Chapter Five-OSI Reference Model

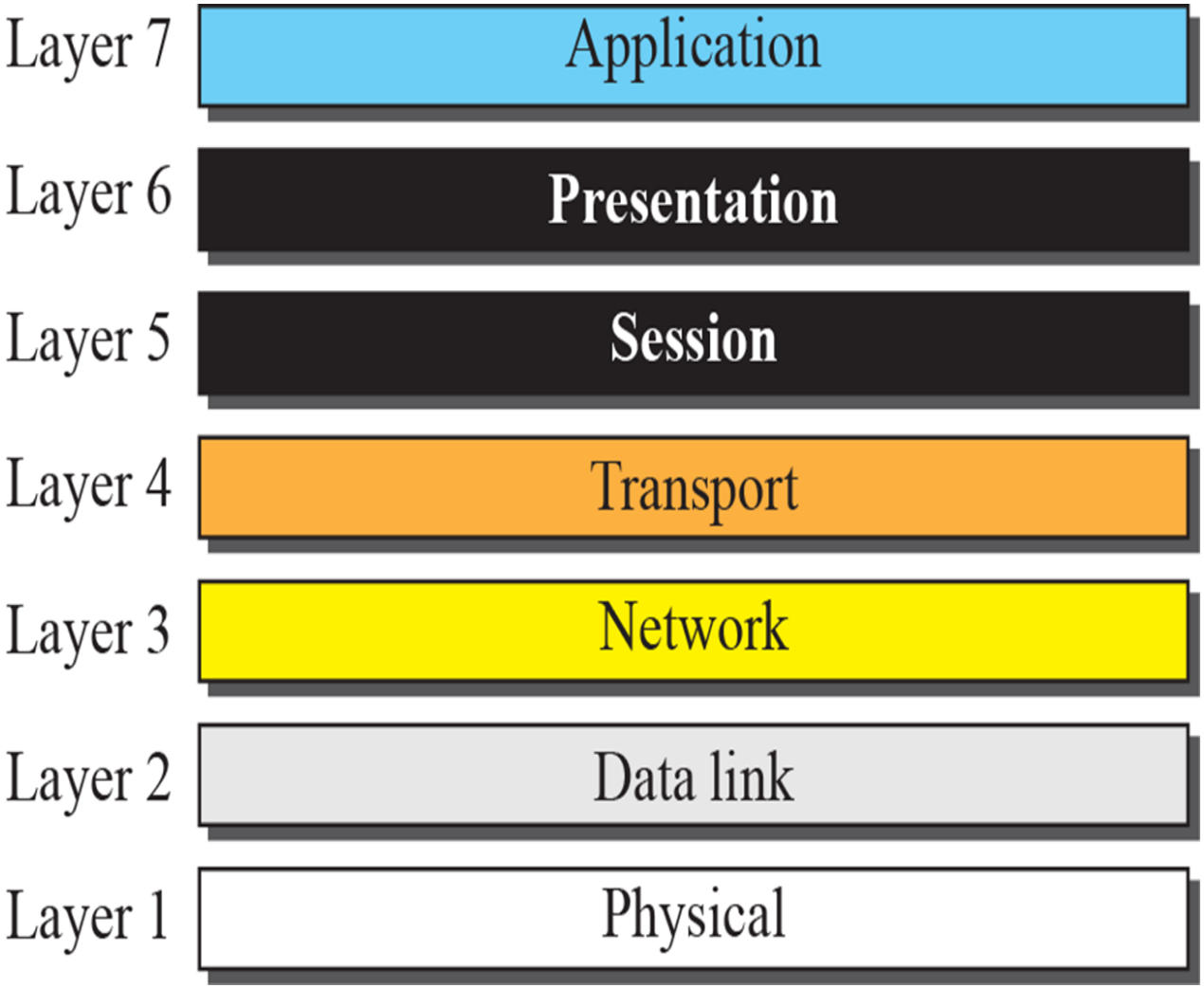
Overview & functions of each layer

Outline of the lecture

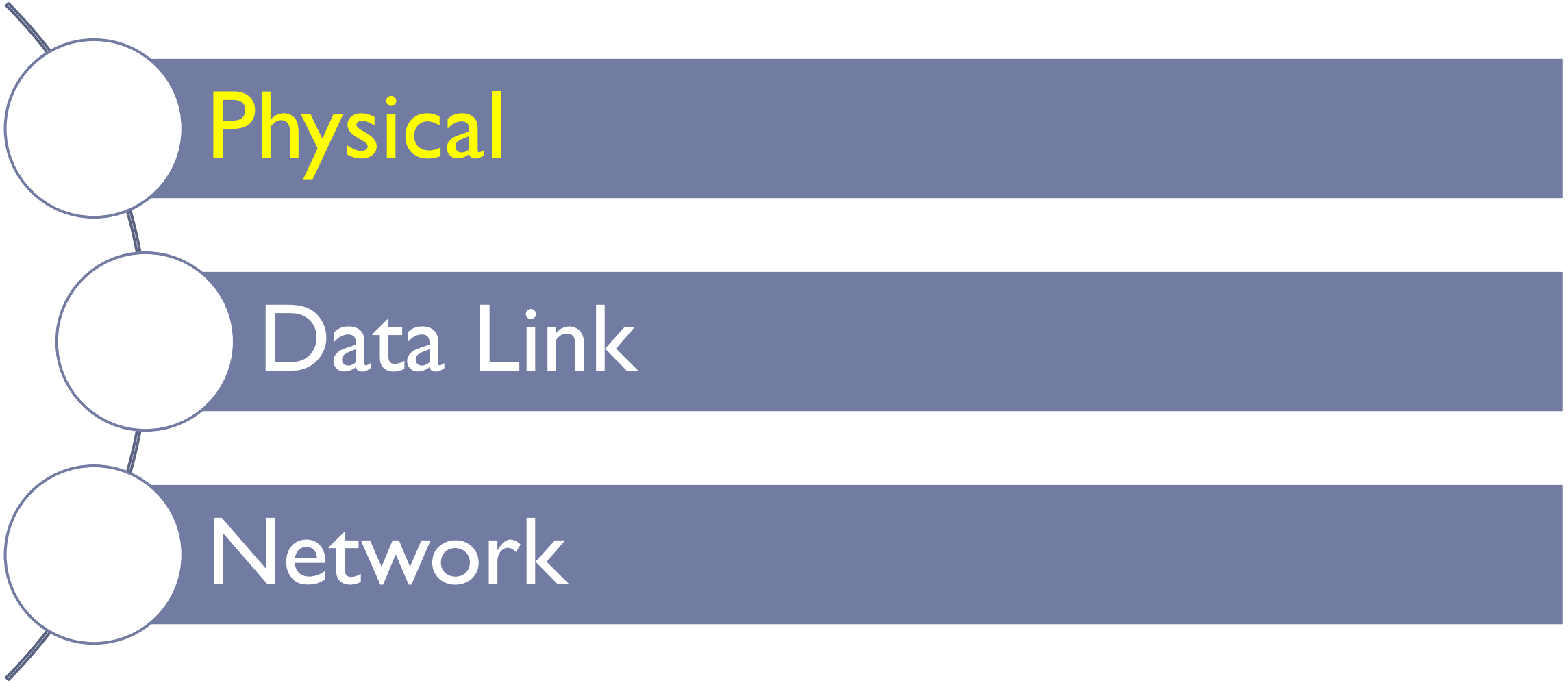
- **Layered Framework of OSI**
- **Overview & functions of each layer**
  - **OSI lower layers**
    - **Physical layer**
    - **Data link layer**
      - Framing
      - Addressing
      - Error detection and correction
      - Data link control and protocol
        - Flow control
        - Error control
      - Multiple access
    - **Network Layer**
      - Internetworking
      - Packetizing and framing
      - Addressing
      - Network layer protocols
  - **OSI Upper layers**
    - **Transport layer**
      - Packetizing
      - Addressing
      - Multiplexing and Demultiplexing
      - Connection control
    - **Session layer**
    - **Presentation layer**
    - **Application**
      - Client server model
      - Addressing
      - Application layers services

Layered frame work of OSI

- Open Systems Interconnection (OSI)
- A theoretical model-not implemented (reference)
- Developed by International Standards Organization (ISO)
- Open – to connect open systems
- Contains seven layers (7)

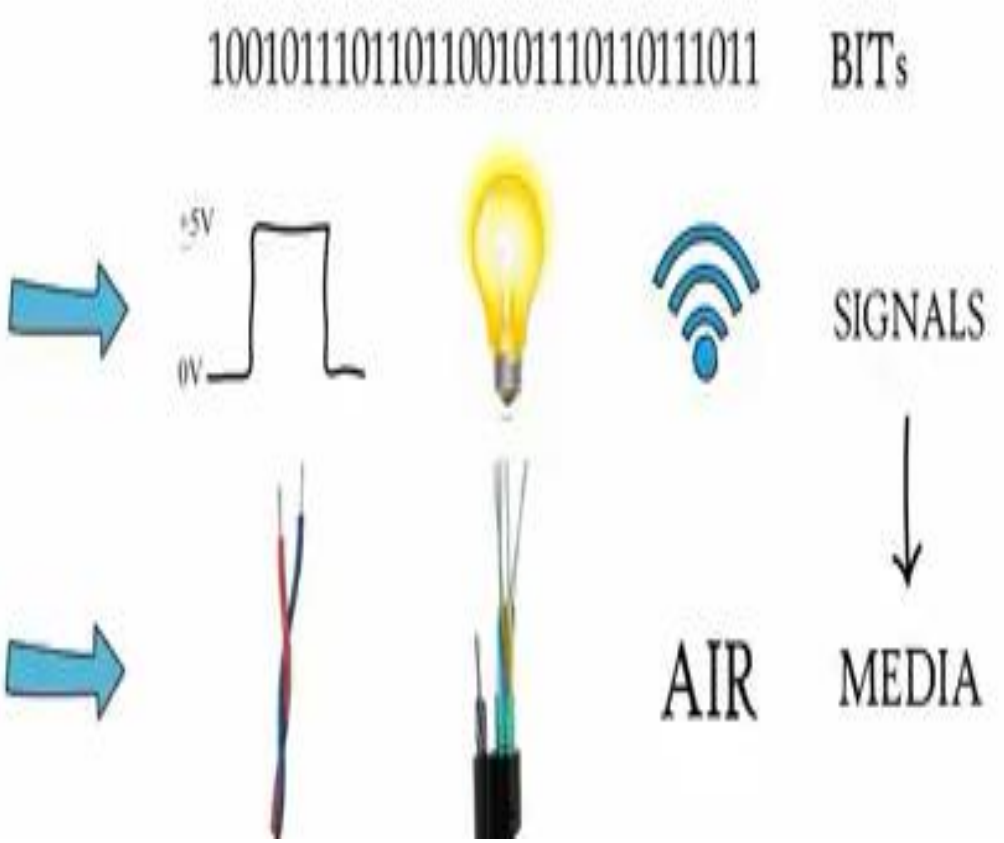


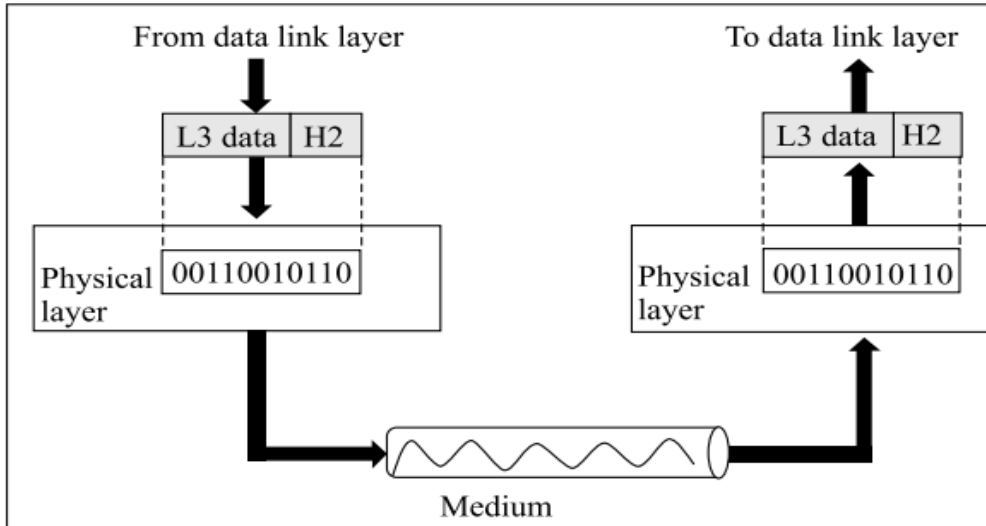
OSI Lower Layers



OSI Physical Lay

- Responsible for transmission of bits
- The type of interface used on the networking device
- The type of cable used for connecting devices
- The connectors used on each end of the cable
- Layer actually interact to the physical medium
- Signal encoding: 0 and 1 representation
- Transmission type: serial/parallel
- Transmission mode: simplex, duplex, 1/2
- Topology and multiplexing: star, bus, TDM, FDM ?
- Bandwidth: which bandwidth used
- Signal type: analog or digital signal ?
- The encoding of a message on a signal by converting binary digits to
- a physical representation based on the media type, such as
- –electrical for copper,
- – light for fiber, or
- –radio wave for wireless

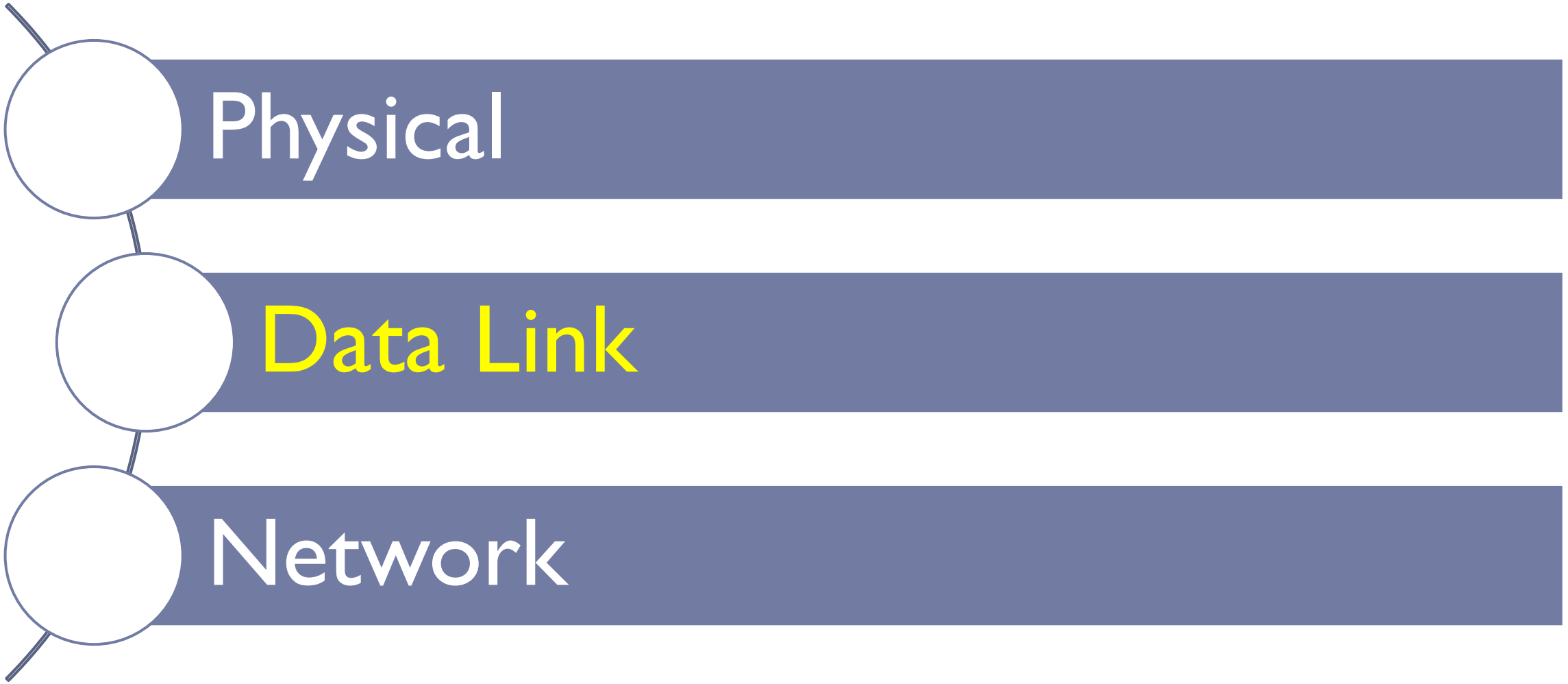




Note

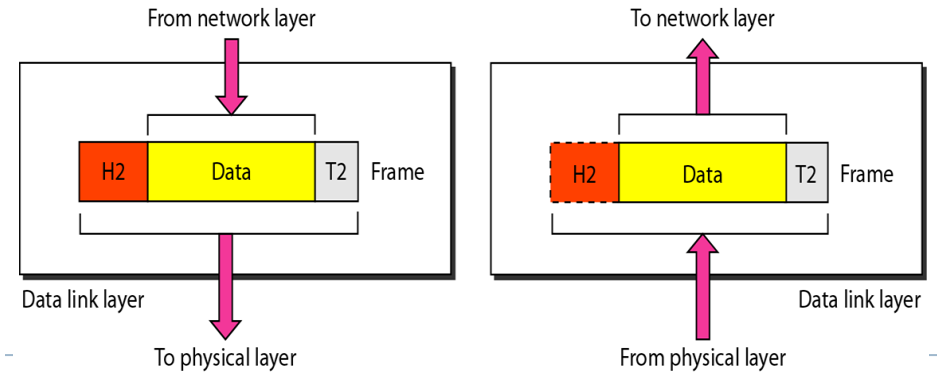
The unit of communication at the physical layer is a bit.

OSI Lower Layers

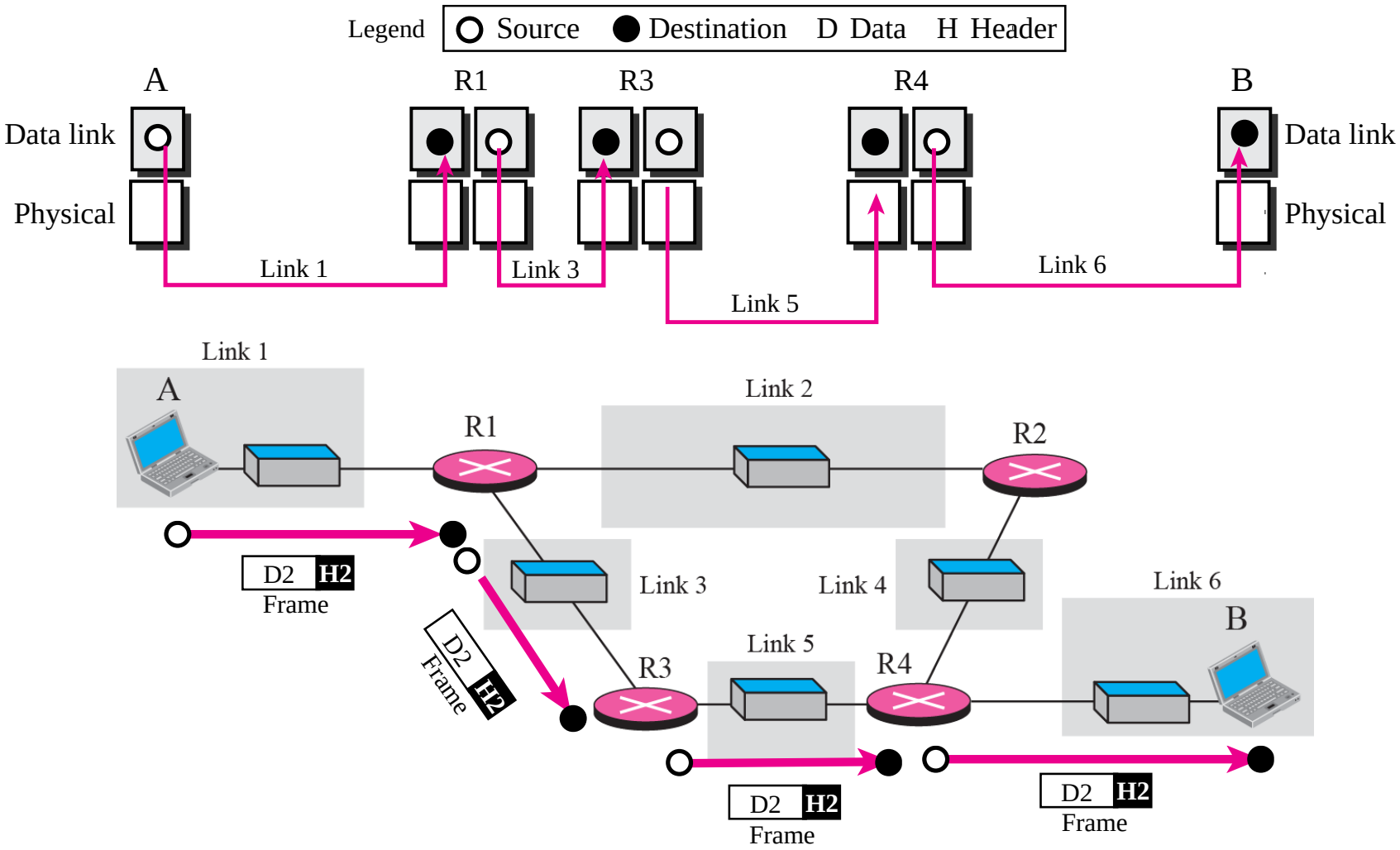


OSI Data Link Layer

1. **Addressing** – Headers and trailers are added, containing the physical addresses of the adjacent nodes, and removed upon successful delivery.
2. **Flow control** – This avoids overwriting on the receiver's buffer by **regulating the amount of data that can be sent.**
3. **Media Access Control (MAC)** – In LANs, it decides who can send data, when and how much.
4. **Synchronization** – Headers have bits, which tell the receiver when a frame is arriving. It also contains bits to synchronize its timing to know the bit interval to recognize the bit correctly. Trailers mark the end of a frame, apart from containing the error control bits.
5. **Error control** – It checks the CRC to ensure the correctness of the frame. If incorrect, it asks for retransmission. Again multiple schemes (positive acknowledgement, negative acknowledgement, go-back-n, sliding window, etc.) exist here.
6. **Node to node delivery** – Finally, it is responsible for error-free delivery of the entire frame/ packet to the next adjacent node (node-to-node delivery).



Communication at the data link layer

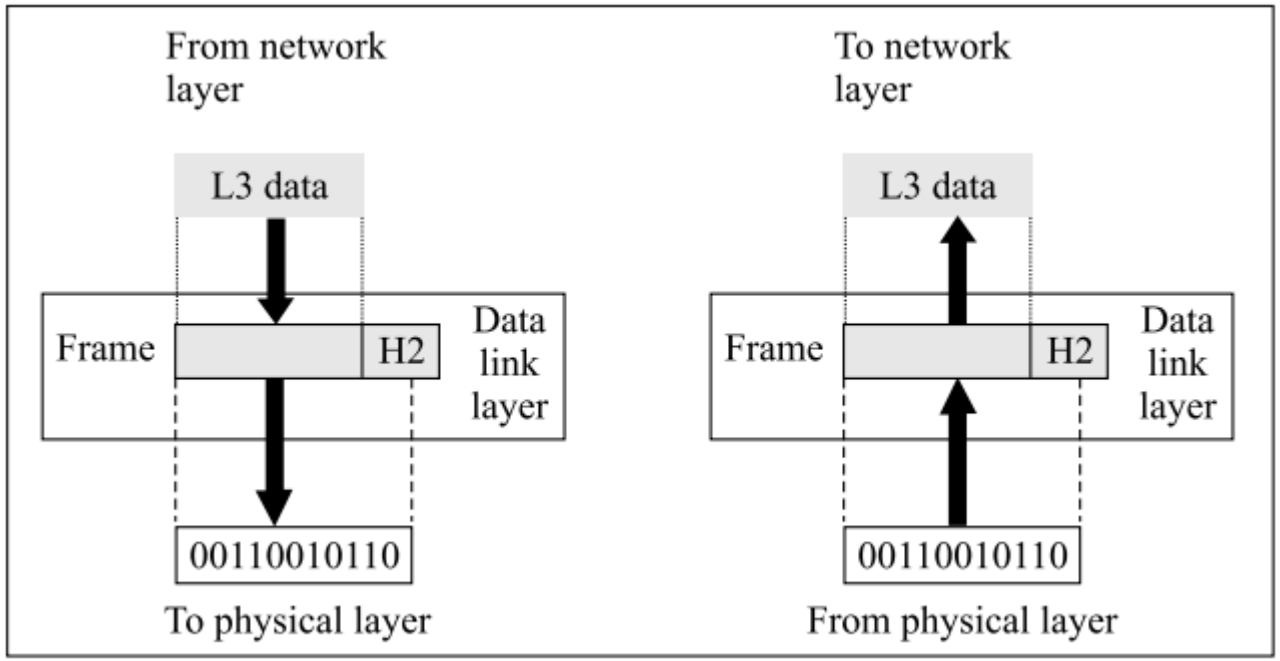


Note

The unit of communication at the data link layer is a frame.

Framing

- Data-link layer takes **packets** from Network Layer and encapsulates them into Frames.
- Then, it sends each frame bit-by-bit on the physical layer.
- At receiver' end, data link layer picks up signals from physical layer and assembles them into frames.



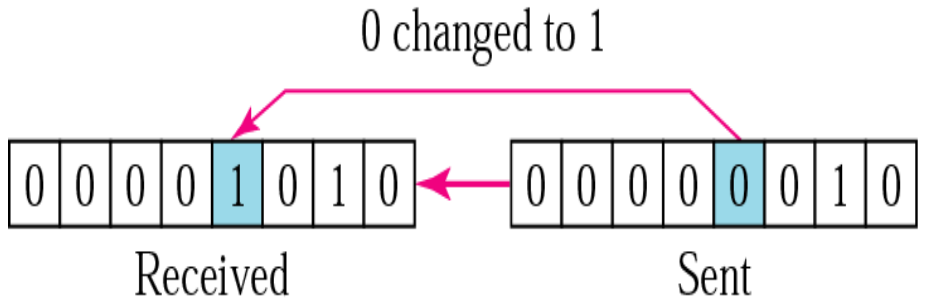
Addressing

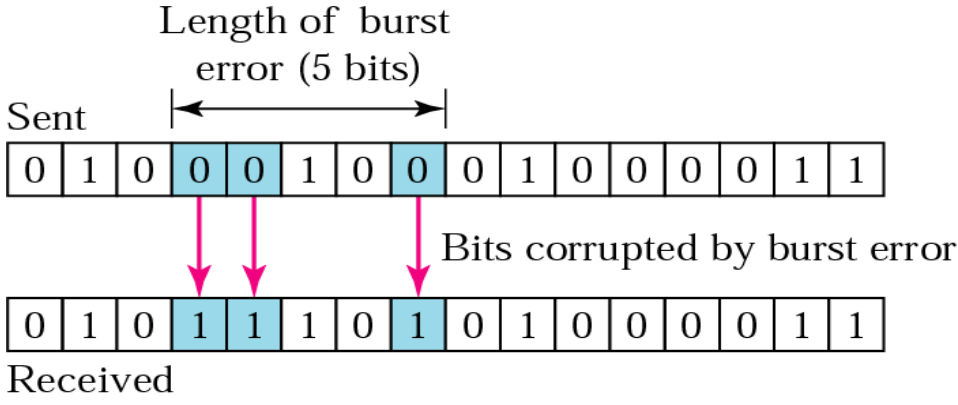
- Data-link layer provides layer-2 hardware addressing mechanism.
- Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- Hardware address is a 6-byte(**48 bits**) physical address (or MAC- Media Access Control address) in hexadecimal;
- written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon/hyphen, as shown below:
- Hardware address or a NIC's address is **permanent** - a LAN address is burned into its ROM during manufacturing

06-01-02-01-2C-4B

Error Detection and Correction

- mainly a data link layer function
- networks must be able to transfer data from one device to another with complete accuracy - our wish
- data can be corrupted during transmission - many factors exist - like transmission impairments
- hence, reliable systems must have a mechanism for detecting and correcting errors
- two types of errors: single-bit and burst
- single-bit error: only *one bit* in a data unit (byte, character, packet, ...) has changed;
- while **Burst** is occurred when *more bit* are affected

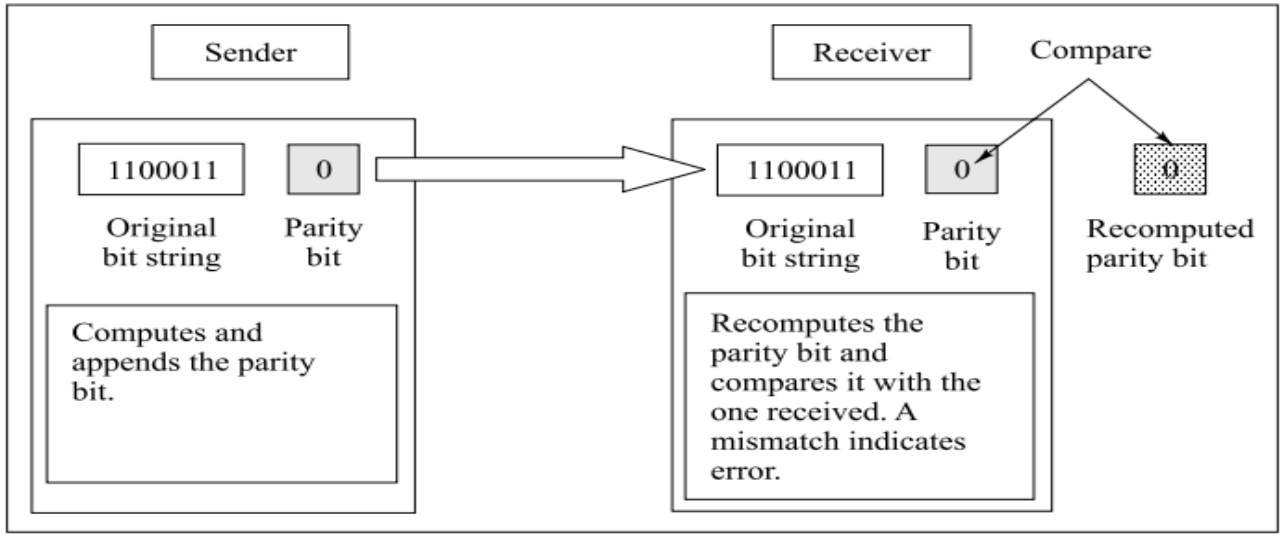




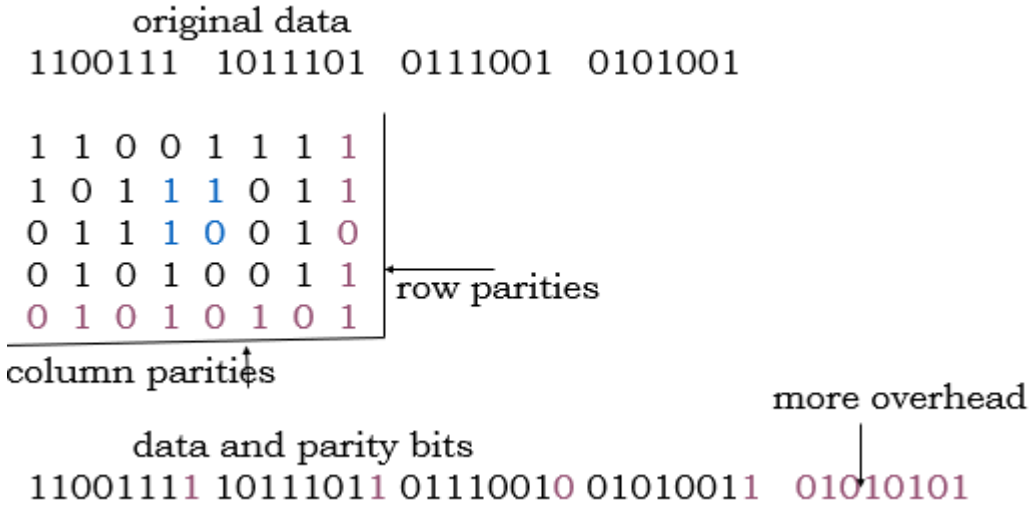
Error Detection and Correction cont'd

- Two types of error-detecting codes: parity and CRC
  - parity check: most common and simple; two varieties

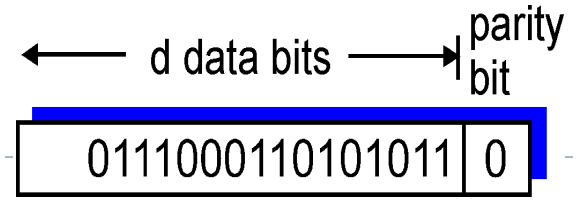
single parity check



2-D parity check:

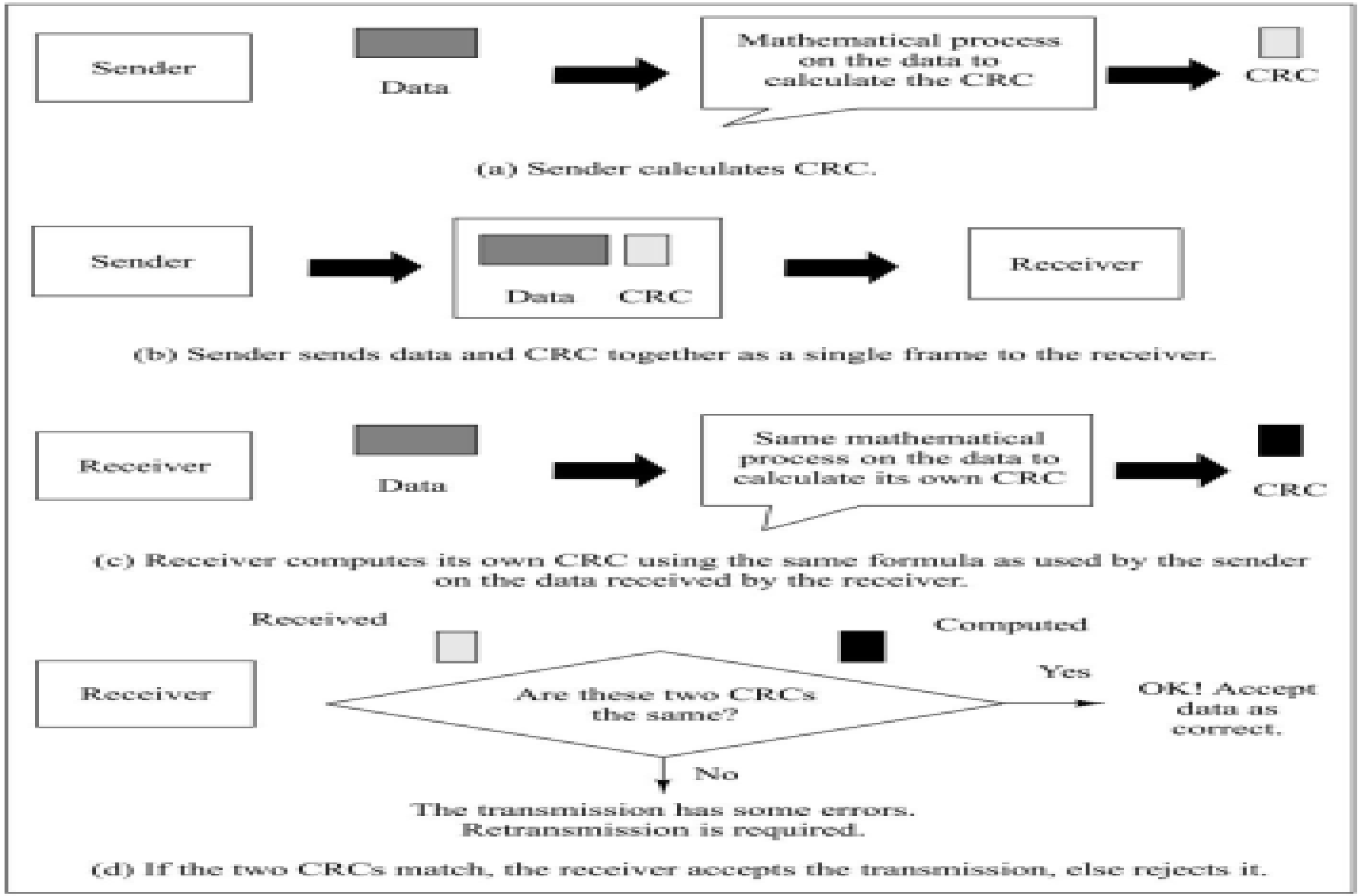


- detect single bit errors



- Can also detect (but not correct) any combination of two errors in a packet

Cyclic Redundancy Check



Error correction

error correction by **retransmission**:

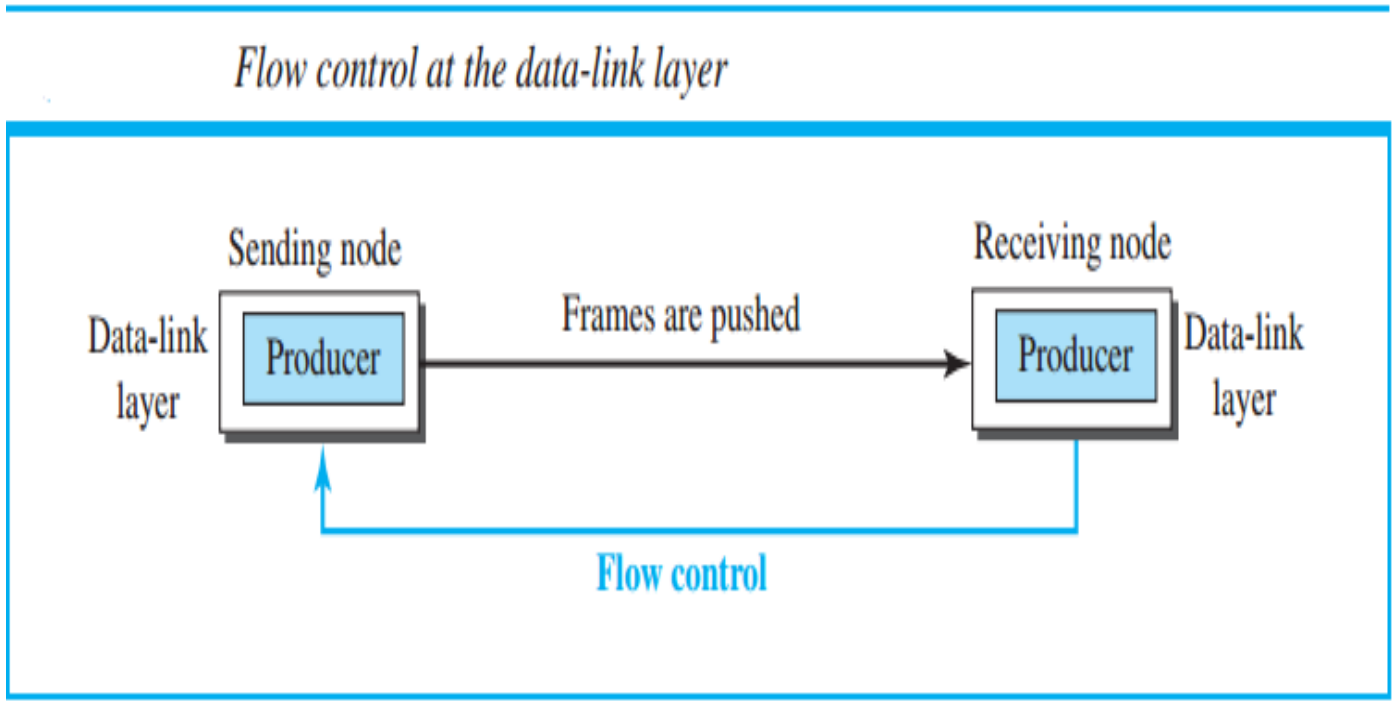
- when an error is detected, the receiver will tell the sender to retransmit the entire data unit; see next: Data Link Control

forward error correction:

- the receiver can use an error-correcting code to correct certain errors;
- the **hamming code** is used to detect and correct errors; you can read more if you are planning to implement error correction

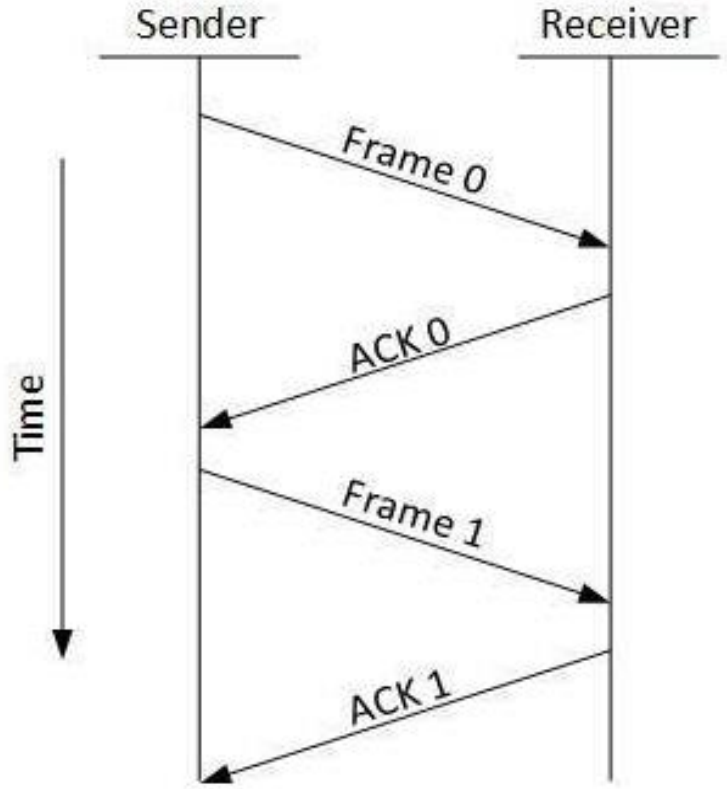
Flow Control

- refers to a set of procedures used to restrict the amount of data that the sender can send before receiving an acknowledgement
- A technique for speed-matching of transmitter and receiver



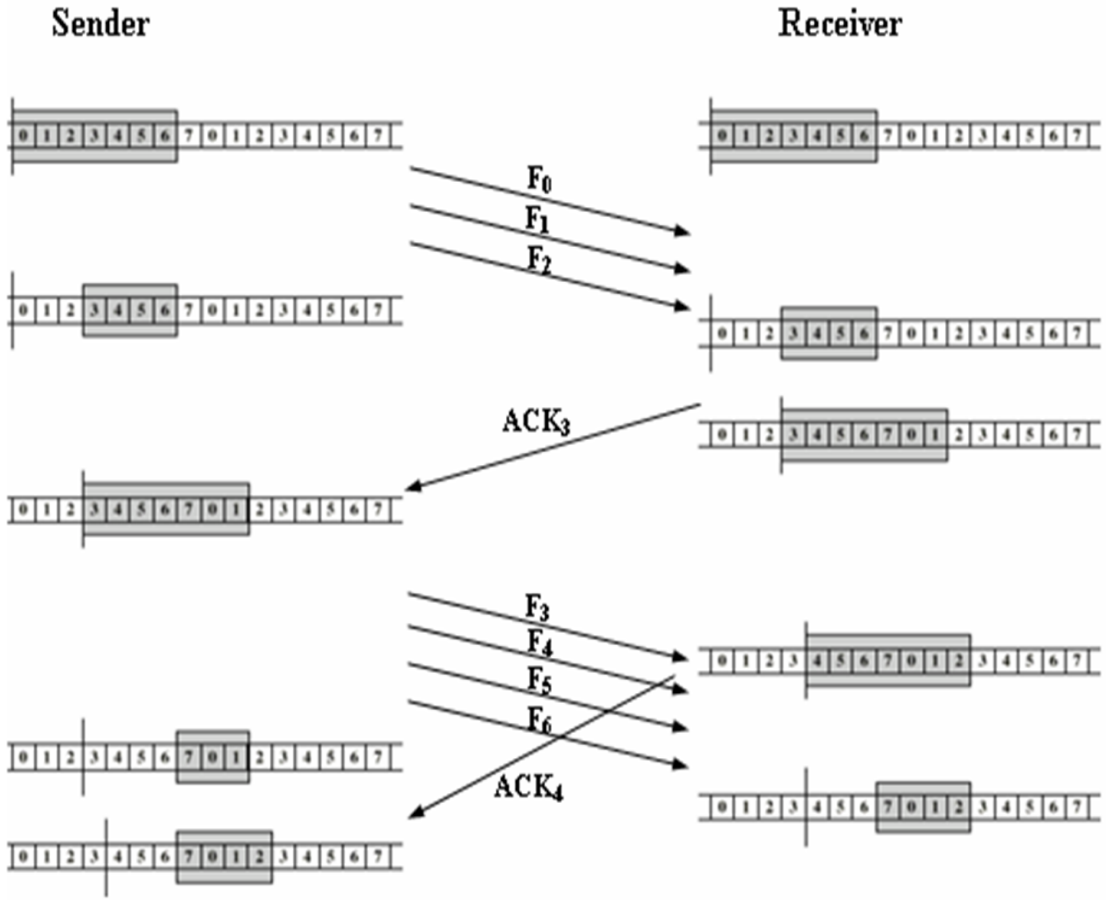
Flow Control Protocols: *Stop-and-Wait Flow Control*

- sender sends one frame, stops until it receives confirmation from the receiver and then sends the next frame.
- only one frame can be transmitted at a time $\Rightarrow$ Inefficiency



Flow Control Protocols: *Sliding Window Flow Control*

- sender can transmit several frames **continuously** before needing an acknowledgement (ACK)
- Each frame is numbered with k-bit sequence number, allowing for 2^k sequence numbers
- Each frame's number is 1 greater than the previous frame and each ACK's number is the number of the *next frame expected* by the receiver



Sliding Window in Action

Error Control

- refers to both error detection and error correction
- in the data link layer, error control refers primarily to methods of error detection and retransmission
- anytime an error is detected, specified frames are retransmitted; this process is called automatic repeat request (ARQ)

Error Control...

Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is *some error in the transit.*
- **Positive ACK** - When the receiver receives a *correct frame*, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

Multi-Access

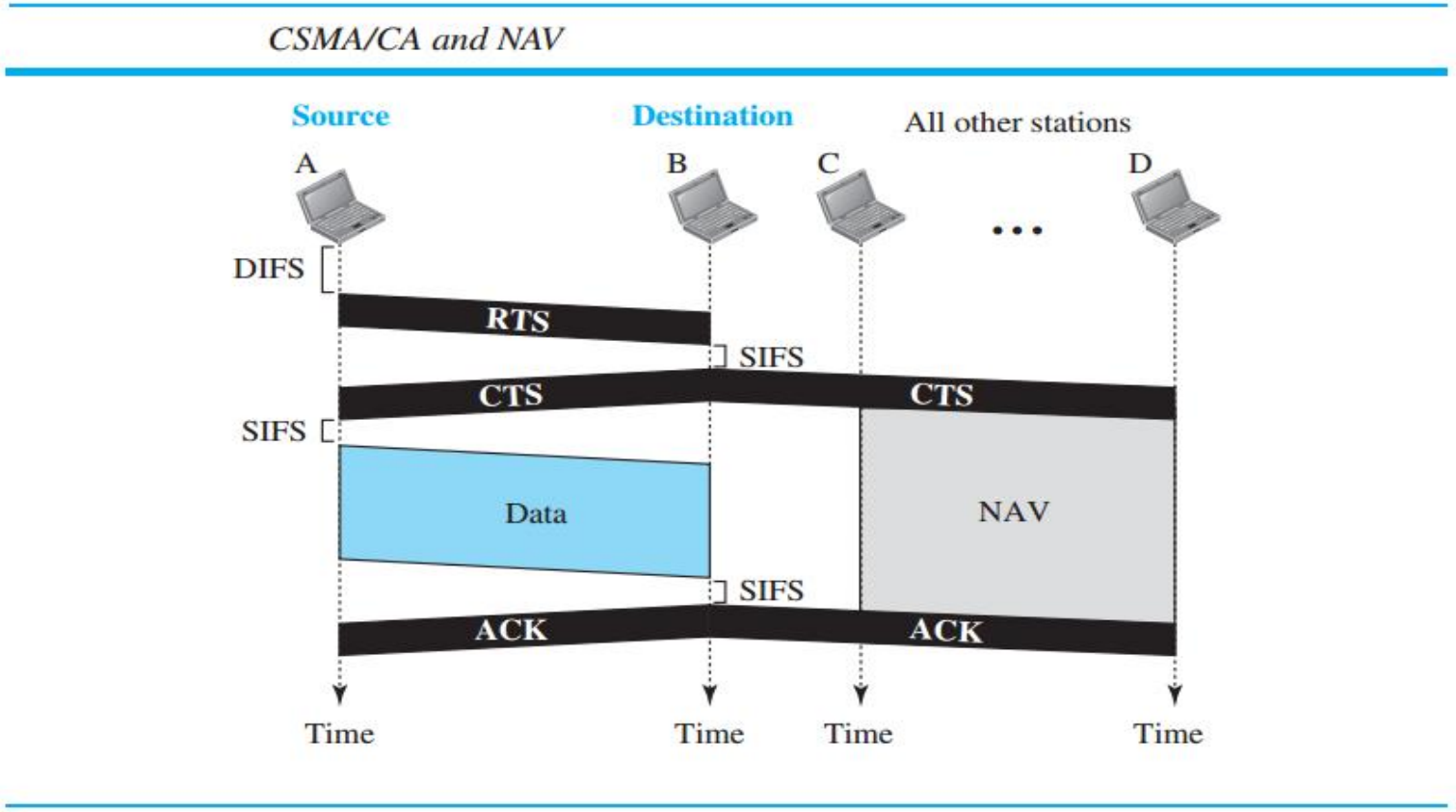
- When host on the shared link tries to transfer the data, it has a high probability of collision.
- Data-link layer provides random access mechanism such as CSMA/CD and CSMA/CA to equip capability of accessing a shared media among multiple Systems.
- There are other multiple access protocols such as
  - Controlled-Access Protocols - get permission
    - Reservation
    - Polling
    - Token Passing
  - Channelization Protocols - simultaneous use
    - FDMA - Frequency-Division MA
    - TDMA - Time-Division MA
    - CDMA - Code-Division MA

Reading(Try your best to understand each)

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

- Carrier Sense Multiple Access/Collision Detection is a technique for multiple access protocols.
- If no transmission is taking place at the time, the particular station can transmit.
- *If two stations attempt to transmit simultaneously*, this causes a collision, which is detected by all participating stations. The devices will wait for random amount of time.**(Back off)**
- *After a random time interval*, the stations that collided attempt to transmit again.
- If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as **exponential back off.**
- Specially designed for ethernet not for Wi-Fi due to
  - Collision detection is difficult for Wi-Fi network due to limited radio range and hidden node problem

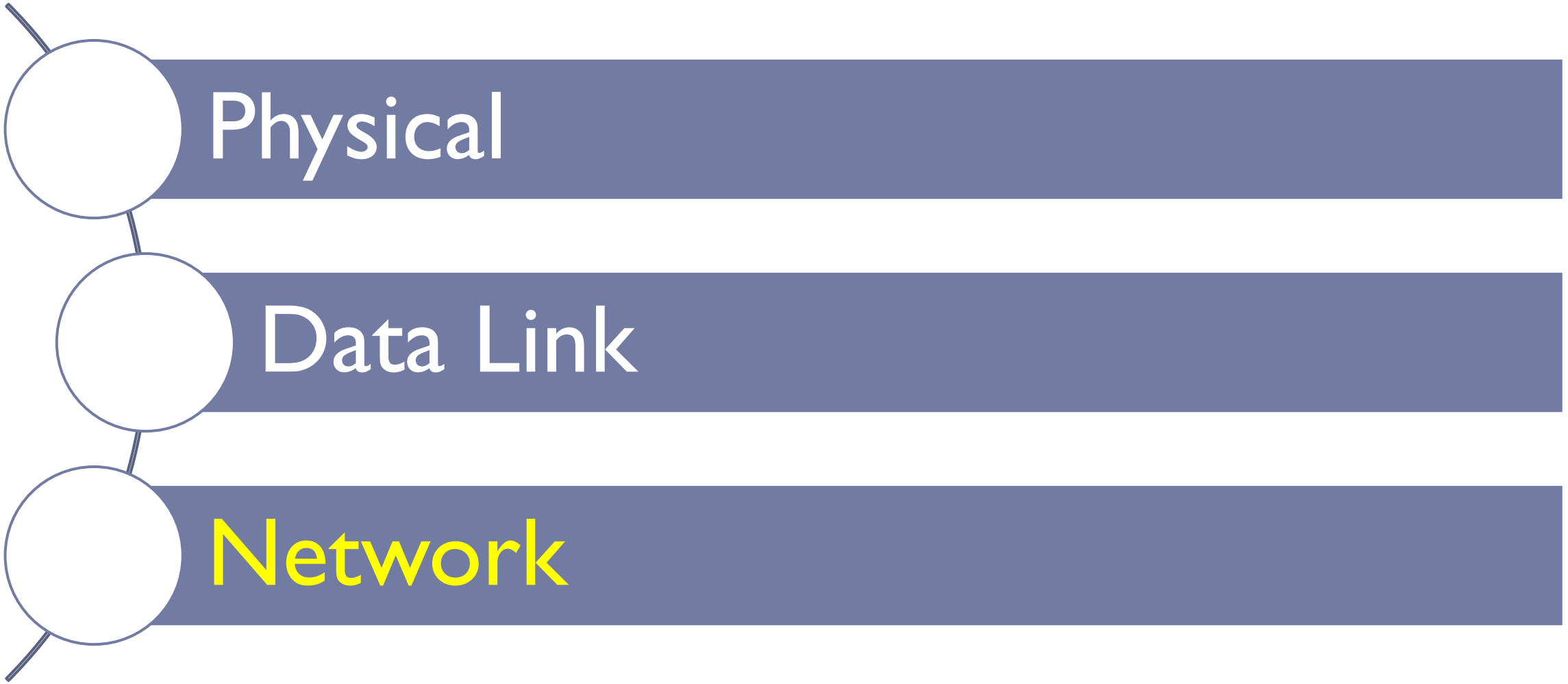
CSMA/CA



NB: Both RTS & CTS frame includes the duration of time that source needs to occupy the channel-transfer duration

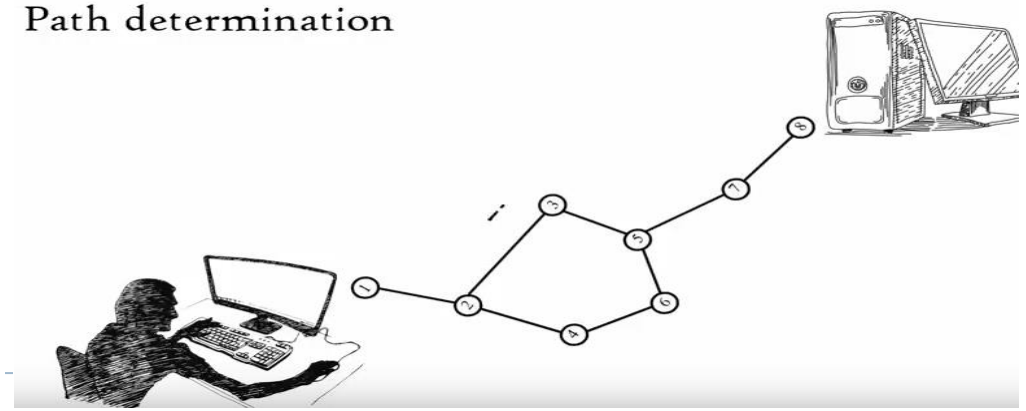
NAV(network animation vector): a period the other station should wait before starting checking for channel idleness

OSI Lower Layers



OSI Network Layer

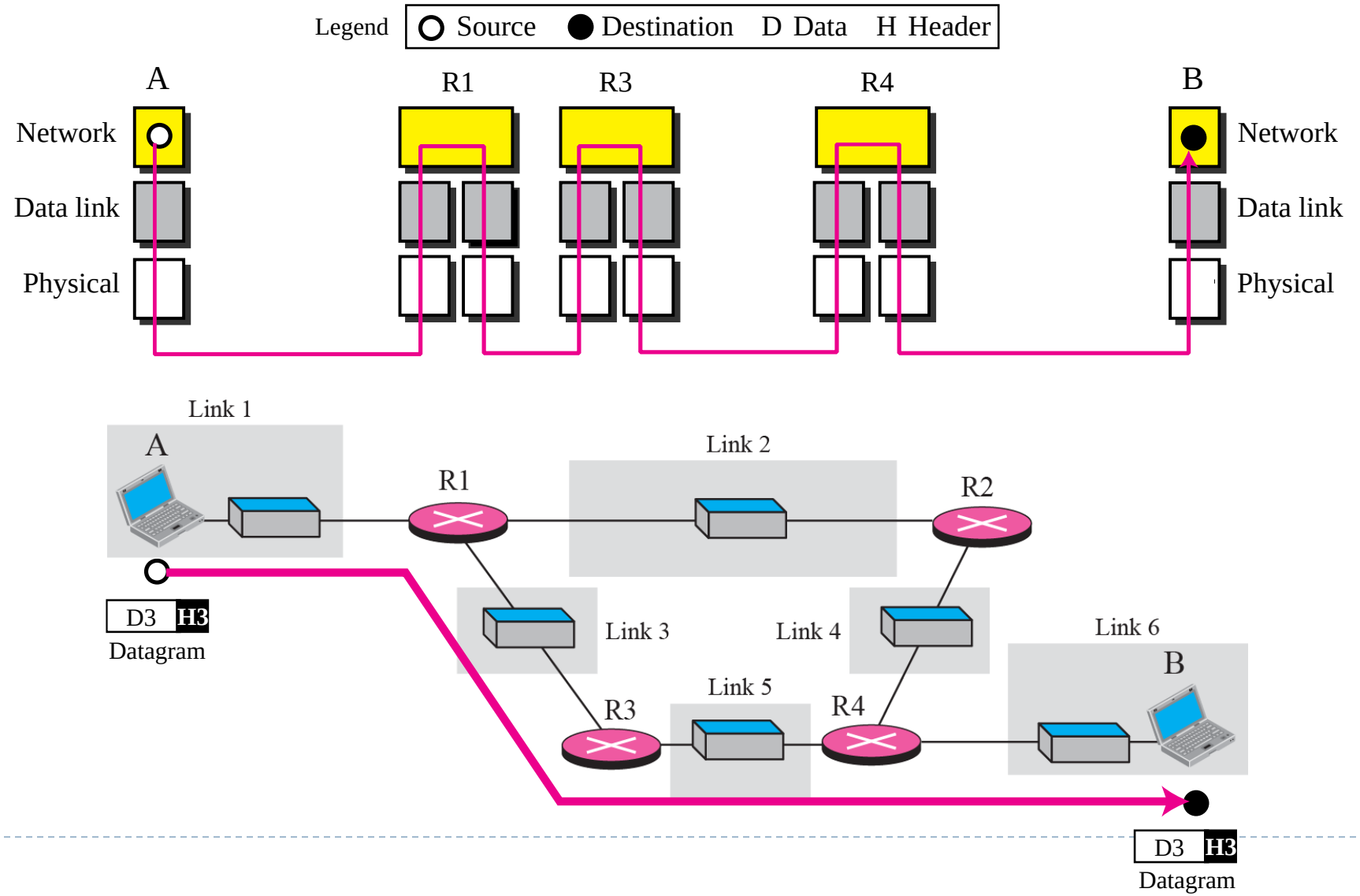
- A key design issue is determining how packets are routed from source to destination→ routing
- path determination
- Routes can be based on ***static tables*** that are "wired into" the network and rarely changed, and can be ***highly dynamic***, being determined a new for each packet
- When two network connected for communication:
  - There may be addressing difference
  - Protocol difference
  - Packet size of each can be different
- It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.



Network Layer has 4 basic functions:

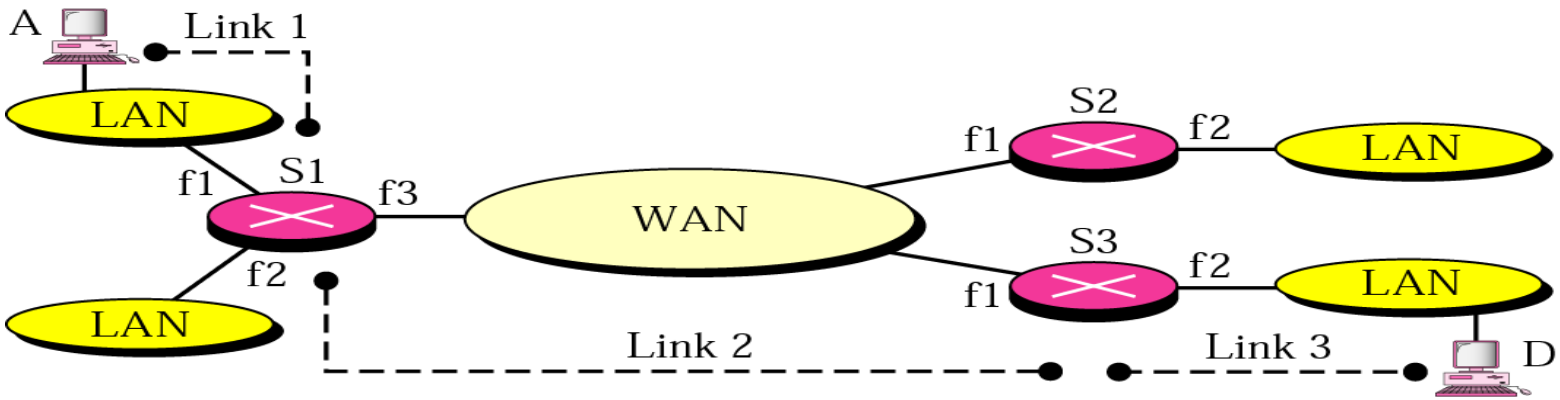
- Internetworking
- Addressing
- Packetizing
- Fragmentation
- Routing

- Main functions of routers (network layer devices)
  - Routing (Path determination): selecting best path b/n end devices
    - Routing protocols(RIP, OSPF, BGP)
  - Forwarding: move packets from router's input to appropriate router output


Legend
Source
Destination
D Data
H Header
A
R1
R3
R4
B
Network
Data link
Physical
Network
Data link
Physical
Link 1
A
Link 2
R1
R2
D3
H3
Datagram
Link 3
Link 4
Link 6
B
Link 5
R3
R4
D3
H3
Datagram

Internetworking

- internetworking refers to the logical gluing of heterogeneous *physical networks* together to look like a *single network* to the upper transport and application layers



- the above internetwork is made up of 5 networks: 4 LANs and 1 WAN
- S_i: switch or router; f_i: interface
- data sent from A to D passes through 3 links
- nomenclature:
  - the source and the destinations are usually referred to as **hosts**
  - a host or a router is referred to as a **hop**

Packetizing and Fragmenting

Packetizing:

- encapsulates packets received from upper-layer protocols and makes new packets out of them; done by the IP protocol in the Internet model

Fragmenting:

- a datagram can travel through different networks; each router decapsulates the IP datagram from the received frame, processes it, and then encapsulates it in another frame
  - the format and size of the
    - received frame depends on the protocol used by the physical network from which the frame has just arrived
    - departing frame depends on the protocol used by the physical network to which the frame is going



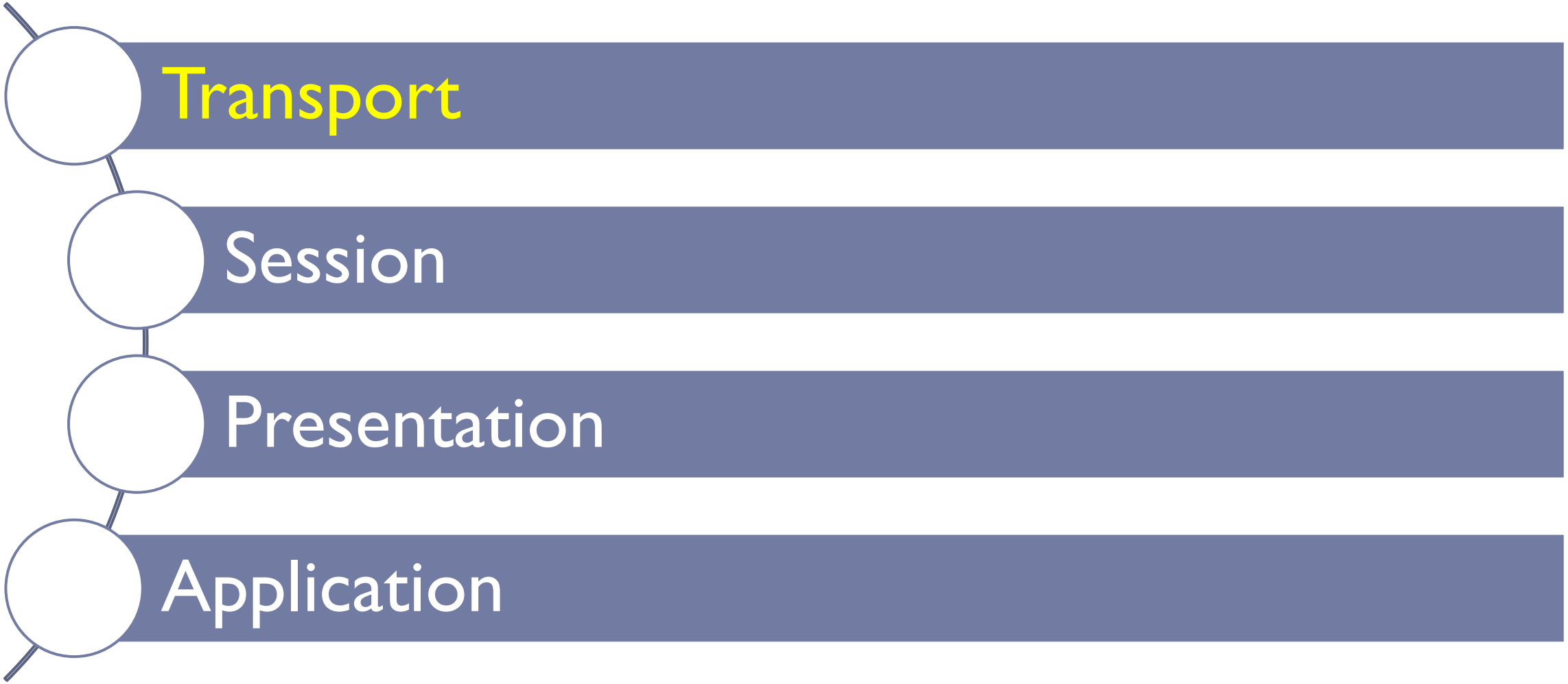
Addressing

- To uniquely and universally identify each device on the internet to allow global communication between all devices
- Analogous to the telephone system; the department of computer science: 251 011 1222922, wherever you are on the globe
- Each address belongs to a single host, but a single host can have multiple addresses (if it has multiple connections to the internet)
- The identifier used in the network layer of the internet model is called the internet address or IP address
- It is a 32-bit binary address (in ipv4)

Network layer protocols

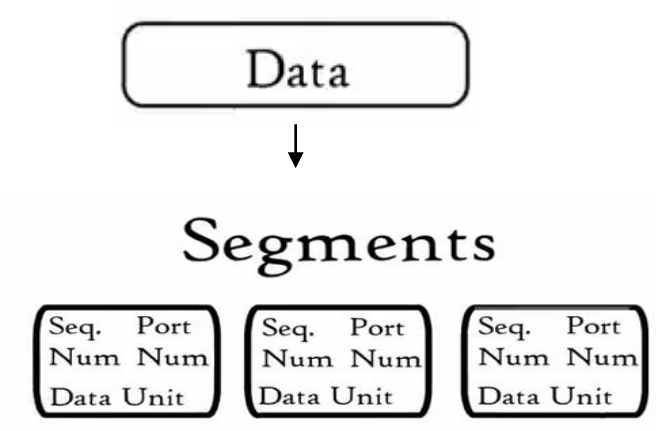
- *There are 5 network layer protocols in the TCP/IP*
- The main protocol is IP, the glue that holds the whole internet together and responsible for host-to-host delivery
- It needs the services of other protocols
  - **ARP (address resolution protocol)** - maps an IP address to a MAC address (of the next hop)
  - **RARP (reverse ARP)** - maps a MAC address to an IP address; usually used in some situations such as when a diskless host is booted; it gets the binary image of its operating system from a remote file server but does not know its IP address; obsolete, replaced by **DHCP-** dynamic host configuration protocol
  - **ICMP (internet control message protocol)** - to handle unusual situations such as the occurrence of an error
  - **IGMP (internet group management protocol)** - for multicasting since IP is designed for unicast delivery;

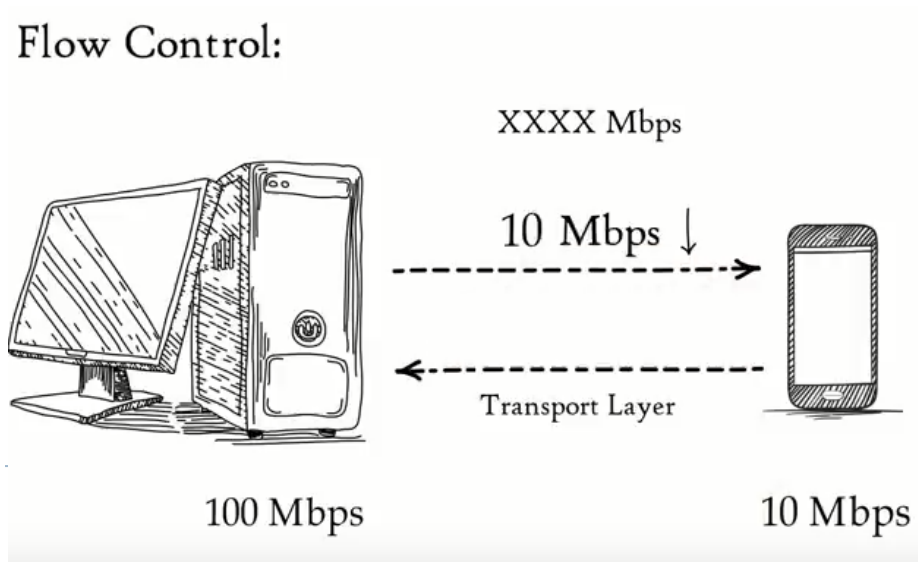
OSI Upper Layers

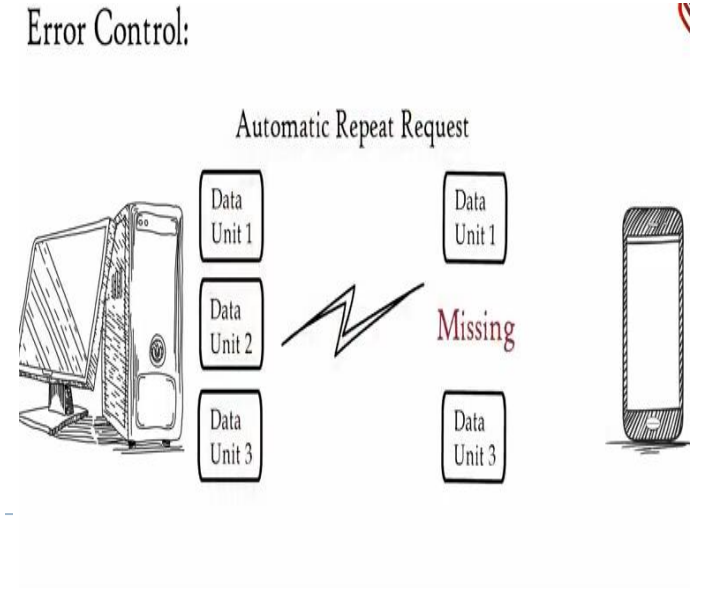


OSI Transport Layer

- Isolates messages from lower and upper layers
- Segmentation: Breaks down message size
- Error control and flow control: Monitors quality of communications channel
- Selects most efficient communication service(connection oriented and connection less transmission service) necessary for a given transmission

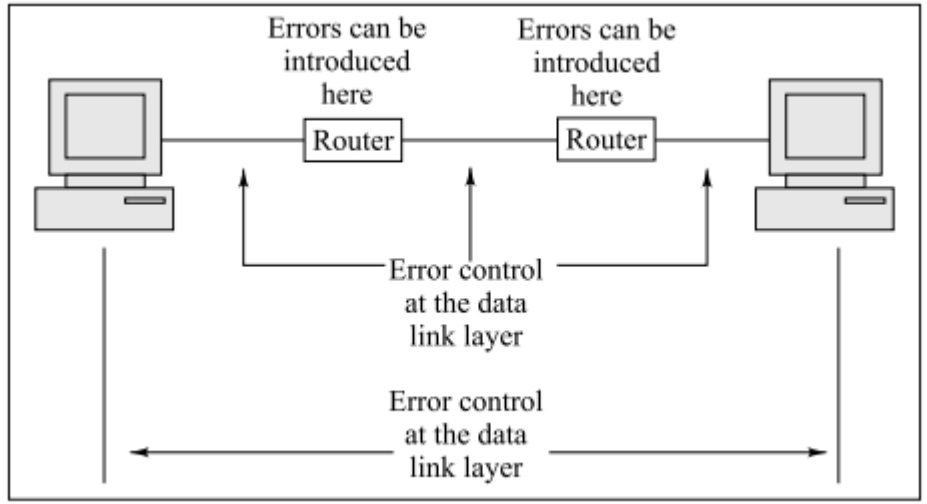






Transport layer Functions

- Process to process communication
- Addressing: port numbers
- Encapsulation and Decapsulation
- Multiplexing and demultiplexing
- Flow control
- Error control
- Congestion control

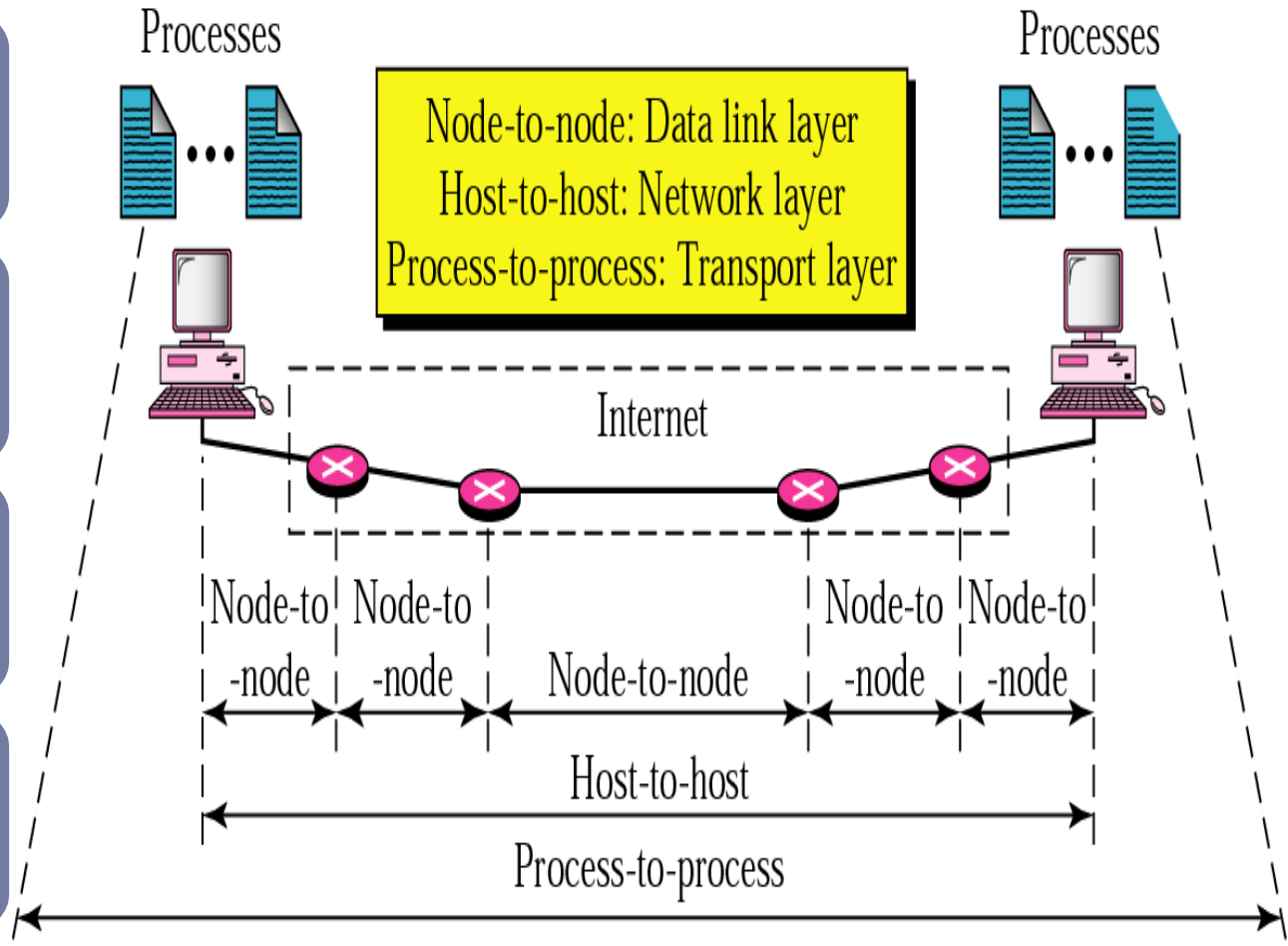


data link layer: node-to-node delivery

network layer: host-to-host delivery

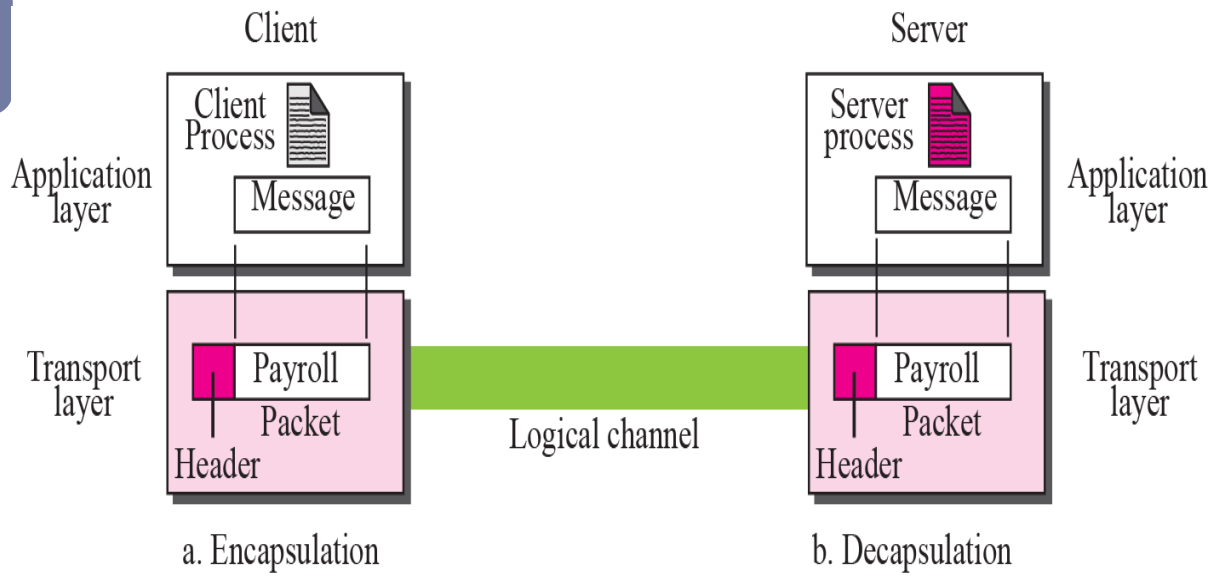
transport layer: process-to-process delivery

several processes may be running on the source as well as the destination; an addressing mechanism is required



Packetizing

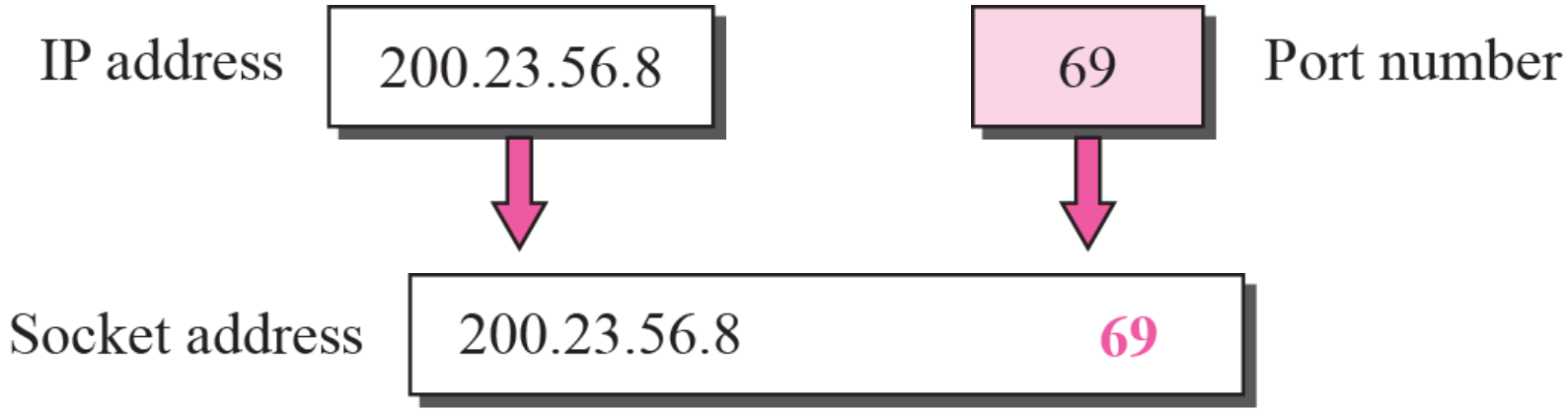
- the transport layer creates packets out of the message received from the application layer
- it divides a long message into smaller ones called segments; they are then encapsulated into the data field of the transport-layer packet and headers are added



Addressing

- at the data link layer, we need a MAC address
- at the network layer, we need an IP address
- at the transport layer, we need a transport-layer address, called a port number, to choose among several processes [0-65,535]

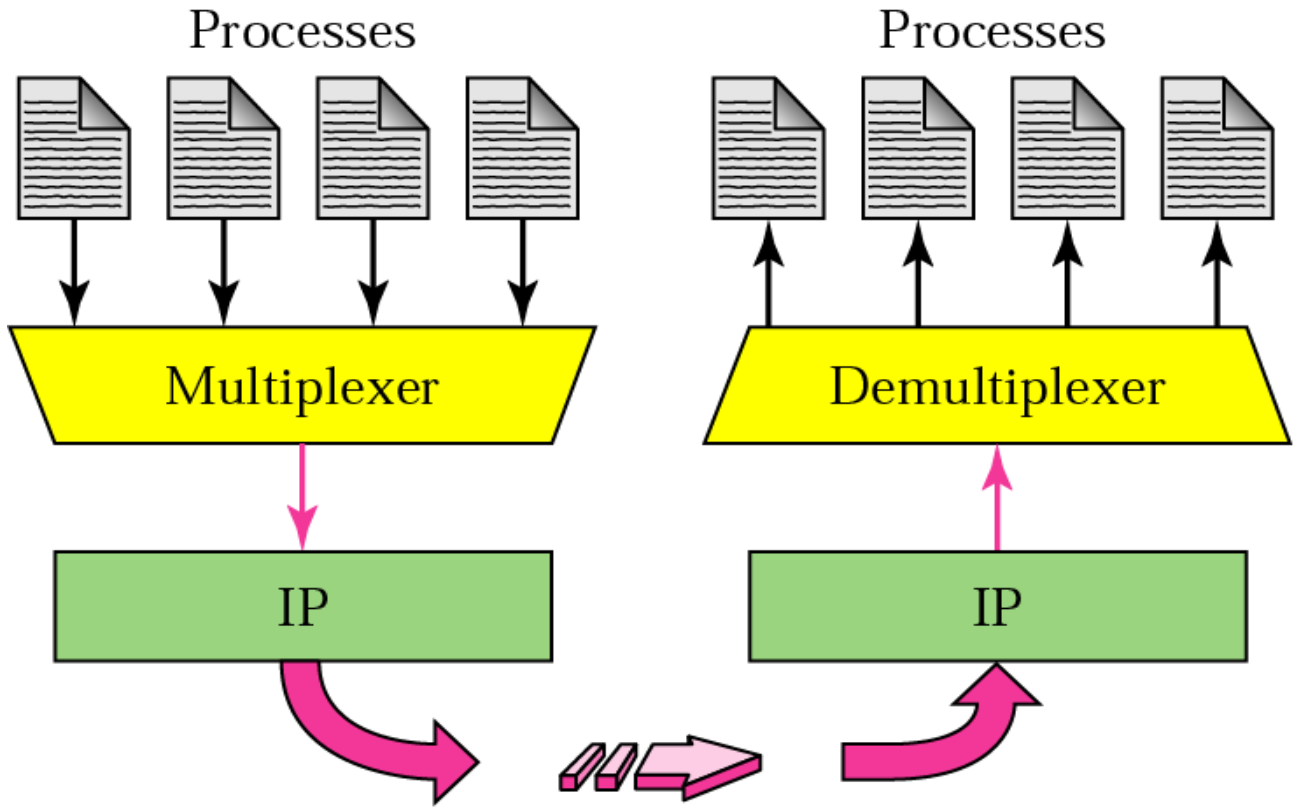
Socket address



- process-to-process delivery needs two addresses: IP address and port number at each end
- the combination of an IP address and a port number is called a socket address

Multiplexing and Demultiplexing

- the addressing mechanism allows multiplexing and demultiplexing by the transport layer since there may be several processes that need to send packets, but there is only one transport-layer protocol (UDP or TCP)

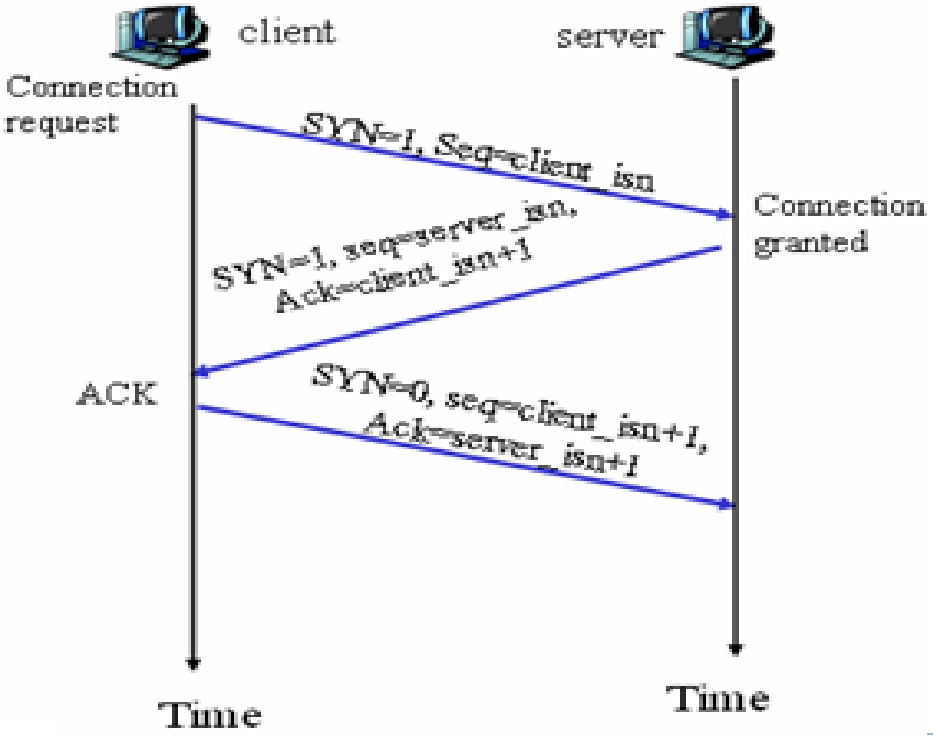


Connection Control Services: Connection less and connection oriented

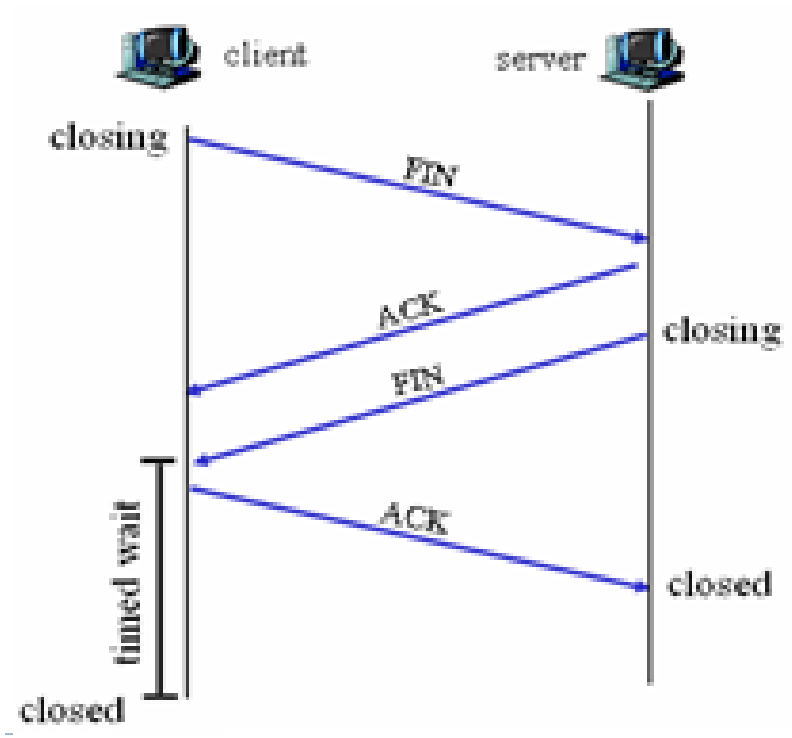
UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
connectionless and unreliable	reliable, but complex
no flow or error control, no retransmission if data is corrupted or lost	Error control, Loss control, Sequence control, Duplication control,
convenient for • multimedia and multicasting applications • for client-server situations • e.g., DNS can use UDP, give me the IP address of the host name www.hu.edu.et	Convenient for: File Transfer Protocol (FTP), Remote login – TELNET, Email – SMTP, World Wide Web – HTTP etc.
Some well known ports used by UDP(more : www.iana.org) DNS 53 Echo 7 TFTP 69	Some well known ports used by TCP(more : www.iana.org) Telnet 23 FTP:Data: 20 FTP: Control: 21

TCP Connection management

- Connection setup (*three-way handshake*) and connection termination in TCP look as follows:
- TCP requires connection establishment before data transfer begins.
- For a connection to be established or initialized, the two hosts must synchronize their Initial Sequence Numbers (ISNs).



TCP Three-way handshake



Closing a TCP Connection

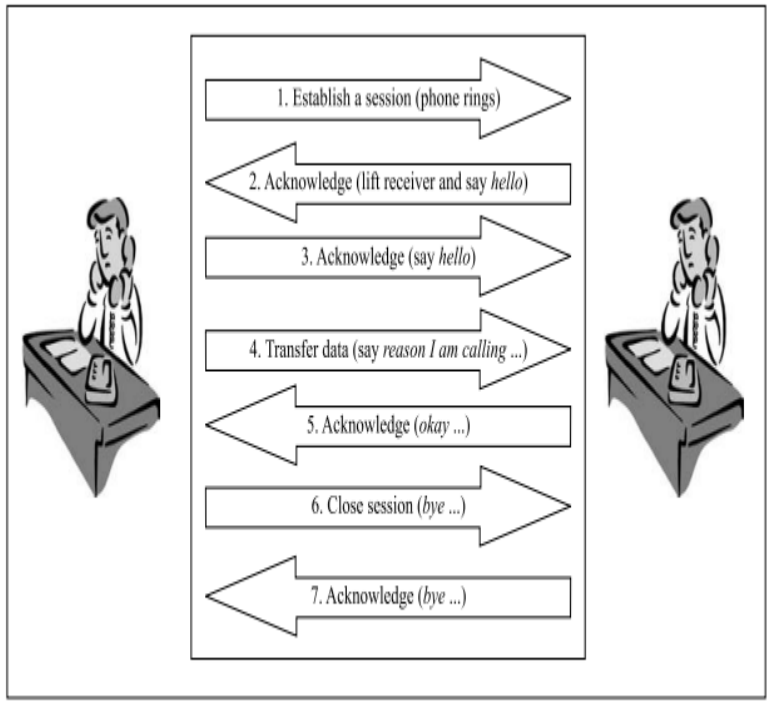
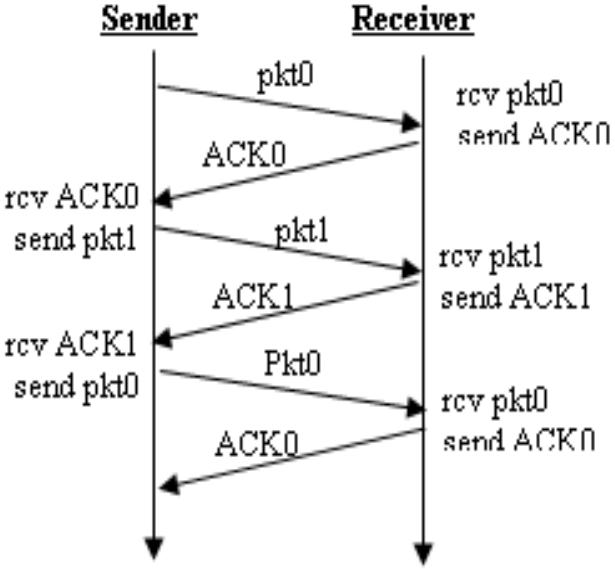


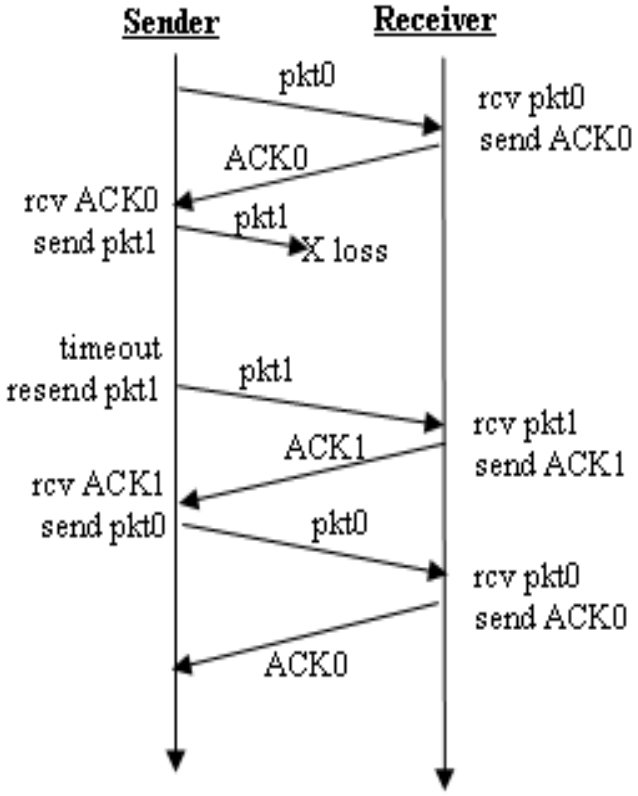
Fig. 18.15 *Concept of a TCP connection with reference to a telephone call*

TCP Transmission

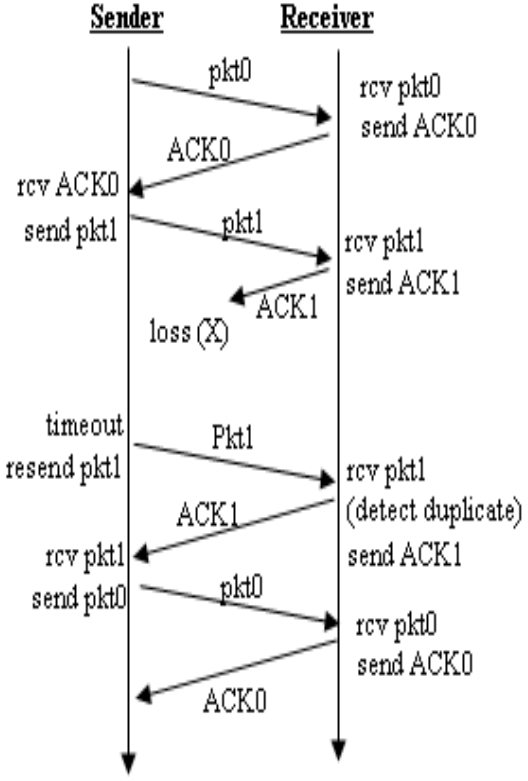
- Reliable delivery in TCP is realized using acknowledgement
- Stop-and-wait protocol scenarios



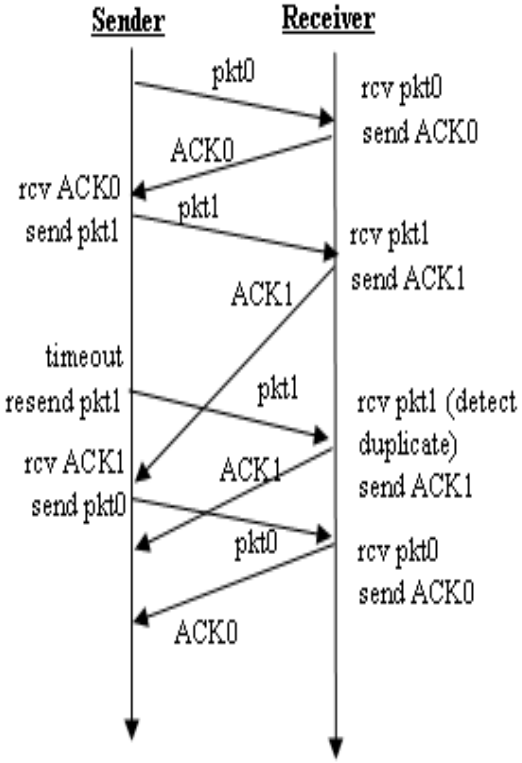
(a) Operation with no loss



(b) Lost packet

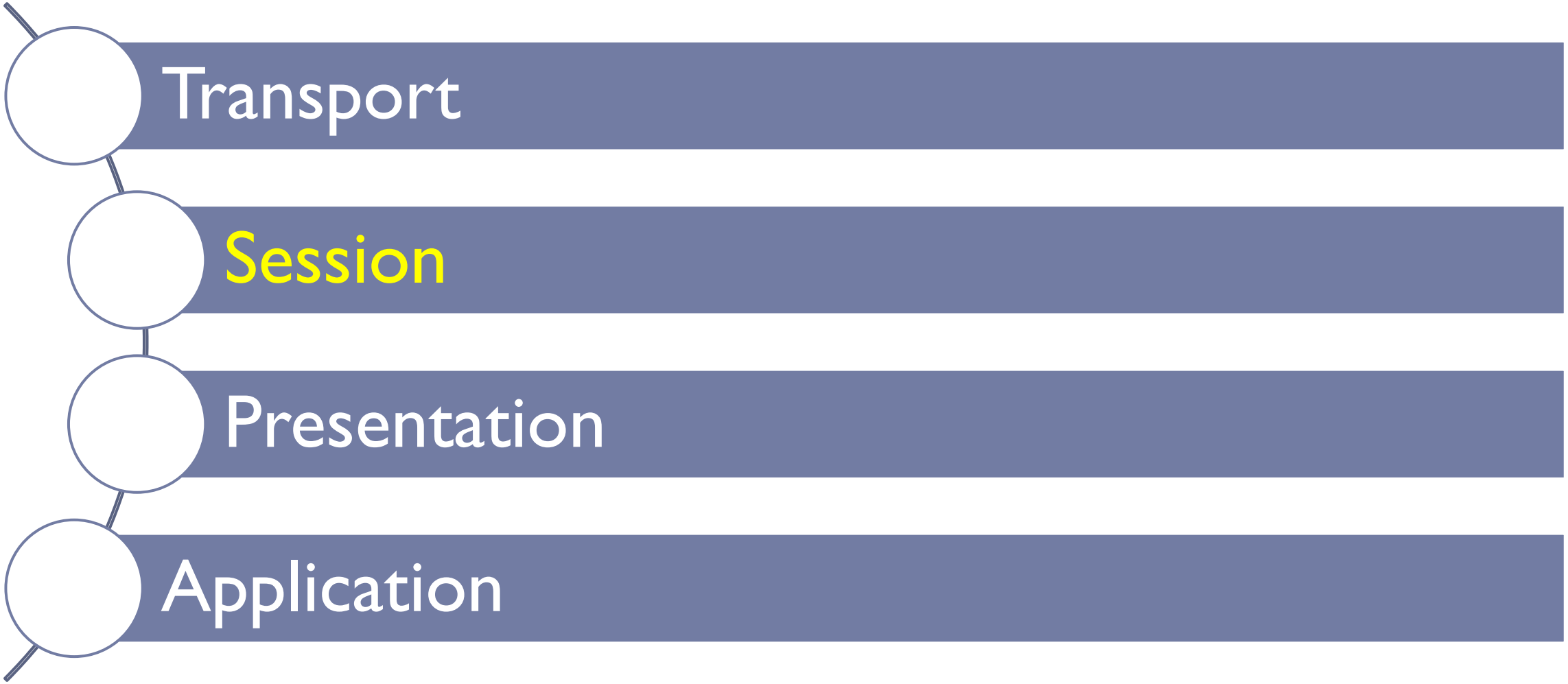


(c) Lost ACK



(b) Premature timeout

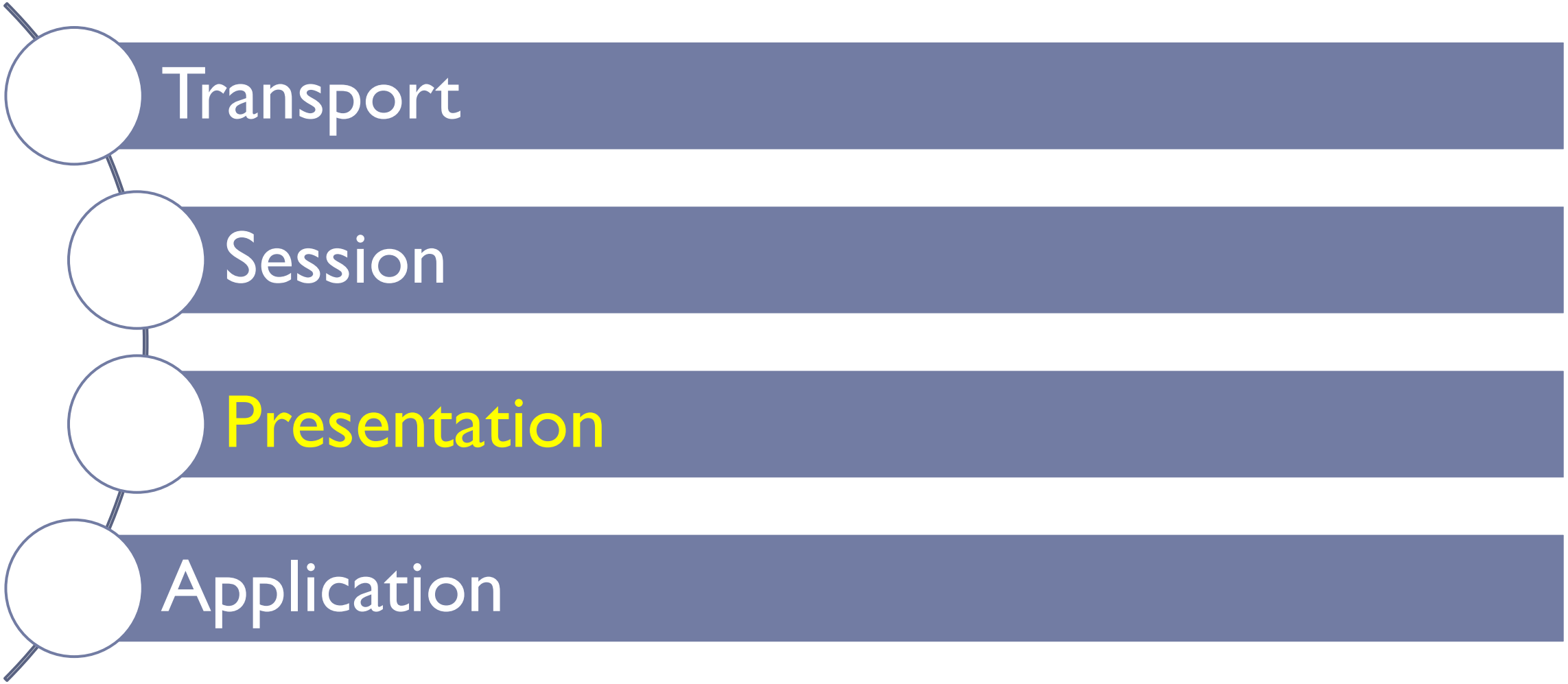
OSI Upper Layers



OSI Session Layer

- Establishes logical connections between systems
- Manages log-ons, password exchange, log-offs
- *Terminates* connection at end of session

OSI Upper Layers



OSI Presentation Layer

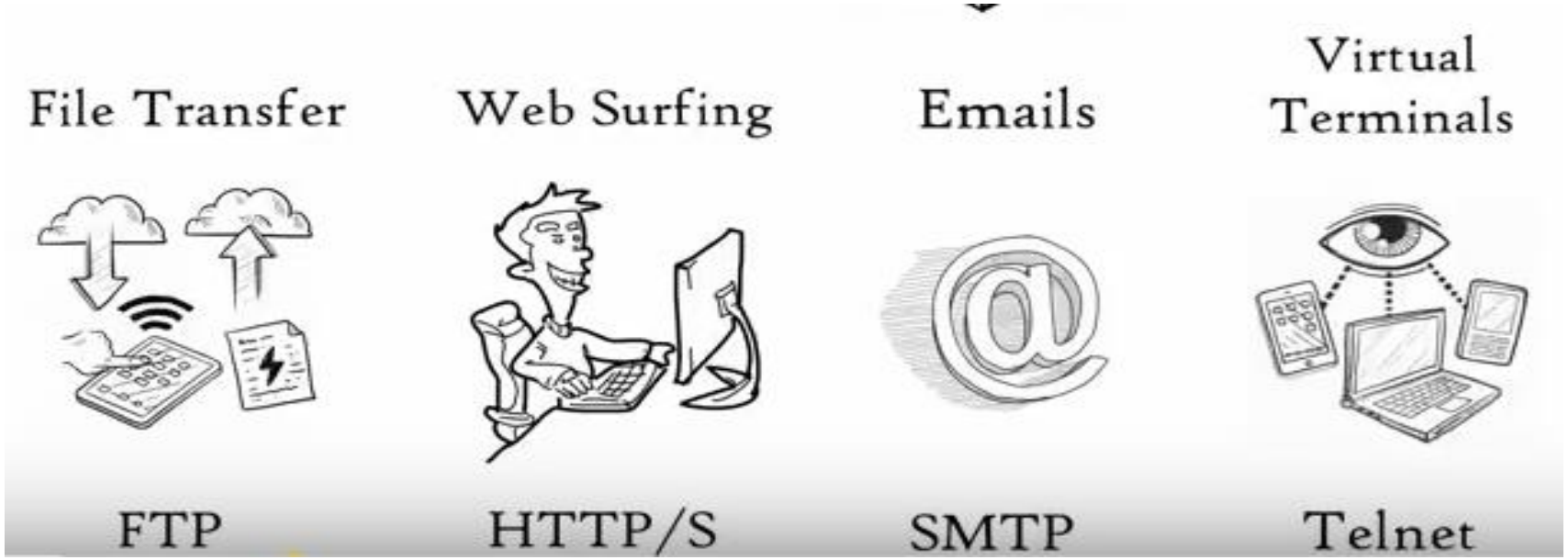
- Provides *format conversion* or translation (original message → machine understandable language)
- Data compression
- Maintain data Integrity through encryption and decryption
- SSL(Secure socket layer) is a protocol used for data encryption

OSI Upper Layers

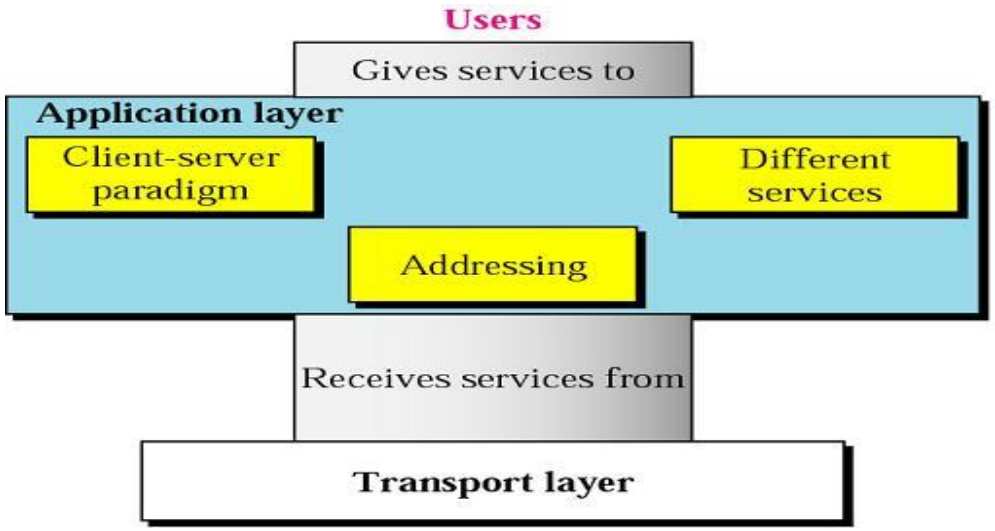


OSI Application Layer

- Provides access to network for *end-user*
- receives services from the transport layer and provides services to users (humans or software)
- provides *user interfaces* and support services such as email, remote file access and transfer, access to the WWW.

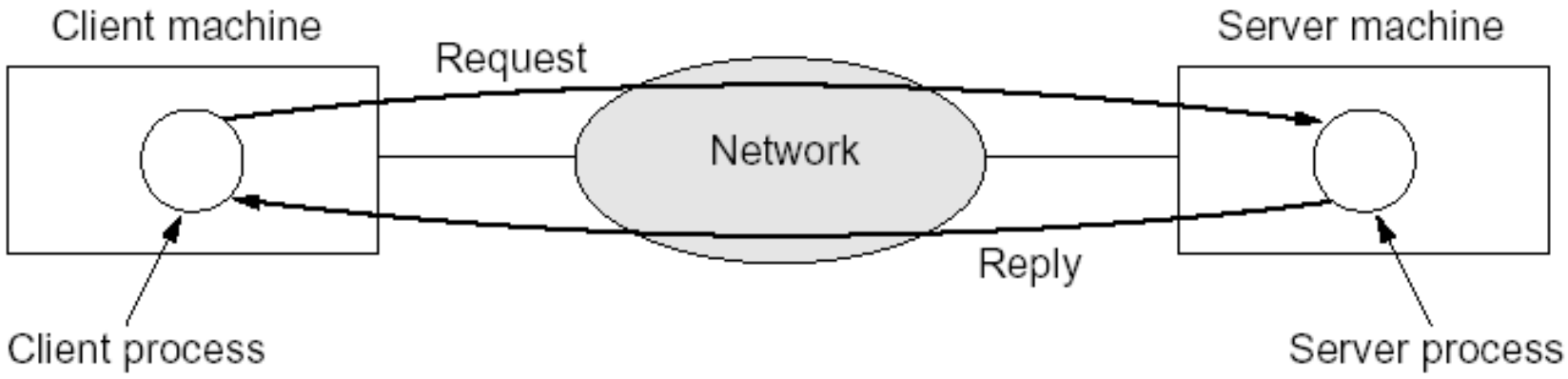


- Receives services from the transport layer and provides services to users (humans or software)
- Provides user interfaces and support services such as email, remote file access and transfer, access to the WWW
- Three general issues related to the application layer:
  - the client-server paradigm,
  - addressing, and services



The Client-Server Model

- to do a task, there must be a client and a server
- a computer runs a program to either request a service from another computer (client) or to provide a service to another computer (server)
- communication takes the form of the client process sending a message to the server process and then waiting for a reply
- a client program runs when needed, but the server program runs all the time



Addressing

A client and a server communicate with each other using addresses

Addressing mechanism in the application layer is different from the ones in other layers

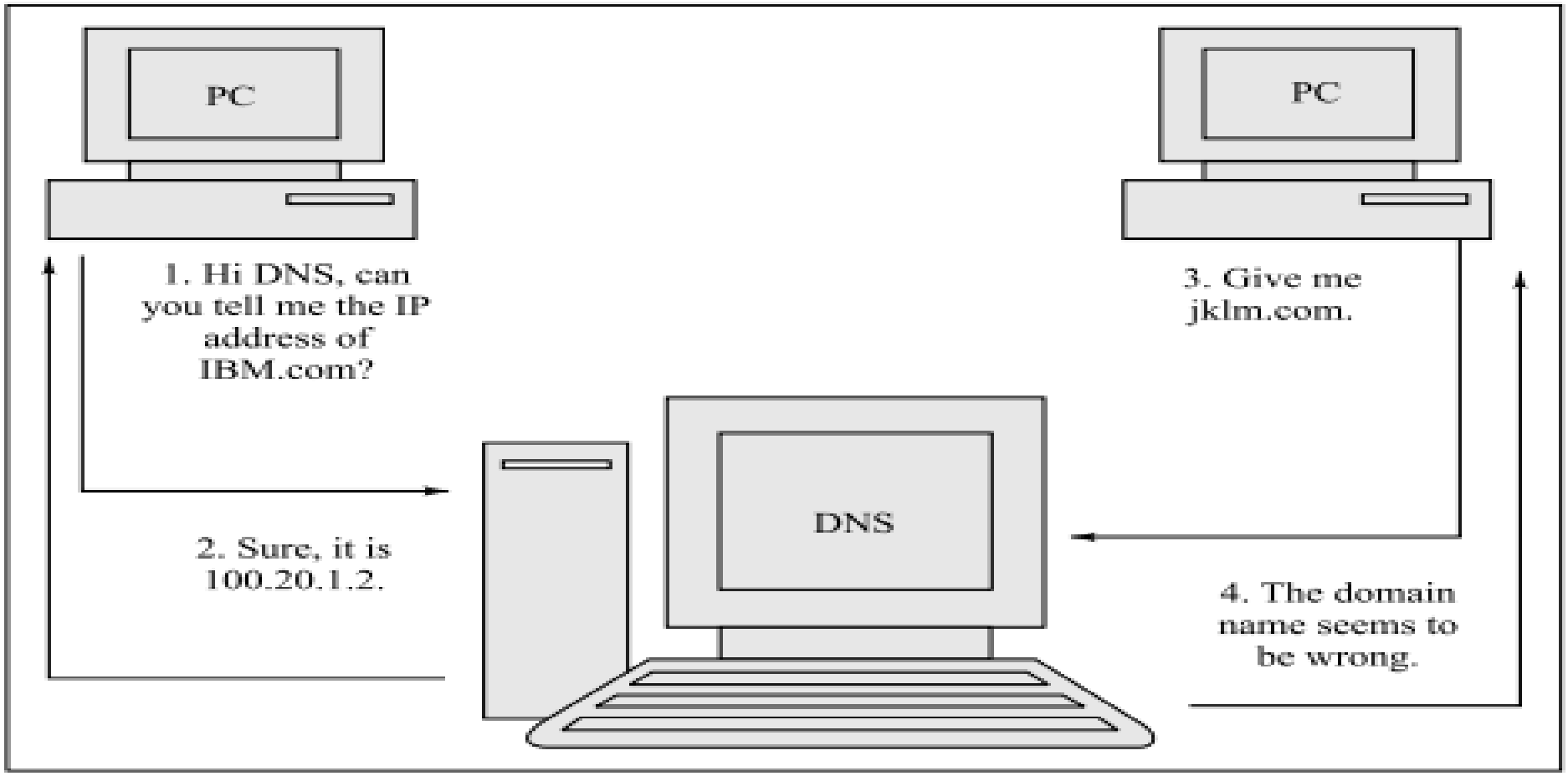
- email address: xy@gmail.com
- Web page (host name): http://www.hu.edu.et

These are aliases convenient for human beings; they must be mapped to IP addresses

An application program needs the services of another program for this; this application program is called DNS - domain name system: it uses port 53

It is not directly used by the user; but by application programs to perform the mapping

Domain Name Resolution

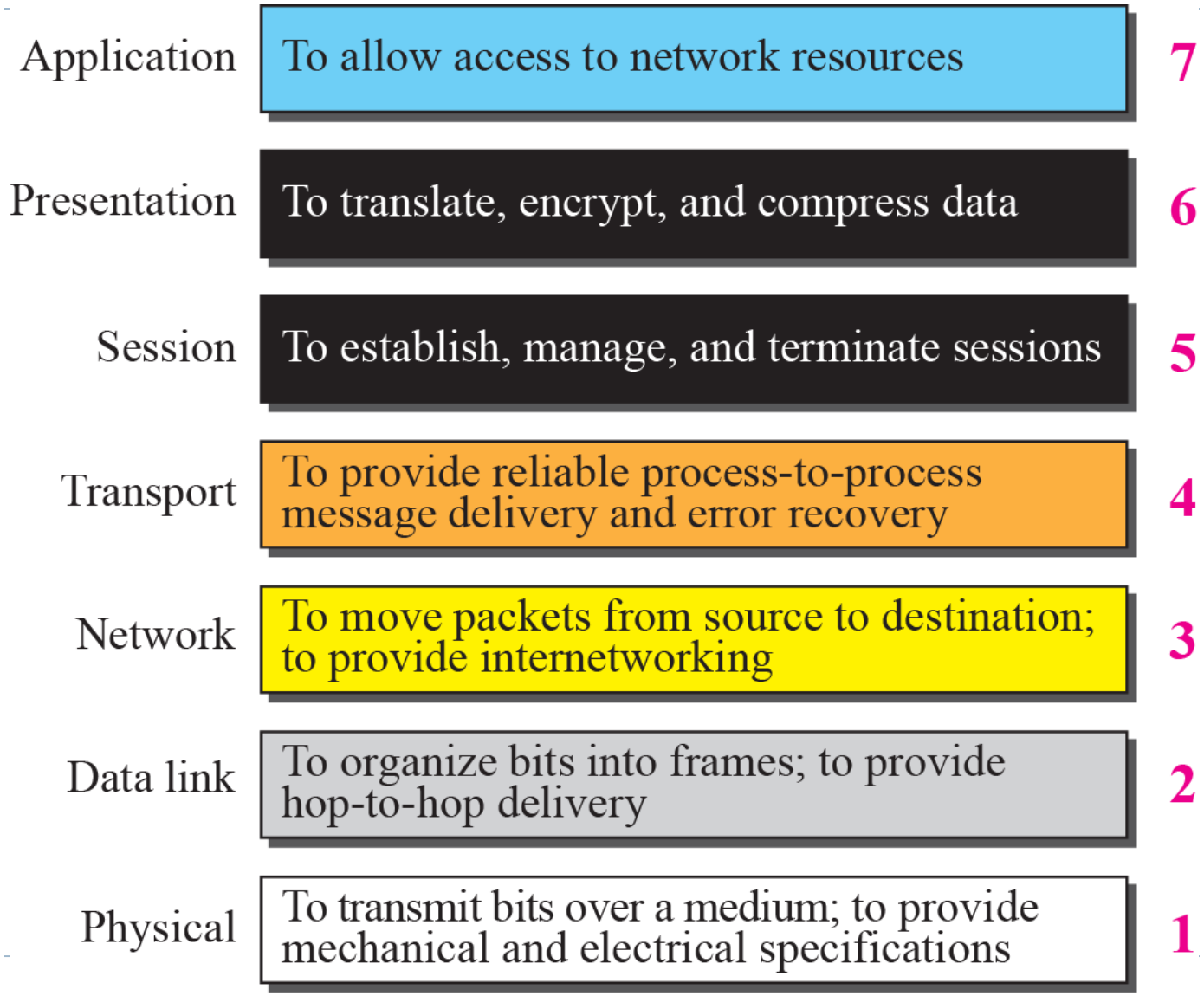


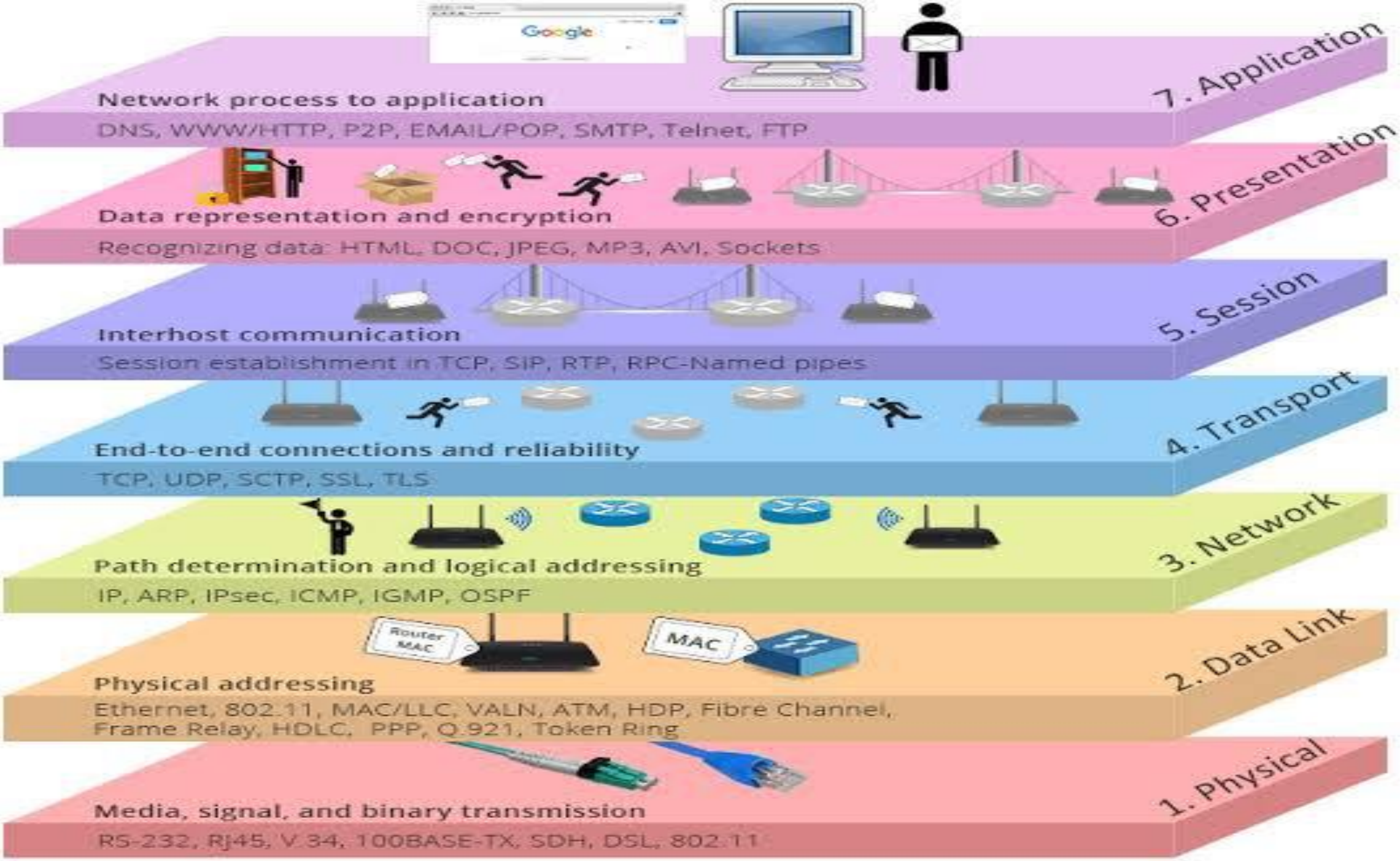
Application Layer Services

- Electronic mail
  - SMTP: simple mail transfer protocol
  - MIME: multipurpose internet mail extensions
  - POP3 : post office protocol 3
  - IMAP : internet mail access protocol
  - Webmail
- File transfer (FTP - file transfer protocol)
- HTTP - hypertext transfer protocol for accessing data on the WWW
- Www
- Multimedia

Application Services	protocols	Remarks
File transfer Protocol	FTP	used to send and received file from a remote host
Simple mail Transfer protocol	SMTP	Used to only send Email over a network
Hyper text transfer protocol	HTTP	Used for Internet to send document that encoded in HTML
Post Office Protocol 3	POP3	the whole mailbox will be cleared (transferred) from server to local computer; view mail only once
Multipurpose Internet Mail Extensions	MIME	allows non-ASCII data to be sent using the existing mail programs and protocols it transforms non-ASCII data at the sender site to ASCII and back to non-ASCII at the receiving site
Internet Mail Access Protocol	IMAP	IMAP is similar to POP3 but with the following additional features a user can: check the email header prior to downloading, search the contents of the email for a specific string, partially download, email; allows you to download emails from your email server onto multiple devices. It keeps your messages on the email server.
Multimedia		the combination of text, graphics, images, video and audio used together; at least one must be continuous (time-dependent like audio, video, animation)
Webmail		some websites provide email service to anyone examples are Yahoo and Hotmail
World Wide Web	WWW	**a repository of information spread all over the world and linked together; strings of text within a page that link to other documents are called hyperlinks**

Summary of OSI Layers




Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
Router MAC
MAC
2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, Rj45, V.34, 100BASE-TX, SDH, DSL, 802.11