ADHIPARASAKTHI COLLEGE OF ARTS AND SCIENCE

(Autonomous)

G.B. Nagar, Kalavai - 632506

Data and Communication Networks

UNIT - I

INTRODUCTION TO DATA COMMUNICATION

- **Data communications** are the exchange of data between two devices via some form of transmission medium such as a wire cable or wireless

Components of a data communication system

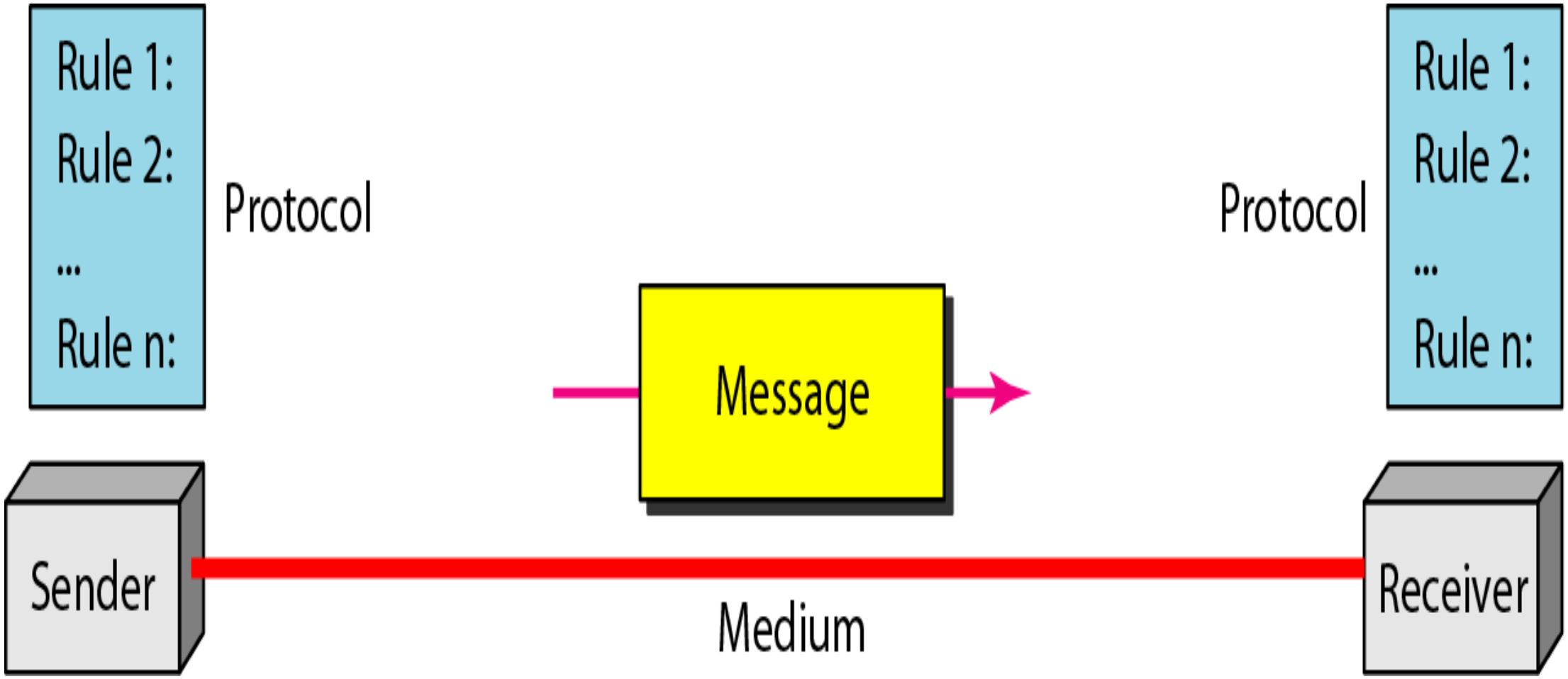
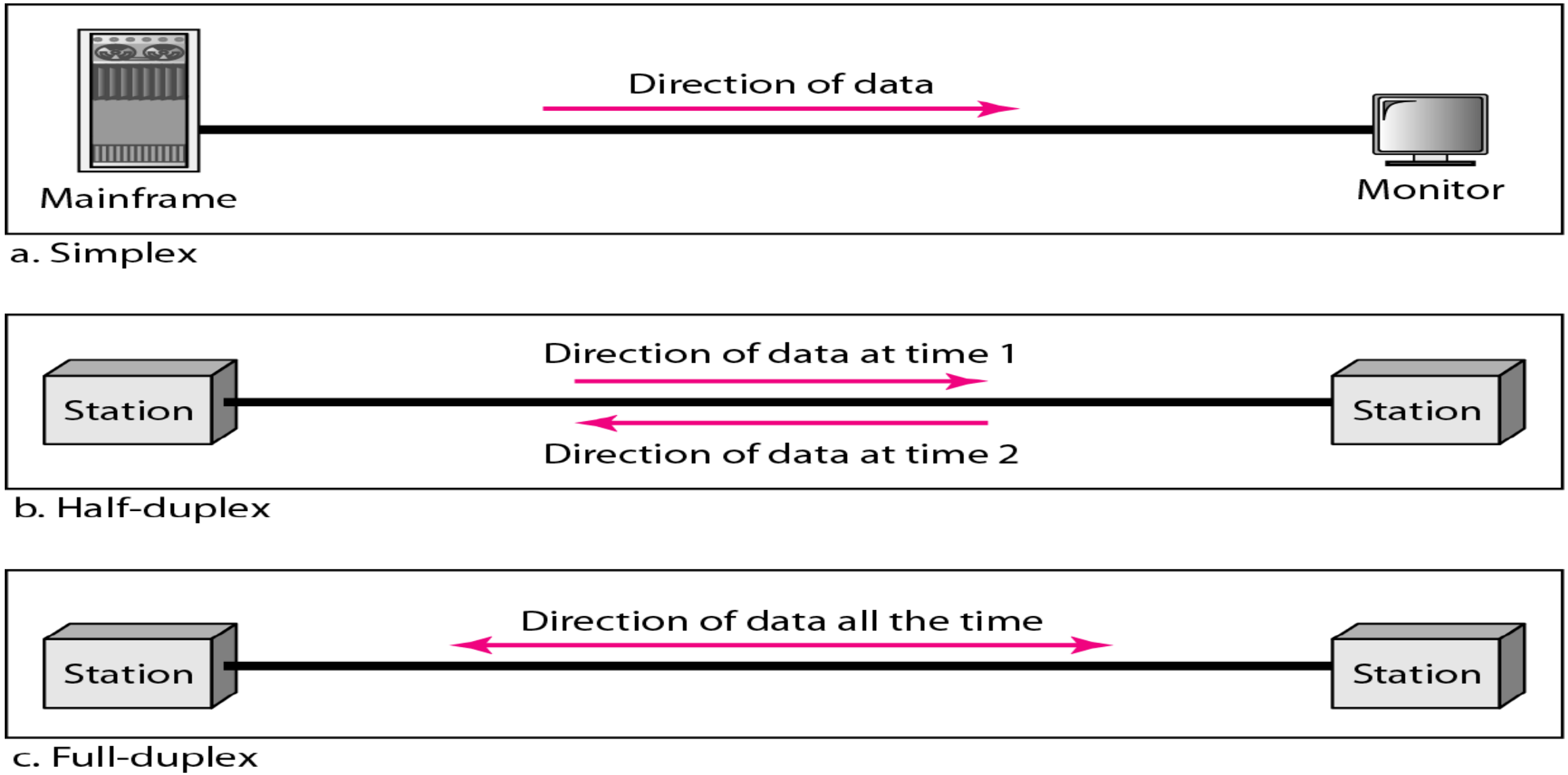


Figure 1.2 *Data flow (simplex, half-duplex, and full-duplex)*



NETWORKS

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

Network Criteria :

Performance

Depends on Network Elements

Measured in terms of Delay and Throughput

- **Reliability**

Failure rate of network components

Measured in terms of availability/robustness

- **Security**

Data protection against corruption/loss of data due to

- Errors
- Malicious users

Physical Structures

Type of Connection

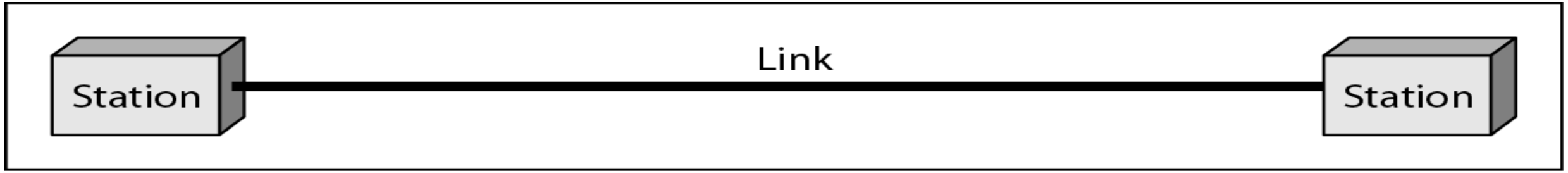
- **Point to Point - single transmitter and receiver**
- **Multipoint - multiple recipients of single transmission**

Physical Topology

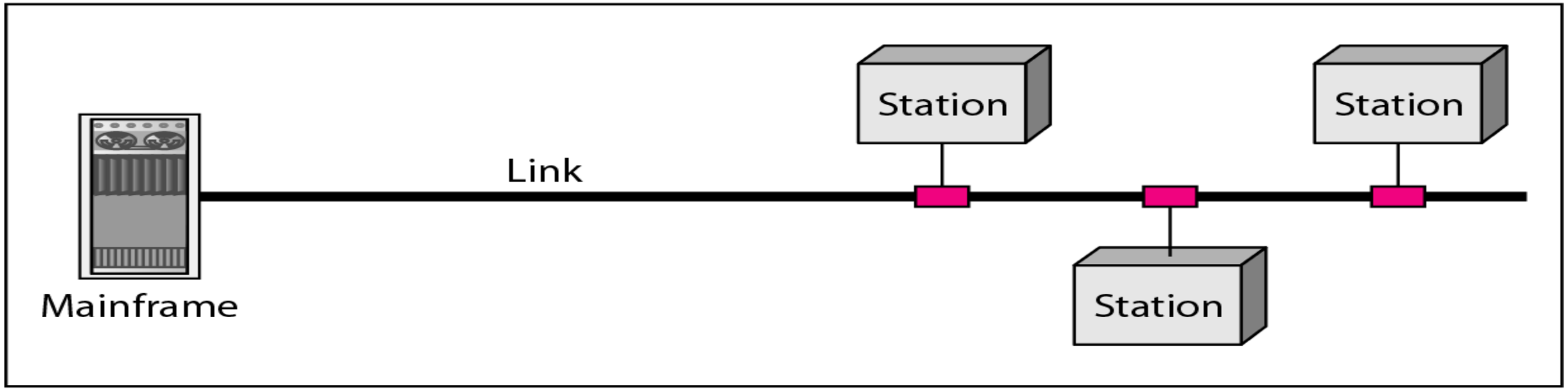
- **Connection of devices**
- **Type of transmission - unicast, multicast, broadcast**

Types of connections:

point-to-point and multipoint



a. Point-to-point



b. Multipoint

Categories of topology

Topology

- **Bus**
- **Ring**
- **Star**
- **Hybrid**
- **Mesh (Complete)**

Figure 1.7 *A bus topology connecting three stations*

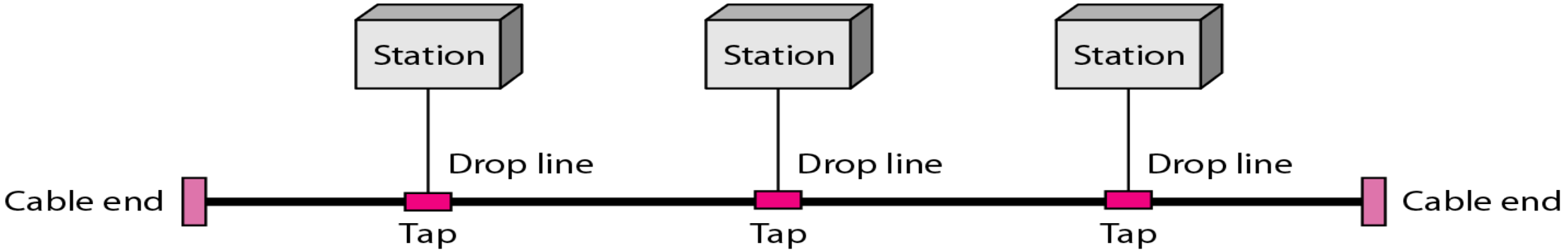
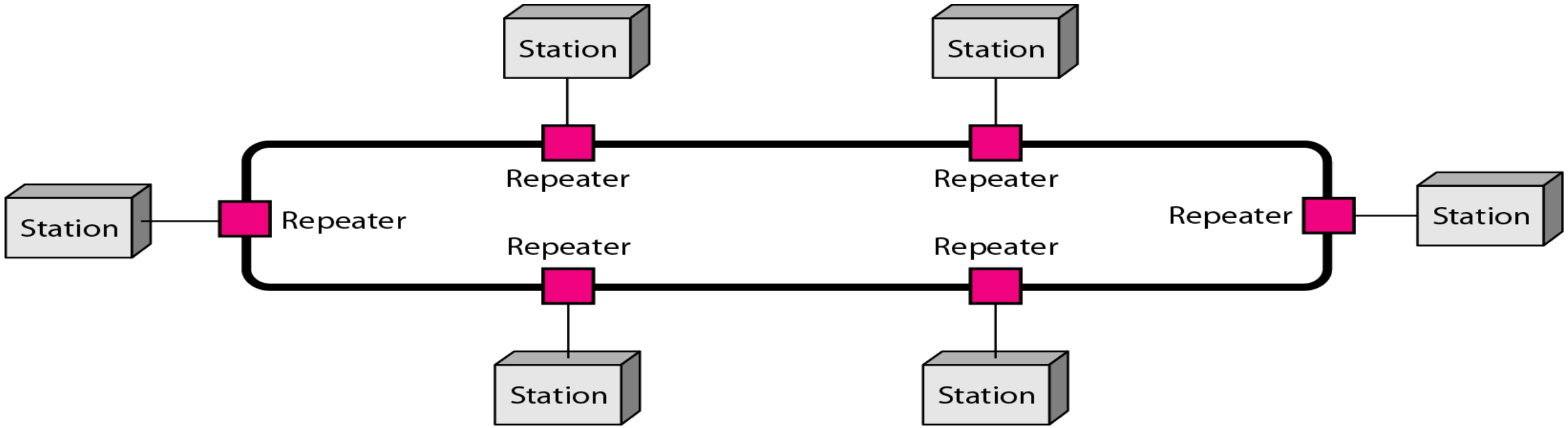
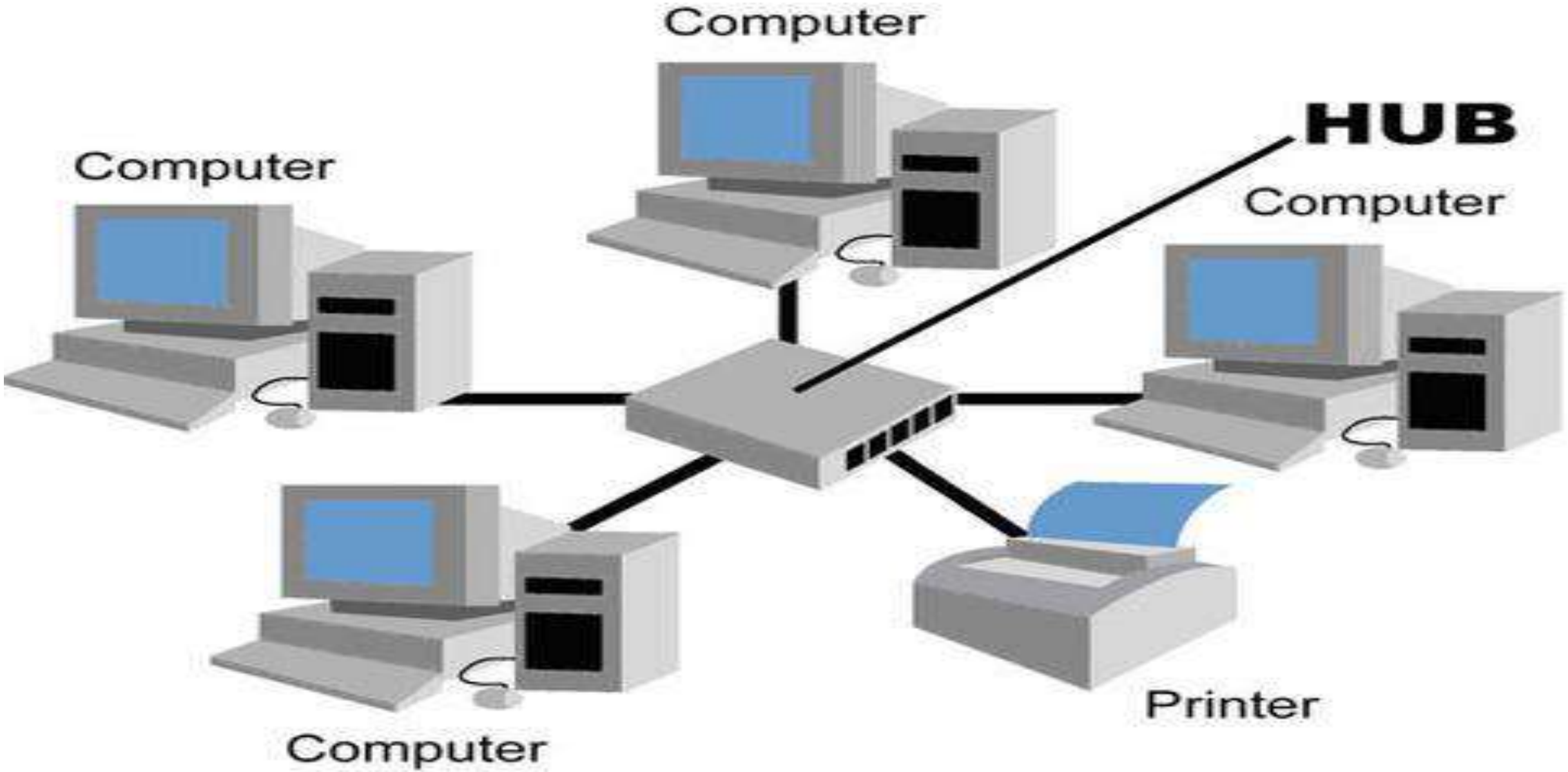


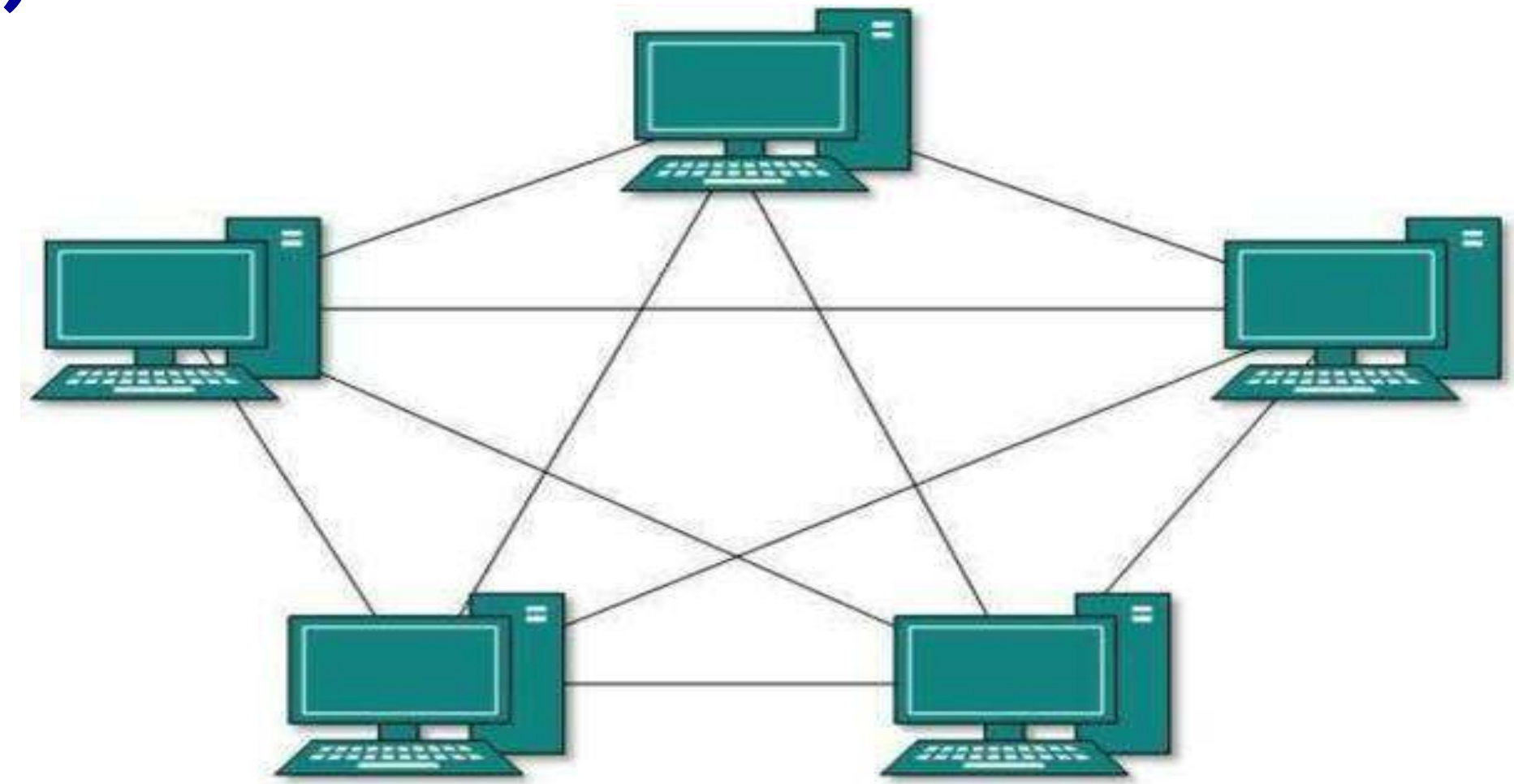
Figure 1.8 *A ring topology connecting six stations*



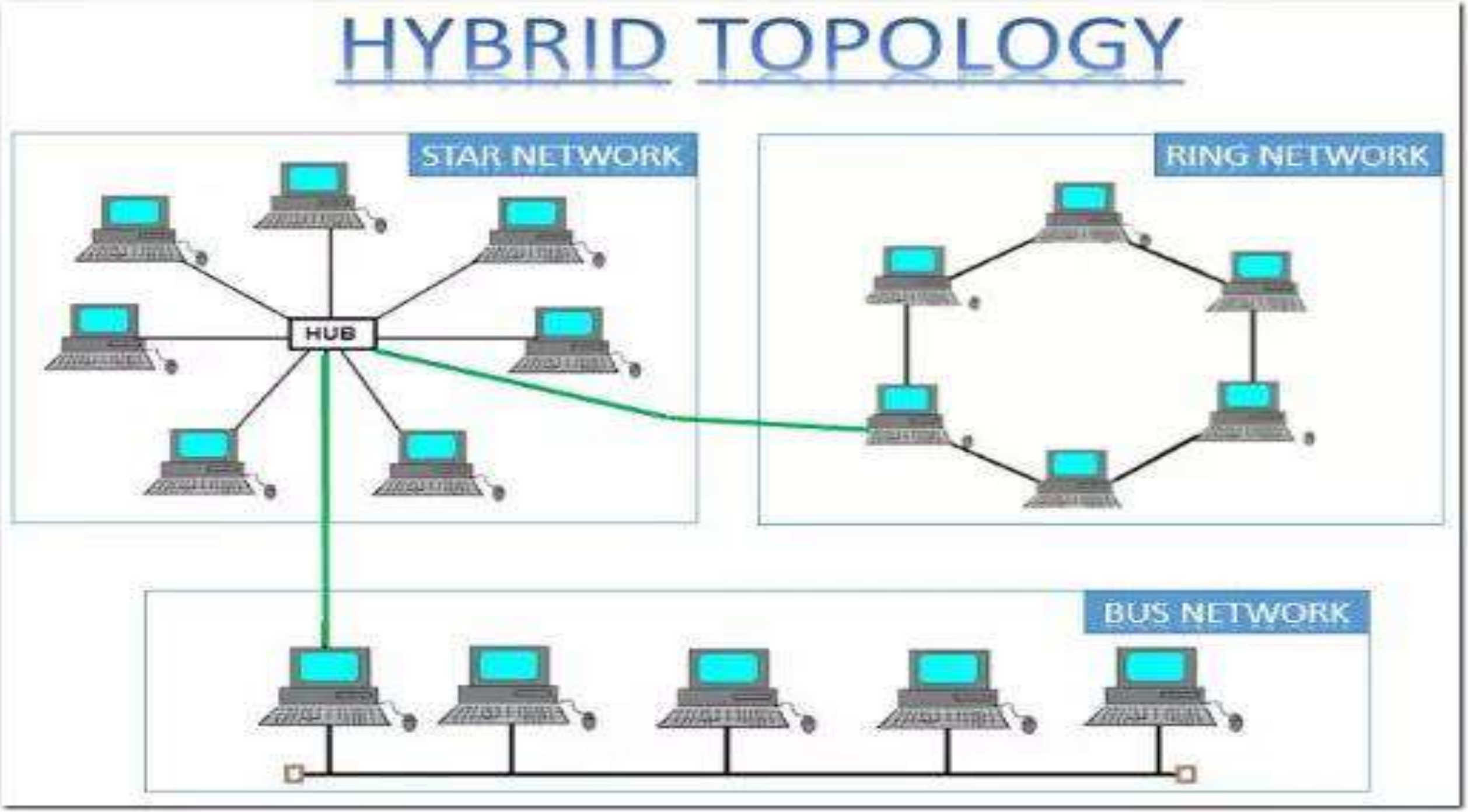
A star topology connecting four stations



A fully connected mesh topology (5 devices)



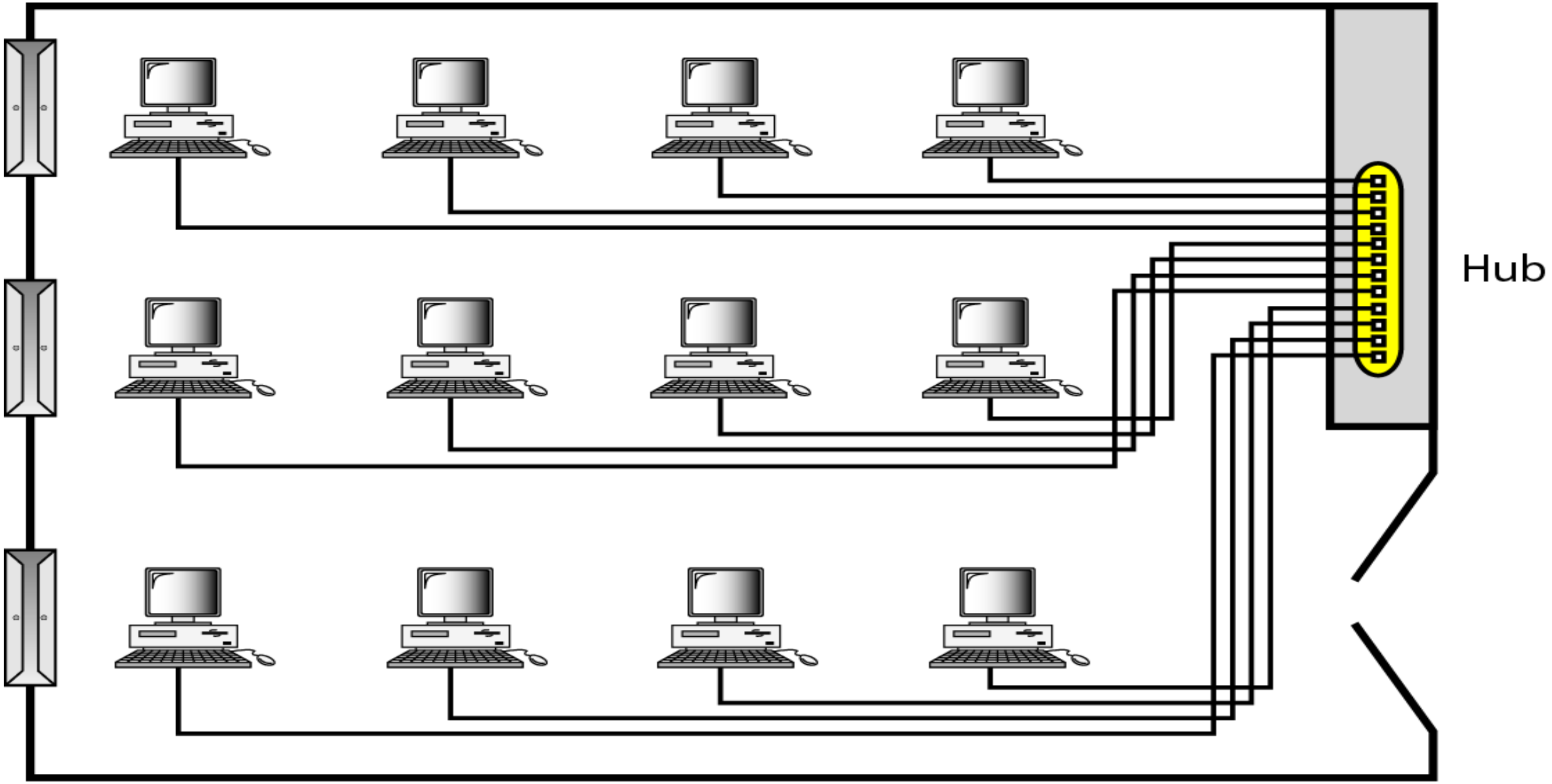
HYBRID TOPOLOGY

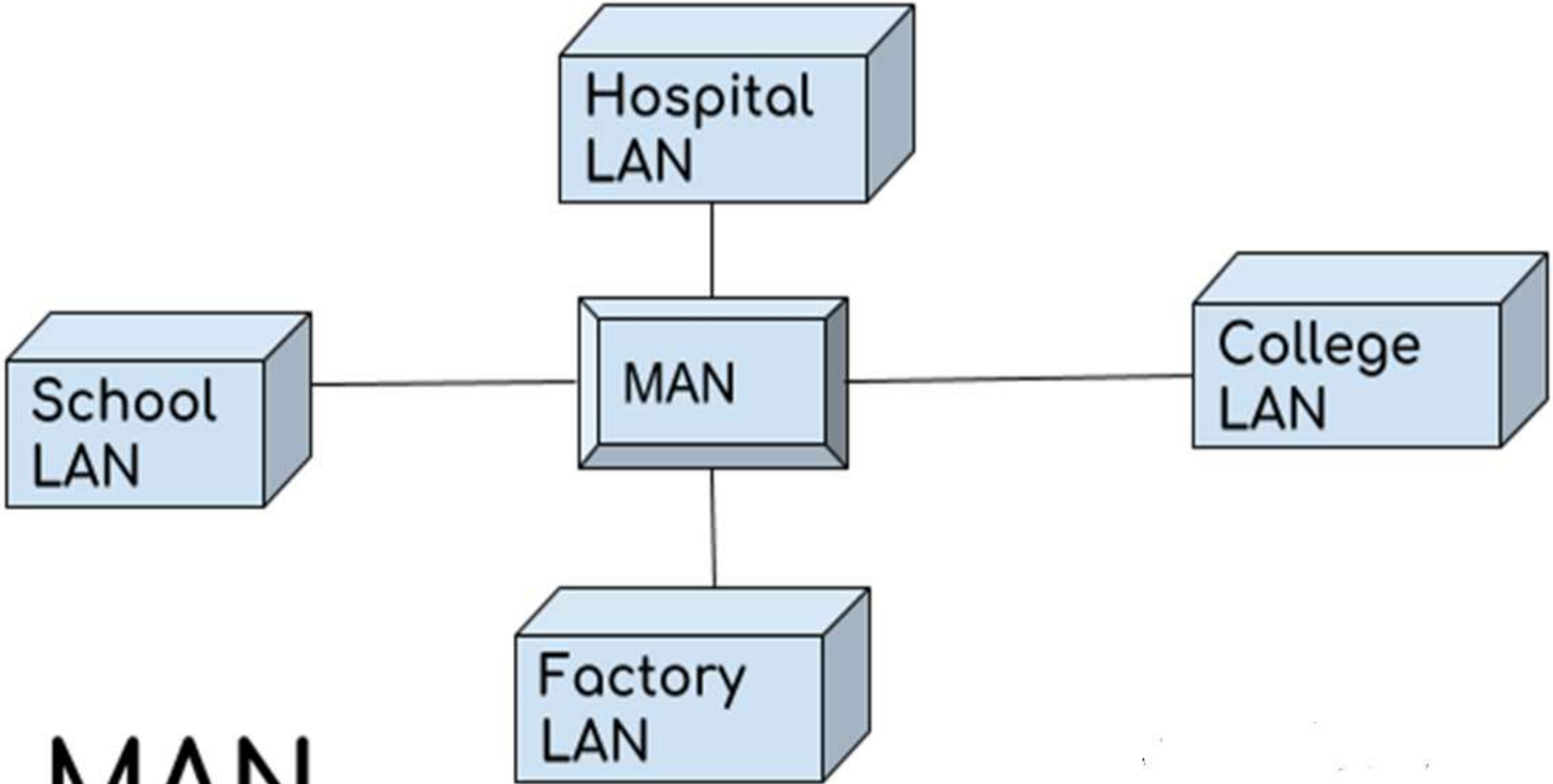


Categories of Networks

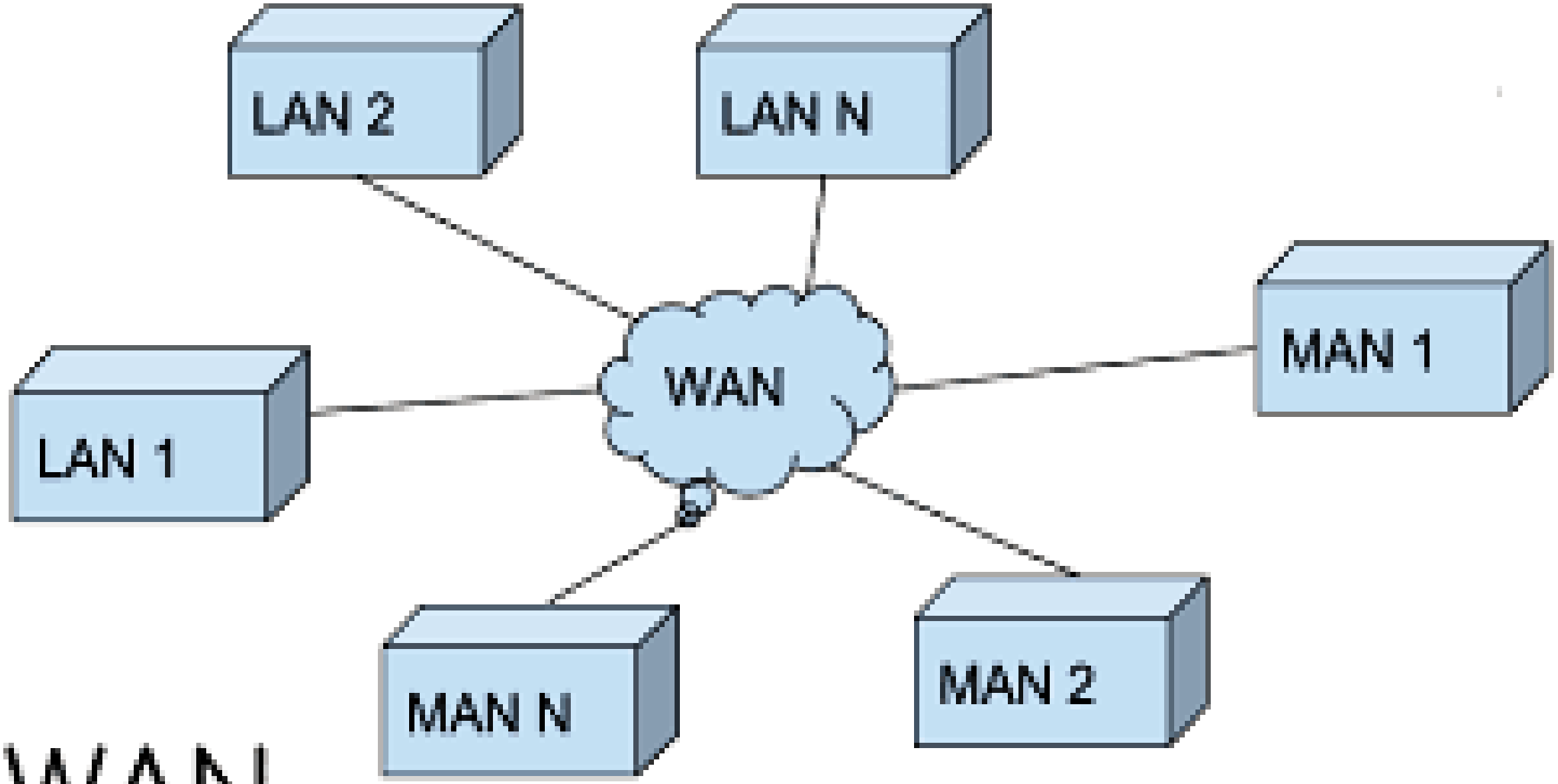
- **Local Area Networks (LANs)**
  - **Short distances**
  - **Designed to provide local interconnectivity**
- **Metropolitan Area Networks (MANs)**
  - **Provide connectivity over areas such as a city, a campus**
- **Wide Area Networks (WANs)**
  - **Long distances, Combination of LAN and WAn**
  - **Provide connectivity over large areas**

An isolated LAN connecting 12 computers to a hub in a closet





MAN



WAN

THE INTERNET

- **The Internet has revolutionized many aspects of our daily lives.**
- **It has affected the way we do business as well as the way we spend our ease time.**
- **The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.**

PROTOCOLS

- **A protocol is synonymous with rule.**
- **It consists of a set of rules that govern data communications.**
- **It determines what is communicated, how it is communicated and when it is communicated.**
- **The key elements of a protocol are**

  syntax,

  semantics and timing

Elements of a Protocol

- **Syntax**
  - **Structure or format of the data**
  - **How it is presented**
- **Semantics**
  - **Interprets the meaning of each section bits (DB)**
  - **How is a particular pattern to be interpreted**
  - **Knows which fields define what action**
- **Timing**
  - **When data should be sent/ received and what**
  - **Speed at which data should be sent or speed at which it is being received.**

STANDARDS

- **A standard provides a model for development of a product, which is going to develop.**
- **Standards are essential to create and maintain a product.**
- **Agencies**

    1. **ANSI (American National Standards Institute)**
    2. **(IEC) International Electro – technical Commission**

3. International Telecommunication Union (ITU)
4. Institute of Electrical and Electronics Engineers (IEEE)
5. International Organization for Standardization (ISO)
6. Internet Society (ISOC) and the Associated Internet Engineering Task Force (IETF)
7. The Internet Architecture Board (IAB)

8. Internet Research Task Force (IRTF)

9. Internet Engineering Steering Group

10. Telecommunication Industry Association (TIA)

ANSI :

- ANSI is a private, non-governmental agency where members are manufactures, users and industry
- It has nearly 1000 members.

IEC

- **IEC is a non-governmental agency, standards for data processing, Interconnections and Safety in office**
- **Involved in the development of the JPEG, compression standards**

ITU

ITU is affiliated with the United Nations, closely communication industries

ITU three sectors:

ITU – R deals with radio communication

ITU – D is development sector

ITU – T deals with telecommunications

ITU sets standards for modems, e-mail and digital telephone systems.

ITU standards

- ‘V’ standards modem communication
- ‘X 400’ international exchange of e-mail
- ‘X 500’ creation of a Worldwide e-mail directory
- ‘X.25’ WAN standards.

IEEE

- IEEE is largest organization in the world.
- Involved computing, communication and the process

Specifications:

802.1 – overview of the 802 standards

802.2 – Logical Link Control and N/w connectivity

802.3 – Multiple Access with Collision Detection

802.4 – Token passing

802.5 – Communication between LANs and WANs

802.6 – LAN and WAN n/w with high-speed connectionless networking

802.7 – Broadband cable technologies

802.8 – Fibre optic cable technologies

802.9 – N/w services, such as voice and data

802.10 – LAN and WAN security

802.11 – Wireless connectivity

ISO

- ISO developed a communication architecture called the Open Systems Interconnections (OSI)
- OSI model contains 7 Layer protocols.

ISOC and IETF

- International community where members include n/w designers, vendors and researchers.
- Operations of the internet and in its evaluation.

- **Technical aspects of the internet such as applications, operations, management, routing security and transport services**
- **Focuses on technical internet issues.**

IAB

- Technical advisory group of the ISOC and a committee of the IETF
- Responsible for advising technical directions.

IRTF

- To promote research of importance
- Related to Internet protocols, applications, architecture and technology

Internet Engineering Steering Group

- Executive committee of the IETF.
- Concerned with Internet protocols and standards.

TIA

- Develop telecommunication and cabling standards.
- Concerned with Internet protocols and standards.

APPLICATIONS OF DATA COMMUNICATIONS

Applications are the software programs used by people to communicate over the network.

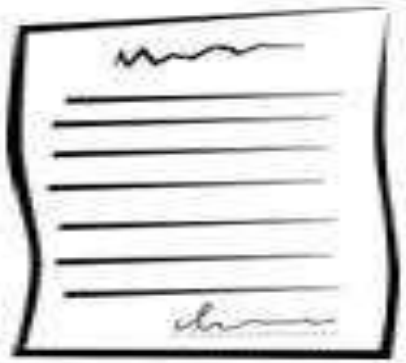
Applications:

1. **Electronic Messing**

   E-mail, it is possible to send a message to remote location. (e.g : Gmail, yahoo, rediffmail, etc...)

2. **Facsimile Machine (Fax) – (net fax, hello fax...)**

   Electronic equivalent of an image on a sheet of paper and then sends the image over Telephone lines. Other end-users creates the original image



1- Fax is Scanned And Encoded By Sending Fax Machine

2 - Transmission Happens Across Telephone Network

orange

verizon

vodafone

telenor

3- Fax is Decoded And Printed by Receiving Fax Machine

3. Teleconferencing (Googlemeet, ZOOM, GoToWebinar...)

- Conference occur without the participants being the same place, Includes
  - Communicate through their keyboards & monitors
  - Voice confe rencing, where participants at a no.of locations communicate simultaneously.
  - Video conferencing where participants can see as well as talk to one another

4. Cellular Telephone

- Services of a telephone company
- Connections establish even while traveling.

5. Information Services (Google, Yahoo, Amazon, Sify….)

- Built boards and data banks
- Free exchange of some s/w, files or other information
- A www offering the technical specifications.

6. Financial Services (Oracle, Ms-Excel)

Financial services includes

Credit history, Foreign exchange, investment services and electronic funds transfer.

7. Marketing and sales

To collect, exchange, and examine data related to customer requires and product development cycles.

OPEN SYSTEMS AND OSI MODEL

- To provide a basis for interconnecting dissimilar systems for the purpose of information exchange.

Guidelines

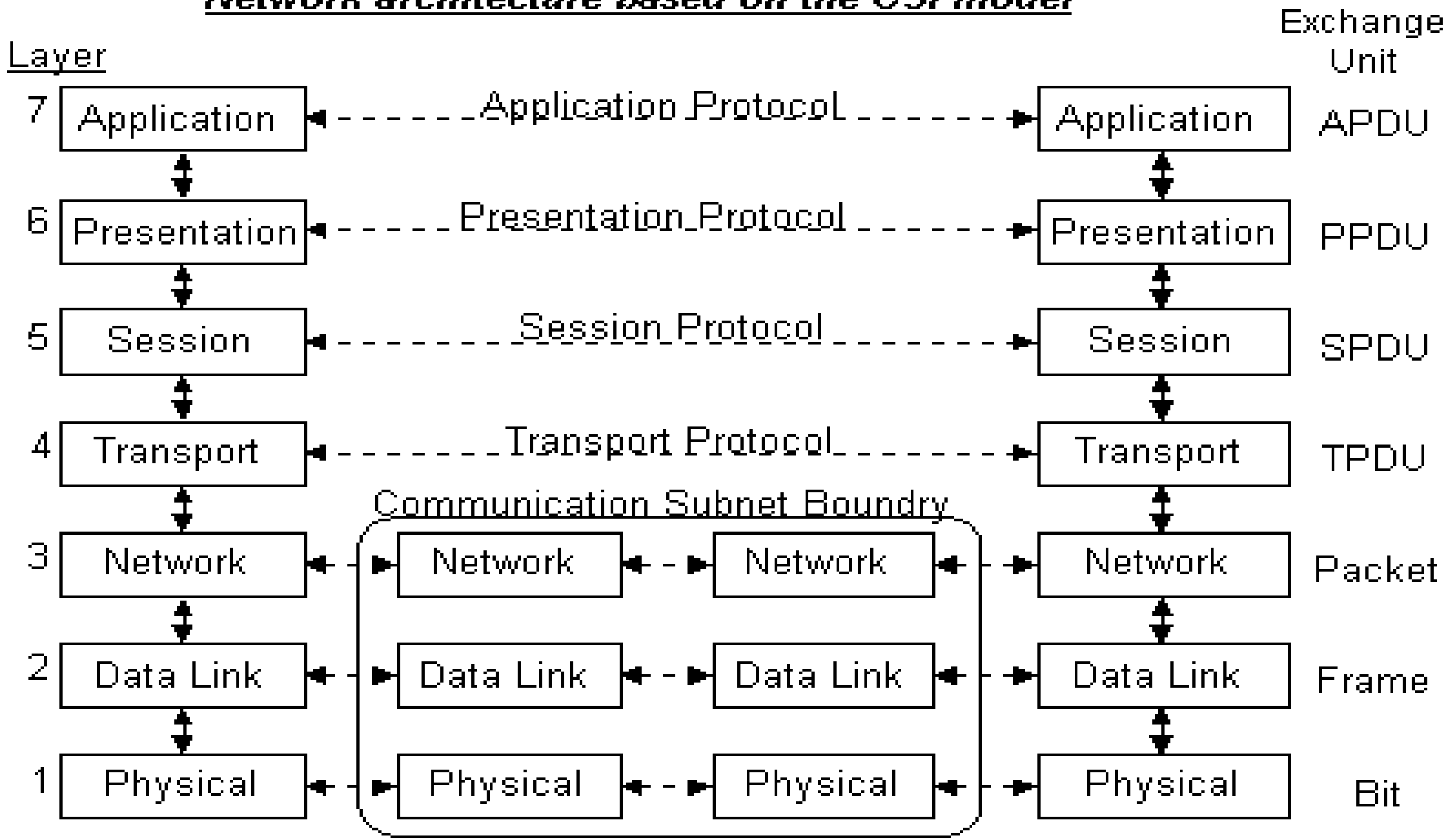
- How n/w devices contact each other?
- How devices using different protocols?
- How a n/w device knows when to transmit or not to transmit?
- How the physical n/w devices are arranged and how they connect?
- Methods to ensure that n/w transmissions are received correctly.

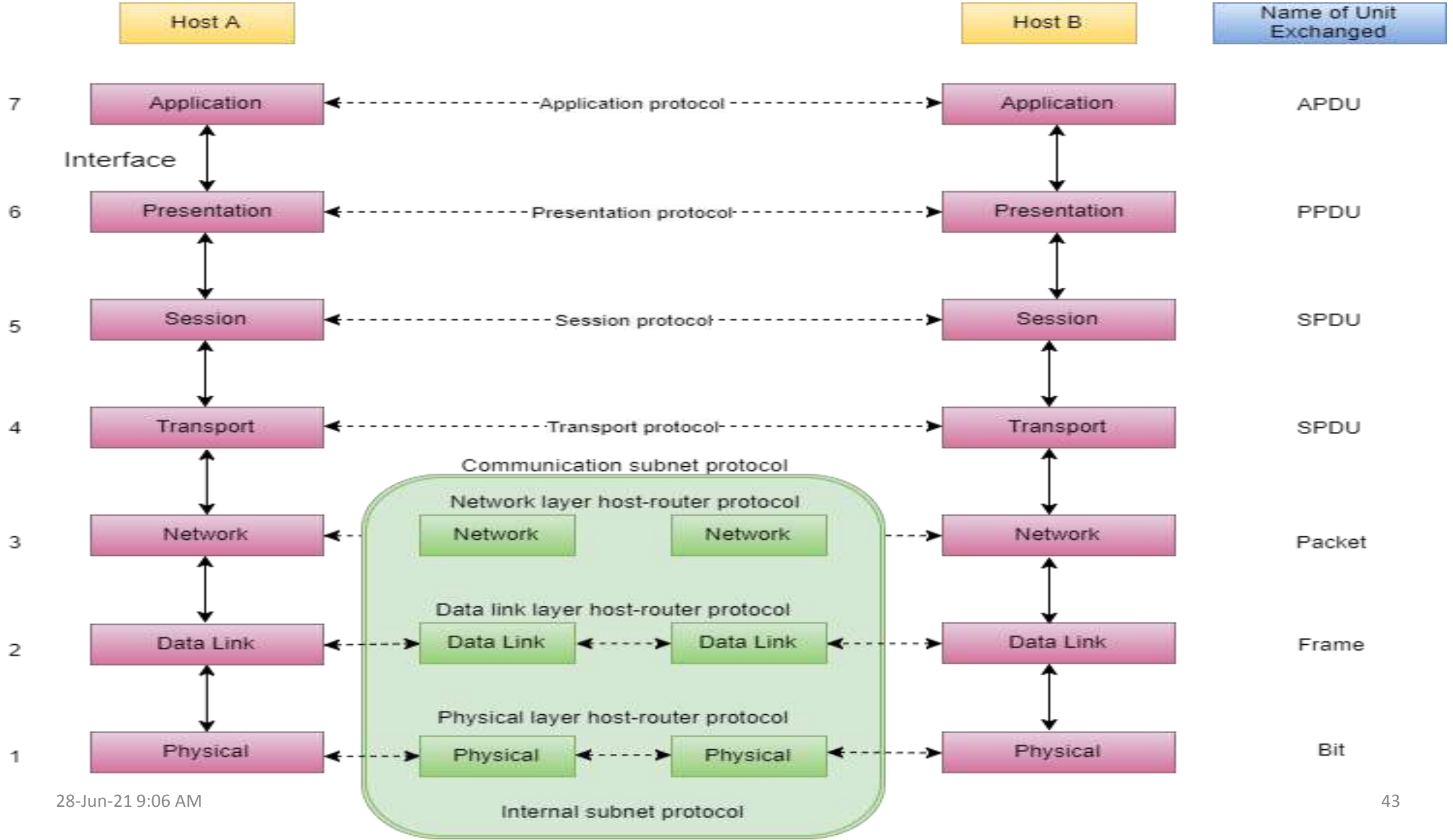
- **How n/w devices maintain a consistent rate of data flow?**
- **How electronic data is represented on the network media?**

Layer of OSI Model

Each layer carries out a specific set of functions.

1. **Application layer (Top position)**
2. **Presentation layer**
3. **Session layer**
4. **Transport layer**
5. **Network layer**
6. **Data link layer**
7. **Physical layer (Bottom position)**


Network architecture based on the OSI model
Layer
Exchange Unit
7
Application
Application Protocol
Application
APDU
6
Presentation
Presentation Protocol
Presentation
PPDU
5
Session
Session Protocol
Session
SPDU
4
Transport
Transport Protocol
Transport
TPDU
Communication Subnet Boundry
3
Network
Network
Network
Network
Packet
2
Data Link
Data Link
Data Link
Data Link
Frame
1
Physical
Physical
Physical
Physical
Bit


Host A
Host B
Name of Unit Exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
SPDU
Communication subnet protocol
Network layer host-router protocol
3
Network
Network
Network
Network
Packet
Data link layer host-router protocol
2
Data Link
Data Link
Data Link
Data Link
Frame
Physical layer host-router protocol
1
Physical
Physical
Physical
Physical
Bit
Internal subnet protocol

Functions of OSI Layers

Physical Layer

- Provides the transfer medium (such as cable)
- Translate data
- Determine the voltage levels used for data
- Determine the signal type : digital or analog
- Includes the physical layout of the n/w

- **It defines the mechanical, electrical, functional and procedural specification.**

Data Link layer

- Constructs data frames with appropriate format
- Check error, recognizes a format.
- Retransmits data if there is an error
- Examines device address and acknowledge
- Uses Error detection and correction technique to ensure that a transmission contains no errors.

Network Layer

- Determines the network path on which to route packets
- Helps reduce network congestion (jamming)
- Establish virtual circuits
- Routes frames to other Networks, re-sequencing packet transmission when needed

- **Its responsible for delivery of a packet from source to destination**

Transport Layer

- **Ensures reliability (consistency)of packet transmission from node to node**
- **Ensures data is sent and received in the same order**
- **Provides acknowledgement when a packet is received**
- **Monitors for packet transmission errors, and resends damaged packets.**
- **Carries out error detection and recovery**

Session Layer

- **Initiates the communications link**
- **Makes sure the communications link is maintained**
- **Determines which node transmits at any point in time (example: which one transmit first)**
- **Session can organize, synchronize and manage the transfer of information.**

Presentation Layer

- **Translates data to a format the receiving node understands (ASCII).**
- **Performs data encryption and decryption**
- **Performs data compression.**
- **Translates data from representation to another.**

Application Layer

- **Enables sharing of remote drives and printers**
- **Handle e-mail, job entry, resource allocation**
- **Provides file transfer services and file management services.**
- **Browser application uses the HTTP to access www document**

TCP/IP ARCHITECURE

- **OSI model was slow**
- **The government's Advanced Research Project Agency (ARPA) developed a protocols called Transmission Control Protocol/ Internet Protocol (TCP/IP).**
- **It support large –sized n/w . UNIX, Windows NT, Novell n/w**
- **TCP/IP protocol suite is made of 5 layers**

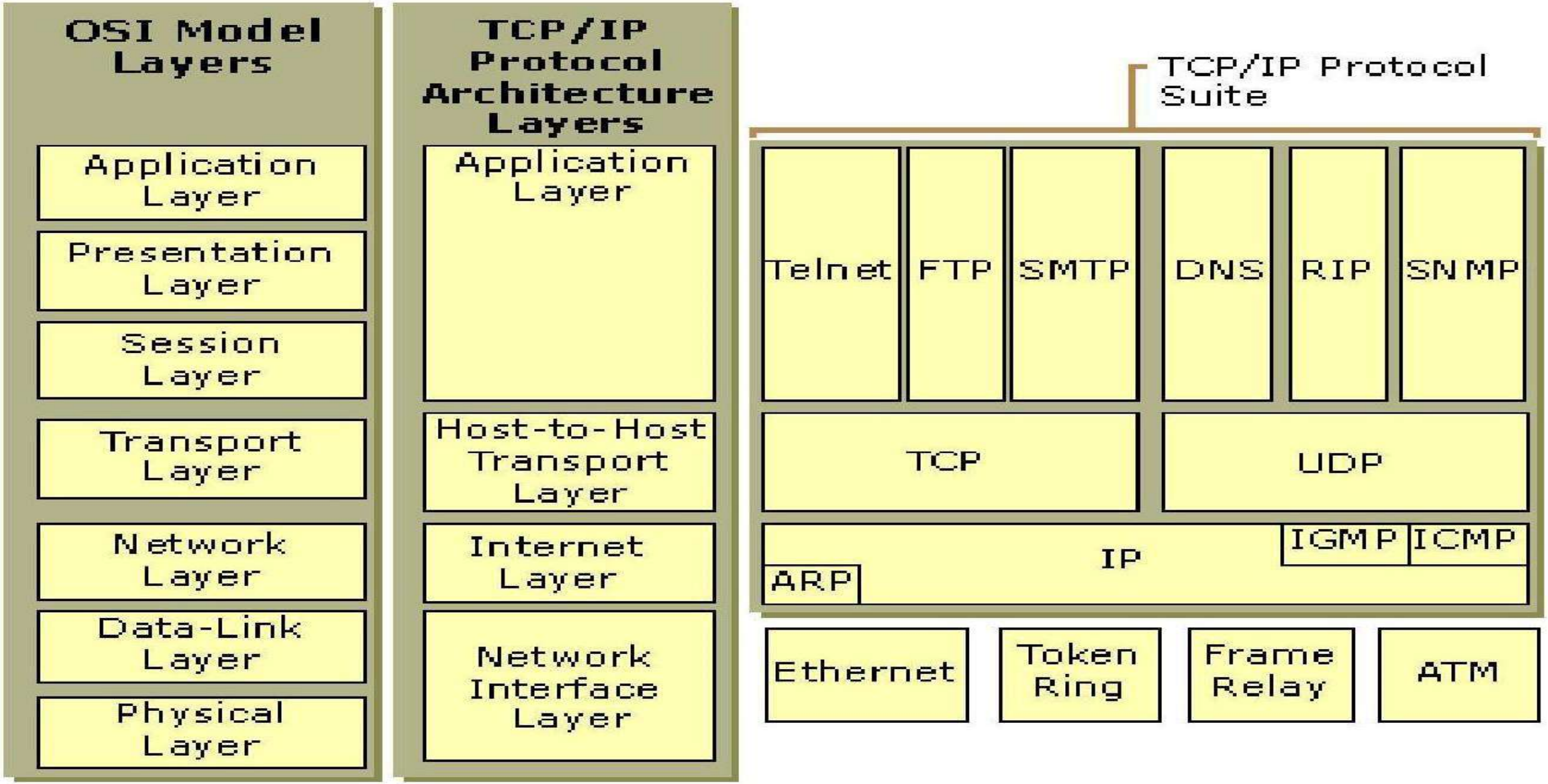


Figure 1.1 TCP/IP Protocol Architecture

Network Interface Layer

- **The Network Interface layer is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium.**
- **TCP/IP was designed to be independent of the network access method, frame format, and medium.**

These include

- **LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay.**
- **Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).**

- **The Network Interface layer encompasses the Data Link and Physical layers of the OSI model.**

Transport Layer

- **It decides if data transmission should be on parallel path or single path.**
- **Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.**
- **The applications can read and write to the transport layer.**

- **It adds header information to the data.**
- **Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.**
- **Transport layer also arrange the packets to be sent, in sequence.**

Host-to-Host Transport Layer

TCP(Transmission Control Protocol):

It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.

UDP(User-Datagram Protocol):

It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Internet Layer

- **The Internet layer is responsible for addressing, packaging, and routing functions.**
- **The core protocols of the Internet layer are**

  IP, ARP, ICMP, and IGMP.

The Internet Protocol (IP):

IP is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.

The Address Resolution Protocol (ARP)

- **ARP is responsible for the resolution of the Internet layer address to the Network**
- **Interface layer address such as a hardware address.**

The Internet Control Message Protocol (ICMP)

ICMP is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.

The Internet Group Management Protocol (IGMP)

IGMP is responsible for the management of IP multicast groups.

Application Layer

- **The TCP/IP specifications of the protocol. TELNET, FTP, SMTP, DNS etc.**

TELNET (Terminal Network)

Telnet is a two-way communication protocol which allows connecting to a remote machine and run applications on it.

FTP(File Transfer Protocol)

FTP is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.

SMTP(Simple Mail Transport Protocol)

SMTP is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.

DNS(Domain Name Server)

- **DNS is resolves an IP address into a textual address for Hosts connected over a network.**
- **It allows peer entities to carry conversation.**
- **It defines two end-to-end protocols: TCP and UDP**

OSI Model	TCP/IP model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.

OSI follows a vertical approach.	**TCP/IP follows a horizontal approach.**
OSI model use two separate layers physical and data link to define the functionality of the bottom layers.	**TCP/IP uses only one layer (link).**
OSI layers have seven layers.	**TCP/IP has four layers.**
OSI model, the transport layer is only connection-oriented.	**A layer of the TCP/IP model is both connection-oriented and connectionless.**

In the OSI model, the data link layer and physical are separate layers.	**In TCP, physical and data link are both combined as a single host-to-network layer.**
Session and presentation layers are a one of the part of OSI model.	**There is no session and presentation layer in TCP model.**
It is defined after the advent of the Internet.	**It is defined before the advent of the internet.**
The minimum size of the OSI header is 5 bytes.	**Minimum header size is 20 bytes.**

DATA TRANSMISSION BASICS

- **The term ‘data’ for describing a set or block of one or more digitally encoded alphabetic and numeric characters being exchanged between two devices**
- **Two communicating parties must also exchange control messages**
- **The loss or corruption of a single bit information can be critical**

- **Take adequate precautions to detect and if necessary, correct any possible loss of information during transmission.**
- **Correct transmission errors.**
- **Keyboard with a unique pattern 7 or 8 bits, means that 128 or 256 elements.**
- **Codes are used EBCDIC and ASCII**

- **EBCDIC is an 8 bit code, manufactured by IBM**
- **ASCII is defined by ITU-T, it is 7 bit code.**
- **Booth coding schemes cater for all the normal alphabetic, numeric and punctuation characters.**

Thank You...

ADHIPARASAKTHI COLLEGE OF ARTS AND SCIENCE

(Autonomous)

G.B. Nagar, Kalavai - 632506

Data and Communication Networks

UNIT - II

WIDE AREA NETWORKS

- **LAN uses include file transfer, e-mail and file servers just as for WAN.**
- **Topics to be covered**
    1. **WAN Transmission Methods**
    2. **WAN carrier Types**
    3. **WAN Transmission Equipment**
    4. **WAN Design and Multicast Consideration**
    5. **WAN protocols**

WAN Transmission Methods

- **Use different switching Techniques**
- **Create one or more data paths called channels for transmitting data.**
- **Switching can enable multiple nodes to simultaneously transmit and receive data.**

Common Switching Techniques

Time- Division Multiple Access (TDMA)

Frequency – Division Multiple Access (FDMA)

Statistical Multiple Access

Circuit Switching

Message Switching

Packet Switching

Time – Division Multiple Access (TDMA)

- **TDMA divides the channels into distinct time slots.**
- **A 24-hours TV programming, where the time has been specified for a particular program.**
- **Synchronization with its time slots.**

Frequency – Division Multiple Access (FDMA)

- **FDMA divides the channels into frequencies instead of time slots.**
- **Each channel has its own broadcast frequency and bandwidth.**
- **Four channels are**

  Listener, Talk show, Base ball game, News

Statistical Multiple Access (SMA)

- **To use in WAN Technologies such as X.25, ISDN and frame relay**
- **Bandwidth is dynamically allocated according to application need.**
- **After file is transmitted, the switch relocates bandwidth to another channel.**
- **It might give 15kb for an active word-processing file, 7MB for an Image from a scanner and 1.2 MB for printing a graphic**

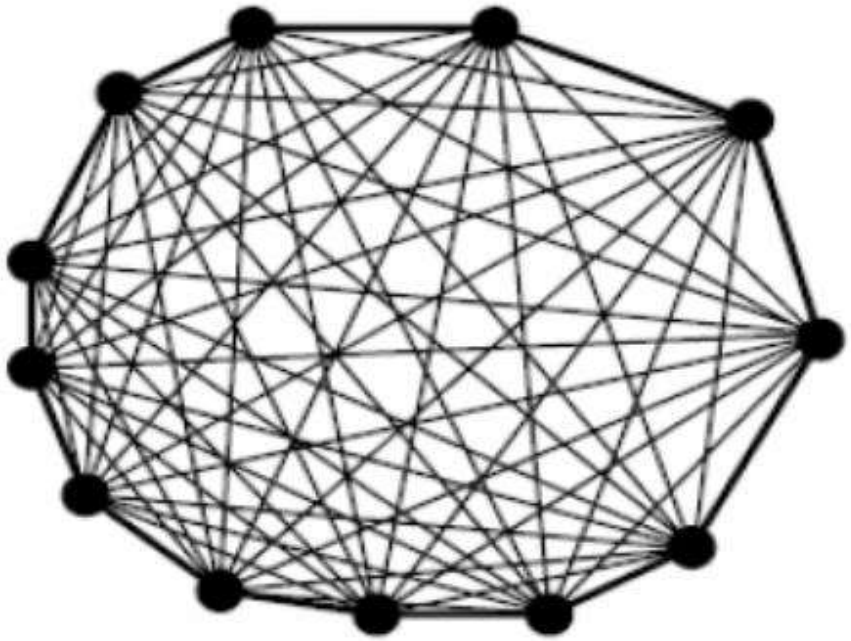
Circuit Switching

- **Creating a physical circuit between the sending and receiving node, similar to a telephone call between two parties.**
- **Three phase :**

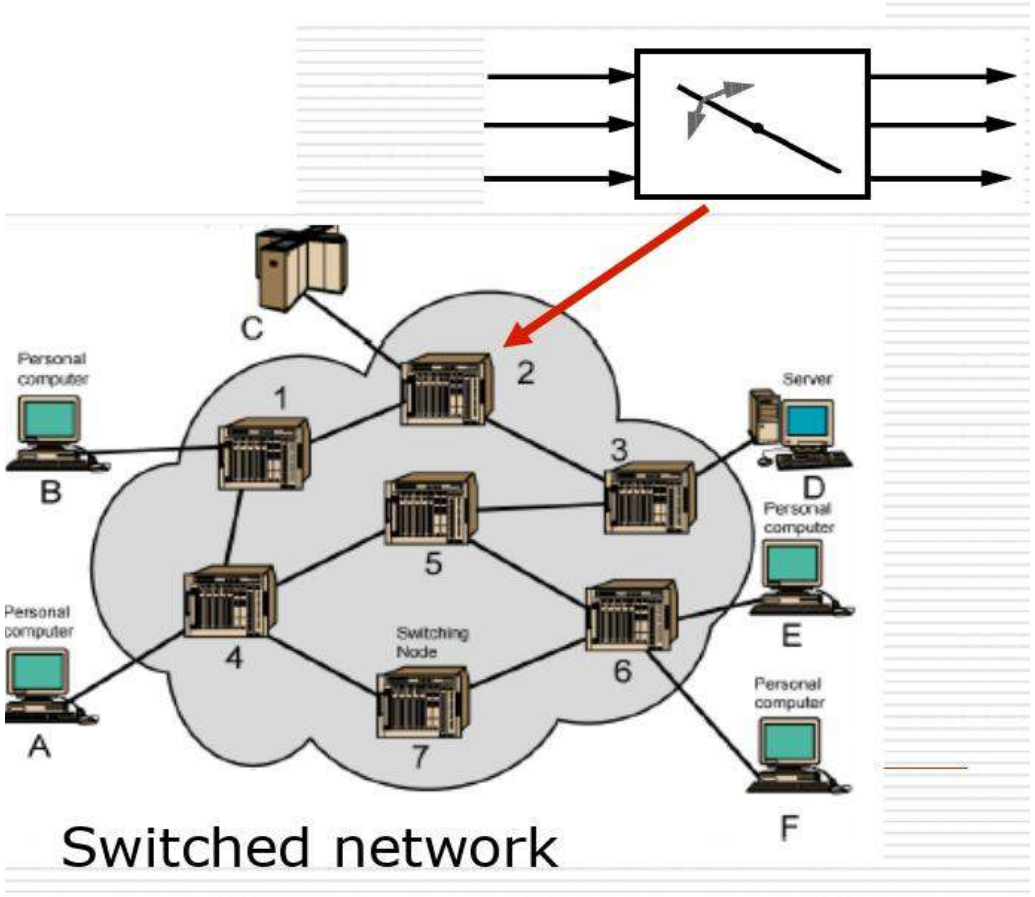
  Circuit establishment

  Data transfer

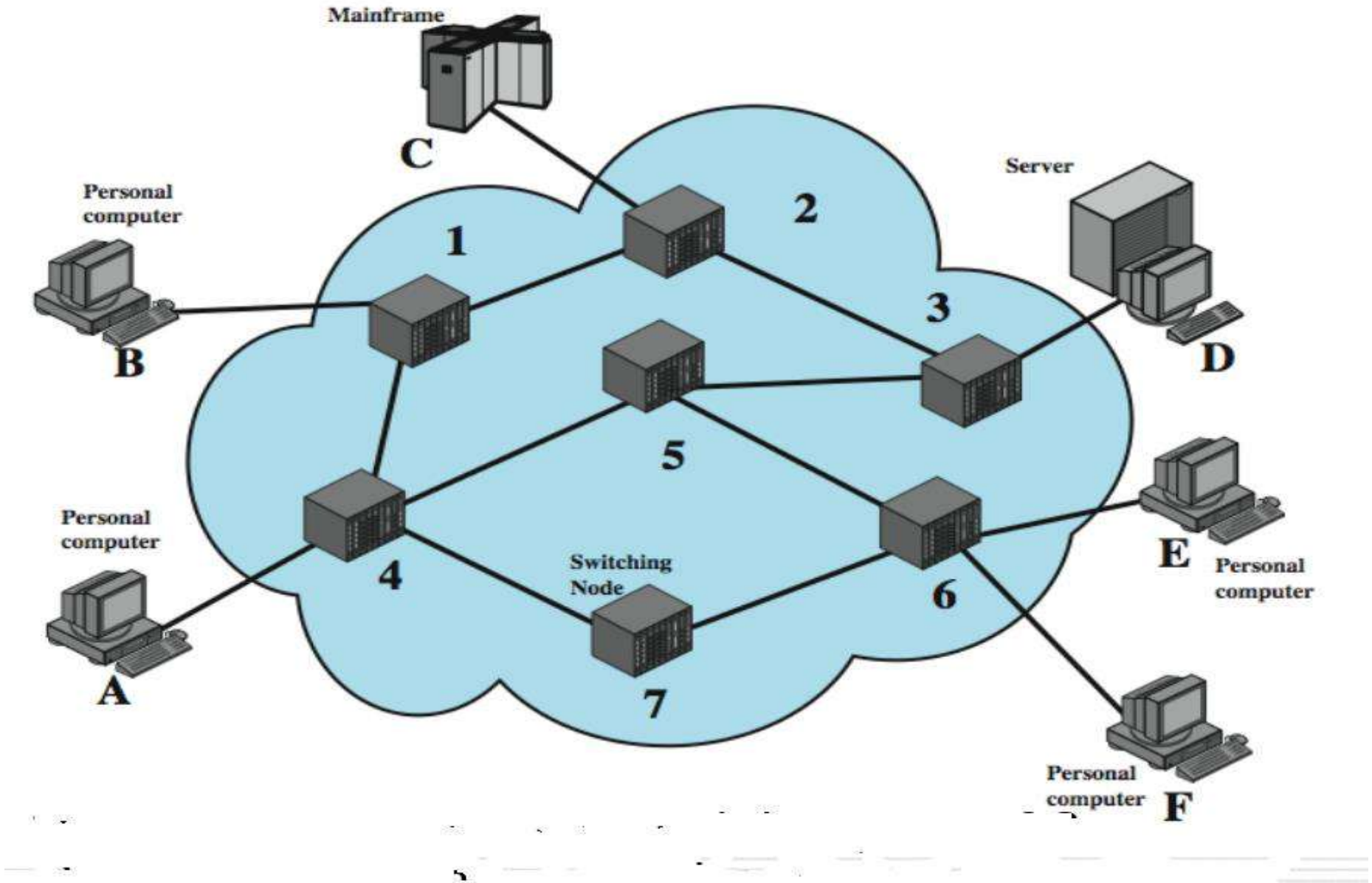
  Circuit disconnect



Point-to-point network



Switched network

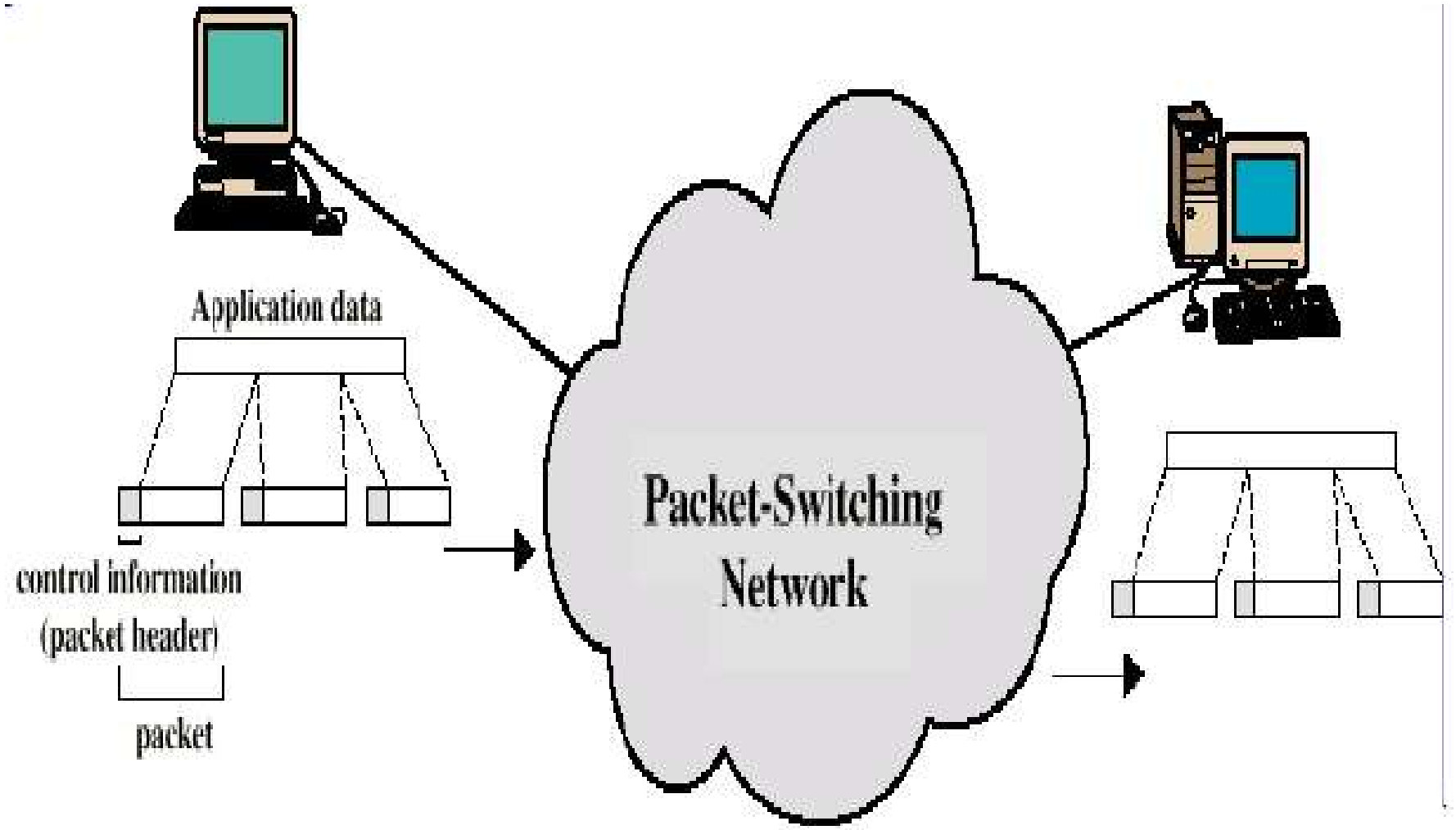

Mainframe
C
Server
Personal
computer
1
2
3
B
D
5
Personal
computer
4
Switching
Node
6
E
Personal
computer
A
7
Personal
computer
F

Message Switching

- **Uses a store – and forward communication method to transmit data from the sending to the receiving node.**
- **Stores it temporarily until a route towards the data's final destination becomes available.**

Message Switching

- **A station transmits data in small blocks, called packets.**
- **A packet length is 1000 bytes**


Application data
control information
(packet header)
packet
Packet-Switching
Network

WAN CARRIER TYPES

- **Point-to-point**
- **T-Carrier**
- **SONET**
- **ISDN**
- **Wireless**

Point – to- Point

- Communication through public dial-up lines and leased telephone lines
- To reduce noise and provide more reliable communication

T- Carrier

- Data communications to connect 2 different locations for continuous point-to-point communication

T-Carrier	Data Transmission Rate	T-1 Switched Channels	Data Signal Level
Fractional T1	64 Kbps	1 of 24 T-1 subchannels	DS-0
T-1	1.544 Mbps	1	DS-1
T-1C	3.152 Mbps	2	DS-1C
T-2	6.312 Mbps	4	DS-2
T-3	44.736 Mbps	28	DS-3
T-3C	89.472 Mbps	56	DS-3C
T-4	274.176 Mbps	168	DS-4
T-5	400.352 Mbps	336	DS-5

SONET (Synchronous Optical Network)

- **Defines the transaction rates, formats, architecture features, n/w operational criteria.**
- **It is multiplexed transport mechanism that does not involve any swithcing.**
- **SONET is its lack of interoperability.**
- **Transmitting data on optical fibres.**

STS – Synchronous Transport Signal level

OC - Optical carrier

STS – Synchronous Transport Signal level :

Higher level data rate like starting from 51.84 mbps

OC - (Optical carrier) is measure for the rate of transmission bandwidth for data being carried by Synchronous Optical Networking (SONET) fiber-optic networks.

STS Level	OC Level	Transmission Rate	T-3 Multiple
STS-1	OC-1	51.84 Mbps	1
STS-3	OC-3	155.52 Mbps	3
STS-9	OC-9	466.56 Mbps	9
STS-12	OC-12	622.08 Mbps	12
STS-18	OC-18	933.12 Mbps	18
STS-24	OC-24	1.244 Gbps	24
STS-36	OC-36	1.866 Gbps	36
STS-48	OC-48	2.488 Gbps	48
STS-192	OC-192	9.95 Gbps	192

ISDN

- **The Integrated Services Digital Network (ISDN).**
- **Developed by ITU-T**
- **It is a WAN technology for delivering voice, data, and video services over telephone lines**
- **It provides efficient multiplexed access to the public n/w**
- **To support integrated voice and data**
- **N/w management and internationally defined.**

Wireless

- **In Wireless technologies, the carrier is a signal released from an antenna or disk.**
- **The convenience of not being tethered to a telephone jack or other communication port.**
- **More security.**
- **Wireless technology refers to technology that allows us to communicate without using cables or wires. With wireless technologies, people and other entities can communicate over very long distances.**


INTERNET
Wireless iPaq
Wireless Laptop
Cable/DSL
Modem
Wired Desktop
Router/Wireless
Access Point
Wireless
Desktop
Wired Laptop
Wireless Print
Server
Wireless Networking

WAN TRANSMISSION EQUIPMENT

- **WAN transmission equipment either converts a signal for long – digital communication or creates multiple channels within a single communication medium for higher bandwidth**
- **Equipments :**

Multiplexers, Channel Banks,

Private Branch Exchange (PBXs)

Private Automatic Exchange (PAXs)

Modems, Access Servers, Routers

Multiplexers

Network devices that can receive multiple inputs and transmit them to a shared network medium.

Channel Banks

Convert multiple incoming voice signals into a single line

PBXs

Manually operated switchboards

PAXs

Includes the switchboards and a manual capacity as well as automatic switching

Carry voice, video, and data communications

Modems (Modulator/ Demodulator)

- **To converts a computer's outgoing digital signal to an analog signal that can be transmitted over telephone line.**
- **It also converts the incoming analog signal to a digital signal that the computer can understand.**

Router

Enables networks to be connected into WANs over long distance.

It can support multiple protocols.

Access server

- **It combines several types of WAN communication into one device.**
- **8 or 16 asynchronous ports and one or two**

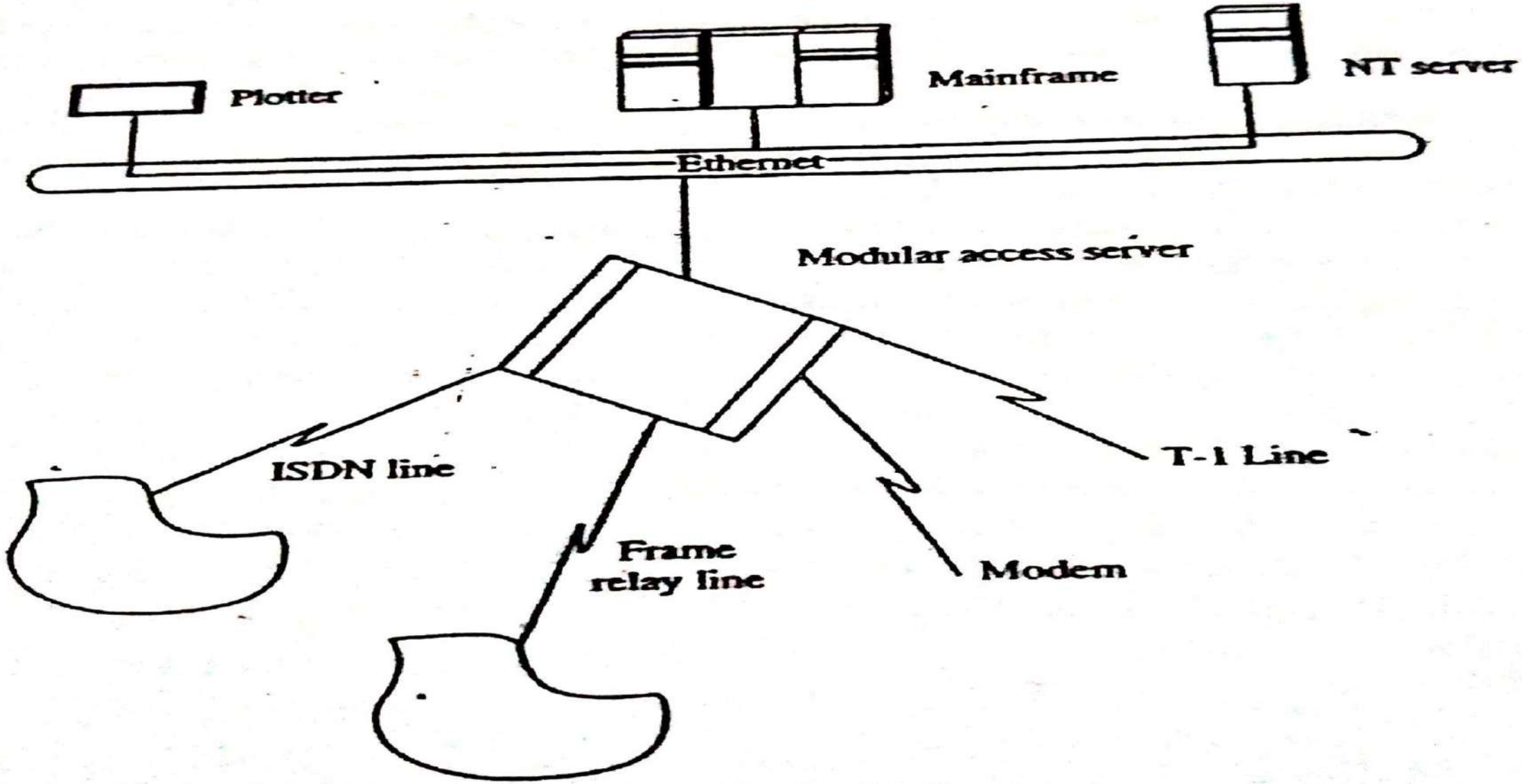


Figure 8.3 Using access server.

WAN DESIGN

- **Connecting LANs through a WAN for long distance voice, video, and Data transmission**
- **Services:**

  Match the WAN bandwidth

  Select a WAN service (multimedia applications)

  SLA (Service Level Agreement)

  Offer QoS

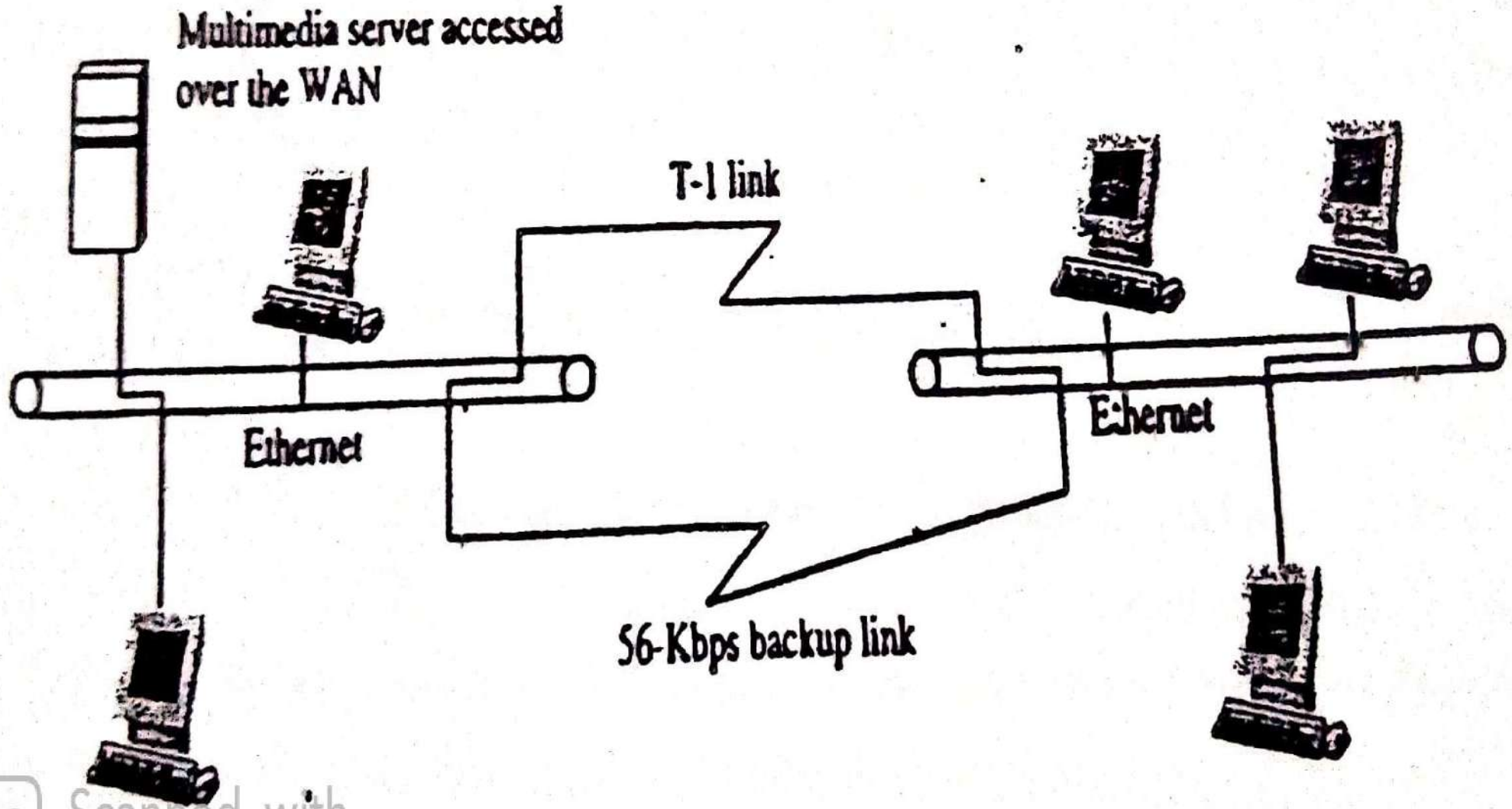


Figure 8.4 Using a backup line.

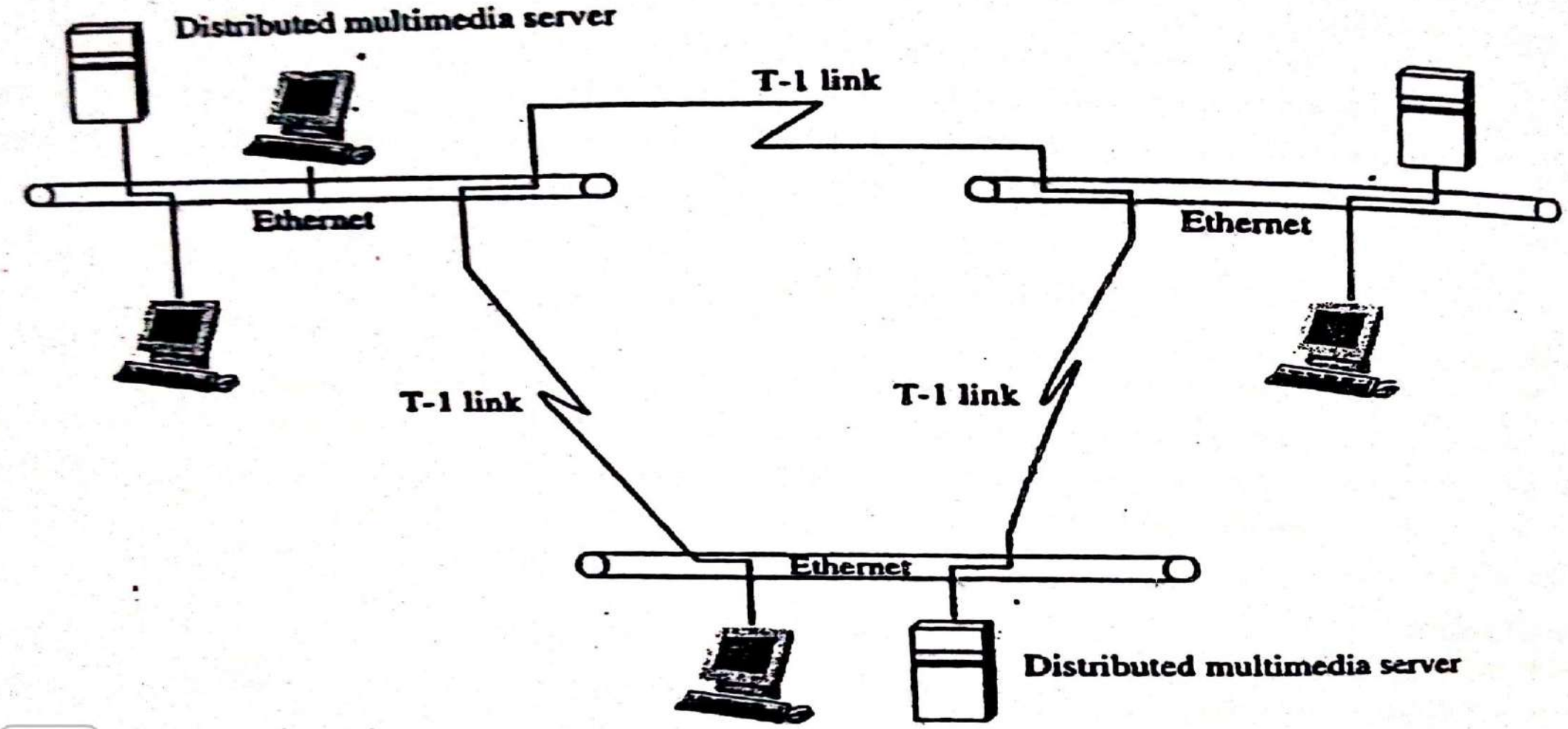


Figure 8.5 Distributed multimedia servers across WANs.

WAN Protocols

- **Designed to be used on WAN media**
- **Ability to capture the commonly used LAN protocols**
- **Protocols**

  X.25

  Serial line Internet protocol (SLIP)

  Point-to-Point protocols (PPP)

X.25

- **The oldest WAN protocols, uses packet switching**
- **Defines how data is sent from data terminal equipment (DTE), such as computers to data circuit, equipment (DCE), such as modem**

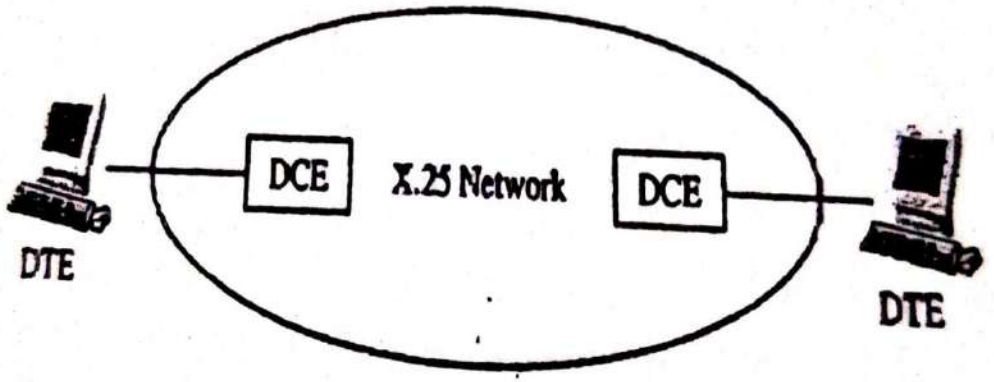


Figure 8.6 X.25.

- **X.25 standards transmission speed of up to 2.048 Mbps**
- **Offer**

  Global acceptance

  Reliability

  Connect older LANs to WANs

  Connect older mainframes and minicomputers to WAN

- **Transmit data packets using 3 nodes**

1. Switched Virtual Circuit

Established from node to node, only for the duration of the data transmission. Once the data transmission is completed, the channel can be made available to other node.

2. Permanent Virtual Circuits

Logical communication channel that remains connected to all times. The connecting remains in place even when data transmission stops.

3. Datagrams

- **Datagrams are packaged data sent without establishing a communication channel. They reach their destination using a form of message switching**
- **Not used on international networks,**

Serial Line Internet Protocol (SLIP)

- **Designed for UNIX environment for point-to-point communications between computers, servers.**
- **Do not support synchronous mode**

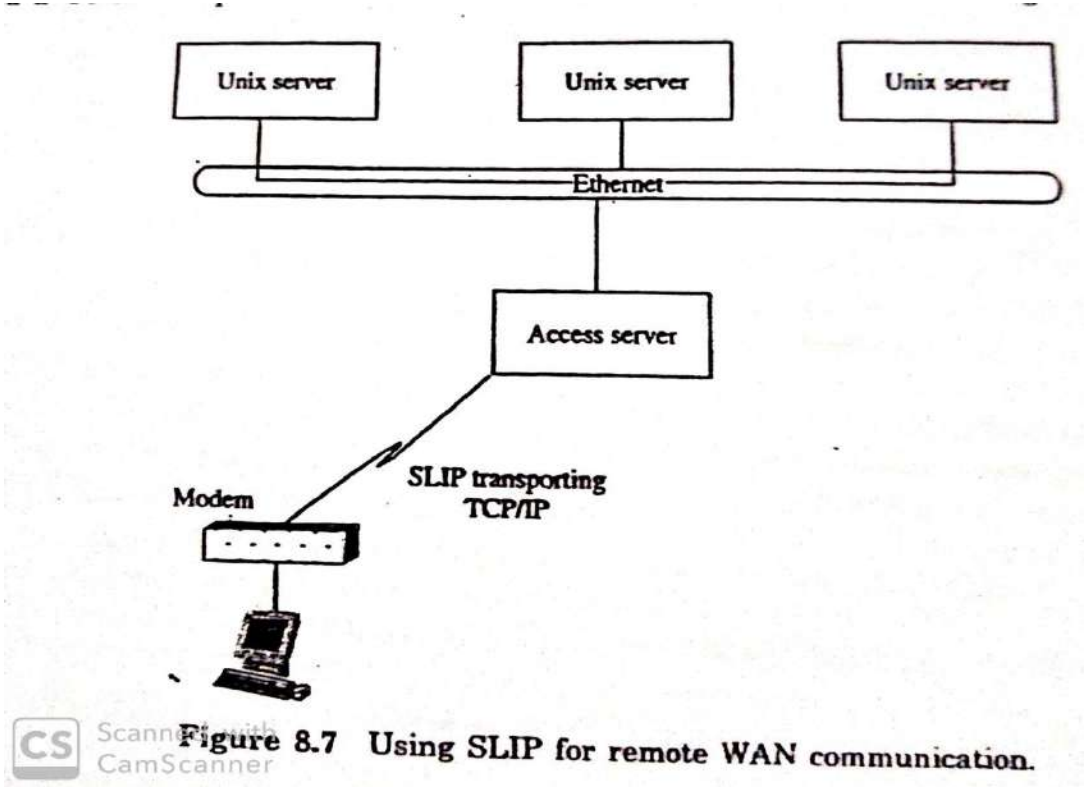


Figure 8.7 Using SLIP for remote WAN communication.

Point-to-Point Protocol (PPP)

- **Performs authentication, data compression, error detection and packet switching**
- **To carry the network layer data**

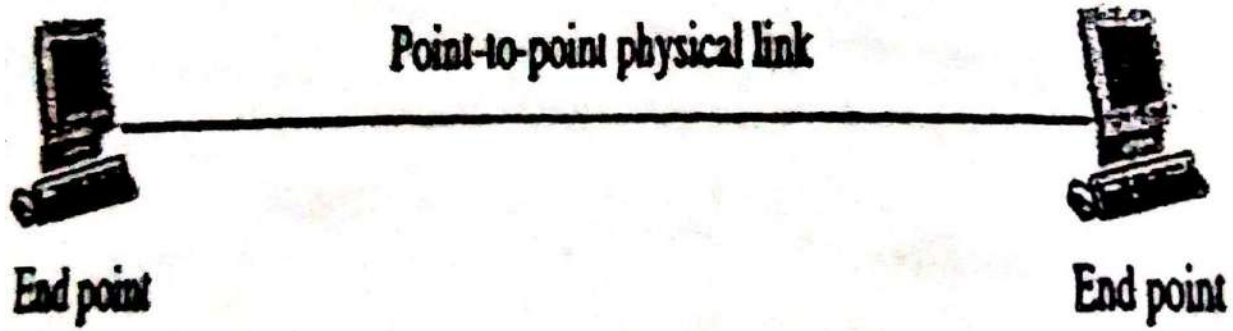


Figure 8.8 Point-to-point link.

Table 8.3 SLIP and PPP Compared

Feature	*SLIP*	*PPP*
Network protocol support	TCP/IP	TCP/IP, IPX/SPX and NetBEUI
Asynchronous communication support	Yes	Yes
Synchronous communication support	No	Yes
Simultaneous network configuration negotiation and automatic connection with multiple levels of the OSI model between the communication nodes	No	Yes
Support for connection authentication	No	Yes

- **PPP has largely replaced an older protocol called SLIP.**
- **PC should be connected to Internet Service Provider**

Steps

1. **The PC calls a router via modem**
2. **The PC and the router exchange Link Control Protocol (LCP) packets to negotiate PPP parameters**
3. **Check identities**
4. **Network Control Protocol (NCP) packets exchanged to configure the network layer,**

5. **Data transport**
6. **NCP user to turn down the n/w layer connection, LCP used to shout down data link connection**
7. **Modem hangs up.**

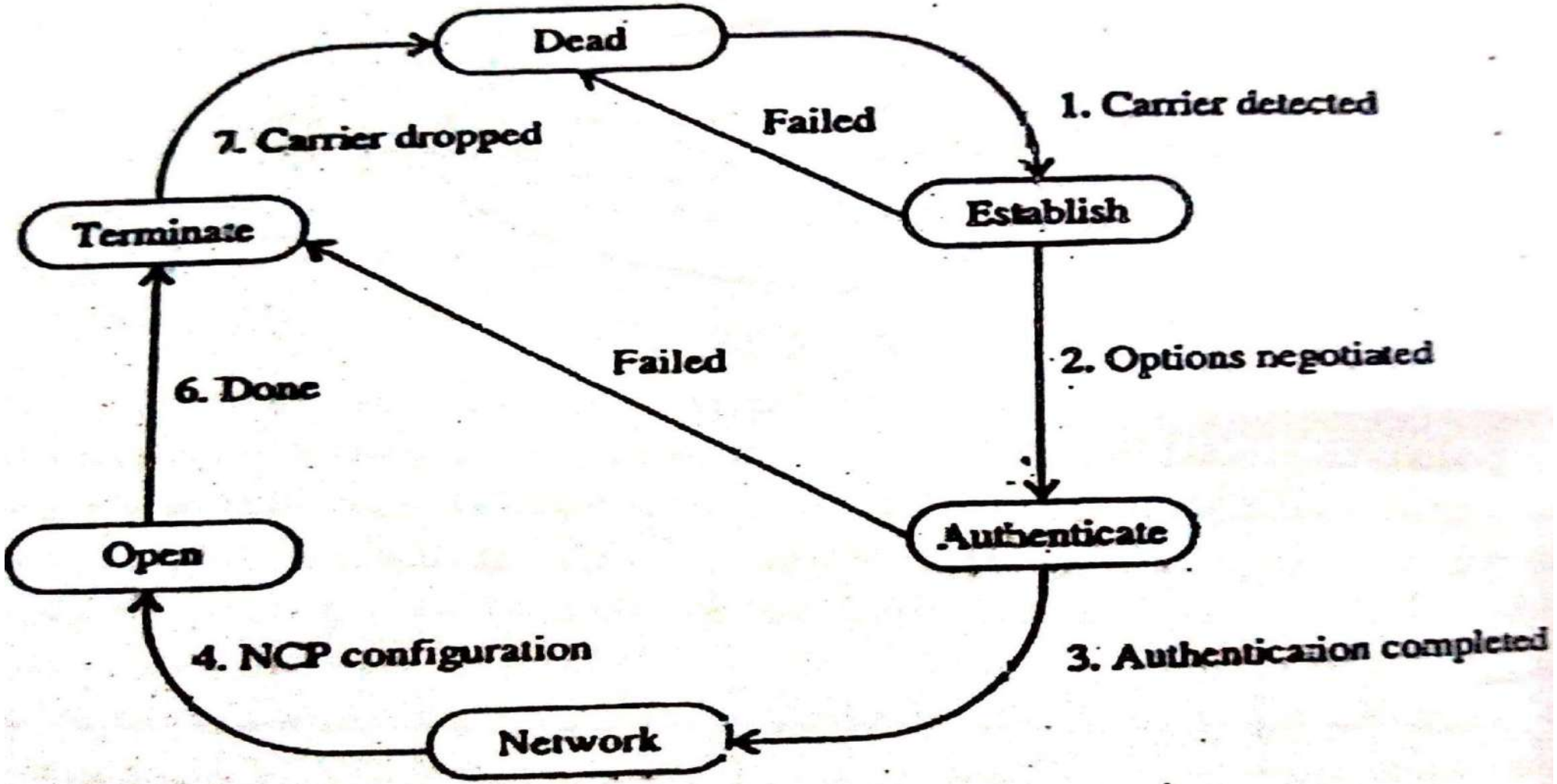


Figure 8.9 PPP phase diagram.

- **LCP is responsible to establishing, maintaining, configuring and terminating the line**
- **PPP is that is includes Password authentication protocols (PAP) and Challenge Handshake Authentication Protocol (CHAP)**

DATA LINK CONTROL AND PROTOCOL CONCEPT

- **Transfer of digital data over a link.**

Functions

To Establish and maintain Effective Communication.

- **Flow Control ->**

  Defines the way in which many frames sent and how the stations do error control.

- **Error Control ->**

  Defines *how a station check frames* for errors & What it does if it finds.

Flow Control

- **Flow control refers to a set of procedures used to restrict the amount of data the sender can send before waiting acknowledgement (ACK)**
- **Defines the way in which many frames sent and how the stations do error control.**

Receiving device has

- **Limited speed**
- **Limited amount of Memory**

So the sending device must not send frames at a rate faster than a receiving station can engage them.

Techniques

Stop and Wait flow control

Sliding window flow control

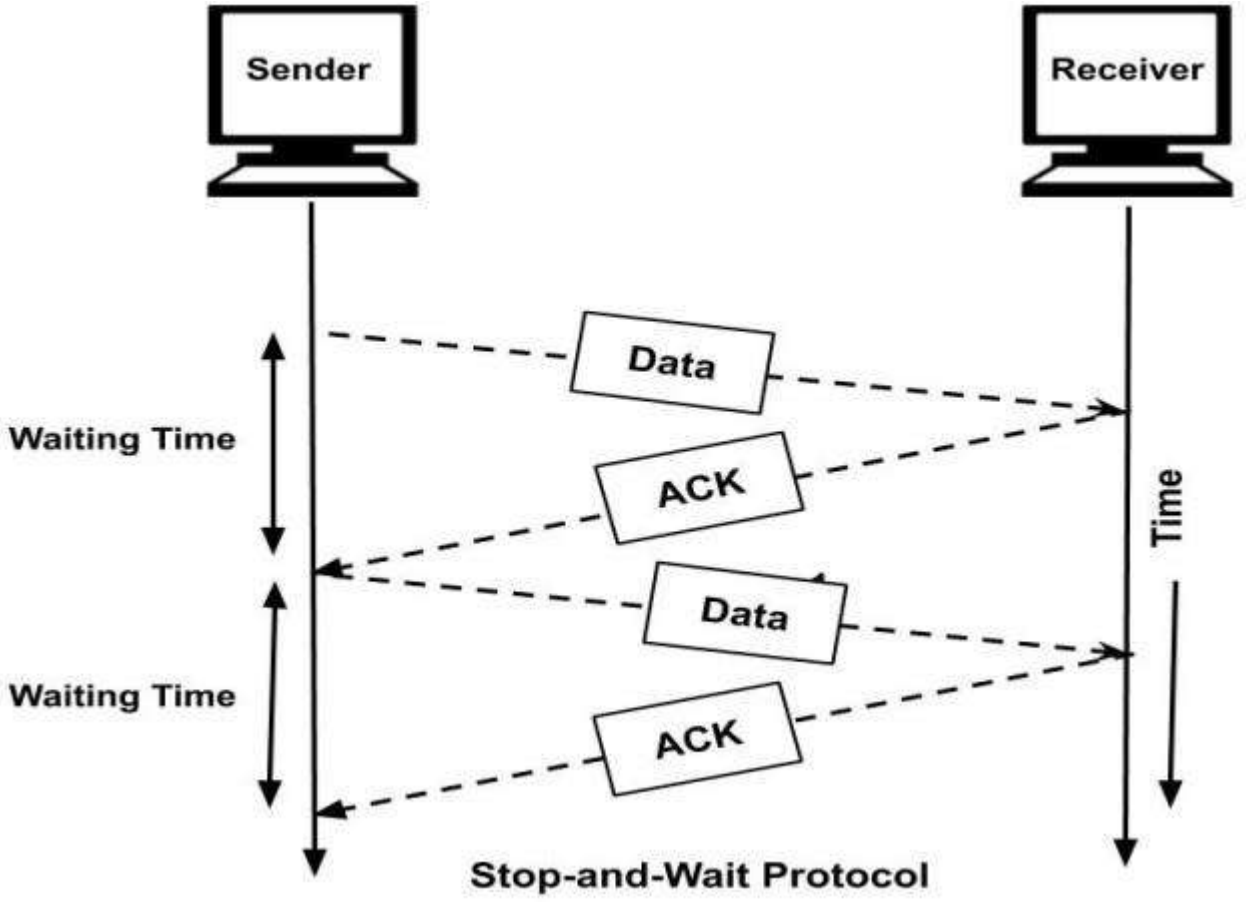
Stop and Wait flow control

Send one frame at a time

Destination receives frame and replies with acknowledgement

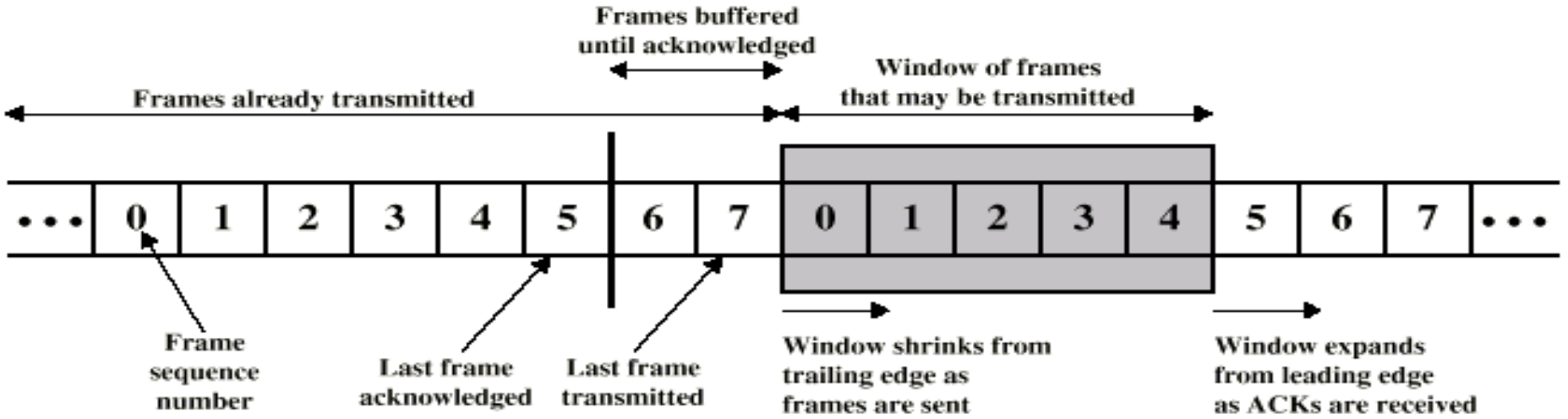
Source waits for ACK before sending next frame

Destination can stop flow by not sending ack.

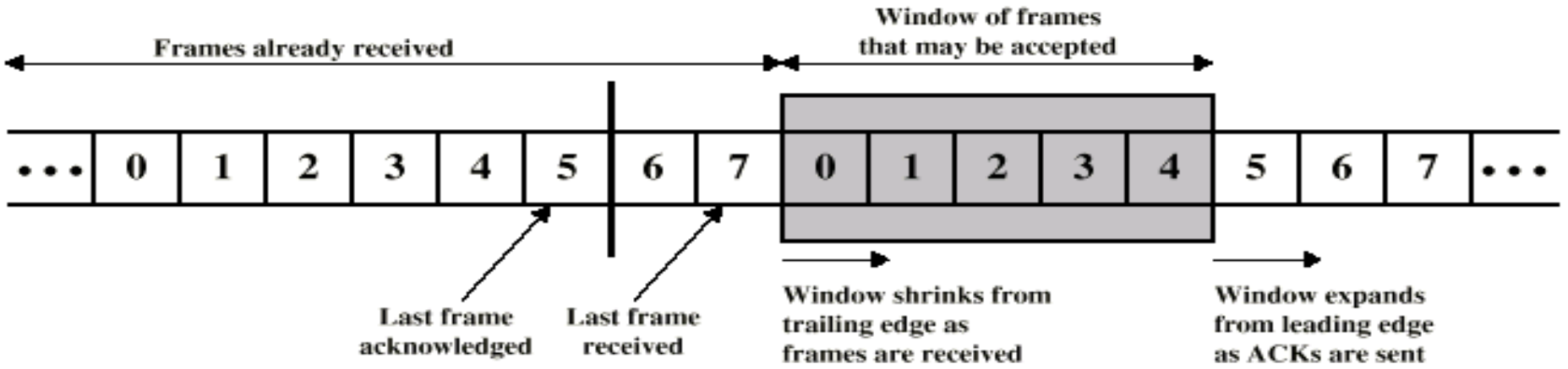


Sliding window flow control

- Allows multiple frames to be in transit
- Receiver sends acknowledgement with sequence number of anticipated frame
- Sender maintains list of sequence numbers it can send, receiver maintains list of sequence numbers it can receive



(a) Sender's perspective



(b) Receiver's perspective

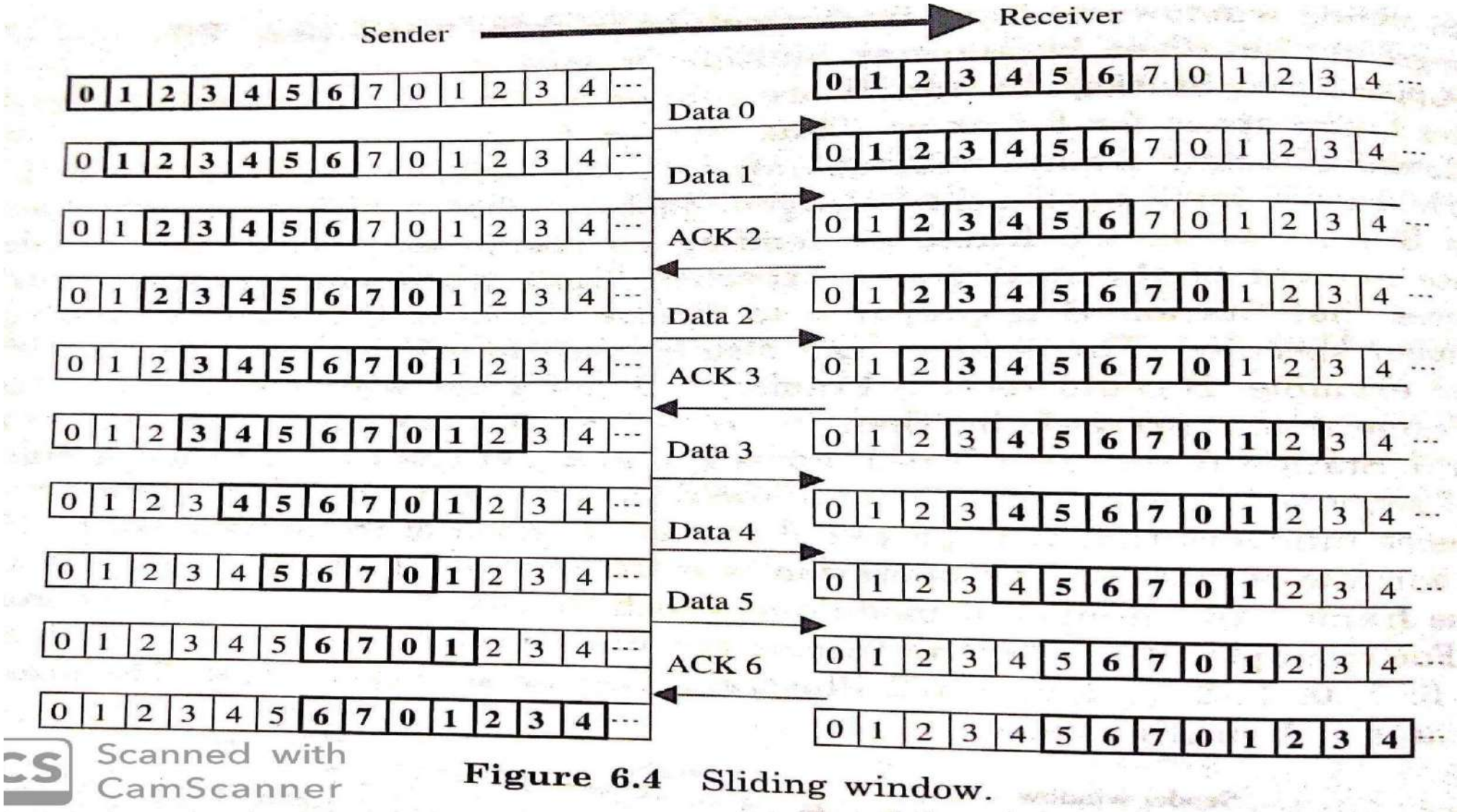


Figure 6.4 Sliding window.

Step 1:

- **When data 0 and data 1 are sent by the sender, sliding window of the sender shrank (minimized) from the left.**
- **The receiver received the data 0 and data 1 and then the sliding window of the receiver minimized from the left**

Step 2:

- **When acknowledgement is sent by the receiver for data 0 and data 1, the sliding window of the receiver is expanded to the right.**
- **The sender received the acknowledgement for data 0 and data 1 and then the sliding window of the sender extended form the right.**

Error Control

- **Error control in the data link layers is based on Automatic repeat request (ARQ)**
- **Retransmission of data in 3 cases:**

  Damaged frame

  Lost frame

  Lost acknowledgement

Damage Frame:

A recognizable frame does arrive, but some of the bits are in error (have been altered during transmission)

Lost Frame:

A frame fails to arrive at the other side.

Example : a noise burst may damage a frame to the extent that the receiver is not aware that a frame has been transmitted.

Lost acknowledgement:

- An acknowledgement fails to arrive at the source.
- The sender is not aware that acknowledgement has been transmitted from the receiver

Three versions of ARQ have been standardized

Stop – and – wait ARQ

Go-back-N ARQ

Selective-reject ARQ

Stop – and – wait ARQ

- **The sender transmit a single frame and then must await an ACK (acknowledgement)**
- **No other data frame can be sent until the receiver's reply (ACK) arrives at the source station**
- **The sender sends a single frame to the receiver.**
- **Chance that a frame that arrives at the destination (receiver) is damaged.**

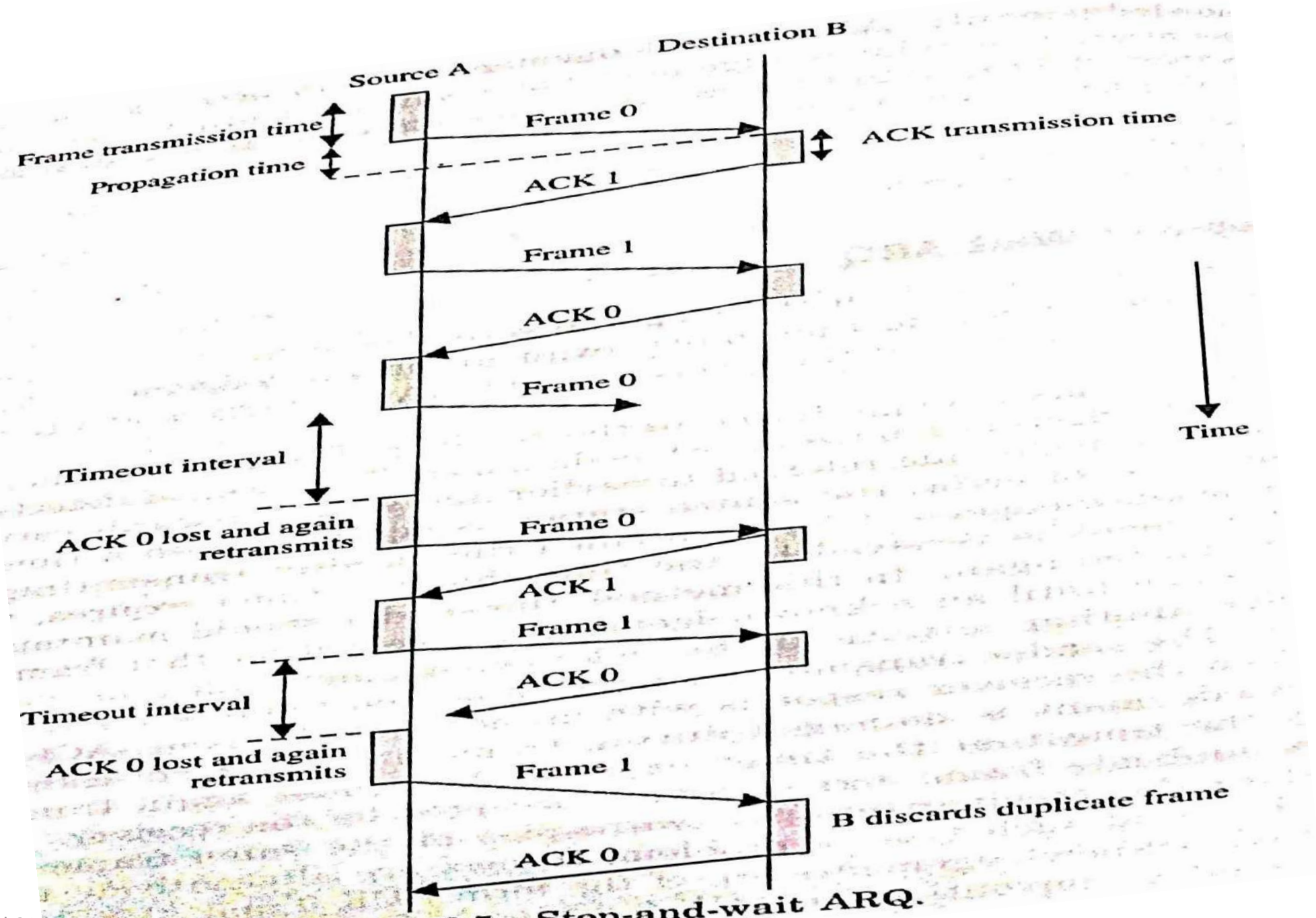


Figure 6.5 Stop-and-wait ARQ.

Go-Back-N ARQ

- **A station may send a series of frames sequentially numbered module.**
- **Consider that Station A is sending frames to Station B. After each transmission, Station A sets an acknowledgement timer for the frame just transmitted.**
- **Suppose that Station B has previously successfully received frame (i-1) and A has just transmitted Frame i.**
- **Go-back-N technique based on damaged frame, lost frame, lost ACK**

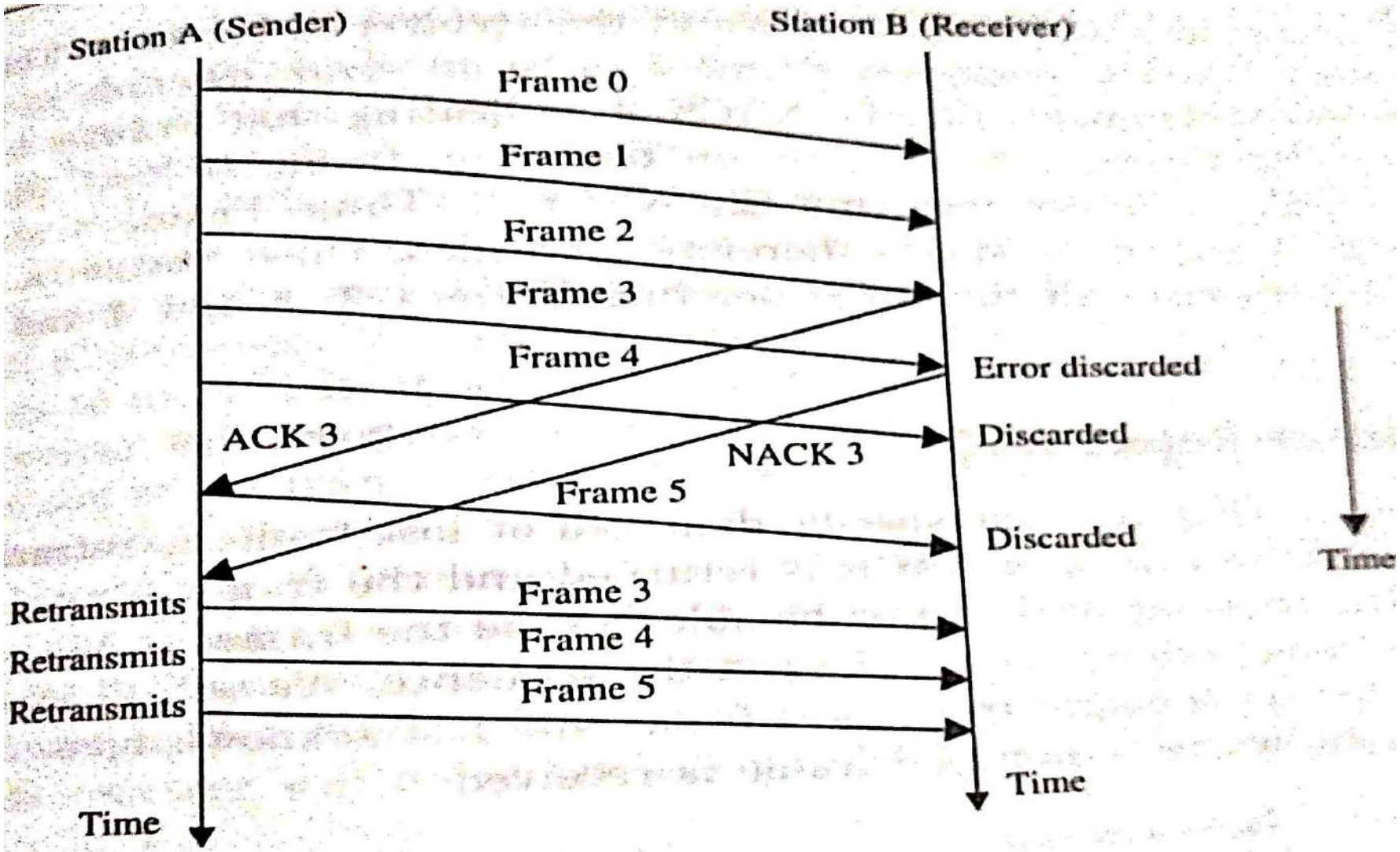


Figure 6.6 Damaged frame.

- **In another case, Station A transmits the Frame 0, 1 and 2 to Station B.**
- **Frames 0 and 1 arrives station B while frame 2 is lost.**

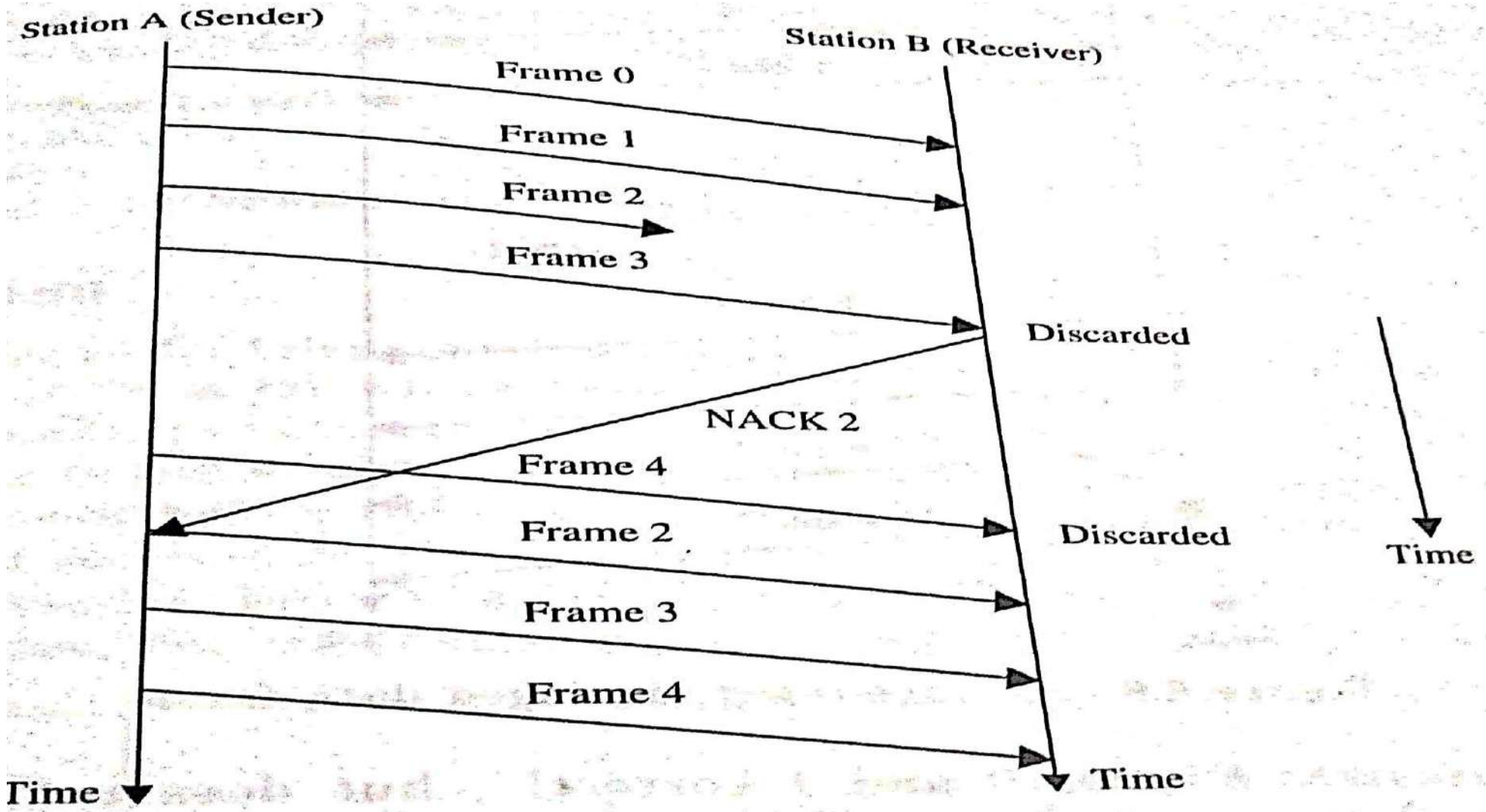


Figure 6.7 Lost frame.

Selective – Reject ARQ

- **In selective-reject ARQ, only the specific damaged or lost frame is retransmitted.**
- **If a frame is corrupted in transmit, a NACK is returned and the frame is retransmitted out of sequence.**
- **The receiving drive must be able to send the frames it has and insert the retransmitted frame into its proper place in the sequence.**

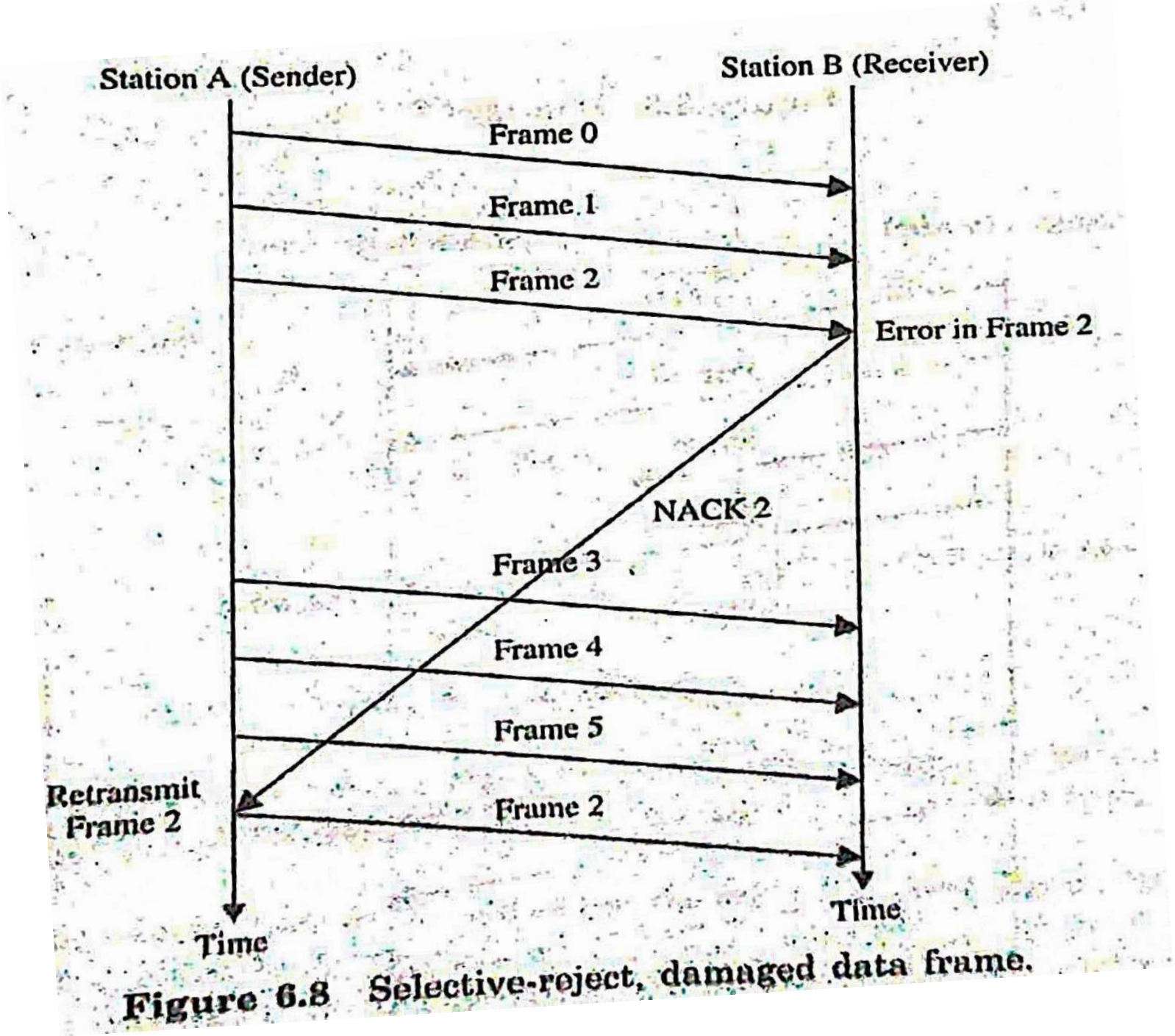


Figure 6.8 Selective-reject, damaged data frame.

ASYNCHRONOUS PROTOCOLS

- **Asynchronous protocols – used primarily in modems – feature start and stop bits and variable – length gaps between characters.**
  - **Protocols**
  - **X-Modem**
  - **Y-Modem**
  - **Z-Modem**
  - **Blocked asynchronous transmission (BLAST)**

X-Modem

- File transfer protocol for telephone –line communication between PCs,
- X-modem is a half –duplex stop-and-wait ARQ protocol
- Transmission begins with the sending of a NACK frame from the receiver to the sender.
- Each time the sender sends a frame, it must wait for an acknowledgement before the next frame can be sent.
- A frame can be resent either if response is not received by the sender after a specific time or if NACK is received by the sender

- **NACK or an ACK, the sender can receive a cancel signal, which aborts the transmission.**
- **The fixed data filed holds 128 bytes of data (binary, ASCII, test).**
- **The first field is one-byte start of header and the last field is CRC, which checks for error in the data field only.**
- **Header is sequence number.**

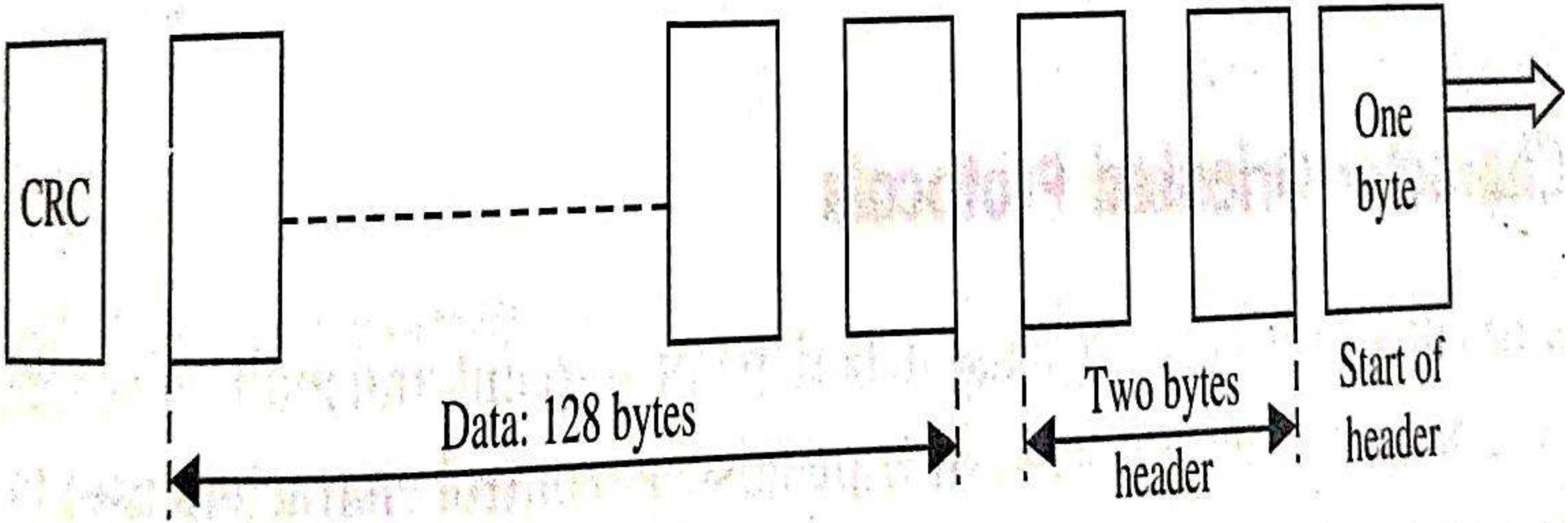


Figure 6.9 X-Modem frames.

Y – Modem

- **The data unit is 1024 bytes**
- **ITU-T CRC – 16 is used for error checking**
- **Multiple files can be sent simultaneously**

Z-Modem

- **Z-Modem is a protocol which combines features of both x-Modem and Y-Modems**

BLAST

- **BLAST is more powerful that X-Modem. It is full-duplex with sliding window flow control. It allows the transfer of data and binary files.**

SYNCHRONOUS PROTOCOLS

Two classes

- **Character-oriented protocols ()**
- **Bit-oriented protocols**

Character – oriented protocols

- **It also called as Byte oriented protocols (8bits)**
- **Transmission of frame or packet as a succession of characters**
- **Use both point-to-point and multipoint applications**
- **Perform various transmission control functions like**

  Management, flow control, error control, data transparency
- **Character sets such as ASCII or EBDIC**

Fig : Control frame for BSC (Binary Synchronous Communication protocol

Table 6.1 Control Characters for BSC

BSC character	*ASCII code*	*Function*
ACK 0	DLE and 0	Good even frame received or ready to receive.
ACK 1	DLE and 1	Good odd frame received.
DLE (Data link escape)	DLE	Data transparency marker.
ENQ (Enquiry)	ENQ	Request for response from another station. Responding stations might send a data frame or an ACK or NAK, depending on their status.

EOT (End of transmission)	EOT	Indicates the end of transmission and tells the stations they may disconnect.
ETB (End of transmission block)	ETB	Indicates the end of an intermediate frame, that is, end of transmission block; ACK required.

ETX (End of text)	ETX	Indicates the end of the last frame in a multiframe message or end of the text in a message.
NAK (Negative acknowledgement)	NAK	Indicates the previous frame was received incorrectly.
NUL (Null)	NULL	Used as a filler character where frames must be a minimum length.

BSC character	*ASCII code*	*Function*
SOH (Start of header)	SOH	Indicates the start of header information in the frame.
STX (Start of text)	STX	Indicates the start of data within the frame.
SYN (Synchronous idle)	SYN	Alerts the station of an arriving frame

- **BSC uses stop-and-wait ARQ: acknowledgement must be either ACK 0 or ACK 1 to specify alternating data frames**
- **SOH tells the receiving station that successive bytes in the arriving frame contain header information.**
- **Header information contains the address of the sending and receiving station.**
- **The header information is followed by an STX character or a DLE-STX combination to be followed.**

SYN	SYN	SOH	Header	STX	…Data…	ETX	BCC

Fig 6.11 (a) Non-transparent data

- **STX indicates the start of text, successive bytes represent data.**
- **Receiving station receives and accepts the bytes as data until it encounters ETX**
- **Block check count (BCC) are included for error detection.**
- **BCC can be one-character longitudinal redundancy check (LRC) or a two –character cyclic redundancy check (CRC)**

SYN	SYN	SOH	Header	DLE	STX	...Data...	DLE	ETX	BCC

Fig 6.11 (b) Transparent data

- **DLE acts like a toggle switch.**
- **Receiving station sees the DLE – STX pair, it disables any checking for control bytes such as ETX or ETB.**
- **The checking remains disabled until the receiving station encounters another DLE character.**
- **Once this DLE is encountered, the receiving station enables its checking for ETX or STX characters.**

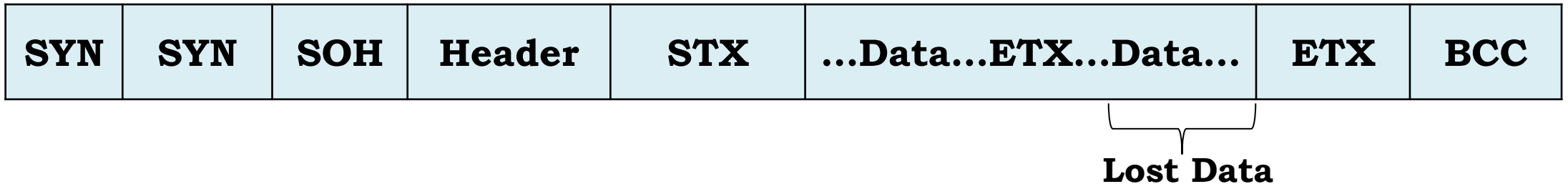


Fig 6.12 Encountering control bytes in data

- **For application in which the data consists of printable character codes, this is a simple way to indicate its end.**

Byte Stuffing

- **A sending station examine the characters it sends as data.**
- **Whenever there is a DLE character, it inserts an extra DLE character.**
- **This process is called byte stuffing**

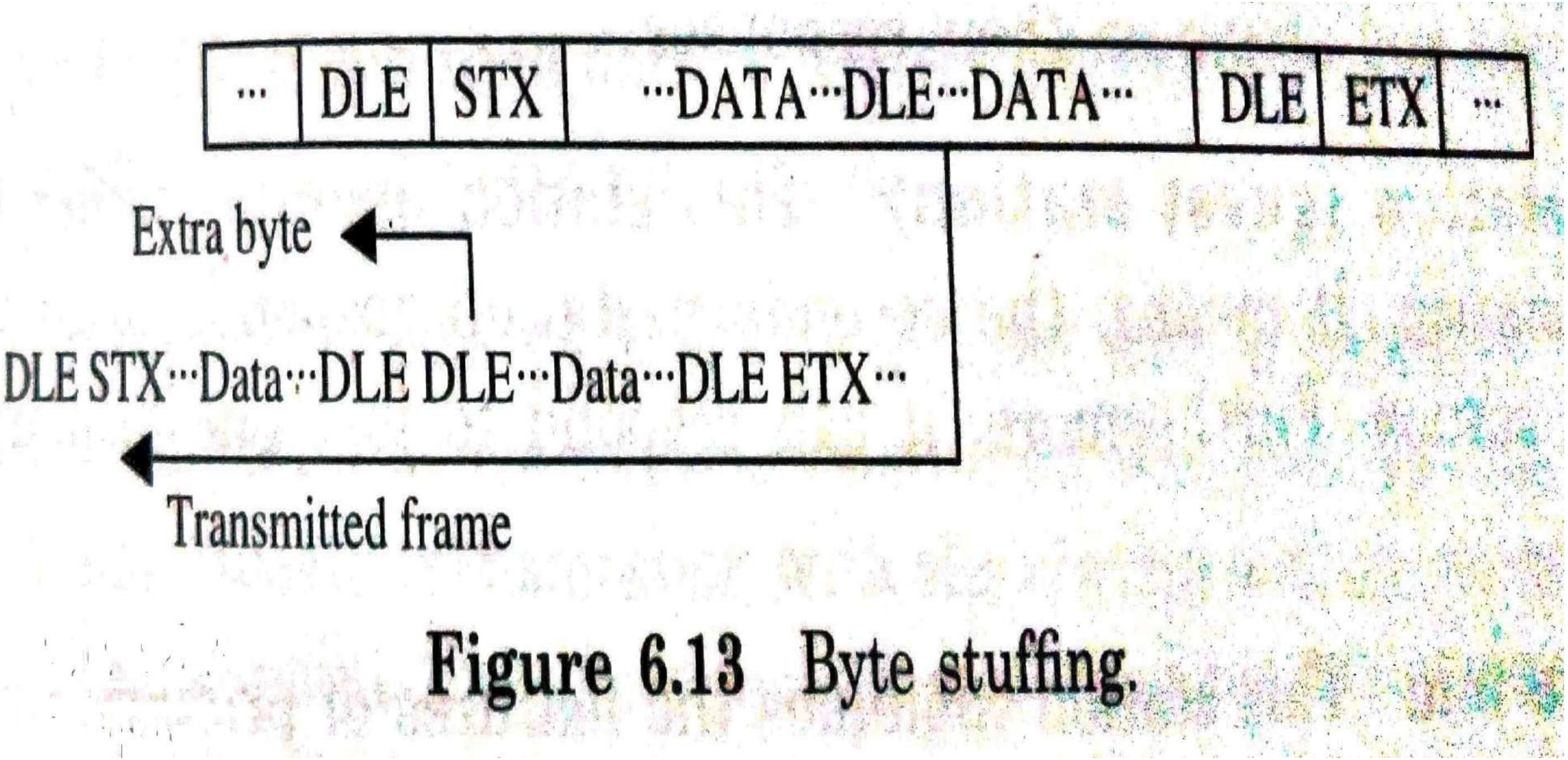


Figure 6.13 Byte stuffing.

Bit-Oriented Protocols

- **Bit – oriented protocols can pack more information into shorter frames and avoid the transparency problems.**
- **Protocols**

  Synchronous Data Link Control (SDLC)

  High-level Data Link Control (HDLC)

  Link access procedures, balanced (LAPB)

  Link access procedures, D-channel (LAPD)

  Link access procedures, modem (LAPM)

High-level Data Link Control (HDLC)

- **To support both half-duplex and full-duplex communication**
- **Types**

  Primary station (control station) ---PS

  Secondary station (guest station) ---SS

  Combined station (CS)

  Unbalanced configuration (1 - PS, 1 or more SS)

  Balanced configuration (2 – CS)

Statin types

Primary station (control station) ---PS

Secondary station (guest station) ---SS

Combined station (CS)

Configuration

Unbalanced configuration (1 - PS, 1 or more SS)

Balanced configuration (2 – CS)

Mode:

Normal response mode (NRM)

Asynchronous response mode (ARM)

Asynchronous balanced mode (ABM)

Link access procedures balanced (LAPB)

Connecting a station to a network

Link access procedures, D-channel (LAPD)

Integrated Services – Digital Network (ISDN)

Link access procedures, modem (LAPM)

Designed to asynchronous to synchronous conversion, error detection and transmission.

LOCAL AREA NETWORKS

- ✓ Types of Networks and Topology
- ✓ LAN Transmission Equipment
- ✓ Ethernet: IEEE Standard 802.3
- ✓ Token Bus : IEEE Standard 802.4
- ✓ Token Ring : IEEE Standard 802.5
- ✓ Fibre Distributed Data Interface (FDDI)
- ✓ Distributed Queue Dual Bus (DQDB) : IEEE standard 802.6
- ✓ LAN Installation and Performance
- ✓ LAN operating Systems and Protocols
- ✓ Ethernet Technologies

LOCAL AREA NETWORKS

- **Used to interconnect distributed communities of computers.**

  Centralized server farms (Google)

  Power workgroup (Whatsapp group, yahoo group,etc.,)

  High-speed local backbone

Types Networks and Topology

- **Networks requires cabling, network equipment, file servers, workstation, software and training.**
- **Three types of networks**
- **Five different types of topologies**
- **When a new LAN is installed, there are several factors that affect its design, including following**

  Network traffic, Redundancy, User Movement, Future growth

  Security, Connectivity.

LAN TRNSMISSION EQUIPMENT

- **Used to connect devices on a single network, to create and connect multiple n/w.**
- **Equipment's are:**
  - **Network Interface Card (NIC)**
  - **Repeaters**
  - **Bridges**
  - **Routers**
  - **Brouters**
  - **Switches**
  - **Gateways**

Network Interface Card (NIC)

Used to enable a network device.

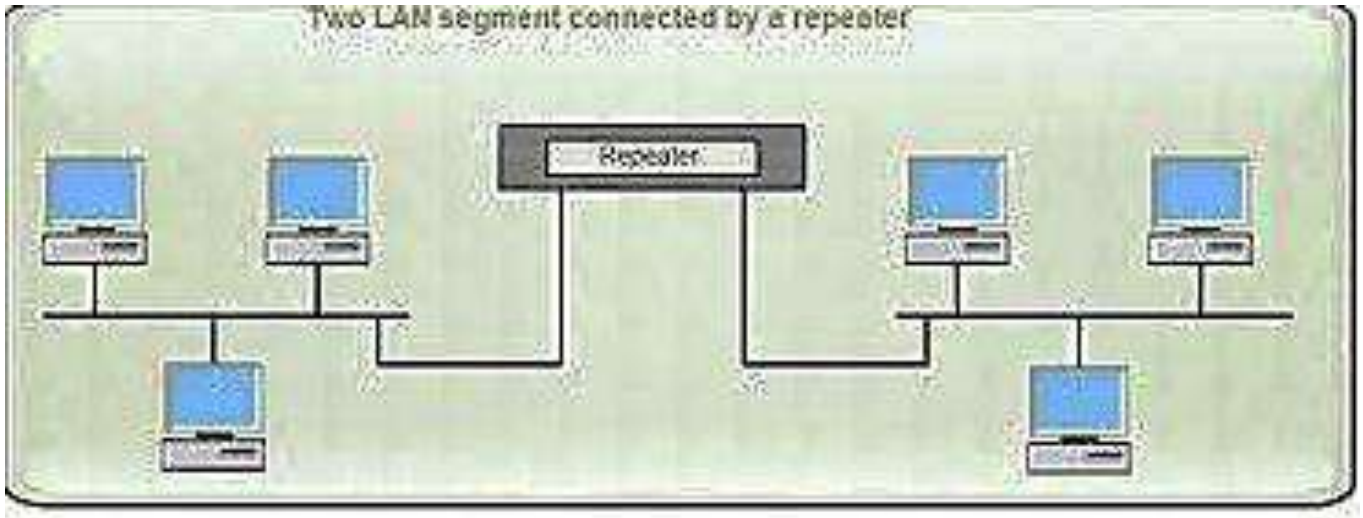
Designed to match particular n/w transport methods.

Four components

- **An appropriate connector**
- **A transceiver**
- **A controller**
- **Protocol**

Repeater:

- **A repeater is an electronic device that operates on only the physical layer.**
- **Connects two or more cable segments and retransmits any incoming signal to all other segments.**
- **Repeater travel 1000 meters.**



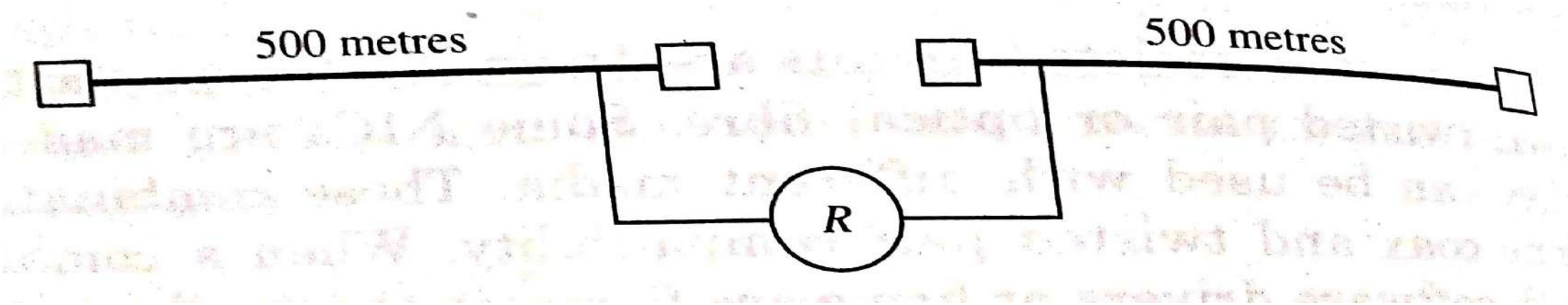


Figure :
A repeater connecting two Ethernets. The repeater connects directly to the cable; it does not use a transceiver

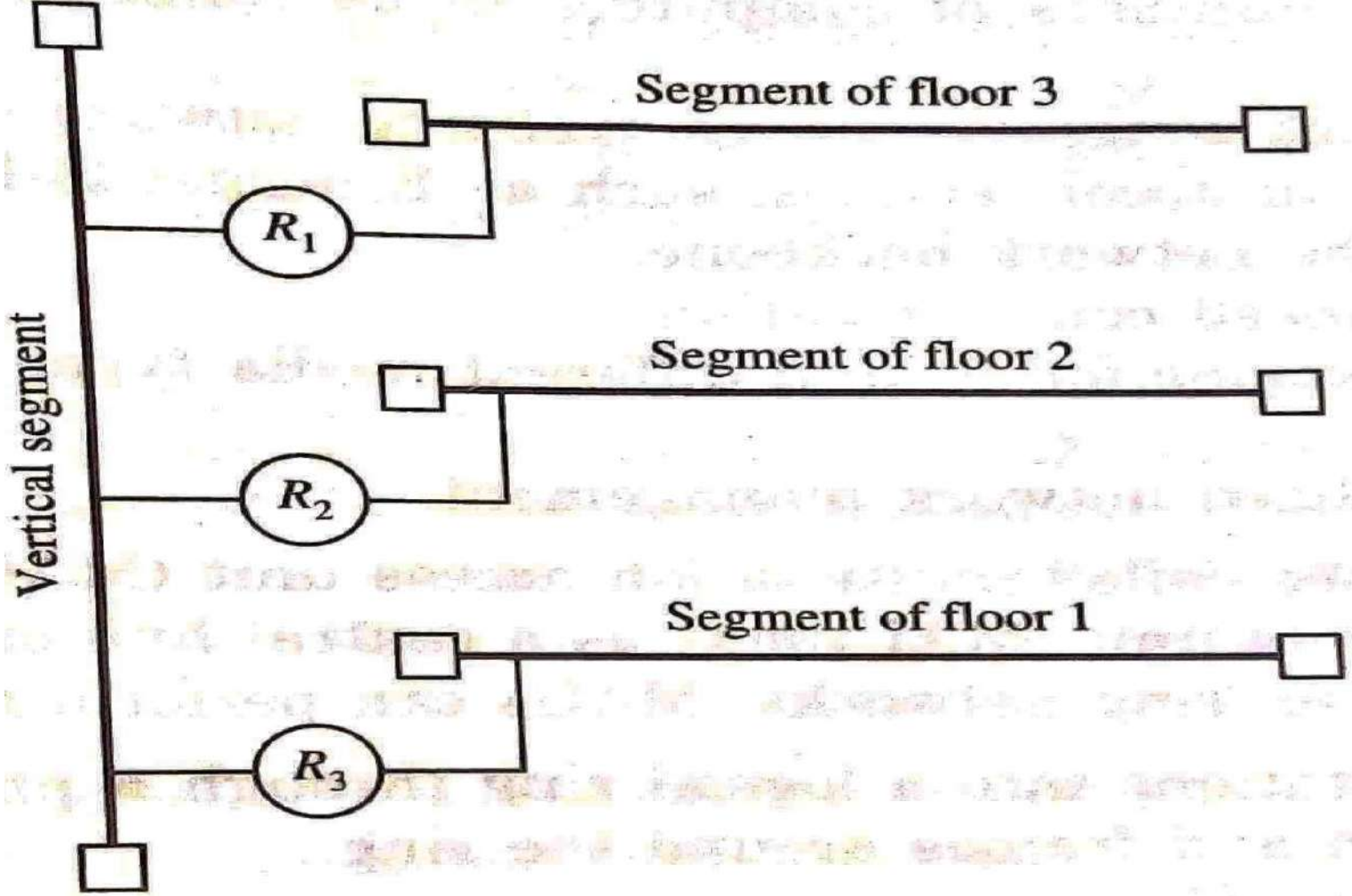


Figure 7.2 Repeaters are used to connect Ethernet segments on three floors of an office building. Each floor has one segment, and one segment is placed vertically in the building

Hub

- **A hub is a central network device that connects network nodes, such as workstations and servers in a star topology.**
- **To as a connector, multiple inputs and outputs, all active at one time.**

Hubs can:

Provide a central unit

Permit large no.of computers

Reduce n/w congestion

Enable high speed communication

Support different media types

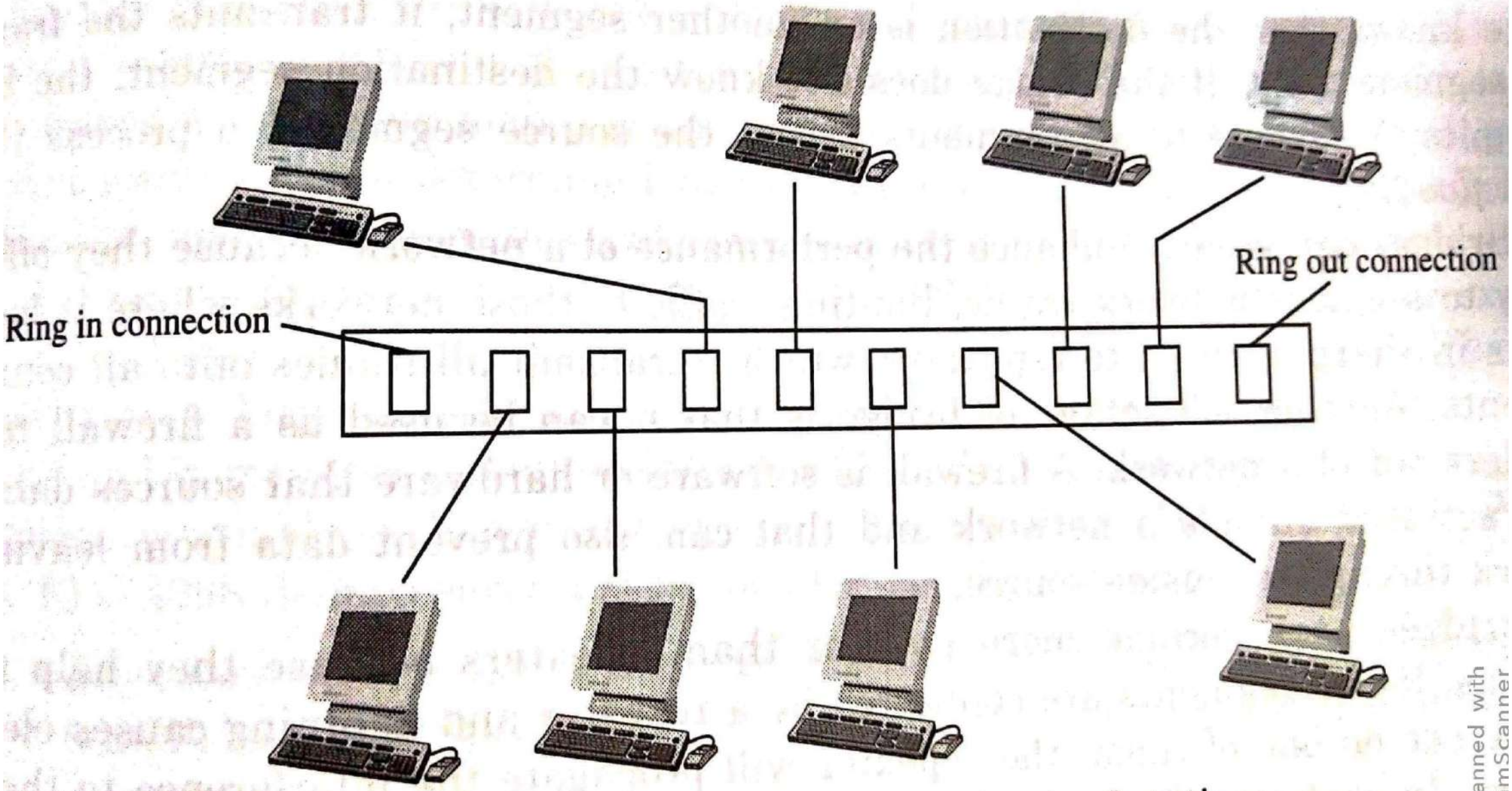


Figure 7.3 MAU connecting token ring workstations.

Bridge

Connects one LAN segment to another

Perform error detection, frame formatting, and frame routing

Used

- **Extend a LAN when the maximum connection limit**
- **Extend a LAN beyond the length limit**
- **Reduce data traffic**
- **Prevent unauthorized access to a LAN**

Router:

- **Performs some of the same functions as a bridge, such as learning, filtering and forwarding**
- **Used for:**

  Efficiently direct packets from one n/w to another

  Join neighboring or distant n/w

  Connect dissimilar n/w

  Prevent n/w

  Secure portion of a n/q from intruders

  Border Gateway Protocol (BGP)

BGP speaking routers:

- Edge router
- Subscriber edge router
- Inter-provider Border Router
- Core Router

Routing protocols

- BGP (Border Gateway protocol)
- EGP (Exterior Gateway protocol)
- OSPF (Open shortest path first)
- RIP (Routing Information Protocol)

Brouter

- **A bridge router (brouter) performs both the functions of bridge and a router**
- **A brouter is a network device that acts as a bridge in one circumstance and as a router in another.**
- **Used**

  Handle packets defiantly on a multiprotocol

  Isolate and direct network traffic to reduce congesstion.

  Join networks

  Secure a certain portion

Switches

- **A Switch is a device that connect two or more n/w segments**
- **Allows different nodes to communicate smoothly with each other as if they are the only two connecting at the time.**
- **Unlike a hub, which rebroadcasts from all ports to all devices on a network.**
- **Makes a direct connection between the transmitting device and the receiving device.**
- **Providing bridging capacity**
- **Examine device addresses of all incoming traffic.**

- **The switch normally has a buffer for each link to which it is connected.**
- **Strategies:**

  Store-and-forward switch

  Cut-Through switch

Gateways:

- **If two n/w operate according to different n/w protocols, a gateway is used to connect them.**
- **Translate the protocols to allow terminals on two dissimilar n/w to communicate.**
- **Workstations to an outside n/w web server is a gateway.**

Use a gateway to:

- **Convert commonly used protocol**
- **Convert message formats**
- **Translate different addressing schemes.**
- **Link a host computer to a LAN**
- **Provide terminal simulation for connections**
- **Direct e-mail to the right n/w destination**
- **Connect n/w with different architecture**

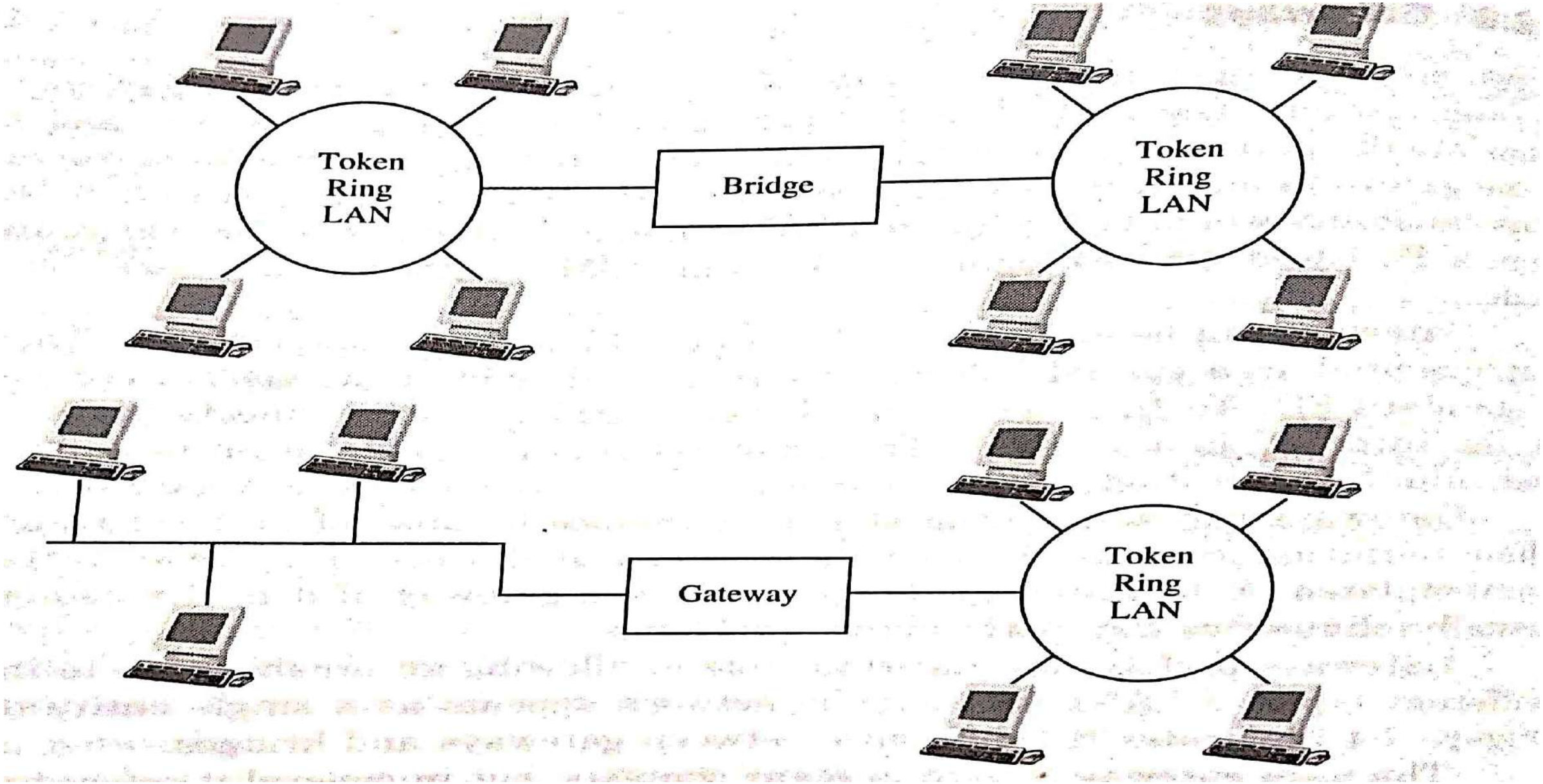

Token
Ring
LAN
Bridge
Token
Ring
LAN
Gateway
Token
Ring
LAN

Table 7.1 A Comparison of Network Hardware

Network hardware	*OSI layer*	*Relative throughput*	*Complexity*	*Capability*
Repeater	Physical layer	Lowest	Simplest	Regenerates signals between two segments
Bridge	Data link layer	Moderate	Simple	Connect two network segments
Switch	Data link layer or network layer	Fastest	Complex	Connects two nodes on separate segments

Router	Network layer	Fast	Most complex	Connects two dissimilar networks, routing data
Brouter	Data link layer/ network layer	Fast	Medium complexity	Fulfills functions of both switches and routers
Gateway	Transport layer	Fast, but can be slowed down by protocol translation	Medium complexity	Connects two types of networks with different protocols.

Ethernet : IEEE standards 802.3

- **Used to connect PCs, workstations, pointers and file servers.**
- **This involves frame formats, error checking and flow control.**
- **Data link layer two sub layers**

  Logical Link Control (LLC),

  Medium Access Control (MAC)
- **LLC handles logical link between the stations**
- **MAC controls access to the transmission medium.**
- **IEEE 802.2 standard is an LLC, IEEE 802.3 is an MAC protocol.**

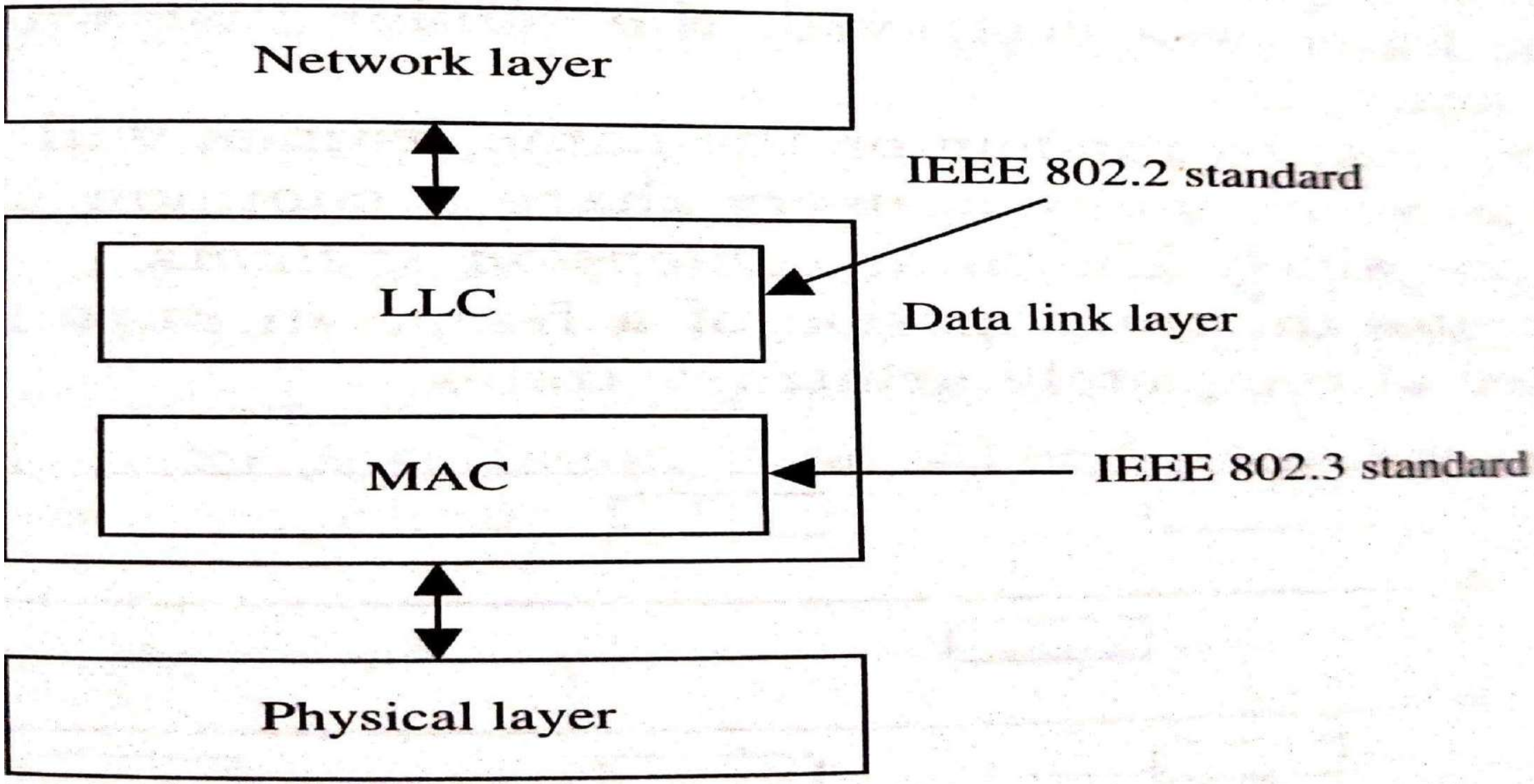


Figure 7.5 Data link layer refinement.

Medium Access sub-layer

Two categories : point-to-point n/w and broadcast n/w

Algorithms :

- **Pure Aloha**
- **Slotted Aloha**
- **Carrier Sense Multiple Access (CSMA)**
- **CSMA with Collision Detection**

Pure Aloha

- **Users transmit whenever they have data to be sent.**
- **There will be collision, of course, and collision frames will be destroyed.**
- **If the frame was destroyed, the sender just waits a random amount of time and sends it again**
- **The waiting time must be random or the same frames will collide over and over, in lockstep.**

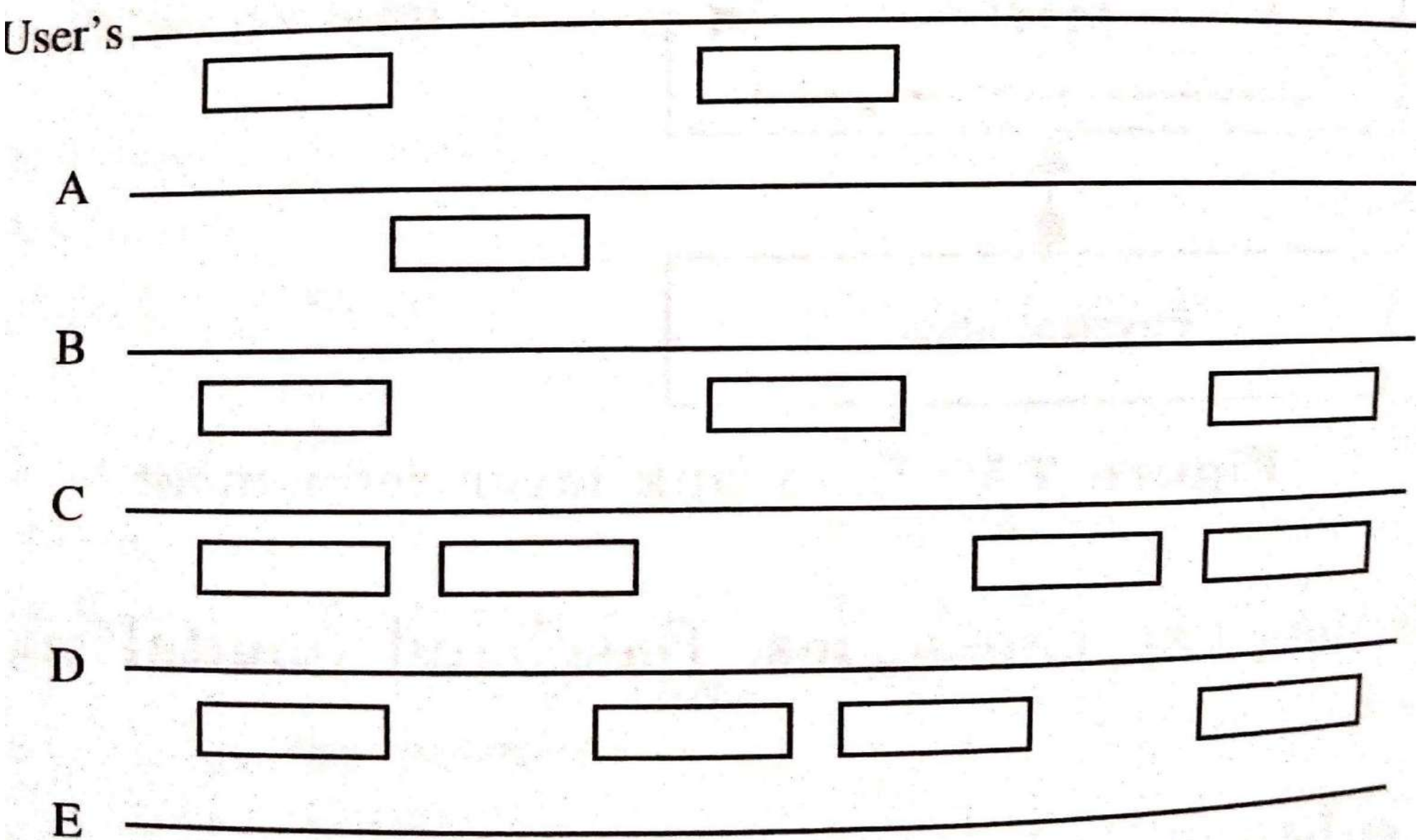
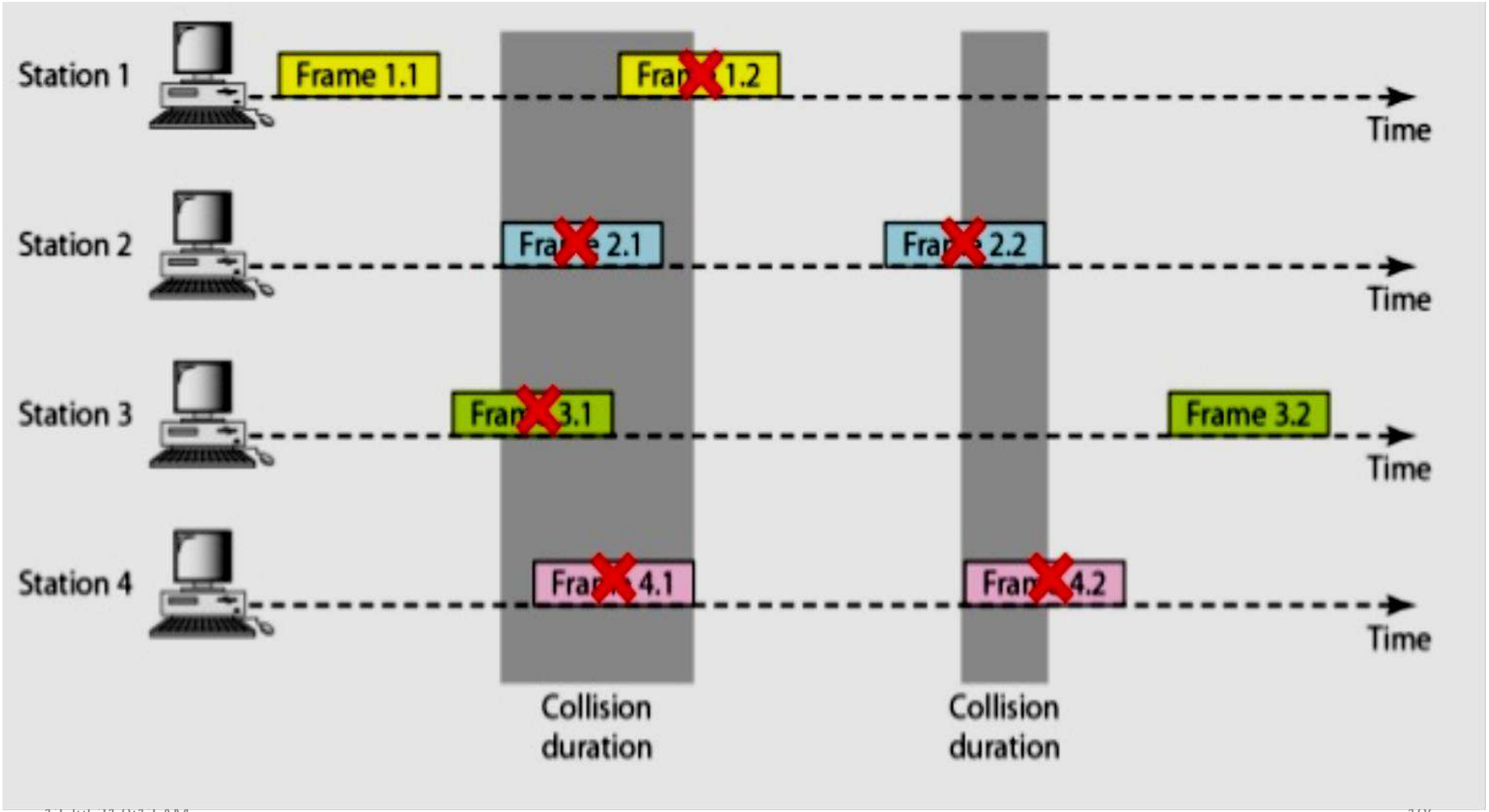
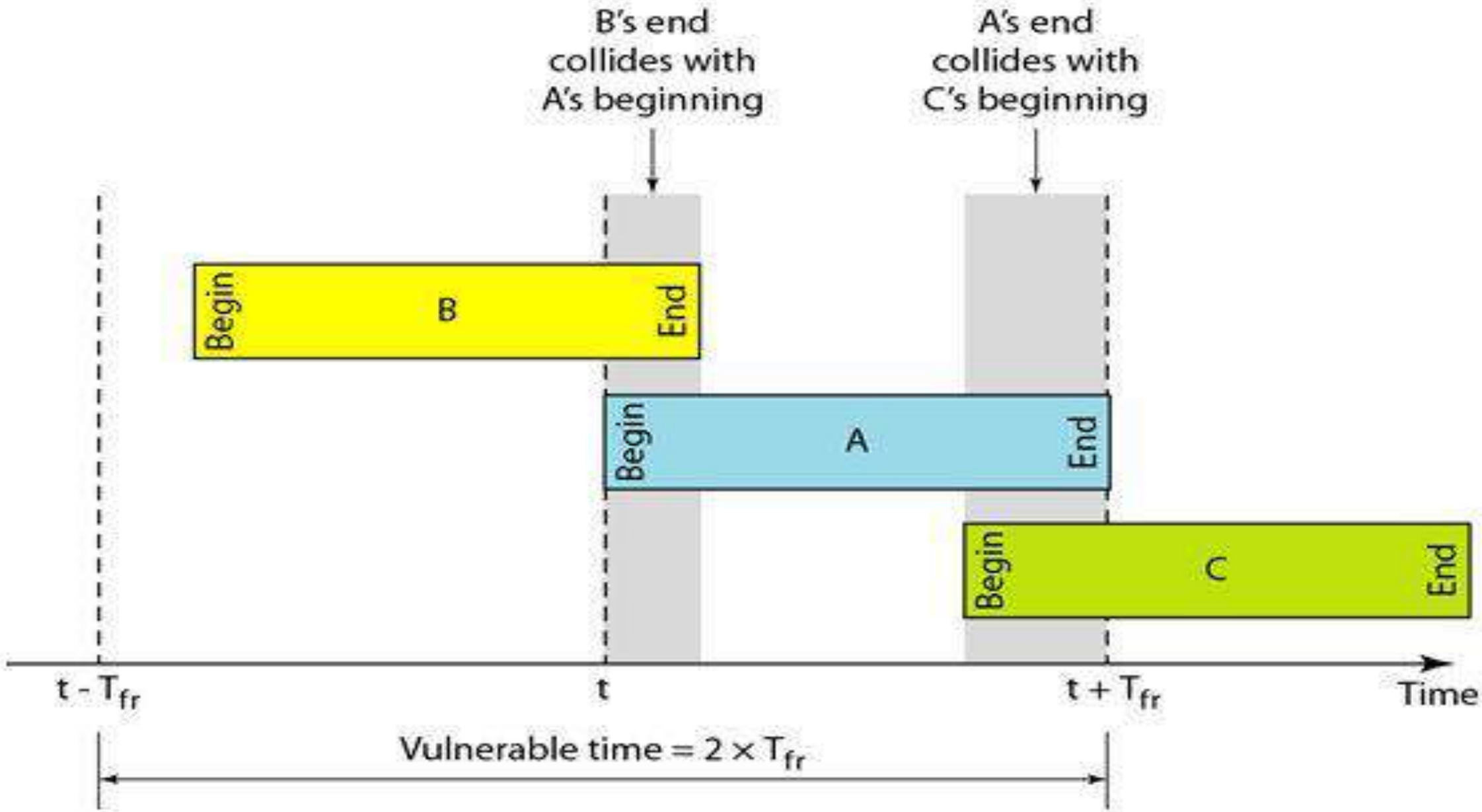


Figure 7.6 Transmission of frames in Aloha.


Station 1
Frame 1.1
Time
Station 2
Time
Station 3
Frame 3.2
Time
Station 4
Time
Collision duration
Collision duration


B's end
collides with
A's beginning
A's end
collides with
C's beginning
Begin
B
End
Begin
A
End
Begin
C
End
t - Tfr
t
t + Tfr
Time
Vulnerable time = 2 × Tfr

- **Whenever two frames try to occupy the channel at the same time, there will be collision and both will be confused.**
- **If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be transmitted later.**

Slotted Aloha

- **In slotted aloha, time is divided into separate intervals, each interval corresponding to one frame.**
- **This approach requires the users to agree on slot boundaries.**
- **A computer is not permitted to send whenever a carriage return is typed.**
- **Instead, it is required to wait for the beginning of the next slot.**

Sr. No.	Key	Pure Aloha	Slotted Aloha
1	Time Slot	In Pure Aloha, any station can transmit data at any time.	In Slotted Aloha, any station can transmit data only at beginning of any time slot.
2	Time	In Pure Aloha, time is continous and is not globally syncronized.	In Slotted Aloha, time is discrete and is globally syncronized.
3	Vulnerable time	Vulnerable time = 2 x Tt.	Vulnerable time = Tt.
4	Probability	Probability of successful transmission of data packet = $G \times e^{-2G}$	Probability of successful transmission of data packet = $G \times e^{-G}$
5	Maximum efficiency	Maximum efficiency = 18.4%.	Maximum efficiency = 36.8%.
6	Number of collisions	Does to reduces the number of collisions.	Slotted Aloha reduces the number of collisions to half thus doubles the efficiency.

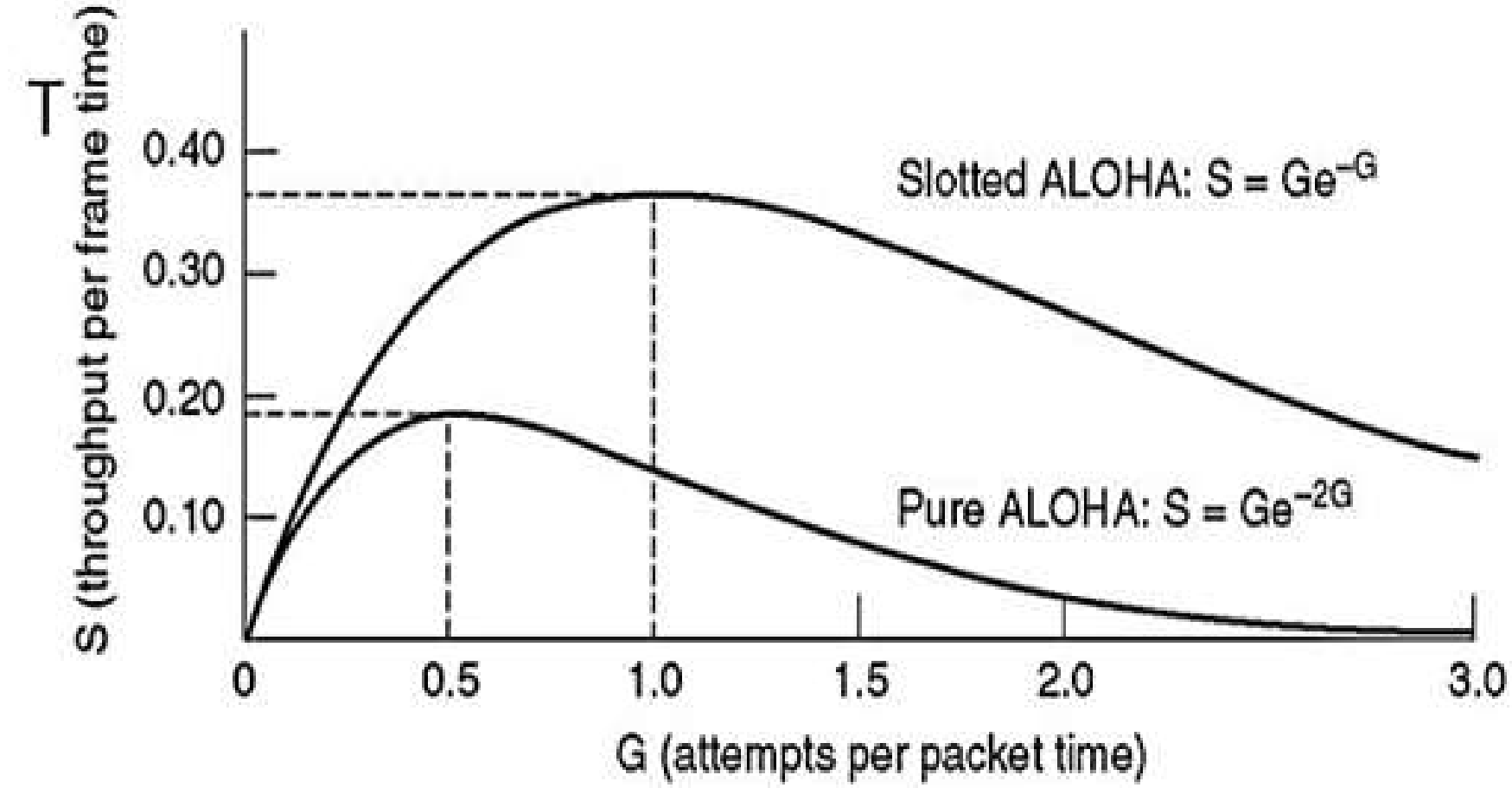


Fig: Pure Aloha and slotted Aloha

Carrier Sense Multiple Access (CSMA) protocols

- **Protocols in which stations listen for a carrier (transmission) and act accordingly are called carrier sense protocols.**
- **When a station has data to send, it first listens to the channel to see if anyone else is transmitting at the moment.**
- **If the channel is busy, the station waits until it detects an ideal channel.**
- **When the station detects an ideal channel, it transmit a frame.**
- **If collision occurs, the station waits a random amount of time and starts all over again.**

- **The protocol is called 1-persistent because the station transmits with a probability of 1, whenever it finds the channel ideal.**
- **A second carrier sense protocol is non-persistent CSMA.**
- **A station senses the channel. If no one else is sending the station begins doing so itself.**
- **However, if the channel is already in use, the station does not continuously sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.**

- **The last protocol is p-persistent CSMA.**
- **When a station becomes ready to send, it senses the channel.**
- **If it is ideal, it transmit with a probability *p*,**

CSMA with Collision Detection (CSMA/CD)

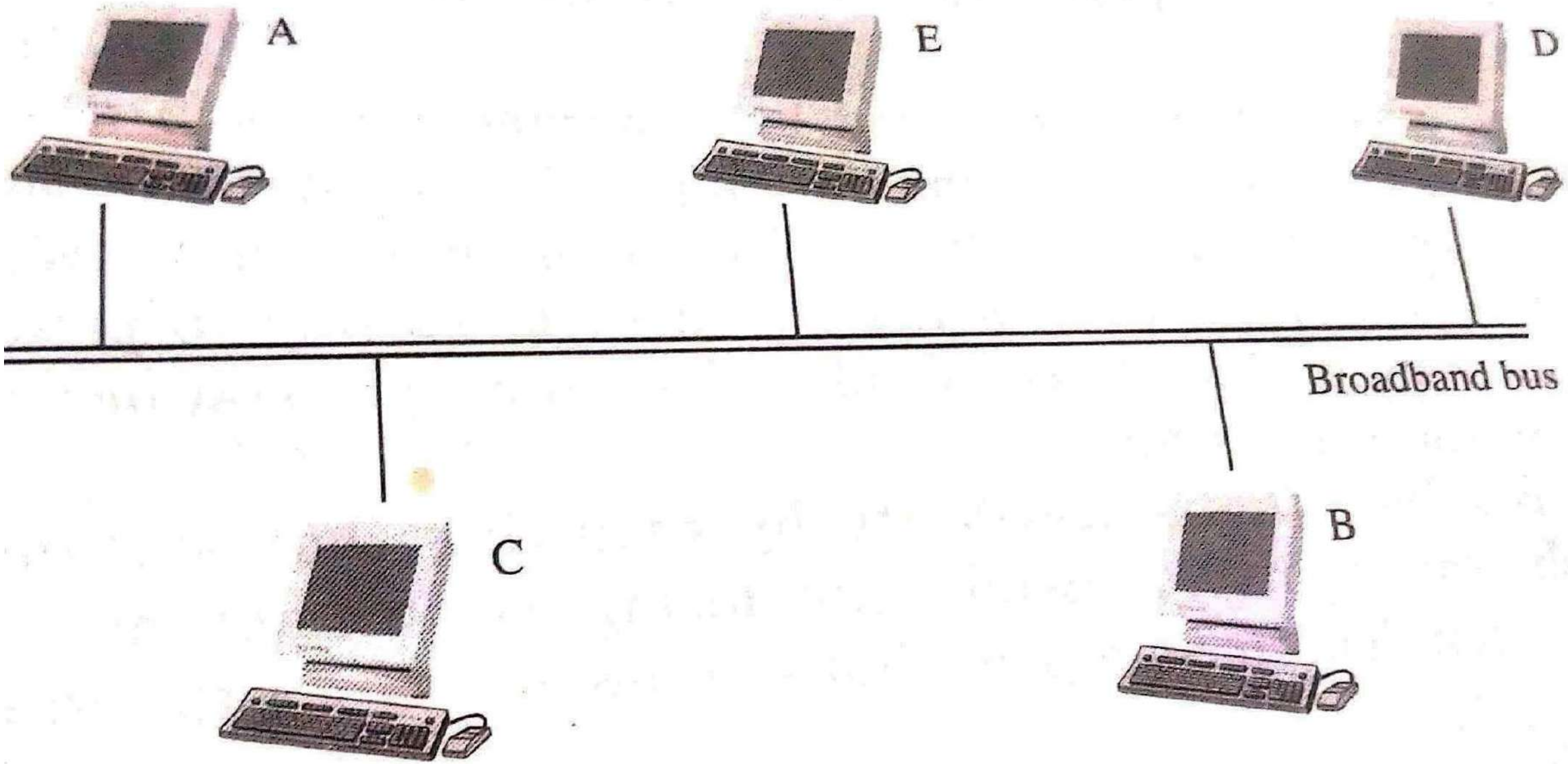
- **They ensure that no station begins to transmit when it sense the channel busy.**
- **A collision is detected, a sending station immediately stops transmitting.**
- **Technically, monitoring a cable during transmission is known as collision detection (CD), and the Ethernet mechanism is known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD).**

- **If two stations sense the channel to be ideal and begins transmitting simultaneously, they will both detect the collision almost immediately.**
- **Rather than finish transmitting their frames, they should abruptly stop transmission as soon as the collision is detected.**
- **Quickly terminating damaged frames save time and bandwidth.**
- **This protocol is CSMA/CD.**

TOKEN BUS: IEEE STANDARD 802.4

It combines the physical configuration of Ethernet (a bus topology) and the collision-free feature of Token Ring.

Station (computer) wanting to send something must wait for the token to arrive.

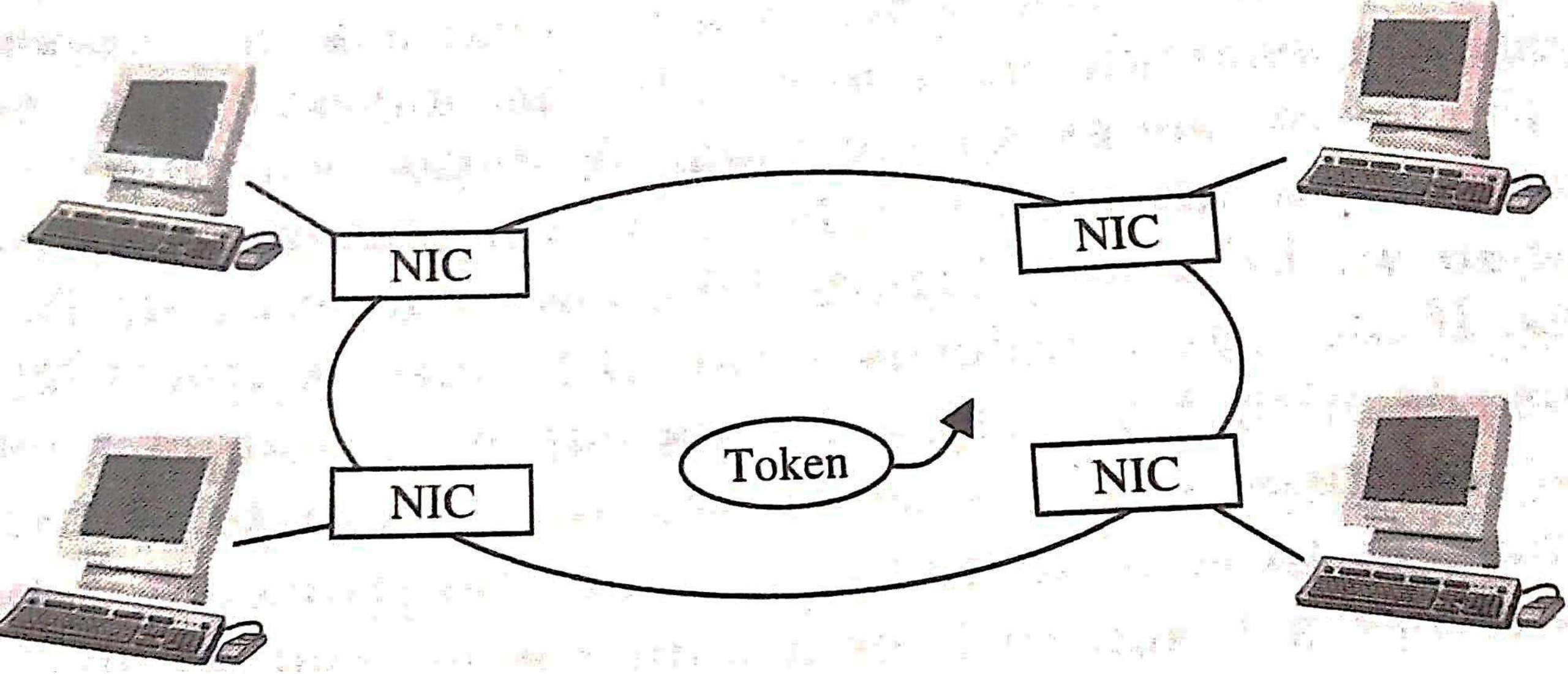


Token circulates: A-B-C-D-E

- **Five stations A, B, C, D and E, connected to a bus.**
- **If the logical order is A-B-C-D-E, then A starts by sending a token to B along the bus.**
- **As with Ethernet, each station is capable of receiving it, but the token's destination address specifies which station is goes it.**
- **When B receive the token, it has permission to send a frame. If it has no frame, it sends a token to C. Similarly C sends either a token to D or a data frame, and so on.**
- **Generally, a station receives a token from its predecessor and sends a token to its successor.**

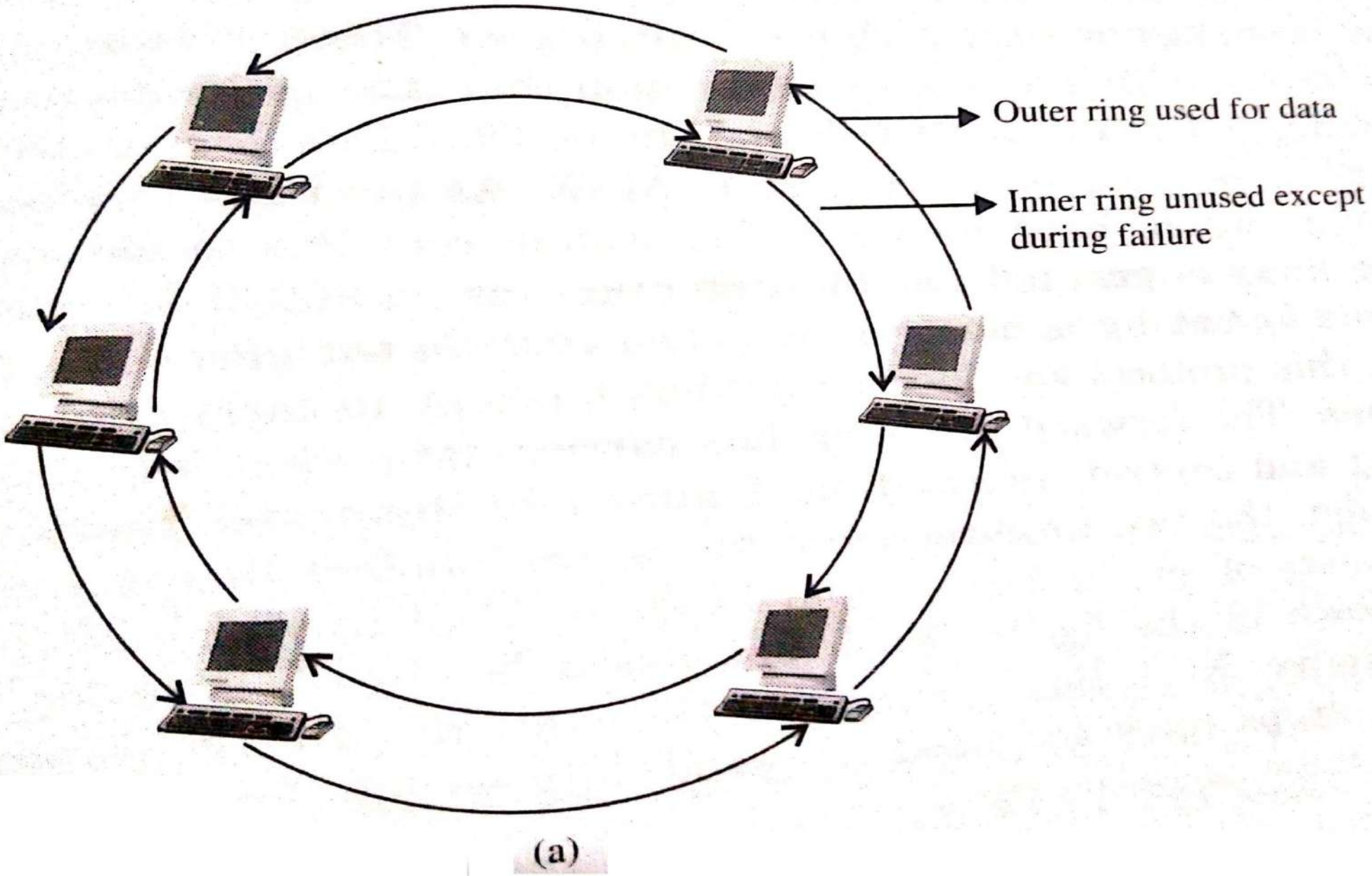
TOKEN RING: IEEE STANDARD 802.5

- **Stations on a token ring LAN are connected in a ring using a NIC**
- **Station can send directly only to its neighbours and in most cases, only to one neighbour (clockwise)**
- **If station wants to send to another**
- **Each computer may transmit only during its turn and may send only one frame during each turn.**


NIC
NIC
NIC
NIC
Token

FIBRE DISTRIBUTED DATA INTERFACE (FDDI)

- **FDDI standards for a 100 Mbps fibre optic LAN.**
- **Contains two complete ring – one that is used to send data when everything is working correctly, and another that is used only when the first ring fails.**
- **A computer always transmits and receives frames on the outer rings, while the network hardware forwards bits on the inner ring without interpreting them.**


Outer ring used for data
Inner ring unused except during failure

(a)

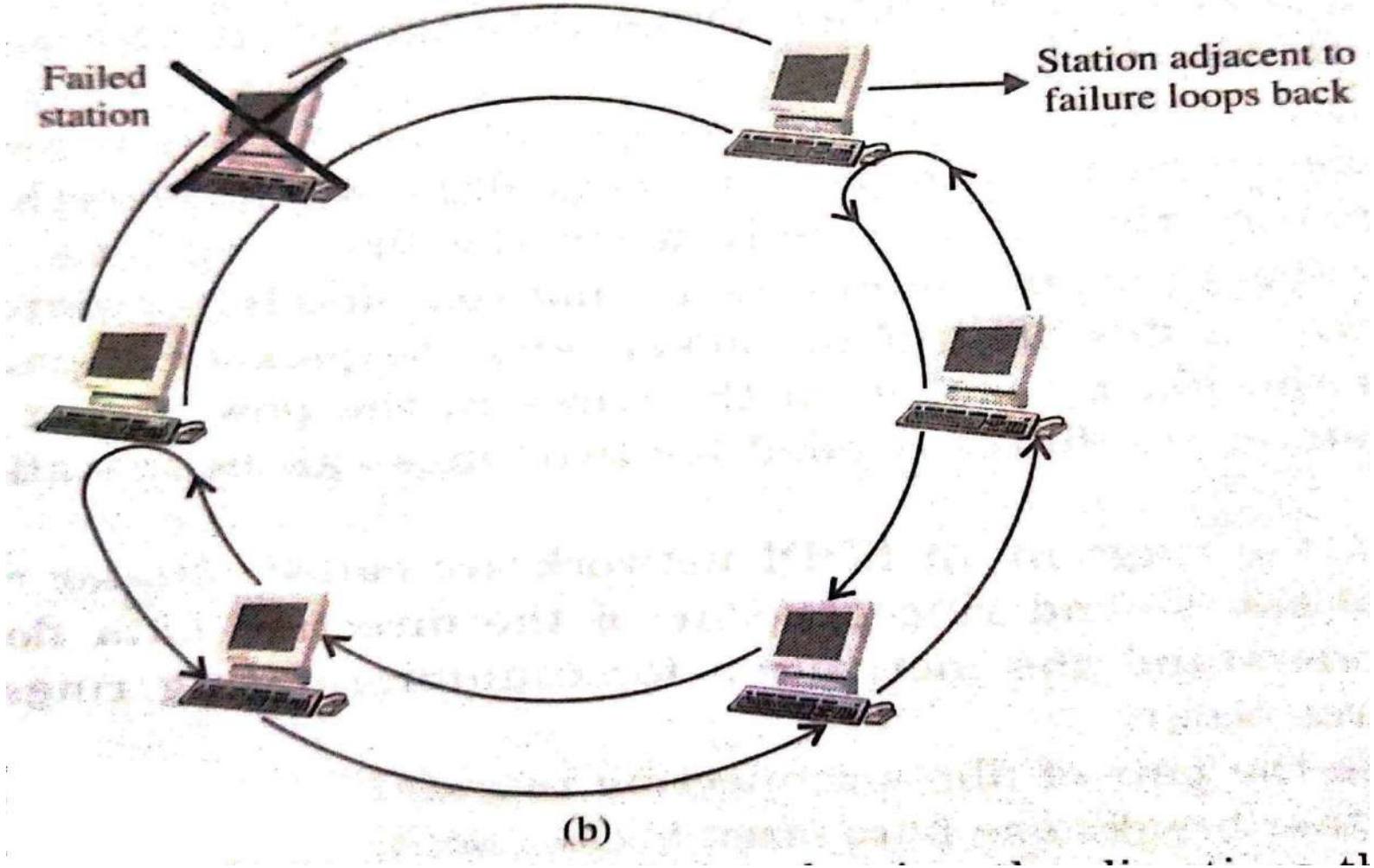


Fig: (a) An FDDI network with arrows showing the directions that data flows and (b) The same network after the station has failed

DISTRIBUTED QUEUE DUAL BUS (DQDB): IEEE STANDARD 802.6

- **It is designed to be used in MAN.**
- **Each device in the system connects to two backbone links.**
- **To carry data in forward and reverse directions.**
- **The forward directions bus carries data while the reverse direction handles queuing and control information**
- **Each bus connects to the stations directly through input and output ports.**
- **To send data on one bus, a station must use the other bus to make a reservation.**

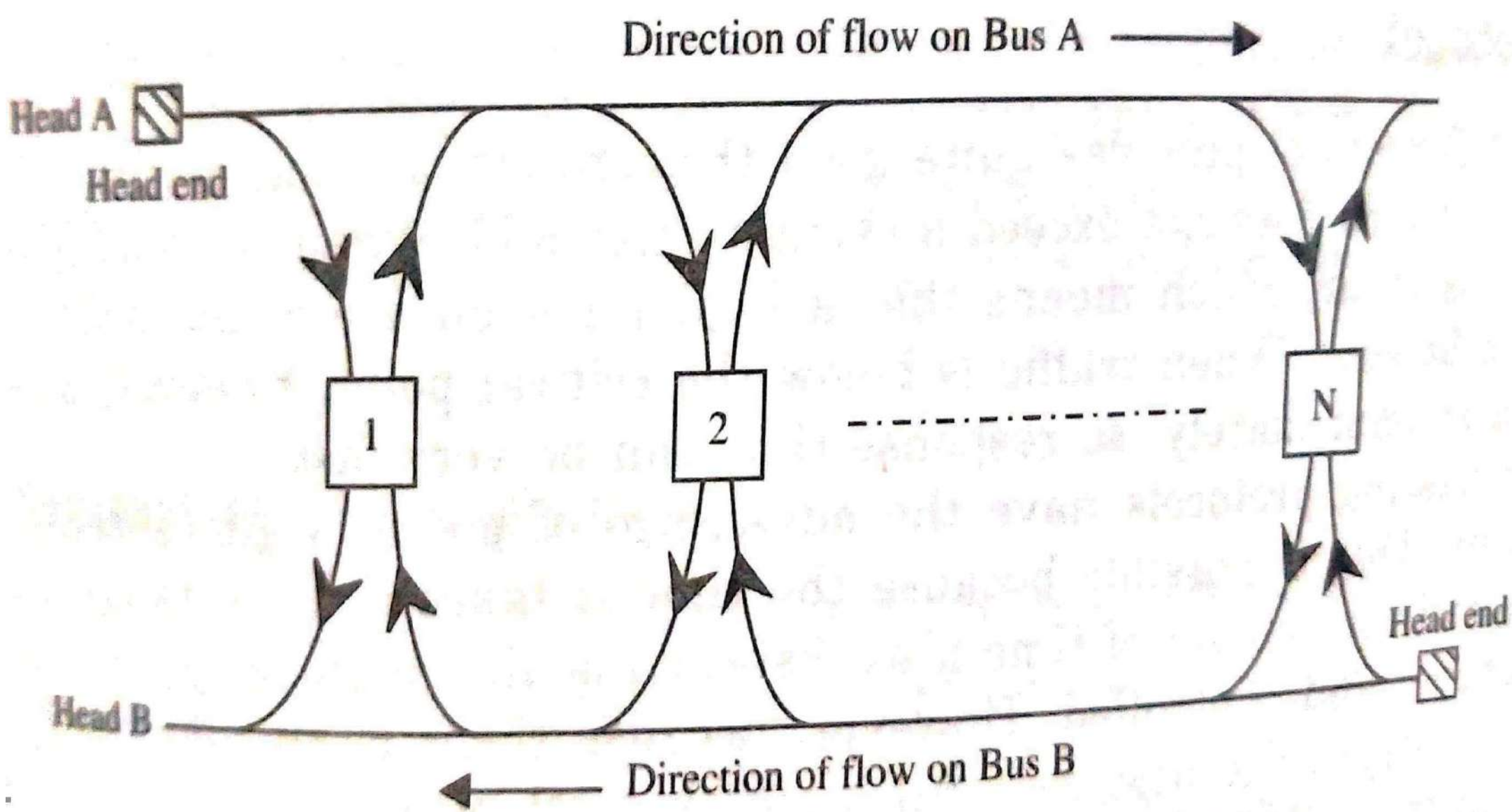


Figure 7.12 DQDB topology.

LAN INSTALLATION AND PERFORMANCE

Tasks of installing a LAN are:

- **Install**

  New workstations

  NIC's on existing workstations

  Wiring or cabling

  Server hardware

  Bridges, routers, brouters or gateways

  LAN software

- **Determine the access and capability required by each user.**

- **Document the LAN's hardware and software configuration**
- **Train the users**
- **Using the LAN and its new capabilities**
- **Troubleshoot any startup problems**

Performance of LAN is based on several factors:

Protocol

Speed of transmission

Amount of traffic

Error Rates

Efficiency of LAN software

Speed of Server

LAN OPERATING SYSTEMS

- **Novell Network**
- **Windows NT**
- **LAN Manage and LAN server**
- **Apple Talk.**

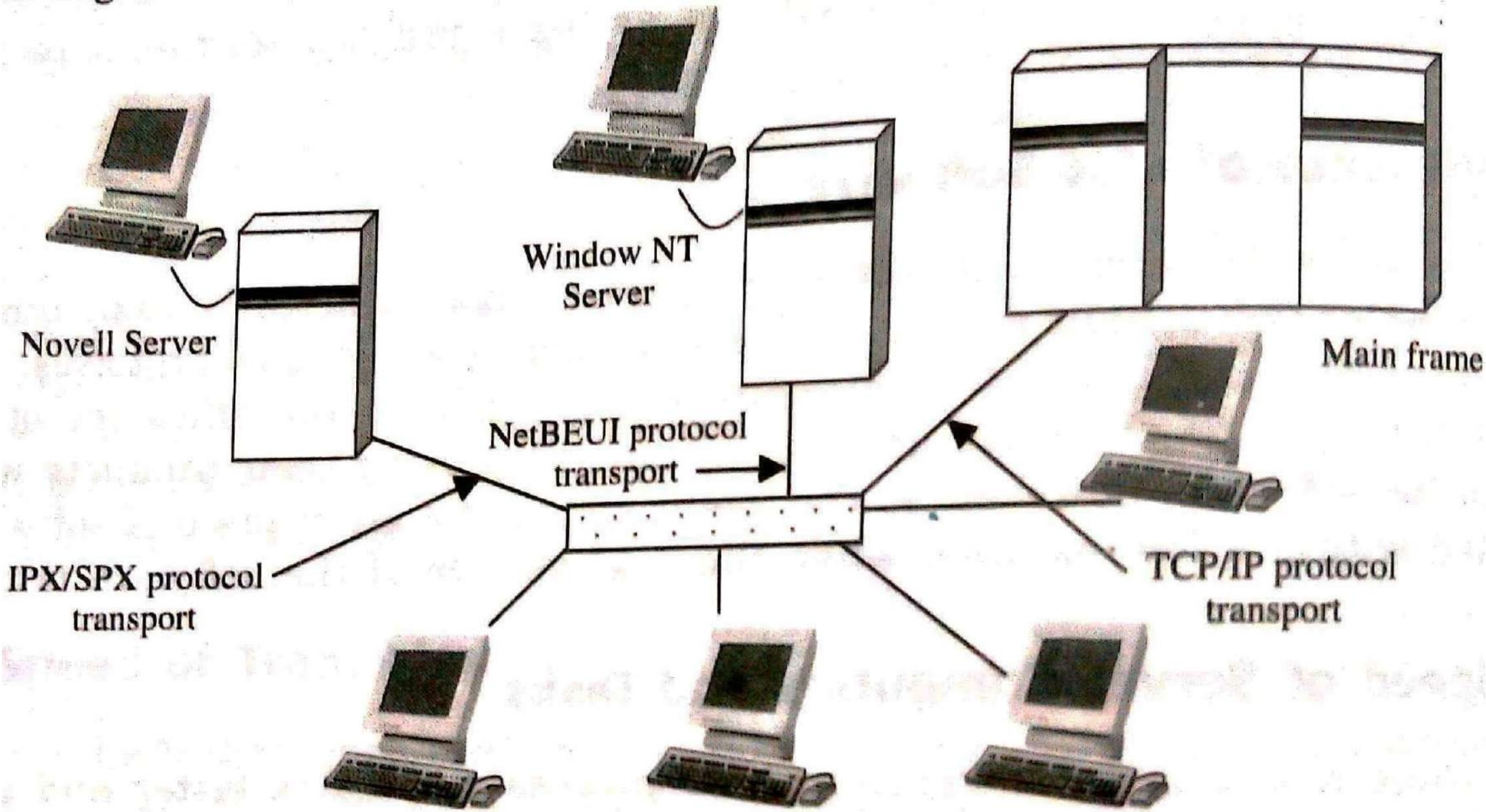


Figure 7.13 Transporting multiple protocols over a single network.

IPX (Internet Packet Exchange)

Protocol is designed for use with Netware

SPX (Sequence Packet Exchange)

Exchange of application specific data with greater reliability than IPX

Windows NT

Compatible with Ethernet and Token ring LANs

NetBEUI (Network Basic Input-Output System)

LAN protocols must provide the following:

- Reliable network links
- Reasonably high speeds
- Source and Destination node address handling
- Adherence to network standards
- IEEE 802 standards

Suppliers of Operating Systems

- Microsoft
- Hewlett Packet (HP)
- Microsystems

ETHERNET TECHNOLOGIES

- **Used network technology**
- **Consisted of a single coaxial cable, called the ether, to which multiple computers are connected.**
- **Ethernet segment is limited to 500 meters in length**
- **Requires a minimum separation of 3 meters between each pair of connection.**
- **Operated at a bandwidth of 10Mbps,**
- **Fast Ethernet operates at 100 Mbps,**
- **Recent version, which is known as 1 Gbps**

- **Common Ethernet Technologies**

  10 Base-2 (thin Ethernet)

  10 Base-5 (thick Ethernet)

  10 Base-T and 100 Base-T

  Gigabit Ethernet

10 Base-2 (thin Ethernet)

- **More flexible coaxial cable, only 0.25” diameter, is often used for PC LANs.**
- **The ‘10’ in 10 Base 2 standards for “10 Mbps”; the ‘2’ stands for “200 meters”**
- **The frame passes through a “T-connector”**
- **One terminator must be connected to ground.**

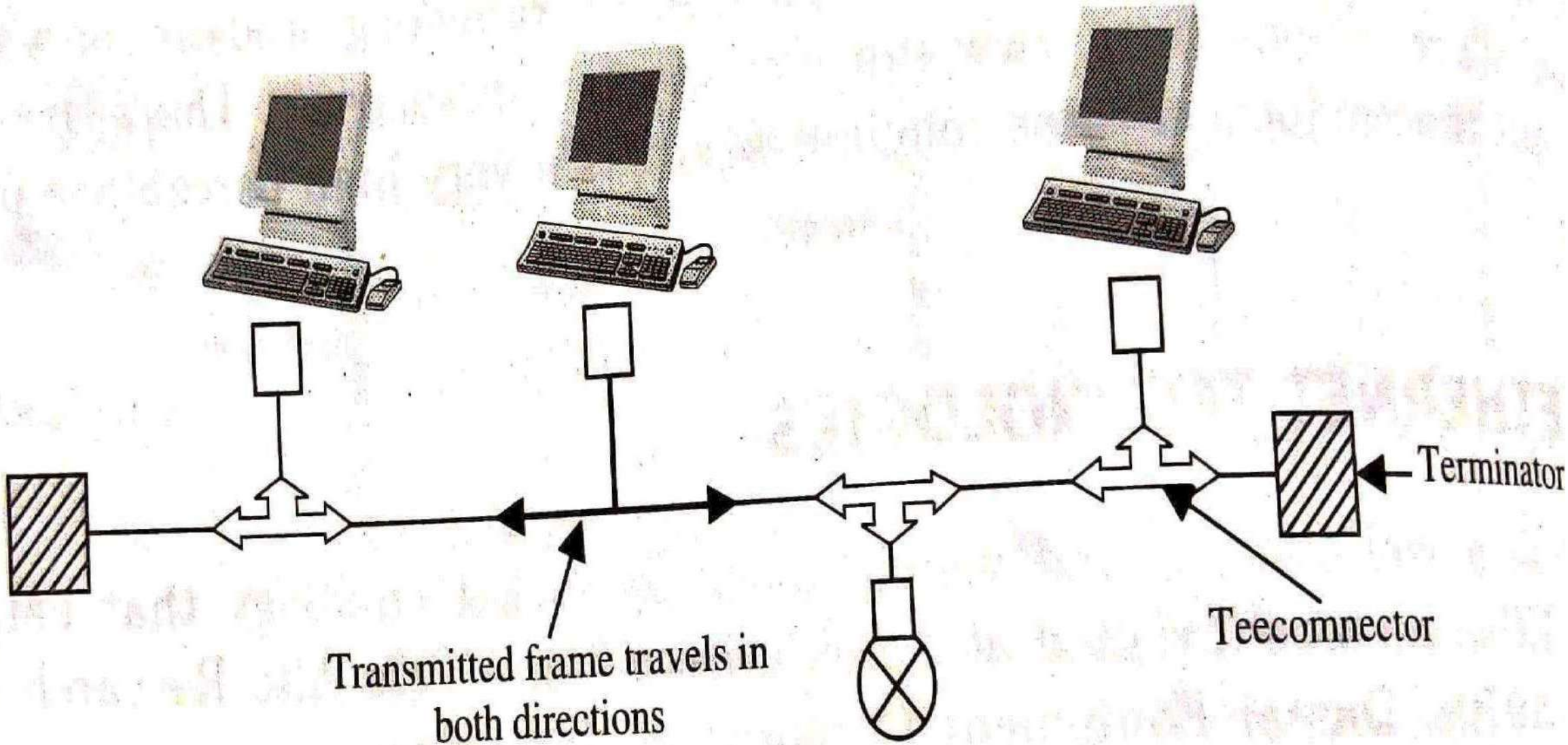


Figure 7.14 A 10 Base-2 Ethernet.

Base- 5 Thick Technology

- **A speed of 10Mbps using baseband transmission for a maximum distance of 500 meters**
- **The 500 meters distance limitation constitutes a segment of the 10 Base-5 Ethernet LAN.**
- **If the distance needs to be exceeded, a second segment must be installed and connected with a switch.**

10 Base-T and 100 Base-T

- **Ethernet use a star topology.**
- **Connection consists of two pairs of twisted-pair copper wire, one for transmitting and the other for receiving.**
- **For both 10 Base-T and 100 Base-T, the maximum length of the connection between an adapter and the hub is 100 meters, the maximum length between any two nodes is thus 200 meters.**
- **Sense the channel to determine if it is ideal**
- **Detect a collision while it is transmitting.**

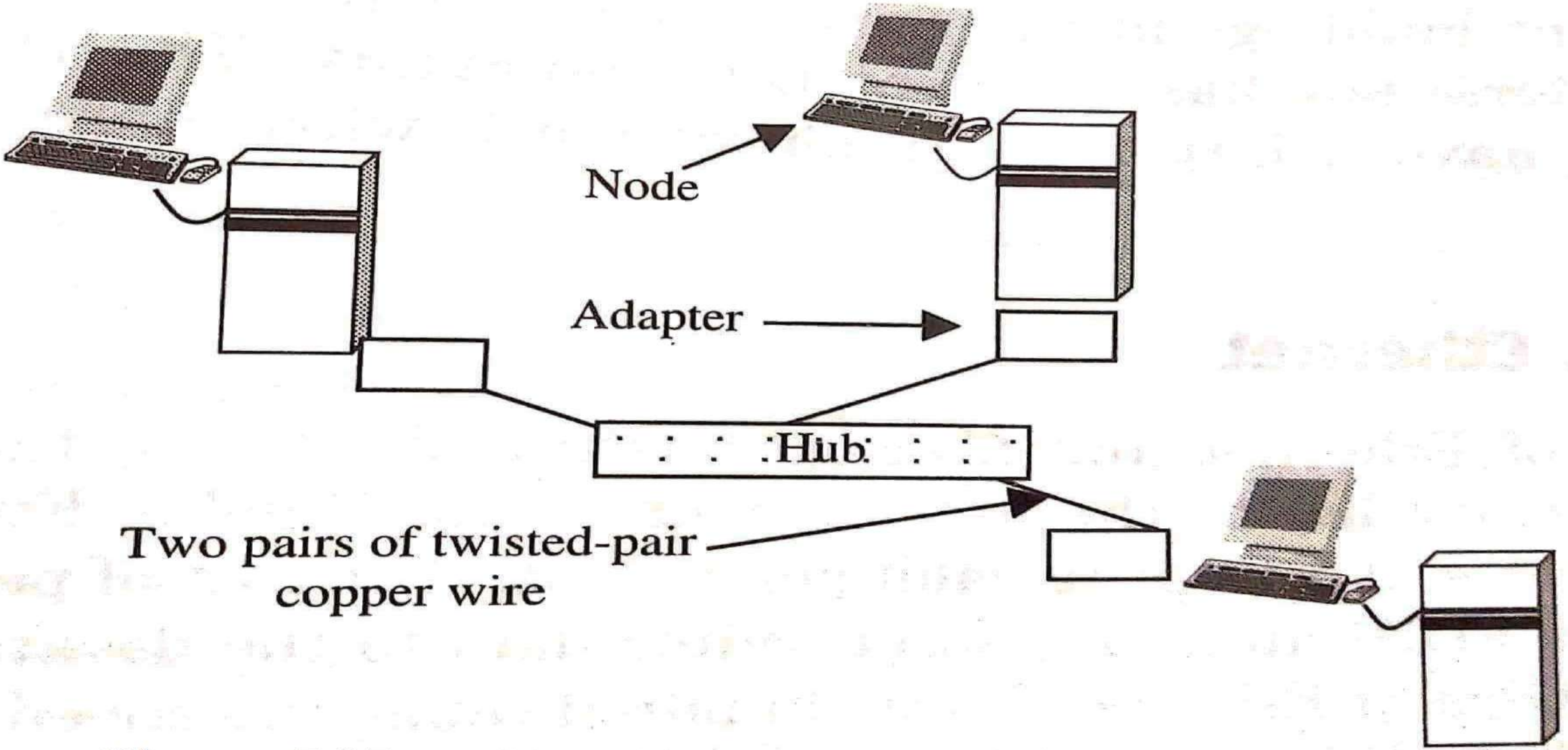


Figure :7.15

Star topology for 10 Base-T and 100 Base-T.

Gigabit Ethernet

- **Fiber-optic communication, the logical evaluation in Ethernet Technology led to the development of the Gigabit Ethernet**
- **Operates 1 Gbps**
- **IEEE 802.3z**
- **Full-duplex operation at 1Gbps in both directions for point-to-point channels.**
- **Star topology with a hub or switch at its centre.**

Thank You...

ADHIPARASAKTHI COLLEGE OF ARTS AND SCIENCE

(Autonomous)

G.B. Nagar, Kalavai - 632506

Data and Communication Networks

UNIT - III

ERROR DETECTION AND CORRECTION

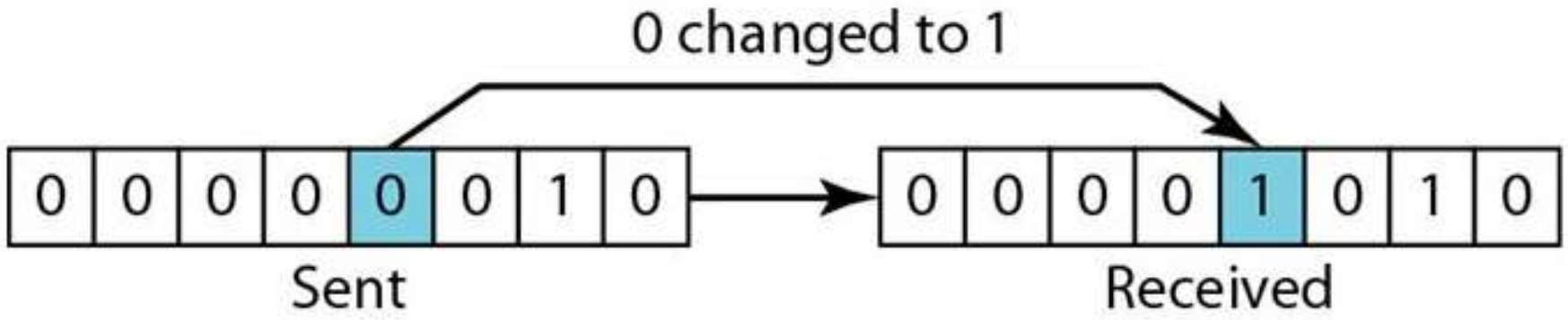
- **Network must be able to transfer data from one device to another with complete accuracy.**
- **Any time data can get corrupted during transmission.**
- **The ability to detect when a transmission has been changed is called *error detection*.**
- **When errors are detected, the message is discarded, the sender is notified, and the message is send again.**

- **When an error is detected, it may actually be fixed without a second transmission. This is called error correction.**
- **For reliable communication, errors must be detected and corrected.**

TYPES OF ERRORS

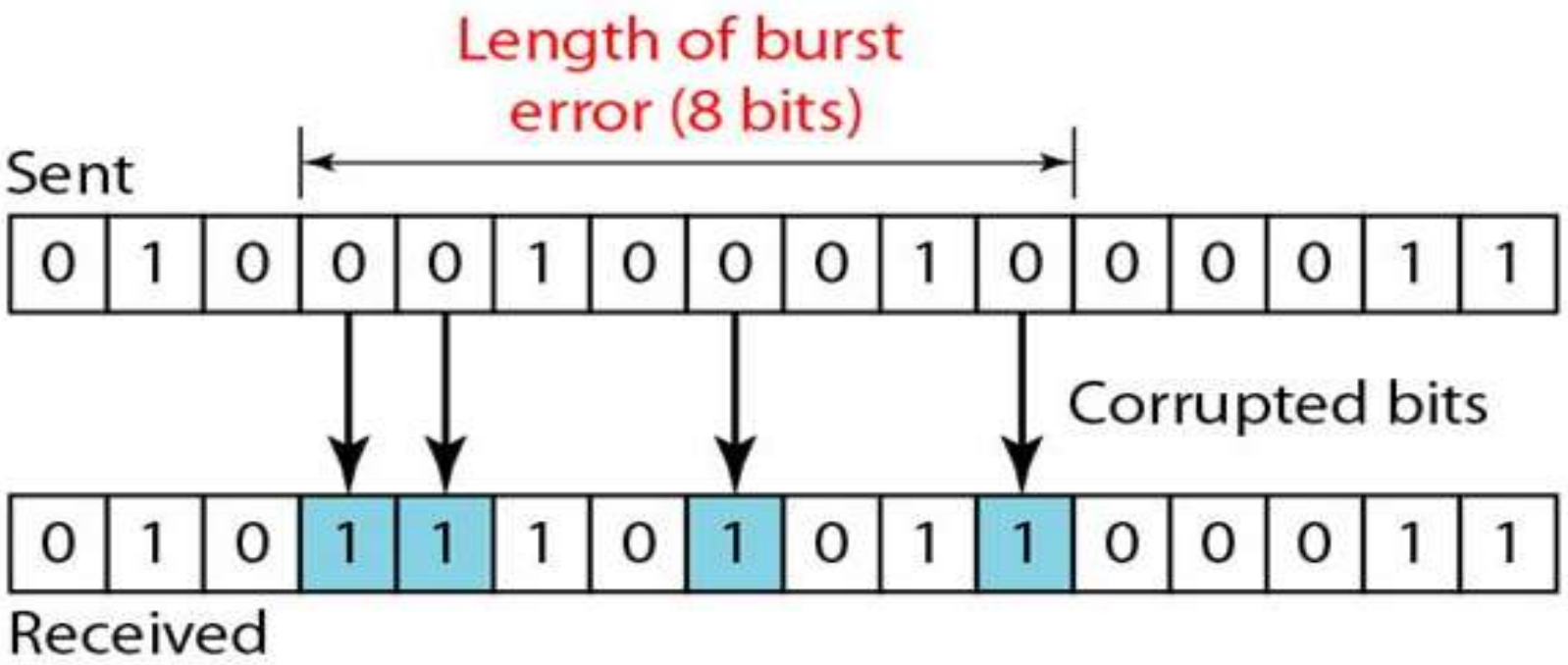
Single-bit error:

- **In a single-bit error, 0 is changed to 1 or 1 is changed to 0.**
- **Only one bit of a given data unit is changed.**



Burst Error:

- **Burst error means that two or more than two bits in the data unit have changed from 1 to 0 or 0 to 1.**



- **The difference between the first corrupted bit and the last corrupted bit is called the length of the burst error.**
- **Burst error can happen in a serial transmission because duration of noise.**

DATA COMPRESSION

- **Compress the data at the sender, then transmit it over the network, and finally to decompress it at the receiver.**
- **Categories : *Lossless compression, Lossy compression***

Loss compression :

- ✓ **Ensures that the data recovered from the compression/decompression process is exactly the same as the original data.**
- ✓ **No data is lost and the decompressed data are identical to the original uncompressed data.**

Lossy compression :

- ✓ **Lossy compression does not promise that the data received is exactly the same as the data sent.**
- ✓ **Example : for image or video compression, the criterion may be that the decompressed image is unclear from the original to the human eye.**

Data encoding is normally classified into two main areas

Entropy encoding

Source encoding

Entropy coding:

- **Statistical encoding**

  If a source of text contains many more ‘e’ characters than ‘z’ characters, then the character ‘e’ could be coded with few bits and the character ‘z’ with many bits.

- **Suppressing repetitive sequence**

  The page contains large amount of ‘white space’. If the image of this page were to be stored, a special character sequence could represent long runs of ‘white space’

Source coding:

- **Characteristics of the information**
- **Ex: Images normally contain many repetitive sequence such as common pixel colours in neighboring pixels.**

Data compression techniques:

- **Image compression (JPEG)**
- **Video compression (MPEG)**
- **Audio compression (MP3)**

Image compression (JPEG)

- **JPEG is an acronym for the Joint Photographic Expert Group.**
- **Used to compress both gray scale and photographic quality colour images.**
- **JPEG is lossy: The image obtained after decompression may not be the same as the original.**
- **Picture is divided into blocks of 8 x 8 pixels.**

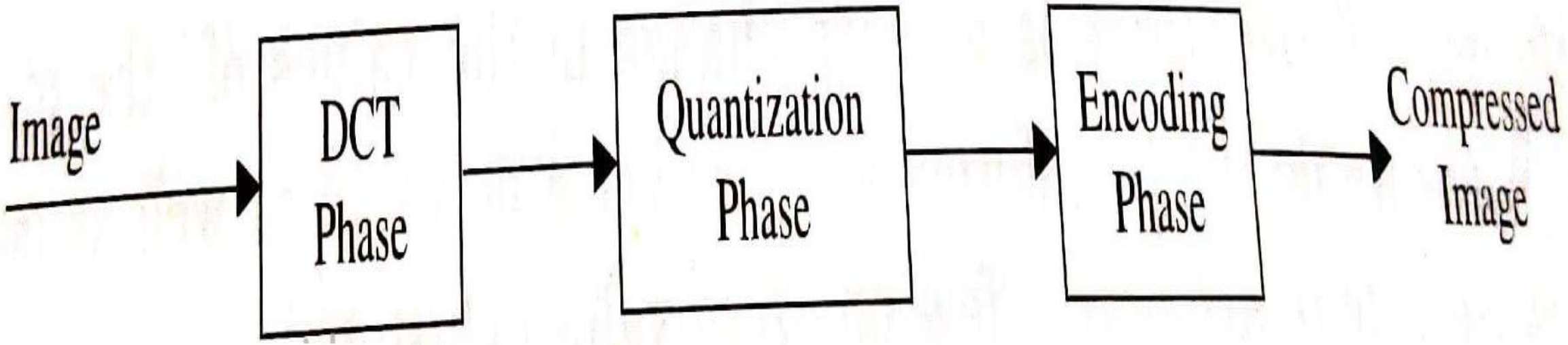


Figure 5.1 Block diagram of JPEG compression.

Discrete Cosine Transform (DCT) Phase

- **DCT takes an 8 x 8 matrix of pixel values as input and output an 8 x 8 matrix of frequency coefficients.**

Case I: Block of uniform gray, and the value of each pixel is 20

Case II: Block with two different uniform gray scale sections

Case III: Block that changes gradually.

Picture

20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20

P (x, y)

160	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

T (m, n)

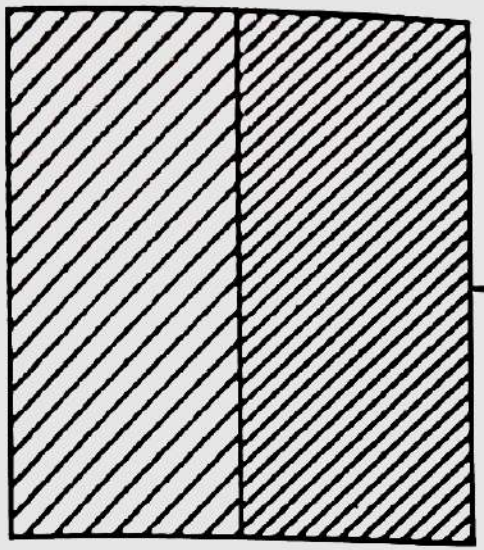
Figure 5.2 Uniform gray scale.

Case I: Block of uniform gray, and the value of each pixel is 20

- **In the first case, do the transformations, we get a non-zero value for the first element (upper left corner), the rest of the pixels have a value of 0 (zero).**
- **T(0,0) is the average of the P(x,y) values and is called the dc value (direct current)**
- **The rest of the values, called ac value in T(m,n) represent changes in the pixel values, there are no changes, the reset of the values are 0's.**

Case II: Block with two different uniform gray scale sections

- **In the second case, there is a sharp changes in the values of the pixels (from 20 to 50)**
- **When we do the transformations, we get a dc value as well as non-zero ac values.**
- **However, there are only a few non-zero values clustered around the dc value.**
- **Most of the values are 0.**



Picture

20	20	20	20	50	50	50	50
20	20	20	20	50	50	50	50
20	20	20	20	50	50	50	50
20	20	20	20	50	50	50	50
20	20	20	20	50	50	50	50
20	20	20	20	50	50	50	50
20	20	20	20	50	50	50	50
20	20	20	20	50	50	50	50

P (x, y)

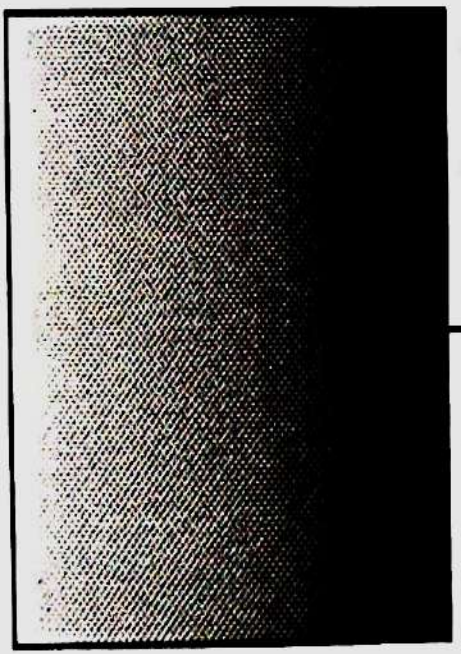
280	–109	0	39	0	–25	22
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

T (m, n)

Figure 5.3 Two different uniform gray scales.

Case III: Block that changes gradually.

- **In the third case, there is no sharp change between the values of neighbouring pixels.**
- **When we do the transformations, we get a dc value , with many non-zero ac values also.**



Picture

20	30	40	50	60	70	80	90
20	30	40	50	60	70	80	90
20	30	40	50	60	70	80	90
20	30	40	50	60	70	80	90
20	30	40	50	60	70	80	90
20	30	40	50	60	70	80	90
20	30	40	50	60	70	80	90
20	30	40	50	60	70	80	90

P (x, y)

400	–146	0	–31	–1	3	–1	–8
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

T (m, n)

Figure 5.4 Gradient gray scale.

We can sate the following based on above diagram

1. **The transformation creates Table ‘T’ from Table ‘P’**
2. **The dc value is the average value of the pixels**
3. **The ac value are the changes**
4. **Lack of changes in neighbouring pixels creates 0’s.**

Quantization Phase

- **Quantization is dropping the irrelevant bits of frequency numbers.**
- **Dropped the fraction from each value and kept the integer part.**

Encoding Phase

- **Starting with the dc value in position (0,0) the values are processed in a zigzag sequence.**
- **The table is read diagonally in a zigzag fashion rather than row by row or column by column**

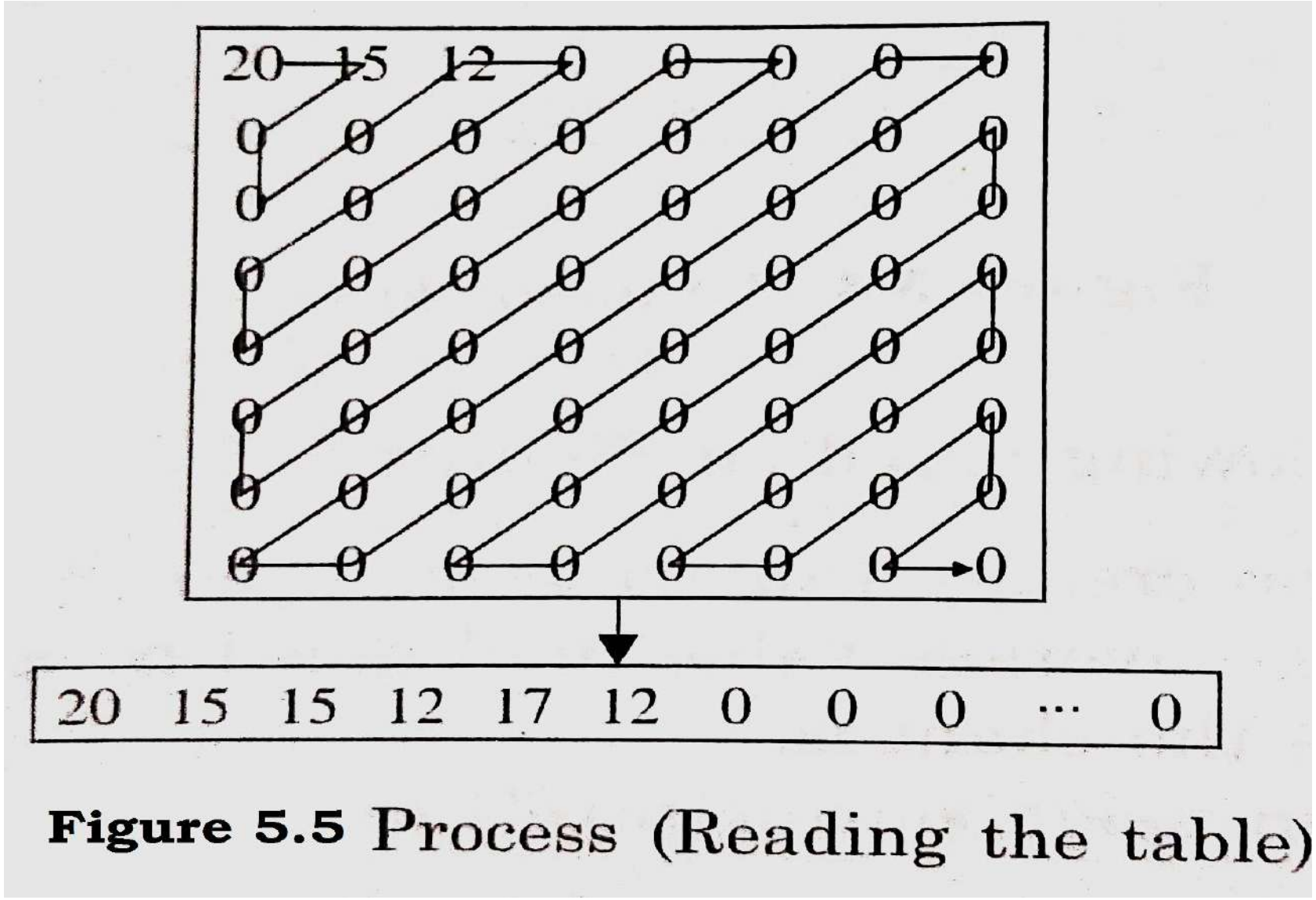


Figure 5.5 Process (Reading the table)

Video Compression (MPEG)

- **The Moving Picture Expert Group (MPEG)**
- **Provides for compression of the sound track associated with the video.**
- **Types: within the frame and between frame.**
- **Within-the-frame compression means that individual frames making up the video sequence are encoded as if they were ordinary still images.**
- **A frame that has been encoded in this way is called an intra-coded or I-picture (intra-picture)**

- **MPEG encodes successive frames as predictive – codded or P-Picture.**
- **(i.e) only the pixels that have changed since the I-Picture are included in the P-picture**

MPEG Standards:

- **MPEG-1:**

  Digital storage media at up to about 1.5 Mbps

  Used on video CD and low quality video on DVD

  Digital satellite/cable TV services, also known as MP3

- **MPEG-2:**

  Standard broadcast interlaced video with good compression

  Transport, video, and audio standards for broadcast TV

  Digital TV set top boxes and DVD's

- **MPEG-4:**

  - ✓ **To provide an audio-video coding standard for very-low-bit-rate applications.**
  - ✓ **Such as mobile applications and non-broadband Internet access.**
  - ✓ **Computer-aided design output or computer generated cartoons.**

- **MPEG – 7:**

  Multimedia Content Description Interface.

  Fast and flexible searching for material.

- **MPEG – 21:**

  Supporting the delivery and use of all content types by different categories.

AUDIO COMPRESSION (MP3)

- **MPEG not only defines how video is compressed, but it also defines a standard for compressing audio.**
- **Sampled at the rate of 44.1kHz (sample is collected approximately once every 23 microseconds)**
- **Each sample is 16 bits, the audio stream results in a bit rate of**

  2 x 44.1 x1000 x 16 = 1.41 Mbps

- **Synchronization and error correction overhead require that 49 bits be used to encode each 16 bits sample. Resulting in an actual bit rate of**

  49/16 x 1.4.1 Mbps = 4.32 Mbps

- **MPEG address this need by defining three levels of compression, as shown in below**

Table : MP3 Compression Rates

Coding	Bit rates	Compression factor
Layer I	384 Kbps	4
Layer II	192 Kbps	8
Layer III	128 Kbps	12

- **Layer III, commonly known as MP3.**
- **The layer III compression option can reduce the bit rate of an audio signal by a factor of 12 with a very lowless in sound quality**

- **MP3 audio is a set to develop the way that music is distributed and licensed.**
- **A typical audio track is sampled at 44100 times / seconds, for two channel at 16 bits / sample.**
- **Thus the data rate is 1.411 Mbps giving a total of 50.47 MB for a five minutes song.**
- **As the storage of a CD is around 650 MB, it is possible to get 64 minutes from the CD**
- **Bandwidths to download a five minute audio file from the Internet in its raw form (over 3 hrs with 56 Kbps)**

- **If the audio file was compressed with MP-3, it can be reduced to one-tenth of its original size, without losing much of its original content.**

ISDN services

- **Provide fully combined digital services to users.**
- **Categories**

  Bearer services

  Teleservices

  Supplementary services

Bearer services:

- **Provide the means to transfer information (voice, data & video)**
- **Used circuit switched, packet switched and frame switched**

Teleservices :

- **Rely on the facilities of the bearer services and are designed.**
- **Include**

  Telephony

  Teletex

  Telefax

  Videotext

  Teleconferencing

Supplementary services:

- **Provide additional functionality to the Bearer services and Teleservices.**
- **Services are :**

  Reverse charging

  Call waiting

  Message handling

  Telephone company services

ISDN Topology

. Integrated with office environment.

. Primary functional group designations

Network Termination 1 (NT1)

Network Termination 2 (NT2)

Network Termination 12 (NT12)

Terminal Equipment 1 (TE 1)

Terminal Equipment 2 (TE 2)

Terminal Adapter (TA)

Network Termination 1 (NT1):

- **Non intelligent devices, physical interface**
- **The boundary between a user's site and the ISDN central office.**

Network Termination 2 (NT 2):

- **Intelligent devices**
- **Functions are:**

  Switching concentration

  Multiplexing

- **NT2 device is a digital PBX, connect a user's equipment.**

Network Termination 12 (NT12):

- Combination of NT1 and NT2 in a single device.

Terminal Equipment 1 (TE1):

- Includes ISDN devices such as an ISDN terminal, digital telephone.
- Connect directly to a network termination devices.

Terminal Equipment 2 (TE2):

- Non ISDN devices including printers, PCs, analog telephones.

Terminal Adapter (TA):

Designed to used with TE2 equipment to convert their signals to an ISDN compatible format.

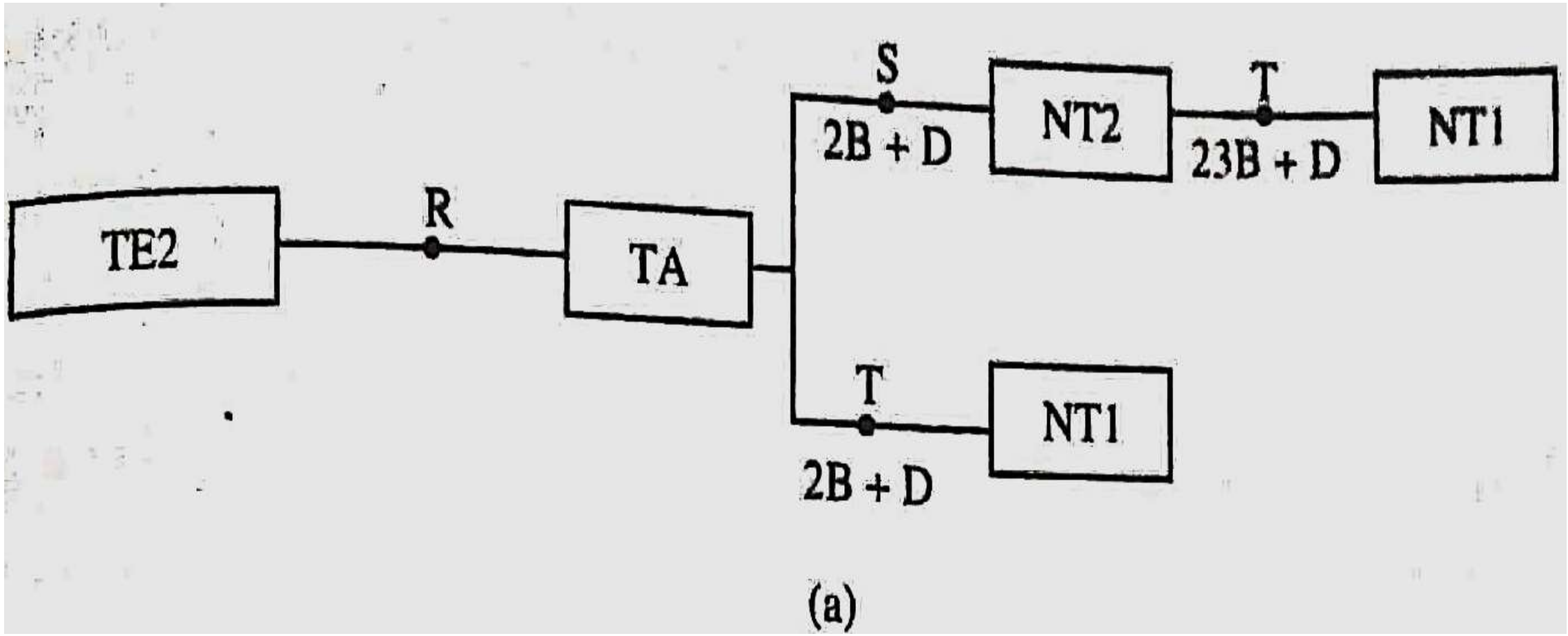
- **Reference point:**

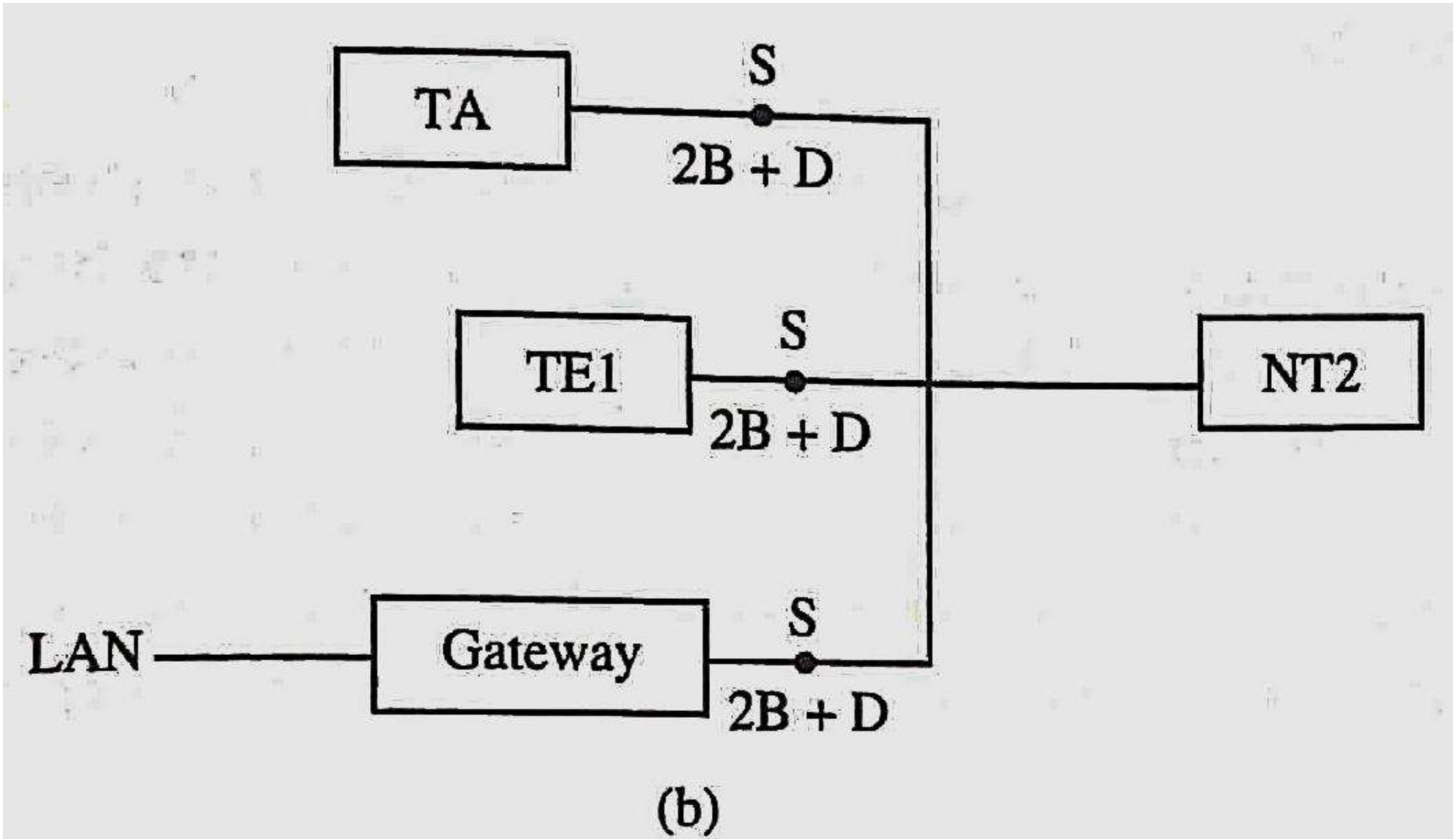
  R – separates TE2 equipment from TA

  S – separates NT2 equipment from ISDN services

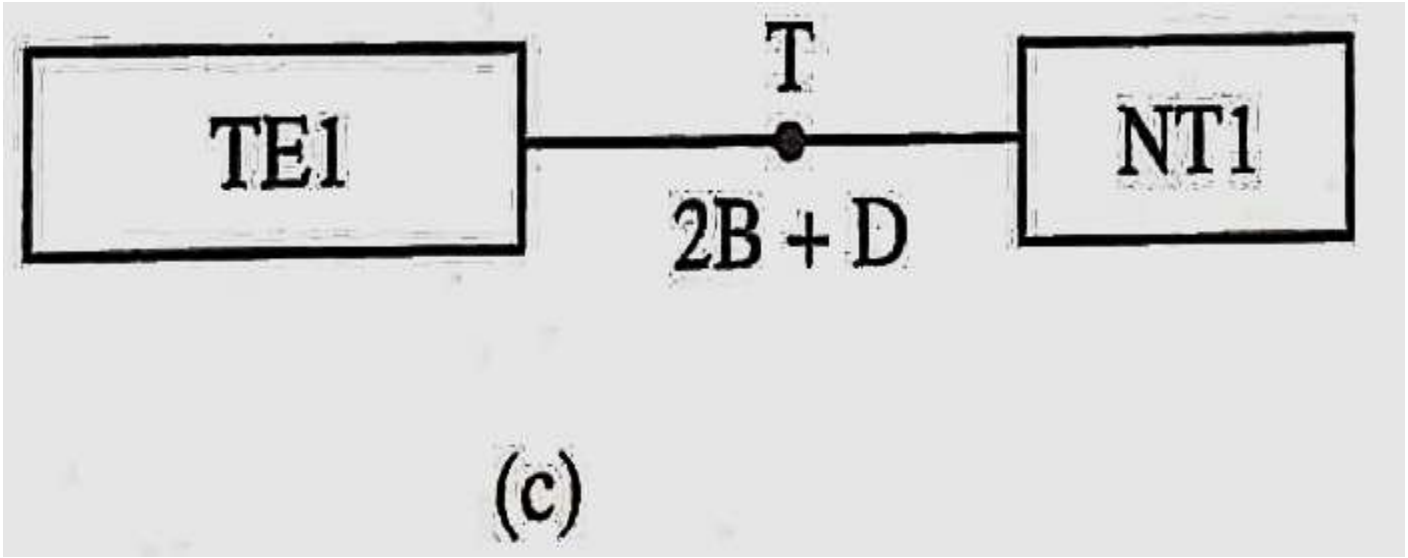
  T – Access point to the customer site

  U – Connection between NT1, and the ISDN central office.


TE2
R
TA
S
2B + D
NT2
T
23B + D
NT1
T
2B + D
NT1
(a)



(b)


TE1
T
2B + D
NT1
(c)

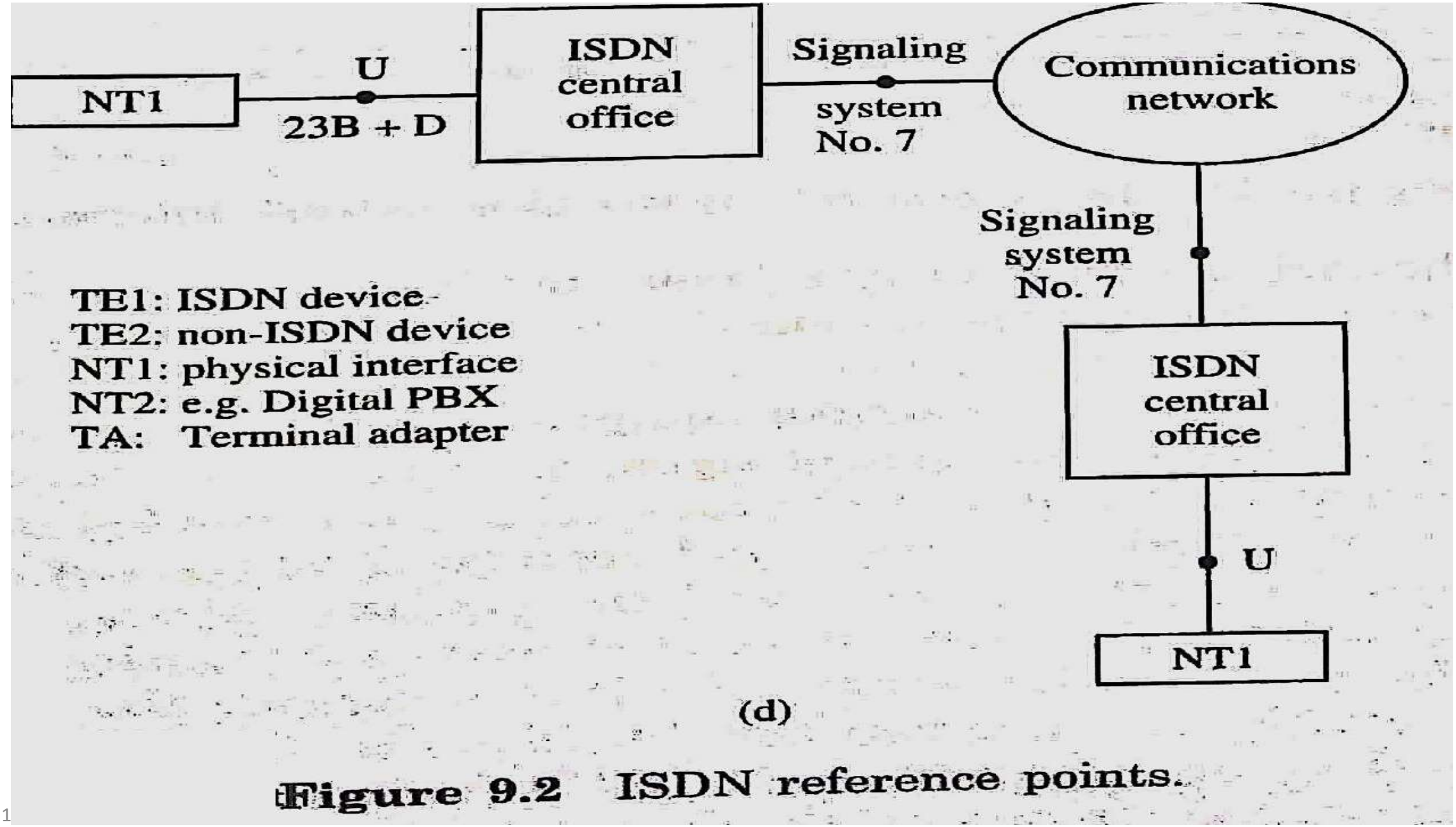


Figure 9.2 ISDN reference points.

ISDN PROTOCOLS

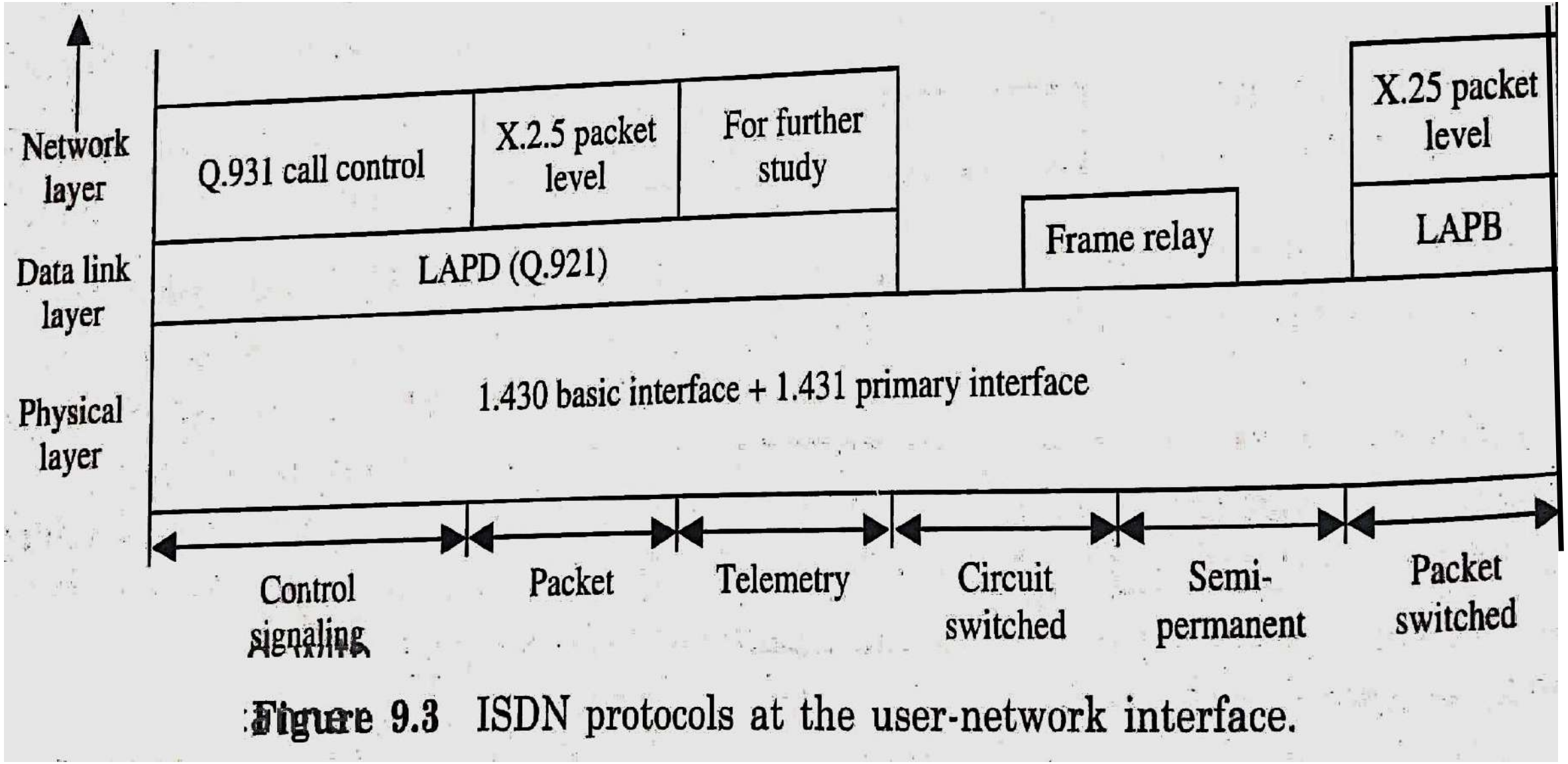


Figure 9.3 ISDN protocols at the user-network interface.

- **I.430 and , I.431 specifies the physical interface.**
- **LAPD frames that are exchanged between the subscriber equipment.**
- **Three applications**

  Control signaling

  Packet switching

  Telemetry

BROADBAND ISDN

- To use high bandwidth technologies to provide services requiring a high transfer rate.
- The data range of 600 Mbps.
- Change from metal cable to fibre-optic cable at all levels of telecommunications
- Services for videoconferencing and video telephones.
- During billing, you are charged depending on your choices.
- Unassigned channels result in wasted bandwidth.
- Uses the Asynchronous Transfer Mode.

Thank You...

ADHIPARASAKTHI COLLEGE OF ARTS AND SCIENCE

(Autonomous)

G.B. Nagar, Kalavai - 632506

Data and Communication Networks

UNIT - IV

INTERNETWORKING

- **The networking environments comprising just a single types of network.**
- **Term internetwork (or internet) to refers to composite network (e.g LAN/WAN/LAN) being used.**
- **Communication path and perform the necessary relaying and routing functions, so that data can be exchanged between devices.**
- **Two types of intermediate systems bridge and router.**

PRINCIPLES OF INTERNETWORKING

Requirements:

- **Link between networks**
- **Routing and delivery of the data**
- **Accounting service that keeps track of the usage.**
- **Services list.**

A connection-oriented Intermediate systems(IS) performs the following key functions.

- **Relaying**

  Data units arriving from one network via the network layer protocol are relayed (retransmitted) on another network

- **Routing**

  When an end-to-end logical connection consisting of a sequence of logical connections is to be set up, must make a routing decision that determine the next hop in the sequence

Internet protocol (IP) provides a connectionless service between systems.

- **A connectionless Internet facility is flexible.**
- **Services can be made highly robust (strong).**
- **It does not impose unnecessary overhead.**

ROUTING PRINCIPLES

- **To transfer packets from a sending host to the destination host, the network layer must determine the path or route that packet are to follow.**
- **Network layer provides a**

  Datagram services,

  Virtual-circuit service

- **Datagram service**

  In which case different packet between a given host-destination pair may take different routes

- **Virtual –circuit service**

  In which case all packets between a given source and destination will take same path

- **Routing algorithm find a ‘good’ path from source to destination.**
- **A ‘good’ path is one that has ‘least cost’**

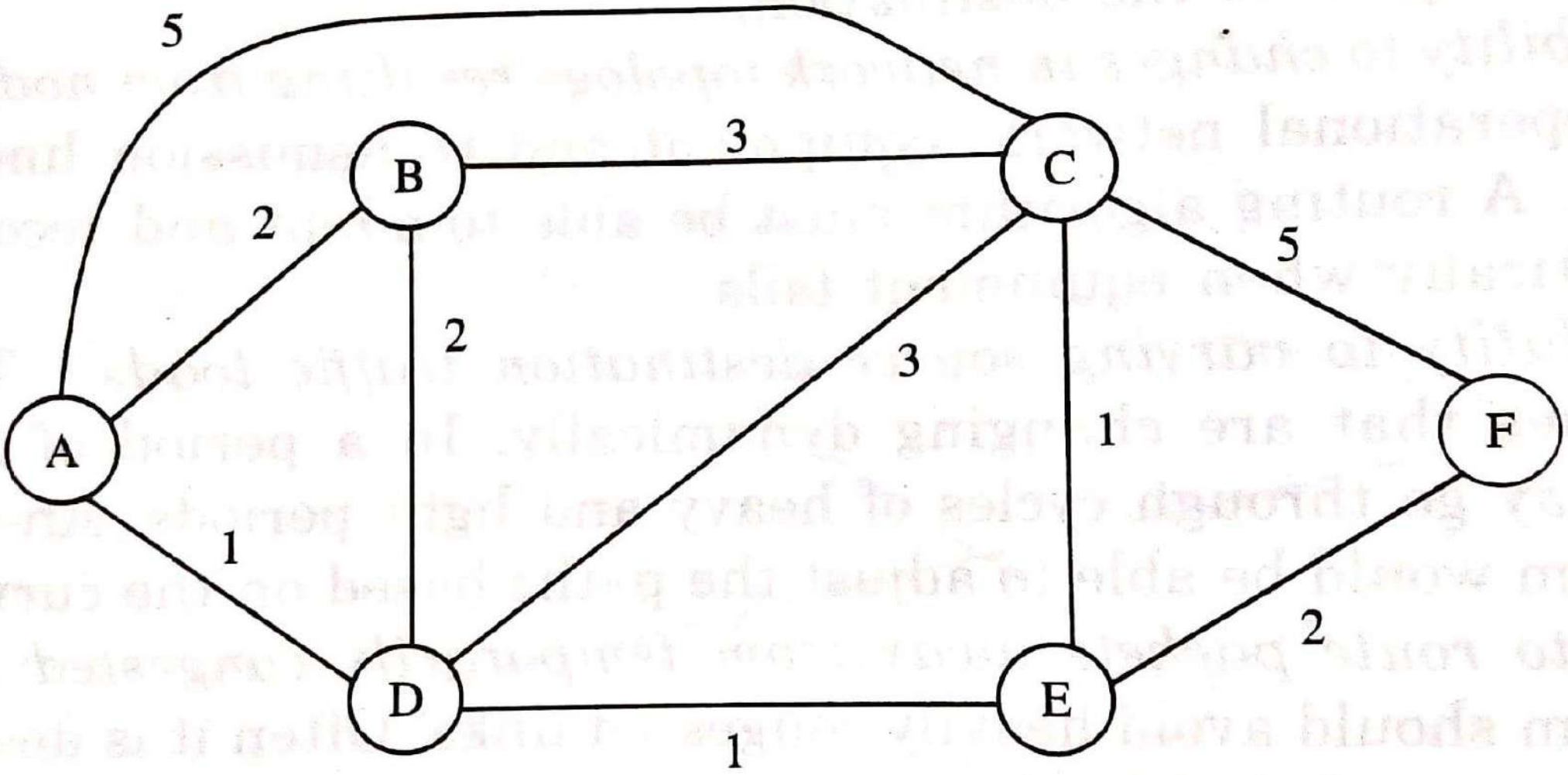


Figure 12.6 Abstract model of a network.

- **Nodes in the graph is routers – the points at which packet routing decisions are made.**
- **Lines (edges) connecting these nodes.**
- **A value representing the “cost” of sending a packet across the link.**

To finding the least-cost path from a source to a destination requires.

- **The first link in the path is connected to the source**
- **The last link in the path is connected to the destination**
- **For all i, the i, and i, - the first link in the path are connected to the same node.**
- **For the least-cost path, the sum of the cost of the links on the path is the minimum over all possible paths between the source and destination.**

The least –cost path between node A (source) and C (destination) is along the path _____

Goal:

- **Rapid and accurate delivery of packets**
- **Adaptability to changes in network topology resulting from node or link failures**
- **Adaptability to varying source destination traffic loads**
- **Ability to route packets away from temporarily congested links**
- **Ability to determine the connectivity of the network**
- **Ability to avoid rooting loops**
- **Low overhead**

Types :

- **Centralized Routing**
- **Distributed Routing**
- **Static Routing**
- **Adaptive Routing**
- **Distance-vector Routing**
- **Link-state (SPF) Routing**
- **Dijikstra Algorithm**

Centralized Routing

- **Centralized routing means that all interconnection information is generated and maintained at a single central location.**
- **Each node may define its own routing table.**
- **Maintain routing information as a matrix (row and column)**
- **A row corresponds to a source node and a column to a destination node.**

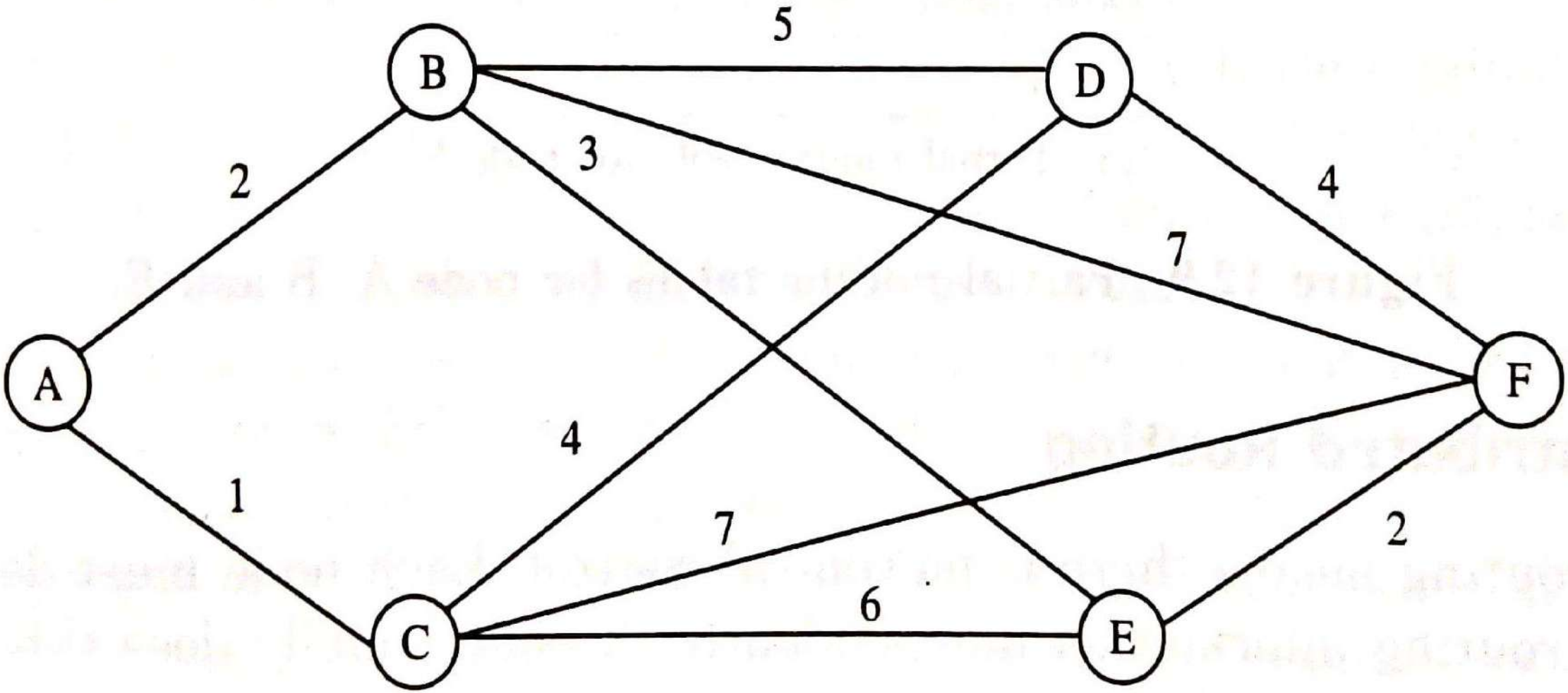


Figure 12.8 Network and associated connection cost.

Source Node	A	B	C	D	E	F
A	–	B	C	C	B	B
B	A	–	A	D	E	E
C	A	A	–	D	E	F
D	C	B	C	–	F	F
E	B	B	C	F	–	F
F	E	E	C	D	E	–

Figure 12.7 Routing matrix for the network in Figure 12.8.

Source	Destination	Next	Cost
A	B	B	2
A	C	C	1
A	D	C	5
A	E	B	5
A	F	E	7

Partial routing table for node A

Source	Destination	Next	Cost
B	A	A	2
B	C	A	3
B	D	D	5
B	E	E	3
B	F	E	5

Partial routing table for node ‘B’

Source	Destination	Next	Cost
C	A	A	1
C	B	A	3
C	D	D	4
C	E	E	6
c	F	F	7

Partial routing table for node C

Source	Destination	Next	Cost
D	A	C	5
D	B	B	5
D	C	C	4
D	E	F	6
D	F	F	4

Partial routing table for node D

Source	Destination	Next	Cost
E	A	B	5
E	B	B	3
E	C	C	6
E	D	F	6
E	F	F	2

Partial routing table for node E

Source	Destination	Next	Cost
F	A	B	7
F	B	E	5
F	C	C	7
F	D	D	4
F	E	E	2

Partial routing table for node F

Distributed Routing

- **Distributed routing is no central control.**
- **Each node must determine and maintain its routing information independently.**
- **A node by knowing who its neighbour to send data to specific destinations.**
- **One node's knowledge of the entire network is very limited.**

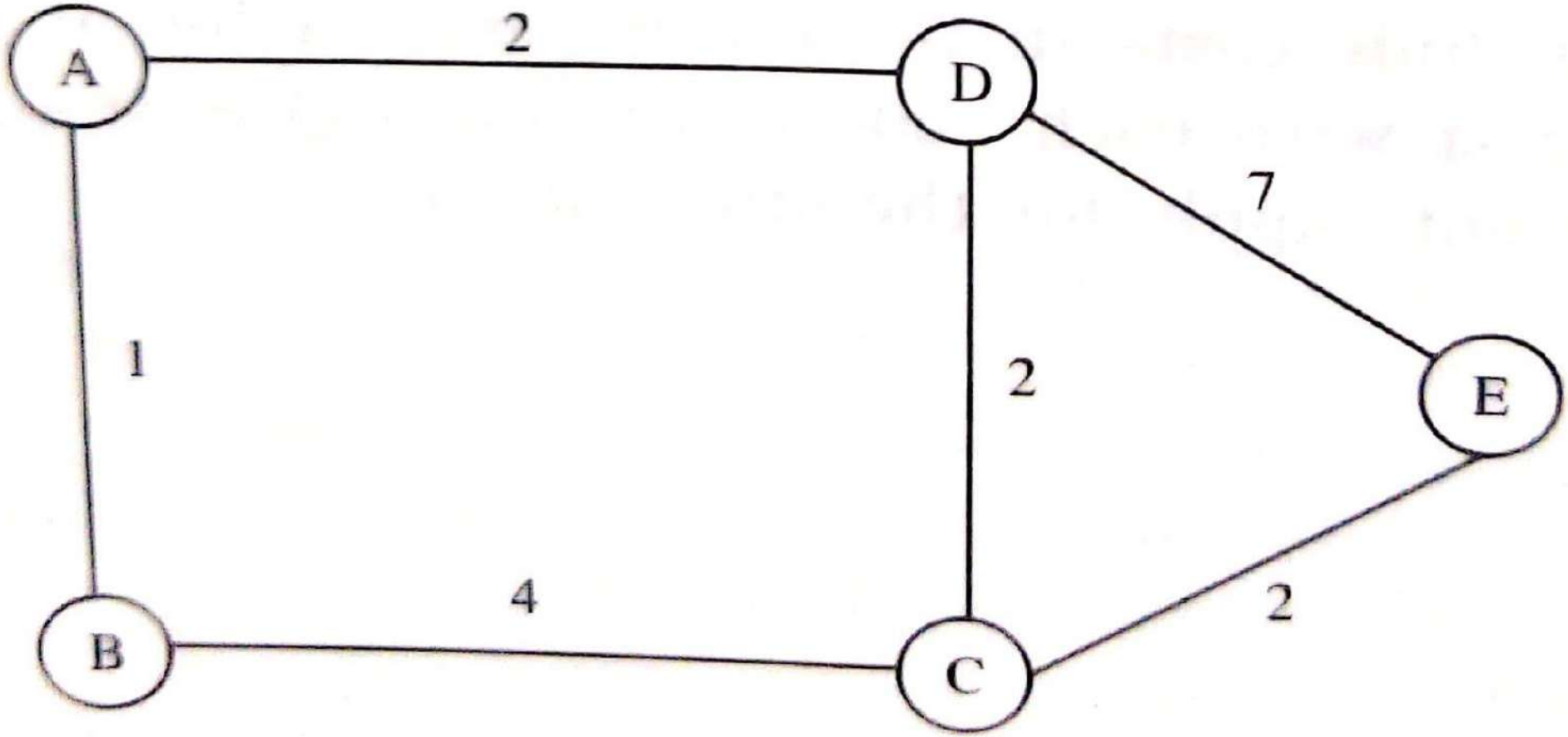


Figure 12.10 Network examples for distributed routing.

Example

- **Node 'A' initially knows only that it can send something to B (Cost = 1).**
- **It has no knowledge whatsoever that nodes C and E even exist.**
- **Periodically exchanging information about neighbouring nodes, each one learns the identity of others in the network and the cheapest paths to them**

Static Routing:

- **Static routing means that once a node determine its routing table, the node does not change it.**
- **Route or routes between two nodes on the network are fixed.**
- **Messages must always be sent on the predefined routes.**

Adaptive Routing

- **Dynamic routing, sometimes called adaptive routing, to chooses the best path for routing a packet to its destination.**
- **The node can adapt to changing network traffic volumes, error rates, circuit outage or other conditions.**
- **An adaptive routing strategy allows a network node to respond to such changes and update its routing tables accordingly**

Distance Vector Routing

- **Exchange route information.**
- **A router will advertise a route as a vector (Destination) of direction and distance.**
- **The term distance-vector comes from the information sent in the periodic messages.**
- **A message contains a list of pairs (V, D) where V identifies a destination and D is the distance to the destination.**
- **When a route changes the information circulates slowly form one route to another.**

Link – State Routing

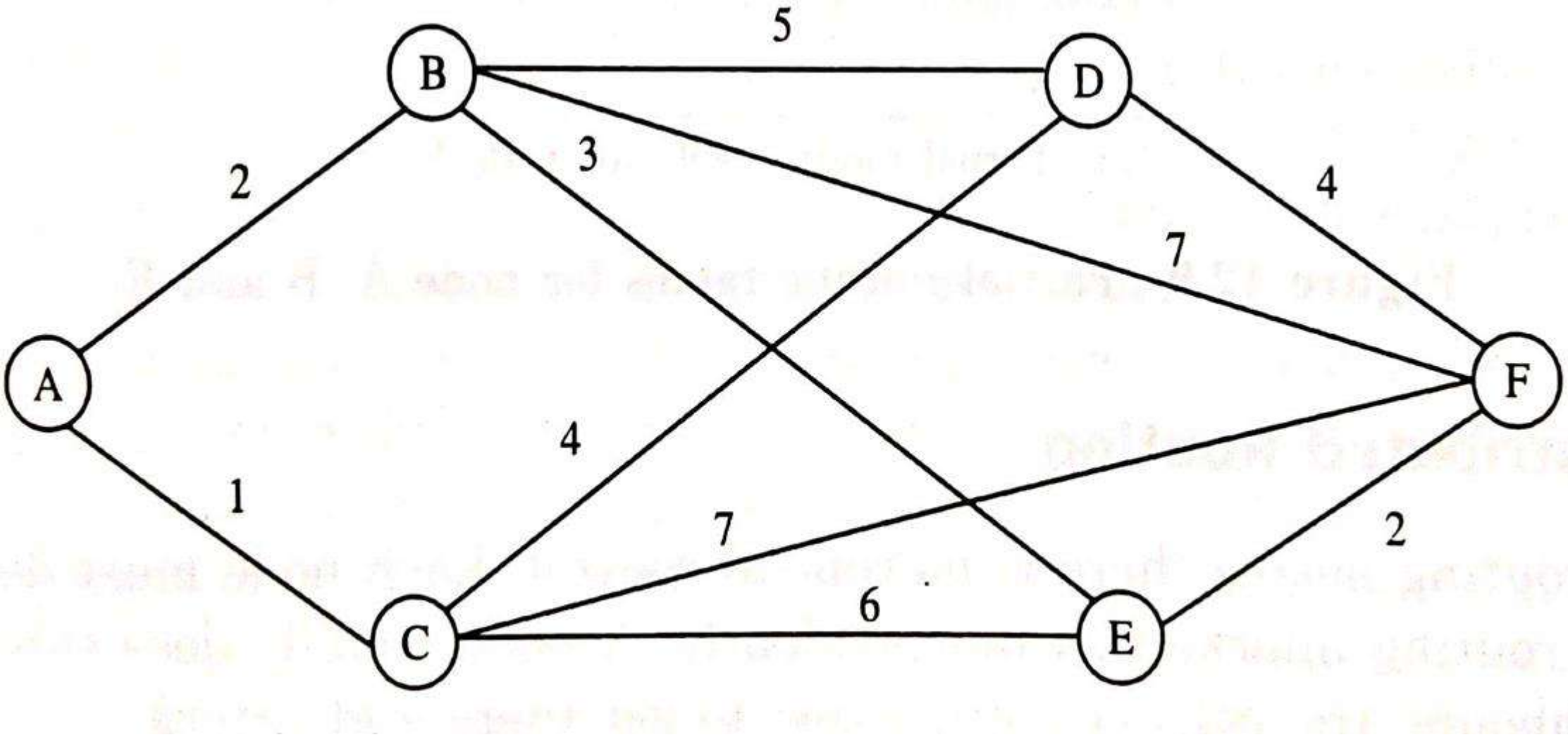
- **Link –static routing maintain complete road map of the network in each router.**
- **Routers running a link state routing protocol originates information about the router, its directly connected links.**
- **Each router will independently calculate its own best paths to reach the destination networks.**
- **Link status messages arrives, a router uses the information to update its map of the internet.**
- **Whenever link status changes, the router re-computes routes.**

Dijkstra Algorithm

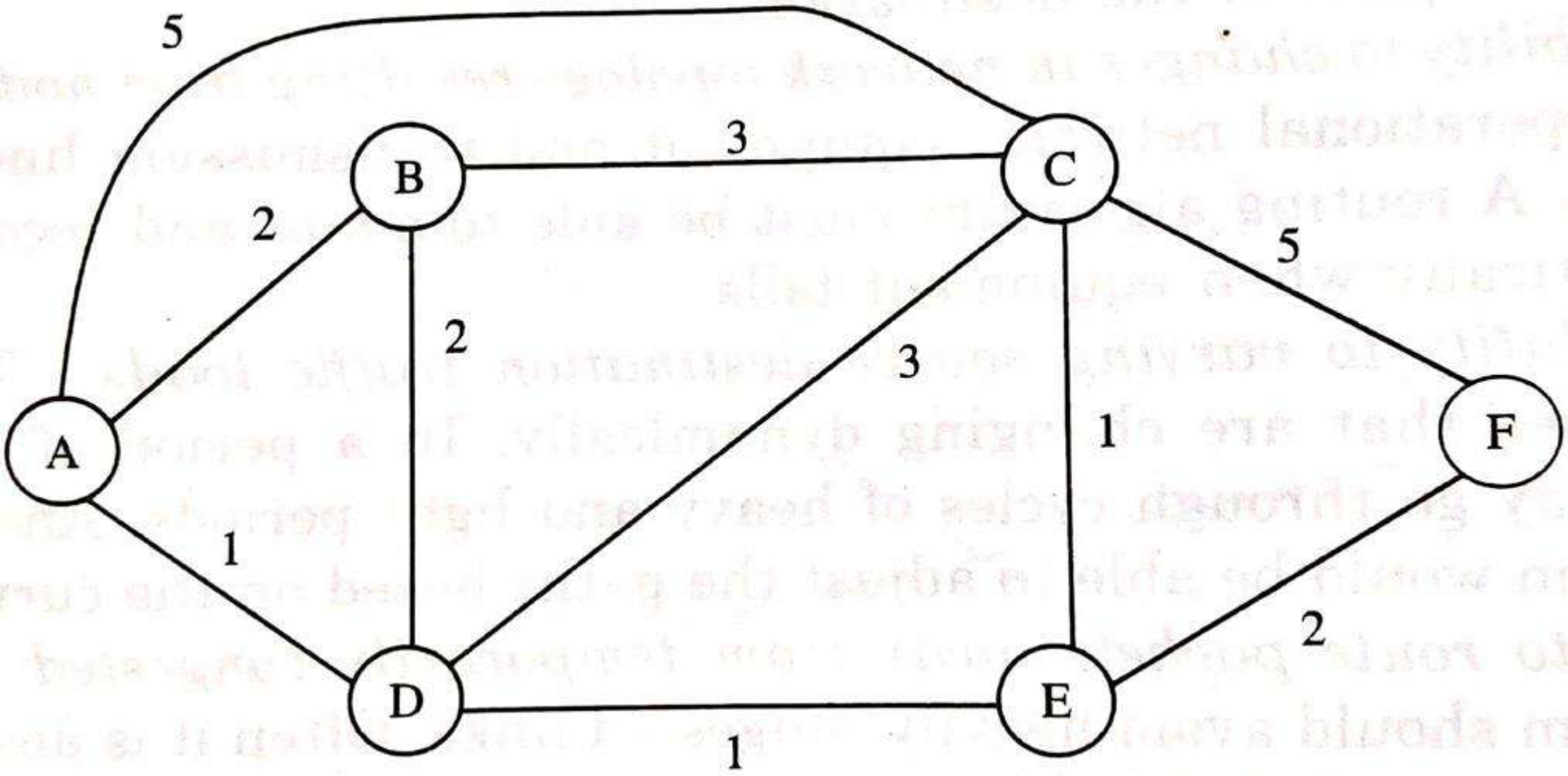
- **Dijkstra algorithm, sometimes called the shortest path algorithm.**
- **To determine the cheapest route to each network node.**

Dijkstra's Algorithm Steps:

1. **The algorithm begins to build the tree by identifying its root. Then attach all nodes that can be reached from the root.**
2. **Identifies the lowest cumulative cost**
3. **Examines the database and identifies every node that can be reached from its chosen nodes.**
4. **The last two steps are repeated until every node in the network has become a permanent part of the tree**



To find the all possible paths and conclude shortest path from A to F_____



To find the all possible paths and conclude shortest path from A to F_____

INTERNETWORK PROTOCOL (IP)

- **The protocol that defines the unreliable, connectionless delivery mechanism is called the Internet Protocol.**
- **Three definitions**
    1. **The IP protocol defines the basic unit of data transfer used throughout a TCP/IP internet.**

       Thus it specifies the exact format of all data.
    2. **IP software performs the routing function choosing a path over which data will be sent.**
    3. **Set of rules for unreliable packet delivery.**

- **The rules characterizes**
  - ✓ **How hosts and routers should process packets,**
  - ✓ **How and when error messages should be generated**
  - ✓ **The conditions under which packets can be discarded.**

- **Example : Post office letters.**

Include

- **IP services**
- **Datagram**
- **Protocol functions**
- **Internet Control Message Protocol**

IP services

- **Expressed in terms of primitives and parameters**
- **Primitives specifies the function to be performed**
- **Parameters are used to pass data and control information**

Send {
Source address
Destination address
Protocol
Type of service indicators
Identification
Don't fragment identifier
Time to live
Data length
Option data
Data
}

Deliver {
Source address
Destination address
Protocol
Type of service indicators
Data length
Option data
Data
}

Figure 12.13 IP service primitives and parameters.

- **Send primitive is used to request transmission of a data unit**
- **The deliver primitive is used to IP to notify a user of the arrival of a data unit.**
- **Parameter to request a particular quality of service.**
- **Services are:**

  Precedence : Provide better management

  Reliability : To minimize the possibility of datagram lost

  Delay : Minimize the delay

  Throughput : Maximize the throughput

Datagram

- **The format of an IP data unit is known as a data gram.**
- **Packets in the IP layer are called datagrams.**

← 4 bits →	← 4 bits →	← 8 bits →	← 16 bists →
Version	HLEN	Service type	Total length
Identification (16 bits)		Flags (3 bits)	Frames offset (13 bits)
Time to live		Protocol	Header checksum
Source IP address			
Destination IP address			
Option			

Figure 12.14 IPv4 Header.

Version:

The current version is 4 (IPv4) with binary value is _____

Header length (HLEN):

The maximum length of 60 bytes

Service type:

Specifies consistency, priority, delay & throughput

Total length: **16 Bits**

Identification:

Used in fragmentation of 16 bits, source & destination address

Flags :

Deal with fragmentation (the datagram can or cannot fragmented ; can be first, middle or last fragmented)

Time to live:

Specifies how long, a datagram is allowed to remain in the internet

Protocol:

To receive the data field at the destination

Header checksum:

16 bits field used to check the integrity of the header.

Source address:

Field is 32 bit internet access. Identify the original source

Destination address:

Field is 32 bit internet access. Identify final receiver

Options:

It can carry fields that control routing, timing, management and alignment

Data (variable): 8 bits length.

Protocol Functions:

1. Fragmentation and reassembly:

The transfer of user messages across network which support smaller packet size than the user data

2. Routing

IP in each source host must know the location of the internet gateway.

Gateway must know the route to be followed to reach other networks

3. Error reporting

3. Error reporting

IP may discard some datagrams with reporting such occurrences

Internet Control Message protocol (ICMP)

- **ICMP message travel across the internet in the data portion of IP datagram.**
- **ICMP main functions:**
  - ✓ **Error reporting**
  - ✓ **Reachability testing**
  - ✓ **Congestion control**

- ✓ **Route change information**
- ✓ **Performance measuring**
- ✓ **Subnet addressing**

Table 12.2 ICMP Message Types and Their Use

Function	*ICMP message(s)*	*Use*
Error reporting	Destination Unreachable	A datagram has been discarded due to the reason specified in the message.
	Time exceeded	Time to live parameter in a datagram expired and hence discarded.
	Parameter error	A parameter in the header of a datagram is unrecognizable.
Reachability testing	Echo request/ reply	Checks the reachability of a specified host or gateway.
Congestion control	Source quench	Requests a host to reduce the rate at which datagrams are sent.

Route exchange	Redirect	Used by a gateway to inform a host attached to one of its networks to use an alternative gateway on the same network for forwarding datagrams to a specific destination.
Performance measuring	Timestamp request/reply	Determines the transit delay between two hosts.
Subnet addressing	Address mask request/reply	Used by a host to determine the address mask associated with a subnet.

Datagram is discarded reasons:

- **Destination network unreachable**
- **Destination host unreachable**
- **Specified protocol not present at destination**
- **Fragmentation needed but don't fragment flag set in datagram header**
- **Communication with the destination network not allowed for administrative reasons**
- **Communication with the destination host not allowed for administrative reasons.**

Each message contains the following three time-related parameters:

- **The time the datagram was sent by the source**
- **The time the datagram was received by the destination**
- **The time the datagram was returned by the destination**

TRANSPORT SERVICE

Transport Protocols:

- **Defines what one station can say to another on behalf of the user.**
- **Focus on how information is exchanged between two entities.**
- **Functions:**
    1. **Connection management**
    2. **Flow control**
    3. **Error detection**

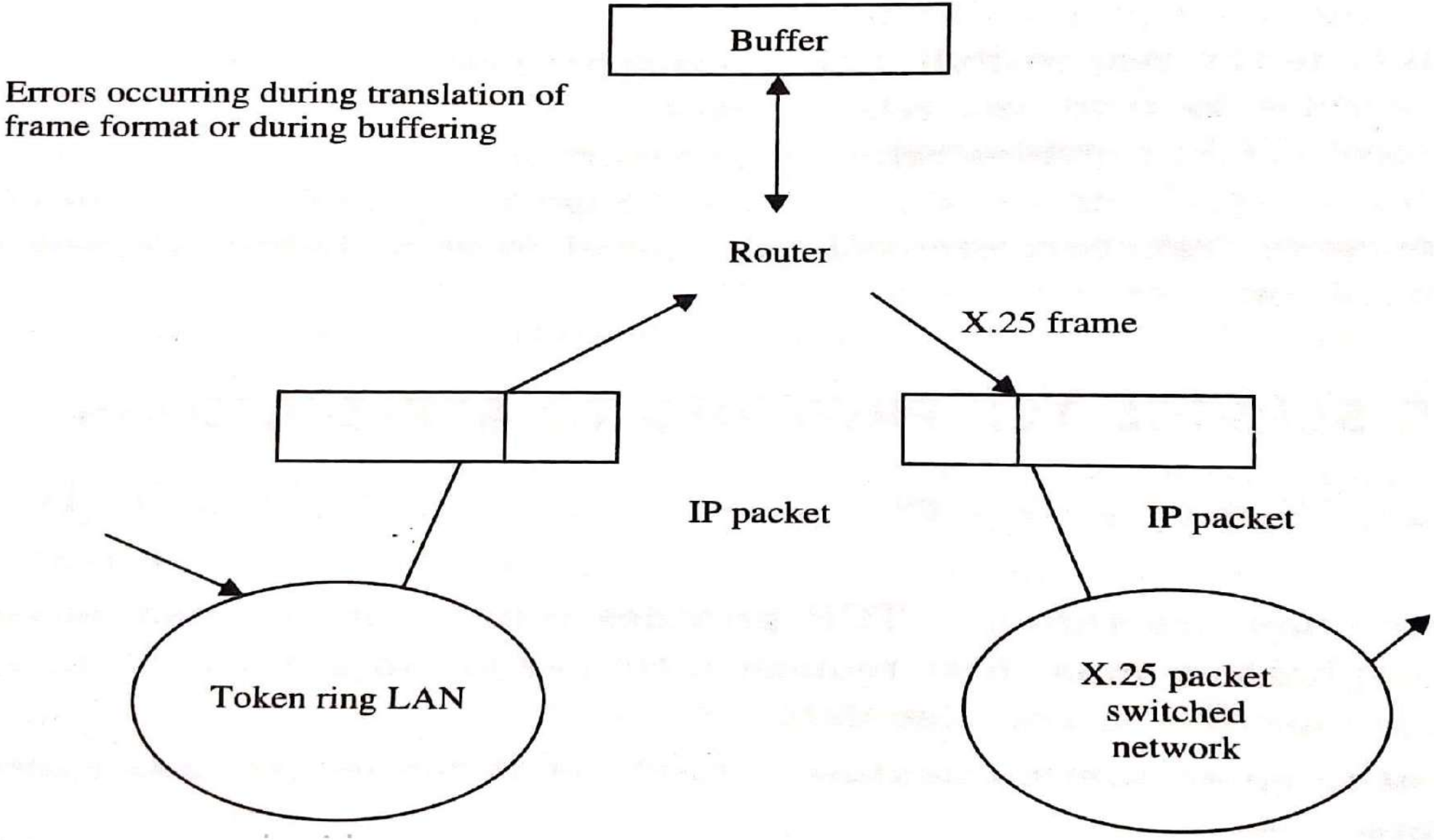


Figure 13.2 Error undetected by lower-layer detection techniques.

- **A transport protocol must provide reliable communication between the end users.**
- **Provide acknowledgments and timers to make sure all of a user's data is send and received.**

TRANSMISSION CONTRO PROTOCOL (TCP)

- **TCP provides a connection-oriented user-to-user byte stream service.**
- **Provides a logical connection between two sites and its capable of transmitting a sequence of bytes between them.**
- **TCP operation is examine the TCP header format.**

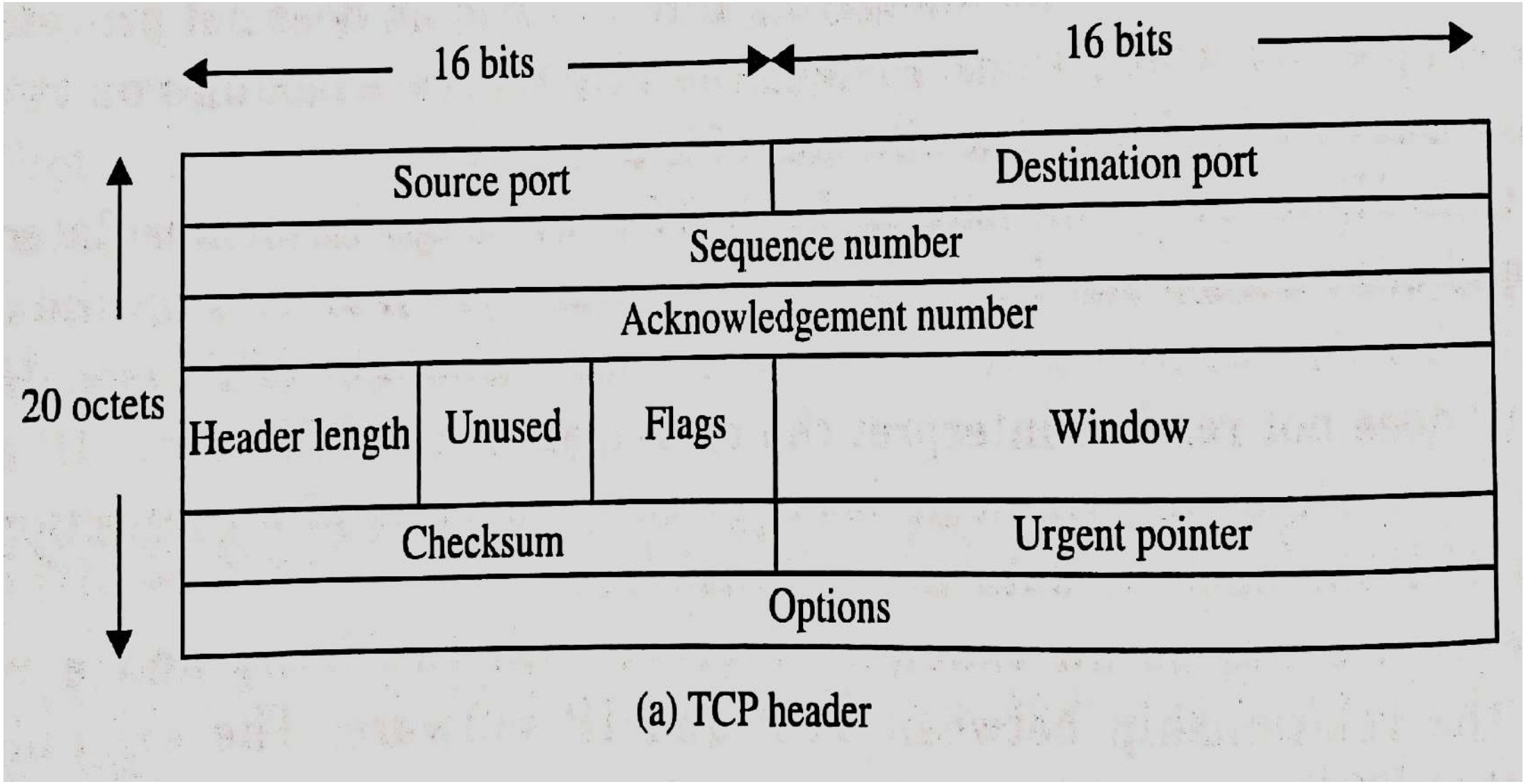


Figure : TCP Header

The fields are

Source port (16 bits) :

Source TCP user specifies the application sending the segment

Destination port (16 bits) :

Destination TCP user identifies the application to which the segment is sent

Sequence number (32 bits) :

TCP sends is numbered. (e.g receipt number)

To Acknowledgement number (32 bits) :

The piggybacked acknowledgement.

TCP entity expected receive

Header Length (4bits) :

Specifies the size of the TCP header as a multiple of four bytes. Number of 32 bits words.

Reserved (6 bits) :

Reserved for further use

Flags (6 bits) : These are

URG : Urgent pointer

ACK : Acknowledgement

PSH : Push function

RST : Reset of the connection

SYN : Synchronize the sequence number

FIN : No more data from sender

Window (16 bits)

Flow control credit allocation.

The sender is willing to accept.

Checksum (16 bits):

Used for error detection

Urgent pointer :

This allows the receiver to know how much urgent data is coming.

Option :

Specifies optional features.

The PUSH and URGENT flags implement two TCP services:

(i) Data stream push :

- **TCP decides when sufficient data have accumulated to transmission**
- **The TCP user can require TCP to transmit all outstanding data up to and including that labeled with PUSH flag.**
- **TCP will deliver these data to the user in the same manner**

(ii) Urgent data signaling:

- This provides a means of informing the destination TCP user that significant or Urgent data are in the upcoming data stream.
- Destination user to determine approximate action.

Include

- **TCP implementation Policy options**
- **How does TCP achieve Reliability?**

TCP implementation Policy Options:

The design areas for which options are specified are the following:

- **Send policy**
- **Delivery policy**
- **Accept policy**
- **Retransmit policy**
- **Acknowledge policy**

Send policy

- As data are provided by the user, they are buffered in the transmit buffer.
- TCP may construct a segment for each batch of data or it may wait until a certain amount of data accumulates before constructing and sending a segment.
- The actual policy will depend on performance considerations.
- If transmissions are frequent and small, then the system provides quick response.

Delivery policy

- **Delivery data as such in order segment is received or it may buffer data from a no.of segments in receive buffer delivery.**
- **The actual policy will depend on performance considerations.**
- **If delivery are infrequent and large, the user may not receive data as promptly as desired.**

Accept Policy

- **Data segment arrive in order over a TCP connection, TCP places the data in a receive buffer for delivery to the user.**
- **Segments to arrive out of order, In such a case, the receiving TCP entity has two options:**

(i) In- Order :

Accept only segments that arrive in order, any segment that arrives out of order is discarded

(ii) *In-window:*

Accept all segments that are within the receive window

Retransmit Policy

- **TCP maintains a queue of segments that have been sent, but not yet acknowledged.**
- **The TCP specification states that TCP will retransmit a segment if it fails to receive an acknowledgement within a given time.**

Retransmission strategies:

(i) First-only

(ii) Batch

(iii) Individual

- **Maintain one retransmission for the entire queue.**
- **If an acknowledgement is received, remove the approximate segment or segments from the queue and reset the timer**
- **If the timer expires, retransmit the segment at the front of the queue and reset the timer.**

Acknowledge policy

- **When a data segment arrives that is in sequence, the receiving TCP entity has two options concerning the timing of acknowledgment**

(i) Immediate :

When data are accepted, immediately transmit acknowledgement number

(i) Cumulative:

When data are accepted, record the need for acknowledgment

How does TCP achieve reliability?

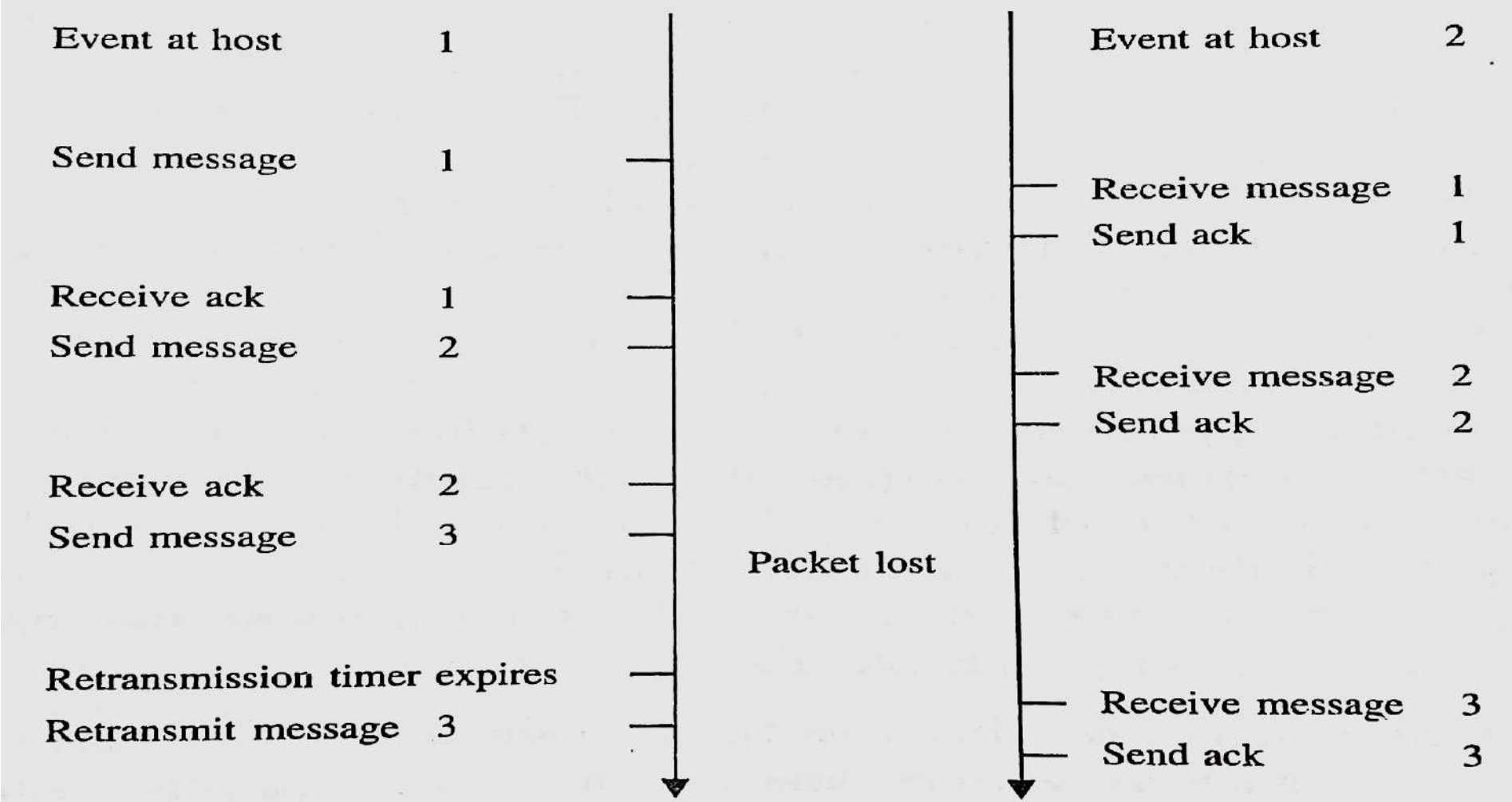


Figure 13.5 Example of retransmission.

Thank You...

ADHIPARASAKTHI COLLEGE OF ARTS AND SCIENCE

(Autonomous)

G.B. Nagar, Kalavai - 632506

Data and Communication Networks

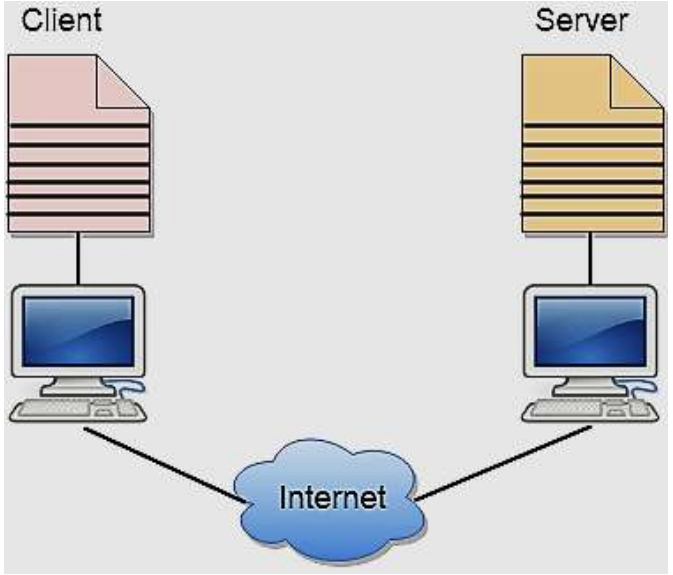
UNIT - V

NETWORK APPLICATIONS

- **Network applications include the classic text-based applications that became popular in the 1980s such as remote access to computers, e-mail, file transfer, newsgroups and chat.**
- **The web is a network applications, allows users to obtain "documents" from web servers on demand.**
- **The web applications consists of documents format, web browsers, web servers, protocols.**

CLIENT – SERVER MODEL

- **The model arranging for one application, to wait passively for another application to intimate communication is called client- server model.**
- **The application that actively initiates contact is called a *client*, while the application that passively waits for contact is called a *server*.**



- **Client running on the local machine.**
- **Server running on the remote machine.**
- **A server can provide a service for any client, not just a particular client, relationship is many-to-one.**
- **Many clients can use the services of one server.**
- **Client program, which request a service, should run only when it is needed. The server program, which provides a service, should run all of the time because it does not know when its service is needed.**

Characteristics of Clients and Servers

In general, client :

- **Client temporarily when remote access is needed, perform locally**
- **Invoked directly by a user, and executes only for one session.**
- **Runs locally on a user's personal computer**
- **Actively initiates contact with a server**
- **Can access multiple services as needed, but actively contacts one remote server at a time**
- **Does not require special hardware or a sophisticated O.S**

In general, Server :

- **Special purpose, privileged program to dedicated to providing one server, but can handle multiple remote clients at the same time**
- **Invoke automatically when a system boots, and continues to execute through many sessions.**
- **Runs on shared computer**
- **Waits passively for contact from arbitrary remote clients.**
- **Offer a single service**
- **Requires powerful hardware and sophisticated system,**

Complex Client-Server Interactions

- **A client application is not restricted to accessing a single service.**
- **A client application is not restricted to accessing a single server**
- **A server is not restricted from performing further client-server interactions**

DOMAIN NAME SYSTEM (DNS)

- **The naming scheme used in the Internet is called the Domain Name System (DNS).**
- **Example : www.apcas.in**
- **Domain names are hierarchical with the most important part of the name on the right.**

Table 14.1 Most Significant Segment of a Domain Name

Domain name	*Assigned to*
com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military group
net	Major network support centre
org	Organization other than those above
arpa	Temporary ARPA domain still used
int	International organization
country code	A country

The proposed names include:

- **firm**
- **store**
- **web**
- **arts**
- **rec**
- **info**
- **nom**

Country domains

- **Use two-character country abbreviation**
- **Example :**

  ca.us (California, a state of the United States of America)

  ac.uk (Academic & United Kingdom)

  ac.in (Academic & India)

The DNS Client- Server Model

- **DNS is autonomy – the system is designed to allow each organization to assign names to computers or to change those names without informing a central authority.**
- **Example : Bsnl.com, ibm.com**
- **Most organizations that have an Internet connection run a domain name server.**
- **The client places the names to be translated in a DNS request message and sends the request to a DNS server.**

TELNET

- **TELNET stands for Terminal Network.**
- **Enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.**

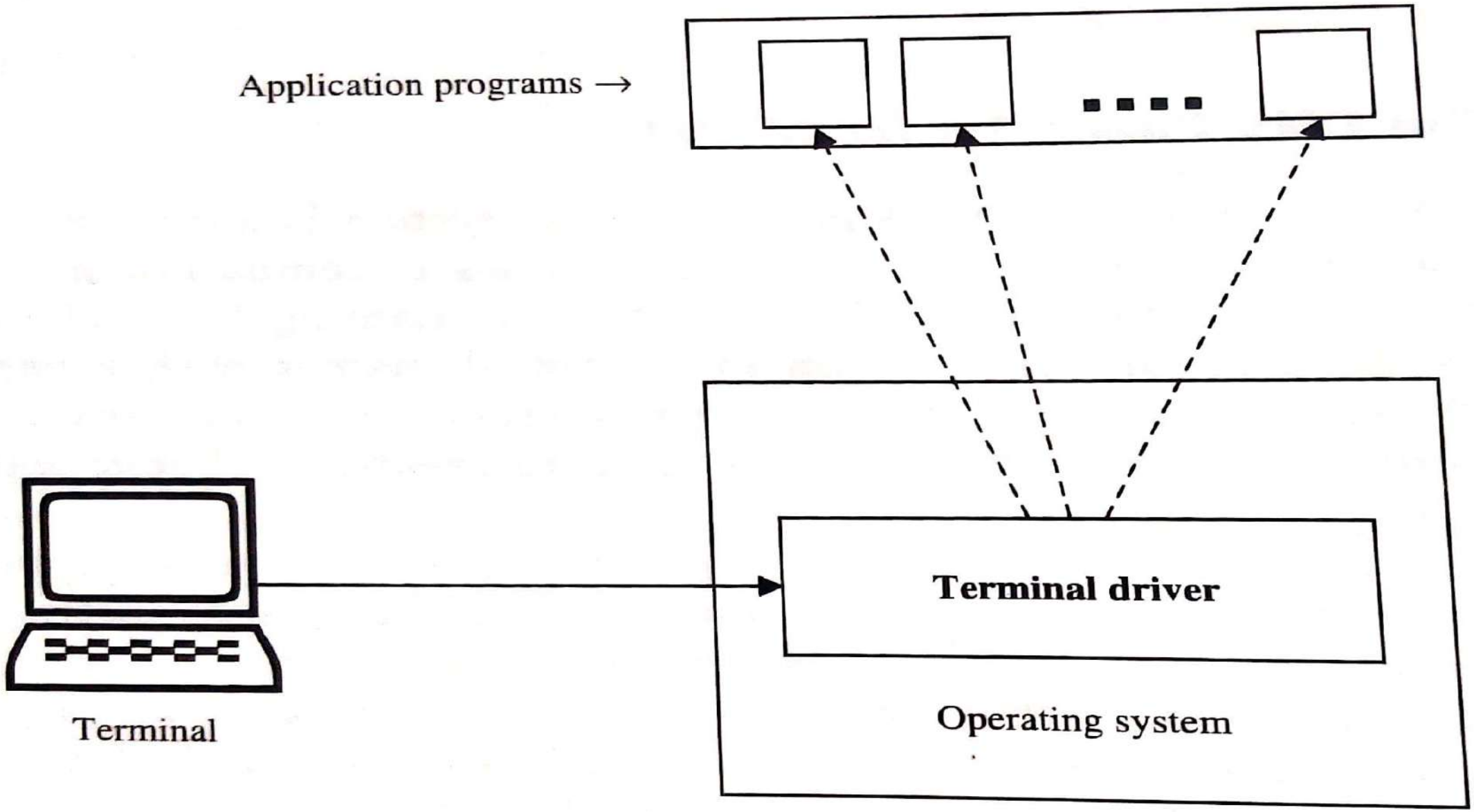


Figure 14.3 Local login.

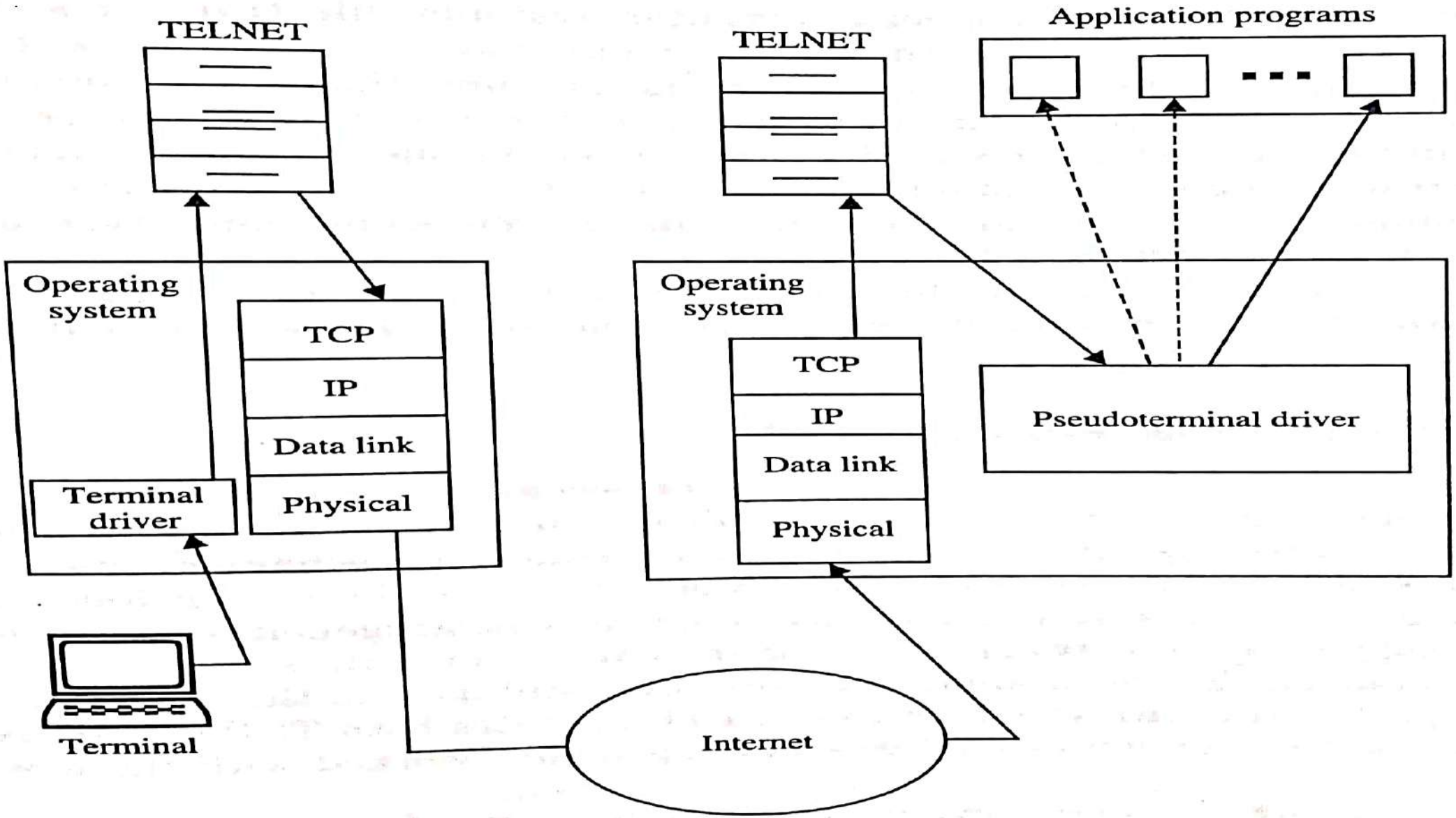


Figure 14.4 Remote login.

FILE TRANSFER AND REMOTE FILE ACCESS

- **Programmers wrote code transfer a complete file from one computer to another.**
- **File transfer software must accommodate in file representations, type of information and file protection mechanism.**
- **Include**

  File Transfer Protocol

  Client-server Integration in FTP

  Trivial File Transfer Protocol (TFTP)

File Transfer Protocol

- **FTP permits transfer of an arbitrary file, that allows file to have ownership and access restrictions.**
- **Used to transfer a copy of a file between pair of computers**
- **FTP client that establishes communication with a specified server to transfer files.**
- **Completely hides the FTP interface from the user.**
- **To establish a control connection to a remote computer before files can be transferred.**
- **To obtain authorization, a user must supply a login and password**

Client – Server Interaction in FTP

- **FTP uses a control connection only to send commands and receive responses.**
- **Client and the Server establish a separate data connection for each file transfer, use it to send one file, and then close the connection.**
- **To avoid conflict between the control and data connections.**
- **Once the transfer completes, the client and the server close the data connection and continue to use the control connections.**

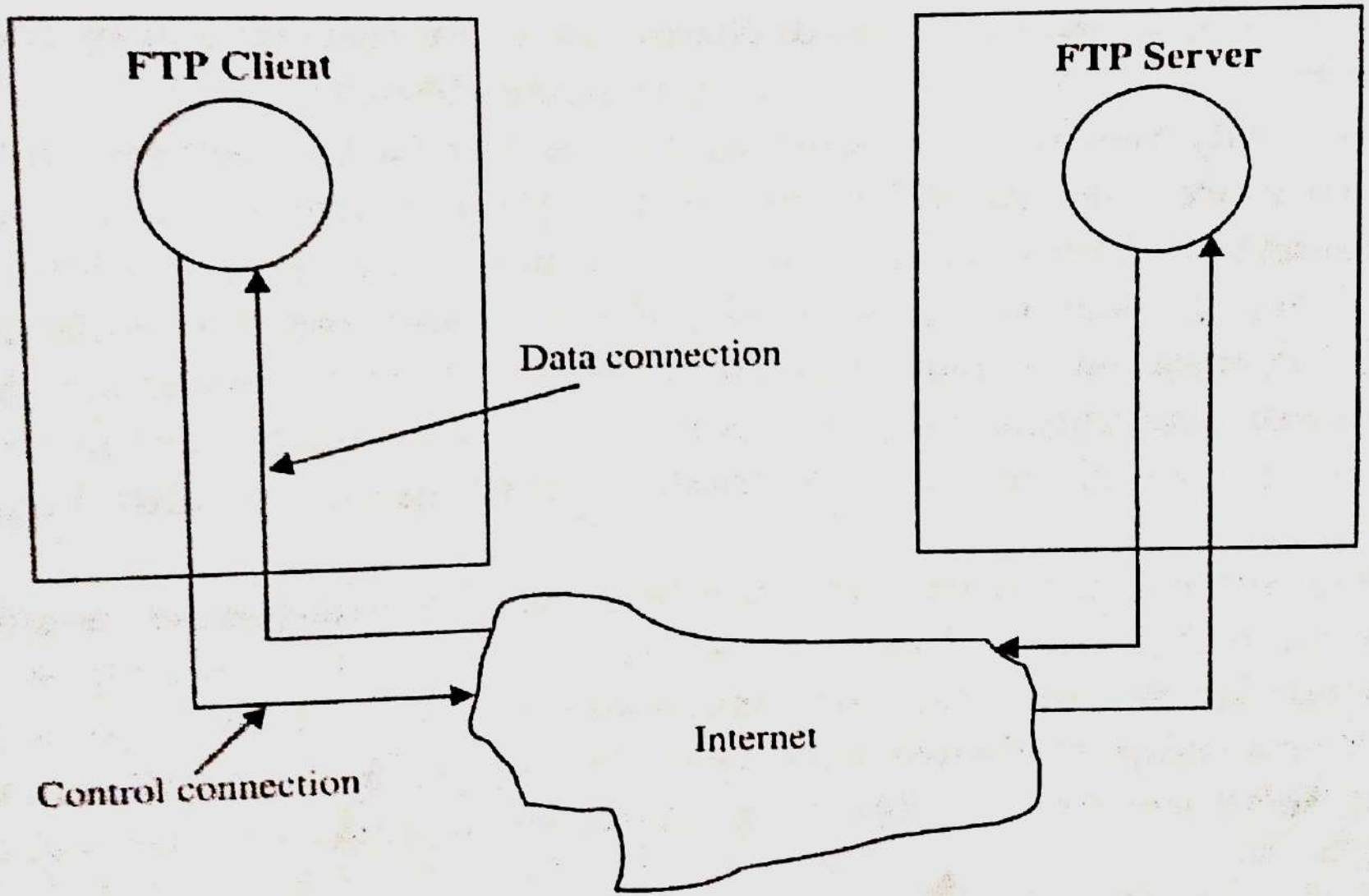


Figure 14.5 TCP connections between FTP client and server during a file transfer.

Trivial File Transfer Protocol (TFTP)

- **The Internet protocol include a second file transfer server known as TFTP.**
- **The communication between TFTP client and server uses User Datagram Protocol (UDP) instead of TCP.**
- **TFTP supports only file transfer, does not have a large set of commands.**
- **TFTP does not permit a user to list the contents of a discovery**
- **Interrogate the server to determine the names of files that are available.**
- **TFTP does not have authorization**

- **A client does not send a login name or password ; a file can be transferred only if the file permission allows global access.**
- **TFTP is less powerful than FTP.**
- **TFTP requires less memory than the code for FTP.**
- **All the device needs is a network connection and a small amount of ROM.**
- **Flexibility and reduces cost, because a separate server exists for each network.**
- **Cost is reduced because software can release a new version of software for the device without changing the hardware on installing a new ROM.**

NETWORK MANAGEMENT

- **Defined as OAMP (Operation, Administration, Maintenance and Provisioning)**
- **Include**

  GOAL OF NETWORK MANAGEMENT

  NETWORK MANAGEMENT STANDARDS

  NETWORK MANAGEMENT MODELS

  INFRASTRUCTURE FOR NETWORK MANAGEMENT

  SIMPLE NETWORK MANAGEMENT PROTOCOLS (SNMP)

  NETWORK MONITORING TOOLS

Goal of network management

- **Quality of service**
- **Establish policy**
- **Groups**

  Network provisioning

  Network operations

  Network installation and maintenance

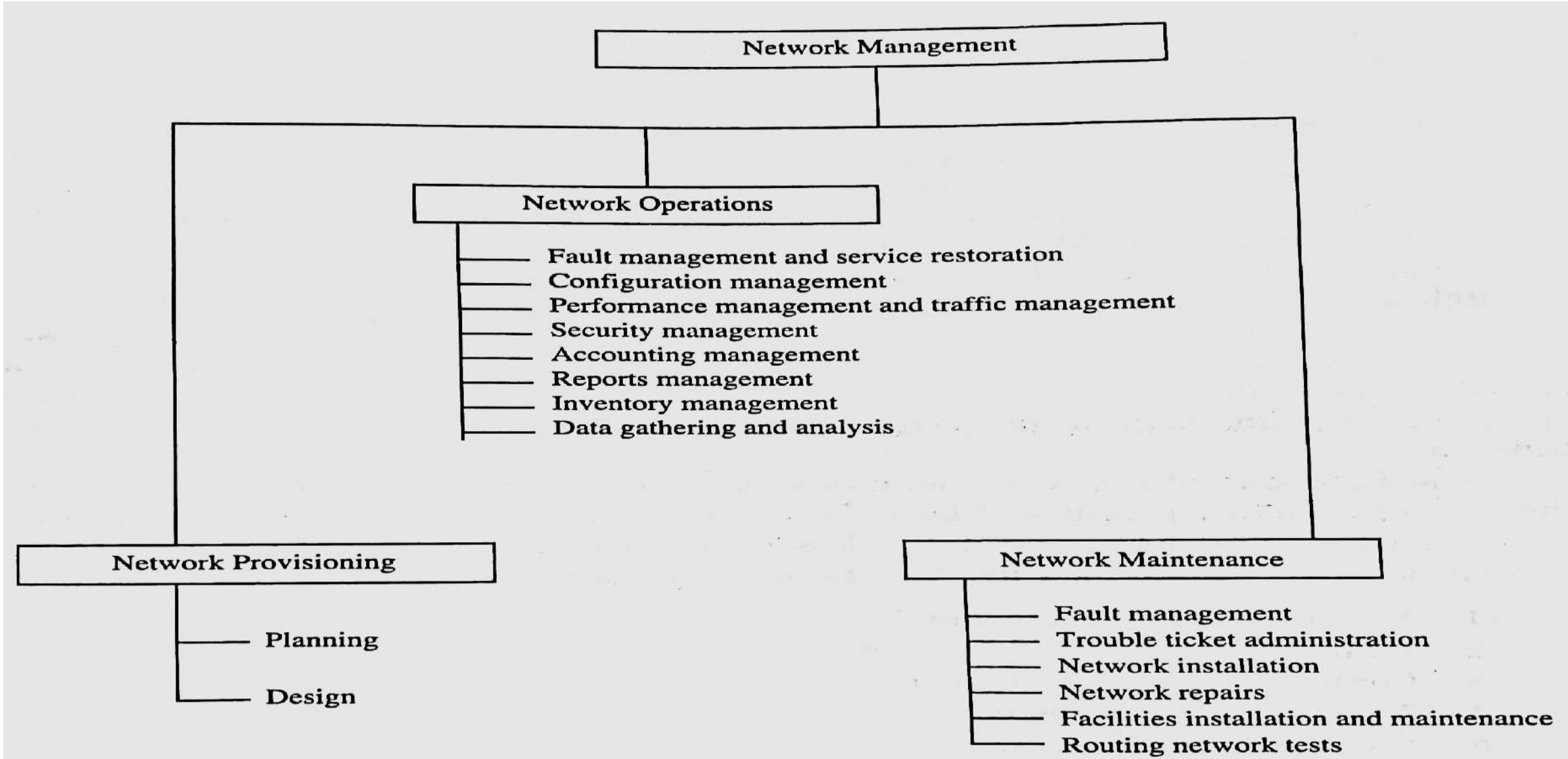


Figure 15.1 Network management functional groupings.

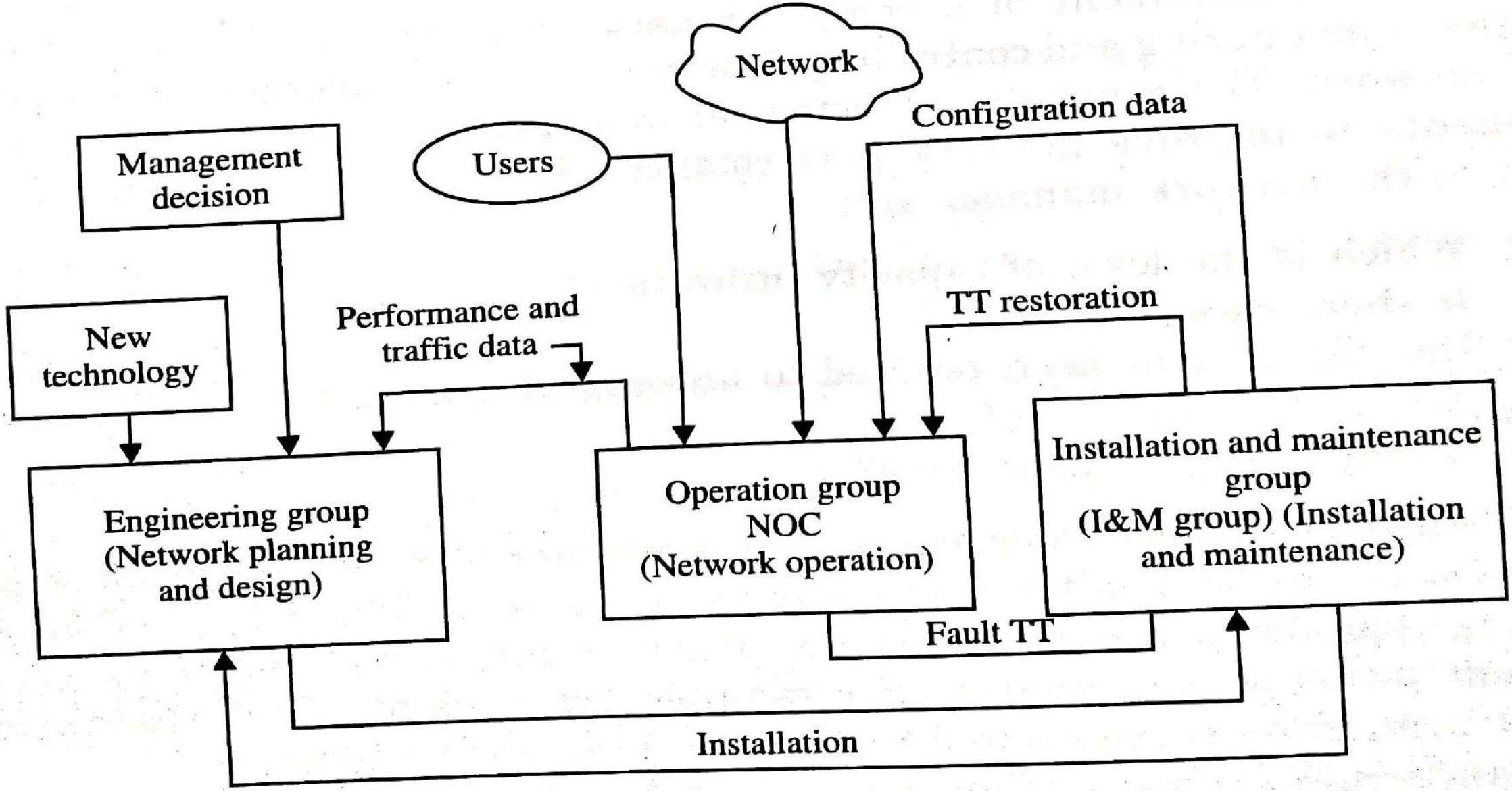


Figure 15.2 Network management functional flowchart.

Network Management Standards

- **OSI/ CMIP**

  Open System Interconnection

  Common Information Protocol

- **SNMP /Internet**

  Simple Network Management Protocol

- **TMN**

  Telecommunication Network Management

- **IEEE**

- **Web-based Management**

Network Management Models

1. **Organization model**

   The components of a network management system, their function, and their infrastructure

2. **Information model**

   The structure and organization of management information.

Network Management Models

3. **Communication model**

   Application process and Layer process.

4. **Functional model**

   User-oriented requirement of network management.

   Functional areas configuration, fault, performance, security and accounting

Infrastructure for Network Management

- **Refers to the activities, methods, procedures,**
- **Tools that pertain to the operation, admin, maintenance and provisioning**
- **Components of network architecture**

  Managing entity (Applications)

  Managing device (modem, communication links, routers)

  Network management protocols (architecture)

The functions of network management are:

- **Staffing**
- **Organizing**
- **Planning**
- **Directing**
- **Controlling**

Network documentation includes

- **Routine operating procedure**
- **Problem escalation procedure**
- **The Contact person details**
- **Vender manuals**
- **Vender contact details**
- **Software list**
- **Disaster recovery plan**

Simple Network Management Protocols (SNMP)

- **SNMP is a management protocol designed to make sure network protocols and work well.**
- **SNMP function to reduce support cost**
- **Extensible to accommodate future updates**
- **Independent of design specifications of hosts or routers.**

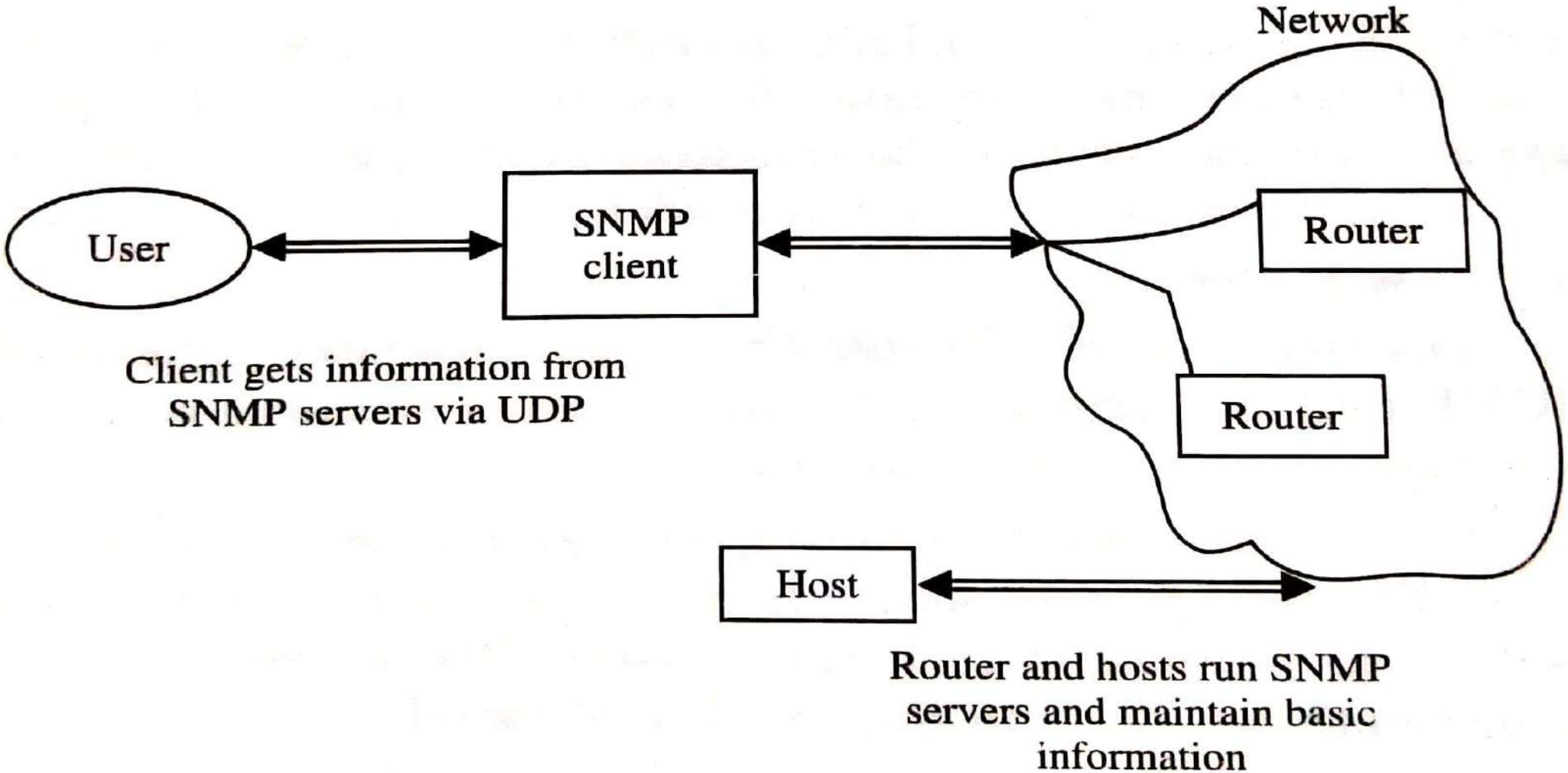


Figure 15.4 SNMP architecture.

Management Information Base (MIB)

Categories:

- **System**
- **Interface**
- **Address Translation**
- **IP**
- **ICMP (Internet Control Message Protocol)**
- **TCP**
- **UDP**
- **EGP (Exterior Gateway protocol)**

SNMP commands

Get Request

Get next request

Get response

Set request

Trap (Changes of operating environments)

- **Coldstart Trap (re-initialized with potential changes)**
- **Warmstart Trap (re-initialized with no changes)**
- **Linkdown Trap (A communication link has failed)**
- **Authentication failure trap (Authentication check)**

Network Monitoring Tools

Network administrator have to keep network up and running to perform daily duties to answer.

- **Monitor network**
- **Analyze bandwidth**
- **To see the exact flow**

Tools

Precondition of network monitoring

UP/Down monitoring

Performance monitoring

Netflow Monitoring &

Data capture tools

NETWORK SECURITY

- **Protecting information system from unplanned access.**
- **The factors that influence security policy**

  mission of the organization

  management support

  risk assessment

  level of security needed

  cost effectiveness

  personal security responsibilities and accountability

  social factors.

- **The factors that influence security mechanisms are:**

  network architecture

  security issues

  security components

  factors that make network in danger to attack

  network security mechanism

  security awareness and training

Include :

FUNDAMENTAL CONCEPTS

IDENTIFICATION AND AUTHENTICATION

ACCESS CONTROL

MODEL FOR NETWORK SECURITY

MALICIOUS SOFTWARE

SECURITY SERVICES AND CRYPTOGRAPHY

SECURITY NETWORK USING FIREWALL

INTRUSION DETECTION

NETWORK SECURITY TOOLS

FUNDAMENTAL CONCEPTS

- **Objectives**
- **Assets**
- **Threats**
- **Vulnerability**
- **Safeguards**
- **Attack**

FUNDAMENTAL CONCEPTS

Objectives

Confidentiality : Ensuring that information is not disclosed

Integrity : Preventing unauthorized

Availability : Ensuring the authorized users not denied

Legitimate (Genuine) use : Ensuring that authorized person misused

Assets

Assets are valuable resources of the organization

Categories :

- **Users,**
- **Applications,**
- **Services,**
- **Servers,**
- **Networks,**
- **Documentation,**
- **Goodwill,**
- **Reputations and Manpower skills**

Threats

Threat (warning) is an future action by a person that attitudes some danger to an asset.

- **Information leakage**
- **Integrity (Truth) violation**
- **Denial of service (Against the usual work)**
- **Illegitimate use**

The above threats can be realized in different ways:

Authorization violation

By passing control

Eavesdropping (Overhearing something)

Interception

Malicious programs

Masquerade

Traffic analysis

Reputation

Resource exhaustion

Social engineering

Vulnerability

- **Vulnerability is weakness or absence of safeguards.**
- **Unlike threats, vulnerabilities usually exist within the organization**

Table 16.1 Examples of Vulnerability

Category	*Vulnerability*
Security policy	Granting higher rates to users than required.
Administration	Circumventing security procedures due to degradation in performance.
Administration	Initialising insecure system.
Administration	Empty root/administrator passwords, particularly during installation.
Implementation	Failure of protection mechanism.
Apathy	Bypassing or disabling security procedures for convenience.
Procedure	Duplication of confidential reports.
Procedure	Unsafe handling of backups containing confidential reports.

Safeguards

Safeguards are physical controls, security policies, security mechanisms and procedures that protect assets from threats.

Physical control :

- **Physical security**
- **Personnel security**
- **Administrative security**
- **Emanations security**

Security policies:

- **Set of rules established by the organization to apply**
- **Management policy**
- **Operational policy**
- **Procedural policy**
- **It establishes who is assigned to perform what role.**

Security services:

- **Identification and authentication service**
- **Access control service**
- **Confidentiality service**
- **Data integrity (honesty) service**
- **Non- repudiation service**

Attack

An attack is the awareness of threat

Broadly the attackers are

hackers,

spies (secret agent)

vandals (criminals) and

professional criminals

Tools

- **Physical attack**
- **Information exchange**
- **User commands**
- **Program and data up.**

Actions

- **Probe (Analysis)**
- **Scan**
- **Flood(overflow)**
- **Bypass control**
- **spoof (skit)**
- **steal (giveaway) and read/copy/modify.**

Target

- **The target of attack are generally account, process, data system components and network**

IDENTIFICATION AND AUTHENTICATION

- **Measures to prevent unauthorized people from entering the system.**
- **Identification is the means by which a user provides a claimed identity to the system. (User ID)**
- **Authentication is the means of establishing the validity of a user's claimed identity.**
- **There are three ways of authenticating a user's identity**

  Proof of knowledge; for example password

  Proof of possession (ownership) : for example card PIN

  Proof of property (biometrics) : for example fingerprint

Proof by knowledge

- Clear password
- Encrypted password
- Threats to password
  - Replay
  - Brute-force attack
  - Password guessing
  - Dictionary attacks
- Safeguards
  - To create a password very strong method.

Proof by Possession

- **System can recognize Bank card with PIN.**
- **Card by locking it and deactivates it if three unsuccessful attempts are made to enter the PIN.**

Proof by property

- **Biometric techniques such as fingerprints, written signatures, voice patterns, retinal scans, face and hand recognization.**
- **Strong authentication**

  Passkeys : To generate cryptography key

  OTP

  Challenge –response protocol (e.g 100+5)

ACCESS CONTROL

- **Enforcing authorization**
- **To prohibit the user from accessing resources not authorized to it.**

Subject :

Access authorization are to be granted.

The subjects may be processes or users.

Object :

Access must be controlled.

The object may be a File, DBs, CPU, Printer or Website

Operation :

Set of operations that may be performed on it.

e.g : Open, Close, Delete, Read and Write

Protection rules

Subject's access to the object.

Access control include by :

Identity-based policies : Individual, group, role based policy

Rule-based policies : Multi-level , compartment based policy

Security requirements : Top secret, confidential, unclassified

Mandatory Access control : Read – only, Write- only

Discretionary Access control : Share the information

Labeling : Human readable outputs.

Auditing : Ensure that all activities changes are updated.

Convert Channel Analysis : Leakage of information to be analyzed

A MODEL FOR NETWORK SECURITY

- **A message is to be transferred from one party to another across some sort of Internet.**
- **Security –related transformation is encryption of the message.**
- **Secret information to be unknown to the opponent.**
- **A trusted third party is secure transmission.**

- **Task:**

  Design an algorithm

  Generate the secret information

  Develop methods

  Specify a protocols.

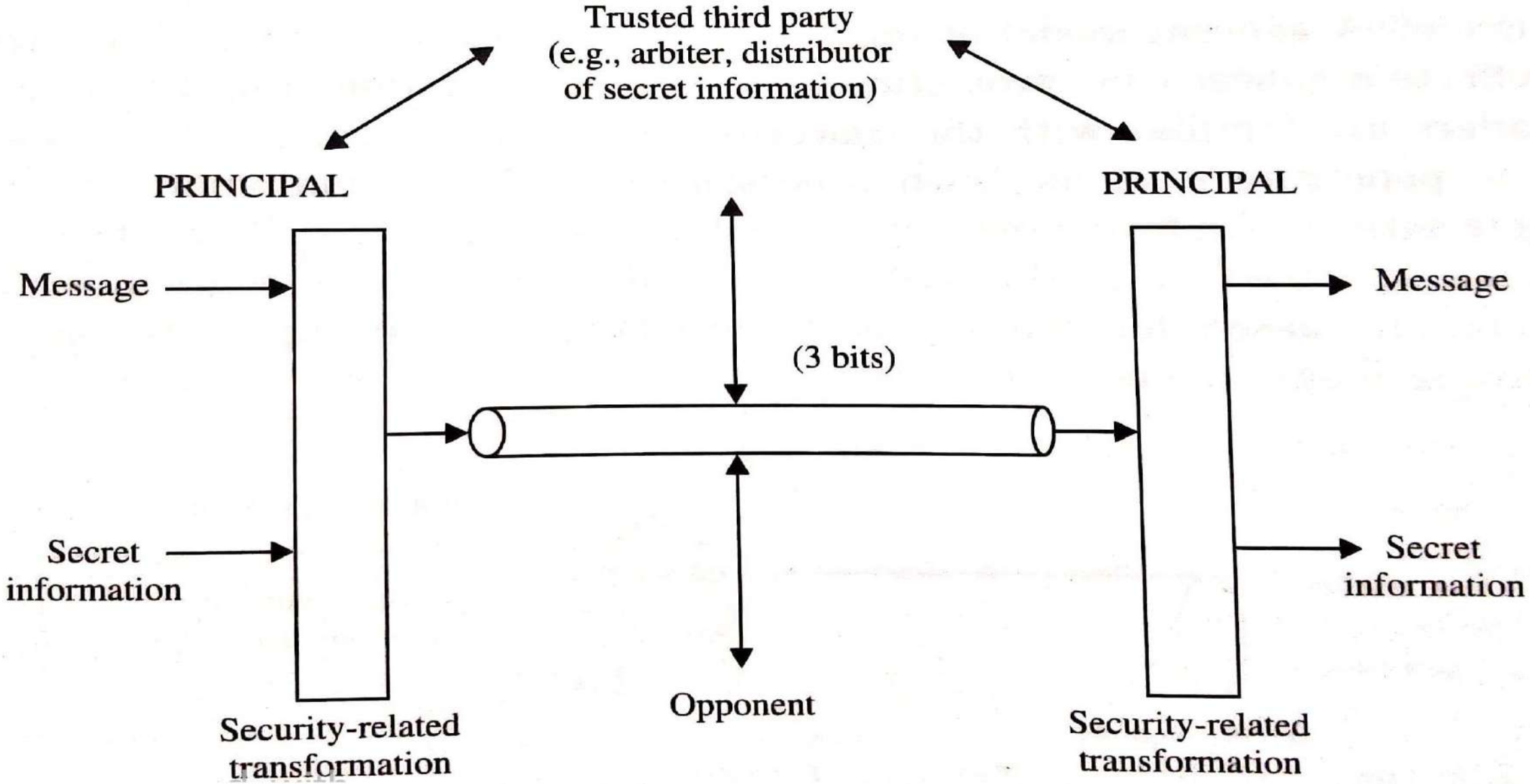


Figure 16.1 Model for network security.

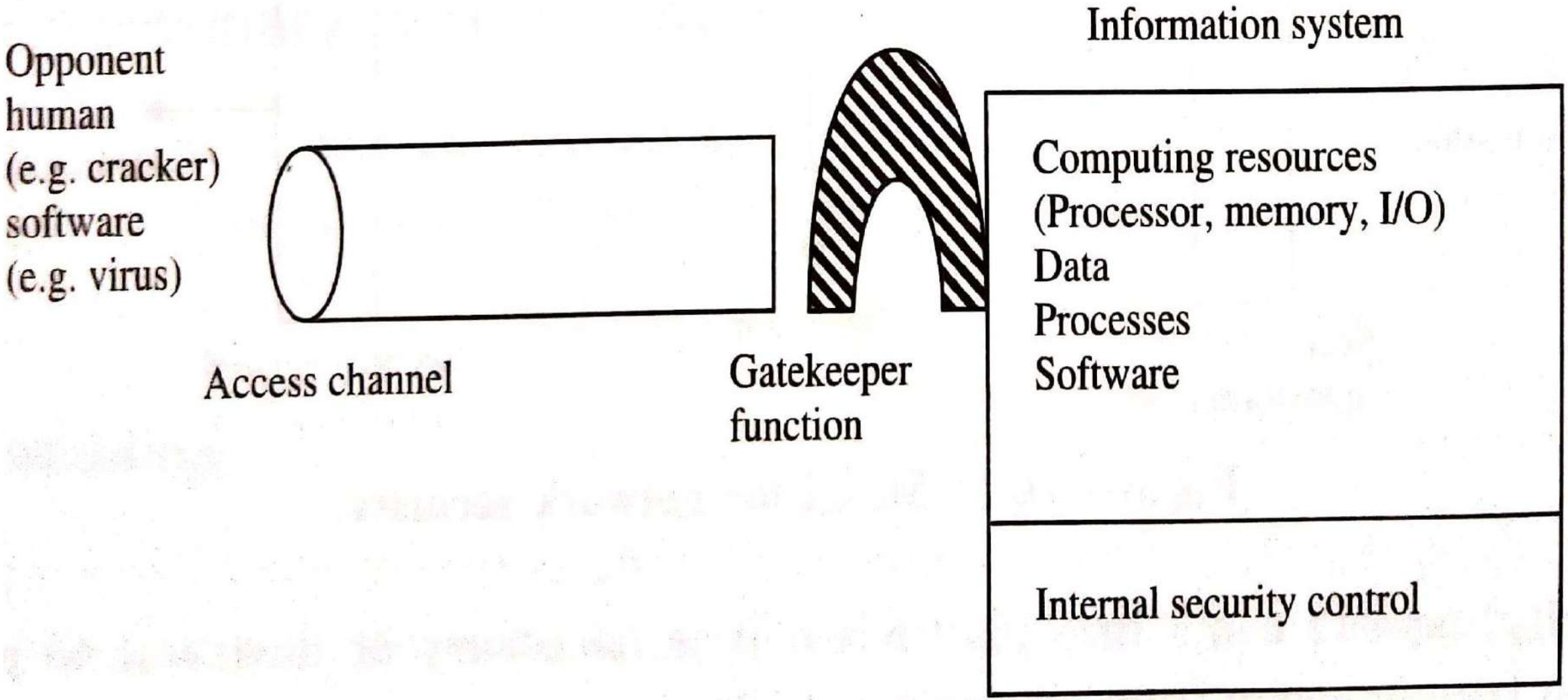


Figure 16.2 Network access security model.

General Vulnerabilities (Weakness)

Password sniffing – capture password

The r-command (‘r’ remote)

Software flaws - buffer overflow

X Window system : used password another window

Denial of services : attack server.

Attacks on Internet protocols

Packet replay : Ref. to recording and re-transmission

IP spoofing : Attacker changes the IP address

Source routing : Malicious packets to be supplied by hackers

Attacks on Internet Services

Telnet : Capture the password between client and server

FTP : Attack if too many files transfers are initiated simultaneously

TFTP : Steal (take) password files

Attacks through e-mail : Repeatedly sending an e-mail msg

It difficult to detect the originator

Denial of service : System crash and create failure of service.

MALICIOUS SOFTWARE

- **Malicious software are programs that corrupt other programs.**
- **Categories**

  Host dependent programs

  Host independent programs

Host dependent programs

Trapdoor : Enter without authentication

Logic bomb : Unauthorized actions by certain conditions.

Trojan horse : Hidden codes, executes unwanted functions

Trojan mule : Login session and terminates

Virus : A self-replicating program that infects other programs

Host independent programs

Bacteria : **Programs that consume system resources by replicating itself. The program does not explicitly damage any file**

Worms : **Sends copies from one computer to another across network connections. It can behave like virus.**

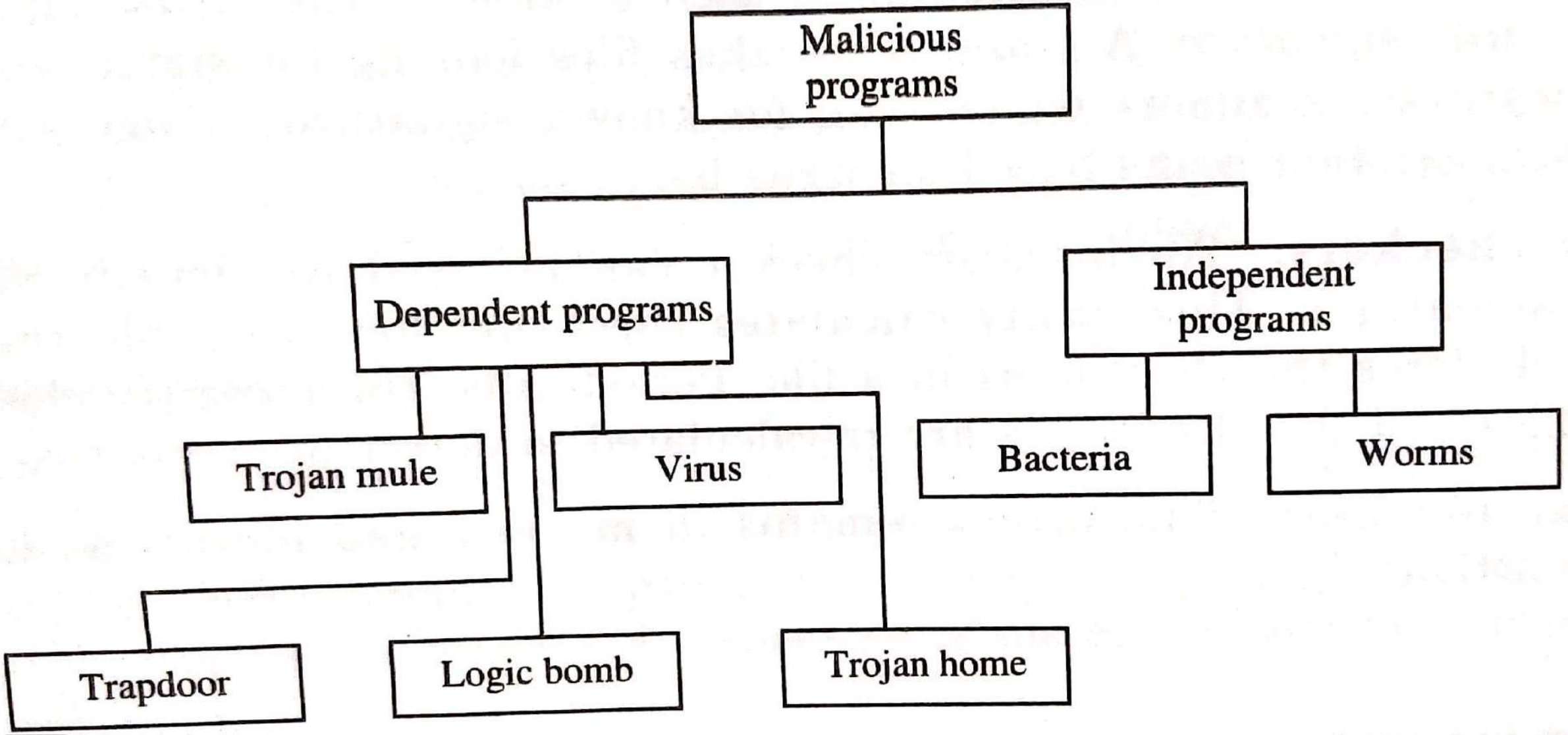


Figure 16.3 Taxonomy of malicious programs.

Safeguards

Scanners : Scans based on virus behavior

Integrity checker : Run again on files and the checksum discrepancies

Behavior blocker : Alerts the user of any doubtful activity.

SECURITY SERVICES AND CRYPTOGRAPHY

- **Protecting information against unauthorized access when it is transmitted through insecure channels.**
- **Used to prevent attacks.**
- **Methods of shifting the letters around to make the text unreadable were attempted.**

- **Include**

  Cryptosystems

  Symmetric cryptosystems

  Asymmetric cryptosystems

  Security Services

  Pretty Good Privacy

  IP Security

Cryptosystems

- **Cryptosystem deals with two primitive operations:**

  Encryption

  Decryption

- **Encryption is a process of transforming a message into unread form called cipher text.**
- **Decryption is a process of transforming the cipher text back to clear text to get the message.**

- **Example**

  Encryption is a function having the form C = E(P,Ke)

  Decryption is a function having the form P = D(C,Kd)

  Also, Decryption function D is the inverse of encryption function E, we have D(E(P,Ke),Kd) = P

  Where P is the Plain text

  C is the Cipher text

  Ke is the encryption key

  Kd is the decryption key

- **The strength of the cryptosystem depends on the algorithm and size of the key**

- **Cryptosystem properties:**

  Encryption and Decryption algorithms are easy and simple

  The security of cryptosystem

  It should be computationally infeasible for an attacker.

Symmetric Cryptosystems

- **In a symmetric cryptosystem, either both the encryption key and the decryption key are the same.**

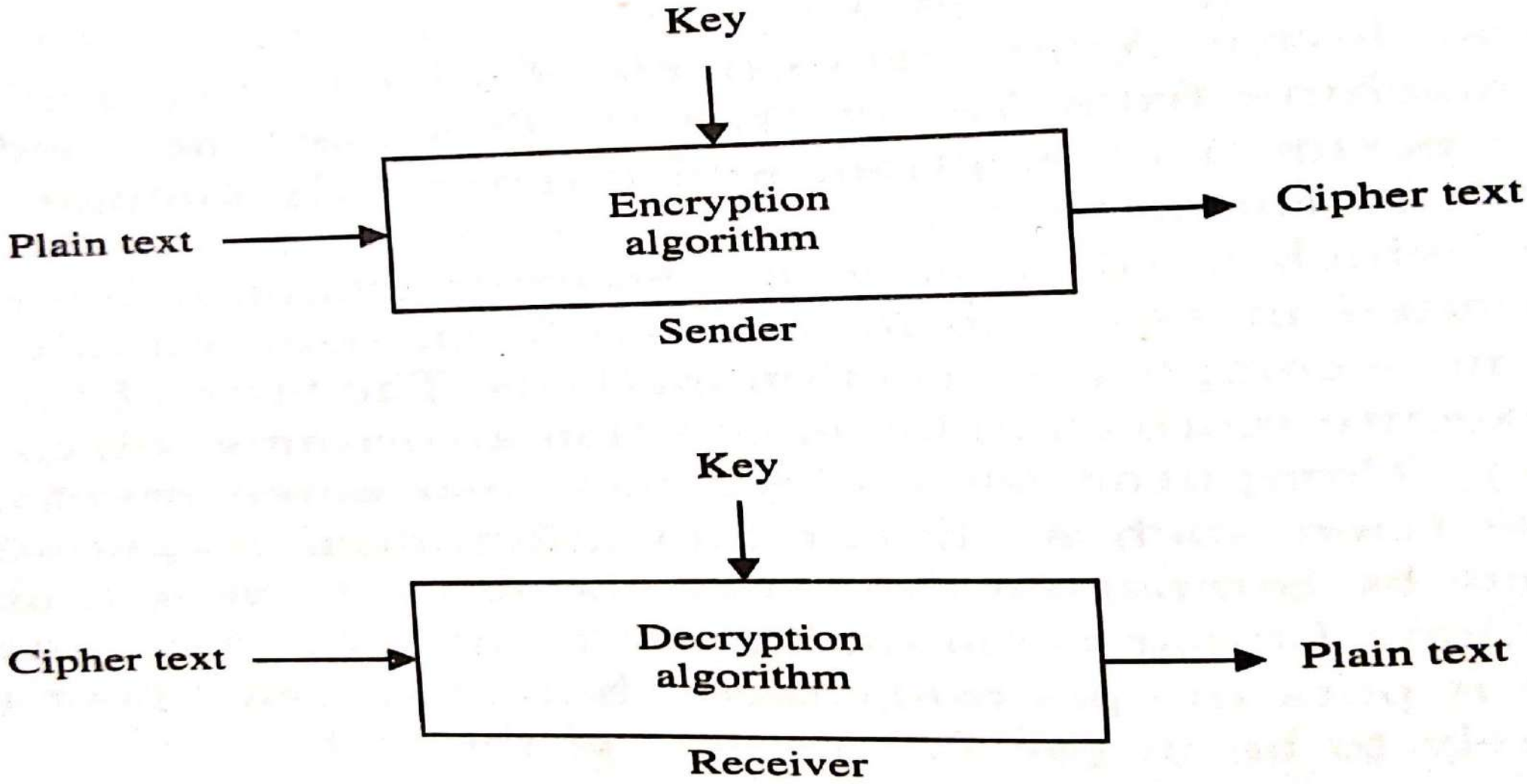


Figure 16.4 Symmetric cryptosystem.

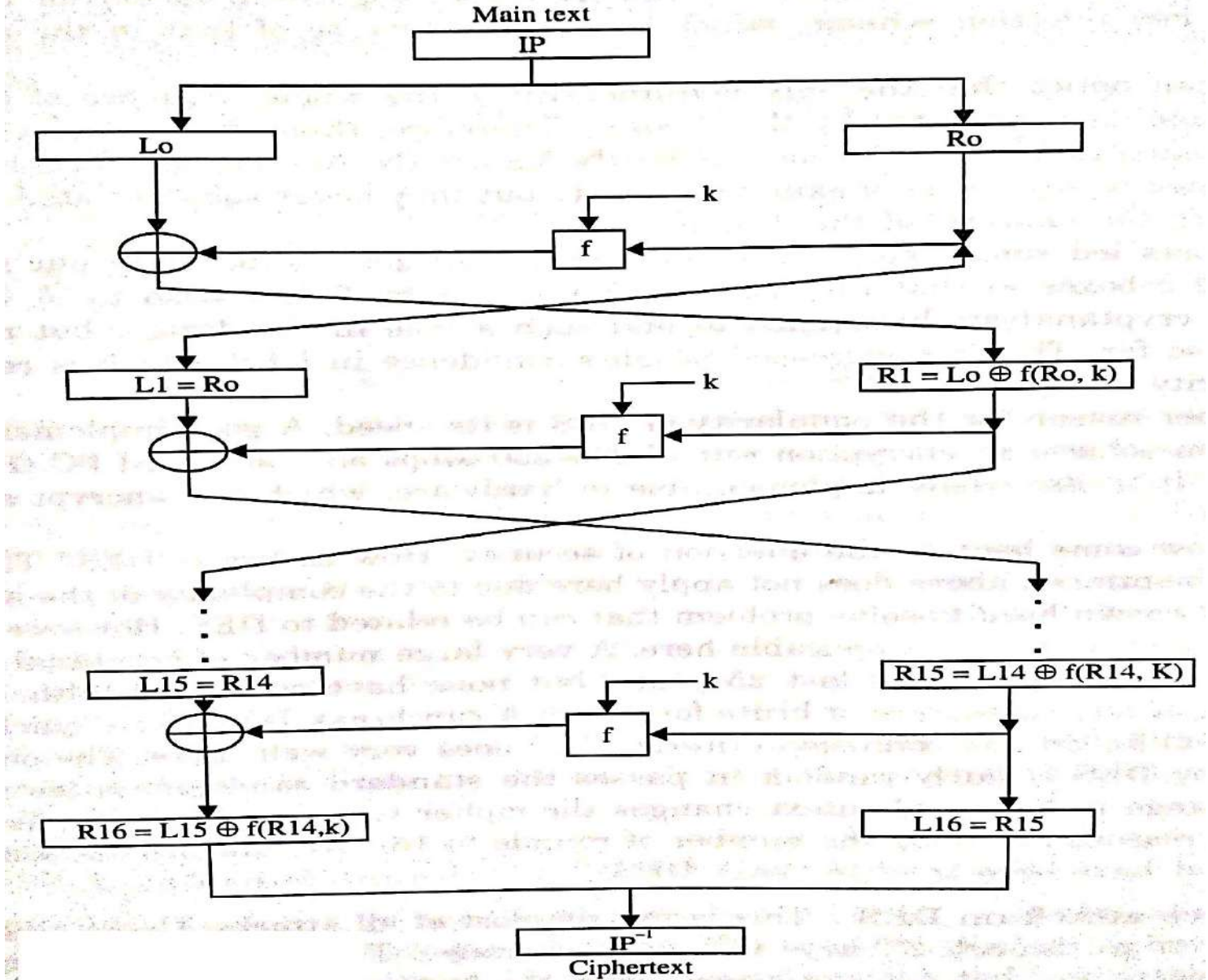
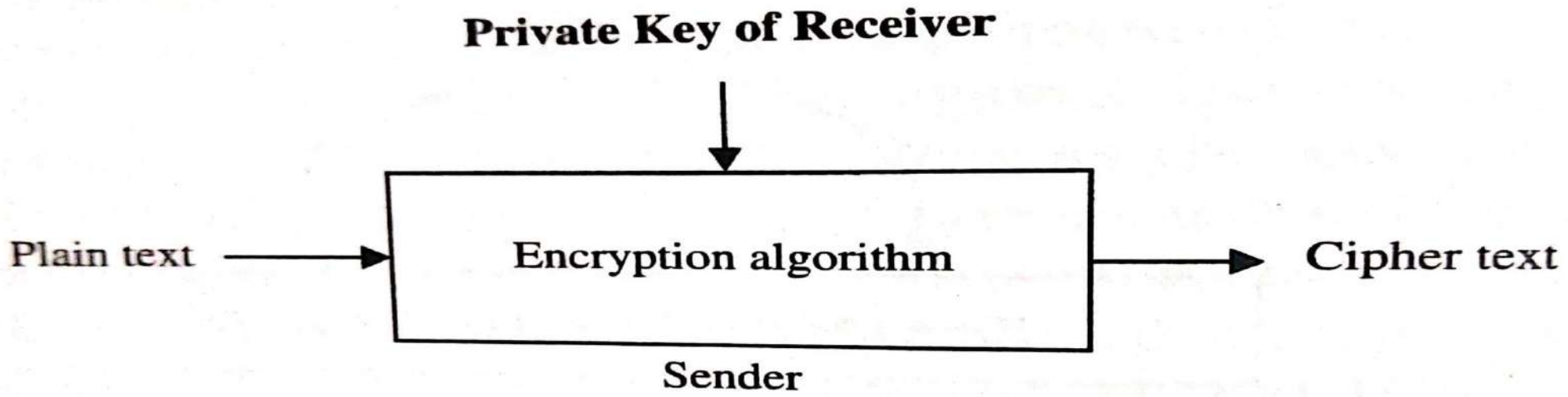


Figure 16.5 DES encryption.

ASymmetric Cryptosystems

- **In asymmetric cryptosystem, the encryption key is different from the decryption key and it is infeasible to computer the decryption key from the encryption key.**
- **Encryption key is made public whereas decryption key is kept secret.**
- **Public key cryptosystems are computationally expensive and hence not suitable for bulk data encryption.**



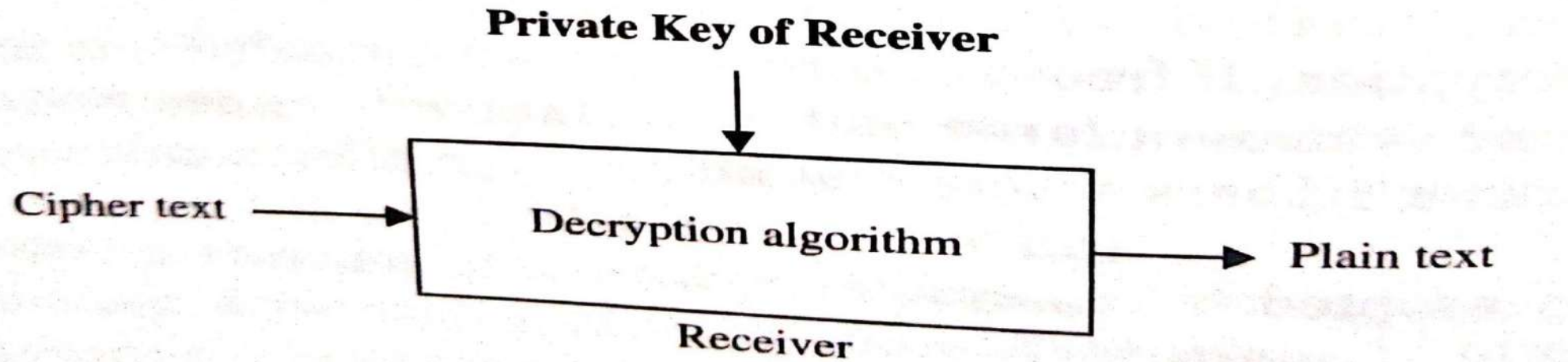


Figure 16.7 Public-key cryptosystem.

System RSA (Rivest, Shamir, Adleman)

The encryption key and the decryption key are defined as follows:

Encryption key:

A pair of numbers (n, e), where n is a product of two prime numbers p and q and e is a number relatively prime to number (p-1) * (q-1)

Decryption key:

Number d such that

$$d * e = 1 \text{ modulo } (p-1) * (q-1)$$

Encryption algorithm:

- **Plaintext is broken into blocks of size b-1 where b is the bit-length number n.**
- **Treating each block m_j as a binary number corresponding cipher text block is obtained by computing m_j modulo n.**

Decryption algorithm:

- **Cipher text is broken into blocks of size b.**
- **For a block C_j, the corresponding plain text is obtained by compuiting C_j^d modulo n.**

The receiver generates the key using the following steps:

1. **Fix the size of number n**
2. **Generate two random prime numbers p and q**
3. **Generates a random number e of size close to that of n such that e and the number (p-1) * (q-1) have no common factors**
4. **Compute number d such that d*e = 1 modulo (p-1) * (q-1)**

Security Services

- **The security services, namely confidentiality, integrity, authentication, non-repudiation and non-replay are described below:**

Confidentiality : Protection against information

Integrity : Ensures that a message is received exactly as it was sent or a discrepancy is detected, in case the content of the message is altered.

Authentication : Confirms that when someone claims to have a particular identity, then the claim is correct.

Non-reputation : Provides assurance that parties involved in the exchange of a message cannot deny having participated in the exchange of information.

Non-reply : Provides assurance that if copy of a authentic communicated message is retransmitted for some criminal purpose, then it is detected.

Table 16.2 Security Services

Security service	*Traditional solution*	*Digital solution*
Confidentiality	Sealed envelopes	Encryption
Integrity	Signatures	Message digest, Digital signatures
Authentication	Notaries, photo identity cards	Digital signatures, Digital certificates
Non-repudiation	Signature receipts	Digital signature
Non-replay	Date and time	Digital timestamps, Nonce.

Pretty Good Privacy (PGP)

- **PGP is an asymmetric encryption/decryption program for e-mail, computer data, and voice conversations.**
- **Protect data on Internet because it is effective, easy to use, and still free.**
- **PGP is based on the asymmetric key method using private and public keys.**
- **Available at http://www.pgp.com/**

IP Security (IP sec)

- **To support the secure exchange of packets at the IP layer.**
- **Security for the transmission of sensitive information over unprotected networks such as the Internet.**
- **Protecting and authenticating IP packets.**
- **Sending and receiving devices must share a public key.**

Security services:

1. Data confidentiality :

The IP sec sending station can encrypt packets before transmitting them across a network

2. Data Integrity:

The IP Sec receiver can authenticate packets sent by the IP Sec sender to ensure that the data has not been altered during transmission.

3. Data Origin authentication:

The IP Sec receiver can authenticate the source of the IP Sec packets sent.

4. Anti reply:

The IP Sec receiver can detect and reject packets that have been received correctly but which are sent more than once (duplicated)

SECURING NETWORK USING FIREWALL

- **Firewall separates an organization's internal network from an outside untrusted network and shields the entire network from access by harmful protocols and services.**
- **Network admin may monitor and control the flow of information.**
- **A firewall examines every data packet passing through it.**
- **Advantages:**

  Filter unwanted protocols and services

  Direct incoming traffic

  Log traffic

  Hide names and addresses

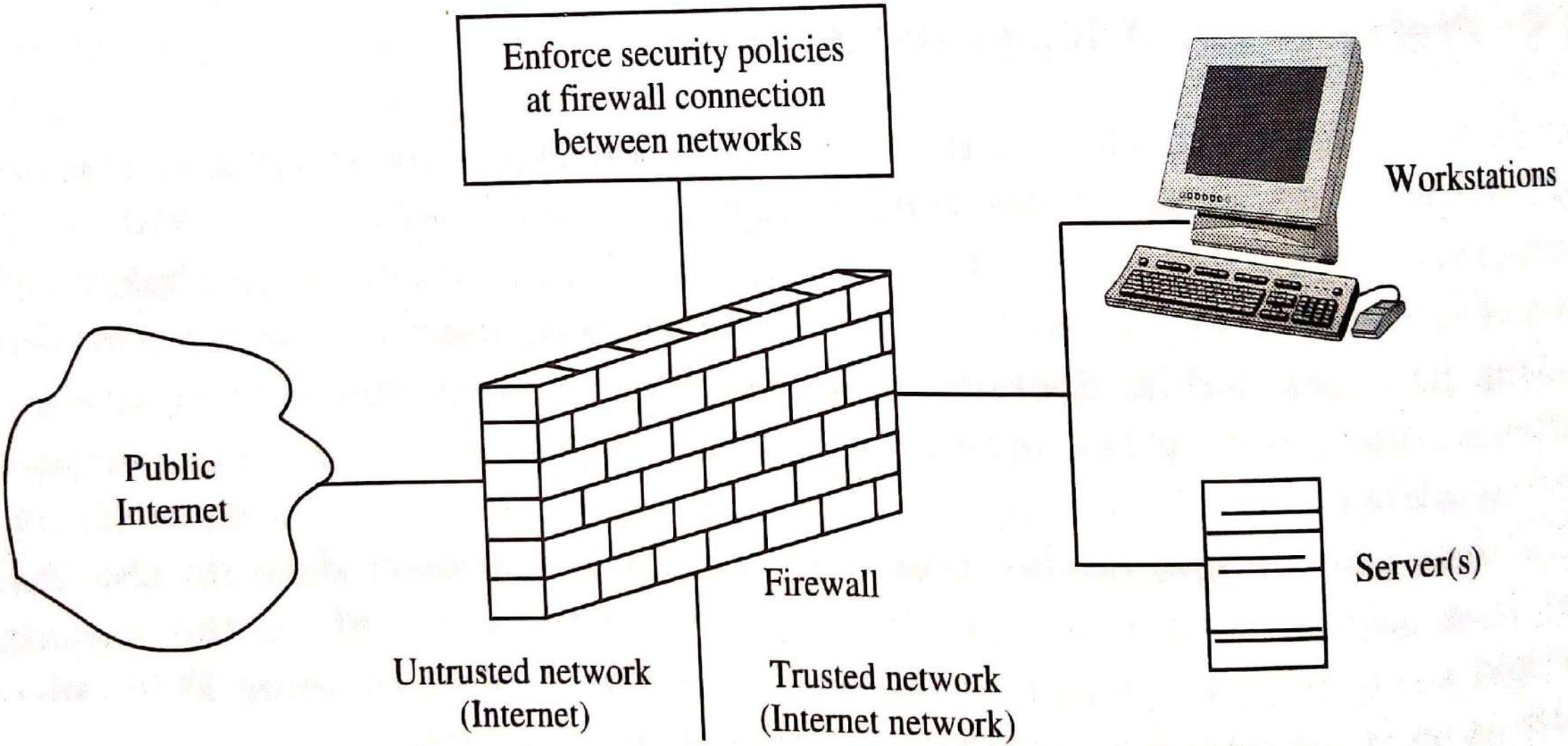


Figure 16.10 A firewall at the boundary of two networks.

When you connect to the Internet, you are putting three things at risk:

Your data – the information you keep in the computers

Your resources – the computer themselves

Your reputation – Which can be affected by others using your identity

- **Firewalls offer excellent protection against network threats, but they are not a complete security solutions.**
- **Firewalls do not protect you against**

  Malicious insiders

  Connections

  Completely new threats.

  Viruses.

- **Types of firewalls**

  Packet filtering firewalls.

  Application Gateways.

Packet filtering firewalls :

- **A router running packet-level firewall software, can examine all network traffic at the packet level allowing or denying packet passage from one network to the other based on the source and the destination addresses.**

- **Check each incoming or outgoing IP packet header against access control rules.**
- **If the address and port information are acceptable, the packet proceeds through the firewall directly to its destination.**
- **If not, the packet is dropped at the firewall.**
- **Unfortunately, they have low security, internal network to attack by direct connection with untrusted external sources.**

The following fields within packets can be filtered.

- **The type of packet, such as IP, UDP, ICMA, TCP**
- **IP source and destination address**
- **TCP/UDP source and destination ports**

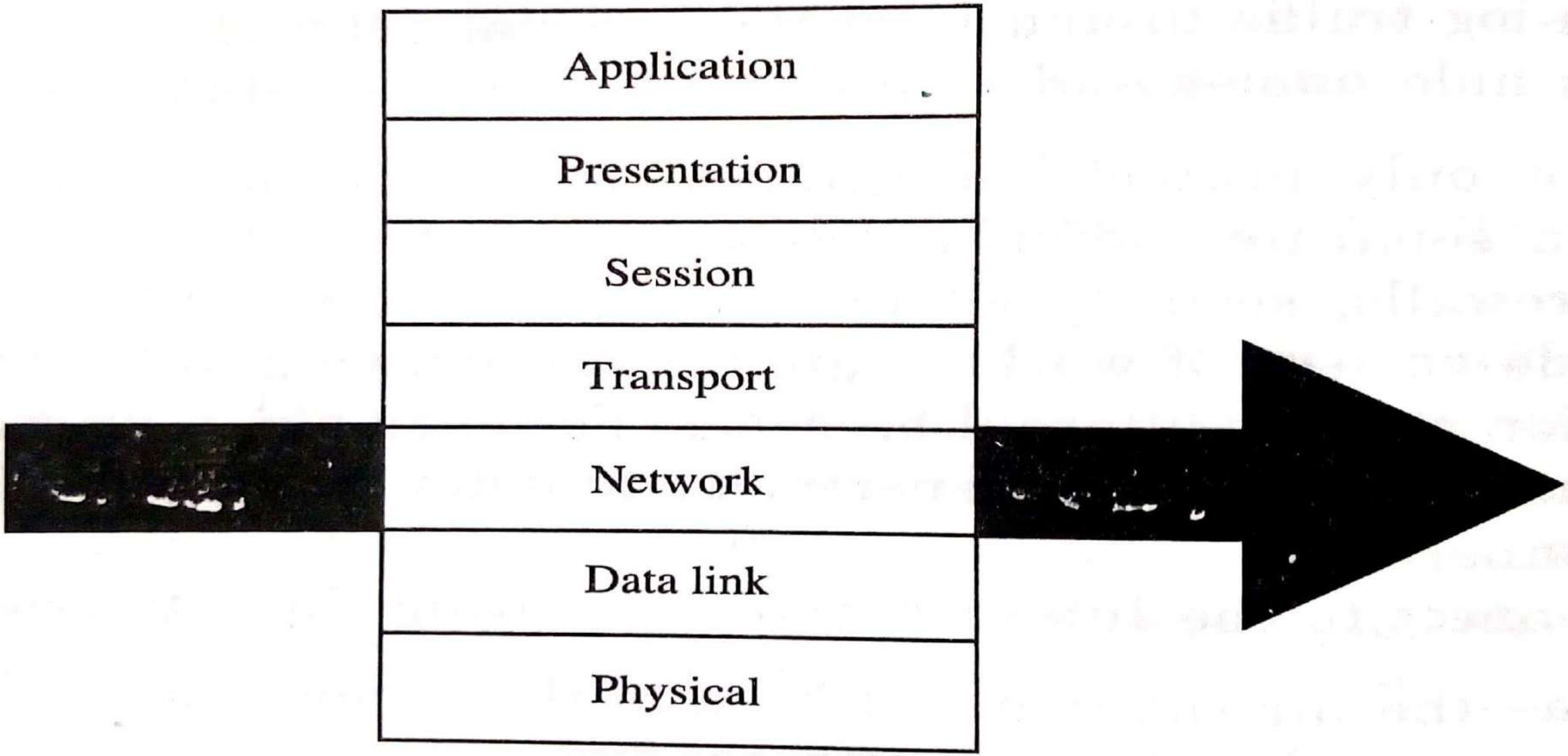


Figure 16.11 Packet filter firewall.

Application Gateways

- **Examines and controls data at the application level.**
- **Application gateway may pass the traffic on to the host or may reject if it is not authorized.**
- **Services**

  Access-telnet

  FTP

  E-mail

  HTTp

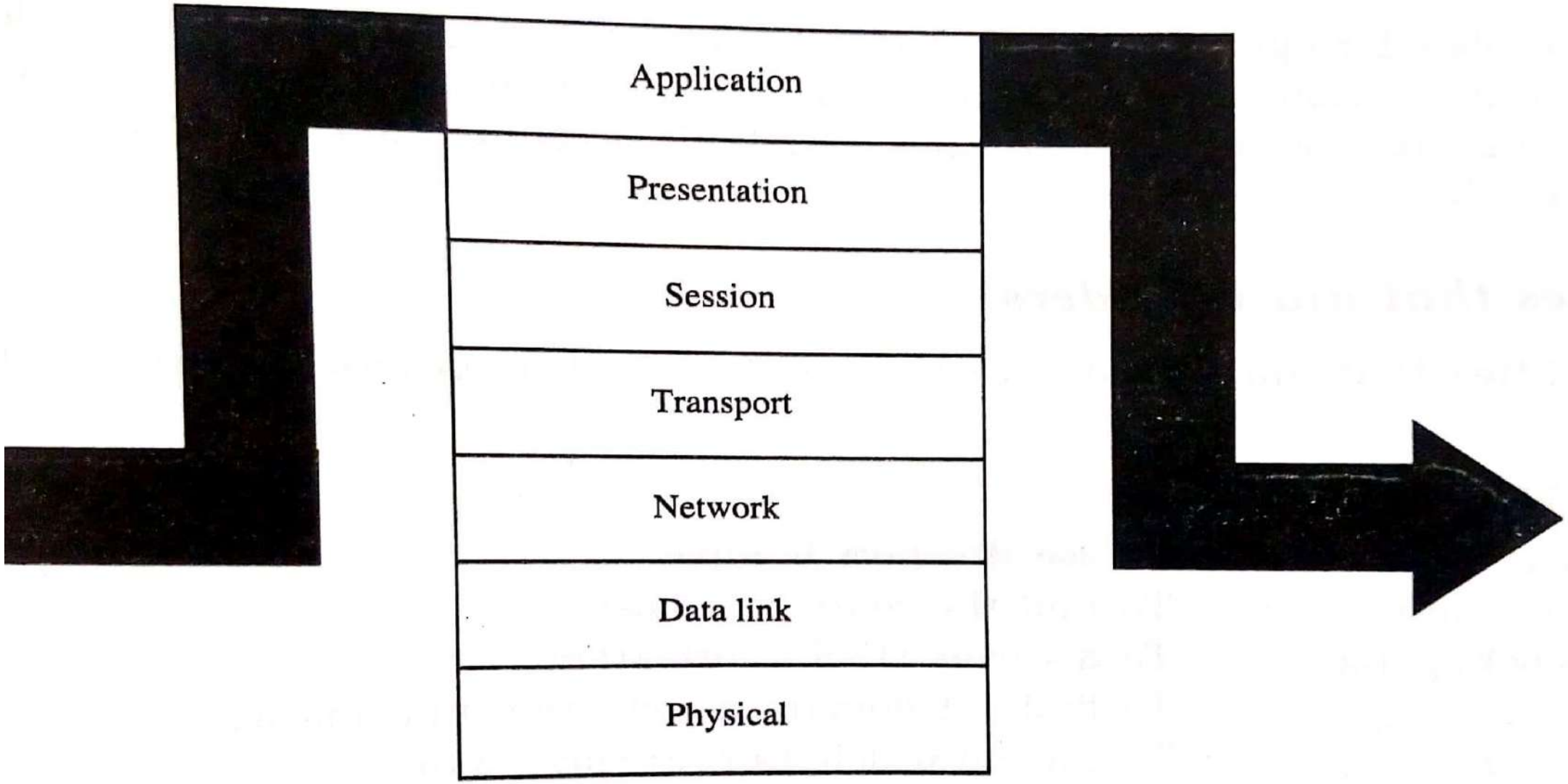


Figure 16.12 Application gateways.

Limitations of Firewalls

The major drawbacks of firewall as security system are:

- **Firewall cannot protect against "content related" attacks**
- **It concentrates security in one spot.**
- **A firewall provides no protection within the network it is protecting.**
- **Firewalls can be "fooled (mislead)" by source routing.**

INTRUSION DETECTION

An intruder attempt to break into a system to misuse it in various ways including denial of service attack.

- **Password cracking**
- **Software bugs and buffer overflow**
- **Weaknesses in Internet protocols and services**
- **Domain name service attack**
- **Attacks through mail protocols**
- **Attack IP address.**

Utilities that aid intruders:

General Utilities:

Ping	**: To see if a host is alive**
Trace route	**: To find the route to a host**
Nslookup/dig	**: To see DNS information**
Whois	**: To find out domain registration information**
Finger	**: To find out which users are logged in and to collect information about them**
r-commands	**: Scans for rlogin, rsh (remote shell)**

Special Utilities:

Crack package	**: To crack passwords, take passwords out of the system.**
Sniffing networks	**: To watch raw network traffic**
Port scanner	**: To scan TCP and UDP ports**
Pint sweepers	**: To ping large no.of machines to see which ones are active.**
Exploit packs	**: To know how to exploit holes on systems when the users are already logged in**
War dialers	**: To dial several phone numbers to locate dial-in ports**

Techniques to Detect Intrusions

- **Signature recognition**
- **Anomaly detection**
  - **Statistical anomaly detection (collection of data)**
  - **Rule-based detection (deviation from previous usage pattern)**
- **Safeguards:**
  - **Examine log files for unusual connection**
  - **Check system executable files**
  - **Check system for unauthorized use of network**
  - **Examine all machines for sings of network intrusion.**

Intrusion detection systems

- **Identifying attempts or successful intrusion of the system.**
- **Monitor packets**
- **Monitor system files**
- **Monitor log files**

Firewall and IDS

- **Double checks misconfigured firewalls**
- **Find attacks that firewalls fail**
- **Catch hacking from insiders**

Network Security tools

- **Bouncy cast**
- **Open SSL**
- **Trinux**
- **Snort**
- **Kerbers**
- **Nmap**
- **IP tables**
- **Tomcat**
- **Clam AV**
- **Spam assain**

Web Security

- **The web is a system with completely accepted standards for storing, retrieving, formatting, and displaying information using a client/server architecture.**
- **The web combines text, hypermedia, graphics and sound.**
- **Web browser software is programmed according to HTML standards.**
- **HTTP which is communication standard used to transfer pages on the web.**

Include

- **Client/ server architecture**
- **Security consideration and Threats**
- **Web traffic security approaches**
- **SSL/ TLS for secure web services (Secure Socket Layer)**
- **(Transport Layer security)**
- **Secure Hypertext Transfer Protocol (S-HTTP)**
- **Secure Electronic transaction (SET)**

Client / Server Architecture

- **The information is stored on the www on web servers and it uses the internet to transmit data around the world.**
- **The www, where a client access services from the server.**
- **These servers can either be local or available through a global network connection.**
- **A local connection normally requires the connection over a LAN.**
- **A global connection normally requires the connection to Internet Service Providers (ISPs).**

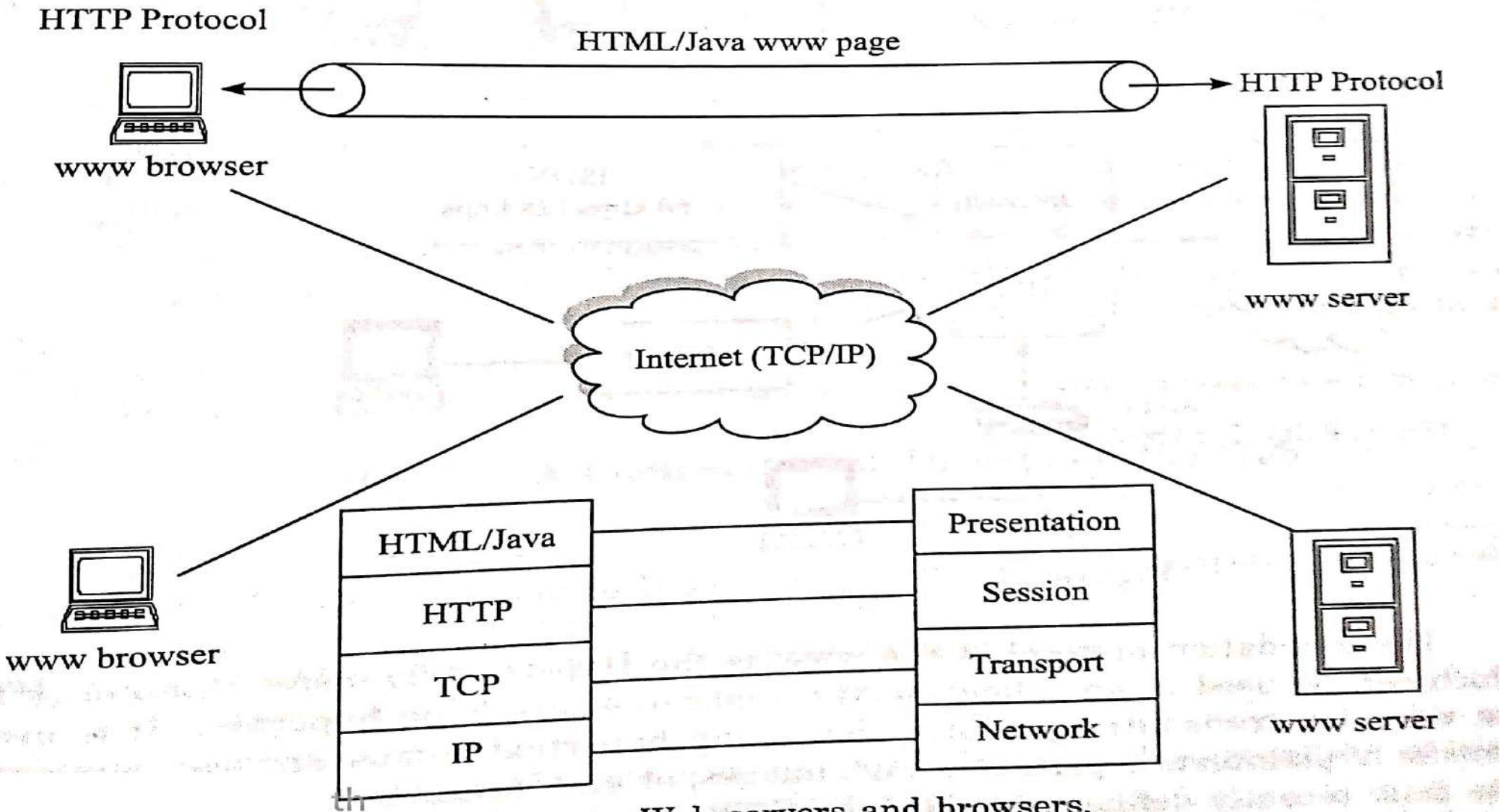


Figure 17.1 Web servers and browsers.

- **Connection to a client computer through a dial-up modem connection (28.8 kbps or 56 kbps)**
- **Connection to a client computer through a dial-up ISDN connection (64 kbps or 128 kbps)**
- **Connection of client computer to a server computer which connects to the Internet through a frame relay router (56kbps or 256 kbps)**
- **Connection of client computer to a LAN which connects to the Internet through T1, 1.544 Mbps router.**

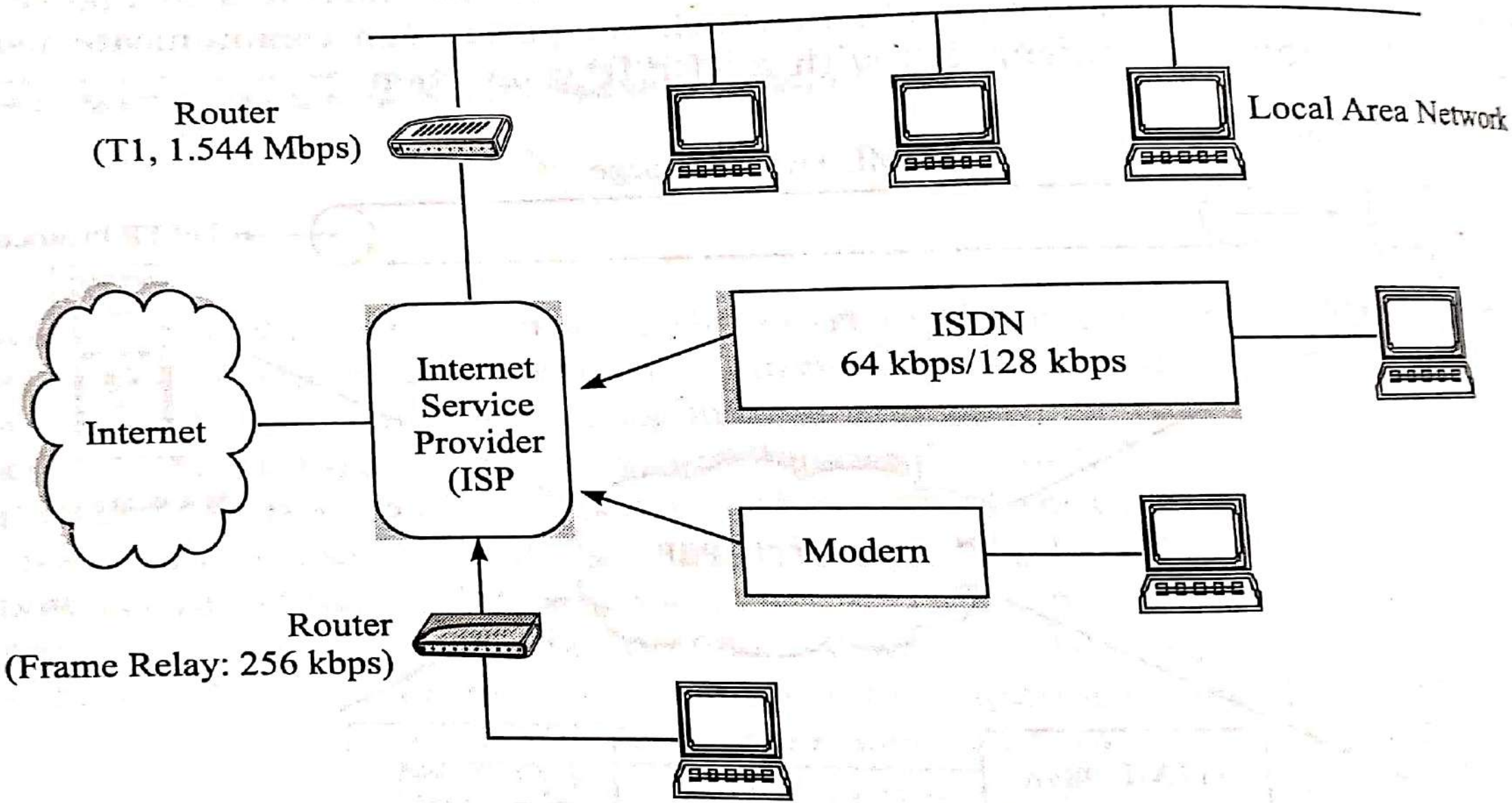


Figure 17.2 Example connections to the internet.

- **HTTP used on www for transmitting information using hypertext and can support the transfer of plaintext, hypertext, audio, images.**
- **Server receives the request, it attempts to perform the requested action, includes status information, a success/error code, extra information.**

SECURITY CONSIDERATION AND THREATS

- **Client/ Server application running over the Internet.**
- **Reputation can be damaged and money can be lost if the web servers are disrupted.**

Table : A Comparison of Threats on the Web

	Threats	*Consequences*	*Countermeasures*
Integrity	**Modification of user data**	**Loss of information**	**Cryptographic checksum**
	Trojan horse browser	**Compromise of machine**	
	Modification of memory	**Vulnerability to all other threats**	
	Modification of message traffic in transit		

Table : A Comparison of Threats on the Web

	Threats	*Consequences*	*Countermeasures*
Confidentiality	Eavesdropping on the net	Loss of information	Encryption, web proxies
	Theft of information from server, Theft of data from client Information about network configuration, Information about which client talks to server	Loss of privacy	

Table : A Comparison of Threats on the Web

	Threats	*Consequences*	*Countermeasures*
Authentication	Impersonation of Legitimate users	Misrepresentation of users	Cryptographic techniques
	Data forgery	Belief that false information is valid	

Table : A Comparison of Threats on the Web

	Threats	*Consequences*	*Countermeasures*
Denial of service	**Killing of user threats**	**Disruptive**	**Difficult to prevent**
	Flooding machine with bogus threats	**Annoying**	
	Filling up disk or memory	**Prevent user from getting work done**	
	Isolating machine by DNS attacks		

- **Threats in terms of passive and active attacks.**
- **Passive attacks include overhearing on network traffic between browser and the server.**
- **Active attacks include copying another user, alternating messages in transit between client and server, and altering information on a web site.**
- **Threats in terms of location of the threats :**

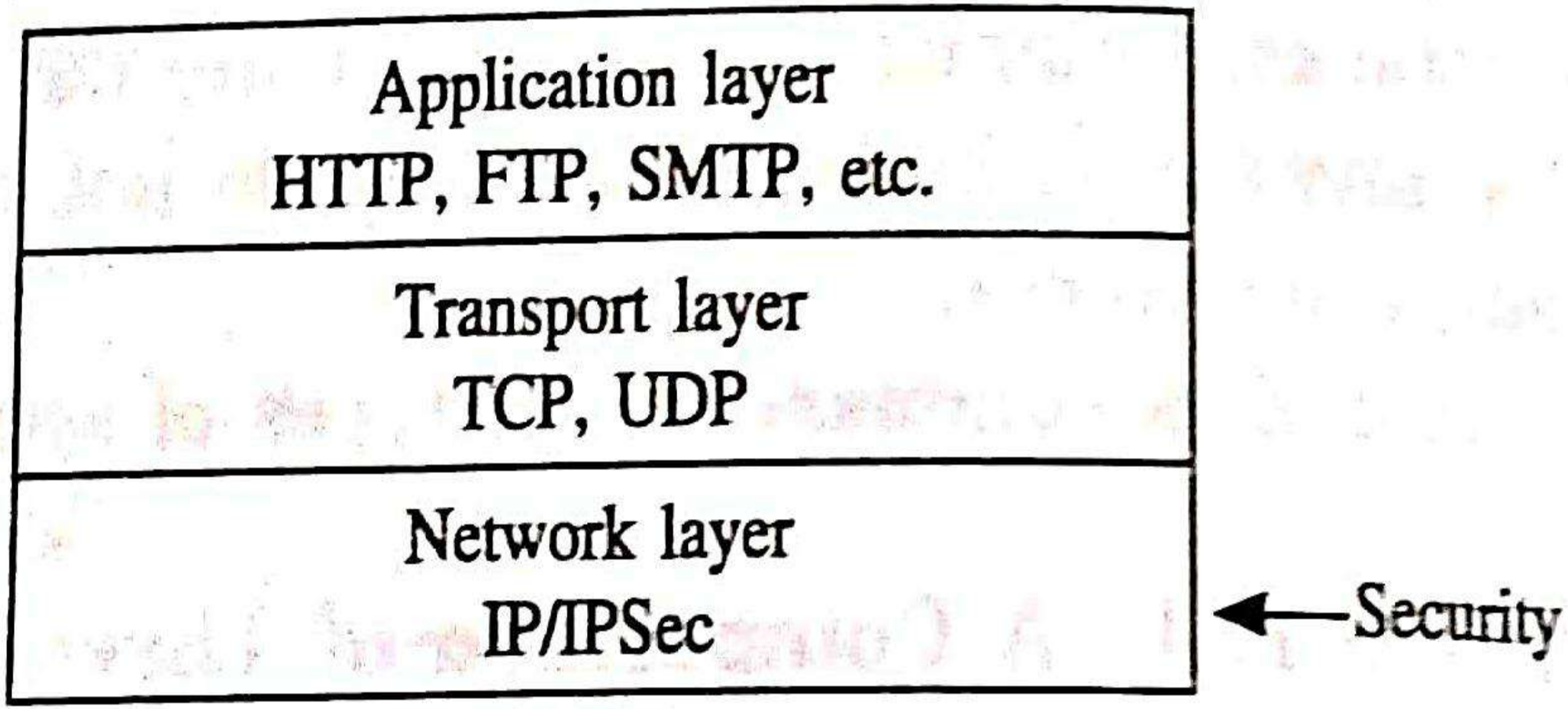
  Web server, Web browser, and network traffic

WEB TRAFFIC SECURITY APPROACHES

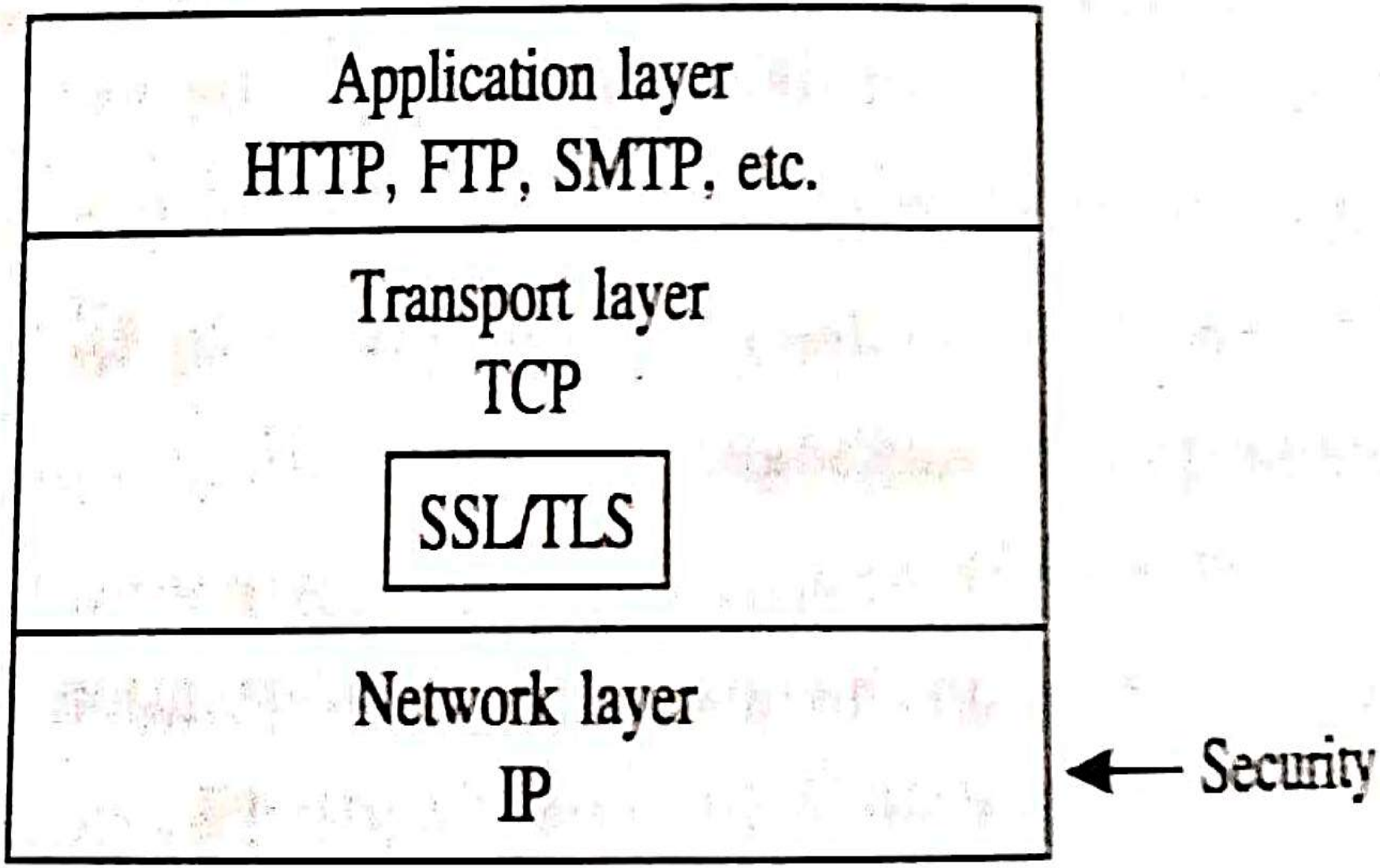
- **IP Security is that it is transparent to end users and applications and provides a general purpose solution.**
- **IP Security includes filtering capability.**

- **Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client**
- **Transport Layer Security(TLS), is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.**
- **A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website.**

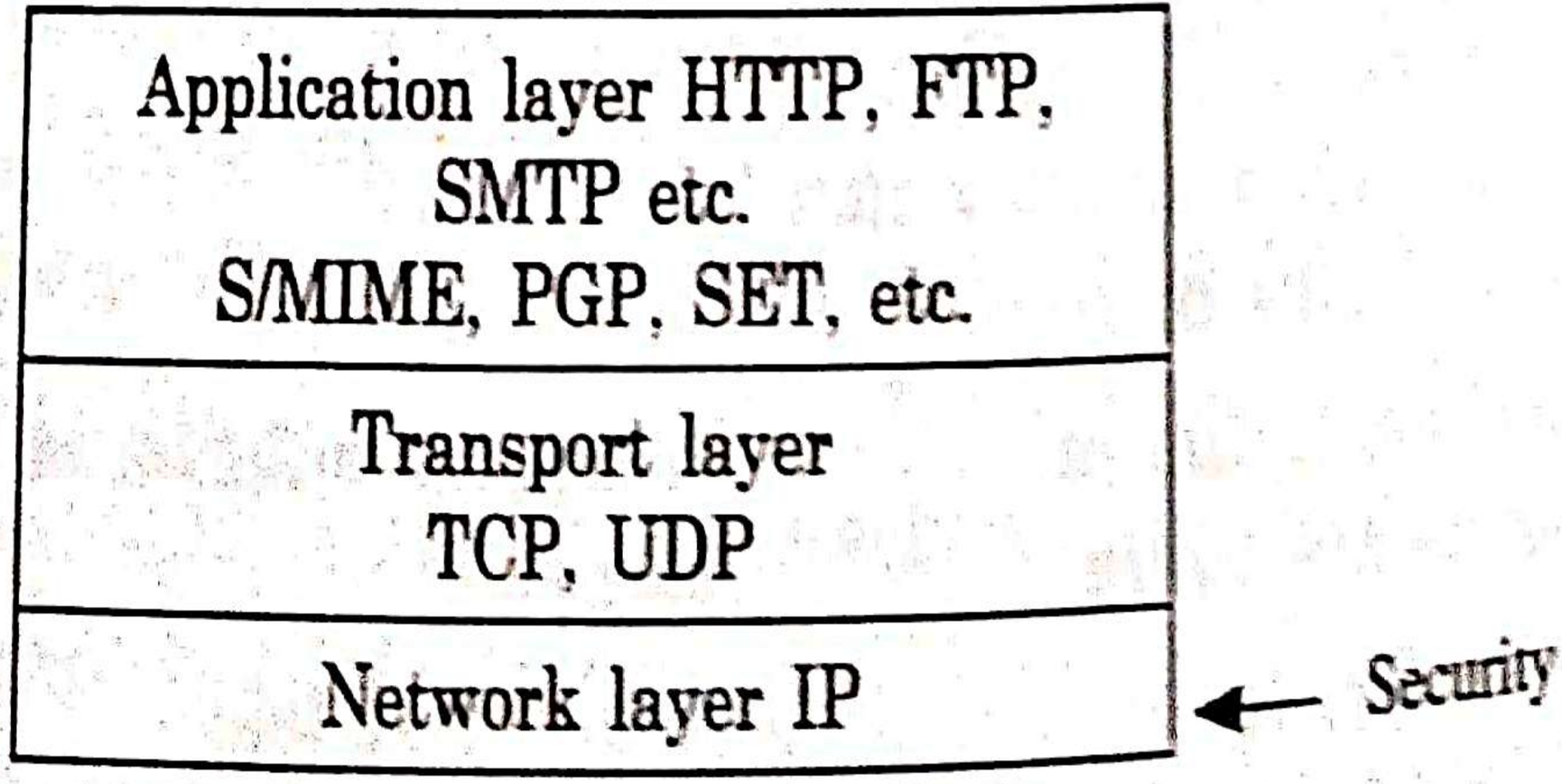
- **Secure Electronic Transaction (SET) is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario.**



(a) Security provided at the network layer with IPSec



(b) Security provided at the transport layer with SSL/TLS



(c) Security provided at the application layer with PGP, SET, etc.

SSL / TLS SECURE WEB SERVICE

- **SSL provides transport layer security.**
- **SSL/TLS allows for either server-only authentication or server -client authentication.**
- **In server -only authentication, the client receives the servers' certificate.**
- **The client verifies the server's certificate and generates a secret key that it then encrypts with the server's public key**

- **The client sends the encrypted secrete key to the server, the server decrypts it with its own private key.**
- **In the server-client authentication, in addition to the secrete key, the client also sends to the server its certificate that the server uses for authenticating the client.**

SSL / TLS SECURE WEB SERVICE

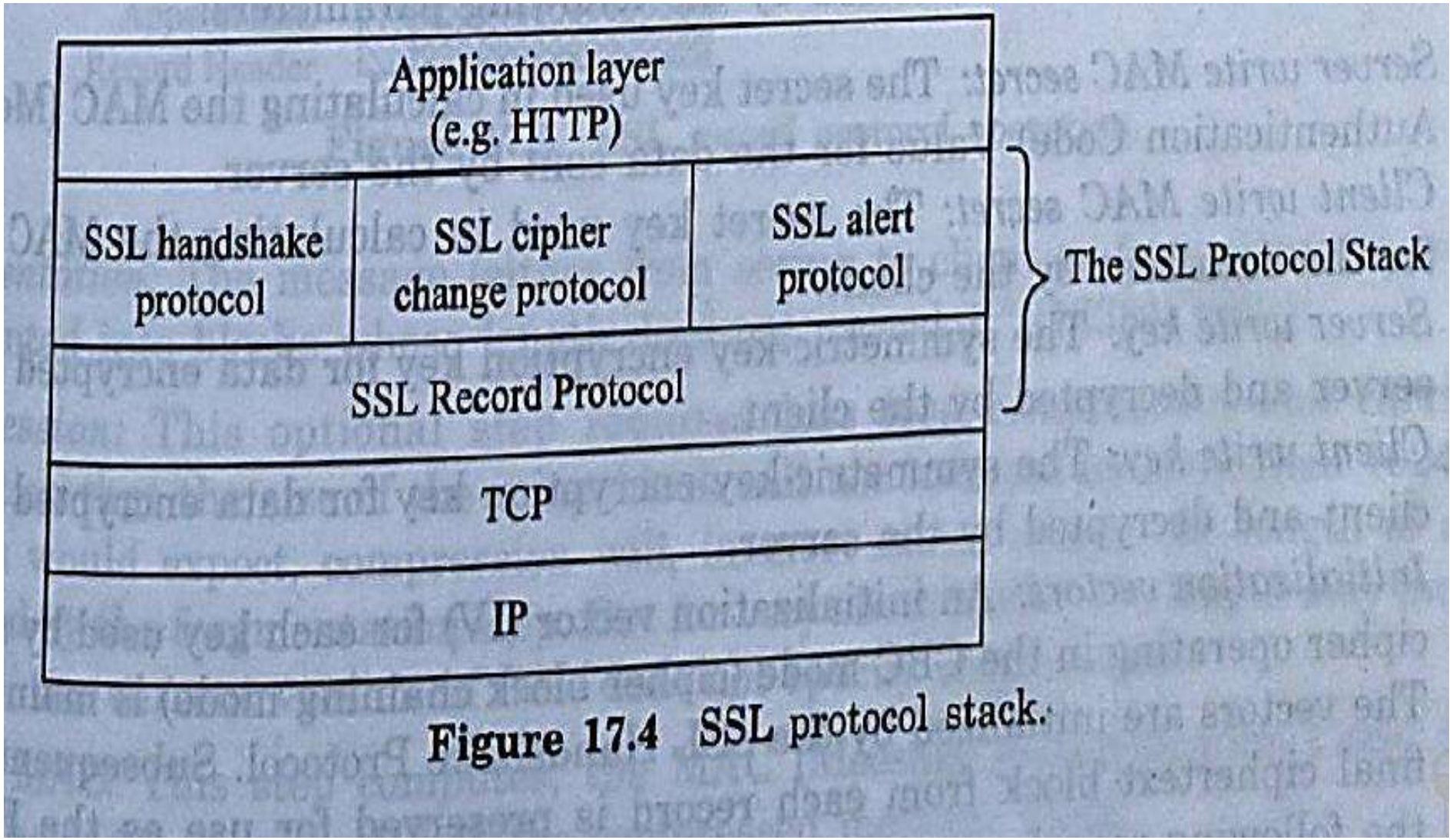


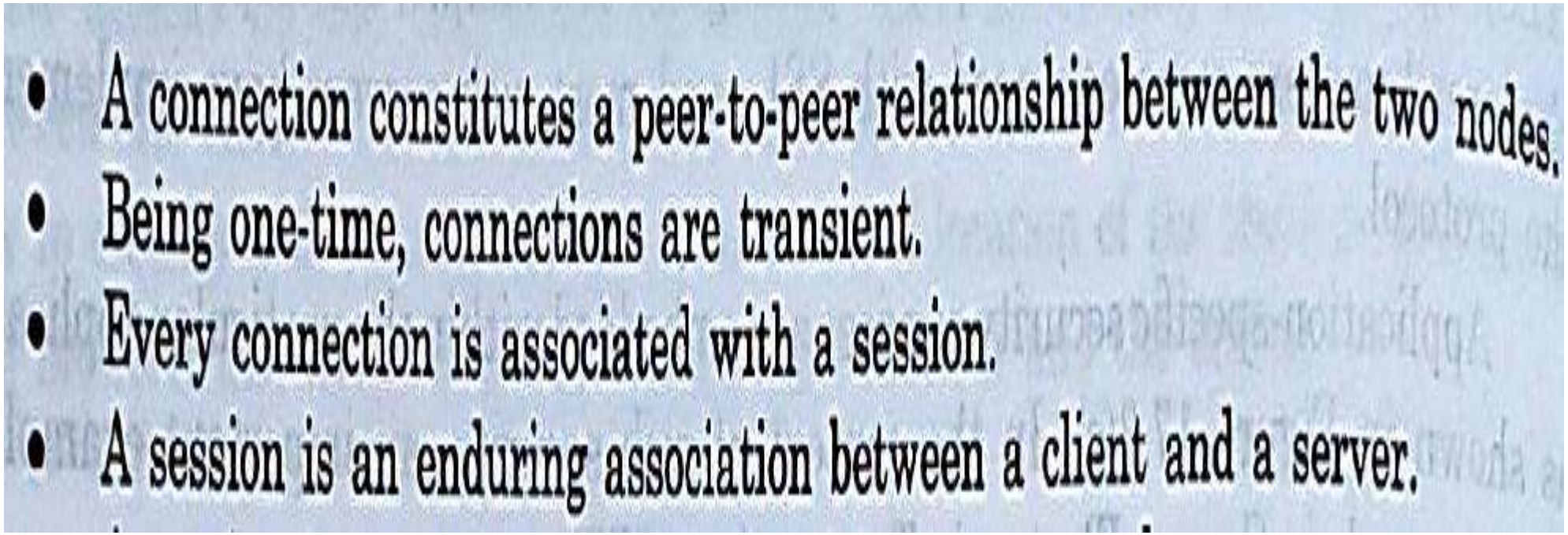
Figure 17.4 SSL protocol stack.

Include

- **The Twin concepts of SSL connection and SSL sessoin**
- **SSL Session State**
- **SSL connection State**
- **SSL Record Protocol**
- **SSL Handshake Protocol**

The Twin concepts of SSL connection and SSL sessoin

- **A connection is a one-time transport of information between two nods in a communication network.**



- A session is created by the SSL handshaking protocol.
- A session can consist of multiple connections.
- A session is characterized by a set of security parameters that apply to all the connections in the session.
- The concept of a session eliminates the need for negotiating the security parameters for each separate connection.

SSL Session State

An SSL session state is characterized by:

Session id : Server to identify an active or resumable session state

Peer Certificate : State may be null

Compression method : Used to compress the data prior to encryption

Cipher specification : **MAC (Message Authentication Code) calculations.**

Master secret : **Shared between the client and the server**

Is resumable : **A flag indicating whether the session is allowed to imitate new connections**

SSL Connection State

An SSL connection state is characterized by

Server write MAC secret : Calculating the MAC value for the data sent by the server

Client write MAC secret : Calculating the MAC value for the data sent by the client

Server write key : Data encrypted by the server and decrypted by the client

Client write key : Data encrypted by the client and decrypted by the server.

Sequence number : Each party maintains separate sequence numbers for the transmitted and received message through each connection.

SSL Record Protocol

- **Provides two services:**

  Confidentiality

  Message integrity

- **Used to actual data that the server wants to send to a client or that the client wants to send to the server, fragmenting the data into blocks, applying authentication and encryption to each block,**
- **On the receiver side, the blocks are decrypted, verified for message integrity, reassembled and delivered to data.**

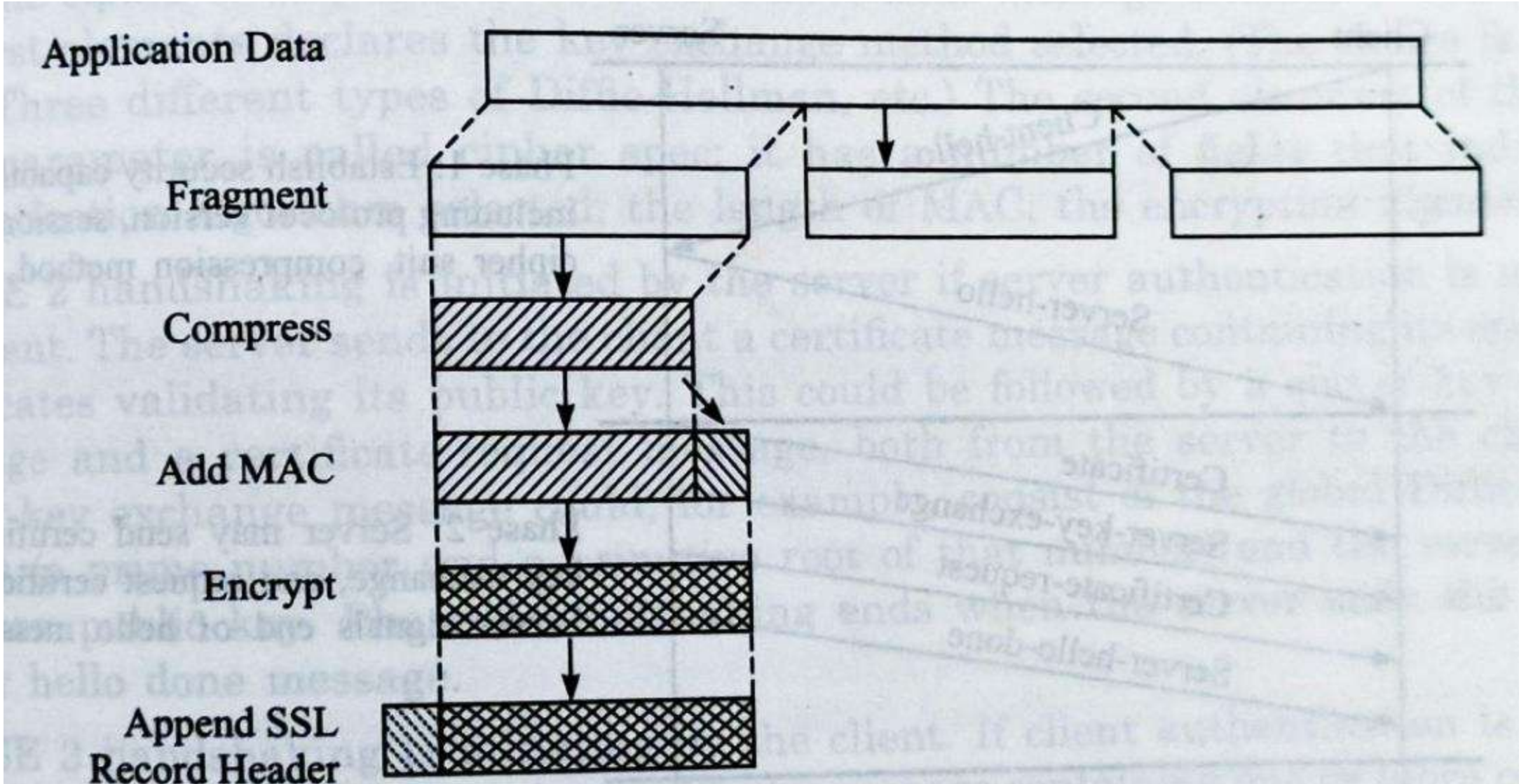
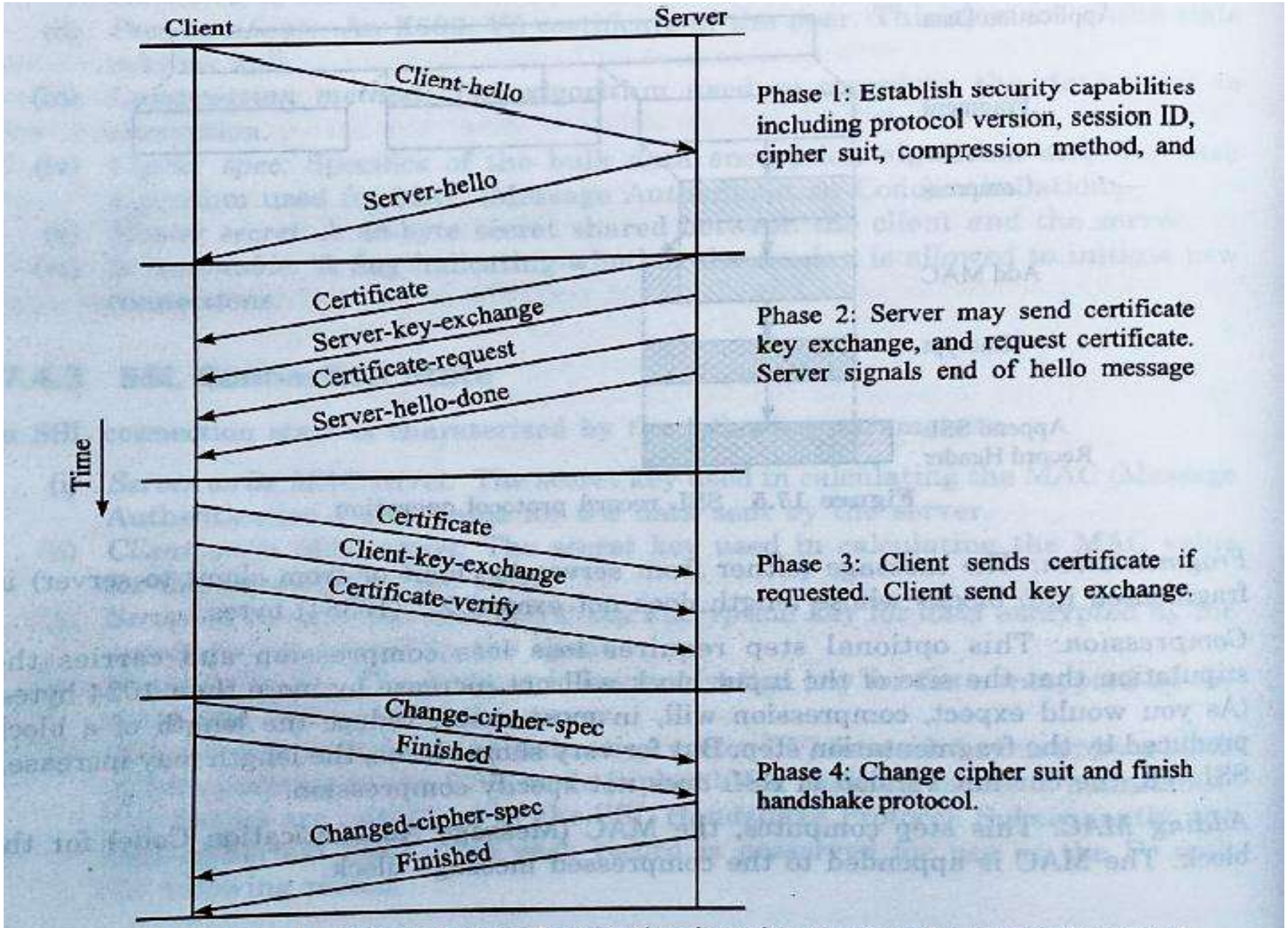


Figure 17.5 SSL record protocol operation.

SSL Handshake Protocol

- **The SSL Handshake Protocol is also responsible for the server and the client to authenticate each other.**
- **Phase 1 : Establish security capabilities including protocol version, session ID, cipher suit, compression method**
- **Phase 2 : Server may send certificate key exchange, and request certificate. Server signals end of hello message**
- **Phase 3 : Client sends certificate if requested. Client send key exchange**
- **Phase 4 : Change cipher suit and finish handshake protocol**



Note: Shared transfers are optional or situation-dependent messages that are not always sent.

Figure 17.6 Handshake protocol action.

S-HTTP (Secure Hyper Text Transfer Protocol)

- **The native protocol that web clients and servers use to communicate is Hypertext Transfer Protocol.**
- **This protocol is ideal for open communications.**
- **It does not provide authentication or encryption features.**
- **S-HTTP provides considerable flexibility in terms of what cryptographic algorithms and modes of operation can be used.**
- **S-HTTP, message may be protected using digital signatures, authentication, and encryption**
- **Sender and the receiver establish preferences for encrypting and processing secure messages.**

Secure Electronic Transactions (SET)

SET is an open encryption and security specification designed to protect credit card transaction on the Internet.

Services:

1. **Provides a secure communications channels among all parties involved in a transaction**
2. **Provides digital certificates**
3. **Ensure privacy because the information is only available to parties in a transaction when and where necessary.**

- **Secure transactions are critical for electronic commerce on the internet.**
- **SET is designed to secure credit card transactions by authenticating cardholders.**

SET include the following features:

- **Required digital signatures to verify that the customer.**
- **Uses multiparty messages that allow information to be encrypted.**
- **Prevent credit card numbers from getting in the wrong hands**
- **Requires mixing into the credit card processing system.**
- **Payment methods could include credit cards, debit cards, electronic cash and cheques.**
- **SET addresses "Electronic wallet" that can identify the use and validate the transaction.**

- **Electronic wallet is a type of software application used by the consumer for securely storing purchasing information.**

Include

Business Requirements

SET Participants

SET Transaction Flow

Business Requirements

- Provide authentication that a cardholder is valid user of a credit card account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution
- Provide confidentiality of payment and ordering information
- Ensure the honesty of all transmitted data.
- Ensure the uses of the best security practices.

- **Ensure the uses of the best security practices.**
- **Create a protocol that neither depends on transport security mechanism nor prevents their use.**
- **Facilitate and encourage interoperability among software and network providers.**

<u>Key features:</u>

Cardholder account authentication

Merchant authentication

Integrity of data

Confidentiality of information

SET Participants:

- Cardholder
- Merchant
- Issuer
- Acquirer
- Payment gateway
- Certification Authority

Cardholder

- **In the electronic environment, consumers and corporate purchasers interact with merchants from computer over Internet.**
- **A cardholder is an authorized holder of a payment card (e.g Master card, Visa) that has been issued by an issuer**

Merchant

- **A merchant is a person or organization that has goods or services (offered by web site or e-mail) to the cardholder.**

Issuer :

This is financial sector, such as a bank that provides the cardholder with the payment card.

Acquirer :

Establishes an account with a merchant and processes payment card authorizations and payments

Payment gateway

Operated by the acquirer or designed third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions

Certification Authority :

Certificates for cardholders, merchants and payment gateways.

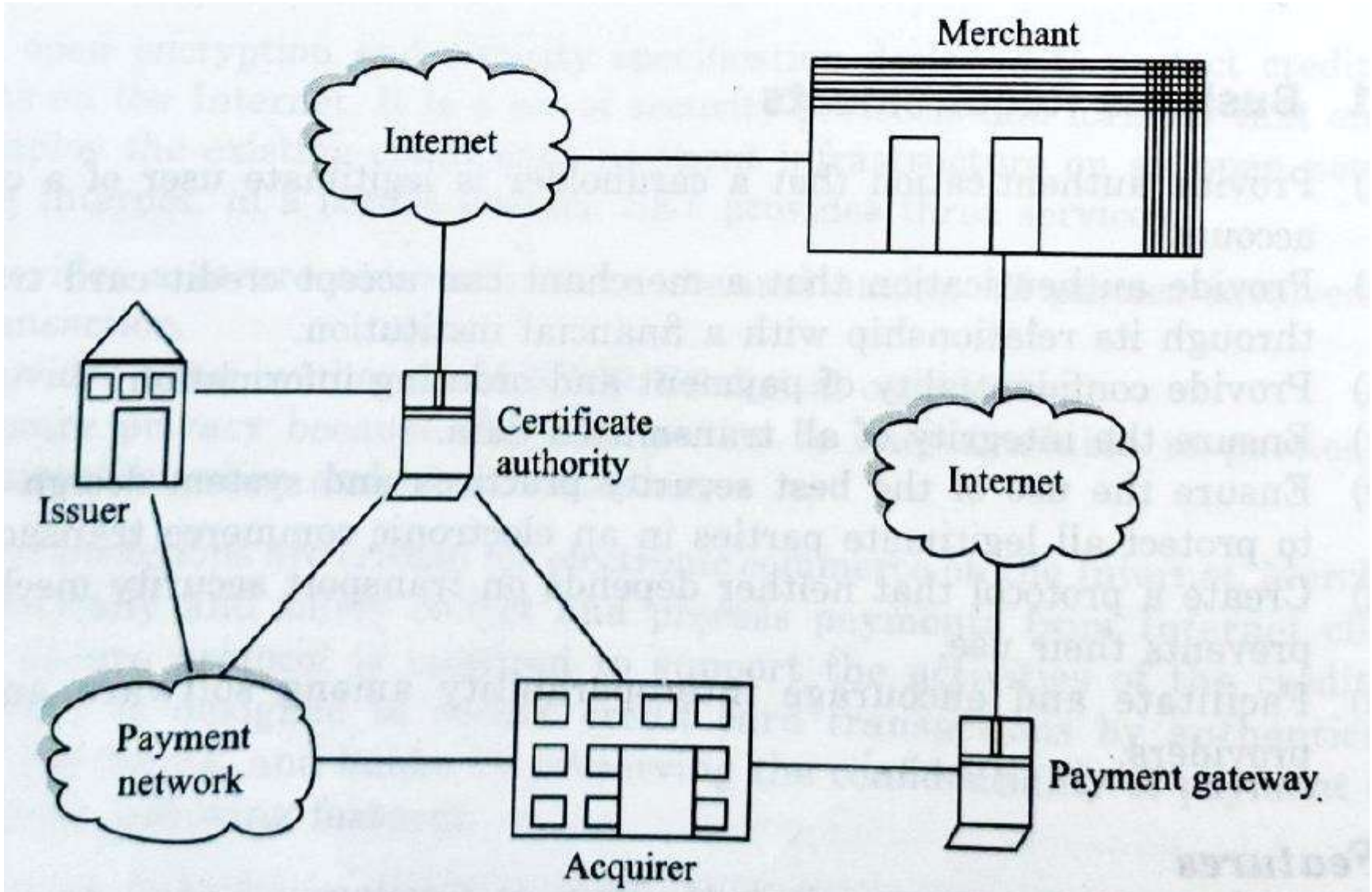


Figure 17.7 SET components and their relationships.

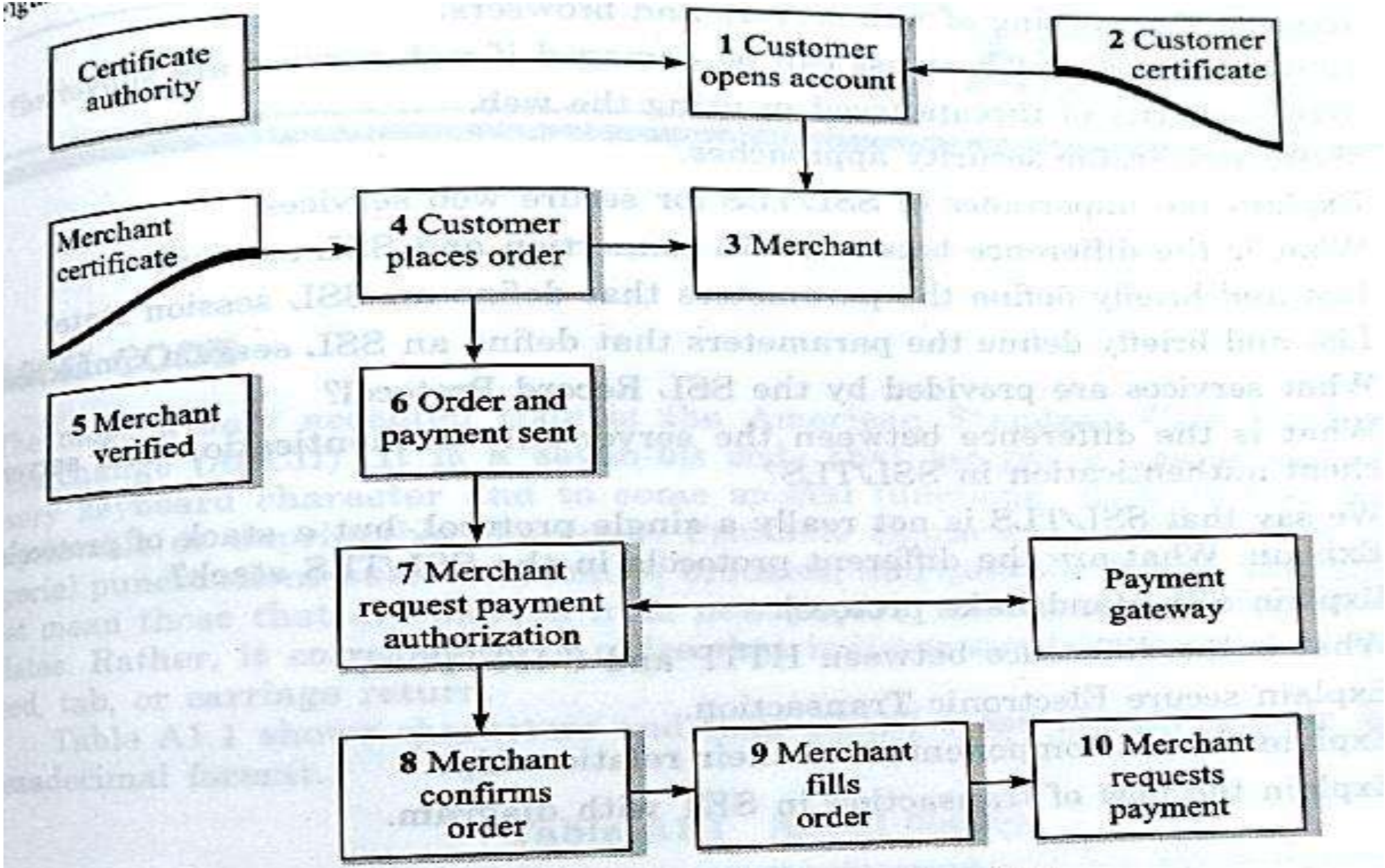


Figure 17.8 SET transaction flow.

1. The customer opens an account and obtains a credit card account with a bank that supports electronic payment and SET.
2. These customers receive a certificate after suitable verification of identity. It establishes a relationship between the customer's key pair and the credit card.
3. Merchants have certificates consisting of one key for signing messages and one for key exchange. They also need a copy of the payment gateway's public key certificate.
4. The customer places an order, which is accepted by the merchant. The order form returned from the merchant includes the items, the cost, and an order number.

number.

5. The customer receives the merchant certificate.
6. The customer sends the order, payment, and this certificate to the merchant.
7. The merchant requests payment authorization through the payment gateway.
8. The merchant provides the customer with order confirmation.
9. The merchant ships the product or service.
10. The merchant request payment gateway, which handles all payment processing.

Thank You...