

SUBJECT: COMPUTER NETWORK

SEM 4
AY: 2023_24

BY: PROF KANCHAN DHURI

Subject details

Course Name: Computer Networks

Course Code: IT06T


Category: Core

Preamble:

This course is to provide students with an overview of the concepts and fundamentals of computer networks. To understand the protocol layering and physical level communication. This subject will help to analyse the performance of a network. It helps to learn the functions of OSI & TCP/IP model and the various routing protocols.

Pre-requisites:

Fundamentals of Computer Hardware and Networking (ES06T)



Course Objectives:

- Discuss the fundamentals of networks for data communication and transmission.
- Describe the various techniques for both analog and digital data communication and its standards.
- Apply the various error detection and correction techniques to solve collisions problems.
- Identify and classify the various network layer protocols to apply in various networks.
- Discuss the various protocols and techniques used in transport layer and application layer.

Course Outcomes:

Students will be able to:

CO1: Describe the functions of each layer in OSI and TCP/IP model.

CO2: Explain the types of transmission media with real time applications.

CO3: Describe the functions of data link layer and explain the protocols.

CO4: Classify the routing protocols and analyze how to assign the IP addresses for the given network.

CO5: Describe the Session layer design issues and Transport layer services.

CO6: Explain the functions of Application layer and Presentation layer paradigms and Protocols.

Scheme & Evaluation Guideline

Course Scheme:

Contact Hours		Credits Assigned	
Theory	Practical	Theory	Practical
2	-	2	-

Assessment guidelines:

Head of Learning	ISA	MSE	ESE	Total
Theory	15	20	40	075

MODULES

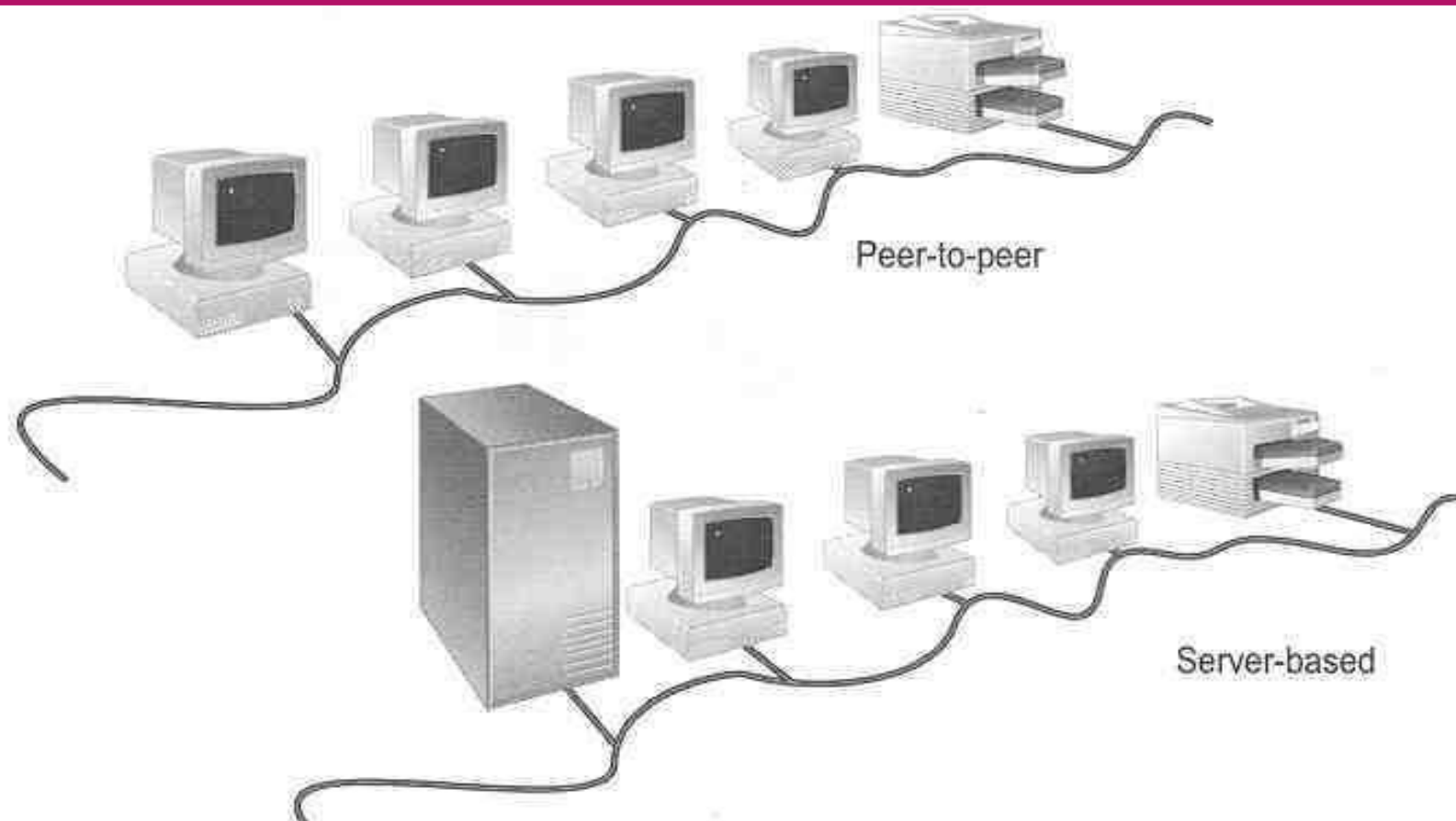
1. Introduction to Computer Network
2. The Physical Layer
3. The Data Link Layer
4. The Network Layer
5. Transportation and Session Layer
6. Presentation and Application and layer

Contents:

- What are Networks
- Network Criteria
- Network Types
- OSI Reference Model
- TCP/IP Model
- Comparison of OSI and TCP/IP
- Network Devices

MODULE 1

INTRODUCTION TO Computer Network





What are NETWORKS?

Network is a system.

Network is a communication system which supports many users.

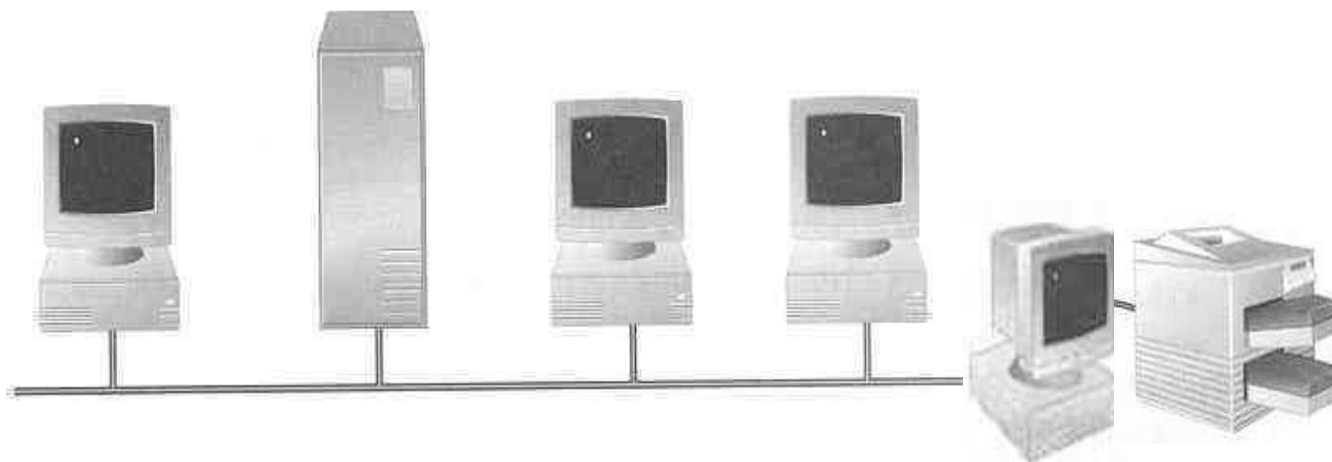
The interconnection of one station to many stations is called networking.

A network is any interconnection of two or more stations that wish to communicate.

Each station in a communication network is called as a node.

Continued...

- ▶ A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.





definition

A computer network is a group of computers & other computing hardware devices are linked together through communication channels to facilitate communication & resource sharing among wide range of users.

Applications of Networks

❏ **Resource Sharing**

- ❏ Hardware (computing resources, disks, printers)
- ❏ Software (application software)

❏ **Information Sharing**

- ❏ Easy accessibility from anywhere (files, databases)
- ❏ Search Capability (WWW)

❏ **Communication**

- ❏ Email
- ❏ Message broadcast

❏ **Remote computing**

❏ **Distributed processing (GRID Computing)**

Information sharing

Email Attachments: One of the simplest ways to share data is by attaching files to emails. This is suitable for small to moderately sized files.

File Transfer Protocols:

FTP (File Transfer Protocol): Allows the transfer of files between computers on a network.

SFTP (Secure File Transfer Protocol): A secure version of FTP that encrypts the data during transfer.

SCP (Secure Copy Protocol): A secure means of copying files between computers.

Cloud Storage Services:

Google Drive, Dropbox, OneDrive: These services allow users to upload, store, and share files in the cloud. Links can be shared with specific individuals or made public.

Box, Amazon S3: Other cloud storage services with various features for data sharing and collaboration.

Collaboration Platforms:

Microsoft Teams, Slack: These platforms include features for team collaboration, file sharing, and communication.

Asana, Trello: Project management tools that often include file-sharing capabilities.



Continued...

Version Control Systems:

1. Git, SVN: These are primarily used for code versioning but can also be used for sharing and collaborating on data files.

Data Sharing Platforms:

1. Figshare, Zenodo: Platforms designed specifically for sharing and publishing research data.
2. Kaggle, GitHub (for data): Platforms where data scientists and researchers share datasets for collaboration and competition.

Peer-to-Peer Sharing:

1. BitTorrent: Used for distributing large amounts of data efficiently by allowing users to download and share files simultaneously.

Database Sharing:

- MySQL, PostgreSQL: Databases that can be accessed and shared among authorized users.
- Firebase, MongoDB Atlas: Cloud-based databases with easy sharing and access controls.



APIs (Application Programming Interfaces):

1. RESTful APIs, GraphQL: Allow programmatic access to data, enabling automated data sharing between systems.

Collaborative Document Editing:

1. Google Docs, Microsoft Office Online: Enable real-time collaboration on documents, spreadsheets, and presentations.

Apps for communication

1.Email:

1. **Gmail, Outlook, Yahoo Mail:** Traditional email platforms for sending and receiving messages.

2.Instant Messaging and Chat:

1. **WhatsApp, Telegram, Signal:** Messaging apps for instant text, voice, and video communication.
2. **Slack, Microsoft Teams:** Collaboration platforms with chat functionality, often used in professional settings.

3.Video Conferencing:

1. **Zoom, Microsoft Teams, Google Meet:** Platforms for hosting virtual meetings with video and audio capabilities.

4.Voice Calls:

1. **Skype, Viber:** Applications that allow users to make voice calls over the internet.

5.Social Media Messaging:

1. **Facebook Messenger, Instagram Direct, Twitter DMs:** Social media platforms with messaging features.



1. Collaborative Document Editing with Communication:

1. **Google Docs, Microsoft Office Online:** Platforms that enable real-time collaboration on documents with integrated communication features.

2. Unified Communication Platforms:

1. **Cisco Webex, RingCentral:** Platforms that integrate various communication tools, including voice, video, and messaging.

3. Project Management Communication:

1. **Asana, Trello:** Project management tools with built-in communication features for team collaboration.

4. Collaboration Suites:

1. **Microsoft 365 (formerly Office 365), Google Workspace:** Suites of productivity tools that include email, document editing, and communication applications.

5. Team Collaboration Apps:

1. **Slack, Mattermost:** Apps focused on team communication, combining channels, messaging, and integrations.



1.VoIP (Voice over Internet Protocol):

1. **Skype, WhatsApp (for voice calls):** Apps that allow voice calls over the internet, often at lower costs than traditional phone calls.

2.Forums and Discussion Boards:

1. **Reddit, Stack Exchange:** Platforms for asynchronous communication and discussion on various topics.

3.Telephony and Video Calling Apps:

1. **Viber, Google Duo:** Apps that support both voice and video calls over the internet.

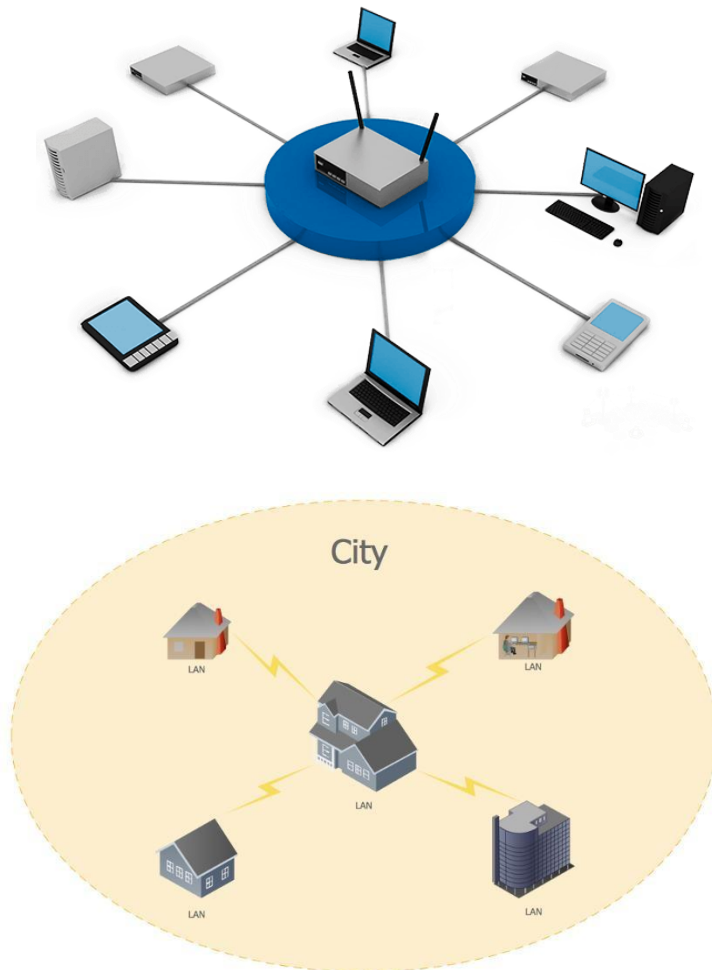
4.Internal Communication Apps:

1. **Slack, Microsoft Teams:** Used for internal communication within organizations, providing chat, channels, and collaboration features.

5.File Sharing and Communication:

1. **Telegram, Signal:** Apps that combine secure messaging with file-sharing capabilities.

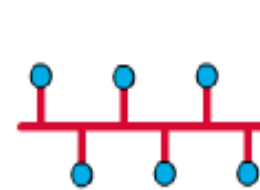
***SO HOW DO YOU CONNECT/PLACE
DEVICES IN A NETWORKS!!!!!!***



TOPOLOGIES OF NETWORK???

Network Topology

■ The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



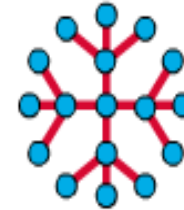
Bus Topology



Ring Topology



Star Topology

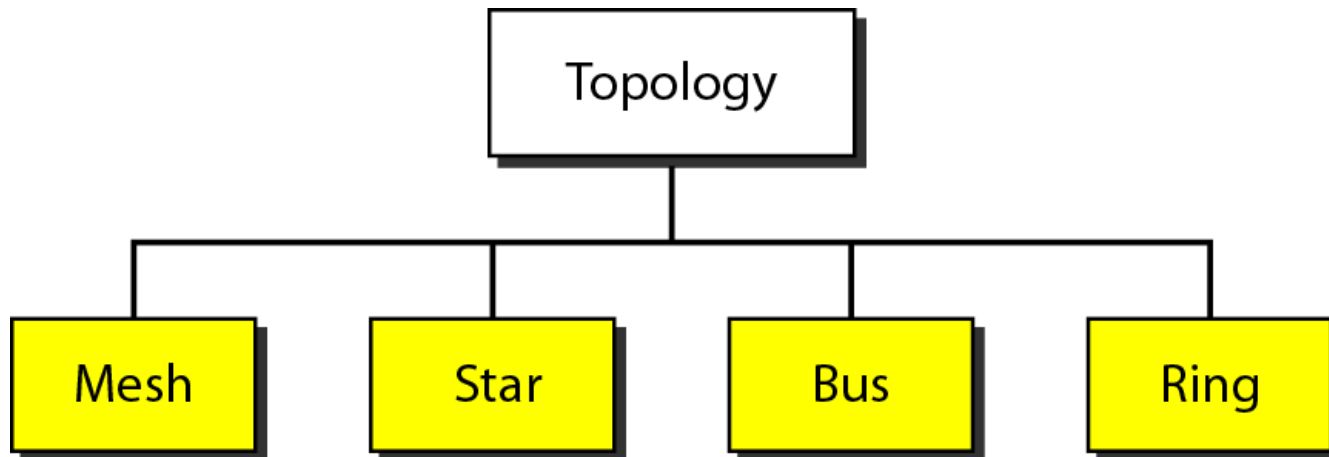


Extended Star Topology

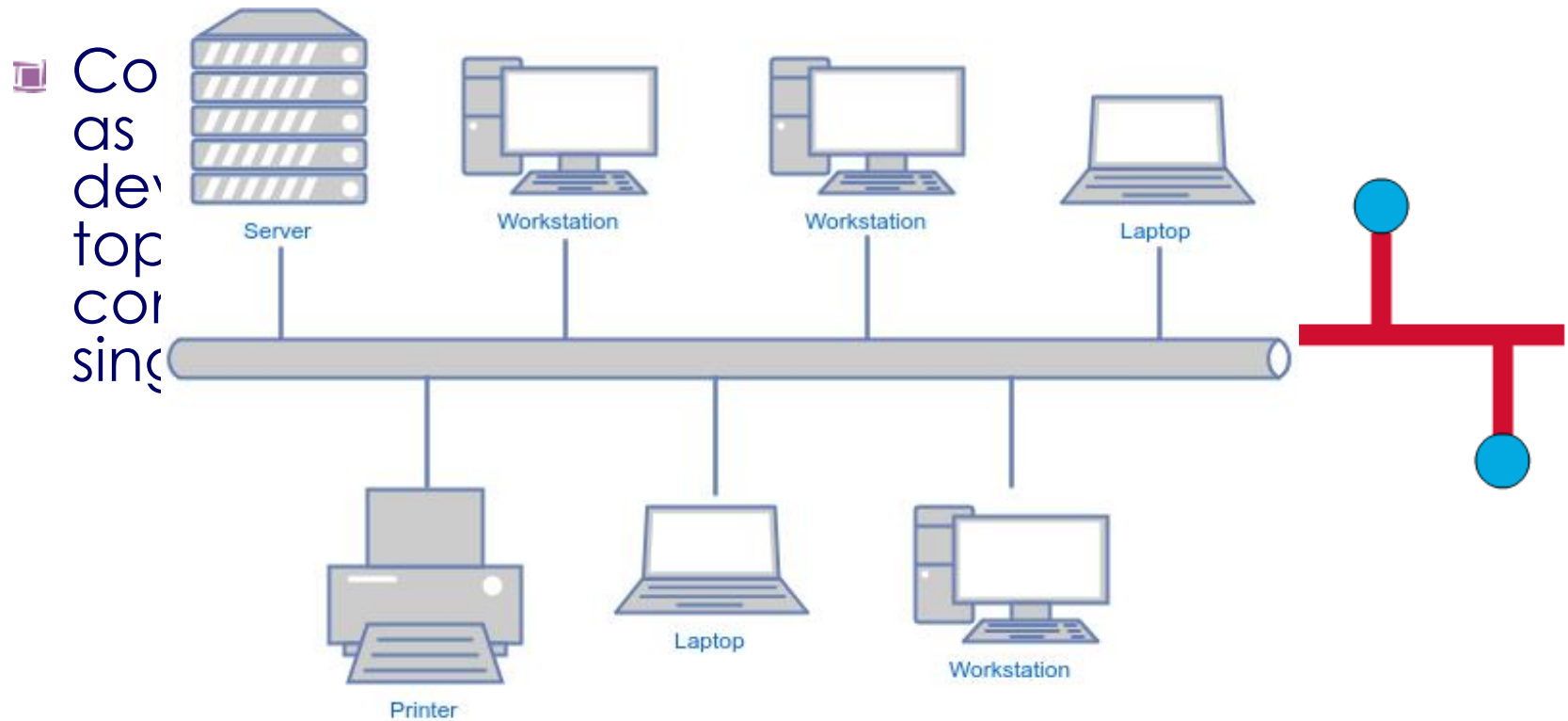


Mesh Topology

Categories of topology



Bus Topology



Bus Topology Network

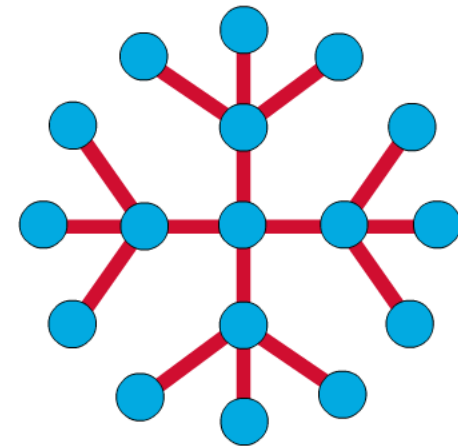
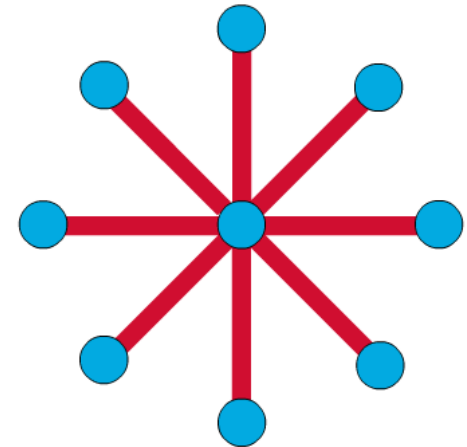
BUS

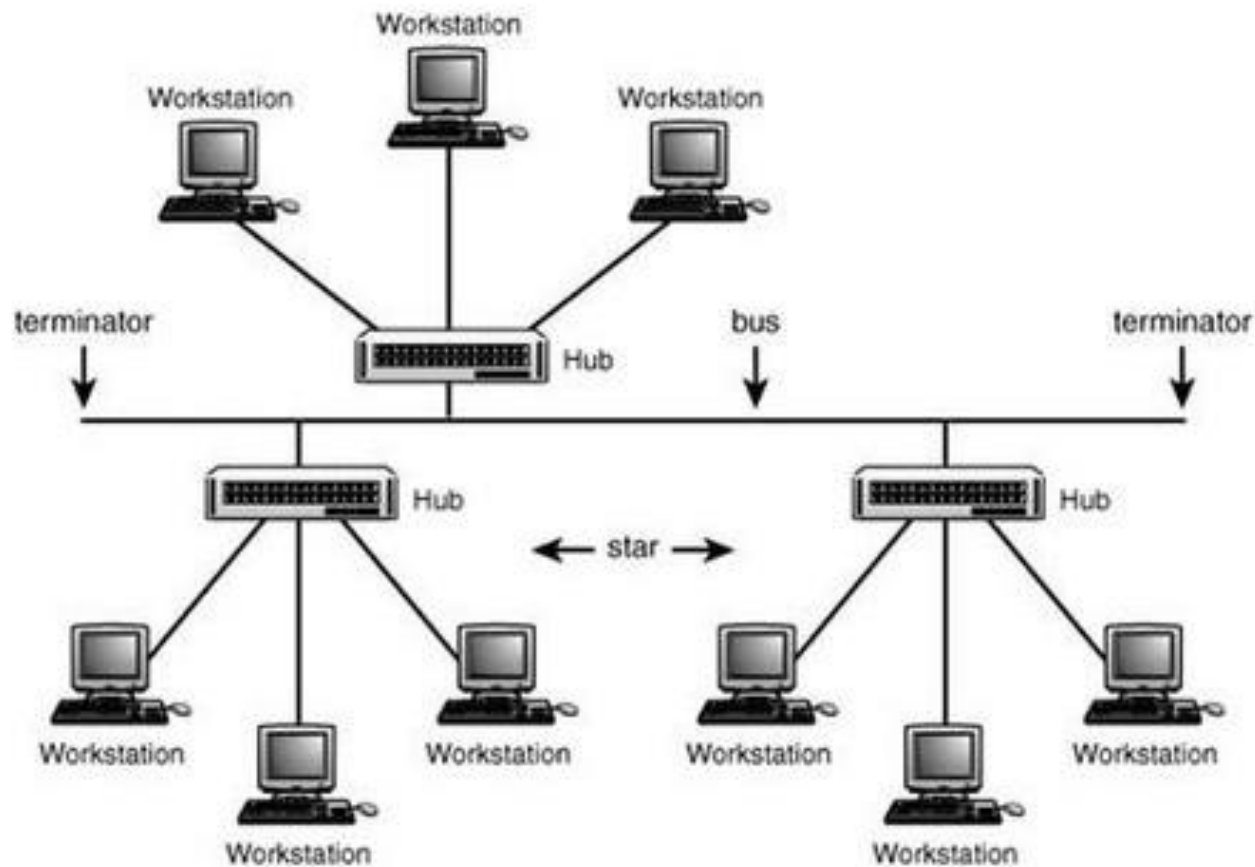
- ▶ A bus is the simplest physical topology. It consists of a single cable that runs to every workstation
- ▶ This topology uses the least amount of cabling, but also covers the shortest amount of distance.
- ▶ Each computer shares the same data and address path. With a logical bus topology, messages pass through the trunk, and each workstation checks to see if the message is addressed to itself. If the address of the message matches the workstation's address, the network adapter copies the message to the card's on-board memory.

Star & Tree Topology

18

- ❑ The star topology is the most commonly used architecture in Ethernet LANs.
- ❑ When installed, the star topology resembles spokes in a bicycle wheel.
- ❑ Larger networks use the extended star topology also called tree topology. When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



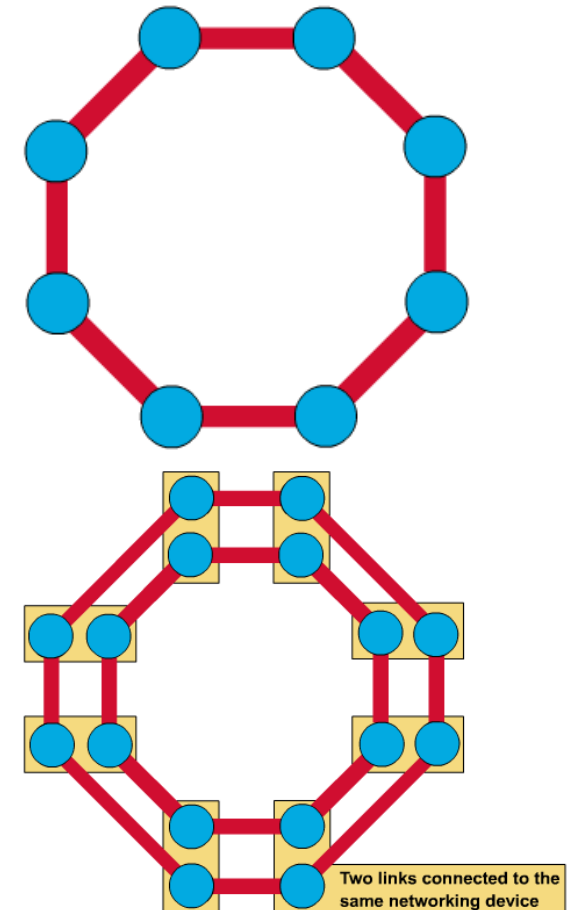


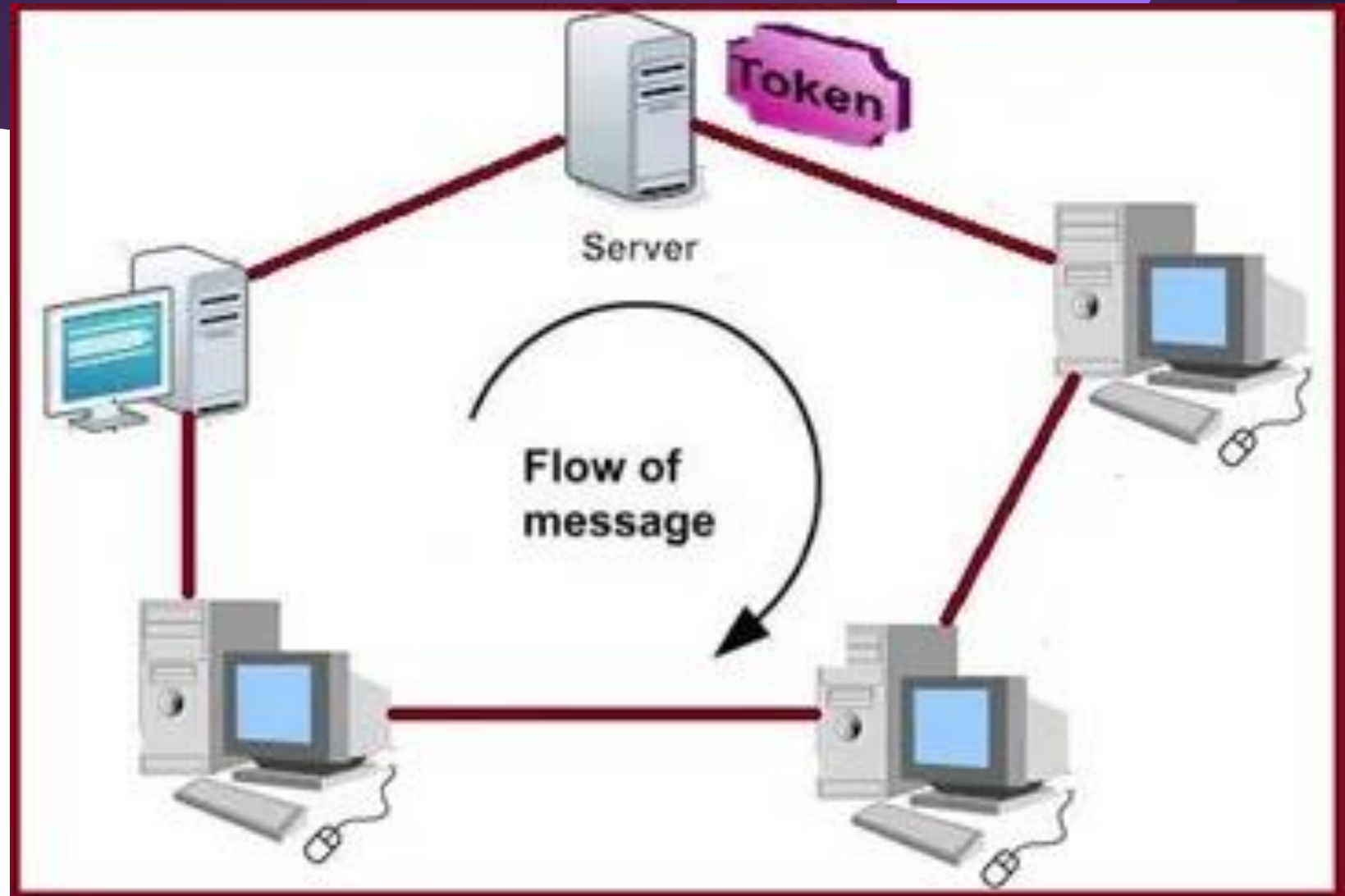
TREE TOPOLOGY

Ring Topology

20

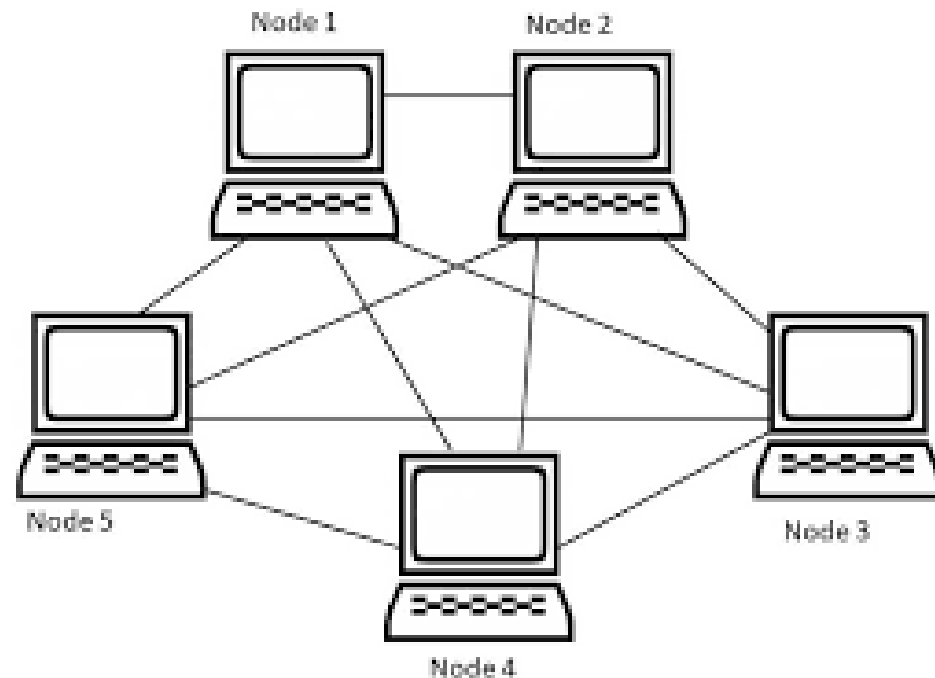
- A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.
- The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.
 - Single ring – All the devices on the network share a single cable
 - Dual ring – The dual ring topology allows data to be sent in both directions.





Mesh Topology

- The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- It is used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.
- Implementing the mesh topology is expensive and difficult.

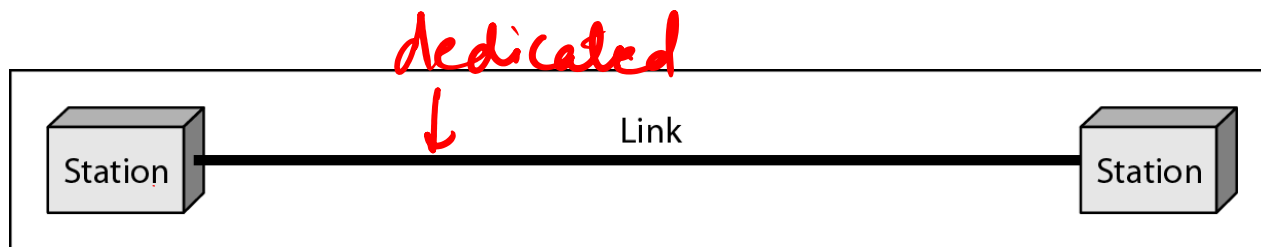


Network Criteria

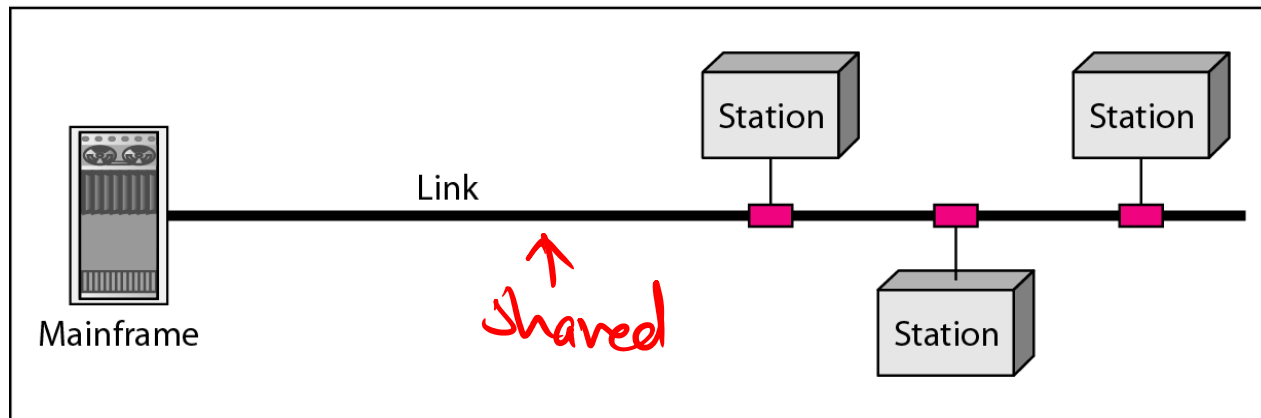
- ▶ Performance
 - ▶ Depends on Network Elements
 - ▶ Measured in terms of Delay and Throughput
- ▶ Reliability
 - ▶ Failure rate of network components
 - ▶ Measured in terms of availability/robustness
- ▶ Security
 - ▶ Data protection against corruption/loss of data due to:
 - ▶ Errors
 - ▶ Malicious users

TYPES OF CONNECTION A NETWORK CAN HAVE!!!

Types of connections: point-to-point and multipoint



a. Point-to-point



b. Multipoint

Types of communication

- ✓ *unidirectional* ▶ **Simplex:** ✓ radio broadcasting, ✓ television broadcasting, ✓ computer to printer communication, and keyboard to computer connections.
- ✓ ▶ **Half duplex:** *Bidirectional* ✓ walkie-talkie, a two-way radio that has a push-to-talk button.
- ✓ ▶ **Full duplex:** Telephone system *bidirectional*

NETWORK ARCHITECTURE

- ▶ Network Architecture is made of
 - ❖ Network Hardware
 - ❖ Network Software
 - ❖ Communication Medium

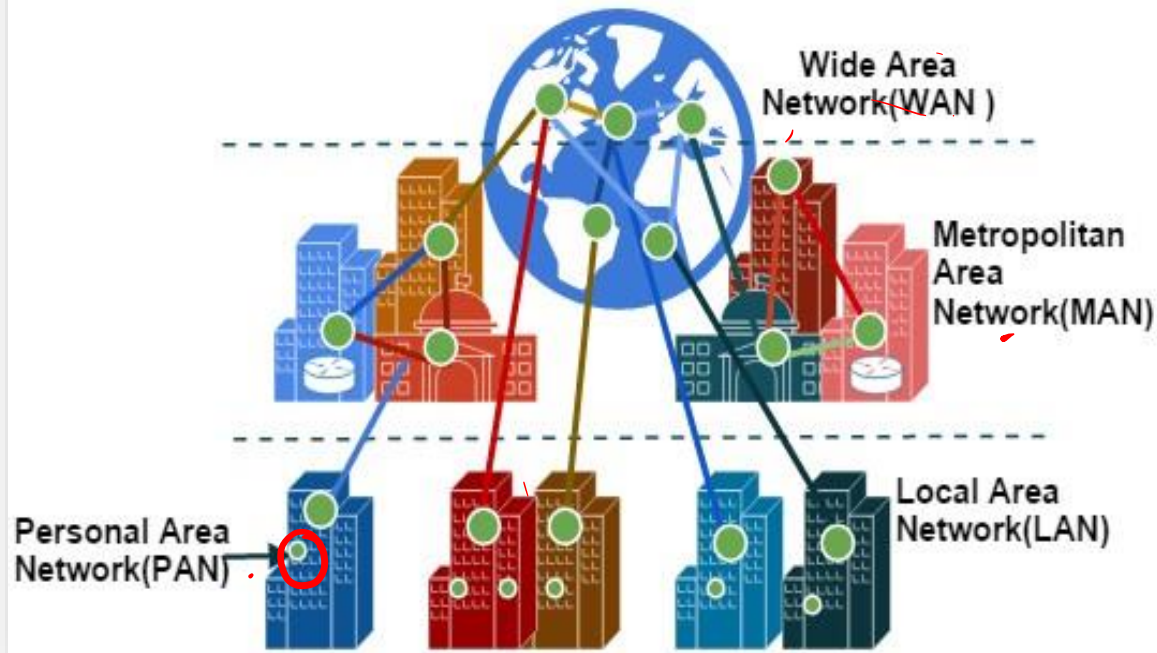
LAN, MAN & WAN

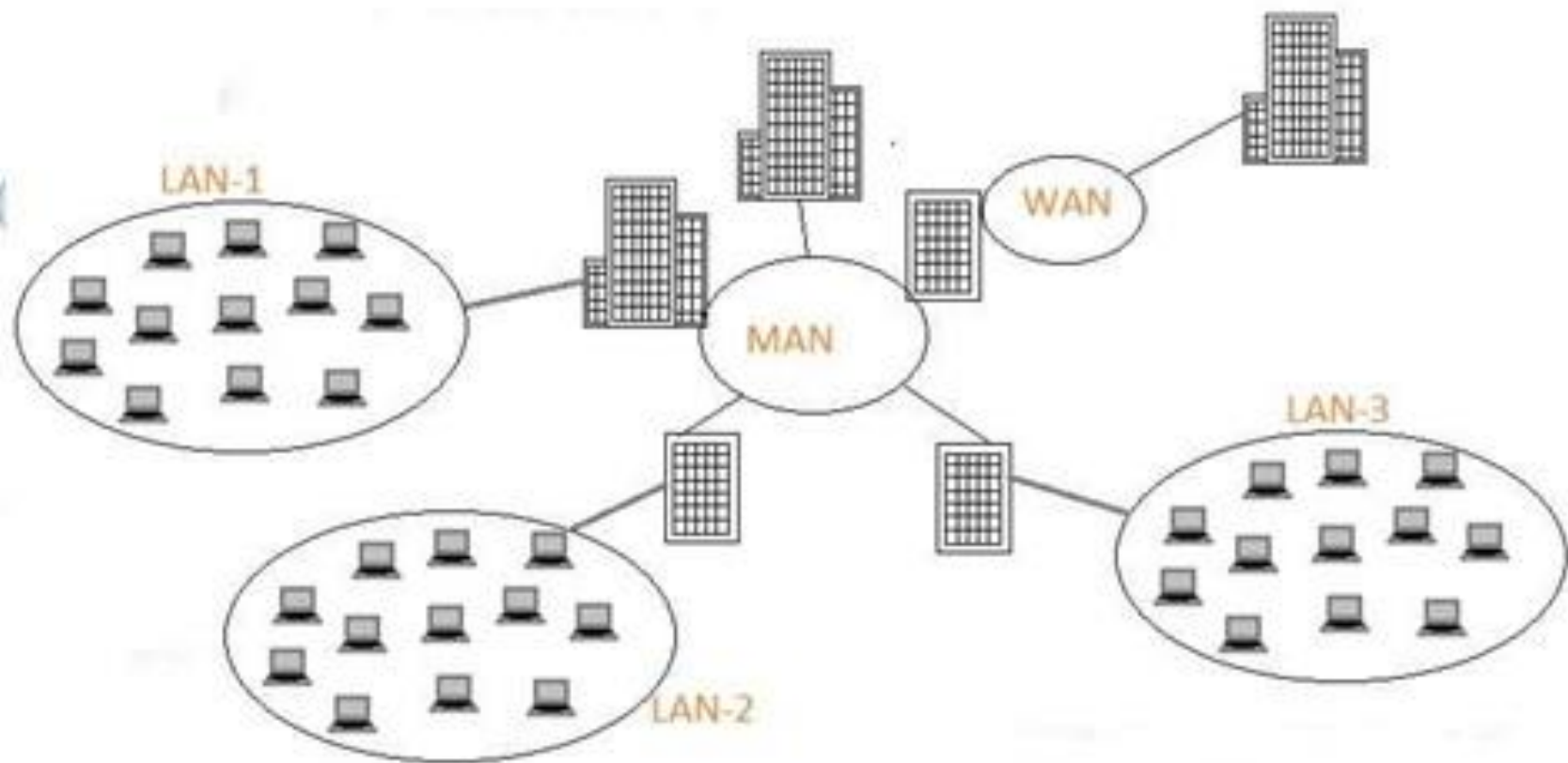
11

- ❏ Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)
- ❏ Network in a City is called MA (Metropolitan Area Network)
- ❏ Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)

LAN, MAN and WAN

Types of Computer Networks





Categories of Networks

- ▶ **Local Area Networks (LANs)**

- ✓ ▶ Short distances

- ✓ ▶ Designed to provide local interconnectivity

- ▶ **Wide Area Networks (WANs)**

- ▶ Long distances

- ▶ Provide connectivity over large areas

- ▶ **Metropolitan Area Networks (MANs)**

- ▶ Provide connectivity over areas such as a city, a campus

Based on physical size

Distance	Example of network	Area
10m	LAN	Same room
100m	LAN	Same building
1Km	LAN	Same campus
10Km	MAN	Same city
100Km	WAN	Same state
1000Km	WAN	Same continent
10,000Km	Internet	Same Planet

LAN: LOCAL AREA NETWORK

- A **Local Area Network (LAN)** is a **collection of networking equipment** located geographically **close together**. E.g. **Single room, campus** etc.
- **Data transferred** in High speed which **ranges from 10 Mbps to 16 Gbps** for **system development** and have a **low implementation cost**.
- Upper limit: **10 km** ; Lower limit: **1 km**
- **Twisted pair cable or Co-axial cable** connects the **plug in cards** to form a network.
- Designed to **share resources** between **PCs and workstation** such as **hardware or data**.
- Local Area Networks are privately-owned networks within a small area, usually a single building or campus of up to a few kilometers.
- Since it is restricted in size, that means their data transmission time can be known in advance, and the network management would be easier.
- Topologies can be used Bus, Ring, Star, Tree etc.

Motivations for Local Area Networking

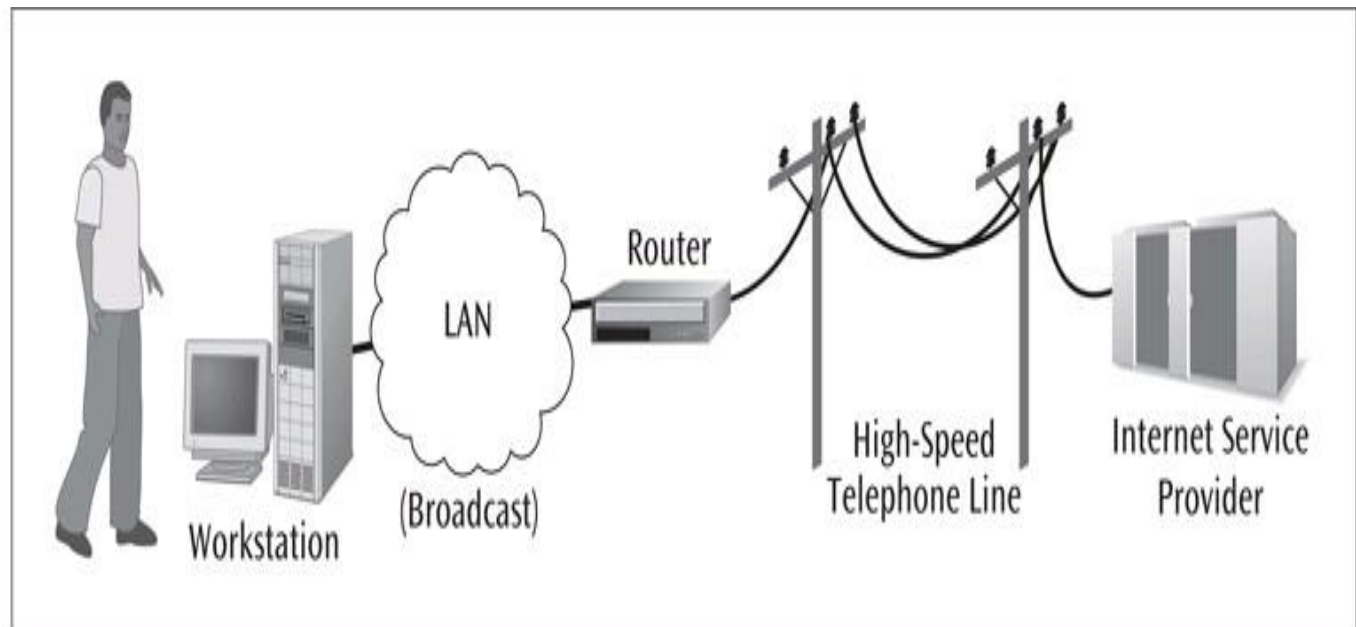
36

- The growing demand for local area networks is due to technical, economic and organizational factors:
 - ❖ Cost reductions through sharing of information and databases, resources and Network services.
 - ❖ Increased information exchange between different departments in an organization, or between individuals.
 - ❖ The trend to automate communication and manufacturing process.
 - ❖ Improve the community security.
 - ❖ Increasing number and variety of intelligent data terminals, PCs and workstations.

USAGE OF LAN

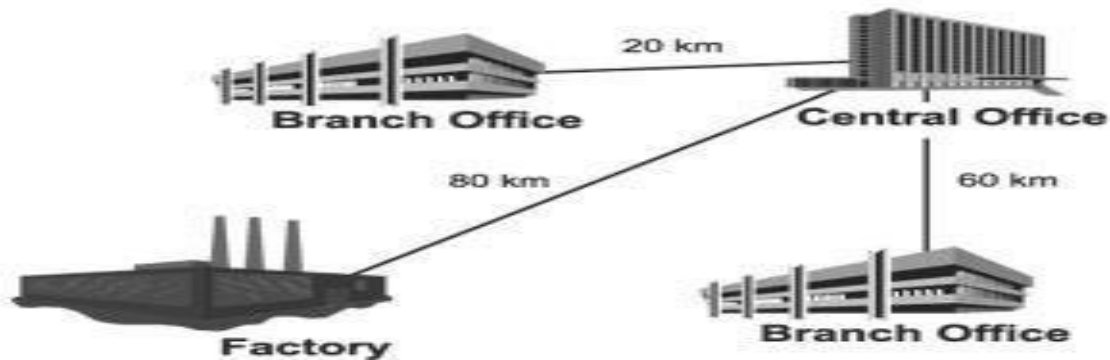
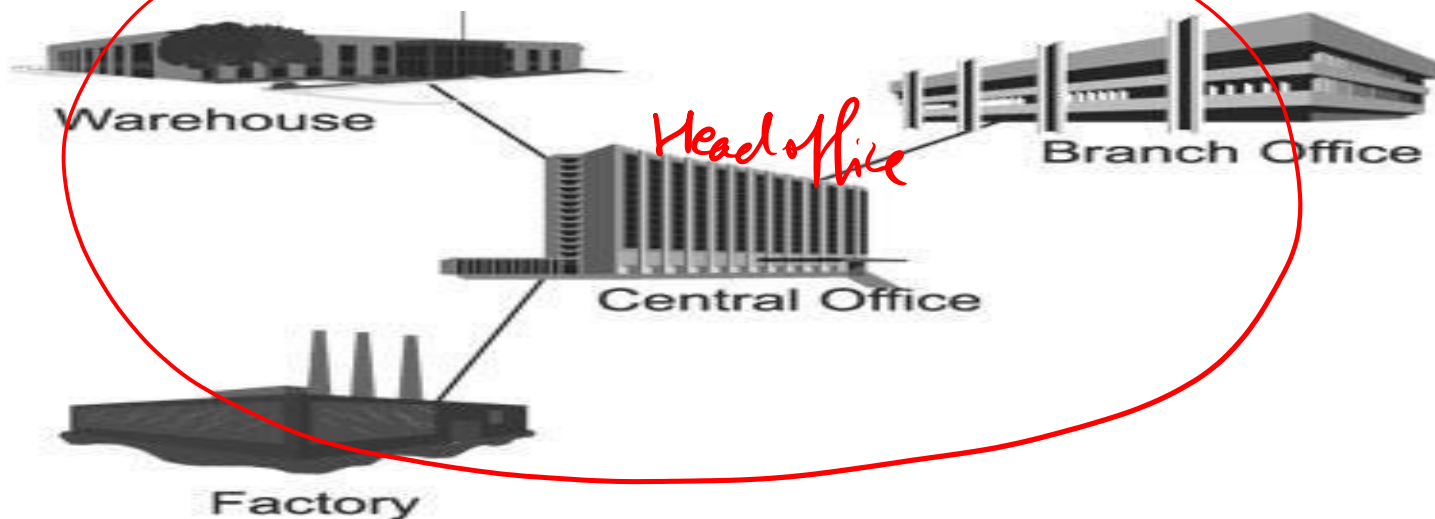
Figure 9-16

User at work using a local area network to access the Internet



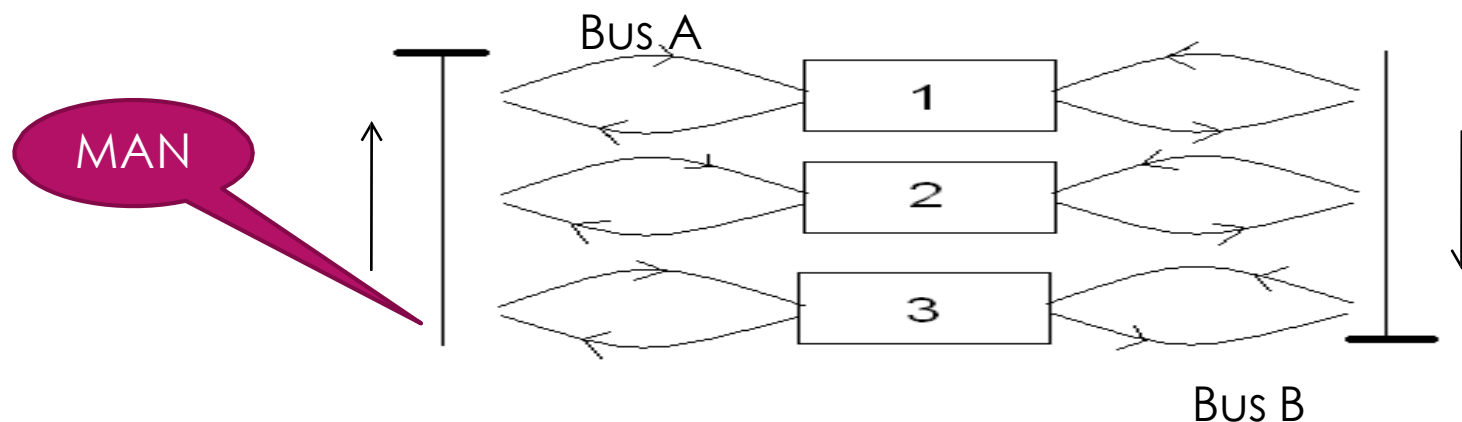
A work to internet connections would most likely require broadcast network (LAN) with a connection to the internet (packet switched network)

MAN: METROPOLITAN AREA NETWORK



MAN

- The **metropolitan area network (MAN)** is designed to extend over an entire **city**.
- It may be a **single network such as cable television network** available in many cities.
- It can be a combination of multiple LANs
- Range: Within **100 km** (a city).

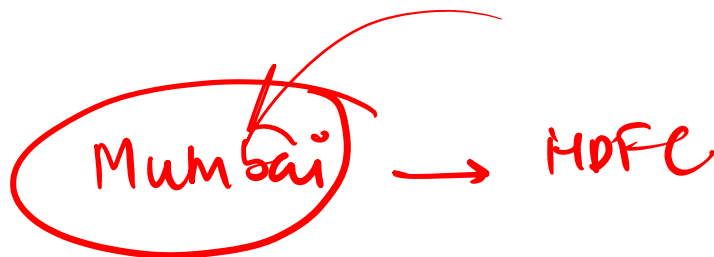


Metropolitan area network

- ▶ A *Metropolitan Area Network* (MAN) is a network that is utilized across multiple buildings
- ▶ Commonly used in school campuses or large companies with multiple buildings
- ▶ Is larger than a LAN, but smaller than a WAN
- ▶ Is also used to mean the interconnection of several LANs by bridging them together. This sort of network is also referred to as a campus network (MAN)

Metropolitan Area Networks (MANs)

- ▶ A Metropolitan Area Network is a system of LANs connected throughout a city or metropolitan area. MANs have the requirement of using telecommunication media such as voice channels or data channels.
- ▶ Branch offices are connected to head offices through MANs. Examples of organizations that use MANs are universities and colleges, grocery chains, and banks.



WAN: WIDE AREA NETWORK

- Network that provides long distance transmission of data, voice, image and video information over large geographical areas that may comprise a country, a continent.
- Range: Beyond 100 km.
- Ex. Airline reservation system



Wide area network

- ▶ A *Wide Area Network* is a network spanning a large geographical area of around several hundred miles to across the globe
- ▶ May be privately owned or leased
- ▶ Also called “enterprise networks” if they are privately owned by a large company
- ▶ It can be leased through one or several carriers (ISPs-Internet Service Providers) such as AT&T, Sprint, Cable and Wireless
- ▶ Can be connected through cable, fiber or satellite
- ▶ Is typically slower and less reliable than a LAN
- ▶ Services include internet, frame relay, ATM (Asynchronous Transfer Mode)
- ▶ Communication can be established using leased telephone lines or satellite links & similar channels.

Features of WAN

Remote data entry & access is possible.

Communication facility is provided.

Centralized information is created & used.

WAN span over a large distance.

It can use the pre-existing PSTN for the links

Provides long distance transmission of data, images & video information.

Comparison between LAN, MAN, WAN

LAN	MAN	WAN
LAN is referred to as Local Area Networks.	MAN is referred to as Metropolitan Area Networks.	WAN is referred to as Wide Area Networks.
Ownership of LAN is private.	Ownership of MAN can be public or private.	Ownership of WAN might not be owned by one organization.
LANs transmit data at high speeds.	The speed of transmission of MAN is average.	WANs transmit data at low speeds.
LAN propagation delays are short.	MAN propagation delays are moderate.	WAN propagation delays are quite long.
LANs tend to be less congested.	MANs tend to be more congested.	WAN is more congested than MAN.
LAN's maintenance and design are easy.	MAN's maintenance and design are more difficult than LAN.	WAN's maintenance and design are also more difficult than LAN as well as MAN.
LAN has more fault tolerance.	MAN has less fault tolerance.	WAN has also less fault tolerance.

BASIS		LAN	MAN	WAN
Full Form	Local Area Network		Metropolitan Area Network	Wide Area Network
Range	A communication network linking a number of stations in same local area. Range is 1 to 10 km		This network shares the characteristics of packet broadcasting networks. Range is 100 km	A communication network distinguished from a Local Area Network. Range is Beyond 100 km
Media Used	Uses guided media		Uses guided as well as unguided media	Uses unguided media
Speed	A high speed i.e. 100kbps to 100mbps		Optimized for a large geographical area than LAN.	Long distance communications, which may or may not be provided by public packet network.
Cost	cheaper		costly	expensive
Equipment needed	NIC, switch and hub		Modem and router	Microwave, radio, infra-red laser
protocols	Attached Resource		Frame relay and	ATM, FDDI, SMDS

Connection oriented Services

Ex. Telephone line

Sequence of operations:

1. Establish a connection
2. use the connection
3. Release the connection

Maintains the sequence of bit transmission

Connection oriented

- ▶ The best ex for connection oriented service is telephone system.
- ▶ The following sequence of operation are:
 - Establish a connection
 - Use the connection
 - Release the connection
- The sequence of order is generally preserved here. It establishes a dedicated connection between users before data is exchanged.
- This type of connection establishment needs some form of resource reservation(BW).
- After the connection the actual data transfer takes place. After the exchange the connection is cleared or broken.

Connectionless services

Ex. Postal service

Each message carries the full address of the destination.

Each message is routed independently from source to destination through the system

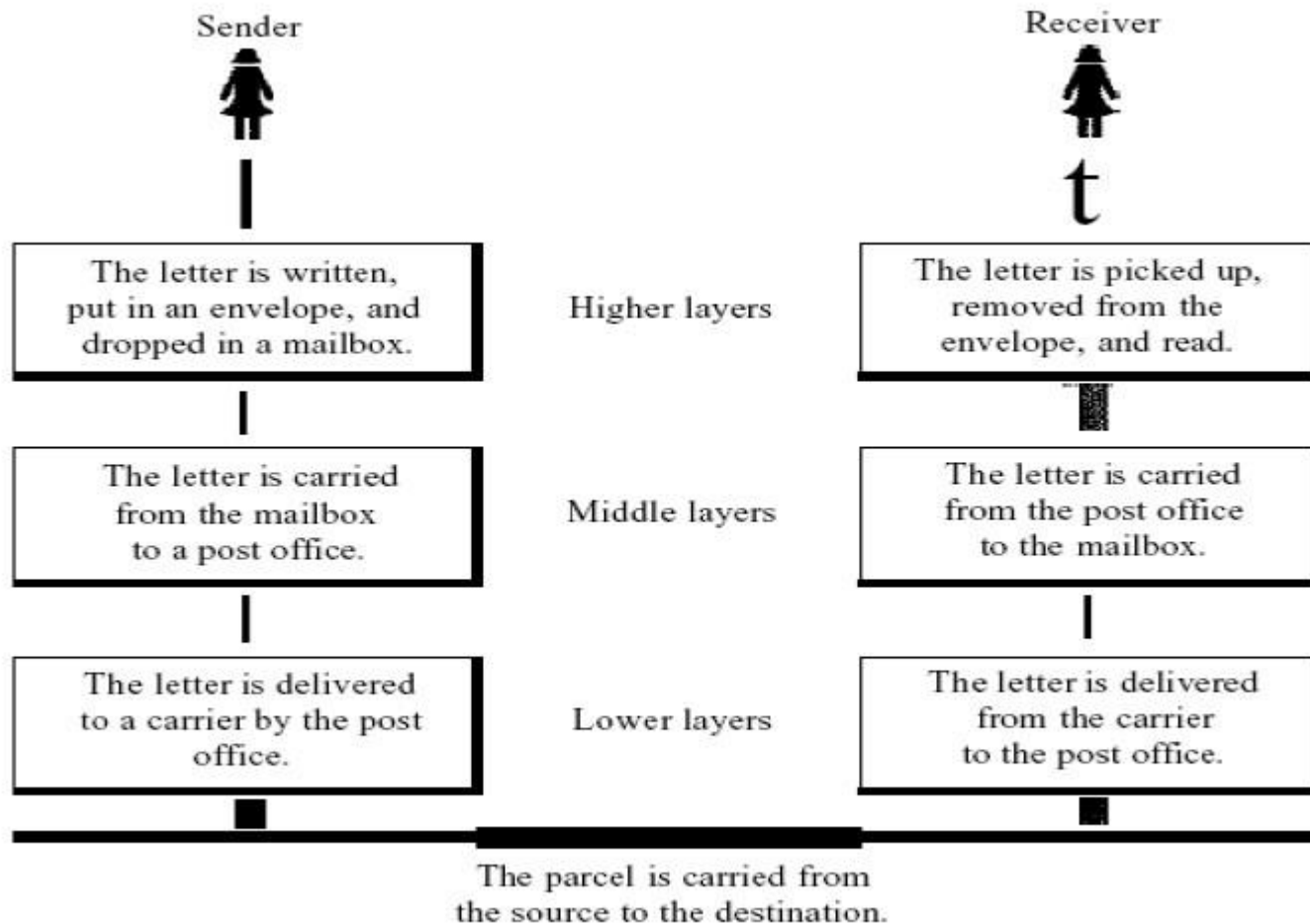
Sequence of data transmission can not be maintained

Difference between connection oriented and connection less service

56

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

Layered Task



Layered task

Sender

Receiver

Get the gift.
Pack it in a box.
Write destination address on
the box.

Receive the box
Unpack it
See the gift

Carry the box to the courier's
office.

The box is carried to the
destination address

Give the box to the person
who takes it to the
destination city.

Box is delivered to the courier
company's office in
destination city

Box carried from the source to destination

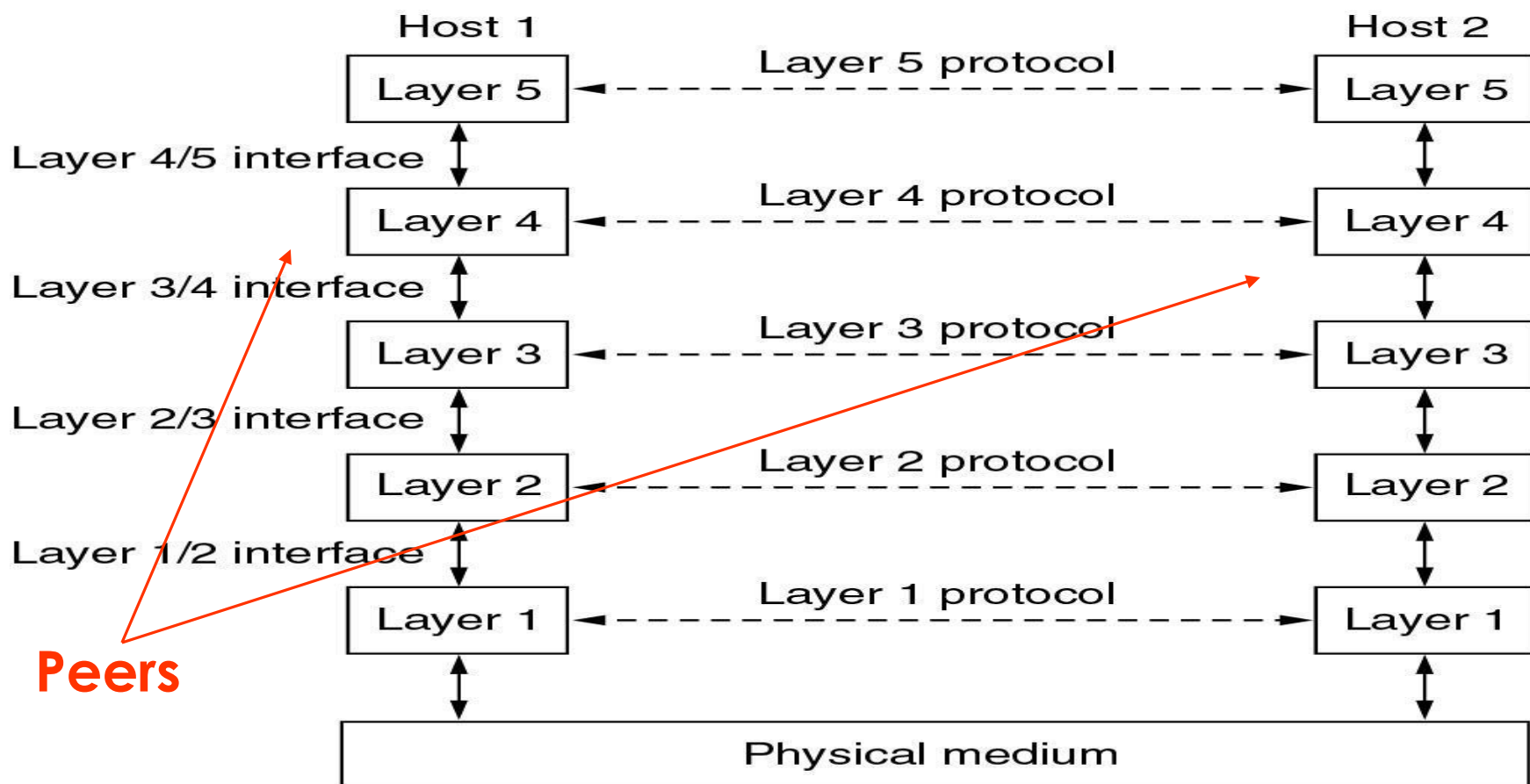
NETWORK SOFTWARE

A single layer protocol

A single-layer protocol



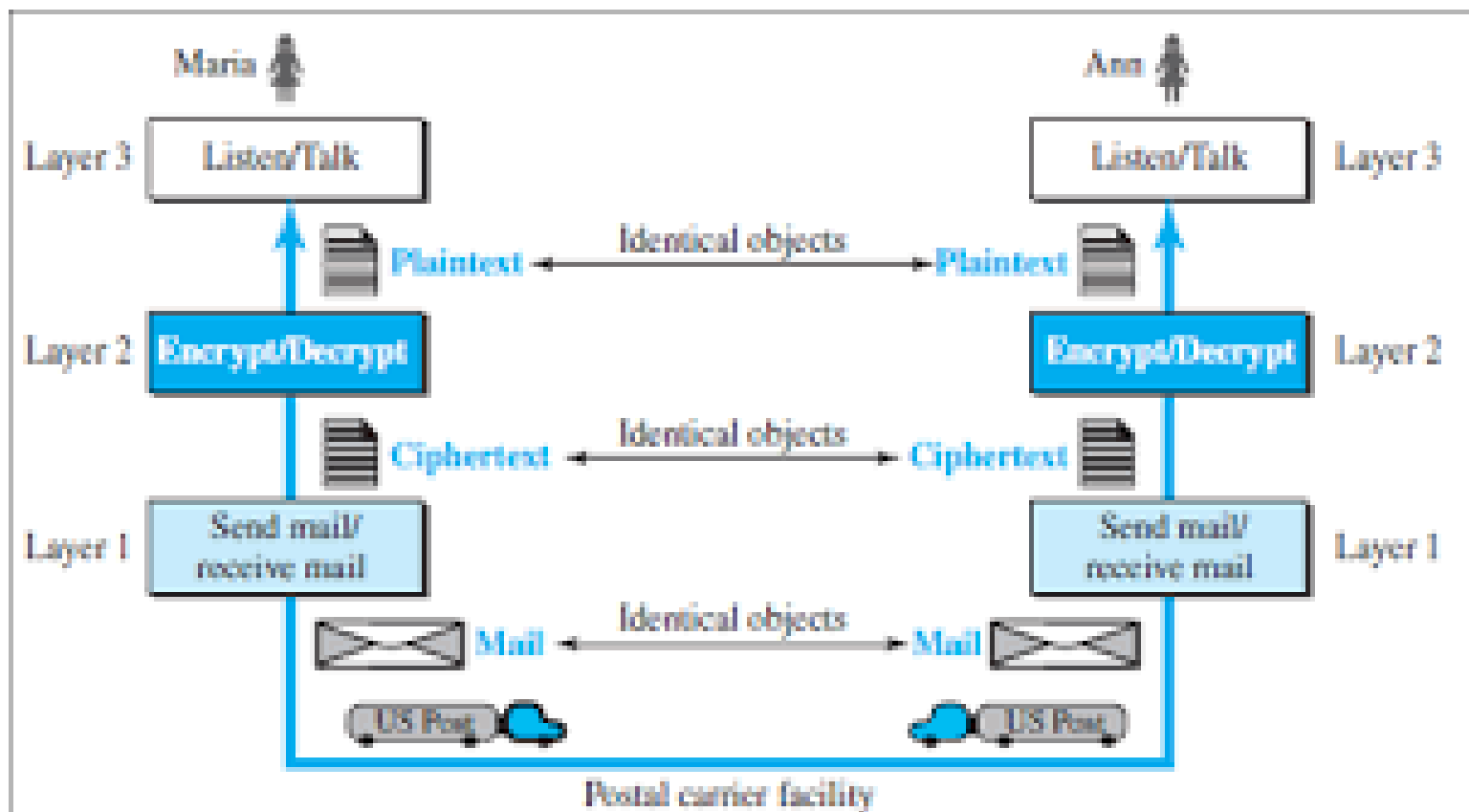
Layered Approach



Layered Approach

- The entities comprising the corresponding layers on different machines are called **peers**
- It is the peers that communicate by using the protocols. Protocols –Rules & conventions used in this communication. It is an agreement between the two communicating machines about how the communication link should be established, maintained & released.
- Actually, data is **not** transferred from layer n on one machine to layer n on another machine
- Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached
- Actual data communication takes place through the lowest layer – the **physical layer**
- **The purpose of each layer is to offer certain services to the higher layers.**

A three layer protocol



2.1.3 Logical Connections

- Layer-to-layer communication.

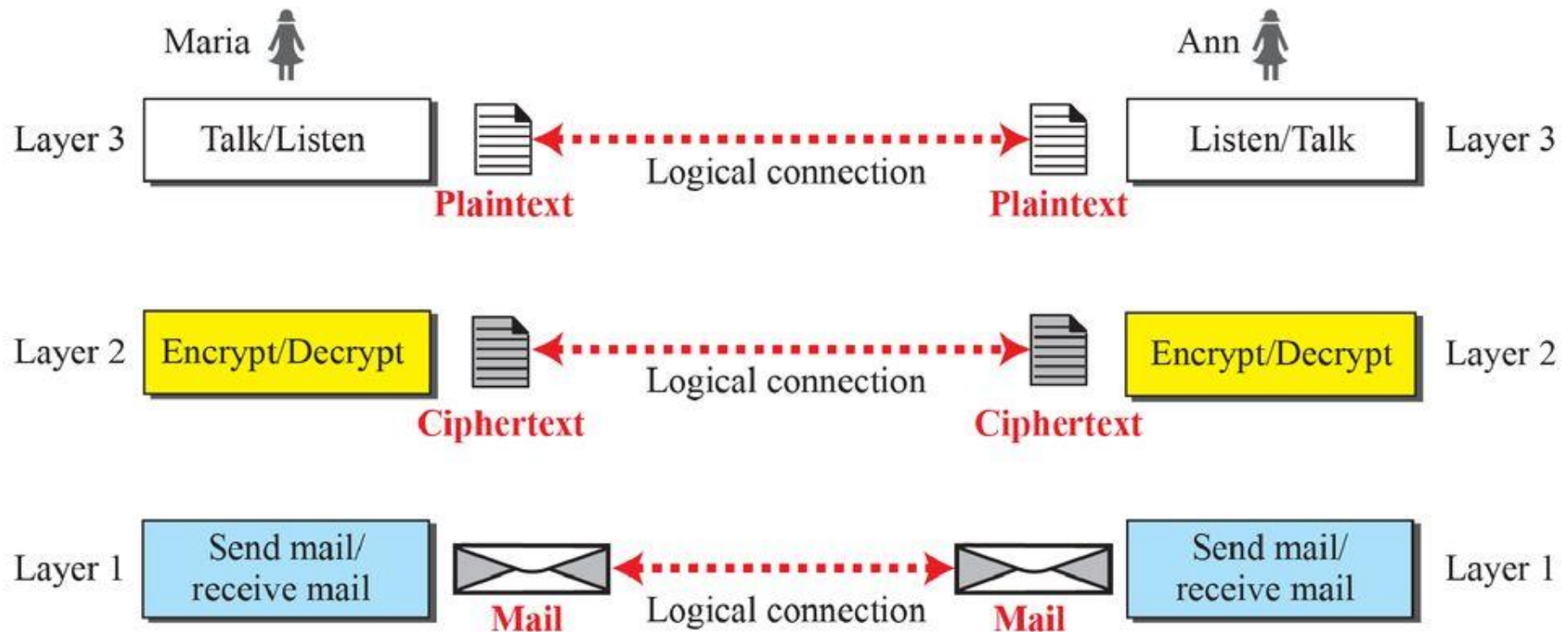
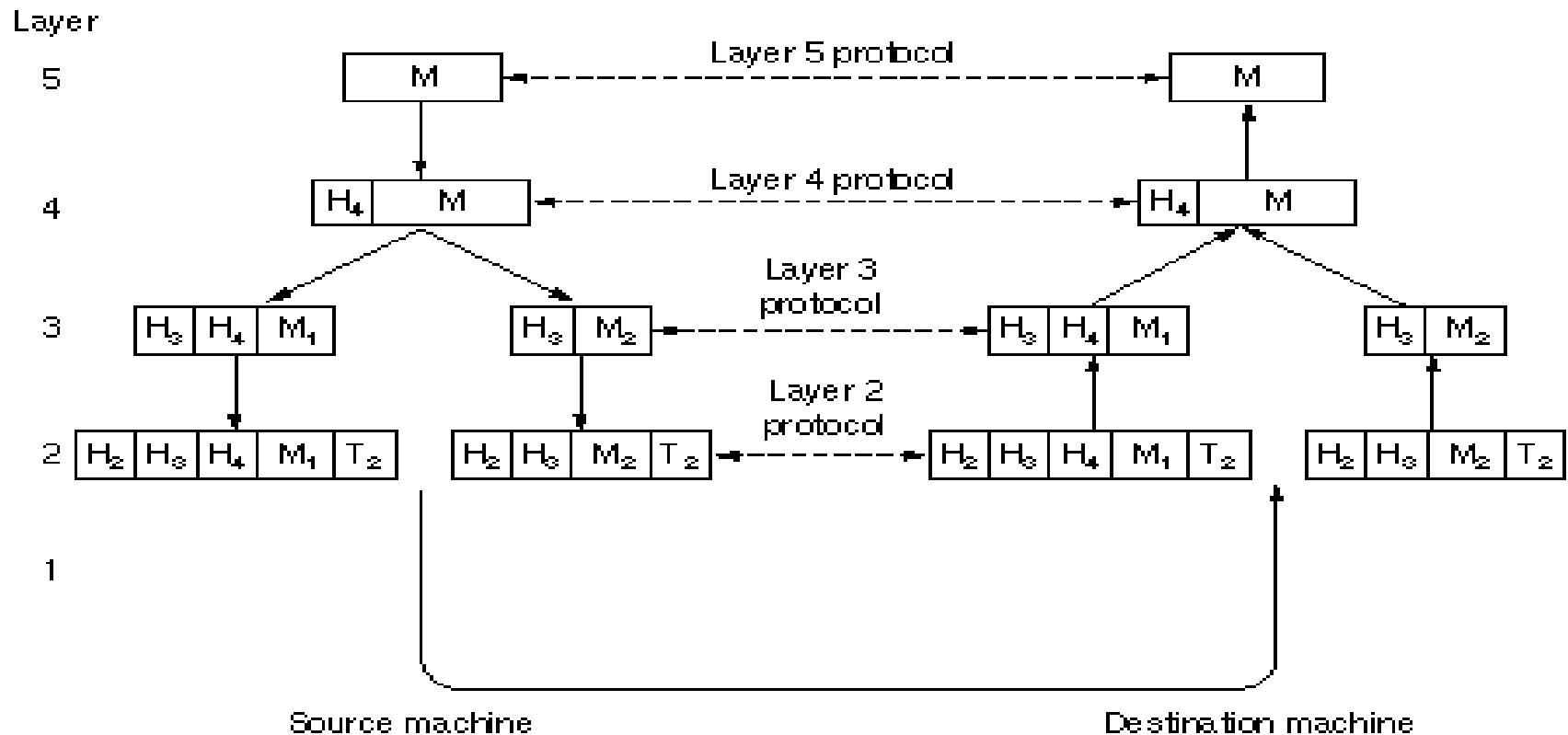


Fig. 2.3 Logical connection between peer layers

Communication between layers

52



Cont....

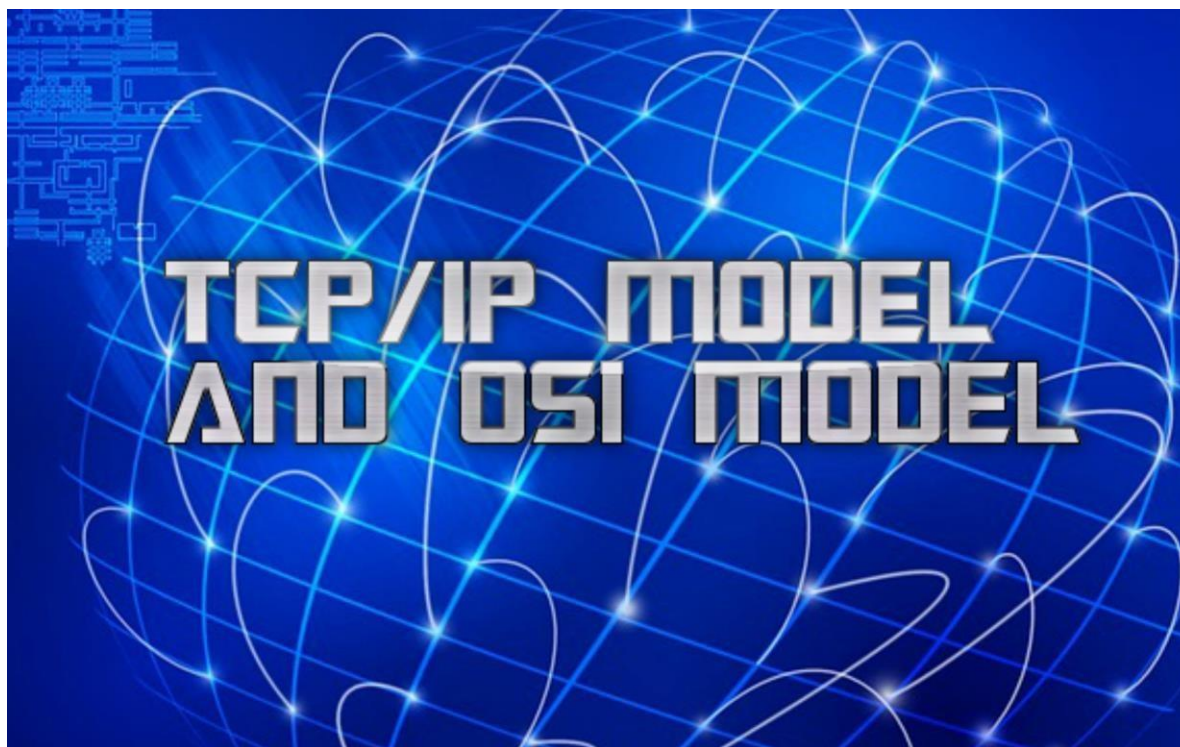
1. A message M is produced by layer 5 of machine 1 and given to layer 4 for transmission.
2. Layer 4 adds a header in front of the message and passes to layer 3.
3. Layer 3 breaks up the incoming message into small units called as packets and appends a layer 3 header to messages and passes to layer 2.
4. Layer 2 adds trailer as well as header to each packet obtained from layer 3 and handover to layer 1 for physical transmission.
5. The control information placed in headers used at the destination machine to convey message to layer 5.
6. Headers are information structures which identifies the information that follows, such as a block of bytes in communication.
7. Trailer is the information which occupies several bytes at the end of the block of the data being transmitted. They contain error-checking data which is useful for confirming the accuracy and status of the transmission.

Design Issues for the Layers

- Addressing
- Error control
- Order of messages must be preserved
- Flow control – fast sender and slow receiver !
- Disassembling, transmitting, and reassembling large messages
- Multiplexing / de-multiplexing
- Routing

Reference Models

OSI MODEL and TCP/IP Model



Objectives

- ▶ Data communication among heterogeneous systems – difficulties and solutions
- ▶ The need for layered architecture
- ▶ Design issues for the layers
- ▶ The OSI model

Network complexities

- Different types of hardware and software
- Different operating systems
- Different types of data to be transferred – text, images, music, video, etc
- Data must be transferred without errors
- Many different paths may have to be taken
- Yet computers must communicate with each other in a network

What is a protocol?

- ▶ It is a formal description of message formats and the rules that two computers must follow in order to exchange messages.
- ▶ This set of rules describes how data is transmitted over a network.

Why are protocols needed?

- ▶ Protocols are needed for communication between any two devices.
 - ▶ In what **format** will the messages be transmitted?
 - ▶ At what **speed** should messages be transmitted?
 - ▶ What to do if **errors** take place?
 - ▶ What to do if parts of a message are **lost**?

Network Model

- What is a model? – A hypothetical description of a complex entity or process.
- Network model - A method of **describing** and **analyzing** data communications networks by **breaking** the entire set of communications process into a number of **layers**
- Each layer has a specific function

Open Systems Interconnect (OSI) Model

- Who made:
 - International Standards Organization (ISO)
- A **Model** of How Protocols and Networking Components Could be Made
- “**Open**” means the concepts are non-proprietary; can be used by anyone.
- OSI is **not** a protocol. It is a **model** for understanding and designing a network architecture that is flexible and robust.

Open Systems Interconnect 64 (OSI) Model

- ▶ The OSI model describes how data flows from one computer, through a network to another computer
- ▶ The OSI model divides the tasks involved with moving information between networked computers into 7 smaller, more manageable sub-task .
- ▶ A task is then assigned to each of the seven OSI layers.
- ▶ Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently.

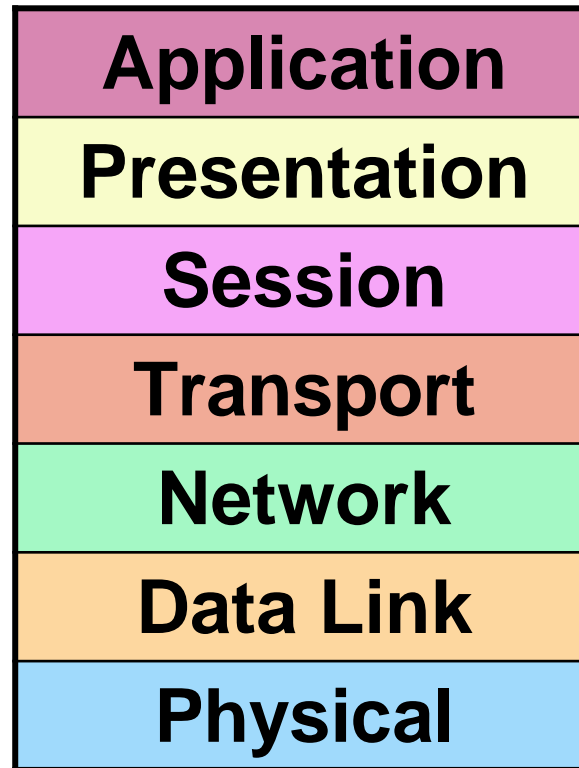
7-layer OSI model

- ▶ Why so many layers?
 - ▶ To reduce complexity, networks are organized as a **stack** of layers, one below the other
 - ▶ Each layer performs a specific task. It provides services to an adjacent layer
 - ▶ This is similar to the concept of a function in programming languages – function does a specific task

The Layers of the OSI Model

Some Mnemonics

All
People
Seem
To
Need
Data
Processing



Please
Do
Not
Tell
Secret
Passwords
Anytime

Physical layer

- Specifications for the physical components of the network.
- **Functions of Physical Layer:**
 - **Bit representation** – encode bits into electrical or optical signals
 - **Transmission rate** – The number of bits sent each second
 - **Physical characteristics** of transmission media
 - **Synchronizing** the sender and receiver clocks
 - **Transmission mode** – simplex, half-duplex, full duplex
 - **Physical Topology** – how devices are connected – ring, star, mesh, bus topology

Application

Presentation

Session

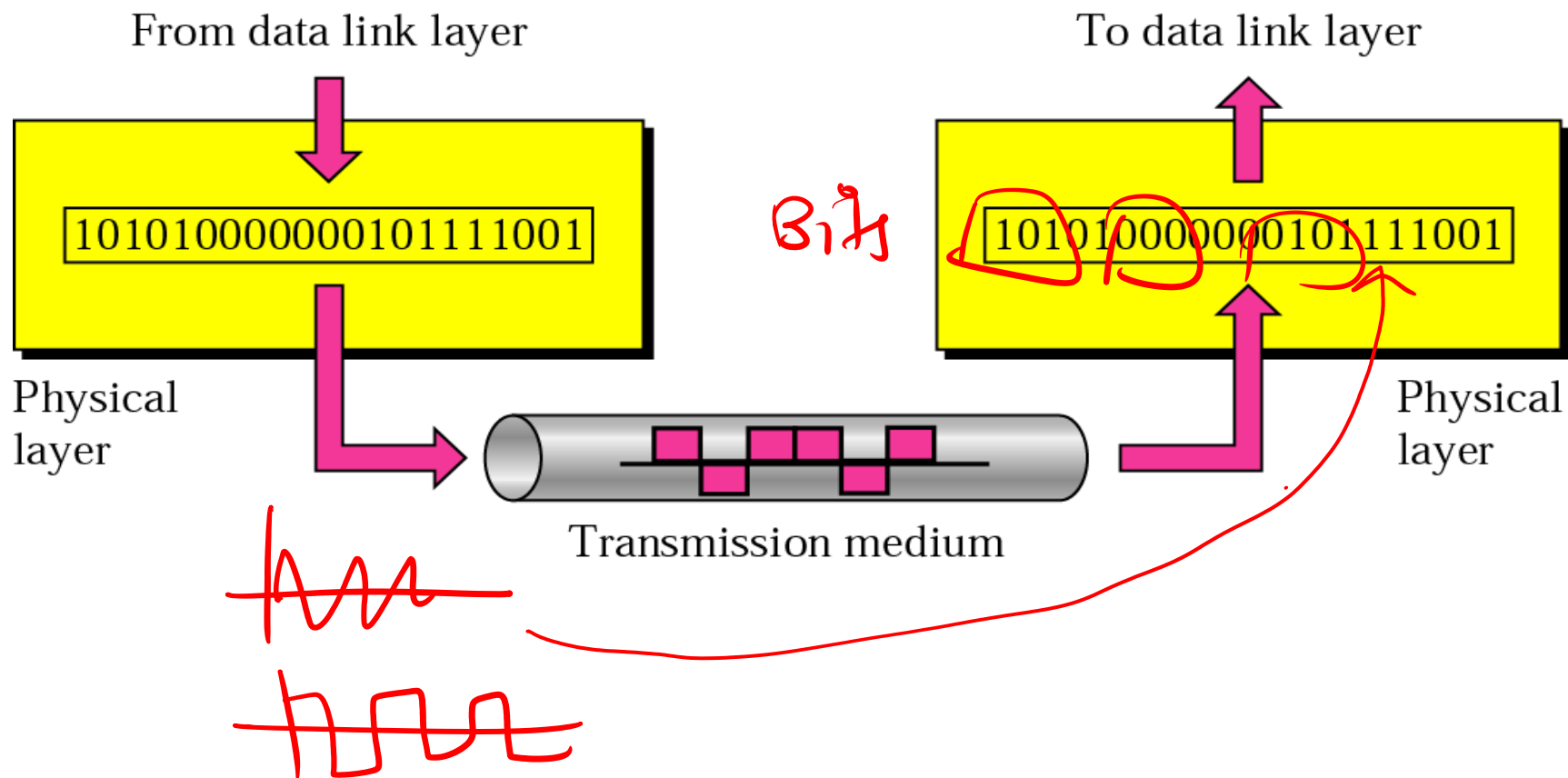
Transport

Network

Data Link

Physical

Physical Layer



Data Link Layer

Responsible for delivery of data between two systems on the same network

Main functions of this layer are:

- **Framing** – divides the stream of bits received from network layer into manageable data units called frames.

MAC **Physical Addressing** – Add a header to the frame to define the physical address of the source and the destination machines.

- **Flow control** – Impose a flow control – control rate at which data is transmitted so as not to flood the receiver (Feedback-based flow control)

Error Control – Adds mechanisms to detect and retransmit damaged or lost frames. This is achieved by adding a trailer to the end of a frame

Application

Presentation

Session

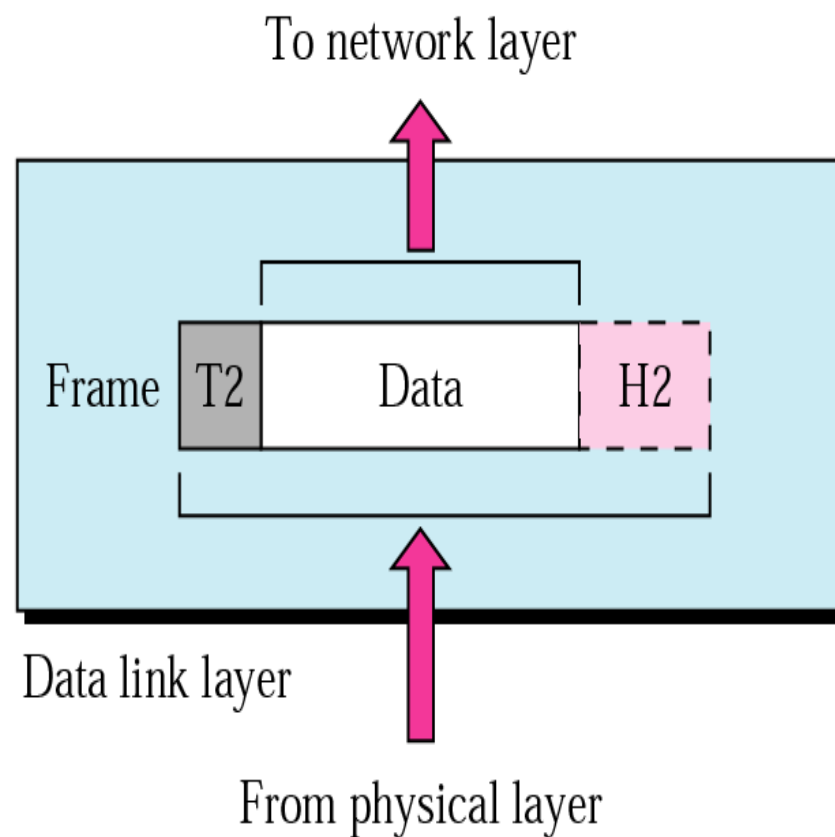
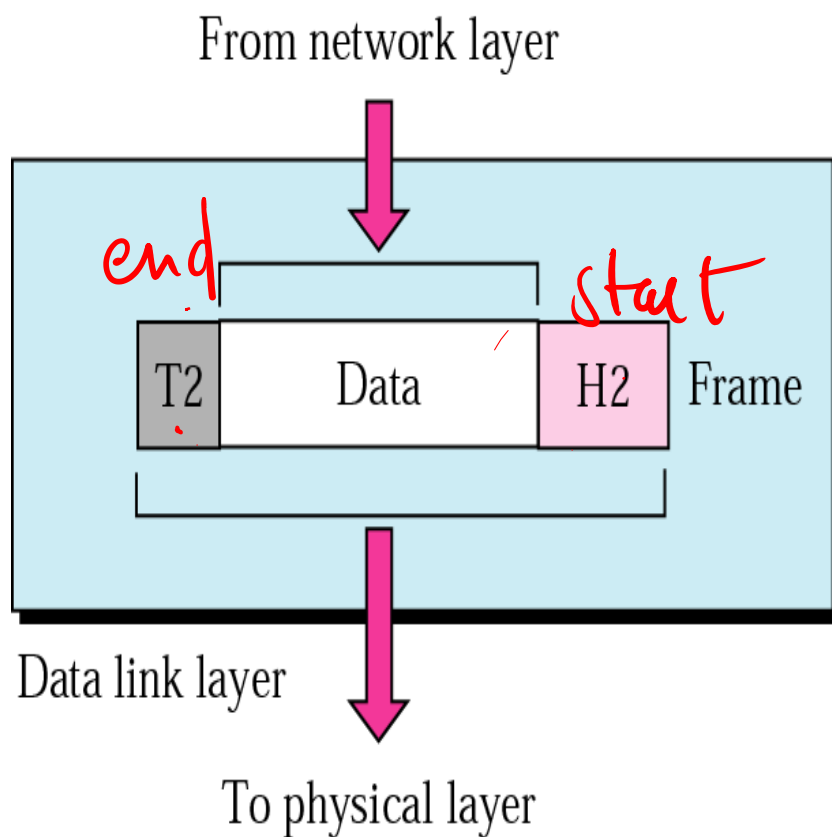
Transport

Network

Data Link

Physical

Data Link Layer



Network Layer

Main functions of this layer are:

- Responsible for delivery of packets across multiple networks
- Routing – Provide mechanisms to transmit data over independent networks that are linked together.
- Network layer is responsible only for delivery of **individual packets** and it does not recognize any relationship between those packets

Application

Presentation

Session

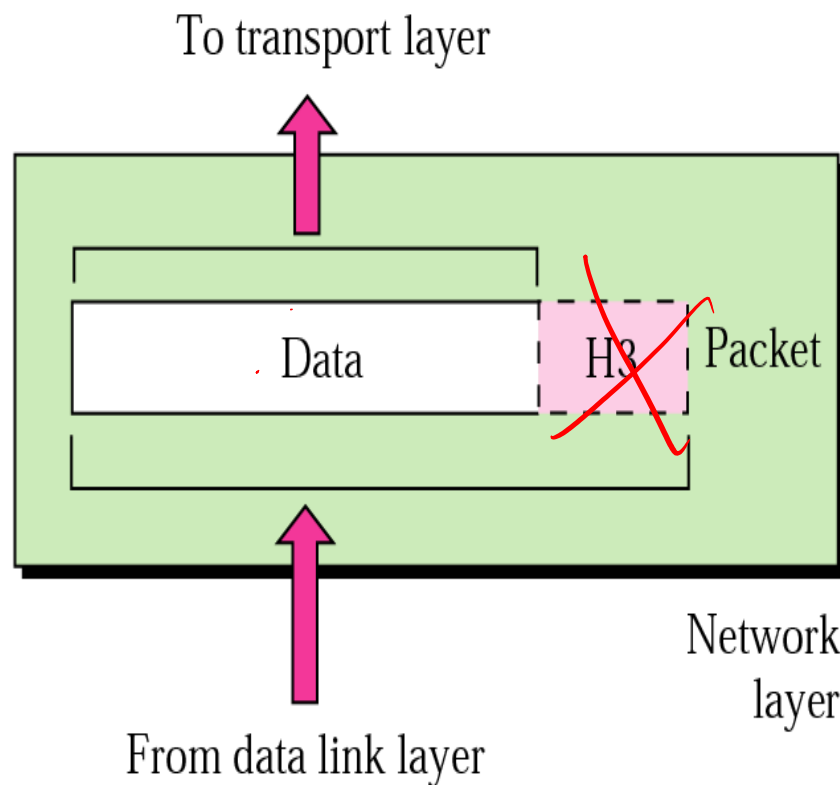
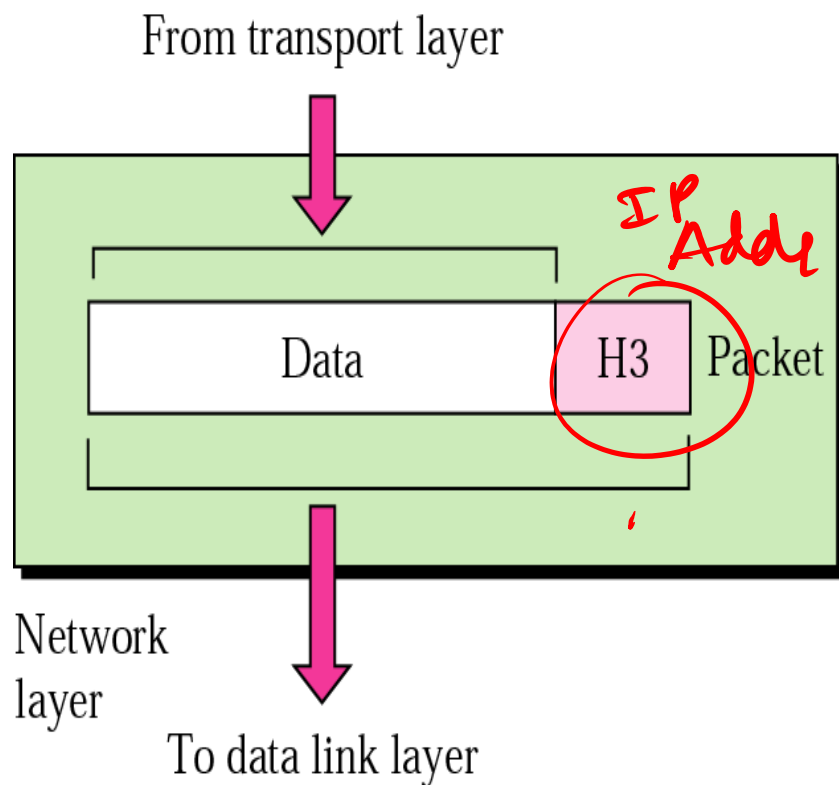
Transport

Network

Data Link

Physical

Network Layer



Transport Layer

Main functions of this layer are:

- Responsible for source-to-destination delivery of the **entire message**.
- Segmentation and reassembly – divide message into smaller segments, number them and transmit. Reassemble these messages at the receiving end.
- Error control – make sure that the entire message arrives without errors – else retransmit.

Application

Presentation

Session

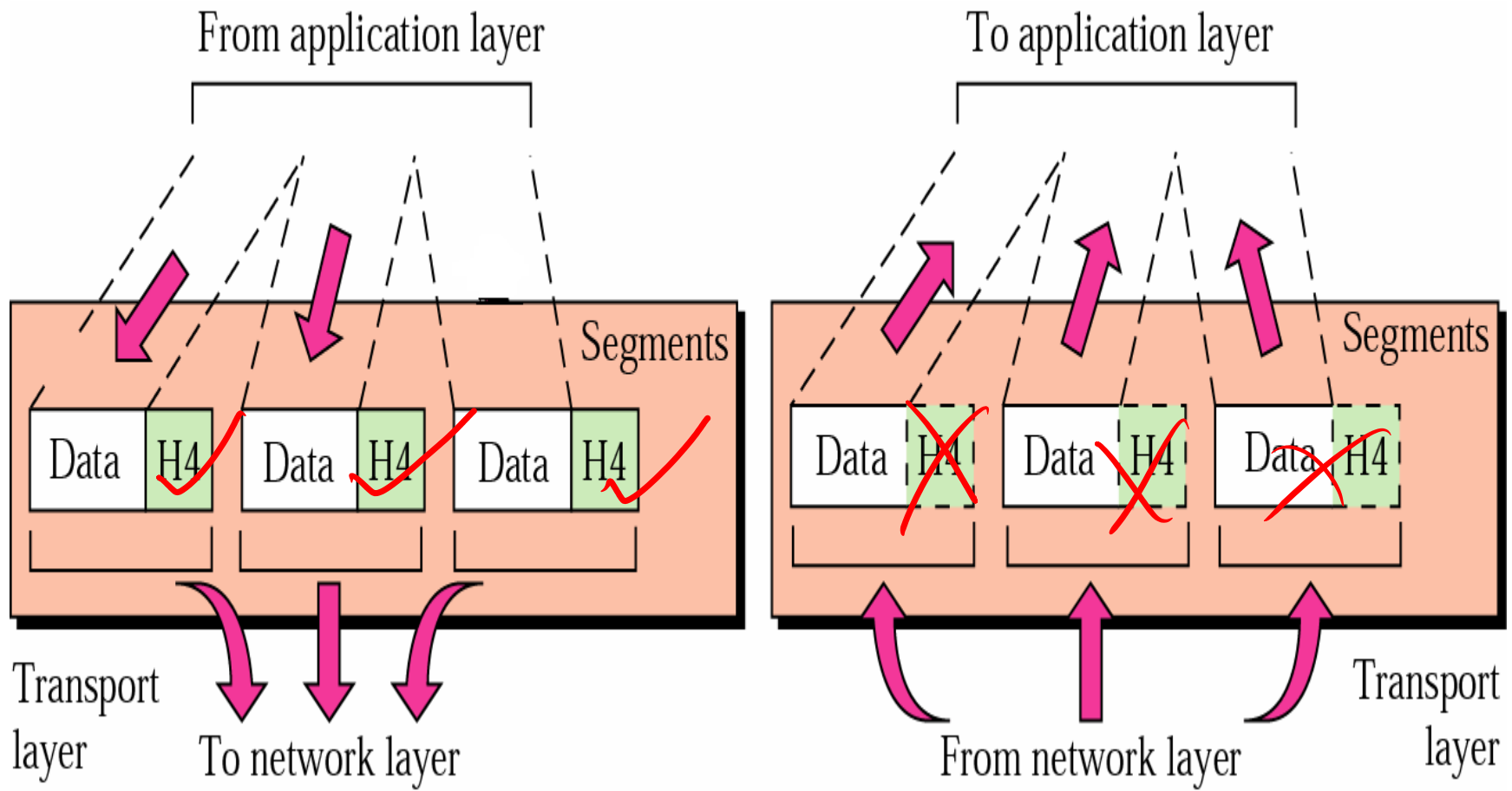
Transport

Network

Data Link

Physical

Transport Layer



Session Layer

Main functions of this layer are:

- Dialog control – allows two systems to enter into a dialog, keep a track of whose turn it is to transmit
- Synchronization – adds check points (synchronization points) into stream of data.

Application

Presentation

Session

Transport

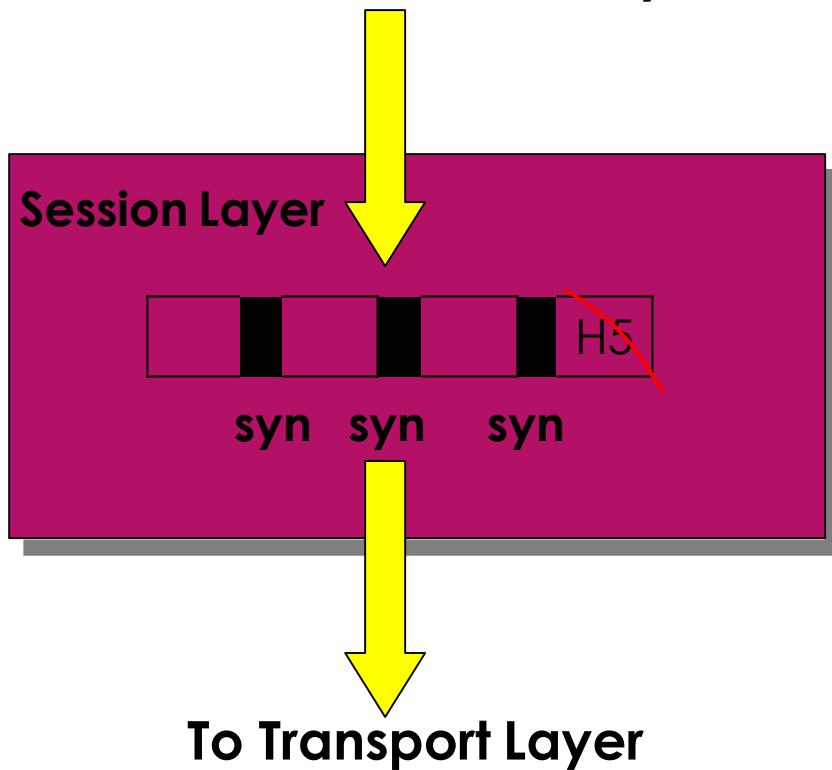
Network

Data Link

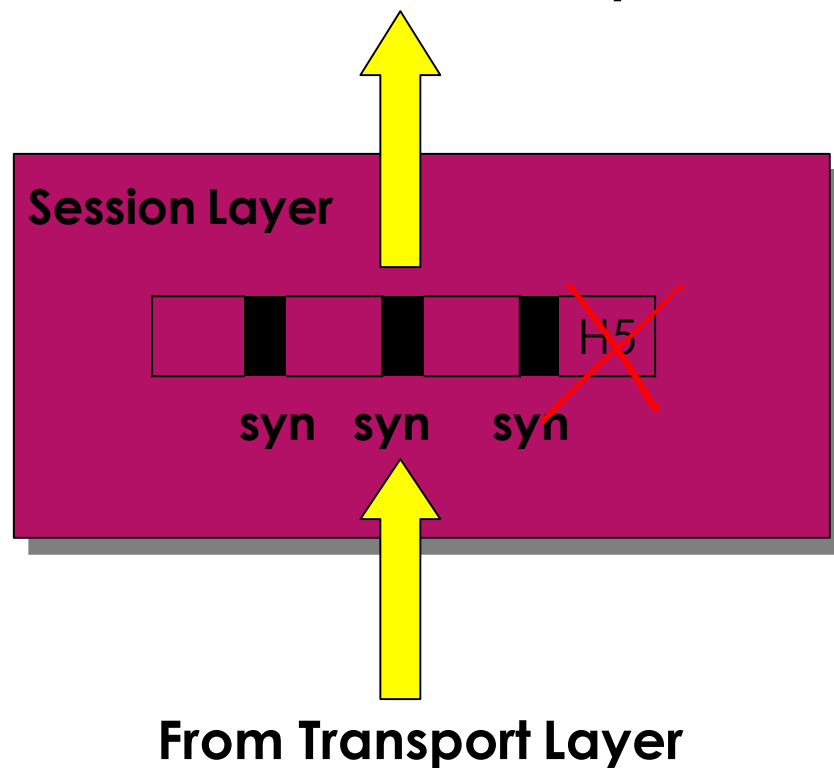
Phy si cal

Session Layer

From Presentation Layer



To Presentation Layer



Presentation Layer

Responsibilities of this layer are:

- Translation
 - Different computers use different encoding systems (bit order translation)
 - Convert data into a common format before transmitting.
 - Syntax represents info such as character codes - how many bits to represent data
 - 8 or 7 bits
- Compression – reduce number of bits to be transmitted

Application

Presentation

Session

Transport

Network

Data Link

Physical

Presentation Layer

- Encryption – transform data into an unintelligible format at the sending end for data security
- Decryption – at the receiving end

Application

Presentation

Session

Transport

Network

Data Link

Physical

Application Layer

- Contains protocols that allow the users to access the network (FTP, HTTP, SMTP, etc)
- **Does not** include application programs such as email, browsers, word processing applications, etc.
- Protocols contain utilities and network-based services that support email via SMTP, Internet access via HTTP, file transfer via FTP, etc

Application

Presentation

Session

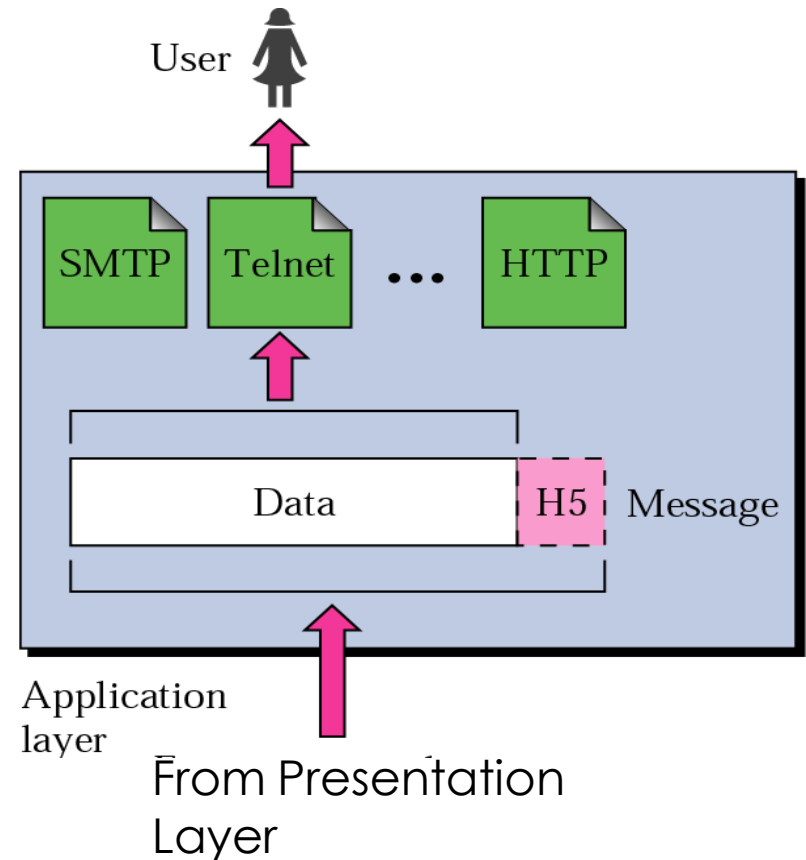
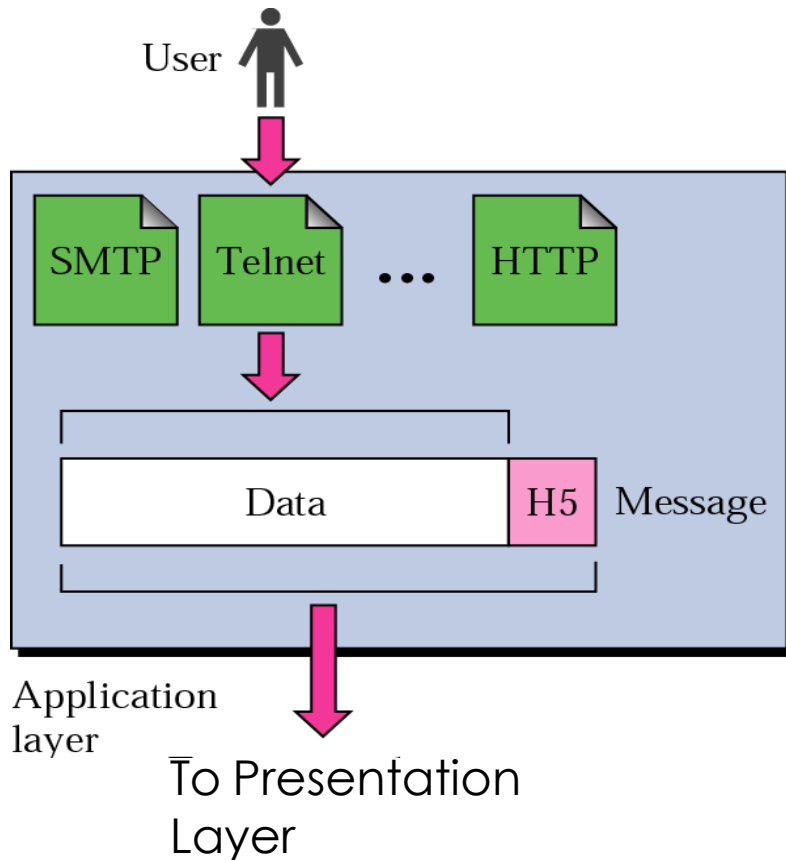
Transport

Network

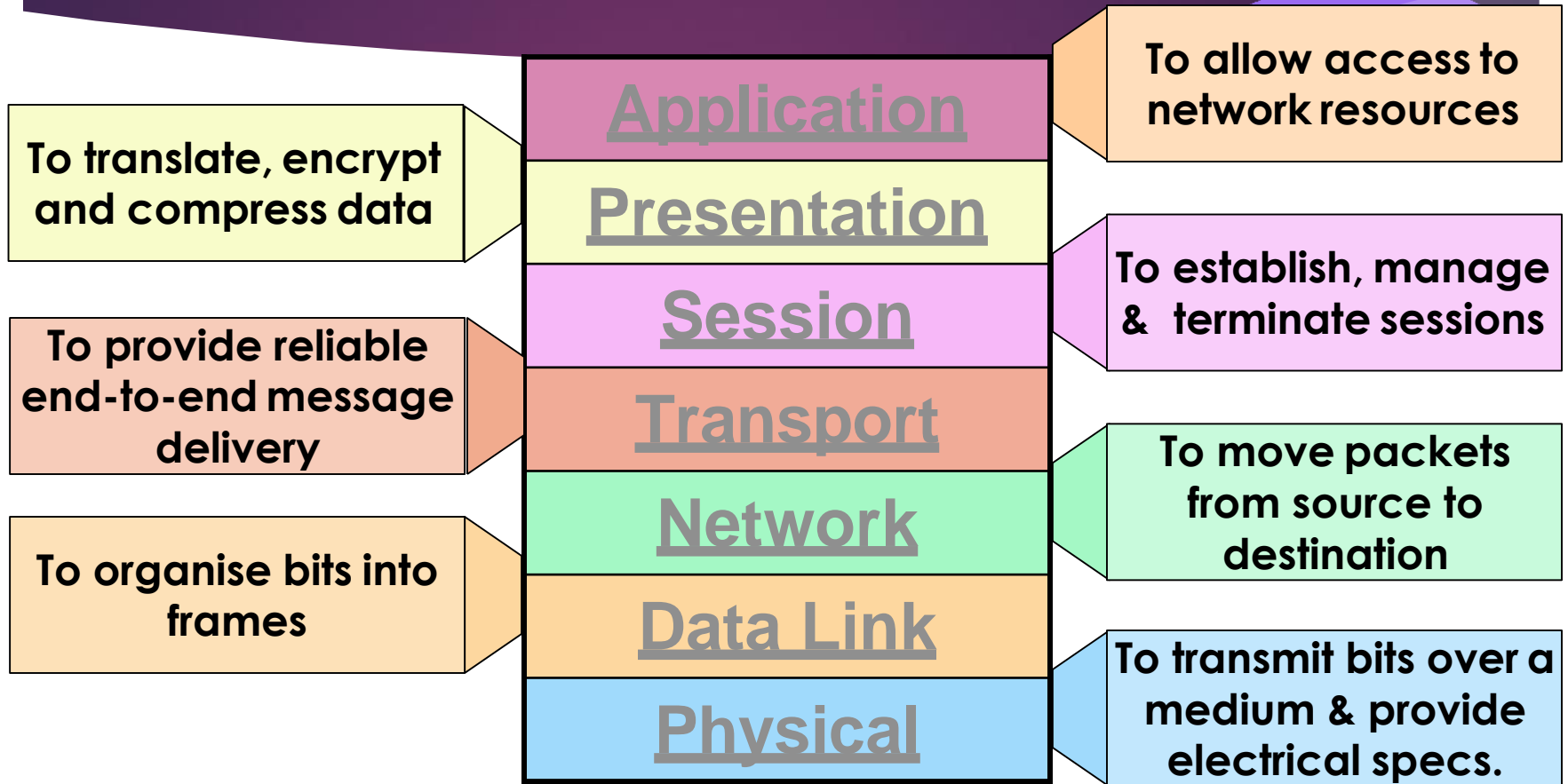
Data Link

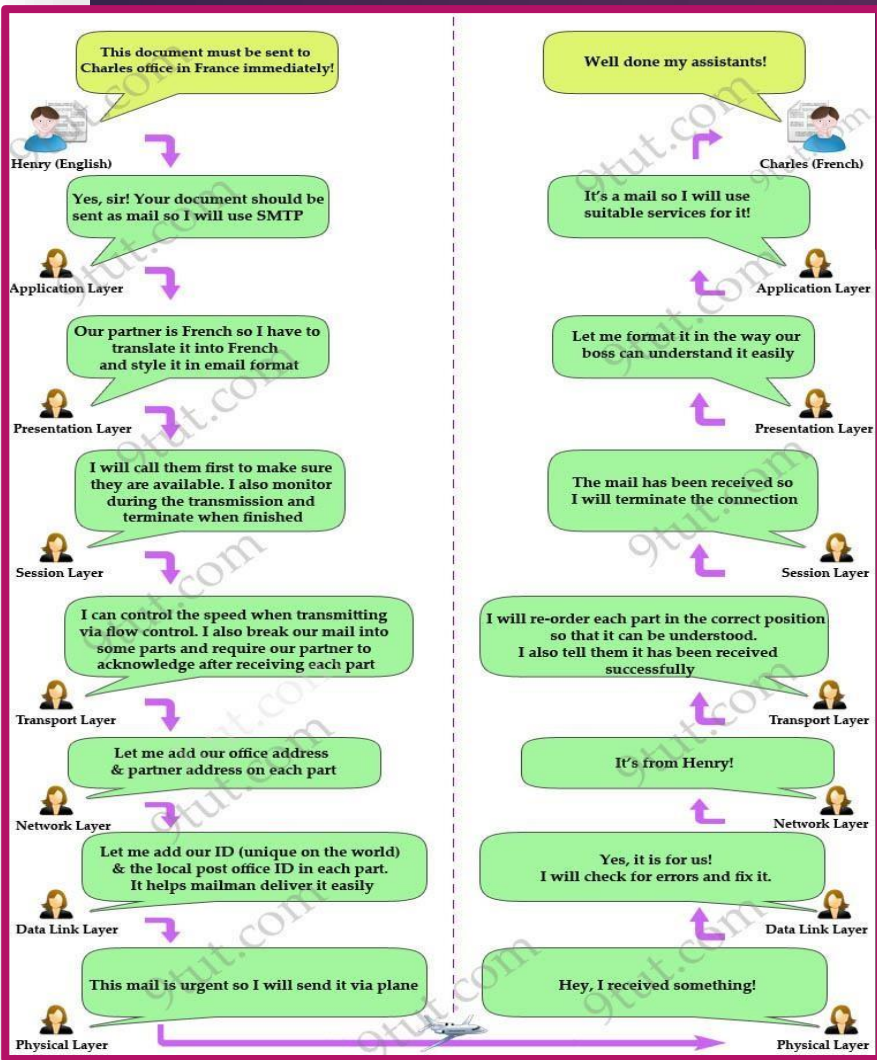
Physical

Application Layer



Summary of Functions of Layers





OSI Layers - Quick Summary

Application

Responsible for determining when access to the network is required.

Presentation

Ensures data is received in a useable format. Data encryption is done here.

Session

Establishing & maintaining connections. Responsible for ports and ensuresquires for services.

Transport

Breaks data into frames & assigns sequence numbers. Also checks for errors in data received. UDP and SPX are protocols that work on this layer.

Network

How systems on different network segments find each other. Source-Destination addresses. Subnets, Path determination exist at this layer. IP & IPX protocols used here.

Datalink

Frames exist here. This layer handles flow control. Specifies topology and provides hardware addressing - MAC.

Physical

Transmission of the raw bit stream. Electrical signalling and hardware interface.

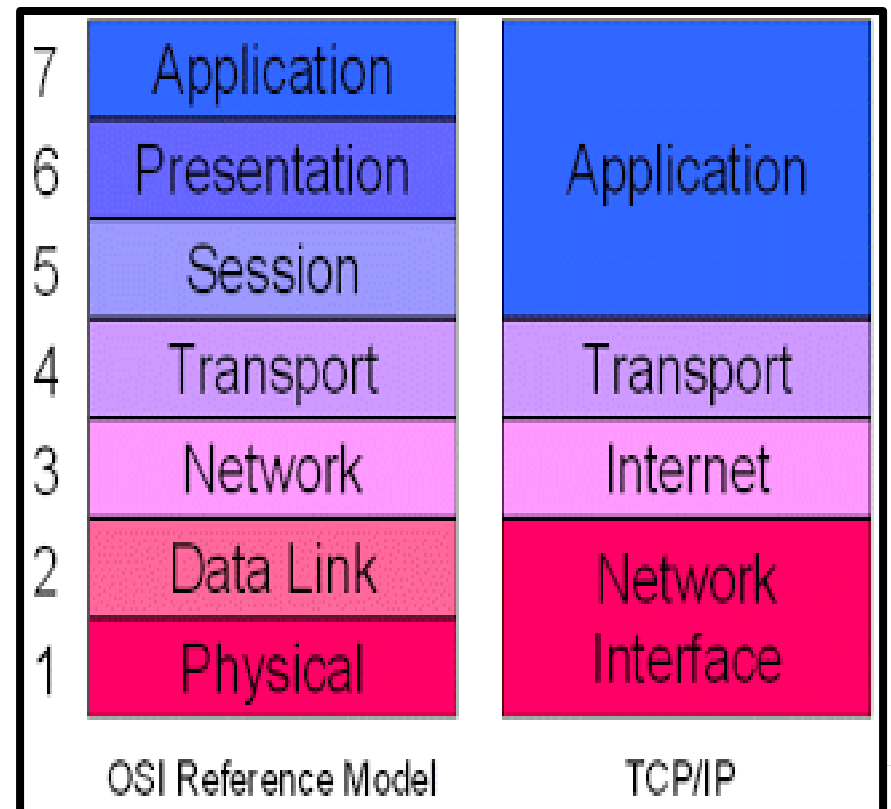
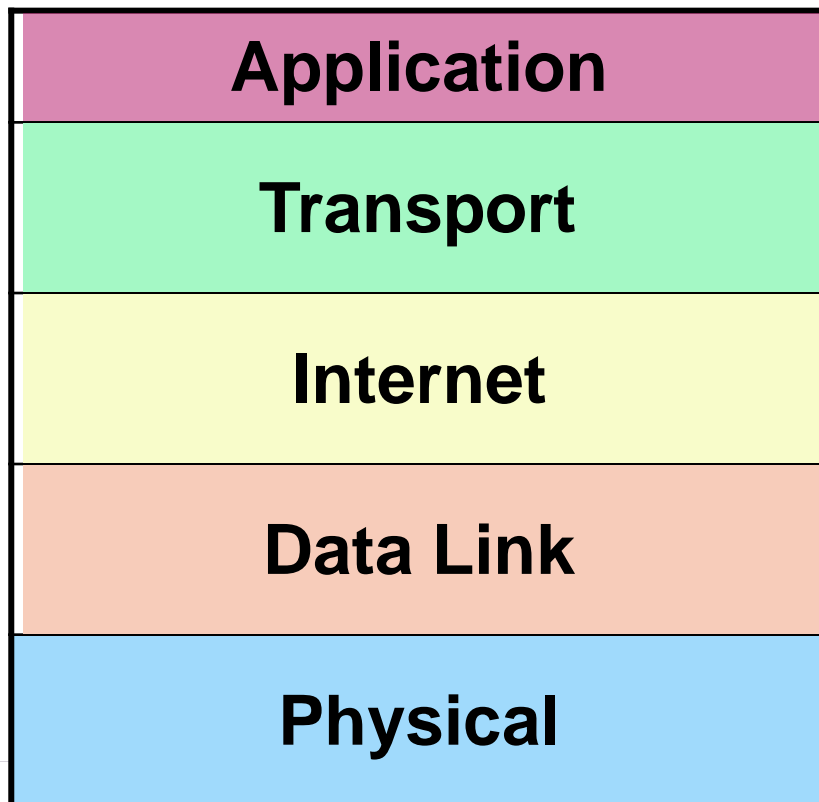
TCP/IP Protocol Suite

- ▶ TCP / IP – **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol
- ▶ Set of protocols organized in different layers
- ▶ Layers of TCP/IP do not match exactly with those in the OSI model
- ▶ Used in the Internet
- ▶ Ability to connect multiple networks in a seamless way was one of the major design goals which led to development of TCP / IP

TCP/IP Protocol Suite

- ▶ TCP / IP – refers to a collection of data communication protocols
- ▶ This name TCP/IP is misleading because TCP and IP are only two of the many protocols that compose the suite
- ▶ TCP / IP has its origins in the work done by the US Department of Defense.
- ▶ Original TCP/IP protocol suite—4 layers built upon the h/w

TCP / IP Layers

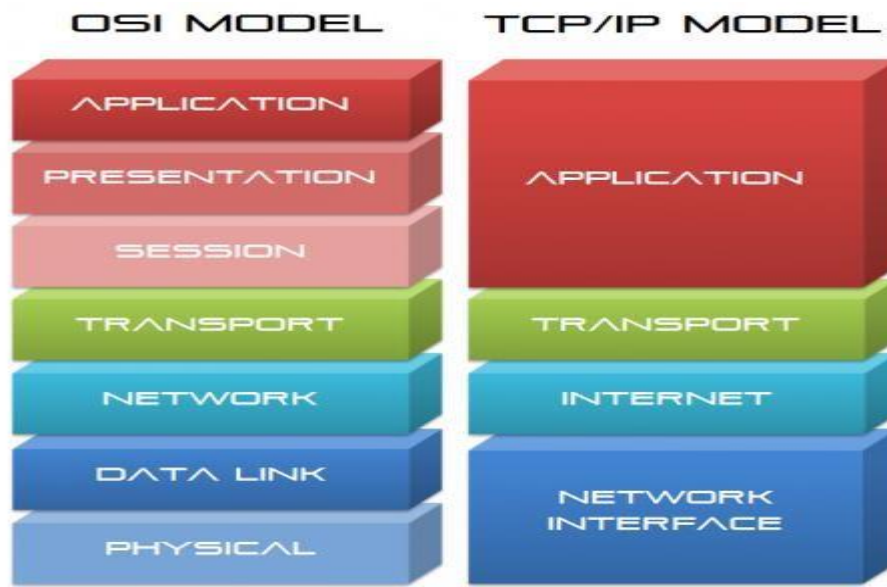


TCP / IP Suite

- ▶ The TCP / IP suite does not define any specific protocols at the data link and physical layers.

Application Layer

- ▶ The Application layer is equivalent to the combined OSI Session, Presentation, and Application layers
- ▶ All the functions handled by these 3 layers in the OSI model are handled by the Application layer in TCP / IP model



Application Layer

- This layer contains all the higher-level protocols
 - FTP – File Transfer Protocol – basic file transfer between hosts (computers)
 - SMTP – Simple Mail Transfer Protocol (for email)
 - HTTP – Hyper Text Transfer Protocol (for web browsing)
- Data unit created at this layer is called a *message*

Encapsulation of Data

- ▶ TCP/IP protocol suite encapsulates data units at various layers of the model
- ▶ At the **Application** layer, the data unit created is called a **message**.
- ▶ The **Transport** layer adds a header to form either a **segment** with TCP.
- ▶ The **Network** (or Internet) layer adds another header to form a **datagram**

Encapsulation of Data

- ▶ **Datagram** – A self-contained message unit which contains sufficient information to allow it to be routed from the source to the destination.
- ▶ The protocol used at the data link layer encapsulates the datagram into a **frame** and this is transmitted across the transmission medium.

Transport Layer - UDP

- ▶ This layer is represented by two protocols – TCP and UDP
 - ▶ TCP – Transmission Control Protocol
 - ▶ UDP – User Datagram Protocol
- ▶ UDP is simpler but is used when reliability and security are less important than size and speed – such as speech, video
- ▶ Since security and reliability are essential for most applications, TCP is used more often

Transport Layer - TCP

- ▶ TCP is a reliable connection-oriented protocol
- ▶ Allows error-free transmission
- ▶ Incoming byte stream is fragmented into a number of shorter messages and these are passed on to the next layer
- ▶ At the receiving end the TCP reassembles the messages into an output stream
- ▶ TCP also handles **flow control** – to control data transfer rate

Transport Layer - TCP

- ▶ A connection must be established between the sender and the receiver before transmission begins
- ▶ TCP **creates** a circuit between sender and receiver for the duration of the transmission
- ▶ TCP **begins** each transmission by alerting the receiver that segments are on their way (connection establishment).
- ▶ Each transmission is **ended** with connection termination

Transport Layer - TCP

- ▶ Each segment created by TCP includes
 - ▶ A sequencing number for re-ordering after receipt.
 - ▶ An acknowledgement ID number
 - ▶ Source address
 - ▶ Destination address
 - ▶ Checksum – for error detection
 - ▶ Data
 - ▶ And other fields

Internetwork or Network Layer

- Also referred to as Network Layer or Internetwork Layer
- Internetwork Protocol (IP) is an unreliable and connectionless protocol
- It offers a best-effort delivery service
 - No error checking
 - IP does its best to get a transmission through to its destination but with no guarantees
 - Noise can cause bit errors during transmission
 - Datagrams maybe discarded due to timeout errors
 - Example of best-effort delivery service is: post-office

Internetwork or Network Layer

- IP transports data in packets called datagrams
- Each datagram is transported separately
- Datagrams can be of variable lengths (upto 64 KB)
- Datagrams may travel along different routes and may arrive out of sequence
- IP does not keep track of the routes
- IP does not have the facility to reorder datagrams once they arrive
- A datagram contains a header and data
- The header contains a number of fields including source and destination address

Comparison of OSI and TCP/IP Models

- ▶ The OSI model makes a clear distinction between services, interfaces and protocols
 - ▶ Each layer performs some **service** for the layer above it
 - ▶ A **layer's** interface tells the processes above it how to access it. It specifies what the parameters are and what results to expect (somewhat like a function declaration)
 - ▶ The protocols used in a layer are used to get the job done.

Comparison of OSI and TCP/IP Models

100

- ▶ The OSI model has 7 layers while the TCP/IP model has 5 layers
- ▶ Both have network, transport, and application layers, but the other layers are different
- ▶ OSI model supports both connectionless and connection-oriented communication
- ▶ TCP/IP supports only connectionless communication

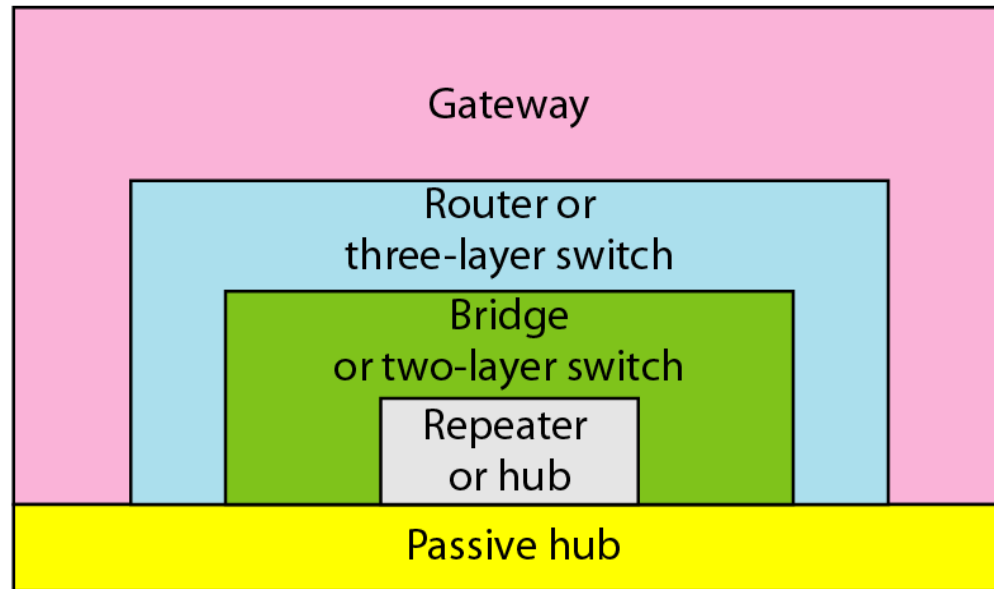
Networking devices

► Five connecting devices

- ❖ Repeaters
- ❖ Hubs
- ❖ Bridges
- ❖ Switches
- ❖ Routers
- ❖ Gateway

Five categories of connecting devices

Application
Transport
Network
Data link
Physical

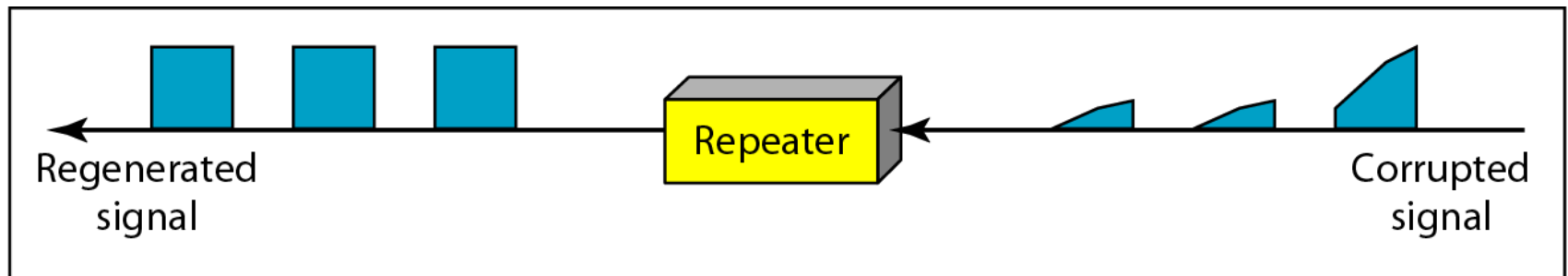


Application
Transport
Network
Data link
Physical

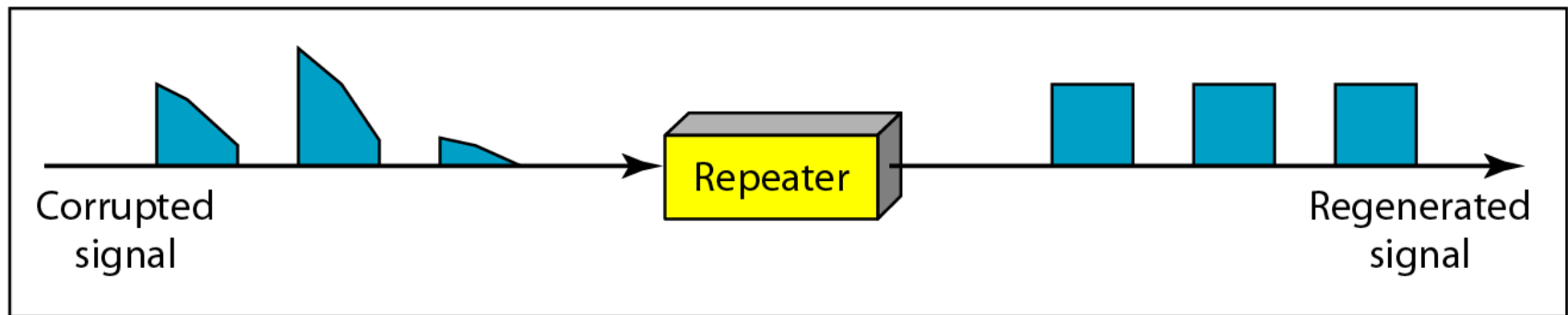
Repeaters

- ▶ A **physical layer** device that acts on **bits** not on **frames** or packets
- ▶ Can have two or more interfaces
- ▶ When a bit (0,1) arrives, the repeater receives it and **regenerates** it, then transmits it onto all other interfaces
- ▶ Used in LAN to **connect cable segments** and **extend the maximum cable length** → extending the **geographical LAN range**
 - ❖ Ethernet 10base5 – Max. segment length 500m – 4 repeaters (5 segments) are used to extend the cable to **2500m**
 - ❖ Ethernet 10Base2- Max. segment length 185m - 4 repeaters (5 segments) are used to extend the cable to **925m**
- ▶ Repeaters do not implement any **access method**
 - ❖ If any two nodes on any two connected segments transmit at the same time **collision** will happen

Function of a Repeater



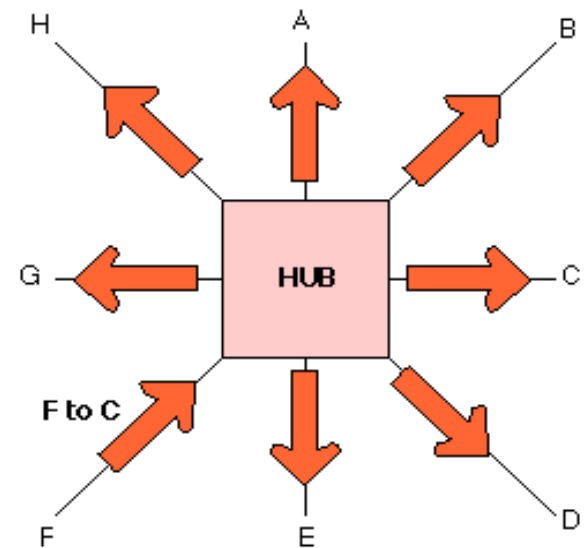
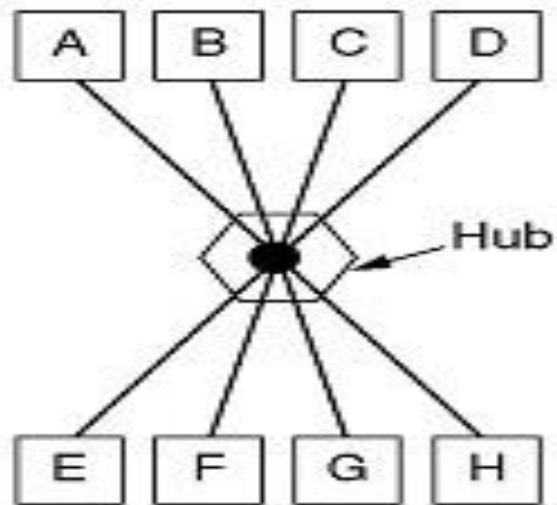
a. Right-to-left transmission.



b. Left-to-right transmission.

HUBS

- ▶ Acts on the **physical layer**
- ▶ Operate on bits rather than frames
- ▶ Also called **multiport repeater**
- ▶ Used to connect stations adapters in a **physical star topology** but **logically bus**
- ▶ Connection to the hub consists of **two pairs of twisted pair wire** one for **transmission** and the other for **receiving**.
- ▶ Hub receives a bit from an adapter and sends it to **all** the other adapters without implementing any access method.
- ▶ does not do **filtering** (forward a frame into a specific destination or drop it) just it copy the received frame onto **all other links**
- ▶ The entire hub forms **a single collision domain**, and **a single Broadcast domain**
 - ▶ **Collision domain:** is that part of the network (set of **NICs**) when two or more nodes transmit at the same time collision will happen.
 - ▶ **Broadcast domain:** is that part of the network (set of NIC) where each NIC can 'see' other NICs' traffic **broadcast messages**.
- ▶ Multiple Hubs can be used **to extend** the network length

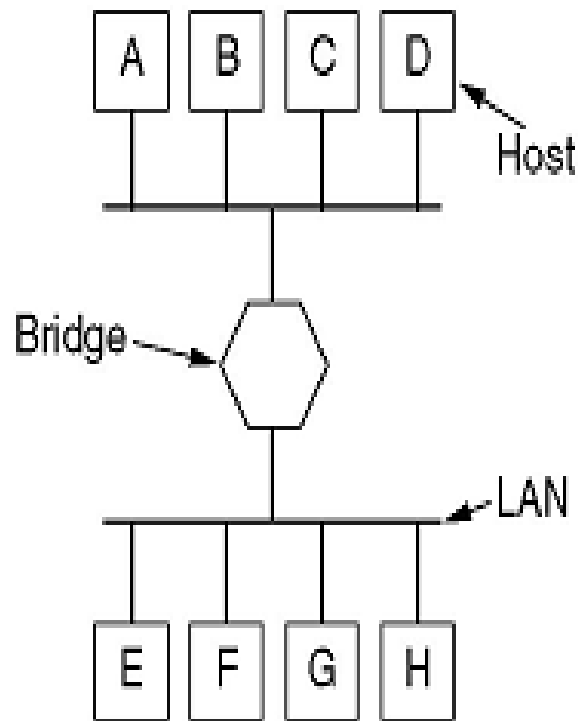


Hubs Vs. Repeaters

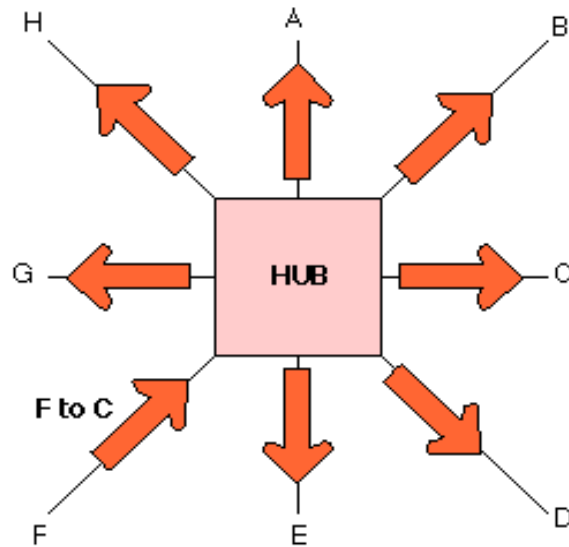
- ▶ Hub are different than repeaters in the following:
 - ❖ The provide **network management features** by gathering information about the network and report them to a monitoring host connected to the hub so some statistics about the network (bandwidth usages, collision rates, average frame sizes) can be generated.
 - ❖ If an adapter is not working the hub can **disconnect** it internally and the network will not be affected.

Bridges/switches

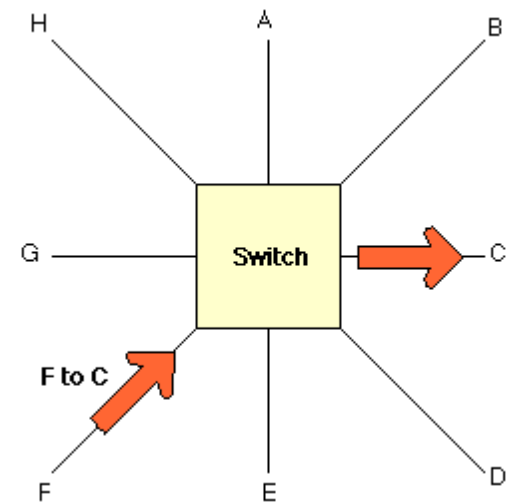
- ▶ Acts on the **data link** layer (MAC address level)
- ▶ Used to **divide** (segment) the LAN into smaller LANs segments, or to **connect** LANs that use identical physical and data link layers protocol (see figure in next slide)
- ▶ Each LAN segment is a **separate collision domain**
- ▶ Bridge does not send the received frame to all other interfaces like hubs and repeaters, but it performs **filtering** which means:
 - ▶ Whether a frame should be **forwarded** to another interface that leads to the destination or **dropped**
- ▶ This is done by a bridge table (**forwarding table**) that contains entries for the nodes on the LAN
 - ▶ The bridge table is **initially empty** and **filled automatically** by **learning from frames movements** in the network
 - ▶ An entry in the bridge table consists of : Node LAN (**MAC**) Address, **Bridge Interface to which the node is connected to**, the **record creation time**



Bridges (Switches) Vs. Hubs

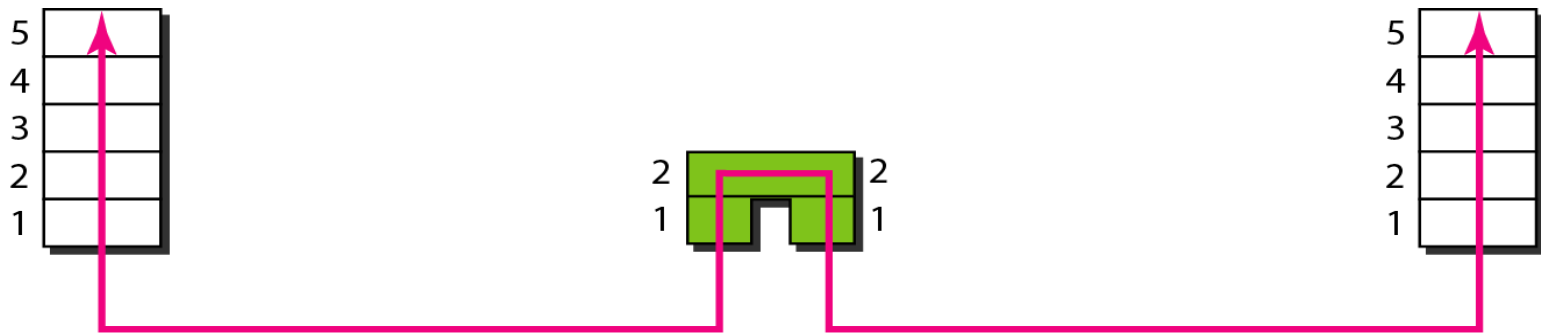


A Hub sending a packet from F to C.



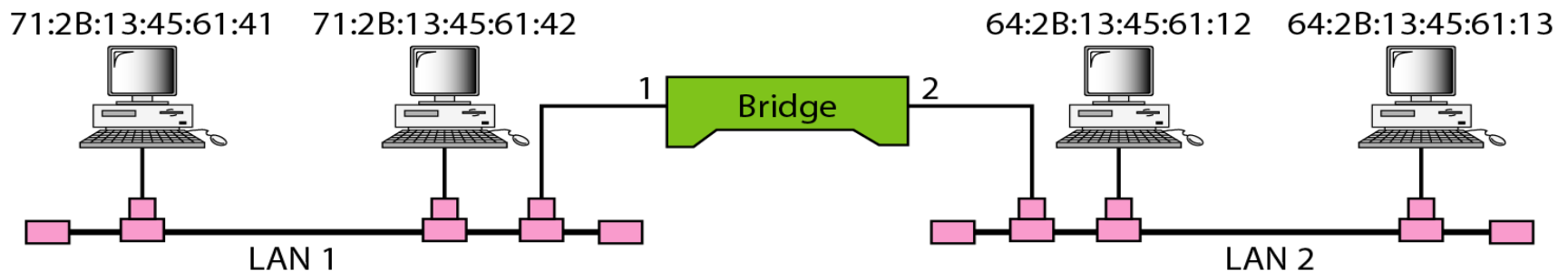
A Switch sending a packet from F to C

A bridge connecting two LANs



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table

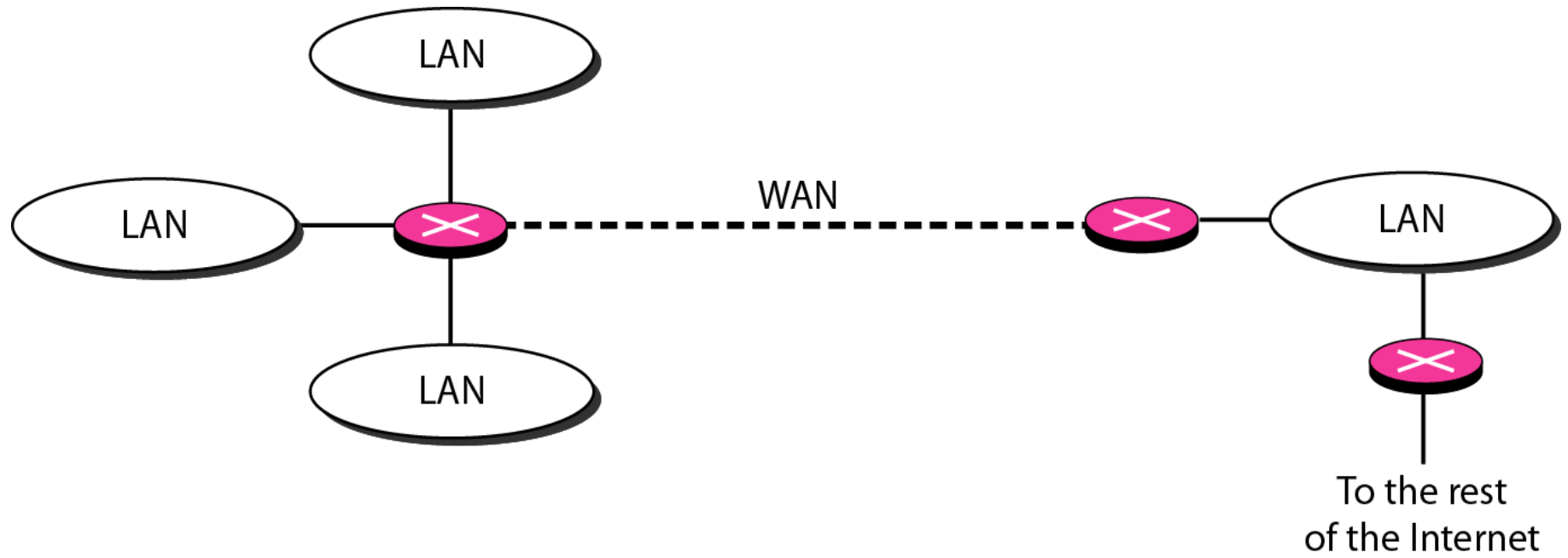


Routers

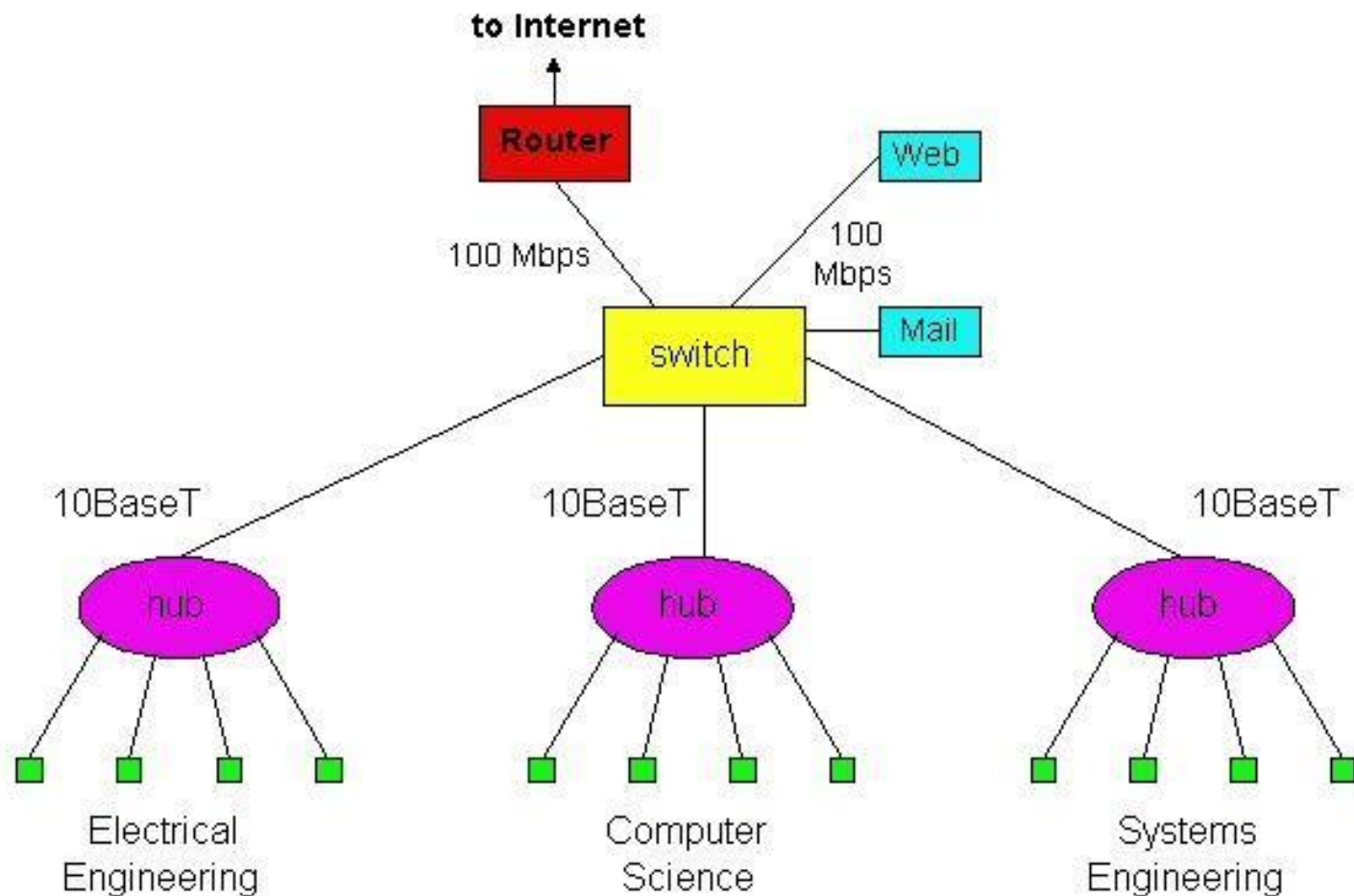
- ▶ Operates at network layer = deals with **packets** not **frames**
- ▶ Connect LANs and WANs with similar or different protocols together
- ▶ Switches and bridges **isolate collision domains** but forward broadcast messages to **all LANs** connected to them. Routers **isolate both** *collision* domains and *broadcast* domains
- ▶ Acts like normal stations on a network, but have **more than one** network address (an address to each connected network)
- ▶ Deals with global address (network layer address (IP)) not local address (MAC address)
- ▶ Routers **Communicate with each other** and exchange routing information
- ▶ Determine best route using **routing algorithm** by special software installed on them
- ▶ **Forward traffic if information on destination** is available otherwise **discard** it (not like a switch or bridge)

Routers connecting independent LANs and WANs

114



An Institutional Network Using Hubs, Ethernet Switches, and a Router



Summary comparison

	<u>hubs</u>	<u>bridges</u>	<u>routers</u>	<u>switches</u>
traffic isolation	no	yes	yes	yes
plug & play	yes	yes	no	yes
optimal routing	no	no	yes	no
cut through	yes	no	no	yes

Networking Devices

