

Ministry of Higher Education and Scientific Researches  
Al-Mansour University College  
Department of Computer Technology Engineering  
Fourth Class



# Computer Networks Protocols

## Lecture Two: Physical & Data Link Layer

**Dr. Mahmoud Shuker Mahmoud**

## Part 1: PHYSICAL LAYER

### SONET\SDH Networks

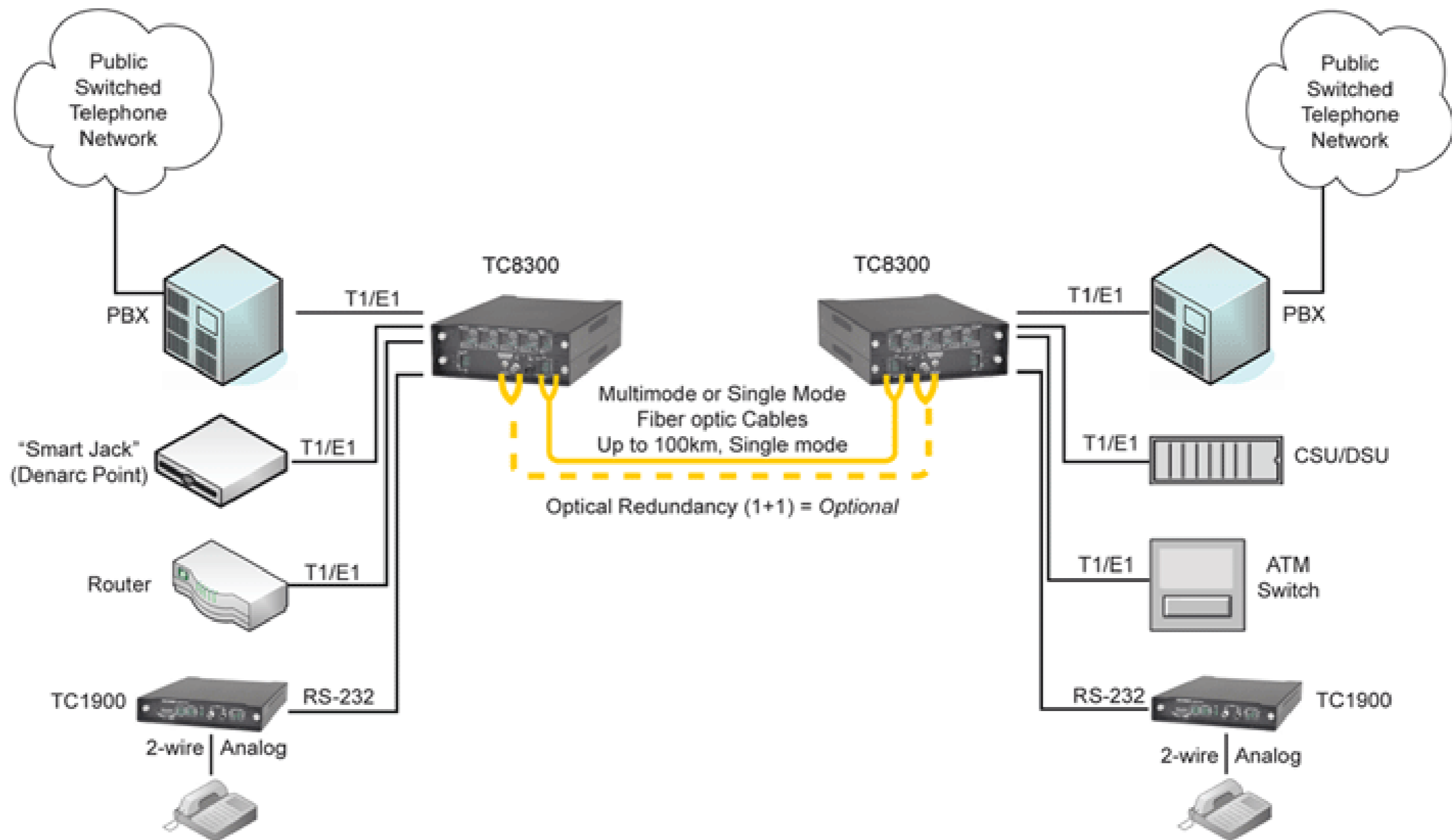
- **Synchronous Optical Networking (SONET)** and **Synchronous Digital Hierarchy (SDH)** are standardized **multiplexing protocols** that transfer multiple digital bit streams over **optical fiber** using **lasers or light-emitting diodes (LEDs)**.
- SONET\SDH, which is used as **a transport network to carry loads from other WANs**.

<b>SDH(Synchronous Digital Hierarchy)</b>	<b>SONET(Synchronous Optical Network)</b>
<ul style="list-style-type: none"><li>• Is <b>European</b> standard network.</li><li>• Is a standard developed by <b>ITU-T</b>.</li><li>• Define a <b>hierarchy of signals</b> called synchronous transfer modules (<b>STMs</b>)</li></ul>	<ul style="list-style-type: none"><li>• Is <b>American</b> standard network.</li><li>• Is a standard developed by <b>ANSI</b> for <b>fiber-optic networks</b>.</li><li>• Define a <b>hierarchy of signals</b> called synchronous transport signals (<b>STSs</b>( where each STS level (STS-1 to STS-192) <b>supports a certain data rate</b>.</li></ul>

## SONET\SDH Architecture

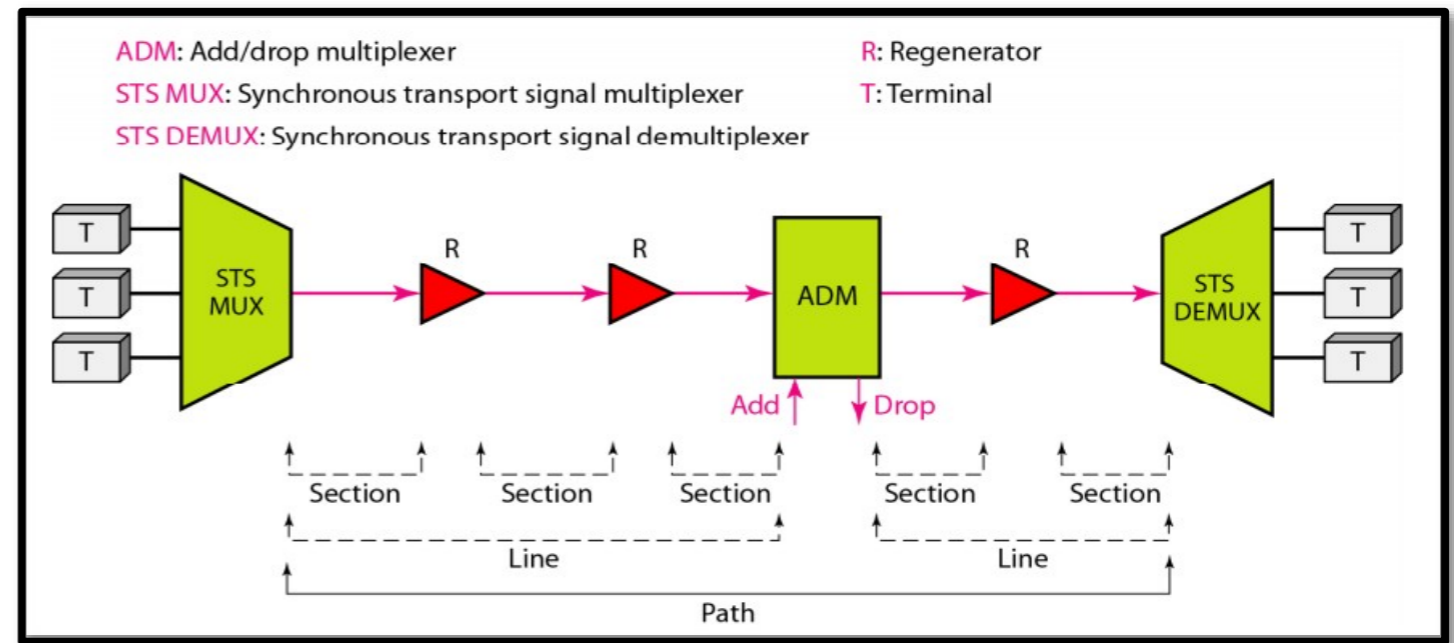
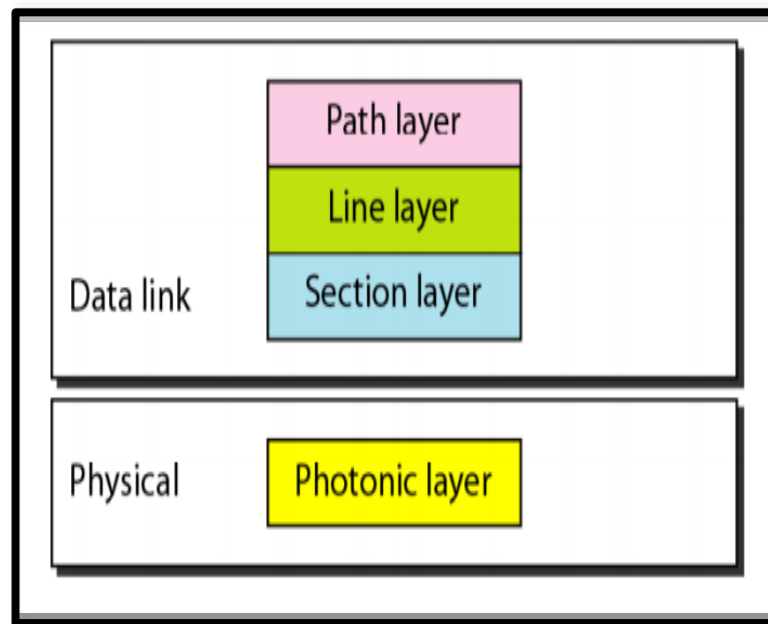
- **Architecture of a SONET system:** signals, devices, and connections
- **Signals:** SONET(SDH) defines a hierarchy of electrical signaling levels called STSs (Synchronous Transport Signals, (STMs)). Corresponding optical signals called OCs (Optical Carriers)

<i>STS</i>	<i>OC</i>	<i>Rate (Mbps)</i>	<i>STM</i>
STS-1	OC-1	51.840	
STS-3	OC-3	155.520	<b>STM-1</b>
STS-9	OC-9	466.560	<b>STM-3</b>
STS-12	OC-12	622.080	<b>STM-4</b>
STS-18	OC-18	933.120	<b>STM-6</b>
STS-24	OC-24	1244.160	<b>STM-8</b>
STS-36	OC-36	1866.230	<b>STM-12</b>
STS-48	OC-48	2488.320	<b>STM-16</b>
STS-96	OC-96	4976.640	<b>STM-32</b>
STS-192	OC-192	9953.280	<b>STM-64</b>



The SONET standard includes **four functional layers** corresponding to the physical and the data link layers shown in the figure below.

- ❖ **Path layer** is responsible for the movement of a signal from its optical source to its optical destination.
- ❖ **Line layer** is for the movement of a signal across a physical line.
- ❖ **Section layer** is for the movement of a signal across a physical section, handling framing, scrambling, and error control.
- ❖ **Photonic layer** corresponds to the physical layer of the OSI model



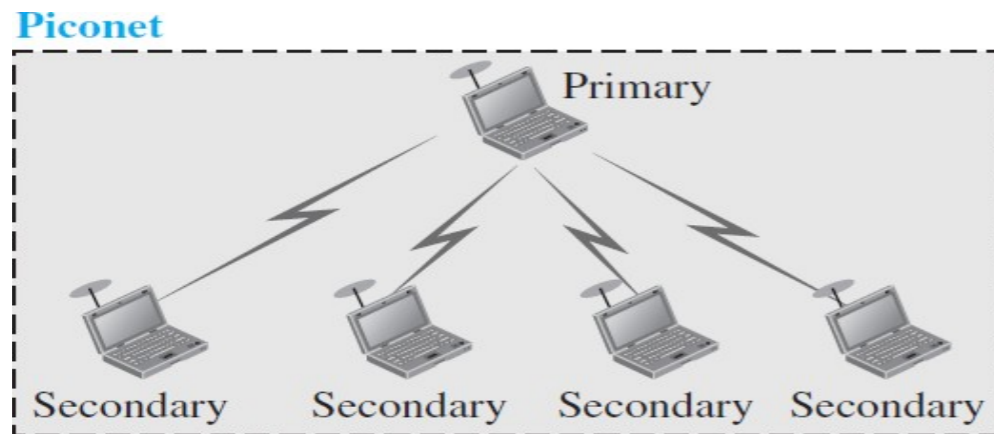
## BLUETOOTH

- **Bluetooth** is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a **short distance** from each other.

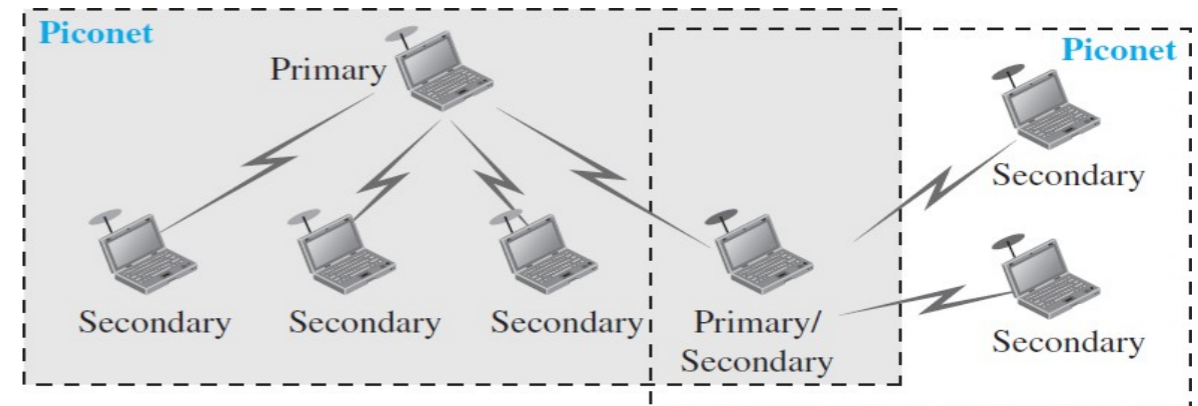
### Architecture of Bluetooth:

- Bluetooth defines two types of networks: **piconet** and **scatternet**.
- A Bluetooth network is called a *piconet, or a small net*. A piconet can have up to eight stations, one of which is called the *primary*; the rest are called *secondaries*.

**Piconet Network**



**Scatternet Network**



## Comparison between Bluetooth Piconet and Scatternet Architecture

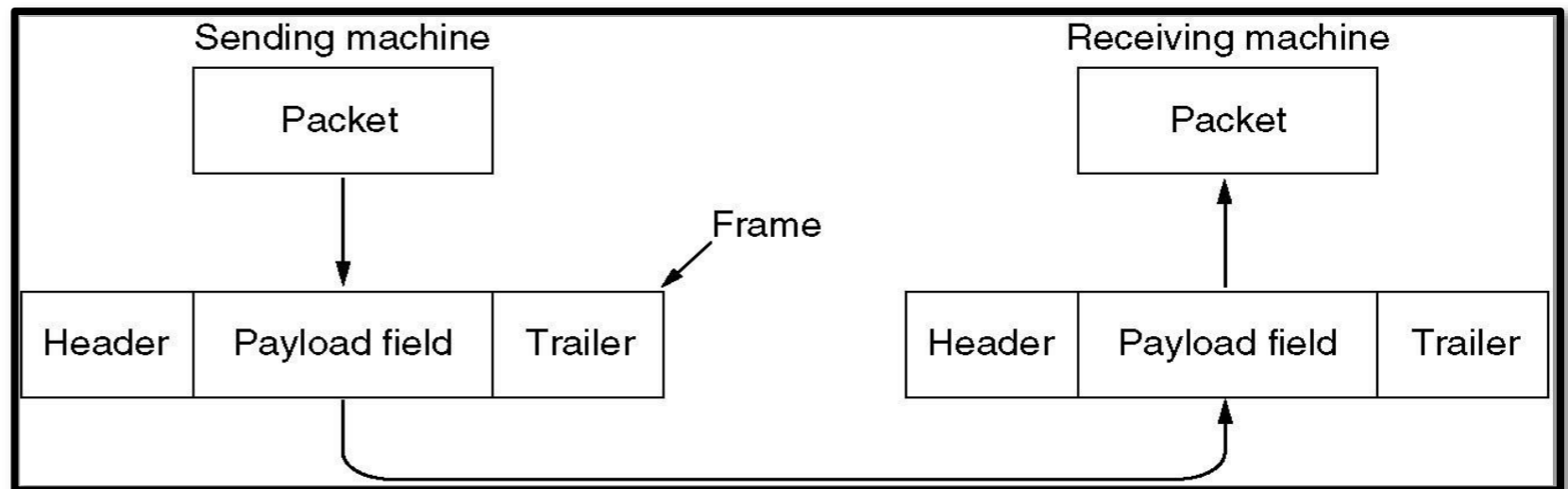
Piconet	Scatternet
In this bluetooth network, device can function either as master or slave.	In this bluetooth network, device can function as master or slave or (master+slave)
It serves smaller coverage area.	It serves larger coverage area.
It supports maximum 8 nodes.	It supports more than 8 nodes.
It allows less efficient use of available bluetooth channel bandwidth.	It allows more efficient use of available bluetooth channel bandwidth.

## Part 2: Data Link Layer

**Data-link layer** has the responsibility of transferring datagram from one **node to physically adjacent node** over a link. The data link layer is divided into two sublayers: **Logical Link Control (LLC)** and **Media Access Control (MAC)**. The LLC sublayer manages communications between devices over a single link of a network. The MAC sublayer governs protocol access to the physical network medium.

### Main Services Provided by Data link layer

- Framing
- Error Control
- Flow Control



# Data Link Protocols

## Elementary Data Link Protocols

The main job of elementary data link layer protocols is to receive packets from network layer, create the frame and send it to physical layer, or vice versa. These are some elementary data link layer protocols:

<b>An Unrestricted Simplex Protocol (SP)</b>	one direction transmitted data
<b>A Simplex Stop-and-Wait Protocol(SWP)</b>	flooding control
<b>A Simplex Protocol for a Noisy Channel(SPN)</b>	limit send and receive between sender and receiver, capacities are limited

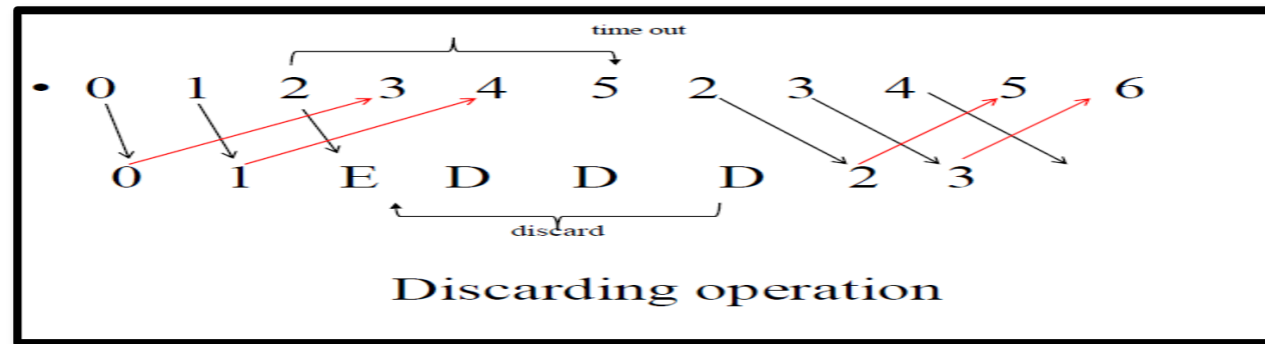
## Sliding Window Protocols

The next three protocols are bidirectional protocols that belong to a class called sliding window protocols.

<b>A One-Bit Sliding Window Protocol(SWP)</b>	1- assign variable 2- define frame 3- accept frame
<b>A Protocol Using Go Back N protocol</b>	Discarding & Buffering
<b>A Protocol Using Selective Repeat (SRP)</b>	accept and buffer delay and effected frames without ACK

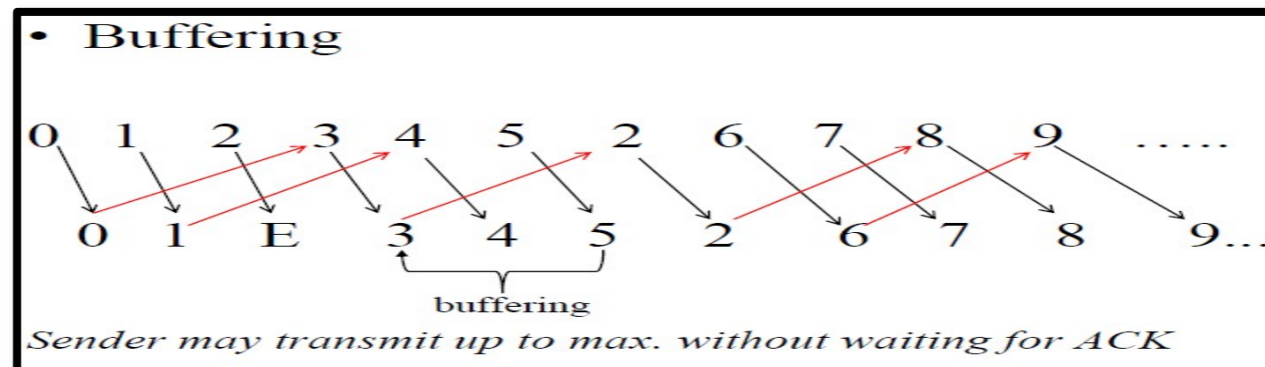
## Go Back N Protocol

If there is one frame  $k$  missing, the receiver simply discards all subsequent frames  $k+1, k+2, \dots$ , sending no acknowledgments. So, the sender will retransmit frames from  $k$  onwards. This can be a waste of bandwidth.



## Selective repeat Protocol SRP

Another strategy is to re-send only the ones that are actually lost or damaged. The receiver buffers all the frames after the lost one. When the sender finally noticed the problem (e.g. no ack for the lost frame is received within time-out limit), the sender retransmits the frame in question.



## PPP – Point to Point Protocol

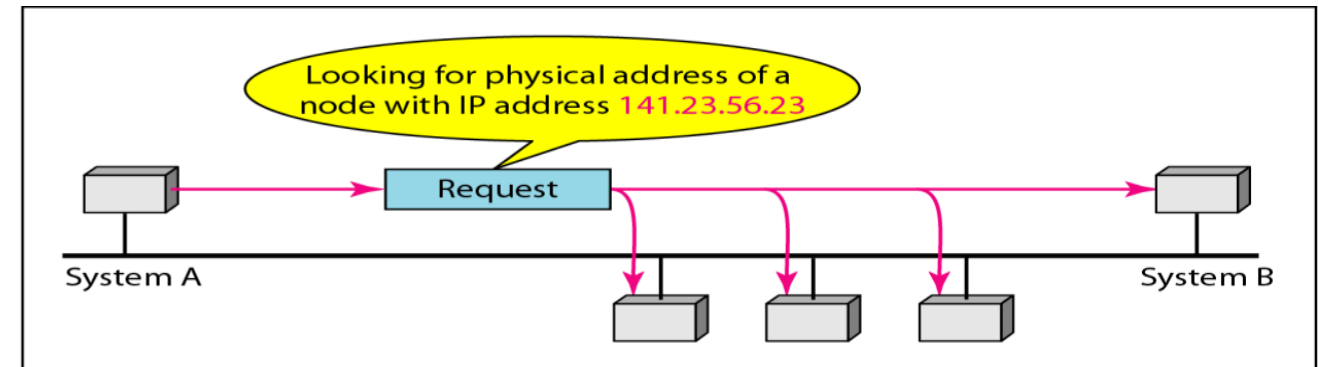
- Carry network data of **any** network layer protocol at **the same time**
- Error detection (**no** correction)
- has a very simple mechanism for **error control**( A CRC field is used to **detect** errors )
- Does **not provide** flow control
- Connection life, signal link, negotiator

## Address Resolution Protocol (ARP)

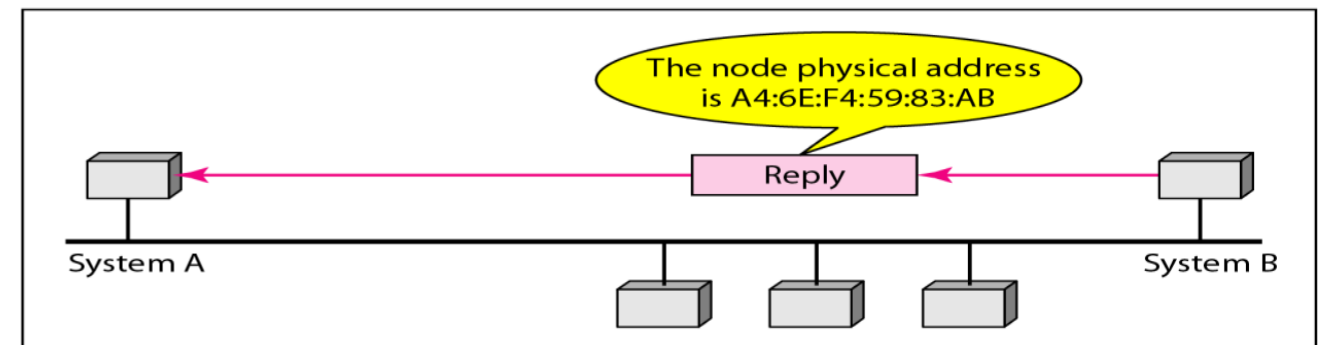
The delivery of a packet to a host or a router requires two levels of addressing: **logical** and **physical**.

- ARP Maps IP addresses to MAC addresses
- ARP **Request** is a broadcast, but ARP **reply** is Unicast.
- **ARP tables** contain the MAC and IP addresses of other devices on the network

### ARP operation



a. ARP request is broadcast



b. ARP reply is unicast

## Layer 2 Tunneling Protocol (L2TP)

- Is an **extension** of the Point-to-Point Tunneling Protocol (PPTP).
- **Used by** an Internet service provider (ISP) to enable the operation of a **virtual private network (VPN)** over the Internet.
- The goal of a Virtual Private Network (VPN) is to **provide private communications within the public Internet Infrastructure**

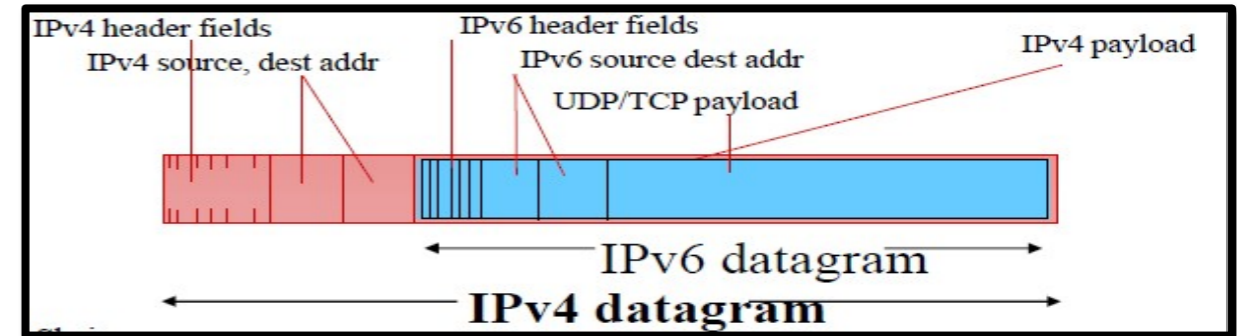
### Why is there a need for VPN?

- **Internet has insufficient security mechanisms**
- IP packets are not authenticated or encrypted
- Users with access to network can read content of IP traffic

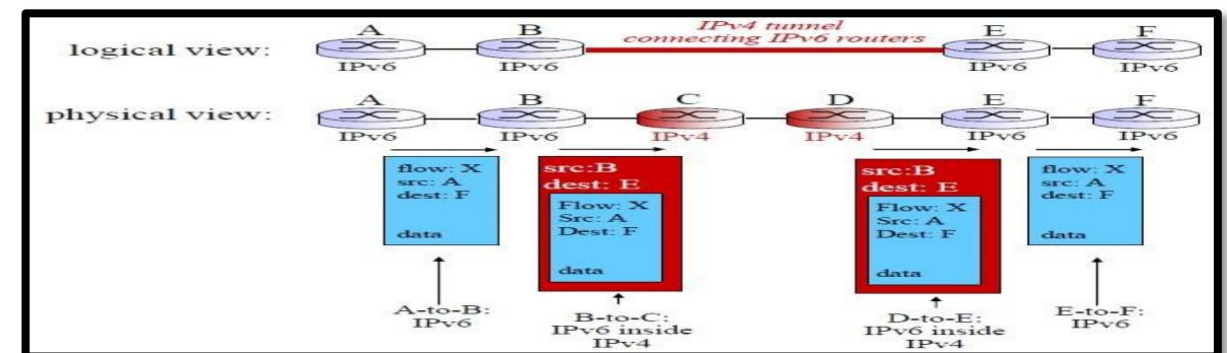
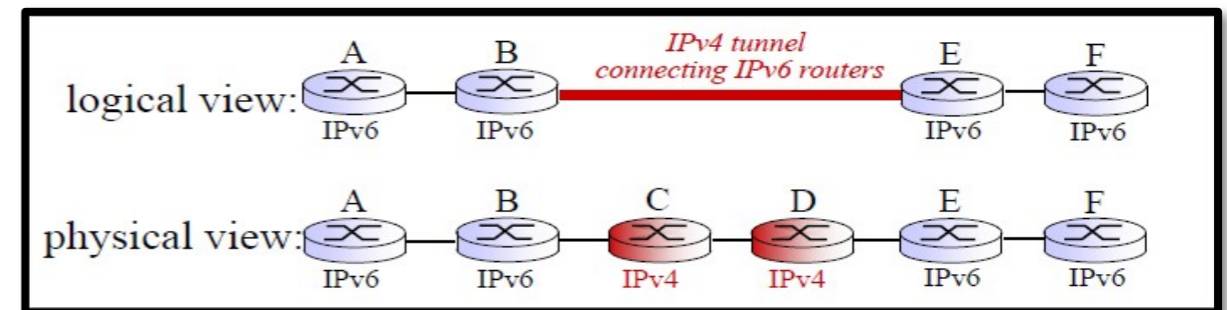
### Transition from IPv4 to IPv6

- Not all routers can be upgraded simultaneously
- How will network operate with mixed IPv4 and IPv6 routers?

*Answer: this can be done by Tunneling: IPv6 datagram carried as payload in IPv4 datagram among IPv4 routers*



## Tunneling



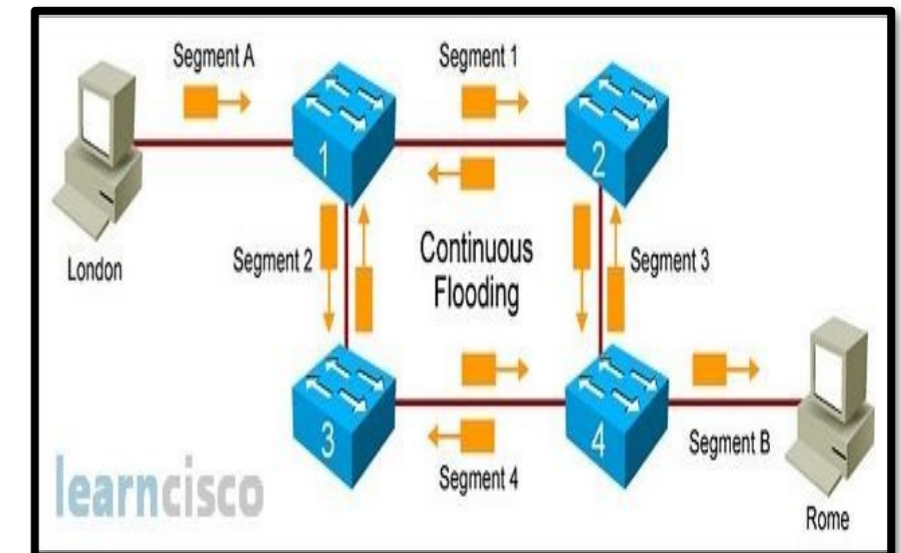
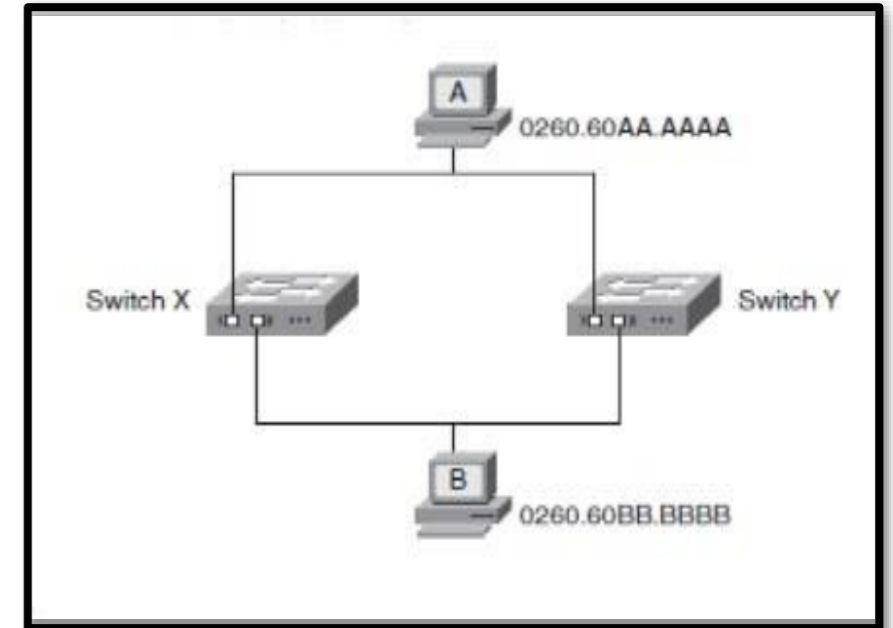
## Switching Loops

**Redundancy** in a network, such as that shown in Figure below, is **desirable** so that communication can still take place if a link or device fails. **For example**, if switch X in this figure stopped functioning, devices A and B could still communicate through switch Y. However, in a switched network, **redundancy can cause problems which is called switching loop**.

When a switching loop is introduced into the network, a destructive **broadcast storm** will develop within seconds. *There are three types of problem occur due to switch looping, these are:*

1. **Broadcast storm** occurs if a broadcast frame is sent on the network.
2. Devices can **receive multiple copies of the same frame** in redundant topologies.
3. The **MAC address table can change rapidly** and contain wrong information.

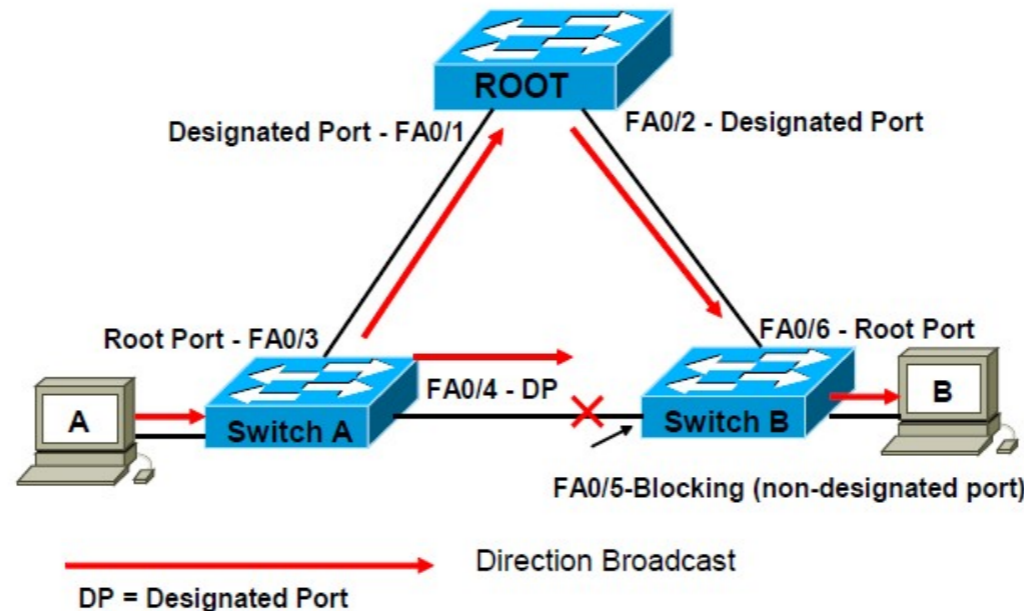
To overcome these problems, you must have a way to logically disable part of the redundant network for regular traffic while maintaining redundancy for the case when an error occurs. Spanning Tree Protocol (STP) does just that.



## Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) was developed to prevent the broadcast storms caused by switching loops. Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on **bridges and switches**. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network.

### Final STP Topology



## Media Access control Protocols

There are three broad classes of MAC protocols, these are:

### ***1.Channel Partitioning (Multiplexing)***

- divide channel into smaller “pieces” (time slots-TDMA, frequency-FDMA, code- CDMA)
- allocate piece to node for exclusive use

### ***2.Random Access (Contention Based)***

- channel not divided, allow collisions
- “recover” from collisions (CSMA/CD)

### ***3.Taking Turns (Controlled Based)***

- nodes take turns, but nodes with more to send can take longer turns (ex. Polling, Token Passing)

## Access Method: CSMA/CD

- Whenever multiple users have unregulated access to a single line, there is a danger of **signals overlapping and destroying each other**. Such overlaps, which turn the signals into unusable noise, are called **collisions**.
- **As traffic increases on a multiple access link, so do collisions. A LAN therefore needs a mechanism to coordinate traffic, minimize the number of collisions that occur, and maximize the number of frames that are delivered successfully.**

- The access mechanism used in an Ethernet is called *carrier sense multiple access with collision detection (CSMA/CD)*, standardized in IEEE 802.3).
- CSMA/CD is the result of an evolution from multiple access (**MA**) to carrier sense multiple access (**CSMA**), and finally, to carrier sense multiple access with collision detection (CSMA/CD).

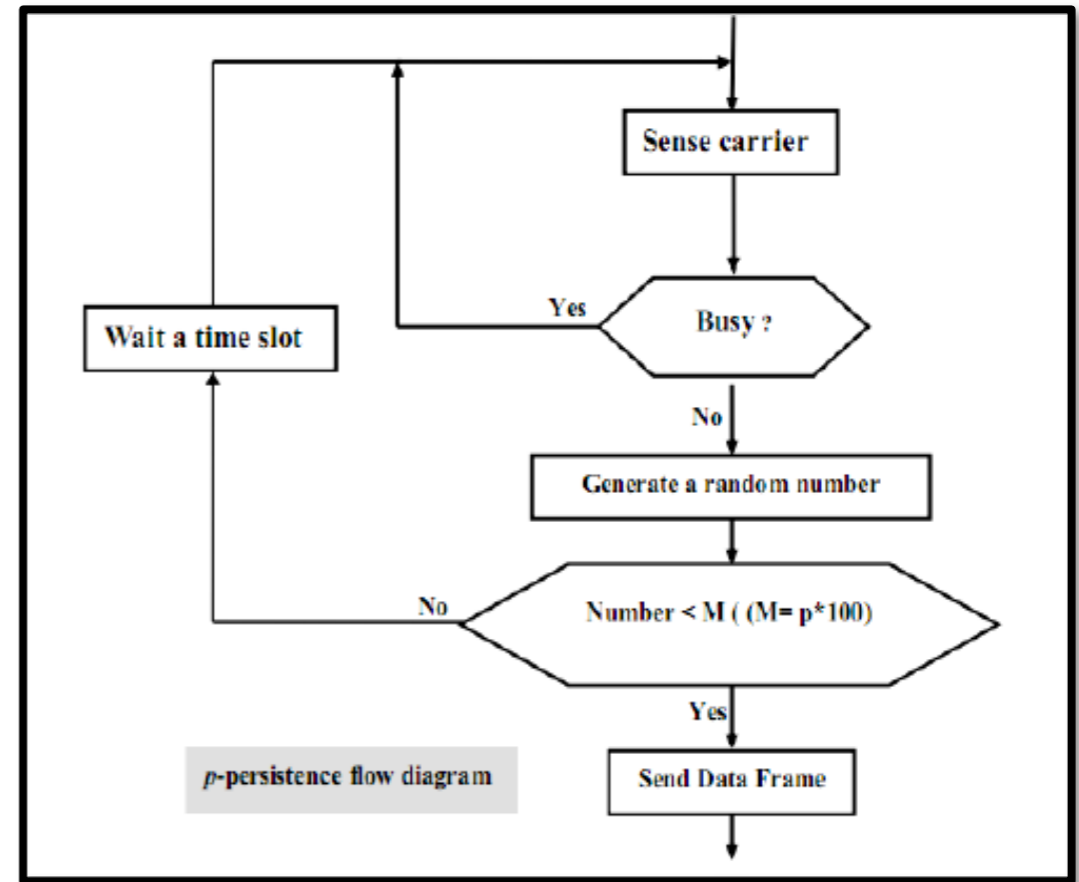
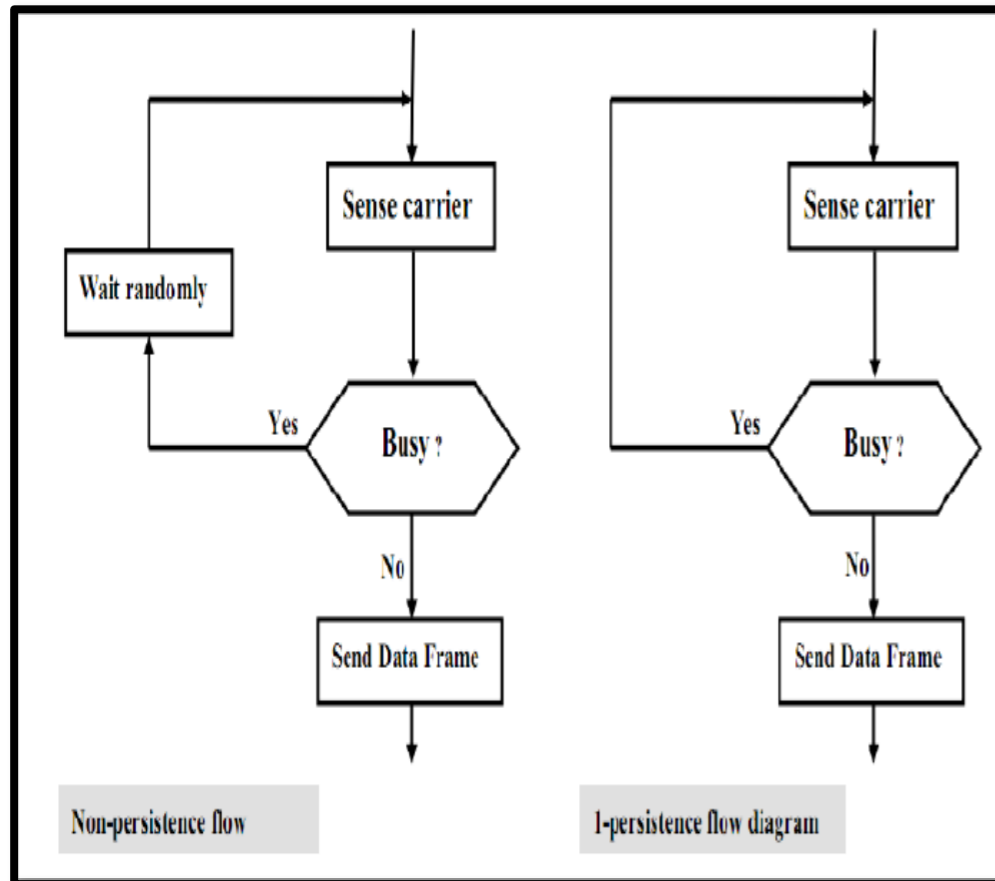
### Q: How CSMA/CD Algorithm works ?

1. NIC **receives datagram from network layer**, creates frame
2. If NIC senses **channel idle**, **starts frame transmission**. If NIC senses **channel busy**, **waits until channel idle**, then transmits.
3. If NIC detects another transmission while transmitting, aborts and sends jam signal
4. After aborting, NIC enters binary (exponential) backoff.

**Carrier Sense:** when a station in an Ethernet network has data to transmit ,it first see the network if it is use by other stations this is carrier sense. under three case of persistence strategy

<b>Non-persistence</b>	senses the line if it is idle it sends immediately if the line busy ,it waits a <b>random time</b> then sense the line again this method reduce the chance of collision but it also reduced network efficiency.
<b>1-persistence</b>	After the station finds the line idle it sends its data immediately (with probability 1) this method increases the chance of collision.
<b>p-persistence</b>	<b>After the station finds the line idle it may transmit or no.</b> here the probability of sending is defined by P and probability of refusing is (1-P) for example if $p=0.3$ then station sends with 30% of the time and refusing 70% of the time . The station generates a <b>random number</b> between 1 and 100 if the number generated is less than 30 the station sends its data else it waits one slot time before sensing the medium again this method reduces the chance of collision and increasing network efficiency.

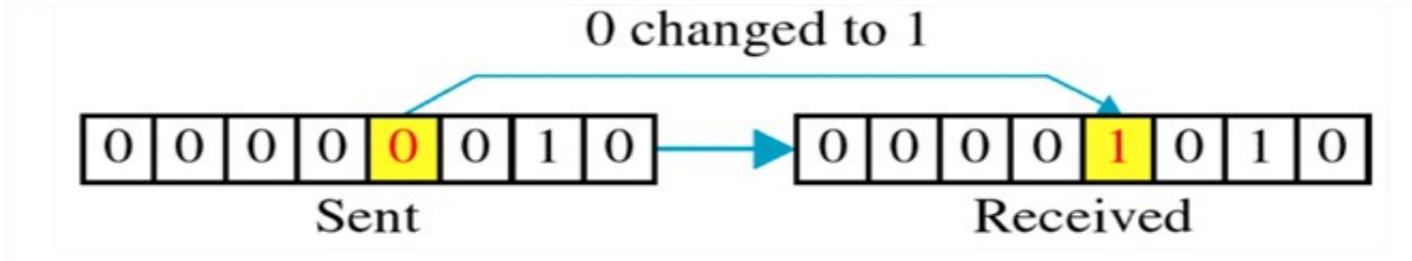
**Jam signal :** when system detected a collision it immediately stop transmitting data and starts sending this signal any system received packet must discard this packet and should not attempt to transmit any data until network has cleared.



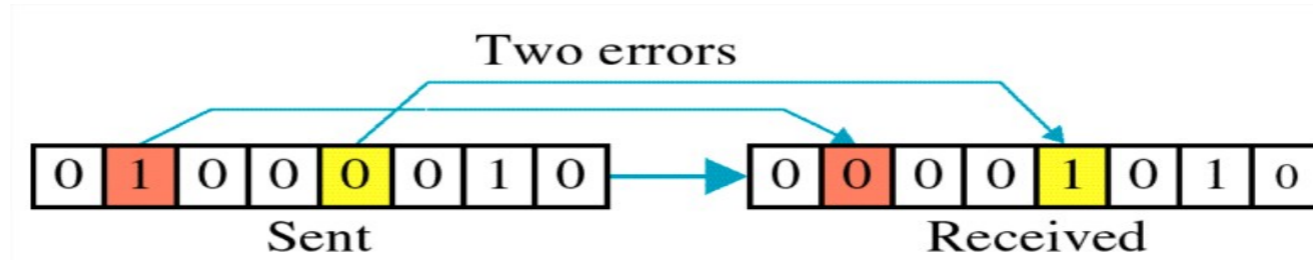
## Types of Errors

There are **three types of error** these are:

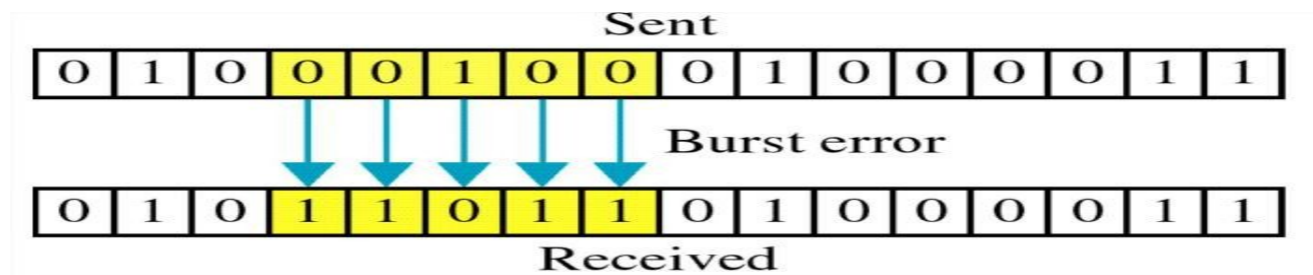
### 1. Single bit error



### 2. Multiple bit error

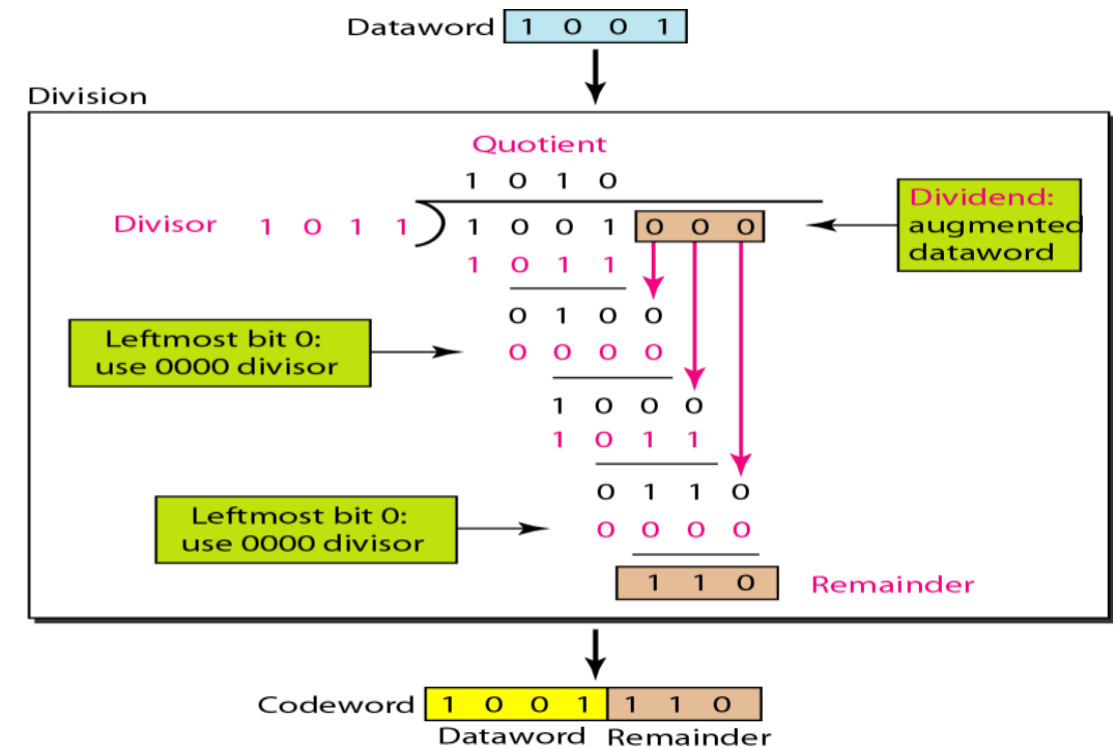
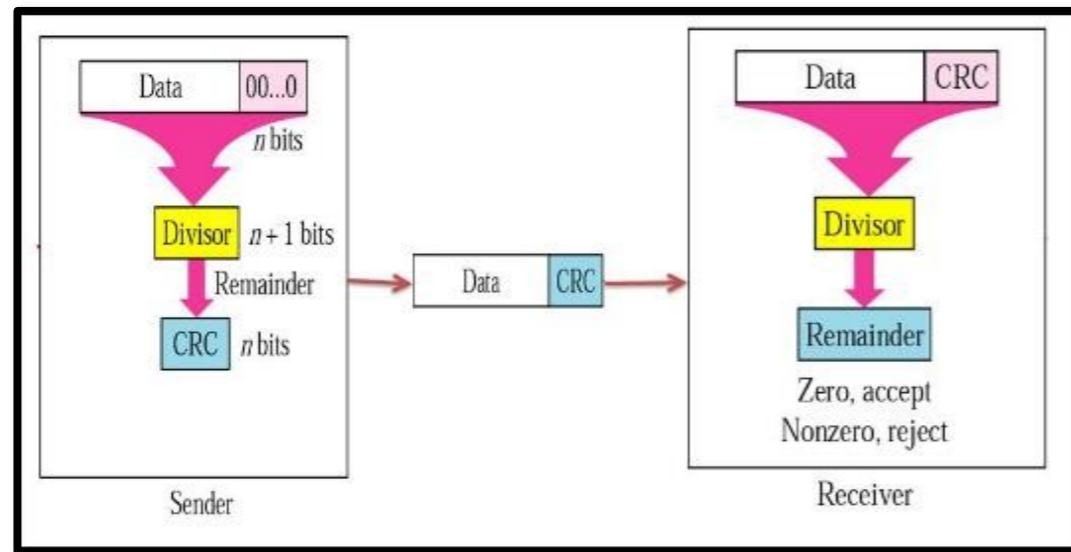


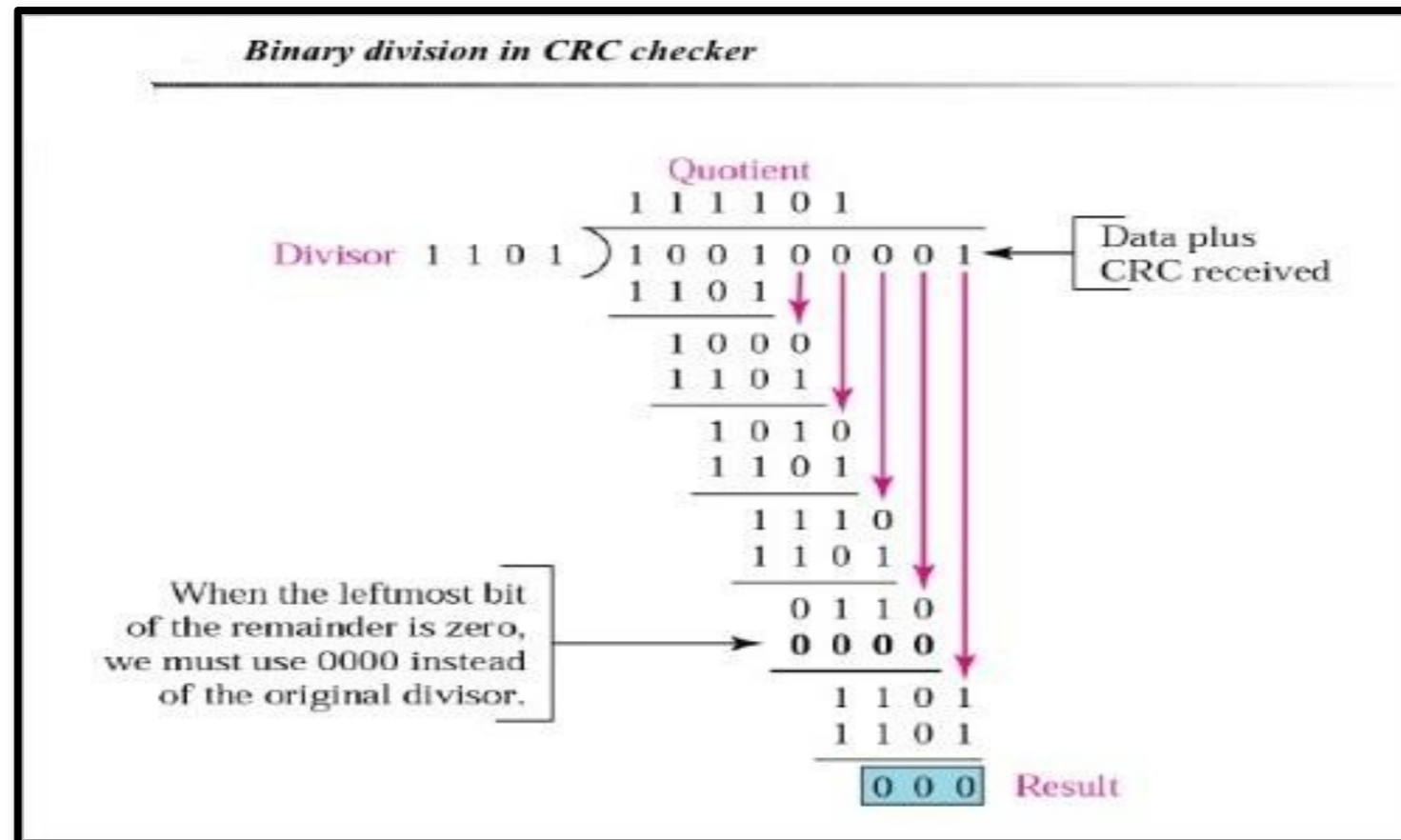
3. **Burst error:** means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



## Cyclical Redundancy Check (CRC)

The *most powerful redundancy technique*, unlike the VRC and LRC, CRC is based on binary division.

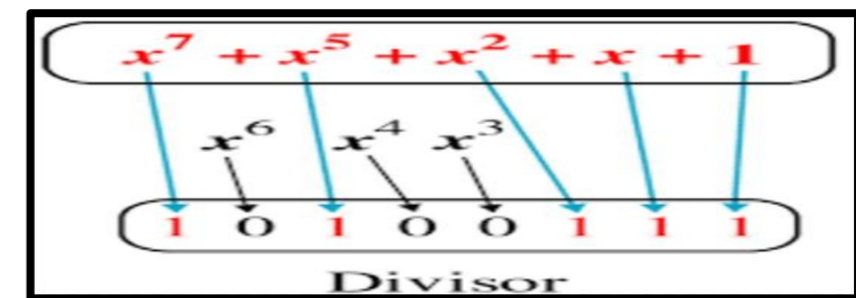




## Polynomial Calculation

To calculate the divisor we can use the polynomial as shown below:

- The polynomial **should not be divisible by X.**
- The polynomial **should be divisible by X+1.**



## Checksum Technique

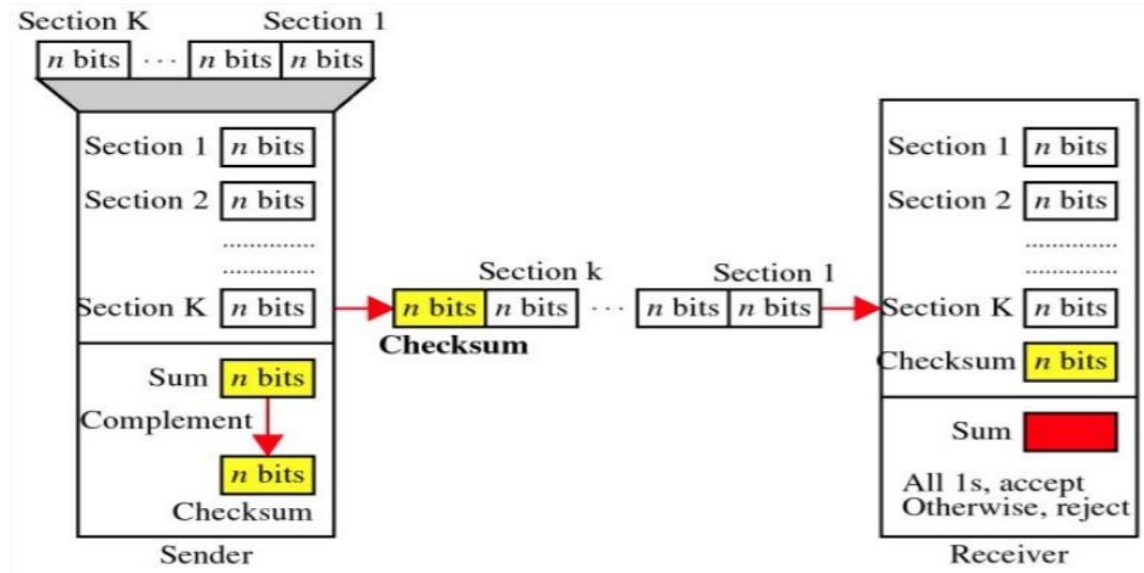
The error detection method used by the *higher layer protocols*. Like other methods, it depends on the concept of redundancy.

- **At the Sender Side**

1. The unit is **divided** in to **k** sections, each of **n bits**.
2. All sections are added using **one's complement** to get the sum in such a way that the total is also **n bits** long.
3. The **sum is then complemented** and **becomes the checksum**.
4. The **checksum** is sent with the data.

- **At the Receiver Side**

1. The received data is divided in to **k** sections, each of **n bits**.
2. All sections are **added using one's complement** to get the sum in such a way that the total is also **n bits** long.
3. The **sum is then complemented**.
4. If the **result is zero**, the **data are accepted**, otherwise they are **rejected**.



### Example:

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

Now suppose the receiver receives the pattern sent 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.

Now suppose there is a burst error of length 5 that affects 4 bits.

10101111 11111001 00011101

When the receiver adds the three sections, it gets

	10101111
	11111001
	00011101
Partial Sum	1 11000101
Carry	1
Sum	11000110
Complement	00111001 the pattern is corrupted.