Data Communication
Chapter 4
Overview of Data Communication and Networking

Himal Acharya

Course Instructor

Outline

1. A)Network Types
   B) Topology
2. A) OSI layers and functions
   B) TCP/IP layer
   C) LAN Architecture
   D) LLC/MAC & Routing
3. A) IEEE Standards
   B) Ethernet (CSMA/CD)
   C) WAN: X.25, Frame Relay, ATM

Networks

- A network is a set of devices (often referred to as nodes) connected by communication links.
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fibre, or any medium which can transport a signal carrying information.

Topics discussed in this section:

- Network Criteria (Discussed in Chapter 1)
- Physical Structures
- Categories of Networks

Physical Structures

- Types of Connection (Already discussed in Chapter 2)
  - ❑ Point to Point
  - ❑ Multipoint

- Physical Topology

➢ The term physical topology refers to the way in which a network is laid out physically.

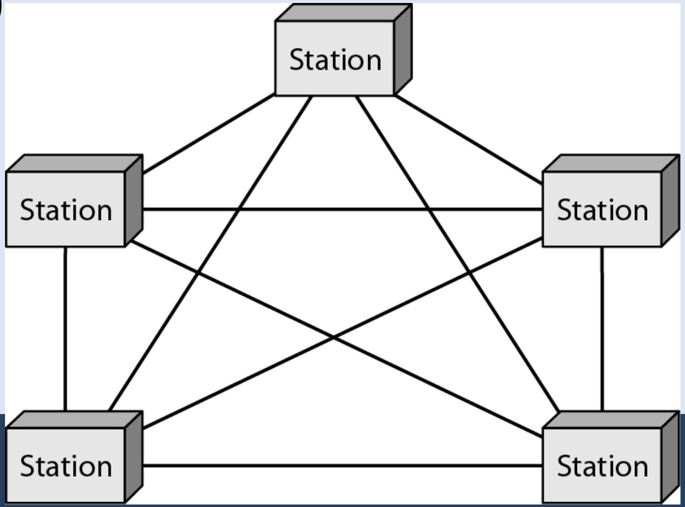
➢ Two or more devices connect to a link: two or more links form a topology.

➢ The topology of a network is the geometric representation of the relationship of all the links and linking devices (nodes) to one another. There are four basic topologies possible: Mesh, Star , Bus and Ring

Mesh Topology

- Every device has a dedicated point-to-point link to every other device
- The term dedicated means that the link carries traffic only between the devices it connects.
- To find the number of physical links in a fully connected mesh network with *n* nodes, at first each node should be connected to every other node. E.g Node 1 must be connected to n-1 nodes, similarly node 2 to remaining n-1 nodes.
- Needs n(n-1) physical link
- Every device on the network must have n-1 input/output (I/O) ports to be connected in other stations.

A fully connected mesh topology (five devices)



Mesh Topology

Advantages

- Use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- Robust – If one link becomes unusable, it does not incapacitate the entire system.
- Privacy or security – When every message travels along a dedicated line, only the intended recipient sees it.
- Point to point links make fault identification and fault isolation easy.

Disadvantages

- Amount of cabling and the number of I/O ports required.
- The sheer bulk of the wiring can be greater than the available space (in walls, ceilings or floors) can accommodate.
- Hardware required to connect each link (I/O ports and cable) can be prohibitely expensive.

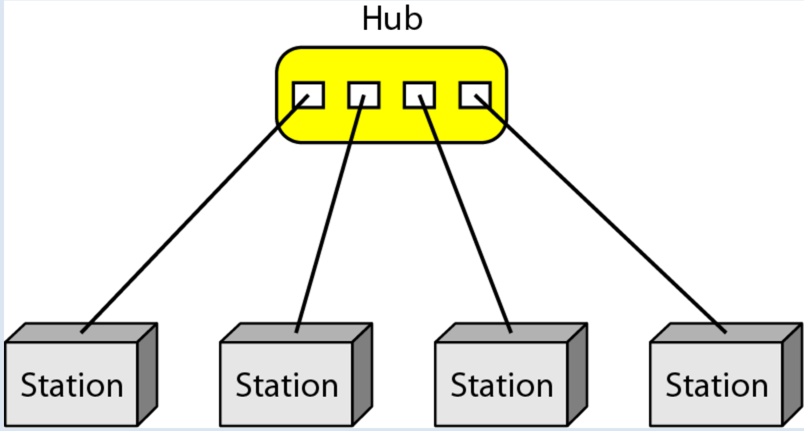
Practical example

- Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

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

A star topology connecting four stations



Star Topology

Advantages

- Less expensive than a mesh topology – In star, each device needs only one link and one I/O port to connect it to any number of others. So, easy to install and reconfigure.
- Robustness – If one links, only link is affected. All other links remain active. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages

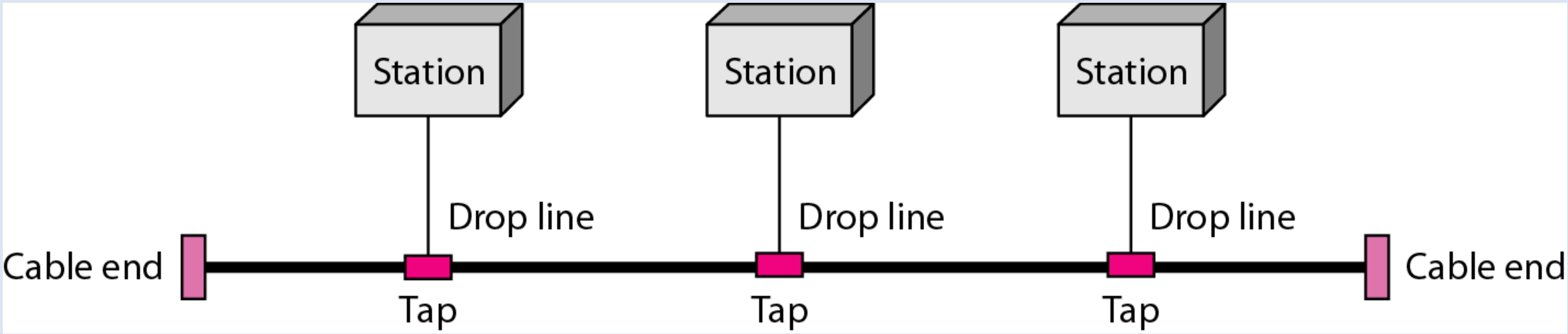
- Dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Application

High-speed LANs often use a star topology with a central hub.

Bus Topology

- Multipoint – One long cable acts as backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps
  - ❑ Drop line is a connection running between the device and the main cable
  - ❑ Tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transmitted into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



Bus Topology

Advantages

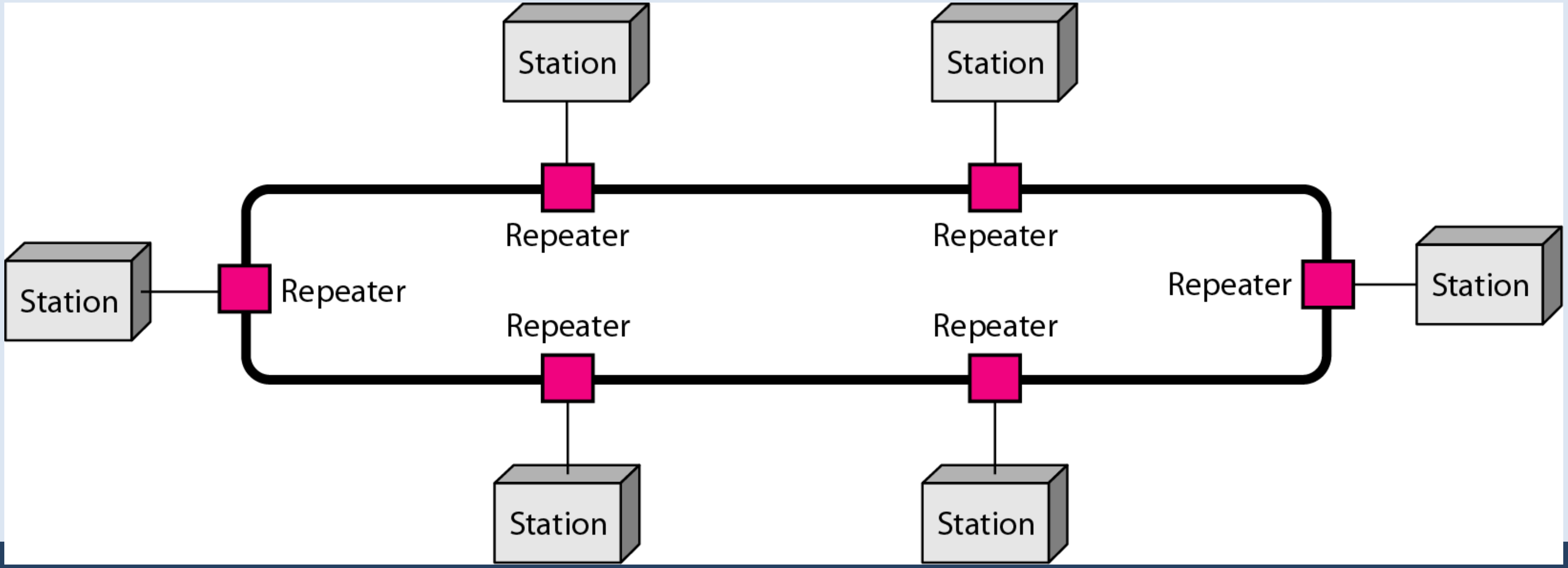
- Ease of installation – Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
- Uses less cabling than mesh or star topologies.
- Easy to expand by using repeaters to boost the signal and increase the distance

Disadvantages

- Difficult reconnection and fault isolation. Difficult to add new devices
- Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new device may therefore require modification or replacement of the backbone,
- A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring Topology

- Each device has a dedicated point-to-point connection with only the two devices on either side of it. Each device in the ring incorporates and regenerates the bits and passes them along
- Data are transmitted in frames
- A signal (frame) is passed along the ring in one direction, past all the other stations, the destination recognizes its address and copies the frame
- Frame continues to circulate; removed when it returns to the source station.



Ring Topology

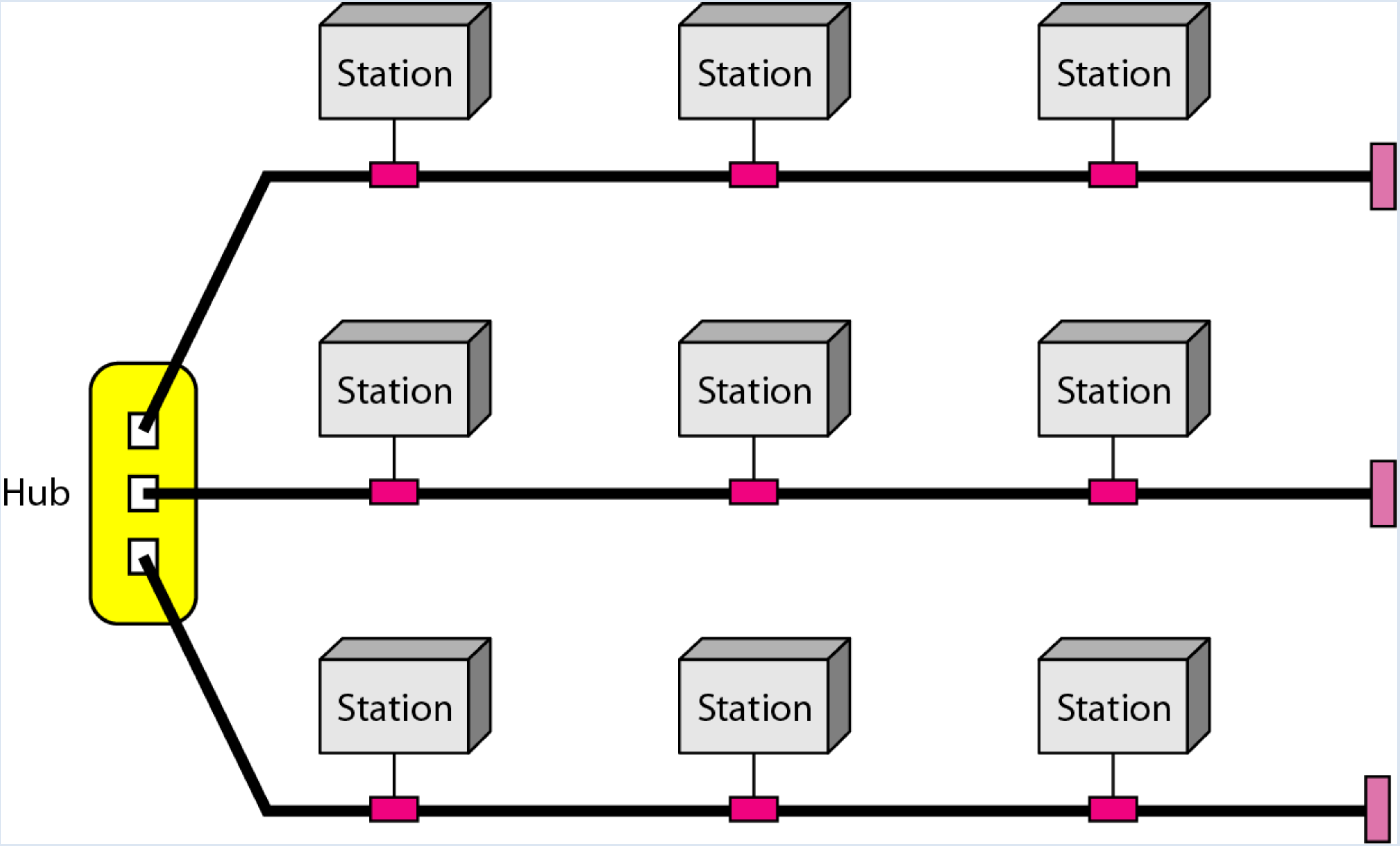
Advantages

- Easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections.
- Fault isolation is simplified. Generally, in a ring a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages

- Unidirectional traffic
- In a simple ring, a break in the ring (such as disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the network.

Hybrid Topology



Network Classification

- Based on connection model

Connection oriented and connectionless networks

- Based on switching technology

Circuit switching and packet switching networks

- Based on geographical coverage

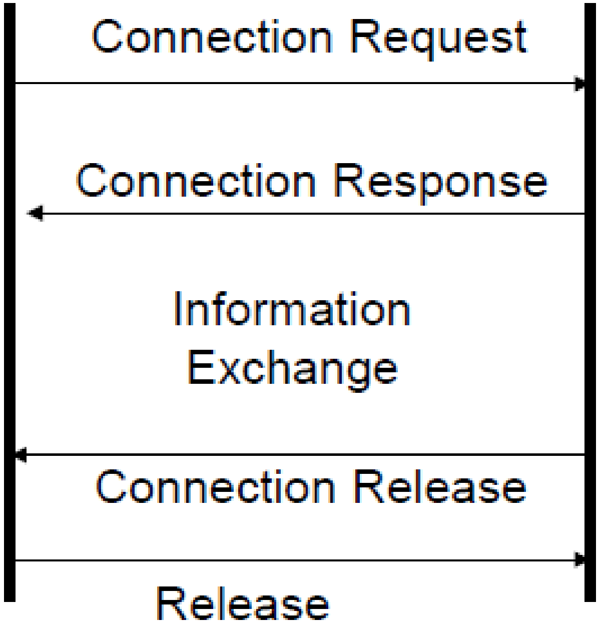
Local Area Networks (LAN) , Metropolitan Area Networks (MAN) and Wide Area Networks (WAN)

- Based on ownership model

Enterprise Networks and Carrier Networks

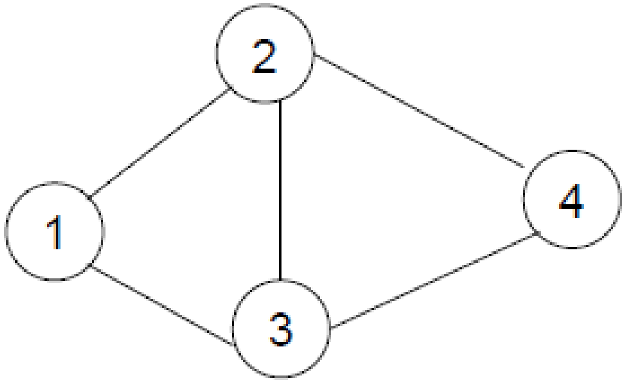
Connection-Oriented (CO) Networks

- In Connection-Oriented (CO) networks a **connection is established** between the source and the destination **before the exchange** of the information
  - Requires **signaling** for the connection establishment with the desired attributes
  - A prominent example is PSTN using signaling system 7 (SS7) for connection establishment

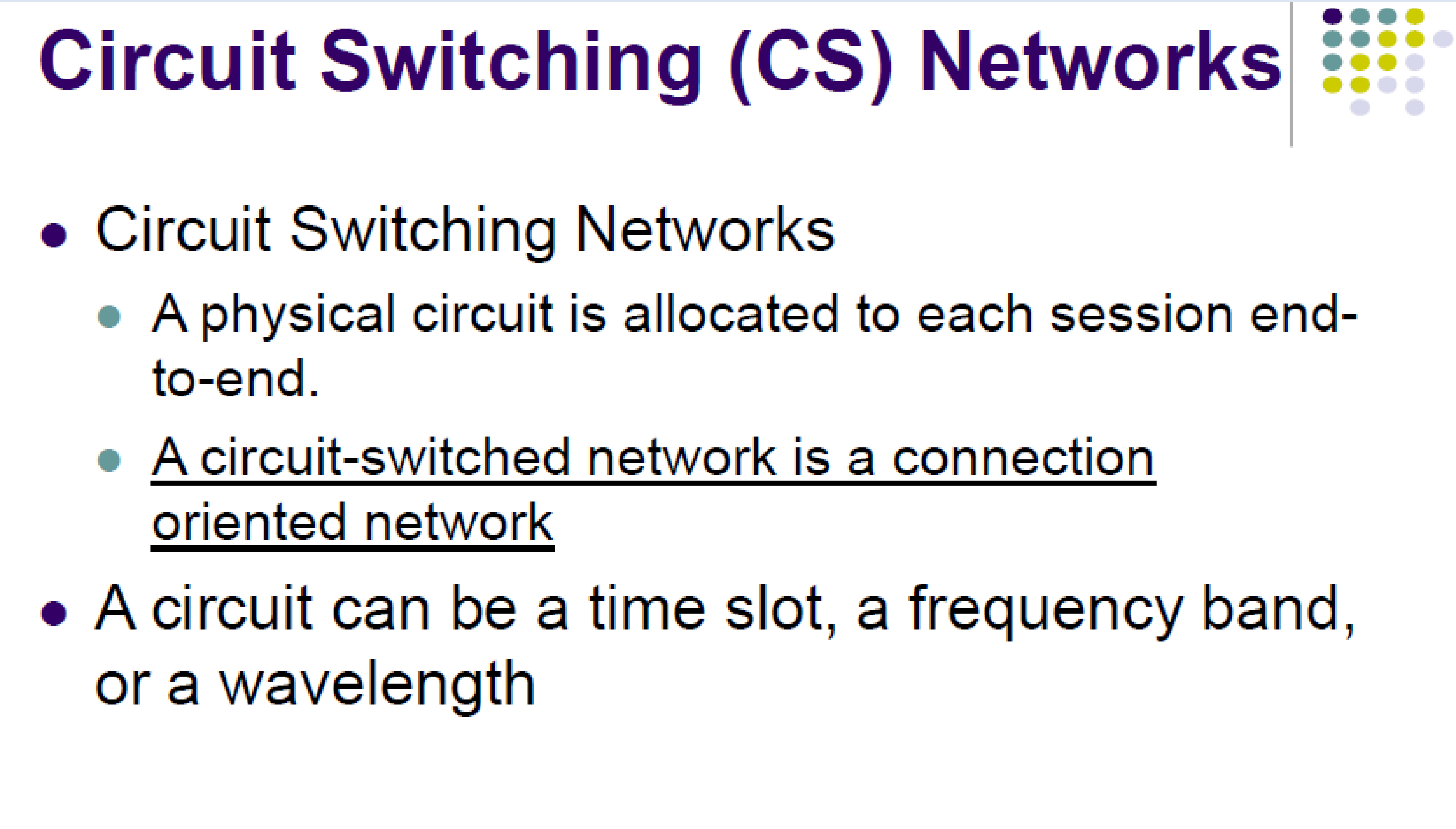


Connectionless (CLS) Networks

- Each unit of transmission includes a source and a destination information
  - This information is used to route the packet from source to destination
  - No explicit signaling is needed. However control information is needed to establish routing tables (routing protocols)
  - Classic example is IP network.

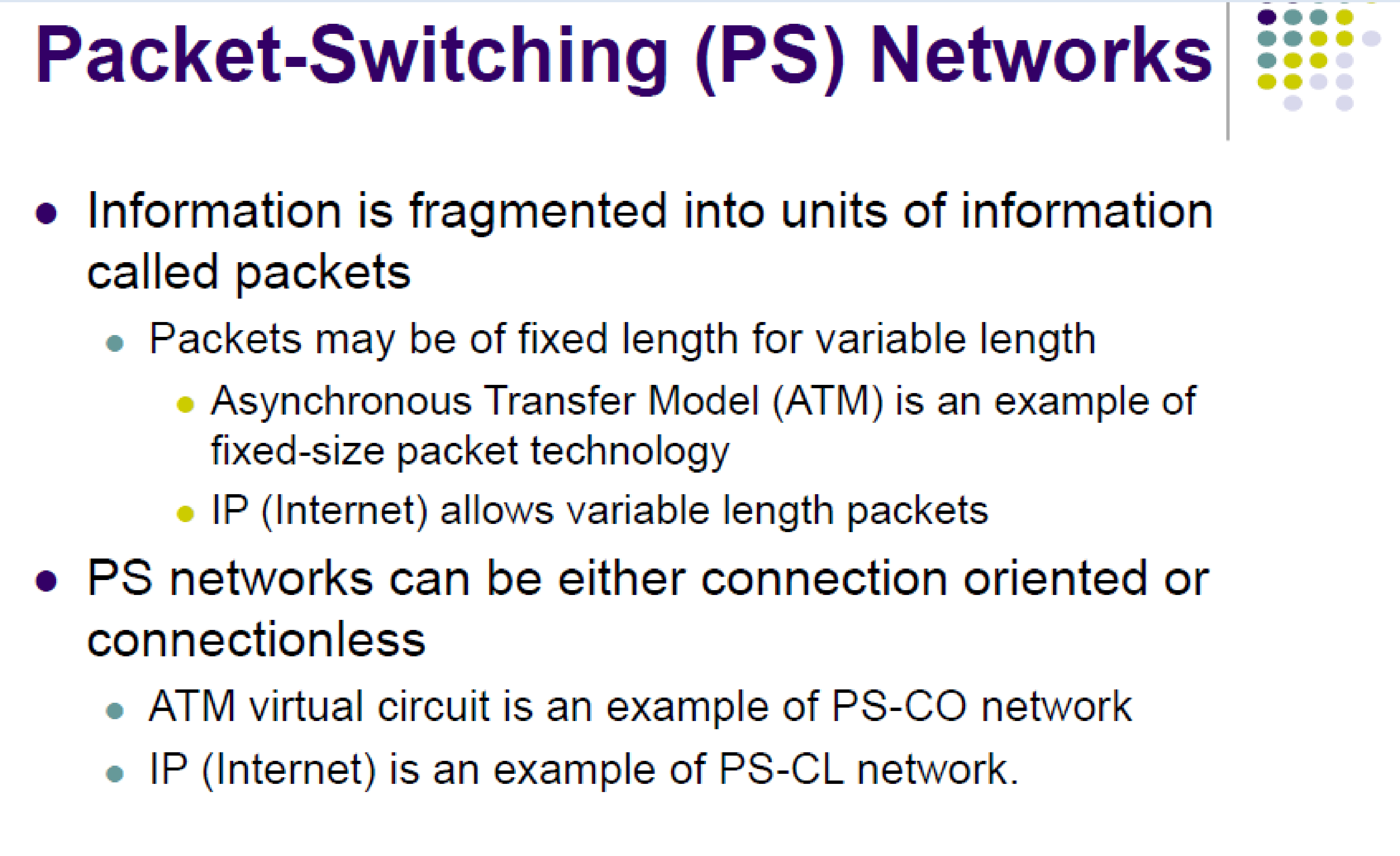


Dest	Next Hop



Circuit Switching (CS) Networks

- Circuit Switching Networks
  - A physical circuit is allocated to each session end-to-end.
  - A circuit-switched network is a connection oriented network
- A circuit can be a time slot, a frequency band, or a wavelength

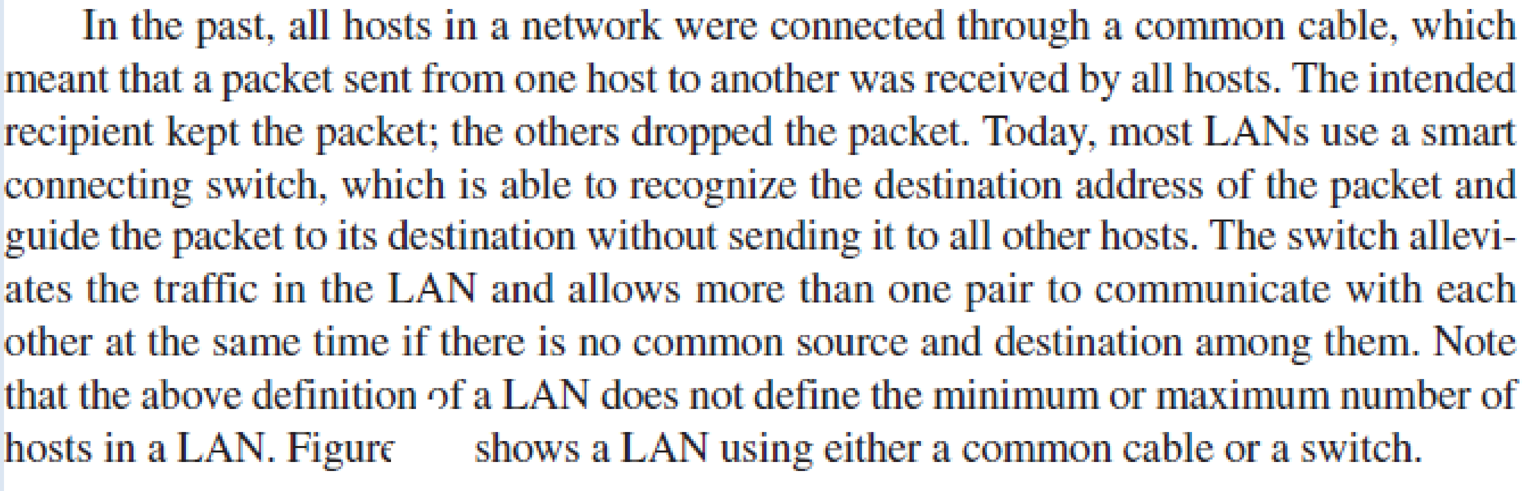


Packet-Switching (PS) Networks

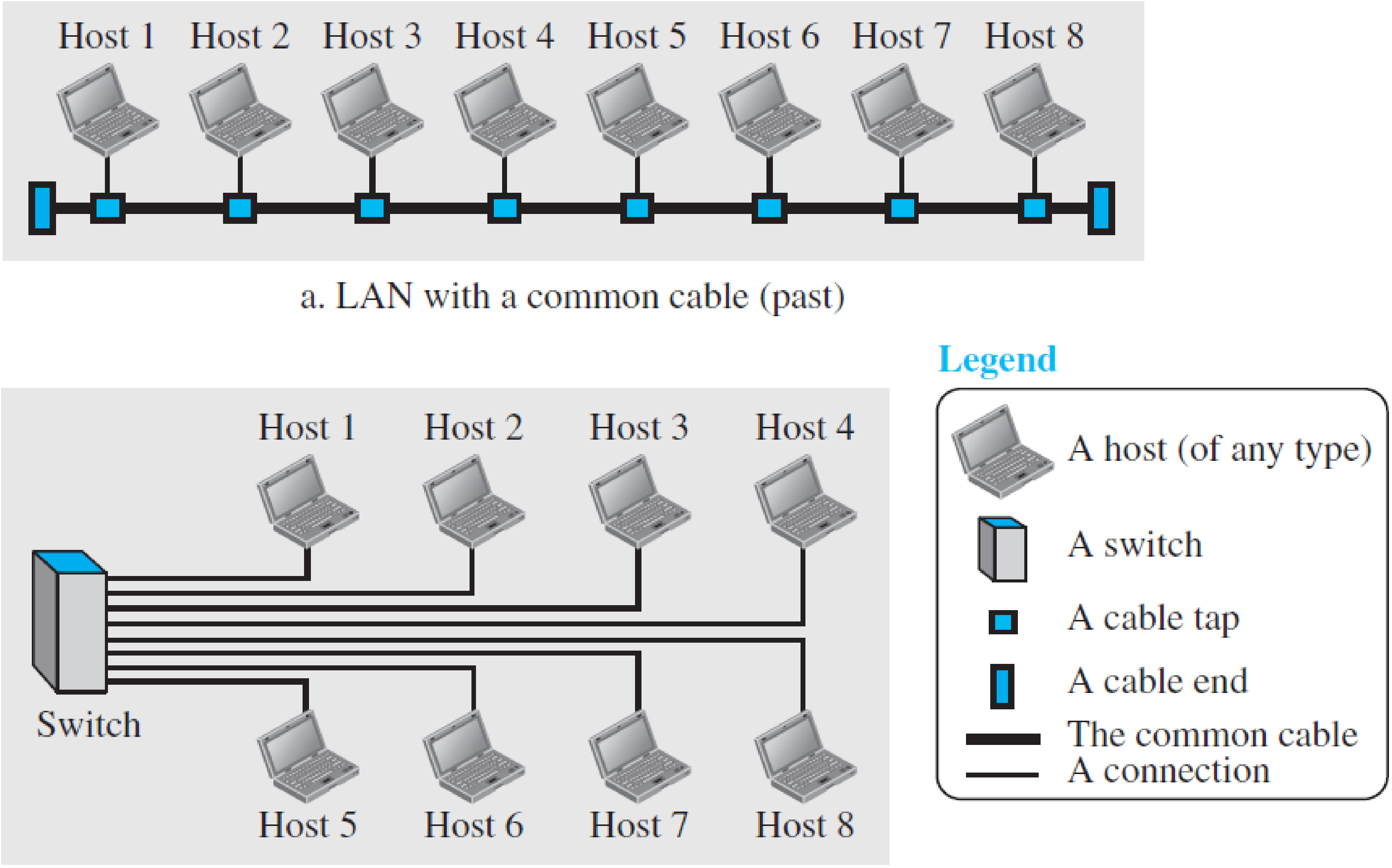
- Information is fragmented into units of information called packets
  - Packets may be of fixed length for variable length
    - Asynchronous Transfer Model (ATM) is an example of fixed-size packet technology
    - IP (Internet) allows variable length packets
- PS networks can be either connection oriented or connectionless
  - ATM virtual circuit is an example of PS-CO network
  - IP (Internet) is an example of PS-CL network.

Local Area Networks (LAN)

- Covers a geographical diameter in the order of 10 meters (within a building or a department)
- Usually employs a bus or a ring topology
  - ❖ Ethernet (IEEE 802.2) is an example of a bus topology
  - ❖ Token Ring (IEEE 802.5) is an example of ring topology
- Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host’s and the destination host’s address.



In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet. Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts. The switch alleviates the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them. Note that the above definition of a LAN does not define the minimum or maximum number of hosts in a LAN. Figure shows a LAN using either a common cable or a switch.

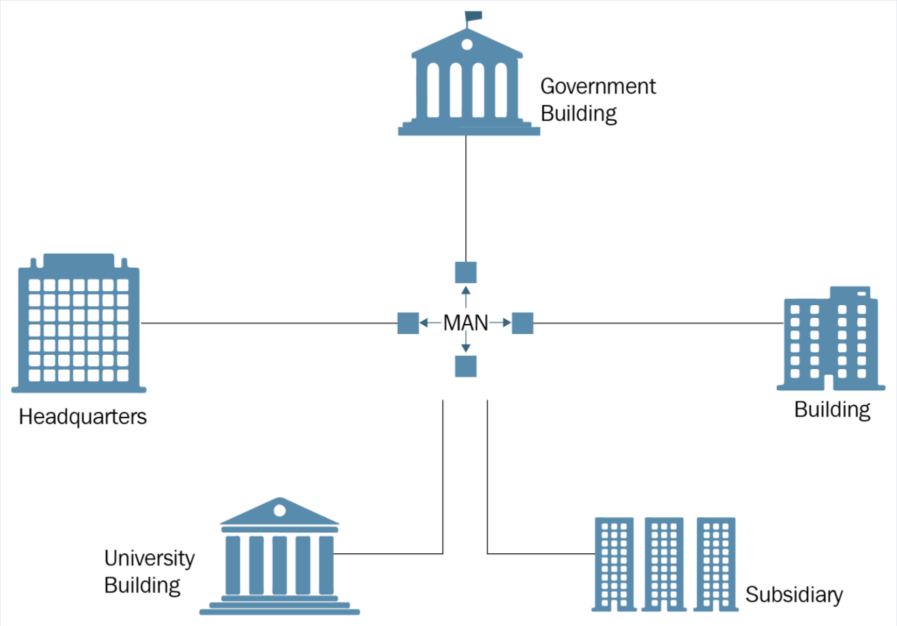


a. LAN with a common cable (past)

b. LAN with a switch (today)

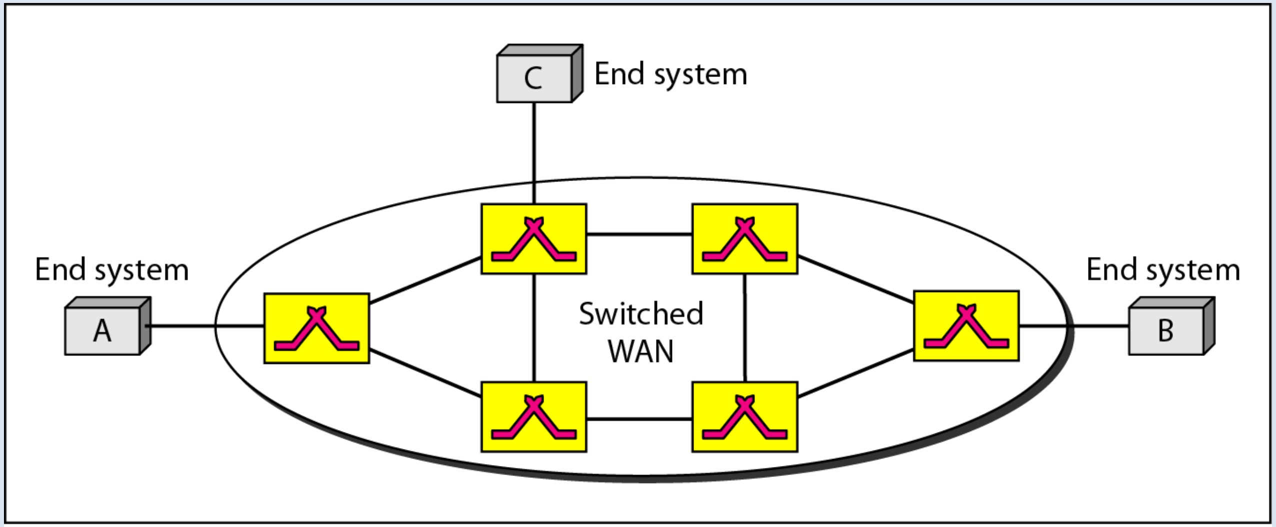
Metropolitan Area Networks (MAN)

- Covers a geographical distance of about 50 km (spans a single city)
- May have a ring, a bus or a mesh topology
- Made up of interconnected multiple LANs using fibre optic cables
- Owned and operated by ISP or a public company such as a local telephone company

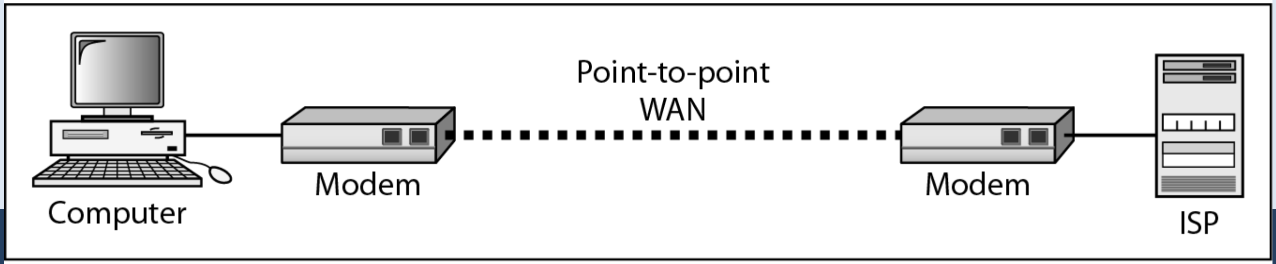


Wide Area Network (WAN)

- Covers a wider geographical areas between cities
- Normally created and run by communication companies and leased by an organization that uses it.



a. Switched WAN

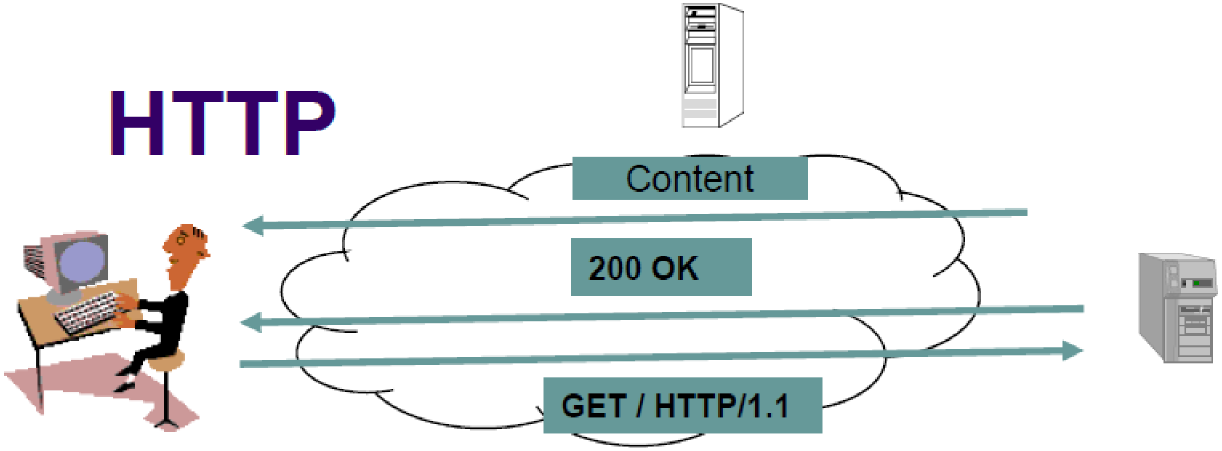


b. Point-to-point WAN

Network Architecture: Layers, Services and Protocols

- The overall communications process between two or more communicating nodes connected across or more networks can become ***very complex***
- **Layering** partitions related communications functions into groups that are manageable
- Each layer provides a service to the layer above
- Each layer operates according to a protocol

HTTP



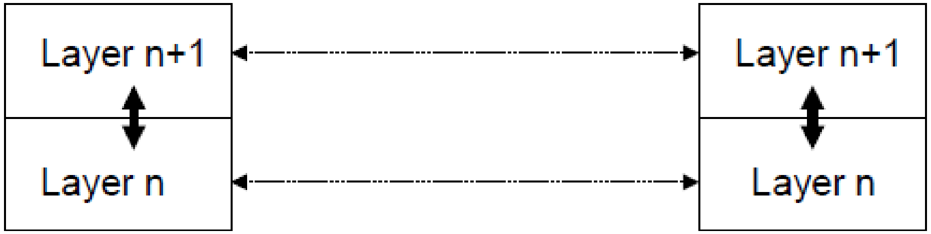
- HTTP client sends its request message: “GET …”
- HTTP server sends a status response: “200 OK”
- HTTP server sends requested file
- Browser displays document
- Clicking a link sets off a chain of events across the Internet!
- Let’s see how protocols & layers come into play…

Protocols

- A *protocol* is a set of rules that governs how two or more communicating entities *in a given layer* are to interact
- Specifies *messages* that can be sent and received
- *Actions* that are to be taken when a certain event occurs, e.g. sending or receiving messages, expiry of timers
- **The purpose of a protocol at a *layer n* is to provide a service to the *layer n+1* above**

Layered Architecture

- A ***Layer*** defines a set of related communication functions that can be managed and grouped together
- Devices communicate at the same layer with the help of ***Protocols***.
- Layer n+1(upper) acts a *client* to layer n(lower). Layer n is the *server* to layer n+1.



Why Layering?

- Layering simplifies design, implementation, and testing by partitioning overall communications process into parts

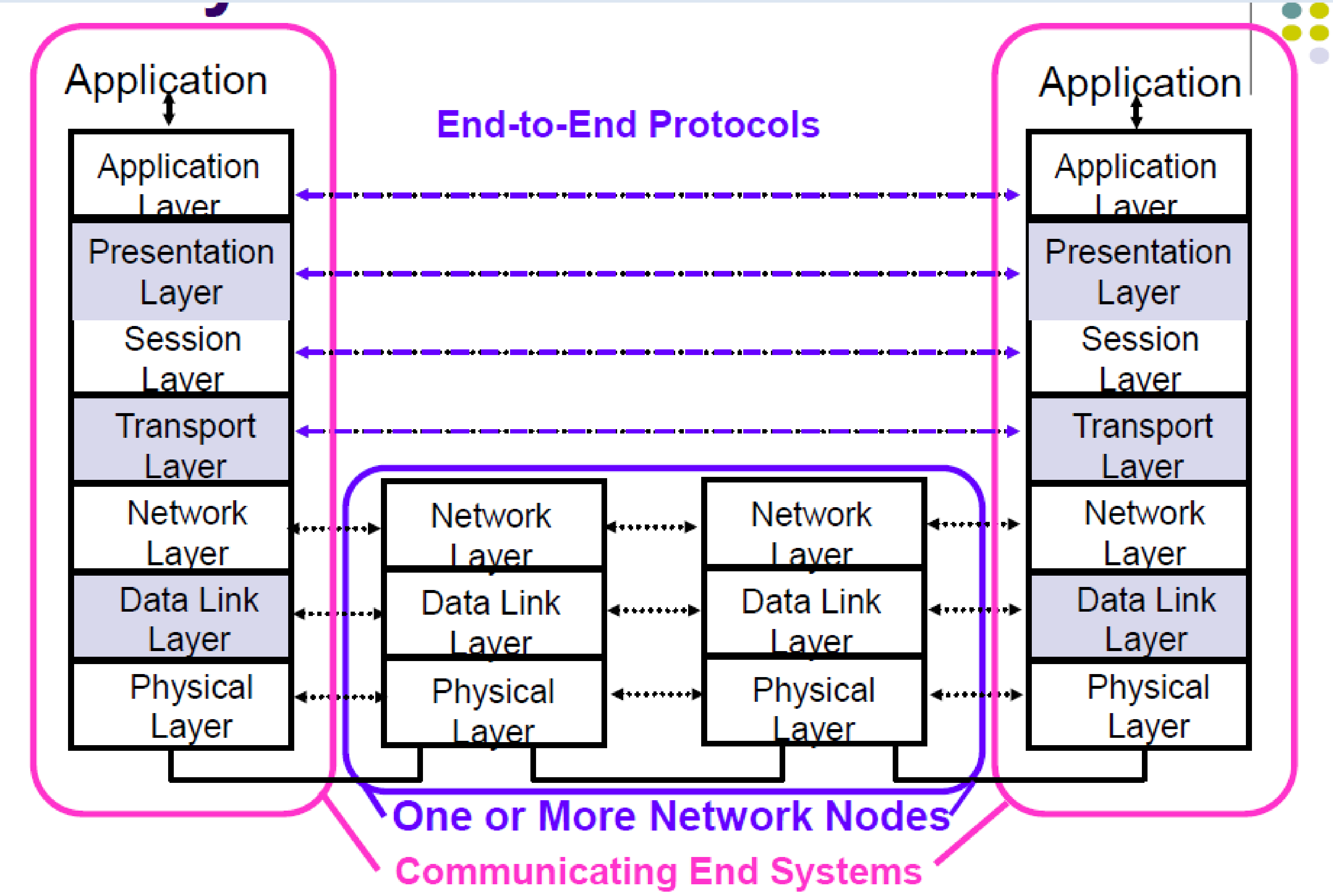
- Protocol in each layer can be designed separately from those in other layers. Protocol makes “calls” for services from layer below

- Layering provides flexibility for modifying and evolving protocols and services without having to change layers below

Open System Interconnection (OSI) Reference Model

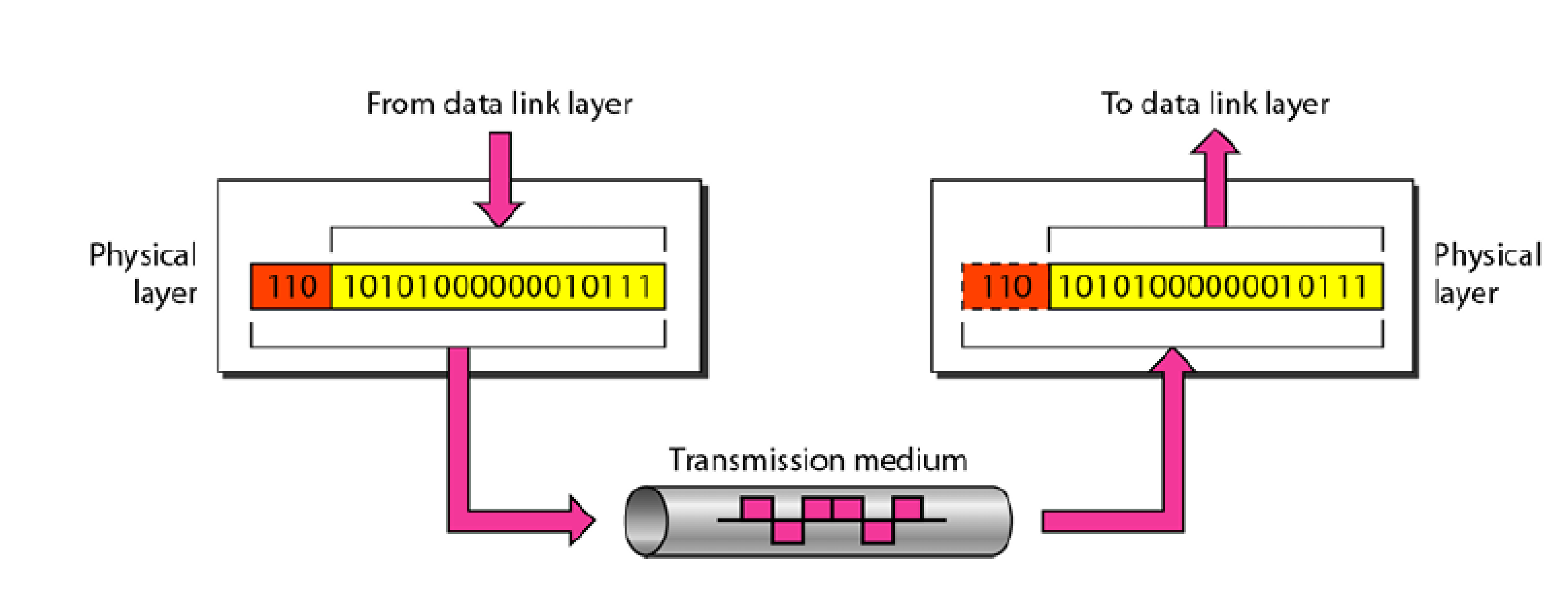
- Describes a seven-layer abstract reference model for a network architecture
- Purpose of the reference model was to provide a framework for the development of protocols
- OSI also provided a unified view of layers, protocols, and services which is still in use in the development of new protocols
- Detailed standards were developed for each layer, but today many of these are not in use
- TCP/IP protocols preempted deployment of OSI protocols

7-layer OSI reference model



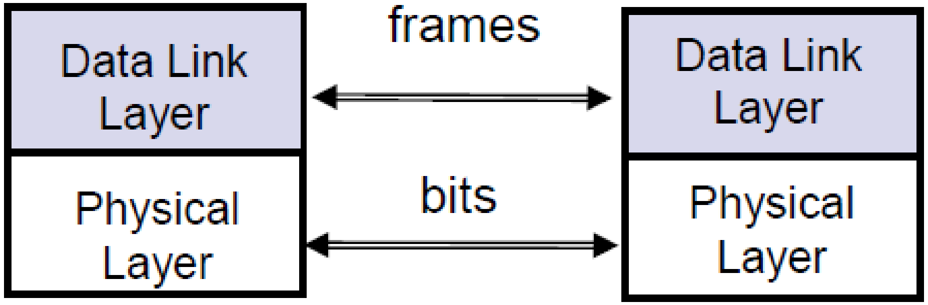
Physical Layer

- Transfers bits across a link.
- Deals with the mechanical and electrical specifications of the interface and transmission media.
- Decide whether the transmission is simplex, half-duplex and full duplex



Data Link Layer

- Transfers *frames* across *direct* connections (point to point)
  - Groups bits into frame
- Detection of bit errors; **Retransmission** of frames
- Activation, maintenance, & deactivation of data link connections
- **Medium access control (MAC)** for local area networks
- **Flow control**



Data Link Layer

- Used for LAN (shared media): Ethernet or token ring
- WAN (point-to-point): ATM, Frame Relay
- **Functionalities**: sequencing, reliability, framing, timing, pacing, flow control, multiplexing, security

- Physical layer is typically in hardware. Data link layer could be a HW – SW mix or in real-time intensive SW (e.g., device driver) Example: PC NIC card and Ethernet driver

Responsibilities of the data link layer

- Framing: To identify the beginning and end of a block of information
- Error detection: Data link layer employs error detection and error correction codes
- Flow control: If the receiver's speed is lower than the sender's speed, this leads to an overflow in the receiver's buffer and some frames may get lost. Responsible for synchronization of the sender's and receiver's speeds and establishing flow control between them
- Access control: When multiple devices share the same communication channel: high probability of collision. -> Responsible to check which device has control over the channel

Sub layers of Data Link Layer

1. Logical Link Control Sublayer LLC

Based on ARQ (Automatic Repeat Request)

WHY?

- Different speed capability between seder and receiver
- Handling transmission errors (at layer 2) by retransmission

Responsible for logical addressing between source and destination

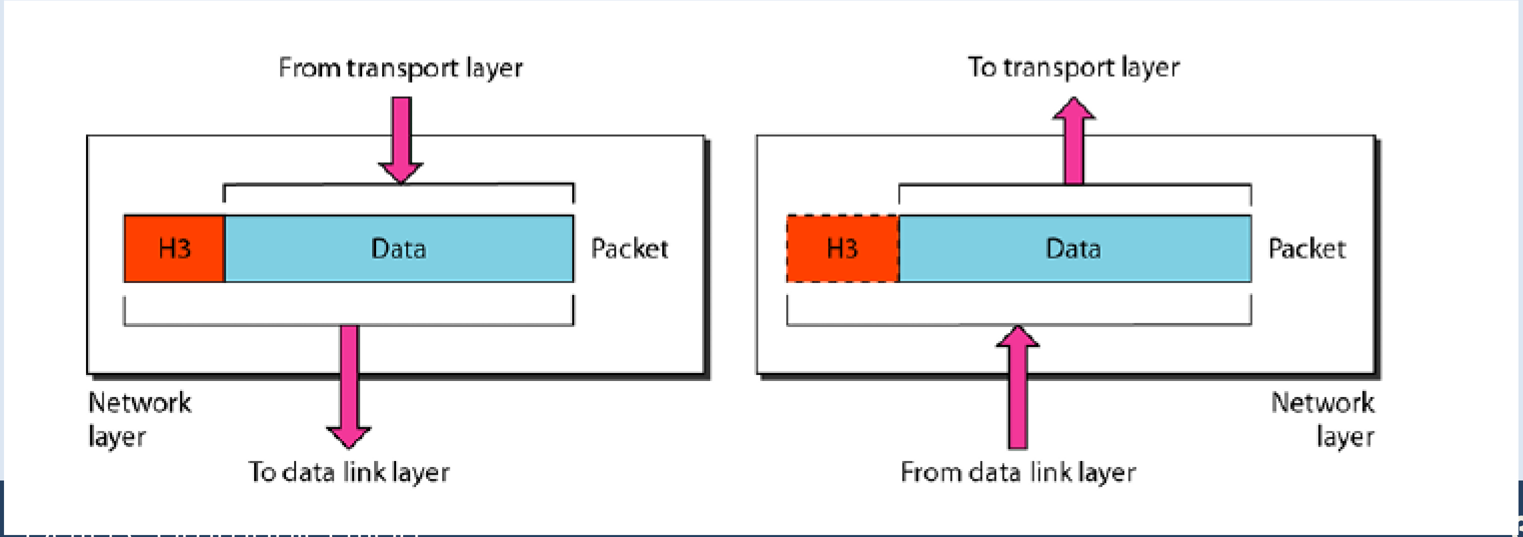
2. Medium Access Control MAC

Protocol to regulate access to the shared media

Access Control: CSMA/CD used to detect collision in a channel

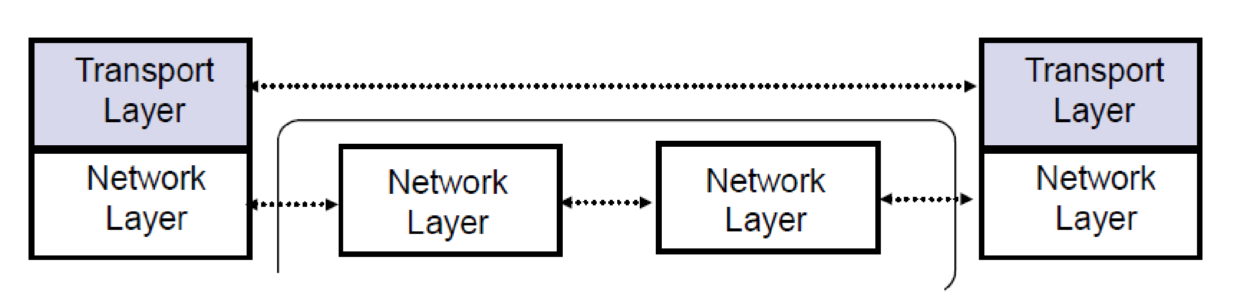
Network layer

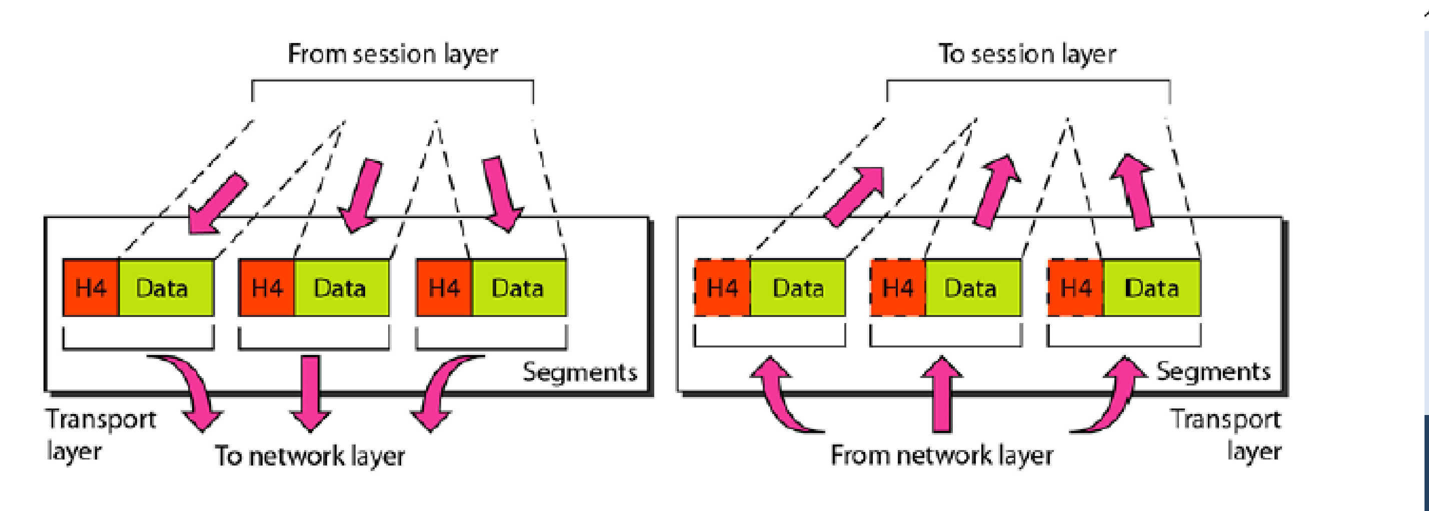
- Responsible for the source to destination delivery of a packet.
- The n/w layer ensures that each packet gets from its point of origin to its final destination
- Nodes jointly execute routing algorithm to determine paths across the network
- Congestion control to deal with traffic surges
- Connection setup, maintenance and teardown when connection-based



Transport Layer

- Transfers data end-to-end (or host-to-host/server) from a process in a machine to a process in another machine
- Reliable stream transfer or quick-and-simple single-block transfer
- Port numbers enable multiplexing
- Message segmentation and reassembly
- Session setup, maintenance and release



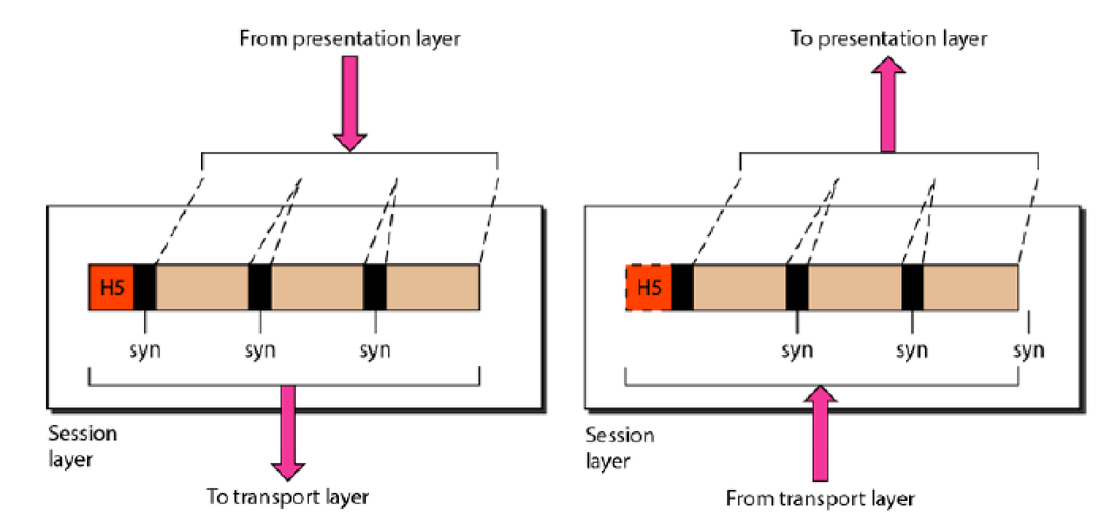


Duties of Transport Layer

- Port Addressing- The transport layer adds port address to the data. So that the message gets to the correct process on the receiving computer
- Segmentation and Reassembly: This layer divides the message into transmittable segments, each segment containing a sequence number which helps to reassemble the segments on the receiver
- Connection control: The transport layer can be either connectionless or connection oriented. In connectionless, each packet is transmitted independently. In connection oriented, first the connection is established, data is transmitted and the connection is terminated.

Session layer

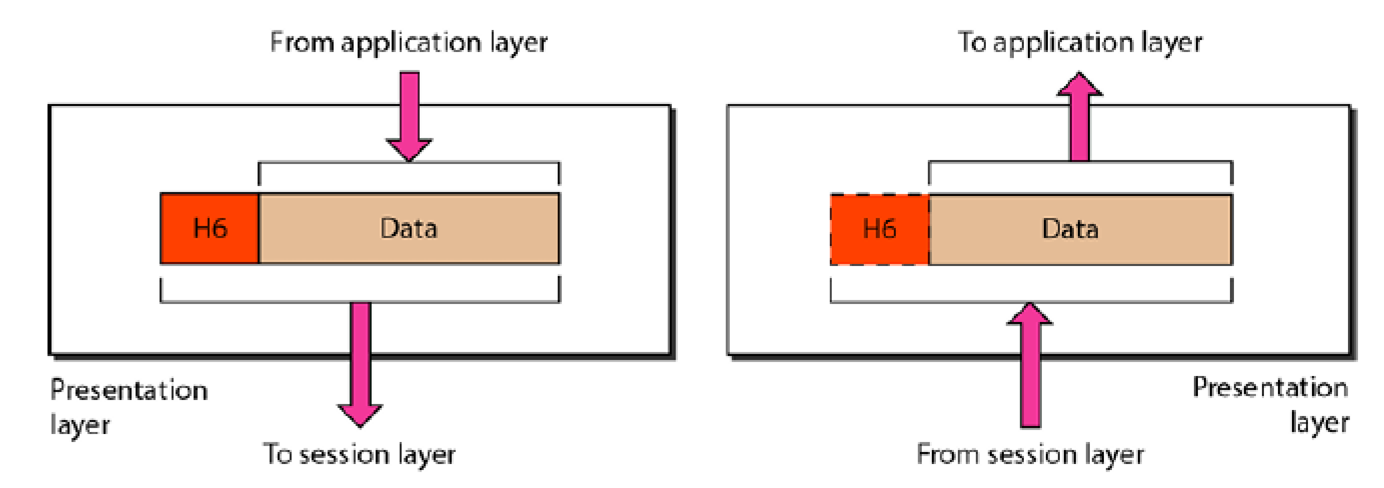
- Allows users of different machine to establish a session between them



- Session layer allows a process to add checkpoints into stream of data. The checkpoints are inserted inside the data and checked for error. The process is error free when checkpoints are detected. In case of crash happens during the transmission, the data can be retransmitted from the checkpoint instead of retransmitting from the start.

Presentation Layer

- Concerned with the syntax and semantics of information transmitted
- Defines how two devices should encode, encrypt and compress data so it is received correctly on the other end



Duties of the presentation layer

- Translation: The presentation layer at the sender changes the information from its sender dependent format into a common format. The presentation layer at the receiving machines change the common format into its receiver dependent format.
- Encryption: The presentation layer encrypts the data at the sender and decrypts them at the receiver
- Compression: This layer compresses the data to reduce the number of bits to be transmitted

Application layer

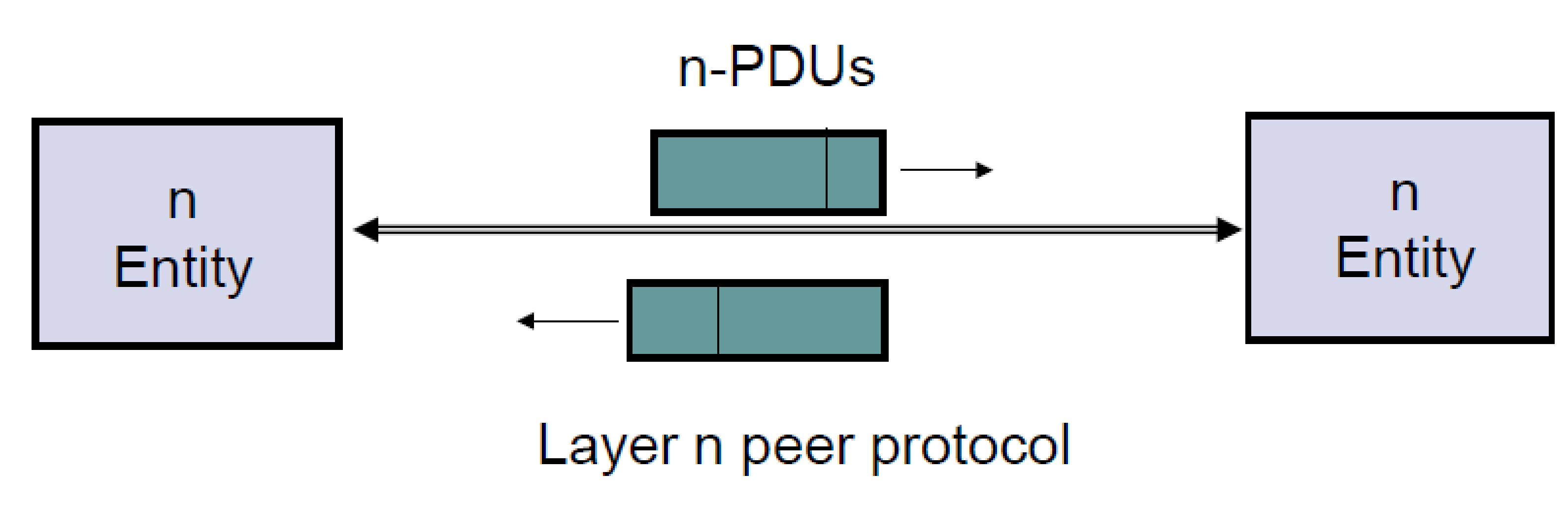
- Contains variety of protocols that are needed by users. E.g. Hyper text transfer protocol (HTTP), File Transfer Protocol (FTP), etc

OSI Unified View: Protocols

- Layer n in one machine interacts with layer n in another machine to provide a service to layer n +1

- The entities comprising the corresponding layers on different machines are called *peer processes*.

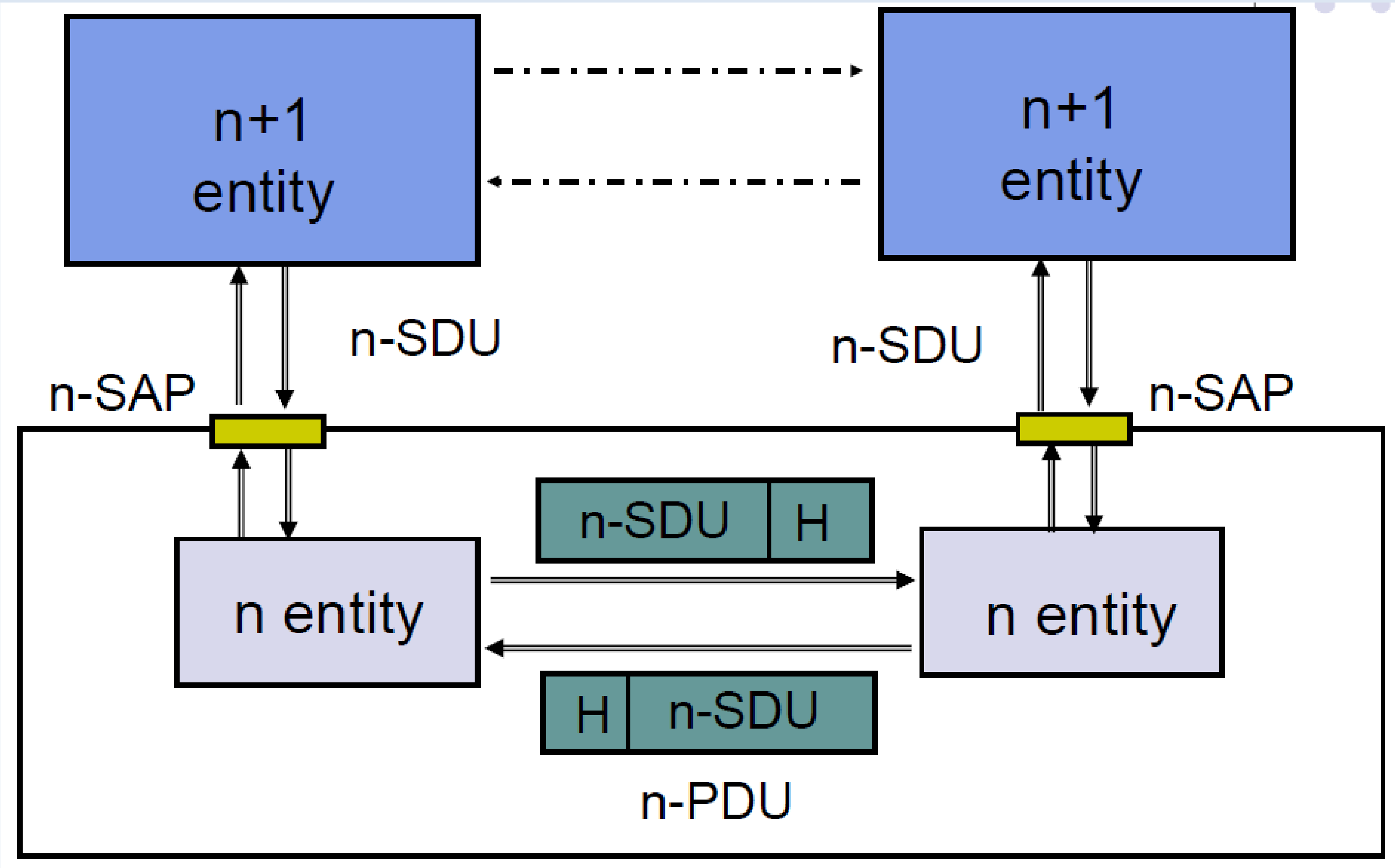
- The machines use a set of rules and conventions (the *layer-n protocol)*.
- Layer-n peer processes communicate by exchanging *Protocol Data Units* (PDUs)



OSI Unified View: Services

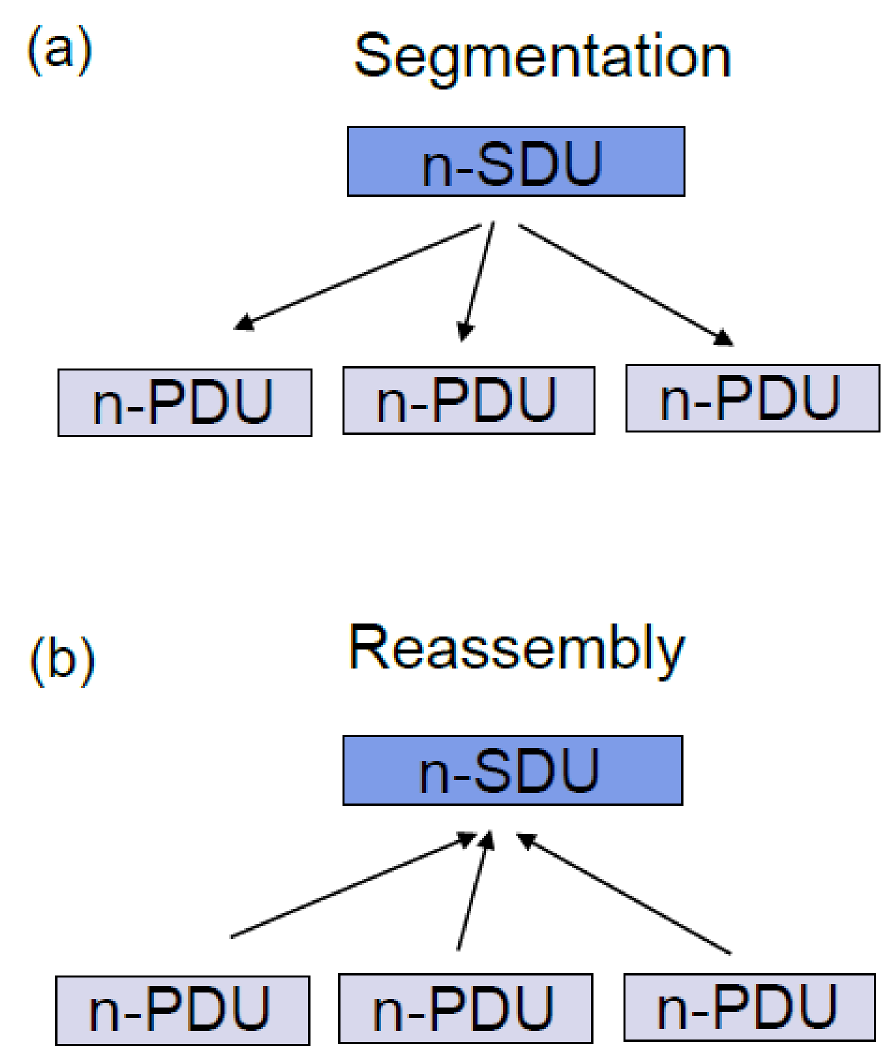
- Communication between peer processes is virtual and actually indirect
- Layer n+1 transfers information by invoking the services provided by layer n
- Services are available at *Service Access Points* (SAP's)
- Each layer passes data & control information to the layer below it until the physical layer is reached and transfer occurs
- The data passed to the layer below is called a *Service Data Unit* (SDU)
- SDU's are *encapsulated* in PDU's

Layers, Services, and Protocols



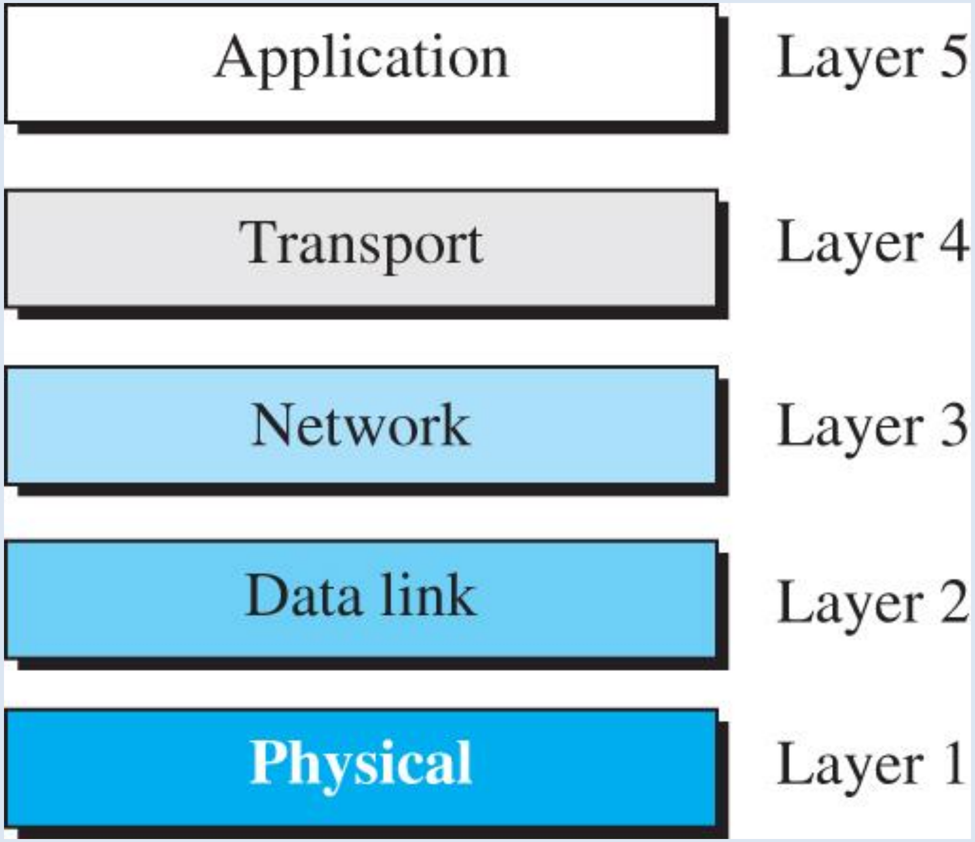
Segmentation and Reassembly

- A layer may impose a limit on the size of a data block that it can transfer for implementation or other reasons
- Thus, a layer-n SDU may be too large to be handled as a single unit by layer (n-1)
- Sender side: SDU is segmented into multiple PDUs
- Receiver side: SDU is reassembled from sequence of PDUs

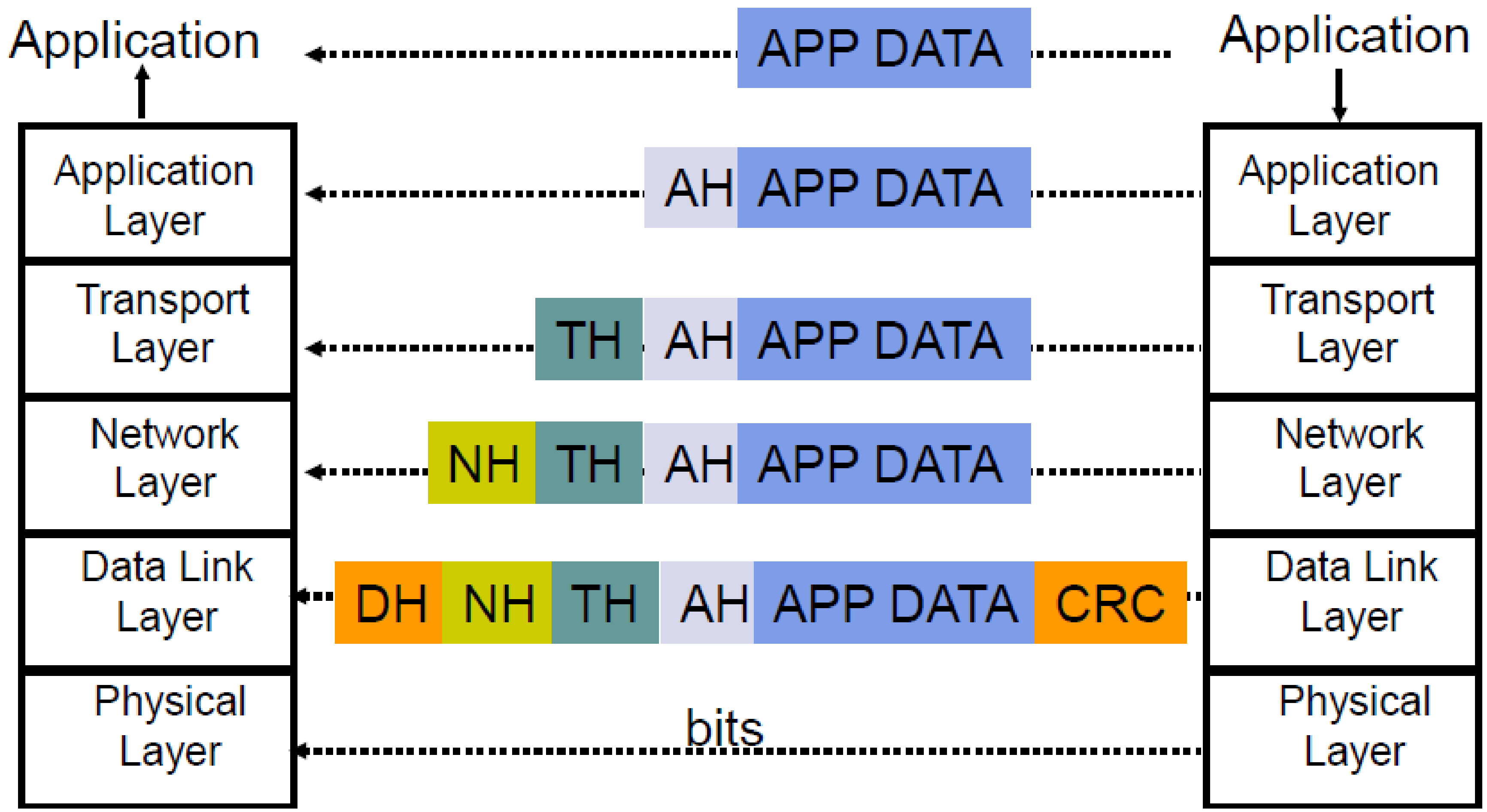


TCP/IP layers

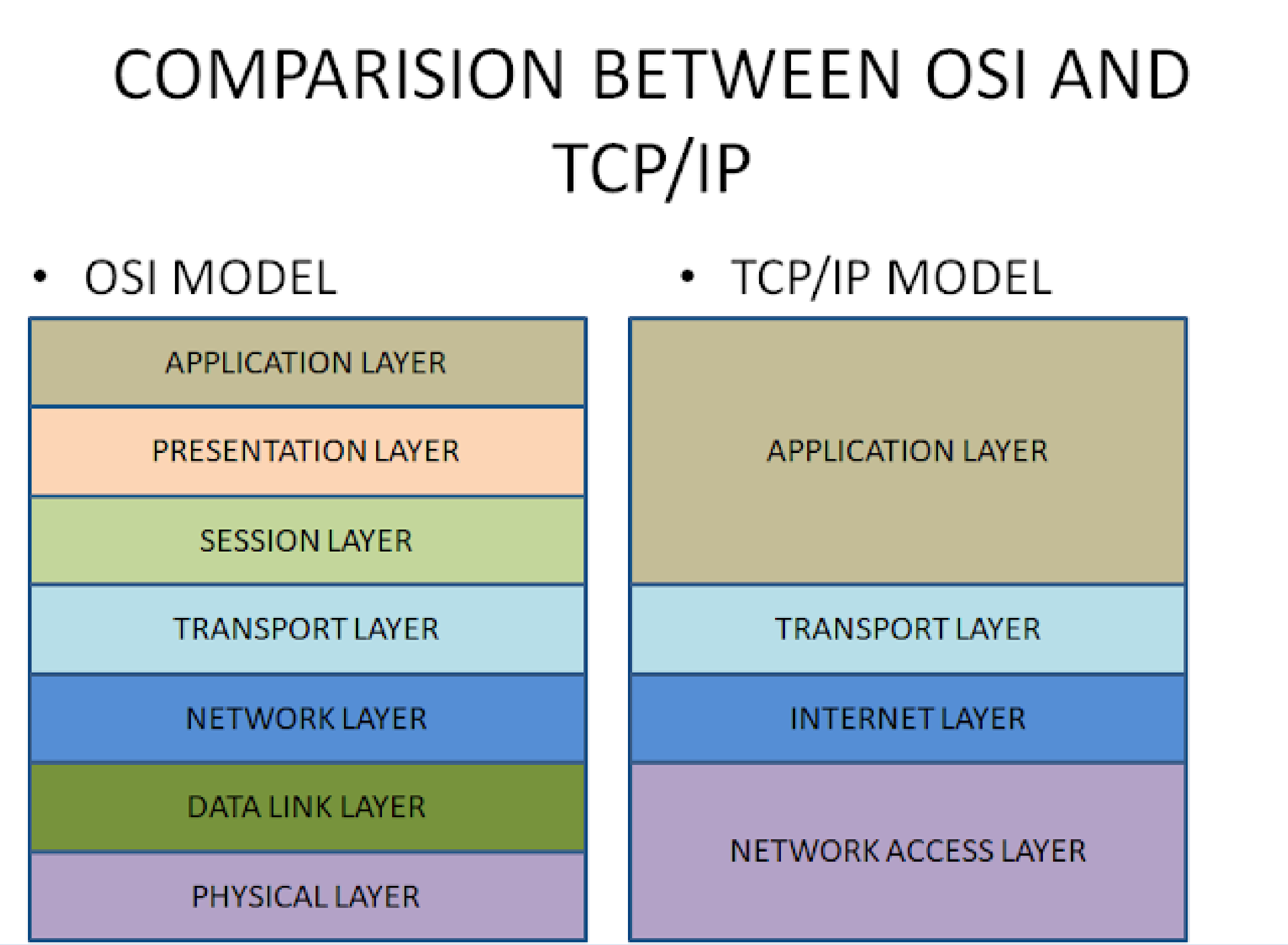
This is the protocol suite used in the Internet today.



Headers and Trailers



Comparison of TCP/IP and OSI model



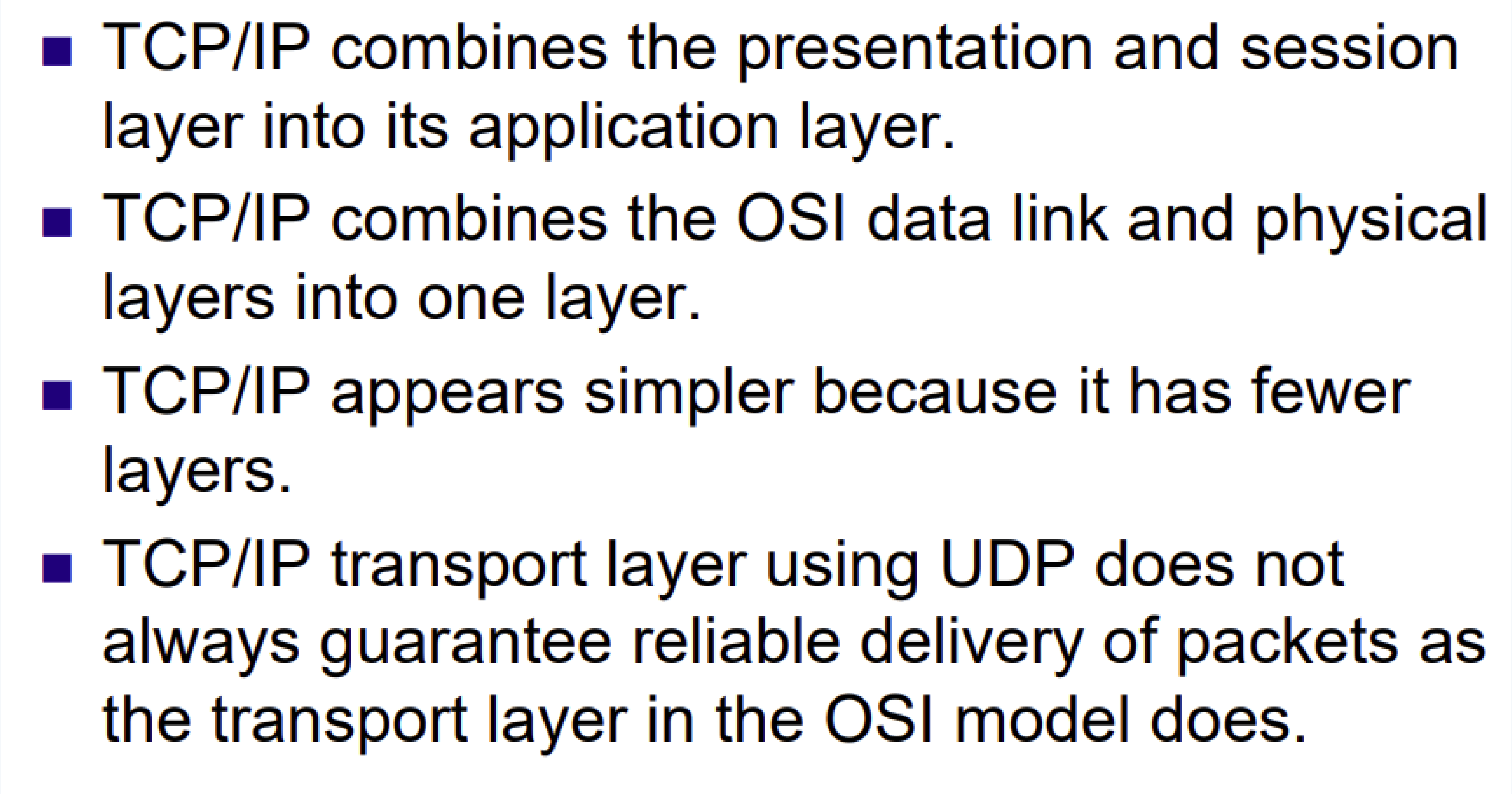
COMPARISION BETWEEN OSI AND TCP/IP

- OSI MODEL
- TCP/IP MODEL

APPLICATION LAYER
PRESENTATION LAYER
SESSION LAYER
TRANSPORT LAYER
NETWORK LAYER
DATA LINK LAYER
PHYSICAL LAYER

APPLICATION LAYER
TRANSPORT LAYER
INTERNET LAYER
NETWORK ACCESS LAYER

Comparison of TCP/IP and OSI model



- TCP/IP combines the presentation and session layer into its application layer.
- TCP/IP combines the OSI data link and physical layers into one layer.
- TCP/IP appears simpler because it has fewer layers.
- TCP/IP transport layer using UDP does not always guarantee reliable delivery of packets as the transport layer in the OSI model does.

1. Network Access Layer

- First layer of the four-layer TCP/IP model.
- It defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fibre, or twisted pair cable.
- The protocols/standards included in Network access layer are Ethernet, Token Ring, X.25, Frame Relay

2. Internet Layer

- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Protocols used in this layer: Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Control (ICMP)

3. Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network. Two protocols used in the transport layer: User Datagram Protocol and Transmission Control layer

UDP

- Best effort (unreliable) datagram service
- Connectionless: No handshaking, no connection state
- No flow control, no error control, no congestion control
- Applications: Multimedia- VoIP, video, RTP, Network Service: DNS,SNMP

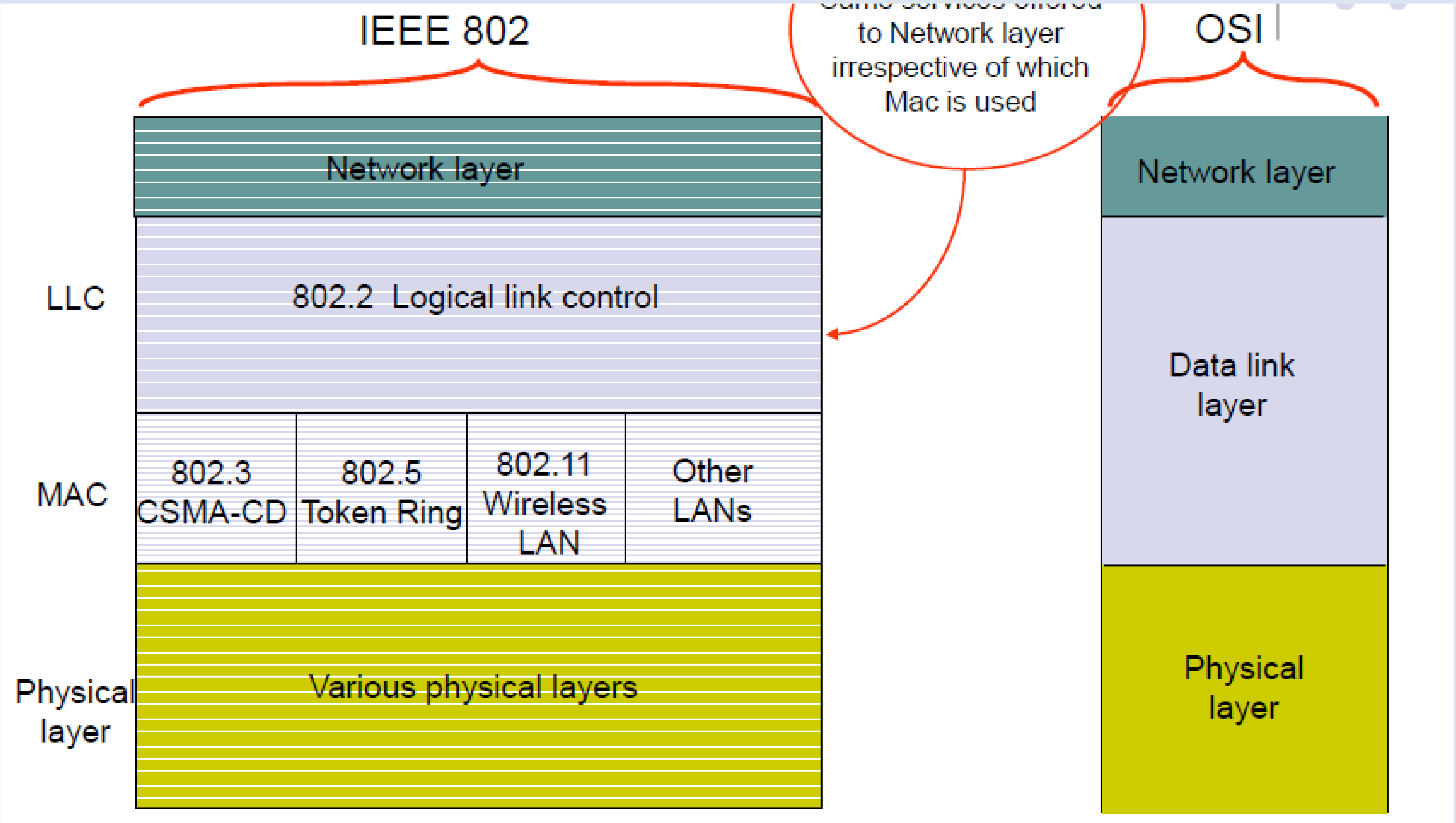
TCP

- Reliable Byte stream service
- Connection oriented: Connection setup, connection state, connection release
- Higher delay than UDP
- Error control, flow control, congestion control
- Most applications use TCP: HTTP, SMTP, TELNET, FTP,..

4. Application Layer

- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- e.g HTTP, DNS,SMTP,SNMP, TELNET, FTP

LAN Protocol Architecture



OSI vs IEEE LAN Models

Two sublayers for IEEE LAN (LLC and MAC)

- Logical Link control sublayer (LLC)

  Framing

  Flow control (Stop and wait, Sliding Window)

  Error Control

- Medium Access Control (MAC) sublayer

  Random Access (Ethernet CSMA /CD)

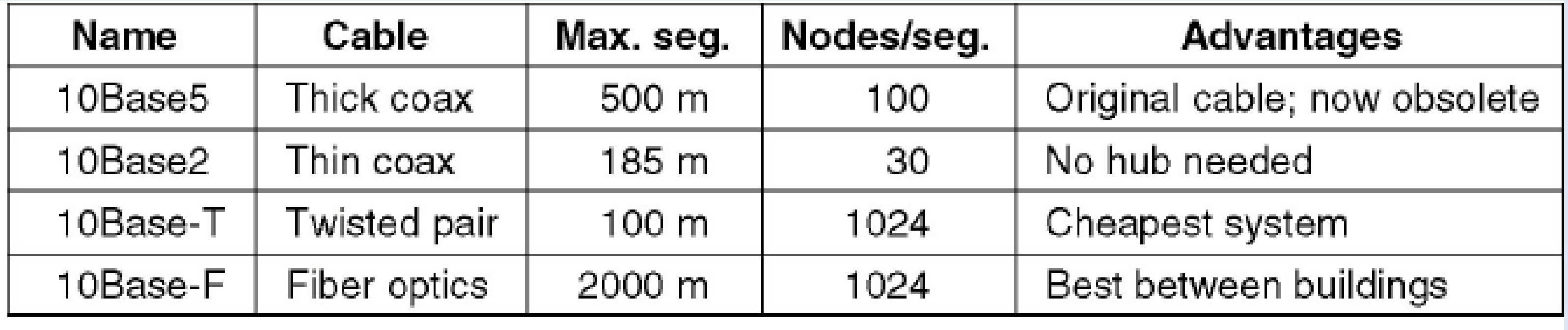
  Token Passing (Token Ring)

IEEE 802 Standards

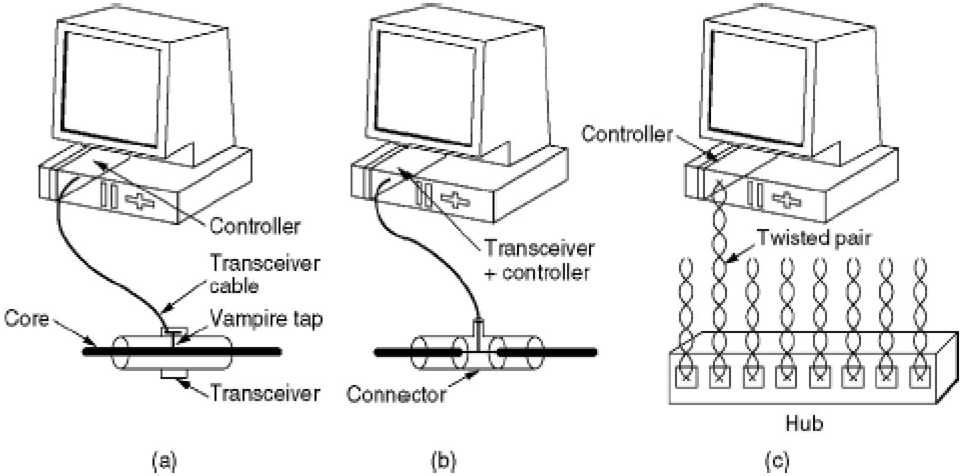
- In OSI terms, higher layer protocols (layer 3 or 4 and above) are independent of network architecture and are applicable to LANs, MANs, and WANs
- LAN protocols are concerned with lower layers of the OSI model
- IEEE LAN standard (IEEE 802 standards) consists of physical, medium access control (MAC), and logic link control (LLC) layers.

Ethernet

Cabling



Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings



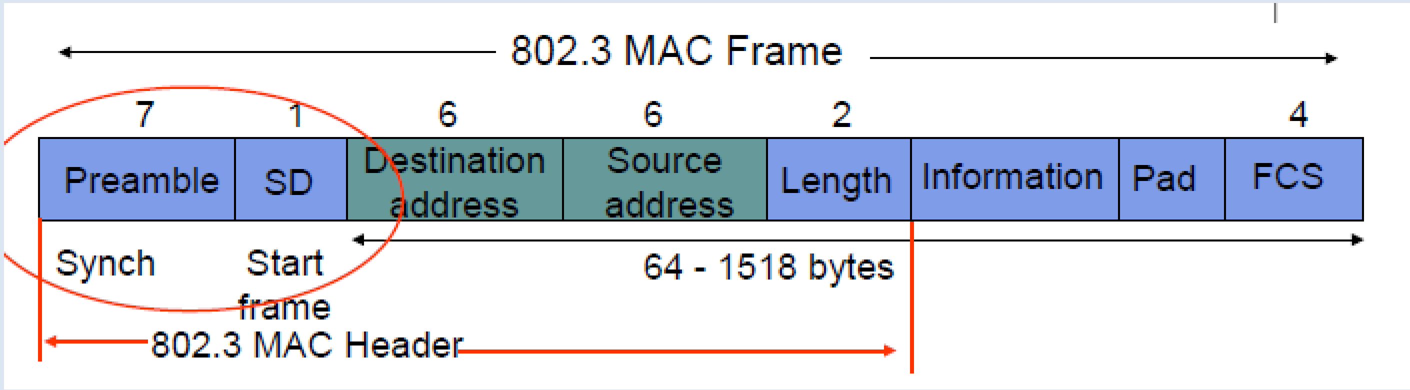
Three kinds of Ethernet cabling.

(a) 10Base5, (b) 10Base2, (c) 10Base-T.

Ethernet Standards

There are two types of Ethernet in use:

- Digital/Intel/Xerox (DIX) Ethernet (Ethernet II): This is the original Ethernet standardized by Digital Equipment Corporation, Intel and Xerox
- IEEE 802.3 Standard: an international standards by the IEEE 802 protocol suite



IEEE 802.3 MAC Frame

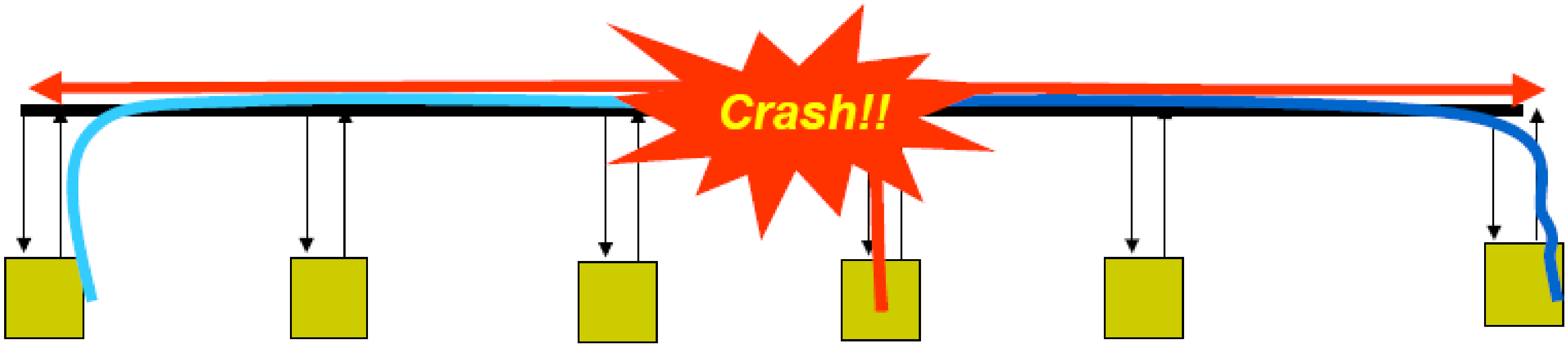
- Every frame transmission begins from scratch
- Preamble helps receivers synchronize their clocks to transmitter bit stream 7 bytes of 10101010 generate a square wave
- Start Frame Delimiter SD Start frame byte changes to 10101011
- Destination Address: Six bytes (48 bits) and contains the address of the destination station
- Source address: Six bytes and contains the address of the sender
- Length: # bytes in information field
  - Max frame 1518 bytes, excluding preamble & SD
  - Max information 1500 bytes: 05DC (hex.)
- Pad: ensures min frame of 64 bytes
- FCS Frame Check Sequence: CCITT-32 CRC, covers addresses, length, information, pad fields NIC discards frames with improper lengths or failed CRC

Multiple Access Overview

- Several terminals (stations) share the same transmission media
  - Transmission media could be over the **air** using radio (Aloha and **WLAN**) or a **shared cable** (**Ethernet**)
- Requires a **Medium Access Control (MAC)** protocol to regulate access to the shared media
  - **Random Access**: Stations submit their information whenever ready following some rules (**Ethernet**)
  - **Scheduling**: Stations take turns transmitting their information (Token ring)
- Focus is on random access techniques

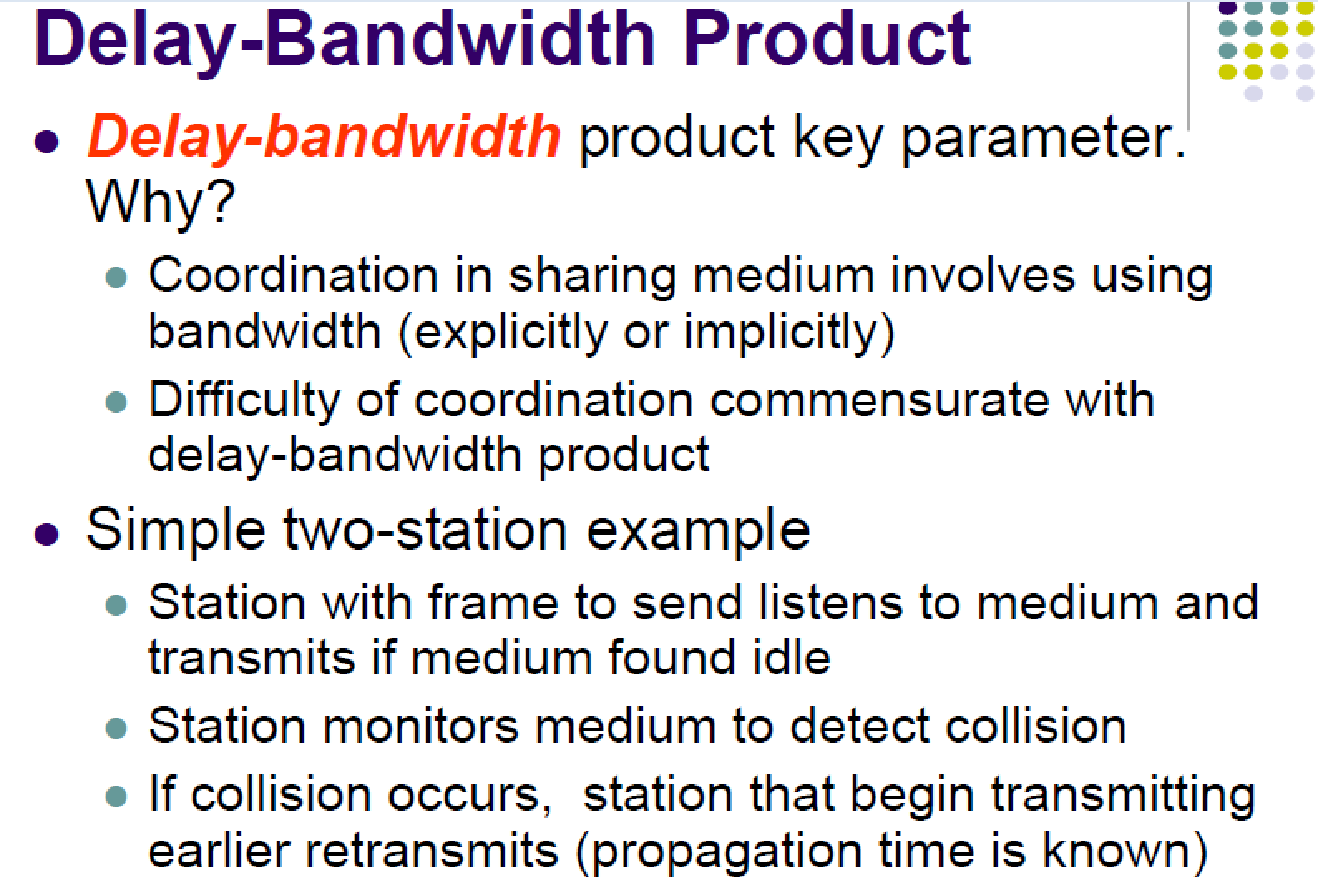
Random Access

Multitapped Bus



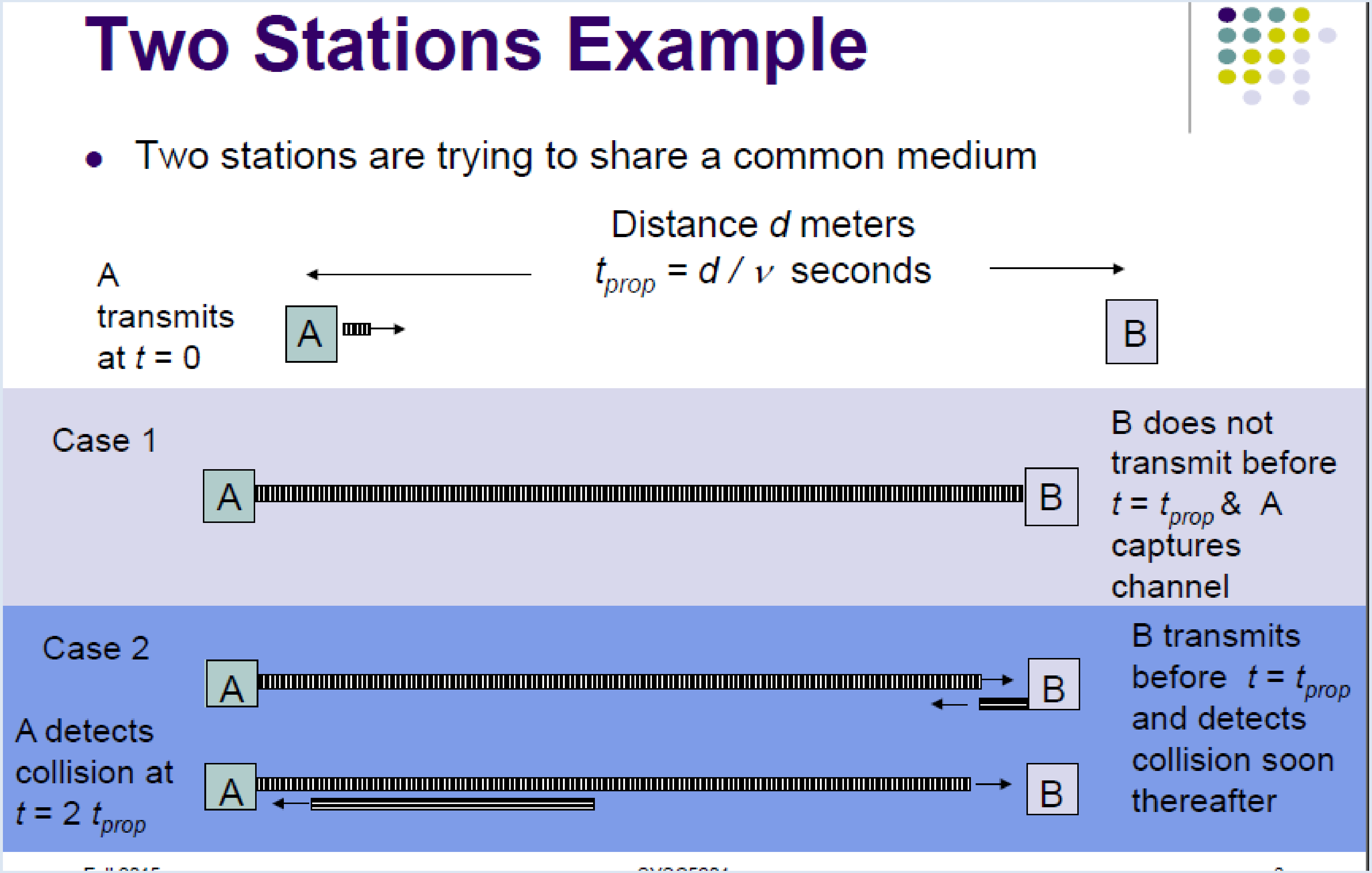
Transmit when ready

Collisions can occur; need retransmission strategy



Delay-Bandwidth Product

- ***Delay-bandwidth*** product key parameter. Why?
  - Coordination in sharing medium involves using bandwidth (explicitly or implicitly)
  - Difficulty of coordination commensurate with delay-bandwidth product
- Simple two-station example
  - Station with frame to send listens to medium and transmits if medium found idle
  - Station monitors medium to detect collision
  - If collision occurs, station that begin transmitting earlier retransmits (propagation time is known)



Two Stations Example

- Two stations are trying to share a common medium

Distance *d* meters

$t_{prop} = d / \nu$ seconds

A transmits at $t = 0$

Case 1

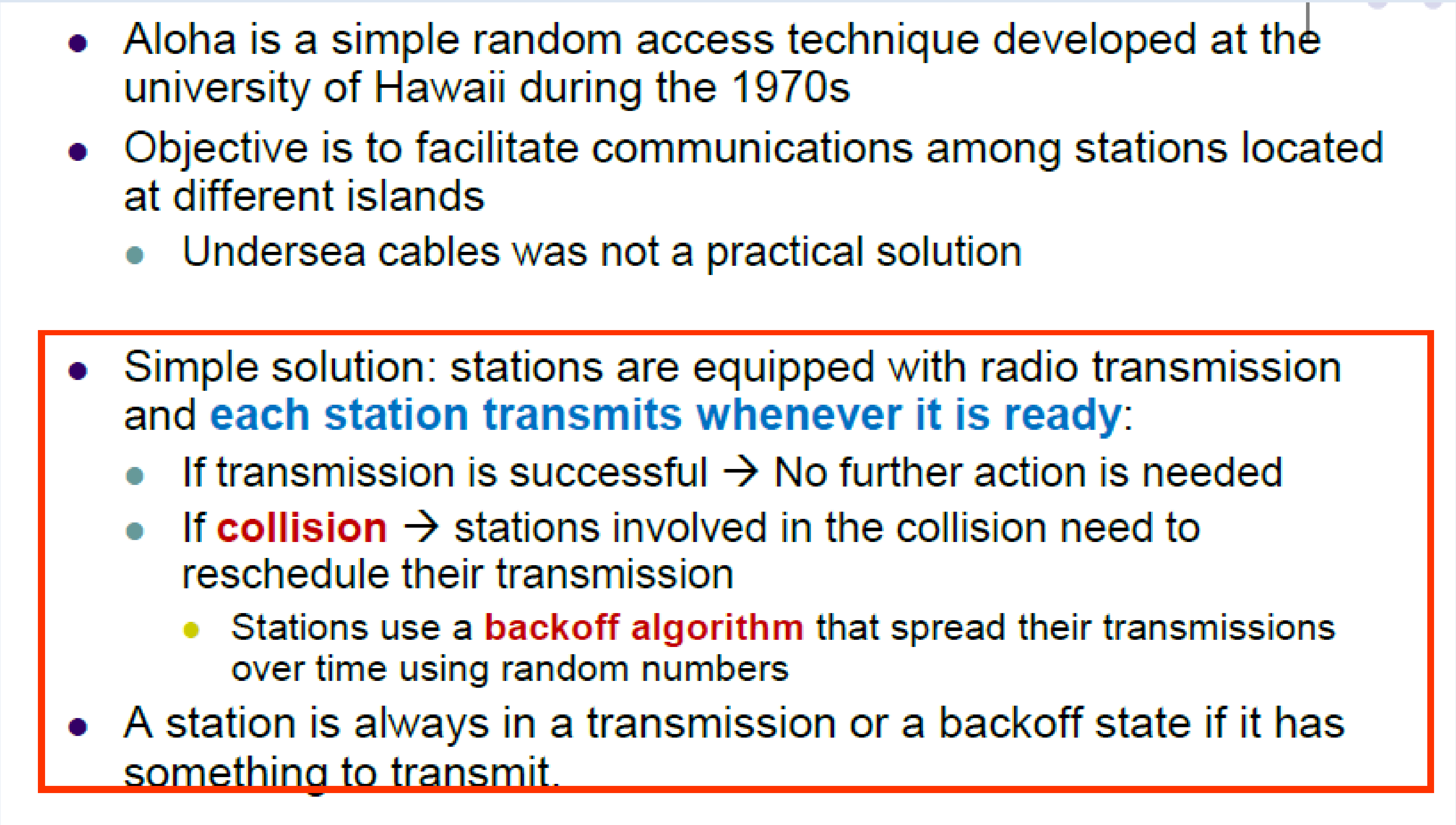
B does not transmit before $t = t_{prop}$ & A captures channel

Case 2

B transmits before $t = t_{prop}$ and detects collision soon thereafter

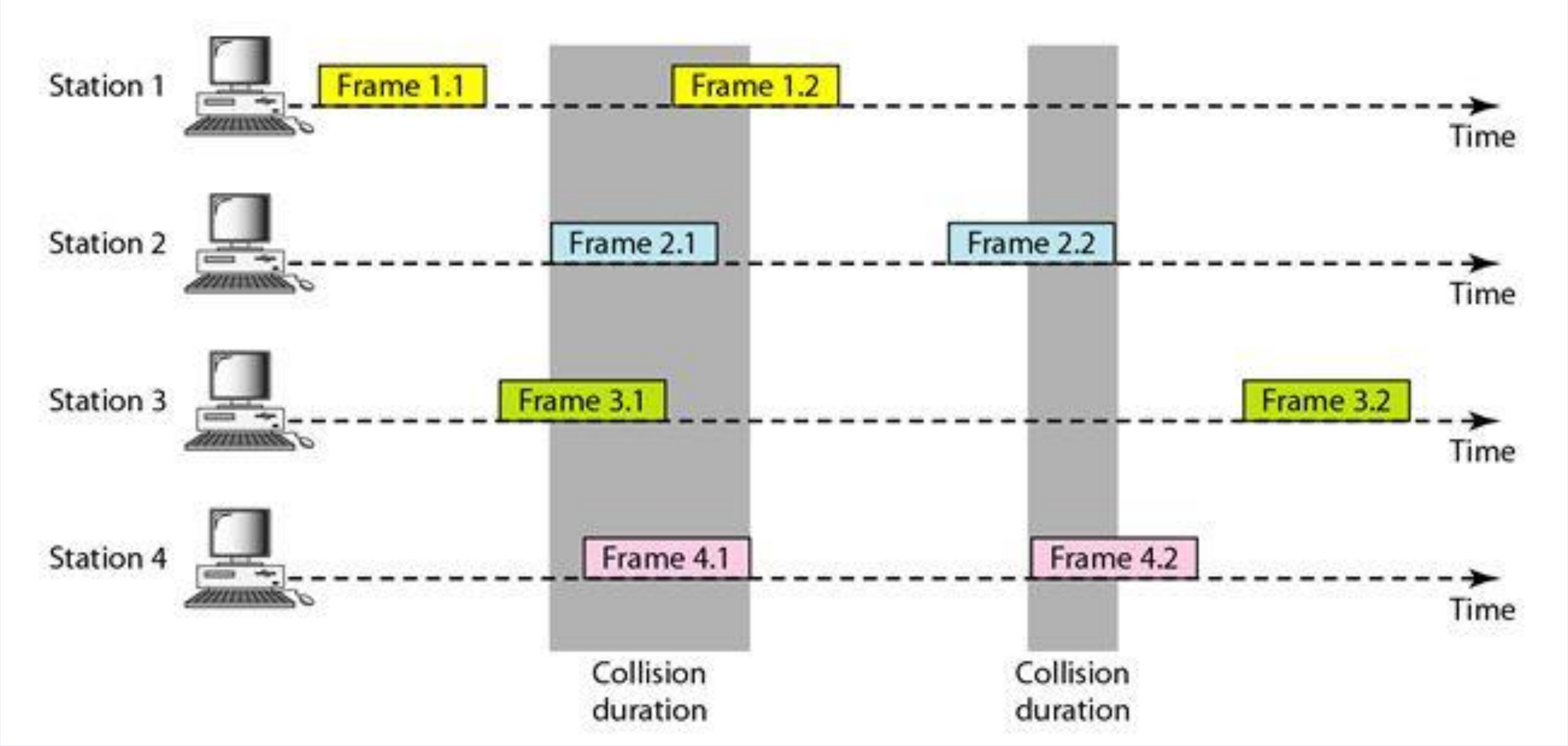
A detects collision at $t = 2\ t_{prop}$

ALOHA

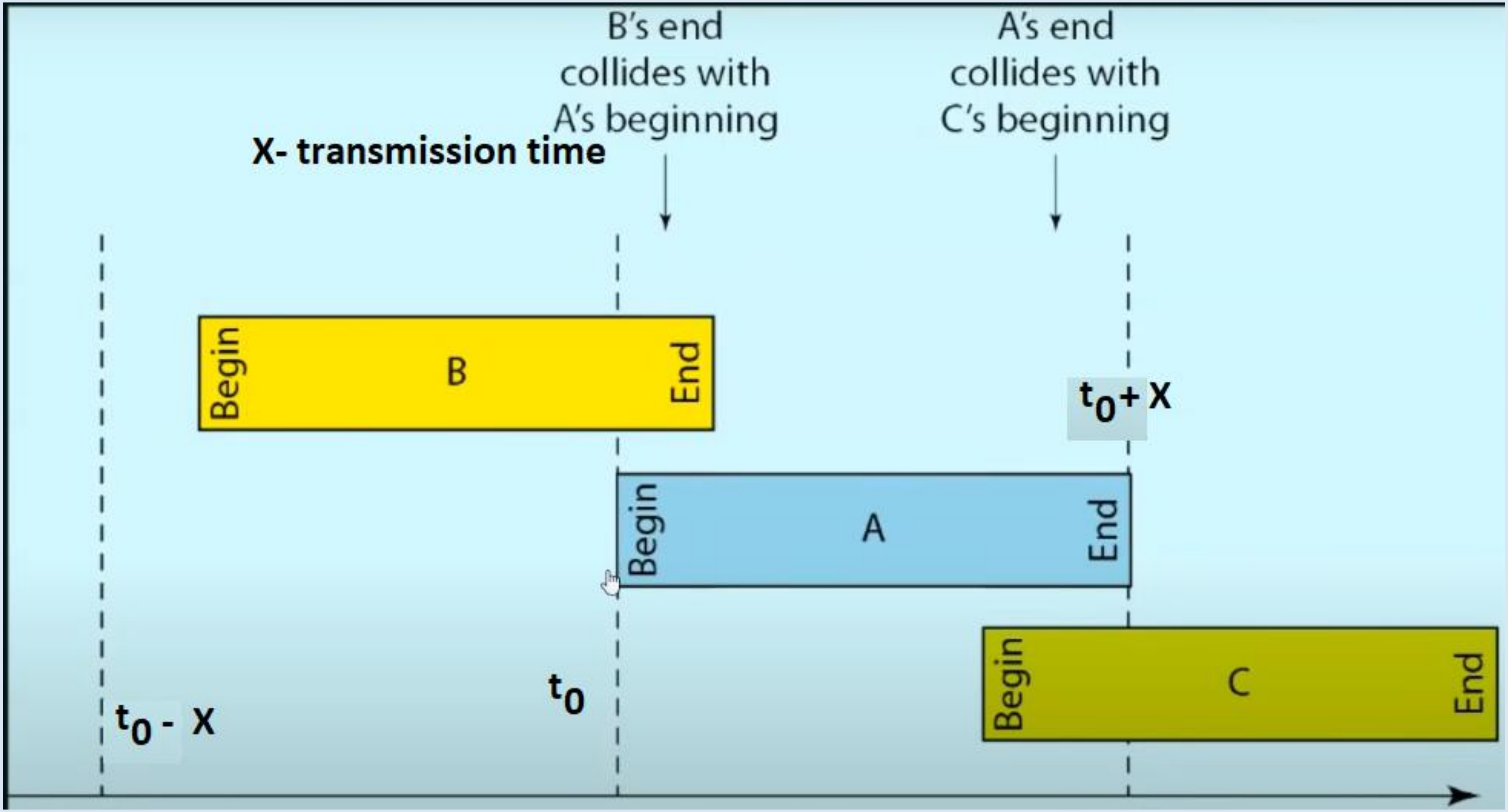


- Aloha is a simple random access technique developed at the university of Hawaii during the 1970s
- Objective is to facilitate communications among stations located at different islands
  - Undersea cables was not a practical solution
- Simple solution: stations are equipped with radio transmission and **each station transmits whenever it is ready**:
  - If transmission is successful → No further action is needed
  - If **collision** → stations involved in the collision need to reschedule their transmission
    - Stations use a **backoff algorithm** that spread their transmissions over time using random numbers
- A station is always in a transmission or a backoff state if it has something to transmit.

Pure Aloha


Station 1
Frame 1.1
Frame 1.2
Time
Station 2
Frame 2.1
Frame 2.2
Time
Station 3
Frame 3.1
Frame 3.2
Time
Station 4
Frame 4.1
Frame 4.2
Time
Collision duration
Collision duration

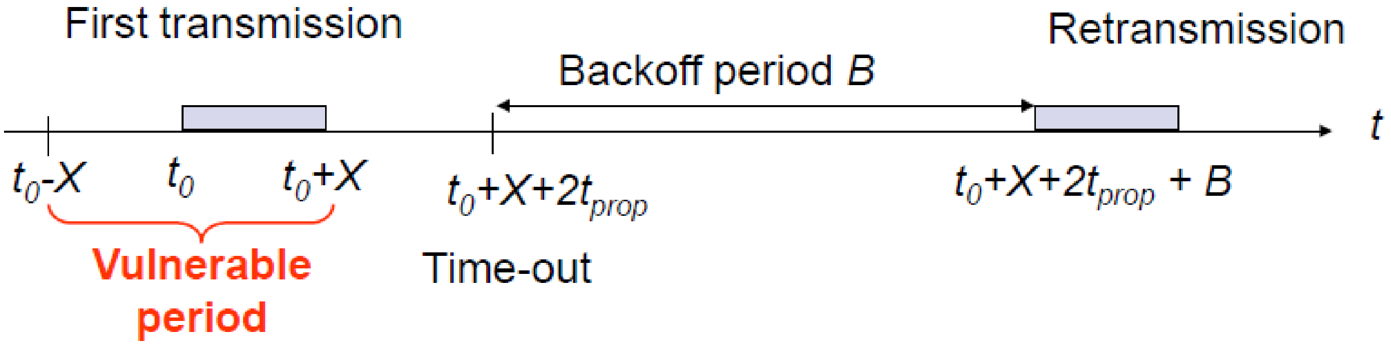
Pure Aloha


B's end collides with A's beginning
A's end collides with C's beginning
X- transmission time
Begin
B
End
$t_0 + X$
Begin
A
End
Begin
C
End
t_0
$t_0 - X$

Aloha Operation

t_0: transmission starts
X: transmission time

t_0+X+2t_{prop}: earliest time to obtain the outcome (ACK or not) of transmission

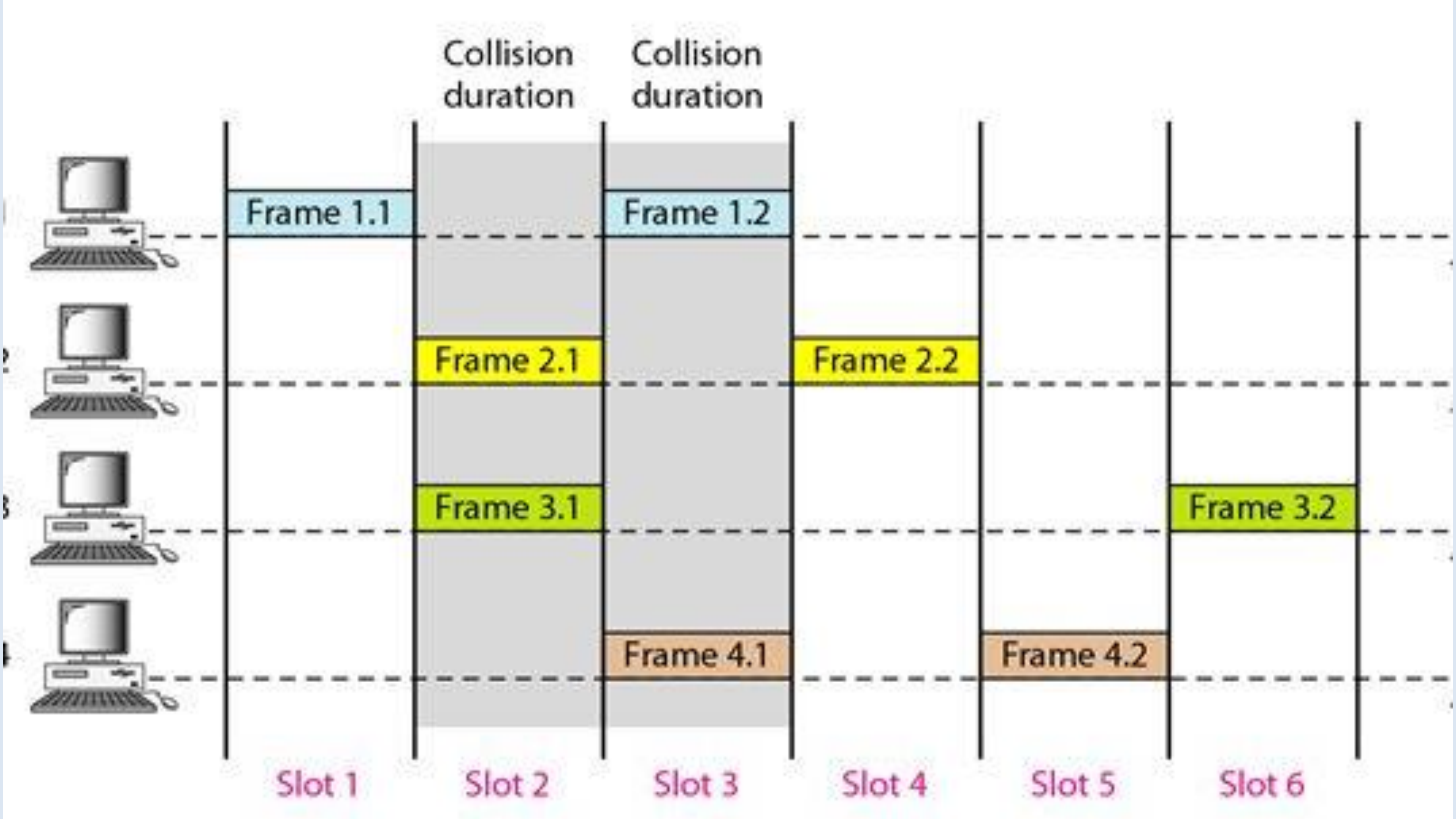


The probability of a successful transmission is that there are no additional frame transmissions in the **vulnerable period**.

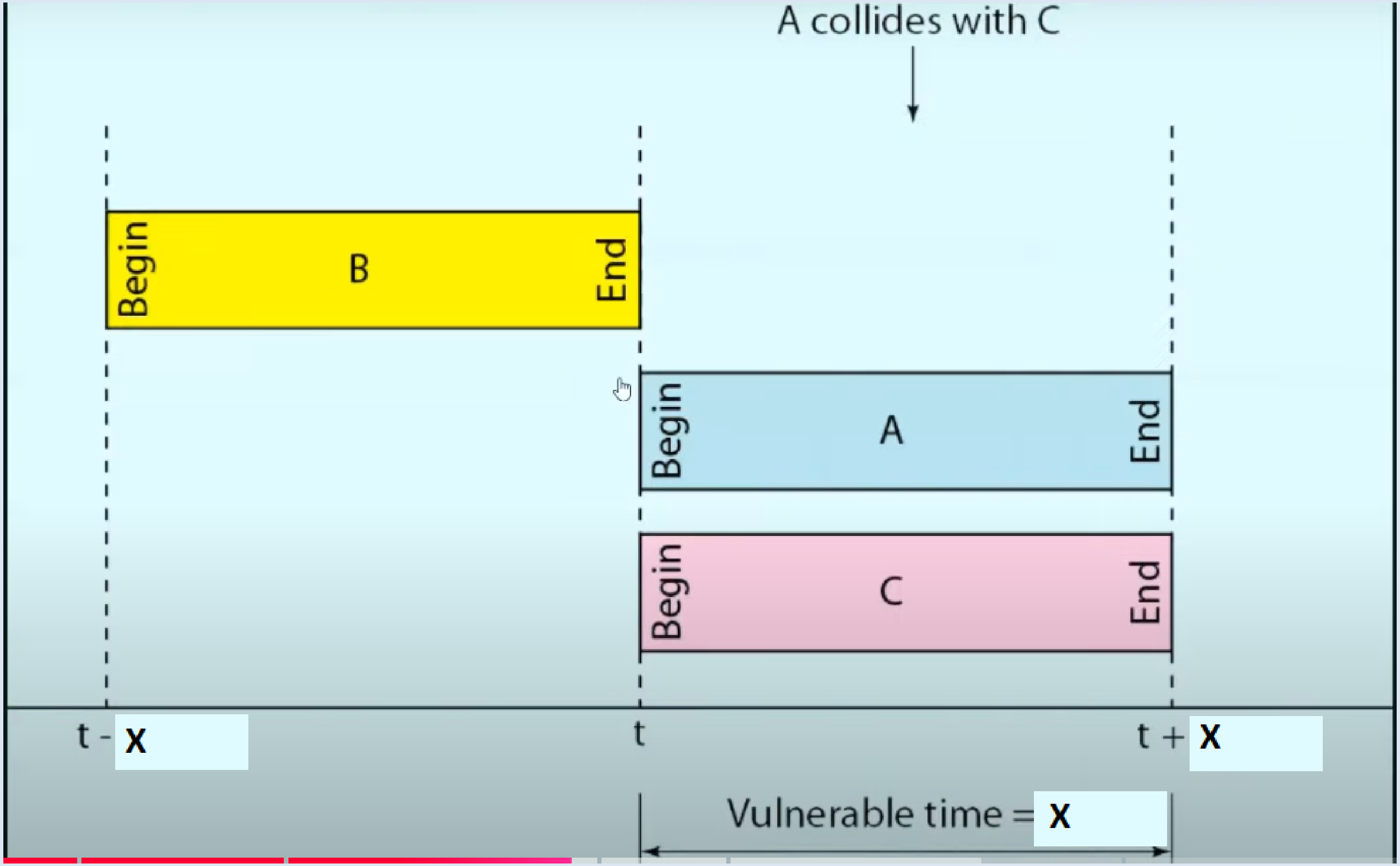
Areas for improvement?
1. Shorten vulnerable period; 2. Medium access: impose rules

- Frame length is constant = L and constant transmission time $X = L/R$
- *Time is normalized to X, called a slot*

Slotted ALOHA

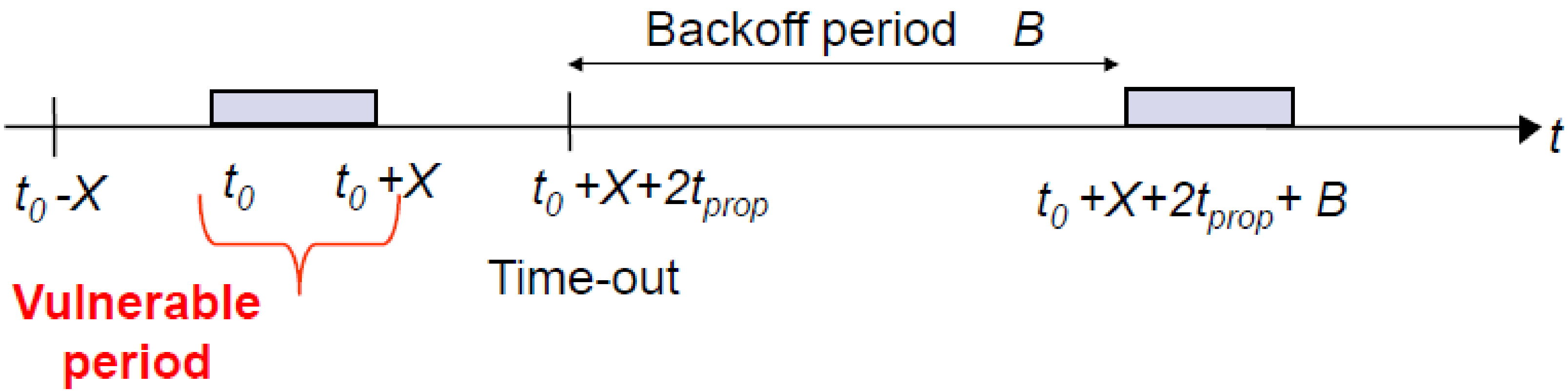


Slotted ALOHA



Slotted Aloha

- **Goal is to reduce the prob. of collisions**
- Time is slotted in X seconds slots
- Stations **synchronized** to frame times
  - achieved by transmitting periodic synch pulses from one designated station in the network
- Stations can initiate transmissions only at the beginning of slot.
- Stations transmit frames in first slot after frame arrival
- ***Backoff intervals in multiples of slots***

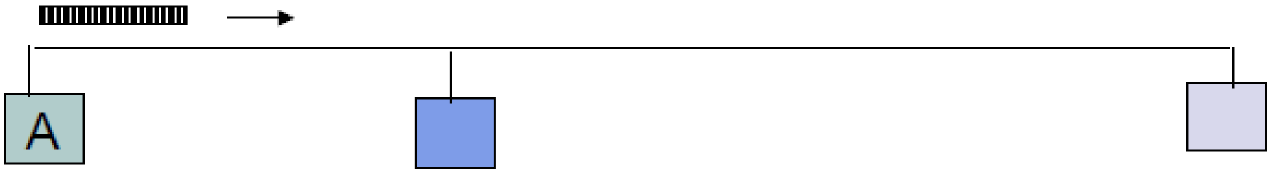


Only frames that arrive during prior X seconds collide

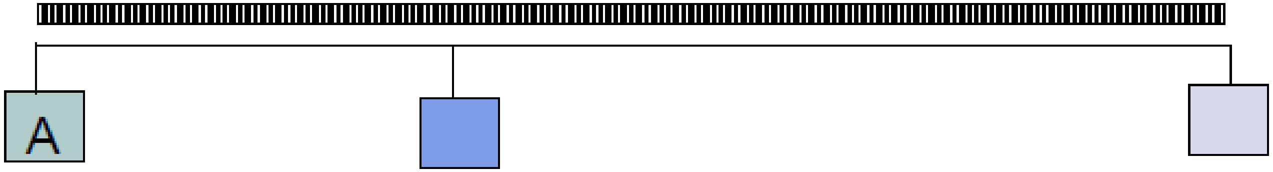
Carrier Sense Multiple Access (CSMA)

- A **station senses the channel** before it starts transmission
  - If busy, either wait or schedule backoff (different options)
  - If idle, start transmission
  - **Vulnerable period is reduced to t_{prop}** (time required so that station A *captures the channel*)
  - When collisions occur they involve entire frame
  - If t_{prop} >= X, no gain compared to ALOHA or slotted ALOHA

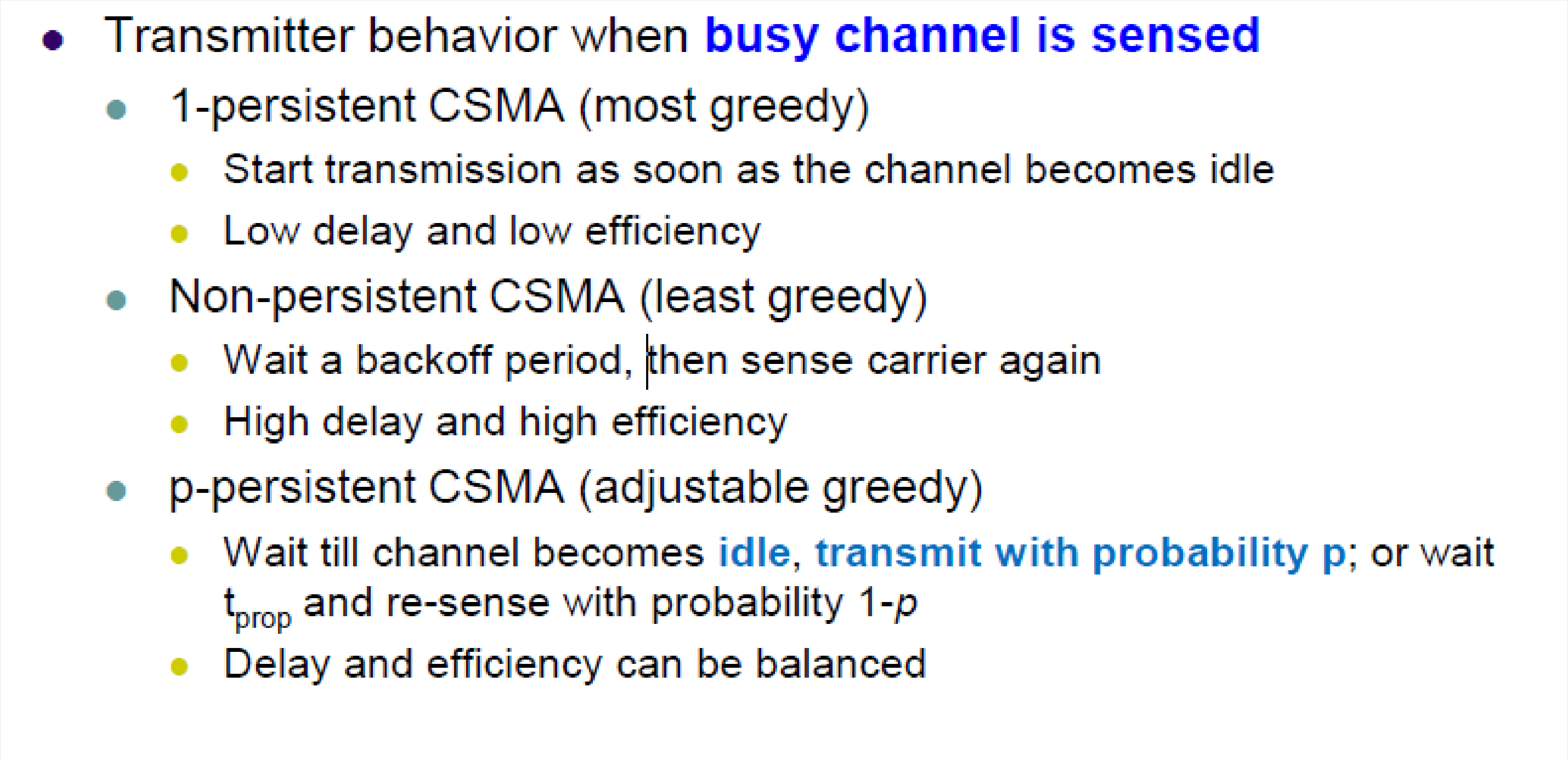
Station A begins transmission at $t = 0$



Station A captures channel at $t = t_{prop}$



CSMA Options



- Transmitter behavior when **busy channel is sensed**
  - 1-persistent CSMA (most greedy)
    - Start transmission as soon as the channel becomes idle
    - Low delay and low efficiency
  - Non-persistent CSMA (least greedy)
    - Wait a backoff period, then sense carrier again
    - High delay and high efficiency
  - p-persistent CSMA (adjustable greedy)
    - Wait till channel becomes **idle**, **transmit with probability p**; or wait t_{prop} and re-sense with probability 1-*p*
    - Delay and efficiency can be balanced

1-persistent CSMA

- Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that moment.
- If the channel is idle, the station transmits a frame.
- If busy, then it senses the transmission medium continuously until it becomes idle.
- Since the station transmits the frame with the probability of 1 when the carrier of channel is idle, this scheme of CSMA is called as 1-persistent CSMA.
- The longer the propagation delay, the more important this effect becomes, and the worse the performance of the protocol.

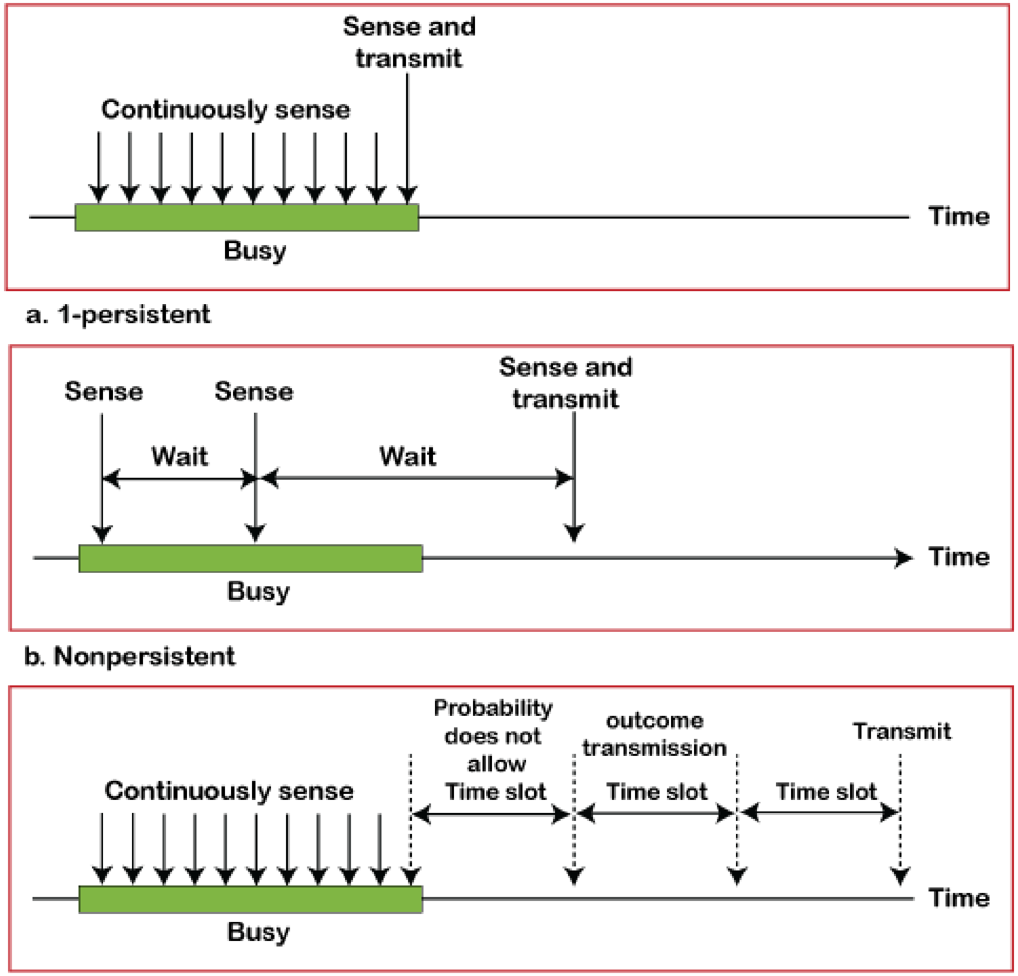
Non-persistent CSMA

- Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself.
- However, if the channel is already in use, the station doesnot continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
- Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

P-persistent CSMA

- It applies to slotted channels.
- When a station becomes ready to send, it senses the channel.
- If it is idle, it transmits with a probability P.
- With a probability 1-P, it defers until the next slot.
- If that slot is also idle, it either transmits or defers again, with probabilities P and 1-P.
- This process is repeated until either the frame has been transmitted or another station has begun transmitting.
- In the latter case, the unlucky station acts as if there had been a collision (i.e. it waits a random time and starts again.)

CSMA

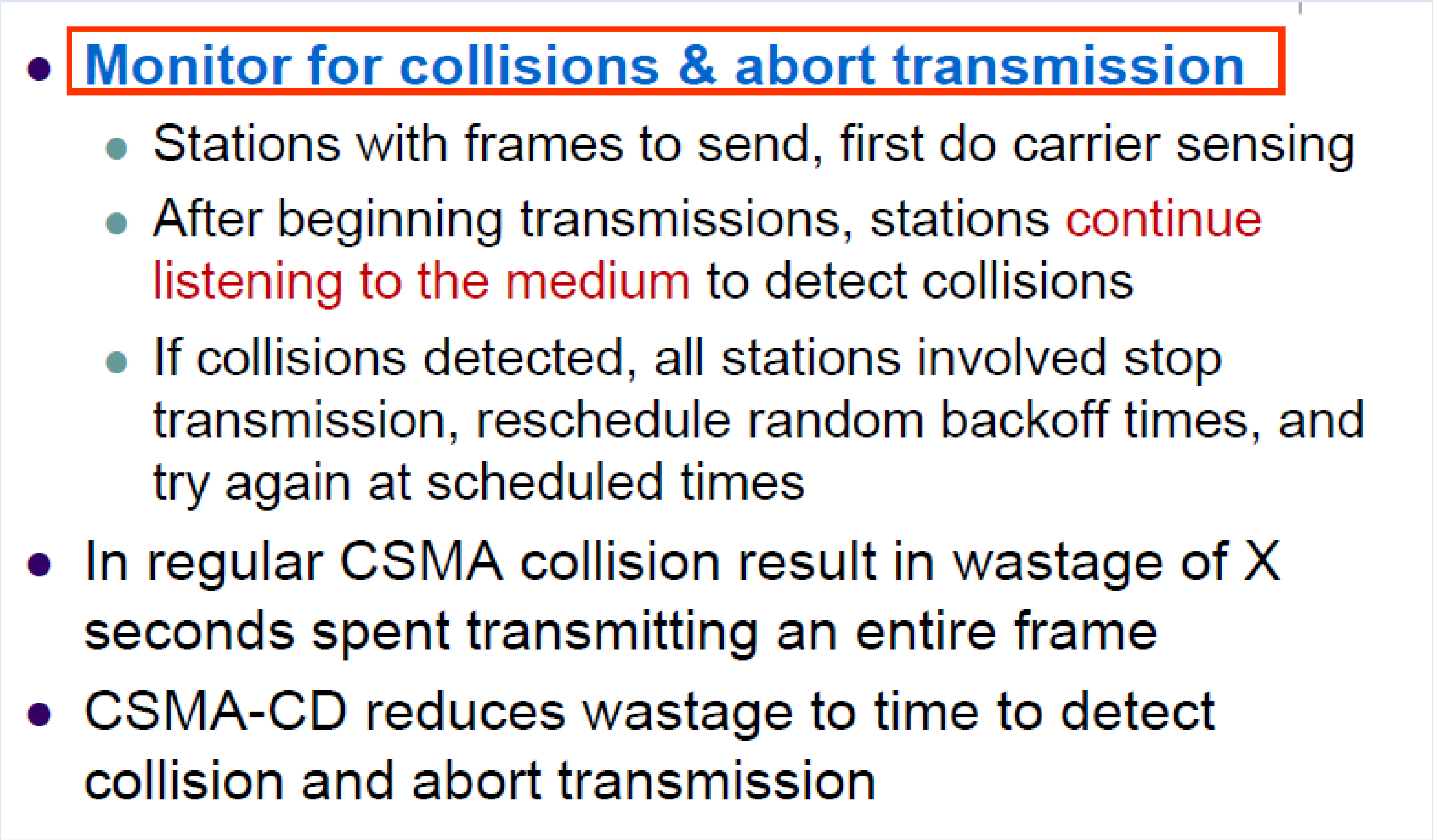


a. 1-persistent

b. Nonpersistent

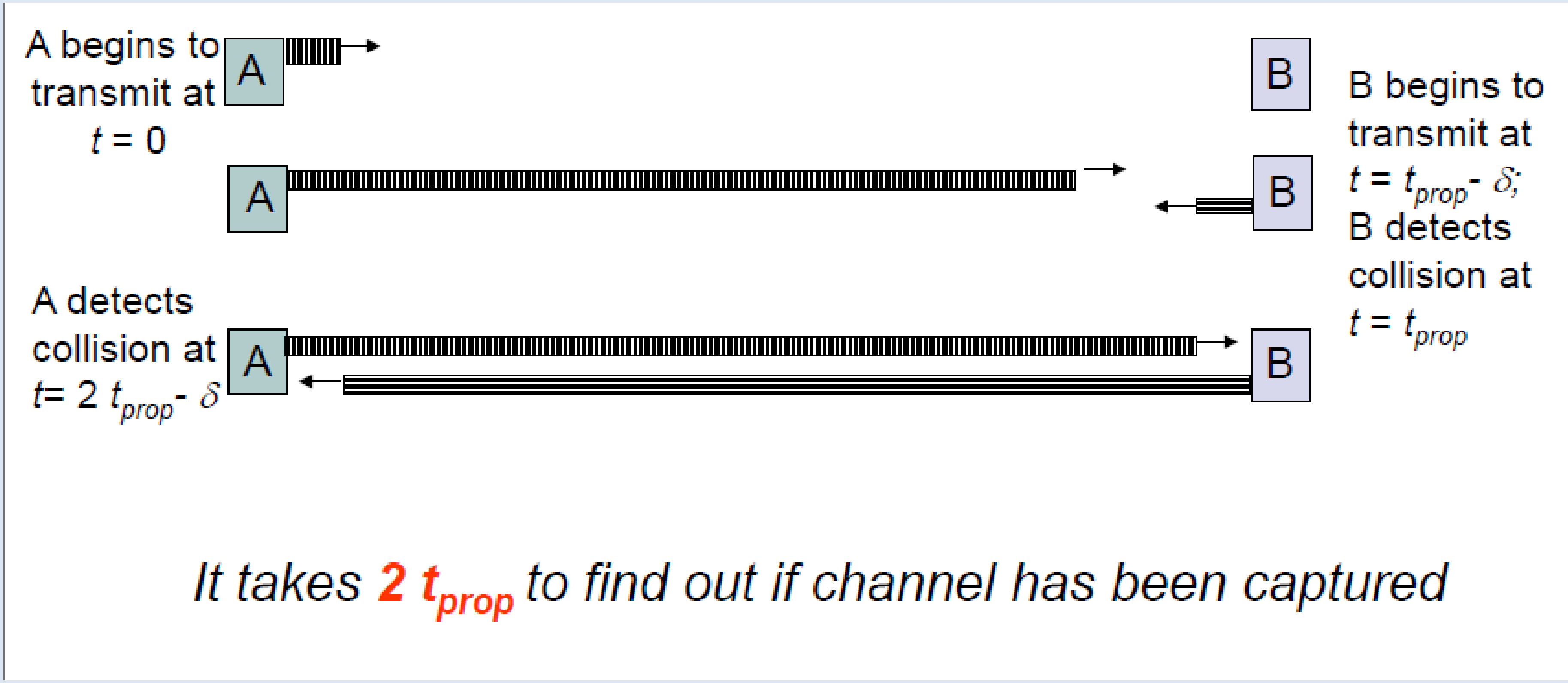
c. p-persistent

CSMA with Collision Detection (CSMA/CD)



- **Monitor for collisions & abort transmission**
  - Stations with frames to send, first do carrier sensing
  - After beginning transmissions, stations continue listening to the medium to detect collisions
  - If collisions detected, all stations involved stop transmission, reschedule random backoff times, and try again at scheduled times
- In regular CSMA collision result in wastage of X seconds spent transmitting an entire frame
- CSMA-CD reduces wastage to time to detect collision and abort transmission

CSMA/CD Reaction Time



A begins to transmit at $t = 0$

B begins to transmit at $t = t_{prop} - \delta$;
B detects collision at $t = t_{prop}$

A detects collision at $t = 2\, t_{prop} - \delta$

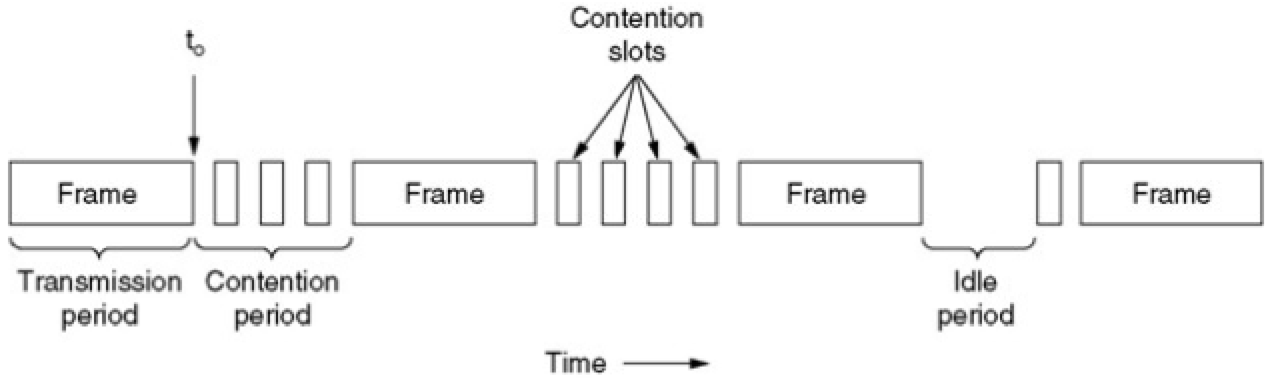
*It takes **2 t_{prop}** to find out if channel has been captured*

CSMA/CD

- CSMA/CD is widely used on LANs in the MAC sublayer.
- Access method used by Ethernet: CSMA/CD
- At the point t0, a station has finished transmitting its frame.
- Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision.
- Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.
- After a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.

CSMA/CD

- Therefore, model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.



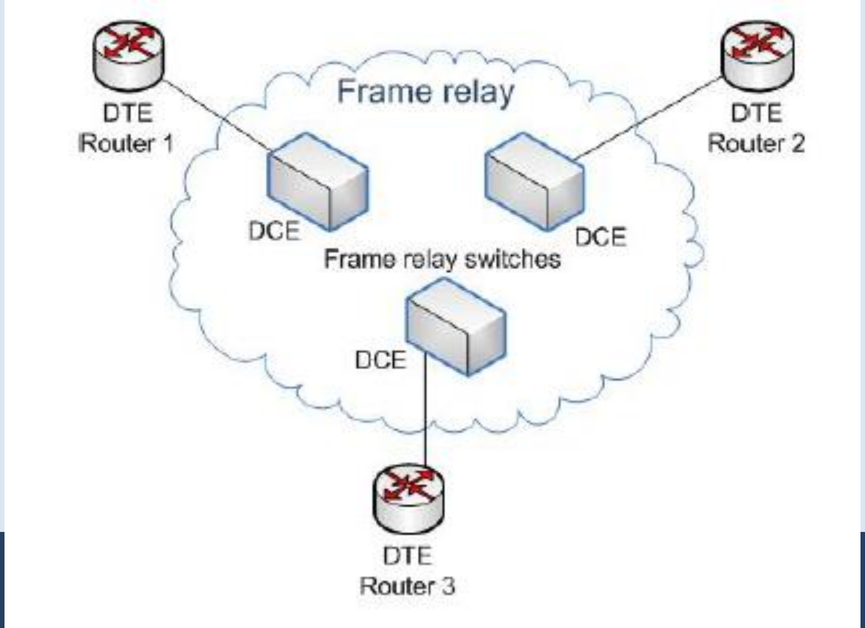
CSMA/CD can be in one of three states: contention, transmission, or idle.

X.25

- Connection-oriented protocol and most widely used protocol in WAN.
- X.25 protocol allows computers on different public networks to communicate through an intermediary computer at the network layer. X.25 standard for packet switching is a lower three layer equivalent of the OSI model – Physical layer, link layer and packet layer
- Physical layer: Physical interface between a attached station (computer terminal and packet switching mode)
- Link level: Provides reliable transfer of data across physical link. Link level is referred as link access protocol.
- Packet level: Provides virtual circuit service enables any subscriber to the network to setup logical connections

Frame relay

- Packet switching network protocol that is designed to work at the data link layer of the network. -> By dividing the data into packets known as frames and transmitting these packets across the network
- Used to connect LANs and transmit data across WANs
- More efficient than X.25, and a higher process speed is achieved (it can transmit over 2.044 Mbps)
- Evolved from X.25 packet switching and the objective is to reduce network delays, protocol overheads and equipment cost.



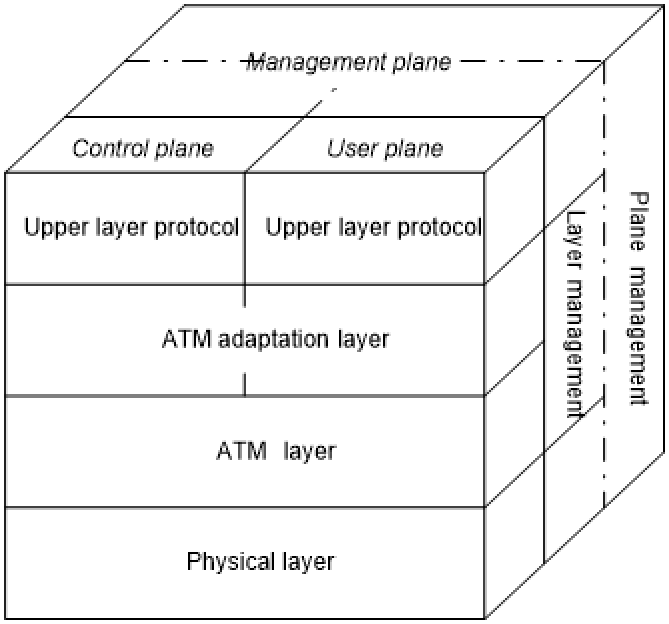
Asynchronous Transfer Mode (ATM)

- ATM is a packet-switched technology

The packets that are switched in an ATM network are of fixed length, 53 bytes (5 bytes header and 48 bytes payload), and are called cells.

- Cells are transmitted asynchronously and the network is connection-oriented. -> requires connection setup before transmitting data i.e. virtual circuit
- Technique utilizes asynchronous time-division multiplexing to encode data into tiny and fixed-size cells.
- Asynchronous represents that the packets obtained from various users are not required to be transmitted at periodic intervals

- User plane: for user traffic including flow and error control
- Control plane: for connection control
- Management plane: manages the system as a whole and coordinates the planes and layers



ATM layers functions

- Physical layer:

✓ Provides transmission channels for ATM cells.

✓ At this layer, cells received from the ATM layer are transferred into a continuous bit stream

- ATM layer

✓ Defines transmission of data in fixed size cells

✓ Also defines the logical connections (Virtual circuits and virtual paths)

✓ Responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing

✓ Handles transmission, switching, congestion control, cell header processing

- ATM Adaption layer

AAL accepts higher layer packets and segments them into fixed sized ATM cells (48 byte payload) before transmission via ATM

- ATM upper-layer protocols

Responsible for WAN interconnection, Layer 3 interconnection