Computer Networks

Course Outline

- Introduction
- Physical Layer
- Data Link Layer
- MAC Sub-layer
- Network Layer
- Transport Layer
- Application Layer

Books

- ***Computer Networks*** by Andrew S. Tanenbaum
  - Pearson

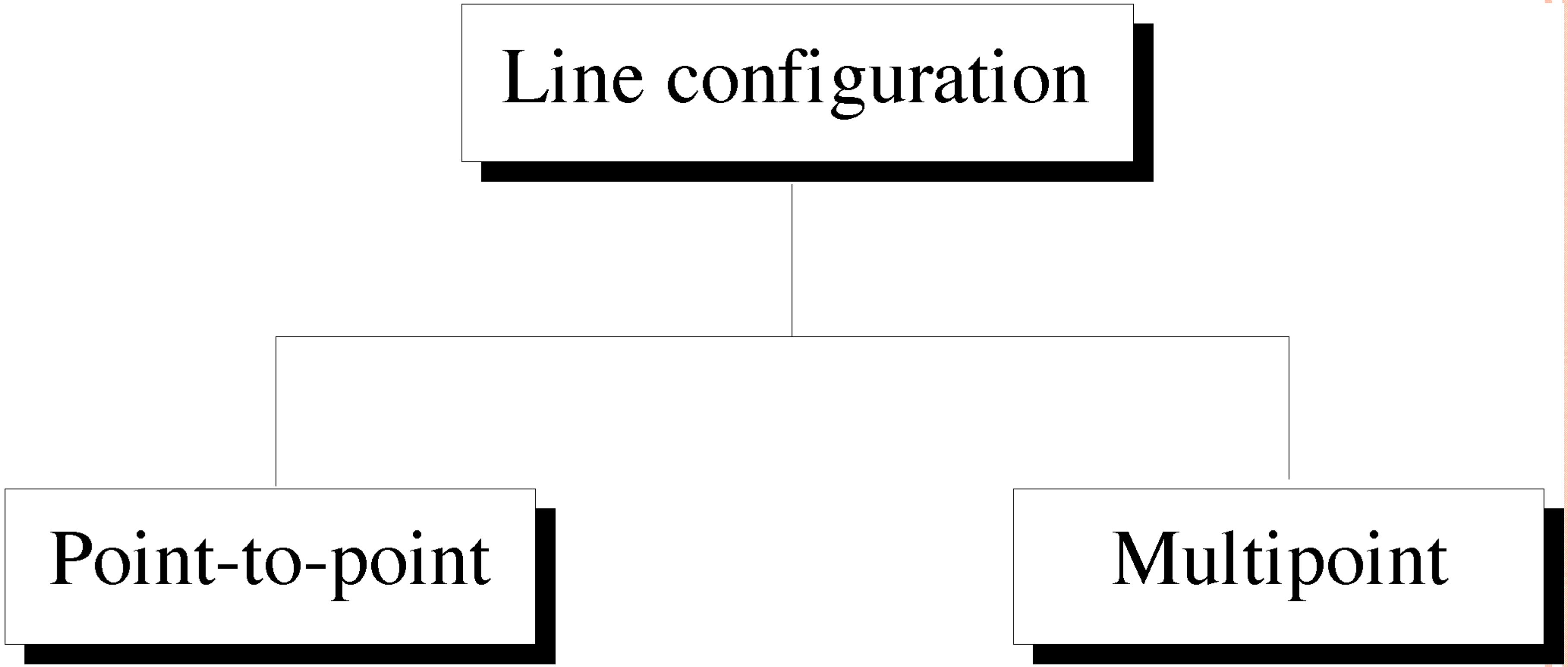
- ***Data Communication and Networking*** by Behrouz A. Forouzan
  - Tata-McGraw Hill

- ***Computer Networking – A Top-Down Approach Featuring the Internet*** by James F. Kurose and Keith W. Ross
  - Pearson

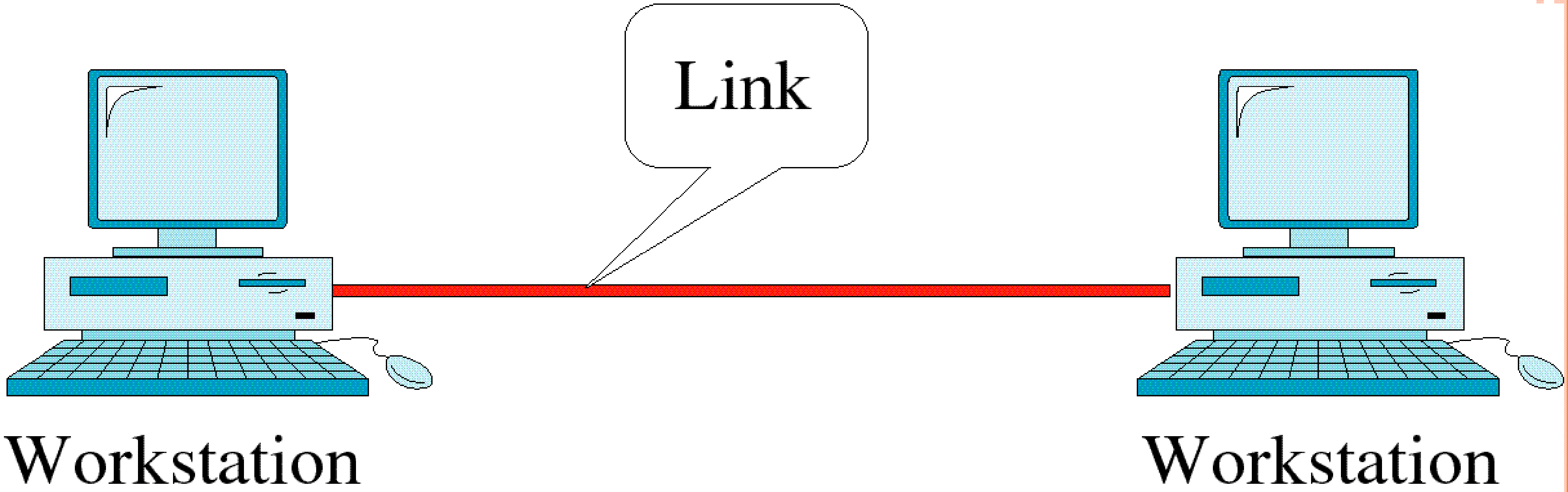
Grading

- Quiz-1: 20%
- Mid Term: 20%
- Quiz-2: 20%
- Final: 40%

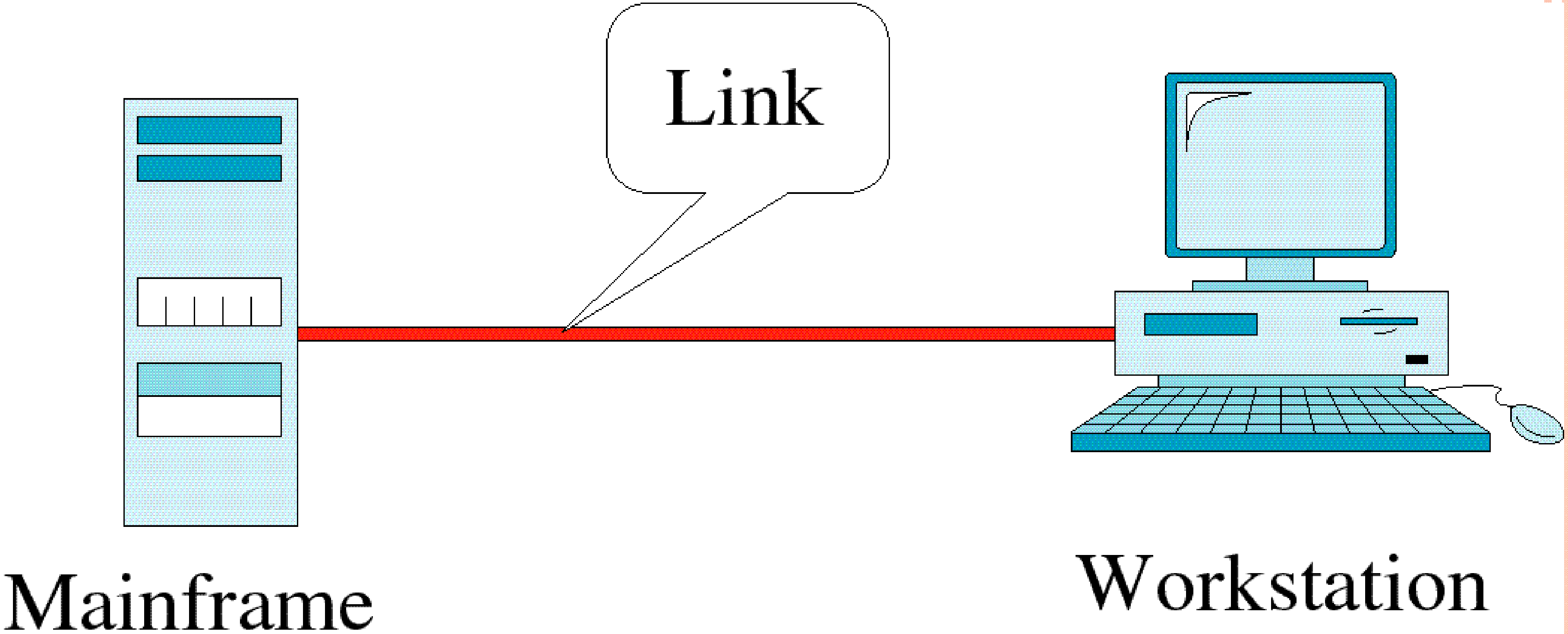
LINE CONFIGURATION



Point to Point Configuration

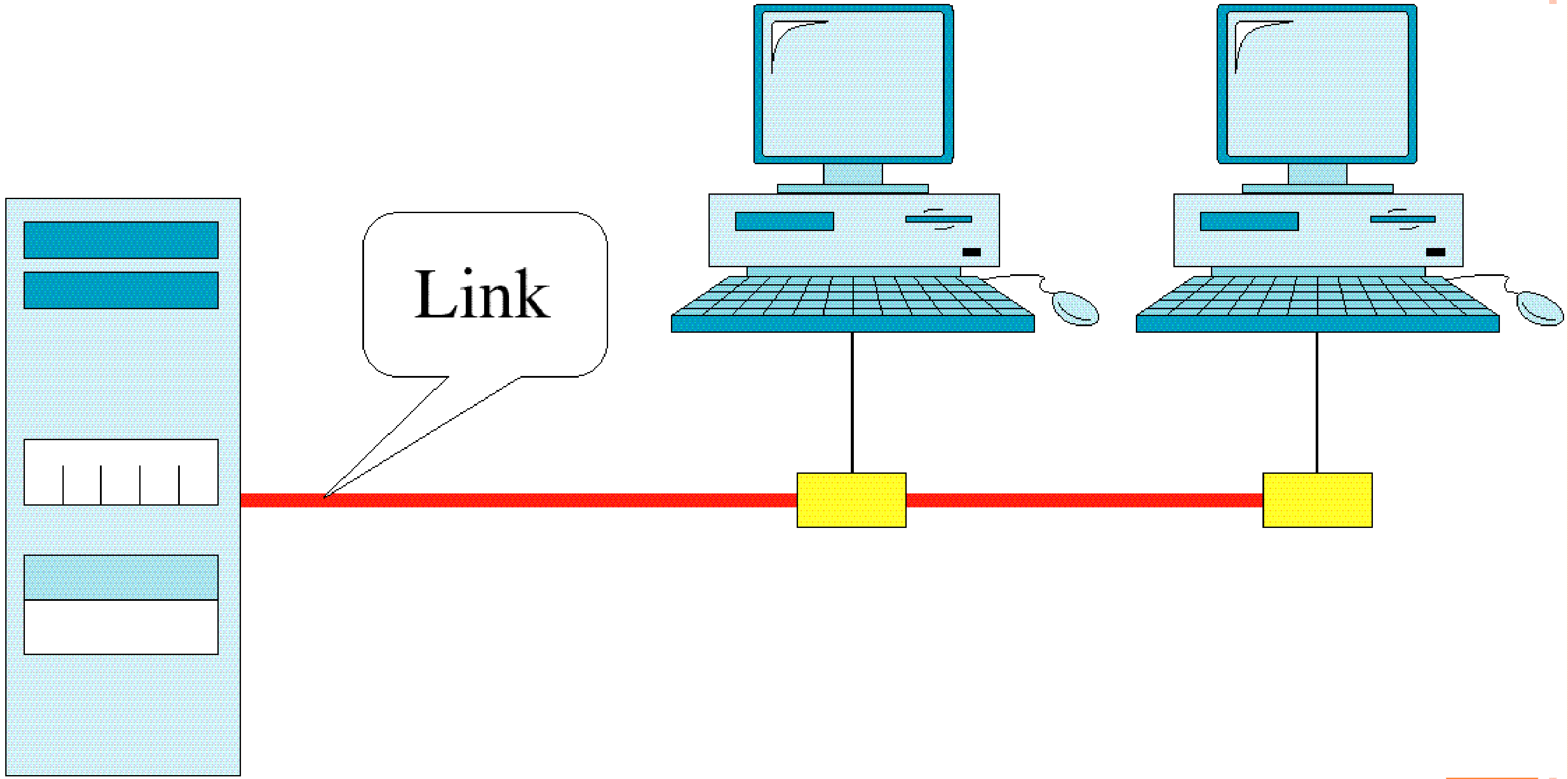


Point to Point Configuration

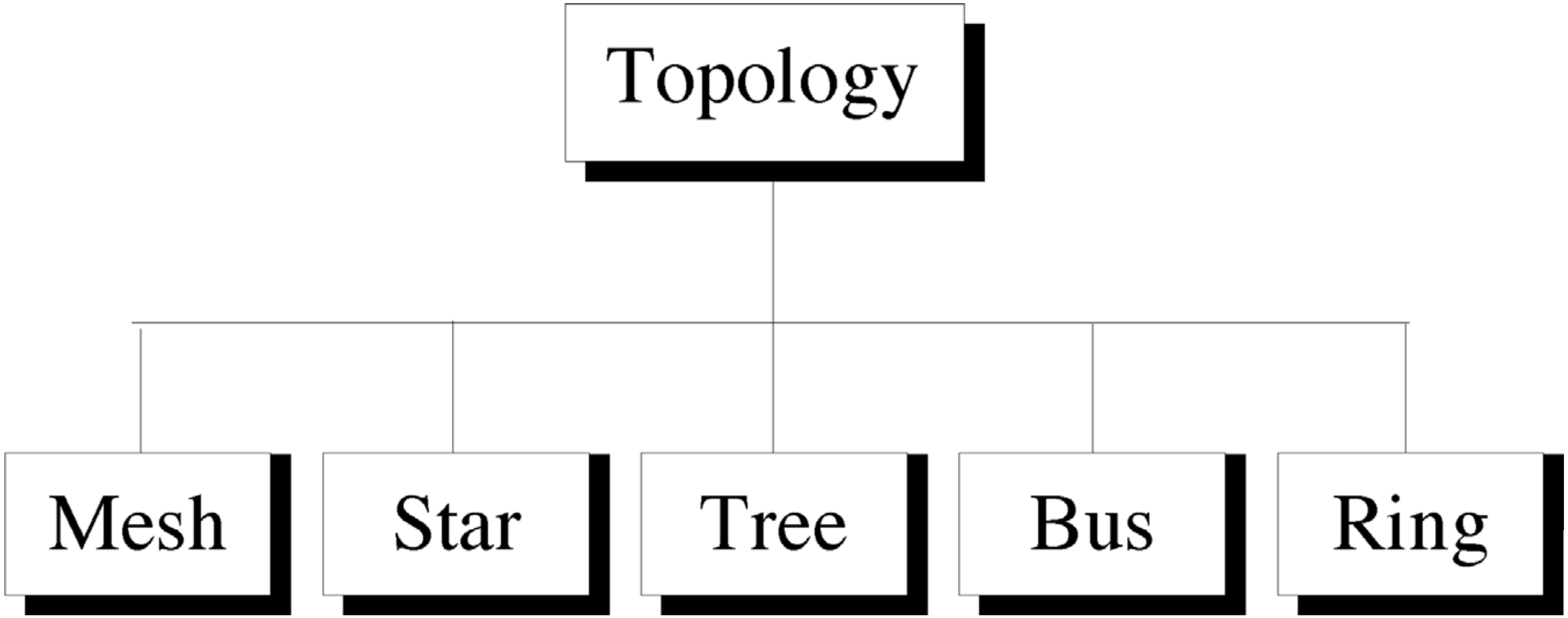


Point to Point Configuration

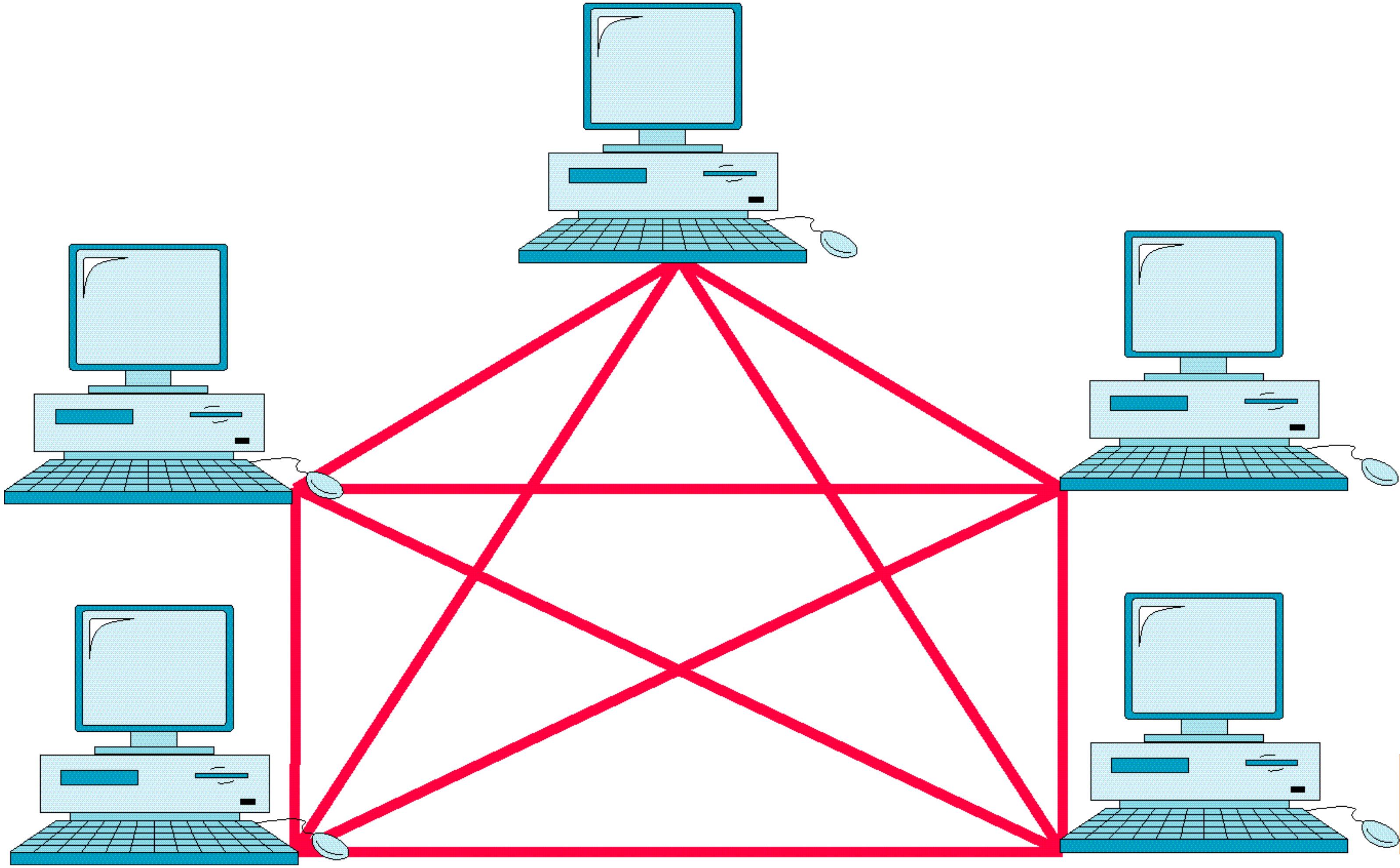
Multipoint Line Configuration



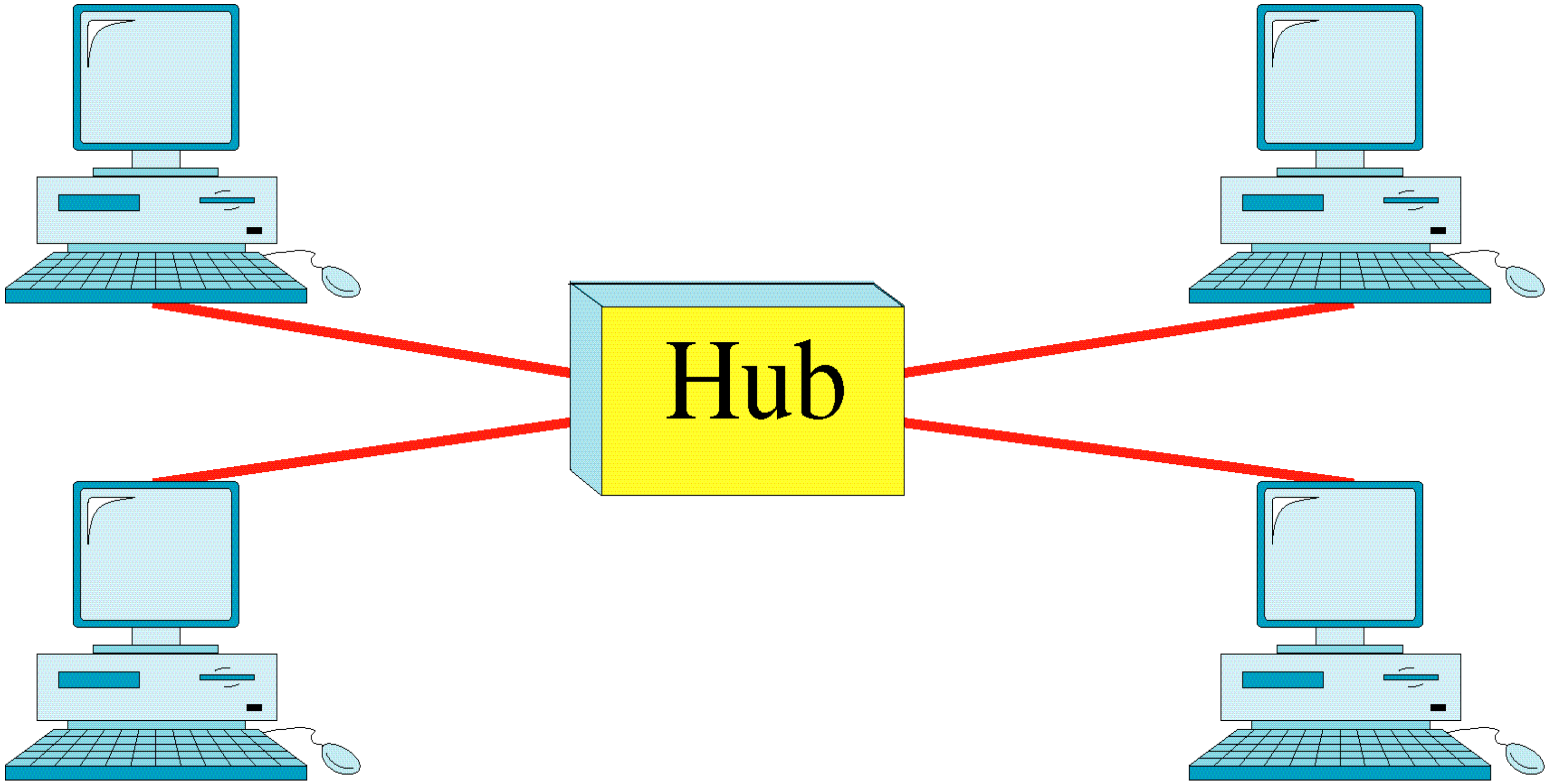
NETWORK TOPOLOGIES



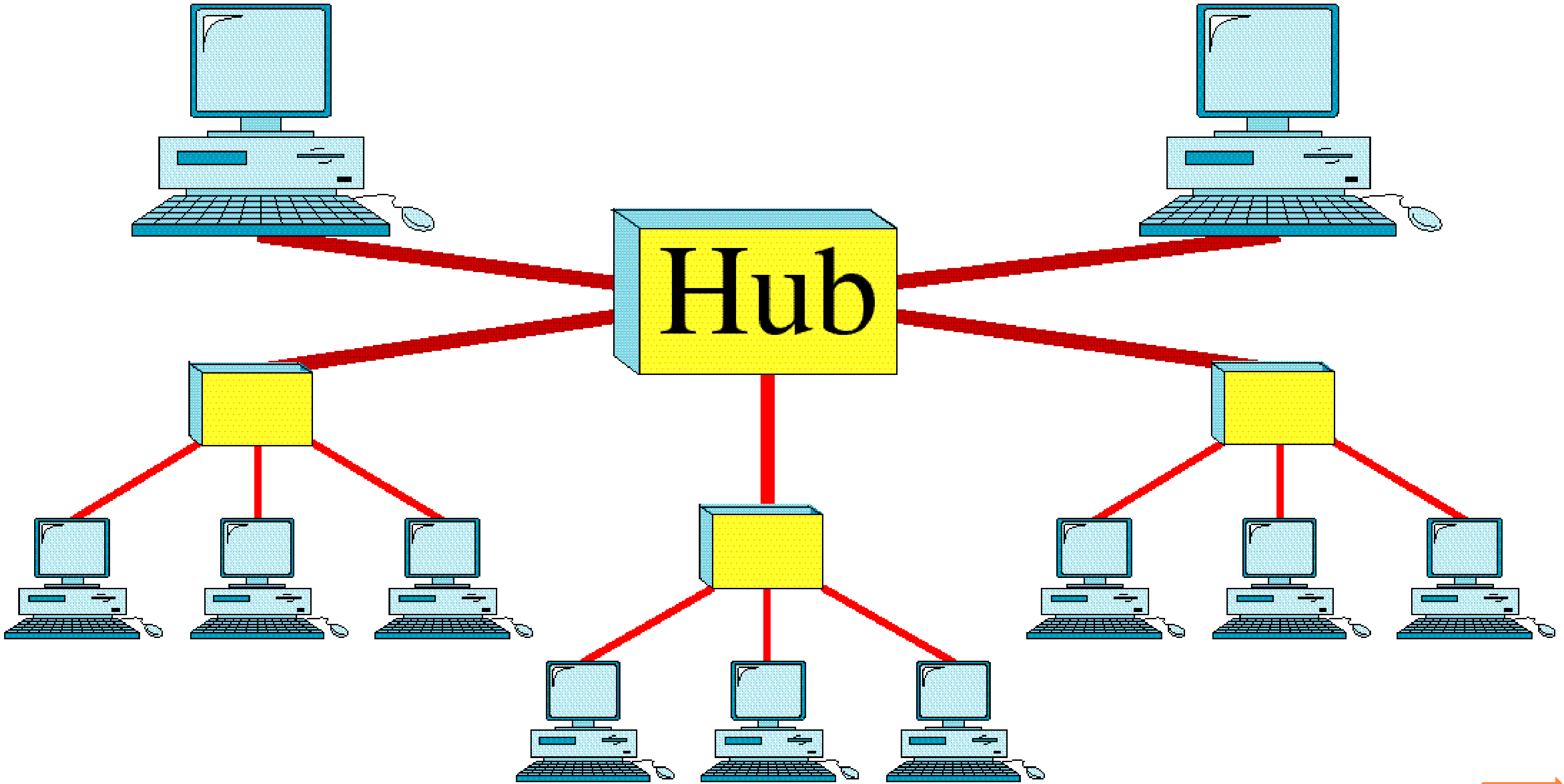
Mesh Topology



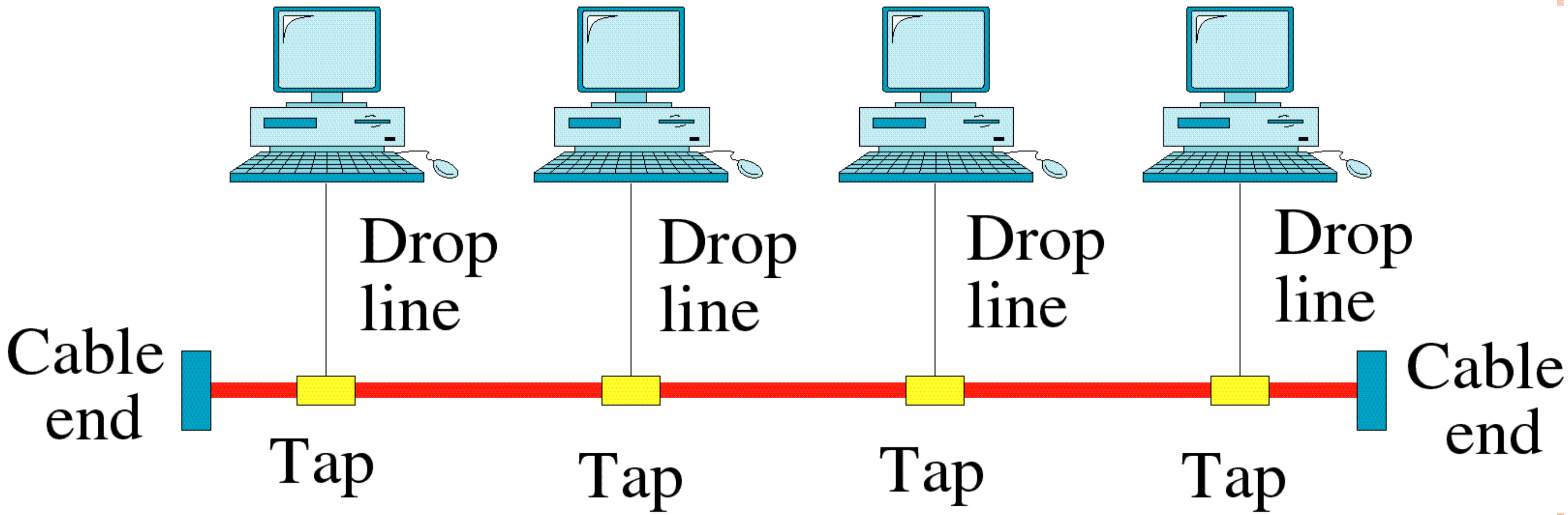
Star Topology



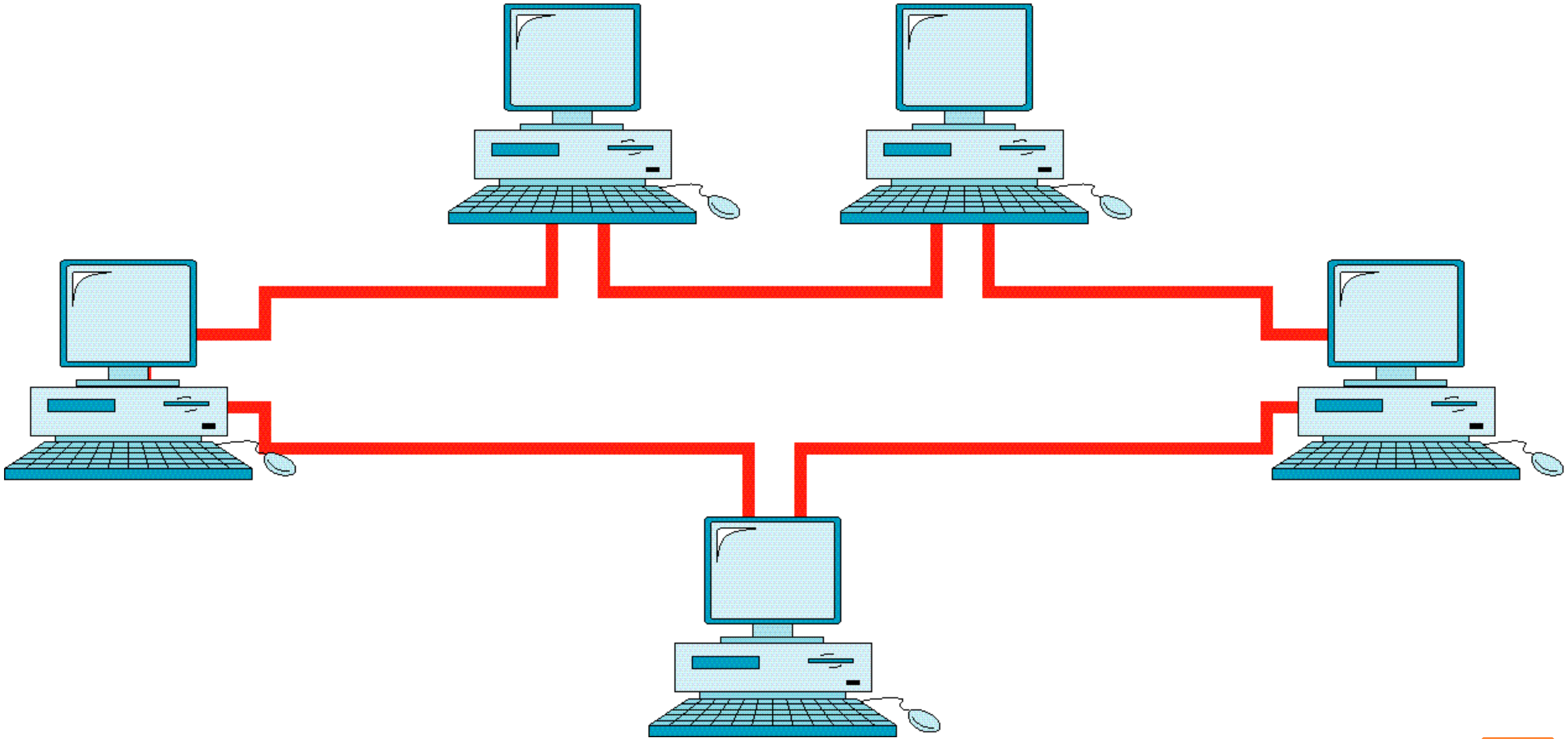
Tree Topology



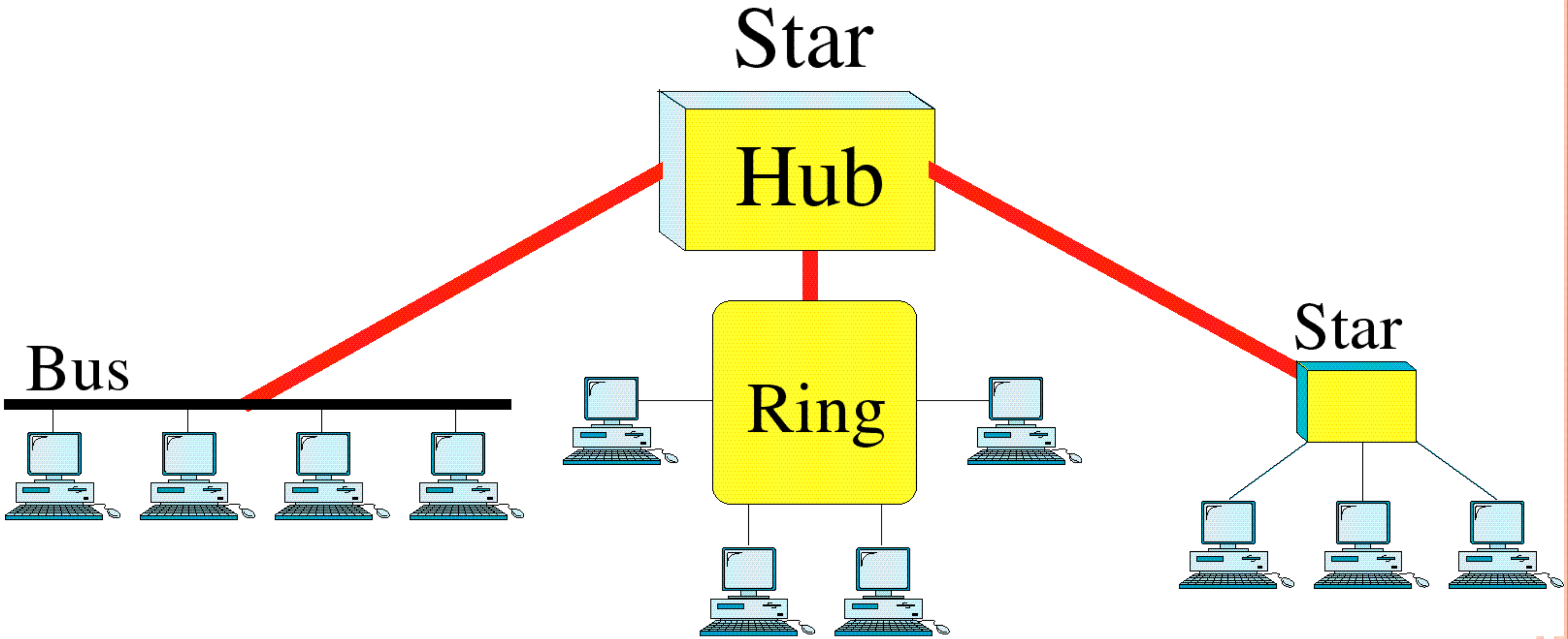
Bus Topology



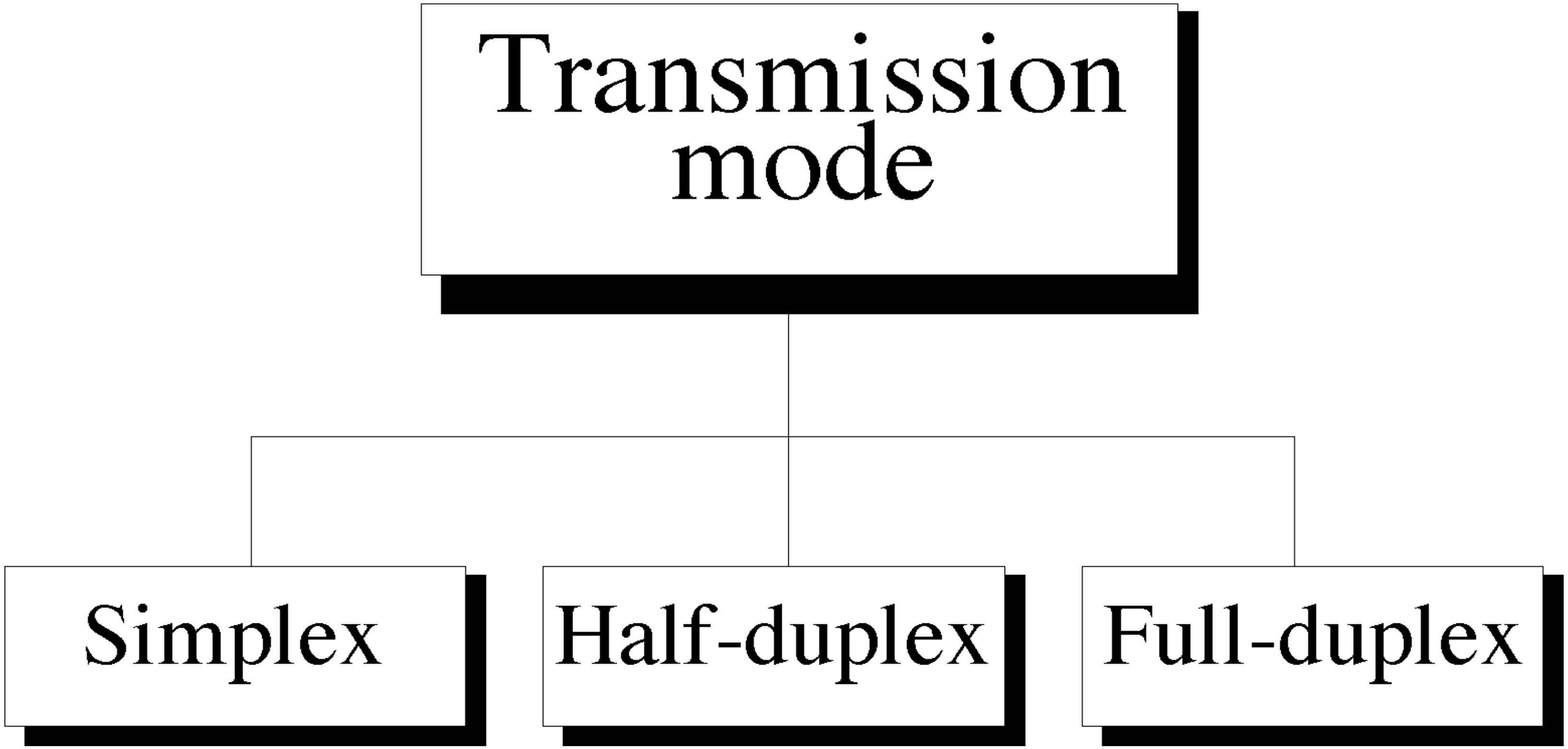
RING TOPOLOGY



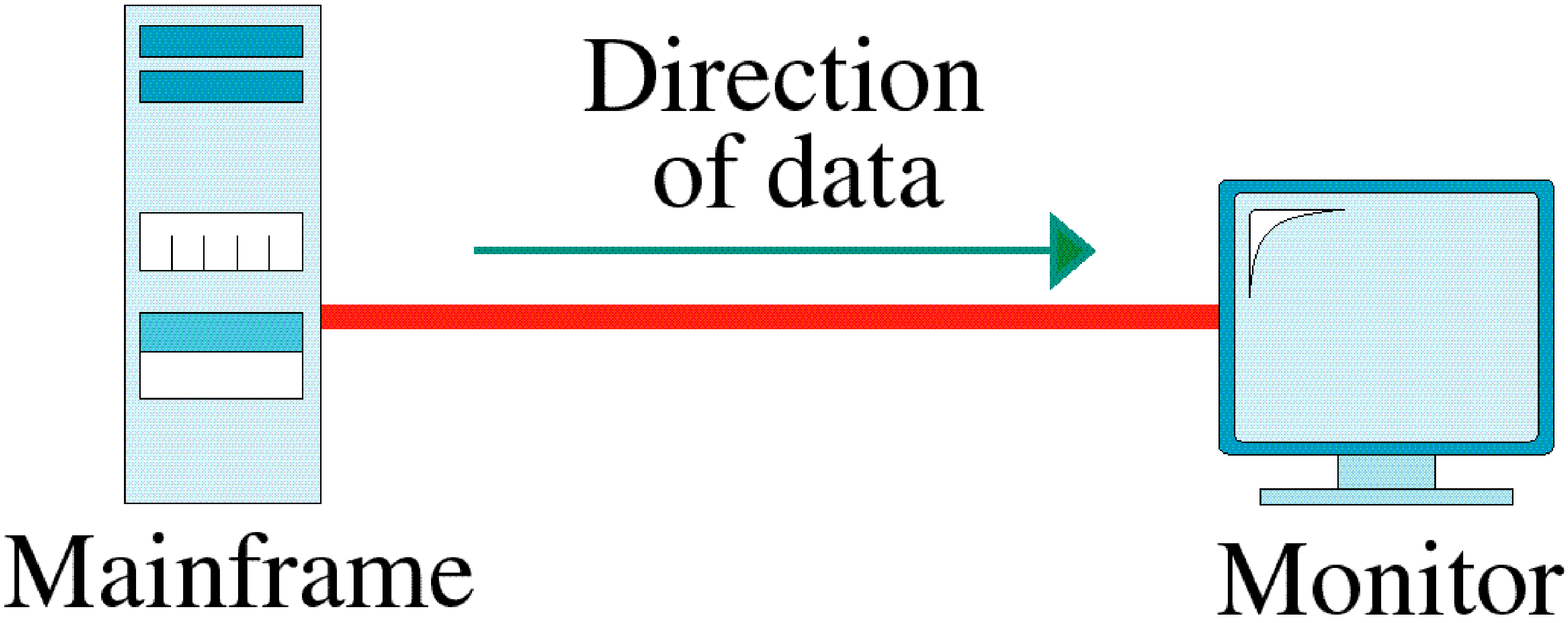
Hybrid Topology



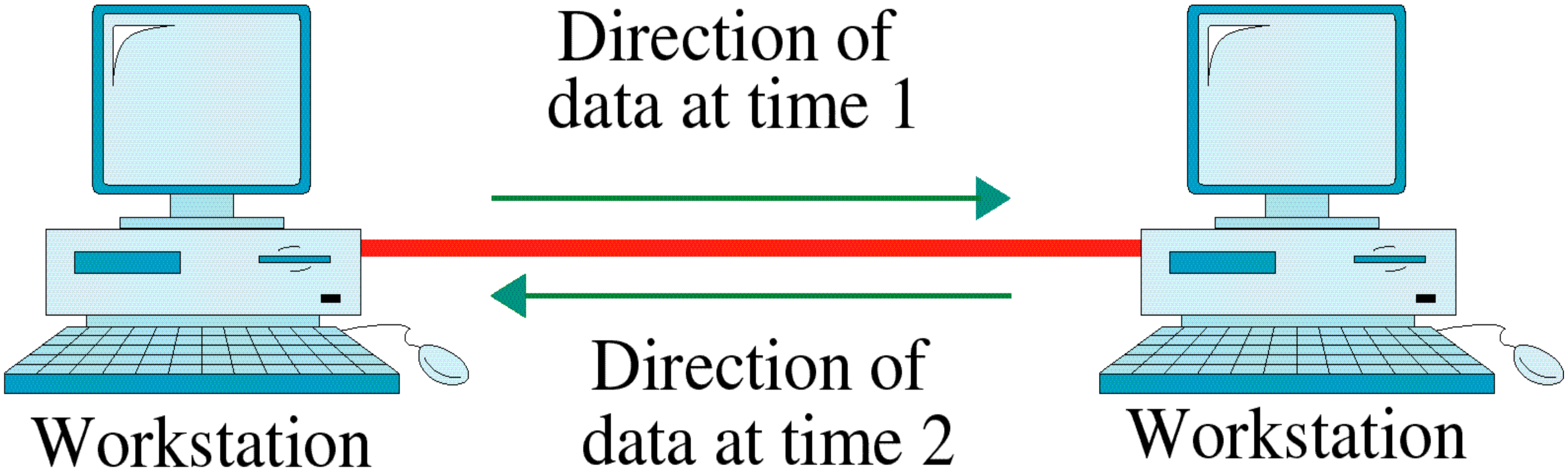
Transmission Mode



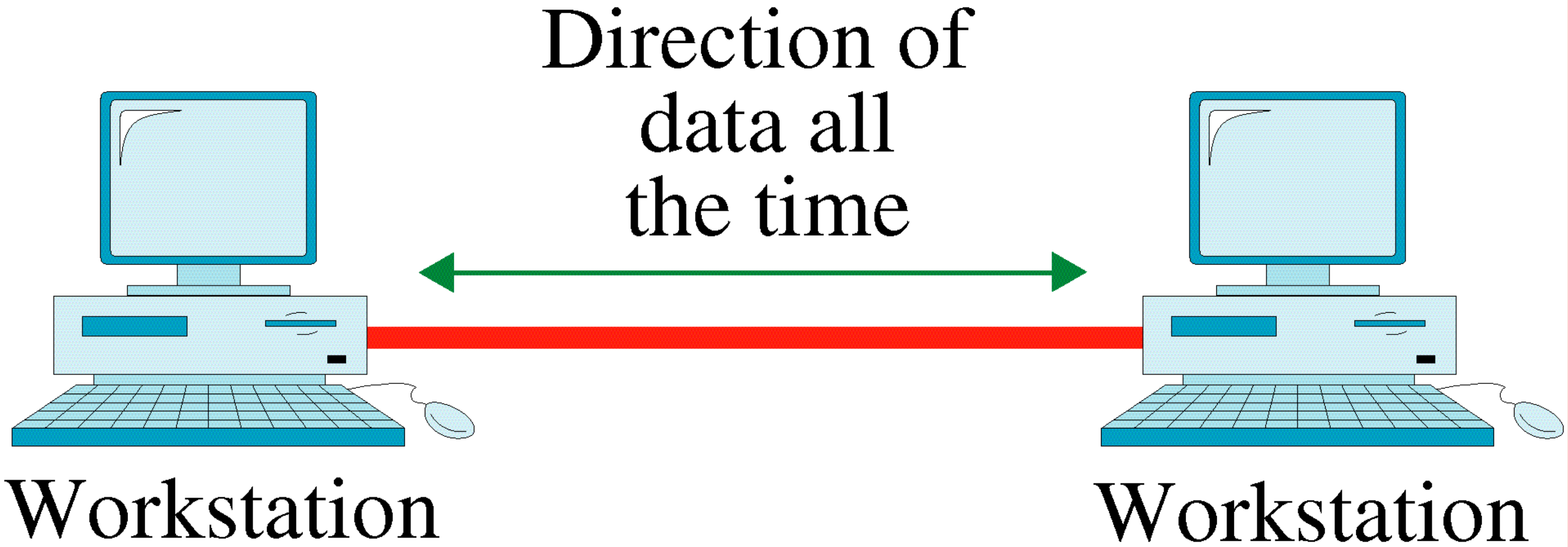
SIMPLEX



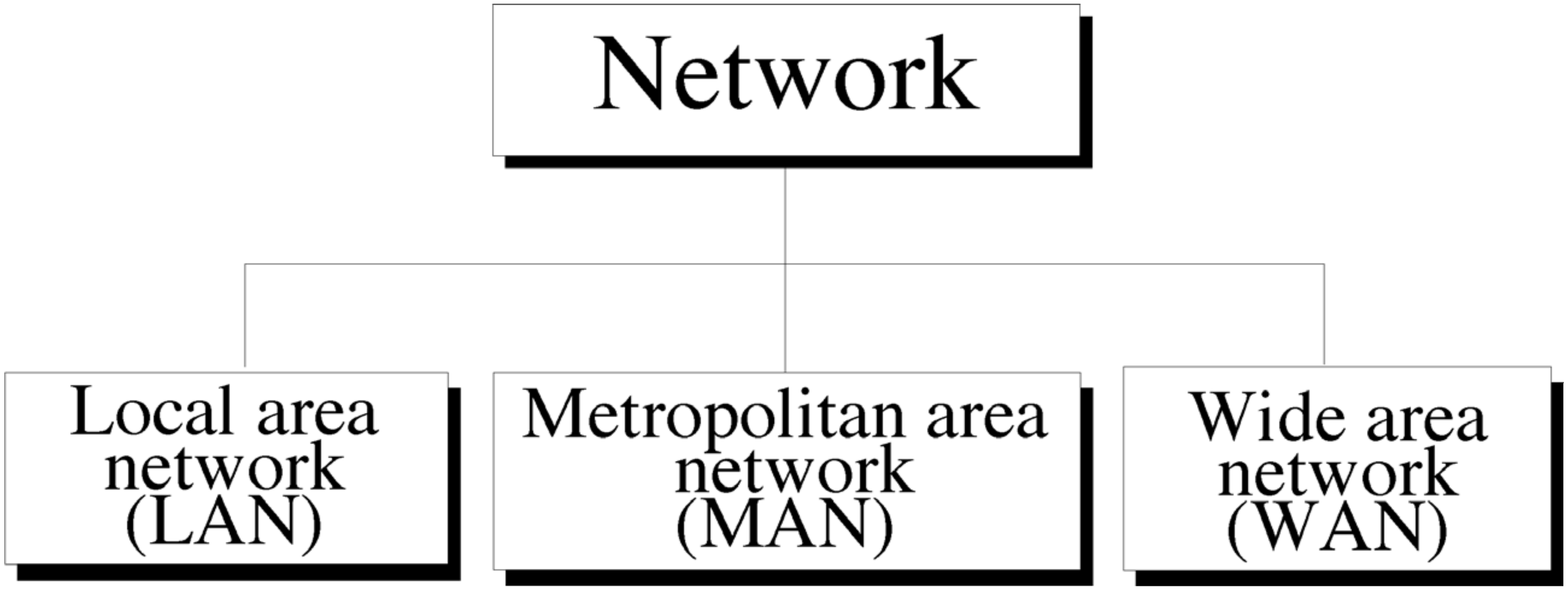
Half Duplex


Direction of
data at time 1
Direction of
data at time 2
Workstation
Workstation

Full-Duplex

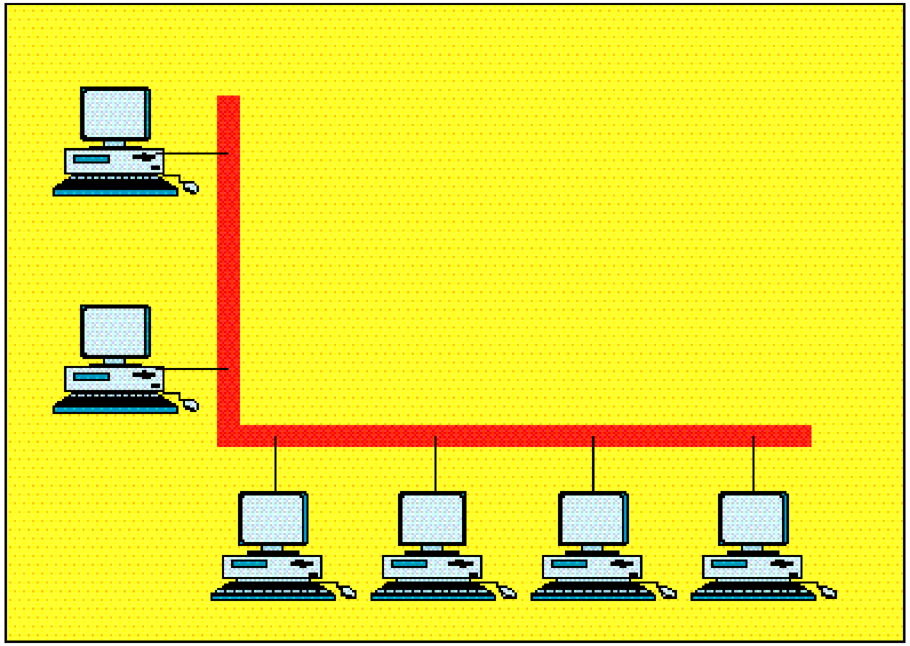


NETWORKS



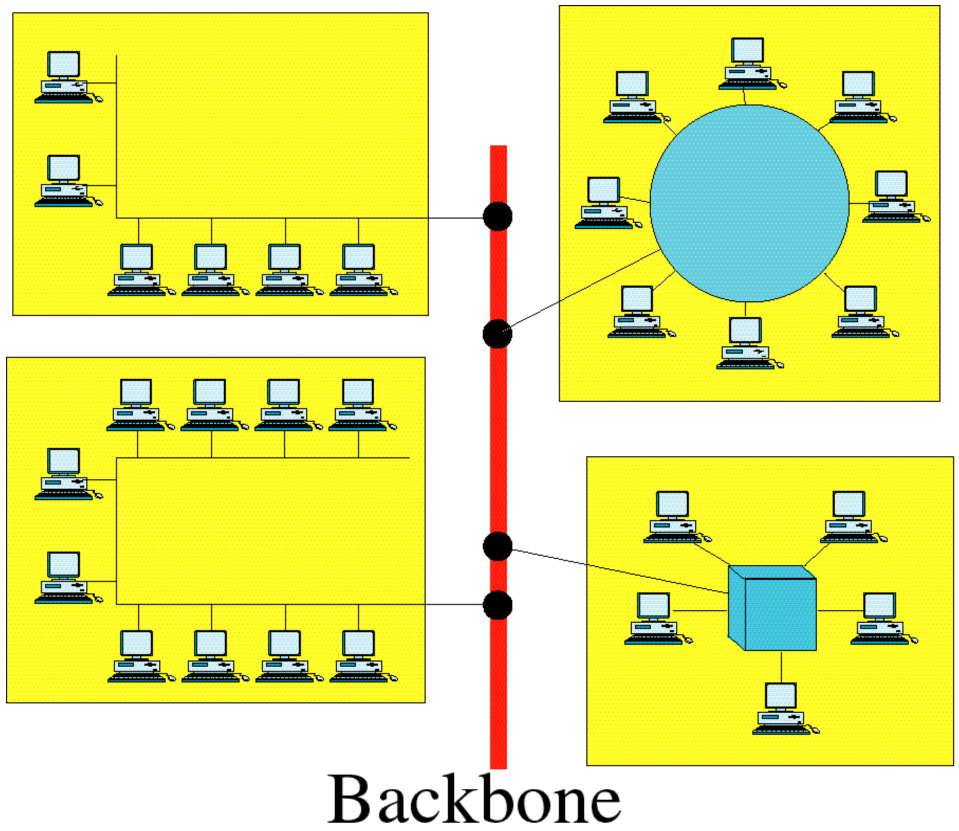
Network
Local area network (LAN)
Metropolitan area network (MAN)
Wide area network (WAN)

LOCAL AREA NETWORK



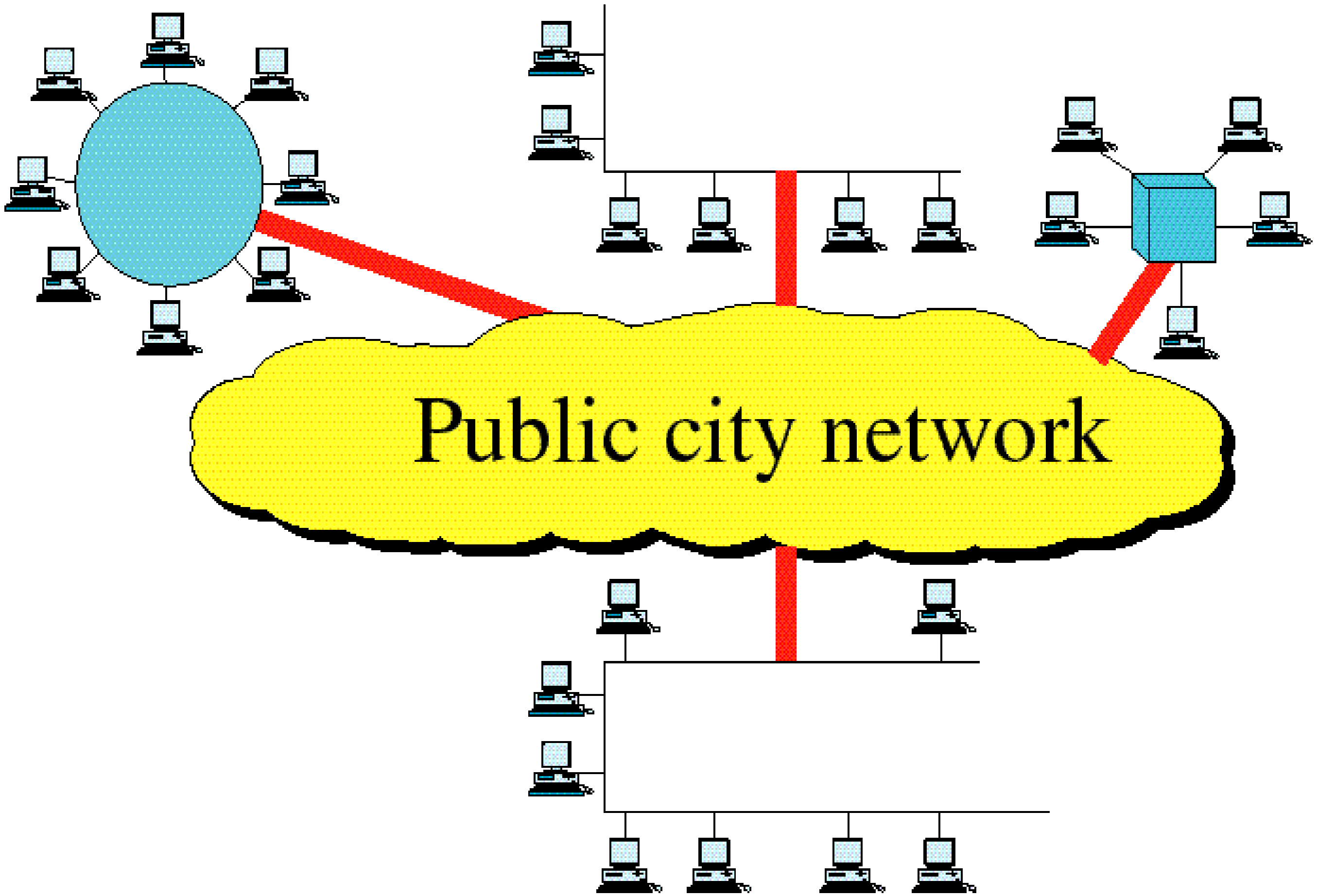
Single building LAN

Local Area Network

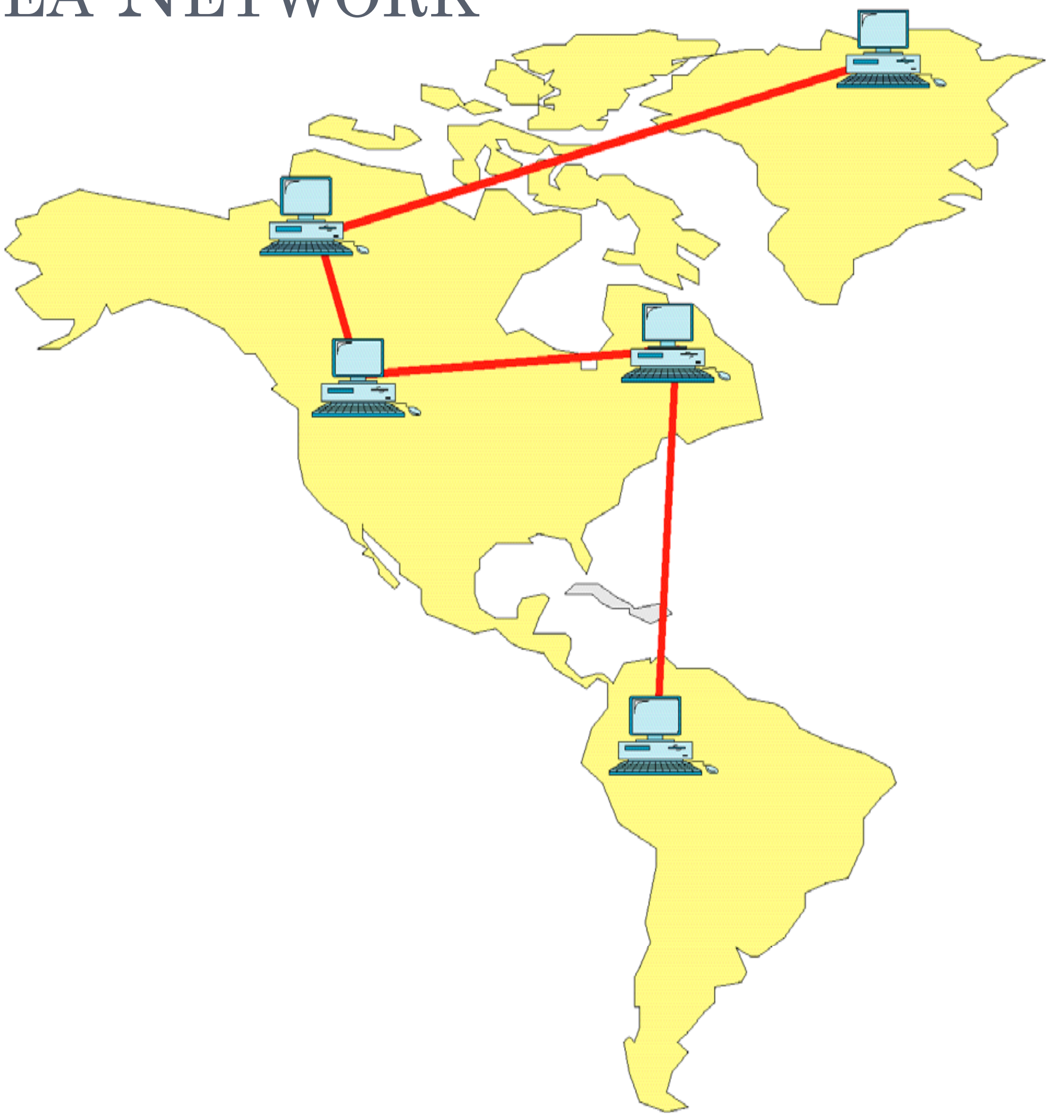


Multiple building LAN

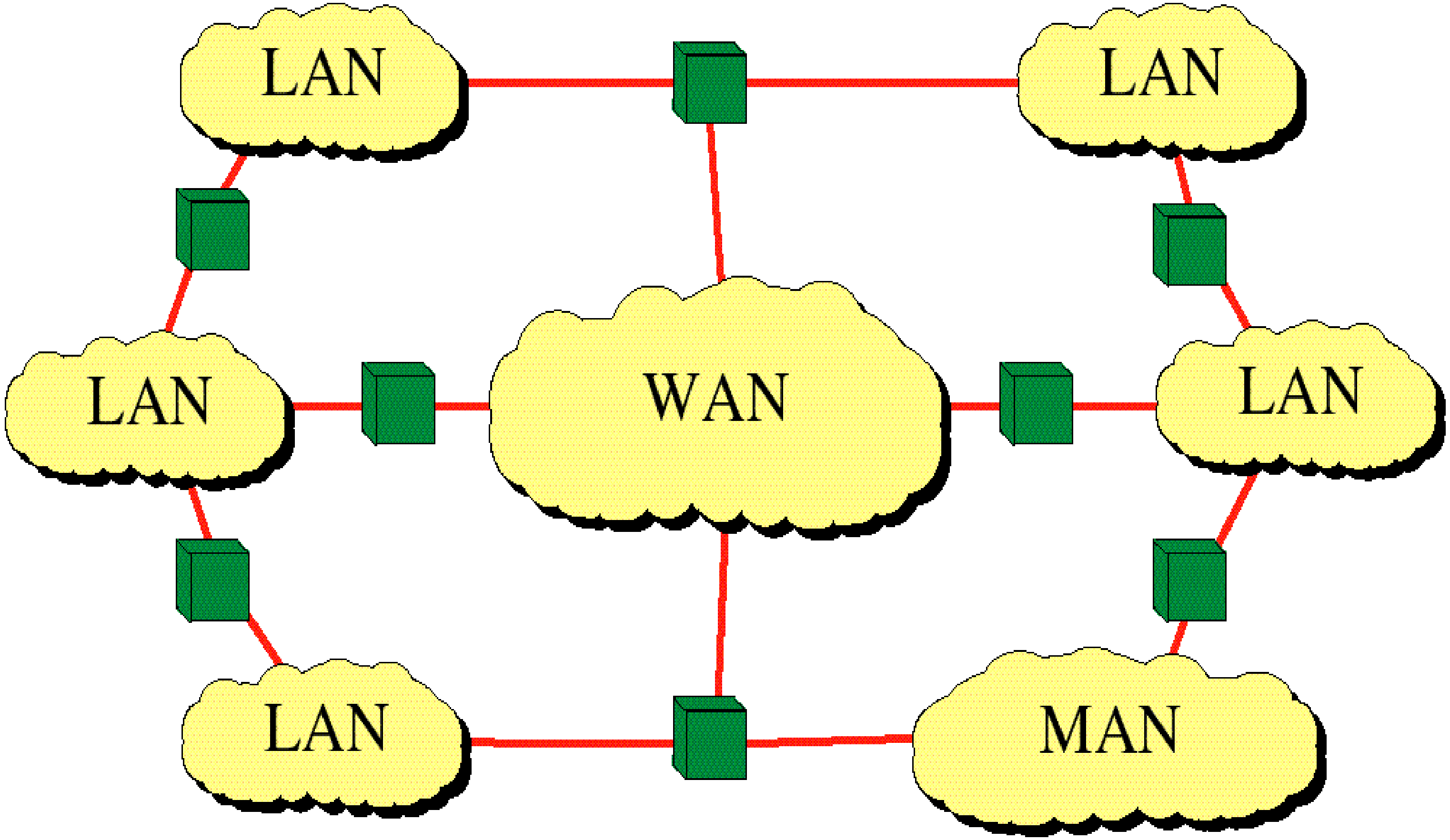
METROPOLITAN AREA NETWORK



Wide Area Network



INTERNETWORK (INTERNET)



Switching Techniques

- Circuit Switching
- Packet Switching

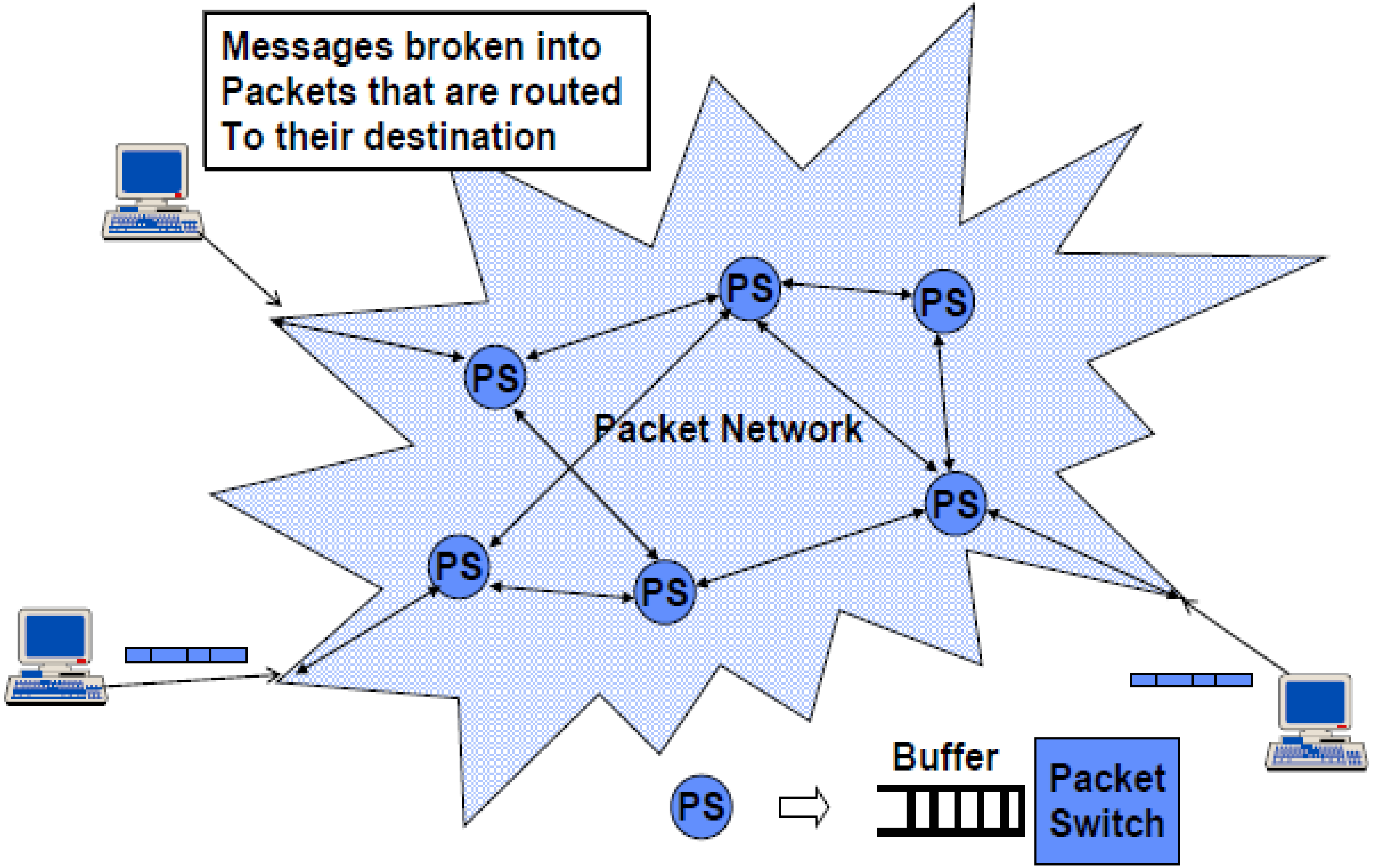
Switching Techniques

- Circuit Switching
  - Each session is allocated a fixed fraction of the capacity on each link along its path
    - Dedicated resources
    - Fixed path
    - If capacity is used, calls are blocked
      - E.g., telephone network
  - Advantages of circuit switching
    - Fixed delays
    - Guaranteed continuous delivery
  - Disadvantages
    - Circuits are not used when session is idle
    - Inefficient for bursty traffic
    - Circuit switching usually done using a fixed rate stream (e.g., 64 Kbps)
      - Difficult to support variable data rates

Problems with circuit switching

- Many data sessions are low duty factor (bursty),
  - (message transmission time)/(message interarrival time) << 1
  - Same as: (message arrival rate) * (message transmission time) << 1
- The rate allocated to the session must be large enough to meet the delay requirement. This allocated capacity is idle when the session has nothing to send
- If communication is expensive, then circuit switching is uneconomic to meet the delay requirements of bursty traffic
- Also, circuit switching requires a call set-up during which resources are not utilized. If messages are much shorter than the call set-up time then circuit switching is not economical (or even practical)
  - More of a problem in high-speed networks

Packet Switched Networks



Packet Switching

- Datagram packet switching
  - Route chosen on packet-by-packet basis
  - Different packets may follow different routes
  - Packets may arrive out of order at the destination
  - E.g., IP (The Internet Protocol)

- Virtual Circuit packet switching
  - All packets associated with a session follow the same path
  - Route is chosen at start of session
  - Packets are labelled with a VC# designating the route
  - The VC number must be unique on a given link but can change from link to link
    - Imagine having to set up connections between 1000 nodes in a mesh Unique VC numbers imply 1 Million VC numbers that must be represented and stored at each node
  - E.g., ATM (Asynchronous transfer mode)

Packet Switching

- Advantages of packet switching
  - Efficient for bursty data
  - Easy to provide bandwidth on demand with variable rates

- Disadvantages of packet switching
  - Variable delays
  - Difficult to provide QoS assurances (Best-effort service)
  - Packets can arrive out-of-order

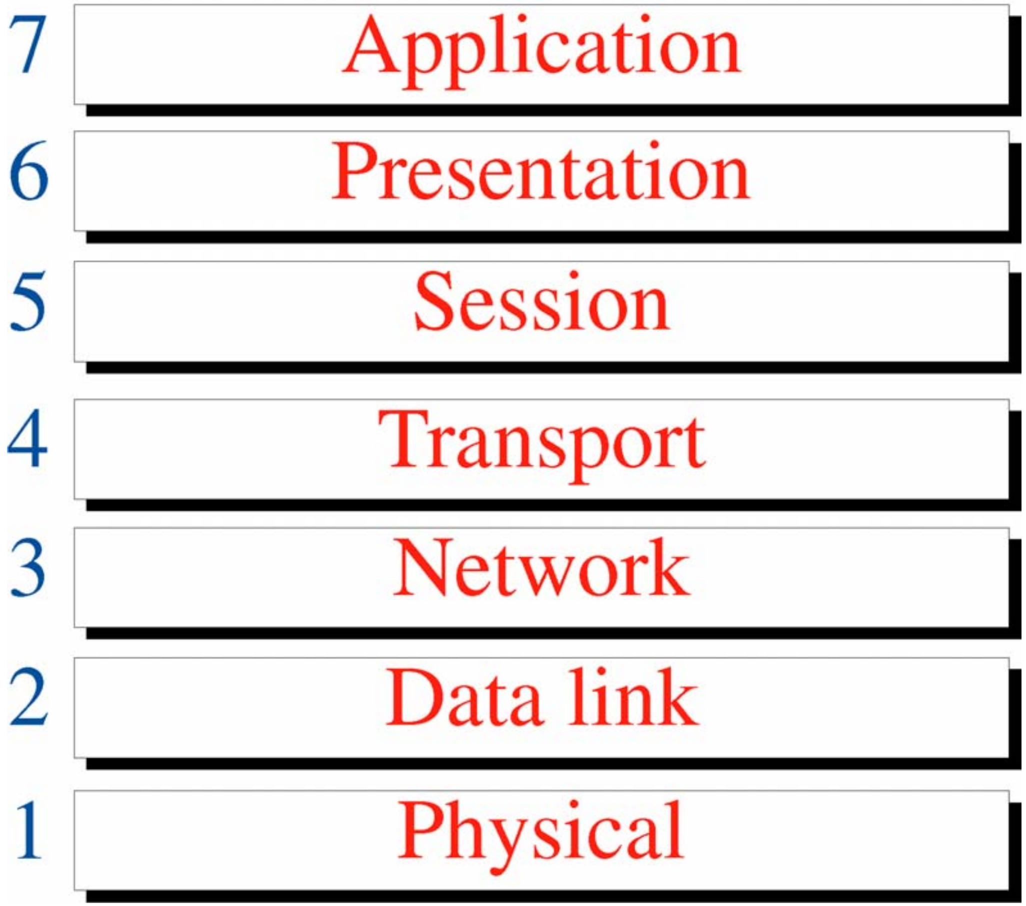
OSI Model

- The model
- Functions of the layers

What is the OSI Model

- OSI: Open Systems Interconnection.
- The OSI model is a layered, abstract description of communications and computer network protocol design.
- OSI model is a set of standards specifications that allows various computer platforms to communicate with each other.
- It is concerned with the interconnection between systems – the way the systems exchange information – and not with the internal function of a particular system.

OSI MODEL

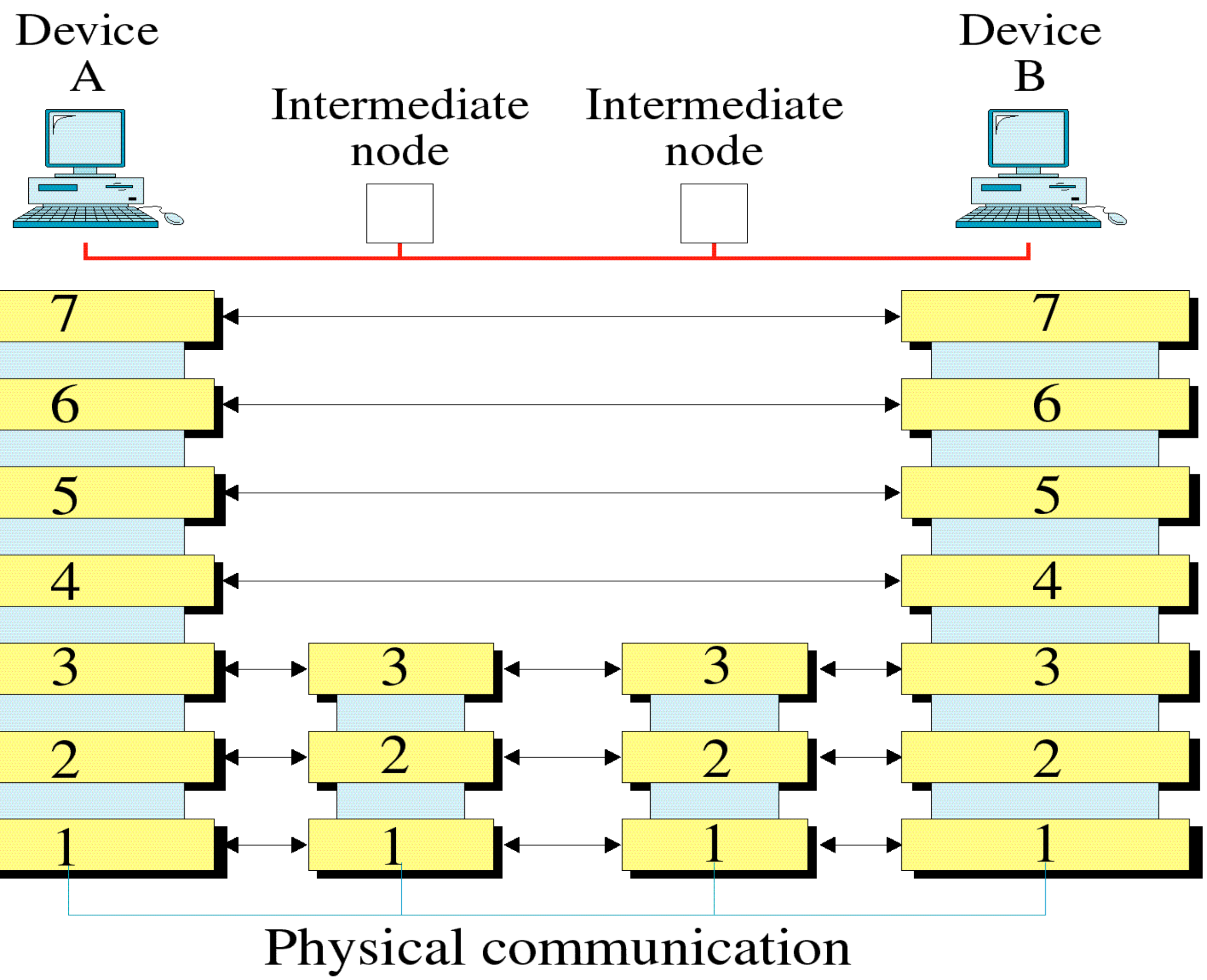


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data link
1 Physical

Advantages of a layered model

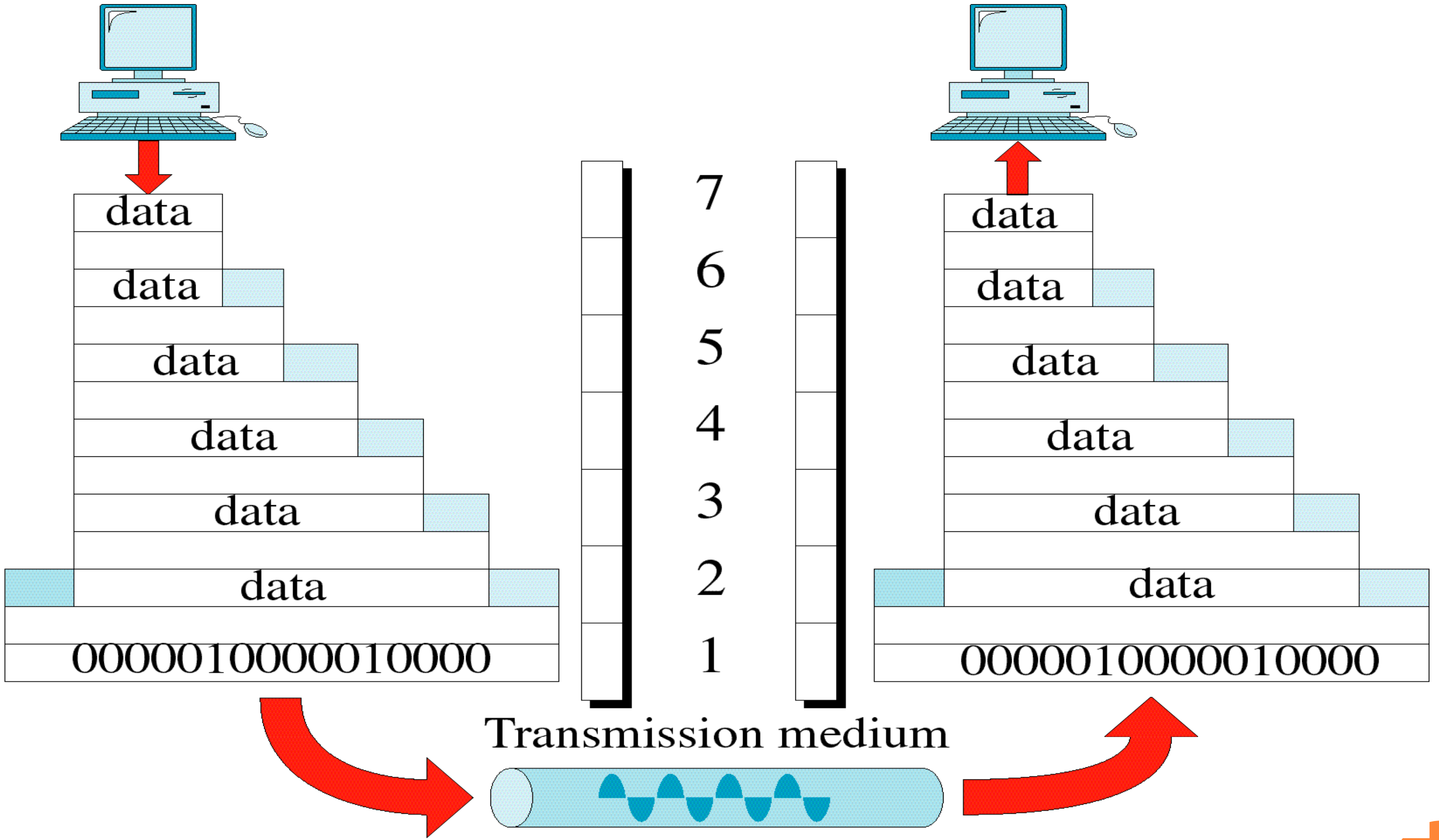
- Change: Changes made to one layer doesn't affect other layers.
- Design: A layered model defines each layer separately. As long as the interconnections between layers are not altered, a protocol designers can specialize in one layer without worrying about other layers.
- Learning: It reduces complexity and simplifies the learning and understanding of each layer.
- Troubleshooting: helps in troubleshooting.
- Standards: It establishes a prescribed guideline for interoperability between various vendors developing products that perform difference data communication tasks.
  - OSI model only provides a guideline and framework… and not a rigid standards fro the manufacturers.

OSI Layers

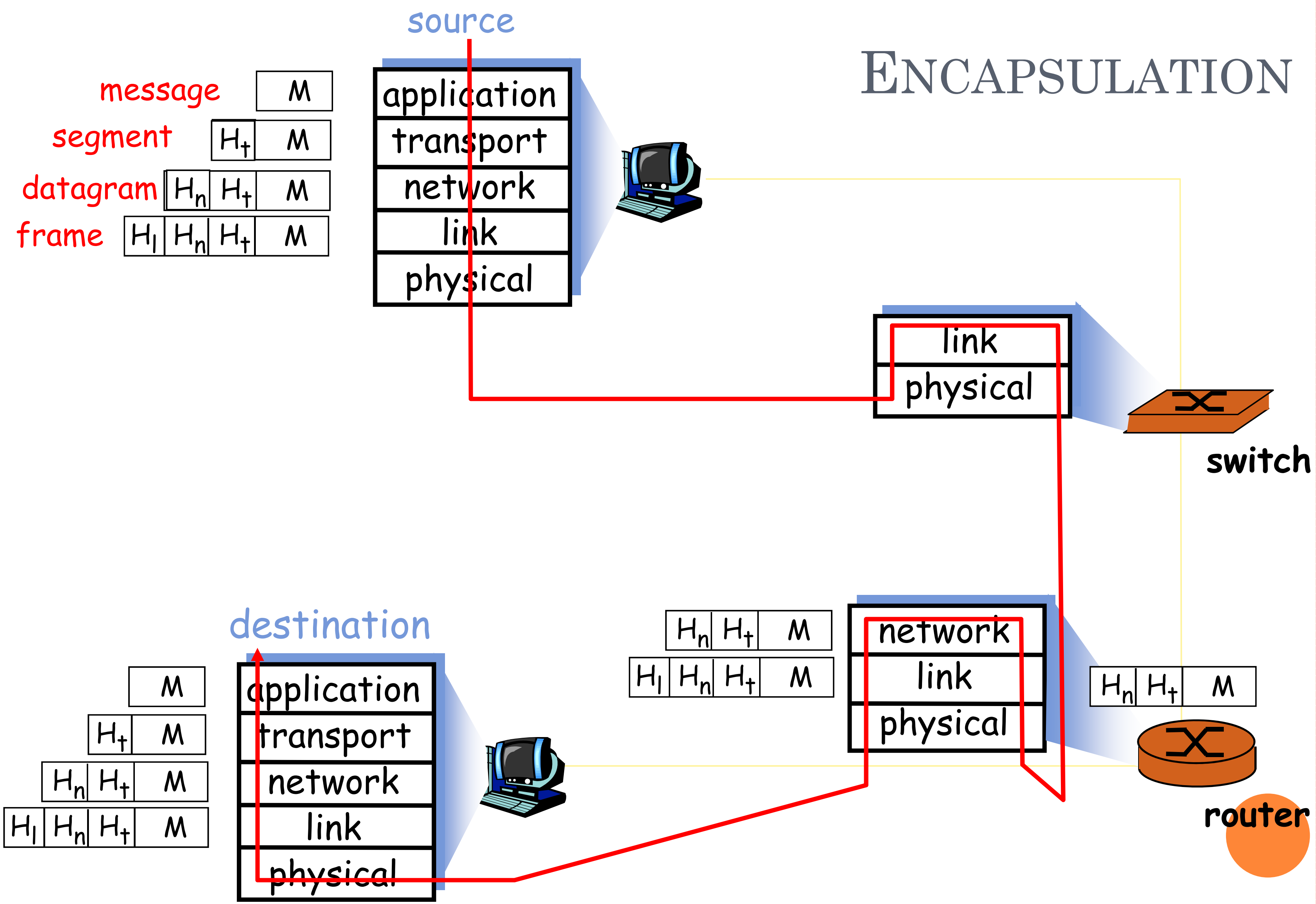


Device A
Intermediate node
Intermediate node
Device B
7
7
6
6
5
5
4
4
3
3
3
3
2
2
2
2
1
1
1
1
Physical communication

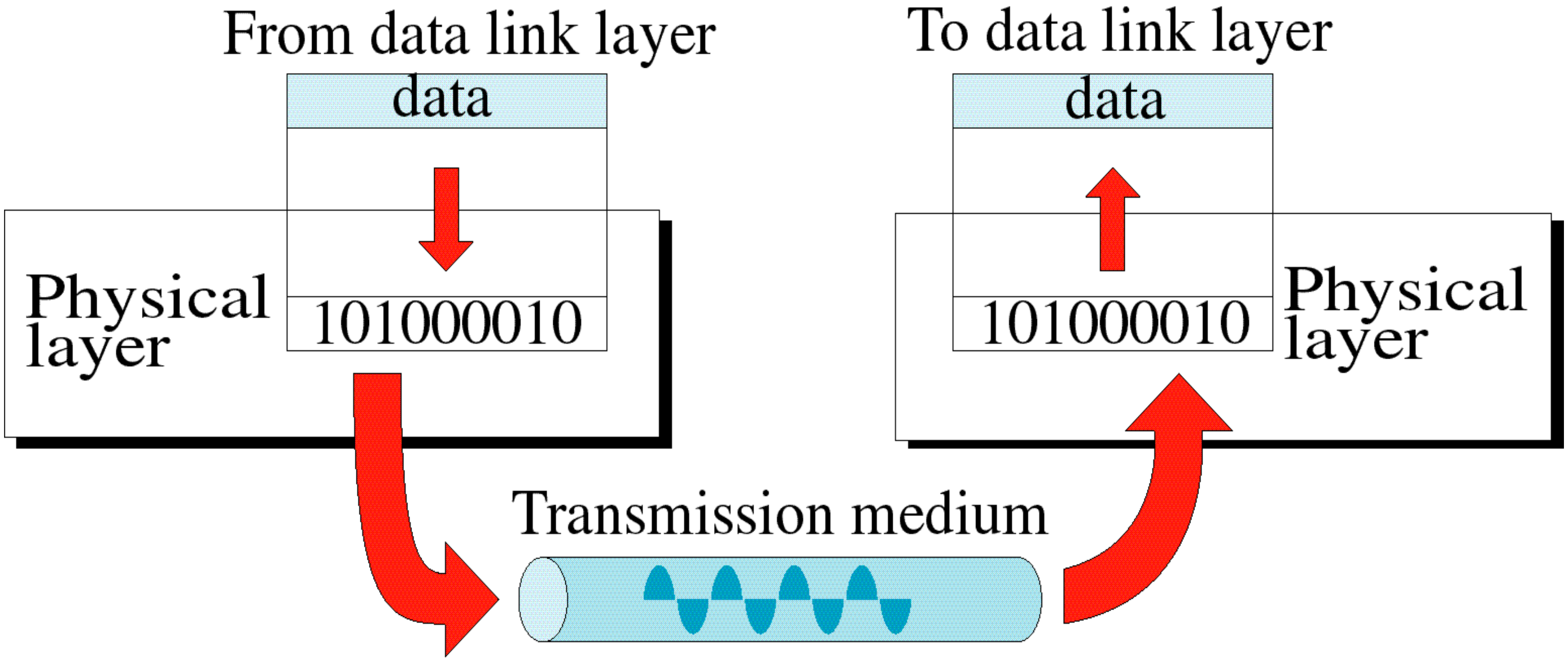
An Exchange Using the OSI Model



ENCAPSULATION



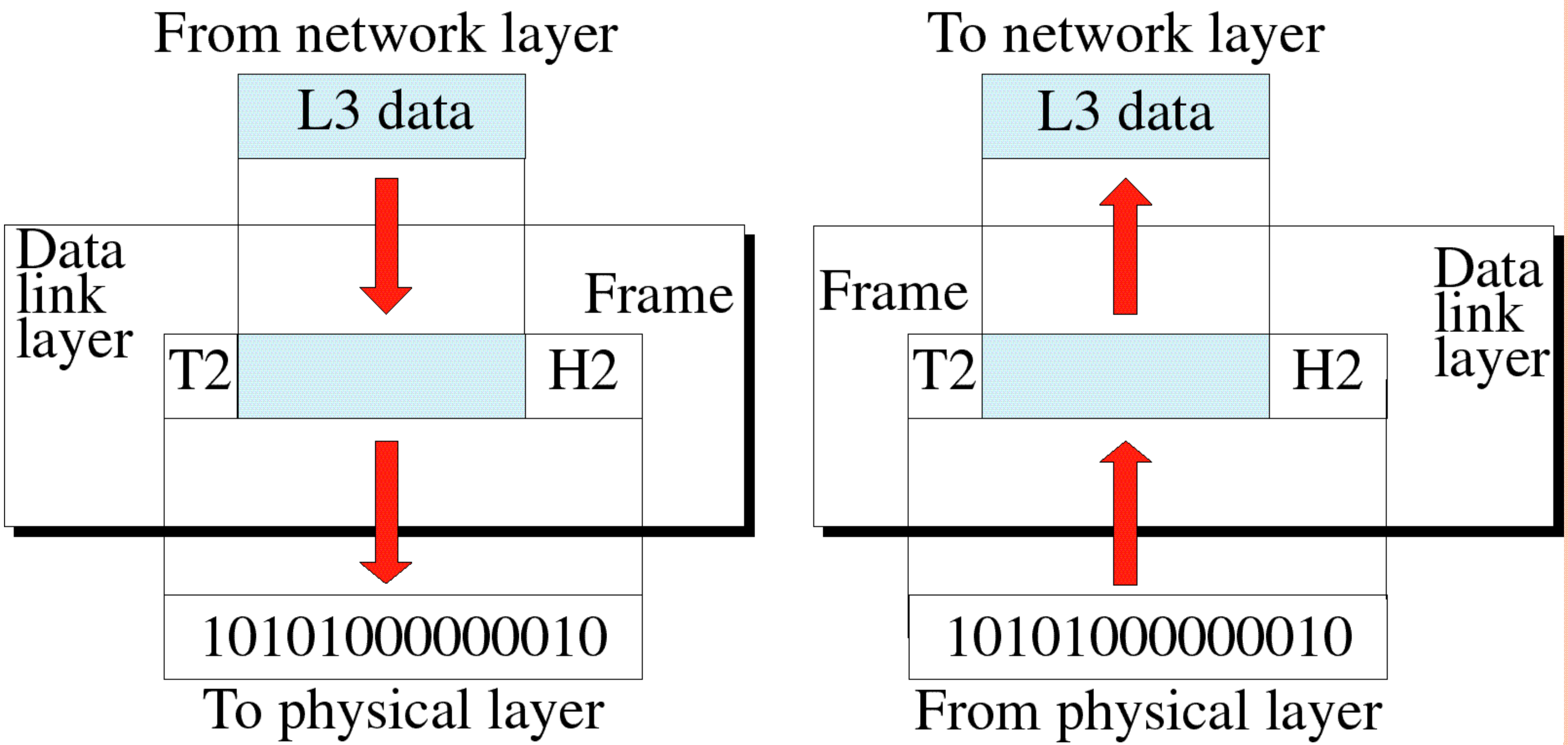
PHYSICAL LAYER



Responsibilities of Physical Layer

- Physical Characteristic of the medium
  - Types of transmission medium.
  - The char of the interface between devices and the transmission medium.
- Representation of the bits
  - For transmitting a stream of bits, it must be encoded into electrical/optical signals.
- Data rate
  - The number of bits sent each second. Duration of a bit.
- Synchronization of bits
  - The clocks of sender and receiver must be synchronized.
- Line configuration
  - Connection of the device to the medium – point-to-point or multipoint configuration.
- Physical topology
  - How devices are connected to the network – bus, star, Ring.
- Transmission mode
  - Simplex, half duplex, full duplex

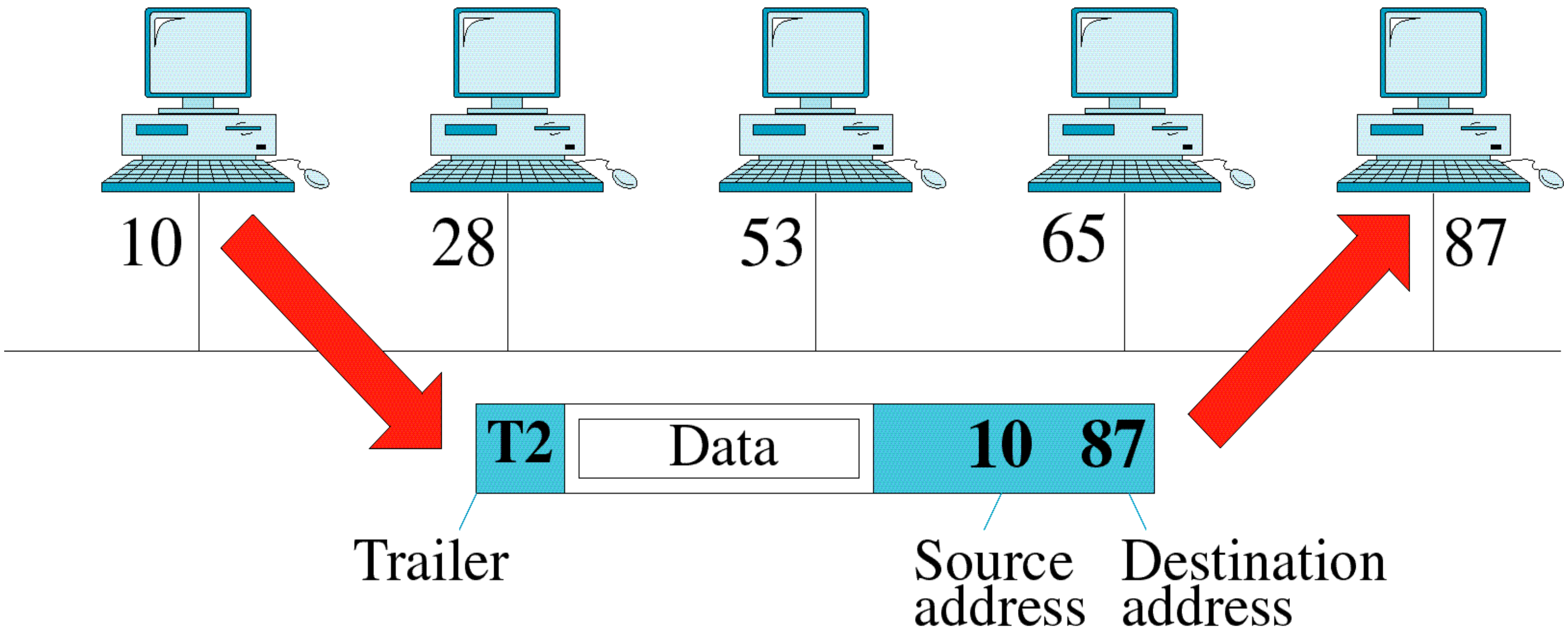
DATA LINK LAYER



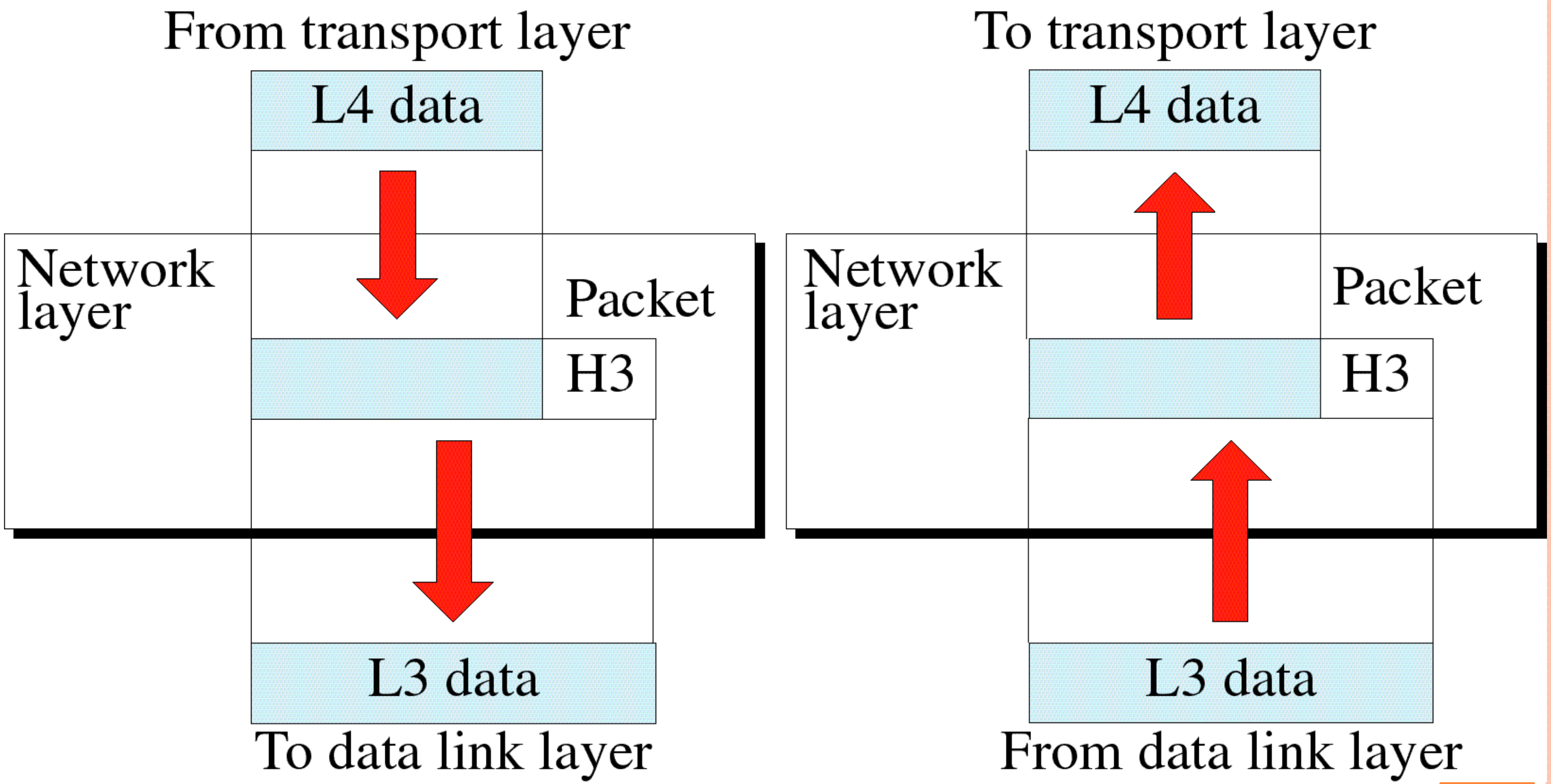
Responsibilities of Data Link Layer

- Framing – DLL divides the stream of bits received from the network layer into manageable data units called frames.
- Physical Addressing – DLL adds a header to the frames to define the physical address of the sender (source address) and receiver (destination address) nodes, if they are in same network. If the destination is in some other network, the receiver address is the address of the device connecting one network to the next.
- Flow Control – control the rate at which the data is produced by the sender and consumed by the receiver.
- Error Control – detects and retransmits damaged/lost frames. DDL adds a trailer to the end of a frame for error control.
- Access Control – If a link is shared by multiple devices, DDL determines which device has control over the link at any given time.

Data Link Layer Example



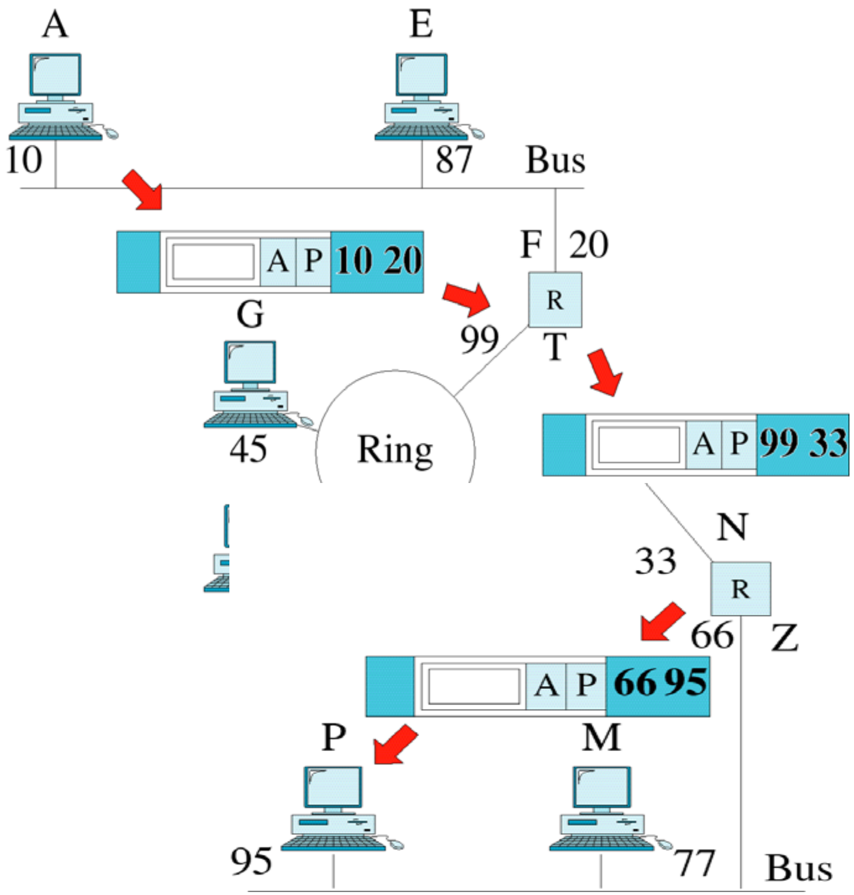
NETWORK LAYER



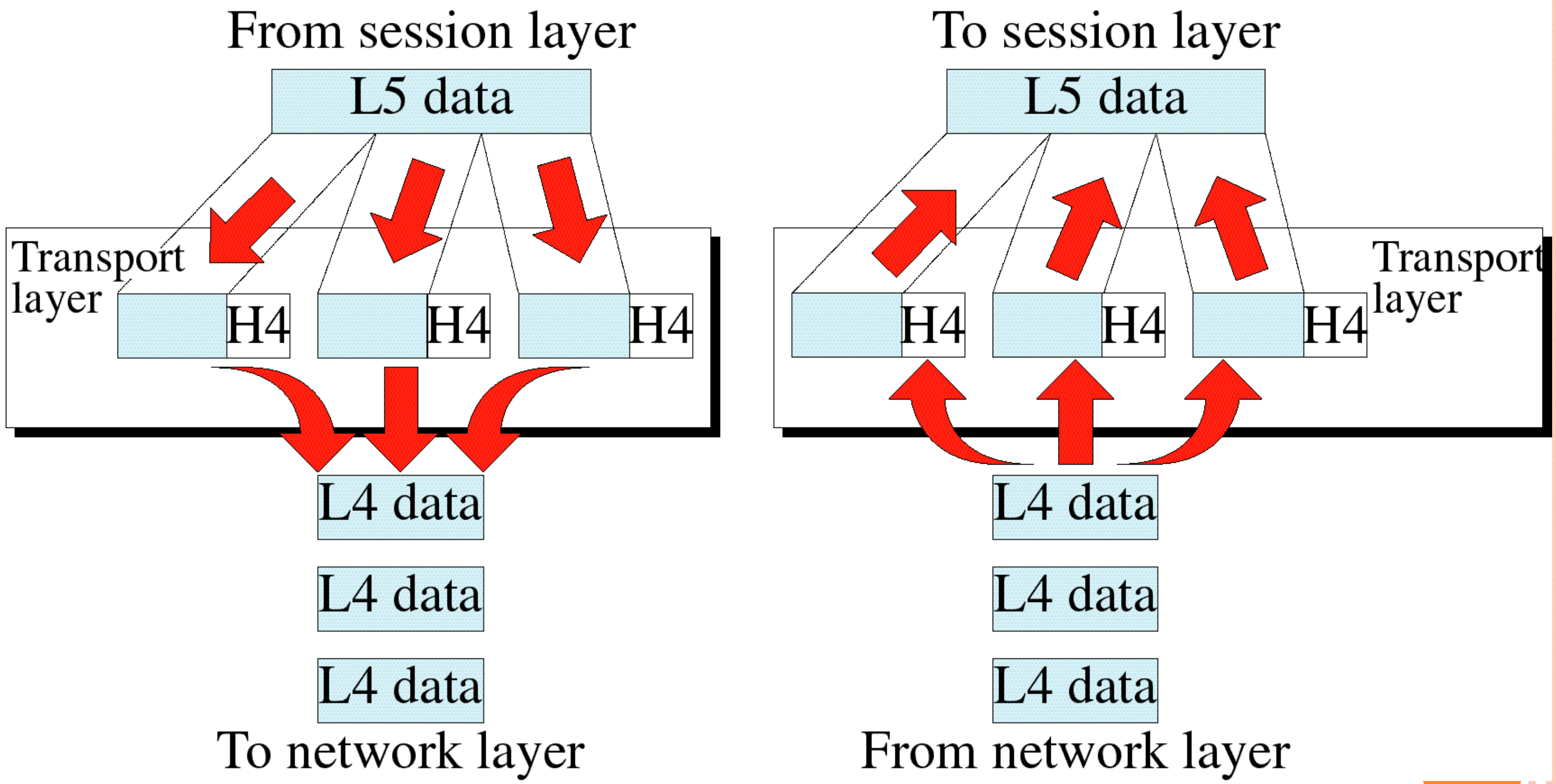
RESPONSIBILITIES OF NETWORK LAYER

- Logical Addressing
  - NL adds a header to include the logical address of the sender and receiver.
  - Used for routing between different networks.
- Routing
  - Routing of packets between networks.

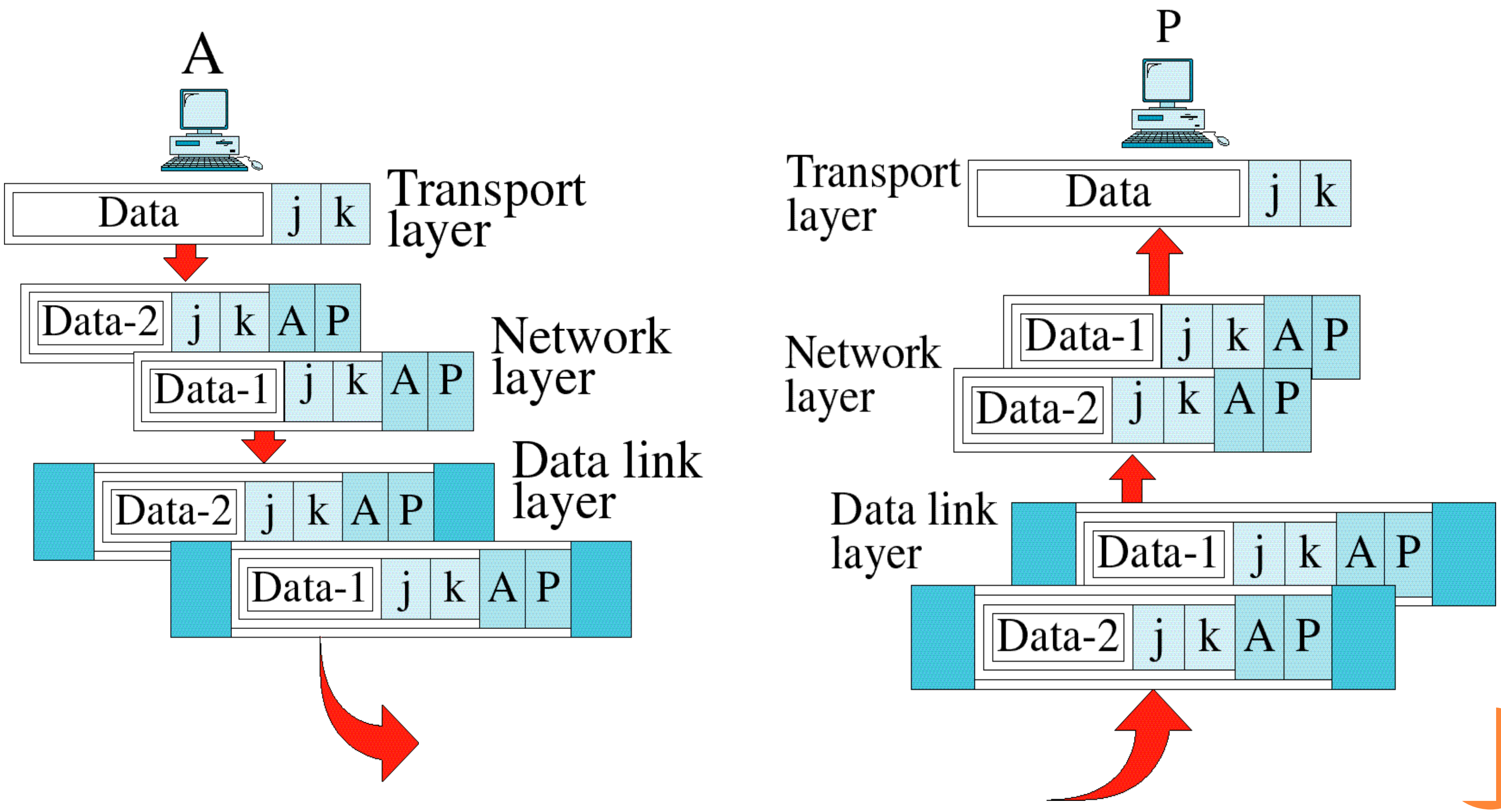
Network Layer Example



Transport Layer



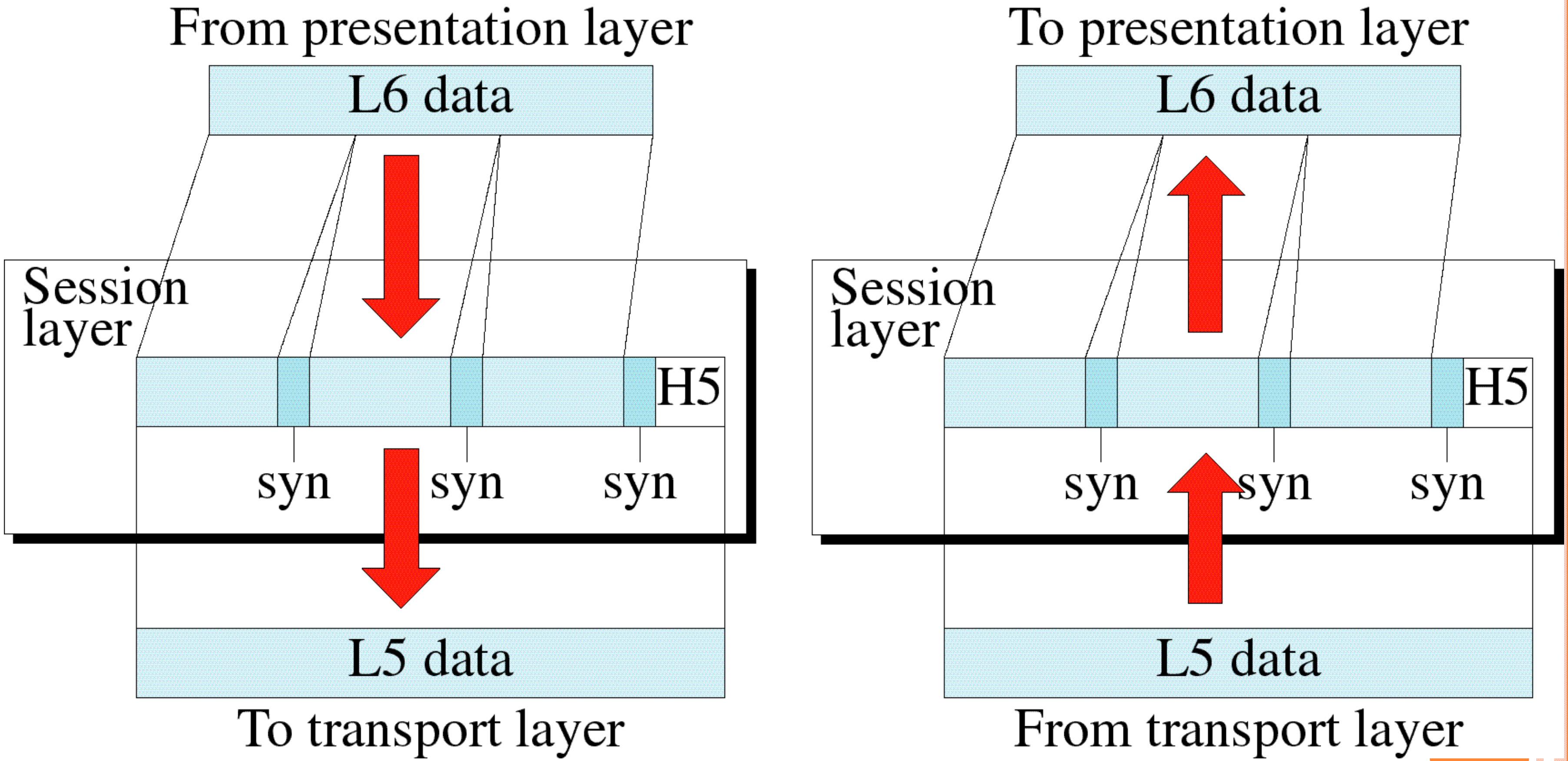
Transport Layer Example



RESPONSIBILITIES OF TRANSPORT LAYER

- Service point addressing
  - Port address of running processes on source and destination machines.
- Segmentation and reassembly
  - On sender side, a massage is divided into segments and a sequence number is added. At destination, the TL reassembles the segments.
- Connection control
  - TL can be either connection oriented or connectionless.
- Flow control
  - Flow control at TL is performed end-to-end rather than across a single link as in DLL.
- Error control
  - End-to-end error control.

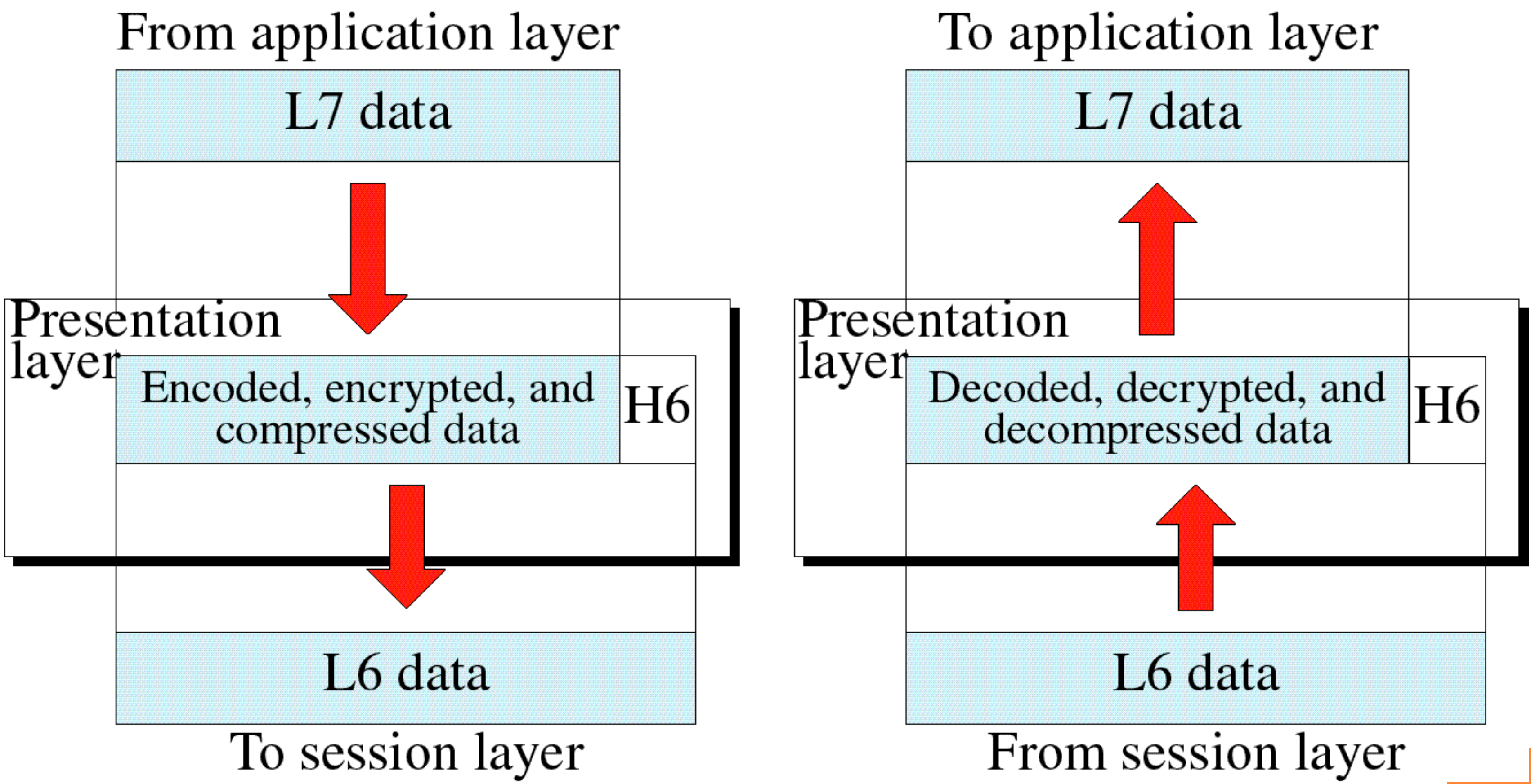
SESSION LAYER



Responsibilities of Session Layer

- Establishes and maintains communication between two nodes.
- Synchronization: The session layer allows a process to add checkpoints (synchronization points) into a stream of data.
- If a commination session breaks, SL determines where to restart the transmission once the session is established.
- This layer is responsible for determining the terms of the communication session – it will determine with computer can communicate first and for how long.

Presentation Layer



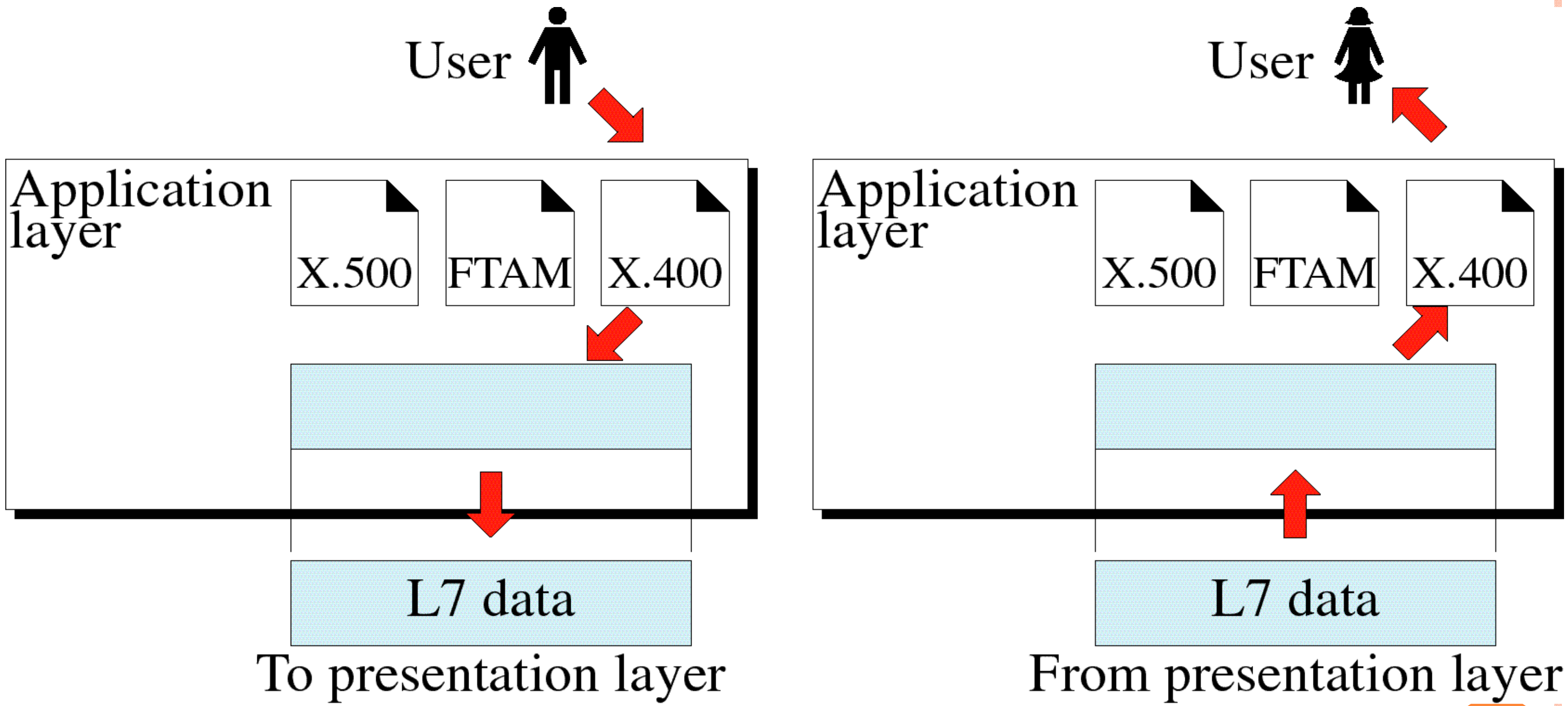
Responsibilities of Presentation Layer

- Serves as a translator between the application and the network. Data from the application layer gets changed to a bit stream before transmitting.

- Encryption: Used to assure privacy.

- Compression: reduces the size of the file to be transmitted.

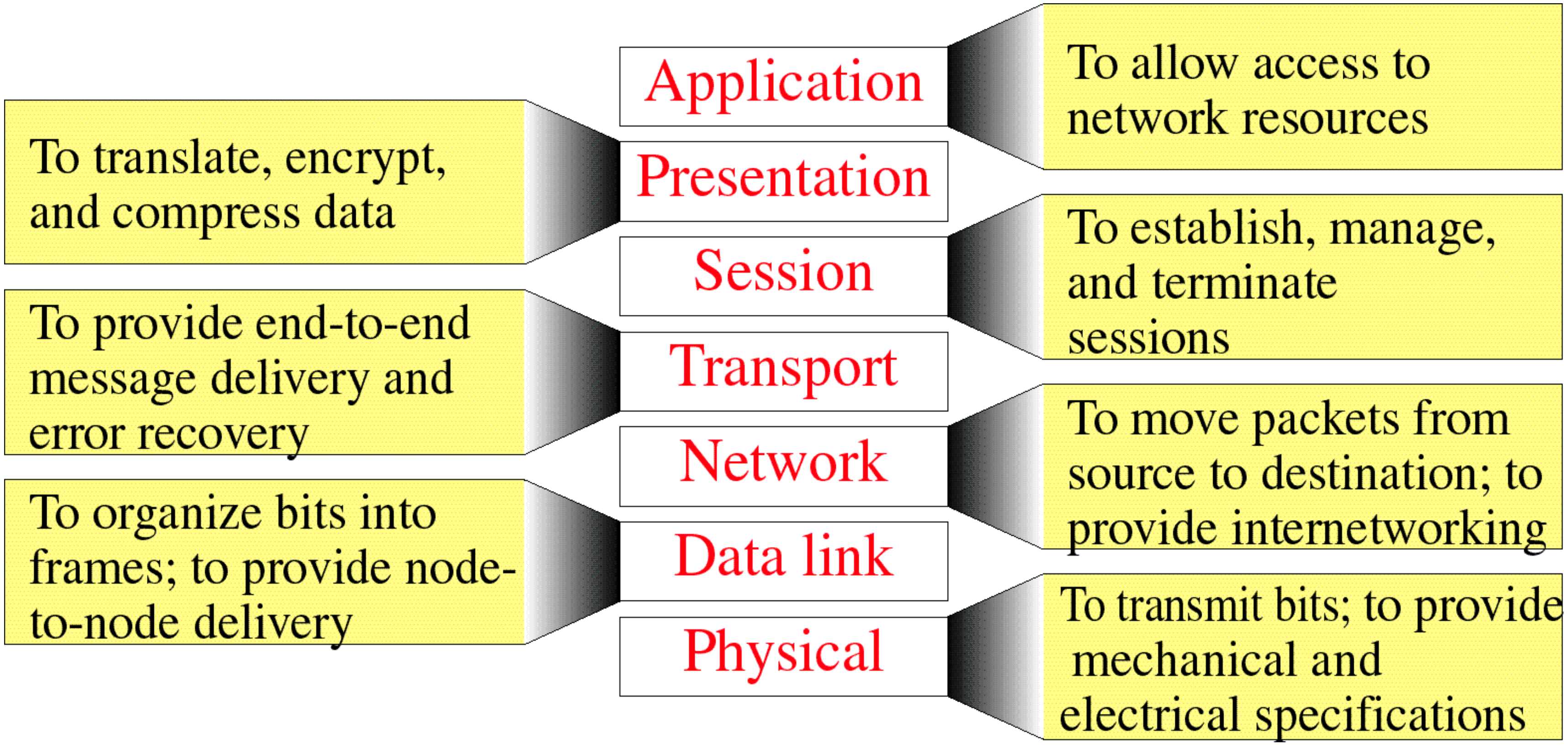
Application Layer



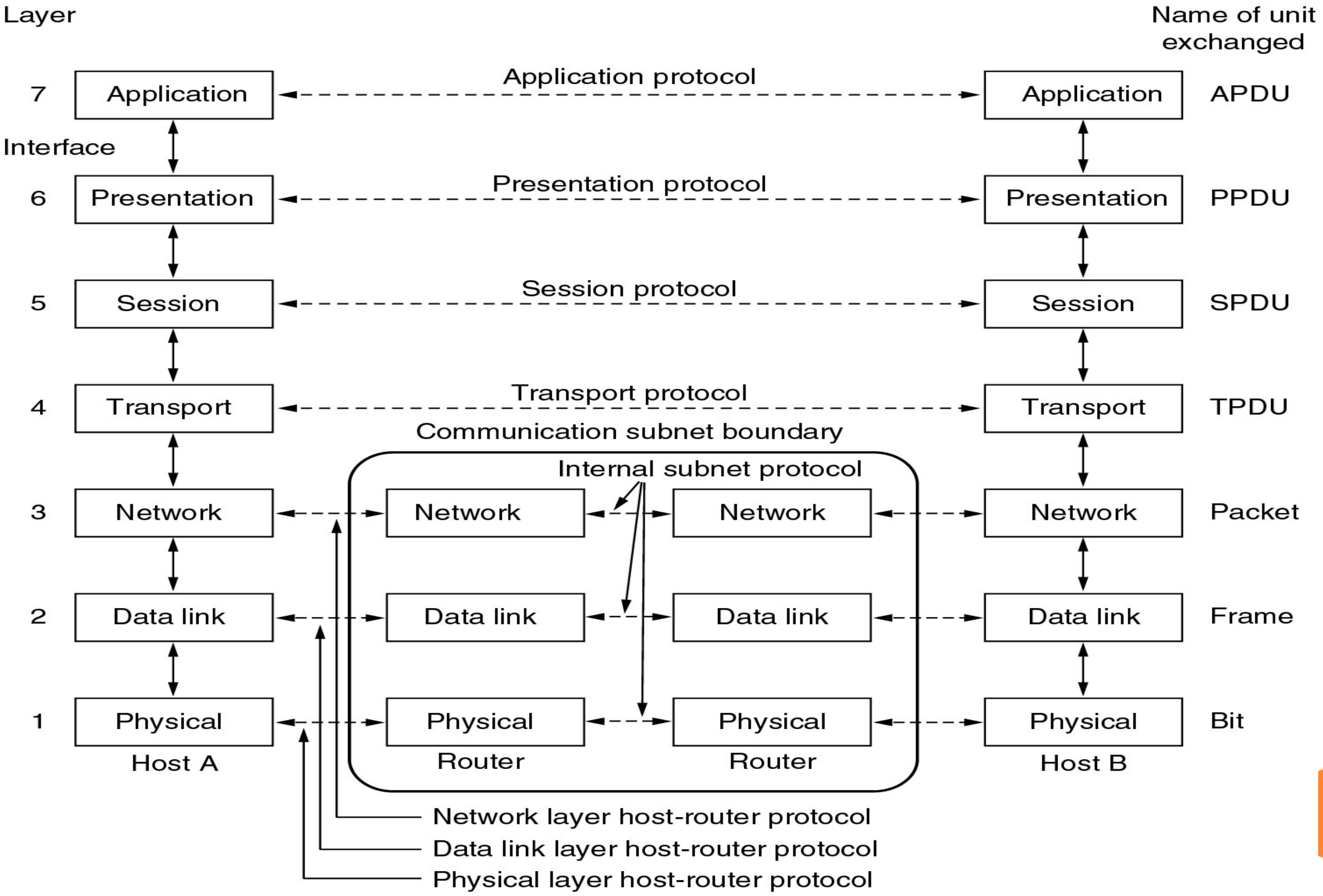
Responsibilities of Application Layer

- No header or trailer are added at this layer.
- Mail services
- File transfer, access and management (FTAM)
- Web services
- …

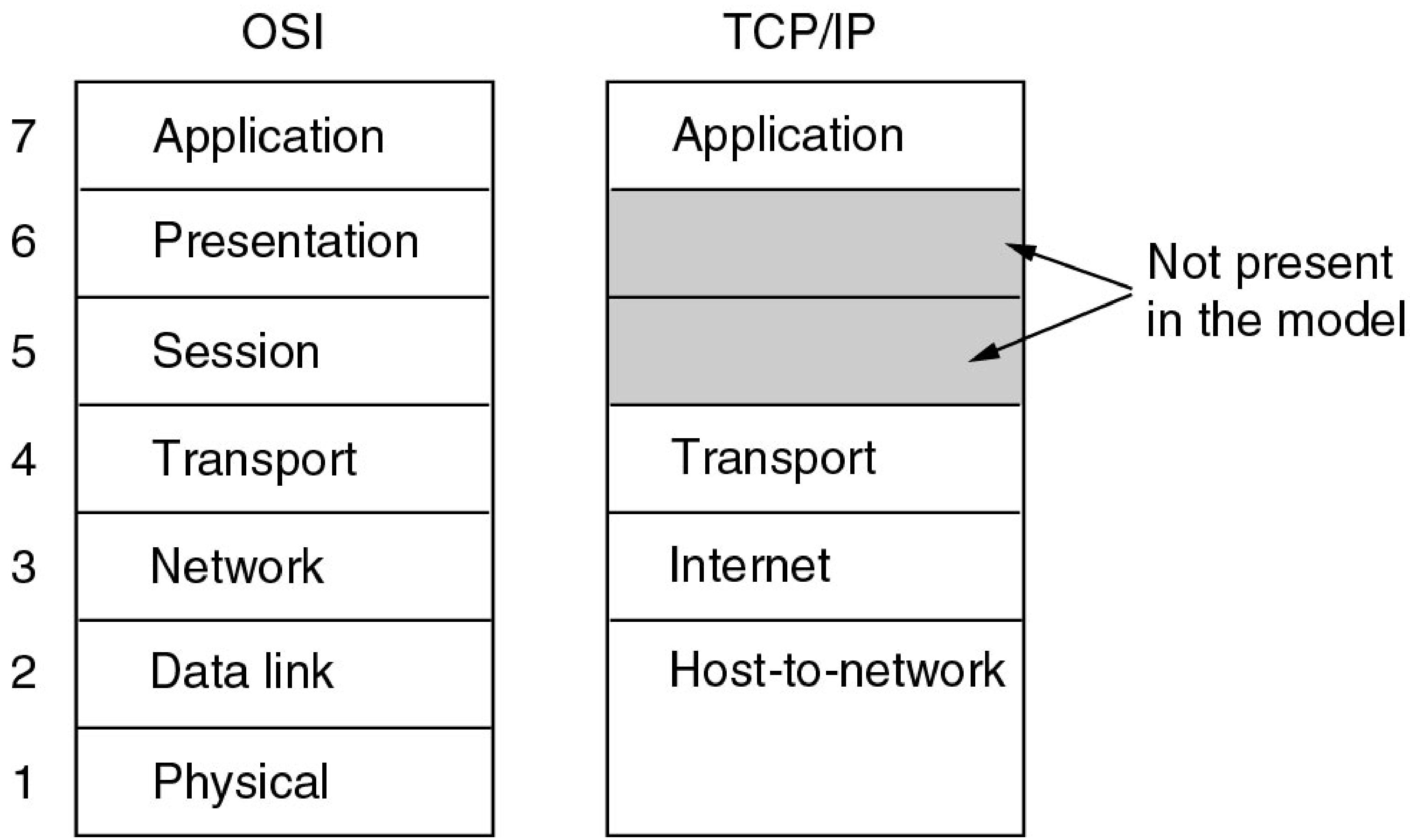
Summary of Layer Functions



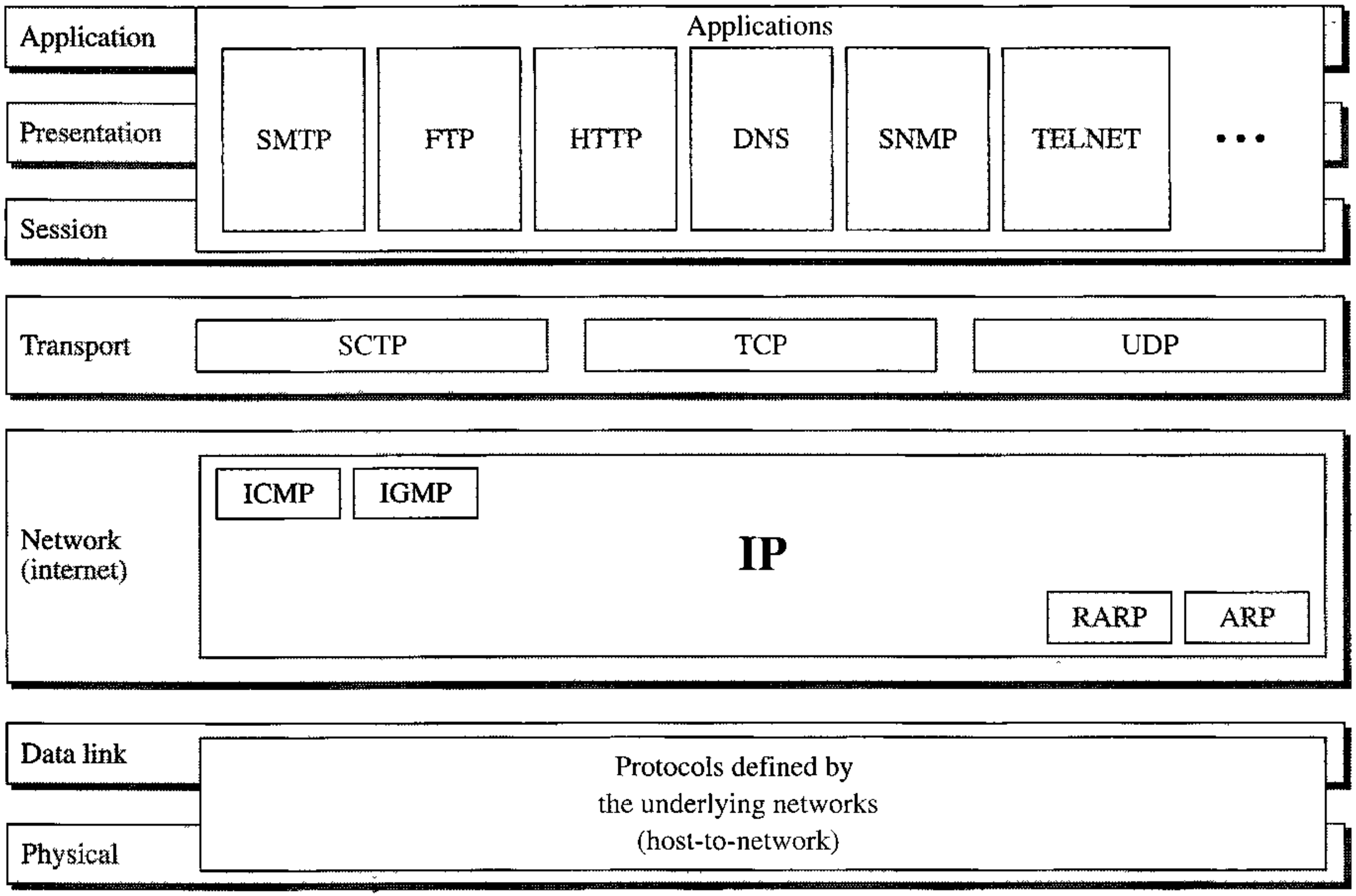
OSI Reference Model



TCP/IP Reference Model



TCP/IP Reference Model



NETWORK SECURITY

- The field of network security is about:
  - how bad guys can attack computer networks
  - how we can defend networks against attacks
  - how to design architectures that are immune to attacks

- Internet not originally designed with (much) security in mind
  - *original vision:* "a group of mutually trusting users attached to a transparent network" ☺
  - Internet protocol designers playing "catch-up"
  - Security considerations in all layers!

Bad guys can put malware into hosts via Internet

- Malware can get in host from a virus, worm, or Trojan horse.
- Spyware malware can record keystrokes, web sites visited, upload info to collection site.
- Infected host can be enrolled in a botnet, used for spam and DDoS attacks.
- Malware is often self-replicating: from an infected host, seeks entry into other hosts

Virus, Worm

- Virus
  - Almost all viruses are attached to an executable file, i.e., virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.
  - Typically, a virus cannot be spread without a human action, (such as running an infected program) to keep it going.

- Worm
  - It is similar to a virus, however, a worm is also a program that propagates itself. Unlike a virus, however, a worm can spread itself automatically over the network from one computer to the next.
  - The biggest danger is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

TROJAN HORSE

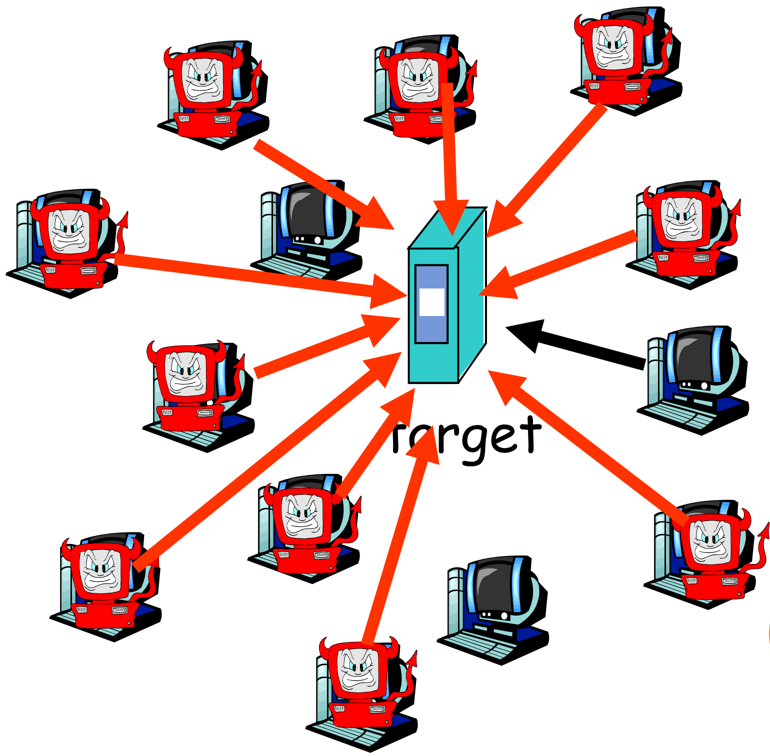
- Trojan Horse appears to be a useful software but will actually do damage once installed or run on your computer.

- Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised.

Bad guys can attack servers and network infrastructure

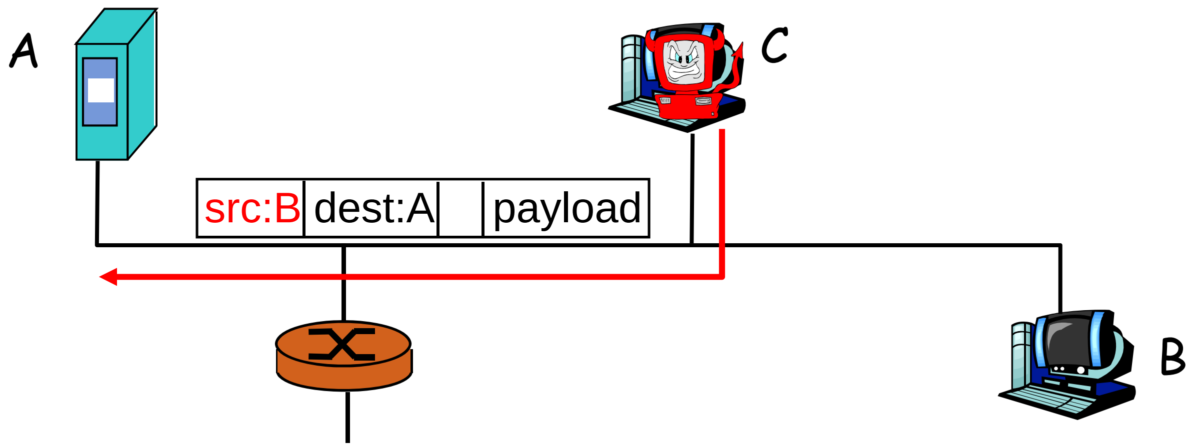
- **Denial of service (DoS):** attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network
3. send packets toward target from compromised hosts



THE BAD GUYS CAN USE FALSE SOURCE ADDRESSES

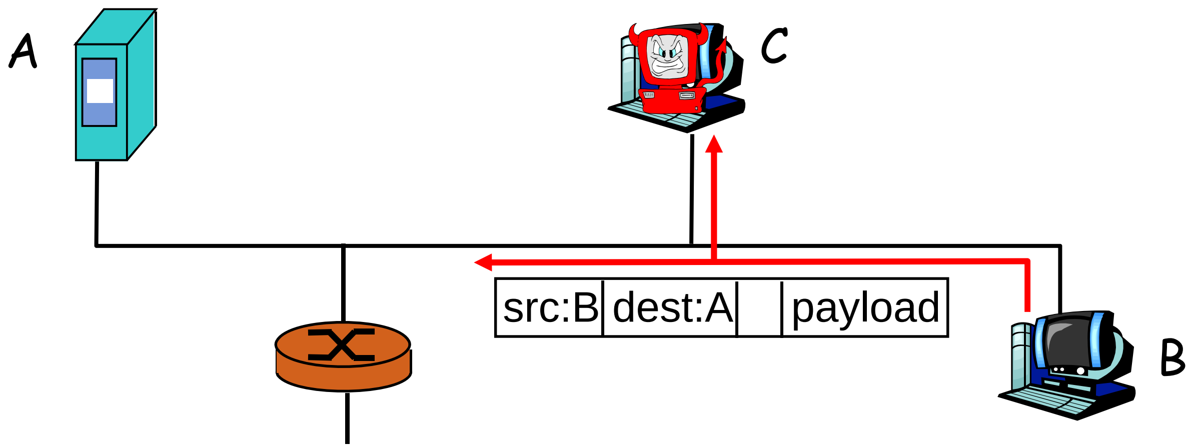
- *IP spoofing:* send packet with false source address



THE BAD GUYS CAN SNIFF PACKETS

Packet sniffing:

- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- Wireshark is a (free) packet-sniffer… try it

Internet History

1961-1972: Early packet-switching principles

- 1961: Kleinrock - queueing theory shows effectiveness of packet-switching
- 1964: Baran - packet-switching in military nets
- 1967: ARPAnet conceived by Advanced Research Projects Agency
- 1969: first ARPAnet node operational
- 1972:
  - ARPAnet public demonstration
  - NCP (Network Control Protocol) first host-host protocol
  - first e-mail program
  - ARPAnet has 15 nodes

Internet History

1972-1980: Internetworking, new and proprietary nets

- 1970: ALOHAnet satellite network in Hawaii
- Telenet, a BBN commercial packet switching network.
- Cyclades, a French packet switching network
- IBM's SNA (1969-1974)

- 1974: (Sponsored by DARPA) Cerf and Kahn - architecture for interconnecting networks
- 1979: ARPAnet has 200 nodes

Internet History

1980-1990: new protocols, a proliferation of networks

- 1983: deployment of TCP/IP
- 1982: smtp e-mail protocol defined
- 1983: DNS defined for name-to-IP-address translation
- 1985: ftp protocol defined
- 1988: TCP congestion control

- New national networks: Csnet, BITnet, NSFnet, Minitel
- 100,000 hosts connected to confederation of networks

Internet History

1990, 2000's: commercialization, the Web, new apps

- Early 1990's: ARPAnet decommissioned
- 1991: NSF lifts restrictions on commercial use of NSFnet (decommissioned, 1995)
- Early 1990s: Web
  - hypertext [Bush 1945, Nelson 1960's]
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, later Netscape
  - late 1990's: commercialization of the Web

Late 1990's – 2000's:

- more killer apps: instant messaging, P2P file sharing
- network security to forefront
- est. 50 million host, 100 million+ users
- backbone links running at Gbps

INTERNET HISTORY

2007:

- ~500 million hosts
- Voice, Video over IP
- P2P applications: BitTorrent (file sharing) Skype (VoIP), PPLive (video)
- More applications: YouTube, gaming
- Wireless, mobility