INTERNET OF THINGS (IOT)

Asst. Prof. DR. MUHANED TH. M. AL-HASHIMI

Tikrit University

Collage Of Computer And Mathematical Science

2024 - 2025

INTRODUCTION TO IOT
&
BASICS OF NETWORKING

LECTURE 1

2204 - 2025

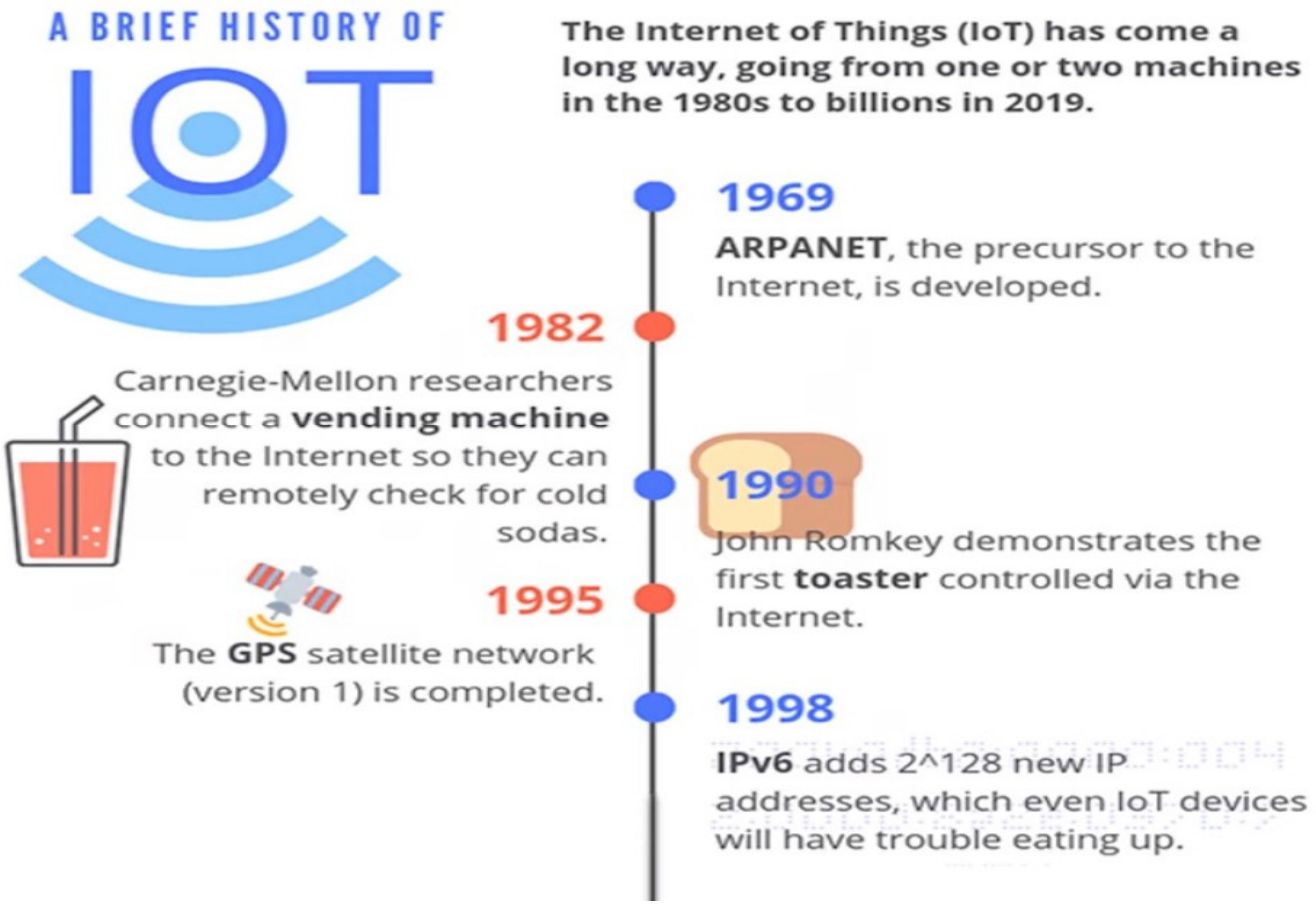
11 Of February

Outline

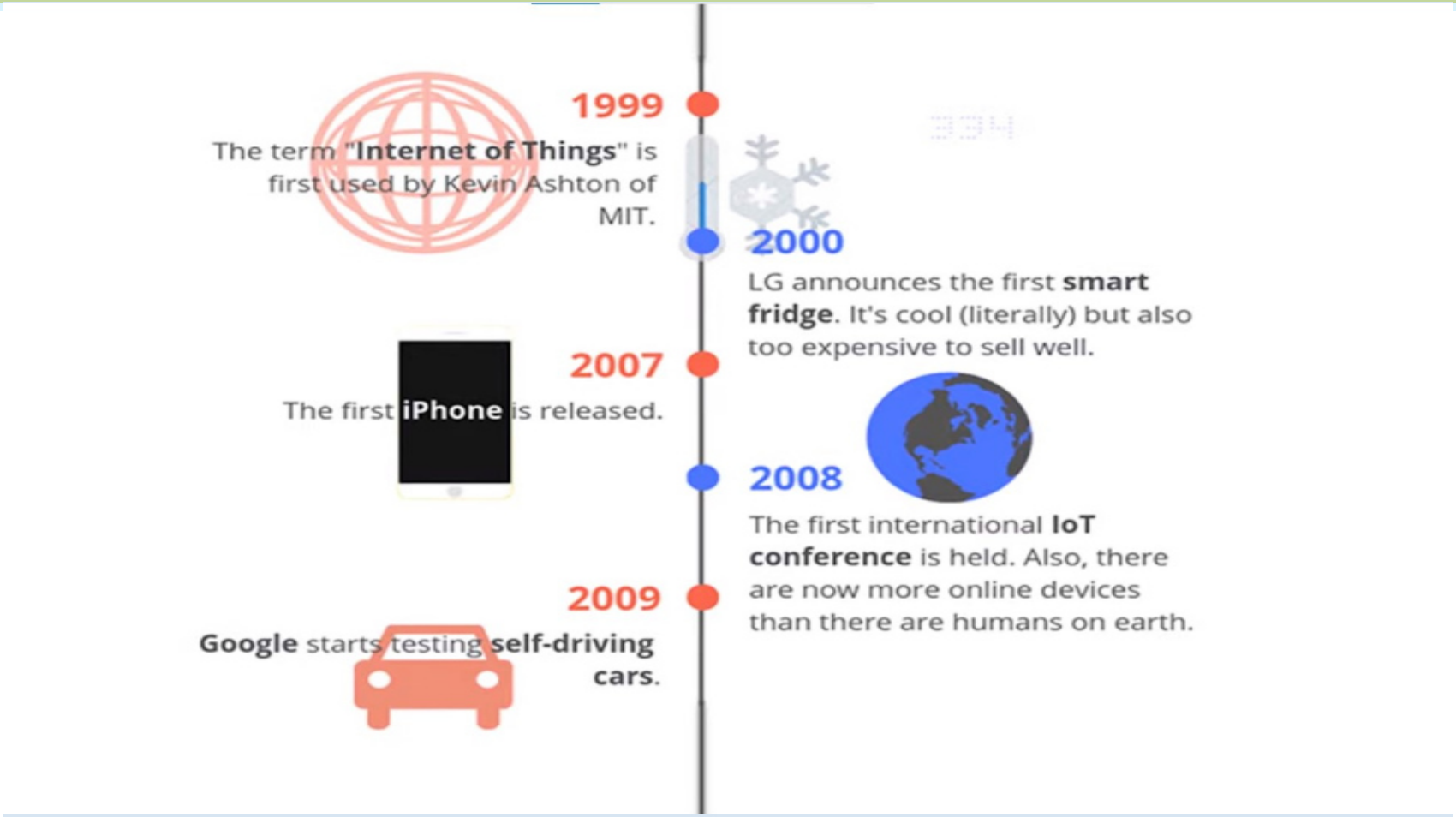
This lecture will talk about:

- IoT Background
- IoT Concept
- IoT Definition
- IoT Characteristic
- Introduction to Basics of Networking
- Network Types
- Layered Network Models
- Addressing
- TCP/IP Transport layer
- The building blocks of IoT

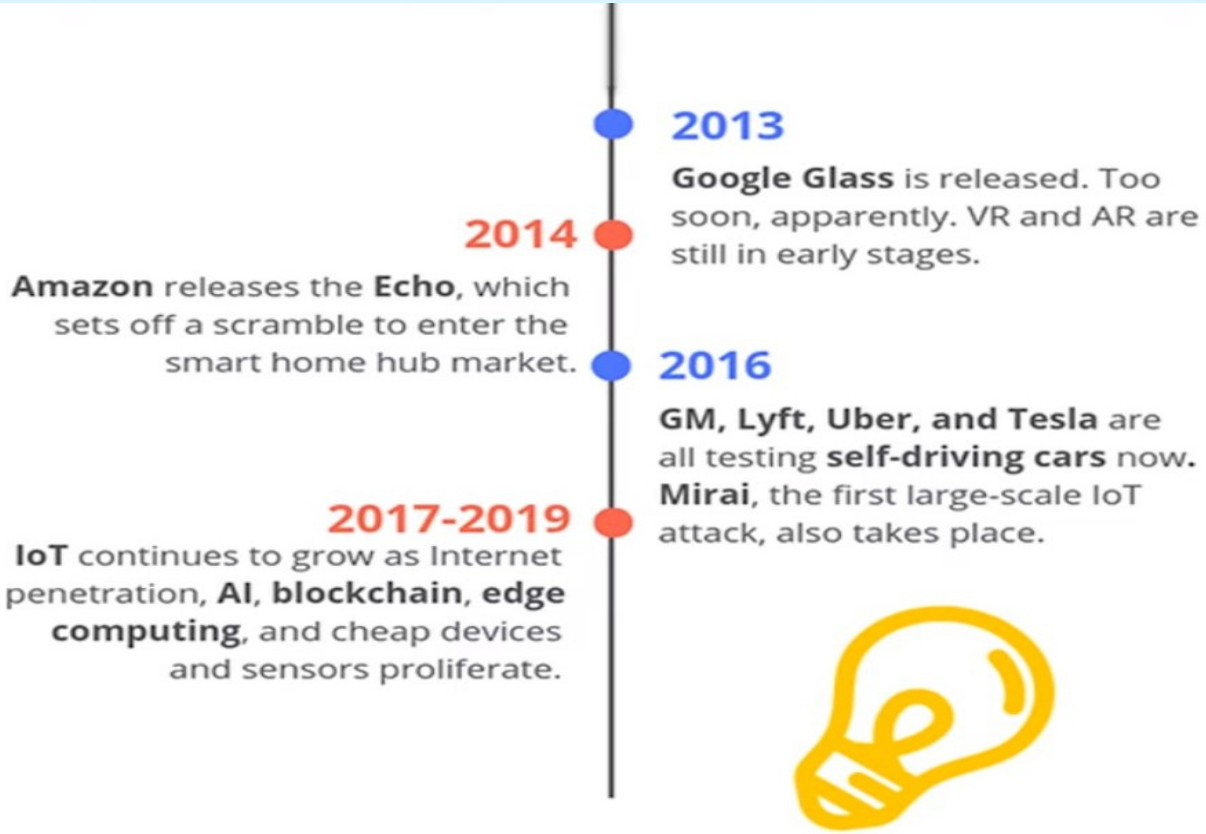
IoT Background



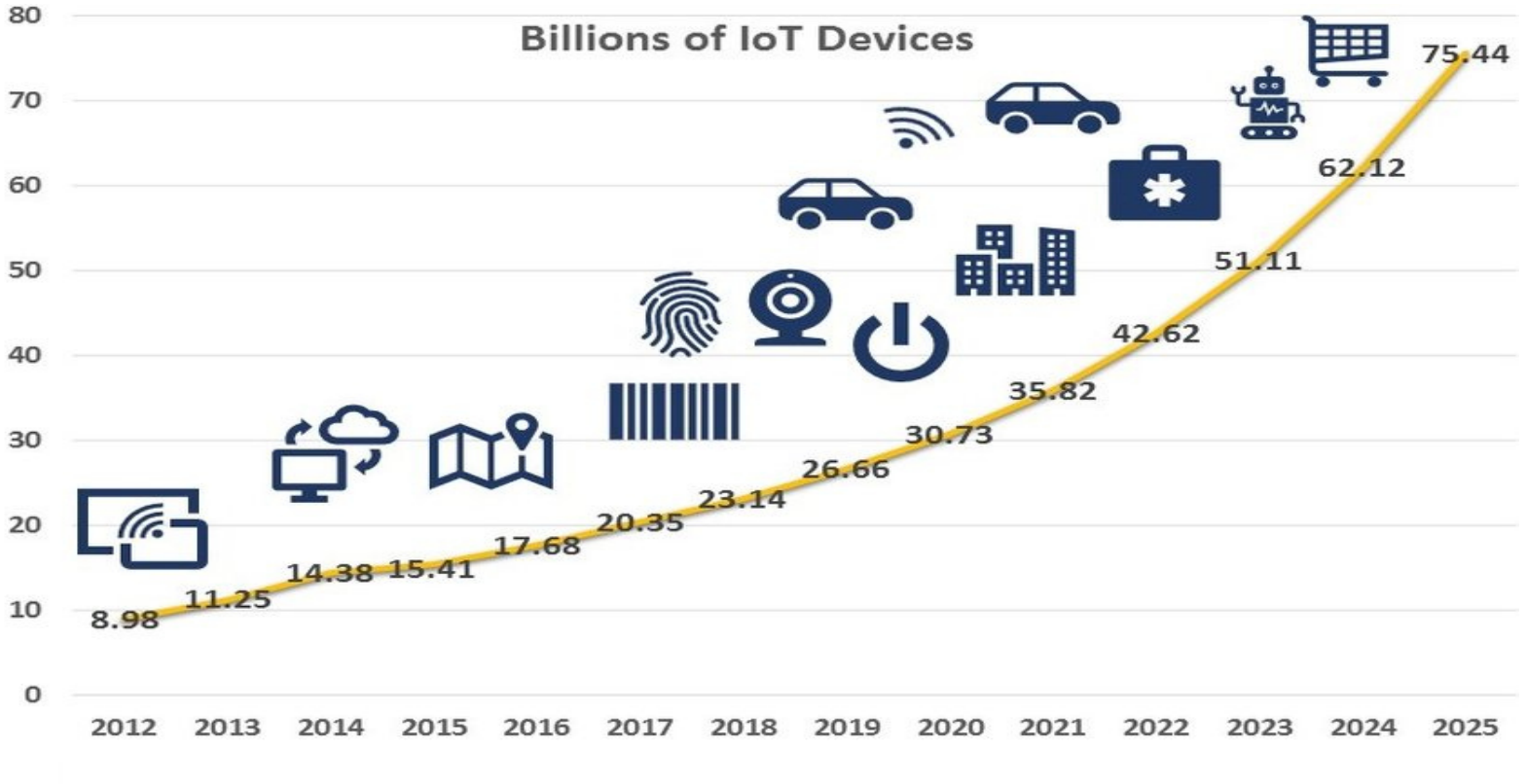
IoT Background



IoT Background



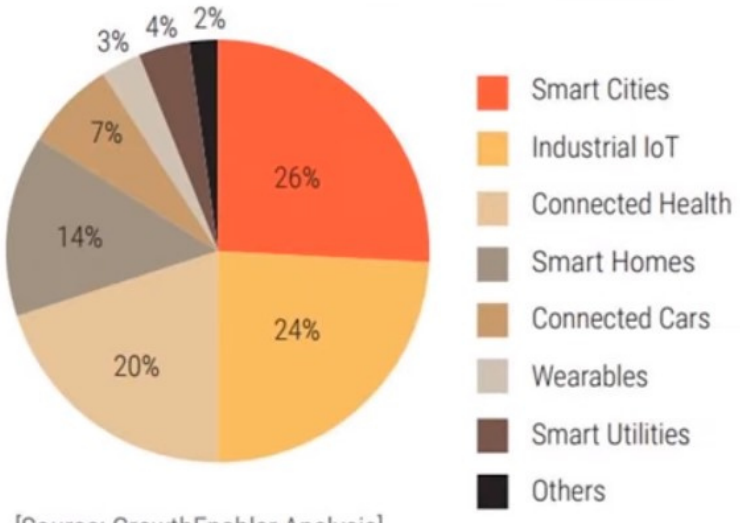
IoT Background & Important



Combined Access Barring Scheme for IoT Devices Using Bayesian Estimation - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Internet-of-things-IoT-devices-in-billions-over-the-years_fig1_347820285 [accessed 6 Feb, 2023] / **https://www.statista.com/**

IoT Background & Important

[Sources: GrowthEnabler Analysis/MarketsandMarkets]



[Source: GrowthEnabler Analysis]

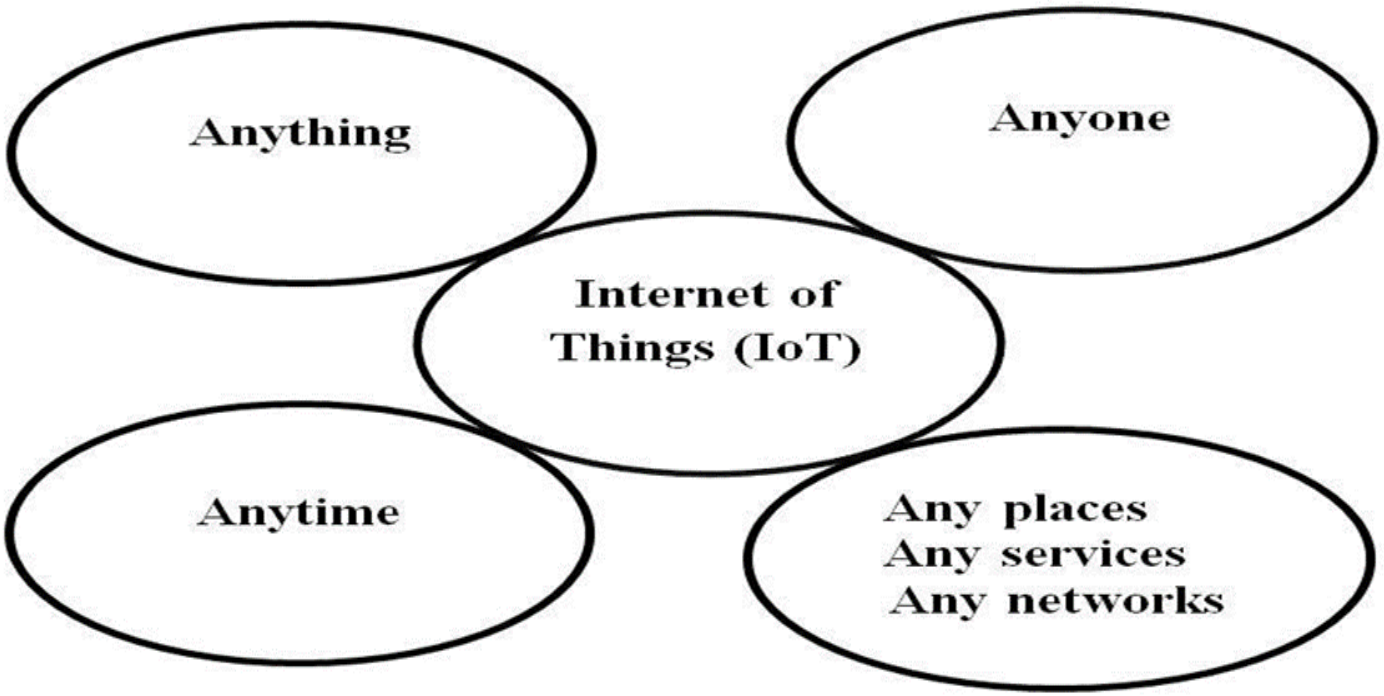
IoT Concept

- The Ubiquitous Computing **vision** of *Mark Weiser* implies that computers, as we currently know them, "**disappear**," or, more precisely, move into the **background**. Everyday objects and our immediate environment then assume the tasks and abilities of computers (Weiser and Brown, **1996**).

IoT Concept

- In another highly regarded article, *Weiser* together with *Brown* introduced the notion of "**Calm Computing**." They also refer to a connected world full of computers. However, only in cases of service provision or when a need exists for interaction do those computers or their respective services become "**visible**"; at other times, those capabilities are "**calm**" in the **background**, and not intrusive or even visible to the users (Weiser and Brown, **1996**).

IoT Concept


Anything
Anyone
Internet of Things (IoT)
Anytime
Any places
Any services
Any networks

IoT Concept

Image Source : https://riberasolutions.com/smart-city-iot-and-ai/

IoT Concept

Core Concepts: *Smart Objects* and *Smart Environments*

- all **physical objects** can be turned into smart objects, for example, conventional everyday objects such as pens, wristwatches, cars ,,, etc.

- **smart environment** is the context information gathered by sensors in order to provide adapted applications and services.

IoT Concept

Related Concepts:

Machine-to-Machine Communications, **Industrial** Internet of Things.

M2M can be viewed as the **forerunner** of IoT.

- **M2M** communications refers to direct wired or wireless communication between devices using any communications channel that does **not necessarily require direct human intervention**.

- **M2M** communication can **include** industrial production facilities, enabling a sensor or meter **to communicate the data** that it records (e.g., temperature, throughput, and inventory level) **to application software** that can further process them (e.g., adjusting an industrial process based on technical parameters, such as temperature or triggering new processes, such as placing orders to replenish inventory).

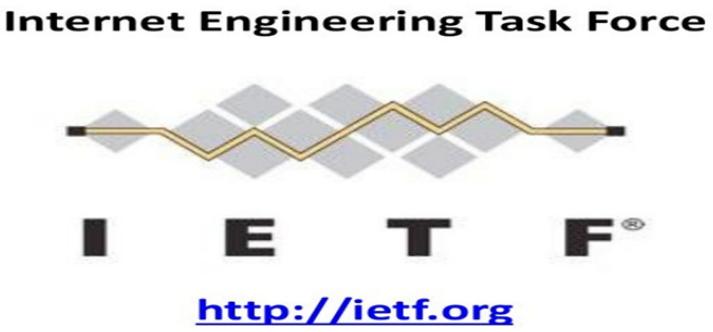
IoT Definition

- **Defintion 1**

A **global infrastructure** for the information society, enabling advanced services by **interconnecting (physical and virtual)** ***things*** based on, **existing and evolving**, information and communication technologies.

IoT Definition

- **Defintion 2**

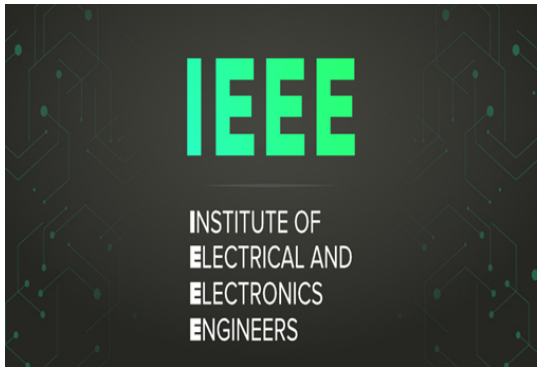


IoT is a **worldwide network** of interconnected **objects uniquely addressable**, based on **standard communication protocols**.

IoT Definition

- **Defintion 3**

A **network** of **items** each **embedded with sensors** which are **connected to the Internet**.



IoT Characteristic

- Dynamic and Self Adapting.
- Self-Configuring.
- Interoperable and Communication Protocols.
- Unique Identity.
- Intergrated into Information Network.

IoT Characteristic

- **Dynamic and Self-Adapting:** IoT devices and systems may have the capability to dynamically adapt to the **changing contexts** and **take actions based on their operating condition**, user's context, or sensed environment. such as **surveillance cameras** day and night.
- **Self-Configuring:** IoT devices may have the self-configuring capability, allowing a large number of devices to **work together** to provide **certain functionality**. such as **weather monitoring**.
- **Interoperable and Communication Protocols:** IoT devices may support a number of interoperable communication protocols and can communicate with other devices.
- **Unique Identity:** each IoT device has a unique identity and a unique identifier. Such as **IP** and Uniform Resource Identifier **URI.**
- **Integrated into Information Network:** it does collaborate with other infrastructure networks. For example data from a large number of connected weather monitoring, IoT nodes can be aggregated and analyzed to predict the weather.

Basics of Networking / Introduction

- Before diving into the details of IoT communication and networking technologies, we need an **overview** of the **current networking environment** and the challenges it brings.

- Understanding **IoT** communication requires **understanding** its **origins** and **progression** throughout the years.

Basics of Networking / Introduction

- Typically, networking refers to the **linking of computers and communication network devices** (also referred to as hosts), which **interconnect** through a **network** (Internet or Intranet) and are separated by **unique device identifiers**.
- These **hosts** may be **connected** by a **single path** or through **multiple paths** for **sending** and **receiving** **data**.
- The **data** **transferred between** the **hosts** may be **text**, **images**, or **videos**, which are typically in the **form** of **binary** bit **streams**.

Basics of Networking / Network Types

- **Computer networks** are **classified** according to various parameters:

1) Type of **connection**.
2) physical **topology**.
3) Network **reachability** (reach of the network).

- These classifications are **helpful** in **deciding** the **requirements of a network setup** and **provide insights** into the **appropriate selection of a network type** for the setup.

Basics of Networking / Network Types

1) Based on **connection** types,

- Depending on the **way** a host **communicates** with other hosts, computer networks are of two types.

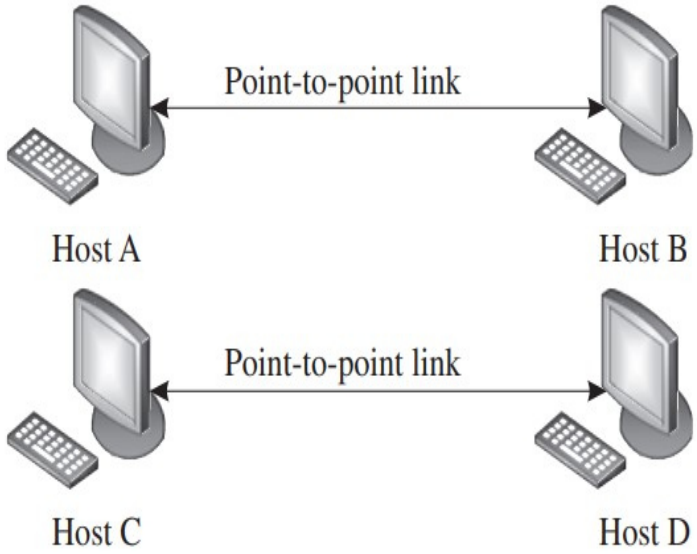
I. Point-to-point:

II. Point-to-multipoint:

Basics of Networking / Network Types

I. Point-to-point:

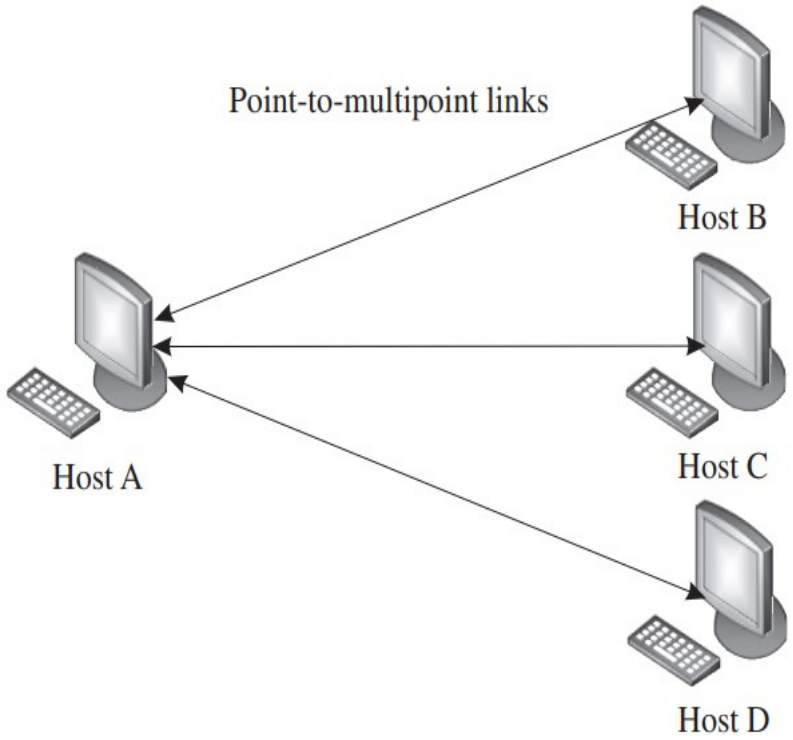
- Point-to-point connections are used to **establish direct connections** between two hosts.
- remote control for an air conditioner or television is a point-to-point connection.
- Regarding **computer networks**, point-to-point connections find usage for **specific purposes**.



Basics of Networking / Network Types

II. Point-to-multipoint:

- In a point-to-multipoint connection, **more than two hosts share the same link**.
- Point-to-multipoint connections find popular use in **wireless networks** and **IP telephony**.
- The channel is shared between the various hosts, either **spatially** or **temporally**.
- **Frequency** Division Multiple **Access** (**FDMA**) & **Time** Division Multiple **Access** (**TDMA**) are the **techniques** used to deploy.



Basics of Networking / Network Types

2) Based on physical topology

- Depending on the physical manner in which communication paths between the hosts are **connected**, computer networks can have the following four broad topologies:

I. Star.
II. Mesh.
III. Bus.
IV. Ring.

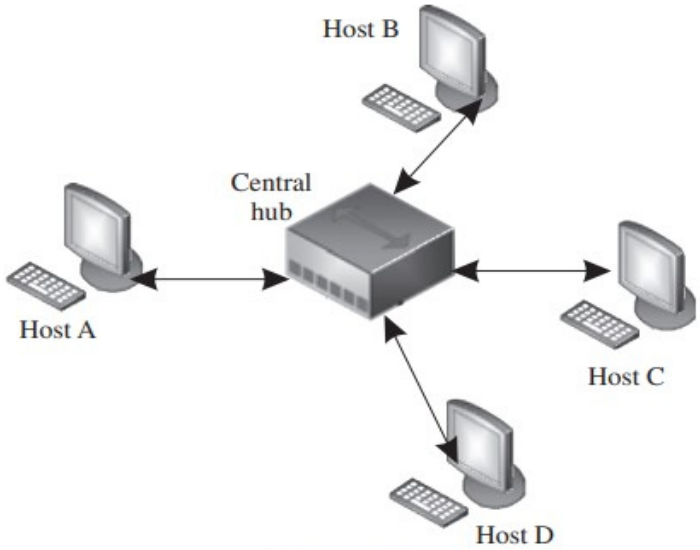
Basics of Networking / Network Types

2) Based on physical topology

I. **Star:**

In a star topology, every host has a **point-to-point** link to a central controller or hub.

- The **hub** acts as the network traffic exchange.
- This topology is cheaper and easier to set up.
- Main disadvantage of this topology is the danger of a single point of failure. If the hub fails, the whole network fails.



(a) Star topology

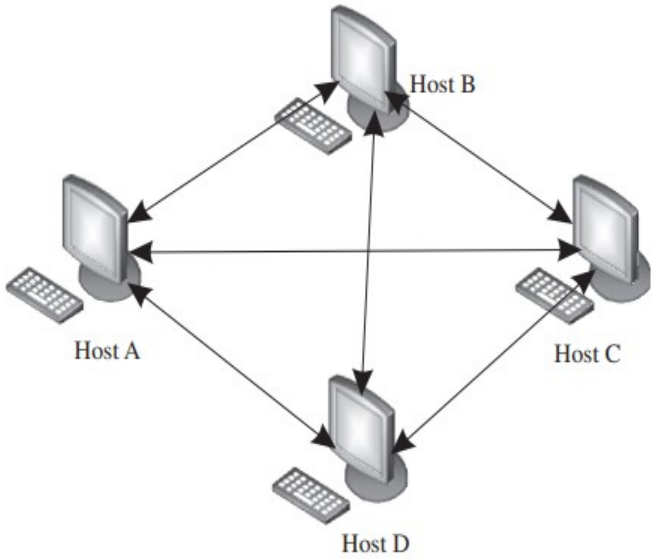
Basics of Networking / Network Types

2) Based on physical topology

II. Mesh:

In a mesh topology, every host is connected to every other host using a dedicated link (in a **point-to-point** manner).

- There are a total of $n(n-1)/2$ dedicated full duplex links between the hosts.
- This massive number of links makes the mesh topology expensive.
- First significant advantage: **robustness** and **resilience** of the system.
- Second advantage: **security** and **privacy** of the traffic as the data.
- Third advantage: **reduced data load**.



(b) Mesh topology

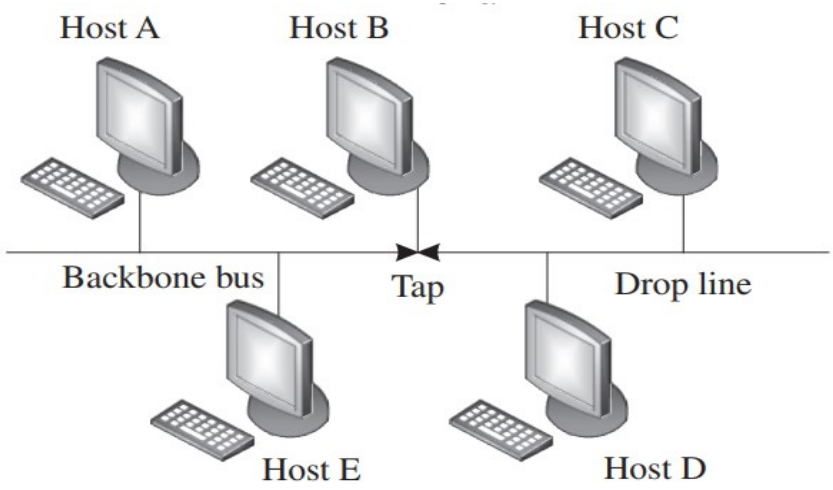
Basics of Networking / Network Types

2) Based on physical topology

III. Bus:

A bus topology follows the point-to-multipoint connection.

- **Backbone cable** or **bus serves** as the **primary** traffic **pathway** between the hosts.
- Restriction on the length of the bus and the number of hosts that can be simultaneously connected.
- Advantage: ease of installation and cheap.
- Disadvantage: difficulty in fault localization within the network.



(c) Bus topology

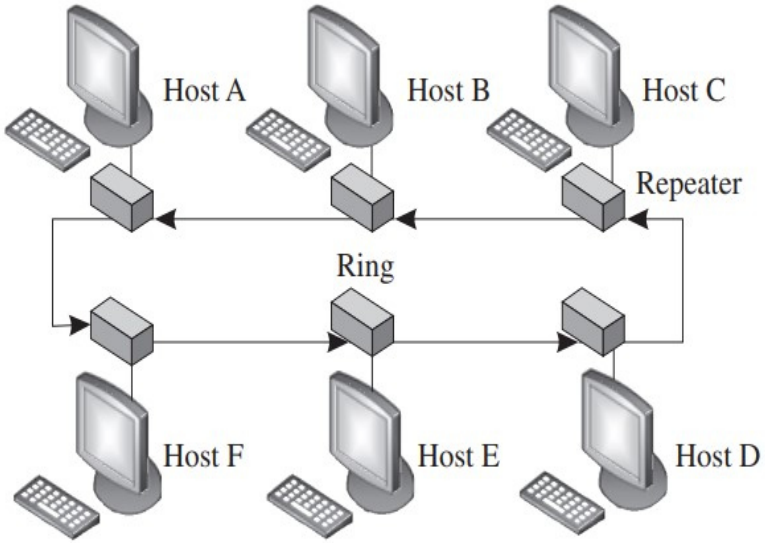
Basics of Networking / Network Types

2) Based on physical topology

IV. Ring:

works on the principle of a connection.

- **Repeaters** will be used on either side of the hosts.
- The **repetition** of this system forms a **ring**.
- repeater **captures**, regenerate and **passes** to the next one.
- Advantage: Fault identification and setup of the ring topology is **quite simple** and straightforward.
- Disadvantage: high probability of a **single point** of failure.



Basics of Networking / Network Types

In Summary: Network topologies

Table 1.1 Network topology comparison

Topology	Feature	Advantage	Disadvantage
Star	Point-to-point	Cheap; ease of installation; ease of fault identification	Single point of failure; traffic visible to network entities
Mesh	Point-to-point	Resilient against single point of failures; scalable; traffic privacy and security ensured	Costly; complex connections
Bus	Point-to-multipoint	Ease of installation; cheap	Length of backbone cable limited; number of hosts limited; hard to localize faults
Ring	Point-to-point	Ease of installation; cheap; ease of fault identification	Prone to single point of failure

Basics of Networking / Network Types

3) Based on Network reachability.

- Computer networks are divided into **four** broad categories based on network reachability:

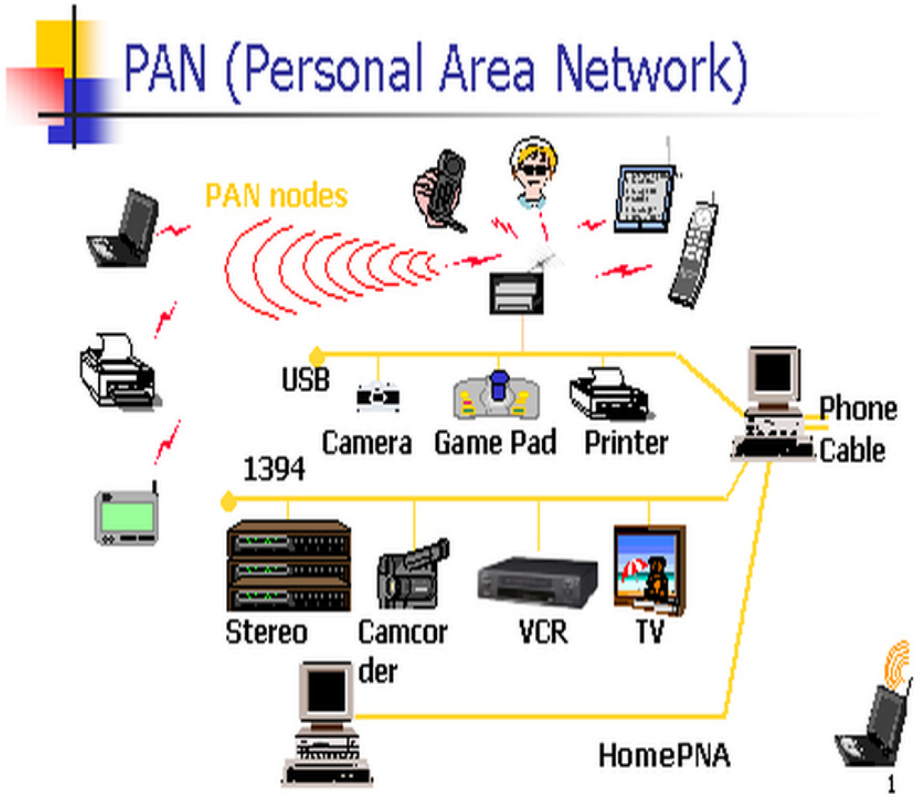
I. personal area networks (PAN).
II. local area networks (LAN).
III. metropolitan area networks (MAN).
IV. wide area networks (WAN).

Basics of Networking / Network Types

3) Based on Network reachability.

I. personal area networks (PAN).

- Mostly restricted to **individual usage**.
- A good **example** of PANs may be connected wireless headphones, wireless speakers, laptops, smartphones, wireless keyboards, wireless mouse, and printers within a house.
- make use of **low-range** and **low-power technologies** such as Bluetooth, zigBEE, xBEE & Wi-fi.
- **reachability** of PANs lies in the range of a **few centimeters to a few meters**.

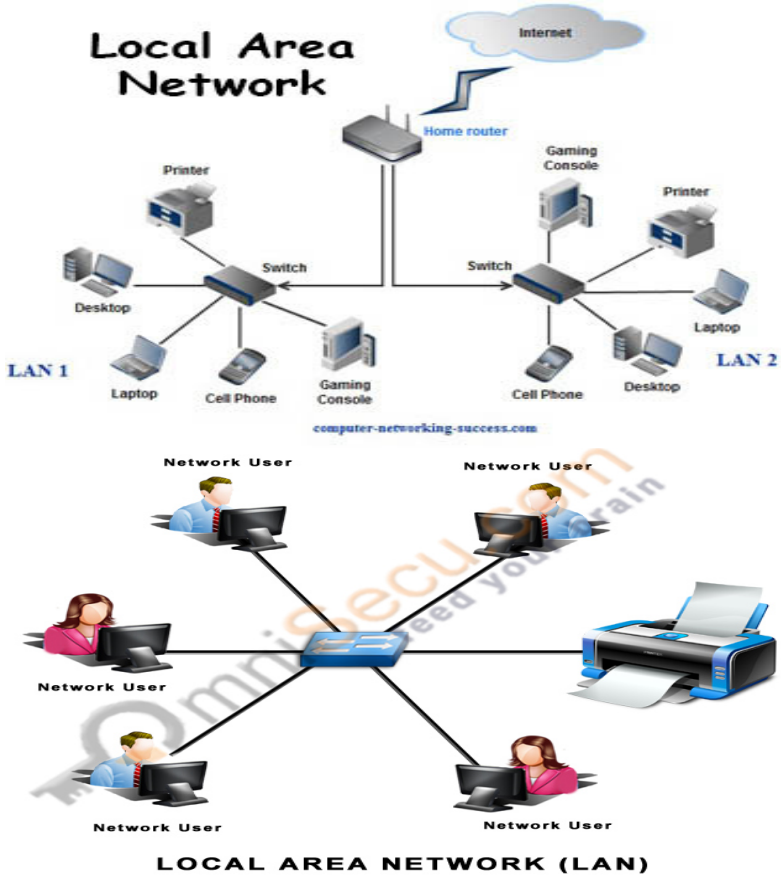


Basics of Networking / Network Types

3) Based on Network reachability.

II. local area networks (LAN).

- A LAN is a **collection of hosts linked to a single network** through wired or wireless connections.
- LANs are restricted to **buildings**, **organizations**, or **campuses**.
- The lines are further **redistributed** to **multiple hosts** within the LAN-enabling hosts.
- LANs **range** from **100 Mbps** to **1000 Mbps**, with very high fault-tolerance levels.
- Commonly used network **components** in a LAN are **servers**, **hubs**, **routers**, **switches**, **terminals**, and **computers**.

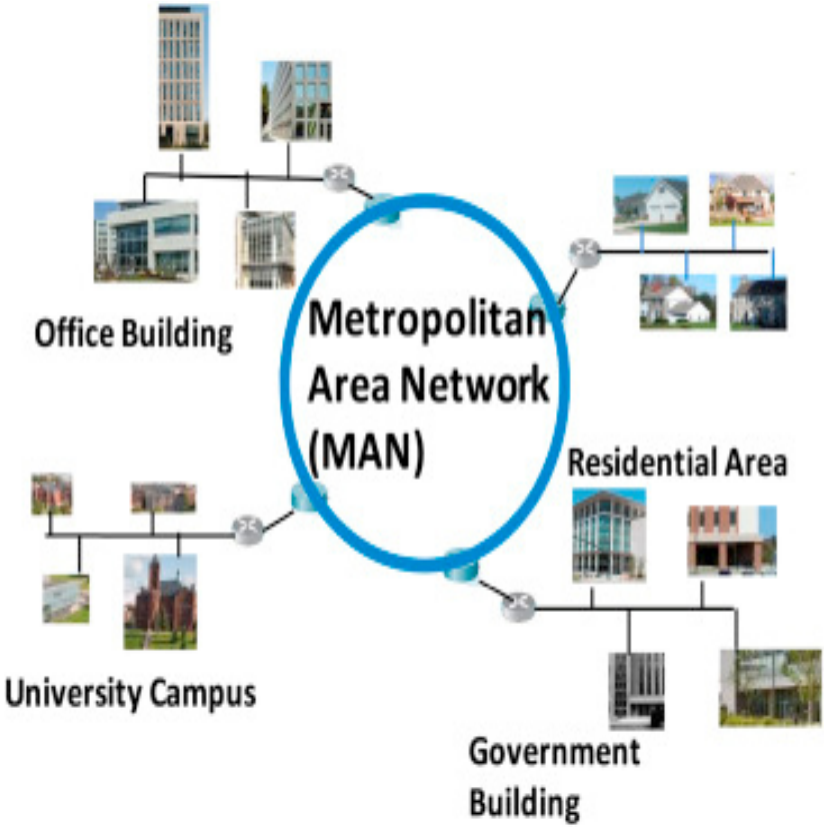


Basics of Networking / Network Types

3) Based on Network reachability.

III. metropolitan area networks (MAN).

- The reachability of a MAN lies **between** that of a **LAN and a WAN**.
- Typically, MANs connect **various organizations** or **buildings** within a given geographic location or **city**.
- An excellent example of a MAN is an **Internet service provider (ISP).**

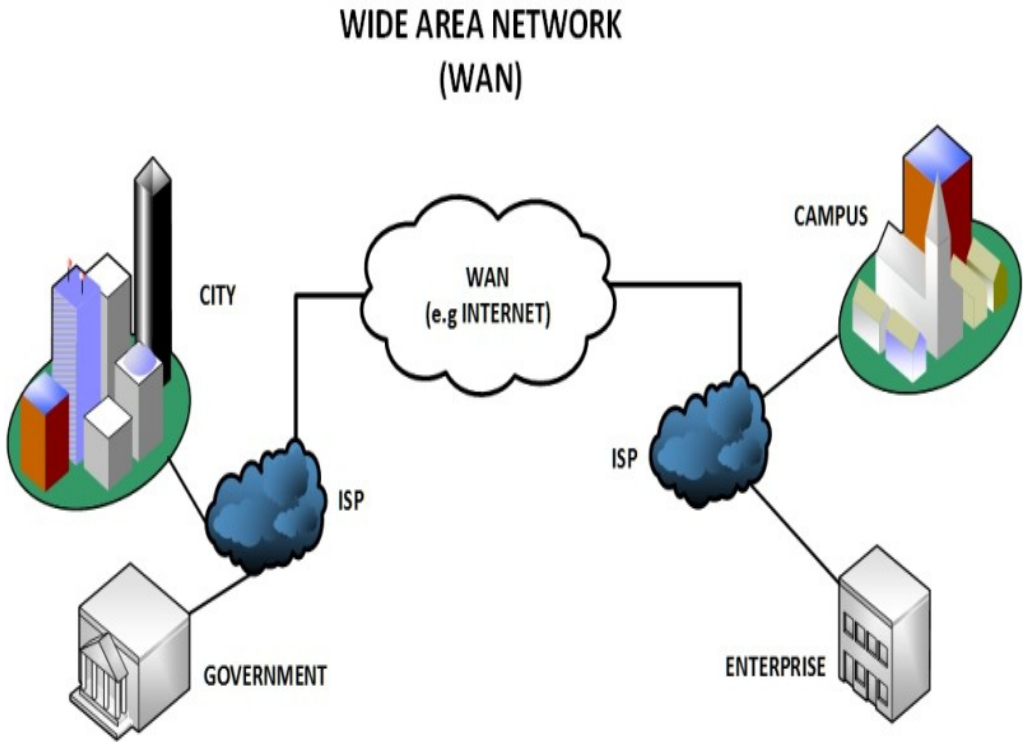


Basics of Networking / Network Types

3) Based on Network reachability.

IV. wide area networks (WAN).

- WANs typically connect **diverse geographic locations**.
- restricted within the boundaries of a **state or country**.
- Public switched telephone networks (**PSTNs**) or **satellite-based links**.
- Due to the **long transmission ranges**, WANs tend to have **more errors and noise** during transmission and are **very costly to maintain**.

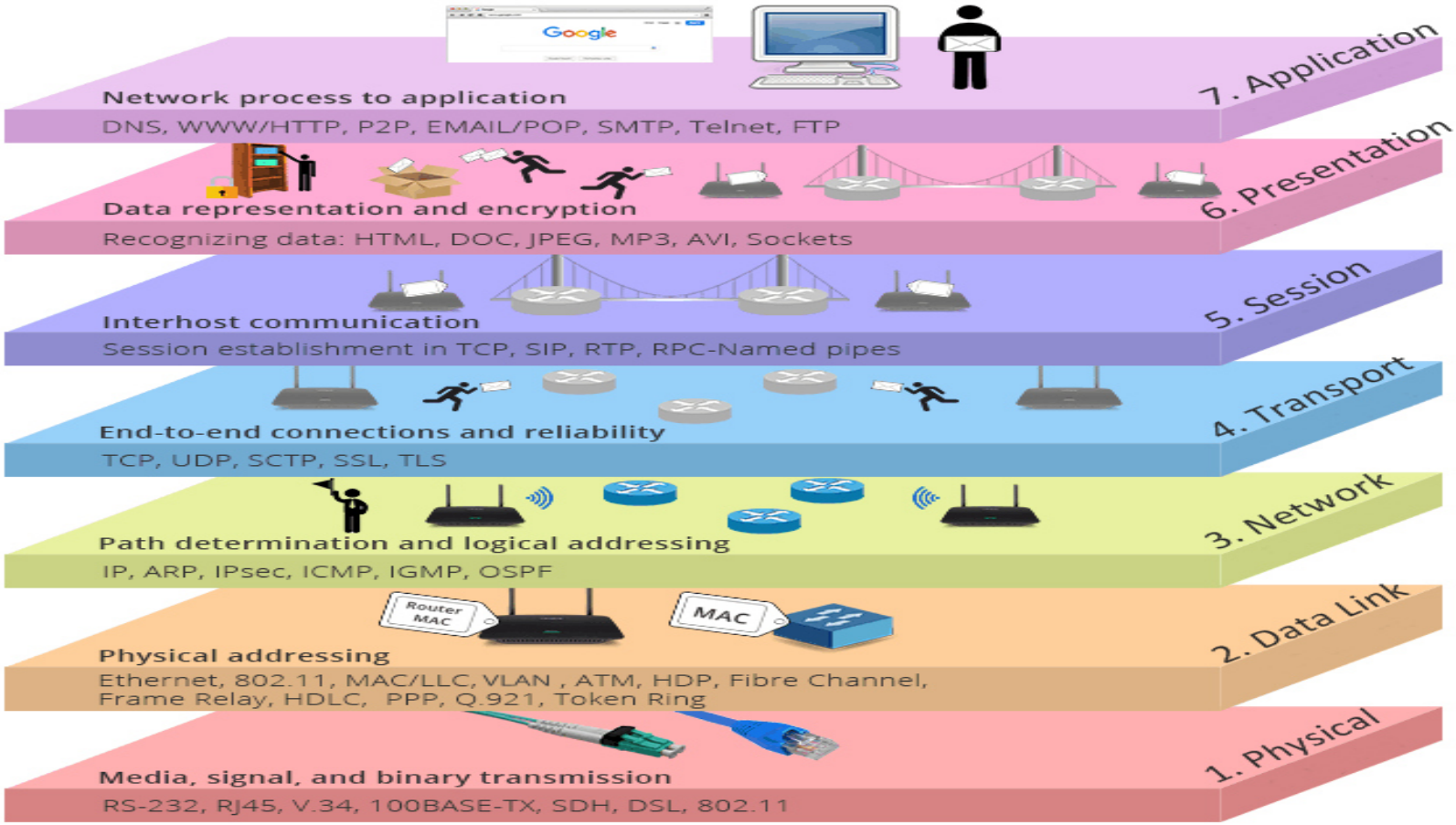


Basics of Networking / Layered Network Models

- The intercommunication between hosts in any computer network, be it a large-scale or a small-scale one is **built upon the premise** of various task-specific **layers**.
- Most **commonly** accepted and used **traditional** layered network models.
  - open systems interconnection (**OSI**) 7-layer model developed by the International Organization of Standardization (ISO).
  - Internet protocol suite (**TCP/IP**) 4-layer model.

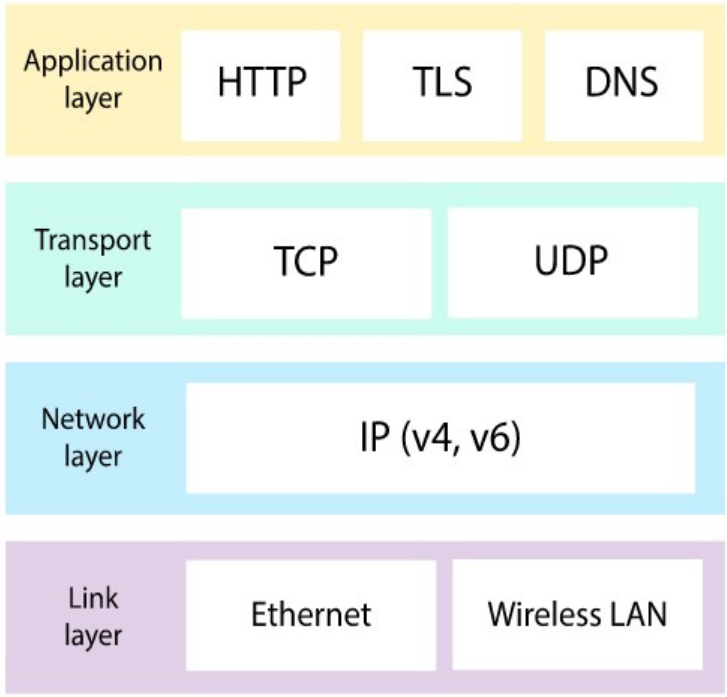
Basics of Networking / Layered Network Models

- open systems interconnection (**OSI**)



Basics of Networking / Layered Network Models

- Internet protocol suite, transmission control protocol (TCP) and Internet protocol (IP), (**TCP/IP**).



Basics of Networking / Layered Network Models

- **(ISO-OSI) reference model**:
  It is a conceptual framework that **divides any networked communication system into seven layers**, each **performing specific tasks toward communicating with other systems**

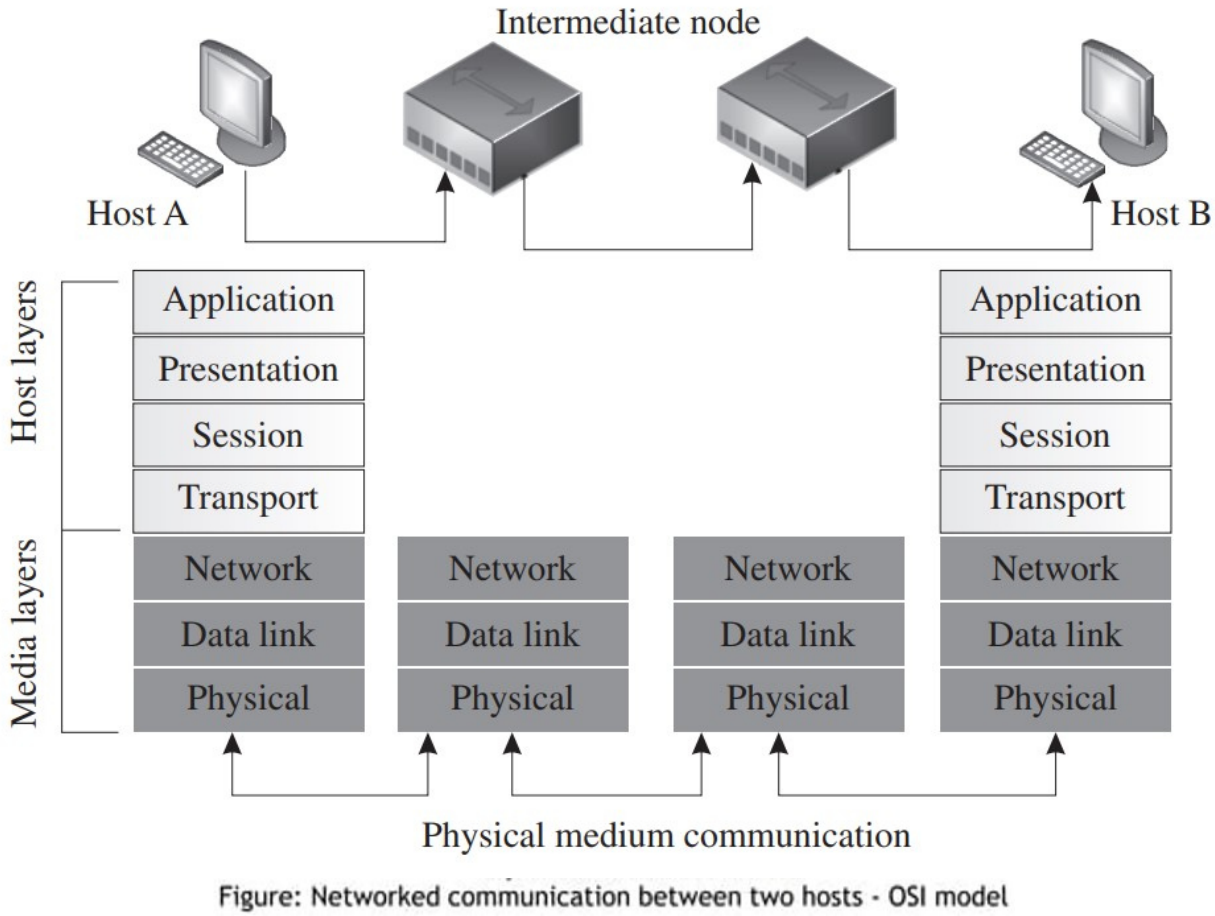
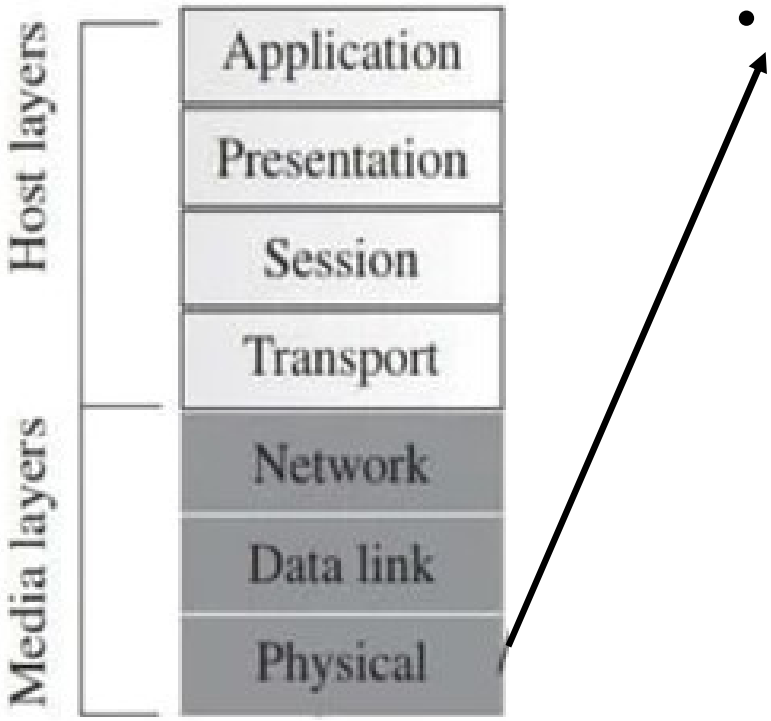


Figure: Networked communication between two hosts - OSI model

Basics of Networking / Layered Network Models

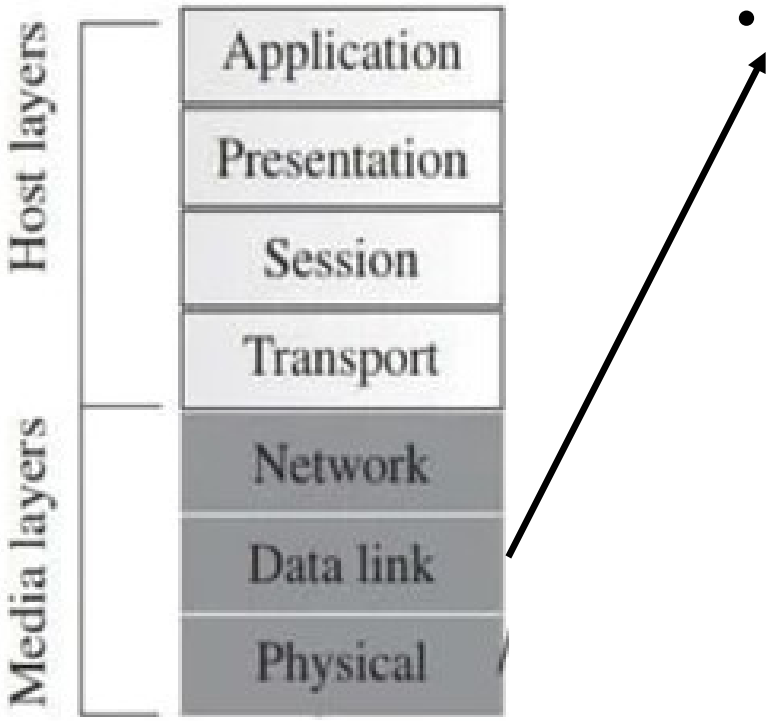
- **(ISO-OSI) reference model**:



- **Physical Layer:**
  - This is a **media layer** and is also referred to as **layer 1** of the OSI model.
  - responsible for taking care of the electrical and mechanical operations.
  - deal with issues relating to **signal generation**, **signal transfer**, **voltages**, the **layout of cables**, **physical port layout**, and **signal loss**.
  - **responsible** for the **topological layout** of the network (star, mesh, bus, or ring), **communication mode** (simplex, duplex, full duplex), and **bit** rate control operations.
  - The protocol **data unit associated** with this layer is referred to as a **symbol**.

Basics of Networking / Layered Network Models

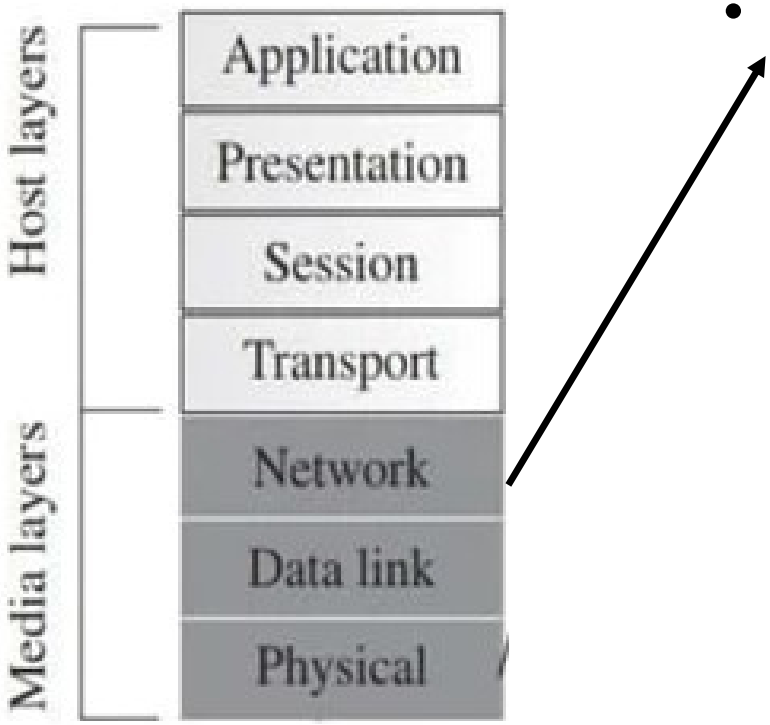
- **(ISO-OSI) reference model**:



- **Data Link Layer:**
  - This is a **media layer** and is also referred to as **layer 2** of the OSI model.
  - mainly concerned with the **establishment** and **termination** of the **connection** **between two hosts**.
  - **detection** and **correction** of **errors** during communication between two or more connected hosts.
  - IEEE 802 divides into two sub-layers: Medium access control (**MAC**) and logical link control (**LLC**).
  - **MAC** is responsible for access control and permissions.
  - **LLC** is mainly tasked with error checking, flow control, and frame synchronization.
  - protocol data unit - **frame**.

Basics of Networking / Layered Network Models

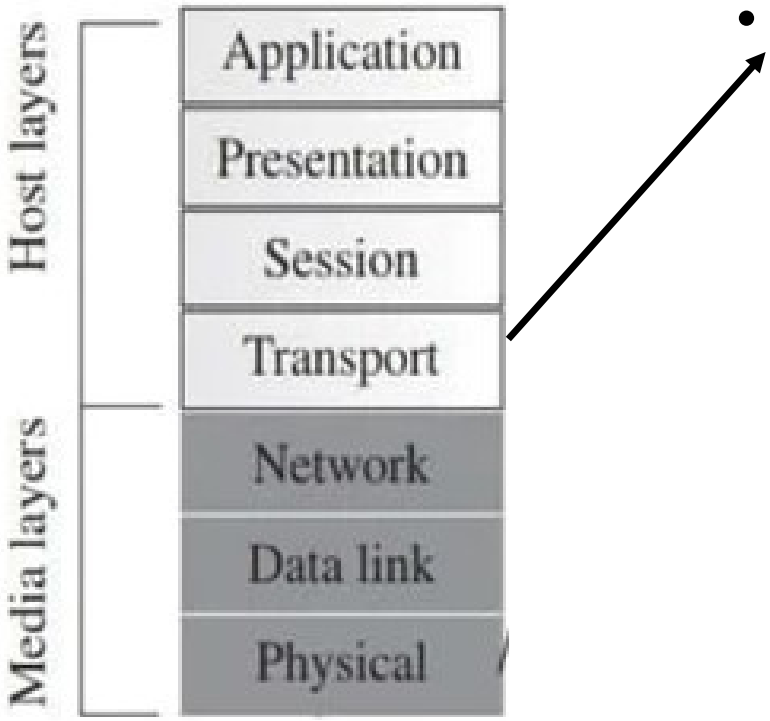
- **(ISO-OSI) reference model**:



- **Network Layer:**
  - This is a **media layer** and is also referred to as **layer 3** of the OSI model.
  - **routing data** to various hosts connected to different networks through **logical paths** called **virtual circuits**.
  - These logical paths may pass through **other intermediate hosts (nodes)** before reaching the actual destination host.
  - The primary tasks of this layer include **addressing**, **sequencing of packets**, congestion control, and error handling.
  - protocol data unit - **Packets**.

Basics of Networking / Layered Network Models

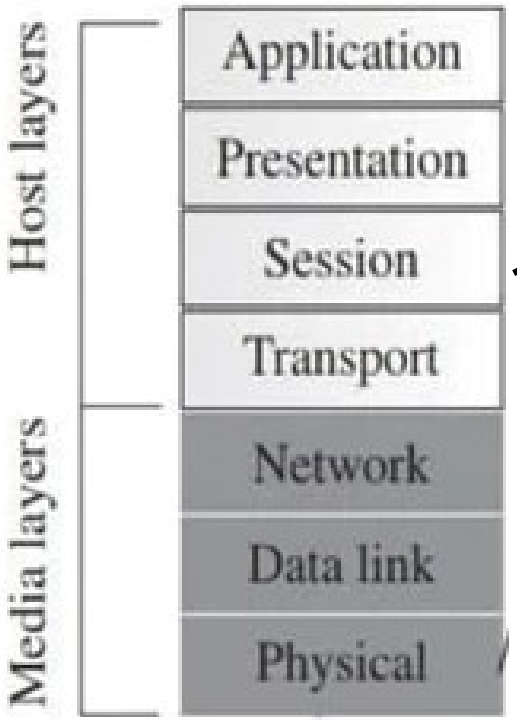
- **(ISO-OSI) reference model**:



- **Transport Layer:**
  - This is a **host layer** and is also referred to as **layer 4** of the OSI model.
  - The transport layer is tasked with **end-to-end error recovery and flow control**
  - **achieve transparent transfer** of data between hosts.
  - keeping track of **acknowledgments** during variable-length data transfer.
  - transport layer **ensures** that the particular **erroneous data segment is re-sent** to the receiving host.
  - protocol data unit – **Segment**.

Basics of Networking / Layered Network Models

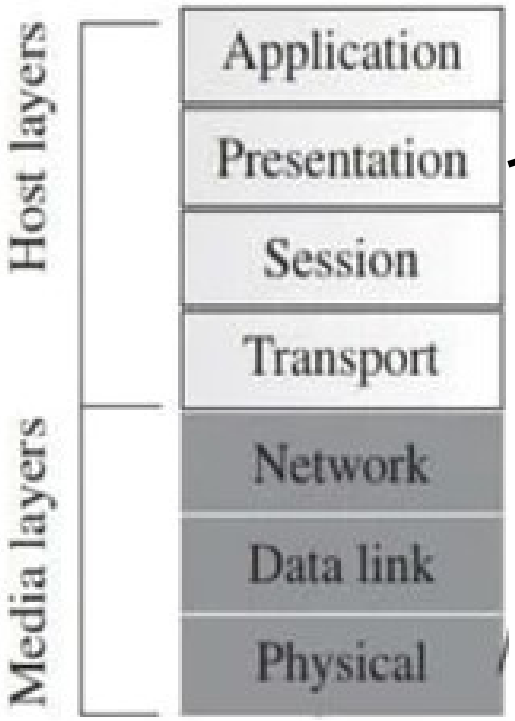
- **(ISO-OSI) reference model**:



- **Session Layer:**
  - **layer 5** of the OSI model & is a **host layer.**
  - **Responsible** for establishing, controlling, and terminating of **communication.**
  - The session layer sees **full utilization during operations** such as remote procedure calls and remote sessions**.**
  - protocol data unit –**Data**.

Basics of Networking / Layered Network Models

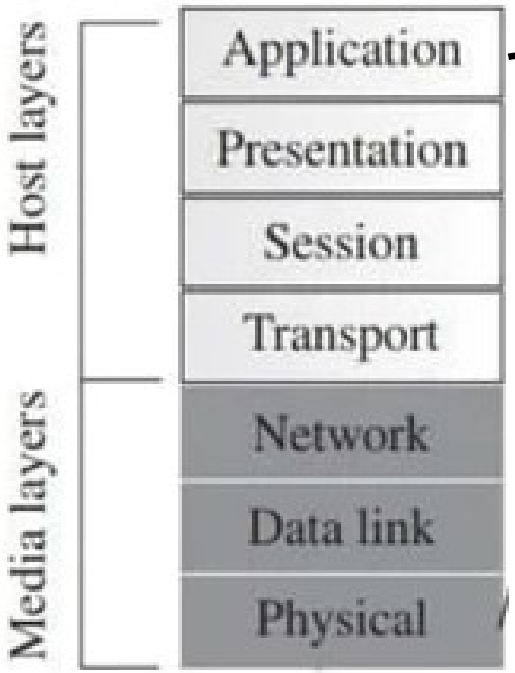
- **(ISO-OSI) reference model**:



- **Presentation Layer:**
  - **layer 6** of the OSI model & is a **host layer**.
  - Responsible for **data format conversions** and **encryption tasks**.
  - **syntactic compatibility** of the - also referred to as the **syntax layer**.
  - protocol data unit –**Data**.

Basics of Networking / Layered Network Models

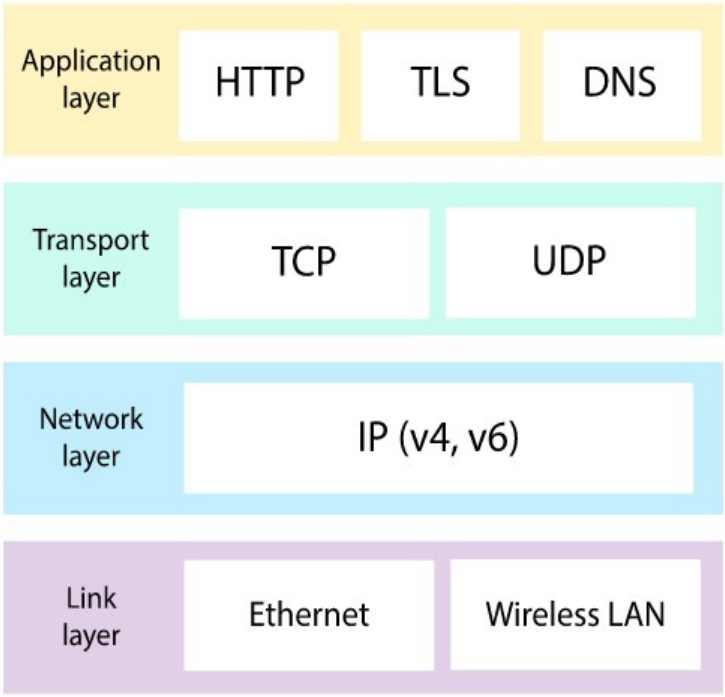
- **(ISO-OSI) reference model**:



- **Application Layer:**
  - **layer 7** of the OSI model & is a **host layer**.
  - It is directly accessible by an end-user through software APIs (application program interfaces) and terminals.
  - Applications such as **file transfers, FTP (file transfer protocol), e-mails,** and other such operations.
  - protocol data unit –**Data**.

Basics of Networking / Layered Network Models

- **Internet protocol suite (TCP/IP)**



1) Link layer.

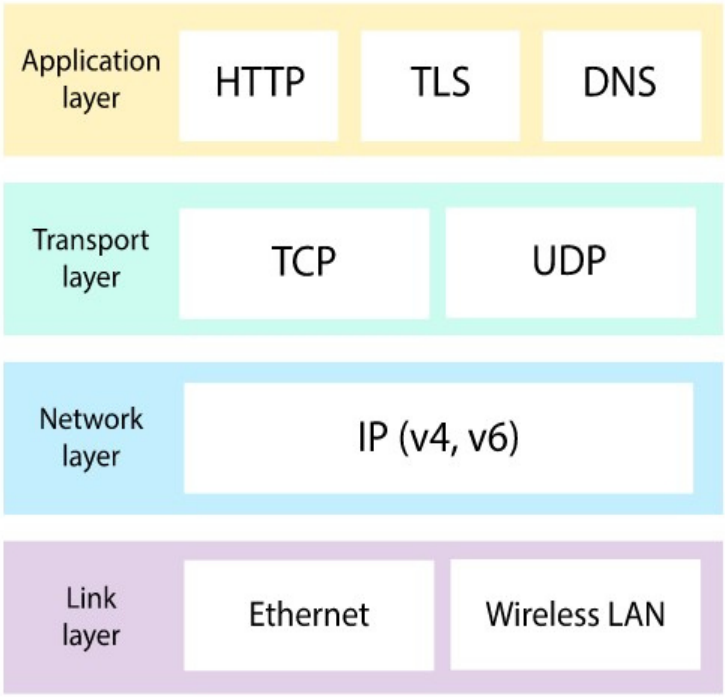
- The **first** and base **layer**.
- This layer is equivalent to the collective physical and data link layer of the OSI model.
- It enables the transmission of TCP/IP packets over the physical medium.
- Link layer is independent of the medium in use, frame format, and network access.
- Ethernet, wireless LAN, and the asynchronous transfer mode (ATM).

Basics of Networking / Layered Network Models

- **Internet protocol suite (TCP/IP)**

2) Internet layer:

- **Layer 2** of the TCP/IP protocol suite is somewhat equivalent to the network layer of the OSI model.
- It is responsible for addressing, address translation, data packaging, routing, and packet delivery tracking operations.
- Address resolution protocol (ARP), Internet protocol (IP), Internet control message protocol (ICMP), and Internet group management protocol (IGMP).

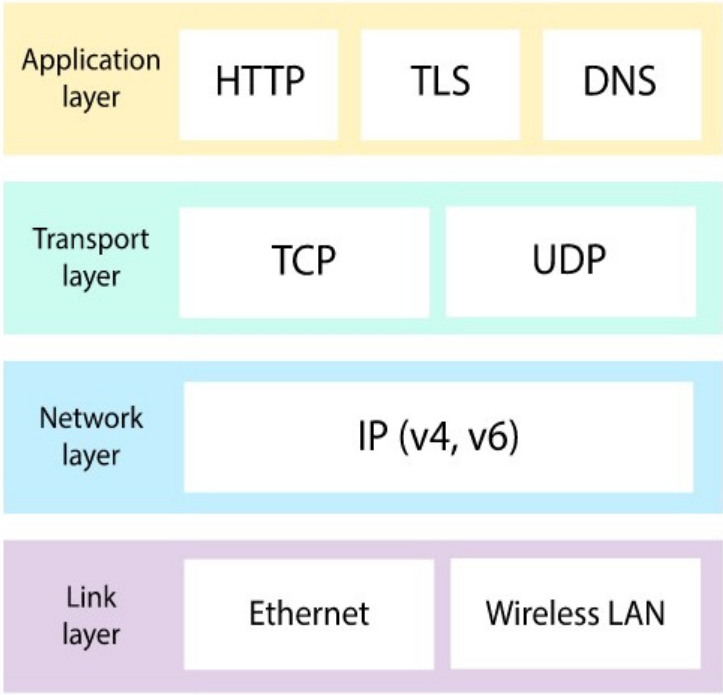


Basics of Networking / Layered Network Models

- **Internet protocol suite (TCP/IP)**

3) Transport layer:

- **Layer 3** of the TCP/IP protocol suite is functionally equivalent with the transport layer of the OSI model.
- **Tasked with** the functions of error control, flow control, congestion control, segmentation, and addressing in an **end-to-end manner**.
- Transmission control protocol (**TCP**) and user datagram protocol (**UDP**) are the core protocols.
- providing connection-oriented or connectionless services between two or more hosts or networked devices.

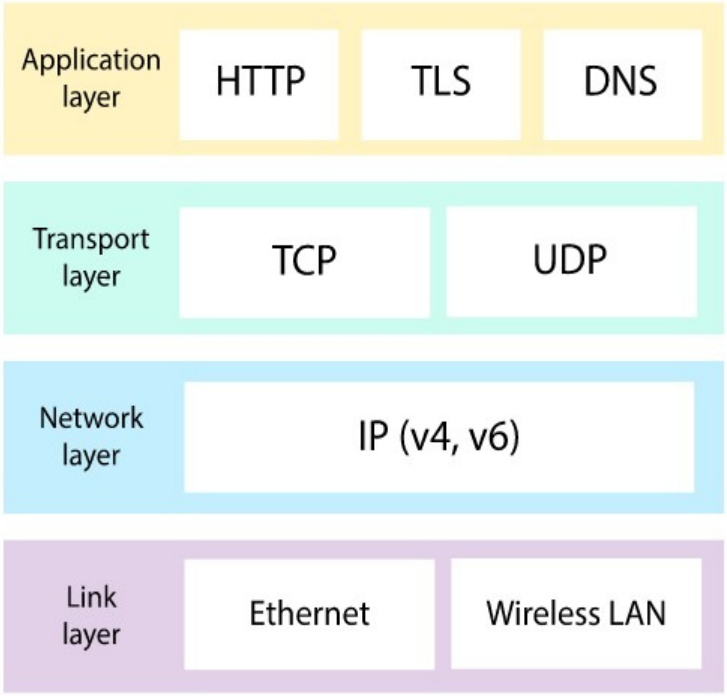


Basics of Networking / Layered Network Models

- **Internet protocol suite (TCP/IP)**

4) Application layer:

- **layer 4**, of the TCP/IP protocol suite equivalent with the collective functionalities of the OSI model's session, presentation, and application layers.
- This layer enables an end-user to access the services.
- Hypertext transfer protocol (HTTP), file transfer protocol (FTP), simple mail transfer protocol (SMTP), domain name system (DNS), routing information protocol (RIP)



Basics of Networking / Addressing

- Addressing in networked devices plays a critical role in ensuring the delivery of packets to the designated/intended receivers.
- Addressing mechanisms can be divided into two parts:

I. one focusing on **data link layer** address.

II. other focuses on **network layer** addressing.

Basics of Networking / Addressing

I. Data link layer addressing:

- These physical addresses are also known as media access control (MAC) addresses.
- MAC addresses are unique 48-bit hardware addresses provided by the device manufacturers.
- **the first 24** bits are organizational identifiers.
- **the last 24** bits are network interface controller identifiers.

- These addresses are unique globally. Data link layer addressing is broadly divided into **three types**:

1) **Unicast**: one-to-one communication.

2) **Multicast**: one-to-many communication within a single link.

3) **Broadcast:** one-to-all communication within a link.

Basics of Networking / Addressing

II. Network layer addressing:

- Network layer addressing is also termed as IP-based addressing or logical addressing.
- IPv4 addressing uses 32-bits long addresses, whereas IPv6 uses addresses that are 128 bits long.
- The mapping of a device/host's logical address to its hardware address is done through a mechanism called address resolution protocol (ARP).

Basics of Networking / Addressing

II. Network layer addressing: **IPv4**

VER: 4 bits long and represents the version of IP

HLEN: 4 bits long & length of the IPv4 packet header.

ToS: It is 8 bits long. The first six bits represent the differentiated services code point (DSCP) & last 2 bits give information about the congestion witnessed in the network.

TOTAL LENGTH: It is 16 bits long and identifies the length of the entire IPv4 packet.

IDENTIFIER: It is 16 bits long

FLAGS: It is a 3-bit field,fragmen

FRAGMENT OFFSET: identifies the exact offset or fragment position of the original IP packet and is 13 bits long.

TTL: It is 8 bits long

PROTOCOL: It is 8 bits long.

HEADER CHECKSUM: It is 16 bits long and used for identifying whether a packet is error-free or not.

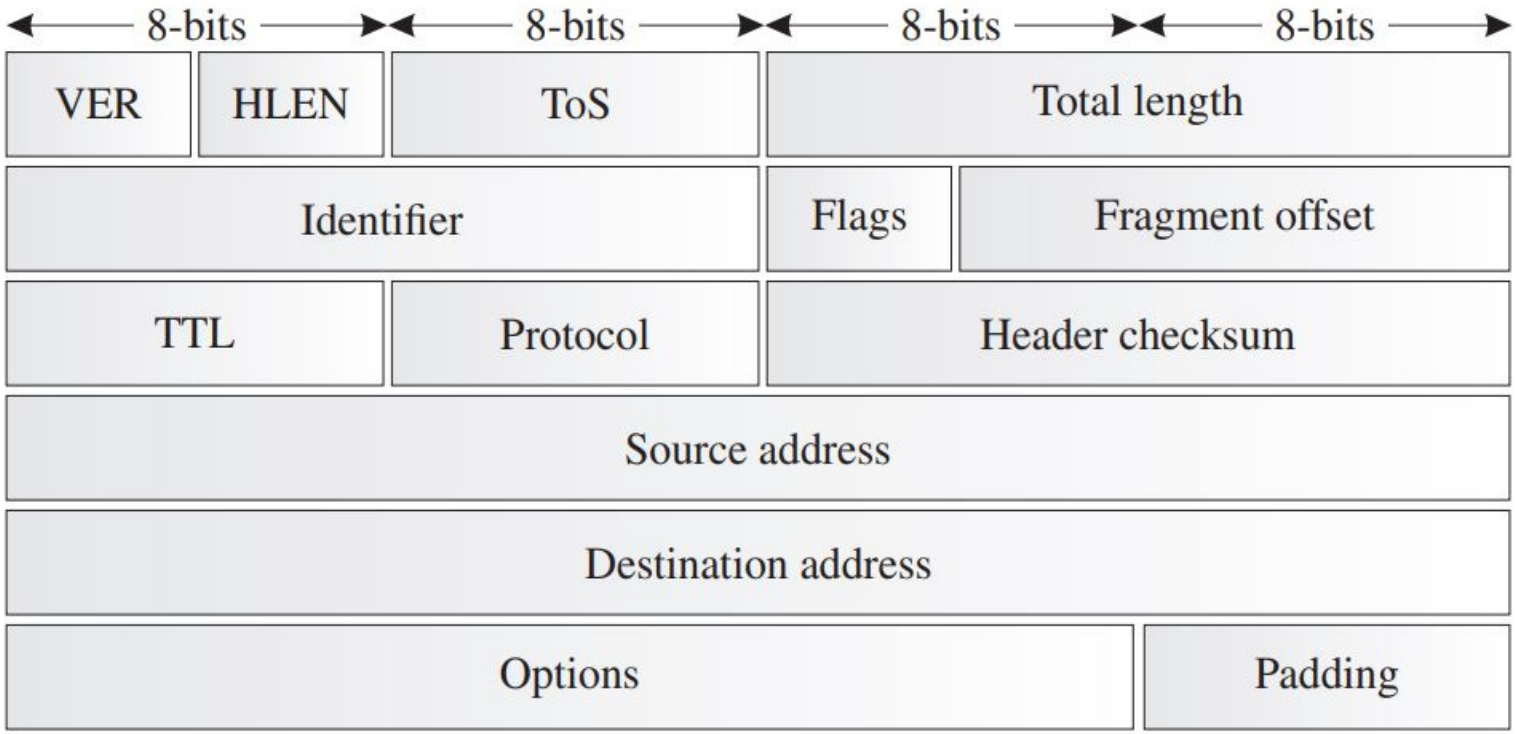
SOURCE ADDRESS: It indicates the origin address of the packet and is 32 bits long.

DESTINATION ADDRESS: It indicates the destination address of the packet and is 32 bits long.

OPTIONS and PADDING: It is an optional field, which may carry values for security, time stamps, route records, and others.

Basics of Networking / Addressing

II. Network layer addressing: IPv4



Basics of Networking / Addressing

II. Network layer addressing: **IPv6**

VER: It is 4 bits long and represents the version of IP.

TRAFFIC CLASS: It is 8 bits long. The first six most significant bits represent the type of service to be provided to this packet (by the routers); explicit congestion notification (ECN) is handled by the last 2 bits.

FLOW LABEL: It is 20 bits long and designed for streaming media or real-time data. The FLOW LABEL allows for information flow ordering; it also avoids packet resequencing.

PAYLOAD LENGTH: It is 16 bits long and provides a router with information about a packet's payload length or the amount of data contained in the packet's payload.

NEXT HEADER: It is 8 bits long and informs the router about the type of extension header the packet is carrying. Some of the extension headers and their corresponding values are as follows: Hop-by-hop options header (0), routing header (43), fragment header (44), destination options header (60), authentication header (51), and encapsulating security payload header (50). In case an extension header is absent, it represents the upper layer protocol data units (PDUs).

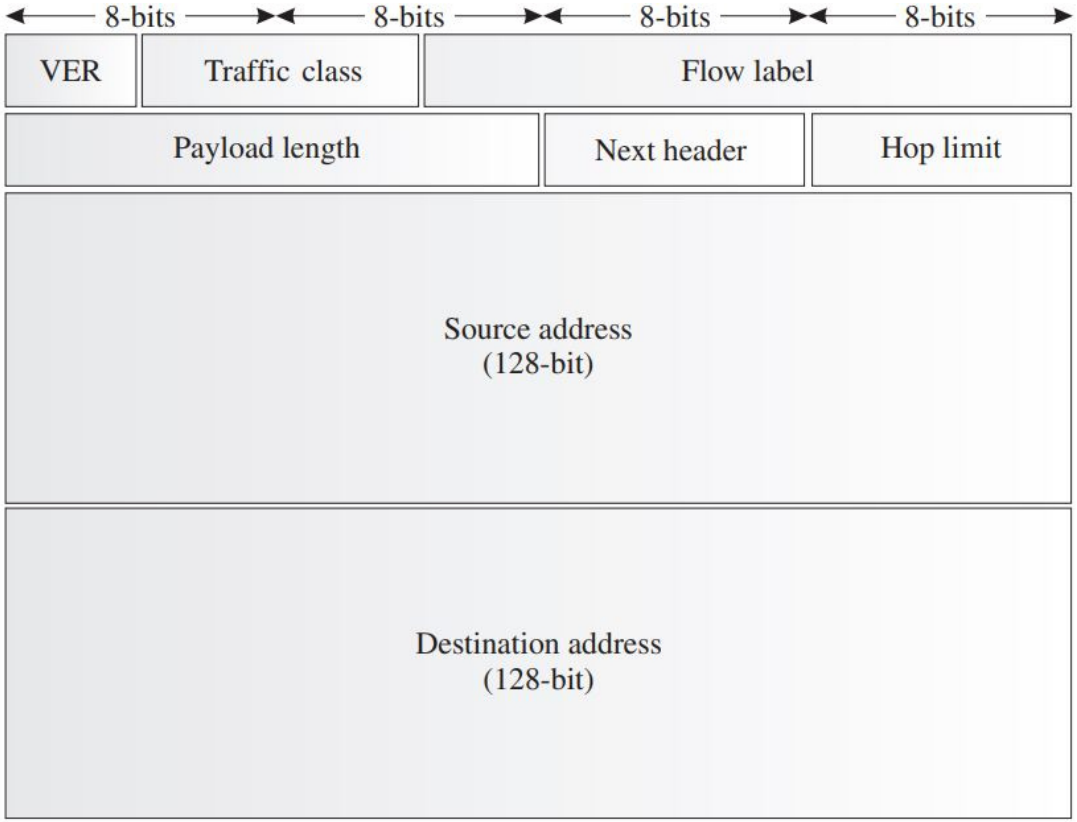
HOP LIMIT: It is 8 bits long and prevents a packet from looping infinitely in the network. As it completes a link, the limit's value is decremented by one.

SOURCE ADDRESS: It is 128 bits long and indicates the origin address of the packet.

DESTINATION ADDRESS: It is 128 bits long and indicates the destination address of the packet.

Basics of Networking / Addressing

II. Network layer addressing: IPv6



Basics of Networking / TCP/IP Transport layer

- As mentioned in the previous sections, the transport layer engages in networking functionalities such as process-to-process communication, encapsulation, and decapsulation of data, multiplexing and demultiplexing of virtual pathways, flow control, error control, and congestion control.

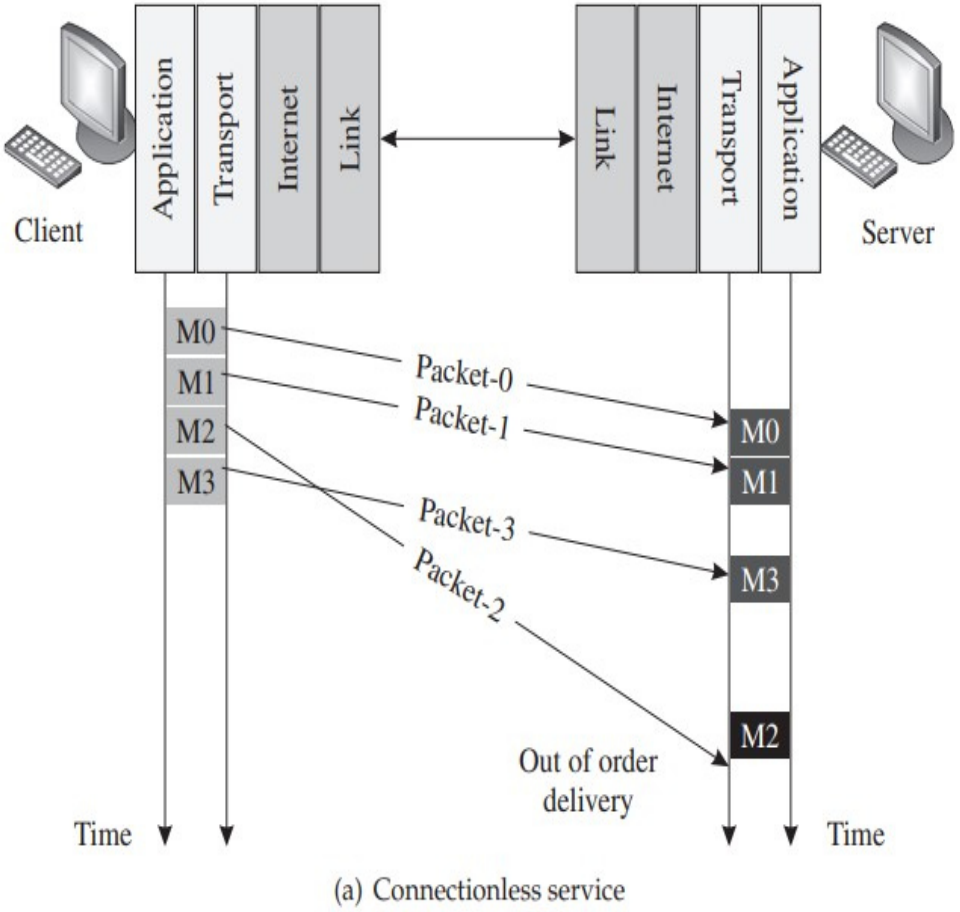
- From a broader perspective, the transport layer provides two types of services:

1) connectionless
2) connection-oriented.

Basics of Networking / TCP/IP Transport layer

1) Connectionless:

- the connectionless service at the transport layer treats each incoming chunk from the application layer as independent units. After these chunks have been packetized, the packets are transmitted over the network with basic information of the source and destination addresses and ports. Even if the packets at the receiving end arrive out of order, they are submitted to the receiving host's application layer as it is, without any sequence maintenance.

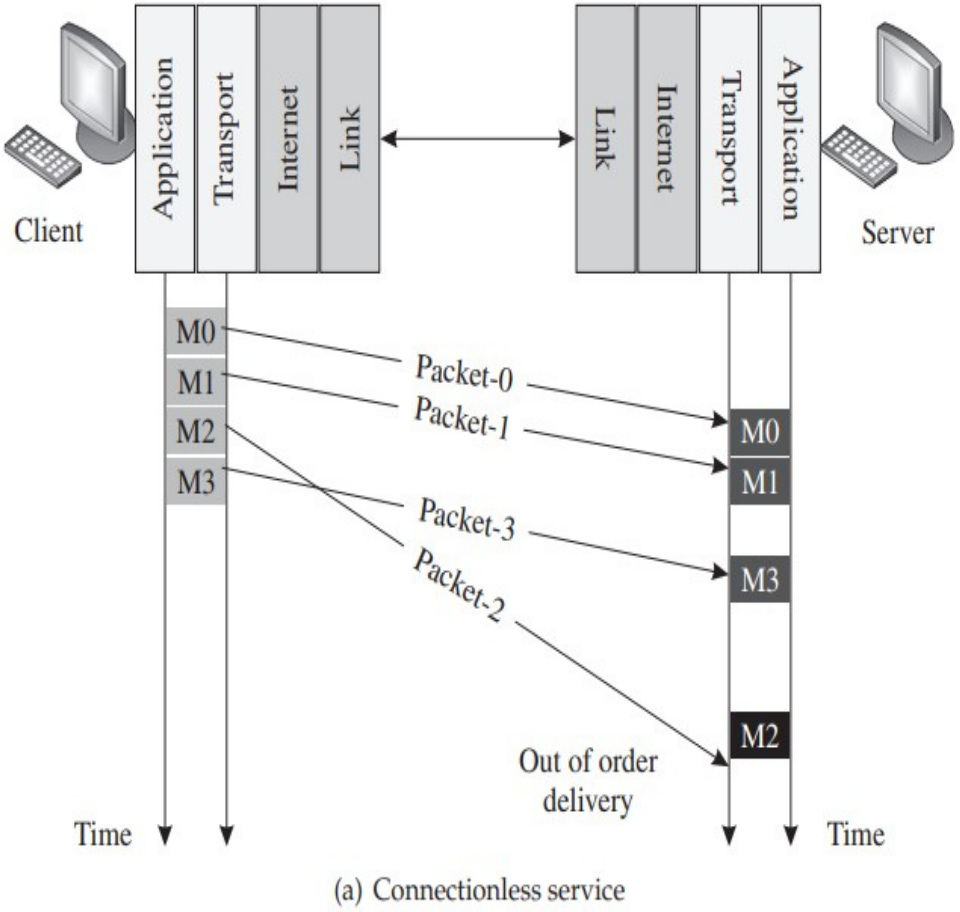


(a) Connectionless service

Basics of Networking / TCP/IP Transport layer

1) Connectionless:

- The client transport layer has four message chunks M0, M1,M2, and M3, which are transmitted in that sequence. However, M2 arrives at the server at a time much later than its subsequent packet M3. As this is a connectionless service, the sequence is not maintained, and the packets are forwarded to the server's application layer as it is (out of sequence). Voice-over-IP (VoIP) is a popular usage of this service type. The most famous protocol associated with this service type is the user datagram protocol (UDP).

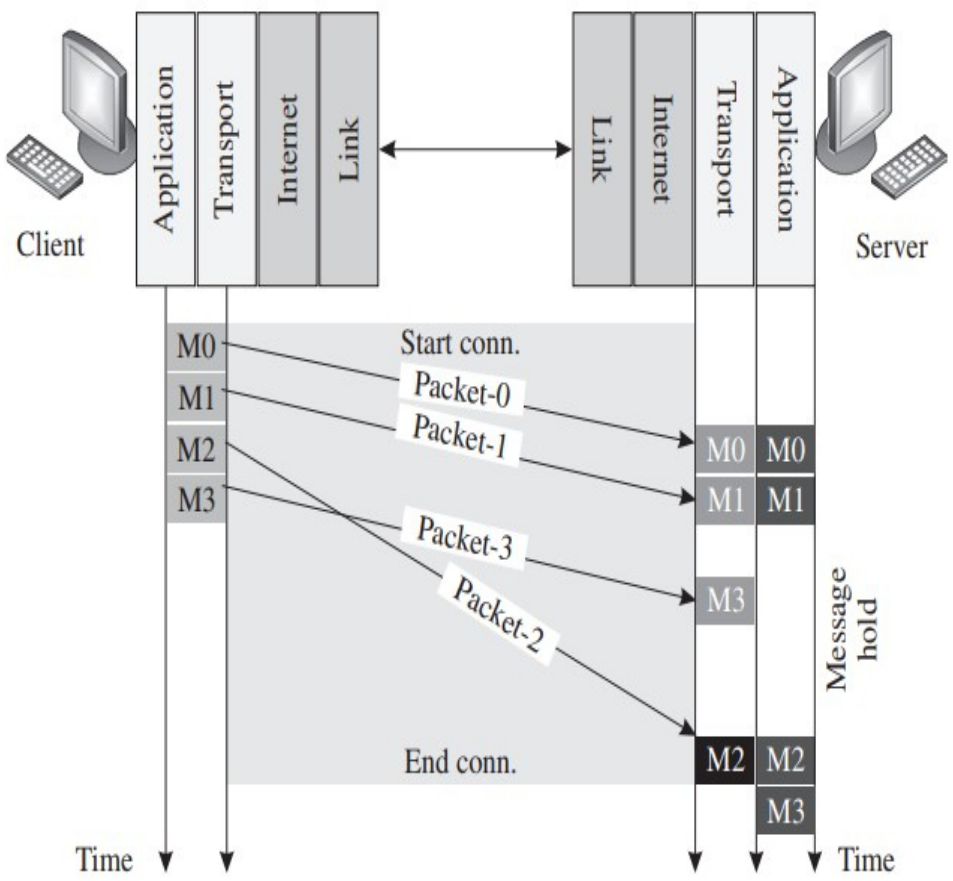


(a) Connectionless service

Basics of Networking / TCP/IP Transport layer

2) connection-oriented:

- The connection-oriented service, in contrast to the connectionless service, has a high dependency on the sequence of packets. Before the transmission of data to the server from the client. the client and server establish a connection employing handshaking using SYN and ACK frames. Once the data transmission is complete, the connection is terminated. In case another message has to be transmitted, the connection establishment process is again followed. This service type ensures that the packets arriving at the client's transport layer from its application layer are delivered in the exact sequence as in the server's application layer, in turn ensuring the quality of service (QoS) for the connection. However, ensuring QoS makes this type of service quite slow in comparison to connectionless services.

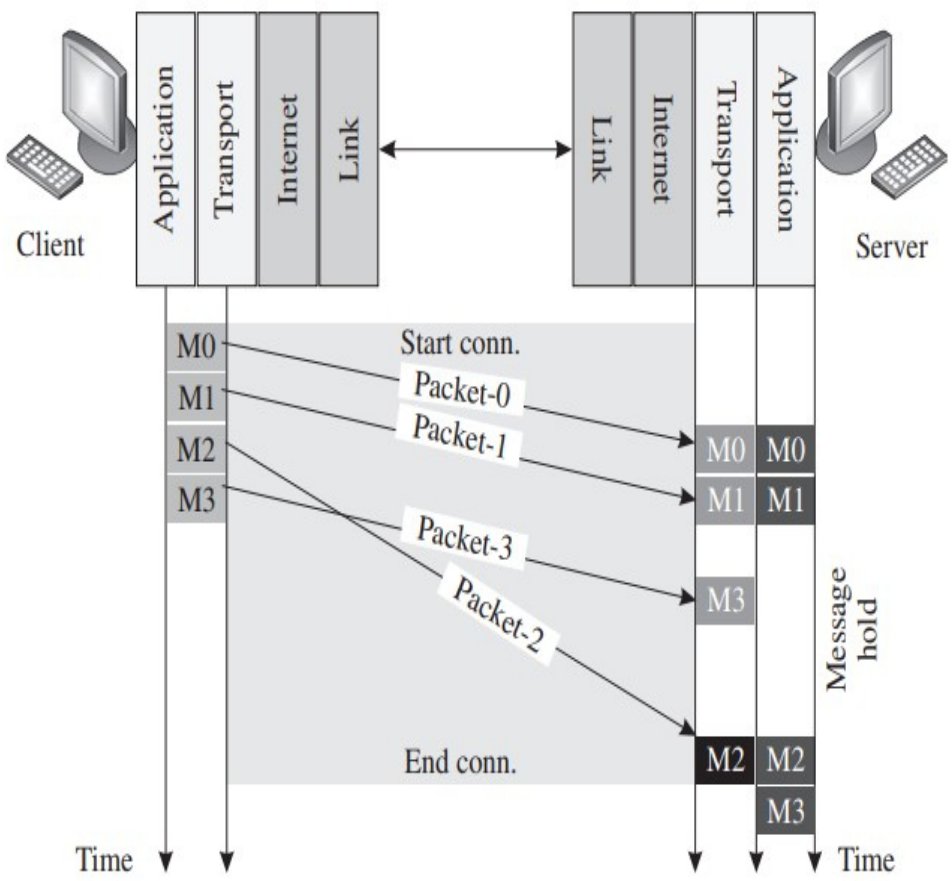


(b) Connection-oriented service

Basics of Networking / TCP/IP Transport layer

2) connection-oriented:

- the client transport layer has four message chunks M0, M1, M2, and M3 (from the client's application layer), which are packetized and transmitted in that sequence once a connection is established between the client and the server. Even if the M2 packet arrives out of sequence at the server's transport layer, the subsequent packets are held back until M2 is received. Upon receiving M2, M2, and the held-back M3 packet are forwarded to the server's application layer in the same sequence that it was transmitted from the client's transport layer. Application layer protocols such as HTTP (hypertext transfer protocol) and HTTPS (hypertext transfer protocol secure) rely on connection-oriented services for their operation. The popular transport layer protocol, transmission control protocol (TCP), is a means of achieving connection-oriented service.



(b) Connection-oriented service

Basics of Networking / TCP/IP Transport layer

Feature	UDP	TCP
Name	User datagram protocol	Transmission control protocol
Type of service	Connectionless	Connection-oriented
Reliability	Low	High
Time-criticality	High	Low
Packet sequencing	No sequencing required	High level of sequencing involved
Speed of transfer	High	Relatively low
Error checking	Present, but it simply discards errorenous packets	Present; Errorenous packets are re-transmitted from the source
Error recovery	Absent	Present
Acknowledgment	Absent	Present; Done by means of ACK frames
Handshake	None	Done by SYN, SYN-ACK, ACK frames
Weight	Lightweight protocol	Heavyweight protocol
Usage	SNMP, TFTP, RIP, VoIP, DNS, DHCP	HTTP, HTTPs, FTP, SMTP, Telnet

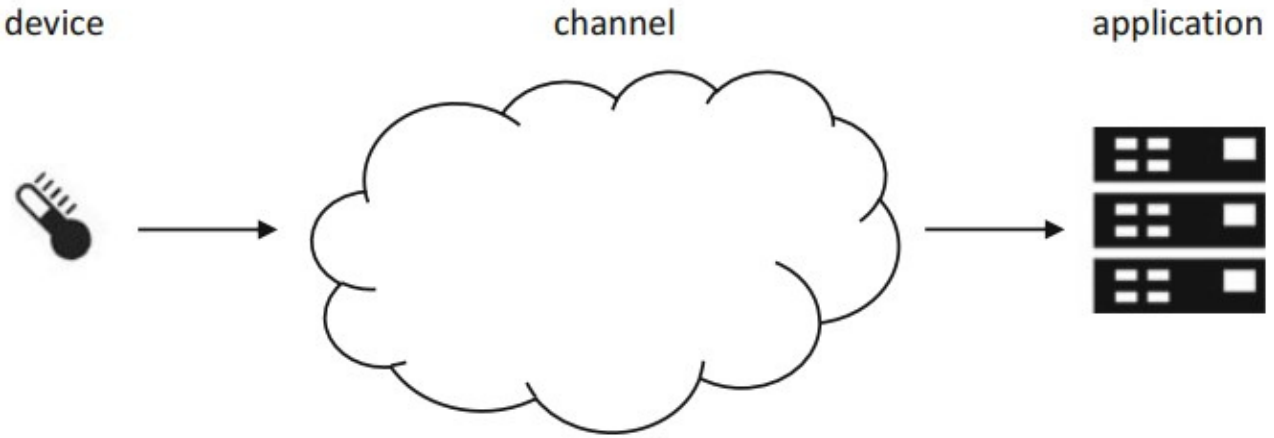
The system components & building blocks of IoT

- **The internet of things** provides fascinating **solutions** to most **problems** that the **workforce** is facing.
- The approach of attaining a solution is based on **how** the *information technology components* were **integrated** with *communication devices* with the **best** *hardware* and *software* **convergence**.
- **Managing** millions of **heterogeneous** connected **devices** via the Internet requires a **flexible**, layered **architecture**.
- Basically, there is not such a **unique or universally** define standard concurrence of **IoT Architecture** Building Blocks.
- **IoT Architecture** Building Blocks **differ on** the basis of their **functionality** and **depending** upon their **solutions**.

The building blocks of IoT

The basic IoT block:

- Two additional and very important components are needed for IoT communication to work, a **device** and an **application**.
- IoT scenario typically involves three main fundamental components: **(1)** devices, **(2)** a communication channel, and **(3)** an application performing analytics.



The building blocks of IoT

- **Devices** are **sensors**, **controllers**, and **actuators** typically running on small constrained **embedded systems/computers** based on system-on-chip (**SoC**) and system-on-module (**SoM**) hardware.

- A **SoC** is a **chip** that provides a central processing unit (**CPU**), **memory**, **storage**, **input/output** digital and analog **interfaces**, and radio-frequency (**RF**) signal processing.

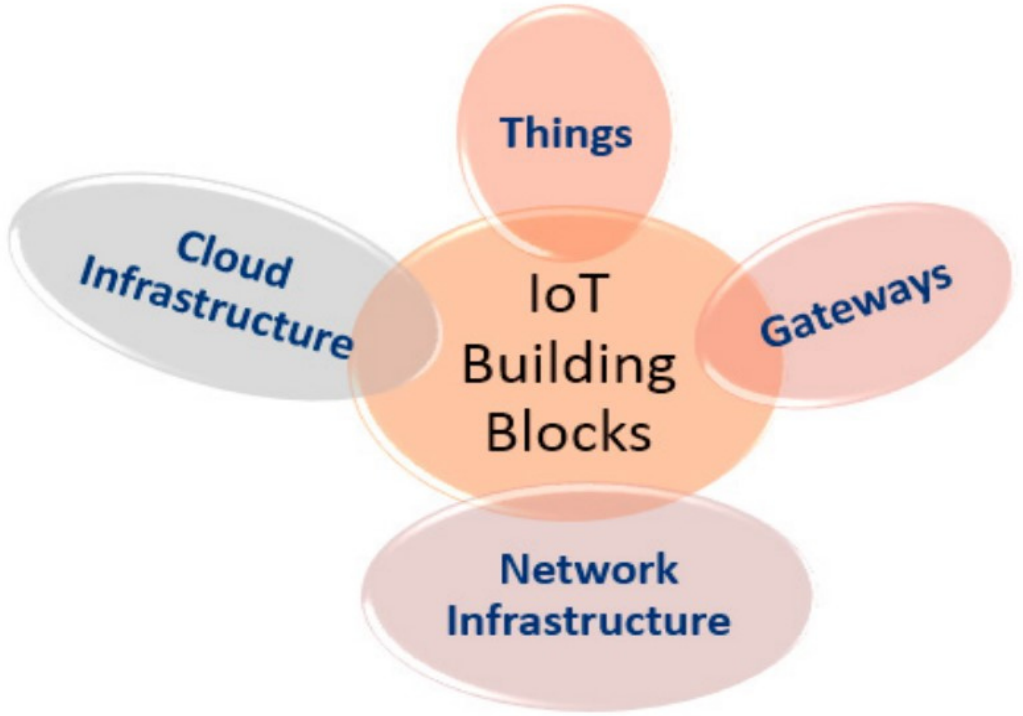
- **SoM** is a circuit board that includes an **SoC** in addition to some other **separate chips** that provide additional functionality.

The building blocks of IoT

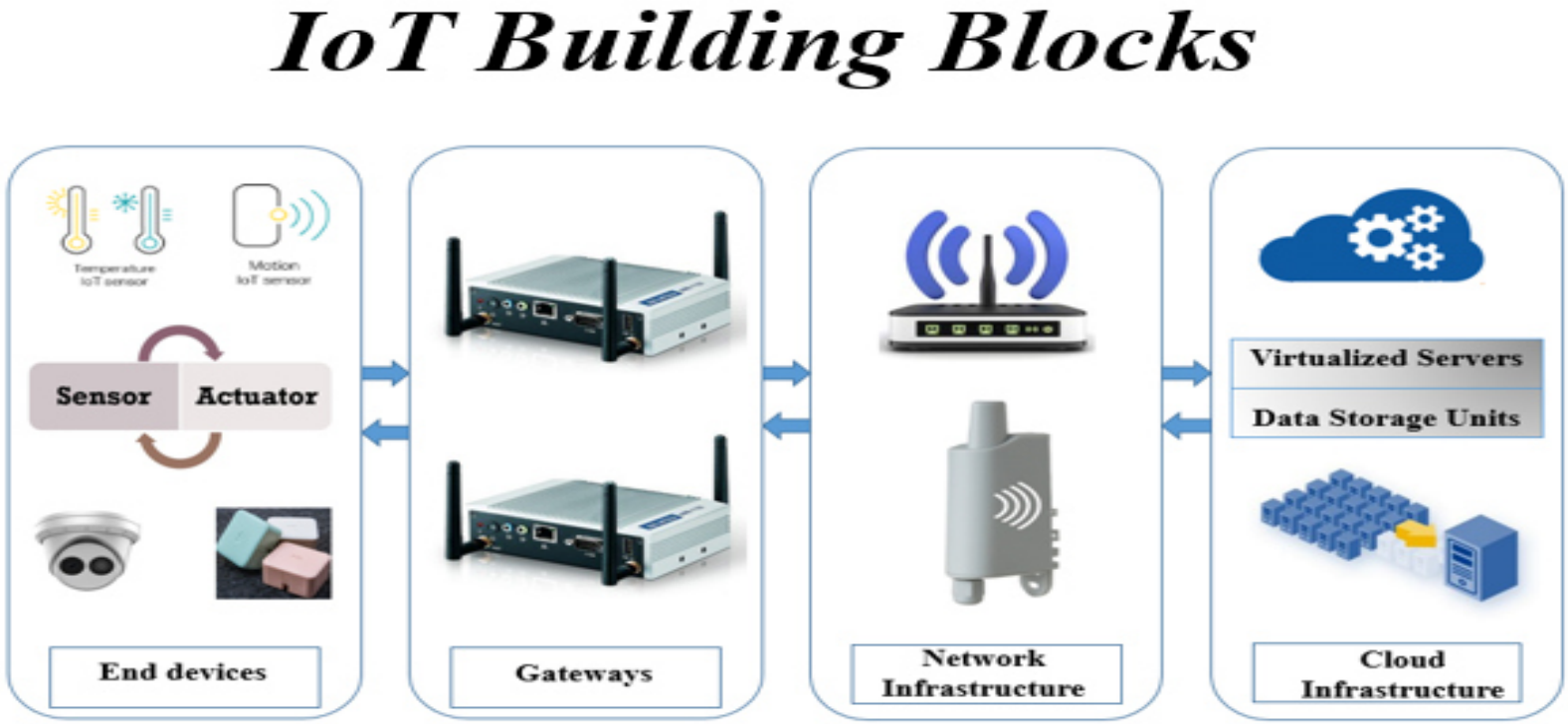
- **communication channel** is the medium that enables the **transmission of signals between devices and applications**.
- **Applications** typically perform **operational analytics** to **extract knowledge** from the **data generated** by **devices**. This knowledge is used, to make **automated actuation decisions** and to provide visualization for human interaction.

The building blocks of IoT

The four main building blocks:



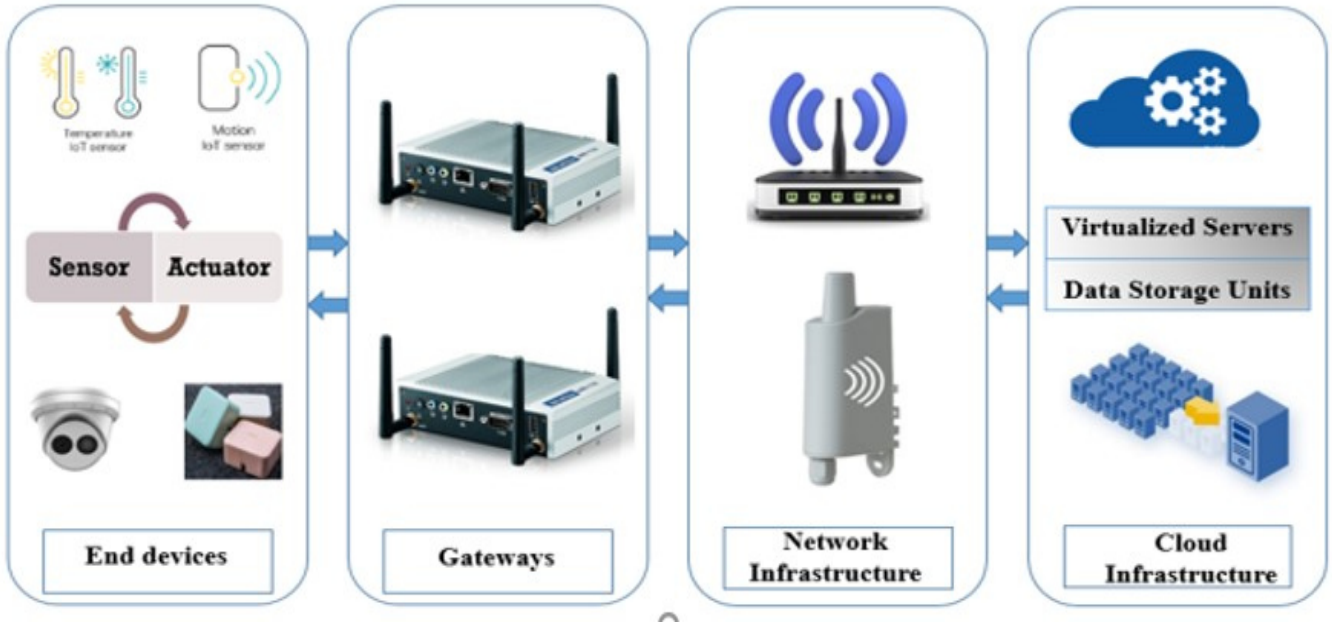
The building blocks of IoT



The building blocks of IoT

- **Things** \ Sensors & Processors

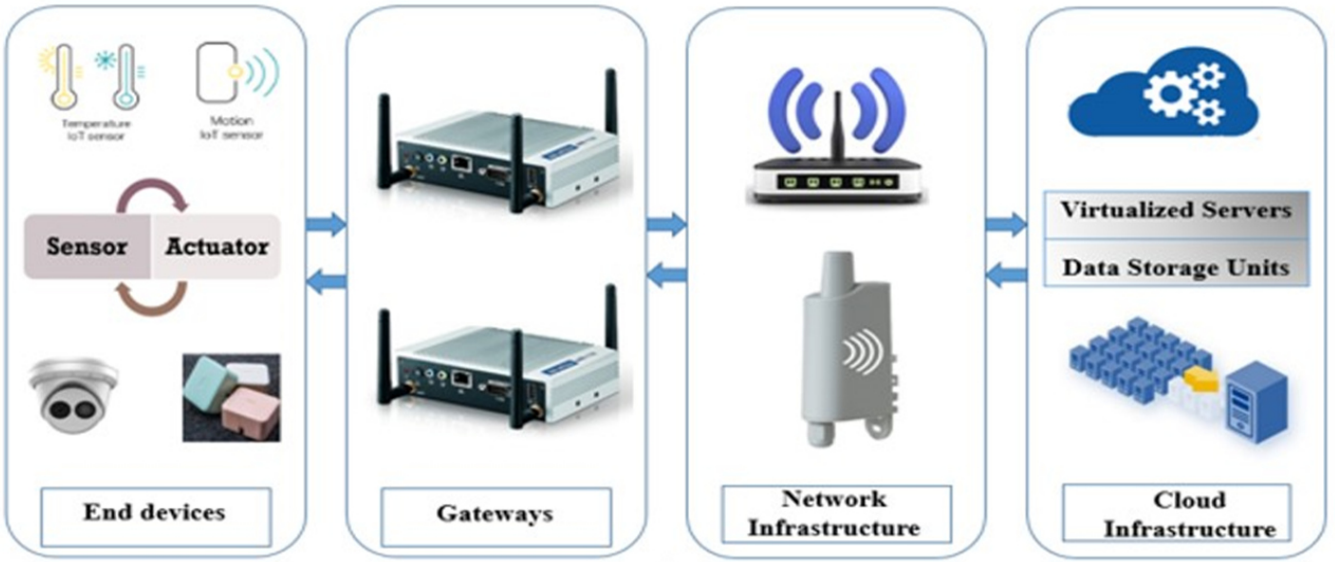
the ‘Things’ are the **sensors** and **actuators**. its **front end** of the IoT architecture building block, **Sensors** take data from the environment and **actuators** give data to the surroundings, without any human interaction, using different connectivity methods.



The building blocks of IoT

❑ Gateways

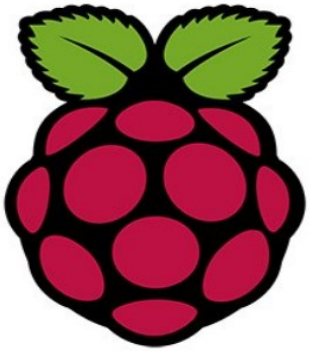
- An IoT gateway is a device (combination of hardware and software) that's **used** for the basic **analysis of data coming from connected sensors**.
- Gateways are responsible for **bridging sensor nodes with the external Internet or World Wide Web**.



The building blocks of IoT

❑ **Gateways**

- In **some cases**, when data analysis requires a **small** number of computing resources, IoT gateways **can serve as decision points, sending certain control commands to actuators** that perform appropriate actions.
- If **more complex** data processing is needed or information is to be stored for further analysis, gateways **send it** to a server located either **on-premises** or in the **cloud**.
- Both **microcomputers** and **microprocessors** can be used as gateways for IoT applications, with the most widely used being open-source platforms such as Raspberry Pi and Arduino.
- LAN, WAN, PAN, etc are also can be an example of network gateways.



The building blocks of IoT

❑ Network infrastructure

- This is comprised of **routers**, **aggregators**, **gateways**, **repeaters**, and other devices that **control** and **secure** data flow.
- It allows the **control** over the **data flow** from **things** to the **cloud** infrastructure.

❑ Cloud infrastructure \ Applications

- **Cloud infrastructure** contains large pools of **virtualized servers** and **storage** that are networked together with **computing** and **analytical** capabilities.
- **Applications** are another **end** of an IoT system. Applications do proper **utilization** of all the data collected and provide an **interface** to users to interact with that data.

Acknowledgment

- **These lecture slides are based on:**

1) **Chapter 1(P 3-10)** from the book "Internet of Things A to Z Technologies and Applications" by Qusay F. Hassan (Editor) (z-lib.org)
2) **Chapter 1(P 23)** Internet of Things A Hands-On Approach by Arshdeep Bahga, Vijay Madisetti (z-lib.org)
3) **Part I (section 1.3 p7-9)** from the book Fundamentals of IoT Communication Technologies
4) **Article** (Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into **the building blocks**, component interactions, and architecture layers. Procedia computer science, 132, 109-117).
5) **Chapter 1(P 3-19)** from the book "Introduction to IoT" by (Sudip Misra, Anandarup Mukherjee, Arijit Roy)

INTERNET OF THINGS (IoT)

END OF LECTURE (1)

Keep connected with the classroom

btukscx

THANK YOU FOR YOUR ATTENTION