Internal Assessment Test 1 – Dec 2023
Solution & Scheme

Sub:	Computer Networks					Sub Code:	21CS52	Branch:	ISE	
Date:	18/12/2023	Duration:	90 min's	Max Marks:	50	Sem / Sec:	V/A, B, C			OBE

	Answer any FIVE FULL QUESTIONS	MARKS	CO	RBT
1 (a)	**Dialog control and synchronization are two responsibilities of the session layer in the OSI model. Which layer do you think is responsible for these duties in the Internet model? Justify your answer.** **Explanation – [3 Marks]** **Example – [2 Marks]** **Answer** In the OSI model, the session layer is responsible for dialog control and synchronization. The Internet model, also known as the TCP/IP model, has fewer layers than the OSI model. The Internet model consists of four layers: Application, Transport, Internet, and Network Access. The session layer (layer 5) is responsible for establishing, managing, synchronizing and terminating sessions between end-user application processes. **The main functions of the session layer are as follows −** • It works as a dialog controller. It allows the systems to communicate in either half-duplex or full-duplex mode of communication. • It is responsible for token management. Through this, it prevents the two users to simultaneously attempt the same critical operation. • It synchronizes communication. It adds synchronization points or checkpoints in data streams for long communications. This ensures that data streams up to the checkpoints are successfully received and acknowledged. In case of any failures, only the streams after the checkpoints have to be re-transmitted.	[5]	CO1	L3

(b) **What is the difference between network layer delivery and transport layer delivery?**

Difference – [1*5=5 Marks]

Answer

Transport Layer	**Network Layer**
The transport layer is the **fourth layer** of the OSI model.	The network layer is the **third layer** of the OSI model.
The transport layer mainly deals with logical communication between the processes running on different hosts.	The network mainly deals with logical communication between the hosts present on the same or different network.
The transport layer focuses on the process to process the delivery of data.	The network layer provides communication between hosts of different networks.
The transport layer receives the data from the upper layer and converts it into smaller parts known as **segments**.	The network layer divides the data received from the transport layer in the form of **packets**.
The transport layer performs the port addressing i.e. the addition of a port number to the header of the data.	The network layer adds the logical address i.e. IP address (Internet Protocol address) if the packet crosses the network boundary.
The transport layer maintains the order of data.	The network layer does not focus on maintaining the order of the data packets
The transport layer deals with the process-to-process communication or port-to-port communication.	The network layer deals with host-to-host communication.
The various protocols used in the transport layer are **TCP** (Transmission Control Protocol), **UDP** (User Datagram Protocol), etc.	The various protocols used in the network layer are **IPv4, IPv6, ICMP** (Internet Control Message Protocol), etc.
The various devices used in the transport are Segments, Load Balancers, etc.	The various devices used in the network layer are Routers, Brouters, etc.

[5] CO2 L1

2 (a) **What is the difference between half-duplex and full-duplex transmission modes?**

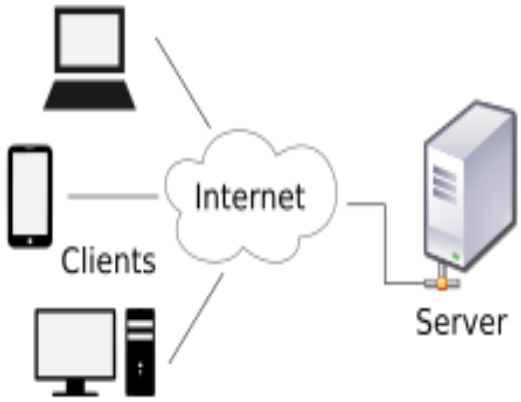
Difference – [1*5=5Marks]

Answer

Half Duplex	**Full Duplex**
The sender can send as well as receive the data but does one task at a time.	The sender can send as well as receive the data at the same time.
In Half duplex data flow is two-directional but one at a time.	In Full Duplex data flow is two directional and is simultaneous.
Usage of one channel while data transmission.	Usage of two channels while data transmission because of splitting of channel for simultaneous sending and receiving.

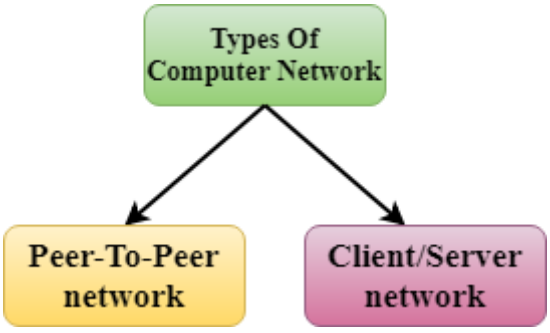
[5] CO1 L1

	Half-duplex mode provides less performance than full-duplex mode.	Full-duplex provides better performance than half-duplex mode.			
	In this there is less utilization of bandwidth during transmission.	In this bandwidth utilization is doubled.			
	Saving bandwidth as it is exchanged alternately between both sides on a single communication channel.	The entire capacity is utilized by splitting the communication channel so that the transmission in both directions is possible at the same time.			
	It is suitable when data needs to be sent in both directions, but in opposite directions.	It is suitable for communicating in both directions simultaneously and without delay.			
	In this, two systems are connected by a point-to-point link to transmit and receive signals. Both ends can transmit signals but one at a time.	In this, signals are transmitted in both directions; both end stations can receive and send data at the same time. Full duplex mode requires two independent channels for transmission, one for receiving the data and the other for transmitting the data.			
	Walkie-Talkies and Text message are example of half duplex mode.	Telephone, Instant Chat rooms, Audio Video Calls are example of full duplex mode.			
	Less efficient due to the need to alternate between sending and receiving data	More efficient as both devices can transmit data simultaneously			
	Collisions can occur when two devices try to transmit data at the same time	Collisions are less likely as both devices can transmit data simultaneously			
(b)	**Explain server client model?** **Explanation – [3 Marks]** **Diagram-[2Marks]** **Answer** A client-server model is a networking computing system design that illustrates a relationship between two or more computers, where the client computers request and receive services or resources from a powerful centralized server computer. It describes specific way devices access the information you store in servers. It also allows multiple clients to open applications or retrieve files from an individual server, which helps maintain consistency across all devices. Many companies across various industries use servers to store and access information, offering more processing power and providing more extensive storage space. This model can use a local area network (LAN) to connect a device to a server using a local path. These connections can be more secure but lack external capabilities, such as cloud computing. A wide area network (WAN) uses the internet to connect devices and servers. WAN networks allow for broader applications and access to more significant data collections, although these connections may need reinforcement in security measures.		[5]	CO1	L2



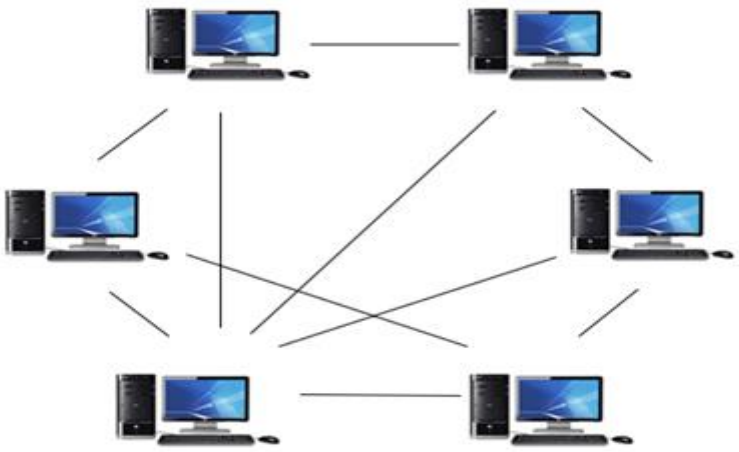
The functions of client-server networks can include

- Interacting with temporary and local storage
- Sending data requests to a server
- Interfacing between servers and users
- Completing database operations
- Connecting with other servers
- Processing user requests
- Writing files on servers
- Accessing server files
- Querying a database
- Creating interactive web applications

3 (a)	**Discuss Network architecture.** **Explanation – [2 Marks]** **Types– [1 Marks]** **Explanation-[2Marks]** **Answer** Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer. The two types of network architectures are used:  	[5]	CO1	L2

1. Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

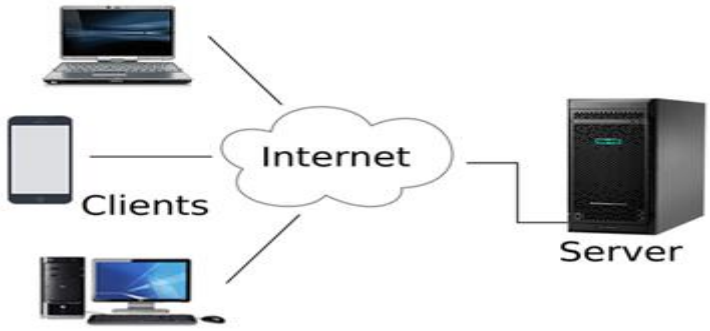
Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as **Server.**
- The central controller is known as a server while all other computers in the network are called **clients.**
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.

- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

(b) Differentiate between Connection-Oriented Versus Connectionless Service [5] CO1 L2

Explanation – [1*4=4Marks]

Example-[1Marks]

Answer

Connection oriented Service	**Connectionless Service**
Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
Connection-oriented Service is feasible.	Connection-less Service is not feasible.
In connection-oriented Service, Congestion is not possible	In connection-less Service, Congestion is possible.

	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.			
	Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.			
	Connection-oriented requires authentication.	Connection-less Service does not require authentication.			
	Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)			
4 (a)	**What are the advantages of fiber optics over copper as a transmission medium? Is there any downside of using fiber optics over copper?** **Explanation – [4 Marks]** **Example – [1 Marks]** **Answer** **1. Greater Bandwidth: -**Copper cables were originally designed for voice transmission and have a limited bandwidth. Fiber optic cables provide more bandwidth for carrying more data than copper cables of the same diameter. Within the fiber cable family, single mode fiber delivers up to twice the throughput of multimode fiber. **2. Faster Speeds: -**Fiber optic cables have a core that carries light to transmit data. This allows fiber optic cables to carry signals at speeds that are only about 31 percent slower than the speed of light—faster than Cat5 or Cat6 copper cables. There is also less signal degradation with fiber cables. **3. Longer Distances: -**Fiber optic cables can carry signals much farther than the typical 328-foot limitation for copper cables. For example, some 10 Gbps single mode fiber cables can carry signals almost 25 miles. The actual distance depends on the type of cable, the wavelength and the network. **4. Better Reliability: -** Fiber is immune to temperature changes, severe weather and moisture, all of which can hamper the connectivity of copper cable. Plus, fiber does not carry electric current, so it's not bothered by electromagnetic interference (EMI) that can interrupt data transmission. It also does not present a fire hazard like old or worn copper cables can. **5. Thinner and Sturdier: -**Compared to copper cables, fiber optic cables are thinner and lighter in weight. Fiber can withstand more pull pressure than copper and is less prone to damage and breakage. **6. More Flexibility for the Future: -** Media converters make it possible to incorporate fiber into existing networks. The converters extend UTP Ethernet connections over fiber optic cable. Modular patch panel solutions integrate equipment with 10 Gb, 40 Gb and 100/120 Gb speeds to meet current needs and provide flexibility for future needs. The panels in these solutions accommodate a variety of cassettes for different types of fiber patch cables.	[5]	CO1	L1

	7. Lower Total Cost of Ownership: - Although some fiber optic cables may have a higher initial cost than copper, the durability and reliability of fiber can make the total cost of ownership (TCO) lower. And, costs continue to decrease for fiber optic cables and related components as technology advances.			
(b)	**Explain the Wireless Transmission.** **Explanation – [2 Marks]** **Types– [3 Marks]** **Answer** Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas. When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data. A little part of electromagnetic spectrum can be used for wireless transmission. Wireless media can send data through radio waves or infrared light on computers. Infrared is a wireless media that transmits infrarouge signals. Broadcast radio is a wireless medium that carries radio signals over long distances, such as between towns, areas, and countries and short distances, as in an office or at home. Mobility is a method of radio transmission that is commonly used for mobile communications, especially modems and mobile telephones. Microwaves are high-speed signal transmission radio waves. Satellite communications is an environment where microwave signals are emitted from an earth-based station, the signals are amplified and signals are distributed through a wide variety of earth-based stations. Different types of Wireless Transmission Media are given as follows • **Light Transmission:** Light or optical signaling is the strongest electromagnetic spectrum that can be used for data transmission. This is achieved by LASER. Owing to the use of frequency light, the sender and recipient must both be in the line of sight exclusively in straight lines. Since the laser transmission is one-way, the laser and the photodetector have to be located at both ends of the contact. The laser beam normally is 1 mm long so that two receptors are correctly matched to each Laser Source. Lasers cannot penetrate barriers like walls, rain, or thick nebulae. Laser beams are often deformed by heat, the temperature of the atmosphere, or changes in trajectory temperature. • **Infrared Transmission:** In the visible spectrum of light and the microwaves, there is an infrared wave. The frequency range is from 300 GHz to 430 THz, and it has a wavelength of 700 NM to 1-mm. The infrared wave is used to communicate with very short distances like TV and remote contact. Infrared travels in a straight line and is thus inherently directional. Infrared is unable to penetrate wall-like barriers due to the high frequency spectrum. • **Microwave Transmission:** Electromagnetic waves over 100 MHz can be transmitted directly and signals can be sent to a specific station by beaming the	[5]	CO1	L2

waves. Because microwaves are moving on a straight line, all transmitters and receivers must be strictly on an aligned line of view. The waves focus on microwave antennas to build a pulse. Multiple antennas can be aligned, as shown in the above image. Microwaves do not penetrate walls like barriers, they have a higher frequency.

- **Radio Transmission:** The wavelength ranges from 1 mm-100,000 km, and the frequency varies from 3 Hz (extremely low frequency) to 300 GHz (extra high frequency), and it can pass through the walls and structures of a region. Six bands separate radio frequencies. Low-frequency radio waves are able to pass through the walls, while higher radio frequencies can pass through in a straight line and rebound. Further power is given by High Frequency Radio Waves.

- **Short Distance Wireless Media:** This can promote contact between a few meters and a few miles or kilometers. Wireless networks are a regular phenomenon. Here are the types of wireless short distance communications:

- **Bluetooth:** Bluetooth uses a Personal area network such as cell phone connection, laptop connection, portable cameras, etc.

- **Wi-max:** Wi-Max reflects worldwide microwave connectivity interoperability. The network is established in the Metropolitan Area Network (MAN) and is covered by the Wi-Max. Cable TV and DSL Internet are examples.

5(a) **What is the main difference between TCP and UDP?** [5] CO1 L1

Difference – [1*5=5 Marks]

Answer

TCP	**UDP**
TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data	UDP has only the basic error-checking mechanism using checksums.
An acknowledgment segment is present.	No acknowledgment segments.

	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.			
	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.			
	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).			
	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.			
	TCP is heavy-weight.	UDP is lightweight.			
	The TCP connection is a byte stream.	UDP connection is a message stream.			

(b) **Why are protocols needed?** [5] CO1 L1

Explanation – [3 Marks]

Example – [2 Marks]

Answer

In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.

Standardized protocols are like a common language that computers can use, similar to how two people from different parts of the world may not understand each other's native languages, but they can communicate using a shared third language. If one computer uses the Internet Protocol (IP) and a second computer does as well, they will be able to communicate — just as the United Nations relies on its 6 official languages to communicate amongst representatives from all over the globe. But if one computer uses IP and the other does not know this protocol, they will be unable to communicate.

In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level.

Protocols are basically needed because it's important for the receiver to UNDERSTAND the sender. In computer communications, protocols also make sure the message gets to its destination properly, in entirety, and without distortion.

6 (a) **What are headers and trailers, and how do they get added and removed?** [5] CO1 L1

Explanation – [3 Marks]

Example – [2 Marks]

	Answer Data added to the front is called a header, while data added to the end is called a trailer. When information is received by a host, the process is reversed. Headers and trailers are removed as the data moves back up the layers until eventually the original information is left for the application to use. Encapsulation marks where a packet, or unit of data, begins and ends. The beginning part of a packet is called the header, and the end of a packet is called the trailer. The data between the header and trailer is sometimes referred to as the payload 			
(b)	**What are the responsibilities of the data link layer in the Internet model? Explanation – [3 Marks]** **Example – [2 Marks]** **Answer** The data link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data. Its major role is to ensure error-free transmission of information. DLL is also responsible for encoding, decode and organizing the outgoing and incoming data. This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers. • The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the underlying physical layer. • **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link. • **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.	[5]	CO1	L1

	• **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link. • **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check. • **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame. • **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.			
7 (a)	**What are the concerns of the physical layer in the Internet model?** **Explanation – [3 Marks]** **Example – [2Marks]** **Answer** Physical layer in the OSI model is the lowest layer of the OSI reference model. It is responsible for sending raw bits from one computer to another computer over a network. It does not deal with the data of these bits and is majorly concerned with the setup of physical connection to the network. It plays the role of interacting with actual hardware and signaling mechanisms. It's the only layer of the OSI network model that deals with physical connectivity and is responsible for establishing, maintaining, and deactivating the physical connection of two different computing devices in a network. This layer defines the hardware equipment, topologies, cabling, modes of transmission, wiring, frequencies, pulses used to represent binary signals, etc. The physical layer is the first layer of the Open System Interconnection Model (OSI Model). The physical layer deals with bit-level transmission between different devices and supports electrical or mechanical interfaces connecting to the physical medium for synchronized communication.	[5]	CO1	L1
(b)	**Explain TCP/IP Reference Model.** **Explanation – [3 Marks]** **Diagram– [2 Marks]** **Answer**	[5]	CO1	L2

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defences) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for "Transmission Control Protocol" and IP stands for "Internet Protocol".

- The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer** −It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.

- **Internet Layer** −It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.

- **Transport Layer** − It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer** − This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

- The following diagram shows the layers and the protocols in each of the layers –