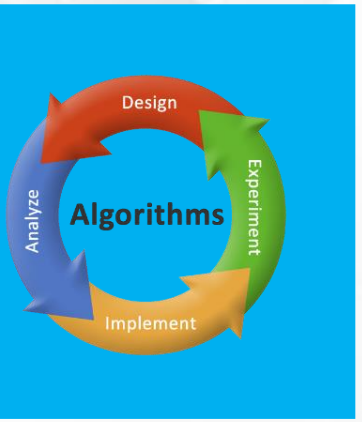
Computer Networks
(CN) CTMTCSE SIV P2

Syllabus and Establishment of this Subject



Dr. Vijeta Khare

Syllabus
and Books

CTMTCSE SIV P2: Computer Networks

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE						
					Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

- To learn about data communication
- To learn about the network devices and its functionality.
- To learn the services running on various network layers.
- To learn the network topologies and their implementation.
- To understand routing protocols.

- **UNIT – I**
- **Data Communication**
- **Data and Signals:** Analog and Digital, Periodic Analog Signals, Digital Signals, performance, **Digital Transmission:** Digital to Digital and Analog to Digital Conversion, Transmission Modes, Analog Transmission. **Bandwidth Utilization:** Multiplexing, Spread Spectrum.
- **UNIT – II**
- **History and Models**
- Introduction, history and development of computer networks and internet, various protocols and standards, network topologies, **Network Categories:** LAN, MAN, WAN, network reference model OSI and TCP/IP protocol suite.
- **UNIT – III**
- **Physical and Link**
- Various transmission media (guided media and unguided media), wireless transmission media, errors in transmission: attenuation, noise. Repeaters. Data Link Layer: Error Detection & Correction Techniques, Elementary Data Link Layer **Protocols:** Simplex, Stop and Wait, Sliding Window Protocol.
- **UNIT – IV**
- **Middle Layer**
- **Medium Access Control sublayer:** channel allocation problem, Multiple Access Protocols: ALOHA, CSMA, CSMA/CA, CSMA/CD, Ethernet, Data link layer switching, VLANs. Networking Devices (hub, switch, bridge, router, gateway, repeater), comparison of network devices, network core (packet switching, circuit switching).
- **UNIT – V**
- **Network Layer**
- Types of Addressing, IPv4 and IPv6 Addressing scheme, Transition from IPv4 to IPv6, IP forwarding, classful and classless addressing (subnet, supernet), NAT, Basics of routing algorithms.

- **Reference Books**
- Computer Network by Andrew S. Tanenbaum and David J. Wetherall, 5th Edition
- Computer Networking- A Top-Down approach (7th edition), Kurose and Ross, Pearson
- Computer Networks- A Top-Down approach, Behrouz Forouzan, McGraw Hill
- TCP/IP Protocol Suite (4th edition), Behrouz Forouzan, McGraw Hill
- Data Communications and Networking By Behrouz A. Forouzan, 5th Edition

Assignment's and practical's

- Are to be done yourself
  - You may discuss the assignments with other students
  - You may help (and get help with) debugging
  - You may *not* give your source code to anyone

Why you should study this course?

Because of Learning:

- How data travel between computers
- You will learn various networking technologies
- Various protocol learning

Because of Importance of the subject:

- Placement in few companies
- Competitive Exams (7% of exam is covered from this subject)

Course Outcome

- Understand the architecture of various networking technologies
- Analyze the requirements of the organization and able to select the appropriate topology and structure of networks.
- Have operational knowledge of managing the networks of organization.
- Design the network for organization with better network efficiency parameters

Pre requisites for this course

- Knowledge of a programming language: C or C++ and basic platform knowledge of Linux
- You should be able to convert high level descriptive algorithm into a working program using C/C++ programming language
- Knowledge of basic mathematics, such as: Basic Discrete mathematics

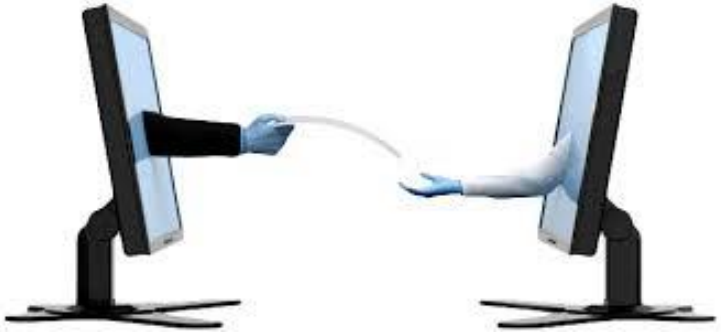
Unit 1

What is Computer Network?

- Computer Network is a system in which multiple computers are connected to each other to share information and resources.

Advantages of Computer Network

File Sharing



Flexible Access

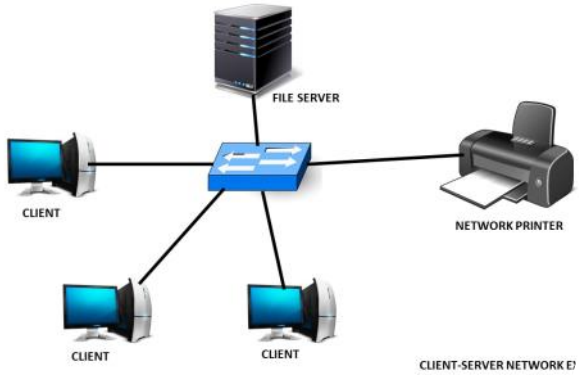
Entertainment

Better Communication

Advantages of Computer Network

Internet Access

Inexpensive System



Instant and Multiple Access

Resource Sharing

Applications of Computer Network

Email Services

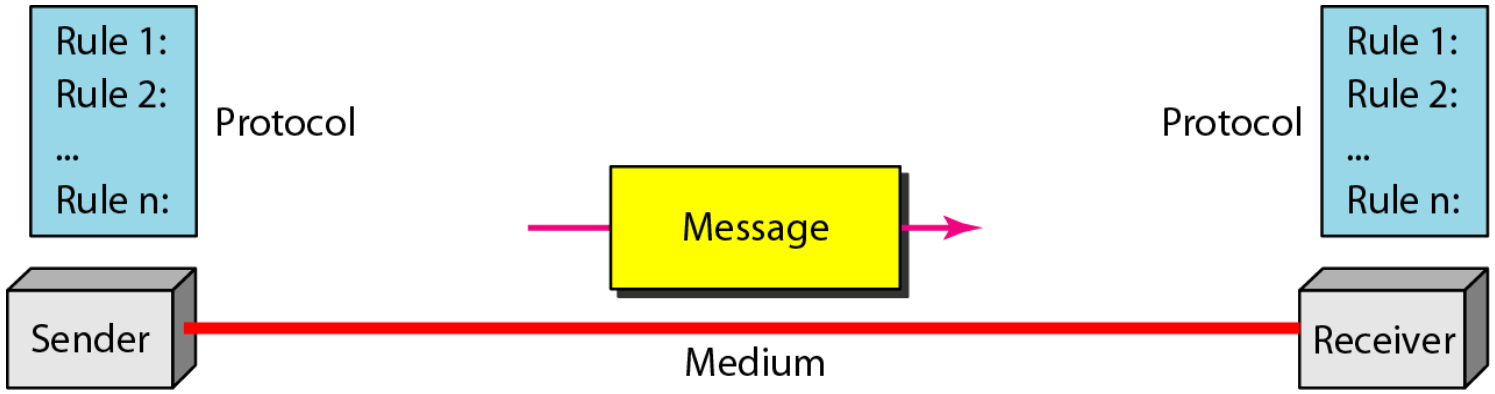
Teleconferencing

Business & Finance

File & Directory Services

& Many More….

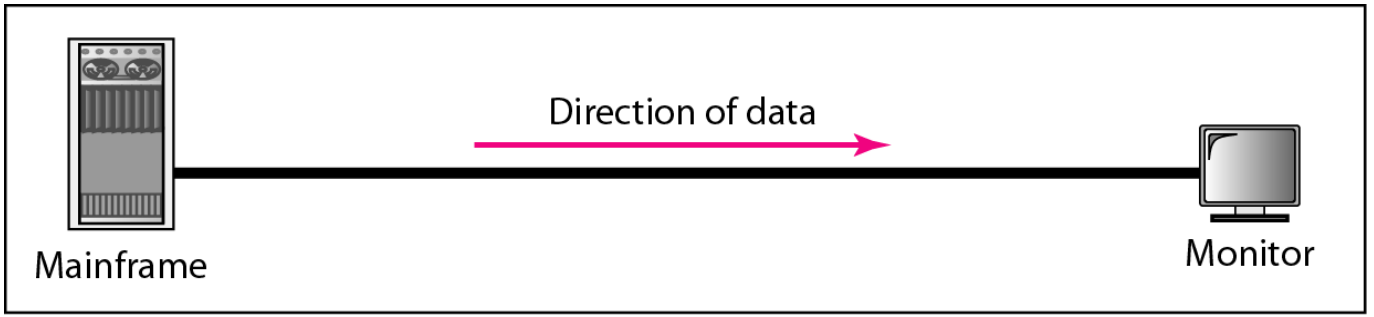
Five Components of Data Communication



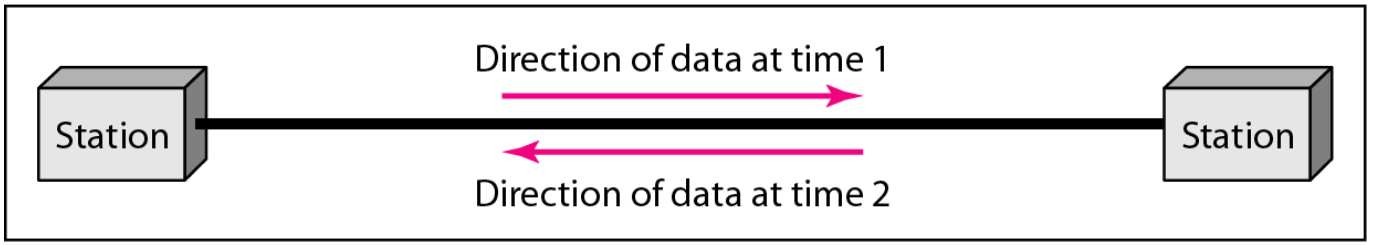
Five Components of Data Communication

- Message:
  - text, number, images, audio, and video
- Sender and Receiver
  - devices that send/receive data message
  - Computer, workstation, telephone, TV, etc.
- Transmission medium
  - Physical path thru which the message travels
- Protocol
  - Set of rules governing data communications

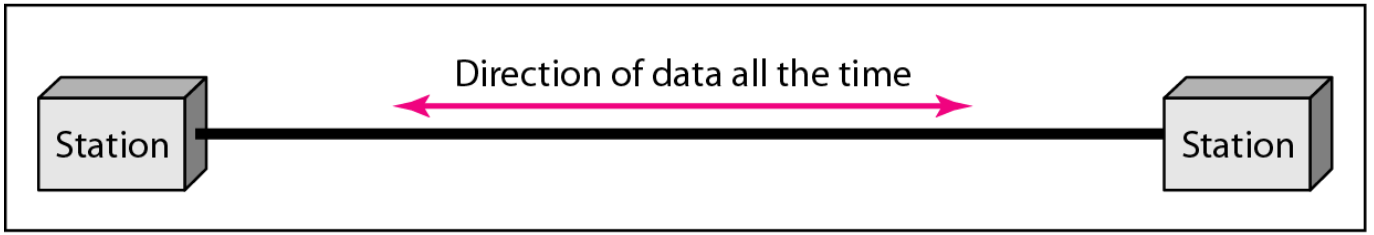
Data flow (simplex, half-duplex, and full-duplex)



a. Simplex



b. Half-duplex



c. Full-duplex

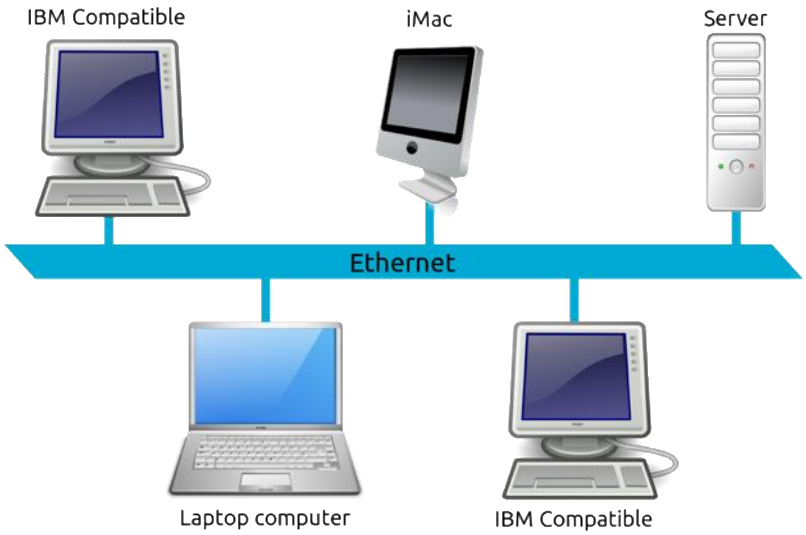
17

Types of Computer Network

- Computer networks can be categories by their size as well as their purpose.
- The size of a network can be expressed by the geographic area.
- Some of the different networks based on size are:
    1. Local Area Network - LAN
    2. Metropolitan Area Network - MAN
    3. Wide Area Network - WAN

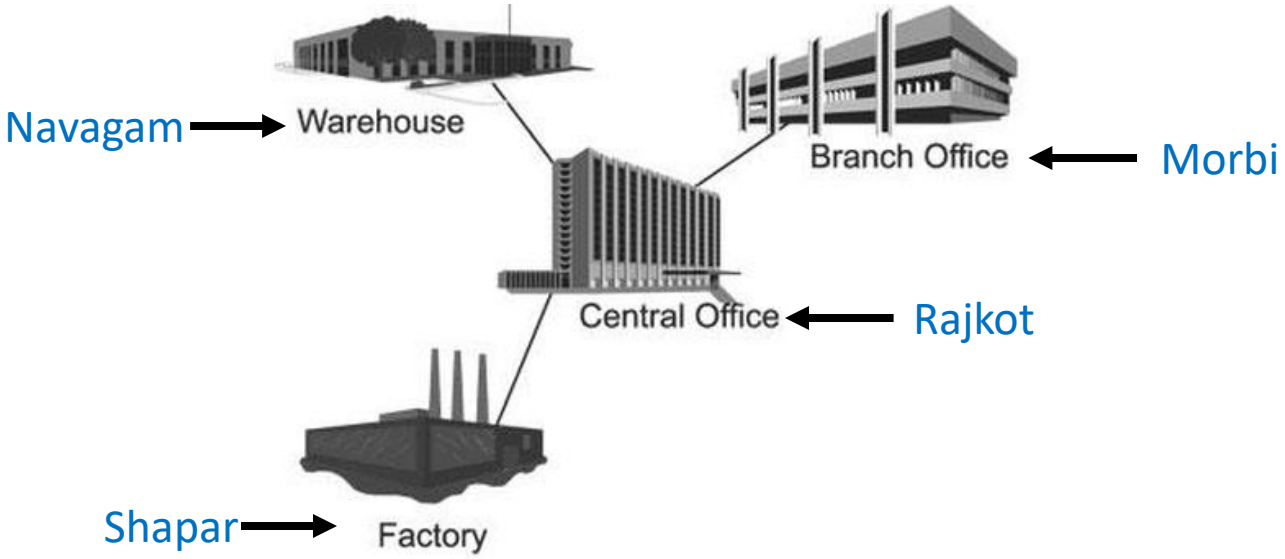
Local Area Network

- A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.



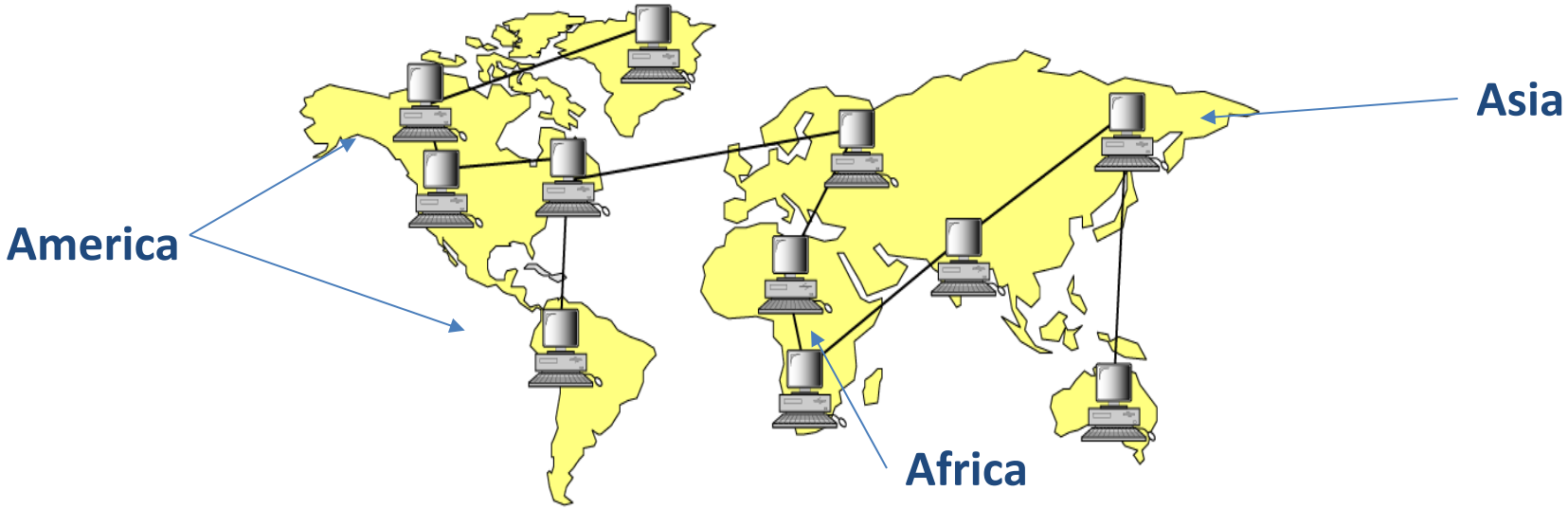
Metropolitan Area Network

- A metropolitan area network (MAN) is a computer network that interconnects with computer in a metropolitan area like city.
- MAN is a larger than LAN but smaller than the area covered by a WAN.
- It is also used to interconnection of several local area network.

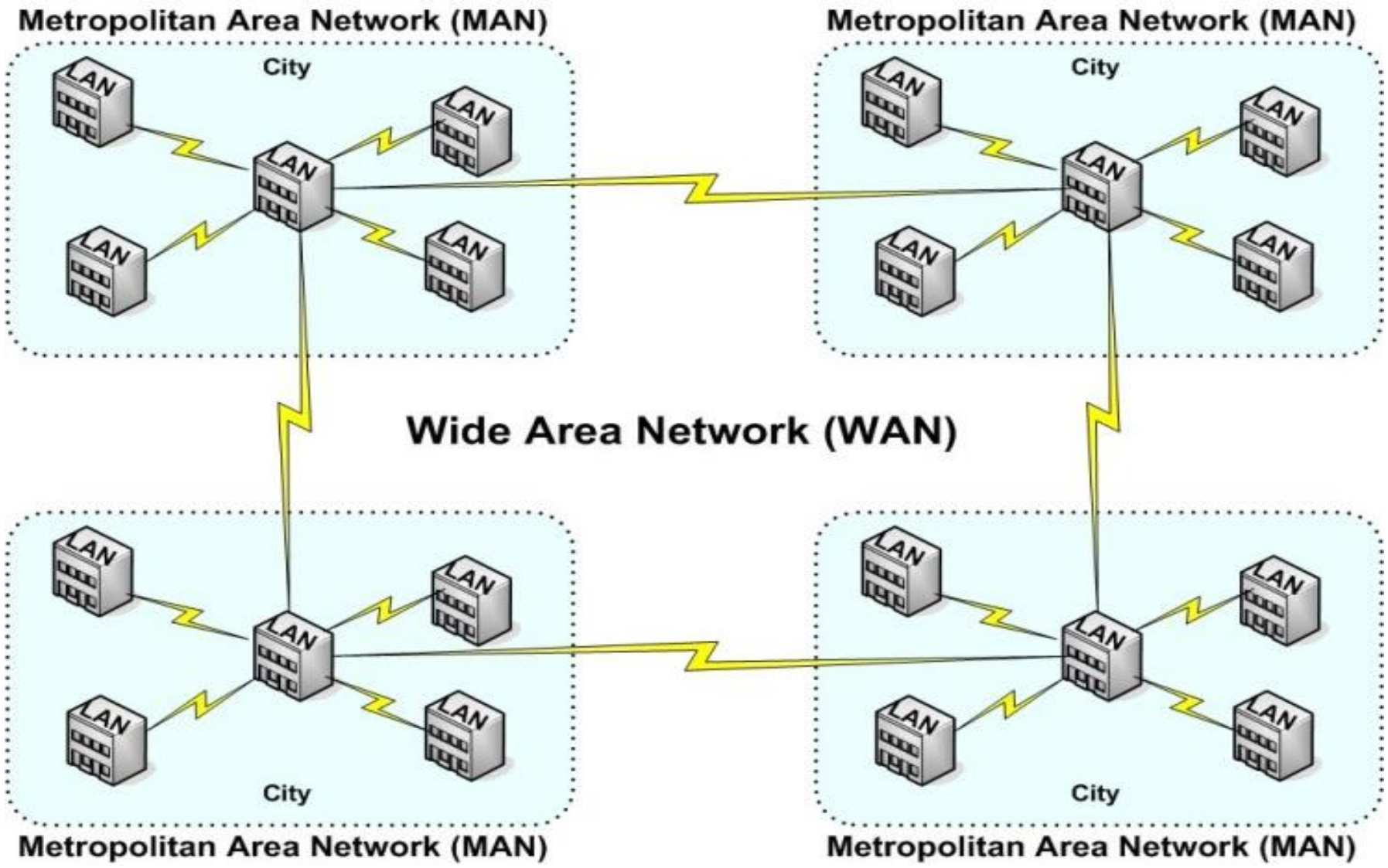


Wide Area Network

- A wide area network (WAN) is a computer network that exists over a large-scale geographical area.
- A WAN connects different networks, including local area networks (LAN) and metropolitan area networks (MAN).
- It may be located with in a state or a country or it may be interconnected around the world.



Types of Computer Networks - Summary

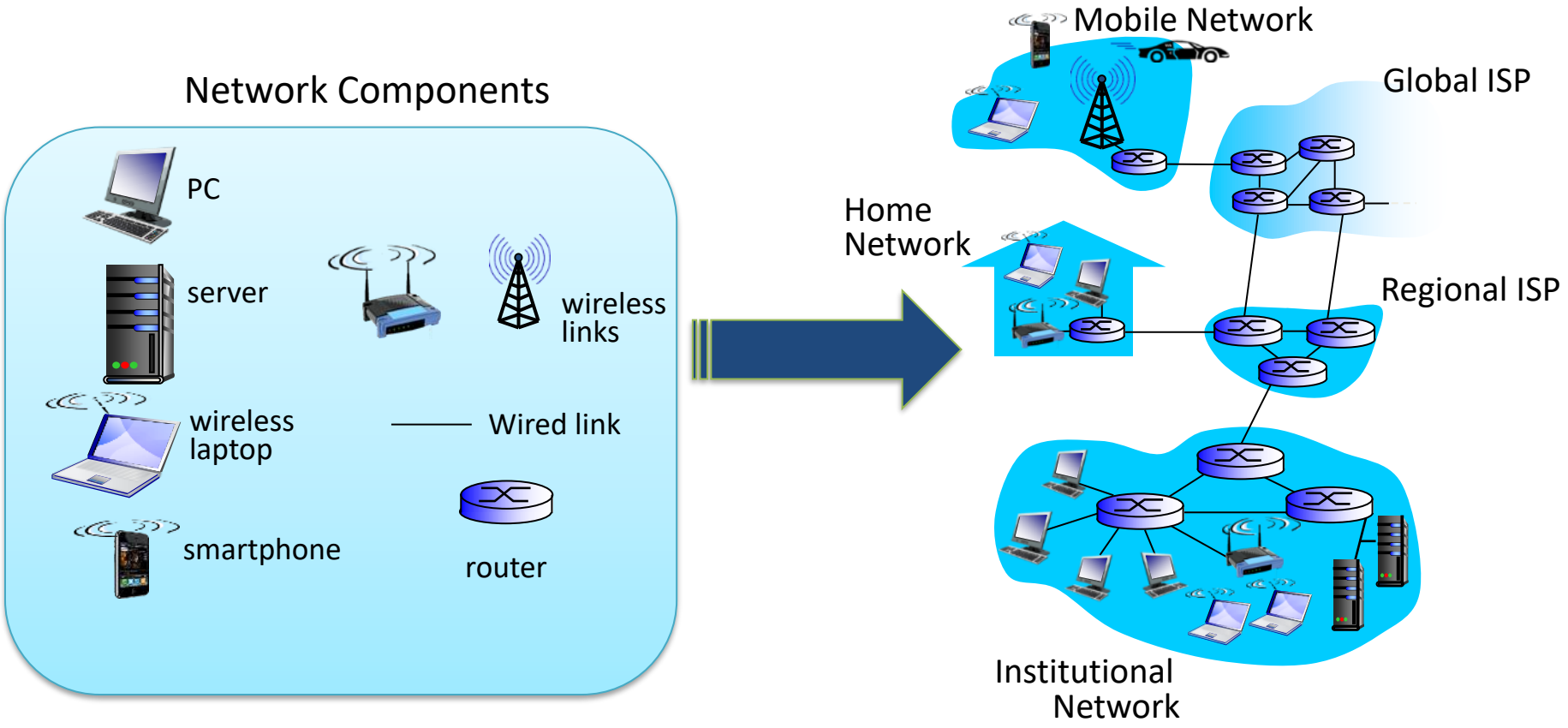


Types of Computer Networks - Summary

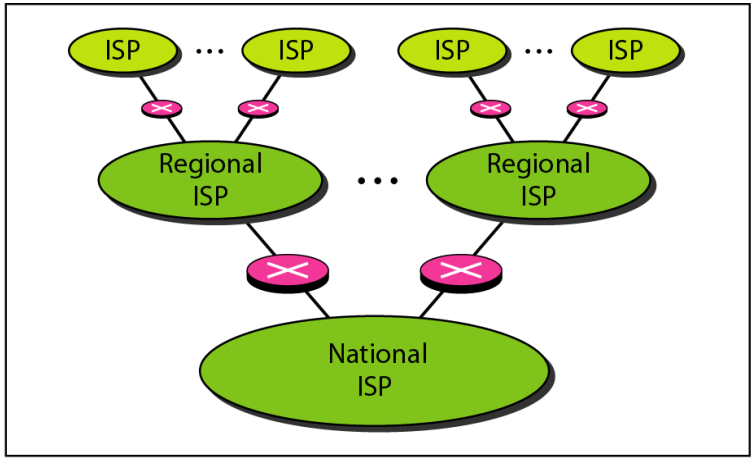
Basis Of Comparison	LAN	MAN	WAN
Full Name	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area	It covers relatively large region such as cities, towns	It spans large locality & connects countries together. e.g. Internet
Ownership of Network	Private	Private or Public	Private or Public (VPN)
Design and Maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Equipment Used	NIC, Switch, Hub	Modem, Router	Microwave, Radio Transmitter & Receiver
Range(Approximately)	1 to 10 km	10 to 100 km	Beyond 100 km
Used for	College, School, Hospital	Small towns, City	State, Country, Continent

What is Internet?

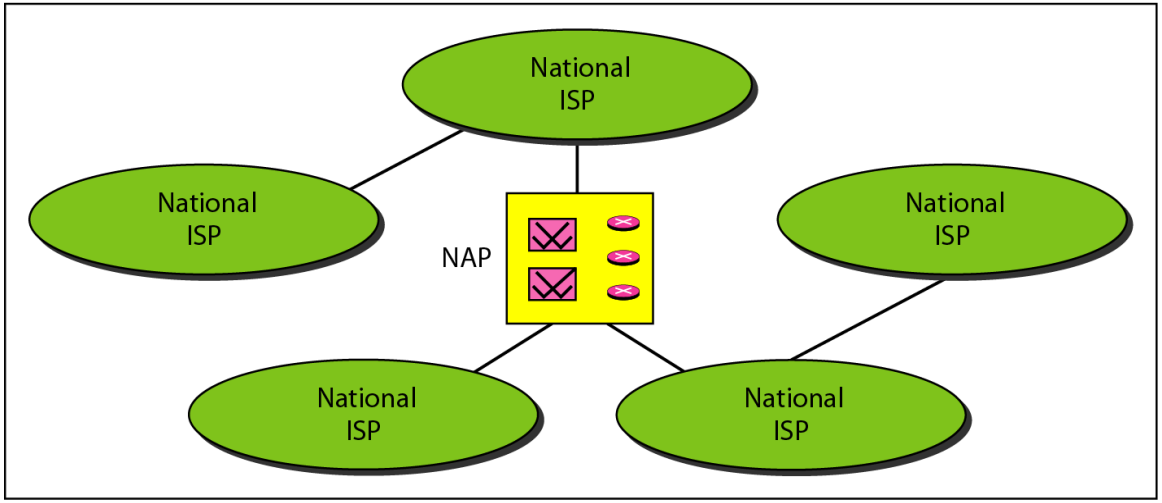
- The internet is a type of world-wide computer network.
- The internet is the collection of infinite numbers of connected computers that are spread across the world.



Hierarchical organization of the Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

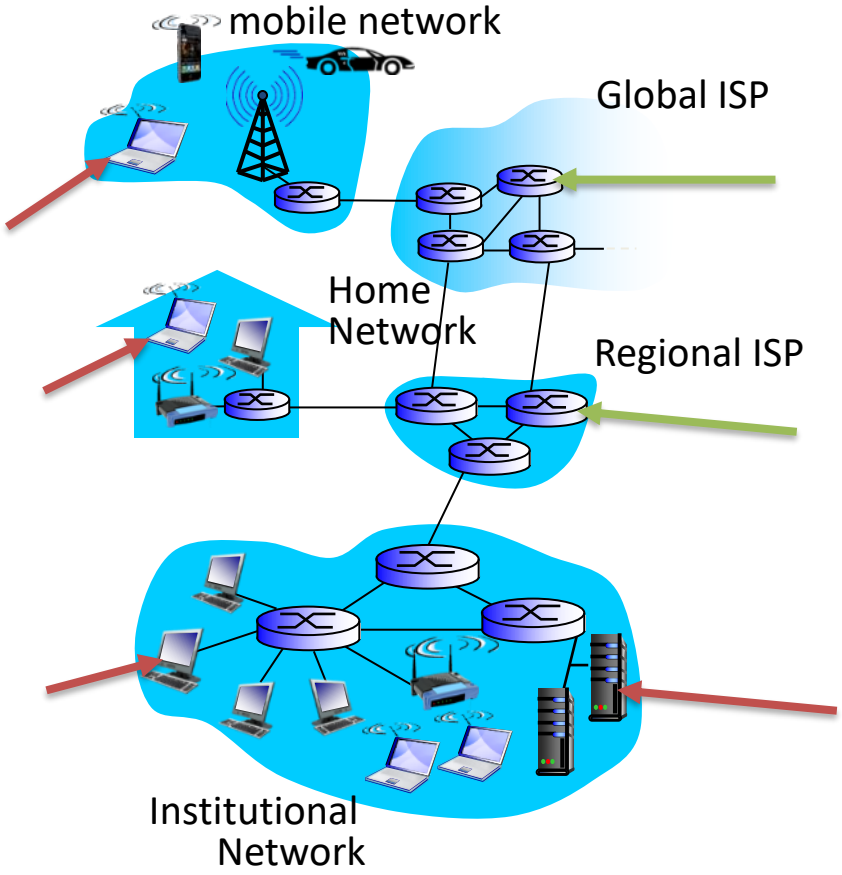
Intranet vs. Internet

- Intranet
  - ✓ A private network that is contained within an enterprise
  - ✓ Could be LANs and WANs
- Internet
  - ✓ A public network of networks
- Both are using TCP/IP

NETWORK EDGE

The Network Edge

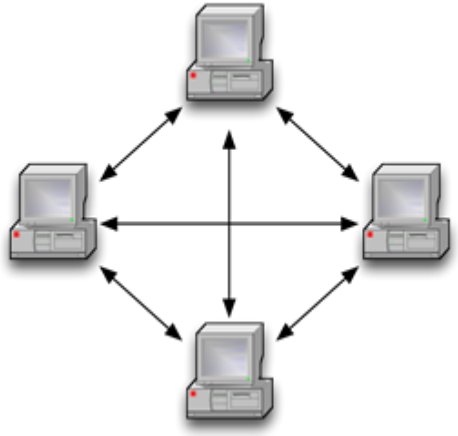
- Computers and other devices are connected at the edge (end) of the network.
- These computers are known as hosts or end systems. Router is known as edge router.



Peer to Peer Network

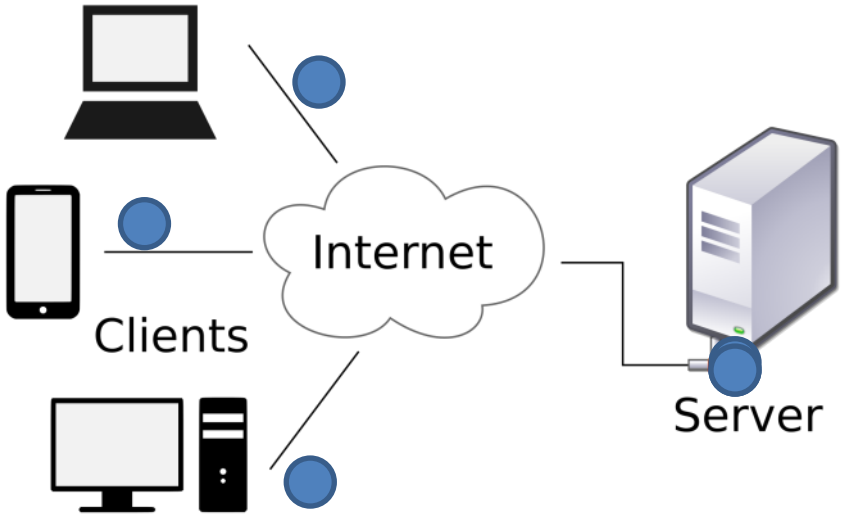
- Computers are connected together so that users can share resources and information.

- There is no central server for authenticating users, each of them works as both client and server.
- e.g. Bit Torrent



Client – Server Network

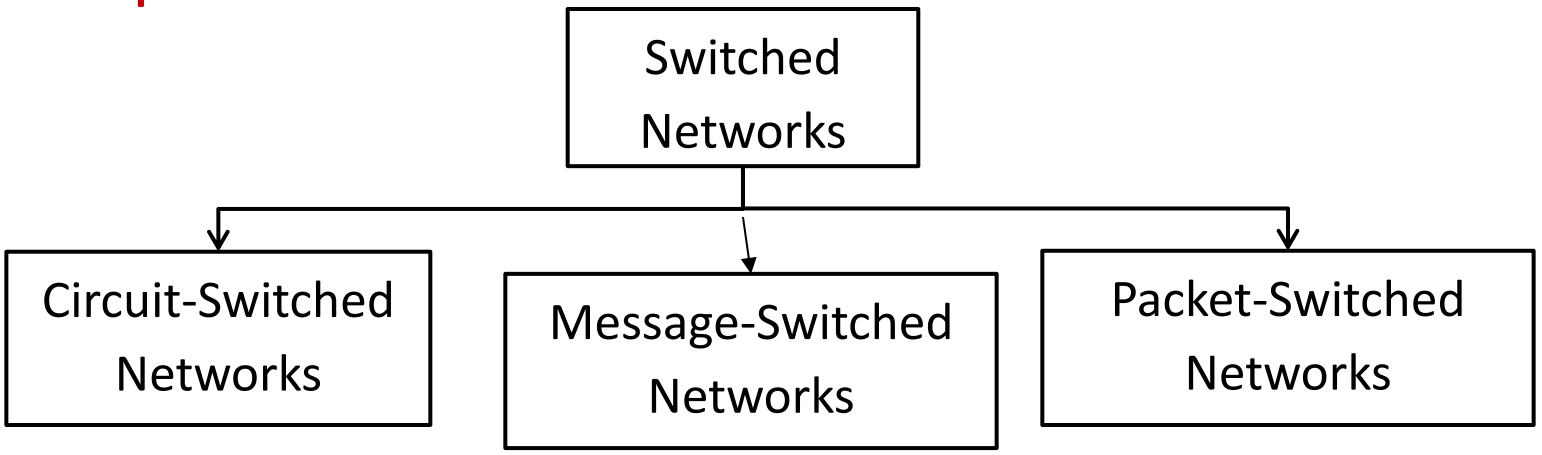
- Client: Request servers for a task.
  - ✓ Generally called desktop PCs or workstations.
- Server: Receive requests from the clients. Process and response them.
  - ✓ e.g. Web Server, Email Server



NETWORK CORE

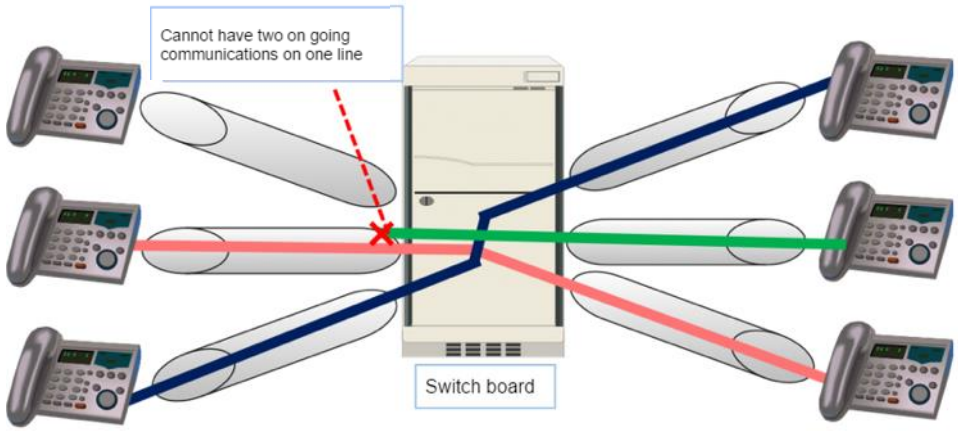
The Network Core: Transmission Techniques

- Defines the connection of different network segments together and process to transmit data across the network.
- It is implemented through the use of switching techniques.



Circuit Switched Network

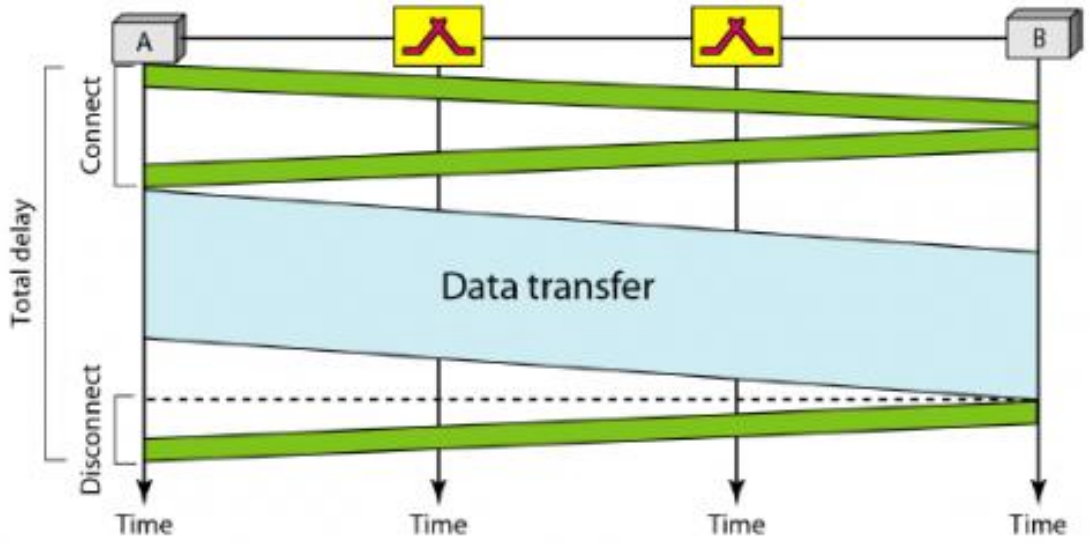
- A dedicated channel has to be established before the call is made between users.
- The channel is reserved between the users till the connection is active.
- For half duplex(one way) communication, one channel is allocated and for full duplex(two way) communication, two channels are allocated.
- It is mainly used for voice communication requiring real time services without delay.



Circuit Switched Network – Cont…

- Communication via circuit switching involves three phases:

1. Circuit Establishment
2. Data Transfer
3. Circuit Disconnect



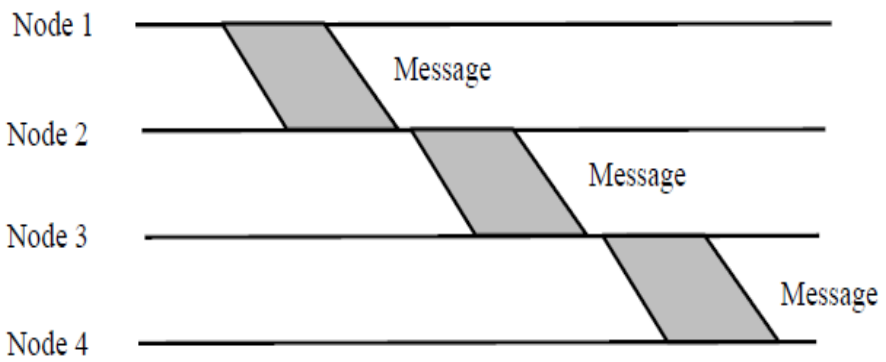
Advantages:

- After path is established, data communication without delay.
- Very suitable for continuous traffic.
- It establishes a dedicated path.
- No overhead after call setup.
- it is transparent and data passes in order.

Disadvantages:

- Provide initial delay for setting up the call.
- Inefficient for heavy traffic.
- Data rate should be same because of fixed bandwidth.
- When load increases, some calls may be blocked.
- In data communication, traffic between terminal and server are not continuous. Sometimes more data may come or sometimes there is no data at all. Circuit switching is not efficient because of its fixed bandwidth.

Message Switching



•In this switching method, a different strategy is used, where instead of establishing a dedicated physical line between the sender and the receiver, the message is sent to the nearest directly connected switching node.

•This node stores the message, checks for errors, selects the best available route and forwards the message to the next intermediate

•The line becomes free again for other messages, while the process is being continued in some other nodes.

•Due to the mode of action, this method is also known as **store-and-forward technology** where the message hops from node to node to its final destination.

•Each node stores the full message, checks for errors and forwards it.

Basic idea:

- Each network node receives and stores the message
- Determines the next leg of the route, and
- Queues the message to go out on that link.

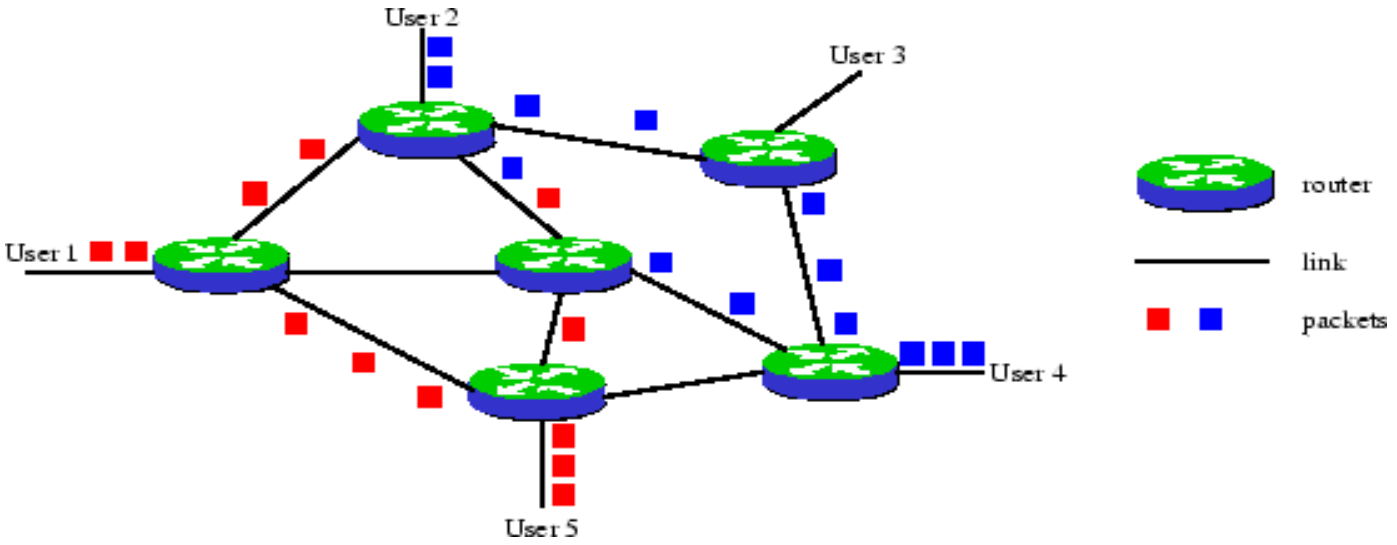
Advantages:

- Line efficiency is greater (sharing of links).
- Data rate conversion is possible.
- Even under heavy traffic, messages are accepted, possibly with a greater delay in delivery.
- Message priorities can be used, to satisfy the requirements, if any.

Disadvantages: Message of large size monopolizes the link and storage

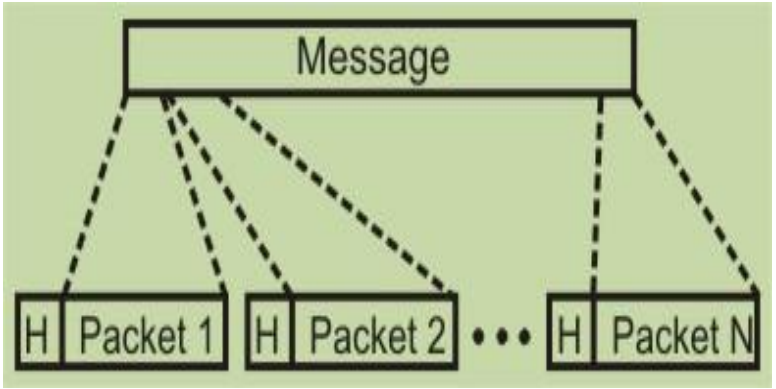
Packet Switched Network

- It is not required to establish the connection initially.
- The connection/channel is available to use by users. But when traffic or number of users increases then it will lead to congestion in the network.
- Packet switched networks are mainly used for data and voice applications requiring non-real time scenarios.



Packet Switching

- The basic approach is not much different from message switching. It is also based on the same ‘store-and-forward’ approach.
- However, to overcome the limitations of message switching, **messages are divided into subsets of equal length called packets.**
- This approach was developed for long-distance data communication (1970) and it has evolved over time.
- In packet switching approach, data are transmitted in short packets (few Kbytes).
- A long message is broken up into a series of packets as shown in Fig. Every packet contains some control information in its header, which is required for routing and other purposes.



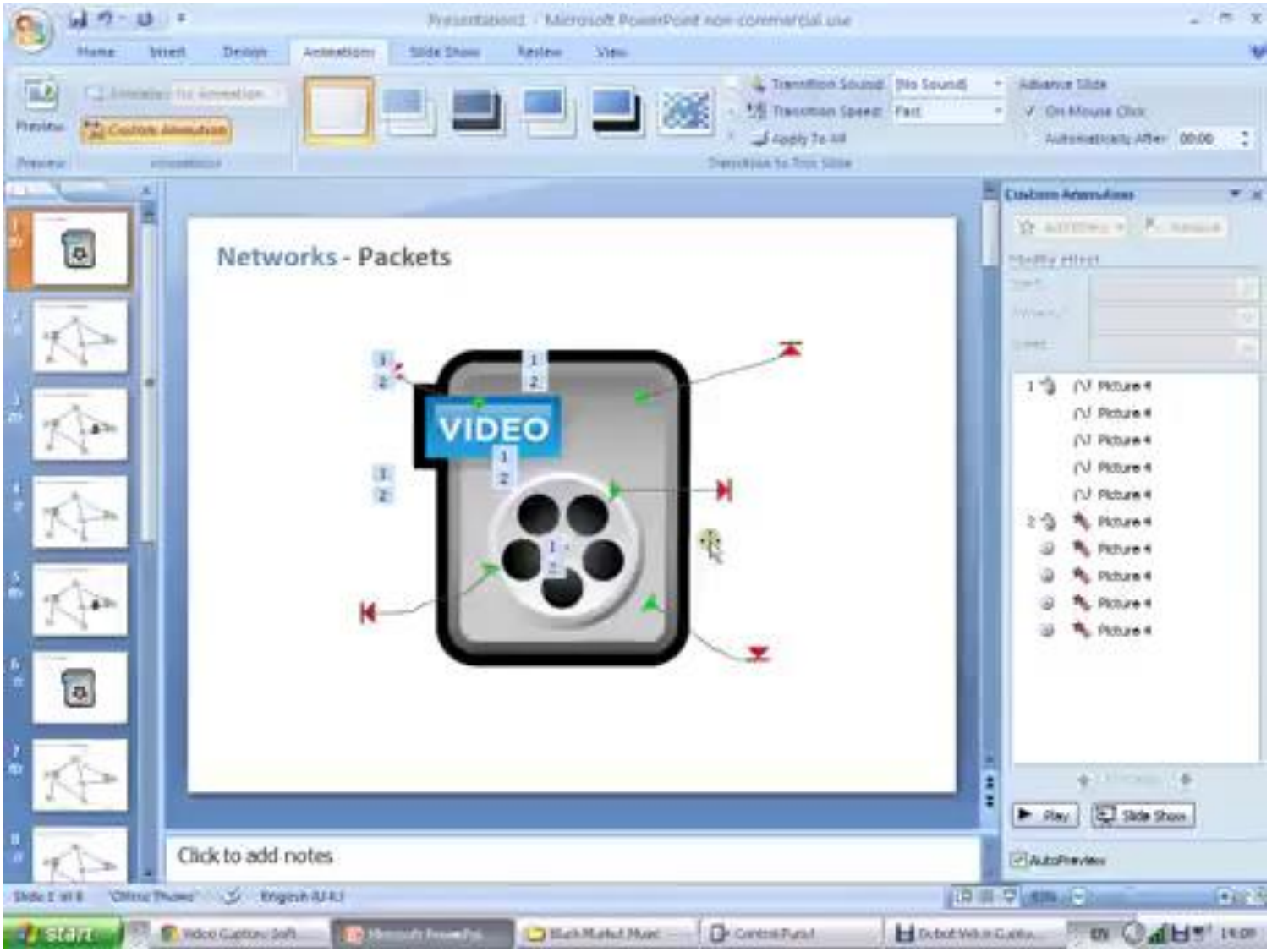
Advantages:

- Call setup phase is avoided (for transmission of a few packets, datagram will be faster).
- Because it is more primitive, it is more flexible.
- Congestion/failed link can be avoided (more reliable).

Problems:

- Packets may be delivered out of order.
- If a node crashes momentarily, all of its queued packets are lost.

Switching Network



Delay, Loss & Throughput

- **Delay**
  - ✓ As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several types of delays at each node along the path.

$$d_{nodal} = d_{proc} + d_{queue} + d_{tran} + d_{prop}$$

Where

d_{nodal} = Total Delay

d_{proc} = Processing Delay

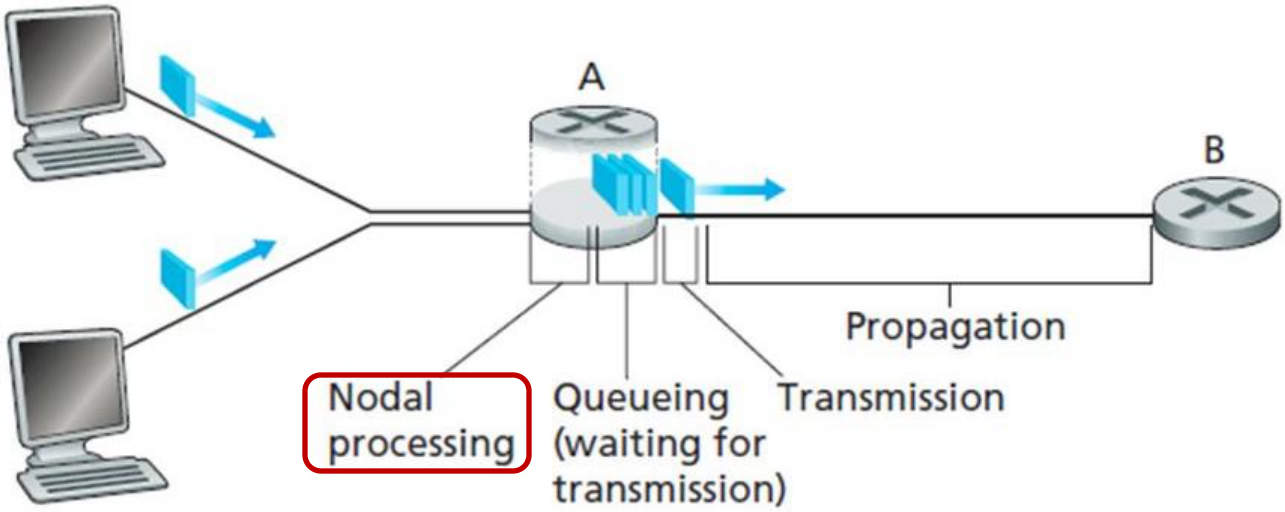
d_{queue} = Queuing Delay

d_{tran} = Transmission Delay

d_{prop} = Propagation Delay

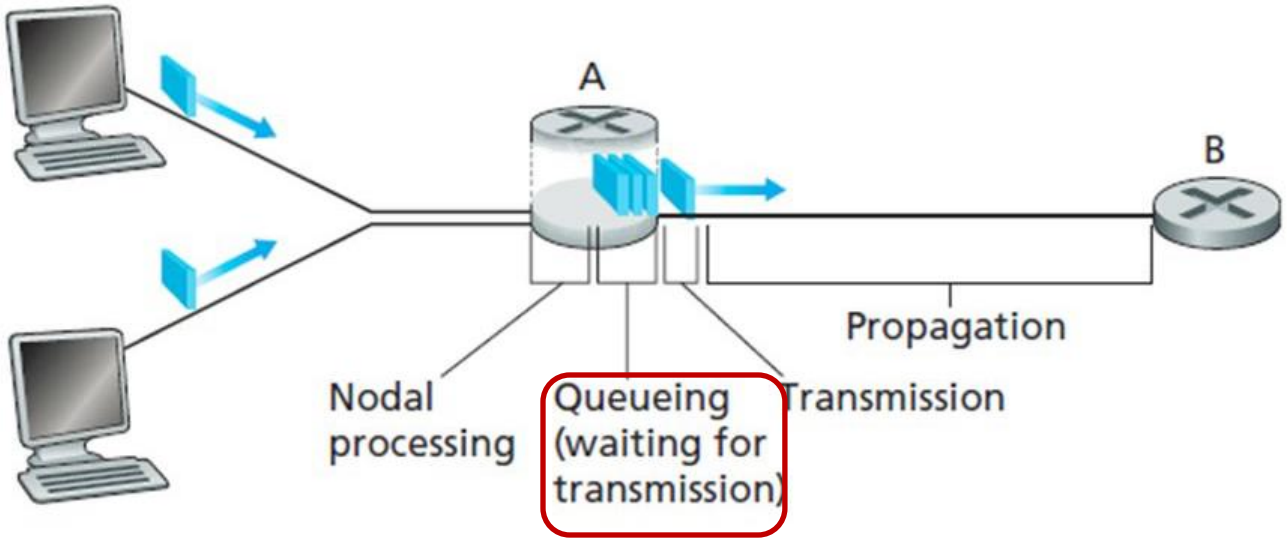
Delay – Cont…

- Processing Delay (d_{proc})
  - ✓ The time required to examine the packets header and determine where to direct the packet.
  - ✓ To check bit level error
  - ✓ Determine output link
  - ✓ Delay in terms of microseconds



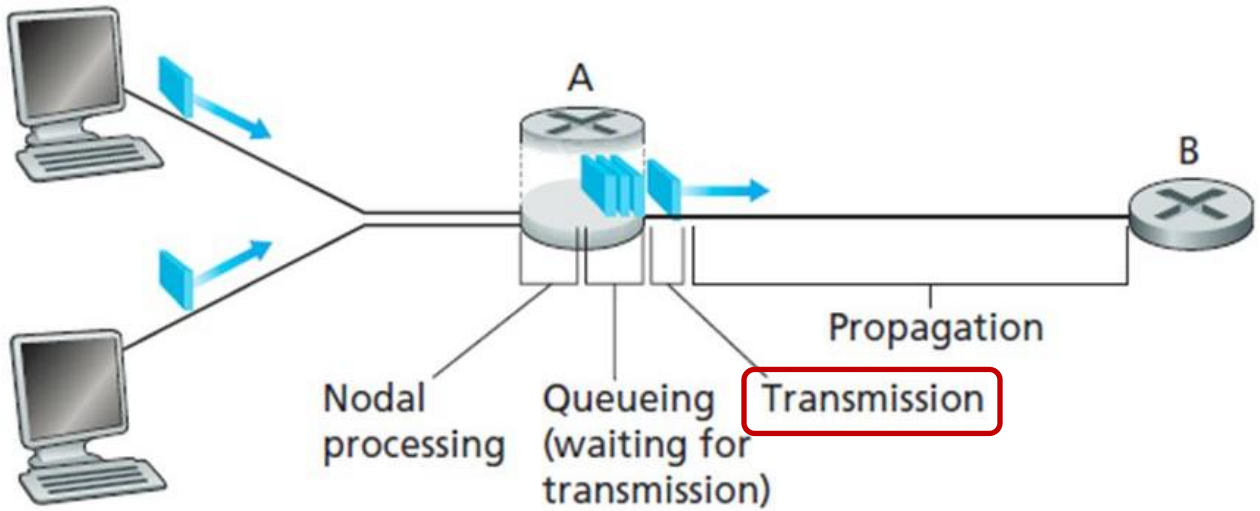
Delay – Cont…

- Queuing Delay (d_{queue})
  - ✓ A time to wait at output link for transmission.
  - ✓ Depends on congestion level of router.
  - ✓ If queue is empty then delay will be zero.
  - ✓ If queue is full (heavy traffic) then delay will be long.
  - ✓ Delay in terms of micro second to millisecond.



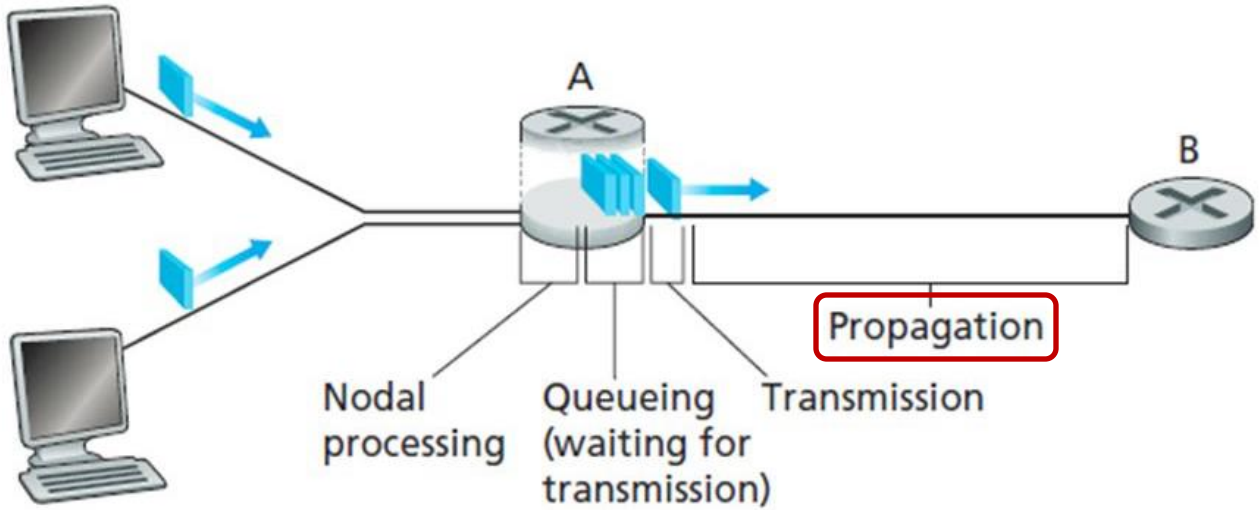
Delay – Cont…

- Transmission Delay (d_{tran} = L/R)
  - ✓ An amount of time required for the router to transmit the packet.
  - ✓ Its depends on packet length(L) and transmission rate(R) of link.



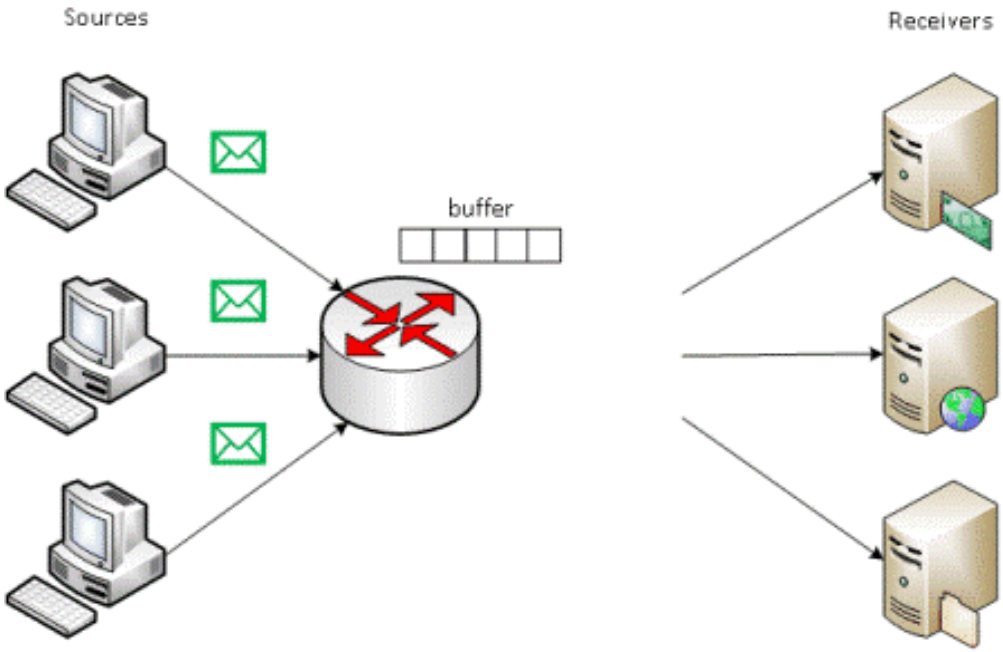
Delay – Cont…

- Propagation Delay (d_{prop}= d/s)
  - ✓ A time required to propagate from the beginning of the link to router B.
  - ✓ Depends on the length of physical medium(d) link and propagation speed(s) of link
  - ✓ Delay in terms of millisecond.



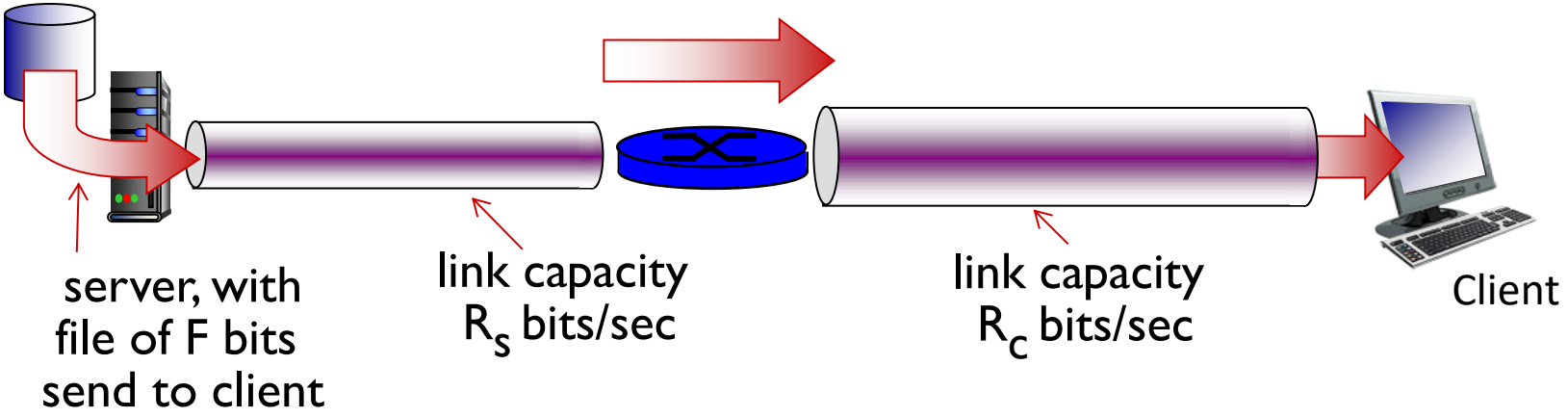
Packet Loss

- Packet loss is the failure of one or more transmitted packets to arrive at their destination.
- The loss of data packets depends on the switch queue/buffer. The loss of data packets increases with the increases in the traffic intensity.
- It affects the performance of the network.



Throughput

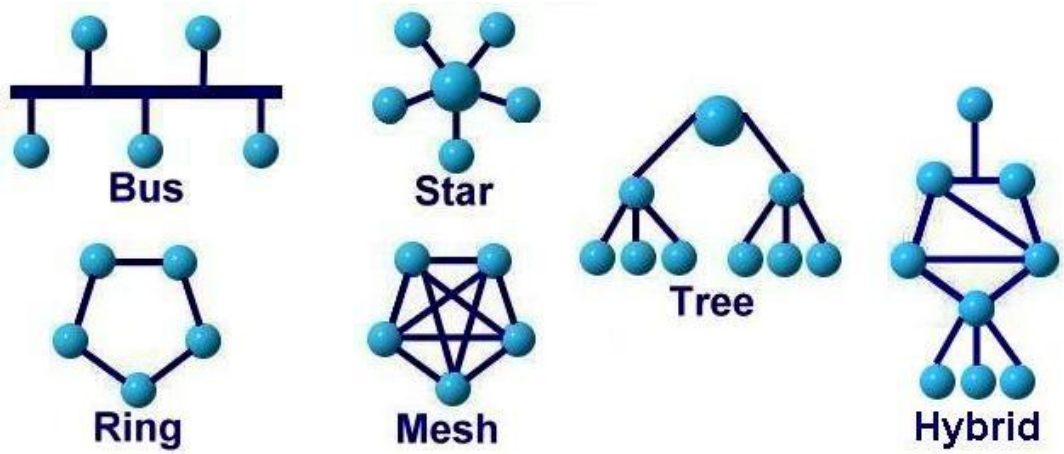
- Throughput or Network Throughput is the rate of successful message delivery over a communication channel.
- Throughput is measured in bits(data) per second (bit/s or bps)



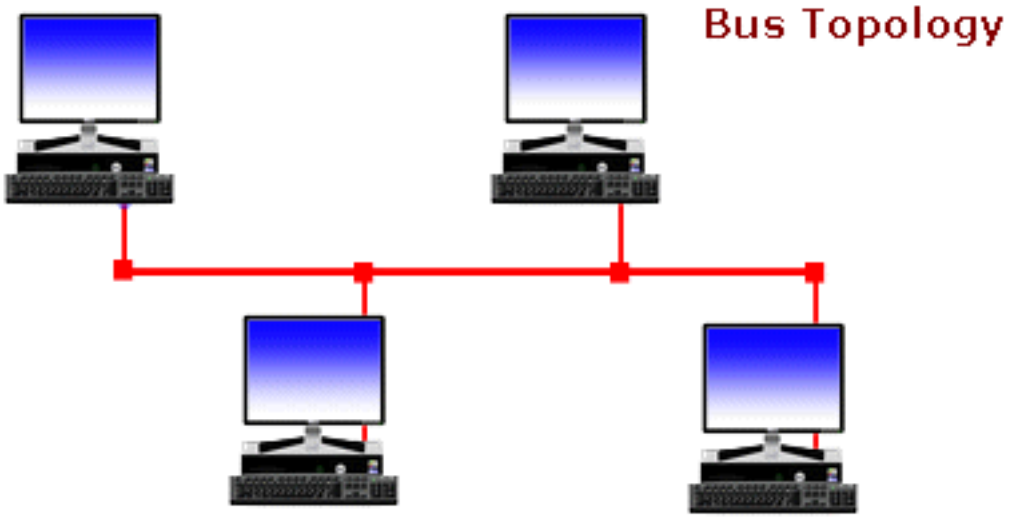
NETWORK TOPOLOGIES

Network Topologies

- Network topology is the arrangement of the various components(links, nodes, etc.) of a computer network.
- Types of network topologies :
  1. Bus
  2. Ring
  3. Star
  4. Mesh
  5. Tree
  6. Hybrid



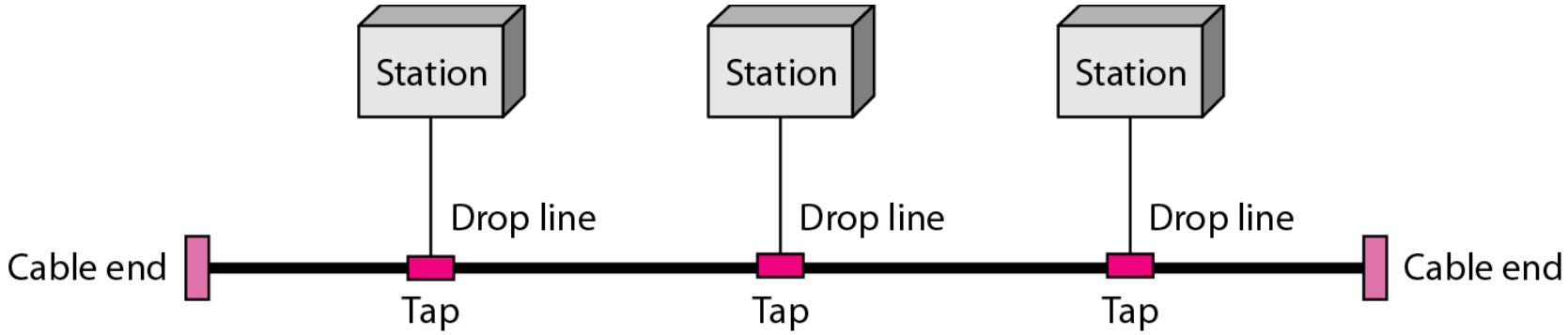
Bus Topology



- Every computer and network device is connected to single cable
- It transmits data only in one direction
- Cost effective
- Used in small networks
- Easy to expand joining two cables together
- It is used in early LAN connection

Bus Topology

- Early Ethernet



Advantages:

- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to built small networks.

Disadvantages:

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network.

Ring Topology

- It forms a ring as each computer is connected to another computer, with the last one connected to the first.
- Transmission is unidirectional & sequential way that is bit by bit.
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand.

Advantages:

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Disadvantages:

- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

Star Topology

- Computers are connected to a single central hub through a cable.
- Fast performance with few nodes and low network traffic.
- Easy to troubleshoot & Easy to setup and modify.
- Only that node is affected which has failed rest of the nodes can work smoothly.
- Hub can be upgraded easily.

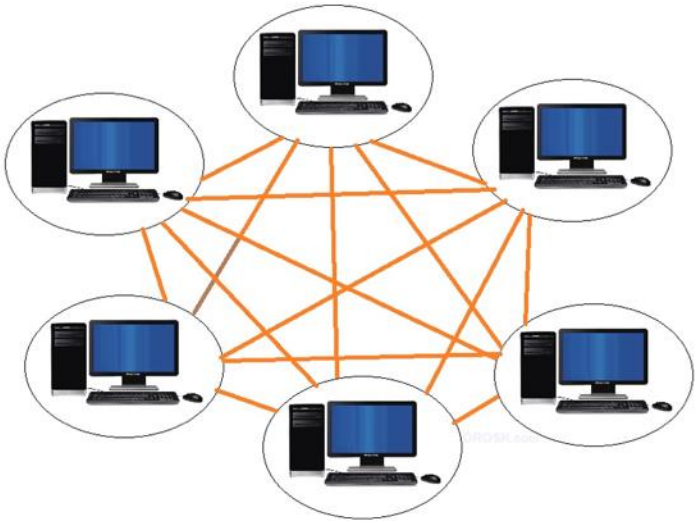
Advantages:

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device require only 1 port i.e. to connect to the hub.

Disadvantages:

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

Mesh Topology



- Point-to-point connection to other devices or fully connected.
- Traffic is carried only between two connected devices.
- Robust, costly but not flexible.
- Fault is diagnosed easily.
- More cable resource used in setup.

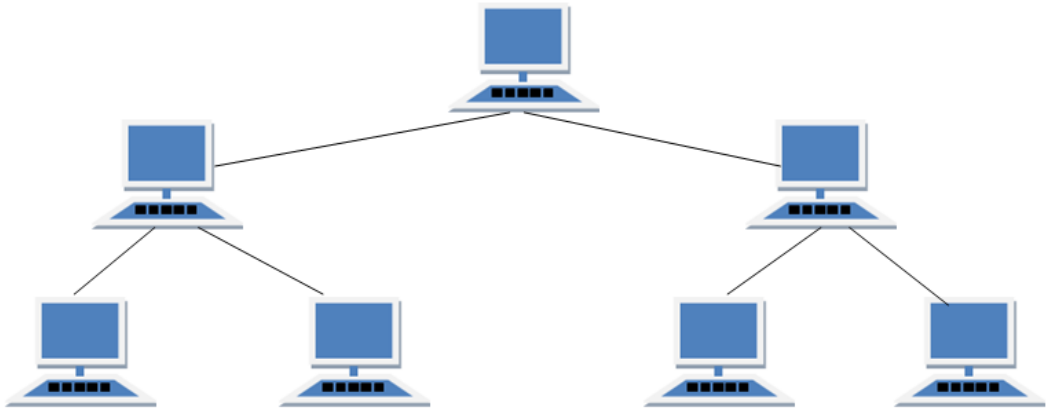
Advantages:

- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages:

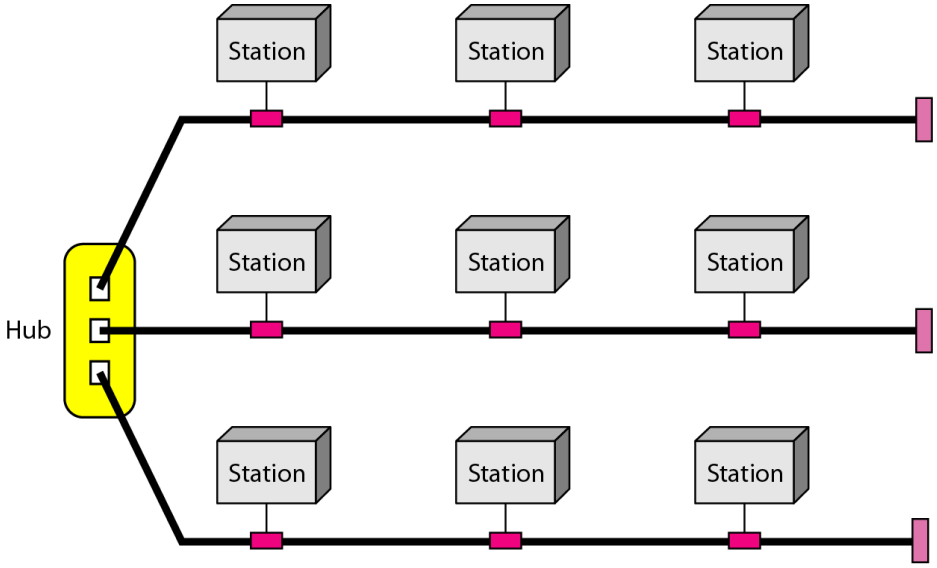
- Installation and configuration is difficult.
- Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
- Cost of maintenance is high.

Tree Topology



- It has a root node and all other nodes are connected to it forming a hierarchy.
- Also called hierarchical topology.
- Mostly used in Wide Area Network – WAN.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.

Hybrid Topology



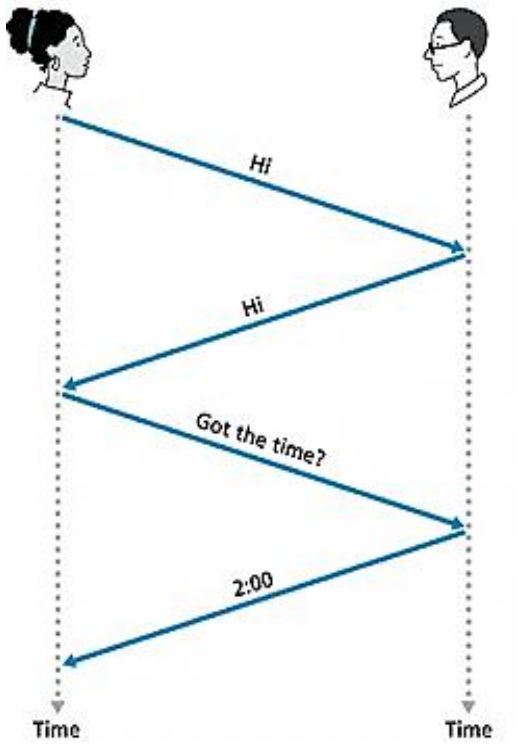
- A network structure whose design contains more than one topology is said to be hybrid topology.
- It is a combination of two or more topologies.
- Flexible & reliable as error detection and easy to troubleshoot.
- Scalable as size can be increased easily.

Comparison of Topologies

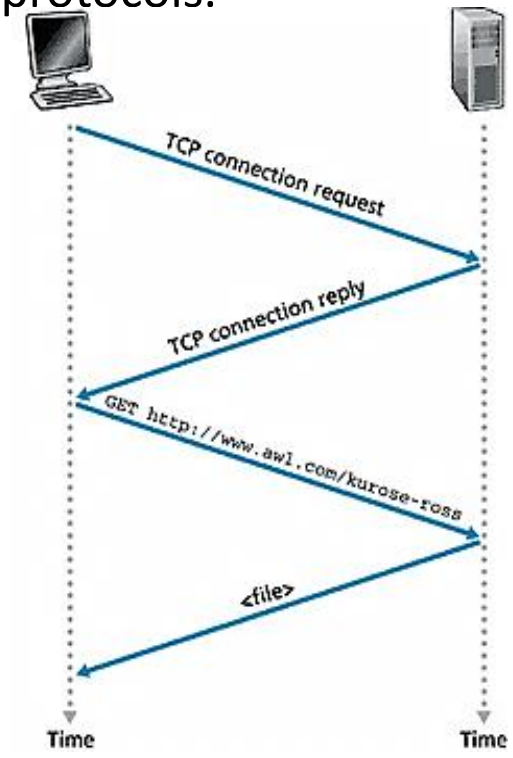
	Bus	Ring	Star	Mesh	Tree
Means	every computer and network device is connected to single cable.	Each computer is connected to another, with the last one connected to the first.	All the computers are connected to a single hub through a cable.	All the network nodes are connected to each other.	It has a root node and all other nodes are connected to it forming a hierarchy.
Cost	Average	Cheap	High	High	High
Used in	Small Network	Expand Network	Small Network	Expand Network	Expand Network
Troubleshoot	Easy, But Cables fail then whole network fails.	Difficult; Failure of one computer disturbs the whole network.	Easy; If the hub fails then the whole network is down.	Easy; Installation and configuration is difficult.	Easy; Central root hub fails, network fails.

What is Protocol?

- Human Protocol(Language)
  - ✓ “what’s the time?”
  - ✓ “I have a question”
  - ✓ Introduction Talk
- Network Protocol
  - ✓ Set of rules
  - ✓ machines rather than humans
  - ✓ all communication activity in Internet governed by protocols.



Protocol is define format, order of message sent and received among network entities, and actions taken on message transmission and reception

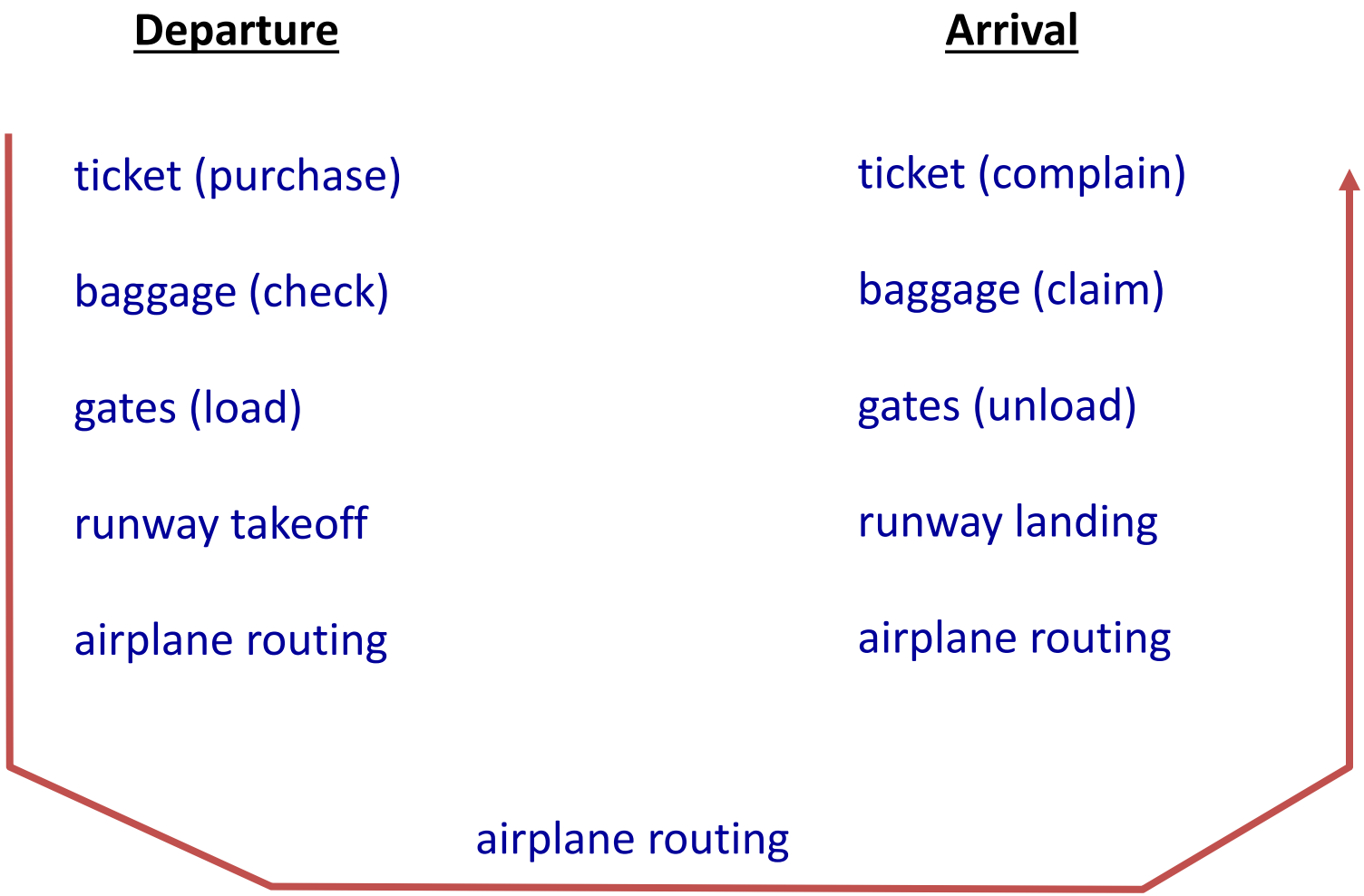


PROTOCOL LAYERS

Protocols Layers

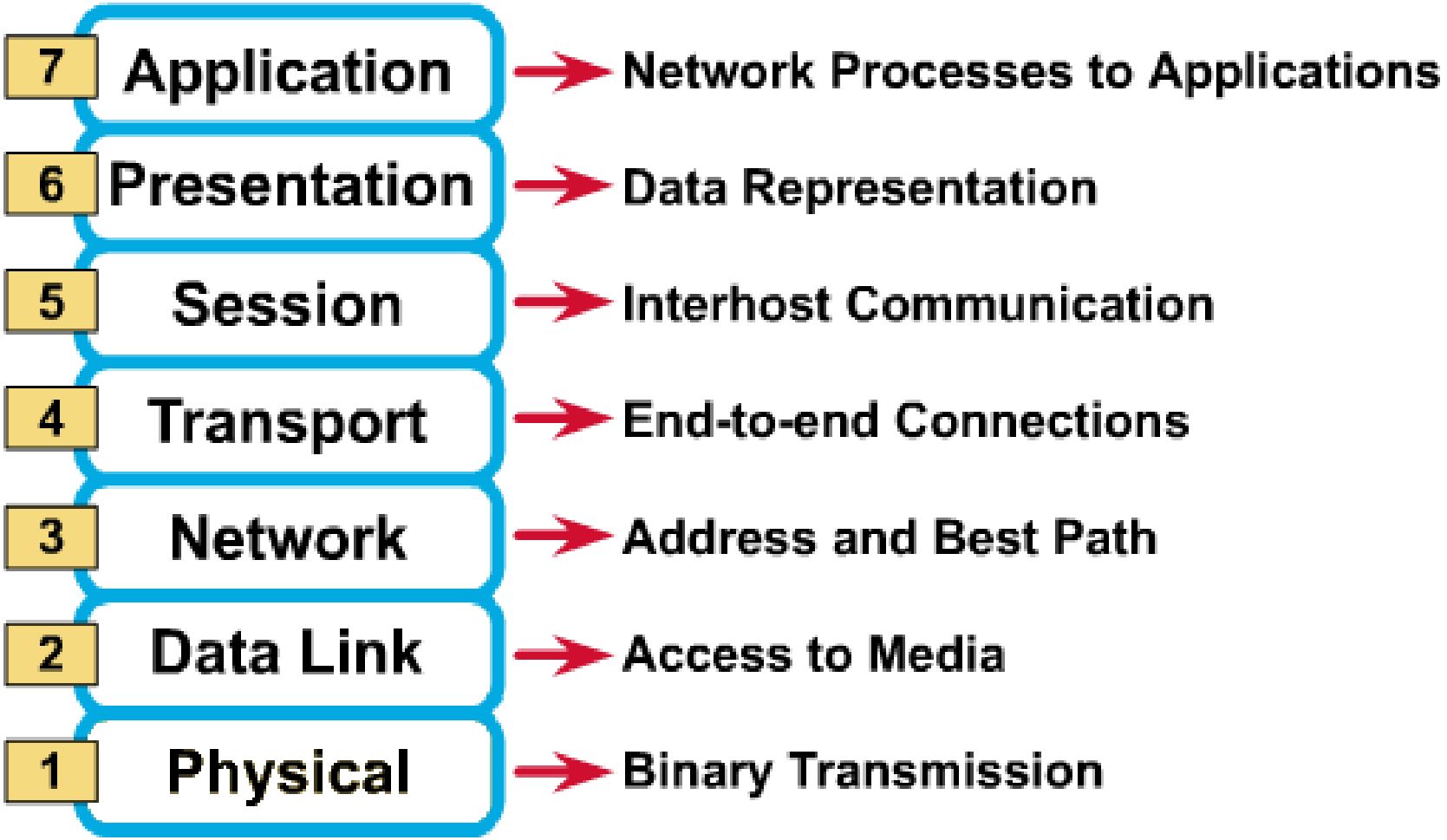
- To deals with connecting systems that are open for communication with other systems.
- OSI Layer Model (Open Systems Interconnection)
- Developed by the International Standards Organization (ISO) with seven different layers.
    1. Physical Layer
    2. Data Link Layer
    3. Network Layer
    4. Transport Layer
    5. Session Layer
    6. Presentation Layer
    7. Application Layer

Example – Air Plane Travel

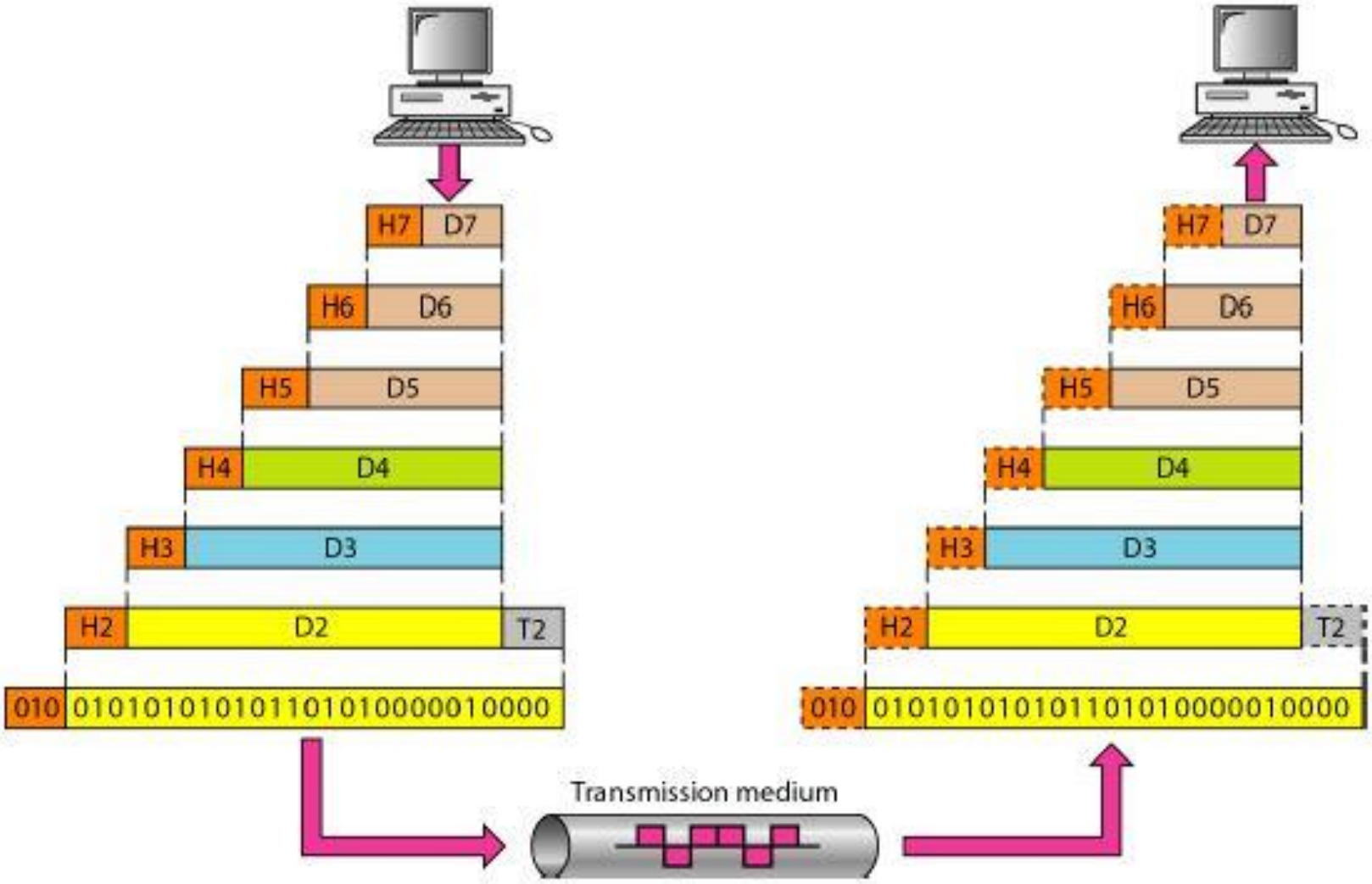


How OSI Layer Works?

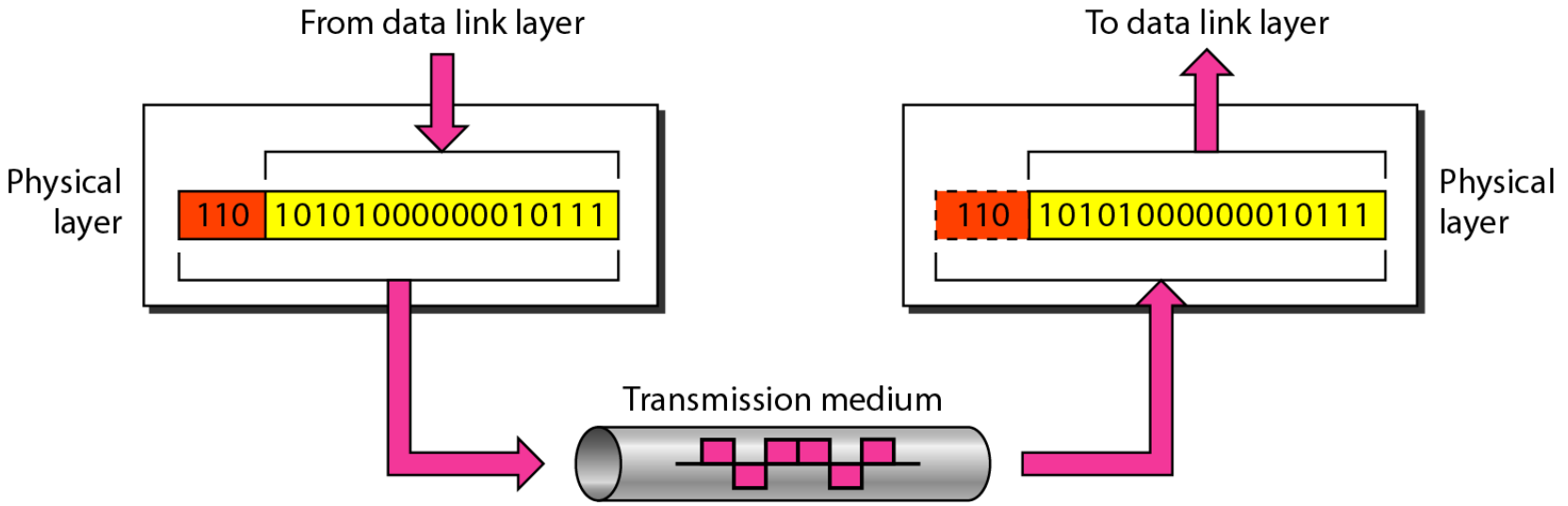
OSI Reference Model: 7 Layers



Exchange using OSI Model



Physical Layer



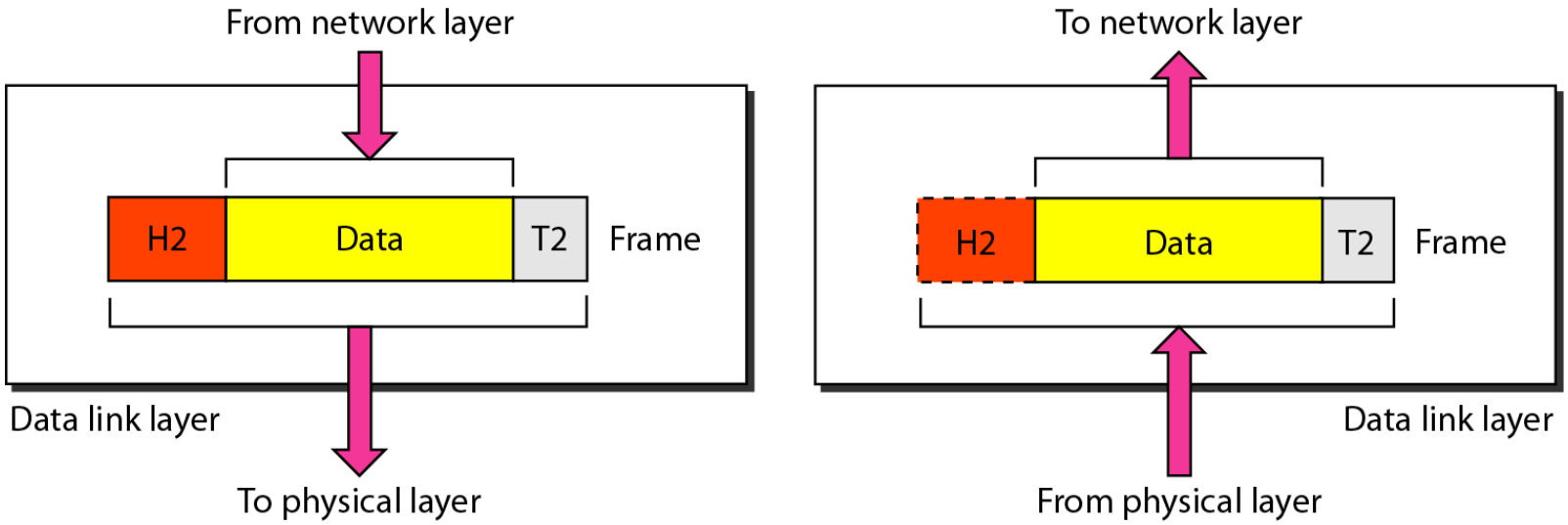
- The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Physical Layer – Cont…

- Carries the bit stream over a physical media.
- Physical Layer is concerned with:
  - ✓ Interface and Medium like guided cables
  - ✓ Representation of bits
  - ✓ Data rate
  - ✓ Synchronization of bits
  - ✓ Line configuration
  - ✓ Physical topology
  - ✓ Transmission mode

  - ✓ Provides physical interface for transmission of information.
  - ✓ Defines rules by which bits are passed from one system to another on a physical communication medium.
  - ✓ Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
  - ✓ Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

Data Link Layer



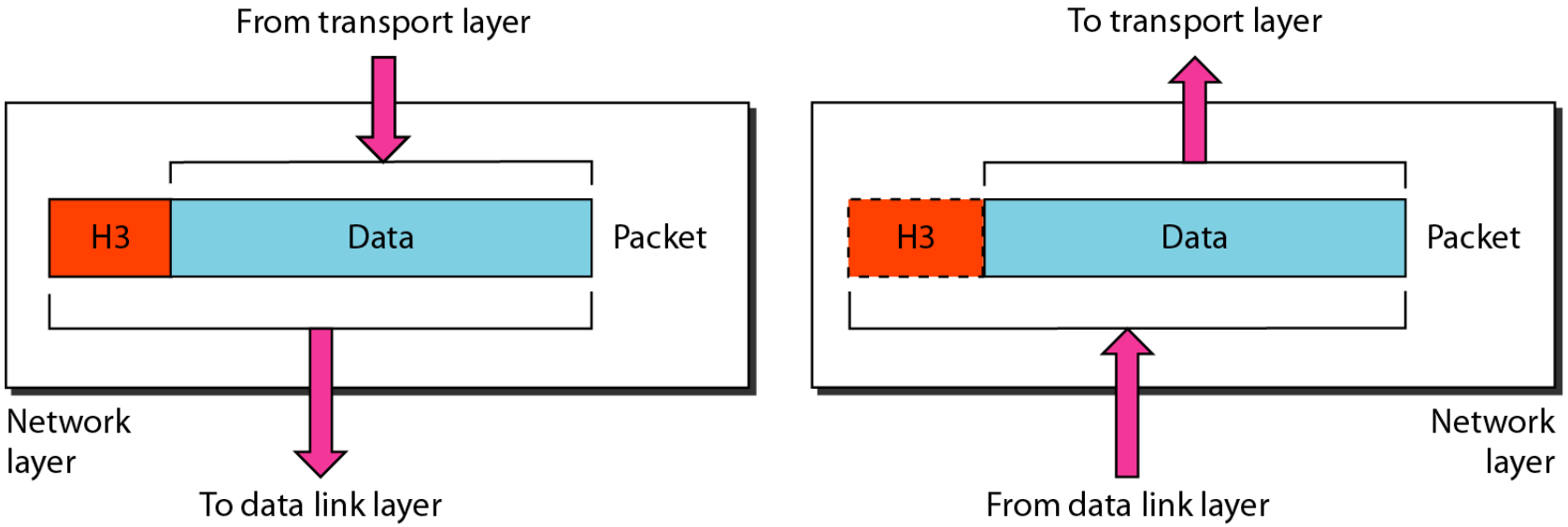
- The data link layer is responsible for moving frames from one hop to the next.

Data Link Layer – Cont…

- Data link layer is concerned with:
  - ✓ Framing – divide bits stream into data unit (frame)
  - ✓ Physical addressing
  - ✓ Flow control – avoid over overwhelming
  - ✓ Error control – bit loses, retransmission
  - ✓ Access control

  - ✓ Data link layer attempts to provide reliable communication over the physical layer interface.
  - ✓ Breaks the outgoing data into frames and reassemble the received frames.
  - ✓ Create and detect frame boundaries.
  - ✓ Handle errors by implementing an acknowledgement and retransmission scheme.
  - ✓ Implement flow control.
  - ✓ Supports points-to-point as well as broadcast communication.
  - ✓ Supports simplex, half-duplex or full-duplex communication.

Network Layer

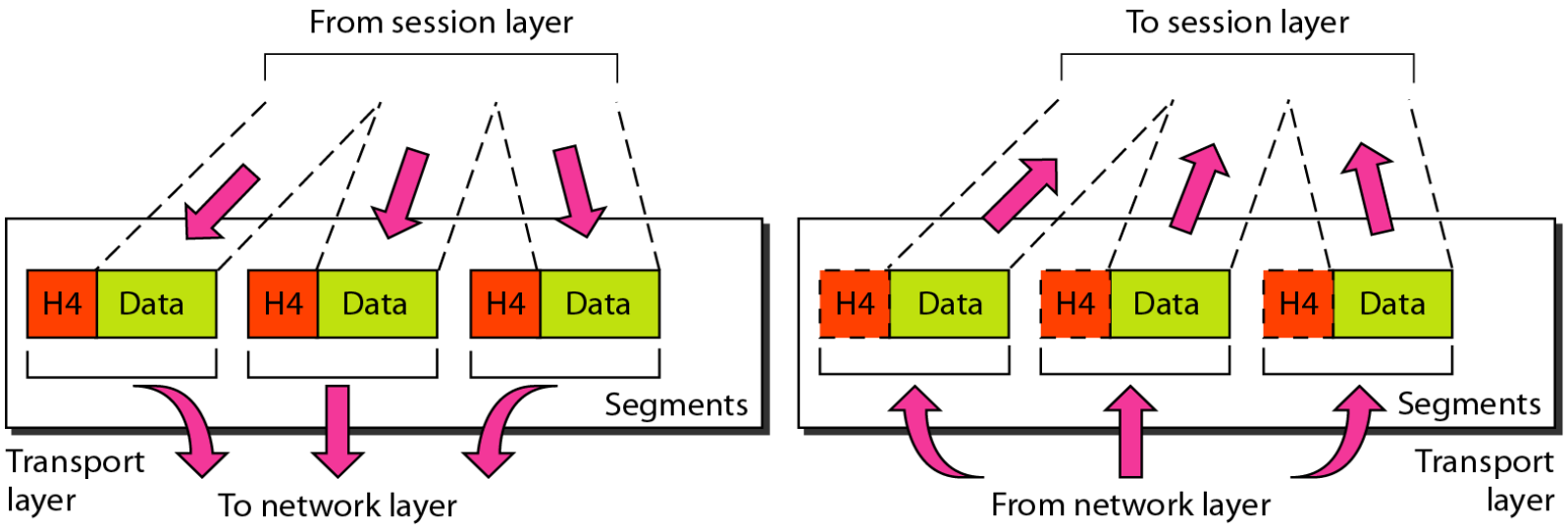


- The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Network Layer – Cont…

- In this layer, packet is combined with header and data.
- In case of data link layer, packet delivers on the same network.
- If two different networks are connected then packet is concern with network layer.
- Network layer is concerned with:
  - ✓ Logical addressing e.g. 192.168.1.1 (IP Address)
  - ✓ Routing

Transport Layer

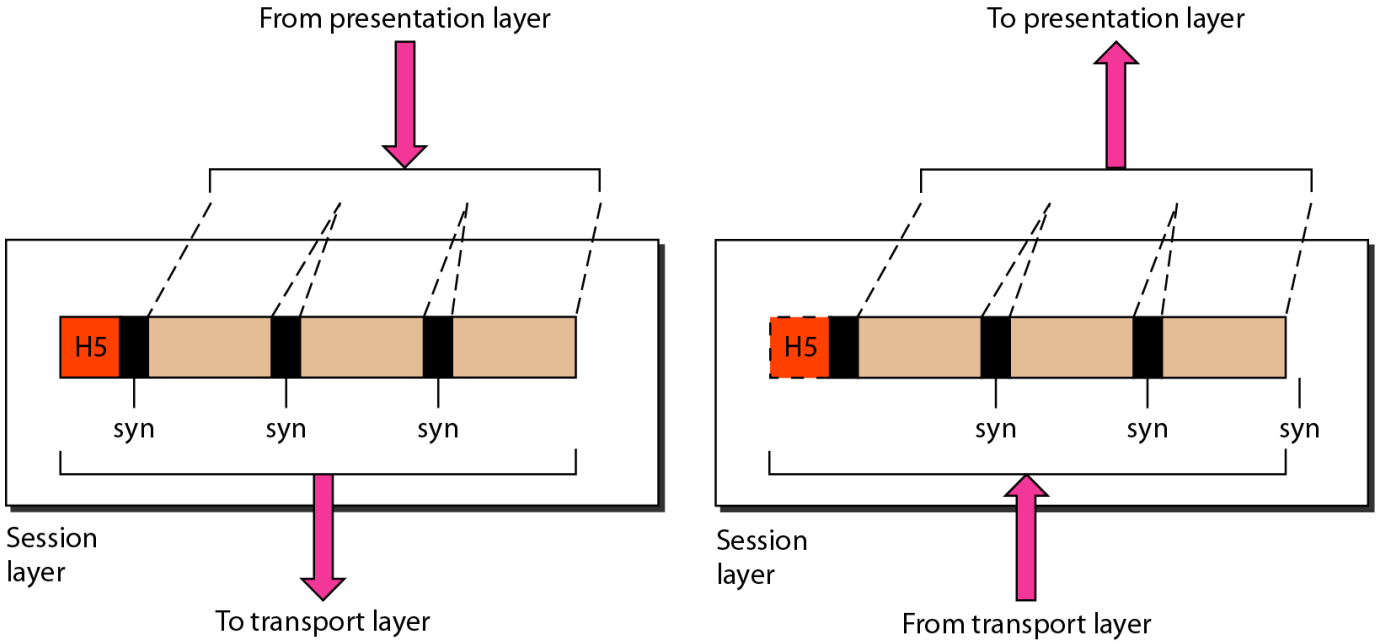


- The transport layer is responsible for the delivery of a message from one process to another.

Transport Layer – Cont…

- This layer ensures that the whole message arrives intact and in order.
- Transport layer is concerned with:
  - ✓ Service-point addressing (port address)
  - ✓ Segmentation and reassembly
  - ✓ Connection control
  - ✓ Flow and error control

Session Layer

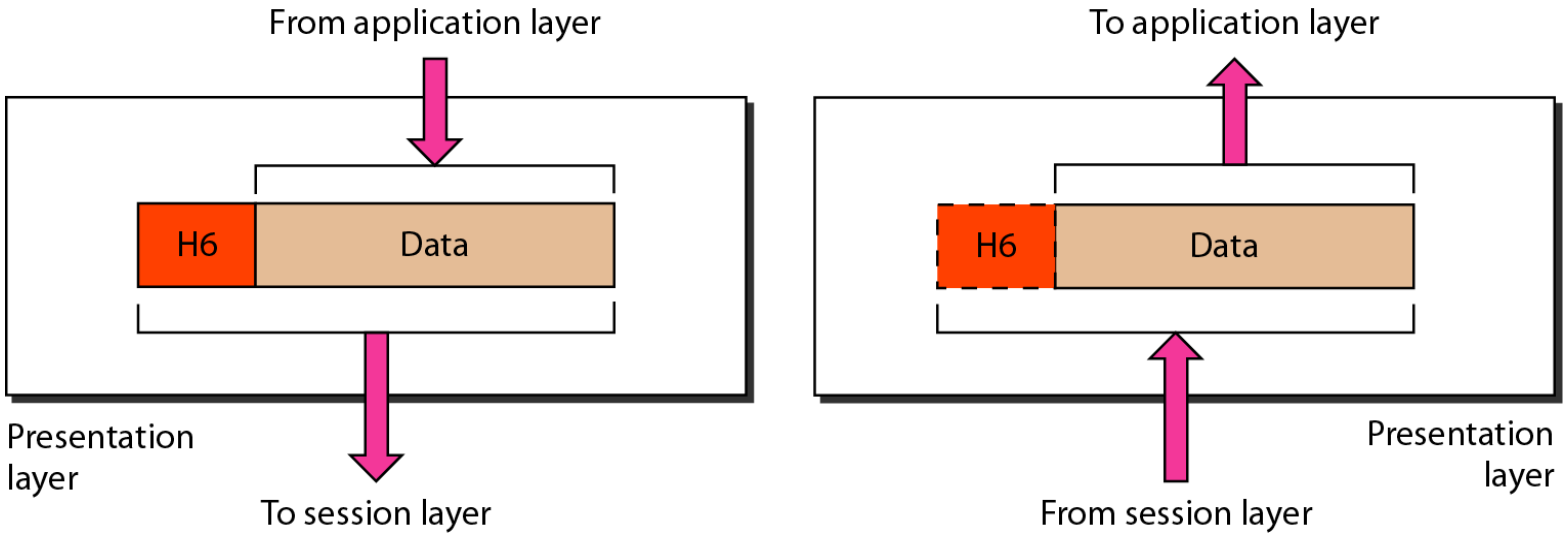


- The session layer is responsible for dialog control and synchronization.

Session Layer – Cont…

- This layer is network dialog controller – establishes, maintains, synchronizes the interaction among computers.
- Session layer is concerned with:
  - ✓ Dialog control
  - ✓ Synchronization

Presentation Layer

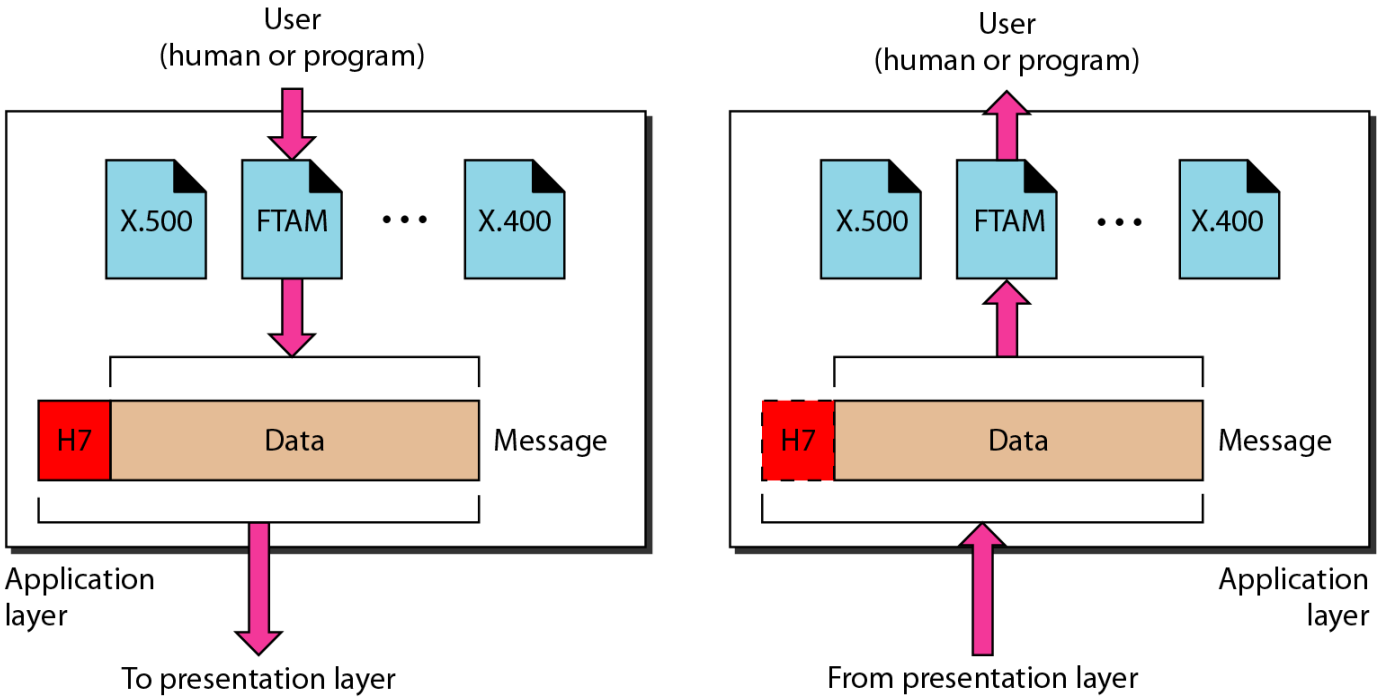


- The presentation layer is responsible for translation, compression, and encryption.

Presentation Layer – Cont…

- This layer is concerned with the syntax which refers to order in which data is presented and semantics helps in interpreting a particular pattern.
- Presentation layer is responsible for:
  - ✓ Translation
  - ✓ Encryption
  - ✓ Compression

Application Layer

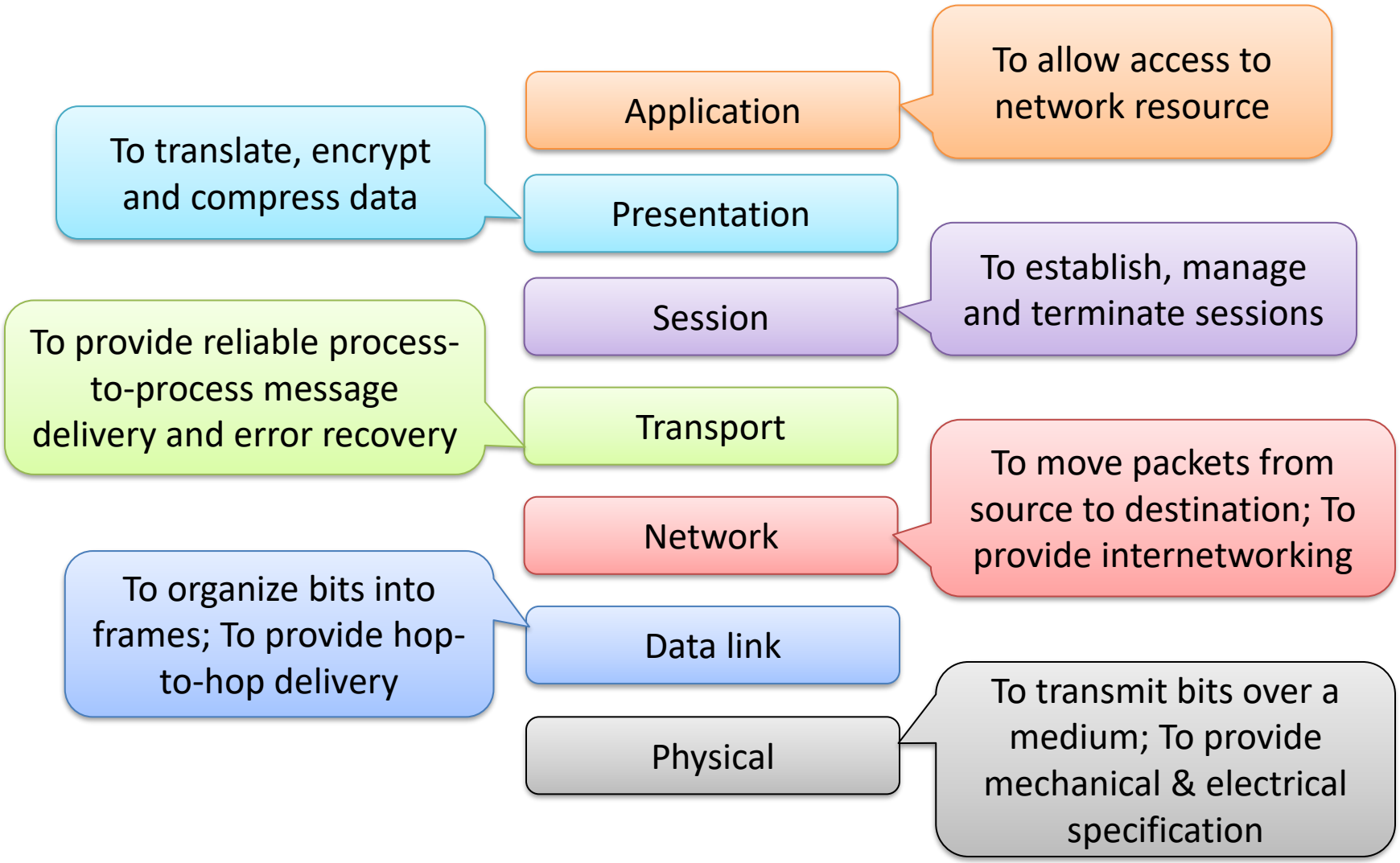


- The application layer is responsible for providing services to the user.

Application Layer – Cont…

- This layer provides various services like:
  - ✓ Network virtual terminal
  - ✓ File transfer, access and management
  - ✓ Mail services
  - ✓ Directory services

Summary – OSI Layer

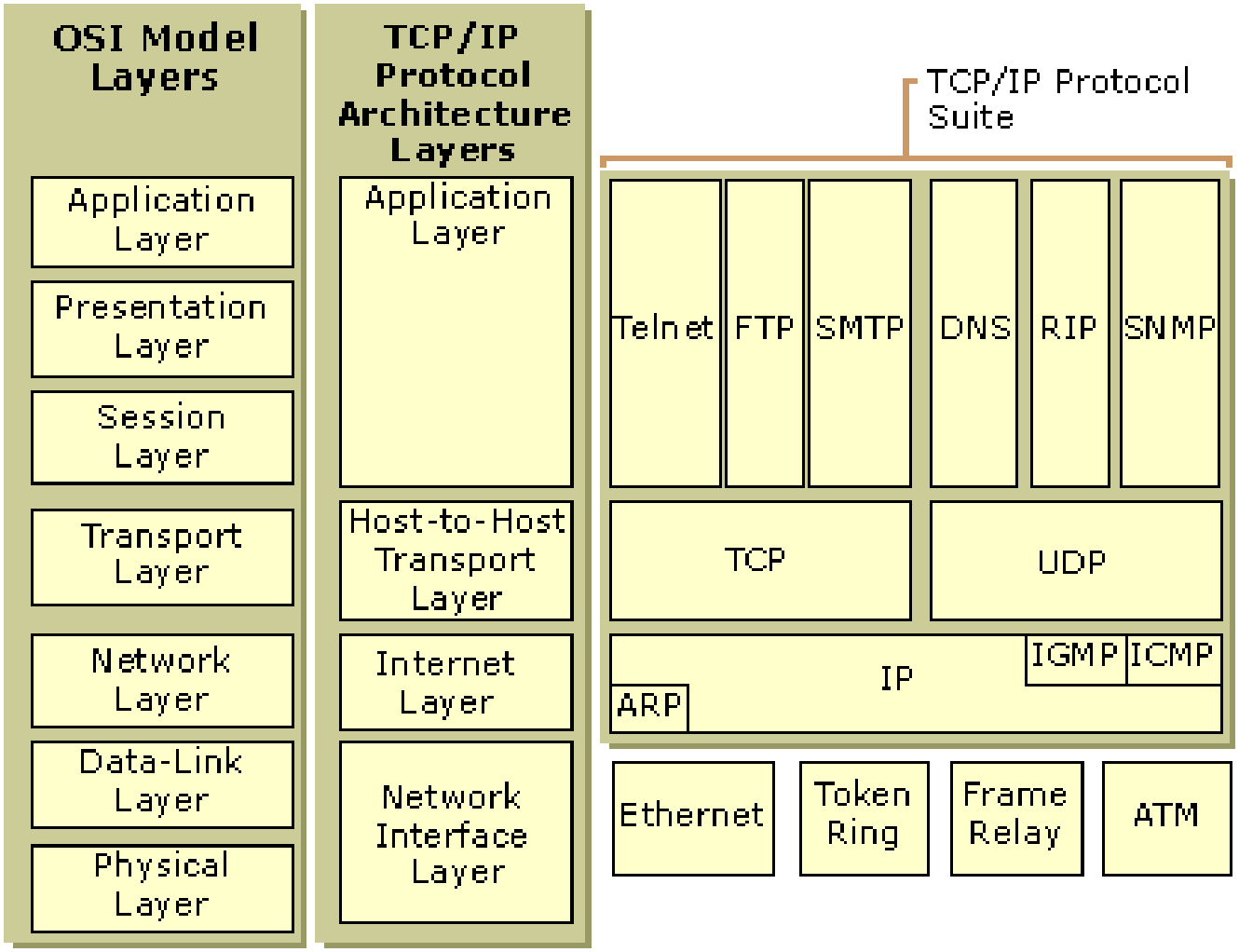


TCP/IP Reference Model

(Transmission Control Protocol/Internet Protocol)

- It was originally defined as having five layers:
- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.
  1. Application Layer
  2. Transport Layer
  3. Network Layer
  4. Data Link Layer
  5. Physical Network

TCP/IP Model Architecture



Thank You