BUSINESS DATA COMMUNICATION & NETWORKING

DATA COMMUNICATION

- Data: Raw and unorganized facts
- Data does not depend on information.
- Data doesn't depend on information

Eg: information collected for writing research paper.

- Information: Information are process, organized data presented iin meaning context.
- Group of data makes information.
- Information depends on data.
- Eg: The final research paper about the particular topic.

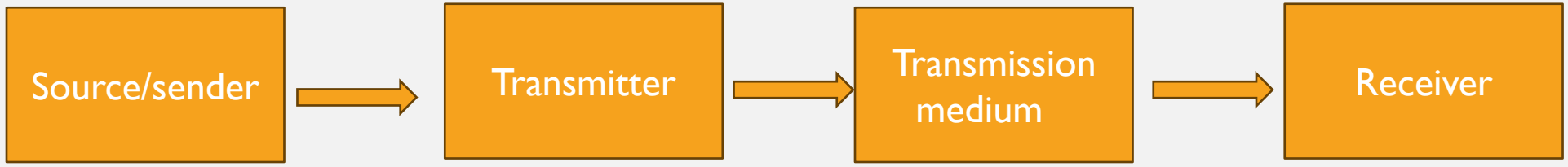
WHAT IS DATA COMMUNICATION?

- Process of using computing and communication technology to transfer data.

Importance of data communication?

- Accuracy
- Delivery
- Improve communication
- Decision making
- Operation efficiency

DATA COMMUNICATION MODEL



- Example: Email:
- Computer → NIC card → ethernet cable → Computer (NIC card)

- Example: Bluetooth – adapter – radio signal- Bluetooth

COMPONENT OF DATA COMMUNICATION

- There are 5 Component:

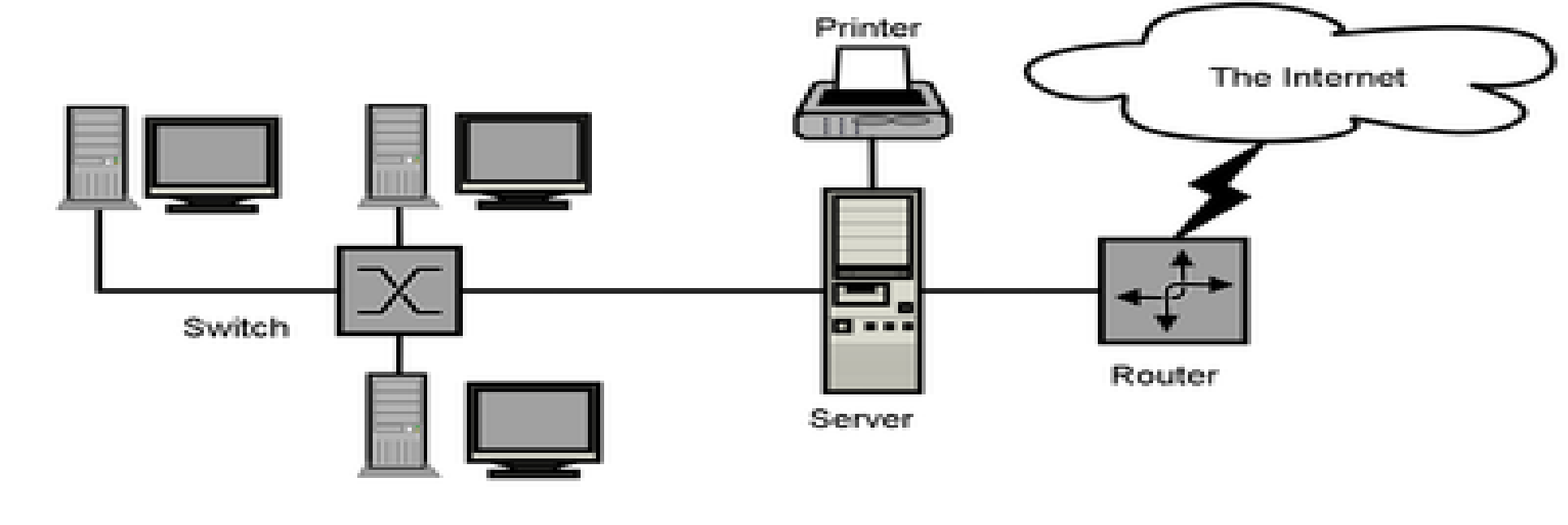
1. Message: It is information to be communicated. Text, photo, audio, video
2. Sender: It is device which will send message, PC, mobile, telephone
3. Receiver: It is device which receives the message, Computer, Phone, any devices
4. Transmission medium: Physical Path through which message travels from sender to receiver. eg cable, radio wave, fiber, etc.
5. Protocol: Set of rules that governs the data communication, with protocol two devices cannot communicate. IP, Transmission control protocol(TCP)

COMPUTER NETWORK

- Computer networking refers to the practice of interconnecting multiple computing devices, such as computer, server, router, firewall etc.
- This can be done using wired or wireless connection and designed to facilitate communication.
- Key aspect : hardware, software, protocols
- Definition: group of computer that are linked together to share information.

- Example: Router, Switches, Firewalls, PC,

DIAGRAM OF COMPUTER NETWORK



DESCRIPTION OF NETWORK COMPONENT

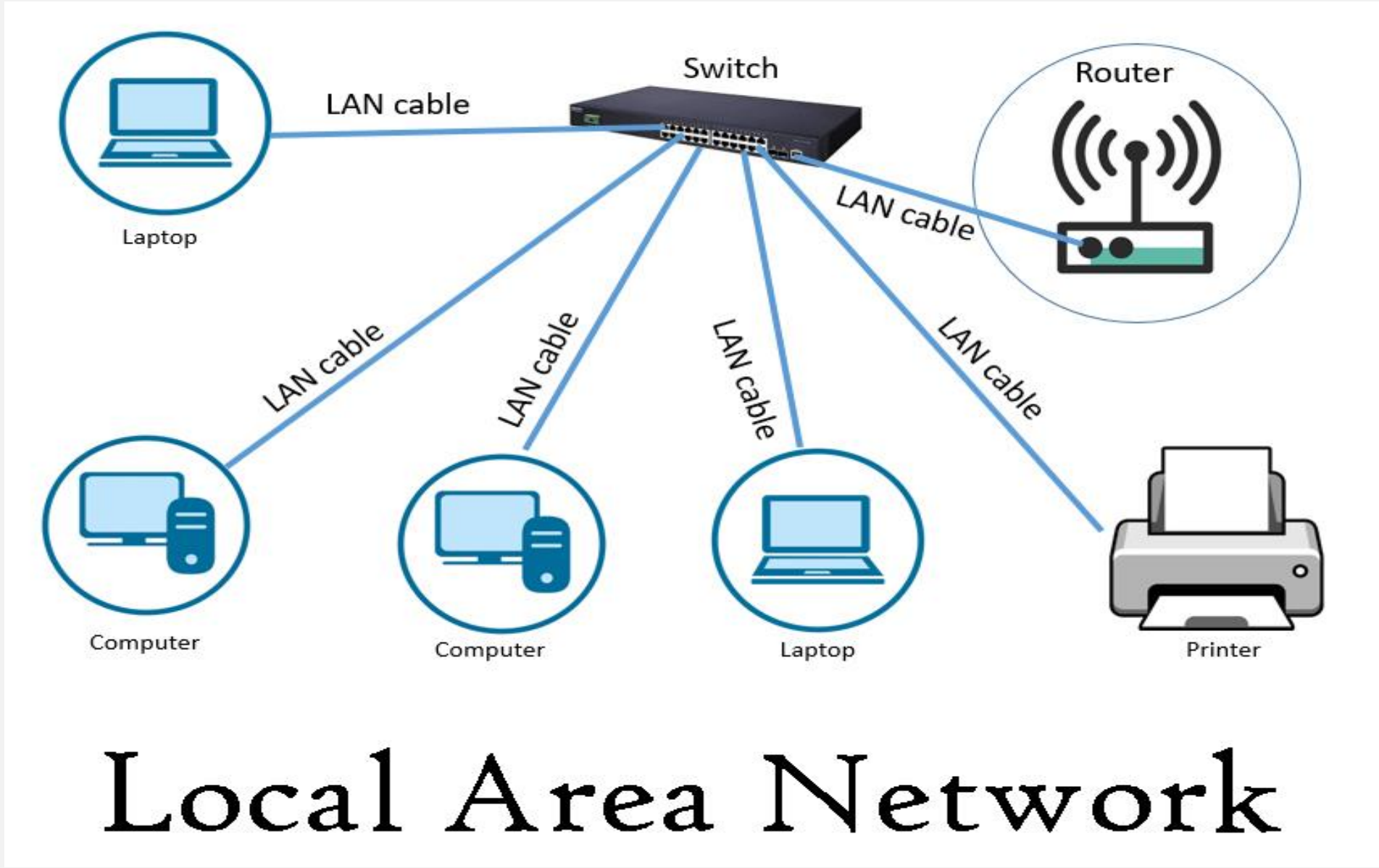
- End Point: Desktop or Laptop
- Server: Host, where application is hosted
- Switches: Hardware devices that switches packets from source to destination
- Firewall: Hardware device that prevents unauthorized access to network
- Hub: Hardware device that broadcast network and connect all endpoint to same network
- Bridge: Hardware device used to connect multiple network in one network.

TYPES OF NETWORK

- Types of network depends on the number of computer and geographic region as well. Network can be of any size. There are several types of network.
- **PAN:** Personal Area Network: smallest and most basic type of network. It is made of small number of devices, computer printer, tablets etc
- Designed for a single user or small group
- Can be wired or wireless.
- **Advantages**
- NO wired required: Pan can be wireless, radio waves
- Reliable and secure: Reliable and stable because it is within 10 meter
- Portability: being wireless it is very portable. Can create own enviroment

LOCAL AREA NETWORK

- LAN covers small geographic area such as single building
- It enable sharing of resources such as file that may be needed by multiple user.
- Speed: 1 Gbps to 10 Gbps
- Primarily use ethernet for connectivity
- Hardware such as switch are used
- It can be wired or wireless


Switch
Router
LAN cable
Laptop
LAN cable
LAN cable
LAN cable
LAN cable
LAN cable
Computer
Computer
Laptop
Printer
Local Area Network

- **Advantage of LAN**
- The basic LAN implementation does not cost too much.
- It is easy to control and manage the entire LAN as it is available in one small region.
- The LAN configuration is very easy due to availability
- With the help of file servers connected on the LAN, sharing of files and folders among peers will become very easy and efficient.
- It is easy to setup security protocols to protect the LAN users from intruders or hackers.

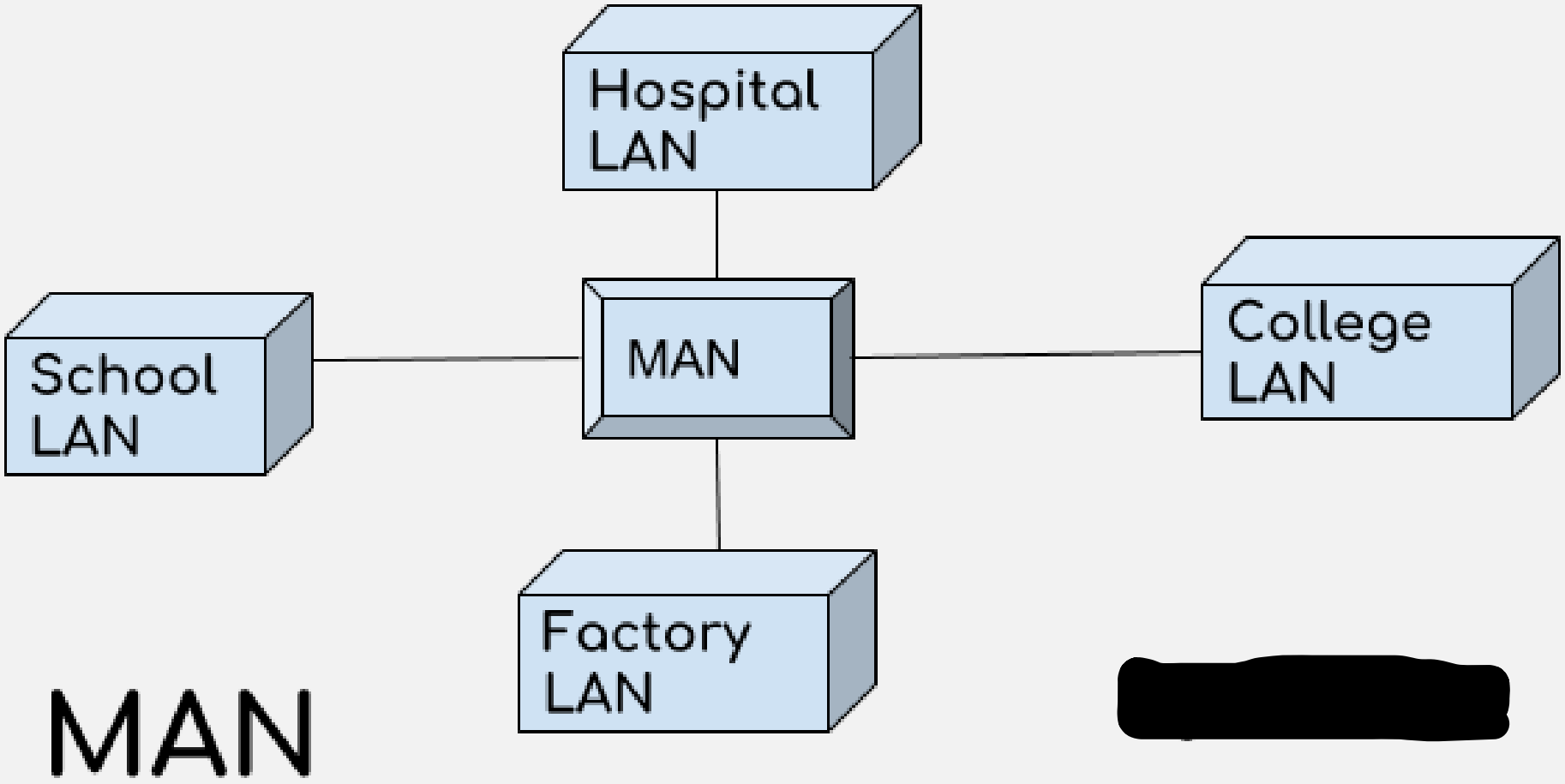
- **Disadvantage**
- LAN covers small geographical area
- It is difficult to setup and maintain LAN and requires skilled technicians and network administrators.
- Appearance of virus in one system can spread very fast to all the LAN users very easily.

CAMPUS AREA NETWORK

- Spans multiple buildings within a limited geographic area, such as a university campus or corporate campus.
- The networking equipment's (switches, routers) and transmission media (optical fiber, Twisted pair cabling etc.) are almost entirely owned by the campus , an enterprise, university, government etc
- Larger than a LAN but smaller than a MAN

METROPOLITAN AREA NETWORK

- A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.
- Examples of MAN: Telephone company network that provides ahigh speed DSL to customers and cable TV network.
- A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).



MAN

[redacted]

ADVANTAGE & DISADVANTAGES

1. **Advantages**

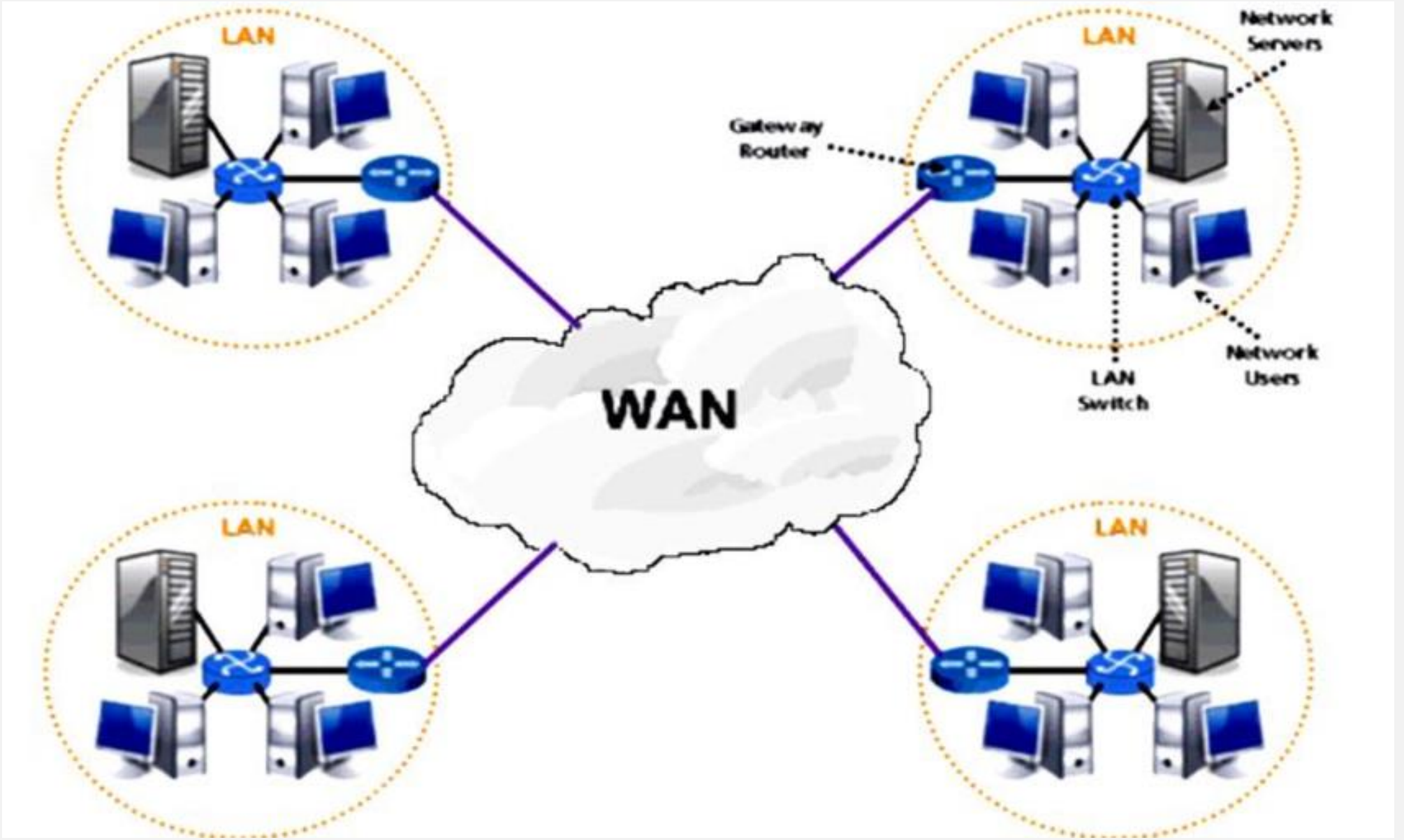
- Metropolitan Area Network allows people to connect LANs.
- Metropolitan Area Network usually encompasses several city blocks or an entire city.
- It improves data handling efficiency while increasing data transfer speed.
- It facilitates the cost-effective sharing of shared resources such as printers.
- The implementation cost of a Metropolitan Area Network are lower than WAN since it requires fewer resources.
- Centralize network management makes it easier to monitor, maintain and troubleshoot

2. Disadvantages

- Compared to LAN, more cable is required to set up a Metropolitan Area Network.
- Because this network comprises multiple LANs, it is difficult to keep hackers out.
- These networks must be implemented by skilled technicians and network administrators.
- This network's implementation and management costs are higher than those of a local area network.
- It is challenging to manage this network because it's an extensive network of numerous local area networks.

WIDE AREA NETWORK

- WAN covers a large geographic area such as country continent or even whole world.
- WANs are used to connect multiple smaller network, LAN & MAN enabling communication and data exchanges.
- To cover great distance, high speed fiber cable or wireless links such as satellites are used
- Organization can form their global integrated network through WAN to share resources and files.


LAN
LAN
Network
Servers
Gateway
Router
WAN
LAN
Switch
Network
Users
LAN
LAN

ADVANTAGE & DISADVANTAGES

- Advantages
- WAN covers larger geographical area. Hence business offices situated at longer distances can easily communicate.
- Like LAN, it allows sharing of resources and application software's among distributed workstations or users.
- The software files are shared among all the users. Hence all will have access to latest files. This avoids use of previous versions by them.

- **Disadvantages**
- Initial investment costs are higher.
- It is difficult to maintain the network. It requires skilled technicians and network administrators.
- There are more errors and issues due to wide coverage and use of different technologies. Often it requires more time to resolve issues due to involvement of multiple wired and wireless technologies.
- It has lower security compare to LAN and MAN due to wider coverage and use of more technologies

STORAGE AREA NETWORK(SAN)

- Storage area network (SAN) is network of storage devices that can be accessed by multiple server or computer
- High Speed network: uses fiber channel or iSCSI (internet small computer system interface) protocol
- Centralized storage management
- Scalability : easy to scale by adding more storage device
- High availability (HA)

- **Enterprise private network (EPN)**
- These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

- **Virtual Private Network (VPN)**
- A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

NETWORK MODEL

- A network model is a blueprint that outlines how different systems (computers, servers, devices) communicate and interact with each other over a network.
- Network models are also known as network stacks or protocol suites because they stack various protocols that work together to handle different aspects of network communication.

- Example of network model:
- **TCP/IP:** The fundamental protocol suite for the internet and most modern networks.
- **NetBIOS (Network Basic Input/Output System):** Provides the foundation for network communication in Microsoft networking environments.
- **AppleTalk:** The network protocol suite used for networking Apple Macintosh computers.

- **Layered Architecture**
- Network models are often composed of multiple layers, each with a specific role or function in the communication process. This is known as a hierarchical or layered architecture.
- Each layer is designed to handle a specific part of the communication process, from the physical transmission of data to the application-level interactions.

- **Protocol within layers**
- Each layer of the model typically has one or more **protocols** associated with it. A protocol is a set of rules or a language that defines how data is transmitted and received.

OPEN SYSTEM INTERCONNECTION (OSI) MODEL

- The OSI model was theorized in 1984 by the International Organization for Standardization (ISO) as a reference framework for understanding how data is transmitted between computers over a network.
- The OSI model is now considered the primary Architectural model for inter-computer communications.
- The OSI model describes how information or data makes its way from application programs (such as spreadsheets) through a network medium (such as wire) to another application program located on another network
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems

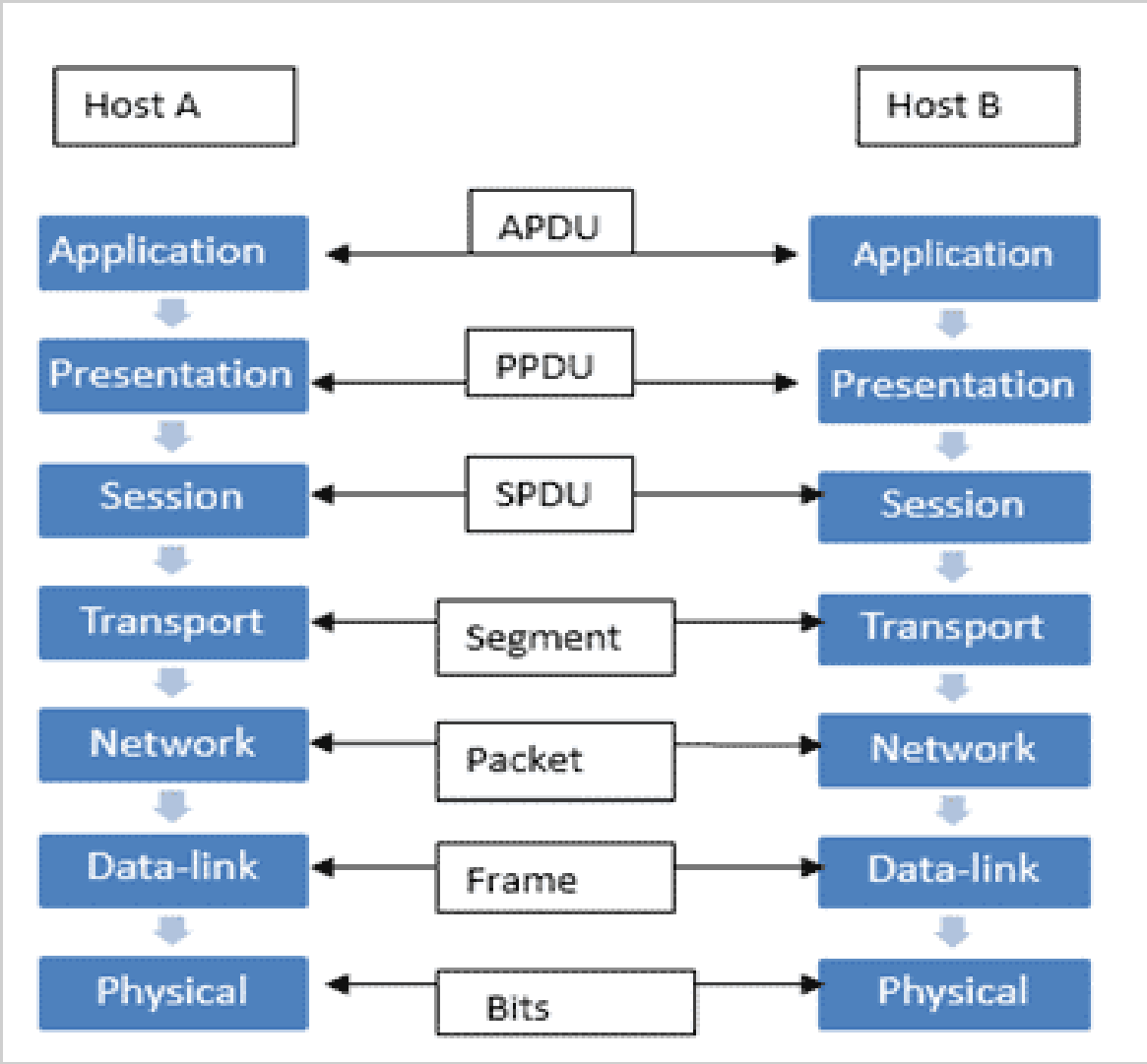
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Software Side

Heart of OSI because it is bridge between Software and hardware

Hardware Side

- **How to Remember?**
- **Please do not throw salami pizza away - Receiver**
- **All people seem to need data processing - Sender**



Host A to host B communication

- The data originates from Application layer and passes through each layer
- At each layer, data is encapsulated with appropriate PDU (Protocol data unit)
- The encapsulated data is transmitted across network to host B
- The data arrives at host b, where it is decapsulated layer by layer from physical to application layer
- Finally host B receivers the original data sent from host A

APPLICATION LAYER(LAYER 7)

- The application layer is the topmost layer of OSI model, responsible for providing service to end user application. This layer interacts directly with software application to provide communication service.
- It is closest to end user which means that both application layer and user interact direct with software.
- It is not application it self, but component within application that controls communication.
- The protocol that run at applicating layer includes, FTP, HTTP, SMTP, Telnet, SSH

MAJOR RESPONSIBILITIES OF LAYER 7

- **Mail service:**
- This application provides the basis of email forwarding and storing.
- **File Transfer/ Access and Management:**
- This application allows a user to access files in a remote hosts, to retrieve files from remote computer for use in the local computer and to manage or control files in remote computer locally.
- **Web Browsing**
- User access website through browser using HPPT/ HTTPS
- **Remote login**
- Users log into remote systems using Telnet or SSH.

PRESENTATION LAYER(LAYER 6)

- The presentation layer is the sixth layer in OSI model.
- It acts as the translator between the network and application layer, ensuring data is in usable format and is properly encoded for network translation.
- Converts application specific data into common format suitable for network transmission.
- Ensure data is transformed into mutually understandable format for both sender and receiver.

RESPONSIBILITIES OF LAYER 6

- **Translation:**
- The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer responsible for interoperability between these different encoding methods.
- **Encryption:**
- To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression:**
- Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.
- **Example** of protocol that run at the presentation layer include SSL (Secure Sockets Layer). The
- Secure Socket Layer is a protocol that provides security to confidential data following the encryption process over the internet.

SESSION LAYER(LAYER 5)

- Session layer fifth is OSI layer
- It is responsible for establishing, maintaining and synchronizing and termination sessions between end user application.
- This layer plays a critical roles in coordinating communication between system, ensuring that data exchanges occur in controlled and organized manner

RESPONSIBILITIES OF SESSION LAYER

- Initiates and establishes sessions between applications on different devices.
- Manages the data exchange during the session, ensuring data is properly synchronized and organized.
- Implements mechanisms for checkpointing and recovery in long-duration transfers**. Example**: if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.
- Sets up parameters for communication such as authentication and session identification.

TRANSPORT LAYER (LAYER 4)

- The main purpose of this layer is making sure that data is delivered error free and in the correct sequence.
- Breaking down data into smaller segments and reassembling them at the receiving end.
- Segments: a segment is unit of data used by transport layer. It contain payload and control information such as port number and sequence number

RESPONSIBILITIES

Segmentation and reassembling

- A message is divided into segment and each segment contains a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination. The packets lost in the transmission is identified and resent.

Control flow

- Control amount of data flow between communication

Error Control

Uses mechanisms like checksums to detect errors in transmitted segments.

NETWORK LAYER

- It is 3rd layer of OSI layer
- It is responsible for source to destination delivery of a packet across multiple network.
- It ensures that each packet gets from its point of origin to its final destination. It treats each packet independent as though each belong to separate message.
- It defines logical network layout so router can determine how to forward packets through an entire network.
- Examples of protocols that run at the network layer include IPv4, Open Shortest Path First etc.

RESPONSIBILITIES

- The network layer determines the optimal path for data to travel from the source to the destination across interconnected networks
- Unlike the data link layer, which uses physical (MAC) addresses, the network layer uses logical addresses (IP addresses). These addresses uniquely identify devices on a network and provide the information necessary to forward packets to their destinations.
- Once the route is determined, the network layer forwards packets to their next hop on the route to the destination. This process involves encapsulating the data from higher layers into packets and adding the necessary network layer headers.

DATA LINK LAYER

- 2nd layer of OSI layer
- Provides access to the networking media and physical transmission across the media
- Breaks down data into small chunks called frames and prepare them for delivery
- Uses MAC (medium access control) address to define hardware in order to control access to media by multiple stations
- **The data-link layer is separated into two sub layers:**
- The logical link control (LLC) layer, the upper of the two layers, which is
- responsible for flow control, error correction, and resequencing functions for connection-oriented communication
- The media access control (MAC) layer, the lower of the two layers, which is
- responsible for providing a method for stations to gain access to the medium. It
- determines hardware address

RESPONSIBILITY

- **Framing:** Divides data into frames.
- **Physical Addressing:** Uses MAC addresses to identify devices
- **Error Detection:** Ensures data integrity
- **Flow Control:** Manages data flow to avoid congestion
- **Access Control:** Ensures orderly use of the network

PHYSICAL LAYER

- The lowest layer of OSI model
- It’s the path that data takes to get from one place to another
- The function is to transmit raw bit of data over medium.
- Hardware component like network cables, switches make transmission possible.
- Use different types of signal method, electrical signal, radio wave to represent the bit of data.

ENCAPSULATION

- All communications on a network originate at a source, and are sent to a destination. The information sent on a network is referred to as data or data packets.
- If one computer (host A) wants to send data to another computer (host B), the data must first be packaged through a process called encapsulation.
- Encapsulation wraps data with the necessary protocol information before network transit. Therefore, as the data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information.

- Example: Sending an Email.
- **Application Layer (Layer 7)**
- **Function**: Provides network services to end-user applications.
- **Example:** You write an email using an email client (like Outlook or Gmail).
- **Data:** The actual email content, including subject, body, attachments, etc.

- **Presentation Layer (Layer 6)**
- **Function:** Translates data between the application layer and the network format; handles encryption, compression.
- **Example:** The email content may be converted from ASCII to binary or encrypted if necessary
- **Encapsulation Added**: None specific to networking protocols but may involve encoding or encryption.

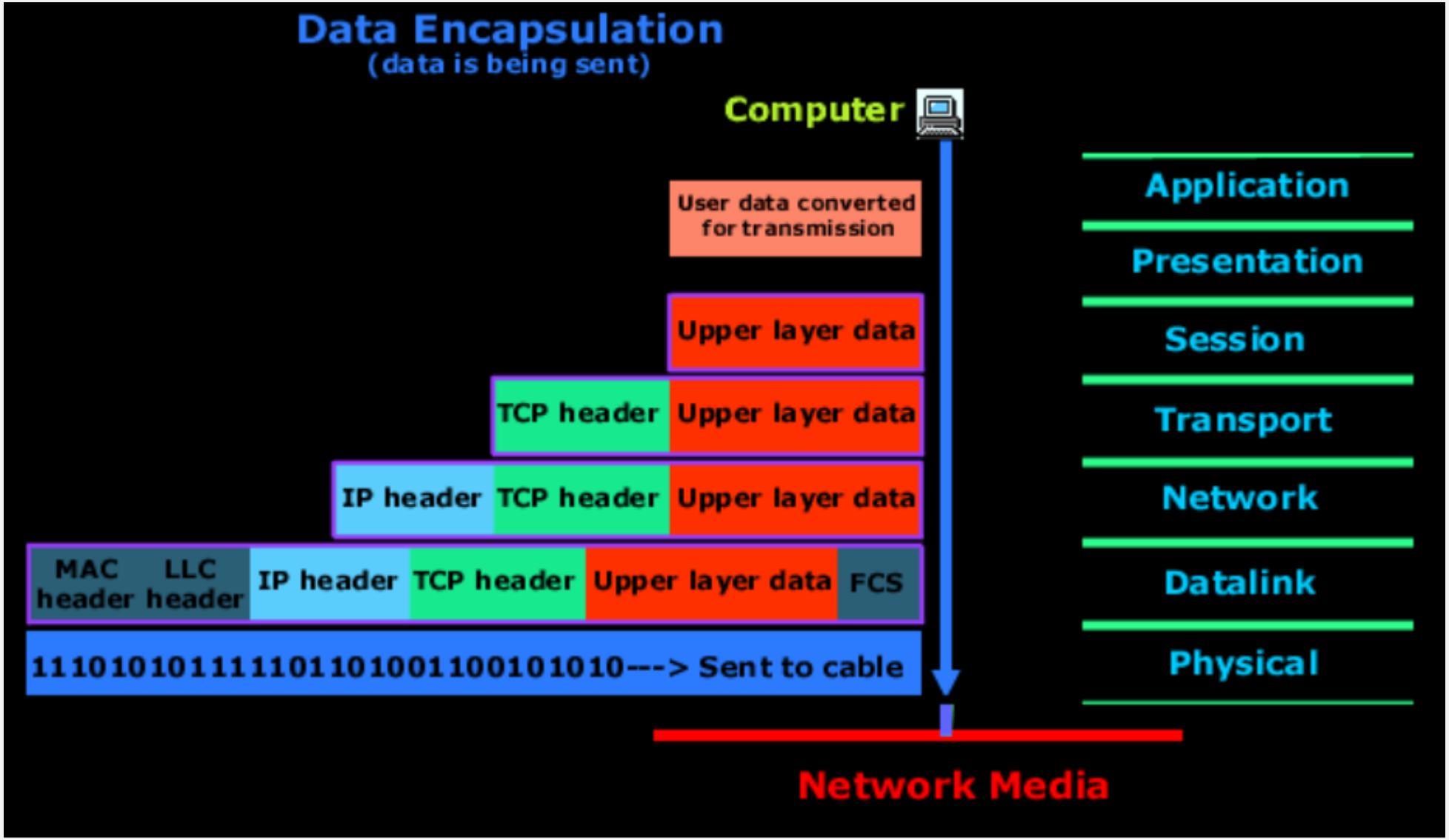
- **Session Layer (Layer 5)**
- **Function:** Manages sessions and dialogs between applications.
- **Example:** Establishing, managing, and terminating the session between your email client and the email server.
- **Encapsulation Added:** Session information such as session ID, but not typically a separate header in most protocol stacks.

- **Transport Layer (Layer 4)**
- **Function:** Provides reliable data transfer services; ensures error recovery and flow control.
- **Example:** The email is divided into segments and TCP is used to ensure reliable delivery.
- **Encapsulation Added:** Transport Header (TCP Header)
    - **Contents of Transport Header:** Source and destination port numbers, sequence numbers, acknowledgment numbers, and error-checking data (checksum).

- **Network Layer (Layer 3)**
- **Function:** Handles logical addressing and routing of packets.
- **Example:** The email segments are encapsulated into packets with IP addressing.
- **Encapsulation Added:** Network Header (IP Header)
    - **Contents of Network Header:** Source and destination IP addresses, protocol information, and other routing-related data.

- **Data Link Layer (Layer 2)**
- **Function:** Provides node-to-node data transfer; handles physical addressing and error detection.
- **Example:** The packets are framed for transmission over the local network (e.g., Ethernet).
- **Encapsulation Added:** Data Link Header and Trailer (Ethernet Header and Trailer)
  - **Contents of Data Link Header:** Source and destination MAC addresses.
  - **Contents of Data Link Trailer:** Frame check sequence (FCS) or error detection.

- **Physical Layer (Layer 1)**
- **Function:** Transmits raw bitstream over the physical medium (cables, wireless, etc.).
- **Example:** The framed data is converted into electrical signals or optical signals for transmission.
- **Encapsulation Added:** None specific to headers, but involves converting the frame into a bitstream of 0s and 1s.


Data Encapsulation
(data is being sent)
Computer
User data converted for transmission
Upper layer data
TCP header
Upper layer data
IP header
TCP header
Upper layer data
MAC header
LLC header
IP header
TCP header
Upper layer data
FCS
11101010111110110100110010101010---> Sent to cable
Application
Presentation
Session
Transport
Network
Datalink
Physical
Network Media

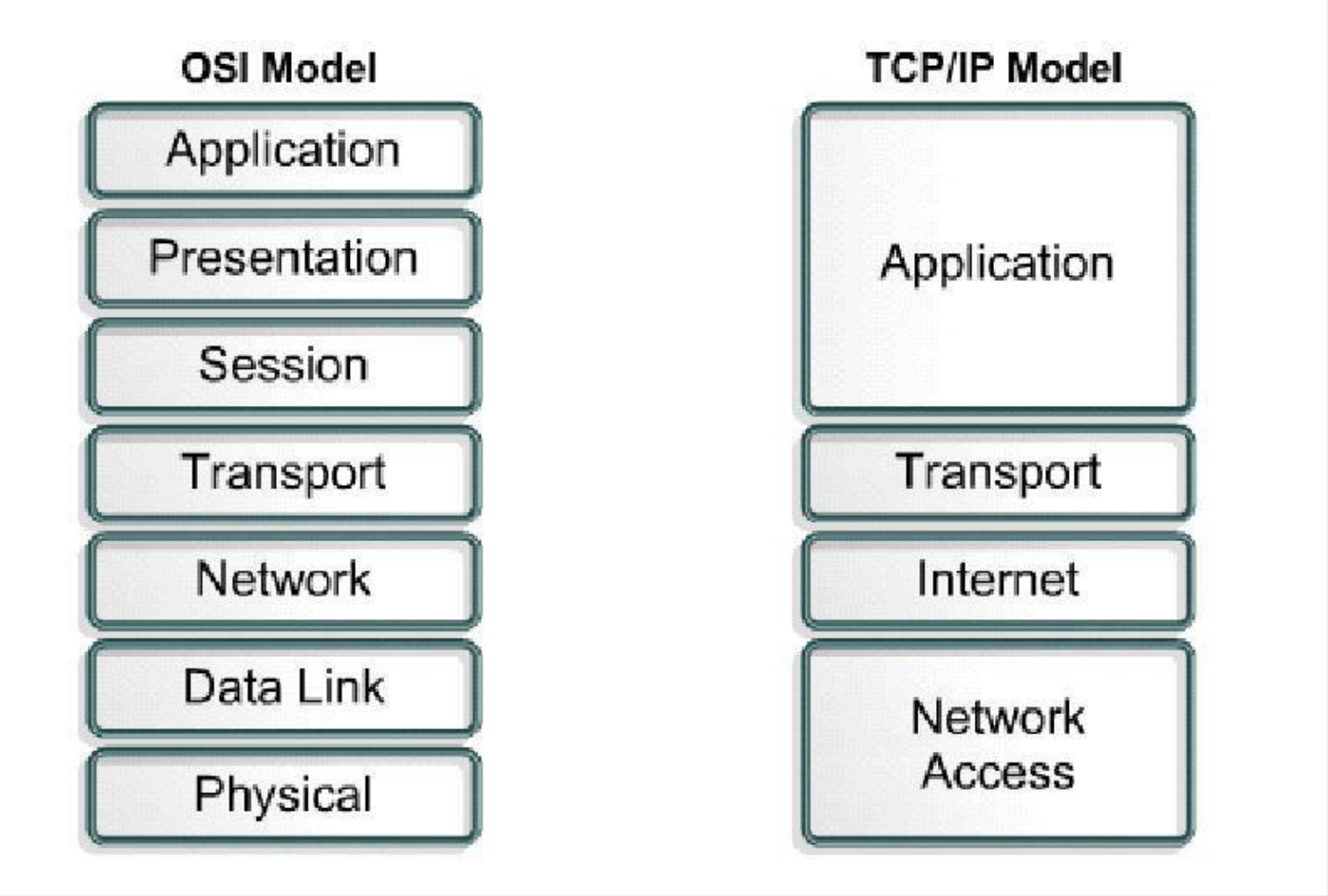
TCP/IP MODEL

- Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks

- The term TCP/IP refers to a set of protocols, or a protocol suite, that defines the rules governing how messages are exchanged in a computer network

- The TCP/IP protocol suite grew out of a research project that began in 1969 and was funded by U.S. Department of Defense.

THE LAYER OF TCP MODEL

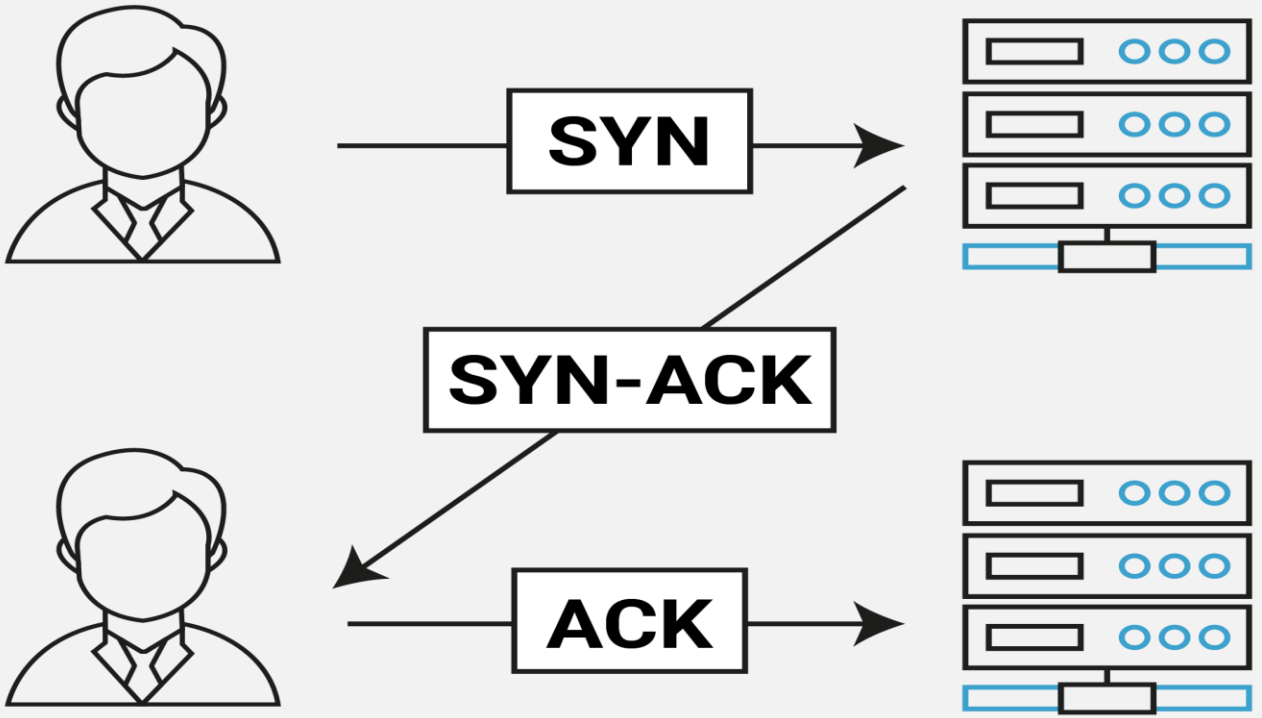


APPLICATION LAYER

- In TCP/IP, the Application layer also includes the OSI Presentation Layer and Session Layer.
- This layer deals with higher level protocols and provides user friendly environment to end user.
- The application determines the presentation of the data and controls the session. In TCP/IP the terms socket and port are used to describe the path over which the applications communicate.
- There are numerous application level protocols in TCP/IP including Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) used for email, HTTP (Hyper Text Transfer Protocol) used for World Wide Web and FTP for file transfer.

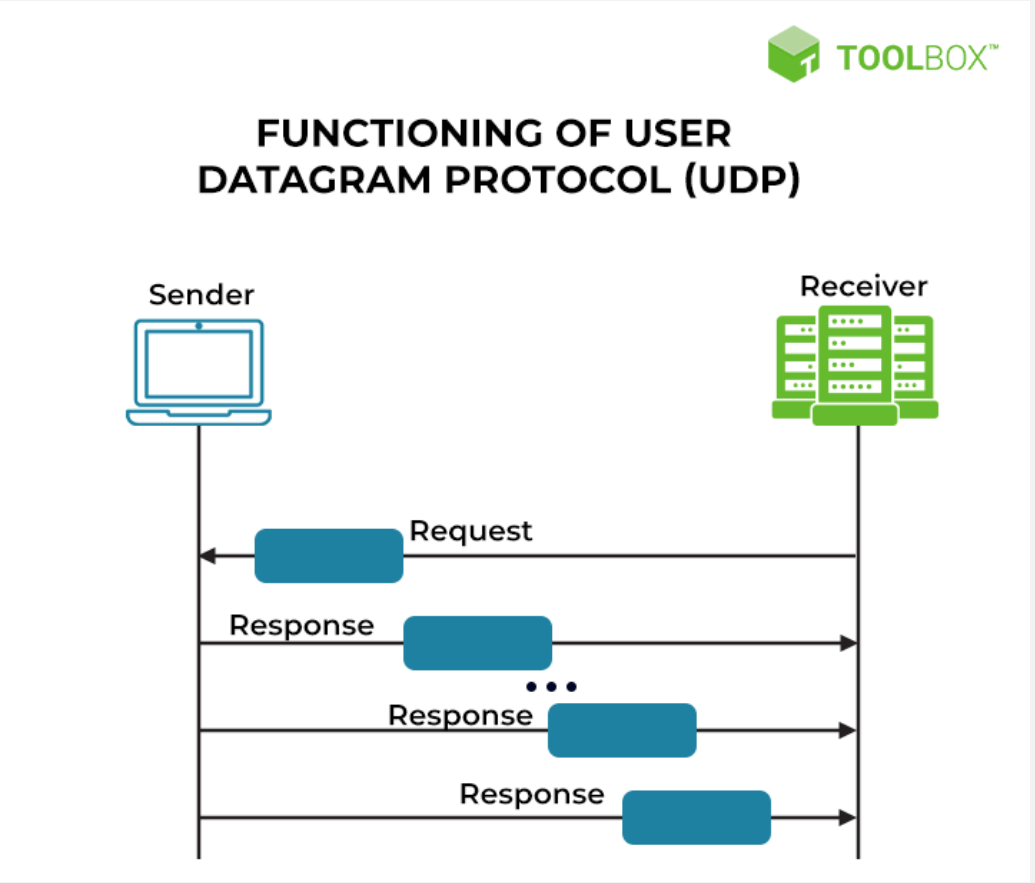
TRANSPORT LAYER

- The major function of transport layer is for end to end delivery of information from source to destination.
- Mainly two protocols are used for this purpose, the first protocol is TCP (Transmission Control Protocol). It is connection oriented protocol; it means that before sending the data from source to destination, first it establishes the fixed path and transmits the data on that path for whole session. It has the acknowledgment facility, it means source is aware whether the packet reaches to the destination or not. If the packet does not reaches to the destination, then source retransmit it until it reaches to the destination.



techopedia

- Second protocol is **UDP (User Datagram Protocol). It is connectionless** protocol, it means source does not make the fixed path to send the data to the destination. Each and every packet follows the different route and finally reaches the destination. Packets may reach to the destination out of order, it is the responsibility of the receiver to make it in proper order. UDP is unacknowledged protocol, source is not aware whether the packet reaches to the destination or no



Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection	Connection-oriented	Connectionless
Reliability	Reliable (ensures data delivery)	Unreliable (no guarantee of delivery)
Error Checking	Yes (checks for errors and ensures data integrity)	Yes (basic error checking but no correction)
Flow Control	Yes (manages the rate of data transmission)	No
Congestion Control	Yes (controls network congestion)	No
Data Sequencing	Yes (ensures packets are received in order)	No
Overhead	High (due to error checking, flow control, etc.)	Low (minimal overhead)
Speed	Slower (due to additional checks and reliability)	Faster (less overhead and processing)
Use Cases	Applications requiring reliable communication (e.g., web browsing, email, file transfers)	Applications where speed is critical and some data loss is acceptable (e.g., video streaming, online gaming, VoIP)

INTERNET LAYER

- **Function**: Handles logical addressing and routing of data packets.

•**Responsibilities**: Determines the best path for data to travel from source to destination; manages the addressing and routing of packets across the network.

•**Protocols**: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

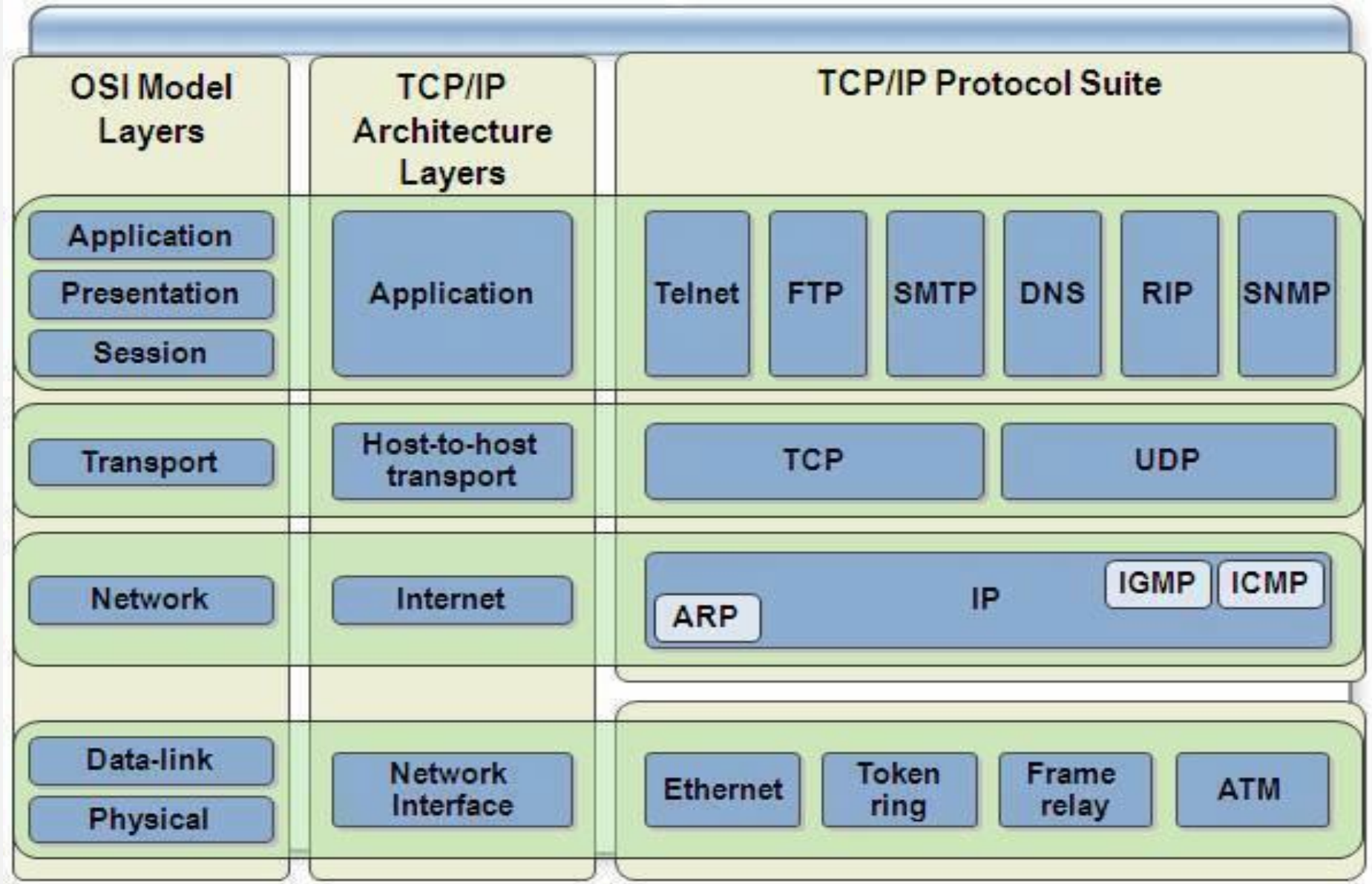
•**Example**: IP addresses are used to identify the source and destination of each data packet, enabling proper routing across the internet.

- The major protocol associated with this layer is IP. Other protocols are ICMP (Internet Control Message Protocol), IP, IGMP (Internet Group Management Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First), EGP (Exterior Gateway Protocol), BGP4 (Broader Gateway Protocol4).

ICMP is used for diagnostics and to report on problems with the IP layer and for obtaining information about IP parameters. IGMP is used for managing multicasting. Routing first protocol (RIP), OSPF, exterior gateway protocol(EGP) and Border gateway protocol BGP4 are examples of routing protocols.

NETWORK LAYER

- In TCP/IP the data link layer and physical layer are normally grouped together. TCP/IP makes use of existing data link layer and physical layer standards rather than defining its own.
- The network access layer, also known as the data link layer, handles the physical infrastructure that lets computers communicate with one another over the internet. This covers ethernet cables, wireless networks, network interface cards, device drivers in your computer, and so on.
- The network access layer also includes the technical infrastructure — such as the code that converts digital data into transmittable signals — that makes network connection possible.


OSI Model Layers
TCP/IP Architecture Layers
TCP/IP Protocol Suite
Application
Presentation
Session
Application
Telnet
FTP
SMTP
DNS
RIP
SNMP
Transport
Host-to-host transport
TCP
UDP
Network
Internet
ARP
IP
IGMP
ICMP
Data-link
Physical
Network Interface
Ethernet
Token ring
Frame relay
ATM

- Network standards
- Importance of standards
- Standards making process: de jure and de facto

- Standard organization
- ISO
- International Telecommunications Union-Telecommunications Group (ITU-T)
- American National Standards Institute (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- Electronic Industries Association (EIA)
- World Wide Web Consortium (W3C)
- Open Mobile Alliance (OMA)

- Future trends
- Wireless LAN and BYOD
- The Internet of Things
- Connected cars:
- Connected homes:
- Smart cities
- Smart buildings
- Massively Online