Unit 2:

Difference between Internet and Internet of Things:

**The main difference between internet of things and internet is the identity of the content creator. On the conventional Internet, content is consumed on a request basis. In the IoT, on the other hand, the material is often consumed by sending a notice or initiating an action when a condition of interest is discovered.**

The internet of things (IoT) is a network of physical items that are infused with technology and link to the internet as well as other gadgets.

The Internet is a vast network that connects numerous computers and other electronic gadgets all around the world.

Anyone can get nearly any information, interact with anyone on the globe, and do a lot more using the Internet.

Decentralization is a feature of the internet. Nobody possesses the internet or has control over who can access it. The [Internet of Things](https://askanydifference.com/difference-between-internet-of-things-and-cloud-computing-with-table/) (IoT) allows objects to communicate directly with one another, make collaborative choices, and share data without the use of a cloud or servers.

IoT, like Numerous Machines to Many Machines, is a development of the Machine to Machine concept with many devices involved.

Physical equipment and gadget, as well as virtualized services and operations, are all represented by the term Things.

Clusters of the IoT are groups of items on a network that communicate directly with one another. Consider a linked house with numerous distinct types of connected gadgets all communicating with one another over the same network.

| **Parameters of Comparison** | **Internet of Things** | **Internet** |
| --- | --- | --- |
| Objective | Focused on the actual world. | Focused more on the virtual world. |
| Tasks that are done so far | Content creation. | Content generation and consumption. |
| Based on | Concepts of physical-first. | Concepts of physical-first and digital-first. |
| Connection type | Multipoint. | Point-to-point as well as multipoint. |
| Content combined with | Explicitly defined operators. | Physical linkages. |

Q: MQTT:

Lightweight and Efficient

MQTT clients are very small, require minimal resources so can be used on small microcontrollers. MQTT message headers are small to optimize network bandwidth.

### Bi-directional Communications

MQTT allows for messaging between device to cloud and cloud to device. This makes for easy broadcasting messages to groups of things.

### Scale to Millions of Things

MQTT can scale to connect with millions of IoT devices.

### Reliable Message Delivery

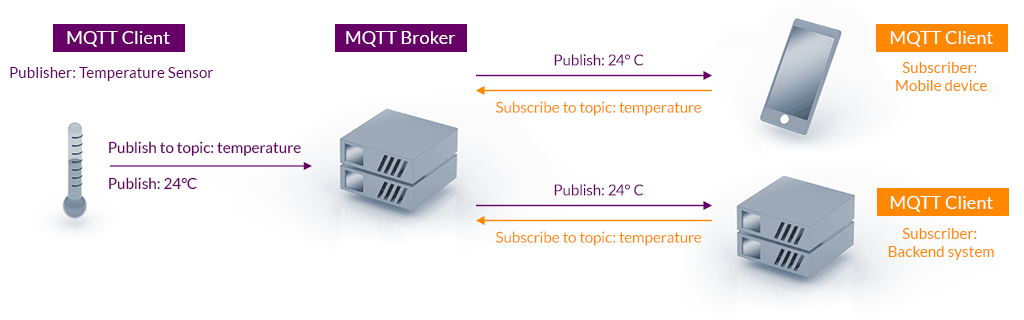
Reliability of message delivery is important for many IoT use cases. This is why MQTT has 3 defined quality of service levels: 0 - at most once, 1- at least once, 2 - exactly once

### Support for Unreliable Networks

Many IoT devices connect over unreliable cellular networks. MQTT’s support for persistent sessions reduces the time to reconnect the client with the broker.

### Security Enabled

MQTT makes it easy to encrypt messages using TLS and authenticate clients using modern authentication protocols, such as OAuth.



# **IoT Messaging Protocols**

IoT devices use various kinds of **messaging** and **communication protocols** in every layer in order to communicate with each other. While constructing an IoT device it is important to keep in mind its type, its functionality, and the layer. There are a wide range of messaging and communication protocols available in the market and the most common ones are discussed below.

Now, let us look at the common messaging protocol adapted in IoT.

### IoT Messaging Protocols

#### **1. Message Queuing Telemetry Transport(MQTT Protocol in IoT)**

MQTT is an IoT communication protocol that is widely gaining popularity due to its lightweight **publish/subscribe** messaging transport. It is a protocol that transfers data between various machines. It has become one of important protocols in the internet of things.

All devices communicate through a **broker or server**. You can install the broker in your PC, MAC, Linux system and even in Raspberry pie. Two of the most famous brokers available in the market these days are **HIVEMQ** and **Mosquito.**

**Client devices** receive or accept information either from the broker or by just subscribing to specific topics. They can also publish specific topic messages to the broker. All devices communicate with each other through the **broker.**

There are three different kinds of**QoS**(quality of service):

* QoS0: messages are sent once, regardless of any feedback from the broker.
* QoS1: messages are sent over and over until they receive a confirmation from broker
* QoS2: for every message sent, broker sends a confirmation message back

MQTT is **lightweight** in size and data power transmission and it is hence available in a large number of devices. MQTT mainly transmits its data through the**TCP/IP protocol**.

#### **Features of MQTT**

* Lightweight protocol suits best for constrained nodes
* Assists publish/subscribe messaging
* Reduces size of data packets
* OASIS standard protocol

#### **Pros of MQTT**

* Flexible options to choose from for quality of service within functionality
* Easy to act upon
* Quick results

Q: CoAP:

### **What Is CoAP?**

Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things. CoAP is designed to enable simple, constrained devices to join the IoT even through constrained networks with low bandwidth and low availability. It is generally used for machine-to-machine (M2M) applications such as smart energy and building automation. The protocol was designed by the Internet Engineering Task Force ([IETF](https://searchmicroservices.techtarget.com/definition/IETF-Internet-Engineering-Task-Force)), CoAP is specified in IETF [RFC 7252](https://tools.ietf.org/html/rfc7252).

Constrained Application Protocol (CoAP) is a [protocol](https://www.techtarget.com/searchnetworking/definition/protocol) that specifies how low-power compute-constrained devices can operate in the internet of things ([IoT](https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT)). Designed by the Internet Engineering Task Force ([ITEF](https://www.techtarget.com/whatis/definition/IETF-Internet-Engineering-Task-Force)), CoAP is specified in IETF RFC 7252.

CoAP is designed to enable simple, constrained devices to join the IoT even through constrained networks with low [bandwidth](https://www.techtarget.com/searchnetworking/definition/bandwidth) and low availability. The protocol is generally used for machine-to-machine ([M2M](https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M)) communication.

CoAP functions as a sort of [HTTP](https://www.techtarget.com/whatis/definition/HTTP-Hypertext-Transfer-Protocol) for constrained devices, enabling such component level equipment as [sensors](https://www.techtarget.com/whatis/definition/sensor) or [actuators](https://internetofthingsagenda.techtarget.com/definition/actuator) to communicate on the IoT, being controlled and passing along their data as part of a system. The protocol is designed for reliability in low bandwidth and high congestion through its low power draw and low network overhead. According to Jullian Vermillard, Sierra Wireless principle engineer of software, in a network with limited connectivity or a lot of congestion CoAP can continue to work where [TCP-](https://www.techtarget.com/searchnetworking/definition/TCP)based protocols such as [MQTT](https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport) fail to complete a handshake.

The efficient and conservative traits of CoAP can enable devices operating in poor signal quality to send their data reliably or enable a [satellite](https://www.techtarget.com/searchmobilecomputing/definition/satellite) in orbit maintain to its distant communication successfully. Despite CoAp’s ability to run on small devices, it supports networks with billions of nodes. For security, the DTLS parameters chosen for default are an equivalent to 3072 bit [RSA](https://www.techtarget.com/whatis/definition/RSA-Security) keys.

### **How Does CoAP Function?**

CoAP functions as a sort of [HTTP](https://searchwindevelopment.techtarget.com/definition/HTTP) for restricted devices, enabling equipment such as sensors or actuators to communicate on the IoT. These sensors and actuators are controlled and contribute by passing along their data as part of a system. The protocol is designed for reliability in low bandwidth and high congestion through its low power consumption and low network overhead. In a network with a lot of congestion or limited connectivity, CoAP can continue to work where [TCP-](https://searchnetworking.techtarget.com/definition/TCP)based protocols such as [MQTT](https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport) fail to exchange information and communicate effectively.

Additionally, the effective and conventional CoAP features enable devices operating in poor signal quality to send their data reliably or enable an orbiting satellite to maintain its distant communication successfully. CoAP’s also supports networks with billions of nodes. For security, the DTLS parameters chosen for default are an equivalent to 128 bit [RSA](https://whatis.techtarget.com/definition/RSA-Security) keys.

COAP uses [UDP](https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol) as the underlying network protocol. COAP is basically a client-server IoT protocol where the client makes a request and the server sends back a response as it happens in HTTP. The methods used by COAP are the same used by HTTP.

### **CoAP Security**

One must take security into account when dealing with IoT protocols. For example, CoAP uses UDP to transport information. CoAP relies on UDP security features to protect information. As HTTP uses TLS over TCP, CoAP uses Datagram TLS over UDP. [DTLS](https://en.wikipedia.org/wiki/Datagram_Transport_Layer_Security) supports RSA, AES, and so on.

The smallest CoAP message is 4 bytes in length, if omitting Token, Options and Payload. CoAP makes use of two message types, requests and responses, using a simple, binary, base header format. The base header may be followed by options in an optimized Type-Length-Value format. CoAP is by default bound to UDP and optionally to DTLS, providing a high level of communications security.

Any bytes after the headers in the packet are considered the message body. The length of the message body is implied by the datagram length. The entire message must fit within a single datagram when bound to UDP. When used with [6LoWPAN](https://en.wikipedia.org/wiki/6LoWPAN), as defined in [RFC 4944](https://tools.ietf.org/html/rfc4944), messages SHOULD also fit into a single [IEEE 802.15.4](https://en.wikipedia.org/wiki/IEEE_802.15.4) frame to minimize fragmentation.

Q: BLE

## **OVERVIEW OF BLUETOOTH LOW ENERGY**

Bluetooth Low Energy or more popular as BLE or Bluetooth LE was introduced in the Bluetooth 4.0 specification and was a low power consumption protocol, especially for IoT-based implementations. Typically one hears about BLE beacons which are BLE devices that send out Bluetooth signals to electronic devices in the vicinity.

## **WHAT IS THE DIFFERENCE BETWEEN BLUETOOTH AND BLE?**

Bluetooth and BLE(Bluetooth Low Energy) are wireless technologies standards. Classic Bluetooth regular works with large chunks of data but consumes a large amount of battery while BLE handles the lesser amount of data but consumes less energy, therefore, can work with even coin cells which have long battery life.

Typically Bluetooth is used in consumer electronic devices where there is a need to exchange data in a continuous stream. BLE which is marketed as Bluetooth smart is used where there is less amount of data transfer needed between devices and this data transfer happens in an intermittent manner.

## **HOW DOES IT WORK?**

BLE operates in the 2.4 GHz ISM band and the standard is maintained by the Bluetooth SIG but it is not compatible with the classic Bluetooth which uses the Basic Rate/Enhanced Basic Rate (BR/EDR) protocol. BLE remains in dormant mode until the connection is initiated. The duration of time of connection is of few ms in BLE.

A Bluetooth beacon which is a small device with power being sourced from a coin cell or USB transmits or broadcasts information. This information is picked by the receiver which may be a phone or a gateway. The BLE can transmit data on 37 data channels, while 3 channels are used for advertisements.

Q: LiFi:

## What is LiFi?

LiFi, also known as "Light Fidelity" is a wireless optical networking technology, which uses light emitting diodes (LEDs) to transmit data.  In 2011, professor Harald Haas made a LiFi demonstration at the TED (Technology, Entertainment, Design) Global Talk on Visible Light Communication (VLC).

## 2. How does LiFi work?

LiFi is a high speed, bidirectional, and fully networked wireless communication of data using light. LiFi constitutes of several lightbulbs that form a wireless network.

When an electrical current is applied to a LED light bulb a stream of light (photons) is emitted from the bulb. LED bulbs are semiconductor devices, which means that the brightness of the light flowing through them can be changed at extremely high speeds. This means that the signal can be sent by modulating the light at different rates. The signal can then be received by a detector that interprets the changes in light intensity (the signal) as data.  Also when the LED is ON, you transmit a digital 1 and when it is OFF you transmit a 0.

Q: 6 LoWPAN:

**6LoWPAN** is an [acronym](https://en.wikipedia.org/wiki/Acronym) of [*IPv6*](https://en.wikipedia.org/wiki/IPv6)*over Low-Power Wireless*[*Personal Area Networks*](https://en.wikipedia.org/wiki/Personal_area_network). [[1]](https://en.wikipedia.org/wiki/6LoWPAN#cite_note-eetimes-1) 6LoWPAN is the name of a concluded working group in the [Internet](https://en.wikipedia.org/wiki/Internet) area of the [IETF](https://en.wikipedia.org/wiki/IETF).[[2]](https://en.wikipedia.org/wiki/6LoWPAN#cite_note-6lowpan-2)

## ***6LoWPAN provides the upper layer system for use with low power wireless communications for IoT and M2M, originally intended for 802.15.4, it is now used with many other wireless standards.***

The 6LoWPAN system is used for a variety of applications including wireless sensor networks. This form of wireless sensor network sends data as packets and using IPv6 - providing the basis for the name - IPv6 over Low power Wireless Personal Area Networks.

6LoWPAN provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks. It provides end-to-end IPv6 and as such it is able to provide direct connectivity to a huge variety of networks including direct connectivity to the Internet.

In this way, 6LoWPAN adopts a different approach to the other low power wireless sensor network solutions.

6LoWPAN is an open standard defined by the Internet Engineering Task Force, IETF in their document RFC 6282. The IETF is the standards body that defines many of the open standards used in the Internet including HTTP, TCP, UDP and many others.

Whilst 6LoWPAN was originally conceived to build on top of IEEE 802.15.4, a standard that set out the lower layers for a 2.4 GHz low power wireless system, it is now being developed and adapted to work with many other wireless bearers including Bluetooth Smart; power line control, PLC, and low power Wi-Fi.

The 6LoWPAN group have then defined the encapsulation and compression mechanisms that enable the IPv6 data to be carried of the wireless network.

The development of the 6LoWPAN system was not as easy as might be thought as the basic natures of the two systems are very different. However it was believed that using packet data over a low power wireless sensor network would offer significant advantages in terms of data handling and management.

The overall system is aimed at providing wireless internet connectivity at low data rates and with a low duty cycle. However there are many applications where 6LoWPAN is being used:

* ***General Automation:***   There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
* ***Home automation:***   There is a large market for home automation. By connecting using IPv6, it is possible to gain distinct advantages over other IoT systems. The Thread initiative has been set up to standardize on a protocol running over 6LoWPAN to enable home automation.
* ***Smart Grid:***   Smart grids enable smart meters and other devices to build a micro mesh network and they are able to send the data back to the grid operator’s monitoring and billing system using the IPv6 backbone.
* ***Industrial monitoring:***   Automated factories and industrial plants provide a great opportunity for 6LoWPAN and using automation, can enable major savings to be made. The ability of 6LoWPAN to connect to the cloud opens up many different areas for data monitoring and analysis.

**Basic Requirements of 6LoWPAN:**

1. The device should be having sleep mode in order to support the battery saving.
2. Minimal memory requirement.
3. Routing overhead should be lowered.

**Features of 6LoWPAN:**

1. It is used with IEEE 802.15,.4 in the 2.4 GHz band.
2. Outdoor range: ~200 m (maximum)
3. Data rate: 200kbps (maximum)
4. Maximum number of nodes: ~100

**Advantages of  6LoWPAN:**

1. 6LoWPAN is a mesh network that is robust, scalable, and can heal on its own.
2. It delivers low-cost and secure communication in IoT devices.
3. It uses IPv6 protocol and so it can be directly routed to cloud platforms.
4. It offers one-to-many and many-to-one routing.
5. In the network, leaf nodes can be in sleep mode for a longer duration of time.

**Disadvantages of 6LoWPAN:**

1. It is comparatively less secure than Zigbee.
2. It has lesser immunity to interference than that Wi-Fi and Bluetooth.
3. Without the mesh topology, it supports a short range.

**Applications of 6LoWPAN:**

1. It is a wireless sensor network.
2. It is used in home-automation,
3. It is used in smart agricultural techniques, and industrial monitoring.

Q: