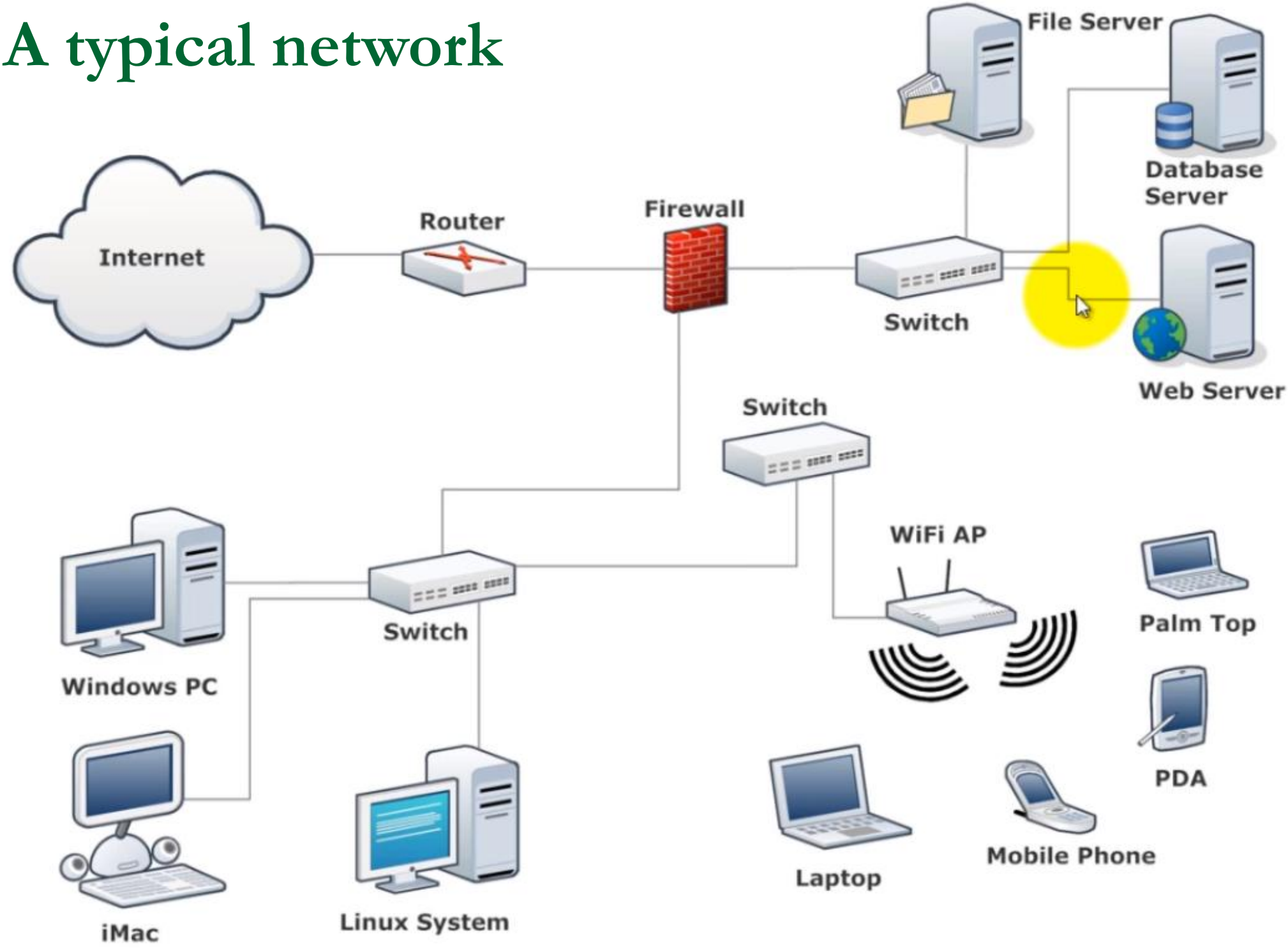
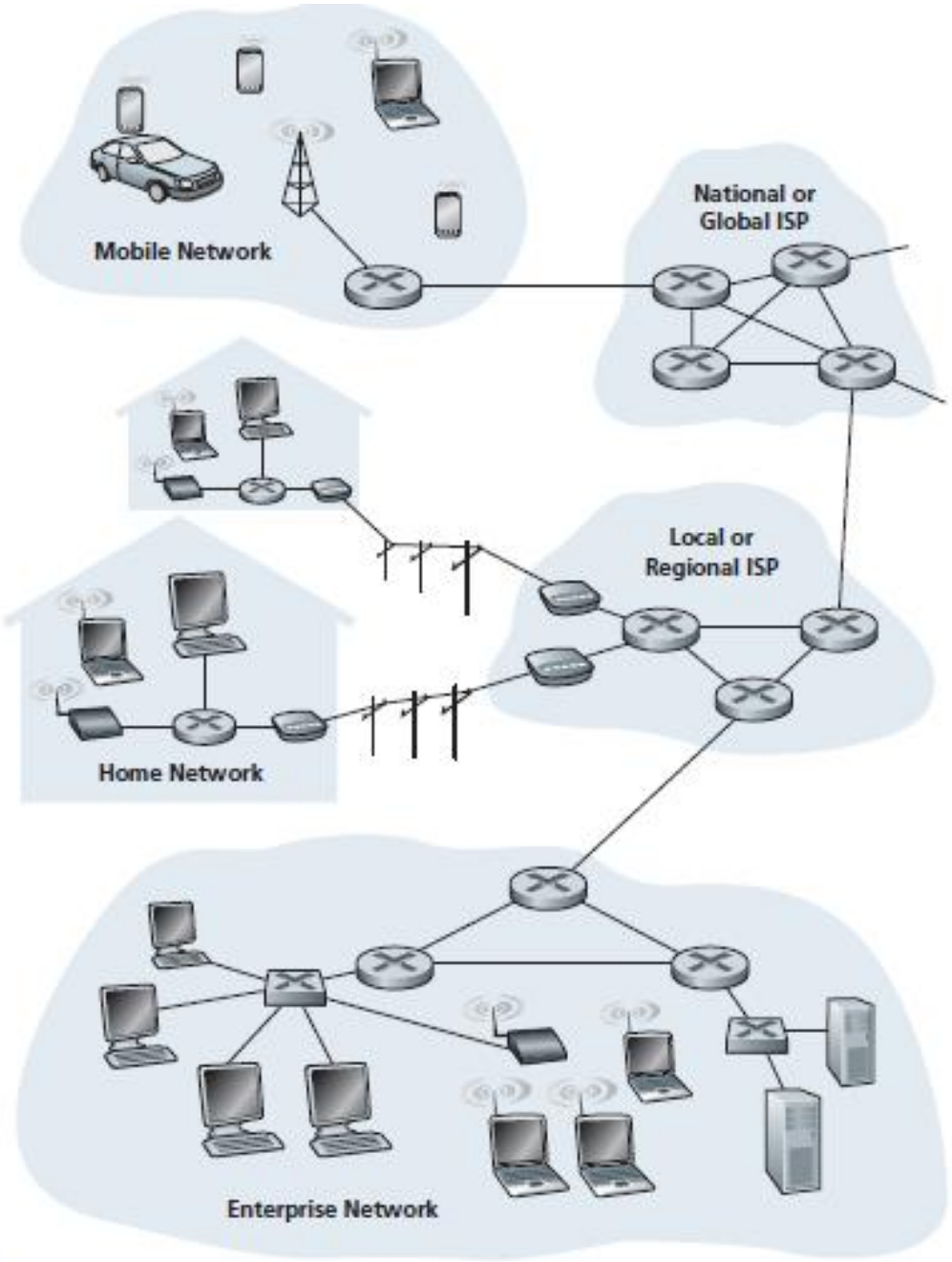
Data Communication and Computer Network

Introduction

"Sometimes when my Internet is down, I forget that the rest of my computer still works"

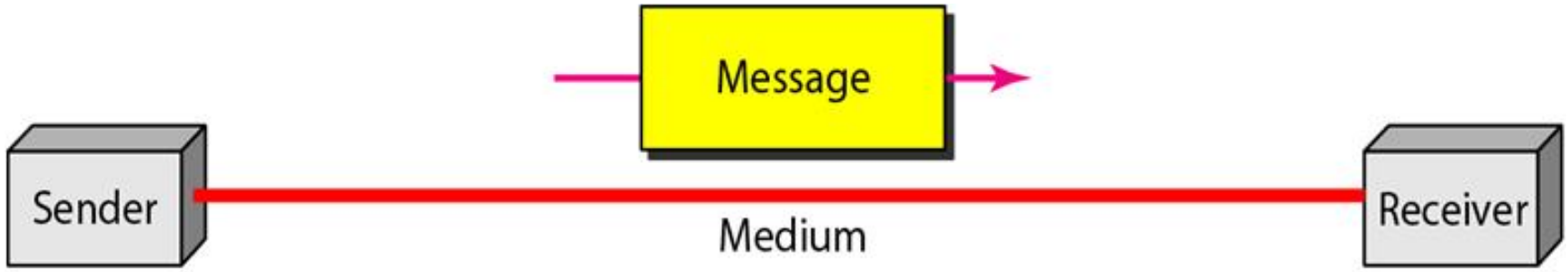
A typical network




Mobile Network
National or
Global ISP
Local or
Regional ISP
Home Network
Enterprise Network

Data Communications

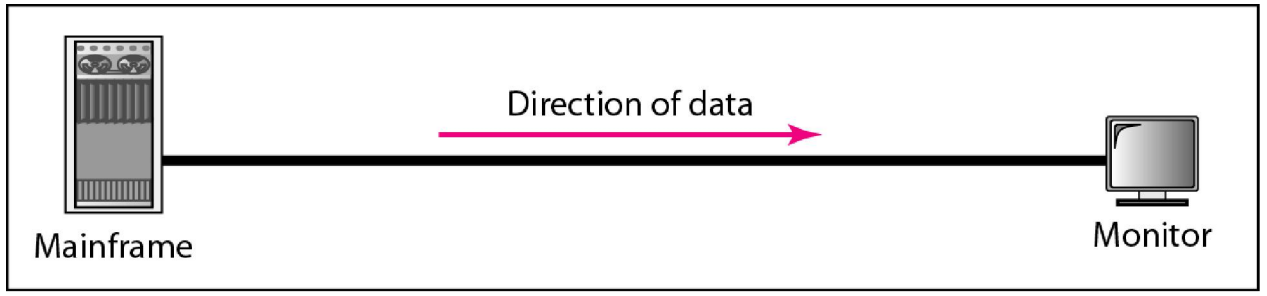
- The term telecommunication means communication at a distance.
- The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- Data communications are the exchange of data between two devices via some form of transmission medium (ex: a wire cable).



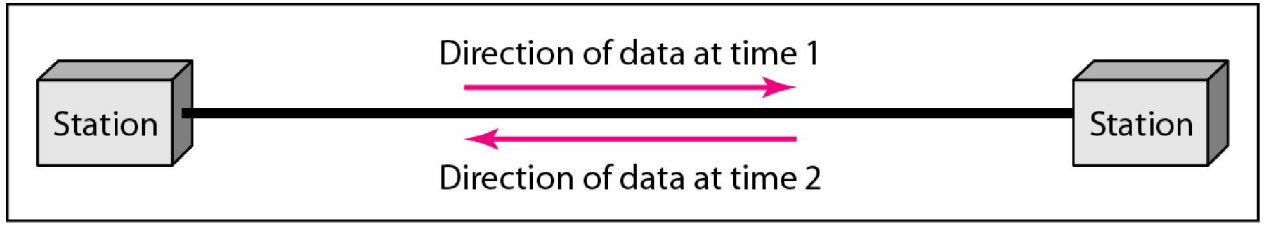
Types of transmissions

Types of transmission

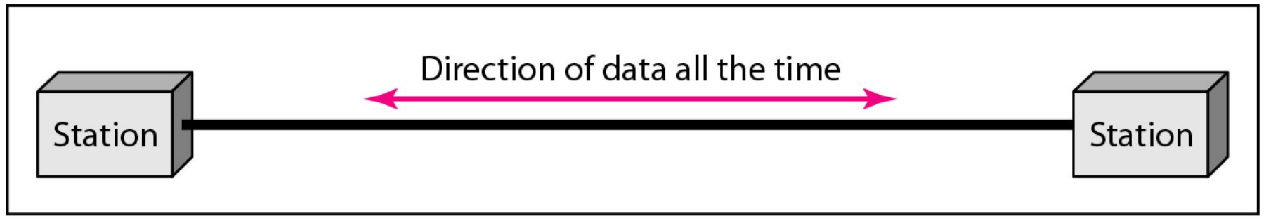
a. Simplex
b. Half-duplex
c. Full-duplex



a. Simplex



b. Half-duplex



c. Full-duplex

Networks

A network is a set of devices (often referred to as nodes) connected by communication links.

- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

Basic Characteristic of CN/ Network Criteria

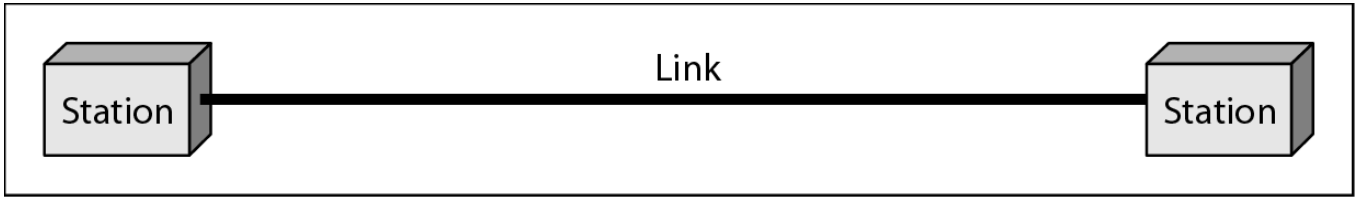
- Scalability and Performance
  - Depends on Network Elements
  - Measured in terms of Delay and Throughput
- Reliability / Fault tolerance
  - Failure rate of network components
  - Measured in terms of availability/robustness
- Quality of Services (QoS)
- Security
  - Data protection against corruption/loss of data due to:
    - ✓ Errors
    - ✓ Malicious users

Physical Structures

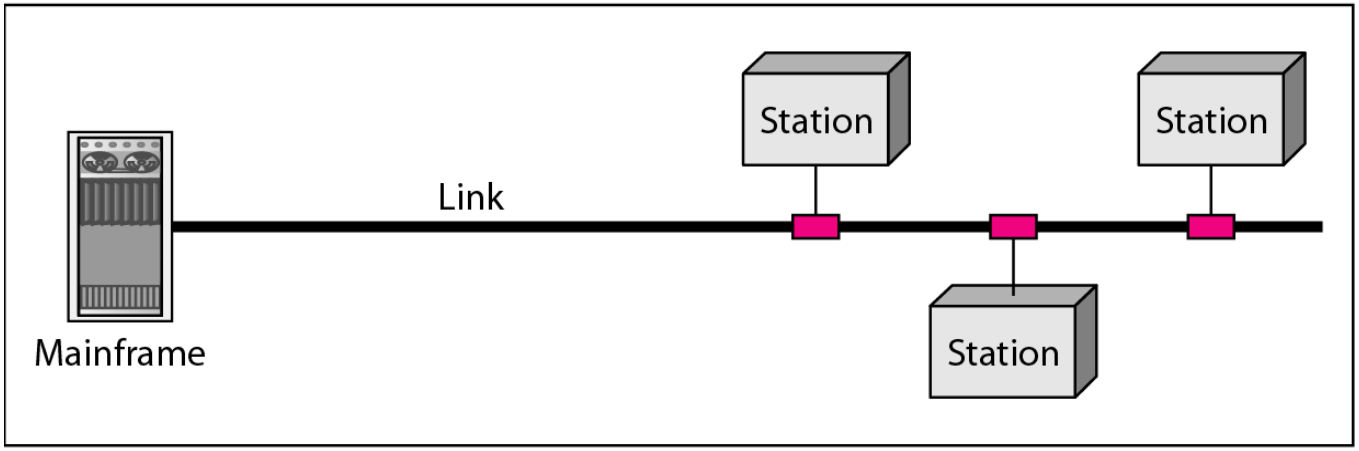
Type of Connection

a. Point to Point - single transmitter and receiver

b. Multipoint (multidrop) - multiple recipients of single transmission



a. Point-to-point

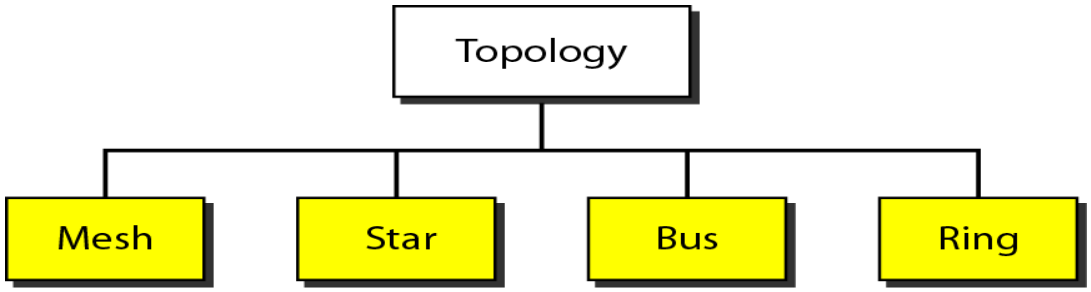


b. Multipoint

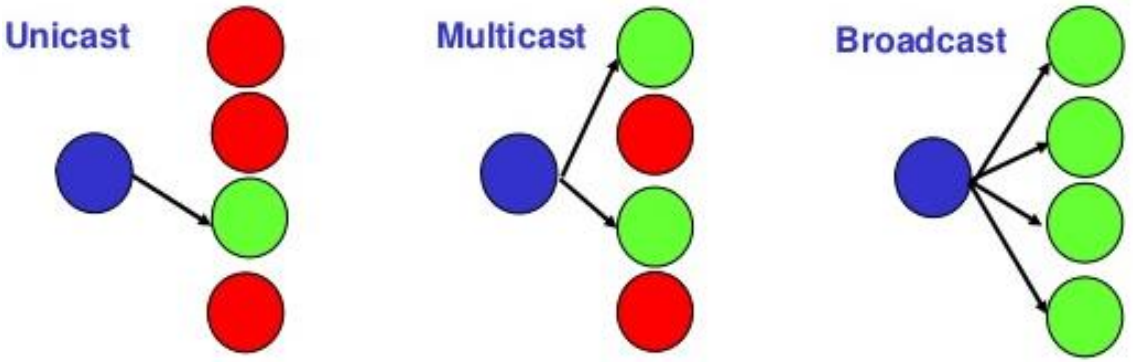
Physical Structures

Physical Topology

- Connection of devices

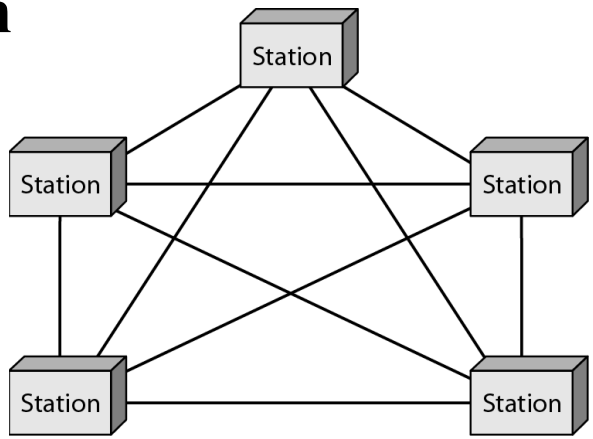


- Type of transmission
  - Unicast,
  - Mulitcast
  - Broadcast

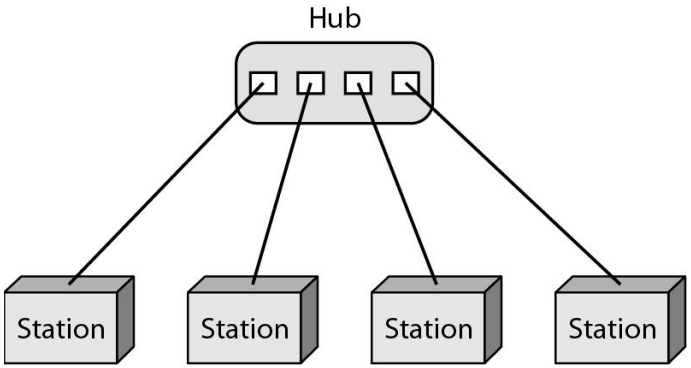


Physical Topology

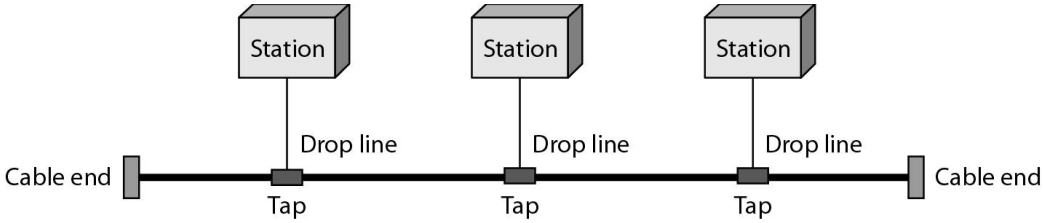
Mesh



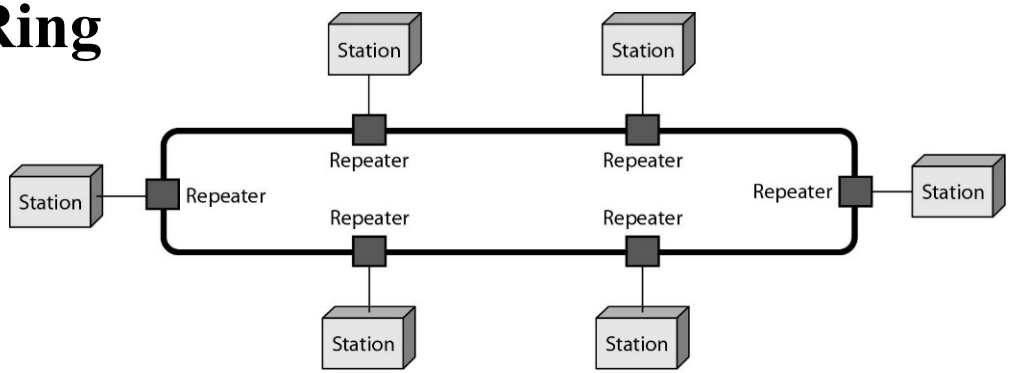
Star



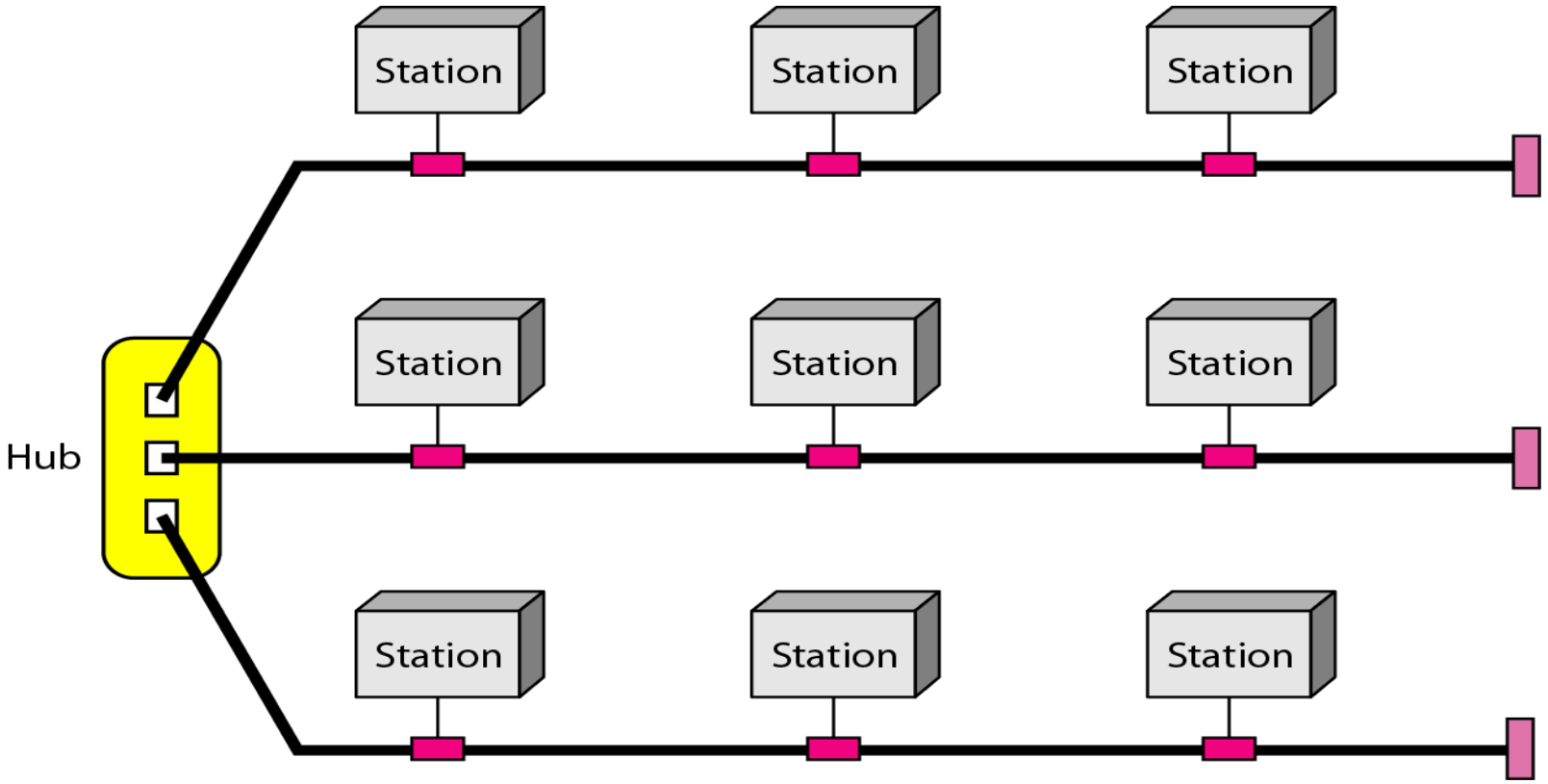
Bus



Ring



A hybrid topology: a star backbone with three bus networks



Categories of Networks

Local Area Networks (LANs)

- Short distances
- Designed to provide local interconnectivity – office, a building or a campus
- Interconnects **hosts**

Wide Area Networks (WANs)

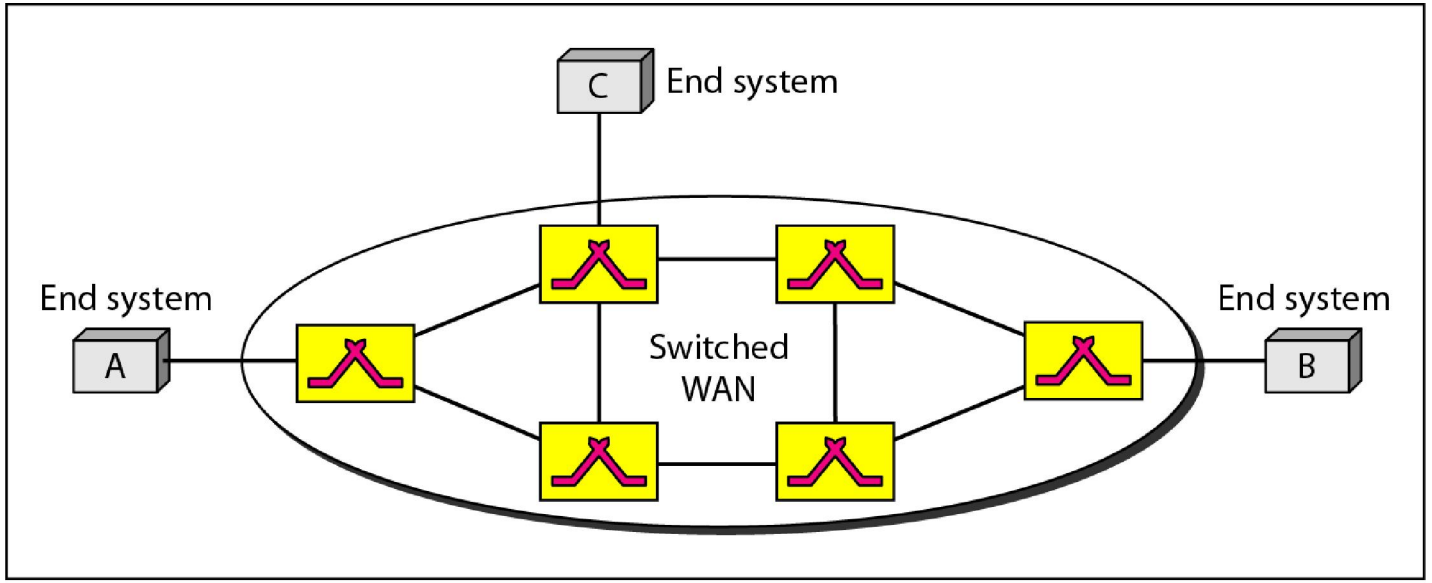
- Long distances
- Provide connectivity over large areas – a town, a state, a country or even world
- Interconnects connecting devices, i. e**. switches, routers, or modem**.

Metropolitan Area Networks (MANs)

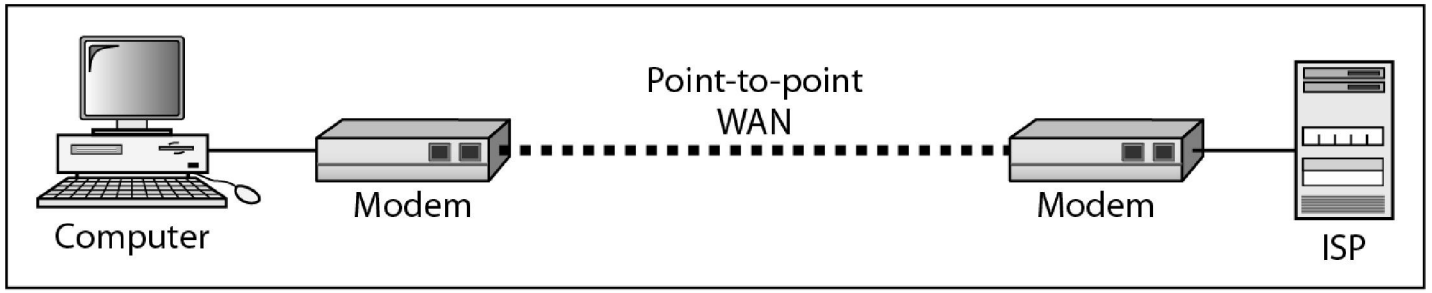
- *Provide connectivity over areas such as a city, a campus*

Type of WAN

a. Switched WAN
b. Point-to-point WAN



a. Switched WAN

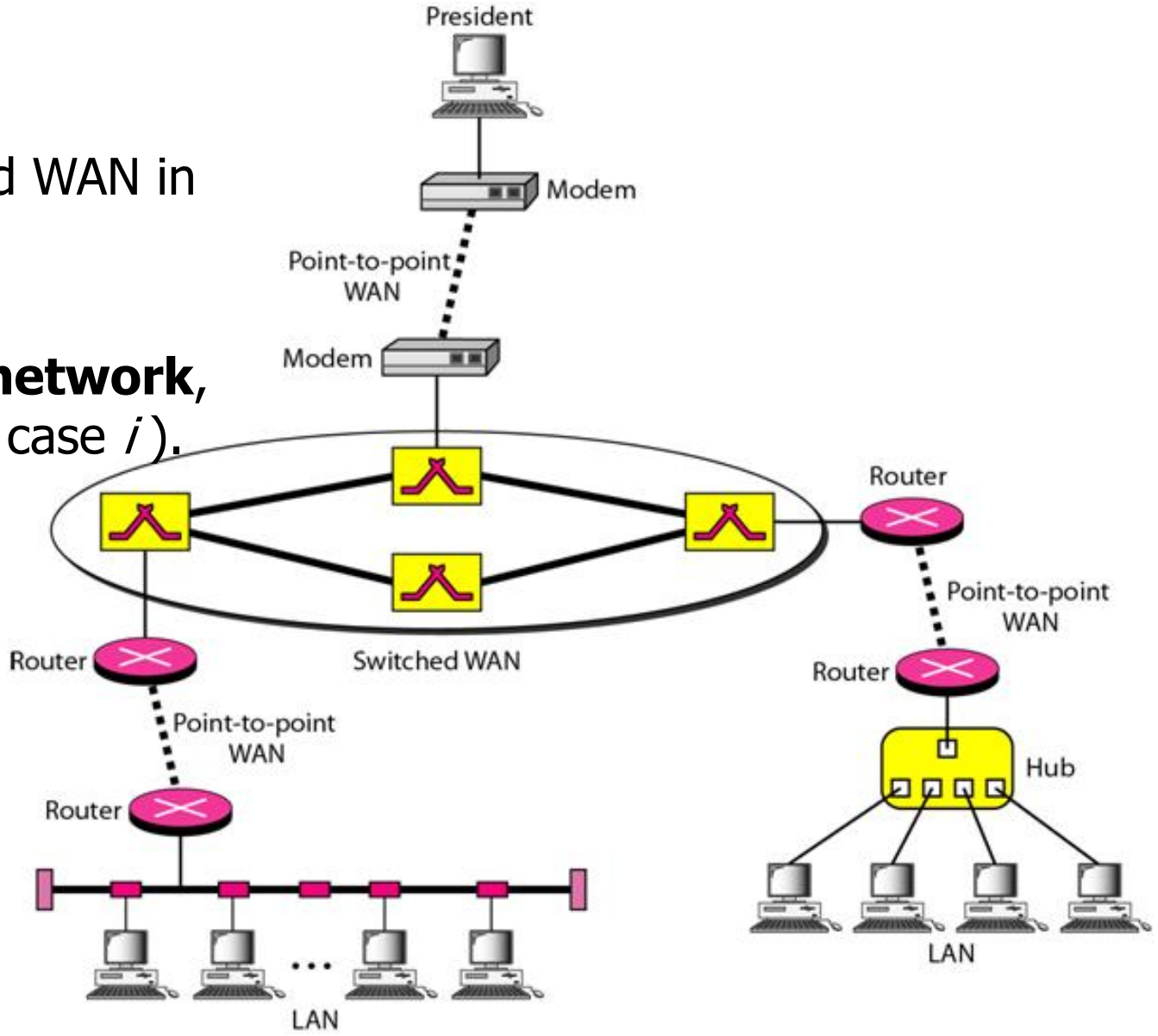


b. Point-to-point WAN

A typical heterogeneous network

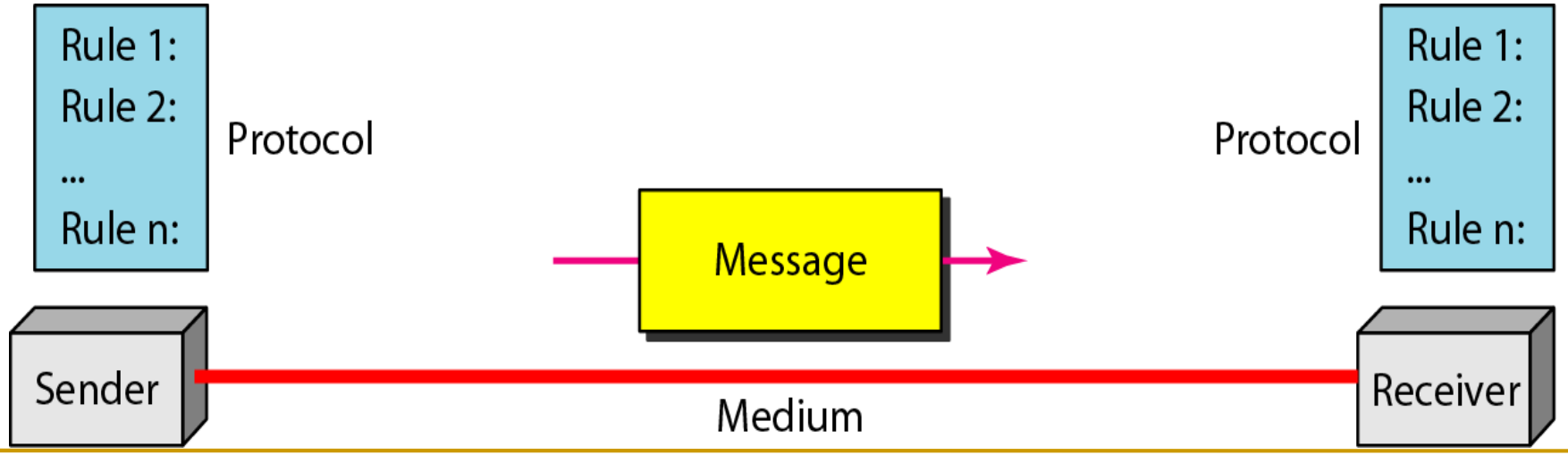
Internetwork

- Very rare to see LAN and WAN in isolation
- Two or more networks connected, forms **internetwork**, or **internet** (with lower case *i*).



Protocols

- A protocol is synonymous with rule. It consists of a set of rules that govern data communications.
- It determines
  - what is communicated
  - how it is communicated
  - when it is communicated
- The key elements of a protocol are syntax, semantics and timing



Elements of a Protocol

Syntax

- Structure or format of the data
- Indicates how to read the bits - field delineation

Semantics

- Interprets the meaning of the bits
- Knows which fields define what action

Timing

- When data should be sent
- Speed at which data should be sent or speed at which it is being received.

Few important terms in Networking

- Modem
- Repeater
- Hub
- Bridge
- Switch
- Router
- Gateways

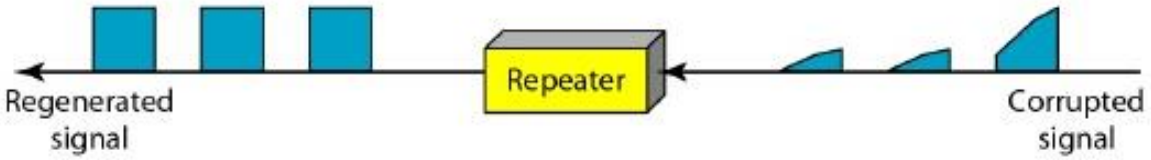
Modem, Repeater

Modem (modulator-demodulator)

- Hardware device works on physical layer
- Can be used with any means of transmitting analog signals
- Modulates one or more carrier wave signals to encode digital information for transmission
- Demodulates signals to decode the transmitted information

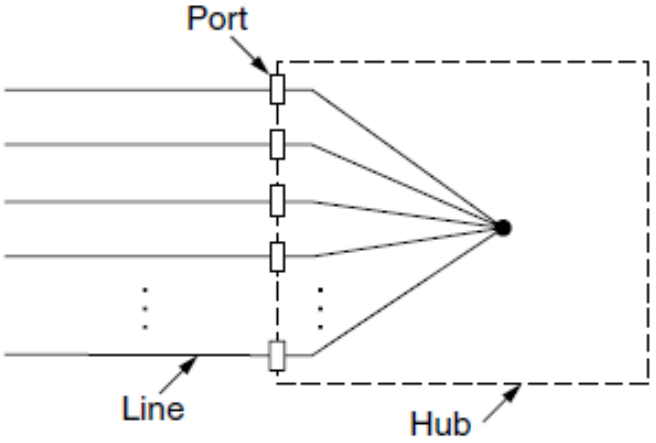
Repeater

- Electronic device that receives a signal and retransmits it
- Used to extend transmissions so that the signal can cover longer distances



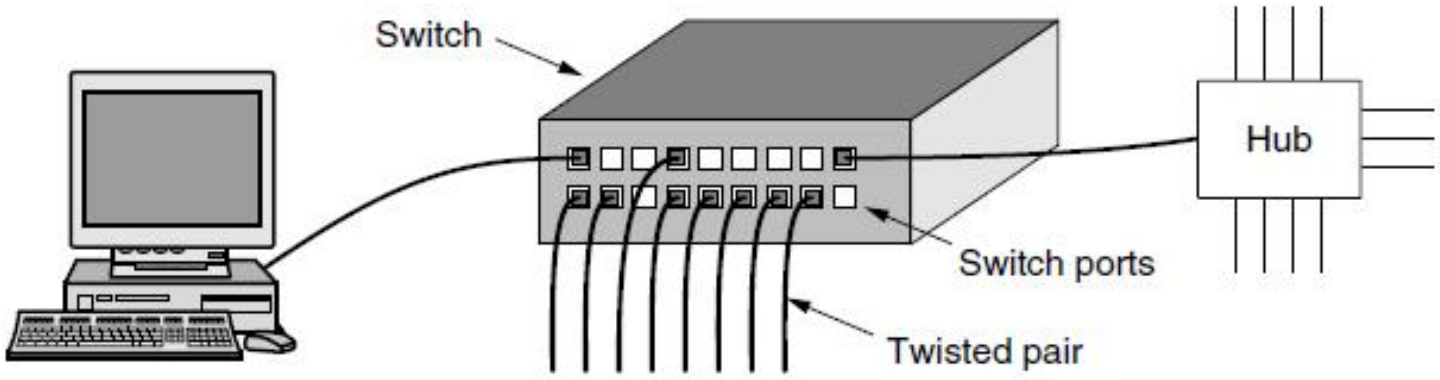
Hub

- Hub (Ethernet hub, network hub, repeater hub, multiport repeater)
  - Network hardware device for connecting multiple Ethernet devices together
  - Multiple Information Outlet (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming
  - Acts as repeater also



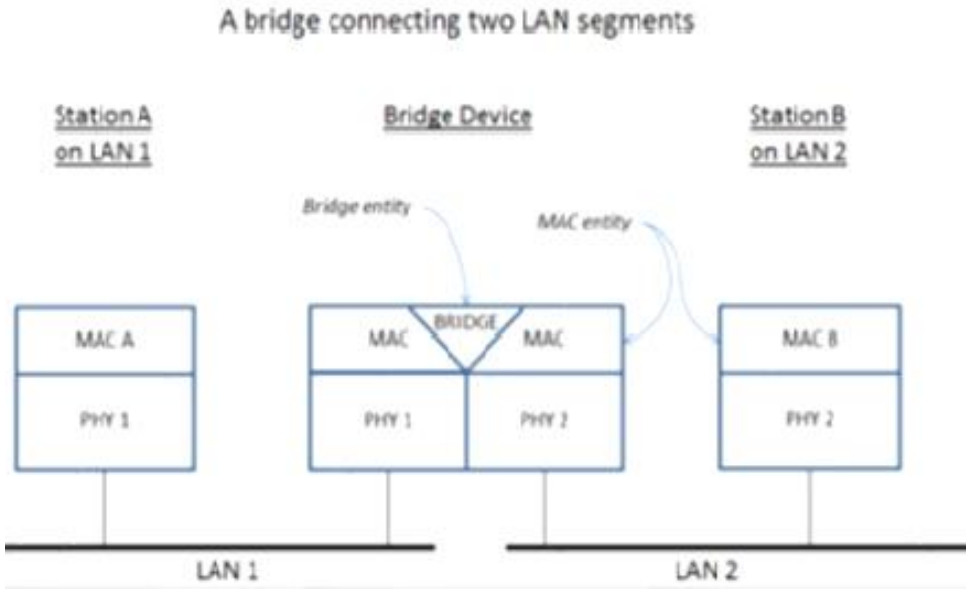
Switch / Bridge

- Switch (or Bridge /switching hub, bridging hub, MAC bridge)
  - Unlike *Hub*, it forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports
  - Process and forward data to the destination device on using hardware addresses (at Layer 2)



Switch / Bridge (contd)

- Switch (or Bridge /switching hub, bridging hub, MAC bridge)
  - Creates a single aggregate network from multiple network segments
  - Allows multiple different networks (of same type) to communicate independently while remaining separate (different collision domain)
  - It can perform error checking before forwarding data



Router, Gateways

Router

- Networking device that forwards data packets between computer networks.
- Perform the traffic directing (routing) functions on the Internet.
- A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node
- Regulates traffic between similar networks (in transport protocols like TCP, UDP, SCTP)

Gateway

- Unlike Router, it regulates traffic between dissimilar networks (TCP ←→ SCTP etc)

References

- *Data Communications & Networking, 5th Edition, Behrouz A. Forouzan*
- *Computer Networks, Andrew S. Tanenbaum and David J. Wetherall*
- *Wikipedia*

Data Communication and Computer Network

Protocol Architecture & Layering

Protocol Architecture

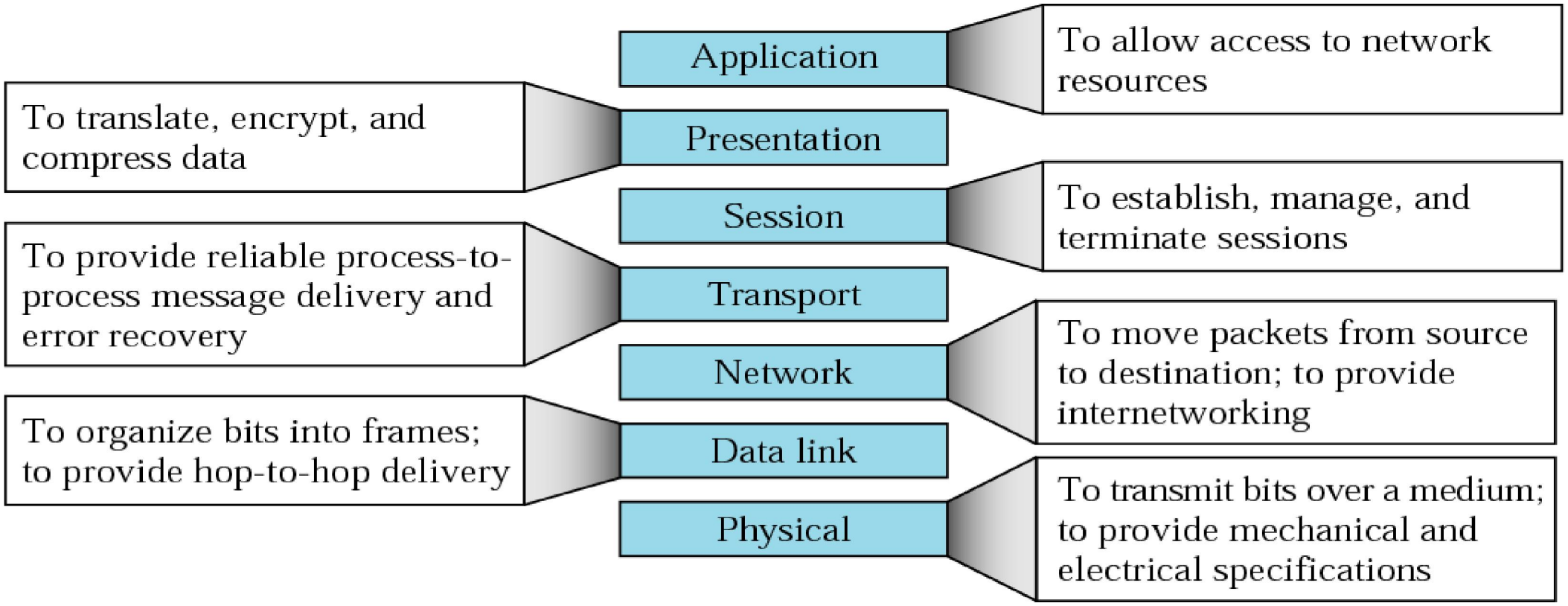
- Task of communication broken up into modules or layers
- Each layer has specific responsibilities

- Reason for layering – if one layer's implementation changed, other layers not affected if interface remains unchanged

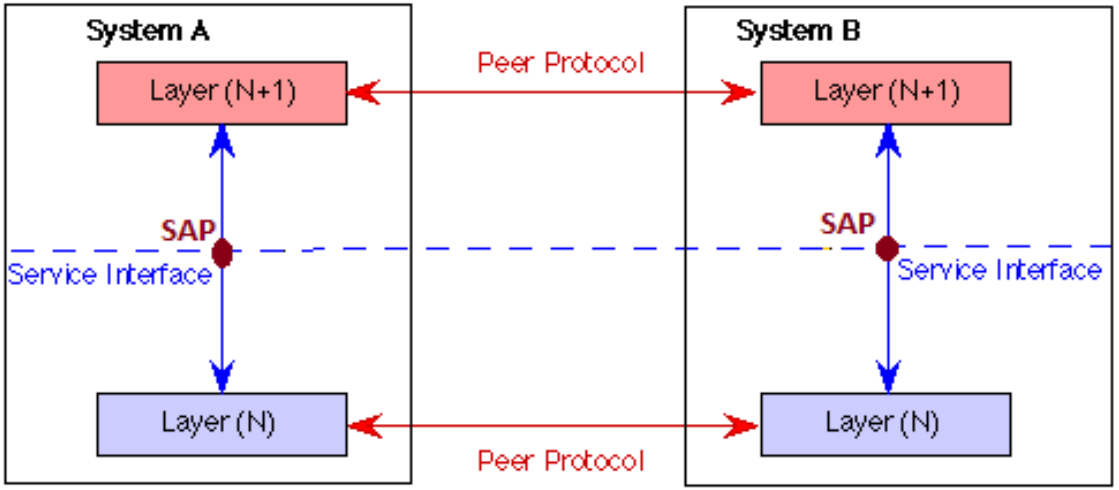
OSI Layers

- OSI Layers (Open Systems Interconnection)
- Developed by International Organization for Standardization (ISO)
- Seven Layers (depending on the complexity of the functionality each of these layers provide.)
  - ✓ Application
  - ✓ Presentation
  - ✓ Session
  - ✓ Transport
  - ✓ Network
  - ✓ Data Link
  - ✓ Physical

OSI Layers in brief



Interface, Protocol & Addressing



- Interface between two layers
  - A Service Access Point (SAP) is a conceptual location at which one OSI layer can request the services of another layer
  - Each layer expects some service from lower layer and provides some service to its higher layer
    - ✓ e.g. application layer expects reliable communication from transport layer (no errors in frames, no lost frames, etc)

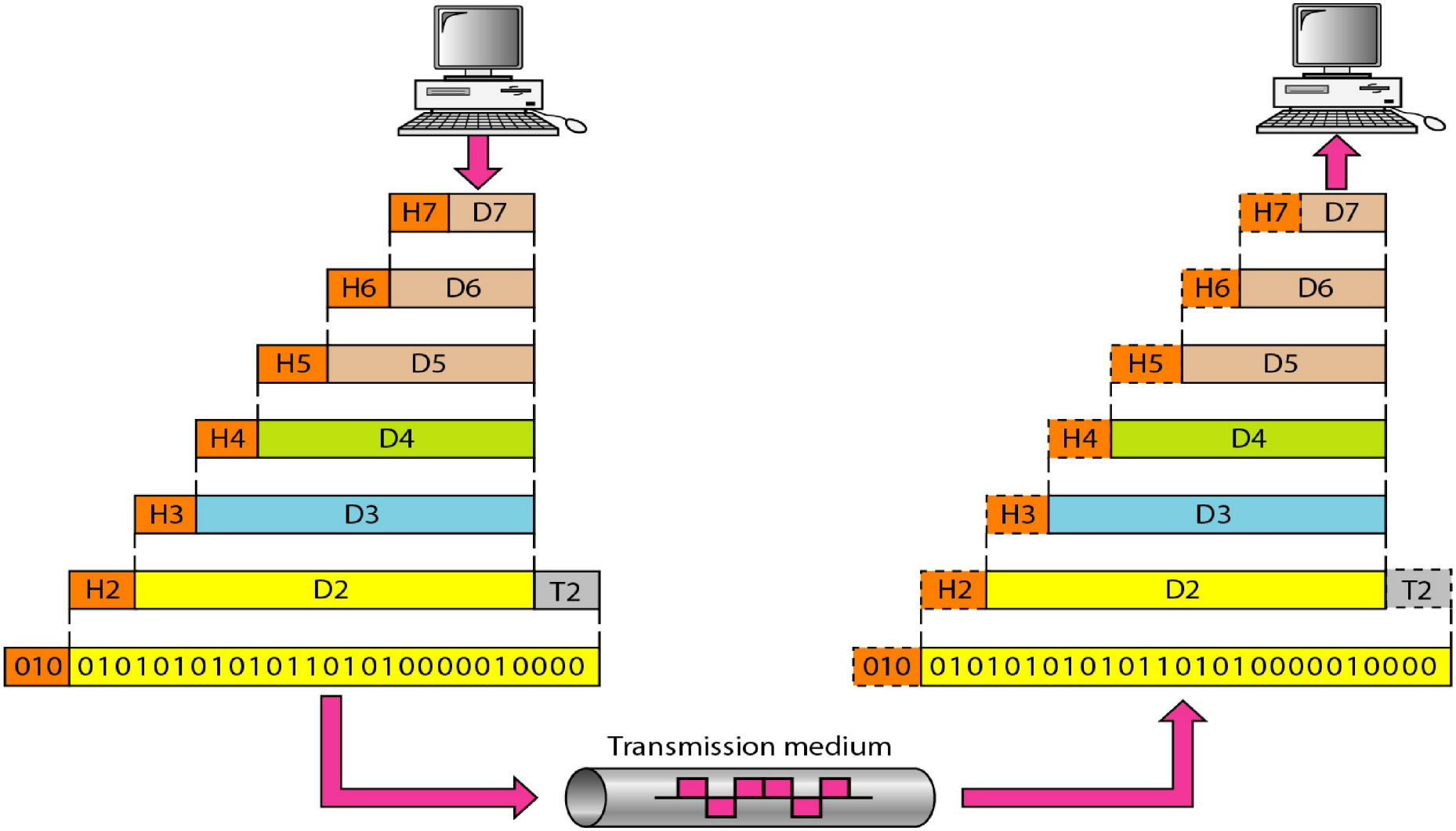
- Protocol – set of rules followed by same layer at different nodes e.g. between the transport layer of Tx and Rx

Protocol Data Units (PDUs)

- Control information added to data at each layer (in the form of header / trailer)
  - Destination node address, sequence number, error detection code, etc
  - Control information added by layer i^{th} at transmitter is used by layer i^{th} at receiver node

- PDUs called differently at different layers
  - frame in data link layer, packet/datagram in network layer, packet/segment in transport layer, message in application layer

Operation of a Protocol Architecture



PDUs (contd.)

- Encapsulation
  - At Tx: as data goes down, each layer adds header
  - At Rx: as data goes up, each layer takes out its own header, carries out checks, hands up rest to higher layers if ok
- Number of layers to be used
  - More the no. of layers, more headers added as the data goes downwards, more wastage
  - Too few layers – defeats the purpose of layering (isolating functionalities in layers) itself

OSI Layers - brief overview

- Physical Layer
  - Physical interface between data transmission device (e.g. computer) and transmission medium or network
  - Specifies raw transmission details like connectors, medium, voltage levels, encodings used, data rate, etc.

- Data Link Layer
  - Ensures reliable communication between two directly connected nodes
  - Sends blocks of data (frames) with the necessary synchronization, error control, flow control
  - Medium Access Control (MAC)

OSI Layers - brief overview (contd. 2)

- Network Layer
  - Deals with **routing**: sending packets from source to destination nodes that are not directly connected
  - Packets may not reach in order, can get lost (does not guarantee reliable communication)
  - Congestion Control and Internetworking
  - Some other functions (like fragmentation)

- Transport layer
  - Ensures reliable, in-order delivery between any two applications ensures no frame loss, no error, no duplicate (Error Control, Flow Control)
  - Segmentation & Reassembly
  - Connection Establishment / Release

OSI Layers - brief overview (contd. 3)

- Session layer
  - It deals with the concept of Sessions
  - Controls the dialogues (connections) between computers
  - Synchronization

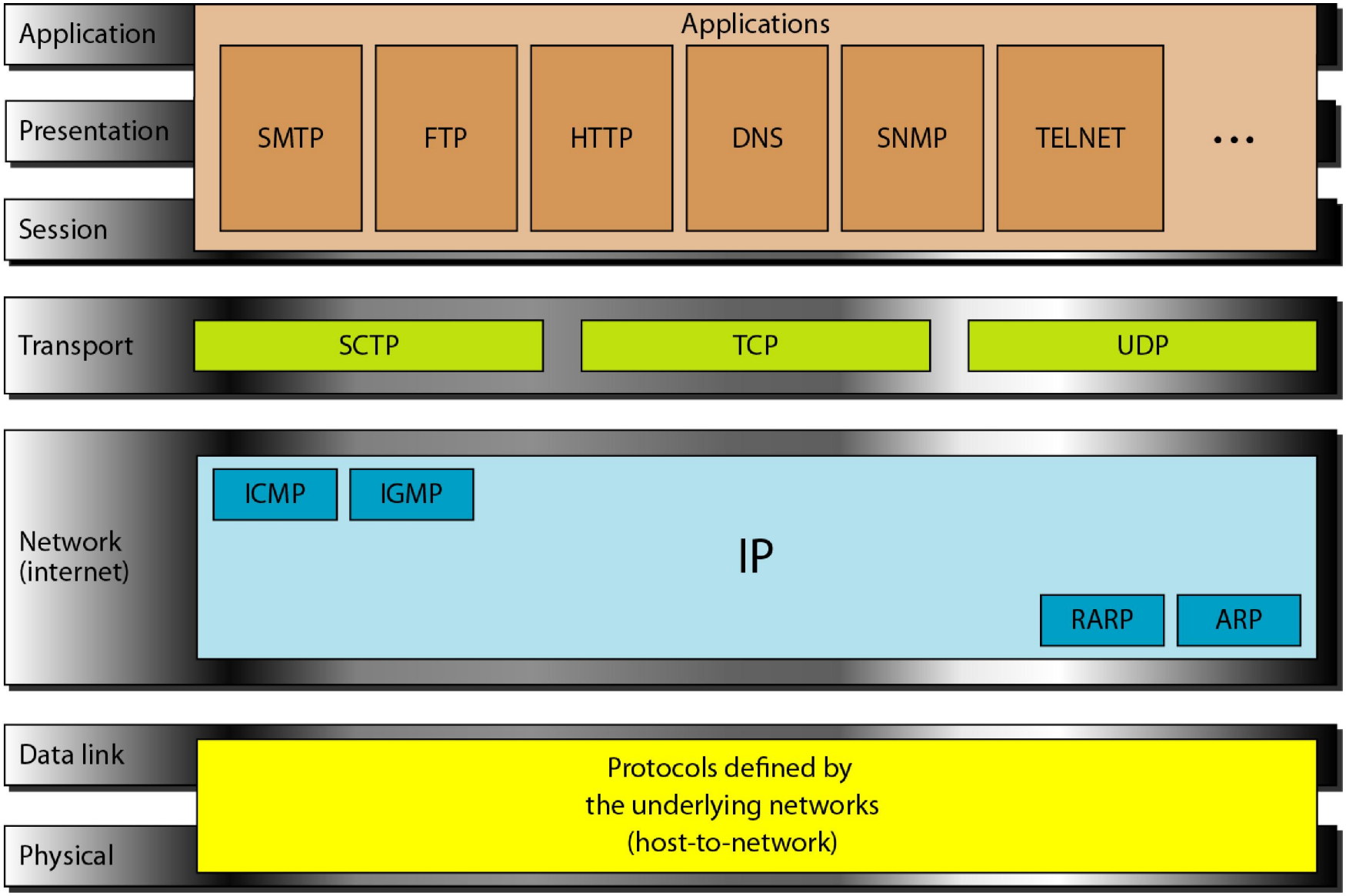
- Presentation layer
  - Compression and encryption
  - Independence from data representation (Endianness, TLV(Type-Length-Value), Basic Encoding Rules(BER) or Packed Encoding Rule (PER) of ASN.1)

- Application layer
  - Supports user applications (e.g. http, ftp)

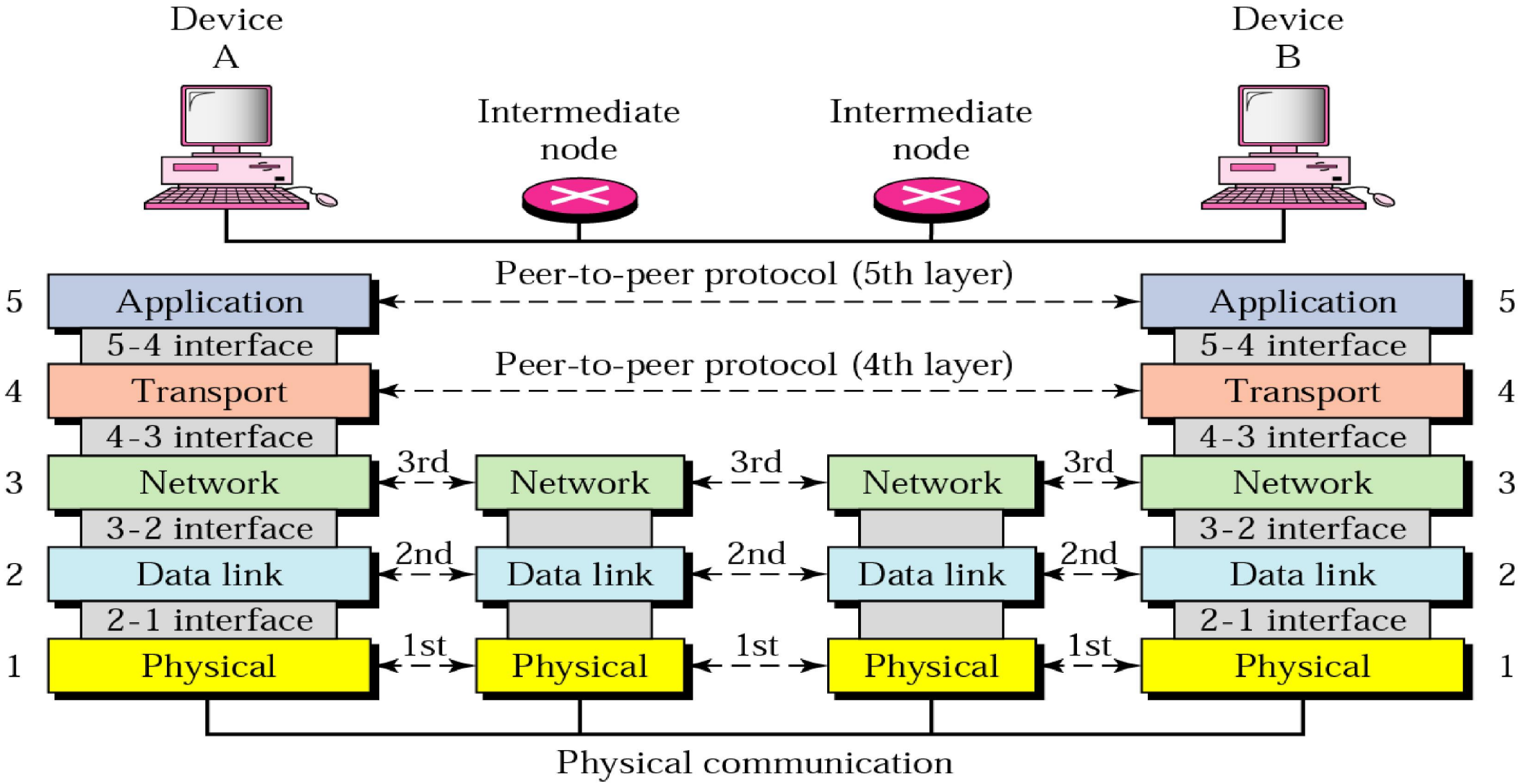
TCP/IP layers

- TCP layers – by US Defense Agency
- De-facto standard (not official, but working model)
- Used by the global Internet
- Five Layers
  - Application
  - Transport
  - Network (Internet)
  - Data Link
  - Physical

OSI model and TCP/IP

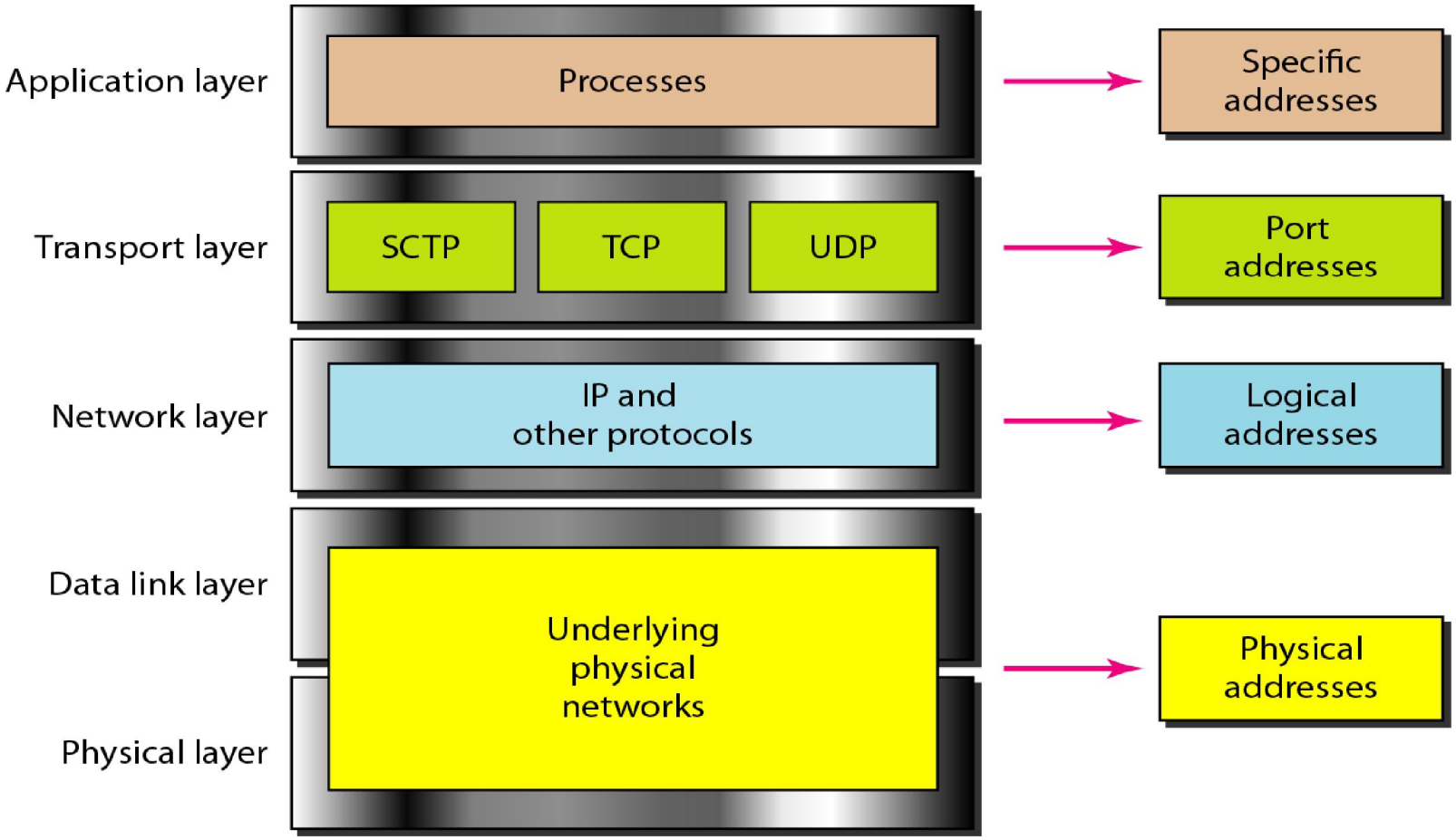


Protocols & Interfaces in TCP/IP stack



Relationship of layers and addresses in TCP/IP

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.



Physical Address / MAC Address

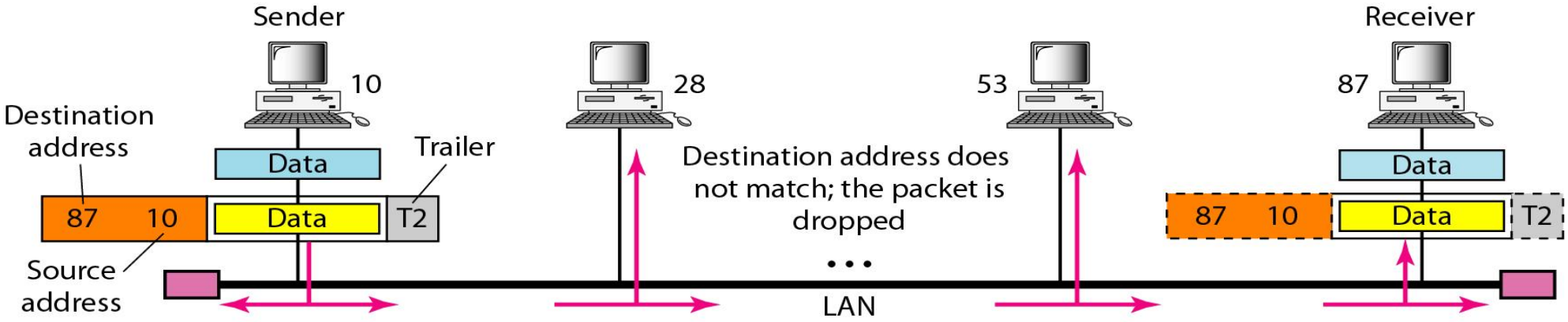
Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

Data communication within a LAN

A node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.



Logical Address /IP Address

An Internet Protocol address (IP address) is a numerical label assigned to each node participating in a computer network that uses the Internet Protocol for communication

Two principal functions: host or network interface identification and location addressing

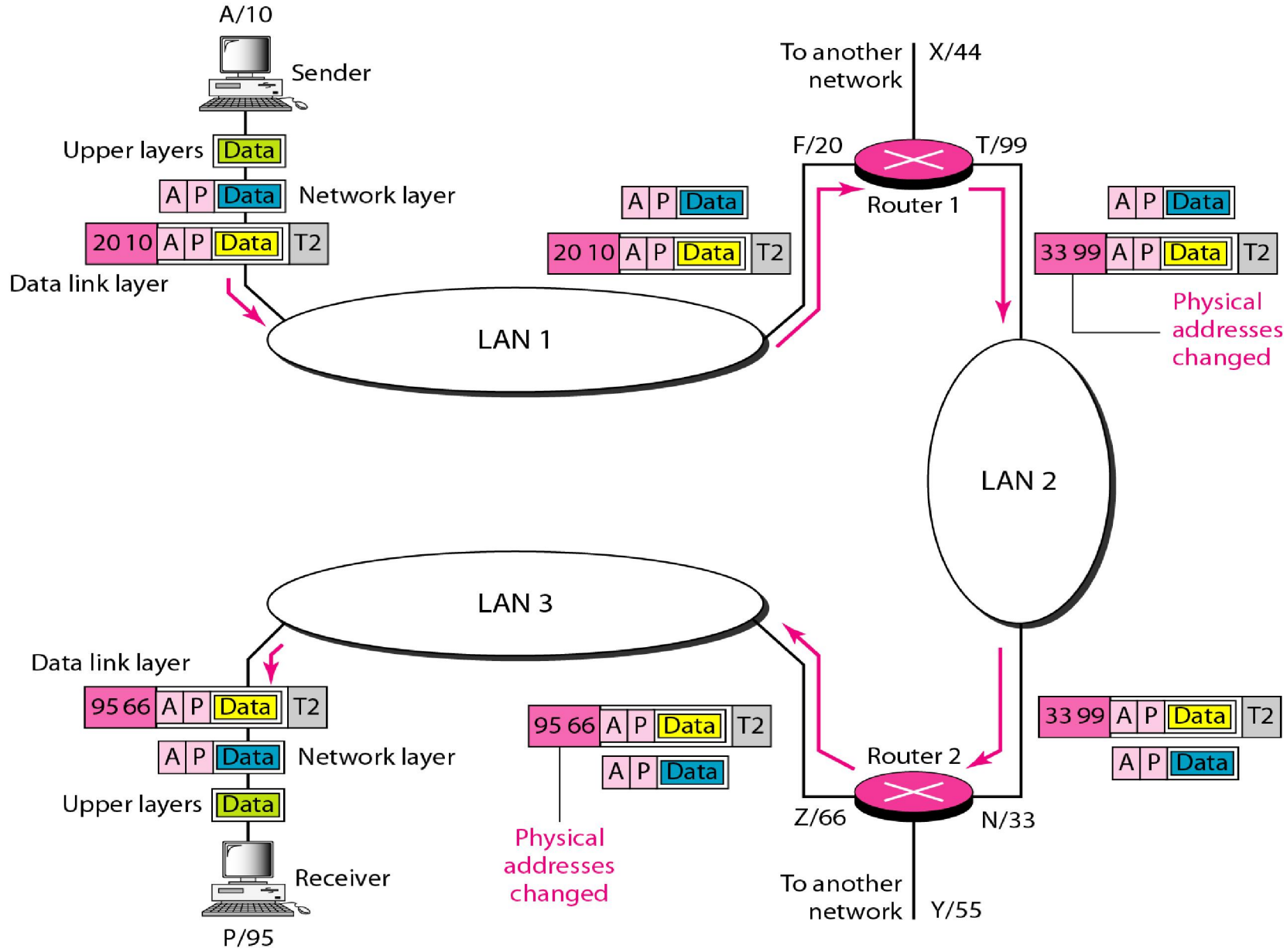
IPv4 : 10.2.1.40
A 4-byte logical address

IPv6 : 2001:db8:0:1234:0:567:8:1
A 16-byte logical address

Data communication across internet

Example shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

Data communication across networks



The physical addresses will change from hop to hop, but the logical addresses usually remain the same

Port addresses

753

A 16-bit port address represented as one single number.

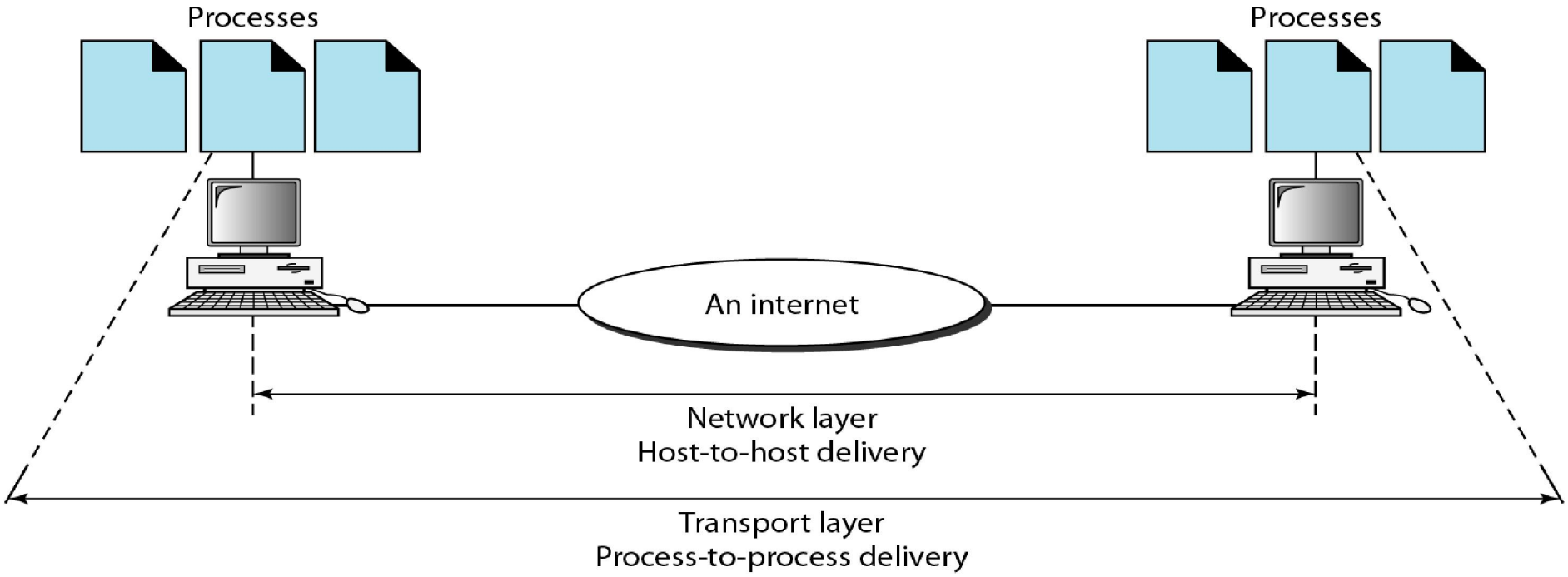
Well known port

```
ftp : 20
Ssh : 22
http : 80
```

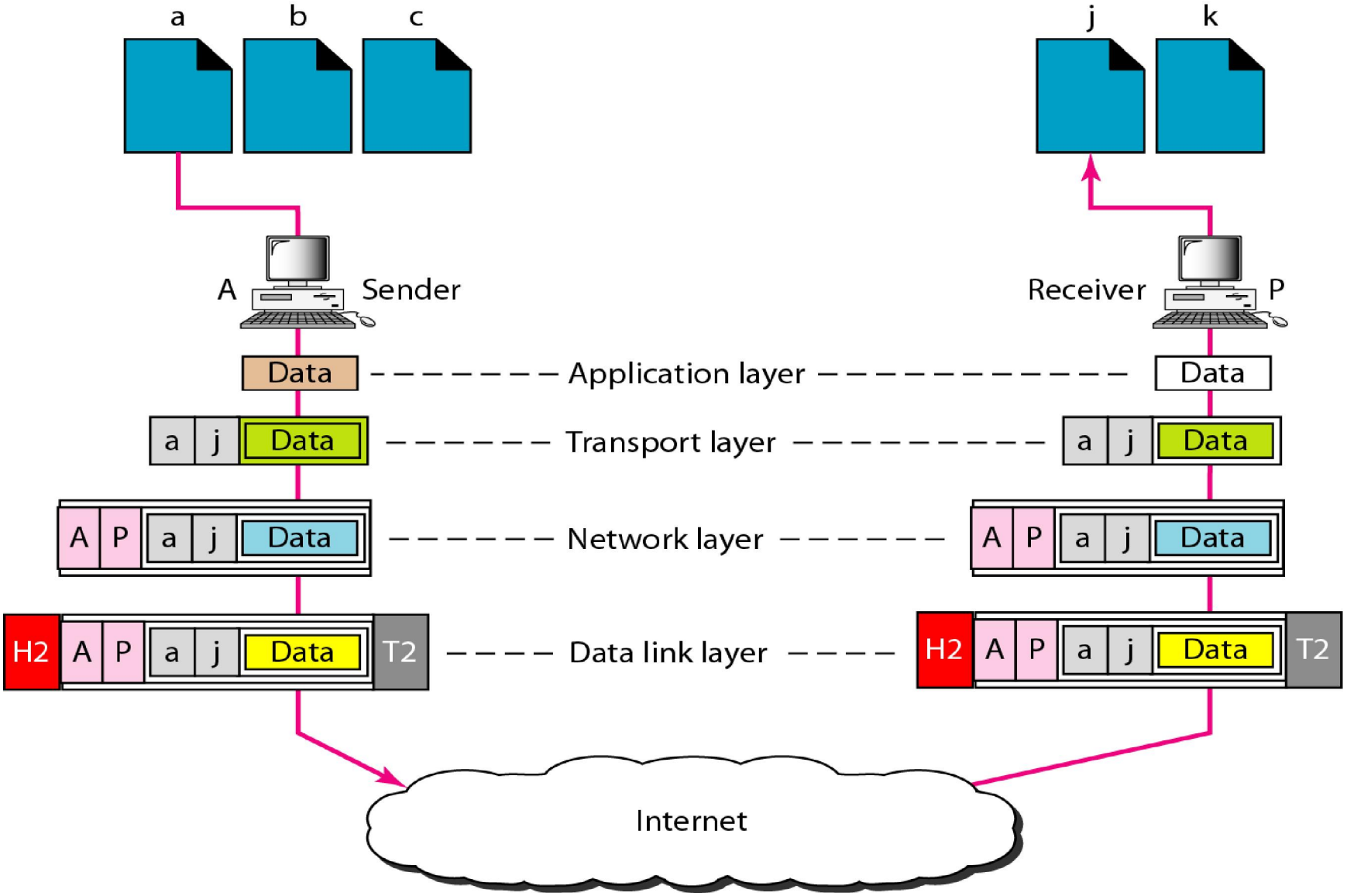
Data communicating via the Internet

Example shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

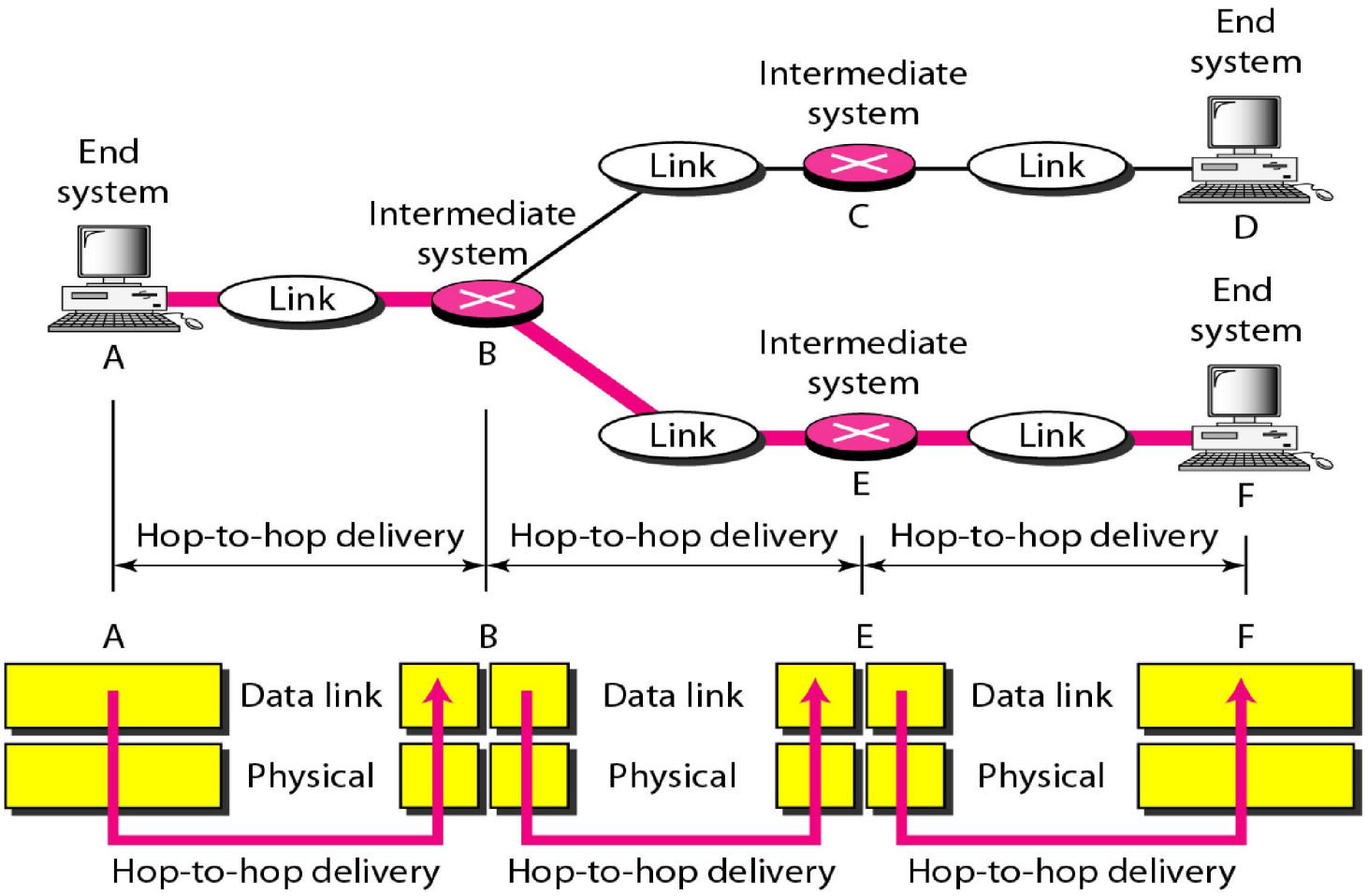
Appendix 4: Reliable process-to-process delivery of a message



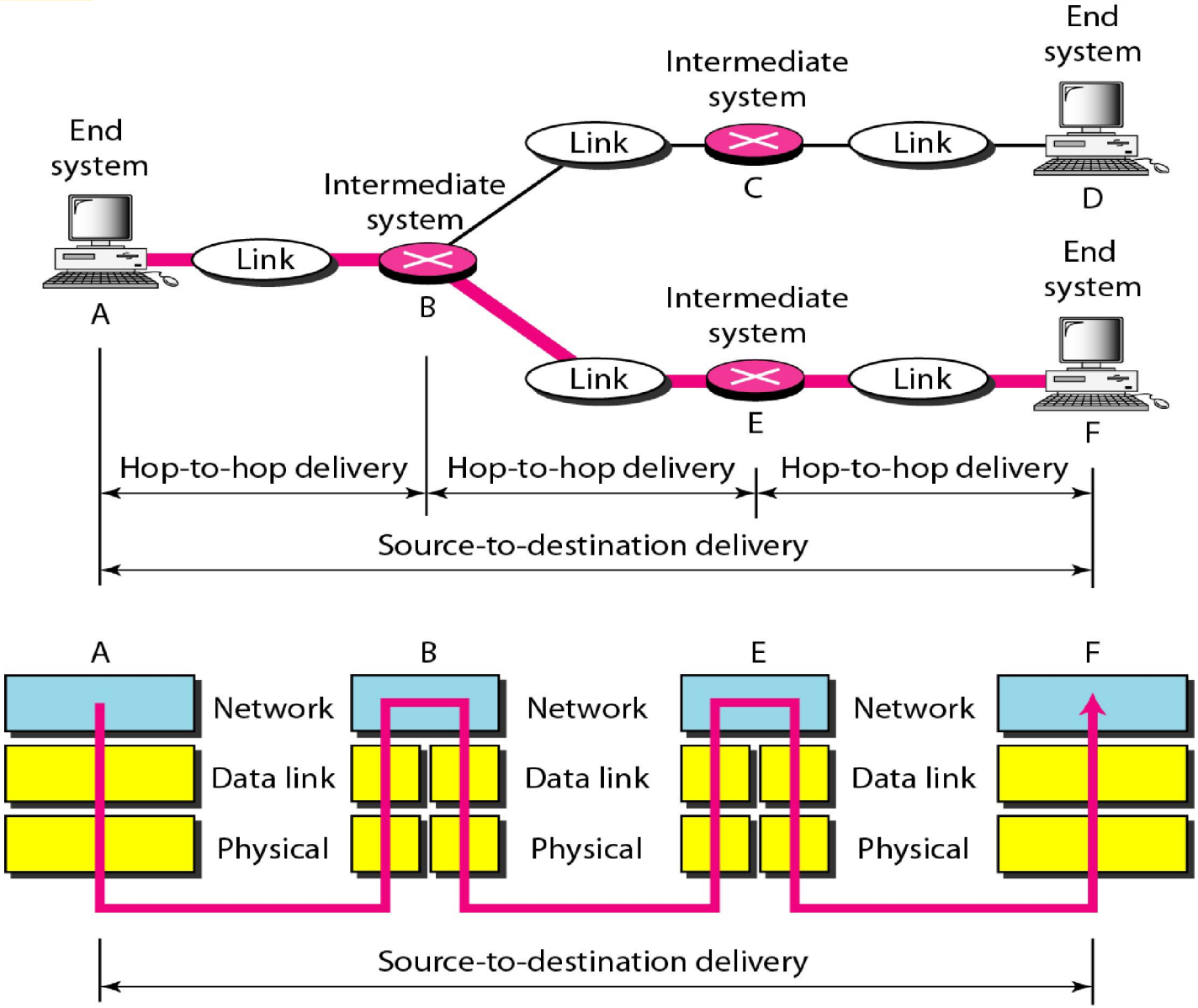
Port addresses



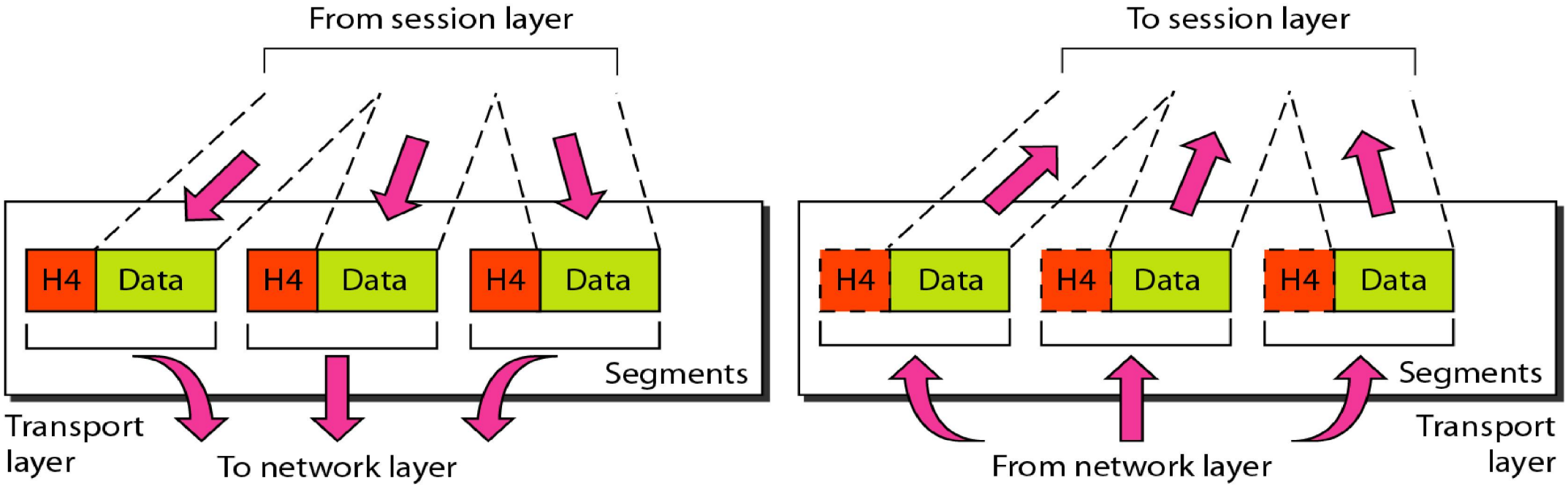
Appendix 1 : Hop-to-hop delivery (L2 switching)



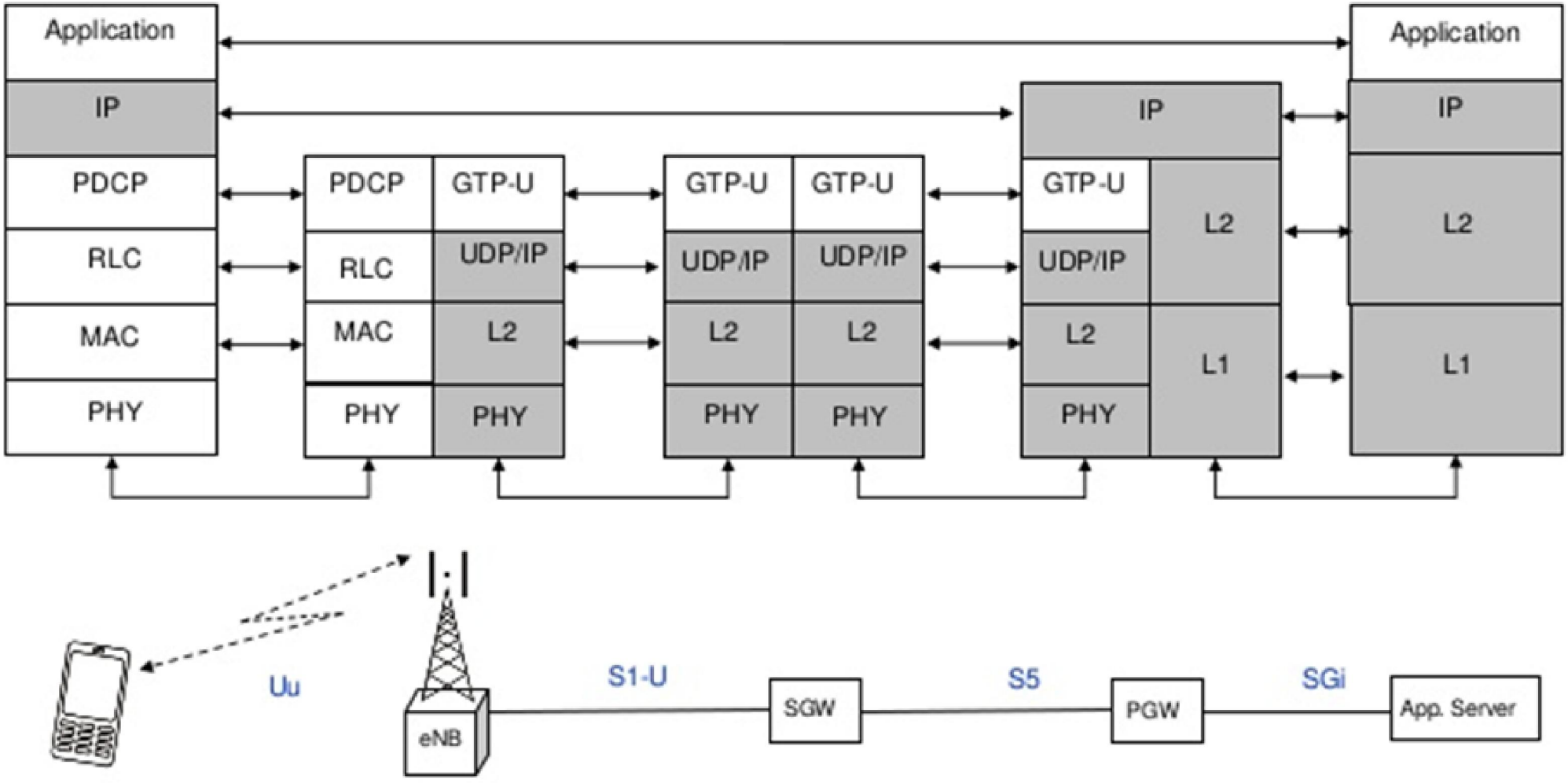
Appendix 2 : Source-to-destination delivery (L3 Switching)



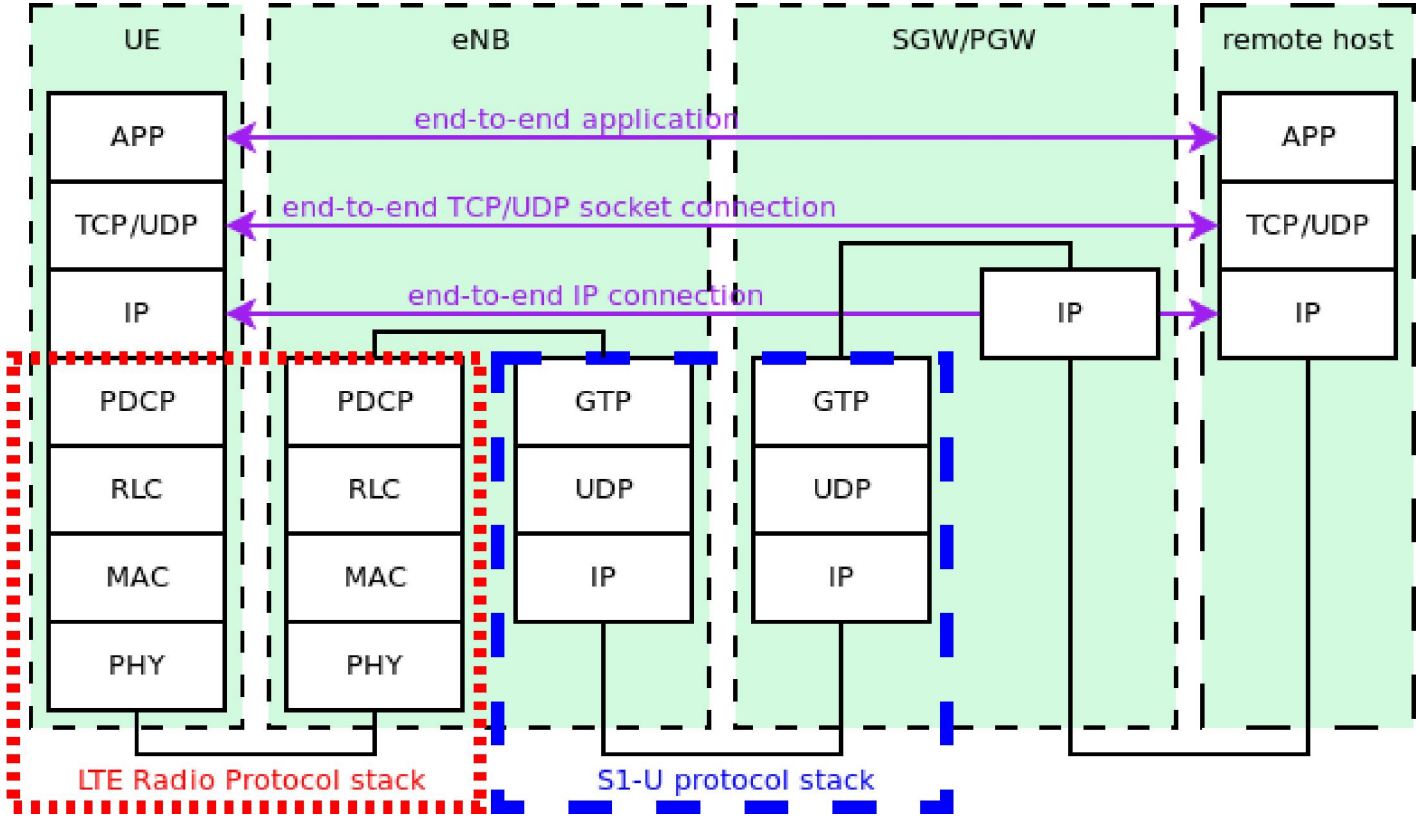
Appendix 3 : Segmentation & Reassembly



Appendix 4 : LTE data plane (User plane) protocol stack



Appendix 5 : LTE data plane (User plane) protocol stack (diff img)



Data Communication and Computer Network

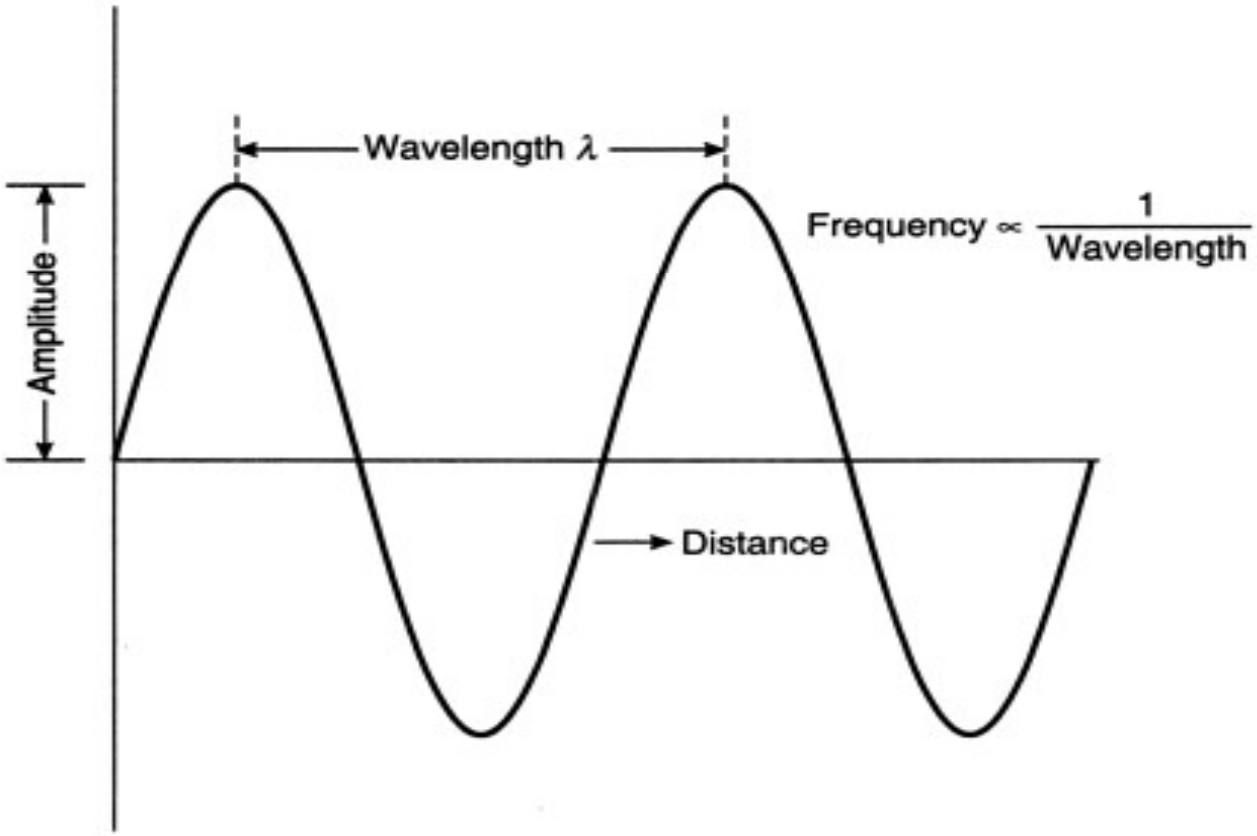
Physical Layer

Electromagnetic Wave

- A wave of energy propagated in an electromagnetic field
- All energy in the universe travels in waves and those waves radiate outwards from a source
- Just as waves ripple outwards from a stone tossed in a pond

Electromagnetic Wave Contd...

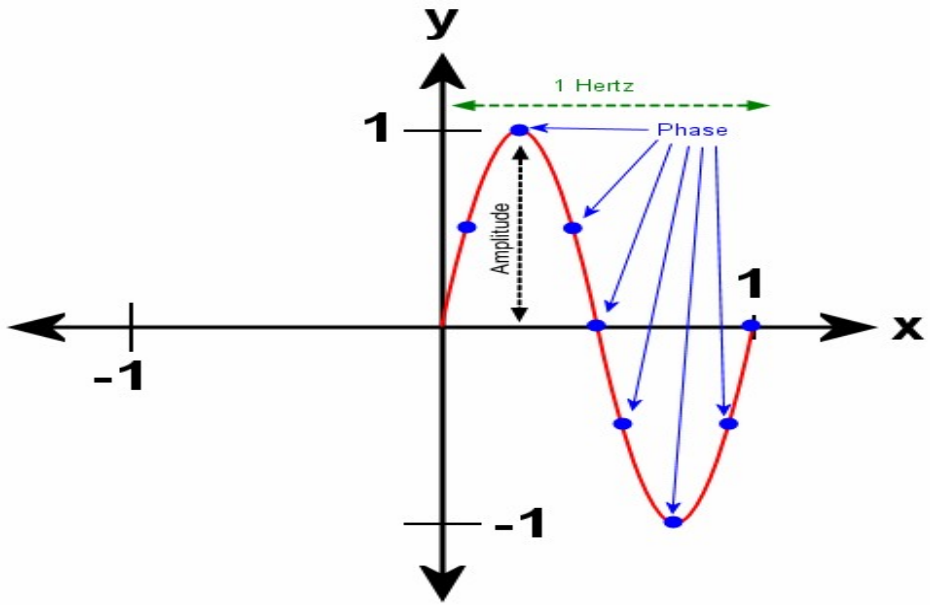
A typical Electromagnetic Wave (time domain representation)



Electromagnetic Wave Contd...

All radiation(electromagnetic energy) is said to have :

- Wavelength : Measured in distance (meters)
- Frequency : Measured in time (cycles per second)
- Amplitude : Measured in power (electron volts)
- Phase (what value the wave has at any single instant in time)



Electromagnetic Wave Contd...

- An electromagnetic wave has a frequency and a wavelength associated with it and travels at the speed of light (in vacuum), or c.

- The relationship among these wave characteristics can be described by

- $vW = f \lambda$
  - where vW is the propagation speed of the wave (here vW = c)
  - f is the frequency
  - λ is the wavelength

  So that for all electromagnetic waves $c = f \lambda$

- Hence $f = c/\lambda$ or $f \propto 1/\lambda \rightarrow$ High frequency electromagnetic wave has lower wavelength

Pulse Code Modulation (PCM): In PCM, the amplitude of the analog signal is sampled at regular intervals, and

Pulse Amplitude Modulation (PAM): PAM is a modulation technique where the amplitude of the analog signal is

Delta Modulation: Delta modulation is a form of analog-to-digital conversion where the difference between succ

Data and Signal

- Data: entities that convey meaning
  - Can be analog (audio, video) or digital (text, numbers)
  - We consider only digital data i.e. the entities consist of sequence of 0's and 1's

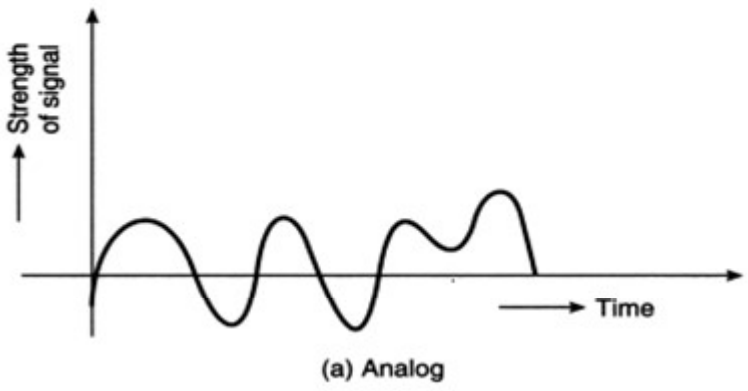
- Signal: Electric / electromagnetic representations of data
  - Can be analog or digital
  - Different signals can be used to represent same data

- Encoding: representing data with signals

- Transmission: communication of data by propagation and processing of signals

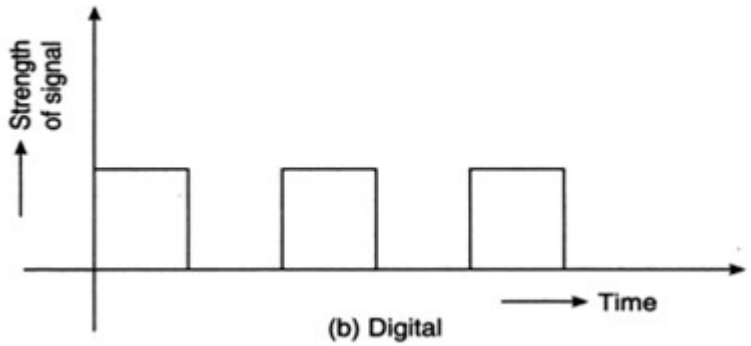
Analog Signal

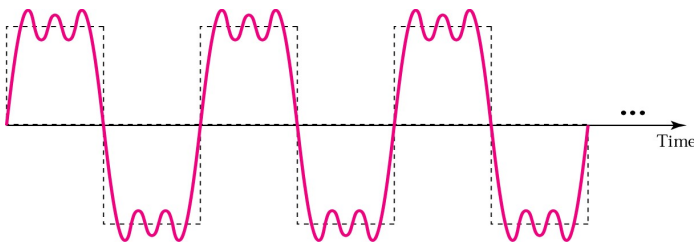
- An Analog signal is one in which the signal intensity varies in a smooth fashion (continuous) over time
  - Could be simple or composite signal
  - A single-frequency sine wave is not useful in data communications, composite signals used



Digital Signal

- A Digital Signal is one in which the signal intensity maintains a constant level (discrete) for some period of time and then changes another constant level
  - Usually non-periodic
  - Bit rate: number of bits sent in 1 second (bps)
  - Digital signal is a composite analog signal, having bandwidth ∞ (infinity)





Digital Signal (Cont'd)

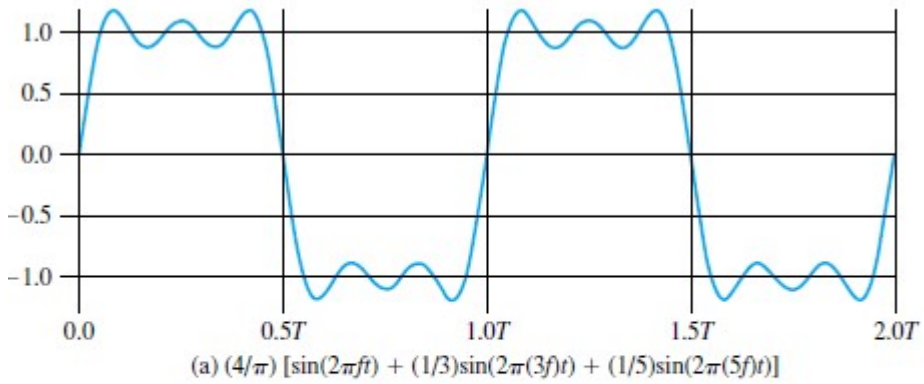
- It can be shown that the frequency components of the square wave with amplitudes A and –A can be expressed as follows:

$$s(t) = A \times \frac{4}{\pi} \times \sum_{k \text{ odd}, k=1}^{\infty} \frac{\sin(2\pi k f t)}{k}$$

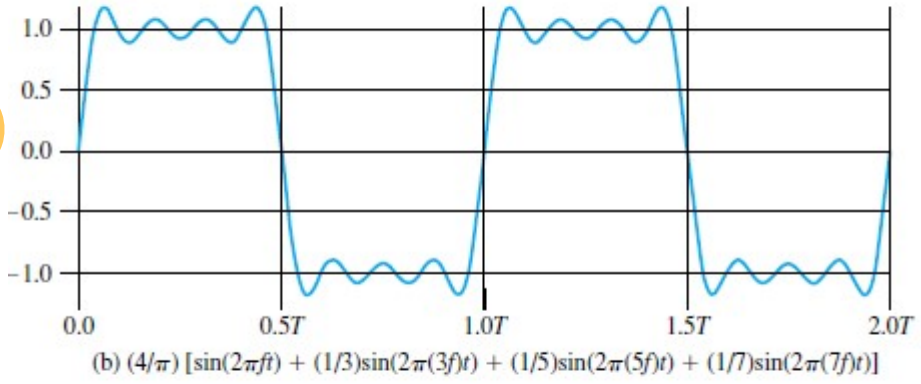
- Thus, this waveform has an infinite number of frequency components and hence an infinite bandwidth.

- As we add additional odd multiples off, suitably scaled, the resulting waveform approaches that of a square wave more and more closely.

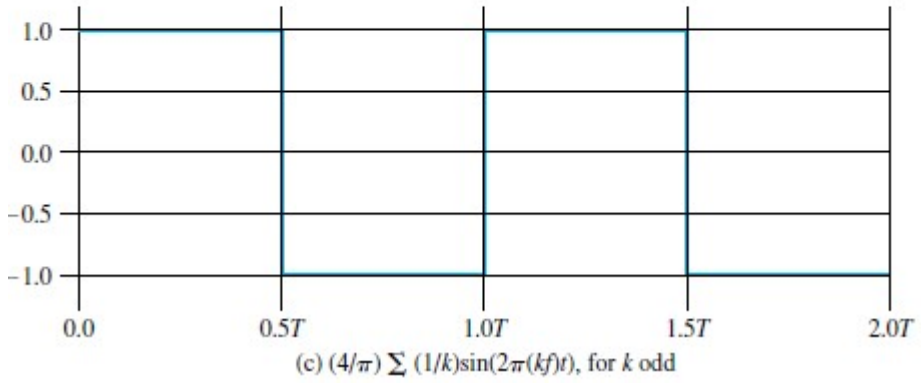
- The shape of the resulting waveform is reasonably close to that of the original square wave.



(a) $(4/\pi)\,[\sin(2\pi ft) + (1/3)\sin(2\pi(3f)t) + (1/5)\sin(2\pi(5f)t)]$



(b) $(4/\pi)\,[\sin(2\pi ft) + (1/3)\sin(2\pi(3f)t) + (1/5)\sin(2\pi(5f)t) + (1/7)\sin(2\pi(7f)t)]$



(c) $(4/\pi) \sum (1/k)\sin(2\pi(kf)t)$, for k odd

Simple Signal

- A Simple signal is the signal having exactly one frequency component – qualified by its frequency of oscillation
  - So a simple signal is the same as any electromagnetic wave
  - A single-frequency sine wave is not useful in data communications, composite signals used

Time domain representation

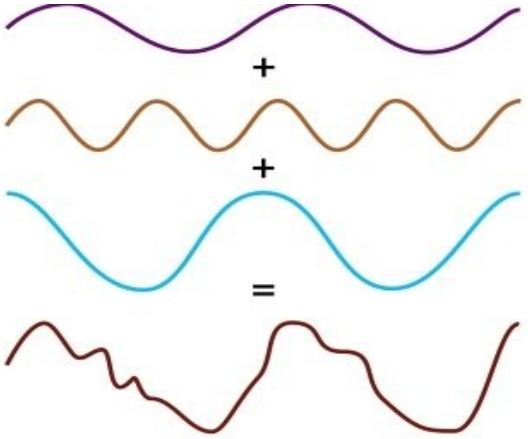
Note : The Carrier Signal used for modulation belongs to this category

Composite or Complex Signal

- A Complex signal is having multiple frequency components and represented by the sum of weighted frequency components

Time domain representation

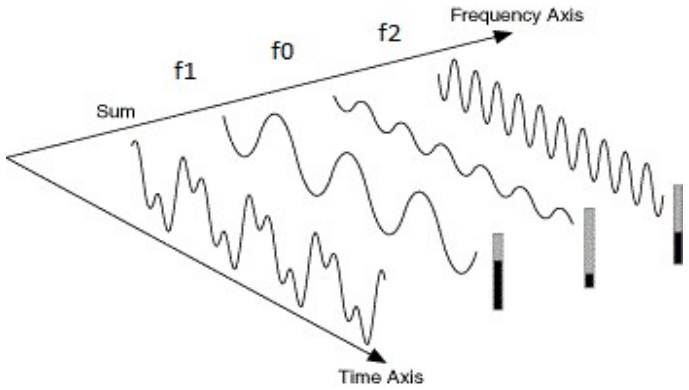
- Fourier analysis: any composite signal is a combination of simple sine waves with different frequencies, amplitudes, phases

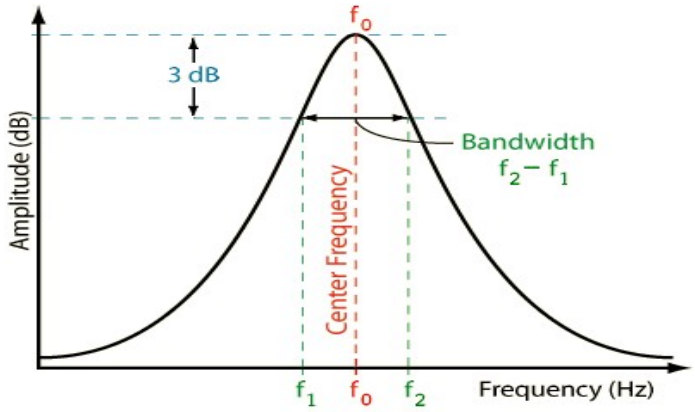


***Note** : The Audio, Video Signals are belongs to complex signal*

Bandwidth of a Signal

- Bandwidth can be imagined as a frequency width, sort of the fatness of the signal
- To convey information, an information signal needs to contain many different frequencies and it is this span of their frequency content that is called its bandwidth.
- The human voice, for example, spans in frequency from 30 Hz to 10 Khz.
- The more information in a signal, the larger the bandwidth of the information signal
- Bandwidth of the RHS signal is (f2-f1)





Relationship between data-rate & bandwidth

- Any transmission medium can accommodate only a limited band of frequencies
  - This limits the data rate that can be carried

- The greater the bandwidth of a medium, the higher is the data rate that can be transmitted, also more expensive the medium

- A given bandwidth can support various data rates, depending on the requirements of the receiver

Analog data, digital signal

- Digitization
  - Conversion of analog data into digital signal
  - Digital signal can then be transmitted using NRZ-L or some other code
  - Sampling rate required?
  - Quantization: approximate the sampled (analog) value to a digital level

- Methods
  - Pulse Code Modulation (PCM)
  - Pulse Amplitude Modulation (PAM)
  - Delta modulation: non-linear encoding
    - ✓ Quantization levels not evenly spaced

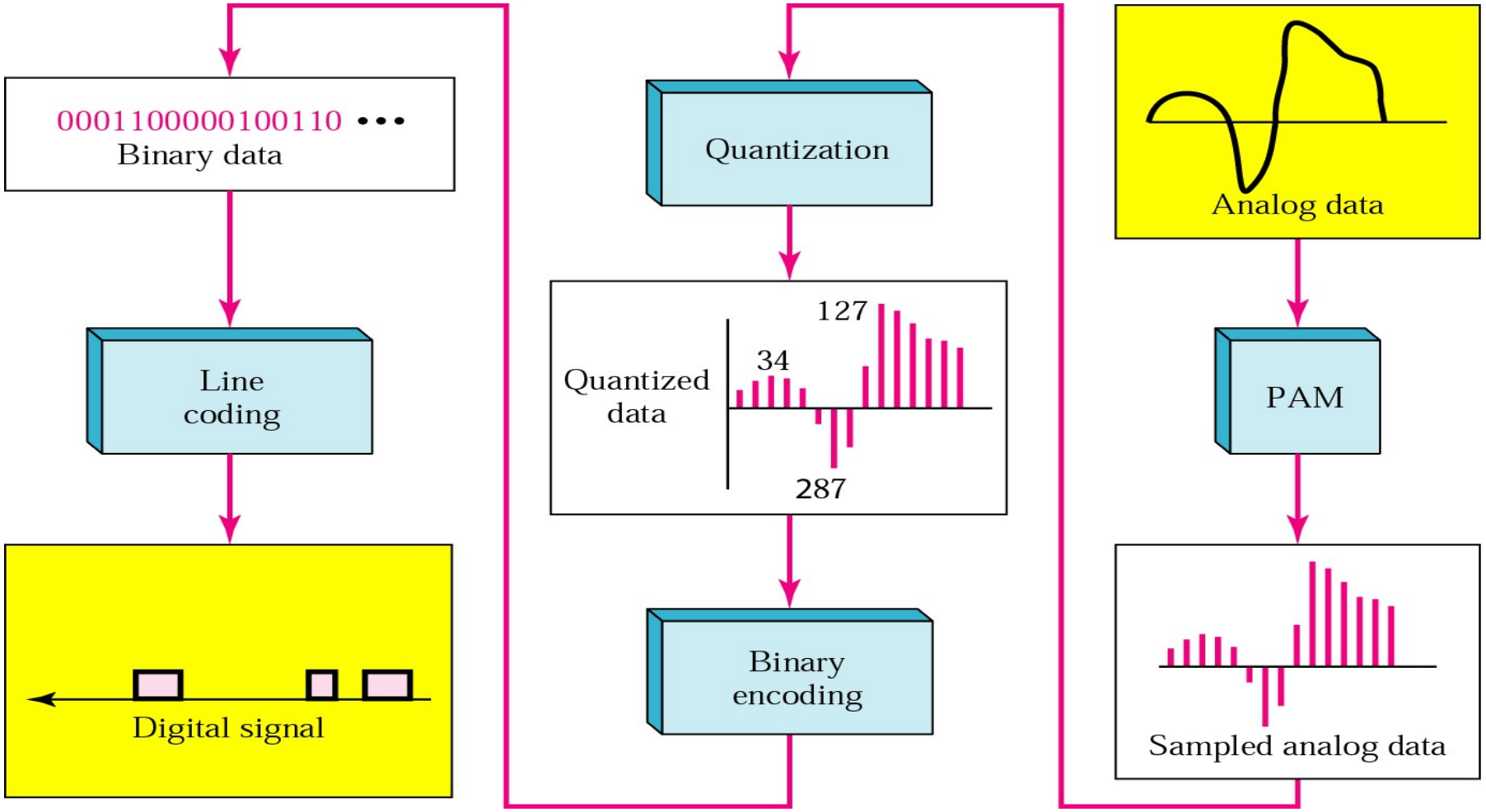
Pulse Code Modulation (PCM): In PCM, the amplitude of the analog signal is sampled at regular intervals, and each sample is quantized to a digital value.

Pulse Amplitude Modulation (PAM): PAM is a modulation technique where the amplitude of the analog signal is represented by the amplitude of the pulses in the digital signal.

Delta Modulation: Delta modulation is a form of analog-to-digital conversion where the difference between successive samples (delta) is encoded rather than the absolute value of each sample. It's a type of non-linear encoding where quantization levels may not be evenly spaced.

Encoding analog data to digital signal

For your study



Analog Transmission

- Analog signal transmitted without regard to content
- May be analog data (e.g. voice) or digital data (e.g. binary data passed through a modem)
- Attenuated over distance
- Use (cascaded) amplifiers to boost signal
- Also amplifies noise

Digital Transmission

- Concerned with content
- Can be transmitted only a limited distance before integrity endangered by noise, attenuation
- Repeaters used
  - Repeater receives signal, recovers the bit pattern
  - Retransmits a new signal
- Digital transmission becoming more and more popular

Transmission Impairments

- Signal received may differ from signal transmitted
- Effect on analog signal
  - degradation of signal quality
- Effect on digital signal
  - bit errors may get introduced
- Caused by
  - *Attenuation and attenuation distortion*
  - *Delay distortion*
  - *Noise*

Modulation

- Modulation is the process of conveying an information message signal (for example a digital bit stream or an analog audio signal) inside another signal (called Carrier signal) that can be physically transmitted over medium (wired or wireless)

- Through modulation information is encoded in a transmitted signal, while demodulation is the process of extracting information from the transmitted signal.

Carrier Signal

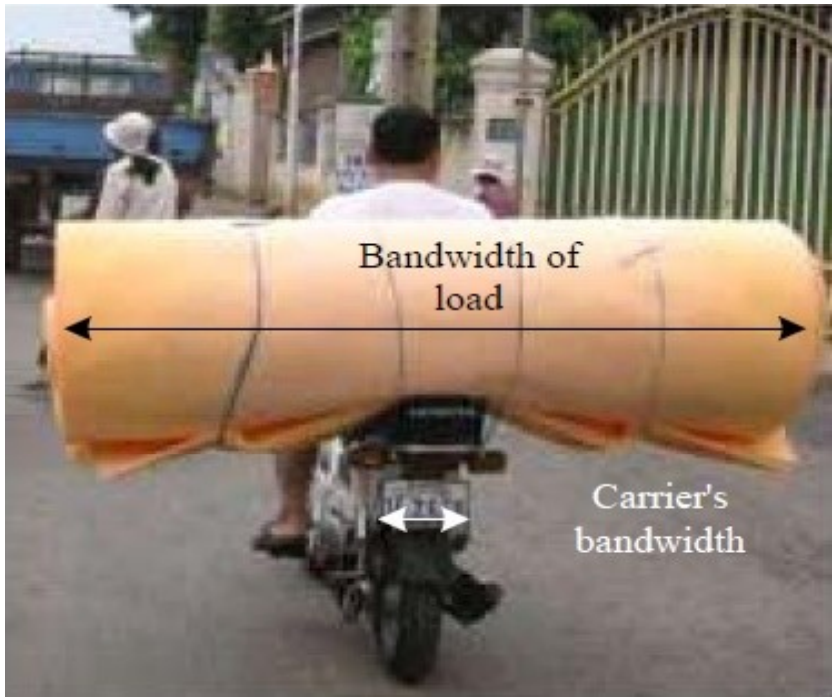
- The purpose of the carrier is usually –
  - Either to transmit the information through space as an electromagnetic wave (as in radio communication)
  - Or to allow several carriers at different frequencies to share a common physical transmission medium
  - The term originated in radio communication

- Carrier signal is very high frequency, as high frequency wave propagation is more suitable for long-distance.

- The bandwidth of a carrier signal is zero. That is because a carrier is composed of a single frequency

- Carrier frequency places the information signal into a suitable position in the electromagnetic spectrum.

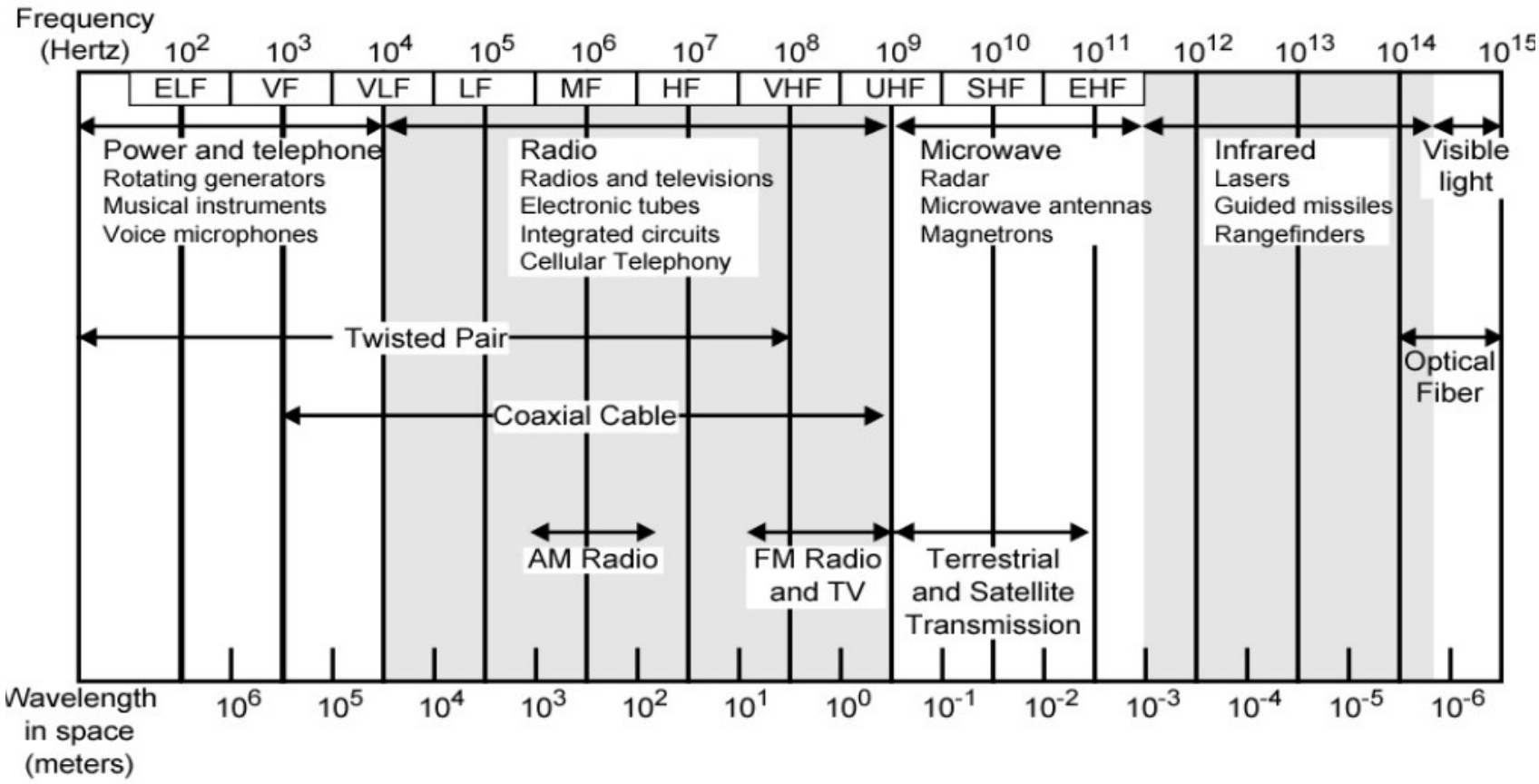
Bandwidth and Carrier Signal Analogy



- The modulated signal takes on the bandwidth of the information signal it is carrying like this person on the motorcycle.
- He is the modulated signal and his bandwidth just went from near zero, without the load, to the size of the mattress which is his "information" signal.

Band or Spectrum

The electromagnetic spectrum is the range of all possible frequencies of electromagnetic radiation



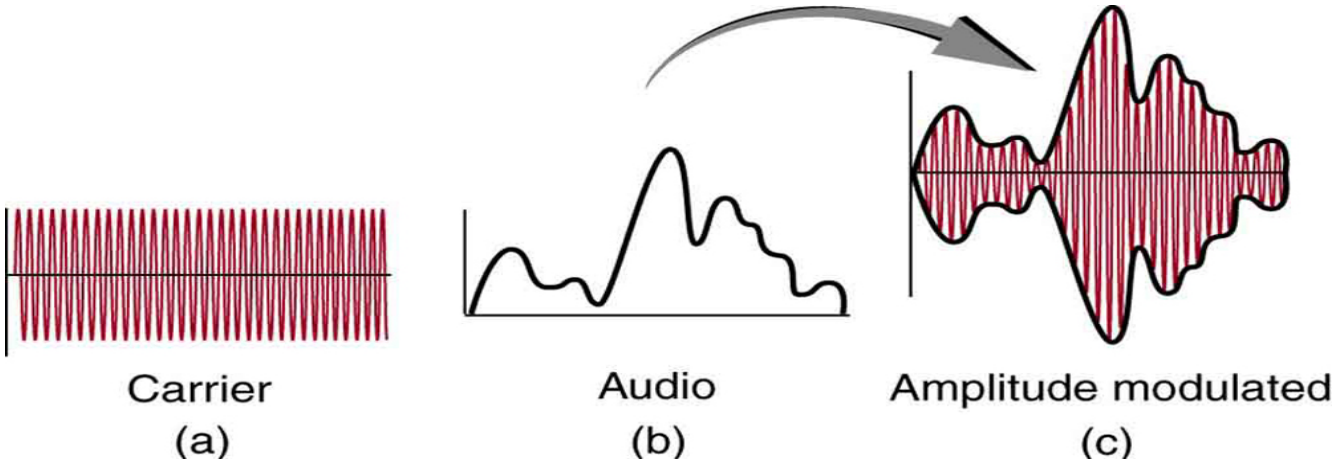
ELF = Extremely low frequency
VF = Voice frequency
VLF = Very low frequency
LF = Low frequency
MF = Medium frequency
HF = High frequency
VHF = Very high frequency
UHF = Ultrahigh frequency
SHF = Superhigh frequency
EHF = Extremely high frequency

Analog Modulation

Analog modulation : Amplitude Modulation (AM)

- AM works by varying the strength (amplitude) of the carrier signal in proportion to the waveform being sent.

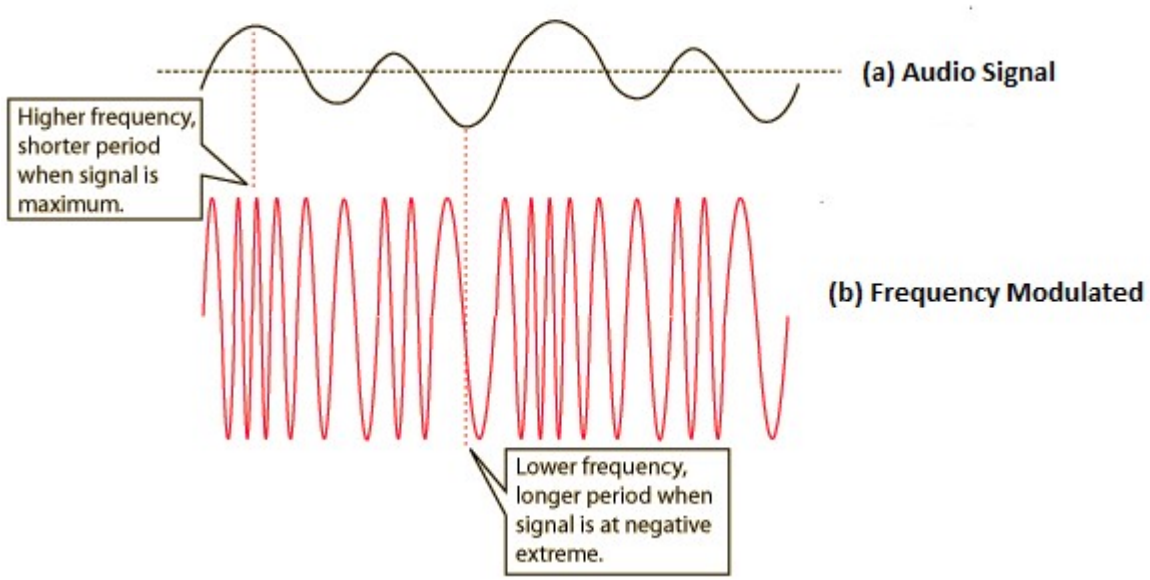
- Note : Frequency and Phase of the carrier signal remains constant



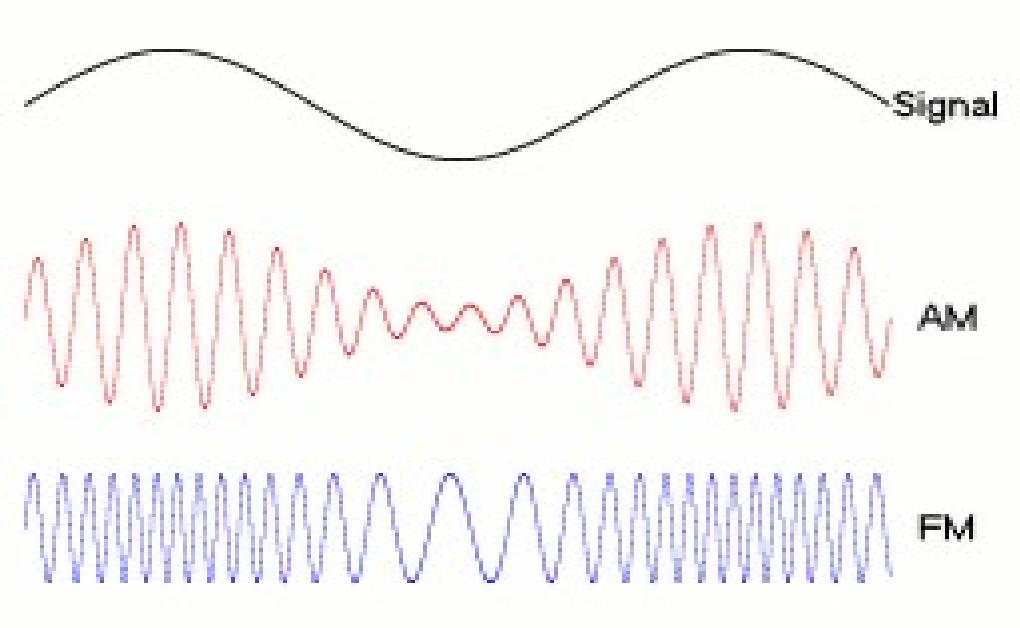
Analog modulation : Frequency Modulation (FM)

- FM works by varying the frequency of the carrier signal in proportion to strength (amplitude) the waveform being sent.

- Note : Amplitude and Phase of the carrier signal remains constant



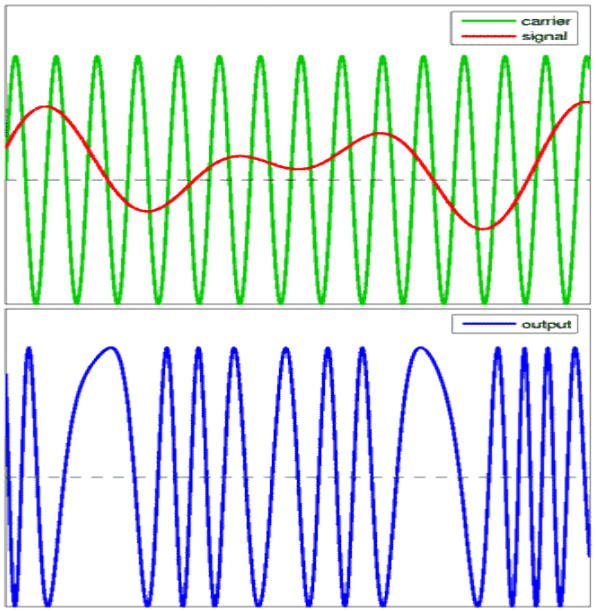
AM and FM demonstration



Analog modulation : Phase Modulation (PM)

- PM works by varying the phase of the carrier signal (advancing or retarding) in proportion to strength (amplitude) the waveform being sent.

- Note : Amplitude and Frequency of the carrier signal remains constant



Digital Modulation (Data Encoding)

Digital Modulation / Data Encoding

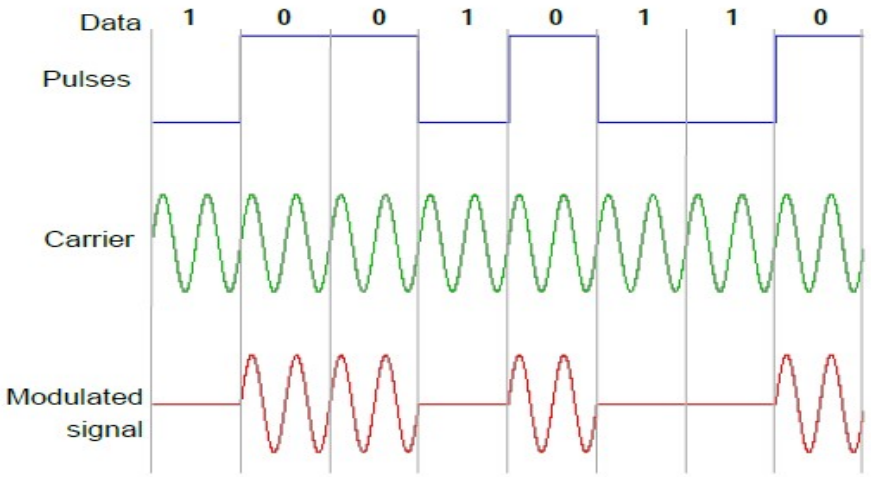
- Digital modulation is a process when an analog carrier signal is modulated by a digital bit stream.

- Digital modulation method can be considered as digital-to-analog conversion and the corresponding demodulation or detection as analog-to-digital conversion.

- A modem (modulator-demodulator) converts digital data to analog signal.
  - There are 3 ways to modulate a digital signal on an analog carrier signal.

Amplitude Shift Keying (ASK)

Two binary values are represented by two different amplitude of the carrier frequencies



Advantage :

✓Simple and Requires low bandwidth

Disadvantage :

✓Very susceptible (not resistant) to noise interference – noise usually (only) affects the amplitude. That causes rapid fluctuations the signal's amplitude

Application :

✓Not used for wireless radio transmissions (apart from infrared systems), but favored for optical transmissions in wired networks

Frequency Shift Keying (FSK)

Two binary values are represented by two different frequencies

<u>Advantage :</u>

✓FSK is less susceptible to errors than ASK – receiver looks for specific frequency changes over a number of intervals, so voltage (noise) spikes can be ignored.

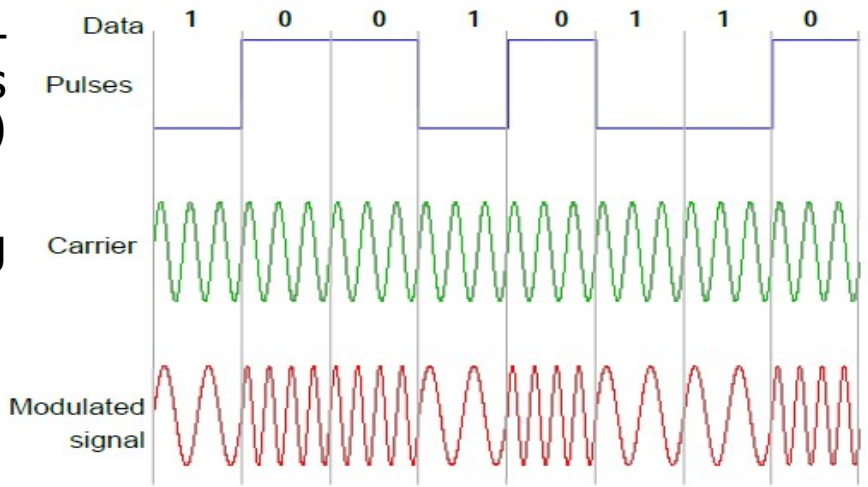
✓Easy to decode and suitable for long distance communication

<u>Disadvantage :</u>

✓FSK requires higher bandwidth than ASK

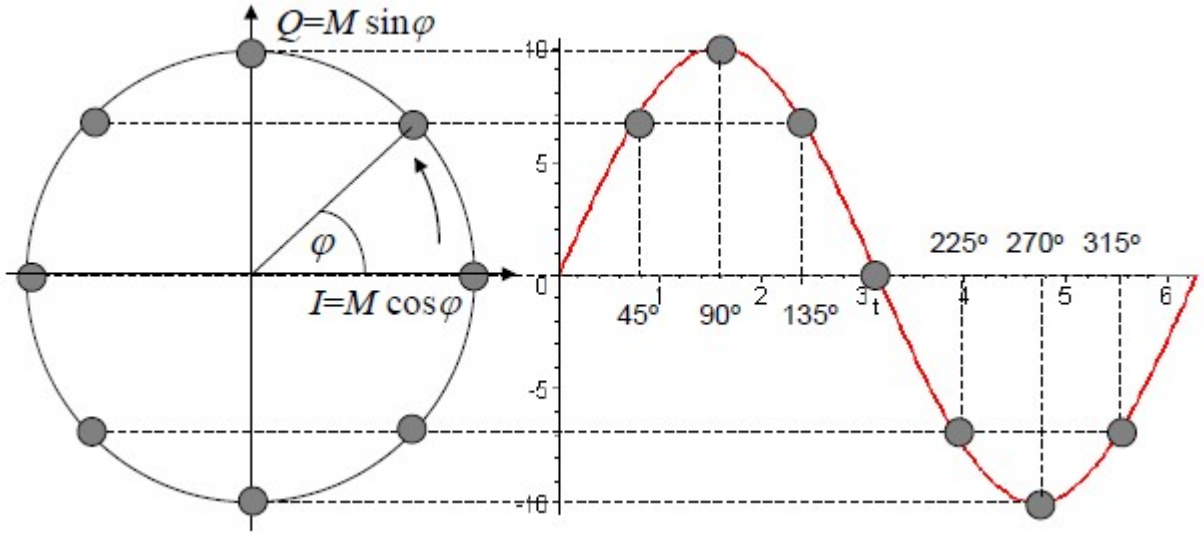
<u>Application :</u>

✓Used over voice lines (telephone lines) as well radio transmission, etc.



Phase Domain

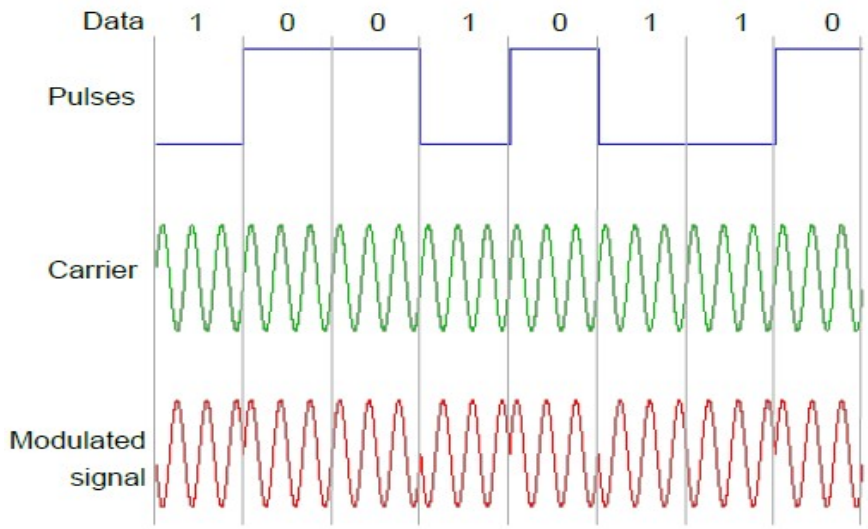
- Third way to represent signals (in addition to time and frequency domain)
- Shows the amplitude M of a signal and its phase ϕ in polar coordinates
- X-axis is called In-Phase(I), y-axis is called Quadrature-Phase(Q)



Phase Shift Keying (PSK)

Two binary values are represented by shift the phase of the carrier signal.

This simple scheme, shifting the phase by 180 degree each time the value of data changes is called BPSK



Advantage :

✓PSK requires less bandwidth than FSK

✓PSK is less susceptible to errors than ASK

✓Suitable for long distance communication

Disadvantage :

✓Decoding is complex as phase changes needs to be tracked

Application :

✓Used for Wireless radio transmission such as UMTS, WLAN

PSK with Multiple Signal States

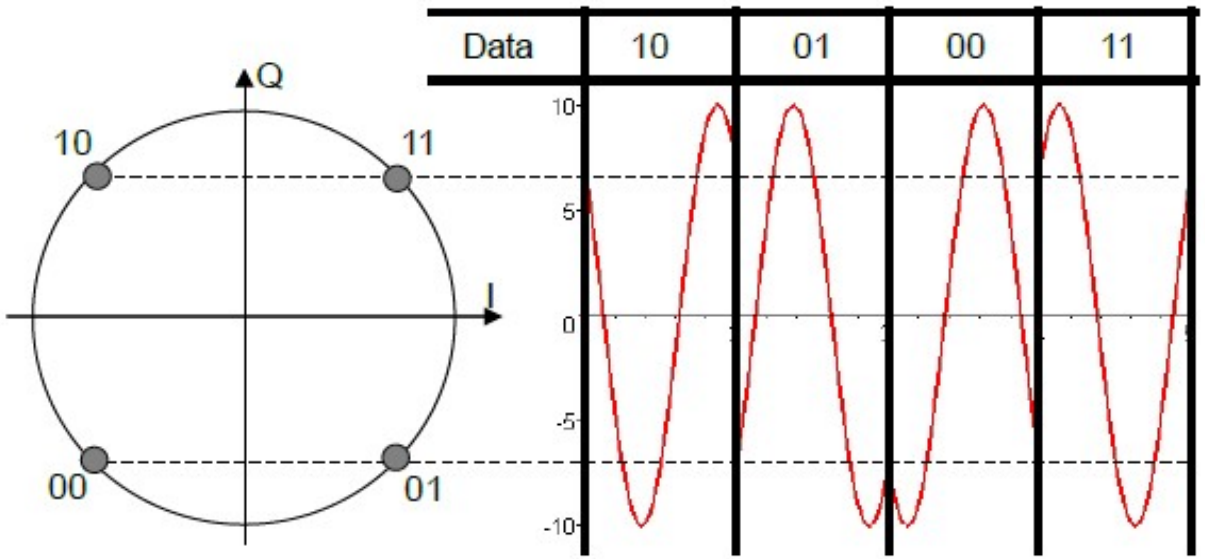
So far: each kind of shift keying defines two signal states for representing binary 0 or 1

But: a shift keying scheme can fix an arbitrary number of signal states (in theory) to increase the number of bits transferred in a single modulation step

Example: Quadrature Phase Shift Keying (QPSK)

- Four signal states. two bits are transmitted in a single step
- Used in UMTS and IEEE 802.11 (WLAN)

Constellation Diagram



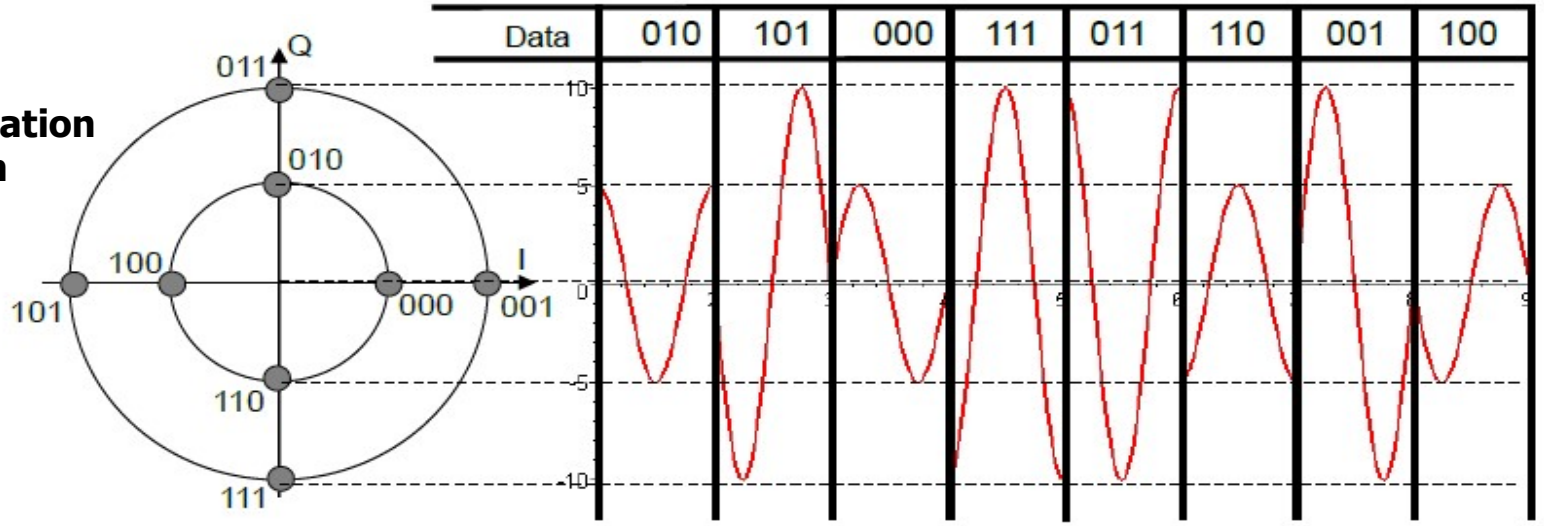
Mixing of Shift Keying Methods

It is also possible to mix different types of shift keying schemes

Example: Quadrature Amplitude Modulation (QAM)

- Combination of ASK and QPSK
- Eight signal states, three bits are transmitted in a single step
- Used as one alternative for IEEE 802.11 (WLAN)

Constellation Diagram



Relationship between data rate and signal rate

- The **data rate** defines the number of bits sent per sec - bps. It is often referred to the bit rate.
- The **signal rate** is the number of signal elements sent in a second and is measured in bauds. It is also referred to as the modulation rate.
- Goal is to increase the data rate whilst reducing the baud rate.
- The baud or signal rate can be expressed as:

$$S = R / n \text{ bauds}$$

where R is data rate (Bit rate)

n is the number of bit / symbol

Note that total number of symbol elements $L = 2^n$

Line codeing

Digital data to digital signals

- A digital signal is sequence of discrete, discontinuous voltage pulses. Each pulses a signal element.
- Encoding scheme is an important factor in how successfully the receiver interprets the incoming signal.
- Considerations for choosing a good signal element referred to as line encoding
  - Baseline wandering
  - DC components
  - Self synchronization
  - Error detection
  - Noise and interference

Line encoding challenges

- Baseline wandering - a receiver will evaluate the average power of the received signal (*called the baseline*) and use that to determine the value of the incoming data elements. If the incoming signal does not vary over a long period of time, the baseline will drift and thus cause errors in detection of incoming data elements.
  - A good line encoding scheme will prevent long runs of fixed amplitude.
- DC components - when the voltage level remains constant for long periods of time, there is an increase in the low frequencies (*around ZERO, called DC component*) of the signal. Most channels are bandpass and may not support the low frequencies.
  - This will require the removal of the DC component of a transmitted signal.

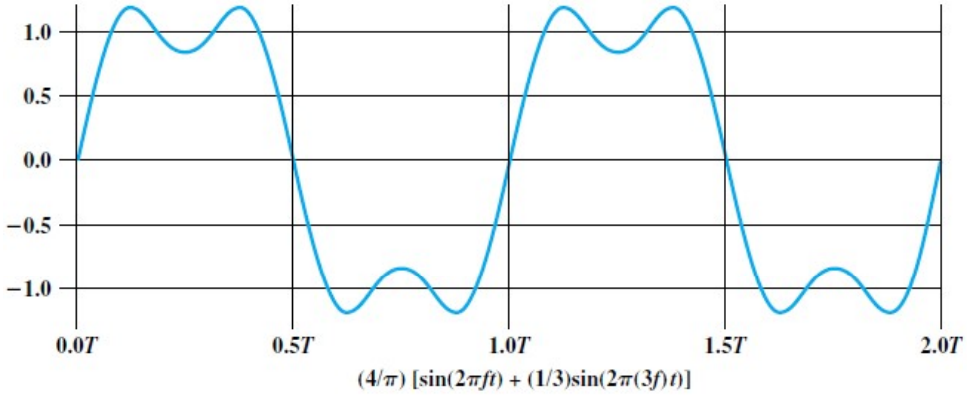
DC Component – an example

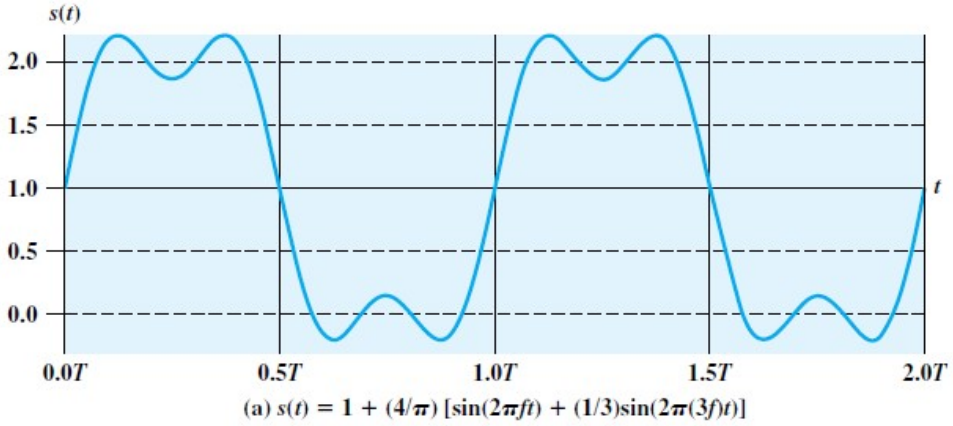
- If a signal includes a component of zero frequency, that component is a direct current (dc) or constant component.

- Fig with no dc component, a signal has an average amplitude of zero, as seen in the time domain.

- With a dc component, it has a f = 0 frequency term and a nonzero average amplitude.

- In a sense, the DC component is like the "zero frequency component", since cos(2π ·0·t) = 1. We often think of offset in this way, and plot the DC offset at f = 0 in the frequency-domain representation.

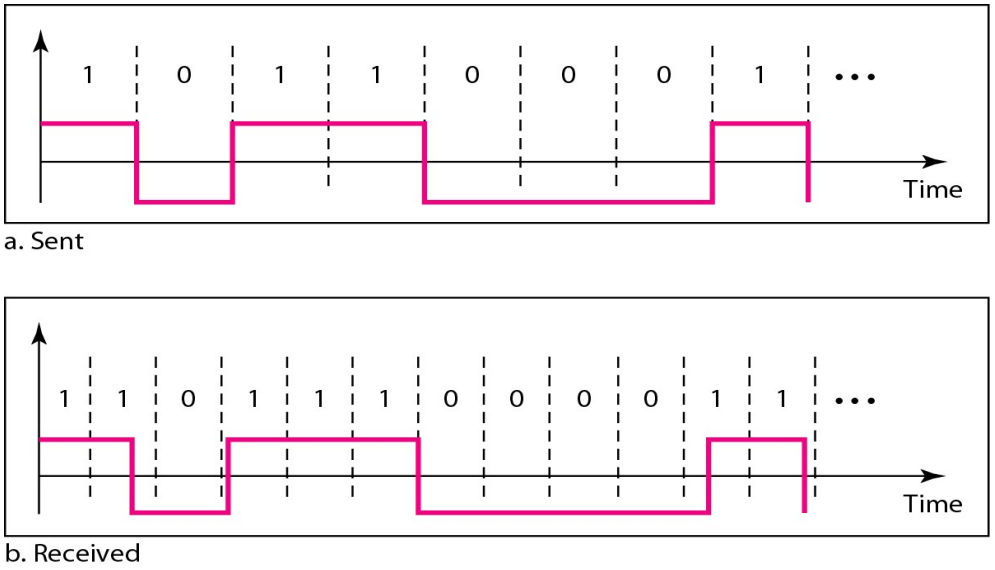




Line encoding challenges (contd.)

- Self synchronization - the clocks at the sender and the receiver must have the same bit interval.
  - If the receiver clock is faster or slower it will misinterpret the incoming bit stream.

Effect of lack of synchronization

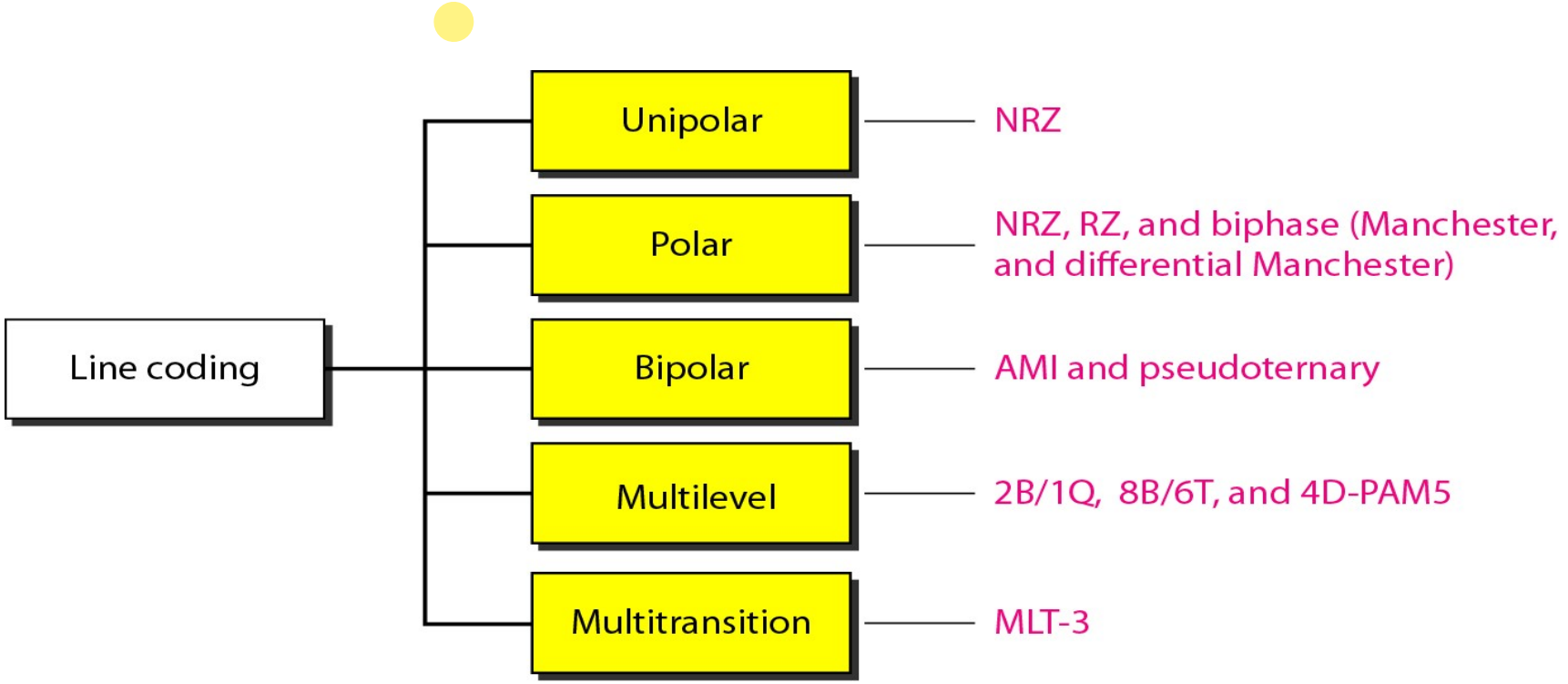


Line encoding challenges (contd. II)

- Error detection - errors occur during transmission due to line impairments.
  - Some codes are constructed such that when an error occurs it can be detected.
    - ✓ For example: a particular signal transition is not part of the code. When it occurs, the receiver will know that a symbol error has occurred.

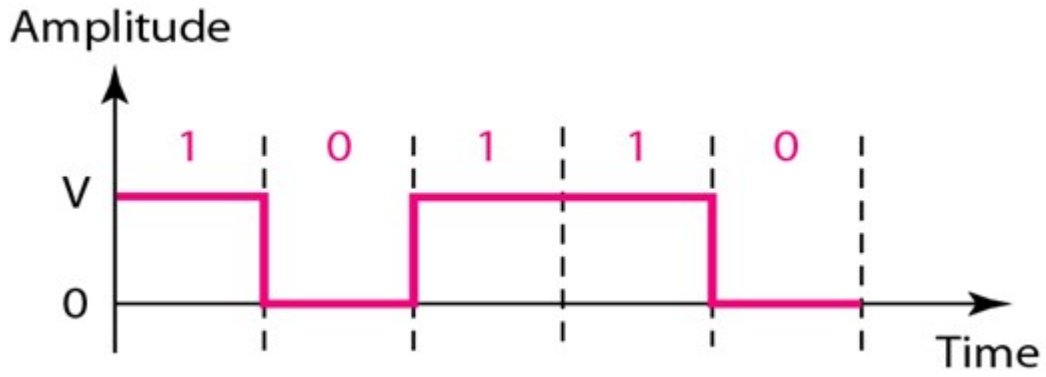
- Noise and interference - there are line encoding techniques that make the transmitted signal "immune" to noise and interference.
  - This means that the signal cannot be corrupted, it is stronger than error detection.

Line coding schemes

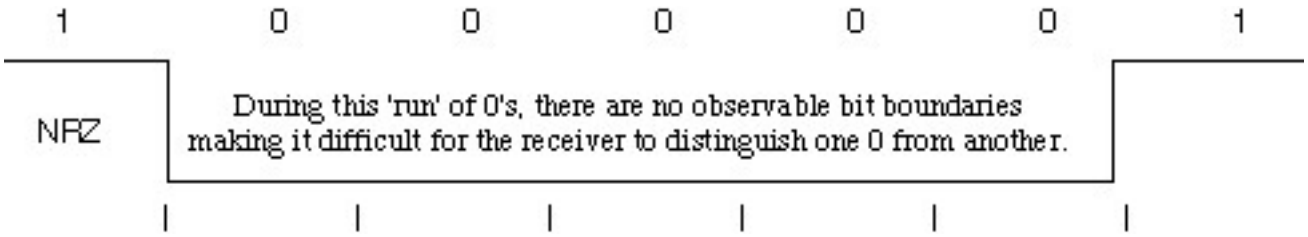


Unipolar

- All signal levels are on one side of the time axis - either above or below
- Voltage held constant during each bit interval
- NRZ - Non Return to Zero scheme is an example of this code. The signal level does not return to zero during a symbol transmission.



Non Return to Zero(NRZ) problem



- ✓ Problem arises when there is a long sequence of 0s or 1s and the voltage level is maintained at the same value for a long time.
- ✓ This creates a problem on the receiving end because now, the clock synchronization is lost due to lack of any transitions and hence, it is difficult to determine the exact number of 0s or 1s in this sequence
- ✓ separate clock line need to be provided.
- ✓ Problem of DC component

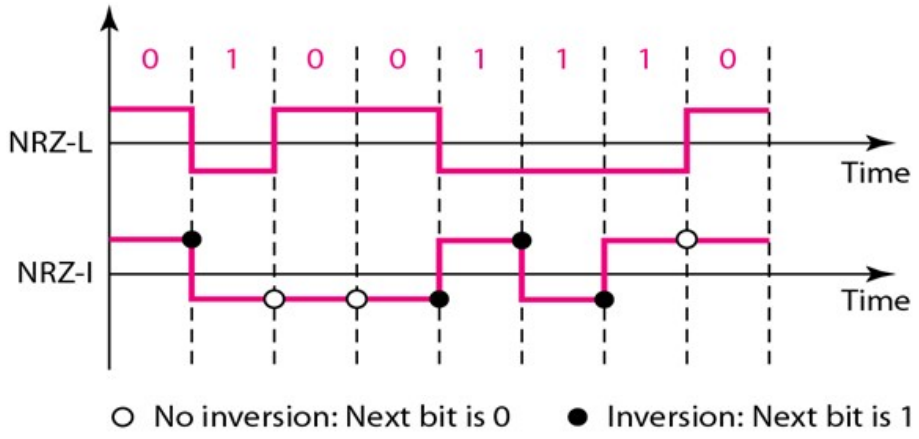
Polar - NRZ

- The voltages are on both sides of the time axis.
- Polar NRZ scheme can be implemented with two voltages. E.g. +V for 1 and -V for 0.
- There are two versions:
  - NZR - Level (NRZ-L)
  - NRZ - Inversion (NRZ-I)
- Problem of long sequence of 0s or 1s persists - baseline wandering and DC component problem

- Relatively simple to implement.

Polar – NRZ (contd.)

- NRZ-Level
  - Binary 1 → negative voltage
  - Binary 0 → positive voltage (or vice versa)
- NRZ-Inverted: Nonreturn to zero, invert on ones
  - Binary 1 → transition (low-to-high or high-to-low) at the beginning of a bit interval
  - Binary 0 → no transition
  - An example of differential encoding (data represented by changes rather than levels)



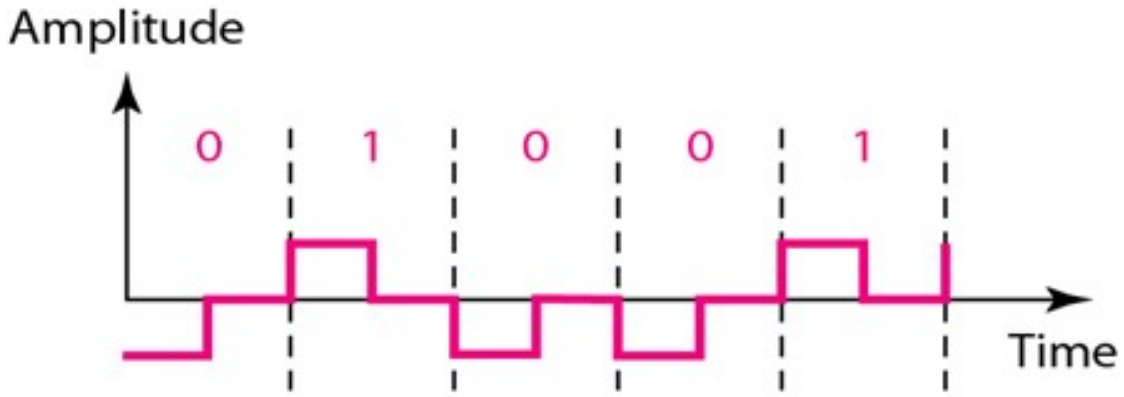
Disadvantages

✓NRZ-L and NRZ-I both have a DC component problem and baseline wandering, it is worse for NRZ-L.

✓Both have no self synchronization & no error detection.

Polar - RZ

- The Return to Zero (RZ) scheme uses three voltage values. +, 0, -.
- Each symbol has a transition in the middle of each bit-period. Either from high to zero or from low to zero.
- Voltage level NOT constant over an entire bit-interval

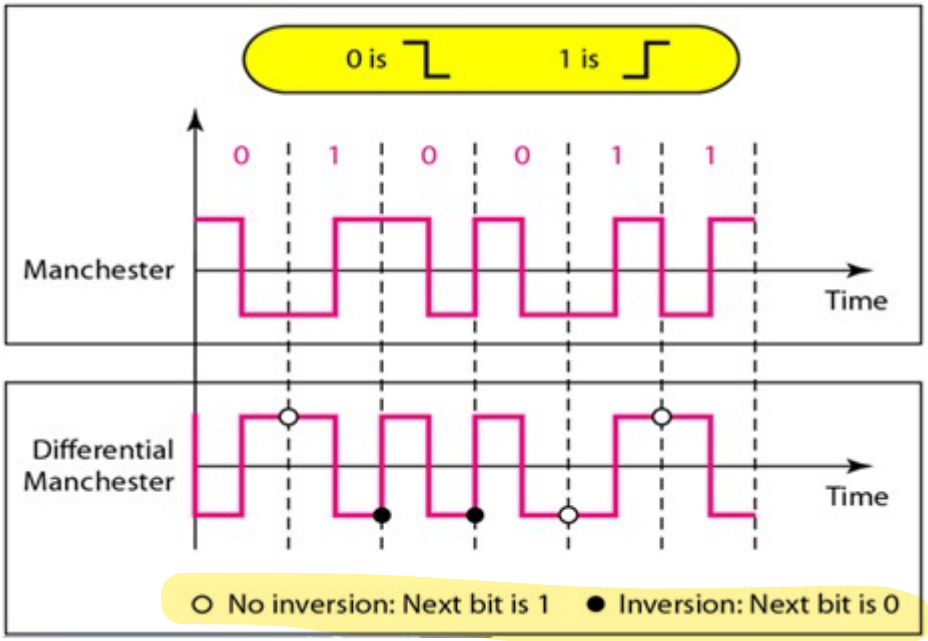


- Advantages
  - ✓ No DC components or baseline wandering.
  - ✓ Self synchronization - transition indicates symbol value.
- Disadvantage
  - ✓ More complex as it uses three voltage level.

Polar - Biphase: Manchester and Differential Manchester

- Manchester coding consists of combining the NRZ-L and RZ schemes.
  - Every symbol has a level transition in the middle: from high to low or low to high. Uses only two voltage levels.

- Differential Manchester coding consists of combining the NRZ-I and RZ schemes.
  - Every symbol has a level transition in the middle. But the level at the beginning of the symbol is determined by the symbol value. One symbol causes a level change the other does not.

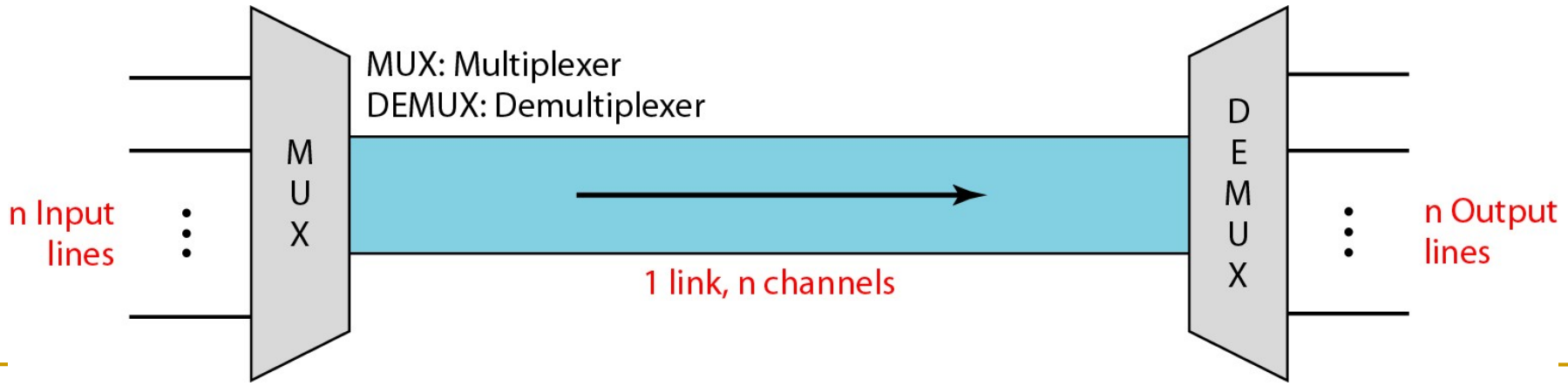


Multiplexing

Multiplexing

Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared.

Multiplexing is the set of techniques that allows the (simultaneous) transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic.



Multiplexing

Motivation

Task of multiplexing is to assign time, frequency, and code to each communication channel with a minimum of interference and a maximum of medium utilization

Communication channel refers to an association of sender(s) and receiver(s) that want to exchange data

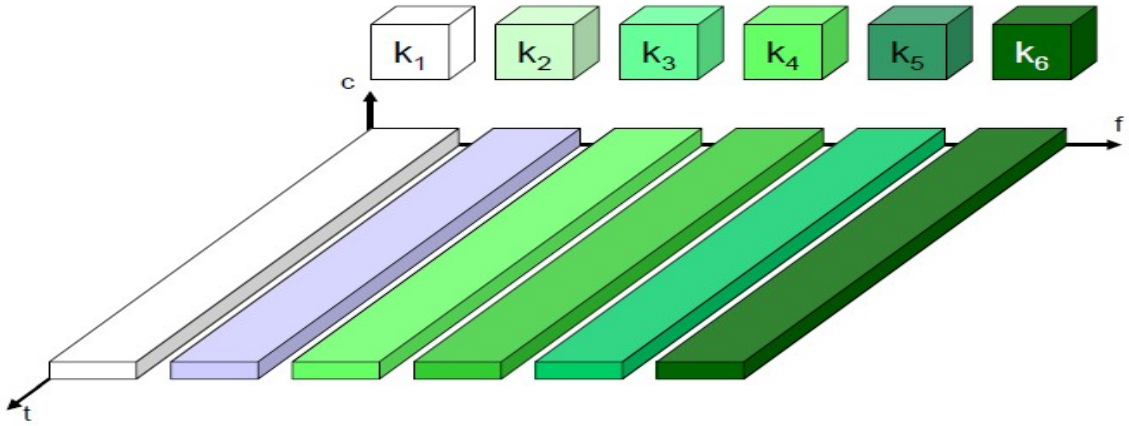
Classification of multiplexing

Four types :

- Frequency
- Time
- Code
- Wavelength

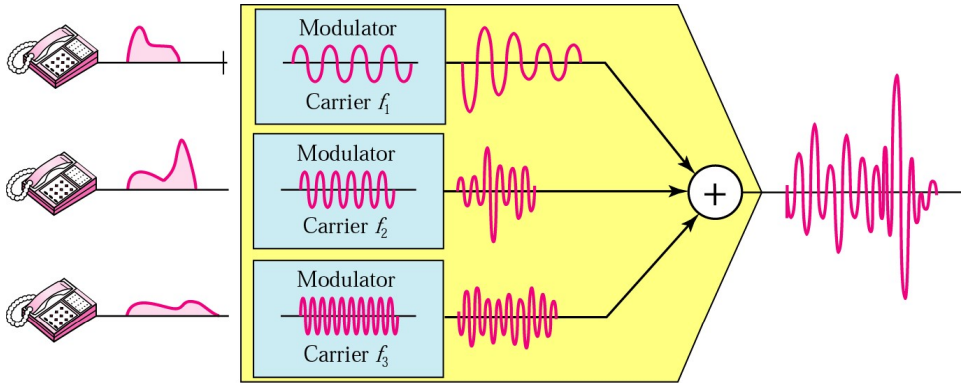
Frequency Division Multiplexing (FDM)

- Subdivision of the frequency dimension into several non-overlapping frequency bands, each continuously carrying one channel
- Guard spaces between frequency bands to avoid overlapping (adjacent channel interference)
- Permanent assignment of a frequency to a sender makes it advantageous for radio transmission (24 hours a day), but inapplicable for mobile communication (assignment of a permanent frequency band for each mobile device would result in a tremendous waste of scarce frequency resources)
- Simultaneously and continuously transmitting
- One circuit per channel

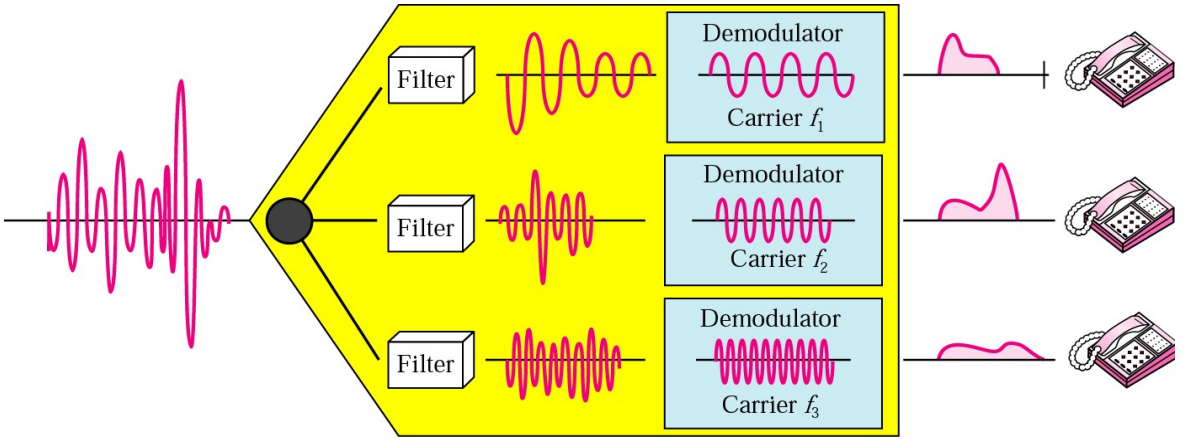


Frequency Division Multiplexing (FDM) contd

Multiplexing

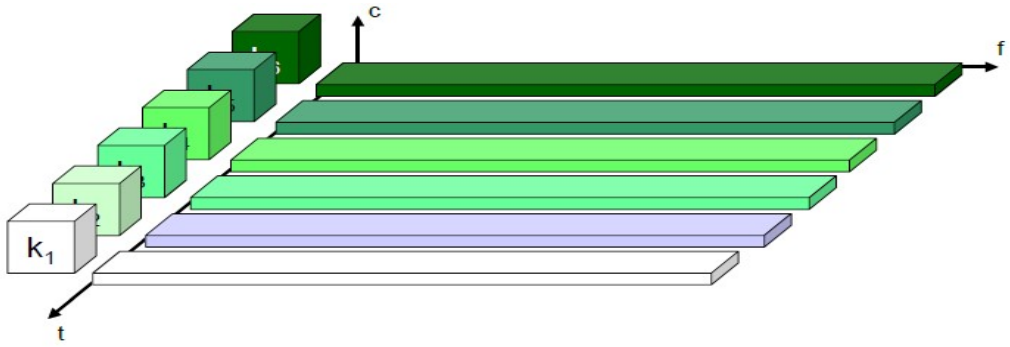


Demultiplexing

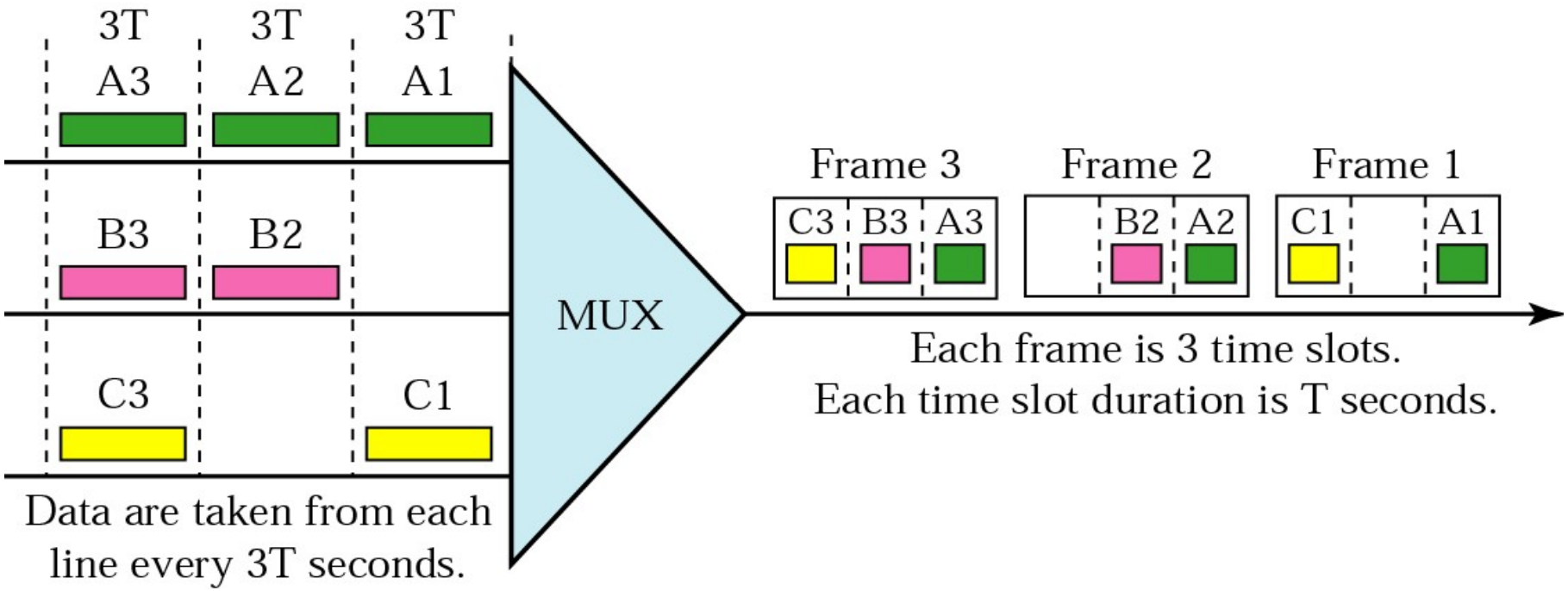


Time Division Multiplexing (TDM)

- All senders alternately use the same frequency at different points in time – a single carrier frequency for several users
- Avoidance of transmission overlaps (co-channel interference) by time gaps (guard spaces)
- Requires precise synchronization between senders (either by a precise clock or by a dedicated synchronization signal accessible for all senders)
- Flexible, as senders with heavy load can be assigned more sending time and senders with light load less sending time
- Transmission in bursts for each user, low battery consumption
- High synchronization overhead – stations has to be time synchronized



Time Division Multiplexing (TDM) example



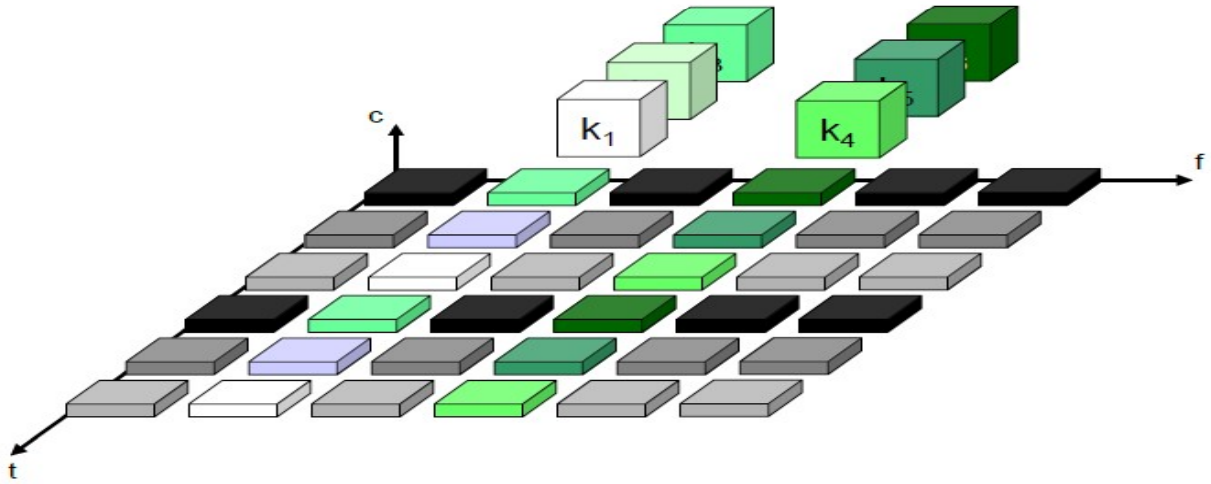
TDM Types

- Synchronous: Fixed number of time slots allocated for each source
  - May leave empty slots in a TDM frame (if one or more sources is not sending data)
  - To synchronize demux (in Rx) with mux (in Tx), extra framing bit transmitted with each TDM frame:
    - ✓ Framing bits define a control channel: similar to an additional channel having 1 bit per frame (say, alternate 101010…)
  - Many slots within a TDM frame may be wasted

- Statistical: Allocates time slots dynamically based on demand of the sources

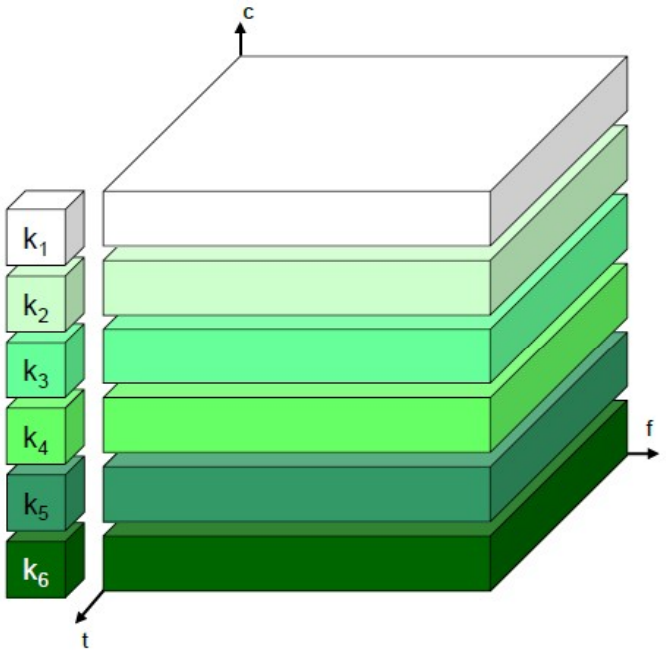
Combination of FDM and TDM

- Channel can use a certain frequency band for a certain amount of time
- Guard spaces in the time and in the frequency dimension
- Robust against small-scale fading by using frequency hopping(fast change of frequency bands)
- Deployed in GSM



Code Division Multiplexing (CDM)

- All channels use the same frequency band at the same time
- Separation by codes, guard spaces corresponds to the distance between codes (orthogonal codes)
- Good protection against interference and tapping (i.e., signals are spread on a broad frequency band, and interpretation of a signal is only possible with matching code)
- High complexity of the receivers
- Precise synchronization between sender and receiver
- Multiplexing technique for WLAN/UMTS



Principle of Spread Spectrum to be discussed later

CDM Analogy

All people are in the same room together.

They can all be talking the same time.

Provided -

- Each of the person talk and understand exactly one language
- Every one talk almost in same loudness (amplitude)

CDMA transmission and reception analogy

Tx 1 : Information Signal **S1**, Spreading Code **C1**. Transmits (**S1.C1**) over the air

Tx 2 : Information Signal **S2**, Spreading Code **C2**. Transmits (**S2.C2**) over the air

From Spreading code's auto-correlation and orthogonal property -

C1.C1 = 1

C2.C2 = 1

C1.C2 = 0

When signal transmitted from two source, over the air it becomes -

(S1.C1 + S2.C2)

Rx 1 : Despreading on reception **(S1.C1 + S2.C2).C1**

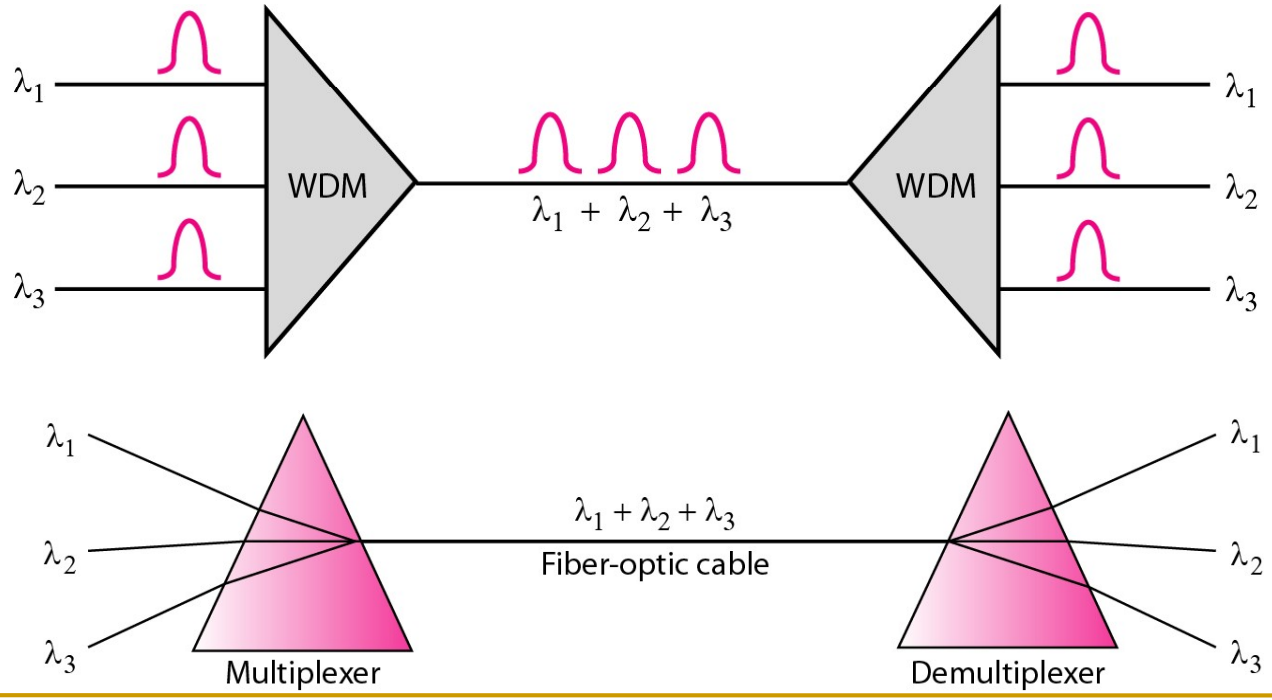
= S1.C1.C1 + S2.C2.C1 = S1

Rx 2 : Despreading on reception **(S1.C1 + S2.C2).C2**

= S1.C1.C2 + S2.C2.C2 = S2

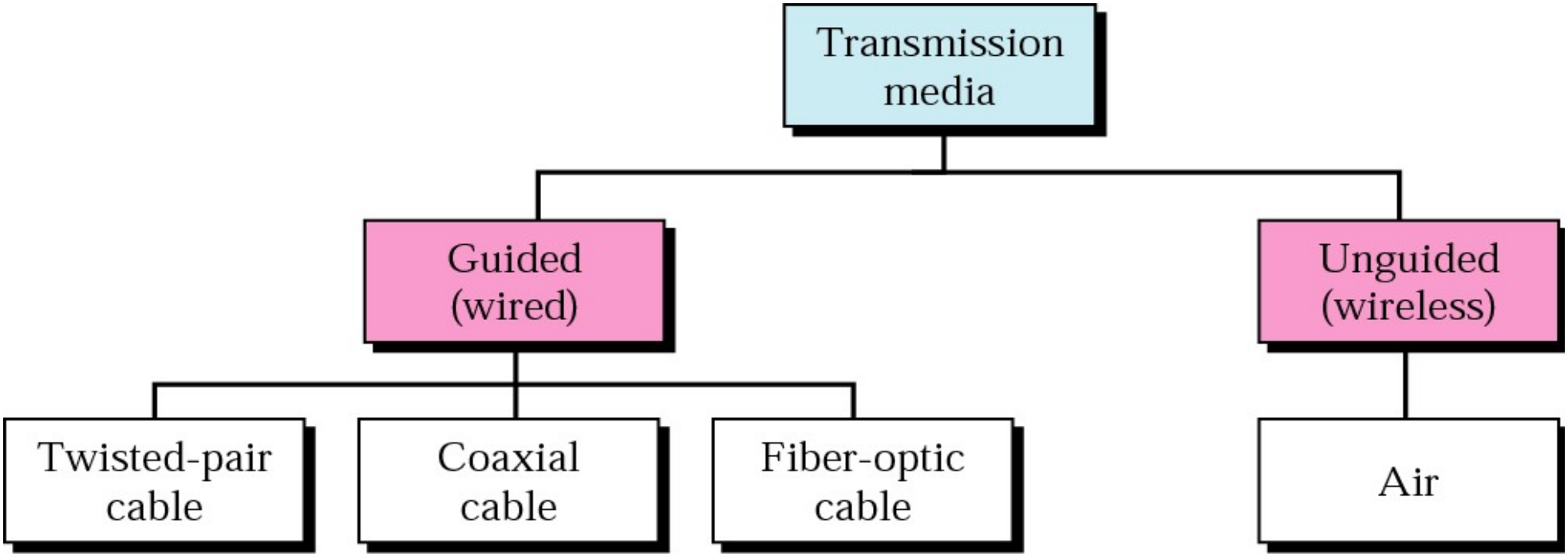
Wavelength-division multiplexing (WDM)

- WDM is an analog multiplexing technique to combine optical signals.
- WDM is same as FDM except that the optical signals are transmitted through the fibre optic cable. WDM is used on fibre optics to increase the capacity of a single fibre. It is used to utilize the high data rate capability of fibre optic cable.



Transmission Media

Types of media



Guided (Wired)

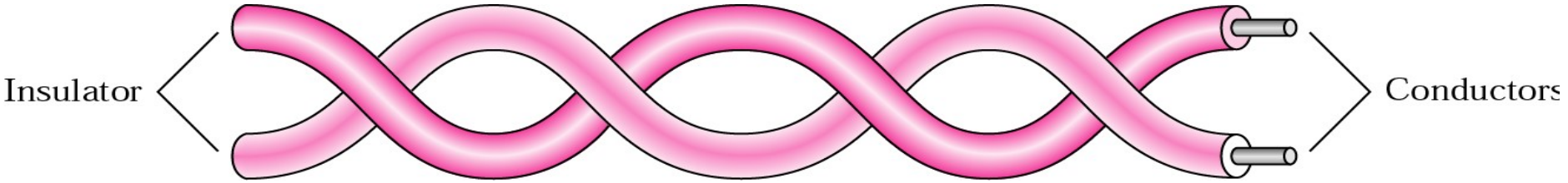
Twisted Pair

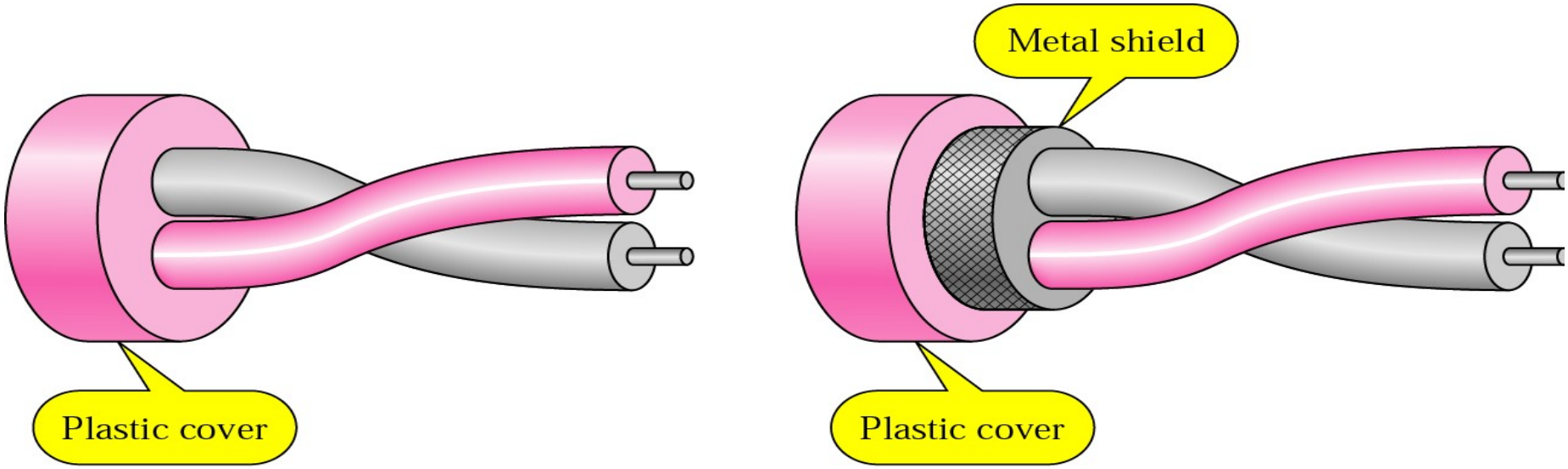
- Consists of two insulated copper wires
- Arranged in a regular spiral pattern to minimize the electromagnetic interference (EMI) between adjacent pairs
- Carries signals in lower frequency ranges
- Advantage – cheap, lightweight
- Disadvantage
  - relatively low bandwidth
  - more susceptible to interference/noise
  - Repeaters needed every 5-6 km for analog signal, every 2-3 km for digital signal

Unshielded and Shielded Twisted Pair

- UTP
  - Cheapest, easiest to install
  - Ordinary telephone wire
  - Suffers relatively more from external EMI
- STP
  - The pair is wrapped with metallic foil to insulate the pair from EMI
  - More expensive

Twisted pair





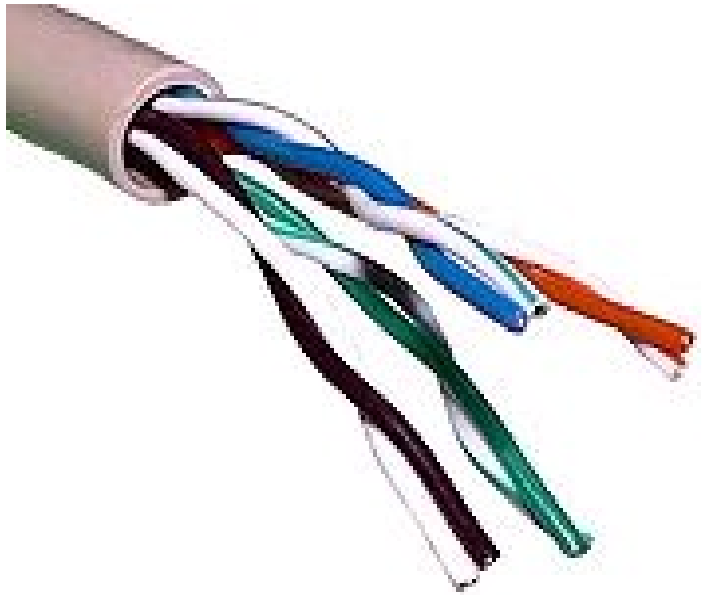
a. UTP

b. STP

Important UTP Categories

- Seven categories of UTP determined by cable quality: cat 1 (lowest quality) to cat 7

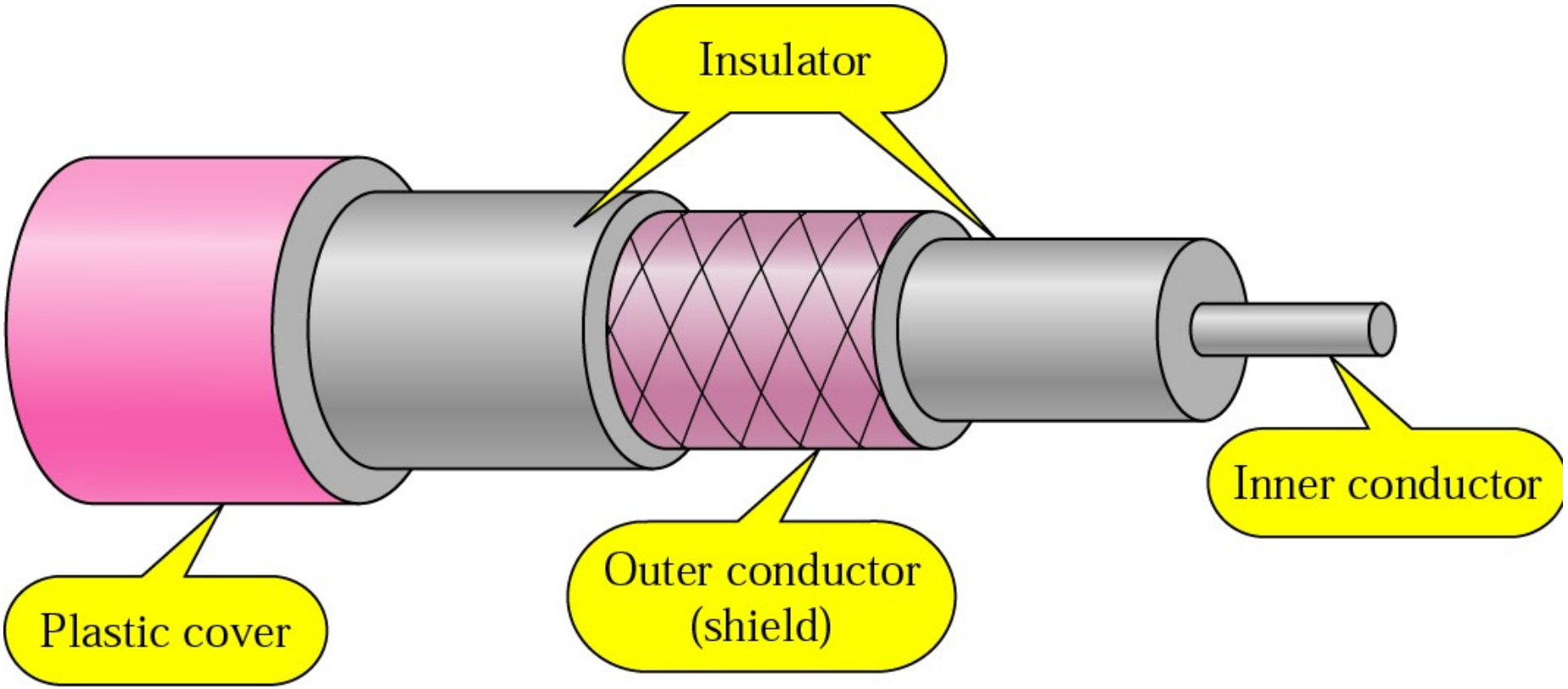
- Cat 5
  - Upto 100 Mbps
  - Commonly used in LANs



Coaxial Cable

- Carries signals of higher frequency ranges (compared to twisted pairs)
- Central core conductor of solid or stranded wire (usually copper)
- Enclosed in an insulating sheath
- Encased in an outer conductor of metal foil
- Outer conductor also enclosed in an insulating sheath, and the whole cable protected by a plastic cover
- Application: cable tv

Coaxial Cable

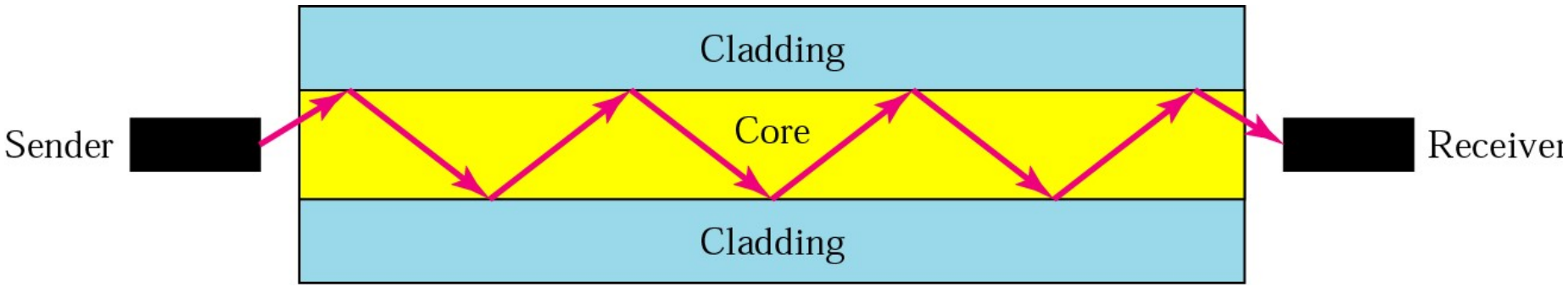


Optical Fiber

- Thin (2-125 micrometer), flexible medium capable of conducting an optical ray
- Cylindrical shape with three concentric sections: the ***core***, the ***cladding***, and the ***jacket***
- Greater data rates
- Smaller size & weight
- Lower attenuation
- Greater repeater spacing – tens of kilometres
- Highly secure
  - Difficult to tap into
  - Lack of signal radiation

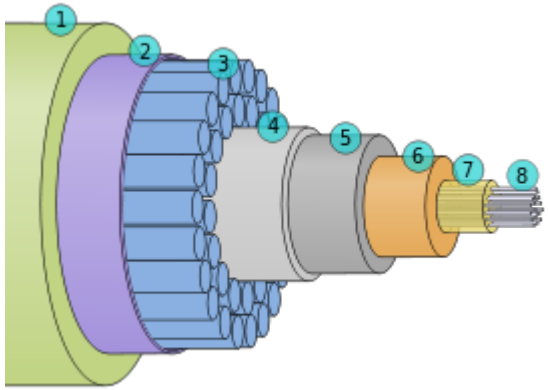
Optical Fiber

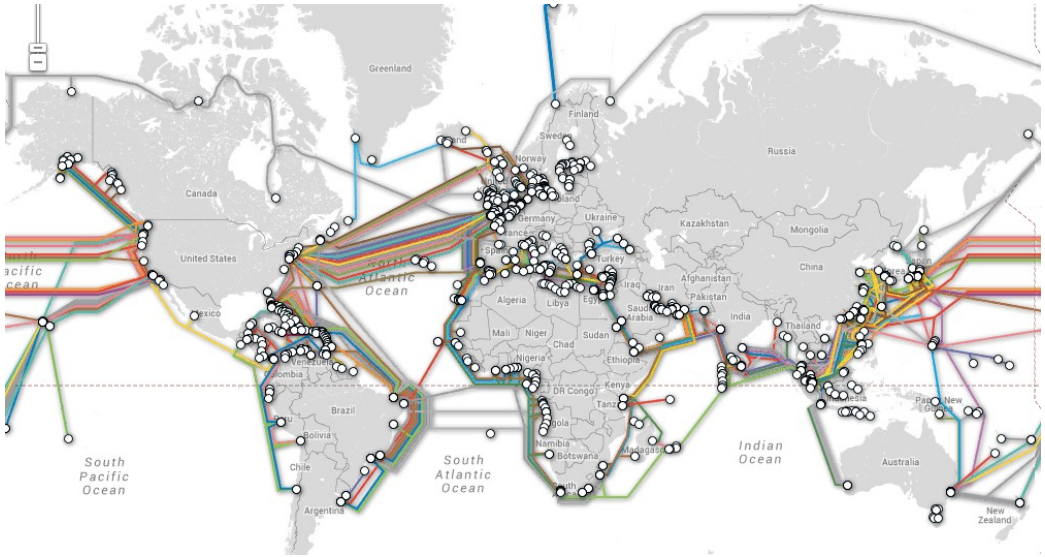
- A glass or plastic **Core** is surrounded by a **cladding** of less dense glass or plastic
- Difference of density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead being refracted into it



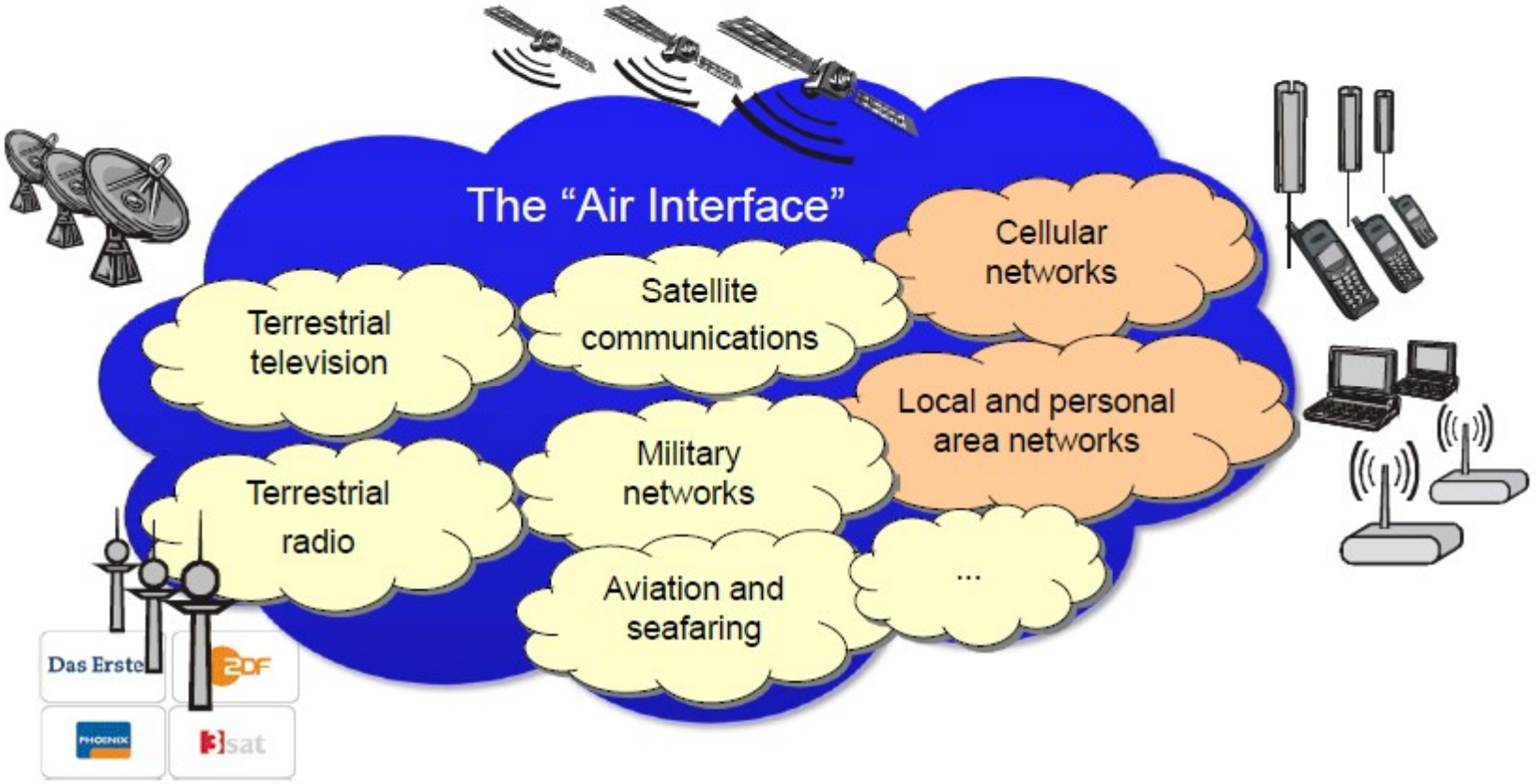
Submarine communications cable (undersea optical fibre cables)

- **Cable** laid on the sea bed between land-based stations to carry telecommunication signals across stretches of ocean
- Connected all the world's continents except Antarctica





Un-guided (Wireless)



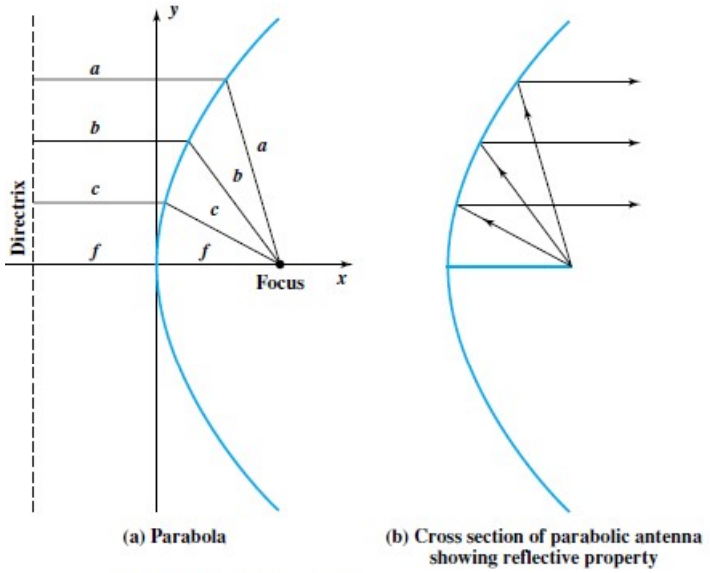
Wireless Transmission

- Unguided media, transmission and reception via antenna

- Directional
  - Signal transmitted as a focused beam
  - Careful alignment of antennae required

- Omnidirectional
  - Signal spreads in all directions
  - Can be received by many antennae

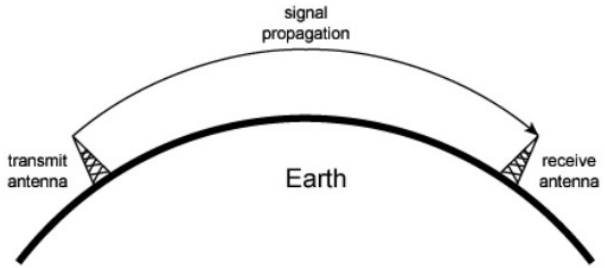
- Examples of wireless transmission
  - Terrestrial microwave transmission
  - Satellite transmission
  - Broadcast radio



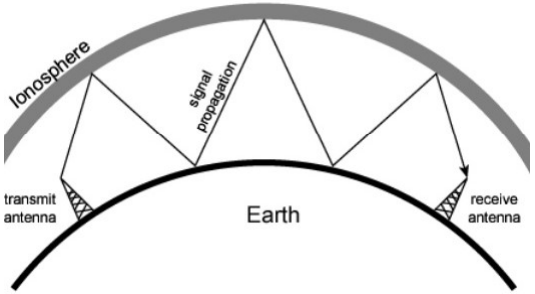
Parabolic Reflective Antenna

Radio Wave Propagation

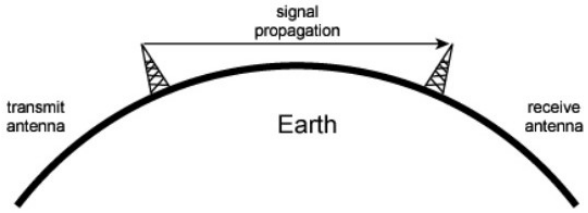
- Ground Wave Propagation
  - Follows contour of earth



- Sky Wave Propagation
  - Signal reflected from ionosphere layer of upper atmosphere



- Line-of-sight Propagation
  - High frequency signal transmitted in straight line



Band & Radio Wave Propagation

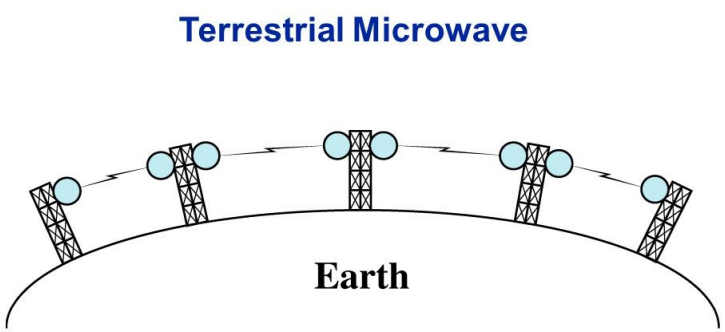
Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3-30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), ship/aircraft 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

Terrestrial Microwave

- Uses the radio frequency spectrum, commonly from 2 to 40 Ghz
- Transmitter is a parabolic dish antenna, mounted as high as possible
- Requires unobstructed line of sight between source and receiver
- Curvature of the earth requires stations (called repeaters) to be ~30 miles apart
- Applications
  - Long-haul voice and television transmission service

Terrestrial Microwave (contd.)

- Advantages
  - No cabling needed between sites
  - Wide bandwidth
  - Multi-channel transmissions possible



- Disadvantages
  - line of sight requirement
  - expensive towers and repeaters
  - subject to interference such as passing airplanes and rain

Satellite Microwave

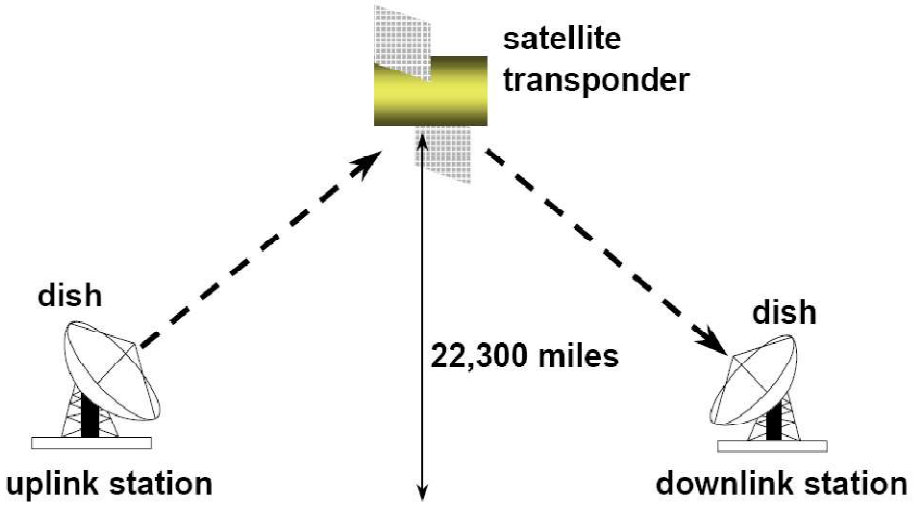
- Satellite: a microwave relay station in space
- Satellite receives signal from earth stations on one frequency (uplink)
- Amplifies or repeats signal and transmits on another frequency (downlink)
- The broadcast nature of the downlink makes it attractive for services such as the distribution of television programming
- Geostationary satellites used

Satellite Microwave (contd.)

- Applications
  - Satellite television distribution
  - Long-distance telephone transmission

- Advantages
  - Can reach a large geographical area
  - High bandwidth, high data rates
  - Cheaper over long distances

- Disadvantage
  - High initial cost
  - Susceptible to noise and interference
  - Propagation delay



Why don't we use satellites more than under-sea optical fibre cables for Internet ?

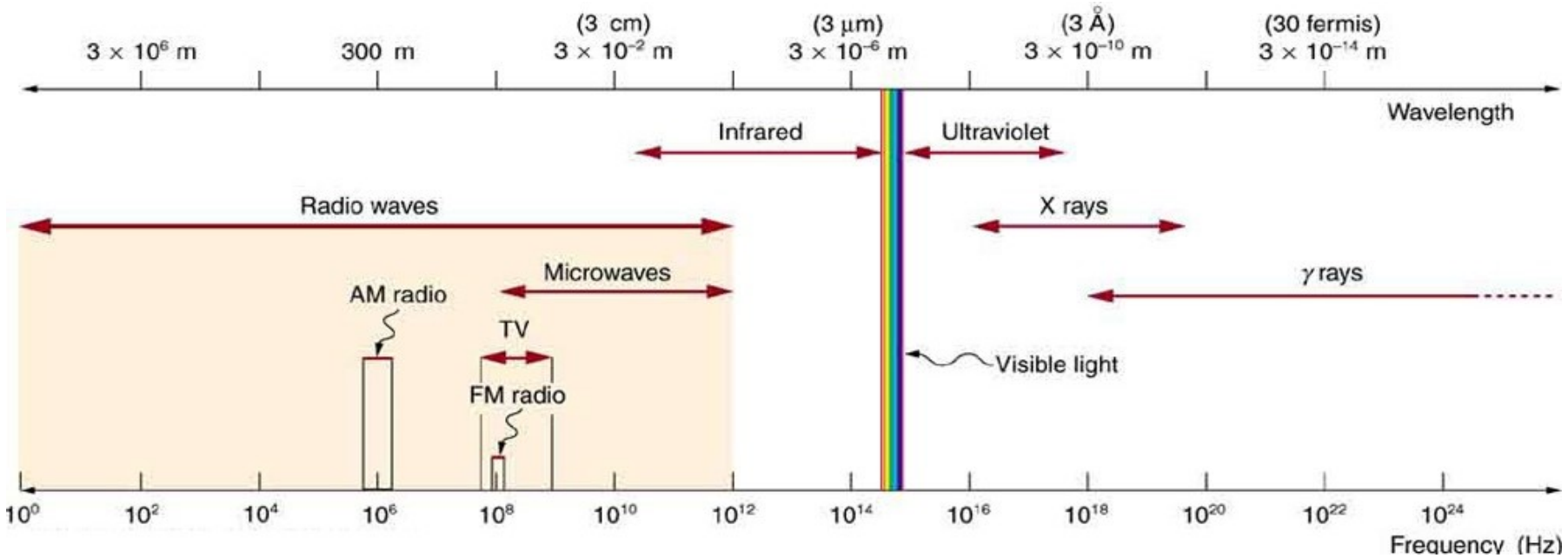
- Large communications satellites cost huge amounts of money but they can deliver coverage over wide areas pretty much irrespective of geography
- The problem with fibre is that it is point-to-point, a satellite can broadcast information to millions of people in parallel with no more effort than to deliver to one person.
- But for fibre to reach millions of people it must be physically dragged to each person.
- A fibre roll-out to a population is hugely expensive but the investment once made is more flexible and powerful than satellite → How ???

Why don't we use satellites more than under-sea optical fibre cables for Internet ? (contd)

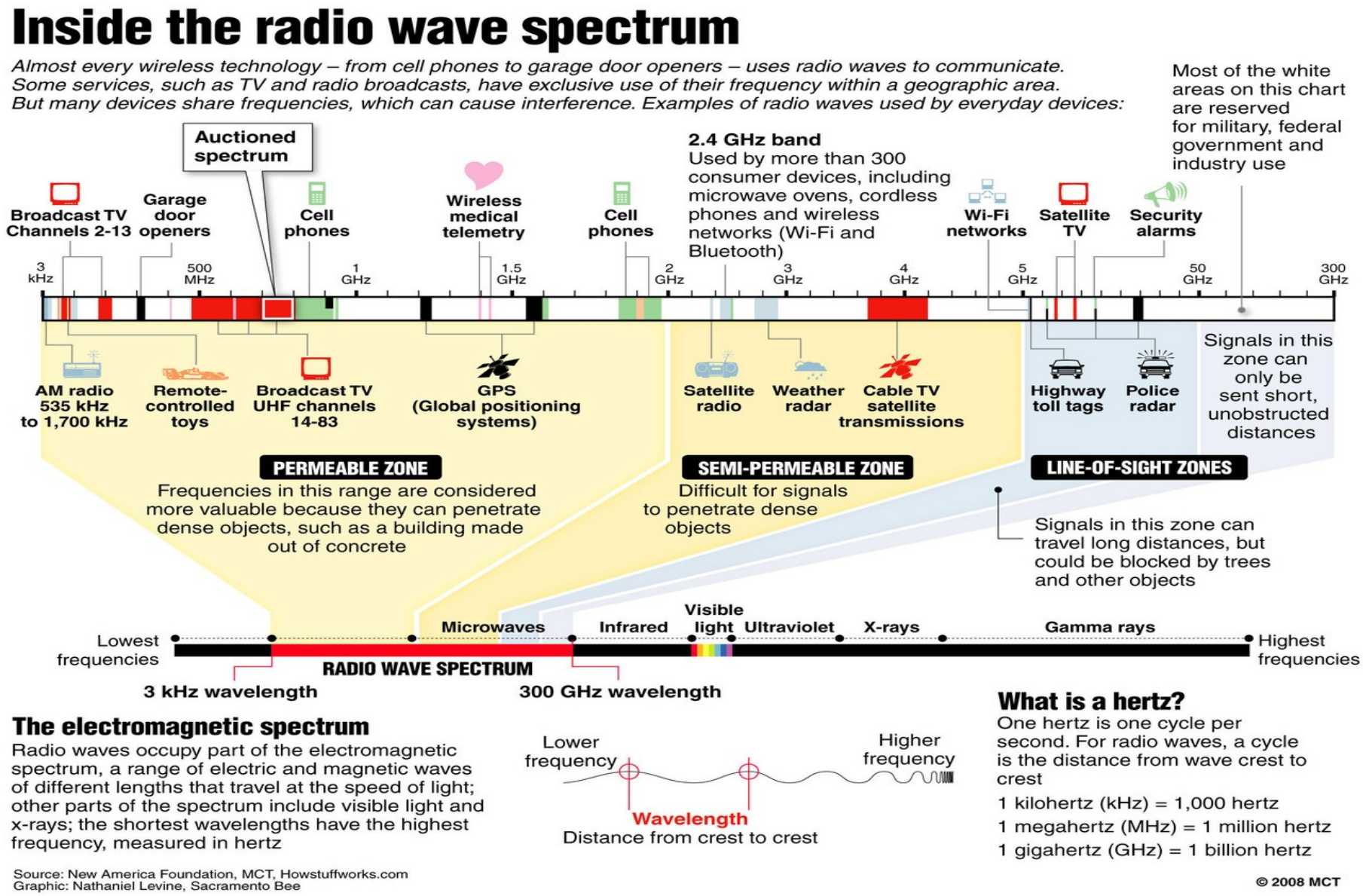
- Compared to fibre is that satellite have a very limited bandwidth in comparison
  - Satellite may only occupy a couple of GHz of radio spectrum, one fibre with DWDM(Dense WDM) could deliver the equivalent of all the bandwidth of every traditional satellite in operation

- Another concern is latency
  - The distance from Earth to the satellite and back creates delays which make real-time communication more difficult than by fibre.

Appendix 1 : Electromagnetic Spectrum



Appendix 2 : Electromagnetic Spectrum (detail)



Data Communication and Computer Network

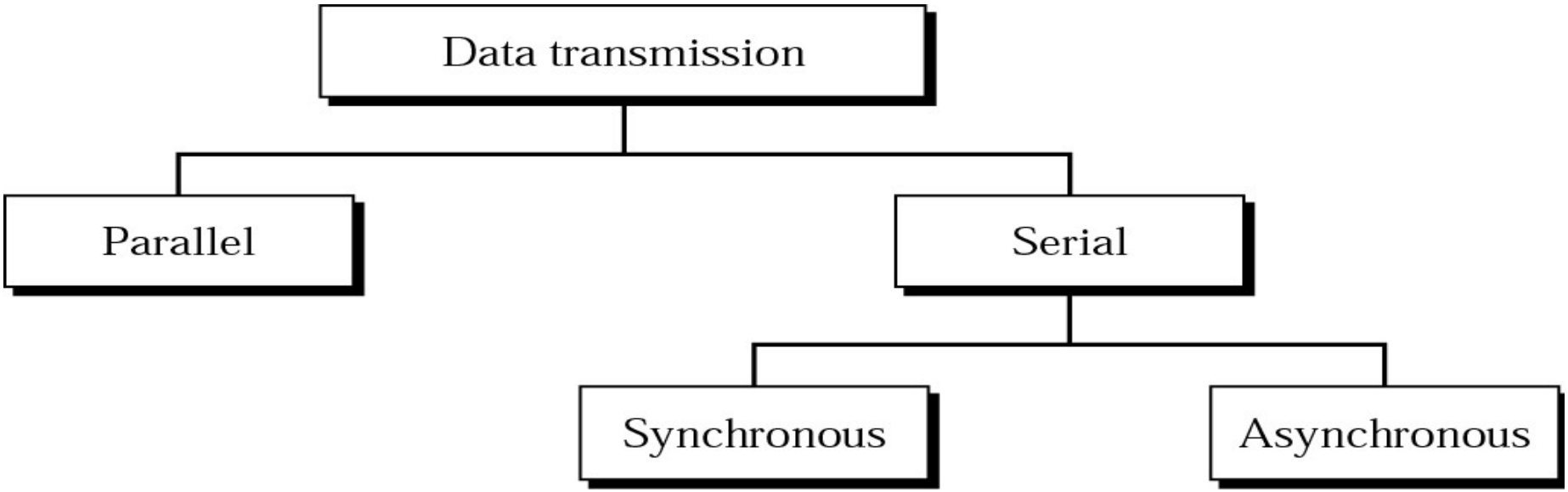
Data Link Layer

Responsibilities

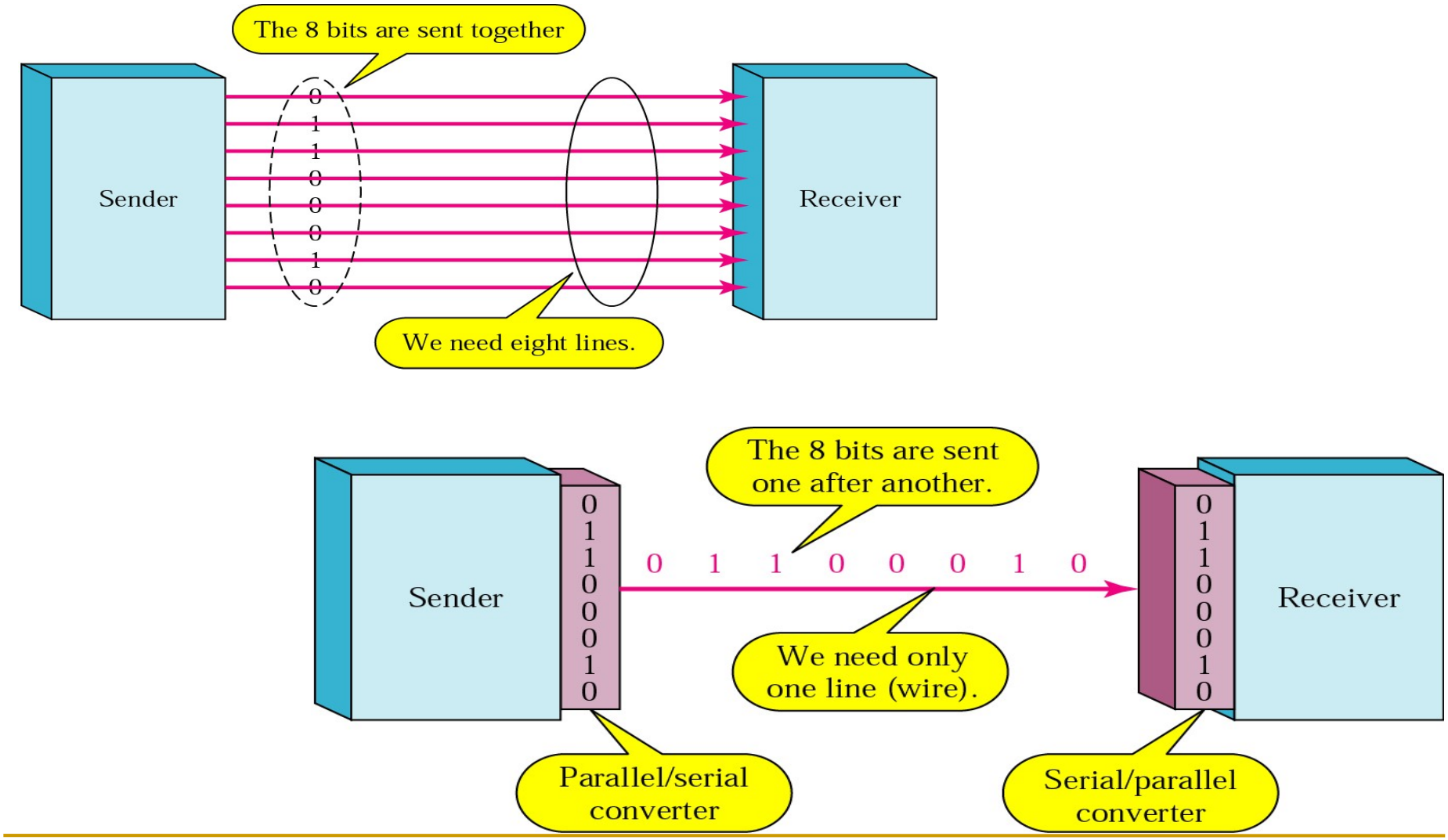
- Framing
- Error Detection
- Error Control
- Flow Control
- Medium Access Control

Framing

Mode of Transmission



Parallel and Serial Transmission



Framing

- Tx sending a sequence of bits to Rx over a link
  - Bits encoded into signal
  - Signal sent as series of voltage levels

- Framing: break up long bit-sequence into multiple relatively small 'frames' before send
  - Fixed / variable sized blocks of bits
  - Why framing?

✓ Needs identifier in each frame to distinguish between frames: frame sequence number

Frame synchronization

- What does the receiver need to know in order to read a frame correctly?
  - Where a frame ends or begins
  - At what intervals to sample the link to read the bits?

- Two common approaches
  - Asynchronous transmission: Rx and Tx agree on a pre-defined data rate
  - Synchronous transmission: Rx does not know the data rate being used by Tx

Asynchronous transmission

- Tx and Rx both know data rate, frame format
- Tx, Rx have separate clocks, no effort made to synchronize them

- Data transmitted one character at a time

  <start bit> 5-8 bits data <stop bit>

- Leading edge of start bit starts Rx clock
  - Once Rx clock starts, it runs at the pre-defined rate known to Rx (expected to be same as in Tx)
- How to tackle clock drift?

Synchronous transmission

- Rx may not know the data rate to be used by Tx

- Before starting to send data, Tx sends a known bit pattern (**fill pattern**)
  - At the same data rate at which it will transfer data
  - For a sufficiently long period of time
  - Rx adjusts own clock so that it can read the known fill pattern properly
- For Rx to detect start/end of data frame

  preamble bit pattern, ***post-amble*** bit pattern
- Fill pattern, pre/post-amble specified by protocol

Synchronous transmission (contd.)

- Desired: data block may be arbitrarily long

- After sending preamble, data transmission begins
  - To counter clock drift, Tx sends clock signals along with data
  - Separate clock signal, or clock signal embedded in encoded data signal e.g. Manchester encoding

✓ Pro: less overhead: few bits for large data block

✓ Con: clock signals need to be sent for some time before actual data is sent

Synchronous transmission (contd.)

- What if fill pattern / preamble / postamble is part of data? Use bit-stuffing

Example of synchronous protocol: HDLC

Preamble = post-amble = inter-frame fill = 01111110

- What if 01111110 is part of data?
  - ✓ whenever five consecutive 1's seen in data, Tx inserts an extra 0 after the five 1's

* HDLC : High-Level Data Link Control

Bit Stuffing

- Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag

Original pattern:

111111111111011111101111110

After bit-stuffing:

111110111111011011111010111111010

Error Detection

Errors

- Data can be corrupted during transmission
- For reliable communication, errors must be detected and corrected
- Types of error
  - Single bit error
  - Burst error

Error detection

- Rx receives a signal, it samples and decodes signal to get binary data
- Error detection: how does Rx know if the data is actually what Tx sent?
- Use redundancy: extra bits added to data bits
- *Error correction*
  - Rx can detect whether errors are present and also correct the errors (can find which bits are in error)
  - Larger number of extra bits required than for error detection
  - Not commonly used, because of large overhead

Parity check

- Tx: one extra 'parity' bit added to each data unit
  - Odd parity: bit added so as to make # of 1's odd
  - Even parity: bit added to make total # of 1's even
- Rx: counts total number of 1's in the data unit, including the parity bit
- Detects any odd number of bit errors, but can be fooled by any even number of errors

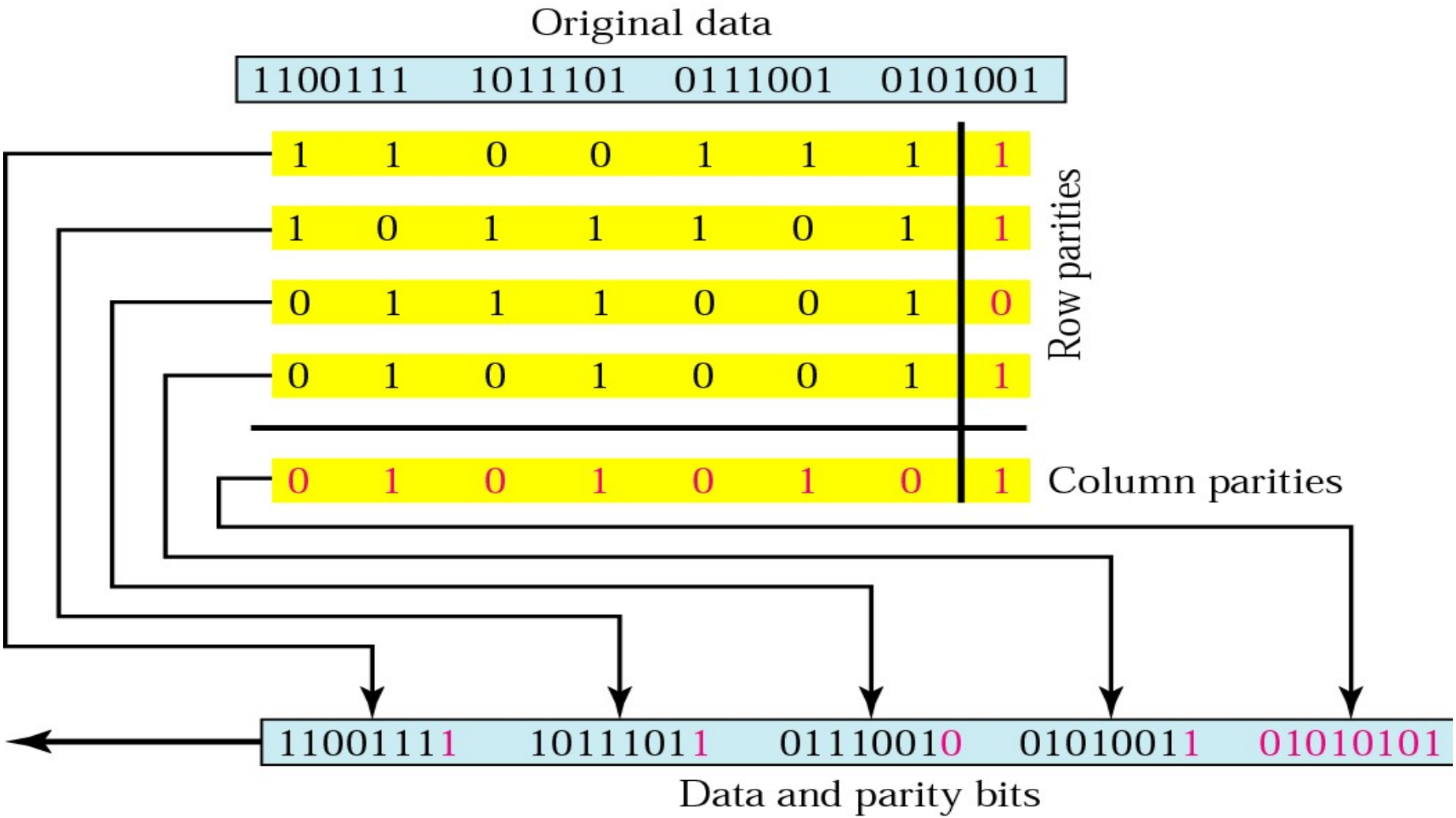
✓ Simple, easy to implement

✓ Not very robust against noise

Two-Dimensional Parity

- A block of bits divided into (say) 7-bit units (row)
- One parity bit computed for each row
- Also, parity bits computed considering the i-th bit in each row as a sequence (column), for all values of i = 0, 1, …, 7
- A redundant row of parity bits (column parity bits) added to the whole block

Two-Dimensional Even Parity



Cyclic Redundancy Check (CRC)

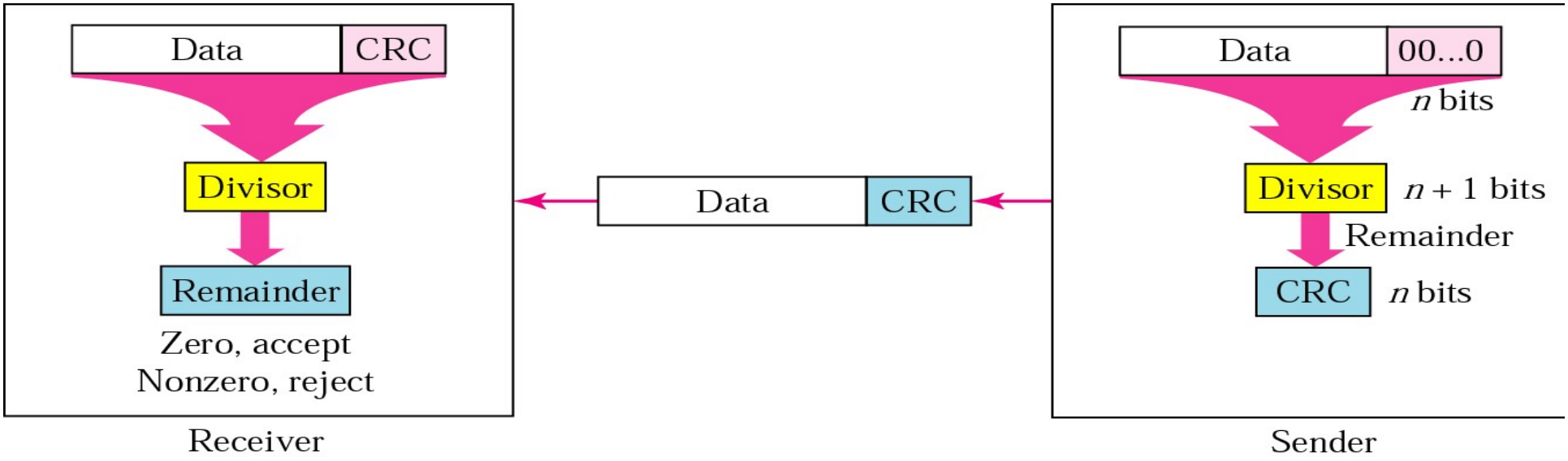
- Much more powerful method, easy to implement
- D: d-bit data
- R: r-bit error detecting code (appended to D)
  - Often called Frame Check Sequence (FCS)
- T: (d+r)-bit frame to be transmitted
- P: (r+1)-bit pattern
- Value of r and pattern P known to Tx, Rx
- Modulo-2 arithmetic
  - Addition, subtraction of bits both implemented as XOR with no carry, no borrow
  - $0 \pm 0 = 0$; $0 \pm 1 = 1$; $1 \pm 0 = 1$; $1 \pm 1 = 0$

CRC – the method

- At transmitter
  1. Extend D with r 0's to the right (less significant bits)
  2. Divide extended D by P (of (r+1)-bits) using mod-2 arithmetic, to get remainder R (of r bits)
  3. Append R to the right of M to get T (d+r bits)
  4. T is transmitted

- At receiver
  1. Divide received T by P, using mod-2 arithmetic
  2. If remainder not zero, then error

CRC – the method



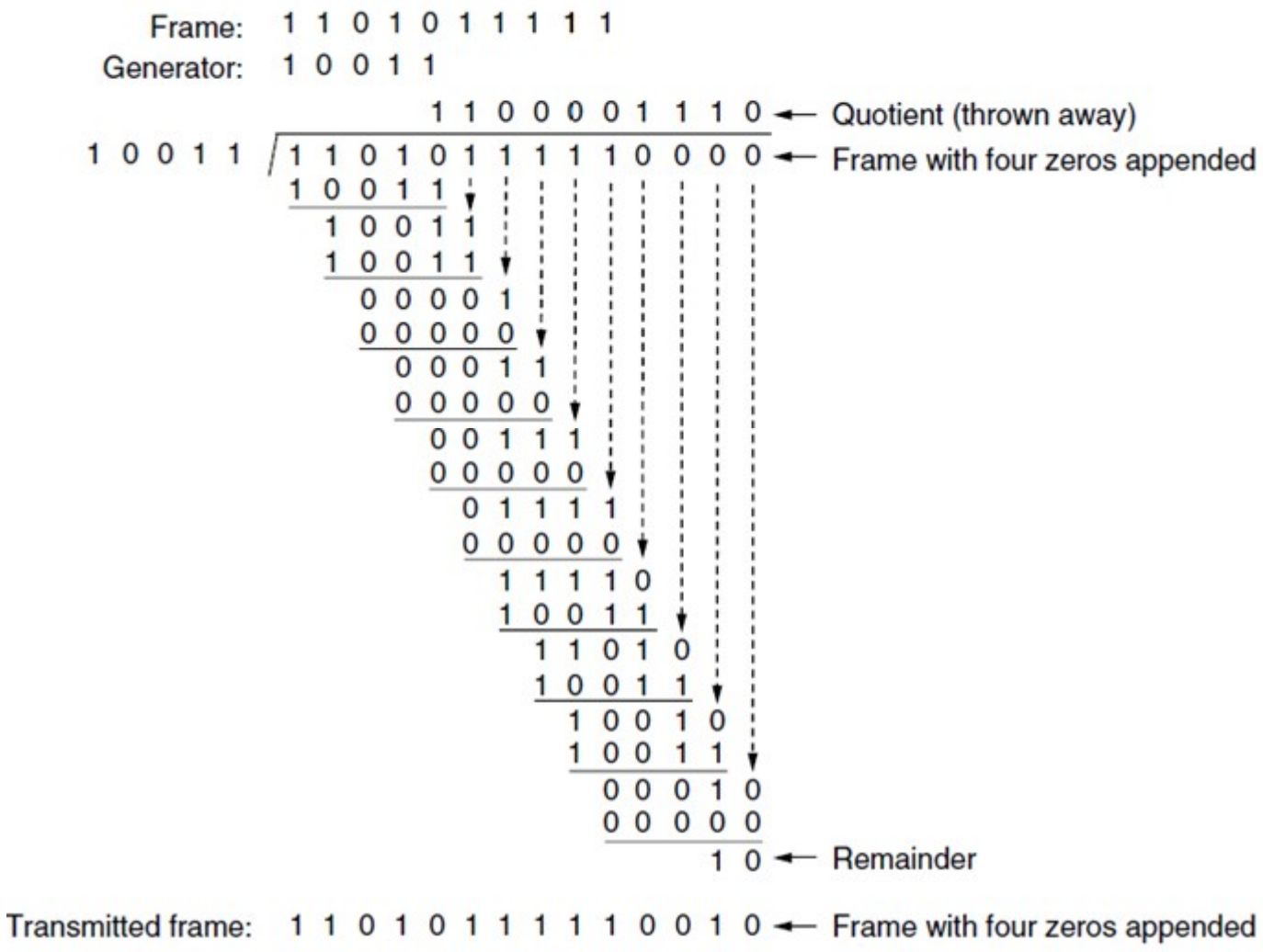
CRC – an example

Message D = 10101, d = 5

Let the divisor be fixed as P = 1101 (r+1 bits), so r = 3 redundant bits will be appended to data

What is the mathematical logic in CRC?

An example of CRC calculation



CRC in terms of polynomials

- Any bit pattern can be expressed as a polynomial in (a dummy variable) x, containing the powers of x corresponding to the '1' bits

  $110011 \equiv x^5 + x^4 + x^1 + x^0$

- Commonly used divisors P

  CRC-16 = $x^{16} + x^{15} + x^2 + 1$

  CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$

  CRC-32 = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^{12} + x^4 + x^2 + x + 1$

What errors can CRC detect?

- ✓ All single-bit errors
- ✓ All double-bit errors, as long as long as P has at least three 1s
- ✓ Any burst error for which the length of the burst is less than or equal to the length of the FCS (frame check sequence)
- ✓ Many other larger burst errors

- ✓ But, still NOT fool-proof

  Errors may occur and may not be detected by CRC

Error Control

Error control

Rx can detect if there is error in the received frame, but if there is, then what?

- Error control
  - Ensures that the finally received bit pattern is same as the sent bit pattern
- Forward error control
  - Error recovery by correction at the receiver
  - Requires large number of error correcting bits to be added to data (e.g. Hamming code)
- Backward error control
  - Error recovery by retransmission: Automatic Repeat Request (**ARQ**)

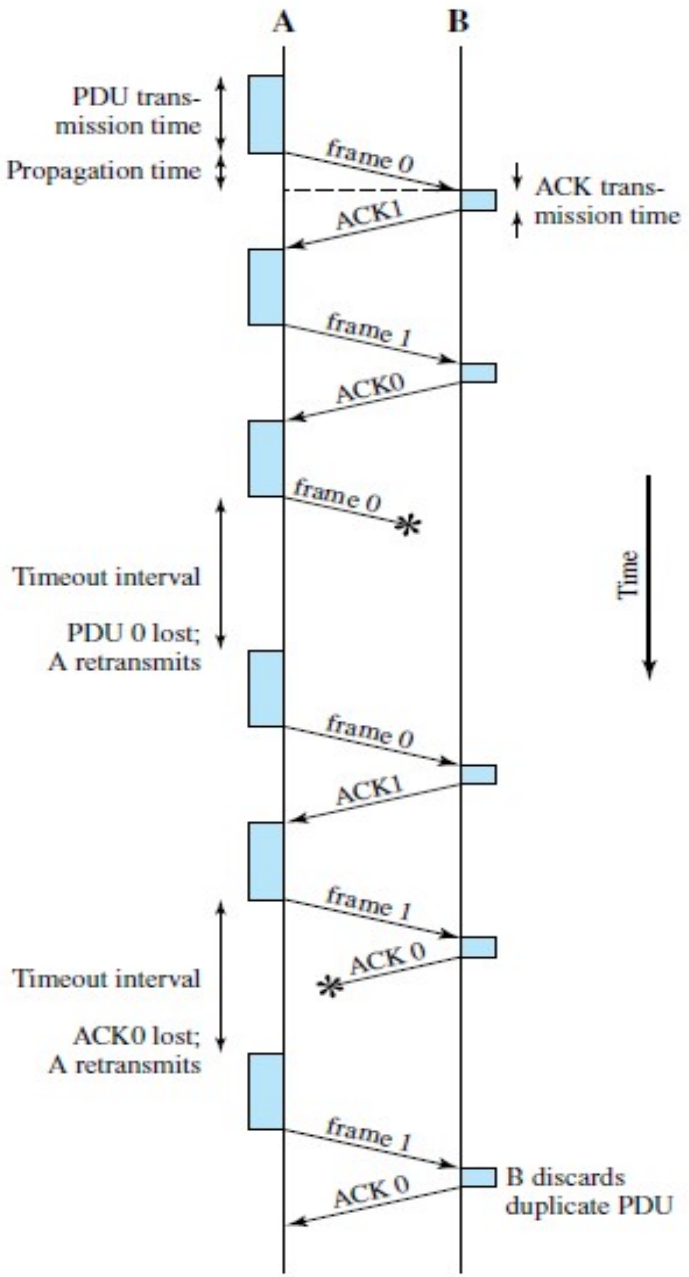
Stop & Wait ARQ

- 1 bit sequence number in each frame (0 or 1)

- Tx: send a frame, wait for ACK / NAK from Rx
- Rx: receive frame, check, send ACK / NAK
  - ACK includes number of next frame expected (0 or 1)
- Tx:
  - Get ACK => send next frame
  - Get NAK => re-transmit previous frame

- Simple and minimum buffer requirement

Stop & Wait ARQ
An Example



Stop & Wait ARQ - complexities

- Frames / ACKs can get lost => use timeout
- Transmitter Tx
  - send a frame, wait for ACK from Rx
  - If get ACK, send next frame
  - If no ACK within a timeout period (or get NAK), re-send previous frame
- Receiver Rx
  - check received frame for errors, send ACK if frame is ok
  - If error in frame, discard the frame and do NOT send ACK (or, may send NAK – time vs message tradeoff)
- Duplicate frames? Duplicate ACKs?

Efficiency of ARQ scheme

K = size of data frame in bits

D = data rate of channel in bits/sec

L = length of channel in meters

V = propagation speed in channel in m/sec

S = size of ACK frame in bits

D is the raw data rate

- at what rate can bits be put onto the channel

Effective data rate E

- At what rate is useful data being transmitted

Channel utilization: E / D

Efficiency of ARQ scheme (contd.)

- Channel utilization = 1 / (1 + 2 (L/V) / (K/D))

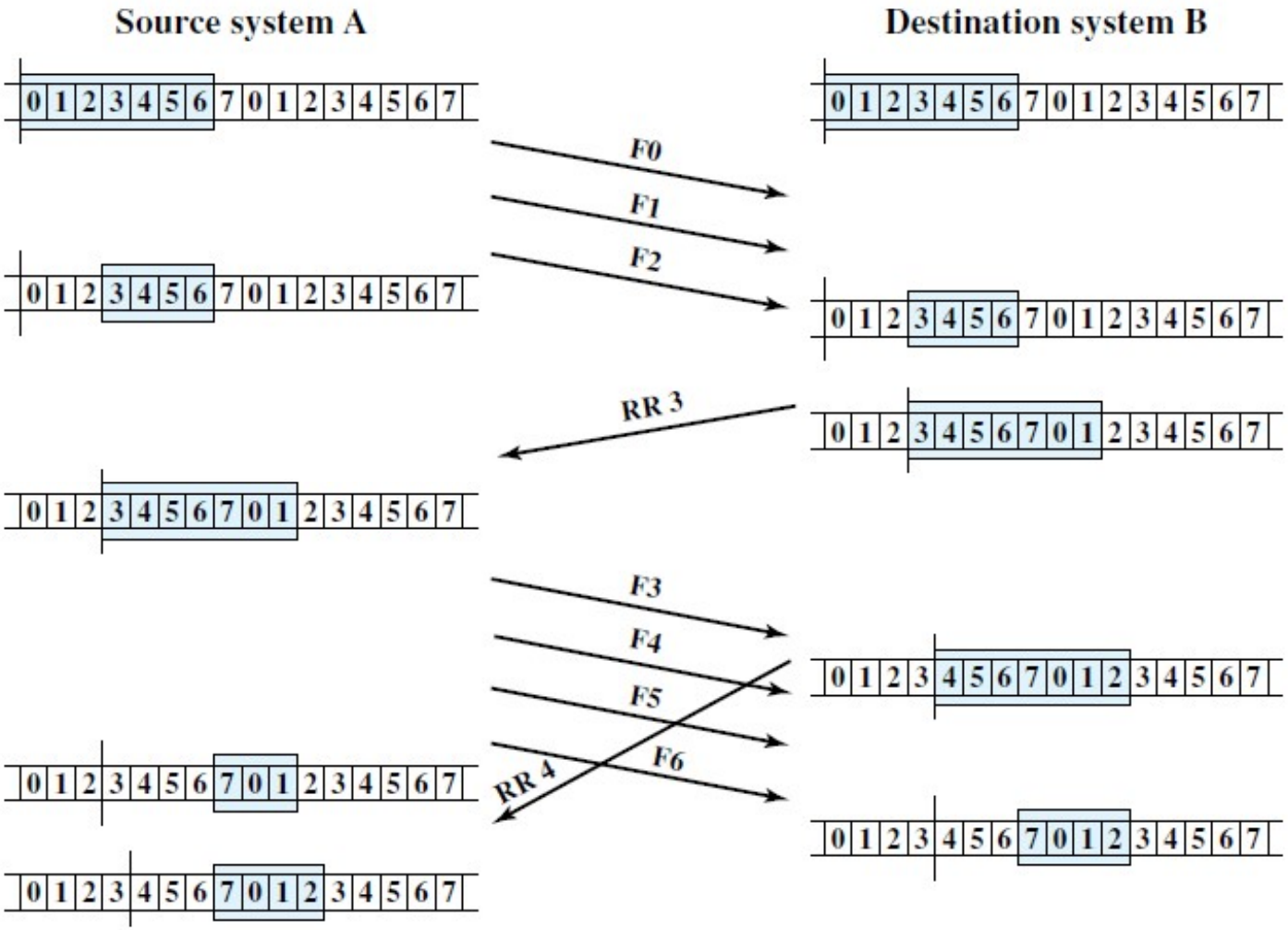
- So, Stop & Wait ARQ is NOT efficient if
  - Long links (high propagation time)
  - High data rate (low transmission time)
  - Frame size is very small (frame transmission time << propagation time)

- If message size (K) increased, utilization increases, but more buffer space required

Go-Back-N ARQ

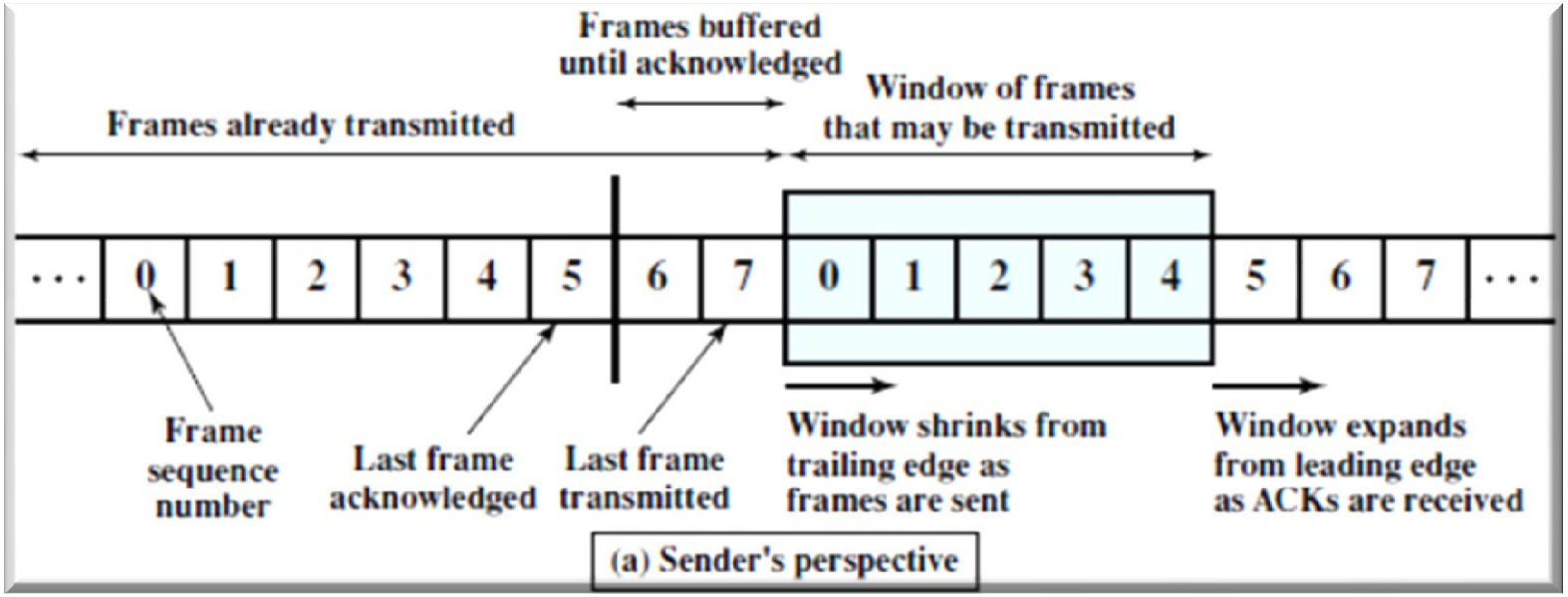
- Tx has a sequence of frames to transmit
- Frame seq. no: assume 3 bits (0,1,…,7,0,1,…)
- Tx allowed to send W (> 1) frames before waiting for ACK
- Window of frames: number of frames that Tx is allowed to send without receiving any ACK
  - W=4 implies Tx can send frames 0, 1, 2, 3 without waiting for any ACK from Rx
- Rx allowed to receive frames in order
- ACKs can be cumulative

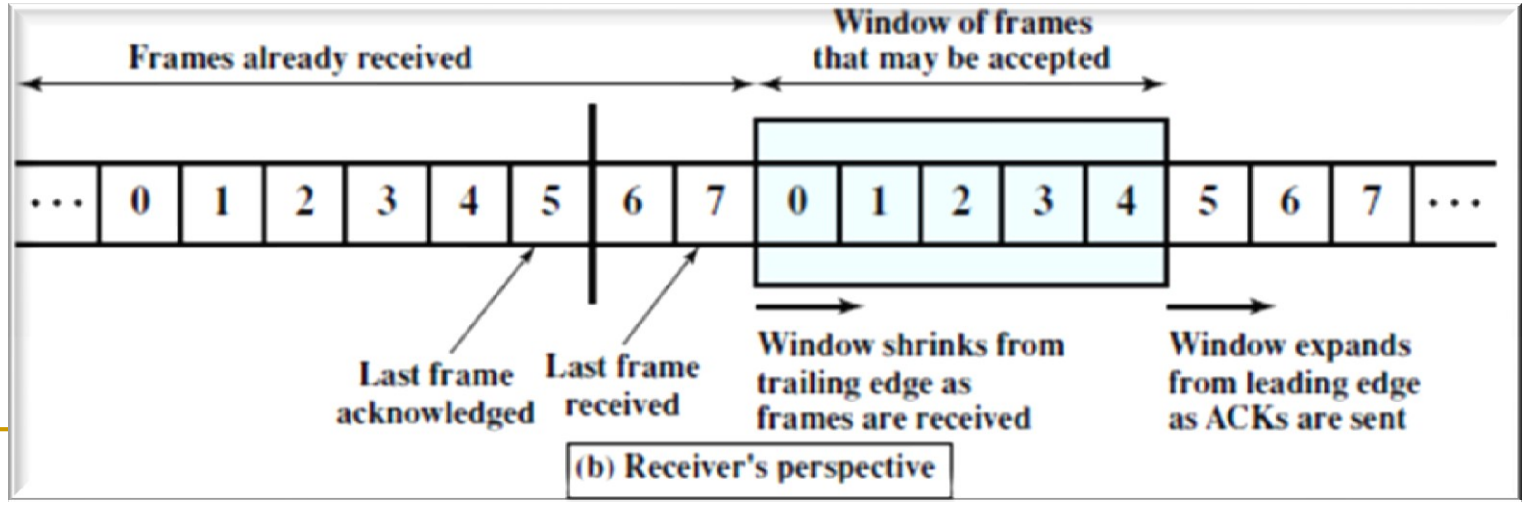
Sliding-Window concept



ACK or RR (Receive Ready) N : "***I have received all frames up through frame number N-1 and am ready to receive frame number N; in fact, I am prepared to receive W frames, beginning with frame number N***"

Sliding-Window concept Cont'd





If error detected in a frame

- Rx detects error in a received frame
  - May send a NAK giving sequence no. of that frame, or may send nothing
  - Discard this and all future frames until the frame in error is correctly received (in-order receipt of frames)
- When Tx gets a NAK for a frame, or does not get ACK for a frame within the timeout period
  - Re-transmit this frame as well as all subsequent frames
- Tx has to remember each unacknowledged frame (at most W frames)

Lost / damaged data frame F_i

- Case 1: Tx has more frames to send
  - Tx sends F_{i+1}, F_{i+2}, ... up to window limit
  - If Rx receives any of these frames, Rx discards them and can send NAKi
  - Tx gets NAKi before timeout, re-sends F_i, F_{i+1}, ...

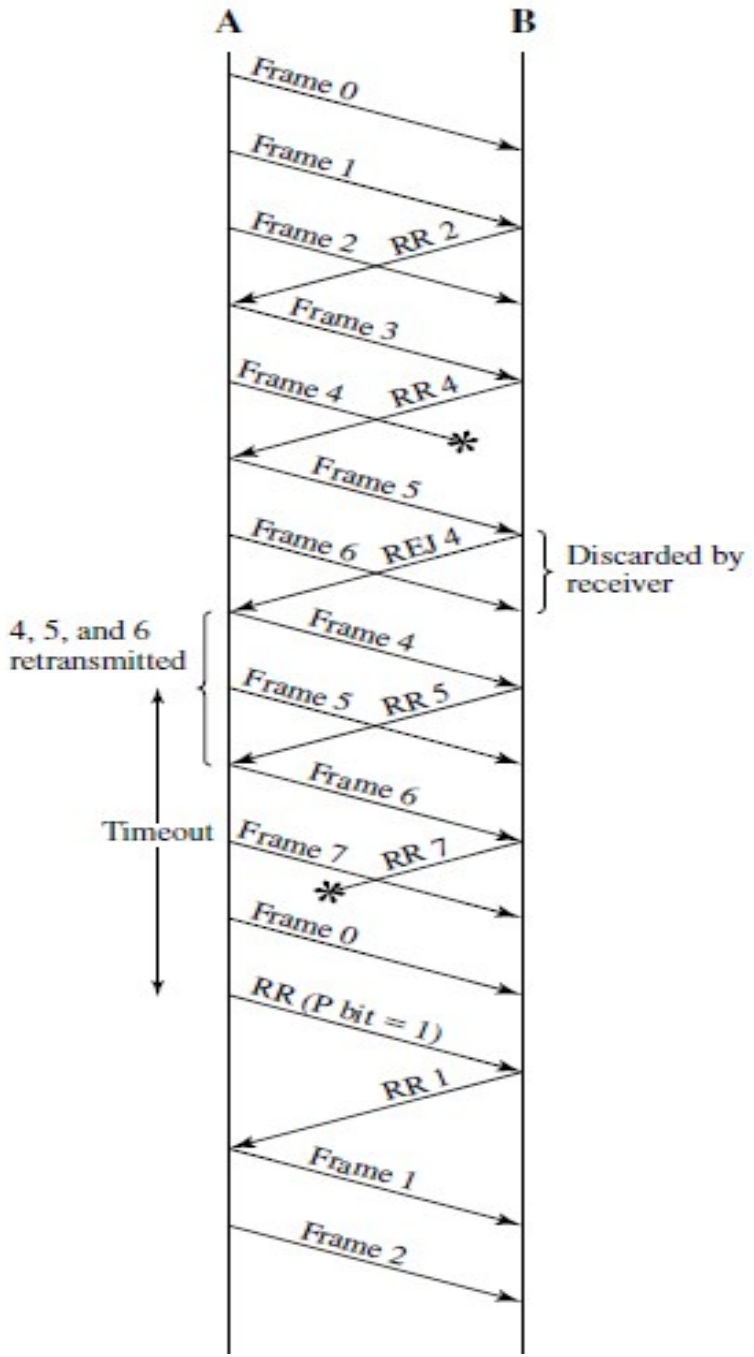
- Case 2: Tx times out
  - Pessimistic approach: Tx re-sends F_i, F_{i+1}, F_{i+2} ...
  - Optimistic approach: Tx sends a poll message RR to ask Rx what frame it expects next, Rx replies with NAKj
  - Tx re-transmits frames F_j, F_{j+1}, F_{j+2} ...

Lost / damaged ACK for frame F_i

- Case 1: Tx gets ACK for frame F_j, F_j sent later than F_i
  - Since ACKs are cumulative, this is implicitly an ACK for frame F_i also, Tx simply extends window
- Case 2: Tx times out
  - Tx does not know whether data frame got lost or whether data reached Rx and ACK got lost
  - Similar to Case 2 for lost data frame

Go-Back-N: An example

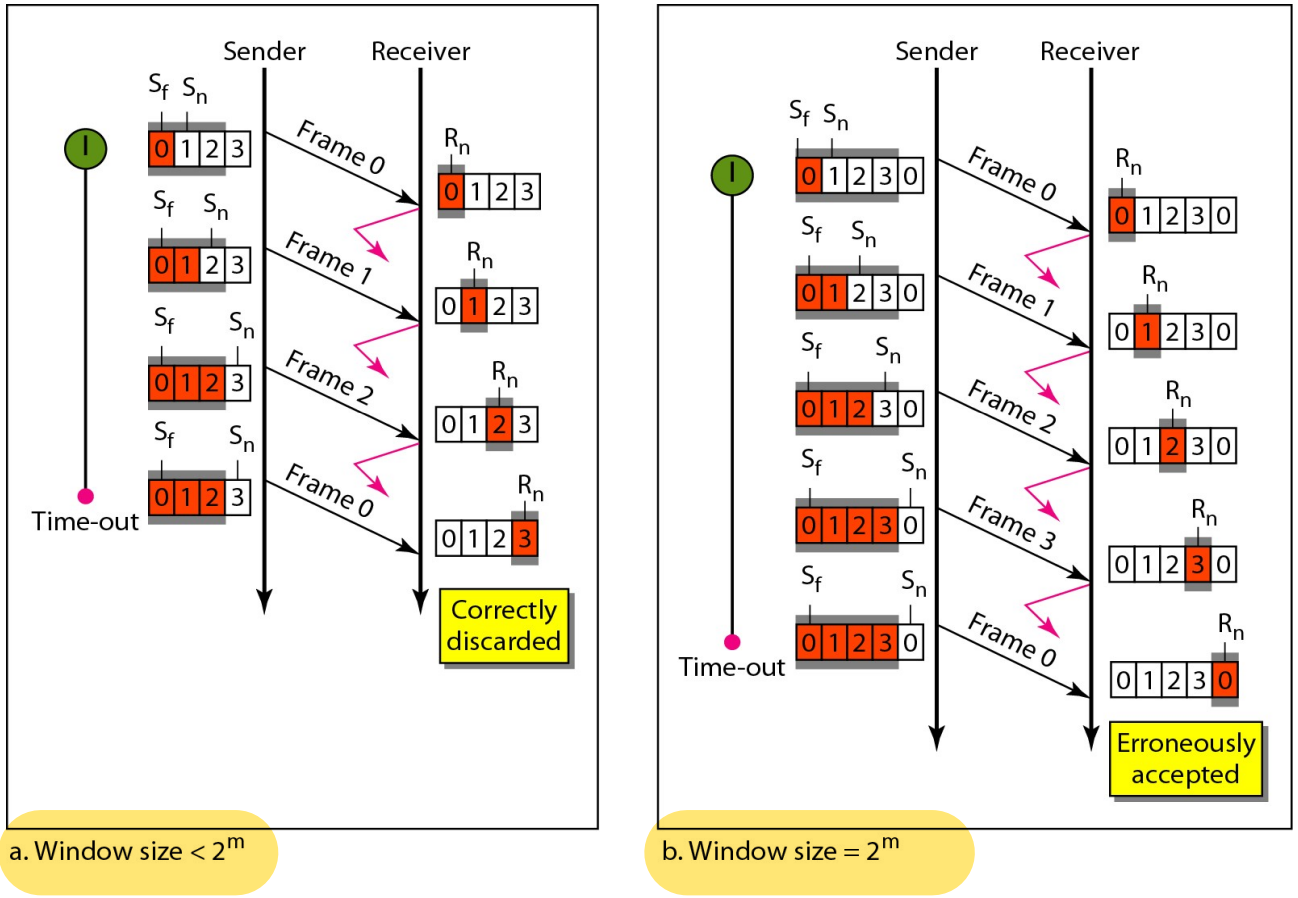
- 3 bit sequence number
- ACKs indicated as RR
- NAKs indicated as REJs



❖In this diagram, Optimistic approach is assumed
❖**RR (Receive Ready) is same as ACK**
❖**REJ (Reject) is same as NACK**

Go-back-N : Relationship of Sequence Number and Window Size

For k-bit sequence numbers, maximum window size for Go-Back-N ARQ is $(2^k - 1)$



In this diagram, Pessimistic approach is assumed

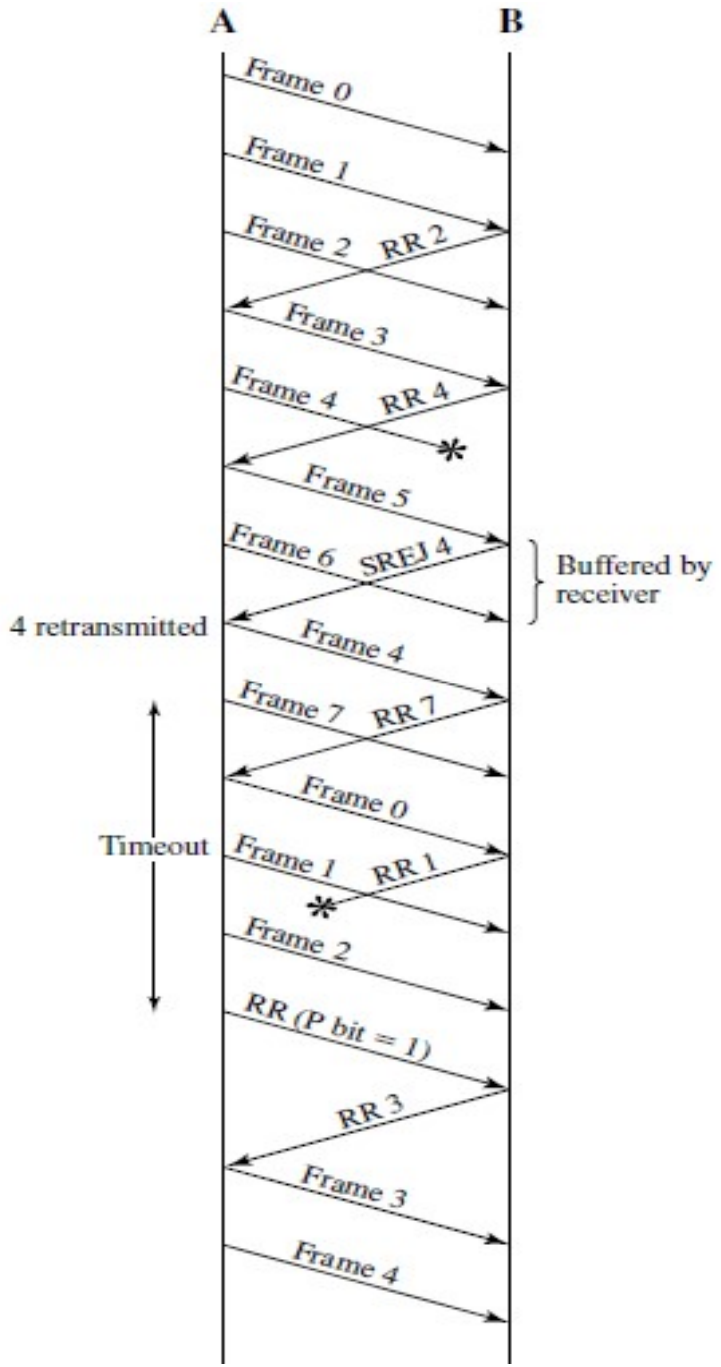
Selective-Reject/Repeat ARQ

- Allow Rx to receive frames out of order
  - If F_i contains errors, Rx discards F_i and sends NAKi
  - ➢ Rx accepts F_{i+1}, F_{i+2}, ... (if they are error-free) even if F_i has not been received properly
- ✓ Motivation: reduce number of re-transmissions

- However, applications at higher layers usually require in-order frames
  - ➢ Rx must buffer frames being accepted out of order

Selective-Reject/Repeat ARQ
An example

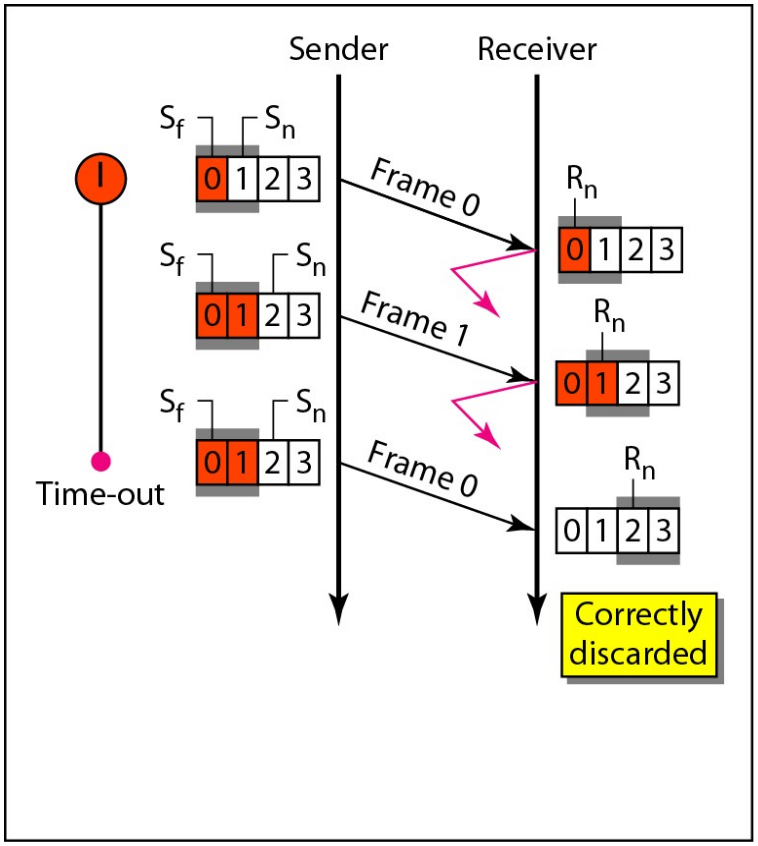
- 3 bit sequence number
- ACKs indicated as RR
- NAKs indicated as SREJs



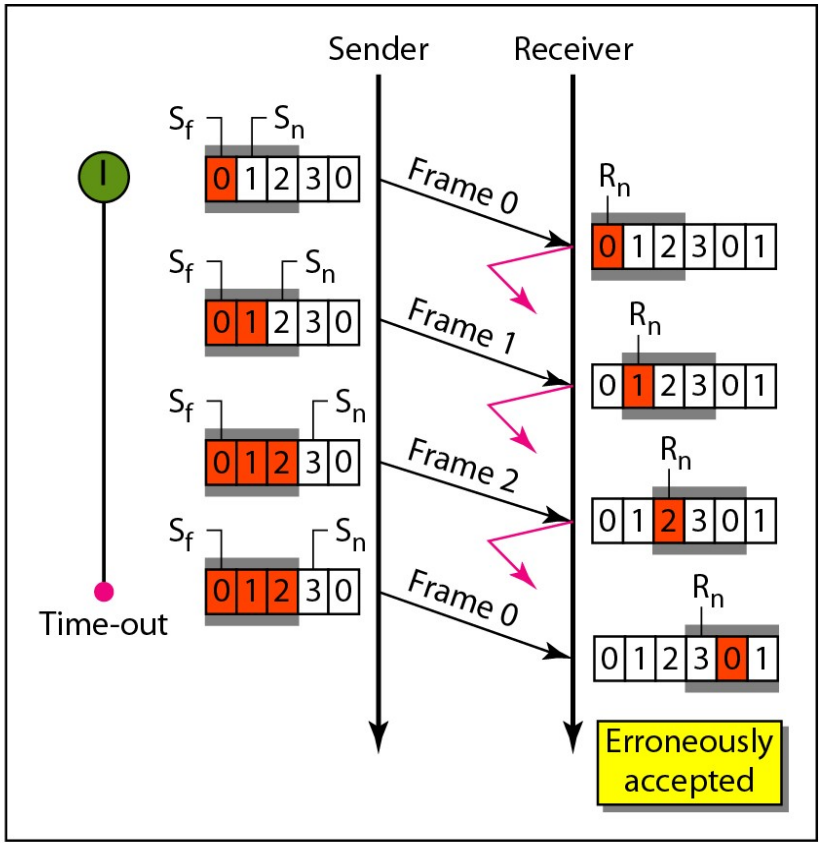
❖In this diagram, Optimistic approach is assumed
❖**RR (Receive Ready) is same as ACK**
❖**REJ (Reject) is same as NACK**

Selective Reject/Repeat : Relationship of Sequence Number and Window Size

For k-bit sequence numbers, maximum window size for Go-Back-N ARQ is 2^{k-1}



a. Window size = 2^{m-1}



b. Window size > 2^{m-1}

In this diagram, Pessimistic approach is assumed

Sliding Window scheme enhancements

- Rx can acknowledge frames without permitting further transmission (Receive Not Ready)
  - When Rx becomes ready, must send a message to allow Tx to resume sending frames
- Piggybacking
  - Often both sides transmit and receive data: each station maintains a sender window and a receive window
  - Suppose A sends a data frame to B, ACK for this frame can be piggybacked on a data frame from B to A
  - Frame format includes a field to hold a sequence number (of this frame) plus a field to hold the sequence number used for ACK

Flow Control

Stop & Wait Flow Control

Sliding Window Flow Control

Flow Control

- What if Tx sends frames too fast for Rx to handle?
  - Rx may not be able to process the data as fast as Tx is sending it
  - Rx can buffer, but buffer has finite size. Once that is filled, data will be lost

- Flow control: technique to control data flow between sender and receiver so that sender is blocked if receiver cannot accept any more data

Stop & Wait Flow Control

- Tx: send a frame, wait for ACK from Rx
- Rx: receive frame, check for errors, send ACK when ready for another frame
- Similar to Stop & Wait ARQ, only difference in the time to send ACK
  - Error control: Rx sends ACK immediately on understanding that there is no error
  - Flow control: ACK delayed till Rx processes the received frame in some way
- Simple, low buffer requirements at both Tx and Rx, but low line utilization

Sliding Window Flow Control

- Similar to Go-Back-N
- Rx can allocate buffer space for W frames
  - So, window size W use
  - Tx maintains sender window: a list of sequence numbers that it is allowed to send without waiting for an ACK
  - Rx maintains receiver window: list of sequence numbers that it is prepared to receive
- Rx sends 'ACK N' only when
  - it has received all frames up to N-1 correctly, and
  - it is ready to receive W more frames starting from frame N

References

- *Data Communications & Networking, 5th Edition, Behrouz A. Forouzan*
- *Computer Networks, Andrew S. Tanenbaum and David J. Wetherall*
- *Wikipedia*

Data Communication and Computer Network

MAC Sub Layer

"Technically, the MAC sublayer is the bottom part of the data link layer, so logically we should have studied it before examining all the point-to-point protocols in Chap. 3. Nevertheless, for most people, it is easier to understand protocols involving multiple parties after two-party protocols are well understood. For that reason we have deviated slightly from a strict bottom-up order of presentation."

From - Computer Networks,

Andrew S. Tanenbaum and David J. Wetherall

Medium Access Control (MAC) Protocols

- Also called Random Access or Contention Protocols
- Protocol followed by nodes to decide **who should transmit when**
- No station is **superior** to another station and none is assigned the control over another
- No station **permits**, or does not permit, another station to send
- Any node may have data to transmit at any point of time
- Needs to avoid collision, i.e. two or more stations transmitting through the medium at the same time

Random Access Protocol Types

- ALOHA
- Carrier Sense Multiple Access (CSMA)
- Carrier Sense Multiple Access with Collision Detection (CSMA-CD)
- Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

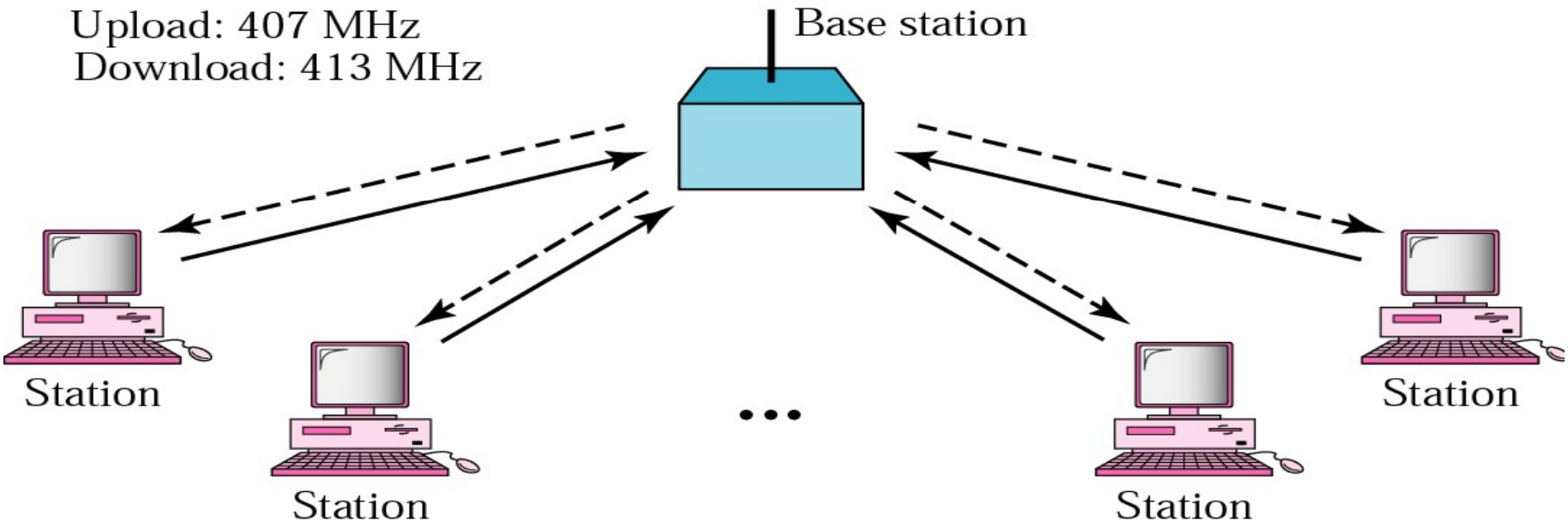
ALOHA

ALOHA

- Developed in University of Hawaii in early 70s
  - Originally developed for packet radio networks
  - Transmission to and from a central station
  - All other sources transmit using same frequency, central station uses another frequency

- Whenever a station has a frame, it sends immediately
  - Station listens for maximum round trip time (plus small increment) for ACK
  - If ACK, fine. If not, wait for a random time and then retransmit frame
  - If no ACK after repeated transmissions, give up

ALOHA network



ALOHA (contd.)

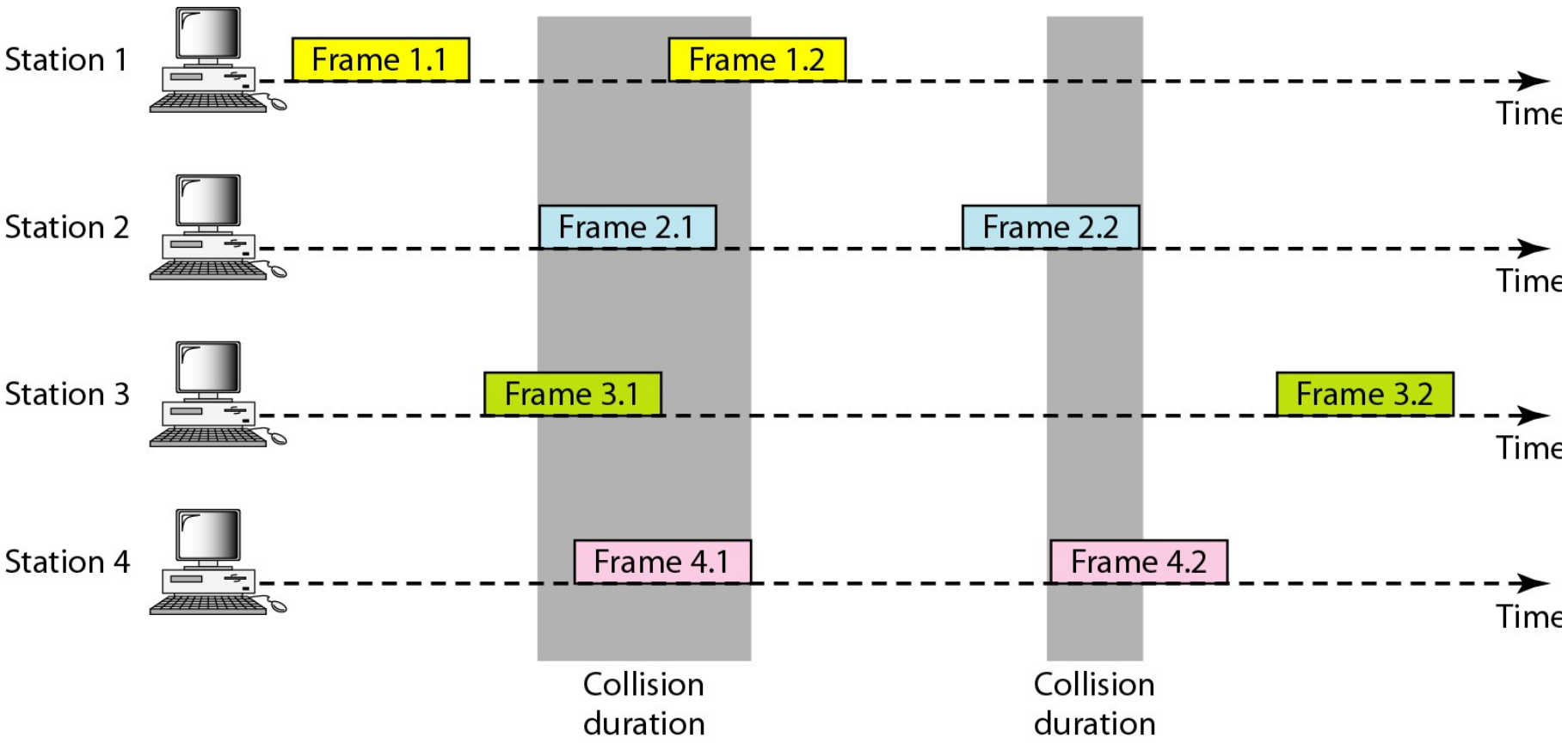
- When a station receives a frame:
  - If frame ok (using FCS) and address matches this station, send ACK frame immediately
  - ACK frames sent on a different frequency

- Frame may become invalid due to noise, or because another station transmitted a frame at about the same time: collision

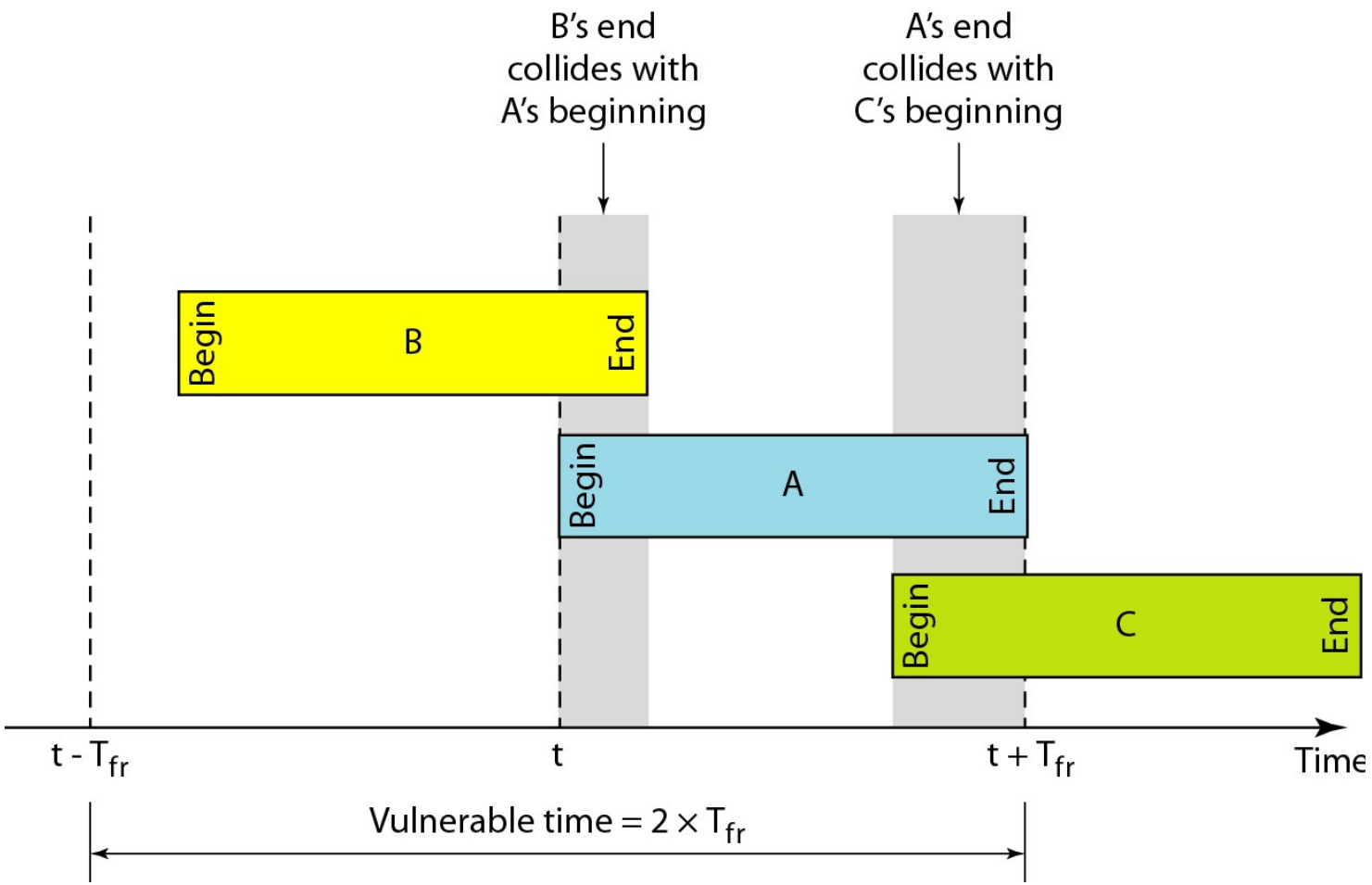
- How is collision detected?
  - If frame found to be invalid, receiver NOT send ACK
  - If no ACK received within some time, sender assumes collision

- Max utilization 18%, very low for large nos. of nodes or for higher transmission rates

Frames in a pure ALOHA network

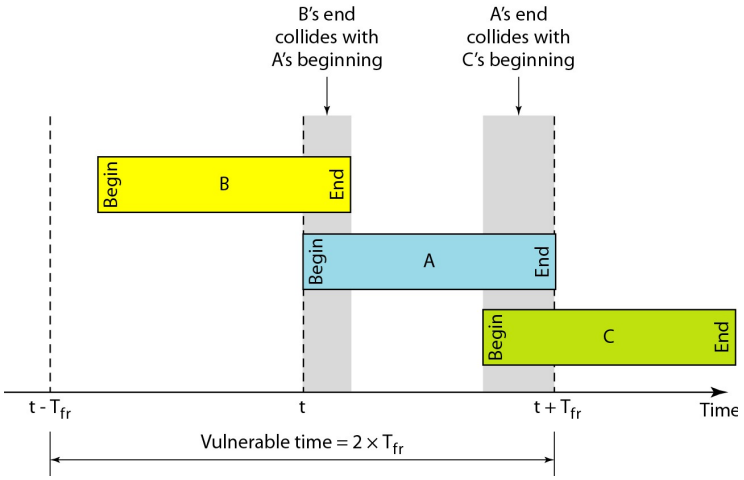


Vulnerable time for pure ALOHA protocol



Vulnerable time for pure ALOHA protocol

- Station A sends a frame at time t.
- Now imagine station B has already sent a frame between (t – Tfr) and t. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame.

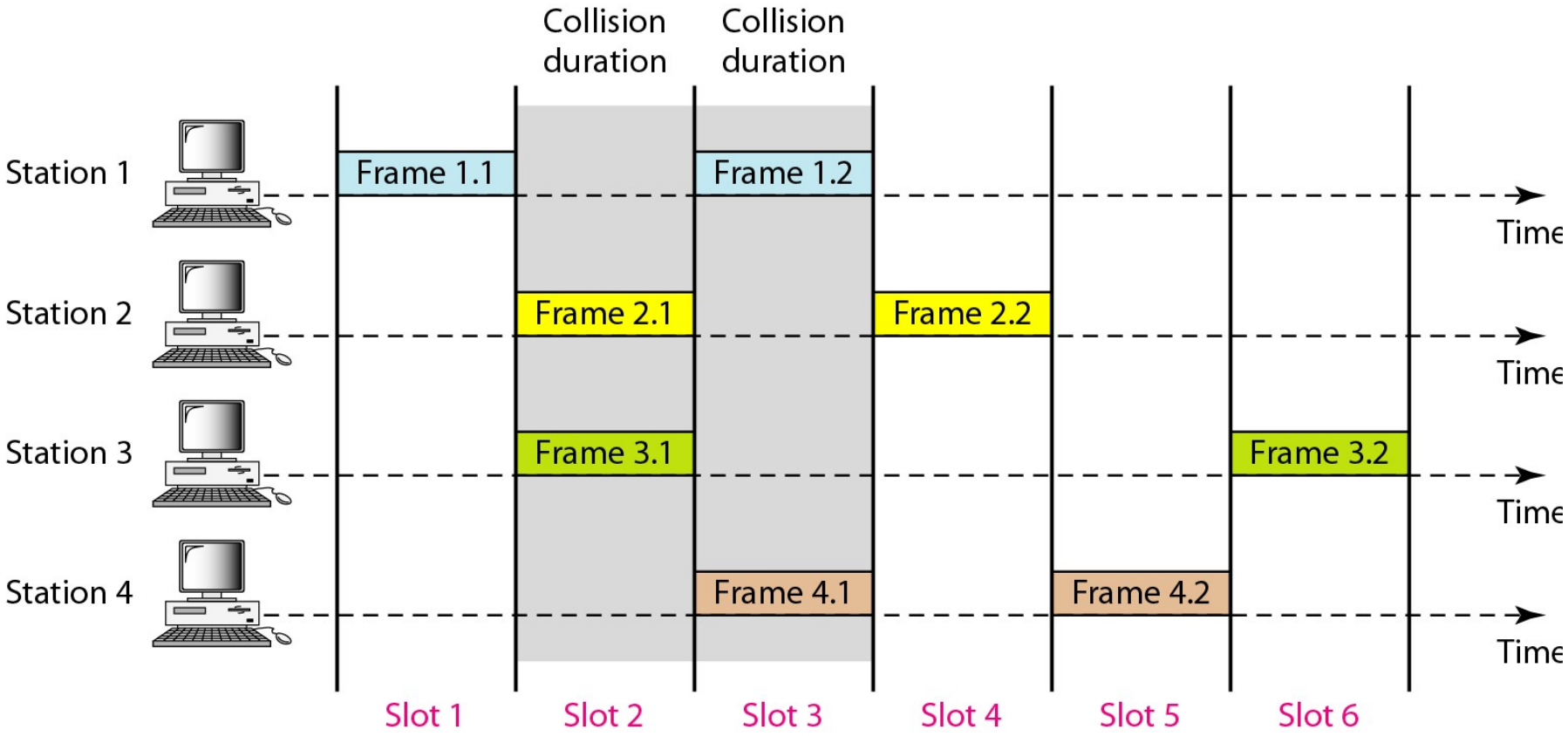


- On the other hand, suppose that station C sends a frame between t and (t + Tfr). Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.
- Hence, the vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.

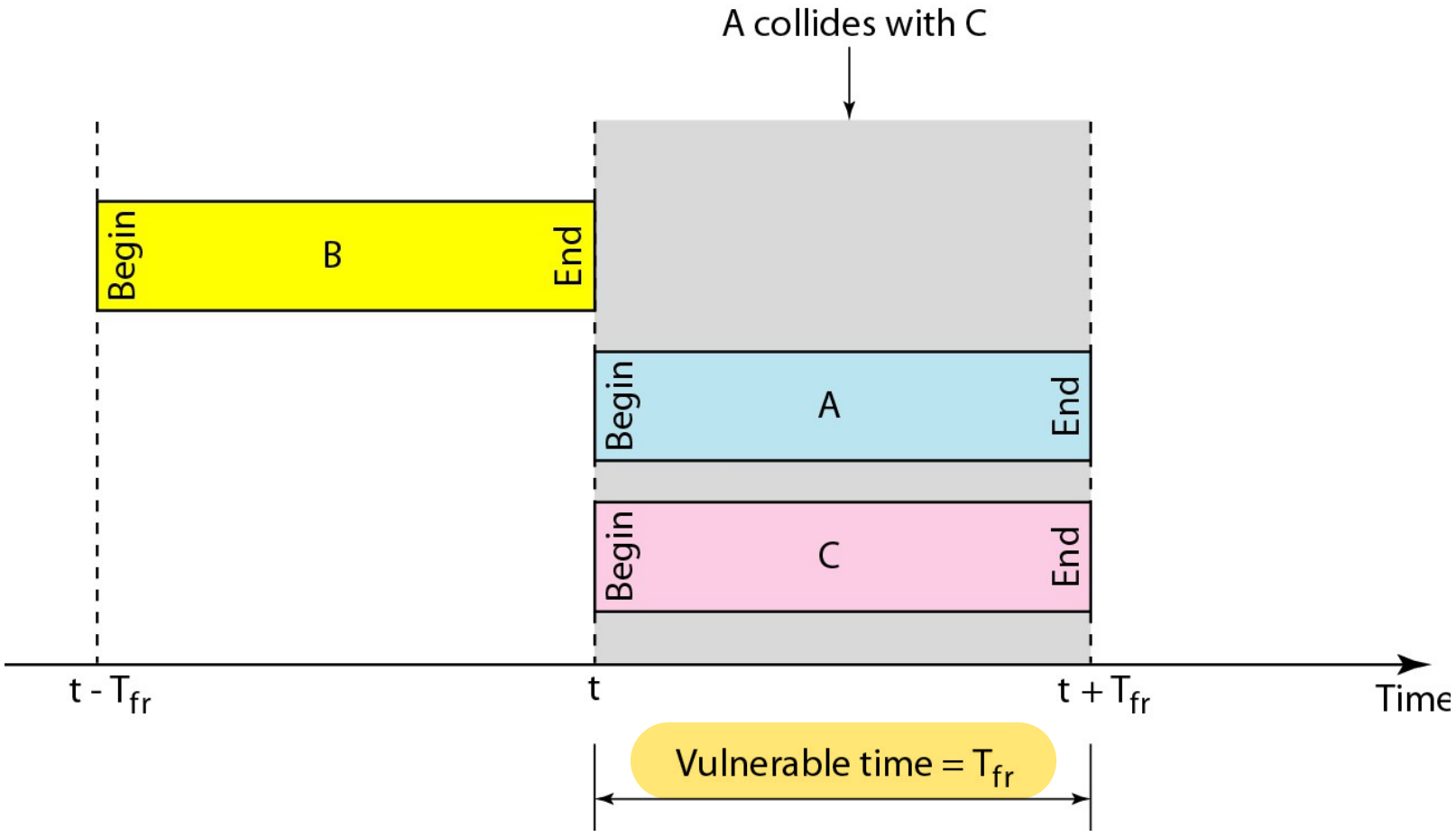
Slotted ALOHA

- Time on the channel **divided into slots** equal to frame transmission time
  - Needs central clock to synchronize all nodes
  - A source can start sending only at the beginning of a slot
- Reduces number of collisions over ALOHA
  - Contention period (time interval in which frames can overlap or collide) is halved compared to ALOHA
  - Collision possible only if more than 1 sources become ready to transmit within the same slot
- Max utilization 37%

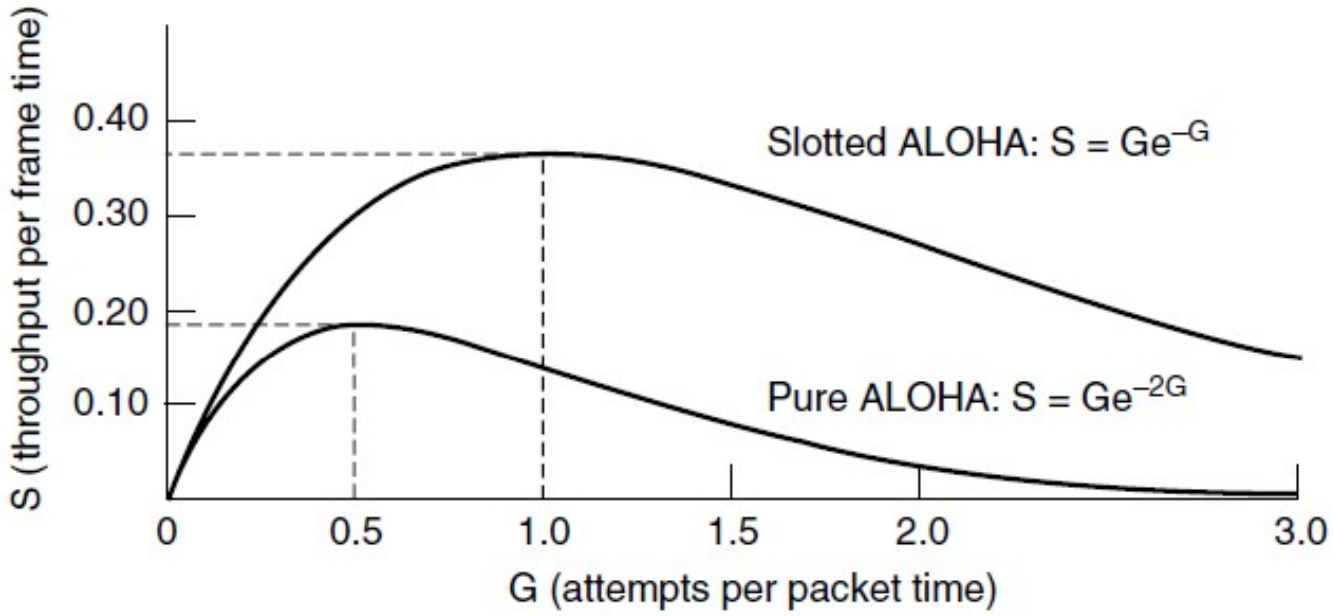
Frames in a slotted ALOHA network



Vulnerable time for slotted ALOHA protocol



Channel utilization of ALOHA and slotted ALOHA



Throughput versus offered traffic for ALOHA systems.

Carrier Sense Multiple Access (CSMA)

Carrier Sense Multiple Access (CSMA)

- Motivation
  - In most small networks, **propagation time** is much smaller compared to **frame transmission time**
- Whenever node N becomes ready to transmit a frame, sense the medium (carrier sense)

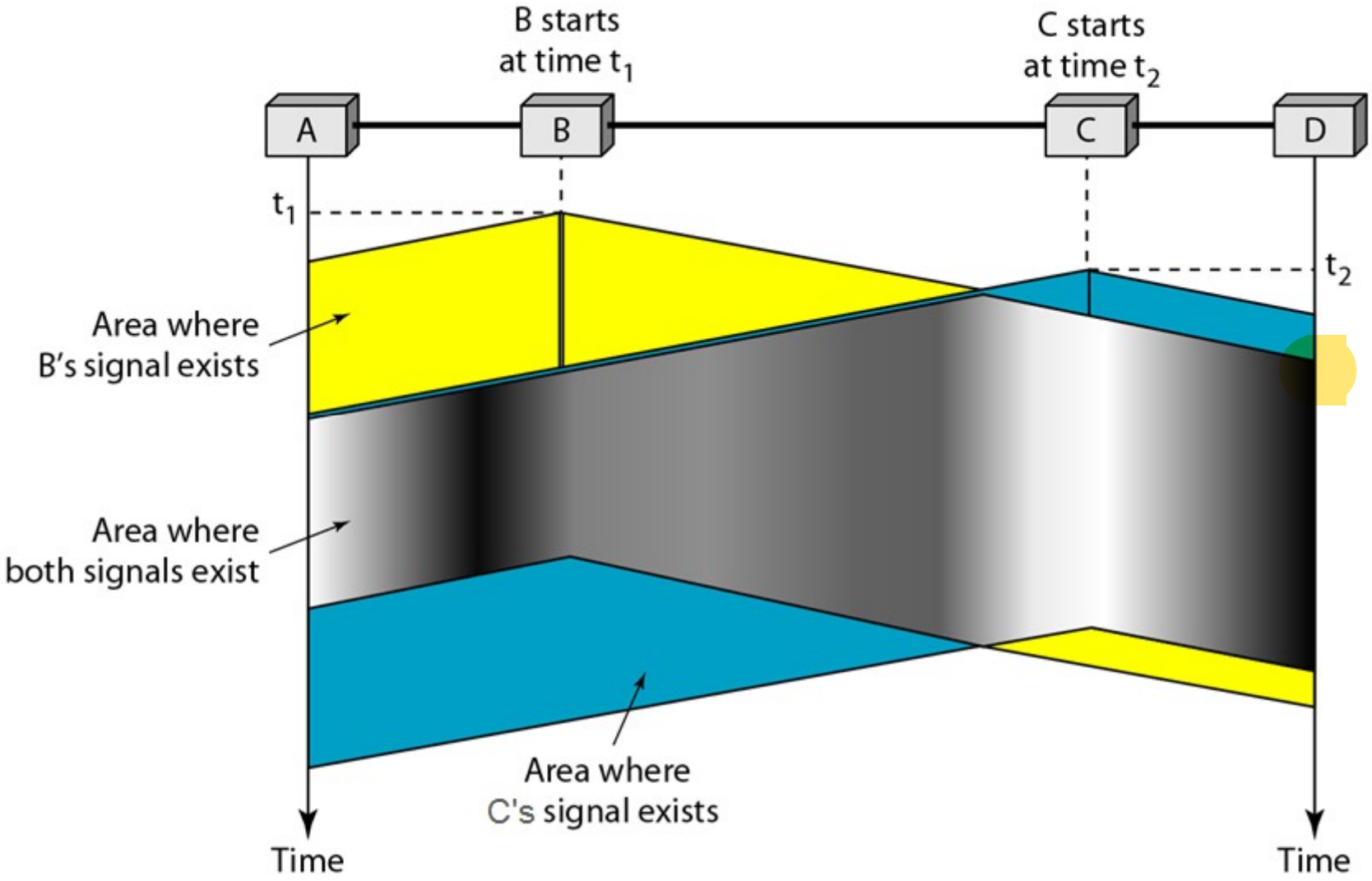
- If line idle, N may transmit frame immediately
- If line not idle
  - Alternatives: (1) non-persistent, (2) 1-persistent, (3) p-persistent
  - Tradeoff between line utilization and chance of collision

CSMA: collisions

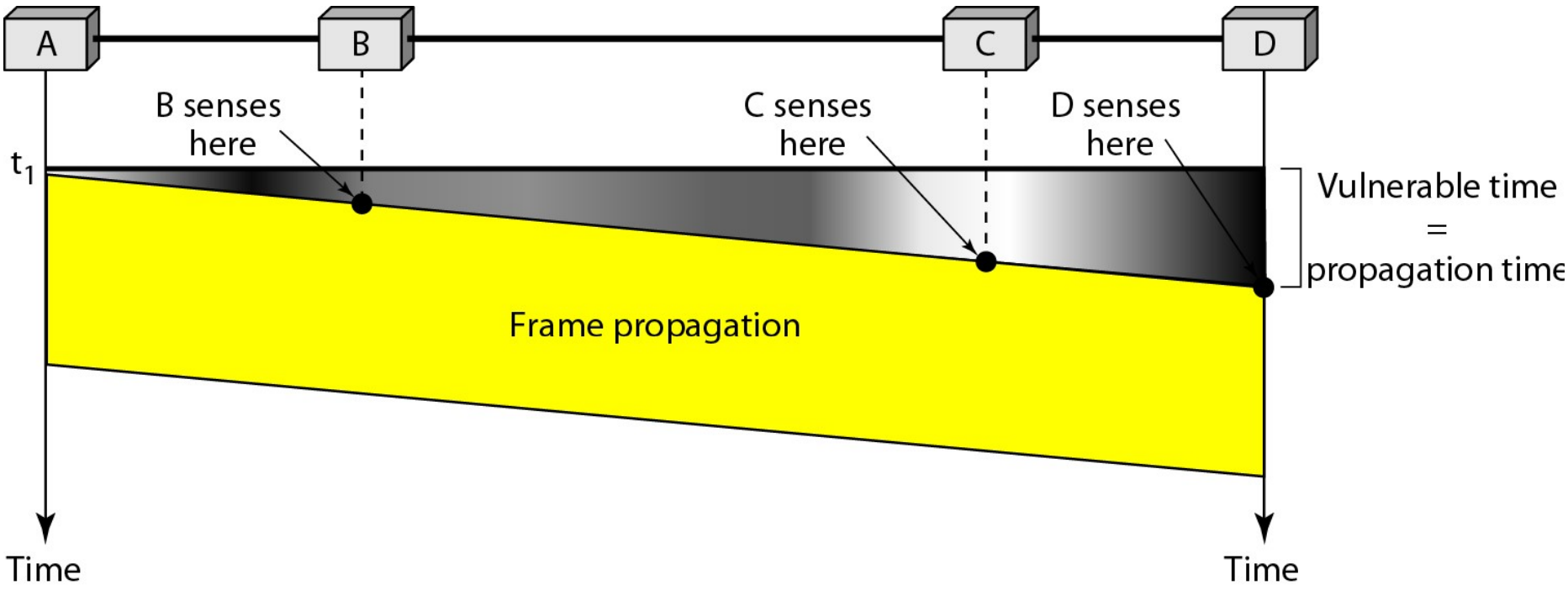
- After transmitting, station waits for ACK for a reasonable time
  - RTT + some allowance (because Rx must also contend for the channel in order to send ACK)
- If no ACK, then repeat process for transmitting
  - Sense medium; if idle, transmit; else wait …

- Collision occurs if another node N' starts transmitting within the time it takes for the first bit sent by N to reach this node N' (within the propagation delay)

Space/time model of the collision in CSMA



Vulnerable time in CSMA



CSMA – what must a node do if line is busy

Non-persistent CSMA

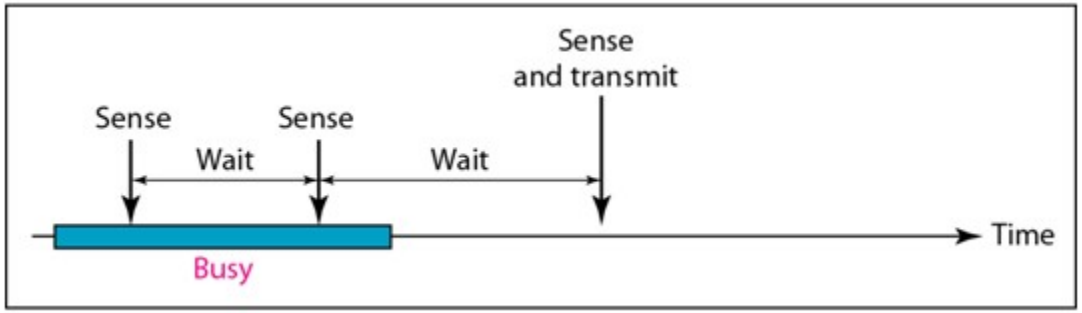
1.sense medium

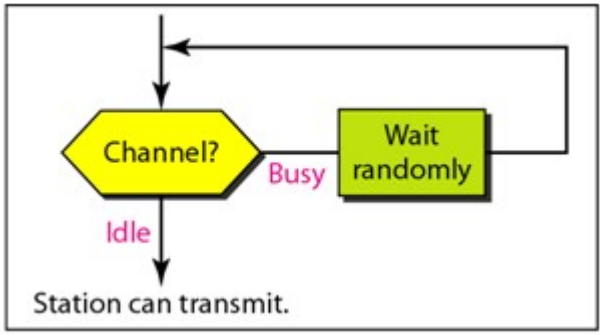
2.if medium idle

- ✓transmit frame

3.else (if medium busy)

- ✓wait for a random time
- ✓repeat from step 1

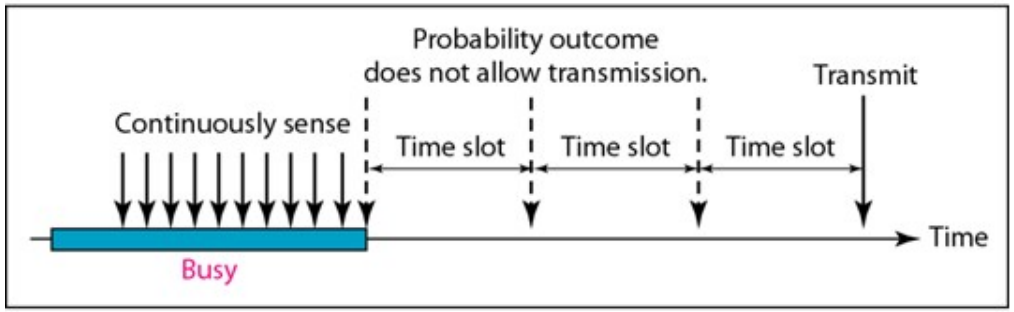


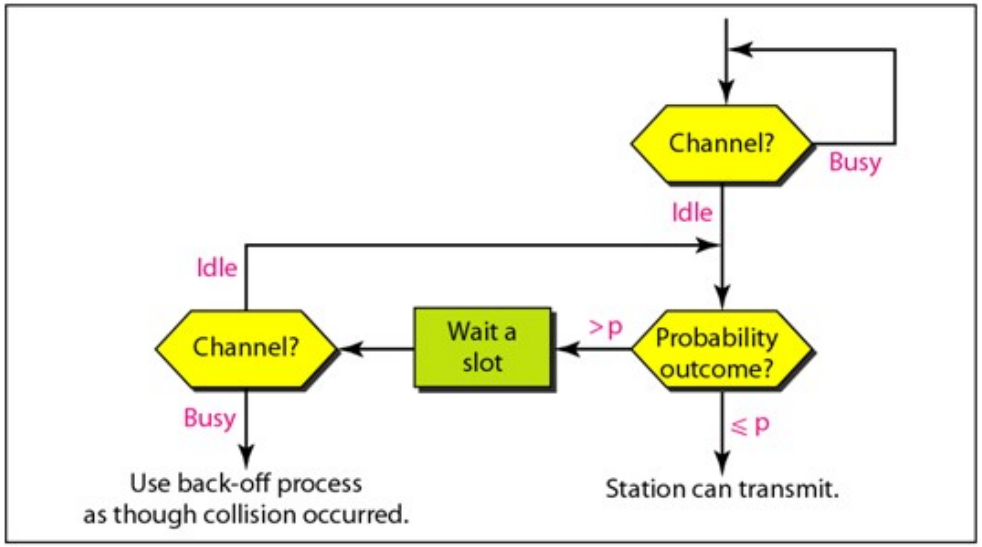


CSMA – what must a node do if line is busy (Contd)

p-persistent CSMA, $0 \le p \le 1$

1. sense medium
2. if medium idle,
   - ✓transmit frame with probability p, or
   - ✓Delay one time slot with probability q = 1-p and repeat from step 1
3. else (if medium busy)
   - ✓continue to sense medium until it is idle
   - ✓after medium becomes idle, repeat from step 2



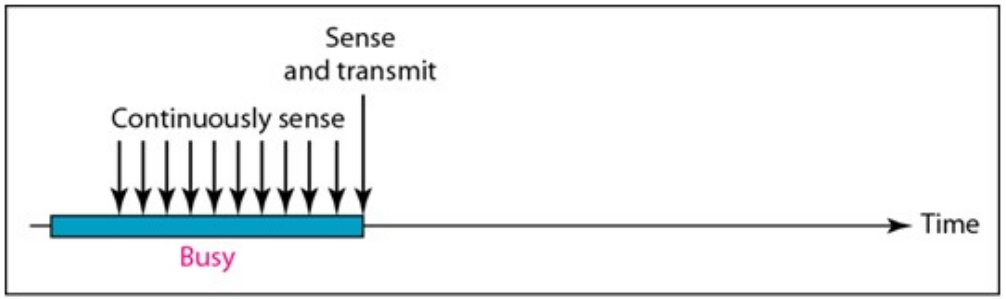


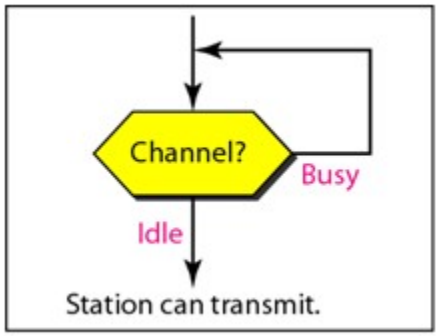
CSMA – what must a node do if line is busy (Contd 2)

1-persistent CSMA : Special case of p-persistent (with p=1)

1. Sense medium
2. if medium idle
   - ➢ transmit frame
3. else (if medium busy)
   - ➢ continue to sense medium until it is idle
   - ➢ transmit frame as soon as medium found idle

If two or more stations waiting to transmit, surely collision

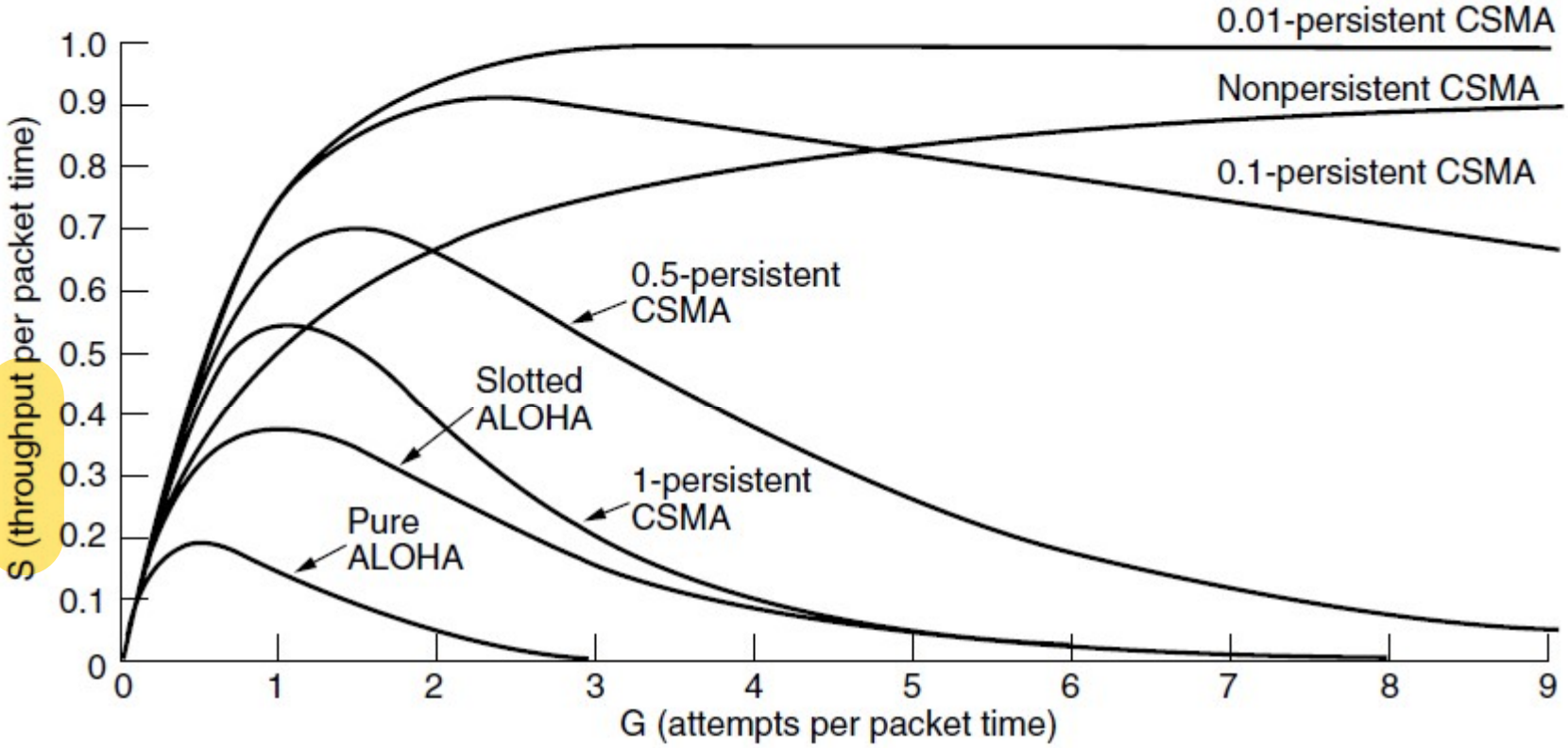




Evaluation of CSMA

- Low values of p
  - Lower chances of collision
  - But, lower channel utilization - medium will generally remain idle after the end of a transmission even if there are one or more stations ready to transmit
- Higher values of p
  - Good channel utilization
  - But, more chances of collision
- 1-persistent
  - Low load: good - prevents unnecessary wait without sensing medium
  - High load: higher chances of collision

Channel utilization of MAC protocols



Comparison of the channel utilization versus load for various random access protocols.

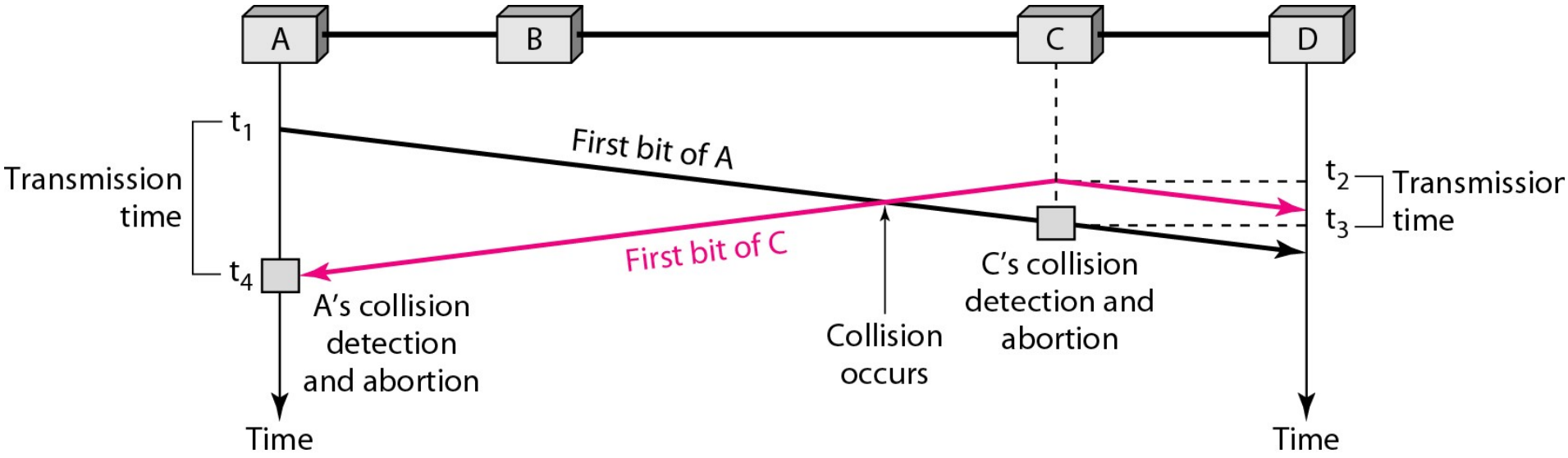
Carrier Sense Multiple Access – Collision Detection (CSMA-CD)

CSMA/CD

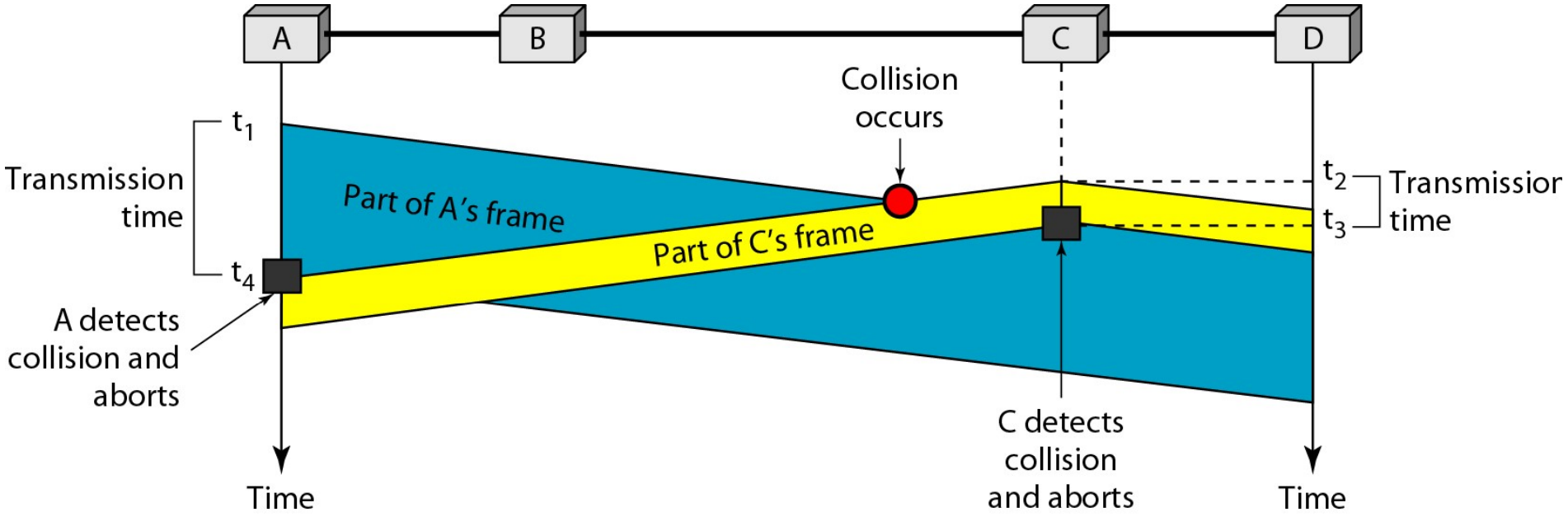
When node N is ready to transmit

1. Sense medium
2. If medium busy
   - ➢ apply standard CSMA using value of p set apriori
3. If medium idle
   - ➢ transmit, listen while transmitting
   - ➢ If collision detected during transmission
     - ✓ Transmit a brief jamming signal (specified by protocol) to ensure that all stations know there has been a collision
     - ✓ After sending jamming signal, wait for a random amount of **time slots** (binary exponential backoff)
     - ✓ Then repeat all above steps starting from step 1

Collision of the first bit in CSMA/CD



Collision and abortion in CSMA/CD



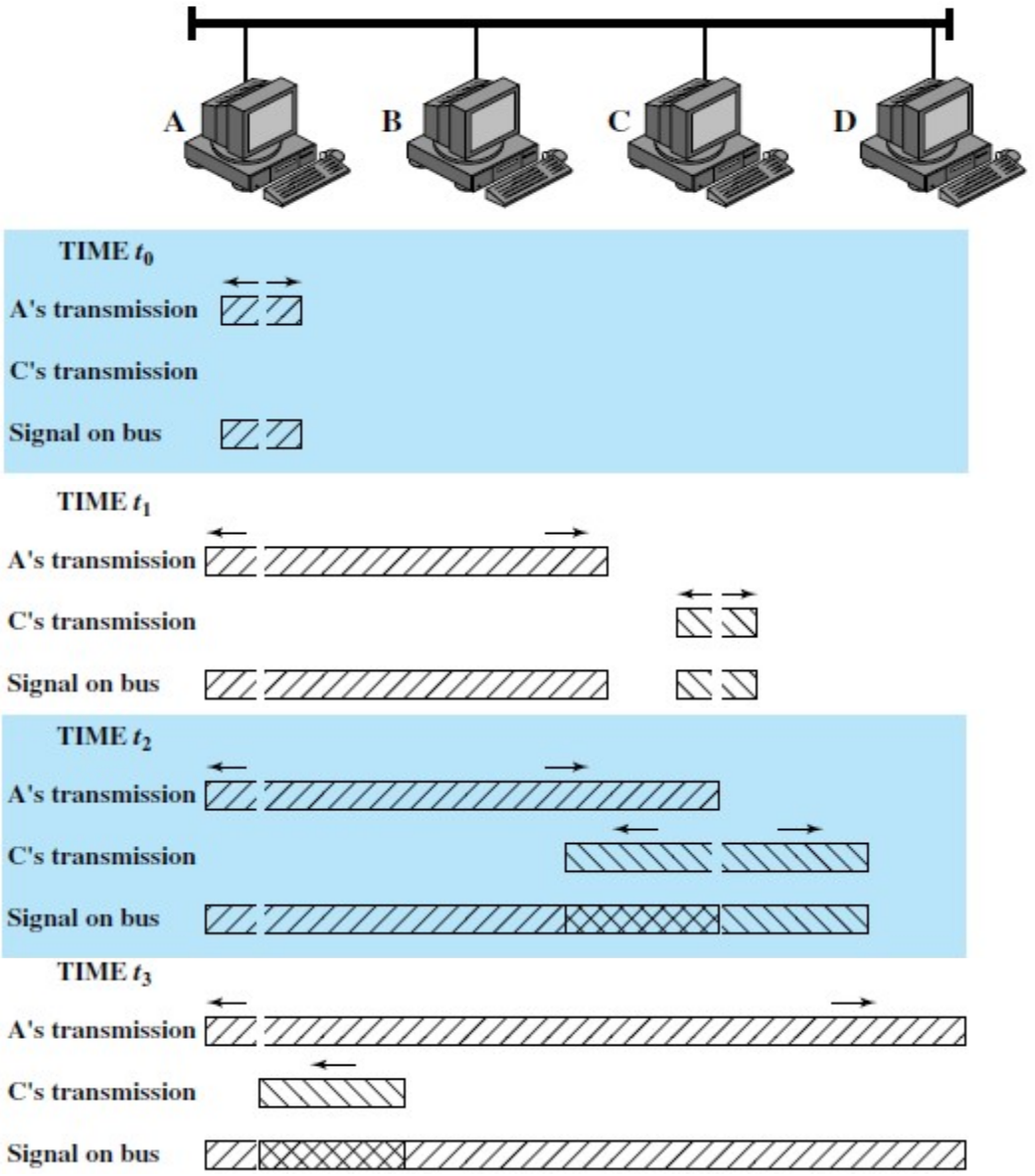
CSMA/CD Operation

At time ***t0***, station A begins transmitting a packet addressed to D.

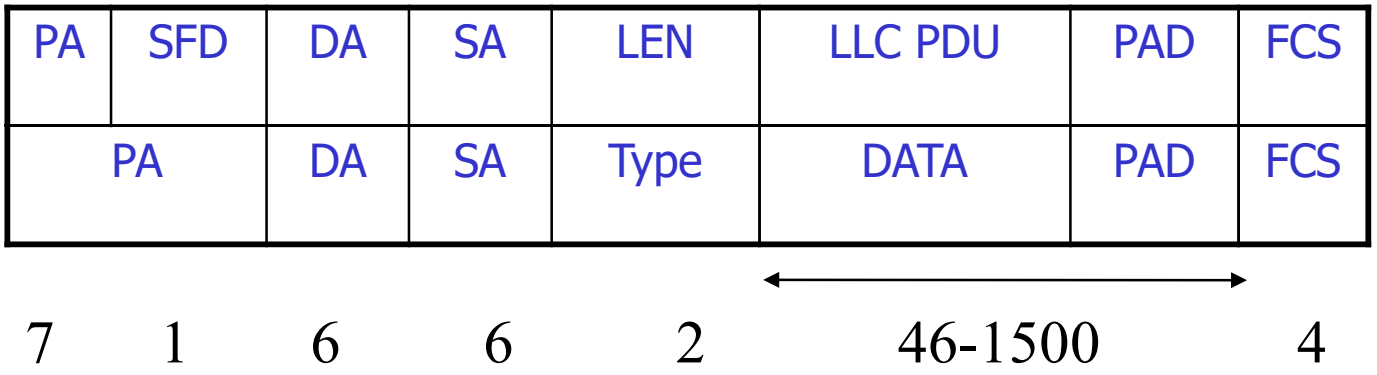
At ***t1***, both B and C are ready to transmit. B senses a transmission and so defers. C, however, is still unaware of A's transmission and begins its own transmission

At ***t2***, when A's transmission reaches C, at C detects the collision and ceases transmission

At ***t3***, the effect of the collision propagates back to A, and then A ceases transmission



Ethernet Frame Format (*to be discussed later*)



IEEE 802.3

DIX Ethernet

- PA: Preamble --- 7 bytes 10101010s for synchronization
- SFD: Start of frame delimiter --- 10101011 to start frame
- DA, SA: Destination & source MAC address
- LEN: Length --- number of data bytes
- Type: Identify the higher-level protocol
- LLC PDU + Pad: minimum 46 bytes, maximum 1500
- FCS: Frame Check Sequence, using CRC

CSMA/CD and Minimum Frame Size

For CSMA/CD to work, there is a 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, because
  - once the entire frame is sent, sender 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. **But Why ?**
  - Consider the worst-case scenario - the two stations involved in a collision are the maximum distance apart
    - ✓ the signal from the first takes time T_p to reach the second
    - ✓ and the effect of the collision takes another time T_p to reach the first
- So the requirement is that the first station must still be transmitting after $2T_p$

CSMA/CD and Minimum Frame Size

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (*including the delays in the devices and ignoring the time needed to send a jamming signal*) is 25.6 μs (micro sec), what is the minimum size of the frame?

Solution:

- The frame transmission time is atleast $T_{fr} = 2 \times T_p = 51.2$ μs.
  - This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision.
- The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes.
- This is actually the minimum size of the frame for Standard Ethernet

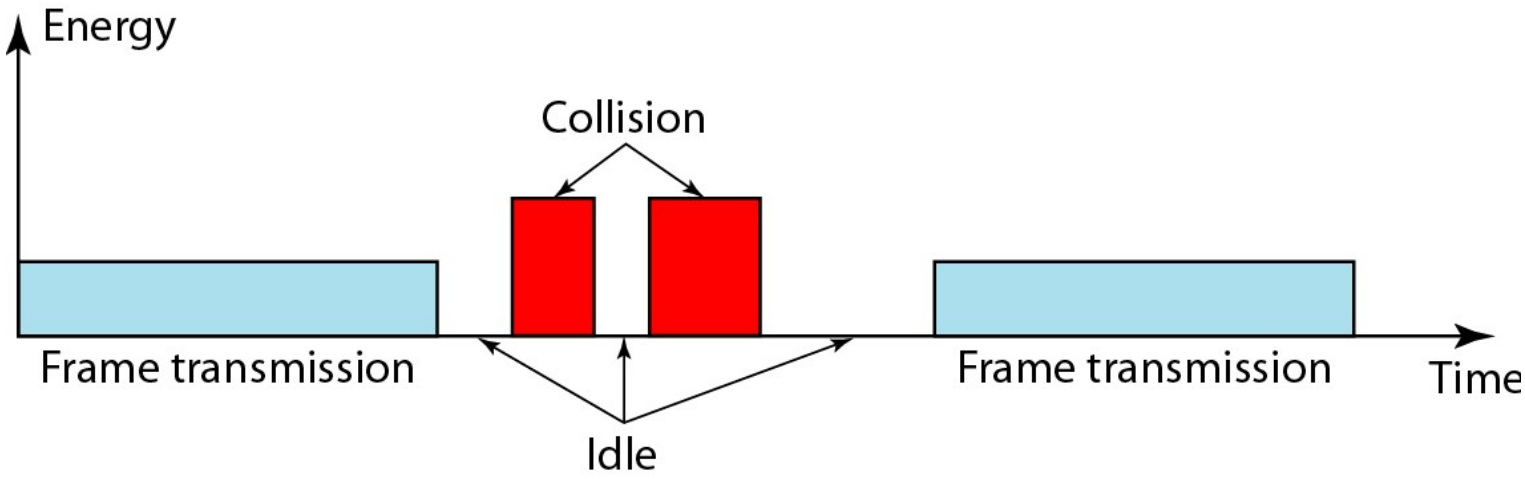
CSMA/CD and Maximum Frame Size

The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.

It has two historical reasons

- First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer.
- Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Contention, transmission, or idle state and their energy level in CSMA/CD

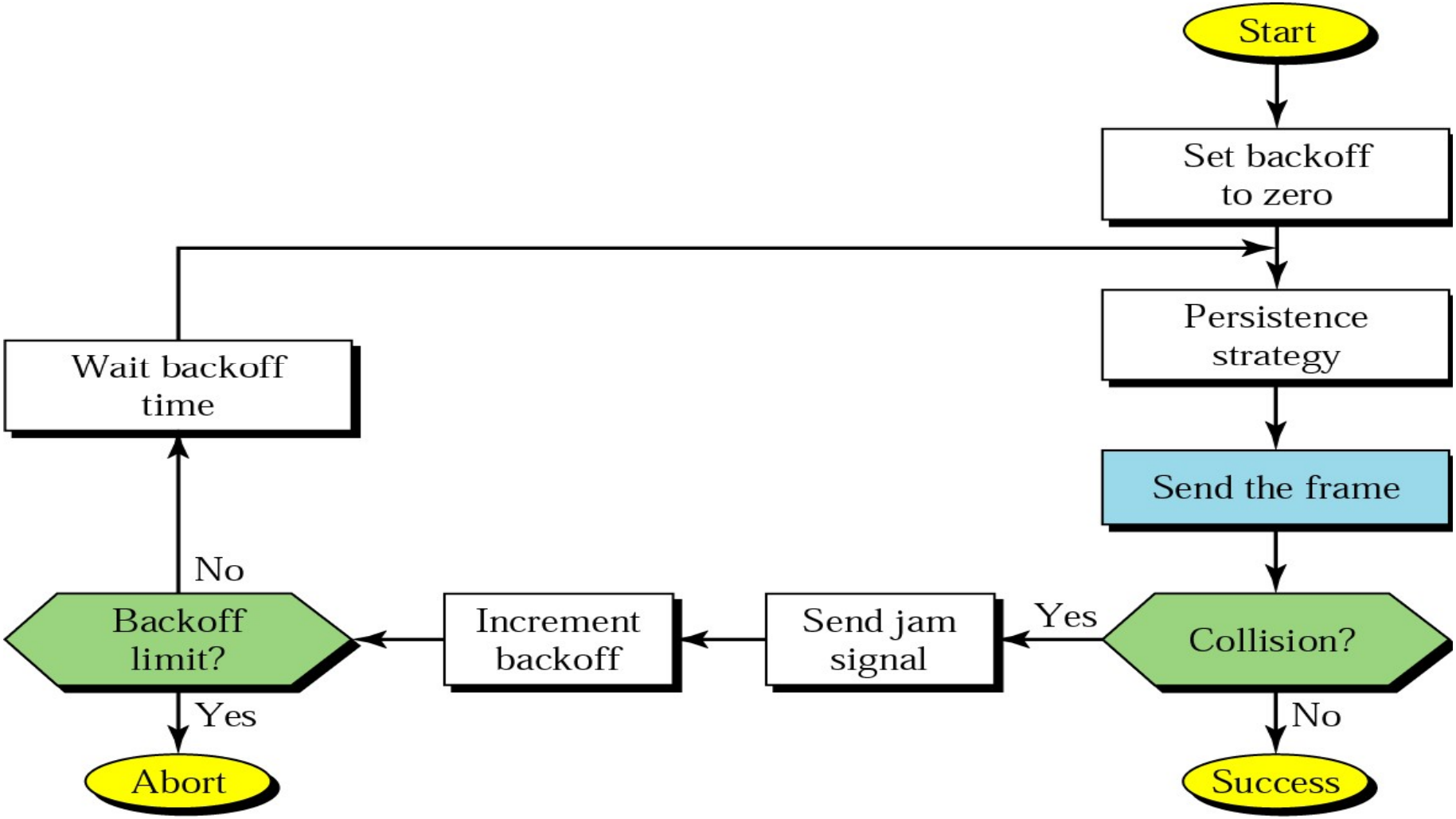


Binary exponential backoff algorithm

- After collision has been detected, waiting time must be adaptive to load
  - Low load => low wait time (high wait time may cause low channel utilization)
  - High load => relatively high wait time (low wait time may cause frequent collisions)

- How to estimate load? By number of repeated collisions
  - After k collisions, choose a waiting time randomly between 0,1,2,…,2^k-1 **slots**, k<=10
    - In the 802.3 ethernet, 51.2μs is considered as fixed slot time
  - After 10 collisions, for 10 <= k <= 16, choose a waiting time between 0 and 2^{10}-1
  - After 16 collisions, give up

CSMA/CD with Binary Exponential Backoff



Carrier Sense Multiple Access - Collision Avoidance (CSMA-CA)

For Your Study

References

- *Data Communications & Networking, 5th Edition, Behrouz A. Forouzan*
- *Data and Computer Communication, William Stallings*
- *Computer Networks, Andrew S. Tanenbaum and David J. Wetherall*

Data Communication and Computer Network

Local Area Network

Local Area Network (LAN)

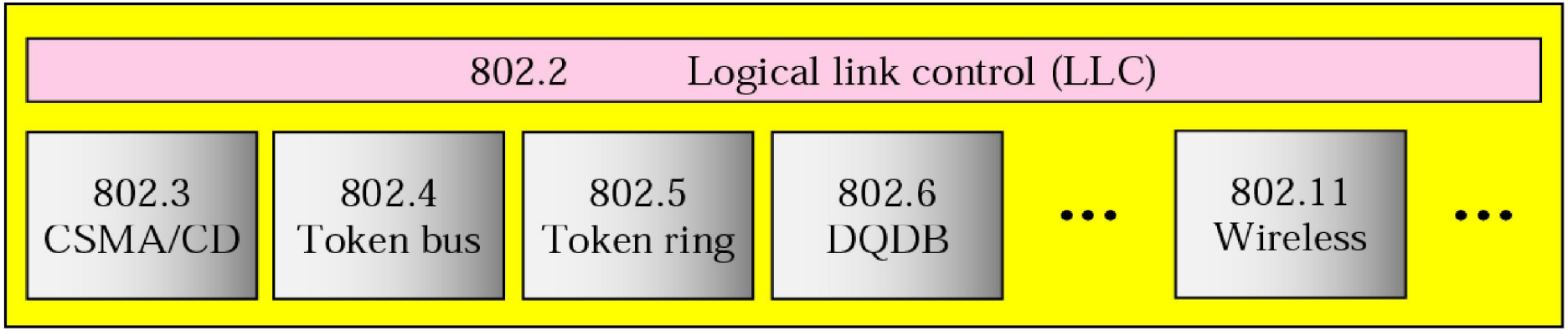
- Characteristics
  - Small geographical area, limited distance
  - Small number of directly-connected machines
  - Relatively high data rate
  - Single management
- Specifications mostly at physical layer and data link layer
- The most used example: Ethernet
- Developed in early/mid 70's in Xerox PARC

Ethernet – two standards

- DIX standard
  - **D**igital / **I**ntel / **X**erox standardized 10 Mbps Ethernet in early 80's
  - Specifies details of physical layer and MAC layer using CSMA/CD

- IEEE 802 standard (1985) split Data Link layer into two sub-layers
  - Logical Link Control: error control, flow control, etc
  - Medium Access Control: error detect (FCS), decides how to access shared medium (CSMA/CD, token ring, wireless, …)

IEEE 802 family of protocols



Project 802

IEEE 802.2 plus one of 802.3, 802.4, … specifies the complete physical & data link layers

Relation between DIX Ethernet standard and IEEE 802 standard

- Frame format for both standards almost same, except for small differences
- TCP/IP implementations use original DIX Ethernet frame format, LLC sub-layer used not used
  - Network layer directly uses Ethernet frames
- Nodes using both types can coexist on same LAN

No LLC

- In real-world *wired* networks (most use TCP/IP), the LLC sub-layer almost never implemented
  - Error & flow control has to be handled from source to destination (over multiple links)
  - Data can be lost within links and at intermediate nodes
  - LLC controls error & flow over a single link only

  - So, ensure error & flow control from source to destination (end nodes) at higher layers, and
  - Do away with the LLC sub-layer

IEEE 802.3 (Ethernet)

- Multiple types within this depending on speed, media type, etc
  - Standard 10 Mbps Ethernet versions
    - 10Base5 : 10 Mbps, thickwire coaxial cable
    - 10Base2 : 10 Mbps, thinwire coax or cheapernet
    - 10Base-T : 10 Mbps, twisted pair, hub-based
    - 10Base-FL : 10 Mbps, optical fiber, hub-based
  - Fast Ethernet (100 Mbps) versions
  - Gigabit Ethernet (1000 Mbps) versions
- All the above have the same frame format, same addressing format
  - differences mostly in physical layer details like medium, connector, encoding used, etc.

IEEE 802.3 (Ethernet) Cabling

Name	Cable	MAX Segment	Nodes/seg.
10Base5	Thick coaxial	500 meters	100
10Base2	Thin coaxial	200 meters	30
10Base-T	Twisted pair	100 meters	1024

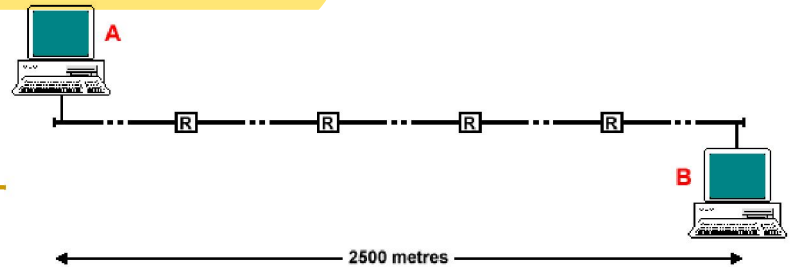
- **10Base5 cabling:** This type of cabling is popularly referred to as **thicknet**. It was one of the earliest types of cables used for LAN's. The notation 10Base5 suggests that the LAN operates at 10 Mbps, uses baseband signaling and can support segments of up to 500 meters.

- **10Base2 cabling:** 10Base2 or **thinnet,** which in contrast to thicknet, bends easily. 10Base2 cables are easier to install and are relatively inexpensive. The only drawback of using the 10Base2 cable is that it can run for only 200 meters and can handle only 30 stations per cable segment.

- **10Base-T cabling**: there is no single, main cable because each station has a cable running to a central **hub** (a big repeater). Adding or removing stations is simpler in this configuration and cable breaks can be detected easily. The disadvantage of 10Base-T is that the maximum cable run from the hub is only 100 meters, sometimes 150 meters (if high quality twisted pairs are used). 10Base-T is most popular due to the ease of maintenance.

Bus topology – used in Ethernet

- Transmission propagates throughout medium, heard by all stations (bi-directional medium)
  - Each station needs unique address
- Signal balancing
  - Signal must be strong enough to meet receiver's minimum signal strength requirements
- Need to regulate transmission
  - To avoid collisions
  - To avoid hogging by a single node, break data into frames
- Multiple segments can be joined by repeaters



Repeaters

- Joins two (or more) segments of cable
- Function
  - Input signal at one of the ports
  - Extracts data from input signal (filters out noise)
  - Amplifies data: encodes data in signal and transmits along all other ports
- Does not understand frame format, does not look inside frame
- There should be only one path of segments and repeaters between any two stations

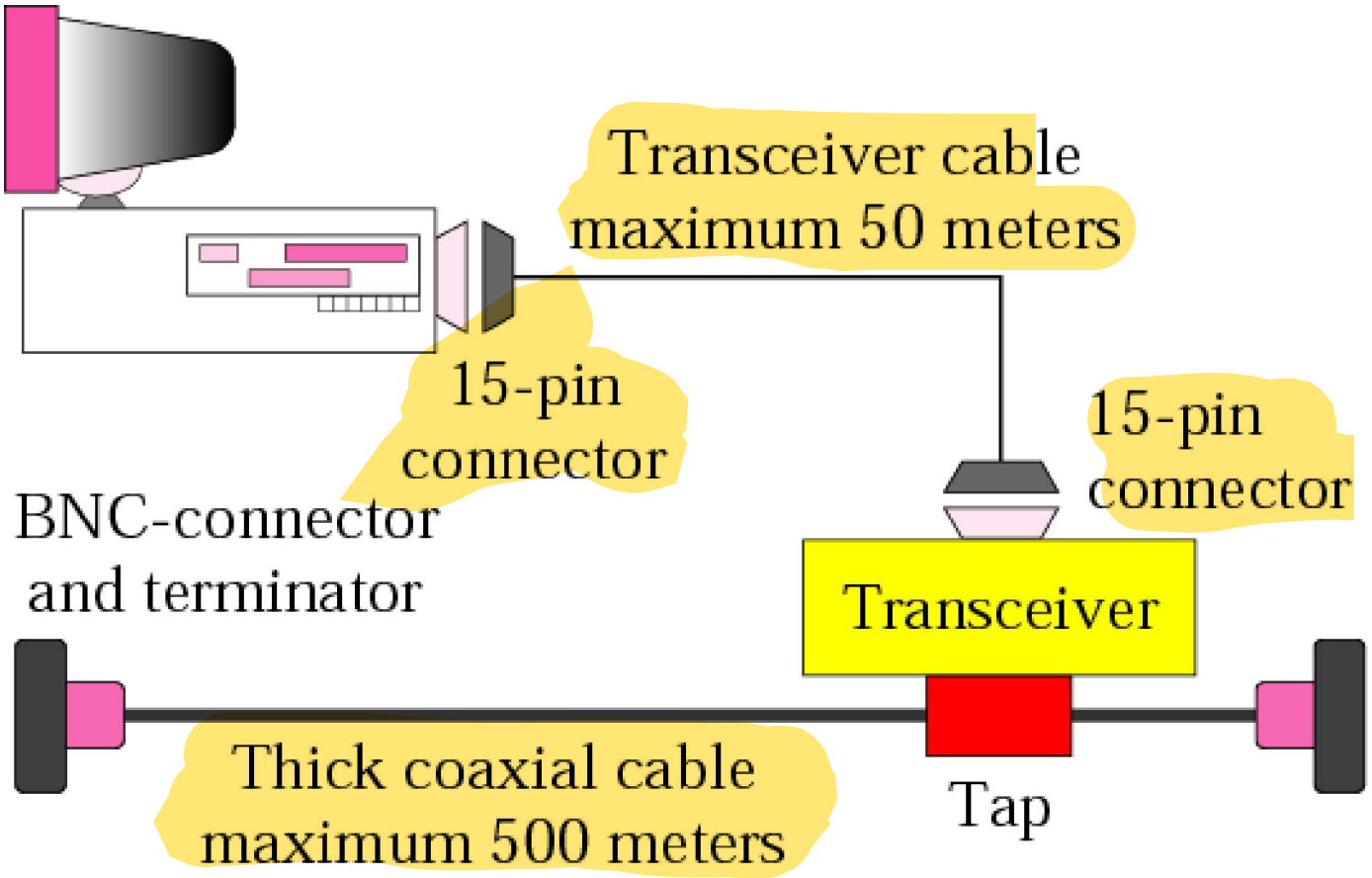
Example of a specific technology: 10Base5

- 10Base5 is the original implementation of Ethernet and 802.3
- Uses shared bus medium – thick coaxial cable (0.4 inch diameter) at 10 Mbps
  - Bus topology
  - Max cable length 500m between repeaters
  - Maximum 4 repeaters (5 segments) => maximum distance between two nodes is 2500 meters
- Distance between taps (nodes): a multiple of 2.5m
  - Hence, maximum 1000 taps
- Manchester encoding used

10Base5 technology (contd.)

- How to sense carrier (to see if line is idle)
  - Is there a transition in the middle of bit-time?
- How to detect collision
  - If two signals overlap, the average DC voltage increases above a threshold value
- Jamming signal
  - 32 or 48 bits of 01010101…
- How to understand end of frame
  - Is there a transition in the middle of bit-time?
- MAC layer specification
  - 1-persistent CSMA/CD for transmission
  - binary exponential backoff for retransmission

Connection of a station to the medium using 10Base5

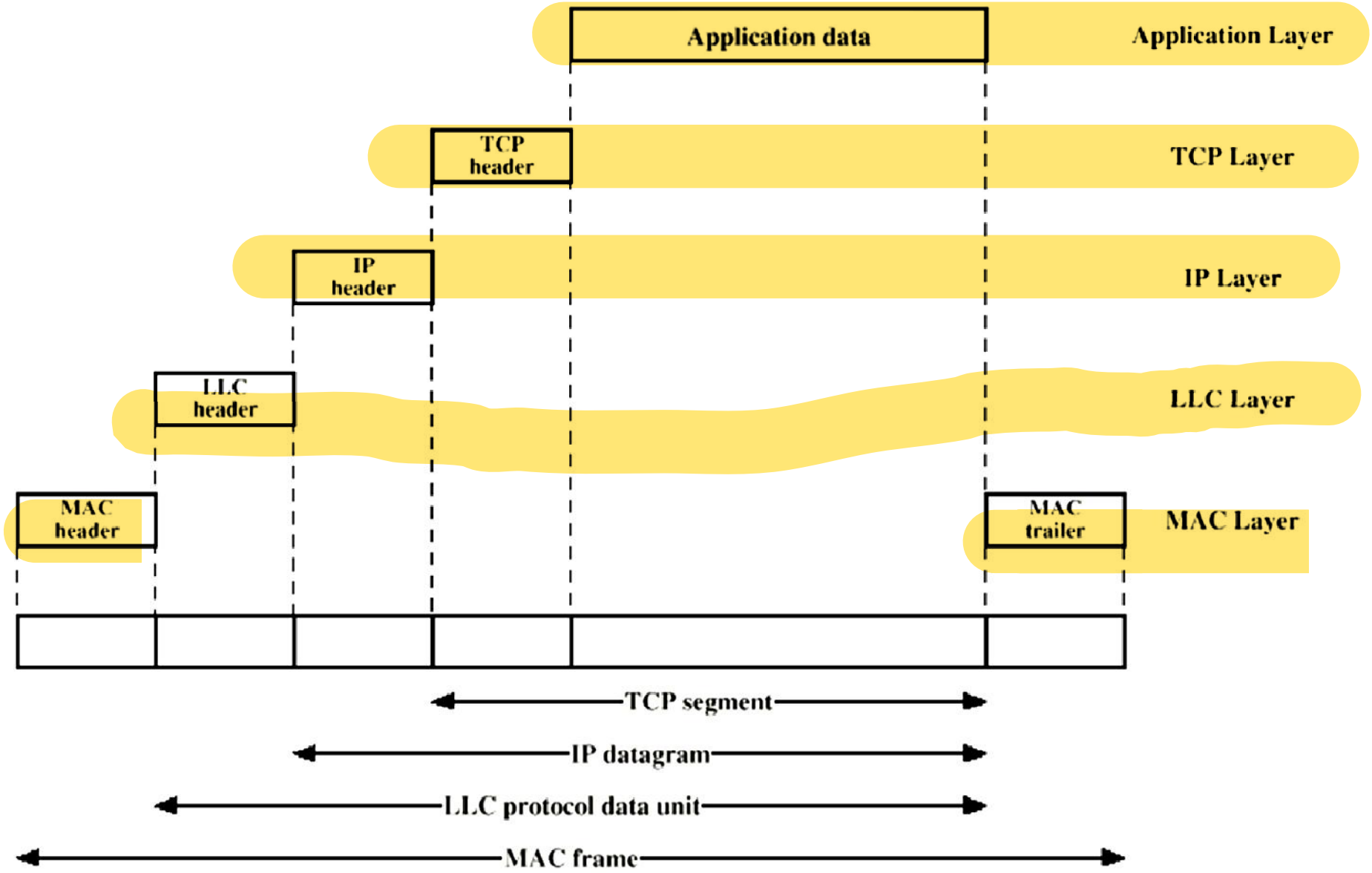


a. 10BASE5

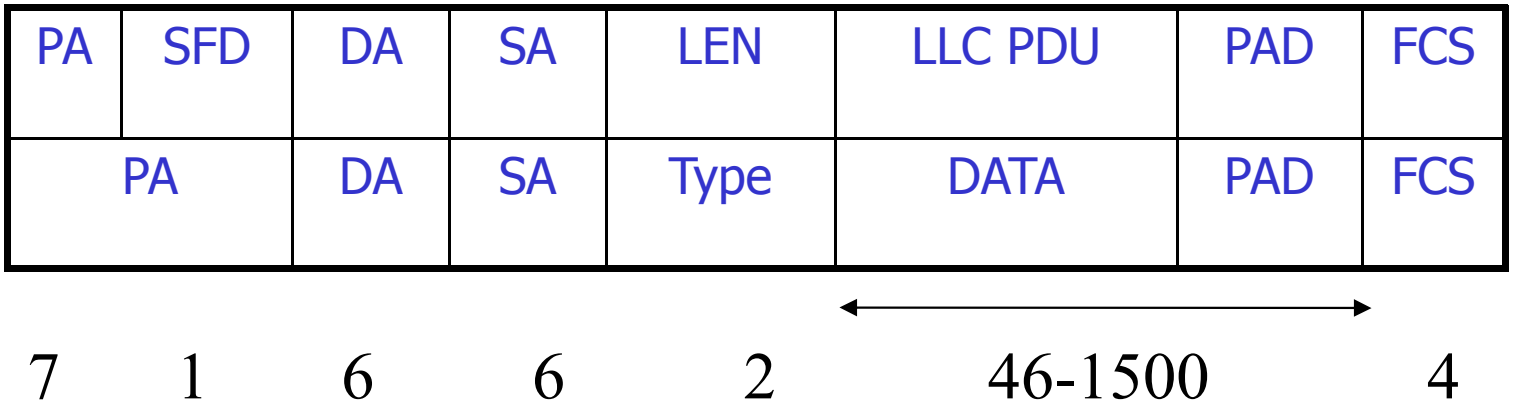
MAC address

- A unique hardware address for each LAN interface
- Hard-coded into Network Interface Card (NIC)
- 48-bit address, expressed as 12 hex digits
  - 24-bit vendor code, 24-bit serial number
  - Different NIC vendors given different vendor codes
- ff.ff.ff.ff.ff.ff is broadcast address: this is Layer 2 broadcast

MAC Layer PDU



Ethernet Frame Format



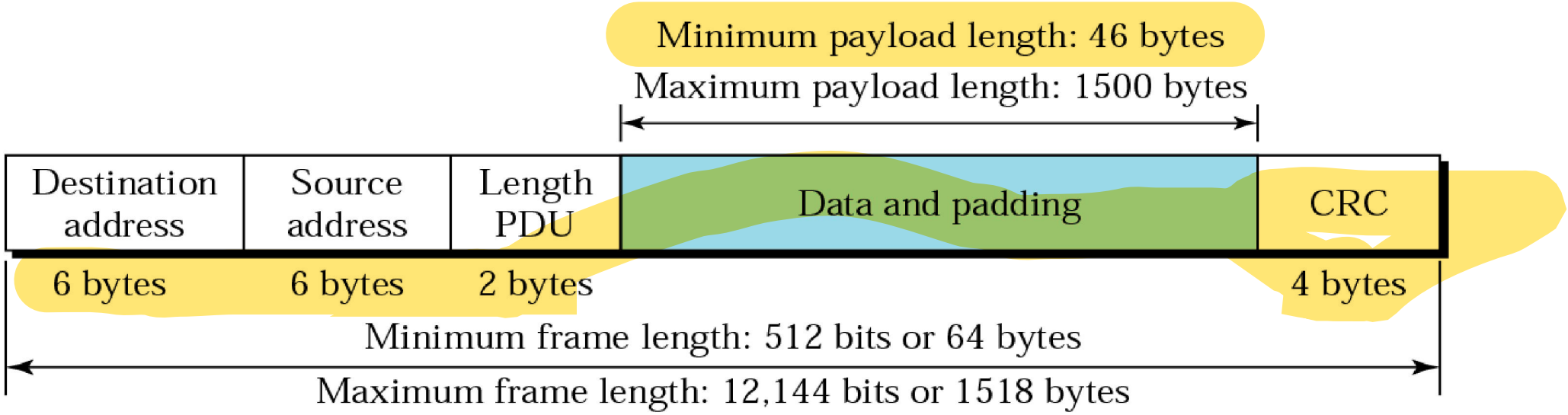
IEEE 802.3

DIX Ethernet

- PA: Preamble --- 7 bytes 10101010s for synchronization
- SFD: Start of frame delimiter --- 10101011 to start frame
- DA, SA: Destination & source MAC address
- LEN: Length --- number of data bytes
- Type: Identify the higher-level protocol
- LLC PDU + Pad: minimum 46 bytes, maximum 1500
- FCS: Frame Check Sequence, using CRC

Minimum frame size in Ethernet

- A frame must take at least 2t time to send
  (t = maximum one-way propagation delay)
- For Ethernet, 2t = 51.2 microseconds
  - This includes delay introduced by four repeaters



Why must the IEEE 802.3 (Ethernet) frame be at least 64 bytes long?

Calculations:

- LAN Length (L) = 500 m (per segment) x 5 segments = 2500 meters
- Velocity of propagation on the cable (V) = $2 * 10^8$ meters/sec
- Delay added by repeater (D) = ~3µsec x 2 (Bi-Direction) x 4 Repeaters = 24µsec
- Round Trip Delay (RTD) = (Total Distance/V) + Repeater Delays (D)
- Total Distance/V = $(2*2500/2 * 10^8) = 25 * 10^{-6}$ sec or 25µsec
- Hence RTD = 25 + 24 = 49 µsec

- Now, time to transmit 64 bytes = 512 bits / $10 * 10^6 = 51.2\ 10^{-6}$ sec or 51.2 µsec (referred to as slot time in the 802.3) which is greater than the RTD of 49 µsec.
- Hence the minimum frame size for the IEEE 802.3 (Ethernet) is 64 bytes.

* µsec → microsecond

Fast Ethernet (100Mbps)

- Fast Ethernet operates at 100Mbps. For the most part, the scheme/protocol remains the same as the 10Mbps case, except now the maximum length of the network is shortened.

- Minimum frame size is still kept at 64 bytes (for backward compatibility), which now arrive 10 times faster than they do in 10Mbps Ethernet.

- Hence the maximum length of the network must be 10 times smaller or about around 250 meters.

Gigabit Ethernet

Carrier extension for 1 Gbps Ethernet

- In Gig Ethernet, it would be necessary to reduce the LAN size to 25m in order to retain the min frame size of 64 bytes.
- Instead, Gigabit Ethernet uses a bigger slot size of 512 bytes. To maintain compatibility with Ethernet, the minimum frame size is not increased, but the "carrier event" is extended.
- If the frame is shorter than 512 bytes, then it is padded with extension symbols. These are special symbols, which cannot occur in the payload. This process is called *Carrier Extension* (performed by the NIC card in hardware and is stripped away before the FCS is calculated on the receiving side).

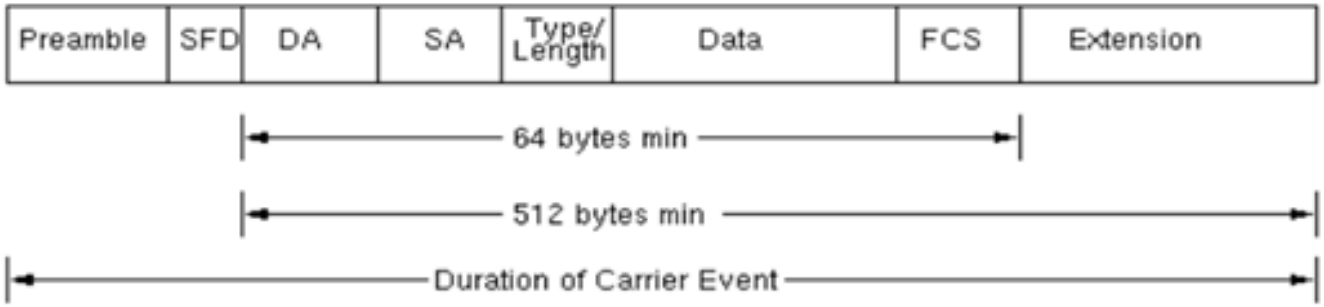


Fig . Ethernet Frame Format with Carrier Extension

IEEE 802.3 (Ethernet) Performance

- Efficiency (line utilization) decreases as the number of stations trying to transmit (under heavy load) increases due to the increased probability of collisions. 30% line utilization (or 3 Mbps throughput) is considered heavy load.

- Larger the frame size the higher the efficiency or utilization (due to higher payload since the header size of the frame is fixed). E.g. for 1024 byte frame, efficiency is about 85% and for a 64-byte frame, efficiency is about 30%.

Switched Ethernet

(Formerly Bridge Ethernet)

Two terms

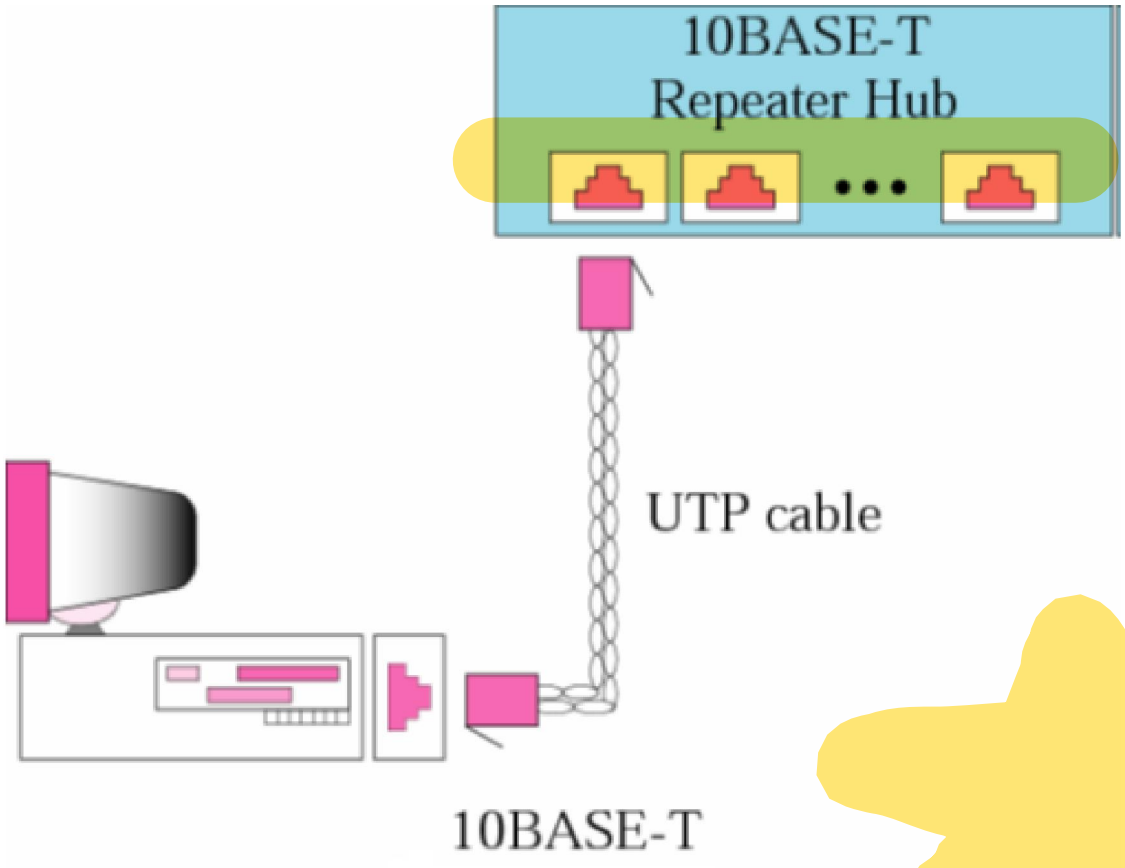
- Segment
  - Part of medium without any repeater
  - One or more stations can connect to a segment
  - Segments can be connected using repeaters
- Collision domain
  - Set of machines such that two machines transmitting can cause collision
  - One or more segments
- Repeaters (physical layer devices) do NOT guard against collision
  - Several segments connected by repeaters are within the same collision domain

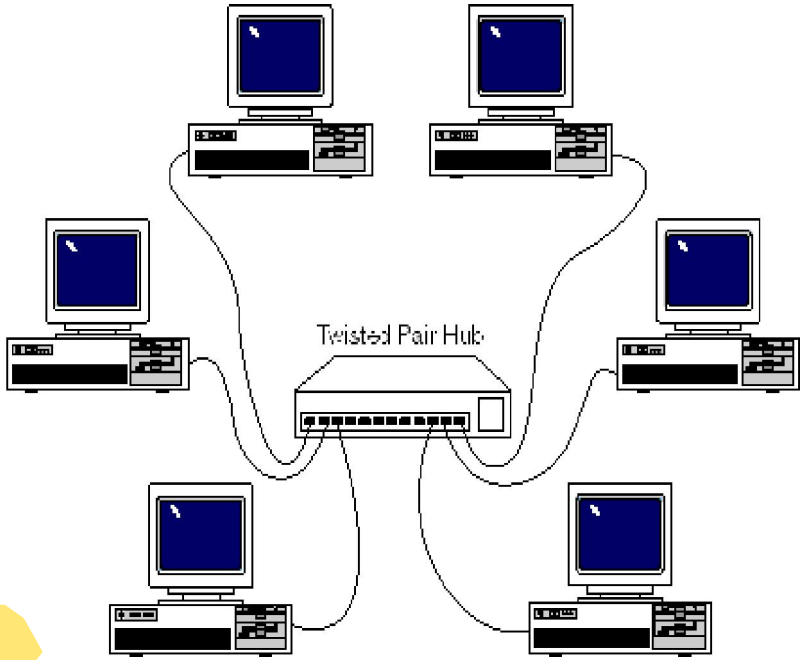
Hubs

- Hub: a multi-port repeater
  - all nodes in a LAN may be connected to a central Hub (physically a star topology)
  - inside hub is a simple medium connecting all nodes, messages sent by each node reach all other nodes (logically a bus topology)

- Hub functions at the physical layer, similar to a repeater
  - Does not guard against collision (logically bus)

Connection of stations to the medium using 10Base-T and Hub





LAN using Hub: 10BaseT

- 10 Mbps, baseband, Unshielded Twisted Pair (two pairs) Cat 3 or better used
- Logical topology bus, physical topology star using hub
- Maximum distance from station to hub = 100 m
- Collision domain: all machines connected to a hub
- Manchester encoding
- 1-persistent CSMA/CD for transmission, binary exponential backoff for retransmission
- Base wait period (Ethernet Slot Time) of 51.2μsec, Inter-frame gap of 9.6 μsec

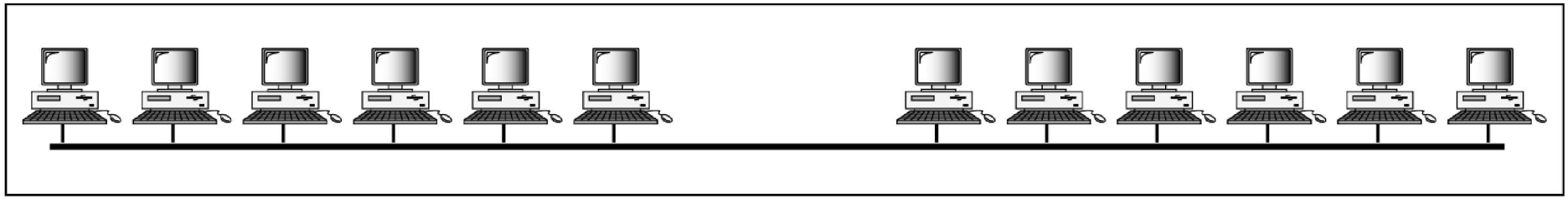
Switches in place of Hubs

- Switch (also called Layer 2 switch)
  - Hubs are nowadays replaced by switches
  - Frames NOT always broadcast, sent to only that port to which destination node is connected

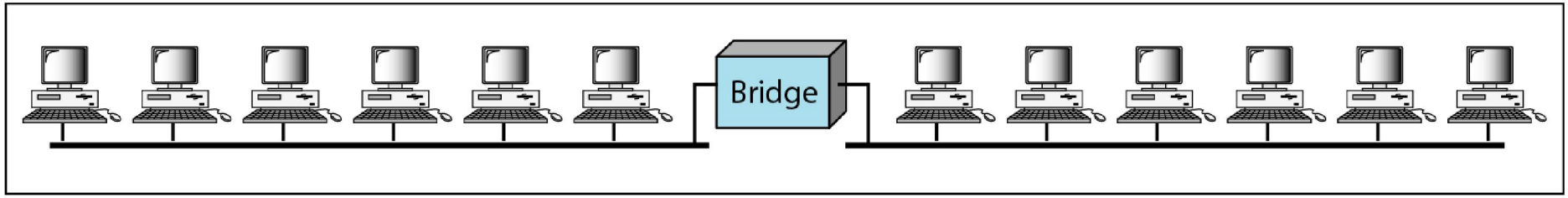
- Advantages of switch over hubs
  - Separates the single collision domain of to multiple collision domains
  - Allows more than one pair of nodes to communicate parallely

A network with and without a Bridge

- The first step in the Ethernet evolution was the division of a LAN by bridges.
- Bridges have two effects on an Ethernet LAN:
  - They raise the bandwidth and they separate collision domains.

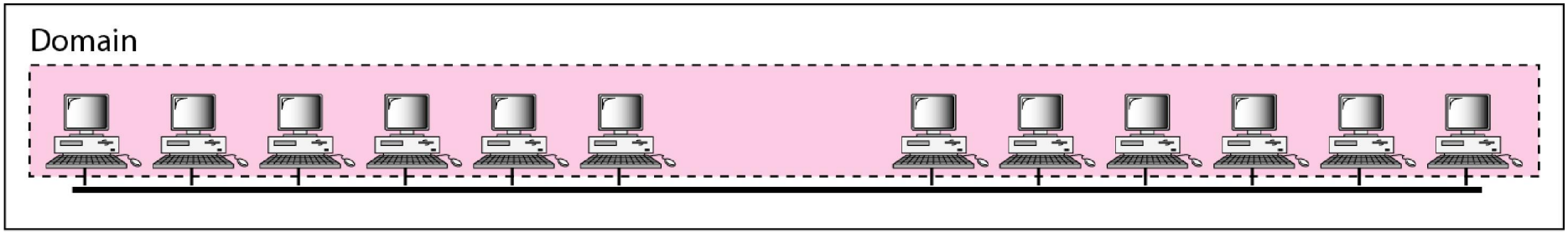


a. Without bridging

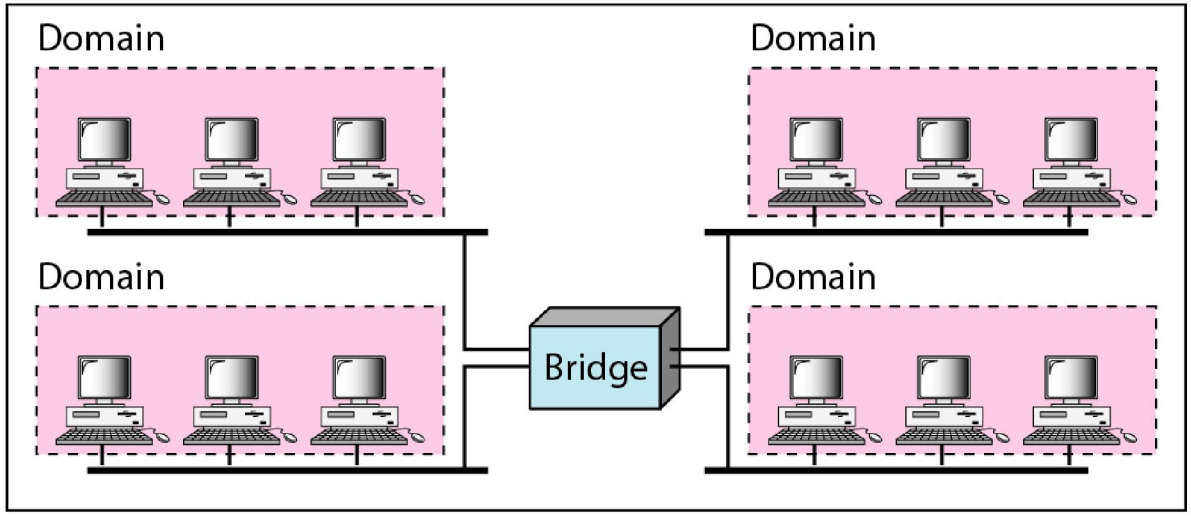


b. With bridging

Collision domains in an unbridged network and a bridged network



a. Without bridging



b. With bridging

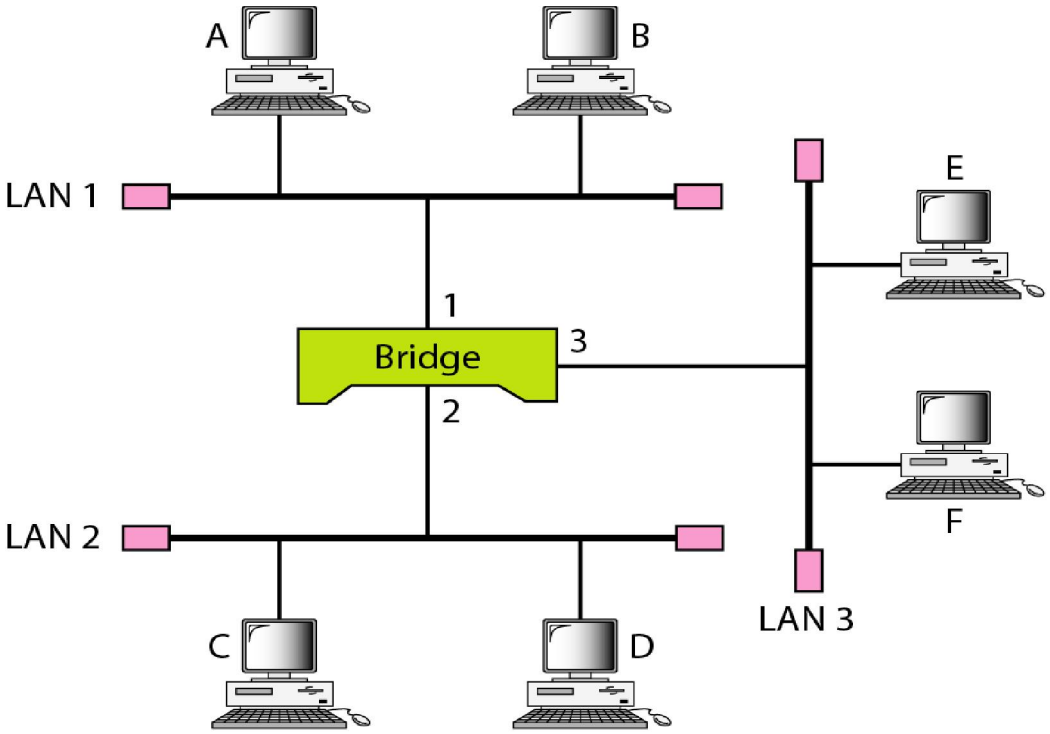
L2 Switches

- As traffic increases (due to increased number of stations) the LAN will eventually saturate. The solution is a switched 802.3 LAN.
- A layer 2 switch is an N-port bridge with additional sophistication
- For selective send of frames, switch needs to know which node is connected to which port
- Switch learns – switch builds up a table of MAC address of nodes and port numbers

L2 Switches

- Suppose m/c A sends frame to m/c B
  - Switch knows nothing initially, so broadcasts to all ports
  - But switch now knows which port A is connected to!
  - Hereafter, if a frame comes for A, it will be forwarded to only A's port
  - Internal table completely built up when every m/c has sent at least one frame

A learning L2 Switch and the process of learning



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

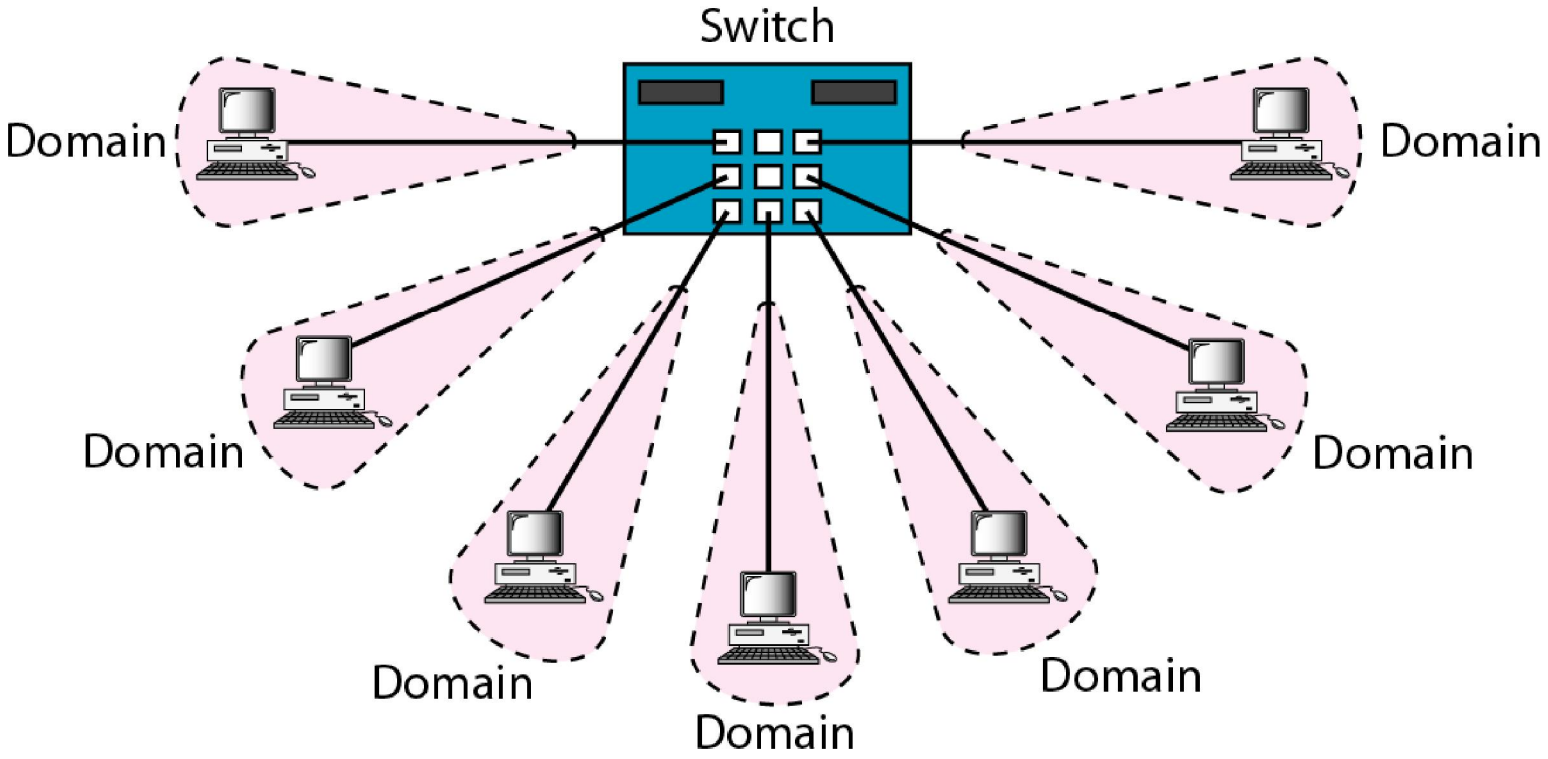
Address	Port
A	1
E	3

c. After E sends a frame to A

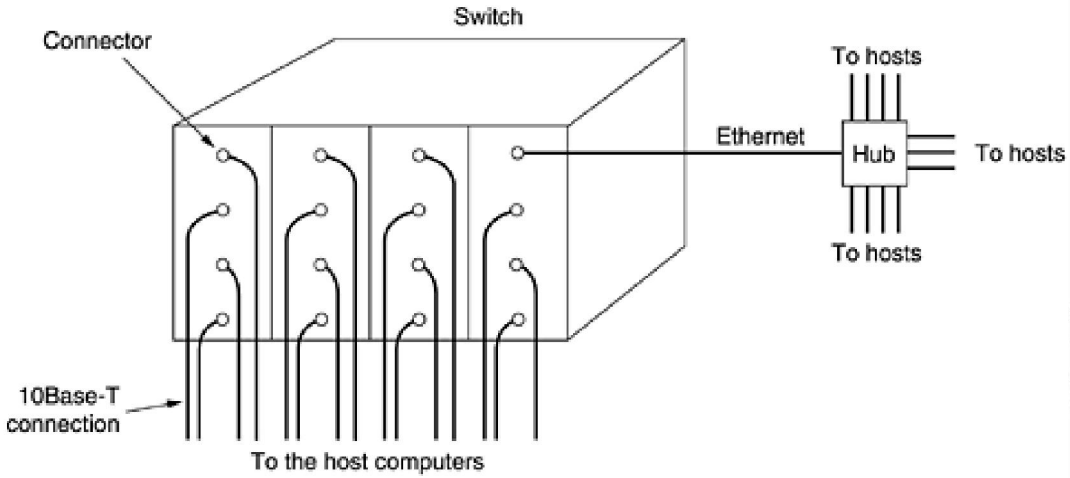
Address	Port
A	1
E	3
B	1

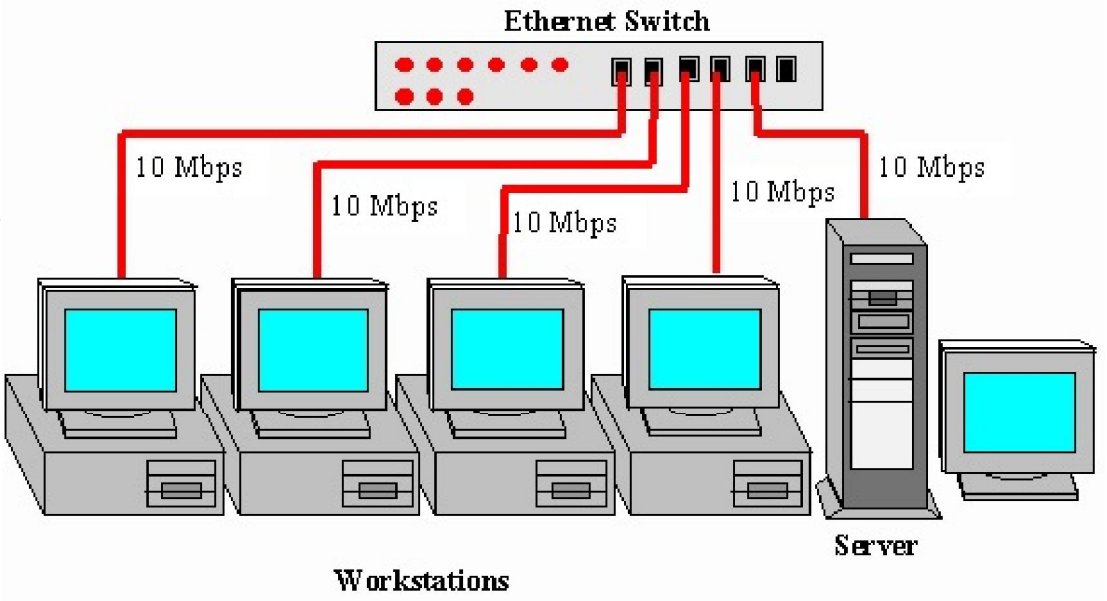
d. After B sends a frame to C

Switched Ethernet (modern days LAN)



Switched Ethernet (modern days LAN)





References

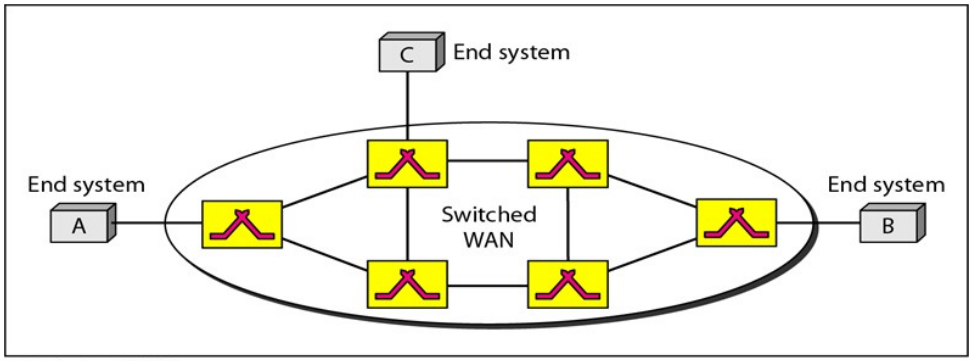
- *Data Communications & Networking, 5th Edition, Behrouz A. Forouzan*
- *Computer Networks, Andrew S. Tanenbaum and David J. Wetherall*
- *Wikipedia*

Data Communication and Computer Network

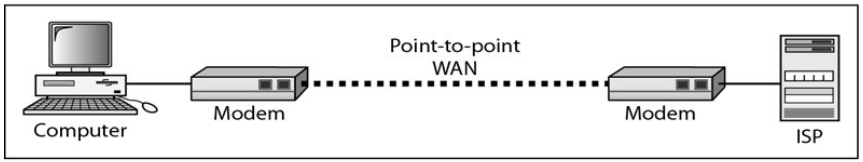
Wide Area Network and Switching

WAN

- A wide area network (WAN) provides long-distance transmission of over large geographic areas that may comprise a country, a continent, or even the whole world.
  - A WAN can be as complex as the backbones that connect the Internet (switched WAN)
  - Or as simple as a dial-up line that connects a home computer to the Internet (point-to-point WAN).



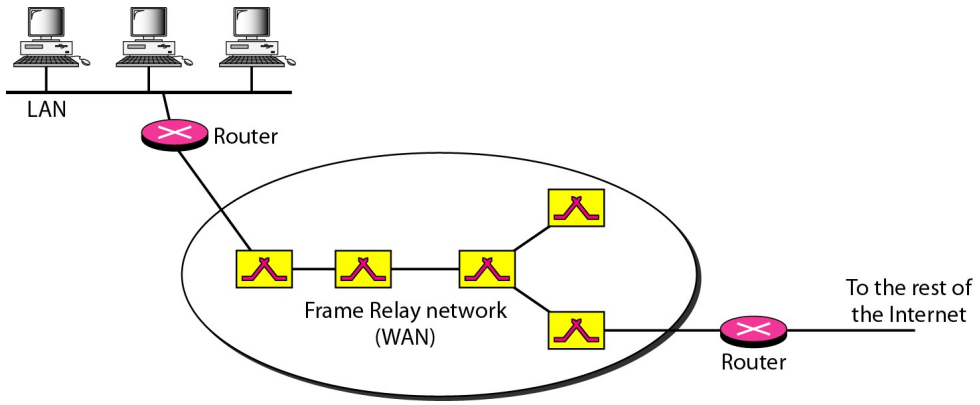
a. Switched WAN



b. Point-to-point WAN

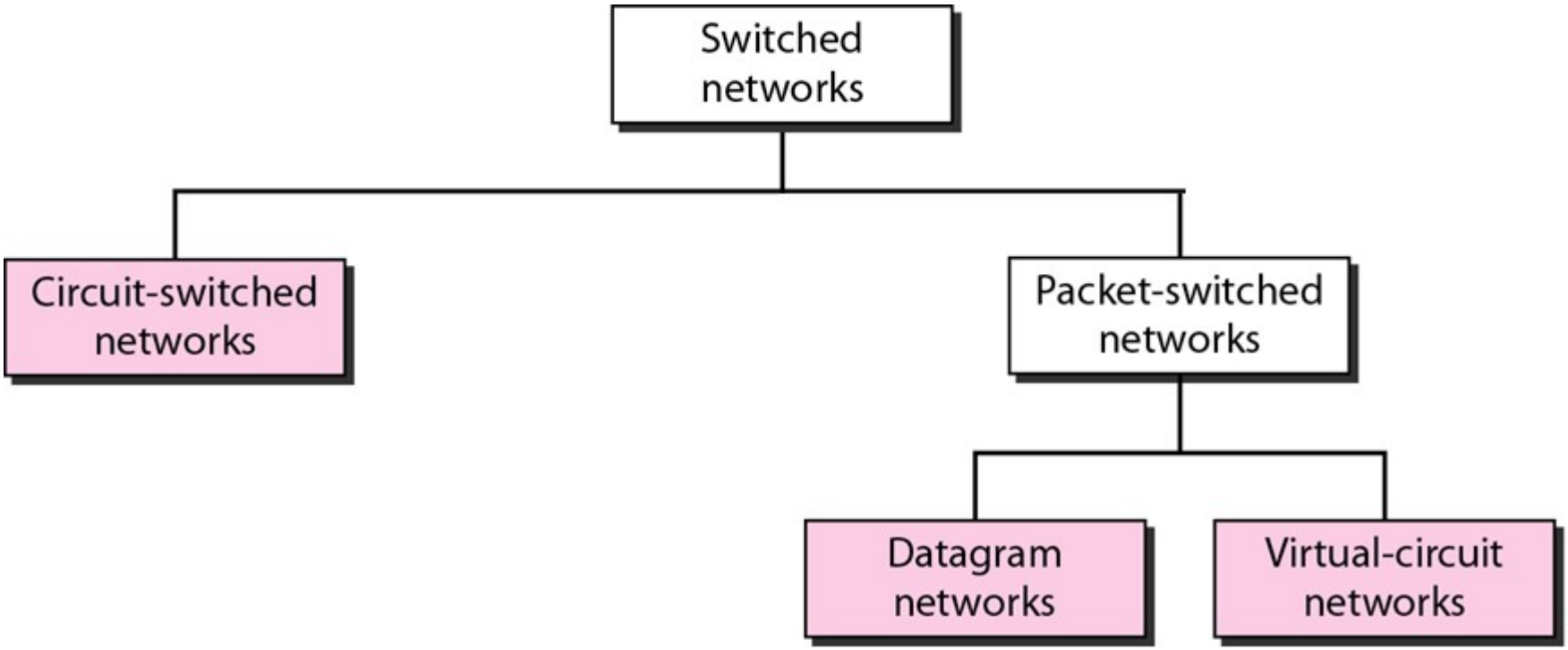
Switched WAN

- Network spread over large geographic area
  - All nodes in WAN may not be directly connected to each other
  - Some redundant connections (multiple paths) desirable for reliability
- Communication network: collections of nodes and connections
- Nodes of two types
  - End devices
  - Switching nodes



- Data sent by source node is switched from node to node until it reaches destination node

Switching Methods



Circuit Switching

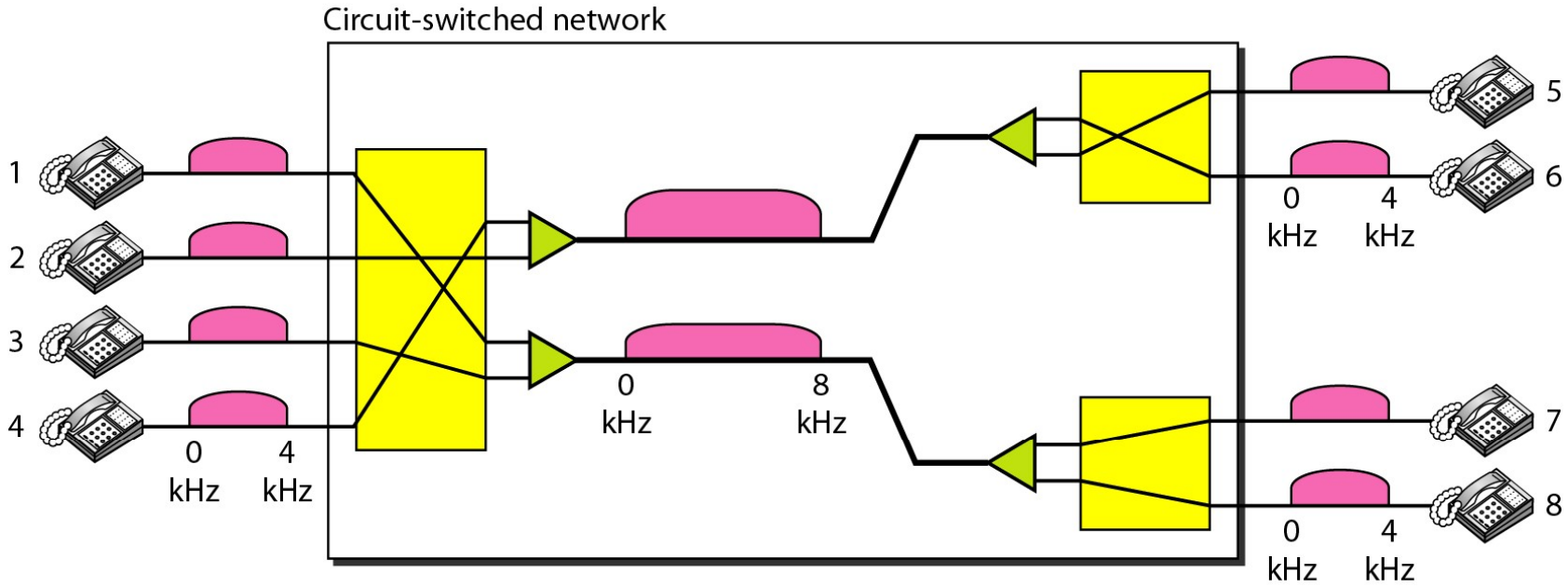
- Before sending data, a dedicated communication path (circuit) set up between source node & destination node, using intermediate nodes
- Three phases
  - Establish: signaling to set up the path
  - Transfer: transfer data through the path
  - Disconnect: signaling to tear down connection
- Links in the path dedicated to a single connection
- All data sent from source follows the same path to the destination

Circuit Switching (contd.)

- Advantages
  - Once connected, data transfer is fast
  - Usually in-order reception of data at receiver

- Disadvantages
  - Inefficient: Channel capacity dedicated for duration of connection, if no data transmitted, capacity wasted
  - Setting up connection takes time (high overhead if only small amount of data to send)
  - Failure of any intermediate node breaks connection
  - Less flexibility: if one node slows down, entire circuit slows down

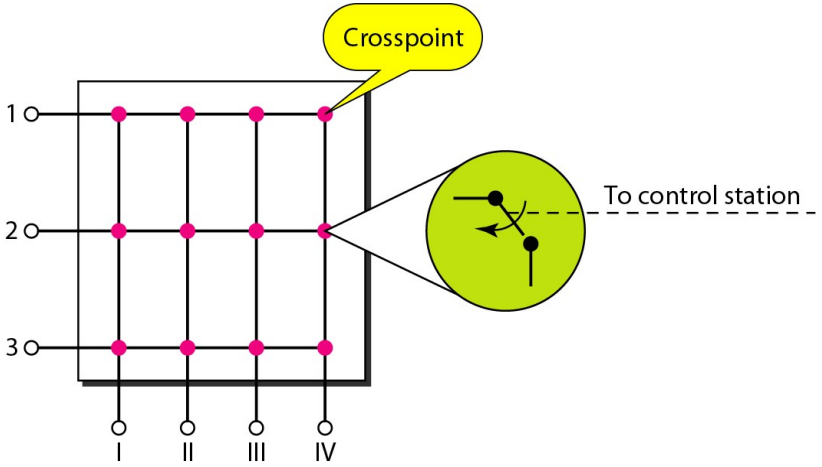
An example of Circuit-switched network



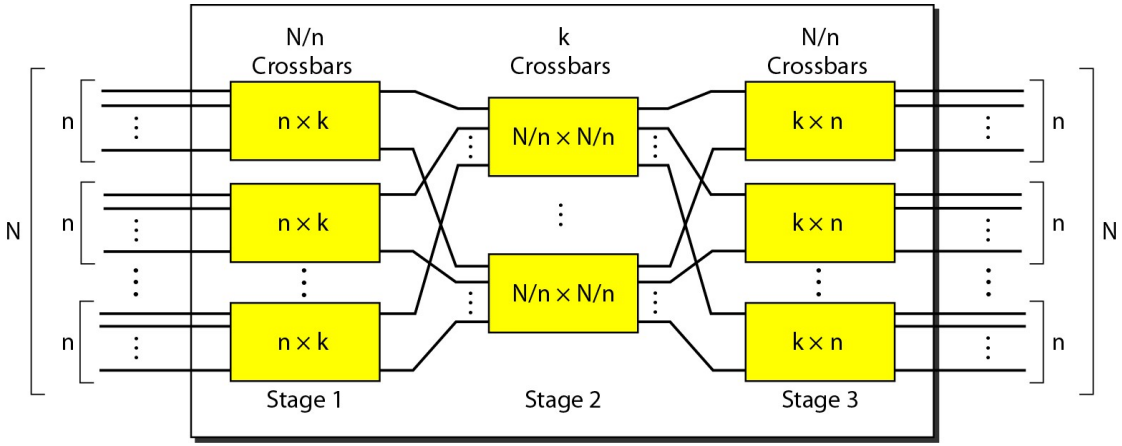
Here assumed that each link uses FDM to connect maximum two voice channels. Bandwidth of each link is then 8KHz.

- Switching at the physical layer in the traditional telephone network uses the circuit-switching approach.

Switches in circuit-switched network

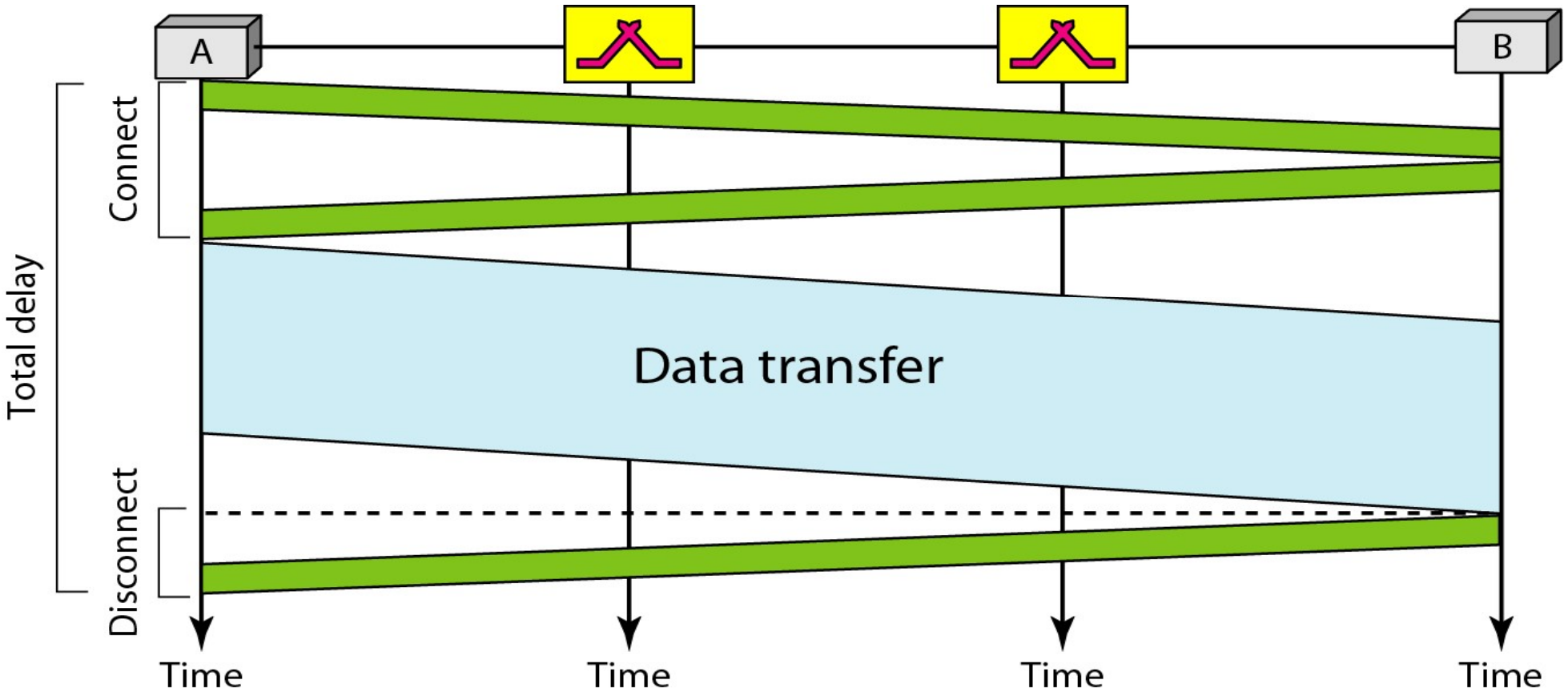


Crossbar switch with three inputs and four outputs



Multistage switch

Delay in a circuit-switched network



Packet Switching

- In a packet-switched network, there is no resource reservation; resources are allocated on demand
- Data transmitted in short units called packets
  - Maximum packet size is pre-defined
  - Longer messages split into sequence of packets
  - Each packet contains a portion of user data plus some control information (address, error check info, sequence info, …)
- Intermediate nodes receive packets, store briefly (buffer) and pass on to next node – Store and Forward
- Packet switching handled in two ways
  - Datagram approach
  - Virtual circuit approach

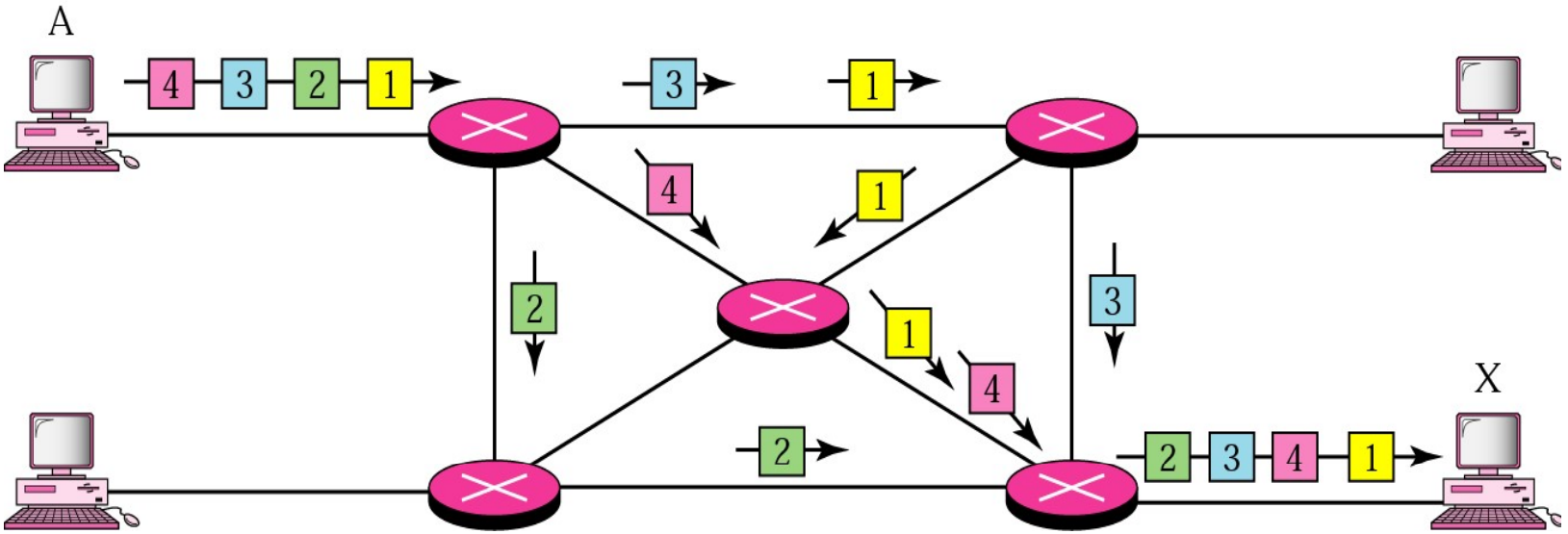
Advantages of packet switching

- Line efficiency
  - Single node to node link can be shared by many packets over time
  - Packets queued and transmitted as fast as possible
- Data rate conversion
  - Nodes buffer data if required to equalize rates
- Packets are accepted even when network is busy
  - Delivery may slow down
- Priorities can be used

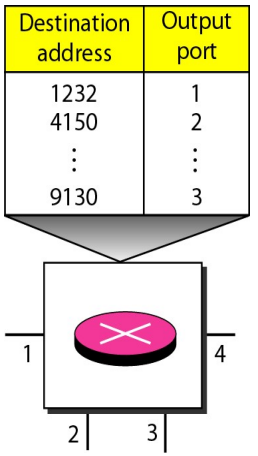
Datagram approach

- Each packet treated independently of any other packet (each packet has destination address)
- Packets sent by a source node can take different routes to the same destination
- Packets may arrive out of order at destination node, may be lost
  - Up to destination node to re-order packets and recover from missing packets

Datagram Approach

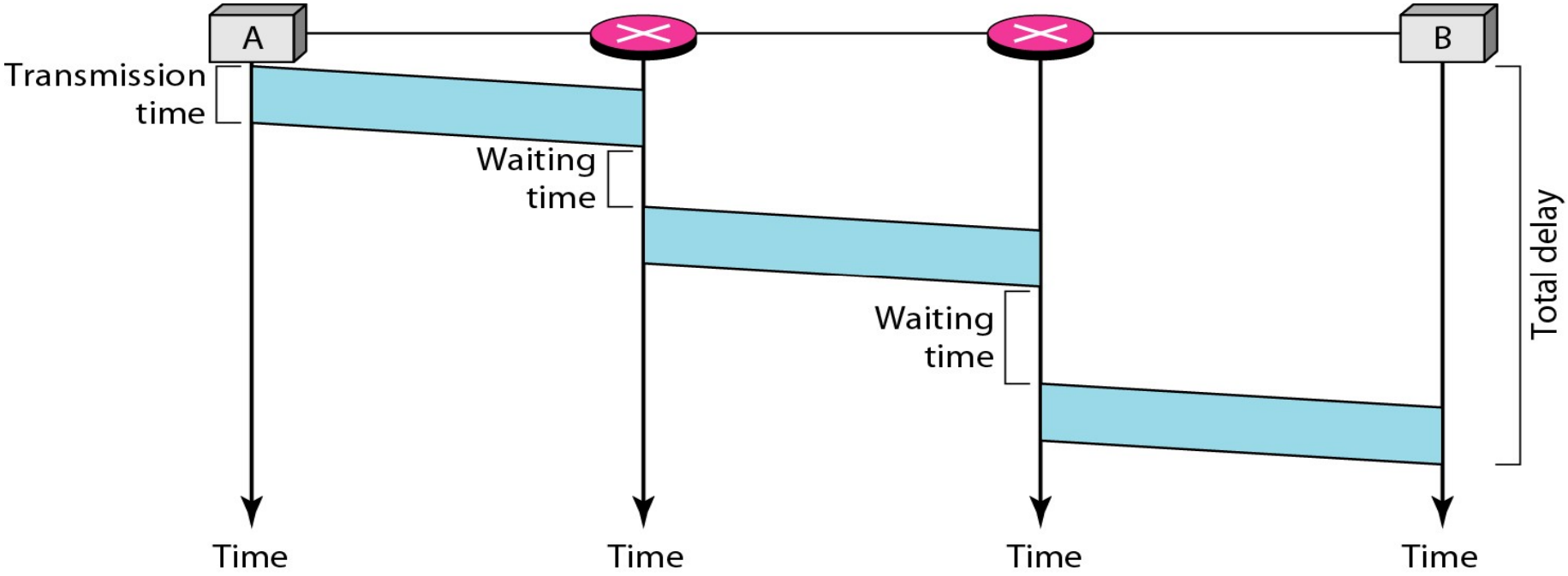


- **A switch in a datagram network uses a routing table that is based on the destination address.**
  - **The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet (*recall IP address*)**



- **Switching in the Internet is done by using the datagram approach to packet switching at the network layer**

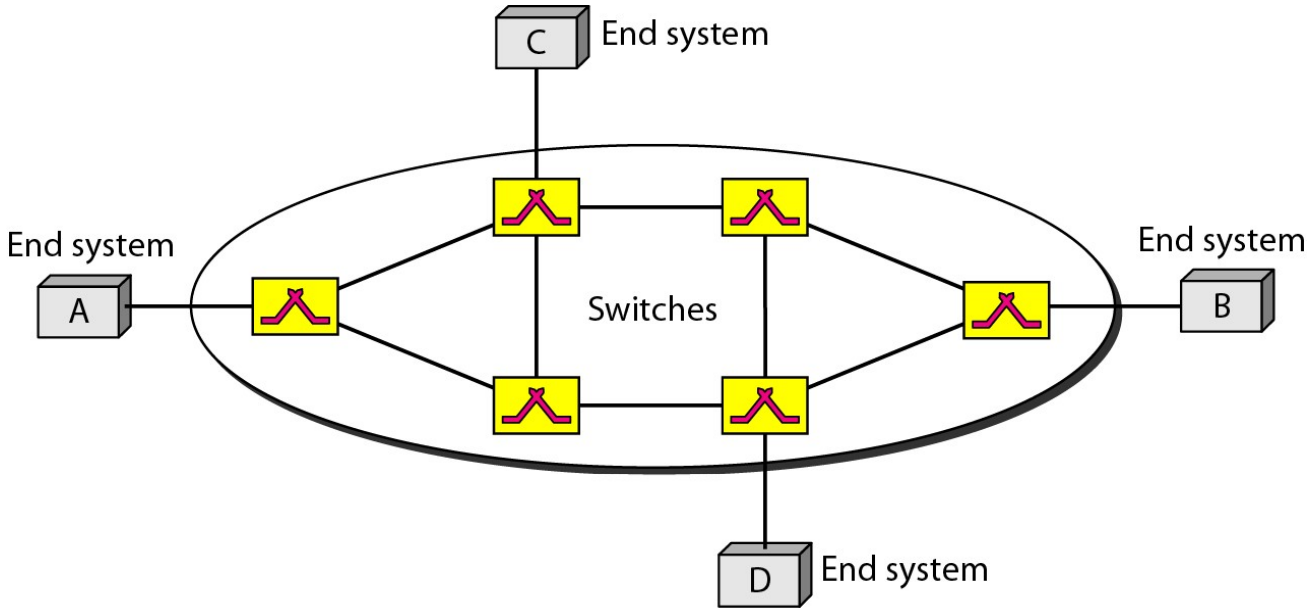
Delay in a datagram network



Virtual-circuit Approach

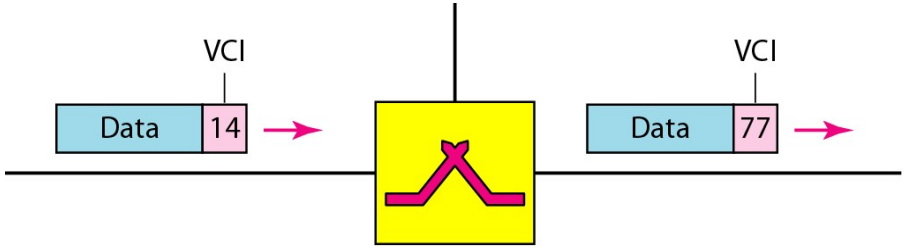
- A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.
- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand as in a datagram network.
- As in a datagram network, data are packetized and each packet carries an address in the header. However this address has only local scope (not end to end scope).
- As in a circuit-switched network, all packets follow the same path established during the connection.
- A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer (in general).

Virtual-circuit network



- Switching at the data link layer in a switched WAN is normally implemented by using virtual-circuit techniques like X.25, Frame Relay, ATM.
- A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

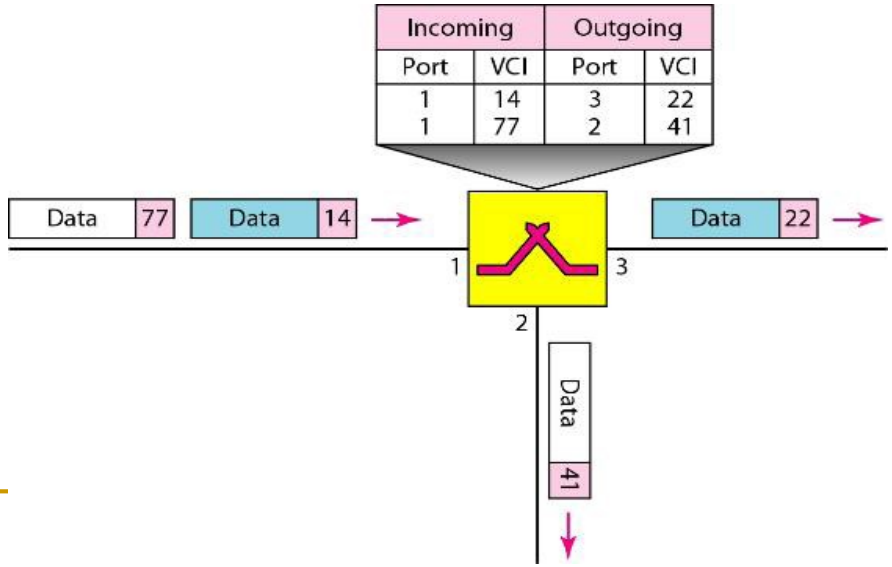
Virtual Circuit Addressing



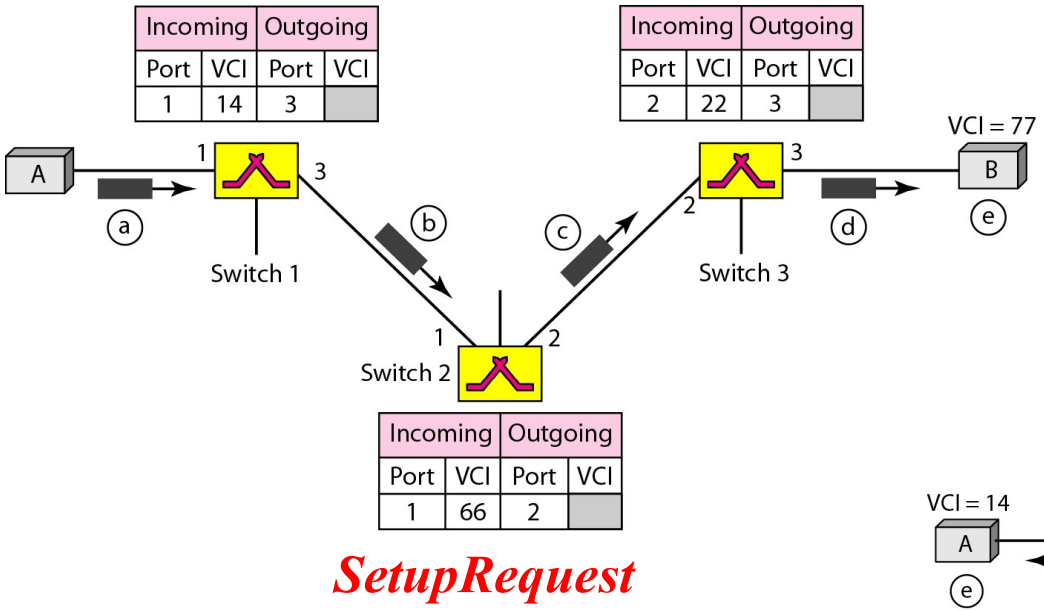
- In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).
- *Global Addressing :* A source or a destination needs to have a global address-an address that can be unique in the scope of the network. However, a global address in virtual-circuit networks is used only to create a virtual-circuit identifier (discussed next).
- *Virtual-Circuit Identifier (VCI) :* This is actually used for data transfer. Unlike a global address, it has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.

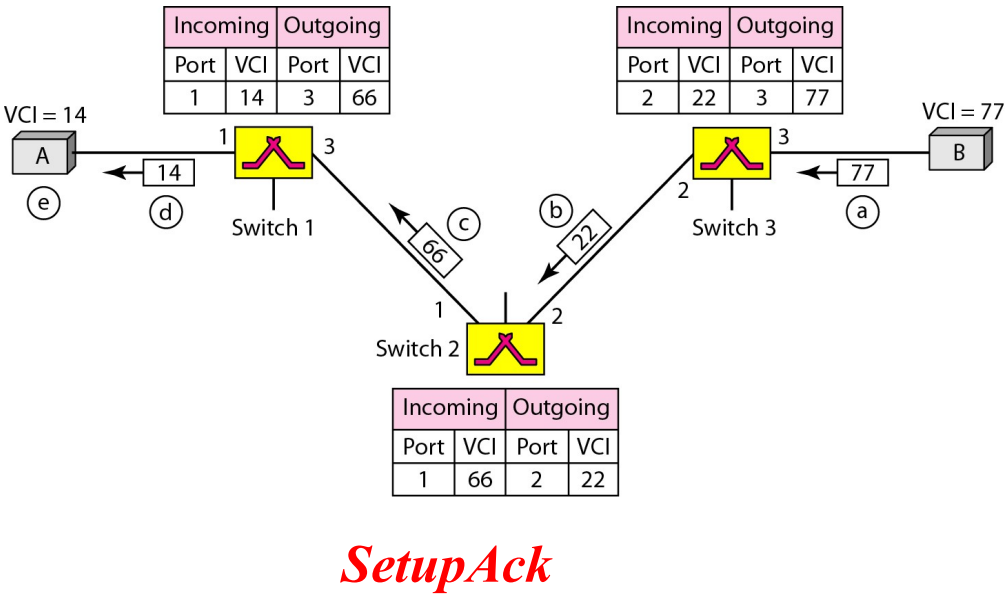
Virtual Circuit Technique

- Three phases of operations : Establish circuit, Data transfer, and Teardown circuit.
- Pre-planned route or 'circuit' established between source & destination before any data packets sent
- Each node maintains information about each virtual circuit passing through itself, in a table
- Each packet contains a Virtual Circuit Identifier (VCI) instead of destination address
- The links in a path are NOT dedicated – may be shared among different virtual circuits

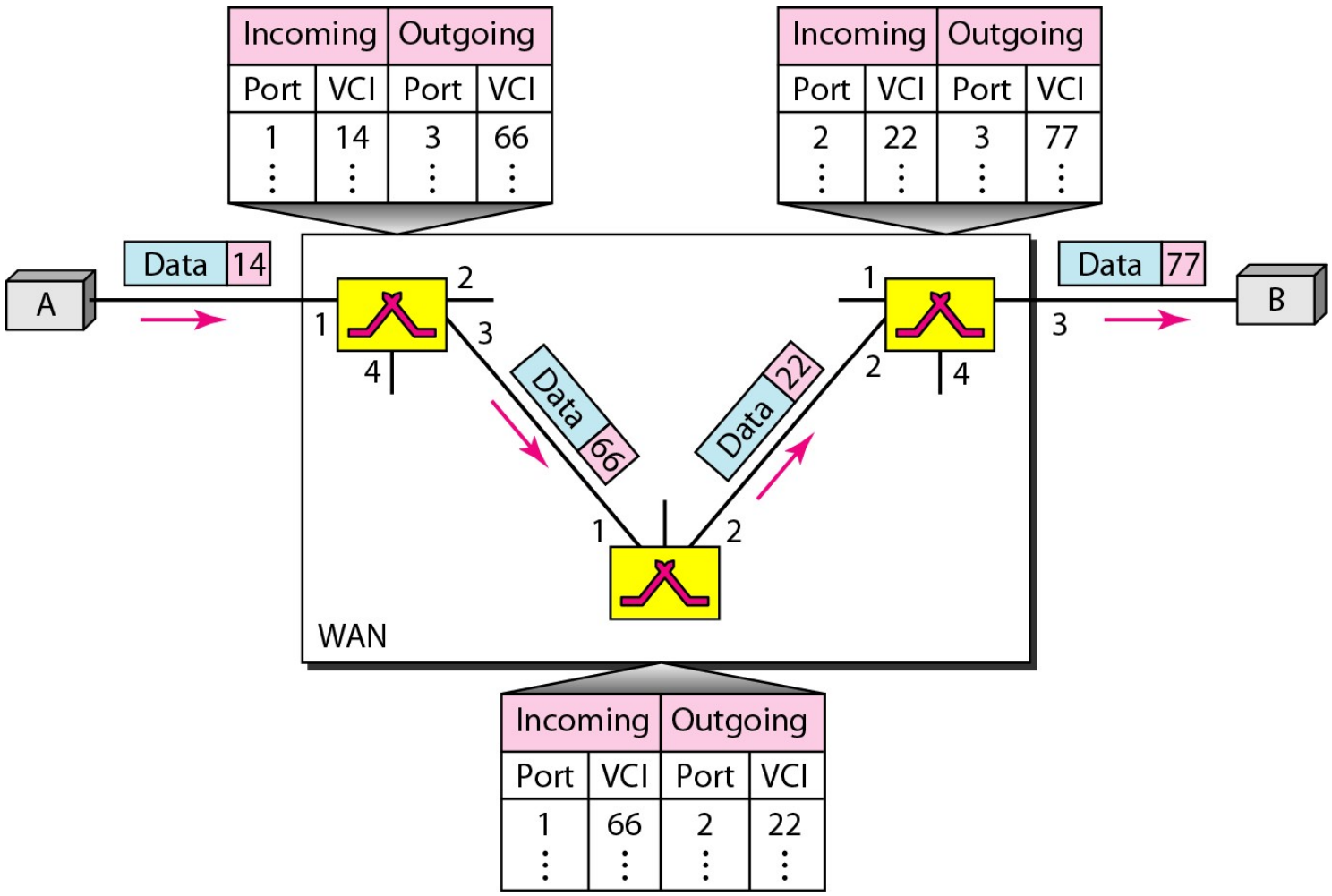


Setup Circuit Phase





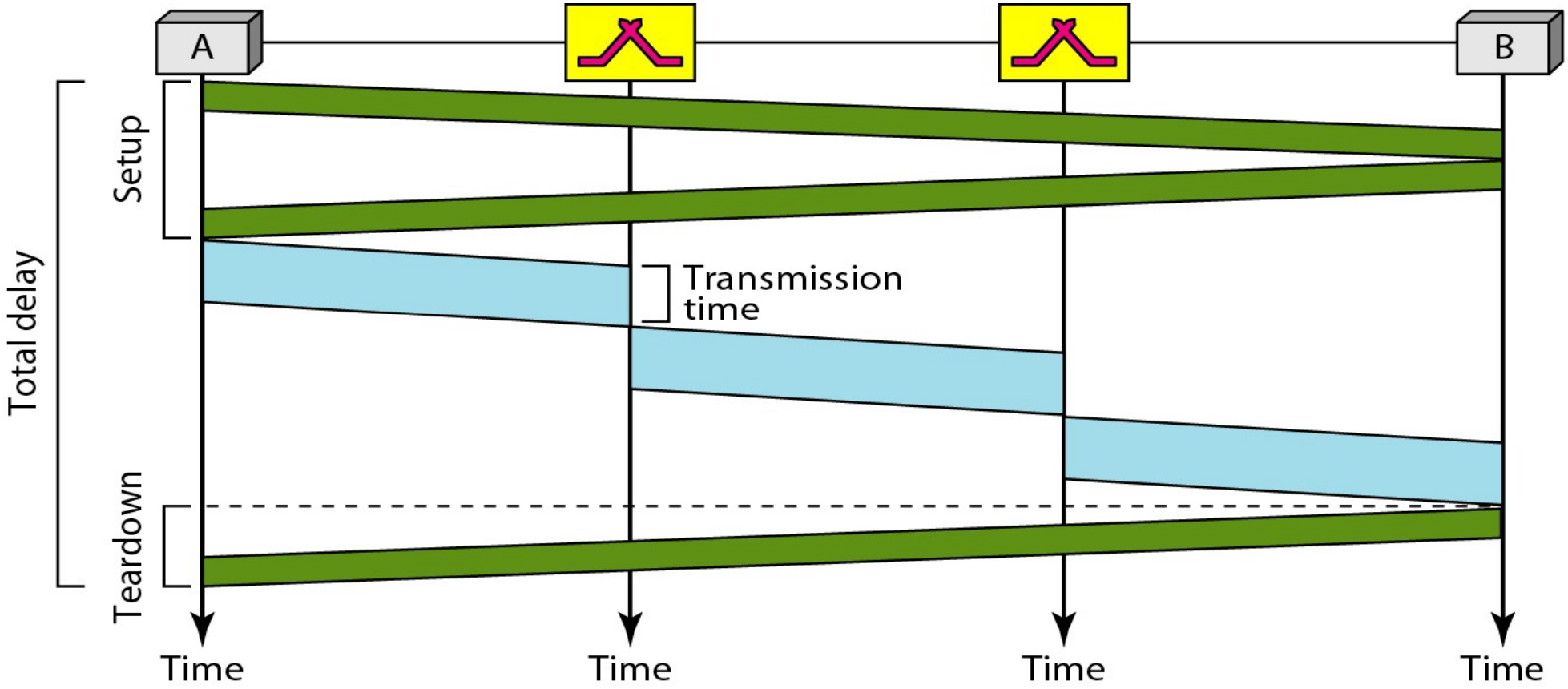
Data Transfer Phase



Teardown Circuit Phase

- In this phase, source A, after sending all frames to B, sends a special frame called a *TeardownRequest*.
- Destination B responds with a *TeardownConfirmation* frame.
- All switches delete the corresponding entry from their tables.

Delay in a virtual-circuit network



Example of Virtual Circuit Networks

- **X.25** is an ITU-T standard protocol suite for packet-switched data communication in a wide-area network designed in the 1970s. It performed switching at the network layer. It has a low 64-kbps data rate.

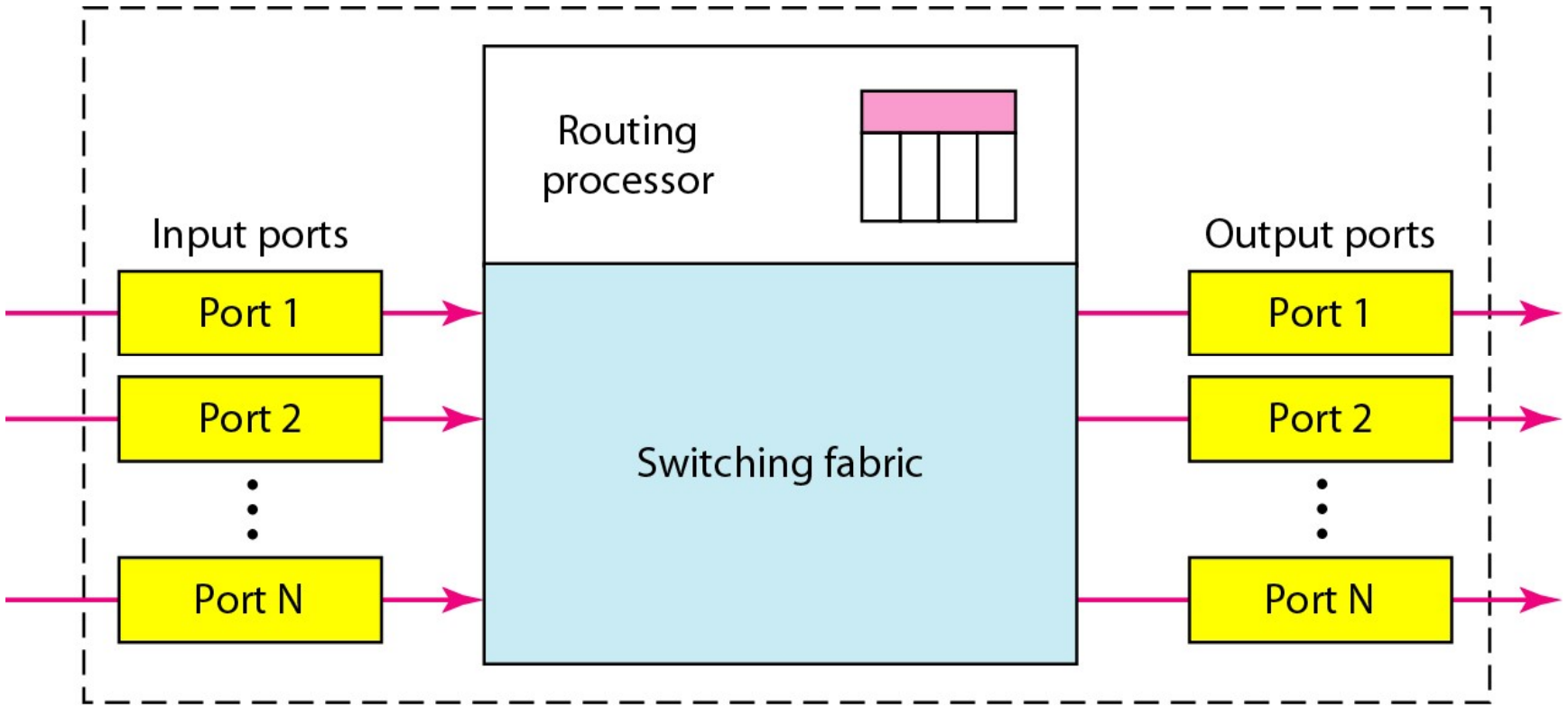
- **Frame Relay** is a virtual-circuit wide-area network that was designed in response to demands for a new type of WAN in the late 1980s and early 1990s. It operates at a higher speed (1.544 Mbps and recently 44.376 Mbps).

- **Asynchronous Transfer Mode (ATM)** is the cell relay protocol designed by the ATM Forum and adopted by the ITU-T. The combination of ATM and SONET will allow high-speed interconnection of all the world's networks.

Virtual Circuit vs Datagram

- Virtual circuit
  - Network can provide sequencing and error control
  - Packets are forwarded more quickly
  - Less reliable: loss of a node disconnects all circuits through that node
- Datagram
  - No call setup phase, better if few packets to be sent
  - More flexible
    - ✓ Routing can be used to avoid congested parts of the network
    - ✓ Communication can go on even if any node fails
  - Packets may arrive out-of-order at destination

Switches in packet-switched network



References

- *Data Communications & Networking, 5th Edition, Behrouz A. Forouzan*
- *Computer Networks, Andrew S. Tanenbaum and David J. Wetherall*
- *Wikipedia*