Unit 1: Introduction to Internet of Things

1.1 Definition & Characteristics of IoT
1.2 Introduction to IoT Architecture
1.3 Physical Design of IoT
1.3.1 Things in IoT
1.3.2 IoT Protocols (Ethernet , WIFI , WIMAX, LR-WPAN(Wireless personal area network), 2G/3G/4G Mobile Communication, IPV6,6LOWPAN,MQTT, WEB SOCKET)
1.4 Logical Design of IoT
1.4.1 IoT Functional Blocks
1.4.2 IoT Communicational Models

- Request – Response
- Publish –Subscribe
- Push –Pull
- Exclusive Pair

1.1 Definition & Characteristics of IoT

There are many IoT definitions. It just depends on how you look at it: the application perspective, the technological perspective, the industry context, the benefits, etc. According to the definition of IoT, It is the way to interconnection with the help of the internet devices that can be embedded to implement the functionality in everyday objects by enabling them to send and receive data. Today data is everything and everywhere. Hence, IoT can also be defined as the analysis of the data generate a meaning action, triggered subsequently after the interchange of data. IoT can be used to build applications for agriculture, assets tracking, energy sector, safety and security sector, defence, embedded applications, education, waste management, healthcare product, telemedicine, smart city applications, etc.

Characteristics of the Internet of Things :

There are the following characteristics of IoT as follows. Let's discuss it one by one.

1.Connectivity–

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, connection between people through internet devices like mobile phones ,and other gadgets, also connection between Internet devices such as routers, gateways, sensors, etc.

2.Intelligence and Identity–

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is

helpful in tracking the equipment and at times for querying its status.

3.Scalability–

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

4.Dynamic and Self-Adapting (Complexity) –

IoT devices should dynamically adapt themselves to the changing contexts and scenarios. Assume a camera meant for the surveillance. It should be adaptable to work in different conditions and different light situations (morning,afternoon,night).

5.Architecture–

IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ' products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

6.Safety–

There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical.

7.Self Configuring –

This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

Component of IOT:

1. **Control Unit:**
   - A small computer containing processor, memory, programmable IO peripheral and the control unit responsible for main operation.
2. **Sensor:**
   - A device that can measure a physical quantity and convert it into a

signal which will be read and interpreted by the microcontroller unit.

- Most of the sensors are categorized into two categories: Digital Sensors or Analog Sensors.

3. Communication Modules:

- These part of the device is responsible for communication with the rest of the IOT platform.
- It provides connectivity depending on whether it is wired or wireless communication.

4. Power Sources:

- It provides power to the device by passing current which generated by the sources like batteries, solar cells, etc.

Advantages of IOT:

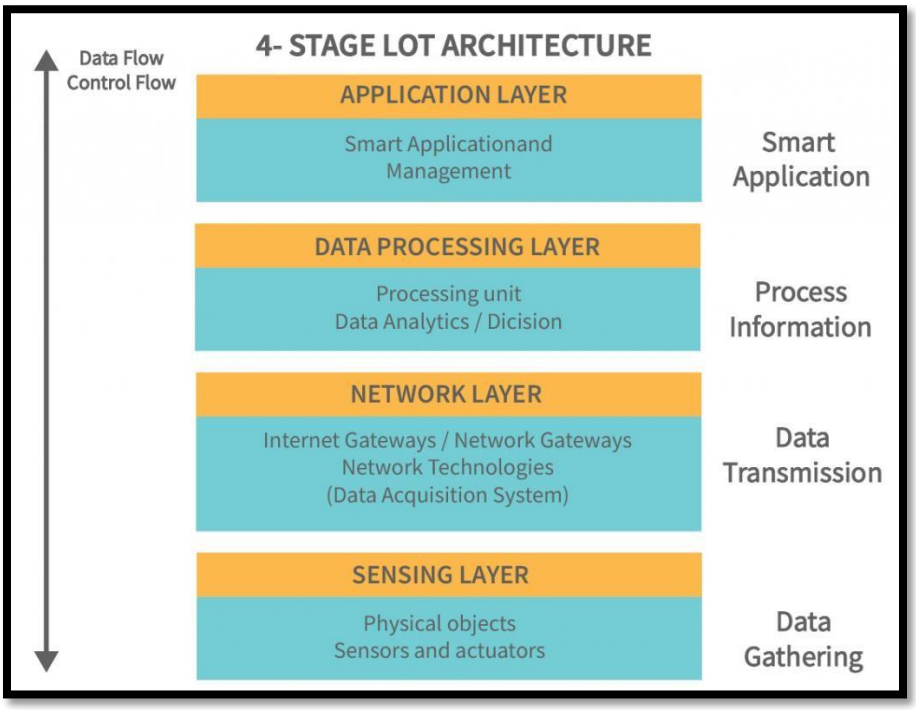
- Improved customer engagement and communication.
- Support for technology optimization.
- Support wide range of data collection.

Disadvantages of IOT:

- Loss of privacy and security.
- Complexity.
- Compatibility.
- Flexibility.

1.2 Introduction to IoT Architecture

- Internet of Things (IOT) technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of IOT, it works accordingly as per it has been designed/developed. But it has not a standard definedarchitecture of working which is strictly followed universally.
- The architecture of IOT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IOT is built.
- So, here in this article we will discuss basic fundamental architecture of IOT i.e., 4 Stage IOT architecture.



1. Sensing Layer –

- Sensors, actuators, devices are present in this Sensing layer.
- These Sensors or Actuators accepts data (physical/environmental parameters), processes data and then emits data over network.

2. Network Layer –

- Internet gateways, Network gateways, Data Acquisition System (DAS) are present in this layer.
- DAS performs data aggregation and conversion function (i.e.collecting data and aggregating data then converting analog data of sensors to digital data etc.).
- Advanced gateways which mainly opens up connection between Sensor networks and Internet also performs many basic gateway functionalities like malware protection, and filtering also sometimes decision making based on inputted data and data management services, etc.

3. Data processing Layer –

- This is processing unit of IOT ecosystem. Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business

applications where data is monitored and managed and further actions are also prepared. So here Edge IT or edge analytics comes into picture.

4. Application Layer –

- Data centers or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

1.3 Physical Design of IoT

1.3.1 Things in IoT

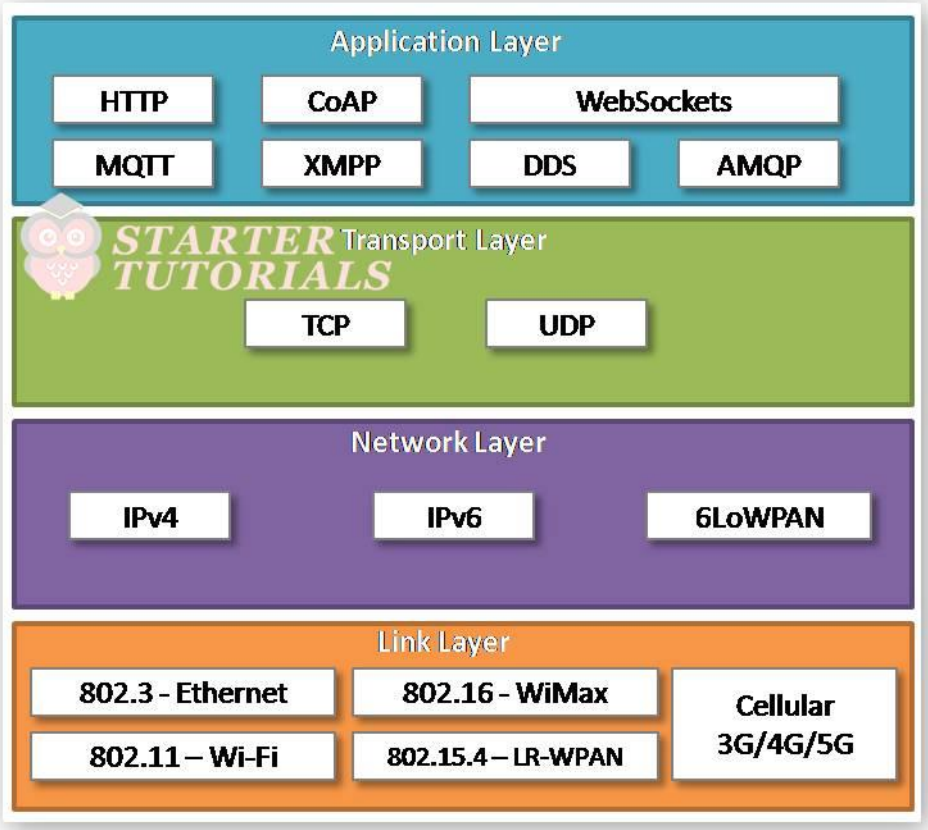
Things in IoT refers to IoT devices. Things have unique identities. Things can perform sensing, actuation, and monitoring. Some of the examples of things in internet of things are shown below.

Some of the examples of IoT devices are:

- Home appliances: smart TV, smart refrigerator, smart AC, etc.
- Smart phones and computers
- Wearables: smart watch, smart sensors, etc.
- Automobiles like self-driving cars
- Energy systems
- Retail : smart payment
- Printers
- Industrial machines
- Healthcare: smart watch, smart healthcare, etc.
- Surveillance: smart cameras, smart trackers, etc.

1.3.2 IoT Protocols (Ethernet , WIFI , WIMAX, LR-WPAN(Wireless personal area network), 2G/3G/4G Mobile Communication, IPV6,6LOWPAN,MQTT, WEB SOCKET)

A protocol is a set of rules that governs the communication between two or more devices. A protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods. An overview of different protocols used in IoT with respect to TCP/IP protocol stack is given below:



Link Layer Protocols

The link layer is responsible for establishing and terminating links between the nodes. The packets or datagrams travel through these links. The link layer also defines the format of packet that is to be communicated across the link and is responsible for physical addressing. The link layer also handles error detection, retransmission, flow control and access of the link. Protocols generally used at this layer are Ethernet, Wi-Fi, WiMax, LR-WPAN, cellular technologies, etc.

The summary of link layer protocols is as shown below:

Standard	Name	Medium	Speed	Range
IEEE 802.3	Ethernet	Coaxial/ Twisted-pair/ Fiber optic	10 Mbps – 40 Gbps +	100 m
IEEE 802.11	Wi-Fi	Radio Waves	1 Mbps – 6.75 Gbps	30 m
IEEE 802.16	WiMax	Radio Waves	1.5 Mbps – 1 Gbps	50 Km
IEEE 802.15.4	LR-WPAN	Bluetooth	40 Kbps – 250 Kbps	10 m
2G/3G/4G	Cellular	Radio Waves	9.6 Kbps – 100 Mbps	16 Km

Network Layer Protocols

The main role of the network layer is transfer the packet from sender to receiving host. The network layer also handles routing, which involves selecting the next node and forwarding the packets across the communication path. The network layer is also responsible for logical addressing (like IP address) and for congestion control which prevents the network from being overloaded with traffic.

Different protocols at network layer are:

- IPv4 (32-bit addresses)
- IPv6 (128-bit addresses)
- 6LoWPAN (IPv6 over Low power Wireless Personal Area Network)

Transport Layer Protocols

The main role of transport layer is providing end-to-end communication between the applications running on hosts. The transport layer provides a logical communication channel through which the end applications can communicate with each other. The transport layer is implemented on the end hosts. It is not present in the routers. The transport layer is also responsible for the reliable delivery of the message across the end nodes, flow control and multiplexing and demultiplexing of the channels at end nodes.

Different protocols at transport layer are:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Application Layer Protocols

The application layer is where the users of an IoT application interact with the IoT application/system. The application layer allows the users to interact with the IoT sensors and access other services provided by the communication network. The application layer provides services like authentication, naming, message formatting, email, etc, to the users.

Different protocols at transport layer are:

- HTTP (HyperText Transfer Protocol)

– Uses TCP, Stateless, Request-Response Model

- CoAP (Constrained Application Protocol)

– Uses UDP, Request-Response Model

- MQTT (Message Queue Telemetry Transport)

– Follows publish-subscribe model

– No security

– Used with low power devices

- XMPP (Extensible Messaging and Presence Protocol)

– Real-time communication, For sending XML data

- AMQP (Advanced Message Queuing Protocol)

– Supports both point-to-point and publisher-subscriber models

– High performance and secure protocol

– Uses TCP

- WebSocket

– Full-duplex connection over a single socket connection

– Uses TCP

- DDS (Data Distribution Service)

– Middleware standard, Reliable than MQTT

– Follows publish-subscribe model

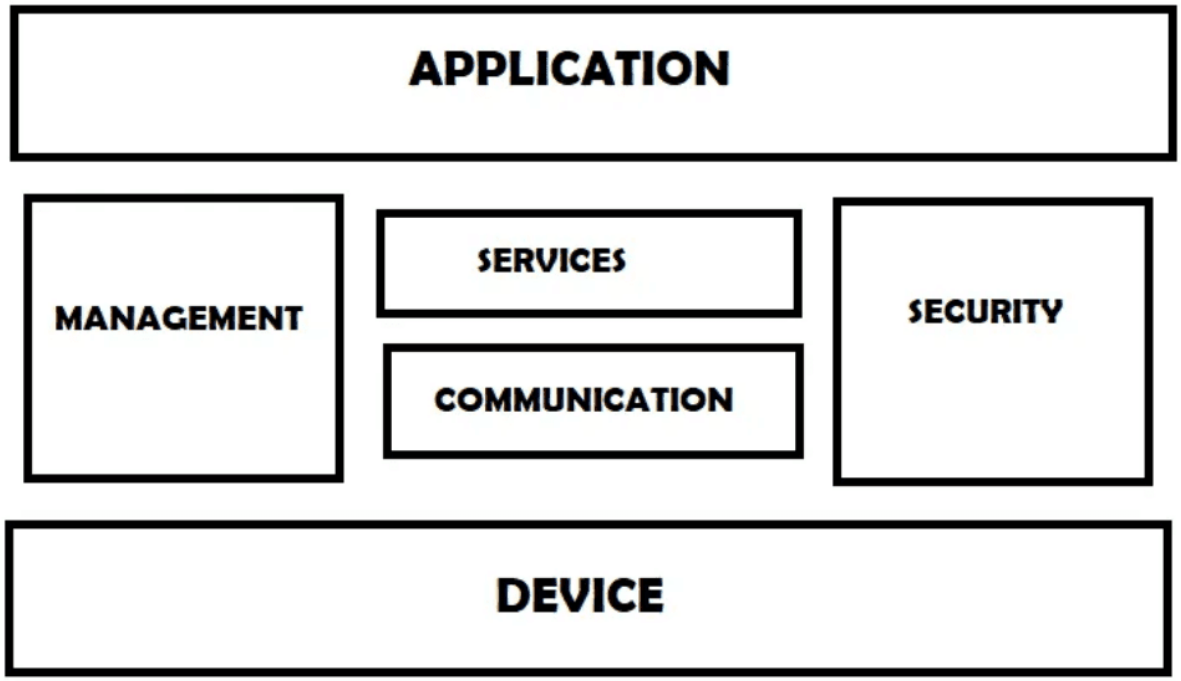
– Uses UDP

1.4 Logical Design of IoT

The logical design of an **IoT** system refers to an abstract representation of entities and processes without going into the low-level specifies of implementation. it uses **Functional Blocks**, **Communication Models**, and **Communication APIs** to implement a system.

1.4.1 IoT Functional Blocks

An IoT system consists of a number of functional blocks like Devices, services, communication, security, and application that provide the capability for sensing, actuation, identification, communication, and management.



These functional blocks consist of devices that provide monitoring control functions, handle communication between host and server, manage the transfer of data, secure the system using authentication and other functions, and interface to control and monitor various terms.

Application

It is an interface that provides a control system that use by users to view the status and analyze of system.

Management

This functional block provides various functions that are used to manage an IoT system.

Services

This functional block provides some services like monitoring and controlling a device and publishing and deleting the data and restoring the system.

Communication

This block handles the communication between the client and the cloud-based server and sends/receives the data using protocols.

Security

This block is used to secure an IoT system using some functions like authorization, data security, authentication, 2-step verification, etc.

Device

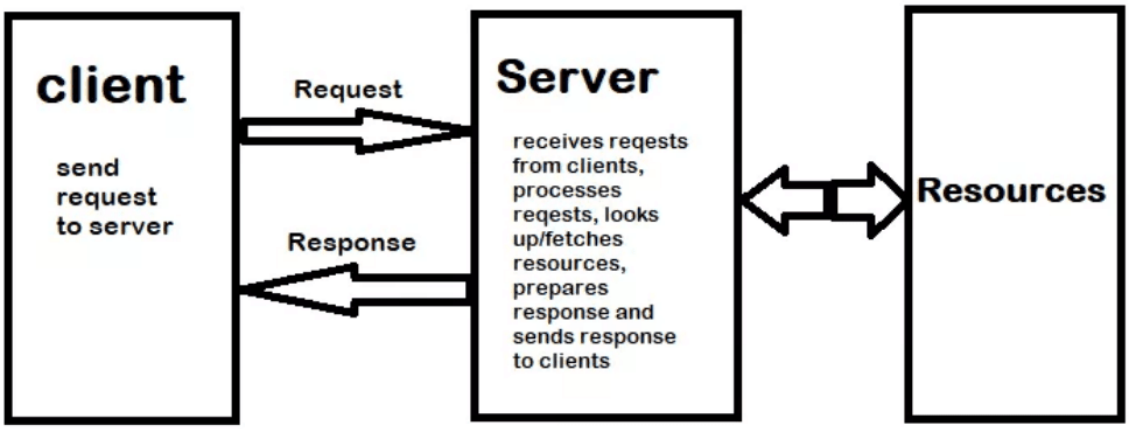
These devices are used to provide sensing and monitoring control functions that collect data from the outer environment.

1.4.2 IoT Communicational Models

There are several different types of models available in an IoT system that is used to communicate between the system and server like the request-response model, publish-subscribe model, push-pull model, exclusive pair model, etc.

Request-Response Communication Model

This model is a communication model in which a client sends the request for data to the server and the server responds according to the request. when a server receives a request it fetches the data, retrieves the resources and prepares the response, and then sends the data back to the client.



Request-Response Communication Model

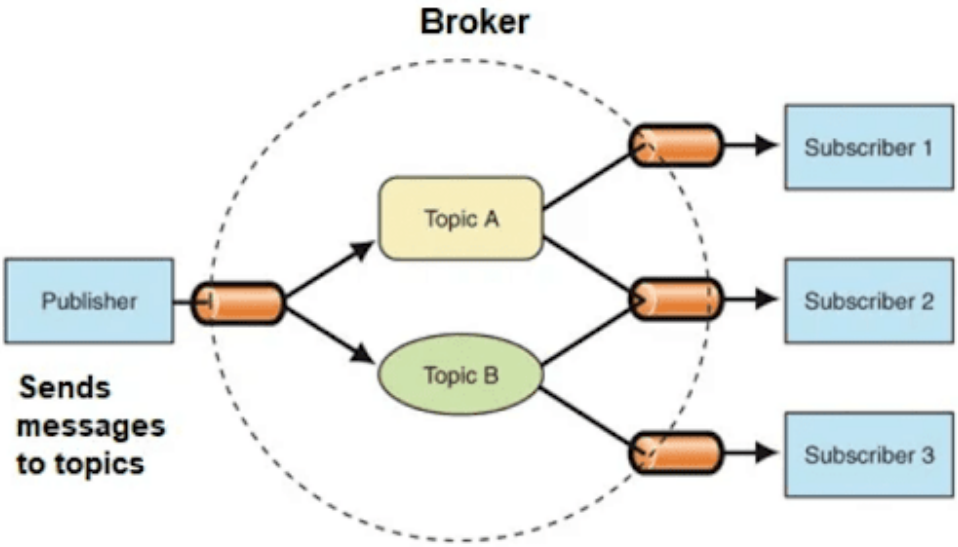
In simple terms, we can say that in the request-response model server send the response of equivalent to the request of the client. in this model, HTTP works as a request-response protocol between a client and server.

Example

When we search a query on a browser then the browser submits an HTTP request to the server and then the server returns a response to the browser(client).

Publish-Subscribe Communication Model

In this communication model, we have a broker between publisher and consumer. here publishers are the source of data but they are not aware of consumers. they send the data managed by the brokers and when a consumer subscribes to a topic that is managed by the broker and when the broker receives data from the publisher it sends the data to all the subscribed consumers.

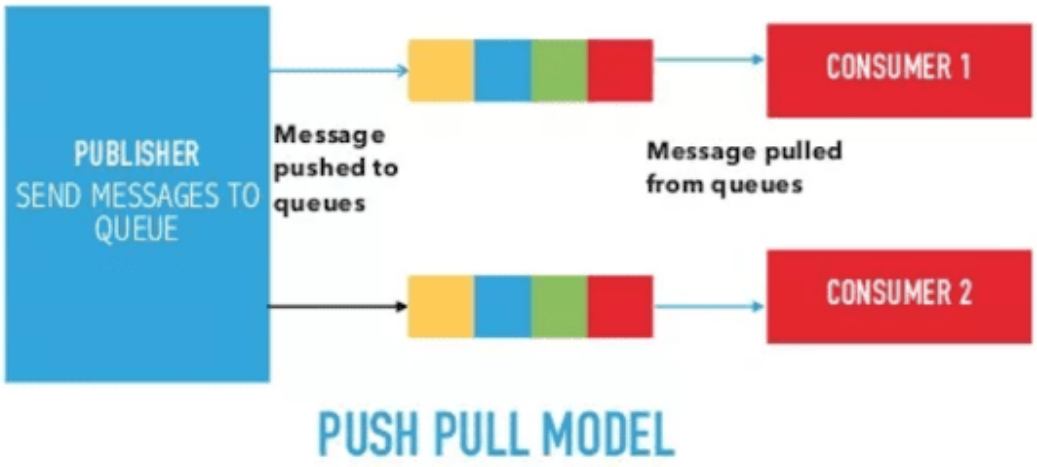


Example

On the website many times we subscribed to their newsletters using our email address. these email addresses are managed by some third-party services and when a new article is published on the website it is directly sent to the broker and then the broker sends these new data or posts to all the subscribers.

Push-Pull Communication Model

It is a communication model in which the data push by the producers in a queue and the consumers pull the data from the queues. here also producers are not aware of the consumers.



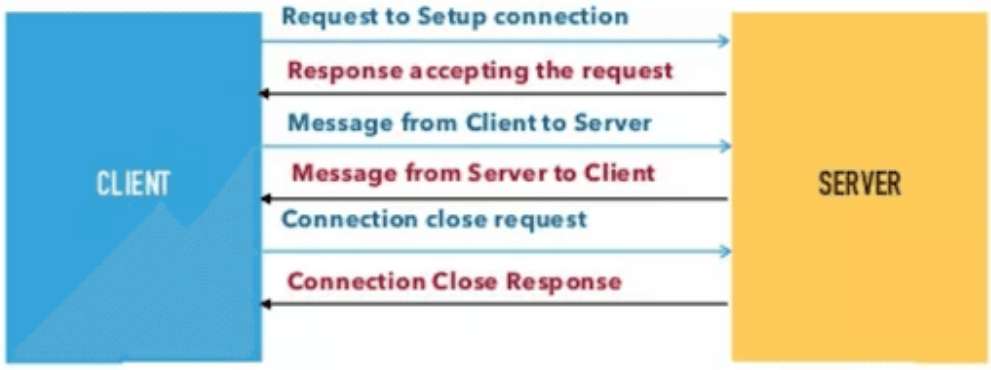
PUSH PULL MODEL

Example

When we visit a website we saw a number of posts that are published in a queue and according to our requirements, we click on a post and start reading it.

Exclusive Pair Communication Model

It is a bidirectional fully duplex communication model that uses a persistent connection between the client and server. here first set up a connection between the client and the server and remain open until the client sends a close connection request to the server.



EXCLUSIVE PAIR COMMUNICATION MODEL