iot chapter 3,4,5 IMP notes

Internet Of Things (University of Mumbai)

Q.1Explain Message Queuing Telemetry Transport [MQTT] protocol with diagram.

- MQTT stands for Message Queuing Telemetry Transport.
- MQTT is a machine to machine internet of things connectivity protocol.
- It is an extremely lightweight and publish-subscribe messaging transport protocol.

Architecture of MQTT

components of the MQTT.

- **Message**
- **Server or Broker**
- **TOPIC**
- **Broker**

Message

- Messages are the information that you want to exchange between your devices. It can be a message like a command or data like sensor readings,

for example.

Temperature sensor temperature is 25 degree celcius.

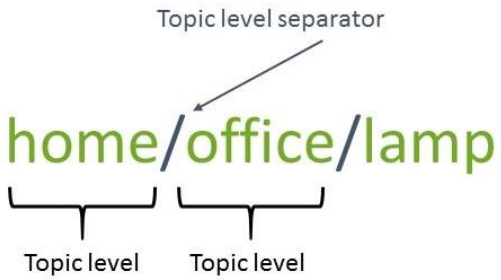
Publish /Subscribe

- The first concept is the publish and subscribe system.
- In a publish and subscribe system, a device can publish a message on a topic, or it can be subscribed to a particular topic to receive messages.

  - For example **Device 1** publishes on a topic.
  - **Device 2** is subscribed to the same topic that **device 1** is publishing in.
  - So, **device 2** receives the message.

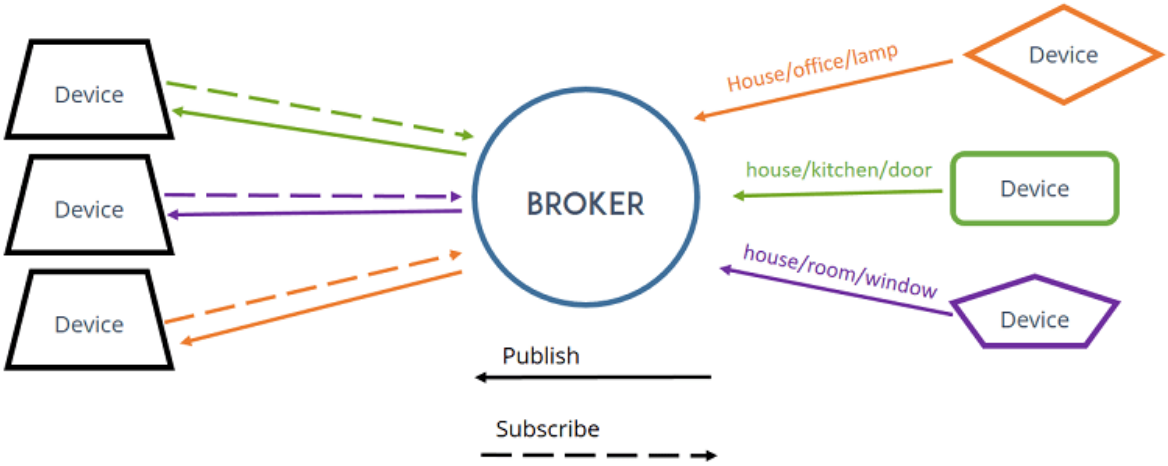
Topic

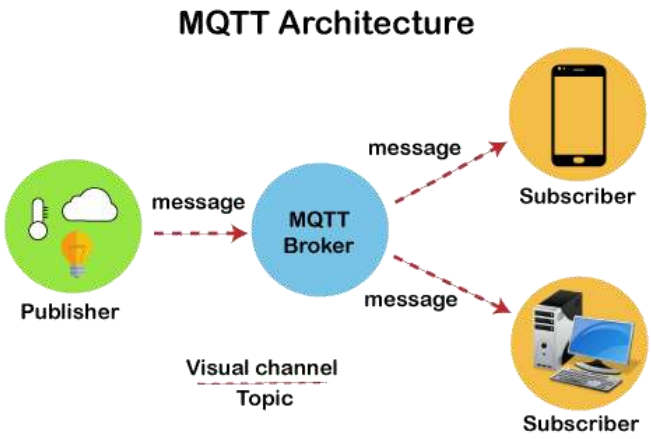
- Another important concept is the *topics*. Topics are the way you register interest for incoming messages or how you specify where you want to publish the message.
- Topics are represented with strings separated by a forward slash. Each forward slash indicates a topic level. Here's an example of how you would create a topic for a lamp in your home office:



Broker

- The **MQTT broker** is responsible for **receiving** all messages, **filtering** the messages, **deciding** who is interested in them, and then **publishing** the message to all subscribed clients.

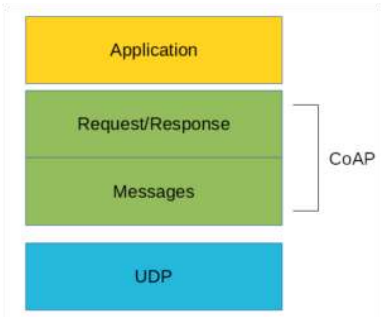




- We will look at the example. Suppose a device has a temperature sensor and wants to send the rating to the broker.
- If the phone or desktop application/subscriber wishes to receive this temperature value on the other side, then there will be two things that happened.
- The publisher first defines the topic; for example, the temperature then publishes the message, i.e., the temperature's value. After publishing the message, the phone or the desktop application on the other side will subscribe to the topic, i.e., temperature and then receive the published message, i.e., the value of the temperature.
- The server or the broker's role is to deliver the published message to the phone or the desktop application.

Q.2. Explain Constrained Application Protocol [CoAP] with its message format and fields.

- CoAP stands for Constrained Application Protocol, and it is defined in RFC 7252.
- CoAP is a simple protocol with low overhead specifically designed for constrained devices and constrained networks.
- This protocol is used in M2M data exchange and is very similar to HTTP.



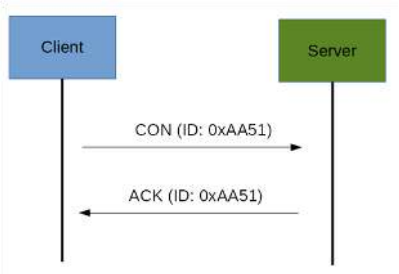
There are two different layers that make CoAP protocol: **Messages and Request / Response**.

Messages

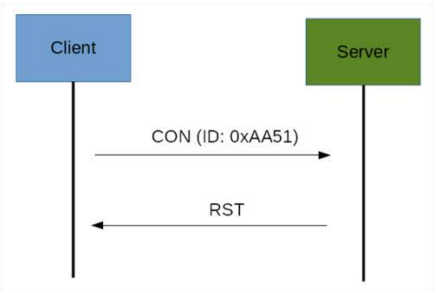
the CoAP protocol uses two kinds of messages:

1) Confirmable message

- A confirmable message is a reliable message.
- Using this kind of message, the client can be sure that the message will received at the server.
- A Confirmable message is sent again and again until the other party sends an acknowledge message (ACK).
- The ACK message contains the same ID of the confirmable message

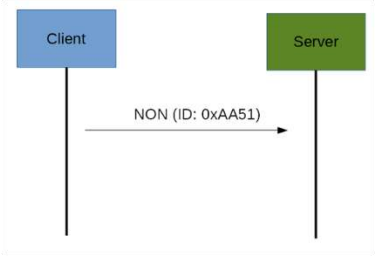


- If the server has troubles managing the incoming request, it can send back a Rest message (RST) instead of the Acknowledge message (ACK).



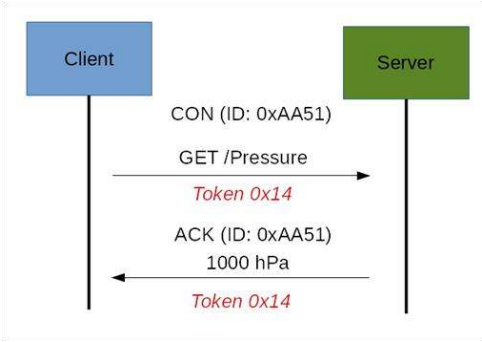
2) Non-confirmable message.

- These are messages that don't require an Acknowledge by the server.
- They are unreliable messages.
- To this category belongs messages that contain values read from sensors.
- Even if these messages are unreliable, they have a unique ID.



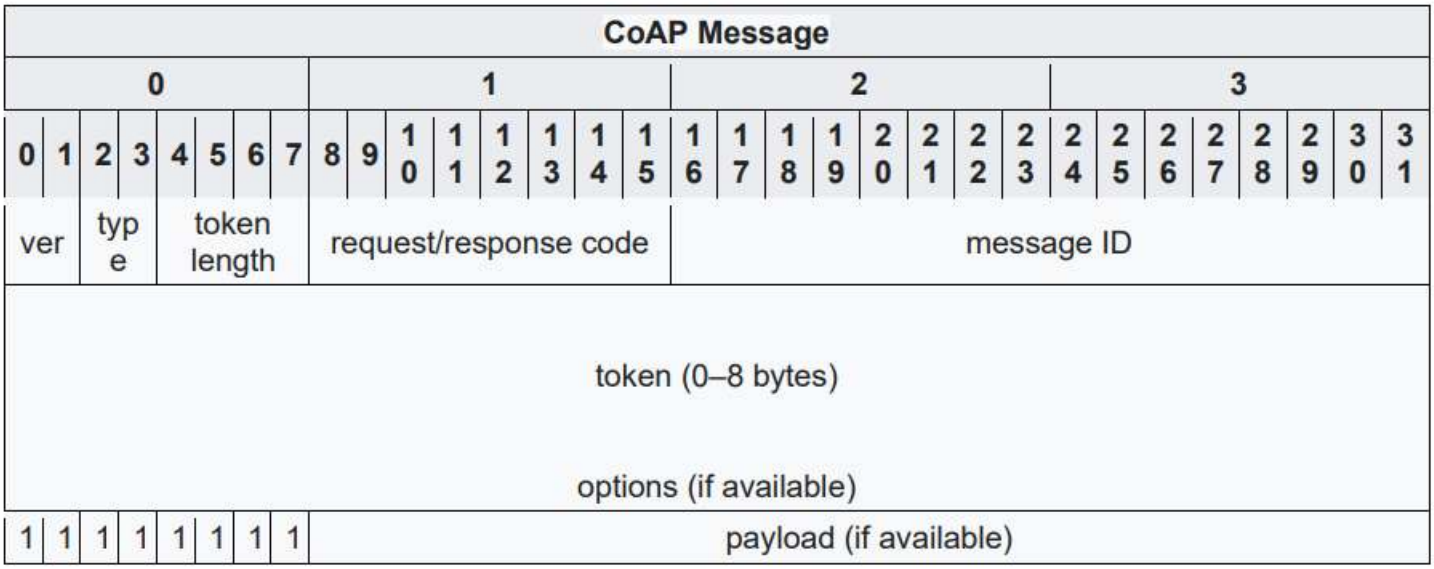
Request / Response

- The CoAP Request/Response is the second layer in the CoAP abstraction layer.
- The request is sent using a Confirmable (CON) or Non-Confirmable (NON) message.



Message Format

- Message formats CoAP makes use of two message types, **requests** and **responses**, using a simple, binary header format.
- CoAP is by default bound to UDP and optionally to DTLS, providing a high level of communications security.
- The smallest CoAP message is 4 bytes in length, if the token, options and payload fields are omitted, i.e. if it only consists of the CoAP header.
- The header is followed by the token value (0 to 8 bytes) which may be followed by a list of options in an optimized type–length–value format.
- The length of the payload is implied by the datagram length.



Ver (Version)

→ It is two bit in length
→ It is denote the version of COAP.

T (type)

→ It is also two bit inthe length
→ It indicate the message type.
i.e.

Request

0 → Confirmable

1 → Non confirmable

Response

3 → Aknowledgement

4 → RESET

Token length

→ Its length is 4 bits
→ Its indicates the length of token.

Code

→ It is a 8 bit in length
→ It indicate the code Responce

0 → Request

2 → Success Responce

4 → client error responce

5 → Server error responce

Message_ID

→ It length is 16 bit
→ It is use to match message of type Aknowledgement /RESET to messages of type comfirmable / non-confirmable

Token

→ It is use to correlate Requests and Responses.

Q.3. Explain The Core IoT Functional Stack.

- The Internet of Things (IoT) is a system of interconnected devices, sensors, and other objects that are able to exchange data and perform actions based on that data.
- he core IoT functional stack is a model that describes the various layers and components involved in building an IoT solution.

- **It is composed of four layers**:

Things Layer:

- This layer is responsible for gathering data from various sensors and devices.
- It includes sensors, actuators, and other hardware components that can collect data.

Network Layer:

- The Network Layer is responsible for transmitting the data collected by the Perception Layer to the next layer. It includes various communication protocols like Wi-Fi, Bluetooth, Zigbee, and other wireless and wired communication technologies.

Data Processing Layer:

- The Data Processing Layer receives the data from the Network Layer and processes it to extract relevant information.
- It includes various analytics tools, machine learning algorithms, and databases.

Application Layer:

- The Application Layer is the topmost layer of the stack, responsible for providing user-facing services and applications.
- It includes various IoT platforms, mobile applications, and web-based dashboards.

Q.4 What SCADA system in IOT ? How SCADA is adapted to IP network?

- SCADA is software used to control industrial processes by gathering real-time data and making data-driven decisions.
- It can manage almost any type of industrial process and includes hardware and software components.
- The hardware gathers data and feeds it to field controllers, which forward it to a human-machine interface (HMI) for processing and presenting in a timely manner.
- SCADA systems also log all events for reporting process status and sound alarms when conditions become hazardous.
- **Components of a SCADA system**
- Sensors and actuators.
- SCADA field controllers.

Applications of SCADA

- **Water Systems**

  Water SCADA systems monitor and control the water being pumped at well sites and treated at water treatment plants. They also use it to fill overhead storage tanks.Additionally, water SCADA systems control booster pumps to regulate water pressurebeing delivered to customers.

- **Wastewater Systems**

  Wastewater SCADA systems monitor and control lift stations that are used to pump wastewater to treatment plants. Once the wastewater reaches the treatment plant, the treatment process is controlled step by step using SCADA. Wastewater SCADA monitoring is also used to document operations and prepare reports that verify compliance with governmental regulations.

- **Electric Generation, Transmission and Distribution Systems**

  Electric generation SCADA software is used to monitor every phase of generating electricity from fuel input to electrical output. Such plants have to be able to respond instantaneously to fluctuations in demand. Electric transmission utilities use SCADA to monitor and control the amount of electrical power being transmitted over long distances.

- SCADA is also used for safety and protection purposes. When a transmission line experiences a fault, the system will quickly attempt to clear the fault and restore power. Electric distribution systems also use SCADA to monitor and control electrical substations and distribution lines.

- **Oil and Gas Systems**

Unlike electric and telecom systems, oil and gas SCADA systems move a physical substance through their infrastructure over a vast area. Oil and Gas SCADA is used to monitor well and pumping sites plus distribution pumping pressure and pipeline flow. In addition to using SCADA to monitor and control compressor stations, SCADA software is also necessary from a safety standpoint because it is used to detect anomalies and prevent catastrophic events from occurring.

- **Manufacturing Plant Systems**

  Manufacturing plant SCADA precisely control all plant operations. For instance, SCADAcan be used to monitor and control temperature, pressure and humidity. It can also be used to monitor production lines to ensure that output goals are being met. SCADA can also control assembly line robots and monitor parts usage so that just-in-time inventory control can be implemented.

- **Food Production Systems**

  Food production SCADA applications are used to ensure food quality and meet production goals. All phases of food preparation are typically monitored and controlled. SCADA can be used to control the exact mix of ingredients as well as the time and temperature required to process foods. This prevents foods from being spoiled due to a heating process that was off by a few degrees. SCADA applications are also important in food production to document the fact that the production process meets industry standards and complies with governmental regulations.

- **Mass Transit Systems**

  Mass transit systems also rely heavily on SCADA. Railways, subways and tramways use it to time their operations and control their switches so that engines and cars can safely pass each other. Railroad crossing signals are also controlled remotely. Traffic control systems also rely on SCADA to improve traffic flow and maximize safety.

Q.5. Write a note on below IOT platforms

a. Arduino

- Arduino is an open-source electronics platform based on easy-to-use hardware and software.
- It is designed to help people create interactive projects by providing an easy-to-use platform for developing embedded systems.
- Arduino boards are equipped with digital and analog inputs and outputs that can be connected to sensors, motors, and other devices.
- The platform includes an integrated development environment (IDE) that makes it easy to write and upload code to the board.
- The code is written in C++ and can be easily modified by users to fit their specific needs. Arduino has become a popular platform for hobbyists, artists, and students interested in creating interactive and electronic projects.
- Its affordability, versatility, and ease of use have made it a favorite among makers and tinkerers.

b. Raspberry Pi

- Raspberry Pi is a popular low-cost, credit-card sized computer that can be used in IoT (Internet of Things) projects.
- It has become a popular choice for IoT applications due to its flexibility, connectivity options, and ease of use.
- Raspberry Pi can run a variety of operating systems, including Linux-based ones, and can be programmed using various languages such as Python and C++.
- It can also be connected to a wide range of sensors, cameras, and other devices to collect and process data, and can communicate with other devices and the cloud via Wi-Fi, Ethernet, or other connectivity options.
- The Raspberry Pi's small size and low power consumption make it ideal for IoT projects where space and energy efficiency are important factors.

Q.6 Explain How IOT can be used in below domains

a. Home automation b. Environment c. Logistics

d. Agricultura. **Home automation:**

- IoT can be used in home automation to control and automate various devices and appliances in a house such as lights, thermostats, security cameras, door locks, and more.
- IoT devices can communicate with each other and be controlled remotely through a smartphone app or voice assistant, providing convenience and energy efficiency.

b. **Environment:**

- IoT can be used to monitor and manage environmental factors such as air quality, water quality, and weather conditions.
- Sensors and devices can be deployed to collect data on temperature, humidity, pollution levels, and other environmental parameters. This data can be analyzed to provide insights for environmental monitoring, climate research, and pollution control.

c. **Logistics:**

- IoT can be used in logistics to track and manage shipments, optimize supply chain operations, and improve inventory management.
- IoT devices such as RFID tags, GPS trackers, and sensors can be attached to packages, vehicles, and equipment to monitor their location, condition, and movement in real-time. This information can be used to improve delivery times, reduce losses and damages, and streamline logistics operations.

d. **Agriculture**:

- IoT can be used in agriculture to monitor crops, soil, and weather conditions, and optimize farming operations.
- IoT devices such as sensors, drones, and satellite imagery can be used to collect data on crop growth, soil moisture, and nutrient levels.
- This data can be analyzed to provide insights for precision agriculture, crop yield prediction, and resource management. IoT can also be used to automate irrigation systems, monitor livestock, and track supply chain operations in agriculture.