18CSS202J- COMPUTER COMMUNICATIONS

UNIT –I Contents

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Evolution of Computer Networks
- Network Categories
- Data Transmission Modes
- Network Topologies
- Circuit Switching and Packet Switching
- Protocols and Standards
- OSI Layers and its functions
- TCP/IP Protocol Suite
- Link Layer Protocols
- Network Layer Protocols
- Transport Layer Protocols
- Serial and Parallel Transmissions
- Addressing

Session 1

Evolution of Computer Networks
Network Categories
Data Transmission Modes
Network Topologies

Evolution of Computer Networks

Computer Networks?

- A group of interconnected computers
- The evolution of two important scientific and technical branches of modern civilization
  - Computing and
  - Telecommunications technologies

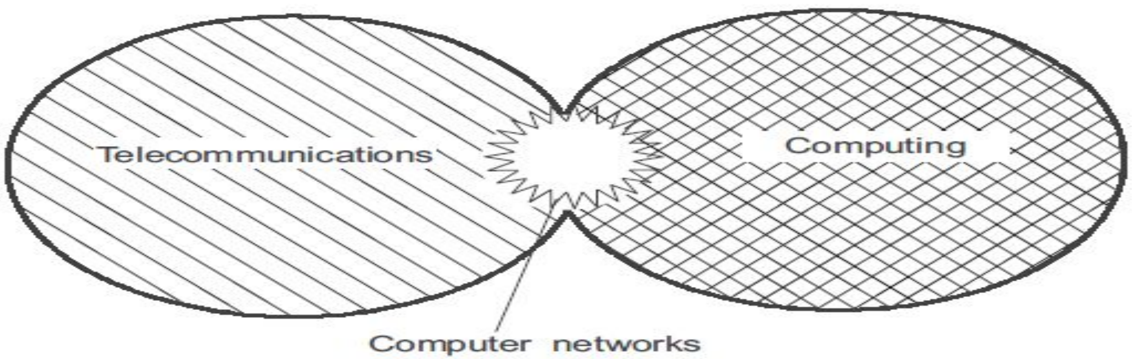


Figure 1.1 Evolution of computer networks at the interfaces of the computing and communications technologies

Evolution of Computer Networks

Communication Network?

- A network of **links** and **nodes** arranged **messages** may be passed from one part of the network to another
- **What are nodes and links**?
  - People and roads
  - Telephones and switches
  - Computers and routers
- What is a **message?**
  - **Information**

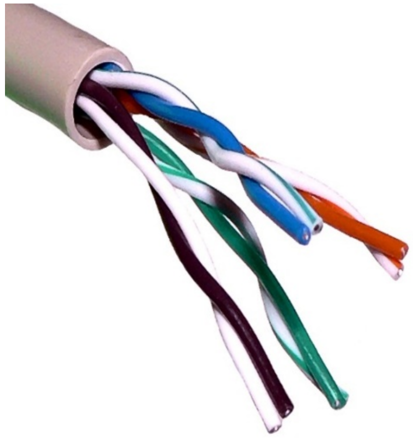
Evolution of Computer Networks

- Networks are Old
  - 2400 BC: courier networks in Egypt
  - 550 BC: postal service invented in Persia
- Problems
  - Speed
  - Reliability
  - Security
- 1837: Telegraph invented by Samuel Morse
  - Distance: 10 miles
  - Speed: 10 words per minute
  - In use until 1985!

Evolution of Computer Networks

INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- 1881: Twisted pair for local loops
- 1885: AT&T formed
- 1892: Automatic telephone switches
- 1903: 3 million telephones in the US
- 1915: First transcontinental cable
- 1927: First transatlantic cable
- 1937: first round-the-world call
- 1946: National numbering plan

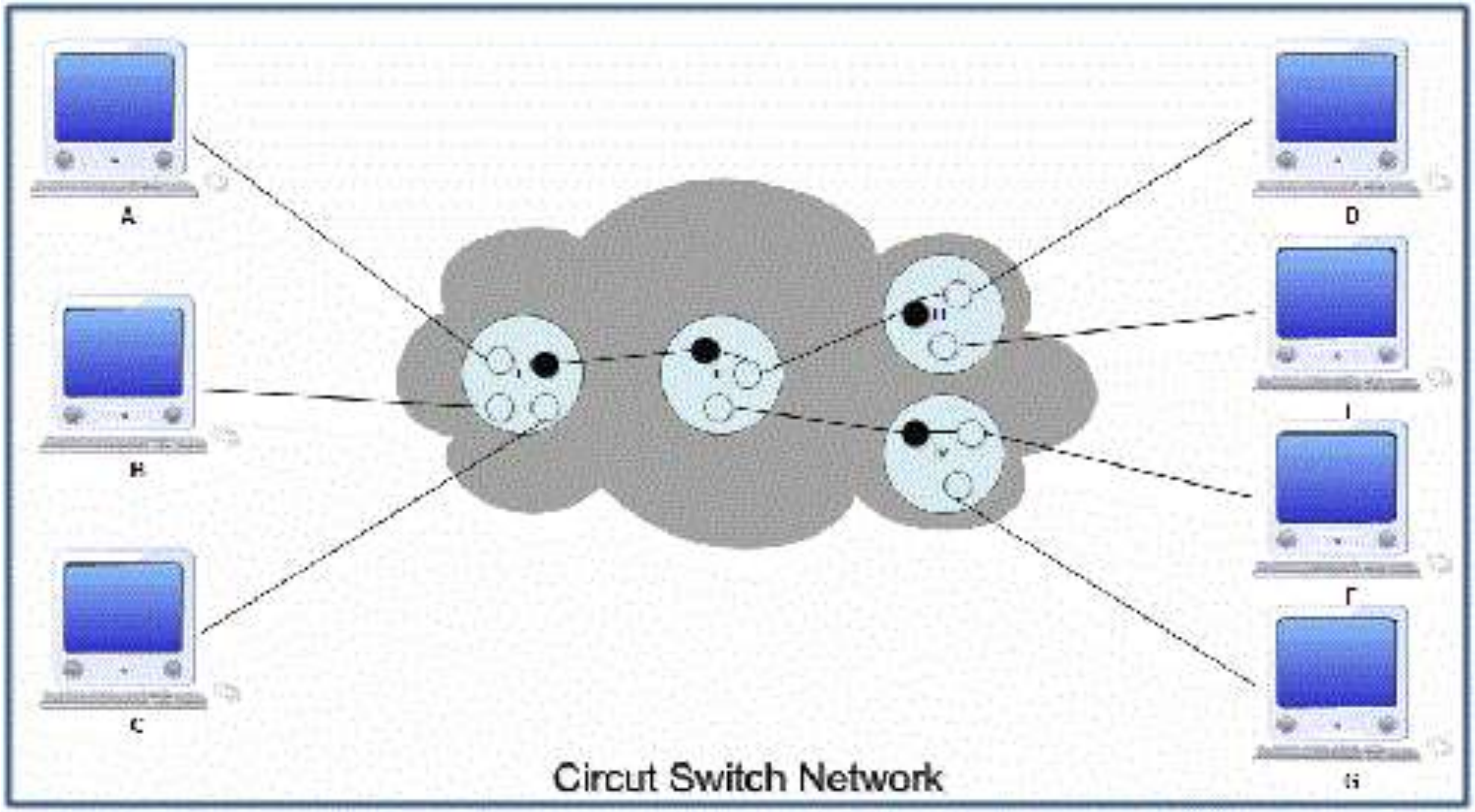


- Telephone network is the dominating communication network

- Used circuit switching

at&t

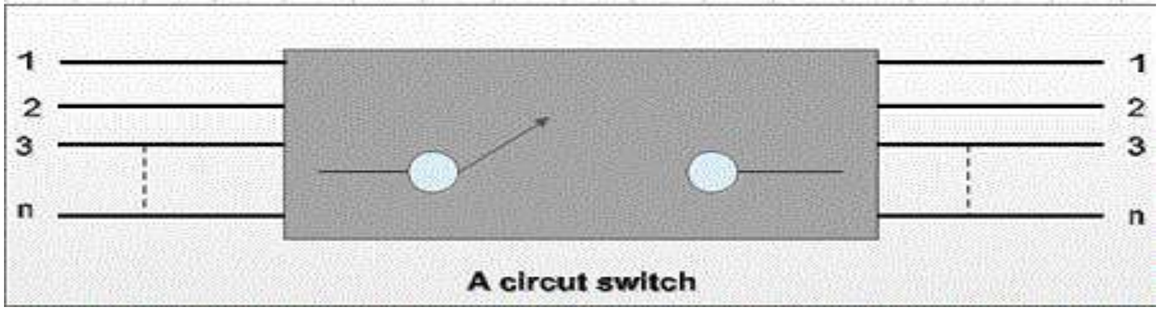
Evolution of Computer Networks



Evolution of Computer Networks

Circuit switching

- Telephone networks are circuit switched
- Each call reserves resources end-to-end
- Provides excellent quality of service

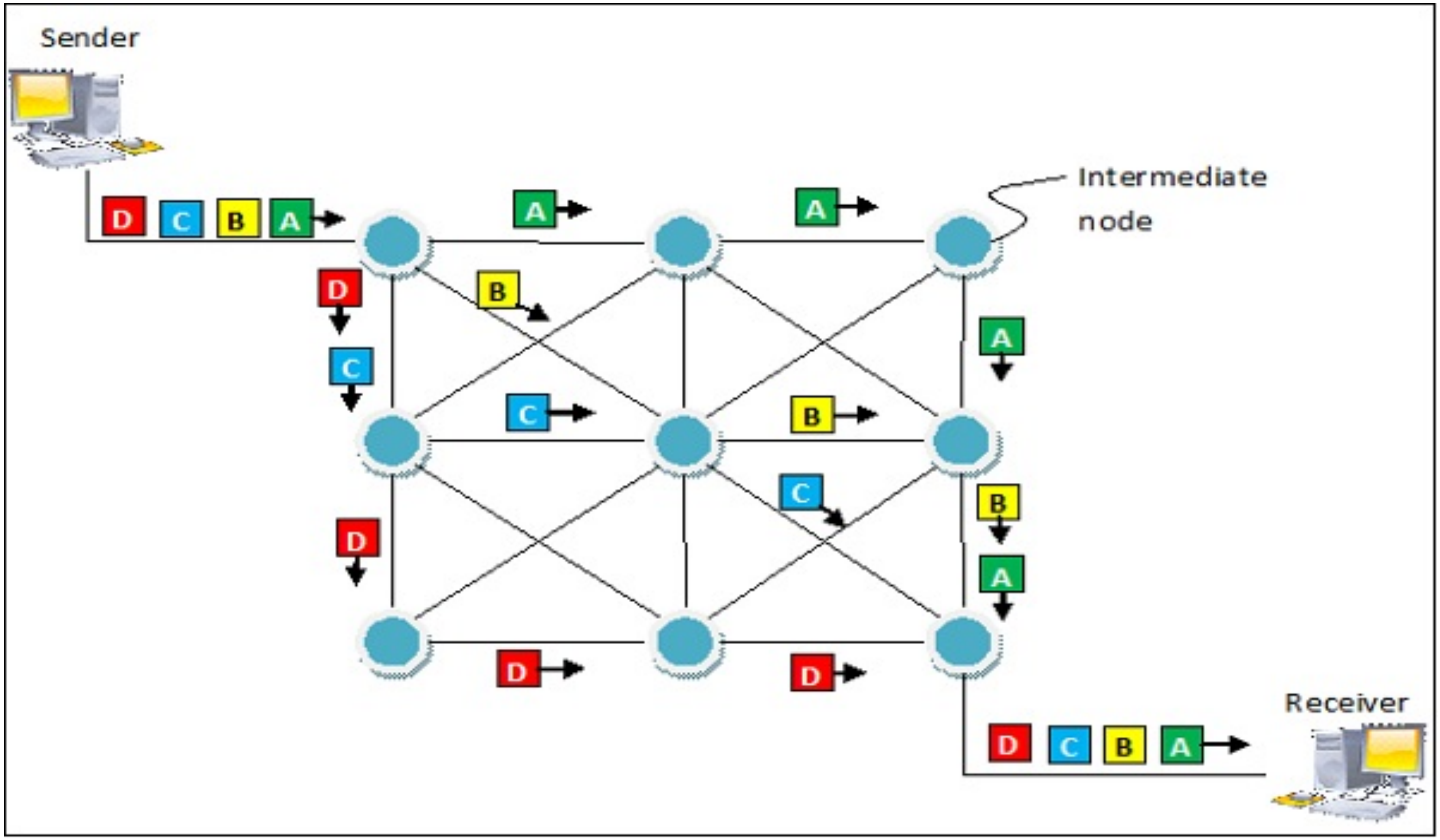


Problems

- Resource intense (what if the circuit is idle?)
- Complex network components
  (per circuit state, security)

Evolution of Computer Networks

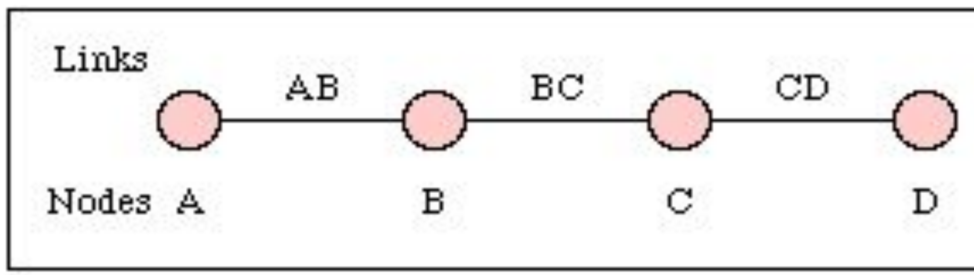
Packet Switching



Evolution of Computer Networks

Packet switching

- No connection state, network is store-and-forward
- Minimal network assumptions
- Statistical multiplexing gives high overall utilization



Problems

- Resource intense (what if the circuit is idle?)
- Complex network components
  (per circuit state, security)

Evolution of Computer Networks

From the ARPANET to the Internet

- **The Advanced Research Projects Agency Network (ARPANET)**
- It is one of the world's first packet switching networks
- The first network to implement TCP/IP, and was the main progenitor of what was to become the global Internet. (later **DARPA**)

Evolution of Computer Networks

Internet

- The **Internet** is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide

- The packet switching of the **ARPANET**, together with **TCP/IP**, would form the **backbone** of how the Internet works

1972:

- ARPAnet is now consistent of 15 nodes
- The first host-to-host protocol

    NCP (Network Control Protocol) enables applications to be written

    First e-mail program

Evolution of Computer Networks

- ALOHAnet
  Enabling communication over microwaves between the Hawaiian Islands.
- NSFNET
  Connection to supercomputing centers
  56kbps backbone, later 1,5Mbps and serving as the linkingbackbonebetween regional networks
- CSNET
  Linking researchers without access to the ARPAnet
- BITNET
  University e-mail and file sharing
- TCP/IP replacing NCP as the standard hostprotocol for ARPAnet

Evolution of Computer Networks

- **Brief History of the Internet**

1961: Kleinrock @ MIT: packet-switched network
1962: Licklider's vision of Galactic Network
1965: Roberts connects computers over phone line
1967: Roberts publishes vision of ARPANET
1969: BBN installs first Interface Msg Processor at UCLA
1970: Network Control Program (NCP)
1972: Public demonstration of ARPANET
1972: Kahn @ DARPA advocates Open Architecture
1972: Vint Cerf @ Stanford writes TCP

Evolution of Computer Networks

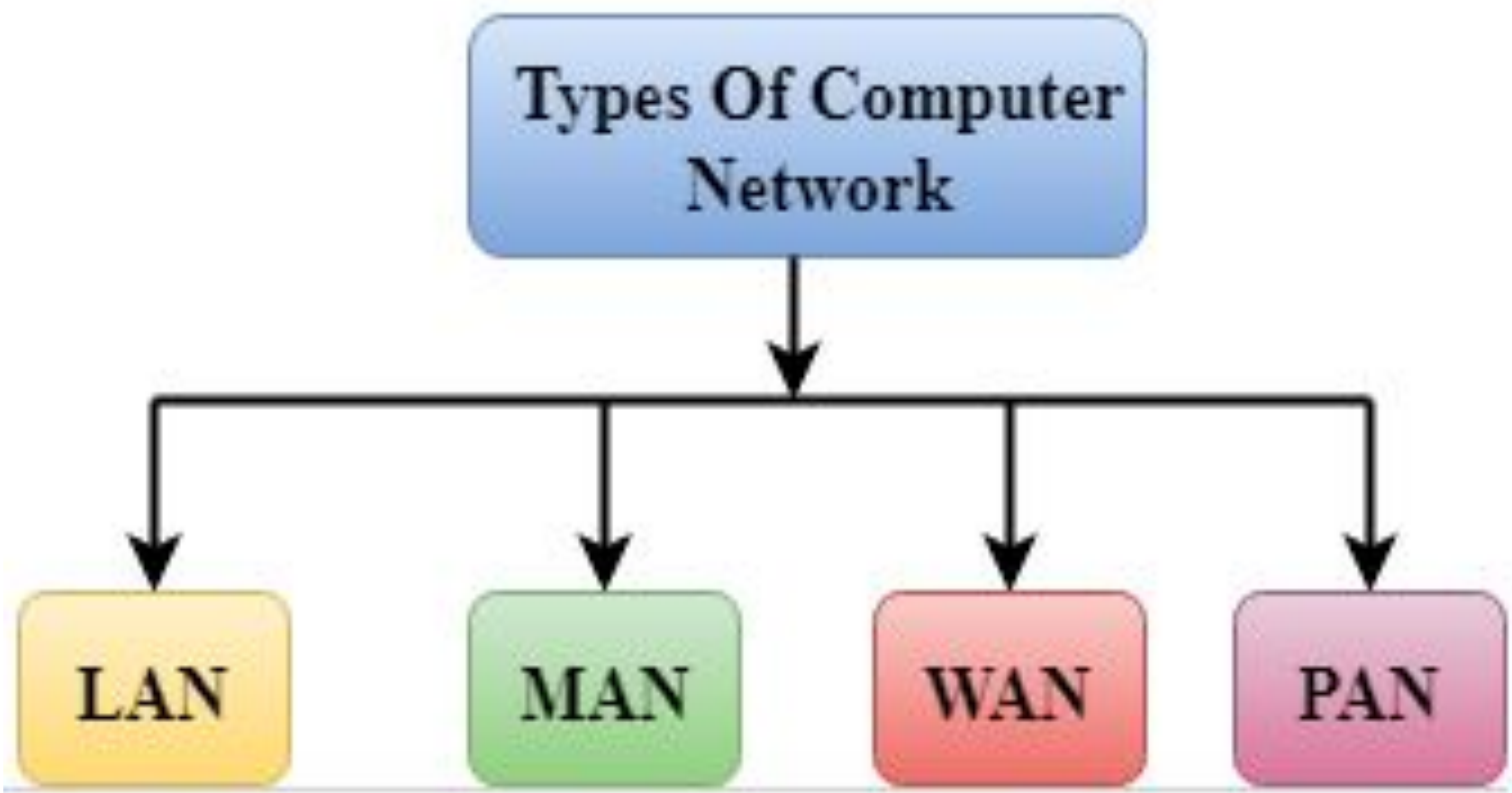
- 1958: **First use of a modem**
  Machine to machine communication
  Analog vs. digital signals
- **Many different computer networks**
  - Local vs. global
    LAN, WAN
  - Public Vs Private
    Internet2, SRMNet
  - General purpose vs. special purpose
    E.g. credit cards, banks, defense

Evolution of Computer Networks

- Early 1990s: WWW
  - Hypertext
  - HTTP: Tim Berners-Lee develops WWW an Internet based hypermedia initiative, and specifies URLs, HTTP and HTML which became basis for today's WWW
  - 1994: Mosaic (Univ. of Illinois), later Netscape the major browsers until late 1990's
  - Commercialization of the WWW, with introduction of HTTPS e-commerce is realized

- Late 1990's:
- 50 million computers on Internet
- 100 million+ users
- backbone links running at 1 Gbps

Network Categories

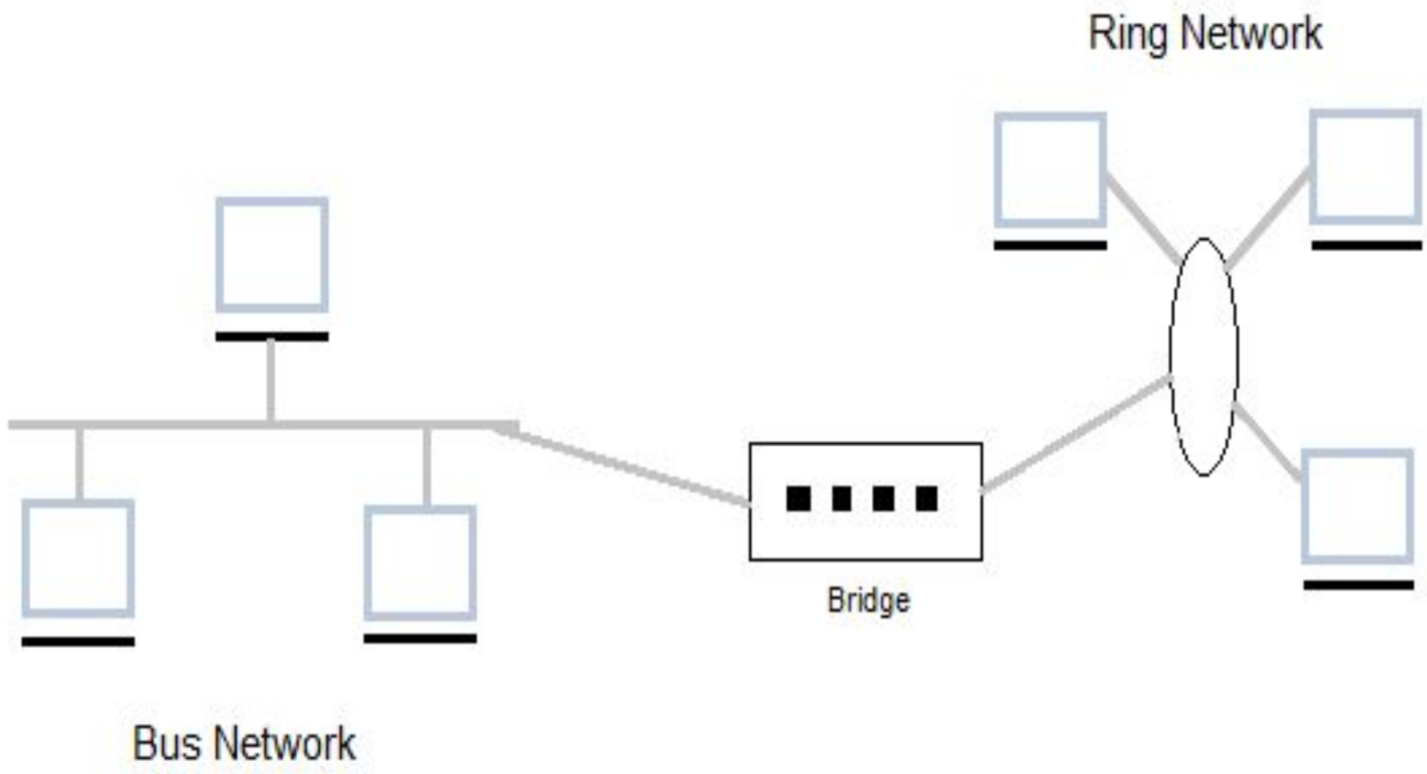


Characteristics of LAN

- LAN – Local Area Network
- MAN – Metropolitan Area Network
- WAN – Wide Area Network
- PAN – Personal Area Network

Network Categories

Local Area Network (LAN)



(Different Topologies interconnected in a Local Area Network)

LAN

- Local Area Network (LAN) is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

Applications of LAN

- One of the computer in a network can become a server serving all the remaining computers called clients.
- Software can be stored on the server and it can be used by the remaining clients.
- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

Advantages of LAN

Resource Sharing: Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.

Software Applications Sharing: It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.

Easy and Cheap Communication: Data and messages can easily be transferred over networked computers.

Advantages of LAN

Centralized Data: The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.

Data Security: Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.

Internet Sharing: Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

Disadvantages of LAN

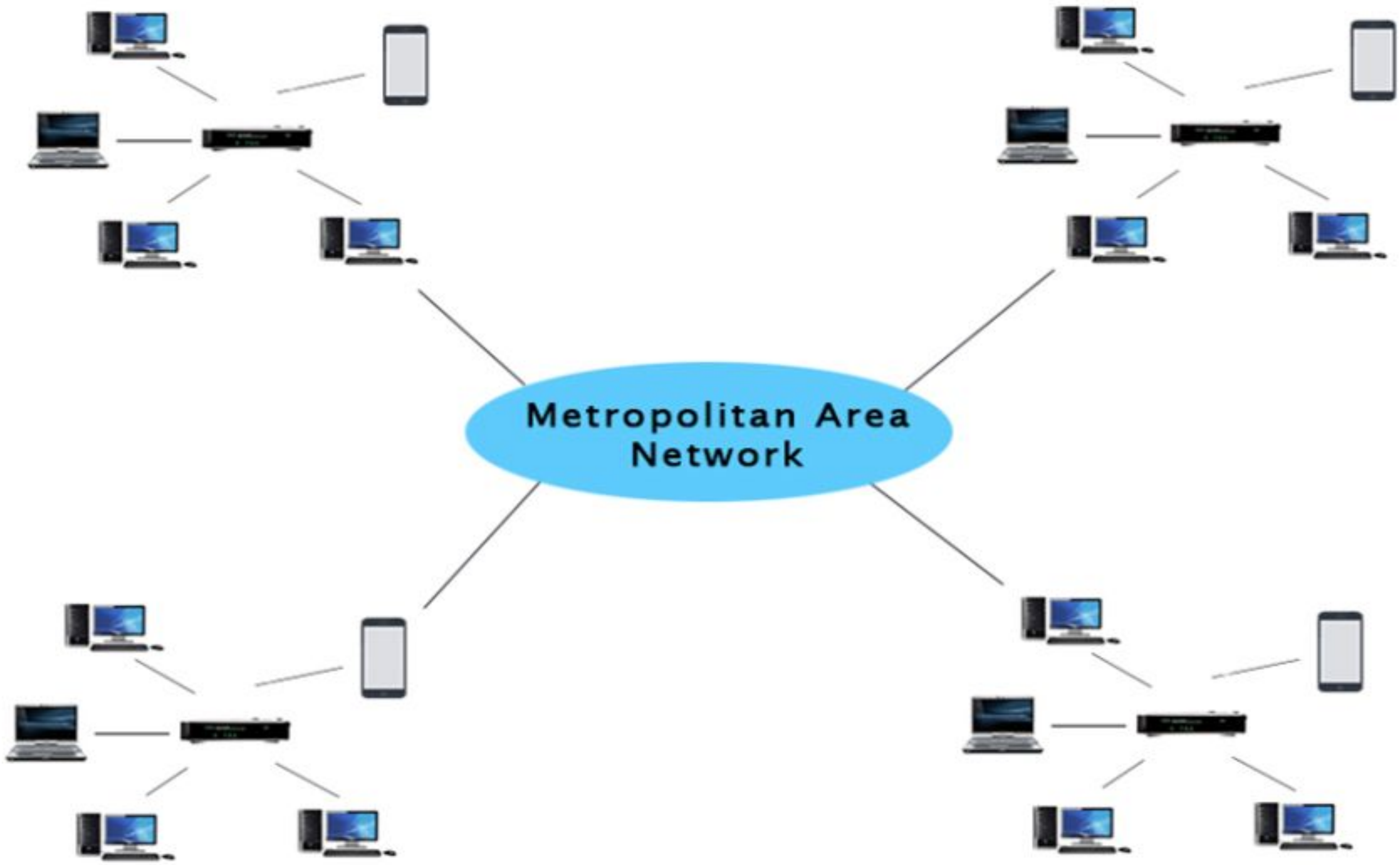
High Setup Cost: Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.

Privacy Violations: The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.

Disadvantages of LAN

Data Security Threat: Unauthorized users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
LAN Maintenance Job: Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
Covers Limited Area: Local Area Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)



Metropolitan Area Network (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

Characteristics of MAN

- It generally covers towns and cities (50 km)
- Communication medium used for MAN are optical fibers, cables etc.
- Data rates adequate for distributed computing applications.

Applications of MAN

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

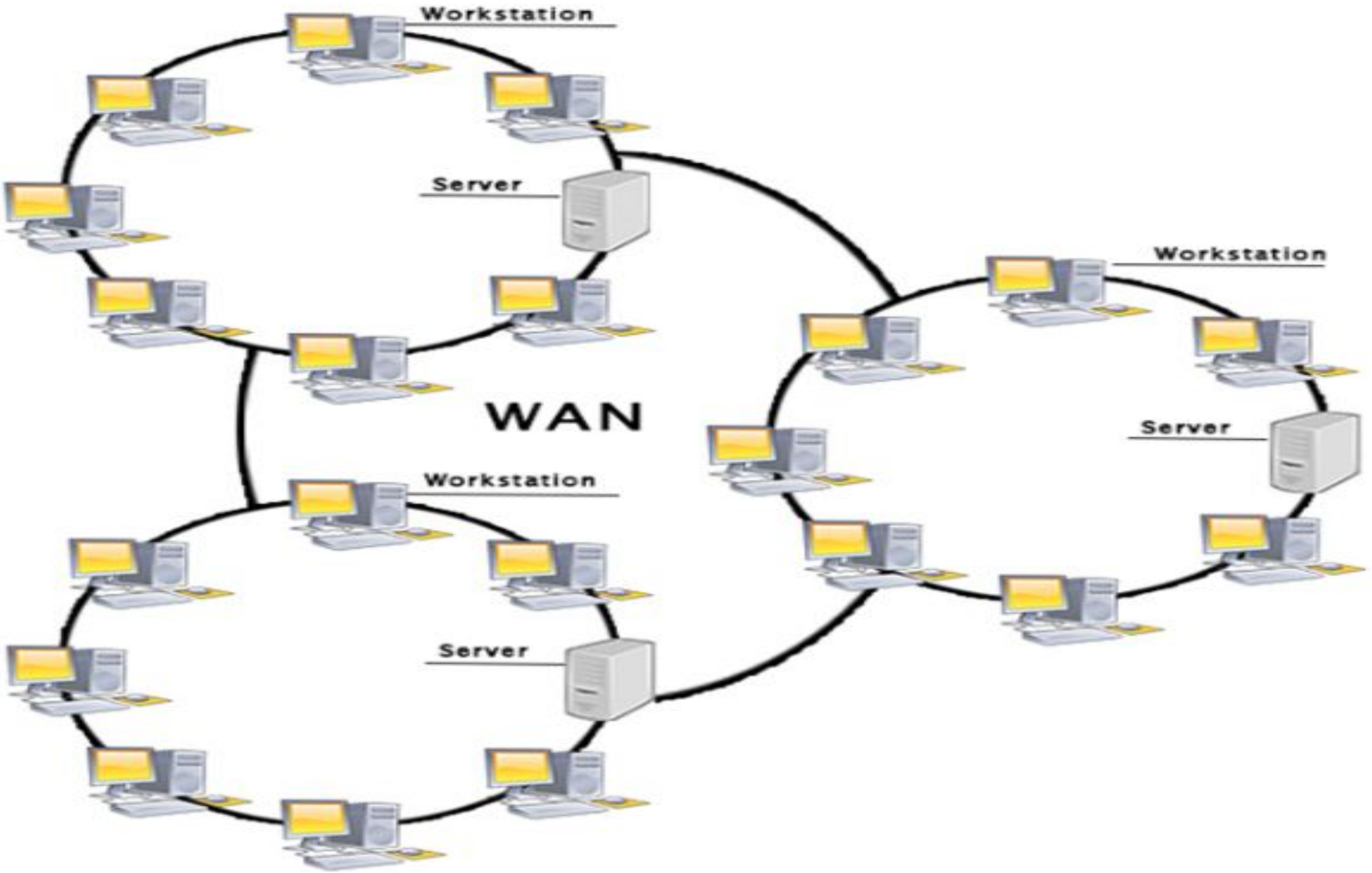
Advantages of MAN

- Extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually encompasses several blocks of a city or an entire city.

Disadvantages of MAN

- More cable required for a MAN connection from one place to another.
- It is difficult to make the system secure from hackers and industrial espionage (spying) graphical regions.

Wide Area Network (WAN)



Wide Area Network (WAN)

- It is also called WAN. WAN can be private or it can be public leased network.
- It is used for the network that covers large distance such as cover states of a country.
- It is not easy to design and maintain.
- Communication medium used by WAN are PSTN or Satellite links.
- WAN operates on low data rates.

Examples for WAN

Mobile Broadband: A 4G network is widely used across a region or country.
Last mile: A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
Private network: A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Characteristics of WAN

- It generally covers large distances(states, countries, continents).
- Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages of WAN

Geographical area: A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.

Centralized data: In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.

Get updated files: Software companies work on the live server. Therefore, the programmers get the updated files within seconds.

Advantages of WAN

Exchange messages: In a WAN network, messages are transmitted fast. The web application like Facebook, WhatsApp, Skype allows you to communicate with friends.
Sharing of software and resources: In WAN network, we can share the software and other resources like a hard drive, RAM.
Global business: We can do the business over the internet globally.
High bandwidth: If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of WAN

Security issue: A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
Needs Firewall & antivirus software: The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
High Setup cost: An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
Troubleshooting problems: It covers a large area so fixing the problem is difficult.

Personal Area Network (PAN)

Personal Area Network (PAN)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**. Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

Examples of PAN

Body Area Network: Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.

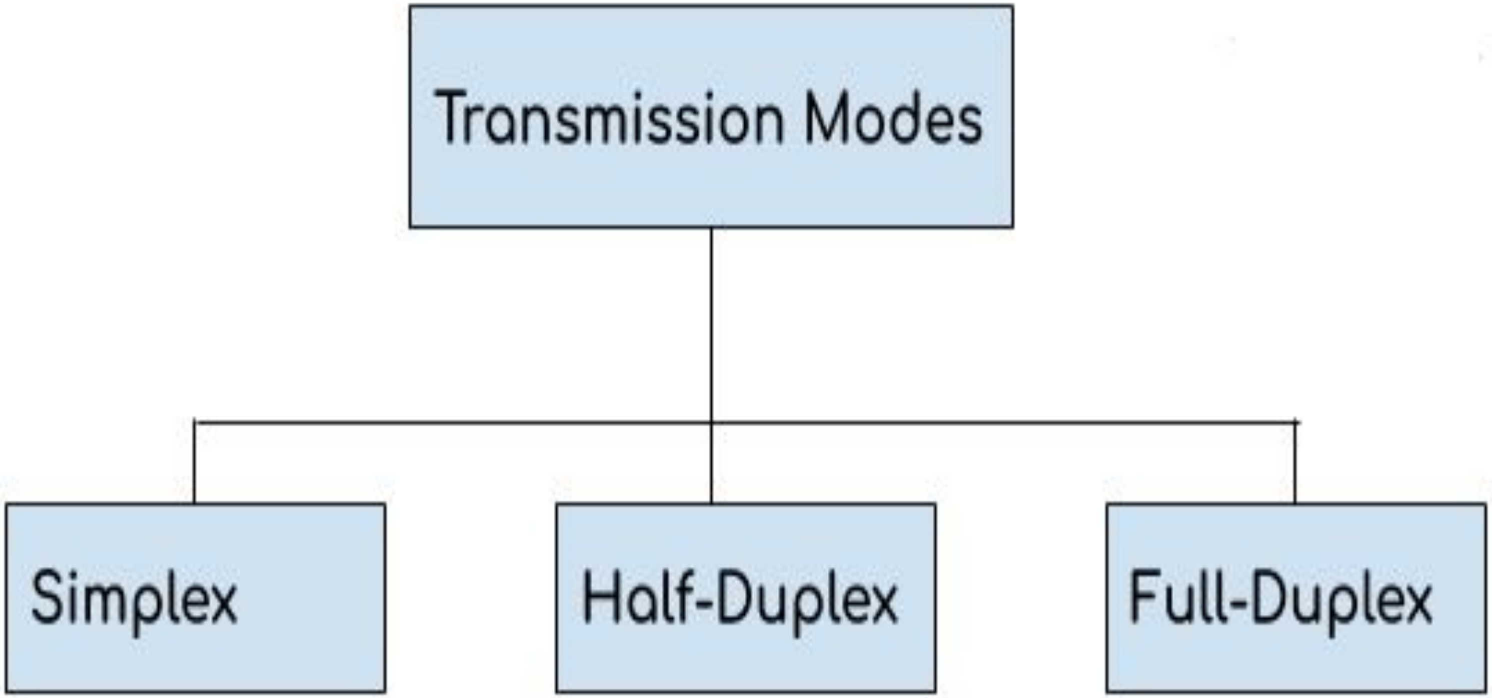
Offline Network: An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.

Small Home Office: It is used to connect a variety of devices to the internet and to a corporate network using a VPN

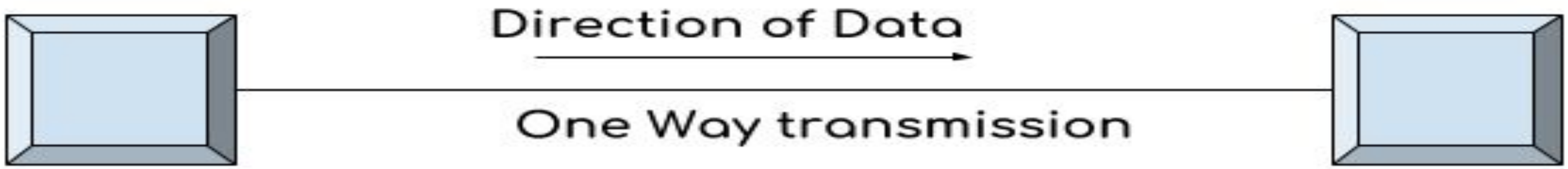
Data Transmission Modes

- The data is transmitted from one device to another device through a **transmission mode**.
- The transmission mode decides the **direction of data** in which the data needs to travel to reach the receiver system or node.
- The transmission mode is divided into three categories:
  1. Simplex
  2. Half-Duplex
  3. Full-Duplex

Data Transmission Modes



Simplex Mode



1. In simplex mode the data transmits in one direction only, from one system to another system.
2. The sender device that sends data can only send data and cannot receive it. On the other hand the receiver device can only receive the data and cannot send it.
3. Television is an example of simplex mode transmission as the broadcast sends signals to our TV but never receives signals back from our TV. This is a unidirectional transmission.

Simplex Mode

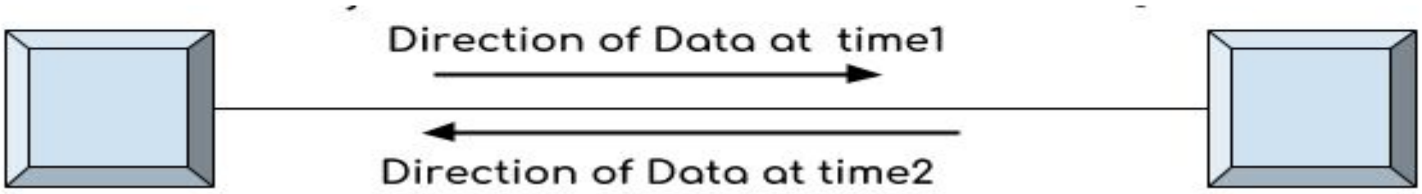
Advantages of Simplex Mode:

The full capacity of the transmission medium is utilized as the transmission is one way and cannot have traffic issues.

Disadvantages of Simplex Mode:

No bidirectional communication is possible. Two devices cannot communicate with each other using simplex mode of transmission.

Half-Duplex Mode



1. In half duplex mode transmission can be done both ways which means if two systems are connected with half-duplex mode of transmission, they both can send and receive data but not at the same time.
2. If one device is sending data then other device cannot send data until it receives the data which is already in transmission. You can say that the communication is not simultaneous.
3. The radio communication device that our soldiers use at the battle fields are the examples of half duplex mode transmission as they send message and then say over and then the person on other hand send his message and this way they communicate but not simultaneously like we used to do on mobile.

Half-Duplex Mode

Advantages of Half-Duplex mode:

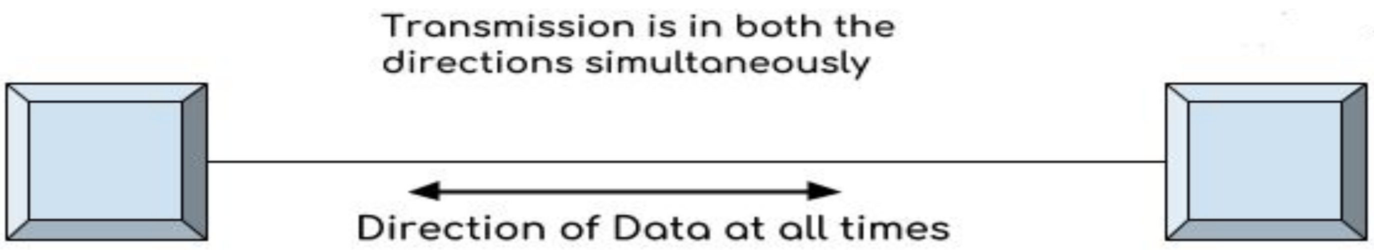
Both devices can send and receive data.

Whole bandwidth can be utilized as at a time only one signal transmits.

Disadvantages of Half-Duplex mode:

The disadvantage in half duplex mode is that the other device cannot send data until it receives the data which is already in transmission, this can cause delays to the communication.

Full-Duplex Mode



1. In full duplex mode both the connected devices can send and receive data simultaneously. The mobile phone we use is an example of full duplex mode where we can communicate simultaneously.
2. Both the devices can send and receive the data at the same time.

Full-Duplex Mode

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Advantages of Full Duplex mode:
No delays in communication as both can send and receive data simultaneously.

Disadvantages of Full Duplex mode:
No proper bandwidth utilization as the same line is used for sending and receiving data at the same time.

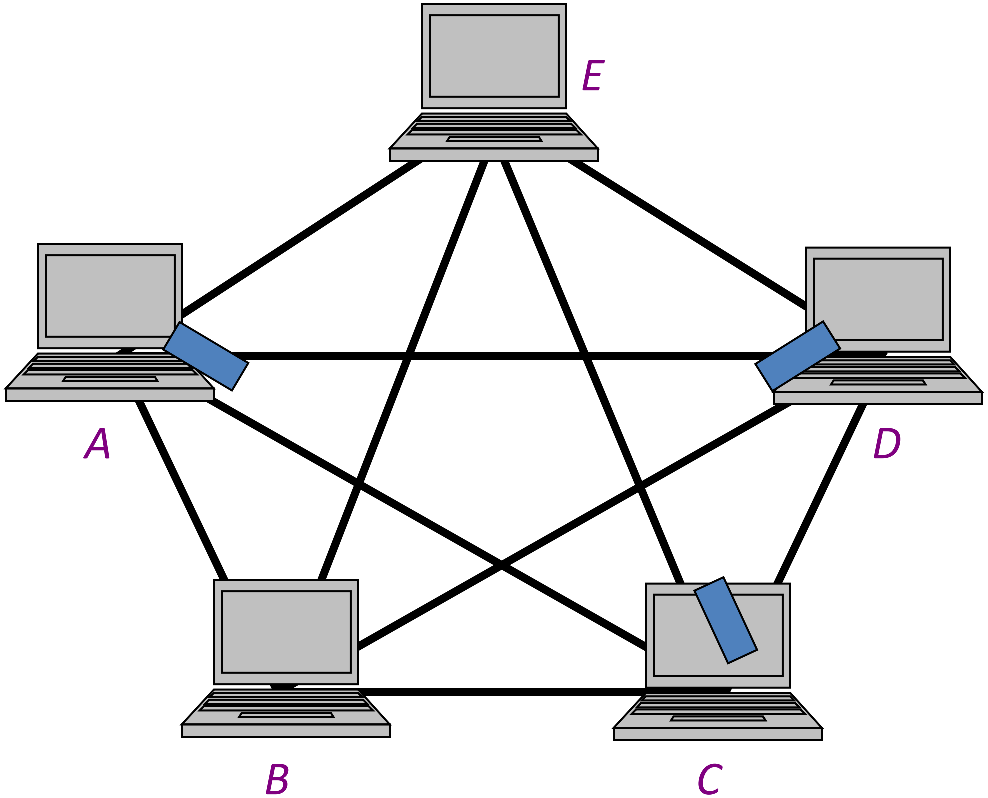
Network Topology- Types

Network Topology- Types

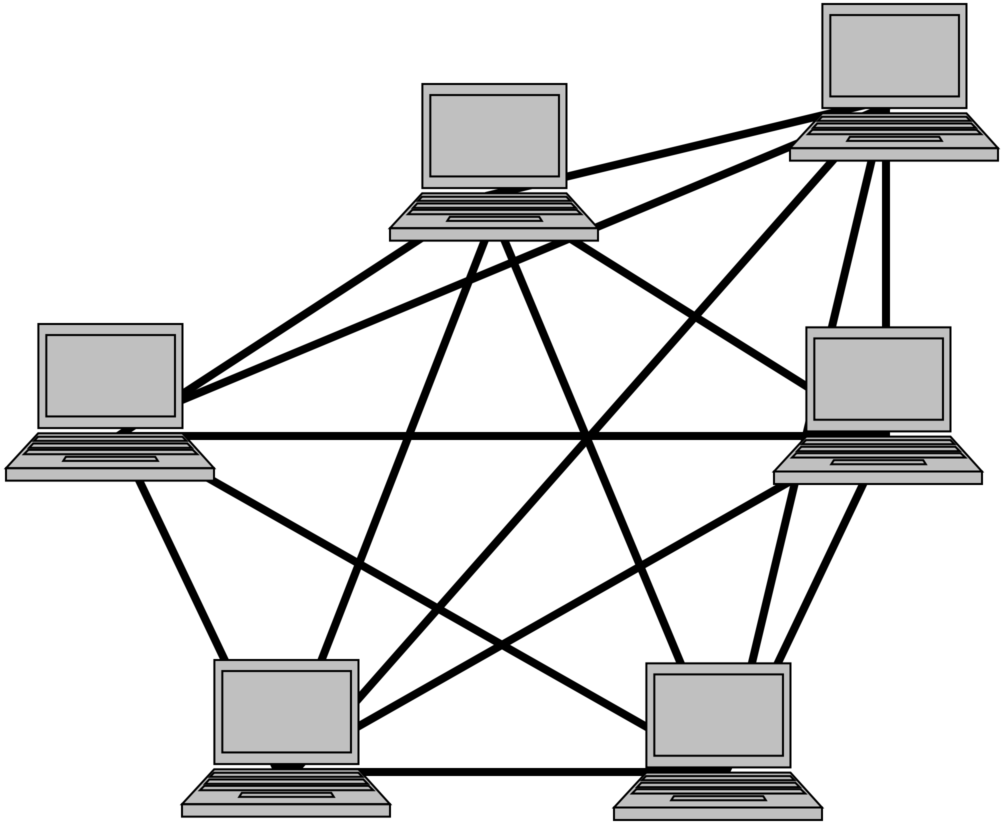
- Topology: physical or logical arrangement of devices
  - Point-to-point
  - Mesh
  - Star
  - Bus
  - Ring
  - Hybrid

Point-to-Point Connection

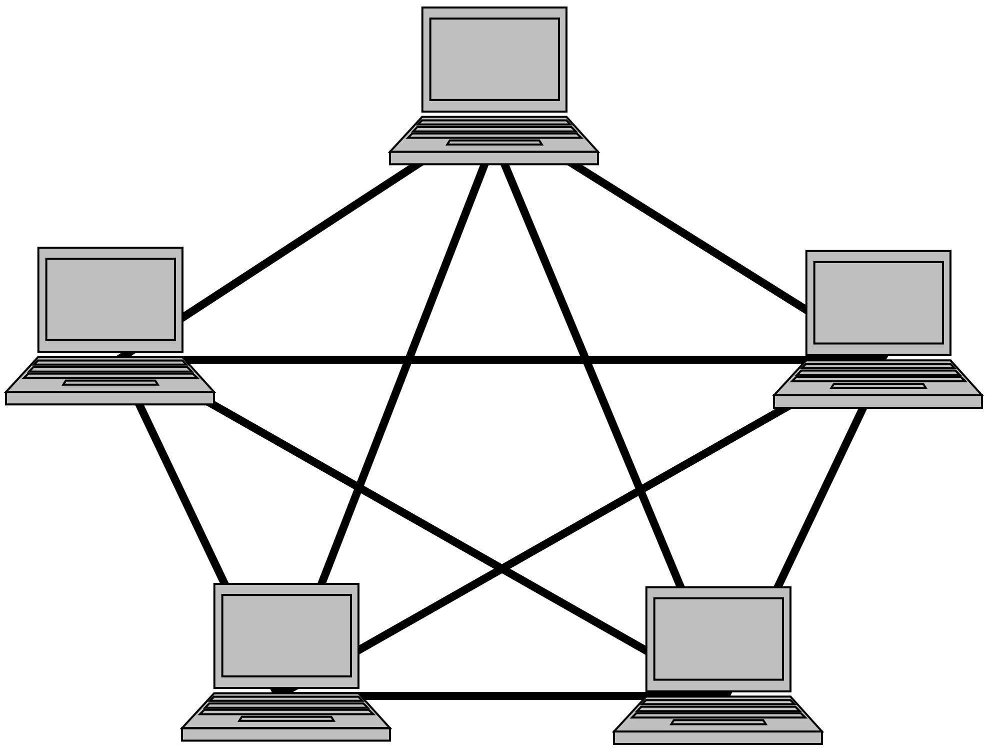
Fully Connected Mesh Topology



Fully Connected Mesh Topology

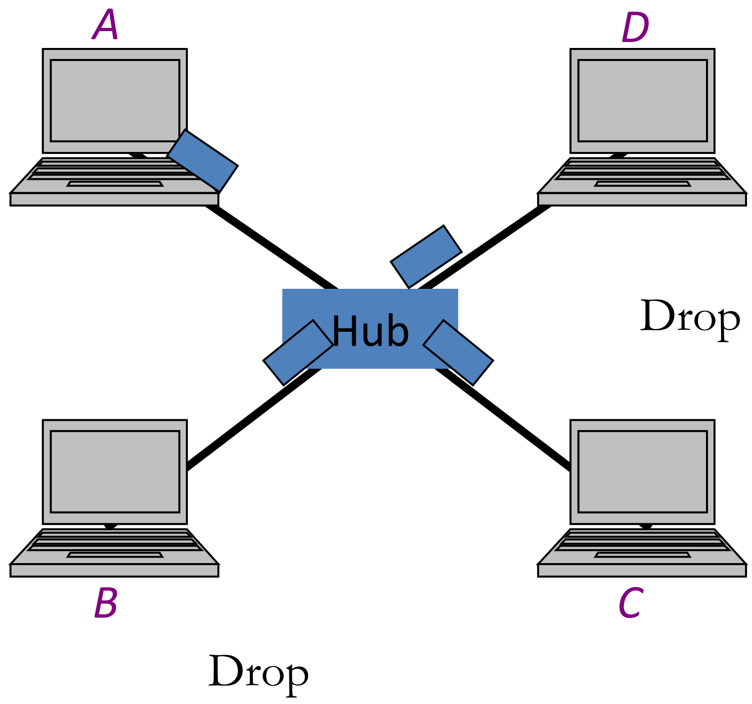


Fully Connected Mesh Topology

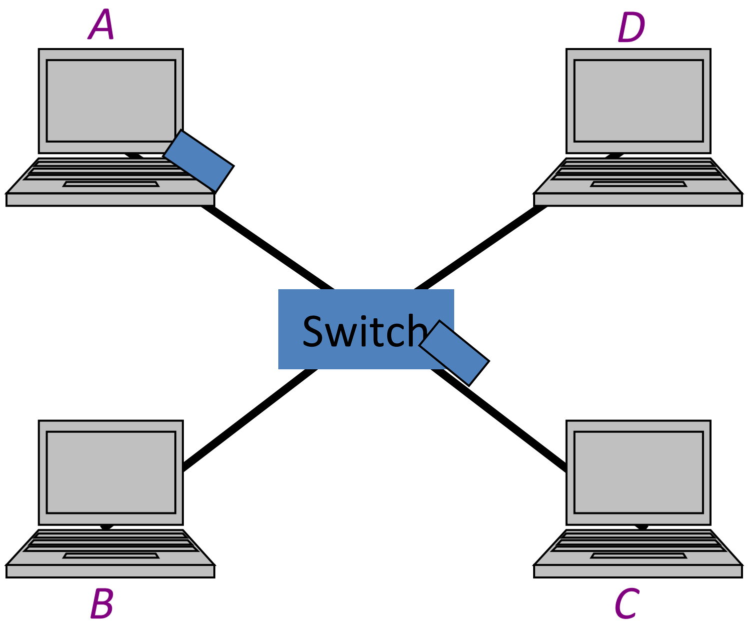


- **Pros:**
  - Dedicated links
  - Robustness
  - Privacy
  - Easy to identify fault
- **Cons:**
  - A lot of cabling
  - I/O ports
  - Difficult to move

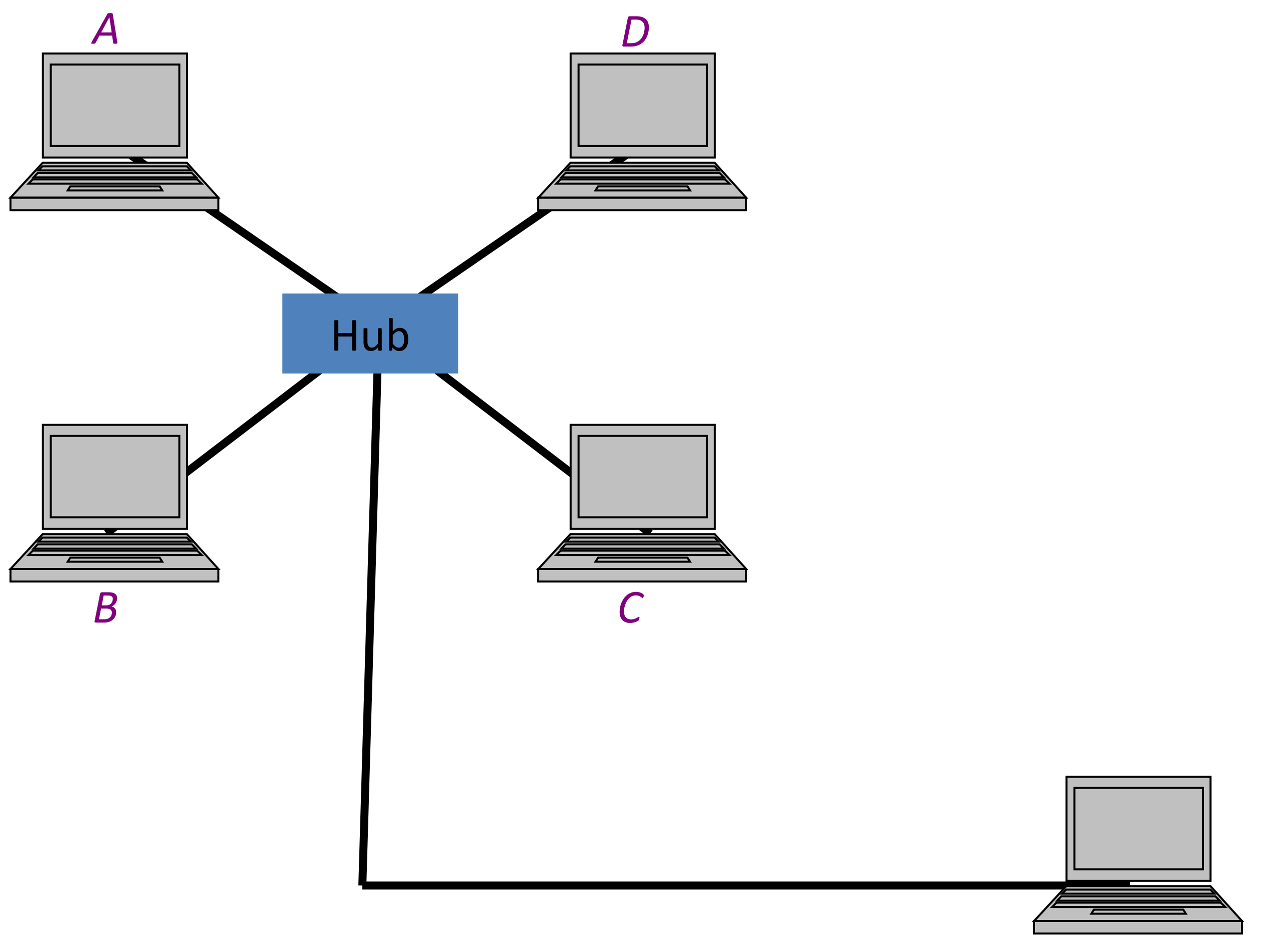
Star Topology



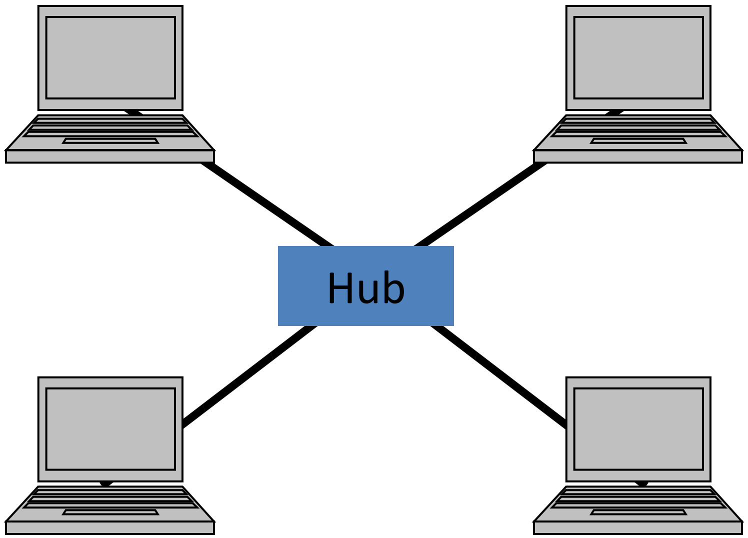
Star Topology



Star Topology



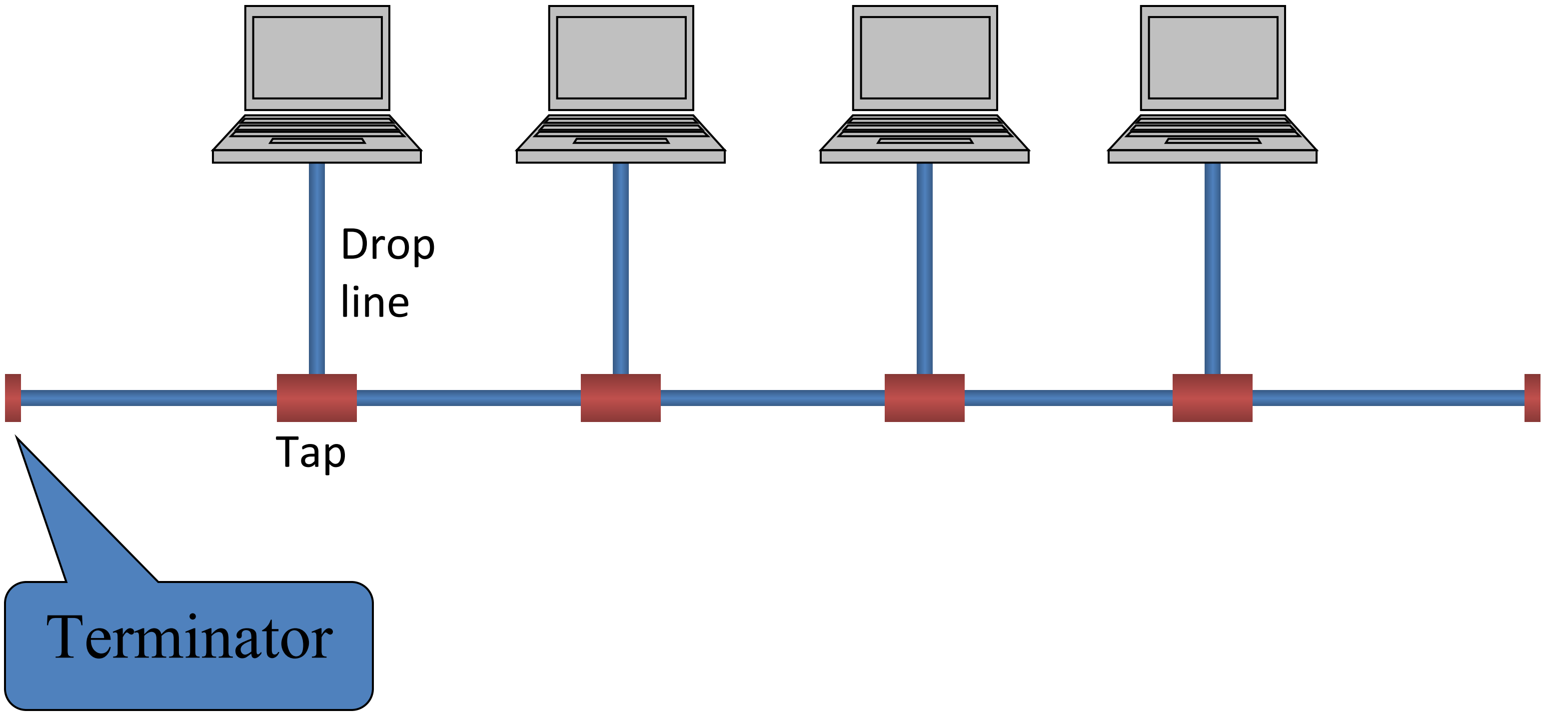
Star Topology



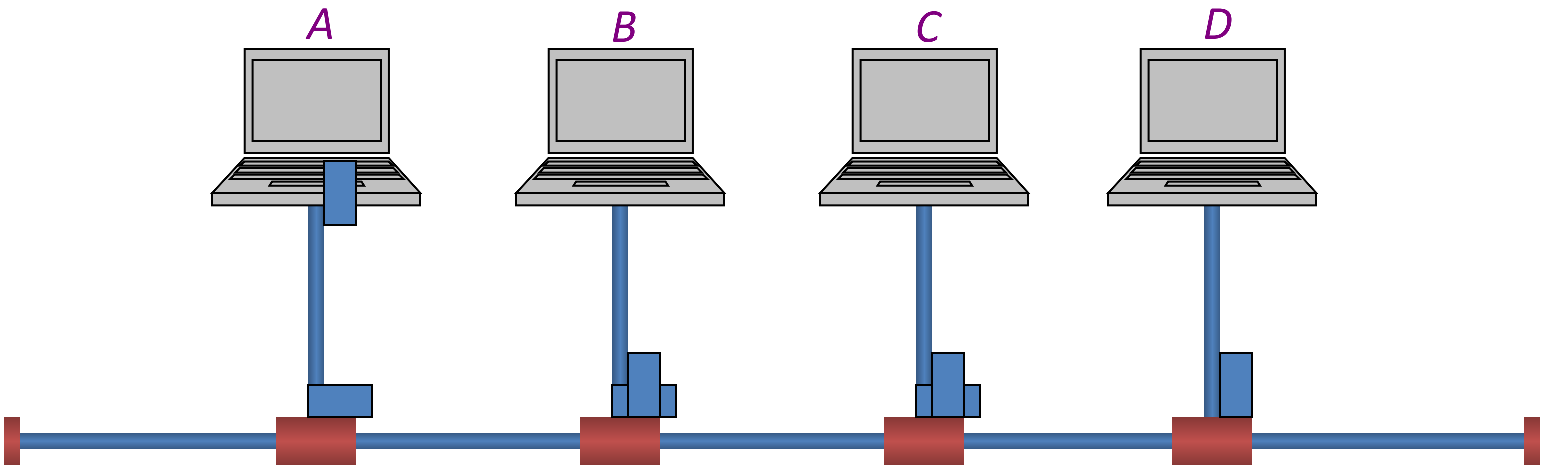
- **Pros:**
  - One I/O port per device
  - Little cabling
  - Easy to install
  - Robustness
  - Easy to identify fault

- **Cons:**
  - Single point of failure
  - More cabling still required

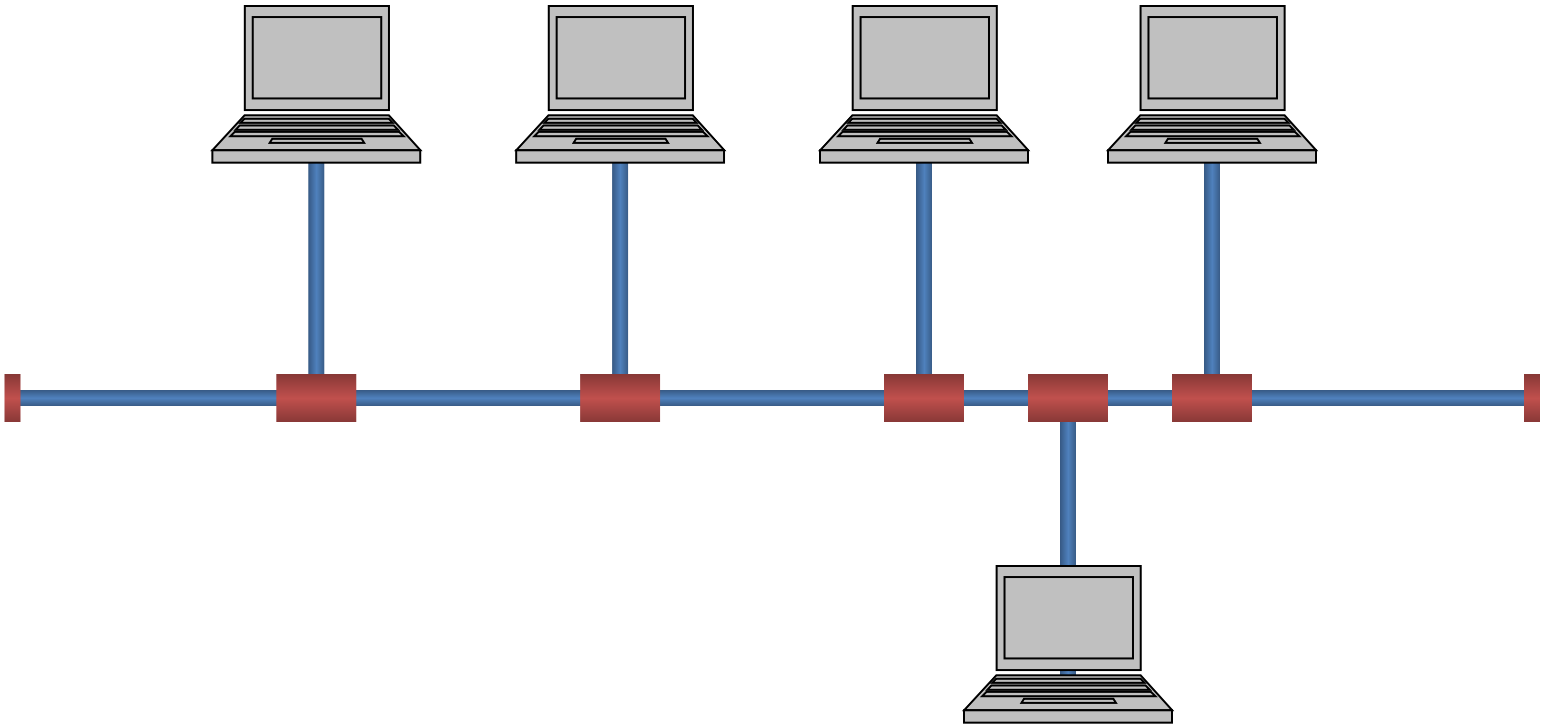
Bus Topology



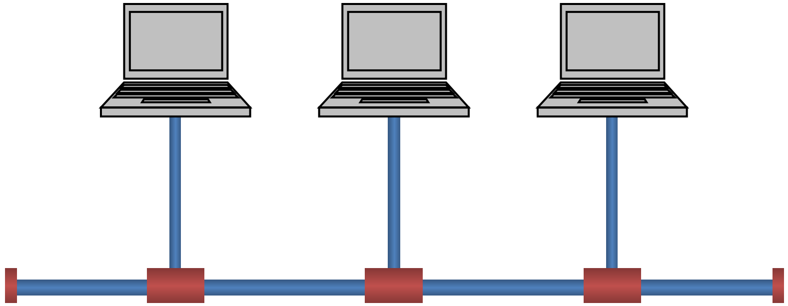
Bus Topology



Bus Topology

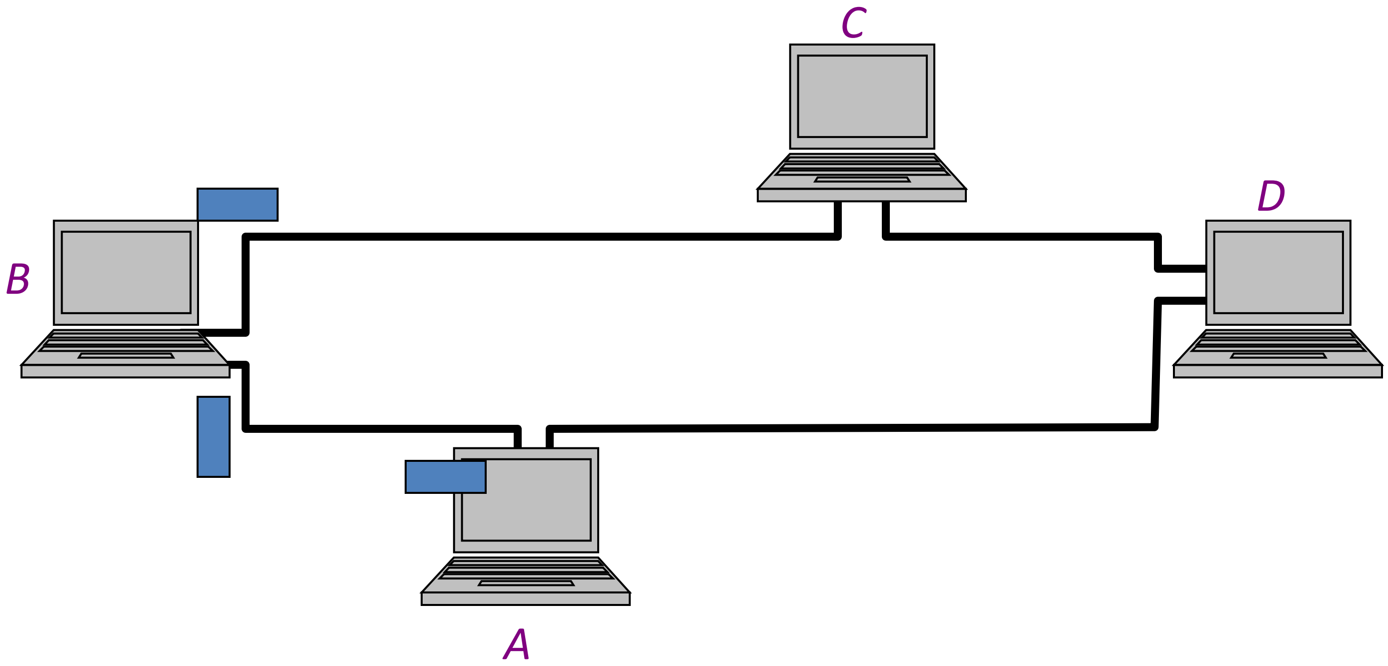


Bus Topology

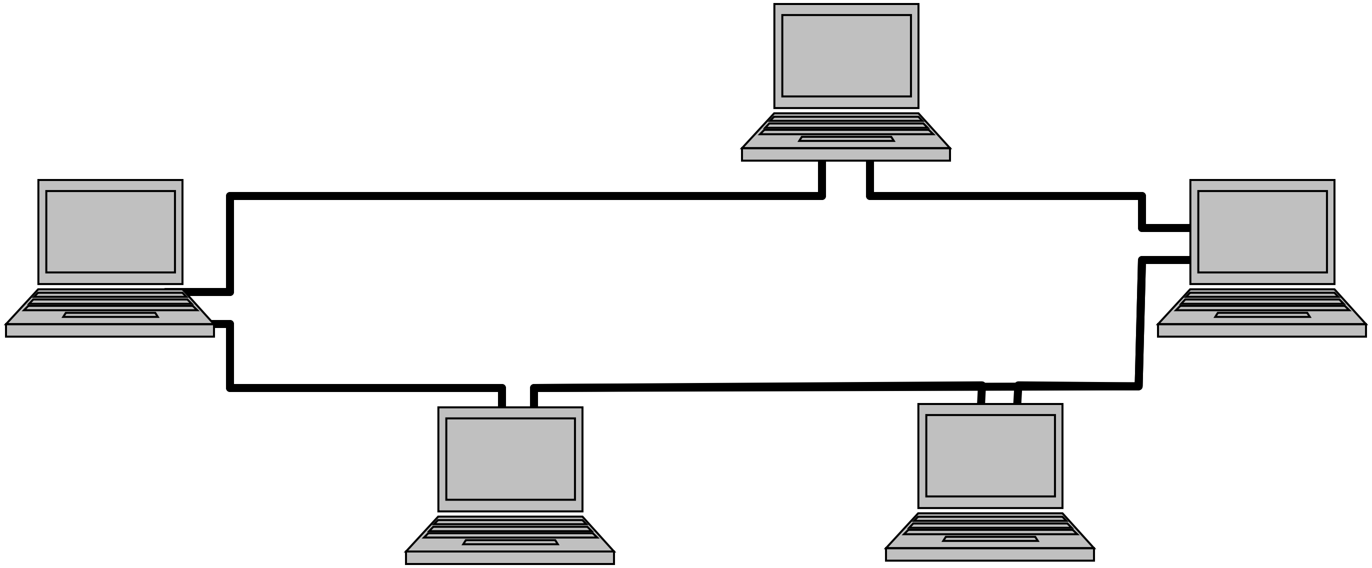


- **Pros:**
  - Little cabling
  - Easy to install
- **Cons:**
  - Difficult to modify
  - Difficult to isolate fault
  - Break in the bus cable stops all transmission

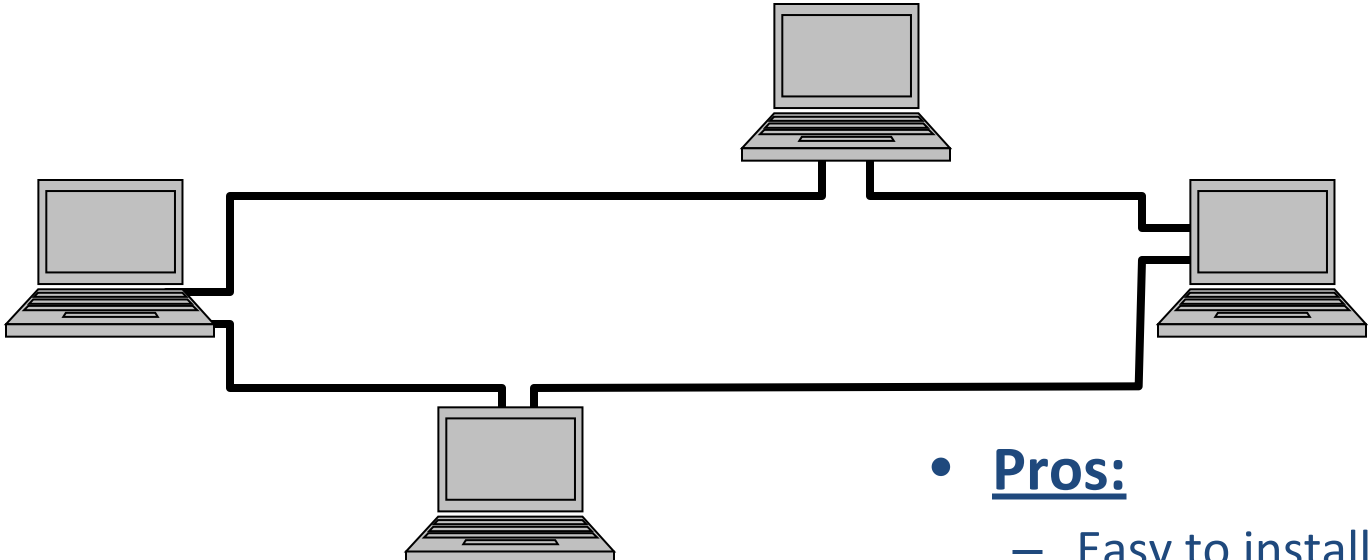
Ring Topology



Ring Topology



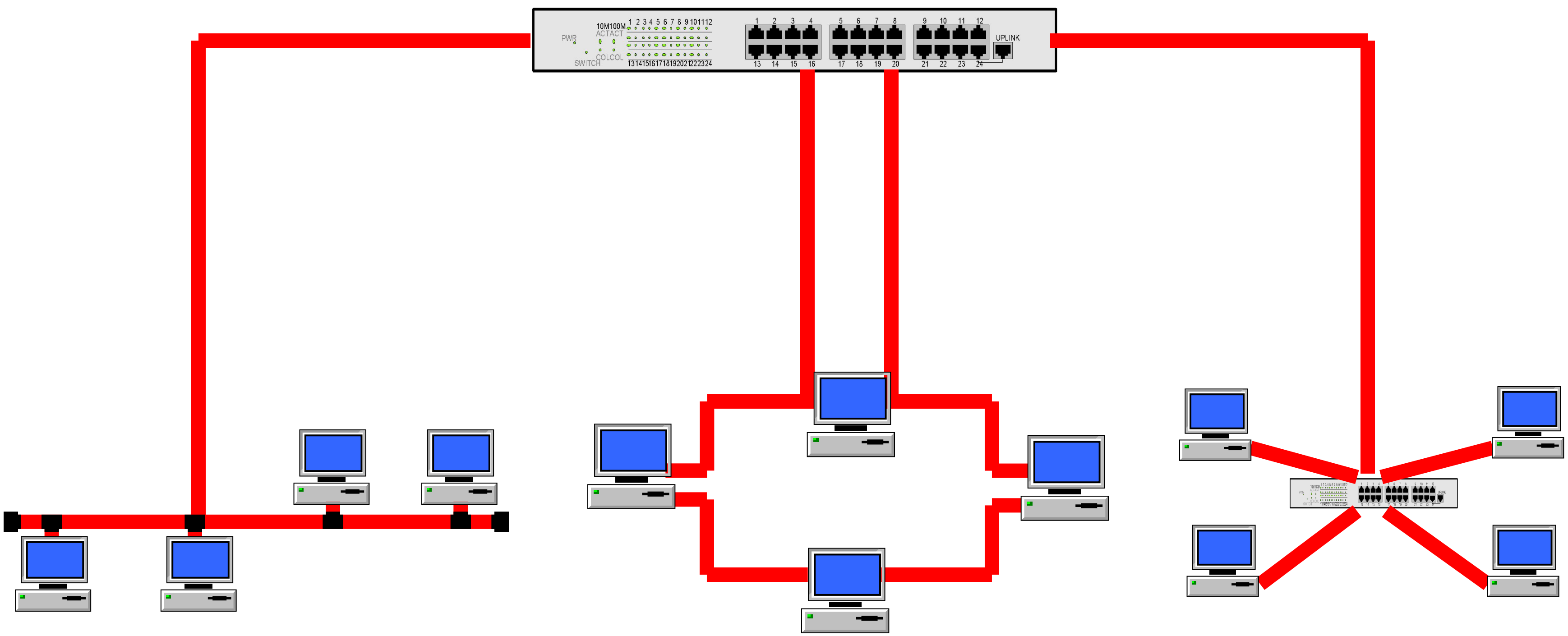
Ring Topology



- **Pros:**
  - Easy to install
  - Easy to identify fault

- **Cons:**
  - Delay in large ring
  - Break in the ring stops all transmission

Hybrid Topologies



Network Topology -Comparison

Parameters	Bus	Ring	Star	Mesh
Network Performance	Small	Small or Large	Small	Small
Cable Length Requirement	Less	Neither less nor	More	More
Traffic	Less	High	Medium	No
Dataflow Efficiency	More	Neither less nor more	More	More
Failure	Easy to solve	Difficult to solve	Easy to solve except hub/switch fails	Easy to solve
Cost	Low	High	High	High

Session 2

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Types of Packet Switched networks
  - Datagram networks and virtual Circuit networks
  - Structure of Circuit and Packet Switches
  - Comparisons
- Protocols and standards
- Standards Organizations, Forums and Regulatory agencies
- Internet Standards
- RFC

Switching

Switching

1 INTRODUCTION

2 CIRCUIT-SWITCHED NETWORK

3 PACKET-SWITCHING

INTRODUCTION TO SWITCHING

- Network connections rely on switches.

- Switches operate at the
  - ✔ Physical layer
  - ✔ Data link layer
  - ✔ Network layer

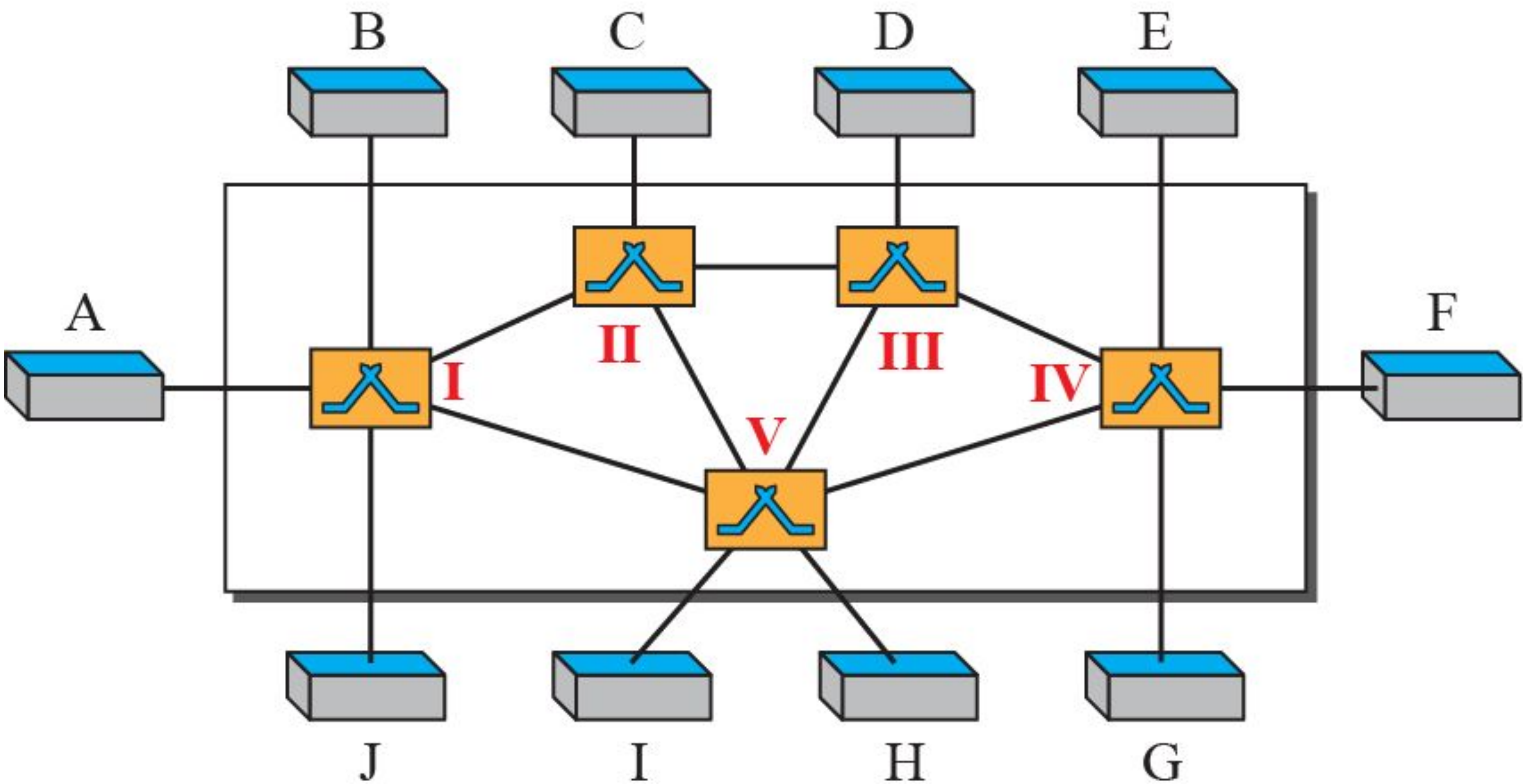


Figure 1: Switched network

Methods of Switching

- These are the two most common methods of switching:

  ✔ circuit switching
  ✔ packet switching

- Packet switching can further be divided into two subcategories,

  ✔ virtual-circuit approach and
  ✔ datagram approach

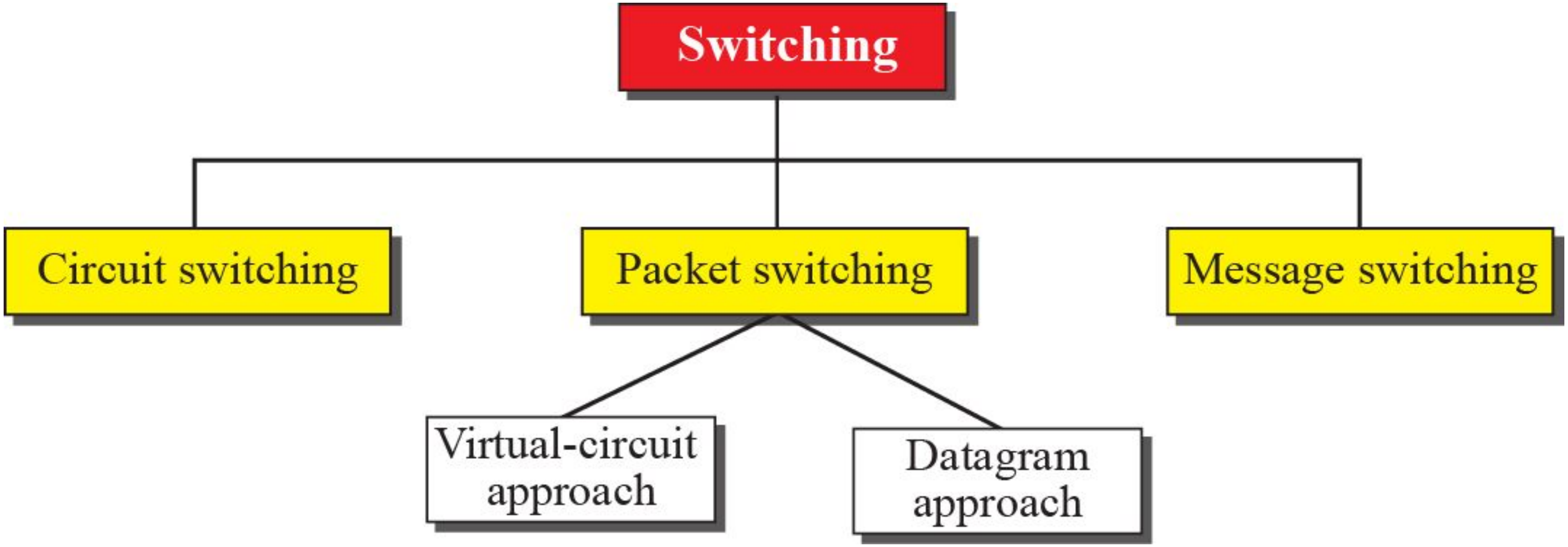


Figure 2: Taxonomy of switched networks

2 CIRCUIT-SWITCHED NETWORKS

- A circuit-switched network consists of a set of switches connected by physical links.

- Circuit-switches operate at the physical layer.

- A circuit-switched network creates a dedicated path to complete a link between the sender and receiver.

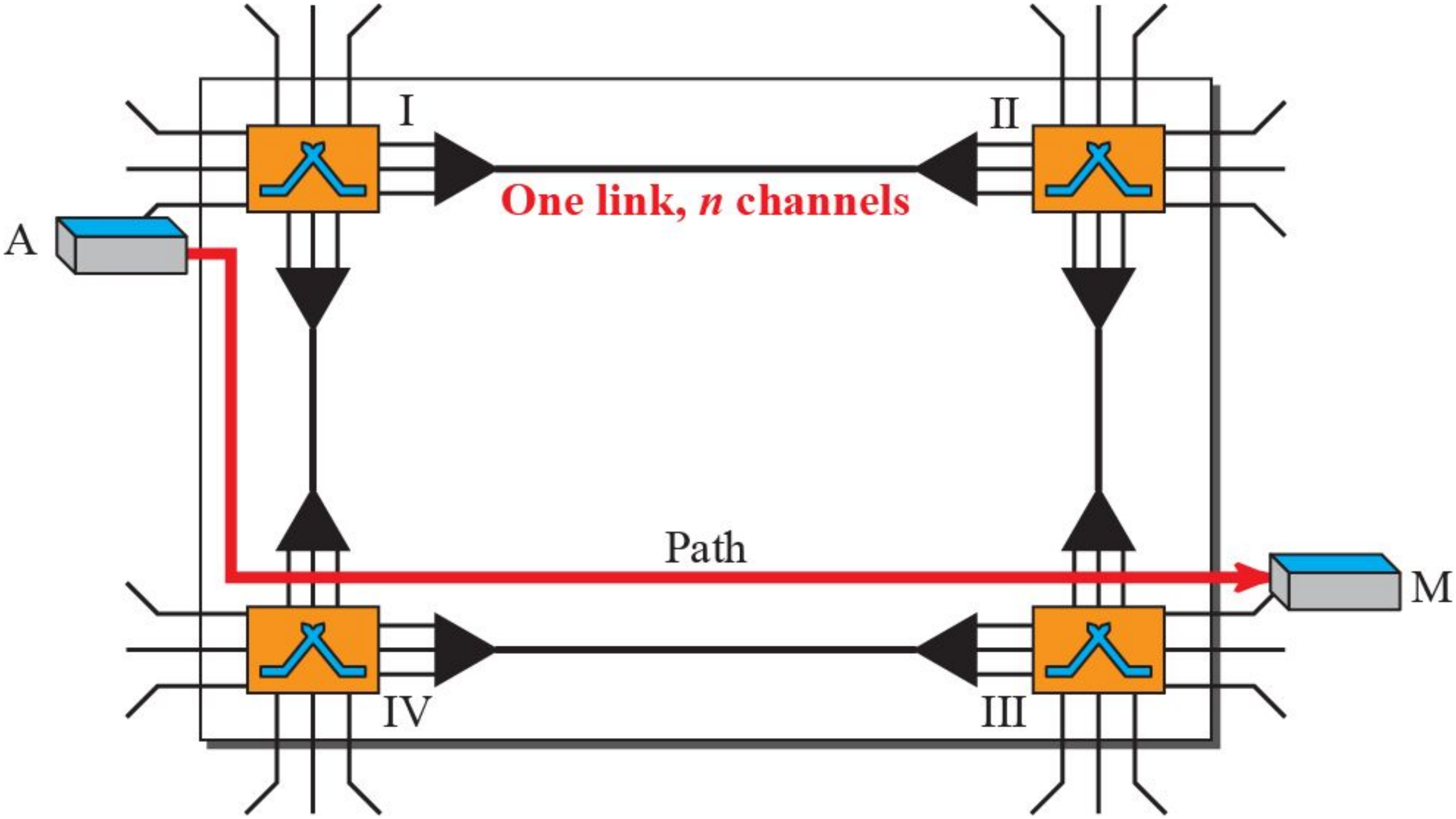


Figure 3: A trivial circuit-switched network

Example 1

As a trivial example, let us use a circuit-switched network to connect eight telephones in a small area. Communication is through 4-kHz voice channels. We assume that each link uses FDM to connect a maximum of two voice channels. The bandwidth of each link is then 8 kHz. Figure 4 shows the situation. Telephone 1 is connected to telephone 7; 2 to 5; 3 to 8; and 4 to 6. Of course the situation may change when new connections are made. The switch controls the connections.

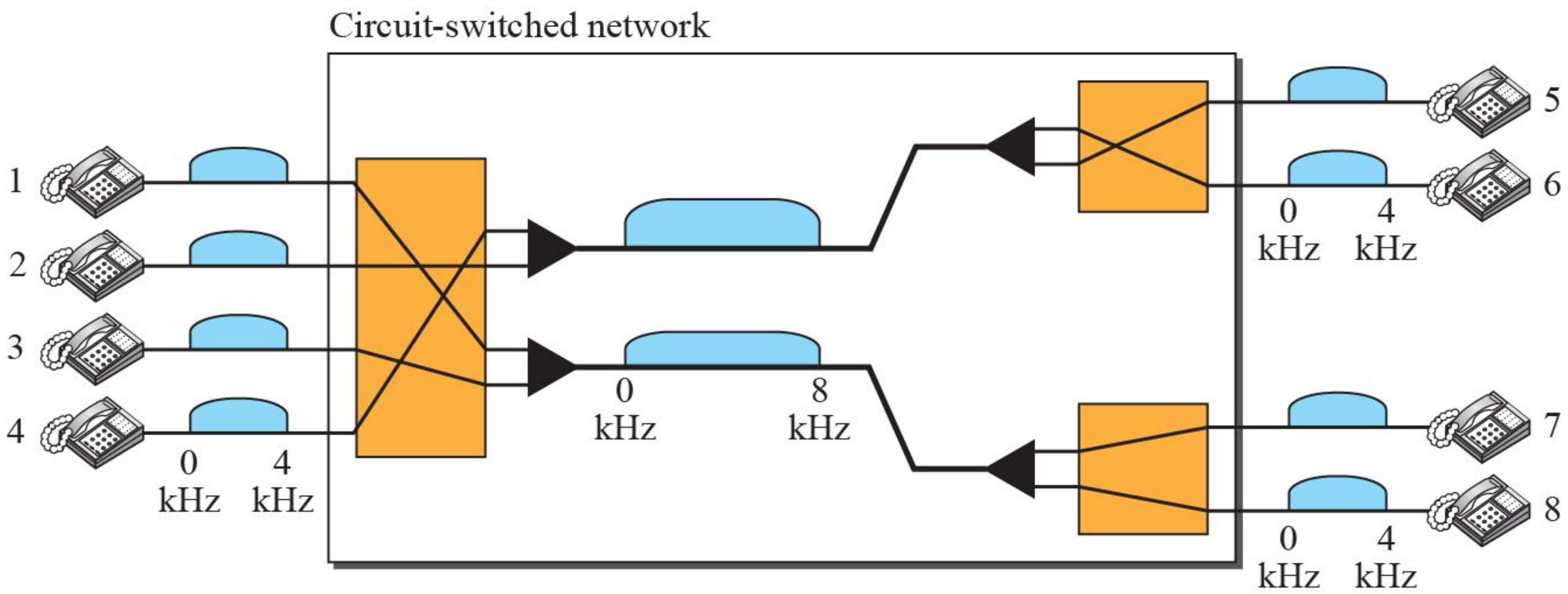


Figure 4: Circuit-switched network used in Example 1

Example 2

As another example, consider a circuit-switched network that connects computers in two remote offices of a private company. The offices are connected using a T-1 line leased from a communication service provider. There are two 4 × 8 (4 inputs and 8 outputs) switches in this network. For each switch, four output ports are folded into the input ports to allow communication between computers in the same office. Four other output ports allow communication between the two offices. Figure 5 shows the situation.

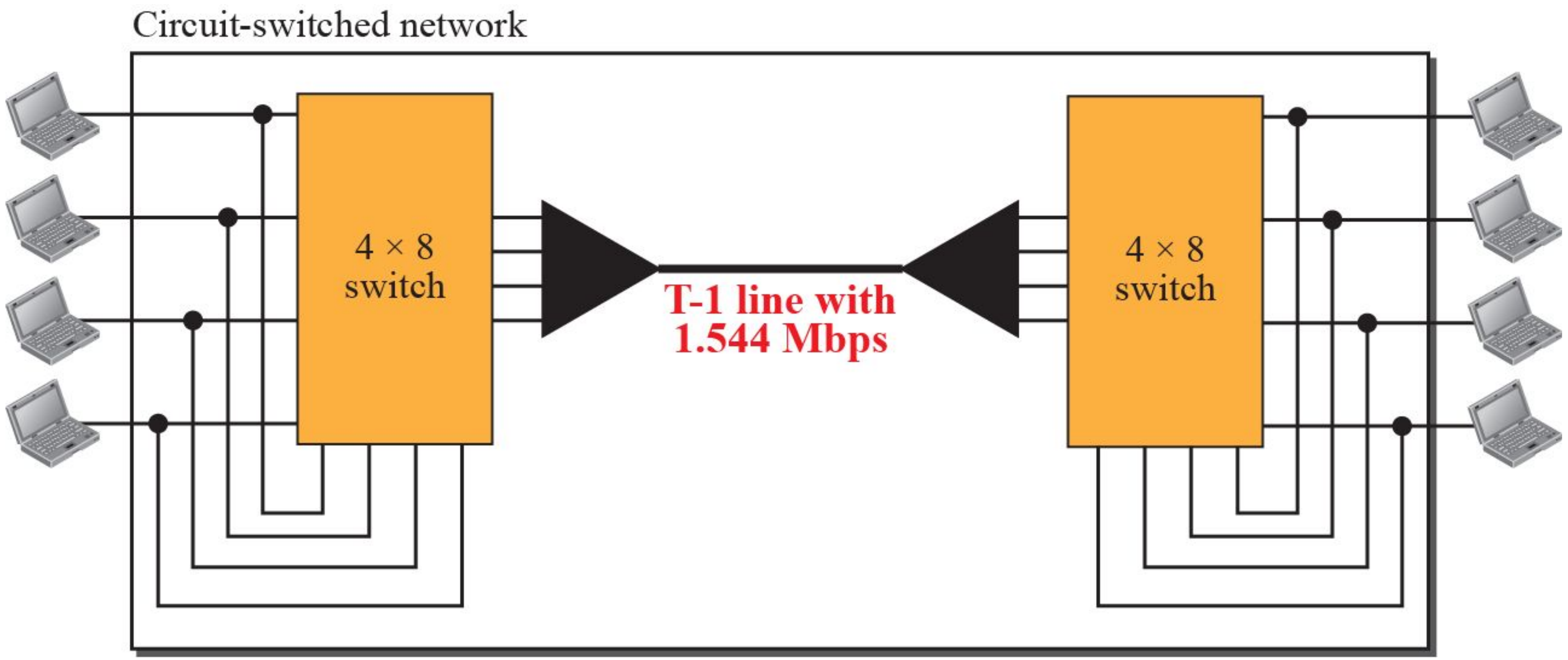


Figure 5: Circuit-switched network used in Example 2

Three Phases

The actual communication in a circuit-switched network requires three phases:

- connection setup,
- data transfer, and
- connection teardown.

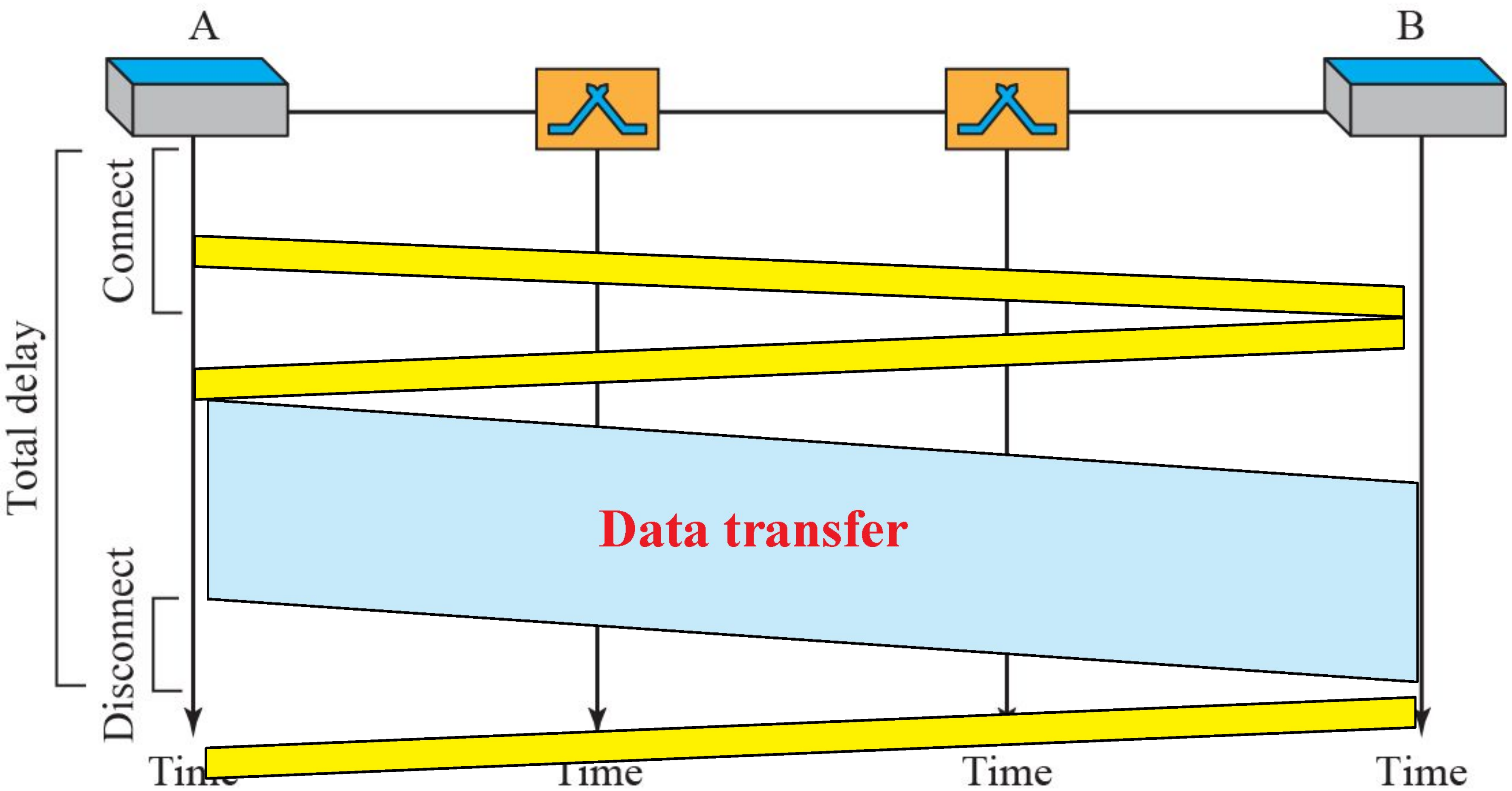


Figure 6 : circuit-switched network three phases

Efficiency

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection.

These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation.

Delay

During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

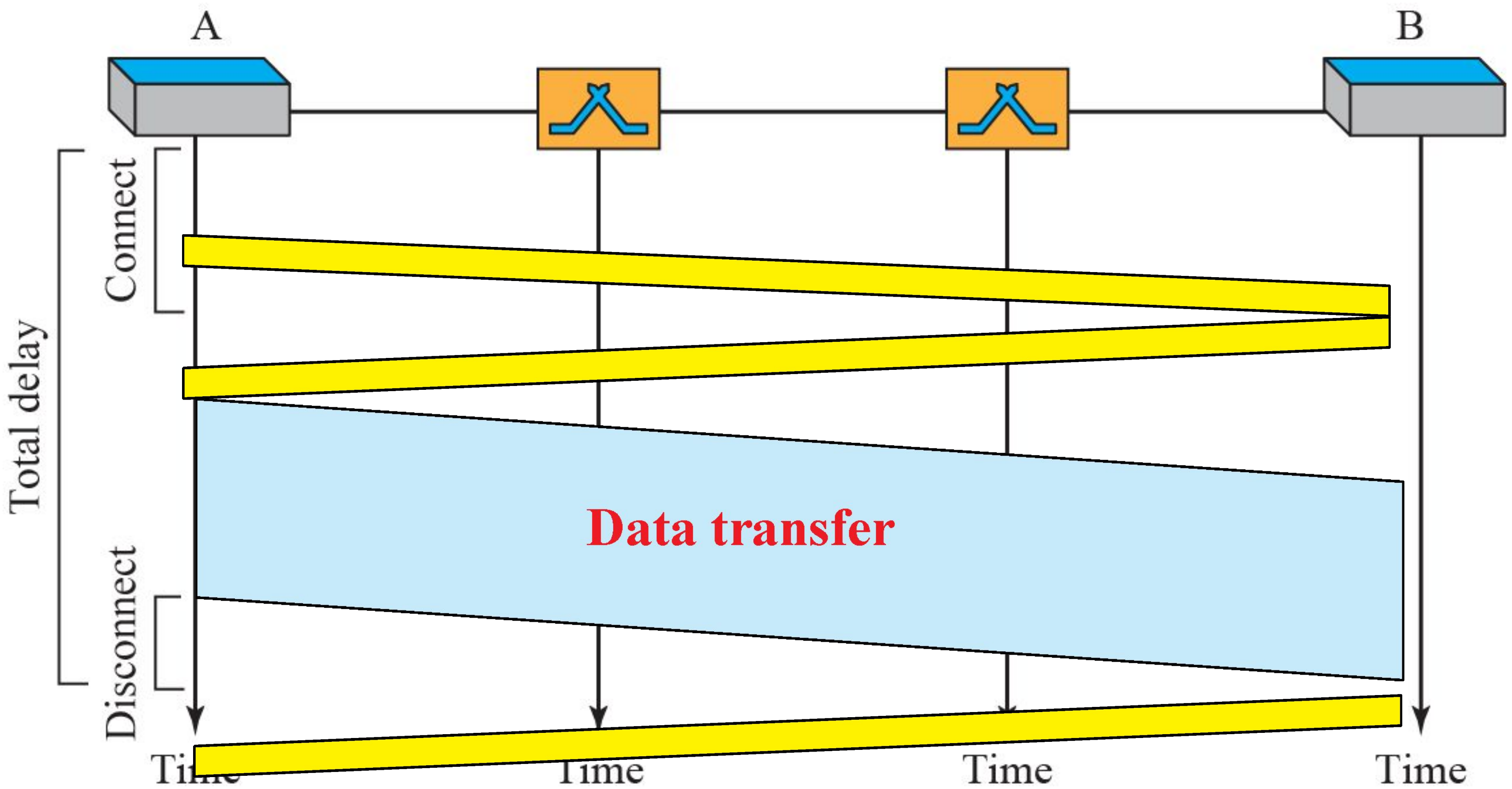


Figure 7: Delay in a circuit-switched network

3 PACKET SWITCHING

A packet-switched network divides the data into packets of fixed or variable size.

The size of the packet is determined by the network and the governing protocol.

Packet switched networks are classified as

a) Datagram Networks

b) Virtual circuit Networks

Datagram Networks

In a datagram network, each packet is treated independently of all others.

In a datagram network, each packet is treated independently of all others.

A datagram network operates at the Network layer.

Even if a packet is part of a multipacket transmission, the network treats packets as though they existed alone.

Datagram Networks

Even if a packet is part of a multipacket transmission, the network treats each packet as an independent message.

Each packet of one message can travel a different route towards their final destination.

Packets using this approach are referred to as datagrams.

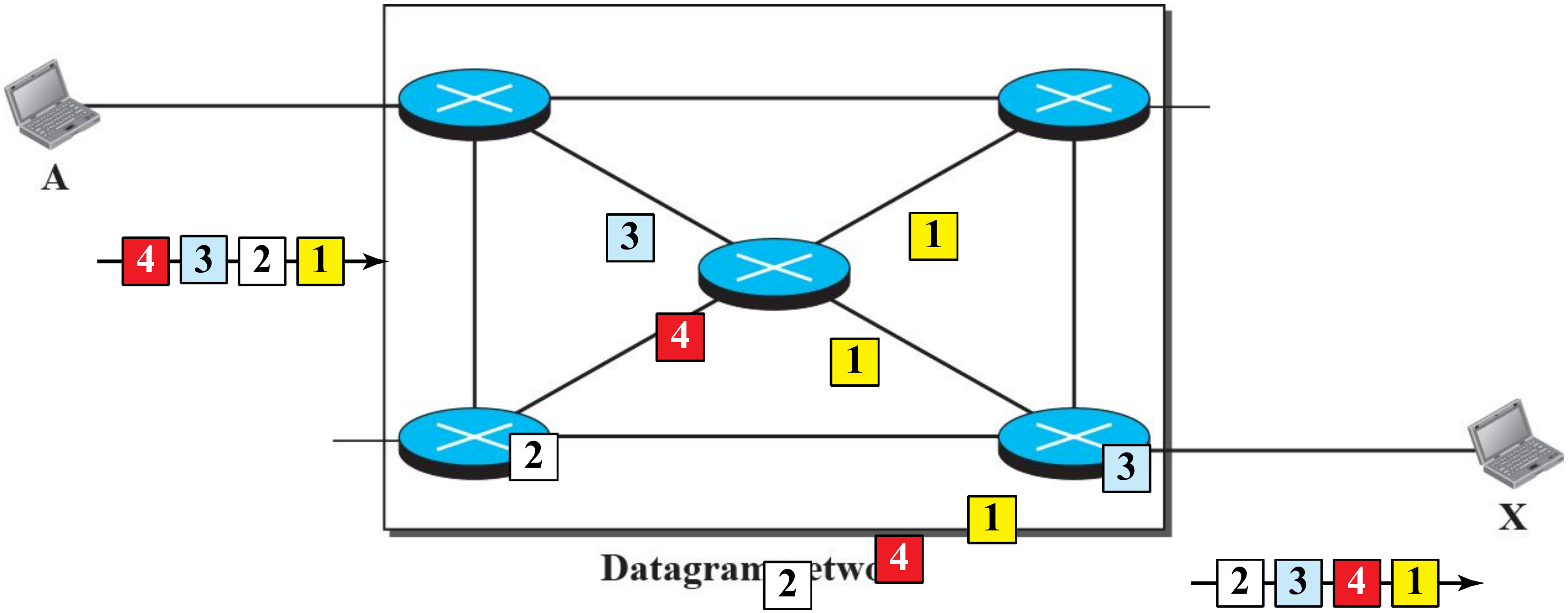


Figure 8: A Datagram network with four 3-level switches

Datagram Networks

All packets have a destination address in the header.

The packets have a destination address in the header.

The destination address for each datagram is used at a router to forward the message towards its final destination.

The packet header contains a sequence number in the header so it can be ordered at the destination.

Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3

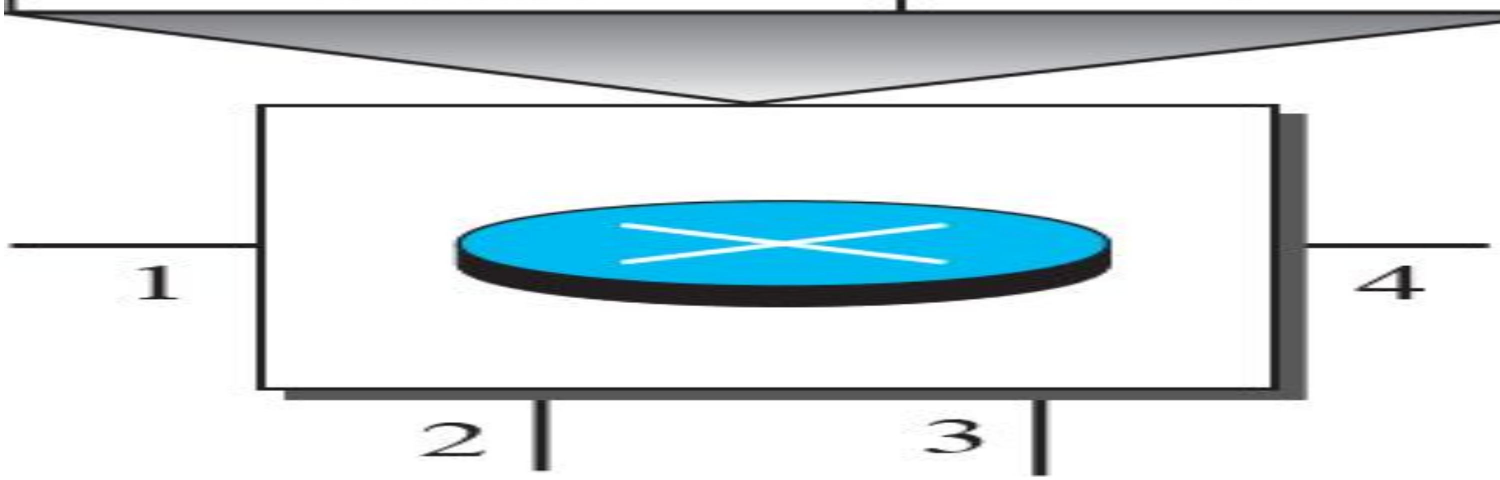


Figure 9: Routing table in a datagram network

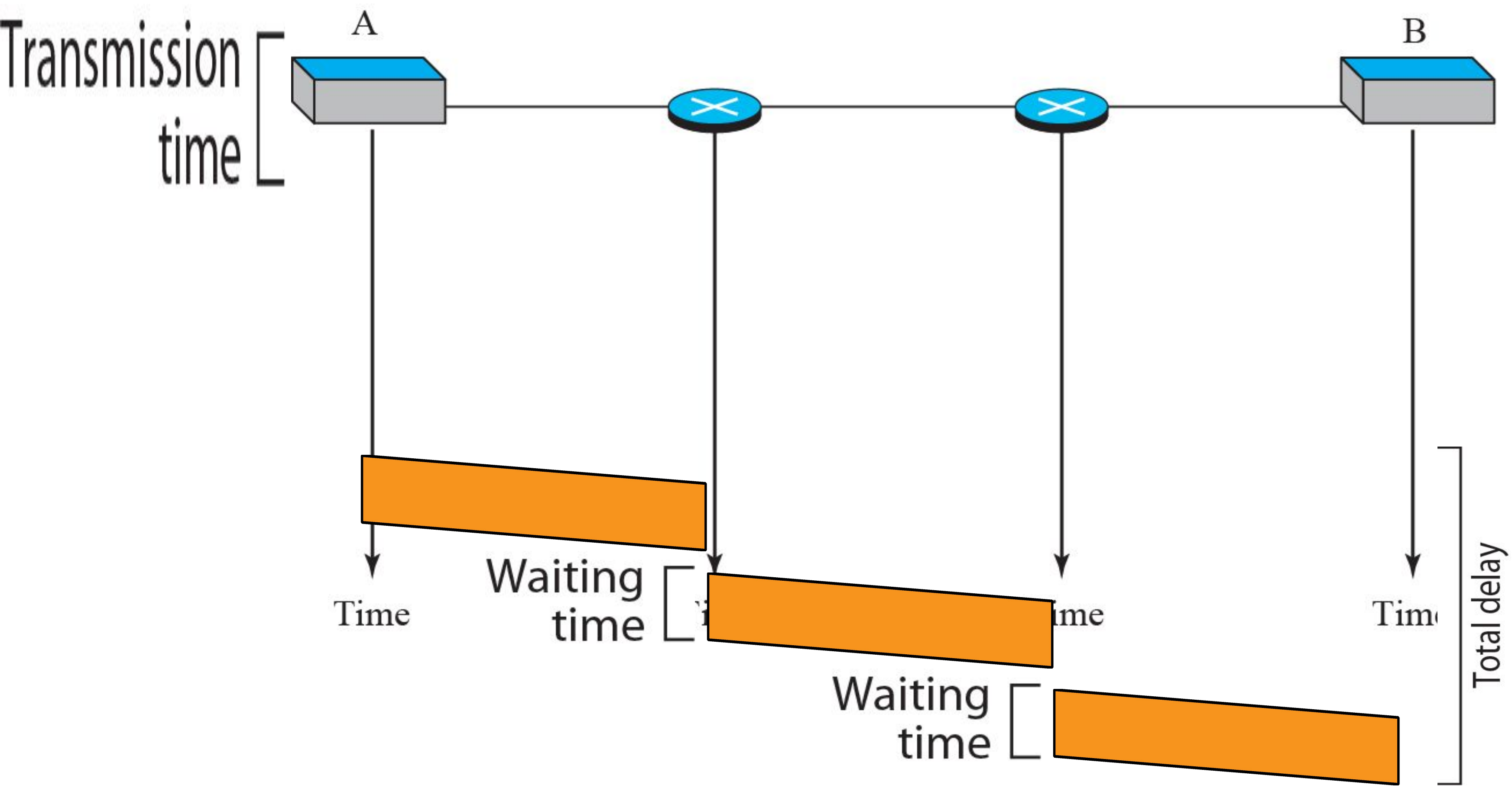


Figure 10: Delays in a datagram network (compare to next slide)

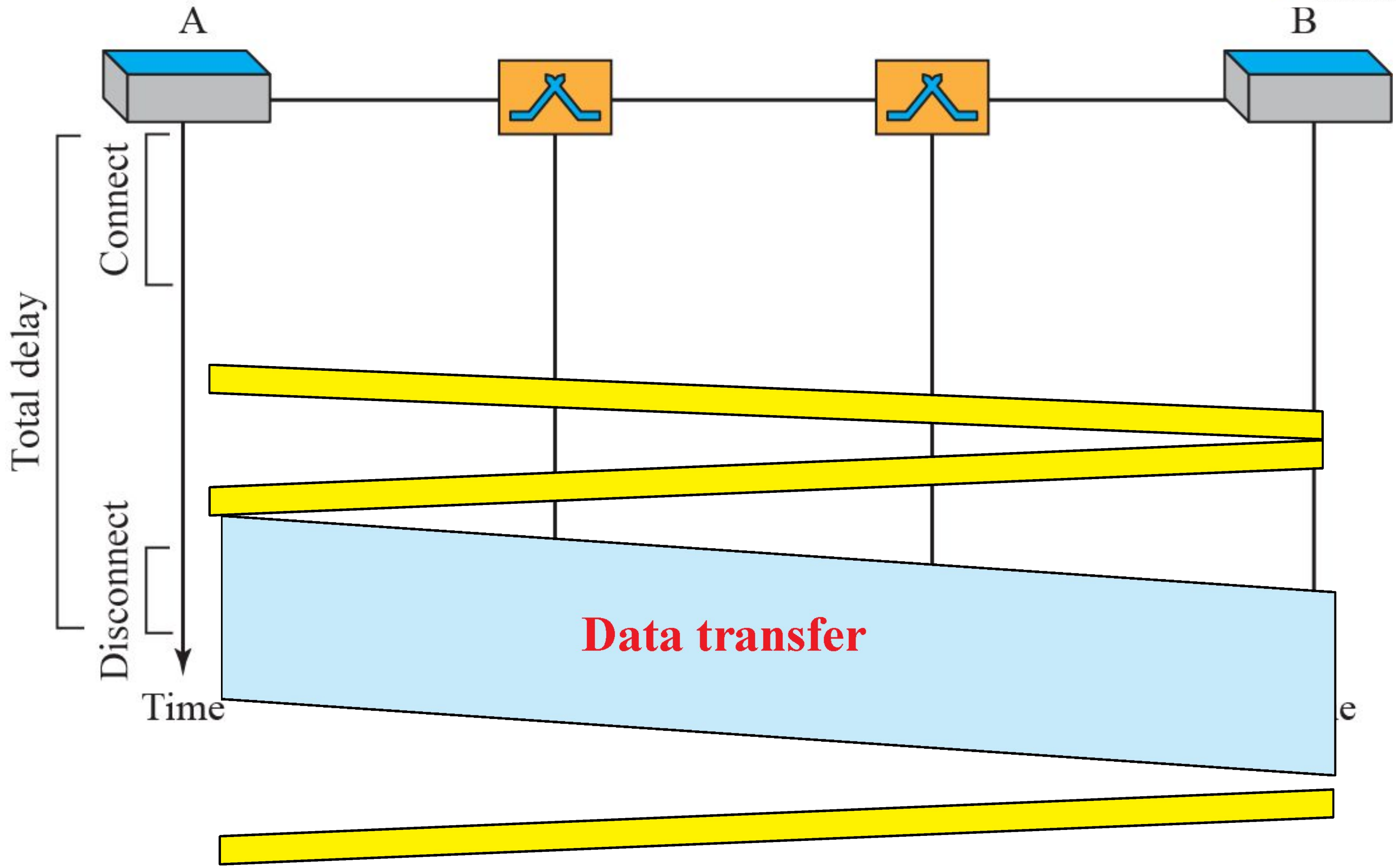


Figure 11: Compare the datagram network to the circuit-switched network

3.1 Virtual-Circuit Networks

A virtual-circuit network is a cross between a circuit-switched network and a datagram network.

The virtual-circuit shares characteristics of both.

The virtual-circuit network operates at the data-link layer.

The packets for a virtual circuit network are known as frames.

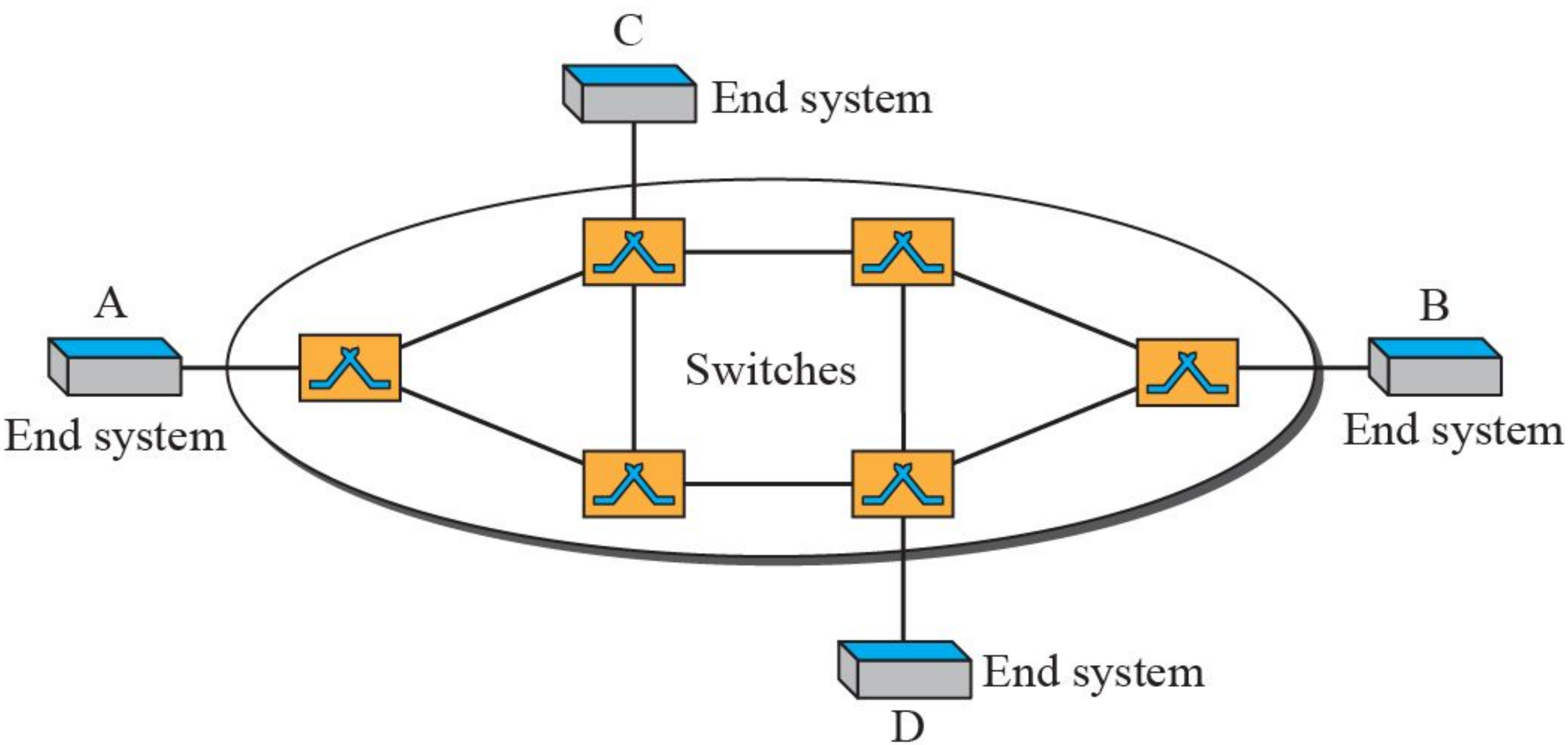


Figure12: Virtual-circuit network

3.2 Virtual-Circuit Networks

A virtual-circuit network uses a series of special temporary addresses known as <u>virtual circuit identifiers (VCI).</u>

The VCI at each switch, is used to advance the frame towards its final destination.

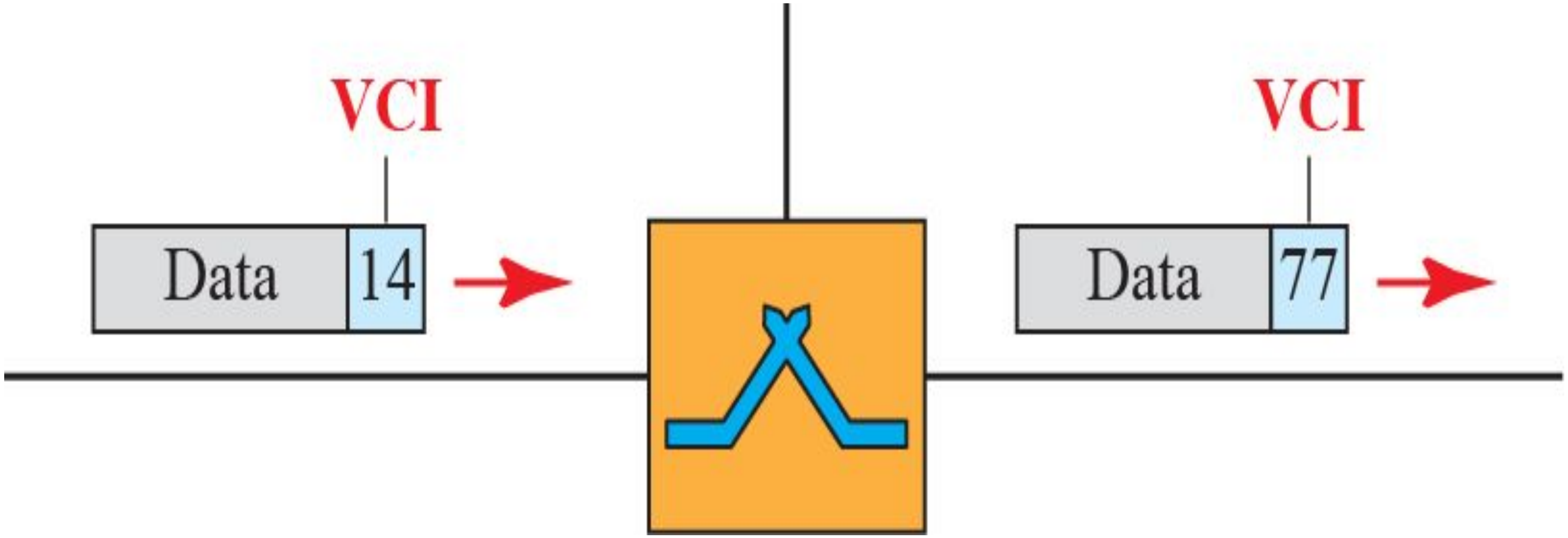


Figure 13: Virtual-circuit identifier (compare the VCI to a Datagram destination address)

3.2 Virtual-Circuit Networks

The switch has a table with 4 columns:

a) Inputs half

- Input Port Number
- Input VCI

b) Outputs half

- Output Port Number
- Output VCI

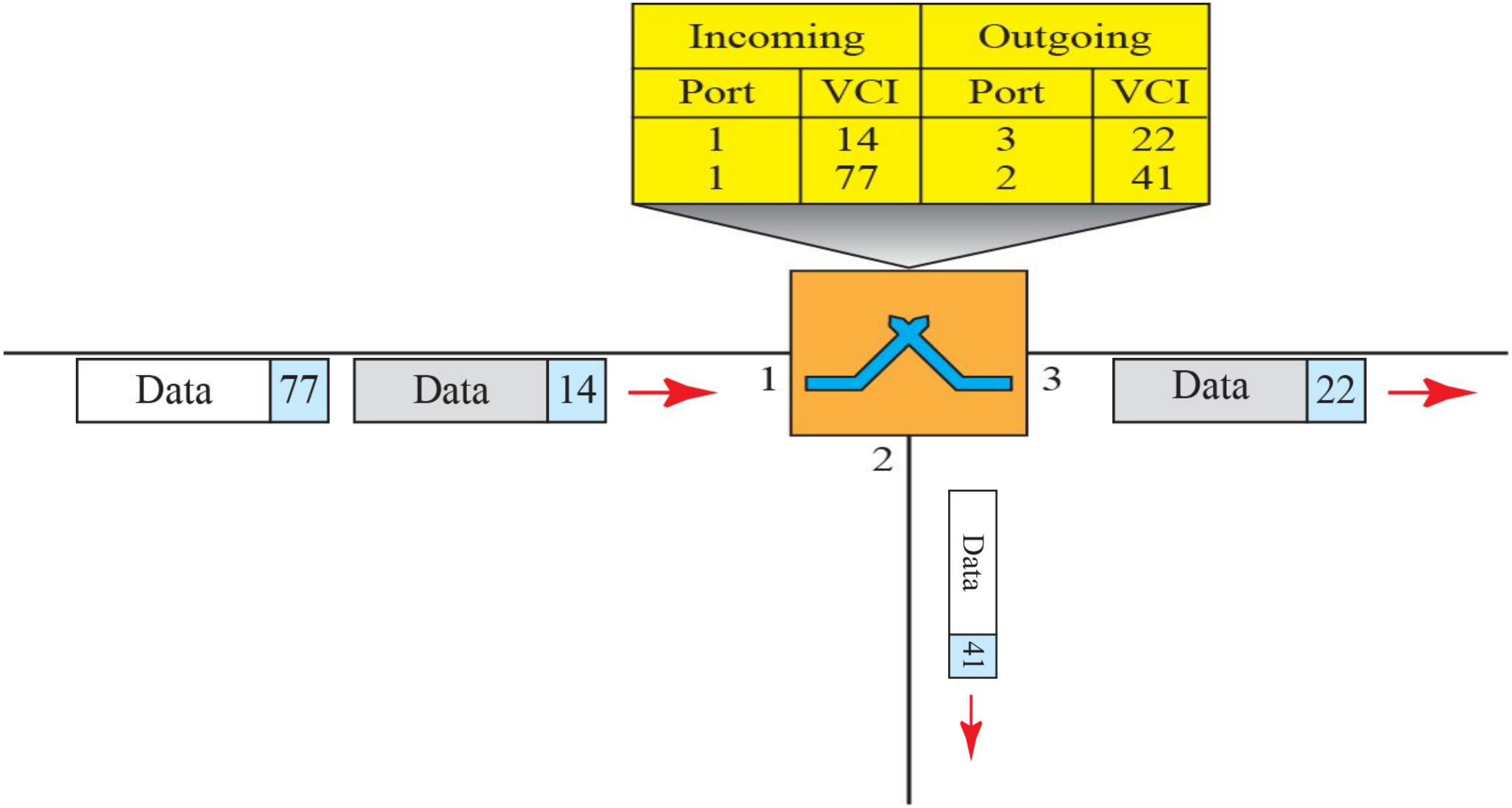


Figure14: Switch and table for a virtual-circuit network

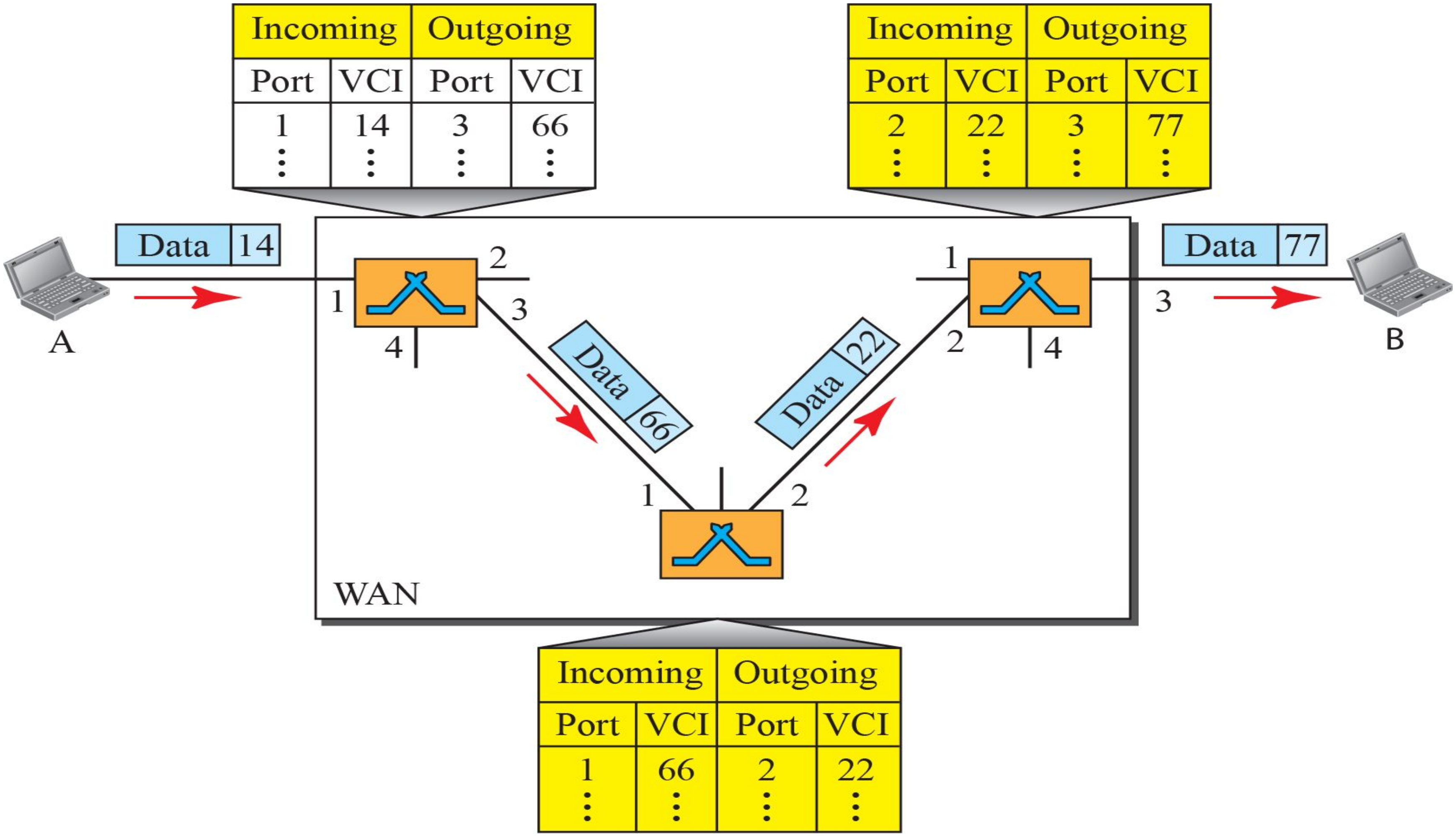


Figure15: Source-to-destination data transfer in a circuit-switch network

Virtual Circuit Networks

The VCN behaves like a circuit switched net because there is a setup phase to establish the VCI entries in the switch table.

There is also a data transfer phase and teardown phase.

.

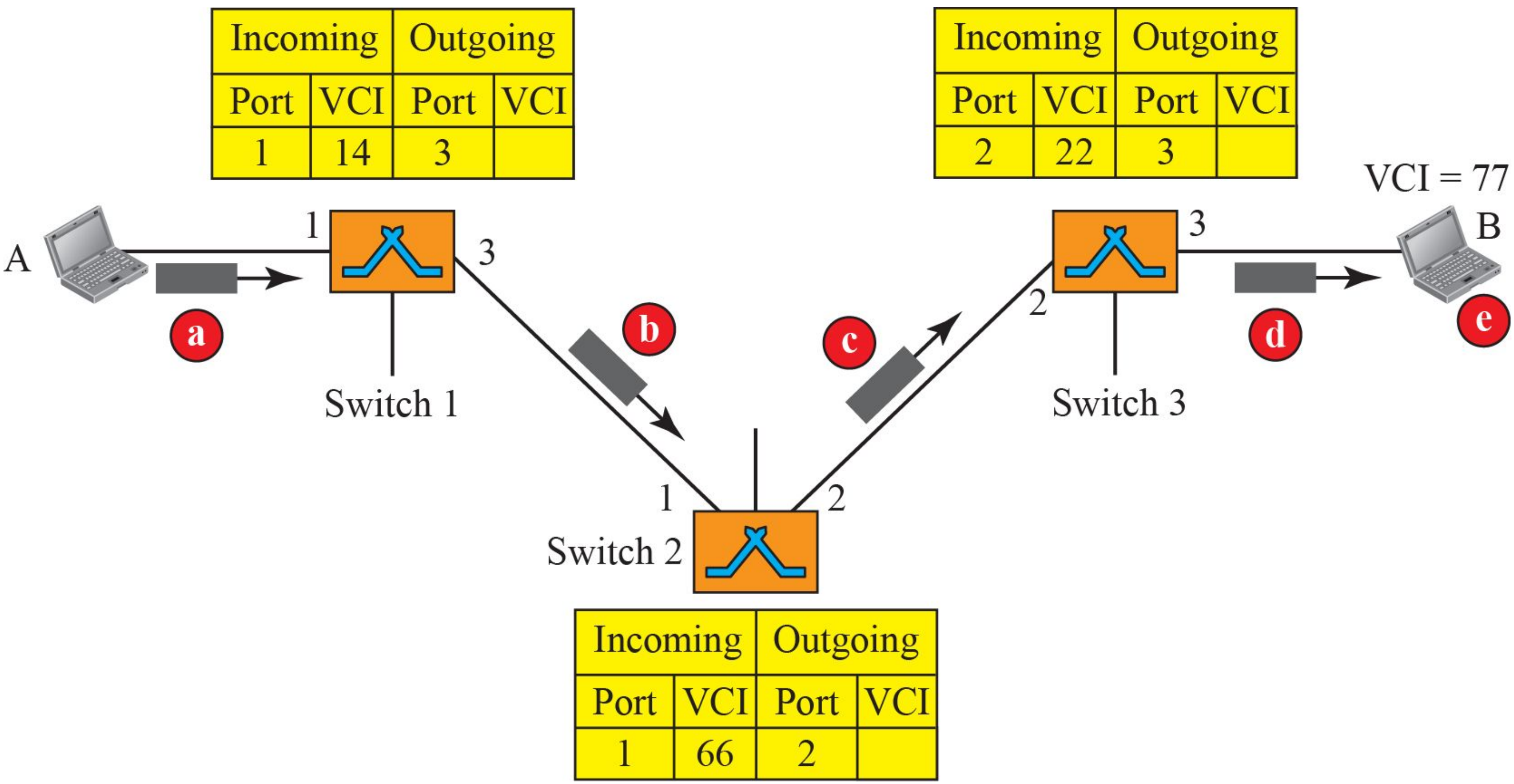


Figure16: Setup request in a virtual-circuit network

All nodes have a VCI

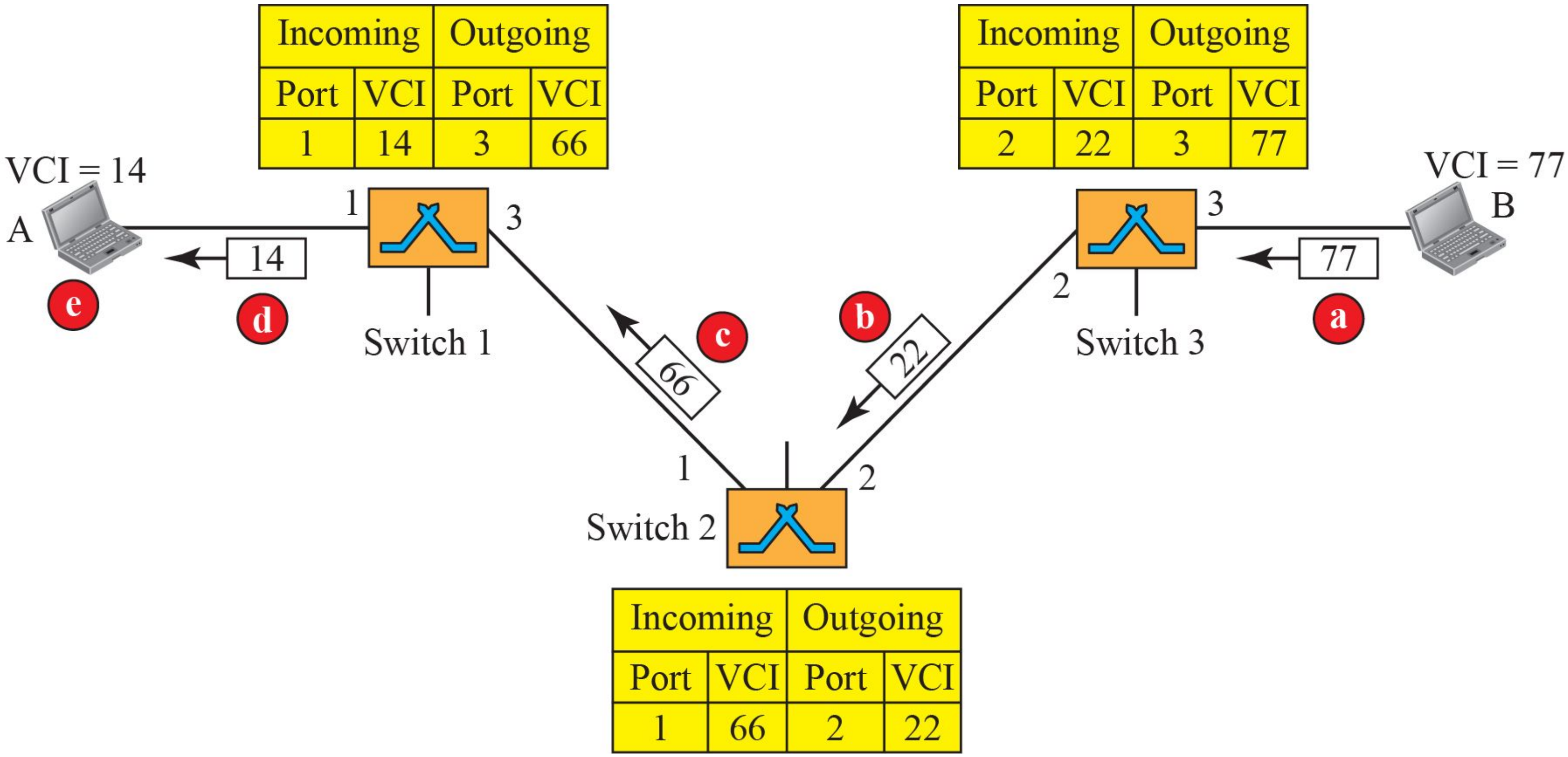


Figure17: Setup acknowledgment in a virtual-circuit network

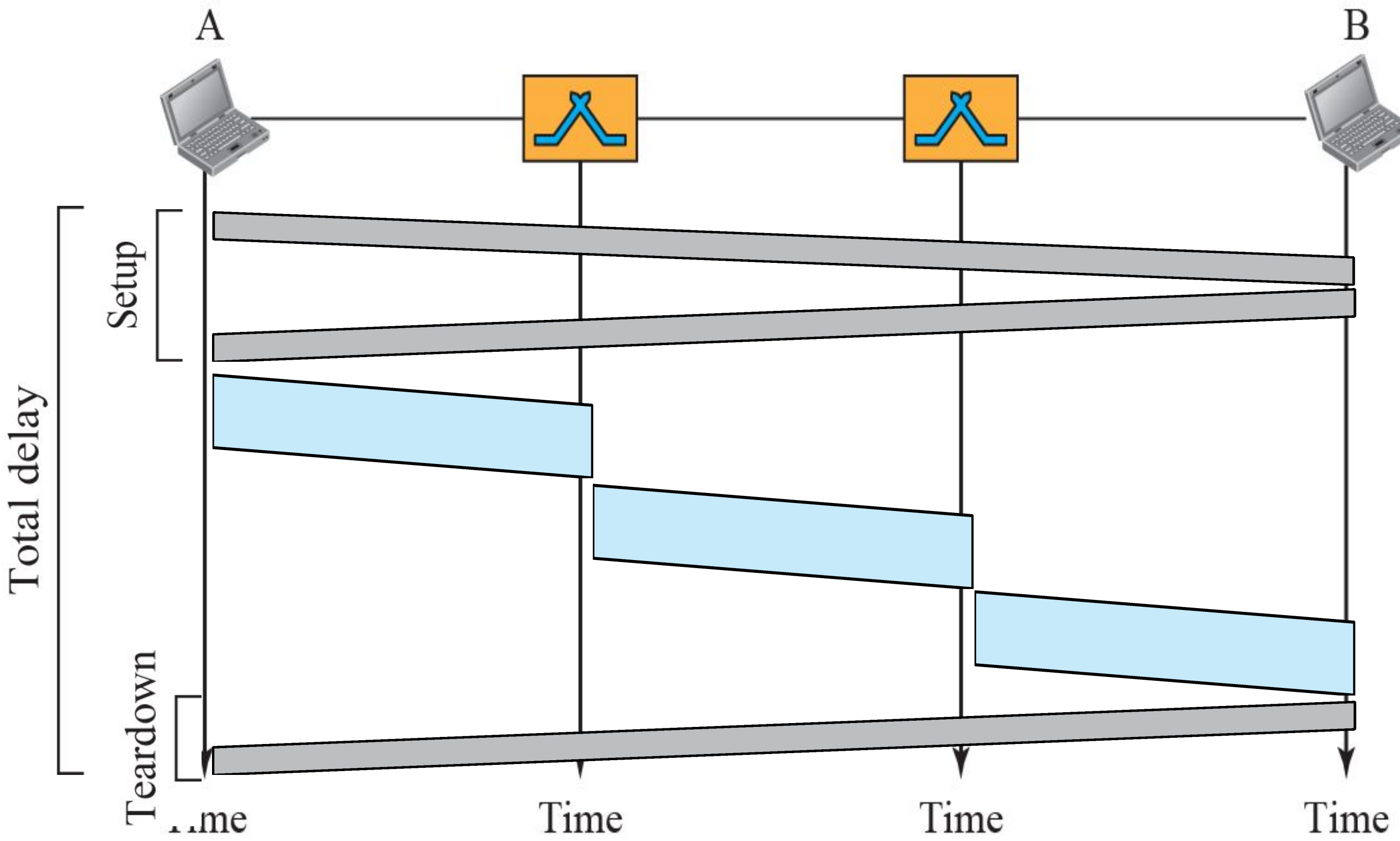


Figure 18: Delay in a virtual-circuit network

Comparison Chart

BASIS	CIRCUIT SWITCHING	PACKET SWITCHING
Orientation	Connection oriented.	Connectionless.
Purpose	Initially designed for Voice communication.	Initially designed for Data Transmission.
Flexibility	Inflexible, because once a path is set all parts of a transmission follows the same path.	Flexible, because a route is created for each packet to travel to the destination.
Order	Message is received in the order, sent from the source.	Packets of a message are received out of order and assembled at the destination.
Technology/Approach	Circuit switching can be achieved using two technologies, either Space Division Switching or Time-Division Switching.	Packet Switching has two approaches Datagram Approach and Virtual Circuit Approach.
Layers	Circuit Switching is implemented at Physical Layer.	Packet Switching is implemented at Network Layer.

Protocols & Standards

Protocols

Communicating worldwide will not be possible if there were no fixed **'standards'** that will govern the way user communicates for data as well as the way our devices treat those data

- For proper communication, entities in different systems must speak the same language

  - there must be mutually acceptable conventions and rules about the content, timing and underlying mechanisms

- Those conventions and associated rules are referred as "PROTOCOLS"

Protocols

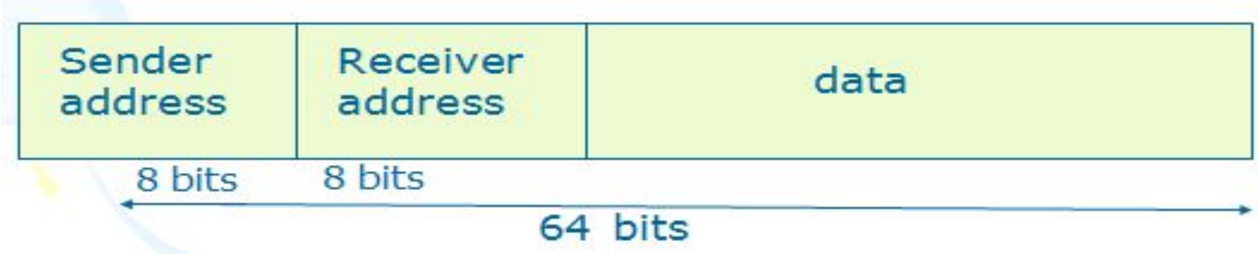
Network Protocols:

"Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures, designs or standards"

Elements of Protocols

i) Syntax: The structure or format of the data.

Eg. A simple protocol;



ii) Semantics: - Refers to the meaning of each section of bits.

- how is a particular pattern to be interpreted, and what action is to be taken based on that interpretation.

Eg. Does an address identify the route to be taken or the final of the message?

Elements of Protocols

iii) Timing

Refers to two characteristics:

a. When data to be sent

b. How fast it can be sent

Eg. If a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

Characteristics of protocol

a) Direct / indirect

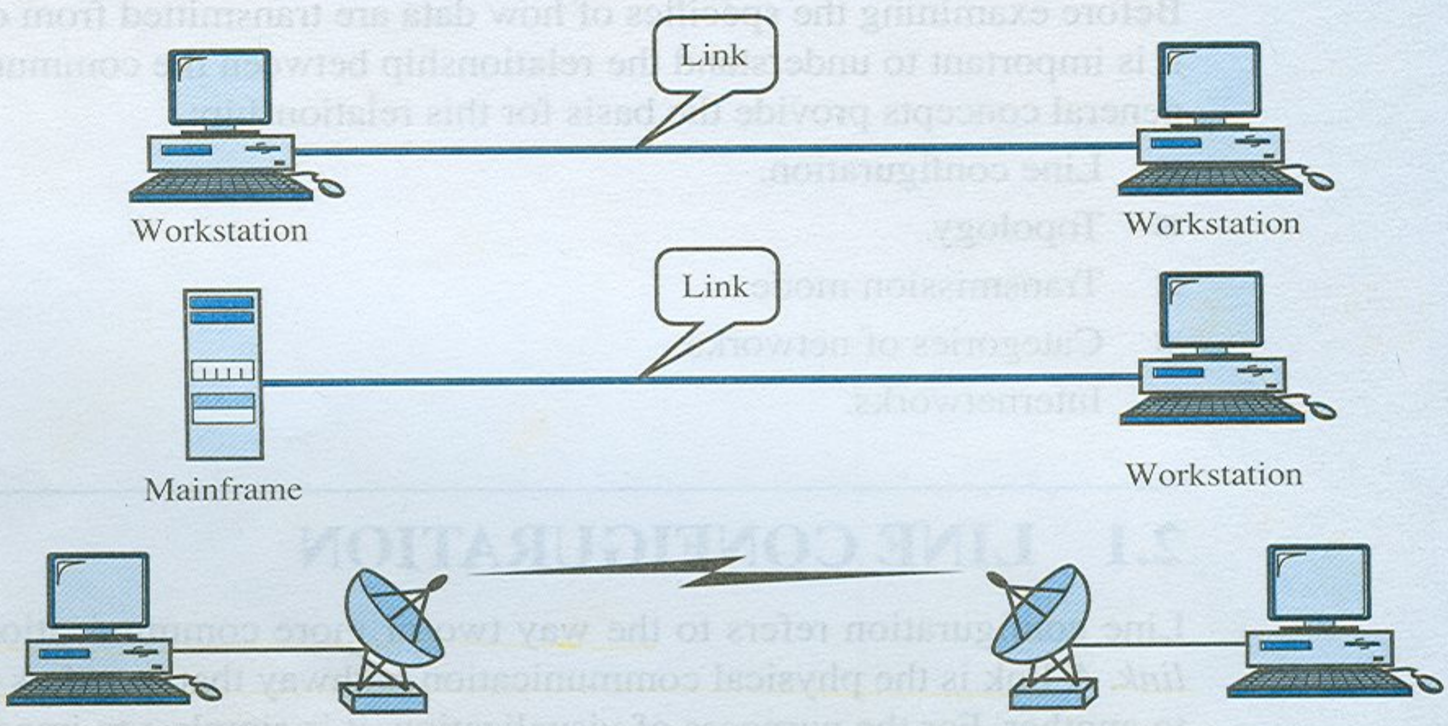
Communication between two entities maybe direct or indirect.

i) point-to-point link

- connection provides a dedicated link between two devices
- the entities in these systems may communicate directly that is data and control information pass directly between entities with no intervening active agent.

Characteristics of protocol

Figure 2.2 *Point-to-point line configuration*



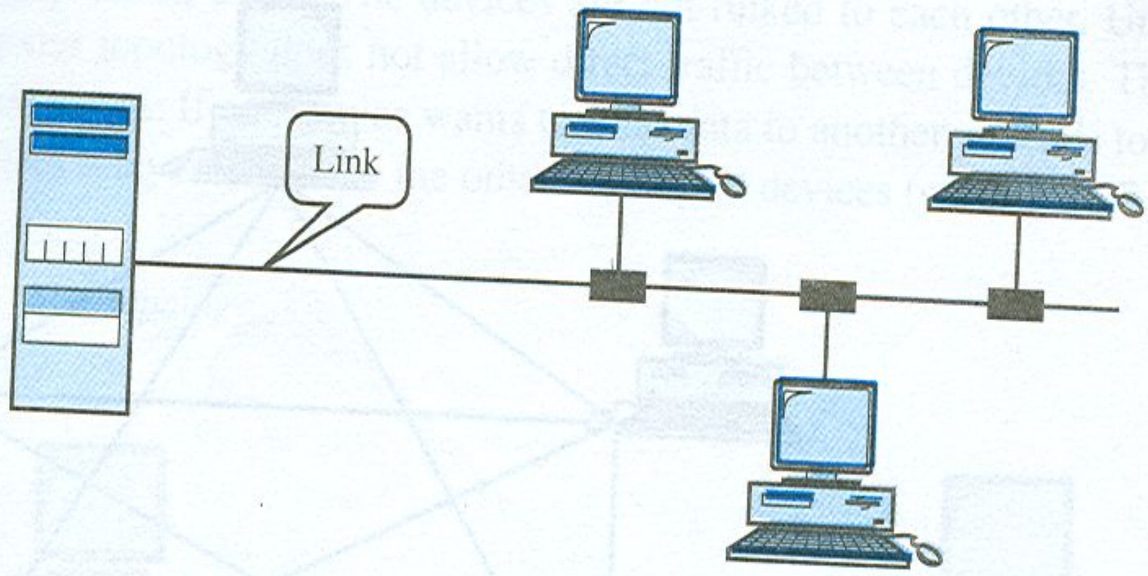
Characteristics of protocol

ii) **multipoint link**

- connection more than two devices can share a single link
- The entities must be concerned with the issue of access control and making the protocol more complex.

Characteristics of protocol

Figure 2.3 *Multipoint line configuration*



Characteristics of protocol

b) **Monolithic / structured**

- The task of communication between entities on different systems is too complex to be handled as a unit.

Eg. An electronic mail package running on two computers connected by a synchronous HDLC link. To be structured, the package would need to include all of the HDLC logic. If the connection were over a packet-switched network, the packaged would still need the HDLC logic to attach it to the network.

Characteristics of protocol

c) Symmetric / asymmetric

- Symmetric is the most use in protocol and involve communication between peer entities.
- Asymmetry may be dictated by the logic of an exchange (eg; client and a server process) the desire to keep one of the entities or systems as simple as possible.

Characteristics of protocol

d) Standard / nonstandard

- If ***K*** different kinds of information sources have to communicate with ***L*** types of information receivers, as many as ***K x L*** different protocols are needed without standards and a total of ***2 x K x L*** implementations are required
- If all systems shared a common protocol, only ***K+L*** implementations would be needed.

Standards

- Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and also in guaranteeing national and international interoperability of data and telecommunications technology and processes.
- They provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communication.

Standards

- Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" and "by regulation").
  - **De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are **de facto standards.** De facto standards are often established originally by manufacturers that seek to define the functionality of a new product or technology.
  - **De jure. De jure standards** are those that have been legislated by an officially recognized body.

Standards and Organizations

- Standards are developed through cooperation of standards creation committees, forums and government regulatory agencies.
- Some of the standards establishment Organizations are:
  - International Standards Organization (ISO) http://www.iso.org/
  - International Telecommunications Union-Telecommunication Standards Sector (ITU-T). http://www.itu.int/ITU-T
  - American National Standard Institute (ANSI).
  - Institute of Electrical and Electronics Engineers (IEEE). http://www.ieee.gov/
  - Electronic Industries Association (EIA).

Forums

- To facilitate the standardization process, many special-interest groups have developed **forums** made up of representatives from interested corporations.
- The forums work with universities and users to test, evaluate and standardize new technologies
- The forums are able to speed acceptance and use of those technologies in the telecommuni --cations community

Forums

The forums present their conclusions to the standards bodies. Some important forums for the telecommunications industry include the following:

- **Frame Relay Forum.** The Frame Relay Forum was formed by digital equipment Corporation, Northern Telecom, Cisco, and StrataCom to promote the acceptance and implementation of frame relay. Today, it has around 40 members representing North America, Europe, and the Pacific rim. Issues under Review include flow control. encapsulation, translation, and multicasting. the forum's results are submitted to the ISO.
- **ATM Forum.** http://www.atmforum.com/ The ATM Forum provides acceptance and use of Asynchronous Transfer Mode (ATM) technology. The ATM Forum is made up of Customer Premises Equipment (e.g., PBX systems) vendors and Central Office (e.g., telephone exchange) providers. It is concerned with the standardization of service to ensure interoperability.

Regulatory Agencies

- All communications technology is subject to regulation by government agencies such as Federal Communication Commission (FCC) in the United States.
- The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications.

  Federal Communications Commission (FCC)

  http://www.fcc.gov/
- The Federal Communications Commission (FCC) has authority over interstate and international commerce as it relates to communications

RFCs

- RFCs go through maturity levels and are categorized according to their requirement level
  - **Maturity Levels**
    An RFC, during its lifetime, falls into one of six **maturity levels:** proposed standard, draft standard, Internet standard, historic, experimental, and Informational.
  - **Proposed Standard.** A proposed standard is a specification that is stable, well understood, and of sufficient interest to the internet community**.** At this level, the specification is usually tested and implemented by several different programs.

RFCs

- **Draft Standard.** A proposed standard is elevated to draft standard status after atleast two successful independent and interoperable implementations. Barring difficulties, a draft standard, with modifications if specific problems are encountered, normally becomes an internet standard.
- **Internet Standard.** A draft standard reaches Internet standard after demonstrations of successful implementation.
- **Historic.** The Historic RFCs are significant from a historical perspective. They either have been superseded by later specifications or have never passed the necessary maturity levels to become an internet standard.
- **Experimental.** An RFC classified as experimental describes work related to an experimental situation that does not affect the operation of the internet. Such an RFC should not be implemented in any functional Internet service

RFCs

– **Informational.** An RFC classified as informational contains general, historical, or tutorial information related to the Internet. It is usually written by someone in a non-Internet organization, such as a vendor.

- **RFC Requirement Levels**
  RFCs are classified into 5 Requirement Levels: required, recommended, elective, limited use and not recommended.

RFCs

- **Required**. An RFC is labeled *required* if it must be implemented by all Internet systems to achieve minimum conformance. For example, IP and ICMP are required protocols.
- **Recommended**. An RFC labeled *recommended* is not required for minimum conformance; it is recommended because of its usefulness. For example, FTP and TELNET are recommended protocols.
- **Elective**. An RFC labeled *elective* is not required and not recommended. However, a system can use it for its own benefit.
- **Limited Use**. An RFC labeled *limited use* should be used only in limited situations. Most of the experimental RFCs fall under this category.
- **Not recommended**. An RFC labeled *not recommended* is inappropriate for general use. Normally a historic (obsolete) RFC may fall under this category.

Protocol Suite

- A set of cooperating network protocols is called a protocol suite.
- For example, the TCP/IP suite includes numerous protocols across layers -- such as the data, network, transport and application layers -- working together to enable internet connectivity.

Types of Network Protocols

Networks have three types of protocols

1. **Communication**, such as Ethernet
2. **Management**, such as the Simple Mail Transfer Protocol (SMTP); and
3. **Security**, such as Secure Shell (SSH)

Falling into these three broad categories are thousands of network protocols that uniformly handle an extensive variety of defined tasks

Implementation of Protocols

- They are coded within software, either
  - a part of the computer's operating system (OS) or
  - as an application, or
  - implemented within the computer's hardware.
- Most modern OSs possess **built-in software** services that implement some network protocols
- Applications, such as **web browsers**, implement protocols in the form of software libraries
- TCP/IP and routing protocol support is implemented in **direct hardware** for enhanced performance

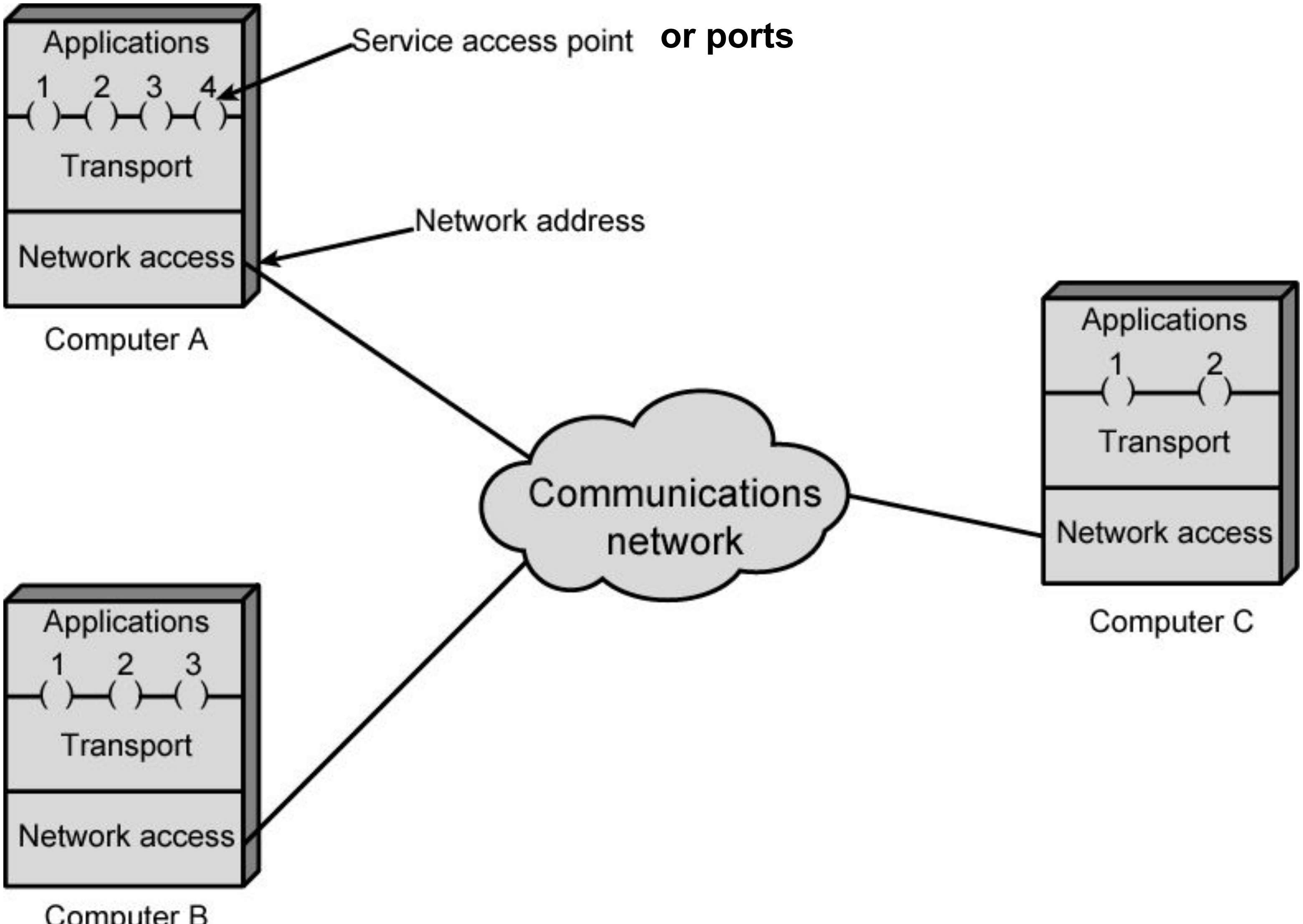
Session 5

- OSI Model - Layered architecture
  - Interfaces between layers
  - Encapsulation
  - Functions of Each Layer in the OSI Model

General protocol architecture principles

- **Layered structure**
  - Protocol stack
- Each layer provides services to upper layer; expect services from lower one
  - Layer interfaces should be well-defined
- **Peer entities communicate using their own protocol**
  - **peer-to-peer protocols**
  - **independent of protocols at other layers**
  - **if one protocol changes, other protocols should not get affected**

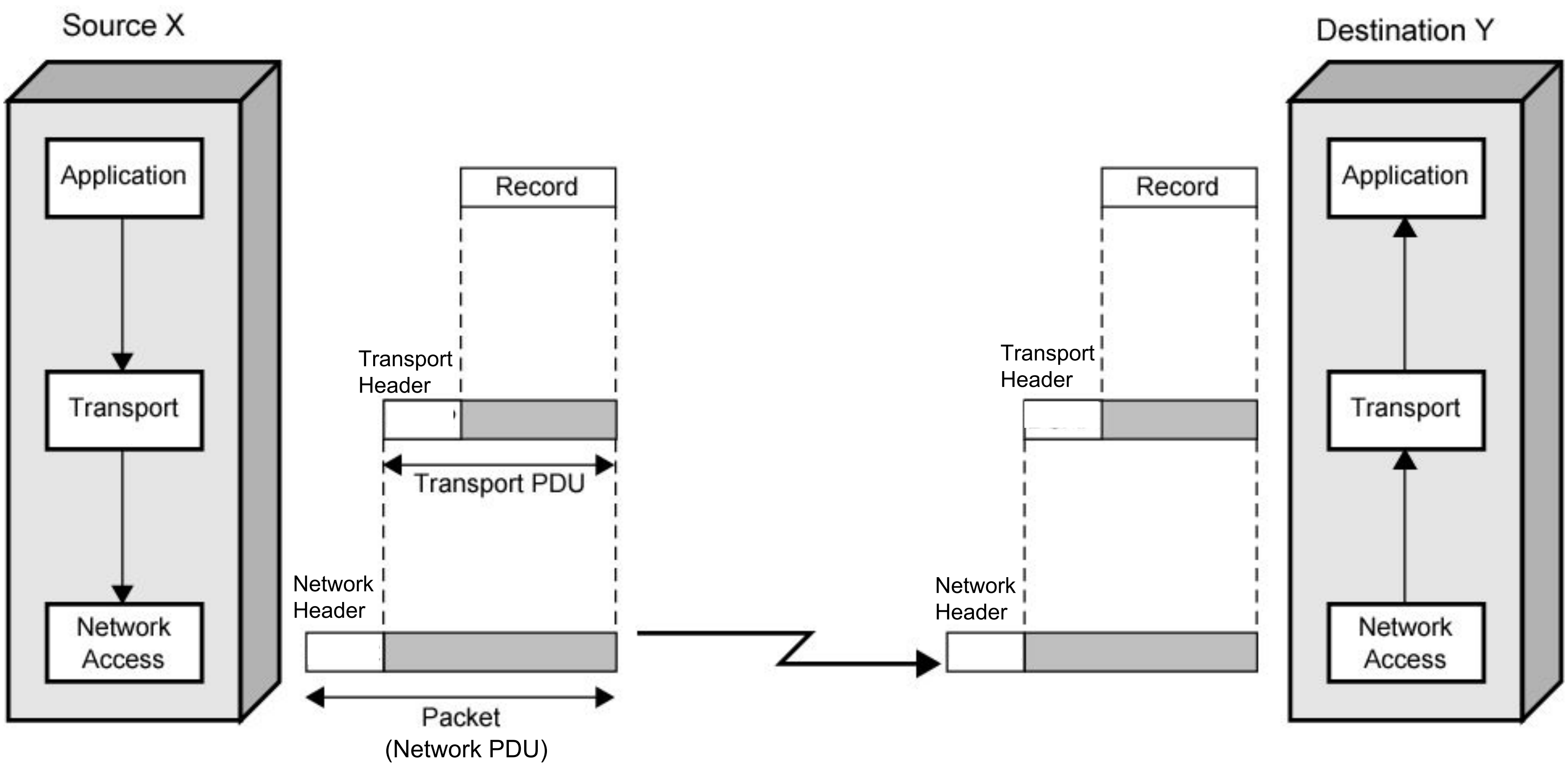
Protocol Architectures and Networks



Protocol Data Unit (PDU)

- User data is passed from layer to layer
- Control information is added/removed to/from user data at each layer
  - Header (and sometimes trailer)
  - each layer has a different header/trailer
- Data + header + trailer = PDU (Protocol Data Unit)
  - This is basically what we call *packet*
  - each layer has a different PDU

Operation of a Protocol Architecture



Standard Protocol Architectures

- Common set of conventions
- Nonstandard vs. standard protocols
  - Nonstandard: K sources and L receivers lead to K*L different protocols
  - If common protocol used, we design only once
- Products from different vendors interoperate
  - Customers do not stick to a specific vendor
  - If a common standard is not implemented in a product, then that product’s market is limited; customers like standard products

Standard Protocol Architectures

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Two approaches (standard)
  - OSI Reference model
    - never used widely
    - but well known
  - TCP/IP protocol suite
    - Most widely used
- Another approach (proprietary)
  - IBM’s Systems Network Architecture (SNA)

OSI Reference Model

- Open Systems Interconnection (OSI)
- Reference model
  - provides a general framework for standardization
  - defines a set of layers and services provided by each layer
  - one or more protocols can be developed for each layer
- Developed by the International Organization for Standardization (ISO)
  - also published by ITU-T (International Telecommunications Union)

OSI Reference Model

- A layered model
  - Seven layers – seven has been presented as the optimal number of layer
- Delivered too late (published in 1984)!
  - by that time TCP/IP started to become the de facto standard
- Although no OSI-based protocol survived, the model is still valid (in the textbooks)
  - For Data Link Layer (that we will see later) OSI protocols are still valid

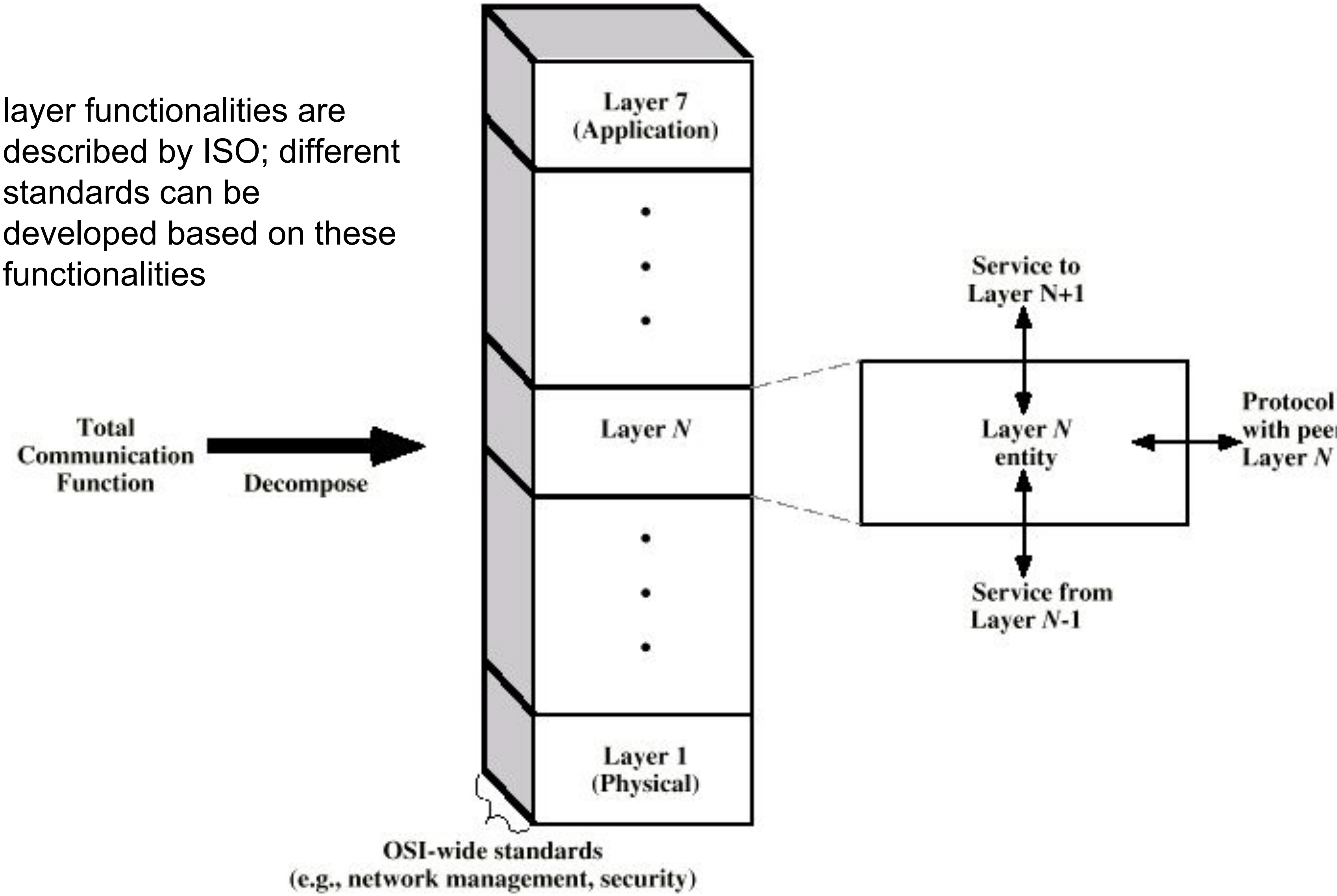
OSI - The Layer Model

- Each layer performs a subset of the required communication functions
- Each layer relies on the next lower layer to perform more primitive functions
- Each layer provides services to the next higher layer
- Changes in one layer should not require changes in other layers

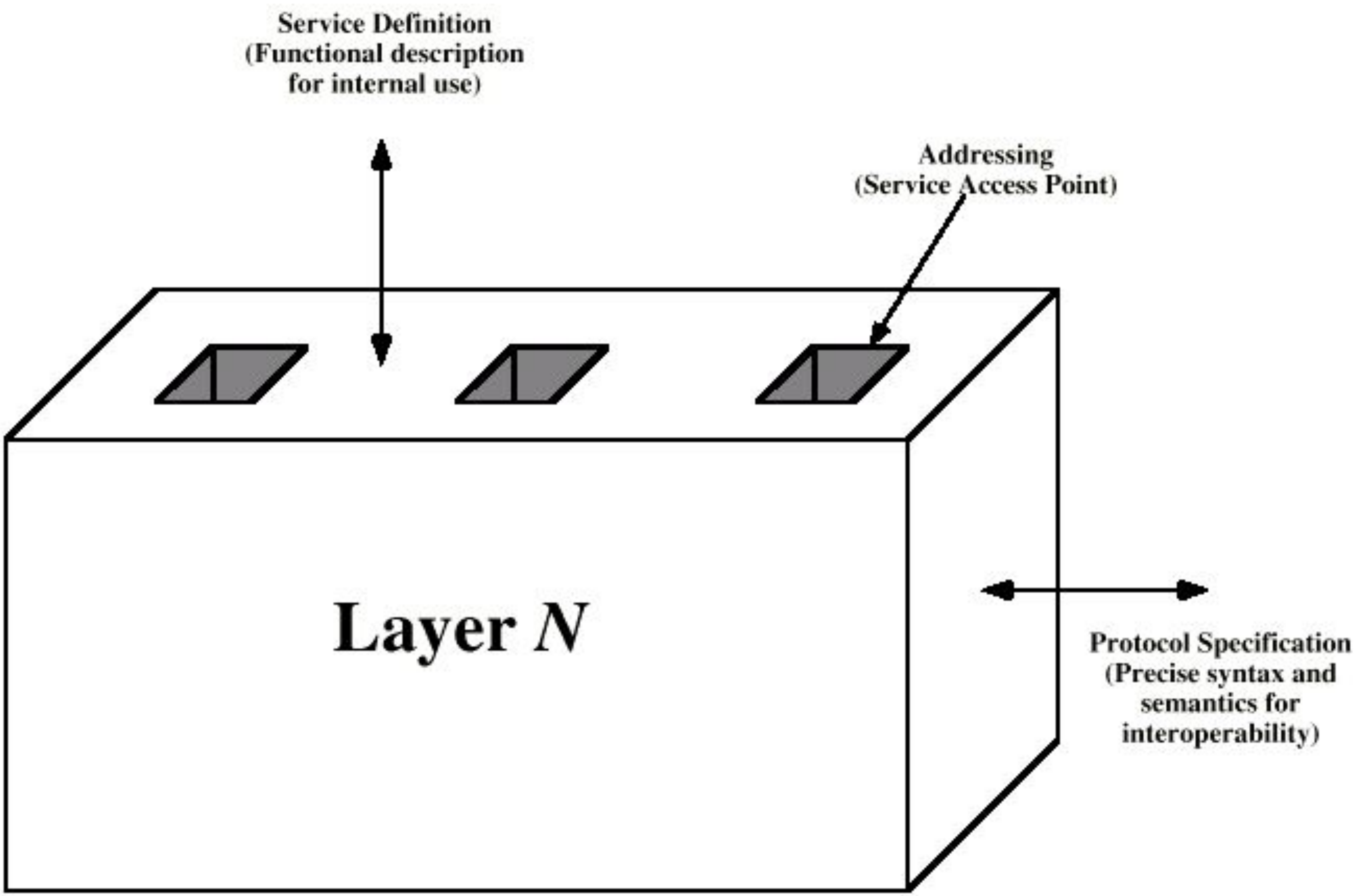
OSI as Framework for Standardization

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

layer functionalities are described by ISO; different standards can be developed based on these functionalities



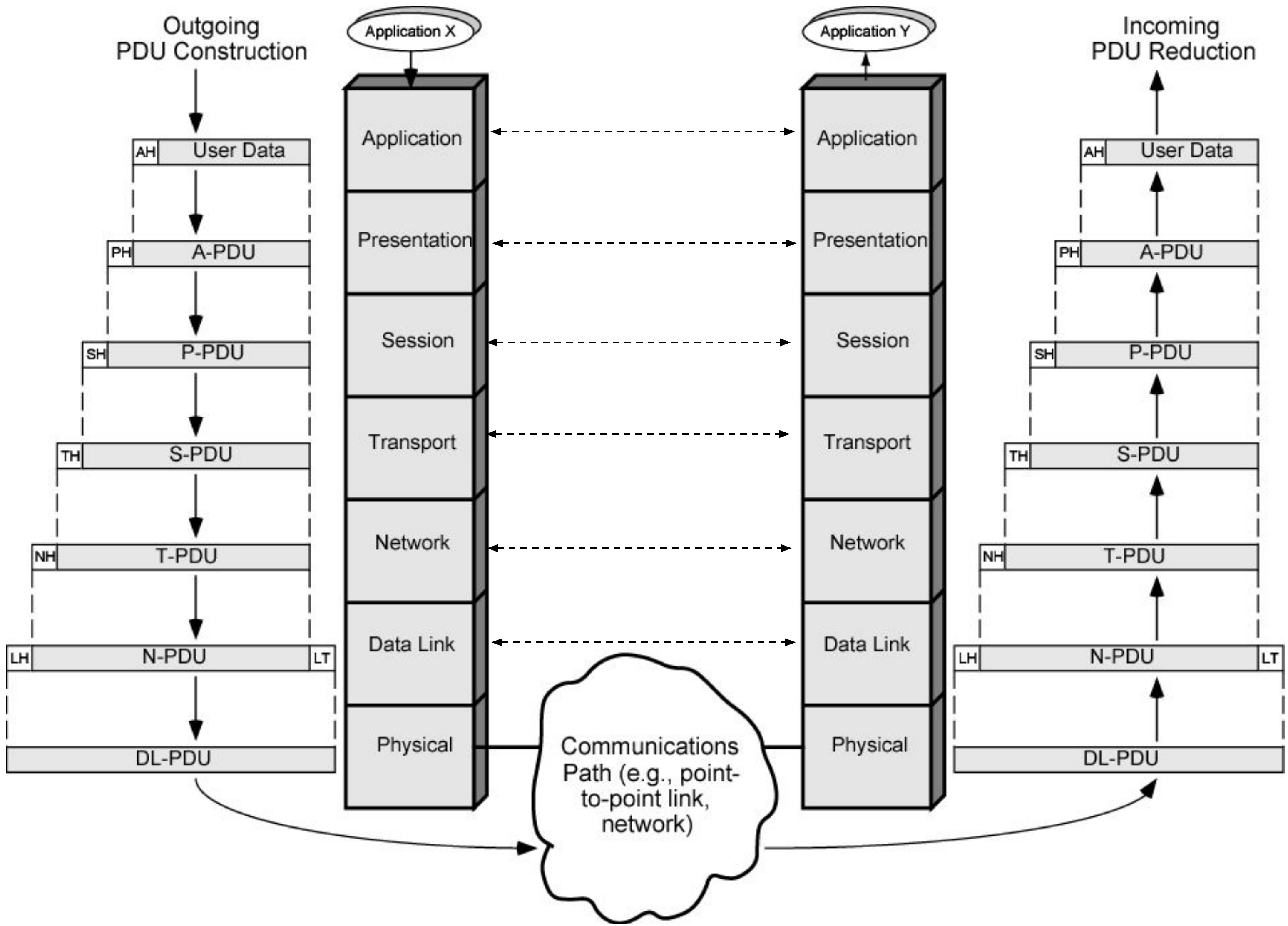
Layer Specific Standards



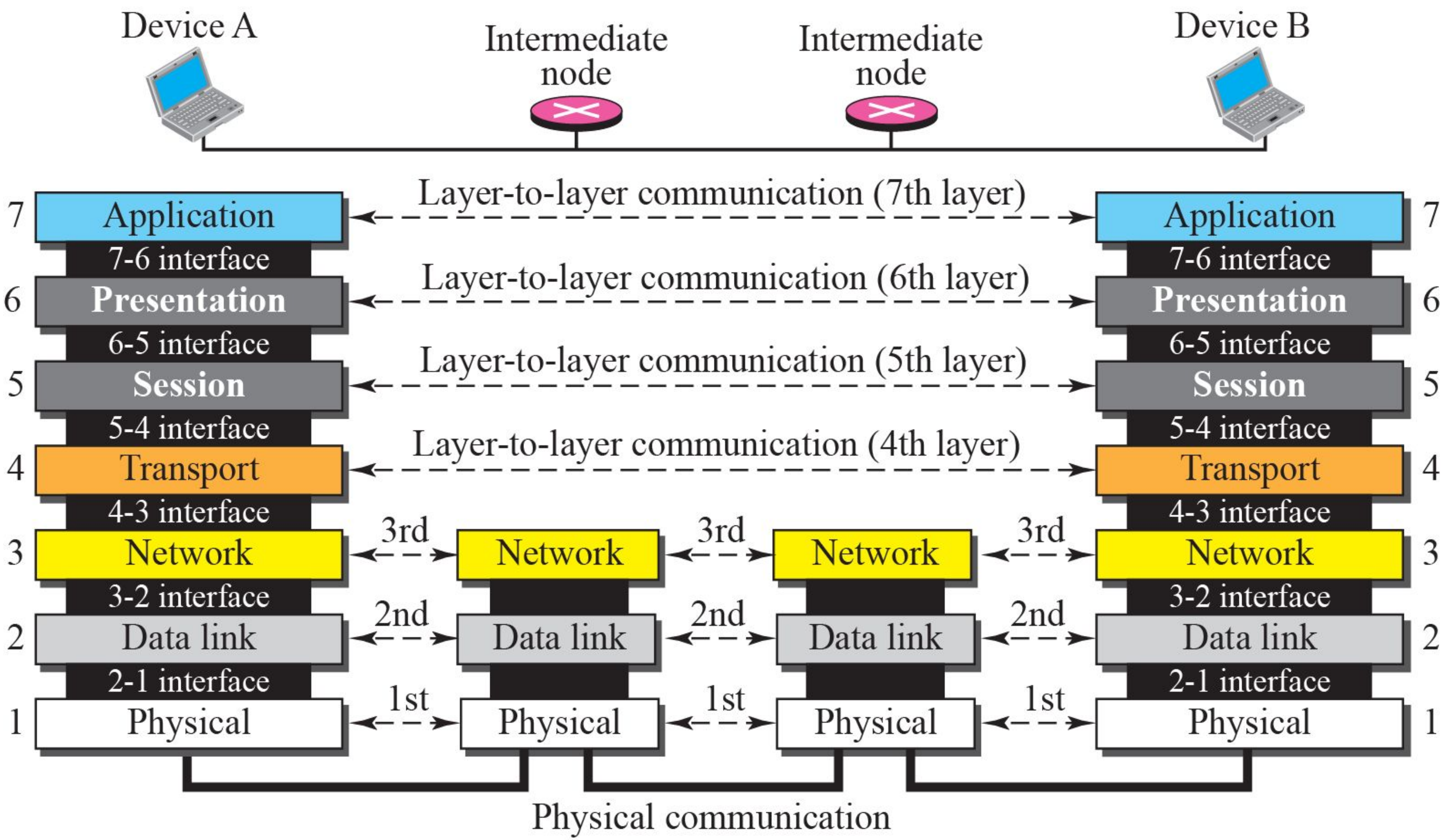
Elements of Standardization

- Protocol specification
  - Operates between the same layer on two systems
    - May involve different platforms
  - Protocol specification must be precise
    - Format of data units
    - Semantics of all fields
- Service definition
  - Functional description of what is provided to the next upper layer
- Addressing
  - Referenced by SAPs

The OSI Architecture



Layer to Layer Communication



Physical Layer

- There is no interpretation at this level, a stream of 1’s and 0’s are put into a form convenient for transmission.
  - Waves (with little regard for their information content) are sent and received.
- This level is the most hardware oriented. It includes specifications about
  - NIC card speeds
  - Types and lengths of cable
  - Voltage characteristics (range, level or edge)
  - Etc.
- The physical layer involves protocols for actual transmission
  - Ethernet
  - FDDI
  - RS232
  - ATM
- These protocols also involve the interface with the next higher layer

Data Link Layer (DLL)

- At this layer one begins to consider bytes instead of just bits, one examines some of the information content of the signal (at least the address and some of the error detection sequencing)
- Recall that bridges operate at this level
  - They know where a packet is headed.
  - They know whether or not it has been involved in a collision.
  - Bit stuffing occurs at this level.
- Data packets are encoded and decoded into bits.
- It directs packets and handles errors from the physical layer

Data Link Layer (DLL)

- It handles synchronization (timing).
  - It must know where one bit ends and the next one begins.
  - It must know where one byte ends and the next one begins
- The data link layer is divided into two sub-layers:
  - The **MAC** (<u>Media Access Control</u>) sub-layer: takes the signal from or puts the signal onto the transmission line ("touches" physical layer).
  - The LLC (<u>Logical Link Control</u>) sub-layer: starts to interpret the signal as data, includes timing (synchronization) and error checking.

Network Layer

- The router acted at this layer.
- One of the main functions of the layer is routing. Store and forward are network layer functions.
- In a connection-oriented scheme, the virtual circuit is established at the network layer.
- Building the routing tables, troubleshooting the routing tables when there is a lot of traffic or if a connection goes down.
- The network layer also gathers related packets (packet sequencing).

Transport Layer

- As stated before, Layer 4 is the dividing line between inter-computer transactions and intra-computer transactions.
- Layer 4 manages end-to-end verification.
  - The lower layers make a "best effort" but if data is lost so be it. Layer 4 must ensure that the information was received intact.
- It does a higher-order error-checking.
- The transfer should be "transparent." The higher layers do not know the data came from another computer.
- At a node Layer 3 collects associated packets if one was dropped it may throw them all away.
- It is the responsibility of the source's Layer 4 to look for some acknowledgement that all packets arrived. If no acknowledgment is received, it should retransmit

Session Layer

INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Recall when discussing connection-oriented schemes, we mentioned the idea of a "session."
- It is an agreement between a source and destination to communicate.
- This layer establishes, manages and terminates sessions between applications (they could be on the same computer or on different computers).

Presentation Layer

- This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa.
- The presentation layer works to transform data into the form that the application layer can accept.
- This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the "syntax layer."

Application Layer

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- This layer supports application and end-user processes.
- Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified
- Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level.
- These are **not applications** (like Word and Excel) but **services for** such **applications**

Mnemonic

- Please Do Not Throw Sausage Pizza Away
  - **P**lease → Physical
  - **D**o → Data Link
  - **N**ot → Network
  - **T**hrow → Transport
  - **S**ausage → Session
  - **P**izza → Presentation
  - **A**way → Application

Session 6

- TCP/IP Protocol suite
- Comparison between OSI and TCP
- Introduction to link layer protocols.- Noiseless Channel and Noisy Channel
- Addressing

TCP/IP Protocol Suite

- Most widely used interoperable network protocol architecture
- Specified and extensively used before OSI
  - OSI was slow to take place in the market
- Funded by the US Defense Advanced Research Project Agency (DARPA) for its packet switched network (ARPANET)
  - DoD (Department of Defense) automatically created an enormous market for TCP/IP
- Used by the Internet and WWW

TCP/IP Protocol Suite

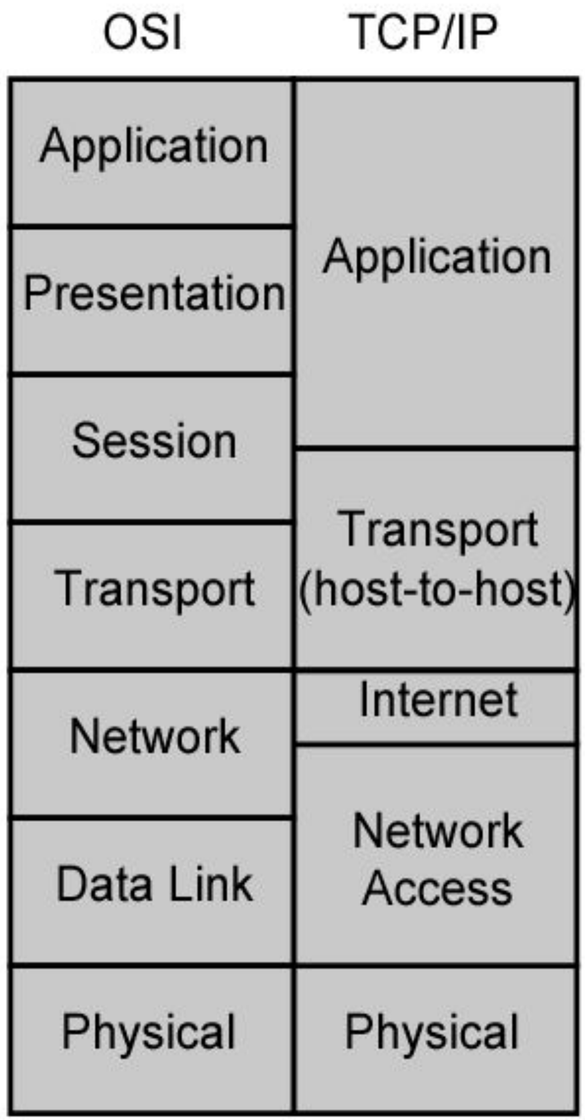
- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not match exactly with those in the OSI model.
- The original TCP/IP protocol suite was defined as four software layers built upon the hardware.
- Today, however, TCP/IP is thought of as a five-layer model with the layers named similarly to the ones in the OSI model

TCP/IP Protocol Suite

- The Layers used in the TCP/IP protocol
  - Application layer
  - Transport (host to host / end to end) layer
  - Internet layer
  - Network access layer
  - Physical layer

- Actually TCP/IP reference model has been built on its protocols
  - That is why that reference model is only for TCP/IP protocol suite
  - and this is why it is not so important to assign roles to each layer in TCP/IP; understanding TCP, IP and the application protocols would be enough

OSI vs. TCP/IP

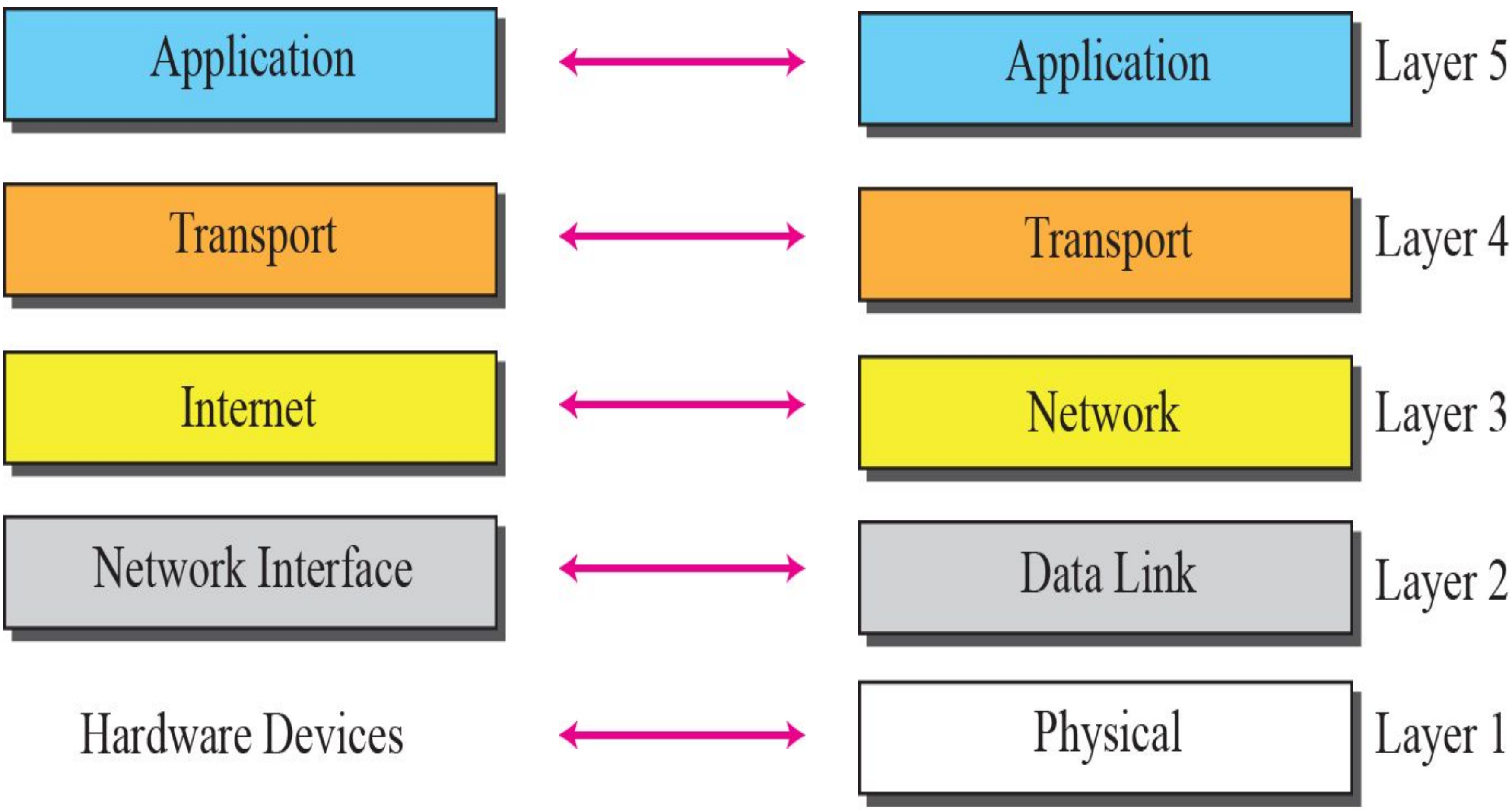


HTTP, SMTP, …

TCP, UDP

IP

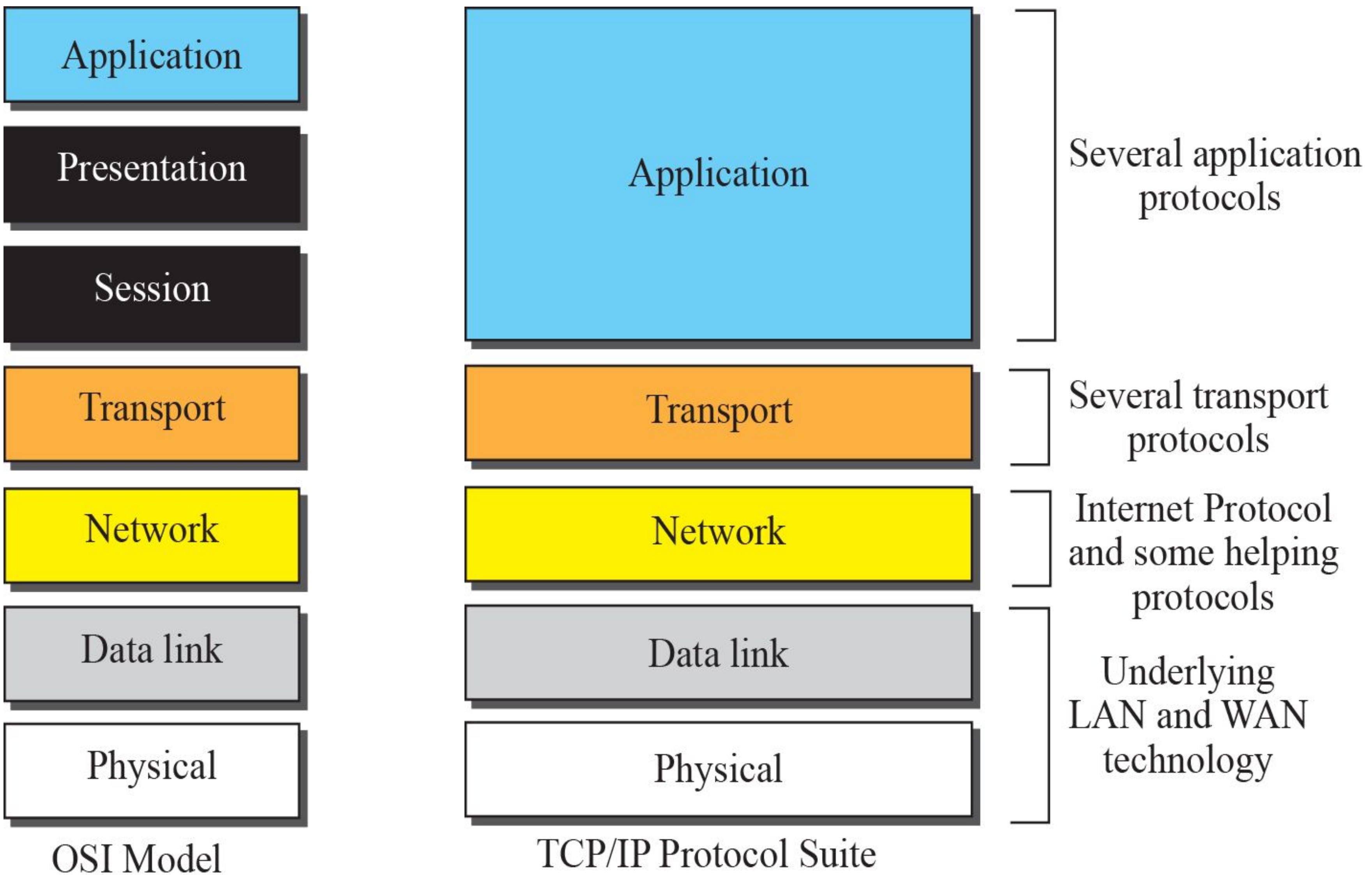
OSI vs. TCP/IP



a. Original layers

b. Layers used in this book

OSI vs. TCP/IP


Application
Presentation
Session
Transport
Network
Data link
Physical
OSI Model
Application
Transport
Network
Data link
Physical
TCP/IP Protocol Suite
Several application protocols
Several transport protocols
Internet Protocol and some helping protocols
Underlying LAN and WAN technology

Network Access and Physical Layers

- TCP/IP reference model does not discuss these layers too much
  - the node should connect to the network with a protocol such that it can send IP packets
  - this protocol is not defined by TCP/IP
  - mostly in hardware
  - a well known example is Ethernet

Internet Layer

- Connectionless, point to point internetworking protocol (uses the datagram approach)
  - takes care of routing across multiple networks
  - each packet travels in the network independently of each other
    - they may not arrive (if there is a problem in the network)
    - they may arrive out of order
  - a design decision enforced by DoD to make the system more flexible and responsive to loss of some subnet devices
- Implemented in end systems and routers as the Internet Protocol (IP)

Transport Layer

- End-to-end data transfer
- Transmission Control Protocol (TCP)
  - connection oriented
  - reliable delivery of data
  - ordering of delivery
- User Datagram Protocol (UDP)
  - connectionless service
  - delivery is not guaranteed
- Can you give example applications that use TCP and UDP?

Application Layer

- Support for user applications
- A separate module for each different application
  - e.g. HTTP, SMTP, telnet

Introduction to link layer protocols

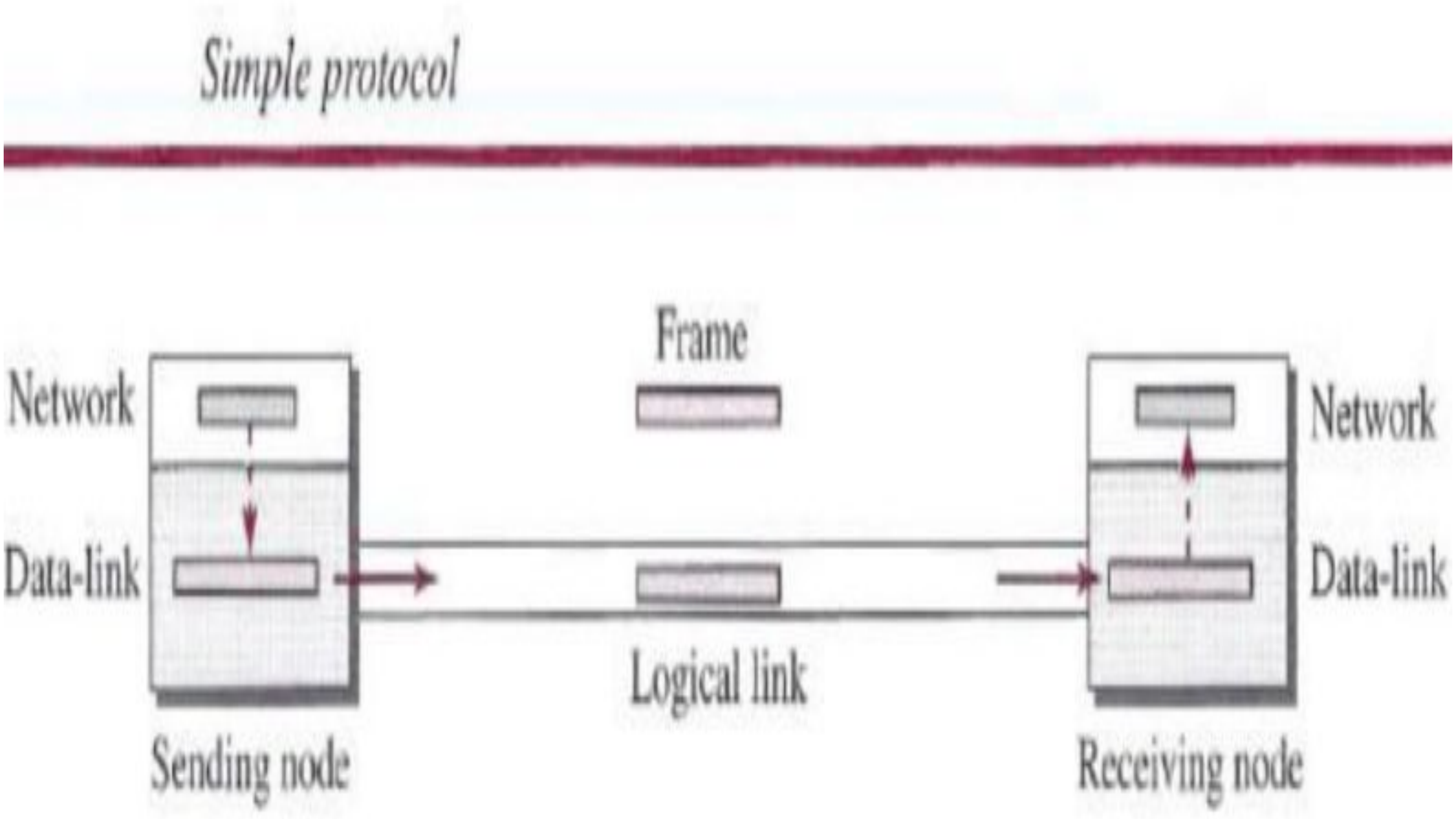
Traditionally four protocols have been defined for the data-link layer to deal with flow and error control:

- Simple,
- Stop-and-Wait,
- Go-Back-N, and (Will be discussed in Unit 4)
- Selective-Repeat (Will be discussed in Unit 4)

Simple Protocol

- The simple protocol neither do flow control nor do error control.
- We assume that the receiver can immediately handle any frame it receives.
- In other words, the receiver can never be overwhelmed with incoming frames.
- Below figure shows the layout for this protocol.

Simple Protocol



Simple Protocol

- The DLL at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.
- The DLL at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.
- The DLLs of the sender and receiver provide transmission services for their network layers

Stop-and-Wait Protocol

- The Stop-and- Wait protocol uses both flow and error control.
- The sender sends one frame at a time and waits for an acknowledgment before sending the next one.
- To detect corrupted frames, we need to add a CRC to each data frame.
- When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded.

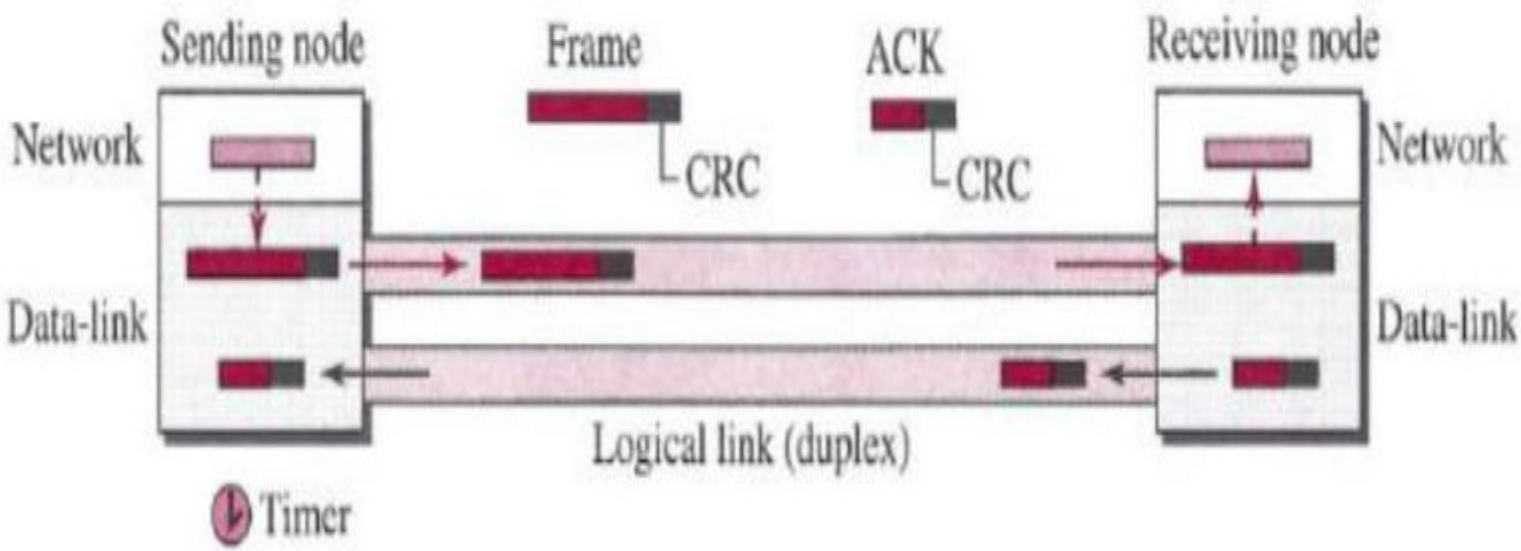
Stop-and-Wait Protocol

- The silence of the receiver is a signal for the sender that a frame was either corrupted or lost.
- Every time the sender sends a frame, it starts a timer.
- If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame.
- If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted.
- This means that the sender needs to keep a copy of the frame until its acknowledgment arrives.

Stop-and-Wait Protocol

- When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.
- Below figure shows the outline for the Stop-and-Wait protocol.
- Note that only one frame and one acknowledgment can be in the channels at any time

Stop-and-Wait Protocol



Other DLL Protocols

- HDLC
- Point-to-Point Protocol (P2P)
- Multiple Access Protocols

Note: They will be discussed in unit 4

Noiseless & Noise Channels

Noiseless Channel

- An ideal channel in which no frames are lost, duplicated or corrupted is regarded as Noiseless Channel.
- Protocols belong to this channel are
  - Simple & Stop-and-wait protocols

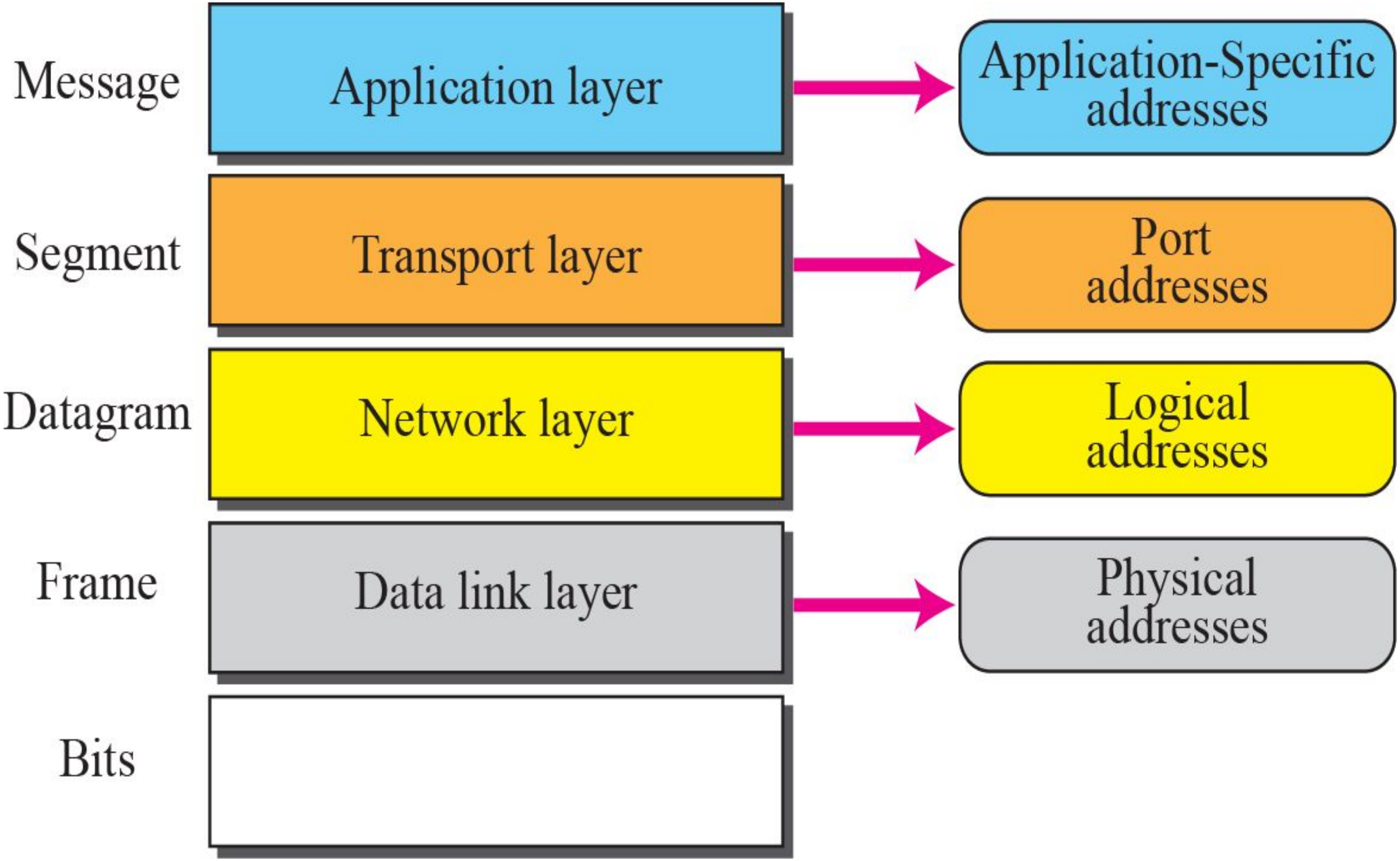
Noisy Channels

- Consider the normal situation of a communication channel that makes errors. Frames may be either damaged or lost completely.
- Protocols belong to this channel are
  - ARQ (Automatic Repeat Request Protocols)

ADDRESSING

- Four levels of addresses are used in an internet employing the TCP/IP protocols:
  - physical address,
  - logical address,
  - port address, and
  - application-specific address.
- Each address is related to a one layer in the TCP/IP architecture, as shown in the following Figure.

ADDRESSING


Message
Application layer
Application-Specific addresses
Segment
Transport layer
Port addresses
Datagram
Network layer
Logical addresses
Frame
Data link layer
Physical addresses
Bits

ADDRESSING

Physical Addresses

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer. It is the lowest-level address.
- The size and format of these addresses vary depending on the network.
- For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).
- Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below.

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

A 6-byte (12 hexadecimal digits) physical address

ADDRESSING

Unicast, Multicast, and Broadcast Physical Addresses

- Physical addresses can be either
  - Unicast (one single recipient),
  - multicast (a group of recipients), or
  - broadcast (to be received by all systems in the network).
- Some networks support all three addresses

ADDRESSING

Logical Addresses

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.
- Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
- The logical addresses are designed for this purpose

ADDRESSING

Port Addresses

- The end objective of Internet communication is a process communicating with another process.
- For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).
- For these processes to receive data simultaneously, we need a method to label the different processes.
- In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address.
- A port address in TCP/IP is 16 bits in length.

ADDRESSING

Application-Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific application.
- Examples include the e-mail address (for example, co_sci@yahoo.com) and the Universal Resource Locator (URL) (for example, www.mhhe.com).
- The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.
- These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

Session 9

Network layer protocols:

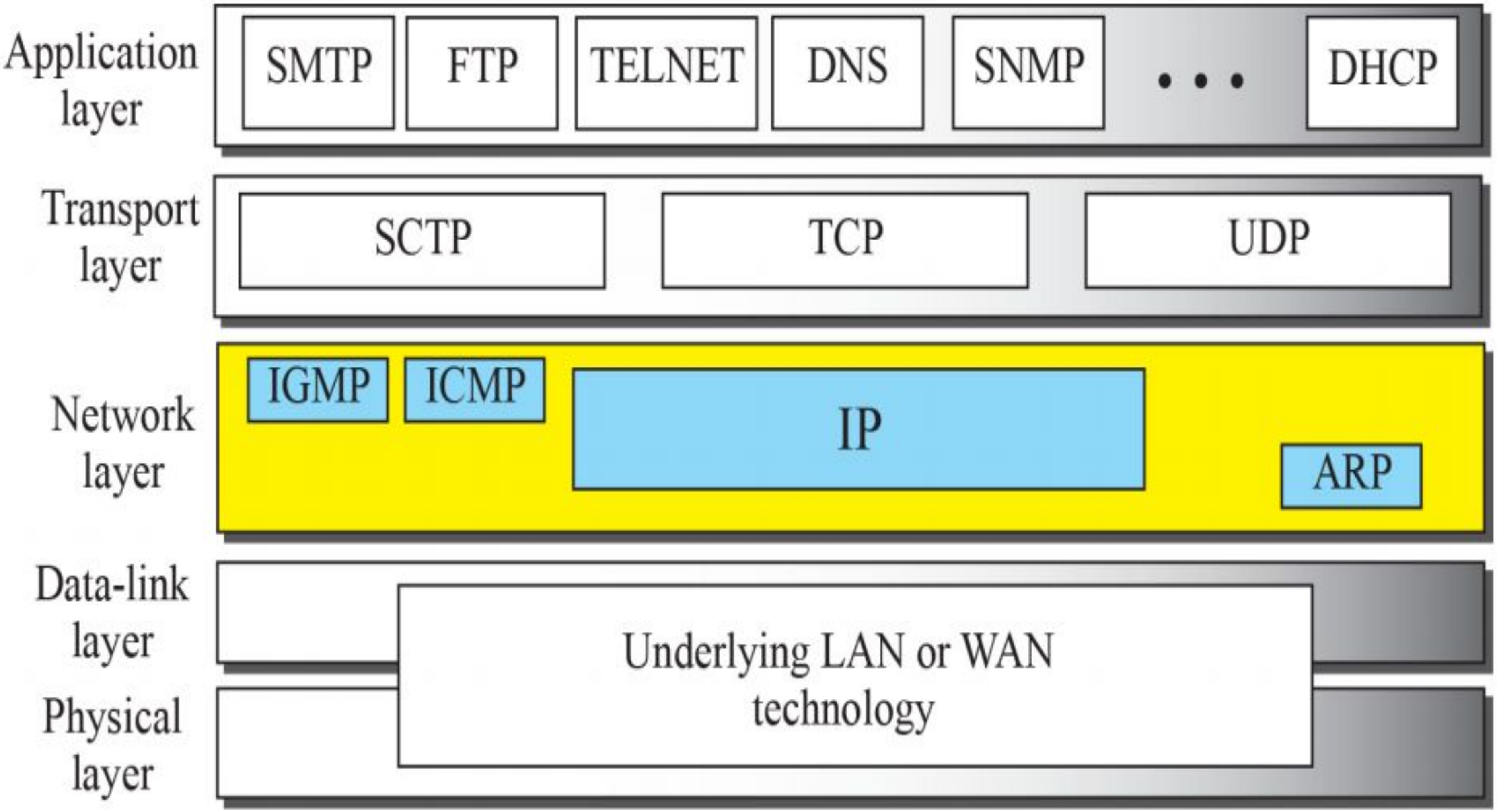
- ARP
- RARP and
- ICMP

Network Layer Protocols

Network layer protocols:

- IPv4 is responsible for packetizing, forwarding, and delivery of a packet.
- ICMPv4 helps IPv4 to handle some errors that may occur in delivery.
- IGMP is used to help IPv4 in multicasting.
- ARP is used in address mapping and
- RARP is also used in address mapping but in reverse

Position of NLP in TCP/IP Stack Suite

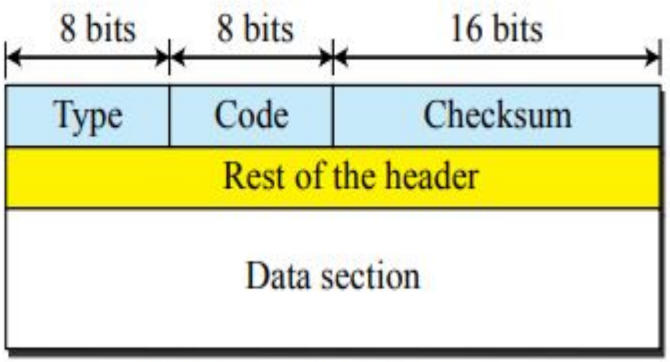


ICMP V4

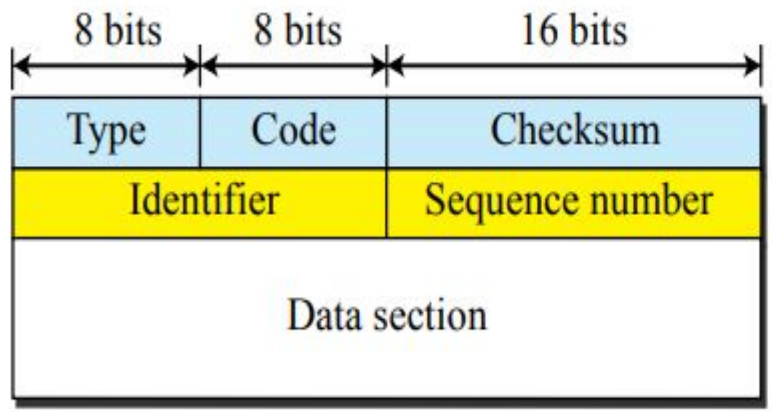
- **ICMPv4** - The IPv4 has no error-reporting or error-correcting mechanism
- The IP protocol also lacks a mechanism for host and management queries
- The Internet Control Message Protocol version 4 (ICMPv4) has been designed to compensate for the above two deficiencies
- **ICMP MESSAGES**
  - **Error-reporting messages** report problems that a router or a host (destination) may encounter when it processes an IP packet.
  - **Query messages** help a host or a network manager get specific information from a router or another host.

ICMP V4

General format of ICMP messages



Error-reporting messages



Query messages

Type and code values

Error-reporting messages

03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

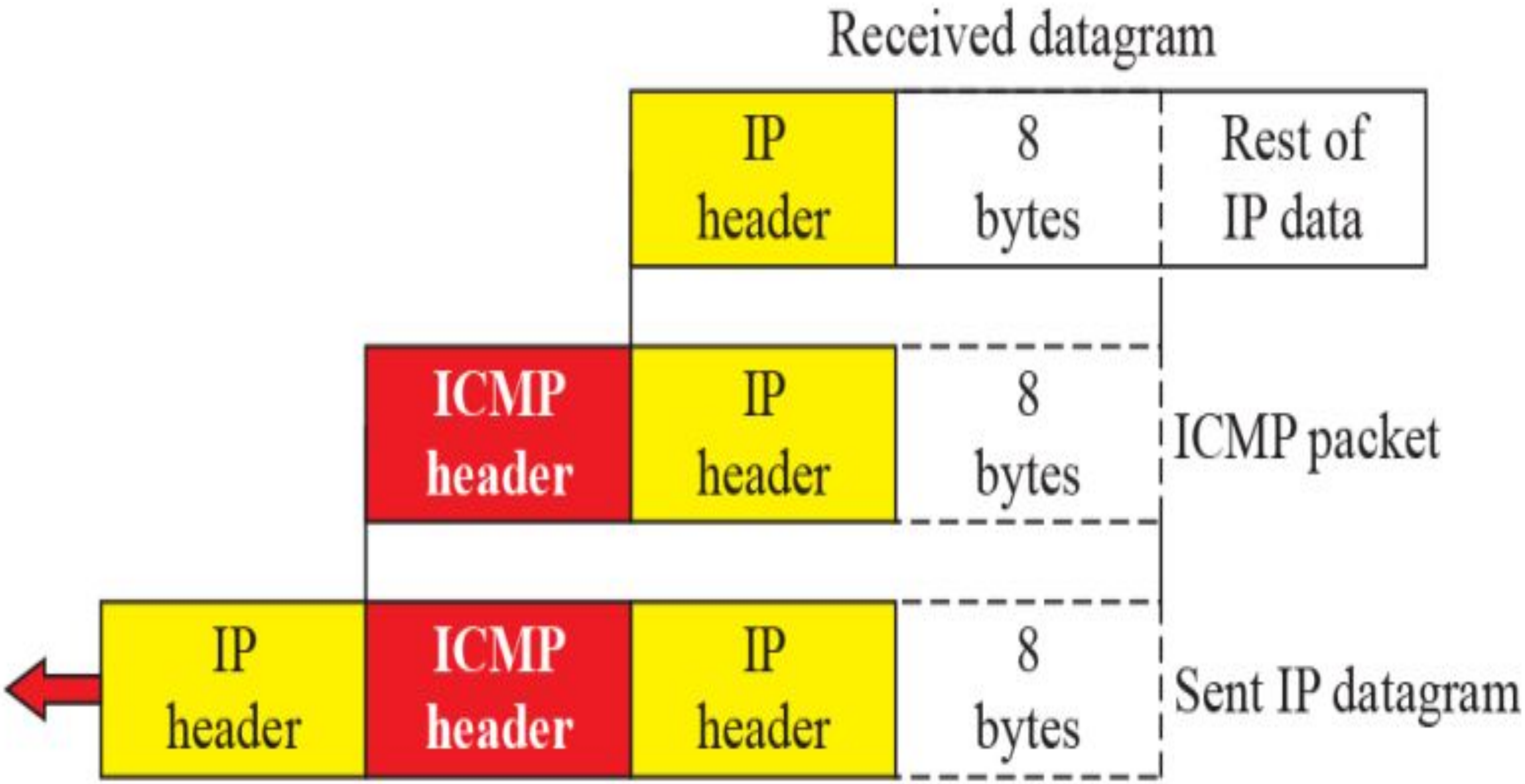
Query messages

08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

Note: See the book website for more explanation about the code values.

ICMP V4

Contents of data field for the error messages



ARP

Address Resolution Protocol

- ➔ **Routing decision for packet X has two possible outcomes:**
  - ⇨ You are arrived to the final network: go to host X
  - ⇨ You are not arrived to the final network: go through router interface Y
- ➔ **In both cases we have an IP address on THIS network. How can we send data to the interface?**
- ➔ **Need to use physical network facilities!**

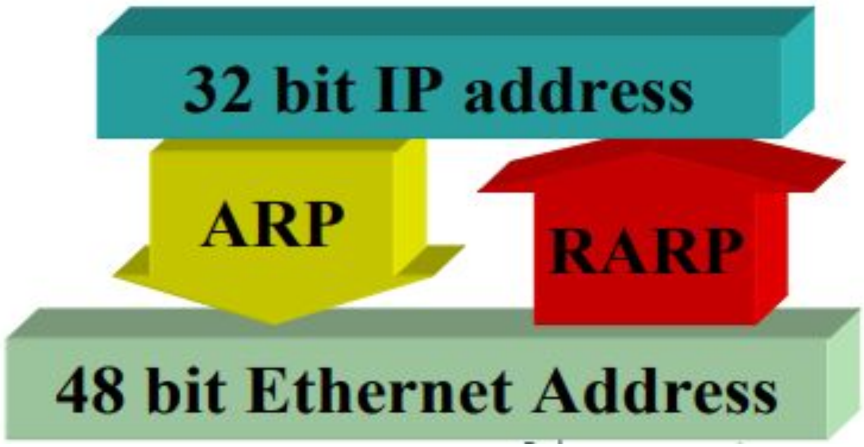
ARP

Reaching a Physical Host

- ➔ **IP addresses only make sense to TCPIP protocol suite**
- ➔ **physical networks have their own hardware address**
  - ⇨ e.g. 48 bits Ethernet address, 16 or 48 bits Token Ring, 16 or 48 bit FDDI, ...
  - ⇨ datalink layers may provide the basis for several network layers, not only IP!

Address Resolution Protocol
RFC 826

Here described for Ethernet, but more general: designed for any datalink with broadcast capabilities



SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

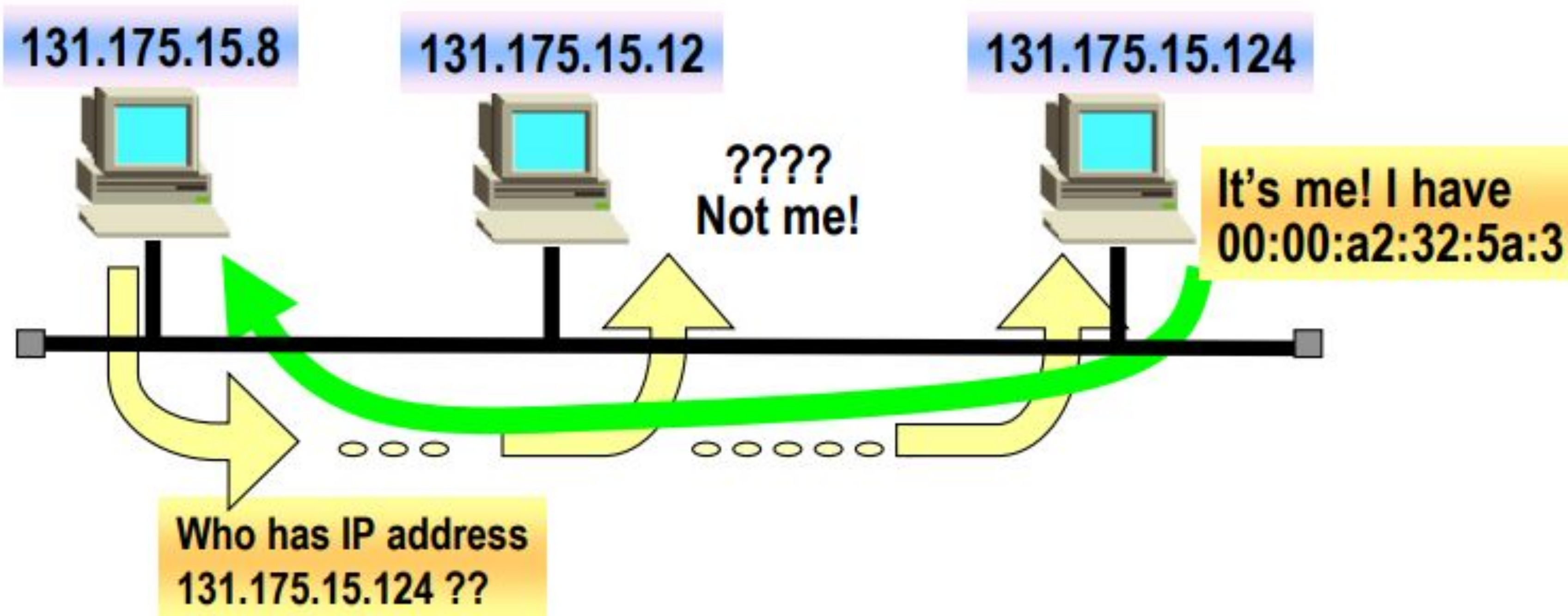
Manual Mapping

- ➔ **A possibility, indeed!!**
  - ⇨ Nothing contrary, in principle
    - → actually done in X.25, ISDN (do not support broadcast)
  - ⇨ Simply keep in every host a mapping between IP address and hardware address for every IP device connected to the considered network
- ➔ **drawbacks**
  - ⇨ tedious
  - ⇨ error prone
  - ⇨ requires manual updating
    - → e.g. when attaching a new PC, must touch all others...

ARP

- ➔ **Dynamic mapping**
  - ⇨ not a concern for application & user
  - ⇨ not a concern for system administrator!
- ➔ **Any network layer protocol**
  - ⇨ not IP-specific
- ➔ **supported protocol in datalink layer**
  - ⇨ not a datalink layer protocol !!!!
- ➔ **Need datalink with broadcasting capability**
  - ⇨ e.g. ethernet shared bus

ARP Idea



➔**Send broadcast request**

➔**receive unicast response**

ARP Cache

- → **Avoids arp request for every IP datagram!**
  - ⇨ Entry lifetime defaults to 20min
    - → deleted if not used in this time
    - → 3 minutes for "incomplete" cache entries (i.e. arp requests to non existent host)
    - → it may be changed in some implementations
      - » in particularly stable (or dynamic) environments
  - ⇨ ***arp -a*** to display all cache entries (arp –d to delete)

try a traceroute or ping to check ARP caching!

- → First packet generally delays more
- → includes an ARP request/reply!

ARP in Ethernet Frame

6 bytes	6 bytes	2 bytes	28 bytes (for IP)	4 bytes
Ethernet destination address	Ethernet source address	frame type	ARP Request / Reply	CRC

- **Ethernet Destination Address**
  - ff:ff:ff:ff:ff:ff (broadcast) for ARP request
- **Ethernet Source Address**
  - of ARP requester
- **Frame Type**
  - ARP request/reply: 0x0806
  - RARP request/reply: 0x8035
  - IP datagram: 0x0800

Protocol demultiplexing codes!

ARP Message Format

0 … 7	8 … 15	16 … 31
Hardware Type		Protocol Type
Hardware len	Protocol len	ARP operation
Sender MAC address (bytes 0-3)		
Sender MAC address (bytes 4-5)		Sender IP address (bytes 0-1)
Sender IP address (bytes 2-3)		Dest MAC address (bytes 0-1)
Dest MAC address (bytes 2-5)		
Dest IP address (bytes 0-3)		

28 bytes

Hardware type: 1 for ethernet

Protocol type: 0x0800 for IP (0000.1000.0000.0000)

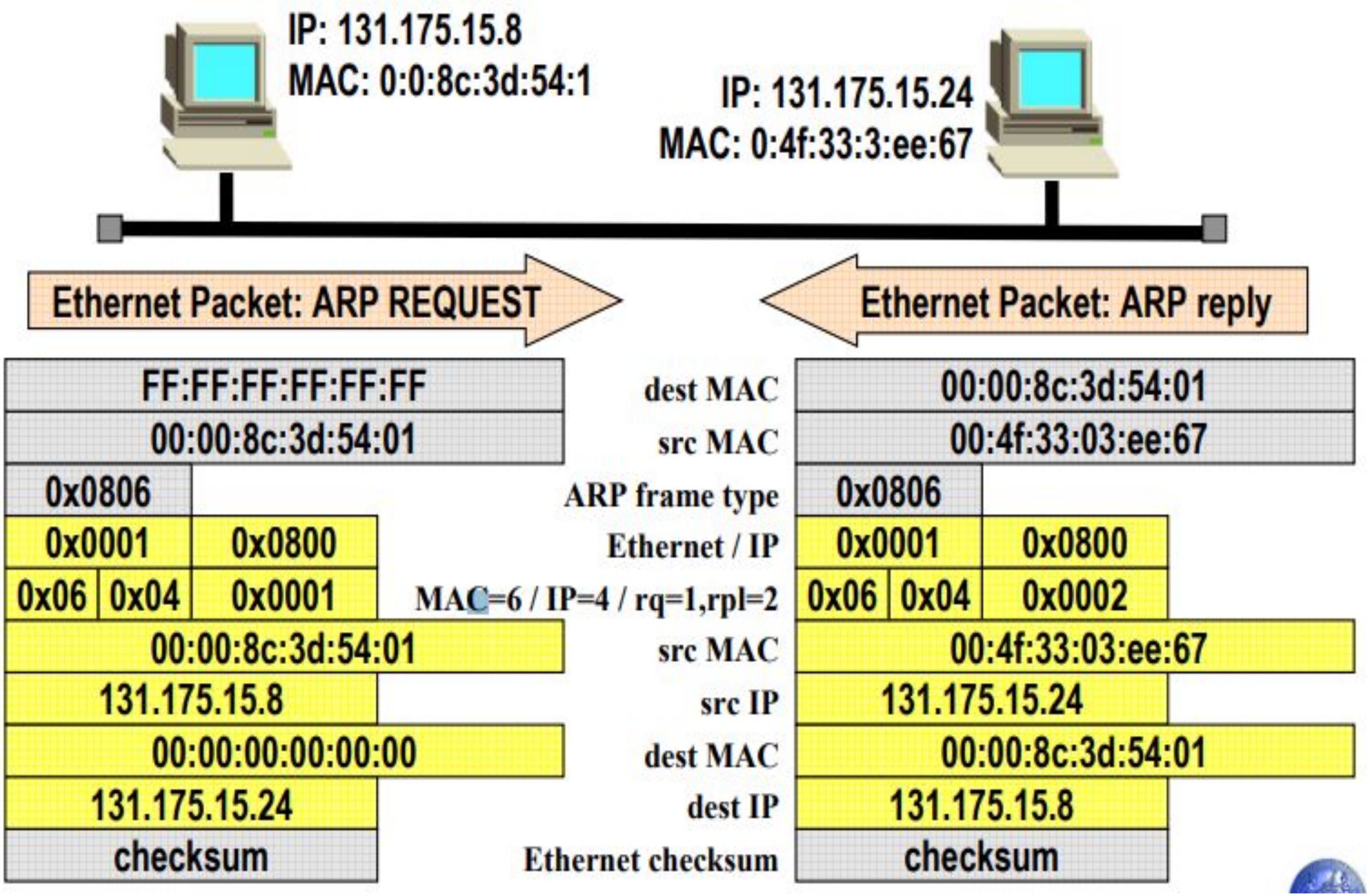
⇨ *the same of Ethernet header field carrying IP datagram!*

Hardware len = length in bytes of hardware addresses (6 bytes for ethernet)

Protocol len = length in bytes of logical addresses (4 bytes for IP)

ARP operation: 1=request; 2=reply; 3/4=RARP req/reply

Simple ARP Request/Reply



ARP Cache Updating

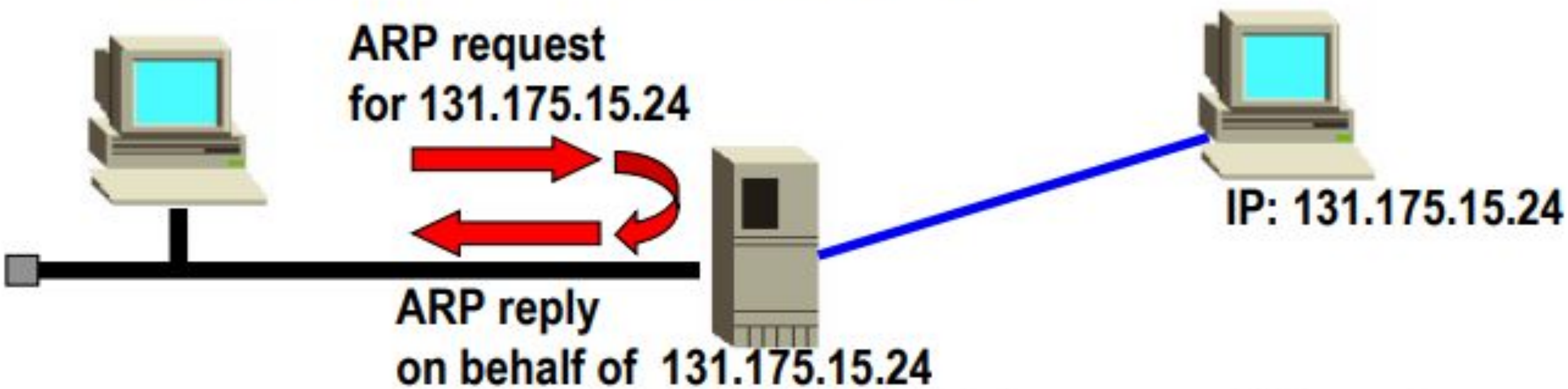
- ➔ **ARP requests carry requestor IP/MAC pair**
- ➔ **ARP requests are broadcast**
  - ⇨ thus, they MUST be read by everyone
- ➔ **Therefore, it comes for free, for every computer, to update its cache with requestor pair**
- ➔ ***Cannot do this with ARP reply, as it is unicast!***

Proxy ARP

INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

➔ **Device that responds to an ARP request on behalf of some other machine**

- ⇨ allows having ONE logical (IP) network composed of more physical networks
- ⇨ especially important when different techologies used (e.g. 100 PC ethernet + 2 PC dialup SLIP)



*returns **router MAC address**! Then router will forward packets to remote host*

Reverse Address Resolution Protocol (RARP)

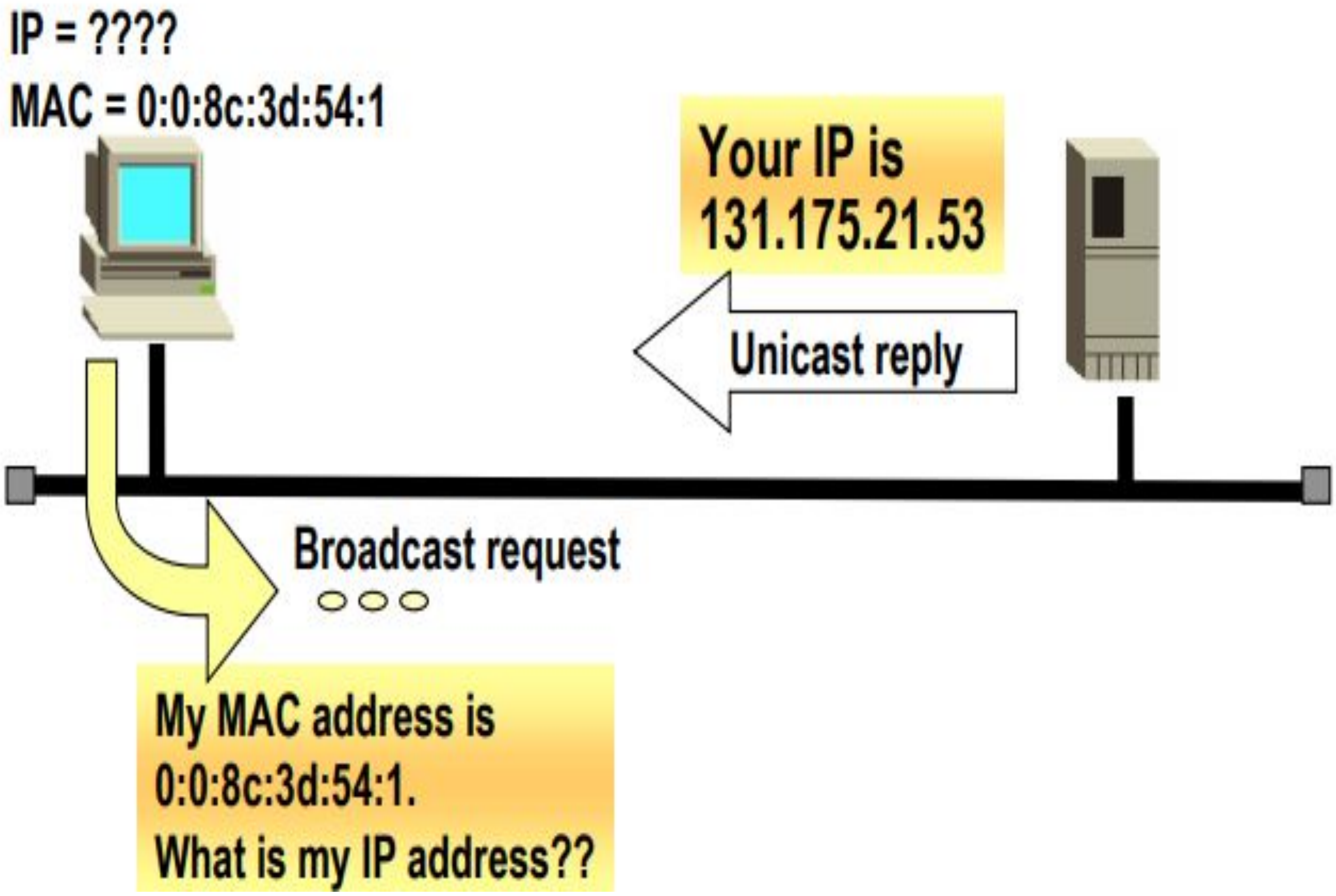
- **Bootstrapping a diskless terminal**
  - this was the original problem in the 70s and 80s
- **Reverse ARP [RFC903]**
  - a way to obtain an IP address starting from MAC address
- **Today problem: dynamic IP address assignment**
  - limited pool of addresses assigned only when needed
- **RARP not sufficiently general for modern usage**
  - BOOTP (Bootstrap Protocol - RFC 951): significant changes to RARP (a different approach)
  - DHCP (Dynamic Host Configuration Protocol - RFC 1541): extends and replaces BOOTP

RARP Packet Format

6 bytes	6 bytes	2B	28 bytes (for IP)	4 bytes
Dest addr	Src addr	ftyp: 0x 8035	RARP Request / Reply	CRC

0 … 7	8 … 15	16 … 31
Hardware Type		Protocol Type
Hardware len	Protocol len	oper: 3 (RARP req) or 4 (RARP reply)
Sender MAC address (bytes 0-3)		
Sender MAC address (bytes 4-5)		Sender IP address (bytes 0-1)
Sender IP address (bytes 2-3)		Dest MAC address (bytes 0-1)
Dest MAC address (bytes 2-5)		
Dest IP address (bytes 0-3)		

RARP Request/Reply



RARP Problems

- ➔ **Network traffic**
  - ⇨ for reliability, multiple RARP servers need to be configured on the same Ethernet
    - → to allow bootstrap of terminals even when one server is down
  - ⇨ But this implies that ALL servers simultaneously respond to RARP request
    - → contention on the Ethernet occurs
- ➔ **RARP requests not forwarded by routers**
  - ⇨ being hardware level broadcasts...

RARP Problems

- ➔ **Allows only to retrieve the IP address information**
  - ⇨ and what about all the remaining full set of TCPIP configuration parameters???
    - → Netmask?
    - → name of servers, proxies, etc?
    - → other proprietary/vendor/ISP-specific info?

- ➔ **This is the main reason that has driven to engineer and use BOOTP and DHCP**

Session 10

- Transport layer Protocols

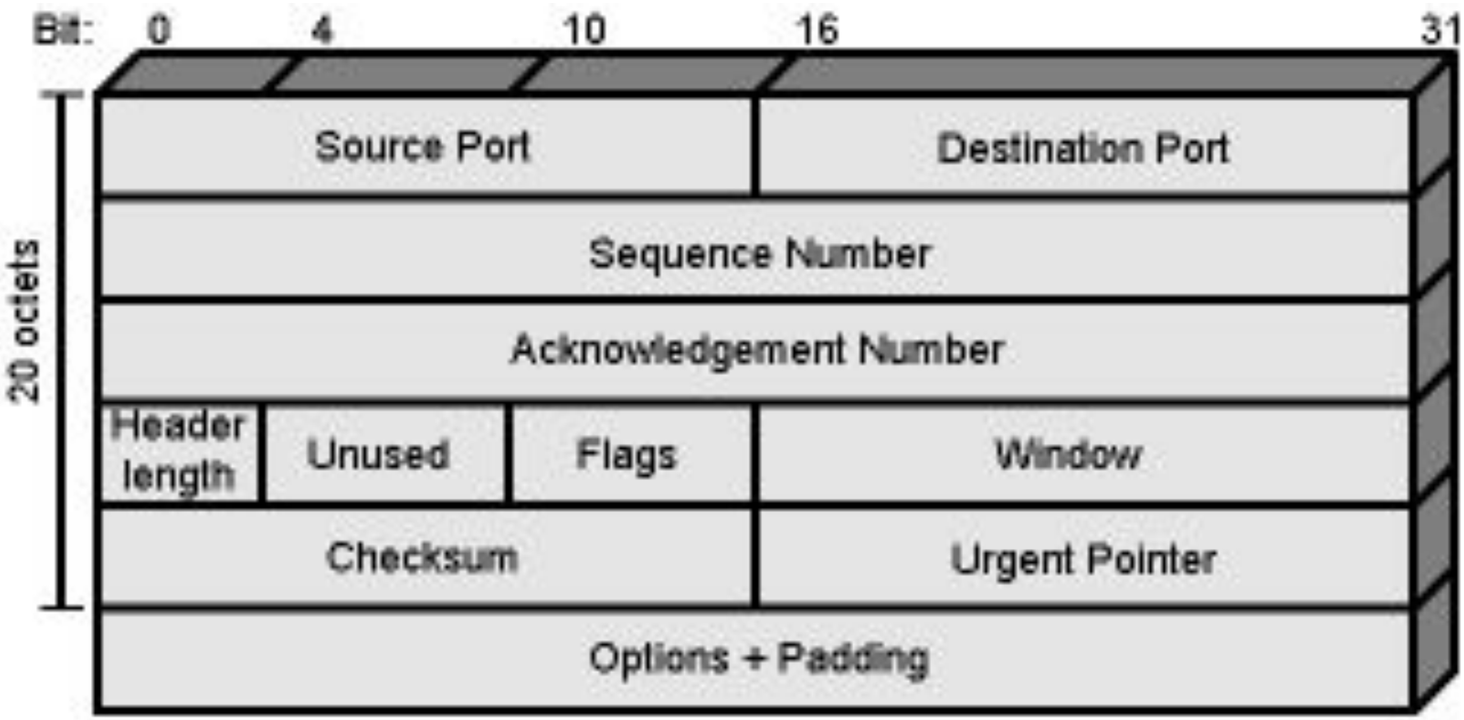
  - TCP and UDP
- Data transmission
  – Parallel and Serial
- Serial transmission types

TCP

- Transmission Control Protocol
  - end to end protocol
  - Reliable connection = provides flow and error control
- In TCP terms, a *connection* is a

  temporary association between entities in different systems
- TCP PDU
  - Called “TCP segment”
  - Includes source and destination port
    - Identify respective users (applications)
    - pair of ports (together with the IP addresses) uniquely identify a connection; such an identification is necessary in order TCP to track segments between entities.

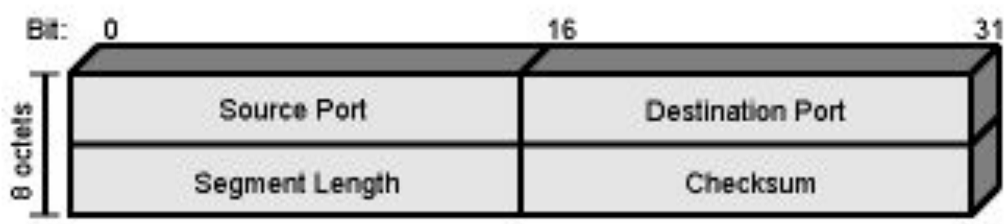
TCP Header



Bit: 0 4 10 16 31
20 octets
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Header length
Unused
Flags
Window
Checksum
Urgent Pointer
Options + Padding

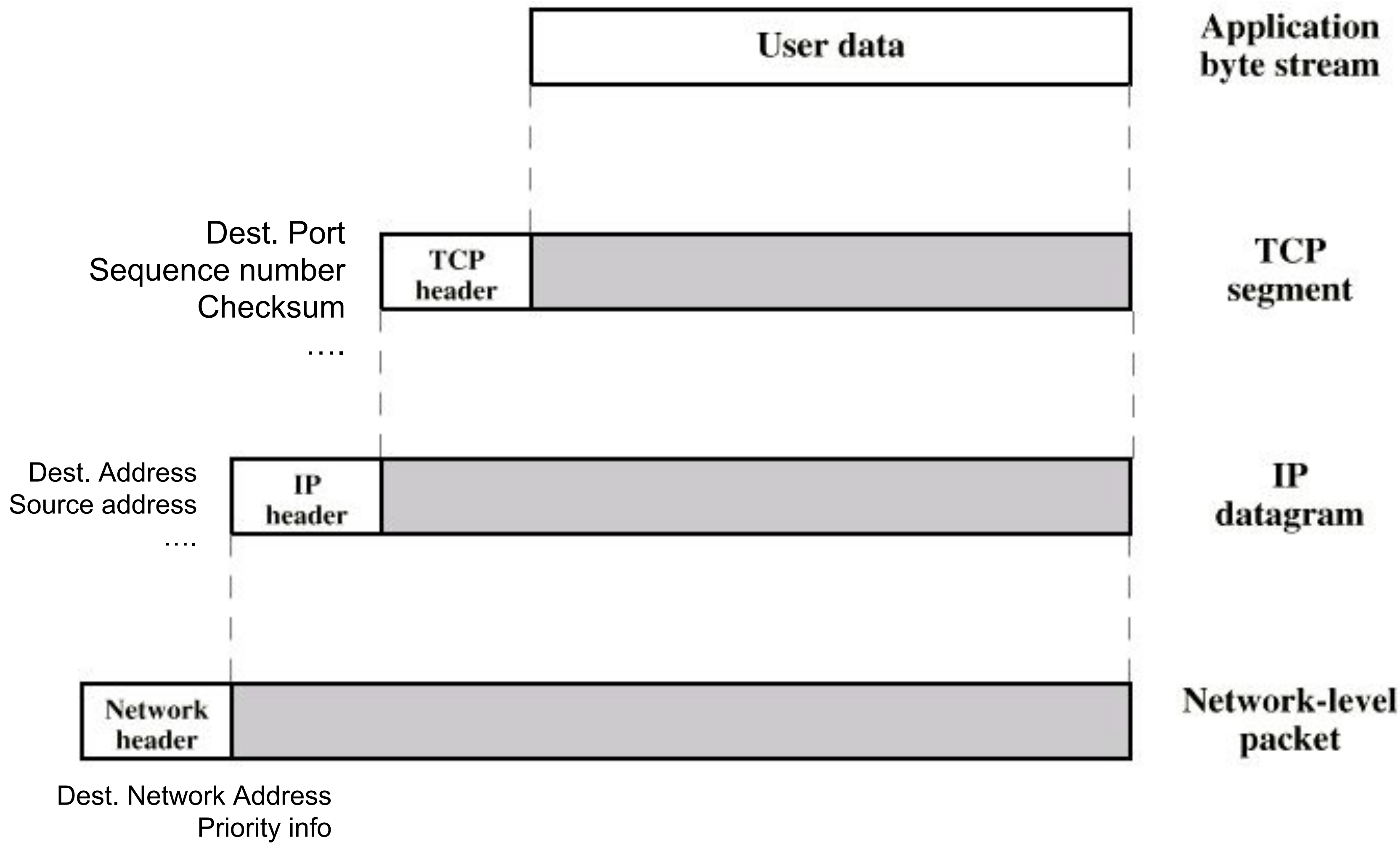
UDP

- User Datagram Protocol
- Alternative to TCP
  - end-to-end protocol
- Not guaranteed delivery
- No preservation of sequence
- No protection against duplication
- Minimum overhead

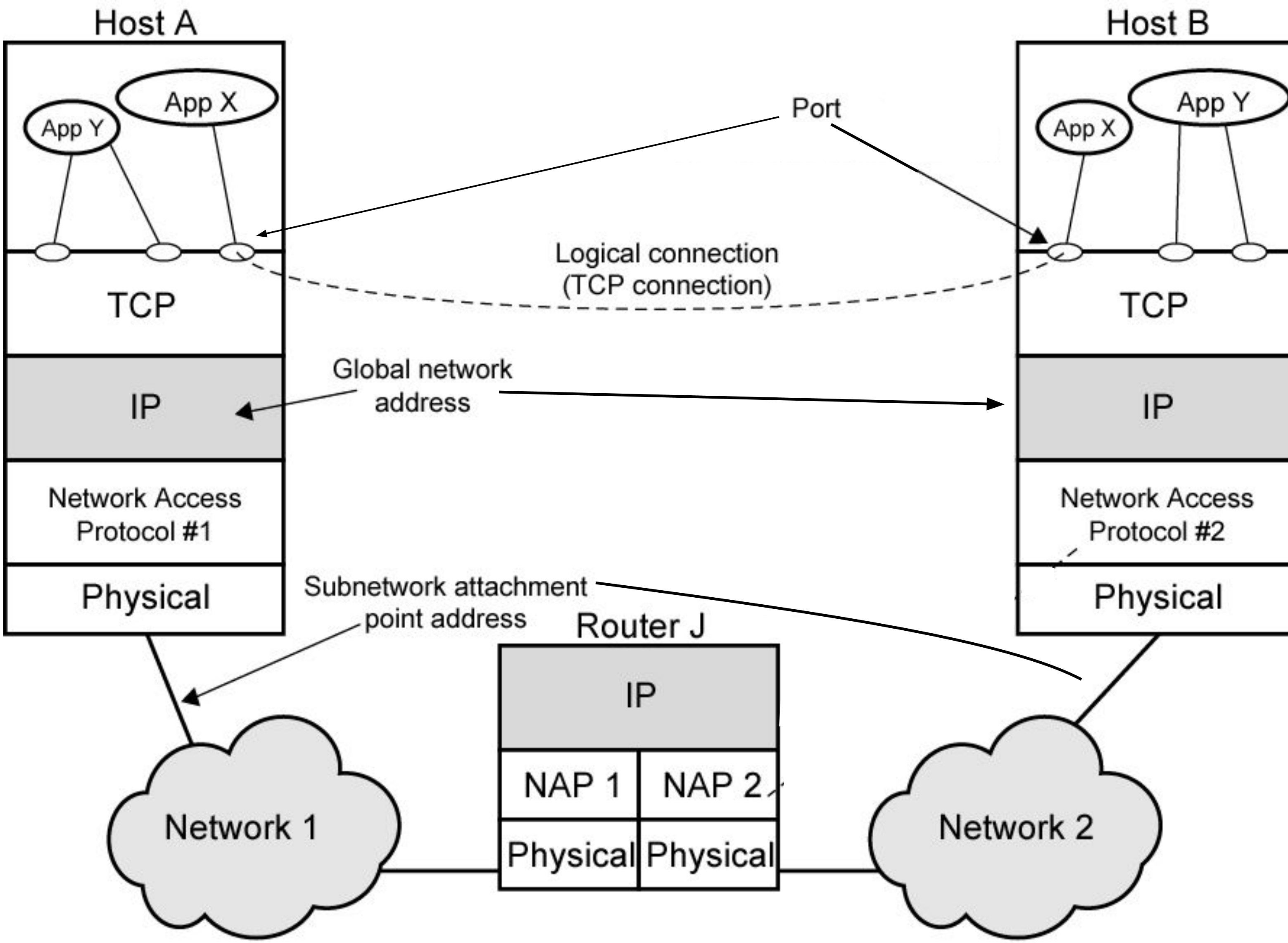


(b) UDP Header

PDUs in TCP/IP



Operation of TCP and IP



Data Transmission

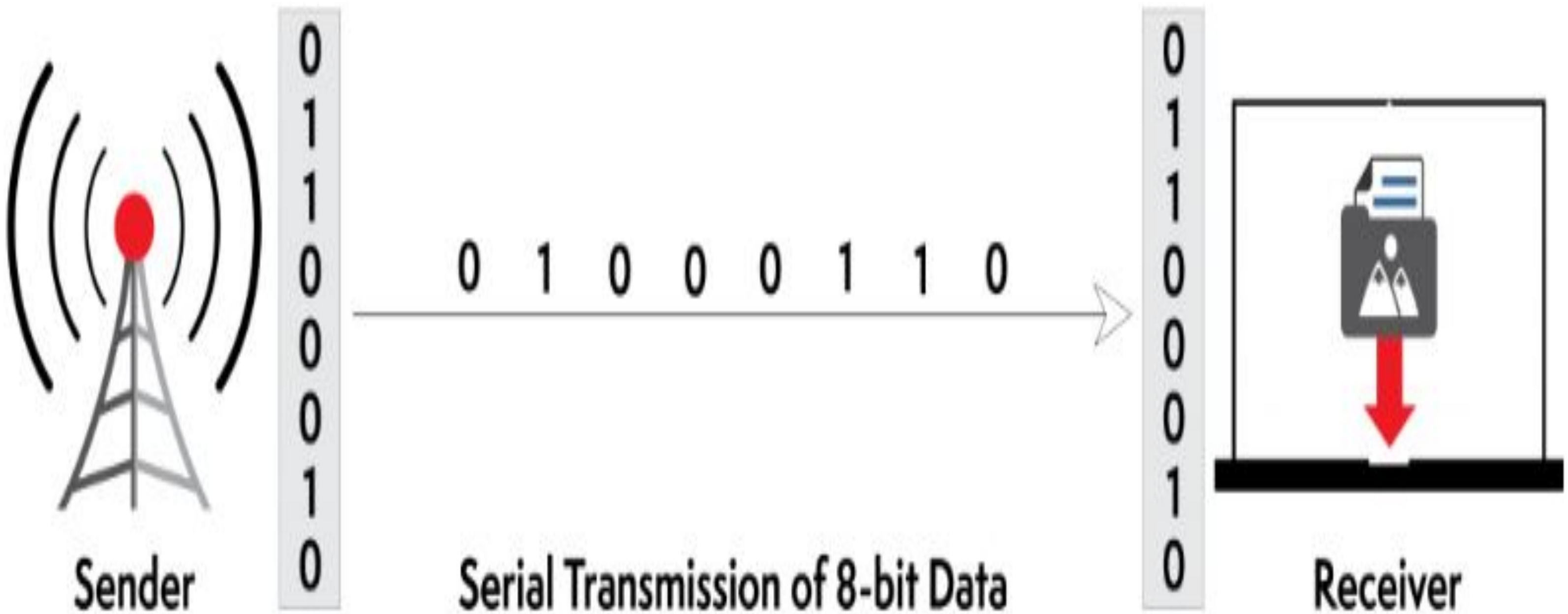
- Data transmission refers to the process of transferring data between two or more digital devices.
- Data is transmitted from one device to another in analog or digital format.
- Basically, data transmission enables devices or components within devices to speak to each other.
- There are two methods used to transmit data between digital devices: serial transmission and parallel transmission

Serial Data Transmission

INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- When data is sent or received using serial data transmission, the data bits are organized in a specific order, since they can only be sent one after another.
- The order of the data bits is important as it dictates how the transmission is organized when it is received.
- It is viewed as a reliable data transmission method because a data bit is only sent if the previous data bit has already been received.

Serial Data Transmission



Serial Data Transmission

- **Asynchronous Serial Transmission**
  Data bits can be sent at any point in time. Stop bits and start bits are used between data bytes to synchronize the transmitter and receiver and to ensure that the data is transmitted correctly. The time between sending and receiving data bits is not constant, so gaps are used to provide time between transmissions.

Serial Data Transmission

- The advantage of using the asynchronous method is that no synchronization is required between the transmitter and receiver devices. It is also a more cost effective method.
- A disadvantage is that data transmission can be slower, but this is not always the case.
- Serial transmission is normally used for long-distance data transfer. It is also used in cases where the amount of data being sent is relatively small. It ensures that data integrity is maintained as it transmits the data bits in a specific order, one after another. In this way, data bits are received in-sync with one another

Serial Data Transmission

Synchronous Serial Transmission

Data bits are transmitted as a continuous stream in time with a master clock. The data transmitter and receiver both operate using a synchronized clock frequency; therefore, start bits, stop bits, and gaps are not used. This means that data moves faster and timing errors are less frequent because the transmitter and receiver time is synced. However, data accuracy is highly dependent on timing being synced correctly between devices. In comparison with asynchronous serial transmission, this method is usually more expensive.

Parallel Data Transmission

- When data is sent using parallel data transmission, multiple data bits are transmitted over multiple channels at the same time.
- This means that data can be sent much faster than using serial transmission methods.

Parallel Data Transmission

- Given that multiple bits are sent over multiple channels at the same time, the order in which a bit string is received can depend on various conditions, such as proximity to the data source, user location, and bandwidth availability.
- Two examples of parallel interfaces can be seen below. In the first parallel interface, the data is sent and received in the correct order.
- In the second parallel interface, the data is sent in the correct order, but some bits were received faster than others.

Parallel Data Transmission

INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Example of Parallel Transmission – Data Received Correctly

Example of Parallel Transmission – Data Received Incorrectly

Parallel Data Transmission

- The main advantages of parallel transmission over serial transmission are:

- it is easier to program;
- data is sent faster.

Although parallel transmission can transfer data faster, it requires more transmission channels than serial transmission. This means that data bits can be out of sync, depending on transfer distance and how fast each bit loads.

- A simple of example of where this can be seen is with a voice over IP (VOIP) call when distortion or interference is noticeable. It can also be seen when there is skipping or interference on a video stream.

Parallel Data Transmission

Parallel transmission is used when:
- a large amount of data is being sent;
- the data being sent is time-sensitive;
- and the data needs to be sent quickly.

- A scenario where parallel transmission is used to send data is video streaming. When a video is streamed to a viewer, bits need to be received quickly to prevent a video pausing or buffering.
- Video streaming also requires the transmission of large volumes of data.
- The data being sent is also time-sensitive as slow data streams result in poor viewer experience.

Serial Vs Parallel

S.NO	SERIAL TRANSMISSION	PARALLEL TRANSMISSION
1.	In serial transmission, data(bit) flows in bi-direction.	In Parallel Transmission, data flows in multiple lines.
2.	Serial Transmission is cost efficient.	Parallel Transmission is not cost efficient.
3.	In serial transmission, one bit transferred at one clock pulse.	In Parallel Transmission, eight bits transferred at one clock pulse.
4.	Serial Transmission is slow in comparison of Parallel Transmission.	Parallel Transmission is fast in comparison of Serial Transmission.
5.	Generally, Serial Transmission is used for long distance.	Generally, Parallel Transmission is used for short distance.

Unit – I End