# IOT UNIT 3 merged - note for the mentioned subject

Mechanical (Jawaharlal Nehru Technological University, Hyderabad)
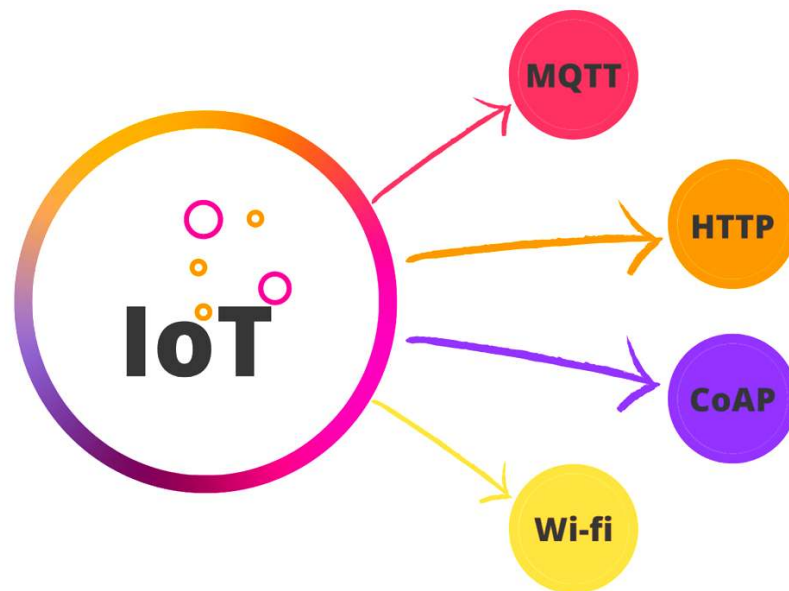


Scan to open on Studocu

# INTERNET OF THINGS

## Lecture Notes

## Unit-III
## Communications in the IOT



## Prepared by
## Dr.V V N BHASKAR
**HOD of Mechanical Engineering**
**ADITYA COLLEGE OF ENGINEERING**
**MADANAPALLE**

**Unit – III**

# COMMUNICATIONS IN THE IOT

**JNTUA Syllabus**
**Communication in the IoT:**
Internet Communications: An Overview, IP Addresses, MAC Addresses, TCP and UDP Ports,
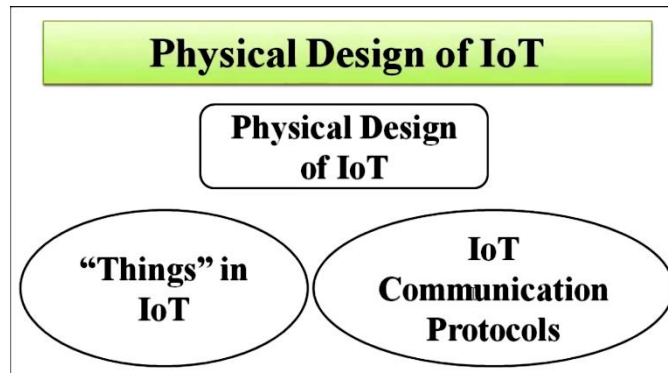Application Layer Protocols
**Prototyping Online Components:**
Getting Started with an API, Writing a New API, Real-Time Reactions, Other Protocols

## CONTENTS

## INTERNET COMMUNICATION

### 3.1 IOT COMMUNICATION PROTOCOLS or LAYERS



**Protocol**
- ➢ A protocol is a set of rules for communication between computers.
- ➢ It includes rules about how to initiate the conversation and what format the messages should be in.
- ➢ It determines what inputs are understood and what output is transmitted.
- ➢ It also specifies how the messages are sent and authenticated and how to handle/correct errors caused by transmission.

**OSI Mdel (Open Systems Interconnection Model) or TCP/IP Protocol Suite**
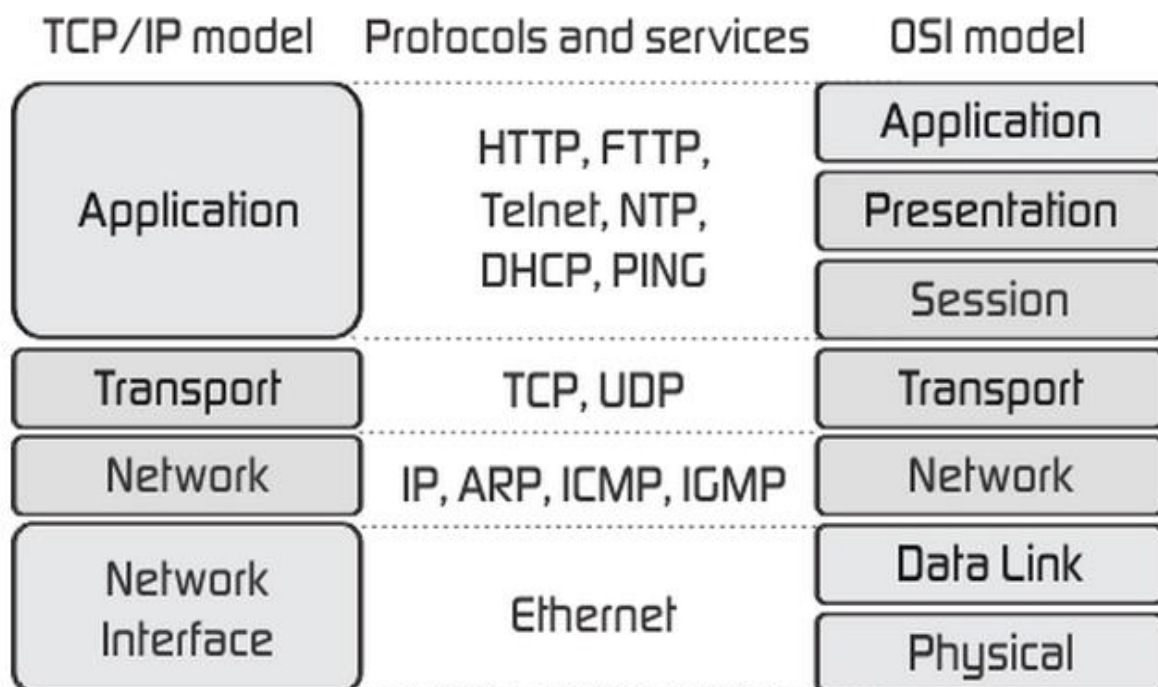


- ➢ The IOT consists of several layers and it operates at those layers/levels during exchange of data between devices.

- The various layers are
    1. **Link layer/Network interface layer**
    2. **Network /Internet layer**
    3. **Transport layer**
    4. **Application layer**

## 1. Link Layer

- ➢ It handles the moving of data into and out of a physical link in a network.
- ➢ The data link layer establishes and terminates a connection between two physically-connected nodes on a network.
- ➢ It determines how the data is send physically over the connecting medium i.e., optical fiber cable or wireless mode.
- ➢ The data link layer takes the data bits and "frames," and creates packets of the data.
- ➢ Data bits are encoded, decoded and organized in the data link layer, before they are transported as frames between two adjacent nodes on the same LAN or WAN.
- ➢ It breaks up packets into frames and sends them from source to destination.
- ➢ This layer is composed of two parts—Logical Link Control (LLC), and Media Access Control (MAC)
- ➢ **Protocols :**
    - 802.3 – Ethernet (Ethernet cables are used to provide an internet connection, connect devices to a local network )
    - 802.11 –WiFi (Wireless Fidelity)
    - 802.16 –WiMAX (Worldwide Interoperability for Microwave Access)
    - 802.15.4 – LR-WPAN (Low Range Wireless Personal Area Network)
    - 2G/3G/4G/5G Mobile communication .

## 2. Network/ Internet Layer

- ➢ This layer is responsible for sending IP datagrams from source network to destination network.
- ➢ The datagrams contain source and destination identity or address.
- ➢ It performs host  and packet routing .
- ➢ **Protocols:**
    - IP – Internet Protocol ( IPV4,IPV6)
    - ARP - Address Resolution Protocol
    - ICMP - Internet Control Message Protocol
    - IGMP stands for Internet Group Message Protocol.
    - RARP - Reverse Address Resolution Protocol

## 3. Transport Layer

- ➢ This layer provides end-to-end message transfer capability.
- ➢ Transport layer performs data encapsulation.
- ➢ It also provides services such as segmentation, error control , flow and congestion control etc.,

- ➢ **Segmentation** - It is the process of dividing a data packet into smaller units for transmission over the network.
- ➢ **Error control** – It is a mechanisms for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error control also includes a mechanism for correcting errors after they are detected.
- ➢ **Flow and Congestion Control** - It is an end-to-end mechanism that controls the traffic between a sender and a receiver.
- ➢ **Protocols :**
    - ▪ TCP  - Transmission Control Protocol
    - ▪ UDP - User Datagram Protocol

## 4. Application Layer

- ➢ The application layer is used by end-user software such as web browsers and email clients.
- ➢ It provides protocols that allow software to send and receive information and present meaningful data to users.
- ➢ It performs data encoding and process-to- process communication using ports.
- ➢ **Protocols :**
    - ▪ HTTP - Hyper Text Transfer Protocol
    - ▪ POP - Post Office Protocol
    - ▪ Telnet- Teletype Network Protocol
    - ▪ DNS -Domain Name System
    - ▪ FTP - File Transfer Protocol
    - ▪ SMTP -Simple Mail Transfer Protocol
    - ▪ SNMP -Simple Network Management Protocol
    - ▪ DHCP -Dynamic Host Configuration Protocol
    - ▪ TFTP -Trivial File Transfer Protocol

## 3.2 IP ADDRESS

- ➢ IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.
- ➢ An  IP address is a unique number assigned to every device on a TCP/IP network.
- ➢ Internet Protocol knows the addresses of the destination and source devices.
- ➢ In the world of low-level computer networking, however, numbers are much easier to deal with. So, IP addresses are numbers.
- ➢ Though this is convenient for computers, it's tough for humans to read, so IP addresses are usually written as four 8-bit numbers separated by dots (from 0.0.0.0 to 255.255.255.255)
- ➢ An IP address is a string of numbers separated by dot(.)
- ➢ IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38.
- ➢ An IP address consists of two parts, i.e., the first one is  network address, and the other one is a host address.

- There are two types of IP addresses:  IPv4 , IPv6
- **IPv4**
  - It is 4<sup>th</sup> version of Internet Protocol.
  - It is deployed in 1980
  - IPv4 is 32-Bit IP address.
  - It  stores $2^{32}$ addresses.
  - It is considered the primary IP and carries 94% of Internet traffic.
  - IPv4 is a numeric addressing method
  - IPv4 binary bits are separated by a dot(.)
  - Example - 192.158.1.38
- **IPv6**
  - It is 6<sup>th</sup> version of Internet Protocol.
  - It is deployed in the year 1995
  - IPv6 is a 128-Bit IP address
  - It stores $2^{132}$ addresses
  - IPv6 is an alphanumeric addressing method.
  - IPv6 binary bits are separated by a colon(:)
  - Example  -  2001:0db8:0000:0000:0000:ff00:0042:7879

- There are two kinds of IP addresses: static and dynamic
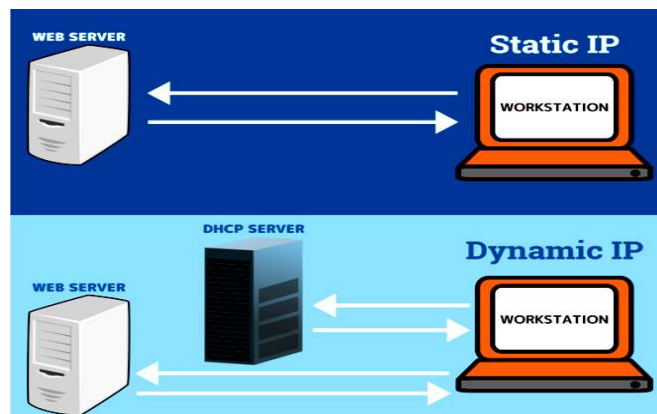


- **Static IP address**
  - It is simply an address that doesn't change.
  - Once the device is assigned a static IP address, that number typically stays the same until the device is decommissioned or your network architecture changes.
  - Static IP addresses generally are used by servers or other important equipment.
  - A static IP address may be IPv4 or IPv6 usually use static IPv4 addresses for permanent addresses.
- **Dynamic IP addresses**
  - This is subject to change, sometimes at a moment's notice.
  - Dynamic IP is the standard used  for consumer equipment.

- Dynamic addresses are assigned, as needed, by Dynamic Host Configuration Protocol (DHCP) servers.
- For example, a hotel probably has a static IP address, but each individual device within its rooms would have a dynamic IP address.
- Within the home or business network, the dynamic IP address is generally used for the devices – Desktop, Laptop, smart phones, streaming media devices, tablet, etc.,
- A static IP address is more likely to be relevant for a business, while a dynamic IP address is appropriate for a home network.

## 3.3 MAC ADDRESS

- MAC stands for Media Access Control.
- It is a 48-bit number, usually written as six groups, separated by colons.
- The MAC address is listed as series of 12 digits, listed as the Physical Address.
- Example -  01:23:45:67:89:ab
- As well as an IP address, every network-connected device also has a MAC
- This MAC address is like the final address on a postal physical envelope.
- It is used to differentiate different machines on the same physical network so that they can exchange packets.
- A MAC address is a hardware identification number that uniquely identifies each device on a network.
- The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed.
- MAC address is a unique number which is used to track a device in a network.
- MAC address provides a secure way to find senders or receivers in the network and helps prevent unwanted network access.
- MAC address is also used in Wi-Fi networks at the airport for a specific device in order to identify it.

## 3.4 DNS (DOMAIN NAME SYSTEM)

- DNS translates human readable domain names to machine readable IP address.
- Although computers can easily handle 32-bit numbers, even formatted as dotted quads they are difficult for humans to remember.
- The Domain Name System (DNS) helps our brains navigate the Internet.
- DNS is a way to identify and locate computers connected to internet.
- A domain name always consists of two or more components separated by dots(.)
- Examples :
  - www.google.co.in
  - www.facebook.com
  - www.jntua.ac.in
  - www.wikipedia.org
  - www.harvard.edu
- Each domain name has a top-level domain (TLD), like .com or .in, which further subdivides into .co .uk and .gov .org, and so on.

### 3.5 TCP AND UDP PORTS

➢ Transmission Control Protocol and User Datagram Protocol are used to connect two devices over the Internet or other networks.

➢ Whenever any TCP/IP message is sent over the internet, it has to be sent to the right port.

➢ To give data packages, an entrance to the PC or server at the other end of the connection, the "doors" have to be open.

➢ These openings into the system are called ports.

➢ TCP ports are referred to by numbers ( 0 to 65535)

➢ For both the TCP and UDP, there are some standard ports which are required when developing the web pages. They are listed below.

| TCP | | UDP | |
|---|---|---|---|
| FTP | 20,21 | DNS | 53 |
| SSH | 22 | BooTPS/DHCP | 67 |
| Telnet | 23 | TFTP | 69 |
| SMTP | 25 | SNMP | 161 |
| DNS | 53 | | |
| HTTP | 80 | | |
| POP3 | 110 | | |
| NTP | 123 | | |
| IMAP4 | 143 | | |
| HTTPS | 443 | | |

✓ TCP - Transmission Control Protocol
✓ FTP –File Transfer Protocol
✓ SSH – Secure Shell
✓ Telnet - Teletype Network Protocol
✓ SMTP -Simple Mail Transfer Protocol
✓ DNS - Domain Name System
✓ HTTP- Hyper Text Transfer Protocol
✓ POP - Post Office Protocol
✓ NTP – Network Time Protocol
✓ IMAP4 –Internet Mail Access Protocol
✓ UDP – User Datagram Protocol
✓ DHCP -Dynamic Host Configuration Protocol
✓ TFTP -Trivial File Transfer Protocol
✓ SNMP -Simple Network Management Protocol

## 3.6 APPLICATION LAYER PROTOCOLS / OTHER PROTOCOLS

➢ This defines how the applications interface with lower layer protocols to send data over the network.

➢ This enables process-to-process communication using ports.

➢ Some of the application layer protocols are

1. **HTTP**: Hyper Text Transfer Protocol that forms foundation of WWW. Follow request response model.

2. **HTTPS** : The HTTPS protocol is actually just a mix-up of plain old HTTP over the Secure Socket Layer (SSL) protocol.

3. **CoAP**: Constrained Application Protocol for machine-to-machine(M2M) applications with constrained devices, constrained environment and constrained networks. Uses client server architecture.

4. **WebSocket** : allows full duplex communication over a single socket connection.

5. **MQTT:** Message Queue Telemetry Transport is based on publish-subscribe model. Uses client server architecture. Well suited for constrained environment.

6. **XMPP**: Extensible Message and Presence Protocol for real time communication and streaming data between network entities. Support client-server and server-server communication.

7. **DDS**: Data Distribution Service is data centric middleware standards for device-to-device or machine-to-machine communication. Uses publish-subscribe model.

8. **AMQP**: Advanced Message Queuing Protocol is open application layer protocol for business messaging. Supports both point-to-point and publish-subscribe model.

## WHAT IS MQTT?

➢ Message Queue Telemetry Transport is a messaging protocol designed for low-bandwidth, high latency, unreliable networks.

➢ This makes it much easier to do one-to-many messaging, compared to HTTP.

➢ MQTT's features make it an excellent option for sending high volumes of sensor messages to analytics platforms and cloud solutions.

➢ It was developed initially by IBM , both open and closed source, are available, together with libraries for many different languages.

➢ MQTT is used for data exchange between constrained devices and server applications.

➢ It keeps bandwidth requirements to an absolute minimum, handles unreliable networks, requires little implementation effort for developers, and is, therefore, ideal for Machine-to-Machine (M2M) communication.

## PROTOTYPING ONLINE COMPONENTS

## 3.7 GETTING STARTED WITH AN API, WRITING A NEW API (APPLICATION PROGRAMMING INTERFACE)
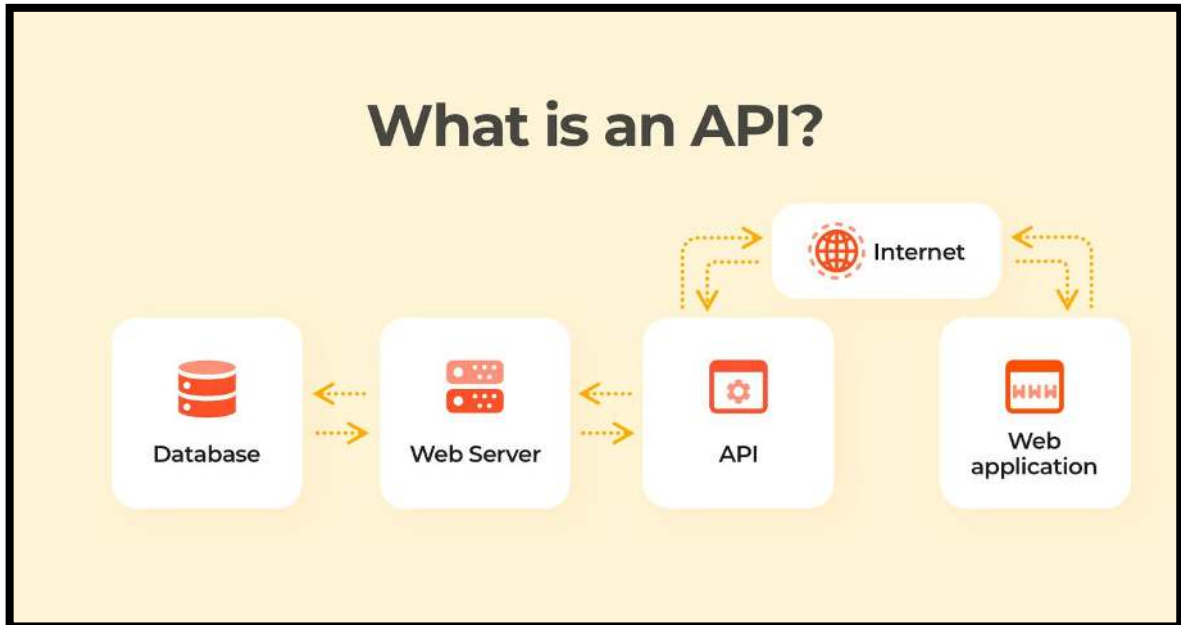


- ➢ API  is a software that allows two applications to talk to each other.
- ➢ An API defines the messages that are sent from client to server and from server to client.
- ➢ API allows apps to send information between each other.
- ➢ **Example** – Through Phonpe app different other sites can be accessed for recharging of mobile phone or payment of electricity bills, booking of gas cylinder, bike insurance etc.,
- ➢ While there are numerous protocols and technologies involved, the main purpose of APIs is always the same: to let one piece of software communicate with another.
- ➢ This can simplify app development, saving time and money.
- ➢ In other words, an API is the messenger that delivers your request to the provider that you're requesting it from and then delivers the response back to you.
- ➢ For example, to look at a friend's photo on Flickr, you might do the following:
  1. Launch Chrome or Firefox.
  2. Search for the Flickr website in Google and click on the link.
  3. Type in your username and password and click "Login".
  4. Look at the page and click on the "Contacts" link.
  5. Click on a few more links to page through the list of contacts till you see the one you want.
  6. Scroll down the page, looking for the photo you want, and then click on it.

## 3.8  REAL TIME REACTIONS

- ➢ While connecting the Arduino or Raspberry boards, the current Ethernet/HTTP shields tend to block during the connection, which means that during that time, the microcontroller can't easily do any other processing.
- ➢ To improve the real time reactions, connection time, an action is to be performed instantly on the board.
- ➢ If the server has to perform an action immediately, that "immediately" will depend on the connection time.
- ➢ The other alternative solutions for HTTP are MQTT, XMPP, and CoAP.
- ➢ There are two types of factors to be considered. They are **"polling" and "Comet"** technologies.
- ➢ **Polling** – The client makes a periodic request in a specified time interval to the server. This is known as Polling.
- ➢ The CPU keeps on checking if the device needs attention i.e make requests at regular intervals.
- ➢ We can make this quicker like polling for every 10 seconds. But this would put load on the SERVER and CLIENT
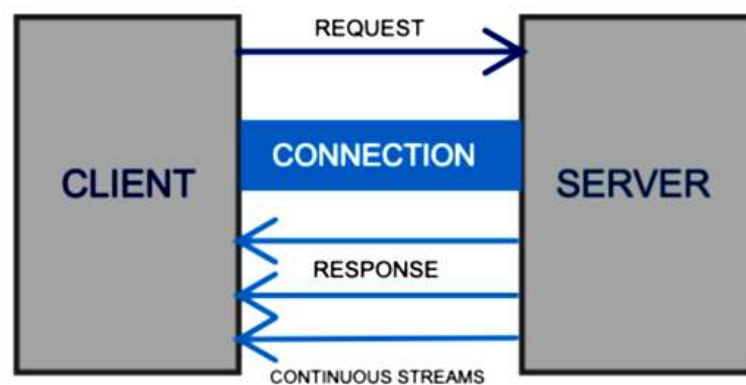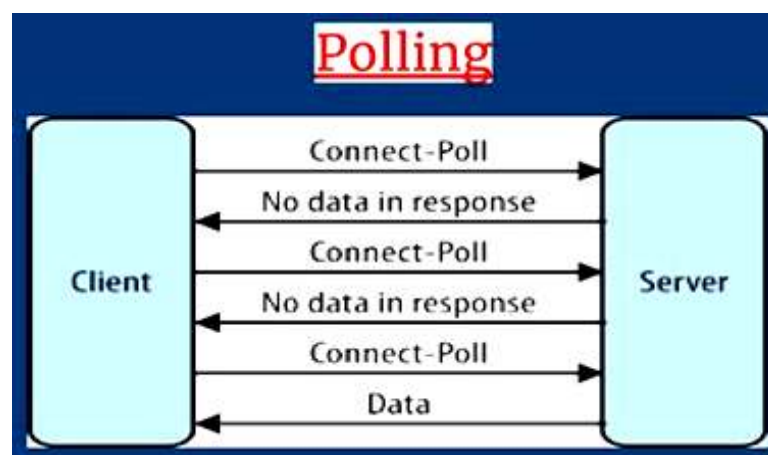




STREAMING

> ➢ **Comet -** This is a web application model in which long held HTTP request allows a web server to push data to a browser. Comet is getting around the inefficiencies of polling.
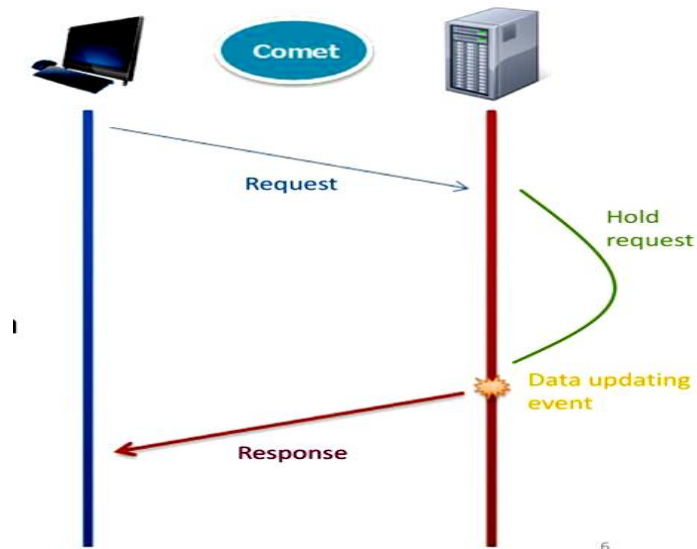


> *"You're going to see this 'IoT' start demanding network performance and making the networks much more aware of what is on top of them."*
>
> *-Hans Vestberg,* Swedish businessman and CEO of Verizon communications

## Question Bank

**Unit III – Communications in IOT**

### 2 Marks Questions

1. What are the seven layers of OSI model?
2. Distinguish between IP address and MAC address.
3. Differentiate between data and information in IoT.
4. Which of the communication protocols are used by IoT?
5. Compare TCP and UDP.
6. Compare Static IP and Dynamic IP.
7. Write a short note on DNS.
8. Define MQTT.
9. What is API?
10. What is Polling and Comet ?

### 10 Mark Questions

1. Explain IOT communication protocols.
2. Explain layered IOT architecture using a figure.
3. What is an IP address? Explain.
4. Explain (i) TCP ports (ii) UDP ports.
5. Explain different application layer protocols for the IoT.
6. Which protocol is used to link all the devices in the IoT? Explain.
7. Illustrate communication protocols used in IoT.
8. What is prototyping the online components? Explain.
9. Enumerate MQTT and AMQP protocol.
10. Explain Real time reactions in IoT.