|  |  |
| --- | --- |
| **1.** | **Define Piconet and Scatternet.** |
| **A** | Piconet:  A piconet is a network consisting of two or more Bluetooth devices that establish a connection to communicate with each other. One device act as a master and can connect up to seven other devices as slaves within a range of approximately 10 meters. The master device controls communication within the piconet.  Scatternet:  A network consisting of multiple Piconets that are connected to each other through shared devices, allowing communication between devices that are not in direct range of each other. |
| **2.** | **List Mobile Generations with their application** |
| **A** | 1G (First Generation):  The first-generation (1G) of mobile technology started in the 1980s, and its primary application was analog voice calling. It was a breakthrough in mobile communication technology, as it enabled people to communicate on-the-go with wireless devices.  2G (Second Generation):  The second-generation (2G) of mobile technology was introduced in the 1990s. Its primary applications were digital voice calls, text messaging (SMS), and basic data services such as mobile internet browsing, MMS (multimedia messaging service), and basic email.  3G (Third Generation):  The third-generation (3G) of mobile technology came into existence in the early 2000s, and its primary applications were high-speed mobile internet browsing, video calling, mobile TV, and online gaming.  4G (Fourth Generation):  The fourth-generation (4G) of mobile technology came into existence in the mid-2010s and was a significant upgrade to 3G. It provided high-speed internet connectivity, better voice quality, and faster data transfer rates, which enabled applications such as video conferencing, mobile gaming, streaming services, and mobile payments.  5G (Fifth Generation):  The fifth-generation (5G) of mobile technology is the latest advancement in mobile technology, and it offers a range of applications such as ultra-fast mobile internet browsing, high-quality video streaming, virtual reality (VR), augmented reality (AR), autonomous vehicles, and remote surgeries. It has the potential to transform industries such as healthcare, transportation, and manufacturing. |
| **3.** | **Draw the Bluetooth architecture and describe it’s working** |
| **A** | Piconet:  • Piconet is a Bluetooth network that consists of one primary (master) node and  seven active secondary (slave) nodes.  • Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or  stations within the distance of 10 meters.  • There can be only one primary or master station in each piconet.  • The communication between the primary and the secondary can be one-to-one  or one-to-many.  • All communication is between master and a slave. Slave-to-slave communication  is not possible.  • In addition to seven active slave station, a piconet can have upto 255 parked  nodes. These parked nodes are secondary or slave stations and cannot take part  in communication until it is moved from parked state to active state.    Scatternet:  • Scatternet is formed by combining various piconets.  • A slave in one piconet can act as a master or primary in other piconet.  • Such a station or node can receive messages from the master in the first piconet  and deliver the message to its slaves in other piconet where it is acting as master.  This node is also called bridge slave.  • Thus, a station can be a member of two piconets.  • A station cannot be a master in two piconets |
| **4.** | **List any four Network Connecting Devices.** |
| **A** | * Router * Switch * Hub * Modem * Gateway * Repeater * Bridges |
| **5.** | **Differentiate between Hub & Switch on the basis of layer, ports, device type, and speed.** |
| **A** | |  |  |  | | --- | --- | --- | | **Factor** | **Hub** | **Switch** | | Layer | Physical layer (Layer 1) | Data link layer (Layer 2) | | Ports | Fewer number of ports, typically 4-8 | More number of ports, typically 8-48 | | Device type | Passive device | Active device | | Speed | Slower speeds due to collisions and broadcast nature | Faster speeds due to switching and dedicated connections | |
| **6.** | **Describe functions of switch with its advantages and disadvantages** |
| **A** | A switch is a networking device that operates at the data link layer of the OSI model and connects multiple devices together in a local area network (LAN). Its main function is to direct network traffic to the intended recipient device based on its Media Access Control (MAC) address.  Functions of a switch:   1. Filtering: A switch filters network traffic and forwards data packets only to the intended recipient device. This reduces network congestion and improves network performance. 2. Learning: A switch automatically learns the MAC addresses of devices connected to it and builds a forwarding table. This allows it to direct network traffic to the correct device without broadcasting the data to all connected devices. 3. Forwarding: A switch forwards data packets to the correct device based on the MAC address in the forwarding table. 4. Switching: A switch creates a dedicated connection between the sender and receiver devices, which minimizes collisions and improves network performance.   Advantages of a switch:   1. Faster data transfer: A switch provides dedicated connections between devices, which reduces network congestion and improves network performance. 2. Better security: A switch can support VLANs, which allows network administrators to segment the network and control access to sensitive information. 3. More control: A switch provides greater control over network traffic, allowing administrators to prioritize and manage network traffic.   Disadvantages of a switch:   1. Higher cost: A switch can be more expensive than other networking devices, such as hubs. 2. Complexity: Configuring a switch can be more complex than other networking devices, and may require more advanced knowledge of networking concepts. 3. Limited scalability: A switch can only support a limited number of devices, and adding more devices may require the use of additional switches or other networking devices. |
| **7.** | **Draw & describe the connecting devices required for LAN for an organization using Tree topology.** |
| **A** | In a tree topology, multiple local area networks (LANs) are connected together in a hierarchical tree-like structure, with a central backbone connecting the different branches. Each branch can have multiple nodes or LAN segments connected to it, creating a larger network that can support more devices.  To connect the LANs in a tree topology, the following networking devices are typically required:   1. Switches: Switches are used to connect devices within each LAN segment, allowing them to communicate with each other. Each LAN segment typically has its own switch. 2. Routers: Routers are used to connect the different LAN segments together, allowing them to communicate with each other. The central backbone of the tree topology is typically connected by a router. 3. Hubs: Hubs can be used to connect multiple switches or devices together within a LAN segment. However, they are less commonly used in modern networks, as they can create network congestion and slow down network performance. 4. Network cables: Ethernet cables are used to physically connect devices to switches and routers within each LAN segment, as well as to connect the different LAN segments together. 5. Network interface cards (NICs): NICs are installed in each device to allow it to connect to the LAN and communicate with other devices. |
| **8.** | **Draw and describe architecture for network using tree topology for an office in 3-storey’s building** |
| **A** | A tree topology is a special type of structure in which many connected elements are arranged like the branches of a tree Here in the diagram the main switch is connected with three separate switches. For each floor separate switch is connected with multiple terminals. |
| **9.** | **Identify appropriate network topology and network connecting devices for following requirement. Draw network design for proposed network. An organization having its office in a building of 5 floor. Each floor it needs 20 PCs. There is one file server. Each floor has two print servers to facilitate printer capacity.** |
| **A** | For this scenario, a star topology with switches would be an appropriate choice. Here is a diagram of a possible network design:  ***\*I’ll update this with a diagram later\****  In this design, each floor has a dedicated switch to connect the 20 PCs and 2 print servers. These switches are connected to a central router, which allows the different LAN segments to communicate with each other and with the file server.  The file server is connected directly to the router, and can be accessed by all devices on the network.  Each device is equipped with a network interface card (NIC) that allows it to connect to the LAN and communicate with other devices. The print servers allow multiple users to access the printers located on each floor |
| **10.** | **Differentiate between ring and bus topology.** |
| **A** | |  |  |  | | --- | --- | --- | | **Feature** | **Ring Topology** | **Bus Topology** | | Transmission | Unidirectional | Bidirectional | | Network Length | Limited by the number of nodes | Limited by the signal strength | | Network Access | Token passing | CSMA/CD | | Failure | One node failure may affect the whole network | Any device can be removed without affecting the rest | | Collision | No collision | Collision may occur | | Network Cost | Expensive | Inexpensive | | Installation | Complex | Easy | | Scalability | Difficult | Easy | | Performance | Good with few nodes | Good with moderate number of nodes | |
| **11.** | **With suitable diagram describe:**  **a) Star Topology**  **b) Ring Topology.**  **c) Hybrid Topology.** |
| **A** | a) Star Topology  Star topology is a network topology where each individual piece of a network is attached to a central node (often called a hub or switch). The attachment of these network pieces to the central component is visually represented in a form similar to a star. The hub and hosts, and the transmission lines between them, form a graph with the topology of a star. Data on a star network passes through the hub before continuing to its destination. The hub manages and controls all functions of the network. It also acts as a repeater for the data flow.  6 Best Network Topologies Explained - Pros & Cons [Including Diagrams]  The star network is one of the most common computer network topologies.  **b) Ring Topology.**  A ring network is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node - a ring. Data travels from node to node, with each node along the way handling every packet.  Ring Topology  Ring topology refers to a specific kind of network setup in which devices are connected in a ring and pass information to or from each other according to their adjacent proximity in the ring structure. This type of topology is highly efficient and handles heavier loads better than bus topology.  **c) Hybrid Topology.**  When a topology is composed of two or more different topologies it is referred to as a hybrid topology. Hybrid topologies are **most-commonly encountered in larger enterprises** where individual departments have network topologies that different from another topology in the organization. Connecting these topologies together will result in a hybrid topology. As a consequence, the capabilities and vulnerabilities depend on the types of topologies that are tied together.  Hybrid Topology  A hybrid topology offers several advantages. It provides the flexibility to tailor the network to specific requirements and can be scaled as needed. For example, a department that requires a star topology for its workstations can be connected to another department that has a bus topology for its printers. The connection between these two topologies would create a hybrid topology that enables the departments to communicate with each other seamlessly. |
| **12.** | **List the advantages and disadvantages of bus topology** |
| **A** | Advantages:   1. Easy to install and expand. 2. Requires less cabling than other topologies. 3. Suitable for small networks with a limited number of nodes. 4. Inexpensive compared to other topologies. 5. Suitable for environments with low network traffic.   Disadvantages:   1. Performance can be impacted as more nodes are added. 2. Faults can be difficult to diagnose and isolate. 3. A single point of failure can bring down the entire network. 4. Limited cable length and number of nodes can be a constraint. 5. Security can be an issue as all nodes can see all data transmitted over the network. |

|  |  |
| --- | --- |
| **13.** | **Describe functions of router with its advantages and disadvantages** |
| **A** | A router is a network device that forwards data packets between computer networks. It is primarily responsible for directing data traffic to its intended destination on the internet. Here are some of the functions of a router:   1. Packet forwarding: The main function of a router is to receive data packets from one network and forward them to the correct destination on another network. 2. Path selection: Routers choose the best path for data packets to travel from the source to the destination network based on factors such as network congestion, speed, and reliability. 3. Traffic control: Routers can also control the flow of data packets, prioritizing more important traffic, and limiting less important traffic to optimize network performance. 4. Security: Routers can provide security by using firewalls, Virtual Private Networks (VPNs), and other security protocols to protect the network from unauthorized access or malicious activity.   Advantages of Routers:   1. Efficient data transfer: Routers can handle large amounts of data traffic and optimize network performance by selecting the best path for data packets to travel. 2. Network segmentation: Routers can be used to segment large networks into smaller, more manageable sub-networks, improving network efficiency and reducing the risk of network congestion. 3. Security: Routers can provide advanced security features such as firewalls, VPNs, and intrusion detection systems, making them an essential component of secure networks.   Disadvantages of Routers:   1. Cost: Routers can be more expensive than other network devices, especially for small businesses or home networks. 2. Complexity: Routers can be complex to set up and configure, requiring some level of technical expertise to manage. 3. Single point of failure: Since routers are critical to network connectivity, they can become a single point of failure if they malfunction, leading to network downtime and disruption. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | |  |  |  | | --- | --- | --- | | **Features** | **Router** | **Repeater** | | Functionality | Routes data packets between networks based on IP addresses | Regenerates weak signals in a network to extend the range | | Network topology | Can be used in any network topology | Typically used in point-to-point or star network topologies | | Range | Can cover long distances between networks | Limited to the range of the original signal | | Performance | Can prioritize and manage network traffic for optimal performance | Can introduce latency and delay in network traffic | | Security | Provides advanced security features such as firewalls and VPNs | Does not provide any security features | | Cost | Tends to be more expensive than repeaters | Relatively less expensive than routers | | Complexity | Can be complex to set up and configure | Easy to set up and use | |
| 15. | **Write following specification of smart hub:**  **a) Protocols**  **b) Radio Bands** |
| A | a) Protocols:  Smart hubs typically support a range of protocols, including Zigbee, Z-Wave, Wi-Fi, and Bluetooth. These protocols enable smart home devices to communicate with the hub and with each other, allowing for centralized control and automation of the home.  b) Radio Bands:  Smart hubs typically support multiple radio bands including 2.4 GHz and 5 GHz for Wi-Fi, as well as the 2.4 GHz band for Zigbee and Z-Wave. The use of multiple radio bands allows the smart hub to communicate with a variety of smart devices and maintain a stable and reliable connection. |
|  |  |

|  |  |
| --- | --- |
| 16. | State use of following devices.  a) Gateway.  b) Bridge. |
| Ans. | 1. Gateway : a gateway is a node (a device or a software) that acts as an entry point to a different network. It enables communication between devices on different networks, by forwarding data between them. 2. Bridge : a bridge is a device that connects two or more network segments, allowing them to communicate with each other as if they were part of the same network. |
| 17. | Why layering is used in ISO OSI Reference Model. |
| Ans. | * It breaks network communication into smaller, simpler parts that are easier to develop. * It facilitates standardization of network components to allow multiple vendor development and support. * Allows different types of network hardware and software to   communicate with each other.   * Prevents changes in one layer from affecting the other layers so that they can develop more quickly. * breaks network communication into smaller parts to make learning it easier to understand. |
| 18 | Describe Peer-to-Peer Processes in OSI Reference Model. |
| Ans. | Peer-to-peer refers to a communication model where two devices communicate directly with each other, without the need for a centralized server  At the Application layer (Layer 7), P2P processes can occur between two or more applications running on different devices.  At the Transport layer (Layer 4), P2P processes occur between two devices that want to communicate directly with each other, without going  through an intermediate device such as a router or switch  At the Network layer (Layer 3), P2P processes can occur between two devices that are on the same network segment, and want to communicate directly with each other  At the Data Link layer (Layer 2), P2P processes can occur between two devices that are directly connected to each other, such as two computers connected by an Ethernet cable. |
| 19. | State functions of Transport Layer of OSI model. |
| Ans | It acts as interface between the higher application oriented layers and the  network dependent protocol layers.  The Transport Layer ensures that data is delivered reliably, efficiently, and accurately across the network, while also managing the various connections between devices and applications. |
| 20. | List the protocols and devices of following OSI layers:  a) Network Layer.  b) Data Link Layer. |
| Ans | 1. protocols : - ip,ipx,appletalk   devices : routers   1. protocols : - Ethernet, Frame Relay, FDDI.   Devices : NIC,switches ,repeaters etc |
| 21. | Describe major functions of network layer in TCP/IP protocol suite. |
| Ans | The purpose of the Internet layer is to send source packets from  any network on the internetwork and have them arrive at the  destination independent of the path and networks they took to  get there.  ◼ Best path determination and packet switching occur at this  layer. |
| 22. | Describe functions of physical layer and data link layer of OSI model. |
| Ans | 1. data link layer   The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of transmission errors to the network layer  Is concerned with physical (as opposed to logical) addressing, network  topology, network access, error notification, ordered delivery of frames,  and flow control   1. physical layer   It concerns with transmitting raw bits over a communication channel  The physical layer deals with the physical characteristics of the  transmission medium  It defines the electrical, mechanical, procedural, and functional  specifications for activating, maintaining, and deactivating the physical  link between end systems (including media) |
| 23. | Describe encapsulation and decapsulation process with diagram. |
| Ans. | 1. Encapsulation :   Encapsulation wraps data with the necessary protocol information  (such as network address, MAC address, error checking codes, etc.)  before network transit.  Network must perform the 5 conversion steps:  ❖ Build the data.  ❖ Pack data for end-to-end transport (to form data segment)  ❖ Append (Add) the network addresses to the network header (to form a  datagram or packet) (includes control information).  ❖ Append (Add) the physical addresses to the data link header (to form a  frame)  ❖ Convert to bits for transmission     1. Decapsulation :   ❖ Decapsulation occurs at the receiving station.  ❖ Protocol information added at each layer is removed and processed  as the data ascends the OSI layer (from the physical to the application  layer)  ➢ When the data link layer receives the frame, it does the following:  ❖ It reads the physical address and other control information provided  by the peer data link layer.  ❖ It strips the control information from the frame, creating a datagram  (or packet).  ❖ It passes the datagram (or packet) up to the next layer, following  the instructions that appear in the control portion of the frame |
| 24. | Draw and explain layered architecture of OSI Reference Model.  OR  List all layers of OSI model & state its function |
| Ans. | 1. Physical :  * It concerns with transmitting raw bits over a communication channel * The physical layer deals with the physical characteristics of the transmission medium  1. Data link :  * The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of transmission errors to the network layer  1. Network :  * Provides connectivity and path selection between two end systems where routing occurs—these may be located on geographically separated networks  1. Transport :  * It acts as interface between the higher application oriented layers and the network dependent protocol layers. * the Transport Layer ensures that data is delivered reliably, efficiently, and accurately across the network, while also managing the various connections between devices and applications.  1. Session :  * The session layer defines how to start, control and end conversations (called sessions) between applications * This includes the control and management of multiple bidirectional messages using dialogue control  1. Presentation :  * The presentation layer ensures that information sent by the application layer of one system is readable by the application layer of another system  1. Application :  * This layer is closest to the user * It provides network service to the user’s application |
| 25. | Give the names of OSI layer where following protocols are relate/belong to:  a) SMTP  b) TCP-UDP  c) IP  d) PPP |
| Ans. | 1. Application layer(Layer 7) 2. Transport layer(Layer 4) 3. Network Layer(Layer 3) 4. Data Link Layer (layer 2) |
| 26. | Describe classes of IPv4 addresses with its range. |
|  | In IPv4, there are five classes of IP addresses: A, B, C, D, and E. Each class has a different range of IP addresses.  Class A addresses are used for large networks with a large number of hosts. The first octet of a Class A address is reserved for network ID, while the remaining three octets are used to identify hosts. The range of Class A addresses is 1.0.0.0 to 126.255.255.255, with a default subnet mask of 255.0.0.0.  Class B addresses are used for medium-sized networks. The first two octets of a Class B address are reserved for network ID, while the remaining two octets are used to identify hosts. The range of Class B addresses is 128.0.0.0 to 191.255.255.255, with a default subnet mask of 255.255.0.0.  Class C addresses are used for small networks. The first three octets of a Class C address are reserved for network ID, while the remaining octet is used to identify hosts. The range of Class C addresses is 192.0.0.0 to 223.255.255.255, with a default subnet mask of 255.255.255.0.  Class D addresses are used for multicast addressing. The first four bits of a Class D address are set to 1110, and the remaining 28 bits are used for identifying multicast groups. The range of Class D addresses is 224.0.0.0 to 239.255.255.255.  Class E addresses are reserved for experimental or research purposes. The first four bits of a Class E address are set to 1111, and the remaining 28 bits can be used for any purpose. The range of Class E addresses is 240.0.0.0 to 255.255.255.255. |
| 27. | Draw & explain TCP/IP protocol suite |
| Ans. | 1. Application Layer :   ◼ The designers of TCP/IP felt that the higher level protocols should include the session and presentation layer details.  ◼ They simply created an application layer that handles high-level protocols, issues of representation, encoding, and dialog control.  ◼ The TCP/IP combines all application-related issues into one layer, and assures this data is properly packaged for the next layer.   1. Transport Layer :   ◼ This layer deals with the quality-of-service issues of reliability, flow control, and error correction.  ◼ One of its protocols, the transmission control protocol (TCP), provides excellent and flexible ways to create reliable, wellflowing, low-error network communications.  ◼ TCP is a connection-oriented protocol. It dialogues between source and destination while packaging application layer information into units called segments   1. Internet / Network :   ◼ The purpose of the Internet layer is to send source packets from  any network on the internetwork and have them arrive at the  destination independent of the path and networks they took to  get there.  ◼ The specific protocol that governs this layer is called the Internet  protocol (IP).   1. Network Access :   ◼ The name of this layer is very broad and somewhat confusing.  ◼ It is also called the host-to-network layer.  ◼ It is the layer that is concerned with all of the issues that an IP  packet requires to actually make a physical link, and then to  make another physical link. It includes the LAN and WAN  technology details, and all the details in the OSI physical and  data link layers. |
| 28. | Compare OSI and TCP/IP reference model. |
| Ans. | |  |  | | --- | --- | | OSI reference model | TCP/IP network model | | 1) It has 7 layers | 1) It has 4 layers | | 2) Transport layer guarantees delivery of packets | 2) Transport layer does not guarantees delivery of packets | | 3) Horizontal approach | 3) Vertical approach | | 4) Separate presentation layer | 4) No session layer, characteristics are provided by transport layer | | 5) Separate session layer | 5) No presentation layer, characteristics are provided by application layer | | 6) Network layer provides both connectionless and connection oriented services | 6) Network layer provides only connection less services | | 7) It defines the services, interfaces and protocols very clearly and makes a clear distinction between them | 7) It does not clearly distinguishes between service interface and protocols | | 8) The protocol are better hidden and can be easily replaced as the technology changes | 8) It is not easy to replace the protocols | | 9) OSI truly is a general model | 9) TCP/IP cannot be used for any other application | | 10) It has a problem of protocol filtering into a model | 10) The model does not fit any protocol stack | |
| 29. | Explain configuration of TCP/IP protocol in network. / Write the steps for configuration of  TCP/IP protocol in network. |
| Ans. | Configuring TCP/IP protocol in a network involves assigning IP addresses to the devices on the network, configuring the subnet mask and default gateway, and configuring DNS servers   1. Determine the IP address range   Determine the range of IP addresses that will be used on the network, taking into account the number of devices that will be connected to the network.   1. Assign IP addresses   Assign a unique IP address to each device on the network, such as computers, printers, and routers.   1. Configure subnet mask   Configure the subnet mask for each device on the network. The subnet mask determines which portion of the IP address is used for the network ID and which portion is used for the host ID.   1. Configure default gateway   Configure the default gateway for each device on the network. The default gateway is the IP address of the router that connects the local network to the internet.   1. Configure DNS servers   Configure the DNS (Domain Name System) servers for each device on the network. DNS servers translate domain names into IP addresses, allowing devices to access websites and other network resources using human-readable names instead of IP addresses.   1. Test connectivity   Once the configuration is complete, test the connectivity between devices on the network to ensure that they can communicate with each other and access resources on the internet. |
| 30. | Describe the process DHCP server configuration |
| Ans | 1. Install the DHCP server role: Open the Server Manager and select "Add Roles and Features". Follow the prompts to install the DHCP server role   .   1. Configure the DHCP server settings: Once the DHCP server role is installed, open the DHCP Manager console. Right-click on the DHCP server and select "Properties" to configure settings such as DNS servers, lease duration, and DHCP options. 2. Create a DHCP scope: In the DHCP Manager console, right-click on "IPv4" and select "New Scope". Follow the prompts to create a DHCP scope, including the range of IP addresses to be assigned, subnet mask, default gateway, and lease duration. 3. Authorize the DHCP server: If the DHCP server is a member of an Active Directory domain, it must be authorized before it can provide DHCP services on the network. In the DHCP Manager console, right-click on the server and select "Authorize". 4. Configure DHCP options: In the DHCP Manager console, right-click on "IPv4" and select "Set Predefined Options". This allows you to configure options such as DNS servers, WINS servers, and other network settings to be automatically assigned to clients. 5. Configure DHCP reservations: DHCP reservations allow you to assign a specific IP address to a device based on its MAC address. In the DHCP Manager console, right-click on the scope and select "Add Reservation". 6. Activate the DHCP scope: In the DHCP Manager console, right-click on the scope and select "Activate". This enables the DHCP server to start assigning IP addresses to devices on the network. |
| 31. | What is static and dynamic IP address? Describe process of DHCP for assigning IP address. |
| Ans. | **Static :** A static IP address is manually assigned to a device and remains the same, even if the device is disconnected from the network. It is typically used for devices that require a fixed IP address, such as servers or network printers.  **Dynamic :** A dynamic IP address is automatically assigned to a device by a DHCP server. When a device connects to the network, it requests an IP address from the DHCP server. The DHCP server assigns an available IP address from a pool of addresses and configures other network settings, such as the subnet mask and default gateway.  *( for process kindly refer the question no 30.)* |