USN

INTERNAL ASSESSMENT
TEST – I

Sub	INTERNET OF THINGS							Code	22BETCK25
Date	06/07/2023	Duration	90 mins	Max Marks	50	Sem	II	Branch	

Answer any 5 full questions

	—	Marks	CO	RBT
1	Explain the classification of sensors.	[10]	CO2	L2
2	Explain the different connection types and network topologies in detail.	[10]	CO1	L3
3	Explain the following i) IoT versus M2M ii) IoT versus CPS iii) IoT versus WoT.	[10]	CO1	L3
4	With a neat diagram explain the functional blocks of a typical sensor node in IoT	[10]	CO1	L2
5	Discuss the highlights of the seven layers of the OSI stack.	[10]	CO2	L2
6	What are the various IoT connectivity terminologies? Differentiate between sensors, transducers and actuators.	[10]	CO2	L3

Faculty Signature CCI Signature HOD Signature

USN

INTERNAL ASSESSMENT
TEST – I

Sub	INTERNET OF THINGS							Code	22BETCK25
Date	06/07/2023	Duration	90 mins	Max Marks	50	Sem	II	Branch	

Answer any 5 full questions

		Marks	CO	RBT
1	Explain the classification of sensors.	[10]	CO2	L2
2	Explain the different connection types and network topologies in detail.	[10]	CO1	L3
3	Explain the following i) IoT versus M2M ii) IoT versus CPS iii) IoT versus WoT.	[10]	CO1	L3
4	With a neat diagram explain the functional blocks of a typical sensor node in IoT	[10]	CO1	L2
5	Discuss the highlights of the seven layers of the OSI stack.	[10]	CO2	L2
6	What are the various IoT connectivity terminologies? Differentiate between sensors, transducers and actuators.	[10]	CO2	L3

Faculty Signature CCI Signature HOD Signature

Scheme Of Evaluation

Internal Assessment Test I – July 2023

Sub:	INTERNET OF THINGS							Code:	22BETCK25
Date:	06/07/2023	Duration:	90 mins	Max Marks:	50	Sem:	II	Branch:	

Note: Answer 5 Questions

	Description	Marks Distribution		Max Marks
1	Explain the classification of sensors.		10	10
	• Based on the power requirement • sensor output, and • property to be measured	4 3 3		
2	Explain the different connection types and network topologies in detail.		10	10
	• Point-to-point and Point-to-multipoint connection. • Star, Mesh, Bus, and Ring topologies	4 6		
3	Explain the following i) IoT versus M2M ii) IoT versus CPS iii) IoT versus WoT.		10	10
	• IoT versus M2M • IoT versus CPS • IoT versus WoT.	4 3 3		
4	With a neat diagram explain the functional blocks of a typical sensor node in IoT.		10	10
	• Block diagram • Explanation	6 4		
5	Discuss the highlights of the seven layers of the OSI stack.		10	10
	• Block diagram • Explanation	5 5		

—

6	What are the various IoT connectivity terminologies? Differentiate between sensors, transducers and actuators.		10	10
	• IoT connectivity terminologies • Differentiate between sensors, transducers and actuators	5 5		

CMR INSTITUTE OF TECHNOLOGY
DEPT OF ECE
INTERNET OF THINGS
INTERNAL ASSESSMENT TEST –1
06-07-2023
SOLUTIONS

Q.No.	Question	Marks
1	i) Explain the classification of sensors.	10
Sol	The various sensors can be classified based on: 1) power requirements, 2) sensor output, and 3) property to be measured.	
	<u>Power Requirements:</u> The way sensors operate decides the power requirements that must be provided for an IoT implementation. Some sensors need to be provided with separate power sources for them to function, whereas some sensors do not require any power sources. Depending on the requirements of power, sensors can be of two types. **(i) Active:** Active sensors do not require an external circuitry or mechanism to provide it with power. It directly responds to the external stimuli from its ambient environment and converts it into an output signal. For example, a photodiode converts light into electrical impulses. **(ii) Passive:** Passive sensors require an external mechanism to power them up. The sensed properties are modulated with the sensor's inherent characteristics to generate patterns in the output of the sensor. For example, a thermistor's resistance can be detected by applying voltage difference across it or passing a current through it.	4
	<u>Output:</u> The output of a sensor helps in deciding the additional components to be integrated with an IoT node or system. Typically, almost all modern-day processors are digital; digital sensors can be directly integrated to the processors. However, the integration of analog sensors to these digital processors or IoT nodes requires additional interfacing mechanisms such as analog to digital converters (ADC), voltage level converters, and others. Sensors are broadly divided into two types, depending on the type of output generated from these sensors, as follows. **(i) Analog:** Analog sensors generate an output signal or voltage, which is proportional (linearly or non-linearly) to the quantity being measured and is continuous in time and amplitude. Physical quantities such as temperature, speed, pressure, displacement, strain, and others are all continuous and categorized as analog quantities. For example, a thermometer or a thermocouple can be used for measuring the temperature of a liquid (e.g., in household water heaters). These sensors continuously respond to changes in the temperature of the liquid. **(ii) Digital:** These sensors generate the output of discrete time digital representation	3

	(time, or amplitude, or both) of a quantity being measured, in the form of output signals or voltages. Typically, binary output signals in the form of a logic 1 or a logic 0 for ON or OFF, respectively are associated with digital sensors. The generated discrete (non-continuous) values may be output as a single “bit” (serial transmission), eight of which combine to produce a single “byte” output (parallel transmission) in digital sensors. **<u>Measured Property:</u>** The property of the environment being measured by the sensors can be crucial in deciding the number of sensors in an IoT implementation. Some properties to be measured do not show high spatial variations and can be quantified only based on temporal variations in the measured property, such as ambient temperature, atmospheric pressure, and others. Whereas some properties to be measured show high spatial as well as temporal variations such as sound, image, and others. Depending on the properties to be measured, sensors can be of two types. **(i) Scalar:** Scalar sensors produce an output proportional to the magnitude of the quantity being measured. The output is in the form of a signal or voltage. Scalar physical quantities are those where only the magnitude of the signal is sufficient for describing or characterizing the phenomenon and information generation. Examples of such measurable physical quantities include color, pressure, temperature, strain, and others. A thermometer or thermocouple is an example of a scalar sensor that has the ability to detect changes in ambient or object temperatures (depending on the sensor’s configuration). Factors such as changes in sensor orientation or direction do not affect these sensors (typically). **(ii) Vector:** Vector sensors are affected by the magnitude as well as the direction and/or orientation of the property they are measuring. Physical quantities such as velocity and images that require additional information besides their magnitude for completely categorizing a physical phenomenon are categorized as vector quantities. Measuring such quantities are undertaken using vector sensors. For example, an electronic gyroscope, which is commonly found in all modern aircraft, is used for detecting the changes in orientation of the gyroscope with respect to the Earth’s orientation along all three axes.	3

2	Explain the different connection types and network topologies in detail.	10

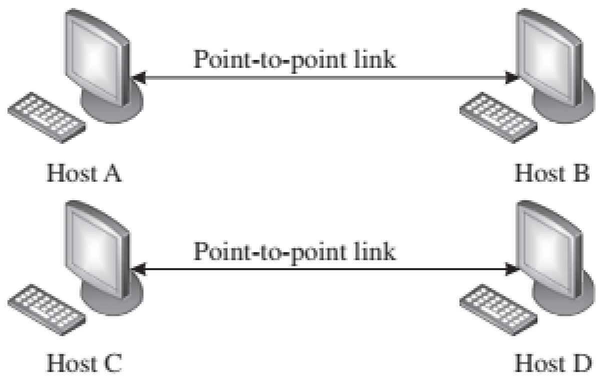
Sol:

<u>CONNECTION TYPES</u>

Depending on the way a host communicates with other hosts, computer networks are of two types namely ***Point-to-point and Point-to-multipoint.***

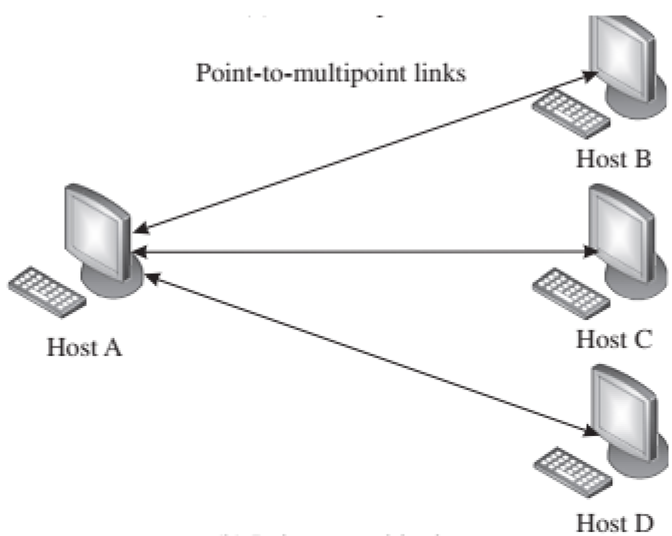
4

(i) **<u>Point-to-point:</u>** Point-to-point connections are used to establish direct connections between two hosts. Day-to-day systems such as a remote control for an air conditioner or television is a point to point connection, where the connection has the whole channel dedicated to it only. These networks were designed to work over duplex links and are functional for both synchronous as well as asynchronous systems. Regarding computer networks, point to point connections find usage for specific purposes such as in optical networks.



<u>Fig 1: Point-to-Point</u>

(i) **<u>Point-to-multipoint:</u>** In a point-to-multipoint connection, more than two hosts share the same link. This type of configuration is similar to the one-to-many connection type. Point-to-multipoint connections find popular use in wireless networks and IP telephony. The channel is shared between the various hosts, either spatially or temporally. Point-to-multipoint connections find popular use in present-day networks, especially while enabling communication between a massive number of connected devices.

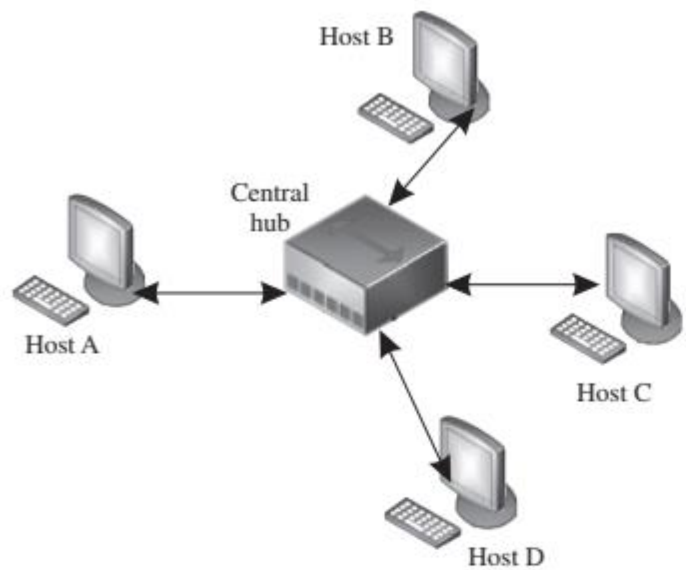


<u>Fig 2: Point-to-multipoint</u>

<u>PHYSICAL TOPOLOGY</u>

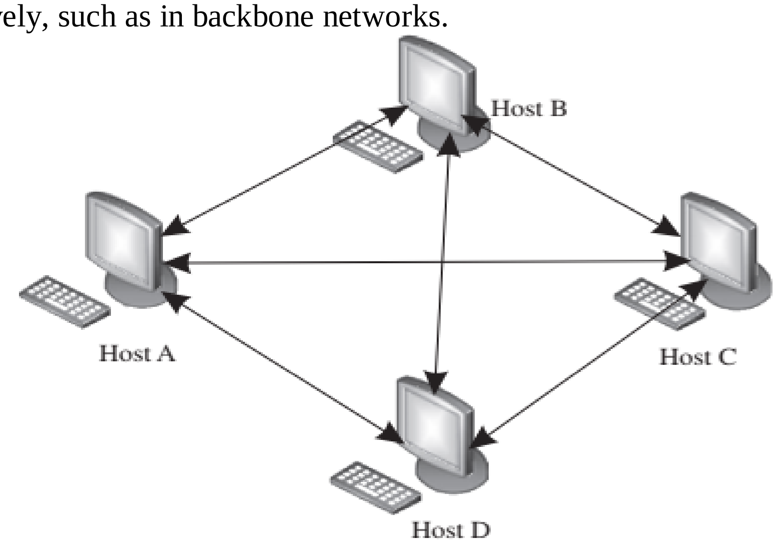
Depending on the physical manner in which communication paths between the hosts are connected, computer networks can have the following four broad topologies—: Star, Mesh, Bus, and Ring.

(i) **<u>Star:</u>** In a star topology, every host has a point-to-point link to a central controller or hub. The hosts cannot communicate with one another directly; they can only do so through the central hub. The hub acts as the network traffic exchange. as there are fewer links (only one link per host), this topology is cheaper and easier to set up. The main advantages of the star topology are easy installation and the ease of fault identification within the network. the main disadvantage of this topology is the danger of a single point of failure. If the hub fails, the whole network fails. 6



<u>Fig 3: Star Topology</u>

(ii) **<u>Mesh:</u>** In a mesh topology, every host is connected to every other host using a dedicated link (in a point-to-point manner). This implies that for n hosts in a mesh, there are a total of $n(n-1)/2$ dedicated full duplex links between the hosts. This massive number of links makes the mesh topology expensive. Mesh networks are used very selectively, such as in backbone networks.



<u>Fig 4: Mesh Topology</u>

Advantages of Mesh Network

1. Robustness and Resilience of the system. Even if a link is down or broken, the network is still fully functional as there remain other pathways for the traffic to flow through.
2. Security and Privacy of the traffic as the data is only seen by the intended recipients and not by all members of the network.
3. Reduced data load on a single host, as every host in this network takes care of its traffic load.

(iii) Bus: A bus topology follows the point-to-multipoint connection. A backbone cable or bus serves as the primary traffic pathway between the hosts. The hosts are connected to the main bus employing drop lines or taps. There is a restriction on the length of the bus and the number of hosts that can be simultaneously connected to the bus due to signal loss over the extended bus. The main drawback of this topology is the difficulty in fault localization within the network.

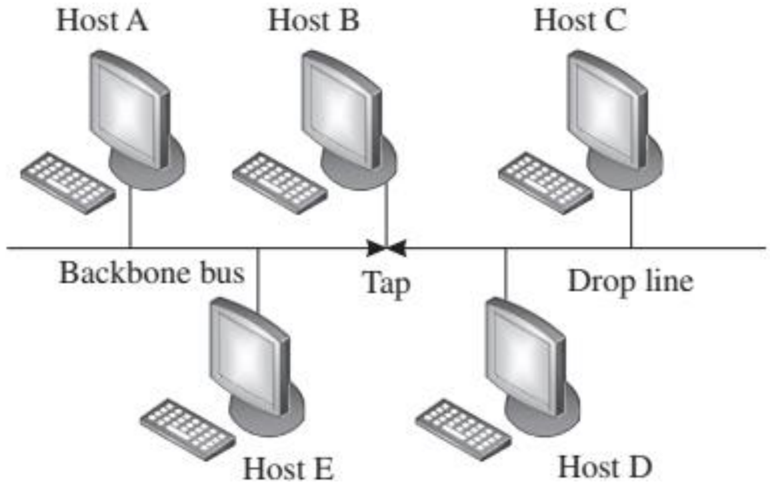


Fig 5: Bus Topology

(iv) Ring: A ring topology works on the principle of a point-to-point connection. Here, each host is configured to have a dedicated point-to-point connection with its two immediate neighboring hosts on either side of it through repeaters at each host. The repetition of this system forms a ring. The repeaters at each host capture the incoming signal intended for other hosts, regenerates the bit stream, and passes it onto the next repeater. Fault identification and set up of the ring topology is quite simple and straightforward.

The main disadvantage of this system is the high probability of a single point of failure. If even one repeater fails, the whole network goes down.

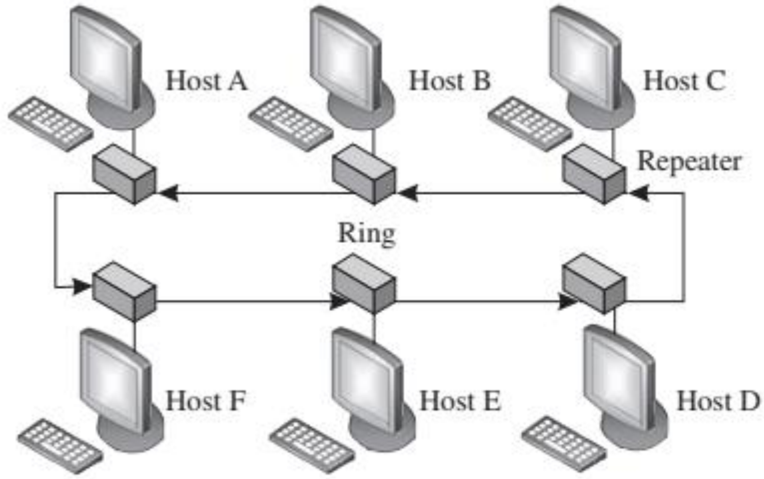


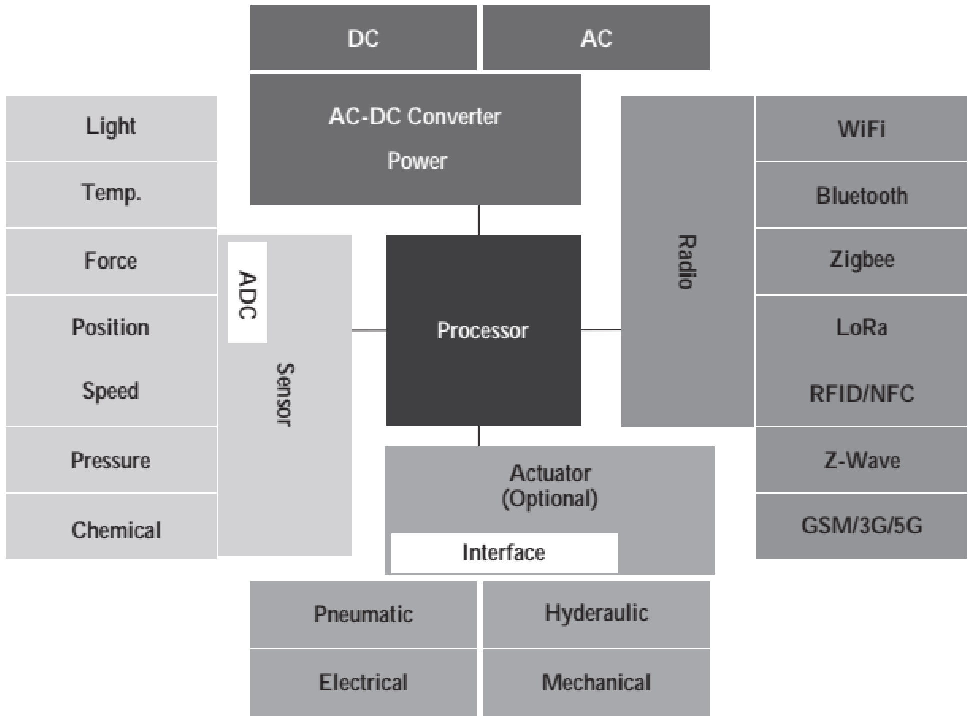
Fig 6: Ring Topology

COMPARISION OF NETWORK TOPOLOGIES

Topology	Feature	Advantages	Disadvantages
Star	Point-to-Point	• Cheap • Ease of installation • Ease of fault identification	• Single point of failure; • Traffic visible to network entities
Mesh	Point-to-Point	• Resilient against single point of failures. • Scalable • Traffic privacy and security ensured.	• Costly • 2. Complex connections
Bus	Point-to-multipoint	• Cheap • Ease of installation	• Length of backbone cable limited. • number of hosts limited • hard to localize faults
Ring	Point-to-Point	• Cheap • Ease of installation • Ease of fault identification.	• Prone to single point of failure

3	Explain the following i) IoT versus M2M ii) IoT versus CPS iii) IoT versus WoT.	10
Sol:	**IoT versus M2M** • M2M or the machine-to-machine paradigm refers to communications and interactions between various machines and devices. • These interactions can be enabled through a cloud computing infrastructure, a server, or simply a local network hub.	4

	• M2M collects data from machinery and sensors, while also enabling device management and device interaction. • M2M is part of the IoT and is considered as one of its sub-domains • M2M standards occupy a core place in the IoT landscape. However, in terms of operational and functional scope, IoT is vaster than M2M and comprises a broader range of interactions such as the interactions between devices/things, things, and people, things and applications, and people with applications; • M2M enables the amalgamation of workflows comprising such interactions within IoT. Internet connectivity is central to the IoT theme but is not necessarily focused on the use of telecom networks. **<u>IoT versus CPS</u>** • Cyber physical systems (CPS) encompasses sensing, control, actuation, and feedback as a complete package. • In other words, a digital twin is attached to a CPS-based system. Digital twin is a virtual system–model relation, in which the system signifies a physical system or equipment or a piece of machinery, while the model represents the mathematical model or representation of the physical system's behavior or operation. • Many a time, a digital twin is used parallel to a physical system, especially in CPS as it allows for the comparison of the physical system's output, performance, and health. • Based on feedback from the digital twin, a physical system can be easily given corrective directions/commands to obtain desirable outputs. • In contrast, the IoT paradigm does not compulsorily need feedback or a digital twin system. IoT is more focused on networking than controls. • Some of the constituent sub-systems in an IoT environment (such as those formed by CPS-based instruments and networks) may include feedback and controls too. In this light, CPS may be considered as one of the sub-domains of IoT. **<u>IoT versus WoT</u>** • Web of Things (WoT) paradigm enables access and control over IoT resources and applications. These resources and applications are generally built using technologies such as HTML 5.0, JavaScript, Ajax, PHP, and others. • REST (representational state transfer) is one of the key enablers of WoT. The use of RESTful principles and RESTful APIs (application program interface) enables both developers and deployers to benefit from the recognition, acceptance, and maturity of existing web technologies without having to redesign and redeploy solutions from scratch. • WoT can be thought of as an application layer-based hat added over the network layer. However, the scope of IoT applications is much broader; IoT also which includes non-IP-based systems that are not accessible through the web.	 3 3

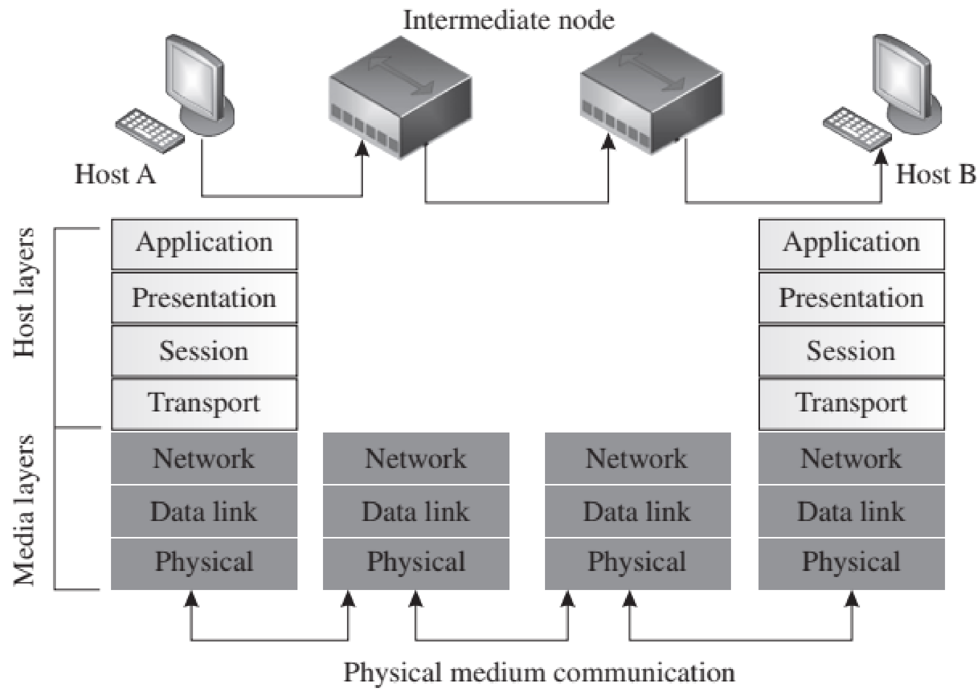
4	With a neat diagram explain the functional blocks of a typical sensor node in IoT.	10
Sol	 **<u>Fig: The functional blocks of a typical sensor node in IoT</u>**	6
	1. A sensor node is made up of a combination of sensor/sensors, a processor unit, a radio unit, and a power unit. 2. The nodes are capable of sensing the environment they are set to measure and communicate the information to other sensor nodes or a remote server. Typically, a sensor node should have low-power requirements and be wireless. 3. This enables them to be deployed in a vast range of scenarios and environments without the constant need for changing their power sources or managing wires. 4. The wireless nature of sensor nodes would also allow them to be freely relocatable and deployed in large numbers without bothering about managing wires.	4
5	Discuss the highlights of the seven layers of the OSI stack.	10

–

Sol

The ISO-OSI model is a conceptual framework that partitions any networked communication device into seven layers of abstraction, each performing distinct tasks based on the underlying technology and internal structure of the hosts. These seven layers, from bottom-up, are as follows:

1) Physical layer,
2) Data link layer,
3) Network layer,
4) Transport layer,
5) Session layer,
6) Presentation layer, and
7) Application layer



5

<u>Fig: Networked communication between two hosts following the OSI model</u>

(i) Physical Layer: This is a media layer and is also referred to as layer 1 of the OSI model. The physical layer is responsible for taking care of the electrical and mechanical operations of the host at the actual physical level. This layer is responsible for the topological layout of the network (star, mesh, bus, or ring), communication mode (simplex, duplex, full duplex), and bit rate control operations. The protocol data unit associated with this layer is referred to as a symbol. 5

(ii) Data Link Layer: This is a media layer and layer 2 of the OSI model. The data link layer is mainly concerned with the establishment and termination of the connection between two hosts, and the detection and correction of errors during communication between two or more connected hosts. IEEE 802 divides the OSI layer 2 further into two sub-layers, Medium access control (MAC) and logical link control (LLC). MAC is responsible for access control and permissions for connecting networked devices; whereas LLC is mainly tasked with error checking, flow control, and frame synchronization. The protocol data unit associated with this layer is referred to as a frame.

(iii) Network Layer: This layer is a media layer and layer 3 of the OSI model. It

	provides a means of routing data to various hosts connected to different networks through logical paths called virtual circuits. These logical paths may pass through other intermediate hosts (nodes) before reaching the actual destination host. The primary tasks of this layer include addressing, sequencing of packets, congestion control, error handling, and Internetworking. The protocol data unit associated with this layer is referred to as a packet. **(iv) Transport Layer:** This is layer 4 of the OSI model and is a host layer. The transport layer is tasked with end-to-end error recovery and flow control to achieve a transparent transfer of data between hosts. This layer is responsible for keeping track of acknowledgments during variable-length data transfer between hosts. In case of loss of data, or when no acknowledgment is received, the transport layer ensures that the particular erroneous data segment is re-sent to the receiving host. The protocol data unit associated with this layer is referred to as a segment or datagram. **(v) Session Layer:** This is the OSI model's layer 5 and is a host layer. It is responsible for establishing, controlling, and terminating of communication between networked hosts. The session layer sees full utilization during operations such as remote procedure calls and remote sessions. The protocol data unit associated with this layer is referred to as data. **(vi) Presentation Layer:** This layer is a host layer and layer 6 of the OSI model. It is mainly responsible for data format conversions and encryption tasks such that the syntactic compatibility of the data is maintained across the network, for which it is also referred to as the syntax layer. The protocol data unit associated with this layer is referred to as data. **(vii) Application Layer:** This is layer 6 of the OSI model and is a host layer. It is directly accessible by an end-user through software APIs (application program interfaces) and terminals. Applications such as file transfers, FTP (file transfer protocol), e-mails, and other such operations are initiated from this layer. The application layer deals with user authentication, identification of communication hosts, quality of service, and privacy. The protocol data unit associated with this layer is referred to as data.	
6	What are the various IoT connectivity terminologies? Differentiate between sensors, transducers and actuators.	10

Sol (a)

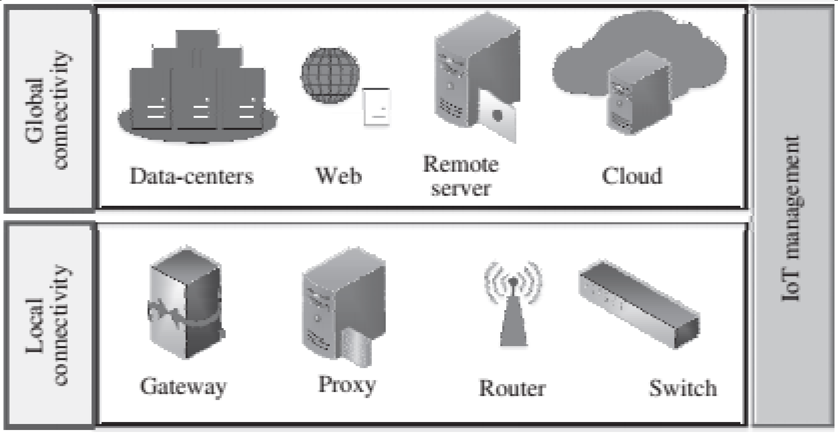


Fig: IoT Connectivity terminologies

5

- The local connectivity is responsible for distributing Internet access to multiple local IoT deployments.
- This distribution may be on the basis of the physical placement of the things, on the basis of the application domains, or even on the basis of providers of services.
- Services such as address management, device management, security, sleep scheduling, and others fall within the scope of this plane.
- The local connectivity plane falls under the purview of IoT management as it directly deals with strategies to use/reuse addresses based on things and applications. The modern-day “edge computing” paradigm is deployed in conjunction with these first two planes: services and local connectivity.
- In continuation, the penultimate plane of global connectivity plays a significant role in enabling IoT in the real sense by allowing for worldwide implementations and connectivity between things, users, controllers, and applications.
- This plane also falls under the purview of IoT management as it decides how and when to store data, when to process it, when to forward it, and in which form to forward it.
- The Web, data-centers, remote servers, Cloud, and others make up this plane. The paradigm of “fog computing” lies between the planes of local connectivity and global connectivity.
- It often serves to manage the load of global connectivity infrastructure by offloading the computation nearer to the source of the data itself, which reduces the traffic load on the global Internet.

(b)

Basic outline of the differences between transducers, sensors, and actuators

5

Parameters	Transducers	Sensors	Actuators
Definition	Converts energy from One form to another.	Converts various forms of energy into electrical signals.	Converts electrical signals into various forms of energy, typically mechanical energy.
Domain	Can be used to represent a sensor as well as an actuator.	It is an input transducer.	It is an output transducer.

Function	Can work as a sensor or an actuator but not simultaneously.	Used for quantifying Environmental stimuli into signals.	Used for converting signals into proportional mechanical or electrical outputs.
Examples	Any sensor or actuator	Humidity sensors, Temperature sensors, Anemometers (measures flow velocity), Manometers (measures fluid pressure), Accelerometers (measures the acceleration of a body), Gas sensors (measures concentration of specific gas or gases), and others	Motors (convert electrical energy to rotary motion), Force heads (which impose a force), Pumps (which convert rotary motion of shafts into either a pressure or a fluid velocity).