AY 2019/2020
EE6403 Distributed Multimedia Systems

Part 4 Media Transmission and Delivery, Quality of Service (QoS)

Dr Yap Kim Hui

Room: S2-B2b-53
Tel: 6790 4339
Email: ekhyap@ntu.edu.sg

References

- Douglas Comer, Computer Networks and Internets (6th ed.), Pearson
- William Stallings, Data and Computer Communications (10th ed.), Pearson
- James F. Kurose and Keith W. Ross, Networking: A Top-Down Approach (6th ed.), Pearson
- Forouzan, Data Communications and Networking, 4th edition, Pearson

Section IV
Media Transmission and Delivery

This Section

- Part 1: Introduction
- Part 2: Physical Layer & Media
- Part 3: Data Link Layer & Technologies
- Part 4: Network Layer & Technologies
- Part 5: Transport Layer & Technologies

Part 1: Introduction

Data Communications Overview

Data Communications Model

source info.

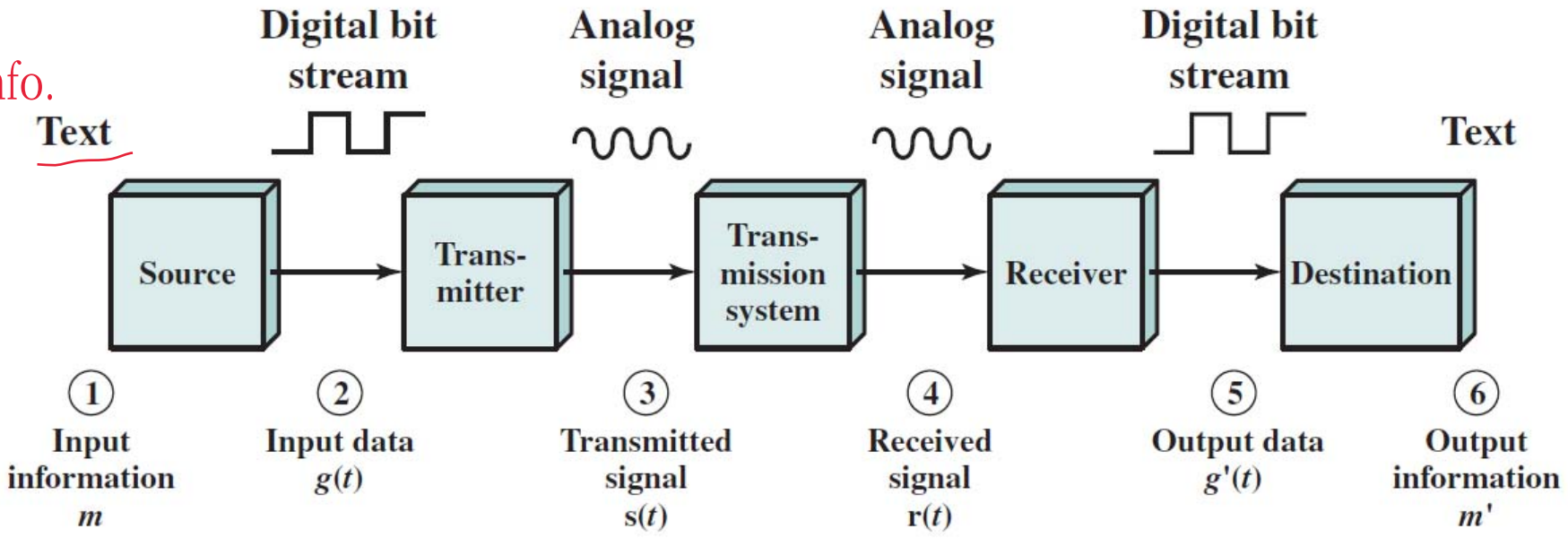
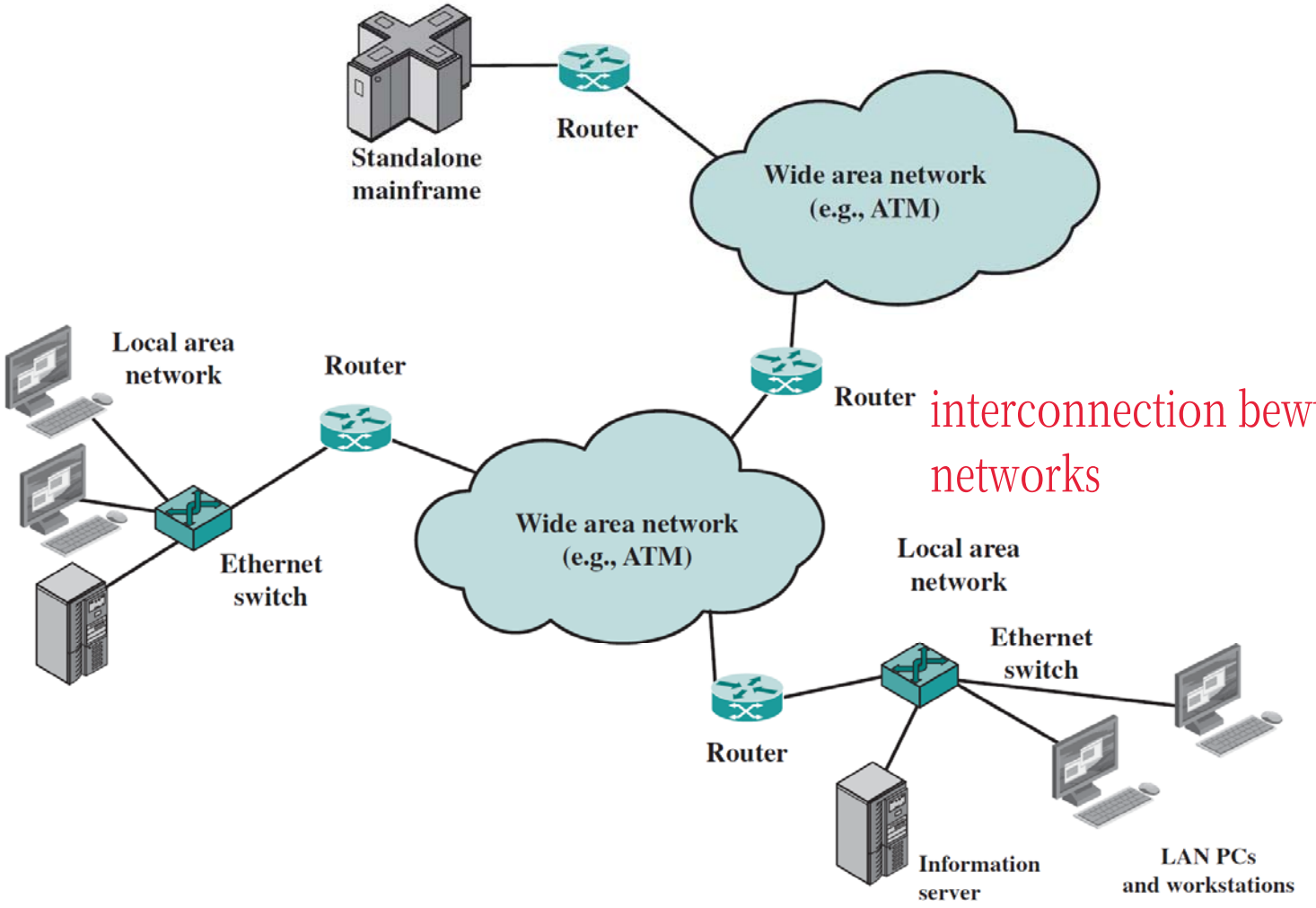


Figure 1.4 Simplified Data Communications Model

Key Element in the Internet



interconnection bewteen 2 diffrent networks

Figure 1.5 Key Elements of the Internet

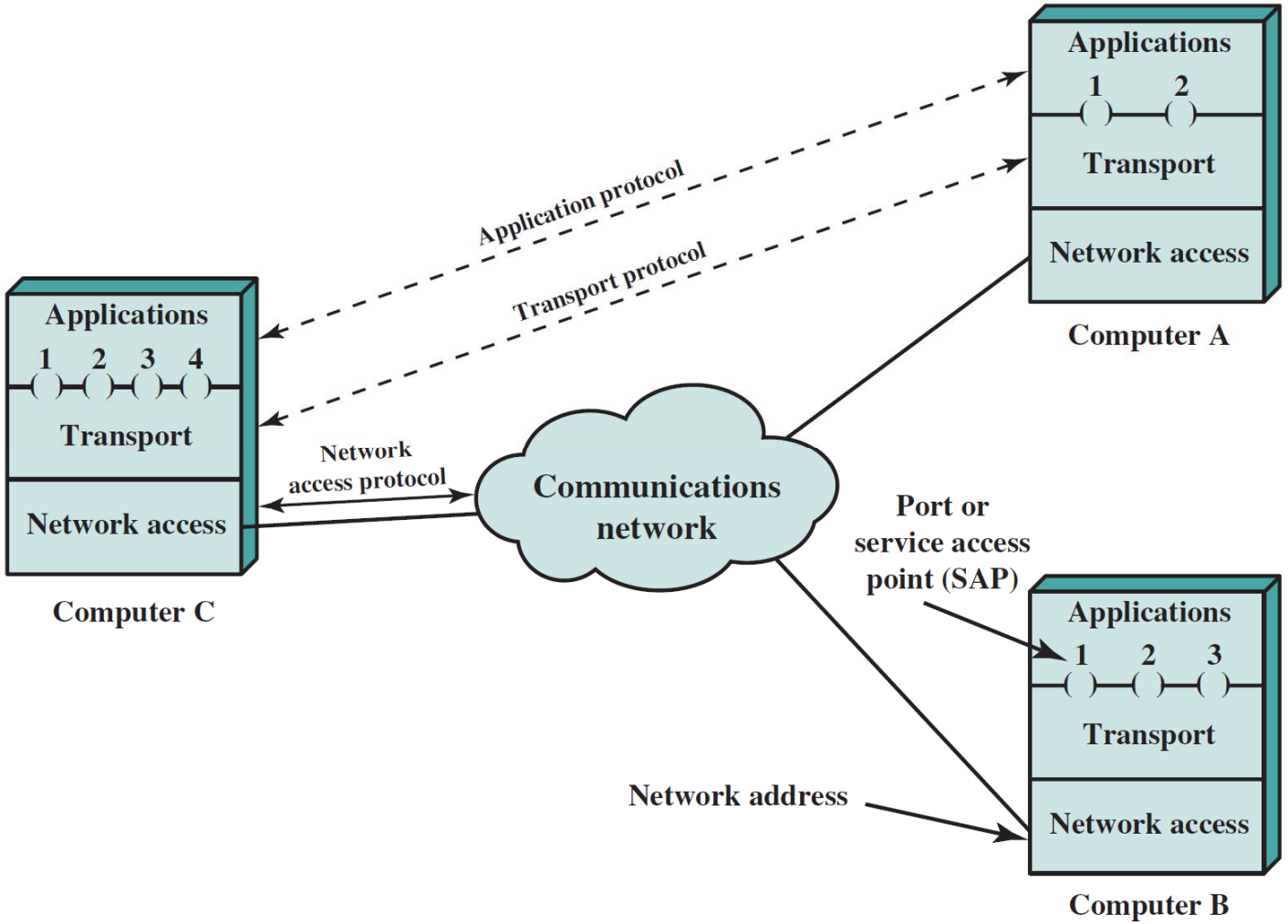
Protocols and Standards

- Why standardize and use protocols?
- Who standardize?

Protocol

- Each protocol specifies how to handle one aspect of communication
- A protocol can specify
  - Low-level details such as voltage and frequency
  - High-level details such as format visible to a user
- Many individual communication protocol standards exist
- Set of protocols designed to work together is known as a suite
  - Example: TCP/ IP Internet protocol suite

Protocol Architectures and Networks



Reference Models & Layers

Protocol Layering

means have different layer in protocol

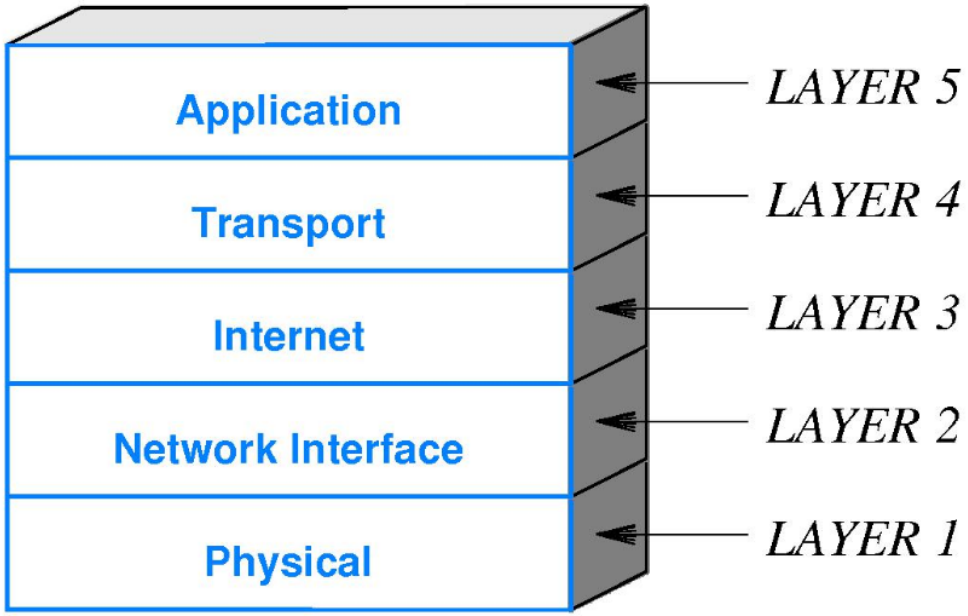
- Needed because communication is complex so need divide and conquer
- Intended primarily for protocol designers
- Divides communication into intellectually manageable pieces
- Provides a conceptual framework that can help us understand protocols
- Notes:
  - Layering gives a guideline, not a rigid framework
  - Optimizations may violate strict layering

Reference Models

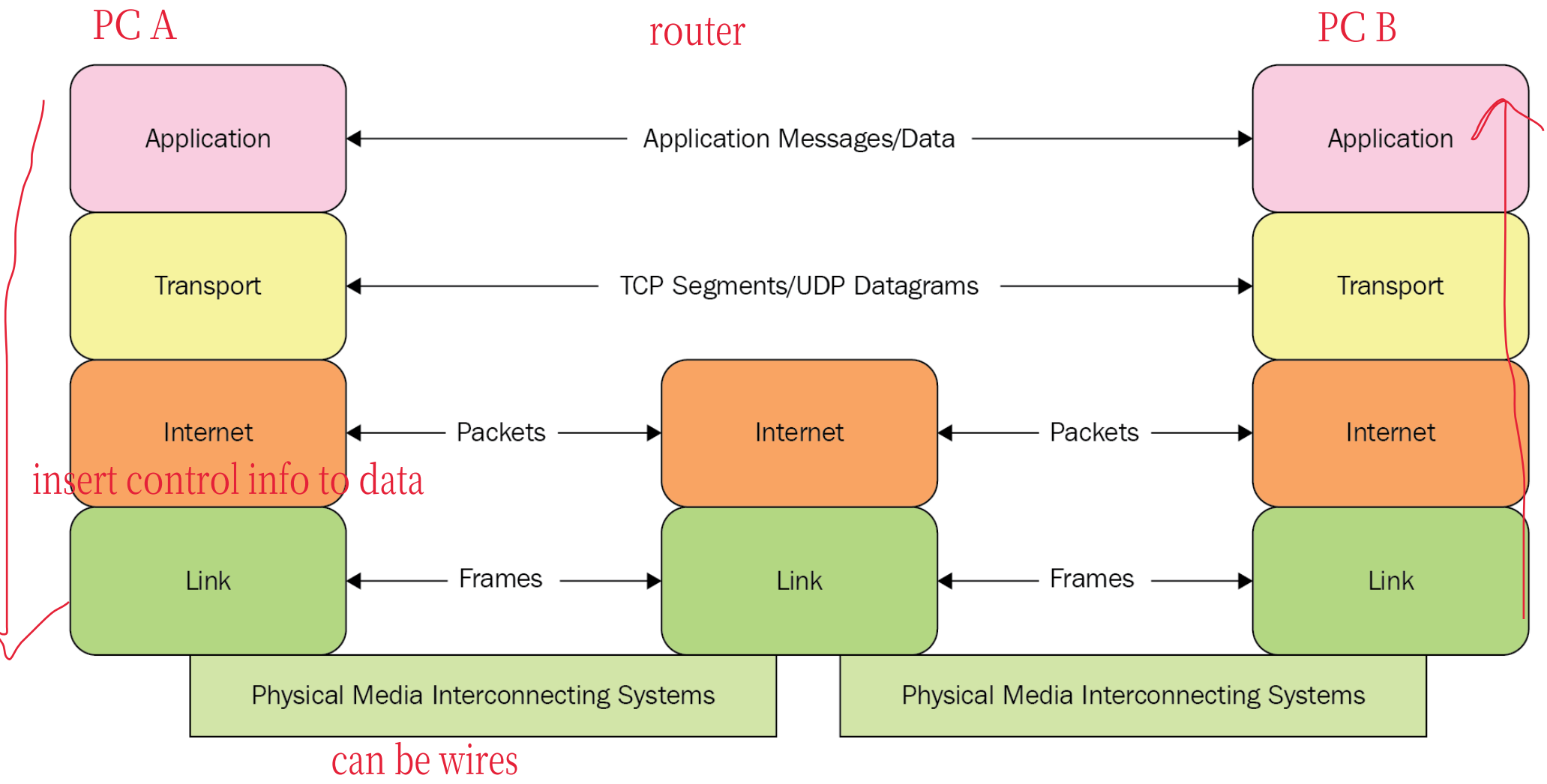
- 5-layer TCP/IP reference model
- 7-layer Open Systems Interconnection (OSI) reference model defined by ISO and ITU

TCP/IP Reference Model

- Descriptive model after TCP/IP protocols were devised
- Used in practice



TCP/IP Protocols



Source: packtpub.com

Physical Layer botom layer

contain:

- Underlying transmission media
- Electromagnetic energy and its use
- Representation of information in signals
- Electrical properties such as radio frequencies and voltage
- Associated hardware

Network Interface/ Network Access/ Data Link Layer

- Communication between a computer and network hardware
- Also called *data link* or *MAC* layer
- Mechanisms for gaining access to shared media
- Hardware Media Access Control (MAC) addressing
- Packet (frame) formats
- Error detection

Internet/Network Layer

- Communication between a pair of computers across the Internet
- Internet packet format (datagram) data format
- Internet addressing model and address assignment
- Forwarding of Internet packets
- Dividing an Internet packet into smaller packets for transmission
- Error detection and reporting

Transport Layer

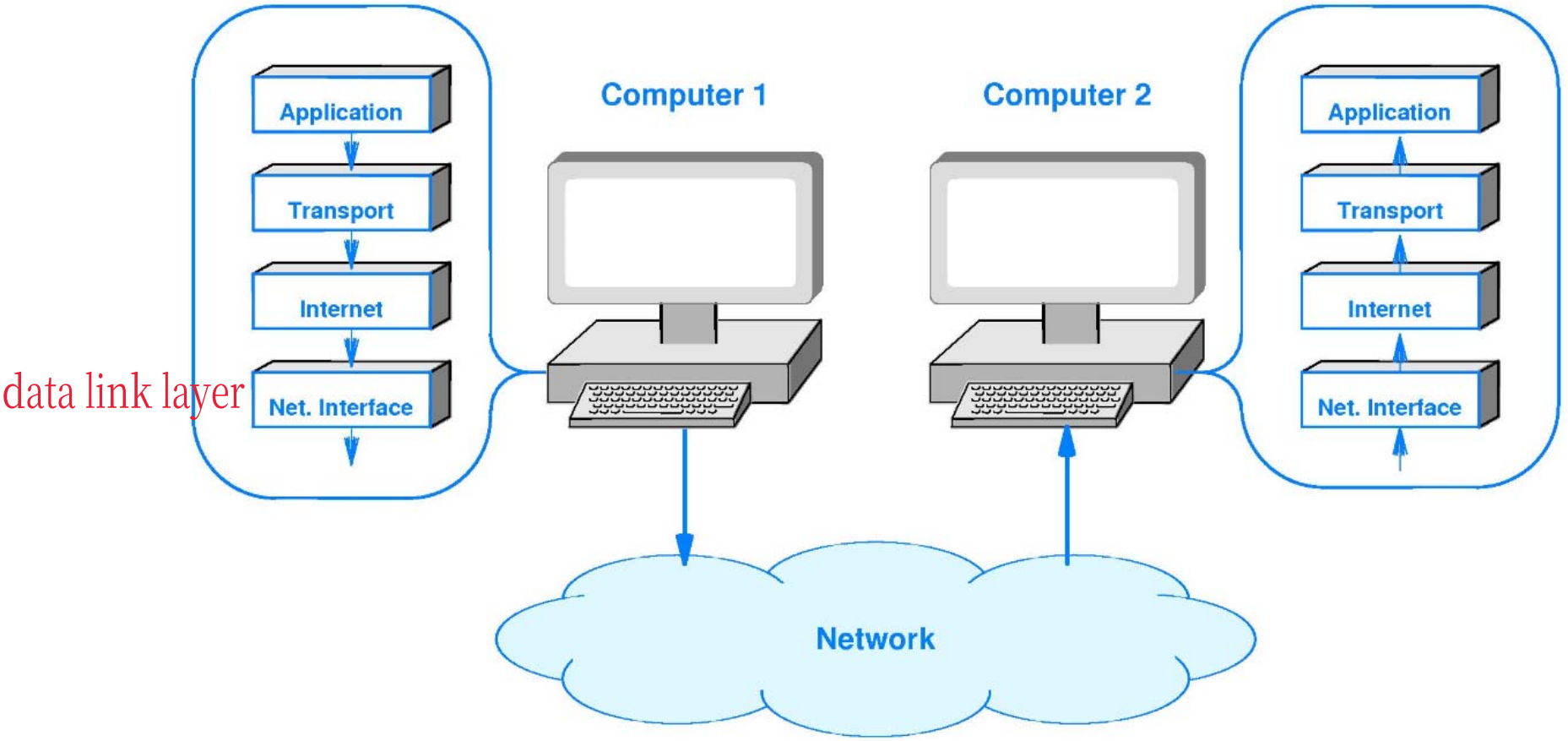
- Communication between a pair of applications
- Reliable delivery and retransmission
- Mechanisms to control data rate and avoid congestion
- Use TCP segment format is segment

Application Layer

- Format and representation of data and messages
- Procedures applications follow to
  - Transfer data
  - Handle errors or unexpected conditions
- Meaning of messages exchanged

Protocol on A Computer

- Protocols on a computer arranged in a conceptual *stack*



data link layer

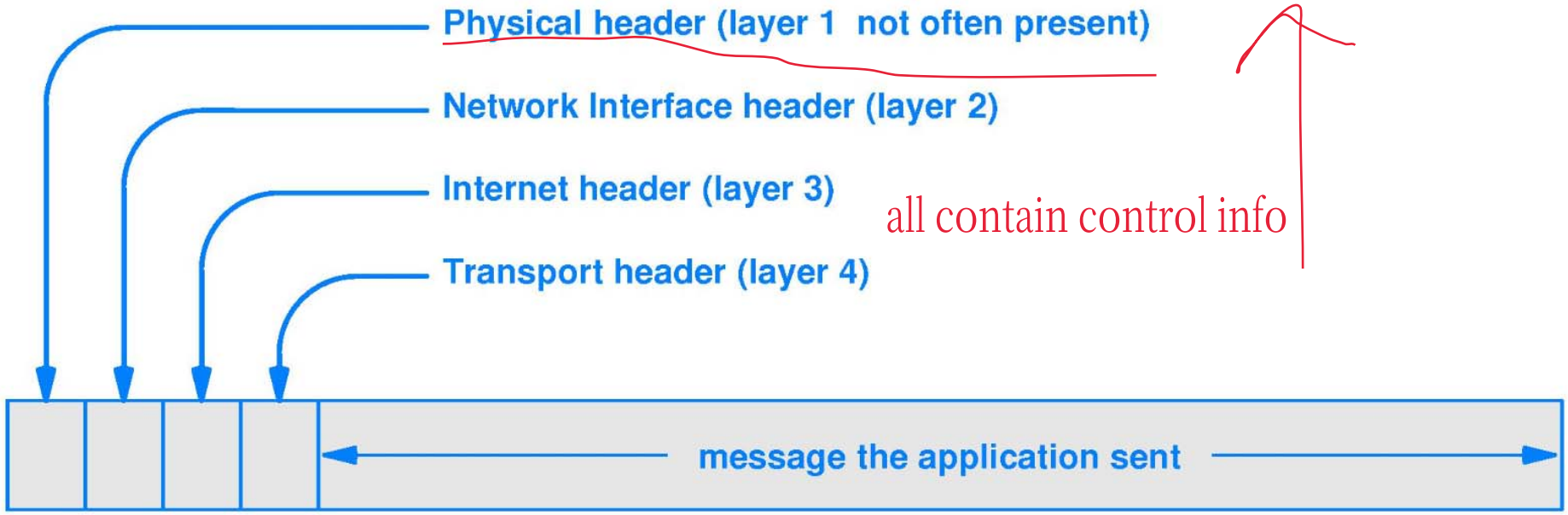
General Idea

- Each computer contains an entire set of layered protocols
- When an application sends a message
  - The message passes down through the layered protocols
  - A given layer adds information and forms a packet
  - The computer transmits the final packet arrive at link layer and ready to transmit
- When a packet arrives
  - The packet passes up through the protocol layers
  - A given layer performs processing and passes the packet up to the next layer
  - The application receives the message that was sent

Packet Headers

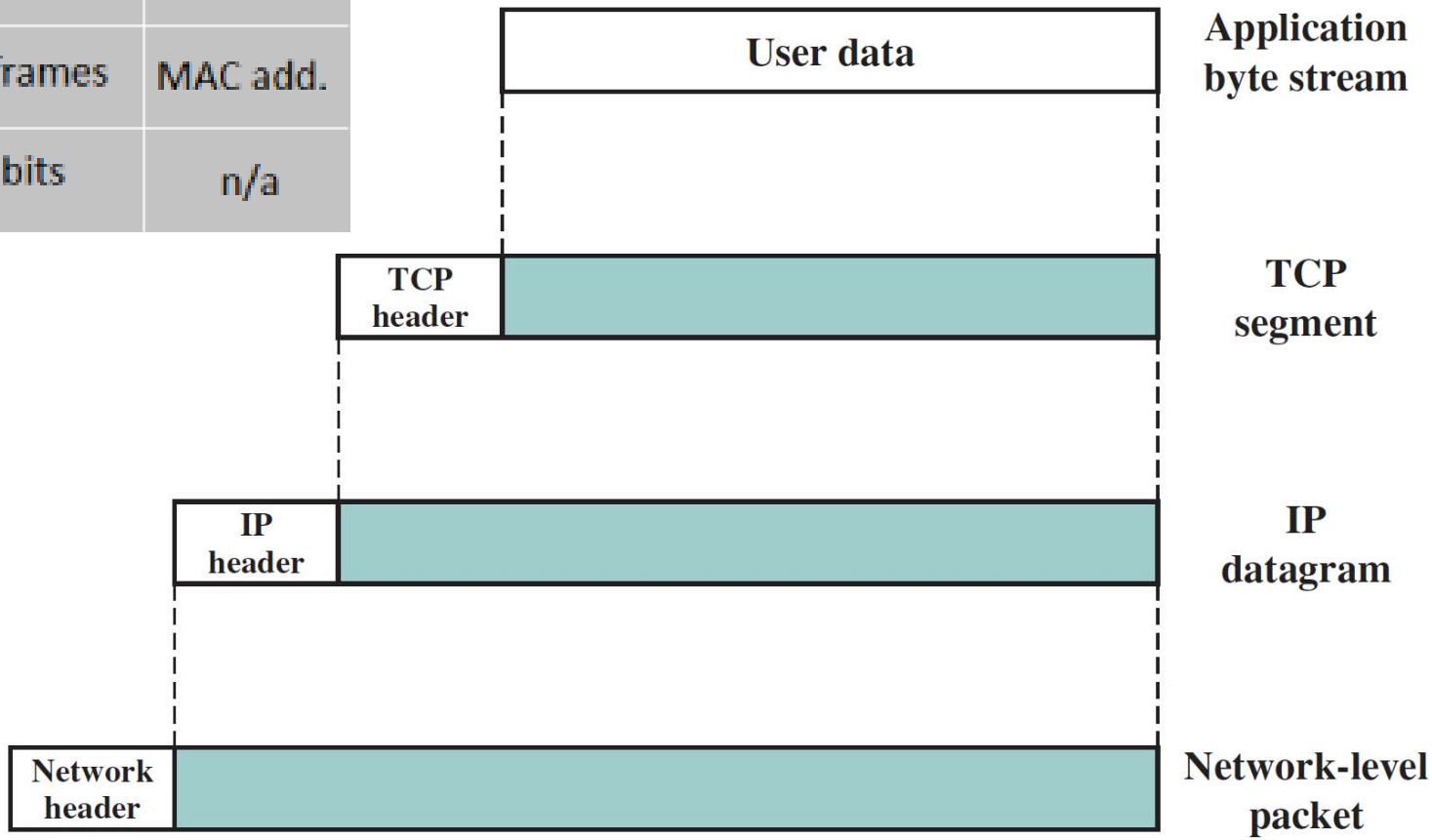
前置

- One header prepended by each layer when message sent
- Result: headers are *nested* with lowest-layer header appearing first

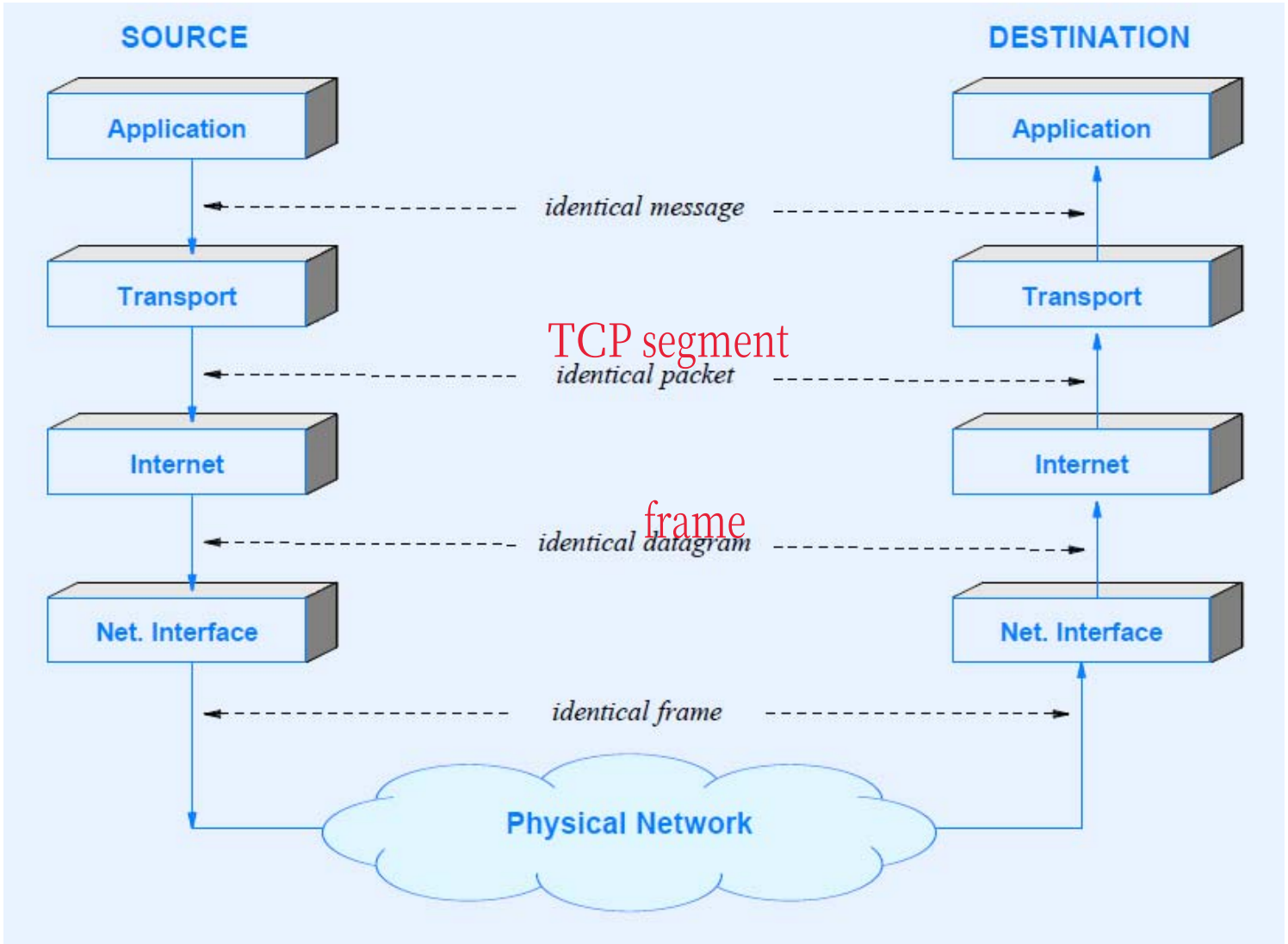


Protocol Data Units (PDUs) in TCP/IP

#	Name	Protocol	Protocol Data Unit	Addressing
5	application	HTTP SMTP, etc	Messages	n/a
4	transport	TCP/UDP	segment	port #'s
3	network	IP	datagram	IP address
2	data link	ethernet wiFi	frames	MAC add.
1	physical	10 base T, 802.11	bits	n/a



Layering Principle



Layering Principle

- Layered protocols enforce an invariant:

  Layer N at the destination receives an exact copy of the message sent by layer N at the source. All headers and other modifications added by lower layers at the source must be removed by lower layers at the destination.

- Allows protocol designer to focus on one layer at a time

Protocol in Simplified Architecture

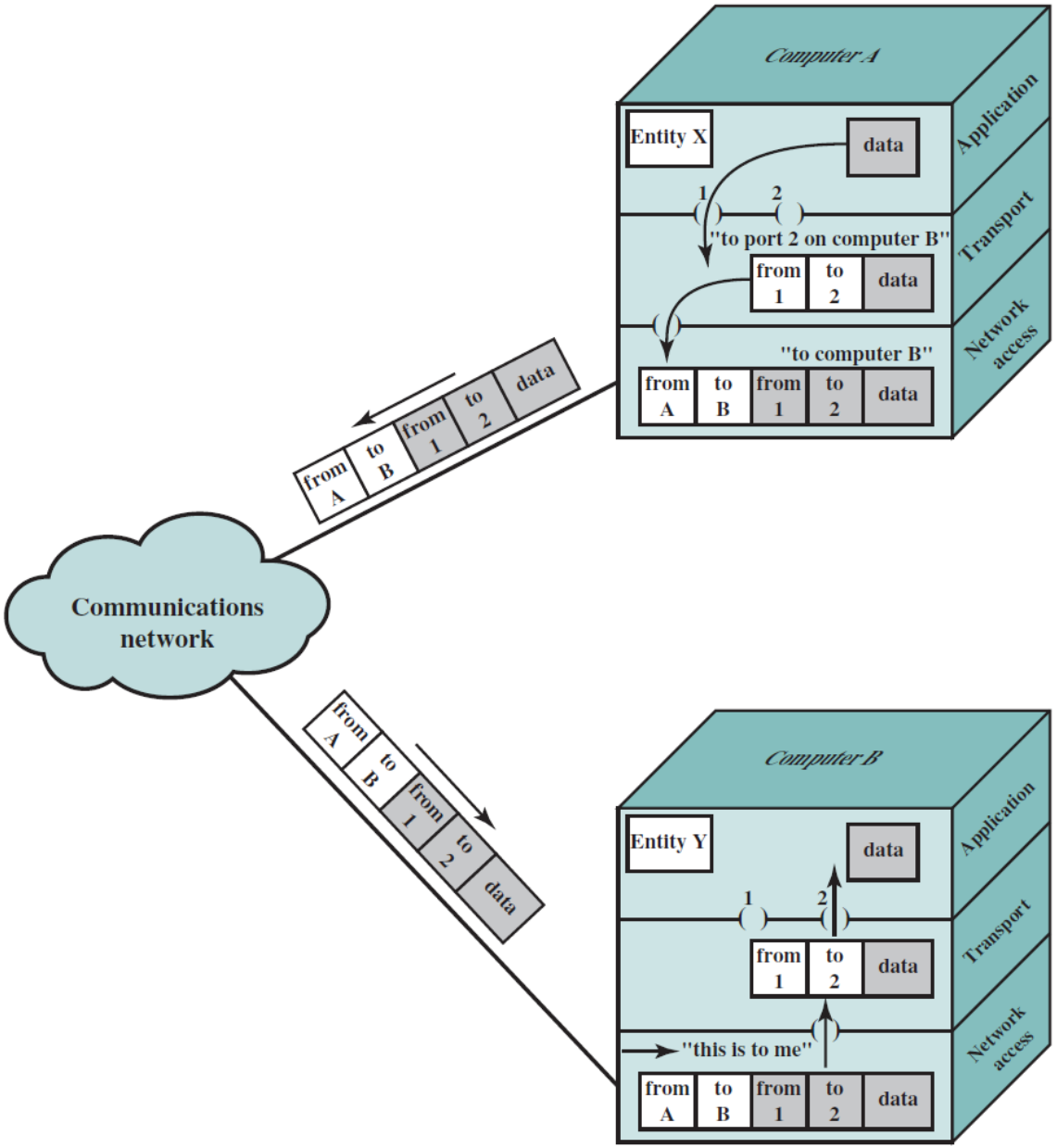
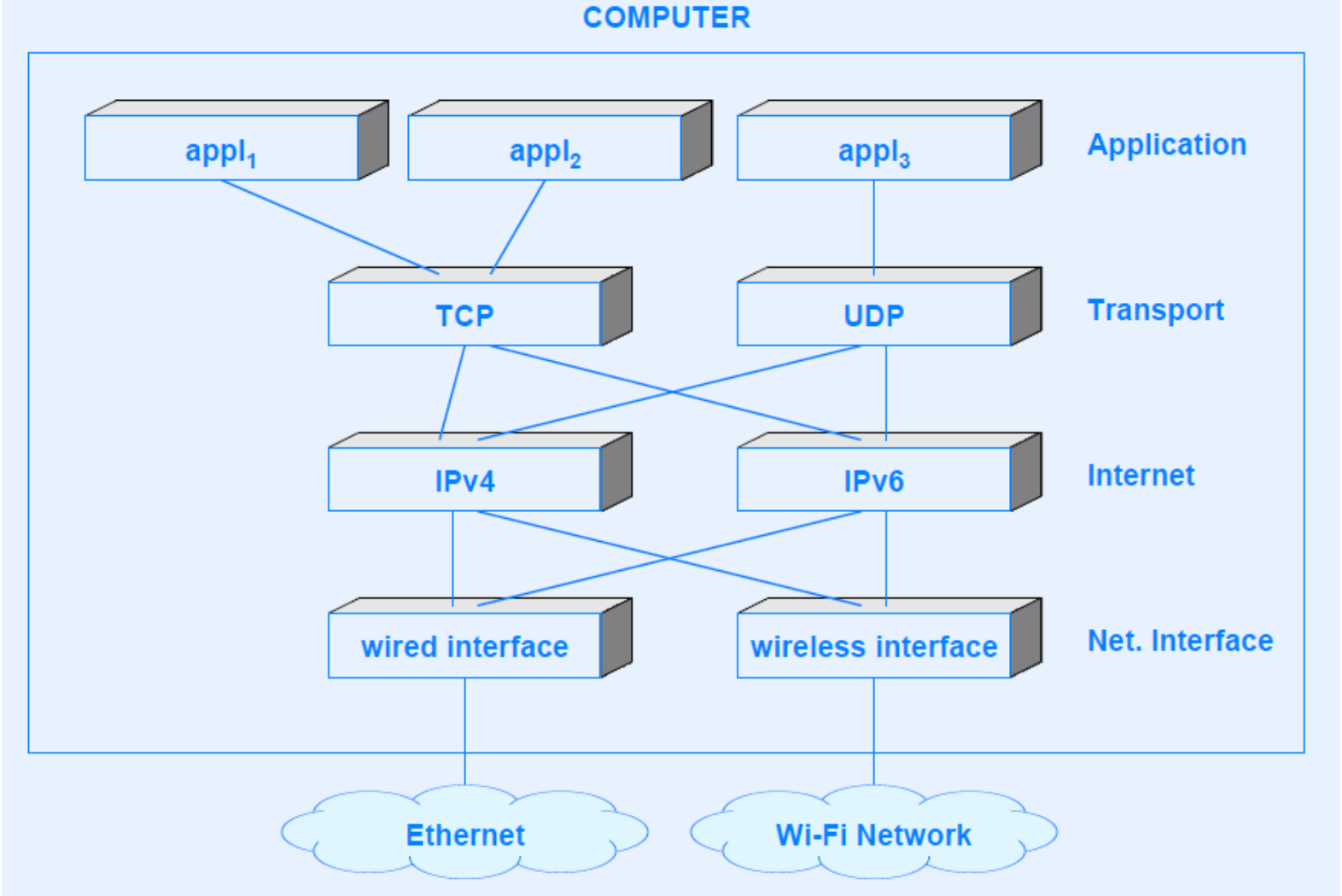


Figure 2.2 Protocols in a Simplified Architecture

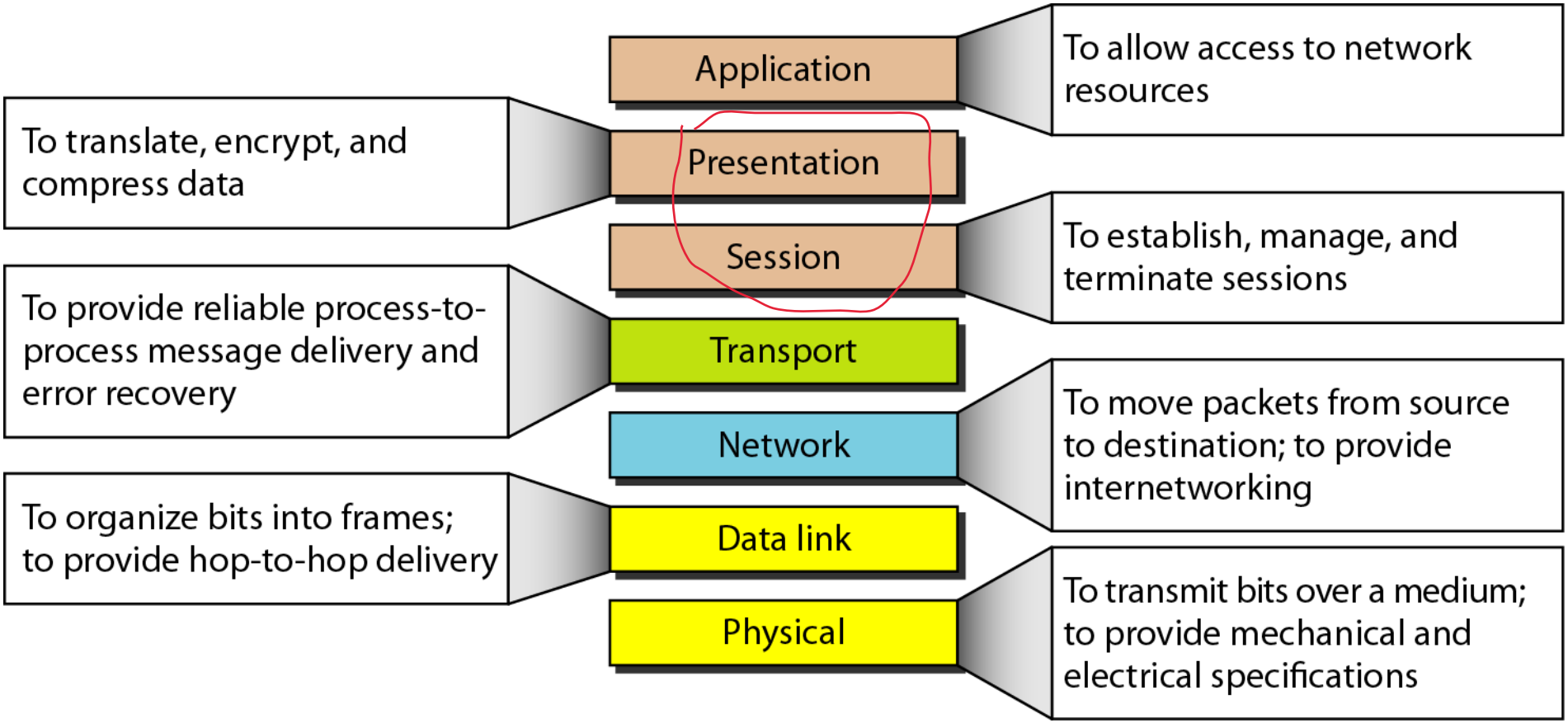
Multiple Protocols At Each Layer



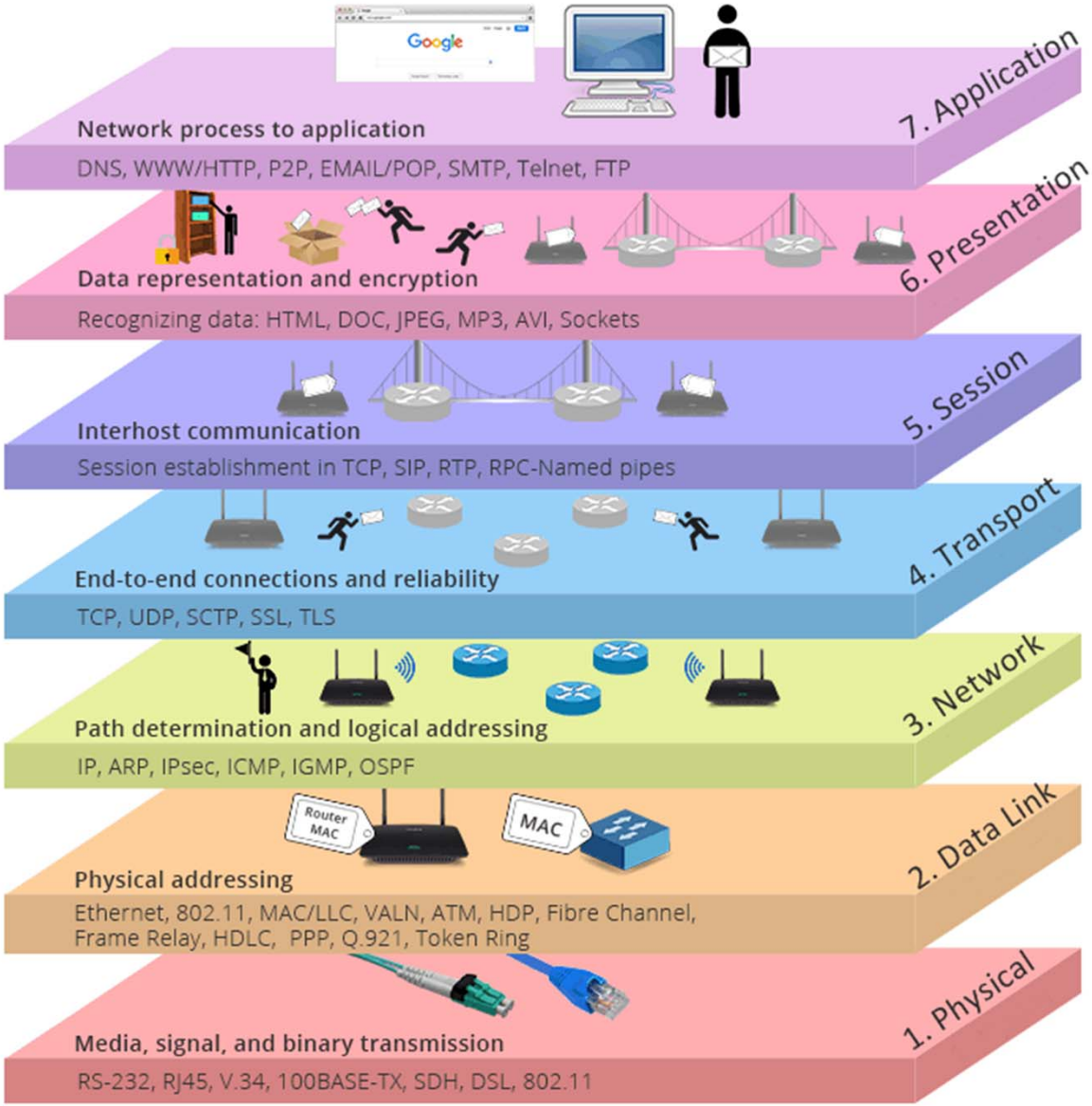
Multiple Protocols Per Layer

- Consider a typical computer
- User can run multiple applications simultaneously
  - Email
  - Web browser
- Computer can connect to multiple physical networks
  - Wired Ethernet
  - Wi-Fi wireless network
- Other layers have multiple protocols as well

7-Layer OSI Reference Model



7-Layer OSI Reference Model



Source: community.fs.com

7-Layer OSI Reference Model

- Session layer
  - Handled details of login and control of send/ receive
  - Provided opportunity for billing and accounting
- Presentation layer
  - Defined data representation
  - Primary intention was to map character sets
- Both layers now superfluous

Review: 5 Layer TCP/IP Reference Model

Source: Network Direction

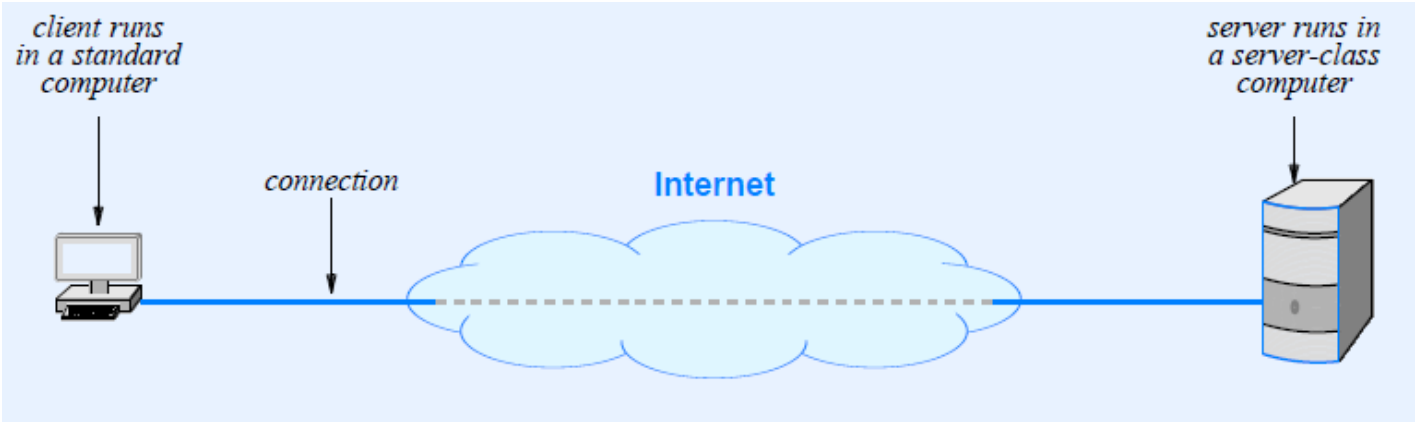
Summary

- A protocol standard can specify data and message representation, rules for message exchange, error handling, or low-level details such as voltage
- A layering model provides a conceptual framework that helps protocol designers create a suite of protocols
- Implementation of layered protocols known as a *stack*
- Internet uses a 5-layer TCP/IP reference model

Client-Server Model

Client-Server Model of Interaction

- Used by applications to establish communication
- One application acts as a *server*
  - Starts execution first
  - Awaits contact
- The other application becomes a *client*
  - Starts after server is running
  - Initiates contact
- Important concept: once communication has been established, data (e.g., requests and responses) can flow in either direction between a client and server



Characteristics of A Client

- Arbitrary application program that becomes a client temporarily
- Usually invoked directly by a user, and usually executes only for one session
- Actively initiates contact with a server, exchanges messages, and then terminates contact
- Can access multiple services as needed, but usually contacts one remote server at a time
- Runs locally on a user's personal computer or smart phone
- Does not require especially powerful computer hardware

Characteristics of A Server

- Special-purpose, privileged program dedicated to providing a service
- Usually designed to handle multiple remote clients at the same time
- Waits passively for contact from arbitrary remote clients and then exchanges messages
- Requires powerful hardware and a sophisticated operating system

复杂的

- Runs on a large, powerful computer

Client-Server Interaction

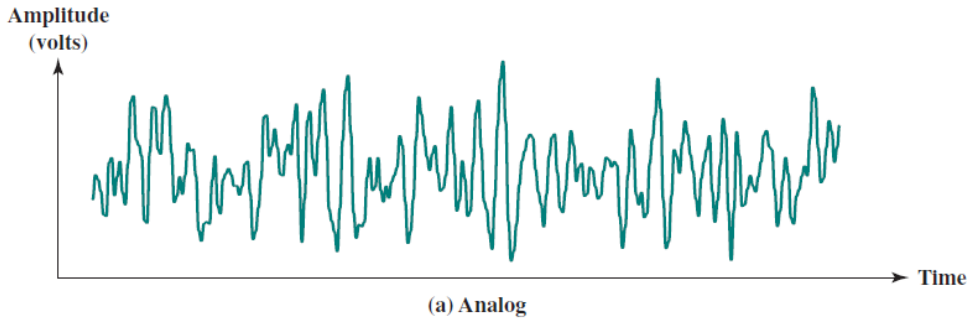
Server Application	Client Application
Starts first	Starts second
Does not need to know which client will contact it	Must know which server to contact
Waits passively and arbitrarily long for contact from a client	Initiates a contact whenever communication is needed
Communicates with a client by sending and receiving data	Communicates with a server by sending and receiving data
Stays running after servicing one client, and waits for another	May terminate after interacting with a server

Part 2: Physical Layer & Media

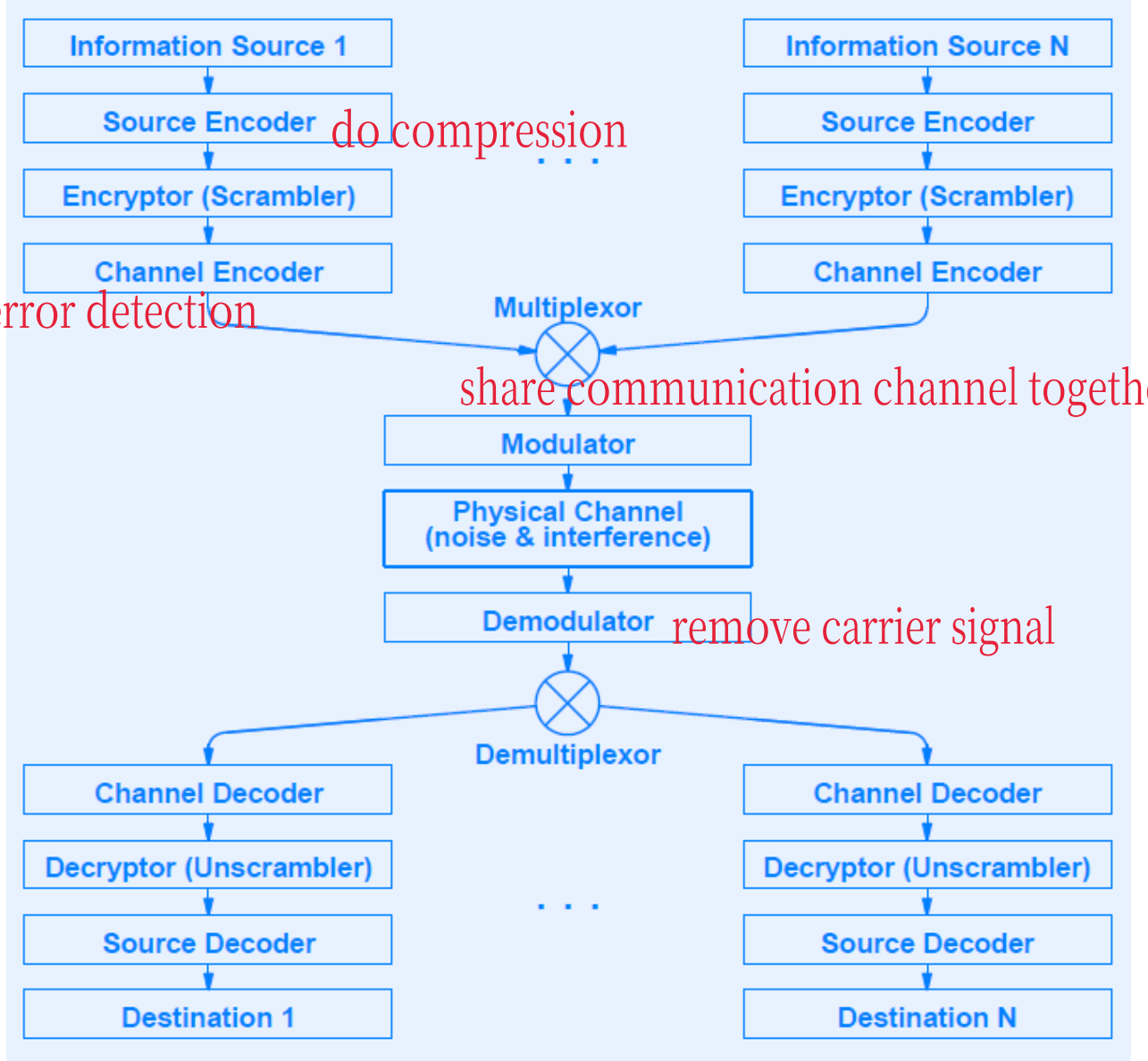
Data Communications Framework

Motivation

- Find ways to transmit analog and digital information
  - Using natural phenomena (e.g., electromagnetic radiation)
  - Allow multiple senders to share a transmission medium
- Data communications provides
  - A conceptual framework
  - Mathematical basis



Data Communications Framework



do compression

insert extra bits for error detection

share communication channel together using multiplexer

remove carrier signal

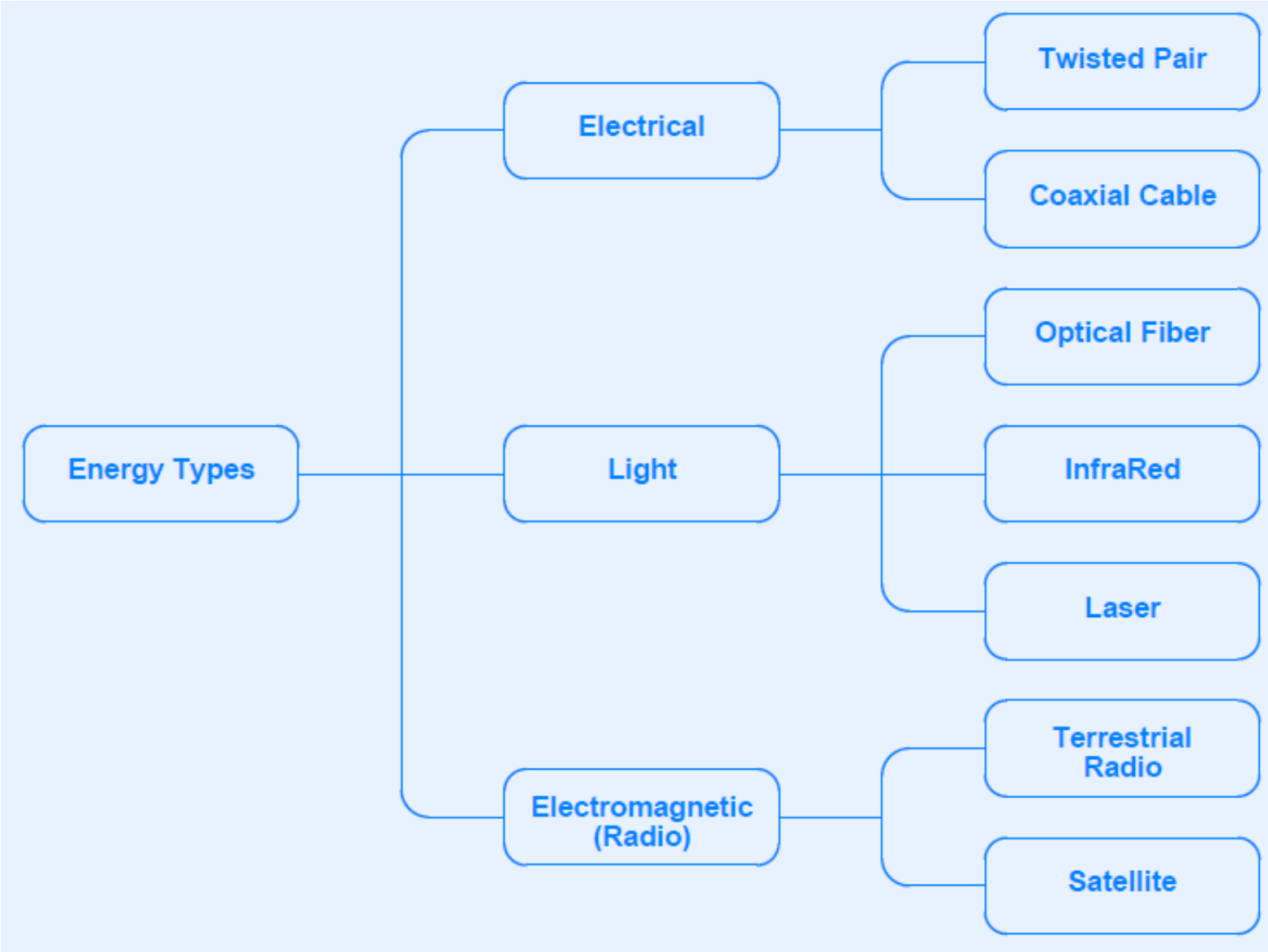
Data Communications Framework

- Which of the modules in the data communication framework involve significant change in data rate? Why?

source encoder, reduce bit rate , for it apply compression
channel encoder, increase bit rate, for it add extra bits for error detection

Transmission Media

Transmission Media



Loss, Interference, and Electrical Noise

- Transmission is plagued with problems
- Problems in the electrical and electromagnetic worlds
  - Resistance (leads to loss)
  - Capacitance (leads to distortion)
  - Inductance (leads to interference)
- Random electromagnetic radiation is called *noise*
  - *Can be generated by specific sources such as electric motor*
  - *Background radiation is an inescapable feature of the universe*

Measures of Transmission Media

通过

- *Propagation delay* - time required for a signal to traverse a medium
- *Channel capacity* - maximum data rate

Channel Capacity

- *Shannon's Theorem* gives the maximum channel capacity, *C*, in the presence of noise

$$C = B \log_2(1 + \mathrm{S}/\mathrm{N})$$

bandwidth B

- Quantity S / N is known as the *signal-to-noise ratio*

Exercise: Channel Capacity

- Suppose that the spectrum of a channel is between 3 MHz and 4 MHz and SNR in dB = 24 dB, find the channel capacity.

convert decibel into real value first

$$B = 4\ \text{MHz} - 3\ \text{MHz} = 1\ \text{MHz} = 10\text{^}6\ \text{Hz}$$

$$\text{SNR}_{\text{dB}} = 24\,\text{dB} = 10\log_{10}(\text{SNR})$$

$$\text{SNR} = 251$$

Using Shannon's formula,

$$C = 10^6 \times \log_2(1 + 251) \approx 10^6 \times 8 = 8\ \text{Mbps}$$

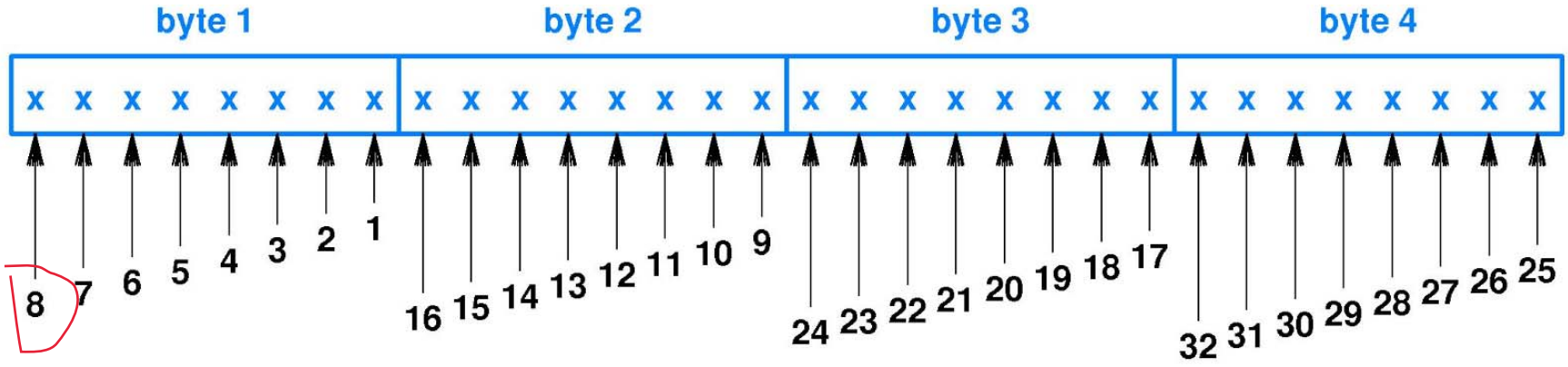
Transmission Modes

Serial Ordering of Bits and Bytes

- Both sides must agree on order in which bits are transmitted
- Two approaches known as *big-endian* and *little-endian*

end with large value

- Example: Ethernet uses byte big-endian and bit little-endian order

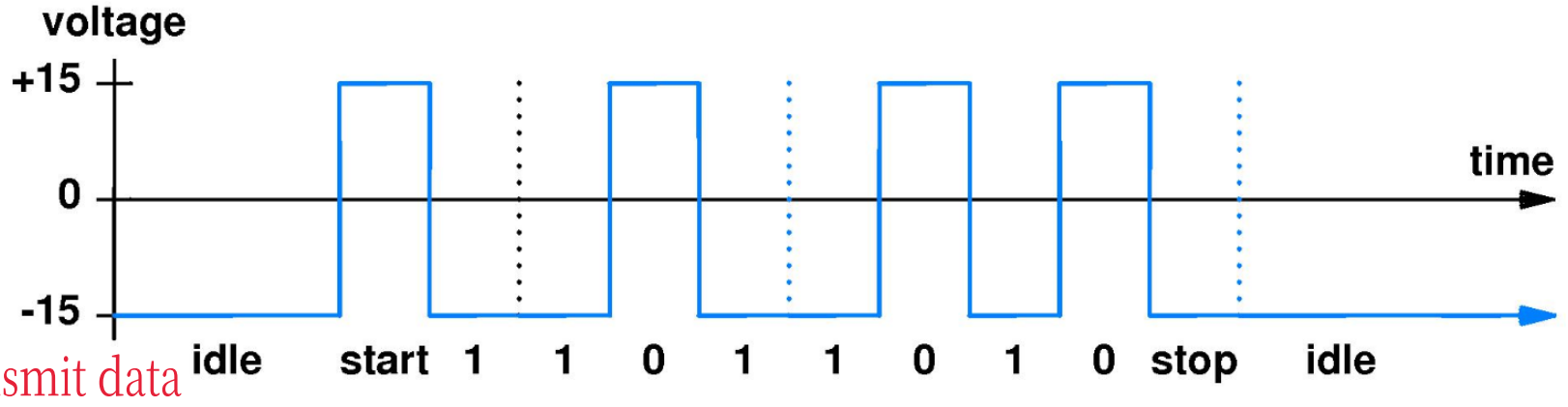


Transmission Mode

- Serial - one bit at a time
- Parallel - multiple bits at a time
- Serial
  - Asynchronous: transmission can occur at any time, with an arbitrary delay between the transmission of two data items.
  - Synchronous: transmission occurs continuously with no gap between the transmission of two data items.

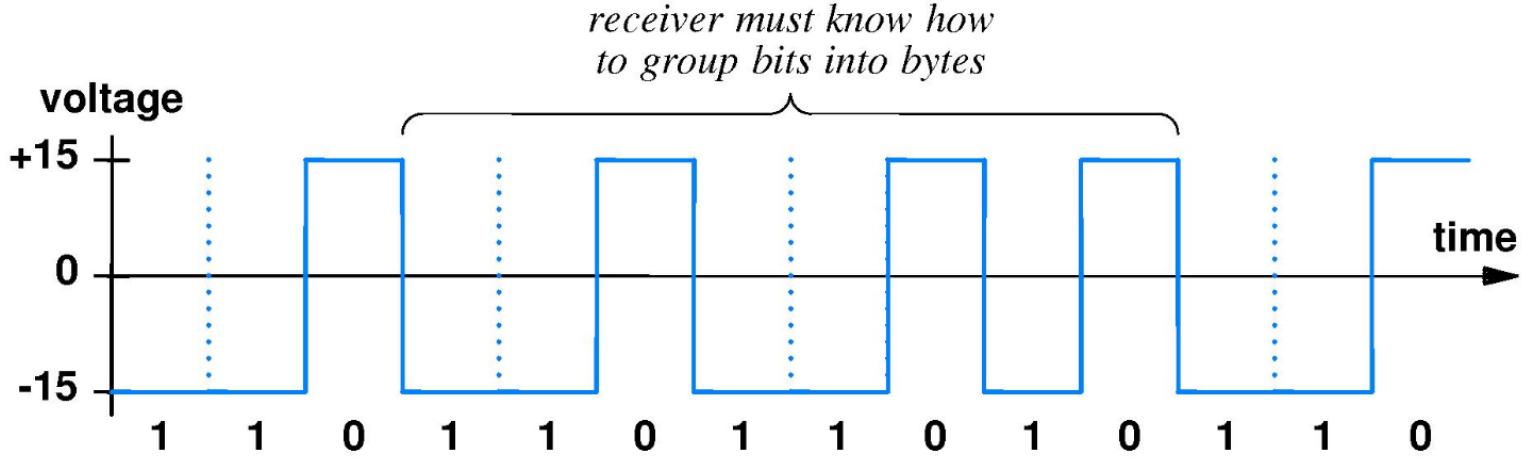
Asynchronous And Synchronous Transmission

- Asynchronous: line idle when not in use; data starts at arbitrary time



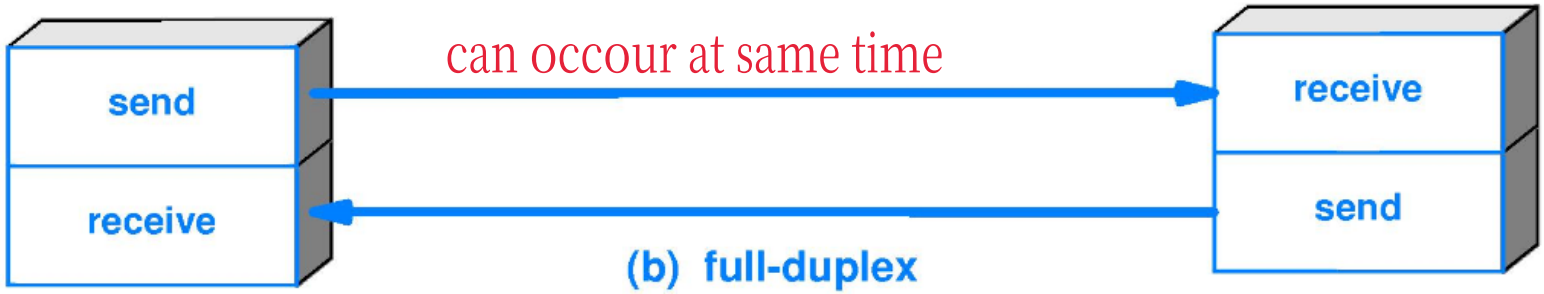
not transmit data

- Synchronous: each bit slot used

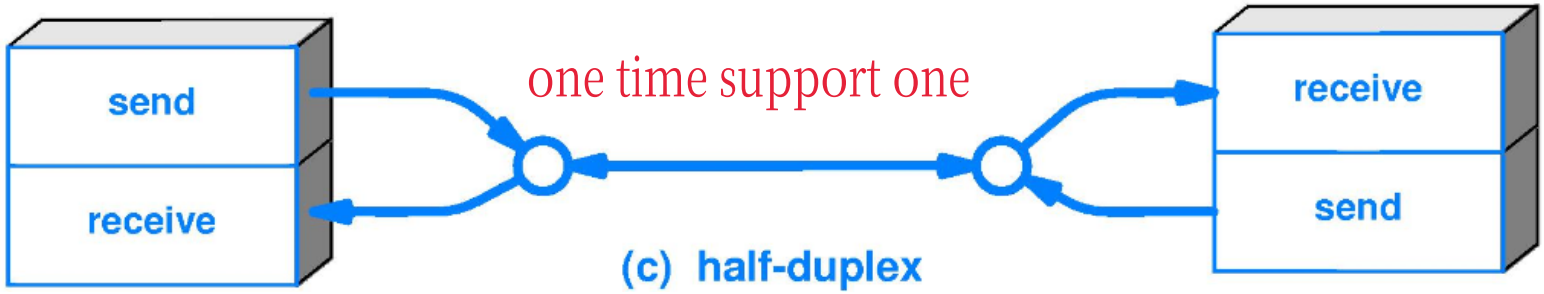


Simplex And Duplex Modes

(a) simplex



(b) full-duplex



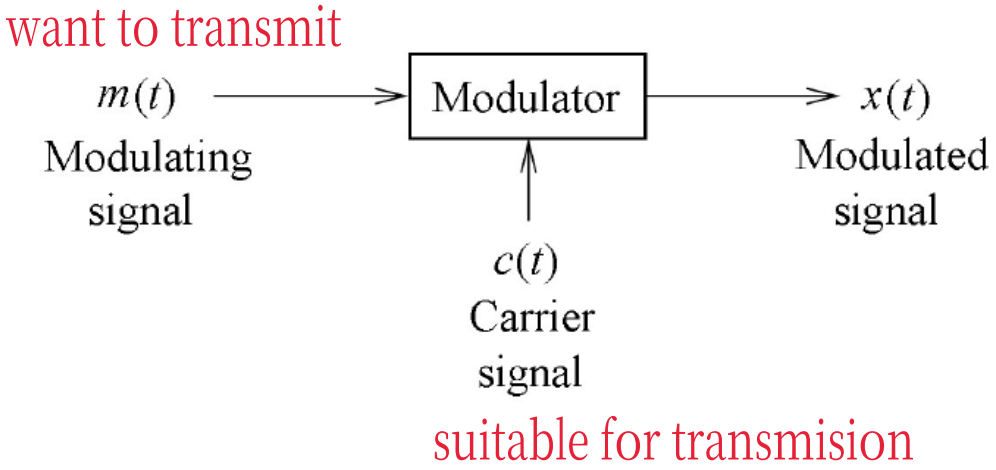
(c) half-duplex


SOCIAL
MEDIA
MUSIC
WEBLOGS
CONTACTS
PICTURES
COMMUNIATION
FRIENDSHIP
RATING
INTERNET
BOOKMARKING
MICROBLOGGING
VIDEO
FORUM

Modulation

Modulation

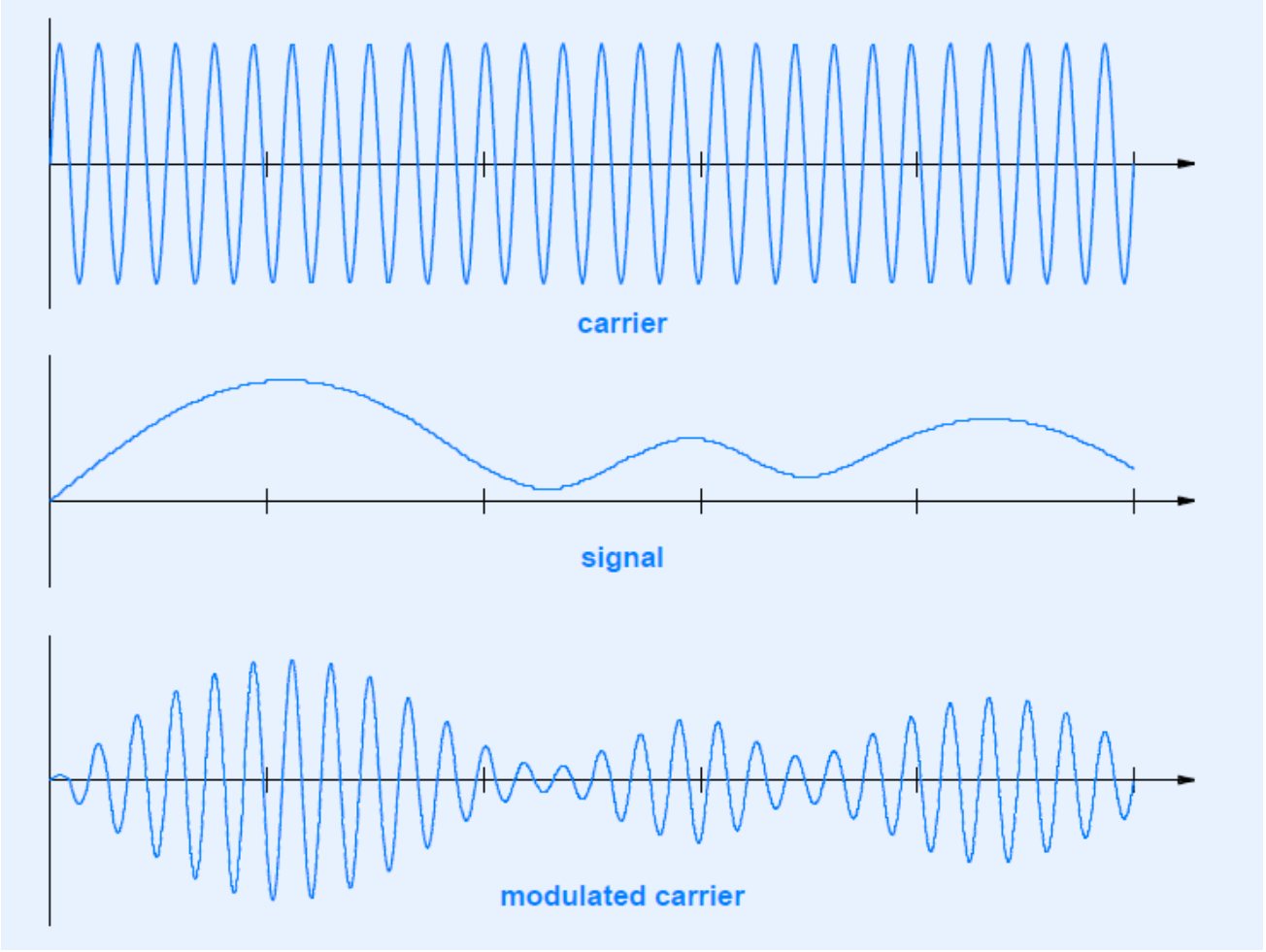
- Modulation aims to change/modulate the carrier using the message information to make it more suitable for transmission over communication channels.
- Common modulation:
  - Analog Modulation:
    - Amplitude modulation (AM)
    - Frequency modulation (FM)
  - Digital Modulation:
    - Amplitude Shift Keying (ASK)
    - Frequency Shift Keying (FSK)
    - Phase Shift Keying (PSK)



Amplitude Modulation

Amplitude Modulation (AM): The carrier amplitude is varied with the message signal

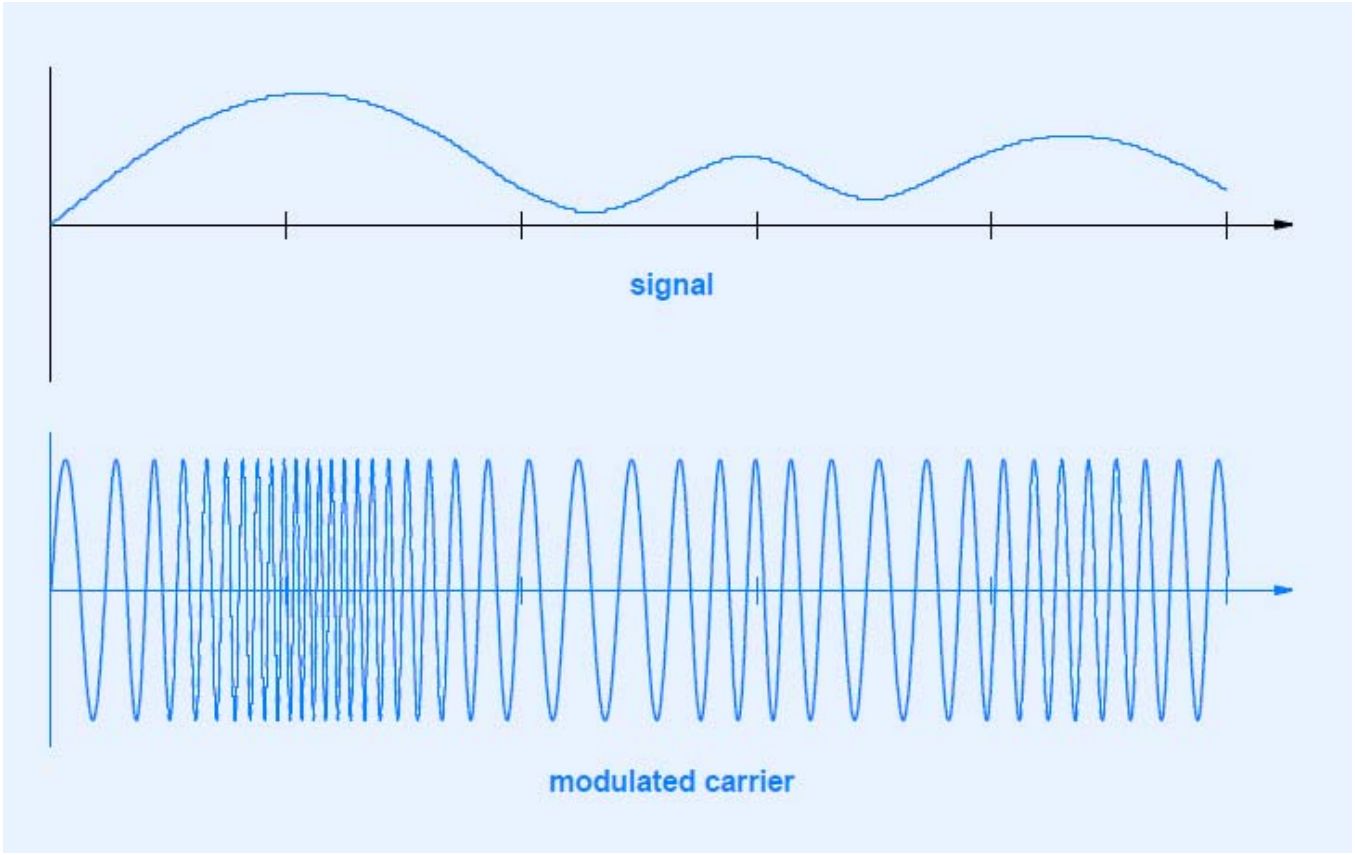
$$x_{AM}(t) = A_c\left[1 + k_a m(t)\right]\cos(2\pi f_c t)$$



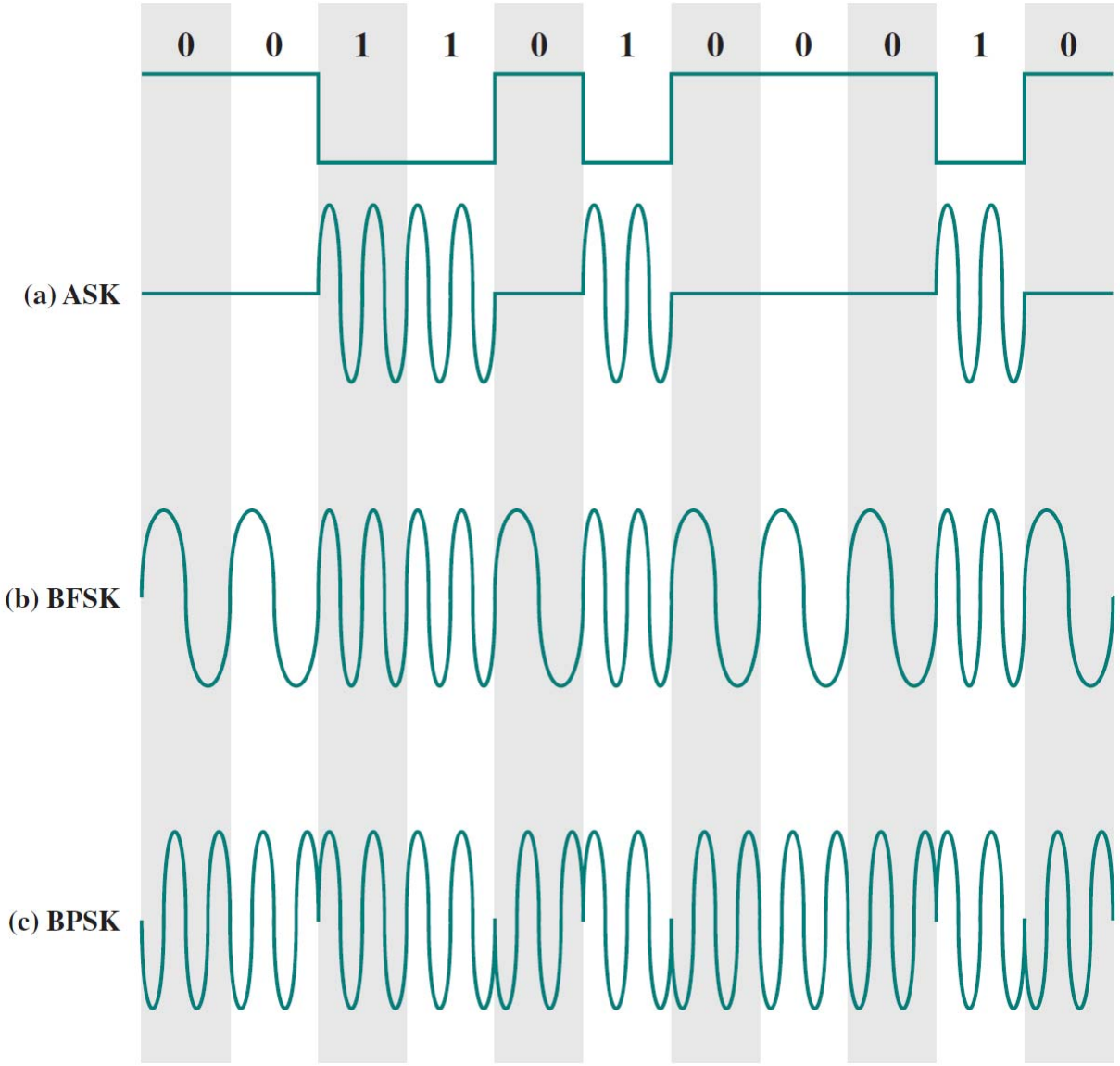
Frequency Modulation

Frequency Modulation (FM): The carrier frequency is varied with the message signal 's amplitude

$$x_{FM}(t) = A_c \cos\left[2\pi f_c t + k_f \int_0^t m(\tau)d\tau\right]$$



Digital Modulation



Amplitude Shift Keying (ASK)

- Modulating signal is digital
- In ASK, the two binary values are represented by two different amplitudes of the carrier frequency. Commonly, one of the amplitudes is zero
- One binary digit is represented by the presence, at constant amplitude, of the carrier, the other by the absence of the carrier 0

Frequency Shift Keying (FSK)

- The most common form of FSK is binary FSK (BFSK), in which the two binary values are represented by two different frequencies near the carrier frequency

$$\textbf{BFSK} \quad s(t) = \begin{cases} A\cos(2\pi f_1 t) & \text{binary 1} \\ A\cos(2\pi f_2 t) & \text{binary 0} \end{cases}$$

Phase Shift Keying (PSK)

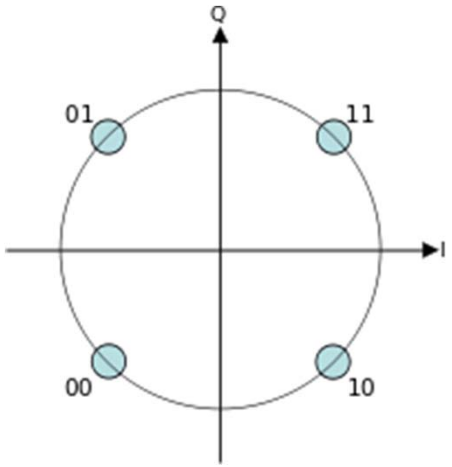
- Two-Level PSK - The simplest scheme uses two phases to represent the two binary digits, and is known as binary phase shift keying (BPSK)

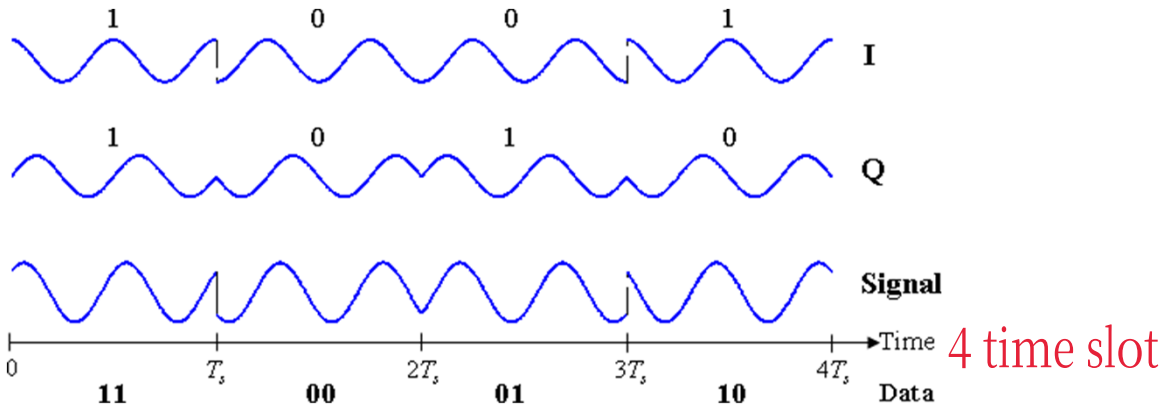
$$\textbf{BPSK} \quad s(t) = \begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t + \pi) \end{cases} = \begin{cases} A\cos(2\pi f_c t) & \text{binary 1} \\ -A\cos(2\pi f_c t) & \text{binary 0} \end{cases}$$

Quadrature Phase Shift Keying (QPSK)

- QPSK uses phase shifts separated by multiples of pi/2 (90°). Each signal element (symbol) represents two bits rather than one.

$$\text{QPSK} \quad s(t) = \begin{cases} A\cos\left(2\pi f_c t + \frac{\pi}{4}\right) & 11 \\ A\cos\left(2\pi f_c t + \frac{3\pi}{4}\right) & 01 \\ A\cos\left(2\pi f_c t - \frac{3\pi}{4}\right) & 00 \\ A\cos\left(2\pi f_c t - \frac{\pi}{4}\right) & 10 \end{cases}$$





4 time slot

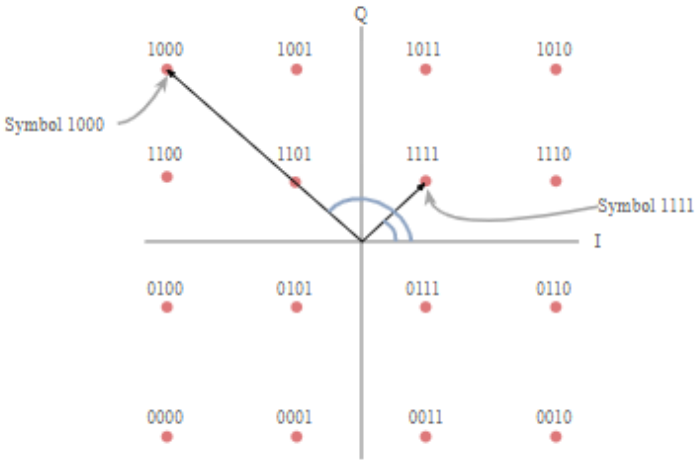
Quadrature Amplitude Modulation (QAM)

- Use in Modems (modulator / demodulator)

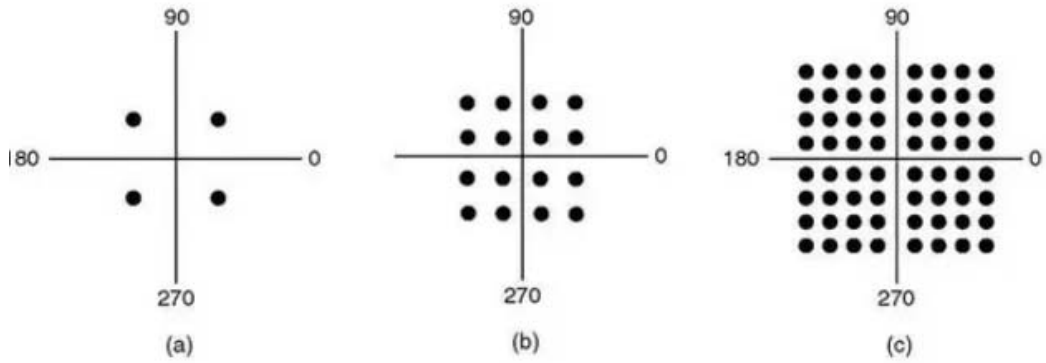
QAM $$s(t) = d_1(t)\cos 2\pi f_c t + d_2(t)\sin 2\pi f_c t$$

QAM can also be viewed as a combination of digital-amplitude and digital-phase modulation. Using trigonometric identities, we can rewrite the QAM equation in the form $s(t) = D(t)\cos(2\pi f_c t + \theta(t))$, where

$$D(t) = \sqrt{d_1(t)^2 + d_2(t)^2}, \quad \theta(t) = tan^{-1}\left(\frac{d_2(t)}{d_1(t)}\right)$$



Bit mapping for a 16QAM signal



(a) QPSK (b) 16-QAM (c) 64-QAM

can transmit 16 possible waveform, carry 4 bits per symbol. bit rate is 4*symbol rate

Source: electronics-notes.com

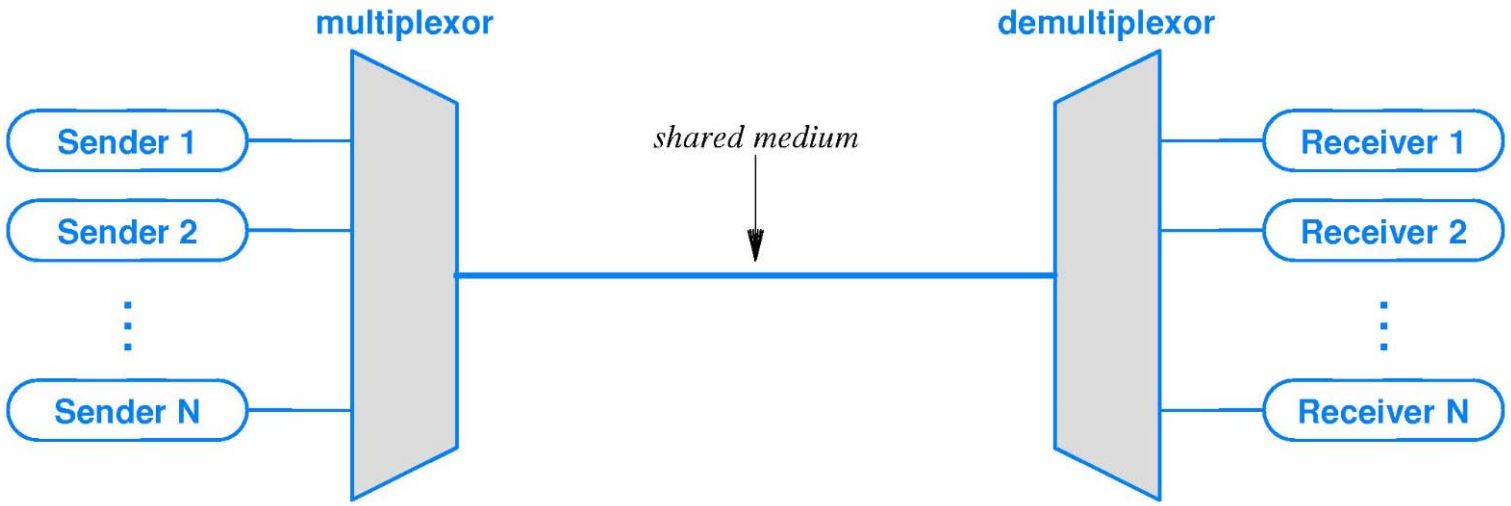
Quadrature Amplitude Modulation (QAM)

- What is the relationship between the symbol rate and bitrate of 16-QAM?

Multiplexing

Multiplexing And Types

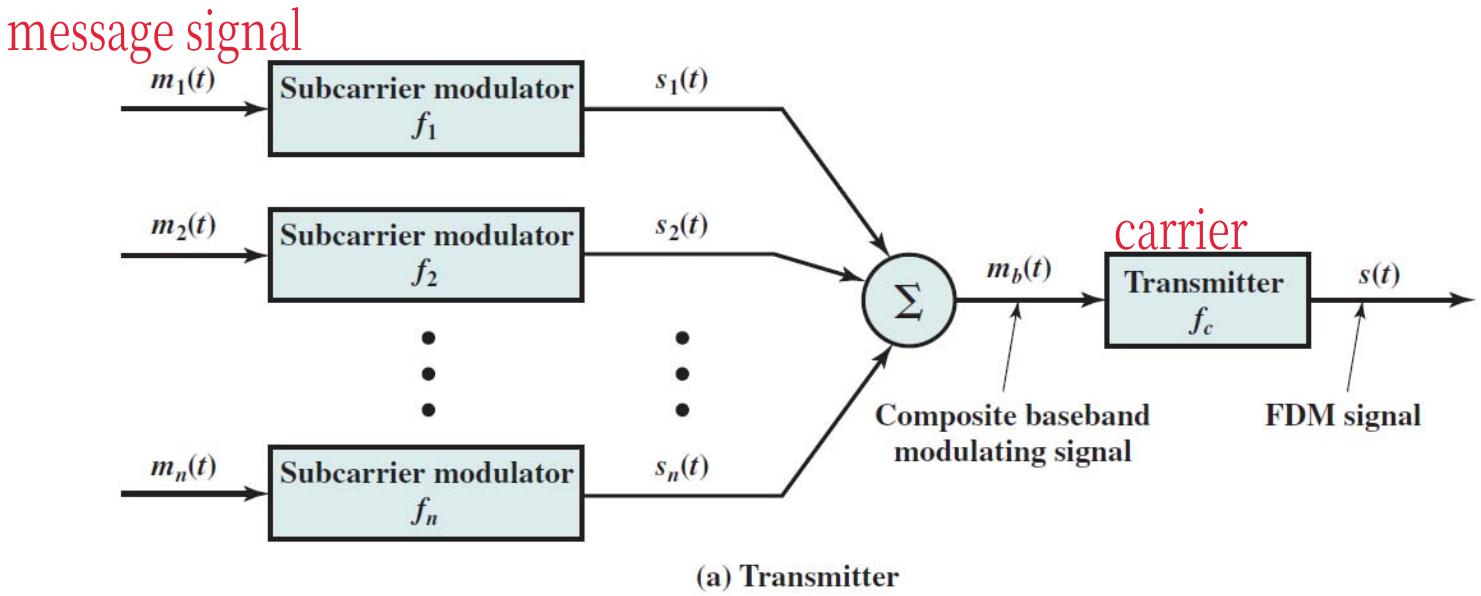
- Multiplexing aims to combine information streams from multiple sources for transmission over a shared medium.
- Types:
  - Frequency division multiplexing
  - Time division multiplexing
  - Code division multiplexing



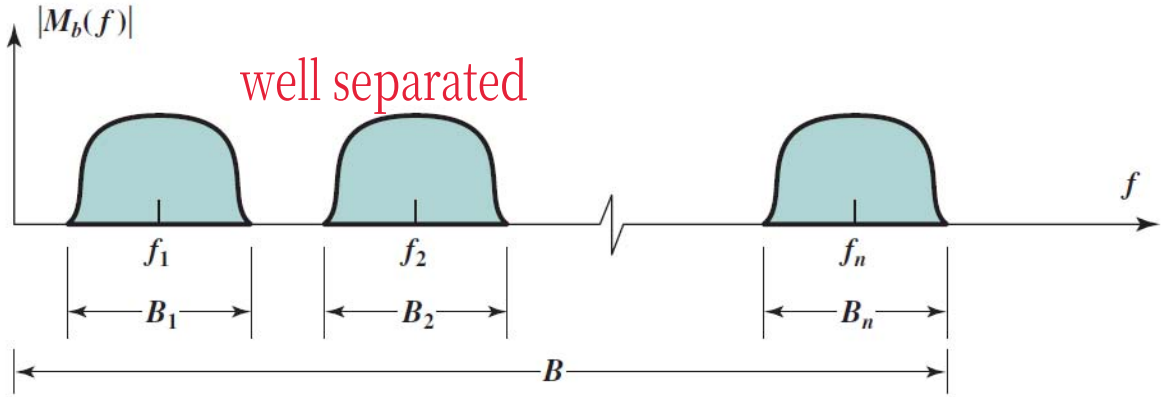
Frequency Division Multiplexing (FDM)

- Used in broadcast radio and cable TV
- Demultiplexing implemented with sets of filters.
- Each channel assigned a range of frequencies
- A *guard band* separates adjacent channels

FDM Transmitter

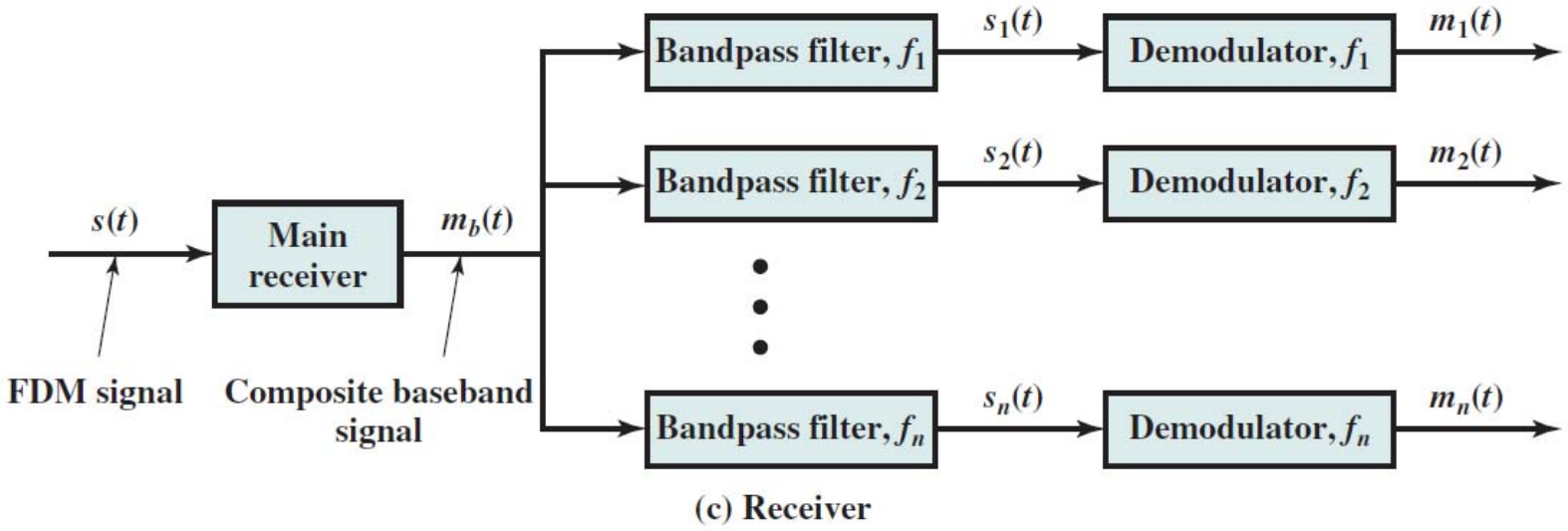


(a) Transmitter



(b) Spectrum of composite baseband modulating signal

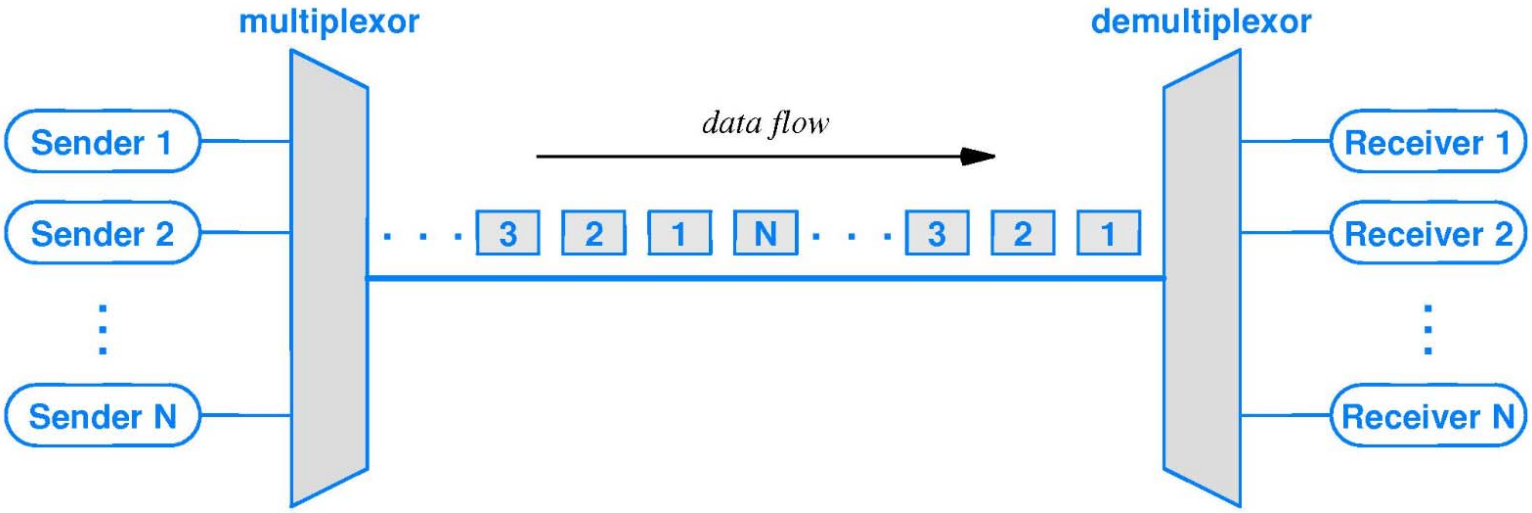
FDM Receiver



(c) Receiver

Time Division Multiplexing

- Senders take turns transmitting

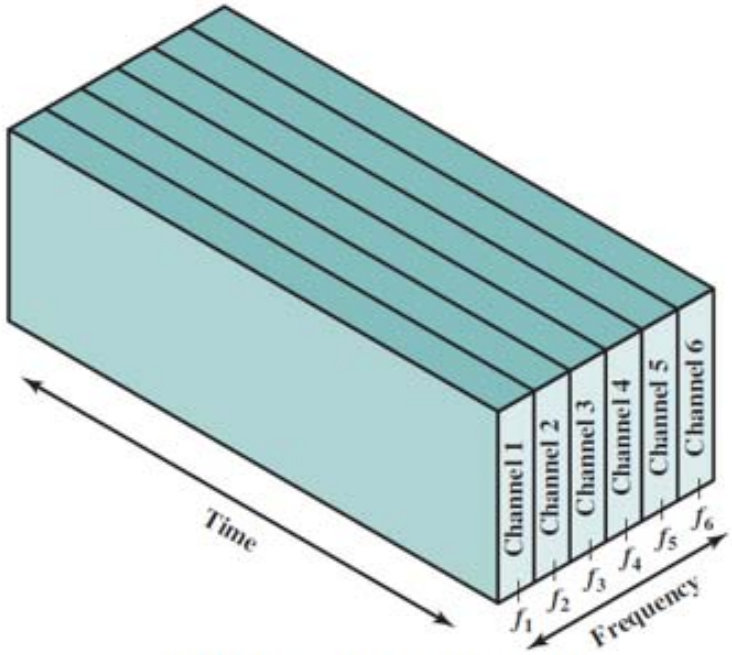


- Synchronous TDM
  - Each sender assigned a slot (typically round-robin)
  - Used by the telephone company

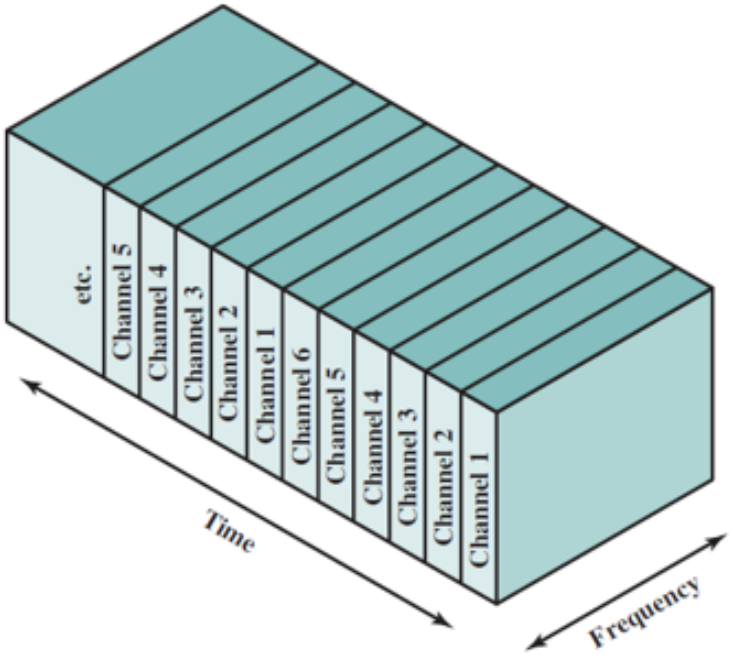
may cause waste for some user may has no message to send

- Statistical TDM
  - Sender only transmits when ready (e.g., Ethernet)

FDM vs TDM



(a) Frequency-division multiplexing



(b) Time-division multiplexing

Code Division Multiplexing

more convenient

- Mathematical form of multiplexing used with cell phones
- Algorithm
  - Each sender/receiver pair is assigned a unique number called a *chip sequence* of 0 and 1
  - *Senders multiply the data value by their chip sequence (orthogonal vector spaces)* correlation is 0, user data signals do not 互相影响, good property
  - *Transmitted value is a sum of all senders* transmit at the same time
  - *Each receiver multiplies incoming value by its chip sequence to extract data*
- *Advantage over statistical TDM: lower delay when network loaded*

Summary

- Data communications deals with the Physical Layer and data transmission
- Concepts include
  - Signals and conversion between digital and analog signal
  - Transmission media
  - Modulation and demodulation
  - Multiplexing and demultiplexing

Part 2: Data Link Layer & Technologies

Channel Coding

deal with noise problem happening in this layer

Sources of Errors and Types

- Error sources: interference, distortion, and attenuation (signal loss)
- Error types: single-bit error vs burst error (many error happen together)
- Channel coding used to detect and correct errors

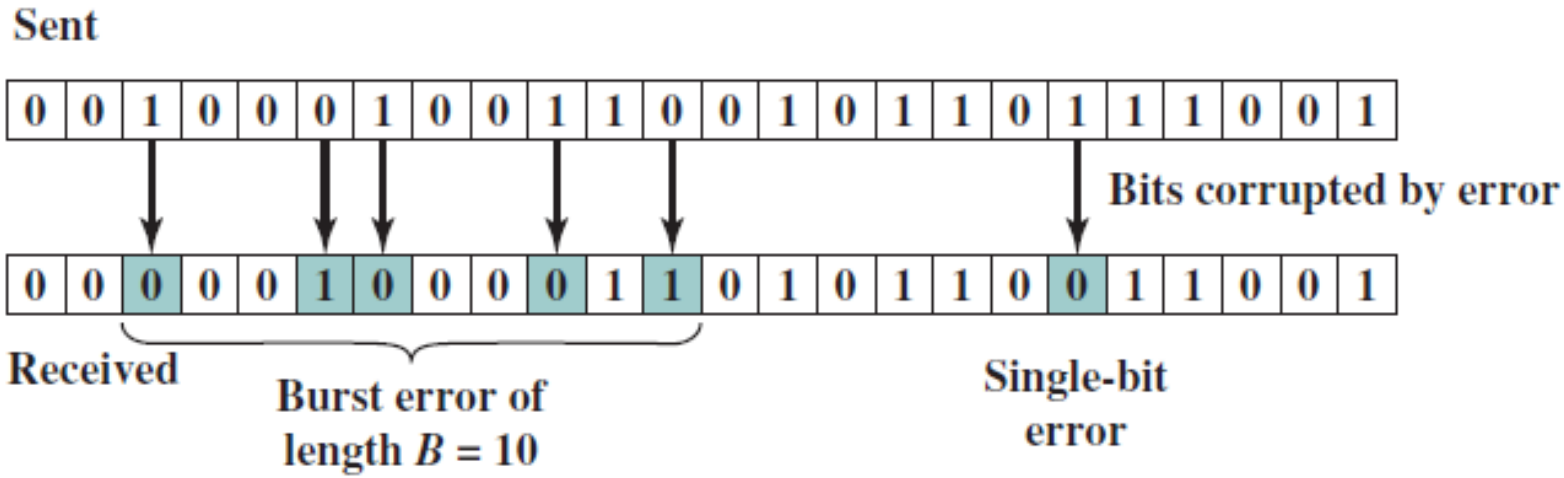
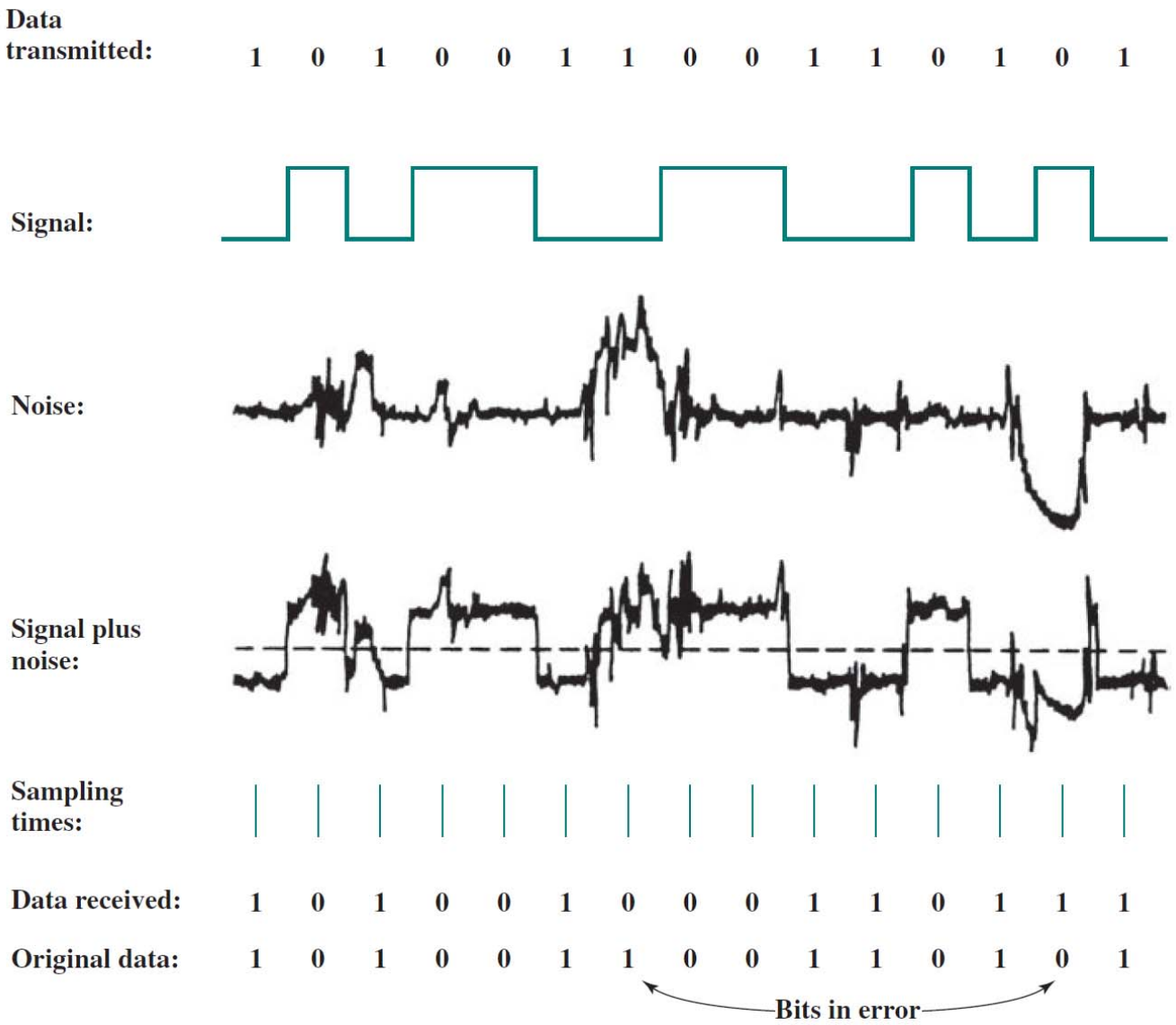


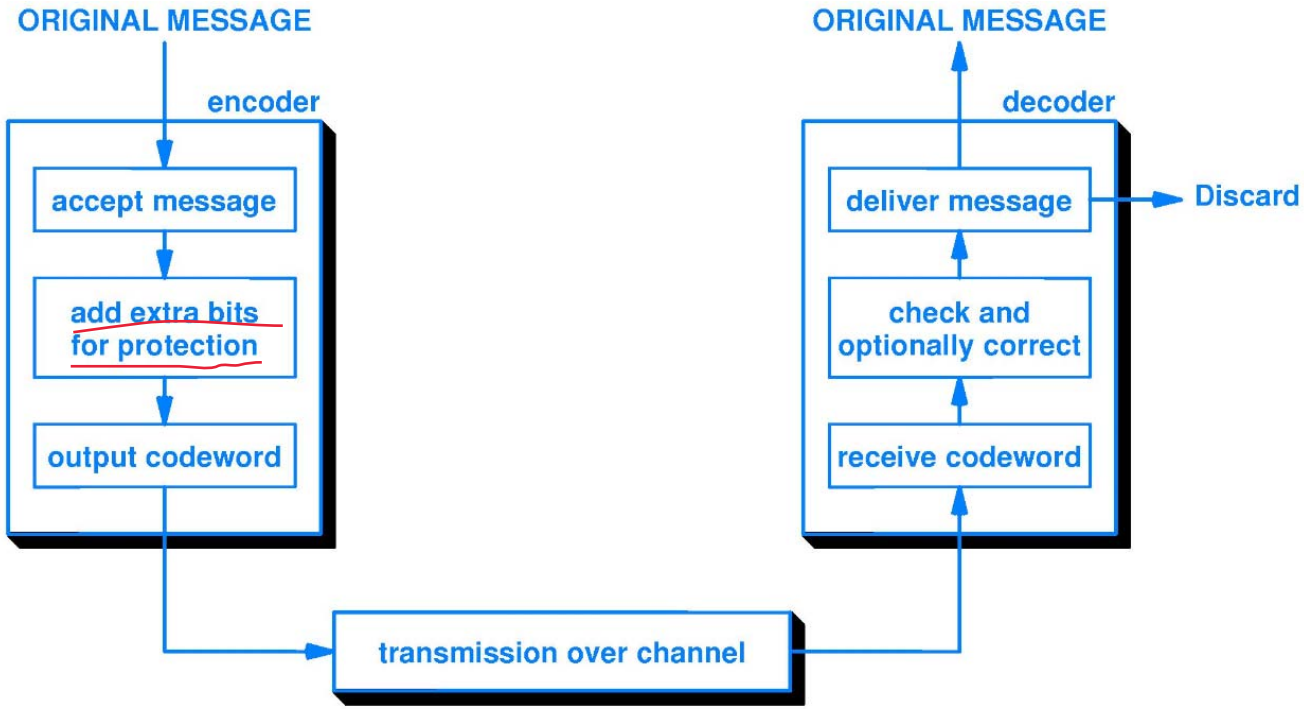
Figure 6.1 Burst and Single-Bit Errors

Effect of Noise on a Digital Signal



Error Detection and Correction

- Techniques:
  - Parity Check: Single parity bit, 2D Row And Column (RAC)
  - Internet checksum
  - Cyclic Redundancy Check (CRC) focus on it



Error Detection

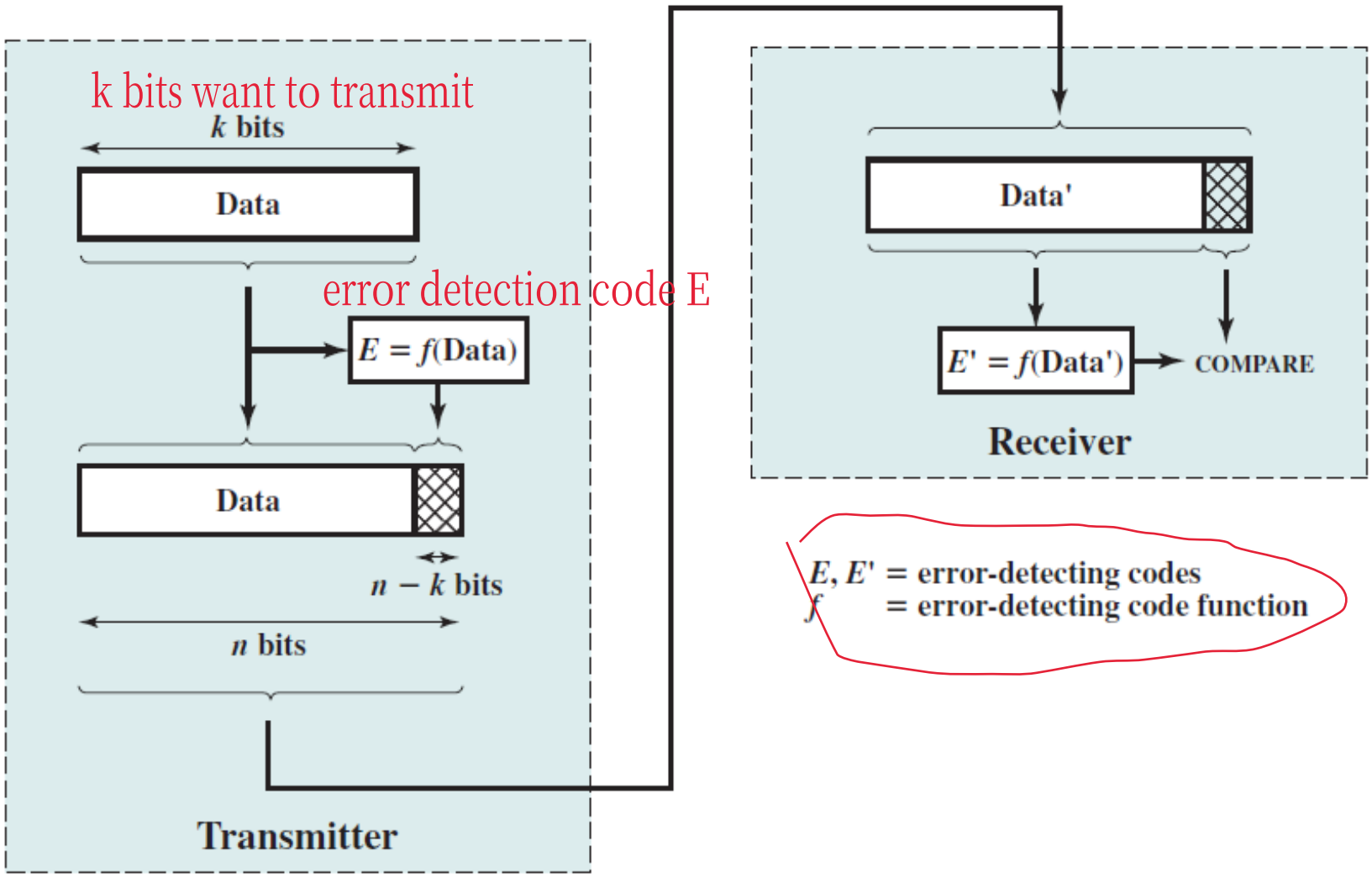


Figure 6.2 Error-Detection Process

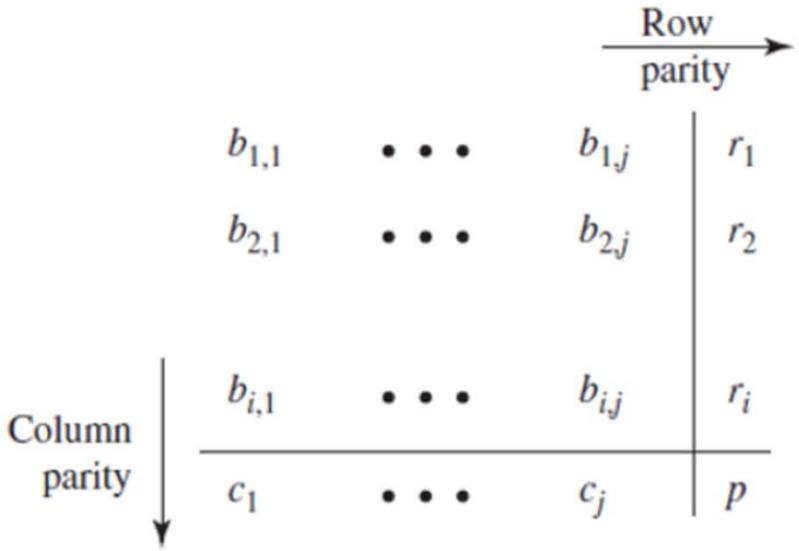
Parity Check

- Single Parity Bit
  - The simplest error detecting scheme is to append a parity bit to the end of a block of data
  - If any even number of bits are inverted due to error, an undetected error occurs

0 or 1

set 0 or 1 's total number is even or odd

Two-Dimensional Parity Check



(a) Parity calculation

0	1	1	1	0	1
0	1	1	1	0	1
0	1	0	0	0	1
0	1	0	1	1	1
0	0	0	1	1	0

(b) No errors

0	1	1	1	0	1
0	0	1	1	0	1
0	1	0	0	0	1
0	1	0	1	1	1
0	0	0	1	1	0

Row parity error

Column parity error

(c) Correctable single-bit error

append parity check bit to let all row and column have even number of 1

2-D Parity Check

- When would 2-D Parity Check fail?

0	1	1	1	1	1	0	1
0	(0)	1	1	0	(1)	1	0
0	0	1	1	0	0	1	1
0	(0)	0	0	0	(0)	0	0
1	0	1	1	1	1	1	0
1	1	0	0	0	1	1	0

(d) Uncorrectable error pattern

Internet Checksum

- Error detecting code used in many Internet standard protocols, including IP, TCP, and UDP

Cyclic Redundancy Check (CRC)

- A common and powerful error-detecting code
- Given a *k*-bit block of bits or dataword, the transmitter generates an (*n* – *k*) bit Frame Check Sequence (FCS), which is exactly divisible by some predetermined number, defined by generator polynomial P(x).

total n bits

- Receiver divides the incoming frame by that number
  - If there is no remainder, assume there is no error

CRC Computation

- Two approaches:
  - Modulo 2 arithmetic
    - Uses binary addition with no carries.
  - Polynomials
    - Express all values as polynomials in a dummy variable X, with binary coefficients.
    - Coefficients correspond to the bits in the binary number.

Modulo 2 Arithmetic (1)

Modulo 2 arithmetic uses binary addition with no carries, which is just the exclusive-OR (XOR) operation. Binary subtraction with no carries is also interpreted as the XOR operation: For example

$$\begin{array}{r} 1111 \\ +1010 \\ \hline 0101 \end{array} \qquad \begin{array}{r} 1111 \\ -0101 \\ \hline 1010 \end{array} \qquad \begin{array}{r} 11001 \\ \times\ 11 \\ \hline 11001 \\ 11001 \\ \hline 101011 \end{array}$$

Modulo 2 Arithmetic (2)

Now define

$T = n$-bit frame to be transmitted

$D = k$-bit block of data, or message, the first k bits of T

generated $F = (n - k)$-bit FCS, the last $(n - k)$ bits of T

P = pattern of $n - k + 1$ bits; this is the predetermined divisor

P will be given, no need to decide by yourself

The pattern *P* (defined by generator polynomial P(x)) is chosen to be one bit longer than the desired FCS. At minimum, both the high- and low-order bits of *P* must be 1.

Modulo 2 Arithmetic (3)

We would like T/P to have no remainder. It should be clear that

$$T = 2^{n-k}D + F$$

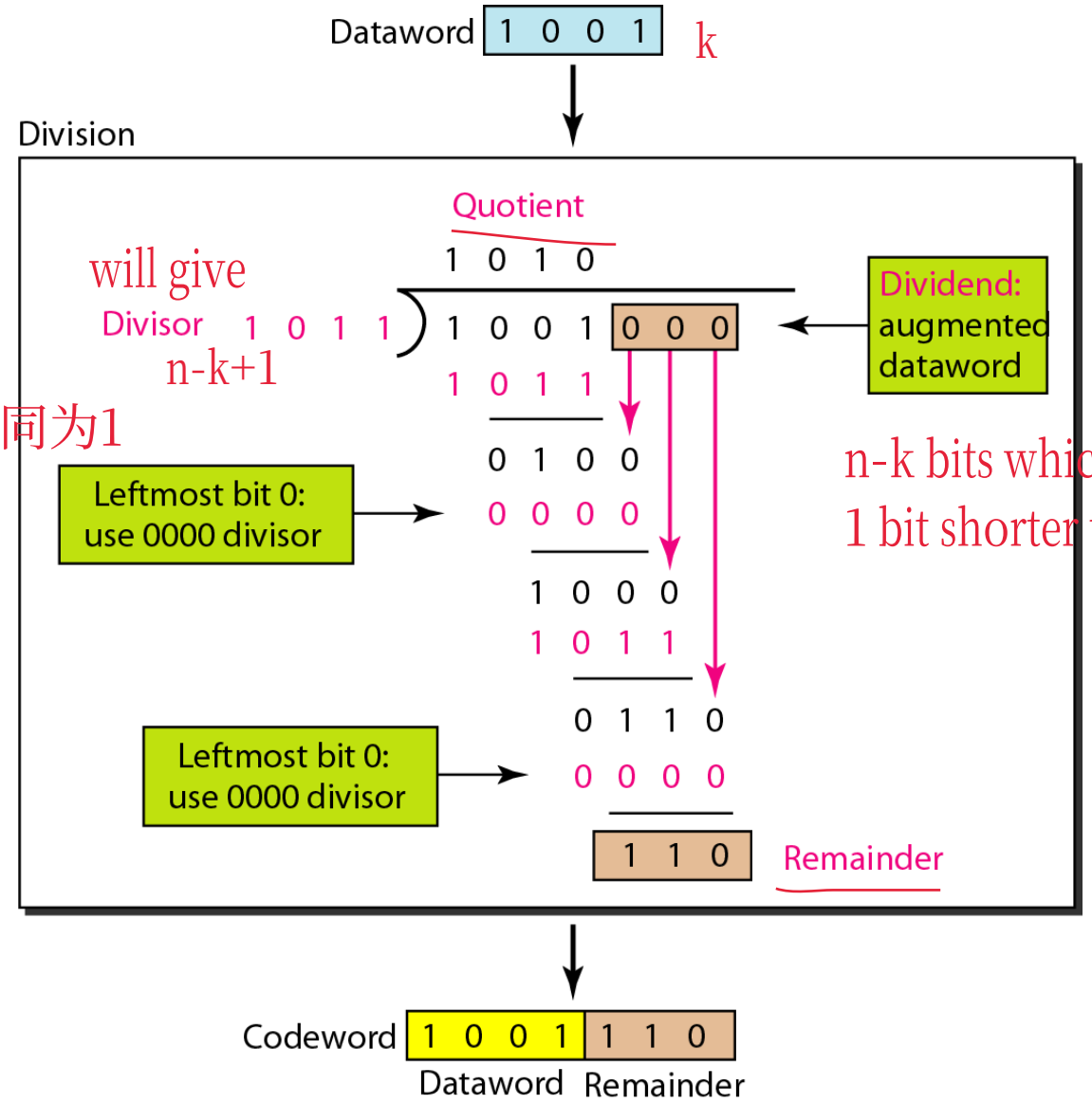
That is, by multiplying D by 2^{n-k}, we have in effect shifted it to the left by $n-k$ bits and padded out the result with zeroes. Adding F yields the concatenation of D and F, which is T. We want T to be exactly divisible by P. Suppose that we divide $2^{n-k}D$ by P:

$$\frac{2^{n-k}D}{P} = Q + \frac{R}{P} \qquad \textbf{(6.1)}$$

There is a quotient and a remainder. Because division is modulo 2, the remainder is always at least one bit shorter than the divisor. We will use this remainder as our FCS. Then

$$T = 2^{n-k}D + R \qquad \textbf{(6.2)}$$

CRC Encoder

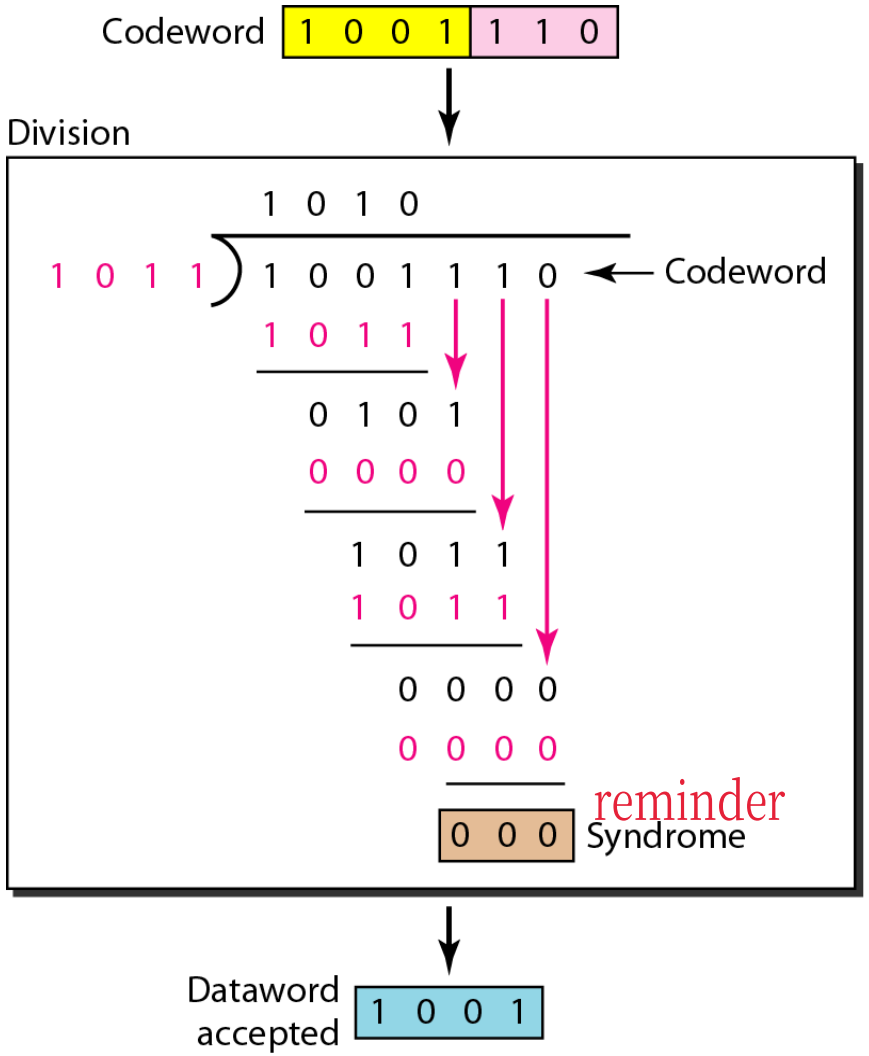


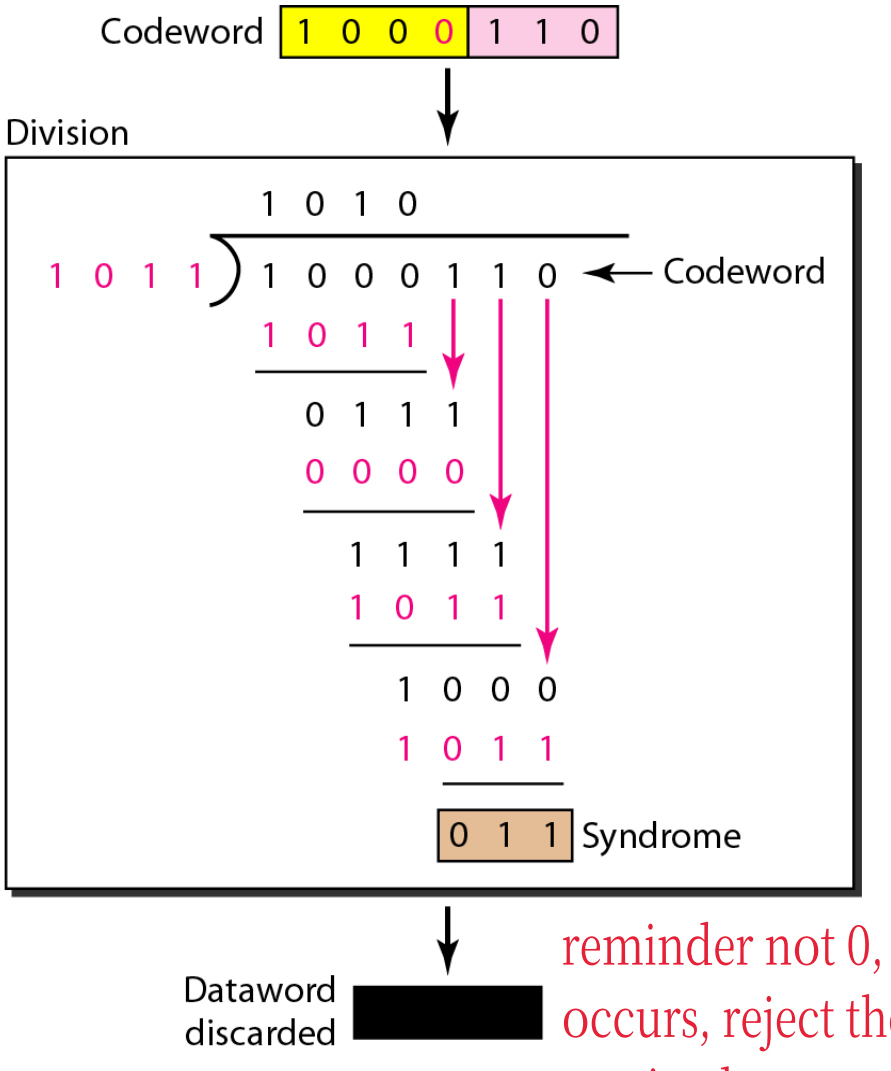
XOR 相同为0，不同为1

n-k bits which is
1 bit shorter than the divisor

CRC Decoder

decide error happen or not





reminder not 0, error occurs, reject the data received

decide first 4 bits is the correct data

Example: CRC (1)

1. Given

$$\text{Message } D = 1010001101 \text{ (10 bits)}$$
$$\text{Pattern } P = 110101 \text{ (6 bits)}$$
$$\text{FCS } R = \text{ to be calculated (5 bits)}$$

k=5

n-k+1=6

n-k=5

Thus, $n = 15$, $k = 10$, and $(n - k) = 5$.

2. The message is multiplied by 2^5, yielding 1010001101**00000**.

Example: CRC (2)

3. This product is divided by P:

quotient

$$
\begin{array}{rl}
 & 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0 \leftarrow Q \\
P \rightarrow 1\ 1\ 0\ 1\ 0\ 1 \;\big/ & 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0 \leftarrow 2^{n-k}D \\
 & \underline{1\ 1\ 0\ 1\ 0\ 1} \\
 & \quad 1\ 1\ 1\ 0\ 1\ 1 \\
 & \quad \underline{1\ 1\ 0\ 1\ 0\ 1} \\
 & \quad\quad 1\ 1\ 1\ 0\ 1\ 0 \\
 & \quad\quad \underline{1\ 1\ 0\ 1\ 0\ 1} \\
 & \quad\quad\quad 1\ 1\ 1\ 1\ 1\ 0 \\
 & \quad\quad\quad \underline{1\ 1\ 0\ 1\ 0\ 1} \\
 & \quad\quad\quad\quad 1\ 0\ 1\ 1\ 0\ 0 \\
 & \quad\quad\quad\quad \underline{1\ 1\ 0\ 1\ 0\ 1} \\
 & \quad\quad\quad\quad\quad 1\ 1\ 0\ 0\ 1\ 0 \\
 & \quad\quad\quad\quad\quad \underline{1\ 1\ 0\ 1\ 0\ 1} \\
 & \quad\quad\quad\quad\quad\quad 0\ 1\ 1\ 1\ 0 \leftarrow R
\end{array}
$$

reminder

4. The remainder is added to 2^5D to give $T = 101000110101110$, which is transmitted.

Example: CRC (3)

5. If there are no errors, the receiver receives T intact. The received frame is divided by P:

```
                                1 1 0 1 0 1 0 1 1 0  ← Q
                              ┌──────────────────────
P → 1 1 0 1 0 1  /  1 0 1 0 0 0 1 1 0 1 0 1 1 1 0  ← T
                    1 1 0 1 0 1
                    ─────────
                      1 1 1 0 1 1
                      1 1 0 1 0 1
                      ─────────
                        1 1 1 0 1 0
                        1 1 0 1 0 1
                        ─────────
                          1 1 1 1 1 0
                          1 1 0 1 0 1
                          ─────────
                            1 0 1 1 1 1
                            1 1 0 1 0 1
                            ─────────
                              1 1 0 1 0 1
                              1 1 0 1 0 1
                              ─────────
                                        0  ← R
```

Because there is no remainder, it is assumed that there have been no errors.

Exercise: CRC Using Modulo 2 Arithmetic

k=10

A dataword D = 1101011111 (most significant from the left), and a polynomial sequence of P=10011 (corresponding to P(x)=x^4+x^1+1) is used to transmit codeword using CRC.

n-k+1=5

FCS、 reminder is n-k=4 bits

(i) Find the transmitted codeword.

n=14

(ii) If the 8th bit (from the left) of the transmitted codeword experiences an error during transmission, can the CRC detect that a transmission error has occurred?

见另一个PPT解答

Solution


SOCIAL
MEDIA
MUSIC
WEBLOGS
CONTACTS
PICTURES
FRIENDSHIP
RATING
INTERNET
BOOKMARKING
MICROBLOGGING
VIDEO
FORUM

Polynomial Approach (1)

A second way of viewing the CRC process is to express all values as polynomials in a dummy variable X, with binary coefficients. The coefficients correspond to the bits in the binary number. Thus, for $D = 110011$, we have $D(X) = X^5 + X^4 + X + 1$, and for $P = 11001$, we have $P(X) = X^4 + X^3 + 1$. Arithmetic operations are again modulo 2. The CRC process can now be described as

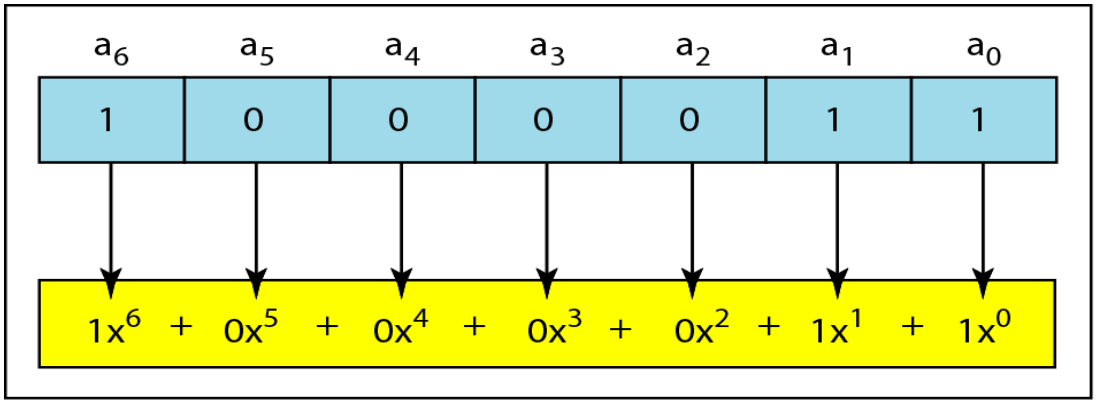
$$\frac{X^{n-k}D(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$T(X) = X^{n-k}D(X) + R(X)$$

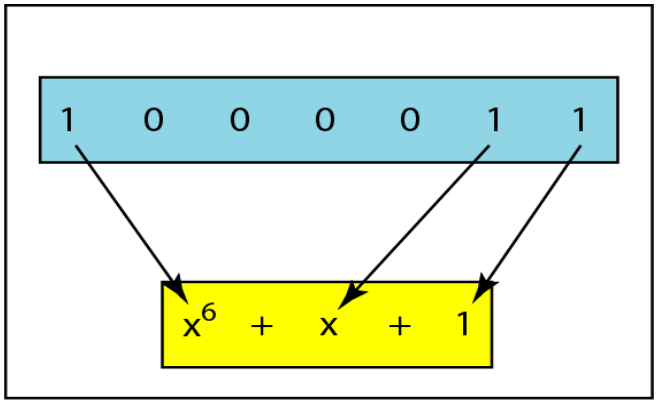
Compare these equations with Equations (6.1) and (6.2).

Polynomial Approach (2)

conversion between binary and decimal

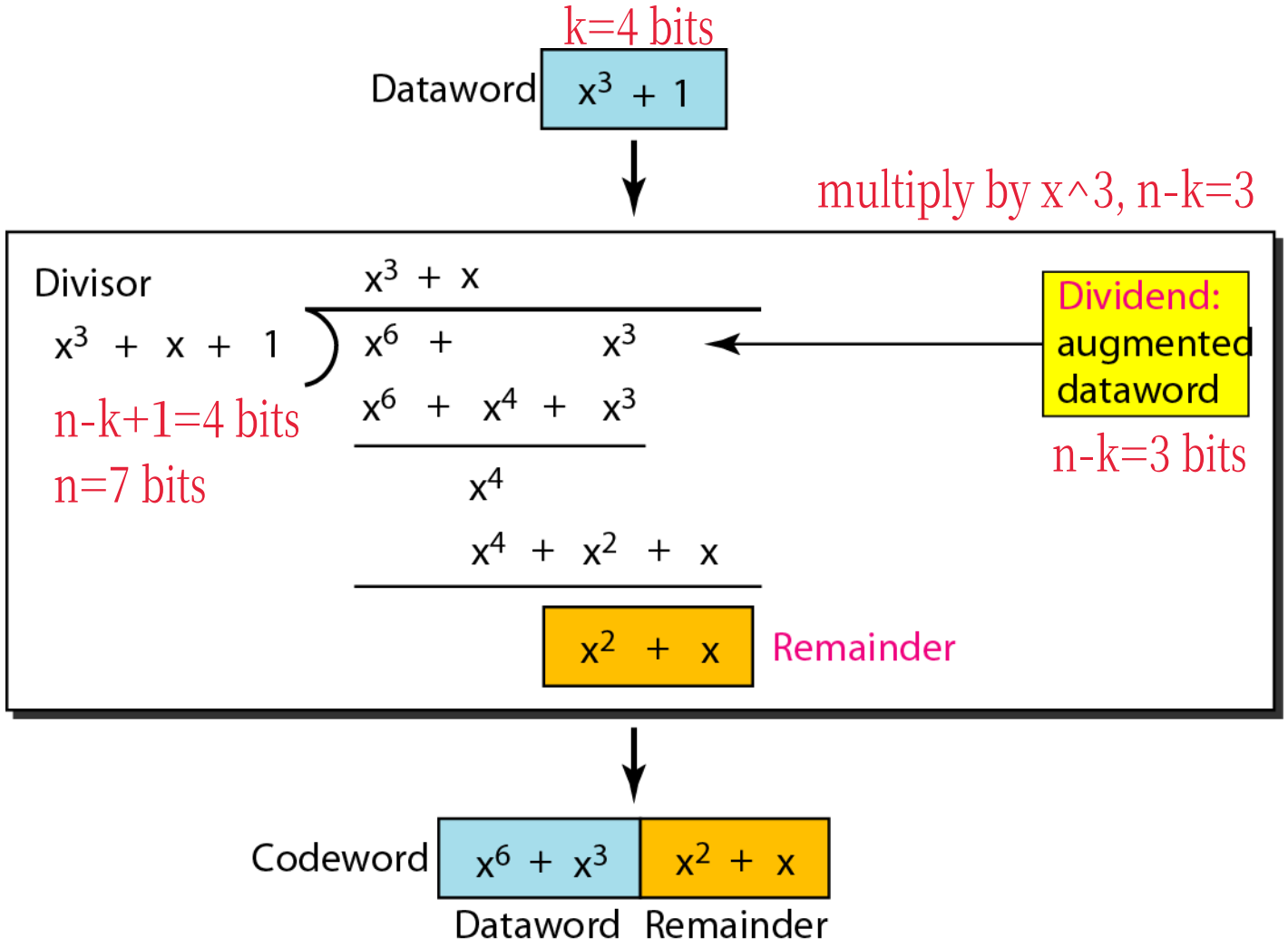


a. Binary pattern and polynomial



b. Short form

Polynomial Approach (3)



Example: CRC Using Polynomial Approach

k=10

EXAMPLE 6.7 Using the preceding example, for $D = 1010001101$, we have $D(X) = X^9 + X^7 + X^3 + X^2 + 1$, and for $P = 110101$, we have $P(X) = X^5 + X^4 + X^2 + 1$. We should end up with $R = 01110$, which corresponds to $R(X) = X^3 + X^2 + X$. Figure 6.5 shows the polynomial division that corresponds to the binary division in the preceding example.

n-k+1=6
so n=15

$$X^9 + X^8 + X^6 + X^4 + X^2 + X \quad \leftarrow Q(X)$$

$$P(X) \rightarrow X^5 + X^4 + X^2 + 1 \;\big/\; X^{14} + X^{12} + X^8 + X^7 + X^5 \quad \leftarrow X^5D(X)$$

6 bits

n-k=5 reminder

$$X^{14} + X^{13} + X^{11} + X^9$$
$$X^{13} + X^{12} + X^{11} + X^9 + X^8$$
$$X^{13} + X^{12} + X^{10} + X^8$$
$$X^{11} + X^{10} + X^9 + X^7$$
$$X^{11} + X^{10} + X^8 + X^6$$
$$X^9 + X^8 + X^7 + X^6 + X^5$$
$$X^9 + X^8 + X^6 + X^4$$
$$X^7 + X^5 + X^4$$
$$X^7 + X^6 + X^4 + X^2$$
$$X^6 + X^5 + X^2$$
$$X^6 + X^5 + X^3 + X$$
$$X^3 + X^2 + X \quad \leftarrow R(X)$$

Figure 6.5 Example of Polynomial Division

Common Generator Polynomial P(x)

Four versions of $P(X)$ are widely used:

$$\text{CRC-12} = X^{12} + X^{11} + X^3 + X^2 + X + 1 = (X + 1)(X^{11} + X^2 + 1)$$

$$\text{CRC-ANSI} = X^{16} + X^{15} + X^2 + 1 = (X + 1)(X^{15} + X + 1)$$

$$\text{CRC-CCITT} = X^{16} + X^{12} + X^5 + 1 = (X + 1)(X^{15} + X^{14} + X^{13} + X^{12} + X^4 + X^3 + X^2 + X + 1)$$

$$\text{IEEE-802} = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

Exercise: CRC Using Polynomial Approach

n-k=4 k=11 so n=15

A CRC is constructed to generate a 4-bit FCS for an 11-bit message. The generator polynomial is X^4 + X^3 + 1. Encode the data bit sequence 00111011001 (most significant bit from the left) using the generator polynomial and give the codeword.

Solution


SOCIAL
MEDIA
MUSIC
WEBLOGS
CONTACTS
PICTURES
FRIENDSHIP
RATING
INTERNET
BOOKMARKING
MICROBLOGGING
VIDEO
FORUM

Why Forward Error Correction (FEC)?

- Correction of detected errors usually requires data blocks to be retransmitted
- Not appropriate for wireless applications:
  - The bit error rate (BER) on a wireless link can be quite high, which would result in a large number of retransmissions
  - Propagation delay is very long compared to the transmission time of a single frame
- Need to correct errors on basis of bits received

Forward Error Correction (FEC)

- On the transmission end, each k-bit block of data is mapped into an n-bit block (n>k) called a codeword, using an FEC encoder.
- During transmission, the signal is subject to impairments, which may produce bit errors in the signal.
- This block is passed through an FEC decoder, with one of four possible outcomes:
  - No errors
  - Detectable, correctable errors
  - Detectable, not correctable errors
  - Undetectable errors

Forward Error Correction

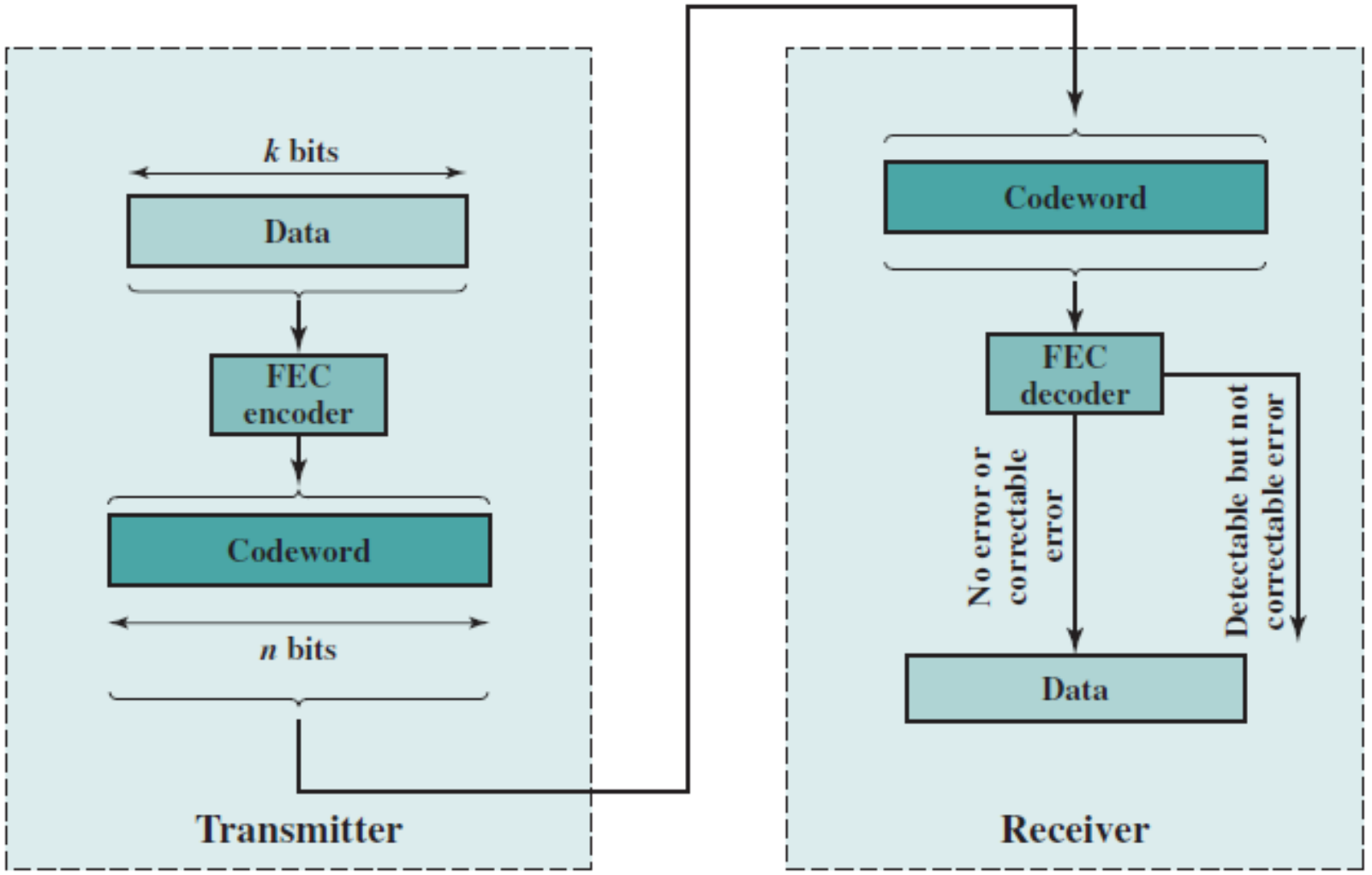


Figure 6.8 Error-Correction Process

Block Code Principles

- Hamming distance
  - d(v1, v2) between two n-bit binary sequences v1 and v2 is the number of bits in which v1 and v2 disagree

2 codewords

$$\mathbf{v}_1 = 011011, \quad \mathbf{v}_2 = 110001$$

$$d(\mathbf{v}_1, \mathbf{v}_2) = 3$$

- Code rate
  - The ratio of data bits to total bits, k/n
  - A measure of how much additional bandwidth is required to carry data

n is bigger after FEC coder

FEC

- Let the minimum distance between all valid codewords be d_{min}

For a code consisting of the codewords $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_s$, where $s = 2^n$, the minimum distance $d_{\min}$ of the code is defined as

$$d_{\min} = \min_{i \neq j} [d(\mathbf{w}_i, \mathbf{w}_j)]$$

- The maximum number of guaranteed correctable errors

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

means if get 2.5, t=2,向下靠近

- The maximum number of errors that can be detected is $d_{min} - 1$

Example: FEC

For $k = 2$ and $n = 5$, we can make the following assignment:

Data Block	Codeword
00	00000
01	00111
10	11001
11	11110

- Pairwise Hamming distance:

$$d(00000, 00111) = 3; \quad d(00000, 11001) = 3; \quad d(00000, 11110) = 4;$$
$$d(00111, 11001) = 4; \quad d(00111, 11110) = 3; \quad d(11001, 11110) = 3$$

- The minimum distance between all valid codewords, d_{min} is 3

The maximum number of guaranteed correctable errors is 1

The maximum number of errors that can be detected is 2

Example: FEC

find best match possible codeword(last page, total 4) based on the invalid one, ensure distance is small

Invalid Codeword	Minimum Distance	Valid Codeword	Invalid Codeword	Minimum Distance	Valid Codeword
00001	1	00000	10000	1	00000
00010	1	00000	10001	1	11001
00011	1	00111	10010	2	00000 or 11110
00100	1	00000	10011	2	00111 or 11001
00101	1	00111	10100	2	00000 or 11110
00110	1	00111	10101	2	00111 or 11001
01000	1	00000	10110	1	11110
01001	1	11001	10111	1	00111
01010	2	00000 or 11110	11000	1	11001
01011	2	00111 or 11001	11010	1	11110
01100	2	00000 or 11110	11011	1	11001
01101	2	00111 or 11001	11100	1	11110
01110	1	11110	11101	1	11001
01111	1	00111	11111	1	11110

Local Area Networks

IEEE 802 Model And Standards

- IEEE (*Institute of Electrical and Electronics Engineers*)
  - Professional society of engineers
  - Standardizes vendor-independent technologies
- Project 802
  - LAN/MAN standards committee
  - Organized in 1980
  - Focuses on layer 1 and layer 2 standards
  - Divides layer 2 into two sublayers
    - Logical Link Control (LLC): addressing and demultiplexing
    - Media Access Control (MAC): access to shared media

hardware

for diff user

IEEE 802 Protocol Layers

7 layers

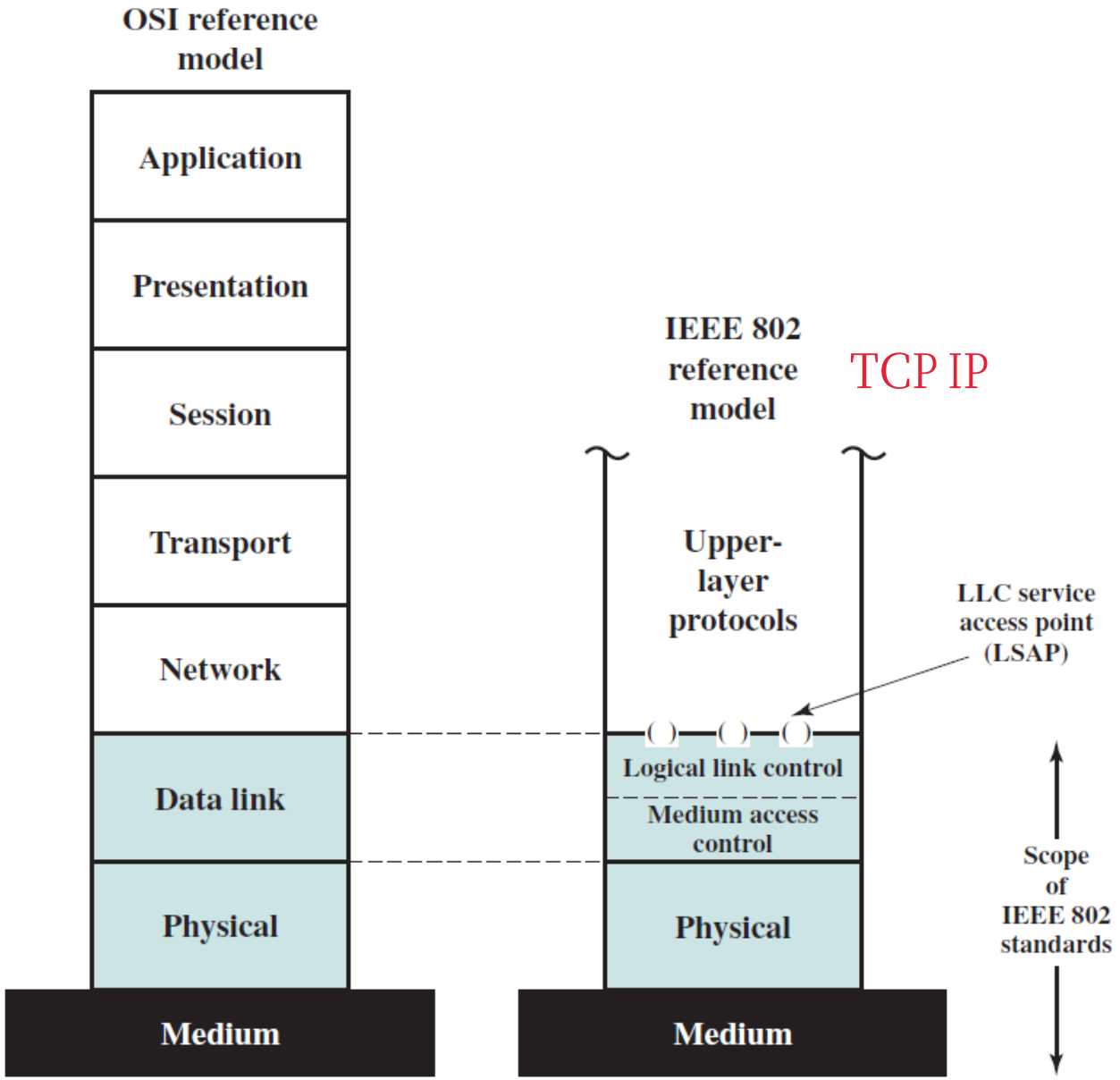


Figure 11.3 IEEE 802 Protocol Layers Compared to OSI Model

Selected IEEE Standards

ID	Topic
802.1	Higher layer LAN protocols
802.2	Logical link control
802.3	Ethernet
802.4	Token bus (disbanded)
802.5	Token Ring
802.6	Metropolitan Area Networks (disbanded)
802.7	Broadband LAN using Coaxial Cable (disbanded)
802.9	Integrated Services LAN (disbanded)
802.10	Interoperable LAN Security (disbanded)
802.11	Wireless LAN (Wi-Fi)
802.12	Demand priority

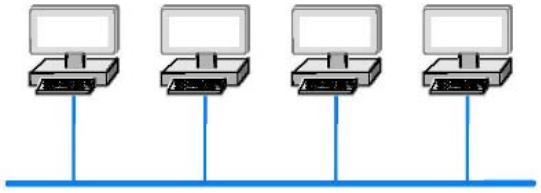
Standards Define …

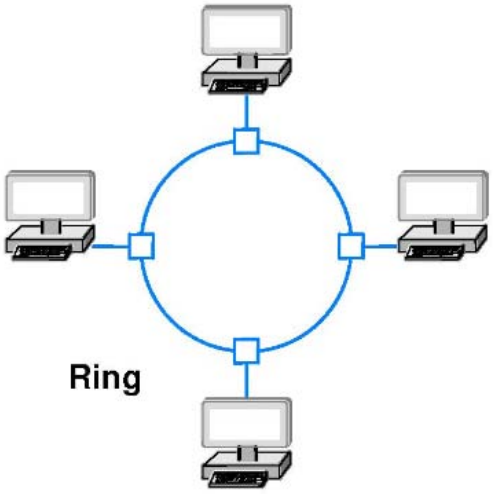
- Network topology (shape)
- Endpoint addressing scheme host
- Frame (packet) format
- Media access mechanism
- Physical layer aspects and wiring

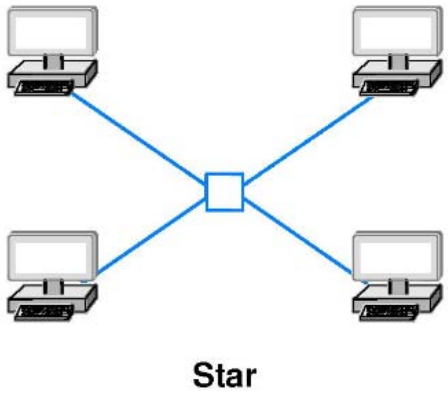
LAN Topologies

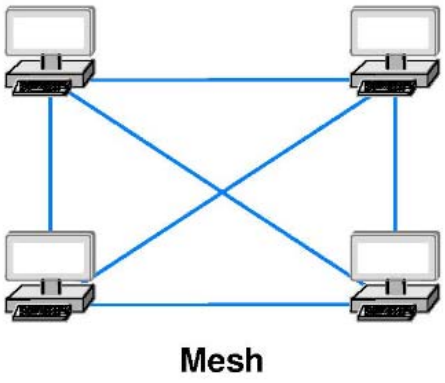
拓扑结构

- Each topology has advantages and disadvantages









LAN Topologies

Computer Networks

Part Four

LAN Topology

Source: Computer Science YouTube channel

LAN Protocols

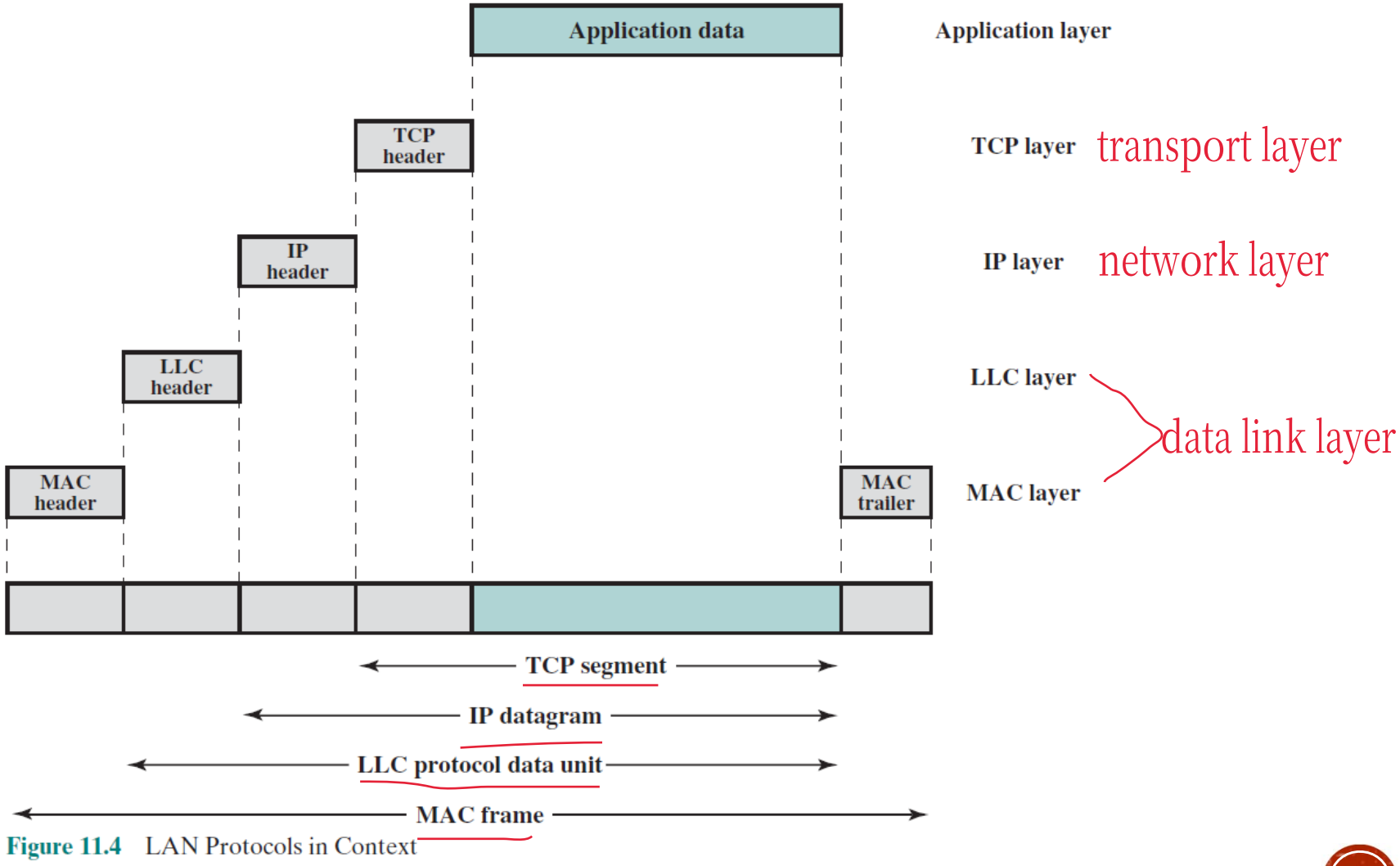


Figure 11.4 LAN Protocols in Context

Endpoint Addressing Scheme

host

- Each station on a LAN is assigned a unique address
- Each packet specifies a destination address

sent to where

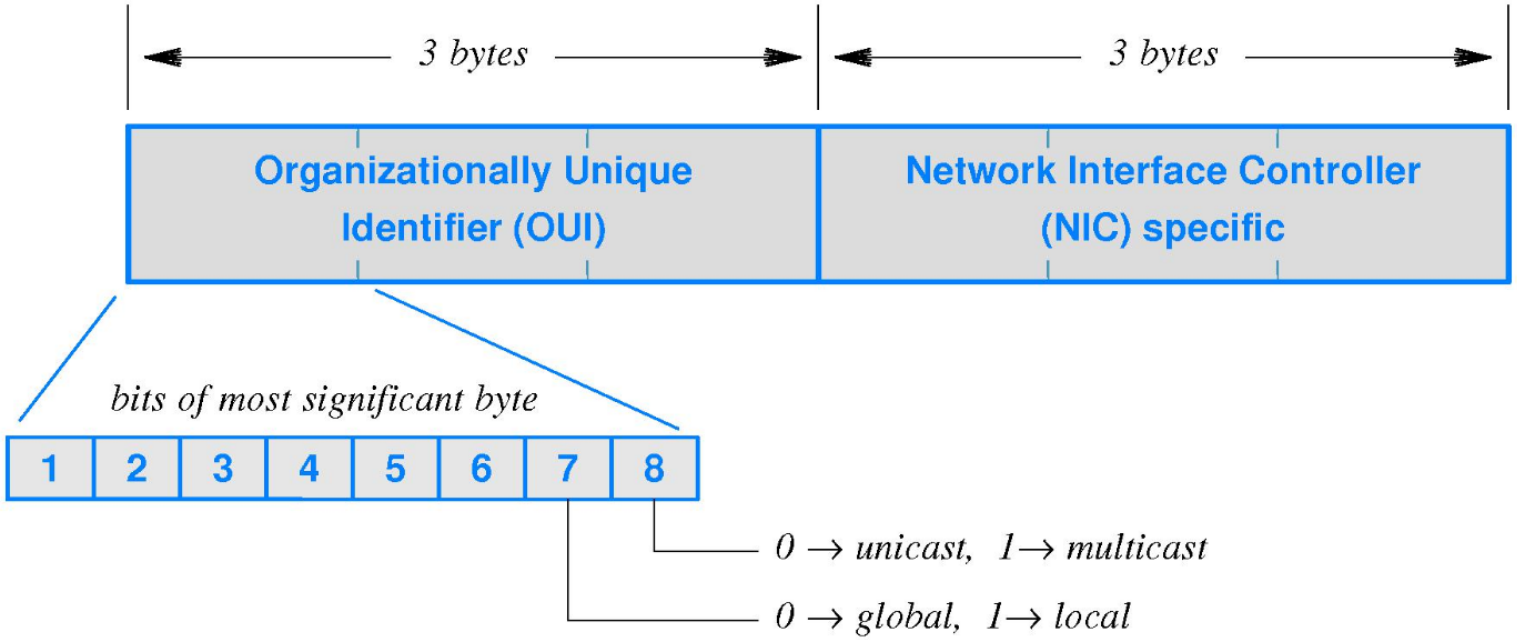
- LAN hardware uses the address in a packet to determine which station(s) receive a copy

MAC Address

physical address

- Formal name: *IEEE Media Access Control address (MAC address)*
- Informally called an *Ethernet address*
- Each address is 48 bits long 6 bytes
- Assigned to *Network Interface Card (NIC)* when device manufactured
- Divided into subfields 2
  - 3-byte *Organizationally Unique ID (OUI) - identifies the equipment vendor*
  - 3-byte *Network Interface Controller (NIC)*

MAC Address Format



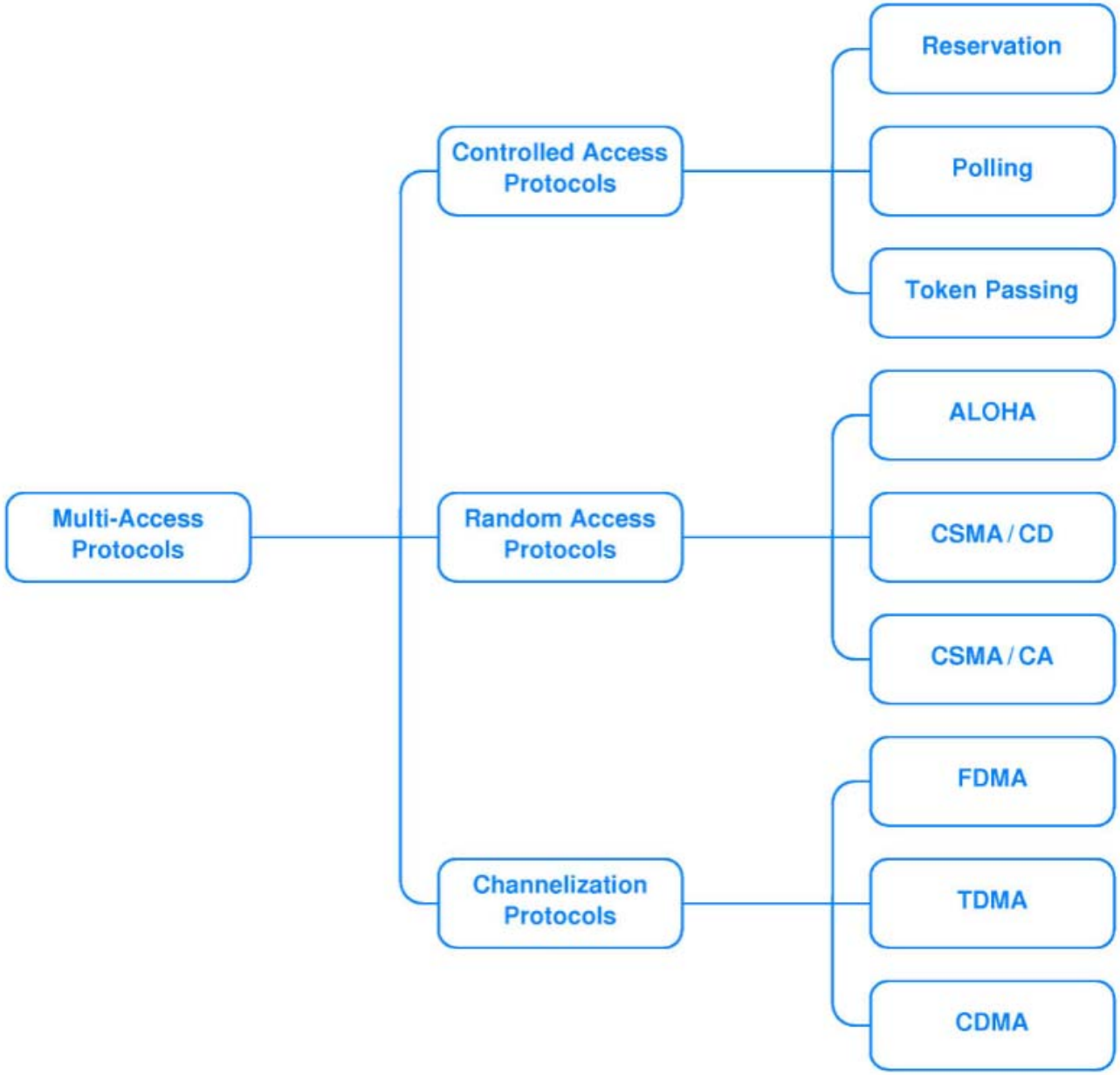
Media Access Control (MAC)

Key Concept

Static channel allocation suffices when the set of communicating entities is known in advance and does not change; most networks require a form of dynamic channel allocation.

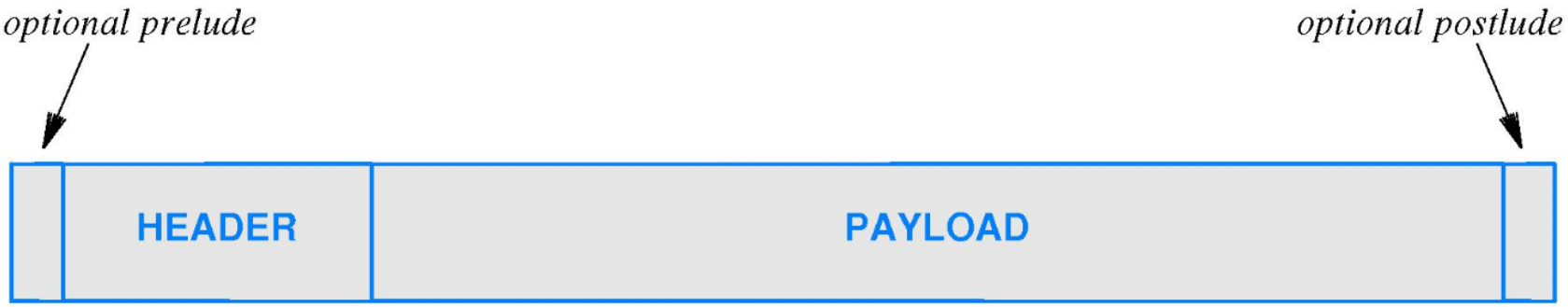
- Control access to shared medium
- Two types of channel allocation
  - Static
  - Dynamic

Media Access Mechanisms



Layer 2 Frame

- Layer 2 packet is called a frame
- General layout of a frame



- Header usually has fixed fields
- Each technology imposes a maximum payload size

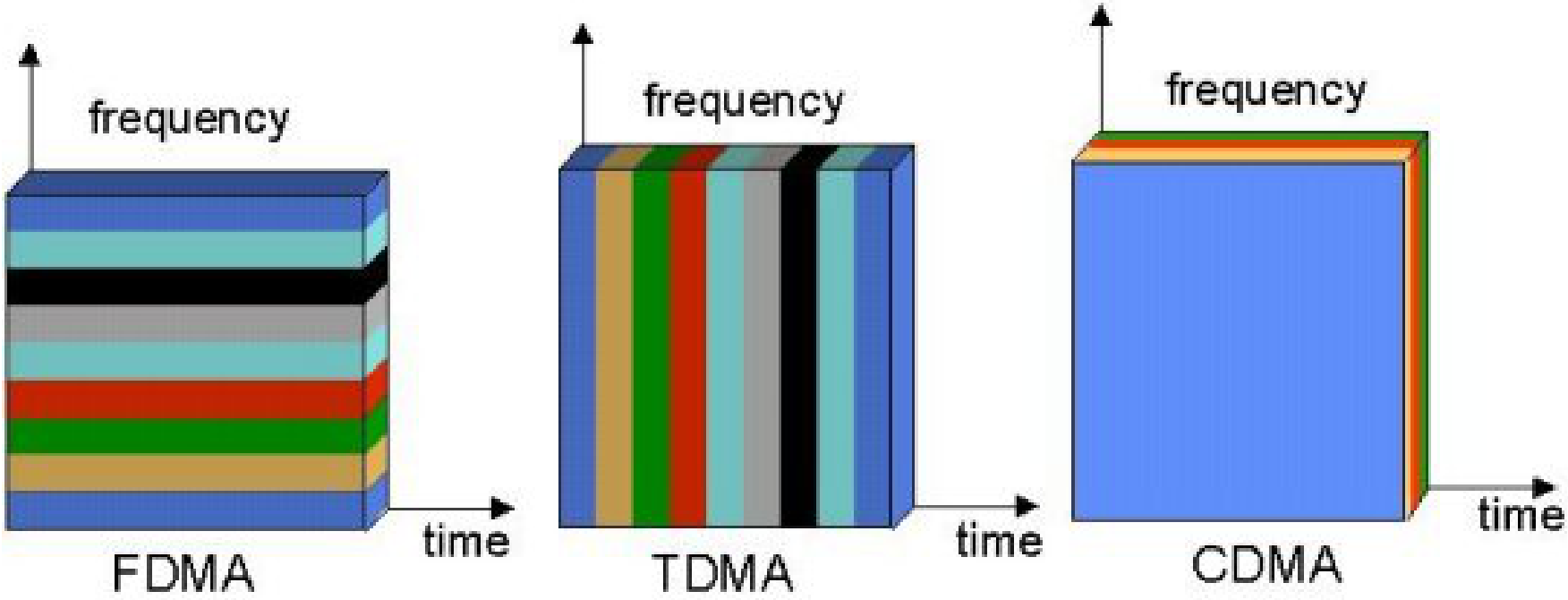
Channelization Protocols

multiply users can share and transmit through same medium

- Employ and extend basic multiplexing techniques
- Three basic types

Protocol	Expansion
FDMA	Frequency Division Multi-Access
TDMA	Time Division Multi-Access
CDMA	Code Division Multi-Access

FDMA vs TDMA vs CDMA



divide to multiple freq. band

each user can use one band at same time

Source: cis-india.org

Controlled Access Protocols

- Three principal forms
- All three have been used in practice

ask each user if want to transmit data one by one, if want, just transmit one packet, if not, just skip, poll one user one by one

Type	Description
Polling	Centralized controller repeatedly polls stations, and allows each to transmit one packet
Reservation	Stations submit a request for the next round of data transmission
Token Passing	Stations circulate a token; each time it receives the token, a station transmits one packet

Algorithm For Polled Access

Purpose:

Control transmission of packets through polling

Method:

Controller repeats forever {

Select a station, S, and send a polling message to S;

Wait for S to respond by sending a packet or passing;

}

Algorithm For Reservation-Based Access

- Often used with satellite systems
- Stations inform a controller if they have data to send

Purpose:

Control transmission of packets through reservation

Method:

Controller repeats forever {

Form a list of stations that have a packet to send;

Allow each station on the list to transmit;

}

Algorithm For Token Passing Access

- Special packet known as a *token* passed among senders
- Station sends one packet each time token arrives

Purpose:

Control transmission of packets through token passing

Method:

Each computer on the network repeats {

Wait for the token to arrive;

Transmit a packet if one is waiting to be sent;

Send the token to the next station;

}

Example Random Access Protocols

Type	Description
ALOHA	Historic protocol used in an early radio network in Hawaii; popular in textbooks and easy to analyze, but not used in real networks
CSMA / CD	Carrier Sense Multi-Access with Collision Detection The basis for the original Ethernet, but no longer used with switched Ethernet
CSMA / CA	Carrier Sense Multi-Access with Collision Avoidance The basis for Wi-Fi wireless networks

CSMA/CD (1)

- Used in original Ethernet (1973)
- Provides access to shared medium
- Principle features
  - Carrier Sense (CS)
  - Multiple Access (MA)
  - Collision Detection (CD)
- Uses binary exponential backoff

CSMA/CD (2)

- Carrier Sense
  - Instead of allowing a station to transmit whenever a packet becomes ready, Ethernet requires each station to monitor the cable to detect whether another transmission is already in progress.

- Collision Detection
  - To handle collisions, each station monitors the cable during transmission. If the signal on the cable differs from the signal that the station is sending, it means that a collision has occurred. When a collision is detected, the sending station aborts transmission.

CSMA/CD (3)

- Binary Exponential Backoff
  - After a collision occurs, a computer must wait for the cable to become idle again before transmitting a frame. The standard specifies a maximum delay, d, and requires each station to choose a random delay less than d after a collision occurs. Doubling the range of the random delay after each collision is known as binary exponential backoff.

CSMA/CD Algorithm

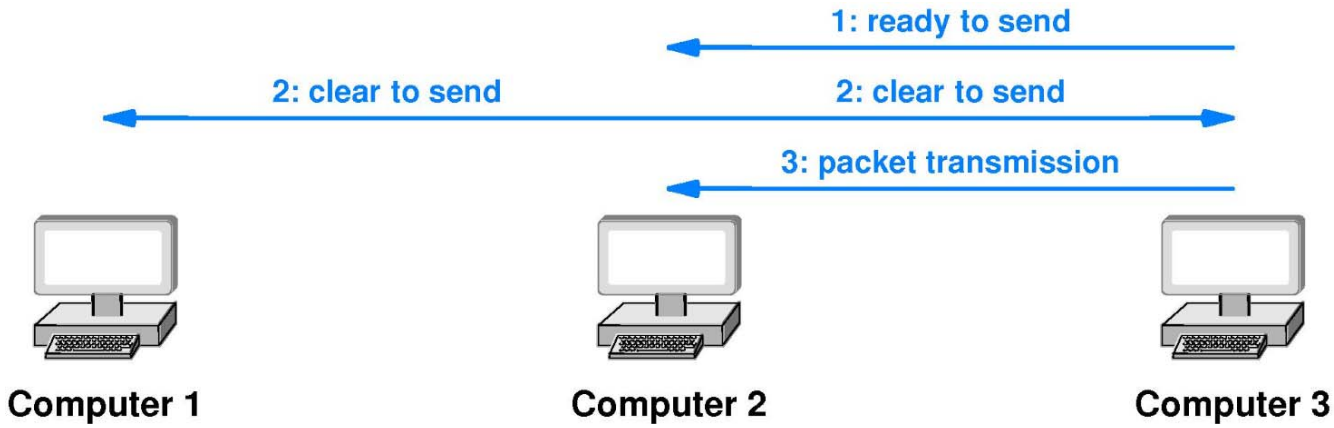
1. If the medium is idle, transmit; otherwise, go to step 2.
2. If the medium is busy, continue to listen until the channel is idle, then transmit immediately.
3. If a collision is detected during transmission, transmit a brief jamming signal to assure that all stations know that there has been a collision and then cease transmission.
4. After transmitting the jamming signal, wait a random amount of time, referred to as the backoff, then attempt to transmit again (repeat from step 1).

CSMA/CA

- Alternative to CSMA/CD
- Used in wireless networks (Wi-Fi)
- Needed because signals have limited distance, δ
- Example:
  - Computer 1 can communicate with computer 2, but cannot receive the signal from computer 3. Thus, if computer 3 is transmitting a packet to computer 2, computer 1's carrier sense mechanism will not detect the transmission. Similarly, if computers 1 and 3 simultaneously transmit, only computer 2 will detect a collision.

CSMA/CA

- Instead of depending on all other computers to receive all transmissions, the CSMA/CA in wireless LANs triggers a brief transmission from the intended receiver before transmitting a packet. The idea is that if both the sender and receiver transmit a message, all computers within range of either will know a packet transmission is beginning.
- Communicating pair exchange Request-to-Send (RTS) and Clear-to-Send (CTS) before packet transmission



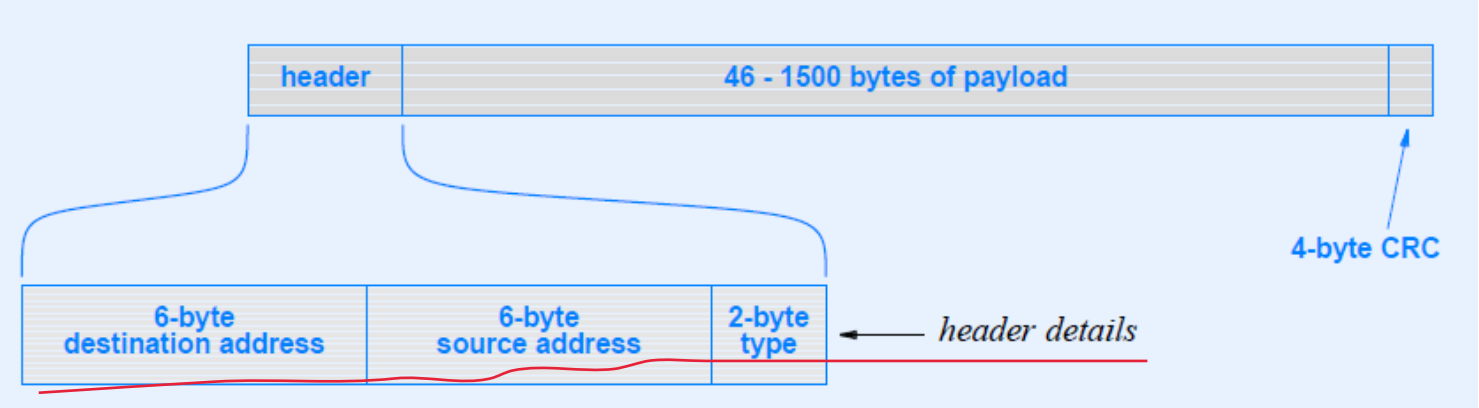
Wired and Wireless LAN

Wired LAN Technologies

- Explosion of technologies and products during 1980s
- Consolidation during the 1990s
- Currently: one de facto wired LAN standard - Ethernet

Ethernet Technology

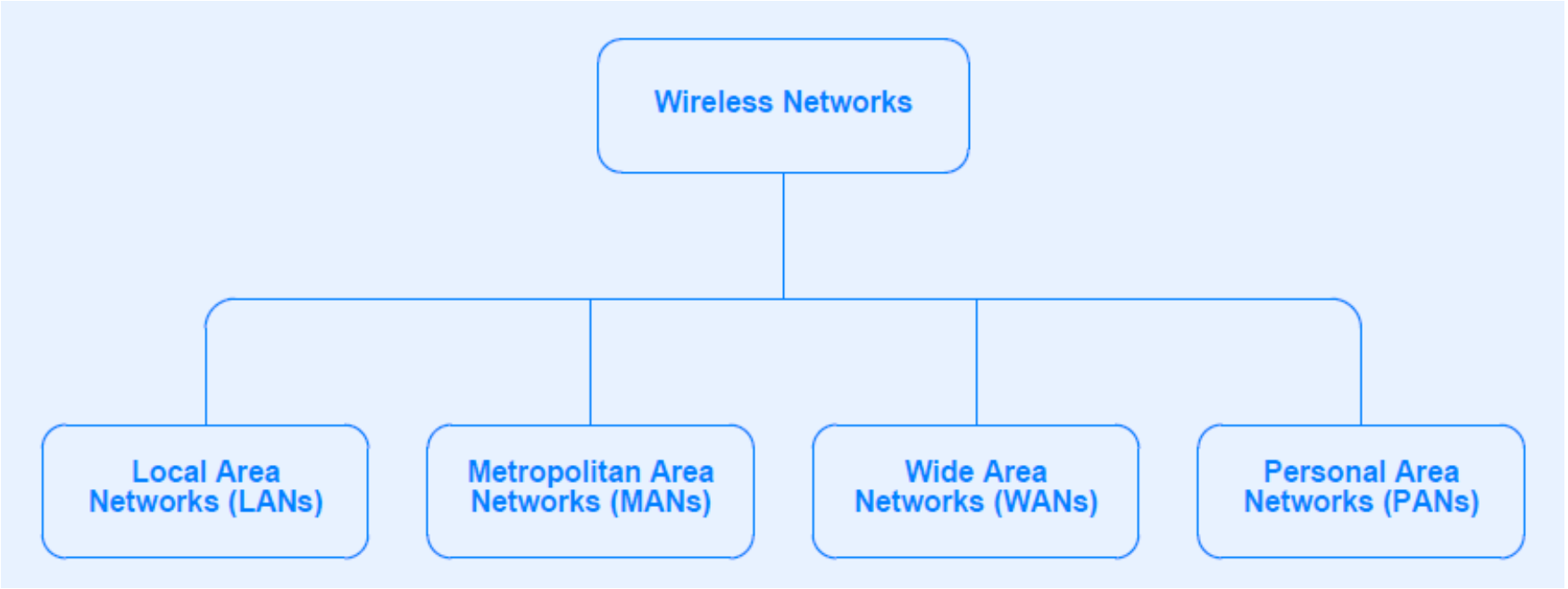
- Invented at Xerox PARC in 1973
- Standardized by Digital, Intel, and Xerox (DIX) in 1978
- Frame has a 14-byte header followed by payload of 46 to 1500 bytes
- Frame format and addressing have survived virtually unchanged



Wireless Networks

- Many types exist
- Technologies differ in
  - Distance spanned
  - Data rates
  - Physical characteristics of electromagnetic energy
    - Ability to permeate obstructions like walls
    - Susceptibility to interference

Taxonomy of Wireless Networks



Wireless LANs And Wi-Fi

- Variety of wireless LANs have been created
- Vendors moved to open standards in 1990s, with IEEE providing most of the standards under 802.11
- In 1999, vendors formed Wi-Fi Alliance
- Example IEEE wireless standards

IEEE Standard	Frequency Band	Data Rate	Modulation Technique	Multiplexing Technique
original 802.11	2.4 GHz	1 or 2 Mbps	FSK	DSSS
	2.4 GHz	1 or 2 Mbps	FSK	FHSS
	InfraRed	1 or 2 Mbps	PPM	– none –
802.11b	2.4 GHz	5.5 and 11 Mbps	PSK	DSSS
802.11g	2.4 GHz	22 and 54 Mbps	various	OFDM
802.11n	2.4 GHz	54 to 600 Mbps	various	OFDM

Part 4: Network Layer & Technologies

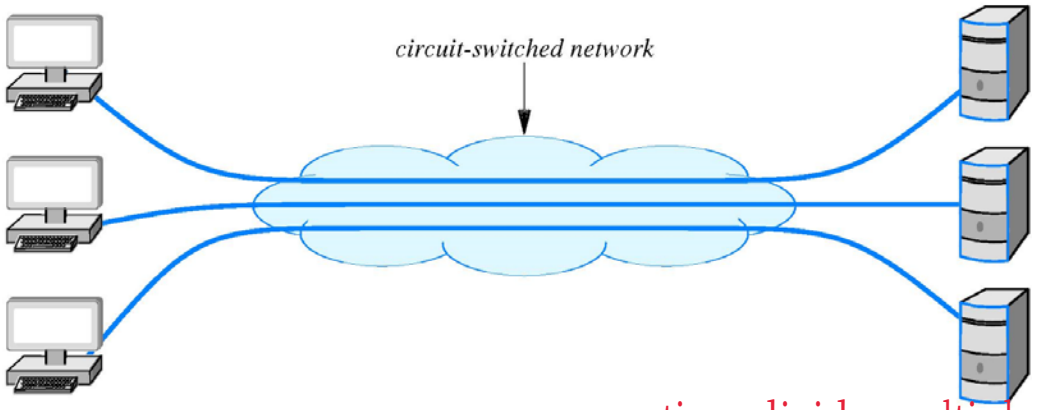
Networks

think like host or PC

- Attach multiple endpoints
- Two broad categories
  - Circuit switched
  - Packet switched

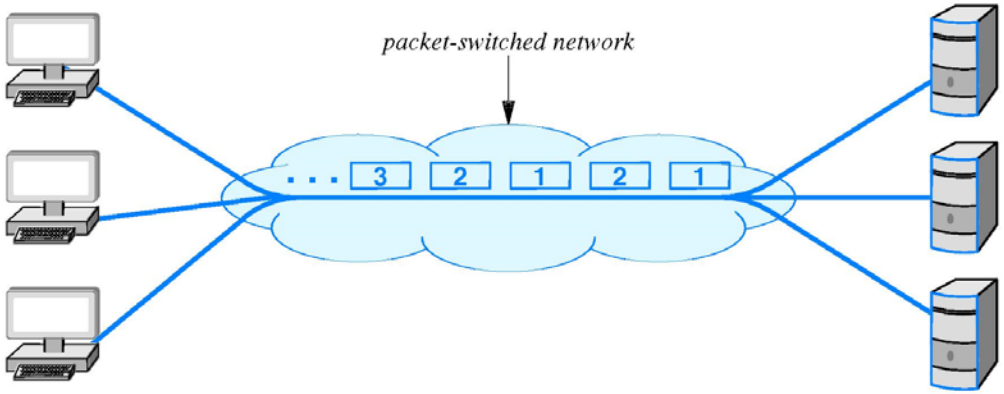
Circuit vs Packet Switching

- Circuit switching provides 1-to-1 dedicated connections



time divide multiplexing

- Packet switching provides statistical TDM sharing

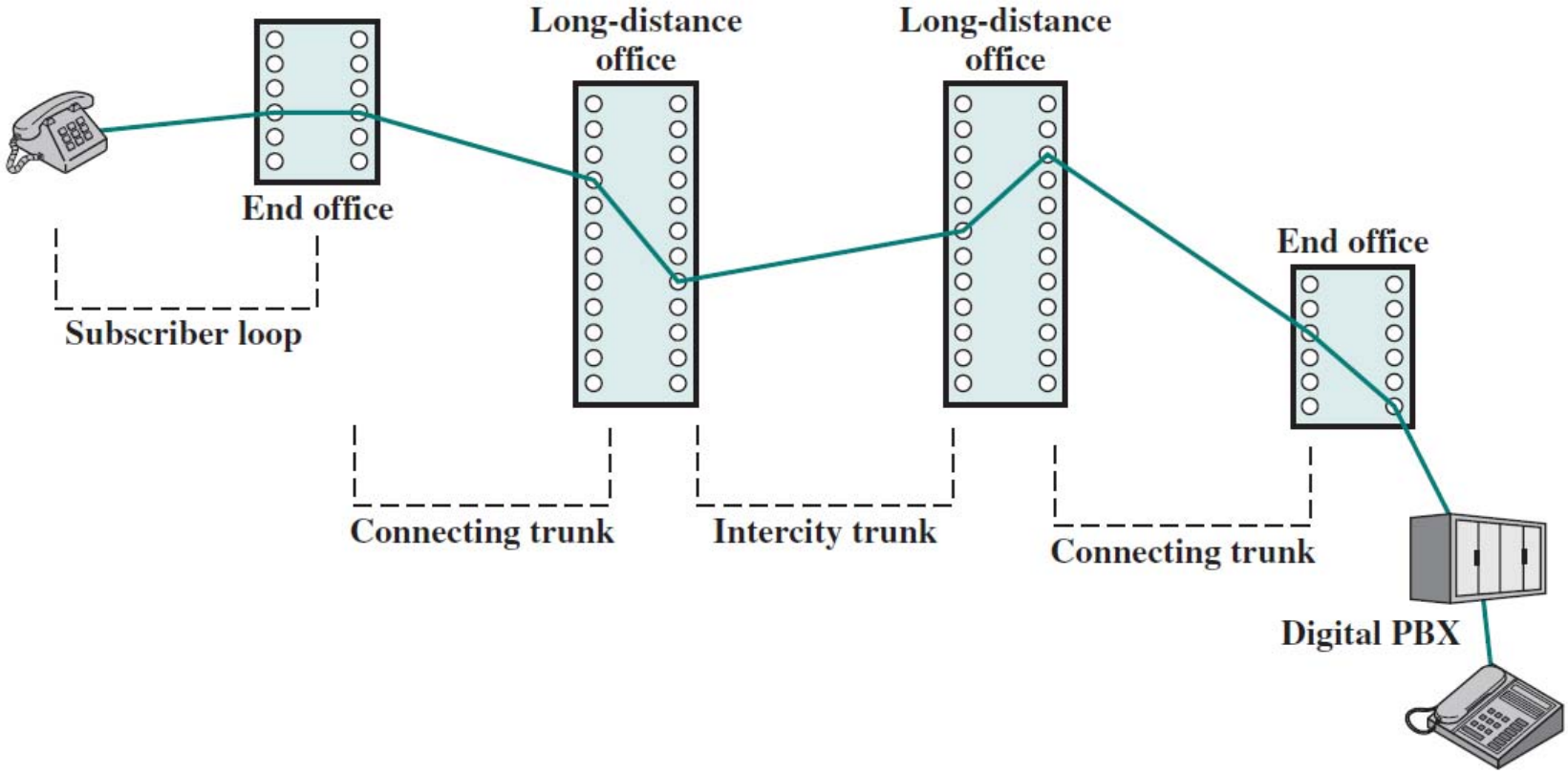


Circuit Switched Networks

- Provide point-to-point communication between pairs of endpoints
- Establish path between sender and receiver
- Separate steps for circuit creation, use, and termination
- Performance equivalent to an isolated physical path
- Circuit can be
  - Permanent/ provisioned (left in place for long periods)
  - Switched (created on demand)
- Concept: user leases piece of underlying infrastructure for a time period

transmit

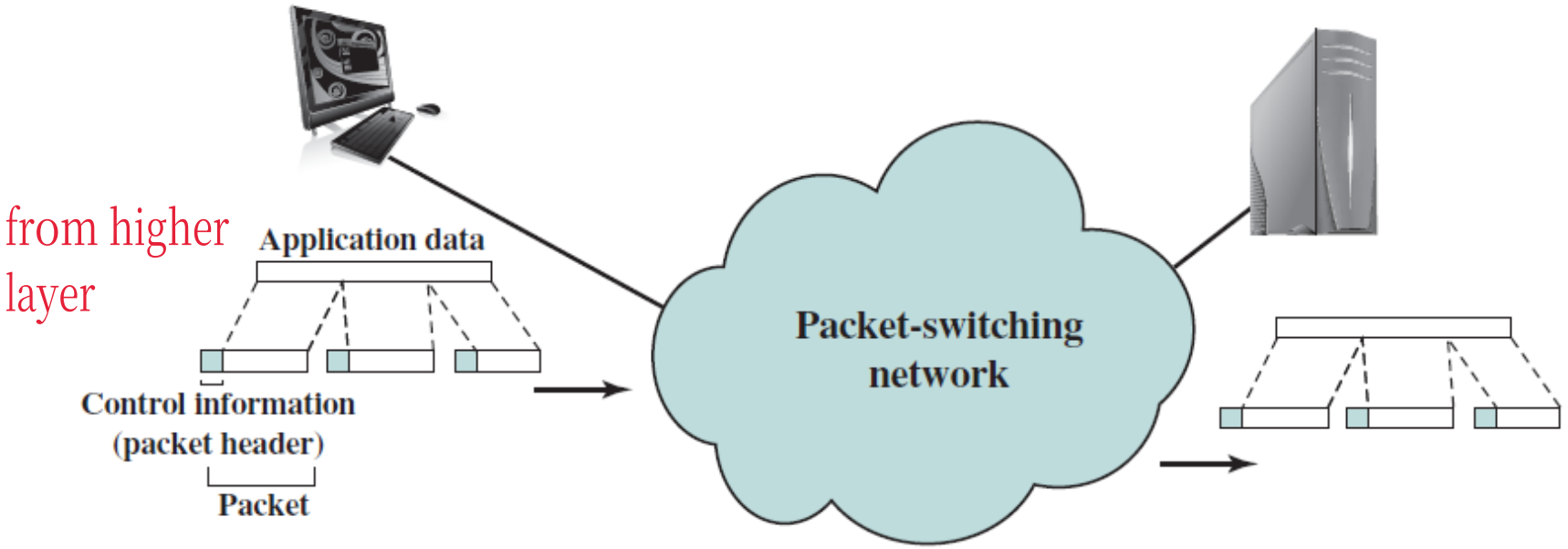
Circuit-Switching Network



Packet Switched Networks

- Form the basis for the Internet
- Multiplex communication over shared media
- All data divided into packets
- After sending one packet, sender allows others a chance to transmit before sending a second packet
- Arbitrary, asynchronous communication
- No set-up required before communication begins
- Performance varies due to statistical multiplexing
- Concept: underlying infrastructure is shared among users

Packet-Switching Network



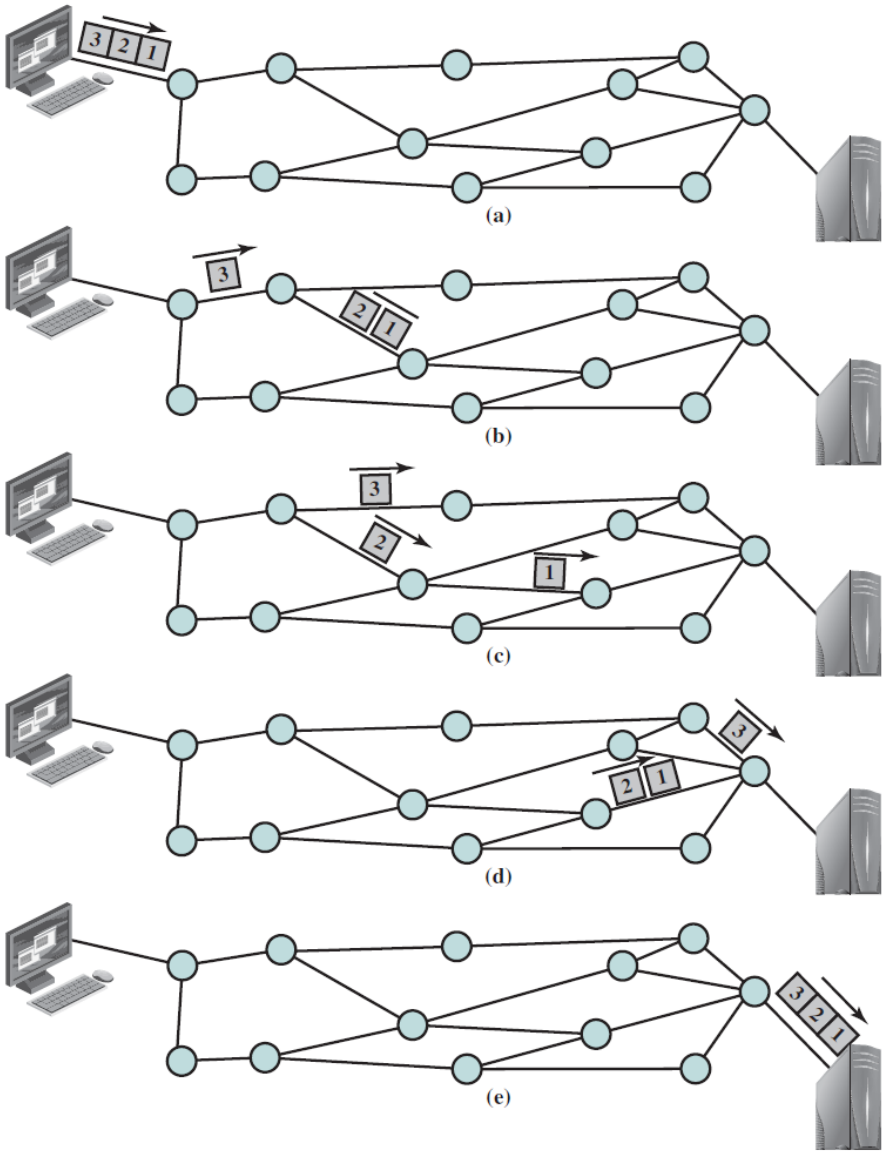
Packet Switching

- Circuit switching was designed for voice
- Packet switching was designed for data
- Transmitted in small packets
- Packets contain user data and control info
  - User data may be part of a larger message from top layer
  - Control information includes routing (addressing)
- Packets are received, stored briefly (buffered) and passed on to the next node

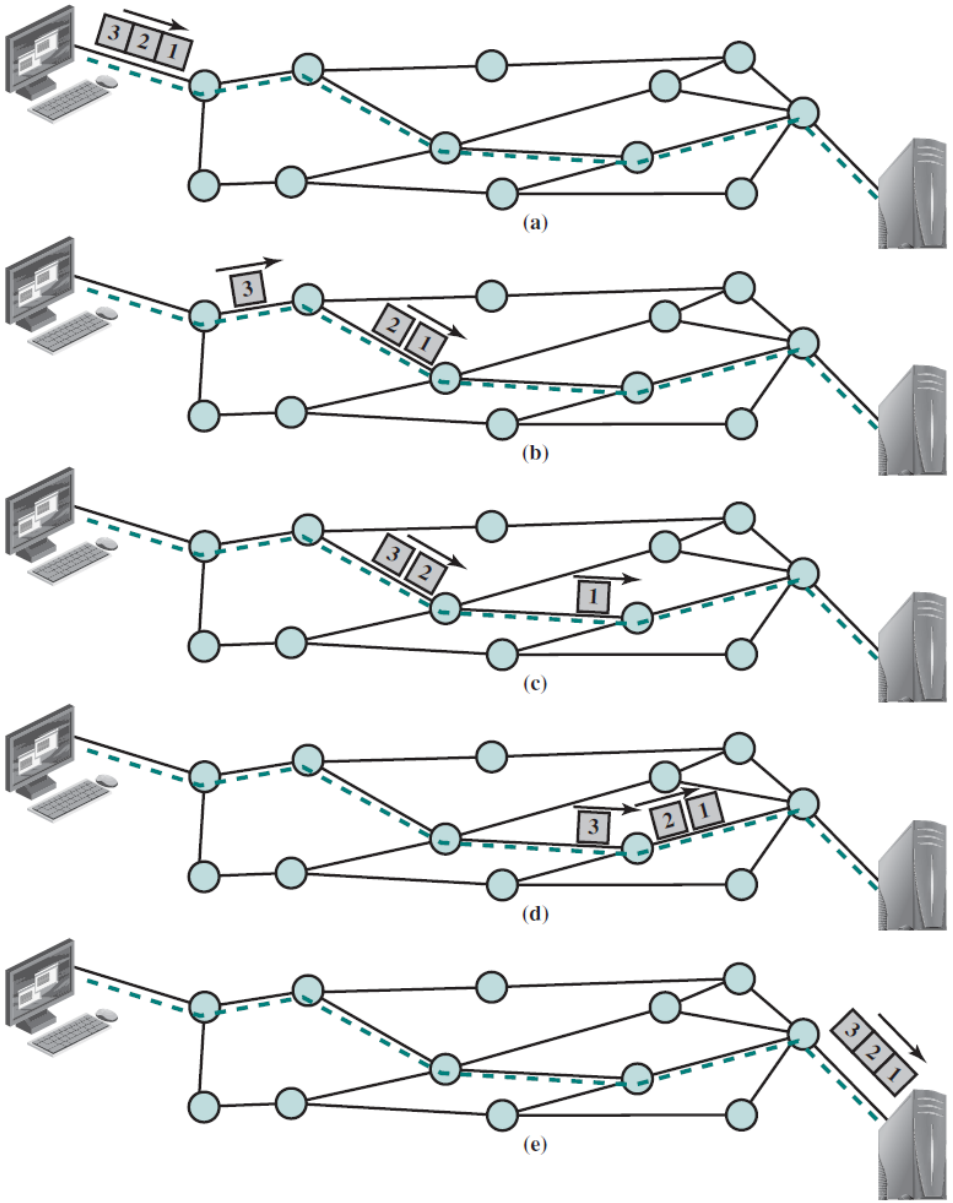
Packet Switching Techniques

- Packets can be handled in two ways:
- Datagram
  - Each packet is treated independently with no reference to previous packets
- Virtual circuit
  - A pre-planned route is established before any packets are sent

Packet Switching: Datagram



Packet Switching: Virtual-Circuit



Comparison of Switching Techniques

Circuit Switching	Datagram Packet Switching	Virtual Circuit Packet Switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Messages are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; packet transmission delay
Busy signal if called party busy	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each packet	Overhead bits in each packet

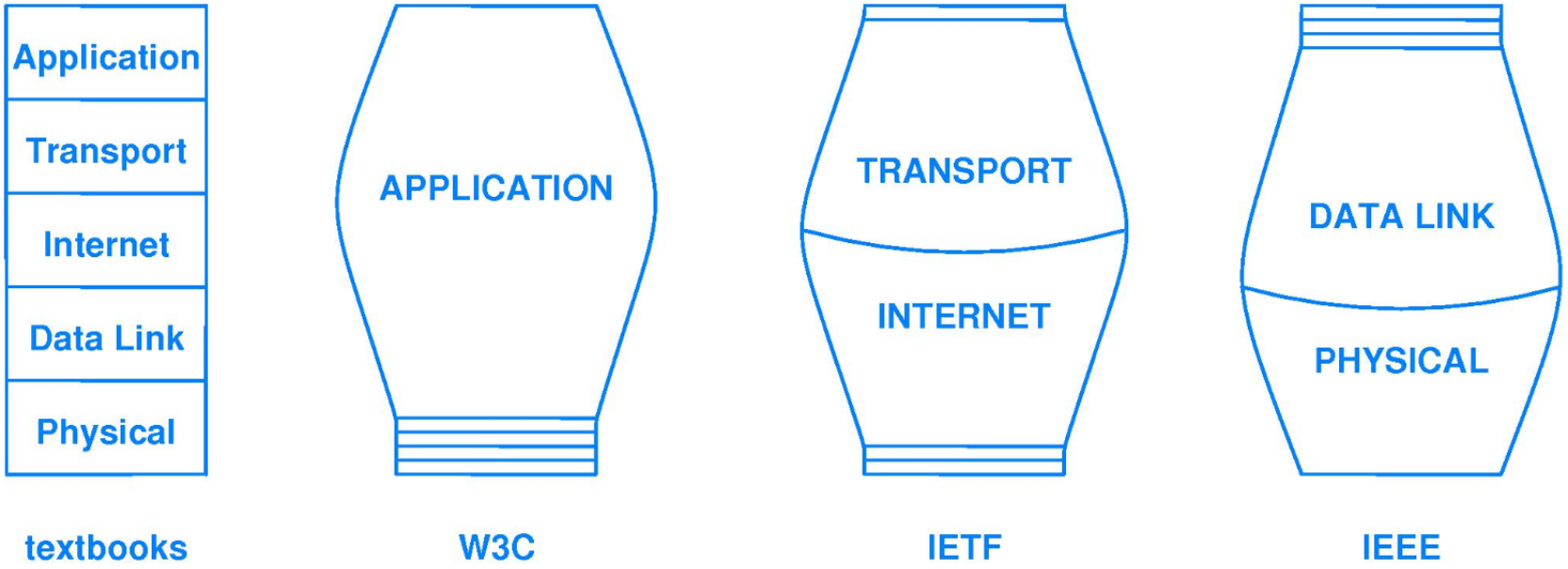
Types of Packet Switched Networks

Name	Expansion	Description
LAN	Local Area Network	Least expensive; spans a single room or a single building
MAN	Metropolitan Area Network	Medium expense; spans a major city or a metroplex
WAN	Wide Area Network	Most expensive; spans sites in multiple cities

Name	Expansion	Description
PAN	Personal Area Network	Spans the area around an individual used for earphones
SAN	Storage Area Network	Spans the distance between a disk farm and processors in a data center
CAN	Chip Area Network	Spans a single chip and connects processor, memories, etc.

Standards Bodies and Their Bias

- Standards bodies and academic departments each emphasize certain layers of a protocol stack, leading to the following views



Networking Concepts

What Is The Internet?

- Users see it as services and applications
  - Web and e-commerce
  - Email, texting, instant messenger
  - Social networking and blogs
  - Music and video download (and upload)
  - Voice and video teleconferencing
- Networking professionals see it as infrastructure
  - Platform on which above services run
  - Grows rapidly

Internet Philosophy

- Infrastructure
  - Provides a packet communication service
  - Treats all attached endpoints as equal (any endpoint can send a packet to any other endpoint)
  - Does not restrict or dictate packet contents
  - Does not restrict or dictate underlying network technologies
- Attached endpoints
  - Run applications that use the network to communicate with applications on other endpoints
  - Control all content and provide all services

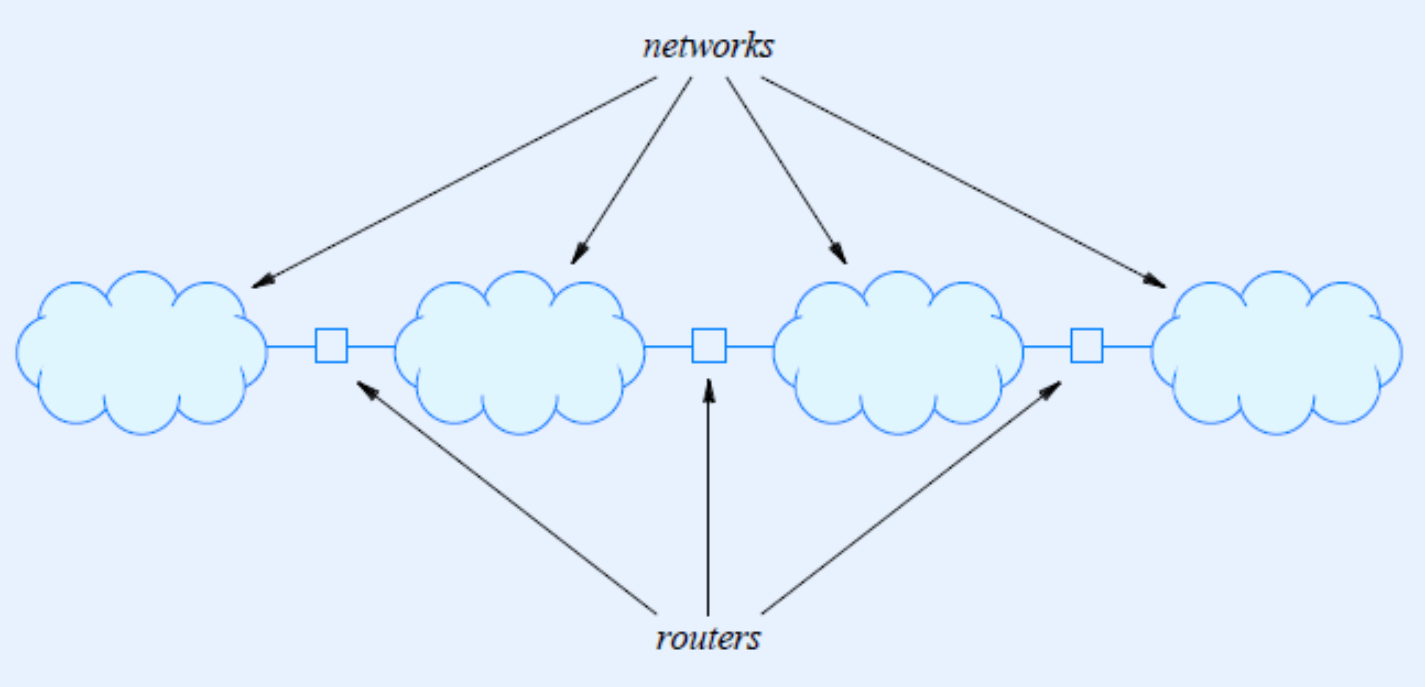
Advantages of Internet Philosophy

diff

- Accommodates heterogeneous underlying networks
- Accommodates arbitrary applications and services
- Separates communication from services

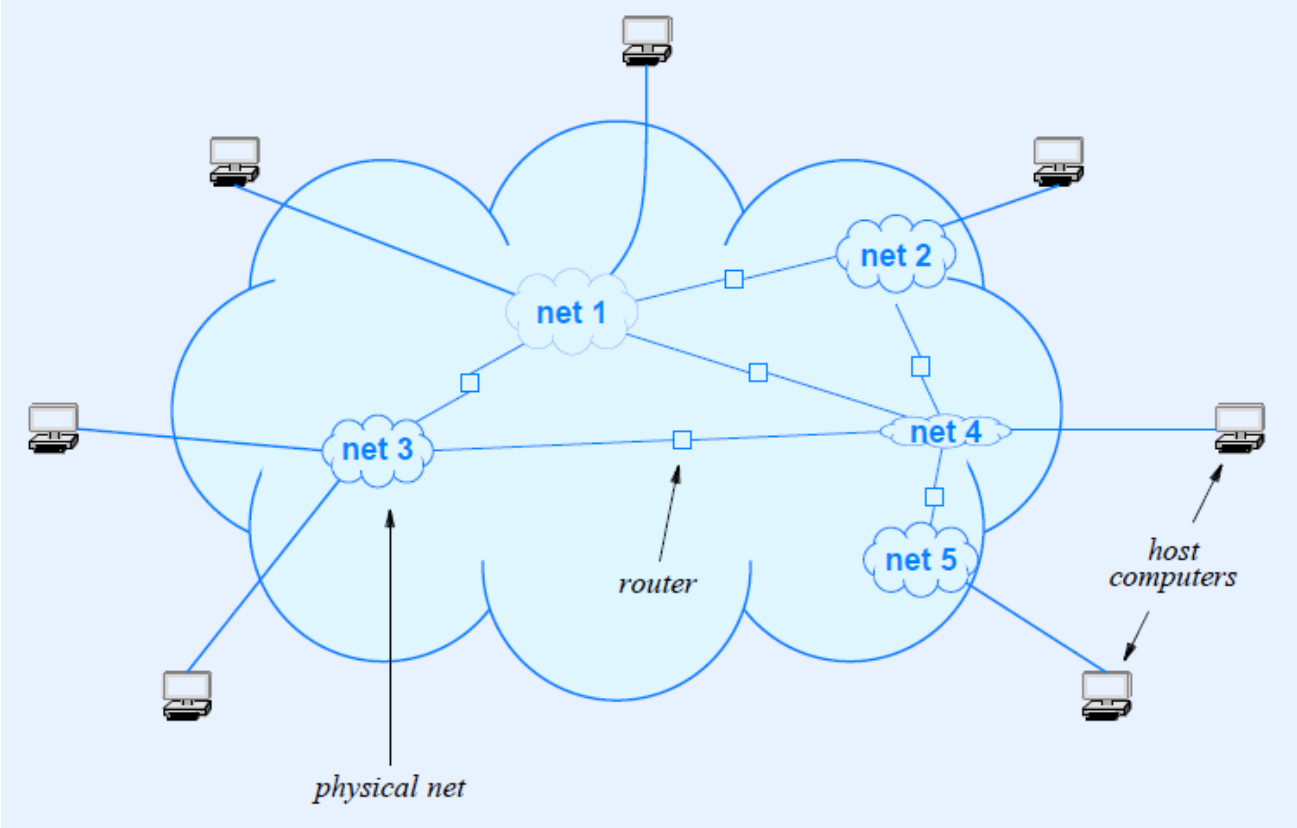
Internet

- Follows *a network of networks* approach
- Allows arbitrary networks to be included
- Uses *IP routers* to interconnect individual networks
- Permits each router to connect two or more networks



Internet Architecture

- Network of heterogeneous networks connected by routers
- Each host attaches to a network



Internet Protocol (IP)

Current Situation

- Internet addressing is defined by the *Internet Protocol (IP)*
- IP is changing
  - Current version is 4 (IPv4)
  - New version is 6 (IPv6)

History of Internet Protocol

- IP separated from TCP in 1978
- Version 1-3 discarded quickly; version 4 was the first version used by researchers
- By early 1990s, a movement started that clamored for a new version of IP because the 32-bit address space would run out “soon”
- In 1993, the IETF received proposals, and formed a working group to find a compromise
- By 1995, a new version had been proposed and documents written

Networking Terms (1)

Communication Network
A facility that provides a data transfer service among devices attached to the network.

Internet
A collection of communication networks interconnected by bridges and/or routers.

Intranet
An internet used by a single organization that provides the key Internet applications, especially the World Wide Web. An intranet operates within the organization for internal purposes and can exist as an isolated, self-contained internet, or may have links to the Internet.

Subnetwork
Refers to a constituent network of an internet. This avoids ambiguity because the entire internet, from a user's point of view, is a single network.

End System (ES)
A device attached to one of the networks of an internet that is used to support end-user applications or services.

Networking Terms (2)

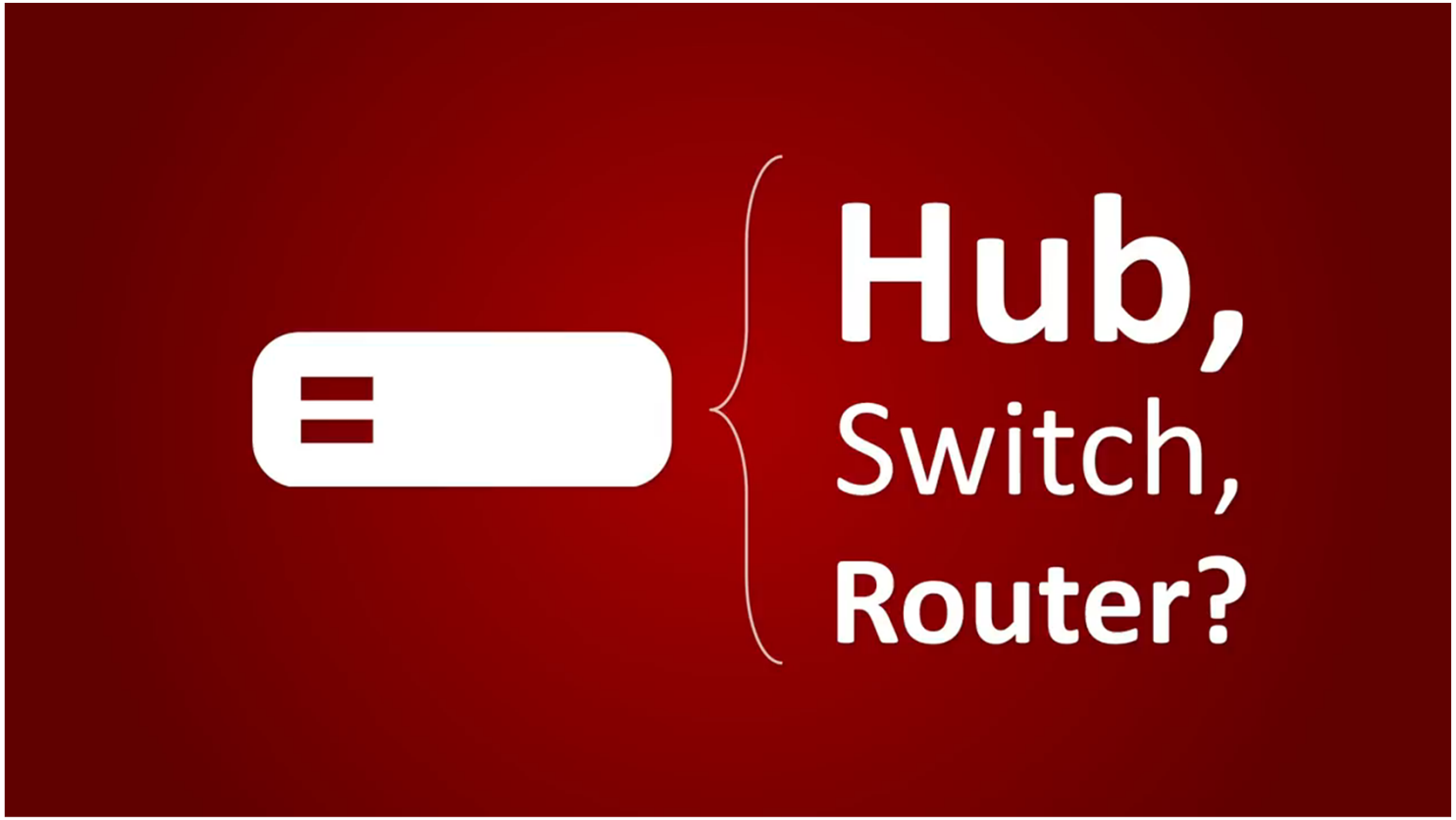
Intermediate System (IS)
A device used to connect two networks and permit communication between end systems attached to different networks.

Bridge
An IS used to connect two LANs that use similar LAN protocols. The bridge acts as an address filter, picking up packets from one LAN that are intended for a destination on another LAN and passing those packets on. The bridge does not modify the contents of the packets and does not add anything to the packet. The bridge operates at layer 2 of the OSI model.

Router
An IS used to connect two networks that may or may not be similar. The router employs an internet protocol present in each router and each end system of the network. The router operates at layer 3 of the OSI model.

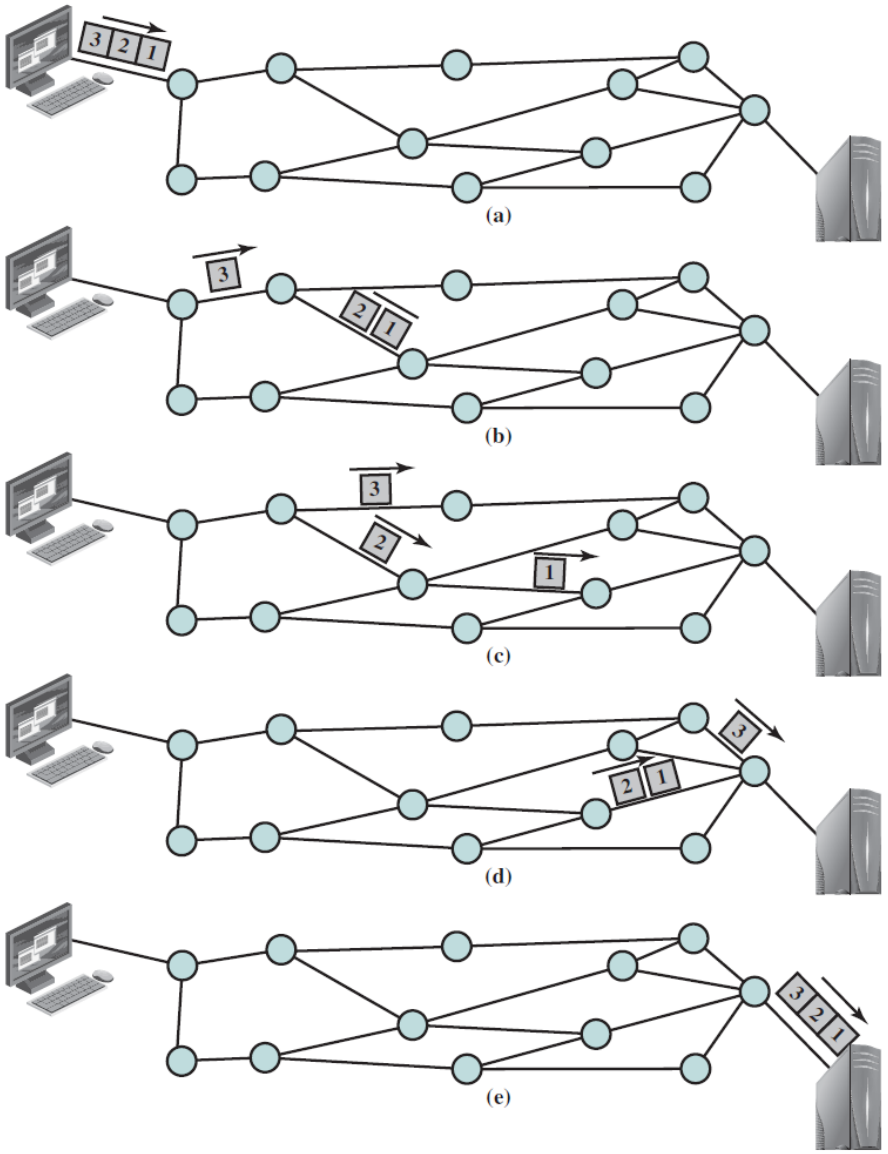
network/
Internet layer

Which Device to Use?

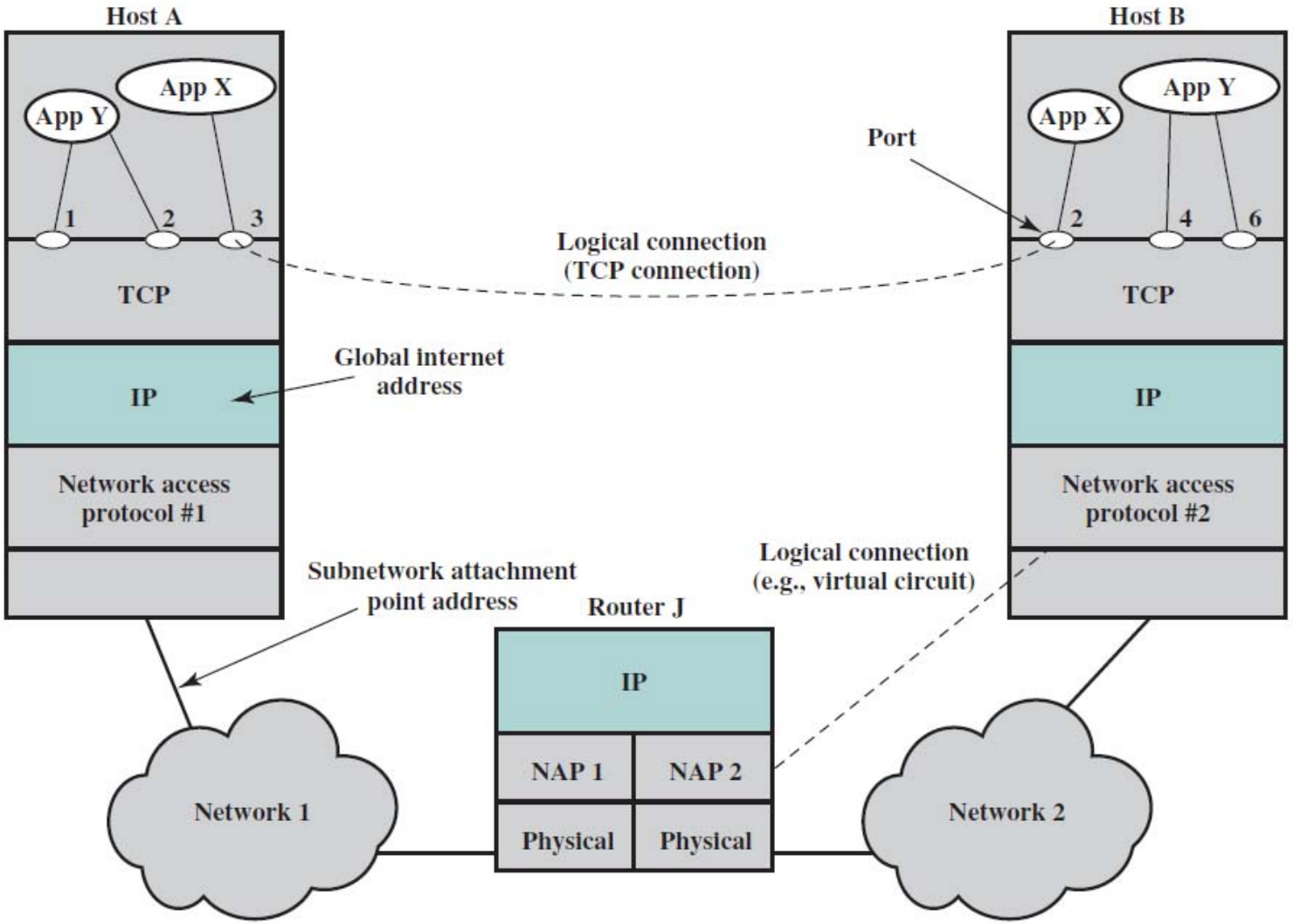


Source: Maddy's World

Recap: Packet Switching



TCP/IP Concepts



Addressing in The Internet

- Can we use MAC addresses across an internet?
- No: heterogeneity means
  - Multiple types of MAC addresses
  - MAC address meaningful on one network not meaningful on another
- Solution
  - Create new addressing scheme that is independent of MAC addresses

IP Addresses

- Identity
  - Unique number assigned to each endpoint
  - Analogous to Ethernet address

类似

- Locator
  - Endpoint address encodes location information, such as
    - Geographic location
    - Location relative to a service provider
    - Computer on a given physical network
- Addressing is inherently linked to routing; the choice of an addressing scheme affects the cost of computing and maintaining routes

IPv4 Addressing Scheme

- Unique number is assigned to each Internet host
- 32-bit binary value known as IPv4 address
- Virtual address, not derived from MAC address
- Divided into two parts
  - Prefix identifies physical network (locator) indicate network address
  - Suffix identifies a host on the network (identity) indicate host address

Dotted Decimal Notation (IPv4)

- Convenient for humans
- Divides IPv4 address into octets of eight bits each
- Represent each octet in decimal separated by dots
- Example

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129.52.6.0
11000000 00000101 00110000 00000011	192.5.48.3
00001010 00000010 00000000 00100101	10.2.0.37
10000000 00001010 00000010 00000011	128.10.2.3
10000000 10000000 11111111 00000000	128.128.255.0

Division between Prefix and Suffix

- Original scheme (*classful addressing*)
  - Each address divided on octet (8-bit) boundary

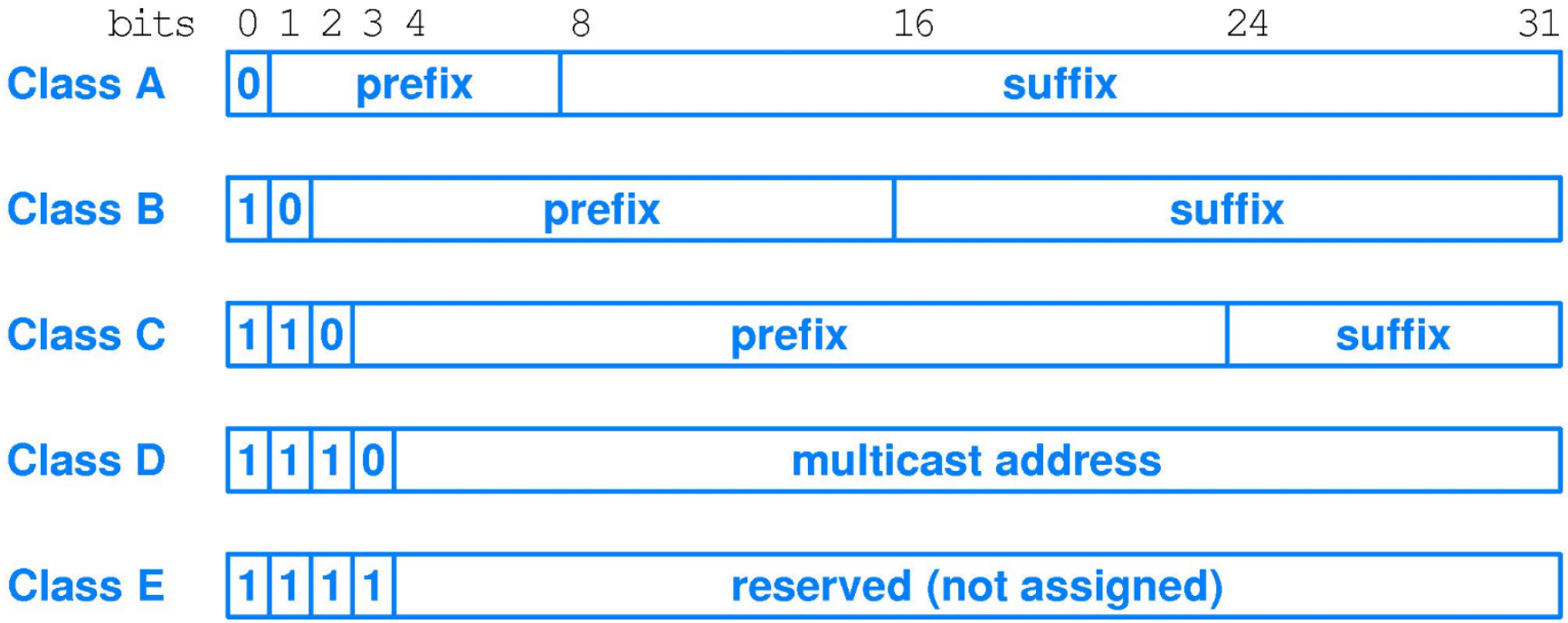
- Current scheme (*classless addressing*)
  - Formal name *Classless Inter-Domain Routing (CIDR)*
  - Division permitted at arbitrary bit position
  - Boundary must be specified external to the address

过时了，不用了

Classful Addressing

- Now historic
- Explains IPv4 multicast range

total 32 bits



Address Mask

- Required with classless addressing
- Specifies division of addresses into network prefix and host suffix for that network
- 32-bit binary value
  - 1-bits correspond to prefix
  - 0-bits correspond to suffix
- Example mask that specifies six bits of prefix

11111100 00000000 00000000 00000000

CIDR Notation

- Used by humans to enter address mask
- Avoids dotted decimal errors
- Follows address with slash and integer X, where X is the number of prefix bits
- Example
  - In dotted decimal, a 26-bit mask is

    255 . 255 . 255 . 192

  - CIDR merely writes

    /26

CIDR And Dotted Decimal Equivalence

1 is prefix
0 is suffix

number of prefix bits

Length (CIDR)	Address Mask	Notes
/0	0 . 0 . 0 . 0	All 0s (equivalent to no mask)
/1	128 . 0 . 0 . 0	
/2	192 . 0 . 0 . 0	
/3	224 . 0 . 0 . 0	
/4	240 . 0 . 0 . 0	
/5	248 . 0 . 0 . 0	
/6	252 . 0 . 0 . 0	
/7	254 . 0 . 0 . 0	
/8	255 . 0 . 0 . 0	Original Class A mask
/9	255 . 128 . 0 . 0	
/10	255 . 192 . 0 . 0	
/11	255 . 224 . 0 . 0	
/12	255 . 240 . 0 . 0	
/13	255 . 248 . 0 . 0	
/14	255 . 252 . 0 . 0	
/15	255 . 254 . 0 . 0	
/16	255 . 255 . 0 . 0	Original Class B mask

CIDR And Dotted Decimal Equivalence

Length (CIDR)	Address Mask	Notes
/16	255 . 255 . 0 . 0	Original Class B mask
/17	255 . 255 . 128 . 0	
/18	255 . 255 . 192 . 0	
/19	255 . 255 . 224 . 0	
/20	255 . 255 . 240 . 0	
/21	255 . 255 . 248 . 0	
/22	255 . 255 . 252 . 0	
/23	255 . 255 . 254 . 0	
/24	255 . 255 . 255 . 0	Original Class C mask
/25	255 . 255 . 255 . 128	
/26	255 . 255 . 255 . 192	
/27	255 . 255 . 255 . 224	
/28	255 . 255 . 255 . 240	
/29	255 . 255 . 255 . 248	
/30	255 . 255 . 255 . 252	
/31	255 . 255 . 255 . 254	
/32	255 . 255 . 255 . 255	All 1s (host specific mask)

Why CIDR is Useful

- ISPs assign IP addresses
- Corporate customer with N computers needs N addresses
- CIDR permits ISP to round to nearest power of two
- Example
  - Assume ISP owns address block 128.211.0.0 /16
  - Customer has 12 computers
  - ISP assigns 4 bits of suffix to customer 可以有16-2种host地址，满足12个电脑的要求
  - Mask used is /28
  - Example: customer is assigned 128.211.0.16 /28 32-28=4 bits to host address
  - Each computer at customer site has unique final 4 bits

Example of A /28 Address Block

notice: not all 0

not all 1

all 1 or 0 is reserved for some special application

Special IPv4 Addresses

- Some address forms are reserved

Prefix	Suffix	Type Of Address	Purpose
all-0s	all-0s	this computer	used during bootstrap
network	all-0s	network	identifies a network
network	all-1s	directed broadcast	broadcast on specified net
all-1s	all-1s	limited broadcast	broadcast on local net
127/8	any	loopback	testing

- *Loopback address* (127.0.0.1) used for testing
  - Packets never leave the local host
- Addresses 240.0.0.0/ 8 and above are *multicast*

Host Address Count

- For a given network prefix, the all-0s and all-1s suffixes have special meaning
- Consequence: if a suffix has *N* bits, $2^N - 2$ hosts can be present

IP Addressing Principle

An IP address does not identify a specific computer. Instead, each IP address identifies a connection between a computer and a network.

host

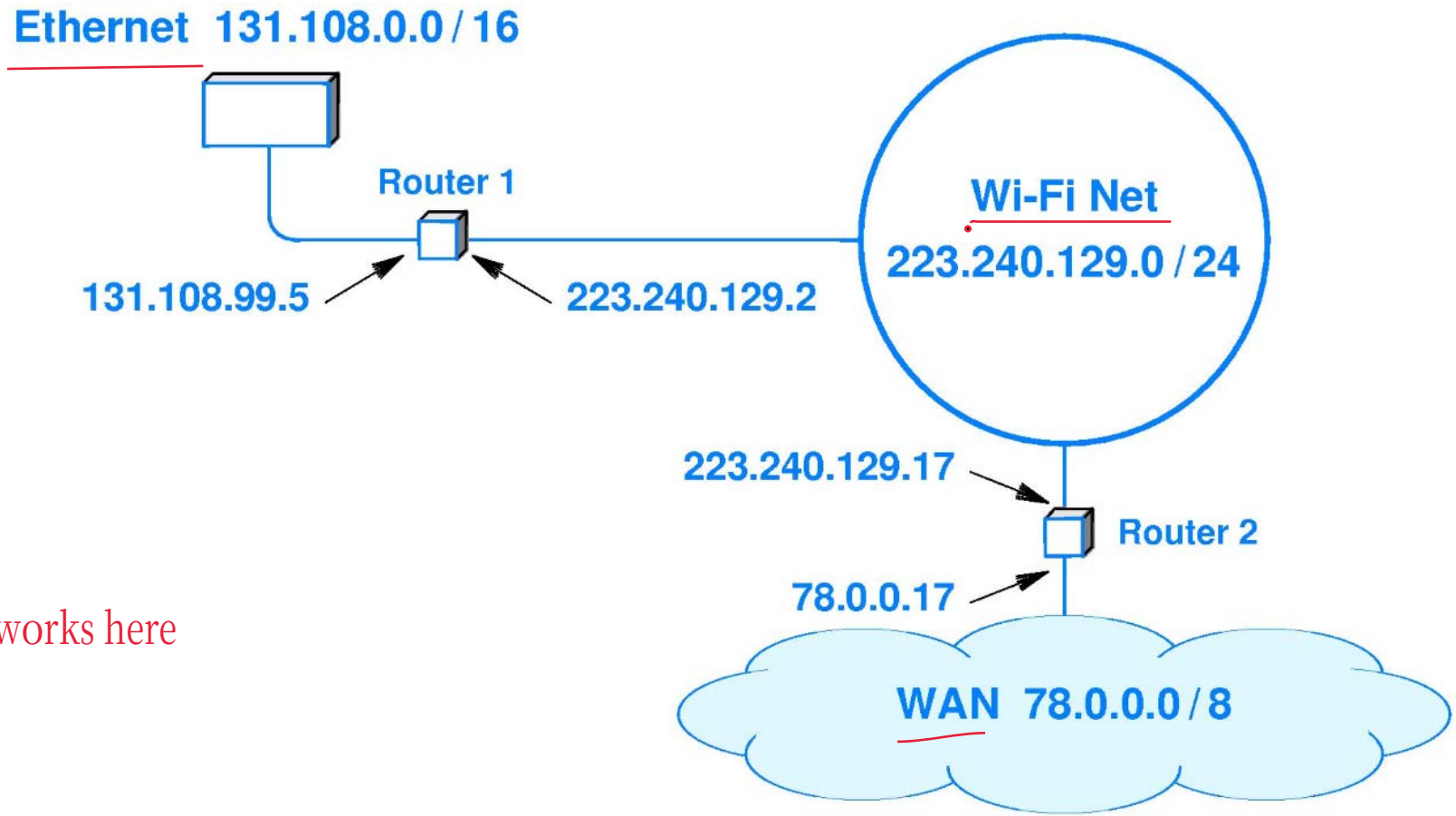
- Consequence

  A router or a host with multiple network connections must be assigned one IP address for each connection.

- Note: host with multiple network connections is called a *multi-homed host*

IPv4 Address Assignment

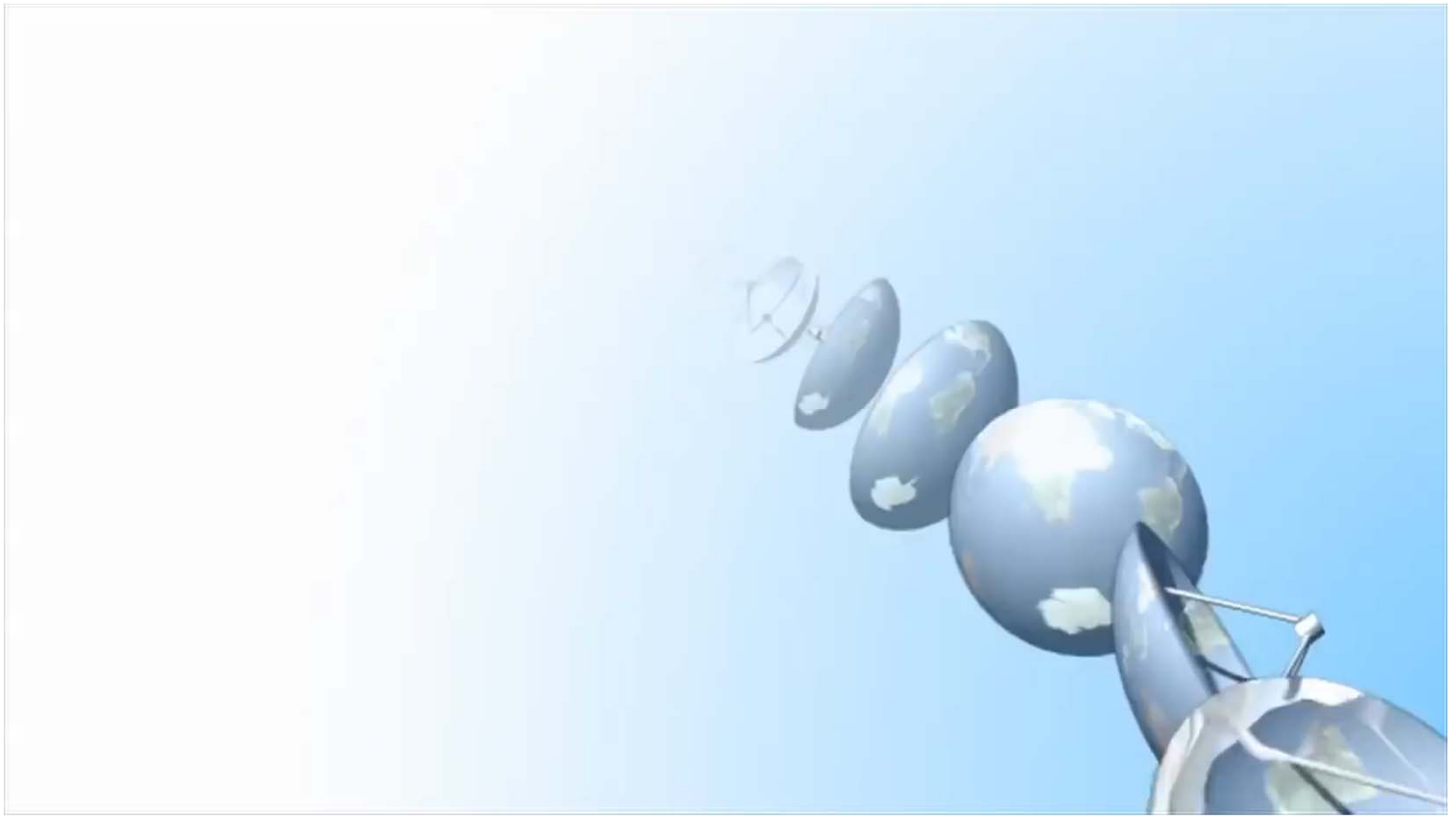
- Each network assigned a unique prefix
- Each host on a network assigned a unique suffix



3 networks here

Summary


SOCIAL
MEDIA
MUSIC
WEBLOGS
CONTACTS
PICTURES
COMMUNIATION
FRIENDSHIP
RATING
INTERNET
BOOKMARKING
MICROBLOGGING
VIDEO
FORUM



from source to destination

Datagram Routing

particular packet

Internet Packets

Because it includes incompatible networks, the Internet cannot adopt a particular hardware packet format. To accommodate heterogeneity, the Internet Protocol defines a hardware-independent packet format.

Routing: each end system and router maintains a routing table that lists, for each possible destination network, the next router to which the internet datagram should be sent.

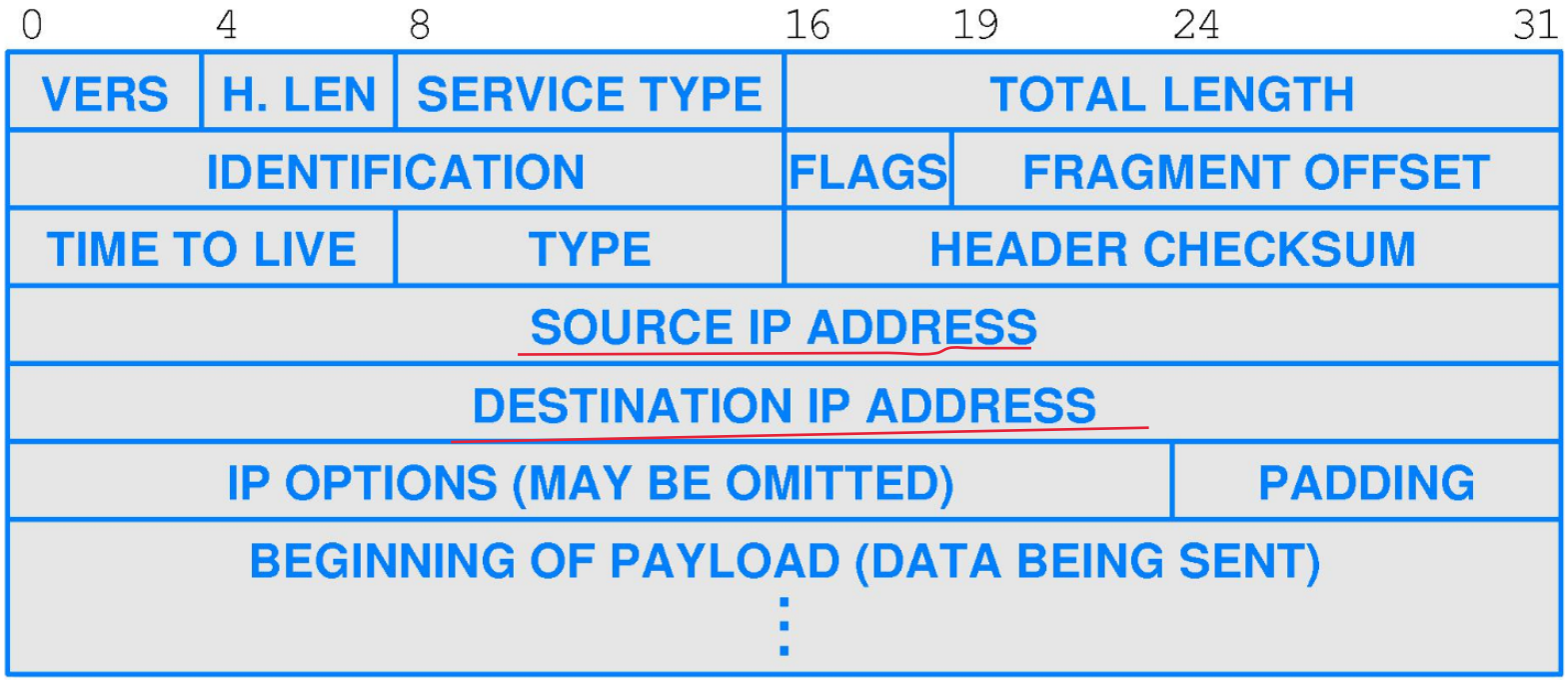
IP Datagram

- Virtual packet format used in the Internet
- Format of header determined by protocol version (IPv4 or IPv6)
- Size of payload determined by application from top layer
  - Maximum payload is almost 64K octets
  - Typical datagram size is 1500 octets

IPv4 Datagram Header

control info.

- Most header fields have fixed size and position
- Header specifies source, destination, and content type



Internet Communication Paradigm

info. from top layer chop to packets, then transmit through network

- Each datagram handled independently
- Datagram formed on source computer
- Source sends datagram to nearest router
- Router forwards datagram to next router along path to destination
- Final router delivers datagram to destination
- Datagram passes across a single physical network at each step

IP packect

Datagram Routing

- Performed by initial host and each router along path
- Selects *next hop* for the datagram as either
  - Next router along the path
  - Ultimate destination

find nearest router to jump to

- Uses a routing/*forwarding table* with one entry per network
- Important point: size of routing/forwarding table proportional to number of networks in the Internet

Internet Communication

- IP uses *best effort delivery* semantics
- IP attempts to deliver each datagram, but specifies that a datagram can be
  - Lost
  - Duplicated
  - Delayed
  - Delivered out-of-order
  - Delivered with bits scrambled

handle

- Motivation: accommodate any underlying network
- Note: in practice, IP works well

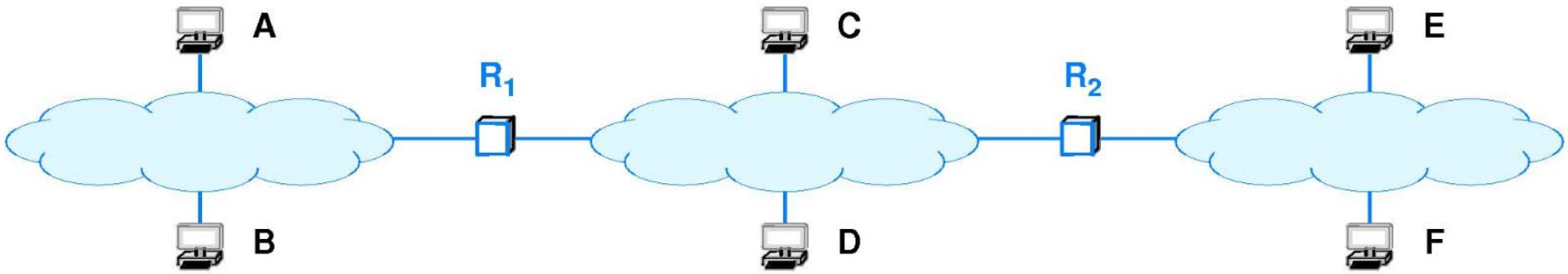
Datagram Transmission

- Underlying network hardware (physical)
  - Only understands MAC addresses
  - Requires each outgoing frame to contain the MAC address of the next hop
- IP forwarding (logical)
  - Deals only with (abstract) IP addresses
  - Computes the IP address of the next hop
- Conclusion

The IP address of the next hop must be translated to a MAC address before a frame can be sent. (down to data link layer)

Address Resolution

- Translates IP address to equivalent MAC address that the hardware understands
- IP address is said to be resolved
- Restricted to a single physical network at a time
- Example: consider computer X sending to computer Y



- A MAC address is needed at each hop

Address Resolution Protocol (ARP)

- Designed for IPv4 over Ethernet
- Used by two computers on the same physical network
- Allows a computer to find the MAC address of another computer based on given IP address
- Operates at layer 2 data link layer
- Uses network to exchange messages
- Computer seeking an address sends request to which another replies

Example Of ARP Exchange

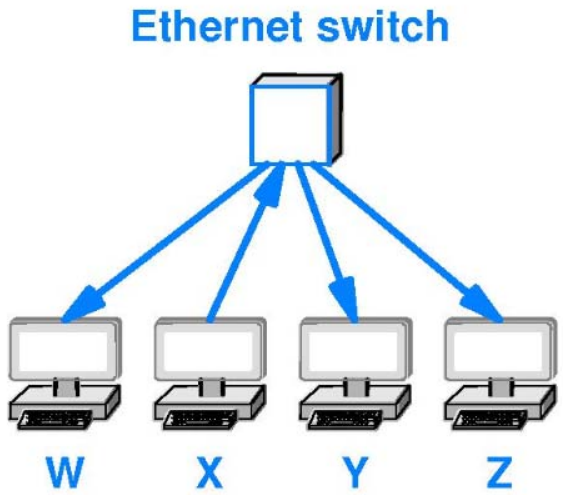
- Assume
  - Four computers attached to an Ethernet
  - Computer B has a datagram to send
- Computer B
  - Uses forwarding table to find next-hop address Ic
  - Broadcasts an ARP request: "I'm looking for a computer with IP address Ic"
- Computer C
  - Receives the request and replies; "I'm the computer with IP address Ic"

ARP Message Exchange

from X, ask which of you have this P address

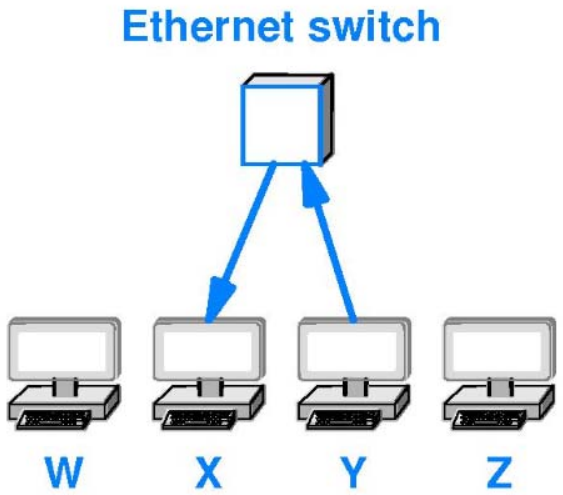
- Request is broadcast to all computers
- Only the intended recipient replies
- Reply is sent unicast

one ditection



want to send

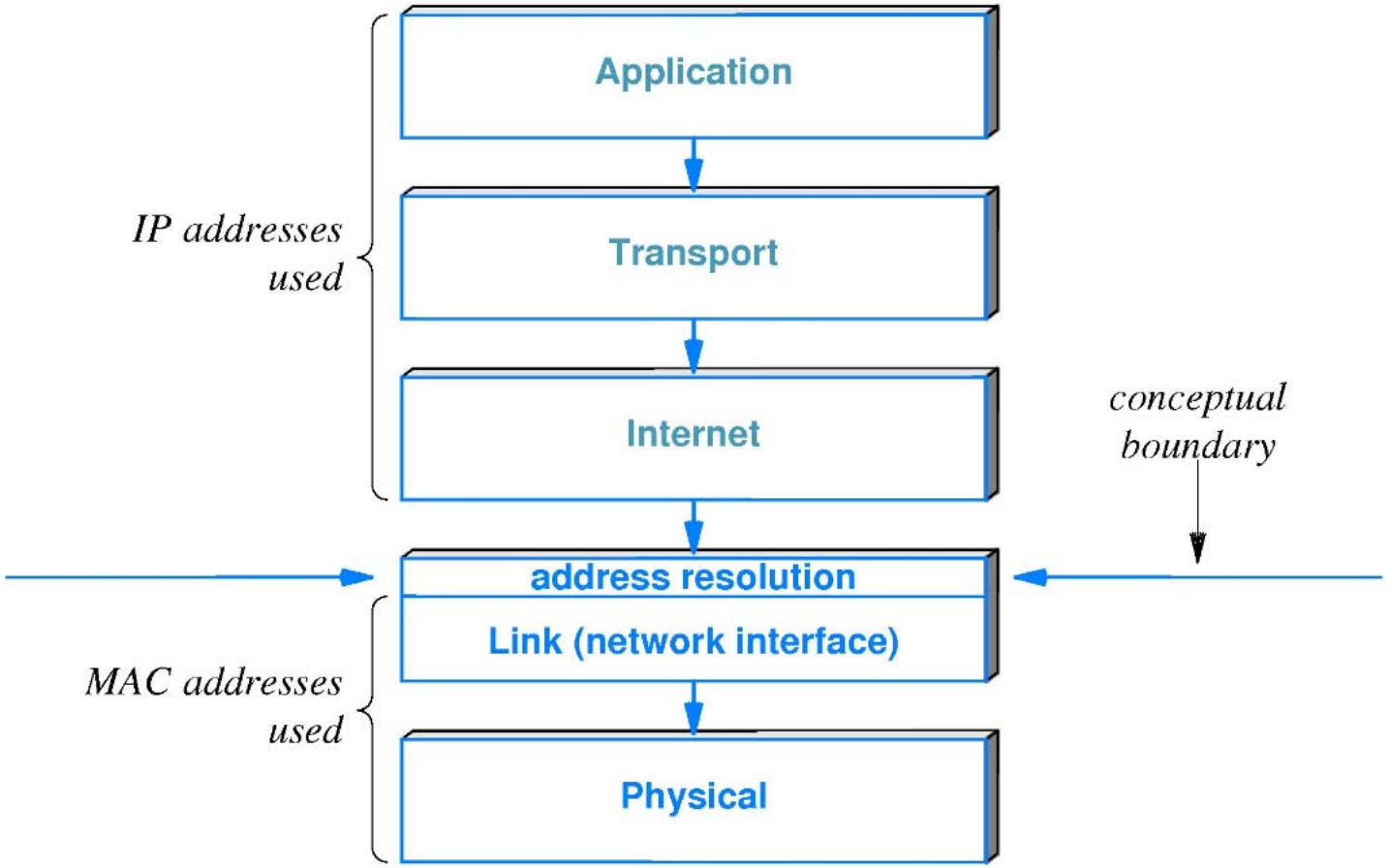
(a)



(a) host

Boundary Between Protocol And MAC Addressing

- ARP isolates hardware addresses, allowing layers above to use only IP



Part 5: Transport Layer & Technologies

Transport Layer Protocols

What Should A Network Provide?

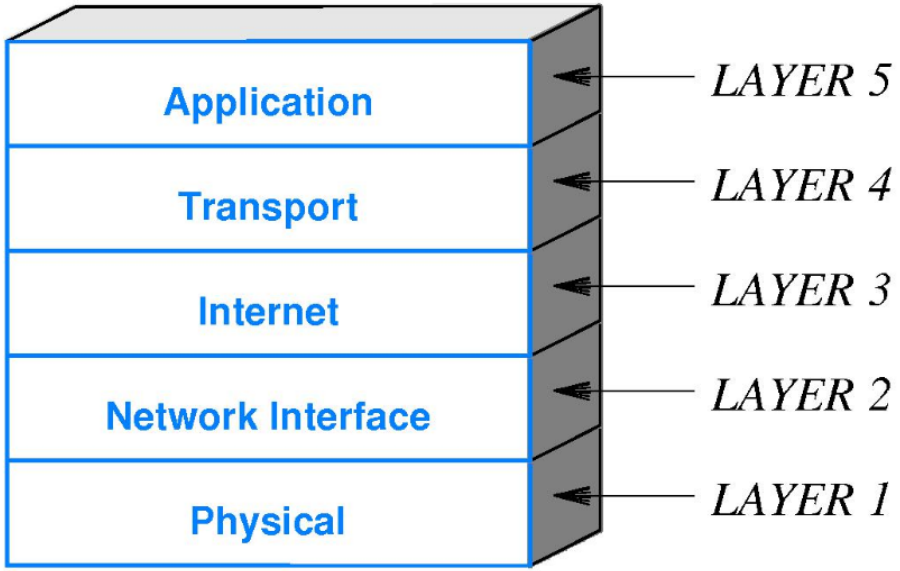
- Network provides communication
  - Network only transfers packets
  - Applications handle everything else, including reliability, flow control, and authentication
  - Known as *end-to-end communication*

End-To-End Communication

- Fundamental concept in the Internet
- Network provides best-effort packet transport
- Endpoints
  - Control communication
  - Provide all reliability
- Consequence:
  Some of the most complex protocols in the Internet protocol suite run in hosts rather than in routers.

Transport Layer

- Layer between applications and IP



- Allows multiple applications on a given host to communicate with applications on other hosts
- Uses IP to carry messages

A Transport Protocol Handles …

- Accommodate speed mismatch between sender and receiver
- Detect and recover from datagram loss
- Eliminate duplicate packets
- Guarantee that messages arrive in order
- Respond to congestion in the Internet
- Prevent delayed packets from being misinterpreted
- Verify that data was not corrupted during transit
- Ensure that each party has agreed to communicate
- Note: a given transport protocol may not handle all problems

Transport Protocol Techniques

- Application demultiplexing split
  - Sender places a value in each outgoing packet that identifies an application on the receiving host
  - Receiver uses the value to determine which application should receive the packet
- Flow-control mechanisms TCP can offer
  - Receiver informs sender of acceptable data rate
  - Sender limits rate to prevent overrunning the receiver

Transport Protocol Techniques

- Congestion control mechanisms
  - Receiver or network informs sender about congestion in the network
  - Sender reduces data rate (packet rate) until congestion subsides
- Sequence numbers
  - Sender places a *sequence number* in each packet
  - Receiver uses the sequence numbers to ensure no packets are missing and that packets are delivered in the correct order

Transport Protocol Techniques

- Positive acknowledgement with retransmission
  - Receiver sends *acknowledgement* to inform sender when a packet arrives
  - Sender *retransmits* packet if acknowledgement fails to arrive within a specified time
- Sliding window
  - Instead of transmitting a packet and waiting for an acknowledgement, a sender transmits *K* packets and each time an acknowledgement arrives, transmits another

Transport Protocols

- Two primary transport protocols used in the Internet
  - User Datagram Protocol (UDP)
  - Transmission Control Protocol (TCP) dominant
- Choice determined by application protocol
  - Many applications specify the use of a single transport (e.g., email transfer uses TCP)
  - Some applications allow the use of either (e.g., DNS queries can be sent via UDP or TCP)

Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP)

- The primary transport-layer protocol used in the Internet
- Accounts for about 90% of all Internet traffic (some estimates are higher)
- Provides reliability
- Appeals to programmers

TCP Characteristics

- End-to-end communication
- Connection-oriented paradigm
- Point-to-point connections
- Complete reliability
- Full-duplex communication
- Stream interface
- Reliable connection startup
- Graceful connection shutdown

End-To-End Communication

- TCP provides communication among pairs of applications
- Allows an application on one host to communicate with an application on another host

N to N communication

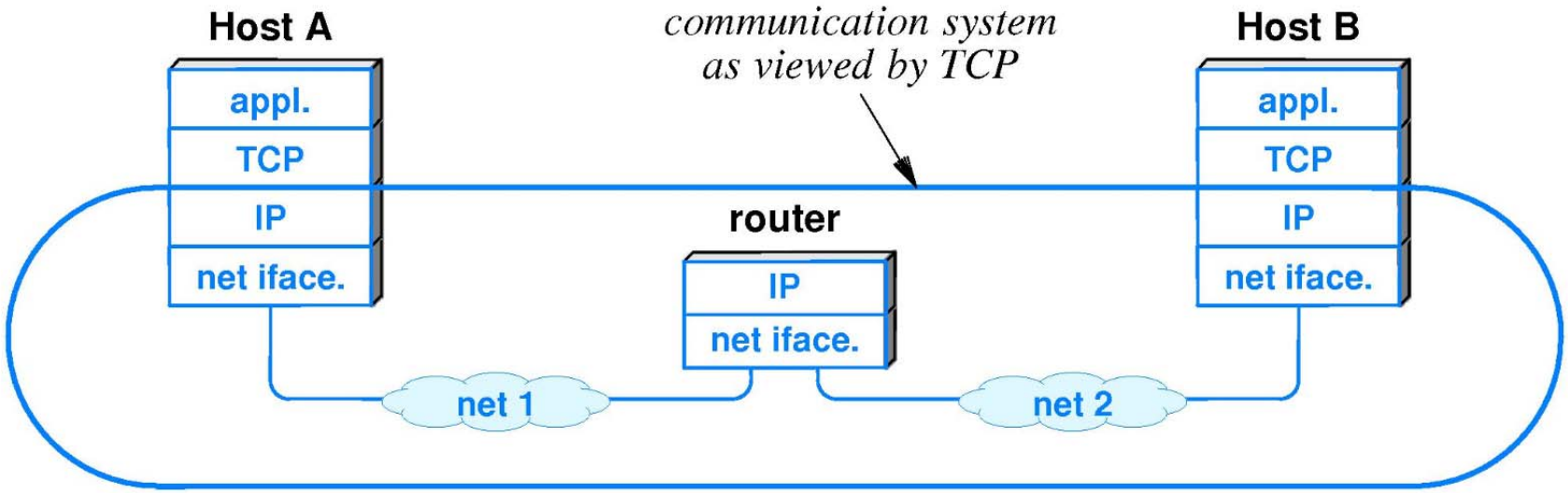
- Permits multiple applications on a given computer to communicate simultaneously without interference

for use diff. pot numbers

- Uses protocol port numbers to distinguish among applications
- Note: TCP ports are completely independent of UDP ports

End-To-End Principle

- Transport protocols operate in end systems, and view the underlying Internet as a virtual network



- IP does not read or interpret TCP packets
- When forwarding datagrams, router only processes layers 1 through 3

d not contain transport protocol

TCP Port Numbers

- 16-bit integers used to identify applications
- Each application needs a port number
- TCP well-known port assignments are independent of UDP assignments
- However, to help humans, the same value chosen if service available via either transport
- Examples
  - Both UDP and TCP assign port 53 to the Domain Name System (DNS)
  - Both UDP and TCP assign port 7 to the echo service

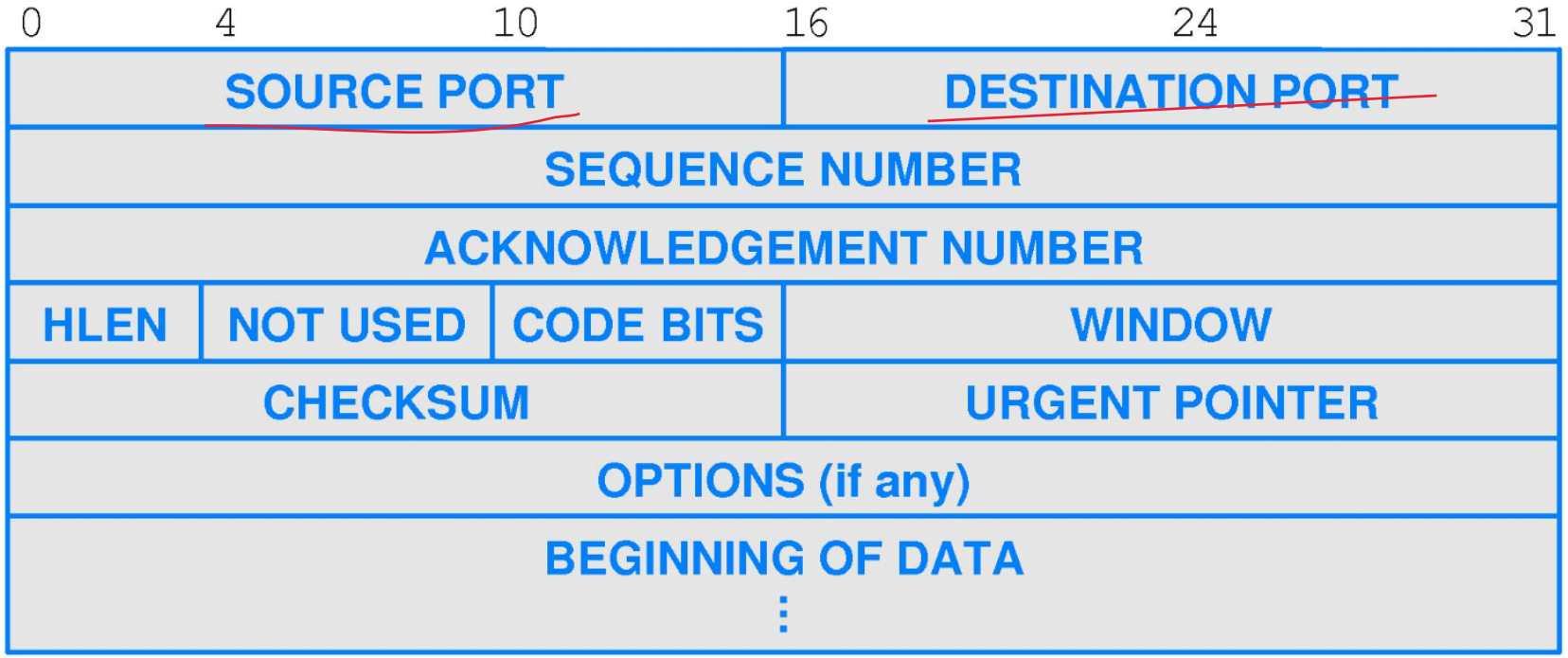
Protocol Ports, Four-Tuple and Flows

- Key concept: because a TCP connection corresponds to a pair of endpoints, the connection is identified by four items
  - IP source address
  - TCP source port
  - IP destination address
  - TCP destination port
- Commonly called the four-tuple
- Explains how an application such as a web server can communicate with multiple clients at the same time

if from diff machine, have diff IP address

TCP Segment Format

- TCP packet is called a *segment*
- Segment is encapsulated in IP for transmission
- Single format used for SYNs, FINs, ACKs, and data



Connection-Oriented Paradigm

- Pair of applications must
  - Establish a TCP connection before communicating
  - Terminate the connection when finished
- Important insights
  - A TCP connection is virtual because only the two endpoints know a connection is in place
  - TCP does not have keep-alive messages: no packets are exchanged unless applications are sending data

Limited Interaction

- A TCP connection only provides communication between a pair of applications
- Known as a *point-to-point* communication
- TCP connection does *not* support
  - Multi-point connections with more than two endpoints
  - Broadcast or multicast delivery

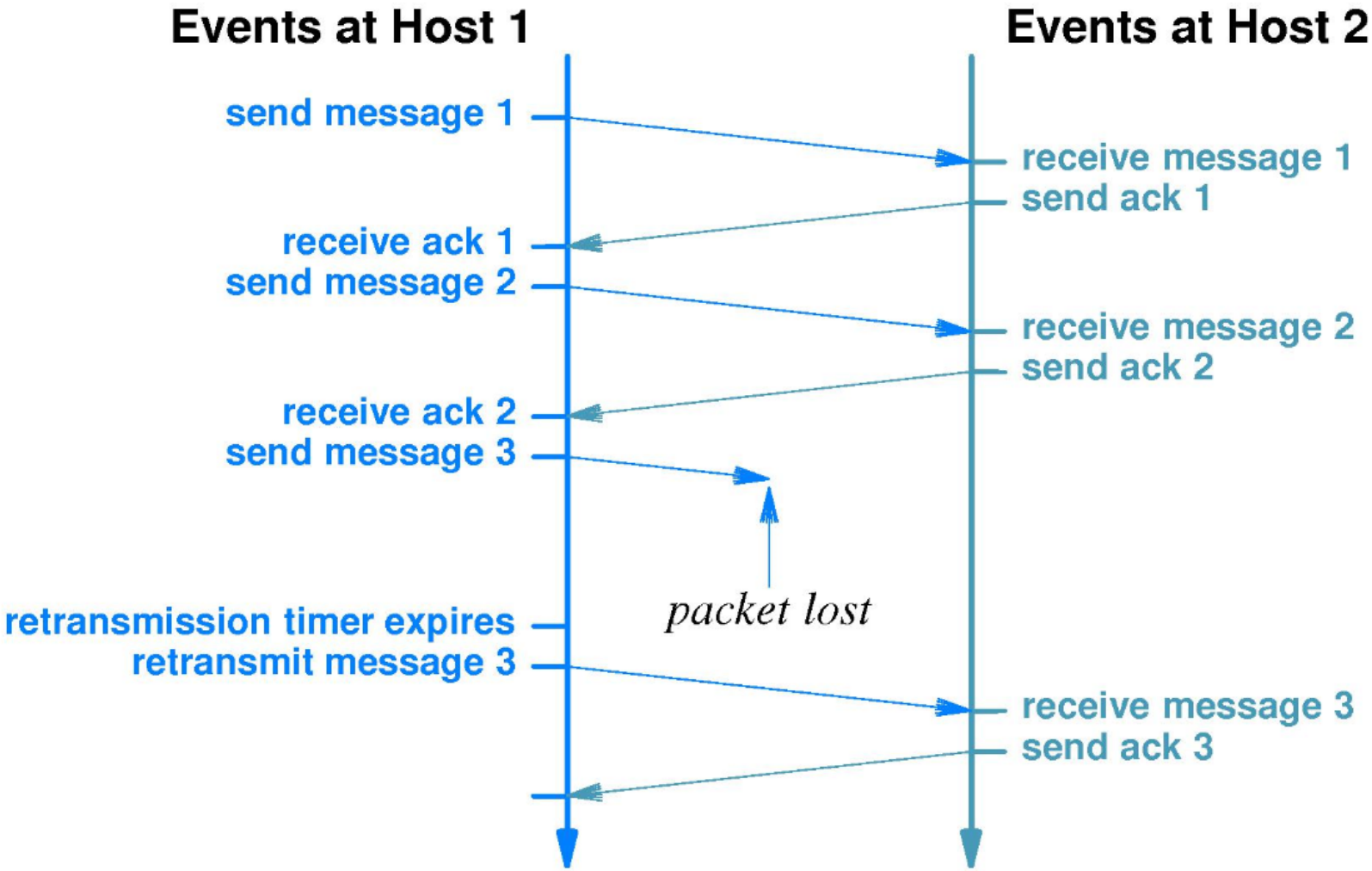
TCP Reliability Guarantee

- TCP provides full reliability
- Compensates for
  - Loss
  - Duplication
  - Delivery out of order
- Does so without overloading the underlying networks and routers
- TCP makes the following guarantee
  - Data will be delivered or sender will (eventually) be notified.

TCP Reliability

- Uses timeout-and-retransmission
- Receiver returns an acknowledgement (ACK) to sender when data arrives
- Sender waits for acknowledgement and retransmits data if no acknowledgement arrives

TCP Retransmission

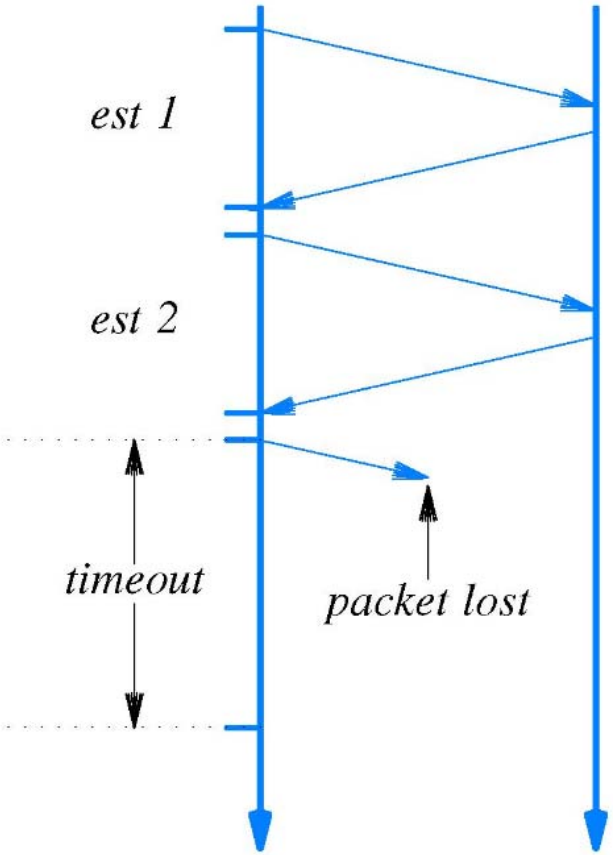


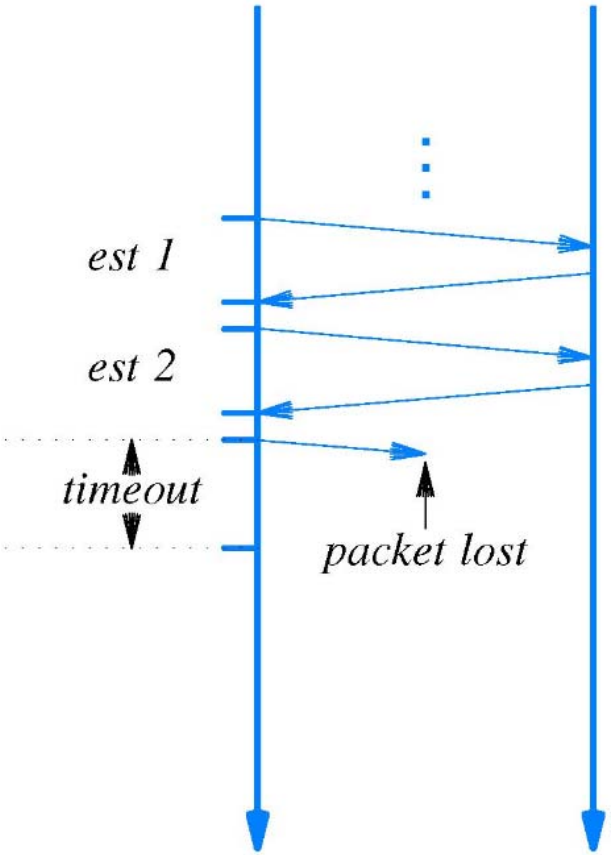
Why TCP Retransmission Is Hard?

- TCP designed for Internet
  - Round-trip delays differ among connections
  - Round-trip delays vary over time
- Waiting too long introduces unnecessary delay
- Not waiting long enough sends unnecessary copies
- Key to TCP's success: *adaptive* retransmission

Adaptive Retransmission

- Continually estimate round-trip time of each connection
- Set retransmission timer from round-trip estimate
- Illustration of timeout on two connections:

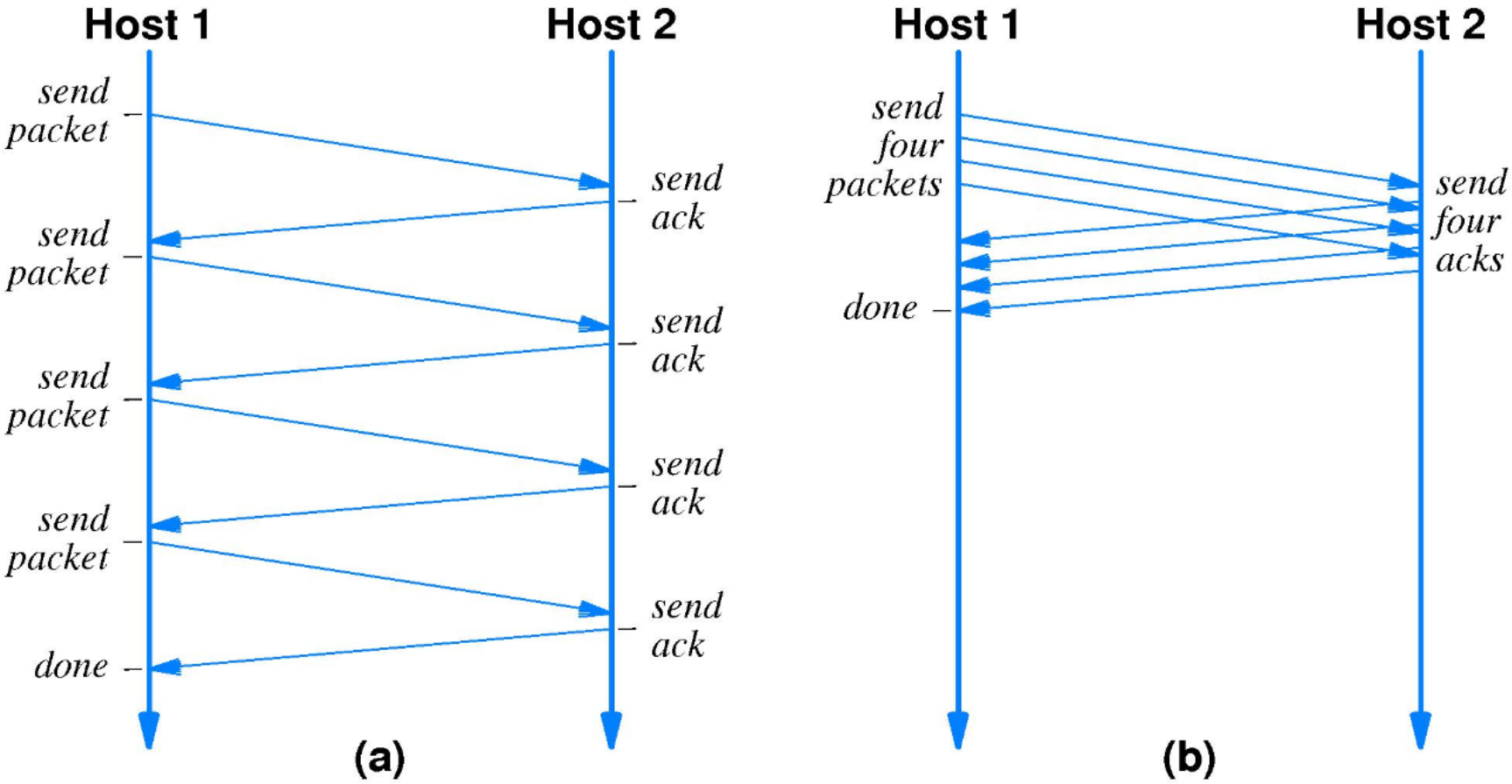




Review of Sliding Window

- Transport protocols use *sliding window* mechanism
- Idea is to send multiple packets before waiting for an acknowledgment
- Window size is relatively small (tens of packets, not millions)
- Motivation is to increase throughput

How Sliding Window Improves Data Rate

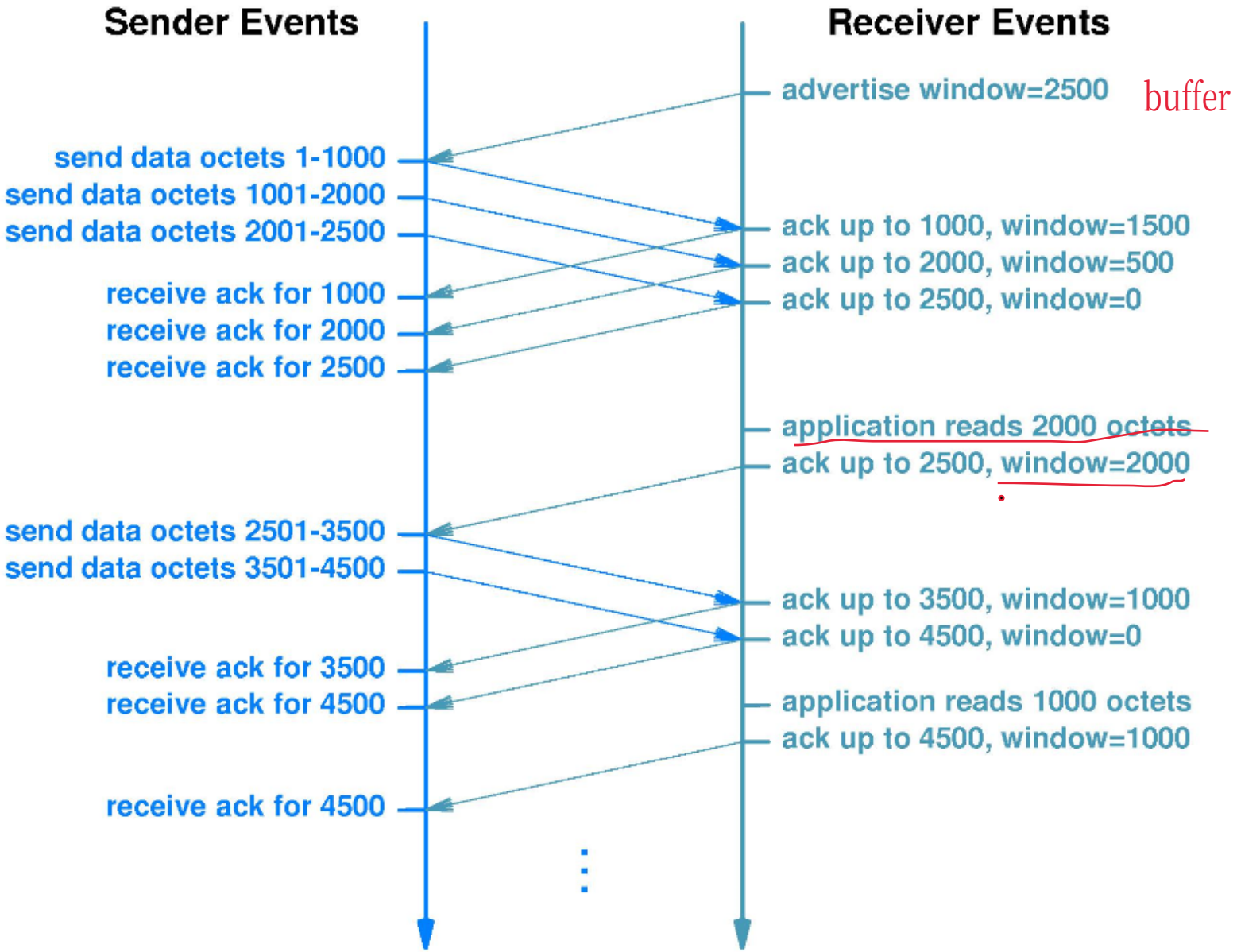


- Window size of K improves data rate by a factor of K

TCP Flow Control

- *Flow control* mechanism coordinates data being sent with receiver's speed
- Buffer size used instead of data rate
- Receiver tells sender size of initial buffer
- Each acknowledgement specifies space remaining in buffer
- Known as *window advertisement*

Illustration Of TCP Flow Control



TCP Congestion Control And Slow Start

- TCP uses loss or changes in delay to infer congestion in the network
- When congestion is detected, sending TCP temporarily reduces the size of the window
- When a packet is lost, TCP temporarily reduces the effective window to one half its current value
- Later, TCP slowly increases the window again
- Congestion avoidance also used when a connection starts
  - Temporarily use a window size of one segment
  - Double the window size when ACK arrives
  - Known as *slow start*

full 2 ways

Full-Duplex Communication

- TCP connection between A and B provides two independent data streams, one from A to B and the other from B to A
- Each side
  - Has a receive buffer
  - Advertises a window size for incoming data
  - Uses sequence numbers to number outgoing data bytes
  - Implements timeout-and-retransmission for data it sends
- Application can choose to shut down communication in one direction

Connection Startup And Shutdown

- Difficult problem
- Packets can be
  - Lost
  - Duplicated
  - Delayed
  - Delivered out-of-order
- Either end can crash and reboot
- Need to know that both sides have agreed to start/ terminate the connection

User Datagram Protocol (UDP)

User Datagram Protocol (UDP)

- Accounts for less than 10% of Internet traffic
- Blocked by some ISPs

UDP Characteristics

- End-to-end communication
- Connectionless communication
- Message-oriented interface
- Best-effort semantics
- Arbitrary interaction 1 t o1 or broadcast
- Operating system independence
- No congestion or flow control

End-To-End Communication

N to N

- UDP provides communication among applications
- Sending UDP
  - Accepts outgoing message from application
  - Places message in a User Datagram
  - Encapsulates User Datagram in an IP datagram and sends
- Receiving UDP
  - Accepts incoming User Datagram from IP
  - Extracts message and delivers to receiving application
- Note: message is unchanged by the network

Connectionless Communication

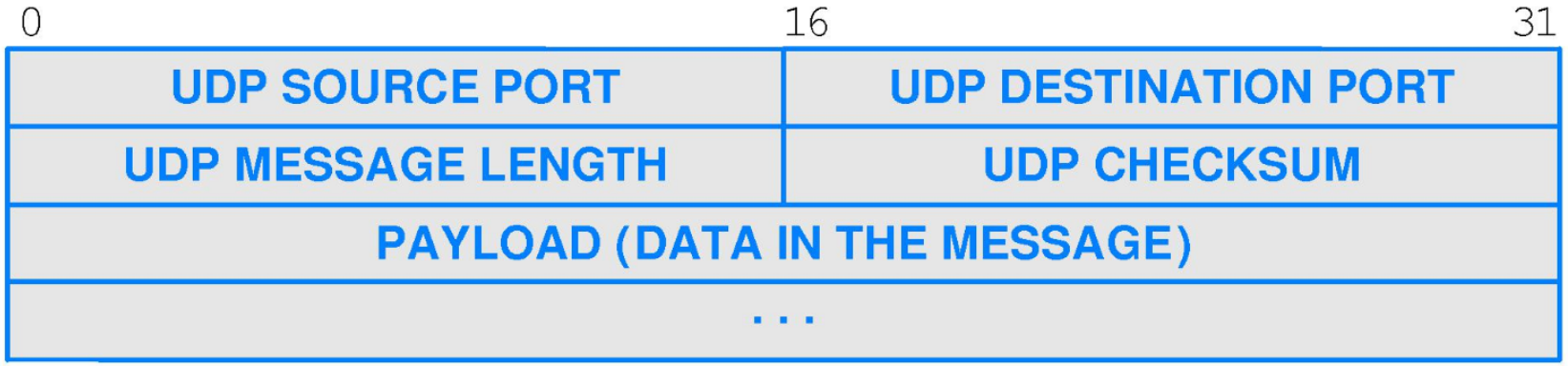
- An application using UDP can
  - Send a message to any receiver (universal)
  - Send at any time (asynchronous)
  - Stop sending at any time (unterminated)
- That is, a sender does not
  - Inform the network before sending (i.e., does not establish a communication channel)
  - Inform the other endpoint before sending
  - Inform the network or other endpoint that no more messages will be sent

Message-Oriented Interface

- UDP
  - Accepts and delivers messages (blocks of data)
  - Does not require all messages to be the same size, but does define a maximum message size
  - Places each outgoing User Datagram in a single IP datagram for transmission
  - Always delivers a complete message to receiving application
- Sending application must divide outgoing data into messages; UDP sends what it is given (or reports an error if the message is too large)

UDP Datagram Format

- Extremely thin layer
- User Datagram is divided into header and payload
- Header contains only 8 octets:



UDP Message Size

- UDP allows up to 64K octet messages
- As a practical limit, the size of a User Datagram is limited by payload area in IP datagram
- Maximum IP payload is 64K octets minus size of IP header
- Therefore, the maximum UDP payload is 64K octets minus size of IP and UDP headers (usually 64K octets minus 28)
- Application can choose any message size up to the maximum UDP payload

UDP Semantics

- UDP uses IP for delivery and offers the same semantics!
- UDP packet can be
  - Lost
  - Duplicated
  - Delayed
  - Delivered out of order
  - Delivered with data bits altered
- Note 1: UDP does not introduce such errors; the errors arise from the underlying networks
- Note 2: UDP does include an optional checksum to protect the data (but the checksum may be disabled)

Best-Effort Semantics

- UDP provides best-effort semantics as it uses IP for transmission.
- UDP is sometimes characterized as a thin protocol layer that provides applications with the ability to send and receive IP datagrams.

Arbitrary Interaction

- UDP permits arbitrary interaction among applications

  1-to-1

  1-to-many

  Many-to-1

  Many-to-many

- Application programmer chooses interaction type
- Ability to send a single message to multiple recipients can be valuable

  advantage over TCP

Efficient Implementation

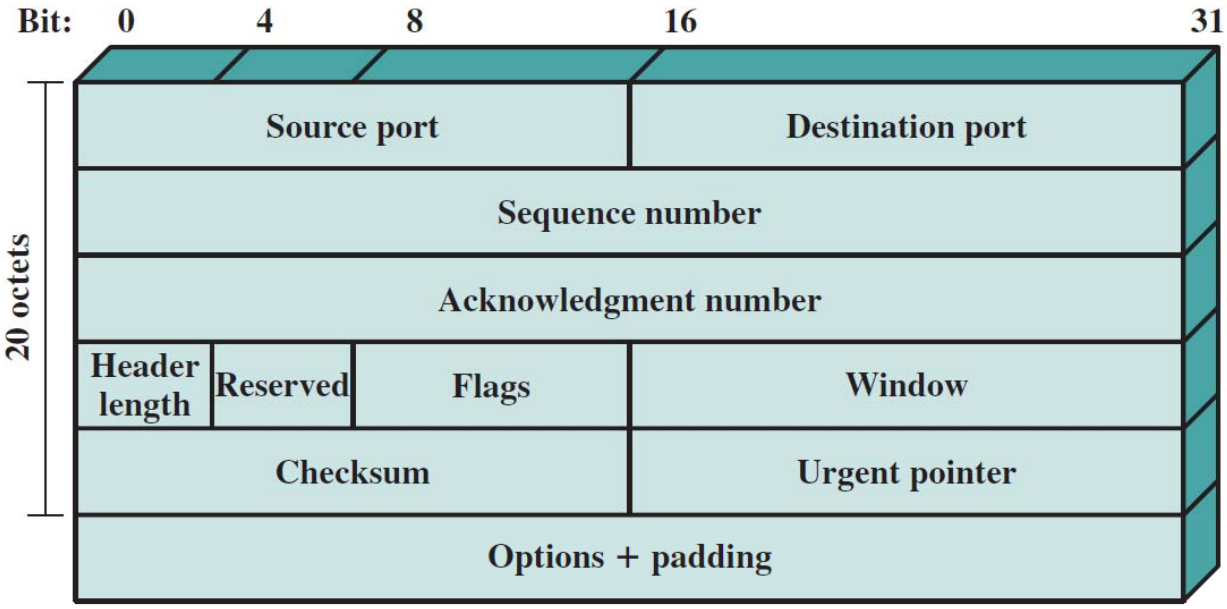
- Key point: UDP can use IP broadcast or multicast to deliver messages
- Provides efficient delivery to a set of hosts
- No need for sender to transmit individual copies
- Broadcast is a significant advantage of UDP over TCP for some applications

UDP Application Identifiers

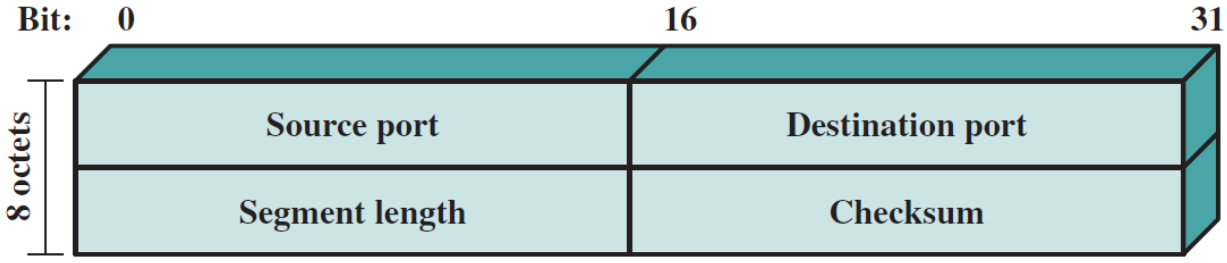
- 16-bit integer known as UDP protocol port number
- Each application using UDP must obtain a port number
- Sending UDP
  - Places a port number in UDP header to identify destination application on receiving host
  - Also includes port number of sending application
- Receiving UDP
  - Uses value in header to select appropriate application

UDP protocol port numbers are universal across all computers, and do not depend on the operating system.

TCP and UDP Headers



(a) TCP header

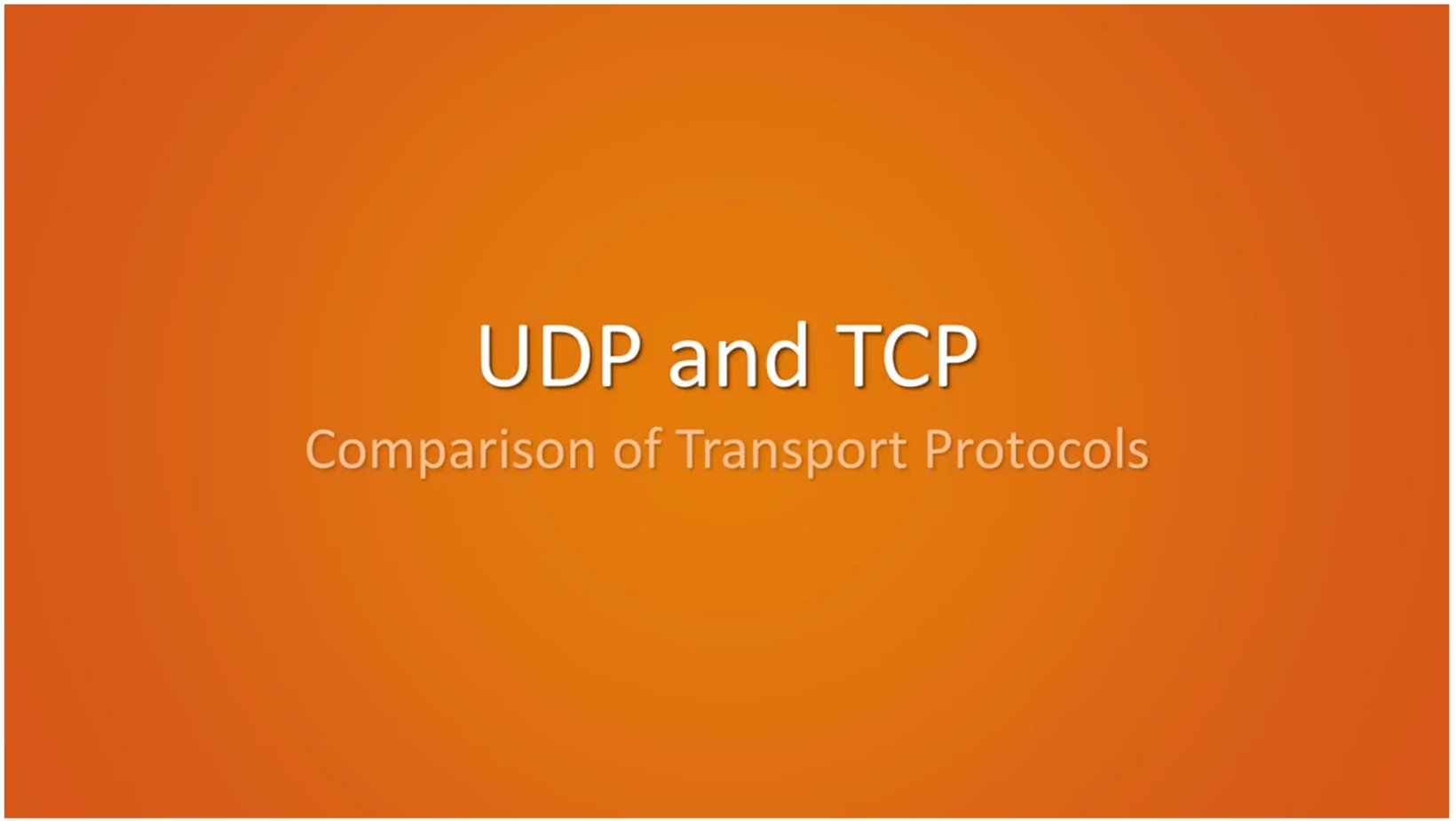


(b) UDP header

Well-Known UDP Ports

Port Number	Description
0	Reserved (never assigned)
7	Echo
9	Discard
11	Active Users
13	Daytime
15	Network Status Program
17	Quote of the Day
19	Character Generator
37	Time
42	Host Name Server
43	Who Is
53	Domain Name Server
67	BOOTP or DHCP Server
68	BOOTP or DHCP Client
69	Trivial File Transfer
88	Kerberos Security Service
111	Sun Remote Procedure Call
123	Network Time Protocol
161	Simple Network Management Protocol
162	SNMP Traps
514	System Log

TCP vs UDP



Source: PieterExplainsTech

Main Differences of TCP vs UDP

- What are the main differences between TCP and UDP?

看另一个PPT的

What is VPN?


MUSIC
SOCIAL
MEDIA
WEBLOGS
CONTACTS
PICTURES
COMMUNICATION
FRIENDSHIP
WEB
RATING
INTERNET
BOOKMARKING
MICROBLOGGING
VIDEO
FORUM