Layered Architecture

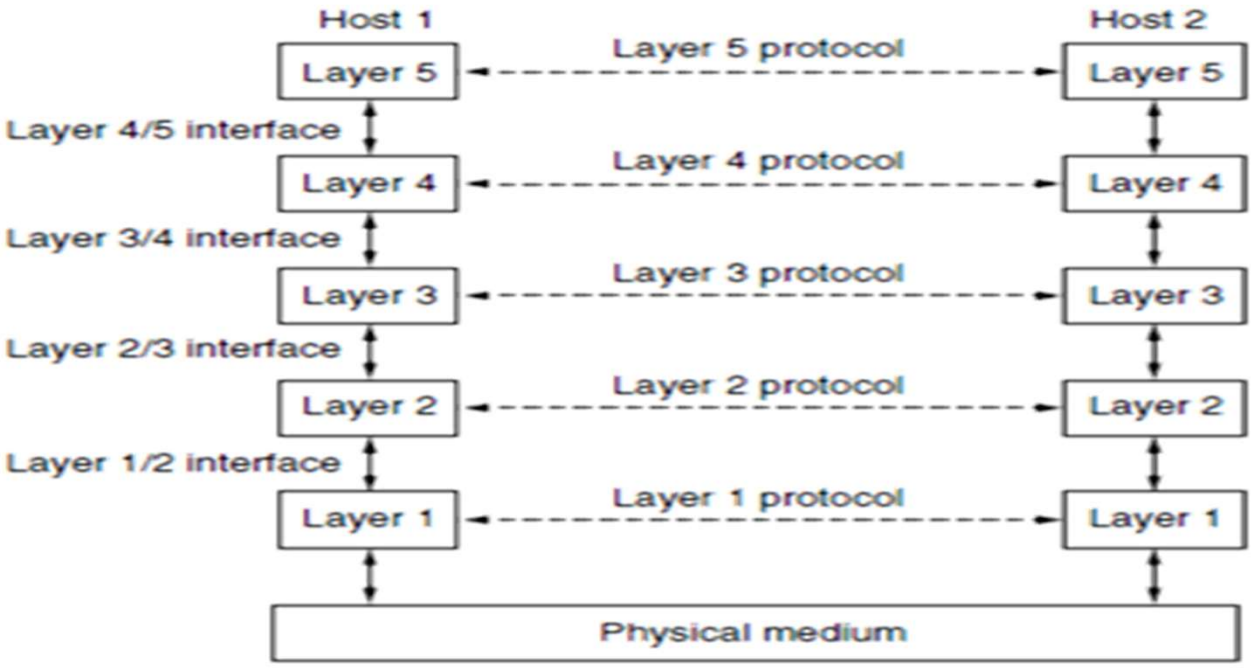
Contents

- Layers
- Protocols and services
- ISO/OSI Reference Model
- Overview of TCP/IP architecture
- Application Protocols

Layers, Protocols and services, ISO/OSI Reference Model, Overview of TCP/IP architecture, Application Protocols and TCP/IP utilities.

Protocol Hierarchies

- To **reduce the design complexity**, most networks are organized as a stack of **layers** or **levels**, each one built upon the one below it.
  - The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- Each layer is a kind of **virtual machine**, offering certain services to the layer above it.
- When layer *n* on one machine carries on a conversation with layer *n* on remote machine, the rules and conventions used in this conversation are collectively known as the **layer *n* protocol**.
- A **protocol** is an agreement between the communicating parties on how communication is to proceed.



- The entities comprising the corresponding layers on different machines are called **peers.** Peers communicate with each other by means of protocols.
- In reality, **no data are directly transferred** from layer *n* on one machine to layer *n* on another remote machine. Instead, each layer passes data and control information to the layer immediately below it.
- It is the **physical medium** through which actual communication occurs.
- Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations and services the lower layer makes available to the upper one
- In Fig. **virtual communication** is shown by **dotted lines** and physical communication by solid lines.

- A set of layers and protocols is called a **network architecture**
- A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack**.

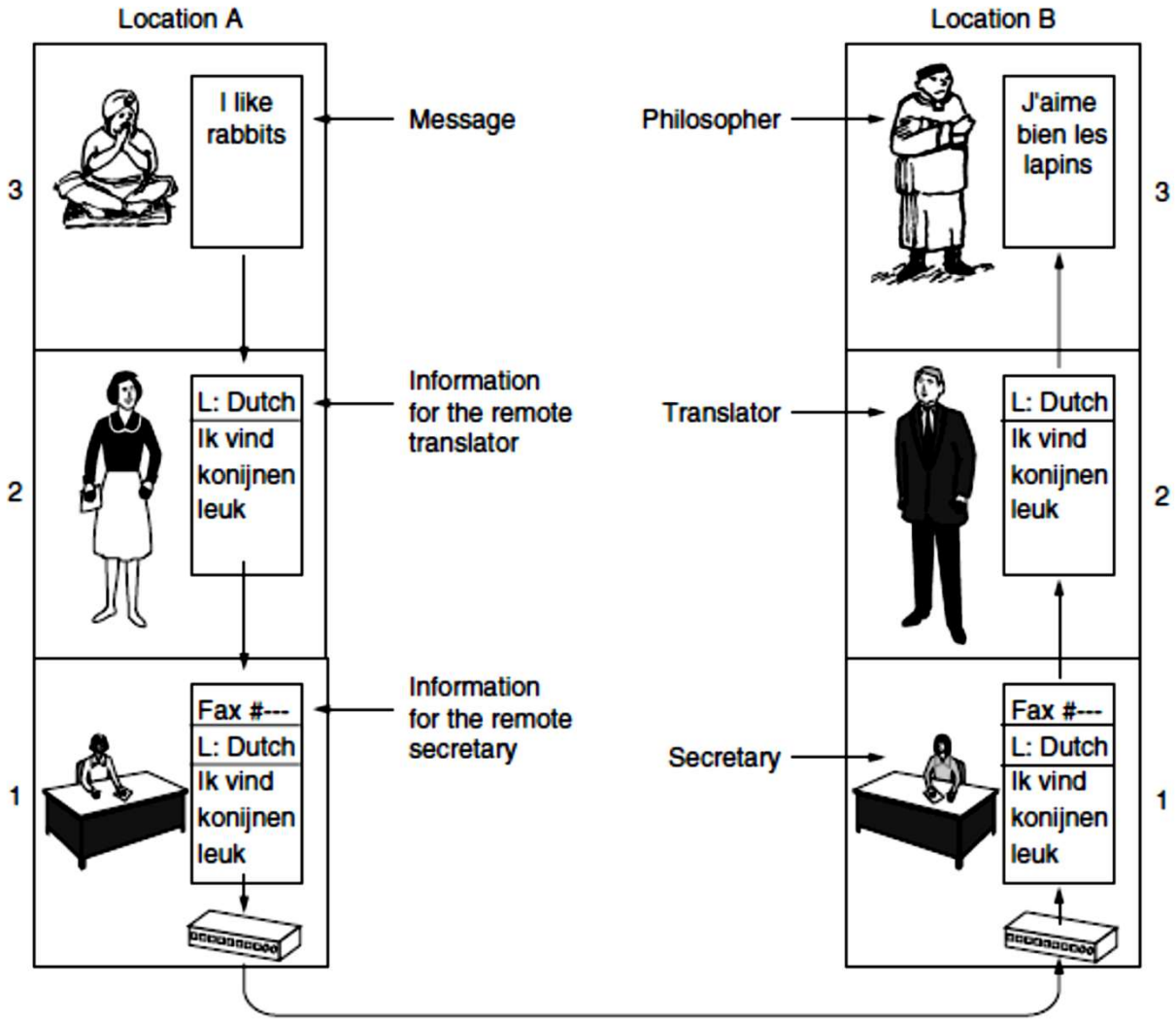
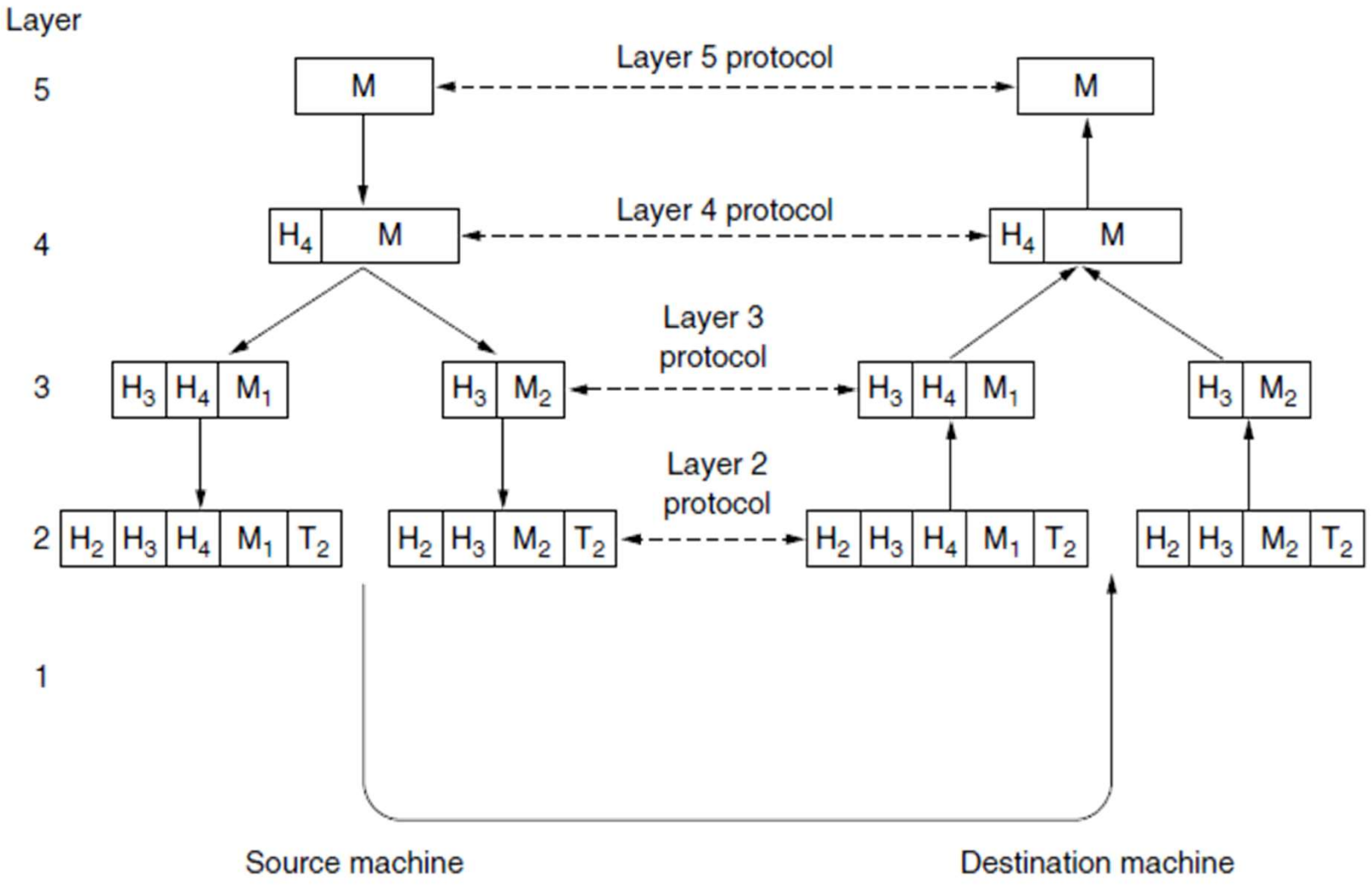


Figure 1-14. The philosopher-translator-secretary architecture.

Flow of information from one source to destination



Transmission efficiency

Transmission efficiency is defined as **the total number of information bits (i.e. bits in the message sent by the user) divided by the total bits in transmission (i.e., information bits plus overhead bits)**.

- A 100-byte message is sent through a private internet using the TCP/IP protocol suite. If the protocol adds a 10-byte header at each three layer, and a 10 byte trailer at 3rd layer, what is the efficiency of the system?

Solution:

Efficiency of a system is defined as the ratio of the number of useful bytes to the number of total bytes.

Thus efficiency = actual size of message / total size (message + 3headers + 1 trailer)

Thus efficiency = 100/140 = 71.4%

Problem

Suppose an application layer entity wants to send an **L-byte** message to its peer process, using an existing TCP connection. The **TCP segment** consists of the **message plus 20 bytes of header**. The segment is **encapsulated into an IP packet** that has an **additional 20 bytes of header**. The IP packet in turn goes inside an **Ethernet frame** that has **18 bytes of header and trailer**. **What percentage of the transmitted bits in the physical layer correspond to message information**, if **L = 100** bytes, **500** bytes, **1000** bytes?

Solution

The message overhead includes:

- **TCP: 20 bytes** of header
- **IP: 20 bytes** of header
- **Ethernet: total 18 bytes** of header and trailer.

Total Header : 20+20+18=58 Bytes

Total Bytes sent: **L(message)+58**

Therefore

- L = 100 bytes, **100/158 = 63%** efficiency.
- L = 500 bytes, **500/558 = 90%** efficiency.
- L = 1000 bytes, **1000/1058 = 95%** efficiency.

Design Issues for Layers

- **Reliability**: How safely the data reaches the destination?
  - Solution : Error Correction and Error Detection Techniques
- **Link errors**
  - Solution: To find an alternate path to reach the destination
- **Protocol Layering:** To support to the changes caused due to the evolution of network without affecting the overall system
- **Addressing** or **naming:** Since there are many computers on the network, every layer needs a mechanism for identifying the senders and receivers uniquely that are involved in a particular message.

- **Scalability:** Designs that continue to work even when the size of the network increases
- Necessary to support **disassembling or segmentation, transmission and reassembling.**
- **Statistical Multiplexing:** Sharing network bandwidth dynamically based on the statistics of demand.
- **Flow control:** The receiver should not be overwhelmed by the sender.
- **Congestion:** To control the flow of traffic
- **Security:** To maintain authenticity, confidentiality, integrity of the message; to ensure that the system is not subjected to any kind of attacks like node impersonation, masquerade attack etc.

The OSI Model and the TCP/IP Protocol Suite

Objectives

Upon completion you will be able to:

- *Understand the architecture of the OSI model*
- *Understand the layers of the OSI model and their functions*
- *Understand the architecture of the TCP/IP Protocol Suite*
- *Differentiate between the OSI model and the TCP/IP Suite*
- *Differentiate between the three types of Internet addresses*
- *Application Protocols*

The OSI Model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

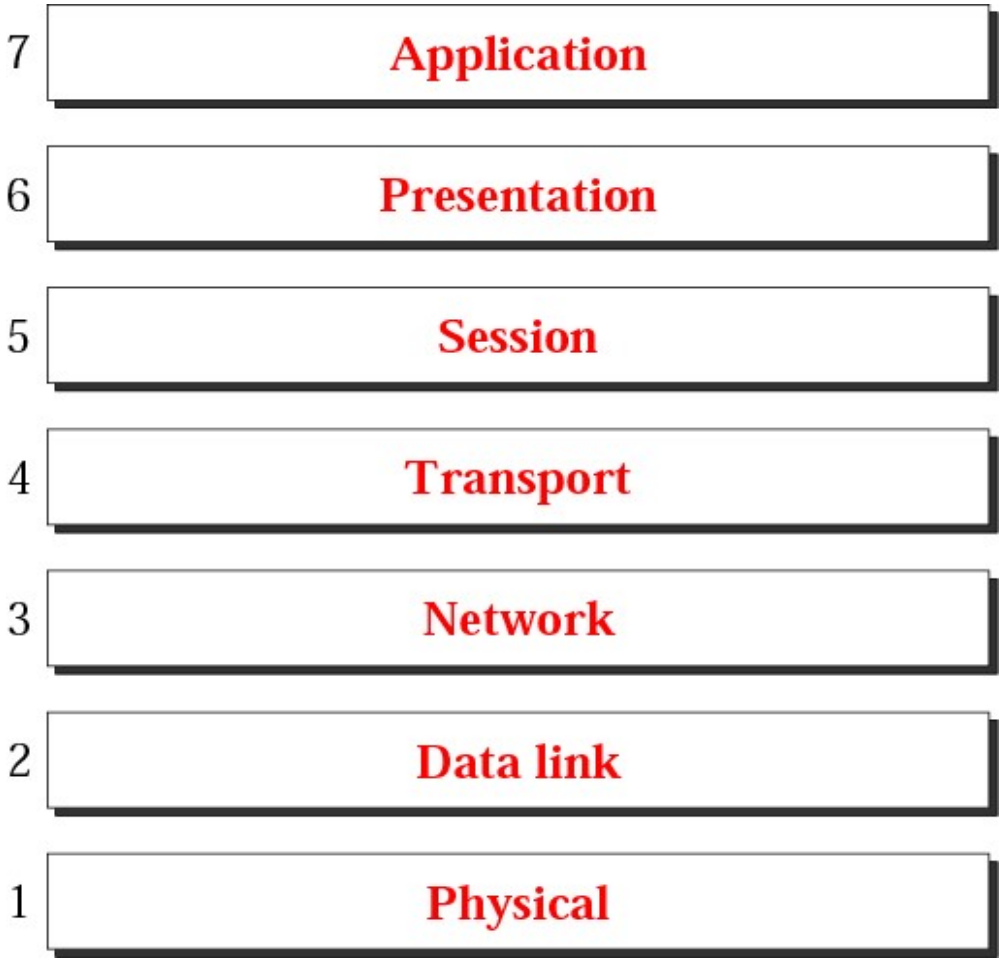
It is a conceptual framework so we can better understand complex interactions that are happening.

The topics discussed in this section include:

Layered Architecture
Peer-to-Peer Processes
Encapsulation

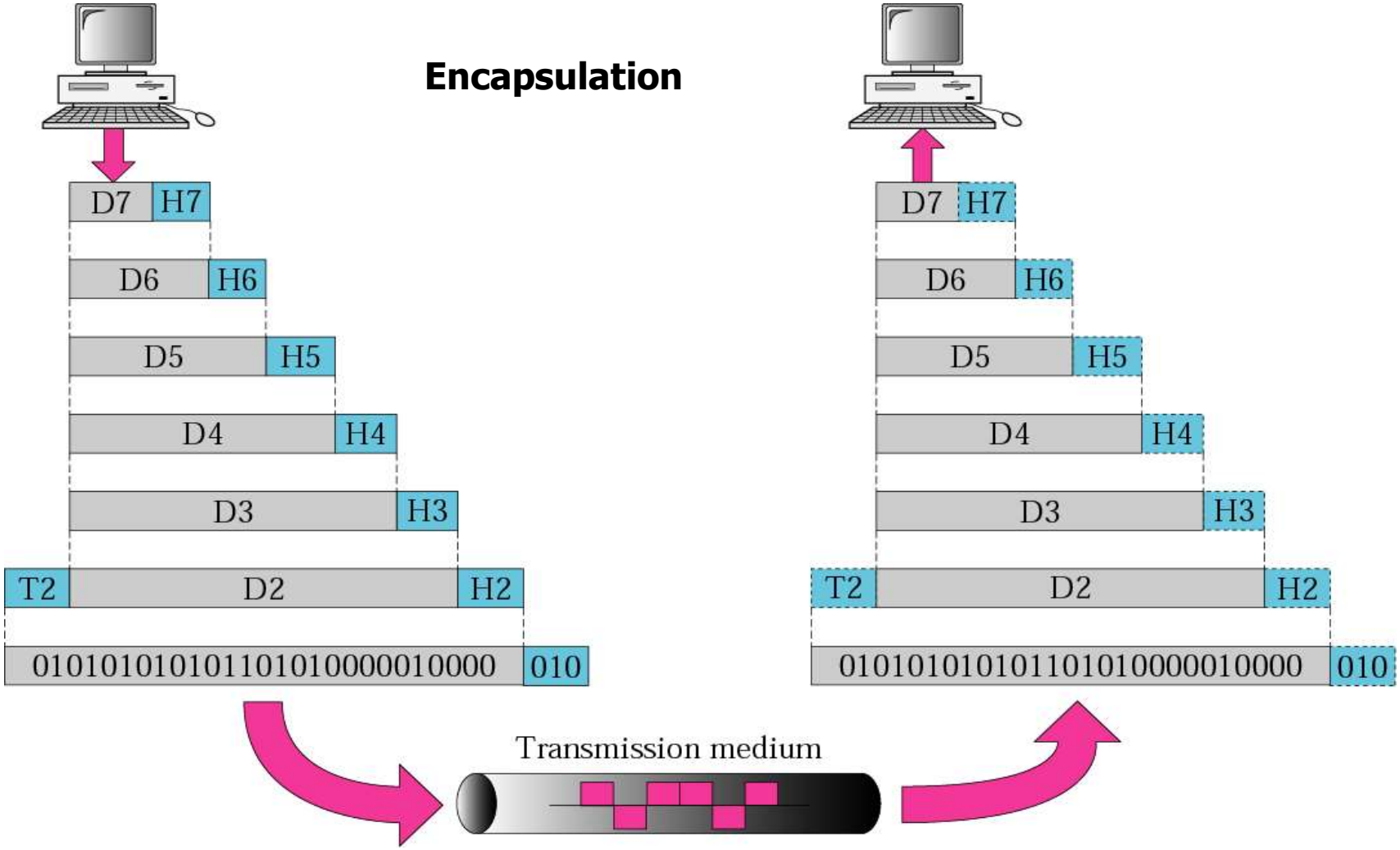
ISO is the organization.
OSI is the model

The purpose of OSI model is to show how the communication between different systems can be carried out without changing the logic of the underlying hardware and software.



The OSI model

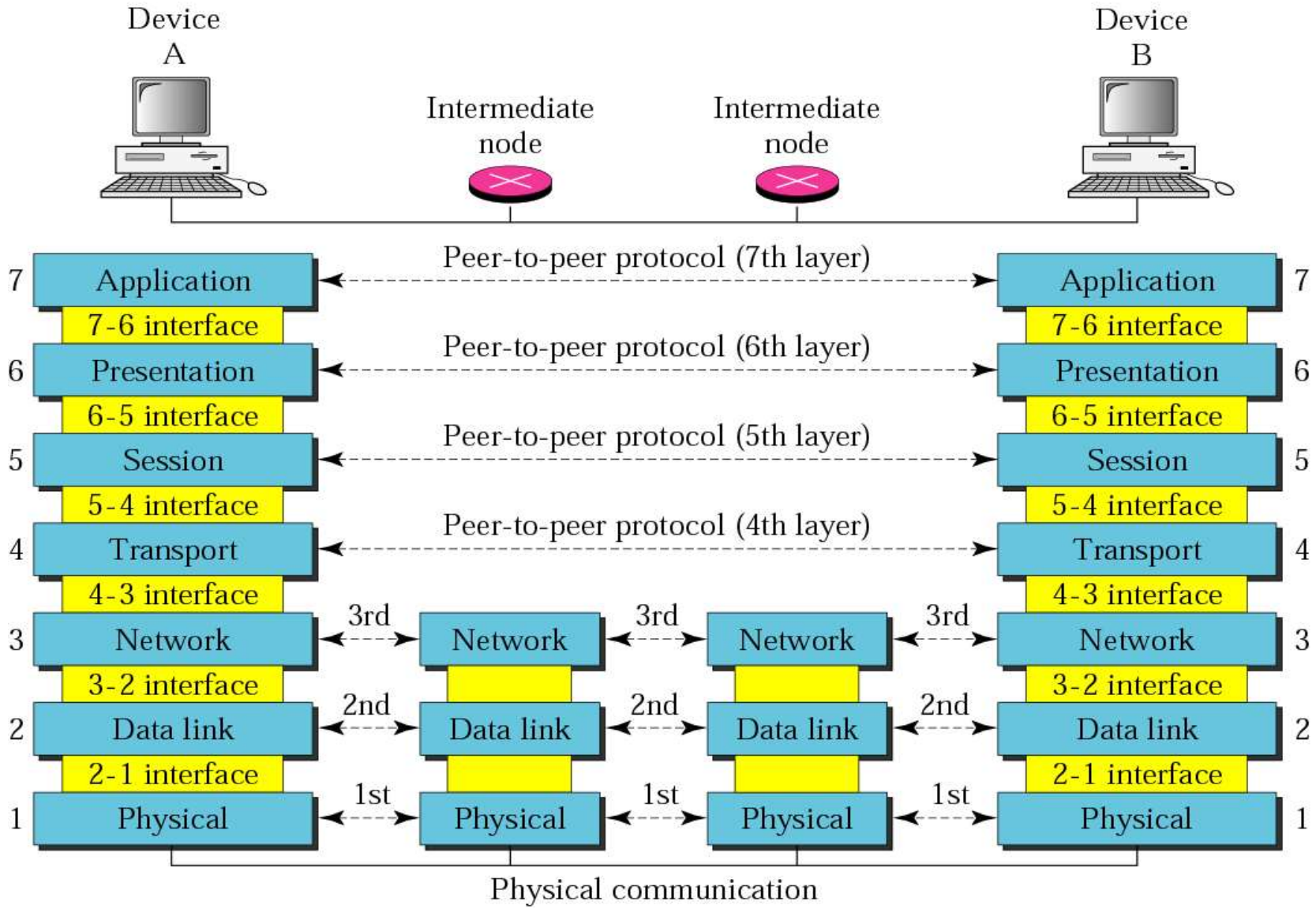
Encapsulation



An exchange using the OSI model

upper OSI layers implemented in software

lower layers are a combination of hardware and software



OSI layers

Layers in the OSI Model

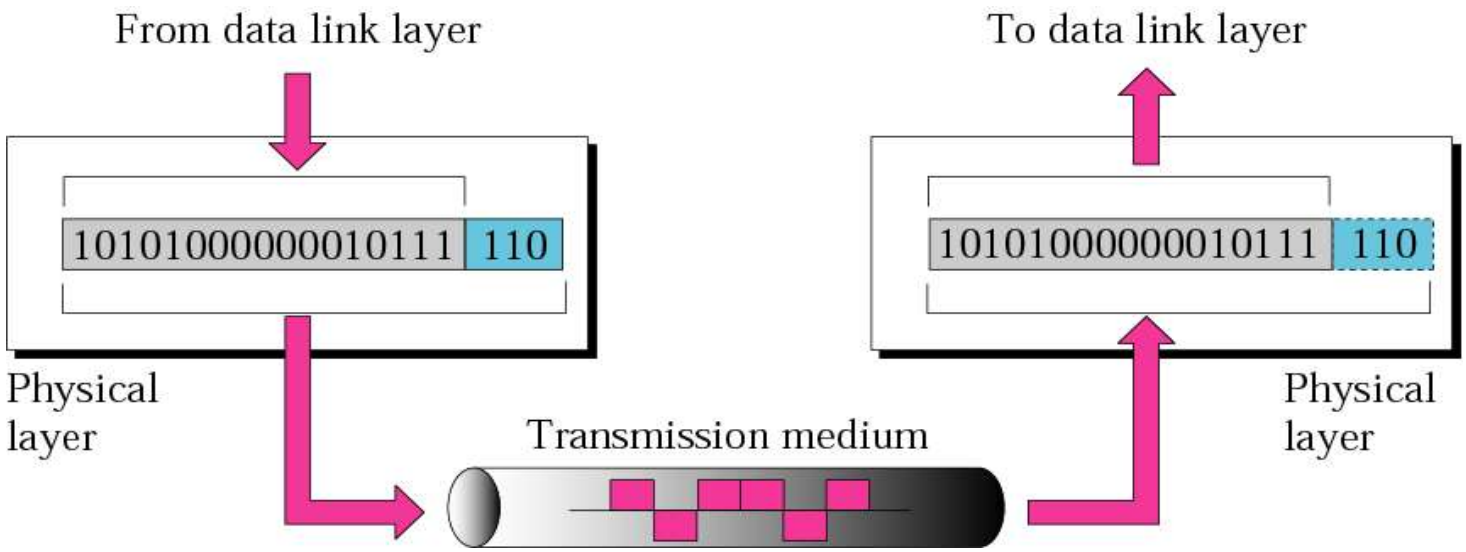
The functions of each layer in the OSI model is briefly described.

The topics discussed in this section include:

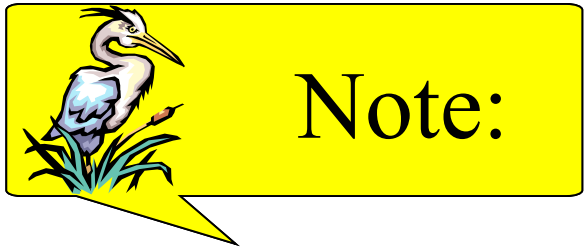
Physical Layer
Data Link Layer
Network Layer
Transport Layer
Session Layer
Presentation Layer
Application Layer
Summary of Layers

Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium.



Physical layer



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

The physical Layer is also concerned with

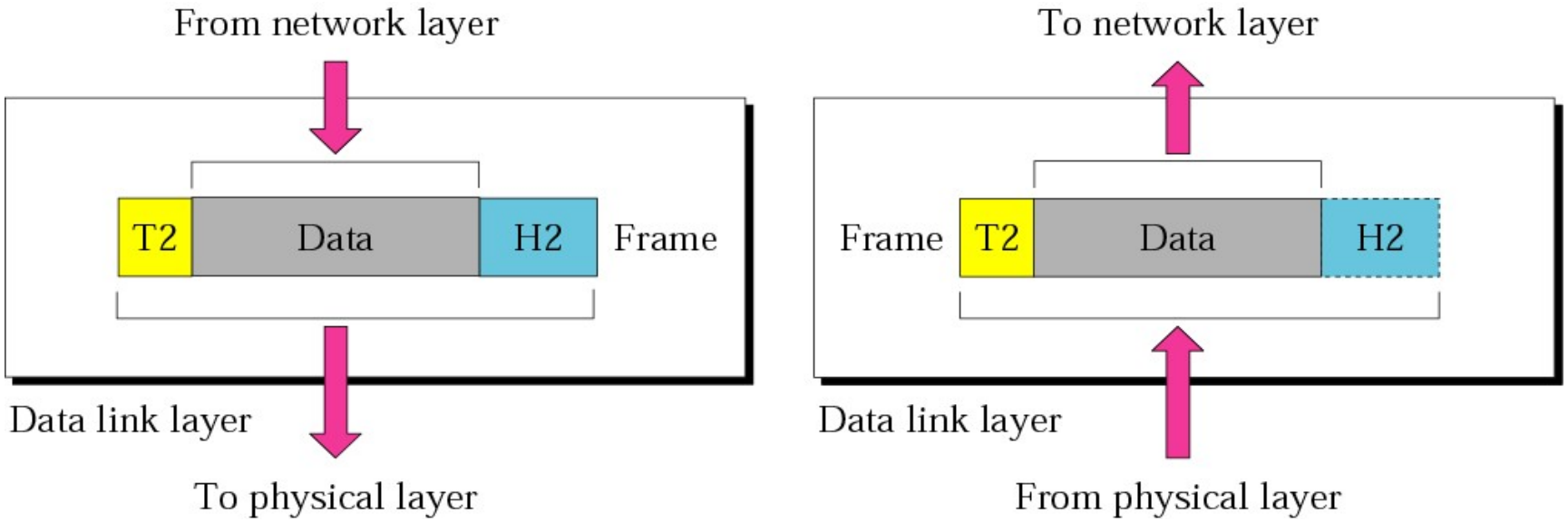
- Physical characteristics of interfaces and media
- Representation of bits
- Data rate
- Line configuration
- Physical topology
- Transmission mode

The physical Layer is also concerned with

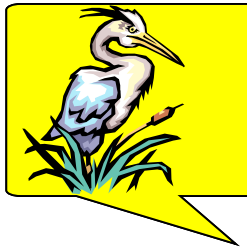
- **Physical characteristics of interfaces and media.** The physical layer defines the characteristics of the interface between the devices and the transmission media.
- **Representation of bits.** The physical layer data consists of a stream of **bits** (sequence of 0^s or 1^s) with no interpretation. To be transmitted, bits must be encoded into signals—electrical or optical. The physical layer defines the type of **encoding** (how 0^s and 1^s are changed to signals, the voltage representation for 0 and 1).
- **Data rate.** The **transmission rate**—the number of bits sent each second—is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

- **Line configuration.** The physical layer is concerned with the connection of devices to the media. In a **point-to-point configuration,** two devices are connected together through a dedicated link. In a **multipoint configuration,** a link is shared between several devices.
- **Physical topology.** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, star, tree, bus, ring topologies.
- **Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

2. Data Link Layer



Data link layer



Note:

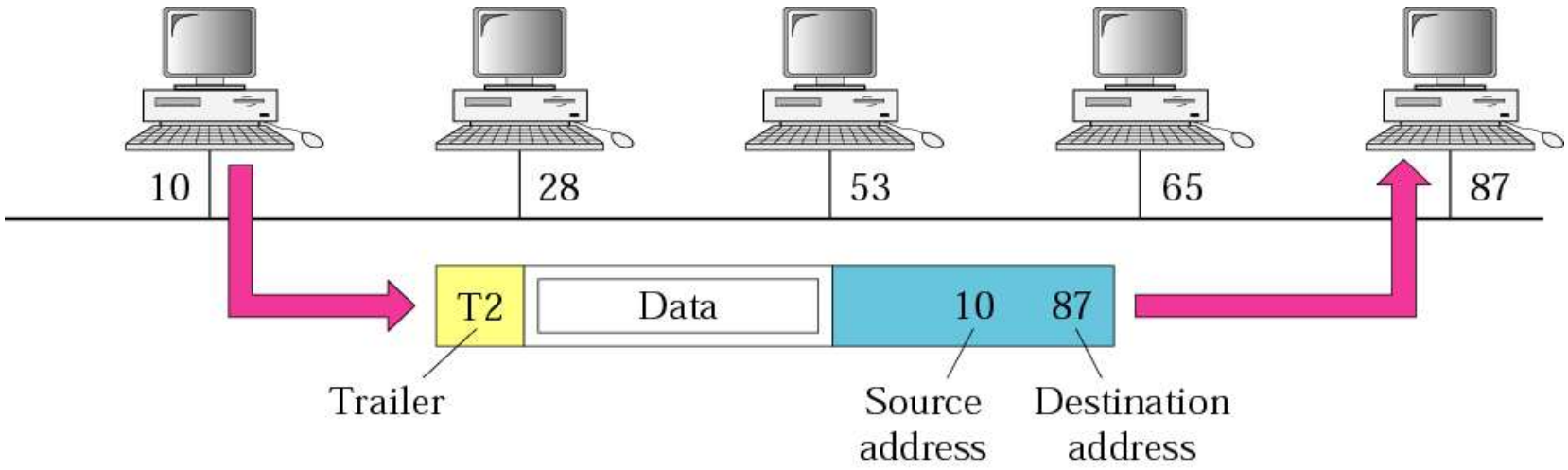
The data link layer is responsible for moving frames from one hop (node) to the next.

The responsibilities of the **data link layer** include the following

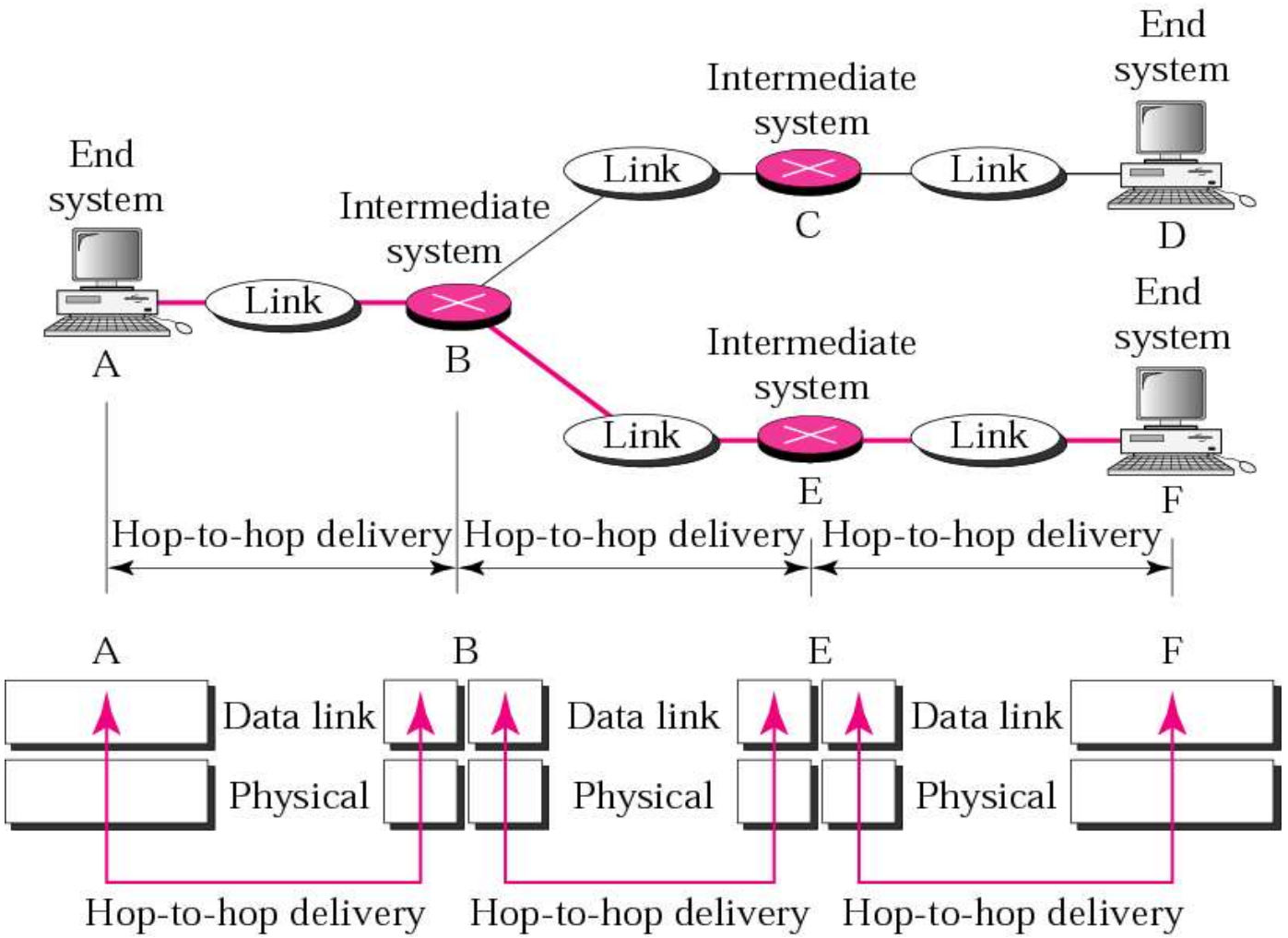
- **Framing.**
- **Physical addressing**
- **Flow control.**
- **Error control.**
- **Access control.**

The responsibilities of the **data link layer** include the following:

- **Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called **frames.**
- **Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the connecting device that connects the network to the next one.
- **Flow control.** If the rate at which the data is absorbed by the receiver is less than the rate produced at the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.
- **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.



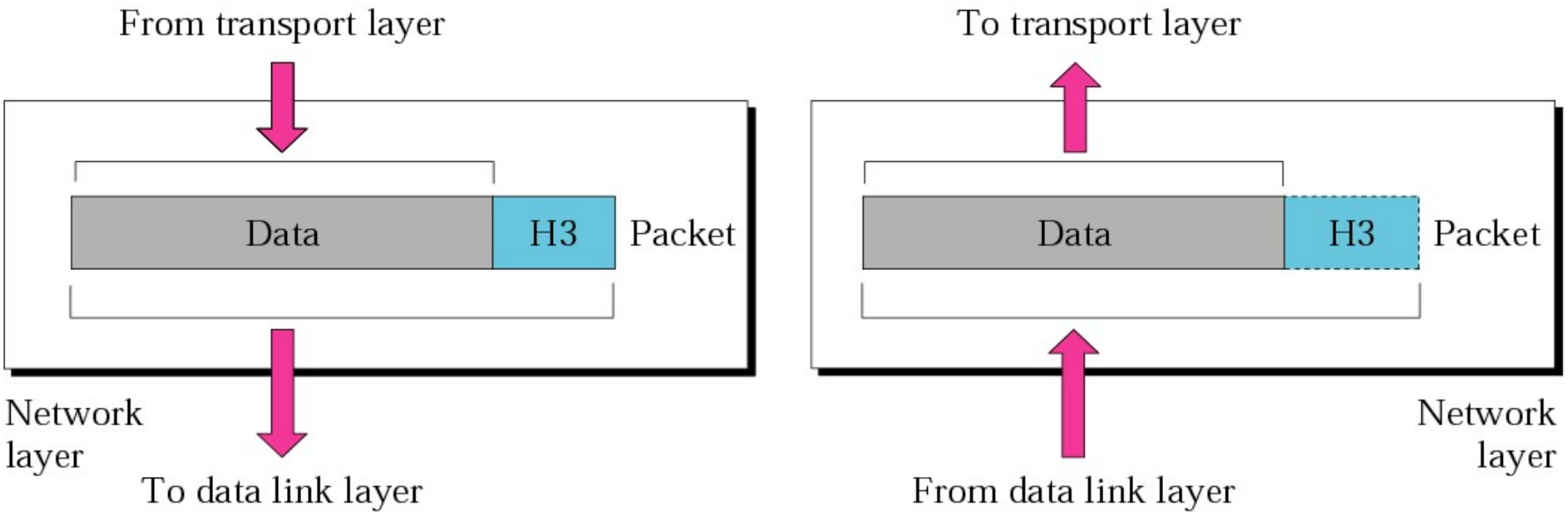
Physical addresses



Hop-to-hop delivery

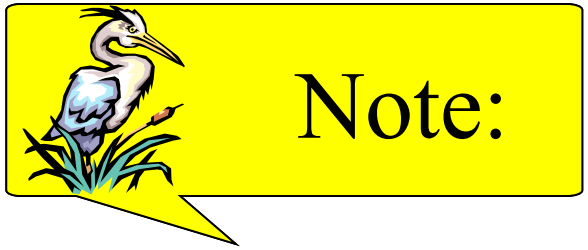
3. Network Layer

N/w layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks



Network layer

…Network Layer



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

…Network Layer

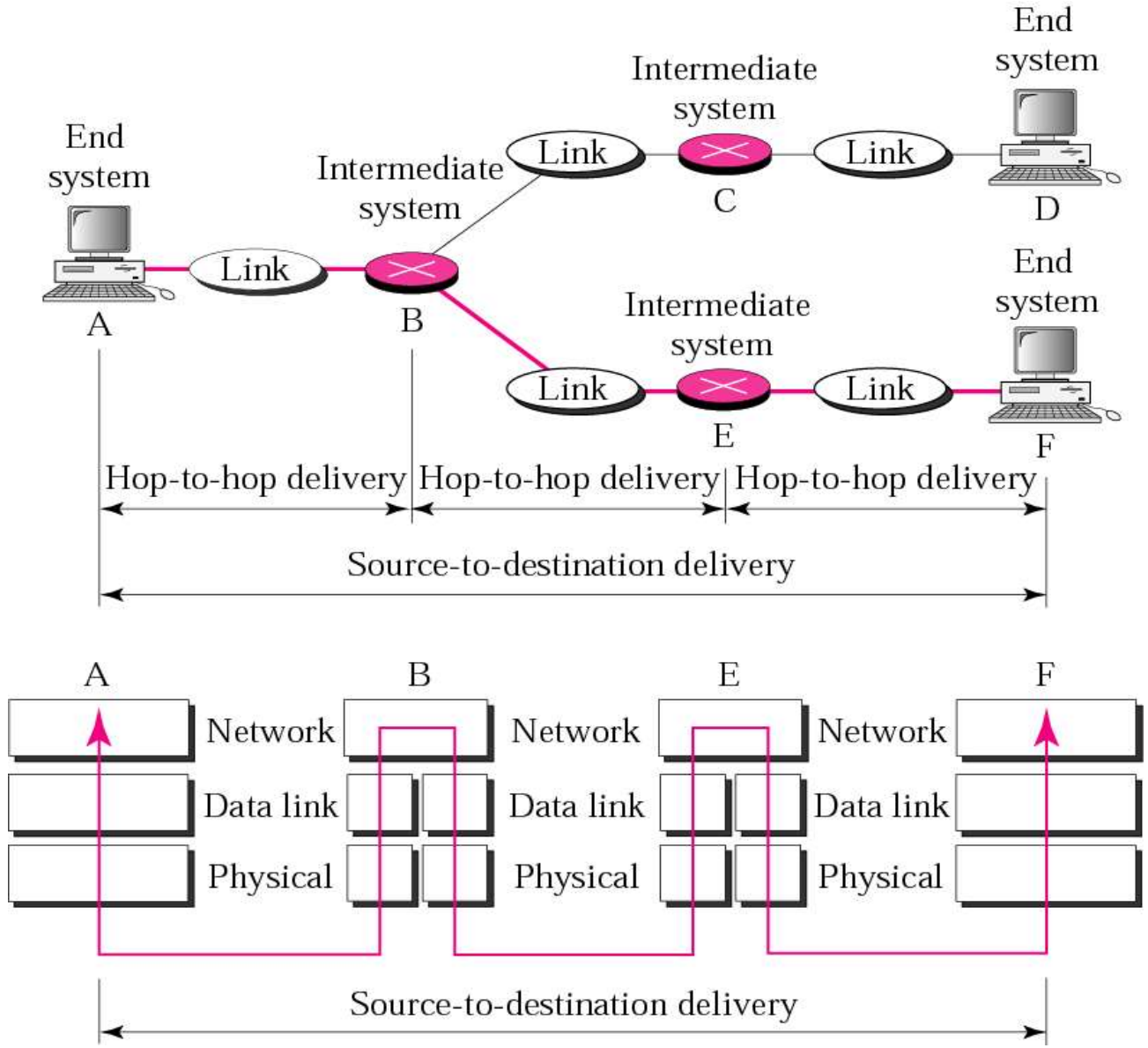
Responsibilities of the Network Layer include the following:

- **Logical addressing.**
- **Routing.**

…Network Layer

- **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally.
  - If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems.
  - The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing.** When independent networks or links are connected together to create **internetworks** (network of networks) or a large network, the connecting devices (called *routers* or *switches*) route or switch the packets to their final destination

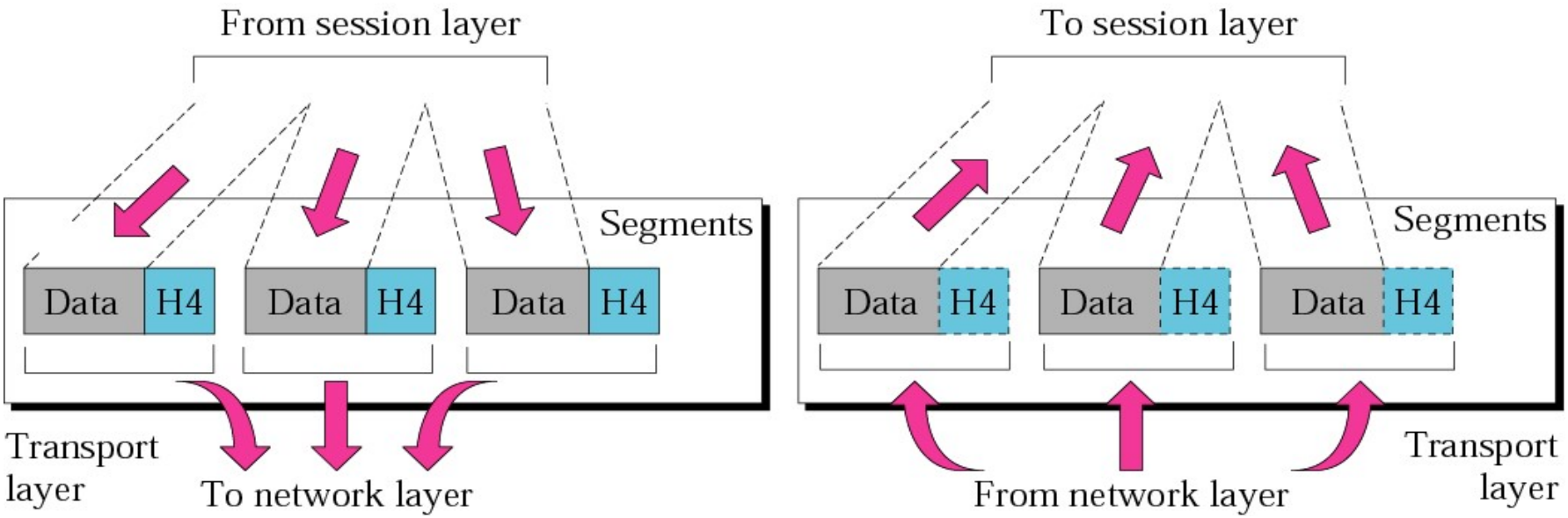
…Network Layer



Source-to-destination delivery

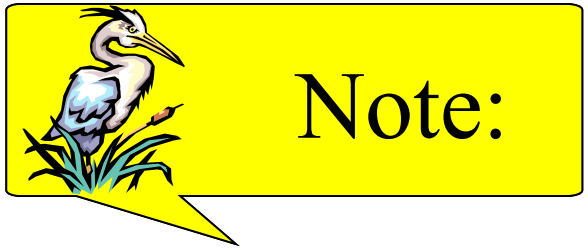
4. Transport Layer

Transport layer is responsible for process-to-process delivery of the entire message.



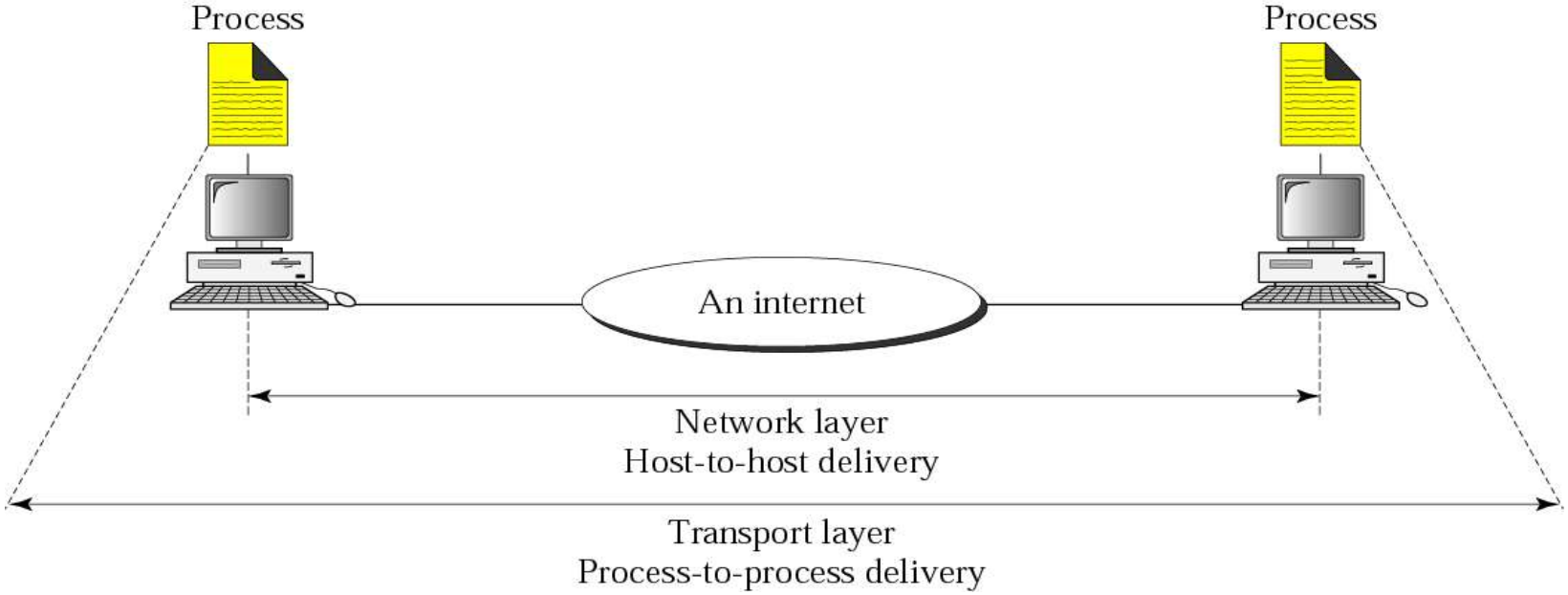
Transport layer

..Transport Layer

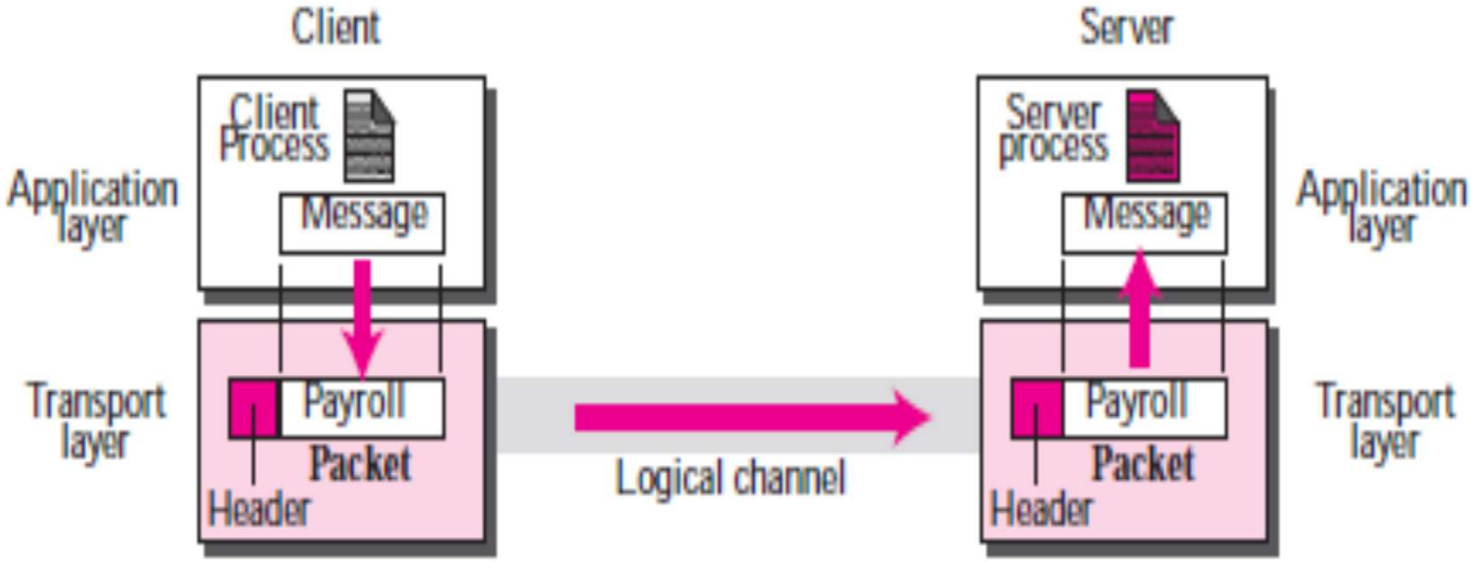


The transport layer is responsible for the delivery of a segment from one process to another.

..Transport Layer



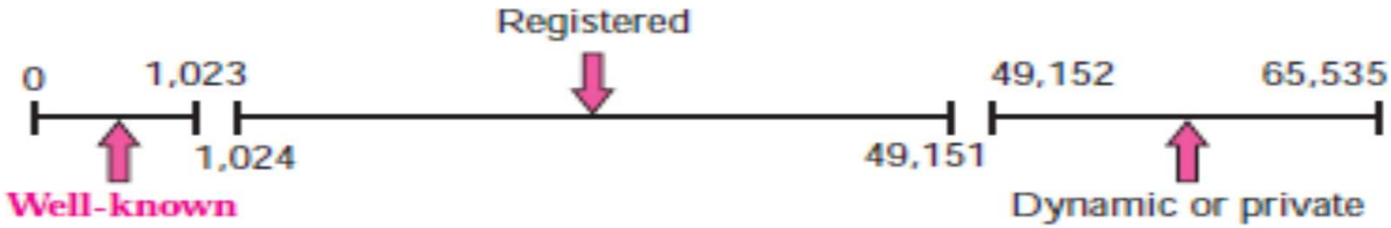
Reliable process-to-process delivery of a message



..Transport Layer

The responsibilities of the transport layer include the following:

- **Service-point addressing.**
  - **Port Address**



- **Segmentation and reassembly.**
- **Connection control.**
  - **Connection less/ Connection oriented**
- **Flow control.**
- **Error control.**

..Transport Layer

Examples: Well Known Port Number

Number	name	protocol	
7	Echo	TCP, UDP	Echo service
20	FTP-data	TCP, SCTP	File Transfer Protocol data transfer
21	FTP	TCP, UDP, SCTP	File Transfer Protocol (FTP) control connection
22	SSH-SCP	TCP, UDP, SCTP	Secure Shell, secure logins, file transfers (scp, sftp), and port forwarding
23	Telnet	TCP	Telnet protocol–unencrypted text communications
25	SMTP	TCP	Simple Mail Transfer Protocol, used for email routing between mail servers
53	DNS	TCP, UDP	Domain Name System name resolver
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP, UDP, SCTP	Hypertext Transfer Protocol (HTTP) uses TCP in versions 1.x and 2.

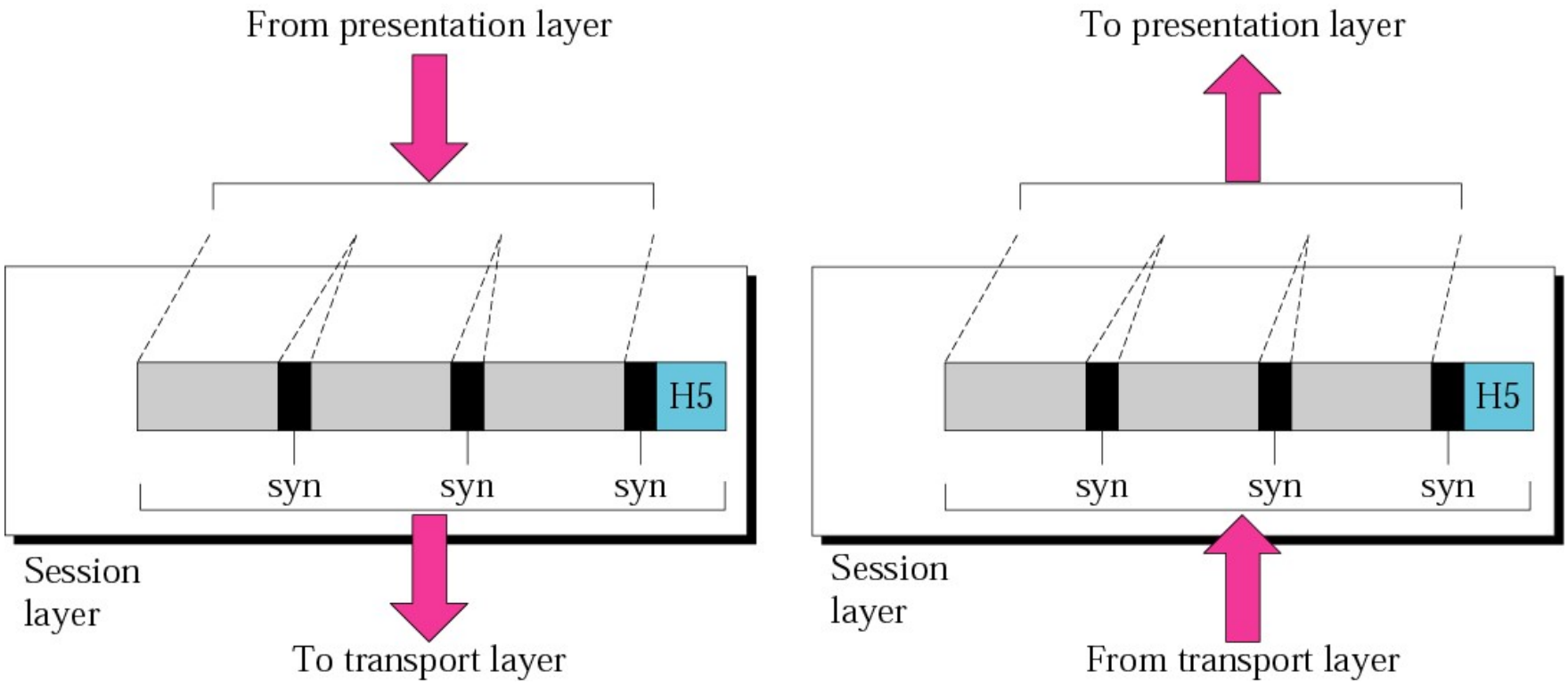
..Transport Layer responsibilities

- **Service-point addressing.** Computers often run several programs at the same time.
  - For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.
  - The transport layer header must therefore include a type of address called a *service-point address* (or port address).
  - The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly.** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

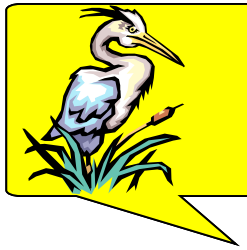
..Transport Layer responsibilities

- **Connection control.** The transport layer can be either connectionless or connection oriented.
- A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
- A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- **Flow control.** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control.** Like the data link layer, the transport layer is responsible for error control. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without *error* (damage, loss, or duplication). Error correction is usually achieved through retransmission

5. Session Layer



Session layer



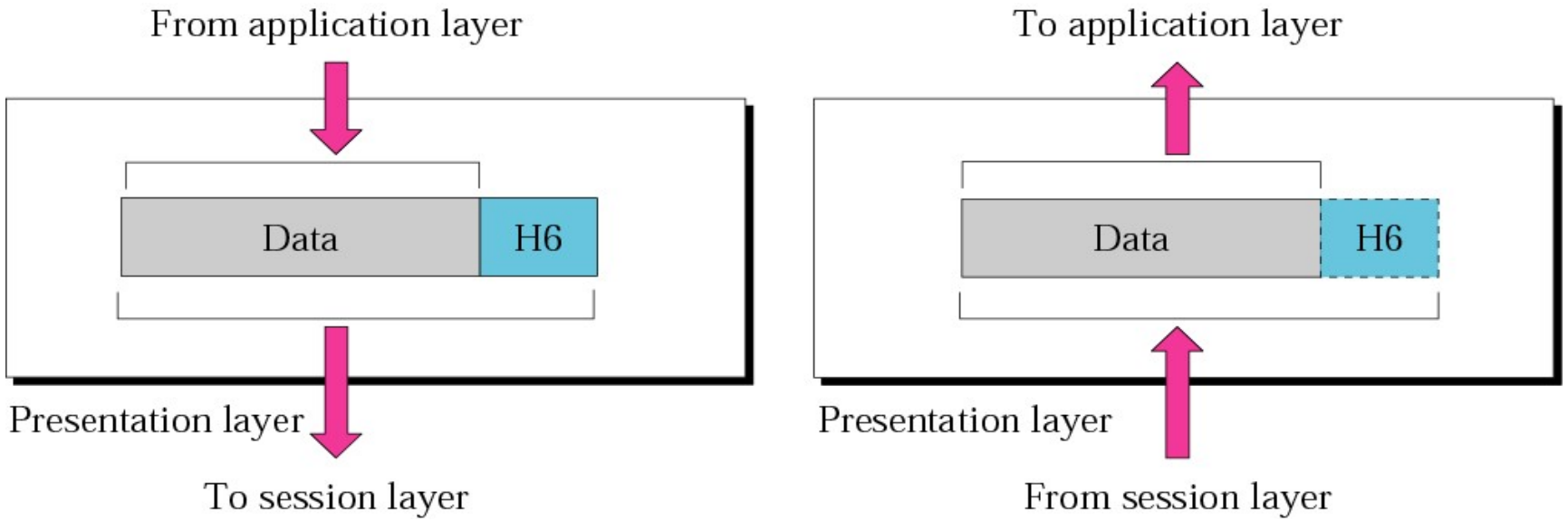
Note:

The **session layer** is the network dialog controller. It establishes, maintains, and synchronizes the interaction between communicating systems.

…Session layer

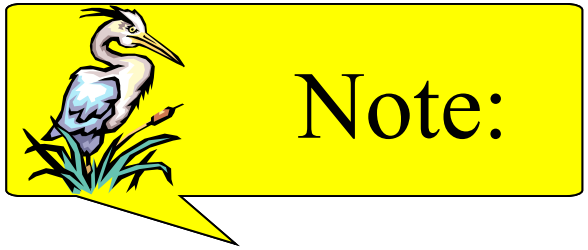
- **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization.** The session layer allows a process to add **checkpoints (synchronization points)** into a stream of data.
  - For example, if a system is sending a file of 2,000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently.
  - In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

6. Presentation Layer



Presentation layer

…Presentation Layer



The **presentation layer** is concerned with the syntax and semantics of the information exchanged between two systems.

…Presentation Layer

Responsibilities of Presentation Layer

Translation.

Different computer architecture use data representation and different encoding systems Common format necessary for Interoperability

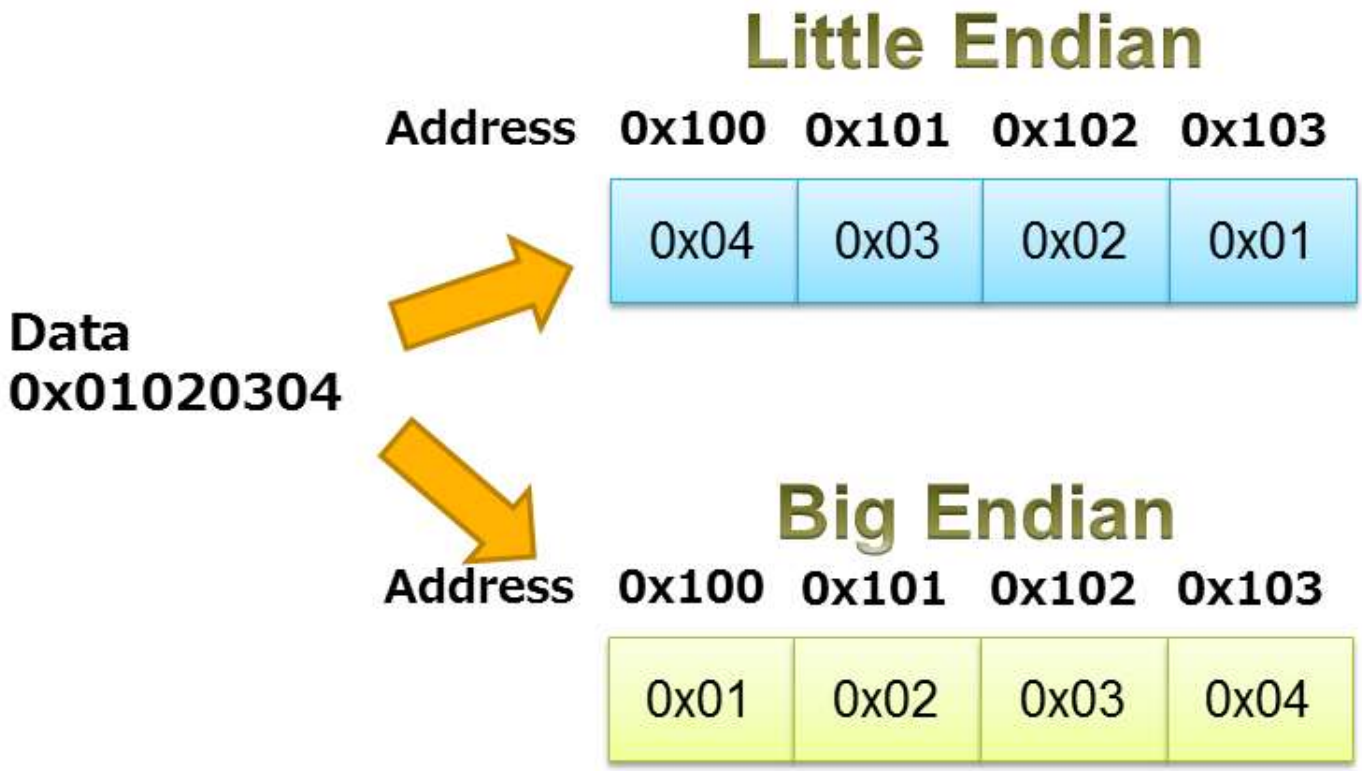
Encryption & Decryption

Compression & Decompression

character	GB18030 encoding	UTF-32 encoding
纵	10111111 01101100	00000000 00000000 01111110 00100111

Representation of a chinees character in two different encoding system.

…Presentation Layer

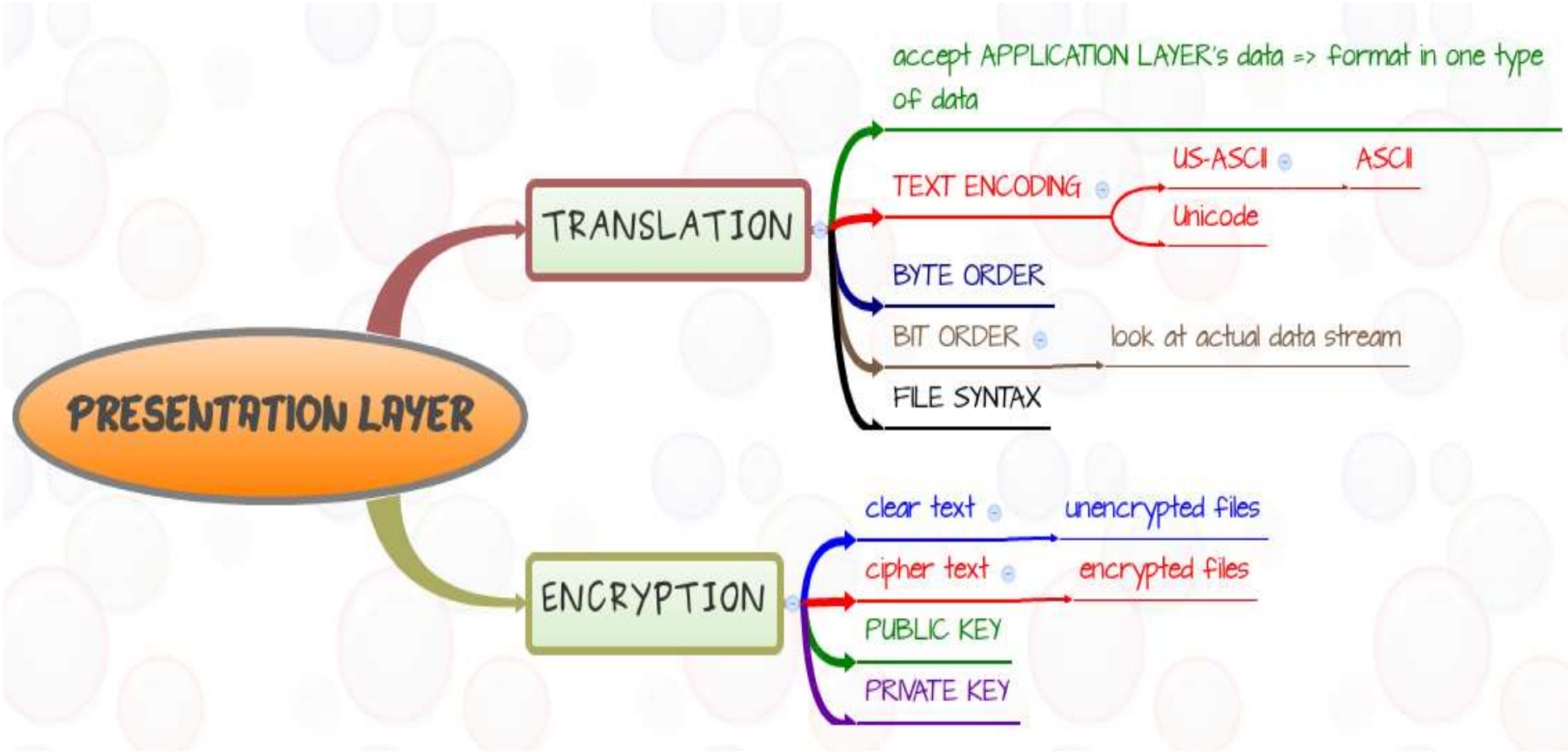


…Presentation Layer

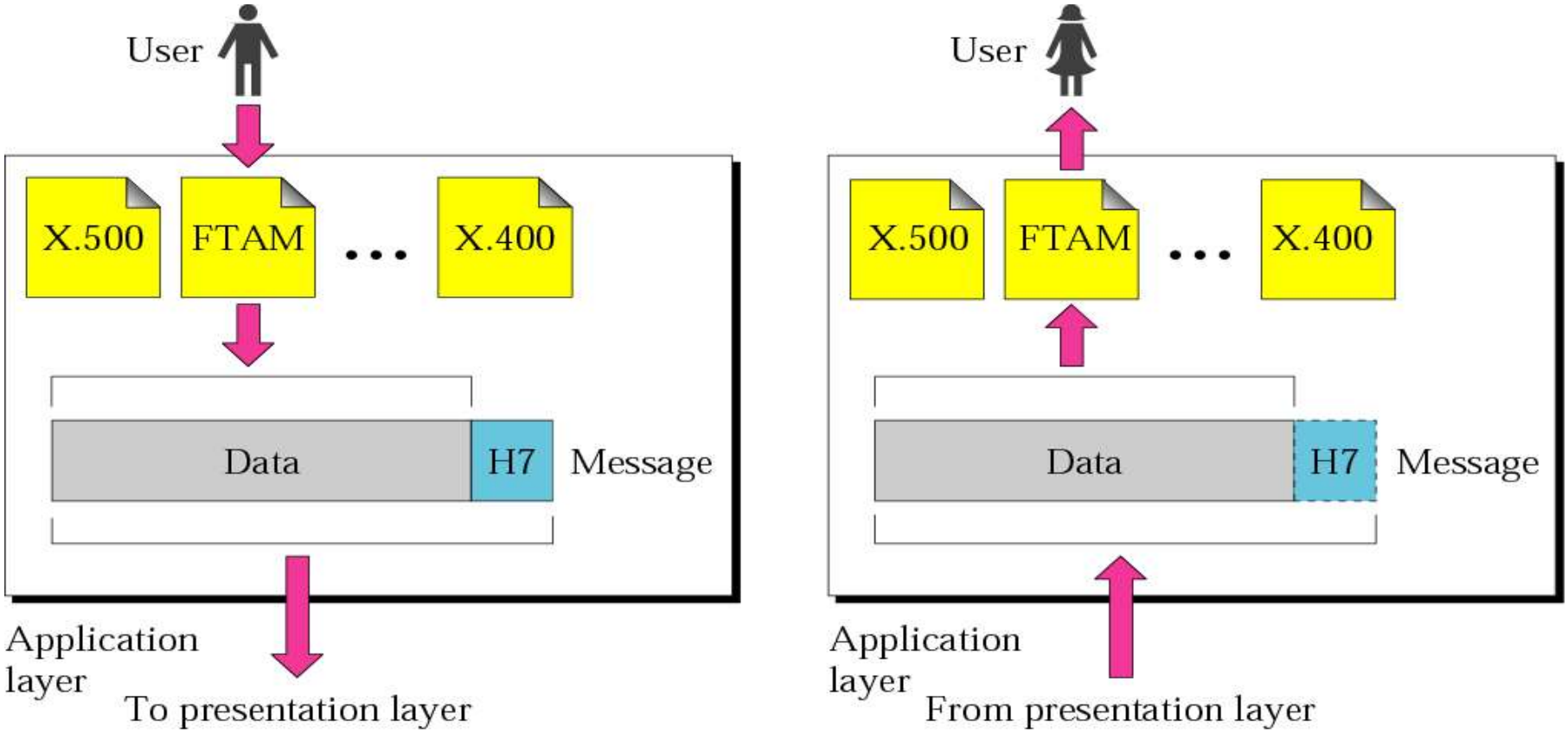
Presentation layer responsibilities

- **Translation.** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on.
  - The information should be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
  - The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- **Encryption.** To carry sensitive information a system must be able to assure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

…Presentation Layer

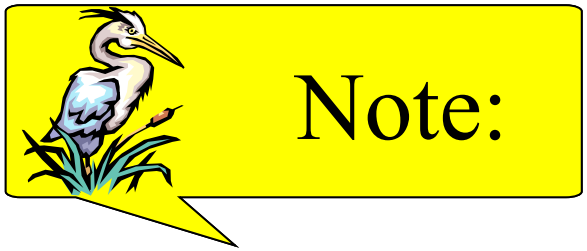


7. Application Layer



Application layer

…Application Layer



The **application layer** provides the interfaces and services to access the network.

The unit of communication at the application layer is a message.

The application layer provides interfaces & allows user to access the services of our private internet or the global Internet.

The application layer only standardizes communication.

Many protocols are defined at this layer to provide services such as electronic mail, file transfer, accessing the World Wide Web, and so on.

…Application layer

- **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. **PuTTY** is an example of a virtual terminal.
- **File transfer, access, and management (FTAM).** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **E-mail services.** This application provides the basis for e-mail forwarding and storage.
- **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

…Application Layer

Application layer uses a number of protocols, the main among which are as follows −

Hyper Text Transfer Protocol, ***HTTP*** − It is the underlying protocol for world wide web. It defines how hypermedia messages are formatted and transmitted.

File Transfer Protocol, ***FTP*** − It is a client-server based protocol for transfer of files between client and server over the network.

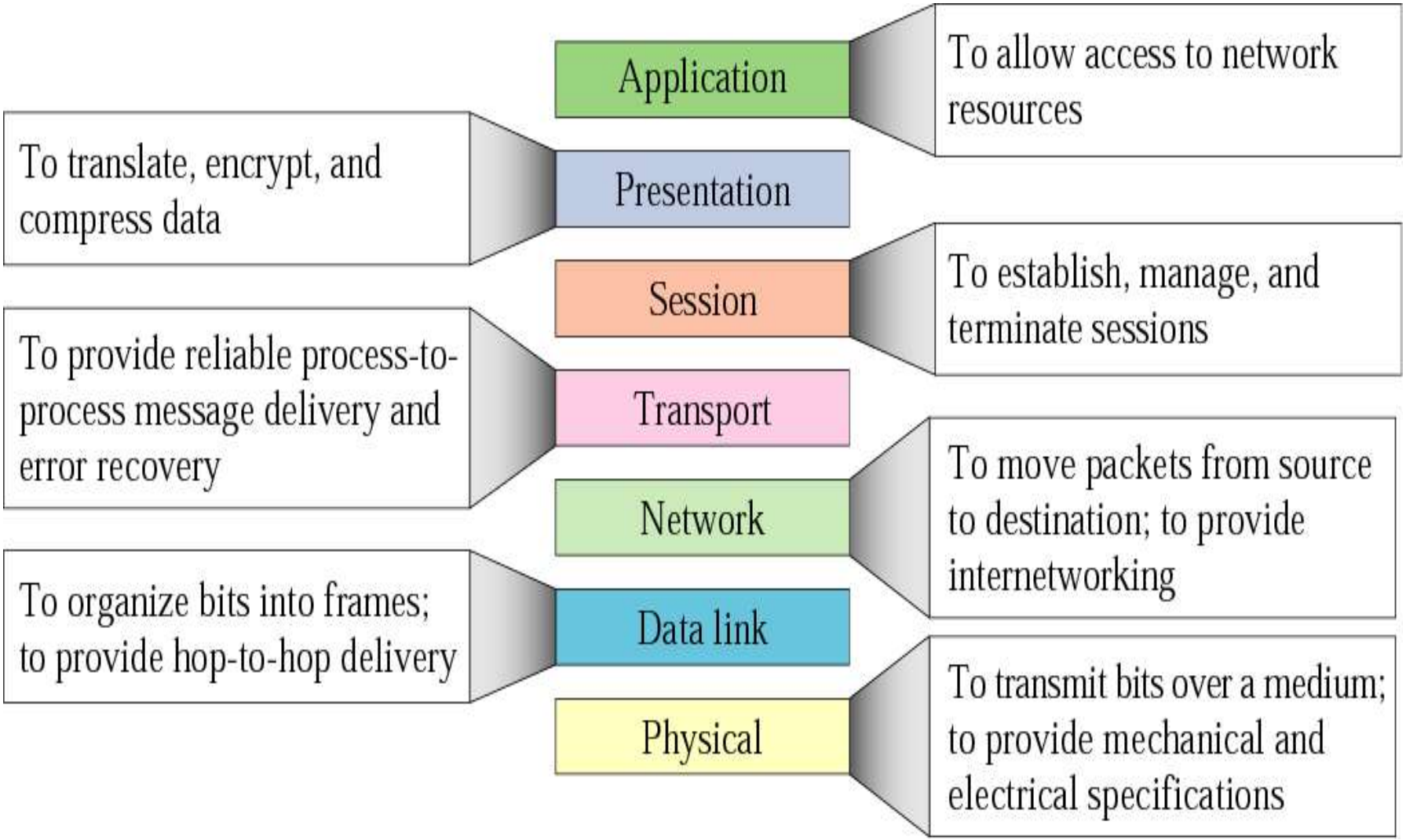
Simple Mail Transfer Protocol, ***SMTP*** − It lays down the rules and semantics for sending and receiving electronic mails (e-mails).

Domain Name System, ***DNS*** − It is a naming system for devices in networks. It provides services for translating domain names to IP addresses.

TELNET − It provides bi-directional text-oriented services for remote login to the hosts over the network.

Simple Network Management Protocol, ***SNMP*** − It is for managing, monitoring the network and for organizing information about the networked devices

OSI specifies a strict modular separation of functionality at these layers and provides protocol implementations for each layer.



Summary of layers

TCP/IP Protocol Suite

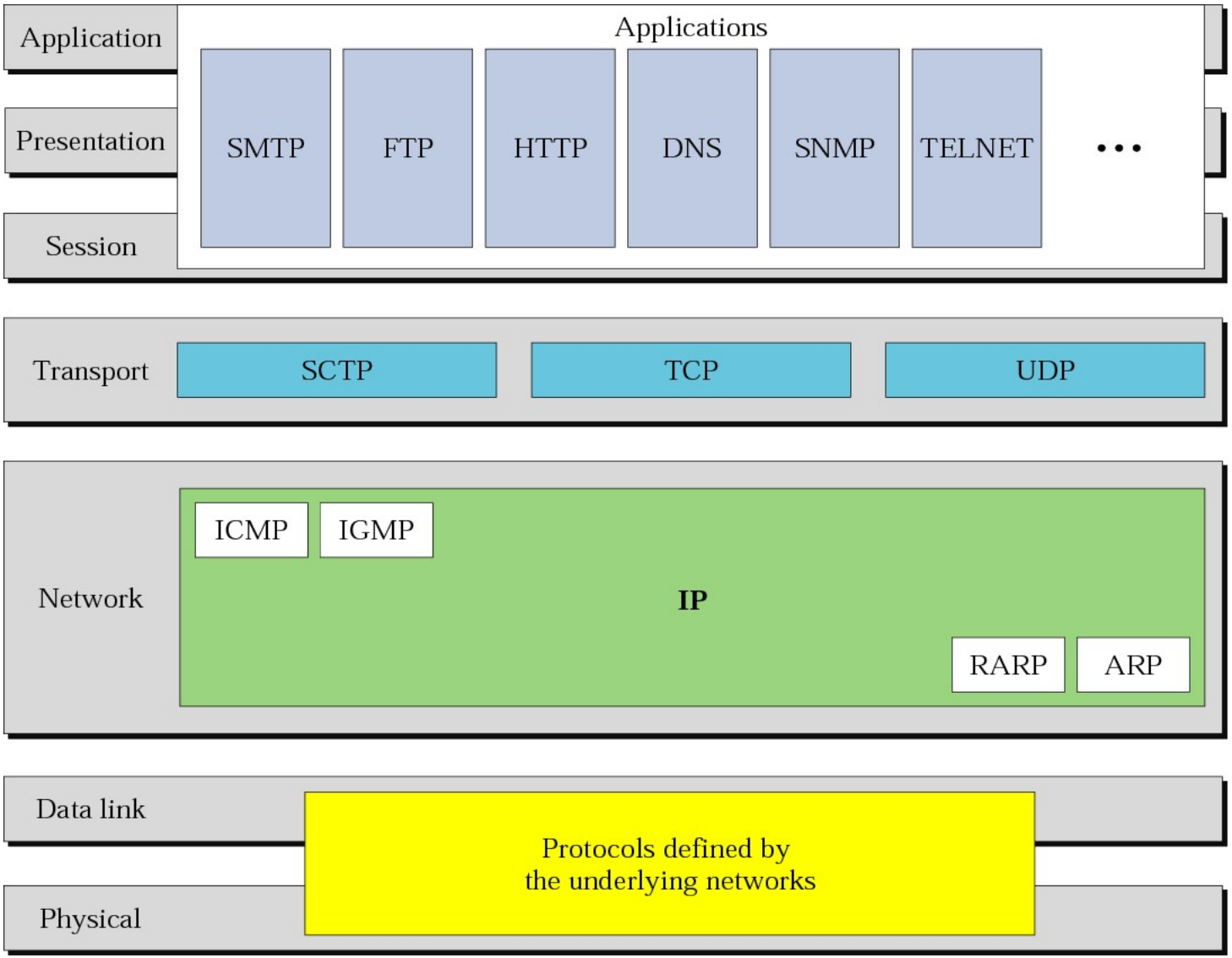
The TCP/IP protocol suite is made of four layers: Network interface layer (physical + data link), network, transport, and application. The first three layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.

It was developed prior to OSI model.

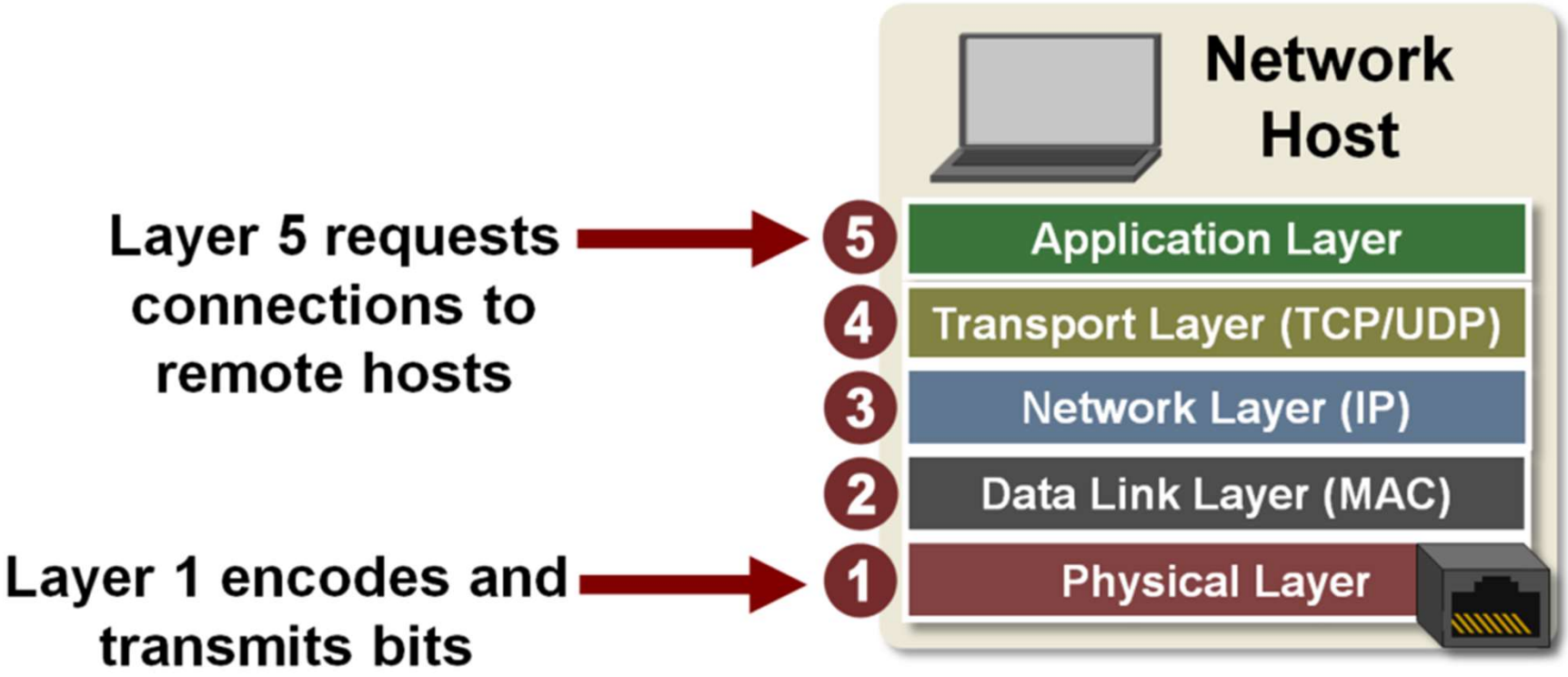
The topics discussed in this section include:

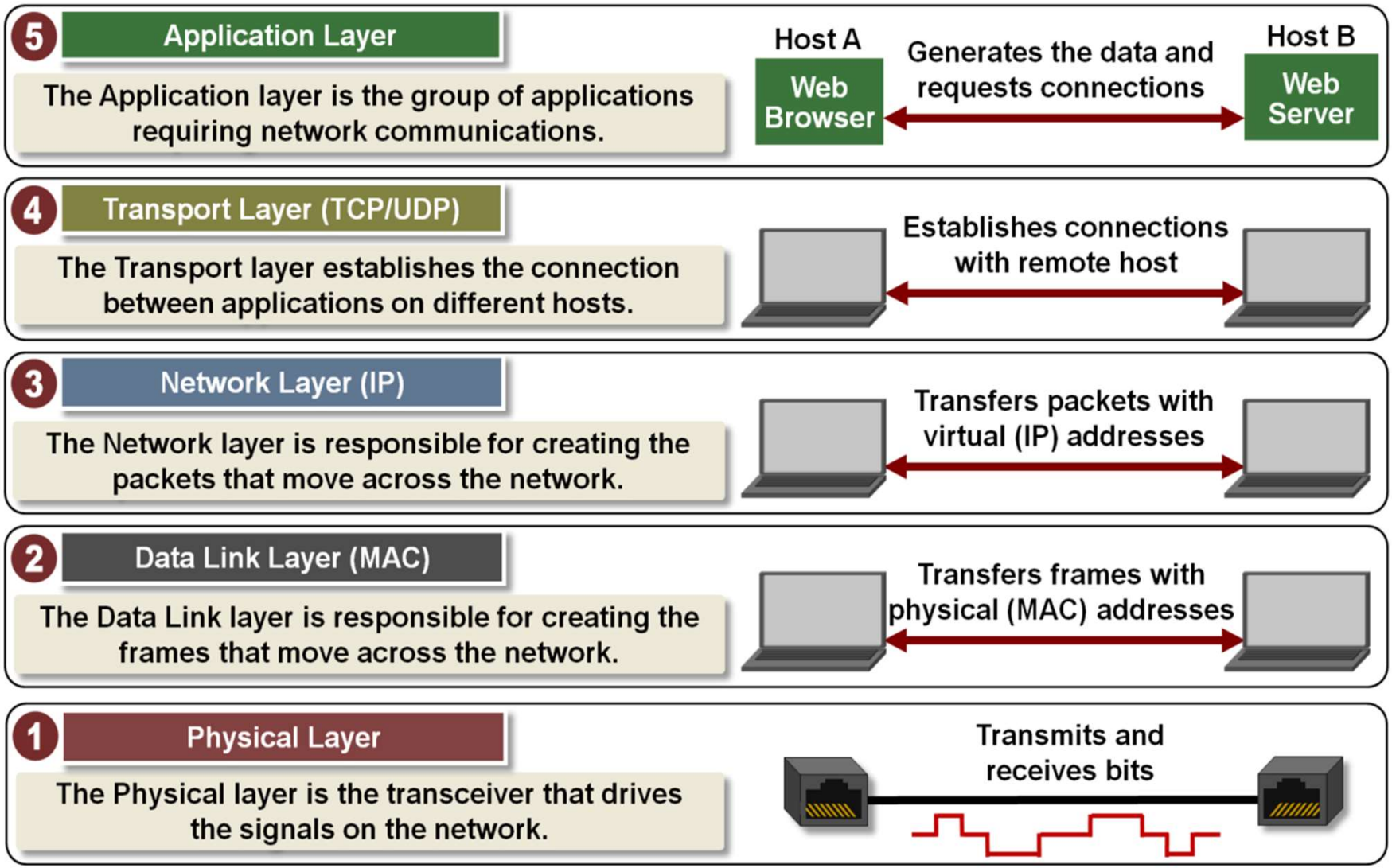
Network Interface Layer
Network Layer
Transport Layer
Application Layer

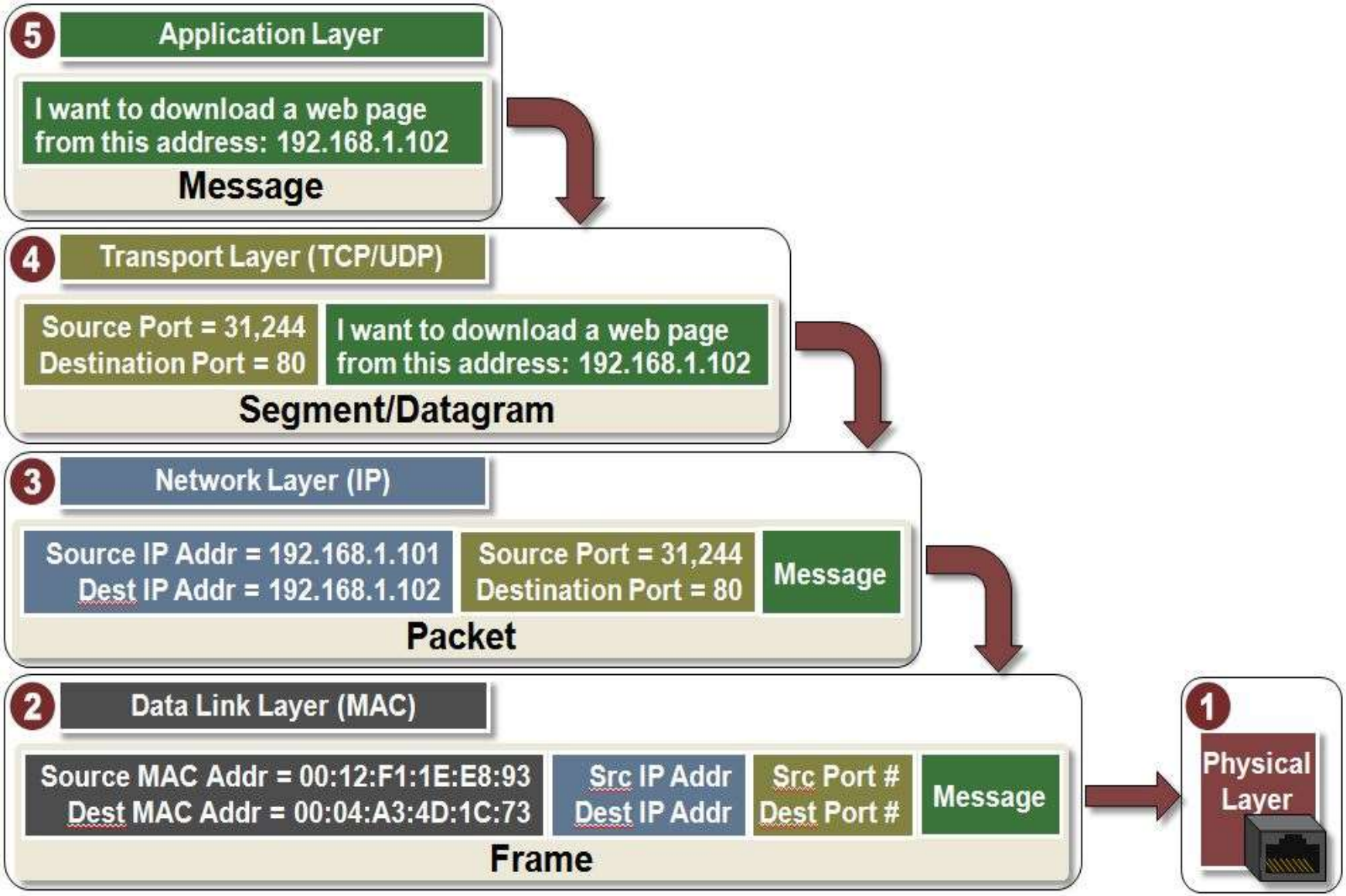
TCP/IP



TCP/IP and OSI model


Network Host
Layer 5 requests connections to remote hosts
5
Application Layer
4
Transport Layer (TCP/UDP)
3
Network Layer (IP)
2
Data Link Layer (MAC)
Layer 1 encodes and transmits bits
1
Physical Layer

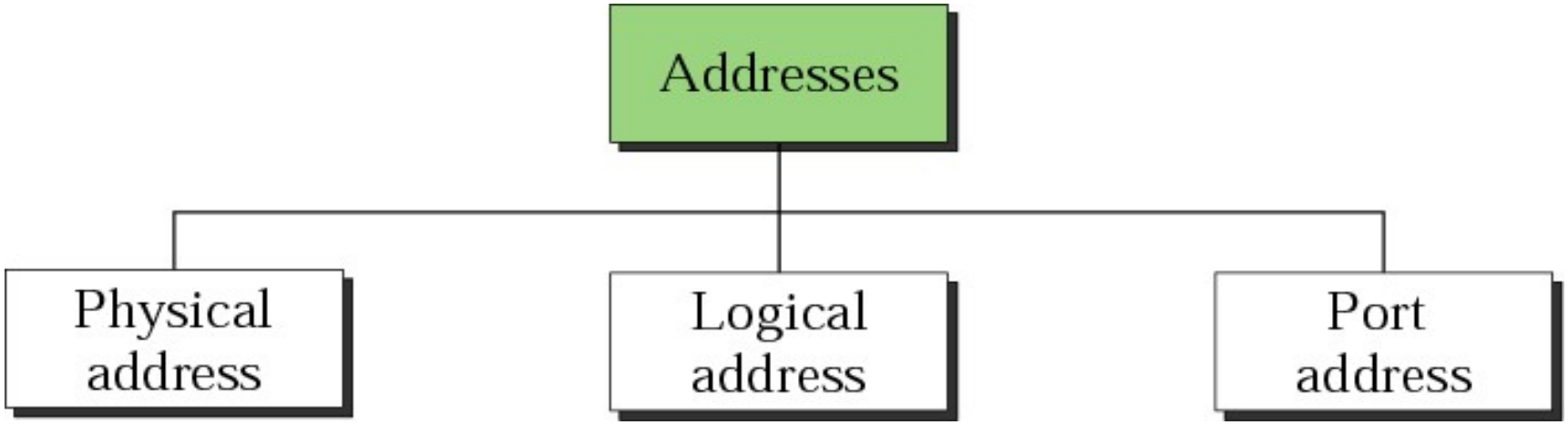

5
Application Layer
The Application layer is the group of applications requiring network communications.
Host A
Web Browser
Generates the data and requests connections
Host B
Web Server
4
Transport Layer (TCP/UDP)
The Transport layer establishes the connection between applications on different hosts.
Establishes connections with remote host
3
Network Layer (IP)
The Network layer is responsible for creating the packets that move across the network.
Transfers packets with virtual (IP) addresses
2
Data Link Layer (MAC)
The Data Link layer is responsible for creating the frames that move across the network.
Transfers frames with physical (MAC) addresses
1
Physical Layer
The Physical layer is the transceiver that drives the signals on the network.
Transmits and receives bits


5
Application Layer
I want to download a web page from this address: 192.168.1.102
Message
4
Transport Layer (TCP/UDP)
Source Port = 31,244
Destination Port = 80
I want to download a web page from this address: 192.168.1.102
Segment/Datagram
3
Network Layer (IP)
Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102
Source Port = 31,244
Destination Port = 80
Message
Packet
2
Data Link Layer (MAC)
Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73
Src IP Addr
Dest IP Addr
Src Port #
Dest Port #
Message
Frame
1
Physical Layer

Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc…	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

The upper layers are almost always implemented in software;

lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.



Addresses in TCP/IP

Addresses

Physical Address: Also known as the link address

- It is address of the node as defined by the LAN or WAN
- Included in the frame by the data link layer.
- Lowest level address.

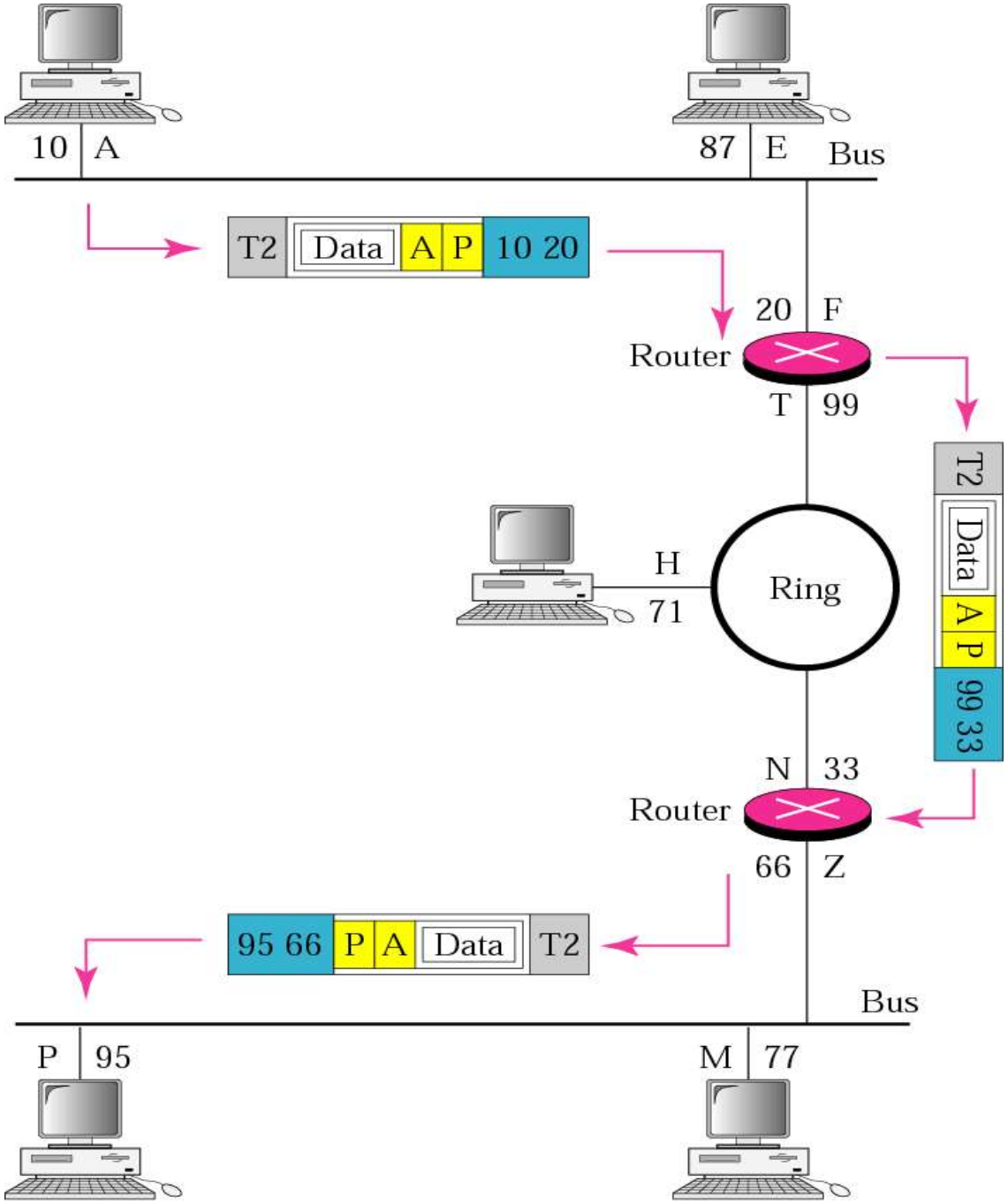
Logical Address: A universal addressing system in which each host can be identified uniquely regardless of the underlying physical network.

- 32 bit address
- No two publicly addressed and visible host on the internet can have same IP address.

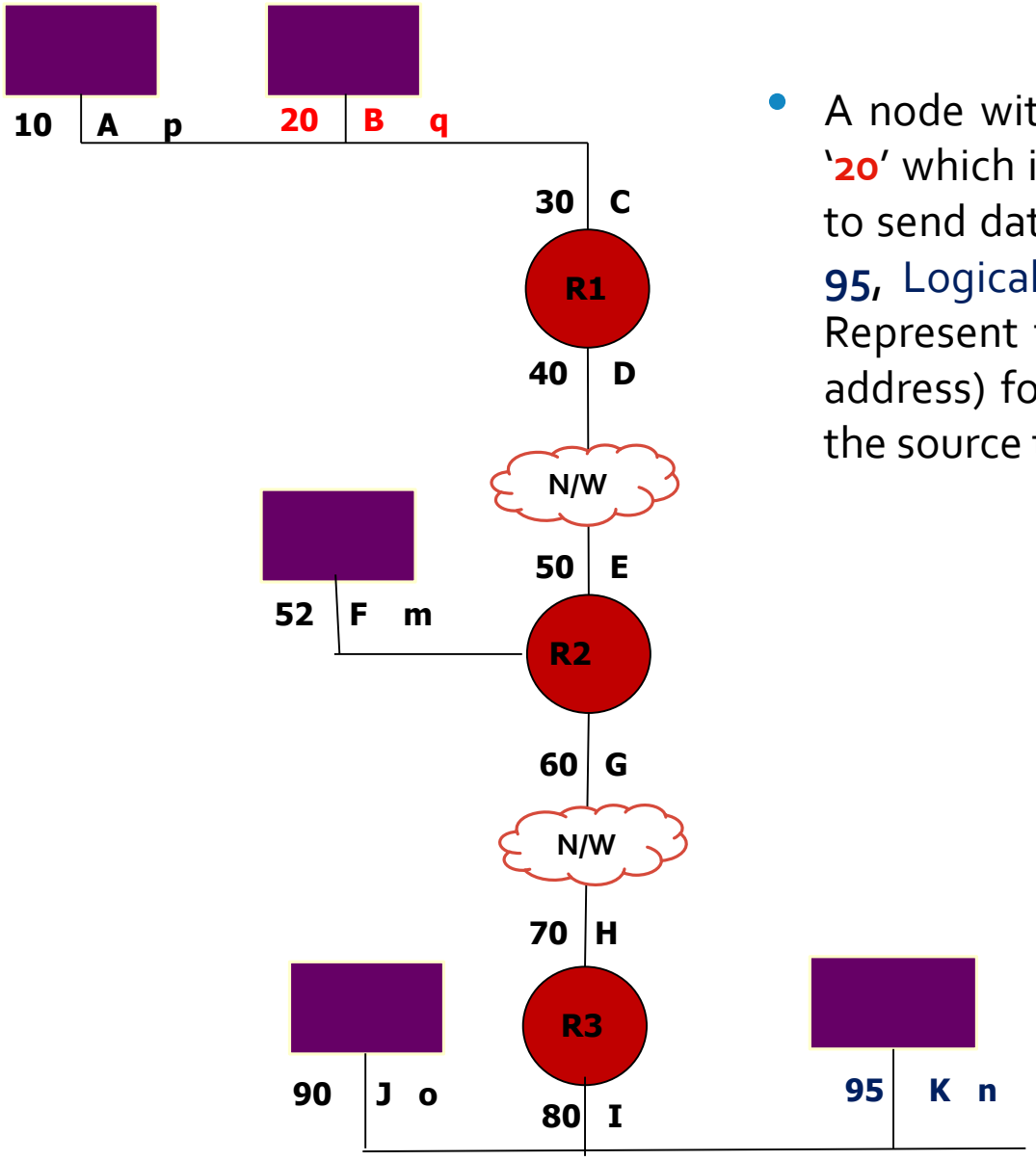
Port Address: Objective of Internet communication is process communicating with another process.

- Computer A can communicate with computer B using TELNET and at the same time computer A can communicate with C using FTP.

IP addresses- hop by hop communication

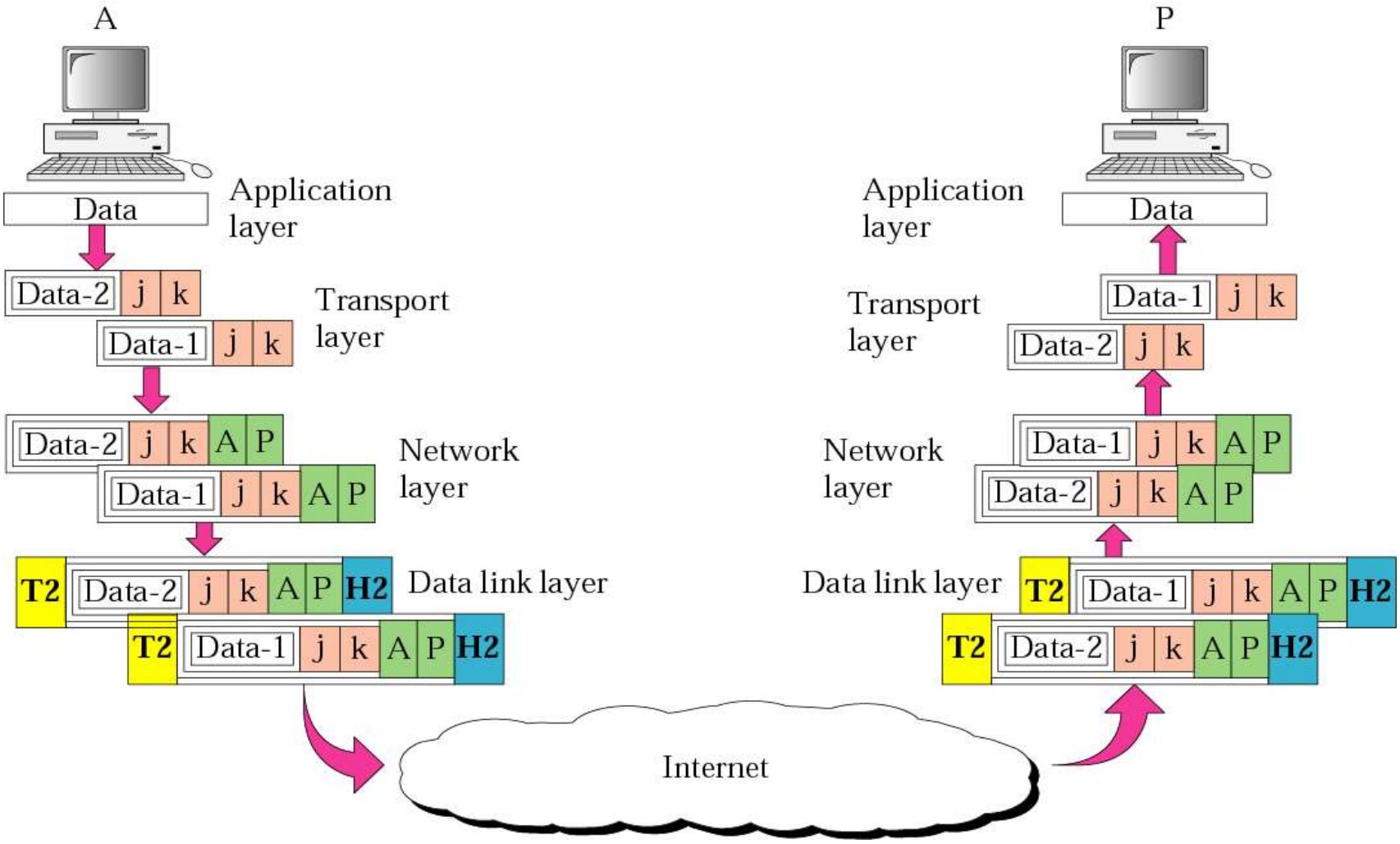


Problem



- A node with IP address **B** and MAC address '**20**' which is using the port address '**q**' wants to send data to a node with physical address **95**, Logical address **K** and port address '**n**'. Represent the addresses (MAC & IP & port address) for the Flow of the datagram from the source to the destination .

Port addresses



Connection Oriented v/s Connectionless Service

- **Connection-oriented - Reliable**
  - **Use of Acknowledgements (ACK)**
    - **Message oriented v/s byte Oriented**
- **Connectionless – Not reliable**
  - **No Acknowledgements (No ACK)**

Connection Oriented v/s Connectionless Service

Connection Oriented

- These are the two types of services that the lower layers provide to the upper layers
- **Connection-oriented** service is modeled after the telephone system
- In a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- In some cases when a **connection is established**, the sender, receiver, and subnet conduct a **negotiation** about the **parameters** to be used, such as maximum message size, quality of service required, and other issues.
- Typically, one side makes a proposal and the other side can **accept it, reject** it, or make a counterproposal.
- **Connection-oriented service is Reliable.**

Connectionless Service

- Based on the destination address the packets are routed from the source to the destination.
- Unreliable (meaning **not acknowledged**) connectionless service is often called datagram service.
- **Connectionless** service is modeled after the postal system, which also does not return an acknowledgement to the sender. .
- In other situations, the convenience of **not having to establish a connection** to send one message is desired, but **reliability is essential**. The **acknowledged datagram** service can be provided for these applications.
- It is like sending a **registered letter** and requesting a return receipt.
- Usually, a **reliable service** is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived.

- The acknowledgement process introduces overhead and delays, which are often worth it but are sometimes undesirable
- A typical situation in which a reliable connection- oriented service is appropriate is file transfer.
- The transit **delays** introduced **by acknowledgements are unacceptable** in some situations.
  - For example the digitized voice traffic over **VoIP**, or the audio video sync. In video conferencing etc.
- In other situations, the convenience of **not having to establish a connection** to send one message is desired, but **reliability is essential**. The **acknowledged datagram** service can be provided for these applications.

Message/ Byte streams

- **Reliable connection-oriented** service has two minor variations: **message sequences** and **byte streams**
- Message sequences have **message boundaries**. For eg When two 1024-byte messages are sent, they arrive as two distinct 1024- byte messages, never as one 2048-byte message.
- Where as if connection is **byte streams** than When 2048 bytes arrive at the receiver, there is no way to tell if they were sent as one 2048-byte message, two 1024-byte messages, or one 2048 byte messages.
- **Example:** If the pages of a book are sent over a network to a phototypesetter as separate messages, it might be important to preserve the message boundaries. On the other hand, to download a DVD movie, a byte stream from the server to the user's computer is all that is needed.

Why unreliable communication is required ?

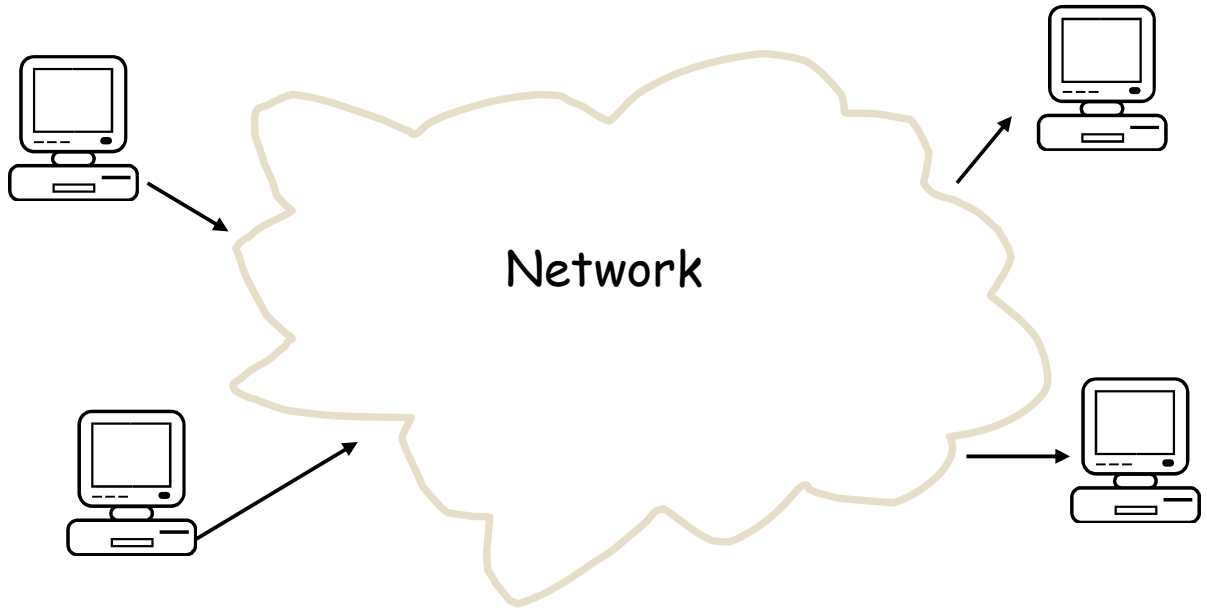
When having having a reliable communication, even unreliable communication is preferred due to the following reasons:

- **First** of all, reliable communication (in our sense, that is, acknowledged) may not be available in a given layer.
  - For example, Ethernet does not provide reliable communication. Packets can occasionally be damaged in transit. It is up to higher protocol levels to recover from this problem.
- **Second**, the delays inherent in providing a reliable service may be unacceptable, especially in real-time applications such as multimedia.
- For these reasons, both reliable and unreliable communication **coexist**.

END oF CHAPTER

Definition

- A network can be defined as two or more computers connected together in such a way that they can share resources.



- The purpose of a network is to share resources.

Cont.…

A resource may be:

- A file
- A folder
- A printer
- A disk drive
- Or just about anything else that exists on a computer.

Advantages of networking

- Connectivity and Communication
- Data Sharing
- Hardware Sharing
- Internet Access
- Data Security and Management
- High reliability
- Performance Enhancement and Balancing
- Entertainment

The Disadvantages (Costs) of Networking

- Network Hardware, Software and Setup Costs
- Hardware and Software Management and Administration Costs
- Undesirable Sharing
- Illegal or Undesirable Behavior
- Data Security Concerns

CONTENTS

- Definition
- Uses
- Classification of Networks
- Network Topology
- Network Topography

Data Communication

The exchange of data between two devices via some form of transmission medium such as a wire cable.

Characteristics of Effective Communication

- Delivery- Reaching Correct Destination.
- Accuracy- Delivering accurate data.
- Timeliness- Deliver data in timely manner.
  - Delivering data in the order they are produced.
- Jitter- Variation in packet arrival time.

What is Computer Networks?

- Computer network is a communication network in which a collection of computers are connected together to facilitate data exchange
- The connection between the computers can be wired or wireless.
- A computer network basically comprises **of 5 components**:
  - Sender
  - Receiver
  - Message
  - Transmission medium
  - Protocols

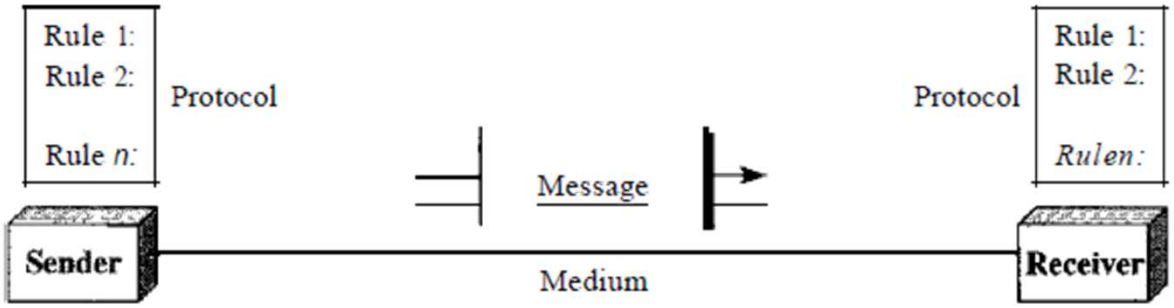


Fig 1: Components of data communication

USES OF COMPUTER NETWORKS

- In general Resource Sharing.
  - Sharing Computerized information between computers.
  - Network for people communication, rather between Computers.
  - Doing business electronically

Client Server model

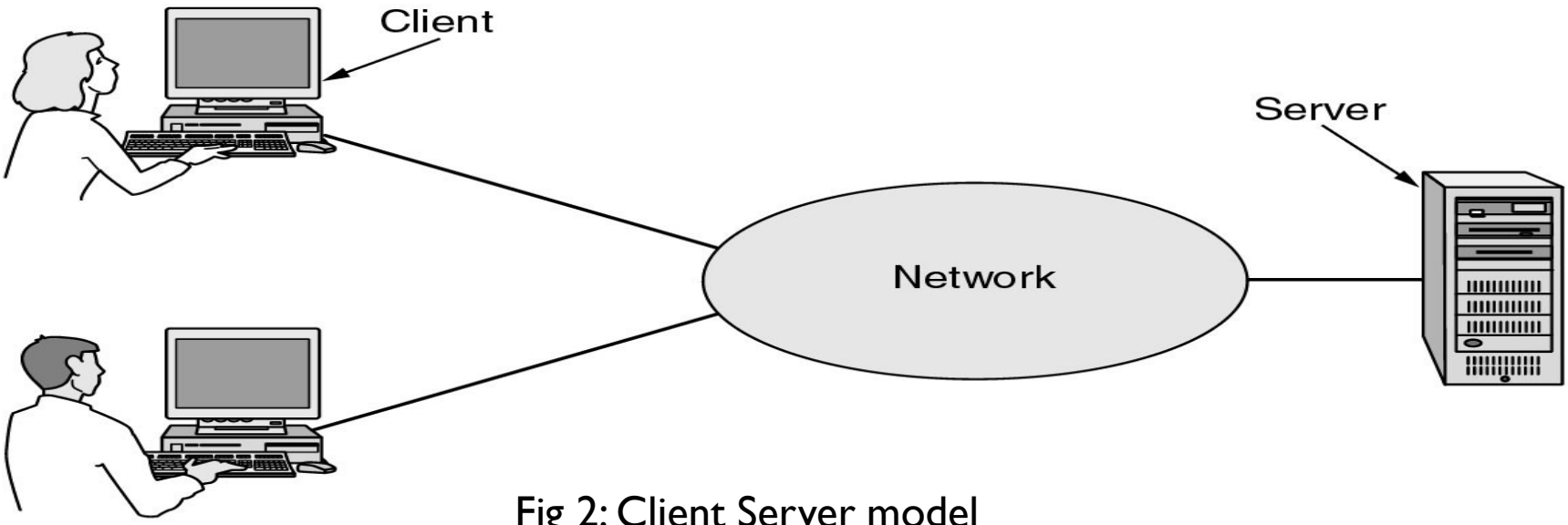


Fig 2: Client Server model

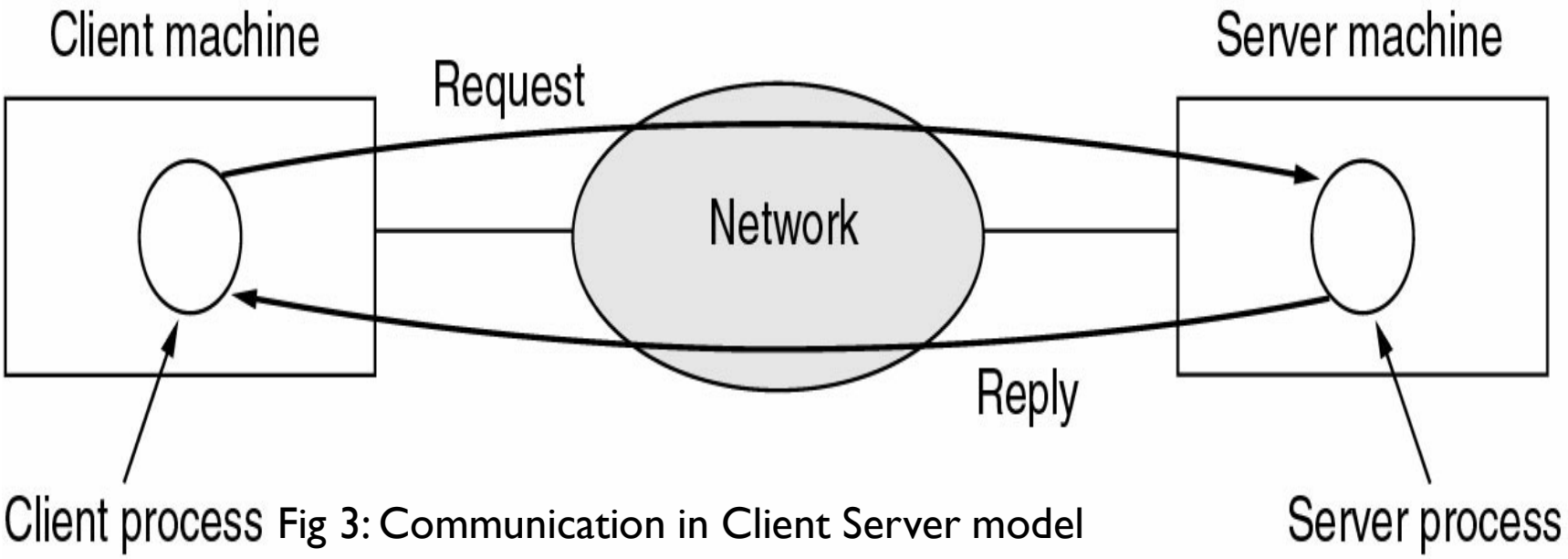


Fig 3: Communication in Client Server model

- Node: The devices in the network
- Link: The connection between the nodes

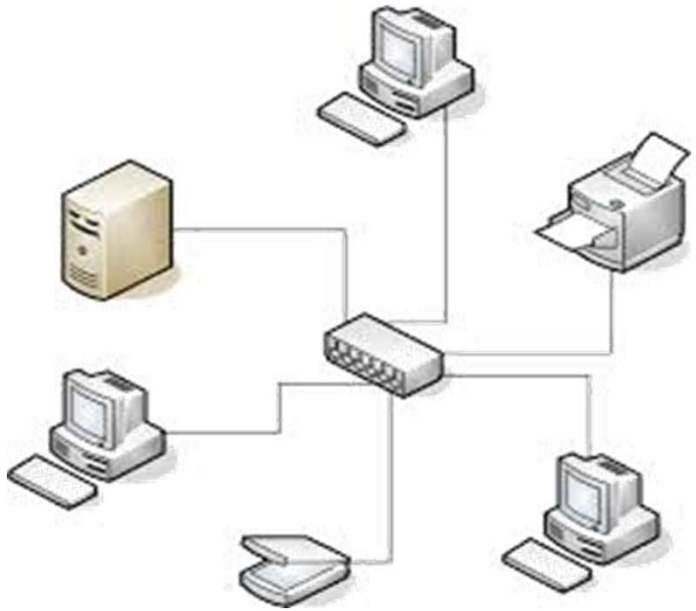


Fig 5: Nodes and Links

Type of Connection

- A **link** is a communications pathway that transfers data from one device to another.
- For communication to occur, two devices must be connected in some way to the same link at the same time.
- There are two possible **types of connections**: point-to-point and multipoint.
- **Point-to-Point** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.
- **Multipoint :** A multipoint connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared.

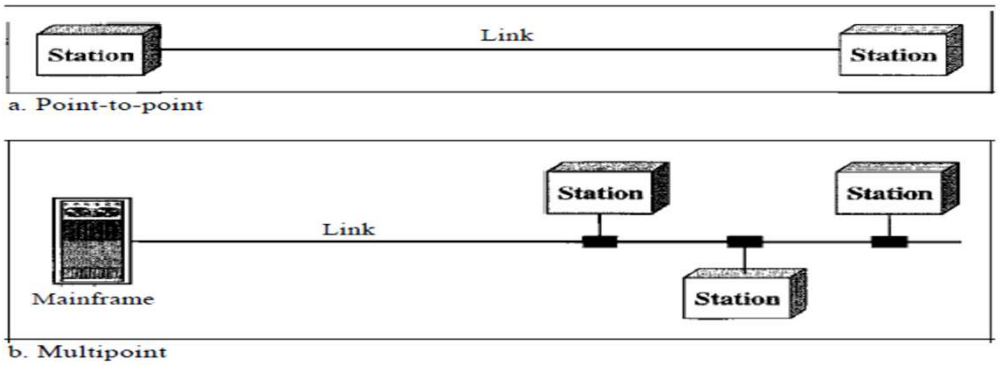


Fig 6: Point to Point and broadcast Connection

Network Topology

- The term *topology* refers to the way in which a network is laid out physically.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are four basic topology

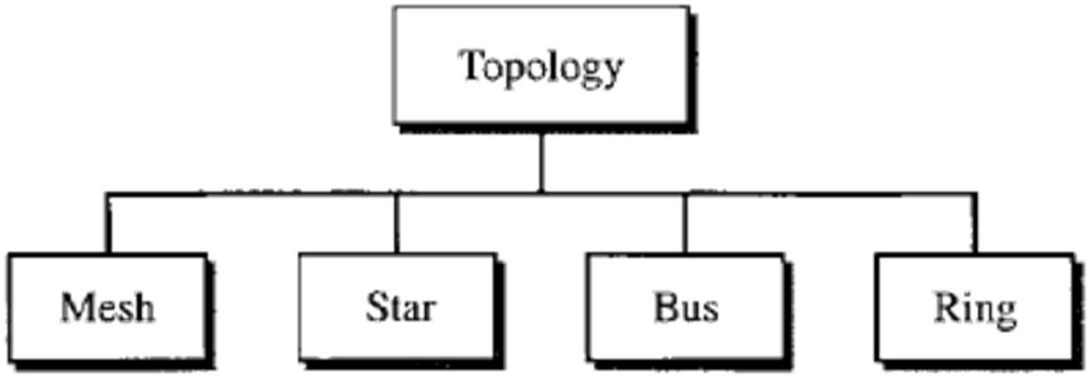


Fig 7: Different Topologies

Mesh Topology

- Every node has a dedicated point-to-point link with every other node
- The total number of links in a mesh topology with 'n' nodes is n(n-1).
- However, if each physical link allows communication in duplex mode, we can divide the number of links divide by 2. In other words, we can say that in a mesh topology, we need n(n-1)/2 duplex mode links.

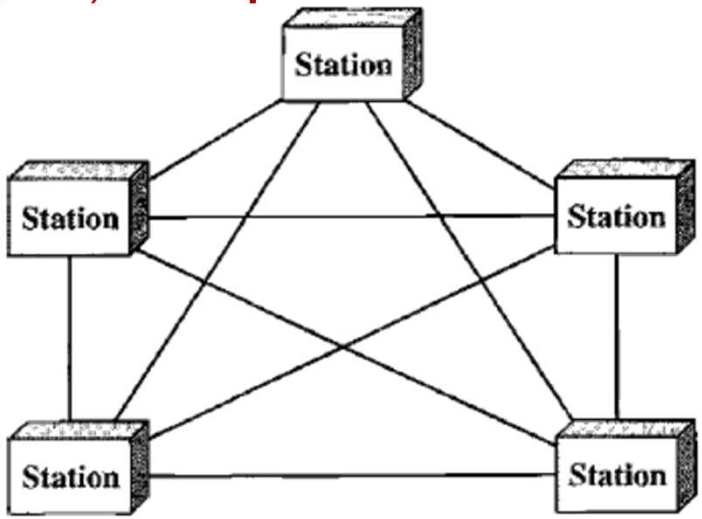


Fig 8: Mesh Topology

Problem 1

- If an organization has 6 nodes, and wants to link the nodes using topology.
- Find the total number of links required for the construction of the entire network for simplex and duplex communication, and the number of ports required by each node

Solution:

Given number of nodes in the organization ‘n’ = 6

As each node is connected to the remaining five (n-1) nodes in simplex mode of communication, thus the total number of links required is n(n-1) = 6 * 5 = 30.

In case of duplex mode the total number of links required is

n(n-1)/2 = 6 * 5 = 30/2 = 15.

Since each node has to connect to the remaining n-1 nodes thus the number of ports required for each node is 6-1 = 5.

Advantages

- First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
- Finally, point-to-point links make fault identification and fault isolation easy.

Disadvantages

- The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.
- First, because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
- For these reasons a mesh topology is usually implemented in a limited fashion.
- One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices.
- If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

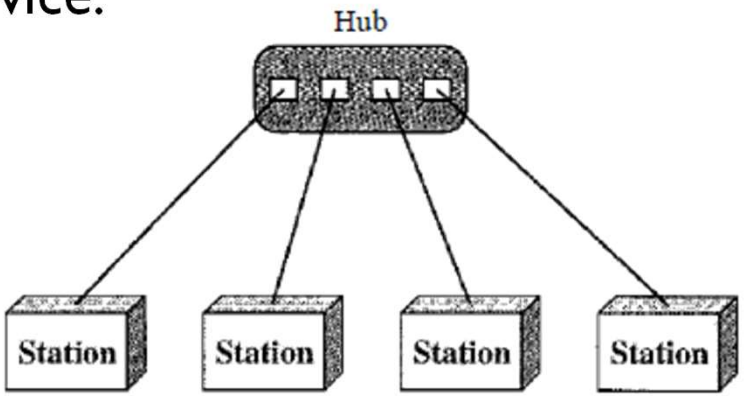


Fig 9: Star Topology

Advantages

- A star topology is less expensive than a mesh topology.
- In a star, each device needs only one link and one I/O port to connect it to any number of others.
- Easy to install and reconfigure.
- If one link fails, only that link is affected. Hence the topology supports robustness.
- Provides easy fault identification and fault isolation

Disadvantages

- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).
- Single point of failure.

- The star topology is used in LANs & High Speed LAN use star topology.

Problem 2

- If an organization has 6 nodes, and wants to link the nodes using star topology. Find the total number of links required for the construction of the entire network for simplex and duplex communication, and the number of ports required by each node

Solution:

Given number of nodes in the organization 'n' = 6

As each node is connected only to the hub, whether it is simplex or duplex the total number of links will be equal to the number of nodes = **6**

Since each node has to connect only to the hub thus the number of ports required for each node is **1**.

Bus Topology

- Bus topology is a multipoint link where one long cable acts as a backbone to link all the devices in the network.
- Eg : Ethernet LAN

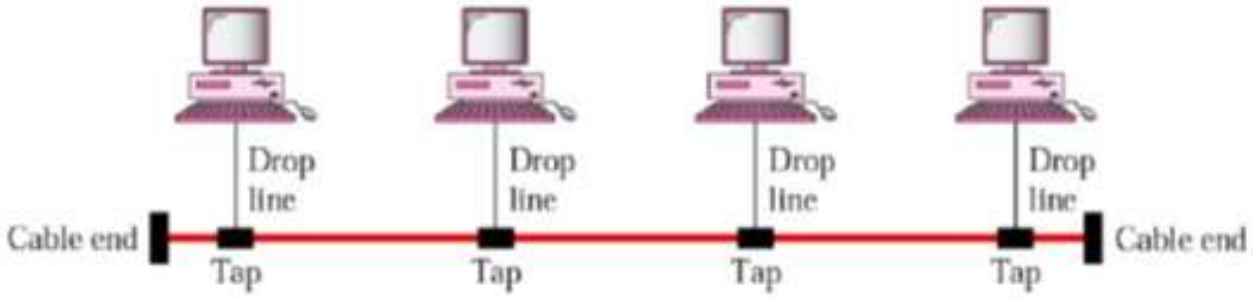


Fig 10: Bus Topology

Advantages

- Advantages of a bus topology include ease of installation.
- Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
- In this way, a bus uses less cabling than mesh or star topologies.

Disadvantages

- Adding new devices may therefore require modification or replacement of the backbone.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side.

Ring Topology

- In a Ring topology, each device has a **dedicated point-to-point connection** with only 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**. When a device receives a signal intended for another device, its repeater **regenerates the bits** and passes them along.

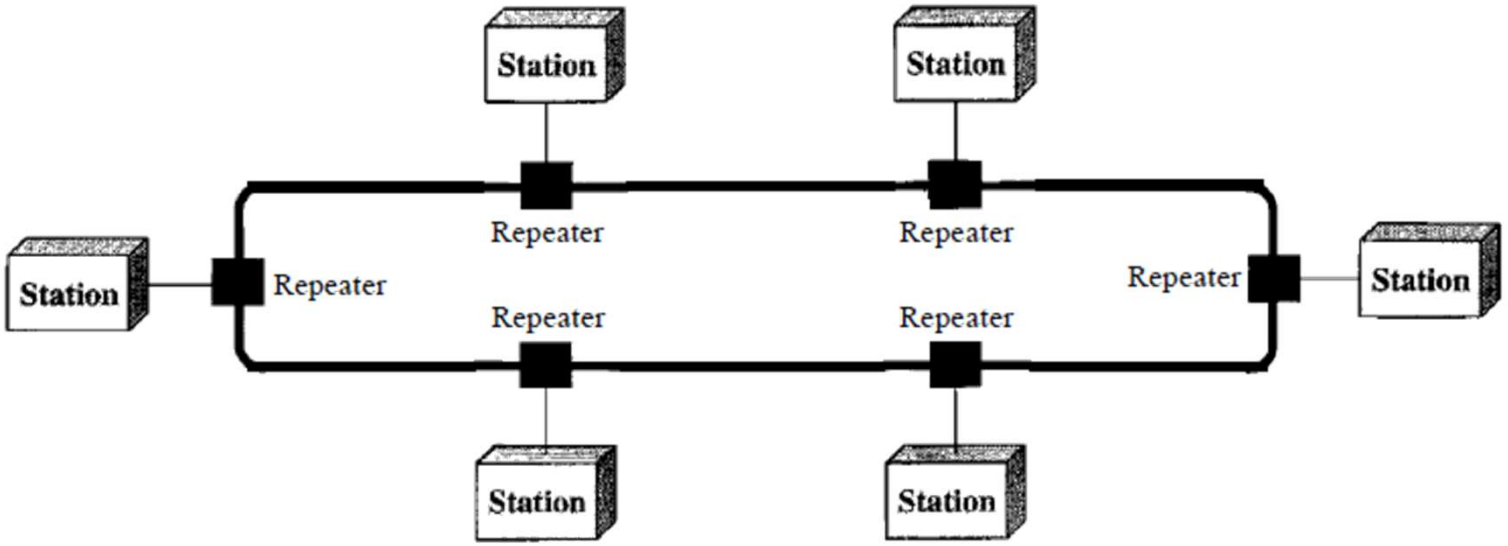


Fig 11: Ring topology

Advantages and Disadvantages

- This topology is relatively easy to install and reconfigure as each device is linked to only its immediate neighbors (either physically or logically).
- To add or delete a device requires changing only two connections.
- Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location. Thus **fault isolation** is simplified.
- However, **unidirectional traffic** can be a disadvantage.
- In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.
- This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Hybrid Topology

- A combination of any of the above technologies

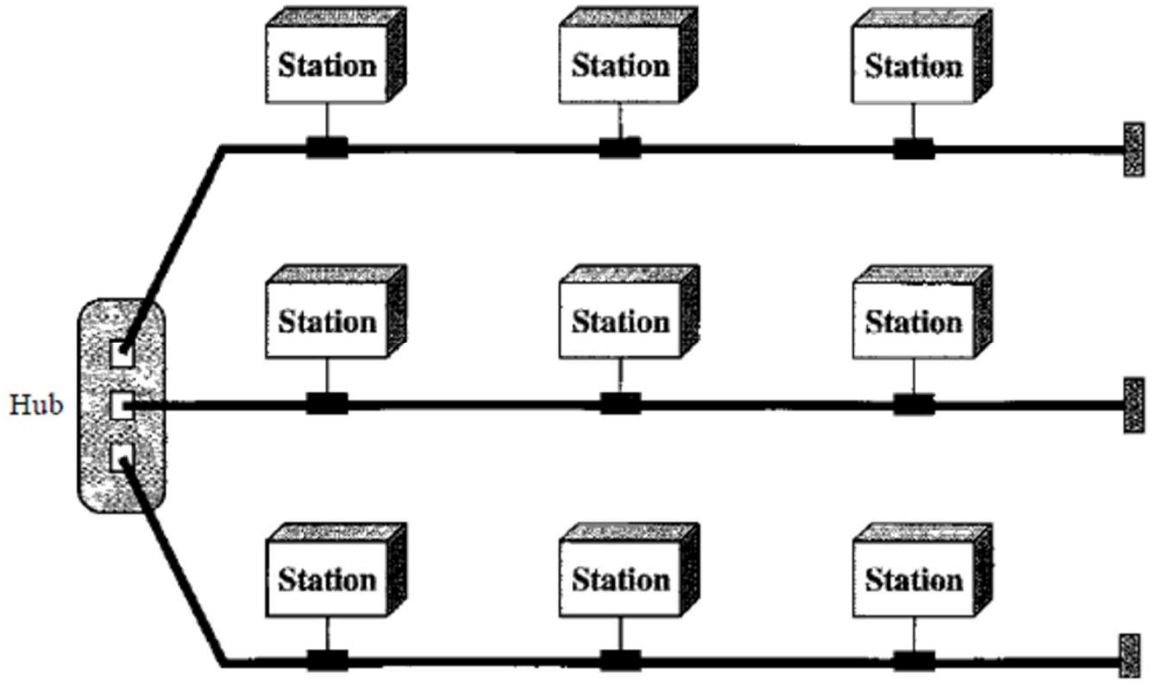


Fig 12: A hybrid topology: a star backbone with three bus networks

Hybrid Topology

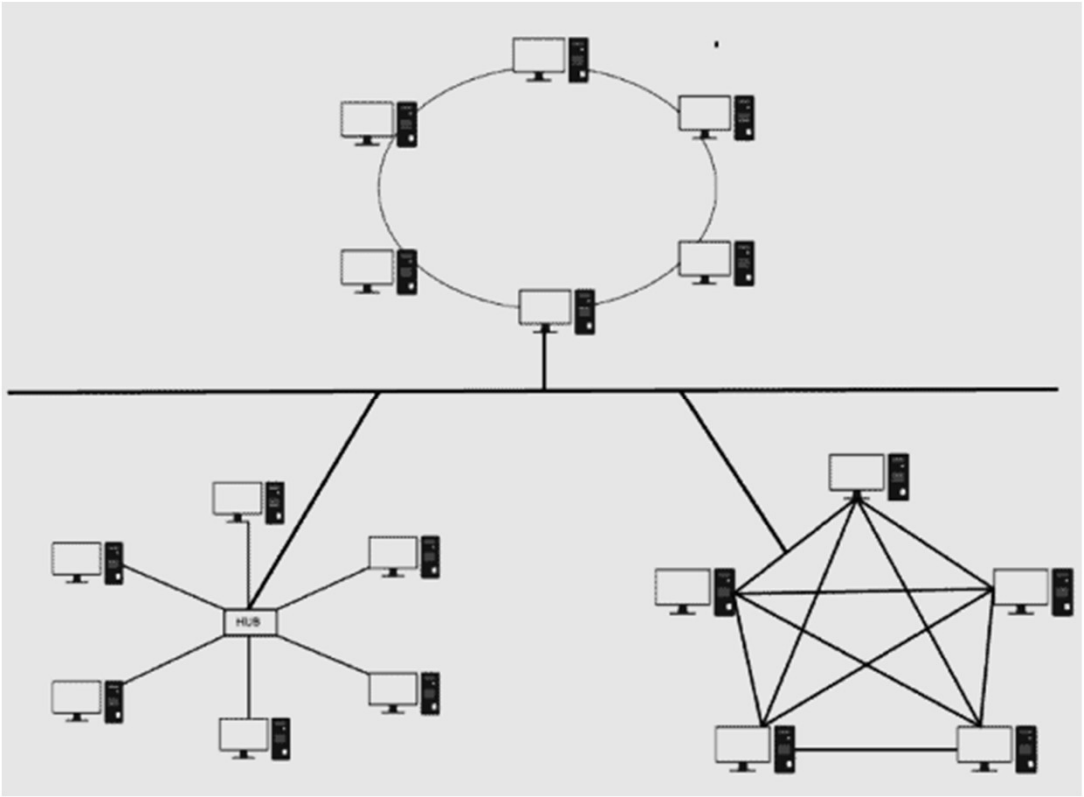


Fig 12: B hybrid topology: a mixture of bus, mesh, ring, star- topology

Tree Topology (a kind of hybrid topology)

- A tree topology connects multiple star networks to a linear bus backbone cable

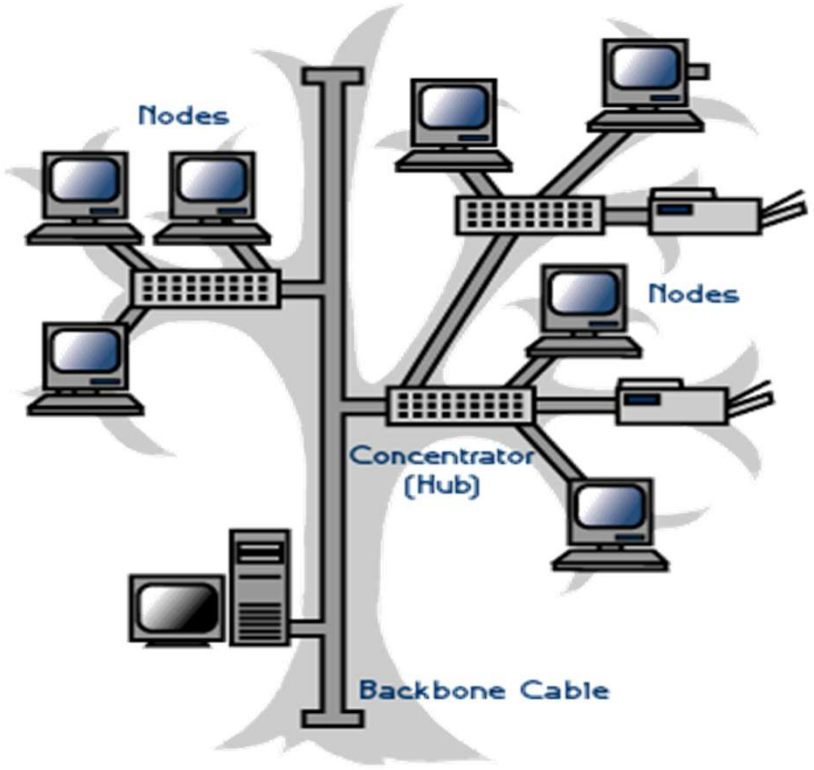


Fig 13: Tree Topology

Topography

- Topography – is the way in which the cables, which provide channels between stations, are positioned.
- For the purposes of cable planning, Topography is more important than Topology.

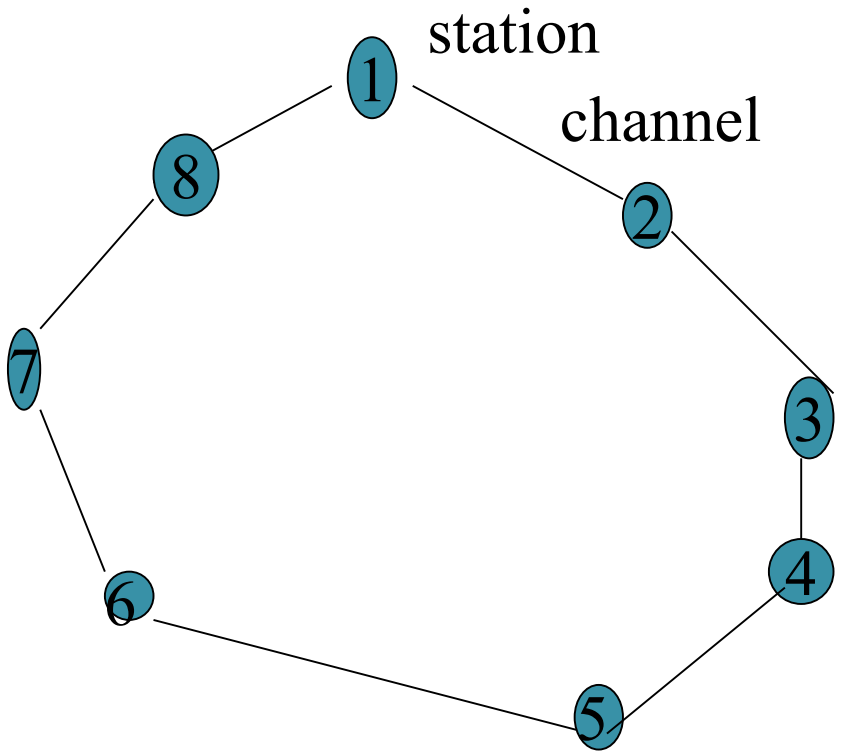


Fig. A A Ring Topology

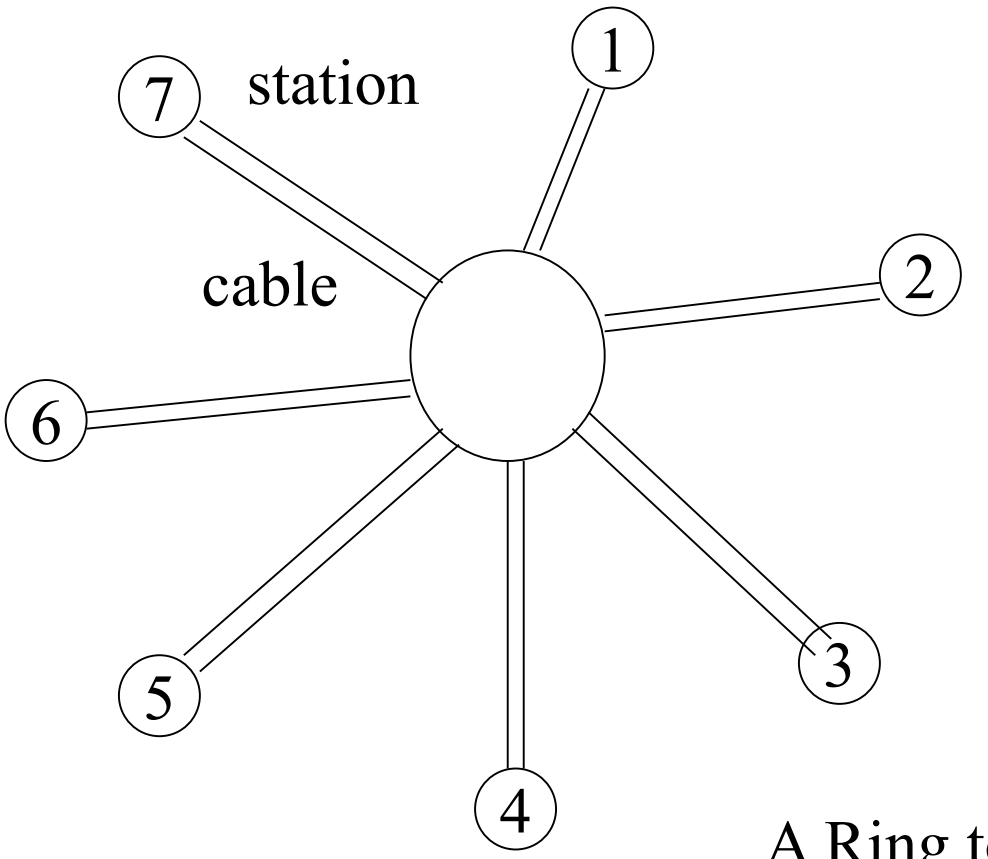
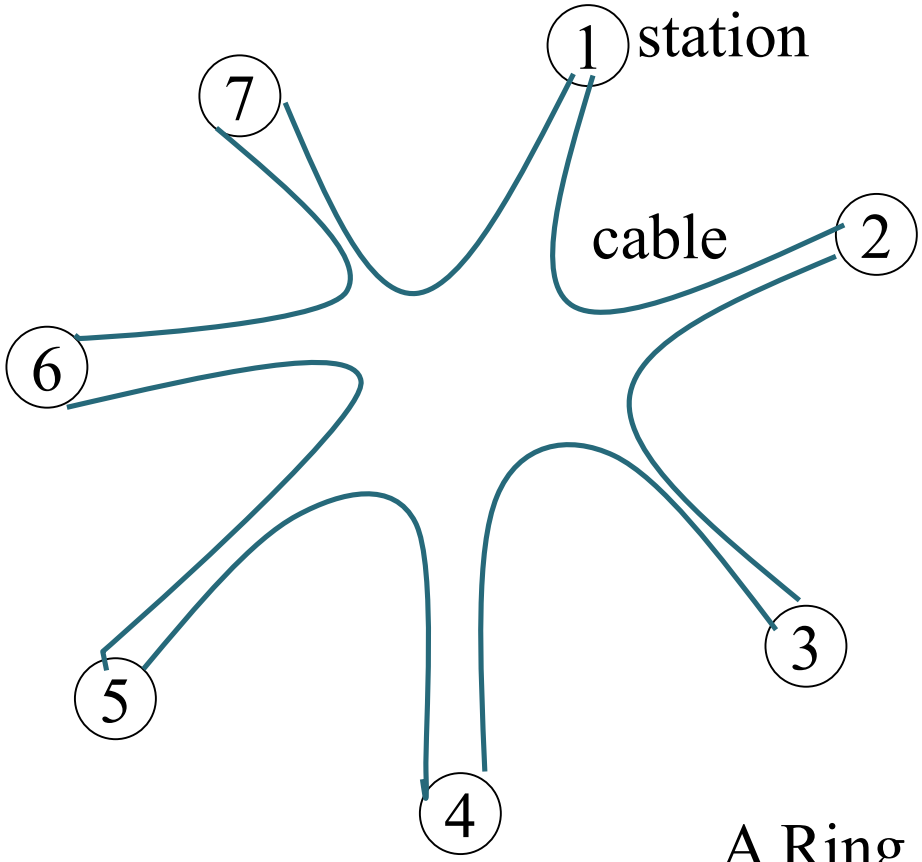


Fig. B

A Ring topology wired in a star Topography



A Ring topology wired in a star Topography

Classification of Networks

- The networks can be classified based on one of the two dimensions:
  - Transmission Technology
  - Scale

Classification of Networks based on Transmission Technology

- Networks can be classified as :
  - Point to point networks
  - Broadcast networks
  - Multicast networks
- Point-to-point networks connect individual pairs of machines. Point-to-point transmission with exactly one sender and exactly one receiver is called **unicasting**.
- Packets sent by any machine is received by all the others.
- An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field.
- If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

Classification of Networks based on Transmission Technology

- **Broadcast** systems usually also allow the possibility of addressing a packet to *all* destinations by using a **special code** in the address field.
- When a packet with this special code is transmitted, it is received and processed by every machine on the network.
- This mode of operation is called **broadcasting**.
- Some broadcast systems also support transmission to a **subset of the machines**, which known as **multicasting**

Classification of Networks Based on Scale

- Distance is considered as an important classification metric

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Classification of networks based on the area of coverage

Personal Area Networks (PAN)

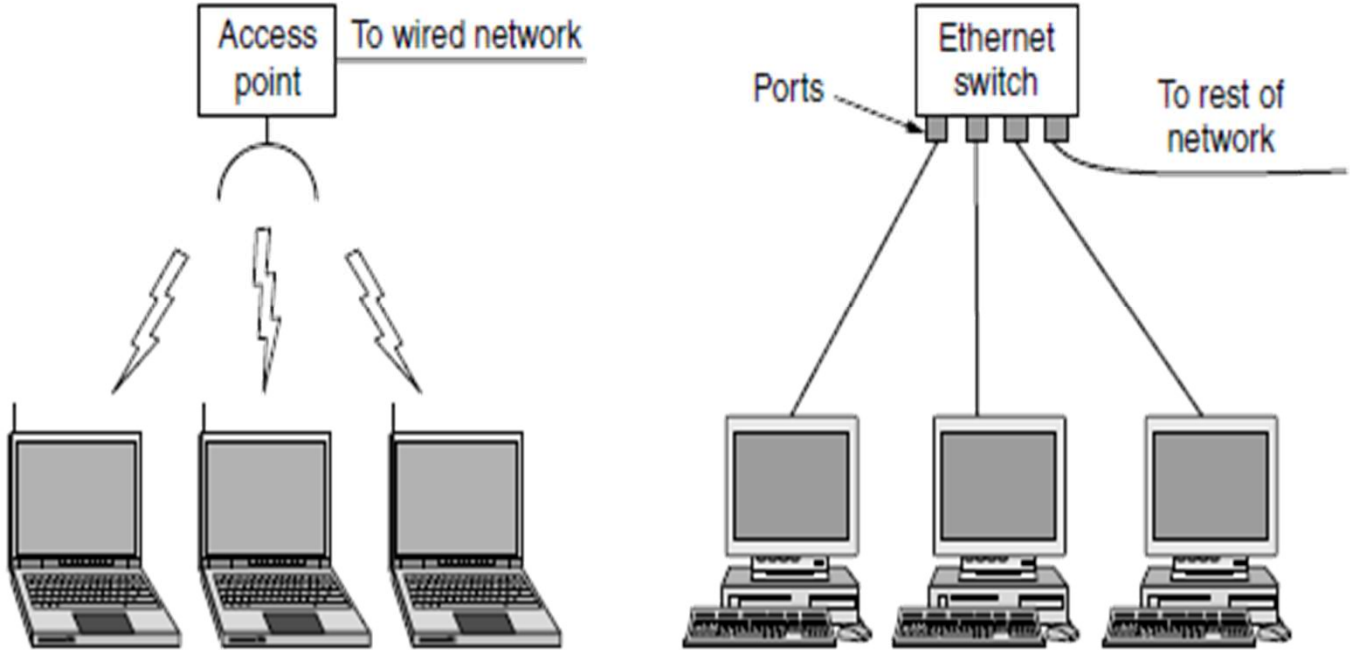
- **PANs** (**Personal Area Networks**) let devices communicate over the range of a person.
- A common example is a wireless network that connects a computer with its peripherals using Bluetooth.
- It is often used to connect a headset to a mobile phone without cords and it can allow your digital music player.
- PANs can also be built with other technologies that communicate over short ranges.

Local Area Networks (LANs)

- A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.
- LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.
- When LANs are used by companies, they are called **enterprise networks**.

Wired and Wireless LANs

- This device, called an **AP** (**Access Point**), **wireless router**, or **base station**, relays packets between the wireless computers and also between them and the Internet.

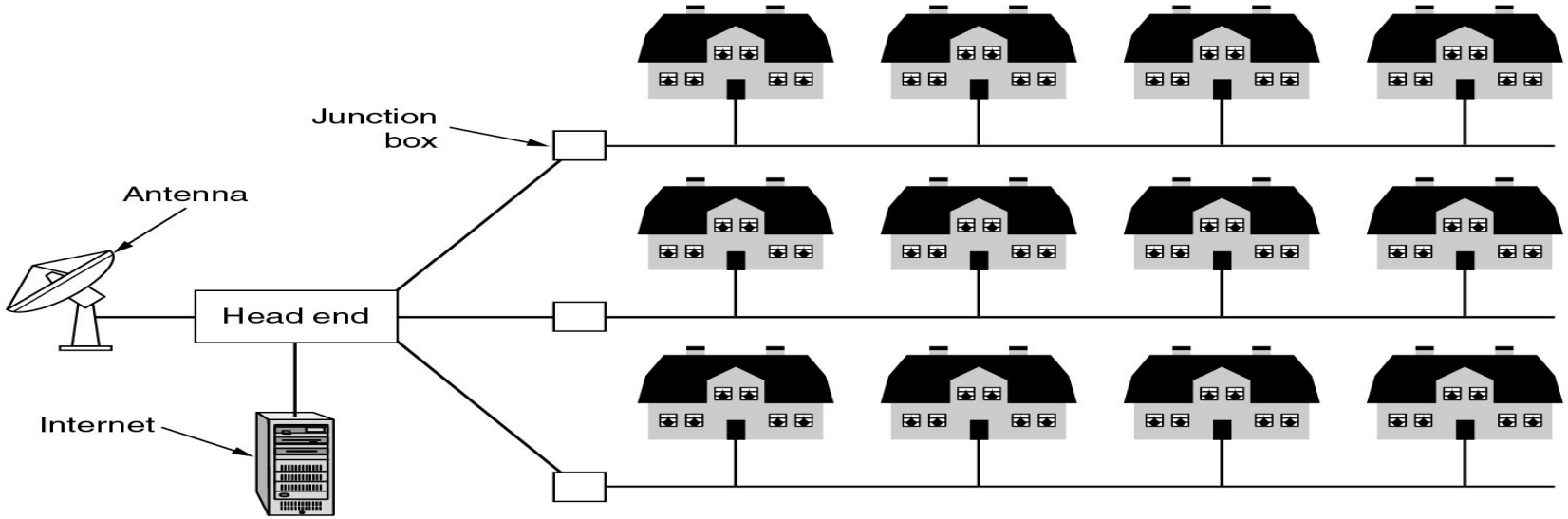


In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers via a device called as access point or wireless router.

- The standard for wireless LANs is called **IEEE 802.11**, popularly known as **WiFi**, which has become very widespread.
- It runs at speeds anywhere from 10Mbps to 100 Gbps
- Wired LANs use a range of different transmission technologies. Most of them use copper wires, but some use optical fiber
- The topology of many **wired LANs** is built from point-to-point links. **IEEE 802.3**, popularly called **Ethernet.**
- Each computer speaks the Ethernet protocol and connects to a box called a **switch** with a point-to-point link.
- A switch has multiple **ports**, each of which can connect to one computer. The switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.

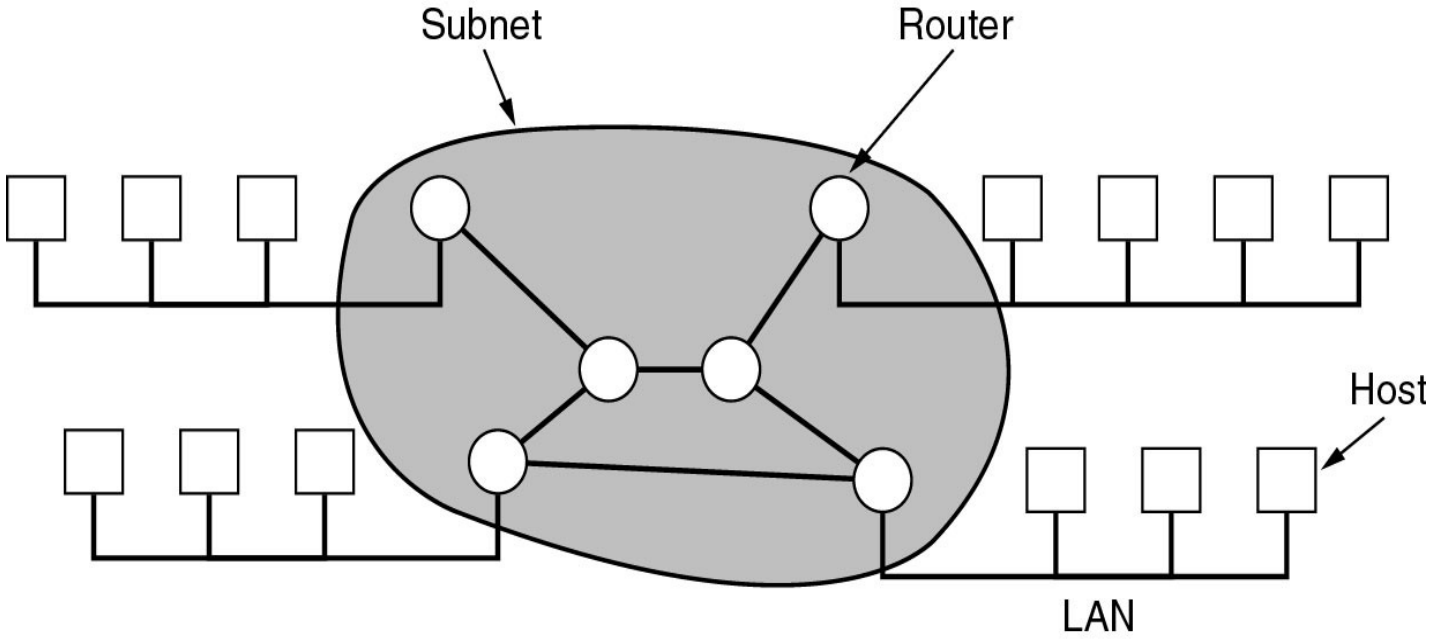
Metropolitan Area Networks (MANs)

- MANs generally cover a city.
- The best-known examples of MANs are the cable television networks available in many cities.
- These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception.
- Cables were being laid to facilitate this approach.
- When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide Internet service in unused parts of the spectrum.



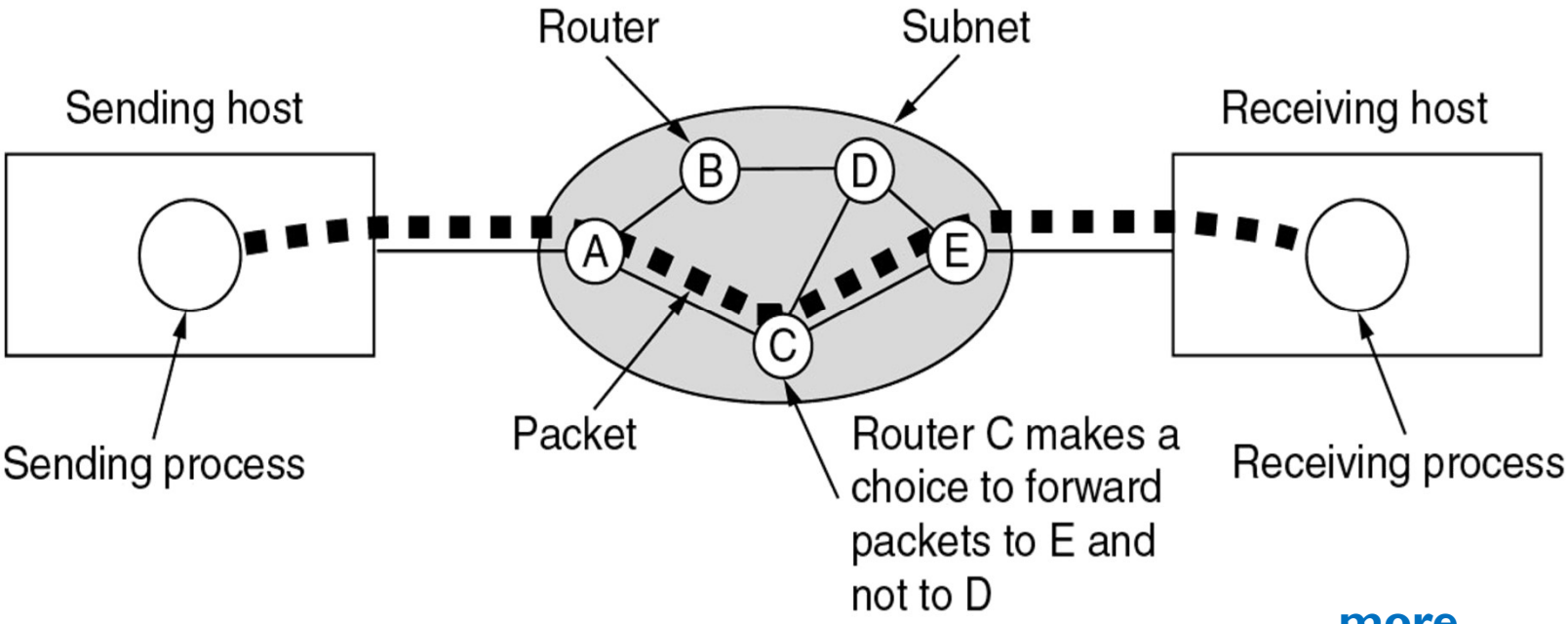
Wide Area Networks (WANs)

- A **WAN** (**Wide Area Network**) spans a large geographical area, often a country or continent.
- It contains a collection of machines called as hosts intended for running application programs.
- These hosts are connected by a communication **subnet**.
- The subnet consists of two components the transmission lines and switching elements (routers).



The **Internet** is the **largest WAN**, spanning the Earth.
WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

- When two routers that are not connected directly need to communicate, then the routers communicate through the intermediate routers.
- Each of the intermediate routers stores the entire data and forwards it once the line is free. This mechanism is called as **Store and Forward** or **Packet Switched**



more

Home Networks

- In these networks the fundamental idea is that every device in home is capable of communicating with every other device, and all of them are accessible over internet.
- Some of the devices that are capable of being networked are:
  - Computers (desktop PC, PDA, shared peripherals
  - Entertainment (TV, DVD, VCR, camera, stereo, MP3)
  - Telecomm (telephone, cell phone, intercom, fax)
  - Appliances (microwave, fridge, clock, furnace, air-conditioner)
  - Telemetry (utility meter, burglar alarm, babycam).

Internetworks

- Many networks exist in the world, often with different hardware and software.
- People connected to one network often want to communicate with people attached to a different one.
- The fulfillment of this desire requires that different, and frequently incompatible, networks be connected.
- A collection of interconnected networks is called an **internetwork or internet**.
- Example connecting a LAN and a WAN or connecting two LANs is the usual way to form an internetwork.
- The general name for a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is a **gateway**.

Difference between subnet, network and internetworks

- The term 'subnet' makes the most sense *in the context of a* WANs where it refers to the collection of routers and communication lines owned by the network operator.
- Network is formed by the combination of a subnet and its hosts.
- Internetwork is formed when distinct networks are interconnected

END

- The TCP/IP model doesn't require strict layering.
- The application layer has the option of by-passing the intermediate layers.

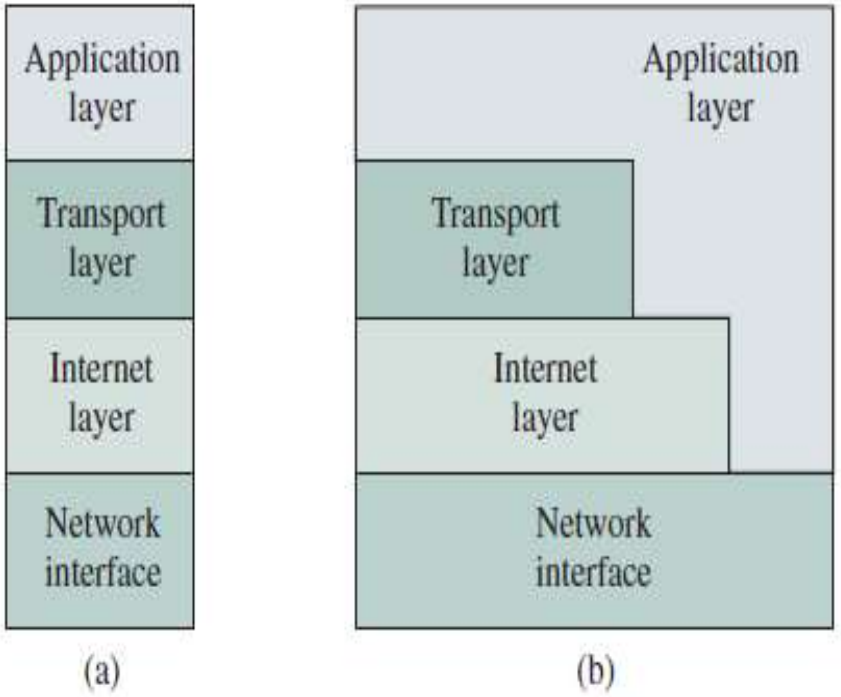


FIGURE 2.10 TCP/IP network architecture

Application Layer

- The application Layer provides services that can be used by other applications.
- Ex: Different protocols have remote login, email, file transfer. Network management etc.

Application Layer Protocols

- TELNET: "Terminal NETwork": enables the establishment of connection to a remote system.
  - Telnet uses TCP connection
  - Telnet connects to servers through the port numbers and users can interact using the command line.
- SMTP: "Simple Mail Transfer Protocol": used for facilitating delivery of e-mail message.
- FTP: " File Transfer Protocol": used for copying a file from one host to another.
  - It requires two TCP connection.
  - Control Connection and Data Connection.

Application Layer Protocols

- HTTP: "HyperText Transfer Protocol": specifies the rules by which the web client and web server interact so as to retrieve the documents.
  - Stateless Protocol : Does not maintain any information about the client.
- DNS: "Domain Name System": Carries out the query to determine the IP address for the corresponding host name

Transport Layer

- The application layer protocols are intended to run directly over the transport layer.
- They are two types of services provided:
  - Transmission Control Protocol (TCP) : Connection Oriented
  - User Datagram Protocol (UDP): Connectionless

Network or Internet Layer

- This layer is responsible for transferring the information across multiple networks with the use of gateways and routers.
- It deals with the same functionalities as that of OSI.
- Routing of packets from router to router across networks.
- The connectionless service makes the system robust, if failures occur in the network, the packets are routed around the point of failure.

Network Interface Layer

- Ethernet, token ring are few of the interfaces used for connecting systems end to end.
- As the packet obtained from network layer is encapsulated into frames, this provides a clear separation of the internet layer from the technology dependent network interface layer.

TCP/IP Protocol Graph

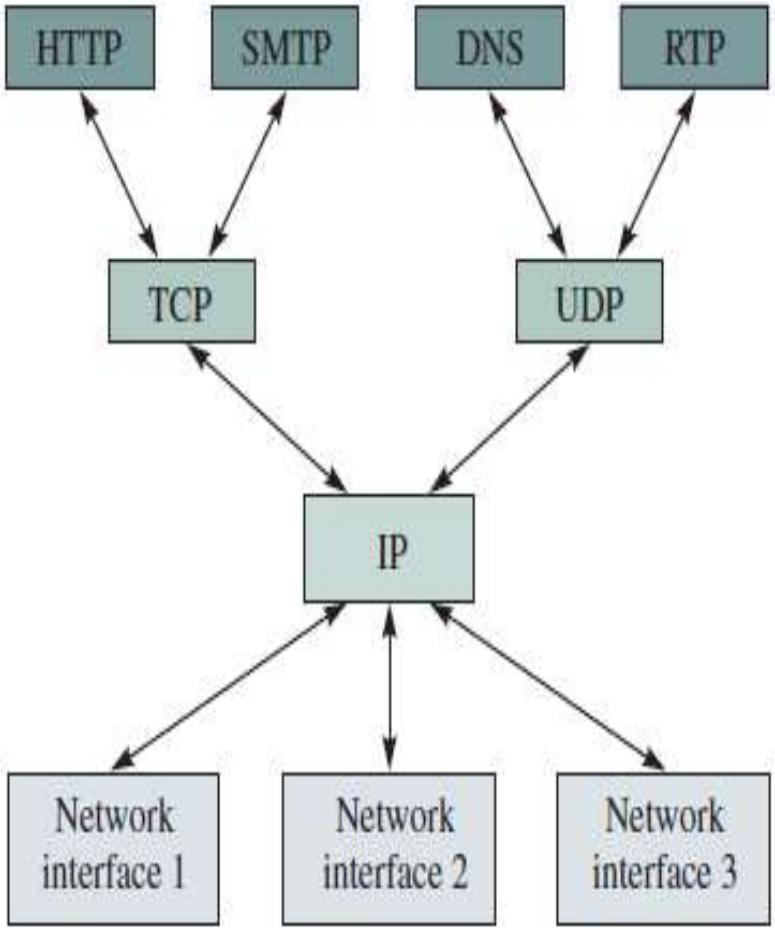


FIGURE 2.12 TCP/IP protocol graph

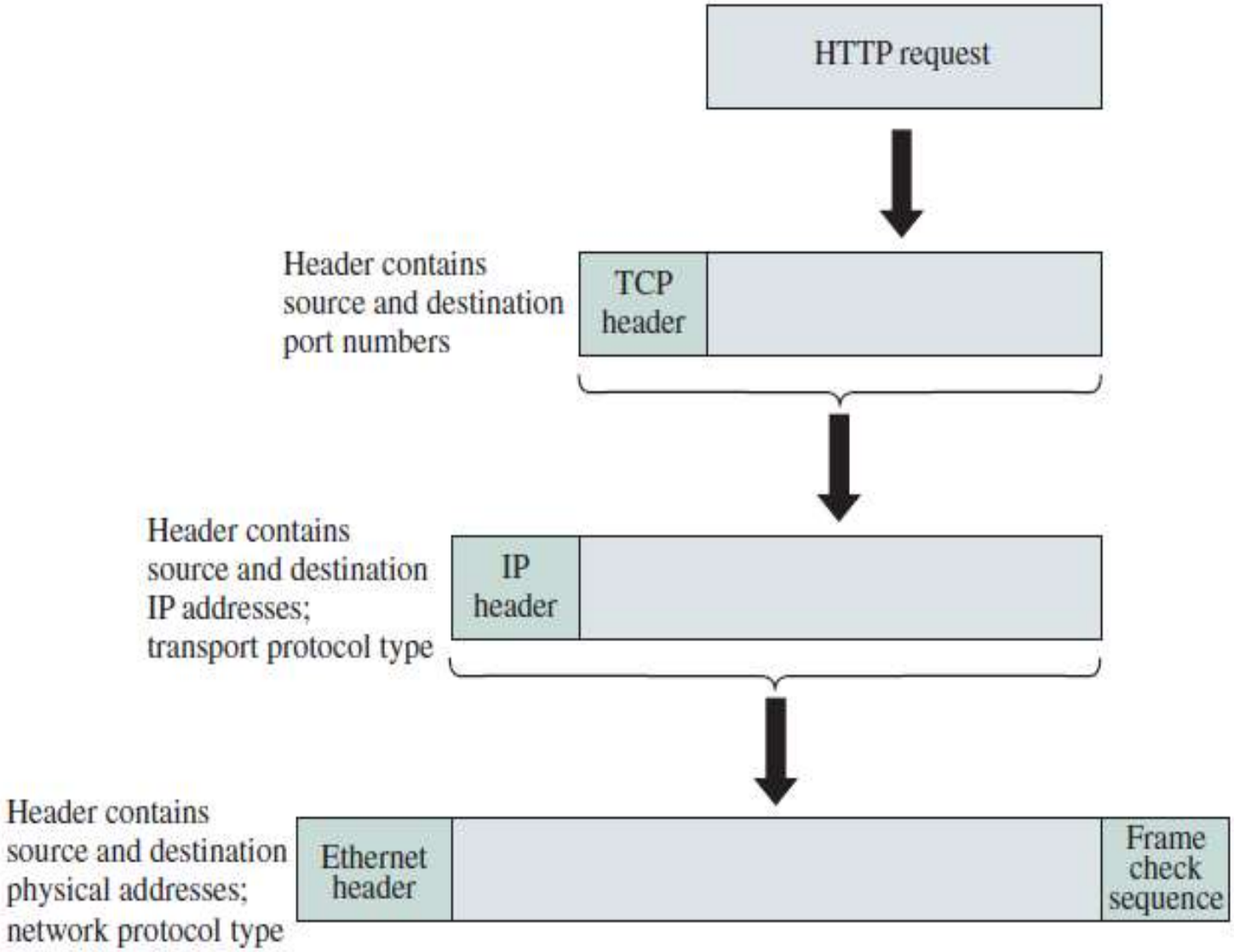


FIGURE 2.15 Encapsulation of PDUs in TCP/IP and addressing information in the headers

IP Utilities

- **PING** : It is used to determine whether a host is online and available.
  - Uses ICMP
  - Often used to measure the round-trip delay between two hosts.
- **TRACEROUTE** : Determine the route that a packet takes from the local host to remote host
  - Determine the latency and reachability from the source to each hop
  - Generally used as debugging tool
  - Uses ICMP and UDP
- **IPCONFIG** : Display the TCP/IP information about a host
  - IP address, subnet mask and default gateway for the host

NETSTAT: Queries a host about its TCP/IP network status

Problem

An internet path between two hosts involves a hop across network A, a packet-switching network, to a router and then another hop across packet-switching network B. Suppose that packet switching network A carries the packet between the first host and the router over a two-hop path involving one intermediate packet switch. Suppose the second network is an Ethernet LAN. Sketch the sequence of IP and non-IP packets and frames that are generated as an IP packet goes from host 1 to host 2.

Problem

- A 100-byte message is sent through a private internet using the TCP/IP protocol suite. If the protocol adds a 10-byte header at each layer, and a 10 byte trailer, what is the efficiency of the system?

Solution:

Efficiency of a system is defined as the **ratio of the number of useful bytes to the number of total bytes.**

Thus efficiency = actual size of message / total size (message + 3headers + 1 trailer)

Thus efficiency = 100/140 = 71.4%

Problem

Suppose an application layer entity wants to send an **L-byte** message to its peer process, using an existing TCP connection. The **TCP segment** consists of the **message plus 20 bytes of header**. The segment is **encapsulated into an IP packet** that has an **additional 20 bytes of header**. The IP packet in turn goes inside an **Ethernet frame** that has **18 bytes of header and trailer**. **What percentage of the transmitted bits in the physical layer correspond to message information**, if **L = 100** bytes, **500** bytes, **1000** bytes?

Solution

The message overhead includes:

- **TCP: 20 bytes** of header
- **IP: 20 bytes** of header
- **Ethernet: total 18 bytes** of header and trailer.

Total Header : 20+20+18=58 Bytes

Total Bytes sent: **L(message)+58**

Therefore

- L = 100 bytes, **100/158 = 63%** efficiency.
- L = 500 bytes, **500/558 = 90%** efficiency.
- L = 1000 bytes, **1000/1058 = 95%** efficiency.

Problem

- A user wishes to send a **message of size 1 MB** (MegaByte) to another user over a **point-to-point link**. The message is divided into **blocks of size 1000 bytes**. **Each** of the **5 layers add a header** of length **20 bytes each** to the block as it goes down the protocol stack. **What is the "user" throughput (as seen by the end-user) if the link capacity is 10 Mbps.** Ignore processing and propagation delays. Express the answer in Mbps.

soln

- **Packet size** is **1000 + 5 * 20 = 1100** bytes out of which **100 bytes is overhead**.
- Alternately **useful data** is only **1000 out of 1100**.
- So user throughput would be
- **1000/1100 * 10 Mbps = 9.09** Mbps.

Syllabus Covered

- Tannenbaum, A.S. – "COMPUTER NETWORKS", Prentice Hall of India [EE Edition], 4th edition, 2003. : chapter 1 – 1.3 (1.3.1, 1.3.2, 1.3.3)
- Behrouz A. Forouzan – "TCP/IP PROTOCOL SUITE", Tata McGraw Hill, Third Edition, 2010 : Chapter 2 – 2.2, 2.3, 2.4
- Alberto Leon – Garcia –"Communication Networks", Tata McGraw Hill, Second Edition, 2004. Chapter 2- 2.3
- Problems refer Chapter 2 of Alberto Leon- Garcia – "Communication Networks", Tata McGraw Hill, 2nd edition, 2004