INTRODUCTION

UNIT-1 (Part-A)

Contents:

- Definition
- Components
- Classification of Networks

Definition & Components

- A network is the interconnection of a set of devices capable of communication.
- Components:
  - Devices(End Devices, Connecting Devices)
  - Transmitter / Receiver
  - Media – Wired / Wireless
  - Data (Text/Multimedia/File..)
  - Rules/Protocols

Fundamental Characteristics

- **Delivery**:

  The system must deliver data to the correct destination.

- **Accuracy:**

  The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

- **Timeliness**:

  The system must deliver data in a timely manner without significant delay. Strict kind of delivery is called real-time transmission.

- **Jitter:**

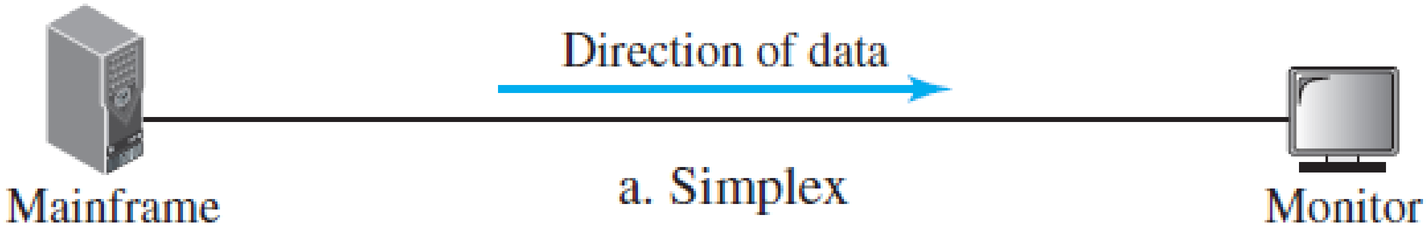
  Jitter refers to the variation in the packet arrival time.

Classification of Networks

- Data Flow
  - Simplex / Half Duplex / Full Duplex
- Size/Scale
  - PAN / LAN / MAN / WAN
- Type of connection
  - Point-to-point / Multipoint or Broadcast
- Physical Topology
  - Mesh / Star / Bus / Ring / Hybrid
- Network Media Connectivity
  - Wired / Wireless / Adhoc / Heterogeneous
- Service offered
  - Connection oriented / Connection less
- Data Forwarding mechanism (Switching)
  - Circuit / Message / Packet Switching

Classification based on Data Flow

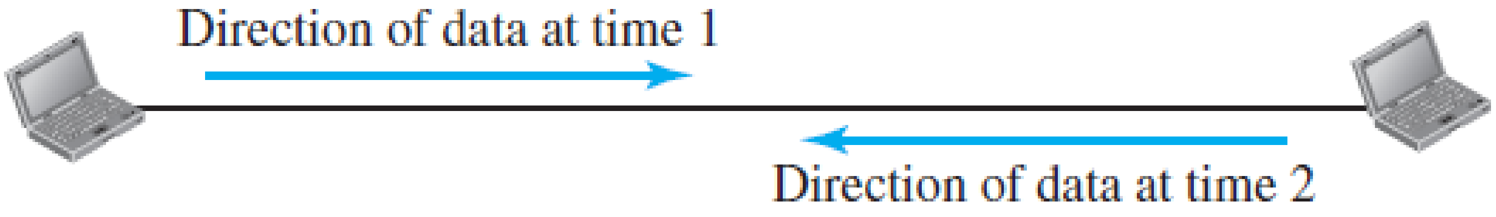
- Simplex:
  - the communication is unidirectional
  - Only one of the two devices on a link can transmit; the other can only receive
  - Ex: keyboard can only introduce input; the monitor can only accept output



a. Simplex

Classification based on Data Flow…

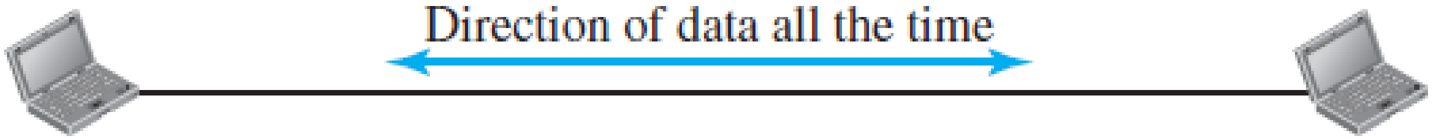
- Half Duplex:
  - each station can both transmit and receive, but not at the same time.
  - When one device is sending, the other can only receive, and vice versa.
  - Ex: Walkie-talkies and CB (citizens band) radios



b. Half-duplex

Classification based on Data Flow…

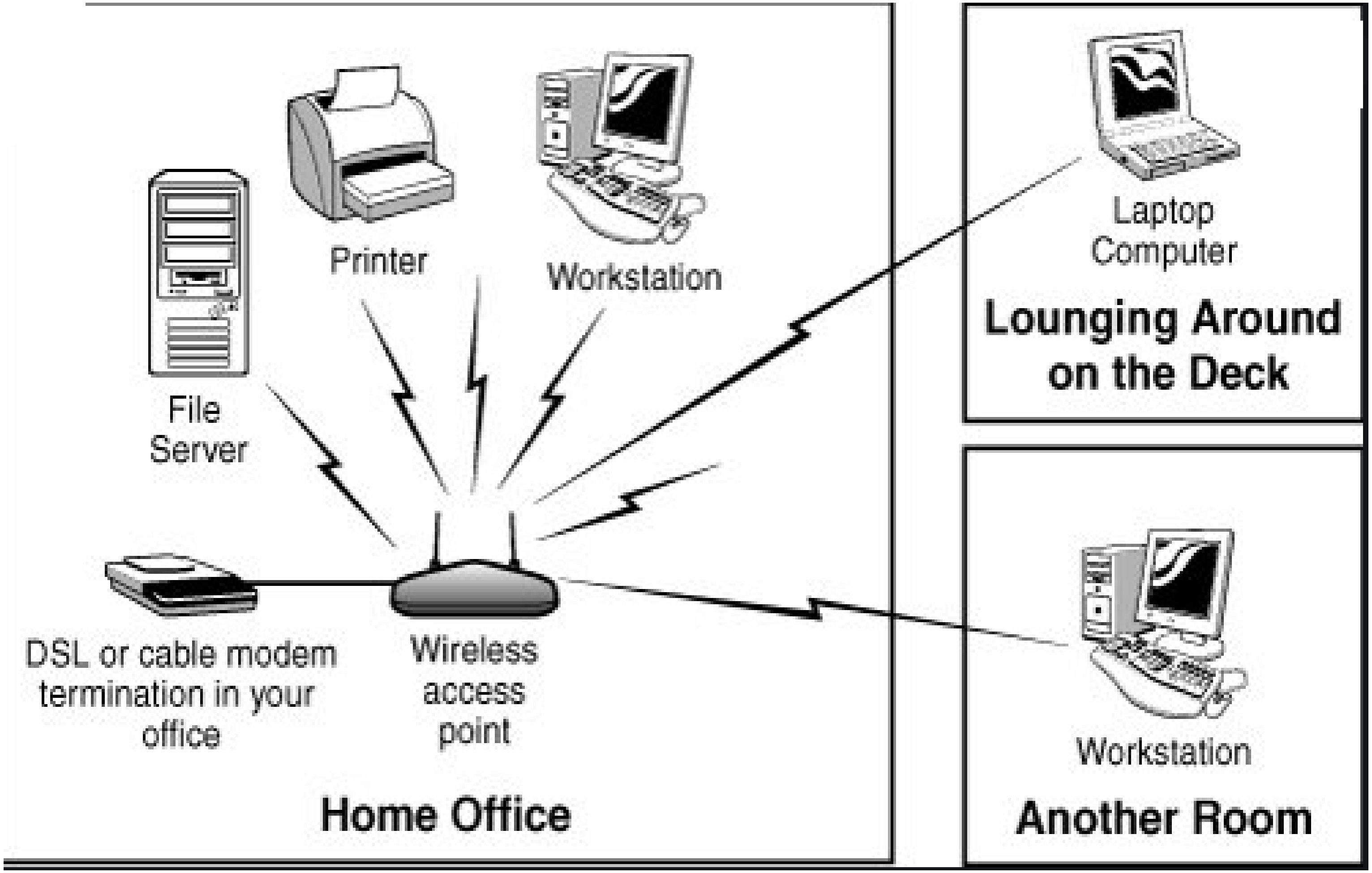
- Full Duplex:
  - both stations can transmit and receive simultaneously.
  - the link must contain two physically separate transmission paths, one for sending and the other for receiving (or) the capacity of the channel is divided between signals traveling in both directions (or) using software mechanism.
  - Ex: Telephone network



c. Full-duplex

Classification based on Size/Scale

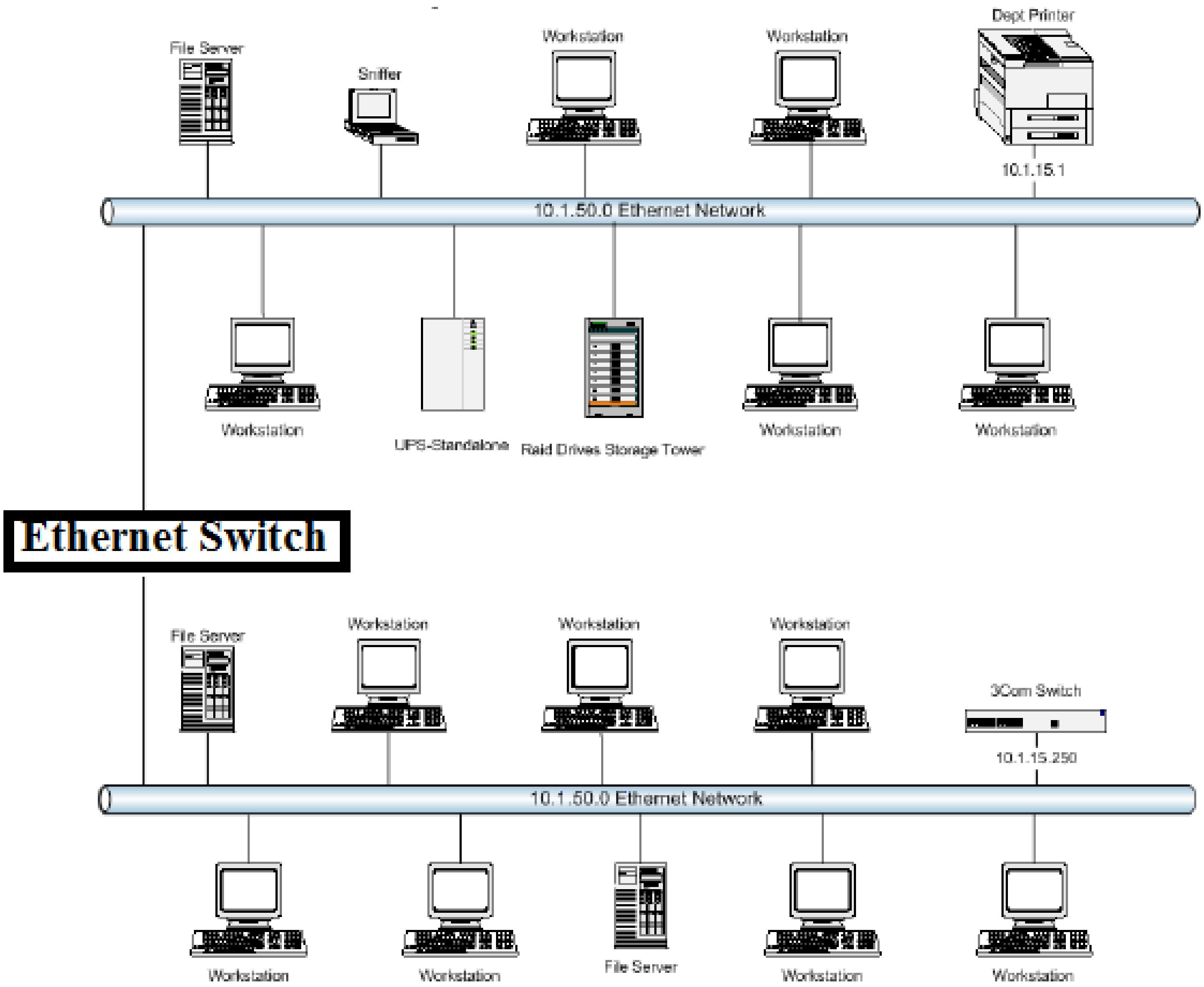
- Personalized Area Network (PAN)
  - The interconnection of devices within the range of an individual person, typically within a small office (SOHO) or residence.
  - Ex: a wireless network connecting a computer with its keyboard, mouse, mobile or printer



Small Office Home Office(SOHO) Network

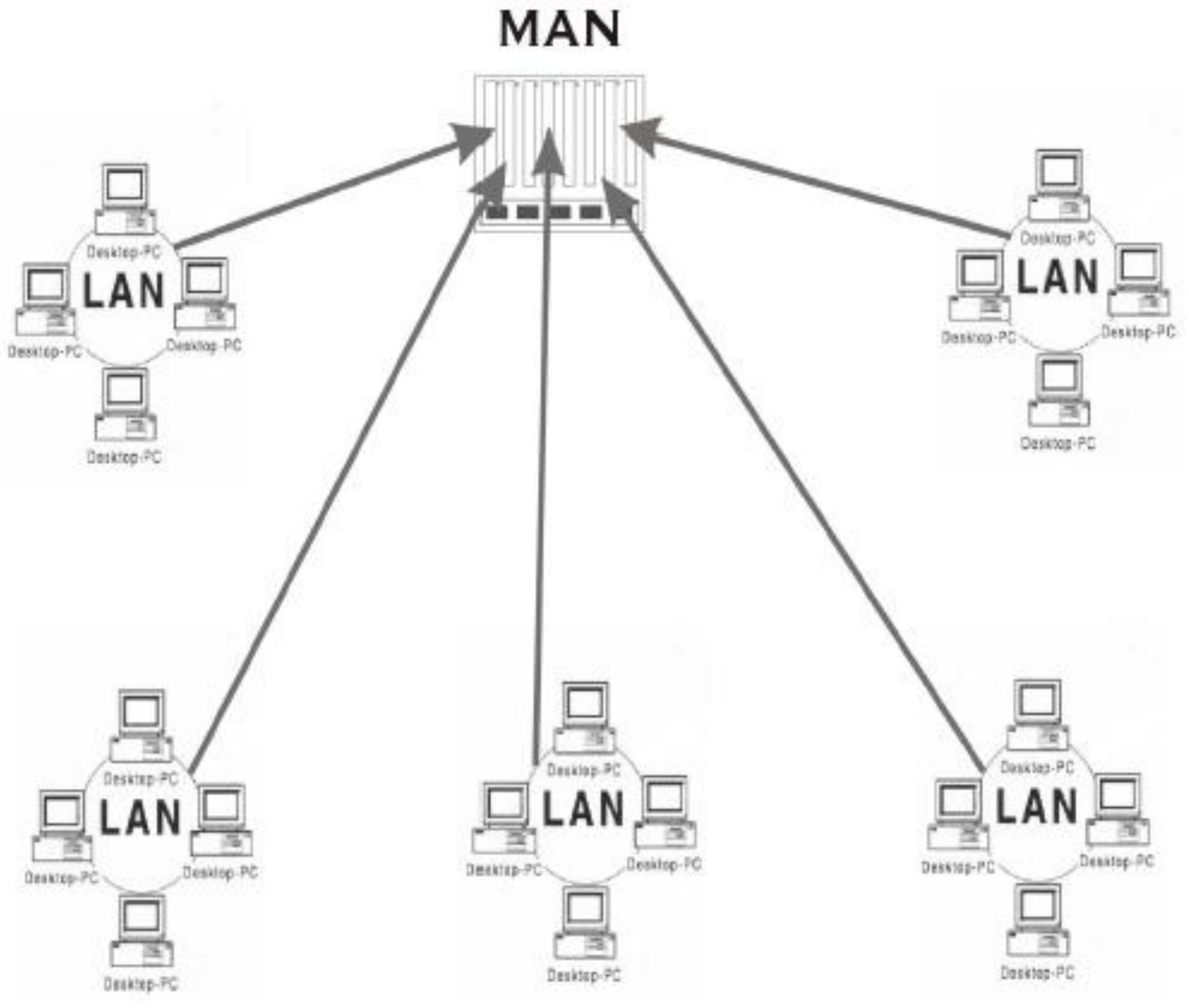
Classification based on Size/Scale…

- Local Area Network (LAN)
  - consists of a computer network at a single site, typically an individual office building.
  - typically used for single sites where people need to share resources among themselves but not with the rest of the outside world.
  - Ex: Network with in our college


File Server
Sniffer
Workstation
Workstation
Dept Printer
10.1.15.1
10.1.50.0 Ethernet Network
Workstation
UPS-Standalone
Raid Drives Storage Tower
Workstation
Workstation
Ethernet Switch
File Server
Workstation
Workstation
Workstation
3Com Switch
10.1.15.250
10.1.50.0 Ethernet Network
Workstation
Workstation
File Server
Workstation
Workstation

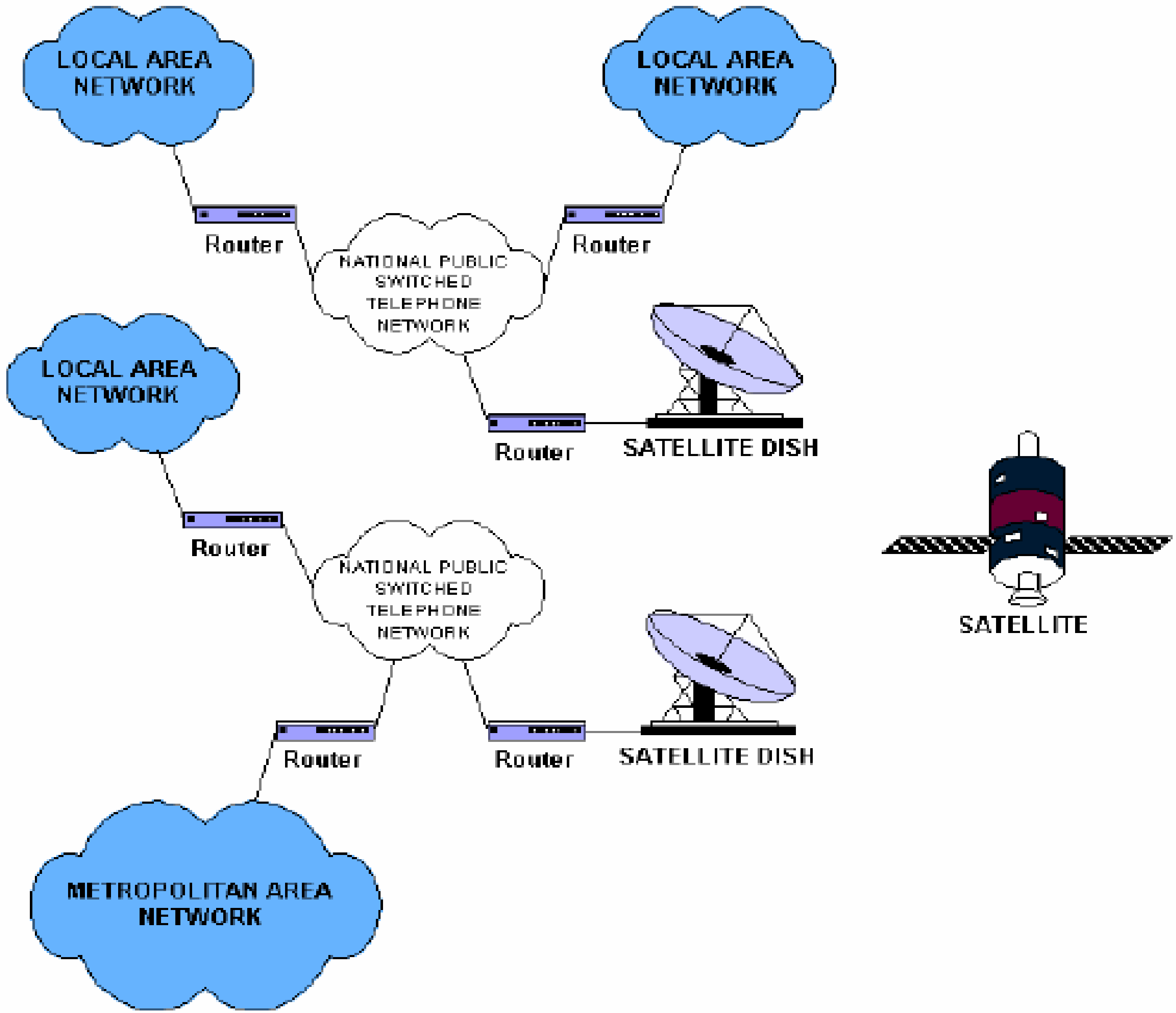
Classification based on Size/Scale…

- Metropolitan Area Network (MAN)
  - consists of a computer network across an entire city, or small region.
  - It is often used to connect several LANs of an organization together to form a bigger network.
  - Ex: Cable Network


MAN
LAN
Desktop-PC
Desktop-PC
Desktop-PC
Desktop-PC
LAN
Desktop-PC
Desktop-PC
Desktop-PC
Desktop-PC
LAN
Desktop-PC
Desktop-PC
Desktop-PC
Desktop-PC
LAN
Desktop-PC
Desktop-PC
Desktop-PC
Desktop-PC
LAN
Desktop-PC
Desktop-PC
Desktop-PC
Desktop-PC

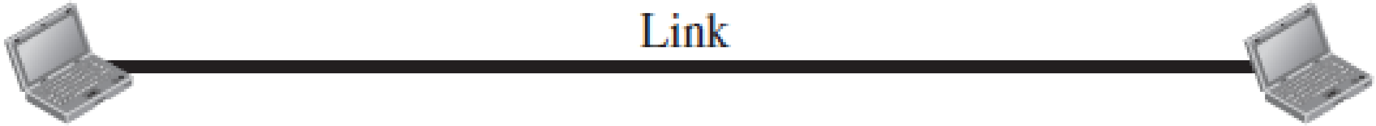
Classification based on Size/Scale…

- Wide Area Network
  - is a computer network that spans a large geographical area
  - are implemented to connect a large number of LANs and MANs.
  - may contain large number of heterogeneous networks.
  - Ex: Telecommunication Network, Internet.

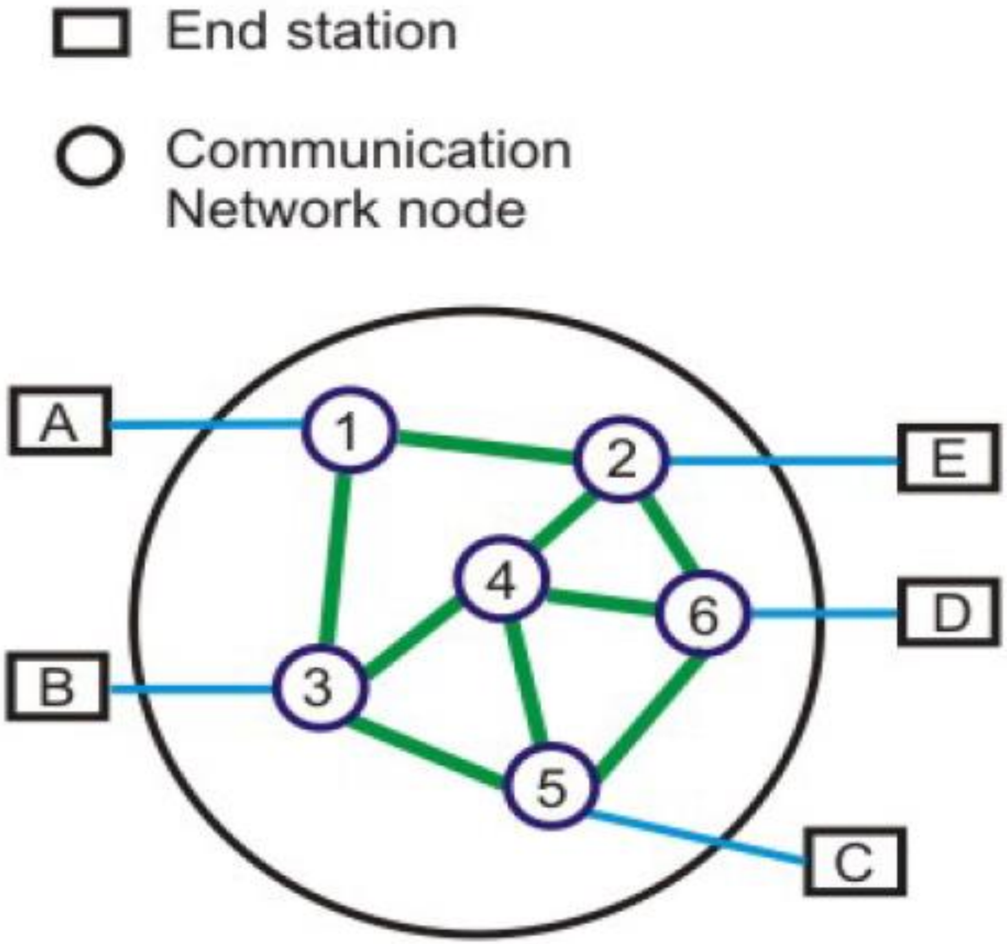

LOCAL AREA NETWORK
LOCAL AREA NETWORK
Router
NATIONAL PUBLIC SWITCHED TELEPHONE NETWORK
Router
LOCAL AREA NETWORK
Router
SATELLITE DISH
SATELLITE
Router
NATIONAL PUBLIC SWITCHED TELEPHONE NETWORK
Router
Router
SATELLITE DISH
METROPOLITAN AREA NETWORK

Classification based on Type of Connection

- Point to Point Networks (P2P)
  - provides a dedicated link between two devices.
  - the entire capacity of the link is reserved for transmission between those two devices.
  - Ex: remote control and the television.



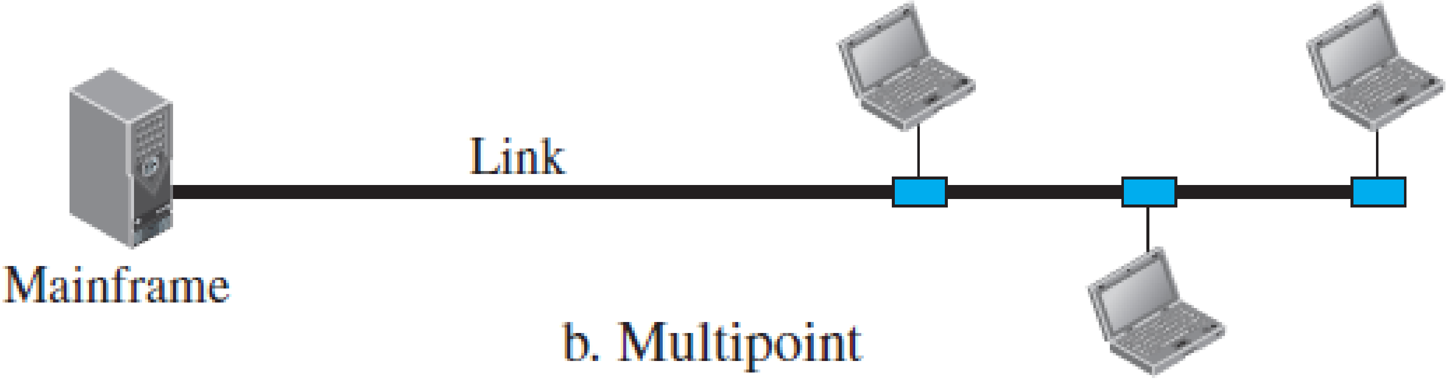
a. Point-to-point



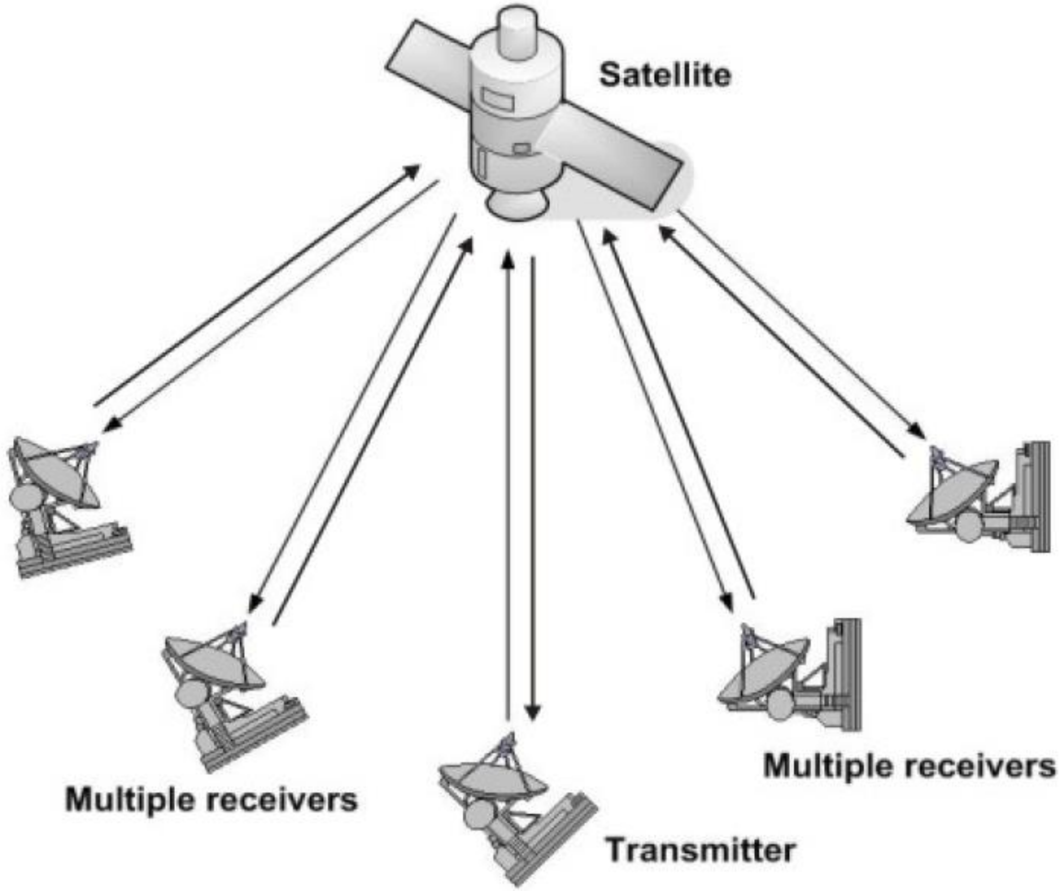
Communication network based on point-to-point communication

Classification based on Type of Connection...

- Multipoint / Broadcast Networks
  - is one in which more than two specific devices share a single link.
  - the capacity of the channel is shared, either spatially or temporally



b. Multipoint

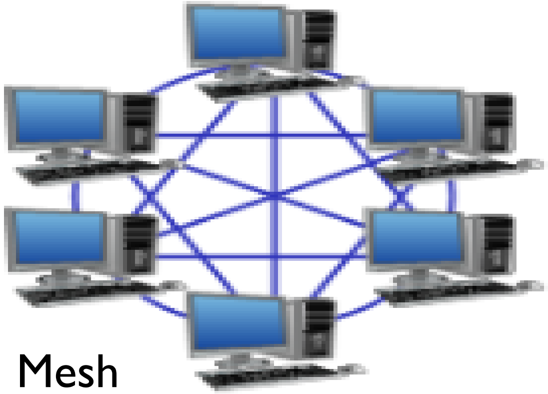


Example of a broadcast network based on satellite communication

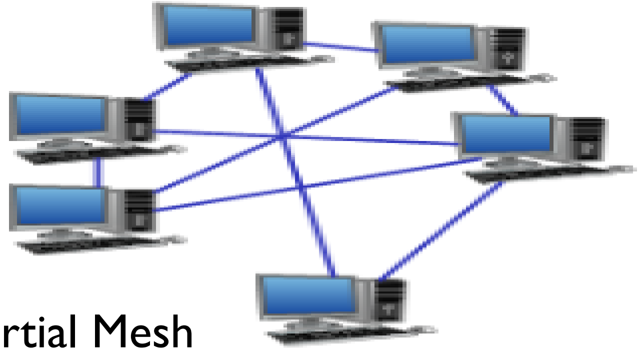
As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks normally use are point-to-point communication.

Classification based on Topology

- Mesh Topology
  - Every networked node is directly connected to every other networked node(Peer to Peer)
  - This topology features the ultimate reliability and fault tolerance
  - Full Mesh - N Nodes → N(N-1)/2 Links
  - Partial Mesh – N Nodes → < N(N-1)/2 Links



Full Mesh

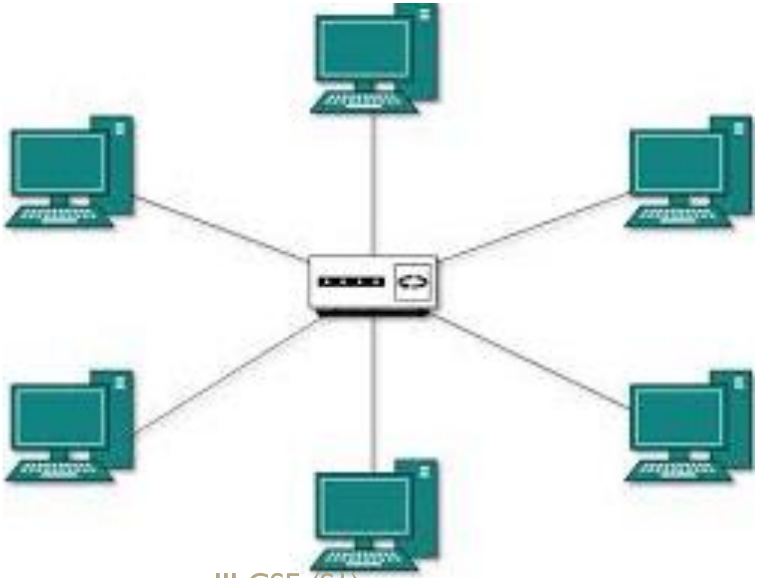


Partial Mesh

- Advantages
  - Minimizes the number of hops between any two network-connected machines
  - Can be built with virtually any transmission technology
- Disadvantages
  - These WANs can be fairly expensive to build
  - A finite (although substantial) limit on the scalability of the network
  - Unlike fully meshed networks, a partial mesh can reduce the startup and operational expenses

Classification based on Topology…

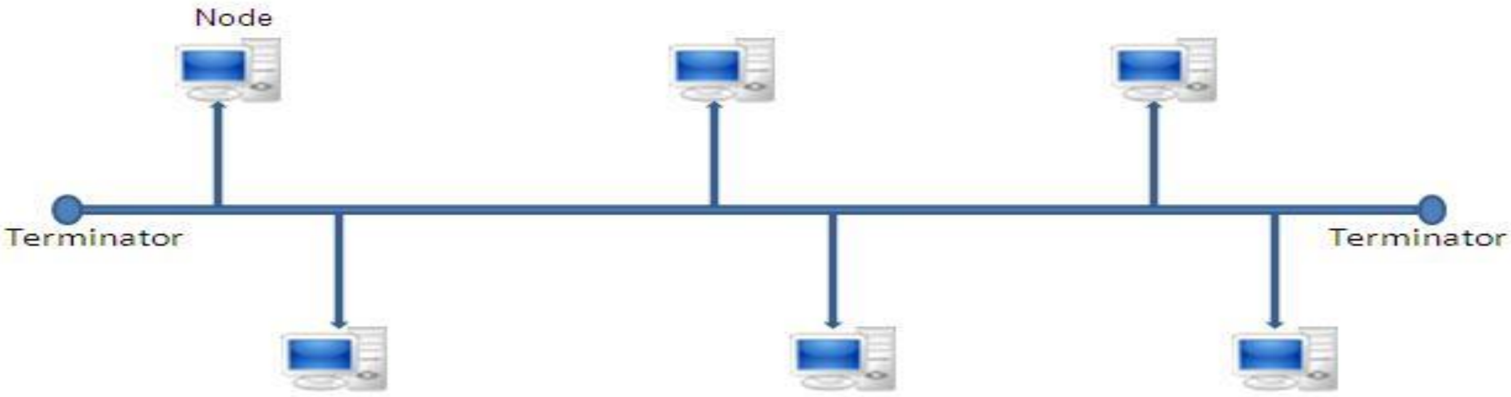
- Star Topology
  - each node is connected to a central hub/switch using a point-to-point connection.
  - it is very popular because the startup costs are low.
  - It is also easy to add new nodes to the network.



- Advantages
  - Centralized management. It helps in monitoring the network
  - Failure of one node or link doesn’t affect the rest of network
- Disadvantages
  - If central device fails whole network goes down
  - Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

Classification based on Topology…

- Bus Topology
  - All networked nodes are interconnected, peer to peer, using a single, open-ended cable
  - Both ends of the bus must be terminated with a terminating resistor to prevent signal bounce

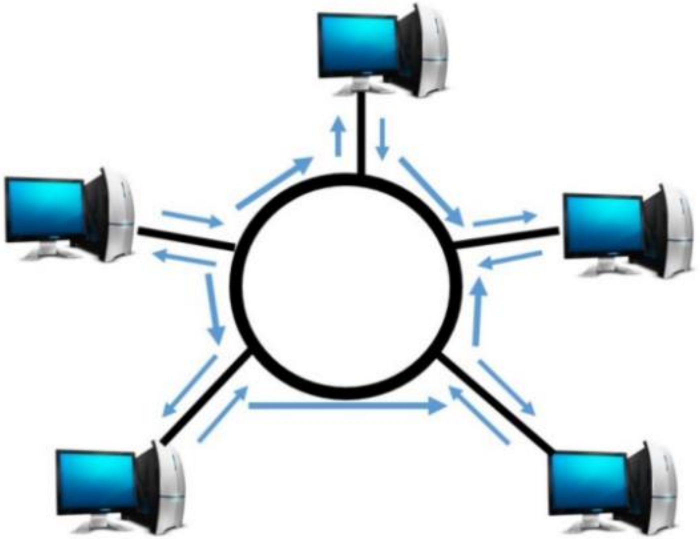


- Advantages
  - Easy to implement and extend
  - Well suited for temporary networks that must be set up in a hurry
  - Typically the least cheapest topology to implement
  - Failure of one station does not affect others

- Disadvantages
  - Difficult to administer/troubleshoot
  - Limited cable length and number of stations
  - A cable break can disable the entire network; no redundancy
  - Performance degrades as additional computers are added

Classification based on Topology…

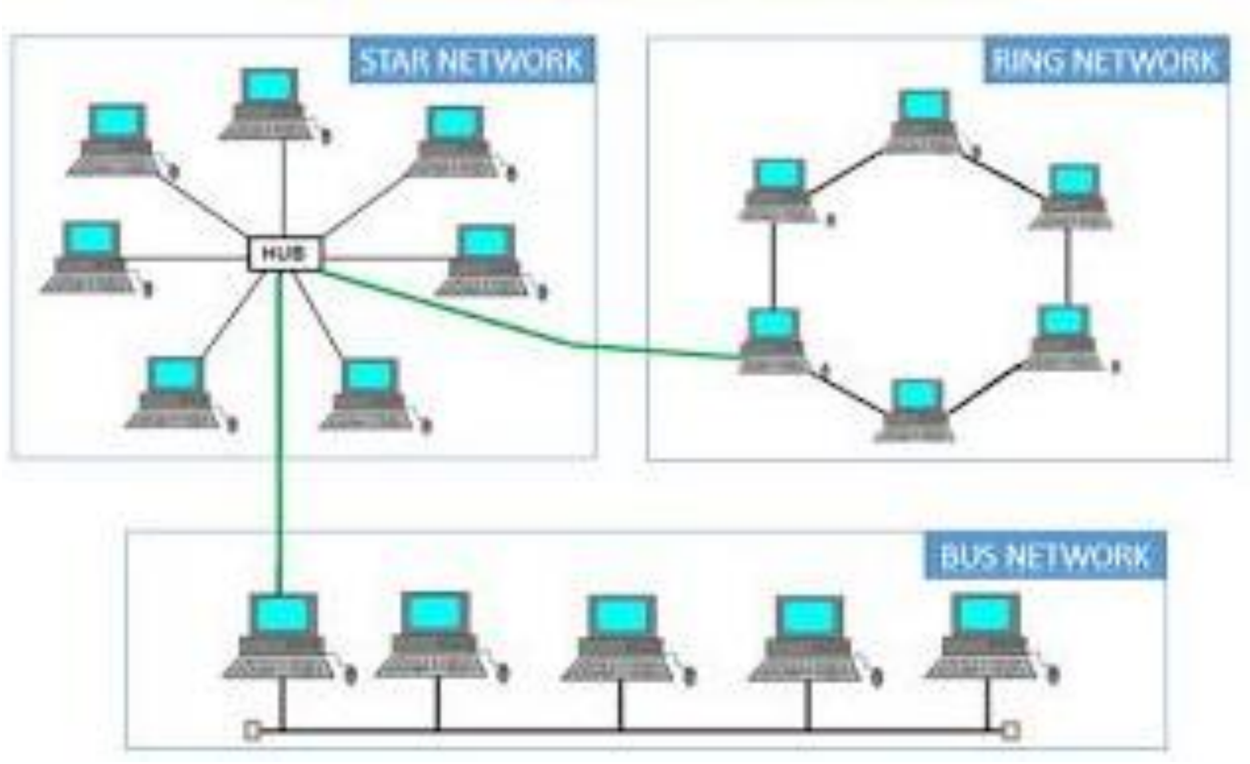
- Ring Topology
  - Each networked workstation had two connections: one to each of its nearest neighbors
  - Data was transmitted unidirectionally around the ring. Sending and receiving of data takes place by the help of TOKEN



- Advantages
  - It provides alternative routes
  - It is less expensive than all
  - It is also good for handling high-volume traffic over long distances since every computer can act as a booster of the signal.
- Disadvantages
  - Depending on the geographic dispersion of the locations, adding an extra transmission facility to complete the ring may be cost prohibitive
  - Rings are not very scalable

Classification based on Topology…

- Hybrid Topology
  - A combination of two or more topology is known as hybrid topology.



- Advantages
  - We can choose the topology based on the requirement
  - Scalable as we can further connect other computer networks with the existing networks
- Disadvantages
  - Fault detection is difficult.
  - Installation is difficult.
  - Design is complex so maintenance is high thus expensive.

Classification based on Kind of Network Media connectivity

- Wired Networks
  - can be defined as the connection of nodes through physical media connection such as Twisted pair, Coaxial Cable, Optical Fiber

Advantages:

- it has high bandwidth and low interference
- security in the wired network is better

Disadvantages:

- more expensive
- Mobility of devices is not possible

Classification based on Kind of Network Media connectivity

- Wireless Networks
  - the network where the connections are made without the physical wired connection i.e. using electromagnetic radiation, satellite communication

  Advantages:
  - low cost and mobility
  - easy to install

  Disadvantages:
  - need a high security because the data is transmitted in air
  - high interference/noise due to external factors

Classification based on Kind of Network Media connectivity

- Adhoc Networks
  - the network which continuously changes i.e. nodes change
  - generally such networks are wireless
  - If mobility is also involved they are called Mobile Adhoc Networks(MANETS)

Advantages:

- Self-configuring & Flexible

Disadvantages:

- more connection failures
- performance considerations
- network connection costs

Classification based on Kind of Network Media connectivity

- Heterogeneous Networks
  - the network which is combination of wired / wireless / adhoc networks
  - mostly used in real time networks

Advantages:

- High scalability

Disadvantages:

- Integration of technologies
- Installation & trouble shooting
- maintenance costs

Classification based on Service Offered

- Connection Oriented Service
  - The **Connection oriented services** establish a **connection** prior to sending the packets belonging to the same message from source to the destination.
  - It includes three stages
    1) Connection Establishment.
    2) Data Transmission.
    3) Connection Release.
  - In connection-oriented service, Handshake method is used to establish the connection between sender and receiver.

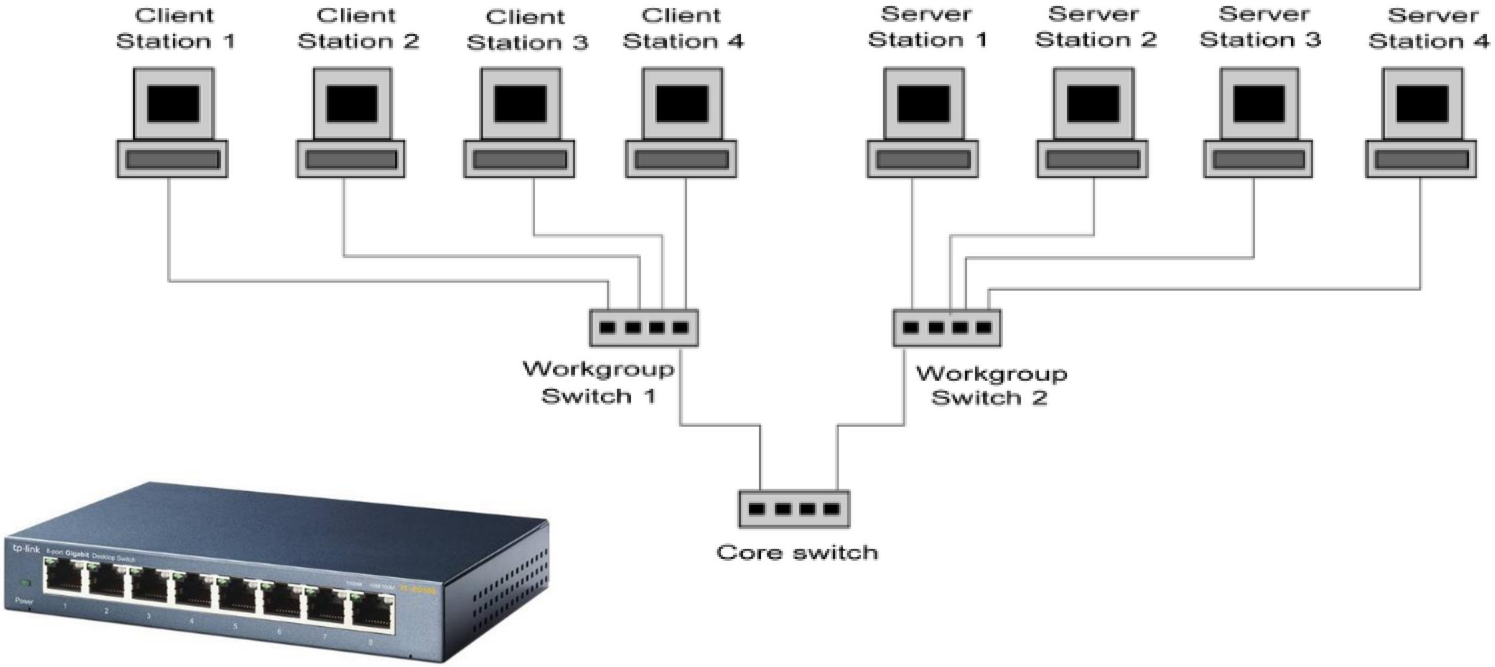
Classification based on Service Offered

- Connectionless Service
  - It does not include any connection establishment and connection termination.
  - Connectionless Service does not give the guarantee of delivery of data.
  - Authentication is not needed.

Switching

- End devices need not be directly connected to each other
- In such cases the end devices are connected by means of set of intermediary devices
- The mechanism of forwarding data between devices of such network is called network switching.

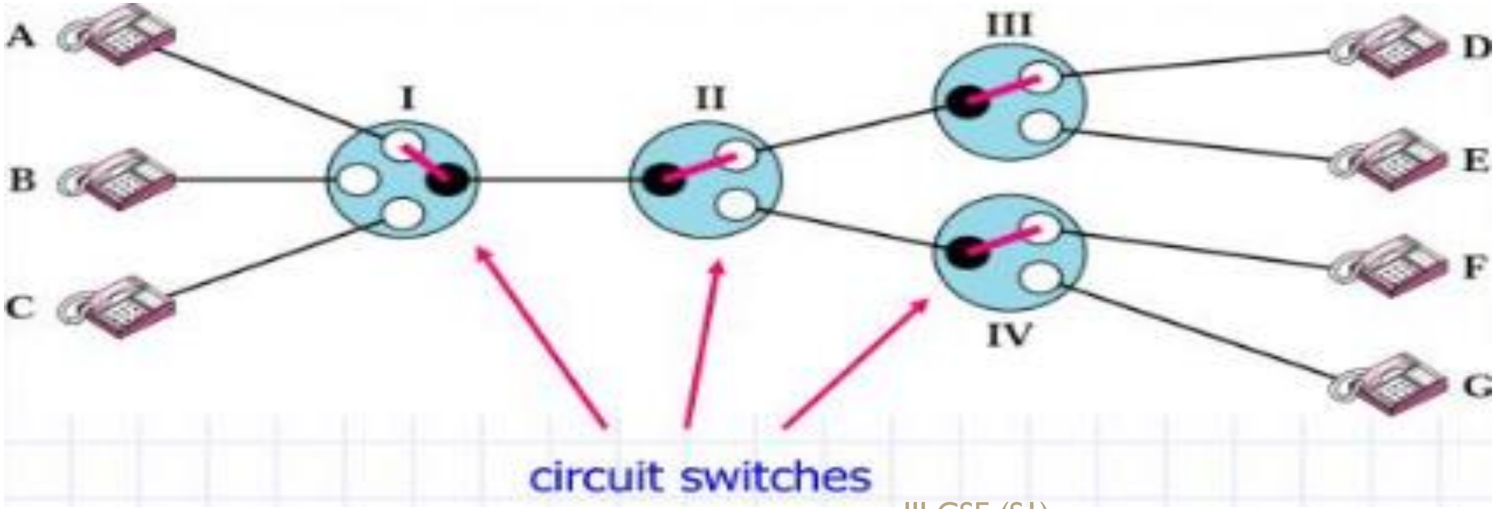
Switching

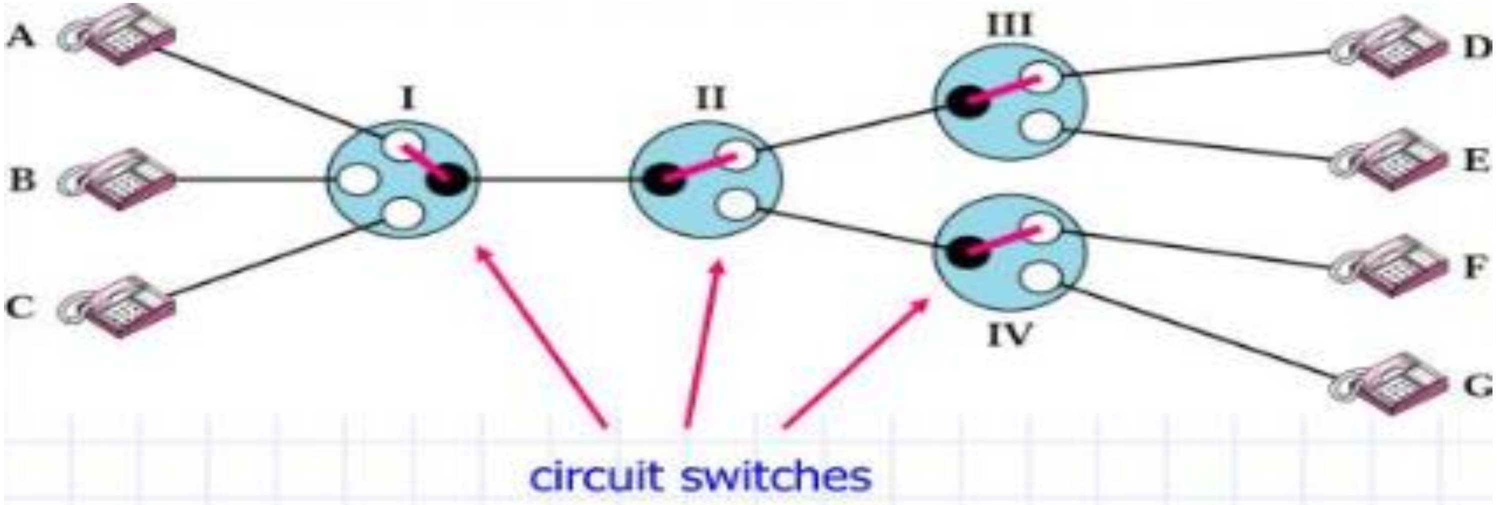


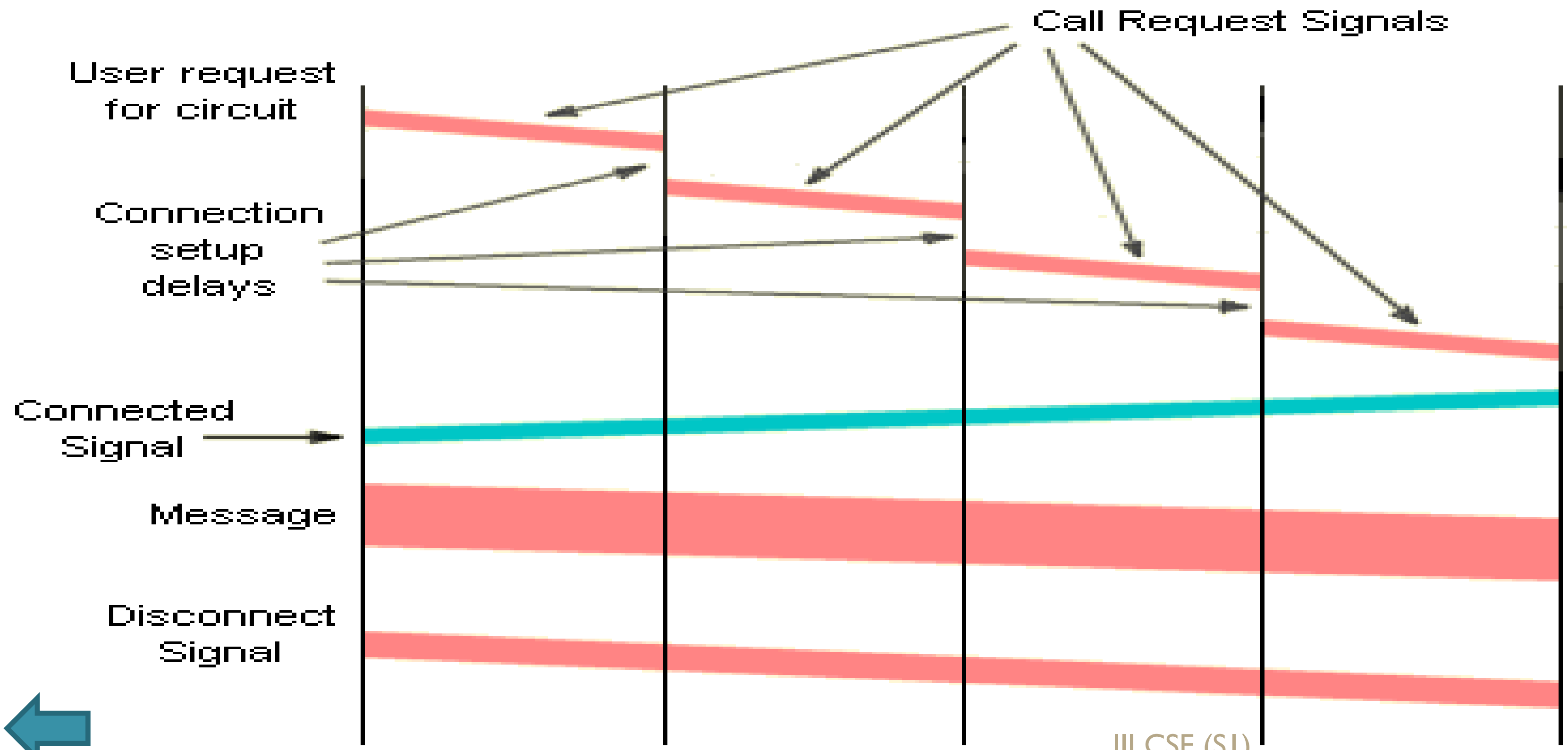
- Data entering through a incoming line/port is referred to as **ingress**, while data leaving through outgoing line/port is referred to as **egress**.

Classification based on Switching

- Circuit Switching
  - A dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive.
  - the delay is observed in establishing a physical connection.



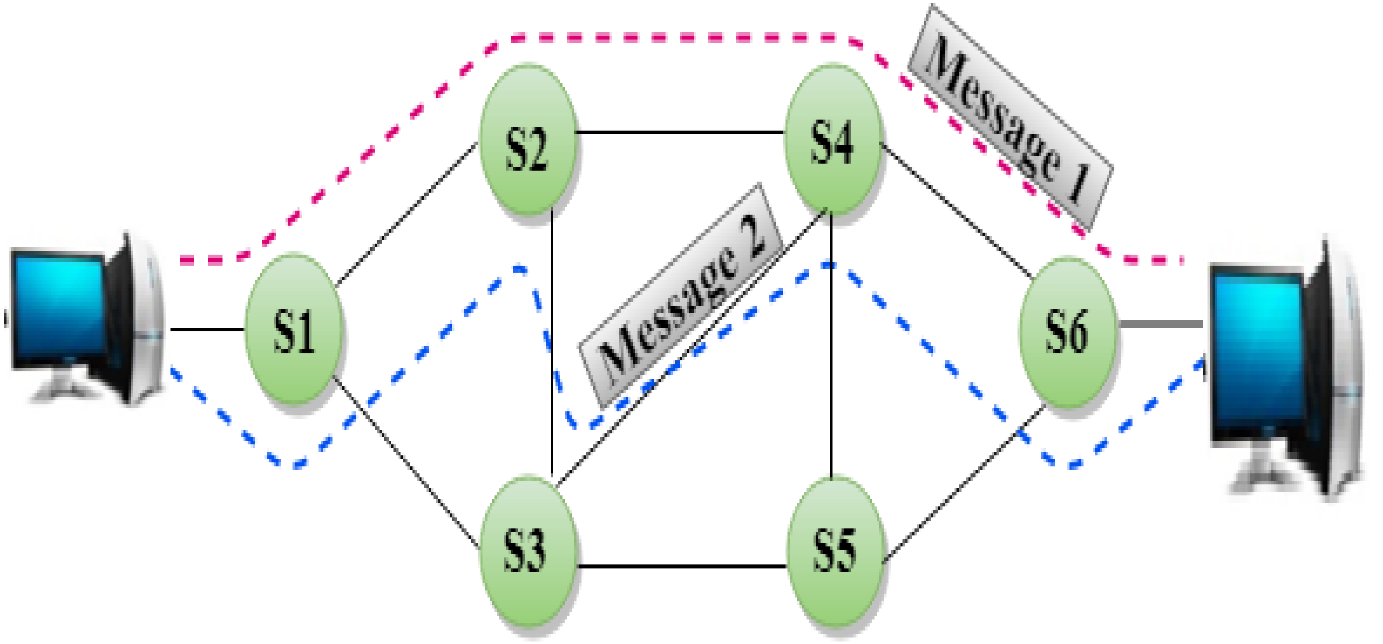

A
B
C
I
II
III
IV
D
E
F
G
circuit switches

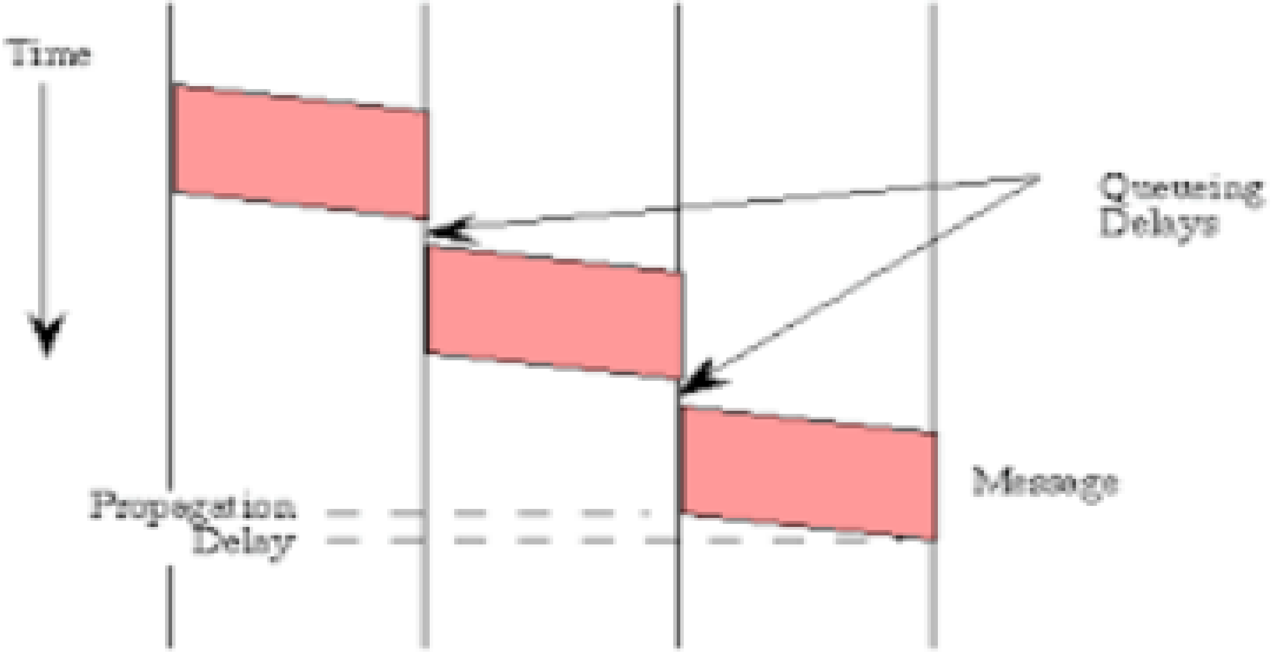

Call Request Signals
User request for circuit
Connection setup delays
Connected Signal
Message
Disconnect Signal

- Advantages
  - The quality of communication is increased as a dedicated communication channel is used.
  - The rate at which the data is transmitted is fixed.
  - It is preferred when the communication is long and continuous.
- Disadvantages
  - Since a dedicated channel is been used, the transmission of other data becomes impossible.
  - The time taken by the two stations for the establishment of the physical link is too long.
  - Circuit switching is expensive because every connection uses a dedicated path establishment.

Classification based on Switching

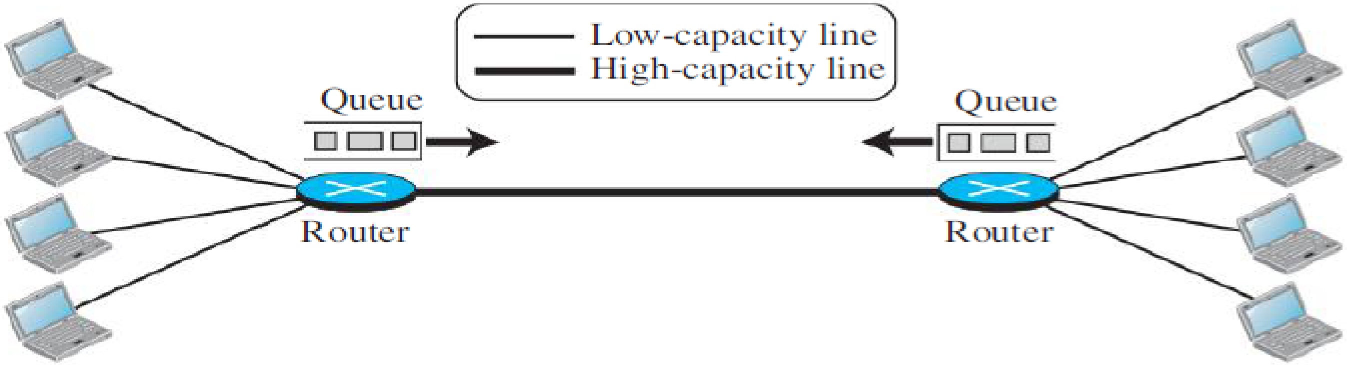
- Message Switching
  - it is not necessary to established a dedicated path in between any two communication devices.
  - Each complete message is then transmitted from one device to another through internetwork.
  - Each intermediate device receive the message and store it until the nest device is ready to receive it and then this message is forwarded to the next device. (Store & Forward Switching)

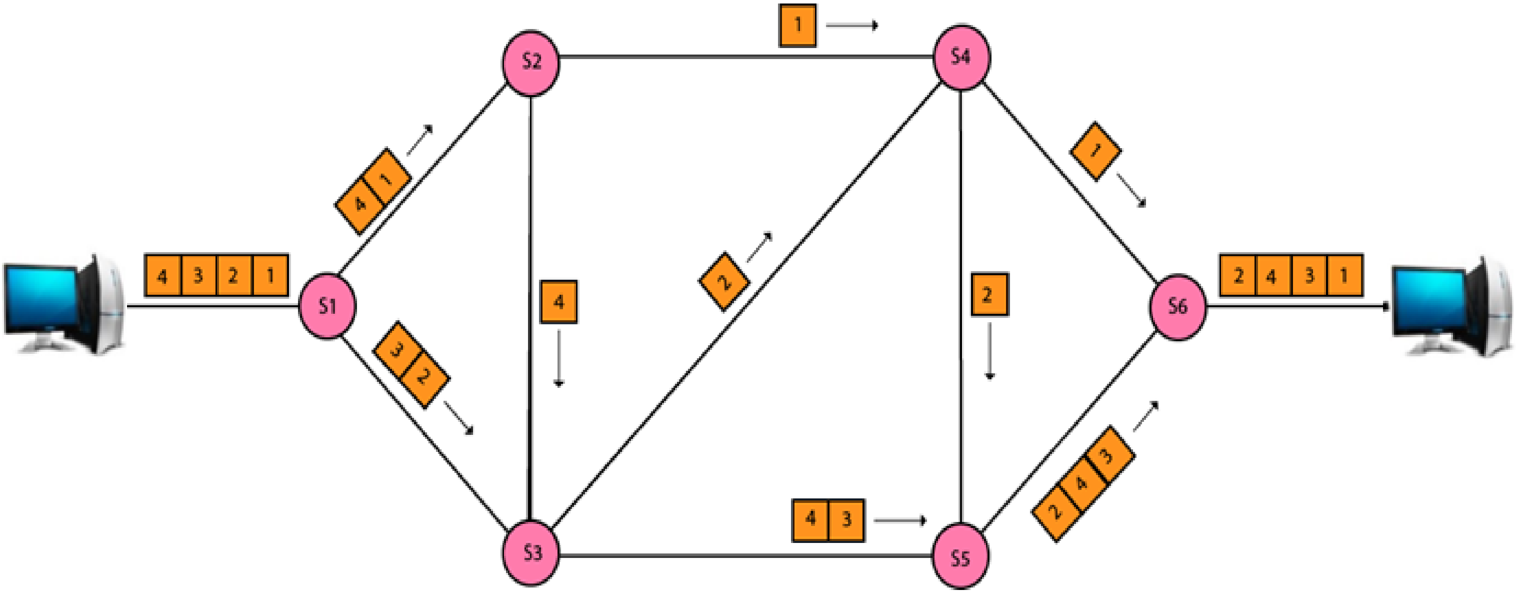

Message 1
S2
S4
Message 2
S1
S6
S3
S5

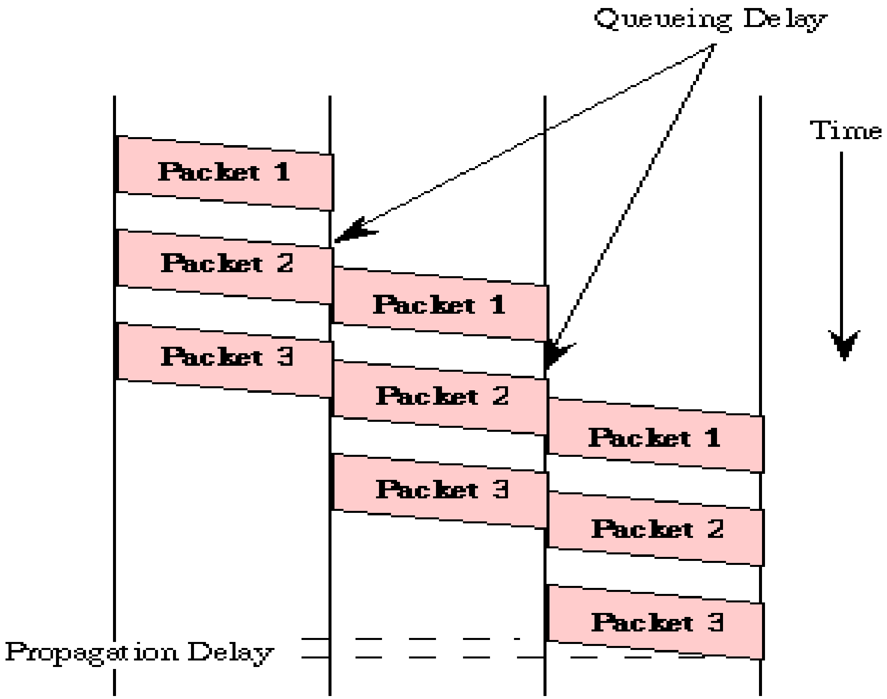

Time
Queueing Delays
Message
Propagation Delay

Classification based on Switching

- Packet Switching
  - It is a connectionless network where the messages are divided into small units of data known as a packet.
  - Each packet is routed from the source to the destination as individually.
  - it is the responsibility of the destination to put these packets in the right order.

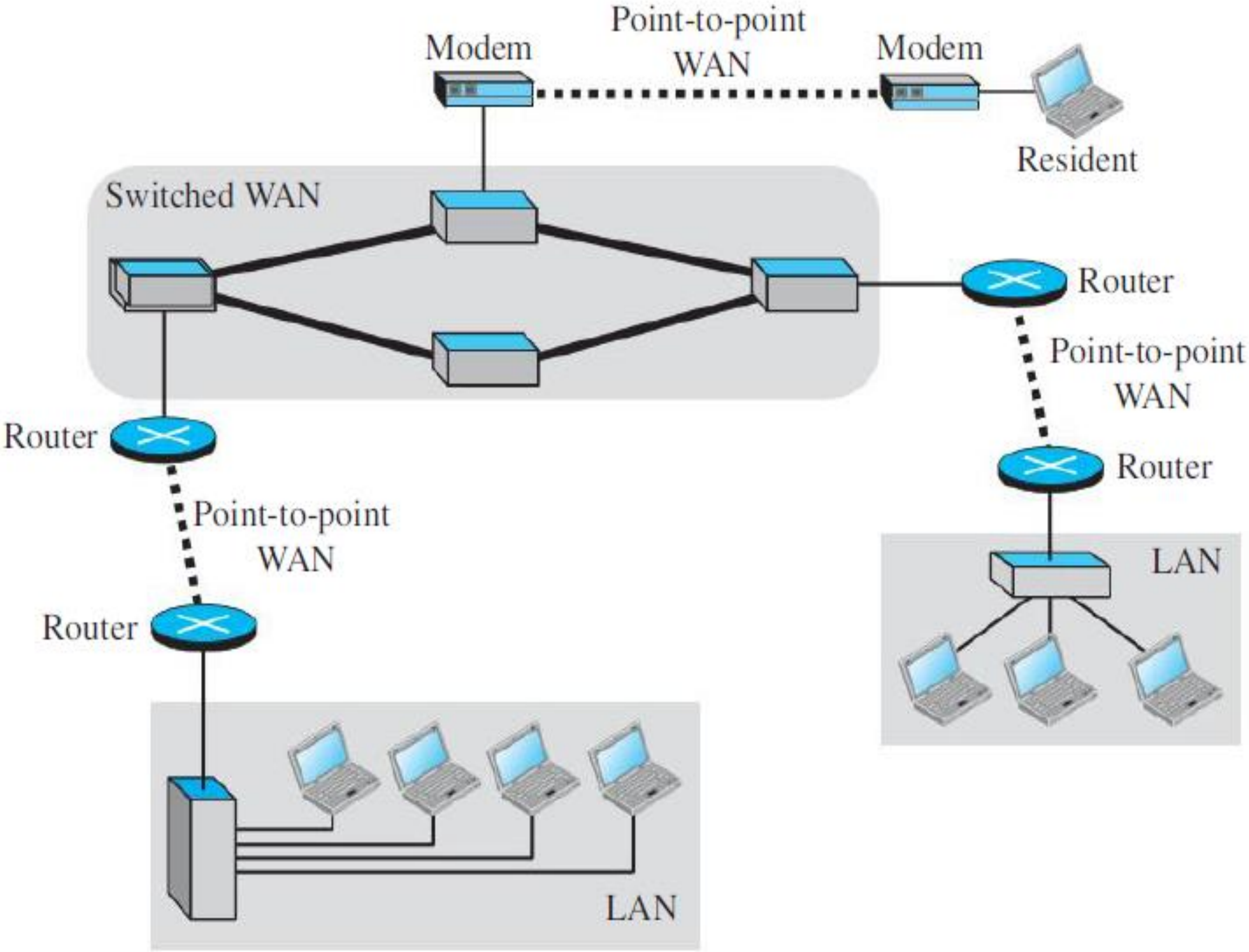



S1
S2
S3
S4
S5
S6
4 3 2 1
4 1
3 2
1
4
2
4 3
2
1
2 4 3
2 4 3 1


Queueing Delay
Time
Packet 1
Packet 2
Packet 3
Packet 1
Packet 2
Packet 3
Packet 1
Packet 2
Packet 3
Propagation Delay

- Advantages
  - There is no requirement for massive storage space as the information is passed on to the destination as soon as they are received.
  - Failure in the links does not stop the delivery of the data as these packets can be routed from other paths too.
  - Multiple users can use the same channel while transferring their packets.
  - The usage of bandwidth is better in case of packet switching as multiple sources can transfer packets from the same source link.

- Disadvantages
  - Installation/maintenance costs of packet switching are expensive.
  - Connectivity issues may lead to loss of information and delay in the delivery of the information.
  - Live communication cannot use packet switching as there is a out of order delivery of packets (if routed through different paths).

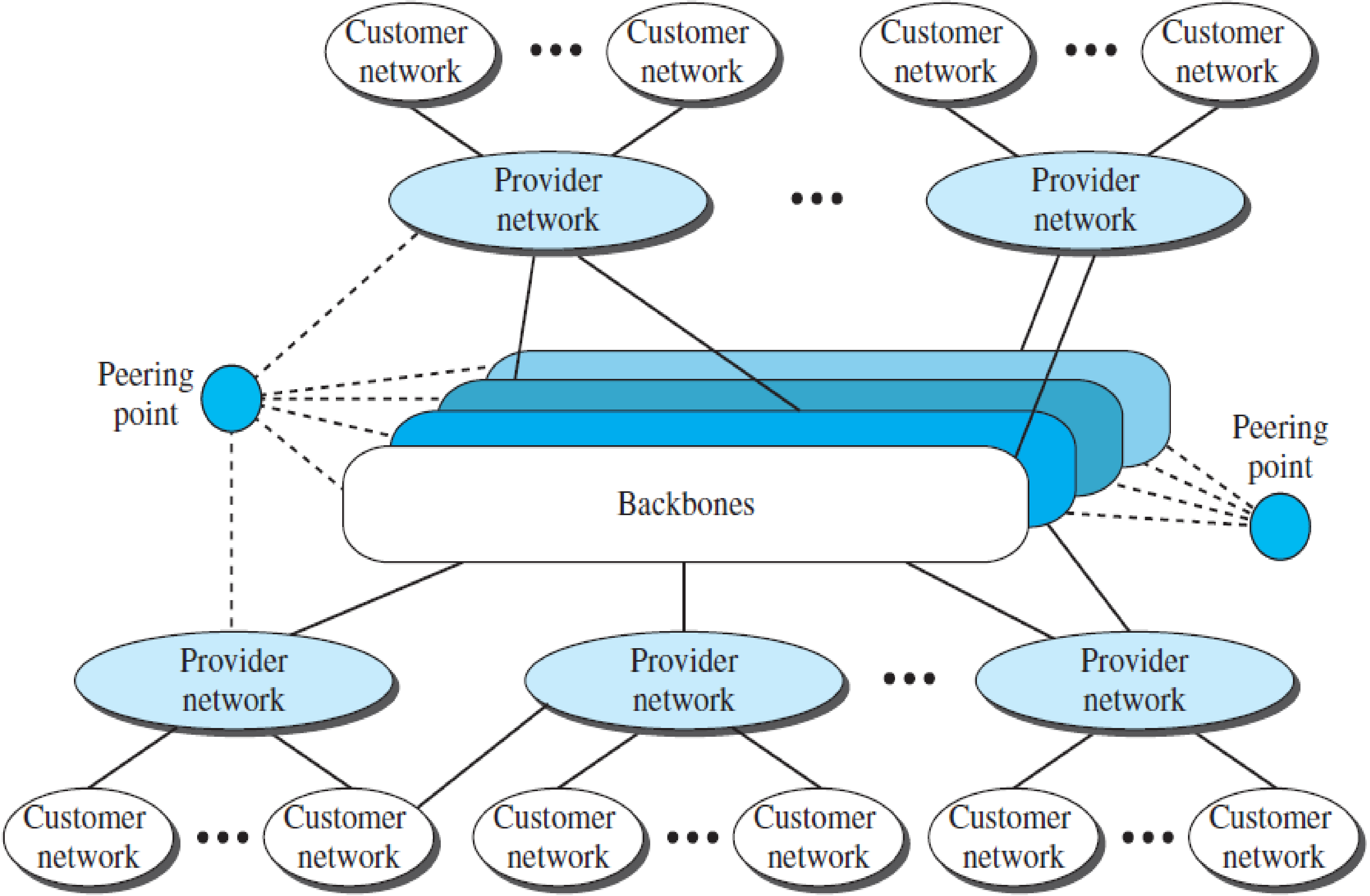


A heterogeneous network made of four WANs and three LANs

Internet

- It is a heterogeneous wide area network composed of thousands of interconnected networks.
- Internet as several backbones, provider networks, and customer networks.
- At the top level, the ***backbones*** are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT. The backbone networks are connected through some complex switching systems, called ***peering points***.
- At the second level, there are smaller networks, called ***provider networks***, that use the services of the backbones for a fee. The provider networks are connected to backbones and sometimes to other provider networks.

- The ***customer networks*** are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.
- Backbones and provider networks are also called **Internet Service Providers (ISPs).** The backbones are often referred to as *International ISPs;* the provider networks are often referred to as N*ational* or *Regional ISPs*.



The Internet today

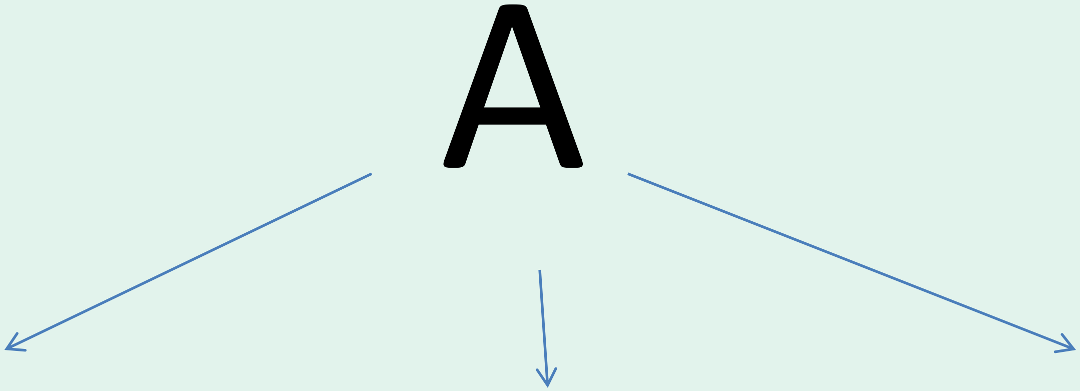
NETWORK SOFTWARE MODELS

UNIT-1(Part-B)

Contents:

- Functionalities of Computer Network
- Introduction to design of Network Software
- OSI Reference Model
- TCP/IP Model
- Comparison between OSI & TCP/IP

Encoding



A

00001010

ASCII - American Standard Code for Information Interchange

01000001

Extended Binary Coded Decimal Interchange Code (**EBCDIC**)

00000000 00000000
00000000 01000001

Unicode Text Format(UTF-32)

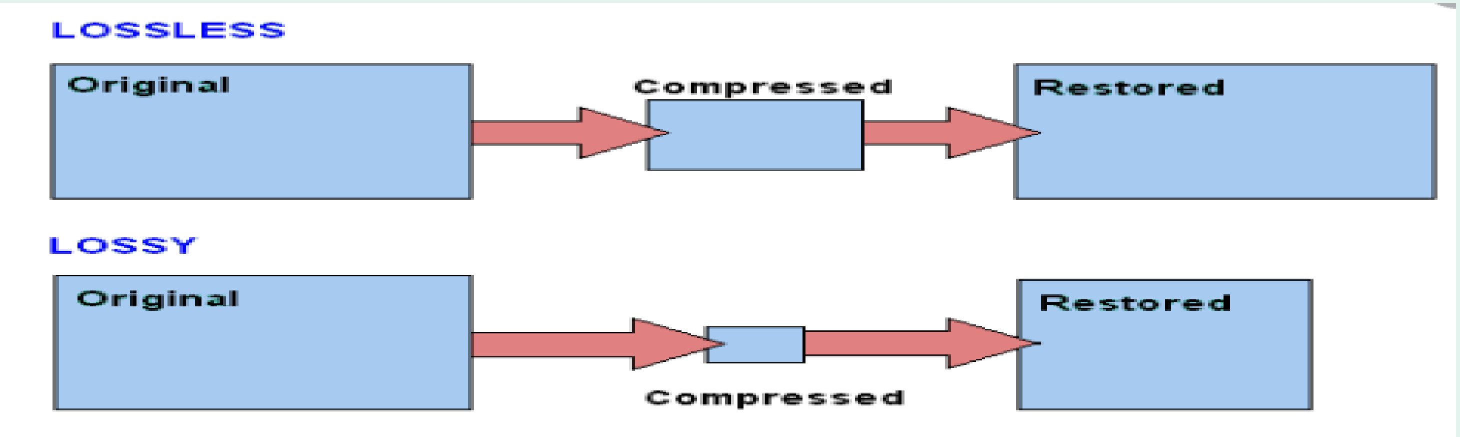
Type of Service

- Connection Oriented Mechanism
  - Connection Establishment
  - Data Transfer
  - Connection Release

- Connectionless Mechanism
  - Direct Data Transfer

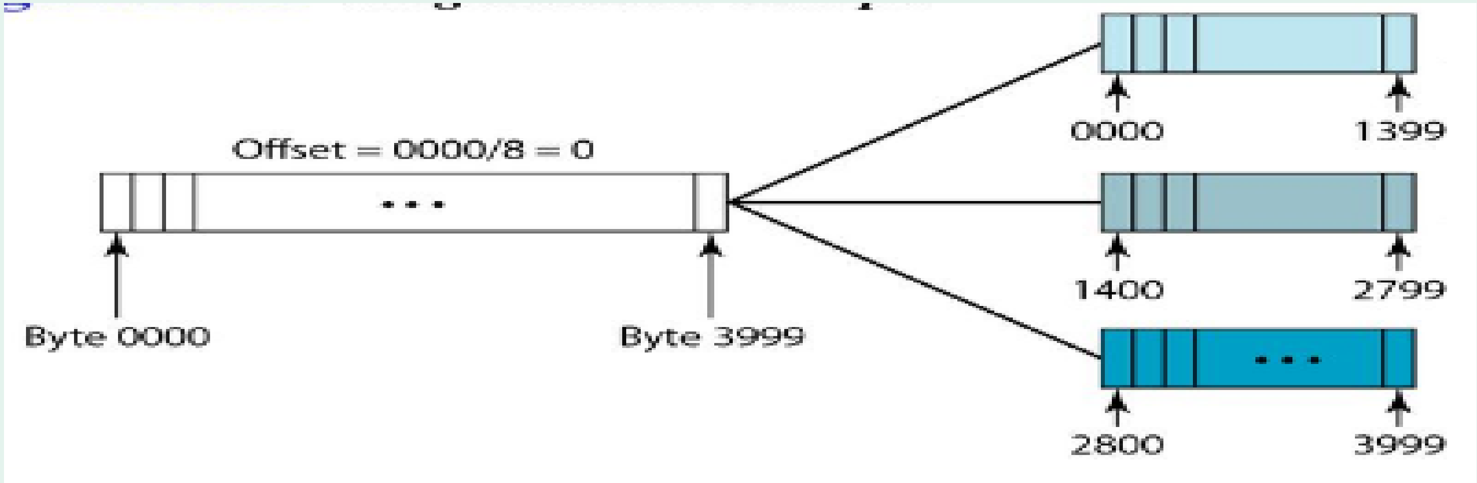
Compression

- **Compression** is the method **computers** use to make files smaller by reducing the number of bits (1's and 0's) used to store the information.
- Compression
  - Lossless Compression
  - Lossy Compression



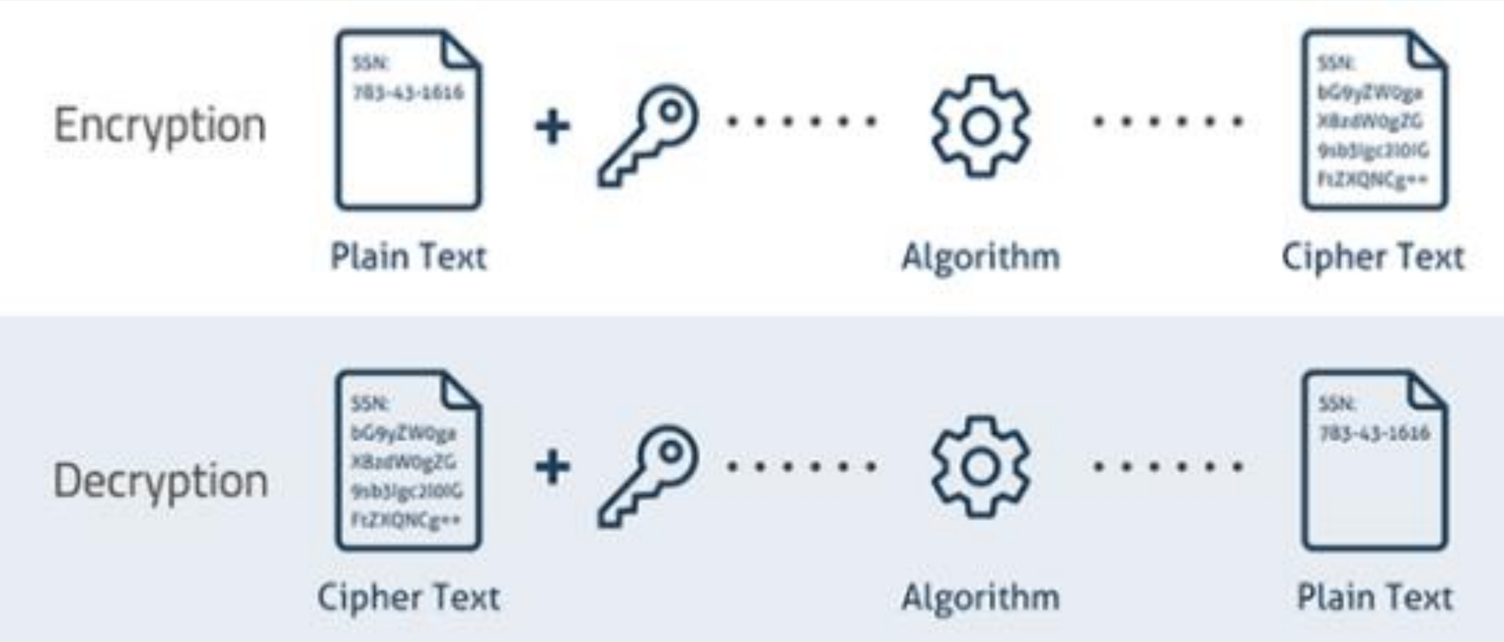
Dividing into Smaller units of data (Segments/Packets/Frames)

- Network Software Support
- Medium Support
- Easy transmission
- Error → Resending



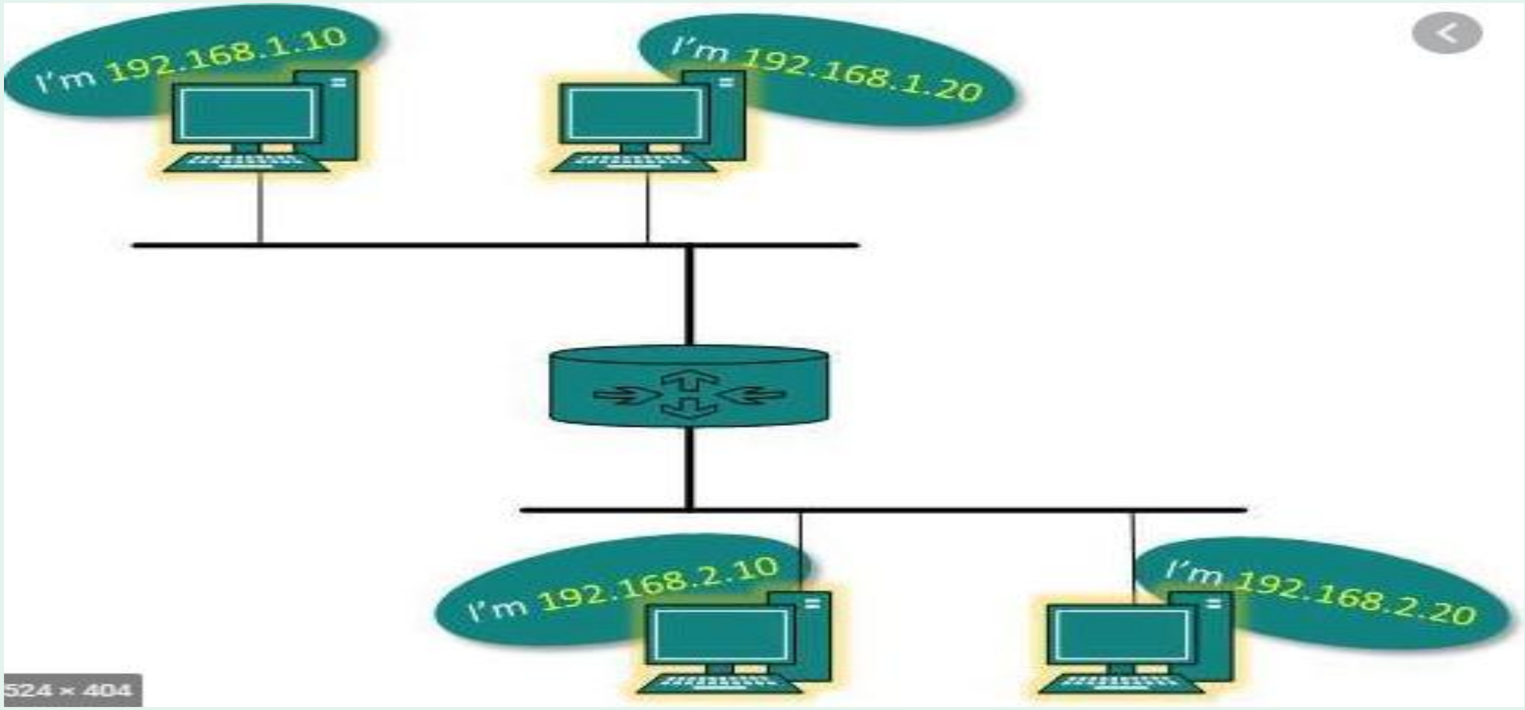
Encryption

- **Encryption** is a process that encodes a message or file so that it can be only be read by certain people



Logical Addressing

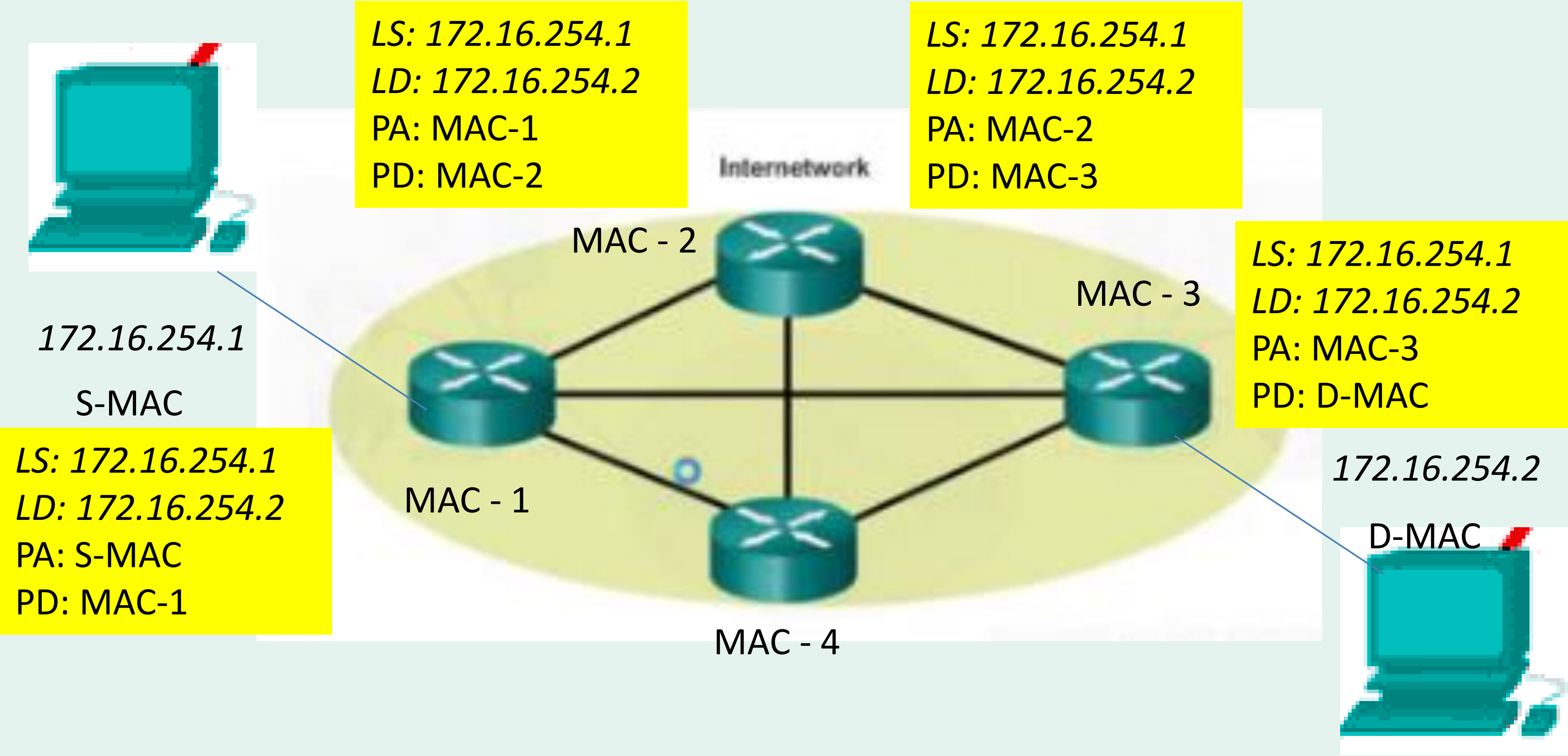
- The method of assigning unique ID to every device connected in network
- End to End communication



- Delivery parameters (cookies)
  - Time
  - When to start & end in Connection Oriented Service
- Delivery confirmation
  - Reliable - Acknowledgement
  - Unreliable - No acknowledgement
- Media
  - Guided
  - Unguided

Physical Addressing

- Hop by Hop communication



LS: 172.16.254.1
LD: 172.16.254.2
PA: S-MAC
PD: MAC-1

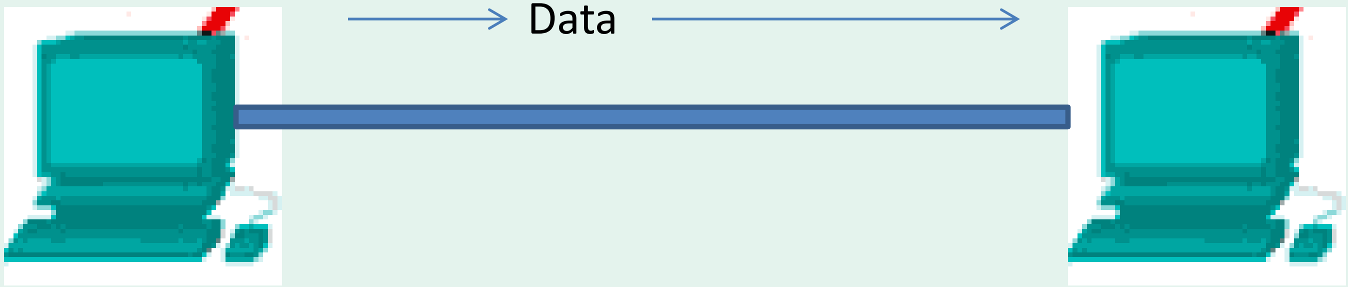
LS: 172.16.254.1
LD: 172.16.254.2
PA: MAC-1
PD: MAC-2

LS: 172.16.254.1
LD: 172.16.254.2
PA: MAC-2
PD: MAC-3

LS: 172.16.254.1
LD: 172.16.254.2
PA: MAC-3
PD: D-MAC

Service

- Process to Process communication



File Transfer
Web Browser
Database server

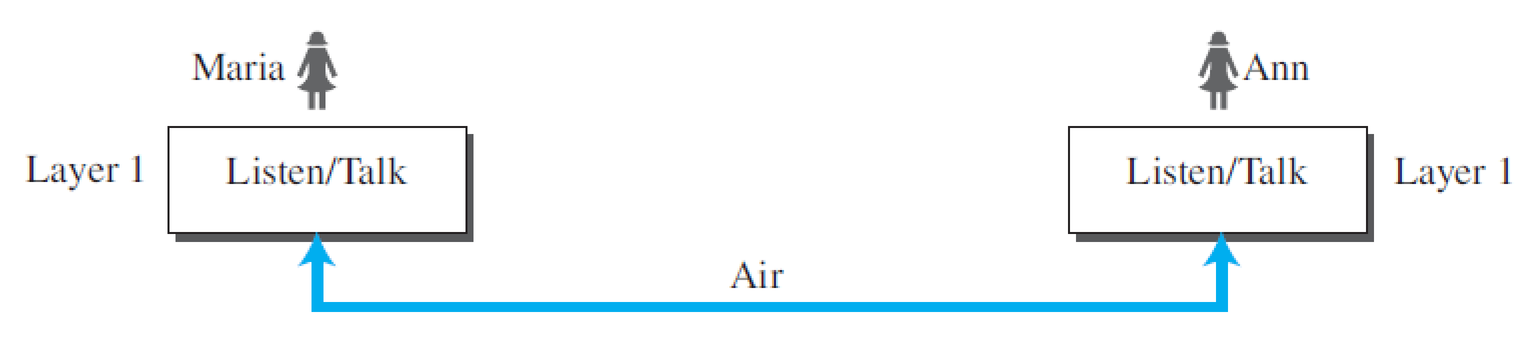
Symmetrical Problems in Network Communication

General Issue	Computer Networks
Language	Encoding (Character / Signal)
Seeking Permission	Connection Oriented/Connectionless
Actual Address	Logical Address
Packing mechanism	Compression
Security	Encryption
Delivery Time	Dialog Control
Delivery Confirmation	Reliability
Postal Package Damage	Error Control (Network/Sender)
Mode of Travel	Media
Intermediary Path	Physical Address
In Person Delivery	Process
Weight	Dividing Data (Segmentation, Packeting, Framing)

Protocol Layering

- A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.
- When communication is simple, we may need only one simple protocol.
- When the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering.

Scenario 1



Maria

Ann

Layer 1

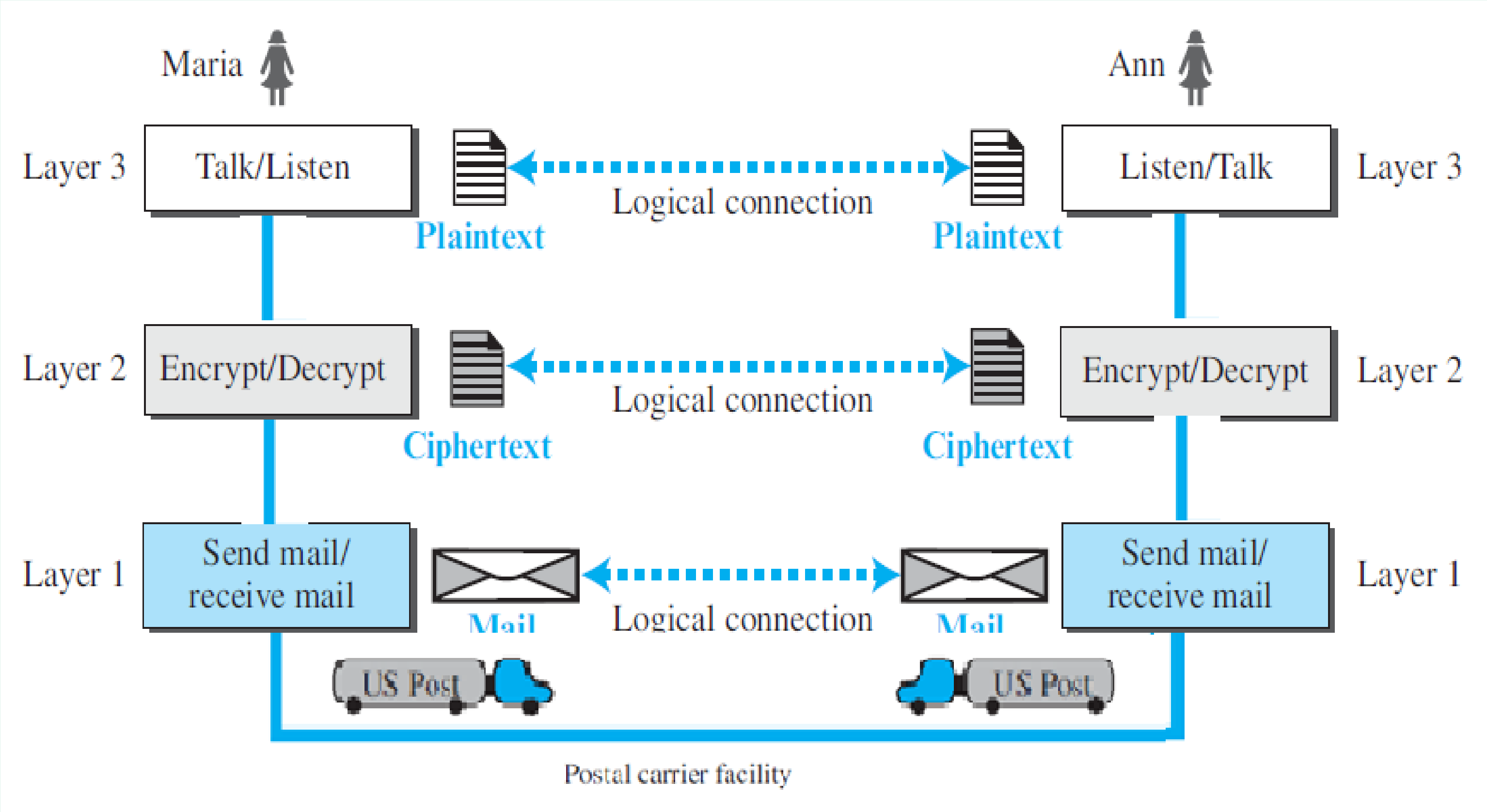
Listen/Talk

Listen/Talk

Layer 1

Air

Scenario 2



Maria

Ann

Layer 3

Talk/Listen

Listen/Talk

Layer 3

Logical connection

Plaintext

Plaintext

Layer 2

Encrypt/Decrypt

Encrypt/Decrypt

Layer 2

Logical connection

Ciphertext

Ciphertext

Layer 1

Send mail/ receive mail

Send mail/ receive mail

Layer 1

Logical connection

Mail

Mail

US Post

US Post

Postal carrier facility

Advantages:

- Enables us to divide a complex task into several smaller and simpler tasks
- It allows us to separate the services from the implementation
- Service gets compromised it is responsibility of that layer which is performing the service
- Intermediate systems that need only some layers, but not all layers(ex. Intermediate mail sender)

Principles in design:

- Make each layer so that it is able to perform two opposite tasks, one in each direction(i.e . talk/listen, encrypt/decrypt, send/receive)
- Two objects under each layer at both sites should be identical (letter, cipher text, piece of mail)

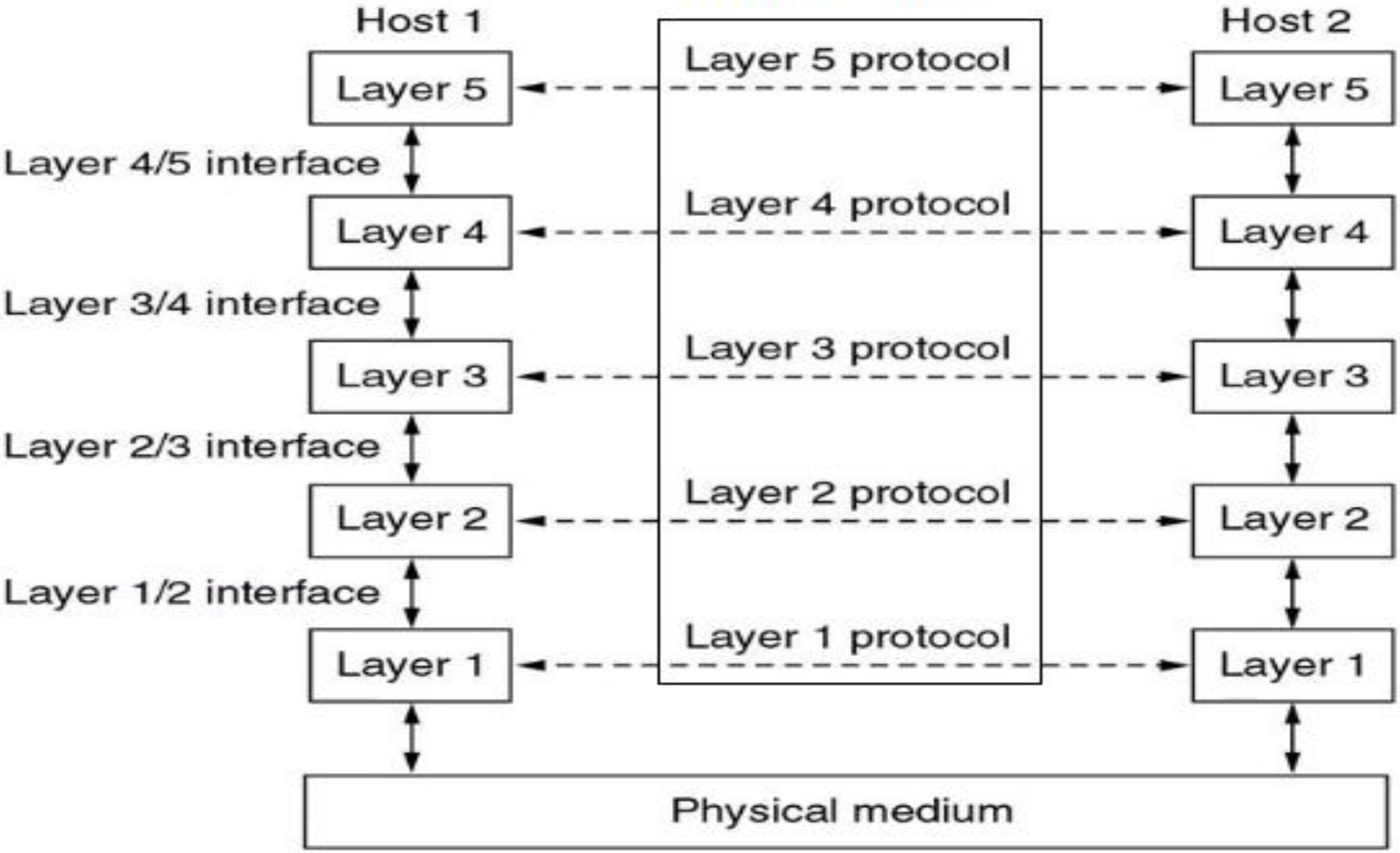
Network Software design

- To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- **A protocol** is an agreement between the communicating parties on how communication is to proceed.
- Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached and vice versa(i.e. hierarchical) .
- 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.

Network Software design

- A set of layers and protocols is called a **network architecture**. The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.
- A list of protocols used by a certain system, one protocol per layer, is called a **protocol stack**.
- A service is formally specified by a set of **primitives (operations)** available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity to the layer above it. (ex. SEND/RECEIVE/ CONNECT/DISCONNECT/LISTEN)
- The set of primitives available depends on the nature of the service being provided.

Protocol Stack



Host 1

Host 2

Layer 5

Layer 5 protocol

Layer 5

Layer 4/5 interface

Layer 4

Layer 4 protocol

Layer 4

Layer 3/4 interface

Layer 3

Layer 3 protocol

Layer 3

Layer 2/3 interface

Layer 2

Layer 2 protocol

Layer 2

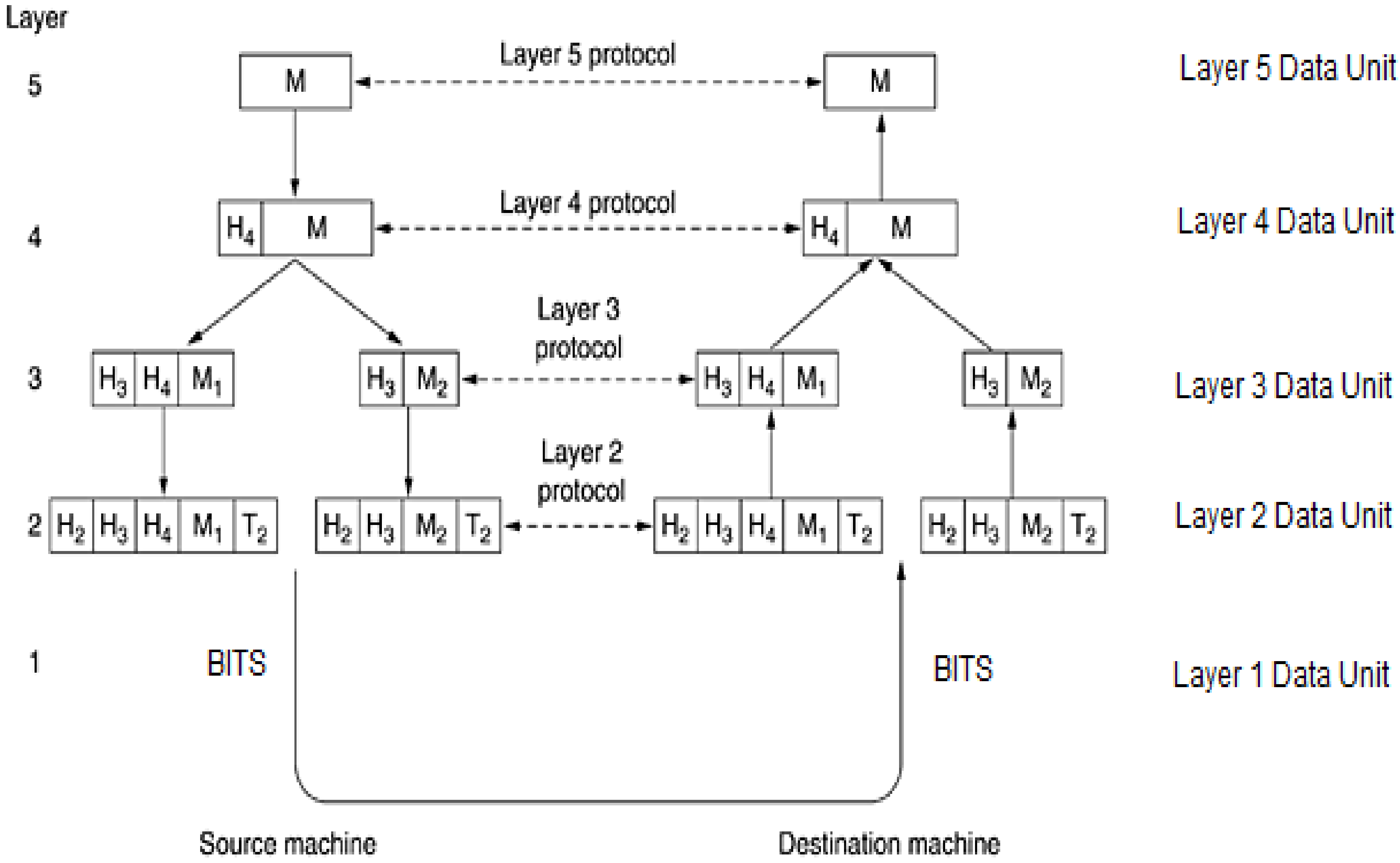
Layer 1/2 interface

Layer 1

Layer 1 protocol

Layer 1

Physical medium

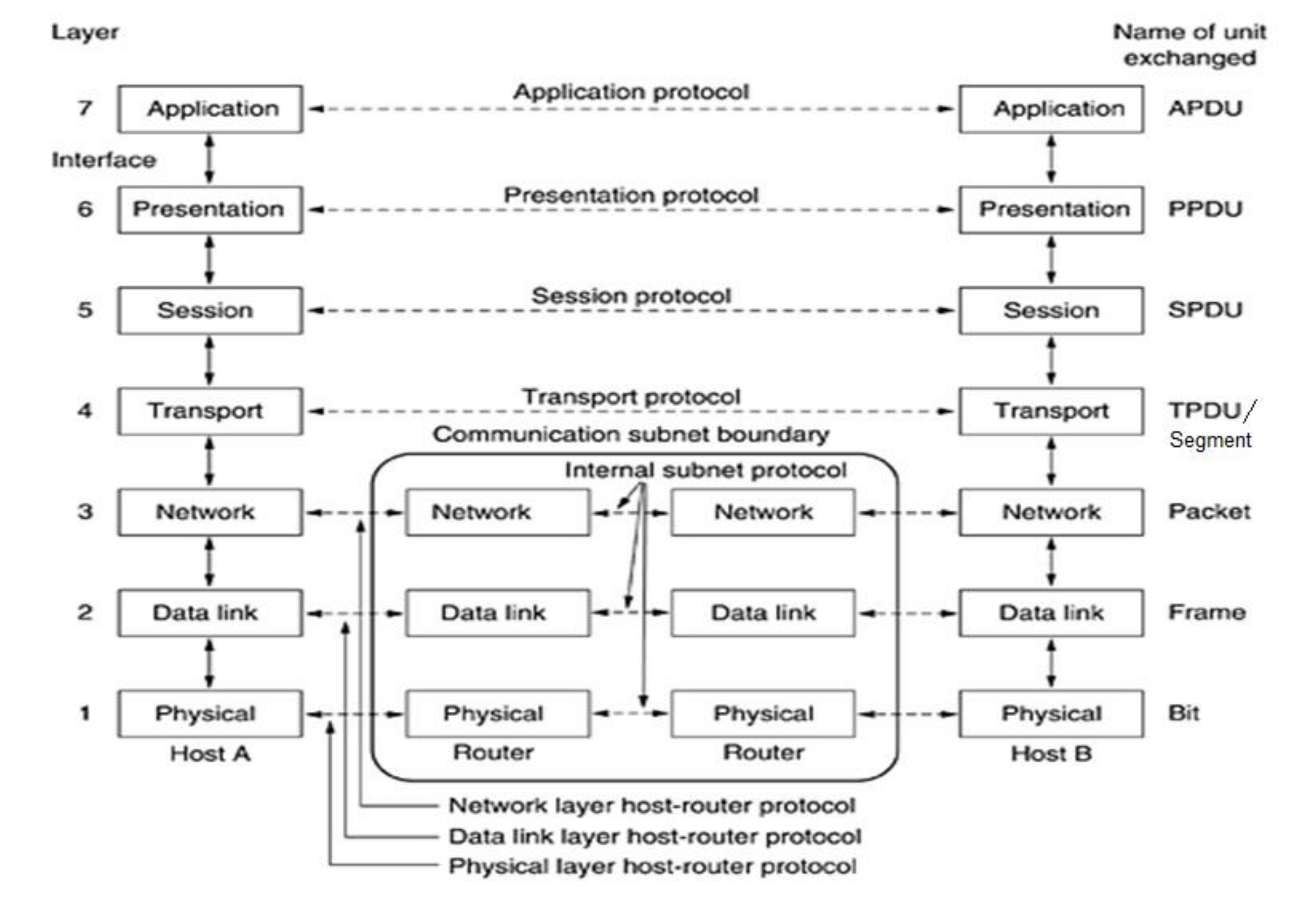

Layer
5
4
3
2
1
M
Layer 5 protocol
M
Layer 5 Data Unit
H_4 M
Layer 4 protocol
H_4 M
Layer 4 Data Unit
H_3 H_4 M_1
H_3 M_2
Layer 3 protocol
H_3 H_4 M_1
H_3 M_2
Layer 3 Data Unit
H_2 H_3 H_4 M_1 T_2
H_2 H_3 M_2 T_2
Layer 2 protocol
H_2 H_3 H_4 M_1 T_2
H_2 H_3 M_2 T_2
Layer 2 Data Unit
BITS
BITS
Layer 1 Data Unit
Source machine
Destination machine

ISO-OSI Reference Model / Open Systems Interconnection(OSI) Model

Principles in Design of OSI Model:

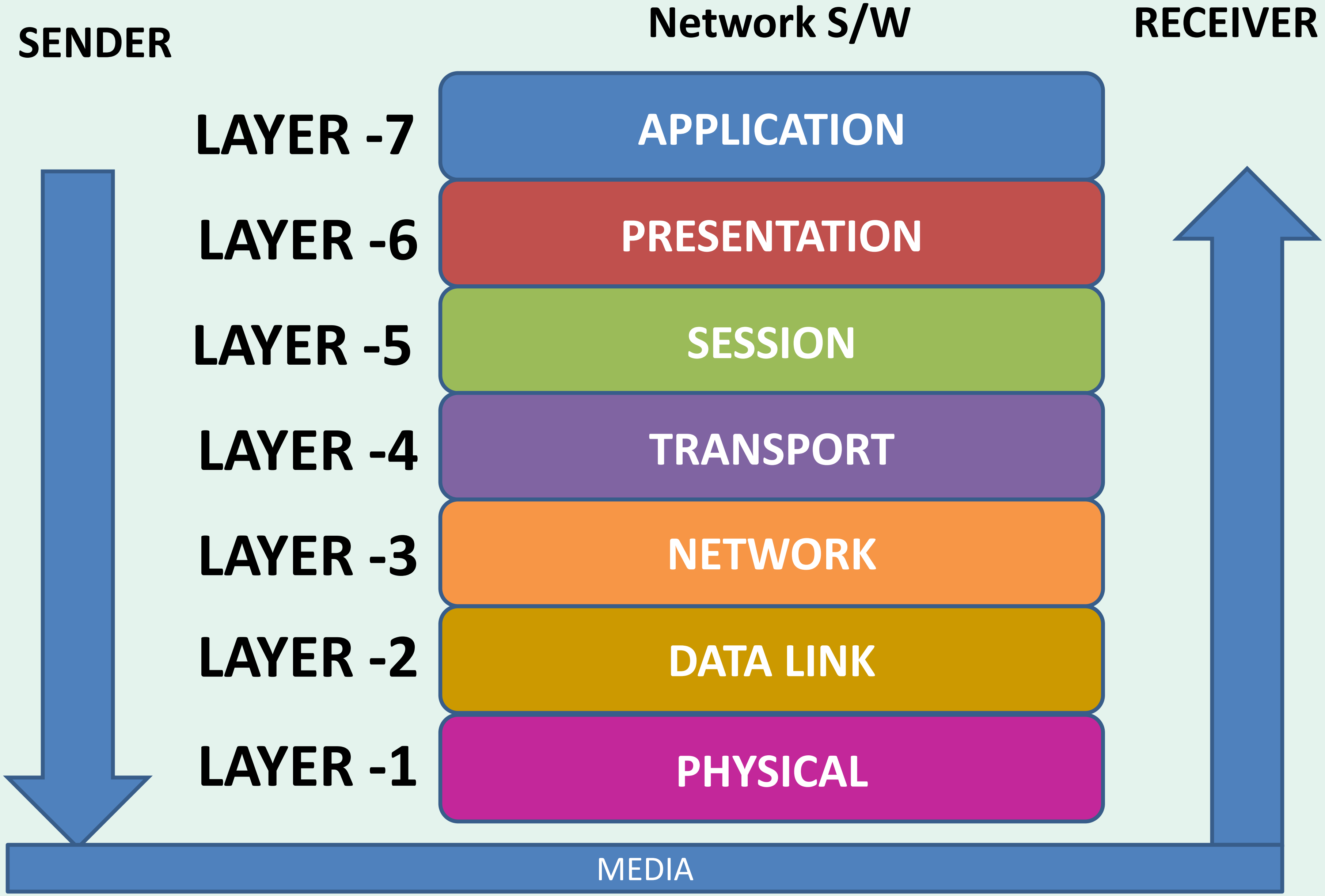
- Layered Architecture
- A layer should be created where a different abstraction is needed.
- The number of layers should be large enough that distinct functions need not be thrown together
- Order of functionality is defined
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- Encapsulation

- OSI Model has 7 Layers



Mnemonic: Please Do Not Throw Sausage Pizza Away (OR) All People Seem To Need Data Processing

OSI Model



SENDER

Network S/W

RECEIVER

LAYER -7 APPLICATION

LAYER -6 PRESENTATION

LAYER -5 SESSION

LAYER -4 TRANSPORT

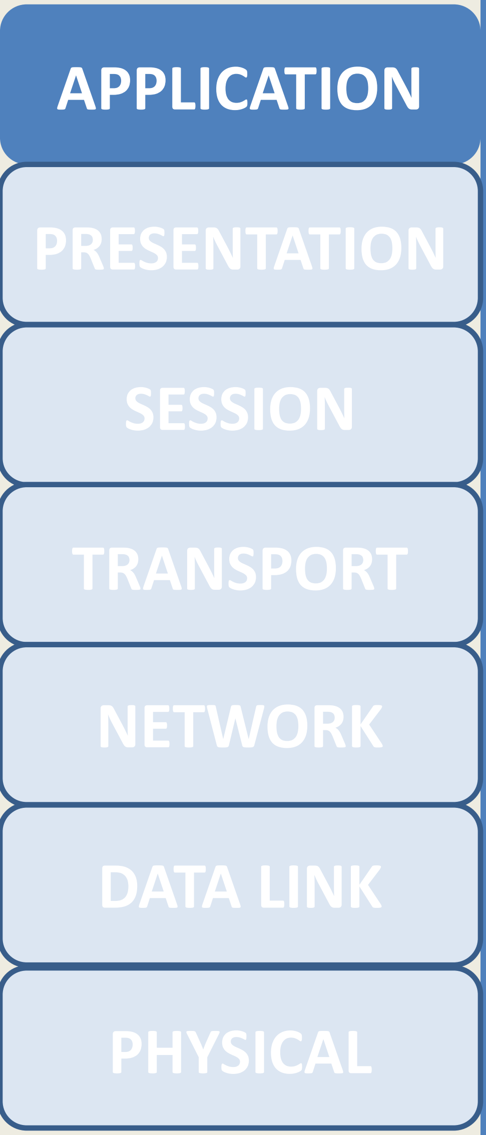
LAYER -3 NETWORK

LAYER -2 DATA LINK

LAYER -1 PHYSICAL

MEDIA

OSI MODEL



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

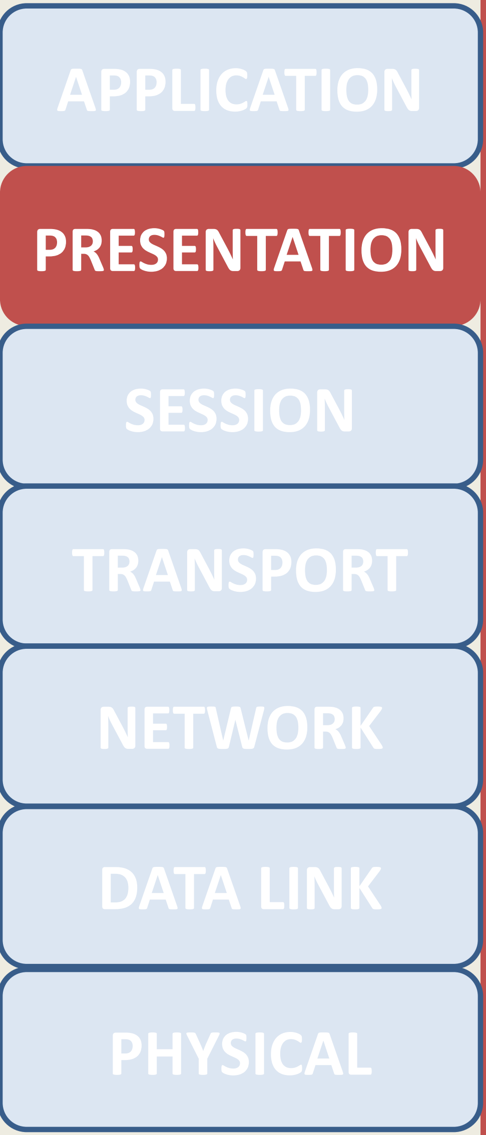
DATA LINK

PHYSICAL

APPLICATION LAYER (LAYER-7)

- It provides user applications with access to network services
- There are several network services
  - Web Services
  - File Transfer and access
  - Remote Login
  - Mail Services
  - News Services
- Data Unit: Application Protocol Data Unit

OSI MODEL



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

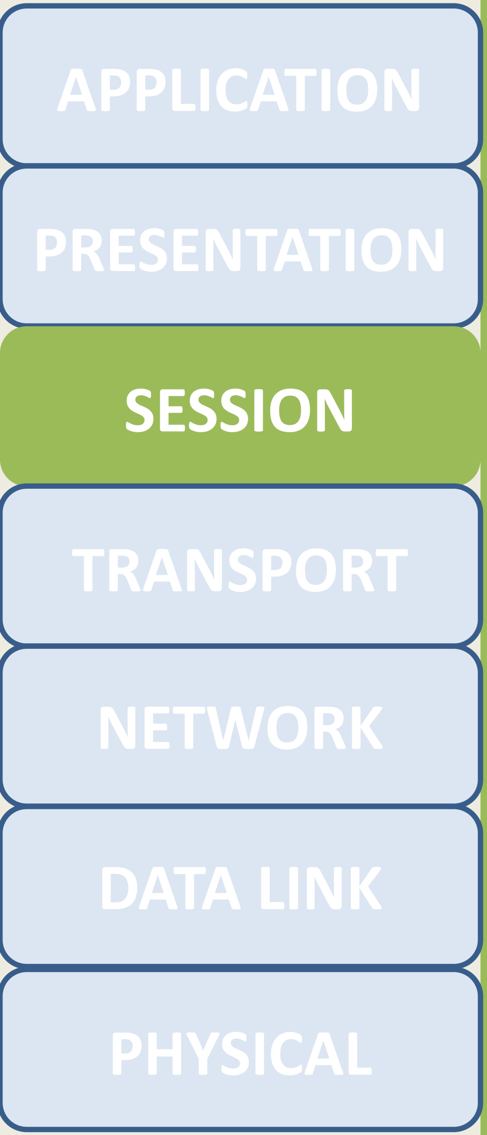
DATA LINK

PHYSICAL

PRESENTATION LAYER (LAYER-6)

- This layer is concerned with syntax and semantics of the information transmitted
- The main functions are:
  - Encoding
  - Compression
  - Encryption
- Data Unit: Presentation Protocol Data Unit

OSI MODEL


APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

DATA LINK

PHYSICAL

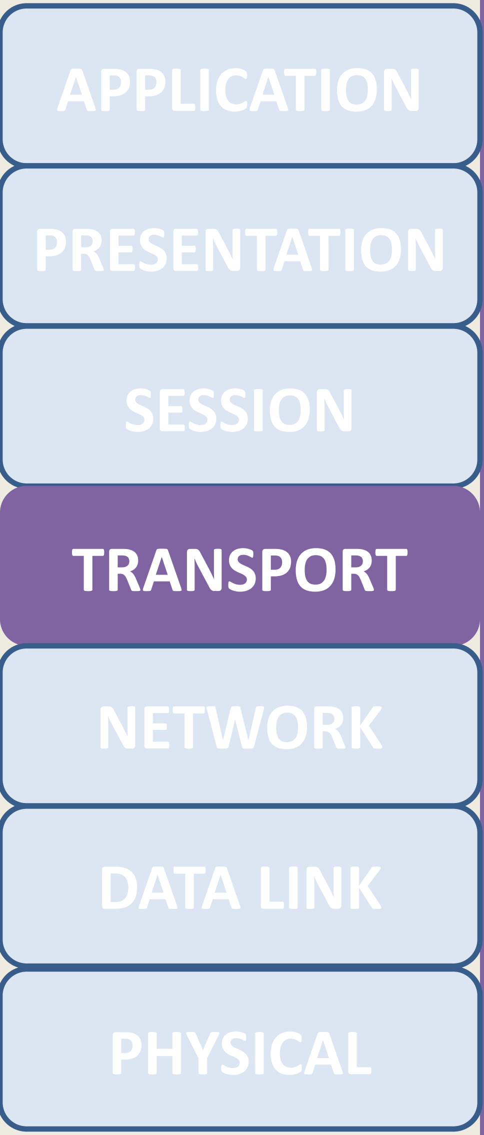
SESSION LAYER (LAYER-5)

- This layer allows users on different machines to establish session between them
- Session establishment is application specific
- The main functions are:
  - Dialog control (Half/Full Duplex)
  - Token management (Who)
  - Synchronization (Time)
- Data Unit: Session Protocol Data Unit

TRANSPORT LAYER (LAYER-4)

- This layer is responsible for **Process to Process** communication
- The main functions are:
  - – Connection control
  - – Port Addressing
  - – Segmentation & Reassembly
  - – Flow Control at segment level
  - – Error control at segment level
  - – Multiplexing & Demultiplexing
- Data Unit: Transport Protocol Data Unit (Segment / User Datagram)

OSI MODEL


APPLICATION

PRESENTATION

SESSION

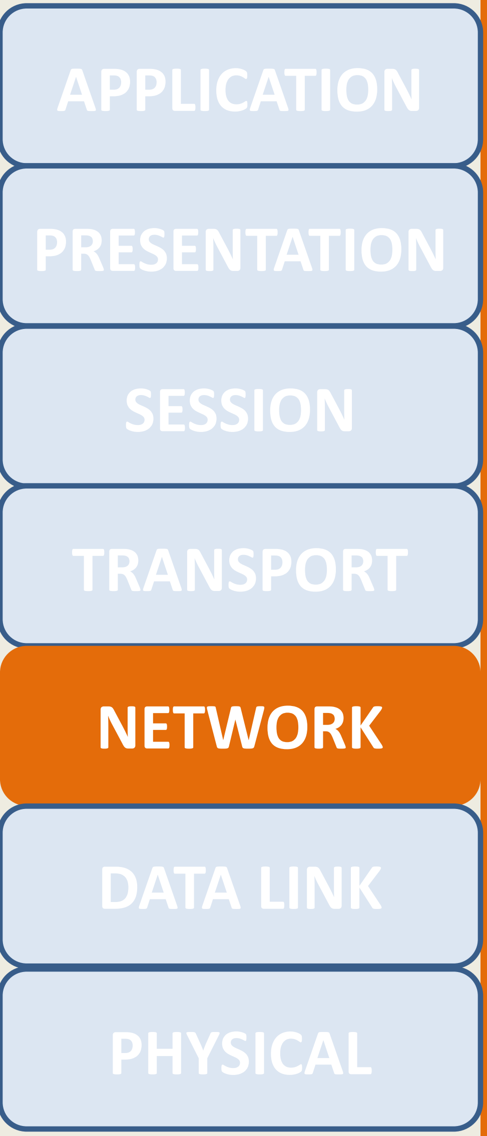
TRANSPORT

NETWORK

DATA LINK

PHYSICAL

OSI MODEL



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

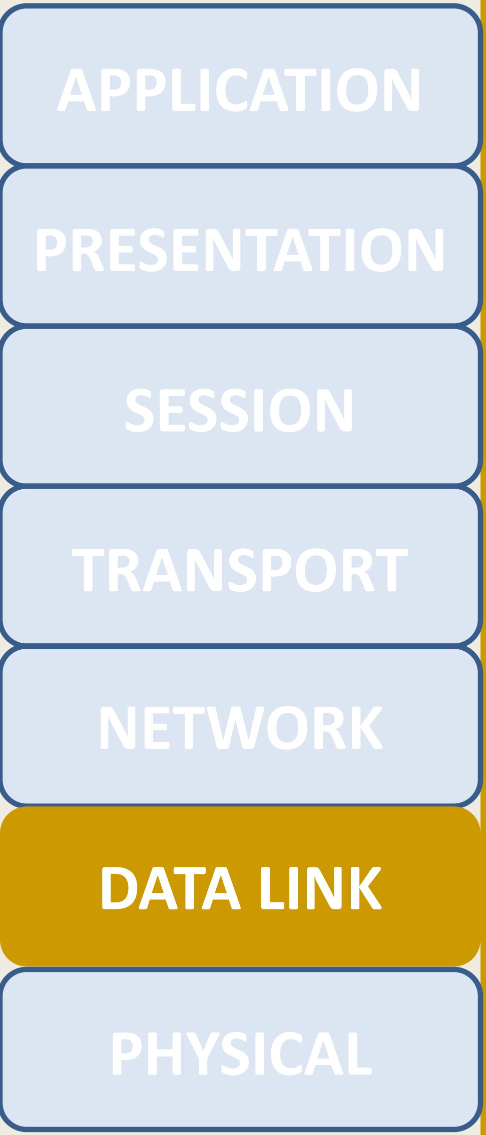
DATA LINK

PHYSICAL

NETWORK LAYER (LAYER-3)

- This layer is responsible for **End to End** delivery.
- Mainly relies on communication subnet
- The main functions are:
  - Logical Addressing
  - Dividing data into Packets/Datagrams
  - Routing
  - Congestion Control
- Data Unit: Packet / Datagram

OSI MODEL



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

DATA LINK

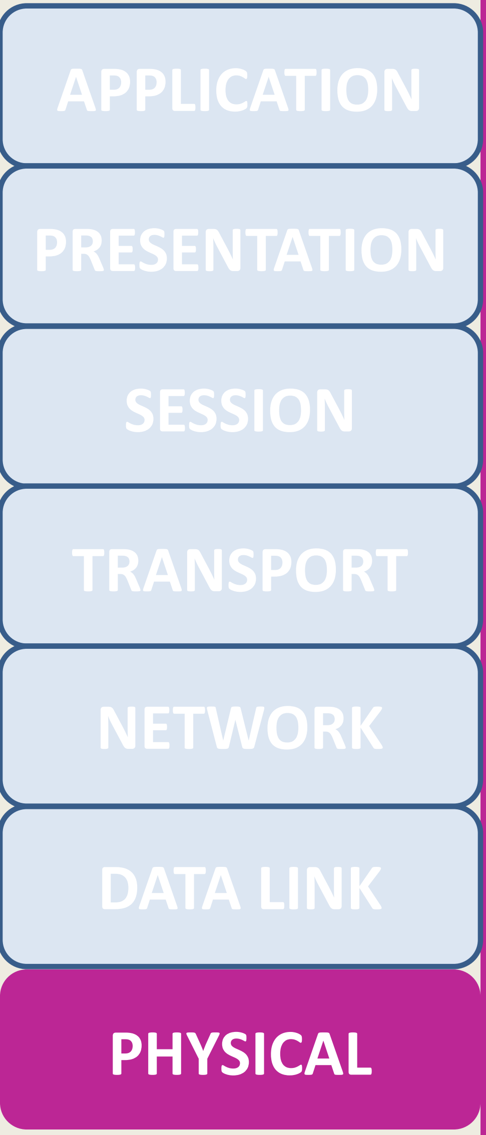
PHYSICAL

DATALINK LAYER (LAYER-2)

- This layer is responsible for Hop to Hop delivery.
- The main functions are:
  - Physical Addressing
  - Error Control
  - Flow Control at Device Level
  - Access Control
  - Framing
- Data Unit: Frame

PHYSICAL LAYER (LAYER-1)

OSI MODEL



APPLICATION

PRESENTATION

SESSION

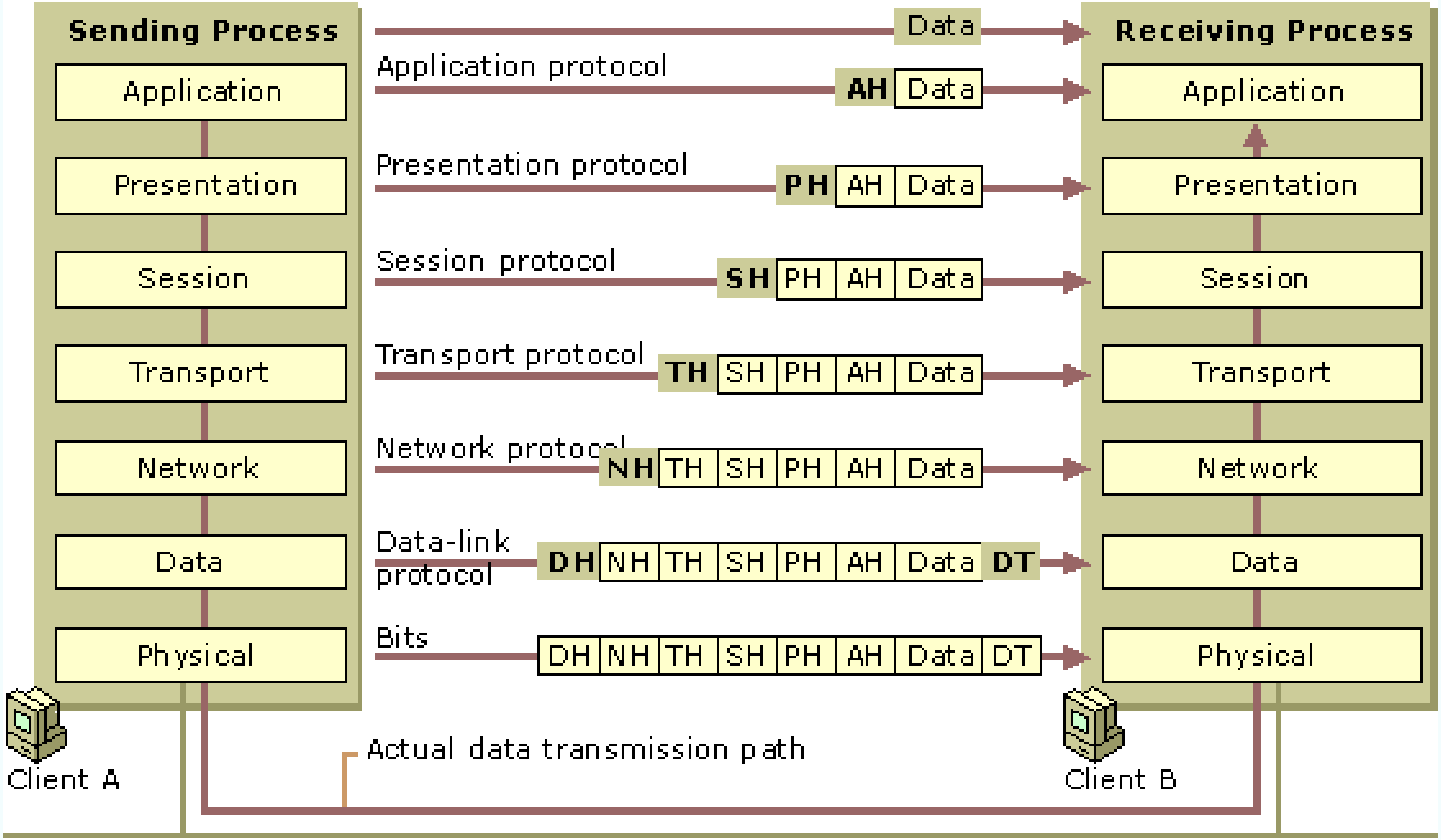
TRANSPORT

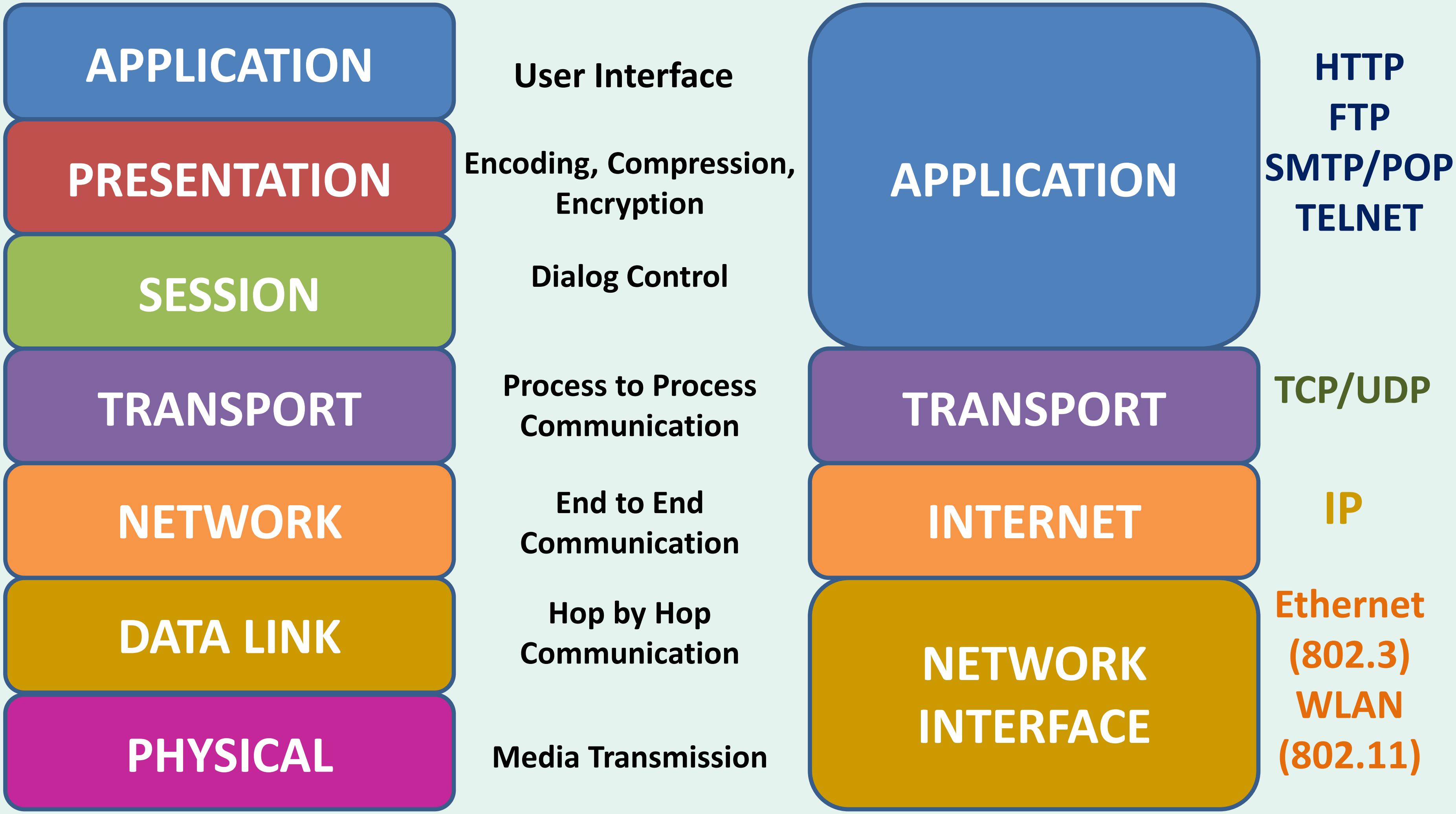
NETWORK

DATA LINK

PHYSICAL

- It is responsible for transmitting bit stream over physical medium (i.e. mechanical & electrical specifications of the media)
- The main functions are:
  - – Physical characteristics of media
  - – Representation of Bits
  - – Data transmission rate
  - – Synchronization of Bits
- Data Unit: Bits


Sending Process
Application
Presentation
Session
Transport
Network
Data
Physical
Data
Application protocol
AH Data
Presentation protocol
PH AH Data
Session protocol
SH PH AH Data
Transport protocol
TH SH PH AH Data
Network protocol
NH TH SH PH AH Data
Data-link protocol
DH NH TH SH PH AH Data DT
Bits
DH NH TH SH PH AH Data DT
Receiving Process
Application
Presentation
Session
Transport
Network
Data
Physical
Client A
Client B
Actual data transmission path

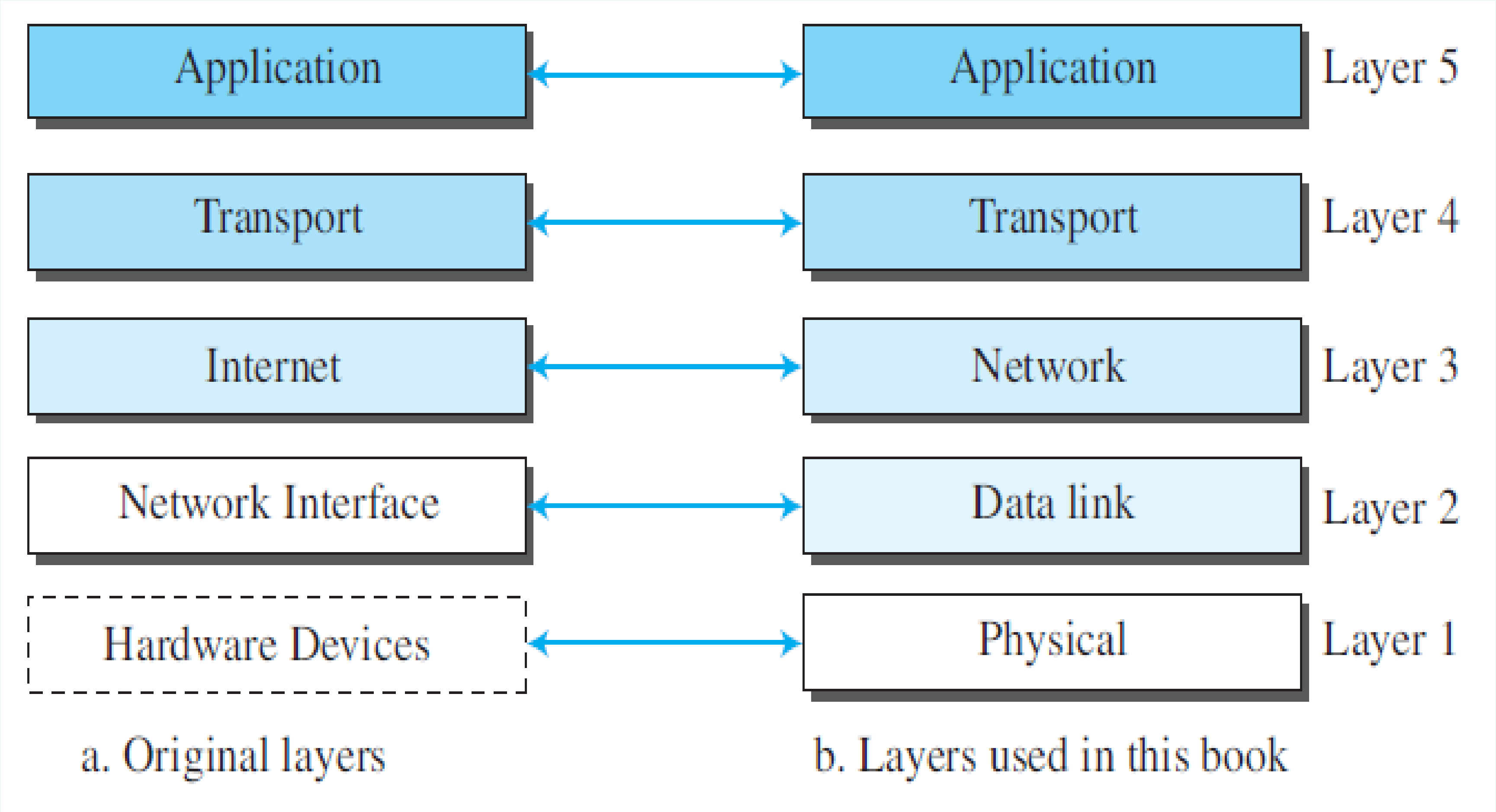


OSI MODEL (Theoretical)	Functionalities	TCP \ IP (Real Time)	Protocols
APPLICATION	User Interface	APPLICATION	HTTP FTP SMTP/POP TELNET
PRESENTATION	Encoding, Compression, Encryption		
SESSION	Dialog Control		
TRANSPORT	Process to Process Communication	TRANSPORT	TCP/UDP
NETWORK	End to End Communication	INTERNET	IP
DATA LINK	Hop by Hop Communication	NETWORK INTERFACE	Ethernet (802.3) WLAN (802.11)
PHYSICAL	Media Transmission		

TCP\IP Protocol Suite

- Transmission Control Protocol / Internet Protocol
- Used in the Internet today
- Initially developed as 4 layers but today perceived as 5 layers
- Each Intermediary device is involved with a set of layers depending on the role of the device in the network.
- Functionalities are similar to OSI Model

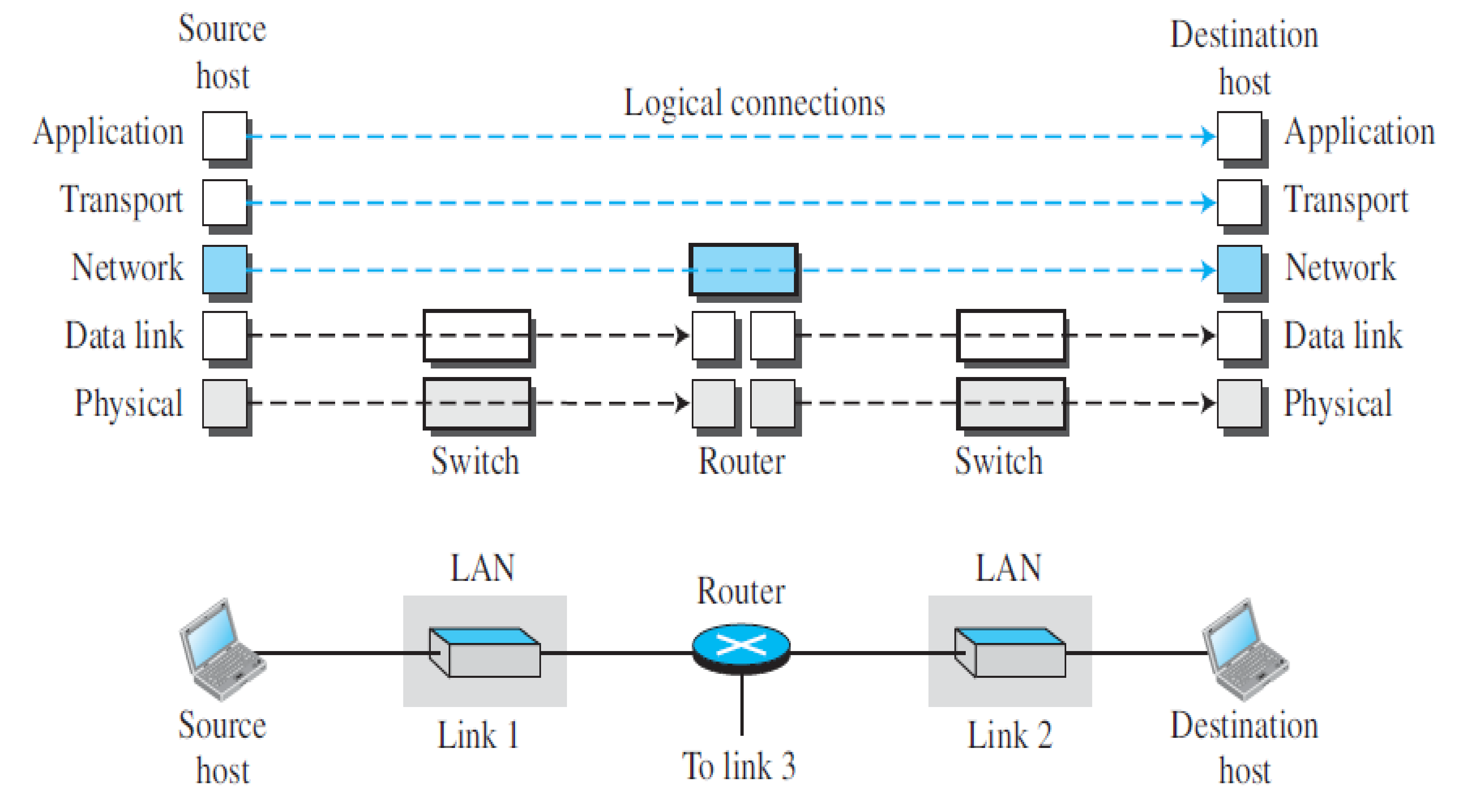
Layers in TCP/IP



a. Original layers

b. Layers used in this book

Logical Connection between Layers



Application Layer

- The logical connection between the two application layers is end to end.
- Communication at the application layer is between two processes
- To communicate, a process sends a request to the other process and receives a response.
  - Hypertext Transfer Protocol (HTTP) → Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP)→ e-mail
  - File Transfer Protocol (FTP) → Transferring files
  - Terminal Network (TELNET) → remote access
  - Simple Network Management Protocol (SNMP) → Managing Network
  - Domain Name System (DNS) → Finding Network layer Address
  - Internet Group Management Protocol(IGMP) → Groups

Transport layer

- The logical connection between the two transport layers is end to end.
- Giving services to application layer
- Services are either Connection Oriented or Connection less (Based on the Application)
- Transmission Control Protocol (TCP)→ Connection Oriented
  - Flow control , Error control, congestion control
- User Datagram Protocol (UDP) → connectionless protocol
- Stream Control Transmission Protocol (SCTP) → One to Many applications

Network Layer

- The logical connection between two network layers is end-to-end.
- Responsible for Routing i.e. choosing best path for in a network
- Internet Protocol (IP) → Logical addressing
- Internet Control Message Protocol (ICMP) → problems in routing
- Internet Group Management Protocol (IGMP) → managing groups
- Dynamic Host Configuration Protocol(DHCP) → get IP address dynamically
- The Address Resolution Protocol (ARP) → finding link address for a given logical address

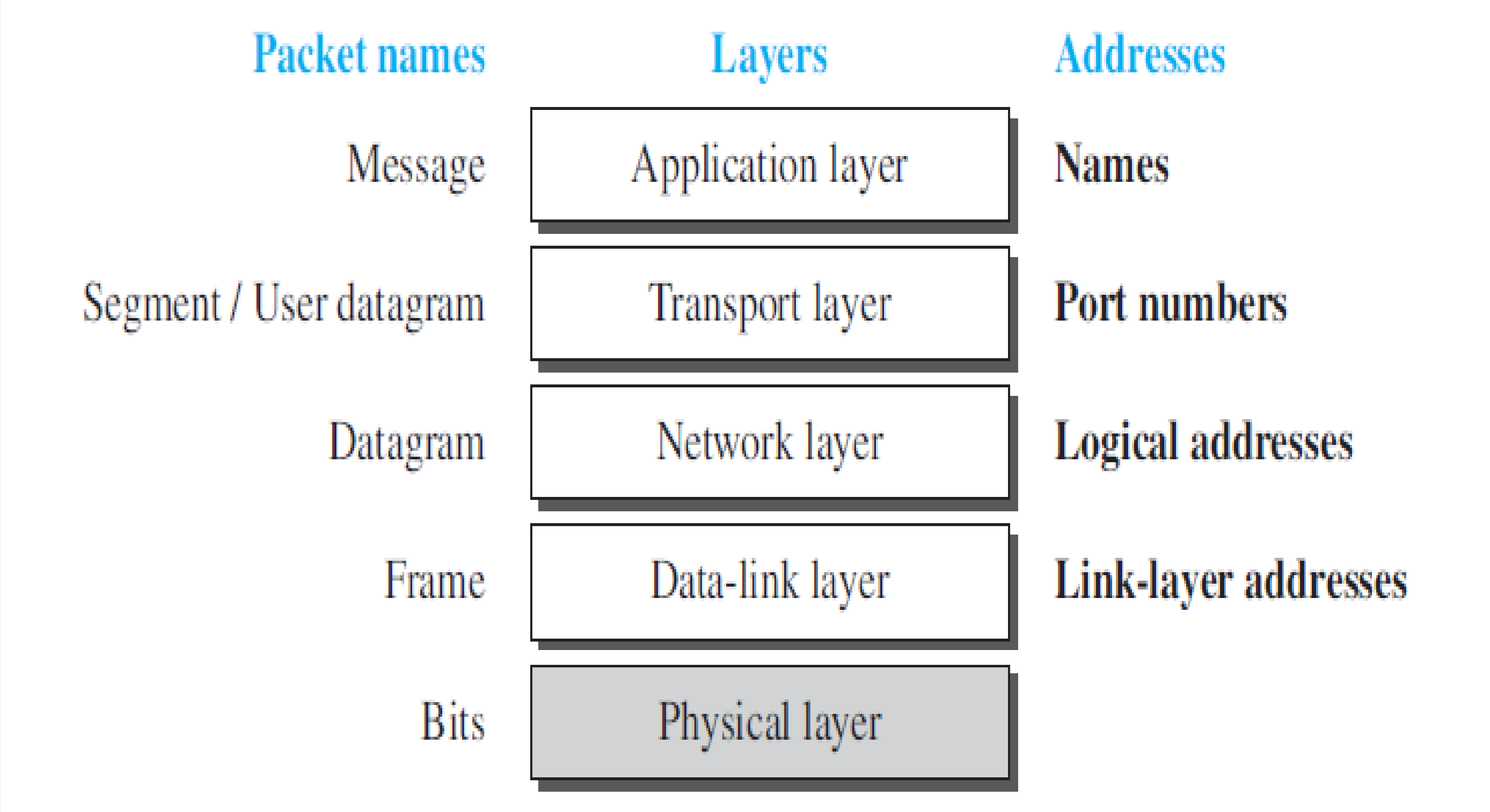
Data link Layer

- The logical connection between two data link layers is hop-to-hop.
- Responsible for link transmission
- Routing select best links from source to destination
- Provides error detection/correction
  - Ethernet → IEEE 802.3 Protocol
  - Wireless LAN→ IEEE 802.11 Protocol
  - Token Ring → IEEE 802.5 Protocol
  - Token Bus → IEEE 802.4 Protocol
  - Bluetooth → IEEE 802.15 Protocol

Physical Layer

- The logical connection between two physical layers is hop-to-hop.
- The physical layer is responsible for carrying individual bits in a frame across the link
- The bits received in a frame from the data-link layer are transformed and sent through the transmission media
- The logical unit between two physical layers in two devices is a ‘bits’
- There are several protocols that transform a bit to a signal

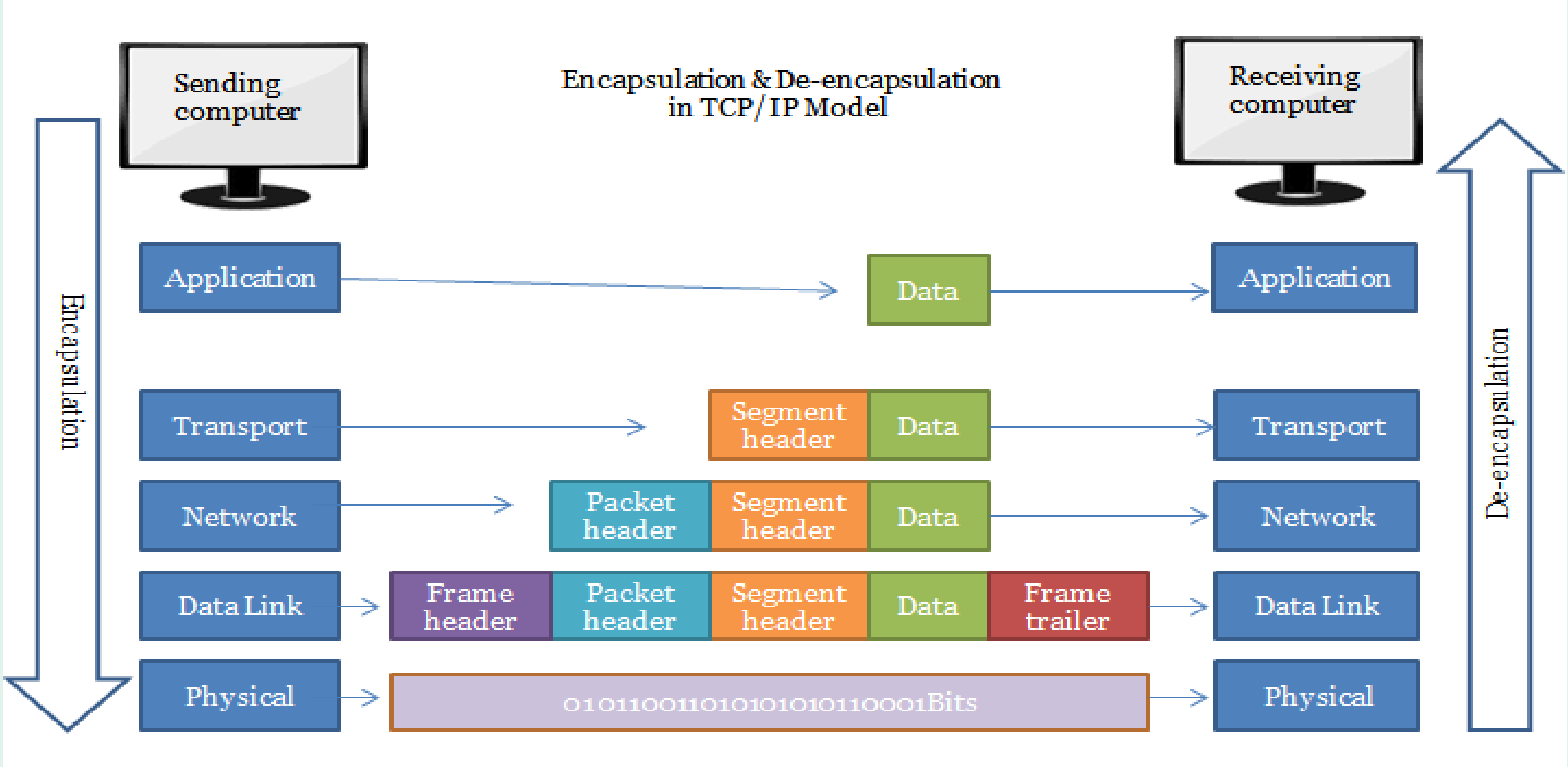
Addressing

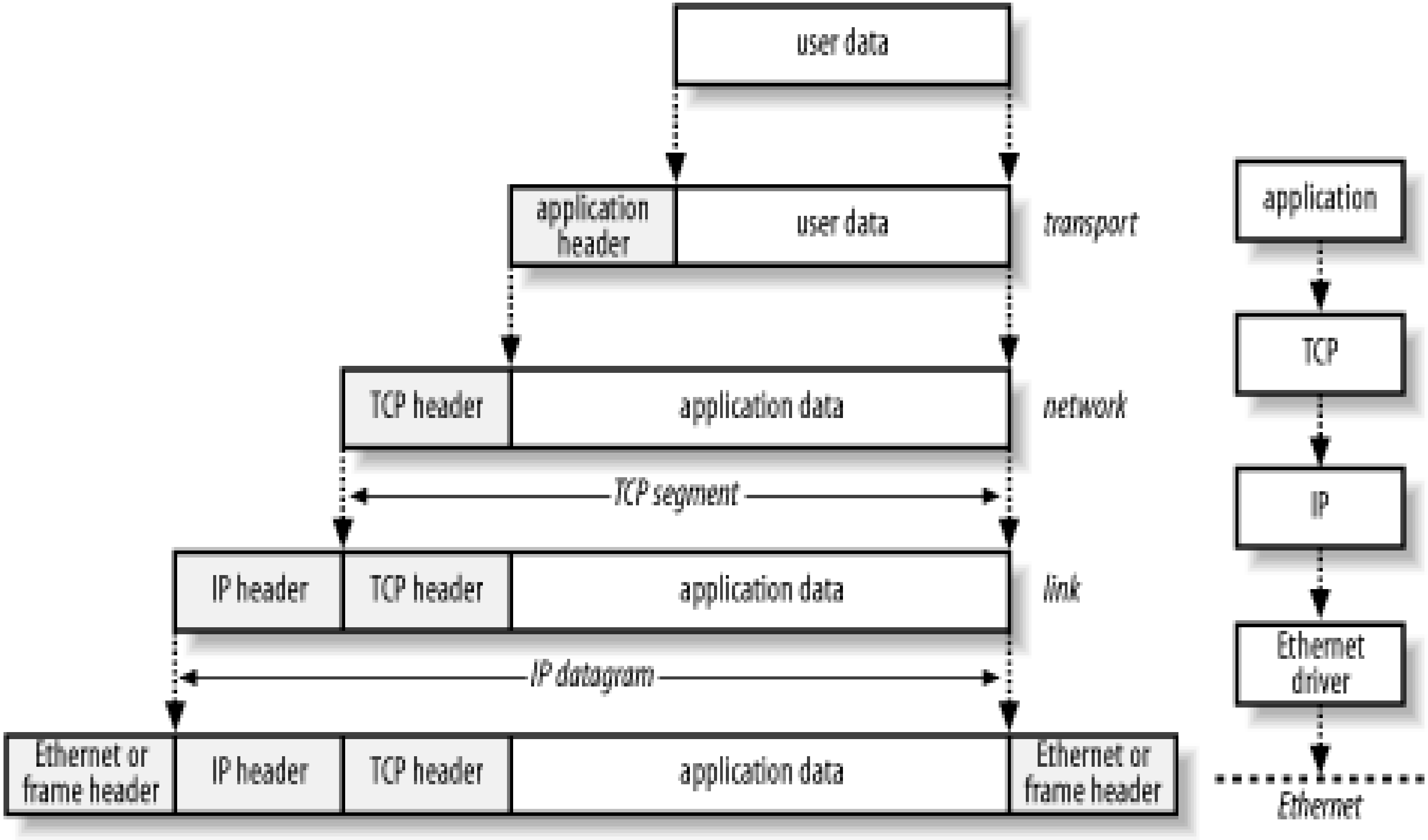


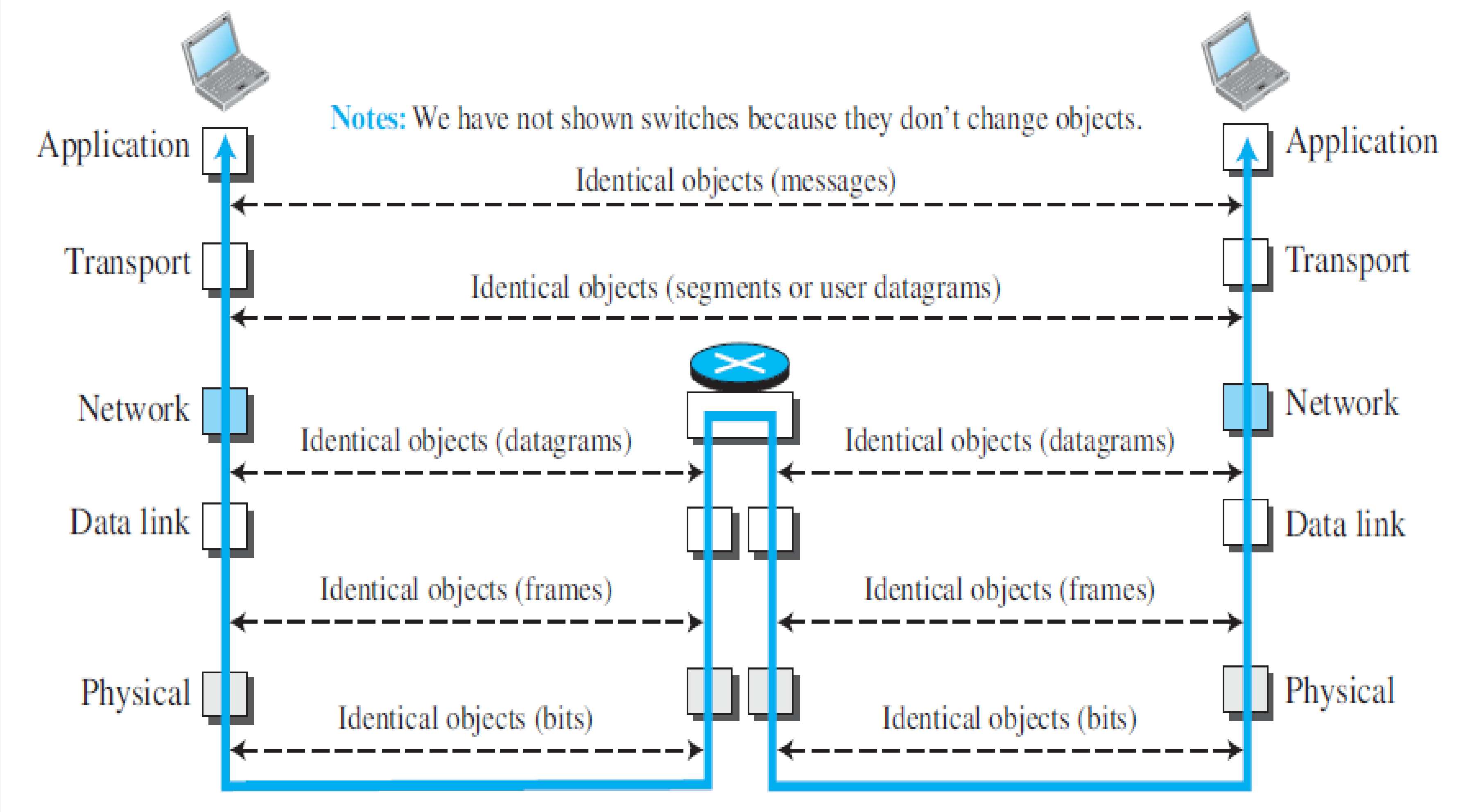
Packet names	Layers	Addresses
Message	Application layer	Names
Segment / User datagram	Transport layer	Port numbers
Datagram	Network layer	Logical addresses
Frame	Data-link layer	Link-layer addresses
Bits	Physical layer	

Encapsulation / Decapsulation

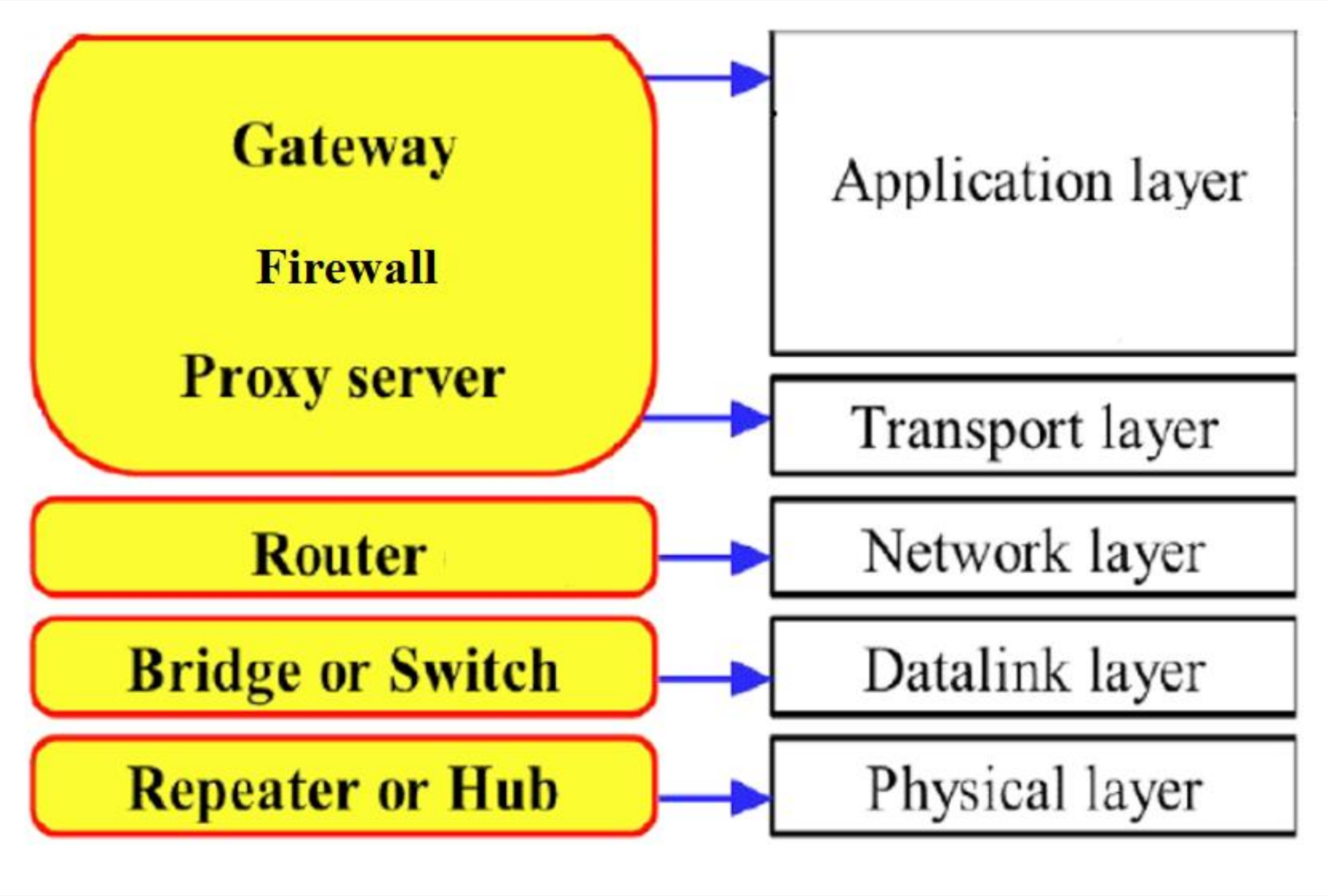
It is used to describe a process of adding / removing headers and trailers around some data.



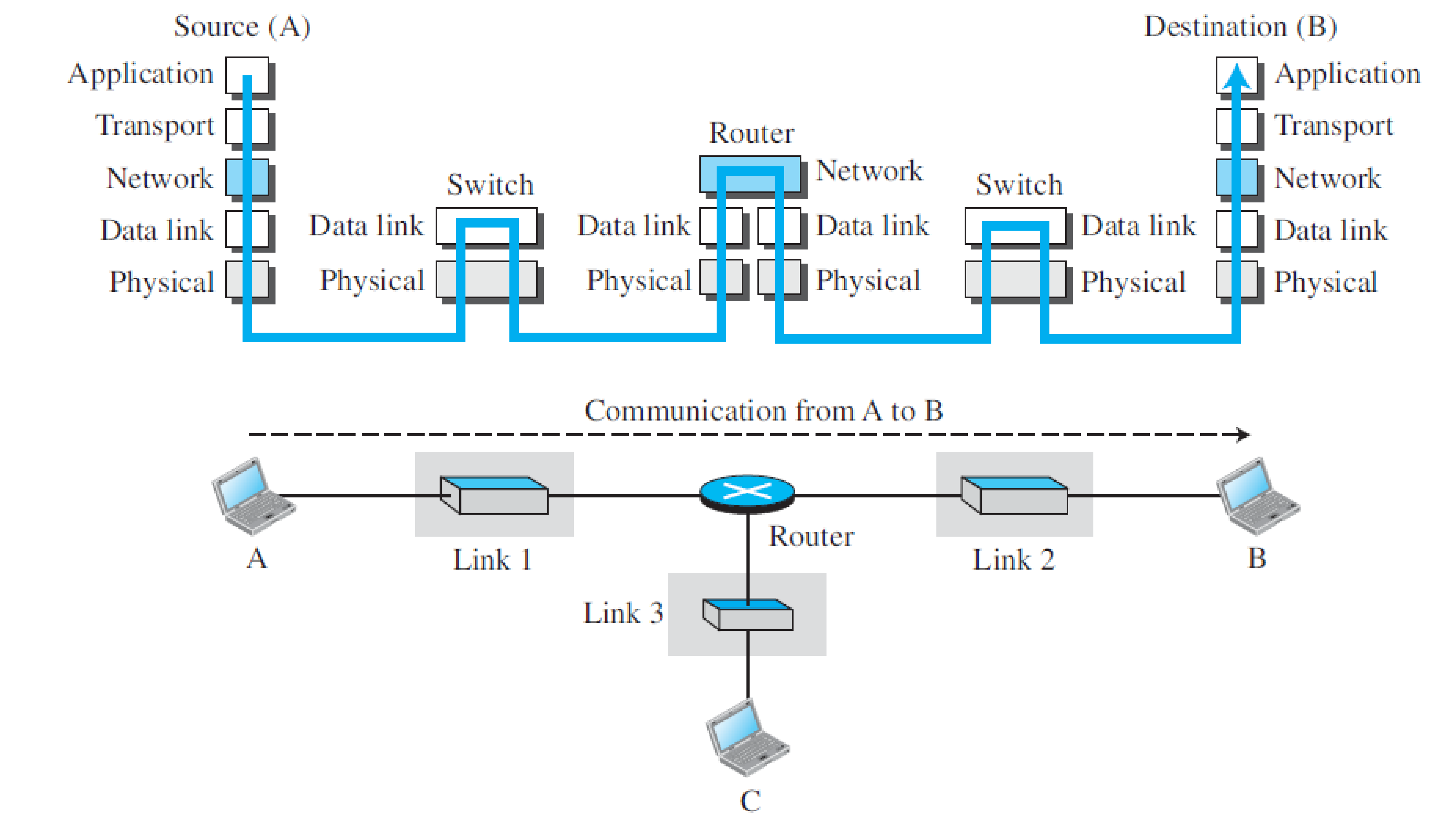

user data
application header
user data
transport
TCP header
application data
network
TCP segment
IP header
TCP header
application data
link
IP datagram
Ethernet or frame header
IP header
TCP header
application data
Ethernet or frame header
application
TCP
IP
Ethernet driver
Ethernet

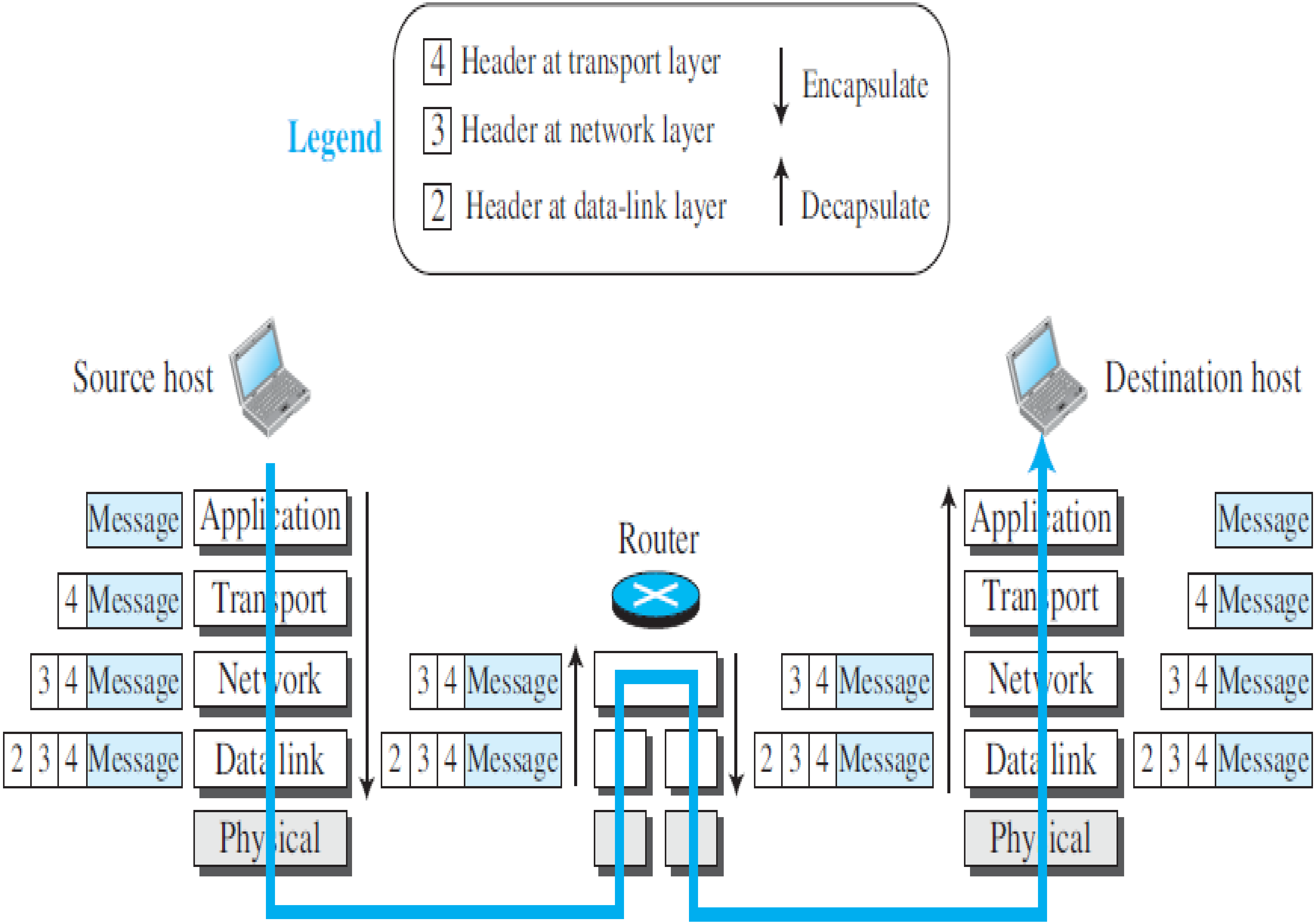

Notes: We have not shown switches because they don't change objects.
Application
Application
Identical objects (messages)
Transport
Transport
Identical objects (segments or user datagrams)
Network
Network
Identical objects (datagrams)
Identical objects (datagrams)
Data link
Data link
Identical objects (frames)
Identical objects (frames)
Physical
Physical
Identical objects (bits)
Identical objects (bits)

Intermediary Devices



Communication through Internet





Legend

4 Header at transport layer

3 Header at network layer

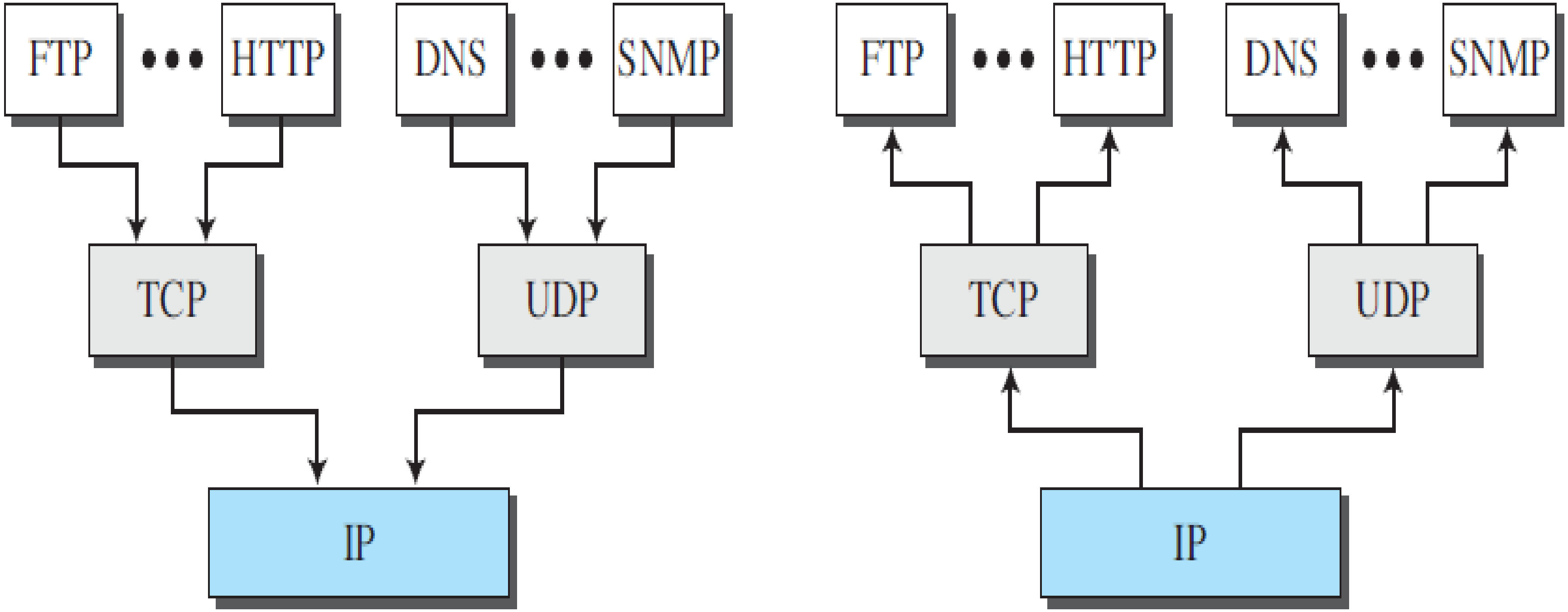
2 Header at data-link layer

Encapsulate

Decapsulate

Multiplexing / Demultiplexing

- Process of simultaneously sending data of several upper layer protocols together



a. Multiplexing at source

b. Demultiplexing at destination

OSI v/s TCP/IP

- The OSI has seven layers while the TCP/IP has four layers.
- OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.
- OSI model distinguishes the three concepts, namely: services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three.
- OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
- In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.

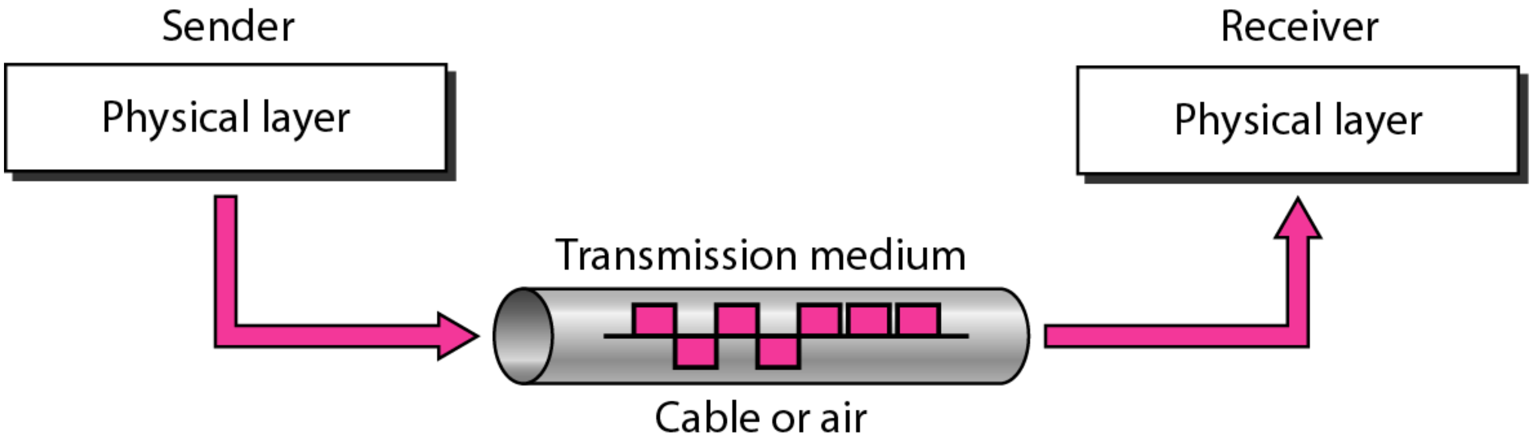
Lack of OSI Model’s Success

- OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot.
- Some layers in the OSI model were never fully defined i.e. Presentation & Session Layer
- It did not show a high enough level of performance to entice the Internet authority

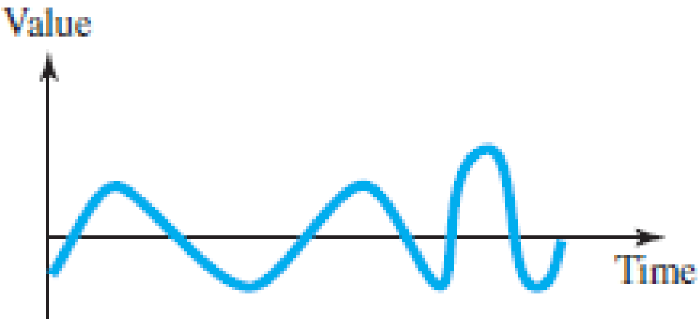
Physical Layer

Transmission Media

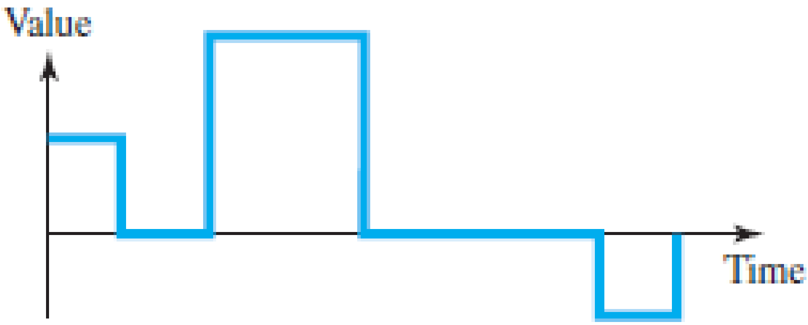
- Transmission media are actually located below the physical layer and are directly controlled by the physical layer.
- A **transmission medium** can be broadly defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable, or fiber-optic cable.
- The information is usually a signal that is the result of a conversion of data from another form.



- Data can be analog or digital.
  - **Analog data** refers to information that is continuous; For example, Analog data, such as the sounds made by a human voice, take on continuous values.
  - **Digital data** refers to information that has discrete states. For example, data are stored in computer memory in the form of 0s and 1s.
- Signals can be either analog or digital.
  - An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path.
  - A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.

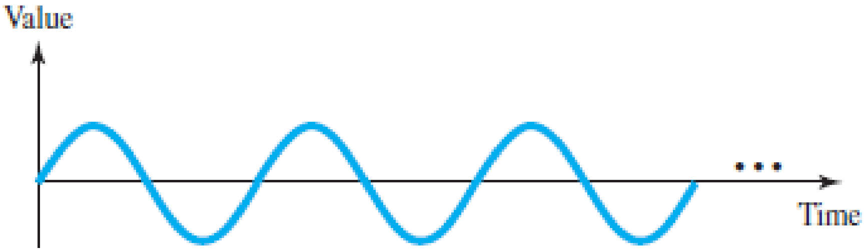


a. Analog signal



b. Digital signal

- Both analog and digital signals can take one of two forms: *periodic* or *nonperiodic*
  - A **periodic signal** completes a pattern within a measurable time frame, called a **period,** and repeats that pattern over subsequent identical periods.
  - A **nonperiodic signal** changes without exhibiting a pattern or cycle that repeats over time.
- In data communications, we commonly use periodic analog signals and nonperiodic digital signals

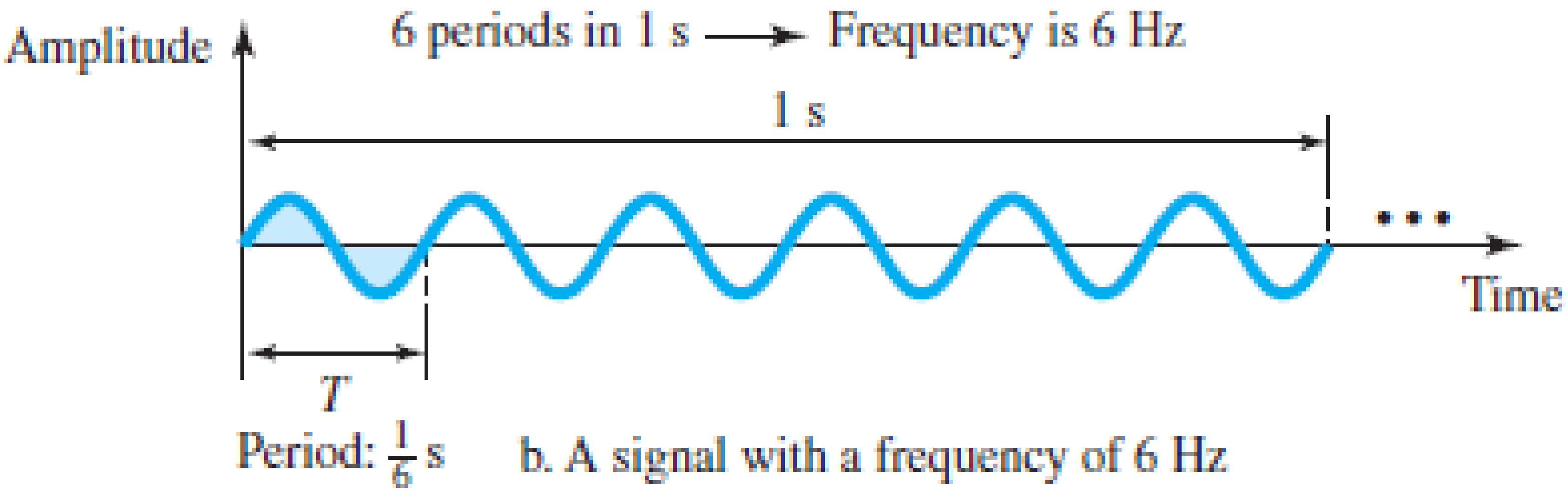


Analog Signal

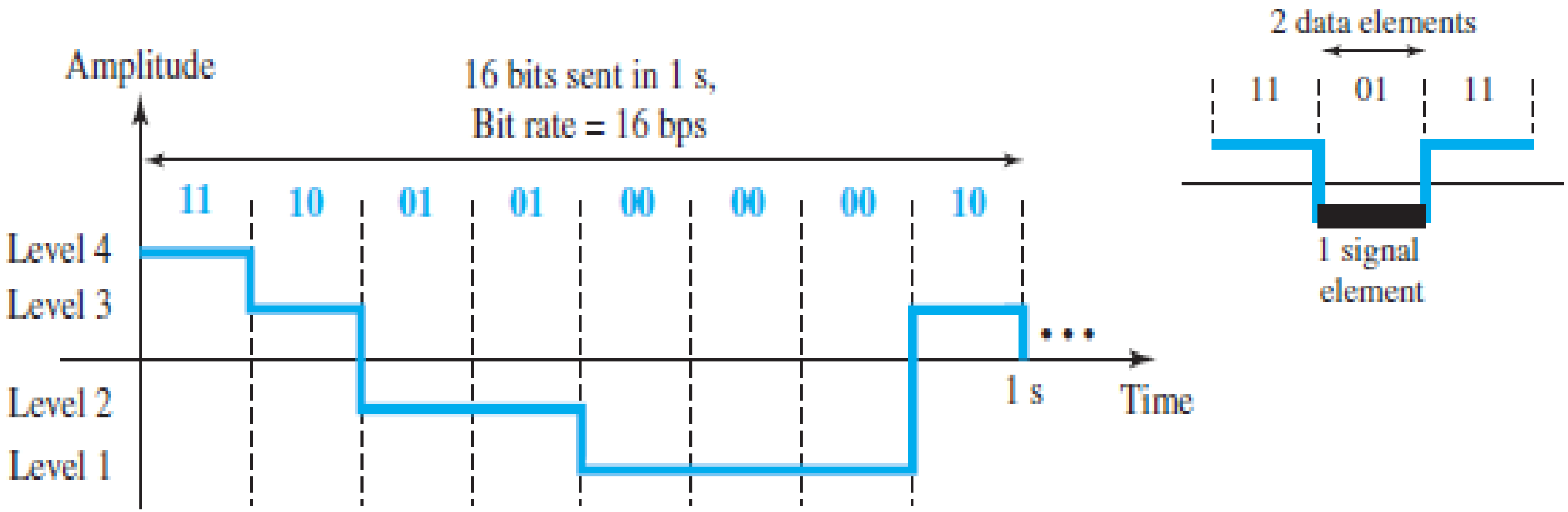
- Sine Wave
- Cycle
- Period
- *Peak Amplitude*
- *Frequency*
- *Phase*
- Wavelength
- Composite Signals
- Bandwidth

Digital Signal

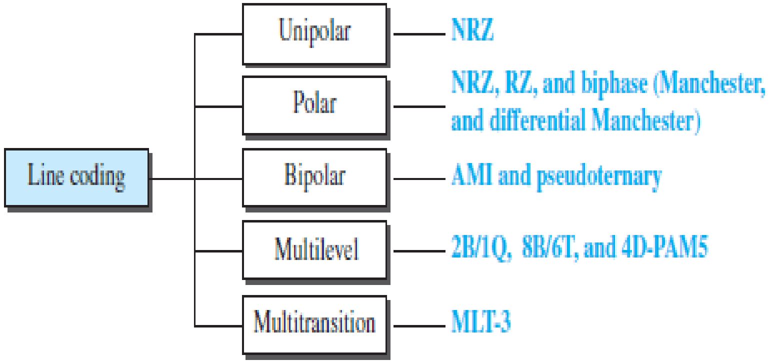
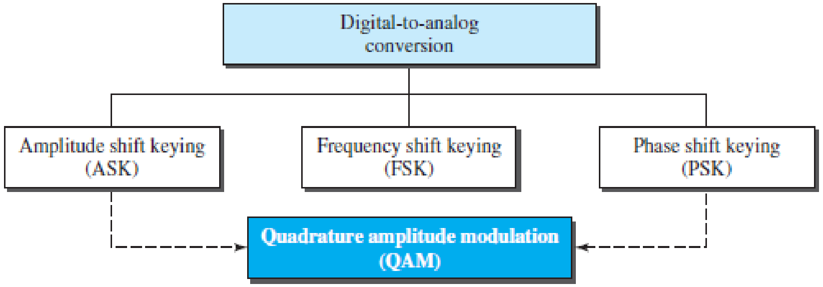
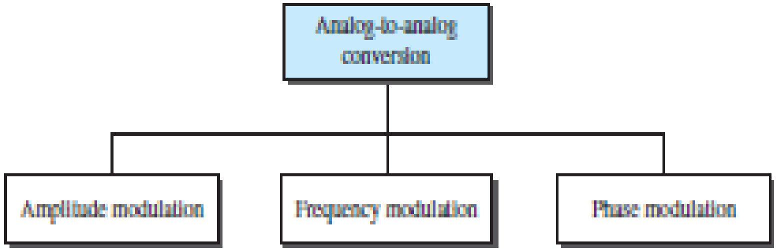
- Discrete Period
- Level
- Signal Element
- Signal Rate
- Data Element
- Bit duration
- *Bit rate*
- Bit length
- Bandwidth(Data Rate)



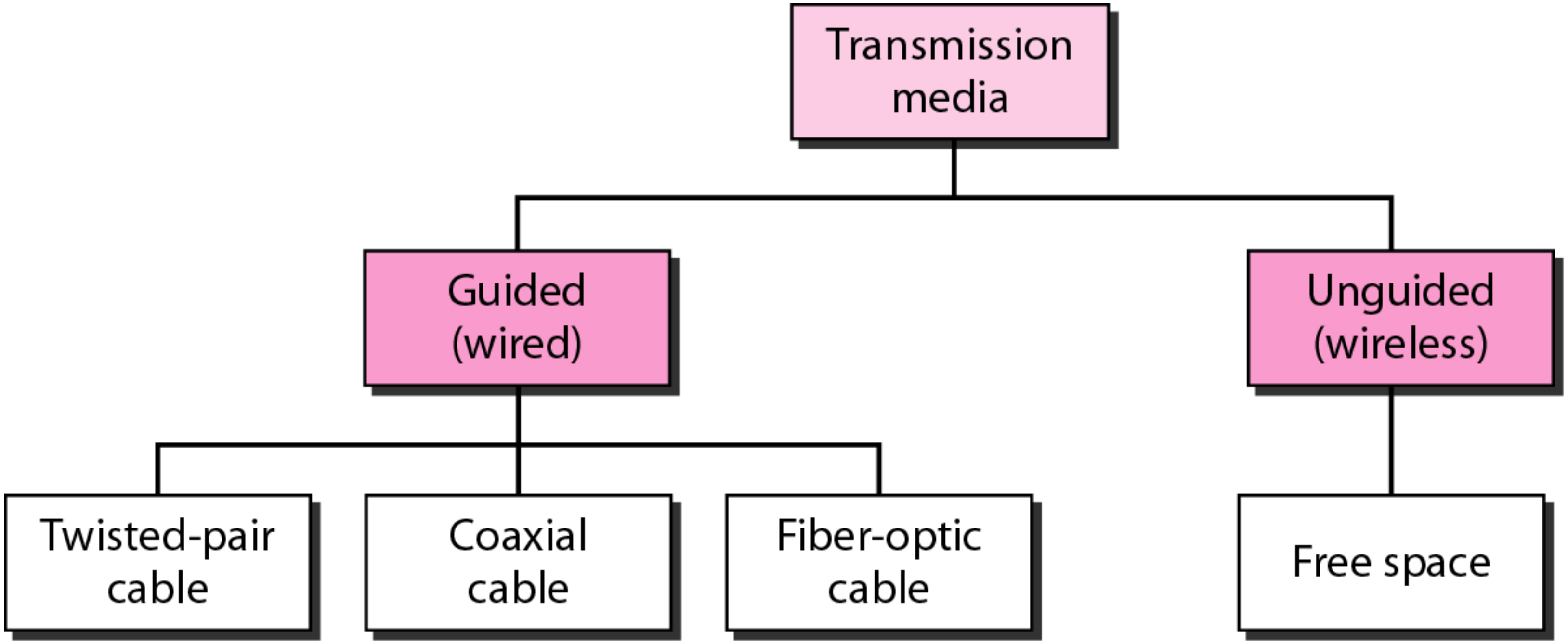
b. A signal with a frequency of 6 Hz



b. A digital signal with four levels

	Digital Signal	Analog Signal
Digital Data	 Line coding Unipolar — NRZ Polar — NRZ, RZ, and biphase (Manchester, and differential Manchester) Bipolar — AMI and pseudoternary Multilevel — 2B/1Q, 8B/6T, and 4D-PAM5 Multitransition — MLT-3	 Digital-to-analog conversion Amplitude shift keying (ASK) Frequency shift keying (FSK) Phase shift keying (PSK) Quadrature amplitude modulation (QAM)
Analog Data	**Pulse Code Modulation (PCM)** **Delta Modulation (DM)**	 Analog-to-analog conversion Amplitude modulation Frequency modulation Phase modulation

Classes of Transmission Media



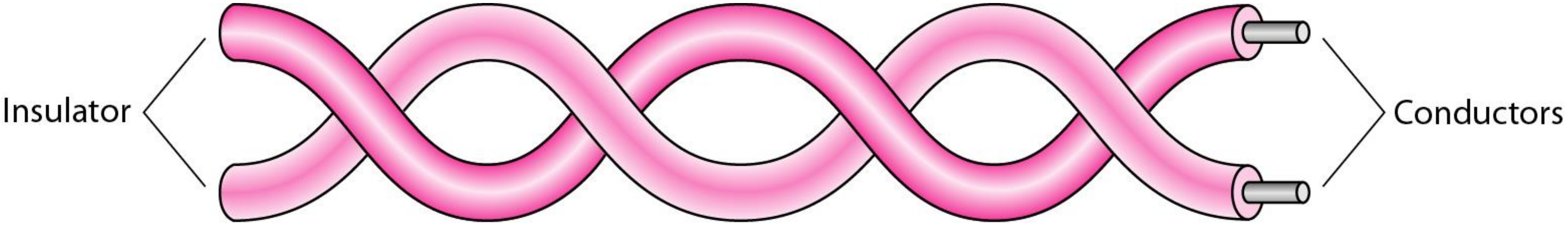
GUIDED MEDIA

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

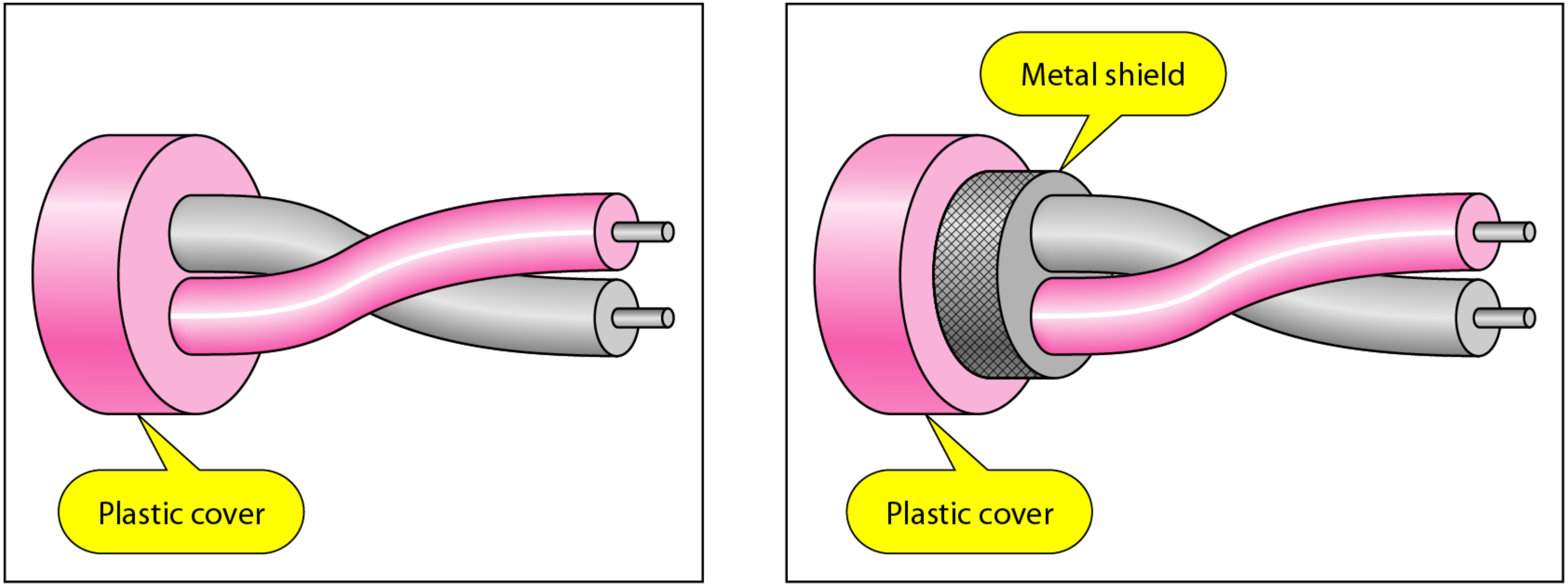
Twisted-Pair Cable
Coaxial Cable
Fiber-Optic Cable

Twisted-pair cable

A twisted pair consists of two conductors (normally copper), each with its own plastic Insulation. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference



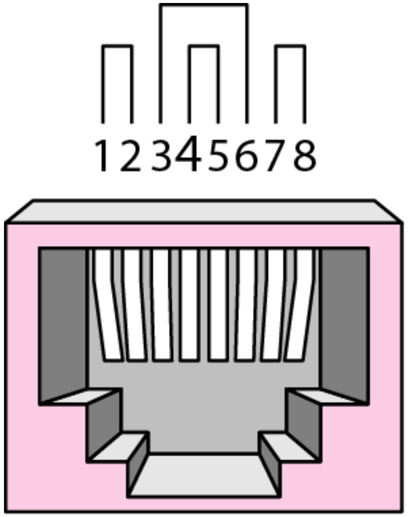
UTP and STP cables



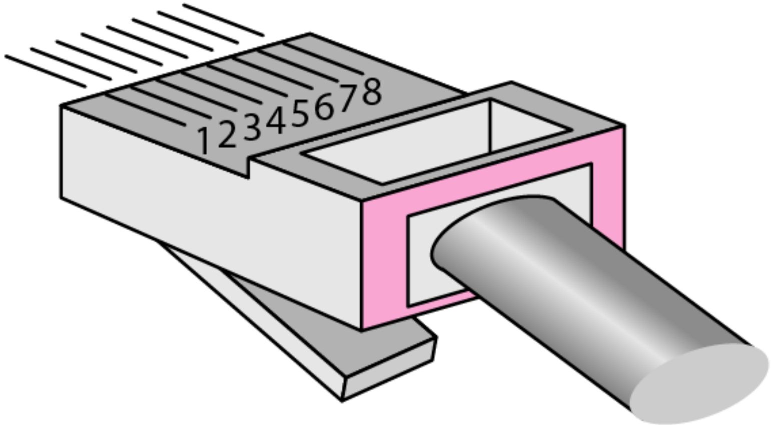
a. UTP

b. STP

UTP connector

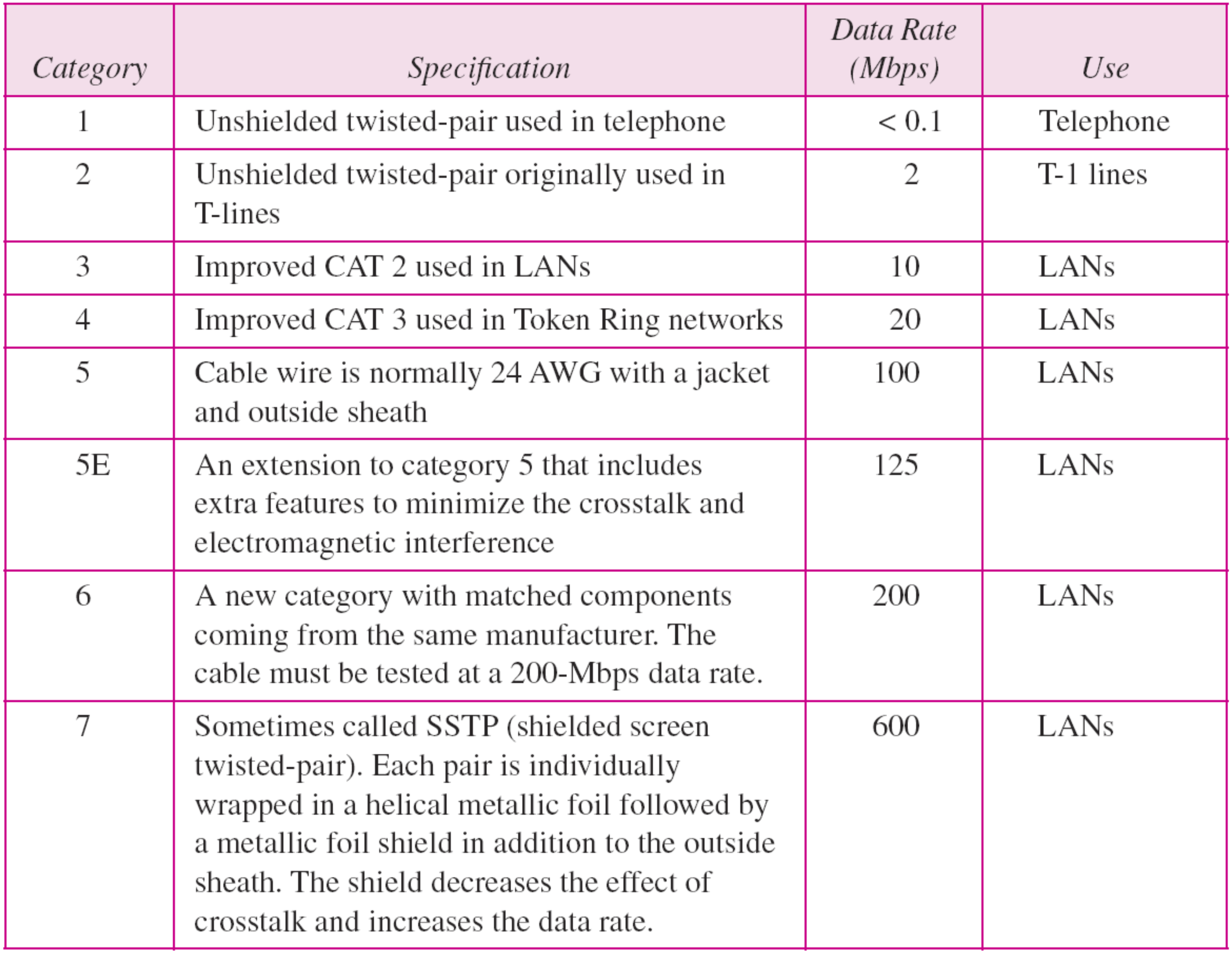


RJ-45 Female



RJ-45 Male

Categories of unshielded twisted-pair cables



Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Twisted Pair performance

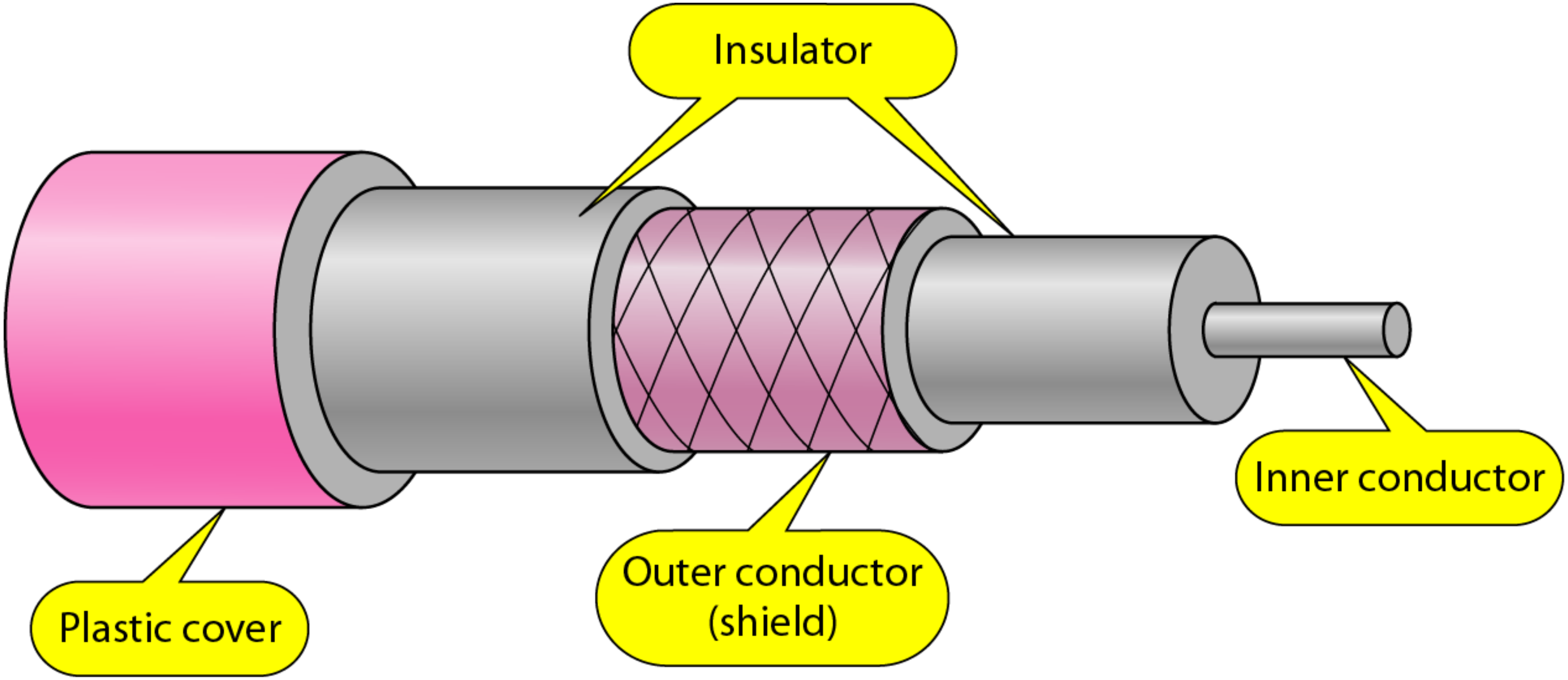
One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance.

Twisted Pair Applications

- Twisted-pair cables are used in telephone lines to provide voice and data channels.
- Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

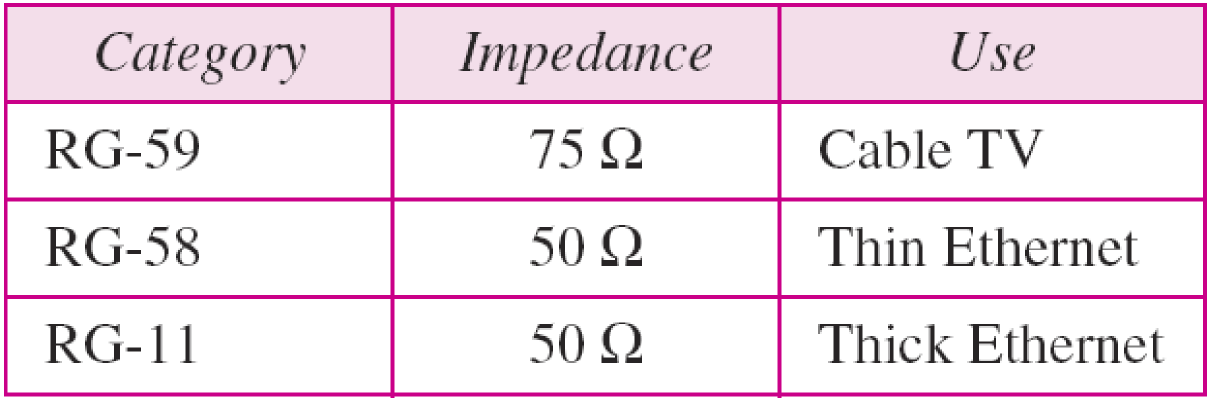
Coaxial cable

Coaxial cable (or *coax*) carries signals of higher frequency ranges than those in twistedpair cable



Categories of coaxial cables

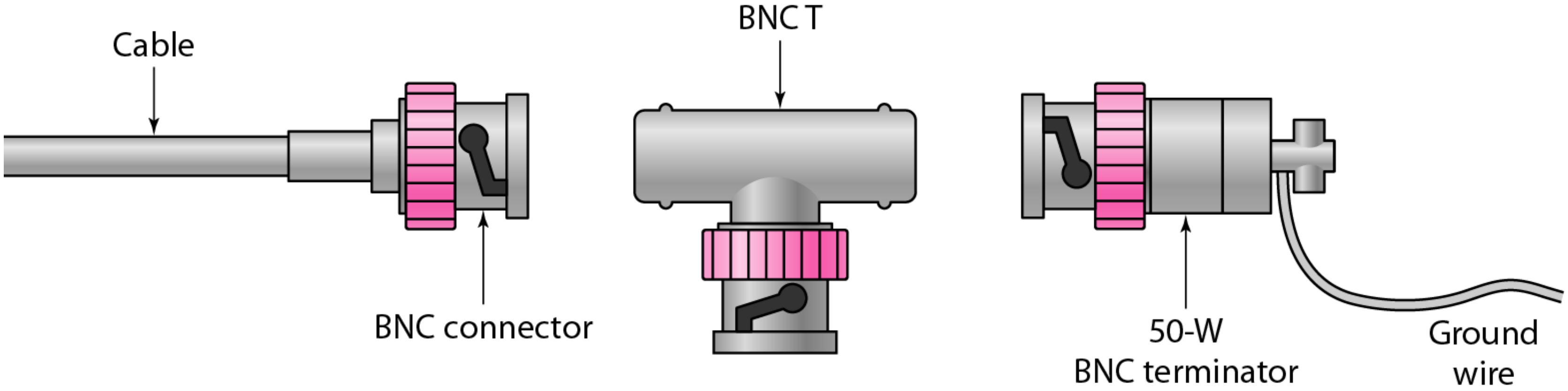
- Coaxial cables are categorized by their **Radio Government (RG)** ratings.
- Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing.



Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

BNC connectors

The most common type of connector used today is the **Bayonet Neill-Concelman (BNC)** connector.

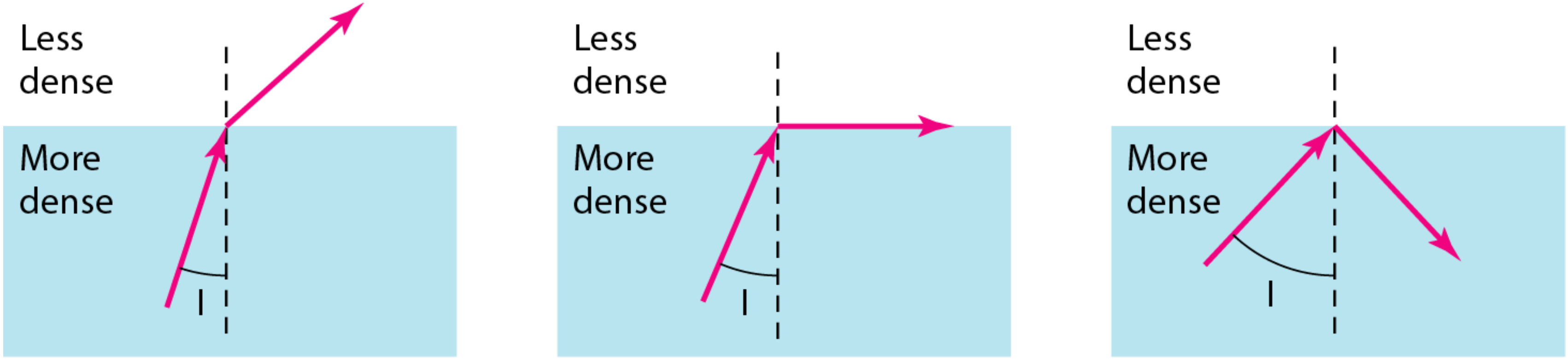


Applications

- Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
- Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps.

Fiber optics

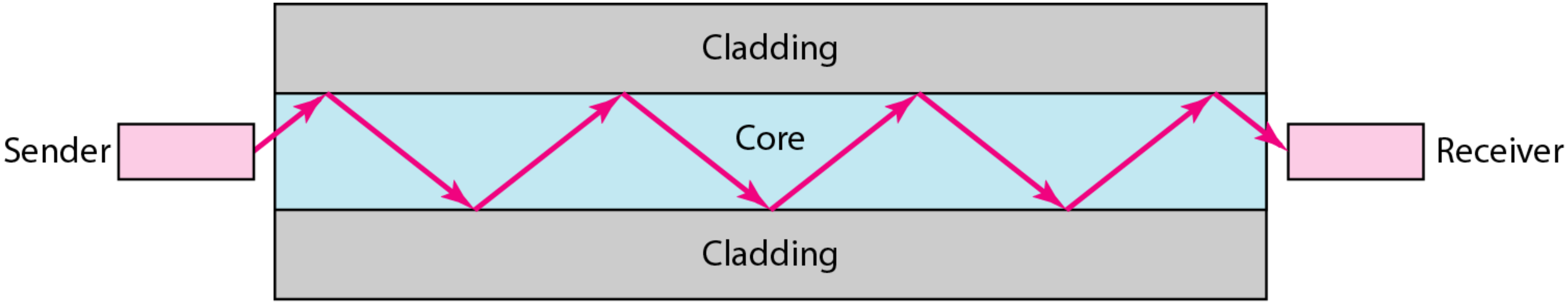
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.



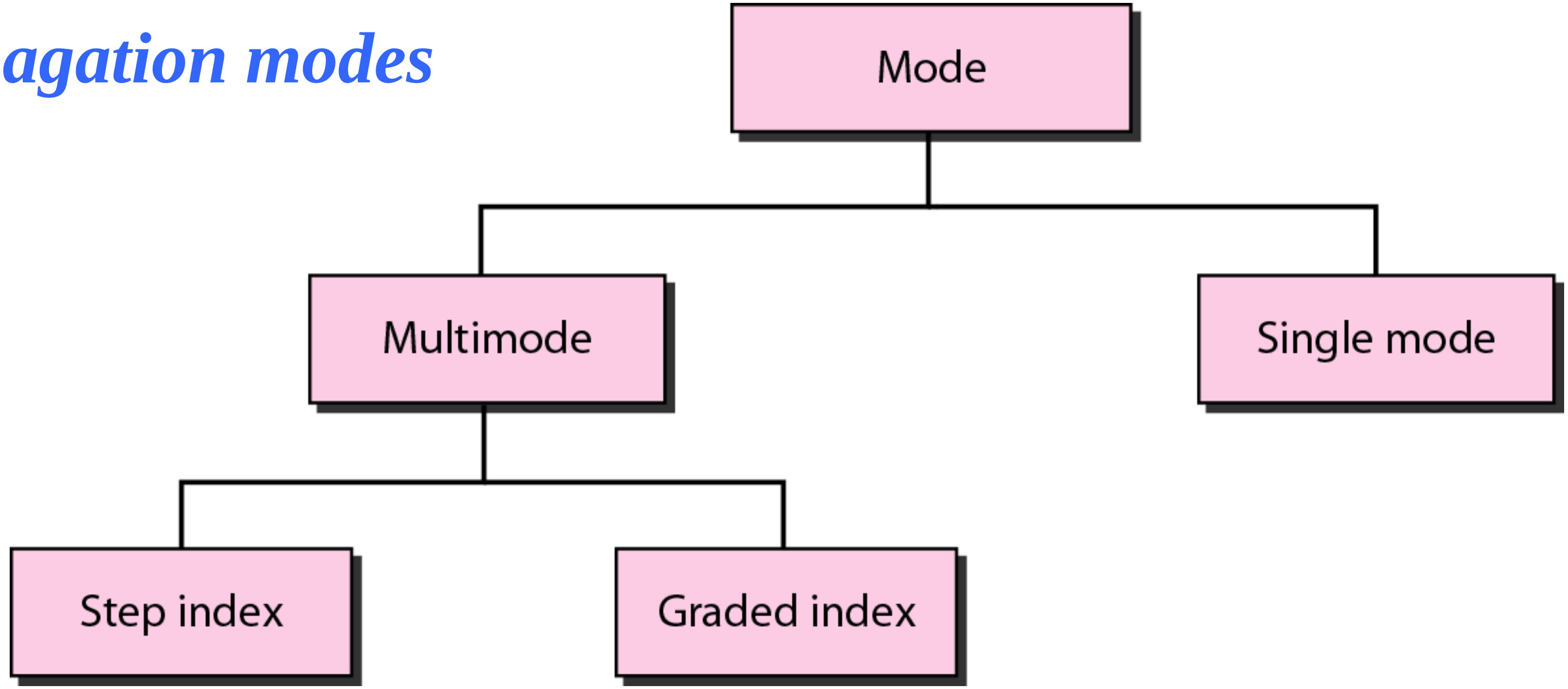
I < critical angle,
refraction

I = critical angle,
refraction

I > critical angle,
reflection

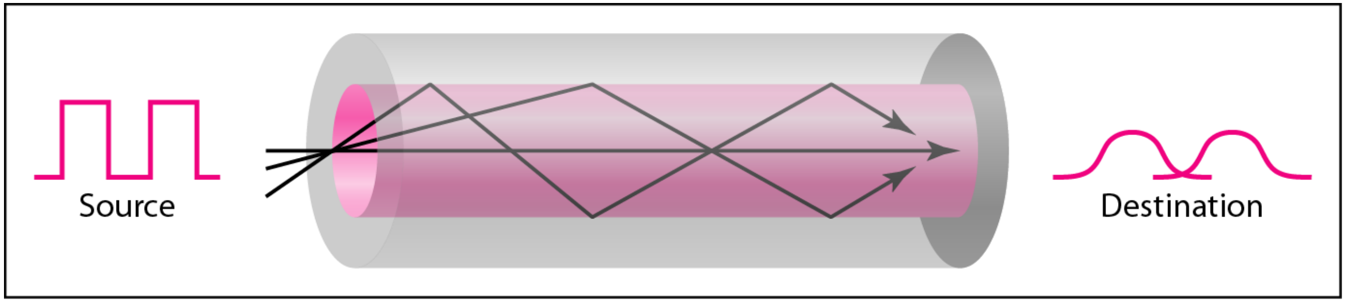


Propagation modes



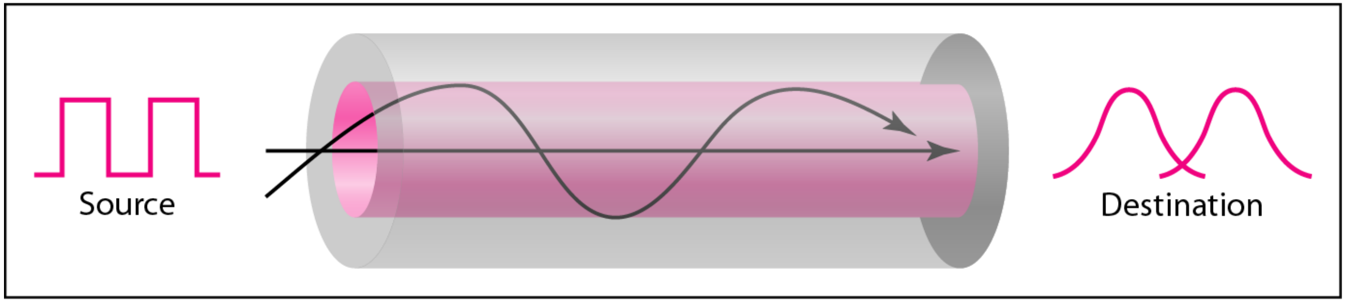
Multimode is so named because multiple beams from a light source move through the core in different paths.

Modes



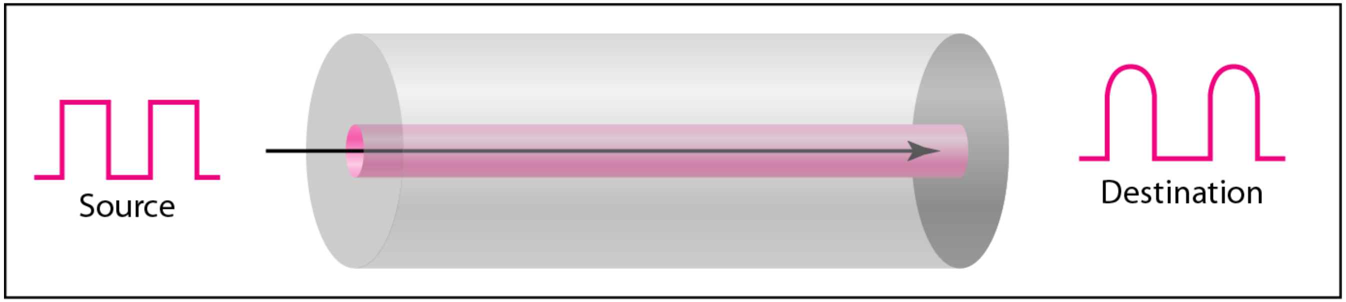
a. Multimode, step index

Density of the core remains constant from the center to the edges.



b. Multimode, graded index

Density is highest at the center of the core and decreases gradually to its lowest at the edge.



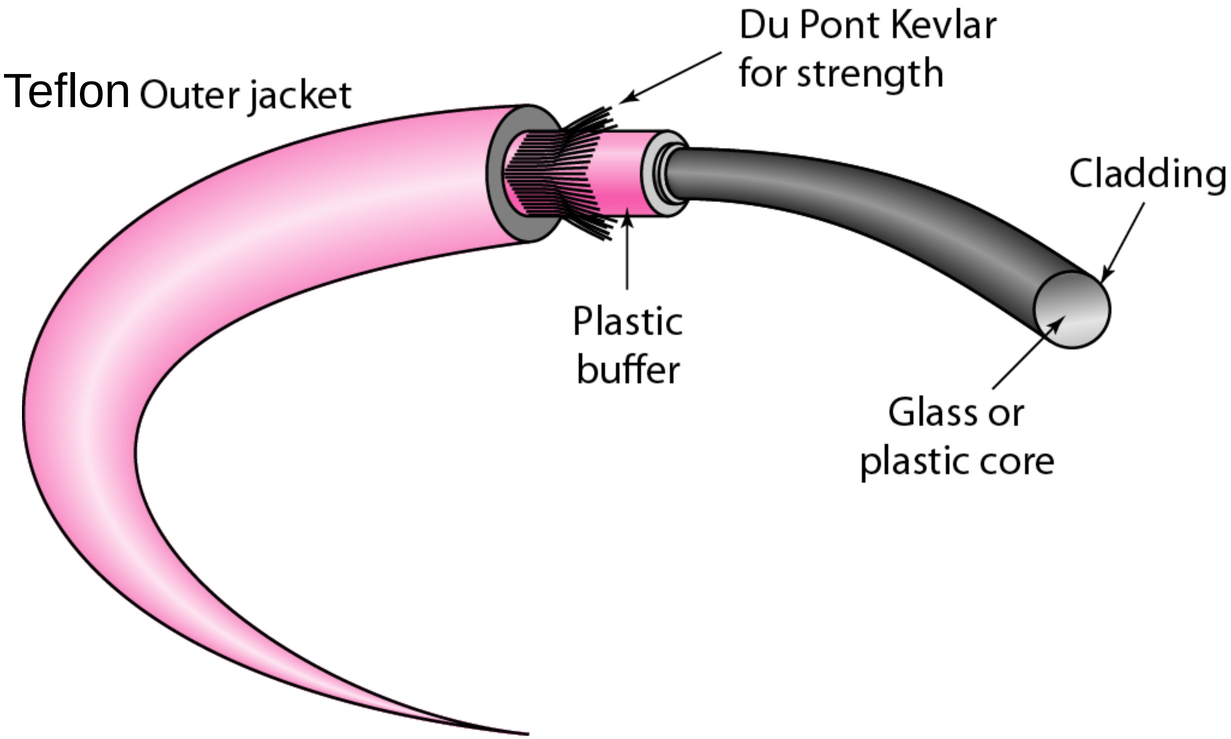
c. Single mode

Smaller diameter and with substantially lower density

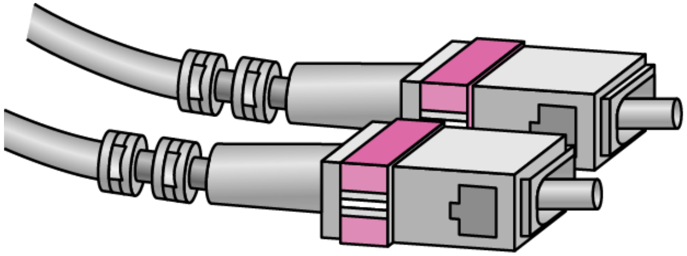
Fiber types

Type	*Core (µm)*	*Cladding (µm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

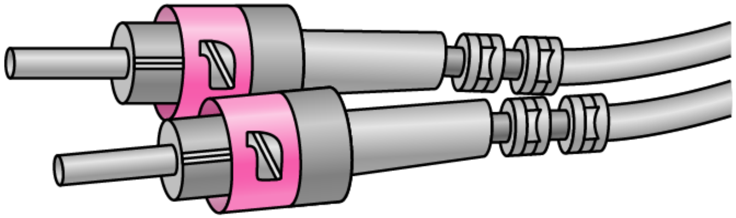
PVC or Teflon



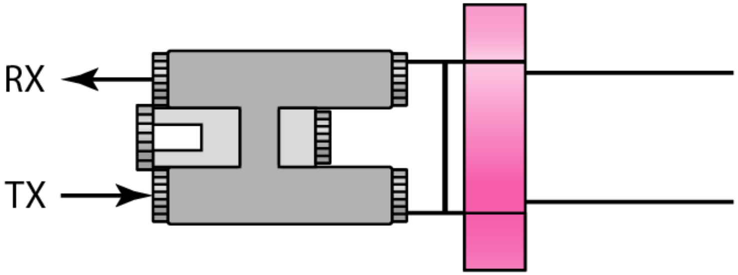
Fiber-optic cable connectors



SC connector



ST connector



MT-RJ connector

Applications

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps.
- Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network.

Advantages

- Higher bandwidth.
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

Disadvantages

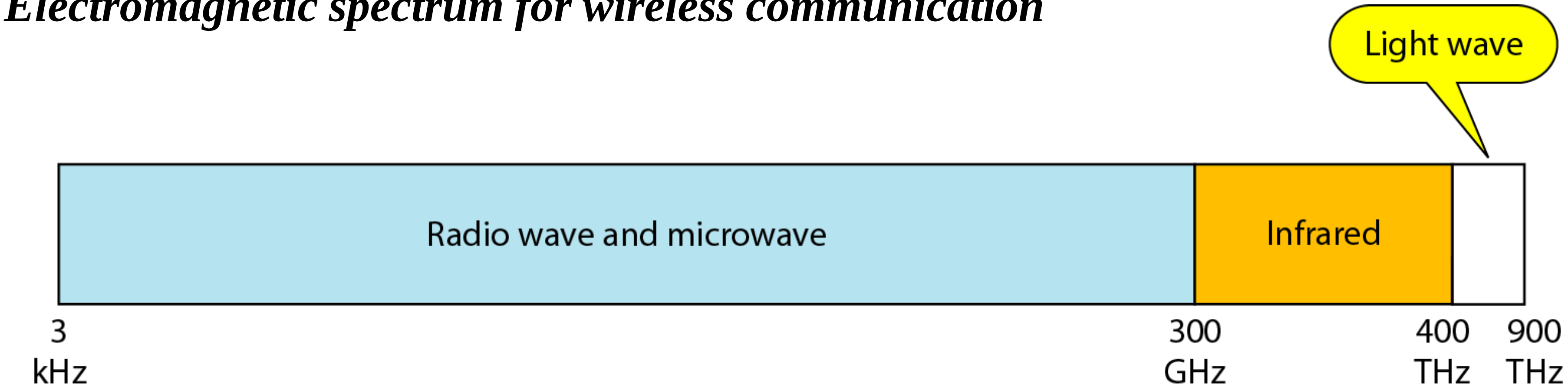
- Installation and maintenance
- Unidirectional light propagation
- Cost

UNGUIDED MEDIA: WIRELESS

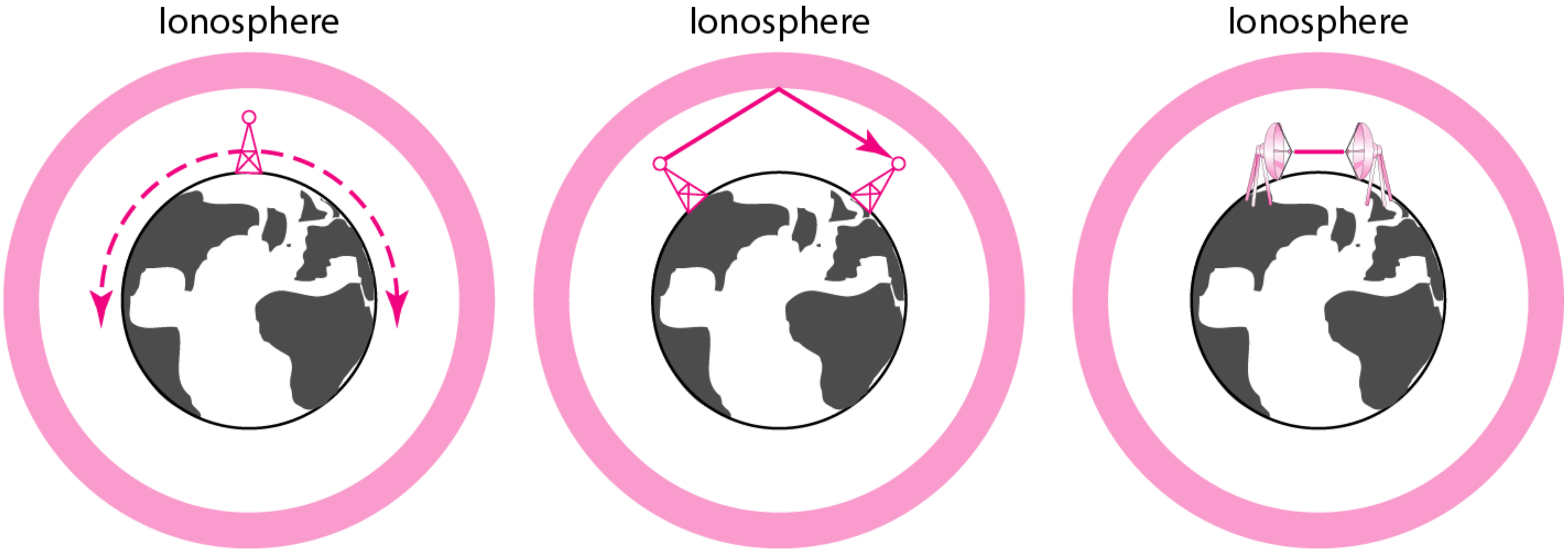
Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Radio Waves
Microwaves
Infrared

Electromagnetic spectrum for wireless communication



Propagation methods

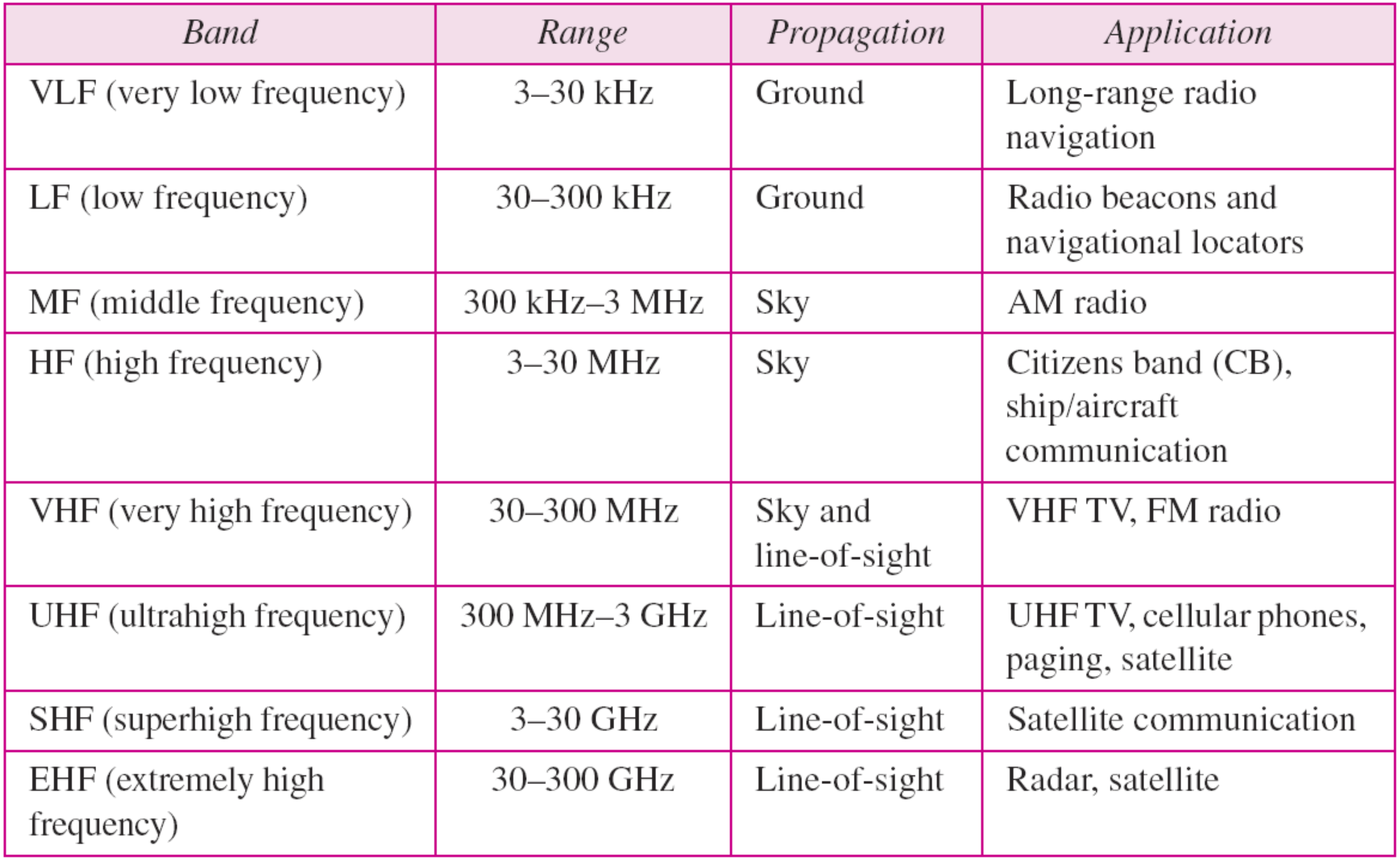


Ground propagation
(below 2 MHz)

Sky propagation
(2–30 MHz)

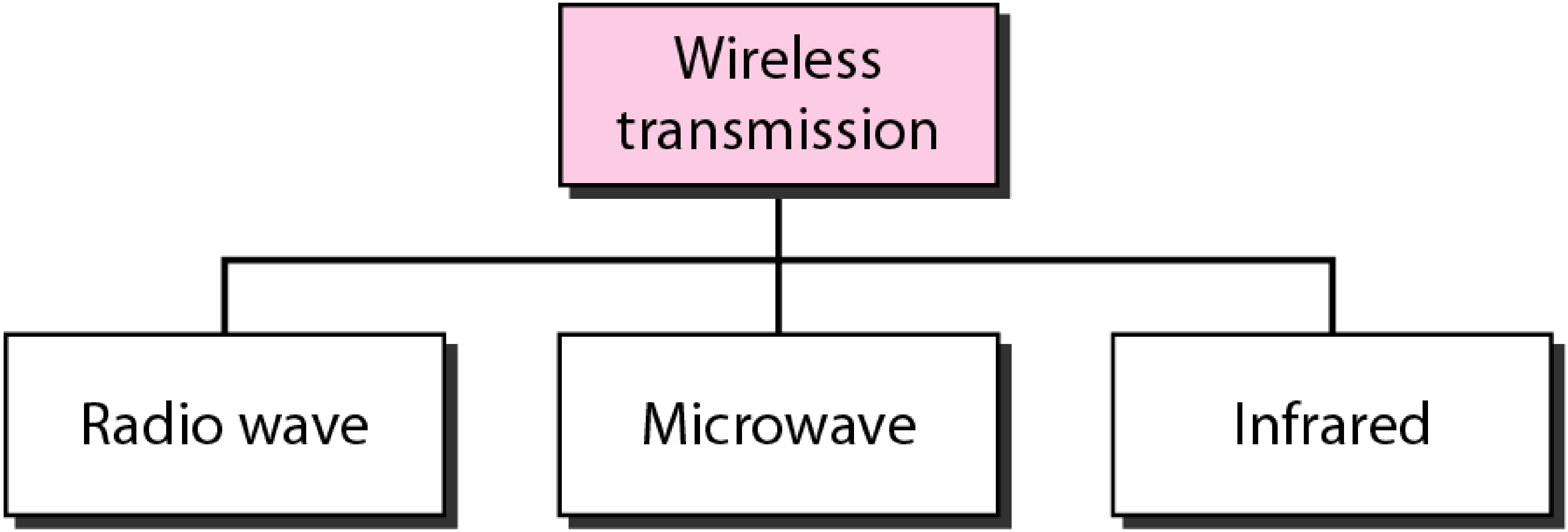
Line-of-sight propagation
(above 30 MHz)

Bands



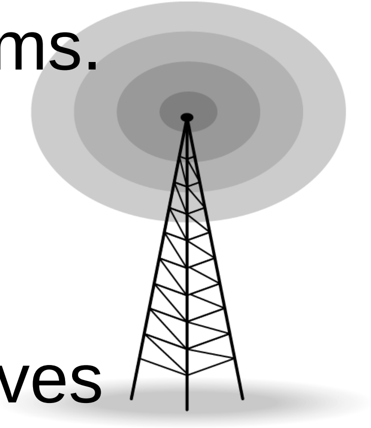
Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite

Wireless transmission waves



Radio Waves

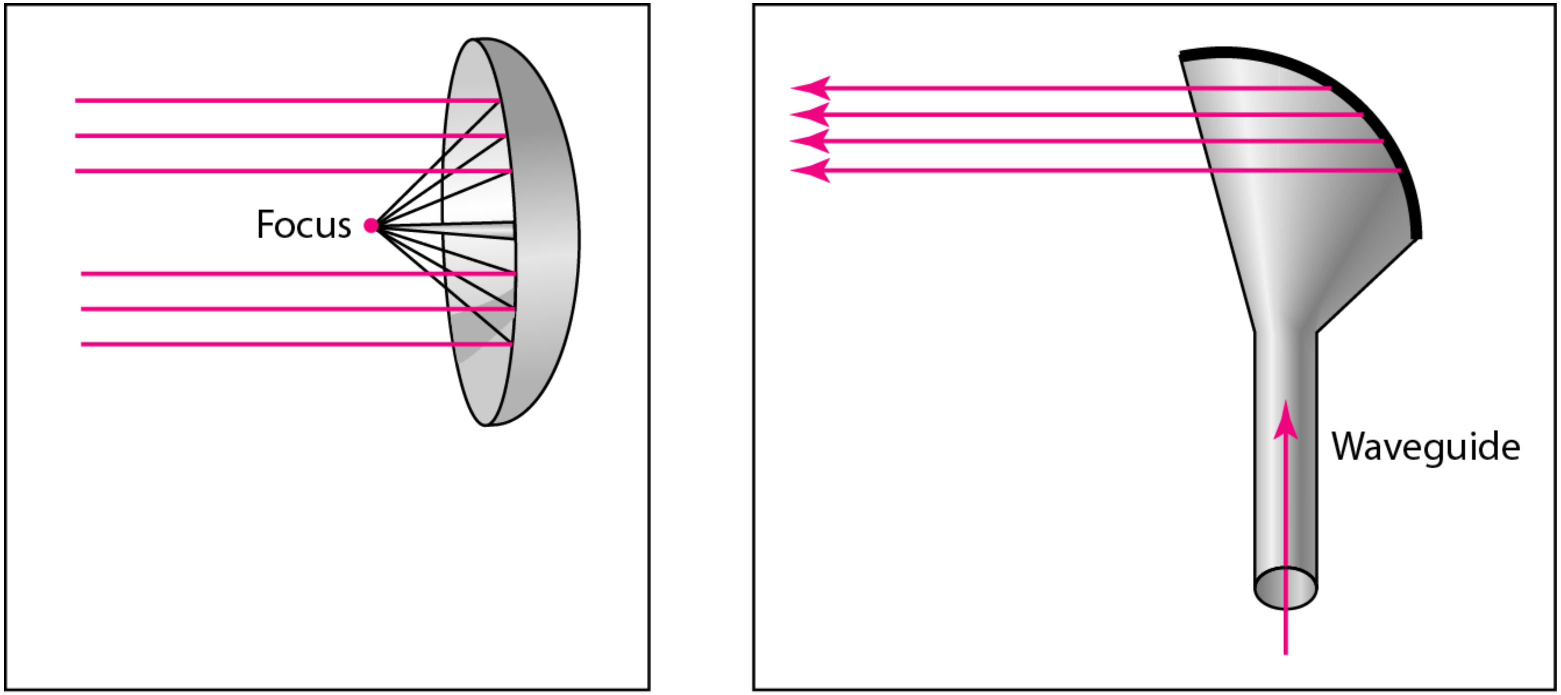
- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called
- **radio waves.**
- Radio waves are used for multicast communications, such as radio and television, and paging systems.
- They can penetrate through walls.
- Highly regulated.
- Use omni directional antennas
- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.



Microwaves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional. Use directional antennas - point to point line of sight communications.
- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.
- Higher frequency ranges cannot penetrate walls.
- The microwave band is relatively wide, almost 299 GHz. Therefore wider sub-bands can be assigned, and a high data rate is possible. Use of certain portions of the band requires permission from authorities

Unidirectional antennas



a. Dish antenna

b. Horn antenna

Applications

Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones ,satellite networks, and wireless LANs.

Infrared

- Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication.
- Infrared waves, having high frequencies, cannot penetrate walls.
- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Applications

For communication between devices such as TV Remotes, keyboards, mice, PCs, and printers

Wireless Channels

- Are subject to a lot more errors than guided media channels.
- Interference is one cause for errors, can be circumvented with high SNR.
- The higher the SNR the less capacity is available for transmission due to the broadcast nature of the channel.
- Channel also subject to fading and no coverage holes.

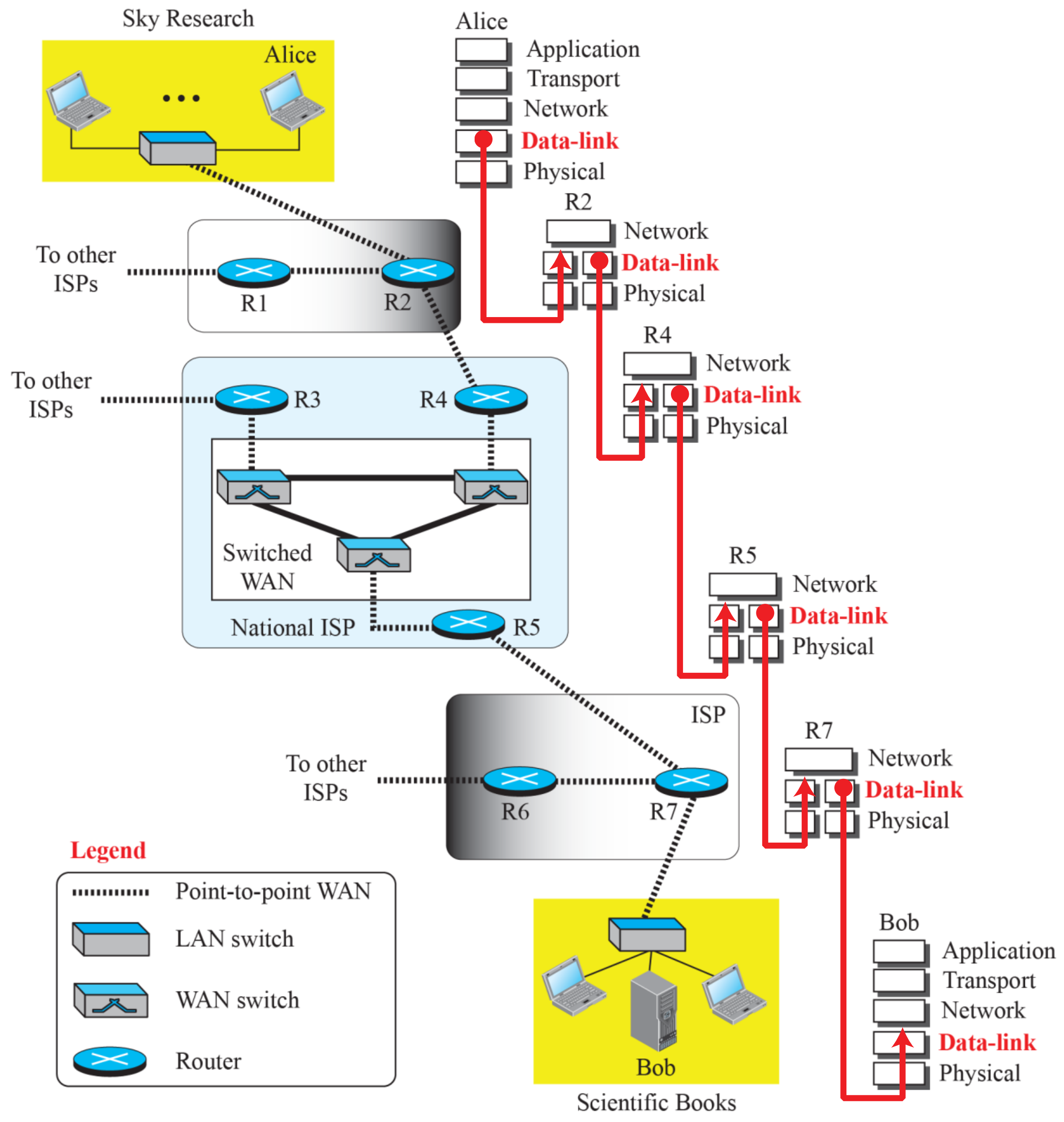
UNIT-1

Data Link Layer

INTRODUCTION

The Internet is a combination of networks glued together by connecting devices (routers or switches). If a datagram is to travel from a host to another host, it needs to pass through these networks.

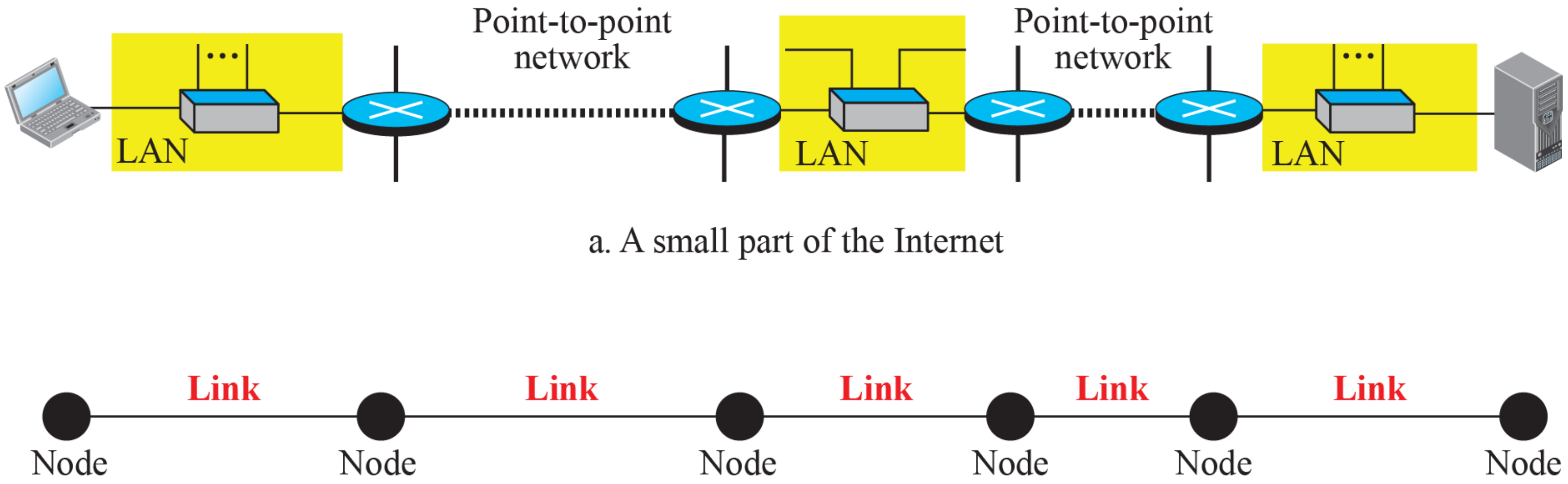
Communication at the data-link layer



Nodes and Links

Although communication at the application, transport, and network layers is end-to-end, communication at the data-link layer is node-to-node. As we have learned in the previous chapters, a data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point. Theses LANs and WANs are connected by routers. It is customary to refer to the two end hosts and the routers as nodes and the networks in between as links.

Nodes and Links



a. A small part of the Internet

b. Nodes and links

Two Types of Links

Although two nodes are physically connected by a transmission medium such as cable or air, we need to remember that the data-link layer controls how the medium is used. We can have a data-link layer that uses the whole capacity of the medium; we can also have a data-link layer that uses only part of the capacity of the link. In other words, we can have a

- Point-to-Point link
- Broadcast link.

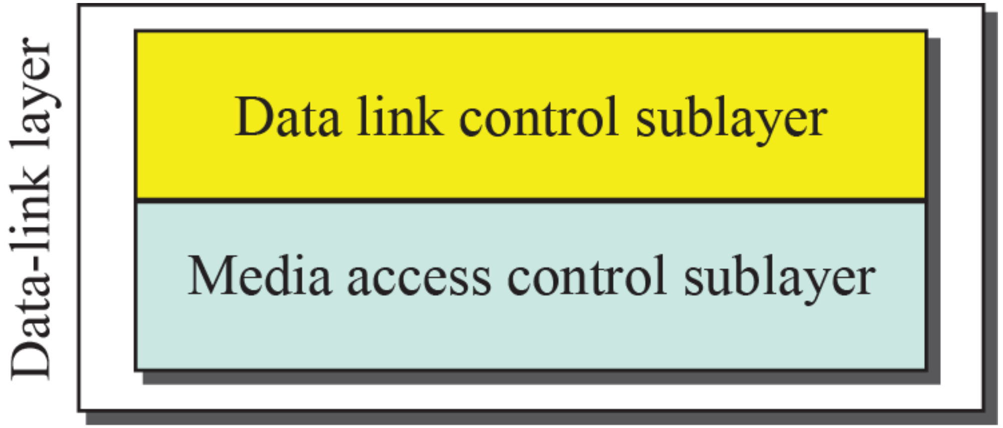
Two Sublayers

To better understand the functionality of and the services provided by the link layer, we can divide the data-link layer into two sublayers:

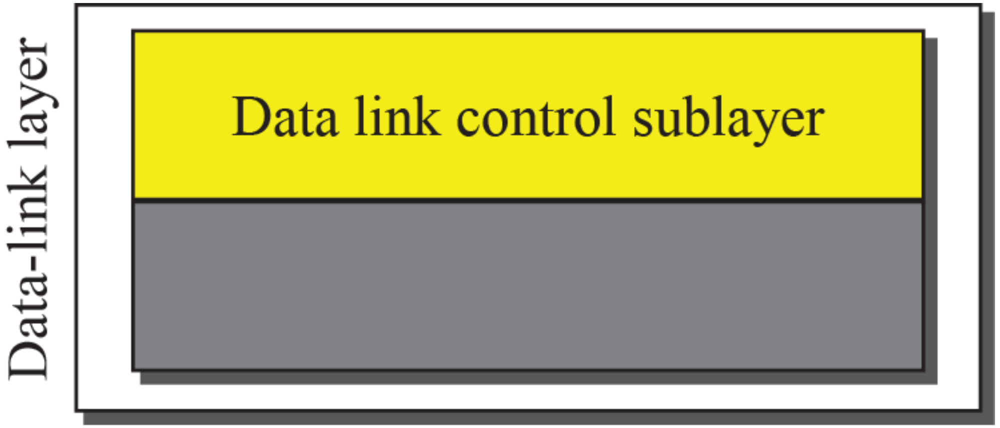
- Data Link Control (DLC) and
- Media Access Control (MAC).

The data link control sublayer deals with all issues common to both point-to-point and broadcast links;
the media access control sublayer deals only with issues specific to broadcast links.

Dividing the data-link layer into two sublayers



a. Data-link layer of a broadcast link

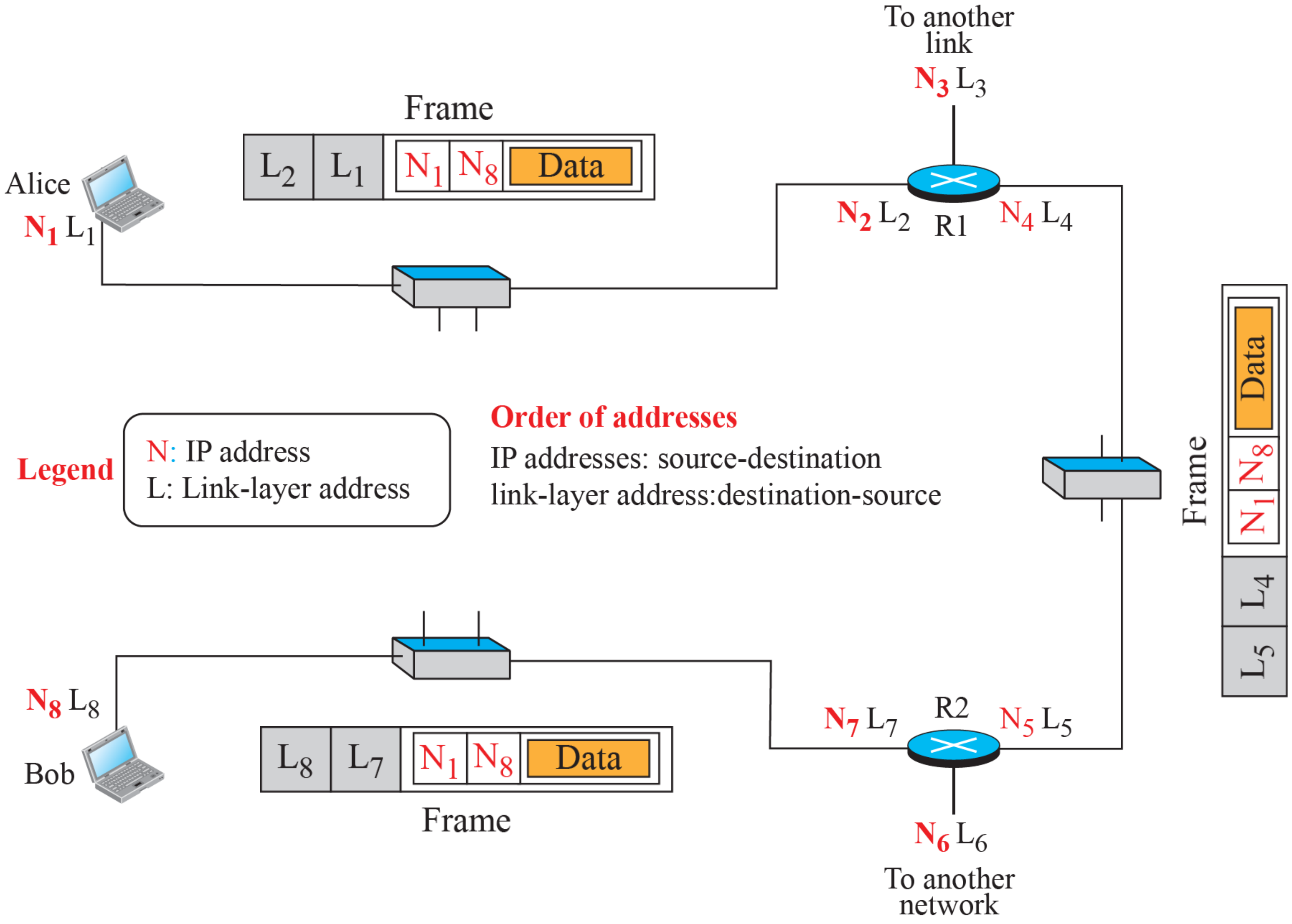


b. Data-link layer of a point-to-point link

DATA LINK CONTROL (DLC)

The data link control deals with procedures for communication between two adjacent nodes. Data link control (DLC) functions include addressing, framing, flow and error control, and error detection and correction.

IP addresses and link-layer addresses in a small internet



Legend

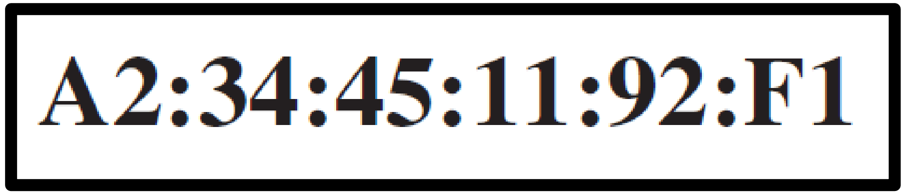
N: IP address
L: Link-layer address

Order of addresses

IP addresses: source-destination
link-layer address:destination-source

LINK-LAYER ADDRESSING

The link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons; for example, the following is a link-layer address of a computer.



A2:34:45:11:92:F1

Three Types of addresses

Unicast Address

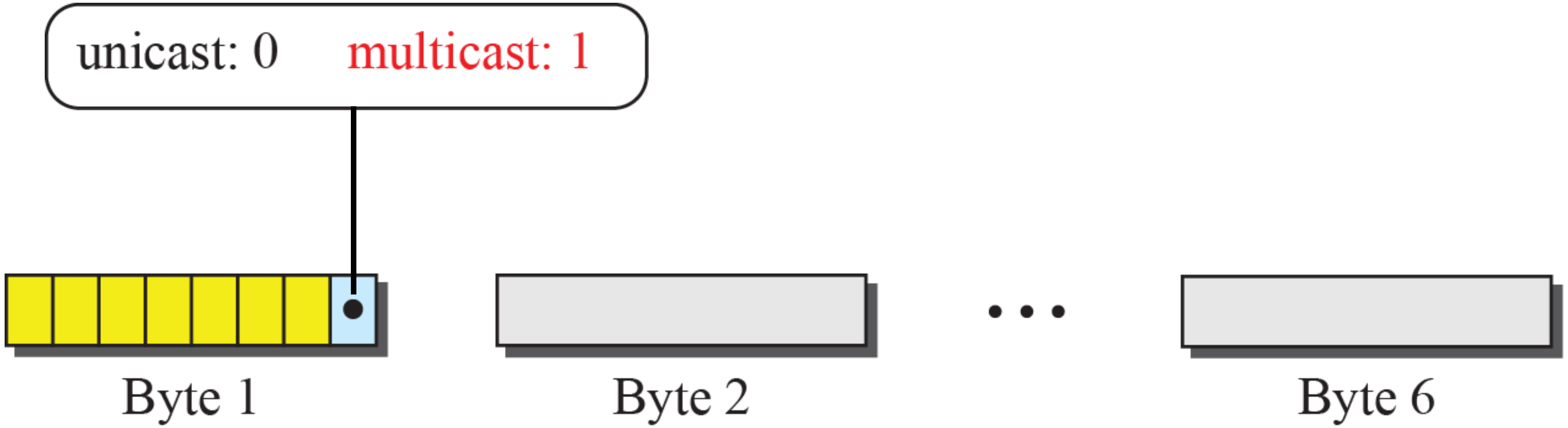
Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

Multicast Address

Some link-layer protocols define multicast addresses. Multicasting means one-to-many communication. However, the jurisdiction is local (inside the link).

Broadcast Address

Some link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link. (**FF:FF:FF:FF:FF:FF**)



Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are Fs, the address is broadcast. Therefore, we have the following:

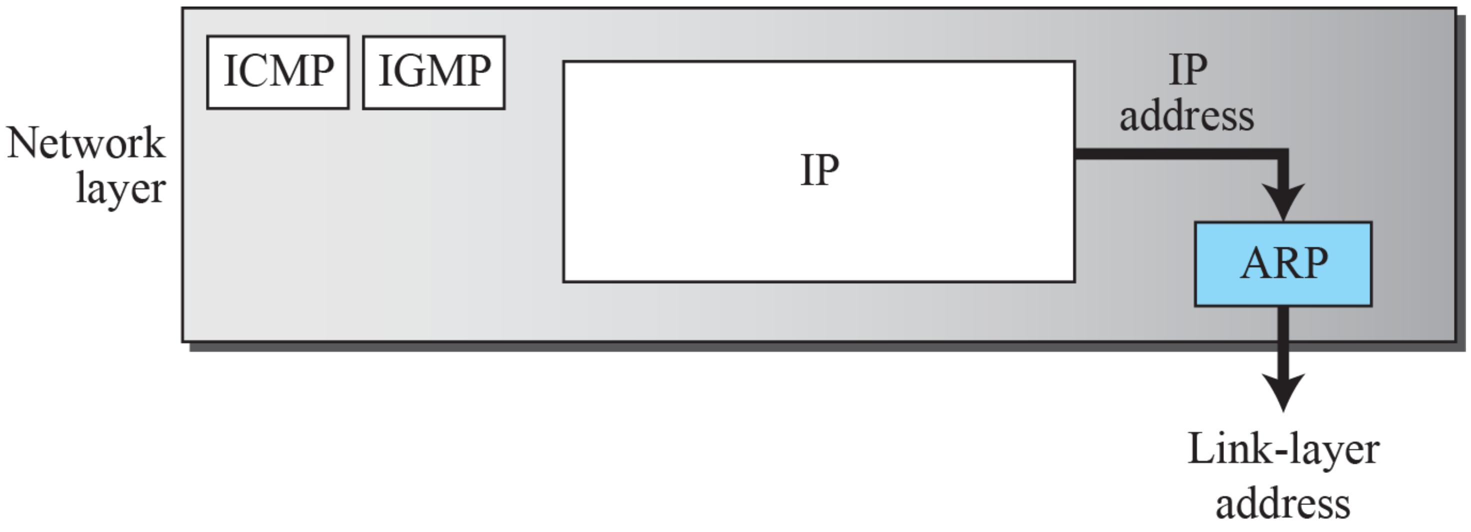
a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are Fs in hexadecimal.

Address Resolution Protocol (ARP)

- ❑ Address Resolution Protocol (ARP)
    - ❖ Packet Format
- ❑ An Example
    - ❖ Activities at the Alice Site
    - ❖ Activities at Routers
    - ❖ Activities at Bob’s Site

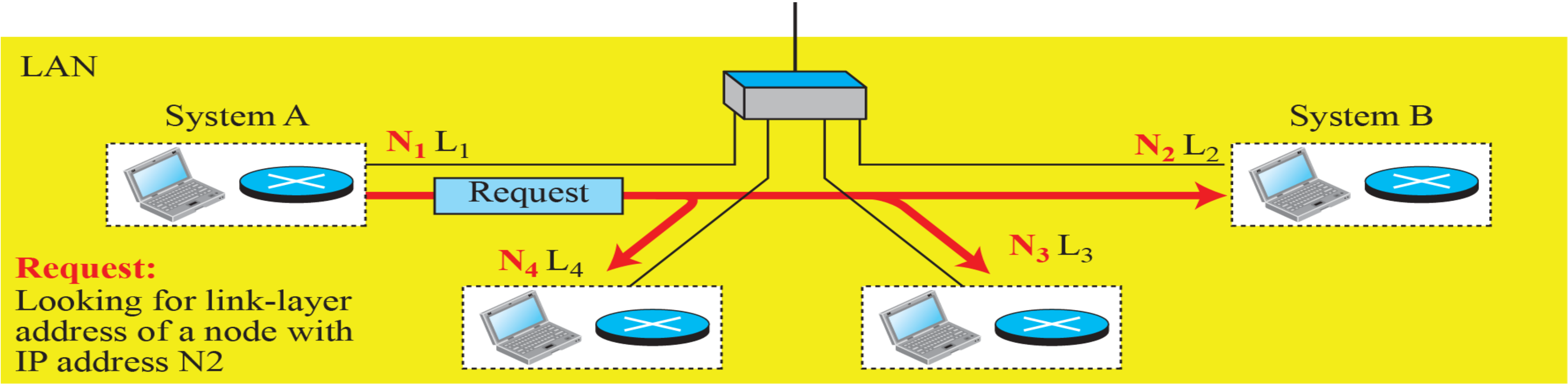
Position of ARP in TCP/IP protocol suite

- The IP address of the next node is not helpful in moving a frame through a link; but we need the link-layer address of the next node. This is the time when the **Address Resolution Protocol (ARP)** becomes helpful.
- It belongs to the network layer, ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.



ARP operation

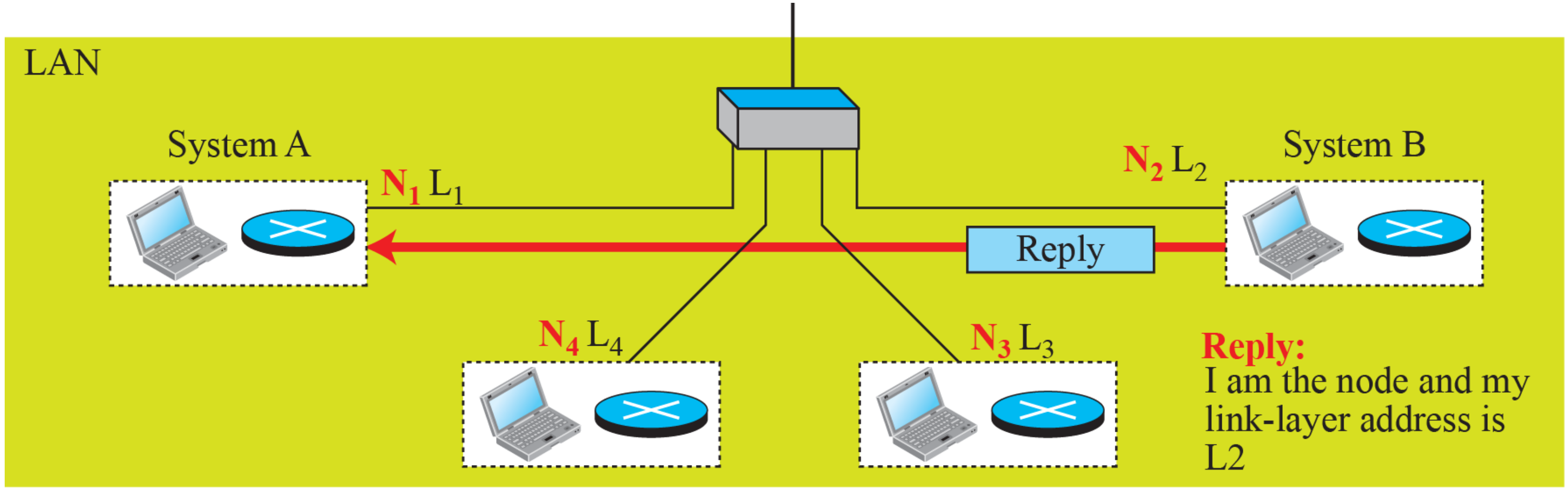
Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an **ARP request packet**. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address.



a. ARP request is broadcast

ARP operation

Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and link-layer addresses. The packet is unicast directly to the node that sent the request packet.



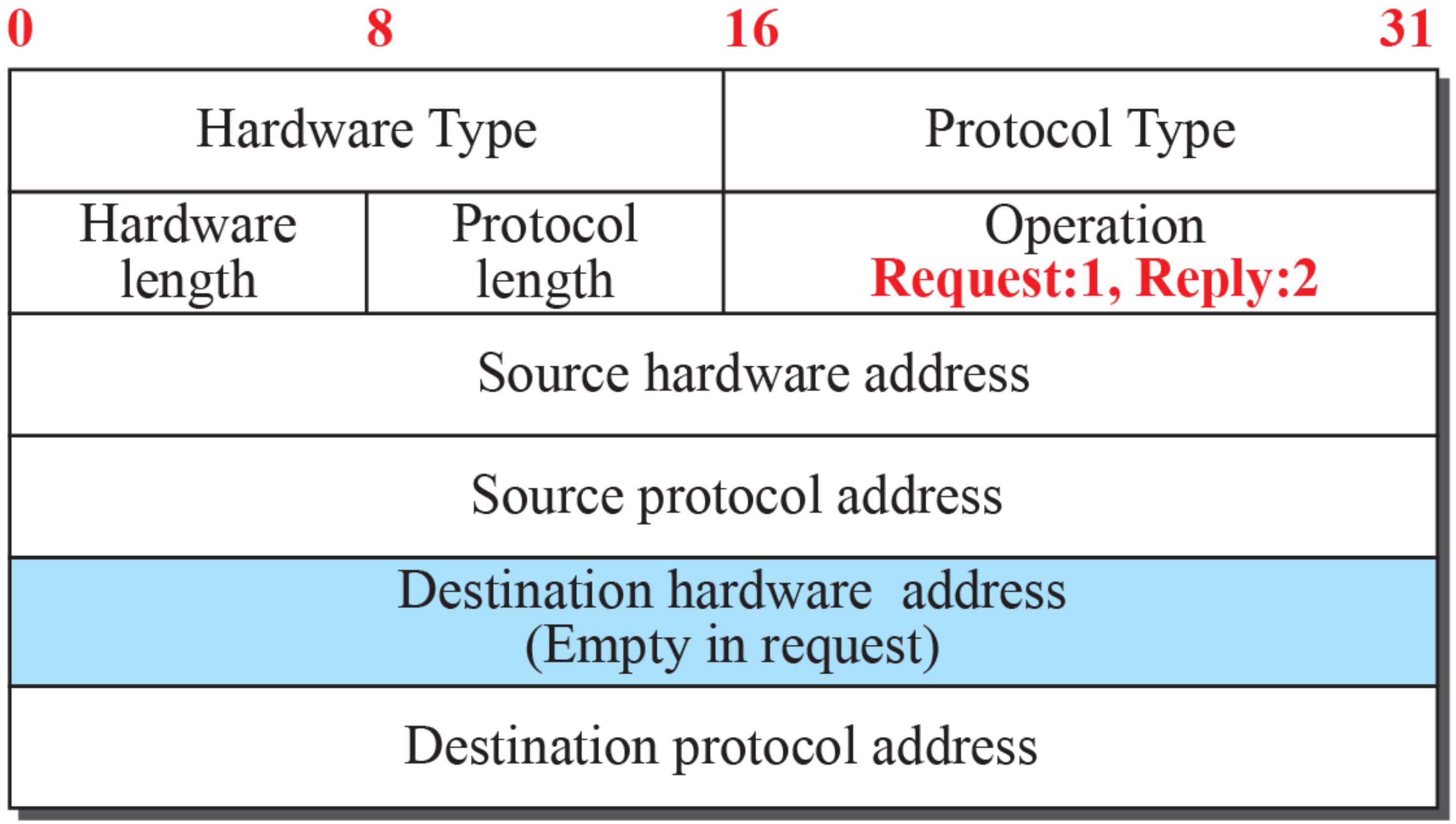
Reply:
I am the node and my
link-layer address is
L2

b. ARP reply is unicast

ARP packet format

Hardware: LAN or WAN protocol

Protocol: Network-layer protocol



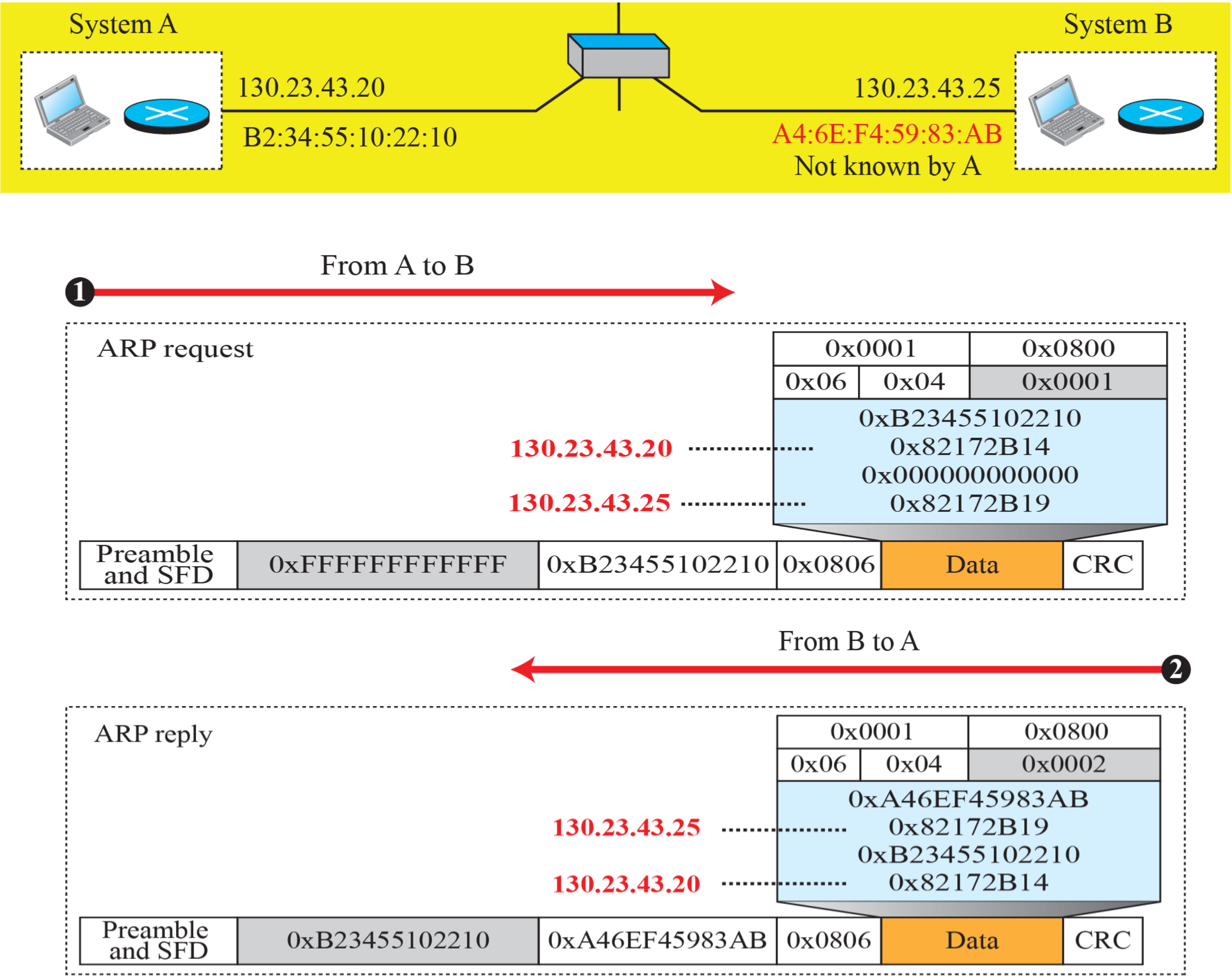
The *hardware type* field defines the type of the link-layer protocol; Ethernet is given the type 1.

The *protocol type* field defines the network-layer protocol: IPv4 protocol is $(0800)_{16}$.

The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of the sender.

The destination hardware address and destination protocol address fields define the receiver link-layer and network-layer addresses.

Example



System A

130.23.43.20

B2:34:55:10:22:10

System B

130.23.43.25

A4:6E:F4:59:83:AB

Not known by A

1 From A to B

ARP request

0x0001	0x0800
0x06 0x04	0x0001

0xB23455102210

130.23.43.20 .... 0x82172B14

0x000000000000

130.23.43.25 .... 0x82172B19

Preamble and SFD	0xFFFFFFFFFFFF	0xB23455102210	0x0806	Data	CRC

2 From B to A

ARP reply

0x0001	0x0800
0x06 0x04	0x0002

0xA46EF45983AB

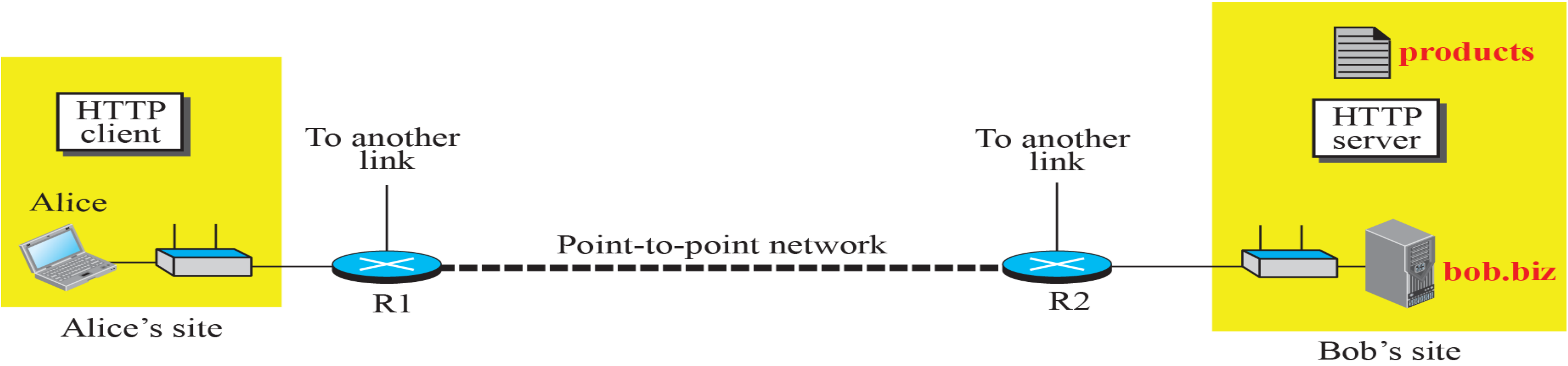
130.23.43.25 .... 0x82172B19

0xB23455102210

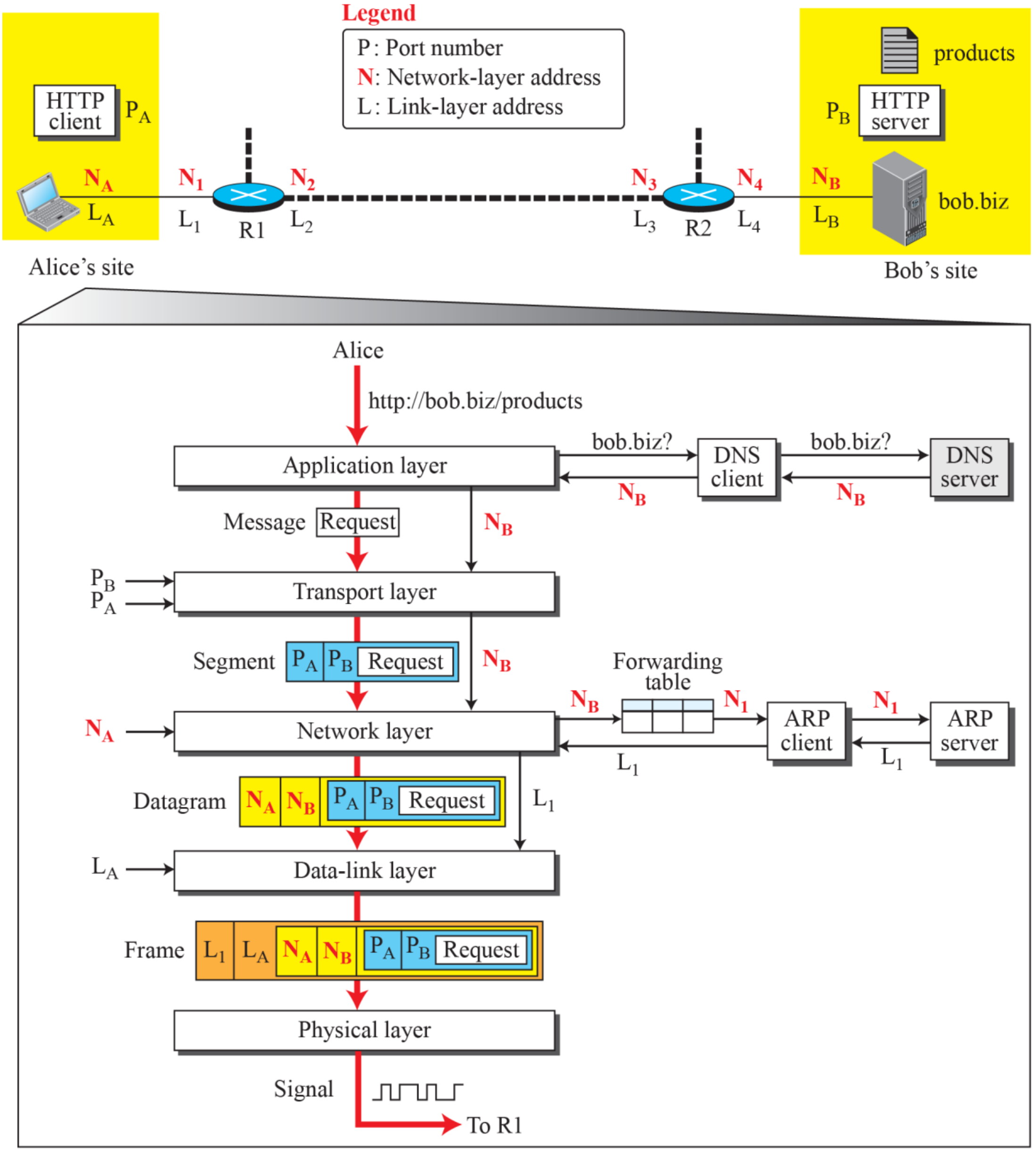
130.23.43.20 .... 0x82172B14

Preamble and SFD	0xB23455102210	0xA46EF45983AB	0x0806	Data	CRC

An Example of Communication

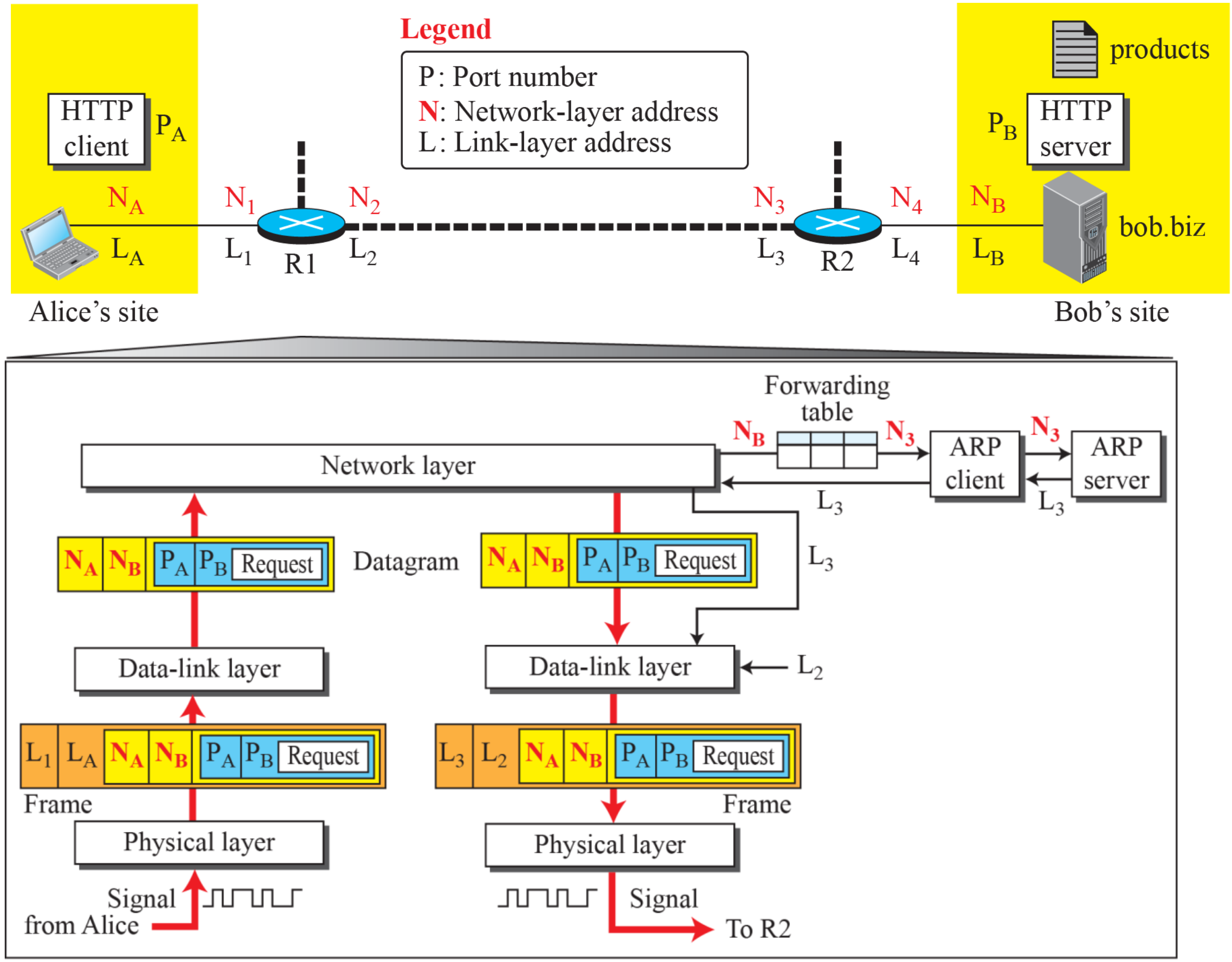


Flow of packets at Alice's computer



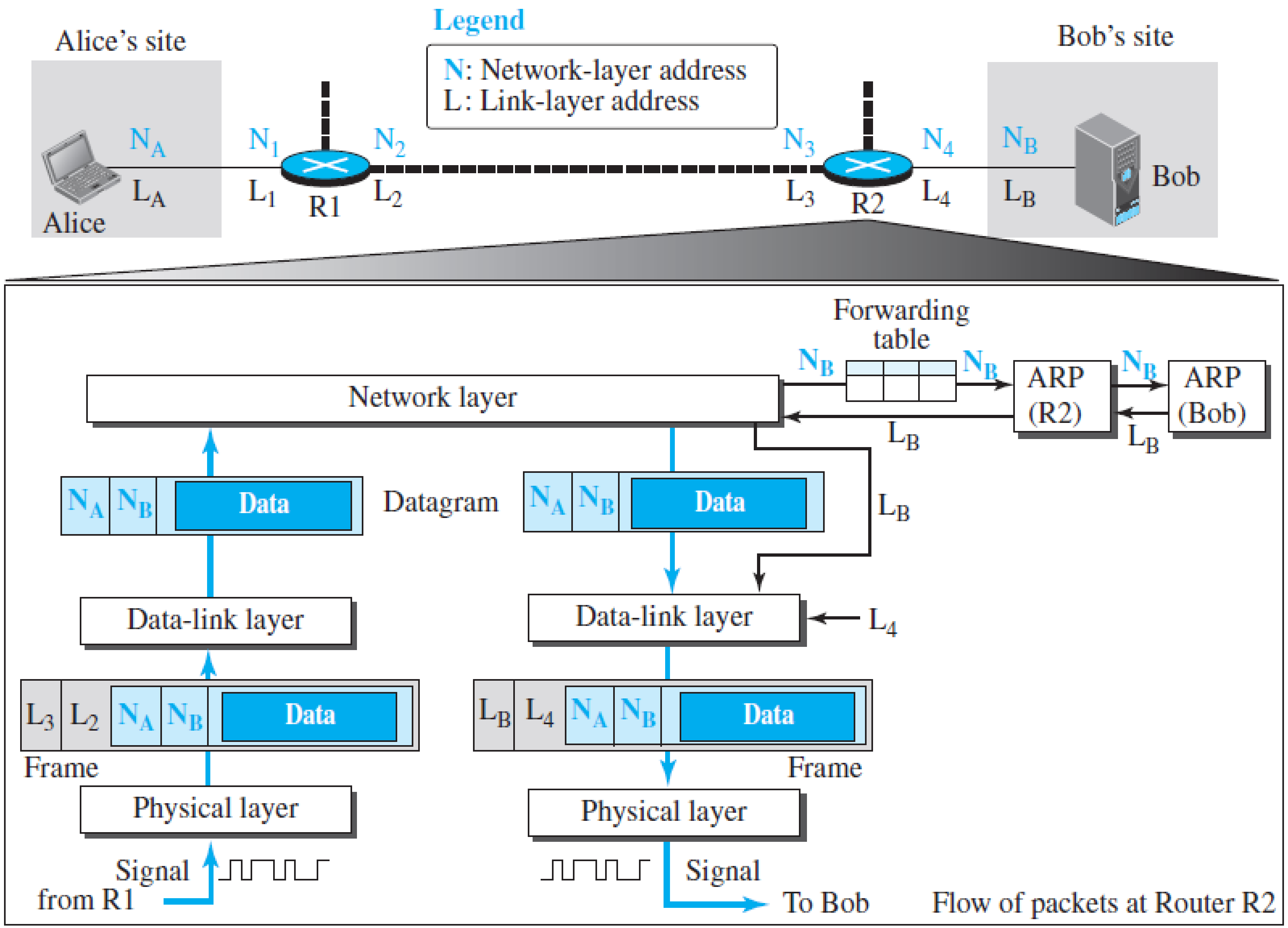
Flow of packets at Alice's computer

Flow of activities at router R1

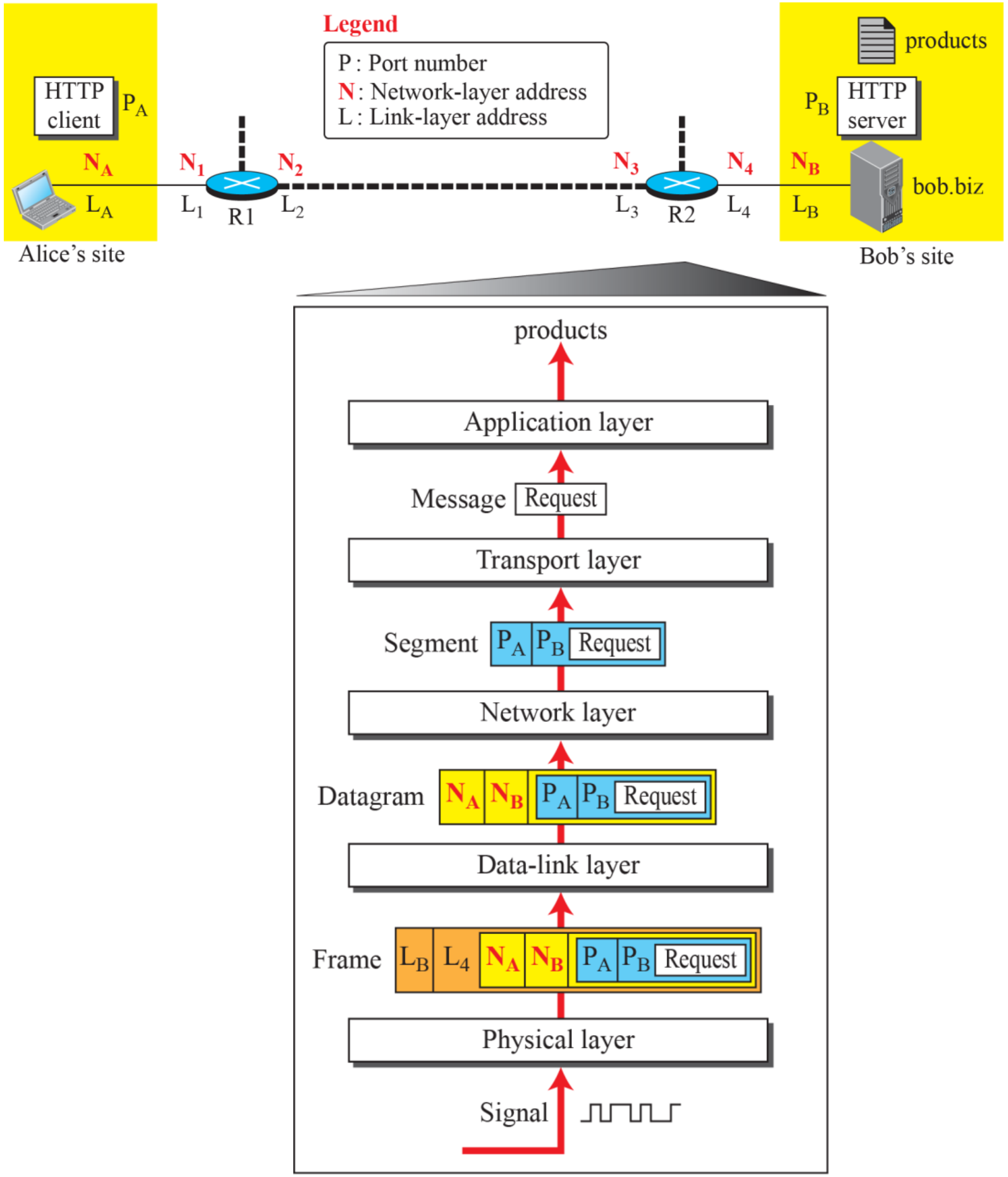


Flow of packets at Router R1

Flow of activities at router R2



Activities at Bob's site



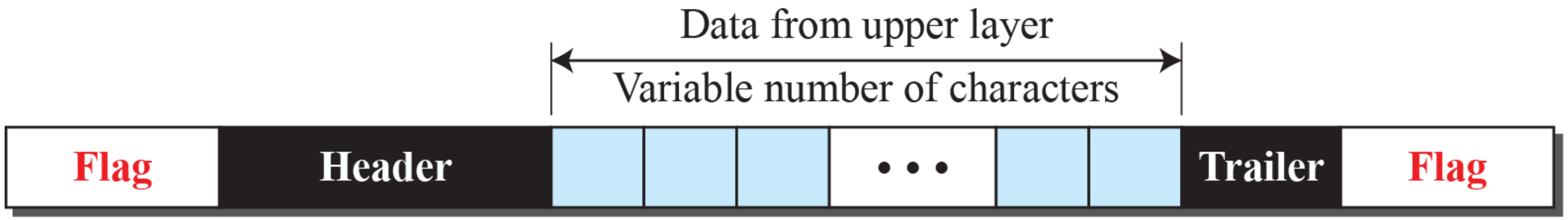
Flow of packets at Bob's computer

Framing

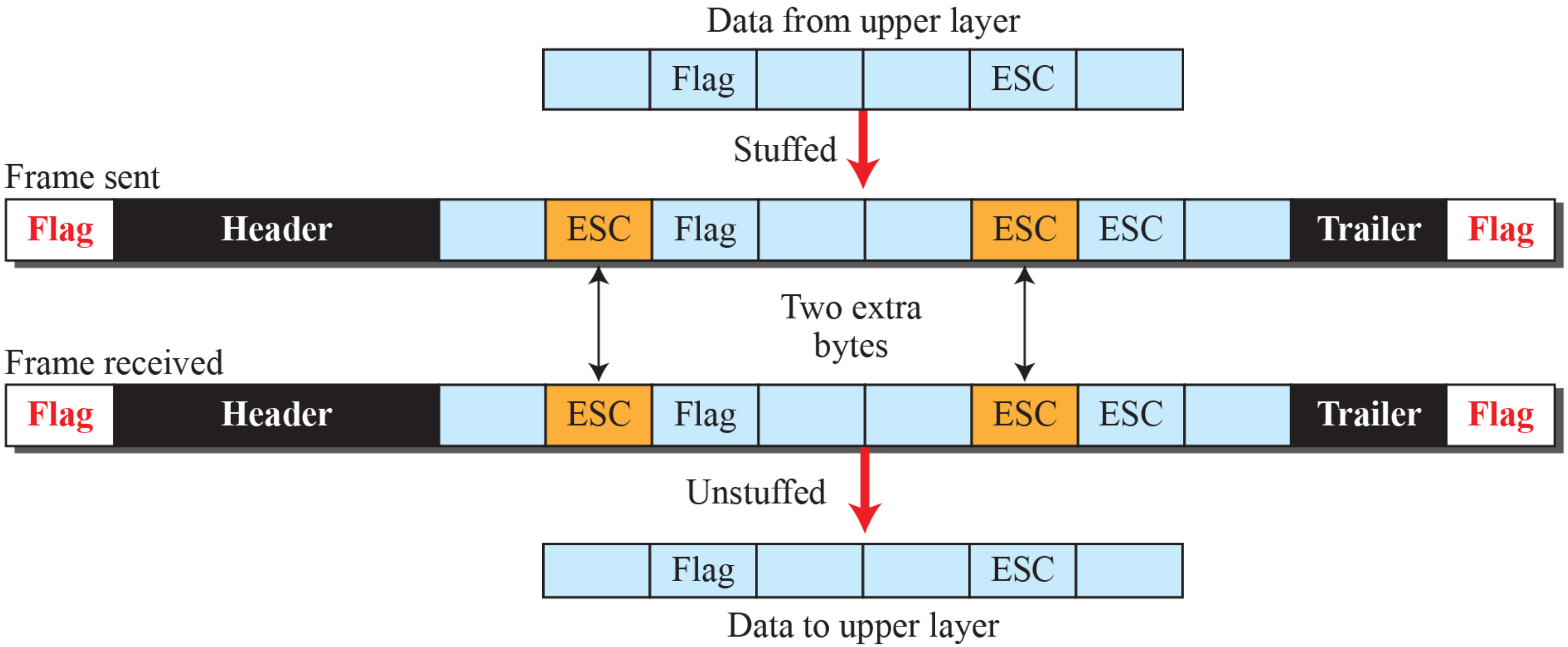
Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The data-link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another.

- Frame Size
  - Character-Oriented Framing
  - Bit-Oriented Framing

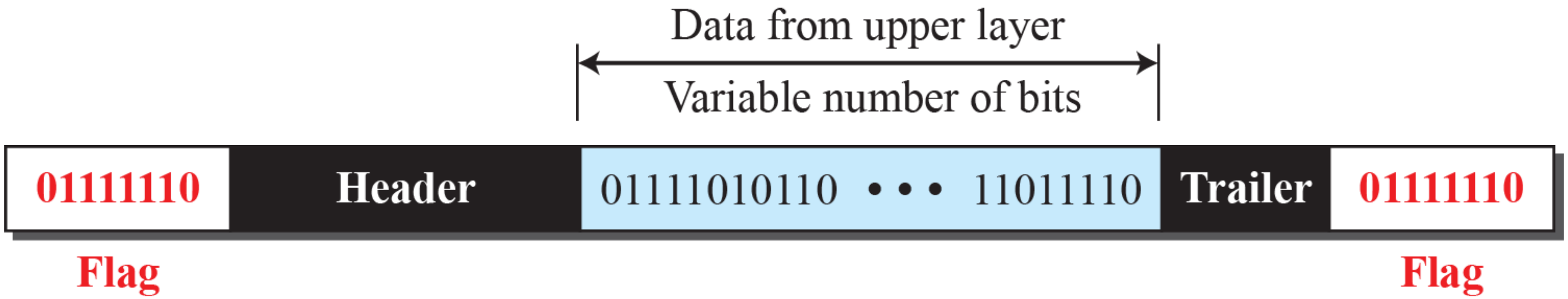
A frame in a character-oriented protocol



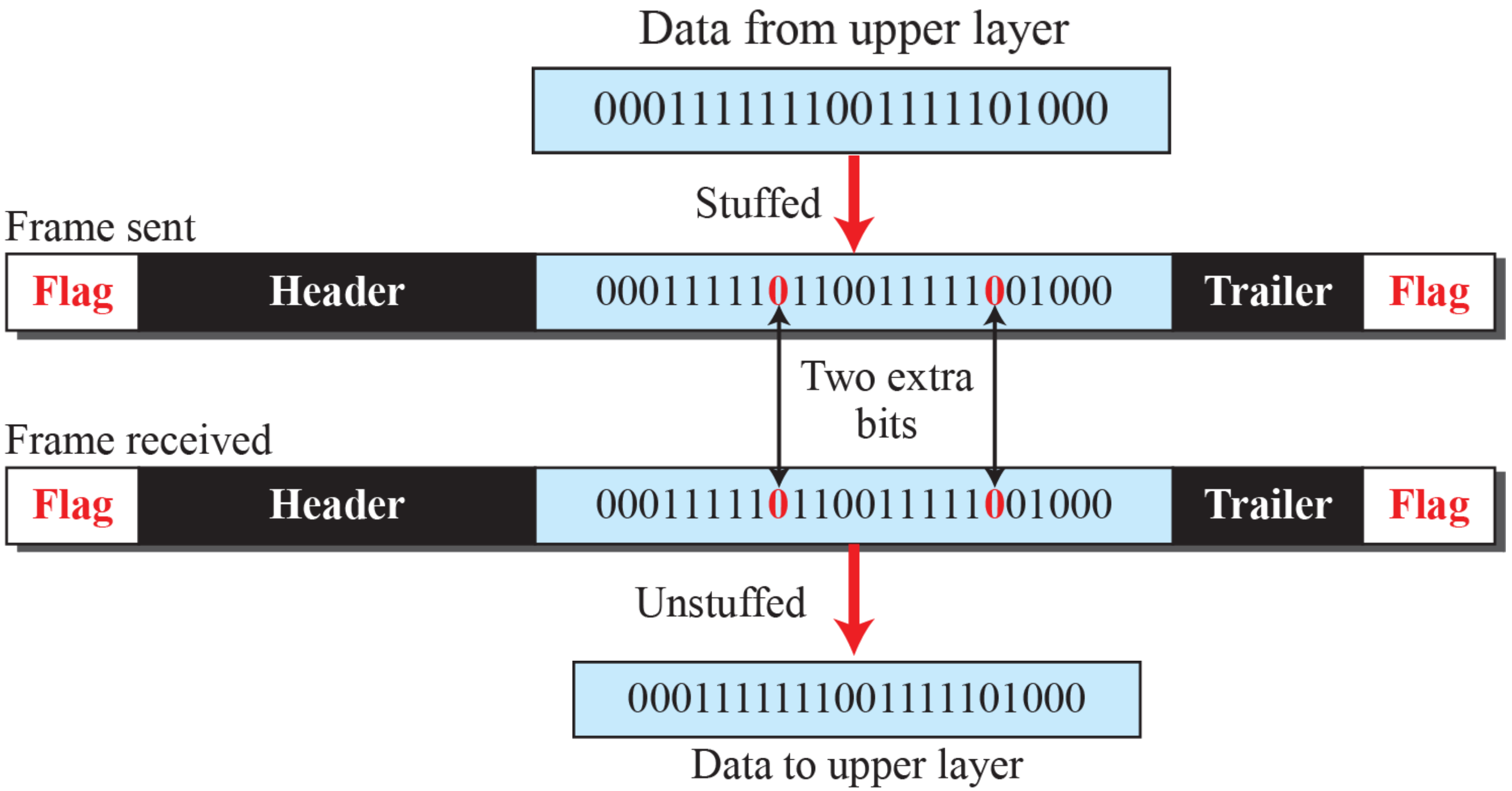
Byte stuffing and unstuffing



A frame in a bit-oriented protocol



Bit stuffing and unstuffing



Data from upper layer

0001111111001111101000

Stuffed

Frame sent

Flag | Header | 000111110110011111001000 | Trailer | Flag

Two extra bits

Frame received

Flag | Header | 000111110110011111001000 | Trailer | Flag

Unstuffed

0001111111001111101000

Data to upper layer

Flow and Error Control

One of the responsibilities of the data-link control sublayer is flow and error control at the data-link layer.

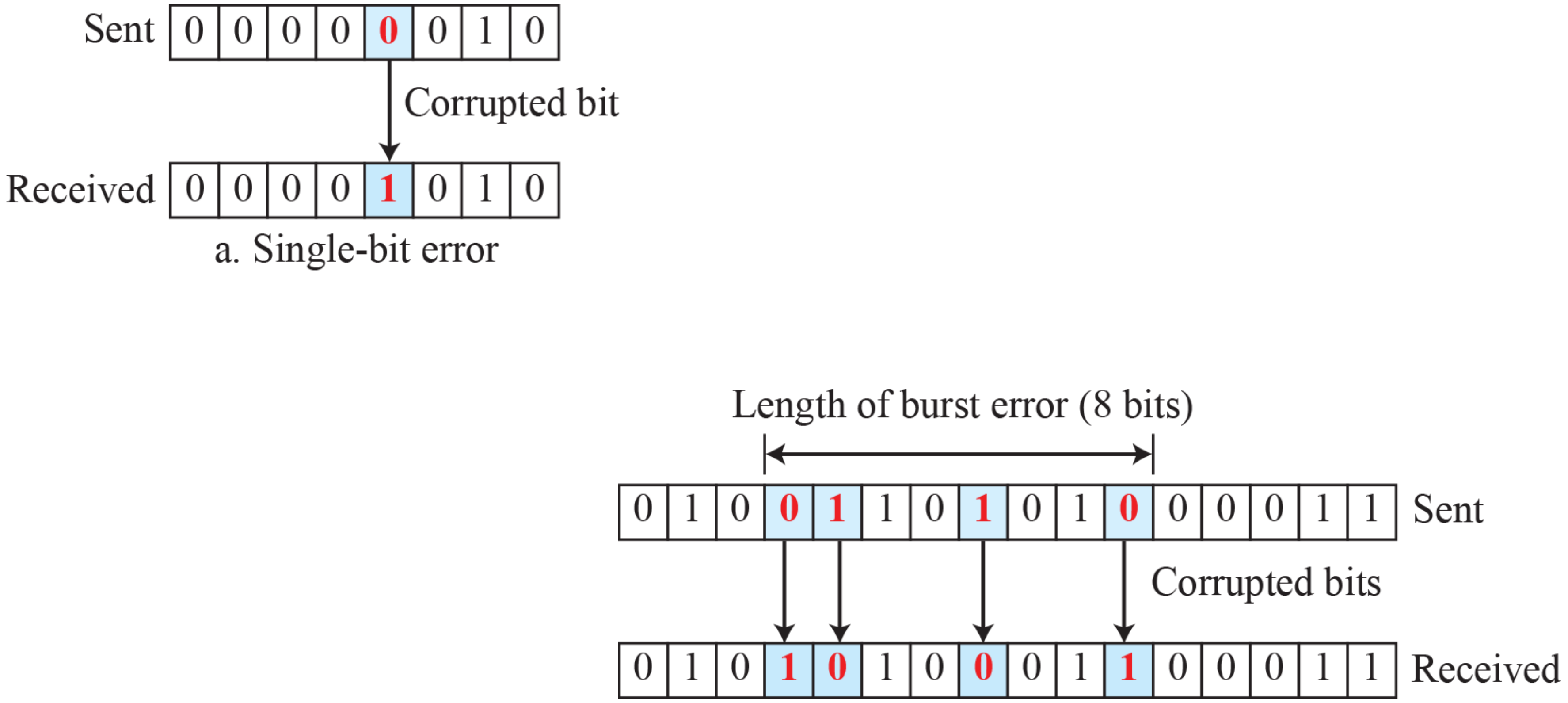
- ❑ Flow Control
- ❑ Error Control

Error Detection and Correction

At the data-link layer, if a frame is corrupted between the two nodes, it needs to be corrected before it continues its journey to other nodes. However, most link-layer protocols simply discard the frame and let the upper-layer protocols handle the retransmission of the frame. Some wireless protocols, however, try to correct the corrupted frame.

- Introduction
  - Types of Errors
  - Redundancy
  - Detection versus Correction
  - Coding
- Cyclic Codes
  - Cyclic Redundancy Check
  - Polynomials
  - Requirement
  - Performance
  - Advantages of Cyclic Codes

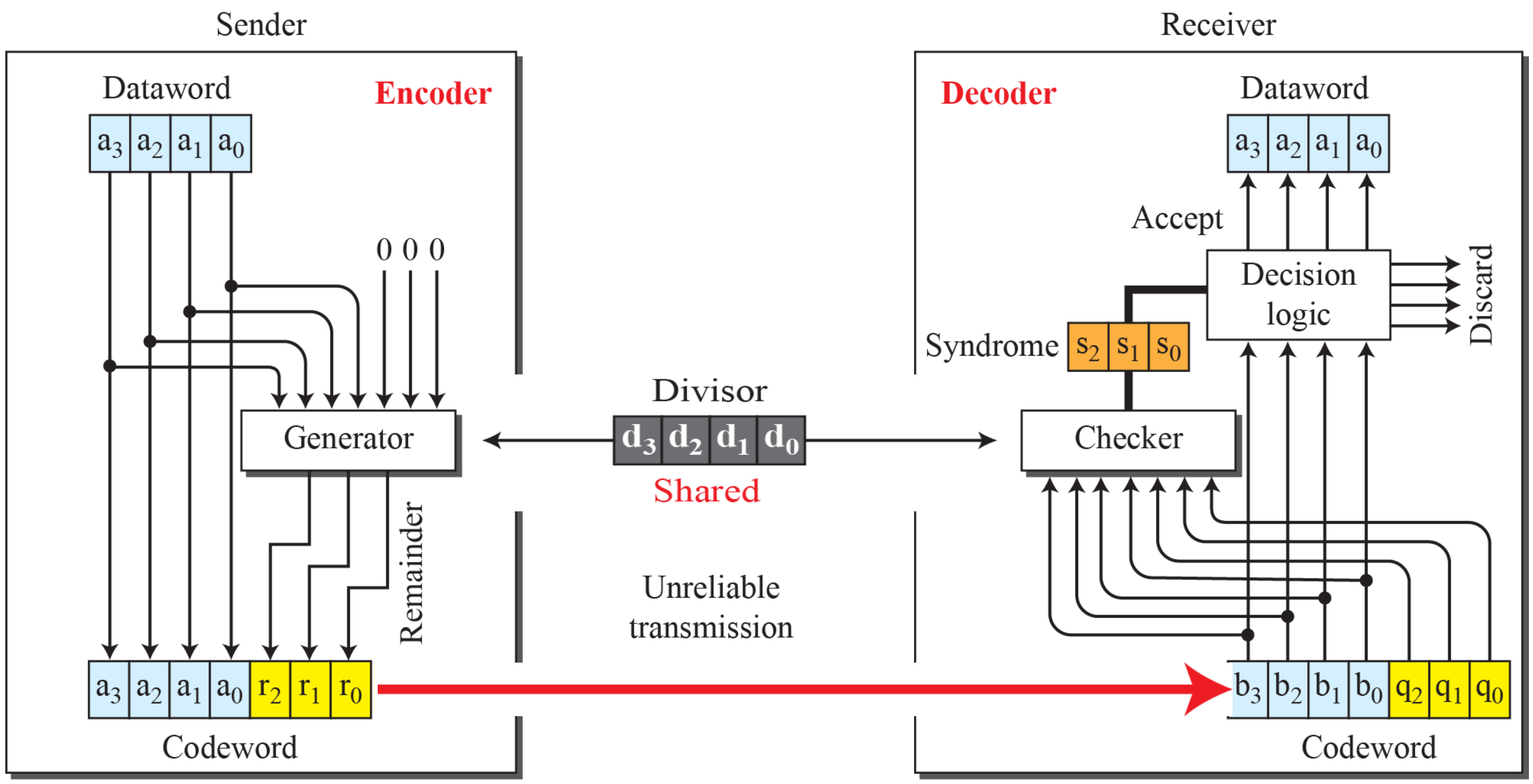
Single-bit and burst error



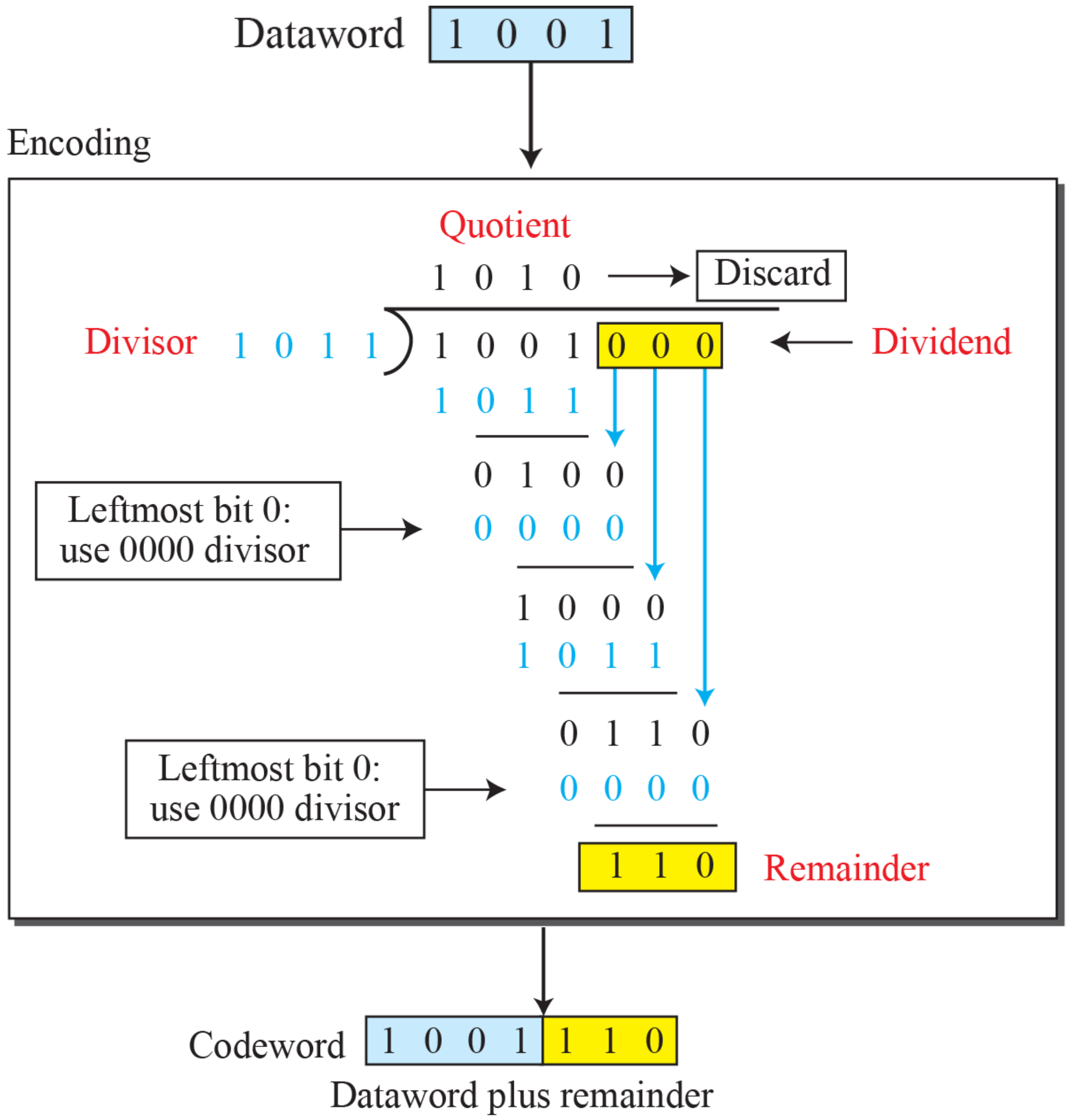
a. Single-bit error

b. Burst error

CRC encoder and decoder



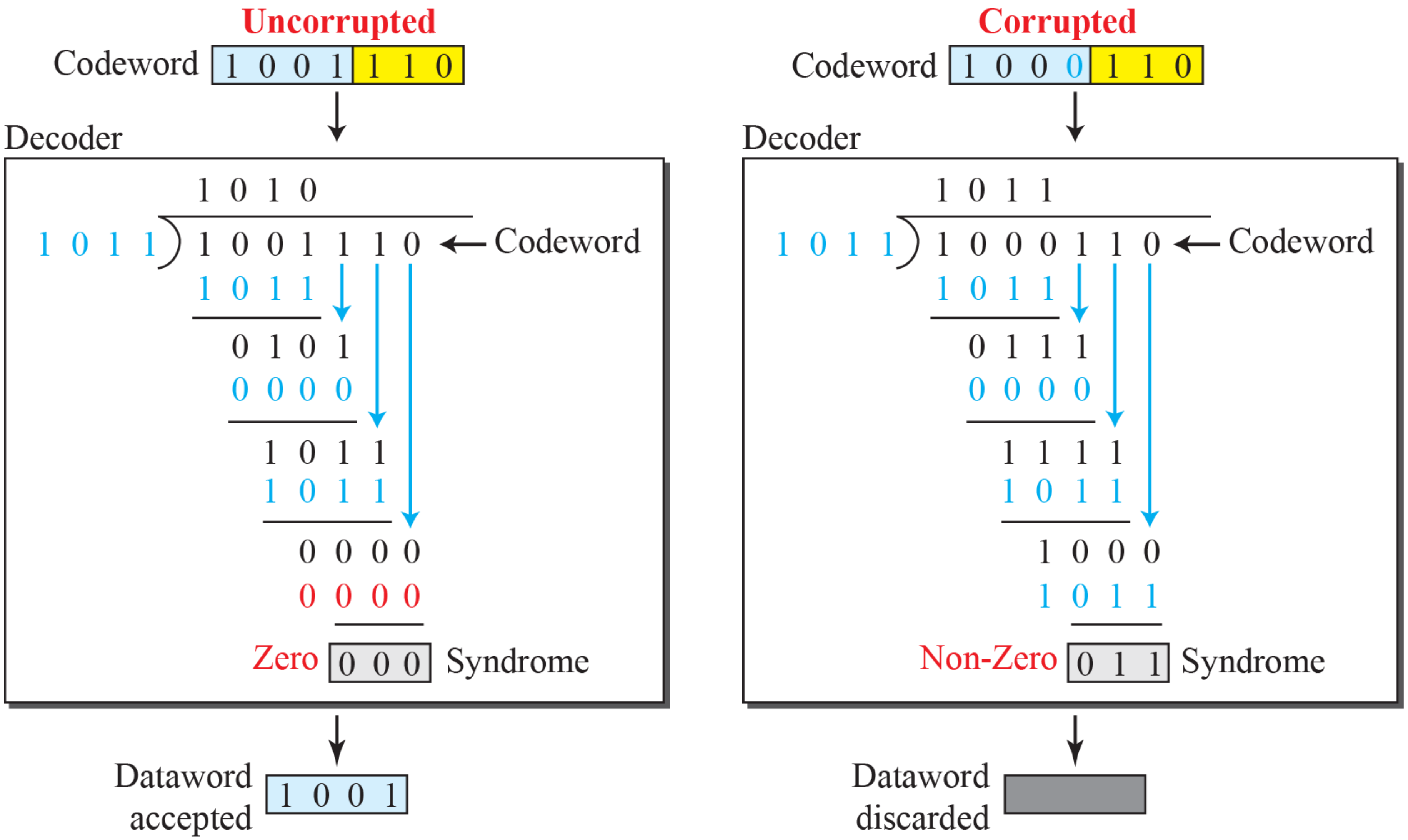
Division in CRC encoder



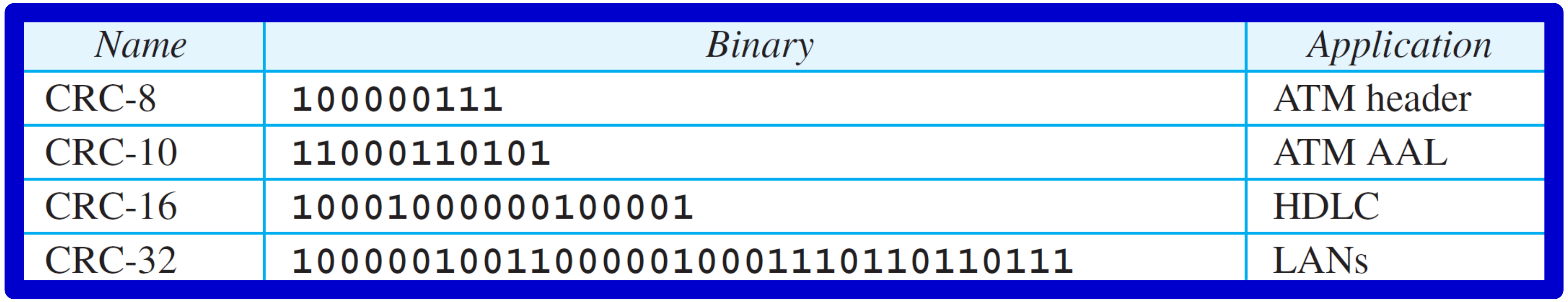
Note:

Multiply: AND
Subtract: XOR

Division in the CRC decoder for two cases



Standard polynomials

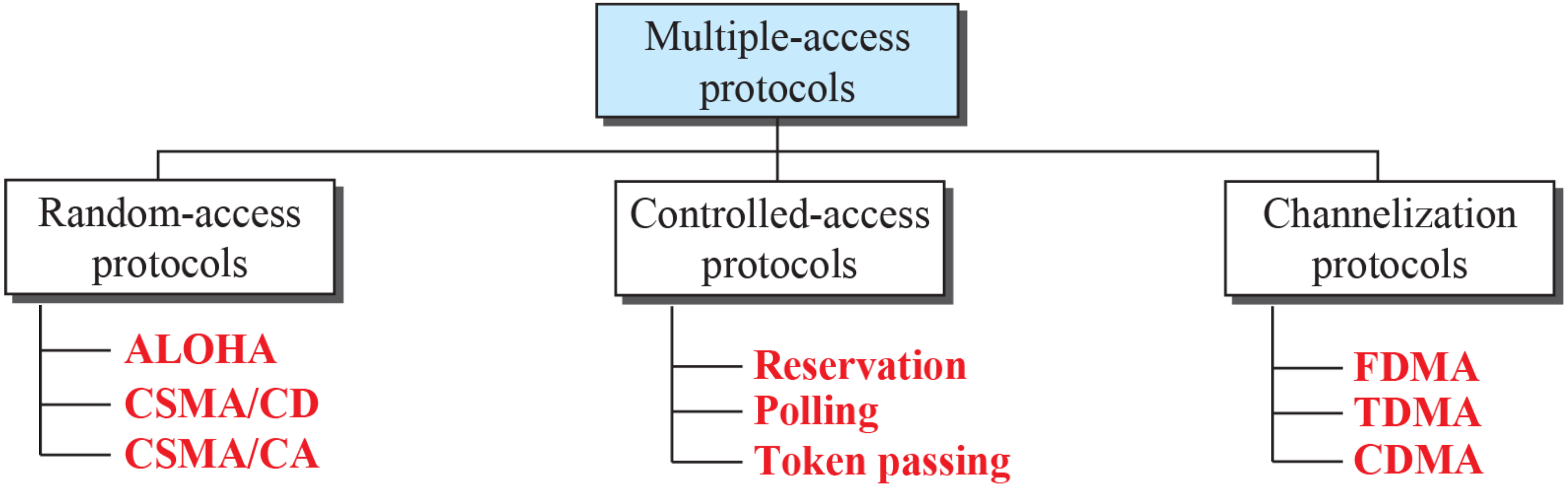


Name	*Binary*	*Application*
CRC-8	100000111	ATM header
CRC-10	11000110101	ATM AAL
CRC-16	10001000000100001	HDLC
CRC-32	100000100110000010001110110110111	LANs

5-3 MULTIPLE ACCESS PROTOCOLS

We said that the data-link layer is divided into two sublayers: data link control (DLC) and media access control (MAC). We discussed DLC in the previous section; we talk about MAC in this section.

Taxonomy of multiple-access protocols



Random Access

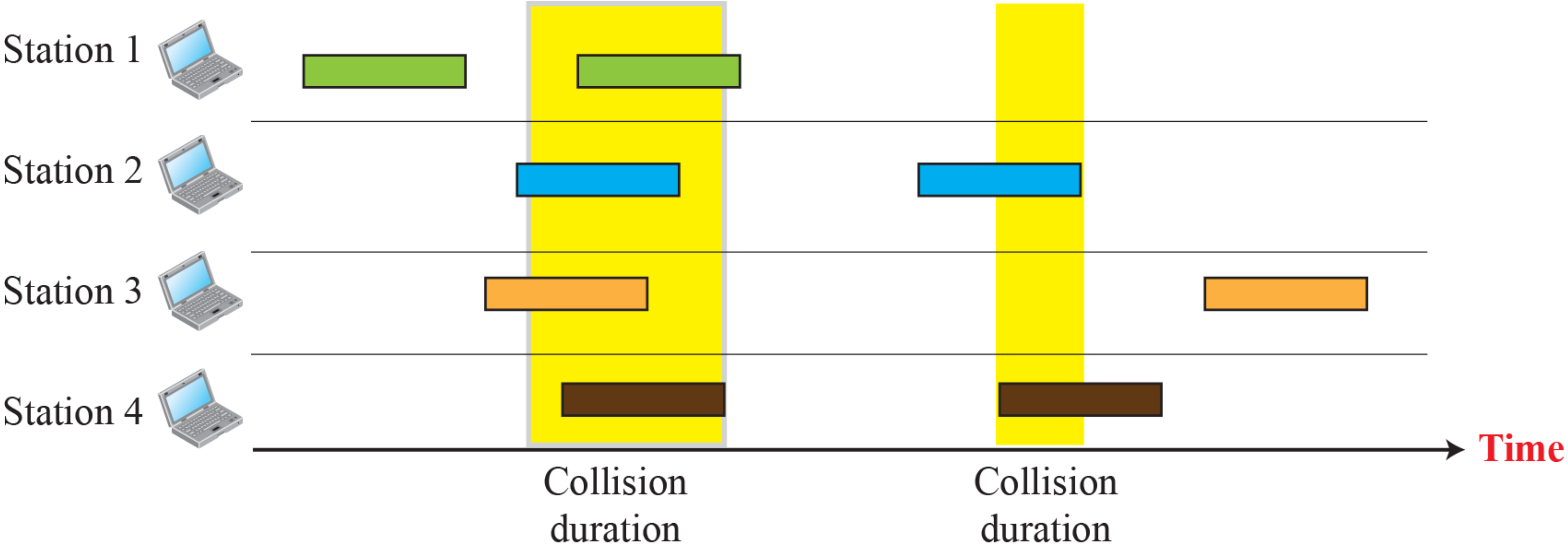
In random-access or contention methods, no station is superior to another station and none is assigned the control over another. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy). In other words, each station can transmit when it desires on the condition that it follows the predefined procedure, including the testing of the state of the medium.

- ALOHA
  - Pure ALOHA
  - Slotted ALOHA
- CSMA
  - Vulnerable Time
  - Persistence Methods
- CSMA/CD
  - Minimum Frame Size
  - Procedure
  - Energy Level
  - Throughput
  - Traditional Ethernet
- CSMA/CA

Pure ALOHA network

- **Pure ALOHA,** the earliest random access method, was developed at the University of Hawaii in early 1970.
- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- The idea is that each station sends a frame whenever it has a frame to send
- there is the possibility of collision between frames from different stations
- The pure ALOHA protocol relies on acknowledgments from the receiver.
- A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again.

Frames in a pure ALOHA network



- Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the *backoff time T_B.*
- The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations or the average time required to send out a frame ($2 \times T_p$) or ($2 \times T_{fr}$) .
- After a maximum number of retransmission attempts K_{max}, a station must give up and try later.
- The formula for T_B depends on the implementation. One common formula is the ***binary exponential backoff.*** In this method, for each retransmission, a multiplier R = 0 to $2^K - 1$ is randomly chosen and multiplied by T_p *or* T_{fr}

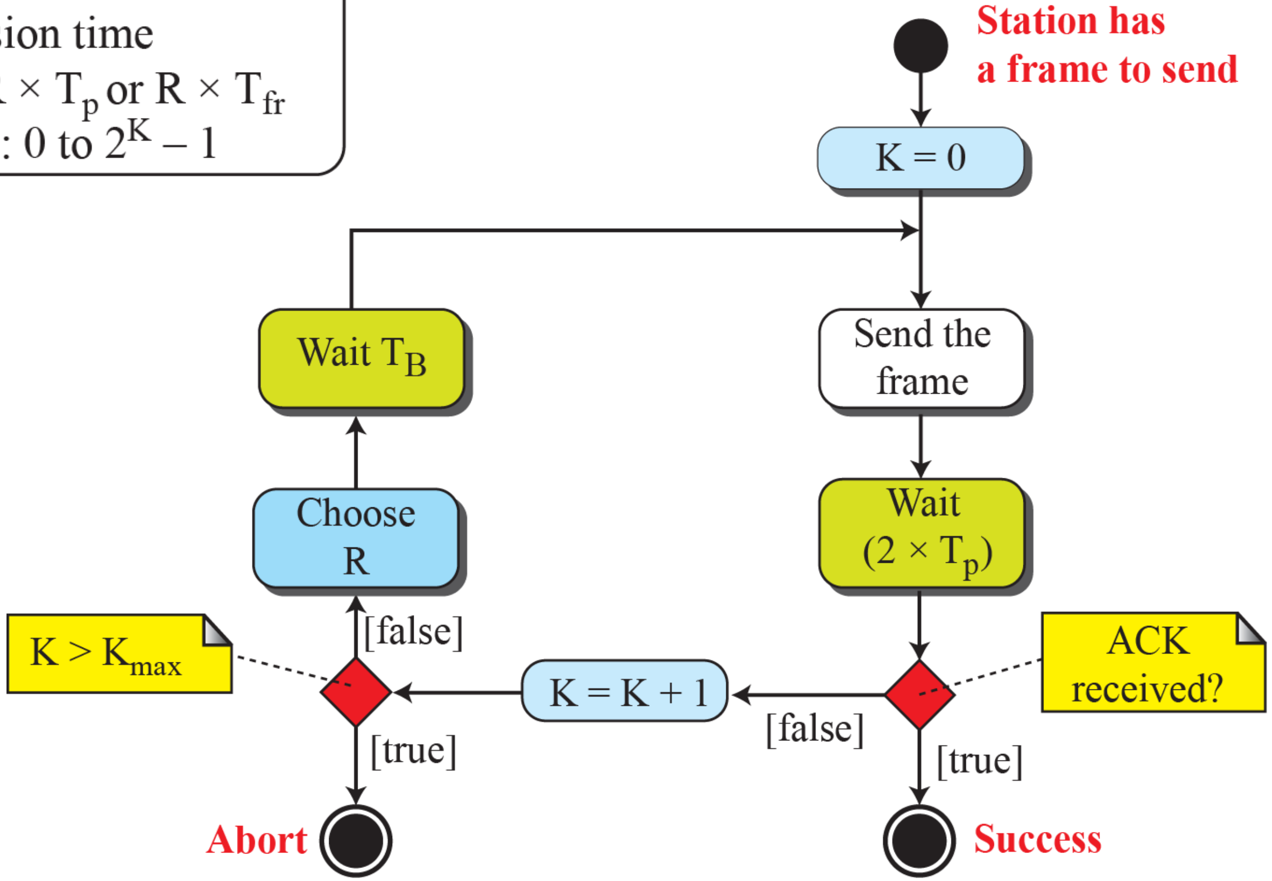
Procedure for pure ALOHA protocol

Legend

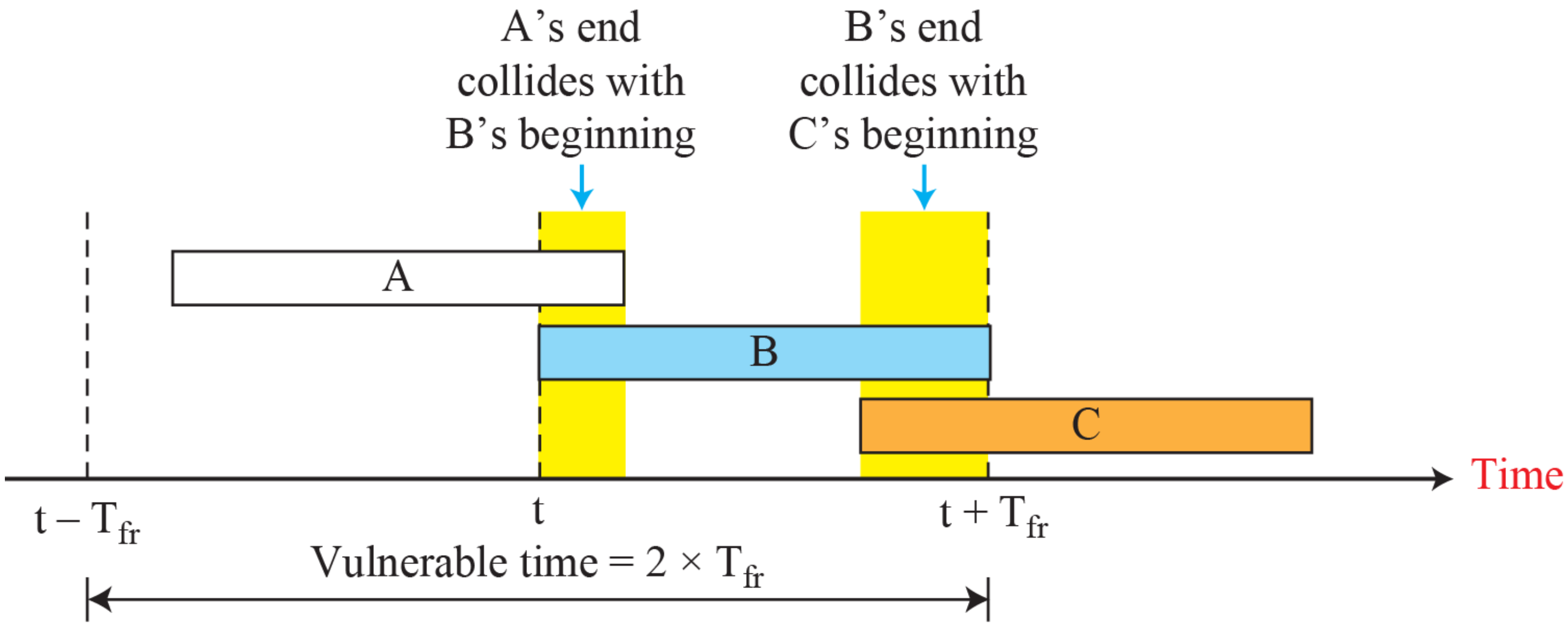
K : Number of attempts
T_p : Maximum propagation time
T_{fr}: Average transmission time
T_B: (Back-off time): $R \times T_p$ or $R \times T_{fr}$
R : (Random number): 0 to $2^K - 1$

Maximum Throughput $S = G \times e^{-2G}$
when G=1/2 → S_{max}= 0.184

Vulnerable time = $2 * T_{fr}$



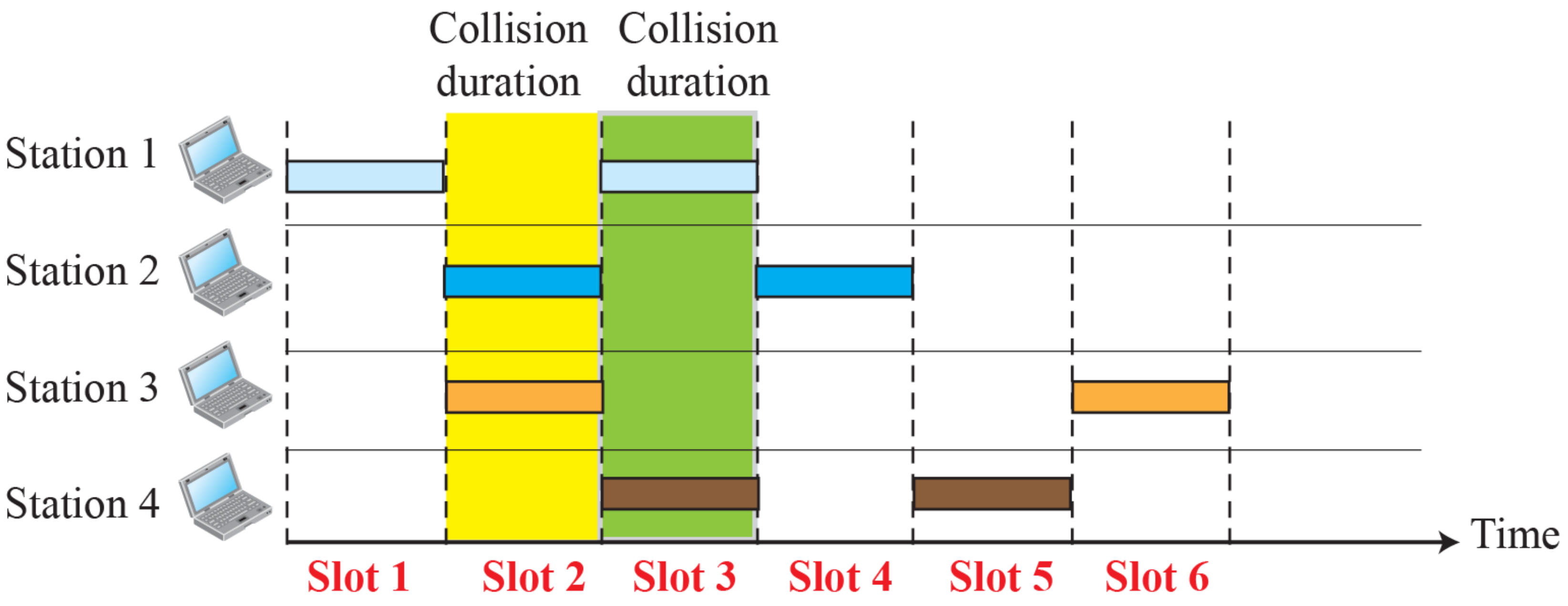
Vulnerable time for pure ALOHA protocol


A's end collides with B's beginning
B's end collides with C's beginning
A
B
C
Time
t – T_{fr}
t
t + T_{fr}
Vulnerable time = 2 × T_{fr}

Slotted ALOHA network

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In **slotted ALOHA** we divide the time into slots of T_{fr} seconds and force the station to send only at the beginning of the time slot
- Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot.
- The Slotted ALOHA protocol relies on acknowledgments from the receiver.
- A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again.
- The vulnerable time is now reduced to one-half, equal to T_{fr}

Frames in a slotted ALOHA network

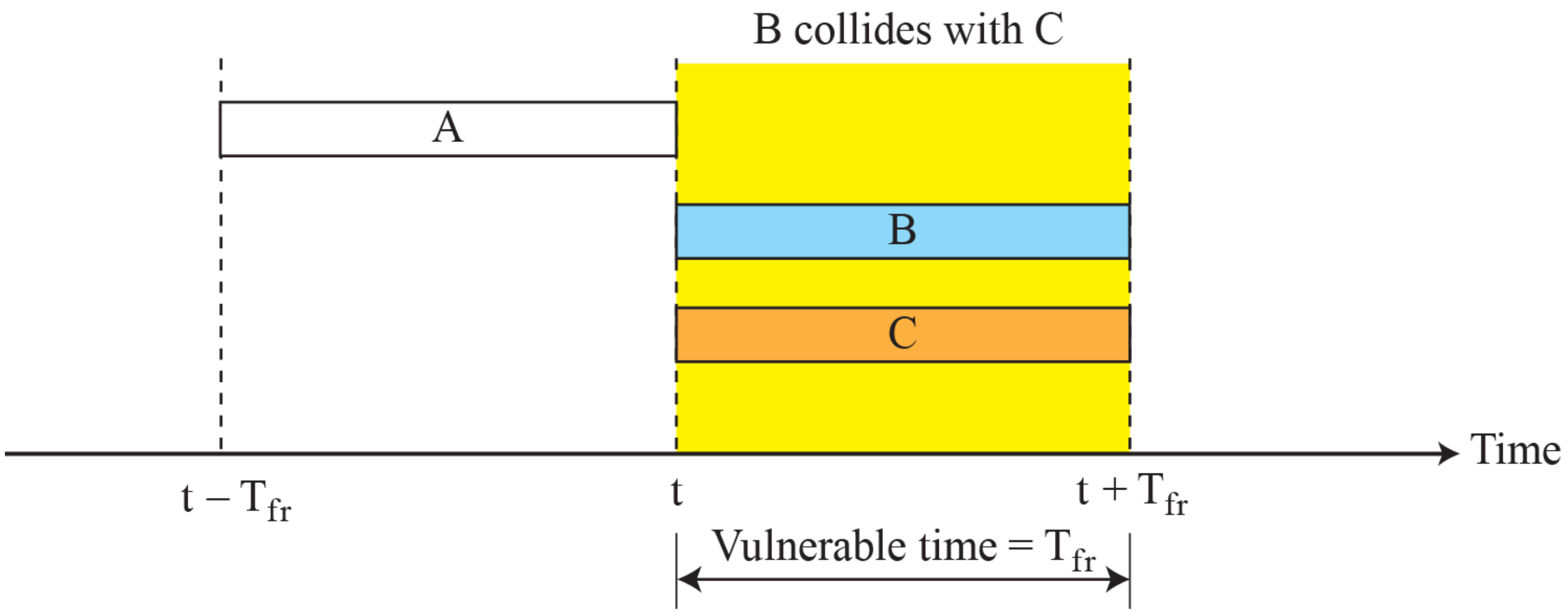


Maximum Throughput $S = G \times e^{-G}$

when G=1 → $S_{max} = 0.36$

Vulnerable time = T_{fr}

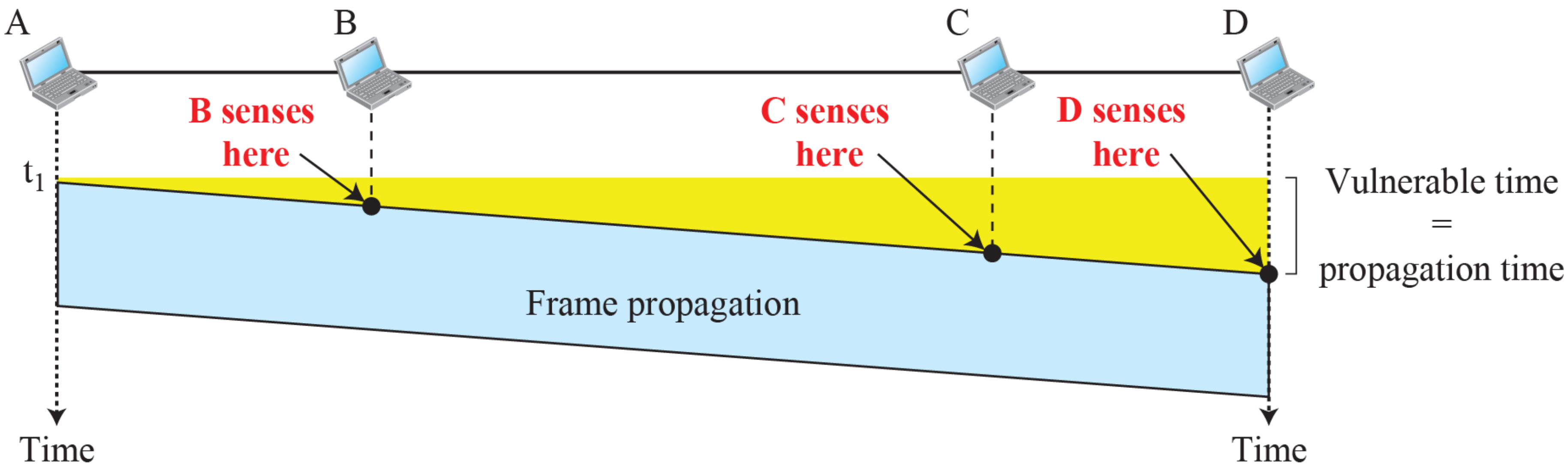
Figure 5.33: Vulnerable time for slotted ALOHA protocol



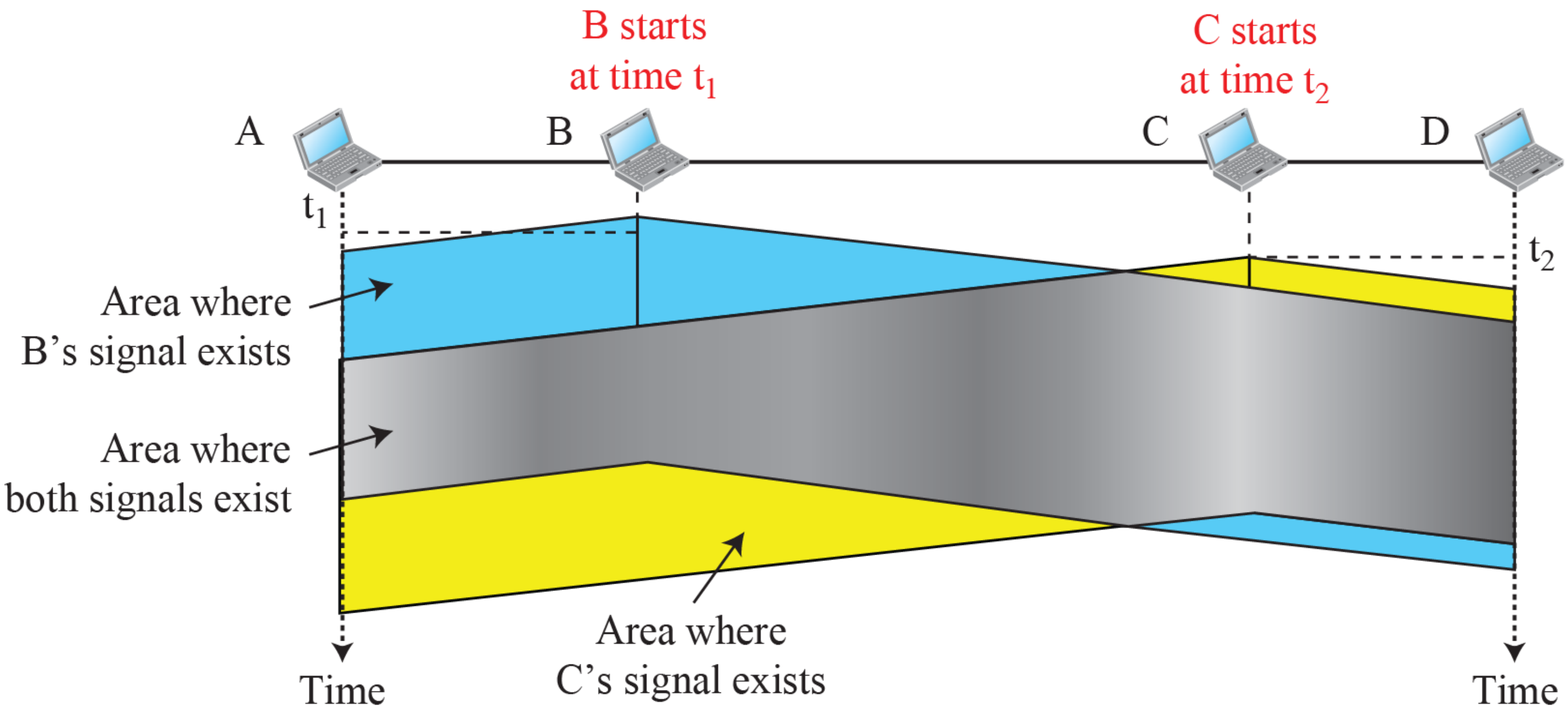
Carrier sense multiple access(*CSMA)*

- **Carrier sense multiple access (CSMA)** requires that each station first listen to the medium (or check the state of the medium) before sending.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.
- The possibility of collision still exists because of propagation delay.
- The vulnerable time for CSMA is the ***propagation time*** T_p.
- A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again.
- The vulnerable time is now reduced to one-half, equal to T_{fr}

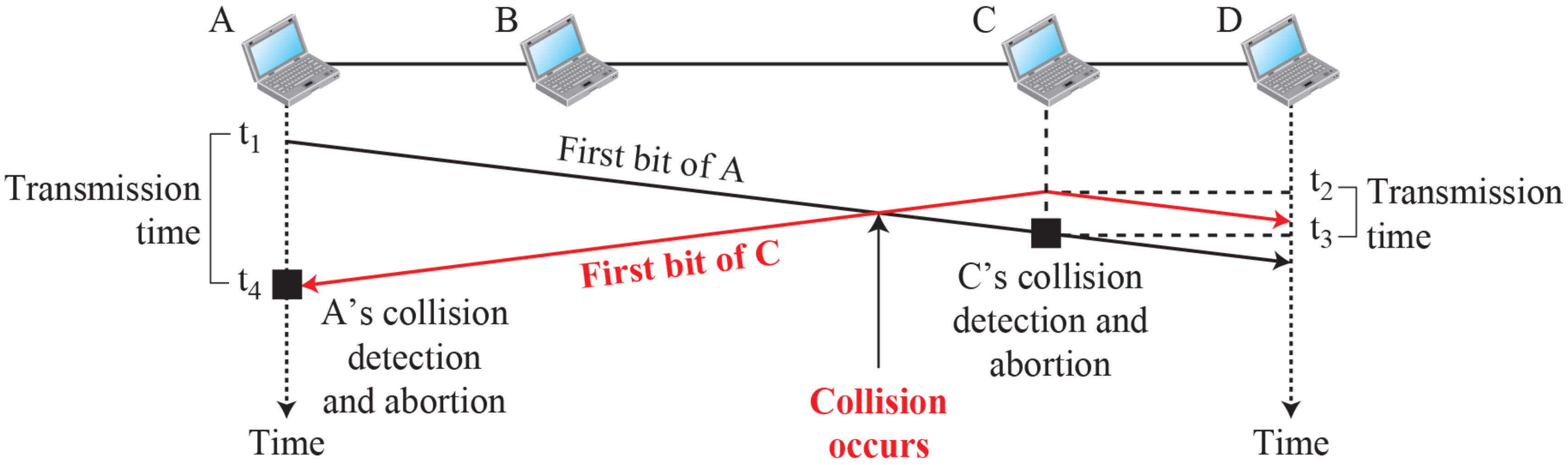
Vulnerable time in CSMA



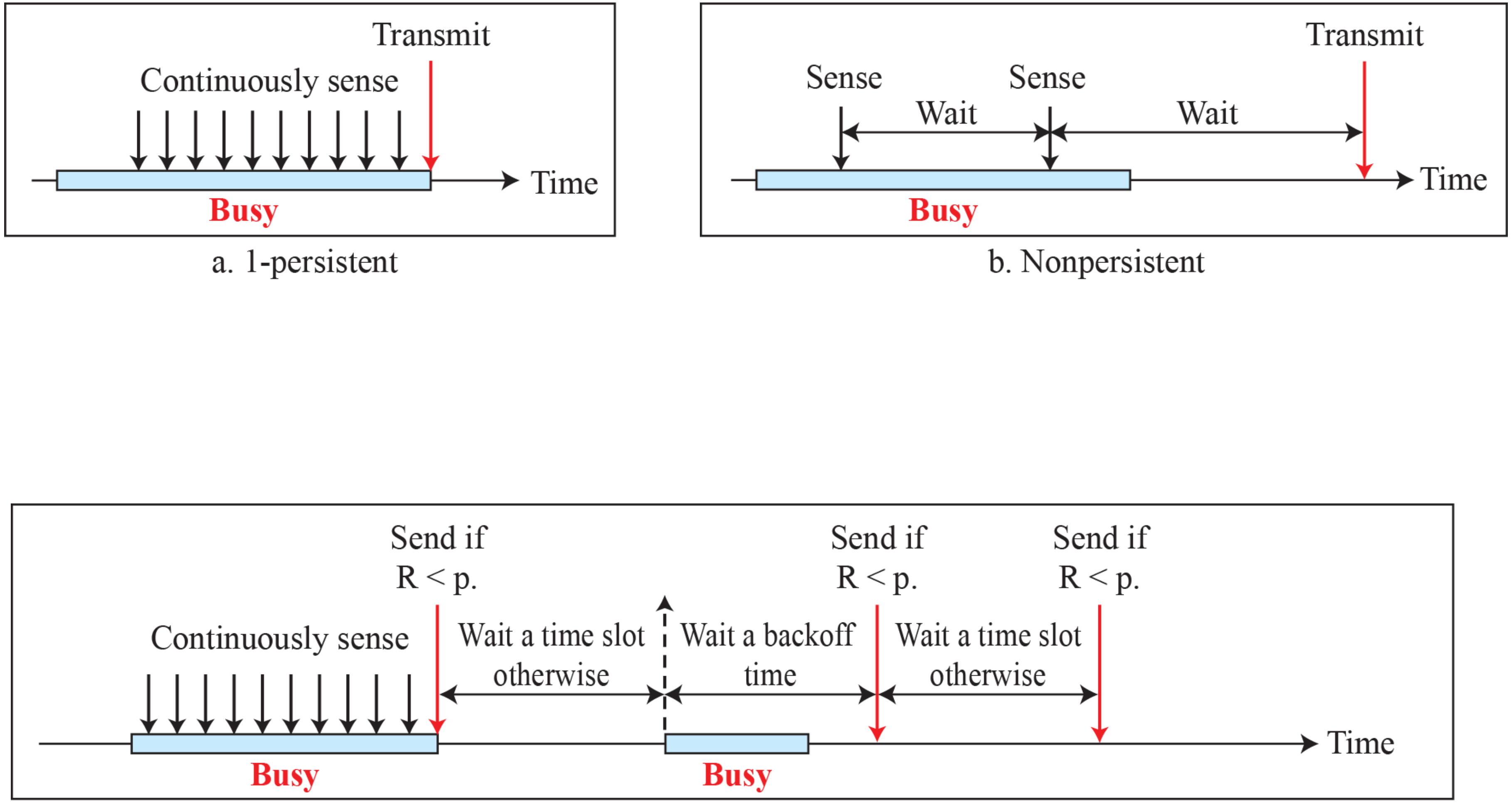
Space/time model of a collision in CSMA



Collision of the first bits in CSMA/CD



Behavior of three persistence methods

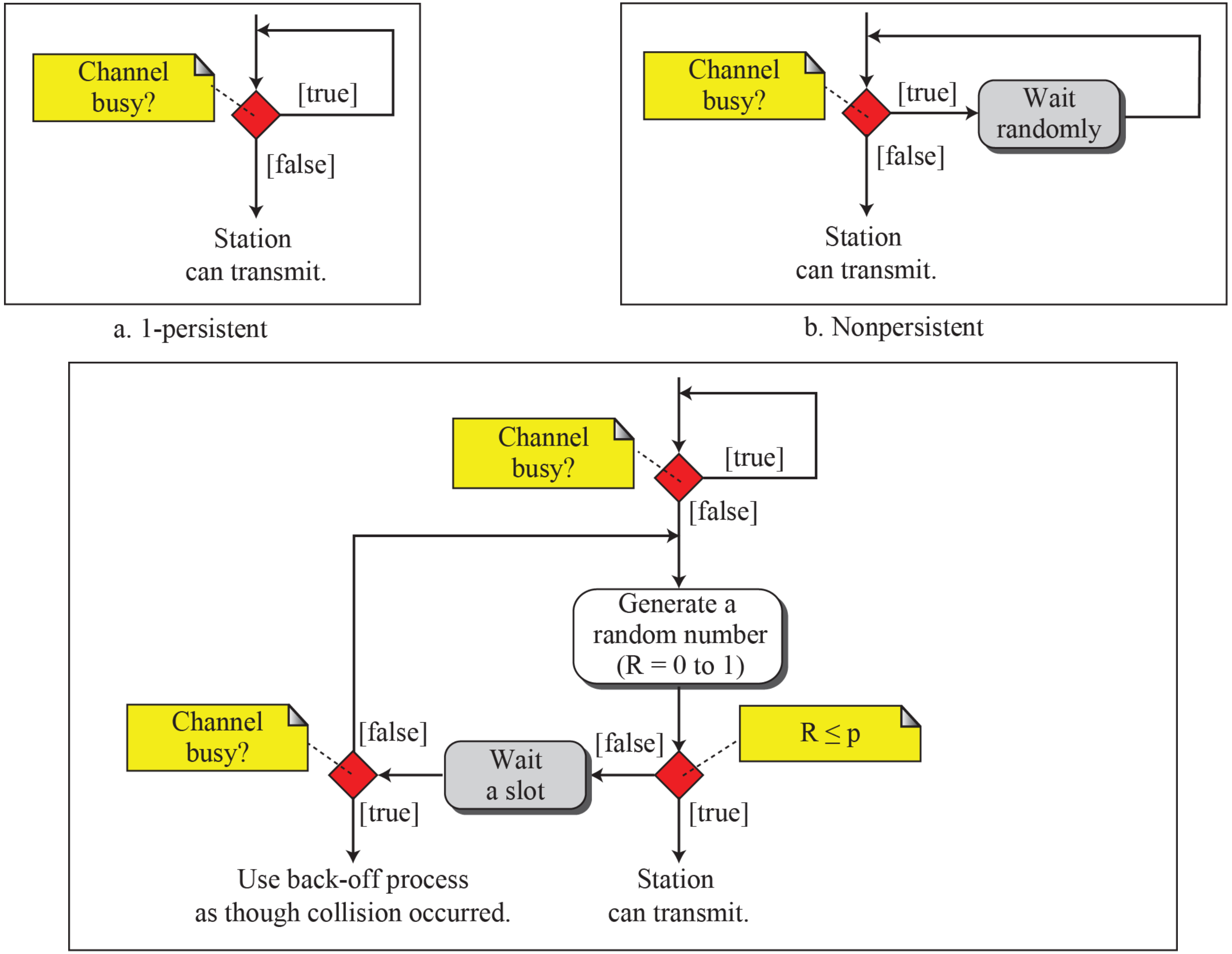


a. 1-persistent

b. Nonpersistent

c. *p*-persistent

Flow diagram for three persistence methods



a. 1-persistent

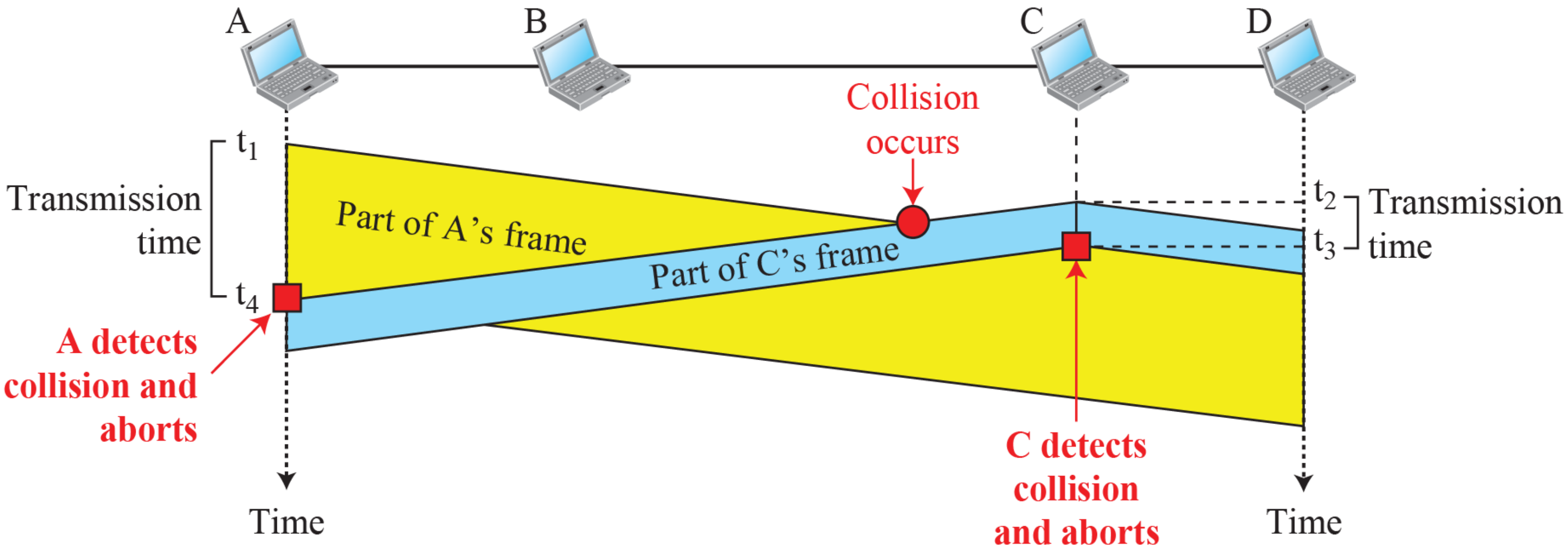
b. Nonpersistent

c. *p*-persistent

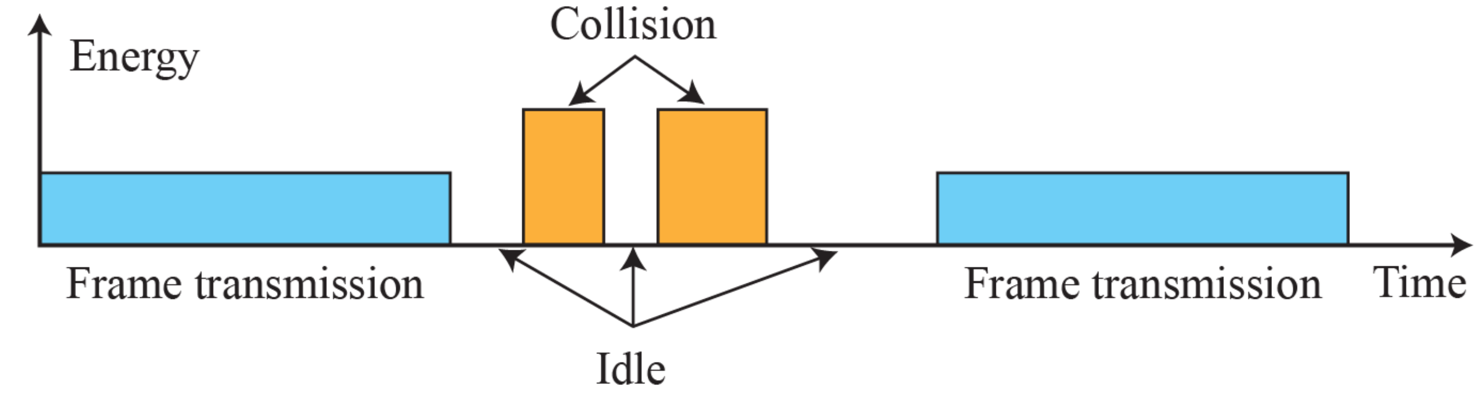
Carrier Sense Multiple Access/ Collision Detection (*CSMA/CD)*

- The CSMA method does not specify the procedure following a collision.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.
- For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.
- This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time T_{fr} must be at least two times the maximum propagation time T_p.
- One of the LAN protocols that used CSMA/CD is the traditional Ethernet with the data rate of 10 Mbps.

Collision and abortion in CSMA/CD



Energy level during transmission, idleness, or collision



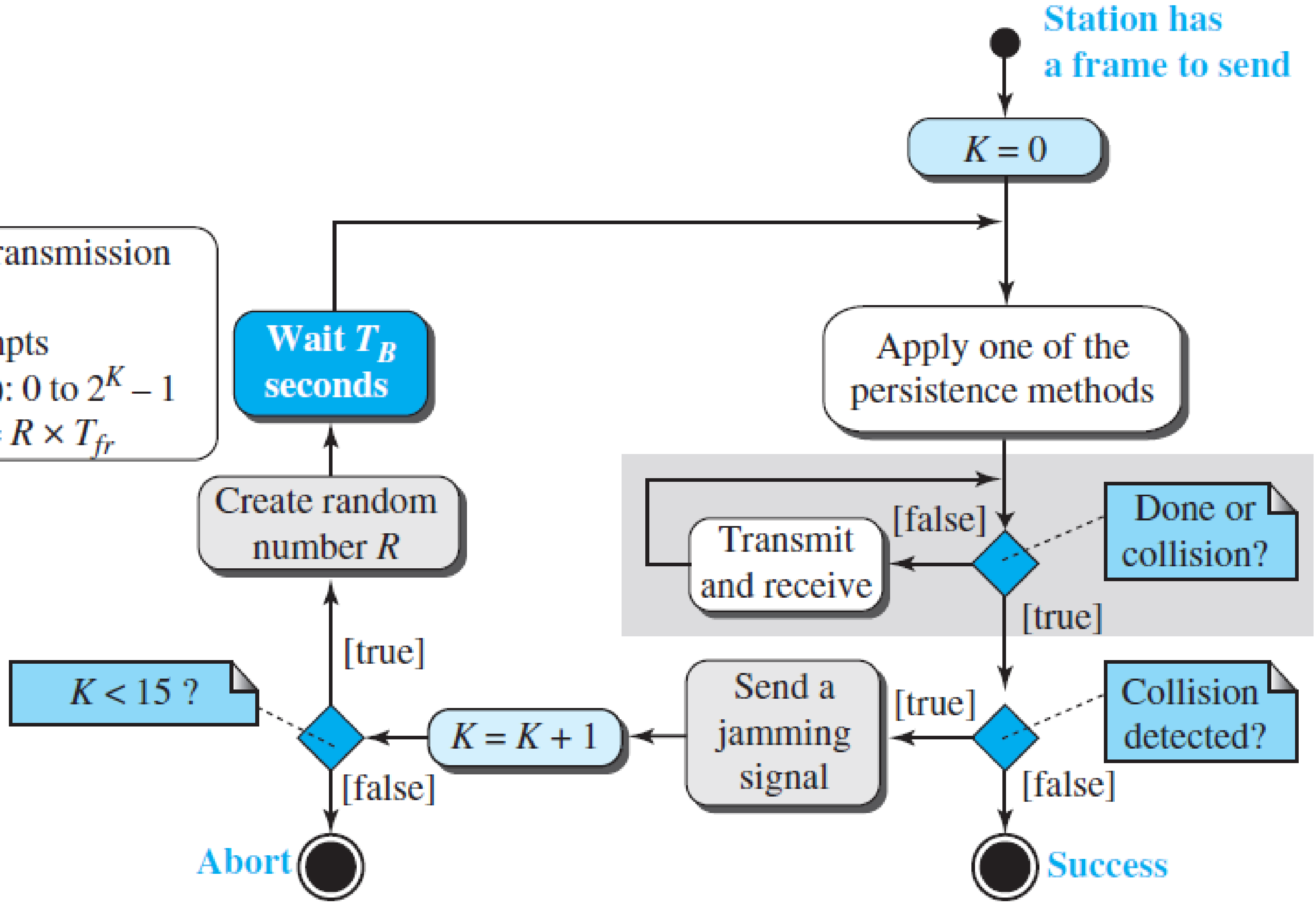
Procedure

- It is similar to the one for the ALOHA protocol, but there are differences.
  - The first difference is the addition of the persistence process
  - The second difference is the frame transmission and acknowledgement
    - CSMA/CD → No ack. i.e. either transmission is finished or a collision is detected. Either event stops transmission.
- The third difference is the sending of a short jamming signal to make sure that all other stations become aware of the collision.

Flow diagram for the CSMA/CD

Legend

T_{fr}: Frame average transmission time
K : Number of attempts
R : (random number): 0 to $2^K - 1$
T_B: (Backoff time) = $R \times T_{fr}$



Carrier Sense Multiple Access/ Collision Avoidance (*CSMA/CA)*

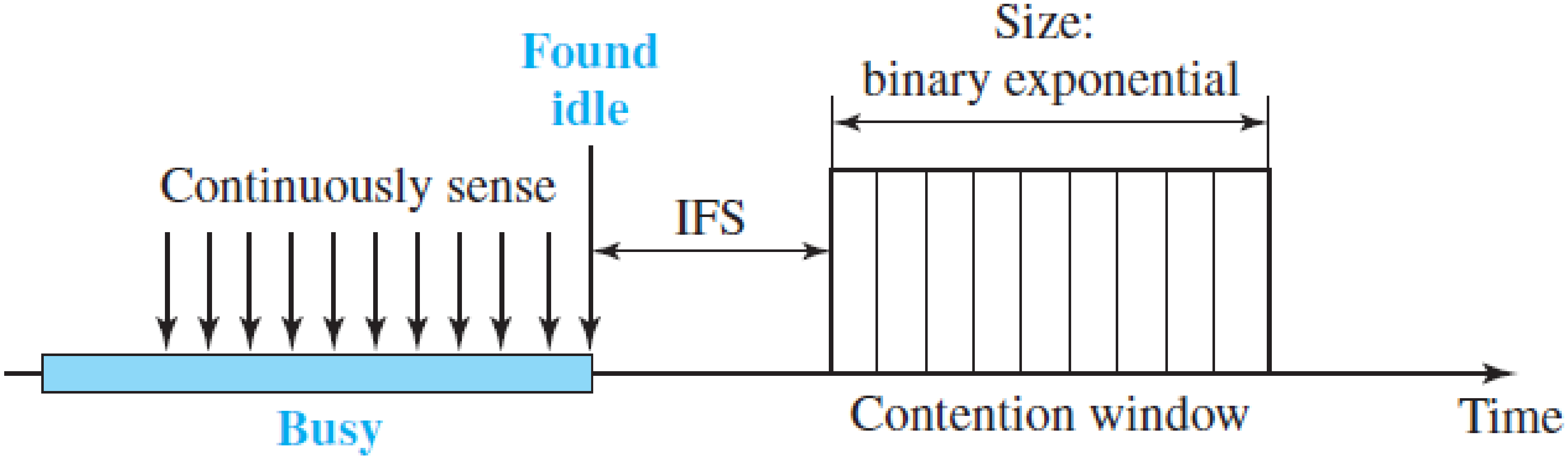
- **CSMA/CA** was invented for wireless networks.
- Collisions are avoided through the use of CSMA/CA's three strategies:
  - Interframe space,
  - Contention window
  - Acknowledgments

Interframe space

First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the ***interframe space*** or ***IFS.*** The IFS time allows the front of the transmitted signal by the distant station to reach this station. After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window.

Contention window

The **contention window** is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy. One interesting point about the contention window is that the station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.



Acknowledgments

With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

Frame Exchange Time Line

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

a. The channel uses a persistence strategy with backoff until the channel is idle.

b. After the station is found to be idle, the station waits for a period of time called the ***DCF interframe space (DIFS);*** then the station sends a control frame called the ***request to send (RTS)*****.**

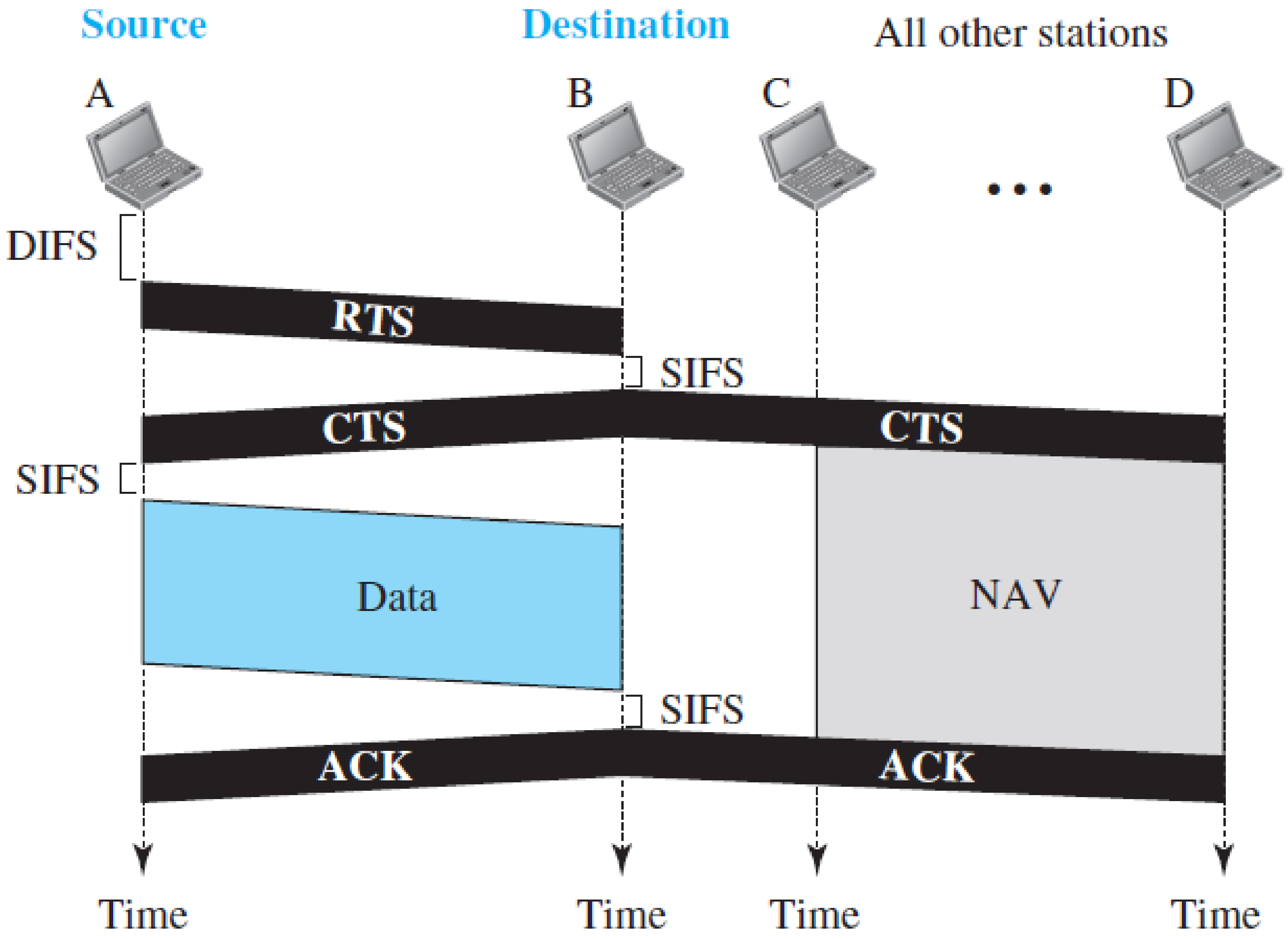
2. After receiving the RTS and waiting a period of time called the ***short interframe space (SIFS),*** the destination station sends a control frame, called the ***clear to send (CTS****),* to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.

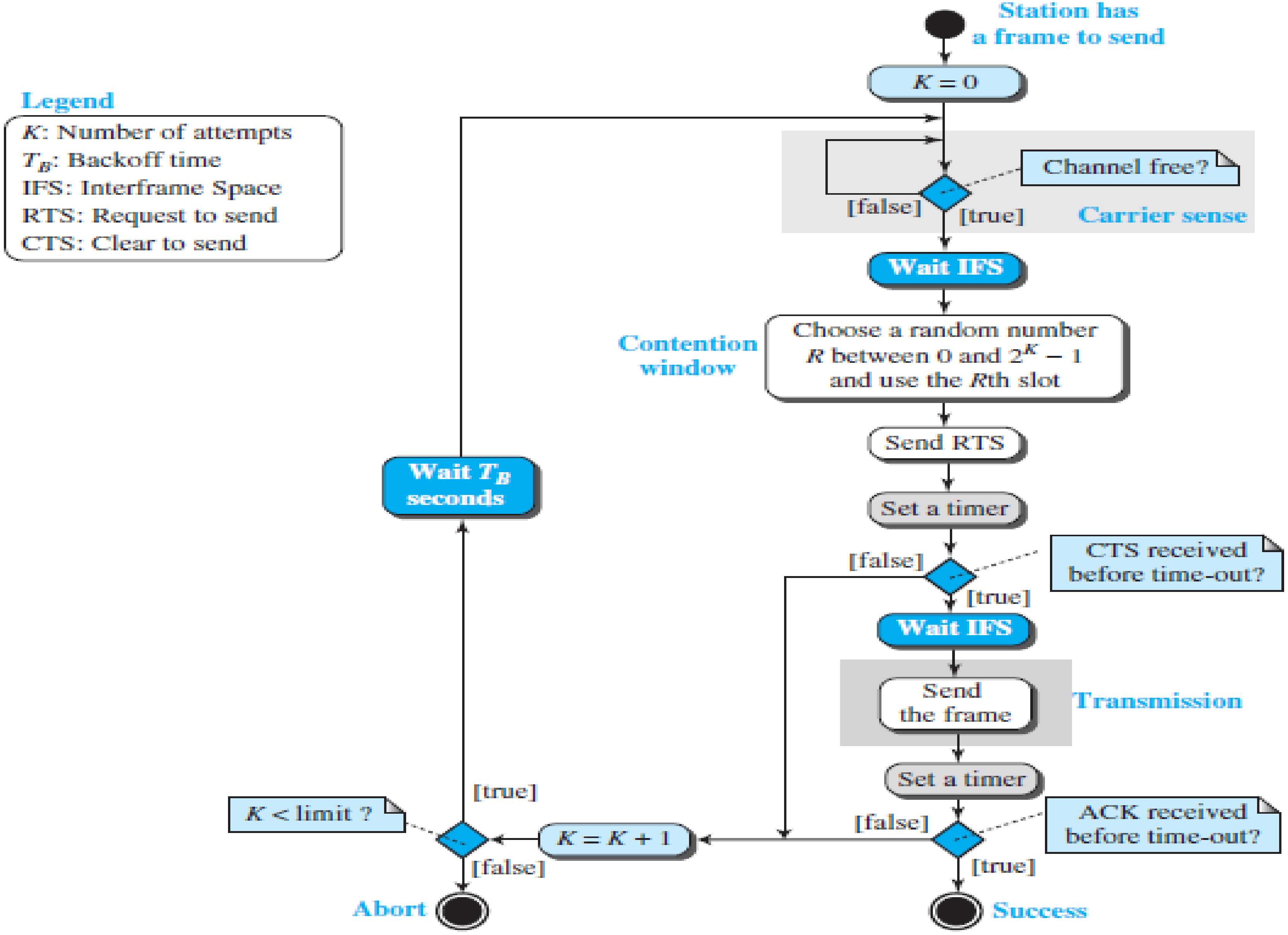
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

Network Allocation Vector

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a **network allocation vector (NAV)** that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired..


Source
Destination
All other stations
A
B
C
D
DIFS
RTS
SIFS
CTS
CTS
SIFS
Data
NAV
SIFS
ACK
ACK
Time
Time
Time
Time

Flow diagram for the CSMA/CA



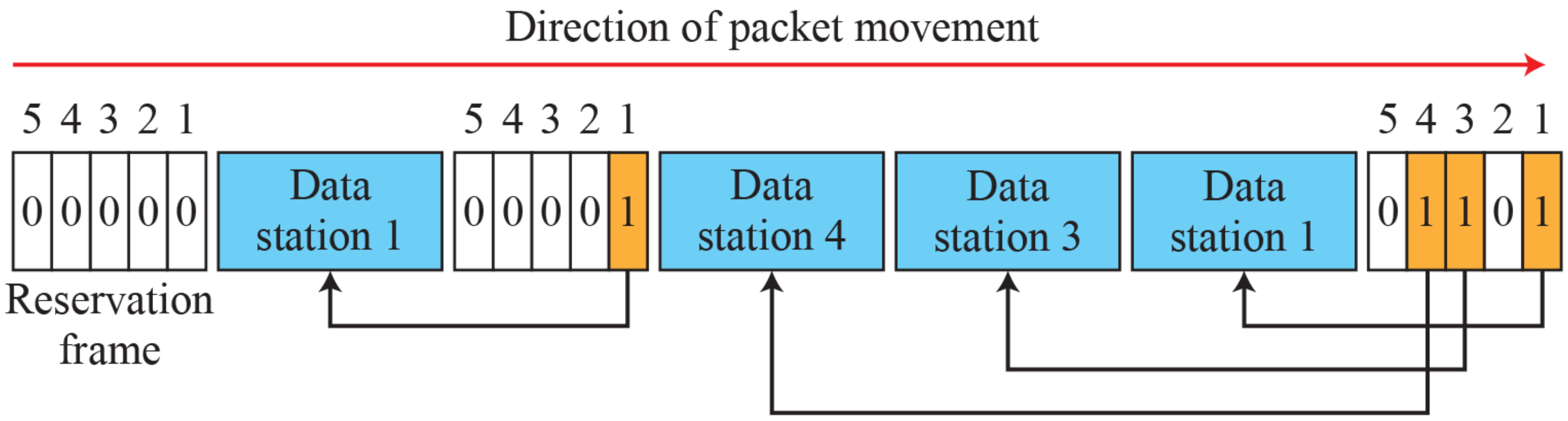
Controlled Access

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

- Reservation
- Polling
  - Select
  - Poll
- Token Passing
  - Logical Ring

Reservation access method

- A station needs to make a reservation before sending data.
- Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.
- If there are *N* stations in the system, there are exactly *N* reservation minislots in the reservation frame. Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame.



Polling-access method

- **Polling** works with topologies in which one device is designated as a ***primary station*** and the other devices are ***secondary stations*.**
- All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions.
- It is up to the primary device to determine which device is allowed to use the channel at a given time
- The drawback is if the primary station fails, the system goes down.

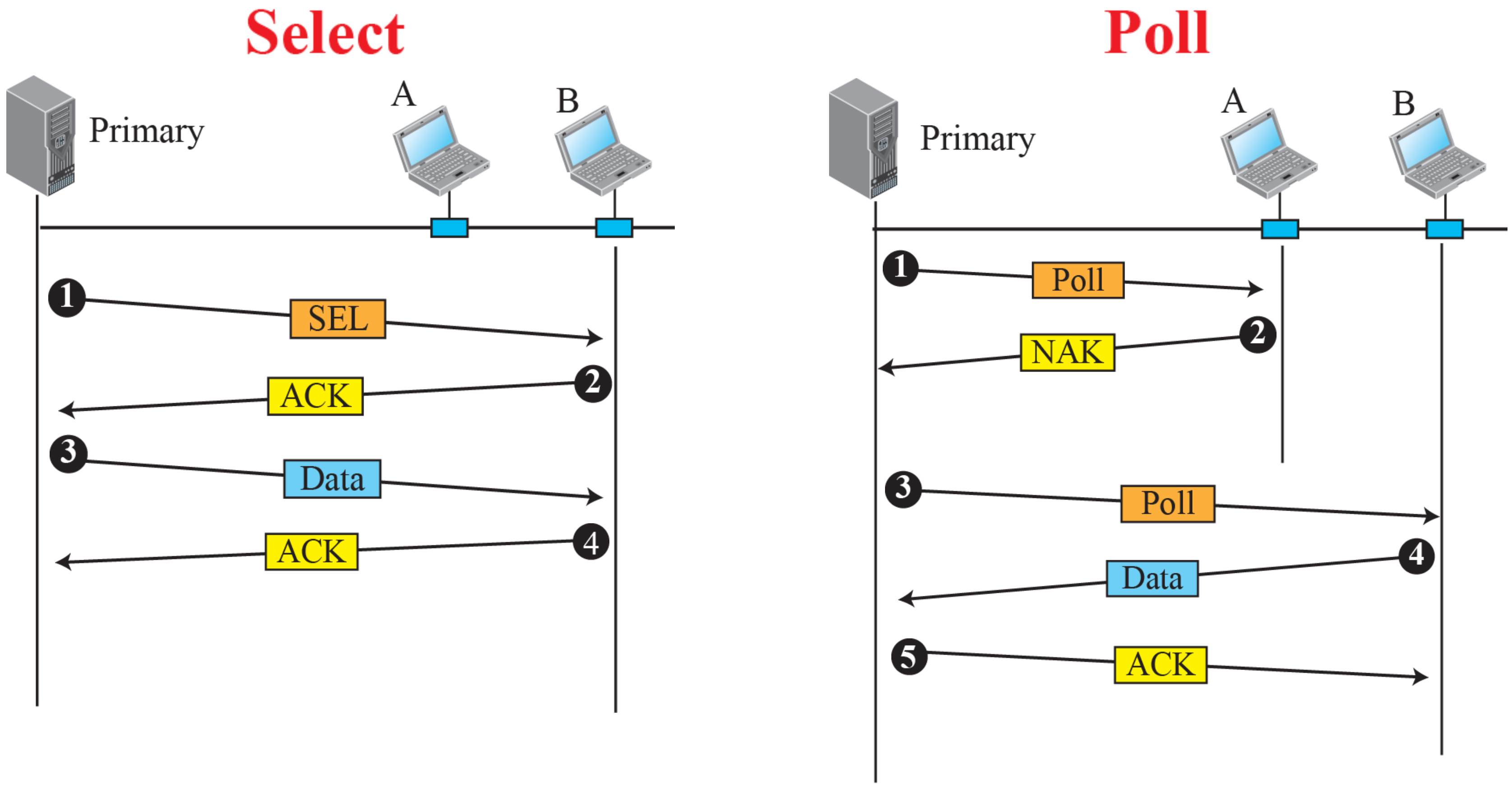
Select

The *select* function is used whenever the primary device has something to send. Remember that the primary controls the link. If the primary is neither sending nor receiving data, it knows the link is available. If it has something to send, the primary device sends it.

Poll

The *poll* function is used by the primary device to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send. When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data.

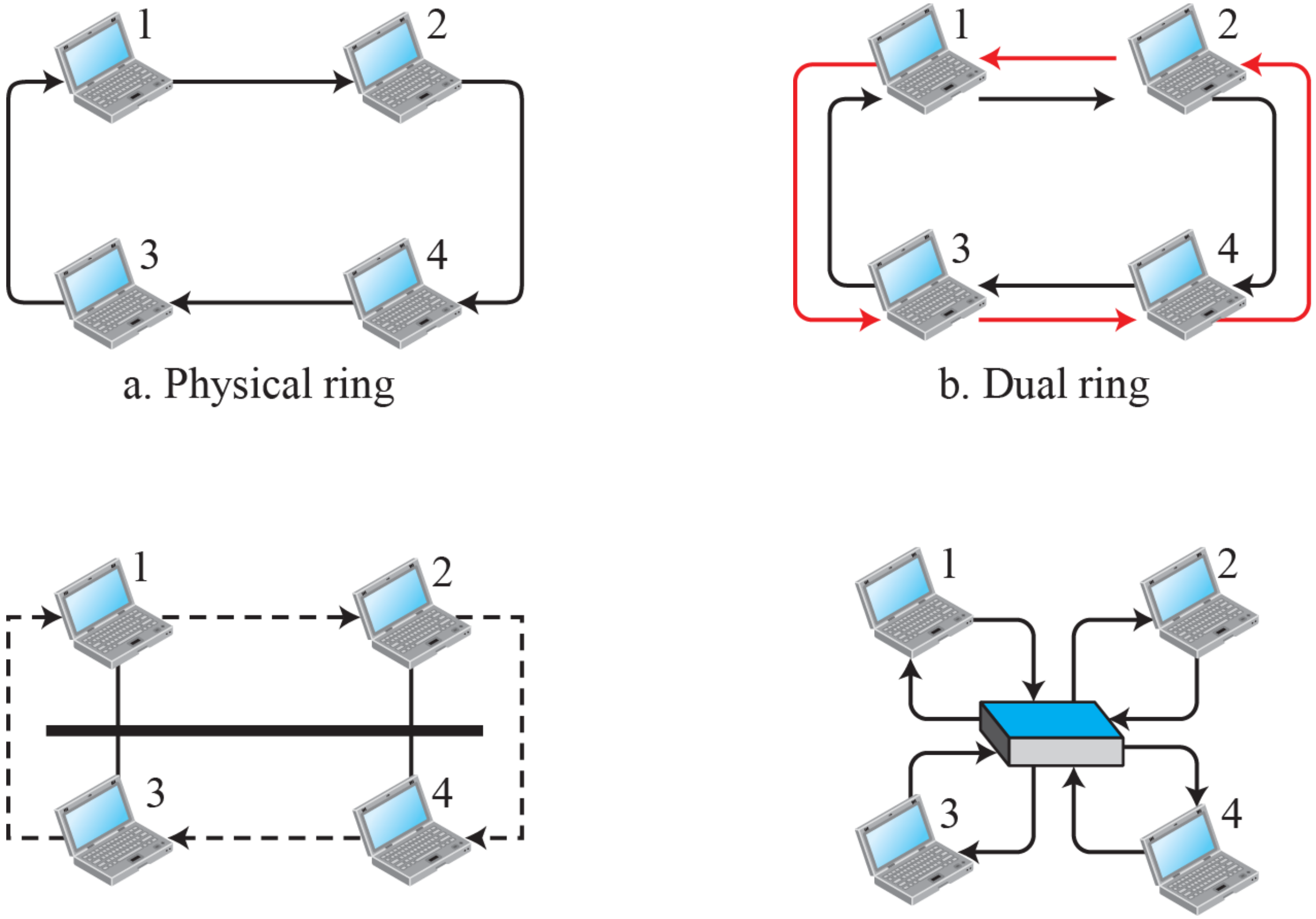
Select and poll functions in polling-access method



Token-passing access method

- The **token-passing** method, the stations in a network are organized in a logical ring.
- For each station, there is a *predecessor* and a *successor*. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now.
- In this method, a special packet called a ***token*** circulates through the ring.
- The possession of the token gives the station the right to access the channel and send its data.
- When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round.
- In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one.

Logical ring and physical topology in token-passing access method



a. Physical ring

b. Dual ring

c. Bus ring

d. Star ring