Computer Networks

Module 1

Introduction to Networking

SOMAIYA VIDYAVIHAR UNIVERSITY

Somaiya TRUST

Outline

- Communication System
- Basic Concepts
  - Line Configuration
  - Transmission mode
- Types of Networks
- Network Topology

What is Networking?

In simple term " *A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically using special hardware and software in order to exchange information.*"

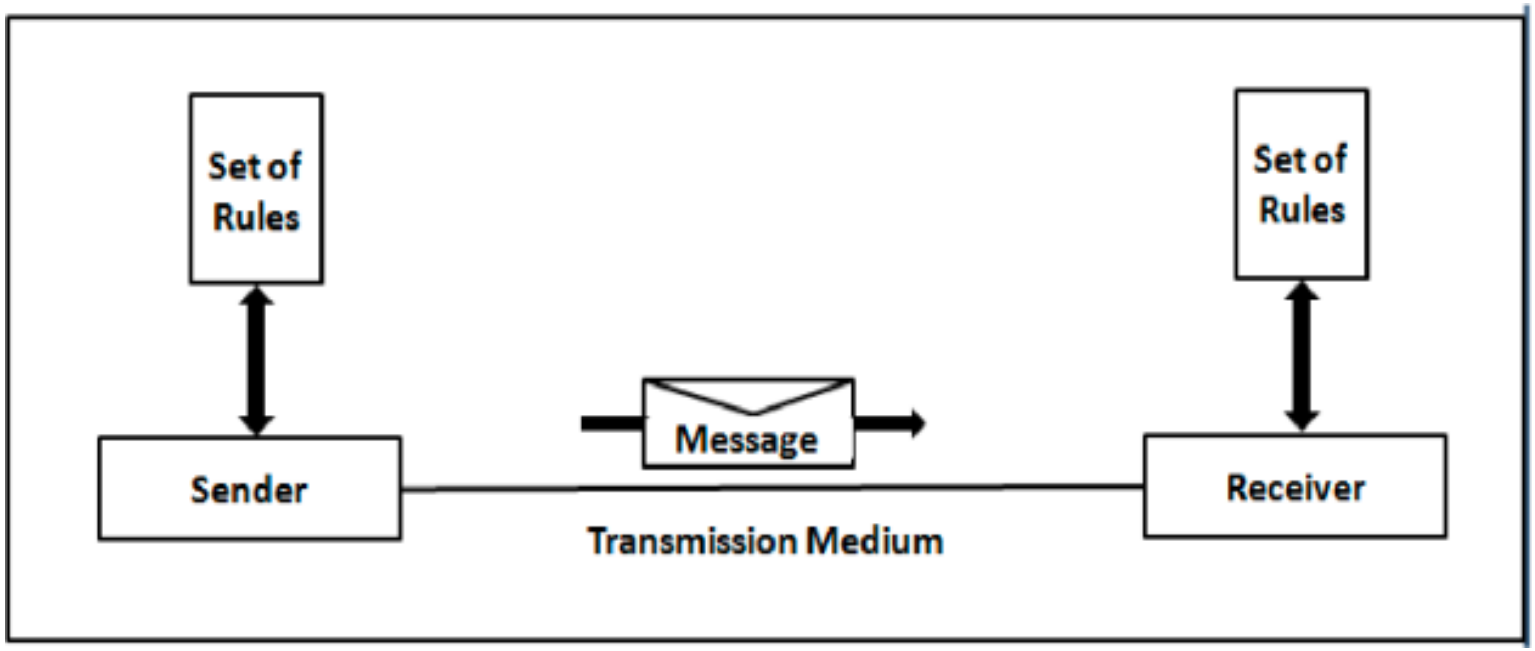
And **Networking** is term that describes the *process involved in design, implementation, management of network* using network technology.

Introduction to Communication System

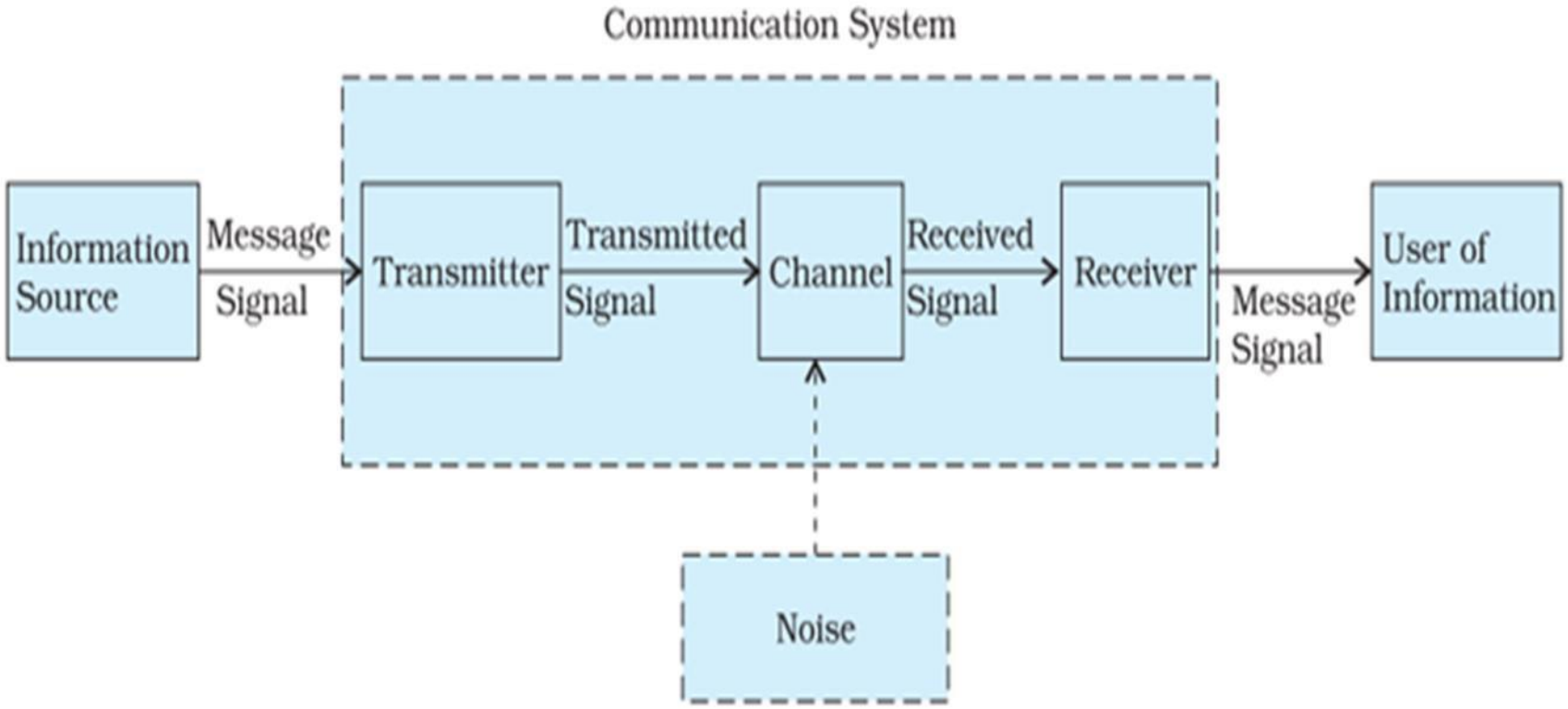
- Data Communication is a process of exchanging data or information and in case of computer networks it done in between two or more devices over a transmission medium.
- Communication system consists of Hardware and Software.
- **Hardware**: Sender, Receiver and Intermediate devices
- **Software**: Set of rules and protocols that need to satisfied.

Components of Data Communication

- Components:
  - Message
  - Sender
  - Receiver
  - Transmission Medium
  - Protocols

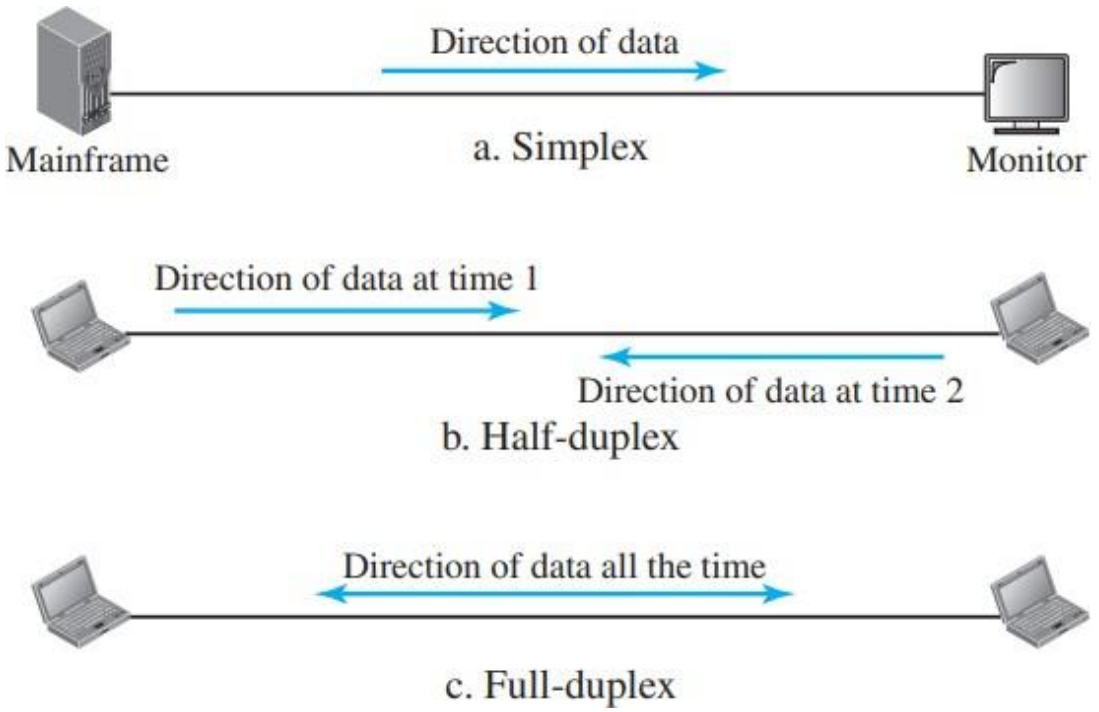


Elements Of Communication System



Data Flow

- Simplex
- Half-Duplex
- Full Duplex



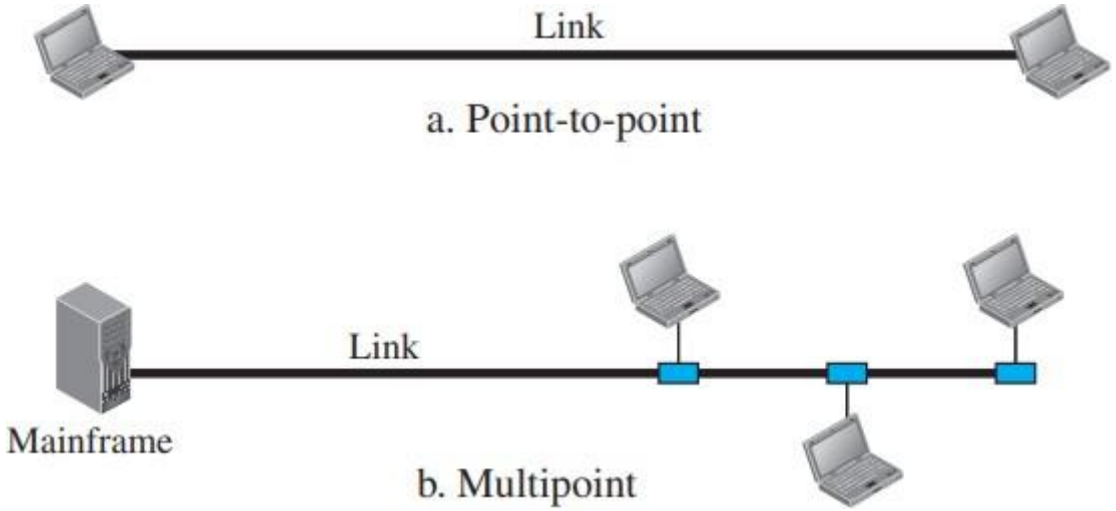
Network Criteria

- **Performance:**
  - Can be measured in terms of
    - Transit time
    - Response time
  - Evaluated by two networking metrics: Throughput & Delay
- **Reliability:** measured by frequency of failure, time taken by link to recover from failure and network robustness ion catastrophe
- **Security:** Securing data from unauthorized access, protecting data from damage, implementing policies, recovery from breaches and data loss.

Physical Structures

Type of Connections:

- Point-to-Point connection:
  - Provides dedicated link between two devices
  - Entire link capacity is reserved between two devices
- Multipoint (Multidrop):
  - More than two devices share a single link.
  - Capacity of channel is shared
  - Channel is shared either *Spatially or Timeshared*.



Physical Topology

Physical Topology refers to a way in which network is laid out physically.

Topology is geometric representation of relationship of all the links and linking devices (also called nodes) to one another.

There are Four basic Topologies:

- Mesh
- Star
- Bus
- Ring

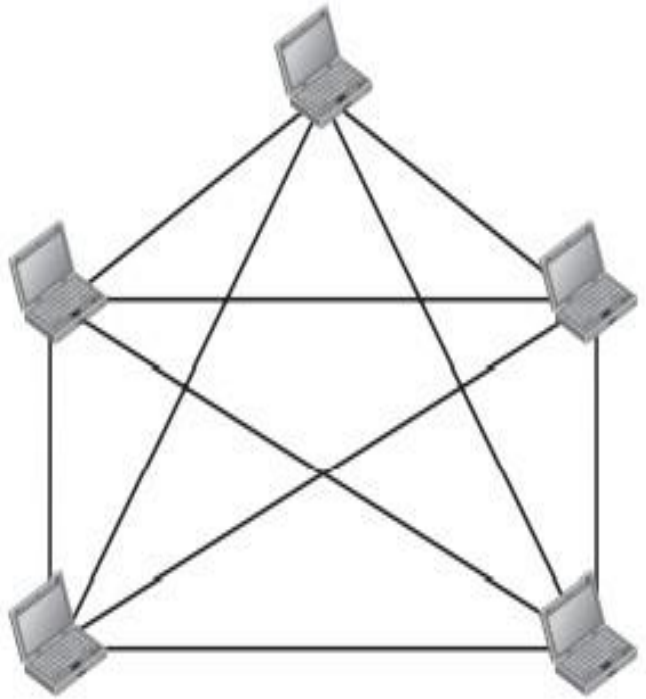
Mesh Topology

- Every device has a dedicated point-to-point link to every other device.
- Link carries traffic only between the two devices it connects.
- Total number of physical links in a fully connected mesh network with n nodes is equal to **n(n-1).**
- In case of communication in both direction : **n(n-1)/2 duplex node links.**
- Every device on network must have **(n-1) input/output** (I/O) ports.

Mesh Topology

- Advantages
  - No traffic problems
  - Robust
  - Privacy and security
  - Point to point link: fault identification and isolation is easy
- Disadvantages
  - Installation and reconnection difficult as devices interconnected.
  - Bulk wiring
  - Expensive: hardware cost

$n = 5$
10 links.



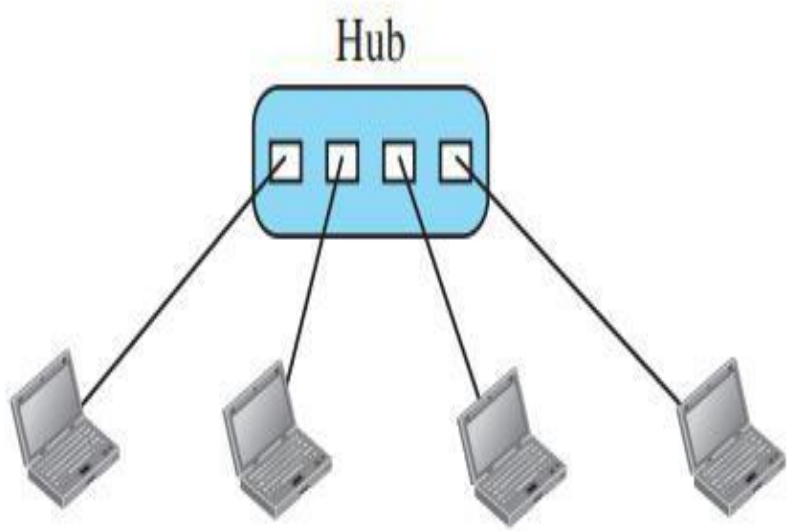
Star Topology

- each device has a dedicated point-to-point link only to a central controller, usually called a ***hub***.
- devices are not directly linked to one another.
- star topology does not allow direct traffic between devices.
- The controller acts as an exchange, it relays the data to the other connected device.
- The star topology is used in local-area networks (LANs)

Star Topology

Advantages

- Less expensive than mesh
- Reconfiguration and installation is easy.
- Robustness
- Easy fault identification as long as hub is worki



Disadvantages

- Dependency on single point controller.
- Each node must be linked to hub: more cabling required compared to other topologies except mesh.

Bus Topology

- A bus topology is multipoint connection.
- One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

Bus Topology

Advantages

- Ease of installation: less cabling as compared to mesh and star.
- A bus uses less cabling than mesh or star topologies

Disadvantages

- It is Difficult to add new devices.
- Difficult reconfiguration and fault isolation.
- A fault in Backbone stops all transmission
- Limited cable length and number of nodes that can be connected.

Ring Topology

- Each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater.

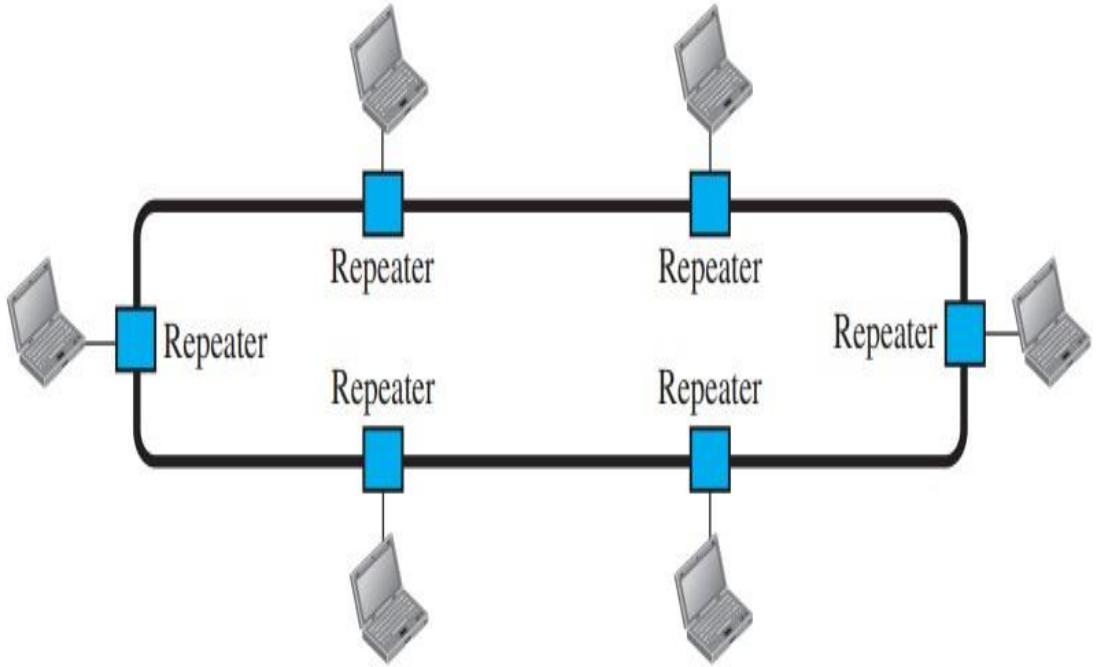
Ring Topology

Advantages

- Easy to install and reconfigure.
- Easy adding and deleting of connections.
- Fault isolation simplified: devices can raise the alarm.

Disadvantages

- Unidirectional traffic can be a disadvantage.
- Breakdown in ring disables the entire network.



SOMAIYA VIDYAVIHAR UNIVERSITY

Somaiya TRUST

Types of Networks

- Local Area Network (LAN)
- Metropolitan Area Network(MAN)
- Wide Area Network(WAN)

Local Area Networks

- A ***l**ocal-**a**rea **n**etwork* (LAN) is a computer network that spans a relatively small area.
- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.
- LAN size is limited to a few kilometers.

Local Area Networks

- LANs are designed to allow resources to be shared between personal computers or workstations.

  Example: hardware or software

- One of the computers may be given a large capacity disk drive and may become a server to clients.

- LAN extends up to 10m to 1km

Local Area Networks

- LANs are distinguished from other types of networks by their transmission media and topology.

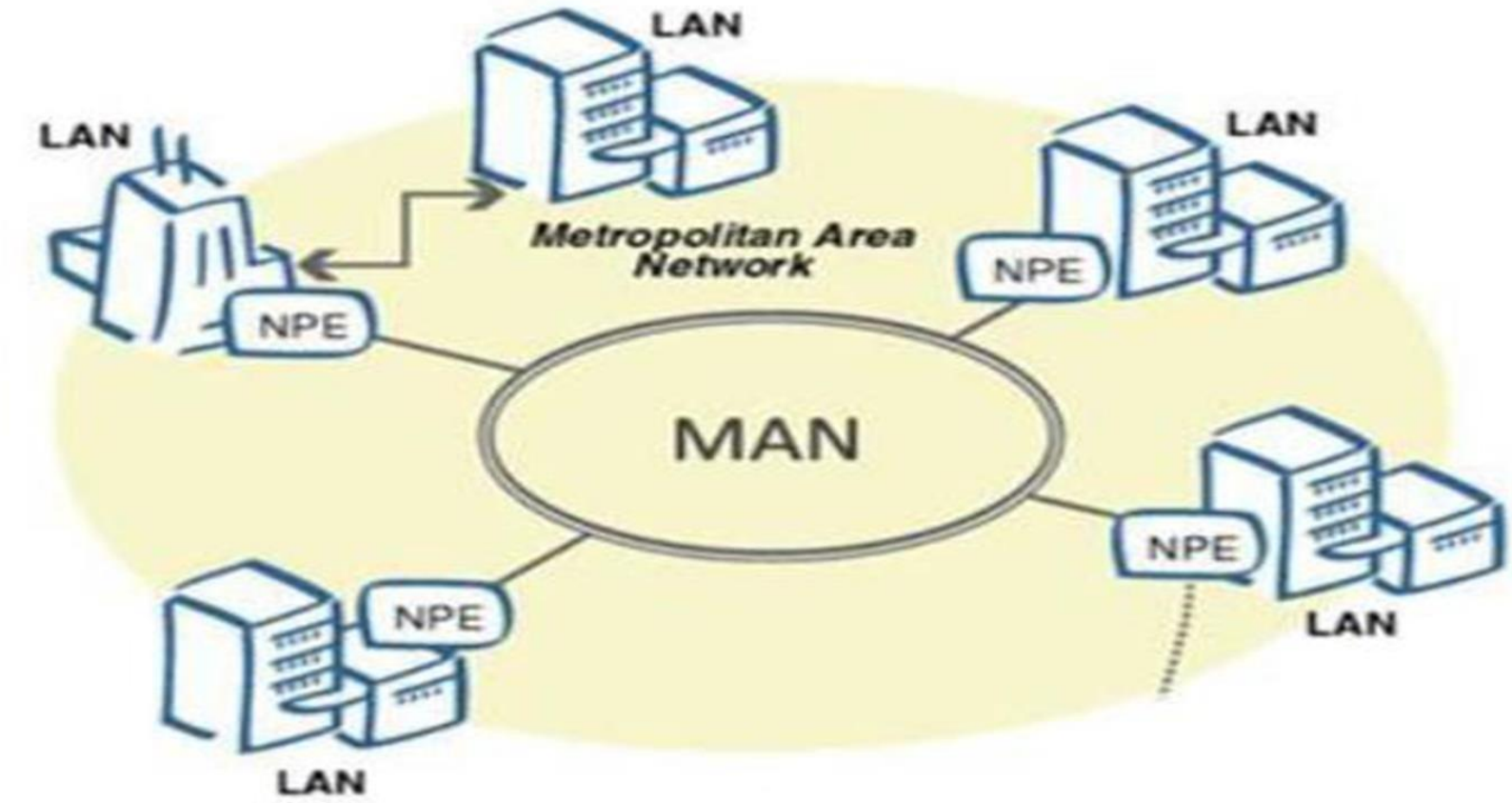
- Speeds: 100 or 1000 Mbps.

Metropolitan Area Networks

- Metropolitan Area Network usually covers area inside a town or a city.
- It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.

  Example: cable TV network
- MAN extends up to 30-40 km.
- Speed of 34–155 Mbit/s.
- MAN uses Guided Media or Unguided media.

Metropolitan Area Networks



Wide Area Networks

- A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent or even the whole world.

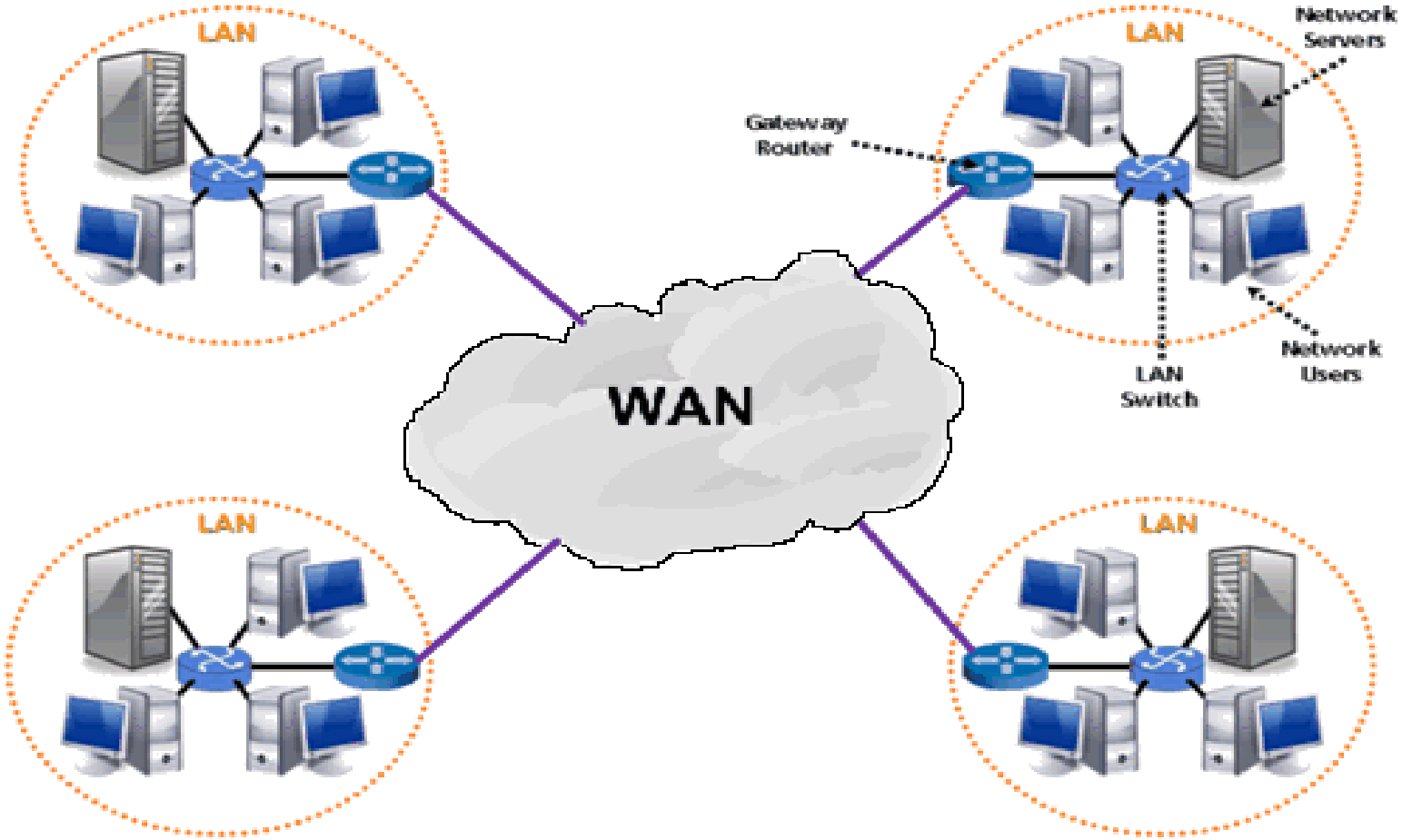
- WAN (Wide Area Network) is a group of computers and other network devices which are connected and not restricted to a geographical location.

- Internet is WAN.

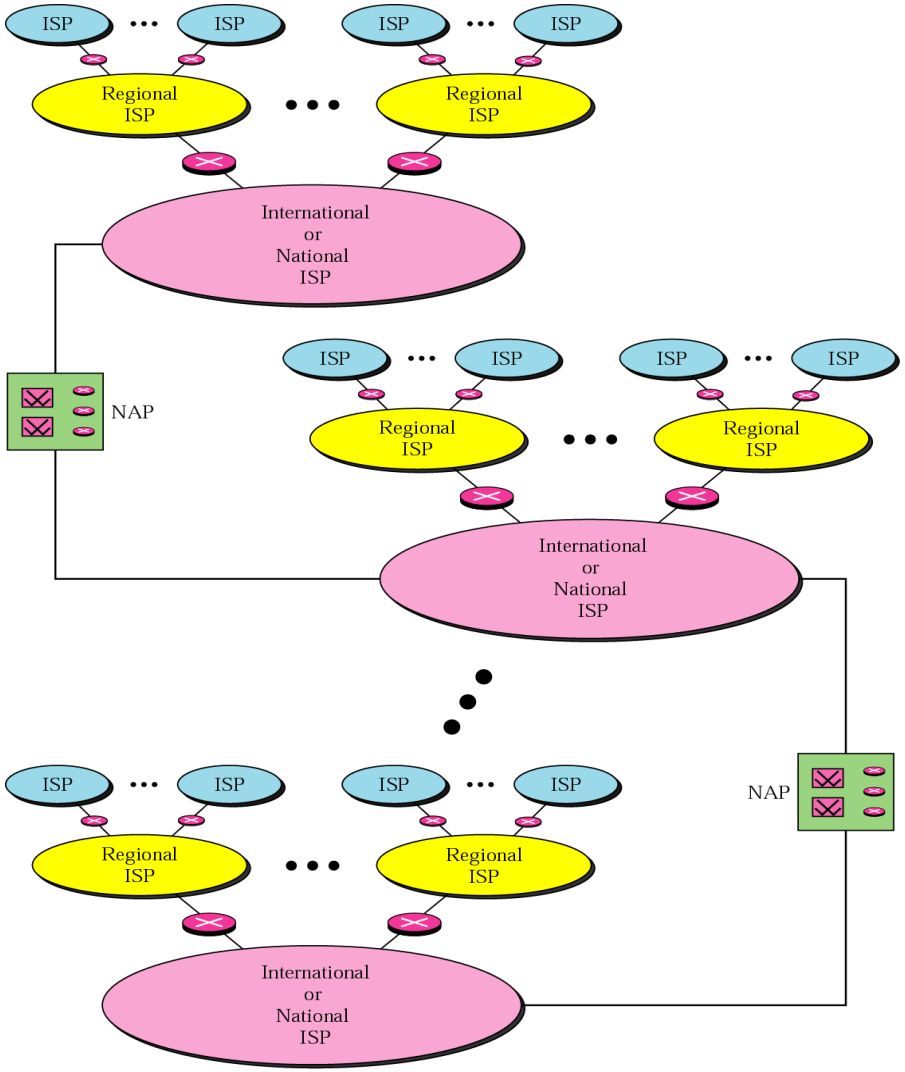
Wide Area Networks

- WAN speed varies based on geographical location of the servers. WAN connects several LANs.
- WAN connection speeds can be 10Mbps or 100Mbps.
- WAN mainly uses Guided Media or Unguided media.

Wide Area Networks



Internet


ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National ISP
NAP
ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National ISP
ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National ISP
NAP

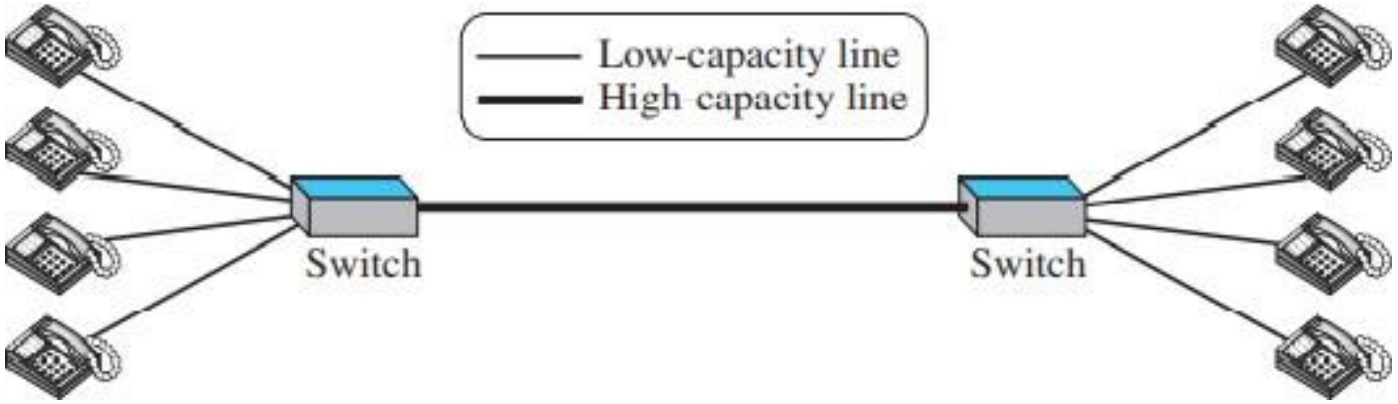
Switching

An internet is a switched network in which a switch connects at least two links together

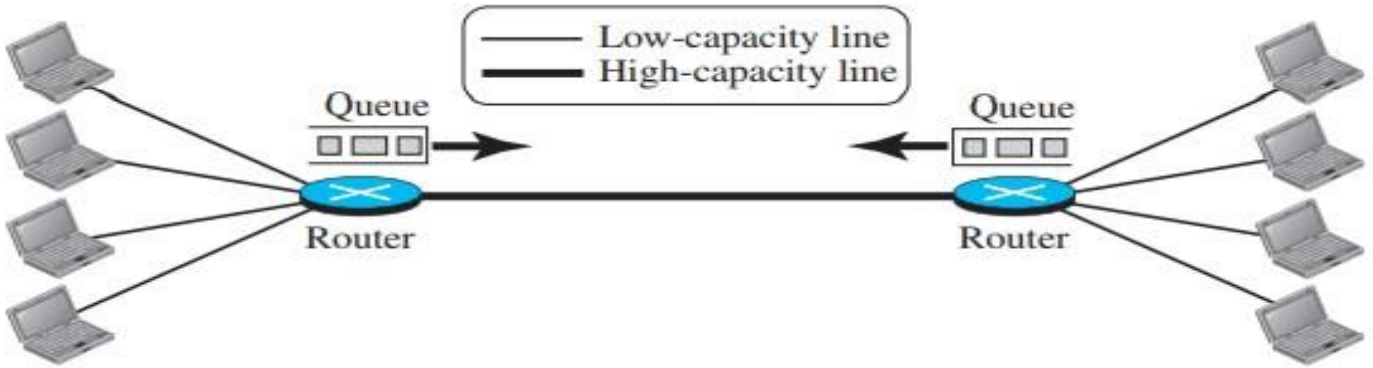
The two most common types of switched networks are circuit-switched and packet-switched networks.

- Circuit-Switched Network
- Packet Switched network

Switching

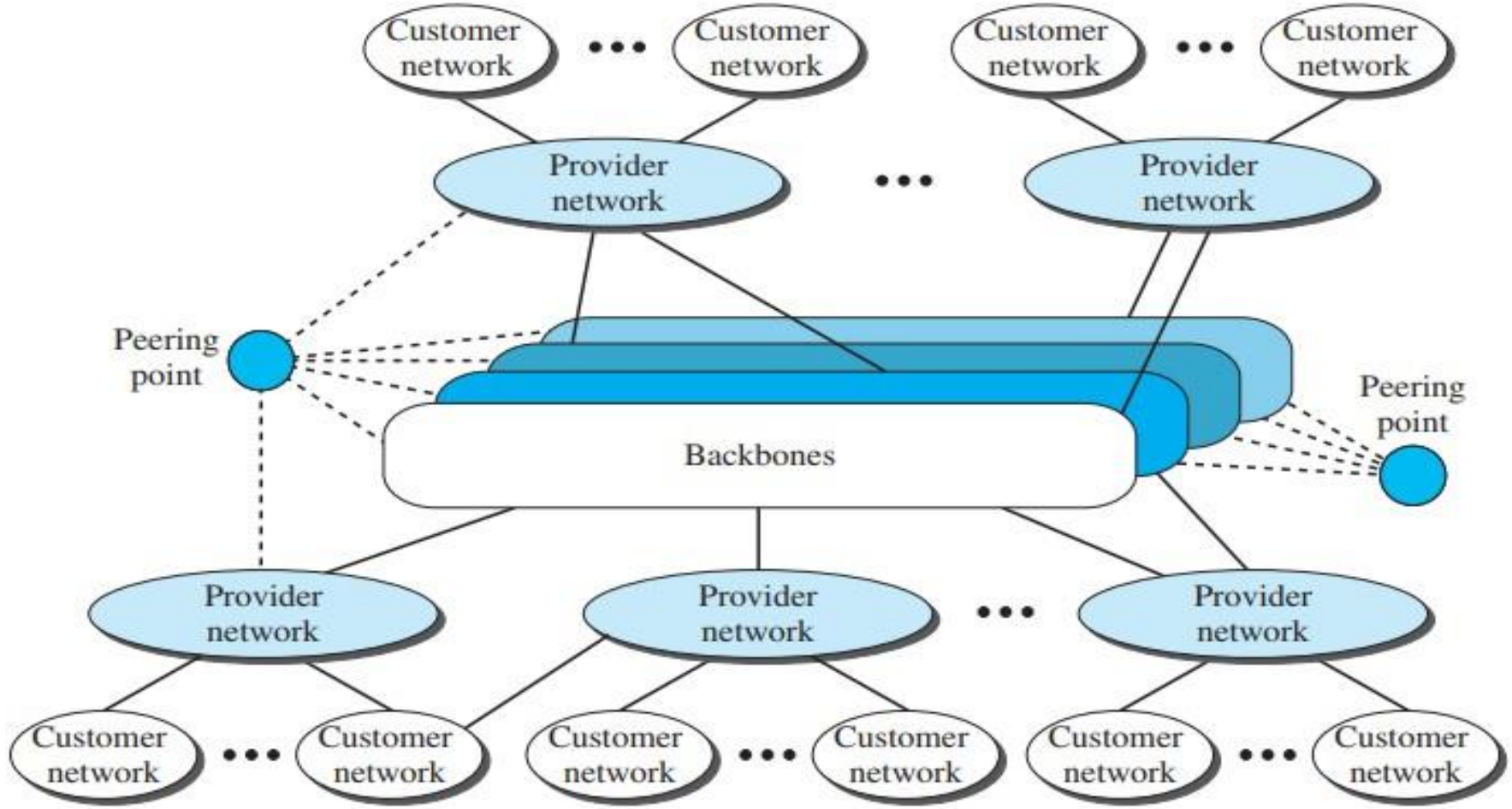


A Circuit Switched network



A Packet Switched network

The Internet Today



Network Models

Protocol Layering:

- ISO OSI Model
- TCP/IP model

Design Issues for Layers

Addressing - whom am I going to talk to? i.e., how do we identify senders and receivers?

Rules for data transfer: Simplex (one-way channels), half-duplex (two-way communication but not simultaneously) and full duplex (2 way)

Logical channels: usually at least 2. One for normal mode and one for urgent transmission.

Design Issues for Layers

Reconstituting messages: Out of order messages need to be numbered.(Flow Control)

Error control: This is all about communicating along imperfect channels and error correction in such cases. (Issues: Attenuation, delay distortion and noise).

Large messages: Procedures for disassembling, transmitting and reassembling. What to do when messages are very small (compared to packet)?

Design Issues for Layers

Multiplexing: One connection per conversation or many on one connection. Important in physical layer where only a few lines are available

Routing: What to do when there are multiple paths between communicating machines

Connection Less Services

- No session connection between sender and receiver.
- No reliability
- Short messages
- Does not maintain state information.
- Less overhead
- Example: Walkie-Talkie

Connection Oriented Services

- Requires session connection (analogous to a phone call).
- Reliable network service.
- Set up virtual links between the end systems through a network.
- Long messages.
- High overhead and places greater demands on B/W.
- Example: Email

Difference

S.NO	Connection-oriented Service	Connection-less Service
1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
7.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
8.	Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
9.	Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
10.	Connection-oriented requires authentication.	Connection-less Service does not require authentication.

Difference -Example

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
Connection-less	Unreliable connection	Digitized voice
	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Reliable and un-reliable services

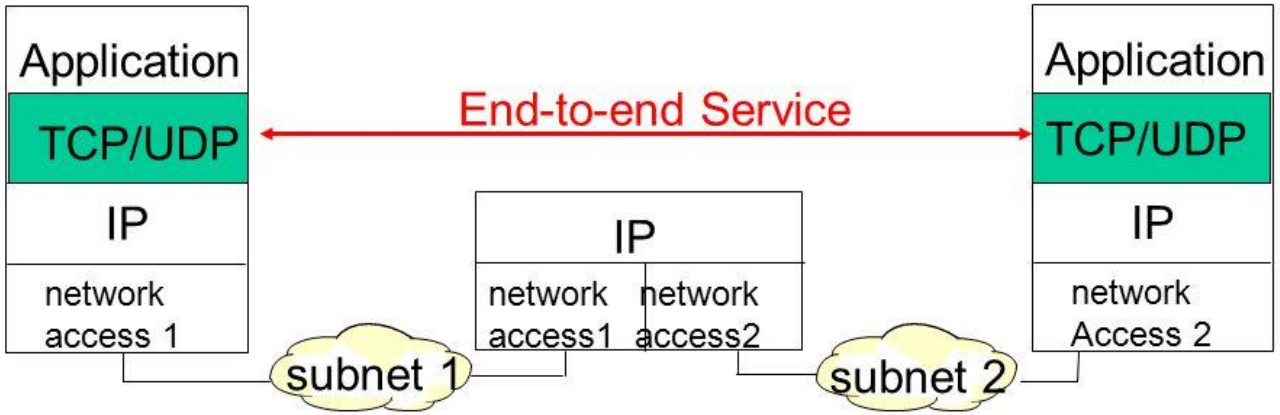
Reliable Versus Unreliable

- Reliable Service
  - If the application layer program needs reliability, we use a reliable transport protocol such as TCP and SCTP.
  - This means a slower and more complex service.
- Unreliable Service
  - If the application layer program does not need reliability because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time application), then unreliable protocol such as UDP can be used.
- Do we need reliability control at the transport layer, even the data link layer is reliable and has flow and error control ?
  - The answer is yes.
  - The network layer in the Internet is unreliable (best-effort delivery), we need to implement reliability at the transport layer.

Reliable and un-reliable services

Reliable vs. Unreliable Service

- If the application-layer program needs reliability, we use a reliable transport protocol.
- If the application has its own flow and error control mechanism or it needs faster service or the kind of a service that does not demand flow and error control(ex, real-time application), then unreliable transport can be used.



The OSI model

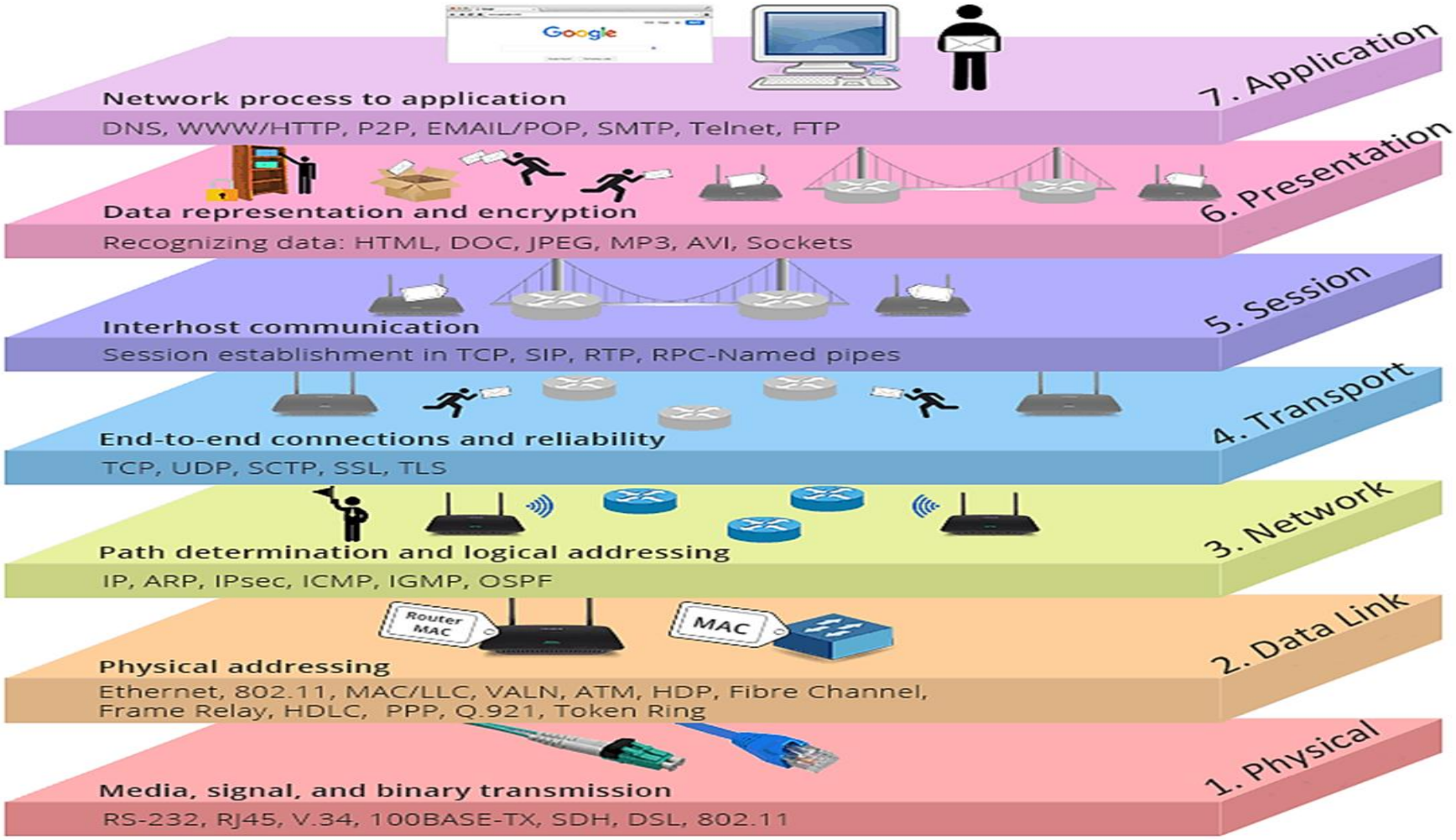
- Over the past couple of decades many of the networks that were built used different hardware and software implementations, as a result they were incompatible, and it became difficult for networks using different specifications to communicate with each other.

- The **Open System Interconnection (OSI)** model includes a set of protocols that allows any two systems to communicate regardless of their architecture.

The OSI model

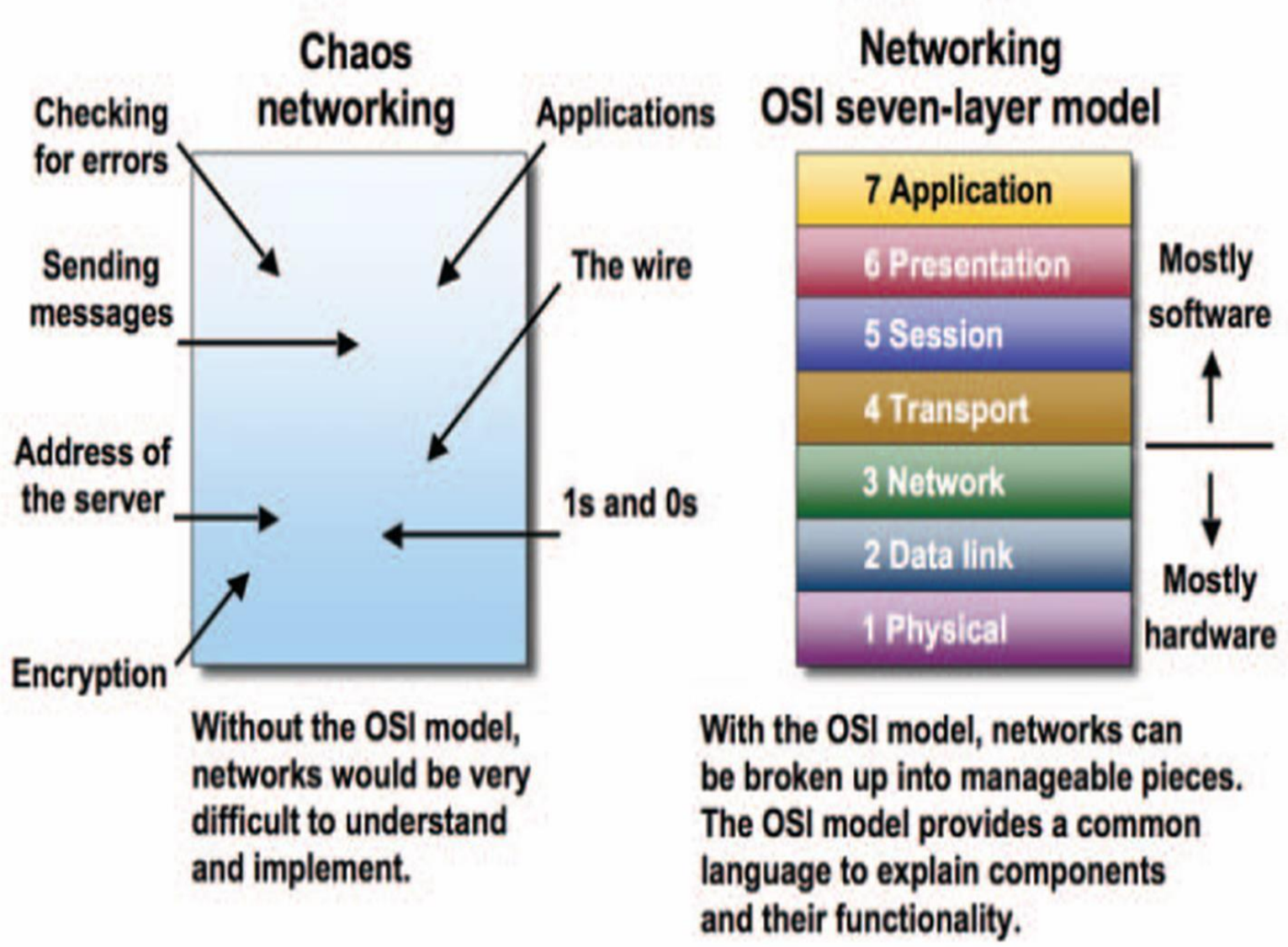
- The OSI model is a concept that describes, how data communications should take place.
- OSI is also called as the framework for design of network systems.
- It divides the process into seven steps called layers.

OSI

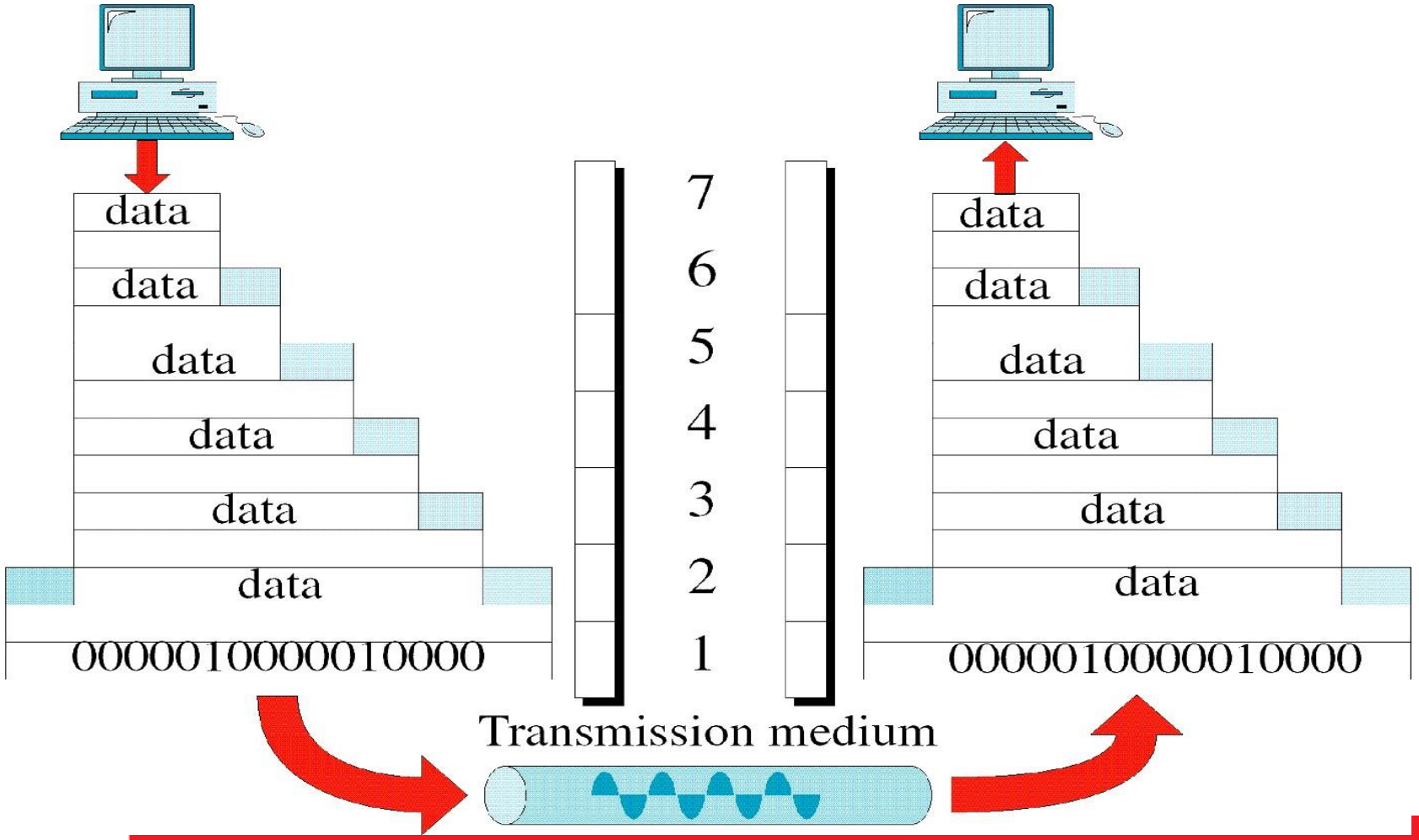


Ref: https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

The OSI model



The OSI model



Physical Layer

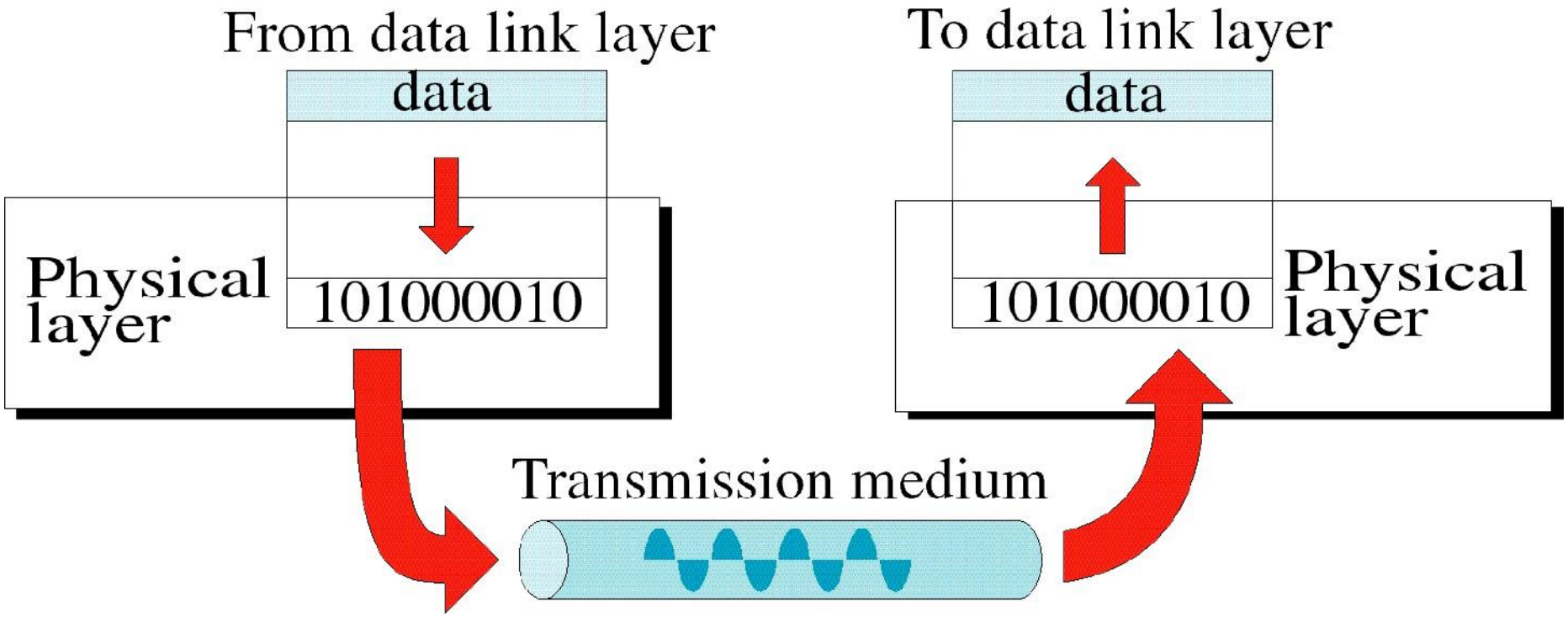
- The physical layer deals with the physical characteristics of the transmission medium.
- This layer consists of simply the wire or media by which the network signals are conducted.
- The physical layer of the OSI model defines connector and interface specifications, as well as the medium (cable) requirements for transmission to occur.

Physical Layer

Functions of physical layer:

- Physical characteristics of interfaces and medium.
- Representation of bits: Conversion from binary to electrical or optical.
- Data rate.
- Synchronization of bits.
- Physical topology
- Line configuration: point to point or multipoint.

Physical Layer



Data Link Layer

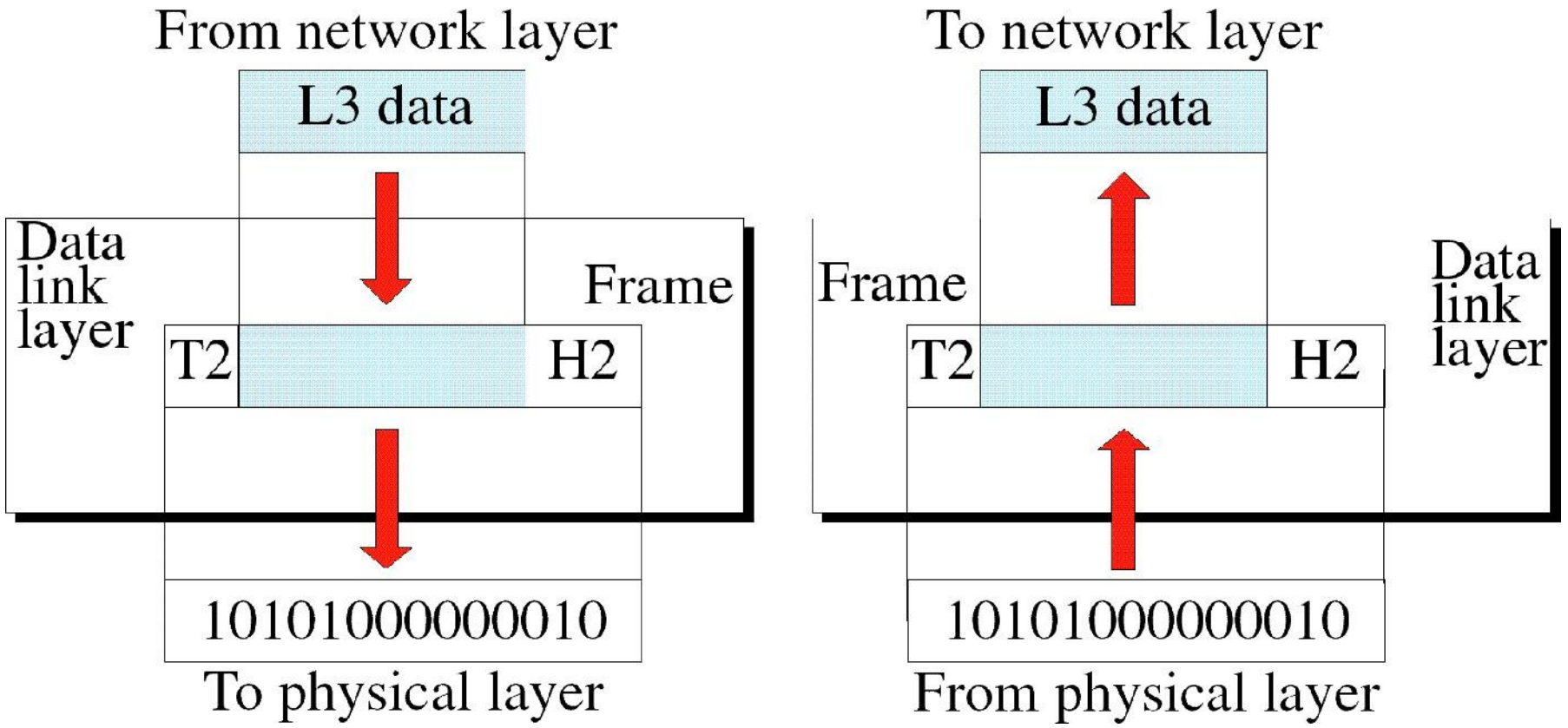
- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
- *Node to node delivery (Hop to Hop Delivery)*
- The data link layer uses the **MAC address** to define a hardware or data link address for multiple stations to share the same medium and still uniquely identify each other.
- Concerned with network topology, network access, error notification, ordered delivery of frames, and flow control.

Data Link Layer

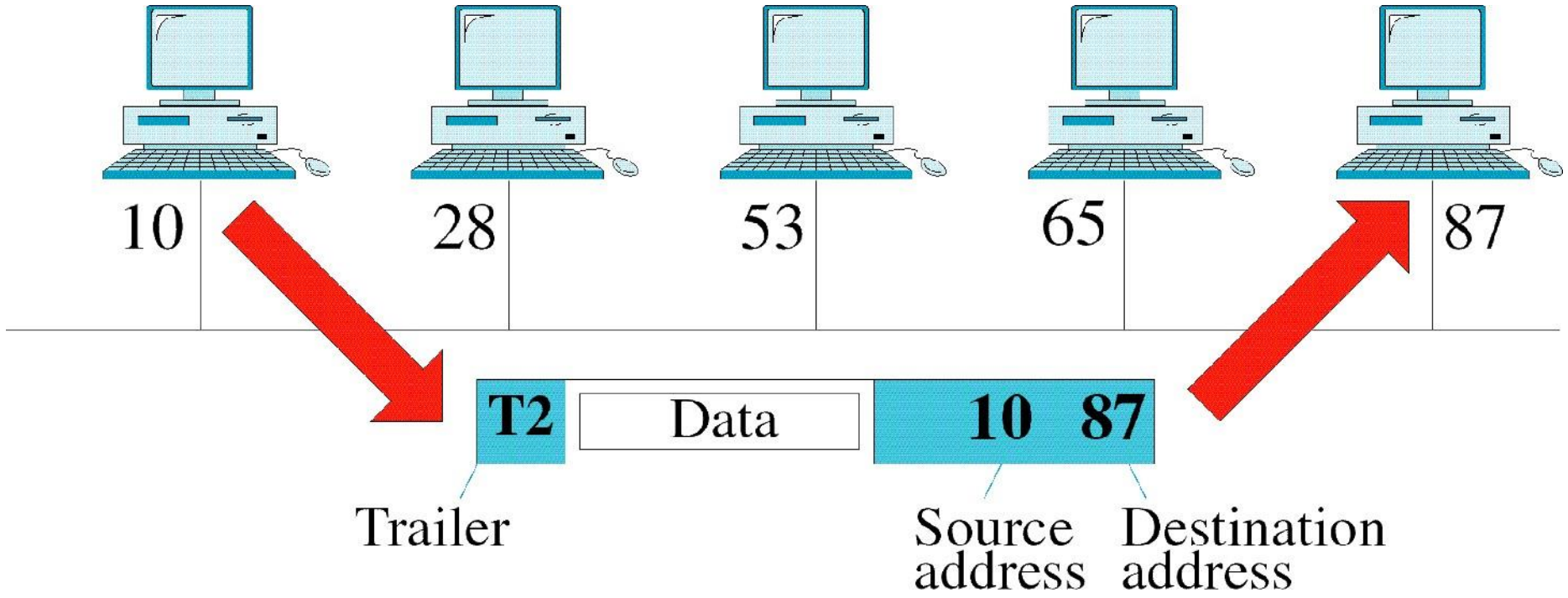
Functions of Data Link layer:

- Framing
- Physical addressing: adding header to frame to identify sender and receiver address.
- Flow control
- Error control
- Access control

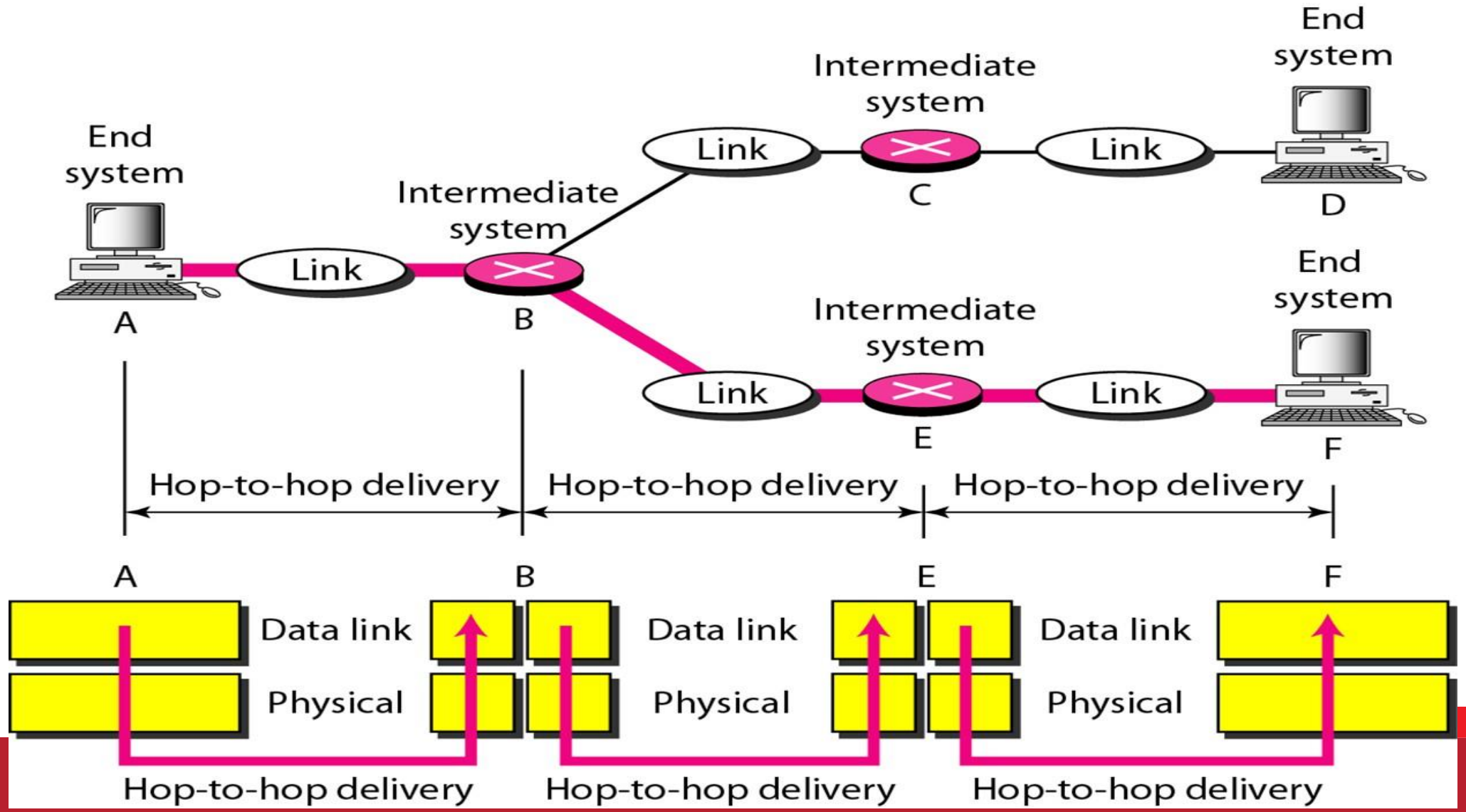
Data Link Layer



Data Link Layer



Hop-to-Hop Delivery



Network Layer

- This layer establishes the route between the sending and receiving stations.
- Responsible for delivery of individual packets from source to destination.
- Two systems connected on same link-no network layer.
- Two systems on different link-need network layer

Network Layer

- It handles the routing of data (sending in the right direction to the right destination on outgoing transmissions and receiving incoming transmission at the packet). The layer does routing & forwarding of data.

- Network layer addresses can also be referred to as logical addresses.

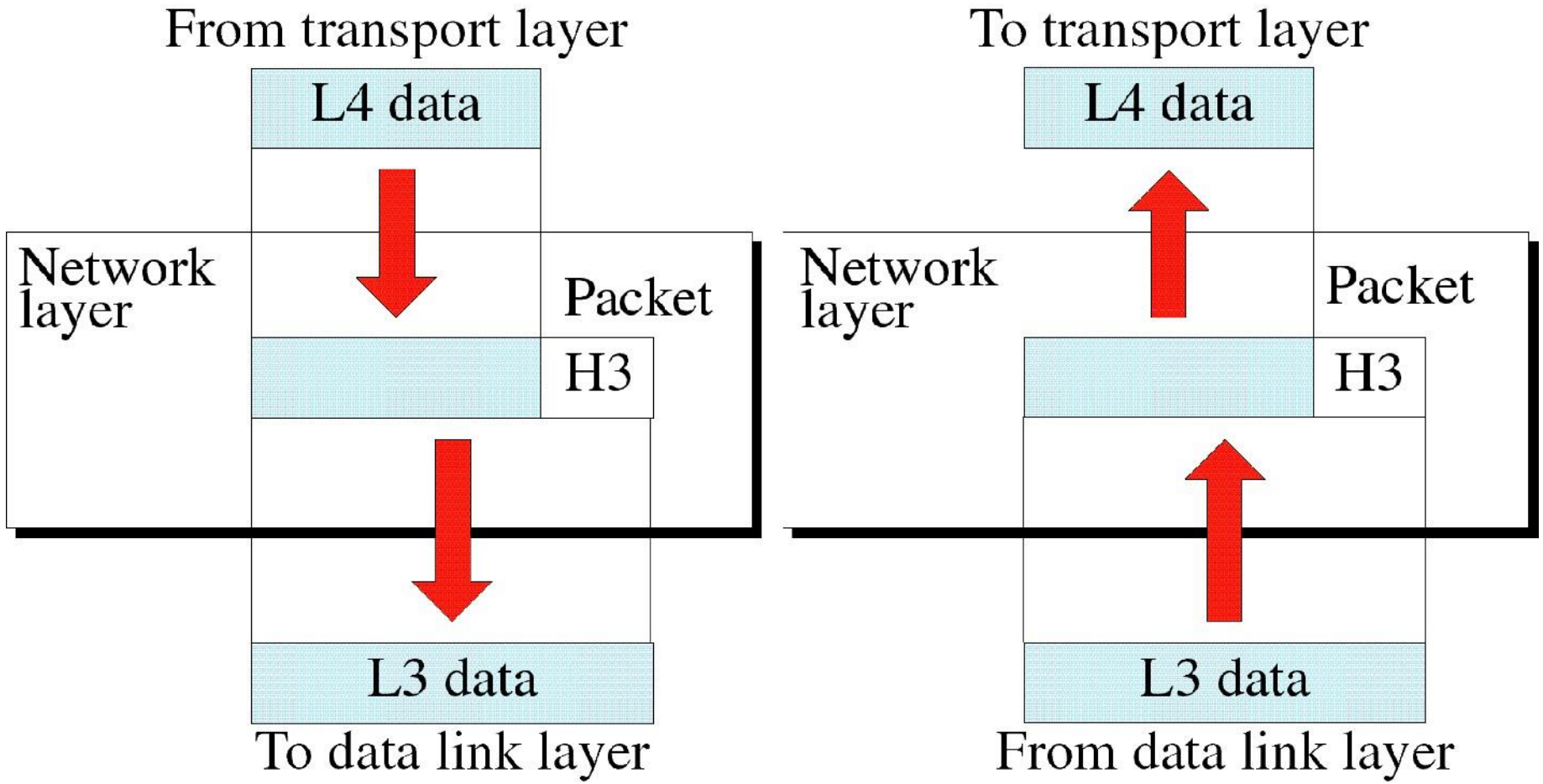
Network Layer

Functions of network layer:

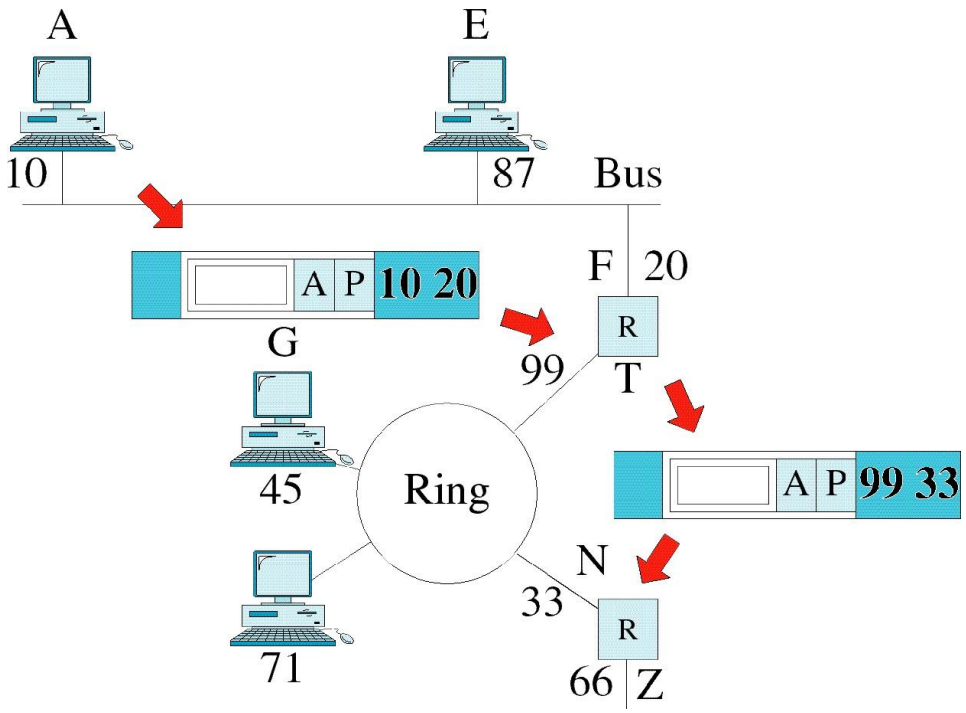
- **Logical addressing:**
  - Data link layer physical addressing-handles addresses locally.
  - Packet crosses network boundary-IP addressing.

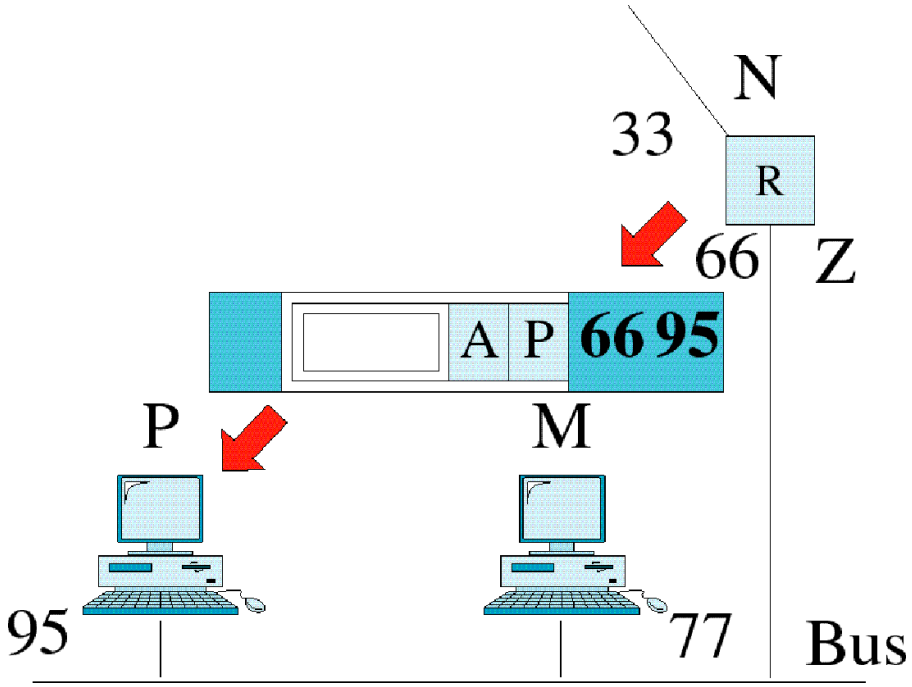
- **Routing** : Routing packets to destination via connecting devices over large networks.

Network Layer

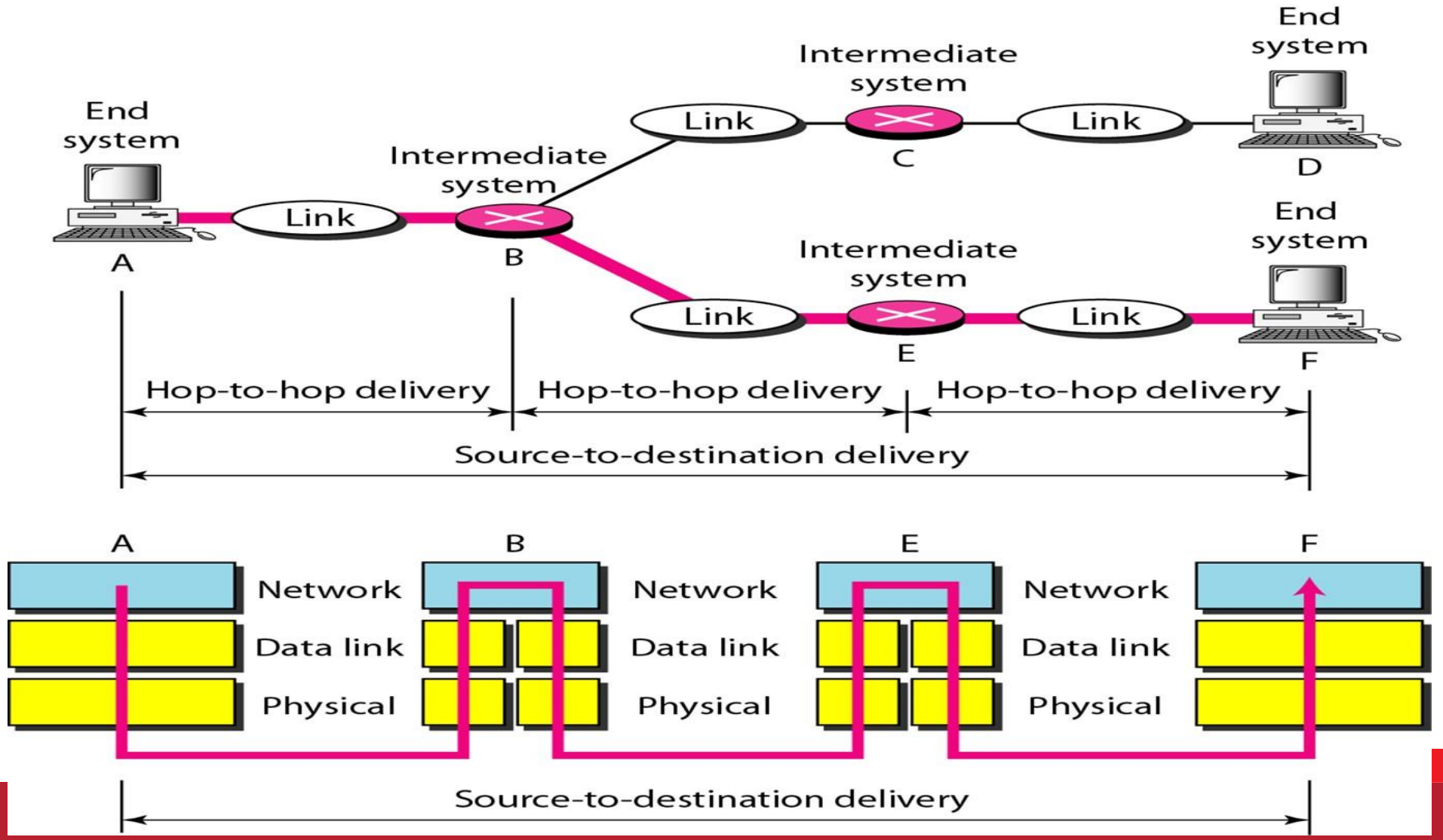


Network Layer Example





Source-to-destination delivery



Transport Layer

- The transport layer is responsible for the delivery of a message from one process to another.
- Transport layer recognizes relationship between the packets and makes sure that the whole message arrives intact and in order.
- It is responsible for constructing stream of data segments, sending and checking for correct delivery.

Transport Layer

- If data is sent incorrectly, this layer has the responsibility to ask for retransmission of the data.
- This layer acts as an interface between the bottom and top three layers.

Transport Layer

Responsibilities of transport layer:

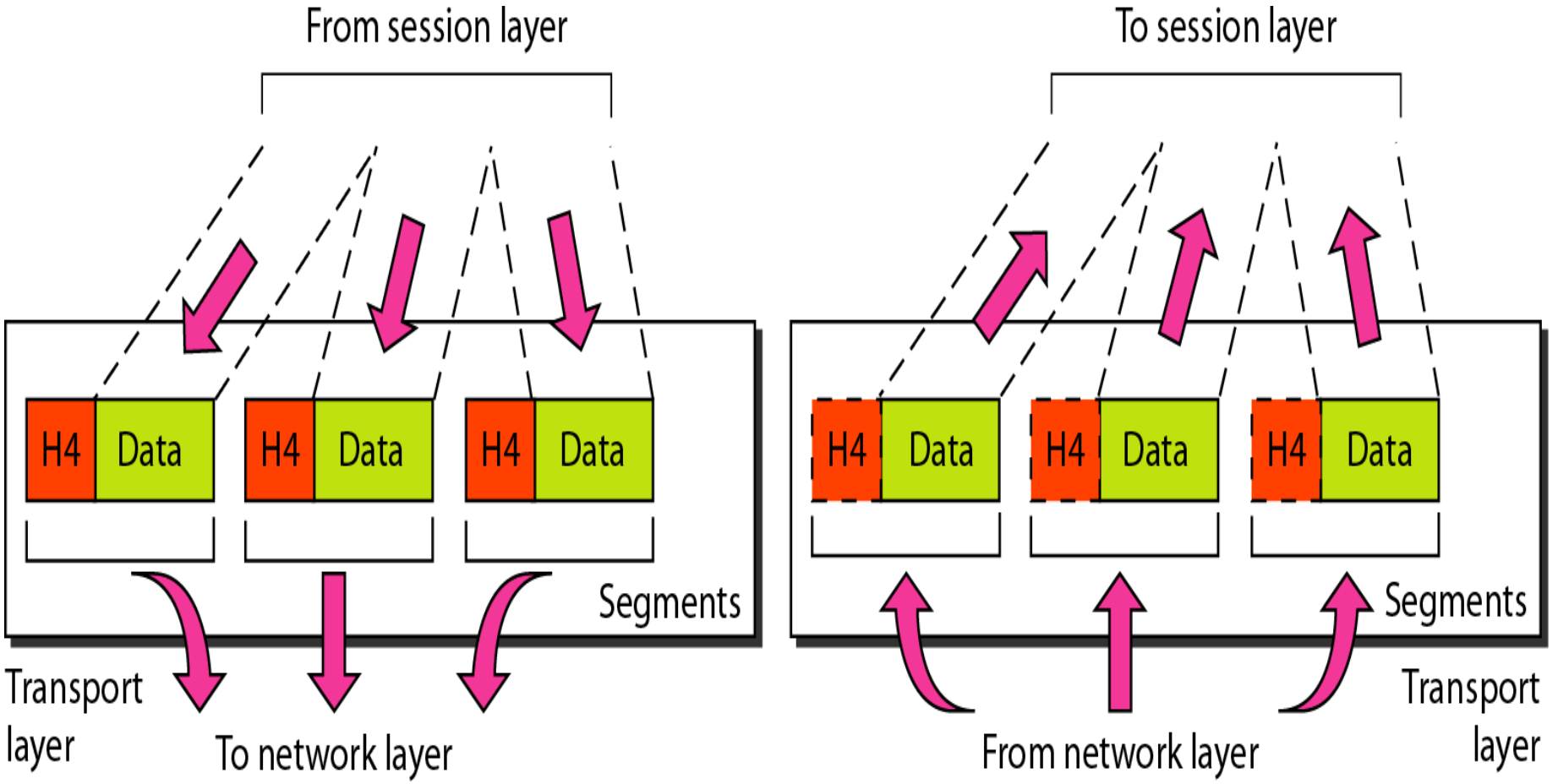
- *Service-point addressing*: Port Address(process to process).
  - Network layer gets each packet to correct computer.
  - Transport layer gets each packet to correct process on that computer.
- *Segmentation and reassembly*: Message divided into segments-sequence number
- *Retransmission* in case of lost segment.

Transport Layer

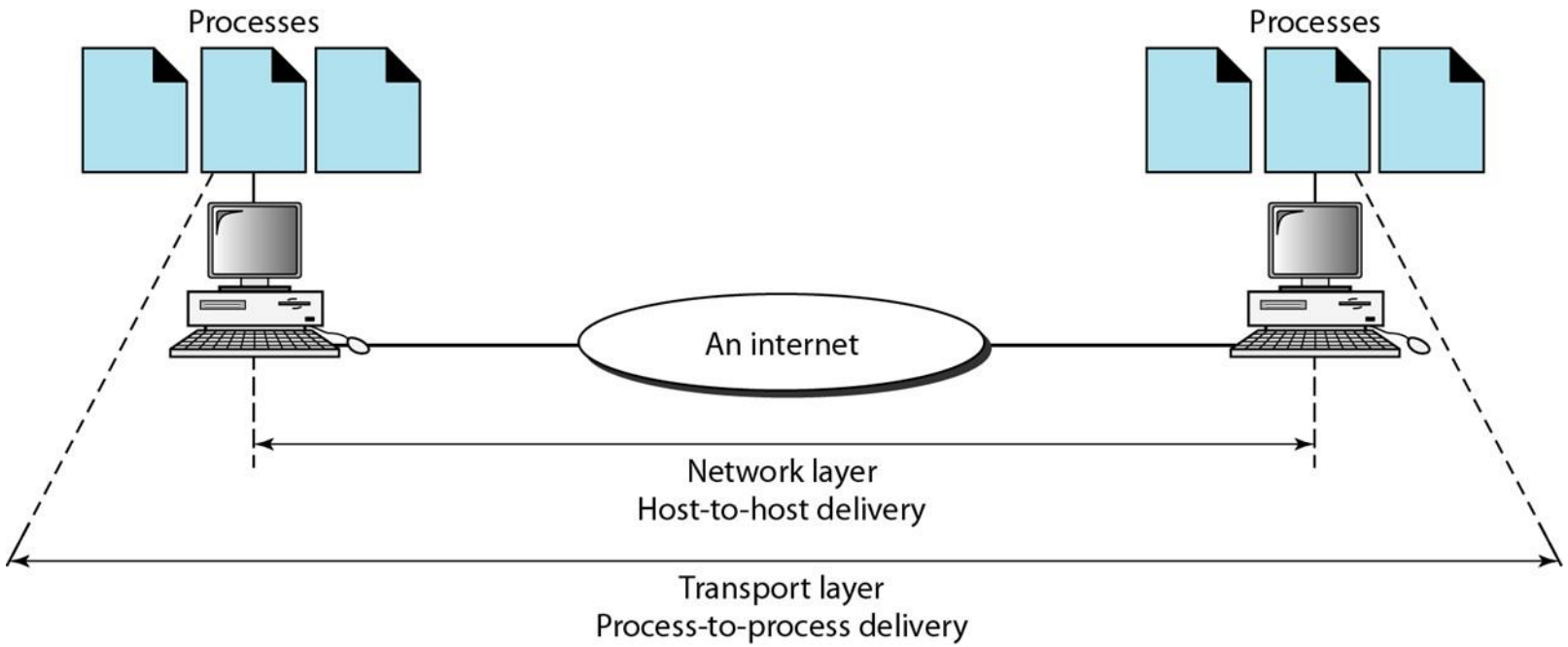
Responsibilities of transport layer:

- *Connection control: Connection-less or connection-oriented.*
- *Flow control : flow control at this layer is performed end to end rather than across a single link.*
- *Error control: error control at this layer is performed process-to-process rather than across a single link.*

Transport Layer



Reliable process-to-process delivery of a message



Session Layer

- The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes.
- The session layer defines how to start, control and end conversations (called sessions) between applications.
- It provides coordination of the communication in an ordering manner.

Session Layer

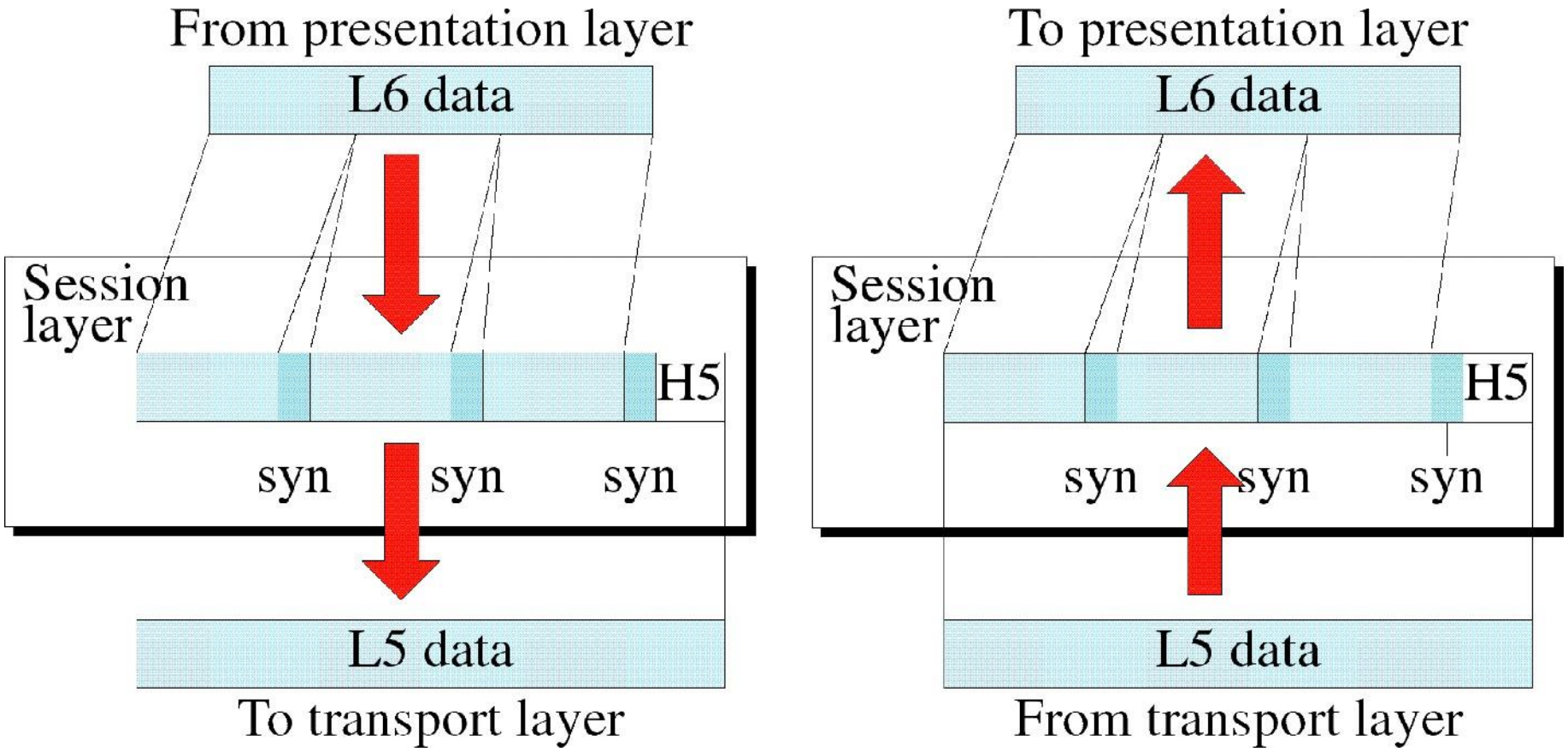
- The session layer offers provisions for efficient data transfer.

Responsibilities of the session layer:

- *Dialog control* : The session layer allows two systems to enter into a dialog.

- *Synchronization*: allows to add checkpoints.

Session Layer



Presentation Layer

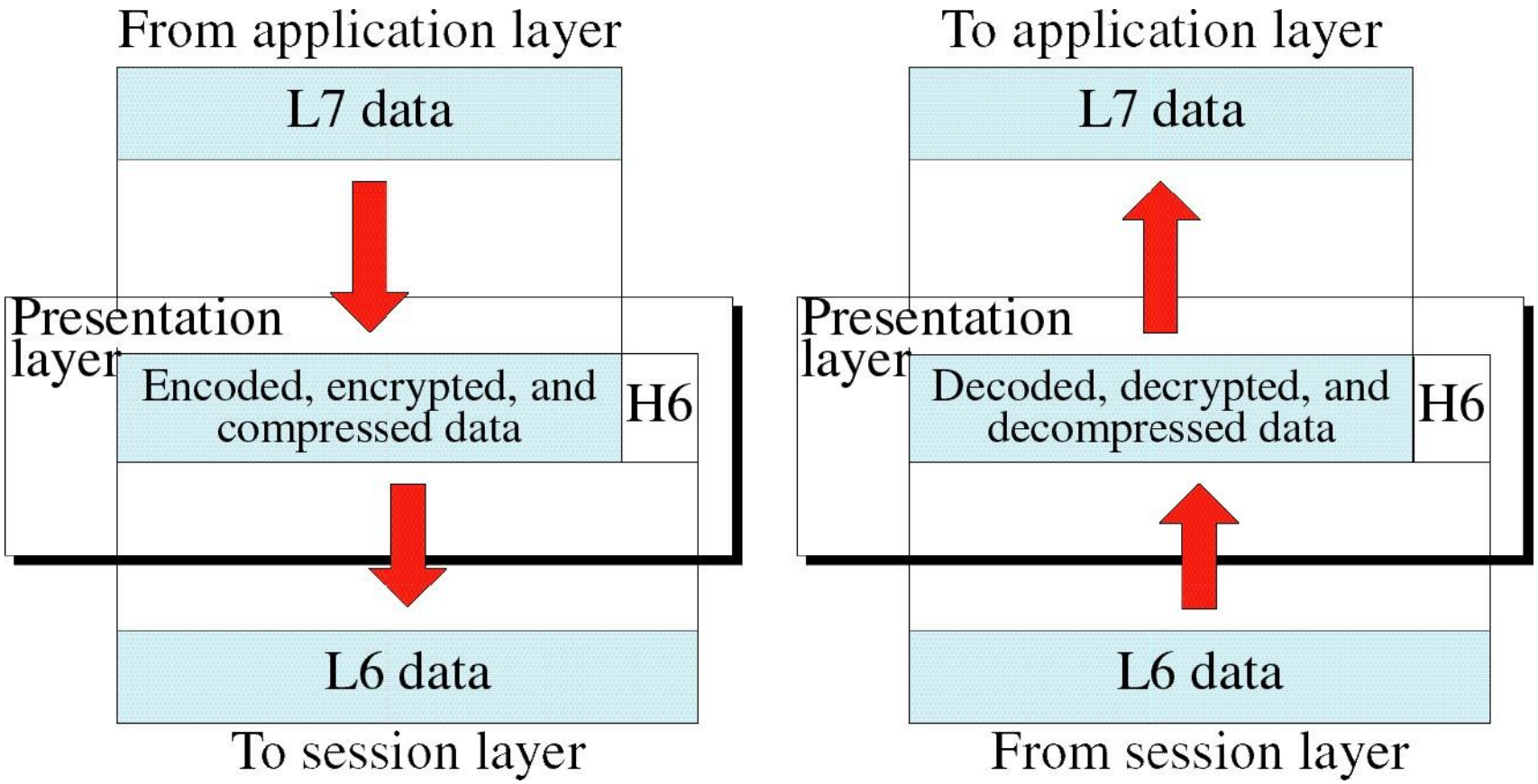
- The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system.
- If necessary, the presentation layer translates between multiple data formats by using a common format.
- The presentation layer basically allows an application to read (or understand) the message.

Presentation Layer

Responsibilities of presentation layer:

- *Translation*: Changes data so that another computer can read it.
- *Compression*: Makes data smaller to move data in same amount of time.
- *Encryption*: Encodes data to protect from interception.

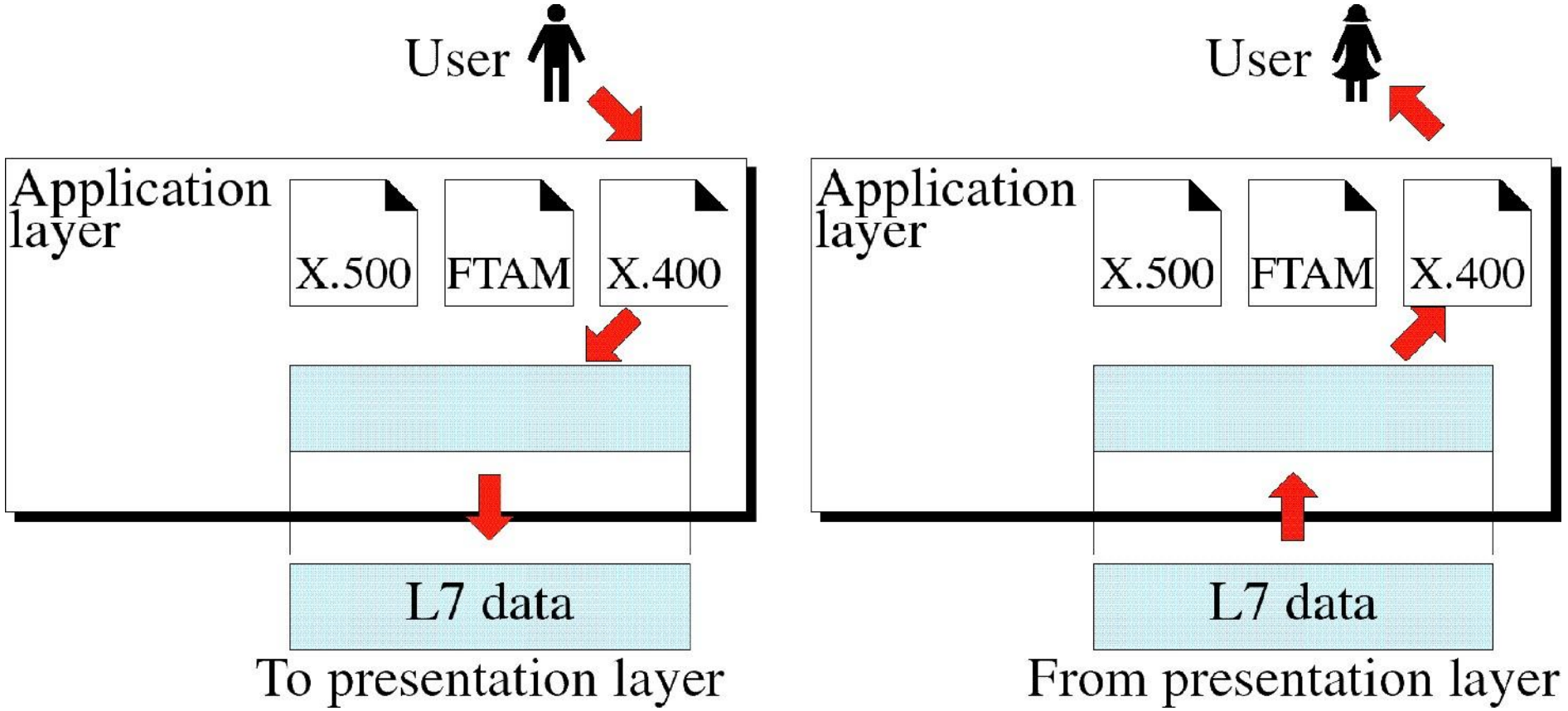
Presentation Layer



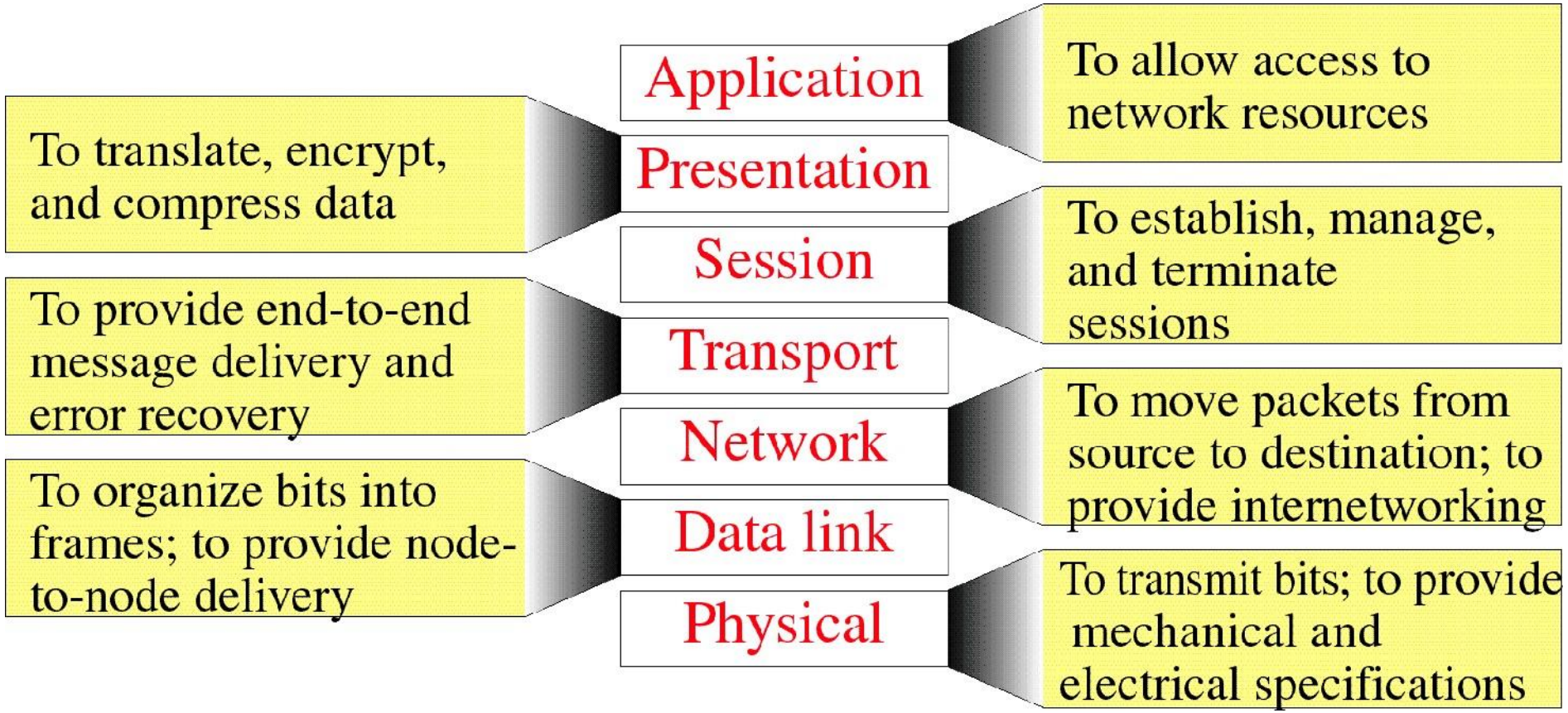
Application Layer

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support – email, shared database , access to remote file etc.
- It differs from the other layers in that it does not provide services to any other OSI layer, but rather, only to applications outside the OSI model.

Application Layer



Summary of Layer Functions

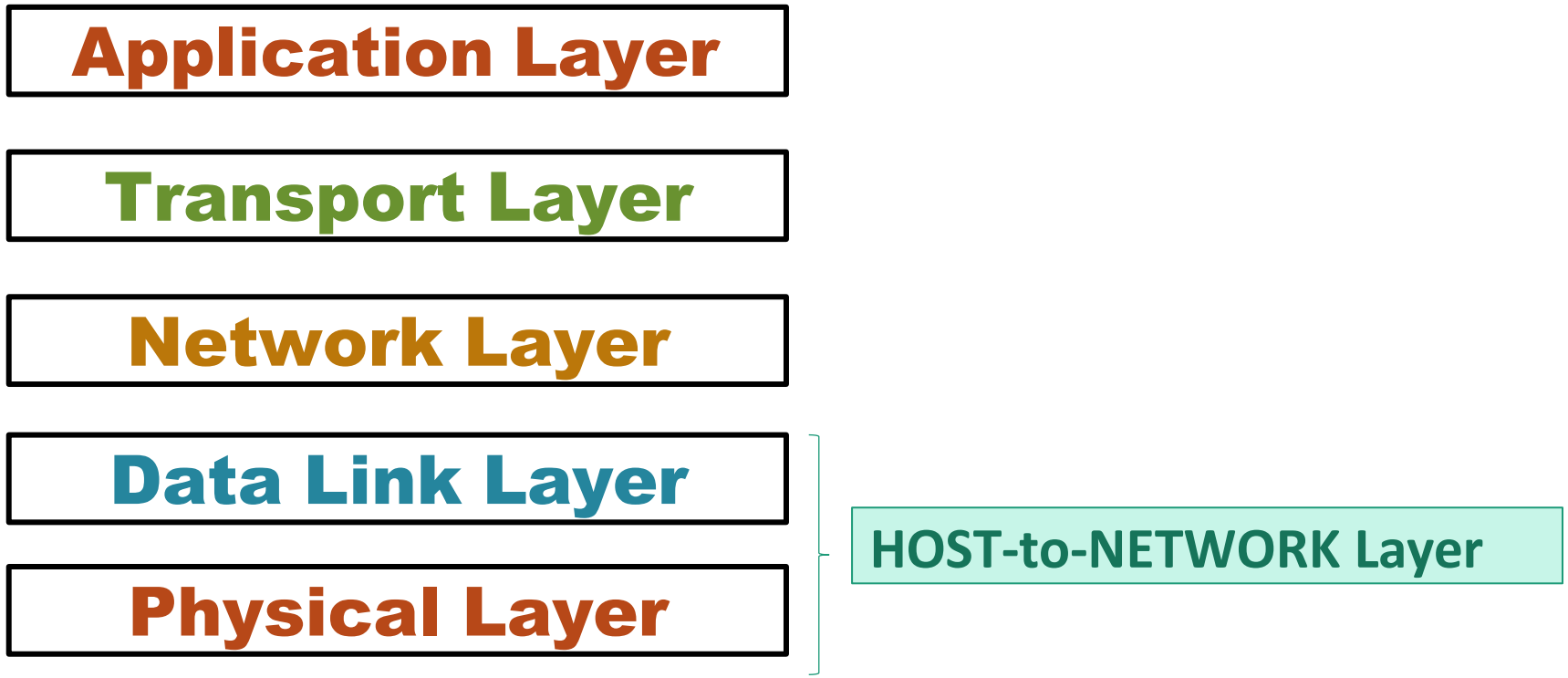


TCP/IP Model

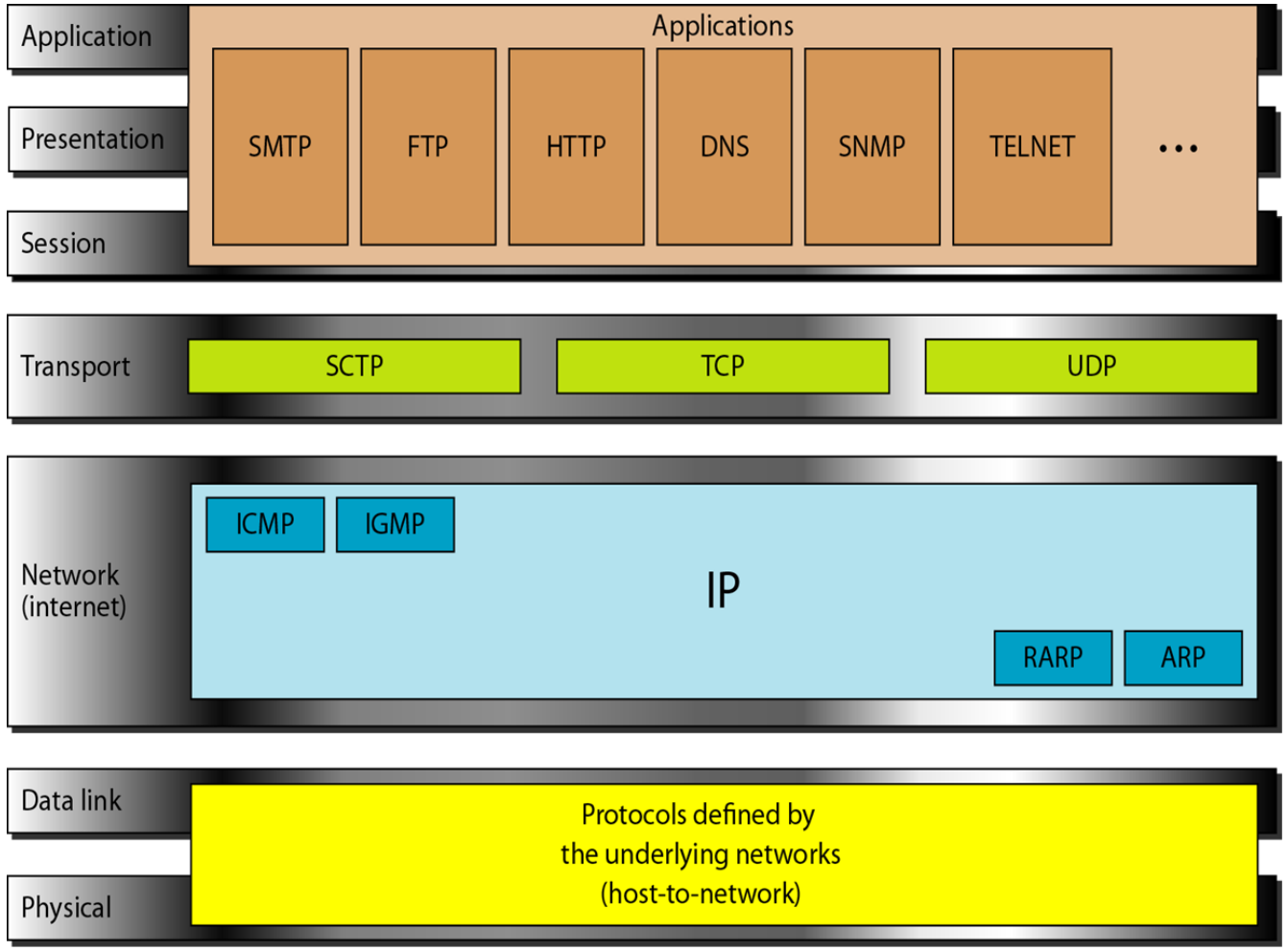
- Developed prior to OSI model
- TCP/IP is a hierarchical protocol made up of interactive modules, each providing specific functionality, but they are not interdependent

TCP/IP PROTOCOL SUITE

- TCP/IP protocol suite is made of five layers:



TCP/IP PROTOCOL SUITE



Network Layer

- TCP/IP does not support any specific protocol
- All standard and proprietary protocols supported at this level.
- At this level TCP/IP supports Internetworking protocol(IP).

IP in turn uses 4 supporting protocols.

- ARP
- RARP
- ICMP
- IGMP

Network Layer

- **Internetworking Protocol (IP)**
  - ✓ IP is transmission mechanism used by TCP/IP
  - ✓ Unreliable and connection-less protocol- *best effort delivery*
  - ✓ No error checking or tracking.
  - ✓ Transports data in packets called *datagrams*.
  - ✓ Does not keep track of routes and no facility reordering.

Network Layer

Address Resolution Protocol (ARP)

- Associates logical address with physical address.
- ARP is used to find physical address of node when logical address is known.

Reverse Address Resolution Protocol (RARP)

- RARP is used to find logical address of node when physical address is known.
- Usually used when computer is connected to network for the first time.

Network Layer

Internet Control Message Protocol (ICMP)

- Used by hosts and gateways to send notification of datagram problem to sender.

Internet Group Message Protocol (IGMP)

- Used to facilitate simultaneous transmission of message to group of recipients.

Transport Layer

- IP is host to host protocol

Transport layer has three protocols:

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

Transport Layer

User Datagram Protocol (UDP):

- Process to Process
- Adds only port address , error control , checksum etc. to data from upper layers.

Transport Layer

Transmission Control Protocol (TCP)

- Reliable stream protocol.
- Data is divided into segments.
- Segment contain sequence number for reordering.
- At receiving end , TCP collects each datagram and reorders it based on sequence numbers

Stream Control Transmission Protocol (SCTP)

- Combines features of TCP and UDP

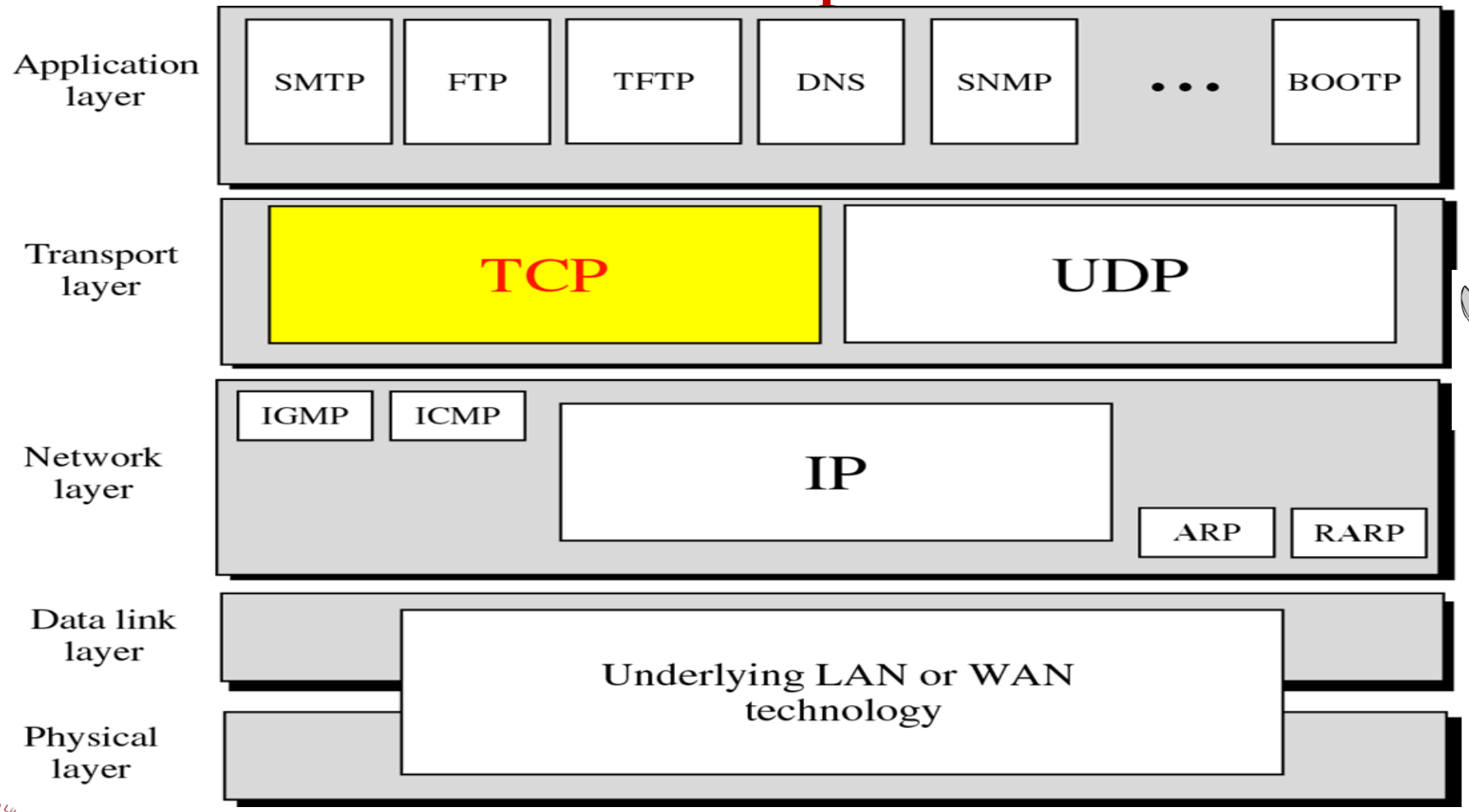
TCP Connection Oriented

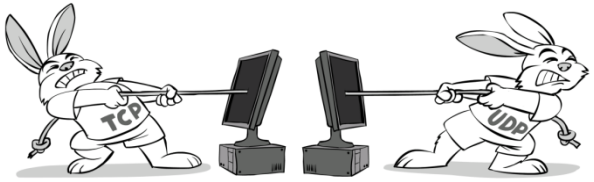
- Usual transport layer is Transmission Control Protocol
  - Reliable connection
- Connection
  - Temporary logical association between entities in different systems
- TCP PDU
  - Called TCP segment
  - Includes source and destination port (Service Access Point (SAP))
    - The SAP is a conceptual location at which one OSI layer can request the services of another OSI layer.
    - Identify respective users (applications)
    - Connection refers to pair of ports
- TCP tracks segments between entities on each connection

UDP- Connection Less

- Alternative to TCP is User Datagram Protocol
- Not guaranteed delivery
- No preservation of sequence
- No protection against duplication
- Minimum overhead
- Adds port addressing to IP

TCP/IP protocol suite





SOMAIYA VIDYAVIHAR UNIVERSITY

Somaiya TRUST

Differences between TCP and UDP

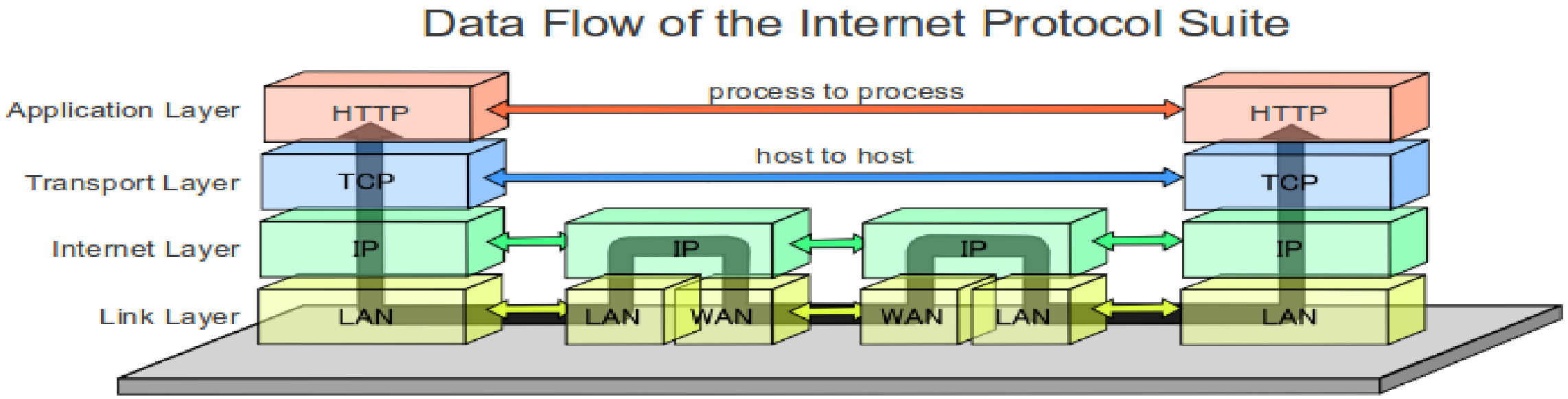
TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

UDP & TCP were primarily designed for data. But popularity of carrying Voice over IP networks forced engineers to design a new transport layer protocol called **SCTP** (**Stream Control Transmission Protocol**).

Inventors of the TCP

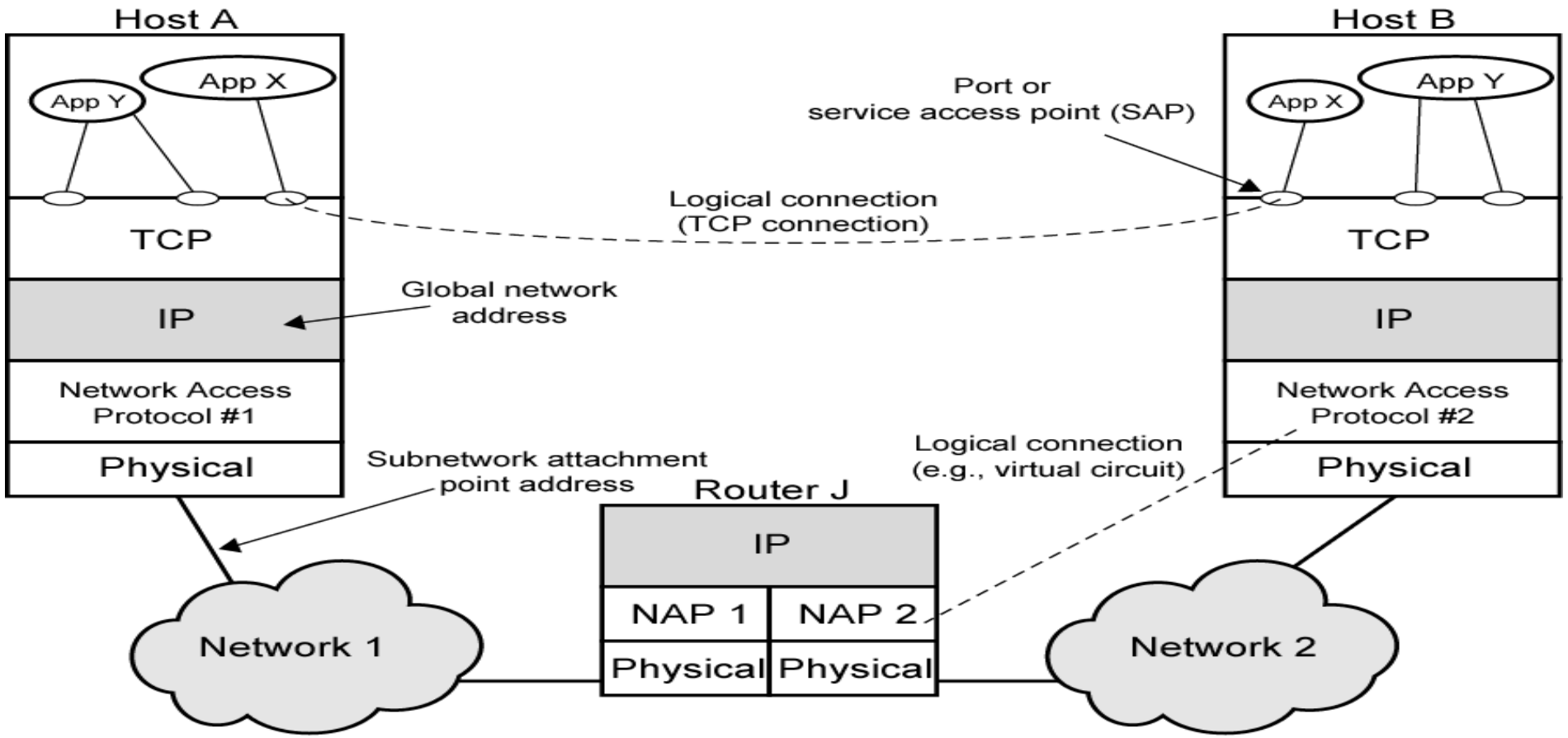
In May, 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper titled "A Protocol for Packet Network Interconnection." The paper's authors -- Vinton Cerf and Robert Kahn -- described a protocol called "TCP" that incorporated both connection-oriented and datagram services.

Transferring data in accordance with the TCP/IP stack.



https://commons.wikimedia.org/wiki/File:Data_Flow_of_the_Internet_Protocol_Suite.PNG

TCP/IP Concepts



SOMAIYA VIDYAVIHAR UNIVERSITY

Somaiya TRUST

Important Points

Data deliveries

The transport layer is responsible for process-to-process delivery.

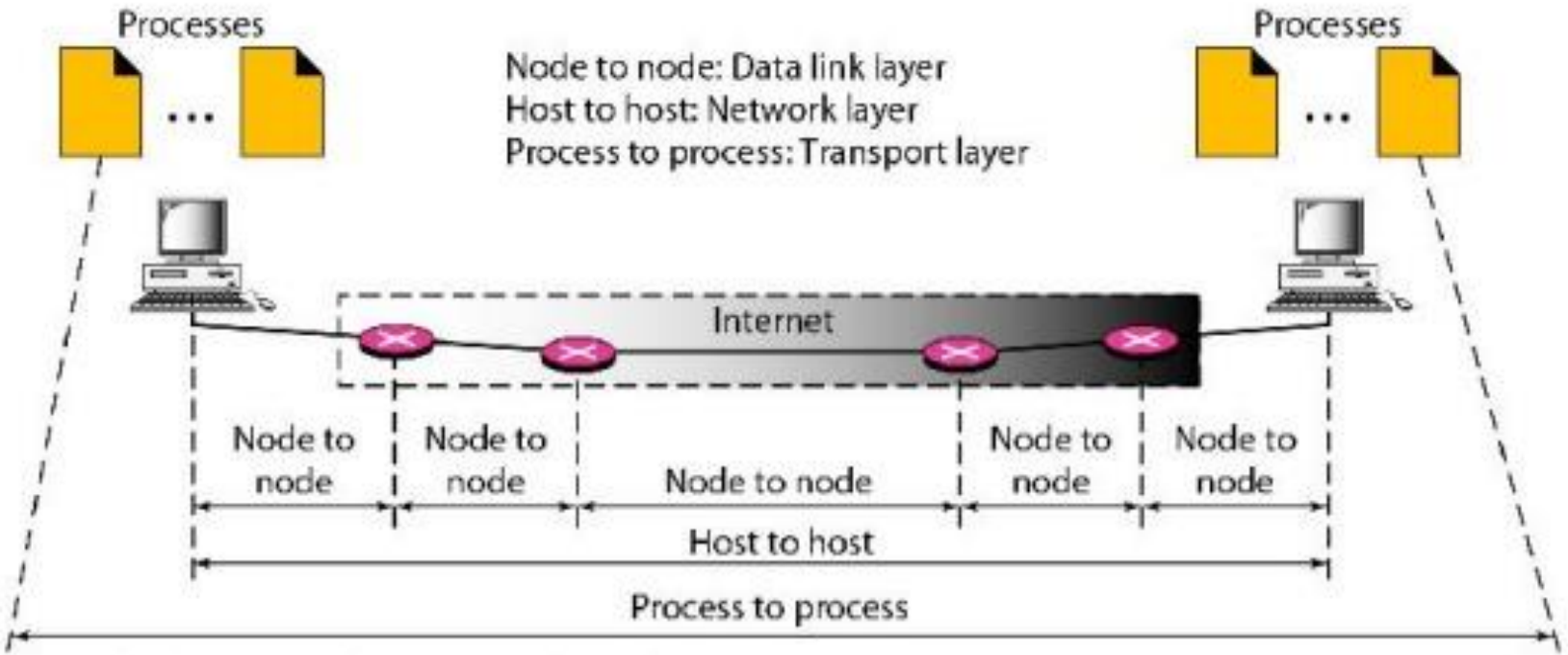


Figure 4.1 Types of data deliveries

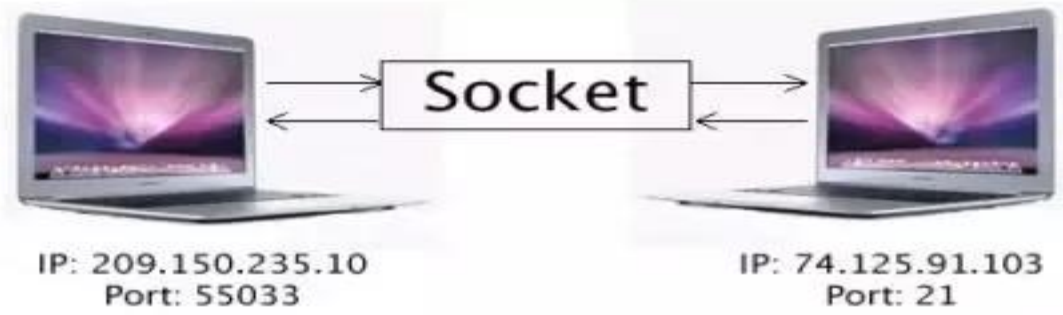
Addressing We learned till now

- Physical Address- MAC
- Logical Address-IP
- **Port Address-** Internet Port 443

✓ This port is used for secure web browser communication.

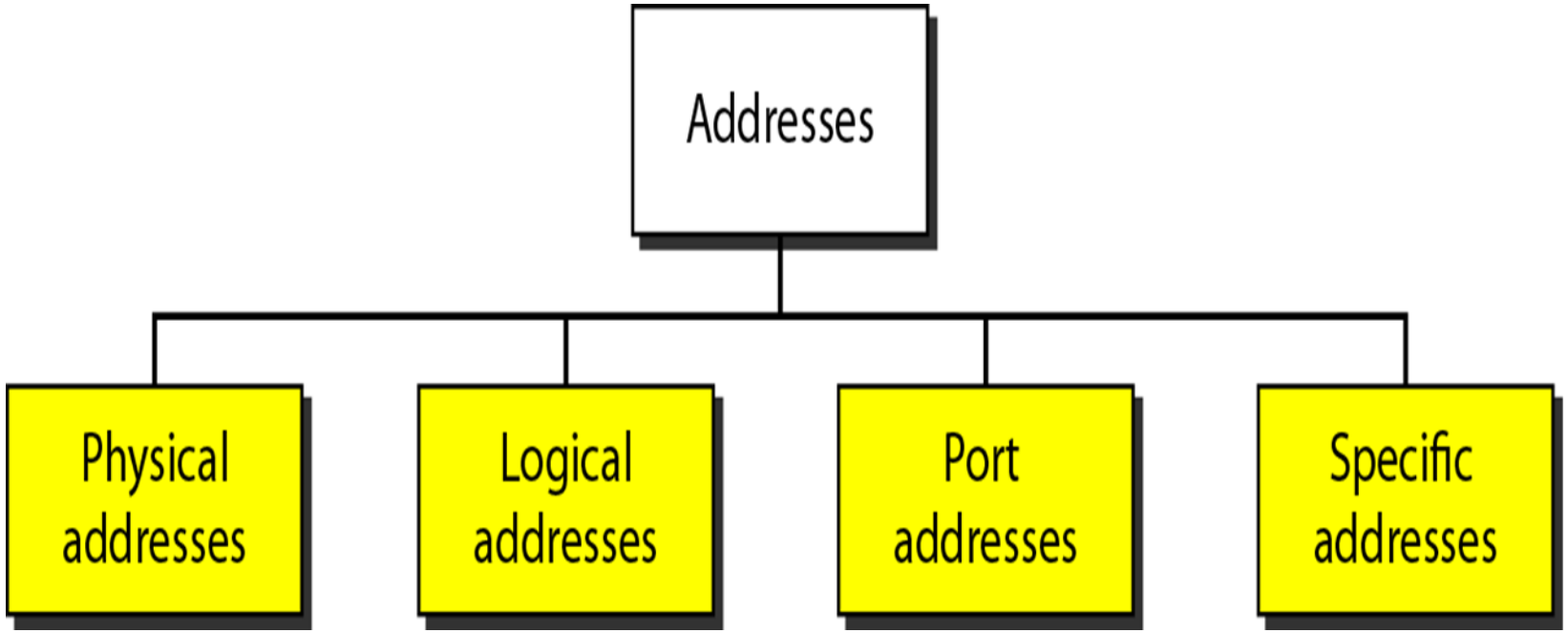
✓ Sockets are created and used with a set of programming requests or "**function calls**" sometimes called the sockets application programming interface (API). The most common sockets API is the Berkeley UNIX

Socket

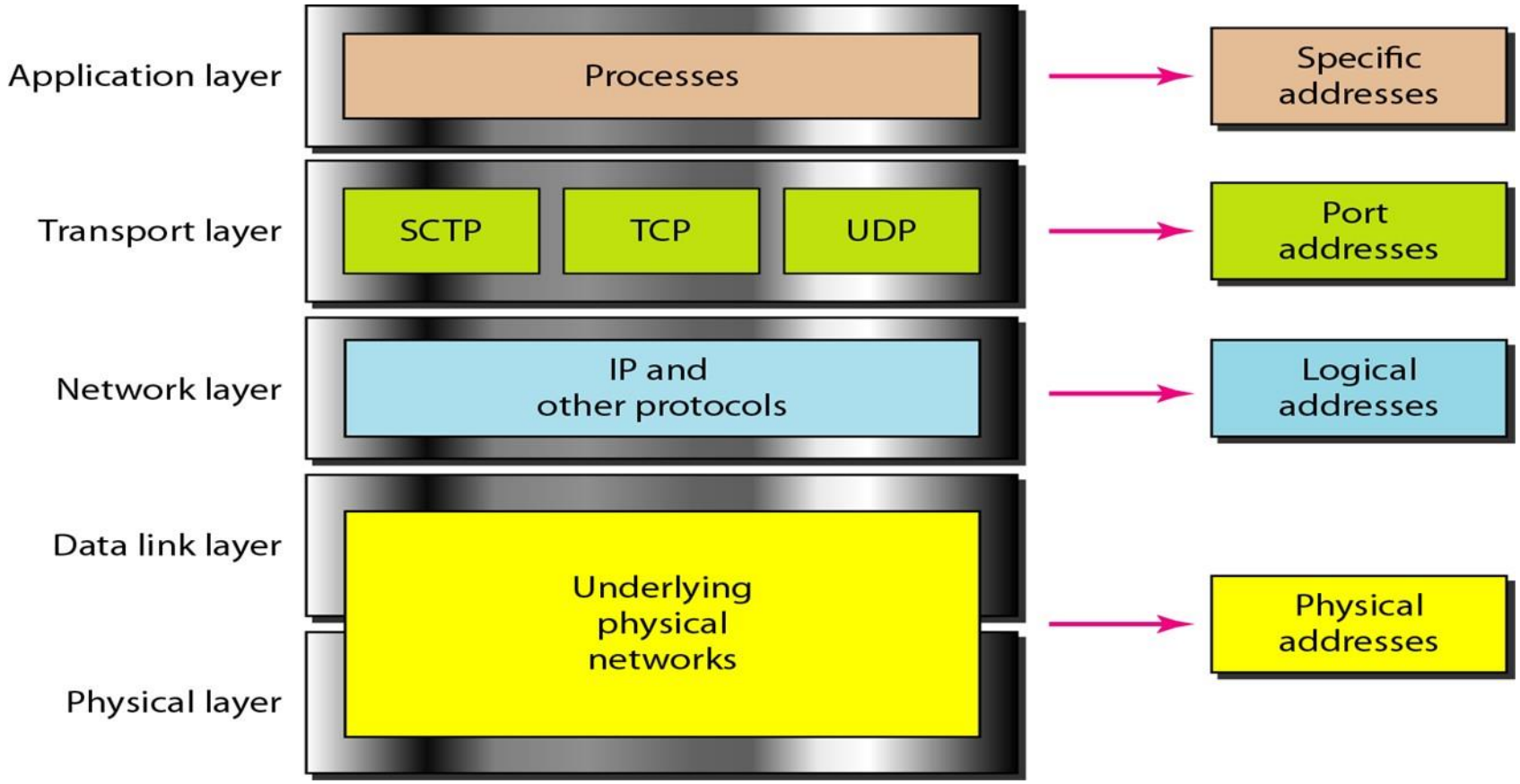


Ref.: https://www.quora.com/What-is-a-socket-in-computer-networks

Addressing

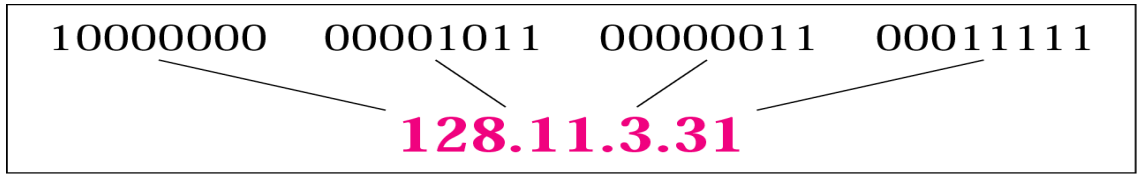


Relationship of layers and addresses in TCP/IP



IP

- ***An IP address is a 32-bit address***
- ***The IP addresses are unique and universal.***

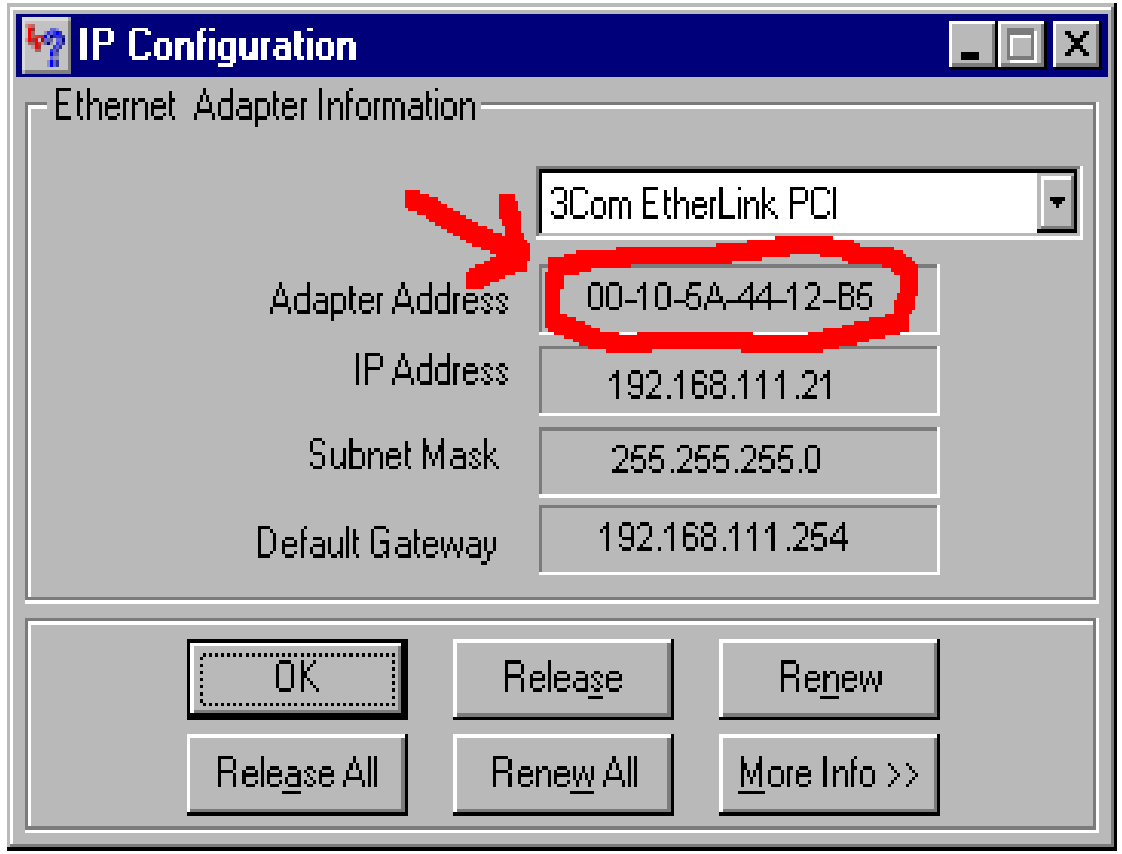


- **Logical Address is** generated by CPU while a program **is** running.
- **Physical Address** identifies a **physical** location **of** required data **in a** memory. ...
- **The** user never directly deals with **the physical address** but can access by its corresponding **logical address**.

Logical Vs Physical Address

BASIS OF COMPARISON	LOGICAL ADRESS	PHYSICAL ADRESS
Description	Logical address is the address that is generated by the central processing unit (CPU) in perspective of a program. Logical address can also be referred to as a virtual address.	Physical address is a location that exists in the memory; it allows accessing a particular storage cell in the main memory.
Address Space	Logical address space is the set of all logical addresses generated by CPU for a program.	Physical address space is the set of all physical address mapped to corresponding logical addresses.
Visibility	The logical address exists virtually and does not have a specific location to exist physically in memory unit hence it is also known as virtual address.	The physical address is an accessible physical location existing within the memory.
Generation	The logical address is generated by the central processing unit (CPU).	Physical address is computed by Memory Management Unit (MMU).
Use	The physical address helps to identify a location in the main memory.	The logical address helps to obtain the physical address.
Flexibility	The logical address is flexible hence will keep changing with the system from time to time.	Physical address of the object always remains constant.
User	The user program can use the logical address to access the physical address.	The user program does not have the ability to view the physical address directly.
Rebooting	Logic address is erased when the system is rebooted.	Physical address is not affected when the system is rebooted.
Example	192.168.20.2(IPV4/IPV6)	00-10-5A-44-12--B5 (48 bit,6 byte)

Logical Vs Physical Address



Reference: https://www.google.com/search?q=mac+address+example&tbm=isch&source=iu&ictx=1&fir=AcSg14XEihOvxM%252CbH_OqFLfsM5BxM%252C_&vet=1&usg=AI4_-kQDktfJgXu0c

SOMAIYA VIDYAVIHAR UNIVERSITY

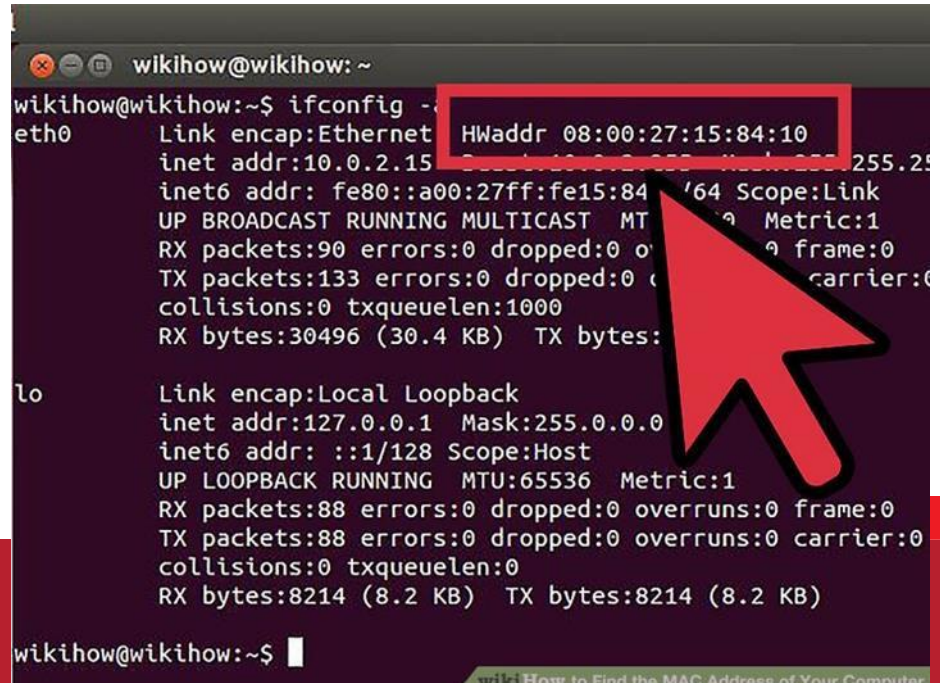
Somaiya TRUST

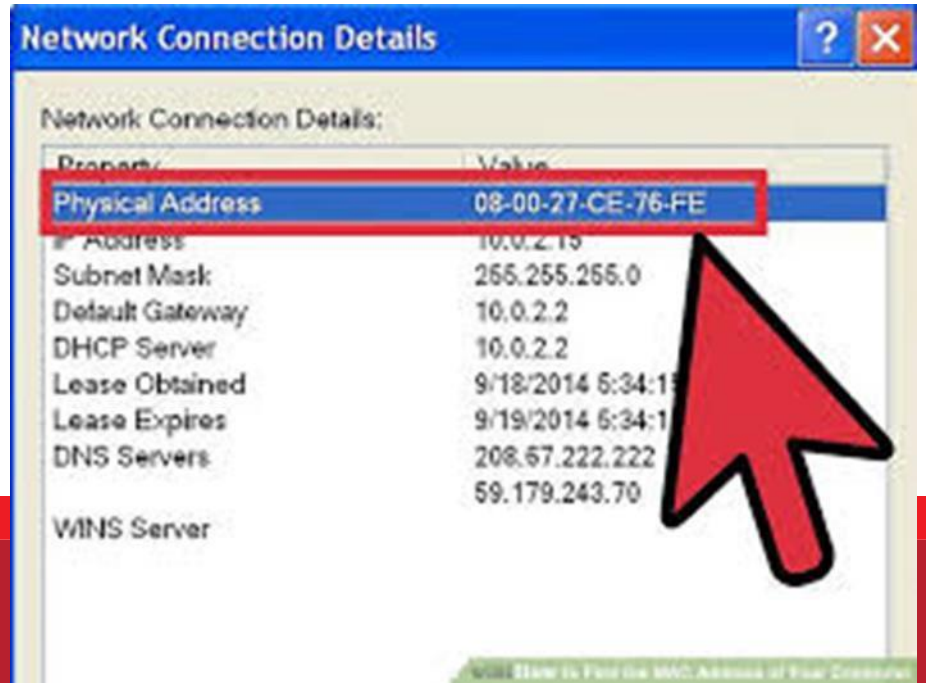
MAC Address

Example MAC Address

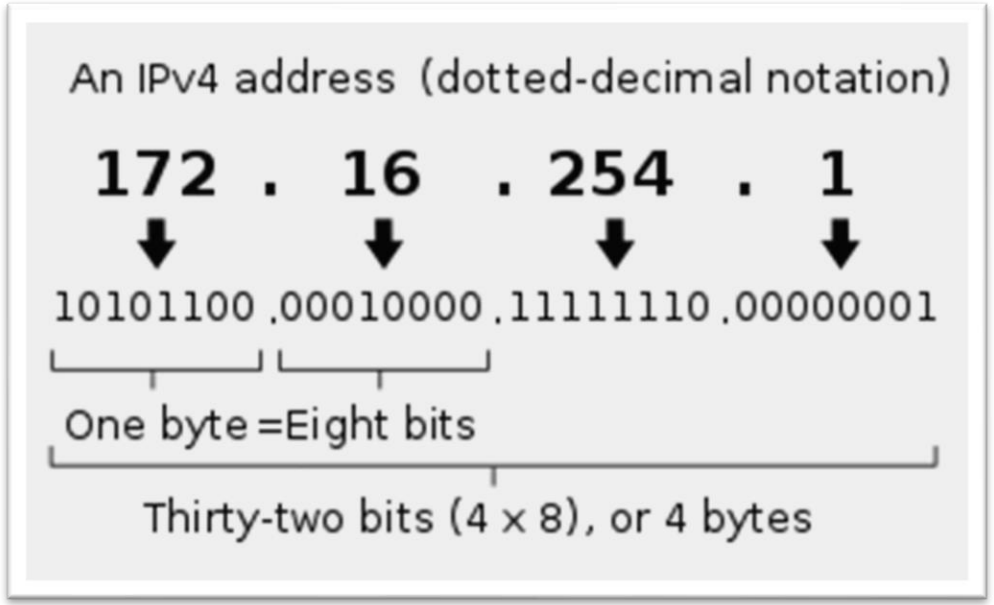
3A-34-52-C4-69-B8

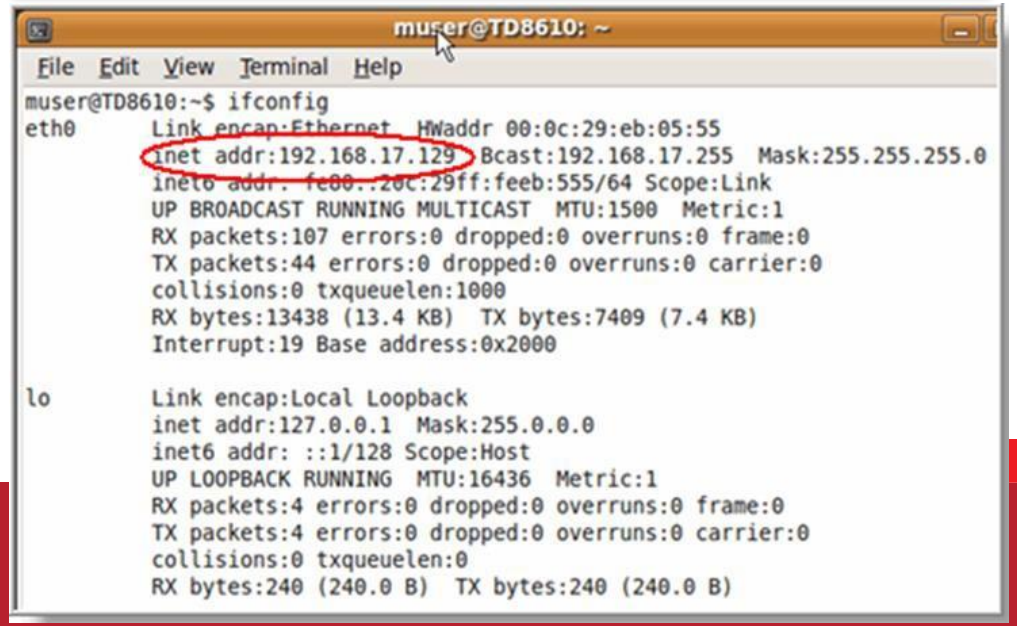
Organizationally Unique Identifier (OUI)	Network Interface Controller (NIC)

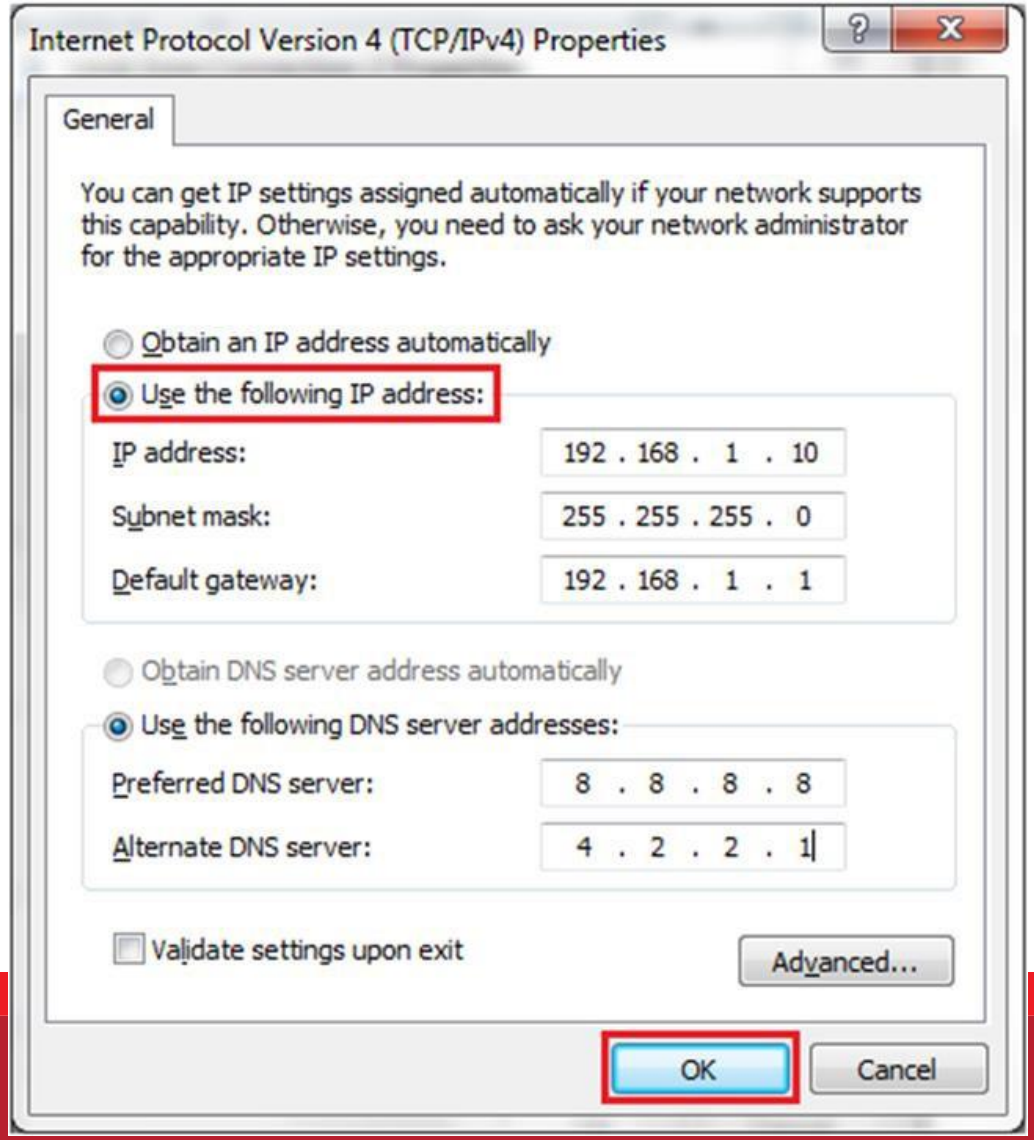




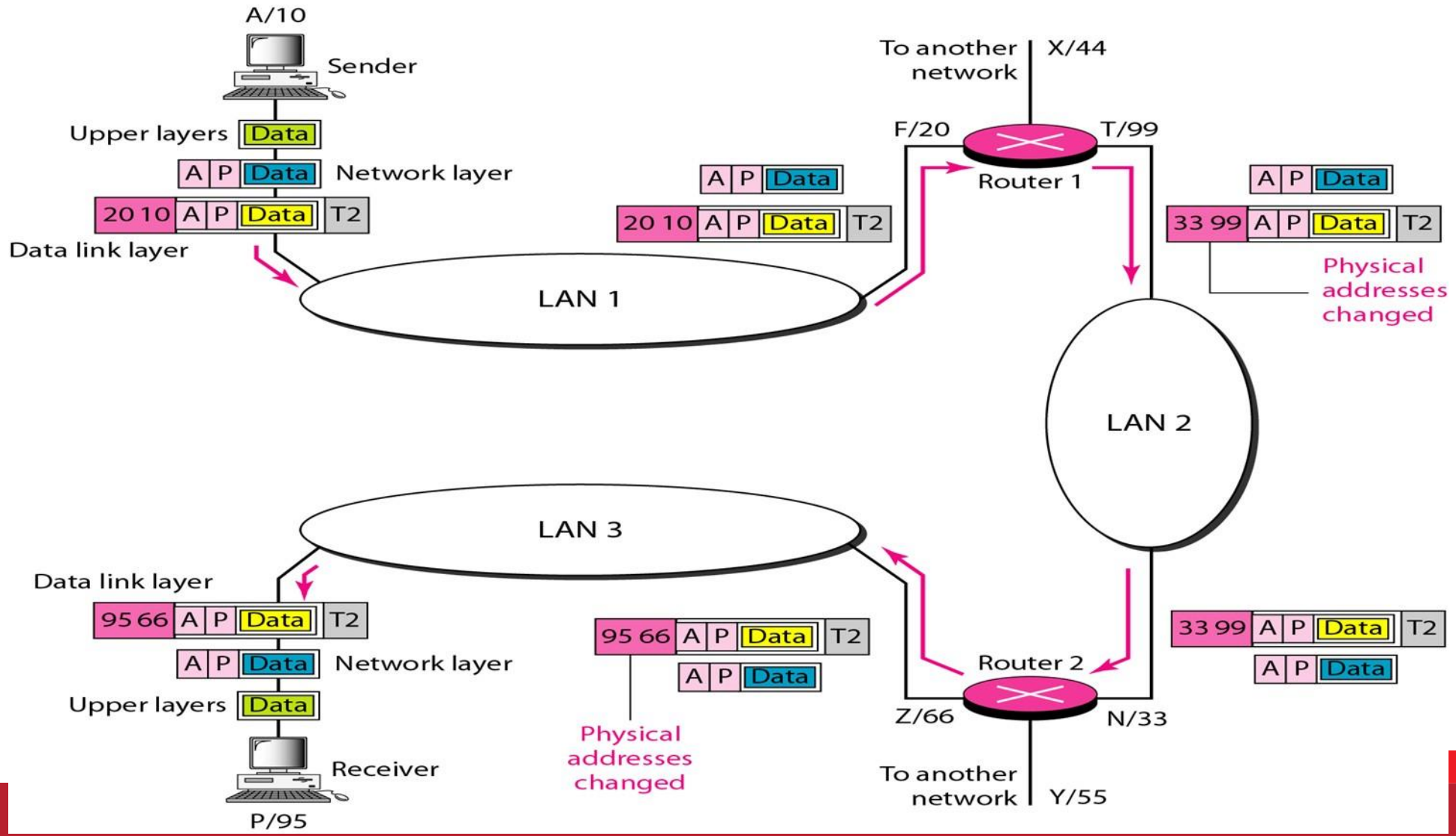
IP Address


An IPv4 address (dotted-decimal notation)
172 . 16 . 254 . 1
10101100.00010000.11111110.00000001
One byte =Eight bits
Thirty-two bits (4 x 8), or 4 bytes


muser@TD8610: ~
File Edit View Terminal Help
muser@TD8610:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:eb:05:55
inet addr:192.168.17.129 Bcast:192.168.17.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:feeb:555/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:107 errors:0 dropped:0 overruns:0 frame:0
TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:13438 (13.4 KB) TX bytes:7409 (7.4 KB)
Interrupt:19 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:4 errors:0 dropped:0 overruns:0 frame:0
TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:240 (240.0 B) TX bytes:240 (240.0 B)


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: 4 . 2 . 2 . 1
Validate settings upon exit
Advanced...
OK
Cancel

Addresses (Example)



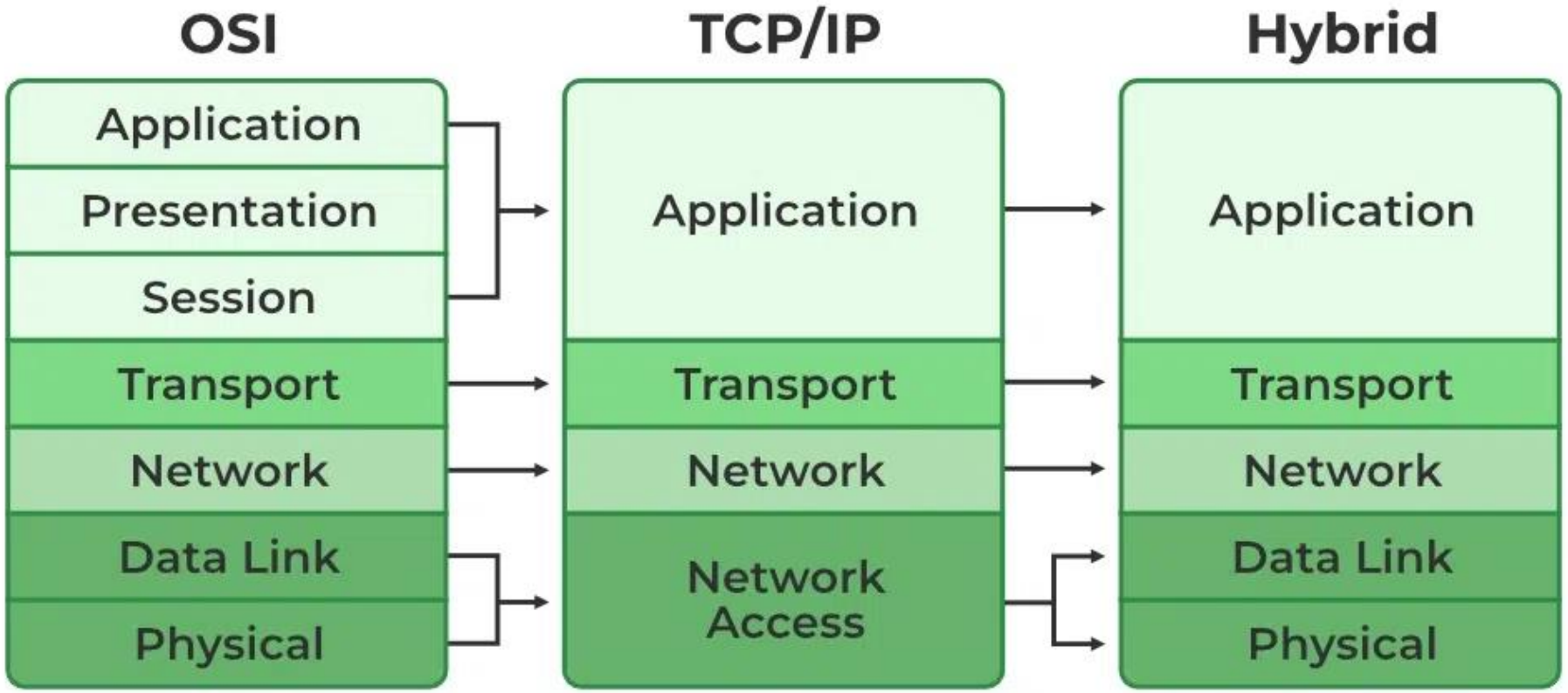
Difference Between OSI and TCP/IP

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard

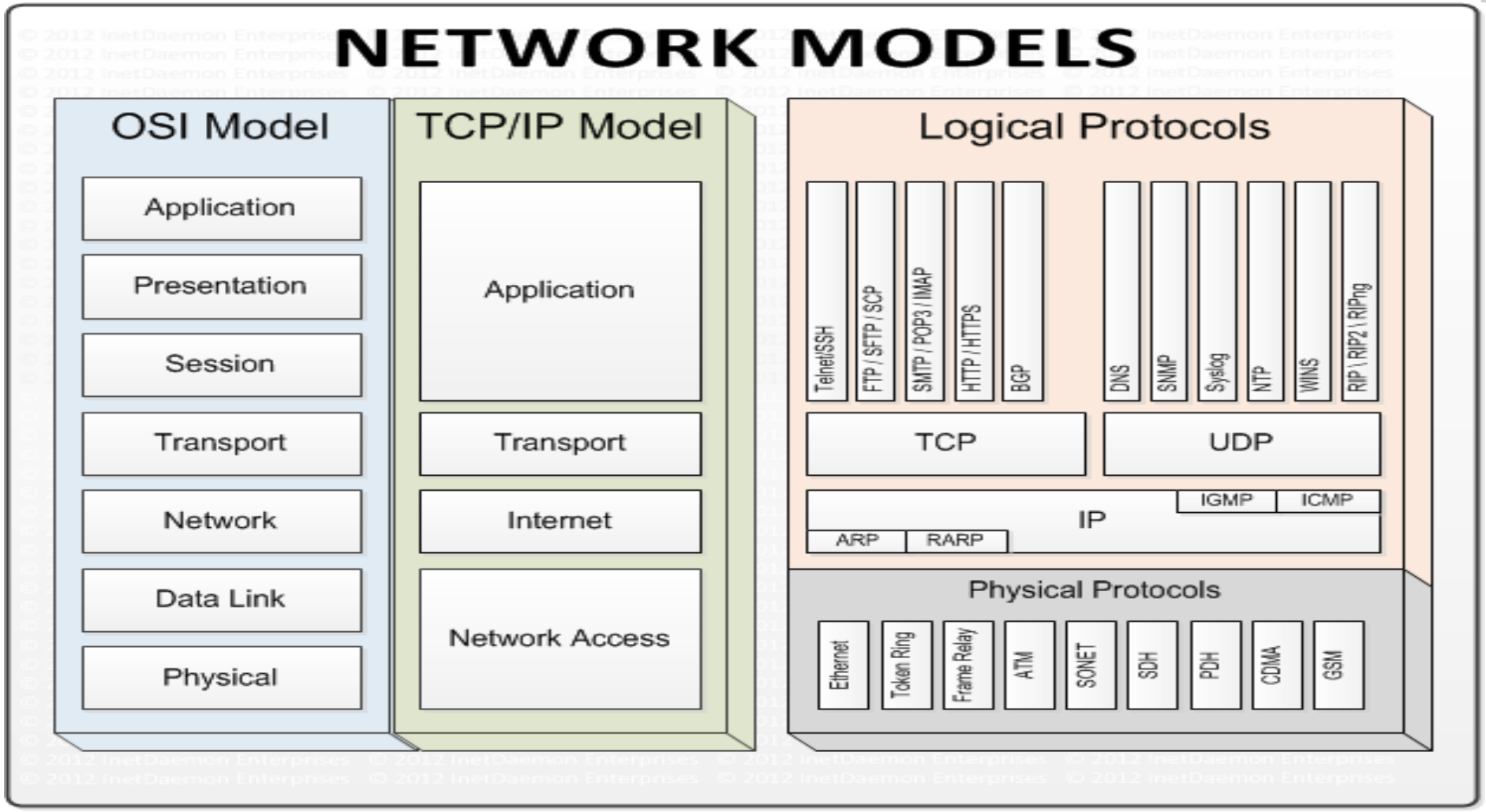
Figure 5: Differences between OSI and TCP/IP Model [28].

16. Conclusion

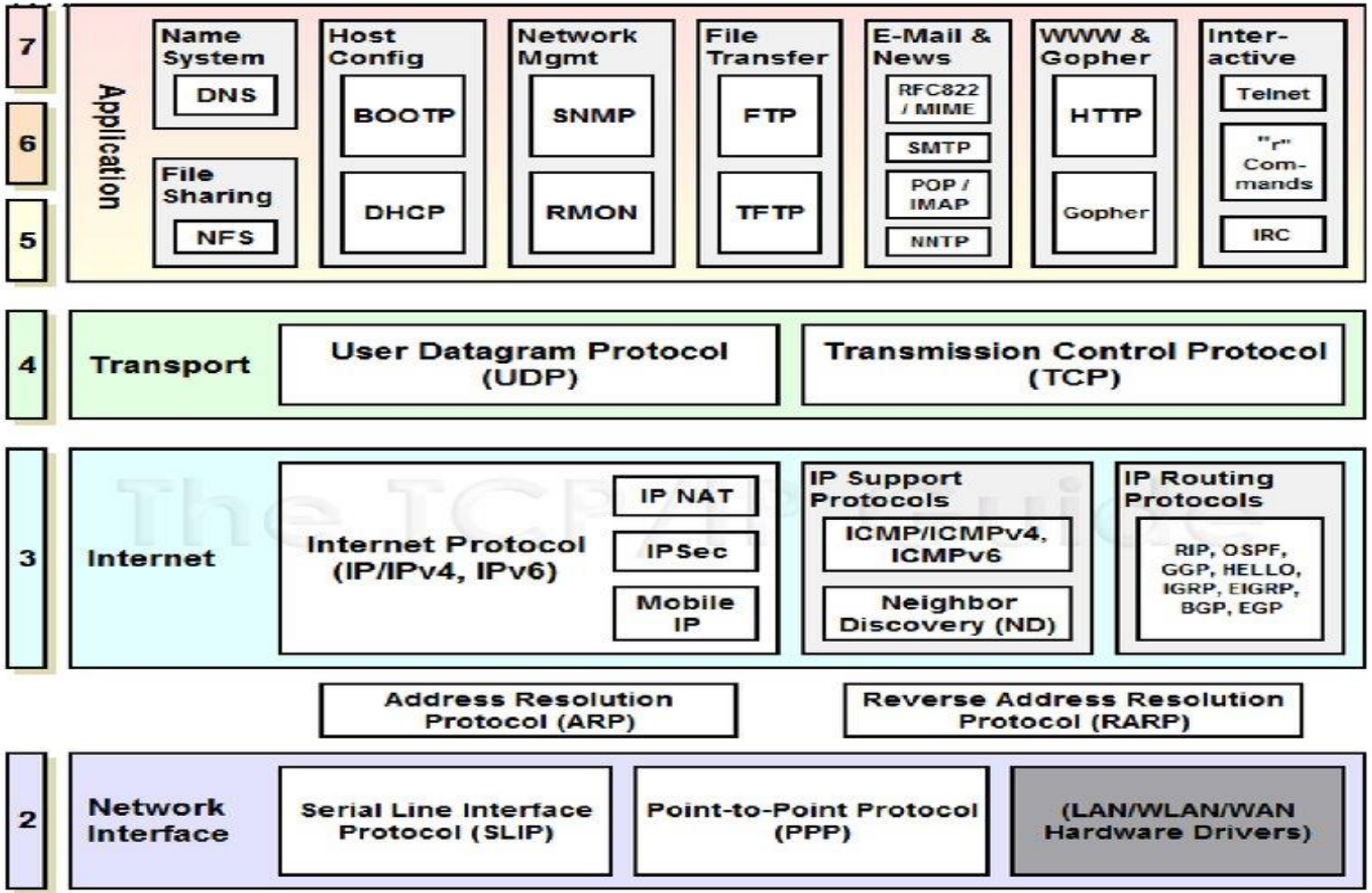
Difference Between OSI and TCP/IP



Difference Between OSI and TCP/IP



TCP/IP Protocols



References

- “Data Communication and Networking”, Behrouz Forouzan 5e
- “TCP/IP Protocol Suite “, Behrouz Forouzan 4e.
- “Computer Networks “, A.S.Tanenbaum 5e.
- https://ppt-online.org/89029
- Internet Images