide flexibility in specifying which parts of an IP address should be matched and which should be ignored when filtering network traffic.

97. Fiber-optic communication.

Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber.

98. What is Leased Line.

A leased line is a dedicated, point-to-point telecommunications line that provides a continuous, private connection between two locations.

99. Explain Circuit switching.

Circuit switching is a traditional method of communication that establishes a dedicated communication path between two devices for the duration of their conversation. Circuit switching was the dominant technology for voice communication, and it's known for its reliability and call quality.

100. Explain Packet Switching.

Packet switching is the foundation of the modern internet, allowing for the efficient, scalable, and flexible transmission of data and supporting various types of communication and services.

101. What is difference between leased line and broadband?

leased lines provide a dedicated, high-quality, and symmetrical connection suitable for businesses and critical applications, while broadband offers cost-effective, shared connectivity suitable for general internet use but with potentially varying speeds and quality due to shared resources.

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

POTS lines are traditional analog telephone lines primarily used for basic voice communication, whereas leased lines are dedicated, higher-capacity digital connections suitable for a range of data and communication needs, offering higher bandwidth and reliability.

103. What is the process of packet switching?

This process of breaking data into packets, routing them independently, and reassembling them at the destination provides flexibility, efficiency, and resilience, making packet switching the foundation of modern network communication, including the internet.

104. Difference between circuit switching and packet switching?

circuit switching is best suited for real-time, continuous communication like voice calls, where a dedicated path is needed for the duration of the conversation. Packet switching is ideal for the internet and data networks, providing efficient, adaptable, and versatile data transmission, accommodating various types of data and applications.

105. What is virtualization?

Virtualization is a technology that allows multiple virtual instances or environments to run on a single physical computer or server.

106. What are two types of virtualization in cloud?

Mainly two types of virtualizations are server and network virtualization.

107. What are the two types of virtualization?

Two forms of virtualization serve distinct purposes in modern computing, with hardware virtualization providing comprehensive isolation and resource allocation for multiple VMs, while container virtualization offers lightweight, portable, and scalable deployment of applications.

108. What is VMware virtualization technology?

VMware is a prominent virtualization technology company that offers a range of virtualization and cloud computing products and solutions. VMware's virtualization technology is primarily known for its server virtualization, although it also provides solutions for desktop, network, and cloud virtualization.

109. What is the difference between cloud and virtualization?

virtualization is a technology that allows for the efficient use of physical hardware by creating virtual instances, whereas cloud computing provides on-demand services over the internet, offering scalability, managed resources, and location independence.

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

By combining virtualization with cloud computing, organizations can leverage the advantages of both technologies to create flexible, efficient, and cost-effective IT environments that can adapt to changing business requirements.

111. What are network vulnerabilities?

Network vulnerabilities refer to weaknesses or flaws in a computer network's security that can be exploited by attackers to compromise the confidentiality, integrity, or availability of data and network resources.

112. Why are network monitoring tools used?

Network monitoring tools used for Visibility, Fault Detection, Performance Monitoring, Security, Capacity Planning, Resource Utilization, Quality of Service (QoS), Reporting and Analysis, Proactive Issue Resolution, Cost Management, Compliance and Reporting, User Experience.

113. Explain firewalls.

Firewalls play a crucial role in protecting networks from unauthorized access, cyberattacks, and other security threats. They are a fundamental component of network security and are used in a variety of network environments, from home networks to large enterprise infrastructures.

114. Explain core switches.

Core switches are a critical component of a computer network, serving as the backbone that connects various distribution switches, routers, and access switches. These switches are typically found in the core or center of the network topology and play a fundamental role in high-speed data routing and aggregation.

115. Explain client systems.

Client systems are a crucial component of any network infrastructure, serving as the endpoints where users interact with the digital world. Network administrators and IT teams manage client systems to ensure security, updates, and access to network resources while supporting the diverse needs of end-users.

116. What is network management?

It involves the planning, deployment, monitoring, optimization, and troubleshooting of network infrastructure to ensure that it meets the organization's requirements and operates efficiently.

117. Explain Event Viewer

Event Viewer is a built-in utility in Microsoft Windows operating systems that allows users to view and analyze event logs generated by the system, applications, and security-related activities. It provides detailed records of events, errors, warnings, and informational messages, helping users.

118. What are the types of network security attacks?

Some common network security attacks include: Malware, Phishing, DoS and DDoS Attacks, Man-in-the-Middle Attacks, Brute Force Attacks, Password Attacks, SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Zero-Day Exploits, Ransomware, Insider Threats, Drive-By Downloads, Botnets, DNS Spoofing and Cache Poisoning, Packet Sniffing, Eavesdropping.

119. What is virus in network security?

viruses that primarily target individual computers, network viruses are designed to spread and propagate within a network infrastructure.

120. What is the difference between virus and antivirus?

virus is a type of malware that poses a threat to computer systems, while antivirus software is a protective tool that helps defend against and eliminate viruses and other malware.

121. Who is vulnerable in network security?

network security, various entities and components can be considered vulnerable such as End Users, Devices and Endpoints, Network Infrastructure, Software and Applications, Data, Websites and Servers, Cloud Infrastructure, Insiders, Supply Chain, Unsecured IoT Devices.

122. How do you assess vulnerability?

Vulnerability assessment involves identifying, evaluating, and prioritizing weaknesses or potential entry points within a system or network that could be exploited by attackers.

123. What are the principles of network security?

Principles of network security includes Confidentiality, Integrity, Availability, Authentication, Authorization, Accountability, Non-repudiation, Defense in Depth, Least Privilege, Security Awareness and Training, Continuous Monitoring and Improvement, Compliance.

124. What is a firewall to use for?

Firewalls are a critical component of network security, providing a barrier between a trusted internal network and potentially untrusted external networks (like the internet). They play a key role in safeguarding data, preventing cyberattacks, and maintaining the integrity and availability of network resources.

Top of Form

125. configure advanced firewall setting?

Done in lab.

126. configure "date and time" option.

Done in lab.