Network Protocol
Physical and Data link layer

ISLAMIC UNIVERSITY COLLEGE
Computer Technical Engineering Department

Computer Networks Protocols

Lecture One: **Introduction**

Description: General definition of Network terminology

وصف المحاظرة: تعاريف عامة لمصطلحات الشبكات.

- **What is the Network Architecture?**

  A ***set of layers and protocols*** is called the network architecture.

- **The Protocol is form in Hierarchies سلم (layered) manners, WHY?**

  Networks are organized as layers to ***reduce design complexity***.

  And Each layer offers services to the higher layers.

- **Each protocol provides services, what they are?**

  Connection Oriented

  Connectionless.

- **How do the adjacent layers communicate?**

  Between adjacent layers is an interface.

  Defines which primitives and services the lower layer will offer to the upper layer.

- **What is the Primitives?**

  operations such as request, indicate, response, confirm.

- **Design Issues for the Layers (functions) الاسباب الرئسية وراء تصميم الطبقات**

  Mechanism for connection establishment

  Rules for data transfer

  Error control

  Fast sender swamping a slow receiver

  Routing in the case of multiple paths

Network Protocols بروتوكول الشبكات

- **What is the meaning of the Protocol:**

  It is a format order of messages sent and received among the devices and action taken on msgs transmission receipt.

- **What are the Protocol process ماهي العمليات التي يقوم بها البرتوكول:**

  - The format or structure of the message
  - The process by which networking devices share information about pathways with other networks
  - How and when error and system messages are passed between devices
  - The setup and termination of data transfer sessions

- **Layering in Networked Computing ماهي انواع انظمة الطبقات في شبكات الحاسوب**
  - OSI Model (open system interconnection)
  - TCP/IP Model

- **Why a layered model?لماذا استخدم نظام الطبقات**
  - Breaks down communication into smaller, simpler parts.
  - Easier to teach communication process.
  - Allows different hardware and software to work together.
  - Reduces complexity

- **What is the OSI model?**

  The Open Systems Interconnection is the model developed by the International Standards Organization. Study the OSI helps us understand how data gets from one user's computer to another.

  It helps to provide an organized structure for hardware and software developers.

- **Why use a reference model? لماذا الحاجة الى نظام موحد**
  - Serves as an outline of rules for how protocols can be used to allow communication between computers.
  - Each layer has its own function and provides support to other layers.

OSI Model

OSI Model	Protocols
Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP,POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	TCP, UDP
Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Benefits(Advantage)	Negative Aspect (disadvantage)
• Interconnection of different systems (open) • Not limited to a single vendor solution	• Systems might be less **secure** • Systems might be less **stable**

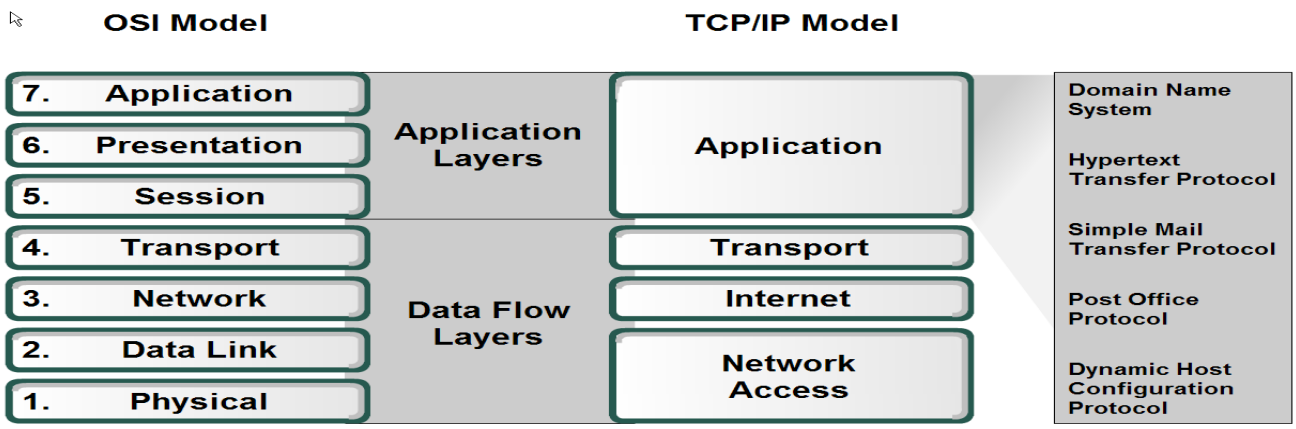
Layer	Main Topics
Physical Layer	• Transmission mediums (transmit bits over medium) • Encoding • Modulation • Repeaters • Hubs (multi-port repeater) • To provide mechanical and electrical specification
Data Link Layer	• Error detection and correction methods • Hop to hop delivery • Flow control • Frame format • IEEE LAN standards • Bridges & Switches (multi-port bridges) • physical addressing(MAC Address)
	• Inter-networking

Network Layer	• Controls the operation of the subnet. • Routing algorithms(Routing packets from source to destination) • Internet Protocol (IP) addressing (Logical addressing) • Routers
Transport Layer	• Connection-oriented and connectionless services • Provide reliable process to process message delivery & error recovery • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • Provides additional Quality of Service. • Port address • End-to-end flow control.
Session Layer	• Allows users on different machines to establish sessions (dialogue) between them. • managing dialogue control. • Token management. • Synchronization.
Presentation Layer	• Concerned with the syntax and semantics of the information. • Preserves the meaning of the information. • Data compression. • Data encryption.
Application Layer	• Provides protocols that are commonly needed. • To allow access to network resource • (FTP), (HTTP), (SMTP), (SNMP),(NFS),(Telnet)

SERVICES

Connection-Oriented	**Connectionless**
before data is sent, the service from the sending computer must **establish** a connection with the receiving computer.	data can be sent at any time by the service from the sending computer.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2. OSI model has a separate presentation layer	2. TCP/IP does not have a separate presentation layer
3. OSI is a general model.	3. TCP/IP model cannot be used in any other application.
4. Network layer of OSI model provide both connection oriented and connectionless service.	4. The Network layer in TCP/IP model provides connectionless service.
5. OSI model has a problem of fitting the protocols in the model	5. TCP/IP model does not fit any protocol
6. Protocols are hidden in OSI model and are easily replaced as the technology changes.	6. In TCP/IP replacing protocol is not easy.
7. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	7. In TCP/IP it is not clearly separated its services, interfaces and protocols.
8. It has 7 layers	8. It has 4 layers

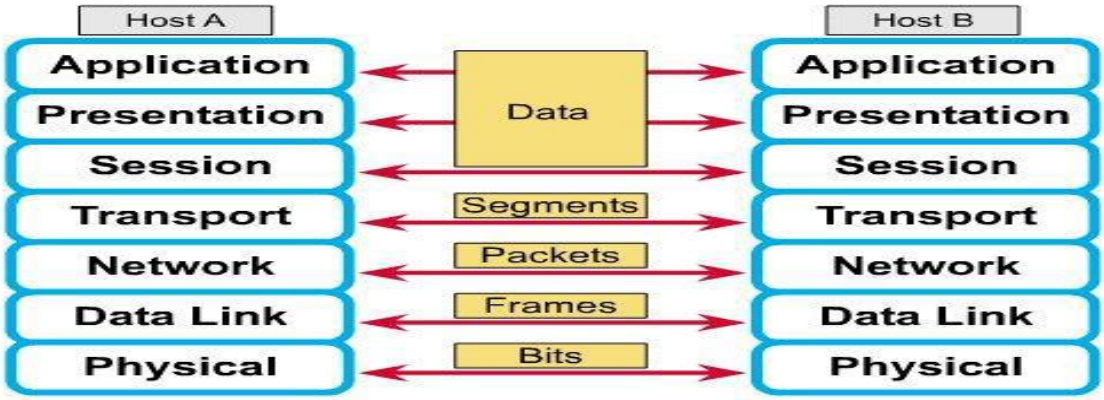


Data Encapsulation

•Each layer contains a **Protocol Data Unit (PDU)**

- PDU's are used for **peer-to-peer contact** between corresponding layers.

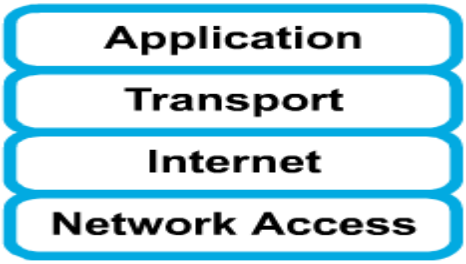
The Layer	Shape of data (PDU)
top three layers	Data
Transport layer	Segment
Network layer	packets
Data Link layer	frames
Physical layer	bits



4 layers of the TCP/IP model

•Layer 4: Application
•Layer 3: Transport
•Layer 2: Internet
•Layer 1: Network access

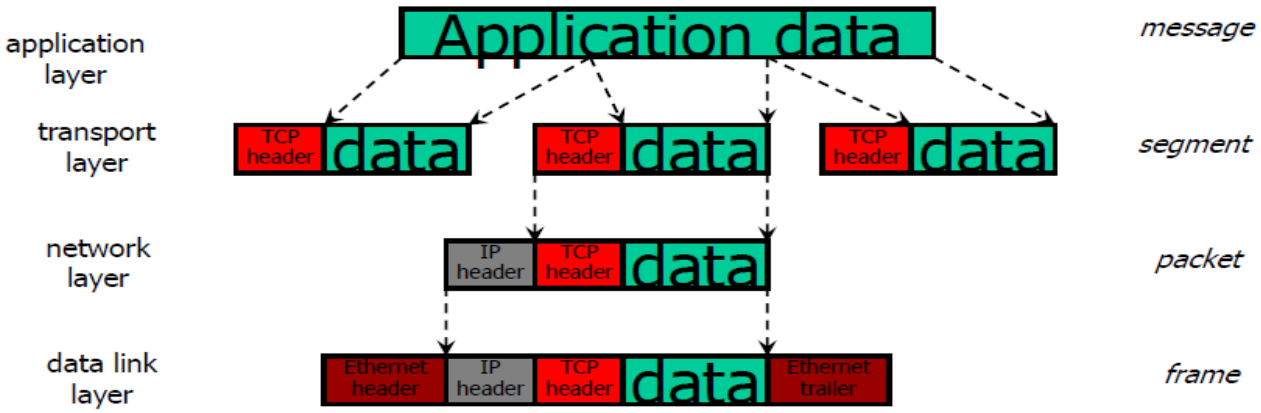
It is important to note that some of the layers in the TCP/IP model have the same name as layers in the OSI model. Do not confuse the layers of the two models.



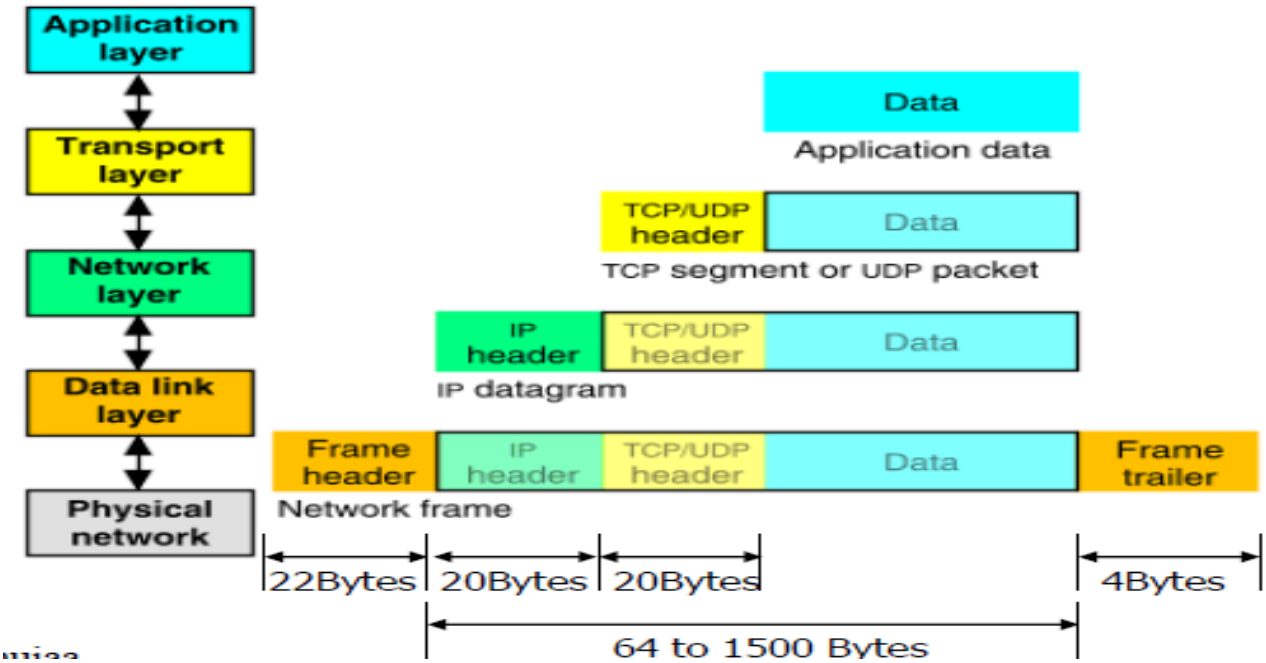
Data Encapsulation In TCP/IP

- Outgoing data is packaged and identified for **delivery** to the layers.
- PDU – Packet Data Unit – the "envelop" information attached to a packet at a particular TCP/IP protocol e.g. header and trailer
- Header (Identifies the protocol in use, the sender and intended recipient)
- Trailer (or packet trailer) (Provides data integrity checks for the payload)

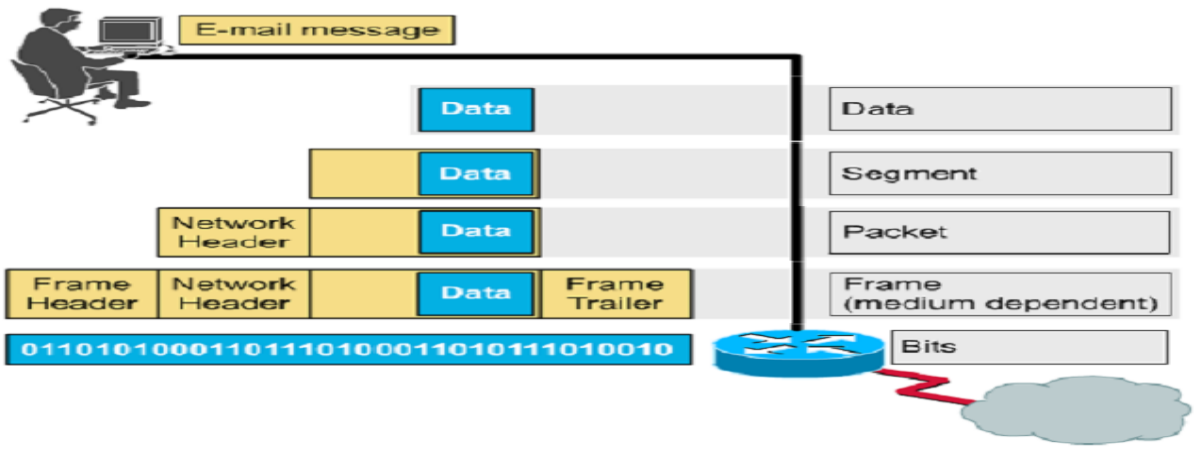
Data Formats



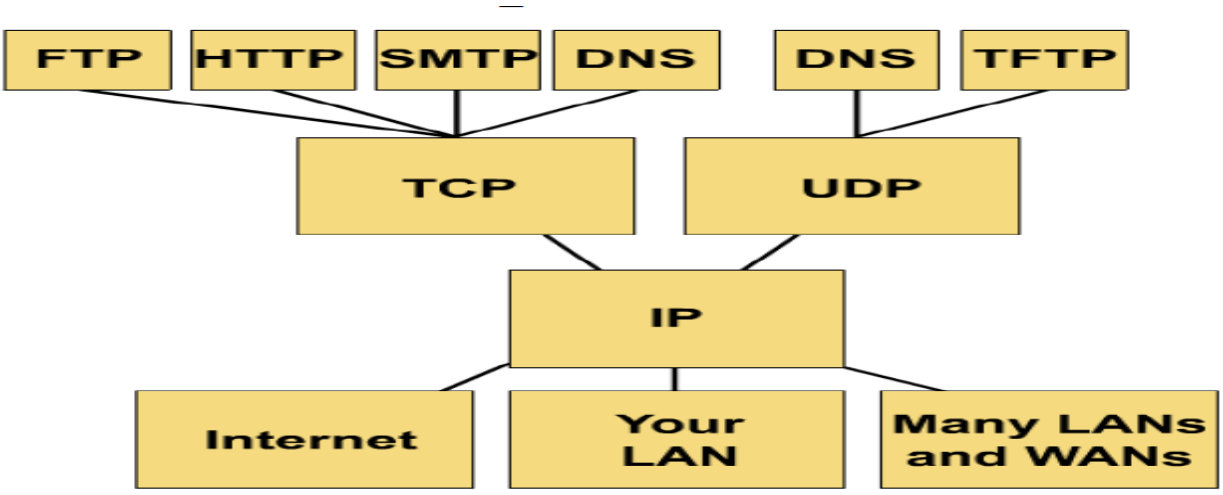
Encapsulation (TCP/IP)



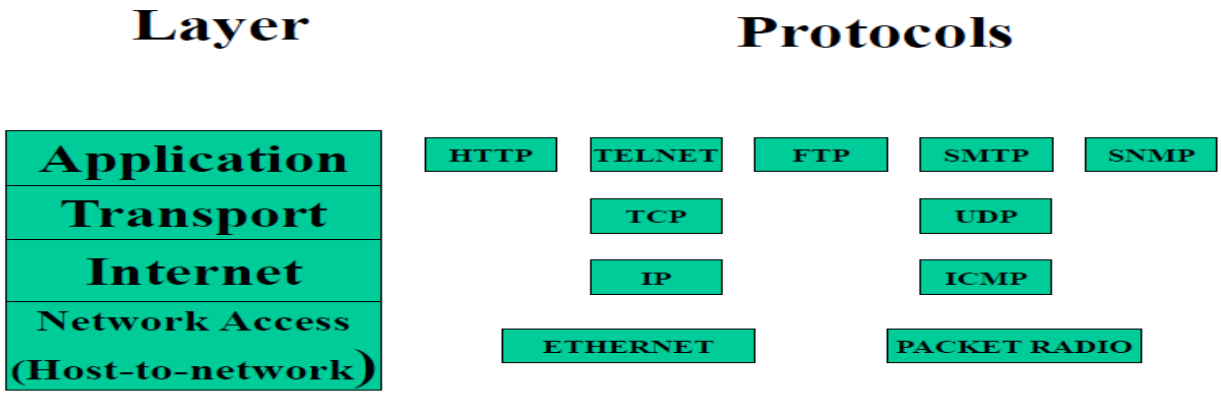
Encapsulation example: E-mail



What is the TCP/IP protocol stack?



TCP/IP Reference Model



What is a socket ?

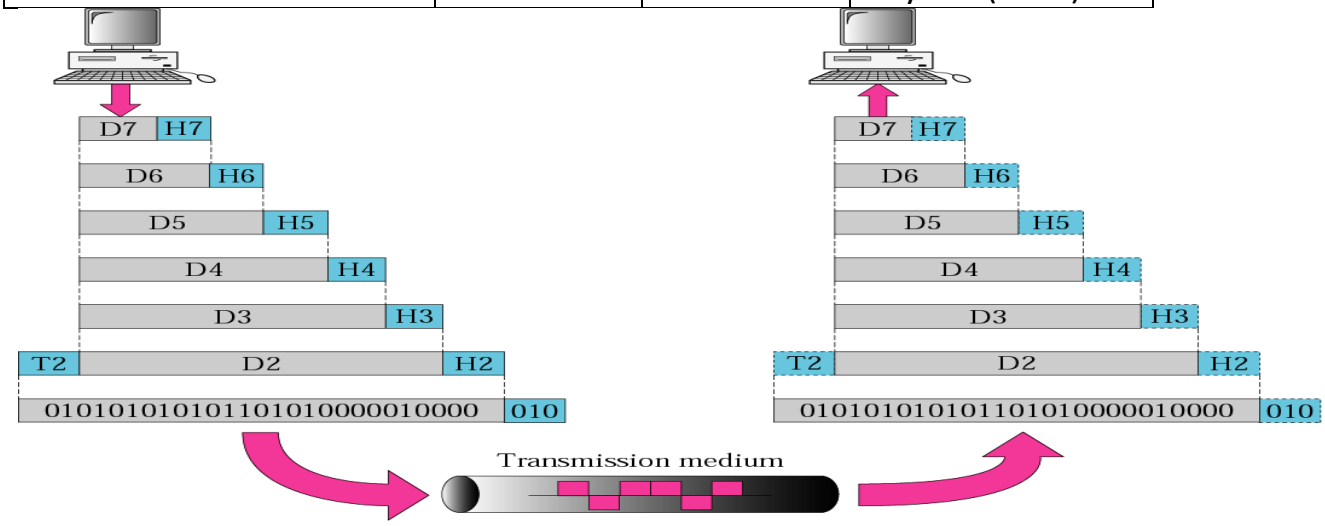
- An interface between application and network(each application create socket)
- Socket (Protocol family, type-of-communication, specific- protocol);
- The socket *type* dictates the style of communication

reliable vs. best effort

connection-oriented vs. connectionless

Q/Explain the delivery of data in Layered model?

Type of delivery	Layer	Shape of data	Type of addressing
End to End process	Transport	Segment	Port (socket)
Source To Destination	Network	Packet	Logical (IP)
Node to Node	Data Link	Frame	Physical(MAC)



Computer Networks Protocols

Lecture No.2: Physical and Data link layer

Prepared By: Mr. Karar Al-jawaheri

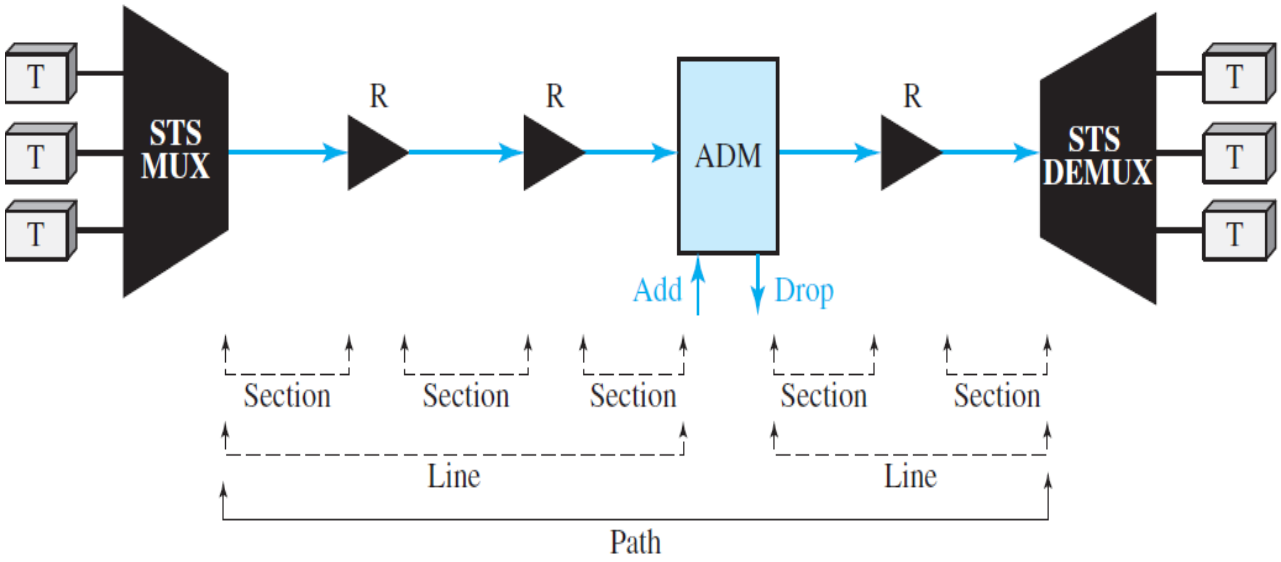
PHYSICAL LAYER

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 (**STSs**) where each STS level (STS-1 to STS-192) **supports a certain data rate**.

ADM: Add/drop multiplexer
STS MUX: Synchronous transport signal multiplexer
STS DEMUX: Synchronous transport signal demultiplexer
R: Regenerator
T: Terminal



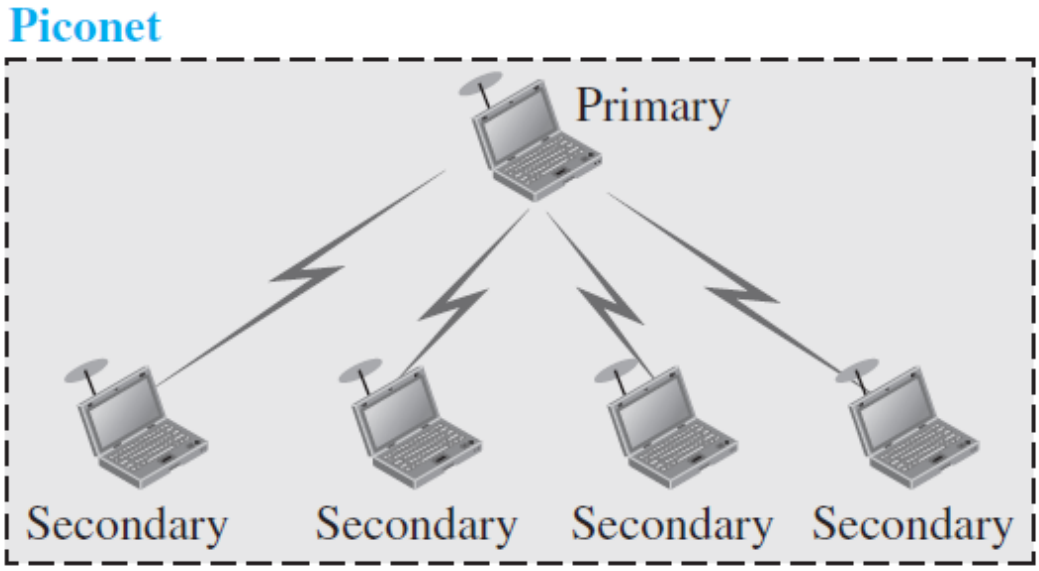
BLUETOOTH

- **Bluetooth is a wireless PAN 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.

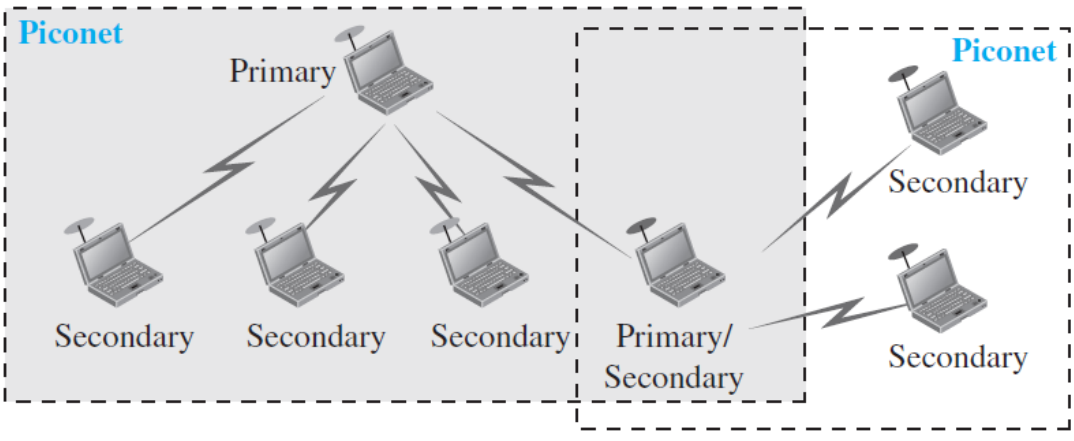
Architecture of Bluetooth:

- 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 7.*

Piconet Network



Scatternet Network



Data Link Layer

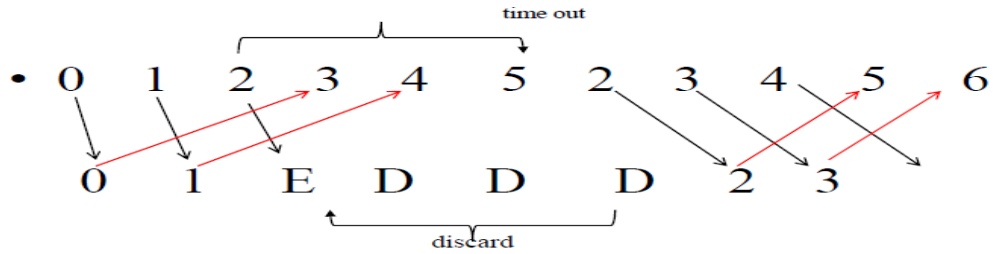
1.Elementary Data Link Protocols

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

2. Sliding Window Protocols (full duplex)

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

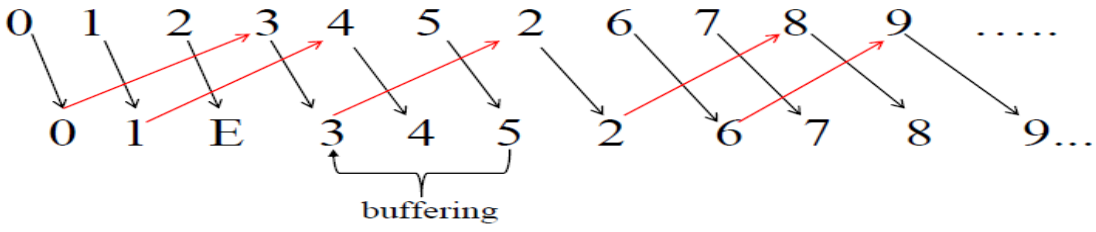
Go Back N Protocol



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)

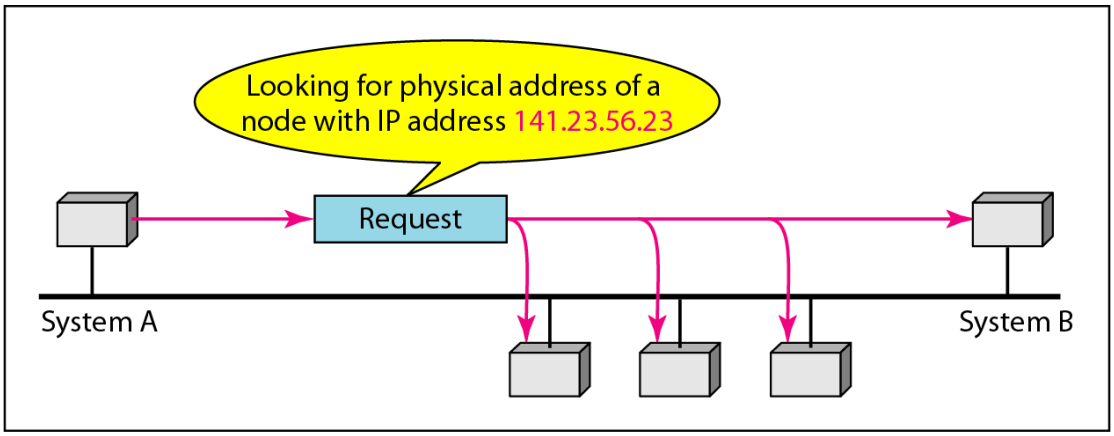
- The delivery of a packet to a host or a router requires two levels of addressing: logical and physical.

–ARP Maps IP addresses to MAC addresses → RARP

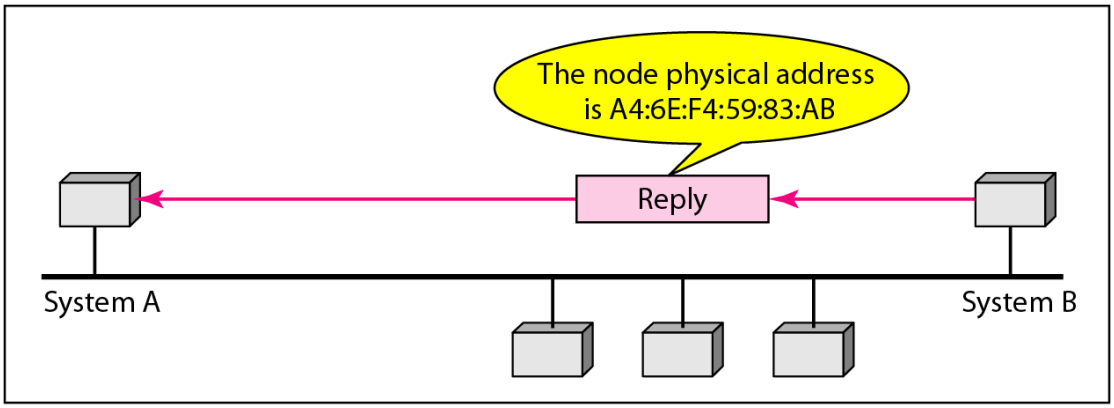
–ARP **Request** is a broadcast but ARP **reply** is Unicast .

–**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**

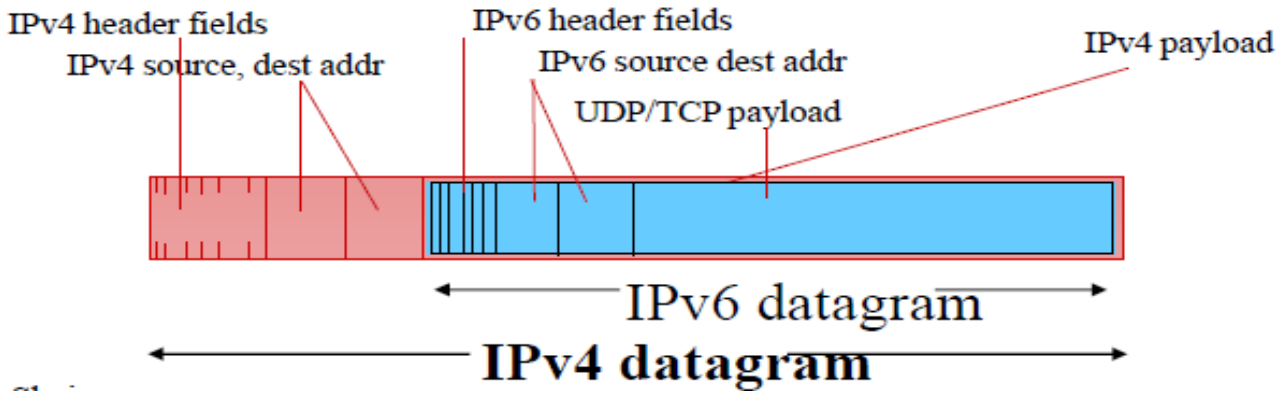
Why is there a need for VPN?

- **Internet has insufficient security mechanisms**
- IP4 packets are not authenticated or encrypted
- Users with access to network can read content of IP traffic

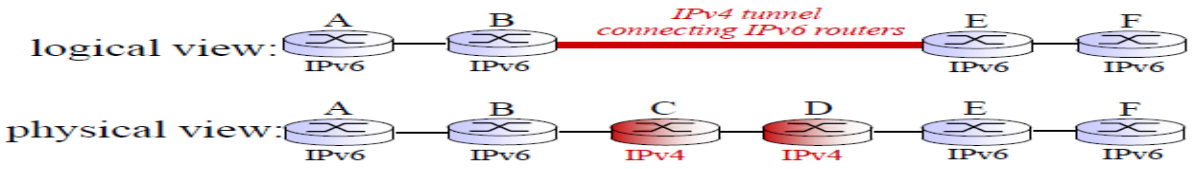
Transition from IPv4 to IPv6

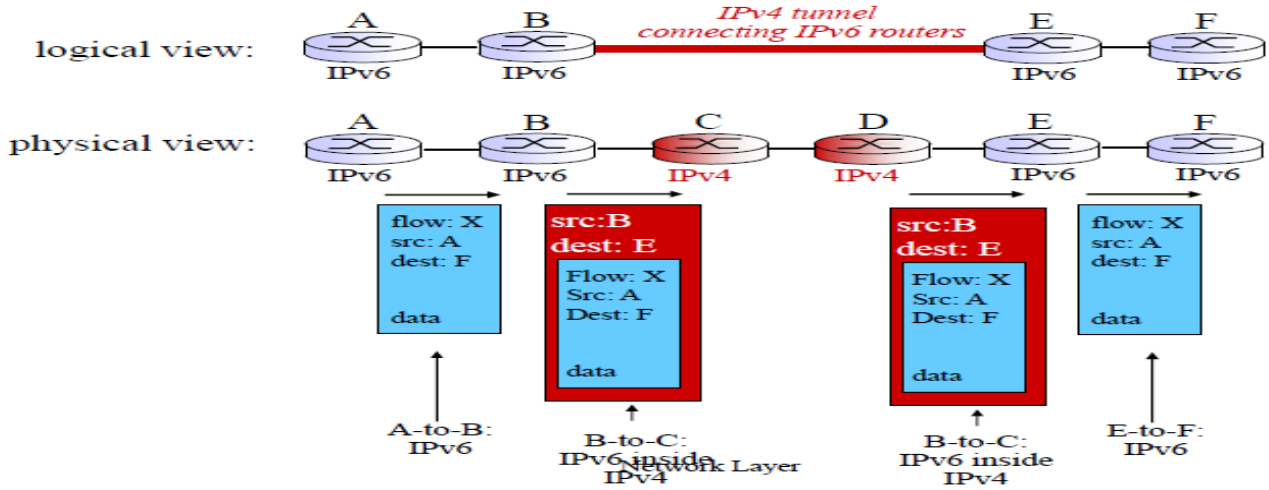
not all routers can be upgraded simultaneously

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



Tunneling



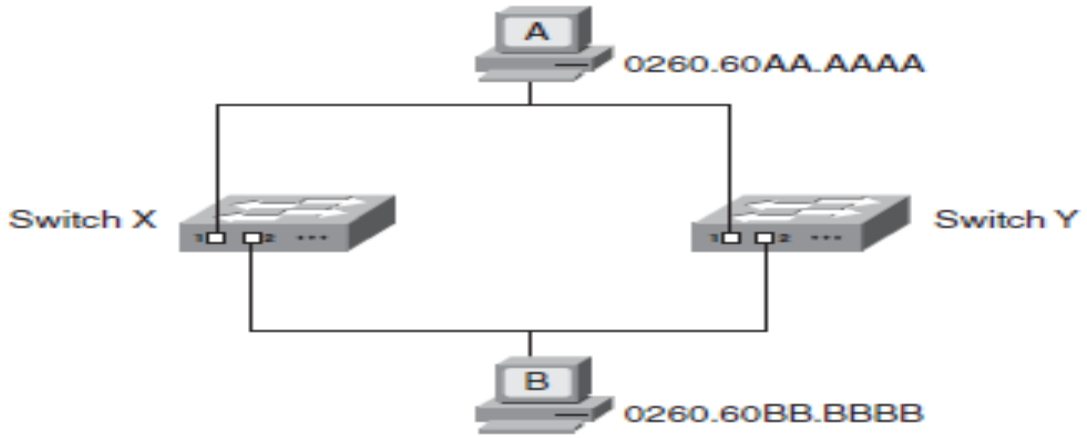


Spanning Tree Protocol (STP)

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 - Ethernet

- 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**.

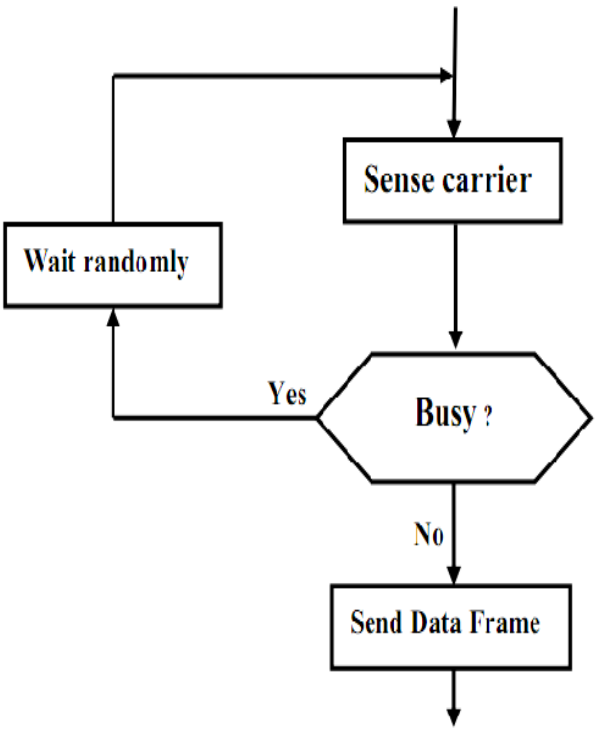
- The access mechanism used in an Ethernet is called ***carrier sense multiple access with collision detection (CSMA/CD,*** standardized in IEEE 802.3).

- 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).

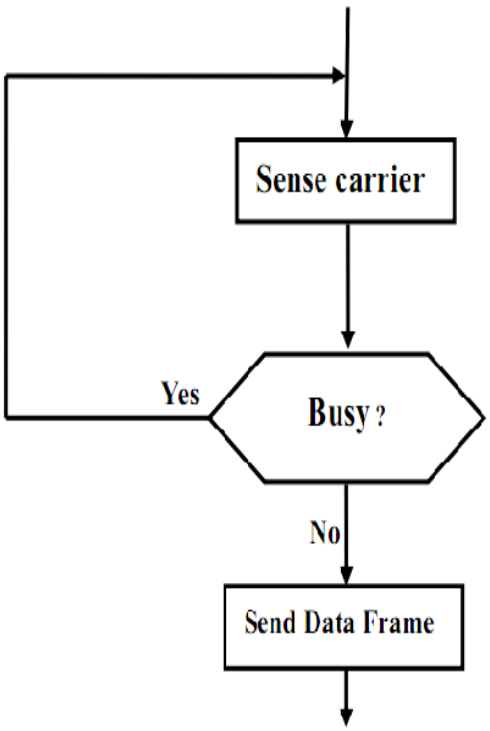
•**Carrier Sense**: when a station in an Ethernet network has data to transmit ,it first see the medium if it is use by other stations or not, this is carrier sense .**<u>under three case of persistence strategy</u>**:

Non-persistence	senses the line, if it is idle, it sends immediately → Not busy if the line busy, it waits a **random time** then sense the line again. busy this method reduces the chance of collision but it also reduced network efficiency.
1-persistence	senses the line , 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.

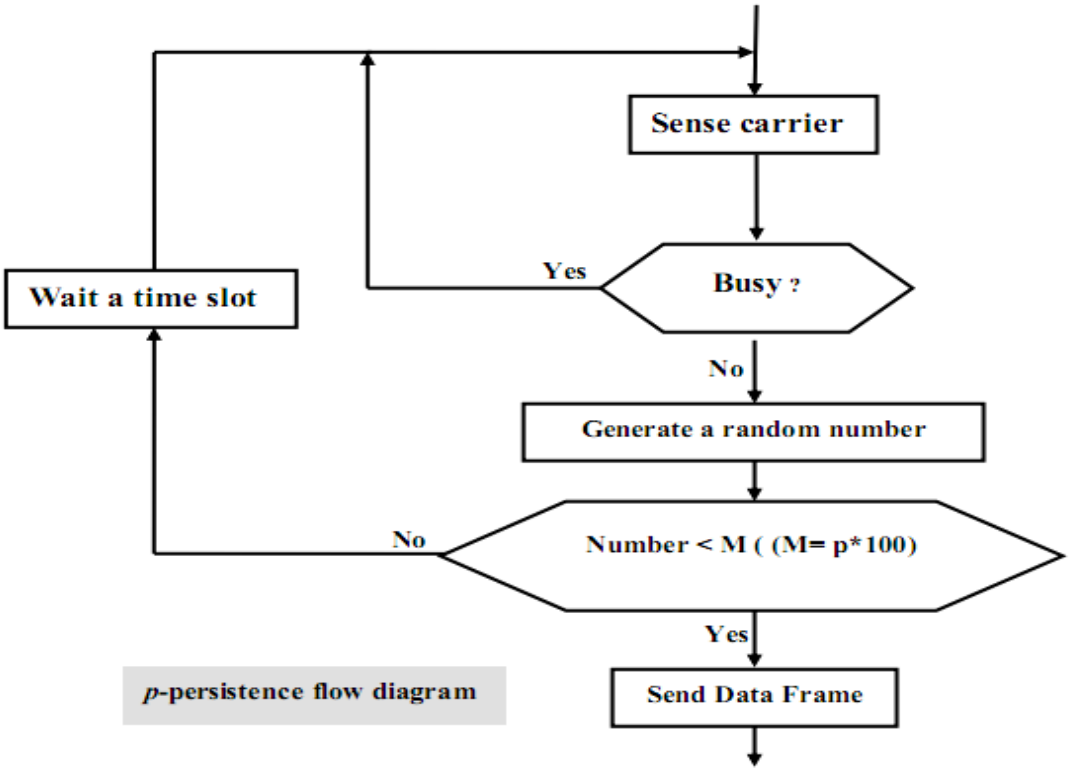
Jam signal: when system detected a collision it immediately stop transmitting data and starts sending this signal any system received packet must discard this packet and should not attempt to transmit any data until network has cleared.



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*

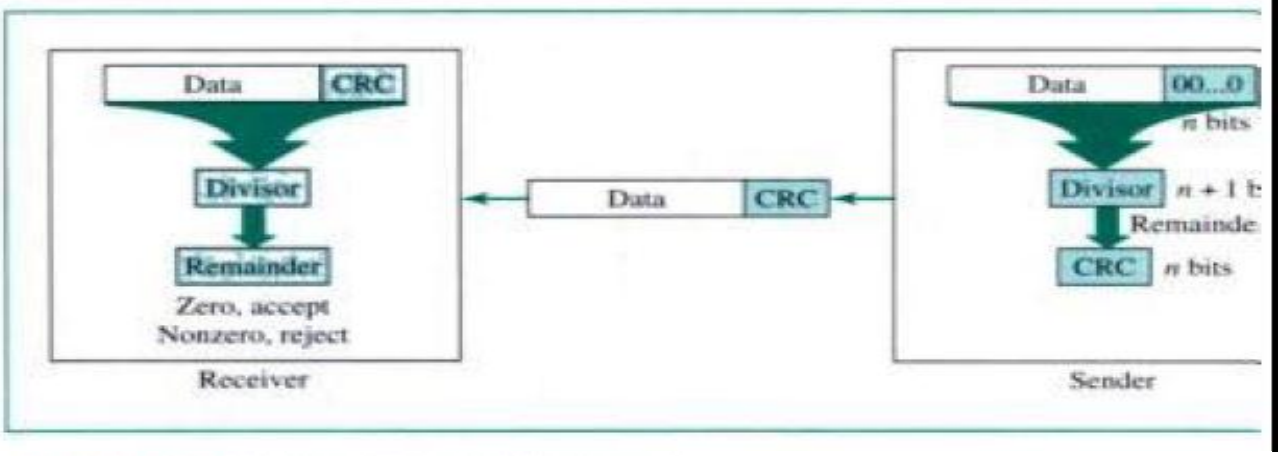


Figure 10.8 *Binary division in a CRC generator*

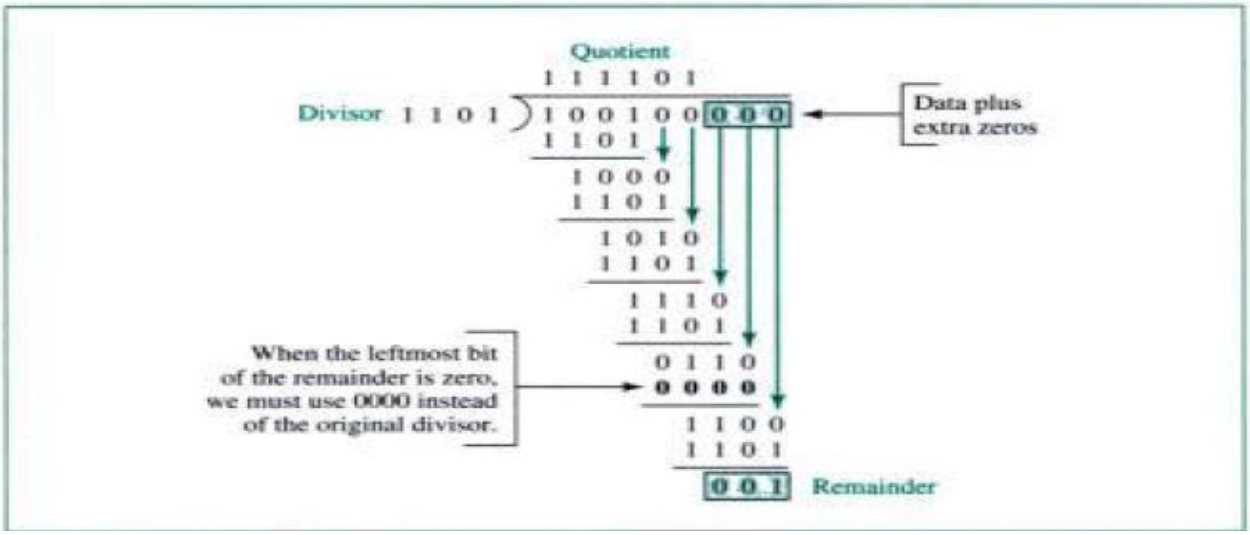
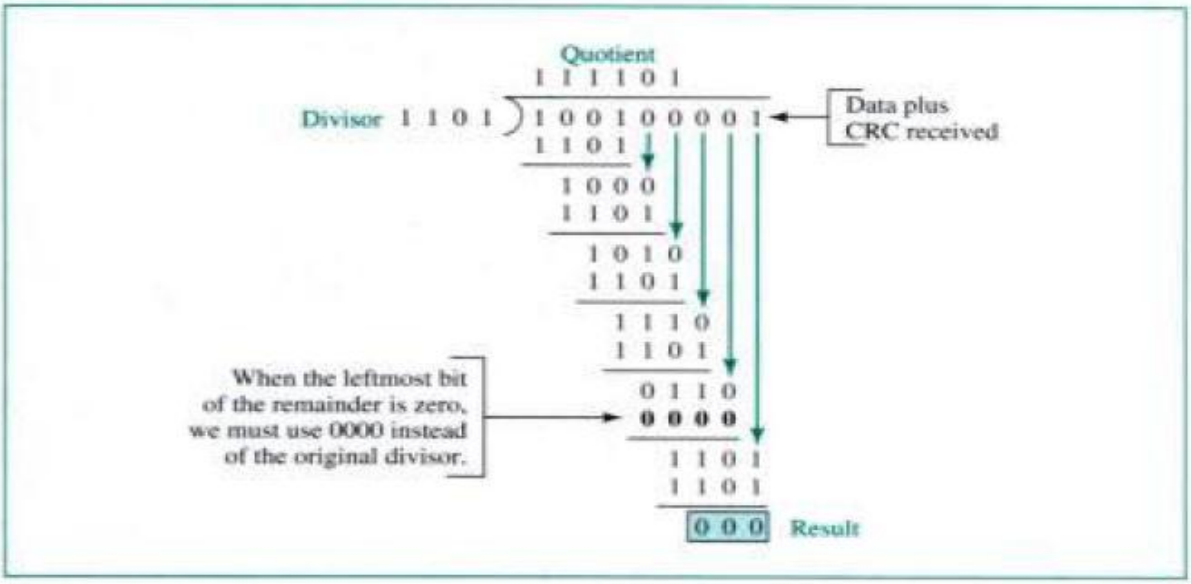
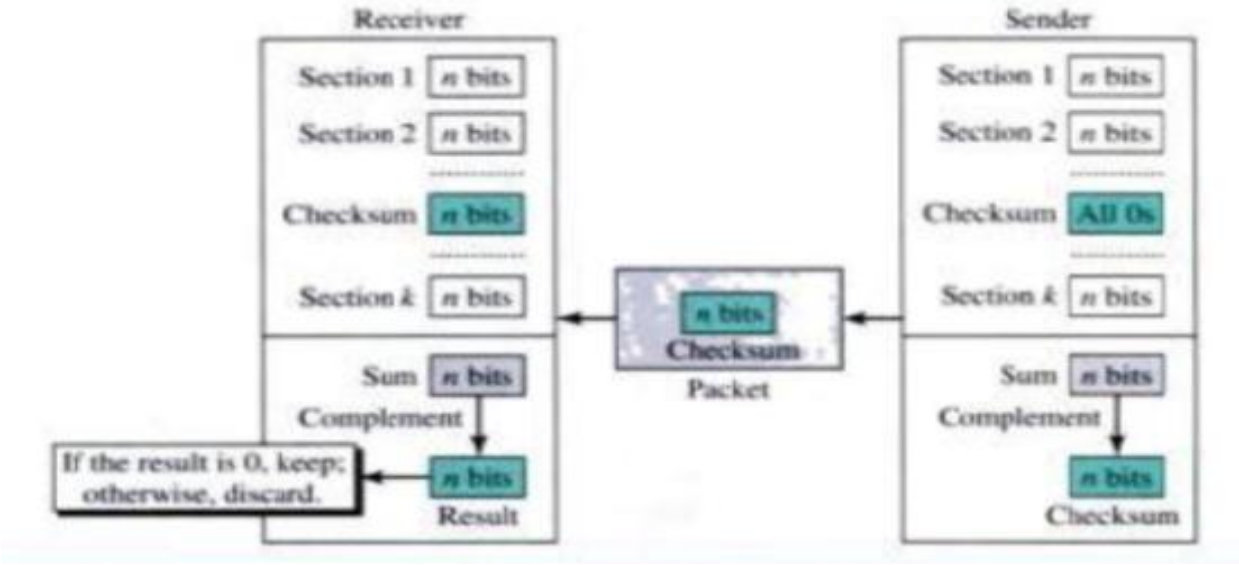


Figure 10.9 *Binary division in CRC checker*



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.

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.
```

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
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.