IOT Question Bank

SECTION 1

Que1. IOT features and applications

**IOT Feature:**

We have listed some of the features that make IOT what it is in the present digital scenario. IOT devices have several sets of features that are common. They are:

1. **Connectivity**

The heart and soul of IOT is its connectivity. Connectivity means the establishment of a connection between different devices so that they can communicate on their own. In IOT, various devices, sensors, computers, and data busses need to interact and communicate with each other. IOT also connects devices with cross-domain technology like cloud computing, artificial intelligence, and block chain technology.

1. **Scaling**

IOT systems are designed in such a way that the number of devices, sensors, or computers can be scaled up and down according to the need. An IOT system should be elastic enough so that it can handle workload during peak demand hours and can resort back to the normal state when the demand is low.

1. **Sensing**

IOT devices gather information about their surroundings (such as temperature, light, sound, acceleration, pressure) and then, after analyzing the data, take a decision.

For example, in an automatic door, sensors would collect data through sensors such as radar sensors and optical sensors. If it detects a person coming, it will open the door automatically. Some sensors used in IoT are- Humidity sensor, temperature sensor, Accelerometer, Gyroscope, Motion sensor, image sensor, level sensor, and Proximity sensor.

1. **Analyzing**

IOT gathers raw data to extract something meaningful out of it. Analyzing the raw data in terms of its structure, correlation, and usability is necessary because, if processed properly, it can be very useful. Like an example of the automatic door for instance, after analyzing the data through sensors, it should be able to differentiate between a person and an animal.

1. **Artificial Intelligence**

IOT becomes a lot more useful when combined with artificial intelligence. For instance, if you are out of groceries, your smart refrigerator can notify you to bring some on your way back home. Things like these have been made possible by the application of artificial intelligence. IOT devices collect raw data from their surroundings and convert them into something useful and insightful.

1. **Smaller Device**

Devices and equipment (like semiconductor chips, sensors) are getting smaller and smaller these days It is fascinating to think that devices so small can deliver so much and enhance our quality of living (for example, small sensors can tell us the quality of air in that area, protecting us from pollution).

1. **Automated**

Every technology comes with a certain degree of automation. IOT was developed to make people’s life and business easier with automation, i.e., IOT farming system automates irrigation and prevents wastage of water as well.

1. **Security**

Security is one of the major concerns among the users of IOT. IOT systems carry and store a lot of sensitive information, so the security of the devices should be given foremost priority. IOT system are huge, but its safety and security must be ensured.

**IOT Application:**

1. Smart home
2. Wearables
3. Smart city
4. Smart grid
5. Connected car
6. Smart farming
7. Smart supply chain

**Que2. M2M**

Machine-to-Machine (M2M) refers to networking of machines (or devices) for the purpose of remote monitoring and control and data exchange.

An M2M area network comprises of machines which have embedded hardware modules for sensing, actuation and communication.

Various communication protocols can be used for M2M local area networks such as ZigBee, Bluetooh, ModBus, M-Bus, Wirless M-Bus, Power Line Communication (PLC), 6LoWPAN, IEEE 802.15.4, etc.

The communication network provides connectivity to remote M2M area networks.

The communication network can use either wired or wireless networks (IP- based).

While the M2M area networks use either proprietary or non-IP based communication protocols, the communication network uses IP-based networks.

**Que3. Different IOT enabling technologies**

**IOT enabling technologies:**

* Wireless Sensor Network
* Cloud Computing
* Big Data Analytics
* Communications Protocols
* Embedded System

\*Explanation In PPT

**Que4. Physical and logical design of iot**

**Logical design:**

* Logical design of an IoT system refers to an abstract representation of the entities and processes without going into the low-level specifics of the implementation.
* An IoT system comprises a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication and management.
* The process of logical design involves arranging data into a series of logical relationships called entities and attributes.
* An entity represents a chunk of information. In relational databases, an entity often maps to a table.
* An attribute is a component of an entity and helps define the uniqueness of the entity. In relational databases, an attribute maps to a column.

**Physical design:**

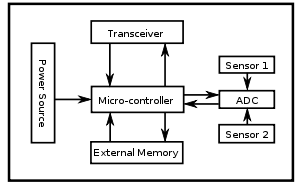
* Things in IoT – refers to devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.
* IoT devices can:
  + Exchange data with other connected devices and applications (directly or indirectly), or
  + Collect data from other devices and process the data locally or
  + Send the data to centralized servers or cloud-based application back-ends for processing the data, or
  + Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints

SECTION 2

Que 2. Sensor node and its architecture

**Sensor Node:**

Sensor node, also known as a mote (chiefly in North America), is a node in a sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. A mote is a node but a node is not always a mote.



**Fig :** Sensor Node Architecture

**Controller:**

1. The controller performs tasks, processes data and controls the functionality of other components in the sensor node.
2. A microcontroller[raspebeeryyp] is often used in many [embedded systems](https://en.wikipedia.org/wiki/Embedded_systems) such as sensor nodes because of its low cost, flexibility to connect to other devices.

**Transceiver:**

1. Sensor nodes often make use of [ISM band](https://en.wikipedia.org/wiki/ISM_band), which gives free [radio](https://en.wikipedia.org/wiki/Radio), spectrum allocation and global availability.
2. Most transceivers operating in idle mode have a power consumption almost equal to the power consumed in receive mode.

**External memory:**

1. From an energy perspective, the most relevant kinds of memory are the on-chip memory of a microcontroller
2. Flash memories are used due to their cost and storage capacity.
3. Memory requirements are very much application dependent

**Power source:**

1. A wireless sensor node is a popular solution when it is difficult or impossible to run a mains supply to the sensor node.
2. However, since the wireless sensor node is often placed in a hard-to-reach location, changing the battery regularly can be costly and inconvenient

**Sensors:**

1. [Sensors](https://en.wikipedia.org/wiki/Sensor) are used by wireless sensor nodes to capture data from their environment.
2. They are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure.

Que1. Smart sensor and its features

**Smart sensor:**

A smart sensor is a device that takes input from the physical environment and uses built-in compute resources to perform predefined functions upon detection of specific input and then process data before passing it on.

**Different types of smart sensor:**

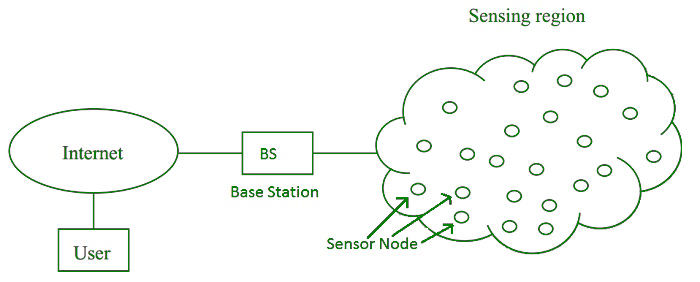
1. Level sensor
2. Temperature sensor
3. Pressure sensor
4. Infrared sensor
5. Proximity sensor

**Characteristics of smart sensor:**

* Analog to digital converter
* Microcontroller with advanced features, mostly it would be PIC
* Sensor identification
* The information should be calibrated
* Data logging and real time clock
* Communication is done by using a serial bus

Que3. Wireless sensor network

* A data acquisition system having smart sensors & which transmits data wirelessly can be said to be a Wireless Sensor Network
* Consists of large number of sensor nodes, densely deployed over an area.
* **Wireless Sensor Network (WSN)** is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.
* Sensor nodes are used in WSN with the on board processor that manages and monitors the environment in a particular area.
* They are connected to the Base Station which acts as a processing unit in the WSN System.
* Base Station in a WSN System is connected through the Internet to share data.



**Applications:**

1. Internet of Things (IOT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection
8. Smart Buildings
9. Tree Monitoring
10. Glacier Monitoring

**Components:**

1. **Sensors:**   
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
2. **Radio Nodes:**   
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
3. **WLAN Access Point:**   
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
4. **Evaluation Software:**   
   The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

**Types of WSN’s:**

Depending on the environment, the [types of networks](https://www.elprocus.com/important-of-network-in-embedded-systems-for-beginners/) are decided so that those can be deployed underwater, underground, on land, and so on. Different types of WSNs include:

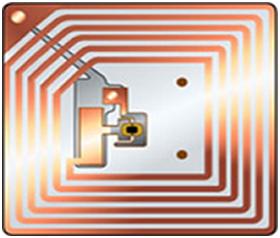
1. Terrestrial WSNs
2. Underground WSNs
3. Underwater WSNs
4. Multimedia and mobile WSNs

Que4. Concept of RFID

### A Basic RFID System:

### There are 3 Main Components of a RFID System are as follows:

* **A RFID tag:** It consists of a silicon microchip attached to a small antenna and mounted on a substrate and encapsulated in different materials like plastic or glass veil and with an adhesive on the back side to be attached to objects.



RFID Tag

* **A reader:** It consists of a scanner with antennas to transmit and receive signals and is responsible for communication with the tag and receives the information from the tag.



An RFID Reader

* **A Processor or a Controller**: It can be a host computer with a Microprocessor or a microcontroller which receives the reader input and process the data.

**2 Types of RFID Systems:**

* **Active RFID system:**

These aresystems where the tag has its own power source like any external power supply unit or a battery. The only constraint being the life time of the power devices. These systems can be used for larger distances and to track high value goods like vehicles.

* **Passive RFID system:**

These are systems where the tag gets power through the transfer of power from a reader antenna to the tag antenna. They are used for short range transmission.

Here we are mostly concerned with the passive RFID system as it is most widely used in regular applications like in retail market organizations.

Que5. Different network configurations

Network configuration is the process of assigning network settings, policies, flows, and controls.

In a [virtual network](https://www.vmware.com/topics/glossary/content/virtual-networking.html" \t "_self), it’s easier to make network configuration changes because physical network devices appliances are replaced by software, removing the need for extensive manual configuration.

**Different network configurations are as follows:**

* Personal Area Network (PAN) ...
* Local Area Network (LAN) ...
* Wireless Local Area Network (WLAN) ...
* Campus Area Network (CAN) ...
* Metropolitan Area Network (MAN) ...
* Wide Area Network (WAN) ...
* Storage-Area Network (SAN) ...
* System-Area Network (also known as SAN)

**Que6. IOT Stack**

**Que7. Study following protocols in detail**

1. **802.15.4 protocol**

Until recently, the main concern in wireless communication was on high throughput

Some applications need a different set of requirements

**Example:** LR-WPAN (Low Rate Wireless Personal Area Network) applications

-Low cost communication network

-Limited power

-Low throughput

Require: reasonable battery life, extremely low cost, short range operation, reliable data transfer

* LR-WPAN needs a simple, flexible protocol
* IEEE 802.15.4 defines protocol via RF for PAN.
* Provides a standard with ultra-low complexity, cost, and power for low-data-rate wireless connectivity among inexpensive fixed, portable, and moving devices.

**Properties of 802.15.4 protocol:**

* Raw Data Rate: 868 MHz, 20 kbps; 915 MHz, 40 kbps; 2.4 GHz, 250 kbps
* Range: 10-30 mtr
* Latency: Down to 15 ms
* Channels: 868 MHz, 1 Channel; 915 MHz, 10 Channels; 2.4 GHz, 16 Channels
* Frequency Band: Two PHYs: 868 MHz / 915 MHz & 2.4 GHz
* Addressing: Short 16-bit or 64-bit IEEE
* Channel Access: CSMA-CA & Slotted CSMA-CA
* Temperature: Industrial temperature range -40 °C to +85 °C

1. **Zingbee**

* Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless [machine-to-machine (M2M)](https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M) and [internet of things](https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT) networks.
* Zigbee is for low-data rate, low-power applications and is an open standard.
* Zigbee is primarily developed to focus on home and building automation and controls, consumer electronics, PC peripherals, medical monitoring, and toys
* Primary drivers in Zigbee popularity are simplicity, long battery life, networking capabilities, reliability, and cost.
* Zigbee Alliance provides interoperability and certification testing

**Features:**

* Global, license free ISM band operation
* Unrestricted geographic use
* Automatic/semi-automatic installation
* Ability to add or remove devices
* Cost advantageous
* 10k-115.2kbps data throughput
* 10-75m coverage range
* Up to 65k slave nodes per network
* Up to 100 co-located networks
* Up to 2 years of battery life on standard Alkaline batteries

**Advantages:**

* This network has a flexible network structure
* Battery life is good.
* Power consumption is less
* Very simple to fix.
* It supports approximately 6500 nodes.
* Less cost.
* It is self-healing as well as more reliable.
* Network setting is very easy as well as simple.
* Loads are evenly distributed across the network because it doesn’t include a central controller
* Home appliances monitoring as well controlling is extremely simple using remote
* The network is scalable and it is easy to add/remote ZigBee end device to the network.

**Disadvantages:**

* It needs the system information to control Zigbee based devices for the owner.
* As compared with WiFi, it is not secure.
* The high replacement cost once any issue happens within Zigbee based home appliances
* The transmission rate of the Zigbee is less
* It does not include several end devices.
* It is so highly risky to be used for official private information.
* It is not used as an outdoor wireless communication system because it has less coverage limit.
* Similar to other types of wireless systems, this ZigBee communication system is prone to bother from unauthorized people.

**What devices uses the Zingbee?**

* Samsung SmartThings
* Yale smart locks
* Philips Hue
* Thermostats from Honeywell
* Amazon Echo Plus

1. **MQTT**

* MQTT is a lightweight message queueing and transport protocol.
* MQTT, as its name implies, is suited for the transport of telemetry data (sensor and actor data).
* MQTT is very lightweight and thus suited for M2M (Mobile to Mobile), WSN (Wireless Sensor Networks) and ultimately IoT (Internet of Things) scenarios where sensor and actor nodes communicate with applications through the MQTT message broker.

**Example:**

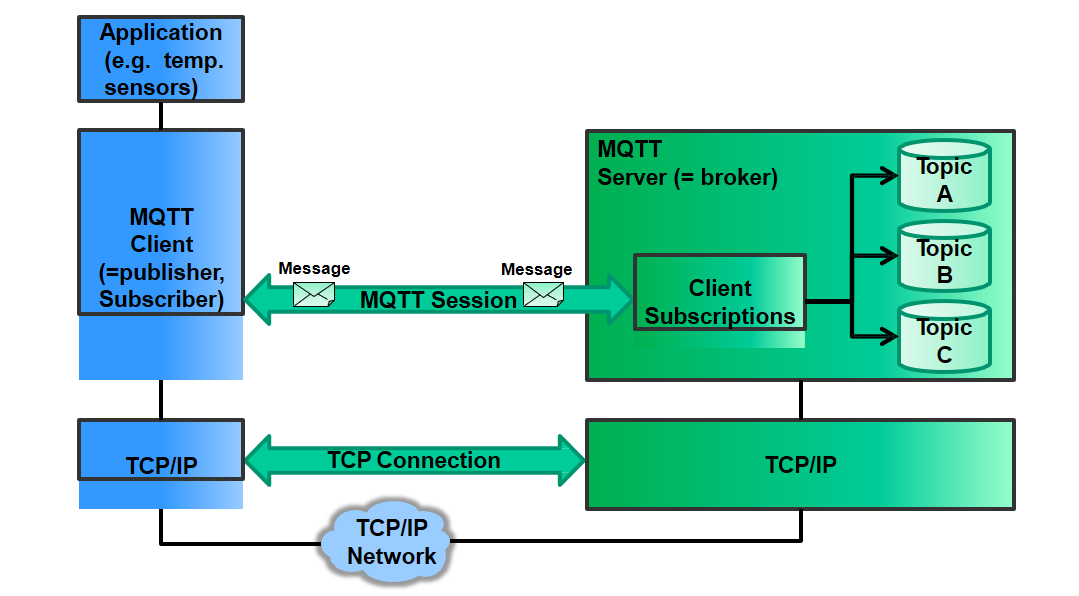
Light sensor continuously sends sensor data to the broker.

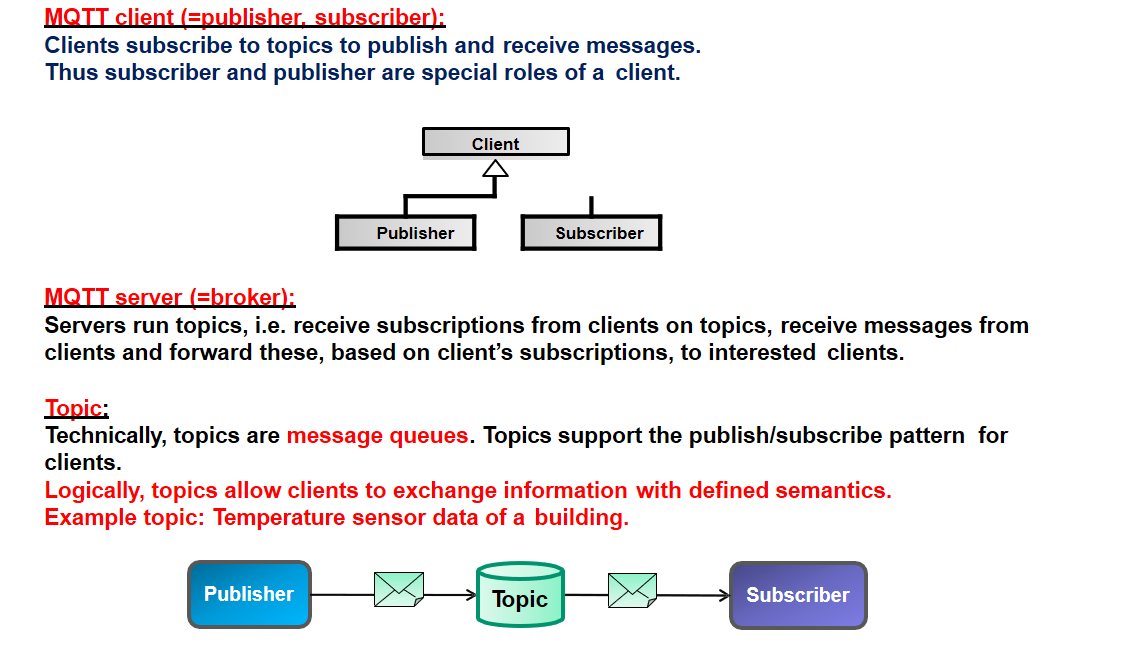
**Key features:**

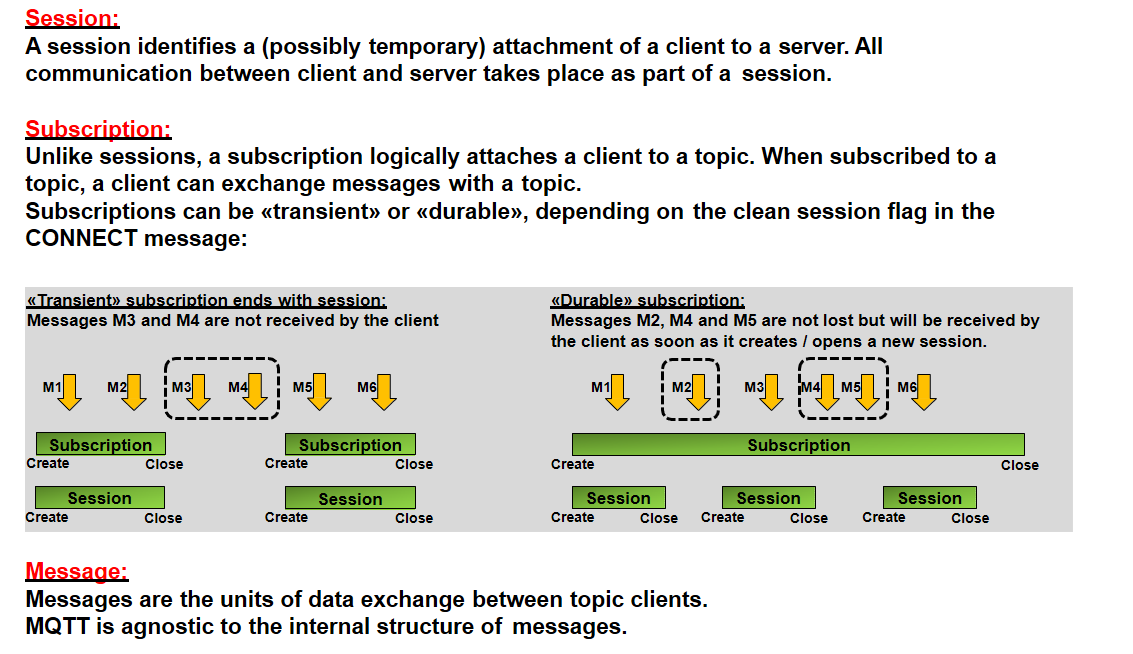
* Lightweight message queueing and transport protocol
* Asynchronous communication model with messages (events)
* Low overhead (2 bytes header) for low network bandwidth applications
* Publish / Subscribe (PubSub) model
* Decoupling of data producer (publisher) and data consumer (subscriber) through topics (message queues)
* Simple protocol, aimed at low complexity, low power and low footprint implementations (e.g. WSN - Wireless Sensor Networks)
* Runs on connection-oriented transport (TCP). To be used in conjunction with 6LoWPAN (TCP header compression)
* MQTT caters for (wireless) network disruptions

**MQTT model**

The core elements of MQTT are clients, servers (=brokers), sessions, subscriptions and topics.







**Que8. Cloud computing fundamentals and types of cloud computing**

**Types of cloud computing:**

1. **Cloud infrastructure**

Cloud infrastructure is a term used to describe the components needed for [cloud computing](https://www.redhat.com/en/topics/cloud), which includes hardware, abstracted resources, storage, and network resources.

An abstraction technology or process—like [virtualization](https://www.redhat.com/en/topics/virtualization)—is used to separate resources from physical hardware and pool them into clouds; [automation](https://www.redhat.com/en/topics/automation/whats-it-automation) software and [management](https://www.redhat.com/en/topics/management)tools allocate these resources and provision new environments so users can access what they need—when they need it.

**Some components of cloud infrastructure:**

* 1. Hardware
  2. Virtualization
  3. Storage
  4. Network

1. **Cloud delivery model**

**There are 4 main types of cloud computing:**

* Public clouds,
* Private clouds,
* Hybrid clouds,
* Multi clouds
  1. **Cloud service model**
  2. **Cloud deployment model**