UNIT II

Syllabus

- Introduction
- Perspective of network
- Protocols and standard
- Network Topologies
- Transmission Mode
- Categories of network
- LAN, MAN, WAN,
- OSI Model
- Functions of the layer
- TCP/IP Protocol suit
- Link Configuration
- Asynchronous and Synchronous mode.

Syllabus continue………

Physical layer

- Digital data transmission
- DTE-DCE Interface
- Other Interface Standard
- V.24 Null Modem
- Modem Standards
- Cable Modem
- Transmission Media

Syllabus continue………

Data Link layer

- Types of Errors
- Error Detection and Correction Methods
- Flow Control
- HDLC
- Brief Details of Data Link Protocols.

Data Communication

Data communication is the exchange of data between two devices by making use of some transmission media.

Data Communication may be of two types

Local

Remote

If the communicating devices are in the same building then it is a type of local communication

If the devices are farther apart then it is a type of remote communication

Effectiveness of data communication

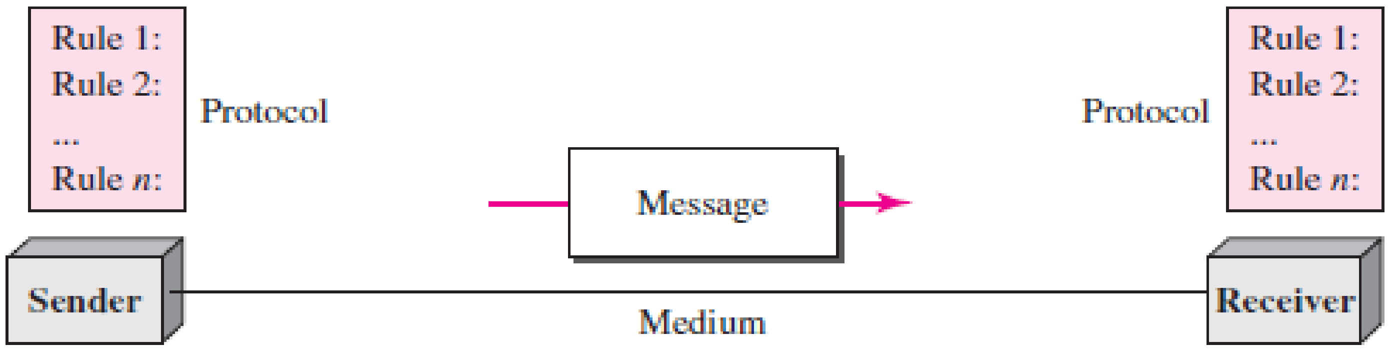
Effectiveness of data communication depends on 3 fundamental characteristics

Delivery

Accuracy

Timeliness

Components of Data communication

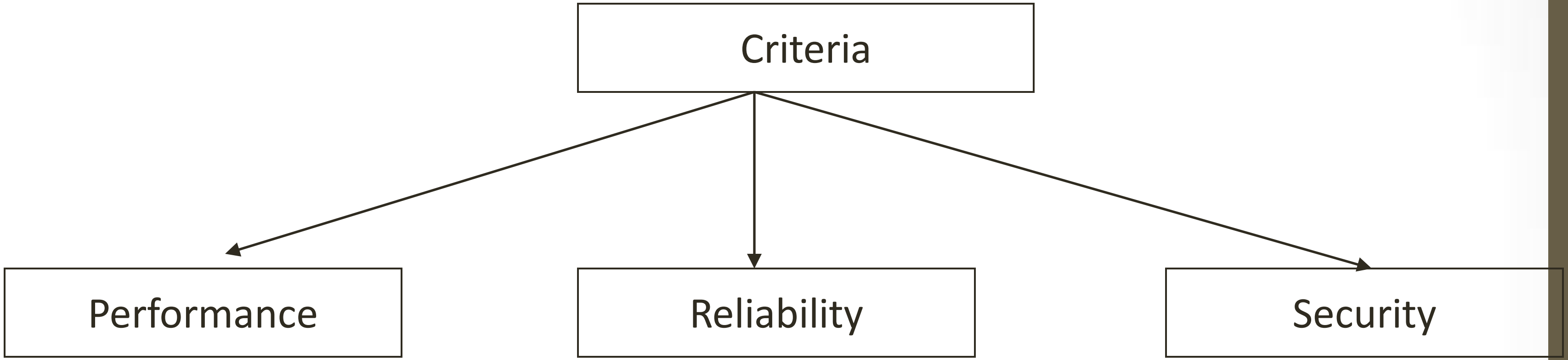


Sender:- Device that sends the message.
Receiver:- Device that receive the message.
Medium:-It is the physical path by which message travels from sender to receiver.
Protocol:-It is a set of rules that govern data communications.
Message:- Information which is to be communicated.

Networks

- A network is a collection of autonomous computer.
- The computer which cannot control by others or by outside forces is autonomous.
- Formal Definition: Computer Network
  - A series of **points** or **nodes interconnected** by communication paths. Networks can interconnect with other networks and contain subnetworks.
- Simple Definition: Computer Network
  - Connecting computers and/or devices in such a way that they can interact with each other.

Efficiency of Networking depends on the 3 Factors



Criteria

Performance

Reliability

Security

It can be measured in many ways. they are:

- Number of users
- Types of Transmission Media
- Hardware
- Software

It is measured by

- frequency of failure,
- the time it takes link to recover from a failure

It includes

- Unauthorized Access
- Viruses

Application of networking

- Marketing and sales
- Financial services
- Manufacturing
- Electronic messaging
- Directory services
- Information services
- Electronic data interchange
- Teleconferencing
- Cable television

Protocols

- Protocols is a set of rules that govern the exchange of data between two separate entities.
- Examples: TCP/IP, HTTP, FTP, SMTP

A protocol defines What is communicated, How it is communicated & When it is communicated

The Key Element of protocol is:

Syntax

Semantics

Timing

Syntax: It refers to the format of the data, i.e. meaning of the order in which they are presented.

Semantics:- It refers to the meaning of each section of the bits.

Timing:- it refers to when the data should be sent and how fast they can be sent.

Standards

- Standards are necessary to ensure that products from different manufacturer can work together as expected.

- A standard provides a model for development that makes it possible for a product to work regardless of the individual manufacturer.

Data communication standards fall into 2 categories:

Defacto (By Fact)

Dejure (By Law)

Defacto: Standards that have not been approved by an organized body but have been adopted as a standard.

De jure: standards that have been approved by an officially recognized body.

De facto standards are of two types

- **Proprietary** standards are those originally invented by a commercial organization as a basis for the operation of its products.
- **Non Proprietary** standards are those originally developed by groups or committees that have passed them into the public domain.

Standards organizations

Some of the organization involved in standards creation

- ISO (international standards organization)
- ITU-T (international telecommunications union-telecommunication standards sector)
- ANSI (American national standards institute)
- IEEE (institute of electrical and electronics engineers)
- EIA (electronic industries association)

TRANSMISSION MODES

TRANSMISSION MODES

- The term transmission mode is used to define the direction of signal flow between two linked devices.

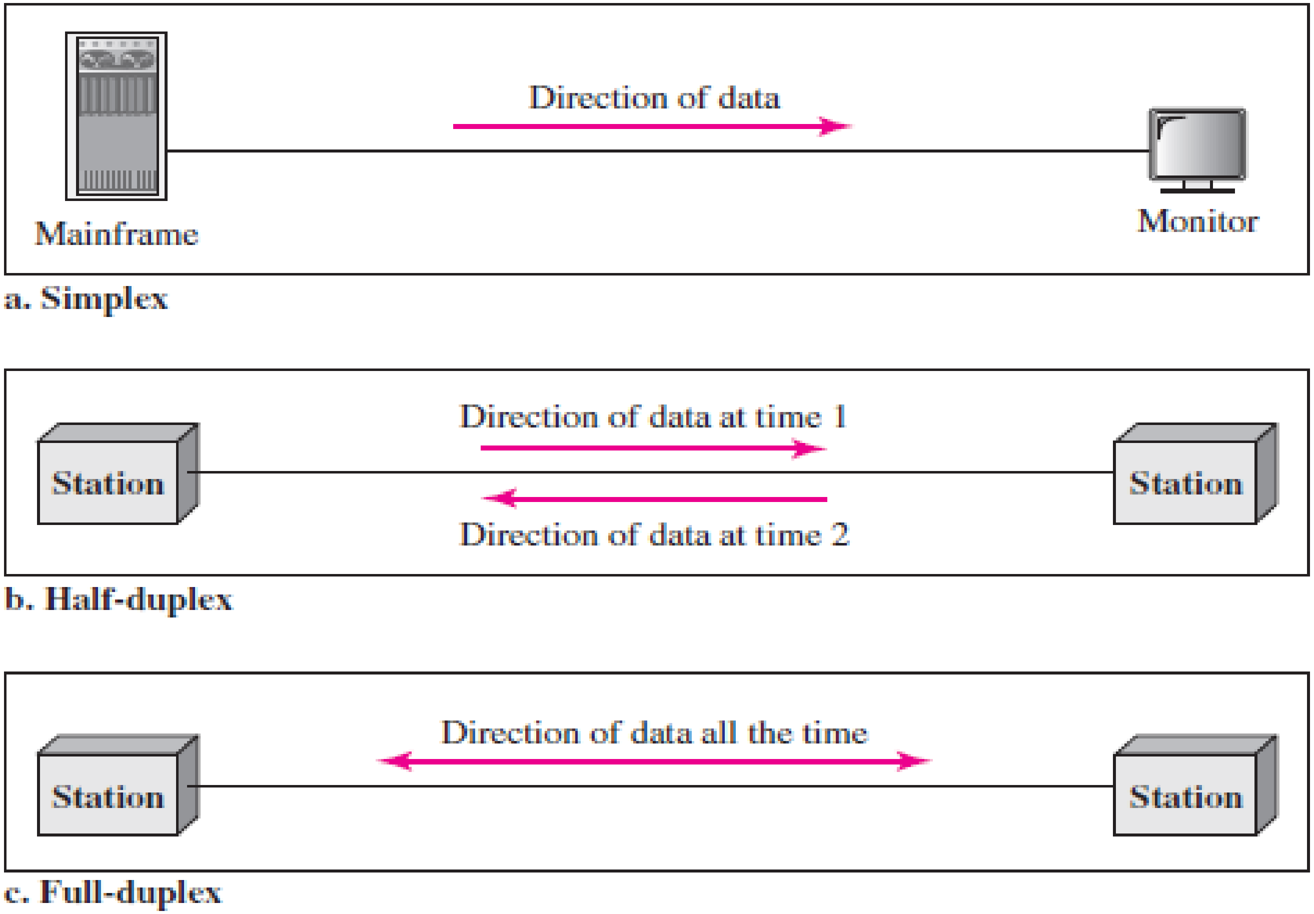
Types of transmission modes

Simplex: the communication is unidirectional, as on a one-way street. Ex: keyboard

Half duplex: each device can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. Ex: walkie-talkie

Full duplex: both stations can transmit and receive simultaneously. Ex: telephone

TRANSMISSION MODES


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

Line Configuration

Line configuration refers to the way two or more devices attach to the link.

A link is the physical connection i.e. the pathway that transfer the data from one device to another. There are 2 possible line configuration

Point-to-Point

Multipoint

Line Configuration

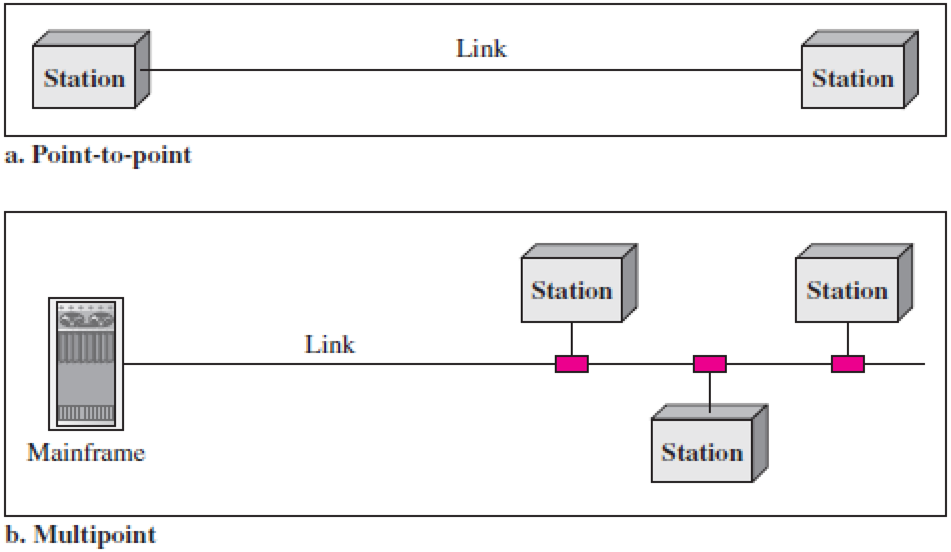
Point-to-Point

It provides a dedicated link between two devices. The entire capacity of the channel is reserved for transmission between those two devices.

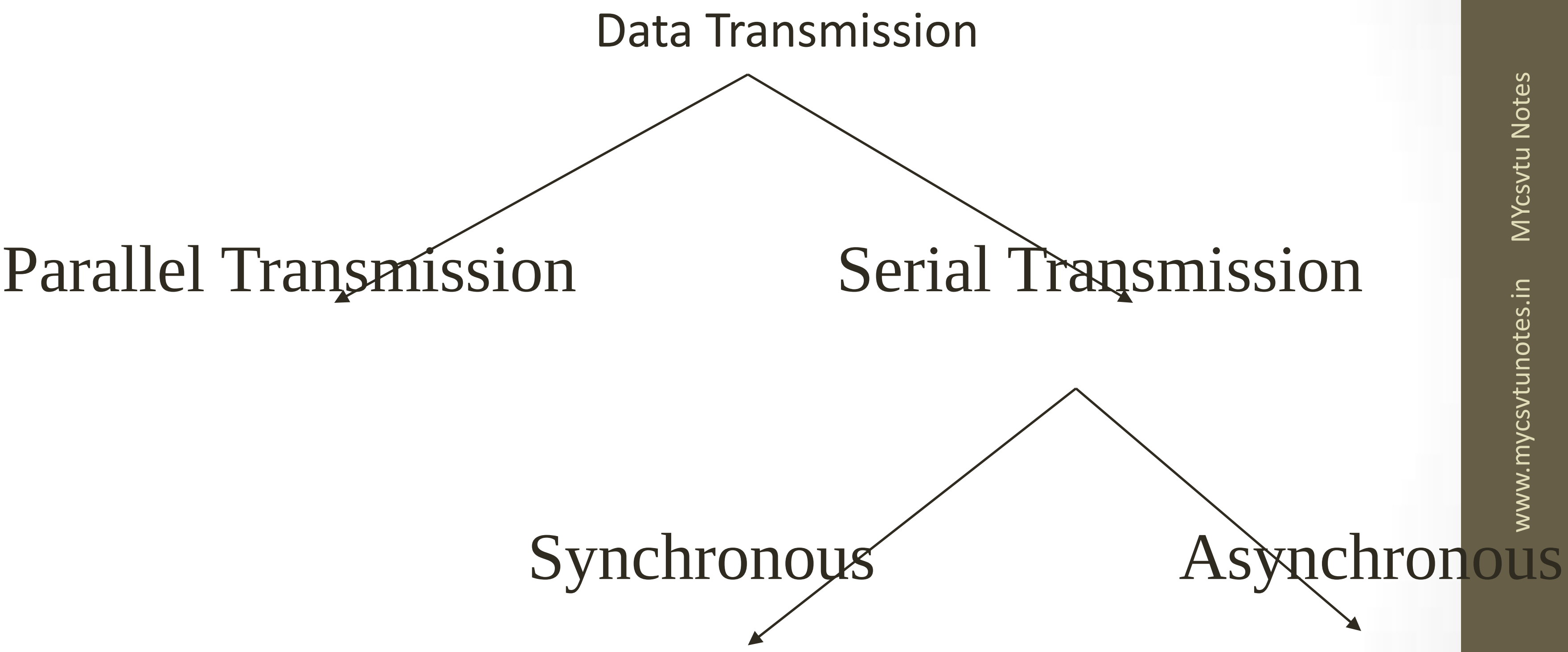
Multipoint

It is also known as multidrop line configuration, it is the one in which more than two specific devices share a single link.

Line Configuration



Data Transmission



Data Transmission

Parallel Transmission

Serial Transmission

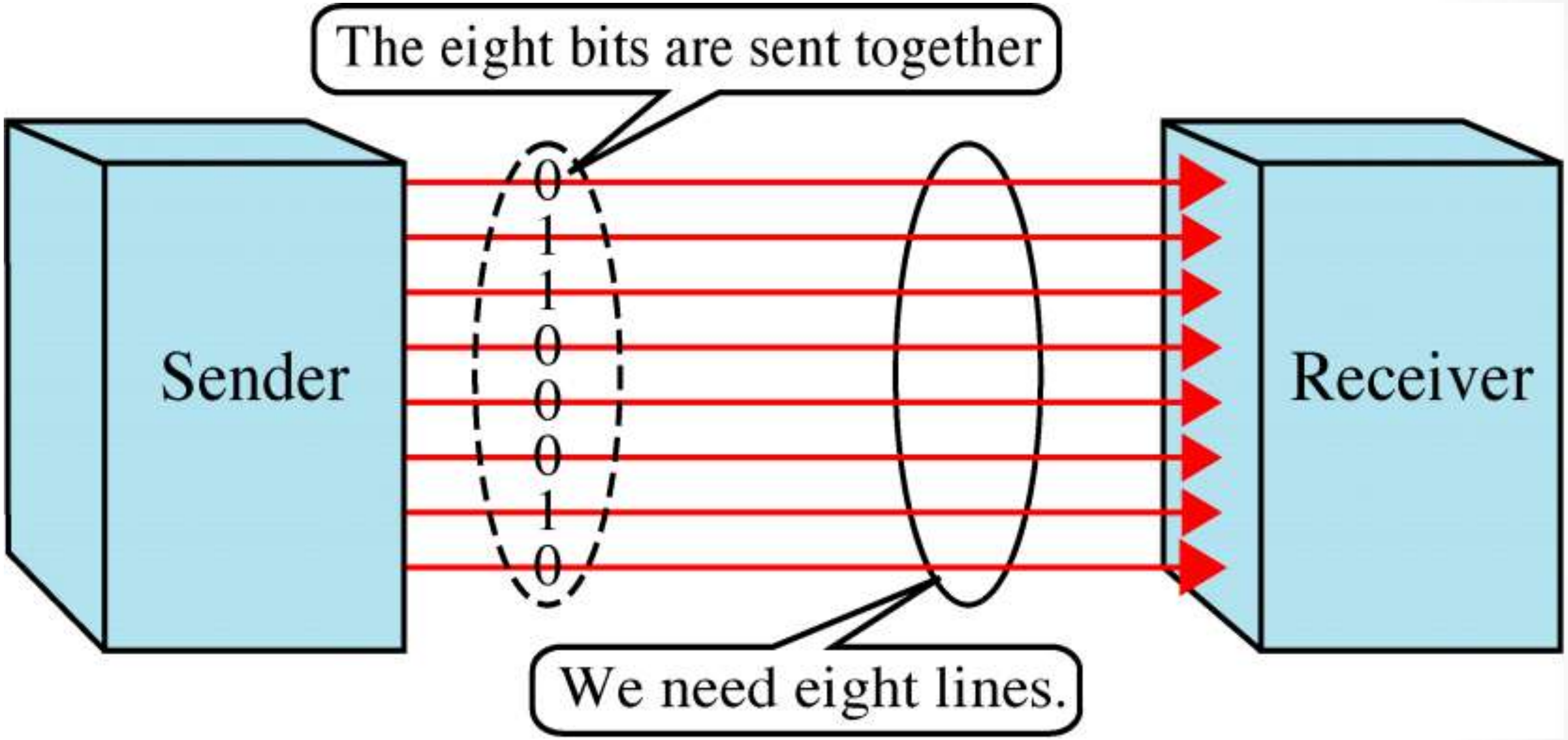
Synchronous

Asynchronous

Parallel Transmission

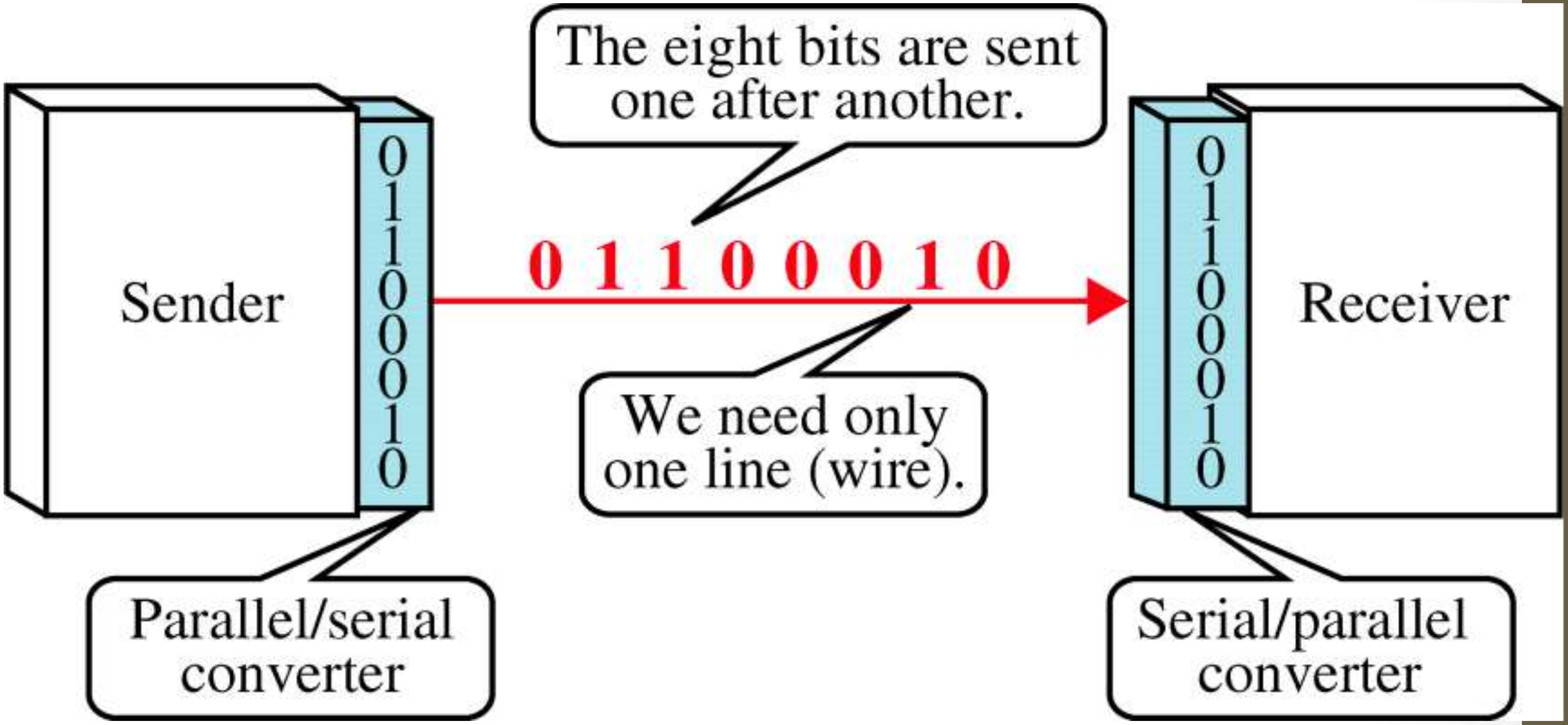
- Parallel connection means simultaneous transmission of *N* bits. These bits are sent simultaneously over *N* different channels (a channel being, for example, a wire, a cable or any other physical medium).

Parallel Transmission



Serial Transmission

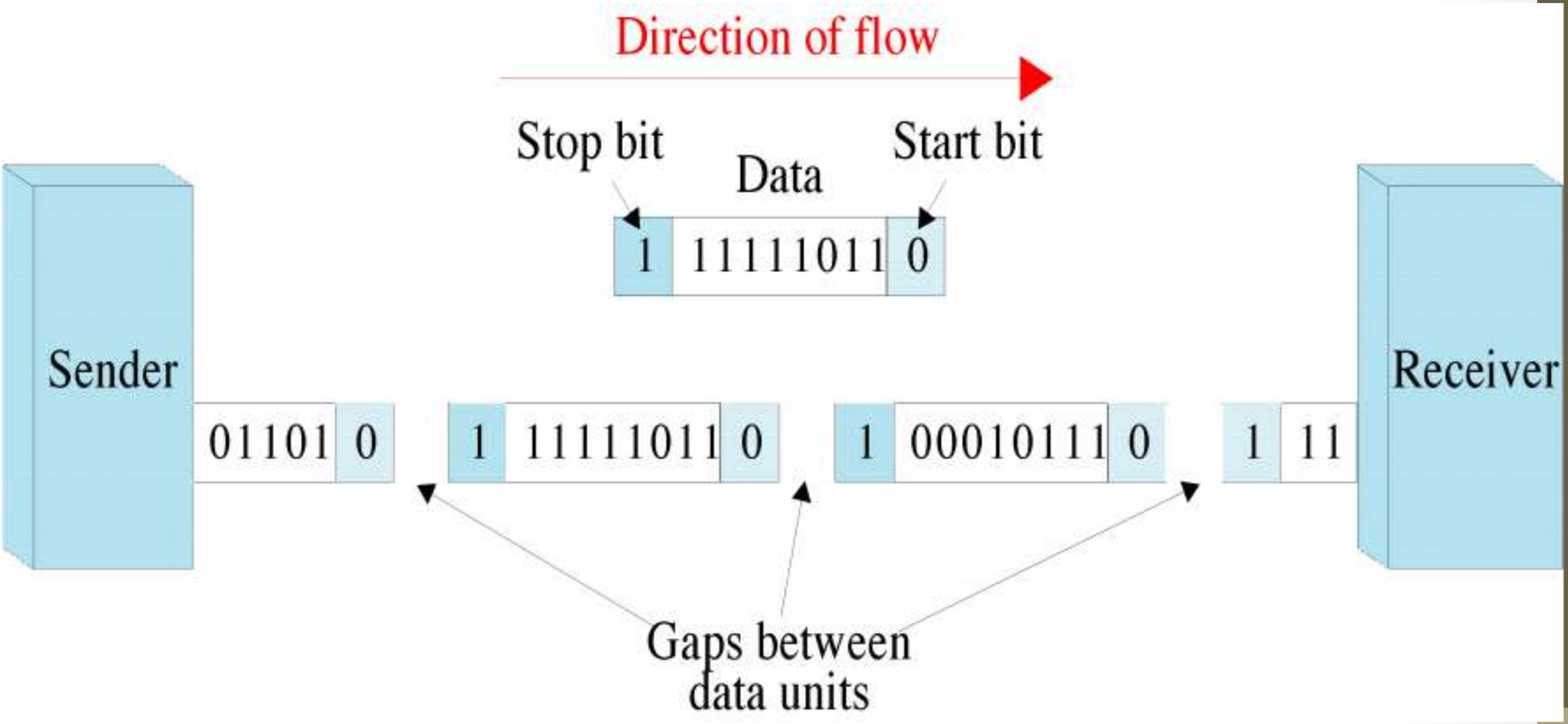
- In a serial connection, the data are sent one bit at a time over the transmission channel.


The eight bits are sent one after another.
Sender
0 1 1 0 0 0 1 0
0 1 1 0 0 0 1 0
Receiver
0 1 1 0 0 0 1 0
We need only one line (wire).
Parallel/serial converter
Serial/parallel converter

Asynchronous Transmission

- To alert the receiver that a new group of data is arriving, two extra bits are added one at the beginning which is known as start bit and the other one is at the end which is known as stop bit . There may be a gap between each byte.
- The start bit is always 0 and the stop bit is always 1.
- The start bit, stop bit and the gap alert the receiver to the beginning and end of each byte and allow it to synchronize with the data stream.

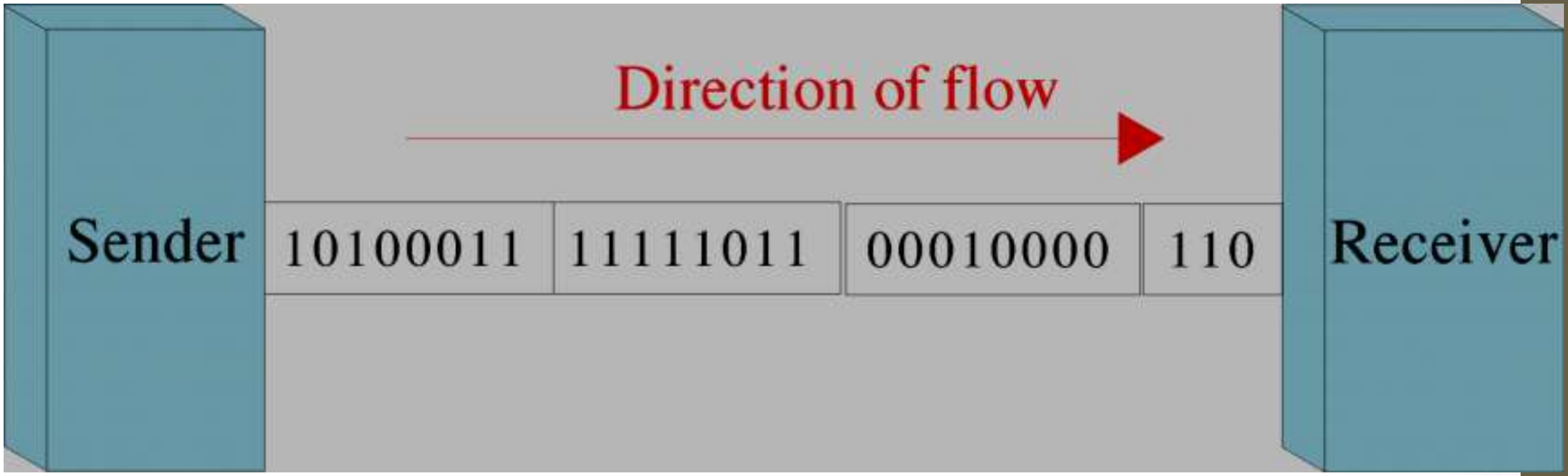
Asynchronous Transmisison



Synchronous Transmission

The transmitter and receiver are paced by the same clock. The receiver continuously receives the information at the same rate the transmitter sends it. This is why the transmitter and receiver are paced at the same speed.

Synchronous Transmission



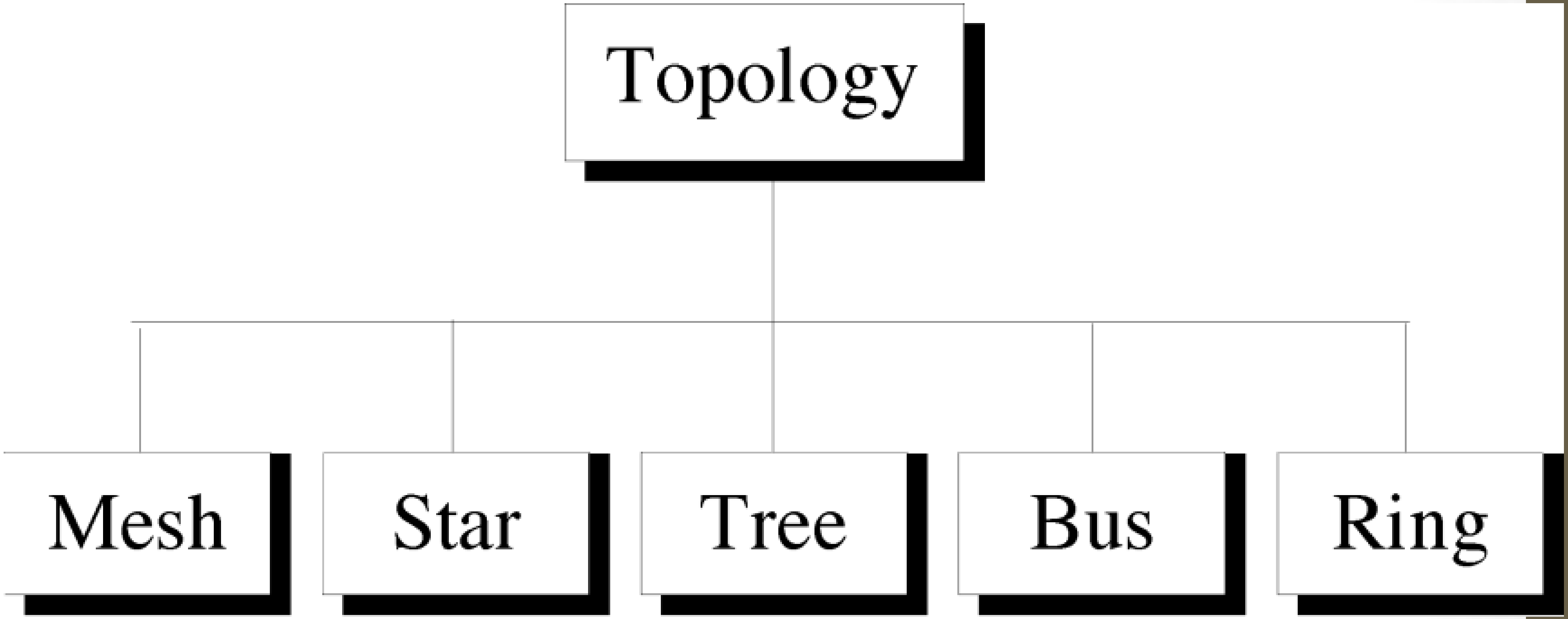
NETWORK TOPOLOGIES

NETWORK TOPOLOGY

- It is the geometrical representation of how the nodes in the network are attached to each other.

Network Topologies (continued)

- Four basic criteria
  - Basic cost
    - Expense required to link various sites in system
  - Communications cost
    - Time required to send message from one site to another
  - Reliability
    - Assurance of site communication if link or site fails
  - User environment
    - Critical parameters for successful business investment



Topology

Mesh

Star

Tree

Bus

Ring

Mesh Topology

- A mesh network has point-to-point connections between every device in the network.
- There are two types of mesh topology they are

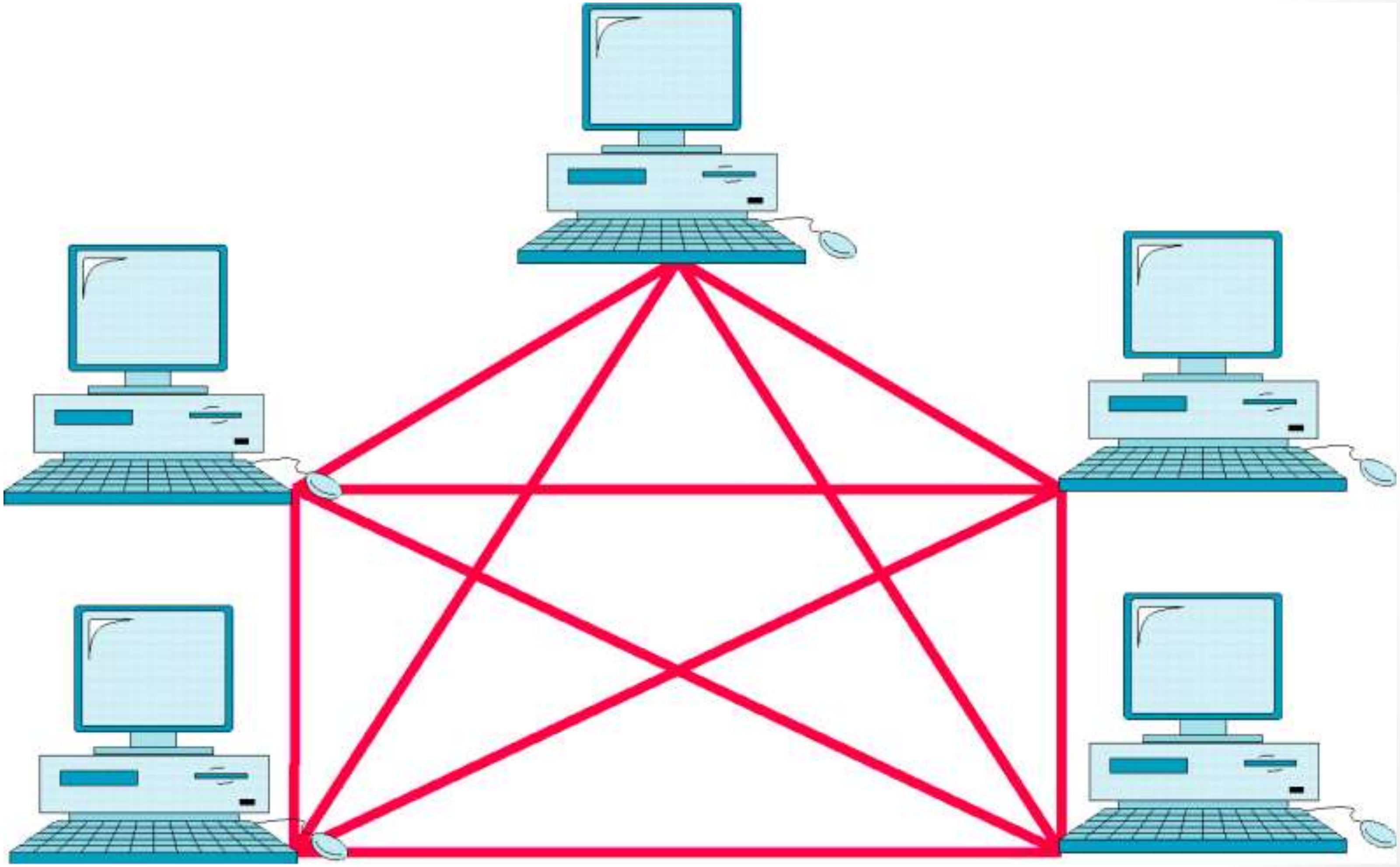
  Fully Connected Mesh Topology

  Partial Connected Mesh Topology

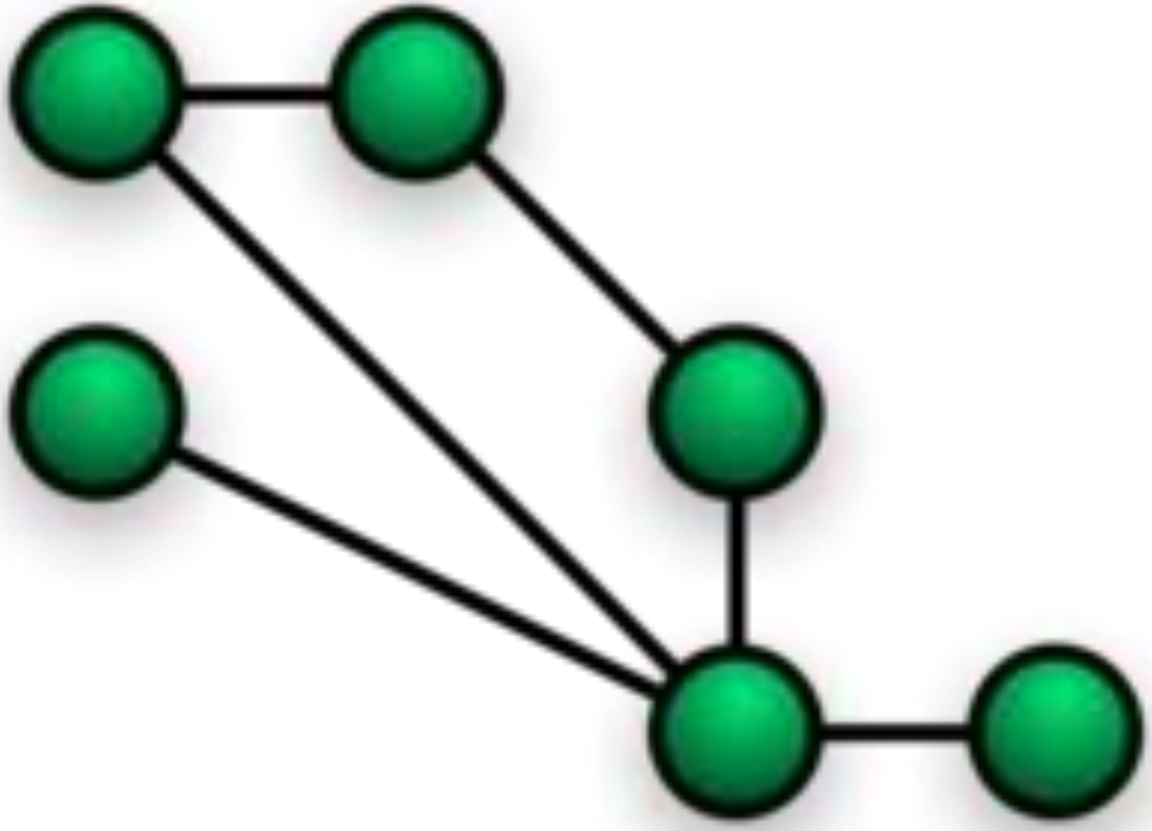
Fully Connected Mesh Topology: Each of the nodes of network is connected to each of the other nodes in the network. The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected.

Partial Connected Mesh Topology: Some of the nodes of the network are connected to more than one other node in the network with a point to point link.

Fully Connected Mesh Topology



Partial Connected Mesh Topology



Advantages:

Eliminating the traffic problems.

Mesh topology is robust.

It provides security.

Point-to-point links make fault identification and fault isolation easy.

Disadvantages:

The amount of cabling and the ports required

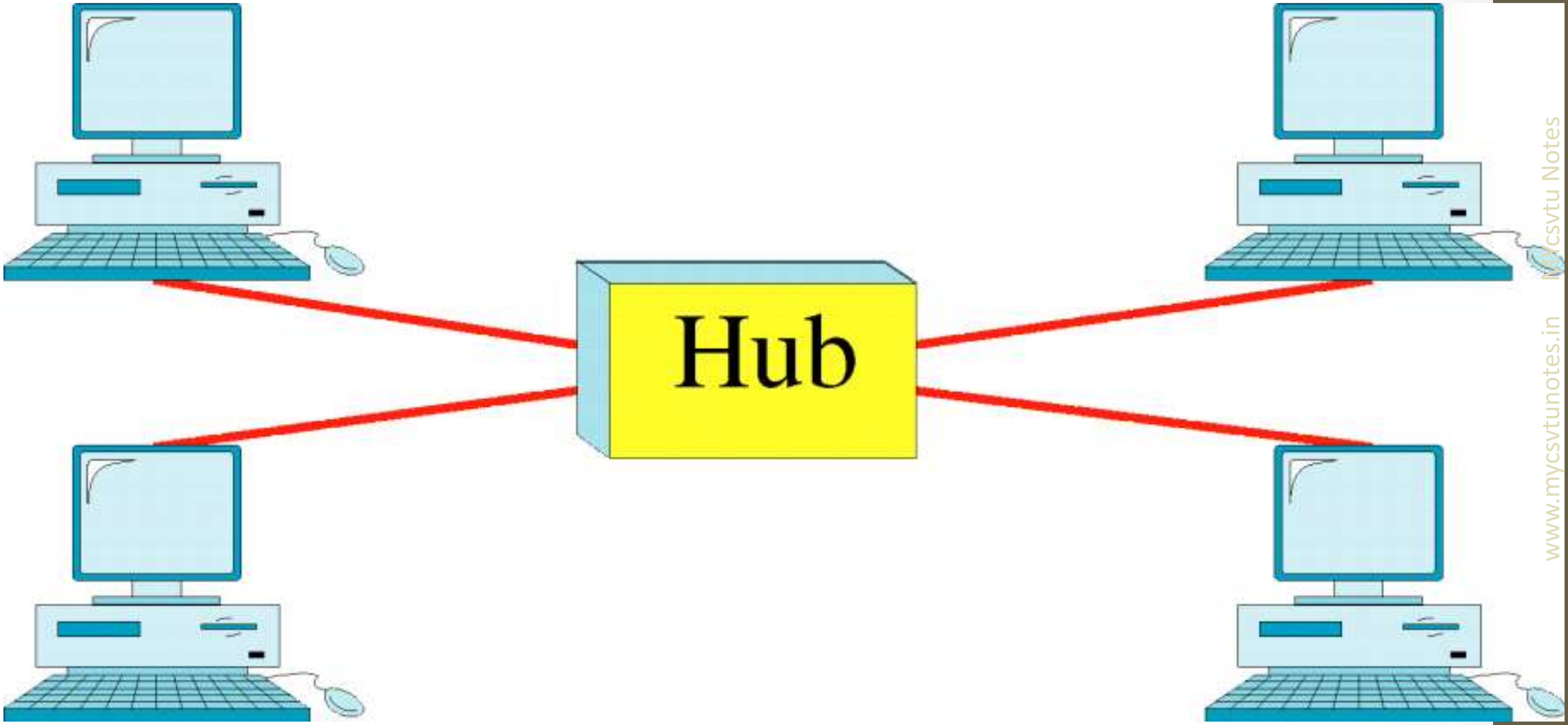
Application

- One **practical example of a mesh topology** is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

- In a star network, several devices or computers are connected to one centralized computer .

Star Topology



Advantages

- A star topology is less expensive than a mesh topology.
- In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active.
- Easy fault identification and fault isolation.

Disadvantage

- Large cable length
- If the hub fails then it affects the whole network.
- Difficult to expand

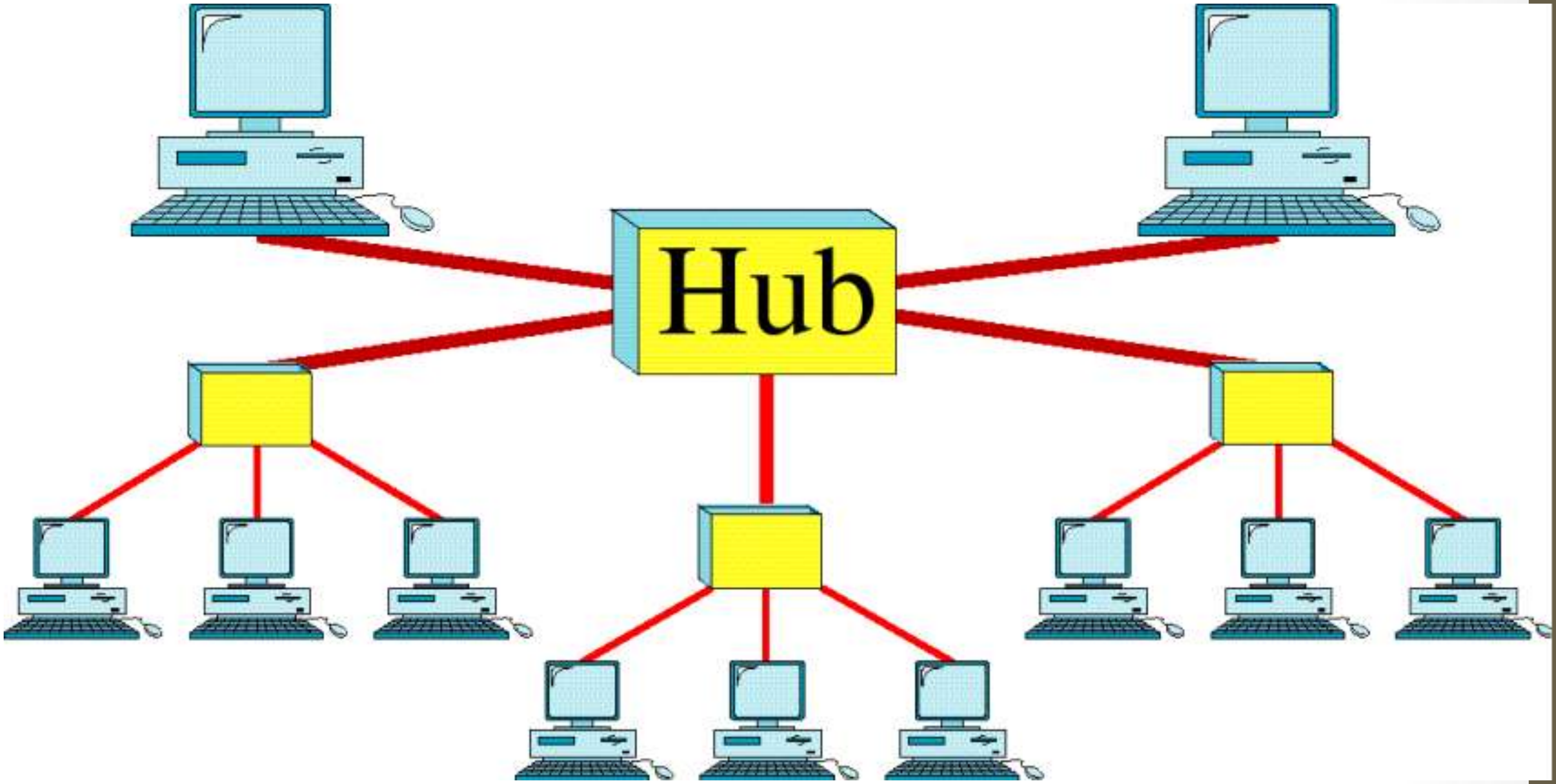
Application

The star topology is used in local-area networks (LANs).

Tree Topology

- In a tree network, several devices or computers are linked in a hierarchical fashion.
- It is also known as hierarchical network.

Tree Topology



Advantages

- Easy to extend
- It allows more devices to be attached to a single central hub.
- It allows the network to isolate and prioritize communication from different computers.

Disadvantage

- Dependent on the root.

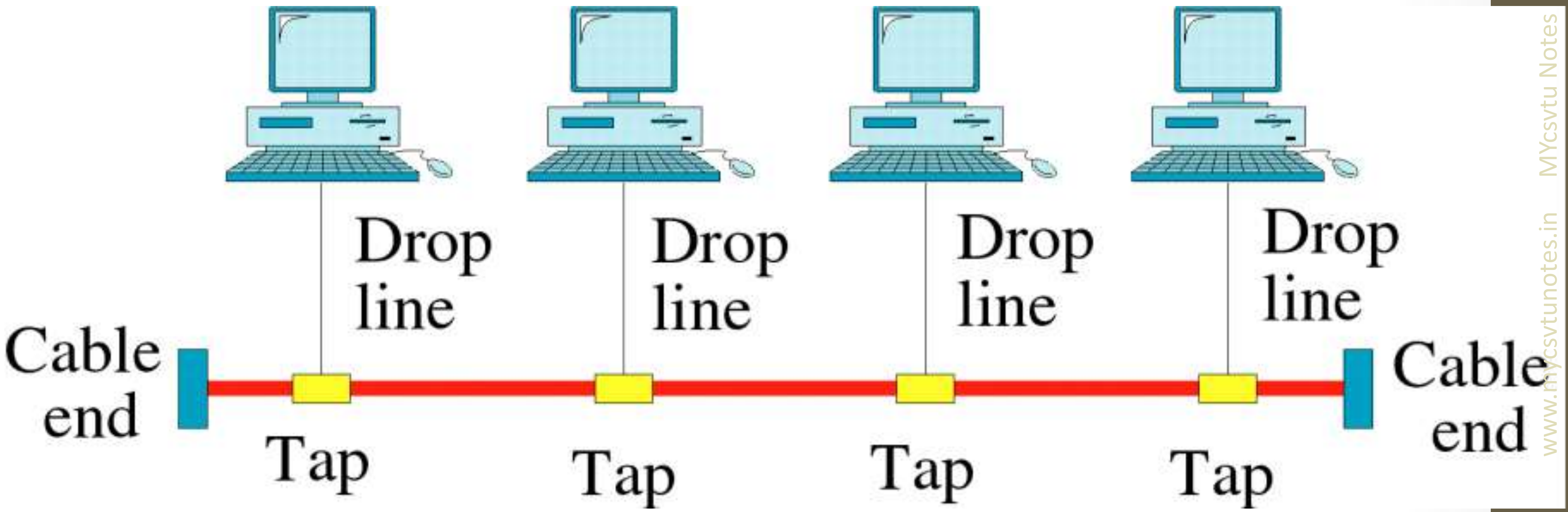
Application

It can be seen in cable TV.

Bus Topology

- In a bus network, each computer is connected to a single communication cable via an interface and every computer can directly communicate with every other computer or device in the network.

Bus Topology



Advantages

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.
- Easy to extend

Disadvantages

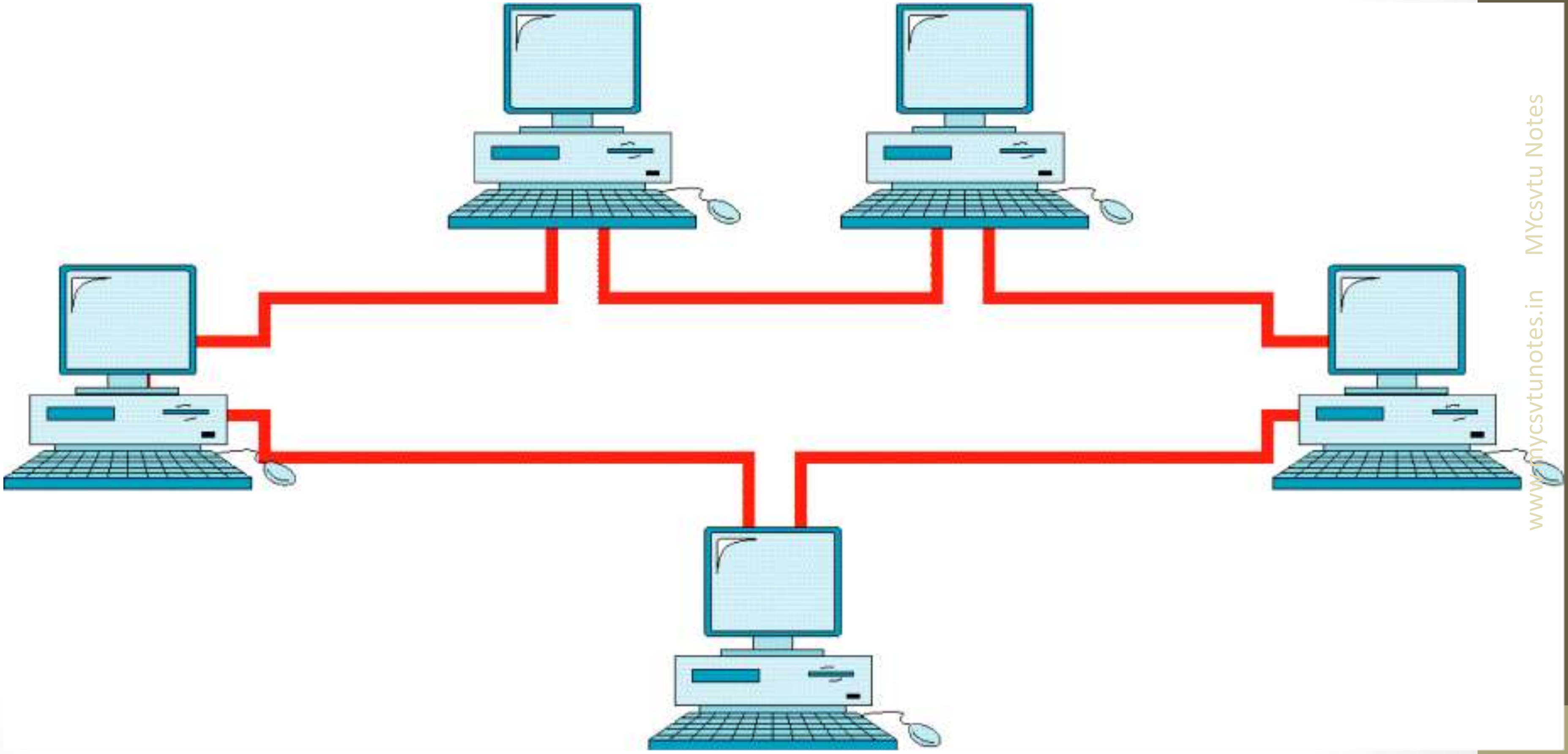
- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

Bus topology was the one of the first topologies used in the design of early local area networks.

Ring Topology

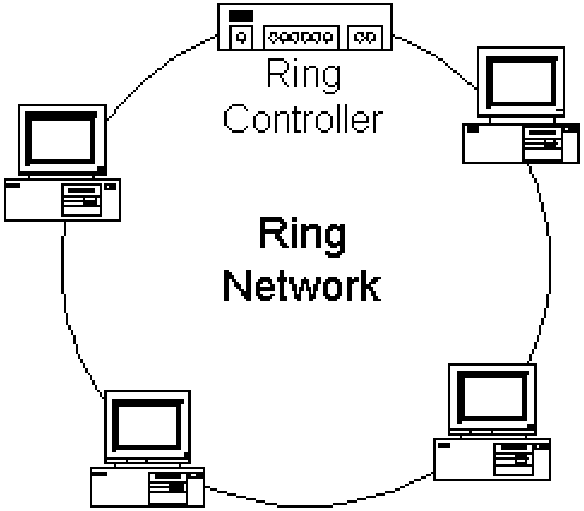
- In a ring network, several devices or computers are connected to each other in a closed loop by a single communication cable.

Ring Topology



Examples of Ring Networks

- Simple Example of a Ring Network:



Advantages

It is relatively easy to install and reconfigure.

Short cable length compare to bus and star.

In this fault isolation is simplified.

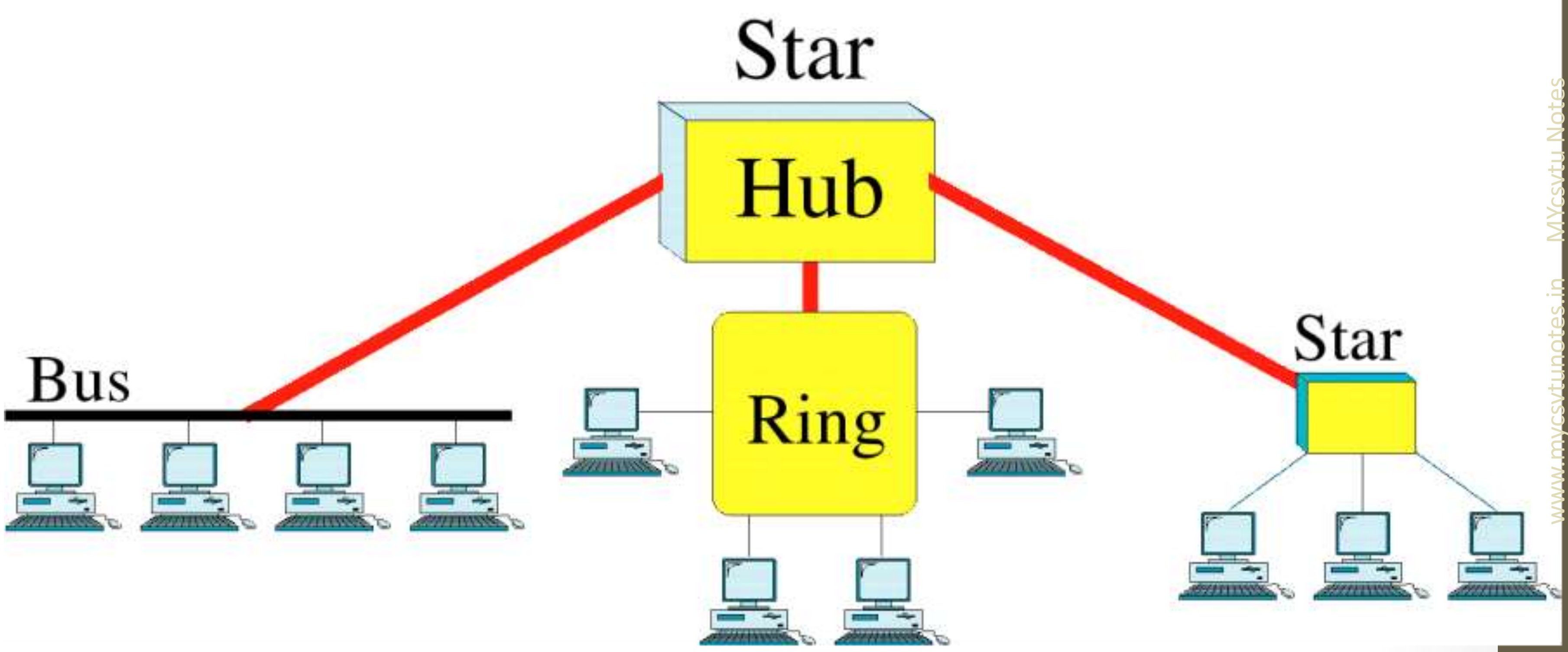
Disadvantages

Unidirectional traffic may be disadvantage.

A break in the ring can disable the entire network.

Applications ???????????

Hybrid Topology

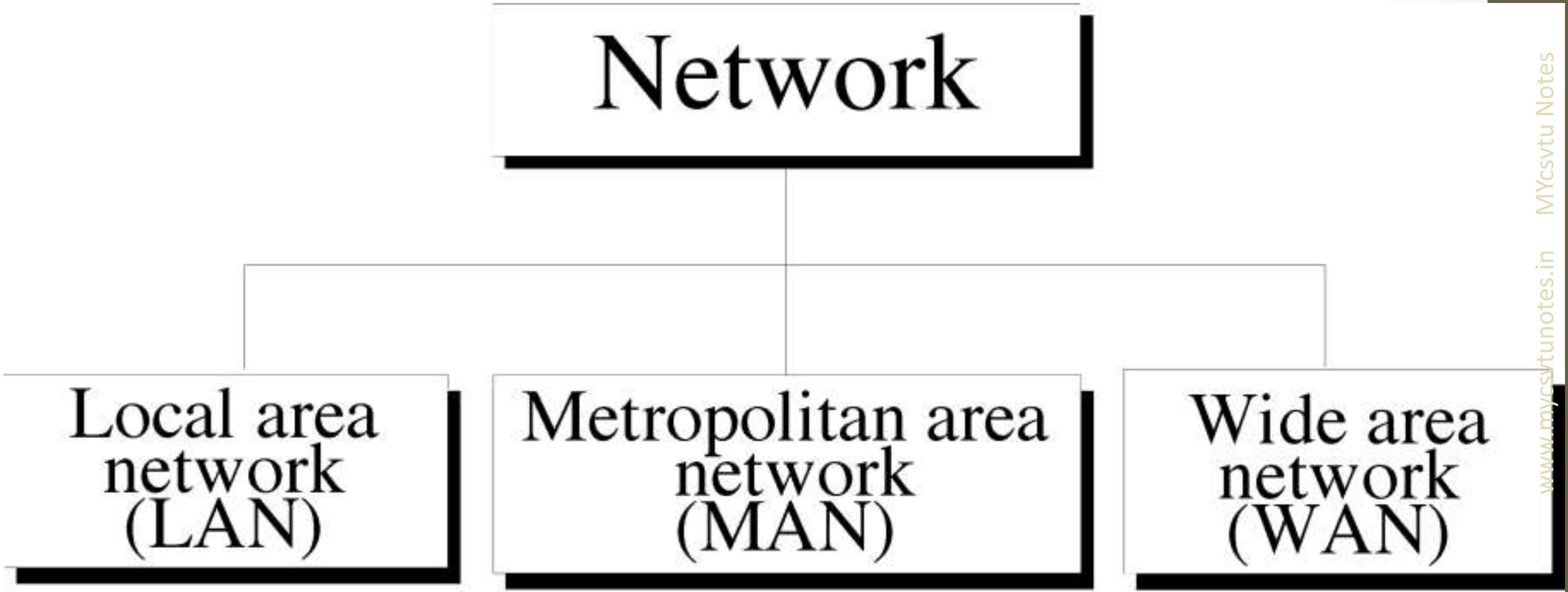


Network Topologies (continued)

Four basic criteria

- Basic cost
  - Expense required to link various sites in system
- Communications cost
  - Time required to send message from one site to another
- Reliability
  - Assurance of site communication if link or site fails
- User environment
  - Critical parameters for successful business investment

Network Categories



Network

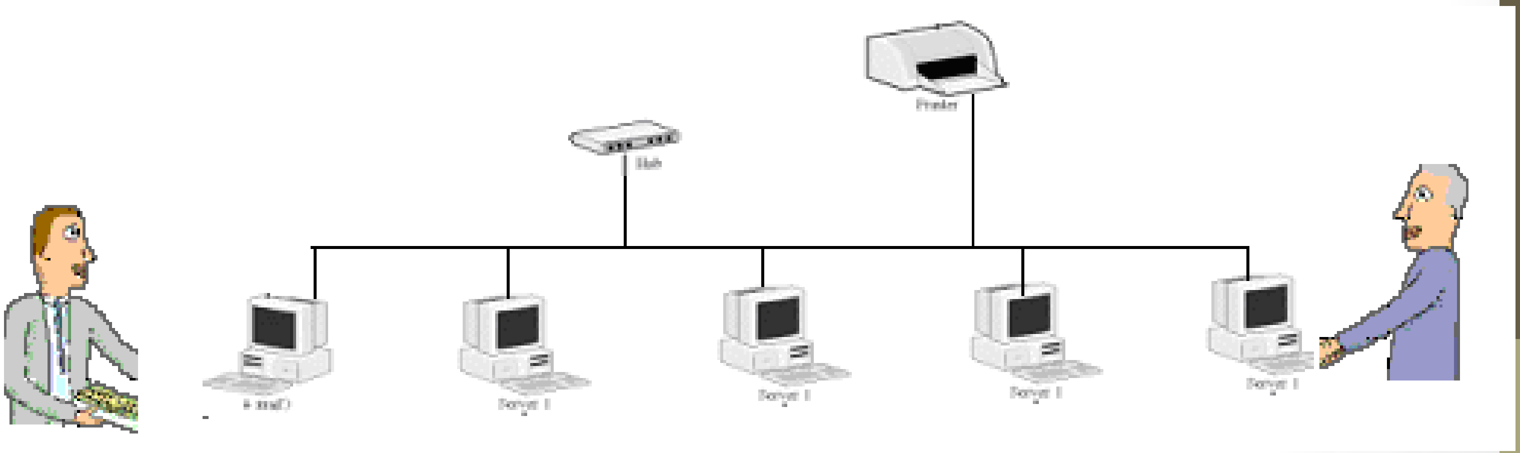
Local area network (LAN)

Metropolitan area network (MAN)

Wide area network (WAN)

LAN

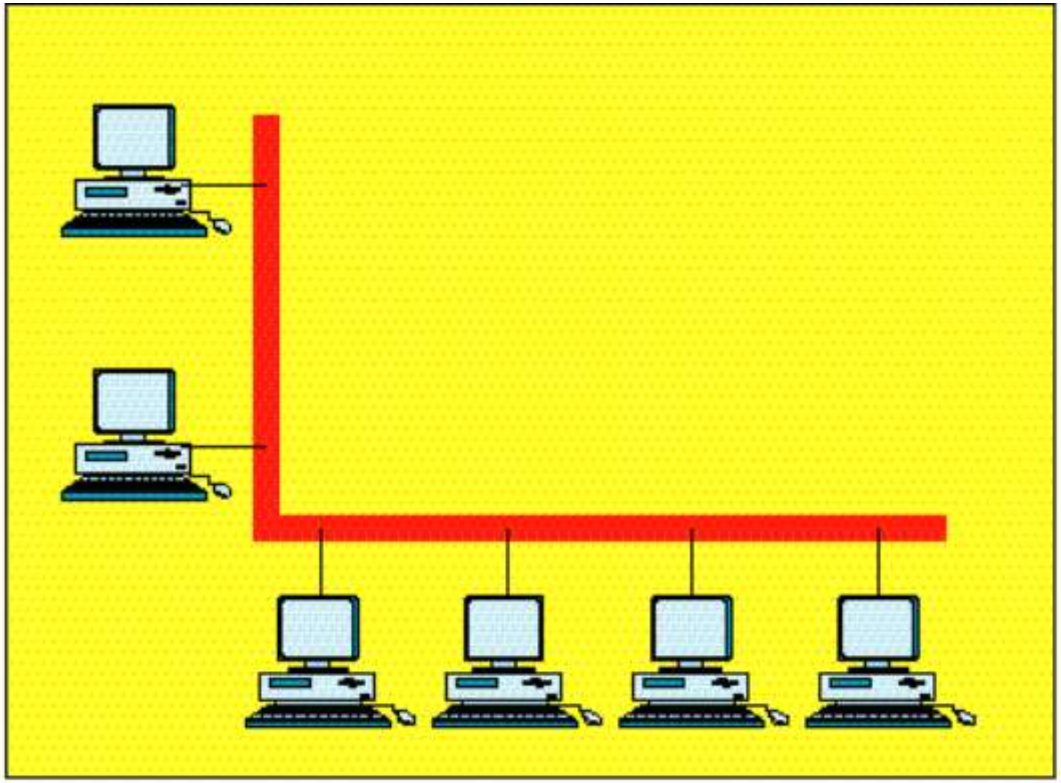
A Local Area Network connects network devices over a relatively short distance. A network in office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs.



Local Area Network (continued)

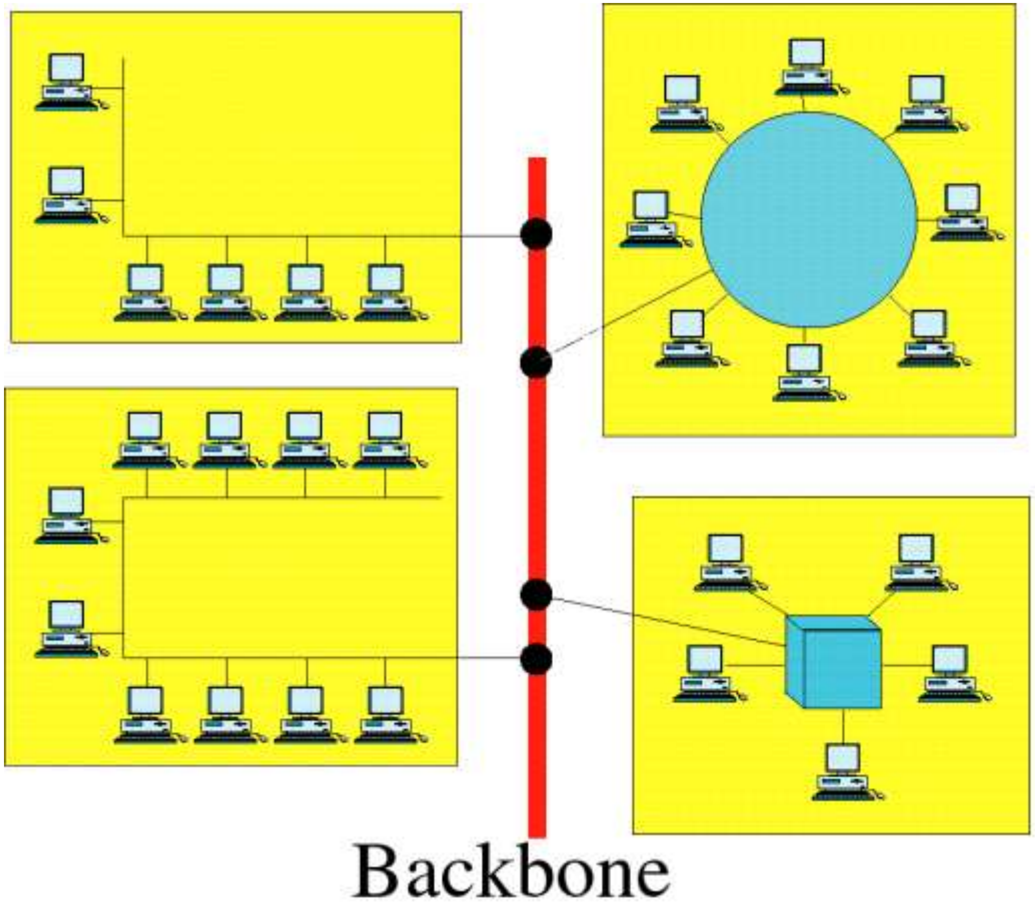
- Data rates: 100 Mbps to more than 40 Gbps
- Close physical nature
  - Very high-speed transmission
- Star, ring, bus, tree, and hybrid
  - Normally used
- Transmission medium: varies
- Factors determining transmission medium
  - Cost, data rate, reliability, number of devices supported, distance between units

Local Area Network



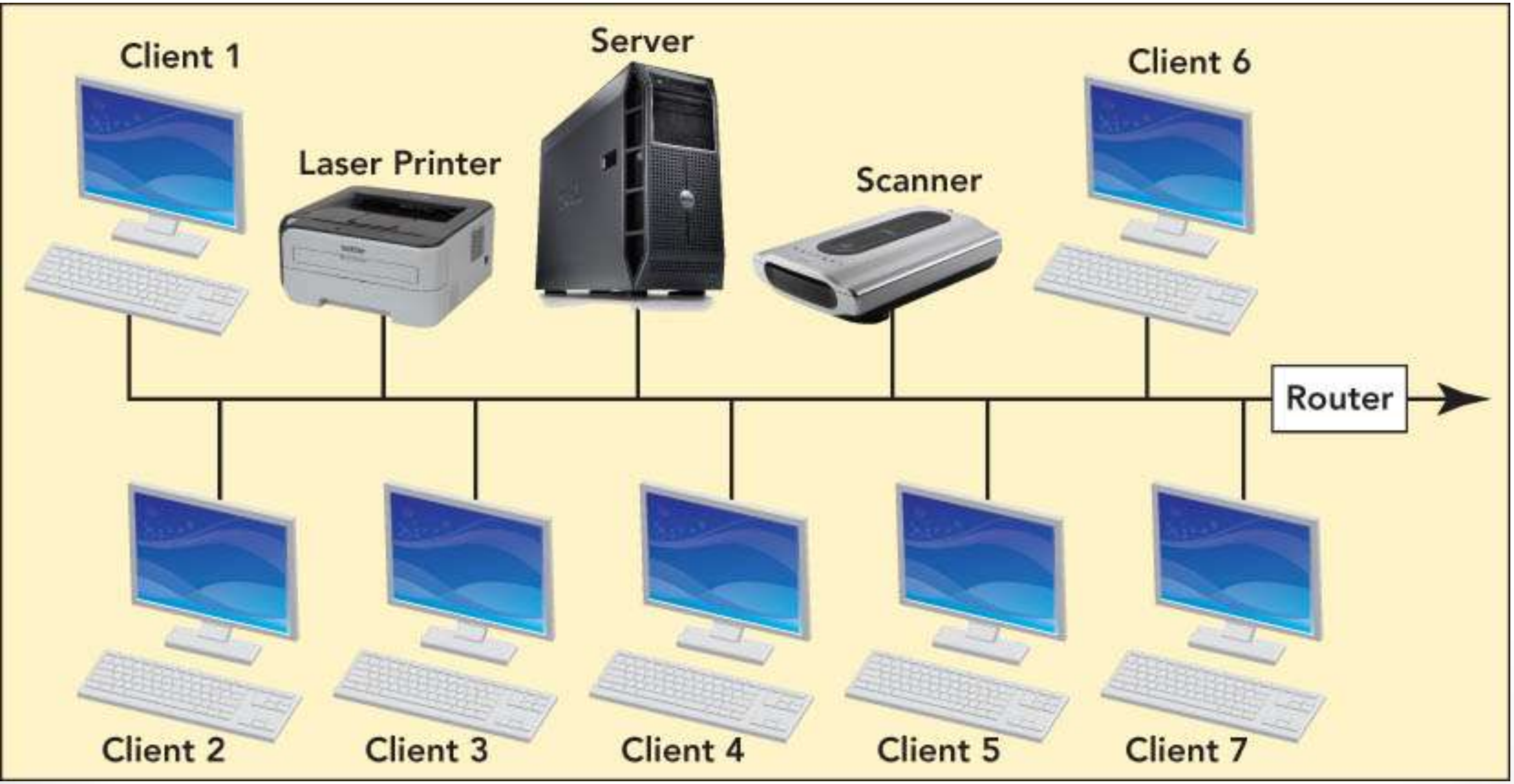
Single building LAN

Local Area Network

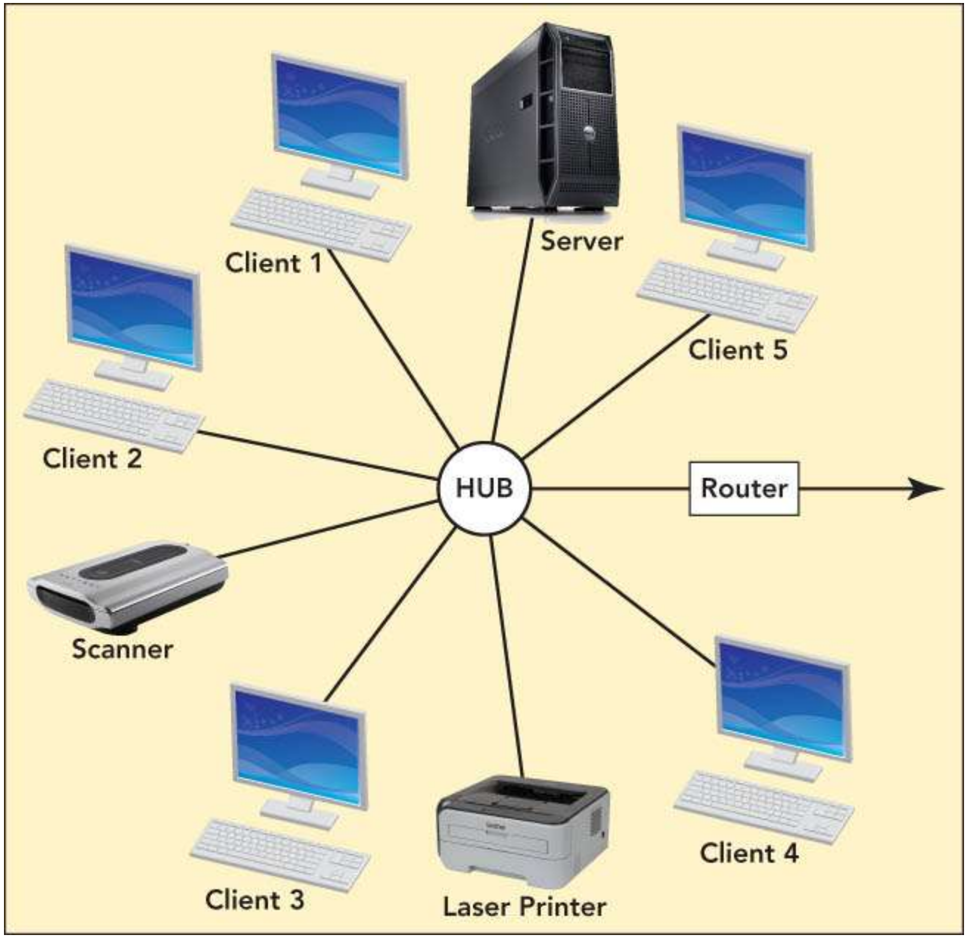


Multiple building LAN

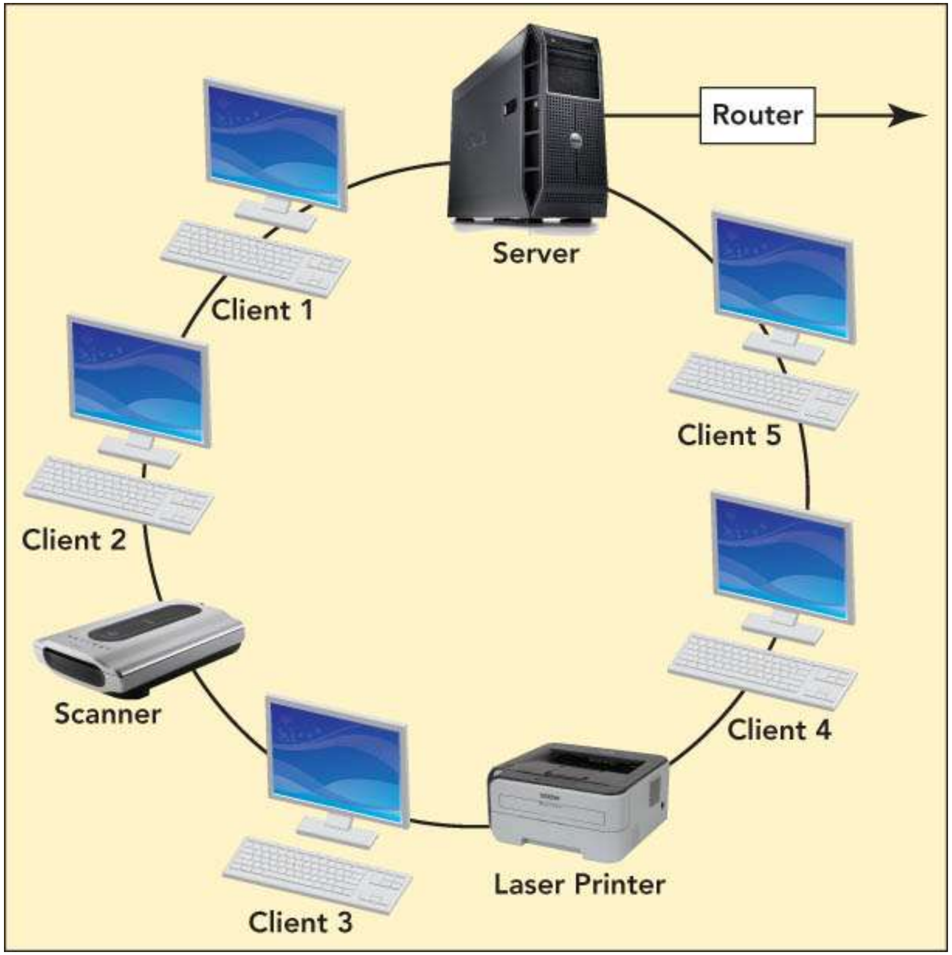
Local Area Networks



Local Area Networks



Local Area Networks



Advantages of connecting computers in a LAN

- Workstations can share peripheral devices like printers. This is cheaper than buying a printer for every workstations.
- Workstations do not necessarily need their own hard disk or CD-ROM drives which make them cheaper to buy than stand-alone PCs.
- User can save their work centrally on the network’s file server. This means that they can retrieve their work from any workstation on the network. They don’t need to go back to the same workstation all the time.
- Users can communicate with each other and transfer data between workstations very easily.
- One copy of each application package such as a word processor, spreadsheet etc. can be loaded onto the file and shared by all users. When a new version comes out, it only has to be loaded onto the server instead of onto every workstation.

Disadvantages of connecting computers in a LAN

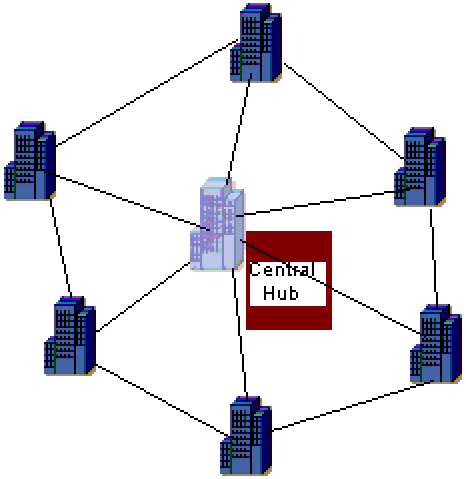
- Special security measures are needed to stop users from using programs and data that they should not have access to;
- Networks are difficult to set up and need to be maintained by skilled technicians.
- If the file server develops a serious fault, all the users are affected, rather than just one user in the case of a stand-alone machine.

In contrast to WAN

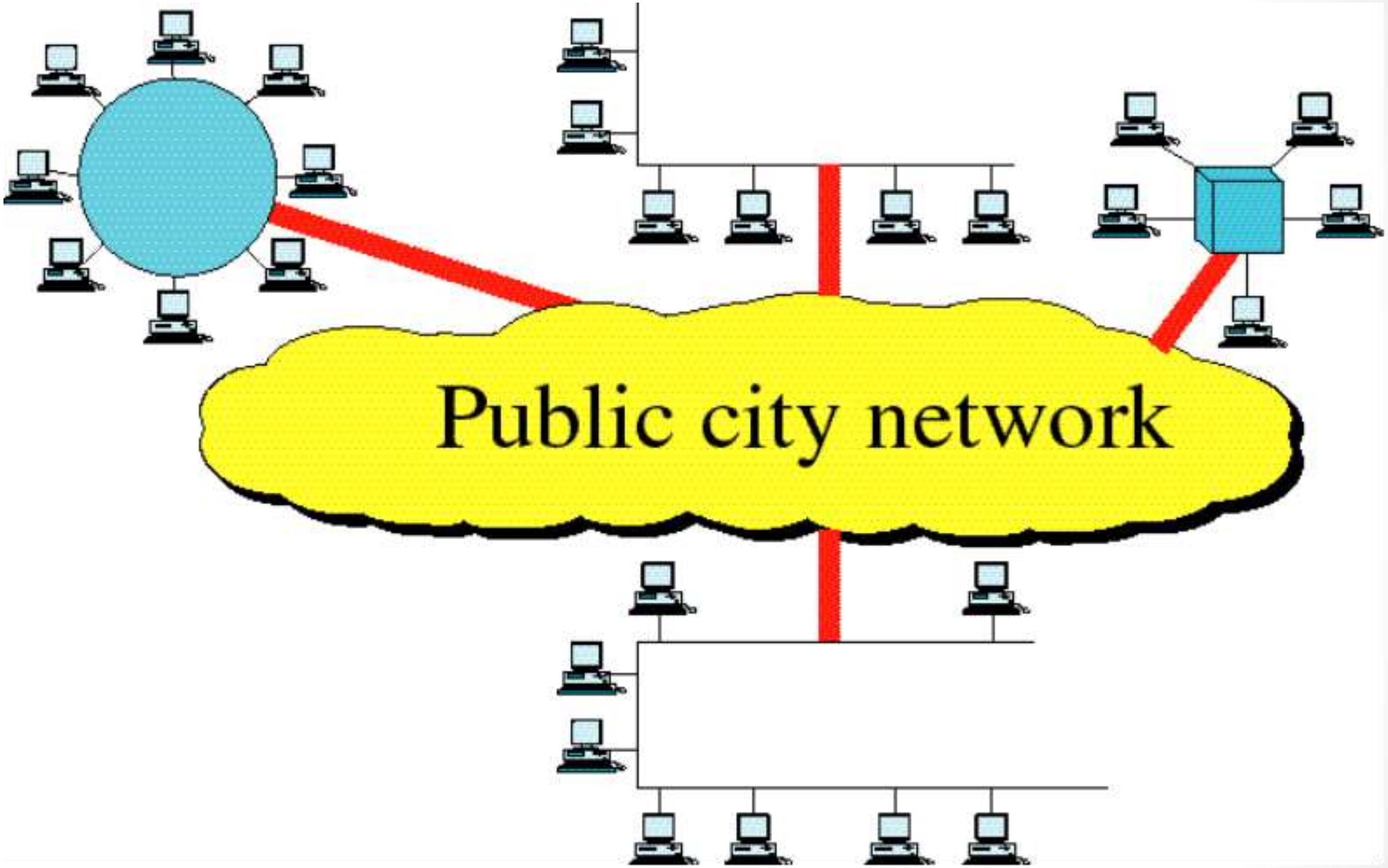
- Higher data-transfer rates,
- smaller geographic area,
- lack of a need for leased telecommunication lines

MAN

- The interconnection of networks in a city into a single larger network will be termed as MAN.
- It is also used to mean the interconnection of several local area networks.
- A MAN connects an area larger than a LAN.

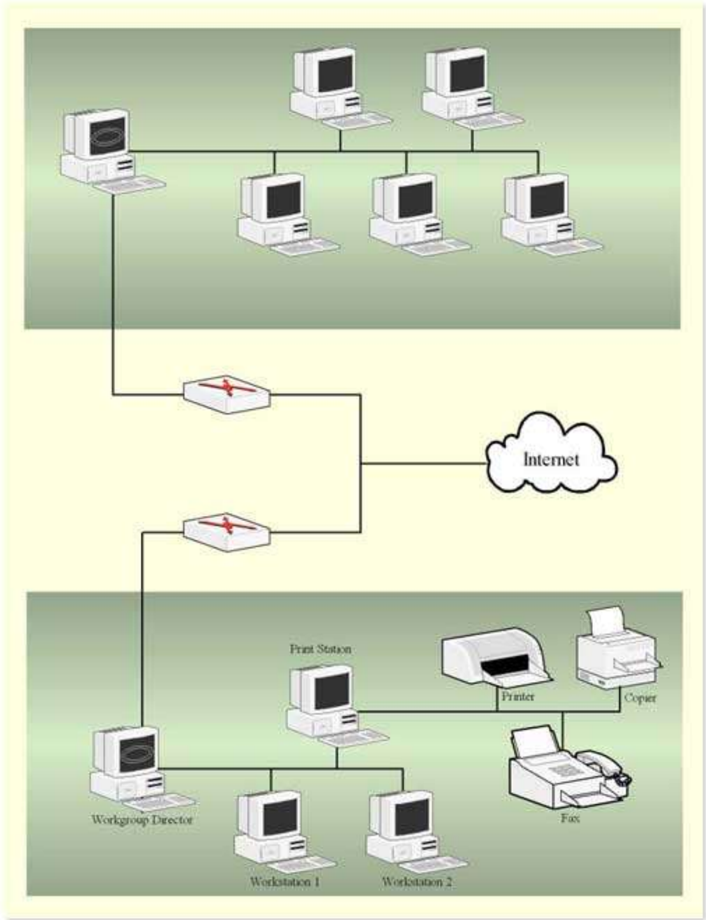


Metropolitan Area Network



WAN

- Wide Area Network is a collection of networks spread over a geographical area.
- The interconnected networks may be anywhere from several hundred miles away to each other.
- A WAN connects an area larger than a MAN.



Wide Area Network

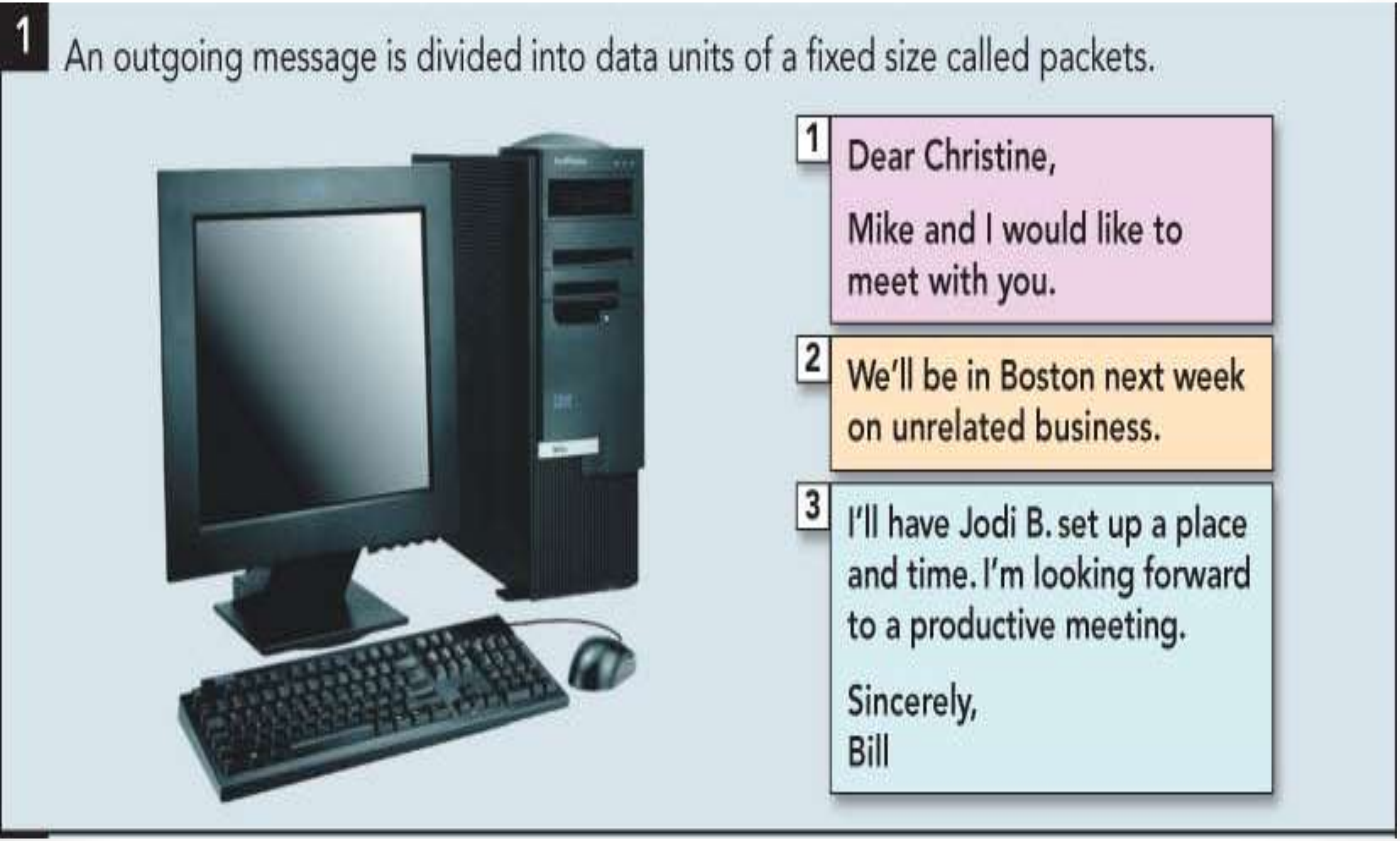
Advantages of a WAN

- Covers a large geographical area so long distance businesses can connect on the one network
- Shares software and resources with connecting workstations

Disadvantages of a WAN

- Are expensive and generally slow
- Need a good firewall to restrict outsiders from entering and disrupting the network

Wide Area Networks



1 An outgoing message is divided into data units of a fixed size called packets.

1 Dear Christine,

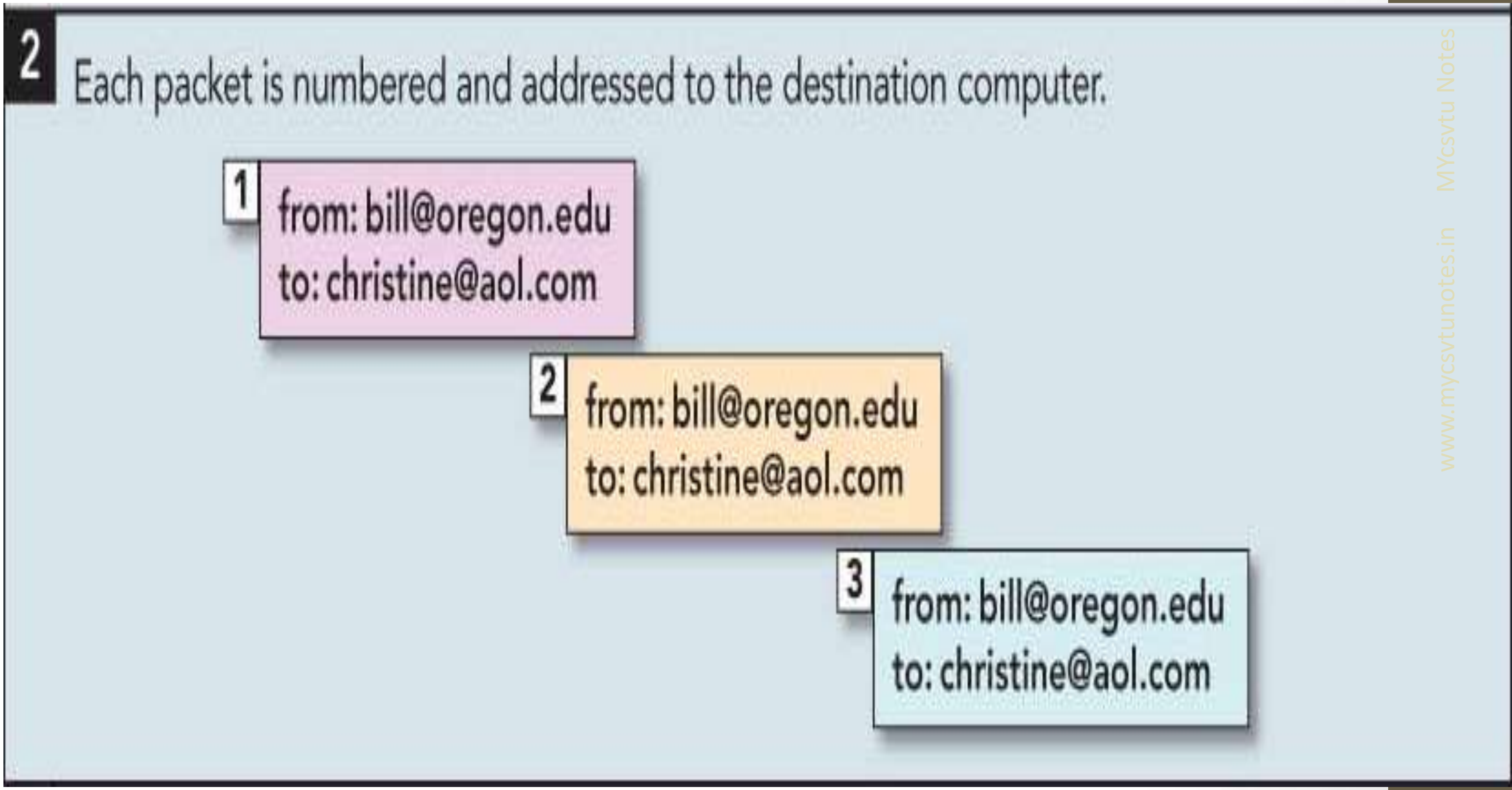
Mike and I would like to meet with you.

2 We'll be in Boston next week on unrelated business.

3 I'll have Jodi B. set up a place and time. I'm looking forward to a productive meeting.

Sincerely,
Bill

Wide Area Networks



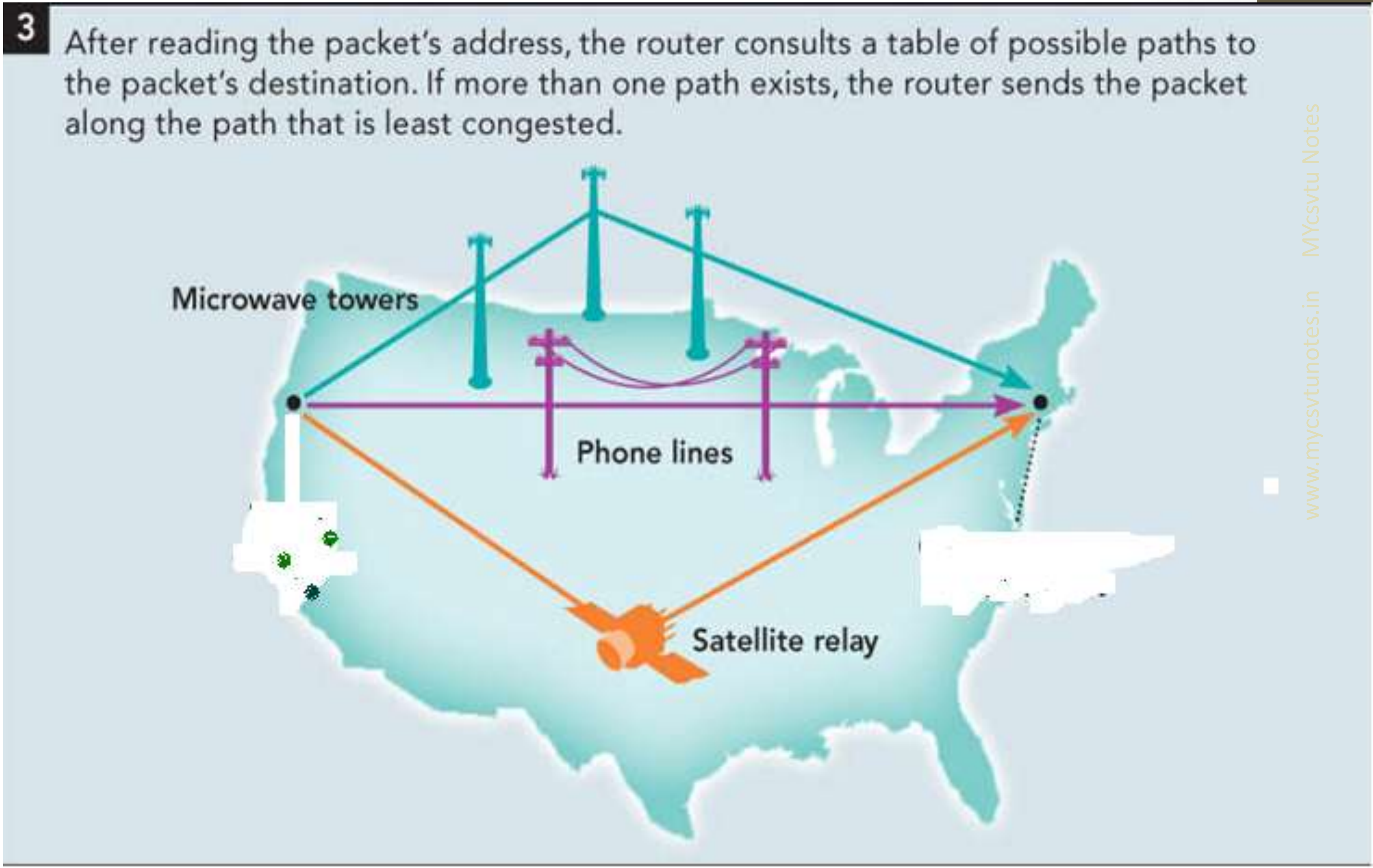
2 Each packet is numbered and addressed to the destination computer.

1 from: bill@oregon.edu
to: christine@aol.com

2 from: bill@oregon.edu
to: christine@aol.com

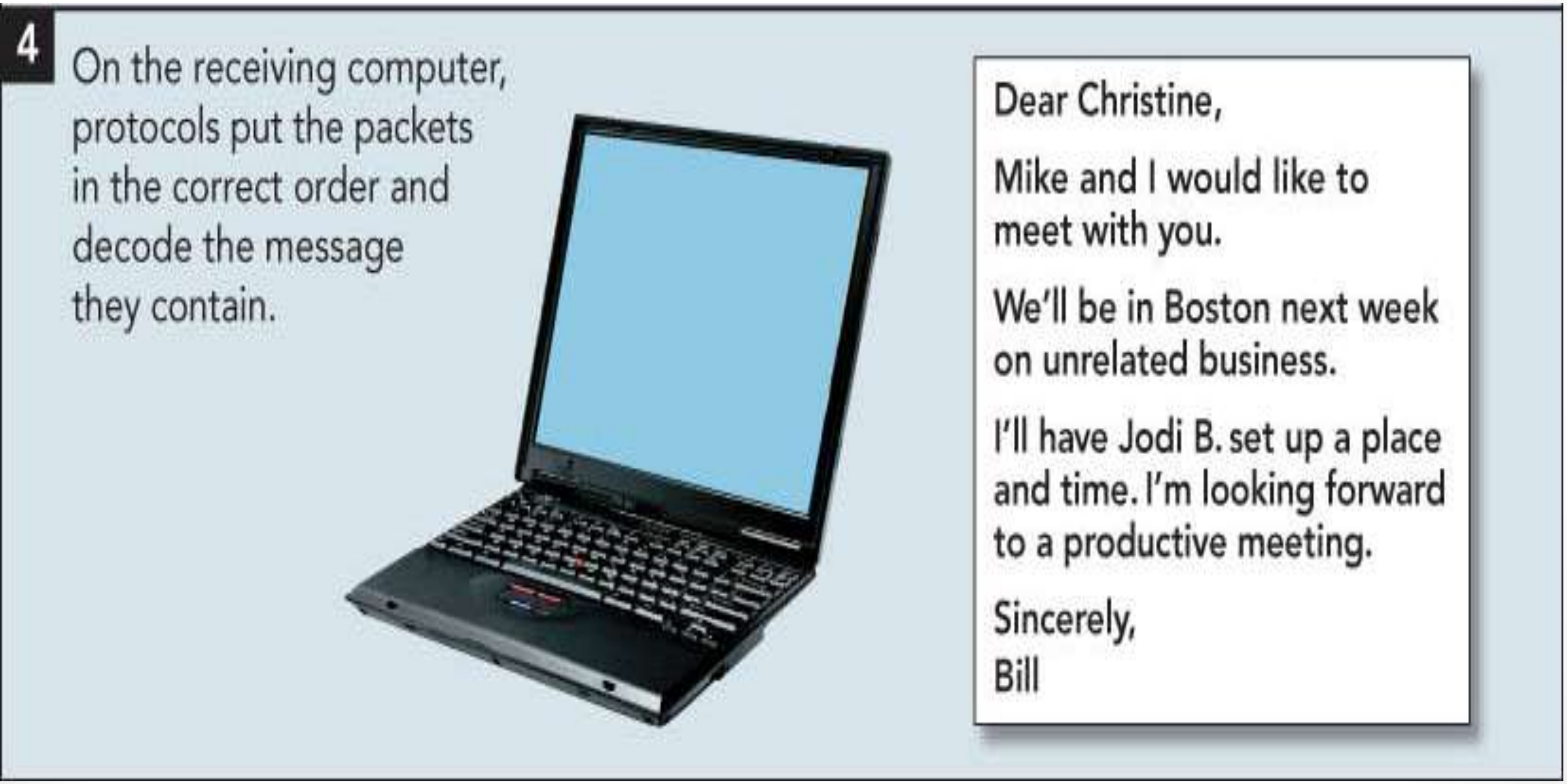
3 from: bill@oregon.edu
to: christine@aol.com

Wide Area Networks



3 After reading the packet's address, the router consults a table of possible paths to the packet's destination. If more than one path exists, the router sends the packet along the path that is least congested.

Wide Area Networks



4 On the receiving computer, protocols put the packets in the correct order and decode the message they contain.

Dear Christine,

Mike and I would like to meet with you.

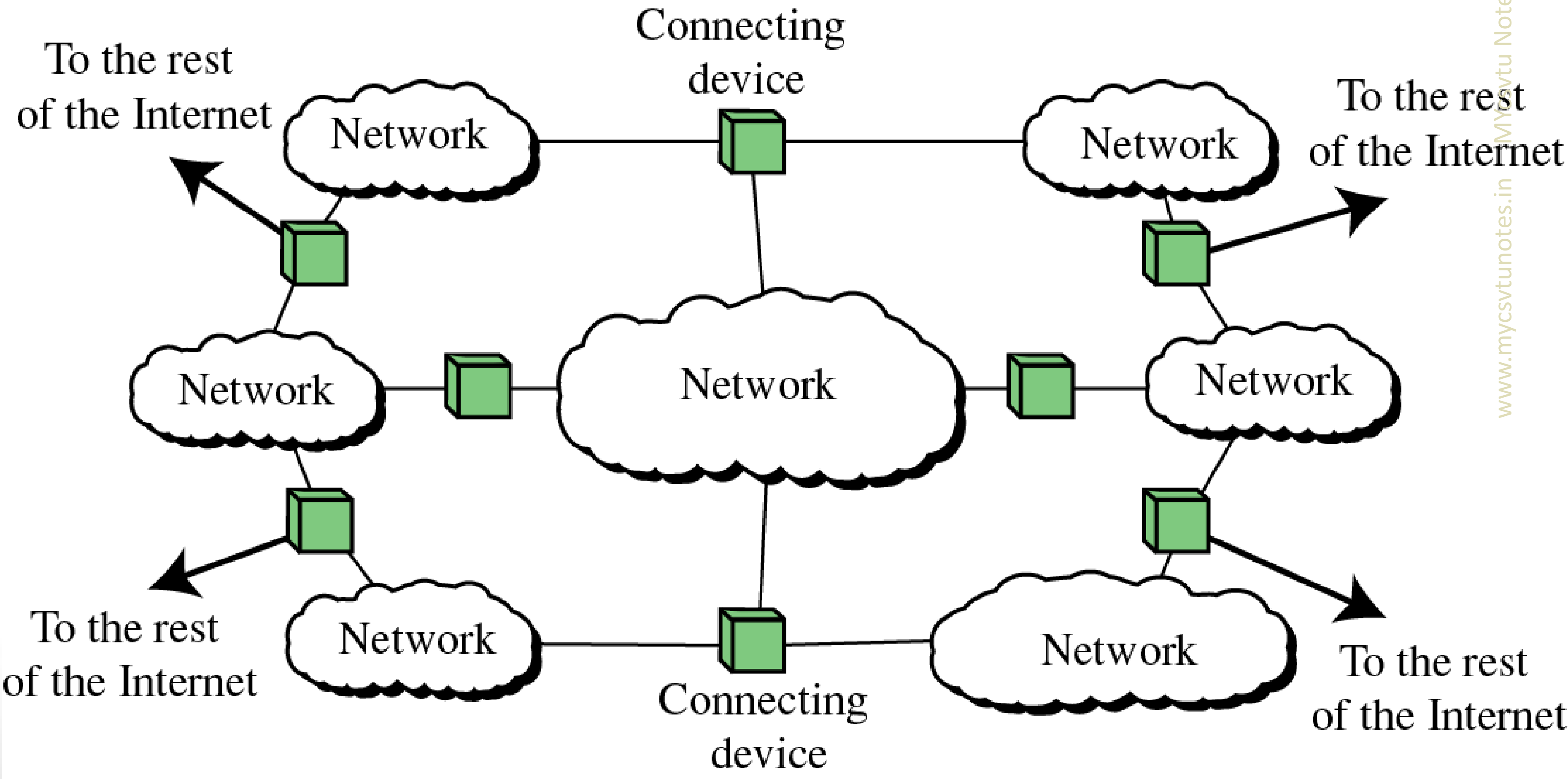
We'll be in Boston next week on unrelated business.

I'll have Jodi B. set up a place and time. I'm looking forward to a productive meeting.

Sincerely,
Bill

Internetworks

When two or more networks are connected together they become an internetwork or internet.



Connecting device
To the rest of the Internet
Network
Network
To the rest of the Internet
Network
Network
Network
To the rest of the Internet
Network
Network
To the rest of the Internet
Connecting device

Difference between LAN,MAN,WAN

OSI MODEL

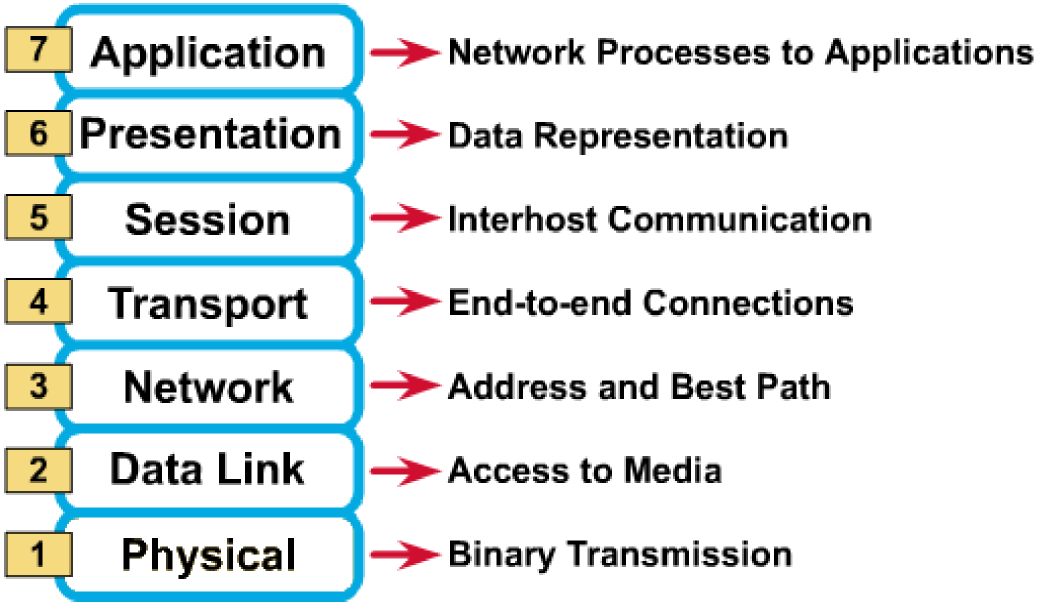
ISO- OSI Reference Model

- International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.
- Open Systems Interconnection (OSI) reference model is the result of this effort.
- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.

Continued….

- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .
- The model designers divided the process of transmitting data down to its fundamental elements.
- They identified which networking functions had related uses and collected those functions into discrete groups that became the layers.

OSI Reference Model: 7 Layers



7	Application	Network Processes to Applications
6	Presentation	Data Representation
5	Session	Interhost Communication
4	Transport	End-to-end Connections
3	Network	Address and Best Path
2	Data Link	Access to Media
1	Physical	Binary Transmission

How to remember?

- Please-- Physical
- Do -----Data link
- Not --- Network
- Teach --Transport
- Solved- Session
- Problem -- Presentation
- Again--Application

Organization of the Layers

- The seven layers can be thought of as belonging to three subgroups.
- Layers 1, 2, 3 are the network support layers; they deal with the physical aspects of moving data from one device to another.
- Layers 5, 6, 7 can be thought of as the user support layers.
- Layer 4, the transport layer, ensures end-to-end reliable data transmission.
- The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

Physical Layer

- It coordinates the functions required to transmit a bit stream over a physical medium.
- It also defines the procedures and functions for physical devices and interfaces.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.

The physical layer is concerned with the following:

- **Physical characteristics of interfaces and media**
- **Representation of bits**
- **Data rate**
- **Synchronization of bits**
- **Line configuration**
- **Physical topology**
- **Transmission mode**

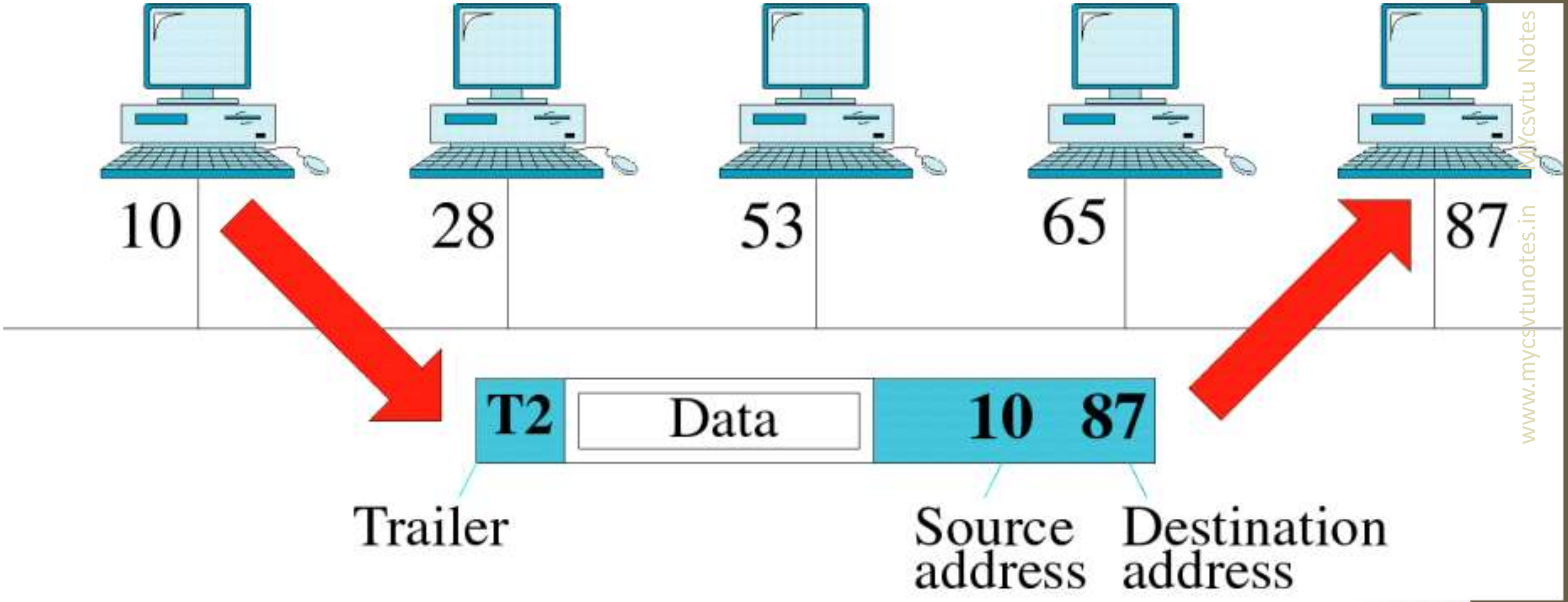
Data Link Layer

- The data link layer organizes the bits into frames; to provide node-to-node delivery.

The data link layer is concerned with the following:

- **Framing**
- **Physical addressing**
- **Flow control**
- **Error control**
- **Access control**

Data Link Layer Example



Different names for physical addressing

- **Ethernet Hardware Address** (EHA),
- **Hardware address**,
- **Adapter address,**
- **Media Access Control address (MAC),**
- P**hysical address**.

Network Layer

- The network layer is responsible for the source-to-destination (Host-to-Host) delivery of a packet possibly across multiple networks.

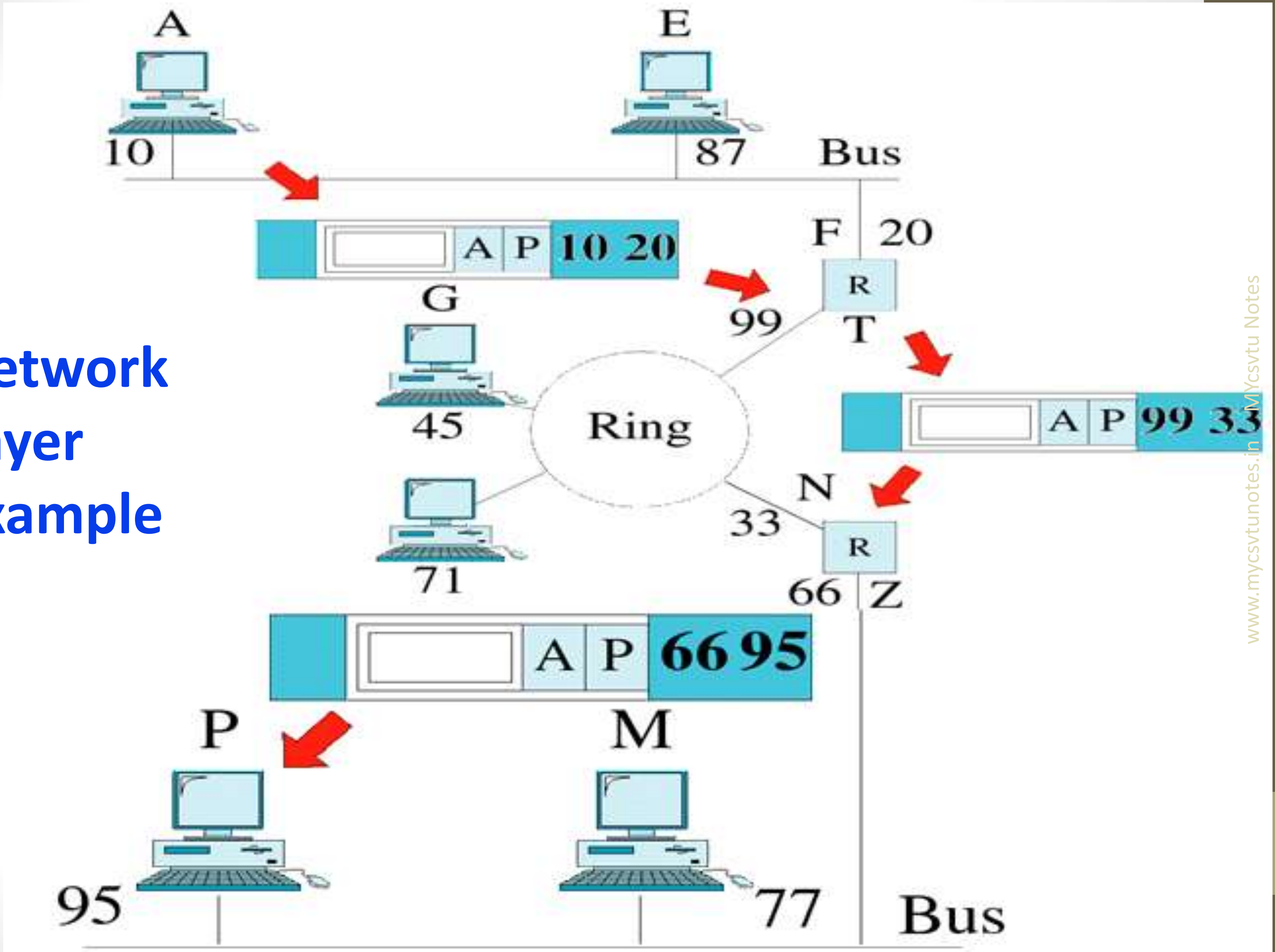
The network layer is concerned with the following:

- **Logical addressing**
- **Routing**

Logical addressing

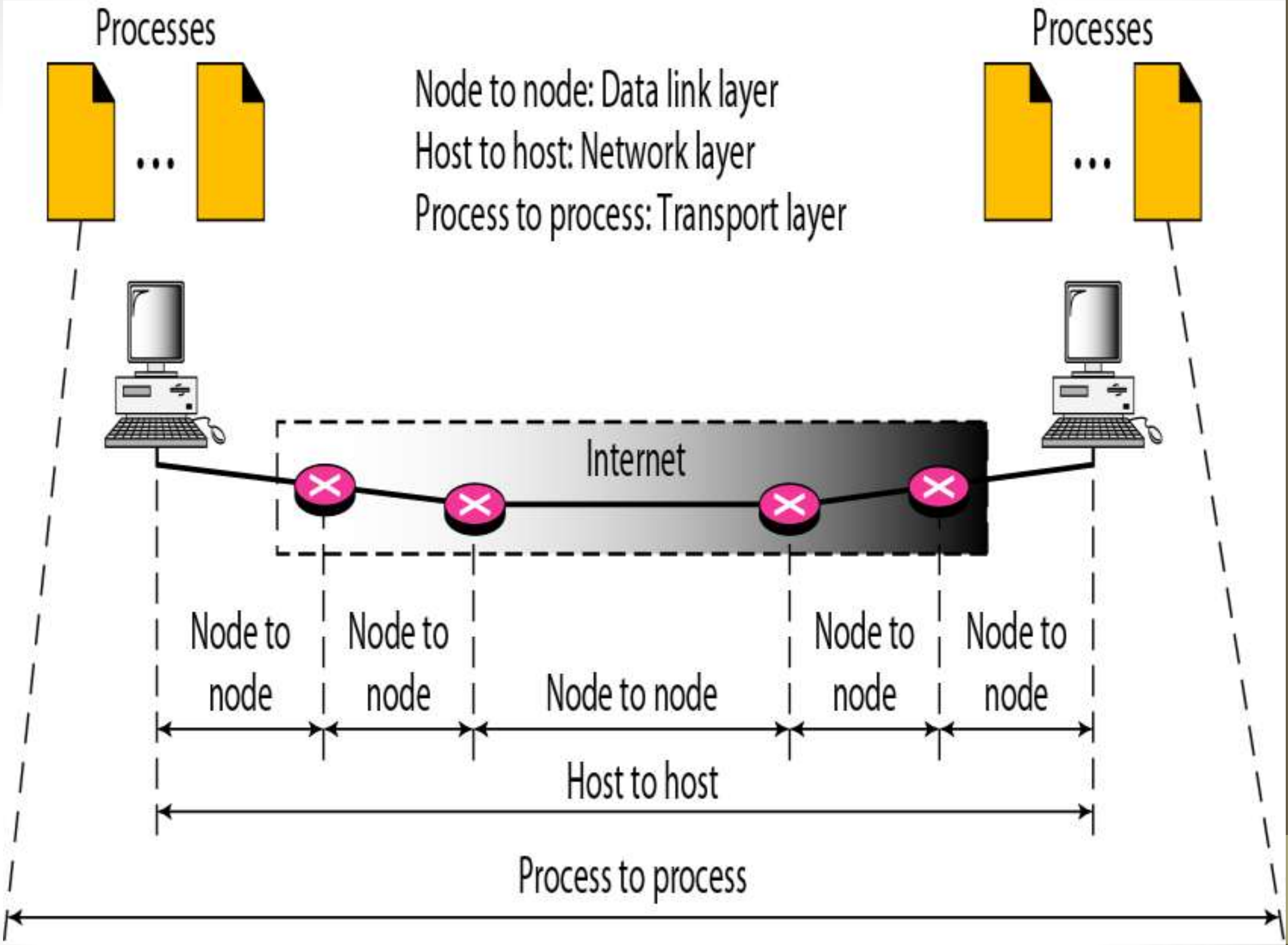
- IP address
- Network address

Network Layer Example



Transport Layer

- The transport layer is responsible for end-to-end delivery of the entire message and error control.

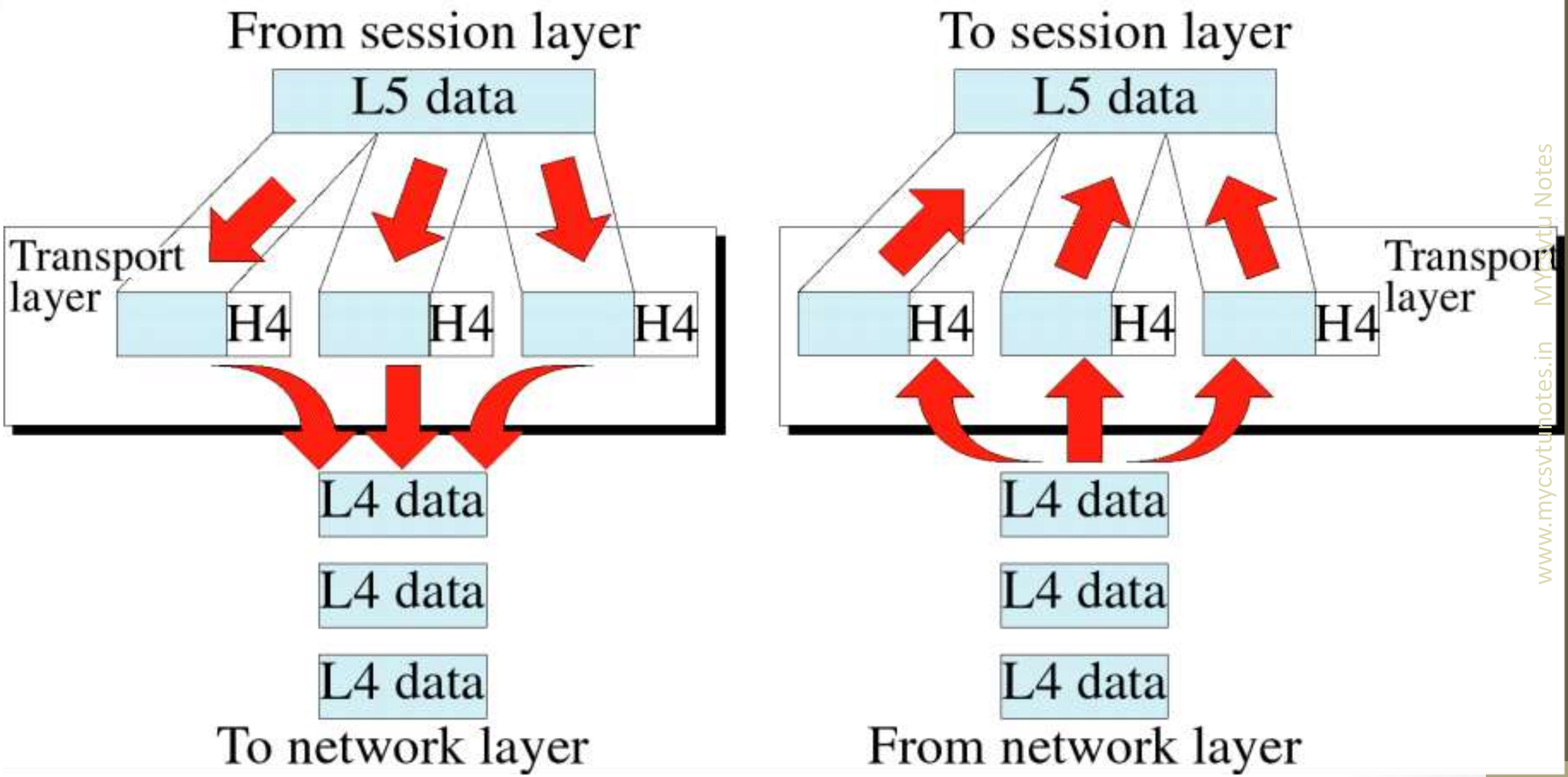


Node to node: Data link layer
Host to host: Network layer
Process to process: Transport layer

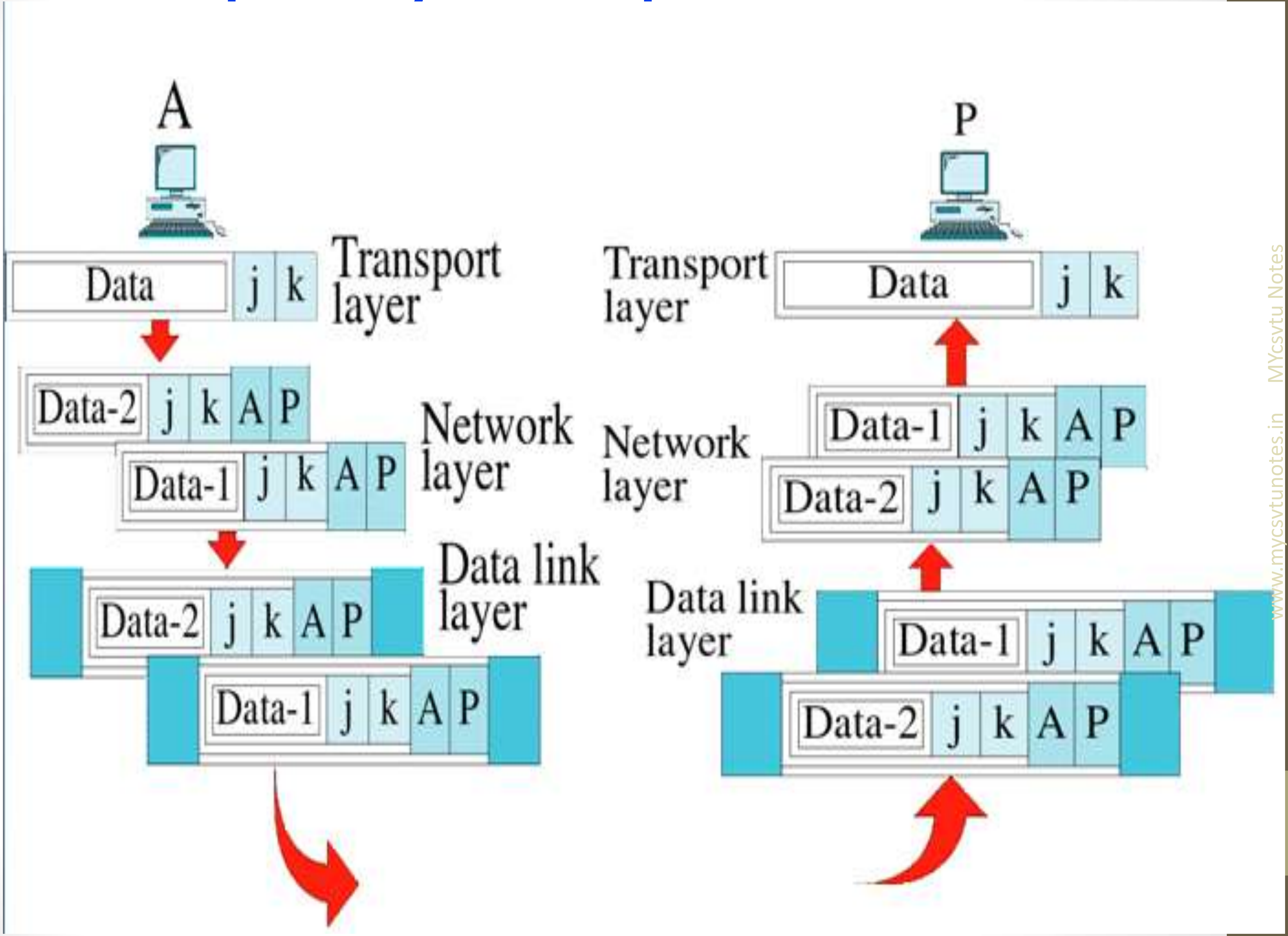
Specific responsibility of the transport layer includes the following:

- **Service-point addressing**
- **Segmentation and reassembly**
- **Connection control**
- **Flow control**
- **Error control**

Transport Layer



Transport Layer Example



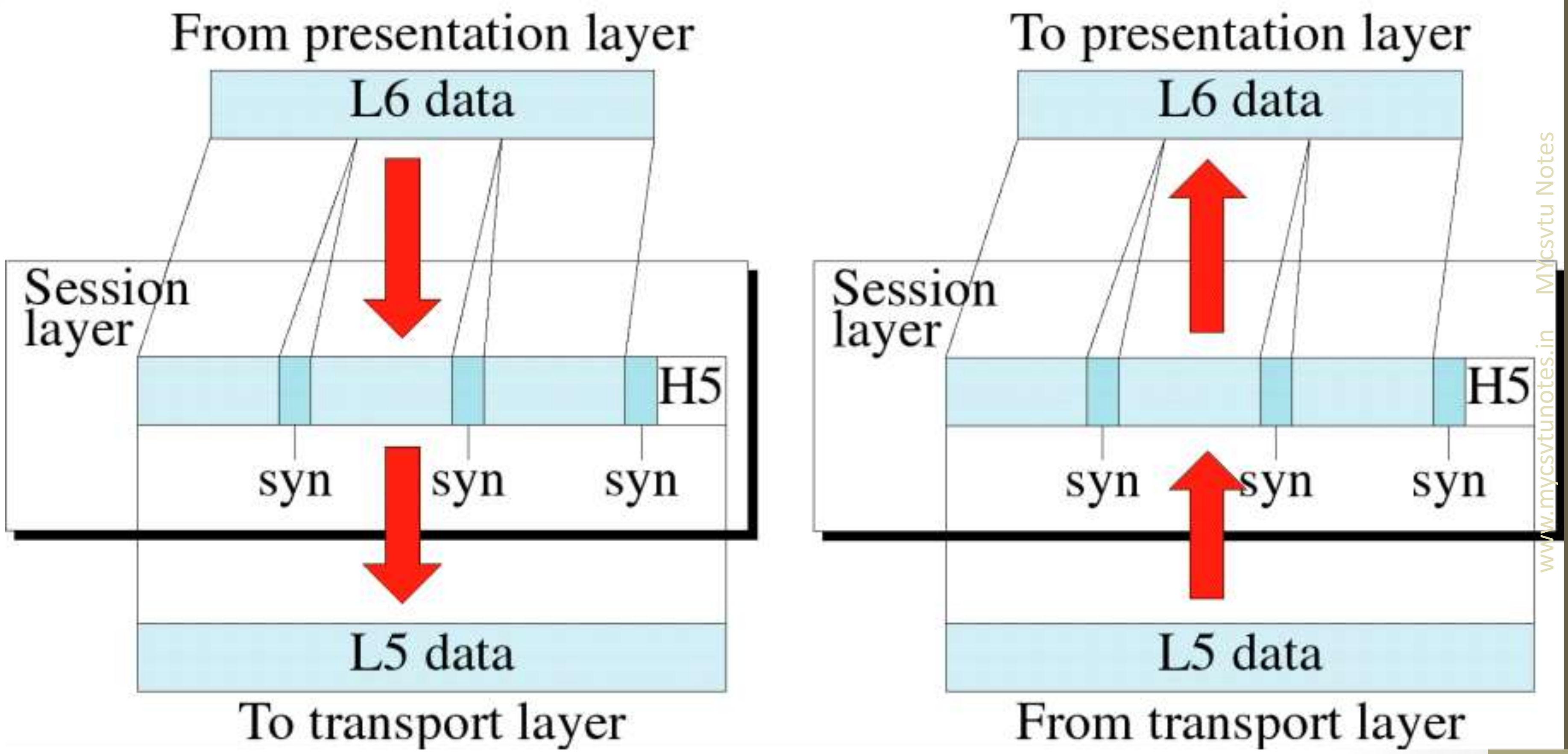
Session Layer

- It establishes, maintains, and terminate sessions.

Specific responsibility of the session layer includes the following:

- **Dialog control:** The Session layer is responsible for coordinating how the communication between systems takes place, which is known as dialog control. In some sessions, only a single system is allowed to communicate at any point in time, referred to as half-duplex.
- **Synchronization**

Session Layer



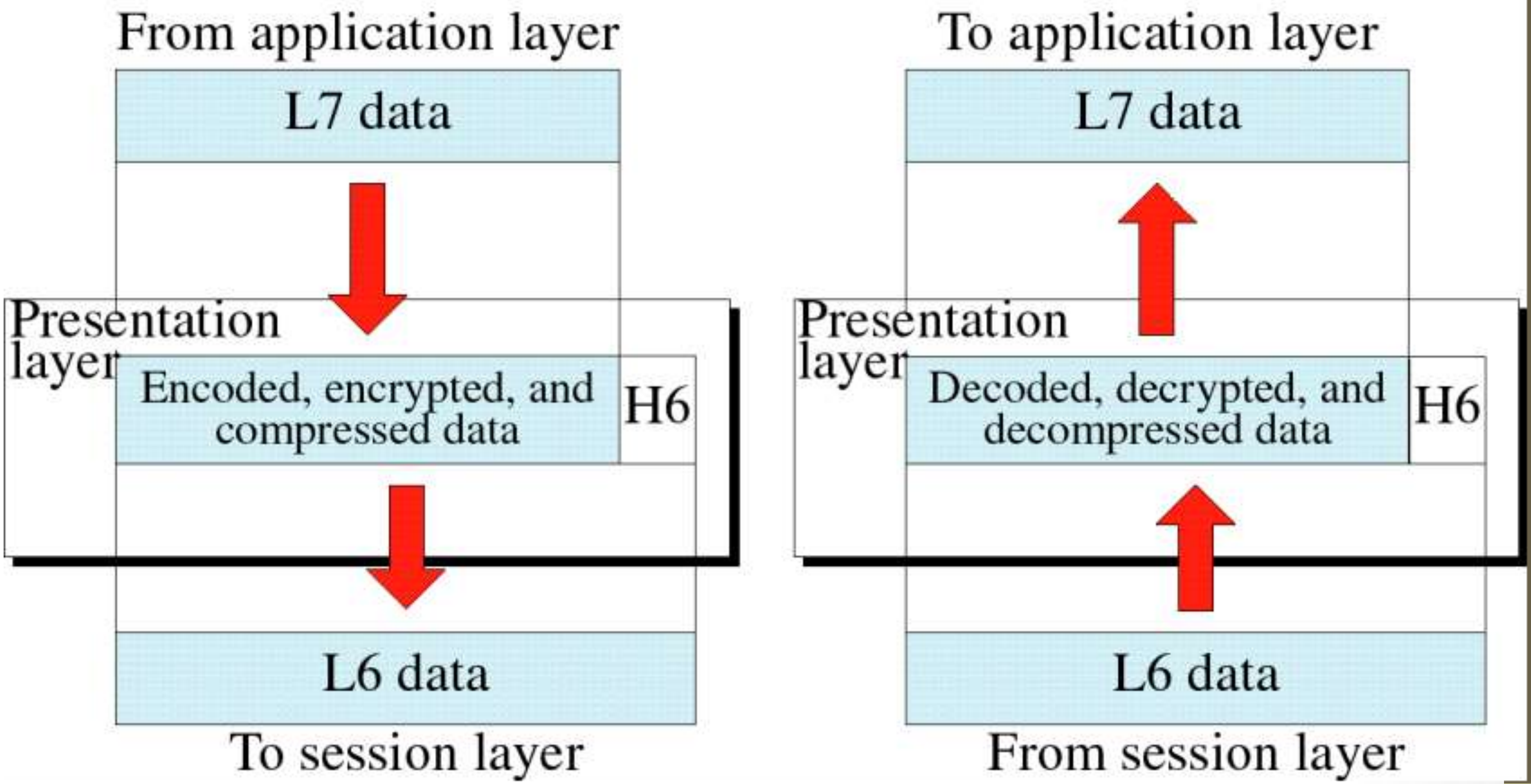
Presentation Layer

- It is concerned with the syntax and semantics of the information exchanged between two systems.

Specific responsibility of the presentation layer includes the following:

- **Translation**
- **Encryption**
- **Compression**

Presentation Layer



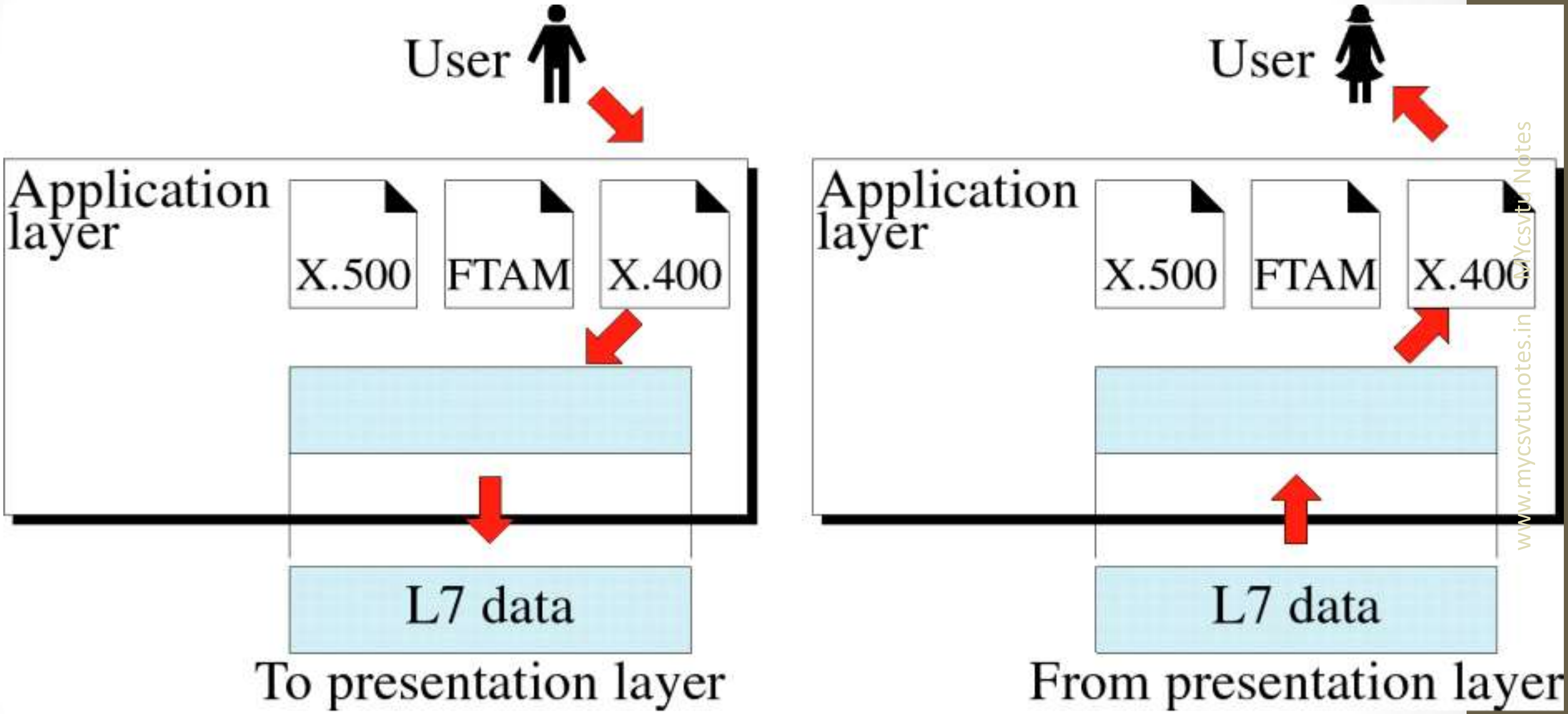
Application Layer

- It enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

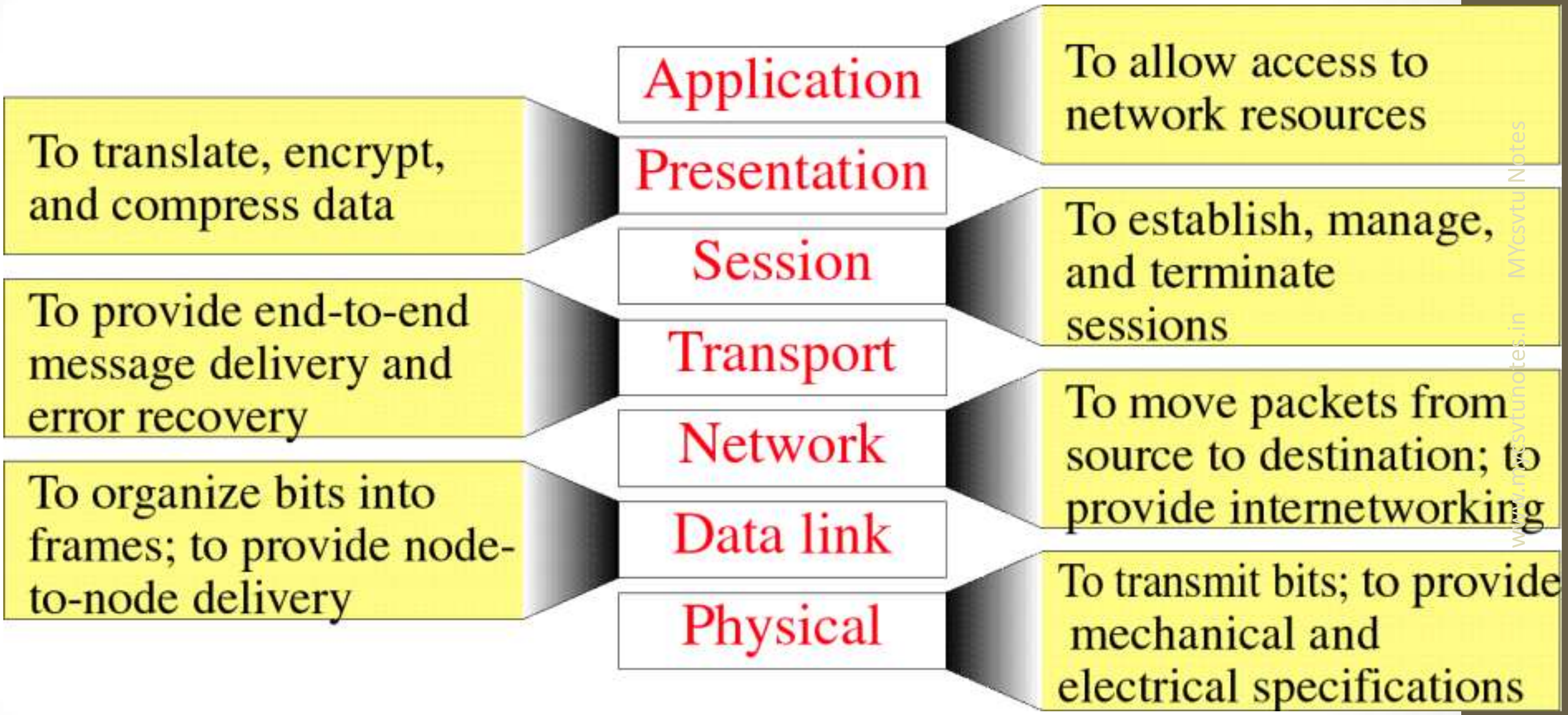
Function of Application Layer

- **File transfer, access, and management (FTAM)**
- **Mail services**
- **Directory services**

Application Layer



Summary of Layer Functions



Application

To allow access to network resources

Presentation

To translate, encrypt, and compress data

Session

To establish, manage, and terminate sessions

Transport

To provide end-to-end message delivery and error recovery

Network

To move packets from source to destination; to provide internetworking

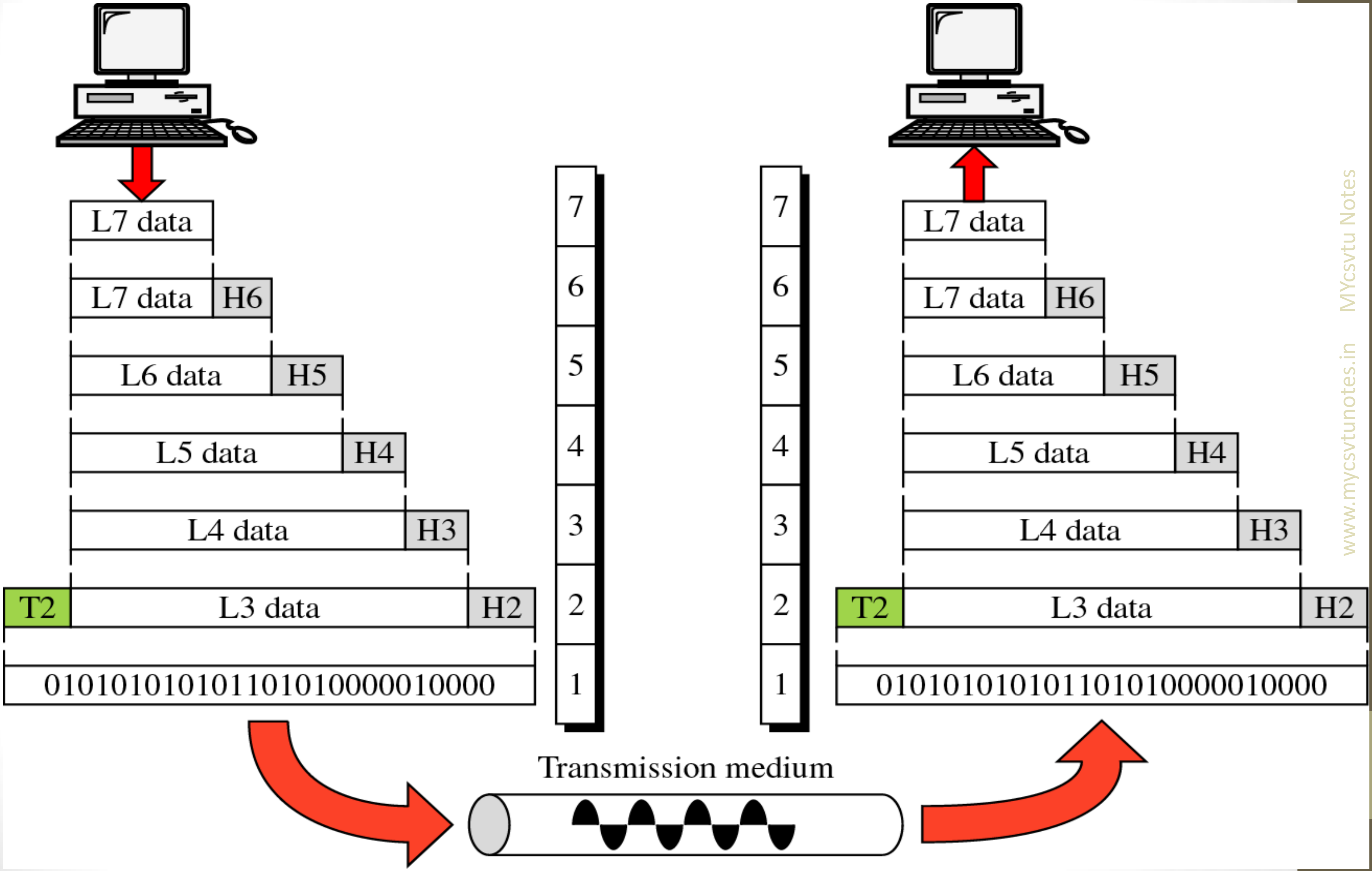
Data link

To organize bits into frames; to provide node-to-node delivery

Physical

To transmit bits; to provide mechanical and electrical specifications

An exchange using OSI Model



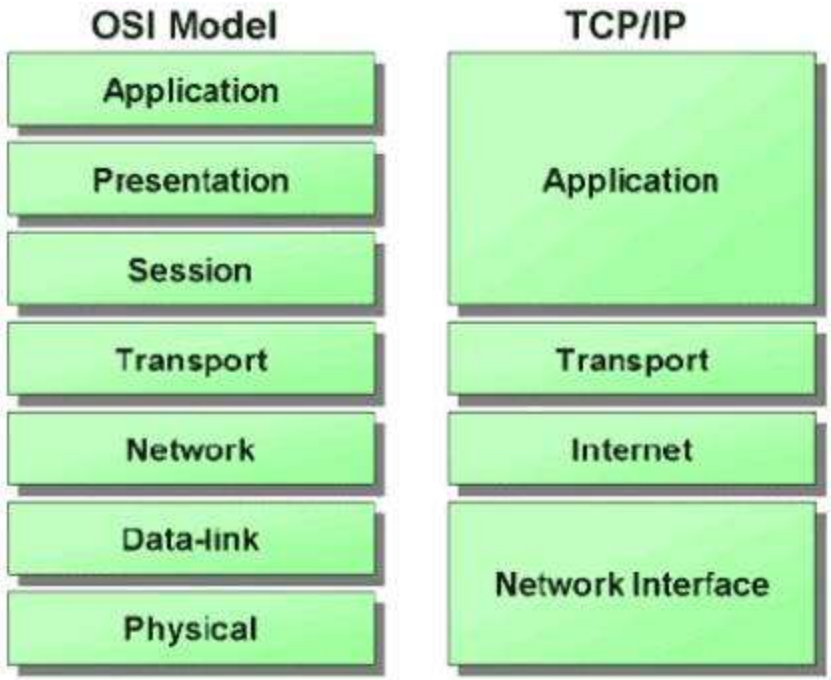
An exchange using OSI Model

- L7 data means the data unit at layer 7.
- The process starts out at layer 7, and then moves from layer to layer in descending sequential order.
- At each layer (except 7 and 1), a header is added to the data unit.
- At layer 2, a trailer is added as well.
- When the formatted data unit passes through the physical layer, it is changed into an electromagnetic signal and transported along a physical link.
- Upon reaching its destination, the signal passes into layer 1 and is transformed back into bits.
- As each block of data reaches the next higher layer, the header and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken.
- By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

TCP/IP Model

- It stands for Transmission Control Protocol/Internet Protocol. It is named from two of the most important protocols in it: the TCP and IP, which were the first two networking protocol defined in this standard.
- The TCP/IP Model, or TCP/IP Suite, or Internet Protocol Suite, describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network.
- The TCP/IP Model was created in the 1970s by DARPA (Defense Advanced Research Projects Agency) , an agency of the United States Department of Defense (DOD).
- The TCP/IP protocol suite was developed before the OSI model was published.
- It evolved from ARPANET (Advanced Research Projects Agency Network), which was the world's first wide area network and a predecessor of the Internet.

Introduction to TCP/IP Model



OSI Model

Application

Presentation

Session

Transport

Network

Data-link

Physical

TCP/IP

Application

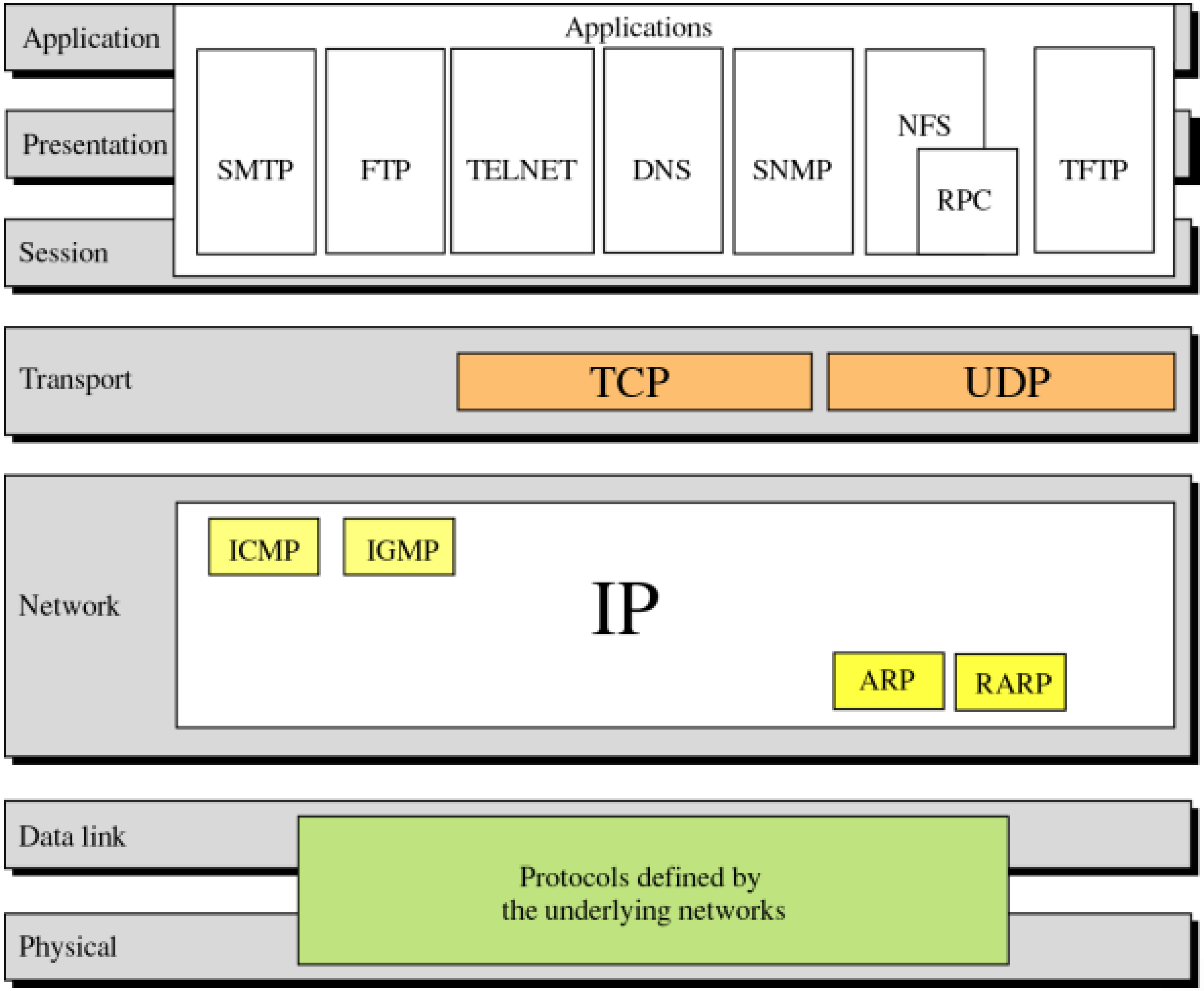
Transport

Internet

Network Interface

TCP/IP and the OSI model

TCP/IP protocol suite



At the application layer TCP/IP defines these protocols

- SMTP (Simple mail transfer protocol)
- FTP (File transfer protocol)
- TELNET (Terminal network)
- DNS (Domain name system)
- SNMP (Simple network management protocol)
- NFS (Network file system)
- RPC (Remote procedure call)
- TFTP (Trivial file transfer protocol)

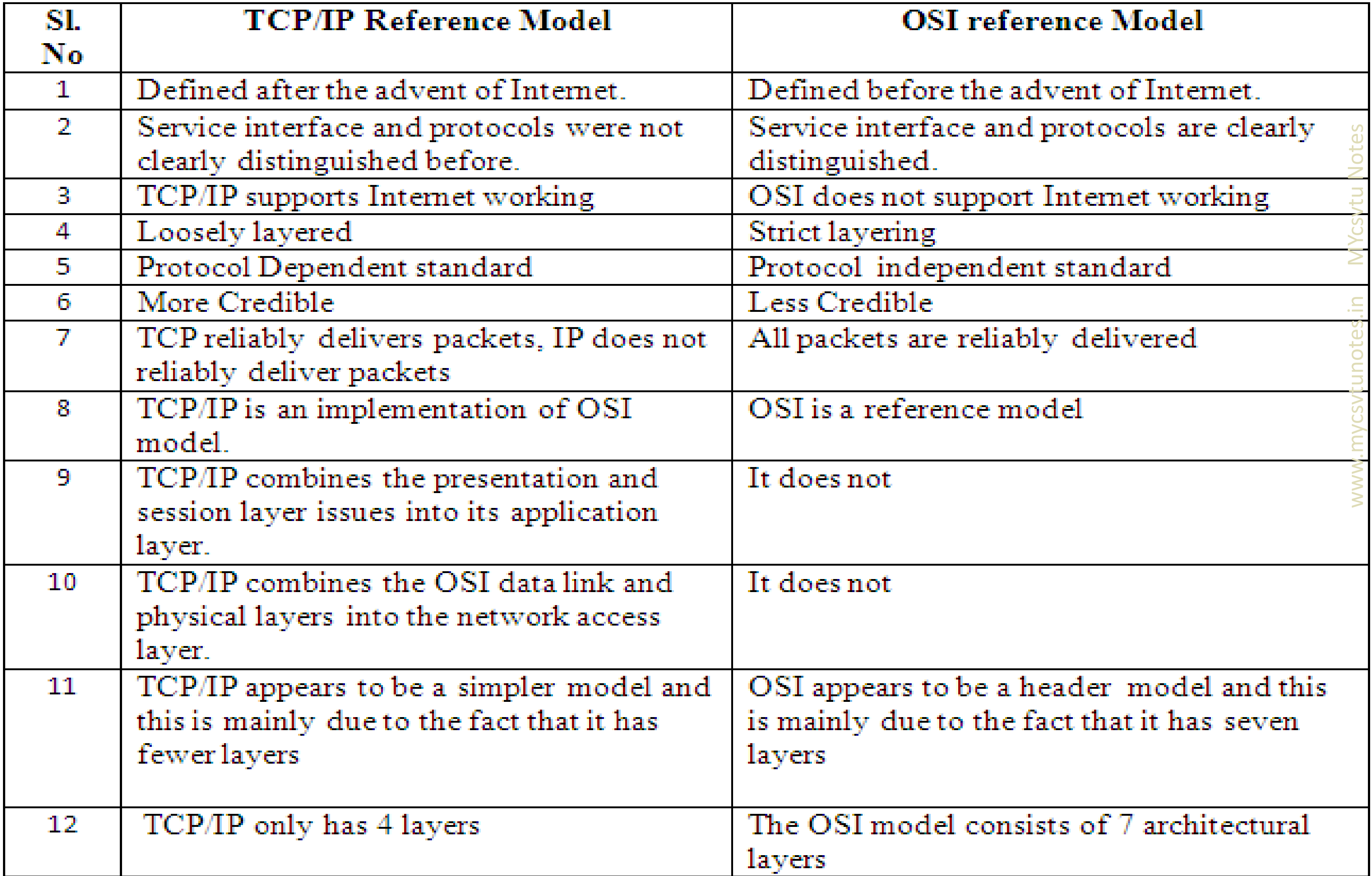
At the transport layer TCP/IP defines two protocols:

- TCP (Transmission control protocol)
- UDP (User datagram protocol)

At the network layer TCP/IP defines these protocols:

- IP (Internetworking protocol)
- ICMP (Internet control message protocol)
- IGMP (Internet group message protocol)
- ARP (Address resolution protocol)
- RARP (Reverse address resolution protocol)

TCP/IP Vs OSI Model



Sl. No	TCP/IP Reference Model	OSI reference Model
1	Defined after the advent of Internet.	Defined before the advent of Internet.
2	Service interface and protocols were not clearly distinguished before.	Service interface and protocols are clearly distinguished.
3	TCP/IP supports Internet working	OSI does not support Internet working
4	Loosely layered	Strict layering
5	Protocol Dependent standard	Protocol independent standard
6	More Credible	Less Credible
7	TCP reliably delivers packets, IP does not reliably deliver packets	All packets are reliably delivered
8	TCP/IP is an implementation of OSI model.	OSI is a reference model
9	TCP/IP combines the presentation and session layer issues into its application layer.	It does not
10	TCP/IP combines the OSI data link and physical layers into the network access layer.	It does not
11	TCP/IP appears to be a simpler model and this is mainly due to the fact that it has fewer layers	OSI appears to be a header model and this is mainly due to the fact that it has seven layers
12	TCP/IP only has 4 layers	The OSI model consists of 7 architectural layers

Why TCP/IP is more credible?

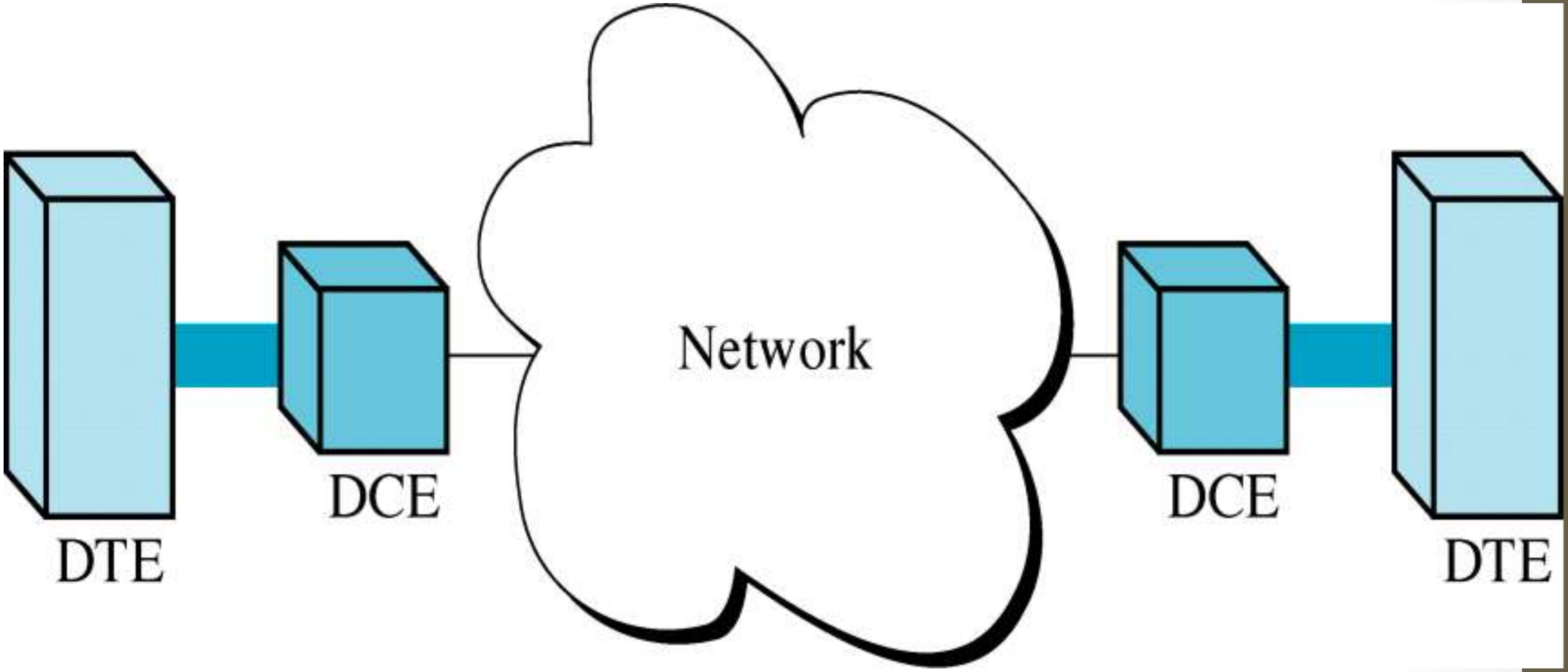
- TCP/IP is considered to be more credible model- this mainly due to the fact because TCP/IP models are the standards around which the internet was developed therefore it mainly gains credibility due to this reason.
- Where as in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool.

Physical Layer

DTE-DCE Interface

- DTE stands for Data Terminal Equipment.
- DCE stands for Data Circuit Terminating Equipment.
- Both of these equipment is used on both the side i.e. sender as well as receiver.
- The DTE generates the data and passes them along with the necessary control character to a DCE.
- The DCE converts the signal to a format appropriate to the transmission medium and introduces it onto the network link.

DTE-DCE Interface



Example

- Think of a DTE as operating the way your brain does when you talk.
- Let's say you have an idea that you want to communicate to a friend.
- Your brain creates the idea but cannot transmit that idea to your friend's brain by itself.
- Your brain passes the idea to your vocal chords and mouth, which convert it to sound waves that can travel through the air or over a telephone line to your friend's ear and from there to his or her brain, where it is converted back into information.
- In this model, your brain and your friend's brain are DTEs.
- Your vocal chords and mouth are your DCE.
- His or her ear is also a DCE. The air or telephone wire is your transmission medium.

Data Terminal Equipment (DTE)

- A DTE is any device that is the source of or destination for binary digital data.
- A DTE can be a terminal , micro computer, computer, printer or fax machine.
- DTE do not often communicate with one another, they generate and consume information by making use of an intermediary device that is DCE.

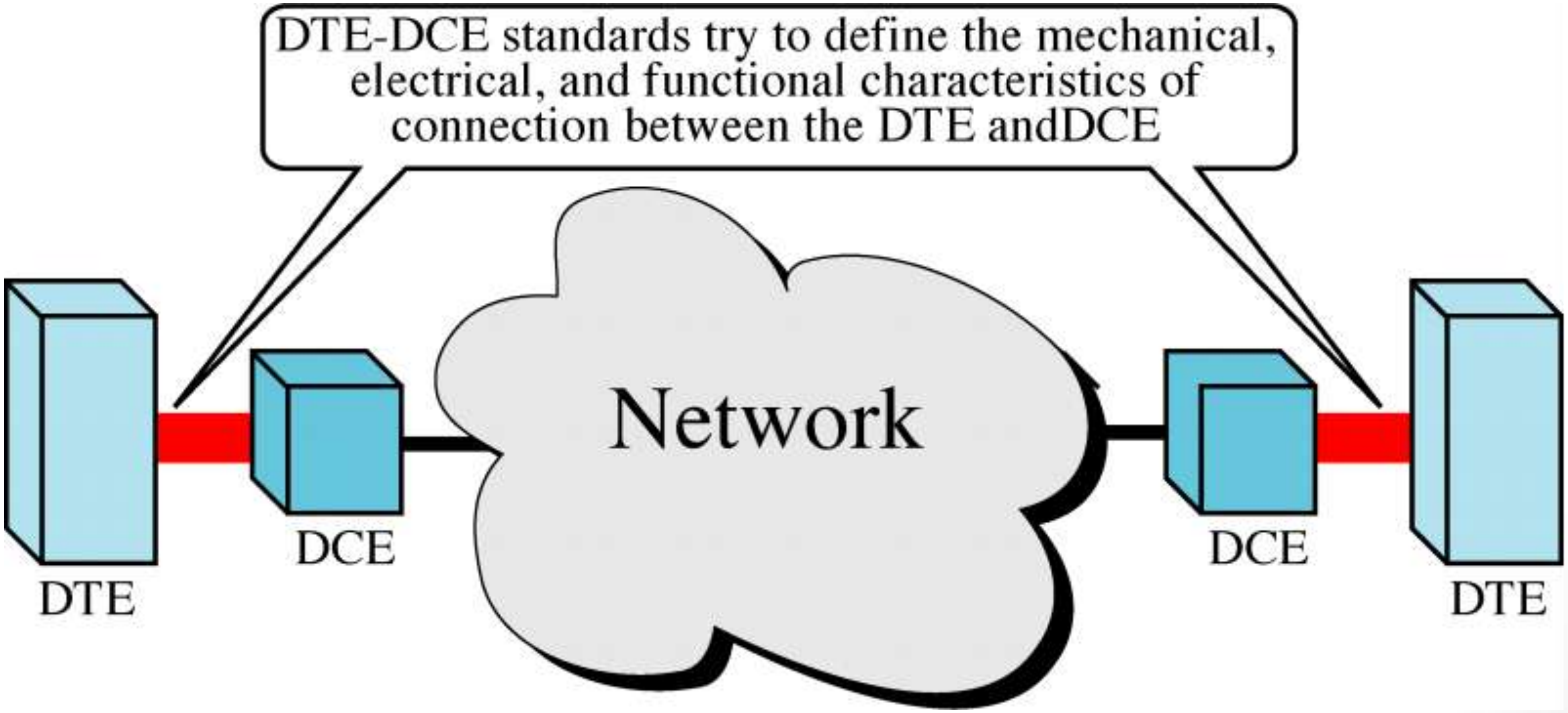
Data Circuit Terminating Equipment (DCE)

- A DCE is any device that transmits or receive data in the form of an analog or digital signal through a network.
- Example: Modem

Standards

- Many standards have been developed to define the connection between a DTE and DCE.
- Through their solutions differ, each standards provides a model for the mechanical, electrical, and functional characteristics of the connection.

DTE-DCE standards



DTE-DCE standards try to define the mechanical, electrical, and functional characteristics of connection between the DTE andDCE

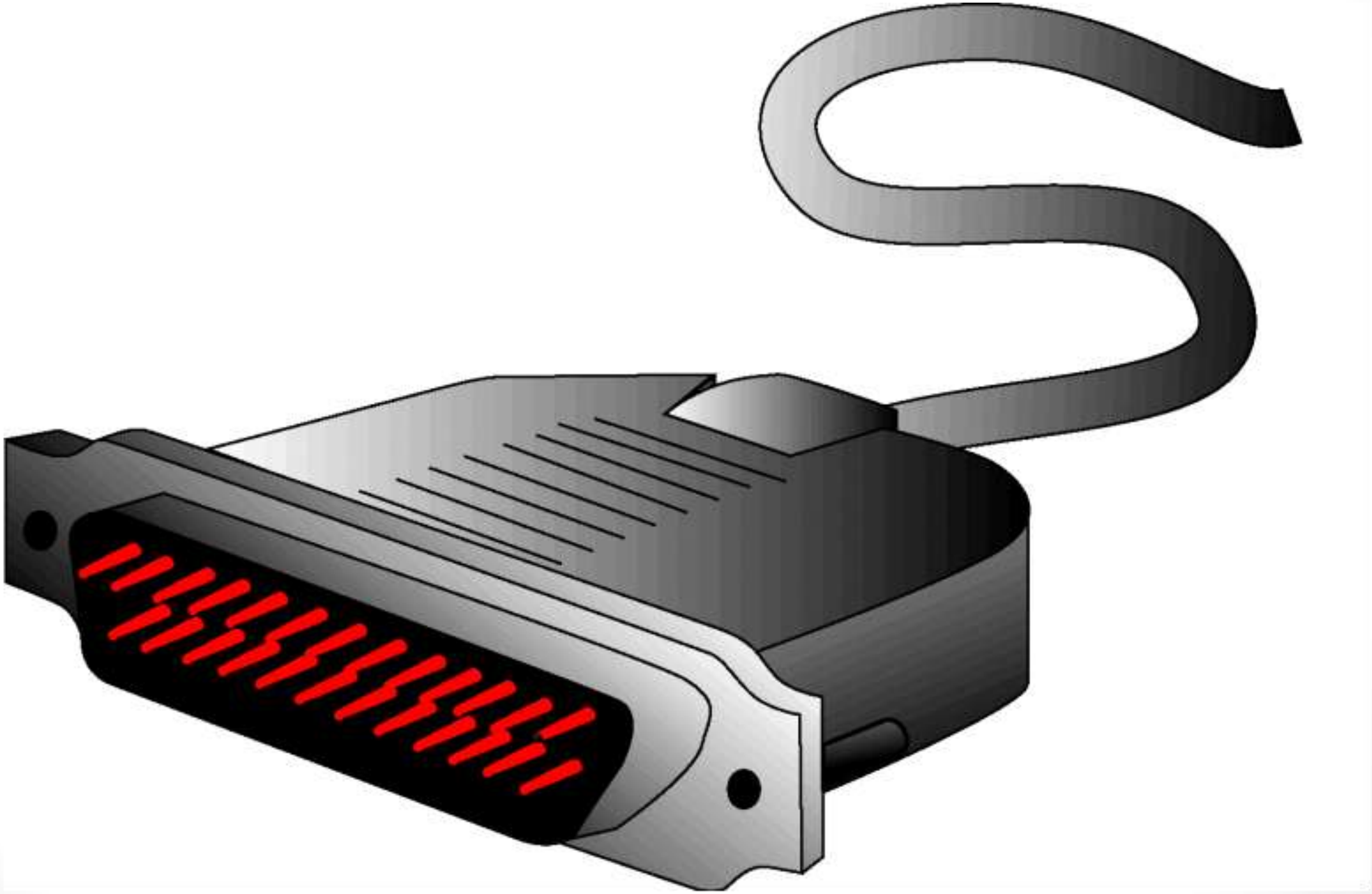
DTE-DCE Interface Standards

- The 2 active organizations those who are involved in developing the DTE-DCE Interface standards. They are:
  - EIA (Electronic Industry Association)
    - EIA-232
    - EIA-442
    - EIA-449
  - ITU-T (International Telecommunication Union-Telecommunication Standards)
    - V-series
    - X-series

EIA-232 Interface

- EIA-232 previously known as RS-232 interface.
- Any Interface is characterized by using 3 major characteristics:
  - Mechanical Specification
  - Electrical Specification
  - Functional Specification

EIA-232



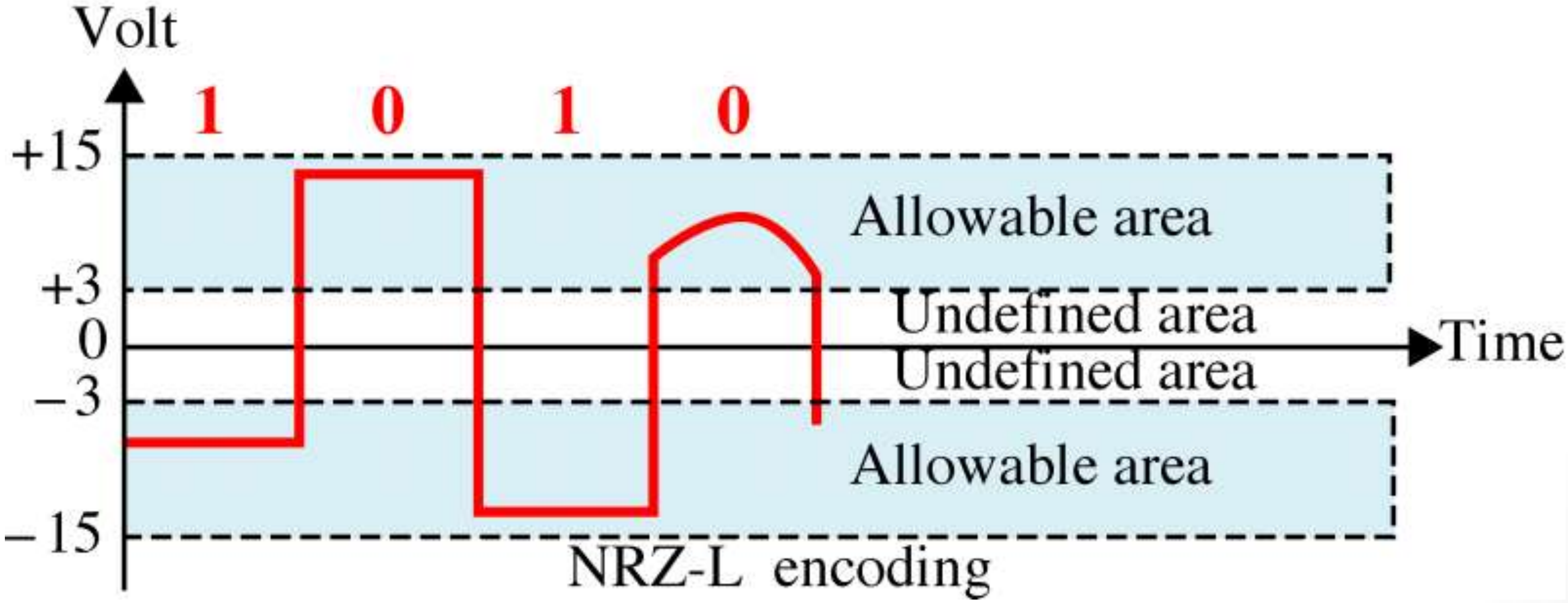
Mechanical Specification

- EIA-232 standard defines an interface as a 25-wire cable with DB-25 pin connector attached to either end.
- The length of the cable may not exceed 15 meters.
- A DB-25 connector is a plug with 25 pins and each pins is attached to a single wire with a specific function.

Electrical Specification

- The electrical specification of the standard defines the voltage levels and the type of signal to be transmitted in either direction between the DTE and the DCE.
- Only 4-wires out of the 25 available in an EIA-232 interface are used for data functions.
- The remaining 21 are reserved for functions like control, timing, grounding and testing.
- EIA-232 allows for a maximum bit rate of 20 Kbps.

Electrical Specification for sending data

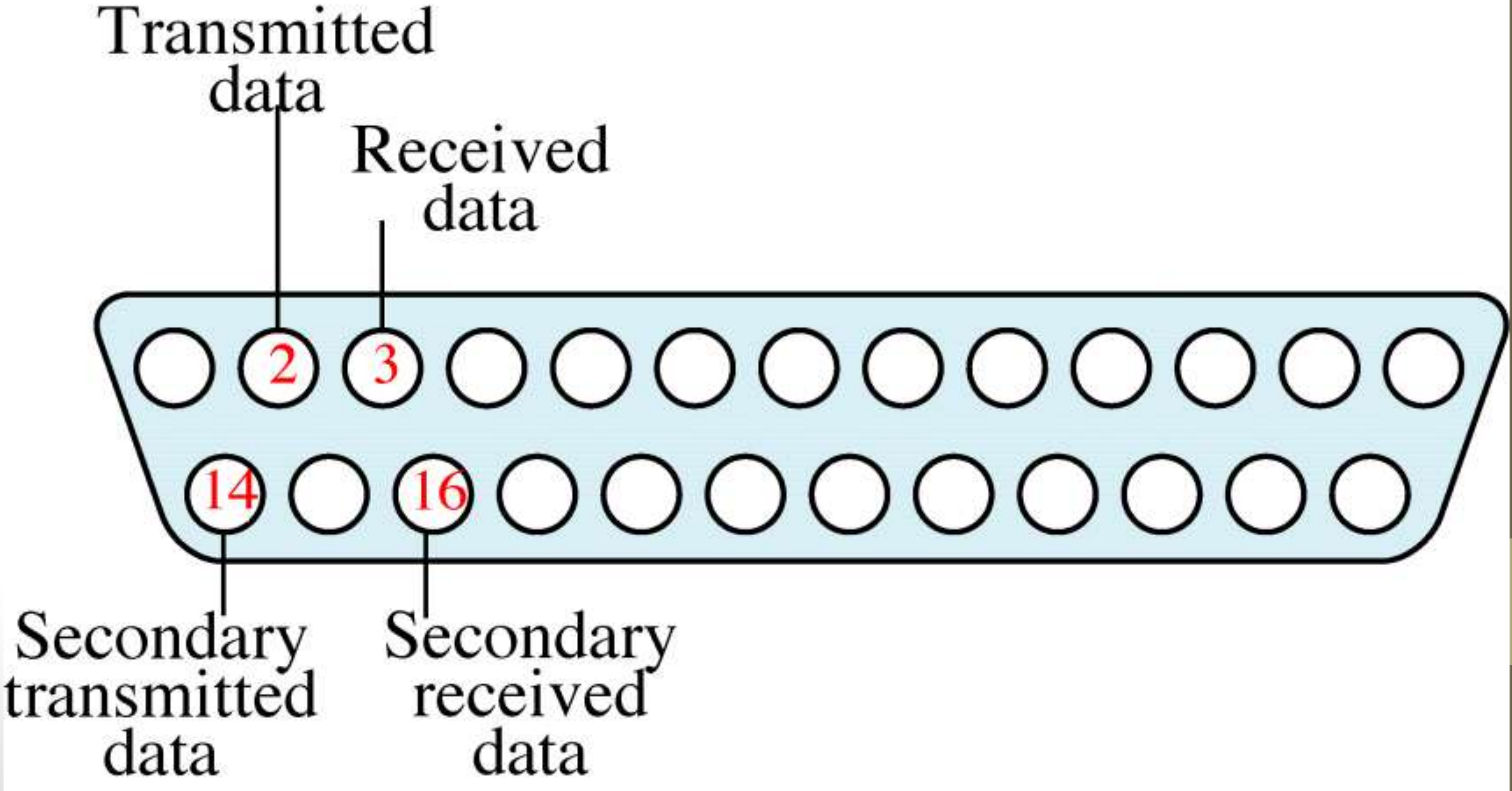


Functional Specification

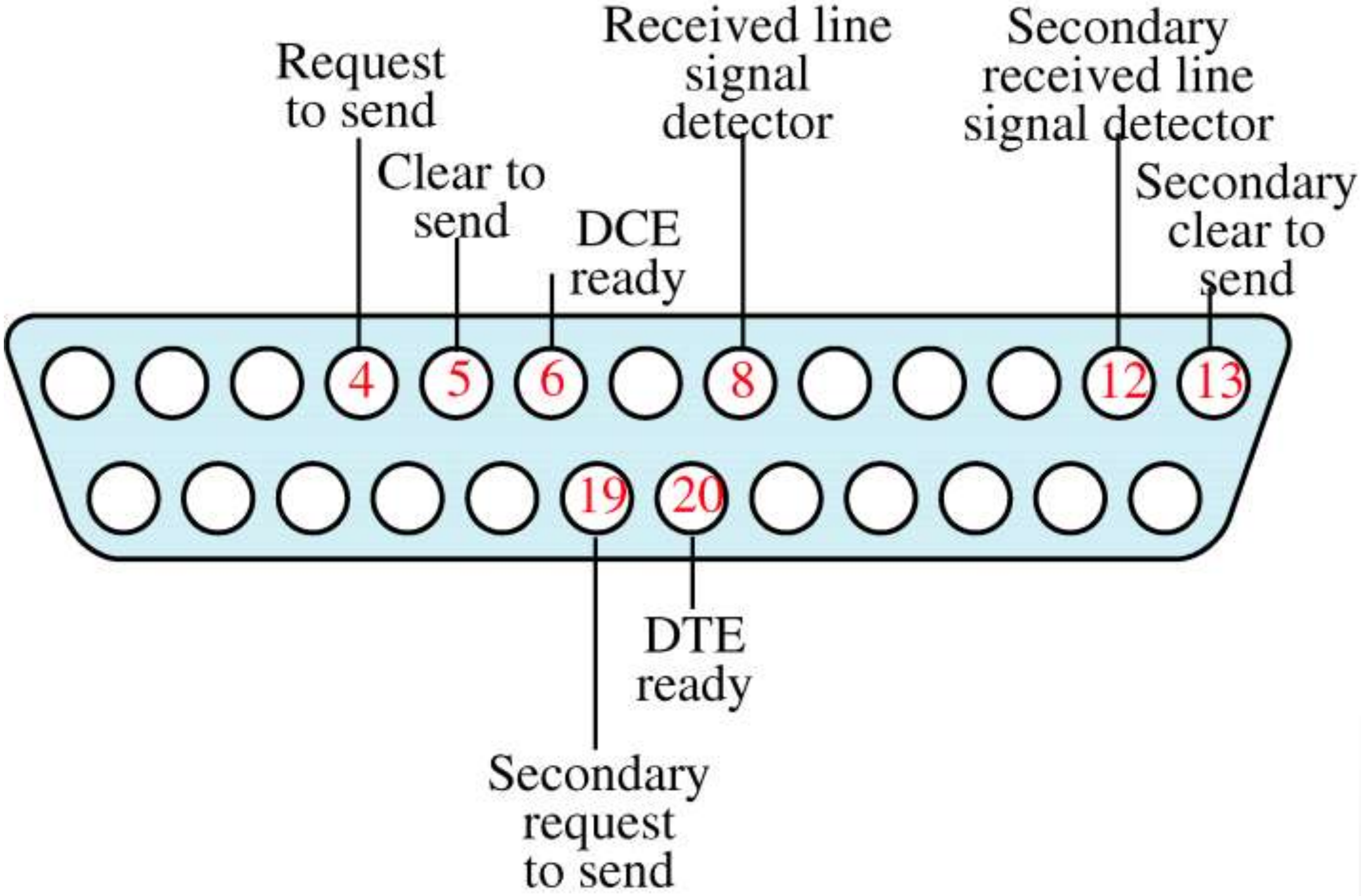
- Two different implementation of EIA-232 are available:
  - DB-25 Pin
  - DB-9 Pin

DB-25 Pin

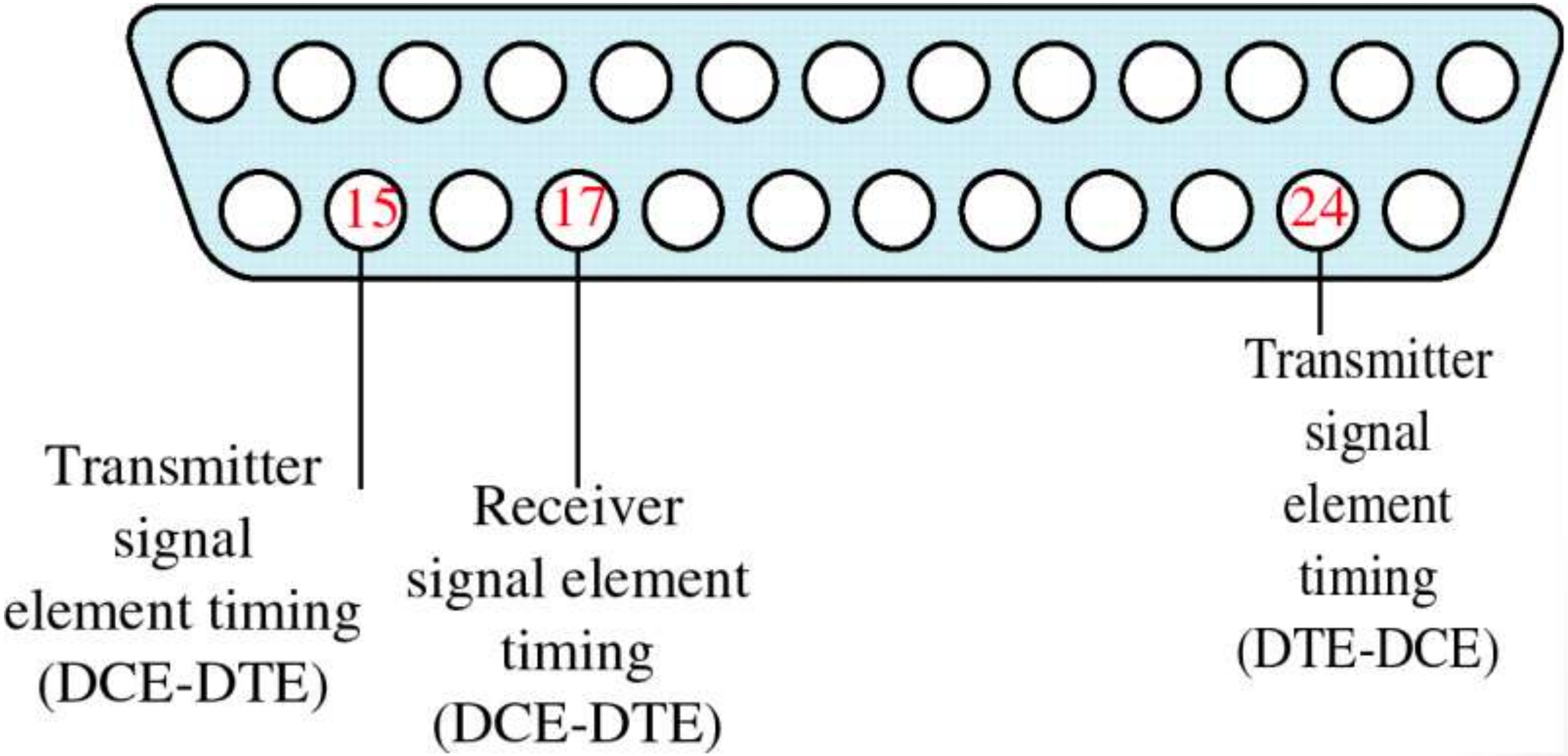
Data Pins



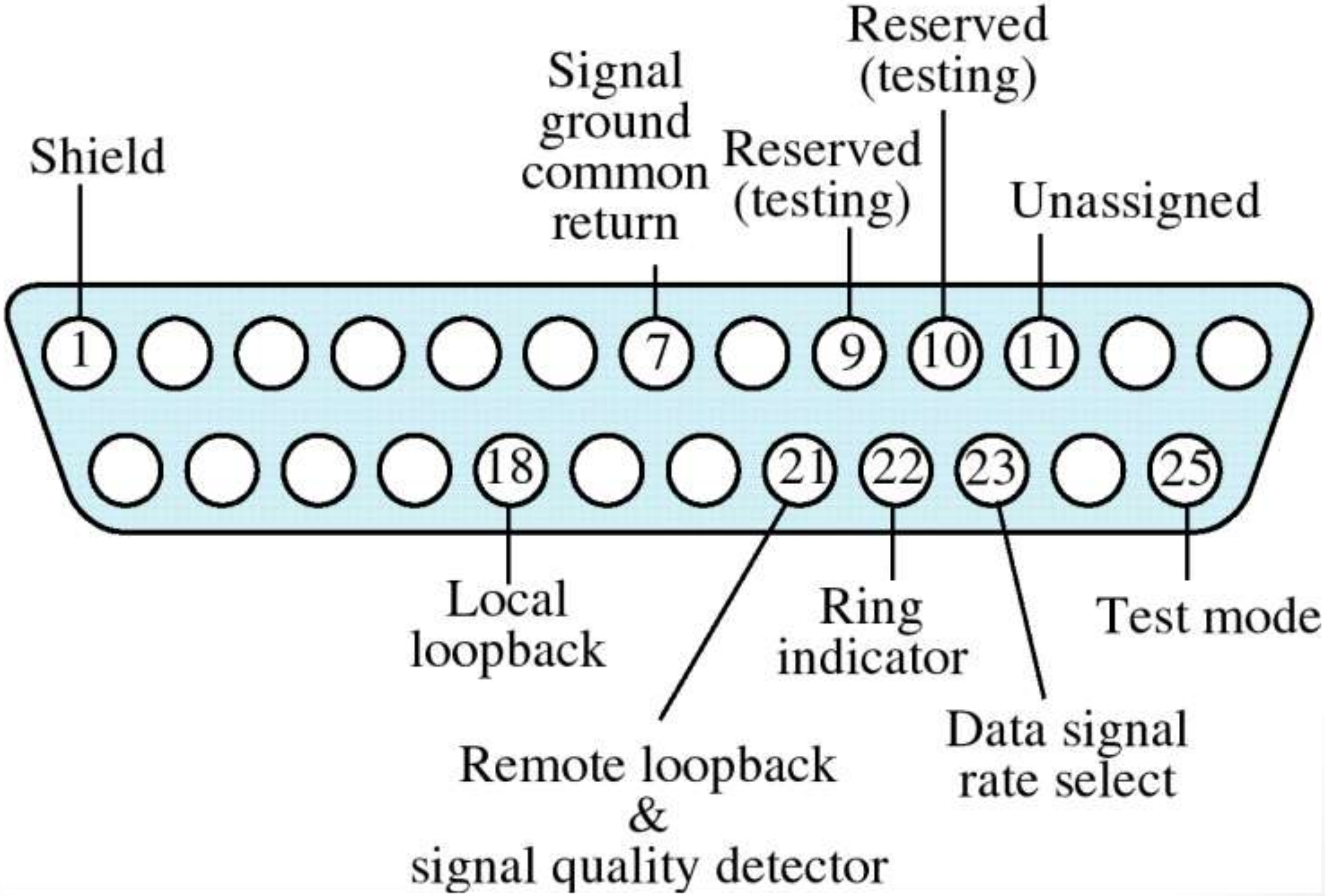
Control Pins


Request to send
Clear to send
DCE ready
Received line signal detector
Secondary received line signal detector
Secondary clear to send
4
5
6
8
12
13
19
20
DTE ready
Secondary request to send

Timing Pins


15
17
24
Transmitter signal element timing (DCE-DTE)
Receiver signal element timing (DCE-DTE)
Transmitter signal element timing (DTE-DCE)

Other Pins


Shield
Signal ground common return
Reserved (testing)
Reserved (testing)
Unassigned
1
7
9
10
11
18
21
22
23
25
Local loopback
Remote loopback & signal quality detector
Ring indicator
Data signal rate select
Test mode

DB-9

- Carrier Detect
- Transmit Data
- Receive Data
- DTE Ready
- Signal Ground
- DCE Ready
- Request to send
- Clear to Send
- Ring Indicator

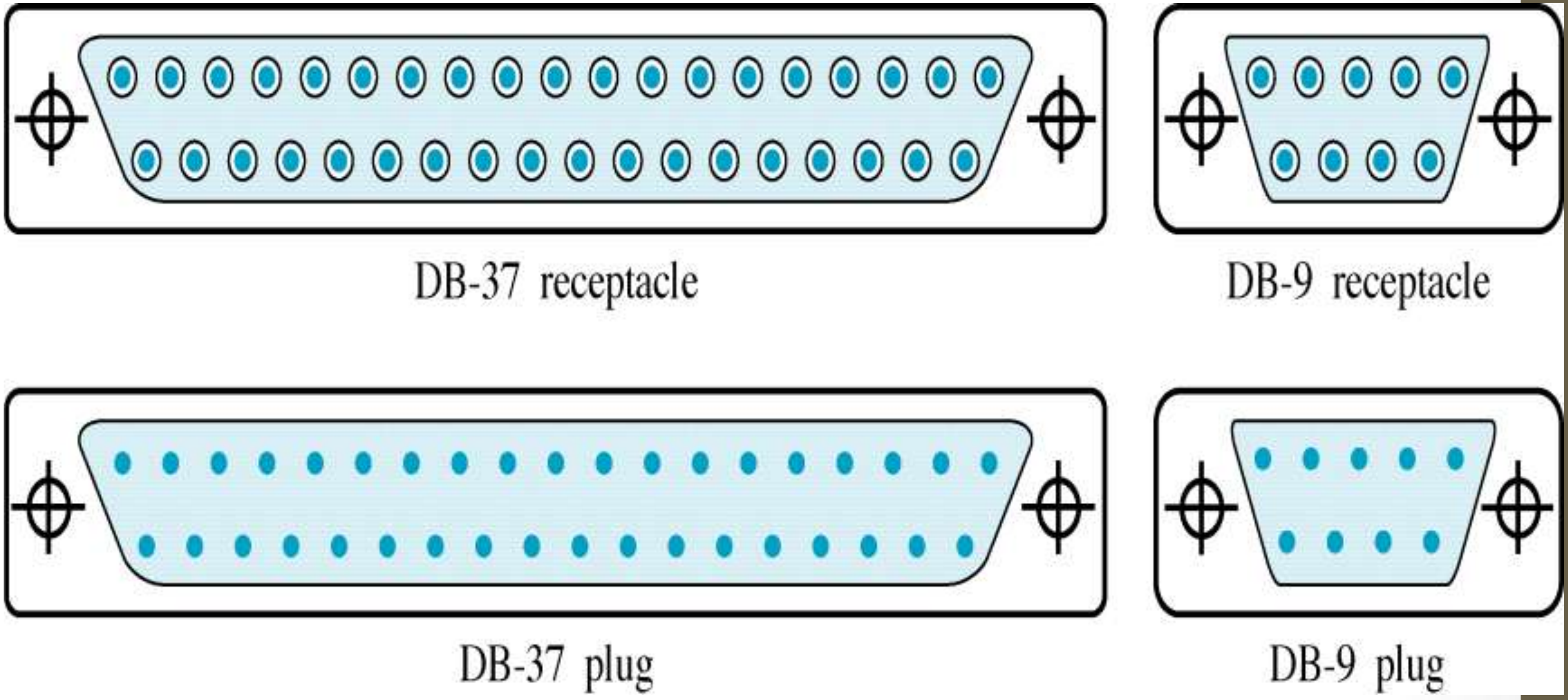
OTHER INTERFACE STANDARD

- EIA-232: data rate and cable length are restricted to 20 Kbps and cable length to 50 feet (15 meters).
- To meet the needs of users who require more speed and/or distance, the EIA and the ITU-T introduced additional interface standards:
  - EIA-449,
  - EIA-530,
  - X.21.

EIA-449

- EIA-449, also known as RS-449 or TIA-449.
- Data rates up to 2,000,000 bits per second.
- The standard specified two connectors with 37 and 9 pins data circuits.

Continued……..



DB-37 receptacle

DB-9 receptacle

DB-37 plug

DB-9 plug

Other Interface Standards(cont’d)

- DB-37 pins

Pin	Functions	Category	Pin	Functions	Category
1	Shield		20	Receive Common	II
2	Signal rate indicator		21	Unassigned	I
3	Unassigned		22	Send data	I
4	Send data	I	23	Send timing	I
5	Send timing	I	24	Receive data	I
6	Receive data	I	25	Request to send	I
7	Request to send	I	26	Receive timing	I
8	Receive timing	I	27	Clear to send	I
9	Clear to send	I	28	Terminal in service	II
10	Local loopback	II	29	Data mode	I
11	Data mode	I	30	Terminal ready	I
12	Terminal ready	I	31	Receive ready	I
13	Receive ready	I	32	Select ready	II
14	Remote loopback	II	33	Signal quality	
15	Incoming call		34	New signal	II
16	Select frequency	II	35	Terminal timing	I
17	Terminal timing	I	36	Standby indicator	II
18	Test mode	II	37	Send common	II
19	Signal ground				

Other Interface Standards(cont'd)

- DB-9 pins

Pin	Function	EIA-232 Equivalent
1	Shield	1
2	Secondary receive ready	
3	Secondary send data	14
4	Secondary receive data	16
5	Signal ground	7
6	Receive common	12
7	Secondary request to send	19
8	Secondary clear to send	13
9	Send common	

Other Interface Standards(cont’d)

- EIA-530

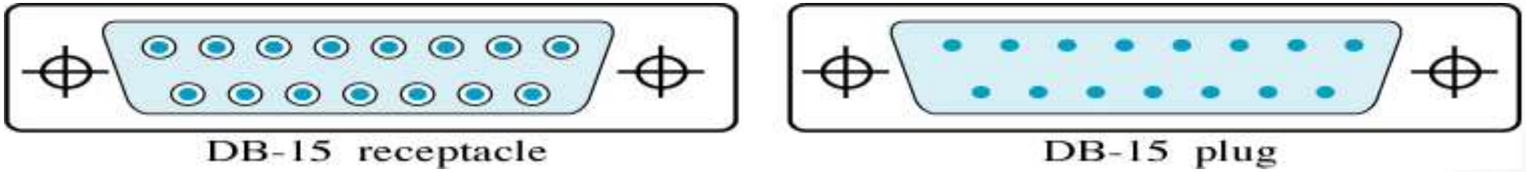
  It is a new version of EIA-449 that uses DB-25 pins

Other Interface Standards(cont'd)

- X.21

  It is an interface designed by the ITU-T

- DB-15 connector



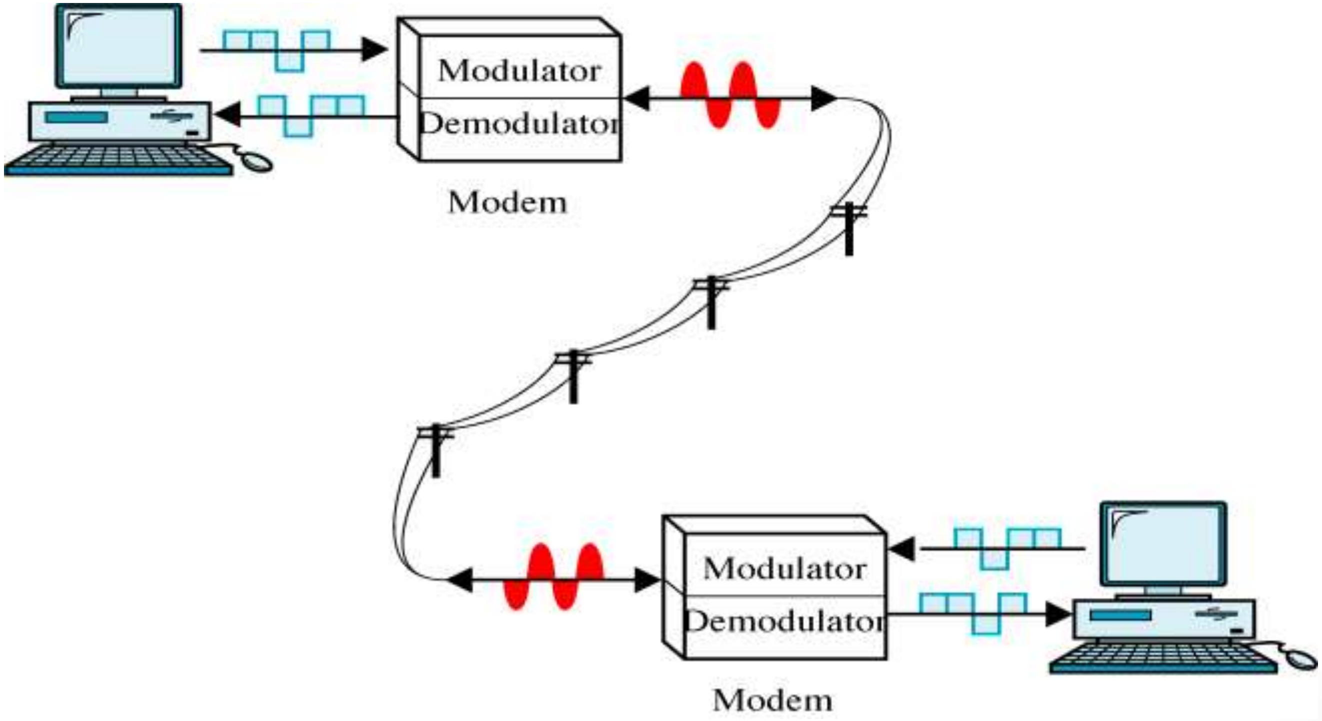
Other Interface Standards

- DB-15 pins

Pin	Function	Pin	Function
1	Shield	9	Transmit data or control
2	Transmit data or control	10	Control
3	Control	11	Receive data or control
4	Receive data or control	12	Indication
5	Indication	13	Signal element timing
6	Signal element timing	14	Byte timing
7	Bye timing	15	Reserved
8	Signal ground		

MODEMs

It is the most familiar type of DCE



MODEMs(cont’d)

- MODEM

  it stands for modulator/demodulator

  - Modulator : converts a digital signal to an analog signal
  - Demodulator : converts an analog signal to a digital signal

MODEMs(cont'd)

- Intelligent Modems

  ~ contain software to support a number of additional function, such as automatic answering and dialing

MODEM STANDARDS

Bell modems

- 103/113 series
- 202 series
- 212 series
- 201 series
- 208 series
- 209 series

ITU-T modem

- V.22
- V.23
- V.24
- V.250
- V.27
- V.28
- V.29

Data Link Control

Data link control

Most important functions in the data link layer

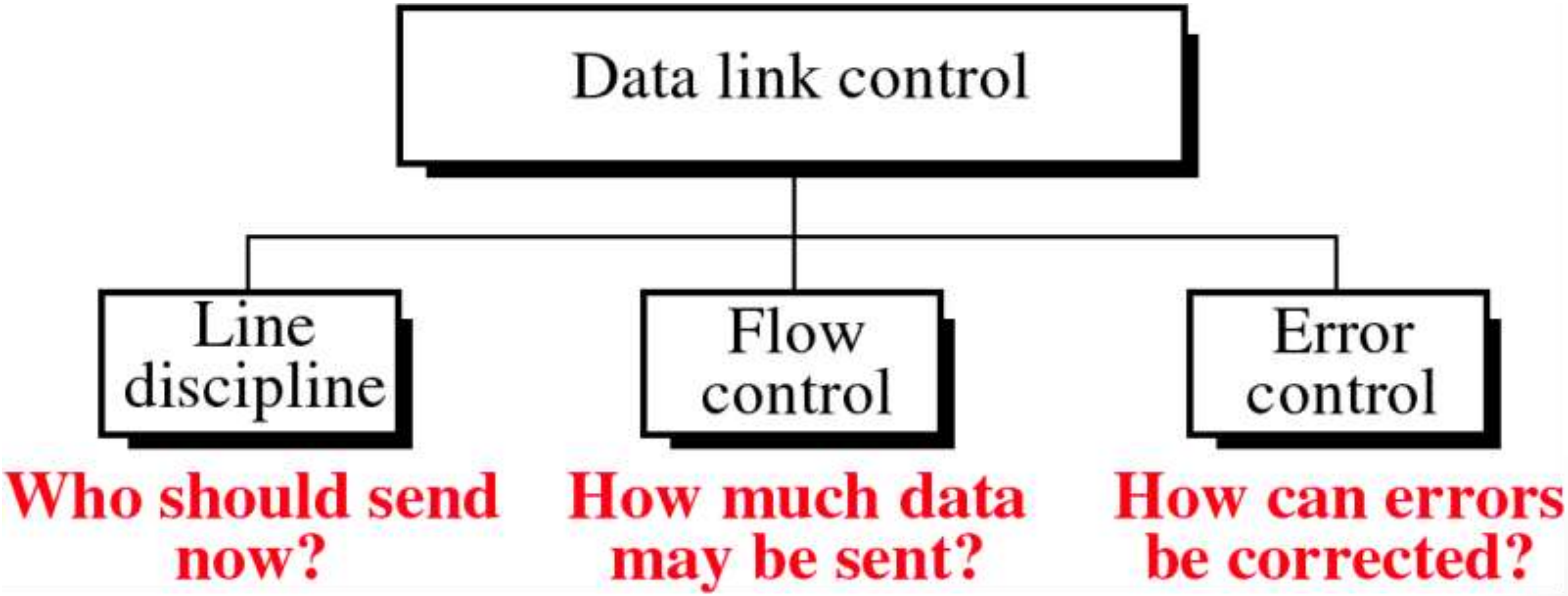
are:

Line control

Flow control

Error control

Collectively, these functions are known as **data link control.**

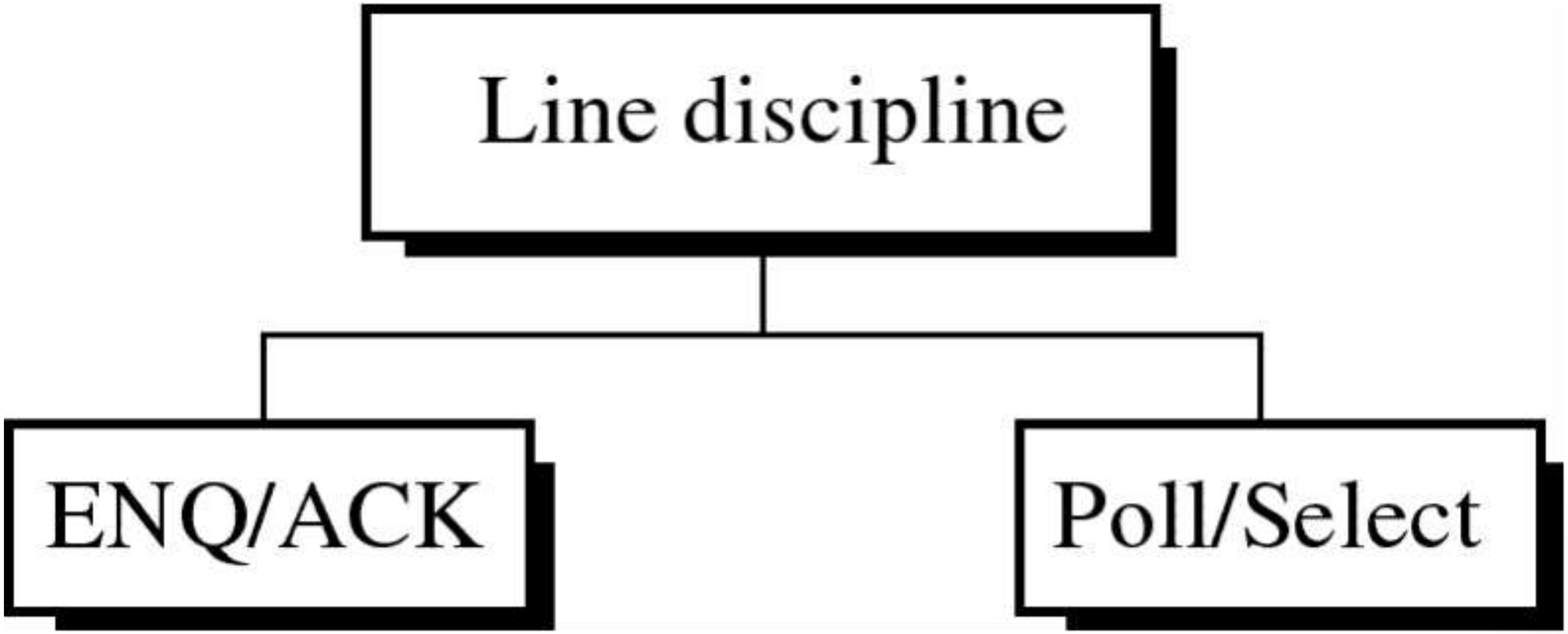


Who should send now?

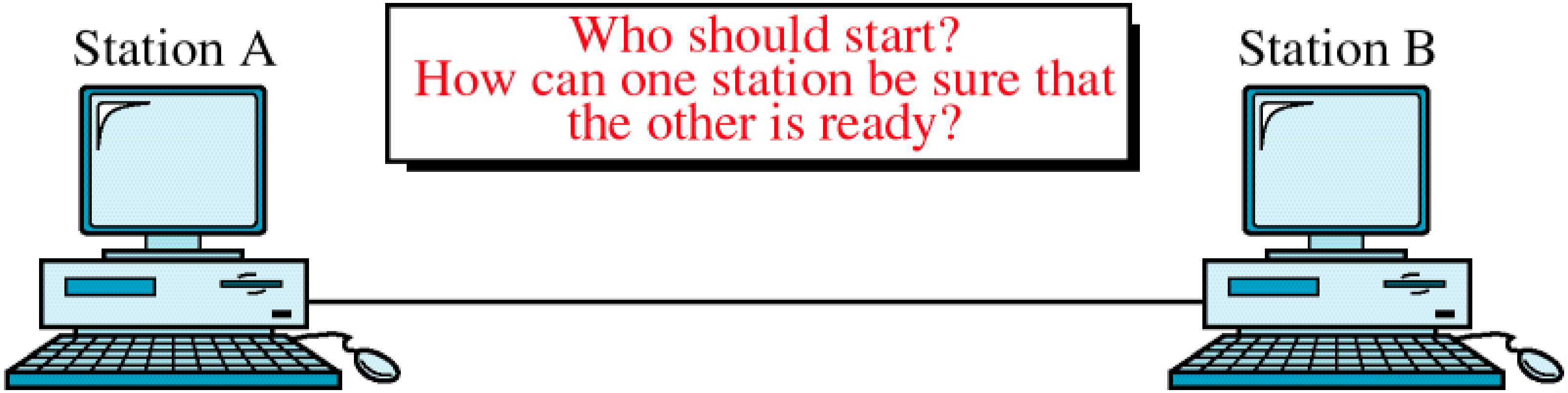
How much data may be sent?

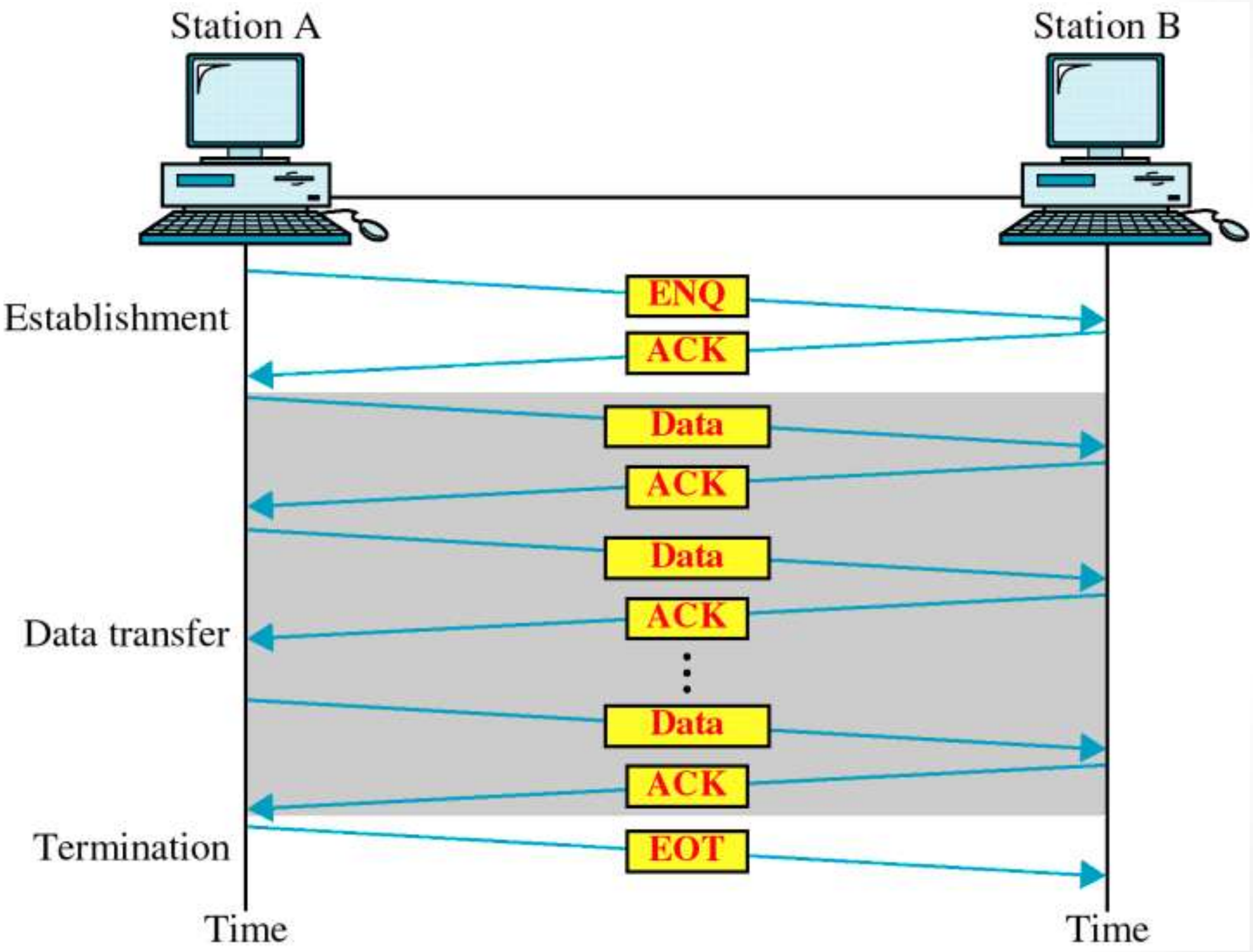
How can errors be corrected?

Line discipline can be done in two ways:



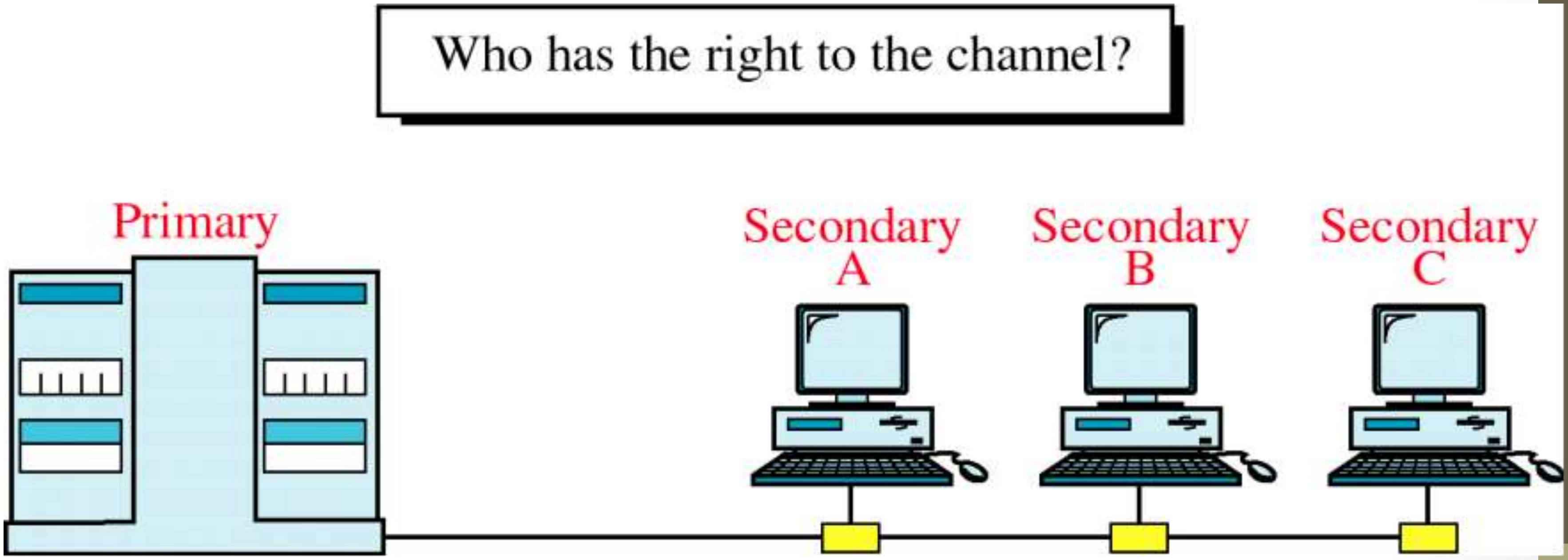
ENQ/ACK


Station A
Who should start?
How can one station be sure that
the other is ready?
Station B

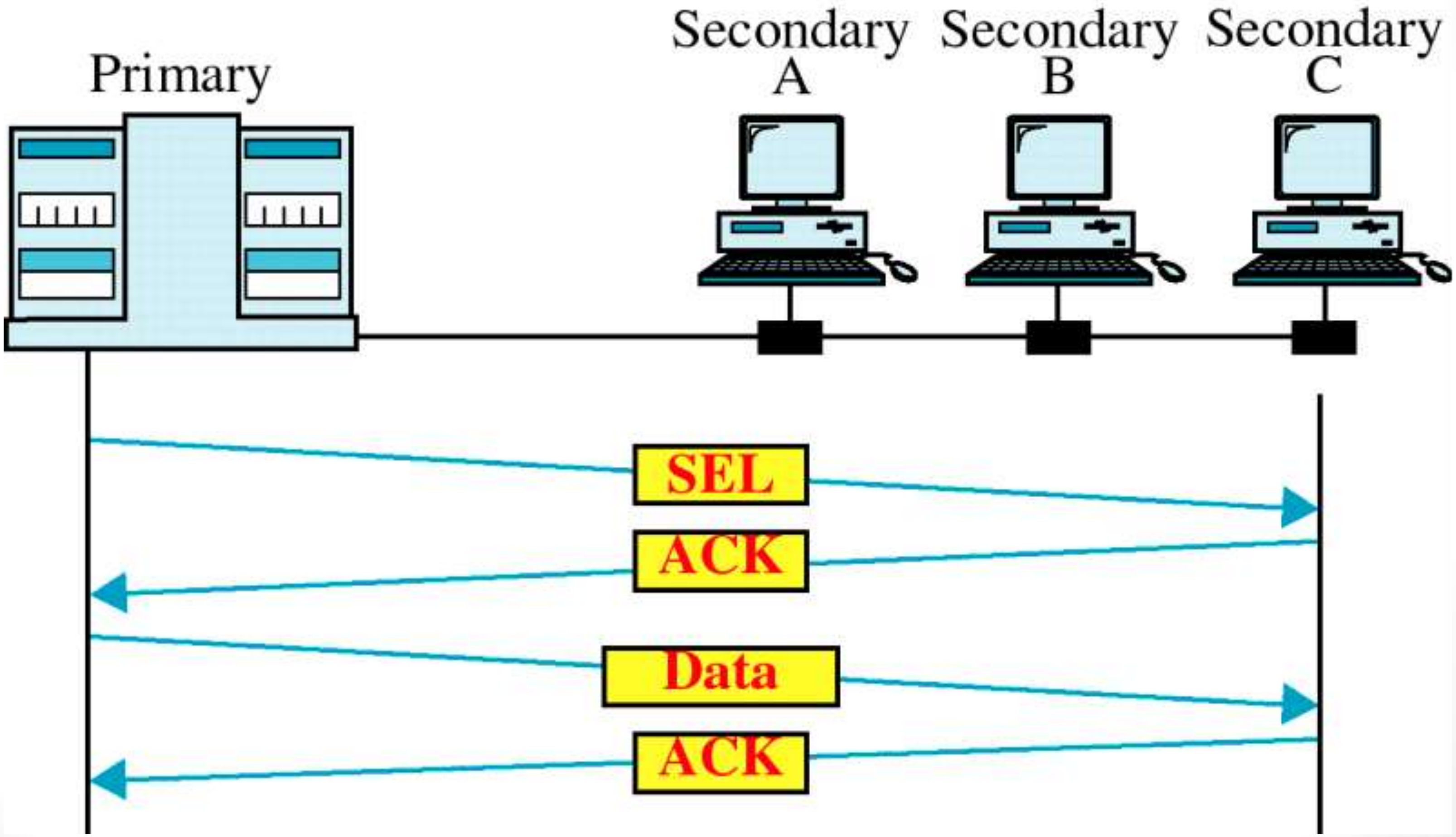

Station A
Station B
Establishment
ENQ
ACK
Data
ACK
Data
ACK
Data transfer
Data
ACK
Termination
EOT
Time
Time

Poll/Select

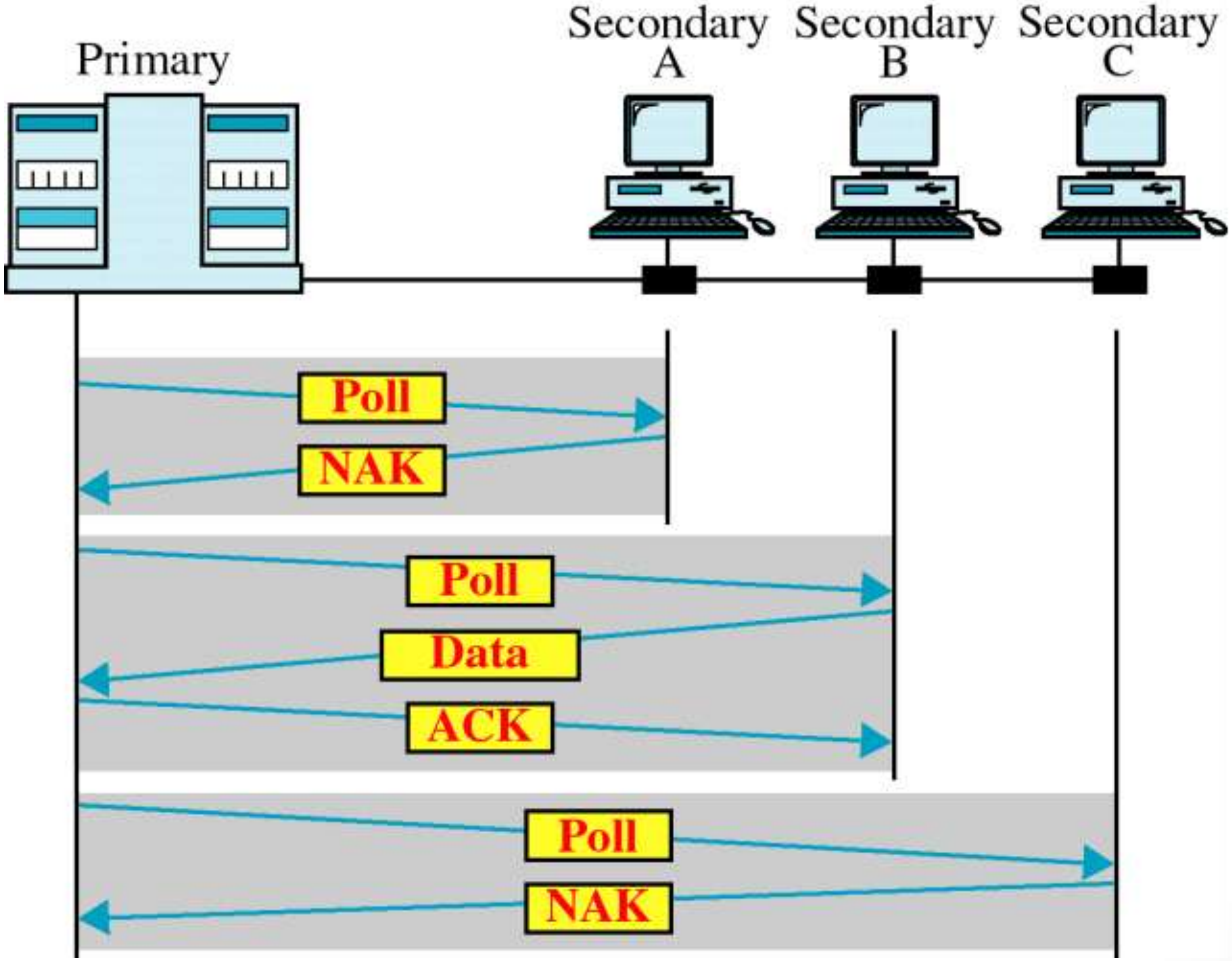
- Multipoint Discipline



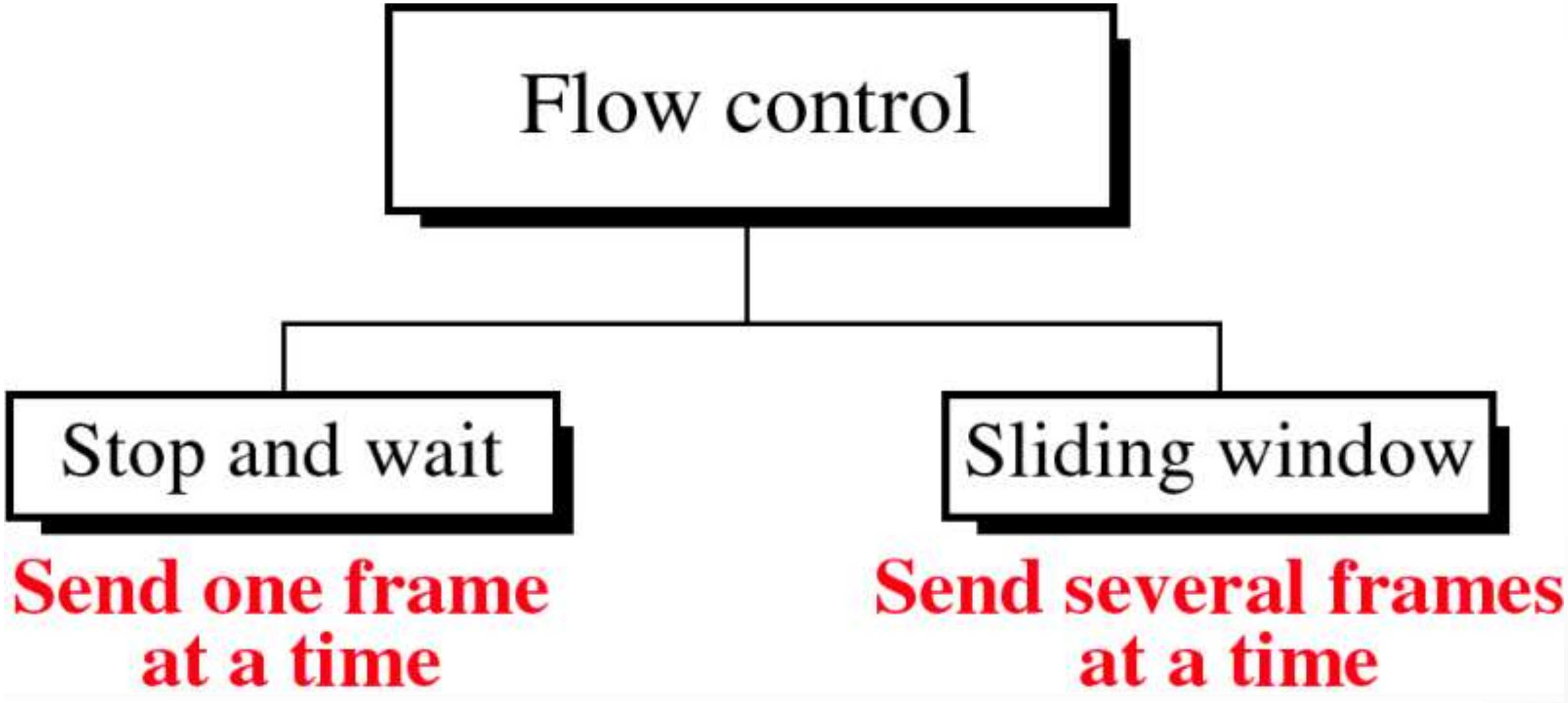
Select


Primary
Secondary A
Secondary B
Secondary C
SEL
ACK
Data
ACK

Poll


Primary
Secondary A
Secondary B
Secondary C
Poll
NAK
Poll
Data
ACK
Poll
NAK

Flow Control



Flow control

Stop and wait

Sliding window

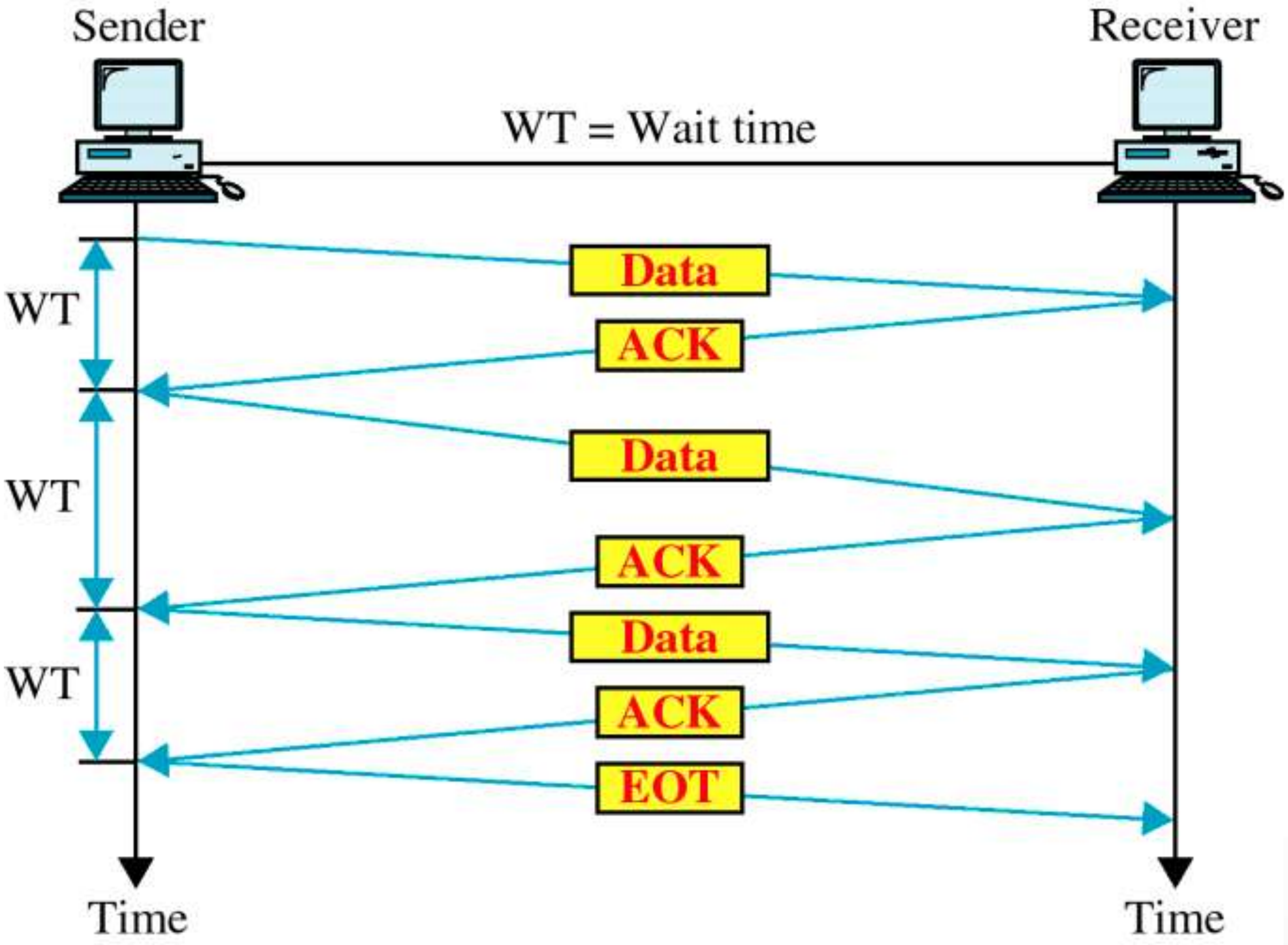
Send one frame at a time

Send several frames at a time

Stop & Wait

- In a stop-and-wait method of flow control, the sender waits for an acknowledgment after every frame it sends.
- Only when an acknowledgment has been received is the next frame sent.
- This process of alternately sending and waiting repeats until the sender transmits an EOT frame.

Stop & Wait


Sender
Receiver
WT = Wait time
WT
WT
WT
Data
ACK
Data
ACK
Data
ACK
EOT
Time
Time

Advantages and Disadvantage

Advantage

- Each frame is checked and acknowledged before the next frame is sent.

Disadvantage

- Inefficient (Very slow transmission)

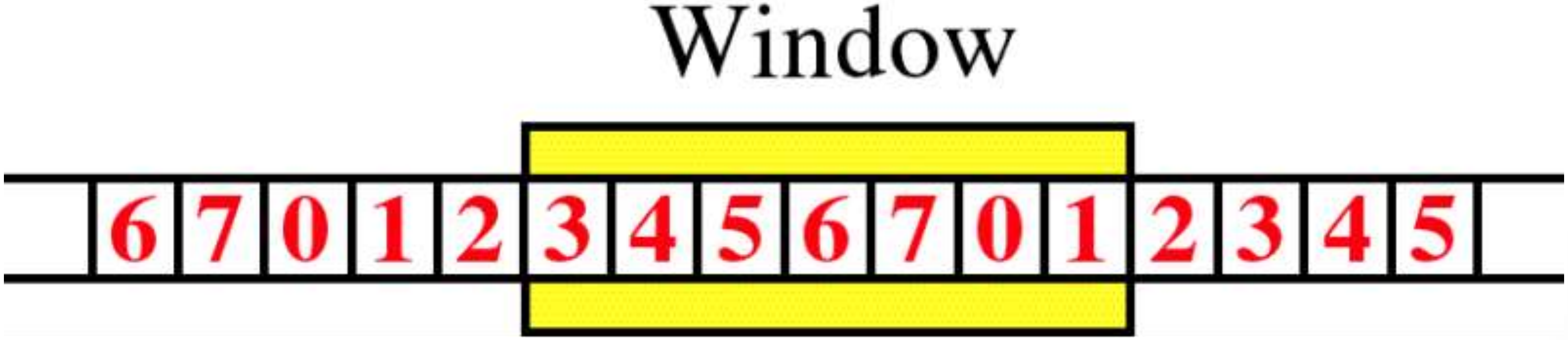
Sliding Window Protocol

- In the sliding window method of flow control, the sender can transmit several frames before needing an acknowledgment.
- Frames can be sent one after another, meaning that the link can carry several frames at once and its capacity can be used efficiently.
- The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

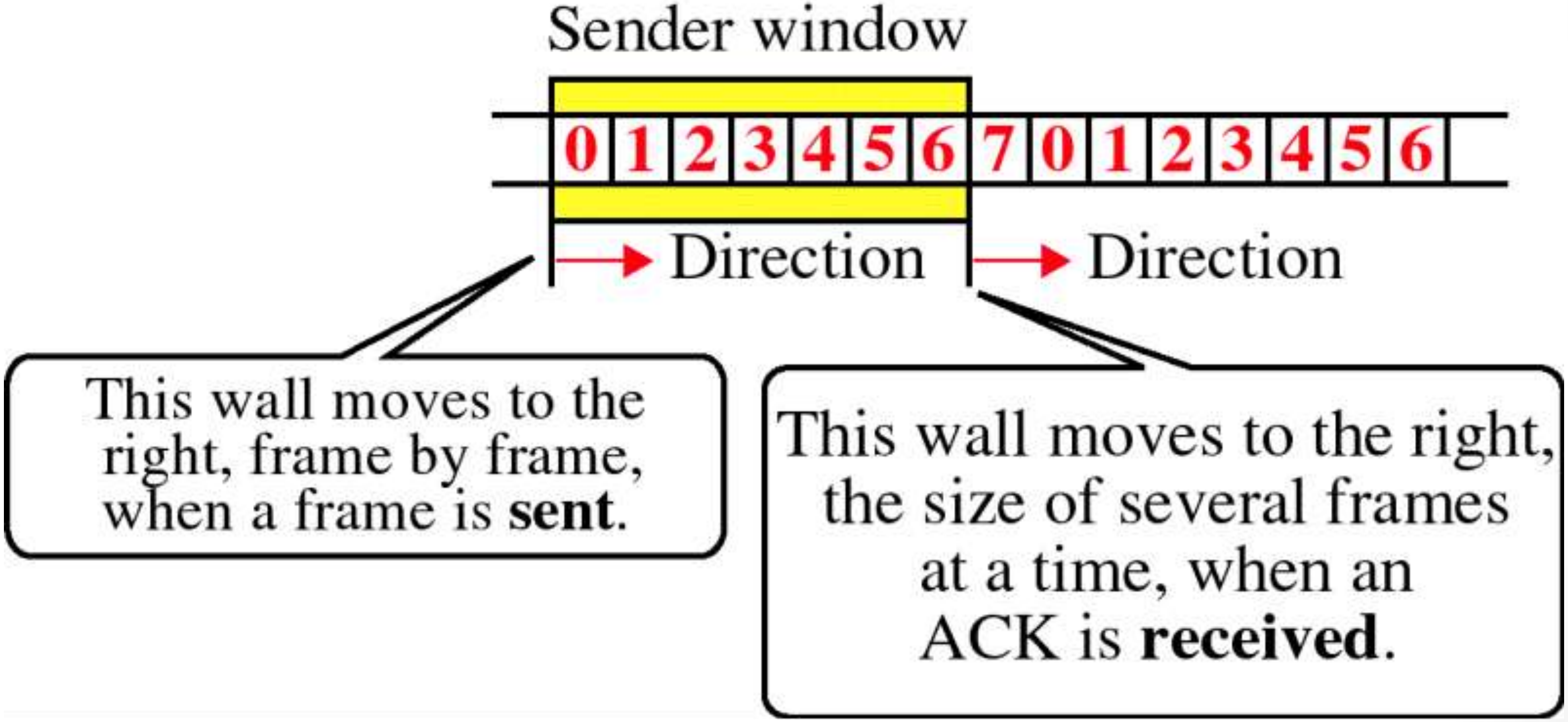
Continued……….

- Sliding window refers to imaginary boxes at both the sender and the receiver.
- The frames are numbered modulo-n, which means they are numbered from 0 to n-1.
- For example, if n=8, the frames are numbered 0,1,2,3,4,5,6,7,0,1,2,3,4,………….
- The size of the window is n-1. The window can hold n-1 frames at either end.

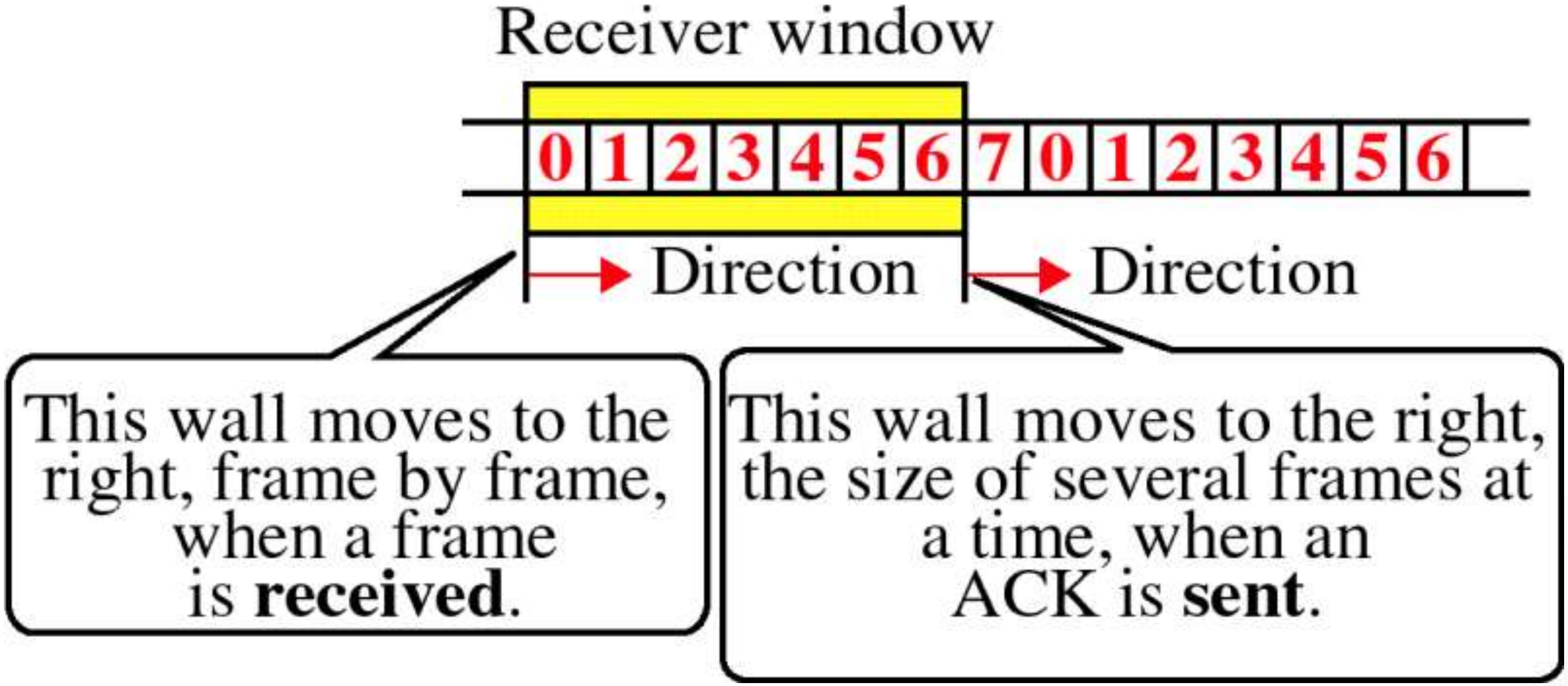
Sliding Window Protocol



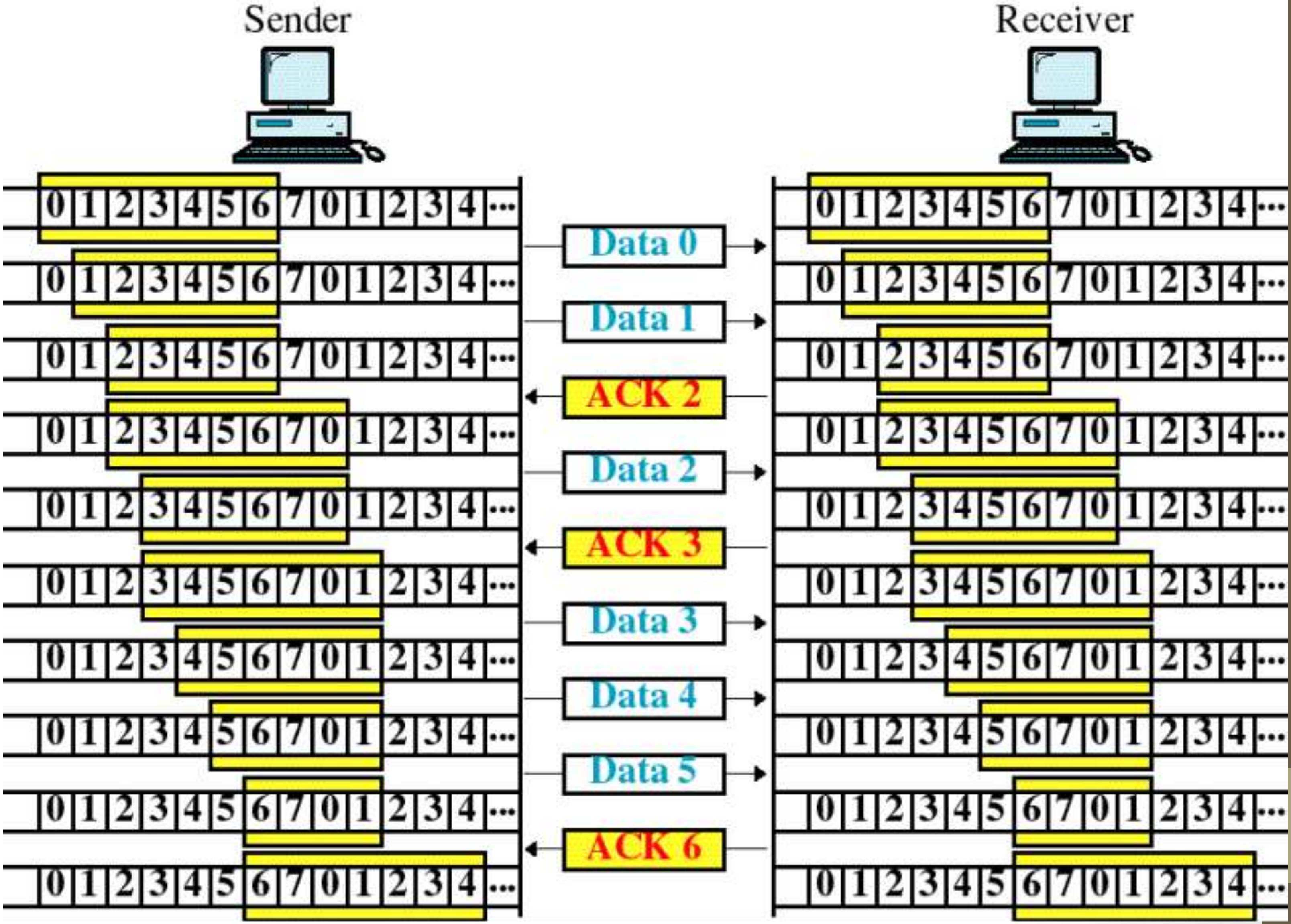
Sender’s Sliding Window


Sender window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right, frame by frame, when a frame is **sent**.
This wall moves to the right, the size of several frames at a time, when an ACK is **received**.

Receiver Sliding Window

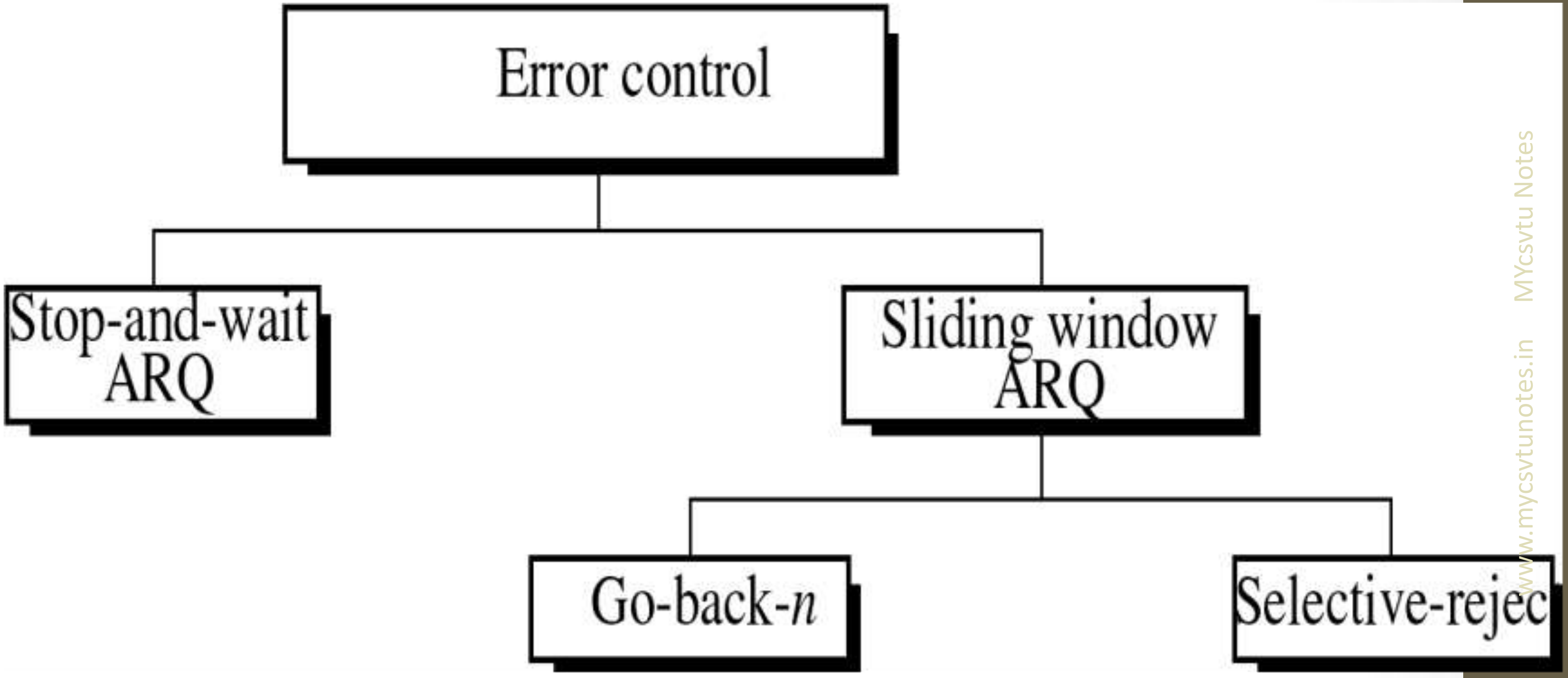

Receiver window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right, frame by frame, when a frame is **received**.
This wall moves to the right, the size of several frames at a time, when an ACK is **sent**.

Example of Sliding Window



Error control

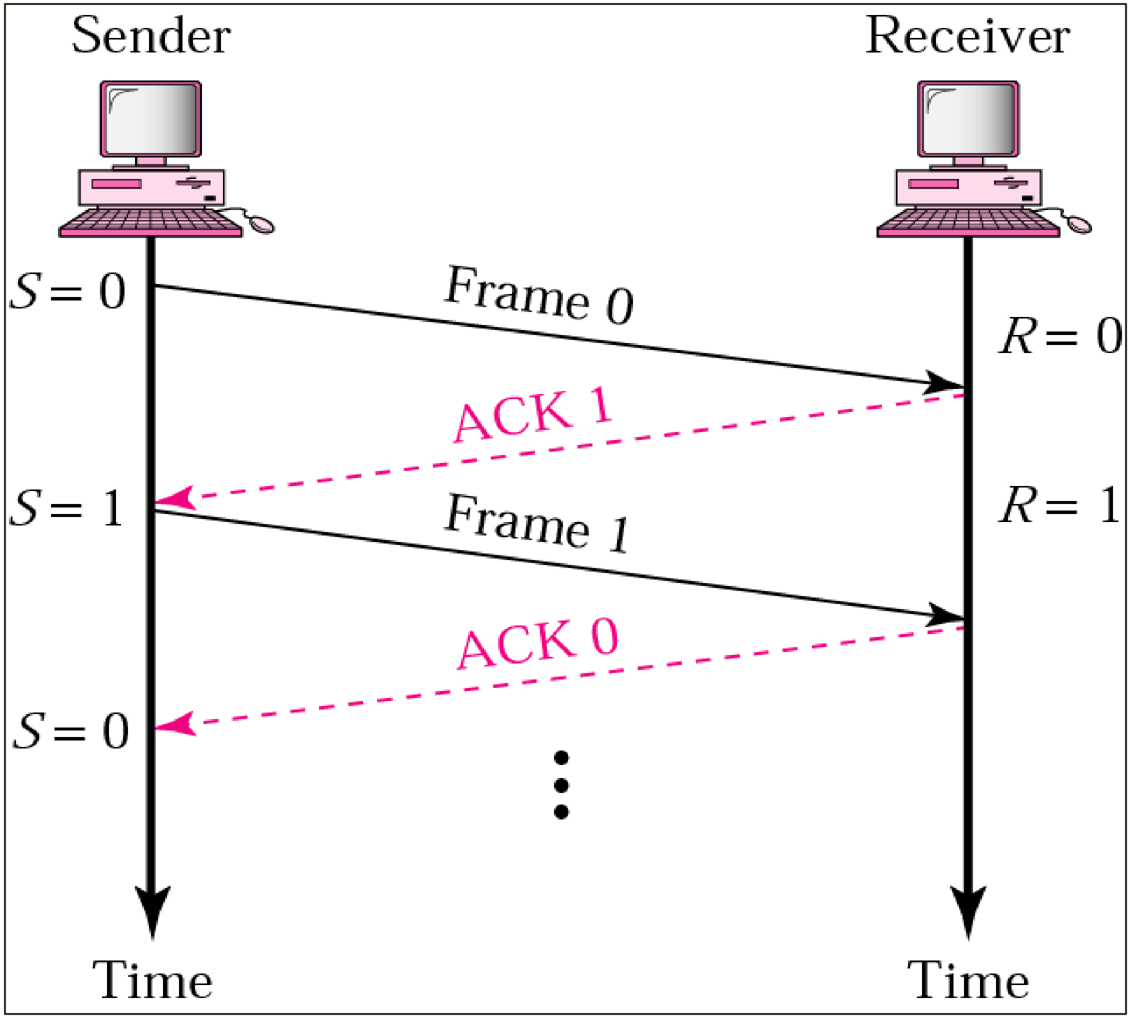
- Error control refers to the methods of error detection and correction.
- Error control is based on automatic repeat request (ARQ), which means retransmission of data in three cases:
  - damaged frame,
  - lost frame and
  - lost acknowledgment


Error control
Stop-and-wait ARQ
Sliding window ARQ
Go-back-*n*
Selective-rejec

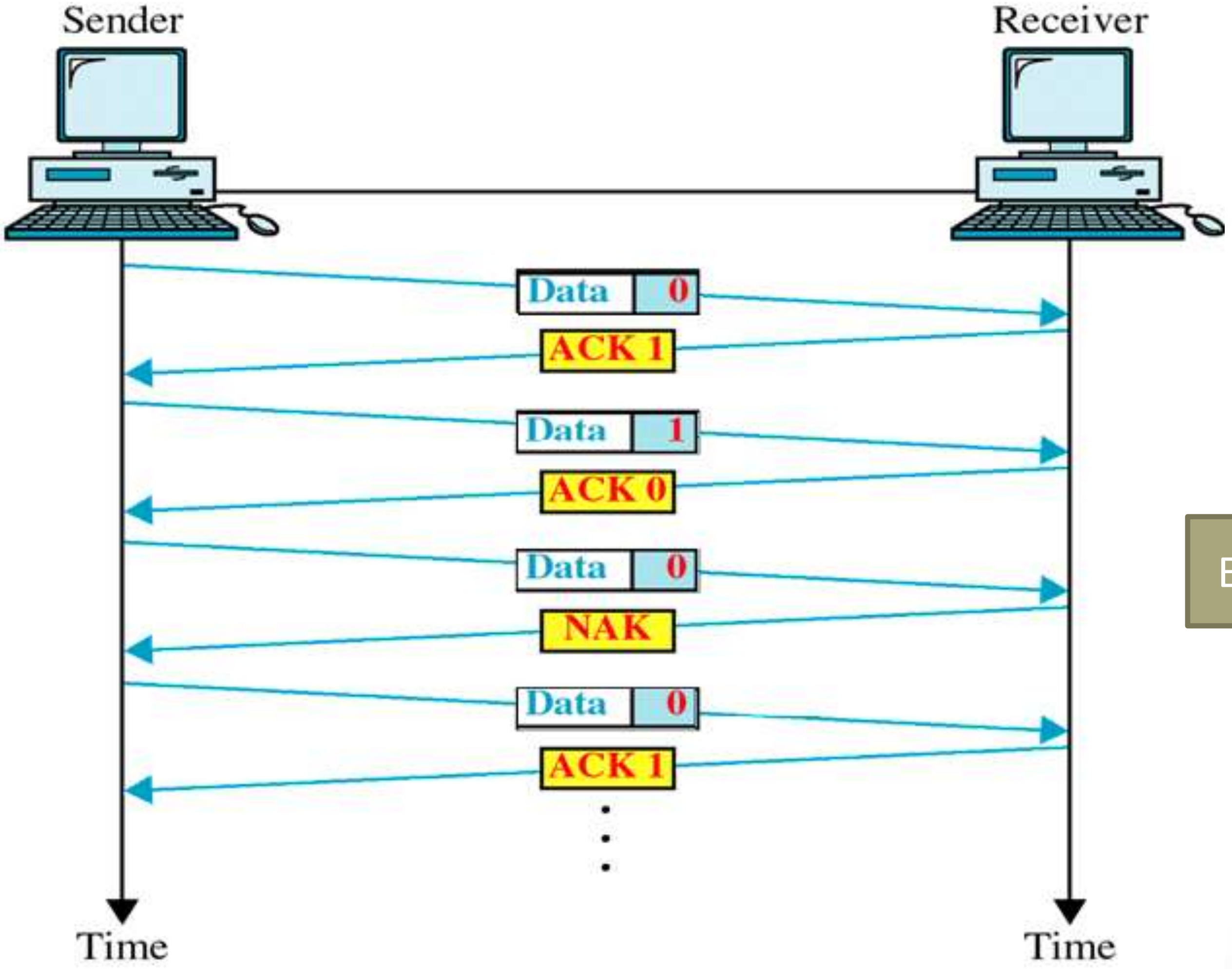
Stop-and-wait ARQ

- Four features are added to the basic flow control mechanism
  - The sending device must keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame.
  - For identification purposes, both data frames and ACK frames are numbered alternately 0 and 1.
  - If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned.
  - The sending device is equipped with a timer.

Normal Operation

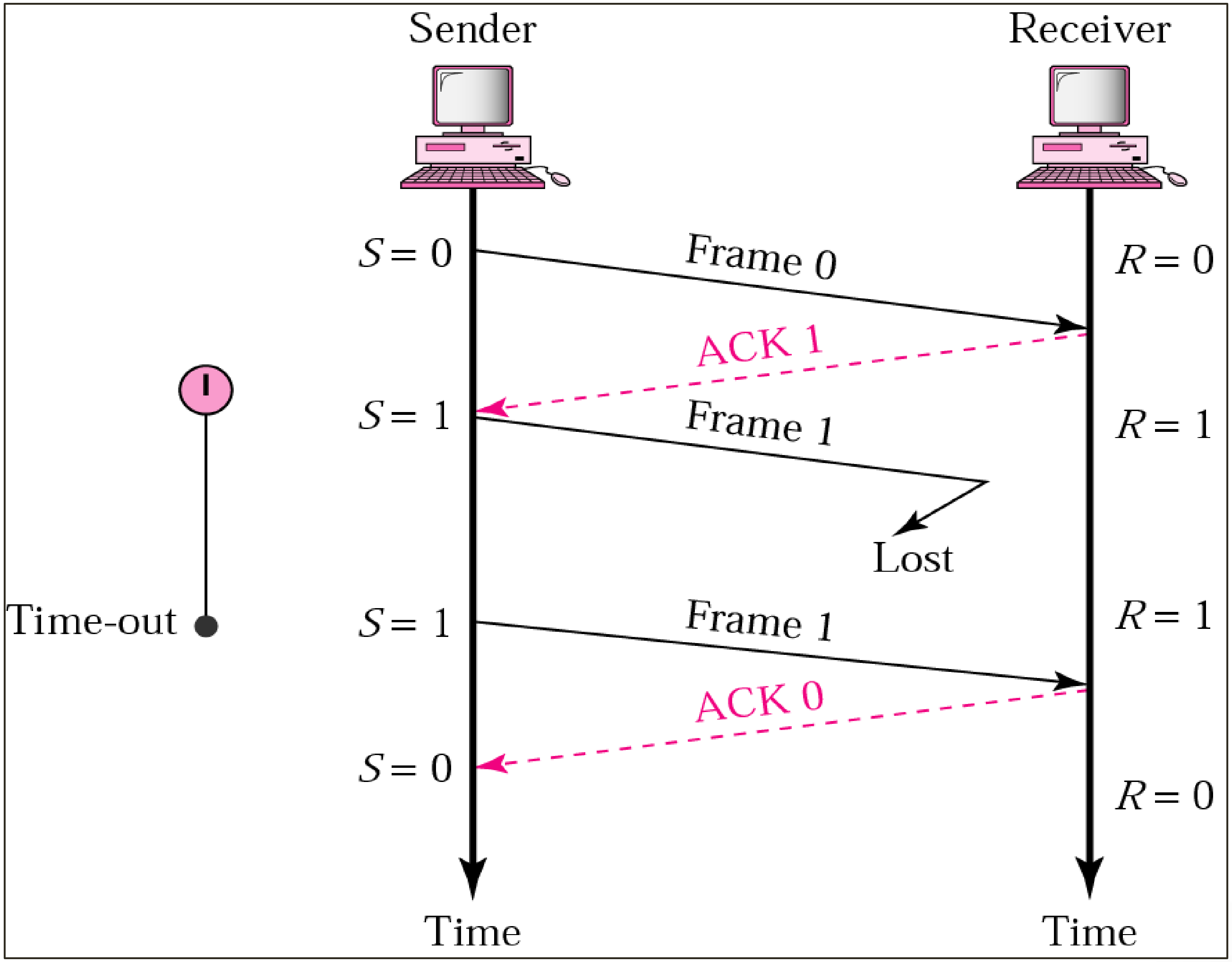


Damaged frame

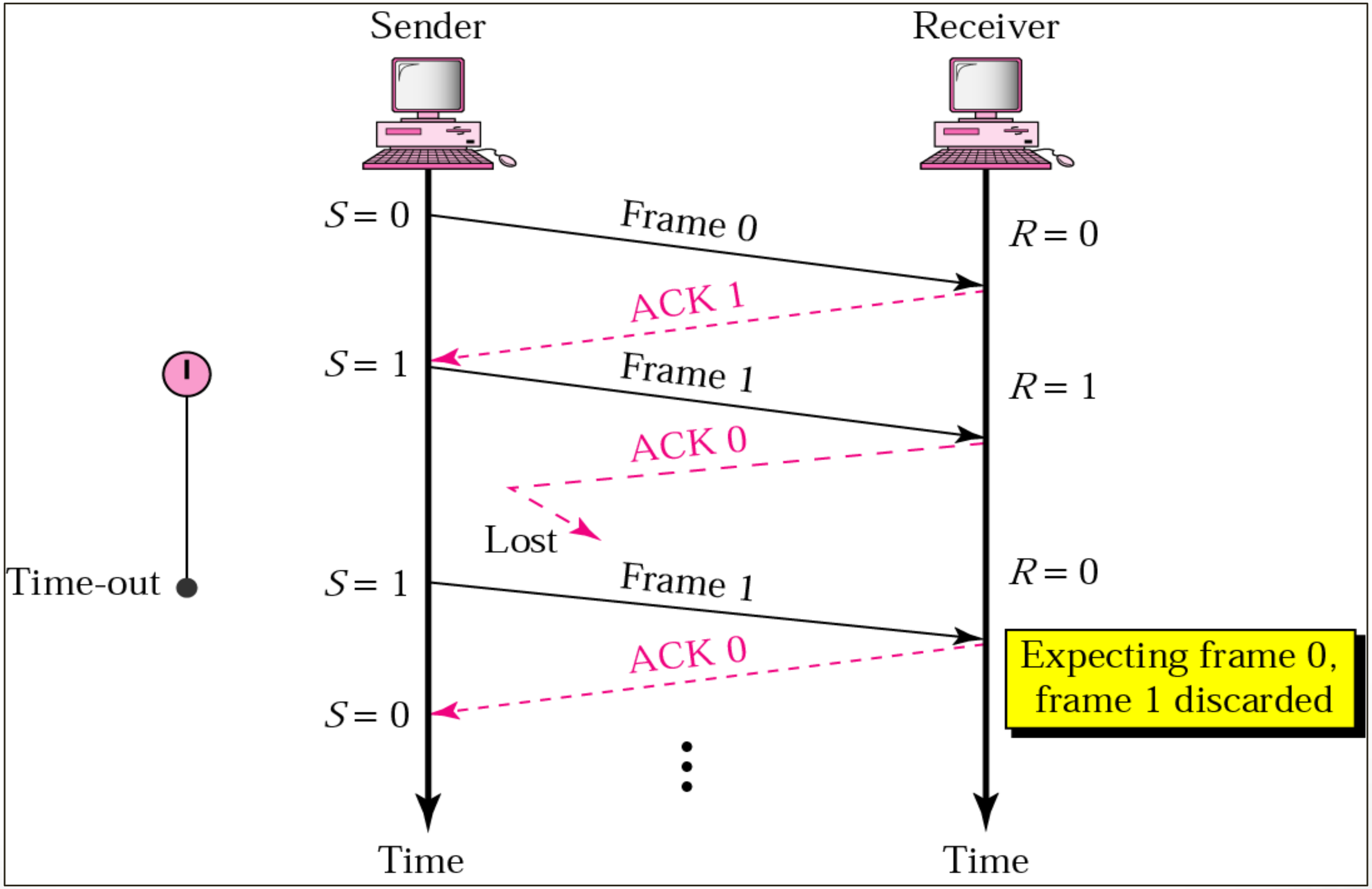


Error in frame 0

Lost frame


Sender
Receiver
$S = 0$
Frame 0
$R = 0$
ACK 1
$S = 1$
Frame 1
$R = 1$
Lost
Time-out
$S = 1$
Frame 1
$R = 1$
ACK 0
$S = 0$
$R = 0$
Time
Time

Lost or Damaged Acknowledgement



Disadvantages of previous method

- Data frames flow in only one direction
- Control information such as ACK and NAK frames can travel in the other direction

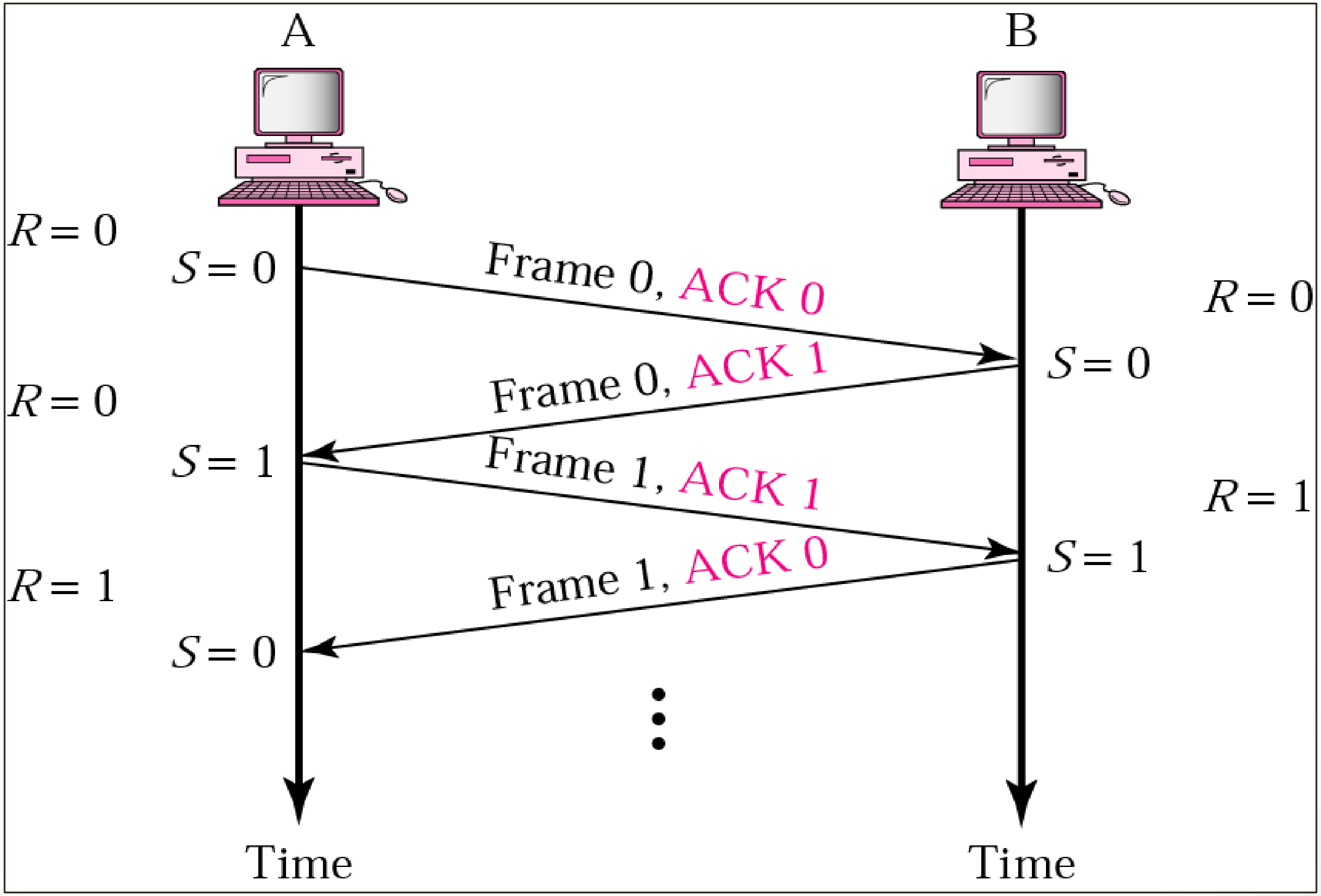
Piggy Backing

- In real life, data frames are normally flowing in both directions: from node A to node B and from node B to node A.
- This means that the control information also needs to flow in both directions.
- A technique called **piggybacking** is used to improve the efficiency of the bidirectional protocols.
- When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B.
- When a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.
- Each node now has two windows: one send window and one receive window. Both also need to use a timer.
- Both are involved in three types of events: request, arrival, and time-out.

Continued……..

- However, the arrival event here is complicated; when a frame arrives, the site needs to handle control information as well as the frame itself.
- Both of these concerns must be taken care of in one event, the arrival event.
- The request event uses only the send window at each site; the arrival event needs to use both windows.

Piggy Backing



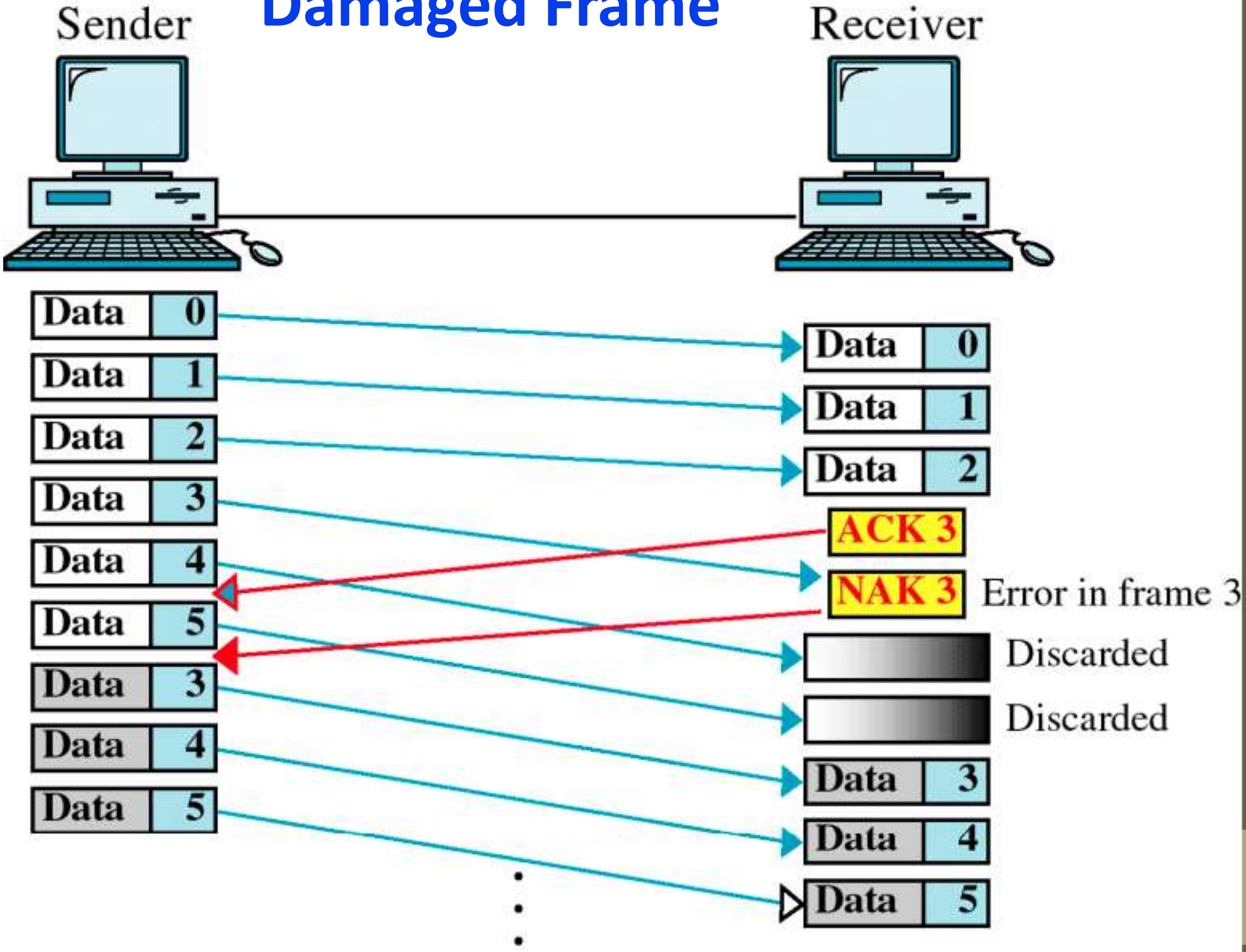
Sliding window ARQ

- Three features are added to the basic flow control mechanism
  - The sending device keeps copies of all transmitted frames until they have been acknowledged.
  - In addition to ACK frame, the receiver has the option of returning NAK frame if the data have bee received damaged.
  - The sending device is equipped with a timer.

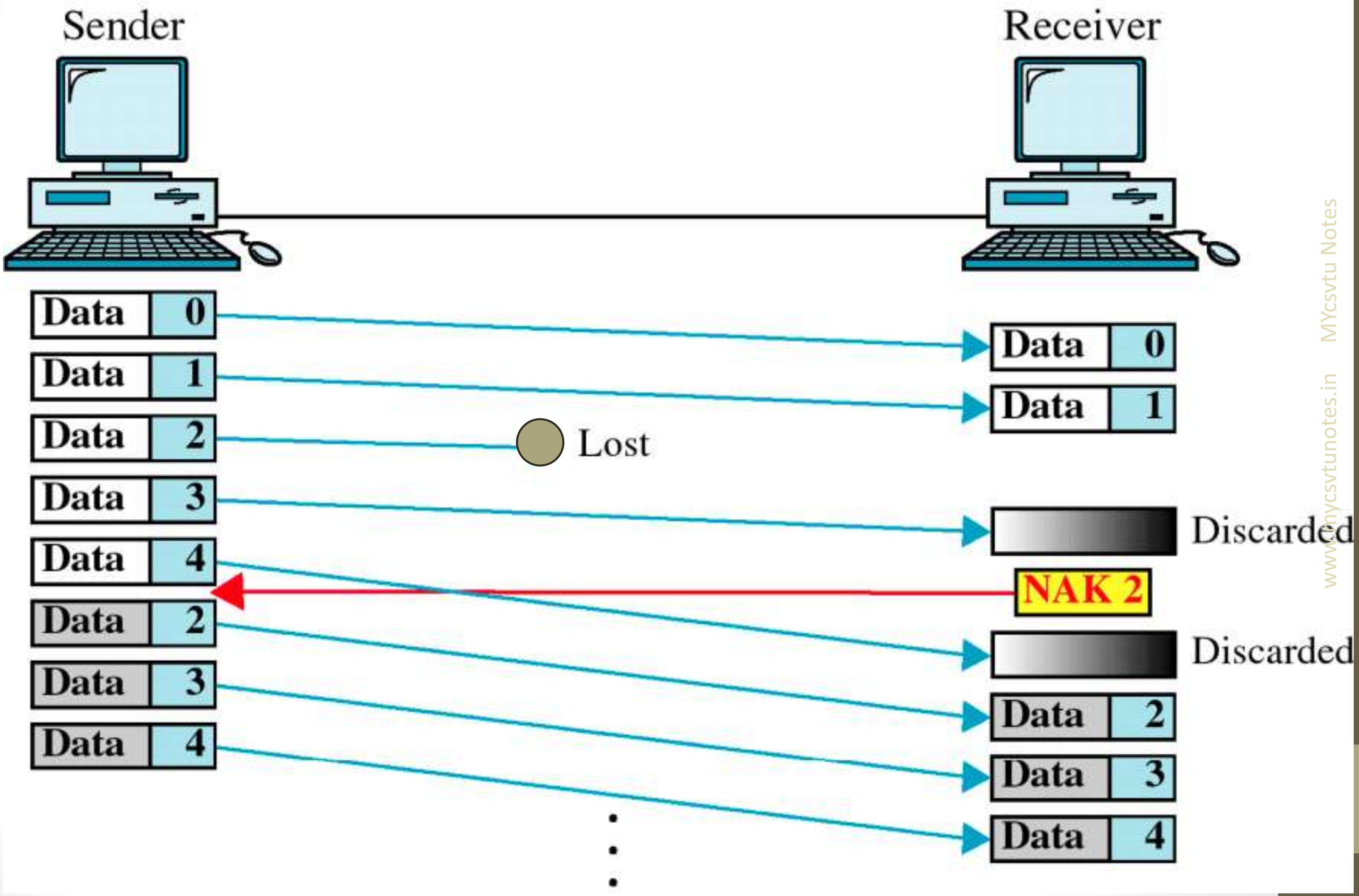
Go-Back-n ARQ

- In this sliding window go-back-n ARQ method, if one frame is lost or damaged, all frames sent since the last frame acknowledged are retransmitted.
-

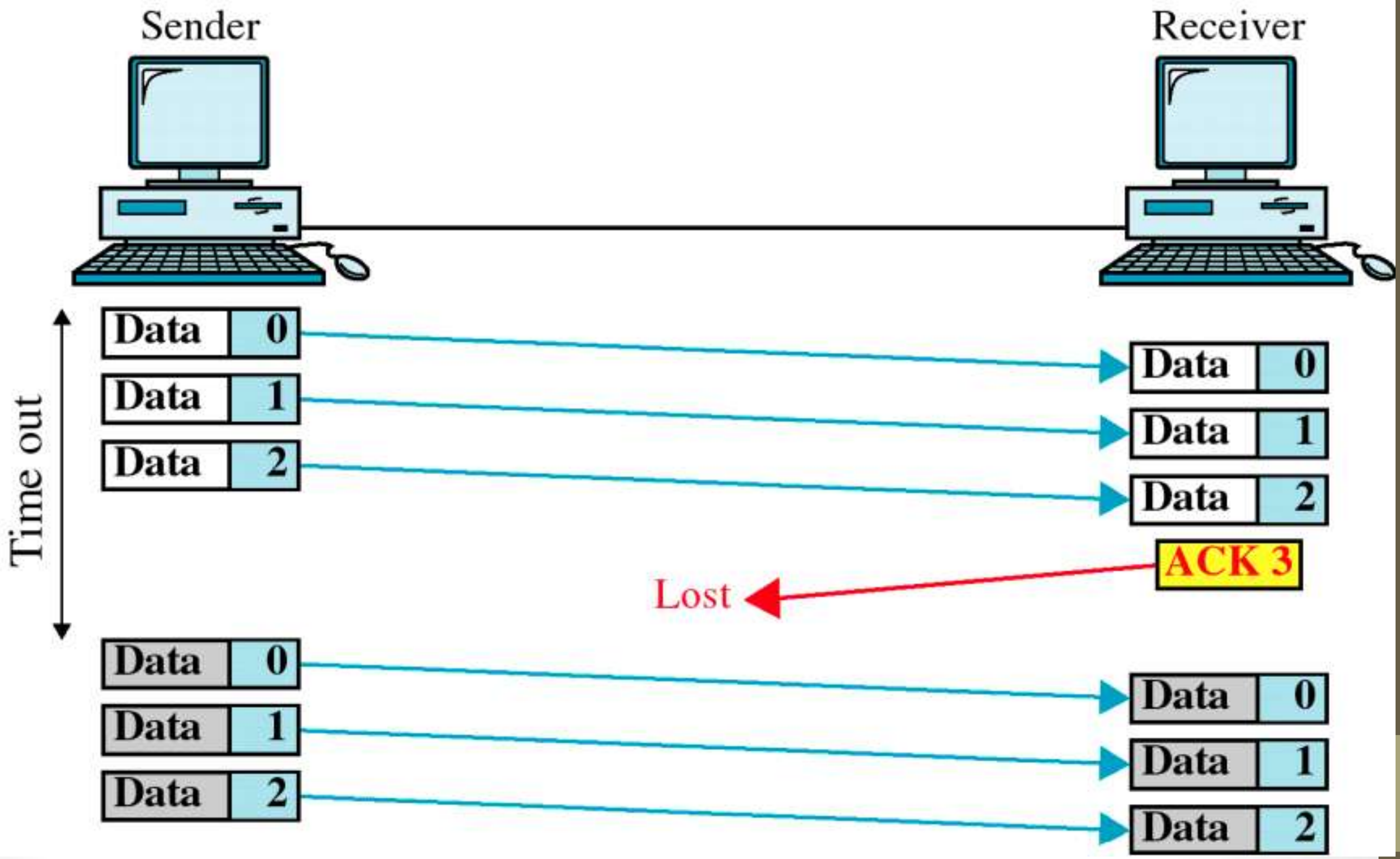
Damaged Frame



Lost Frame


Sender
Receiver
Data 0
Data 1
Data 2
Data 3
Data 4
Data 2
Data 3
Data 4
Lost
Data 0
Data 1
Discarded
NAK 2
Discarded
Data 2
Data 3
Data 4

Lost ACK


Sender
Receiver
Time out
Data 0
Data 1
Data 2
Data 0
Data 1
Data 2
ACK 3
Lost
Data 0
Data 1
Data 2
Data 0
Data 1
Data 2

Selective Reject

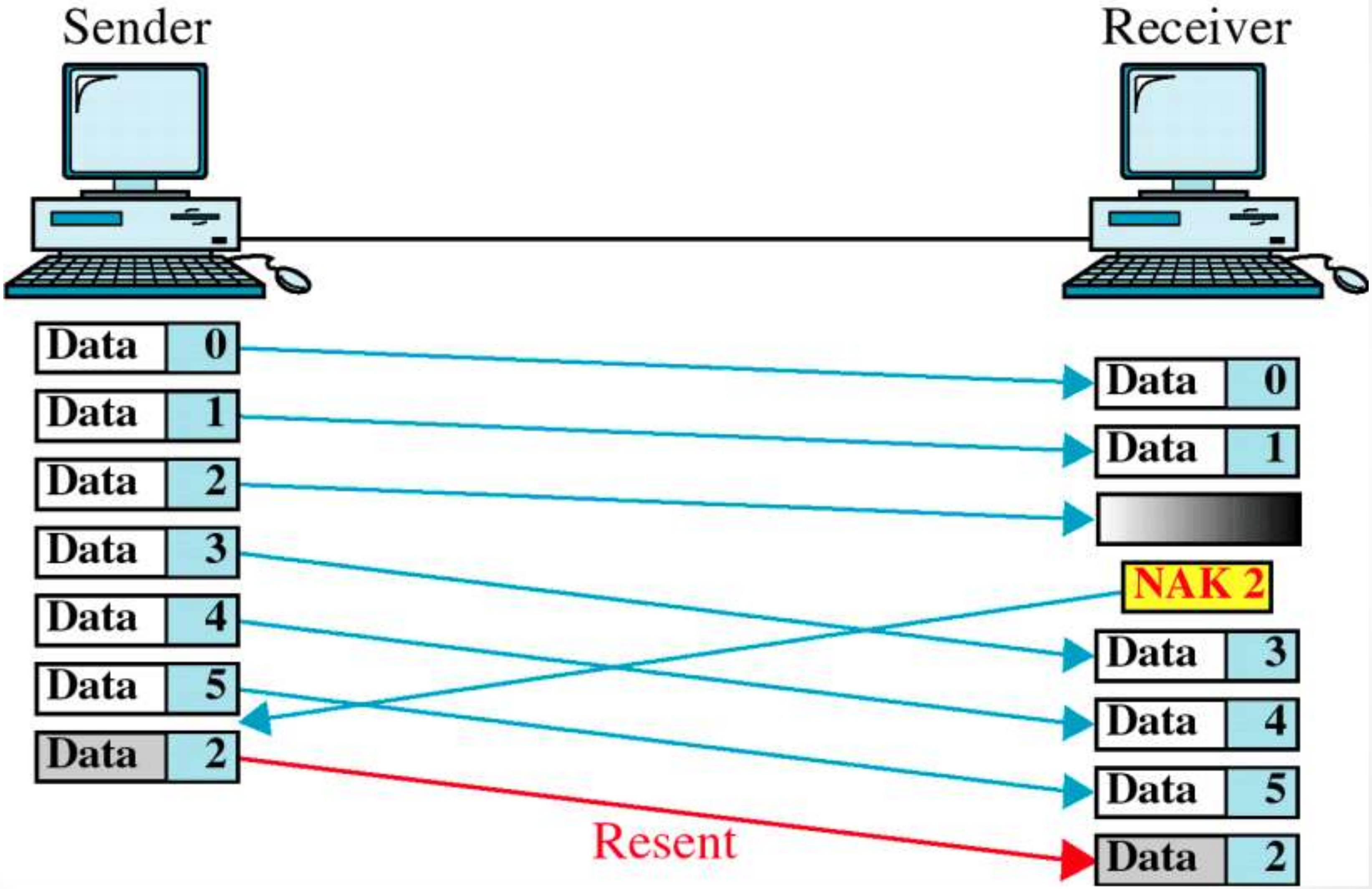
- In this, only the specific damaged or lost frame is retransmitted.
- If a frame is corrupted in transit, a NAK is returned and the frame is resent out of sequence.

Continued….

To make such selectivity possible, a selective reject ARQ system differs from a go-back-n ARQ system in the following ways:

1. The receiving device must contain sorting logic to enable it to reorder frames received out of sequence.
2. The sending device must contain a searching mechanism that allows it to find and select only the requested frame for retransmission.
3. A buffer in the receiver must keep all previously received frames on hold until all retransmissions have been sorted and any duplicate frames have been identified and discarded.

Selective Reject



Error Detection and Correction

Note:

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.

Types of Error

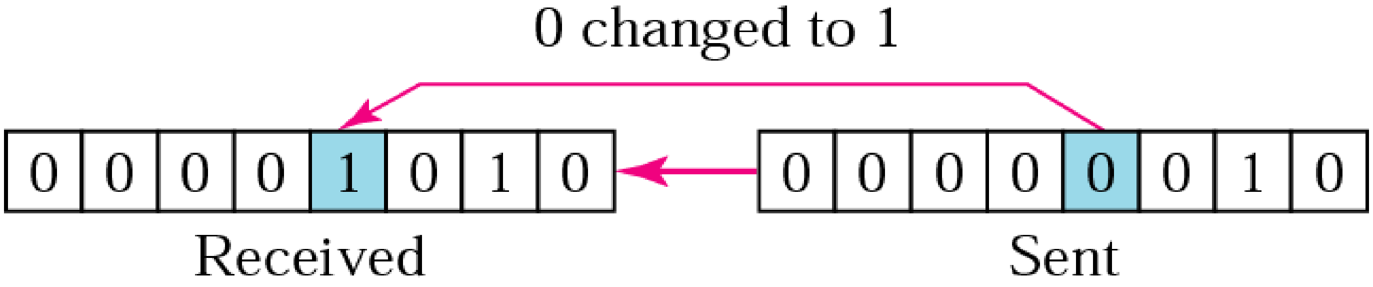
Single-Bit Error

Burst Error

Note:

In a single-bit error, only one bit in the data unit has changed.

Single-bit error



0 changed to 1

0 0 0 0 1 0 1 0

Received

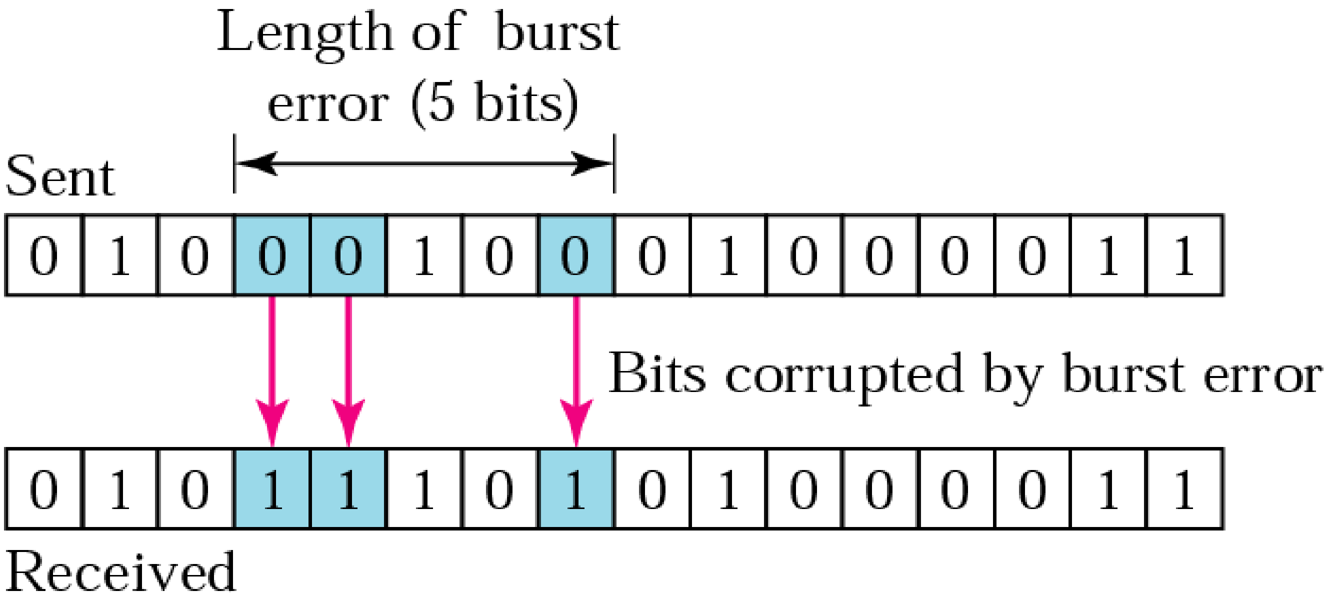
0 0 0 0 0 0 1 0

Sent

Note:

A burst error means that 2 or more bits in the data unit have changed.

Burst error of length 5



Sent	0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1
Received	0	1	0	1	1	1	0	1	0	1	0	0	0	0	1	1

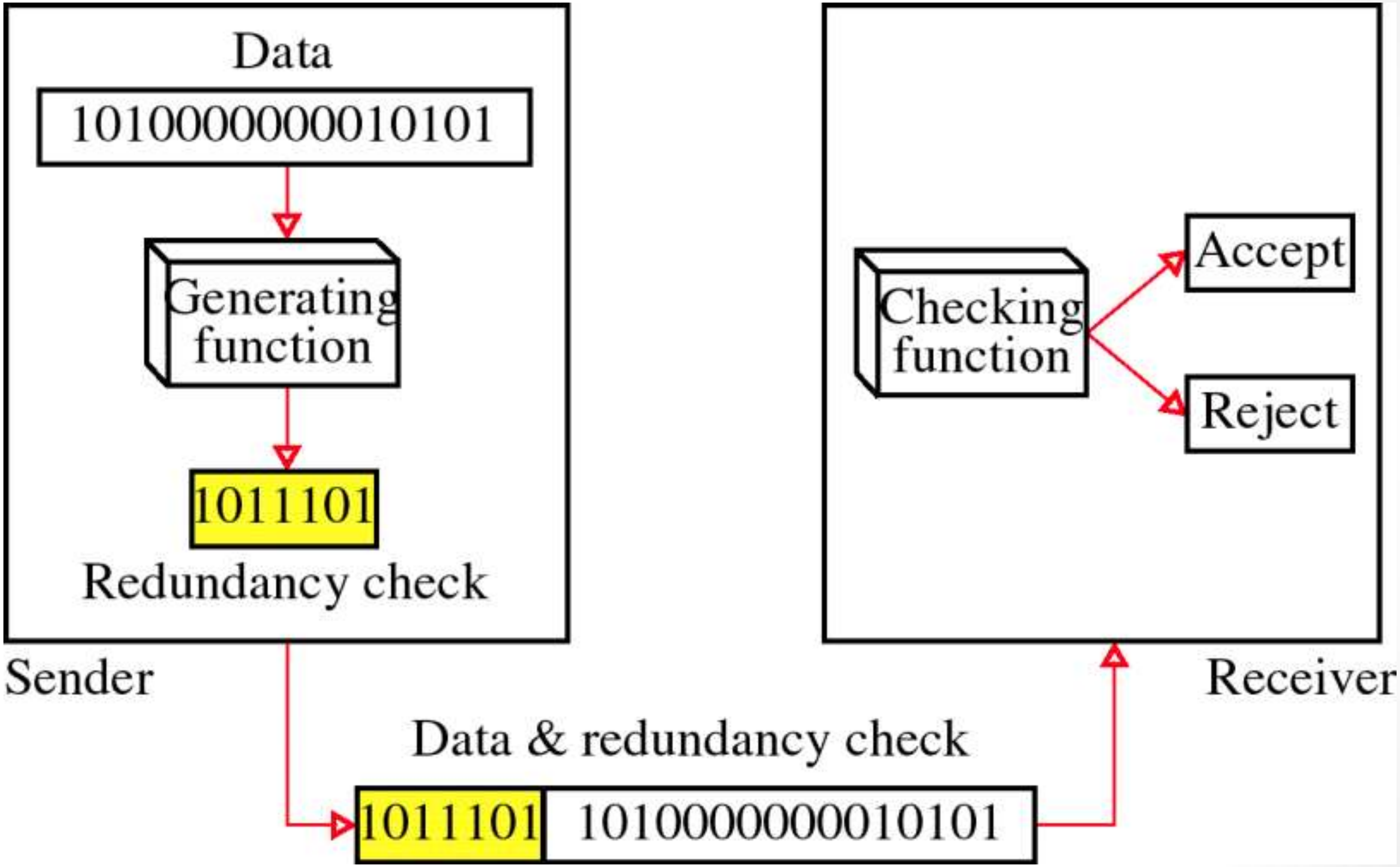
Error Detection Methods

- Vertical redundancy check (VRC) or Parity Check
- Longitudinal redundancy check(LRC)
- Cyclic Redundancy Check (CRC)
- Checksum

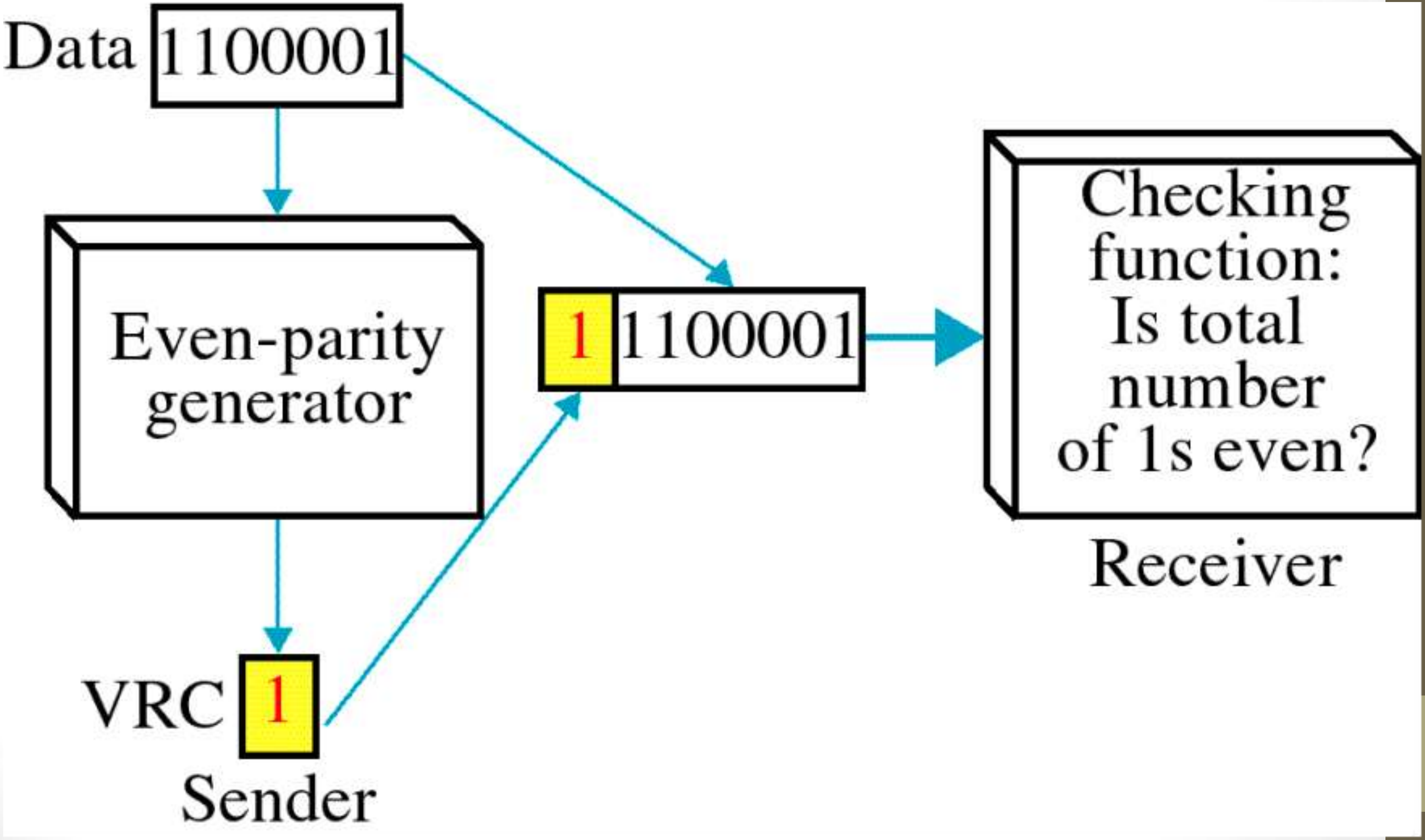
Note:

Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.

Redundancy


Data
1010000000010101
Generating function
1011101
Redundancy check
Sender
Checking function
Accept
Reject
Receiver
Data & redundancy check
1011101
1010000000010101

Vertical redundancy check (VRC)



Note:

In parity check, a parity bit is added to every data unit so that the total number of 1s is even (or odd for odd-parity).

Example 1

Suppose the sender wants to send the word *world*. In ASCII the five characters are coded as

W-1110111	even	11101110
O -1101111	even	11011110
R- 1110010	even	11100100
L- 1101100	even	11011000
D- 1100100	odd	11001001

The following shows the actual bits sent

11101110 11011110 11100100 11011000 11001001

Example 2

Now suppose the word world in Example 1 is received by the receiver without being corrupted in transmission.

11101110 11011110 11100100 11011000 11001001

The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4, 4). The data are accepted.

Example 3

Now suppose the word world in Example 1 is corrupted during transmission.

11111110 11011110 11101100 11011000 11001001

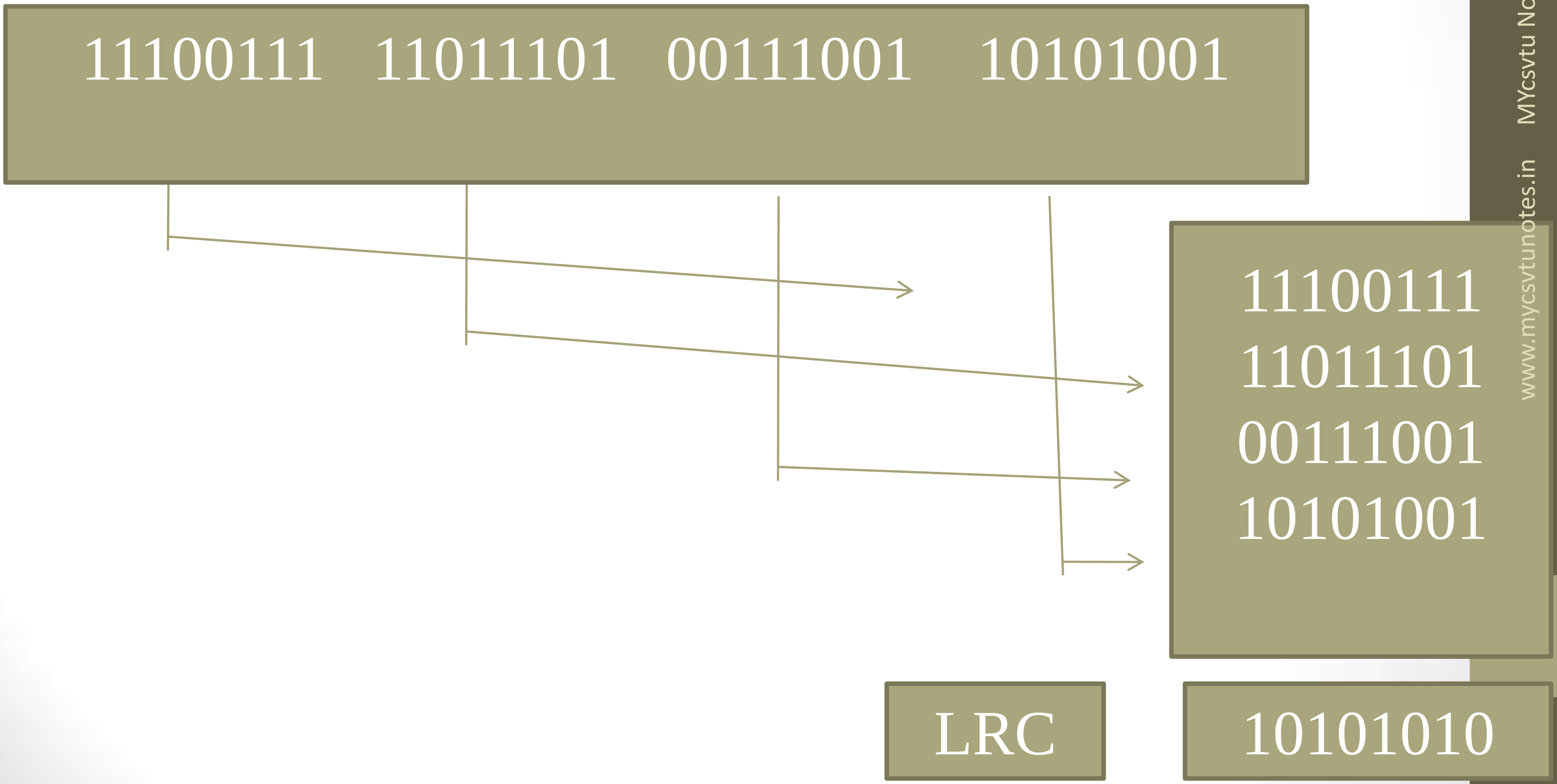
The receiver counts the 1s in each character and comes up with even and odd numbers (7, 6, 5, 4, 4). The receiver knows that the data are corrupted, discards them, and asks for retransmission.

Performance

- VRC can detect all single-bit error.

Longitudinal redundancy check(LRC)

- A block of bits is divided into rows and a redundant row of bits is added to the whole block.



11100111 11011101 00111001 10101001

11100111
11011101
00111001
10101001

LRC

10101010

Example 4

Suppose the following block is sent:

10101001 00111001 11011101 11100111 10101010

However, it is hit by a burst noise of length 8, and some bits are corrupted.

10100011 10001001 11011101 11100111 10101010

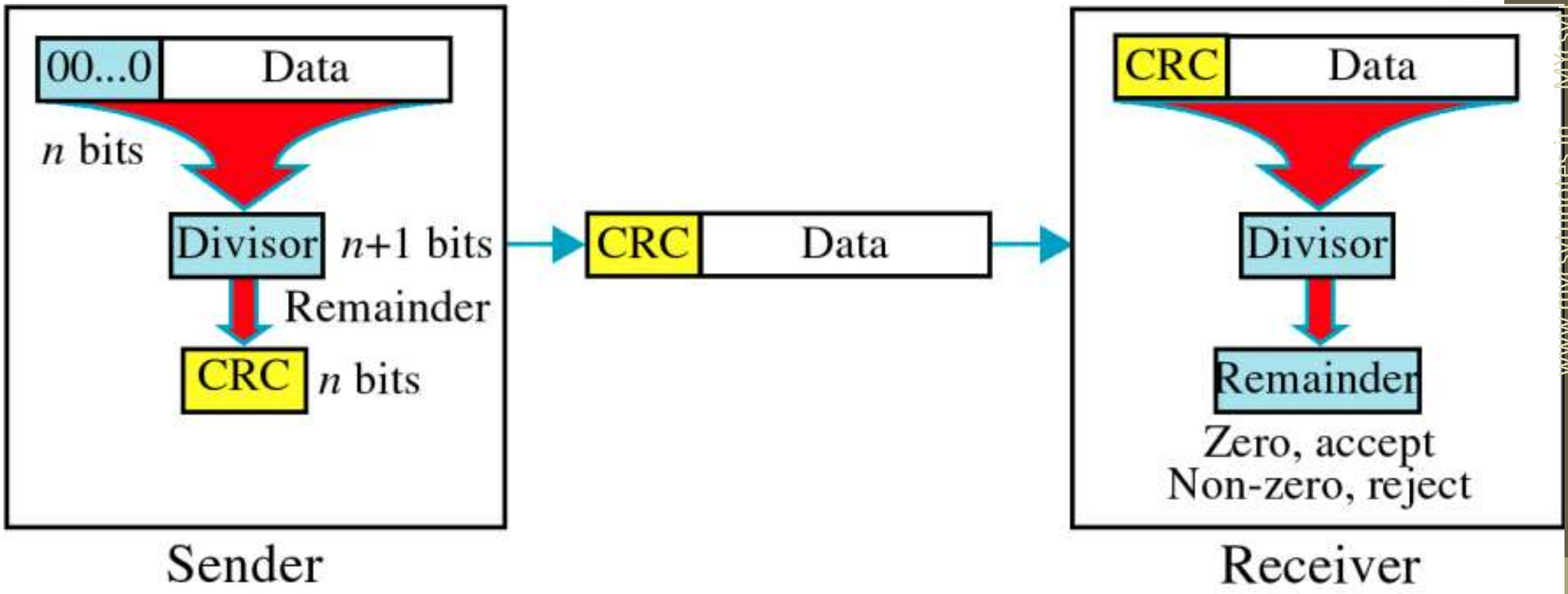
When the receiver checks the parity bits, some of the bits do not follow the even-parity rule and the whole block is discarded.

10100011 10001001 11011101 11100111 10101010

Performance

- LRC increases the likelihood of detecting burst errors.

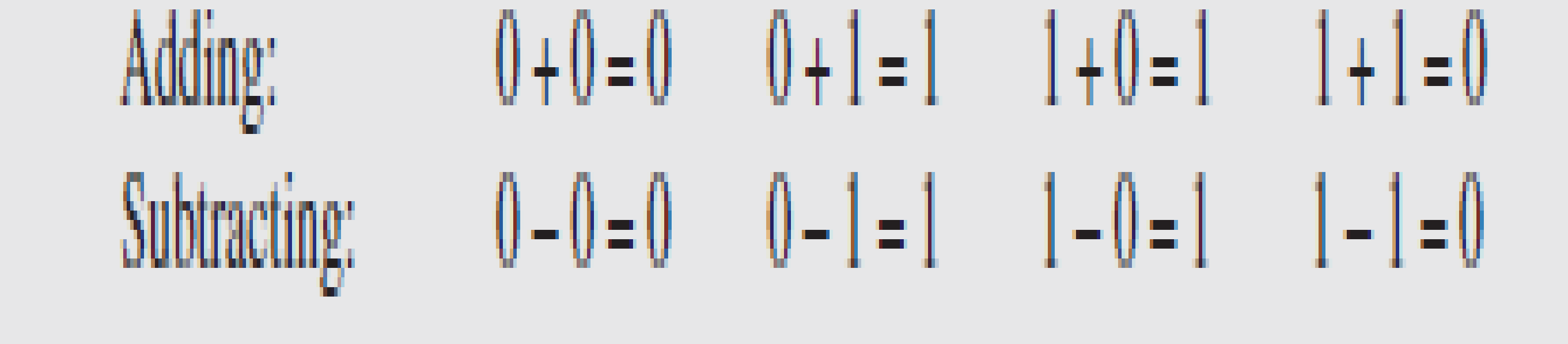
Cyclic Redundancy Check (CRC)



Steps

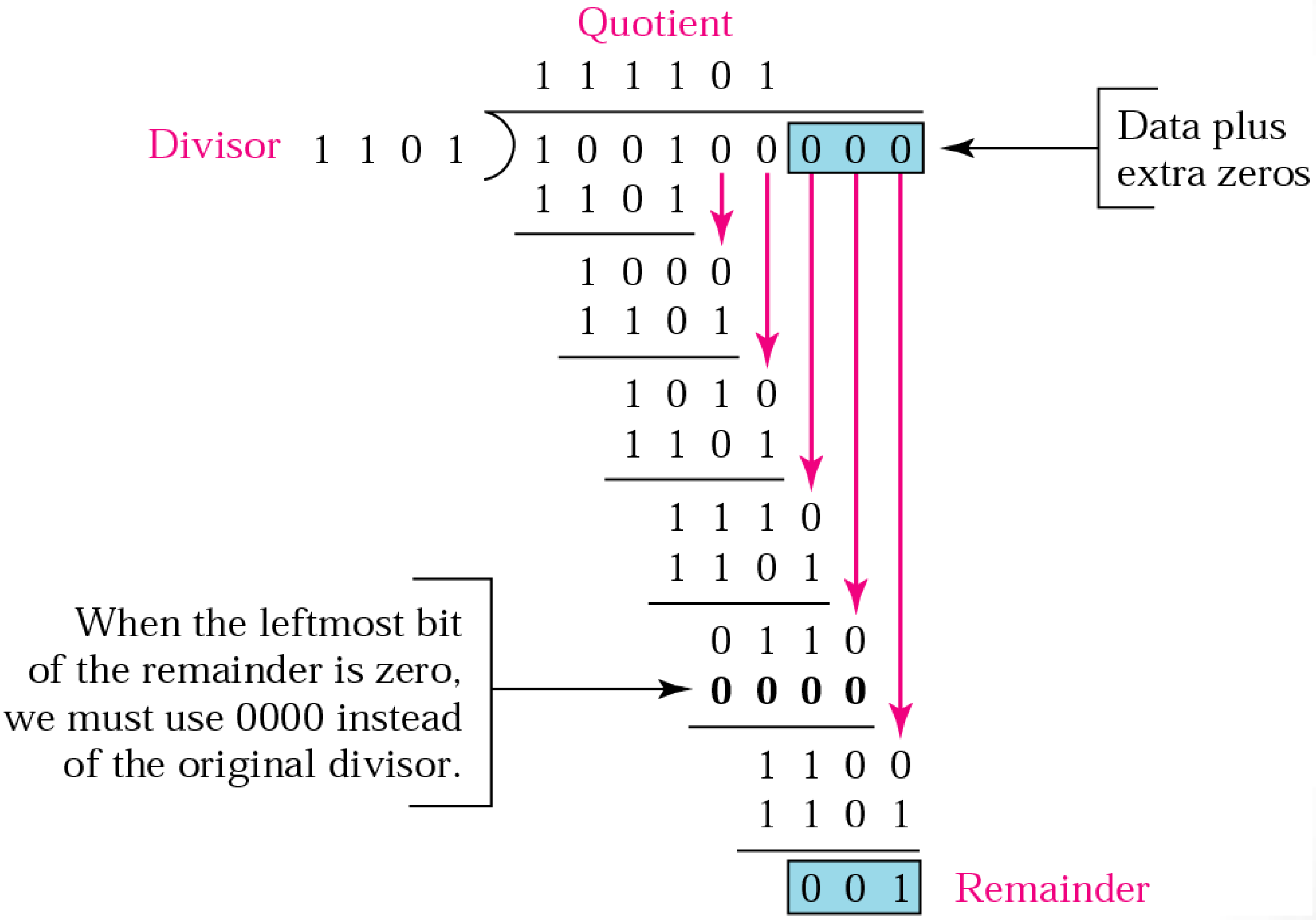
1. A string of n 0s is appended to the data unit. The number n is one less than the number of bits in the predetermined divisor, which is n+1 bits.
2. The newly elongated data unit is divided by the divisor using a process called binary division. The remainder resulting from this division is the CRC.
3. The CRC of n-bits derived in 2nd step replaces the appended 0s at the end of the data unit.
4. The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole string as a unit and divides it by the same divisor.
5. If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes.

Modulo-2 Arithmetic



Adding:	0 + 0 = 0	0 + 1 = 1	1 + 0 = 1	1 + 1 = 0
Subtracting:	0 − 0 = 0	0 − 1 = 1	1 − 0 = 1	1 − 1 = 0

Binary division in a CRC generator



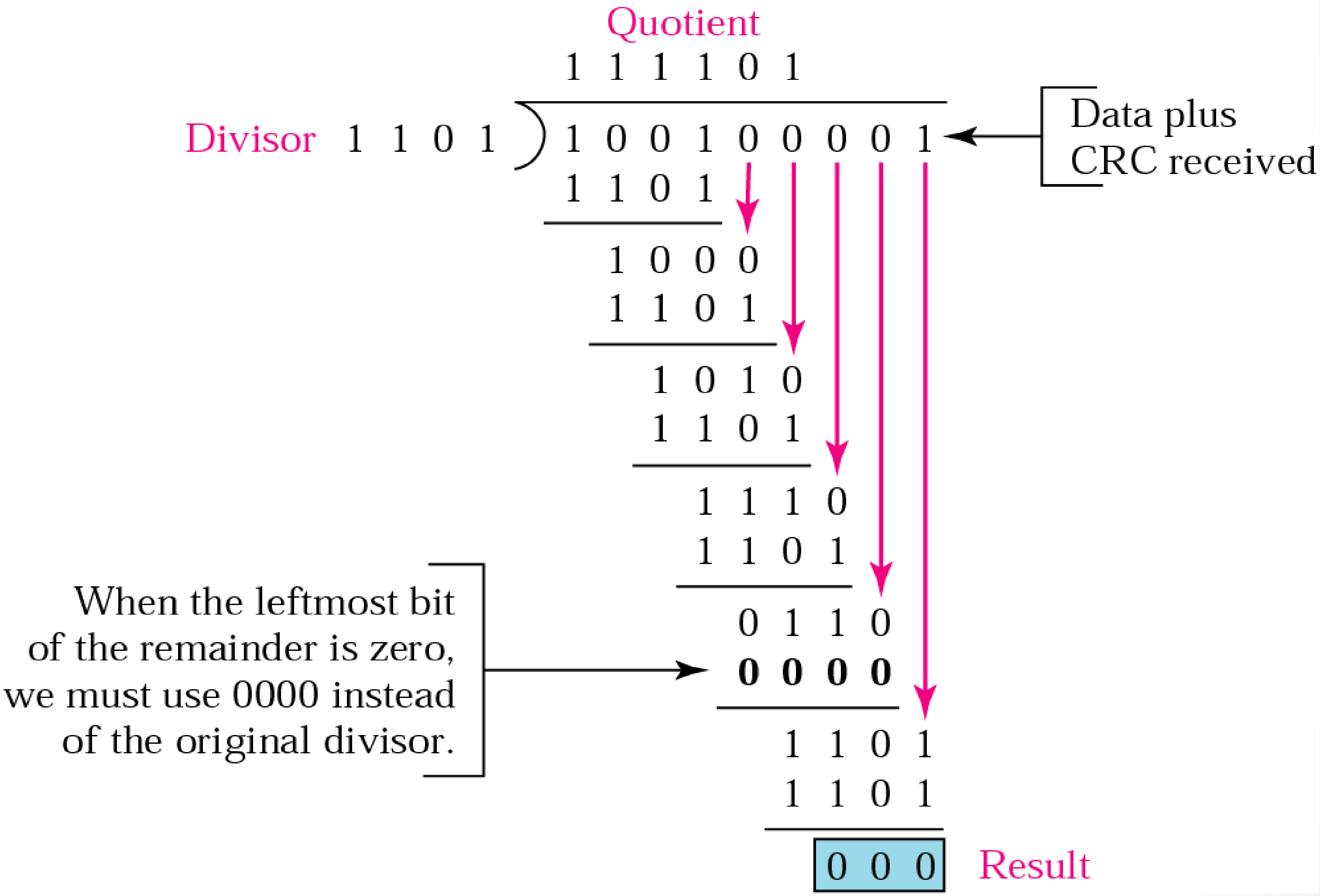
Quotient

```
                     1 1 1 1 0 1
                   _____________________
Divisor  1 1 0 1  ) 1 0 0 1 0 0 | 0 0 0 |
                    1 1 0 1
                    -------
                      1 0 0 0
                      1 1 0 1
                      -------
                        1 0 1 0
                        1 1 0 1
                        -------
                          1 1 1 0
                          1 1 0 1
                          -------
                            0 1 1 0
                            0 0 0 0
                            -------
                              1 1 0 0
                              1 1 0 1
                              -------
                              | 0 0 1 |  Remainder
```

Data plus extra zeros

When the leftmost bit of the remainder is zero, we must use 0000 instead of the original divisor.

Binary division in CRC checker



Quotient

```
             1 1 1 1 0 1
Divisor 1 1 0 1 ) 1 0 0 1 0 0 0 0 1
                  1 1 0 1
                    1 0 0 0
                    1 1 0 1
                      1 0 1 0
                      1 1 0 1
                        1 1 1 0
                        1 1 0 1
                          0 1 1 0
                          0 0 0 0
                            1 1 0 1
                            1 1 0 1
                              0 0 0
```

Result

Data plus CRC received

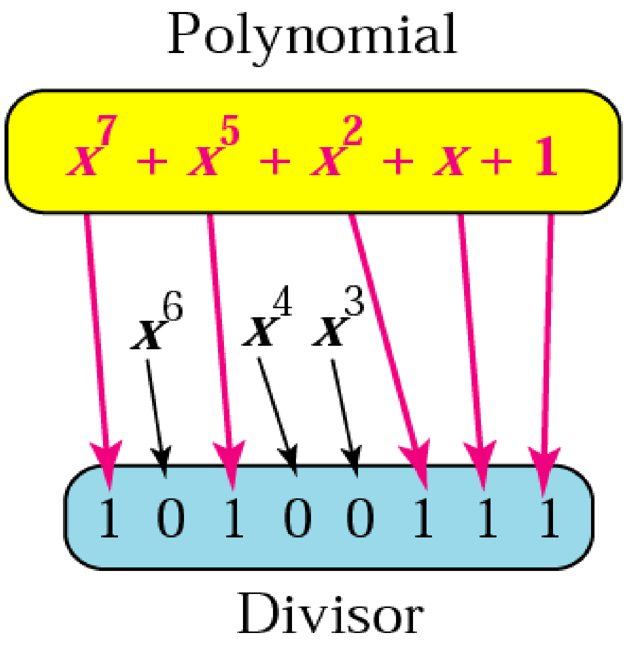
When the leftmost bit of the remainder is zero, we must use 0000 instead of the original divisor.

A polynomial

The CRC generator is most often represented not as a string of 1s and 0s, but as an algebraic polynomial.

$$\boxed{x^7 + x^5 + x^2 + x + 1}$$

A polynomial representing a divisor



Performance

- CRC is a very effective error detection method.

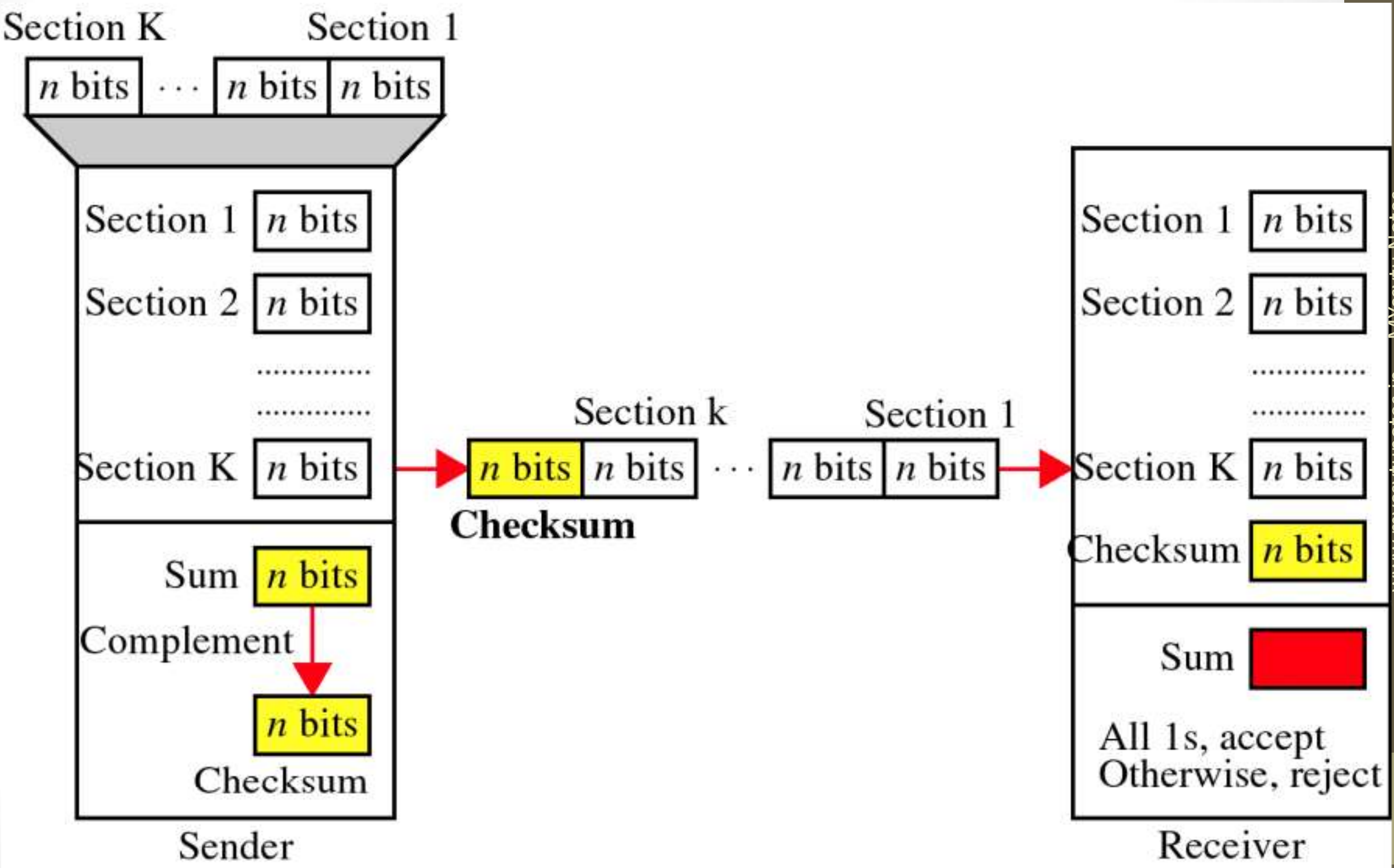
Solve

1. Find out CRC remainder for data unit 1101011011 if divisor is 10011.
2. Given a 10 bit sequence 1010011110 and a divisor of 1011, find the CRC. Check your answer.

Checksum

- The error detection method used by the higher-layer protocols is called **checksum**.

Checksum


Section K
Section 1
n bits
· · ·
n bits
n bits
Section 1
n bits
Section 2
n bits
....
....
Section K
n bits
Sum
n bits
Complement
n bits
Checksum
Sender
Section k
Section 1
n bits
n bits
· · ·
n bits
n bits
Checksum
Section 1
n bits
Section 2
n bits
....
....
Section K
n bits
Checksum
n bits
Sum
All 1s, accept
Otherwise, reject
Receiver

Note:

The sender follows these steps:

- *The unit is divided into k sections, each of n bits.*
- *All sections are added using one's complement to get the sum.*
- *The sum is complemented and becomes the checksum.*
- *The checksum is sent with the data.*

Example 7

Suppose the following block of 16 bits is to be sent using a checksum of 8 bits.

10101001 00111001

The numbers are added using one’s complement

```
                10101001
                00111001
                ------------
Sum             11100010
Checksum        00011101
```

The pattern sent is 10101001 00111001 00011101

Note:

The receiver follows these steps:

- The unit is divided into k sections, each of n bits.
- All sections are added using one’s complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted: otherwise, rejected.

Example 8

Now suppose the receiver receives the pattern sent in Example 7 and there is no error.

10101001 00111001 00011101

When the receiver adds the three sections, it will get all 1s, which, after complementing, is all 0s and shows that there is no error.

	10101001
	00111001
	00011101
Sum	11111111
Complement	00000000 means that the pattern is OK.

Correction

Error correction can be handled in two ways.

- When an error is discovered, the sender retransmit the entire data unit.
- A receiver can use an error-correcting code, which automatically corrects certain errors.

Hamming Code

Used for ……

- Error Detection
- Error Correction

Redundancy Bits

- We can calculate the number of redundancy bit (r) required to correct a given number of data bits(m) by the relationship

  $2^r >= m + r + 1$

Data and redundancy bits

Number of data bits m	Number of redundancy bits r	Total bits m + r
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Calculating the Hamming Code

1. Mark all bit positions that are powers of two as parity bits. (positions 1, 2, 4, 8, 16, 32, 64, etc.)

2. All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)

3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.

Position 1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc. (1,3,5,7,9,11,13,..)

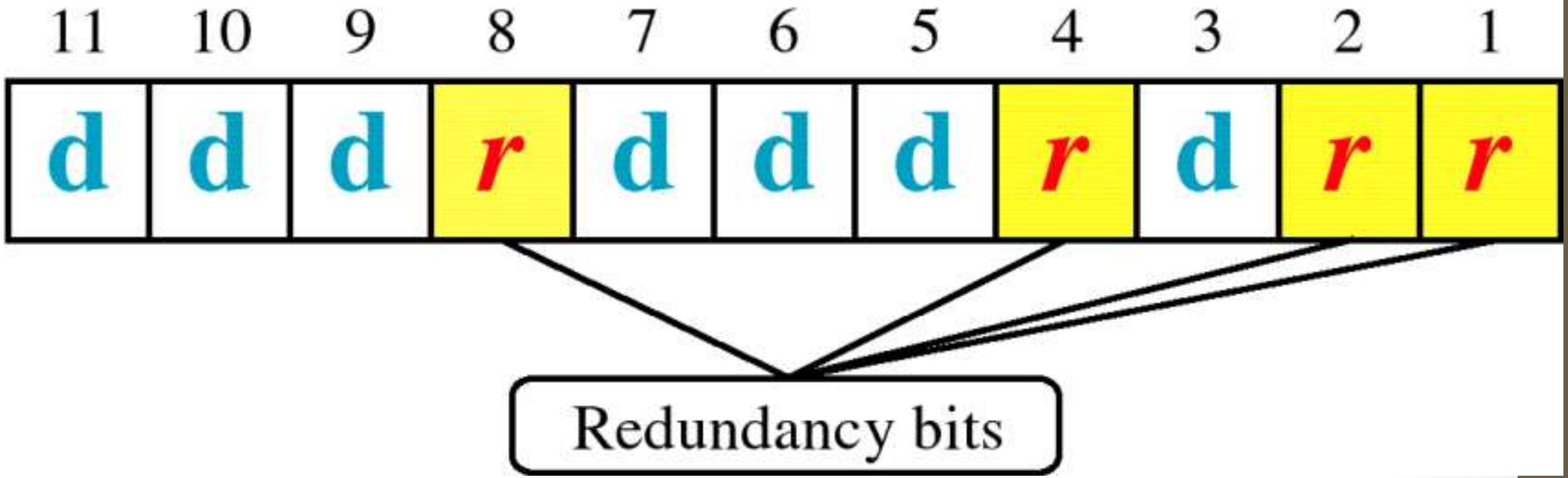
Position 2: check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2,3,6,7,10,11)

Position 4: check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4,5,6,7,12,13,14,15)

Position 8: check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8-15,24-31)

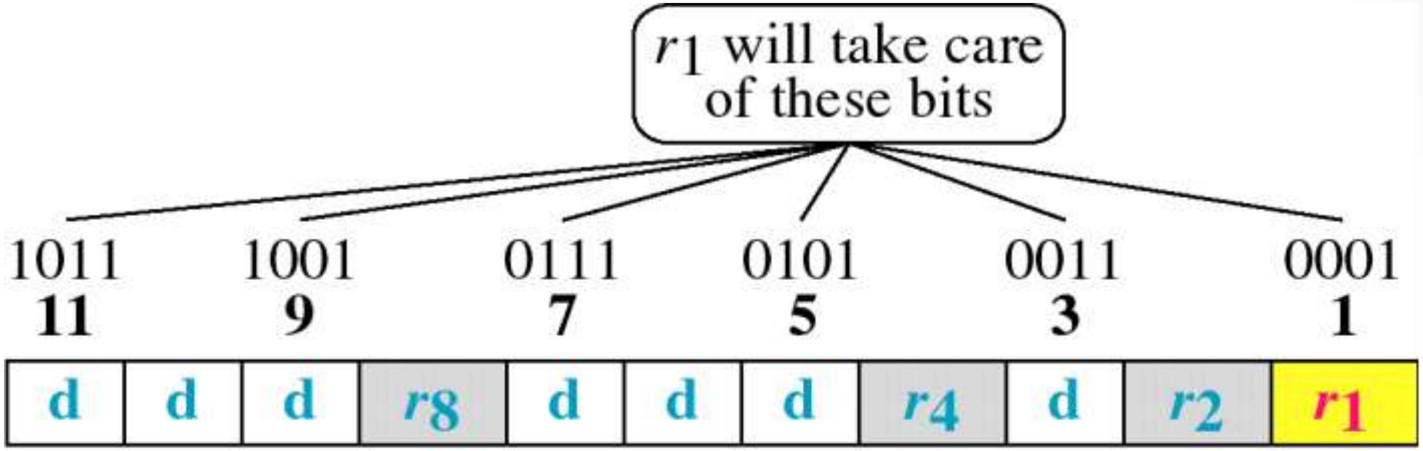
4.Set a parity bit to 1 if the total number of ones in the positions it checks is odd. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Hamming Code

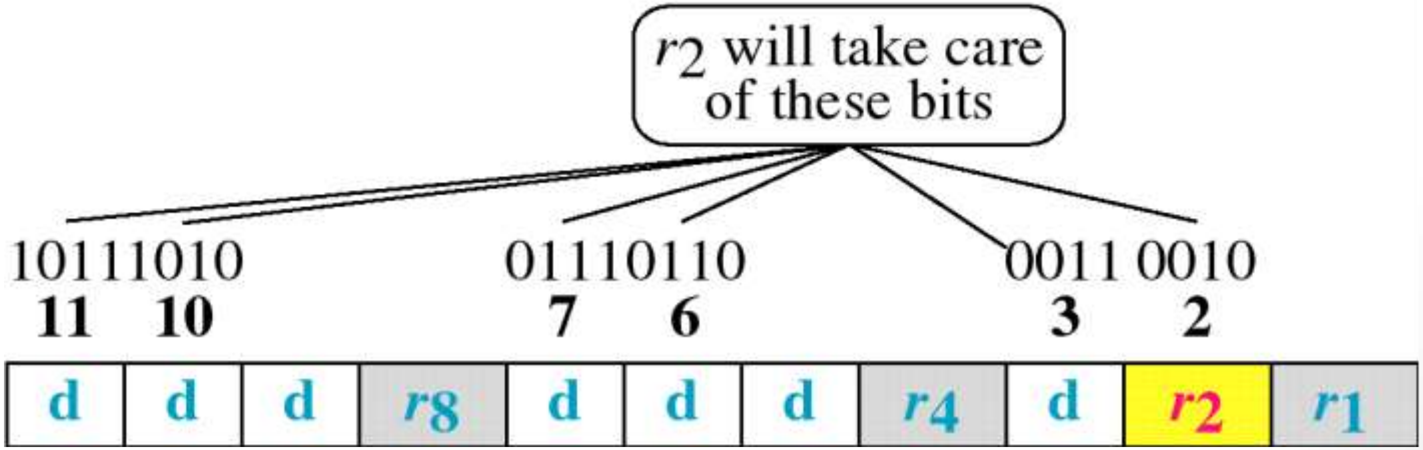


11	10	9	8	7	6	5	4	3	2	1
d	d	d	*r*	d	d	d	*r*	d	*r*	*r*

Hamming Code

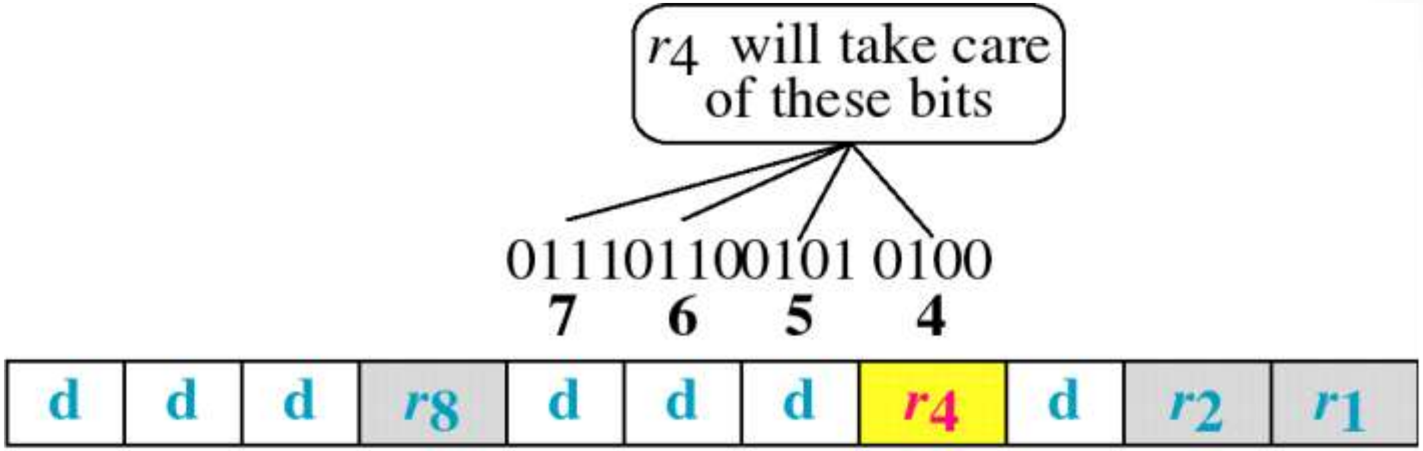


r_1 will take care of these bits

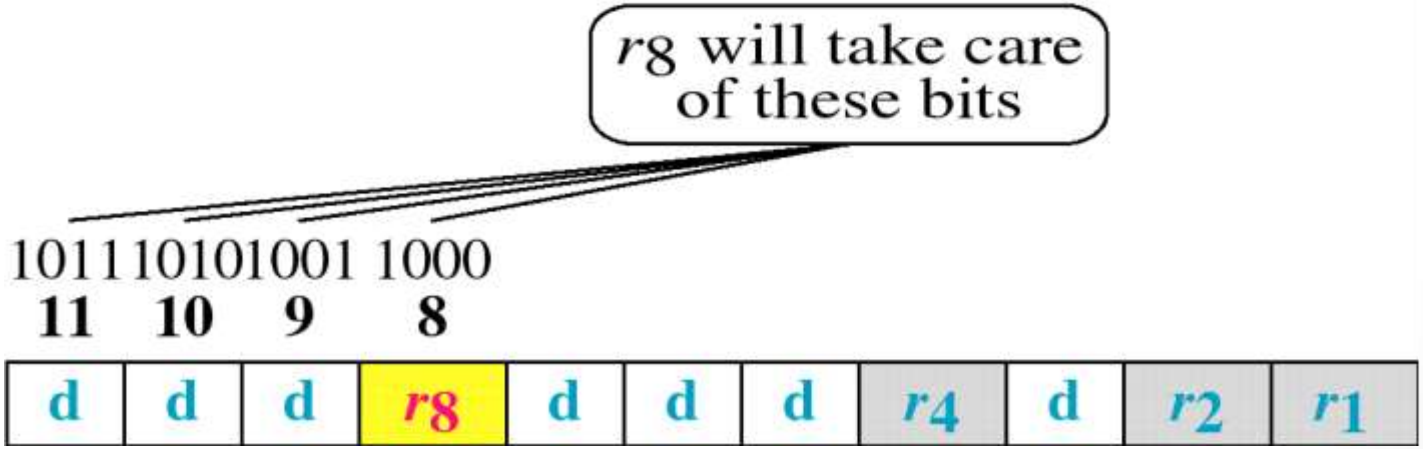


r_2 will take care of these bits

Hamming Code

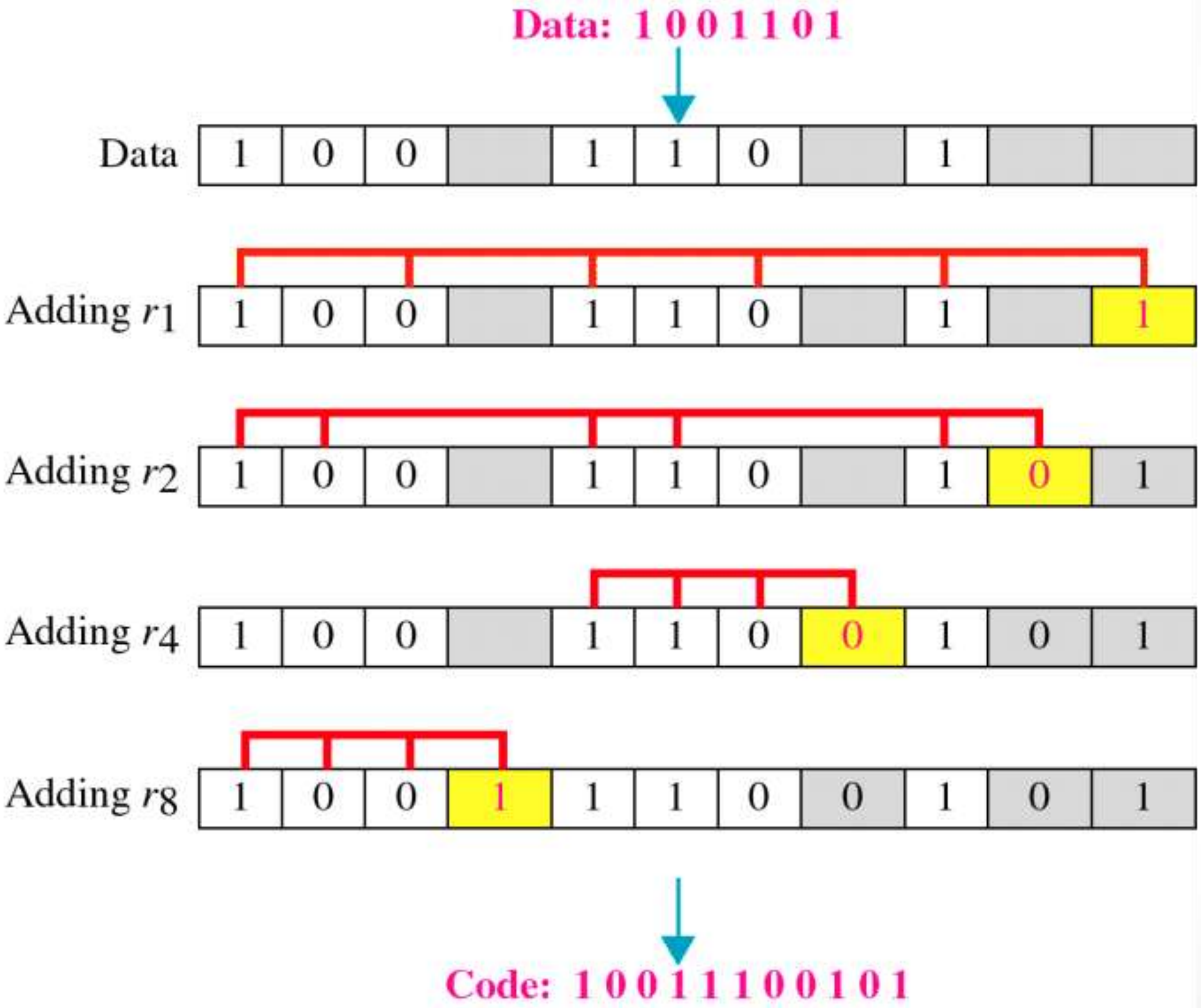


r4 will take care of these bits



r8 will take care of these bits

Example of Hamming Code

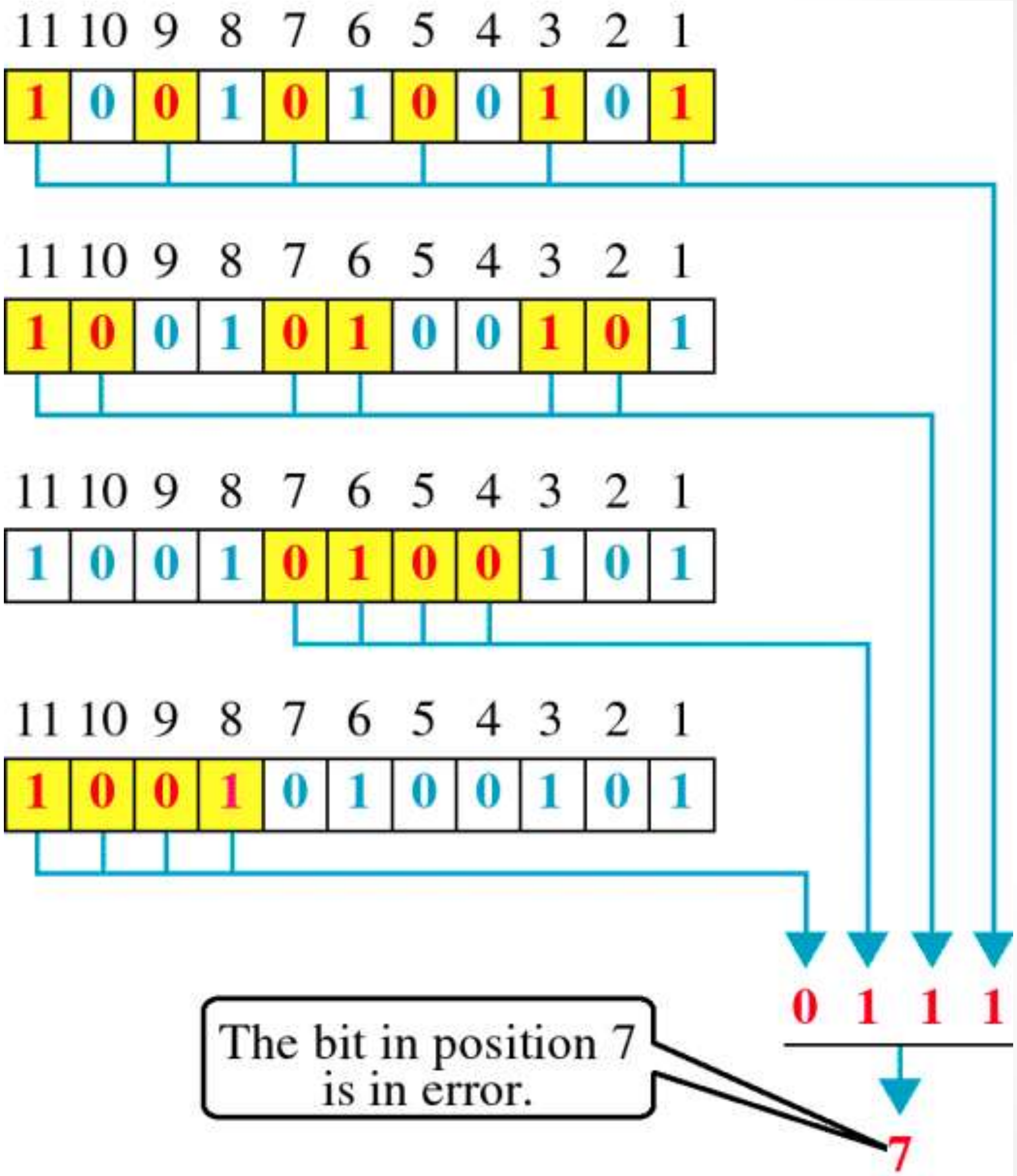


Data: 1 0 0 1 1 0 1

Data	1	0	0		1	1	0		1		
Adding r_1	1	0	0		1	1	0		1		1
Adding r_2	1	0	0		1	1	0		1	0	1
Adding r_4	1	0	0		1	1	0	0	1	0	1
Adding r_8	1	0	0	1	1	1	0	0	1	0	1

Code: 1 0 0 1 1 1 0 0 1 0 1

Error Detection

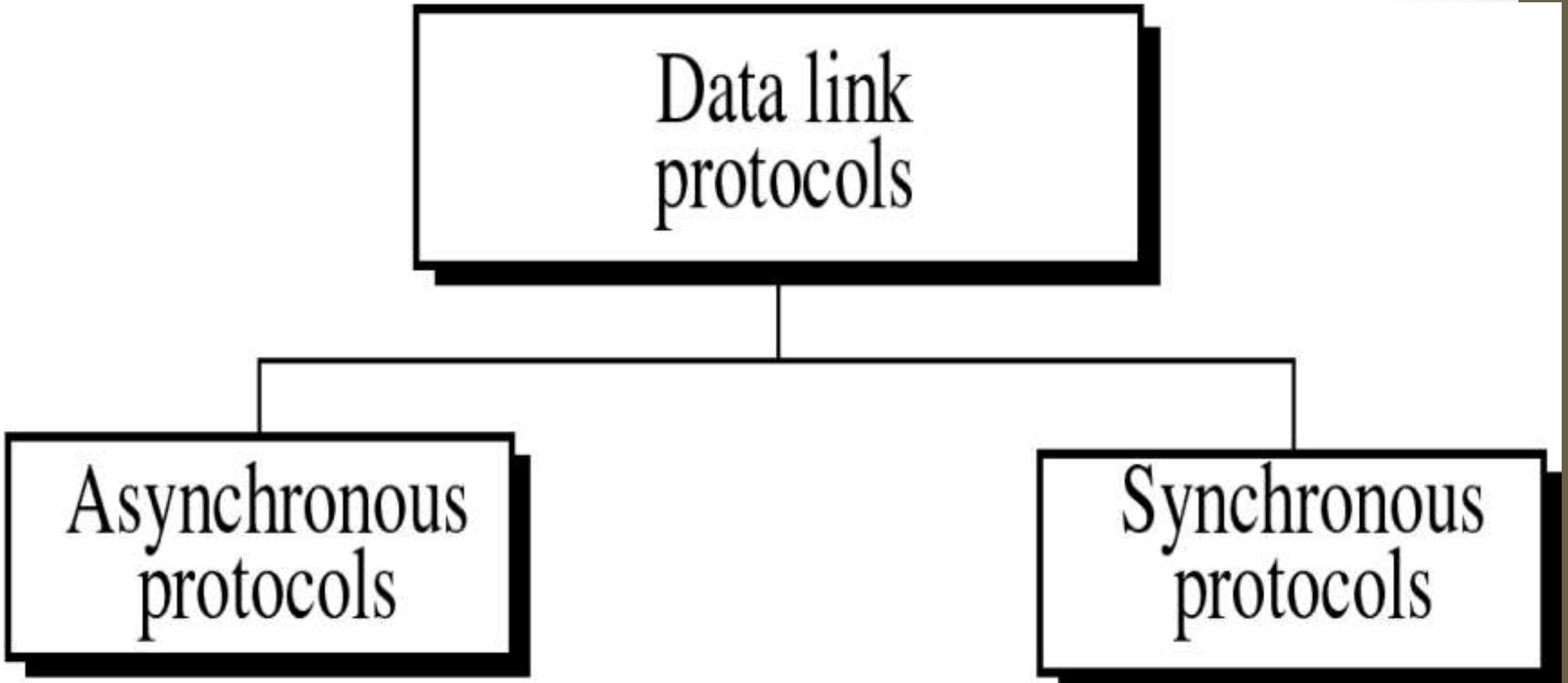


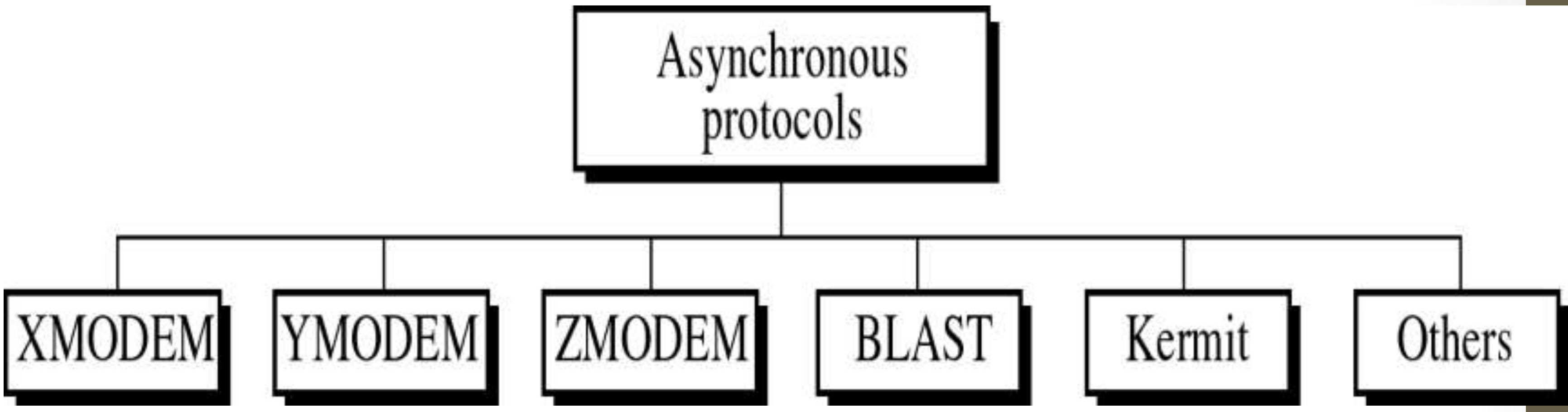
The bit in position 7 is in error.

Questions

1. Also generate complete Hamming code for a message M=1011101.
2. Consider 10 bit binary code 1100111011 is to be transmitted over the network and during transmission 6th bit is inverted, how this code will detect and correct the error.

Data Link Protocol


Data link protocols
Asynchronous protocols
Synchronous protocols



Asynchronous protocols

XMODEM

YMODEM

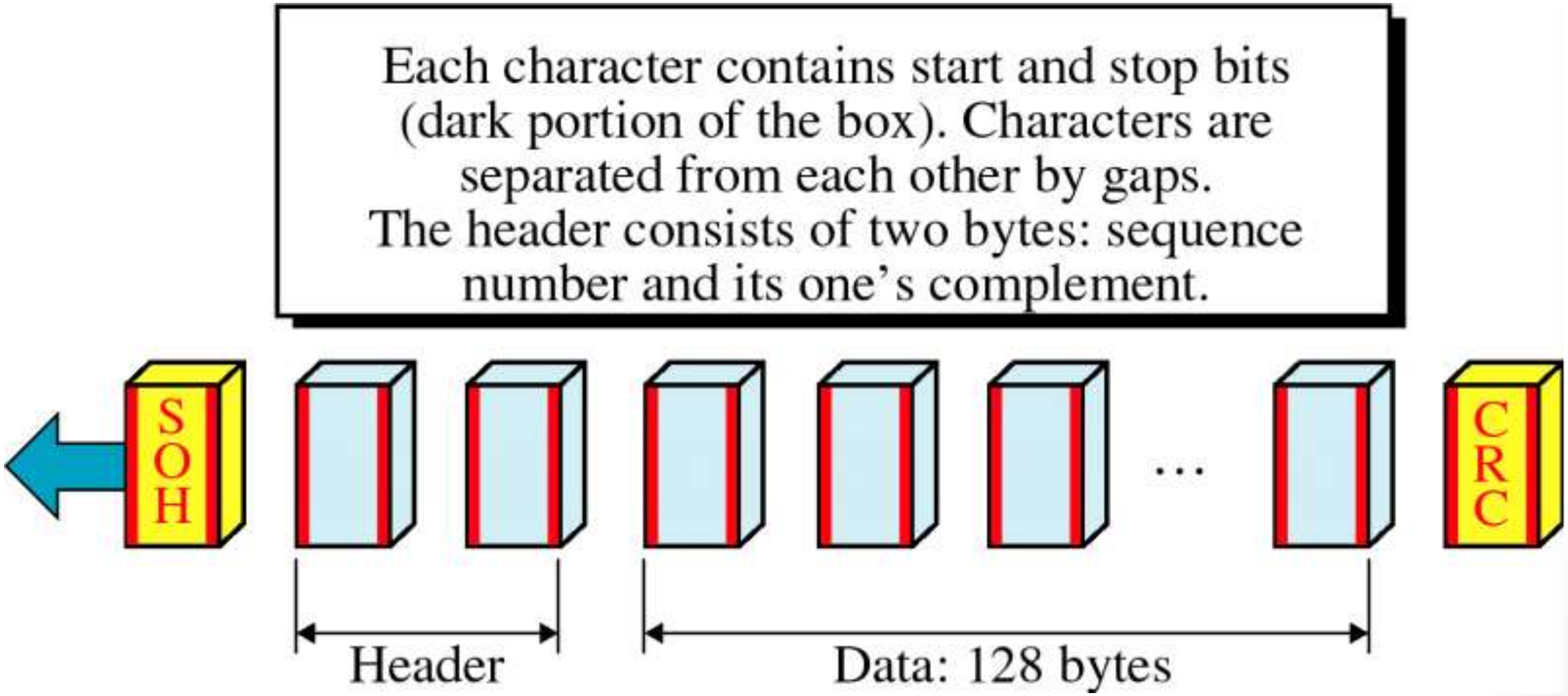
ZMODEM

BLAST

Kermit

Others

XMODEM



Each character contains start and stop bits (dark portion of the box). Characters are separated from each other by gaps.
The header consists of two bytes: sequence number and its one's complement.

XMODEM

- It is a half-duplex, stop-and-wait ARQ protocol.
- The first field is 1-byte start of header(SOH).
- The second field is a two-byte header. The first header byte, the sequence number, carries the frame number. The second header byte is used to check the validity of the sequence number.
- The fixed data field holds 128 bytes of data.
- The last field, CRC, checks for errors, in the data field only.

Working

- Transmission begins with the sending of a NAK frame from the receiver to sender.
- Each time the sender sends a frame, it must wait for an acknowledgement(ACK).
- If NAK is received, the previously sent frame is sent again.
- A frame can also be resent if a response is not received by the sender after a specified amount of time.
- The sender can receive a cancel signal (CAN), which aborts the transmission.

YMODEM

Similar to XMODEM, but major differences are:

- Data unit 1024 bytes.
- Two CAN are sent to abort a transmission.
- ITU-T CRC-16 is used for error checking.

ZMODEM

- Newer protocol combining features of both XMODEM and YMODEM.

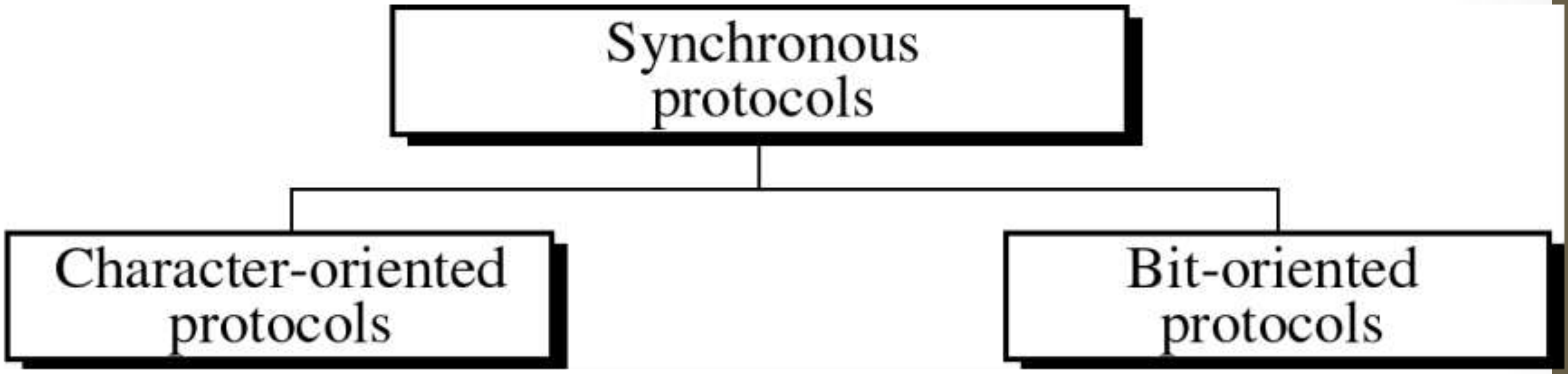
BLAST

- BLOCKED asynchronous transmission (BLAST) is more powerful than XMODEM.
- It is full-duplex with sliding window flow control.

Kermit

- Kermit is similar to XMODEM. Most widely used.

Synchronous Protocol



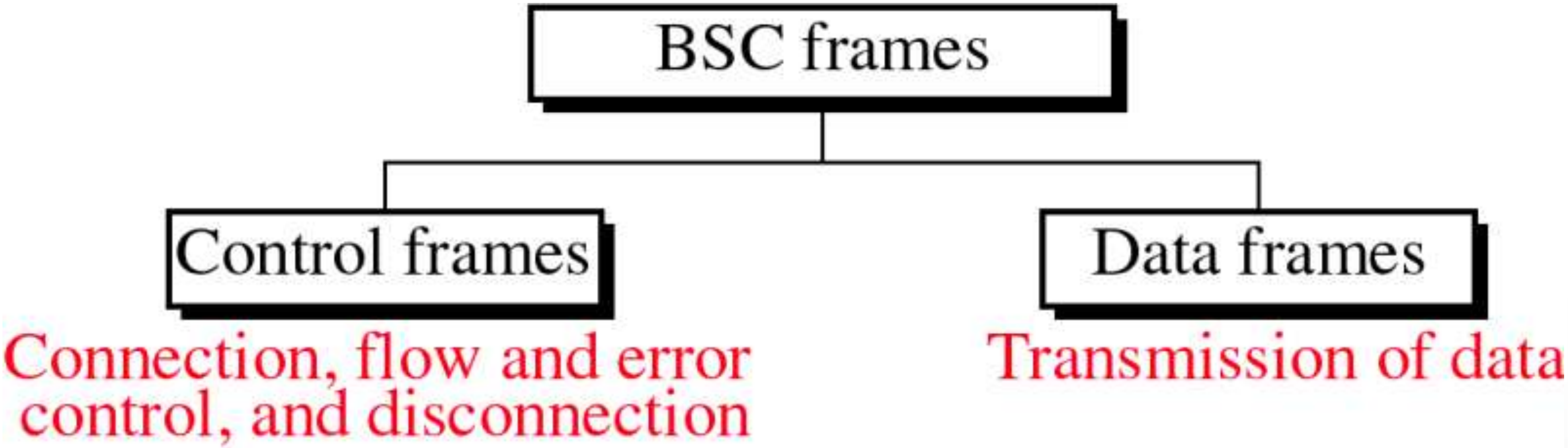
Synchronous Protocol

- **Character-oriented Protocols** also called **byte oriented protocols** interpret a transmission frame or packet as a series of characters, each usually composed of one byte.

- **Bit-oriented protocols** interpret a transmission frame or packet as a series of individual bits.

Character Oriented Protocol

A popular character-oriented data link protocol is binary synchronous communication(BSC). Developed by IBM. It uses half-duplex transmission with stop-and-wait ARQ.



BSC frames

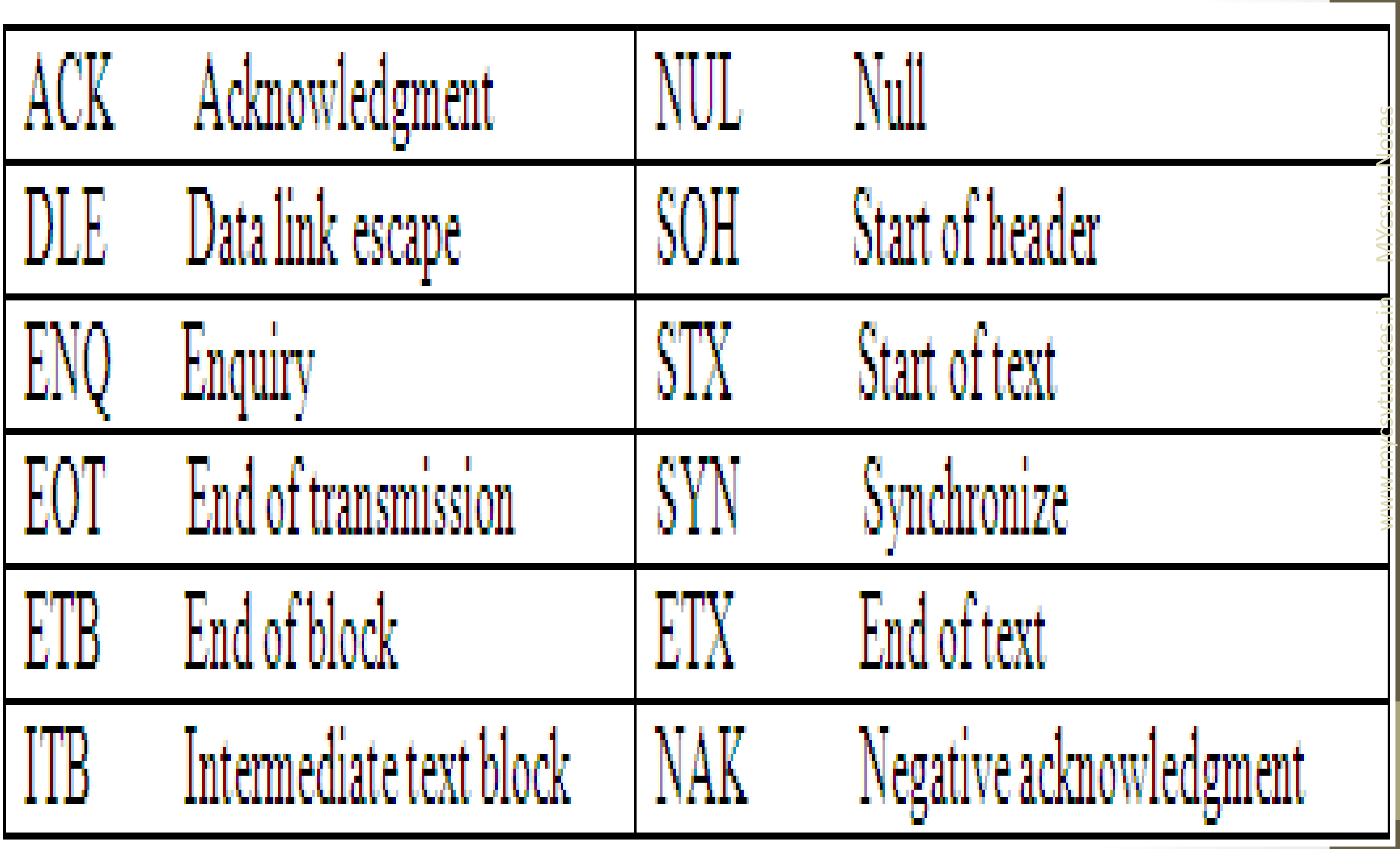
Control frames

Data frames

Connection, flow and error control, and disconnection

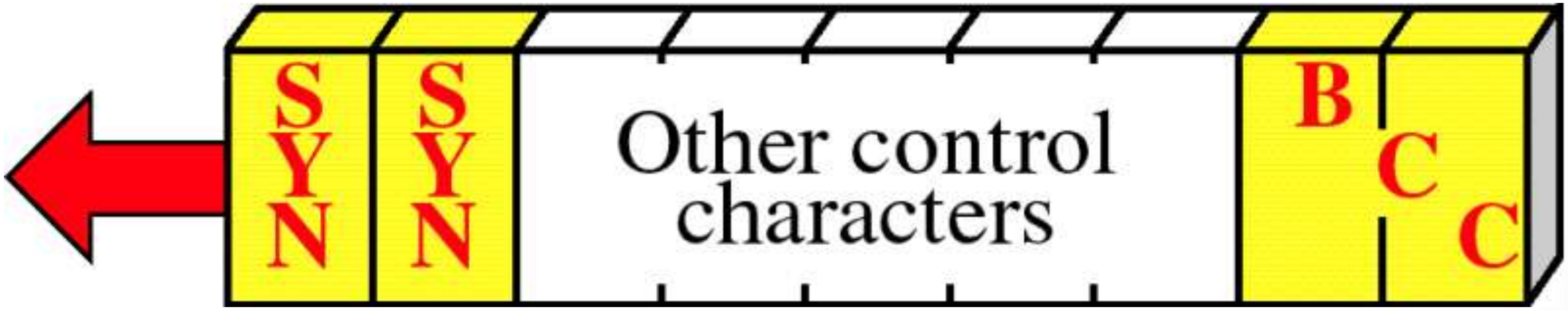
Transmission of data

Control characters for BSC



ACK	Acknowledgment	NUL	Null
DLE	Data link escape	SOH	Start of header
ENQ	Enquiry	STX	Start of text
EOT	End of transmission	SYN	Synchronize
ETB	End of block	ETX	End of text
ITB	Intermediate text block	NAK	Negative acknowledgment

Control Frame



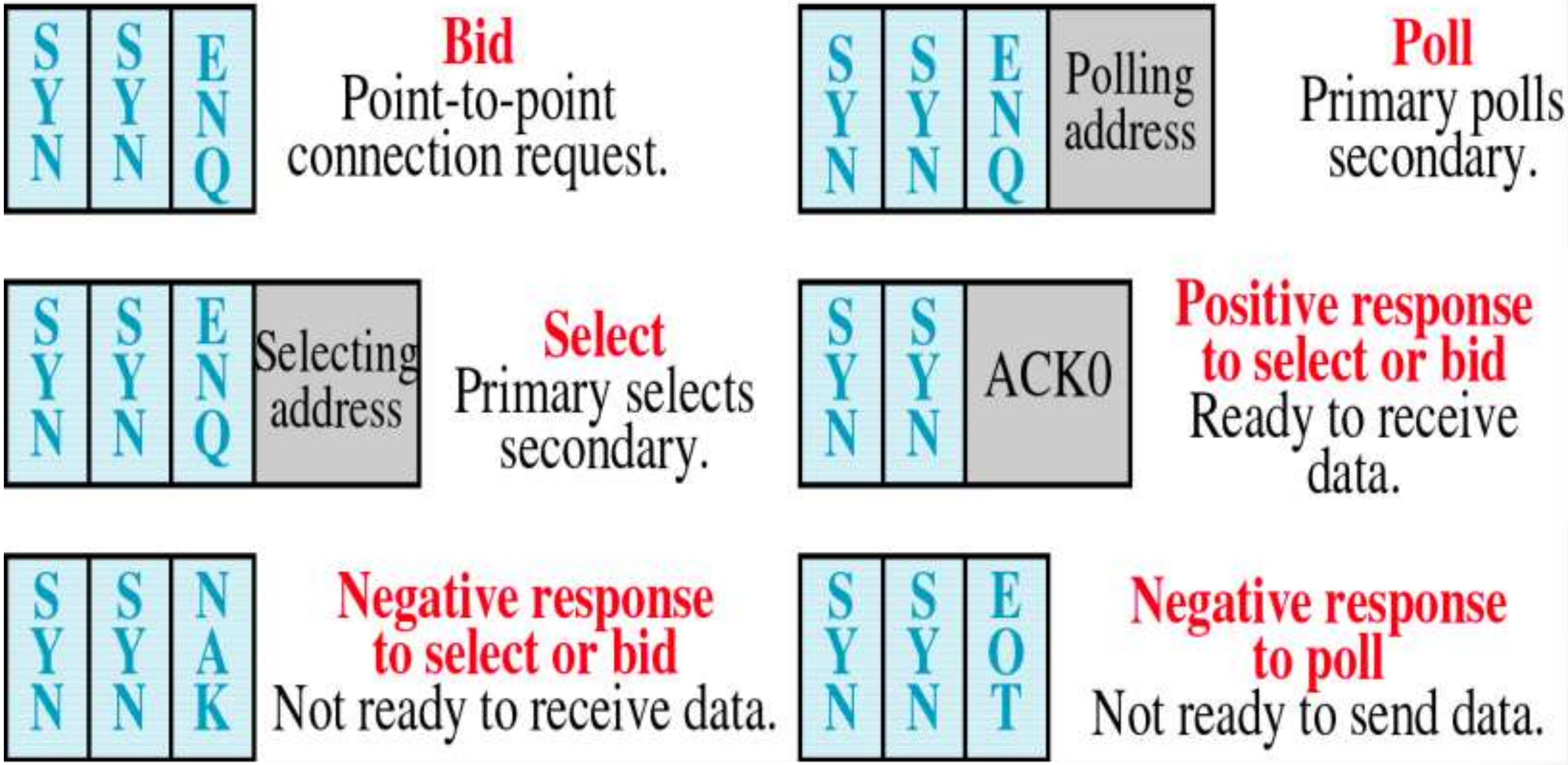
Control Frames

- A control frame is used by one device to send commands or receive information from another device.

Control frames

- Control frames serve three purposes
  - Connection establishing
  - Maintaining flow and error control during data transmission
  - Terminating connections

Connection establishment



Bid
Point-to-point connection request.

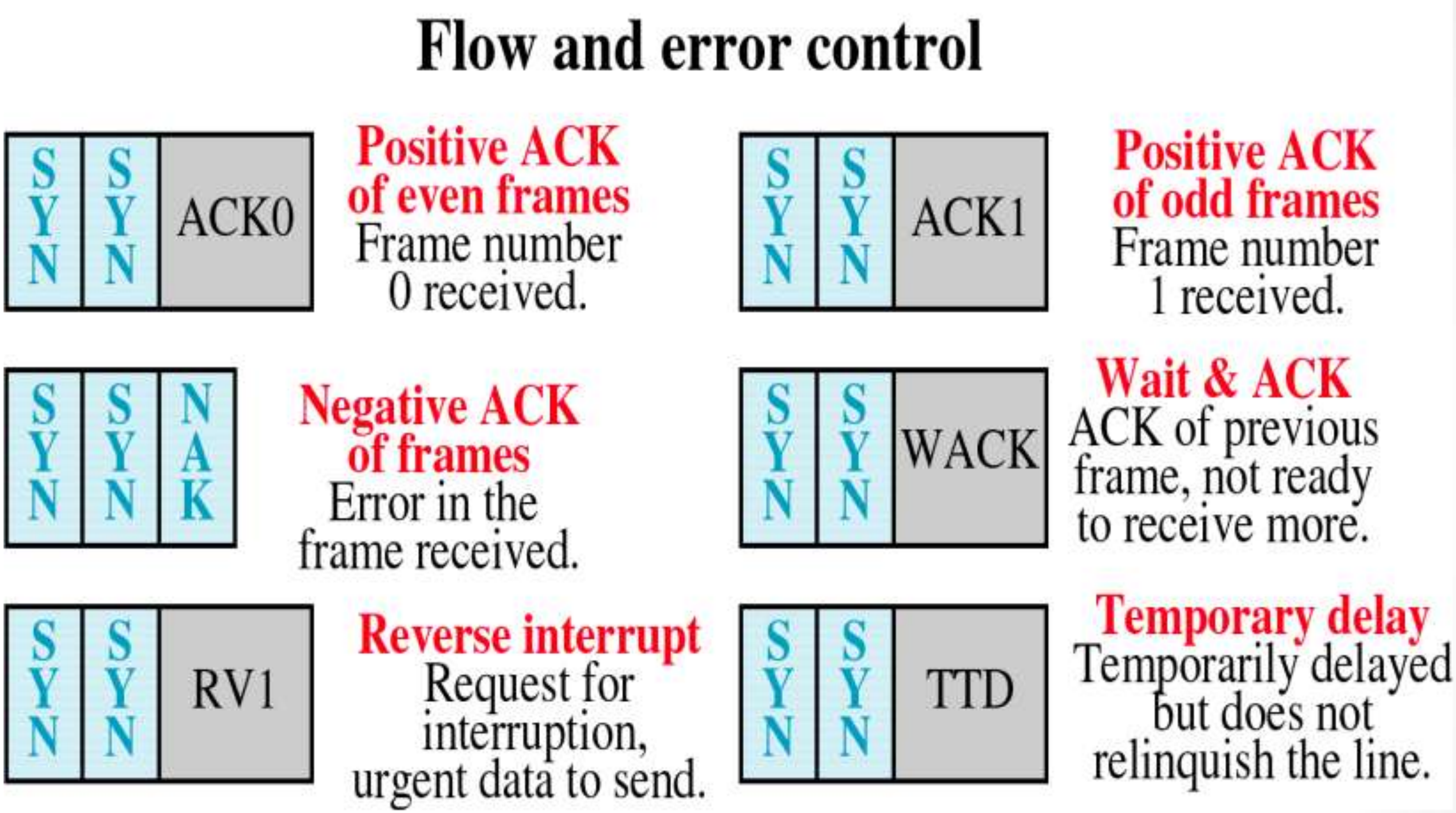
Poll
Primary polls secondary.

Select
Primary selects secondary.

Positive response to select or bid
Ready to receive data.

Negative response to select or bid
Not ready to receive data.

Negative response to poll
Not ready to send data.



Flow and error control

Positive ACK of even frames
Frame number 0 received.

Positive ACK of odd frames
Frame number 1 received.

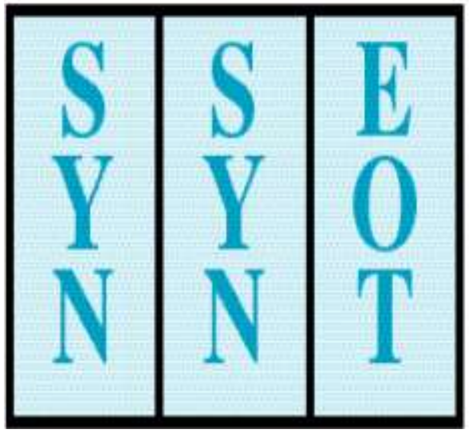
Negative ACK of frames
Error in the frame received.

Wait & ACK
ACK of previous frame, not ready to receive more.

Reverse interrupt
Request for interruption, urgent data to send.

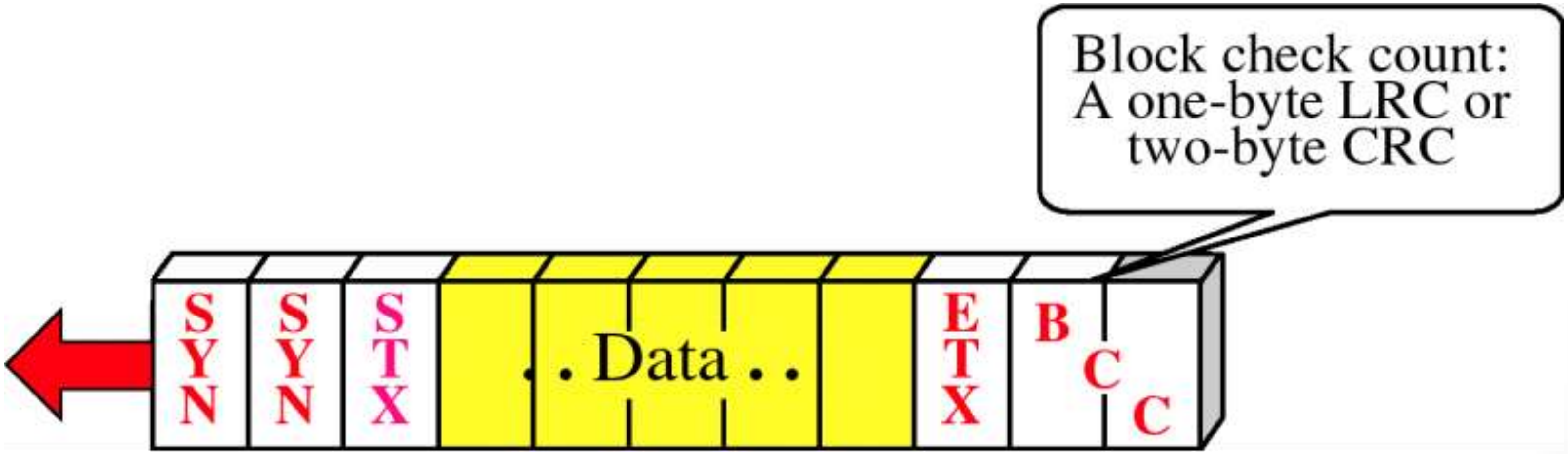
Temporary delay
Temporarily delayed but does not relinquish the line.

Connection termination



End of transmission
Station finished sending data.

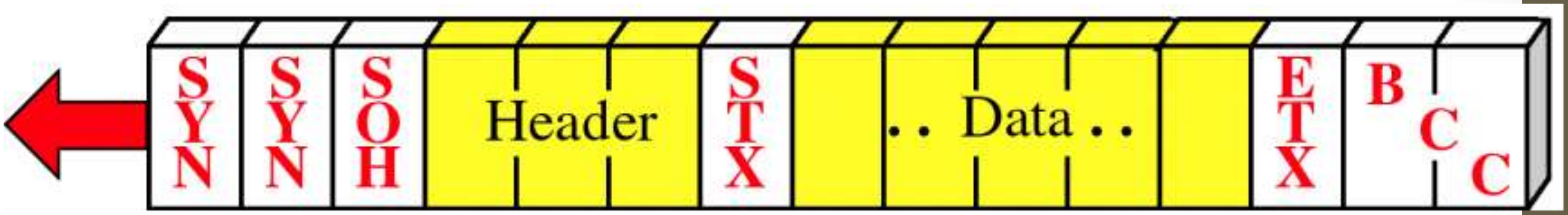
Data Frame


Block check count: A one-byte LRC or two-byte CRC
S Y N
S Y N
S T X
. . Data . .
E T X
B C C

Data Frame

- The arrow shows the direction of transmission.
- The frame begins with two or more synchronous (SYN) characters.
- These characters alert the receiver to the arrival of a new frame.
- STX (start of text) signals to the receiver that the control information is ending and next byte will be data.
- ETX (end of text)
- Finally, one or two characters called the block check count(BCC) are included for error detection.
- A BCC field can be a one-character LRC or a two-character CRC.

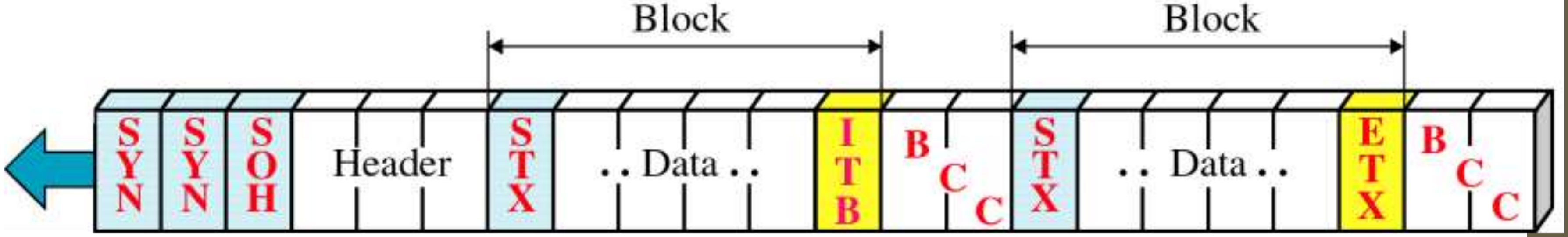
A Frame With Header



Header fields

- Header is used to include the address of the receiving device, the address of the sending device, and the identifying number of frame.
- Header begins with a SOH (start of header).
- Everything received after the SOH field but before the STX character is header information.

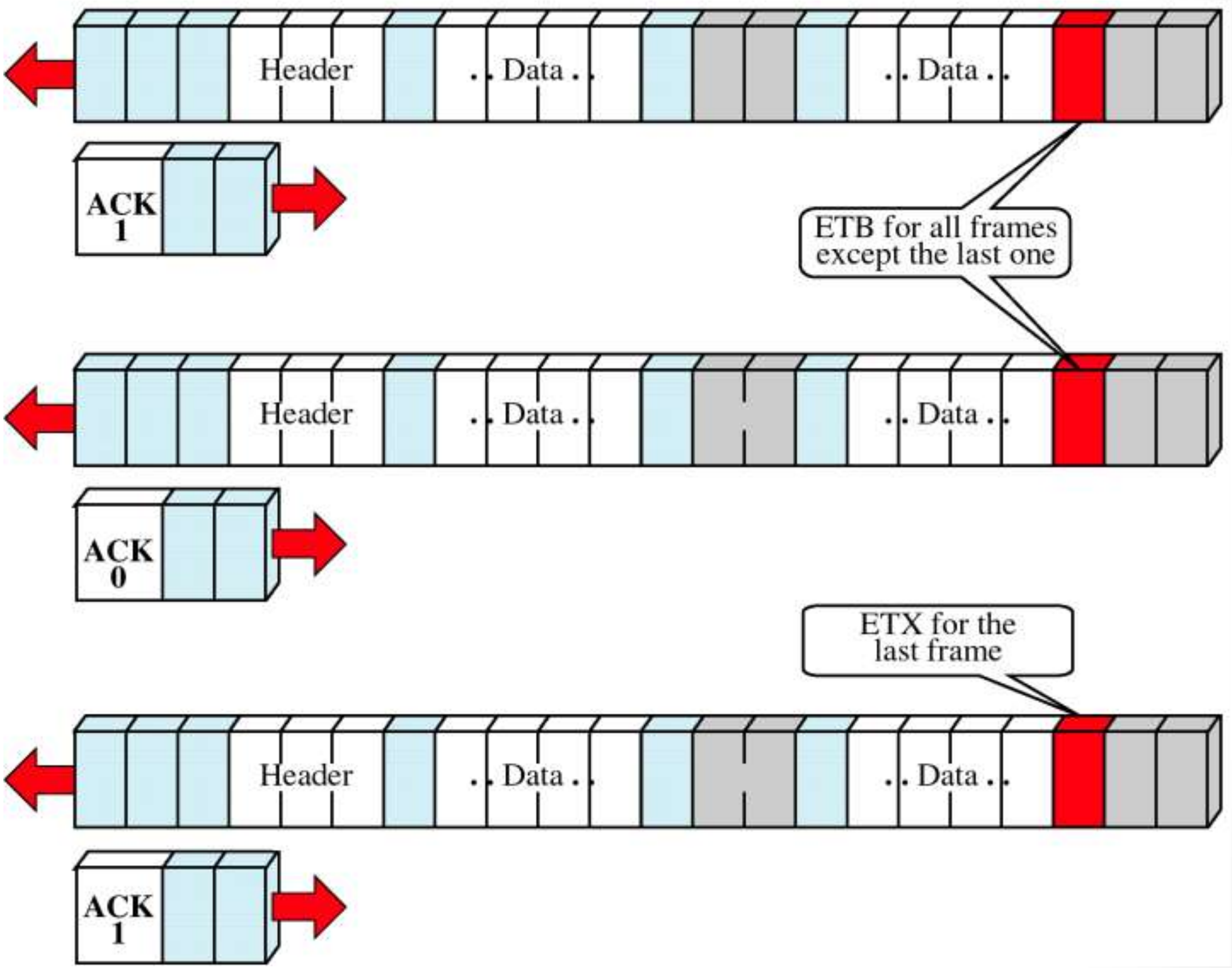
Multiblock Frame



Multiblock Frame

- The probability of an error in the block of text increases with the length of frame.
- For this reason, text in a message is often divided between several blocks.
- Each block, except the last one, starts with an STX character and ends with an intermediate text block (ITB).
- The last block starts with an STX but ends with an ETX.
- Immediately after each ITB or ETX is a BCC field.

Multiframe Transmission



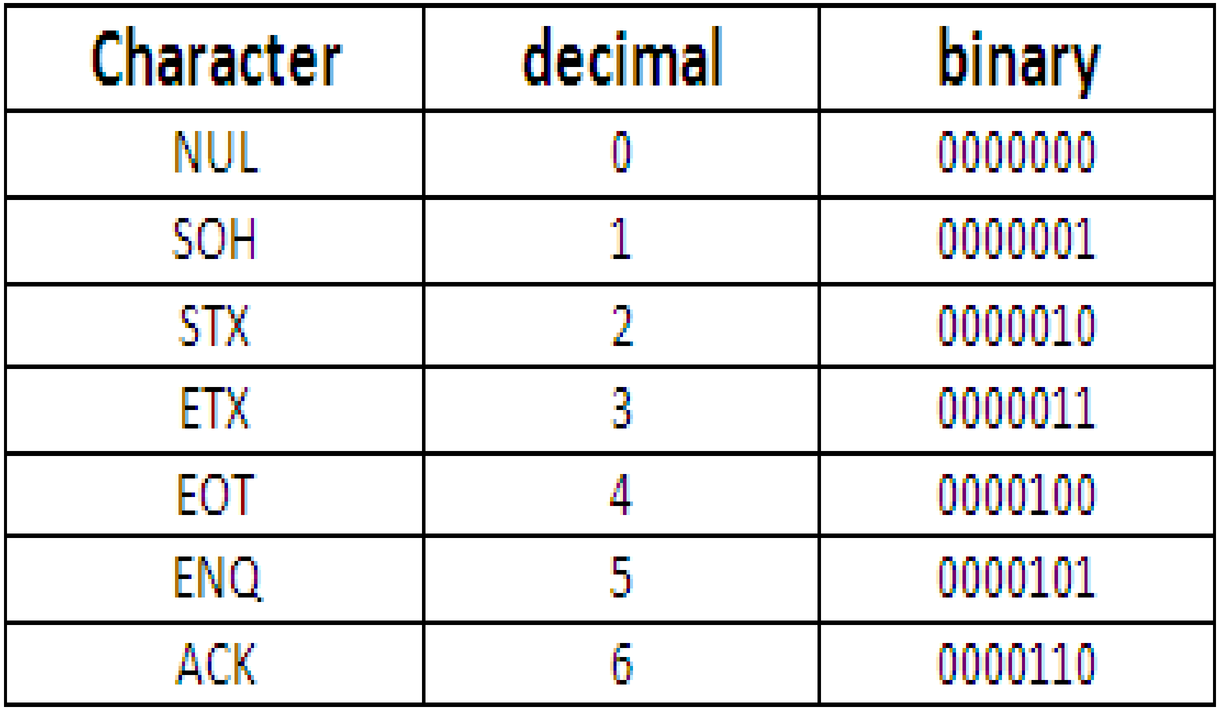
Multiframe Transmission

- Some message, may be too long to fit into the format of a single frame.
- In such cases, the sender can split the message not only among blocks but among frames.
- To let the receiver know that the end of the frame is not the end of the transmission, ETX character in all frames is replaced by ETB except last one.

Data transparency

- Confusion between control information and data is called a lack of **data transparency**.
- **Data transparency** in data communication means we should be able to send any combination of bits as data.
- Data transparency in character-oriented protocol is achieved by a process called **byte stuffing.**

ASCII table

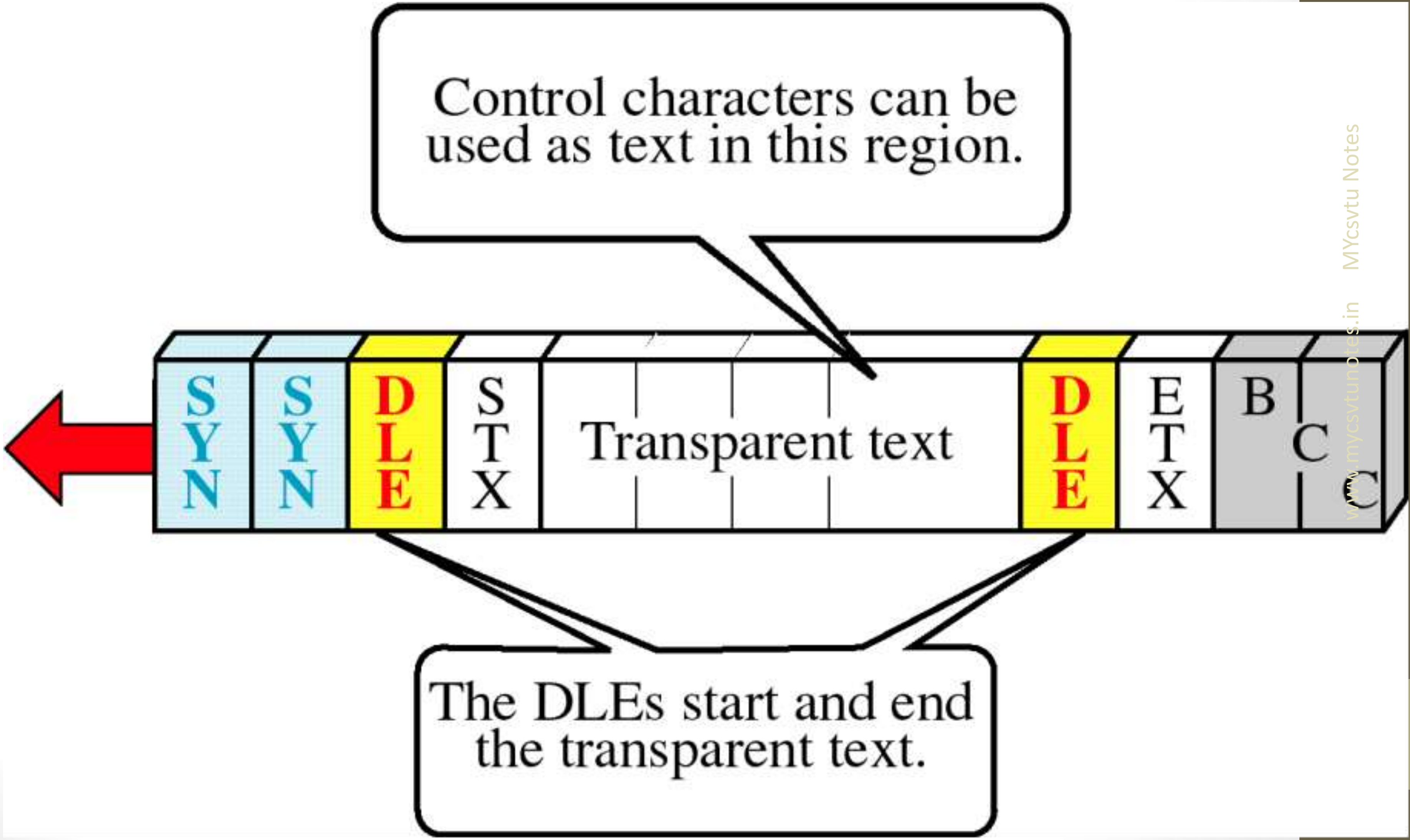


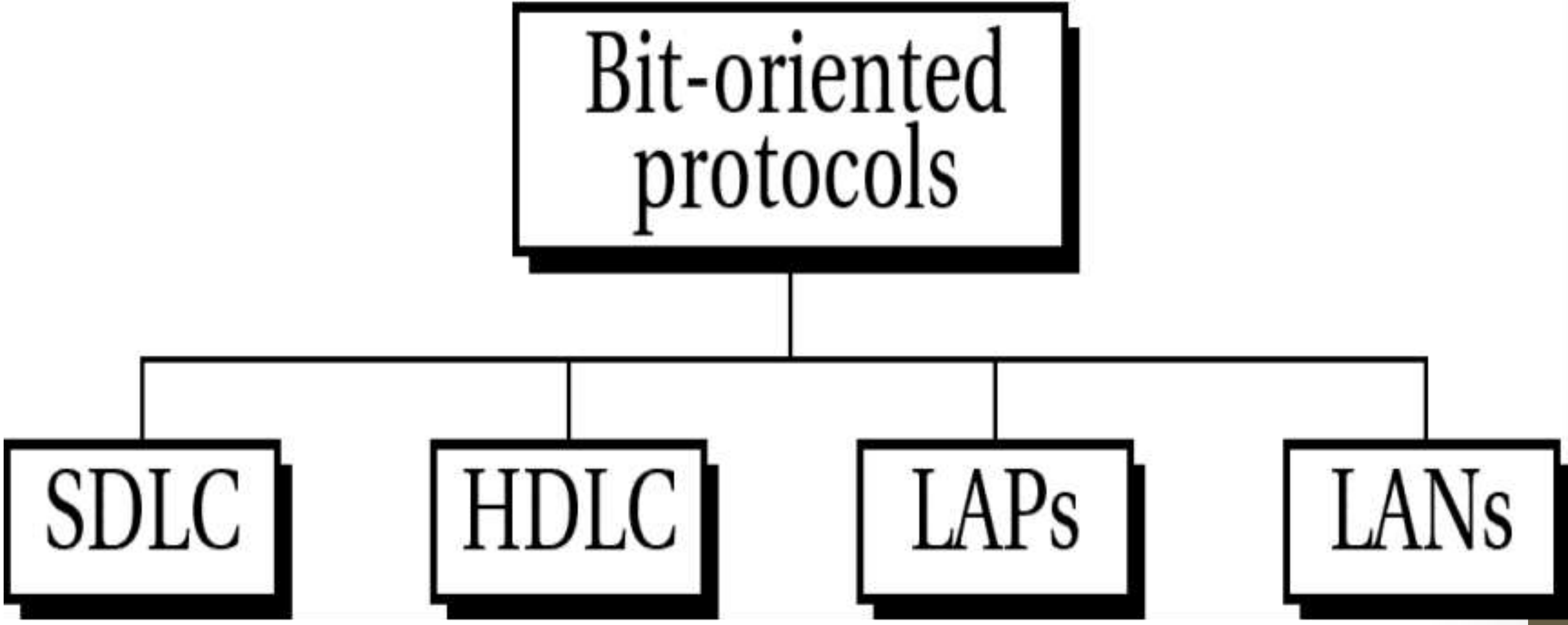
Character	decimal	binary
NUL	0	0000000
SOH	1	0000001
STX	2	0000010
ETX	3	0000011
EOT	4	0000100
ENQ	5	0000101
ACK	6	0000110

Byte Stuffing

- It involves two activities:
  1. defining the transparent text region with the data link escape (DLE) characters
     - The first DLE tells the receiver that the text may contain control characters and to ignore them.
     - The last DLE tells the receiver that the transparent region has ended.
  2. Preceding any DLE character within the transparent region by an extra DLE character.

Byte Stuffing


Control characters can be used as text in this region.
S Y N
S Y N
D L E
S T X
Transparent text
D L E
E T X
B C C
The DLEs start and end the transparent text.



Bit-oriented protocols

SDLC

HDLC

LAPs

LANs

Bit-oriented protocols

- Synchronous data link control (SDLC)
- High-level data link control (HDLC)
- Link access procedure (LAP)
- Local area network (LAN)

HDLC

- **High-level Data Link Control (HDLC) is a bit-oriented protocol for communication** over point-to-point and multipoint links.
- It operates in half duplex and full duplex mode.
- It implements the ARQ mechanisms.

Station Types

- Primary: it sends commands
- Secondary: it sends response
- Combined : it sends commands and responses

(behave either as a primary or as a secondary depending on the nature and direction of the transmission)

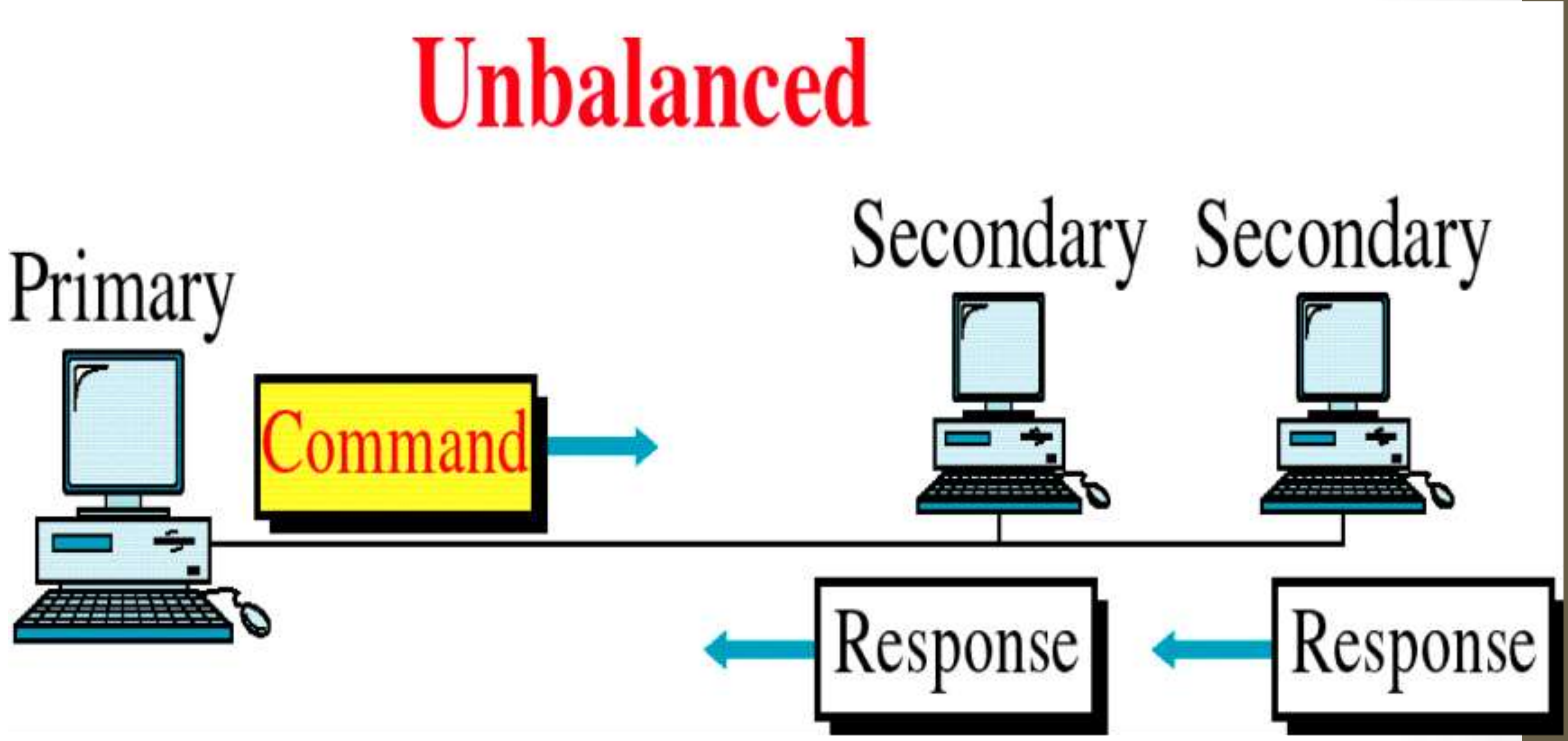
Configurations

The word configuration refers to the relationship of hardware devices on link.

- Unbalanced(Master/Slave)
- Symmetrical
- Balanced

Unbalanced

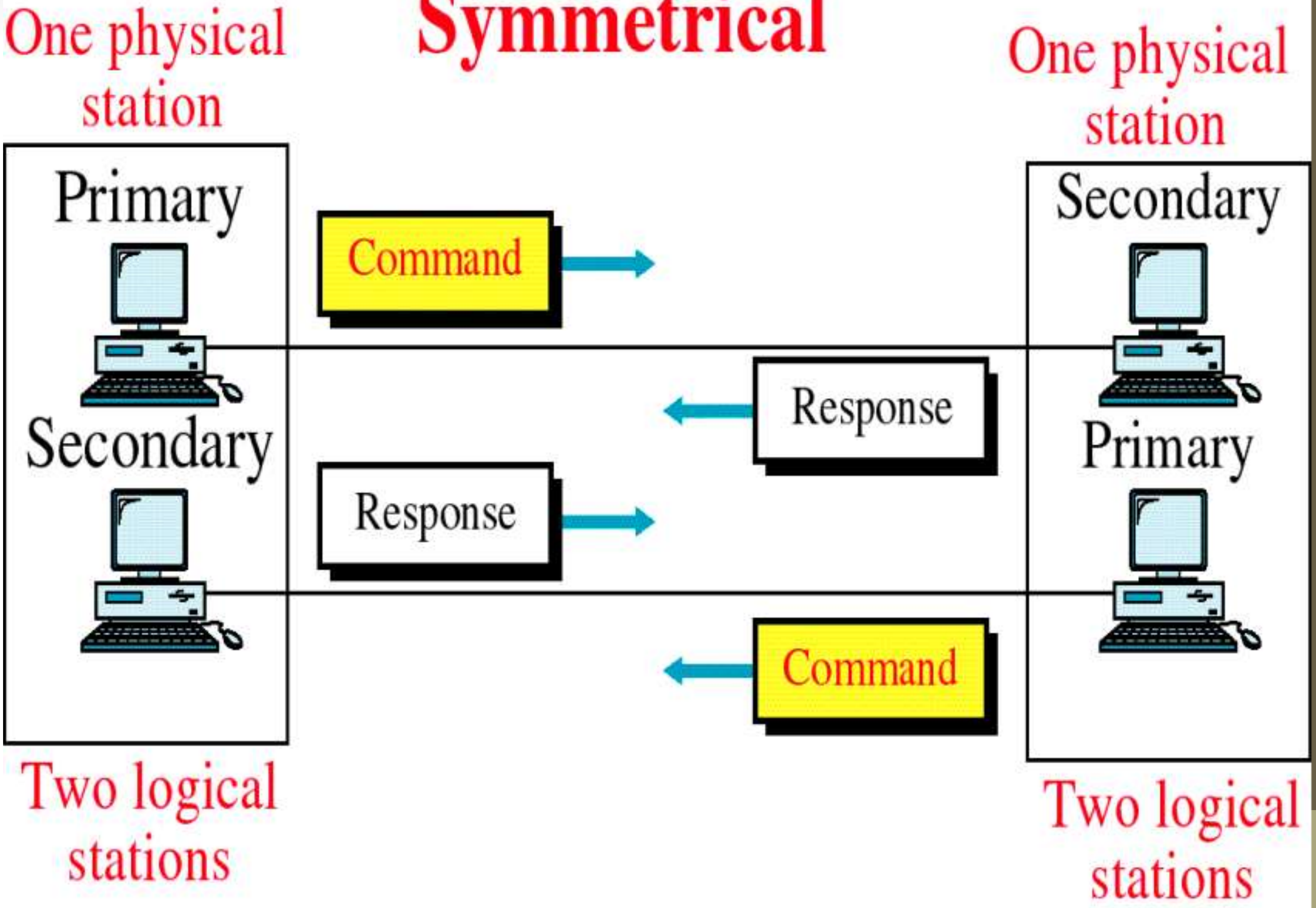
- It is one in which one device is primary and the others are secondary.
- It is point-to-point if only two devices are involved.
- It is multipoint when one primary controlling several secondary.


Unbalanced
Primary
Command
Secondary
Secondary
Response
Response

Symmetrical

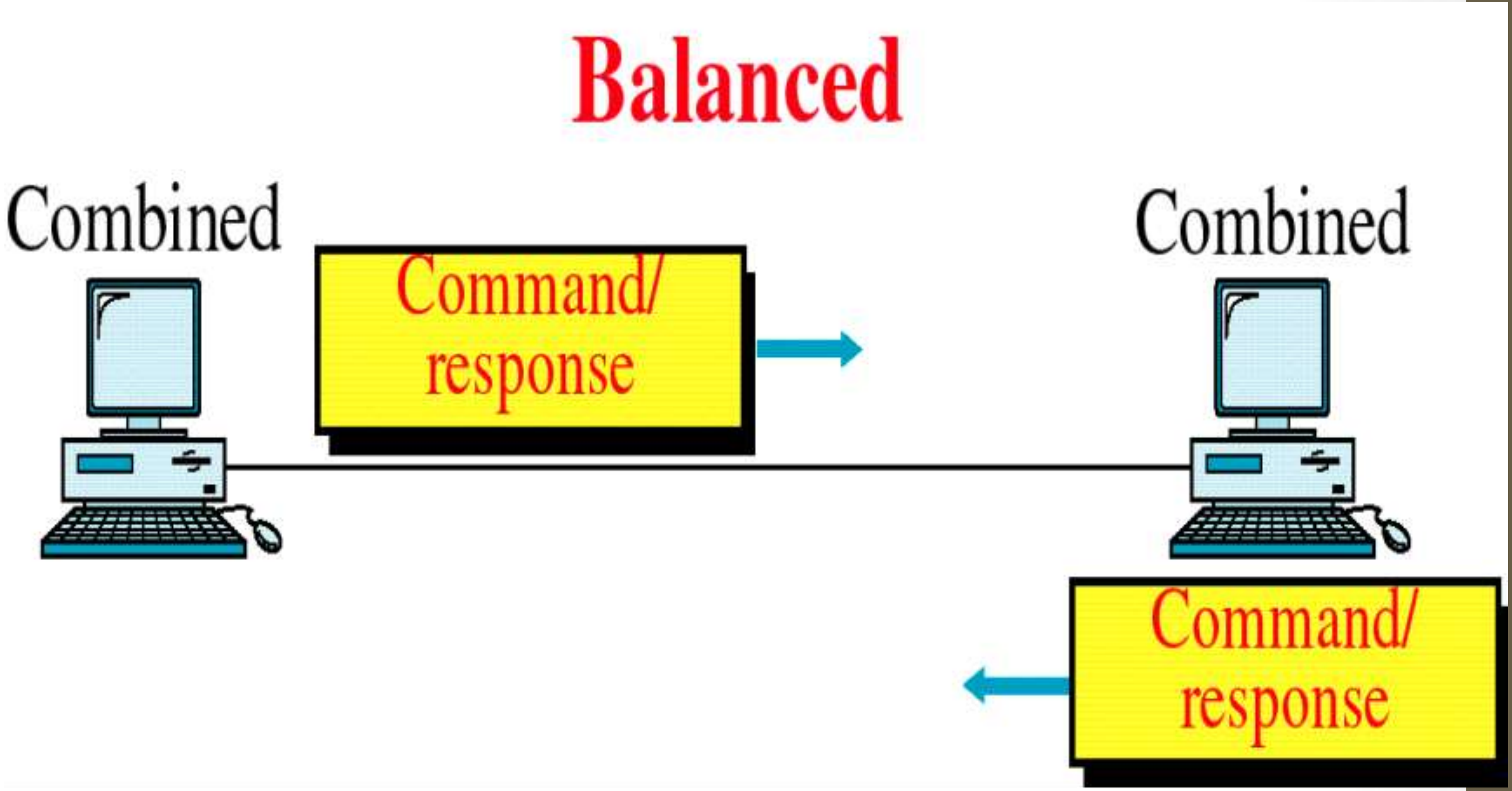
- It is one in which each physical station on a link consists of two logical stations, one is primary and the other a secondary.

Symmetrical



Balanced

- It is one in which both stations in a point-to-point topology are of the combined type.


Balanced
Combined
Combined
Command/
response
Command/
response

Modes of Communication

- NRM (Normal response mode)
- ARM (Asynchronous response mode)
- ABM(Asynchronous balanced mode)

NRM

- Refers to the standard primary secondary relationship.
- In this mode, a secondary device must have permission from the primary device before transmitting.
- Once permission has been granted, the secondary may initiate a response transmission of one or more frames containing data.

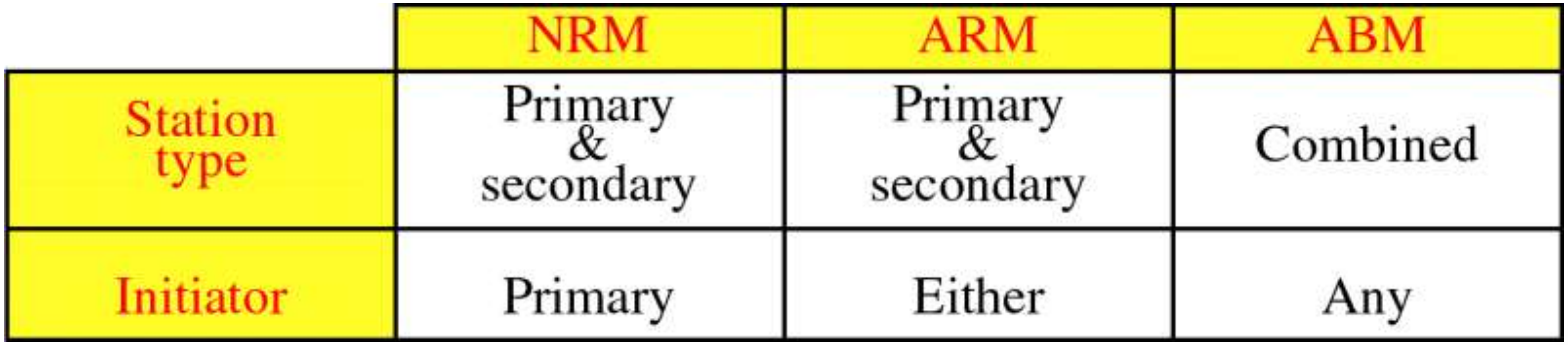
ARM

- A secondary may initiate a transmission without permission from the primary whenever the channel is idle.

ABM

- All stations are equal and therefore only combined stations connected in point-to-point are used.
- Either combined station may initiate transmission with the other combined station without permission.

HDLC Modes



	NRM	ARM	ABM
Station type	Primary & secondary	Primary & secondary	Combined
Initiator	Primary	Either	Any

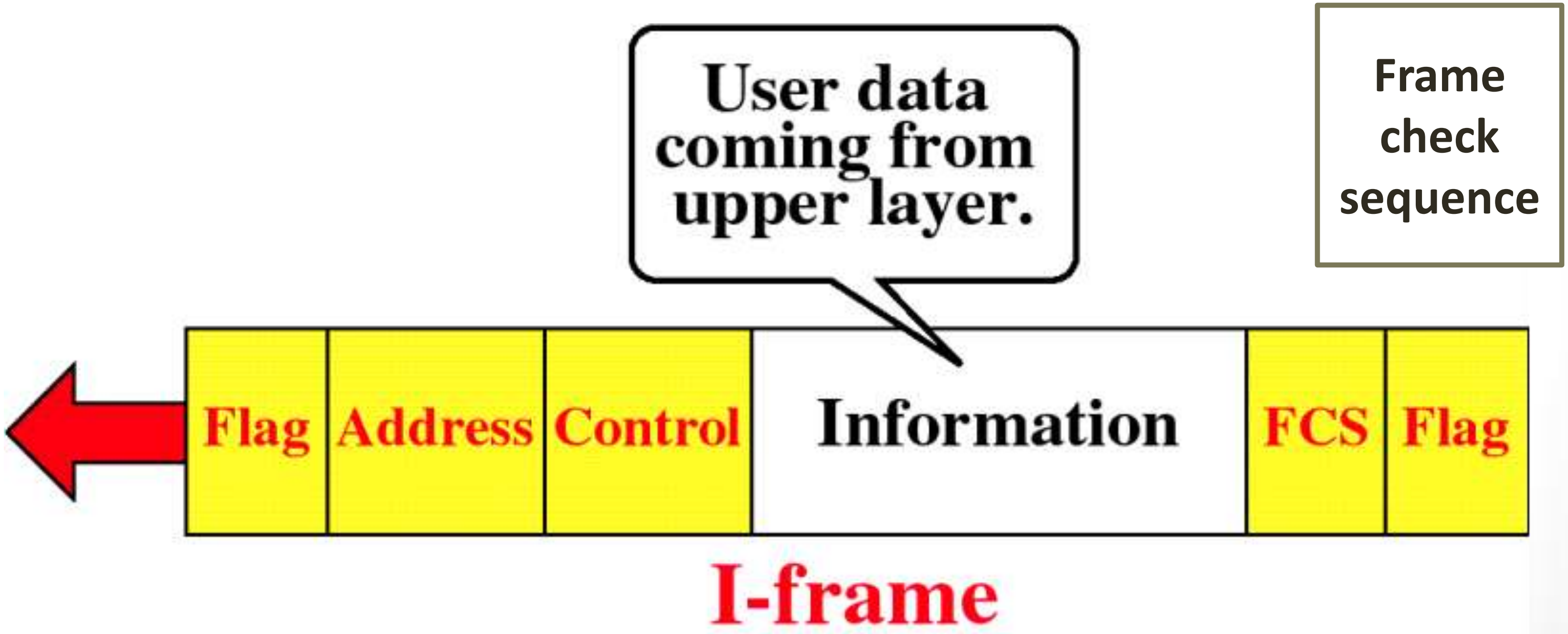
HDLC Frames

- HDLC defines 3 types of frames
  - I Frames (Information Frames)
  - S Frames (Supervisory Frames)
  - U Frames (Unnumbered Frames)

Frames

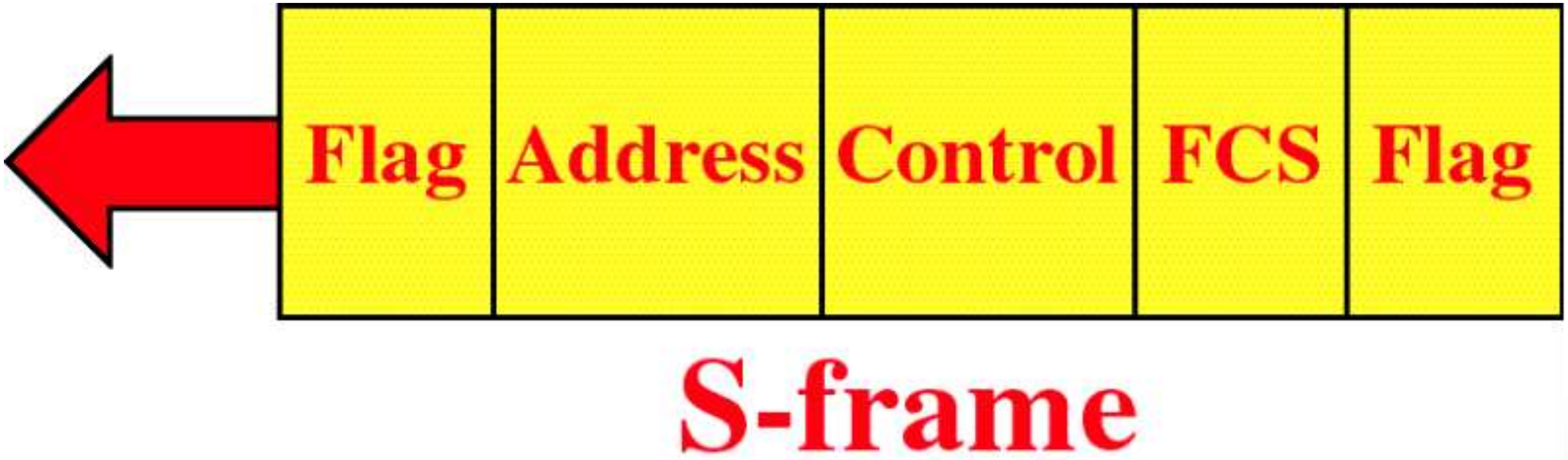
- I-frames are used to transport user data and control information relating to user data.
- S-frames are used only to transport control information, primarily data link layer flow and error control.
- U-frames are reserved for system management.

I Frames



Frame check sequence

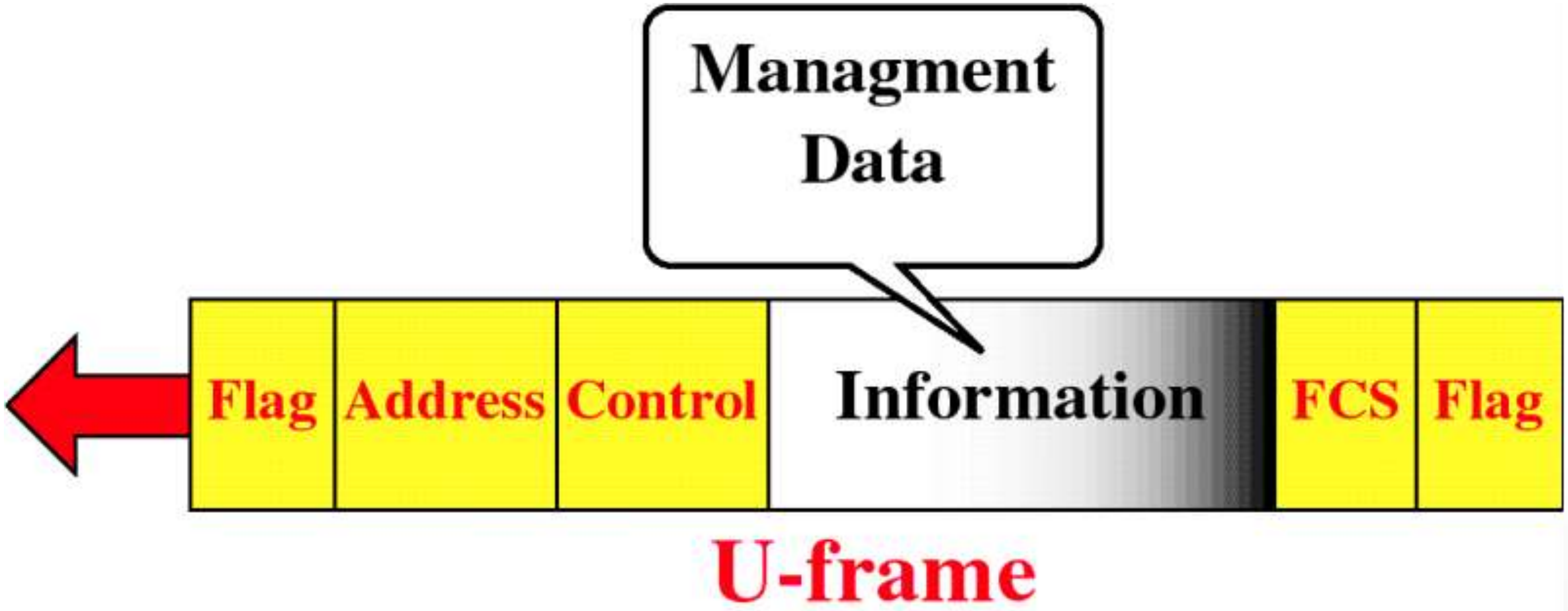
S-Frame



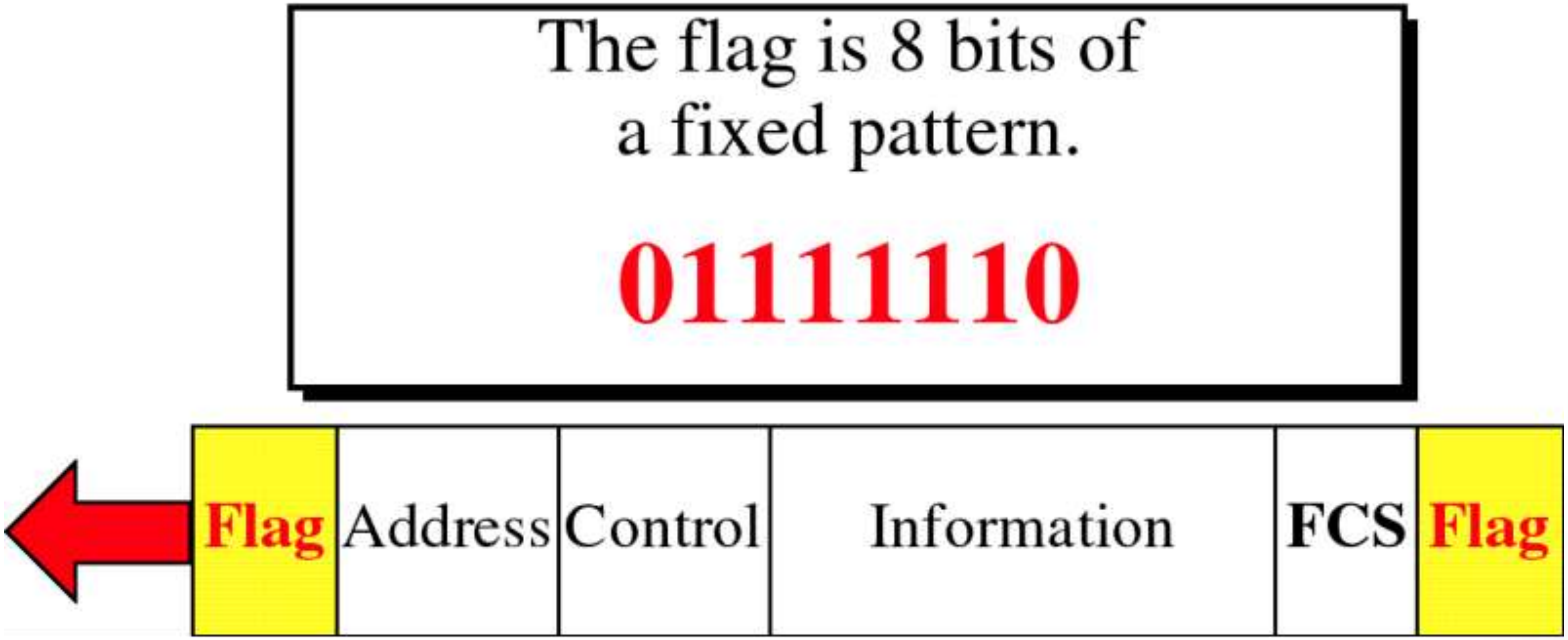
Flag	Address	Control	FCS	Flag

S-frame

U-Frame


Managment
Data
Flag
Address
Control
Information
FCS
Flag
U-frame

HDLC Flag Field



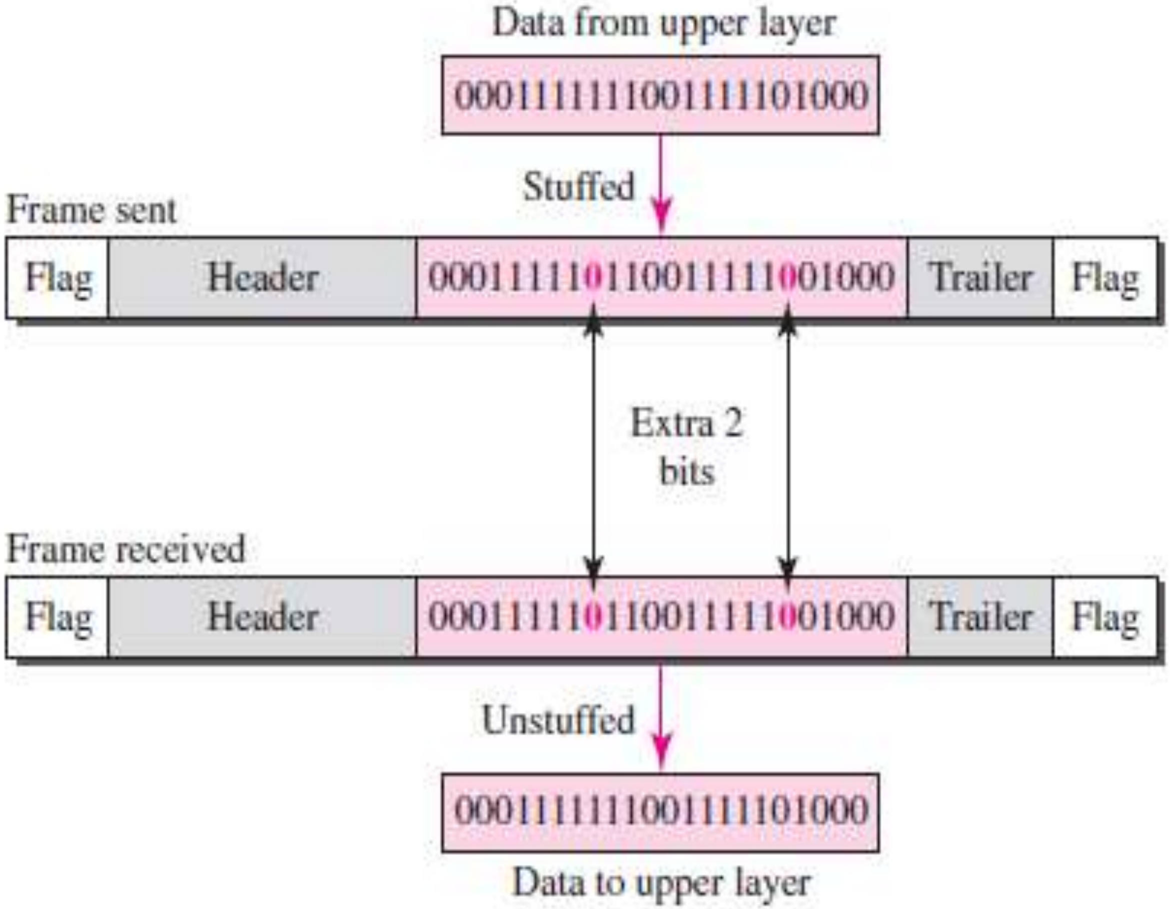
The flag is 8 bits of a fixed pattern.

01111110

Bit stuffing

- To guarantee that a flag does not appear anywhere else in the frame, HDLC uses a process called bit stuffing.
- Every time a sender wants to transmit a bit sequence having more than five consecutive 1s, it inserts one redundant 0 after the fifth 1.

Bit Stuffing & Unstuffing



Data from upper layer

0001111111001111101000

Stuffed

Frame sent

Flag	Header	000111110110011111001000	Trailer	Flag

Extra 2 bits

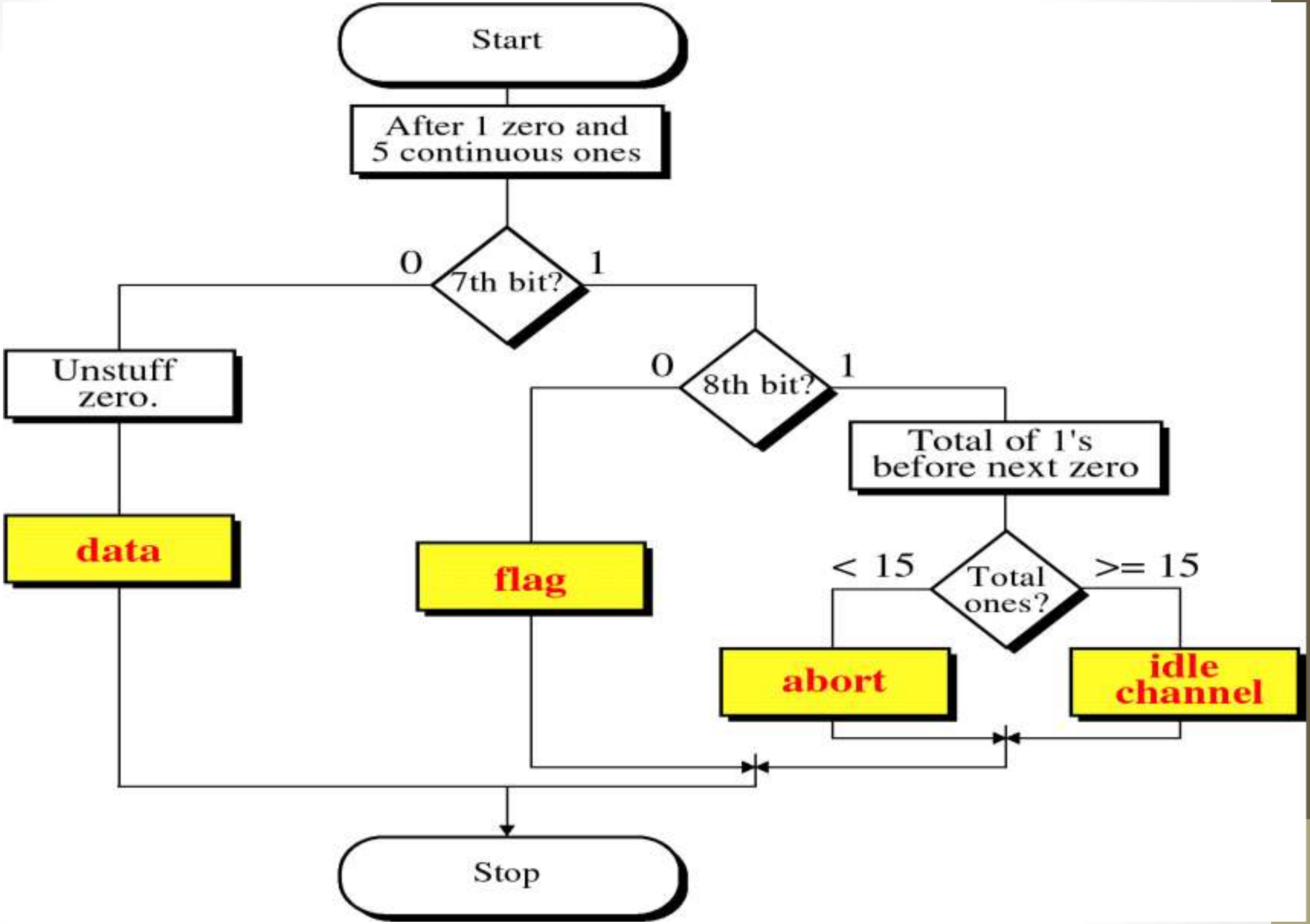
Frame received

Flag	Header	000111110110011111001000	Trailer	Flag

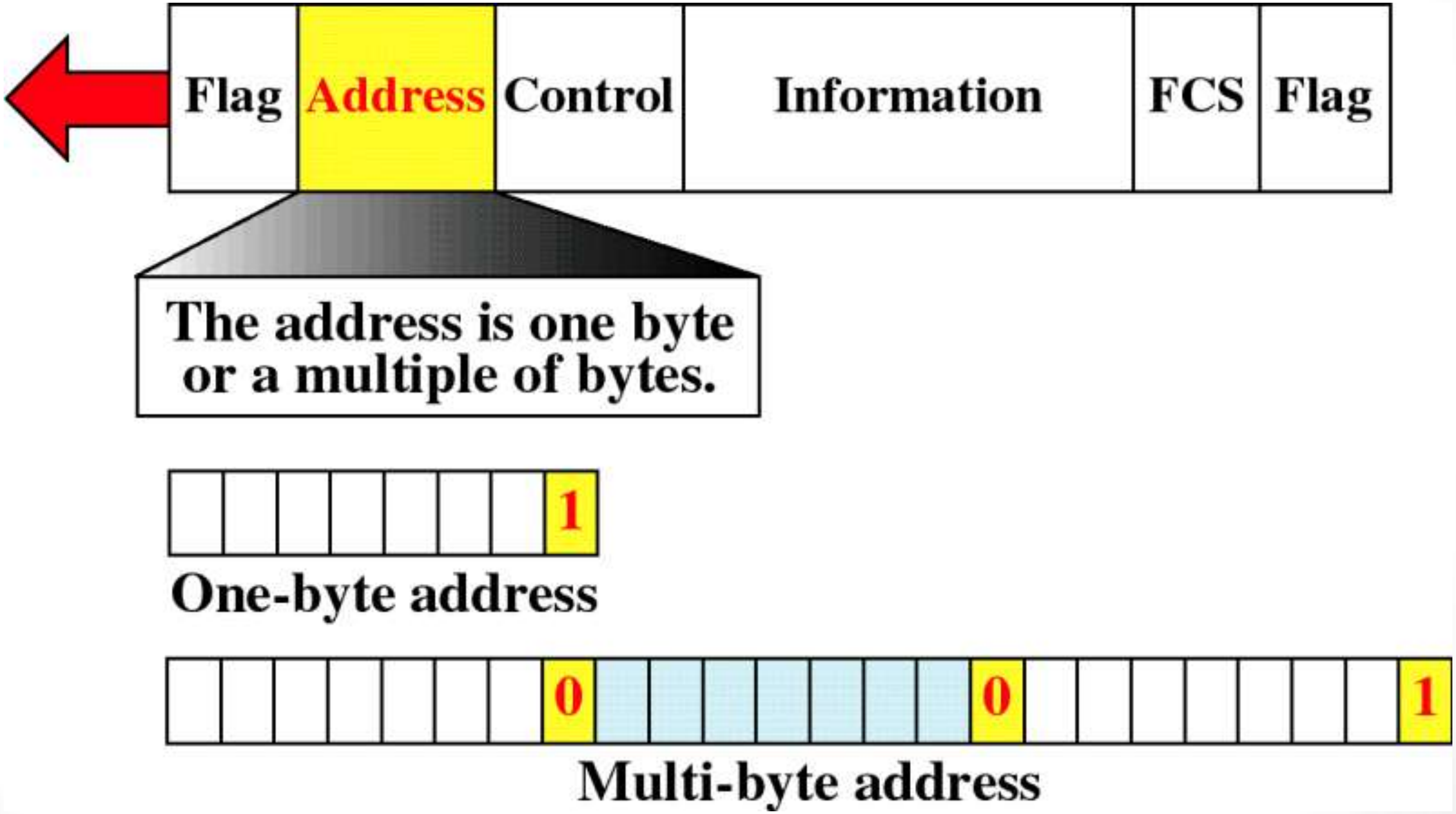
Unstuffed

0001111111001111101000

Data to upper layer


Start
After 1 zero and 5 continuous ones
0
7th bit?
1
Unstuff zero.
data
0
8th bit?
1
flag
Total of 1's before next zero
< 15
Total ones?
>= 15
abort
idle channel
Stop

HDLC Address Field

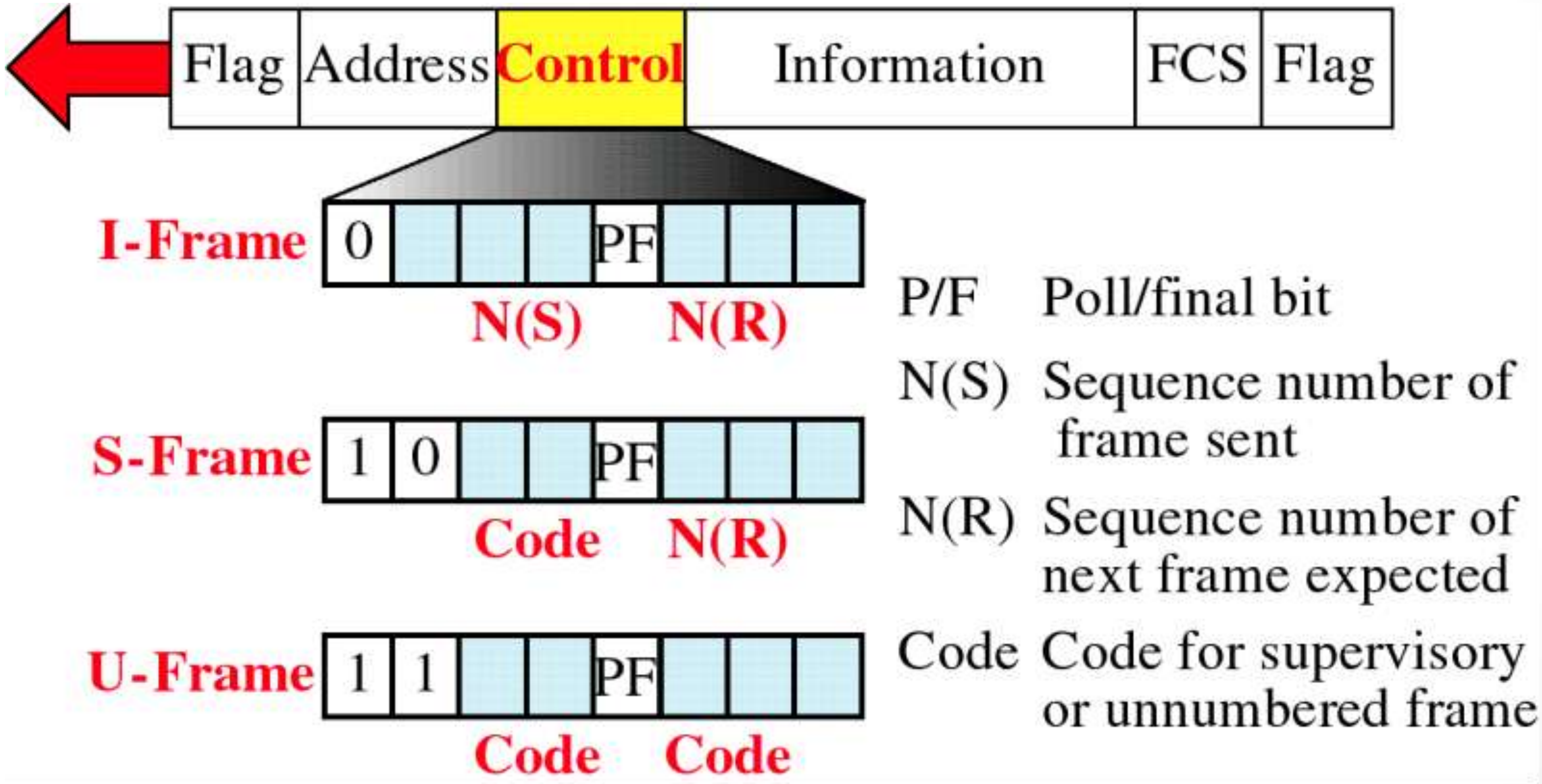


The address is one byte or a multiple of bytes.

One-byte address

Multi-byte address

HDLC Control Field



Flag | Address | Control | Information | FCS | Flag

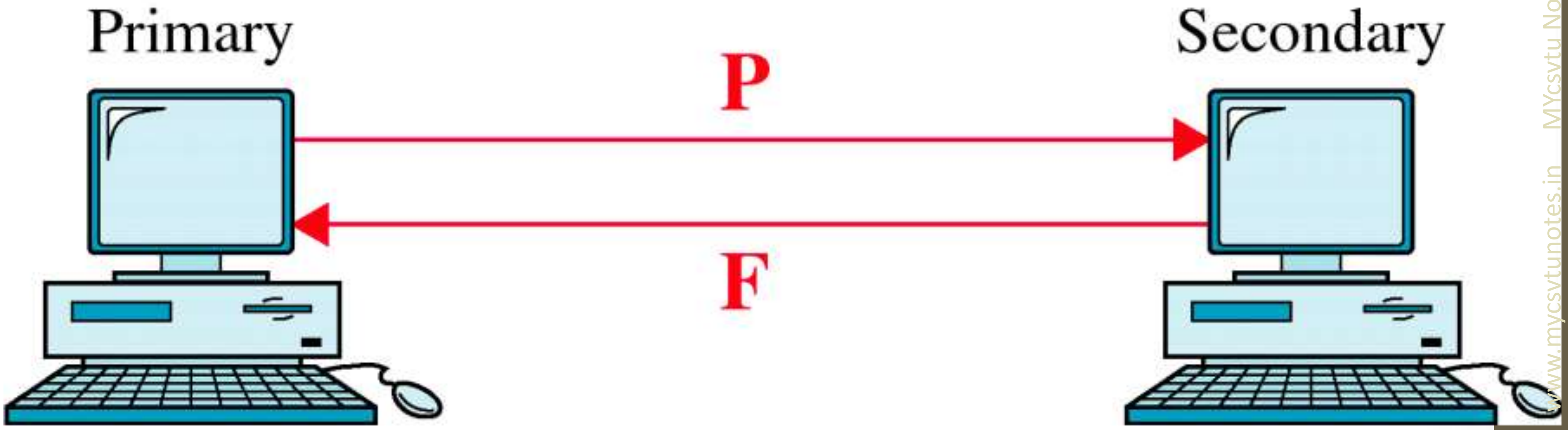
I-Frame: 0 | N(S) | PF | N(R)

S-Frame: 1 0 | Code | PF | N(R)

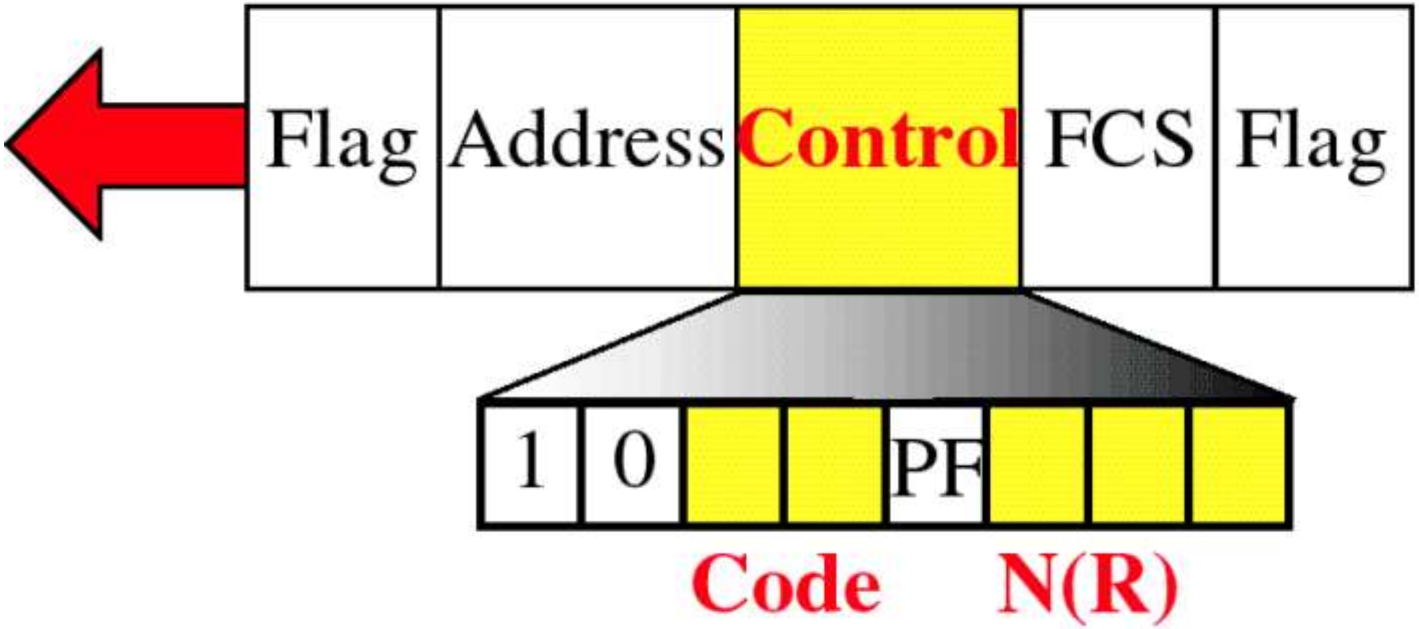
U-Frame: 1 1 | Code | PF | Code

P/F	Poll/final bit
N(S)	Sequence number of frame sent
N(R)	Sequence number of next frame expected
Code	Code for supervisory or unnumbered frame

Poll/Final

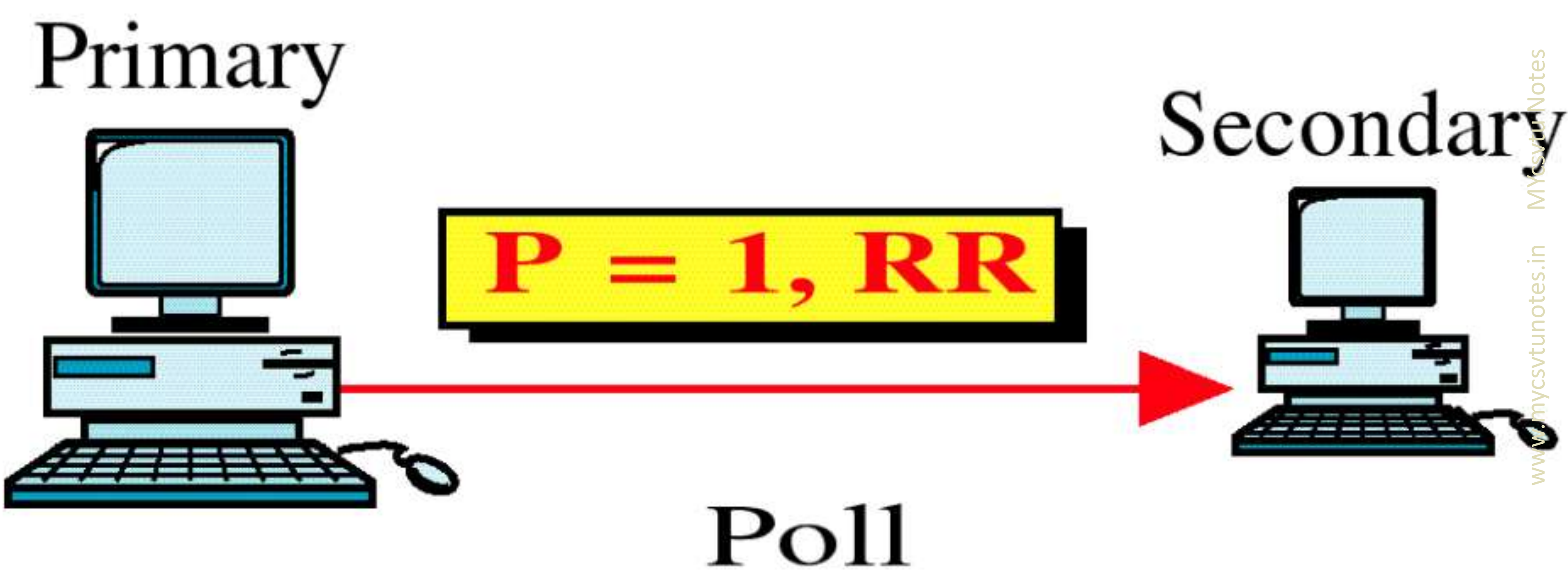


S-Frame

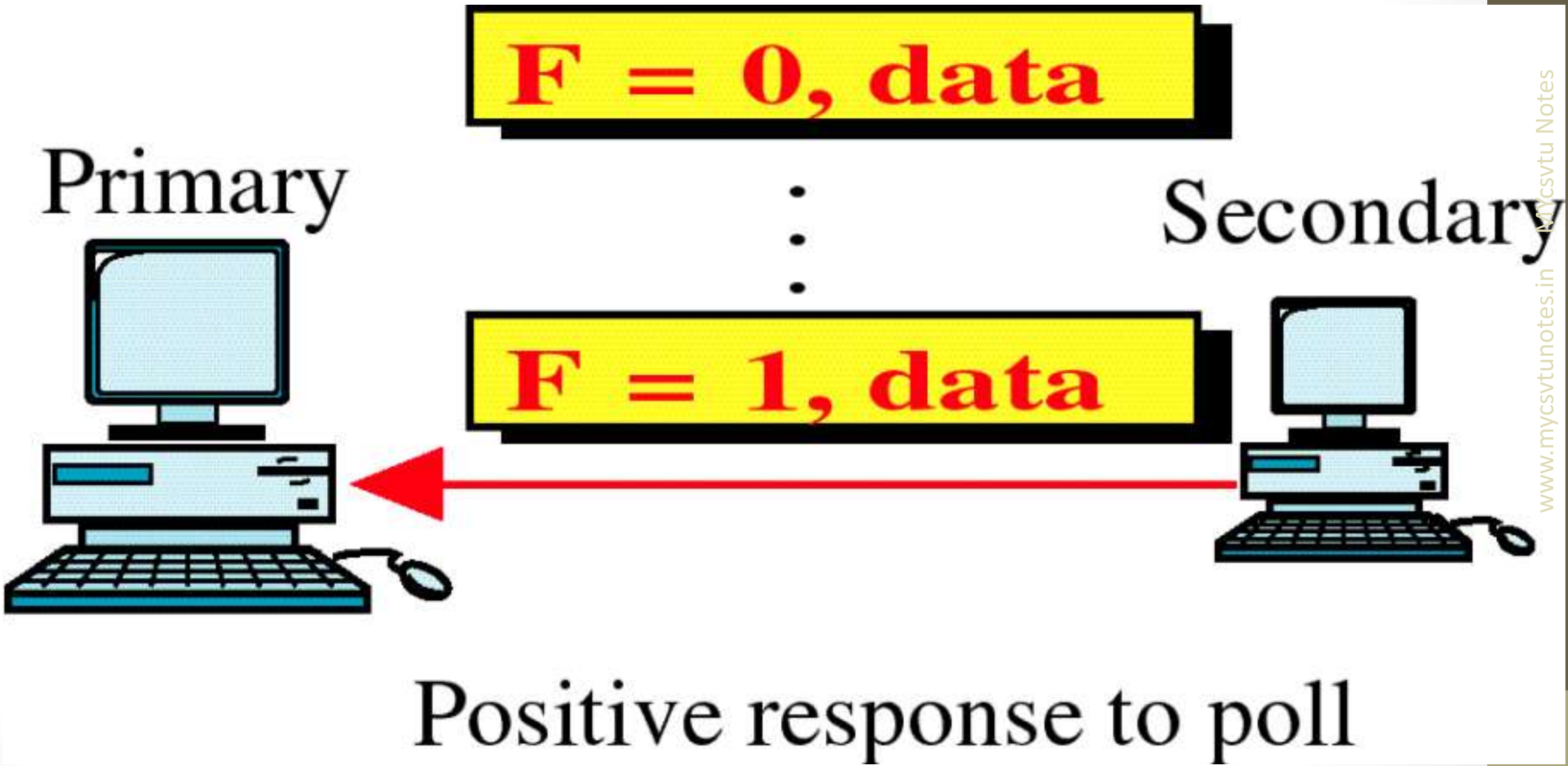


Code	Command	
00	RR	Receive ready
01	REJ	Reject
10	RNR	Receive not ready
11	SREJ	Selective-reject

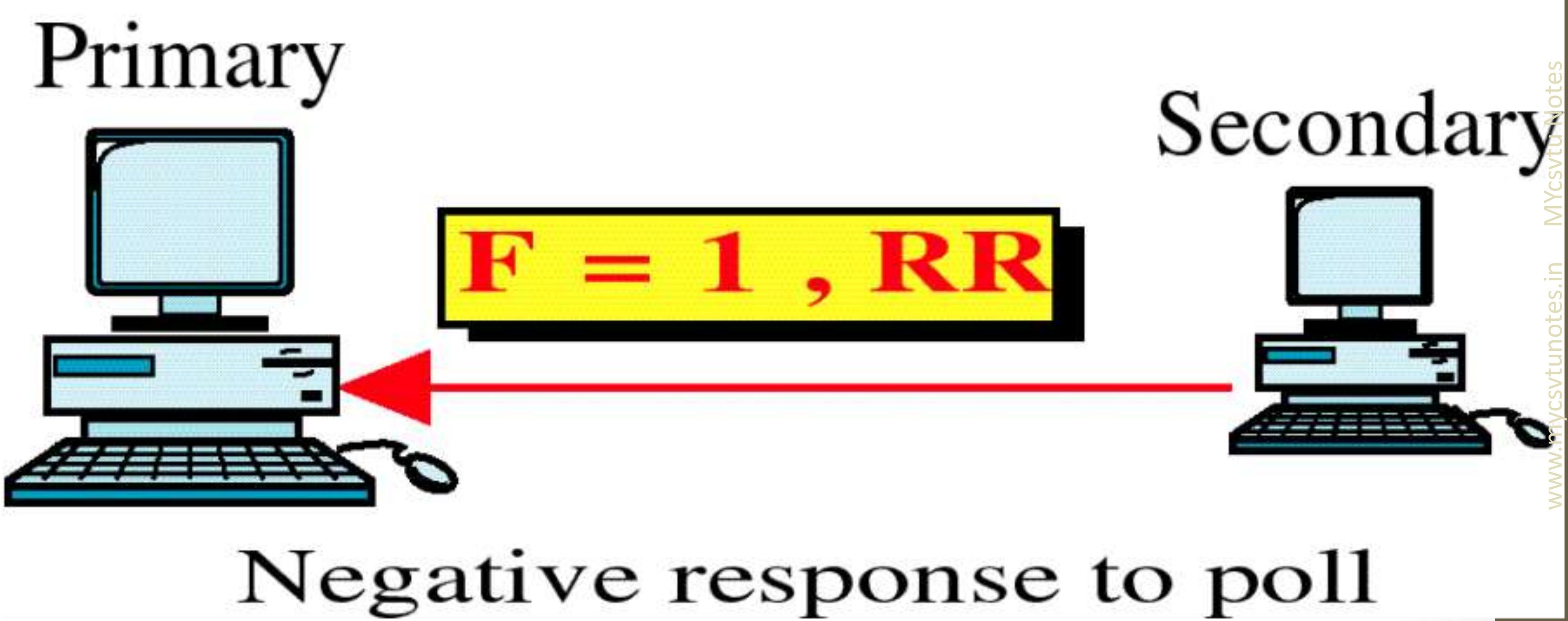
Use of P/F Field



Use of P/F Field



Use of P/F Field



Use of P/F Field

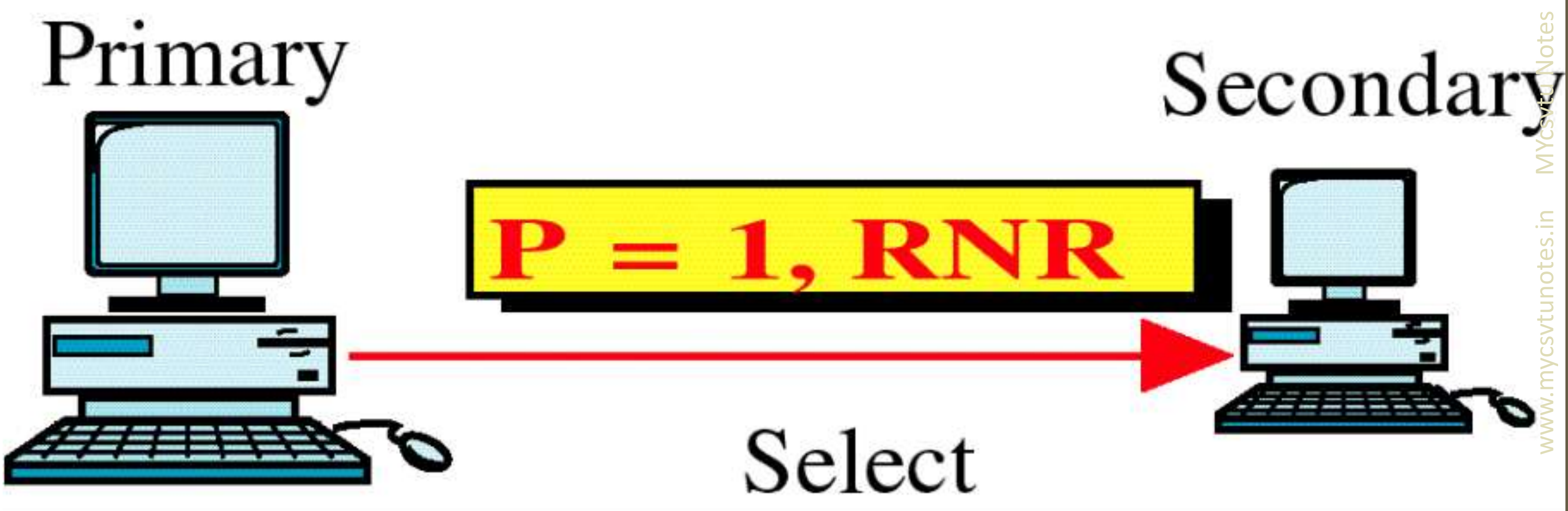
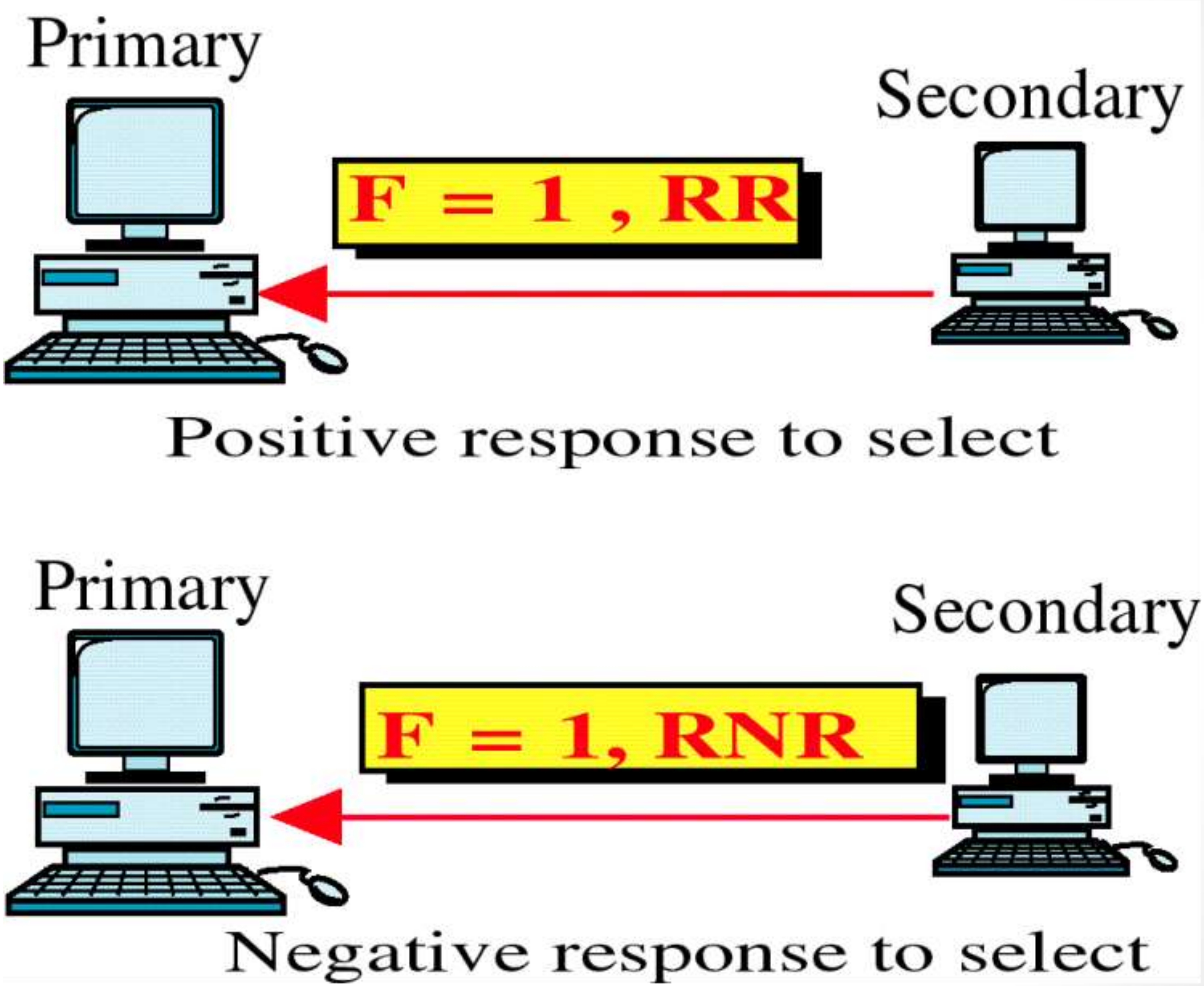


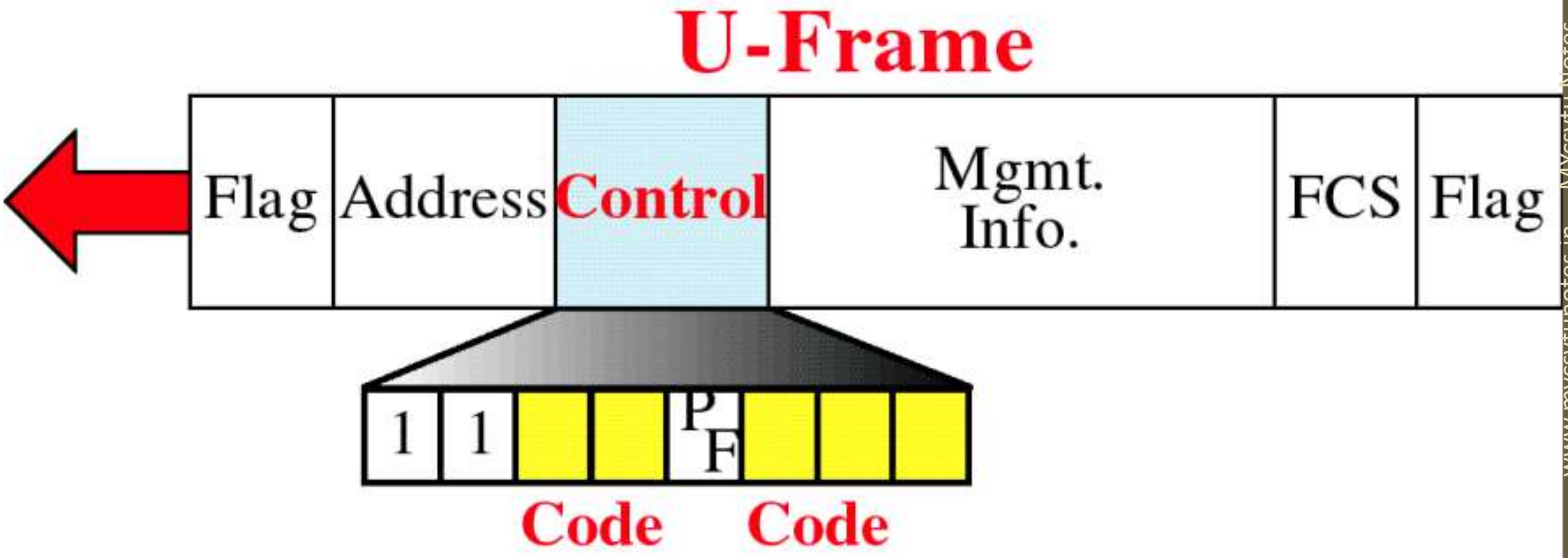
Figure 11-25-continued

Use of P/F Field

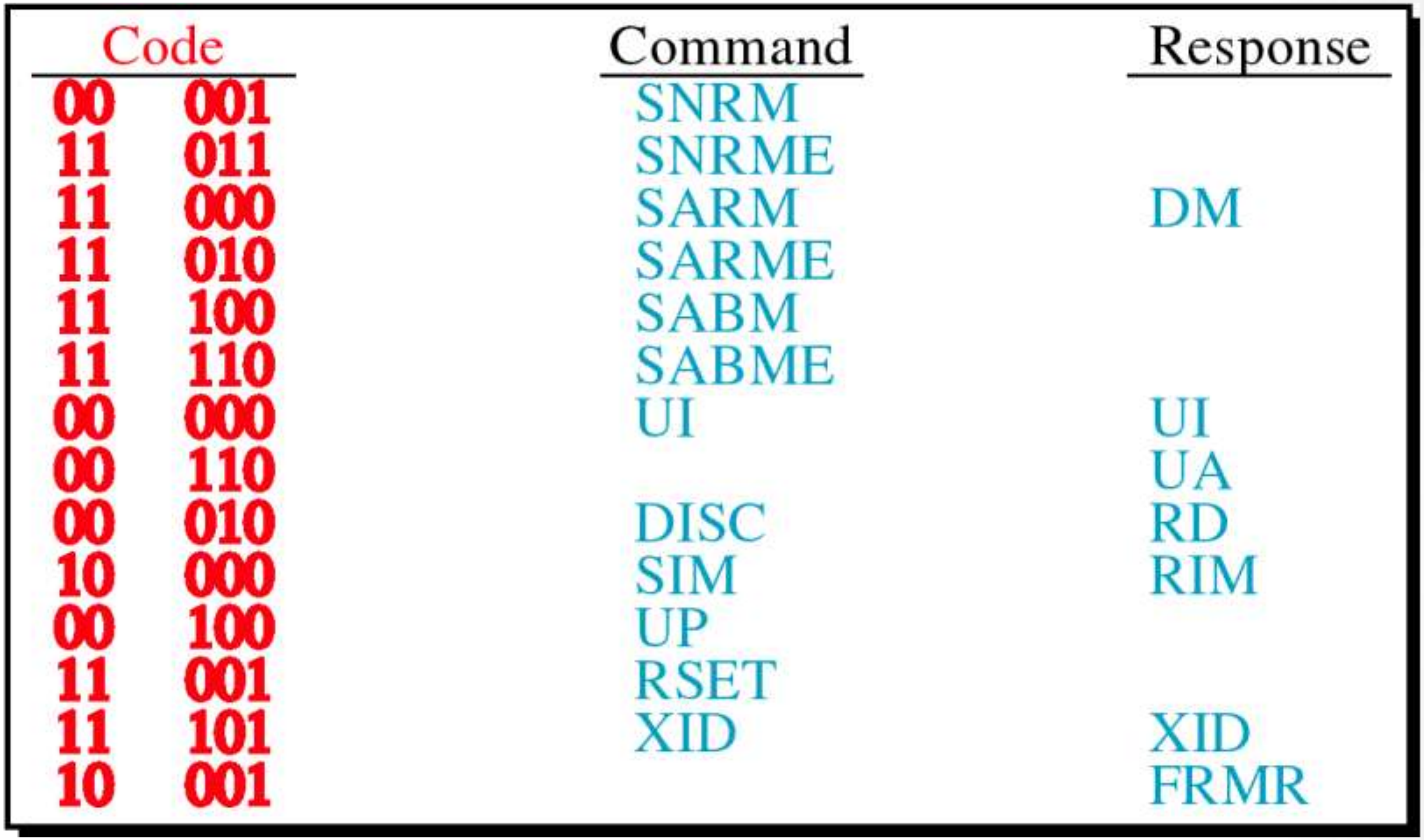


WCB/McGraw-Hill

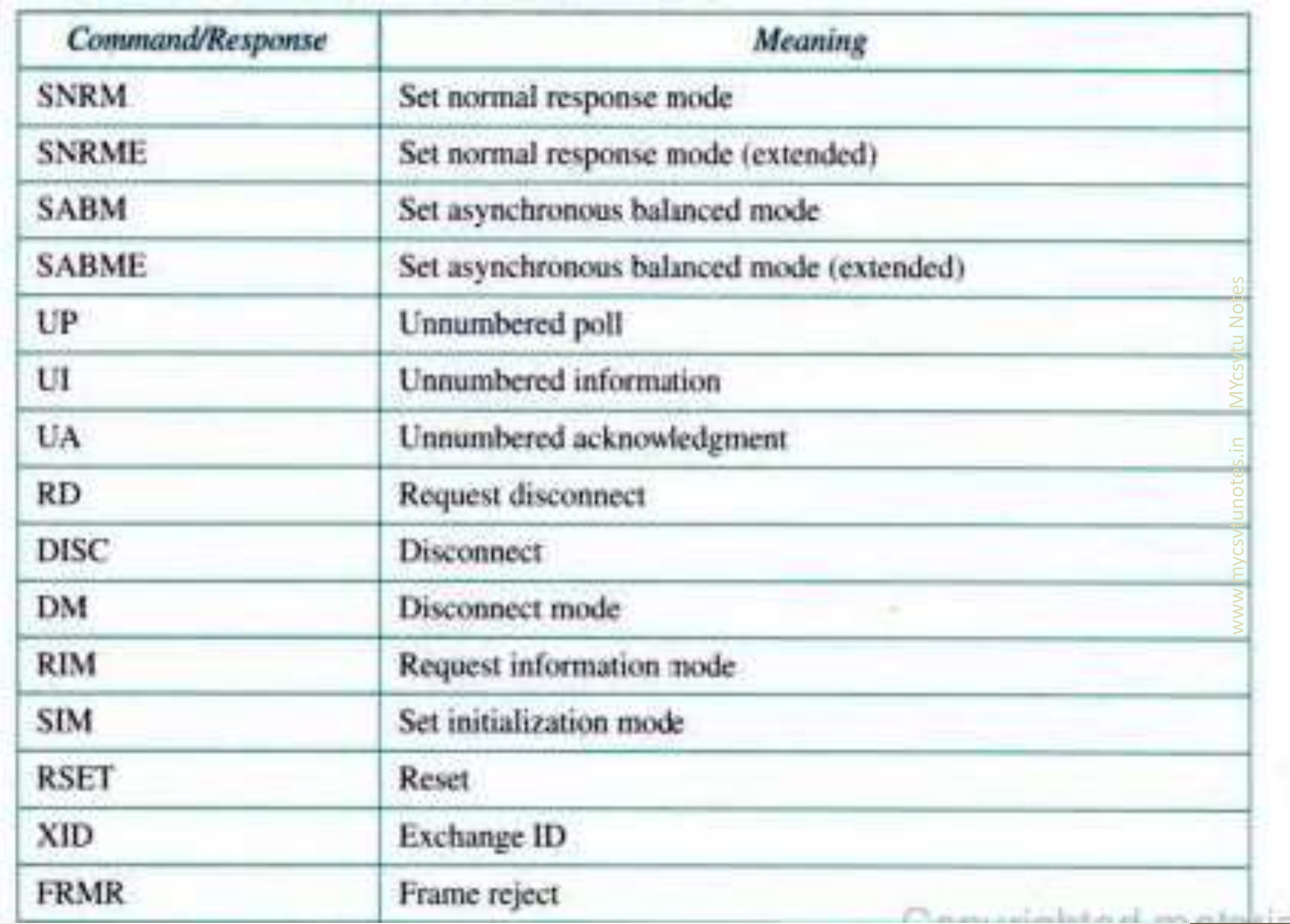
U-Frame Control Field



U-Frame Control Field

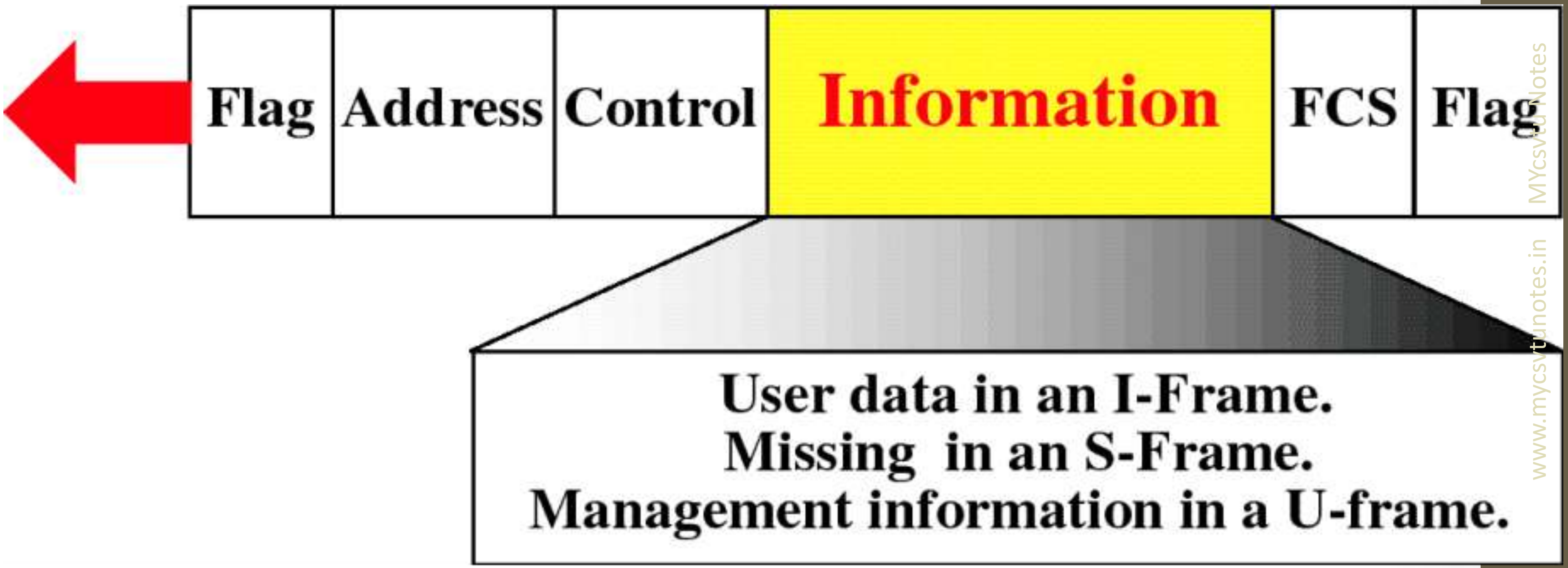


Code		Command	Response
00	001	SNRM	
11	011	SNRME	
11	000	SARM	DM
11	010	SARME	
11	100	SABM	
11	110	SABME	
00	000	UI	UI
00	110		UA
00	010	DISC	RD
10	000	SIM	RIM
00	100	UP	
11	001	RSET	
11	101	XID	XID
10	001		FRMR



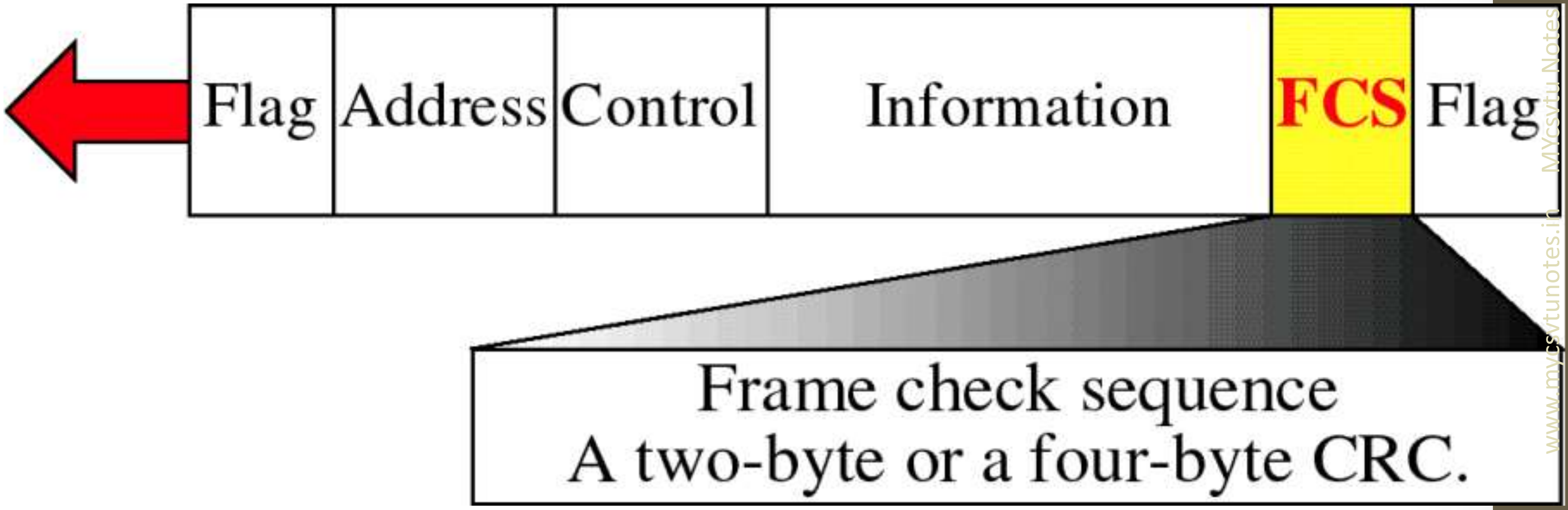
Command/Response	*Meaning*
SNRM	Set normal response mode
SNRME	Set normal response mode (extended)
SABM	Set asynchronous balanced mode
SABME	Set asynchronous balanced mode (extended)
UP	Unnumbered poll
UI	Unnumbered information
UA	Unnumbered acknowledgment
RD	Request disconnect
DISC	Disconnect
DM	Disconnect mode
RIM	Request information mode
SIM	Set initialization mode
RSET	Reset
XID	Exchange ID
FRMR	Frame reject

HDLC Information Field

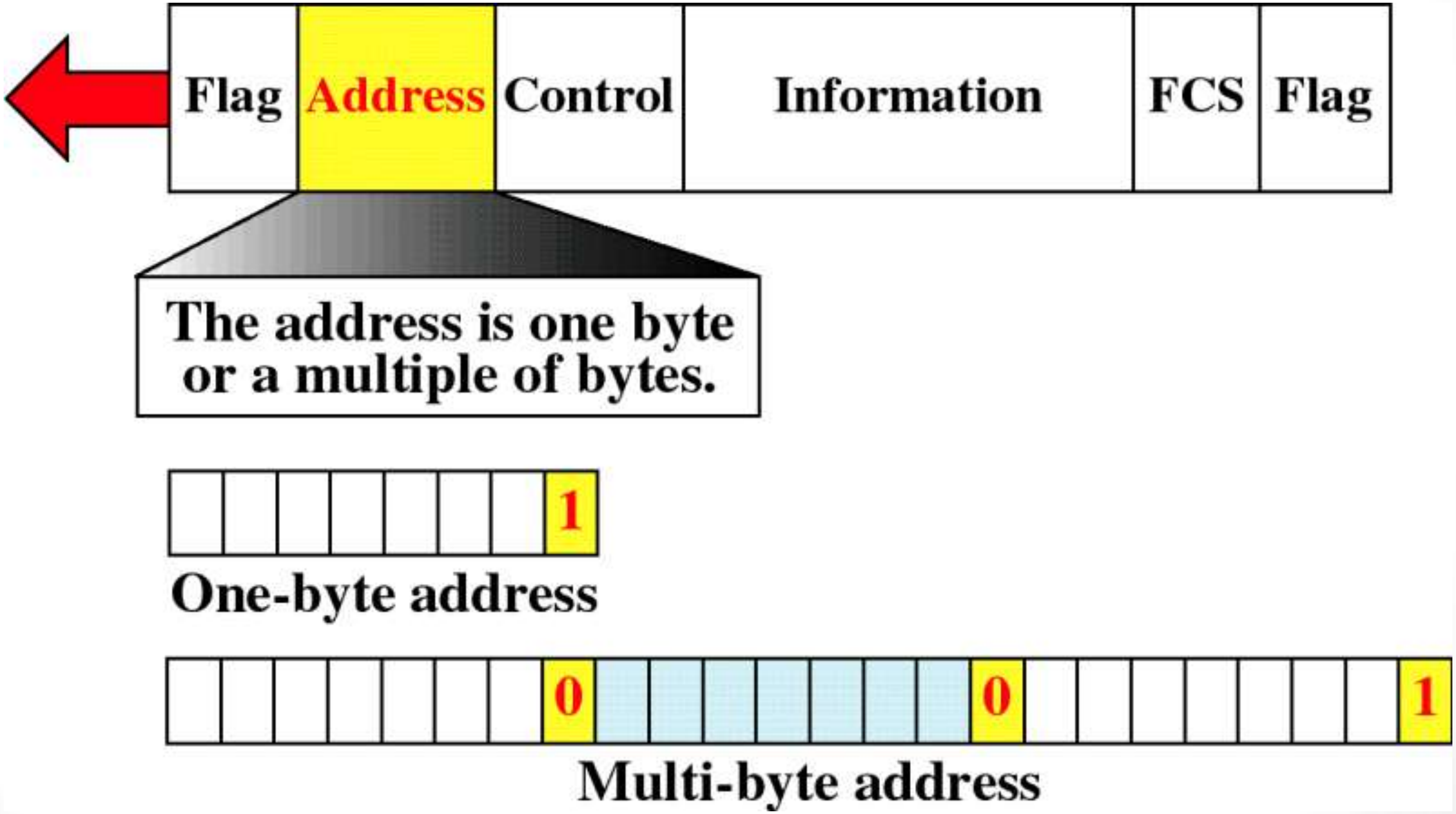


User data in an I-Frame.
Missing in an S-Frame.
Management information in a U-frame.

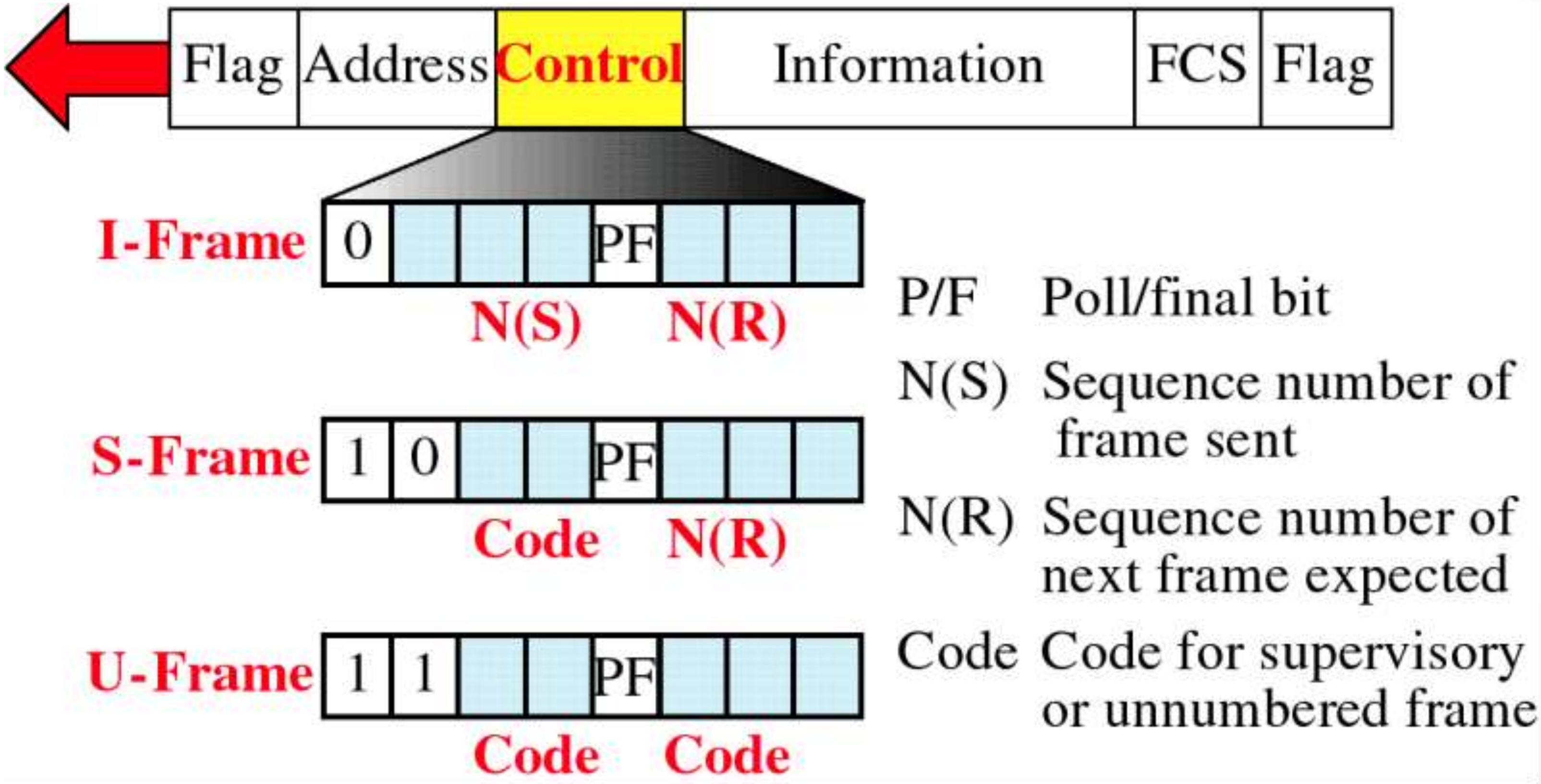
HDLC FCS(Frame check sequence) Field



HDLC Address Field

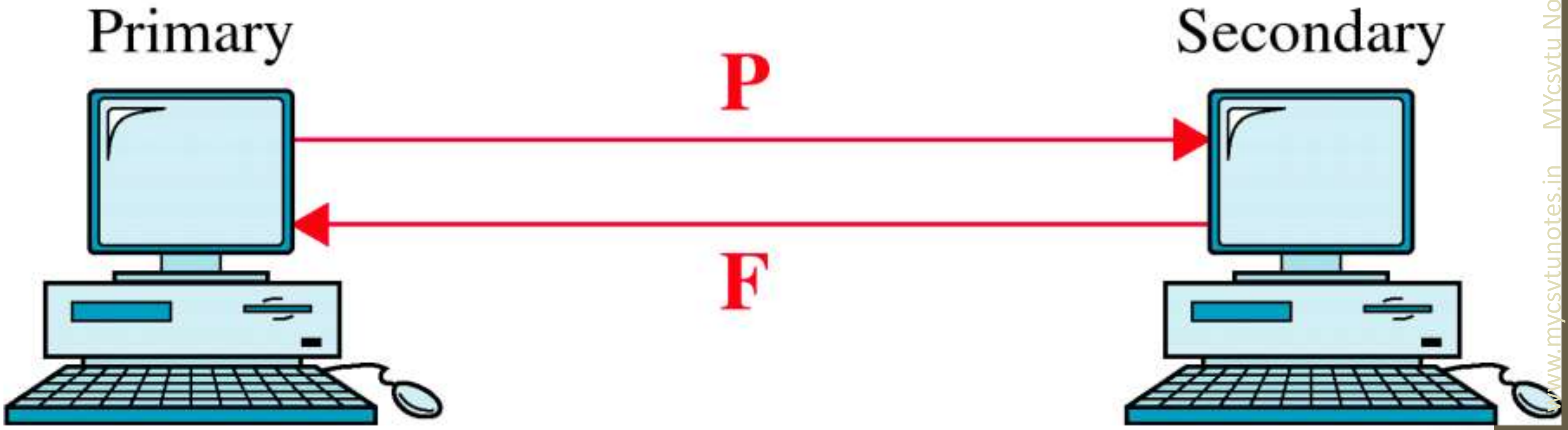


HDLC Control Field



P/F	Poll/final bit
N(S)	Sequence number of frame sent
N(R)	Sequence number of next frame expected
Code	Code for supervisory or unnumbered frame

Poll/Final



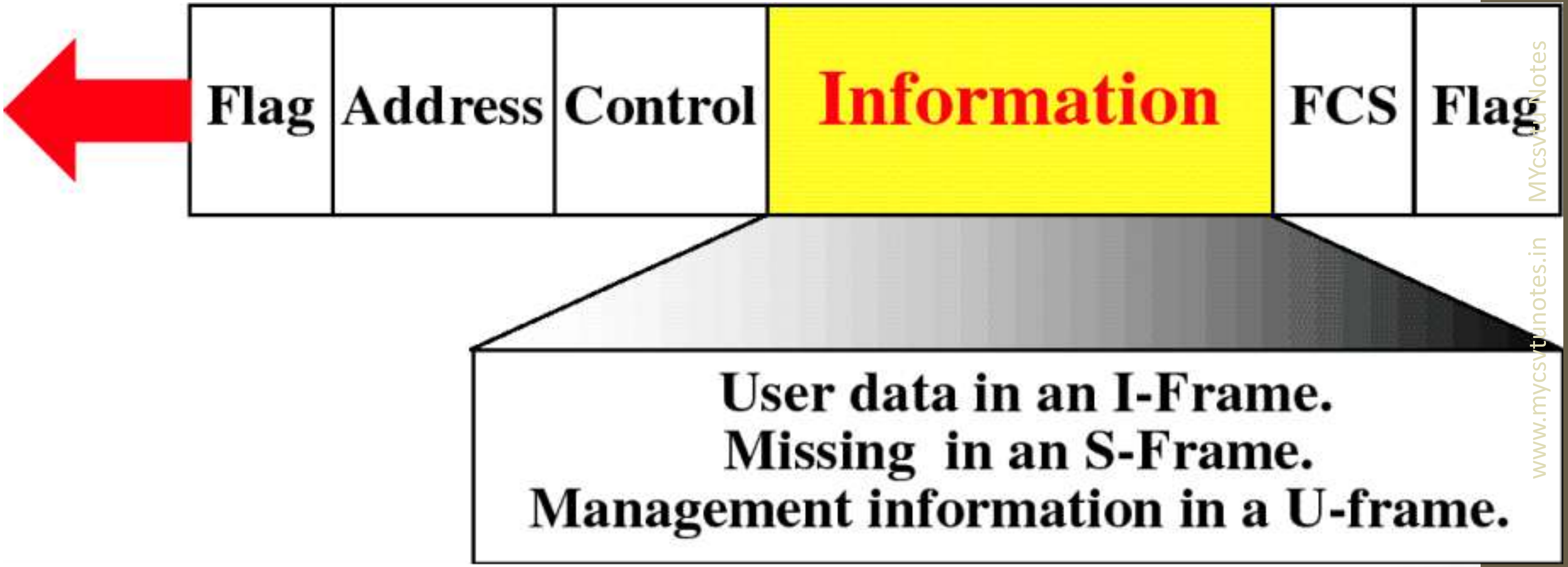
Poll/Select

- To poll a given secondary, a primary sends a frame to the secondary, with the P/F bit=1
- Only the last frame transmitted from the secondary has the P/F bit=1

Code

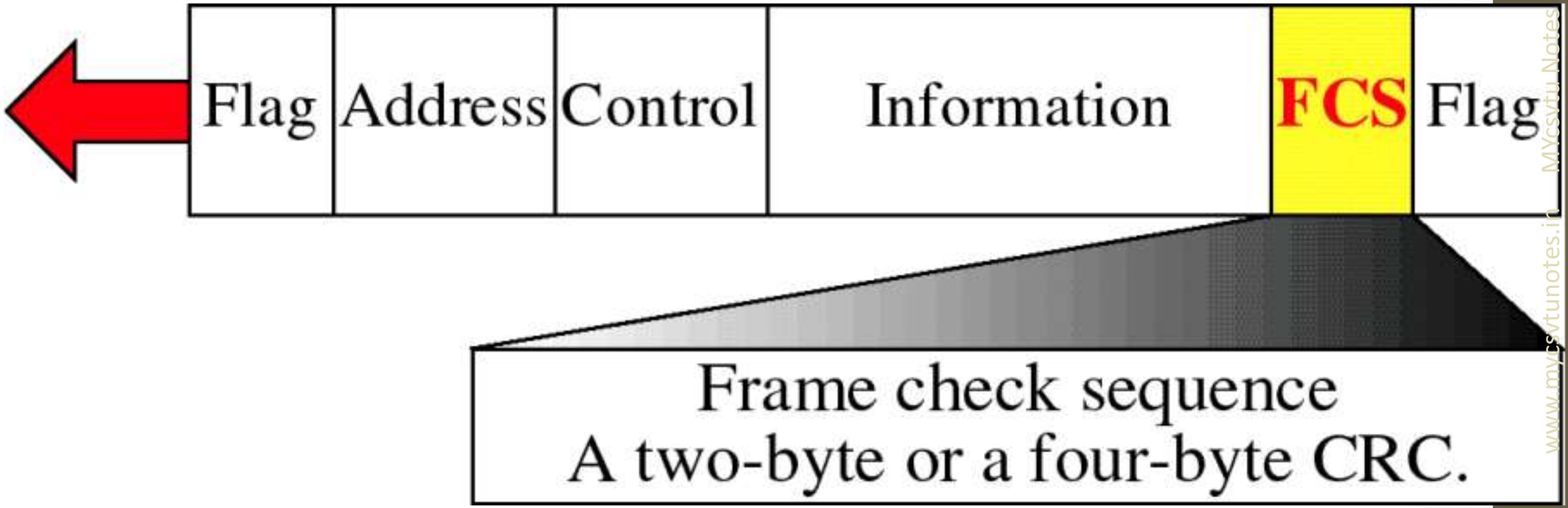
- 00-Receive ready(RR)
- 01-reject(REJ)
- 10-receive not ready(RNR)
- 11-Selective reject frame(SREJ)

HDLC Information Field



User data in an I-Frame.
Missing in an S-Frame.
Management information in a U-frame.

FCS(Frame check sequence) Field


Flag
Address
Control
Information
FCS
Flag
Frame check sequence
A two-byte or a four-byte CRC.