

Computer Networks Protocols

Lecture No.2: Physical & Data link layer

PHYSICAL LAYER

SONET\SDH Networks

- SONET\SDH, that is used as a **transport network to carry loads from other WANs.**

SDH(Synchronous Digital Hierarchy)	SONET(Synchronous Optical Network)
• Is European standard network. • Is a standard developed by ITU-T. • Define a hierarchy of signals called synchronous transfer modules (STMs)	• Is American standard network. • Is a standard developed by ANSI for fiber-optic networks. • Define a hierarchy of signals called synchronous transport signals (STs) where each STS level (STS-1 to STS-192) supports a certain data rate.

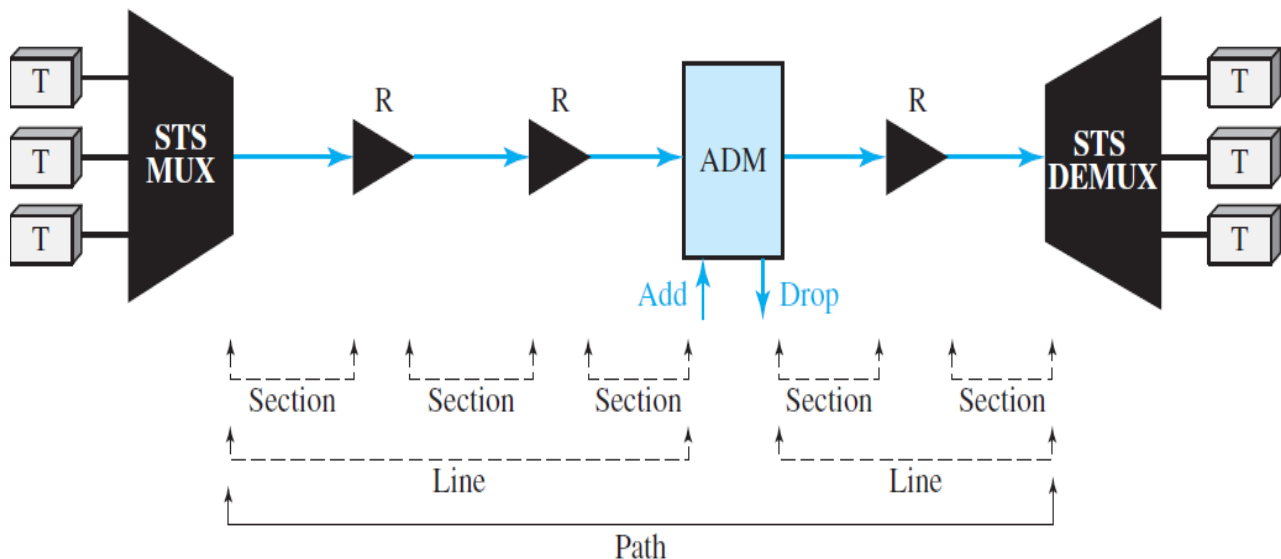
ADM: Add/drop multiplexer

R: Regenerator

STS MUX: Synchronous transport signal multiplexer

T: Terminal

STS DEMUX: Synchronous transport signal demultiplexer



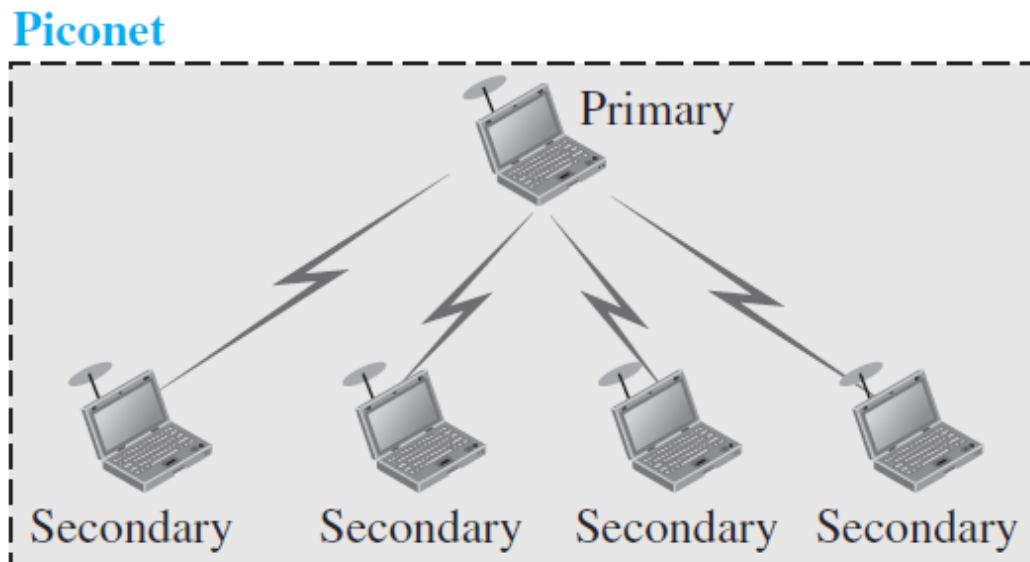
BLUETOOTH

- **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.

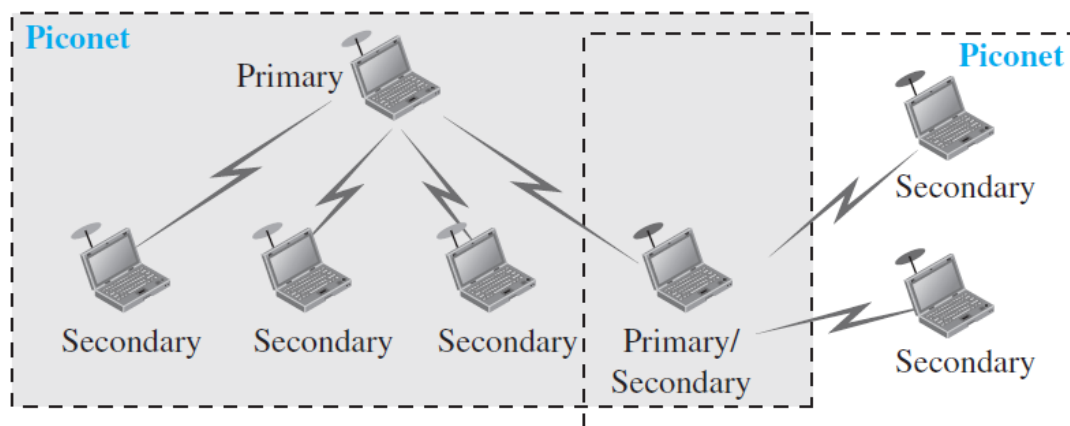
Architecture of Bluetooth:

- 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



Data Link Layer

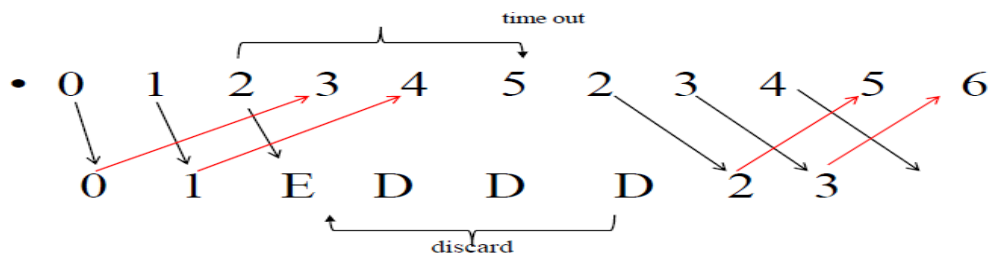
1.Elementary Data Link Protocols

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

2. Sliding Window Protocols

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

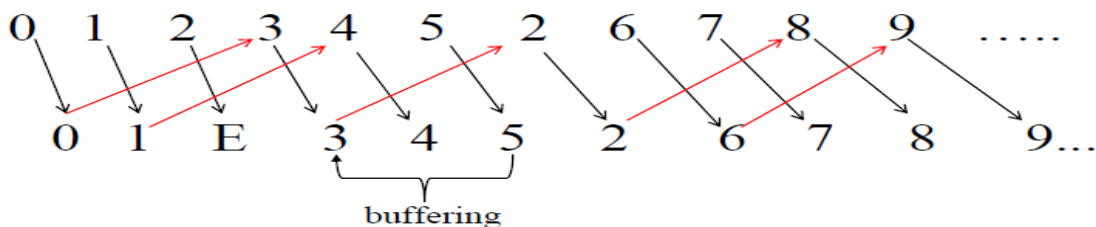
Go Back N Protocol



Discarding operation

Selective repeat Protocol SRP

• Buffering



Sender may transmit up to max. without waiting for ACK

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)

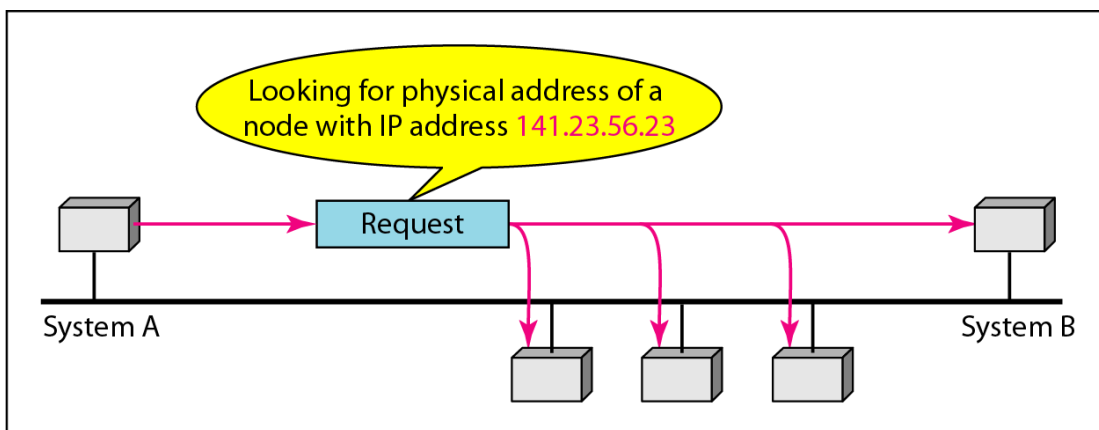
•The delivery of a packet to a host or a router requires two levels of addressing: logical and physical.

–ARP Maps IP addresses to MAC addresses

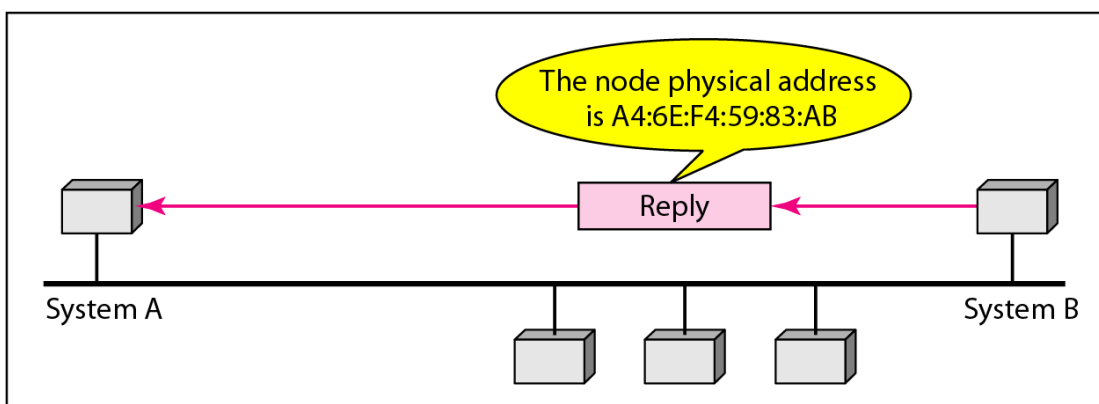
–ARP **Request** is a broadcast but ARP **reply** is Unicast .

–**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.
- VPN The goal of a Virtual Private Network (VPN) is to **provide private communications within the public Internet Infrastructure**

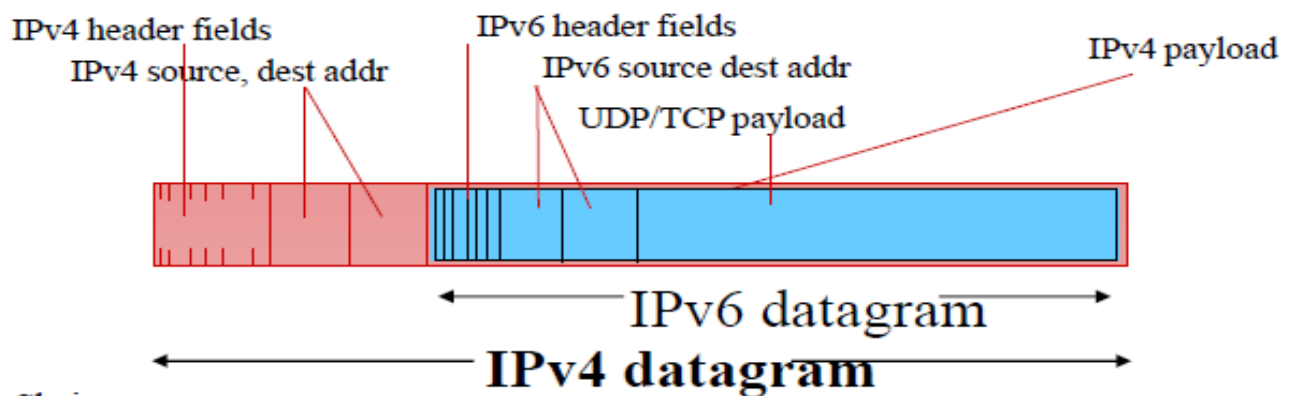
Why is there a need for VPN?

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

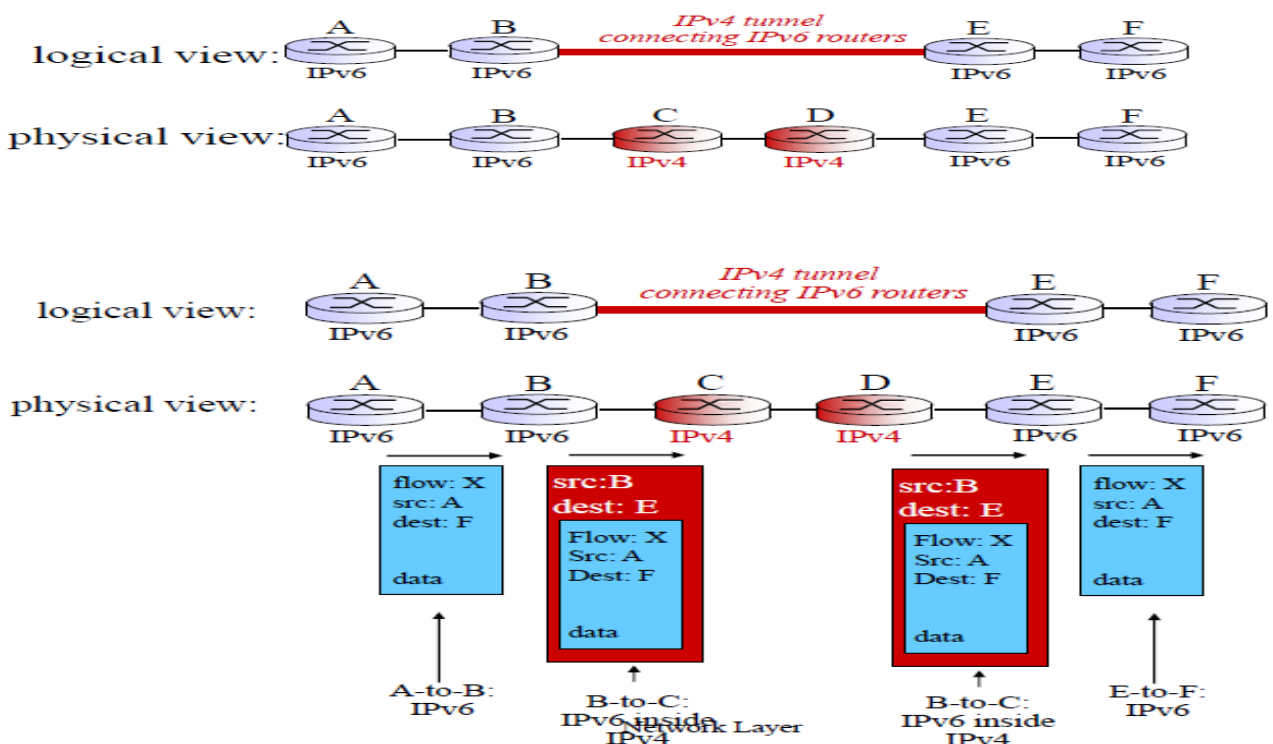
Transition from IPv4 to IPv6

not all routers can be upgraded simultaneously

tunneling: IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers



Tunneling

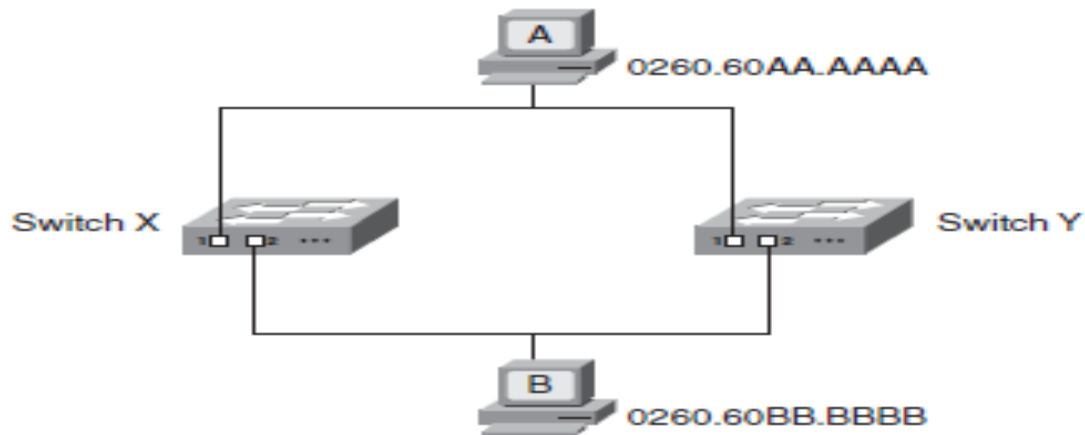


Spanning Tree Protocol(STP)

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.

Redundancy in a Switched Network Can Cause Problems



There are 3 problems:

1. occurs if a broadcast frame is sent on the network(*broadcast storm*).
2. that can occur in redundant topologies is that devices can receive multiple copies of the same frame.
3. that can occur in a redundant situation is within the switch itself—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. STP does just that.

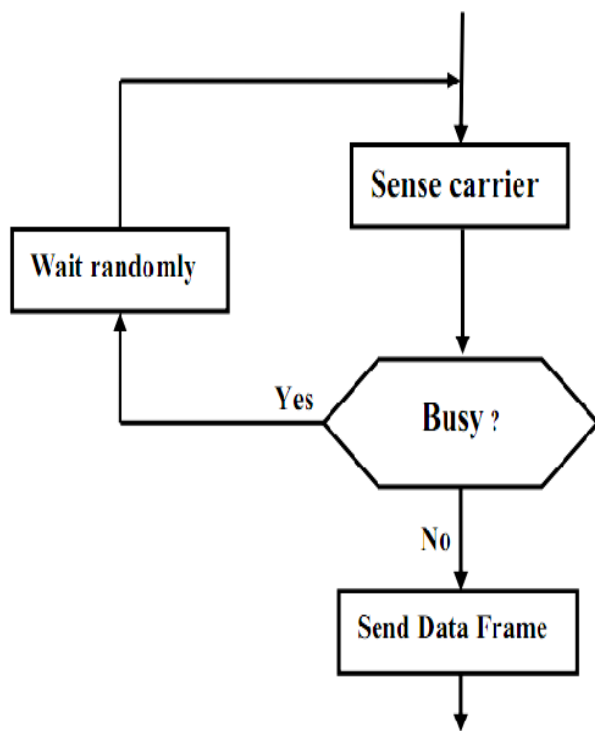
Access Method: CSMA/CD

- 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).

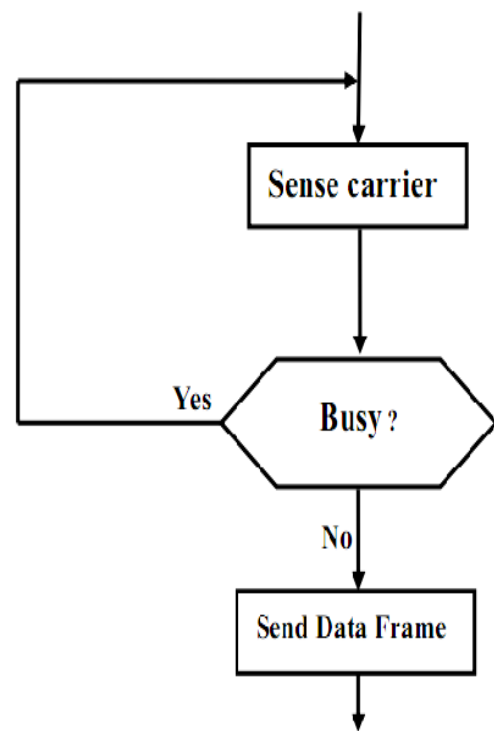
•**Carrier Sense**: when a station in an Ethernet network has data to transmit ,it first see the network if it is use by other stations this is carrier sense .**under three case of persistence strategy**

Non-persistence	senses the line if it is idle it sends immediately if the line busy ,it waits a random time then sense the line again this method reduce the chance of collision but it also reduced network efficiency.
1-persistence	after the station finds the line idle it sends its data immediately (with probability 1) this method increase the chance of collision.
p-persistence	after the station finds the line idle it may transmit or no . 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 random number 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.

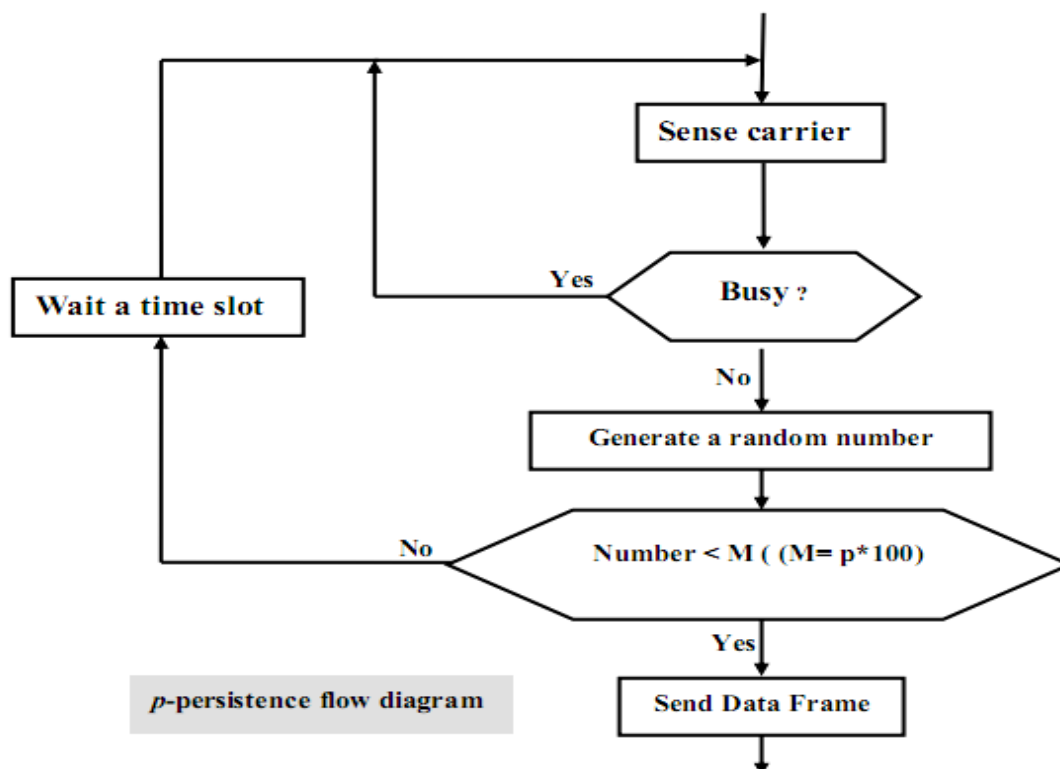
.Jam signal : when system detected a collision it immediately stop transmitting data and starts sending this signal any system received packet must discard this packet and should not attempt to transmit any data until network has cleared.



Non-persistence flow



1-persistence flow diagram



p -persistence flow diagram

Cyclical Redundancy Check (CRC)

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

Figure 10.7 CRC generator and checker

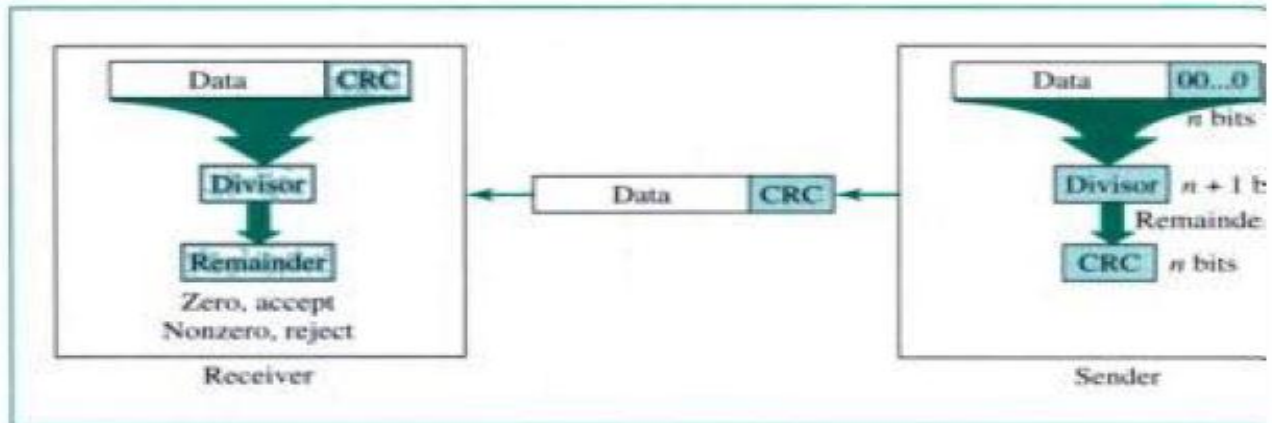


Figure 10.8 Binary division in a CRC generator

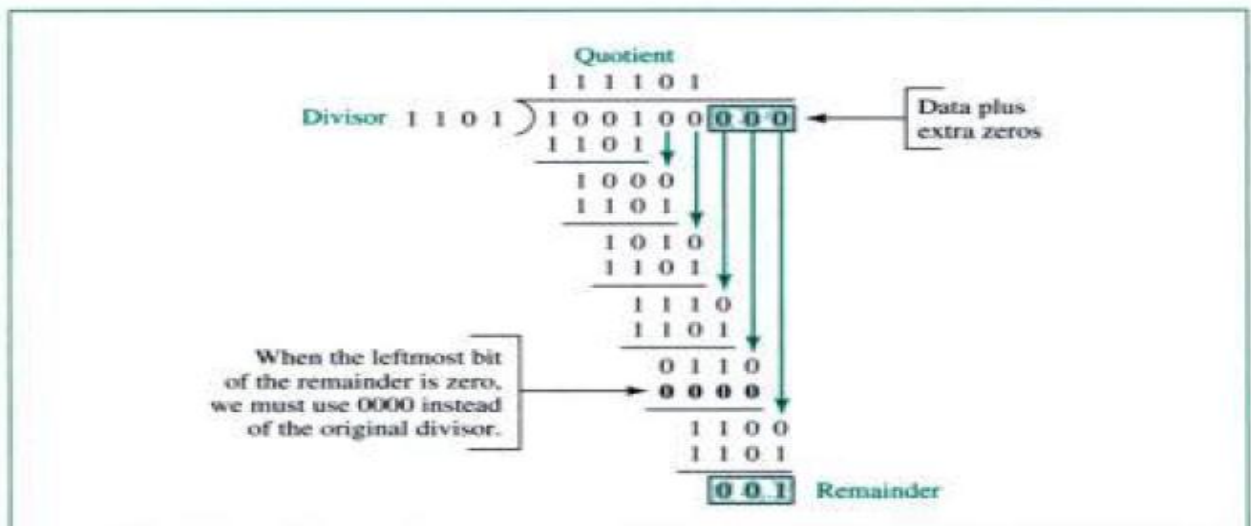
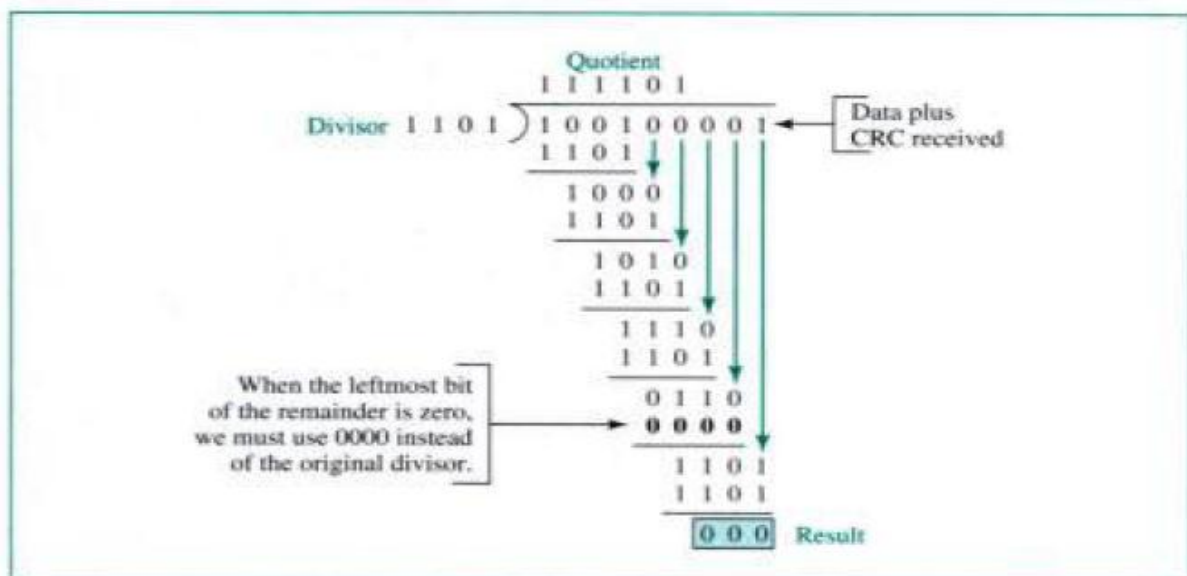
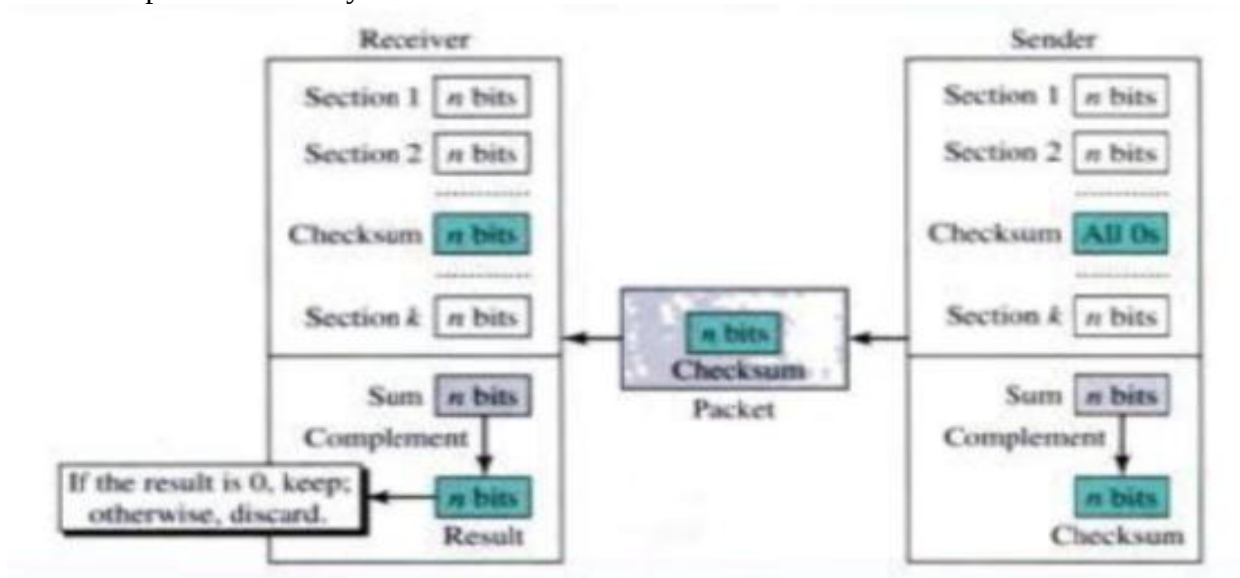


Figure 10.9 Binary division in CRC checker



Checksum

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



The sender follows these steps:

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

Example

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

1010111111111001 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.

Example

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

1010111111111001 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.

Example

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.

Example

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	
Result	1 11000101	
Carry	1	
Sum	11000110	
Complement	00111001	means that the pattern is corrupted.