Al-Furat Al-Awsat Technical University

Technical Engineering College / Al-Najaf

Communications Techniques Eng. Dpt.

Computer Networks

4th Class

2015/2016

By: *Laith Wajeeh Abdullah*

e-mail: laithwajeeh@yahoo.com

الهدف من المادة

تعد مادة شبكات الحاسبات والإتصالات من المواد التخصصية المهمة لمهندسي الإتصالات ولذلك جاء وضع هذا المنهج للمرحلة الرابعة لغرض بناء الطالب بناءاً رصيناً من الناحية النظرية اضافة الى إكسابه المهارات العملية الكفيلة بأن تكون منطلقاً يمكن أن يستند اليه خريجو قسم هندسة تقنيات الإتصالات لتكملة المشوار أكاديمياً أو في سوق العمل.

Syllabus

Week	Item
1	***Networks; overview and important concepts: Network categories*** *(PAN, LAN, MAN,WAN, GAN)****, Circuit switching vs. Packet switching, Baseband vs. Broadband transmission, Transmission modes*** *(simplex, half duplex, full duplex)****, Segments and backbones, Pear to Pear vs. Client/Server Networks , Protocols*** *(elements, functions)* ***, Transfer Rate*** *(Digital BW, Throughput****)***
2,3	***Networking Models: OSI reference model*** *(Layer1: Physical Layer, Layer2: Data-link Layer, Layer3: Network Layer, Layer4: Transport Layer, Layer5: Session Layer, Layer6: Presentation Layer, Layer7: Application Layer)****, TCP/IP model*** *(Network access layer ,Internet layer, Transport layer, Application layer)*
4	***Physical Layer:*** *Mediums* ***[Copper****(Coaxial cable, Twisted Pair Cables),****Fiber Optics*** *(multimode, singlemode)* ***,Wireless*** *(RF, Microwaves, satellites, IR, FSO)****], Networking topologies*** *(Bus, Ring, Dual Ring ,Star, Extended Star, Mesh, Wireless)****), Physical vs. logical topologies***
5	***Physical Layer (continued): Noise*** *(Cross talk, thermal, AC power noise, reference ground noise , EMI/RFI),* ***Losses*** *(Copper medium losses, Fiber optics losses)* ***,Timing issues*** *(Dispersion, Jitter, Latency)****, Coding [Liner coding*** *(NRZL, NRZI, Manchester, Differential Manchester, MLT3)* ***, Block coding*** *(4B/5B, 8B,10B)****], Layer1 Devices*** *(Repeaters, Hubs****)***

Syllabus

Week	Item
6,7	***Data-link layer protocols: Ethernet (IEEE 802.3) [Regular Ethernet*** *(mediums, topologies, encoding),* ***Fast Ethernet*** *(mediums, topologies, encoding),* ***Gigabit Ethernet*** *(mediums, topologies, encoding),* ***10Gigabit Ethernet*** *(mediums, topologies, encoding),* ***frame format ,Data-link Sublayers*** *(MAC, LLC),* ***CRC, MAC addresses*** *(unicast, multicast, broadcast),* ***MAC mechanism (CSMA/CD)]***
8	***Data-link layer protocols (continued):Token Ring(IEEE 802.5) [Physical layer specifications*** *(mediums, speeds, topologies, encoding),* ***Frame types and Formats****(Data Frame, Token Frame, Command Frame, Abort Delimiter Frame),* ***Priority and reservation, MAC mechanism (Token passing)]***
9	***Data-link layer protocols (continued):Fiber Distributed Data Interface FDDI [Physical layer specifications****(mediums, speeds, topologies, encoding),* ***Frame types and Formats****(Data Frame, Token Frame, Station management Frame),* ***MAC mechanism (Early Token Release)]***
10, 11	***Data-link layer protocols (continued):WiFi (IEEE 802.11)*** *[****Physical layer specifications****(topologies, FHSS, DSSS, OFDM, architecture, speeds),* ***Versions*** *(legacy, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n),* ***Frames Formats, MAC mechanism (CSMA/CA)****],* ***Bluetooth (IEEE 802.15)*** *(architecture, format, layers)*

Syllabus

Week	Item
12	***Layer2 Devices :NIC , Ethernet Bridge*** *(collision domains, broadcast domains, transparent bridging)****, Ethernet Switches, Access point.***
13, 14,15	***Network Layer: IPv4 [Datagram format, fragmentation, classfull addressing (subnetting, supernetting), classless addressing]***
16	***Network Layer (continued): IPv6 (datagram format, addressing extension headers, tunneling)***
17	***Network Layer (continued): ICMP****(messages, format, error reporting, queuing)****, IGMP*** *(group management, messages, format, error reporting)****, ICMPv6****(messages, format, error reporting)*
18	***Network Layer (continued): ARP, DNS*** *(Name Space, Resolution, Messages)****, NAT***
19, 20	***Network Layer (continued): Routing [routing tables, static routing, Dynamic routing, unicast routing, multicast routing, Protocols*** *(RIP, OSPF, BGP)****]***

Syllabus

Week	Item
21, 22, 23	***Transport Layer: UDP*** *(format, port numbers, sockets)****, TCP*** *(format, port numbers, connection establishment and connection termination, flow control, error control, congestion control)****, SCTP*** *(format, flow control, error control, congestion control)* ***QoS*** *(Flow characteristics, flow classes)*
24, 25,26	***TCP/IP application layer protocols: e-mail*** *(SMTP, POP3),* ***file transferring*** *(FTP),* ***web*** *(HTTP, HTML, XML)****, VoIP*** *(RTCP, SIP, H323)****, Management*** *(SNPM)*
27, 28	***Security: Encryption ,Viruses , Hacking, Firewalls, VPNs, IPsec, SSL, WEP, WAP***
29, 30	***WAN: Protocols (PPP, PDN), Systems (ATM, SONET , ISDN, DSL)***

Syllabus (LAB)

Week	Item
1	*NIC installation*
2,3	*Cat 5e cabling, cross and straight through*
4	*Peer to Peer 2- PC Network*
5	*LAN via Switches, Extended star LAN*
6	*Sharing (folders, drives)*
7	*Sharing Printers*
8	*Remote Desktop Connection*
9, 10	*Privileges and Security in Win XP*
11	*Ad hoc WLAN*
12	*Infrastructure WLAN via AP*
13, 14	*AP as (Client, PTP bridge, PTMP bridge)*
15,16	*WLAN security (MAC filtering, WEP, WAP)*

Syllabus (LAB)

Week	Item
17	*Routers*
18,19	*Subnetting (Class A, Class B, Class C)*
20,21	*Utilities (ping, Ipconfig, telnet,traceout, nslookup)*
22	*Internet Connection Configuration and Sharing*
23,24,25,26	*Web Site Design (HTML, ASP)*
27	*Win Server 2003 Installation*
28,29,30	*Administration and configuration of Win Server 2008*

References

- Data communications and Networking by Forouzan
- TCP/IP protocols by Berouz and Forouzan
- Data Communications by G. Held

Lec.#1: Introduction to Networking

By: Laith W. Abdullah

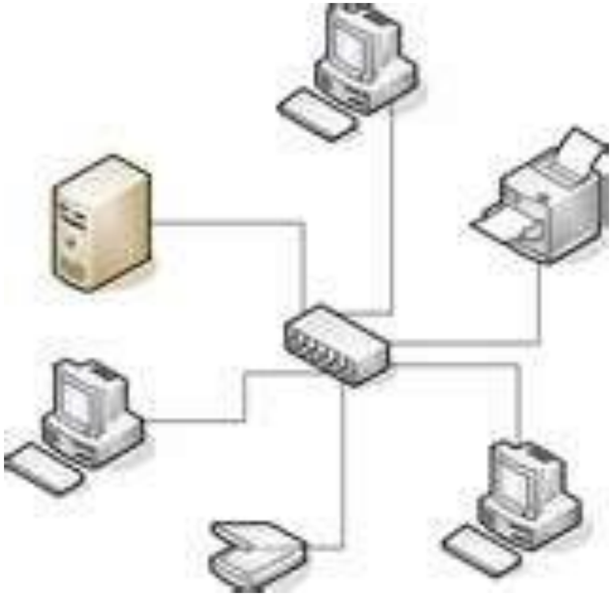
Objectives

- Define computer networks and their basic aims.
- Give an introduction to protocols basic functions and elements.
- Clarify different networks classifications
- Gives basic ideas of switching and data transmission methods.
- Explains how data transfer rates is expressed in computer networks

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Basic Definition

- A network is a connected system of objects or people. The most common example of a network is the telephone system, which is widely known as the Public Switched Telephone Network (PSTN).
- Computer network is defined as having two or more devices (mainly computers) such as workstations or servers and their accessories (like printers, faxes, cameras , etc). These devices are linked together using different kinds of mediums and depending different types of protocols to achieve a variety of aims.



Main Elements

- Protocols
- Devices
- Mediums

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Main Aims

- **Sharing resources** (HW like printers, scanners, cameras or SW like files and applications).
- **Connecting people** (text messaging, IP telephony or video calls and conferencing, blogs and social webs).
- **Higher Security** (restricted policies and permissions).
- **Better Management** (via databases, archives and definite authorities).
- Other complicated functions of networking may be achieved through these basic aims. This may include; **Faster processing, Marketing** (via e-shopping and e-banking), **Navigation and Transportation systems** (by interconnected complicated databases and communication systems), **Better education** (by e-learning and on-line courses) etc..

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Protocols

Definition:

The protocol is a set of rules that governs data communications. Protocols are considered as the common languages used by networking devices to understand each other. The computers may use many of protocols during even the simplest exchanges of network data.

Key Elements:

1) **Syntax: It refers to the structure or format of data. In other words it expresses the way in which the data can be presented.**
2) **Semantics: refers to the meaning of each section or field of the data. It defines how each section is interpreted and what action is to be taken depending on that interpretation.**
3) **Timing: - it defines when the data should be sent and fast it could be sent.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Protocols

Main Functions

Protocols usually have one or more of the following functions:-

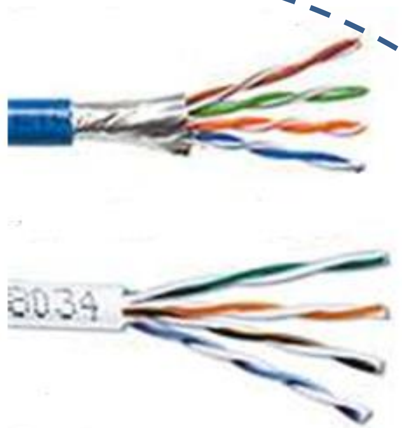
- Addressing
- Acknowledgment
- Segmentation /reassembling
- Flow control
- Error detection
- Error correction
- Compression/decompression
- Encapsulation/de capsulation
- Encryption/decryption

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Mediums

These are the physical means by which data and control information can be transferred between networking devices; they could be

- ❑ Wired (copper or fiber optic)
- ❑ Wireless



Copper Cables

Fiber Optics

Devices

Networking Devices are mainly divided into :

- **End user** devices (such as PCs, laptops, servers ,IP phones, IP cameras , etc.)
- **Intermediate** devices (such as routers, switches, etc.)

End-user devices

Intermediate devices

Networks Classification

I. **By Geographiy:** Depending on the geographical scope networks can be divided into:

1) **Personal Area Networks (PAN):**

   It is characterized to limited distance, usually limited speed, and low volume. Common example is laptop or PDA and a desktop PC or printer using IR or Bluetooth technologies to communicate.

2) **Local Area Network (LAN):**

   A LAN can connect many computers in a relatively small geographical area. These areas can be in a home, an office, or a campus. In most cases all computers on a LAN use the same medium, topology and protocols.

3) **Metropolitan Area Network (MAN):**

   It is a network designed to be extend over an entire city, it may be a single network or may be consists of many interconnected LANs. MANs may be owned and operate by private company or usually a public company.

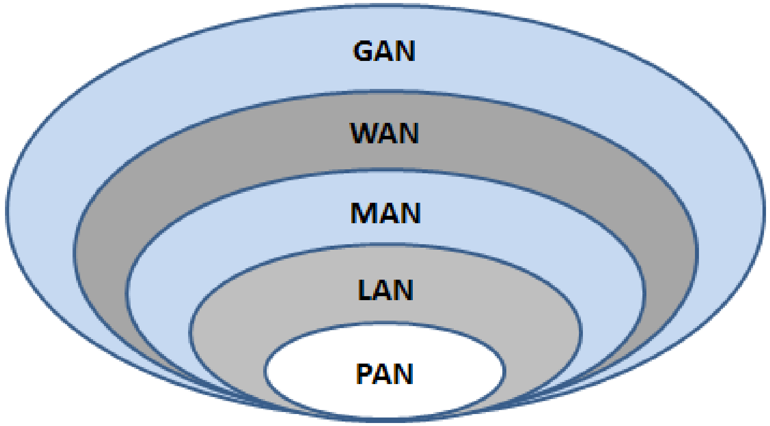
Networks Classification

4) **Wide Area Network (WAN):**

WAN connects devices across a large distance that often crosses the geographical boundaries of cities or states. WAN connections can use telephone lines, radio waves, or any one of many other technologies. WANs are usually owned and operated by public companies.

5) **Global Area Network (GAN):**

GAN provides connectivity between countries around the globe. Internet is the most obvious example on GANs where it connects a huge number of LANs, MANs, and WANs into an interconnected network.

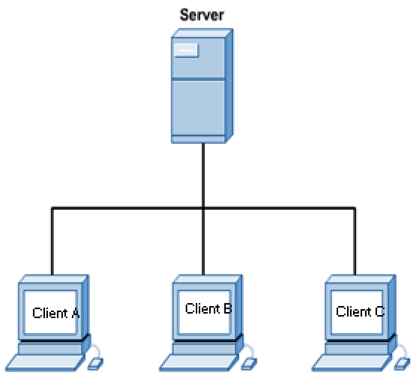


Networks Classification

II. By Relationships: Computer networks can be classified depending on the relationships between network devices into:

1) Client/Server:

- Server is simply a computer (or more precisely, an application running on a computer) that provides a service to other computers.
- Client is a computer that avails itself of the services provided by servers.



Features

- Centralized management.
- Centralized backup and maintenance.
- Easy access to information and resources.
- Higher security.

Drawbacks

- High cost.
- They introduce a single point of failure.
- Need more trained and expert staff to administrate and maintain.

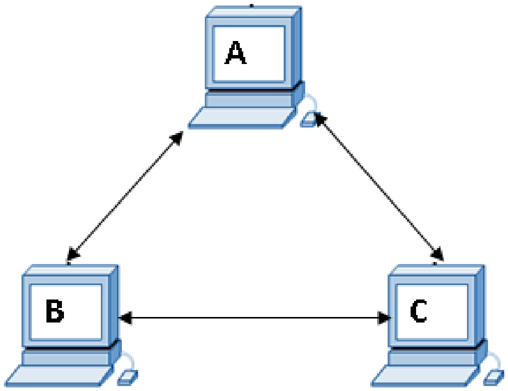
Networks Classification

2) Peer-to-Peer networks:

in peer-to-peer network, every computer is an equal and functions as both a client and a server.

Features

- Easy to install.
- Low cost.



Drawbacks

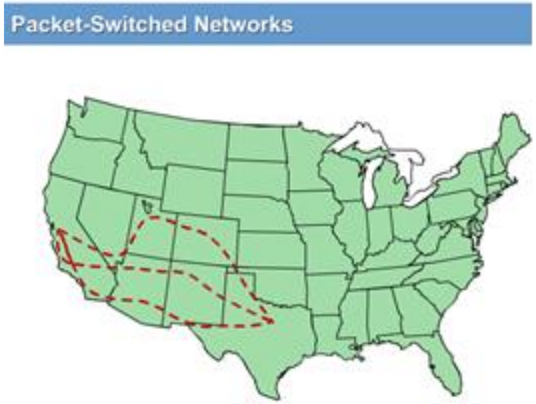
- No centralized backup.
- Difficult to manage where there is no centralized management.
- Limited scalability.
- Less secure than client/server networks

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Switching Methods

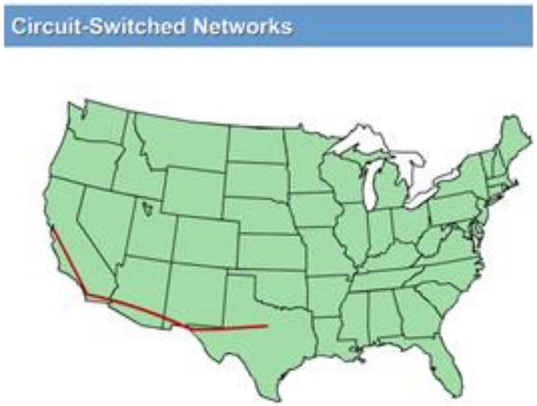
❖ Packet switching

- Here data is divided into blocks called packets.
- No dedicated pathway or circuit is established.
- Each individual packet can take a different route when going from one computer to another.
- Although all packets arrives at the same destination, it does not all travel the same path to get there. Internet traffic uses packet-switching technology



❖ Circuit switching

- The alternative to a packet-switching network is a circuit-switching network,
- here the two systems wanting to communicate establish a path through the network that connects them (called a circuit) before they transmit any information.
- That circuit remains close throughout the life of the exchange and is broken only when the two systems are finished communicating.



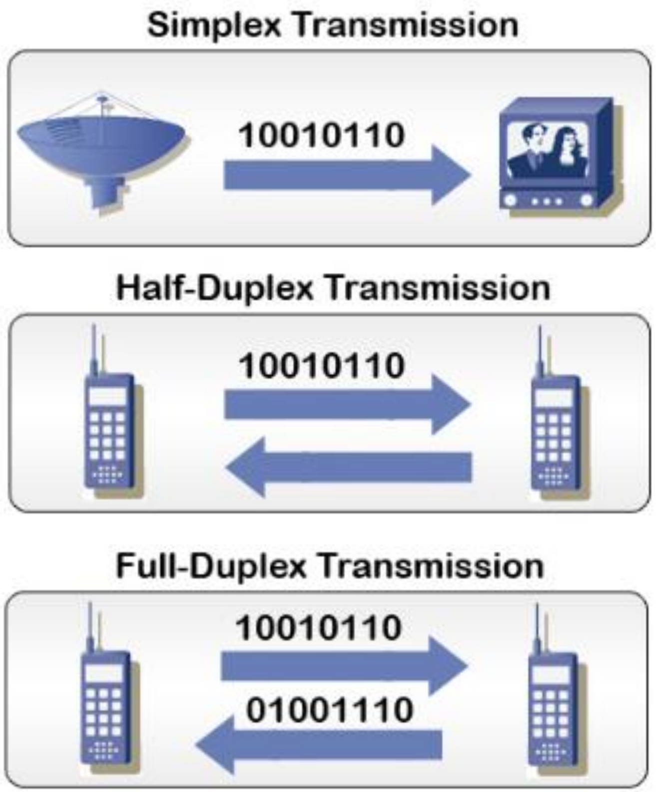
Transmission Modes

A data channel, over which a signal is sent, can operate in one of three modes:

1-Simplex: it is a single one-way baseband transmission. A common example is the signal sent from the TV station to the home television.

2-Half-duplex: it is possible in both directions but not at the same time. An example of a half-duplex communication system is a two-way radio.

3-Full-duplex: here the two systems that can communicate in both directions simultaneously. The most common example of a full-duplex network is the telephone system.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

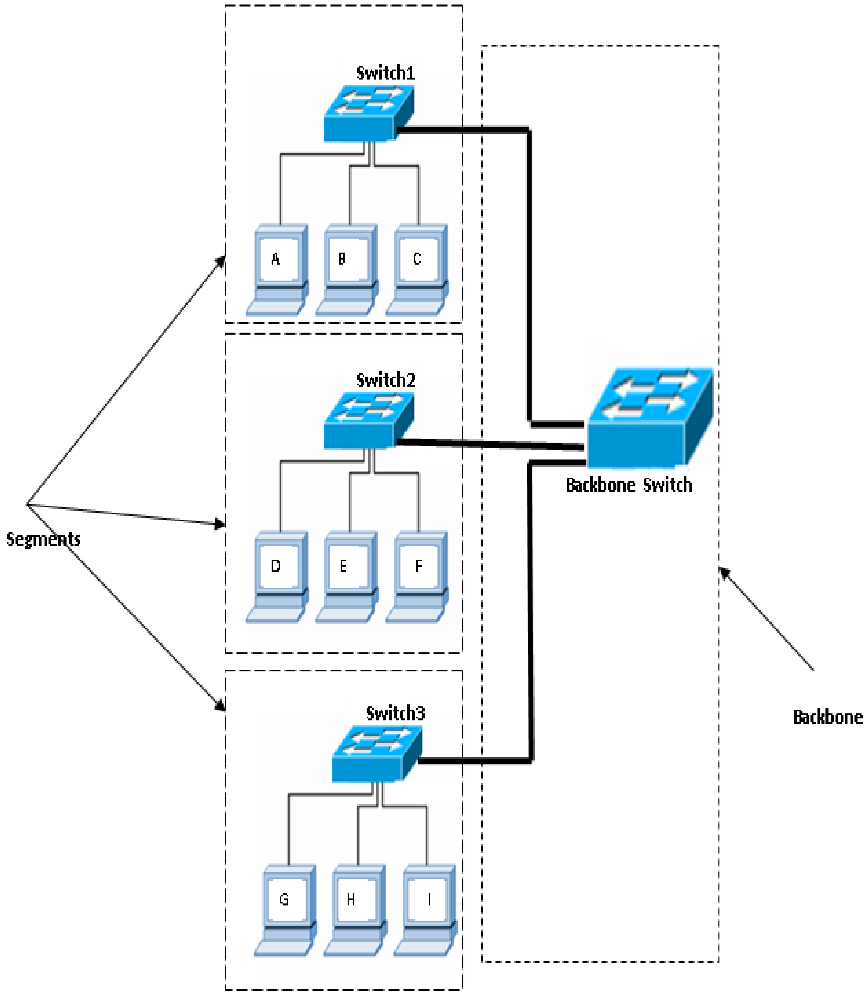
Segments & Backbones

- **Segment:**

  The term segment refers to a LAN composed of user workstations and other end-user devices, such as servers, printers, IP phones, etc.

- **Backbone:**

  The backbone exists primarily as a conduit that enables the segments to communicate with each other.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Transfer Rates

Usually three different terms can be used to describe the rate at which data is transferred, these are:

- **Bandwidth:**

  Also called digital bandwidth is the measure of how much information can flow from one place to another in a given amount of time. When we use the term “Digital Bandwidth” in networking, it usually means the maximum transfer rate of this network.

- **Throughput:**

  It refers to actual, measured bandwidth at a specific time. Unfortunately, for many reasons, the throughput is often far less than the maximum possible digital bandwidth of the medium that is being used.

- **Goodput:**

  It is the measure of usable data transferred over a given period of time, and is therefore the measure that is of most interest to network users.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@yahoo.com

Lec.#2: Networking Models Part I

By: Laith W. Abdullah

Objectives

- Give an idea about the most important standards organizations' in the field of computer networking.
- Clarify the function of layered models in networking.
- Present OSI ref. model as the most common model used in computer networks.
- Define the concept of protocol stack and PDU.
- Give basic idea about encapsulation and decaplsulation processes in OSI ref model.
- Give a brief description about the role of the first two layers of the OSI ref. model.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Standards Organizations'

Standards organizations' generate, control, and administrate standards. In the field of our interest there are two main standards organizations.

- **ISO (International Organization for Standardization)**
- **IAB (Internet Architecture Board)**

❖ ISO

Created in 1946, ISO is responsible for standardization on a wide range of subjects including graphics, document exchange, system compatibility, quality enhancement and many other fields. The bulk of the work of ISO is done by the 2700 technical committees, subcommittees and working groups. In our field of interest, ISO supervised other three standards organizations these are:

- **ITU-T (International Telecommunication Union-Telecommunication Sector)**
- **IEEE (Institute of Electrical and Electronic Engineers)**
- **ANSI (American National Standards Institute)**

Standards Organizations'

- **ITU-T**

  It is one of the three Sectors of the International Telecommunication Union (ITU), which was founded in 1865. The function of ITU-T is to provide global telecommunication standards by studying technical, operating and tariff questions.

- **IEEE**

  Even IEEE was found in United Sates, it is now the world's largest professional society with over 200,000 member. It focuses on the fields of electrical, electronic and communication engineering.

- **ANSI**

  It is the official standards agency for United States. It is responsible for many other committees and associations. The most regarded to our field are EIA (Electronics Industry Association) and TIA (Telecommunication Industry Association).

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Standards Organizations'

❖ **IAB**

It is a technical advisory group of the Internet society. It focuses on Internet protocols, applications, architectures, and technologies. The work of the IAB is carried by two groups. These are:

- **IETF (Internet Engineering Task Force)**
- **IRTF (Internet Research Task Force)**

➢ **IETF**

IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

➢ **IRTF**

While IETF focuses on the shorter term issues of engineering and standards making, IRTF focuses on longer term research issues related to the Internet. IRTF promotes research of importance to the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.

Networking Models

Usually people deals with networking process as if the process is represented of a multilayer model where each layer can carry some of the networking functions.

Why Networking Models?

1) It breaks network communication into smaller parts to make learning it easier to understand.
2) It standardizes network components to allow multiple-vendor development and support.
3) It allows different types of network hardware and software to communicate with each other.
4) It prevents changes in one layer from affecting the other layers, so that they can develop more quickly.

Most Common Models

- OSI (Open System Interconnection) reference model
- TCP/IP (Transmission Control Protocol/Internet Protocol) model

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

OSI ref. model

- It was created by ISO in 1980.
- It is an open system model
- It is seven layer model
- Data in each layer of the model is described by a term which specifically define data in this layer,. This term is called Protocol Data Unit **(PDU)**.

Layer No.	Layer Name	Layer PDU
7	Application	Data
6	Presentation	Data
5	Session	Data
4	Transport	Segment
3	Network	Datagram
2	Data Link	Frame
1	Physical	Bits

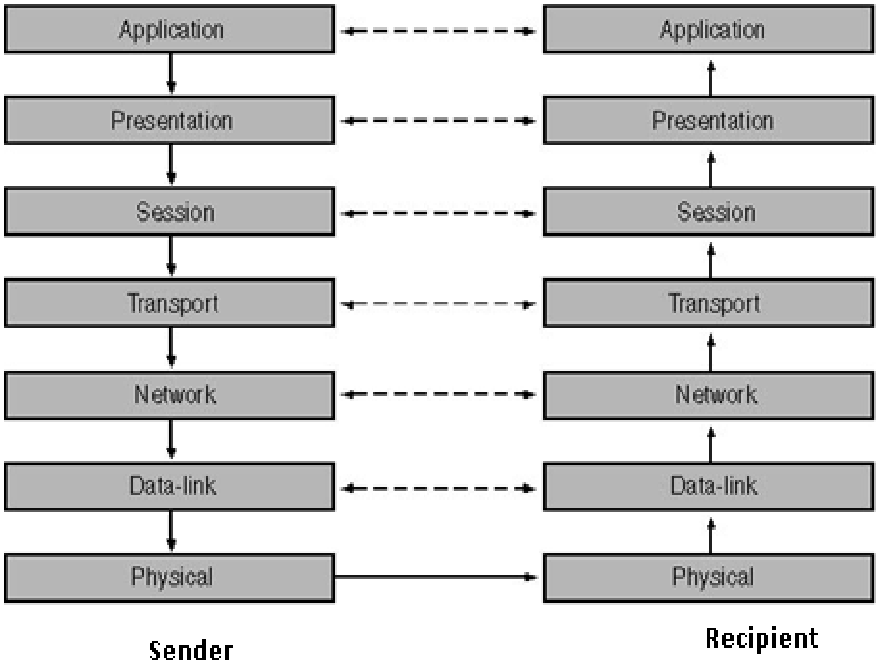
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Protocol stack:

The protocols operating at the various OSI layers confirms a structure that is referred to as protocol stack.

Protocols Interaction

- The data on a transmitting system originates in an application at the top of the protocol stack and works its way down through the layers.
- When the data arrives at its destination, the receiving computer performs the same procedure as the transmitting computer, except in reverse.

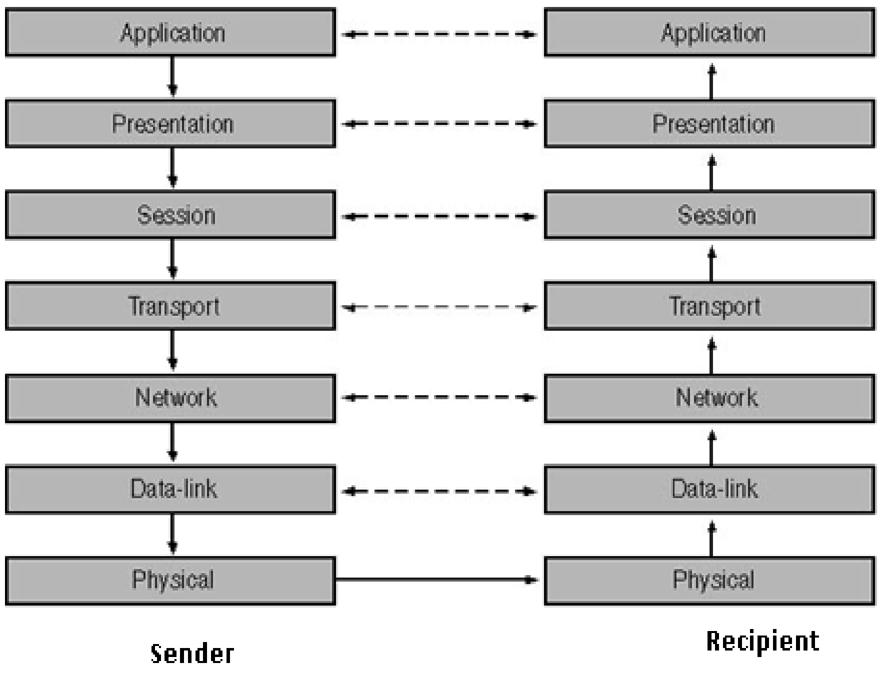


Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Protocol stack:

Protocols Interaction

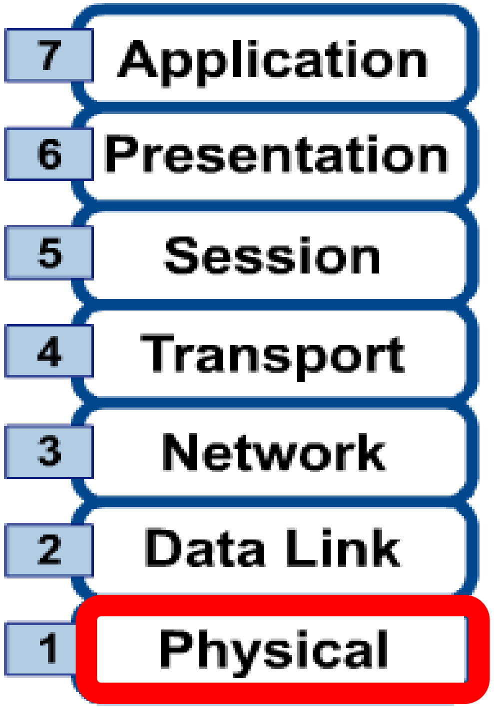
- Protocols at adjacent layers in the stack provide services to each other, depending on the direction in which the data is flowing.
- protocols at the various layers in the transmitting system communicate indirectly with their equivalent protocols operating at the same layer in the receiving system.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Physical Layer

- it is the layer at the bottom of the OSI reference model.
- It deals mainly with networking hardware, this includes:
  - Medium specifications (types, distances, transfer rates , connectors)
  - Signaling (types, encoding, P/S and S/P conversion, modulation)
  - Physical topologies.
- There are no networking protocols in the physical layer.



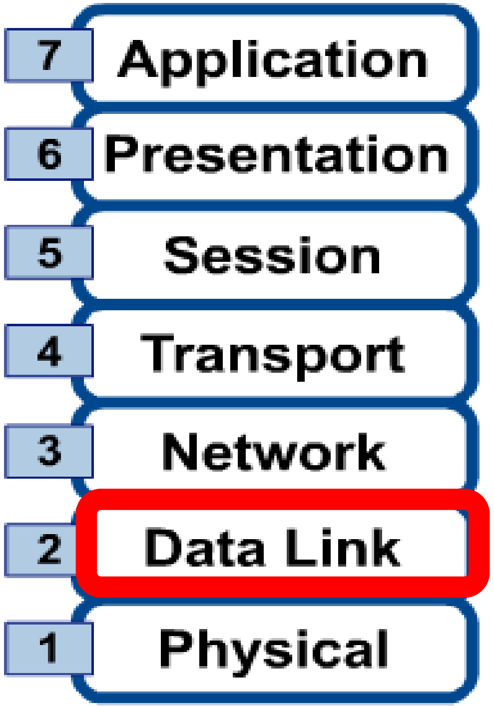
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link Layer

- **The protocol at the data-link layer is the conduit between the computer's networking hardware and its networking software.**

- **Common Data-link Layer Protocols:**
  - **Ethernet (IEEE 802.3)**
  - **Wi Fi WLAN (IEEE 802.11)**
  - **Token Ring (IEEE 802.5)**
  - **FDDI**

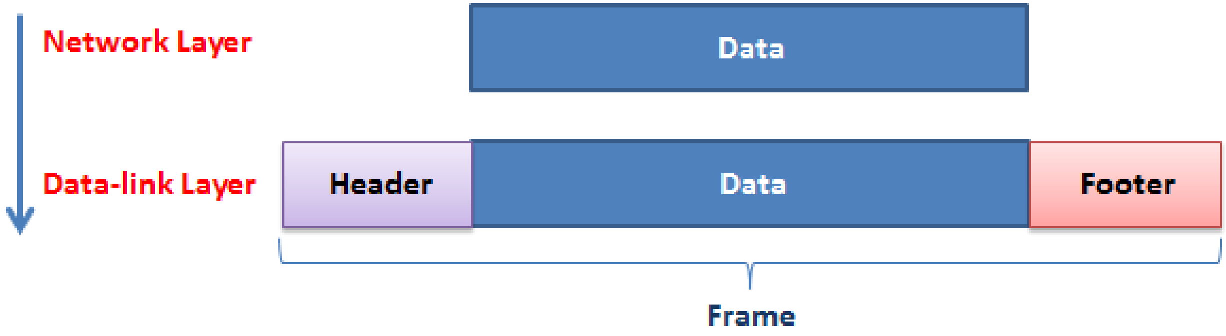
- **Data-link layer protocol specifications typically include the following three basic elements:**
  - **Frame format**
  - **Media Access Control (MAC)**
  - **Physical layer specifications**



Data-link Layer

❖ Frame Format

- The frame is the data unit resulting from adding extra information as a header and footer to upper layer data.
- The process of adding the header and/or footer to the upper layer data is called encapsulation
- header usually contains the source and destination addresses and protocol identifier fields.
- footer usually contains the error detection field (usually depends CRC)



Data-link Layer

MAC mechanism

- This mechanism decides who can access the media and how it can access the media.
- Mainly MAC mechanisms can be classified into:
  - Contention-based.
  - Controlled.
- Common examples on MAC control mechanisms are:
  - Carrier Sense Multiple Access / Collision Detection (CSMA/CD) used in Ethernet.
  - Carrier Sense Multiple Access / Collision Detection (CSMA/CA) used in WLAN.
  - Token Passing used in Token Ring and FDDI.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link Layer

Physical Layer Specifications

- It is the data link layer protocol who decides the physical specifications.
- Physical layer specifications includes:
  - Medium type.
  - Signaling.
  - Topology.
  - Transfer rates.
  - Connectors Types.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The organization that is responsible for Ethernet standardization is

a- FTE
b- IETF
c- ANSI
d- IEEE

MAC mechanism used by WLANs is called

a- CSMA/NA
b- CSMA/CD
c- CSMA/CA
d- None of the previous.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Data encapsulation is a

a- process by which header and footer are striped from upper layer data.
b- process by which header and footer are added to the physical layer data
c- process by which header and footer are added to upper layer data
d- process of correcting errors of a frame

Layer of the OSI ref. model that is responsible of modulation/demodulation is

a- Application layer
b- Data-link Layer
c- Circuit Layer
d- Physical Layer

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#3: *Networking Models* *Part II*

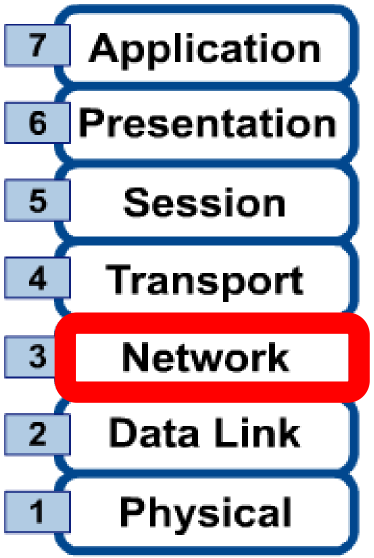
By: *Laith W. Abdullah*

Objectives

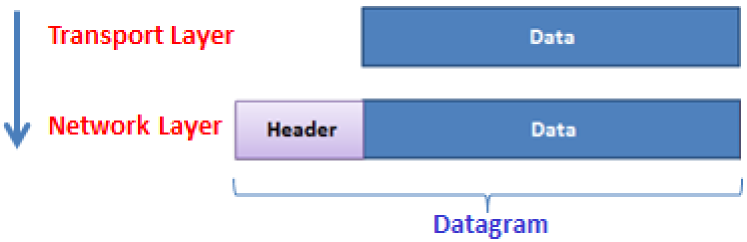
- List the main functions of Network, Transport, Session , Presentation and Application layers of the OSI ref. model.
- Discuss the concepts of connectionless and connection oriented protocols.
- List the four layers of the TCP/IP model with a brief description of the role of each layer.
- Give the main similarties and differences between OSI and TCP/IP models.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Network Layer



- Network layer protocols are mainly responsible for end-to-end communications, whereas data-link layer protocols function only on the local LAN.
- <u>Common network layer protocols:</u>
  - Internet Protocol (IP)
  - Internetwork Packet Exchange (IPX)
- <u>The PDU of network layer protocol</u>
  - The PDU of network layer protocol is called datagram.
  - The datagram is formed by adding header to upper layer data.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Network Layer

Main functions

- **Addressing**

  Define the source and destination addresses of the end-to-end communicating systems

- **Fragmenting**

  Splitting the datagram into smaller blocks called fragments due to the limitation of the Data-link layer protocol of the outgoing network.

- **Routing** :

  Directing a datagram from its source, through an internetwork, and to its ultimate destination using the most efficient path possible. This process is done by an intermediate networking devices called routers.

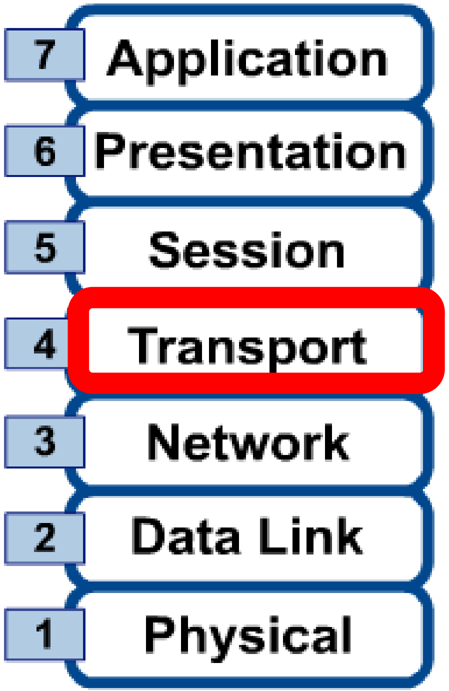
- **Identifying the transport layer protocol:**

  The header of the network layer protocol must contain a field that identifies the protocol where the data comes from.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Transport Layer

- The main function of transport layer is to transport upper layer data form the source host application to the final destination host application; this type of communication is called process-to –process communication



- Common Transport layer protocols:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - NetWare Core Protocol (NCP)
  - Sequenced Packet Exchange (SPX)
- TCP and UDP used with IP
- NCP and SPX are used with IPX
- <u>The Transport Layer PDU</u>

The PDU of Transport layer is called Segment, it is formed by adding transport layer protocol header to a block of upper layer data

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Transport Layer

Main functions

- **Addressing:** The headers for transport layer protocols usually include numbers called the port numbers that identify the applications from which application the packet originated and for which application it is destined.
- **Segmentation:** splitting the data stream of upper layer data into blocks, adding a header to each block to form segments.
- **Transportation:** transport layer protocols transport the data from the source application to the final destination application . Depending on the way the source and destination can communicate; Transport layer protocols can be:
  - Connection oriented
  - Connectionless

Transport Layer

❖ Connection-oriented Protocols

- Here the two communicating systems exchange messages to establish a connection before they transmit any application data.
- it provide additional services such as
  - Packet acknowledgment
  - Flow control
  - Error detection
- Usually used for transferring large amount of data.
- The drawback of this type of protocol is that it greatly increases the amount of control data exchanged by the two systems.
- TCP is an example on Connection-oriented transport layer protocols.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

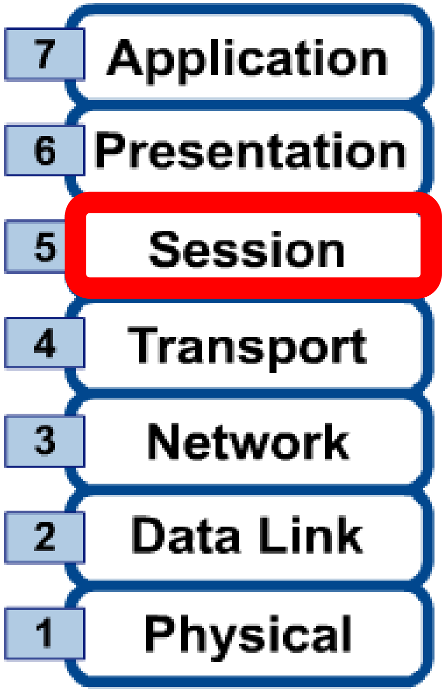
Transport Layer

Connectionless Protocols

- Here, there is no preliminary communication between the two systems before the transmission of application data.
- The sender simply transmits its data to the destination without knowing if the system is ready to receive data, or even if the system exists.
- Usually used for brief transactions that consist only of single requests and responses.
- Connectionless Protocols are fast as compared to connection oriented protocols.
- They have low overhead
- They are not not reliable
- UDP is an example of connectionless Transport layer protocol.

Session Layer

- There are no separate session layer protocols, where Session layer functions are instead integrated into other protocols that also include presentation and application layer functions.
- The session layer establishes, manages, and terminates sessions between two communicating hosts.
- The session layer provides services which are mainly concerned with the ways in which networked systems exchange information (called dialogs). The most important of these services are:
  - Dialog control
  - Dialog separation



Session Layer

- **Dialog Control :-**

  is the selection of a mode that the systems will use to exchange messages. When the dialog is begun, the systems can choose one of two modes:-

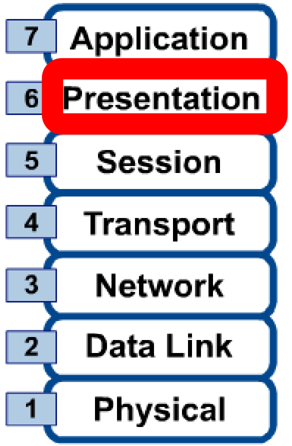
  - **Two-way Alternate (TWA) mode:-** (for two communicating computers, only one is permitted to transmit at a time)
  - **Two-way Simultaneous (TWS) mode:-** (is more complex where the two communicating computers, can transmit at the any time, and even simultaneously)

- **Dialog Separation :-**

  Is the process of creating checkpoints in a data stream that enable communicating systems to synchronize their functions.

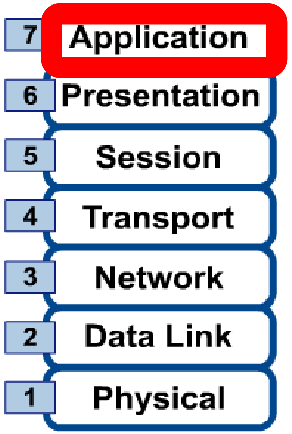
Presentation Layer

- The main function found at the presentation layer: the translation of syntax between different systems from the abstract syntax each system use to a transfer syntax throw the communication process.
- This translation may also include compression and encryption



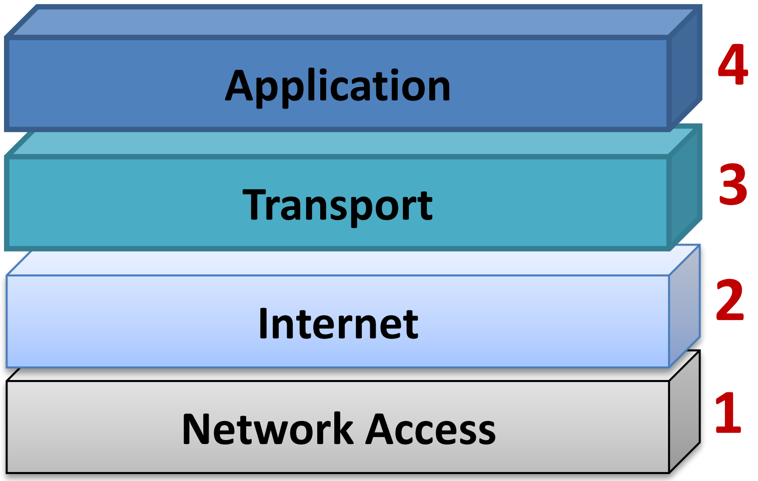
Application Layer

- The application layer is the OSI layer that is closest to the user.
- It provides network services to the user's applications.
- Examples on application layer protocols are:
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)



TCP/IP Model

- It is developed by the DoD (Department of Defense) in USA.
- It created in the 1970s
- It evolved from ARPANET, which was the world's first WAN and a predecessor of the Internet.
- The TCP/IP Model is sometimes called the Internet Model
- It is a four layer model.

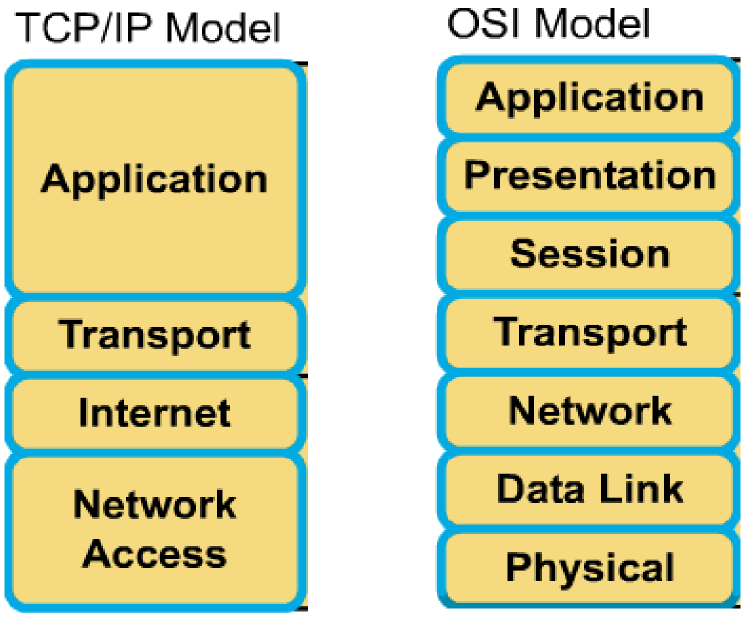


TCP/IP Model

❖ TCP/IP & OSI

Similarities

- Both are layered models
- Both have application layers, though they include very different services
- Both have comparable transport and network (internet) layers
- Packet-switched (not circuit-switched) technology is assumed

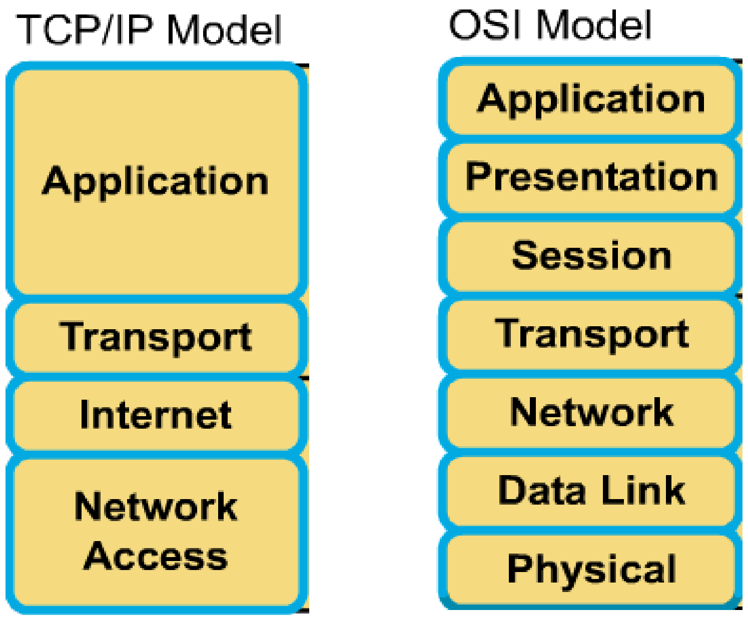


TCP/IP Model

TCP/IP & OSI

Differences

- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into one layer
- TCP/IP appears simpler because it has fewer layers, however this is a misconception. The OSI reference model, with its less complex and multiple layers, is simpler to develop and troubleshoot.



???? Quiz ????

TCP/IP model that responsible of data encryption is:

a- Session
b- Presentation
c- Application
d- Transport

One of the followings is a reliable Transport layer protocol

a- Ethernet
b- PDU
c- UDP
d- TCP

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

MAC mechanism is one of the functions of

a- Physical layer in the TCP/IP model.
b- Network access layer in the OSI reference model.
c- Network layer in the TCP/IP model.
d- Network Access layer in the TCP/IP model

One of the followings is an end to end communication protocol

a- IP
b- TCP/IP
c- FDDI
d- RFC

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Lec.#3: Networking Models Part II

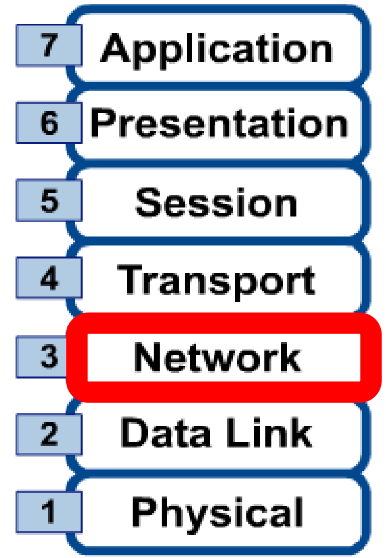
By: Laith W. Abdullah

Objectives

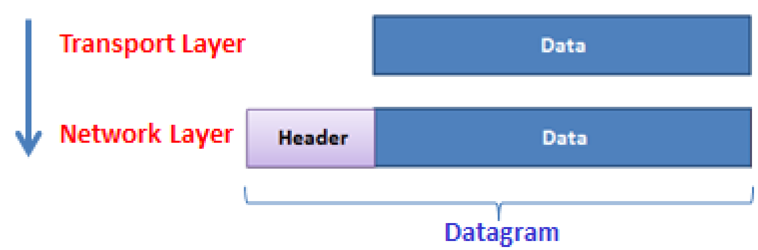
- List the main functions of Network, Transport, Session , Presentation and Application layers of the OSI ref. model.
- Discuss the concepts of connectionless and connection oriented protocols.
- List the four layers of the TCP/IP model with a brief description of the role of each layer.
- Give the main similarties and differences between OSI and TCP/IP models.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Network Layer



- Network layer protocols are mainly responsible for end-to-end communications, whereas data-link layer protocols function only on the local LAN.
- Common network layer protocols:
  - Internet Protocol (IP)
  - Internetwork Packet Exchange (IPX)
- The PDU of network layer protocol
  - The PDU of network layer protocol is called datagram.
  - The datagram is formed by adding header to upper layer data.



Network Layer

Main functions

- **Addressing**

  Define the source and destination addresses of the end-to-end communicating systems

- **Fragmenting**

  Splitting the datagram into smaller blocks called fragments due to the limitation of the Data-link layer protocol of the outgoing network.

- **Routing :**

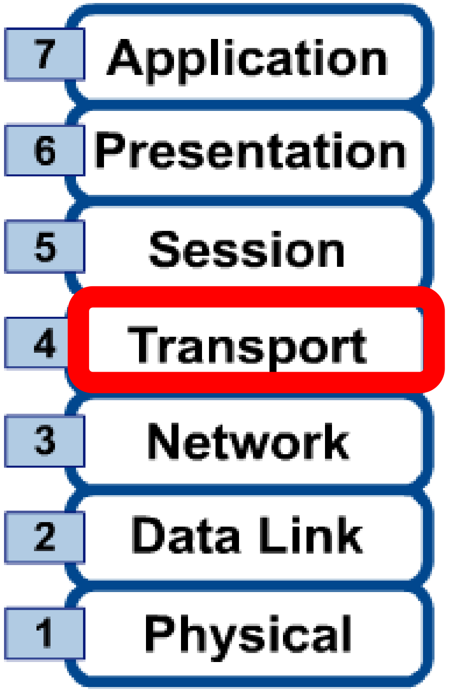
  Directing a datagram from its source, through an internetwork, and to its ultimate destination using the most efficient path possible. This process is done by an intermediate networking devices called routers.

- **Identifying the transport layer protocol:**

  The header of the network layer protocol must contain a field that identifies the protocol where the data comes from.

Transport Layer

- The main function of transport layer is to transport upper layer data form the source host application to the final destination host application; this type of communication is called process-to –process communication



- Common Transport layer protocols:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - NetWare Core Protocol (NCP)
  - Sequenced Packet Exchange (SPX)
- TCP and UDP used with IP
- NCP and SPX are used with IPX
- The Transport Layer PDU

The PDU of Transport layer is called Segment, it is formed by adding transport layer protocol header to a block of upper layer data

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Transport Layer

Main functions

- **Addressing:** The headers for transport layer protocols usually include numbers called the port numbers that identify the applications from which application the packet originated and for which application it is destined.
- **Segmentation:** splitting the data stream of upper layer data into blocks, adding a header to each block to form segments.
- **Transportation:** transport layer protocols transport the data from the source application to the final destination application . Depending on the way the source and destination can communicate; Transport layer protocols can be:
  - Connection oriented
  - Connectionless

Transport Layer

Connection-oriented Protocols

- Here the two communicating systems exchange messages to establish a connection before they transmit any application data.
- it provide additional services such as
  - Packet acknowledgment
  - Flow control
  - Error detection
- Usually used for transferring large amount of data.
- The drawback of this type of protocol is that it greatly increases the amount of control data exchanged by the two systems.
- TCP is an example on Connection-oriented transport layer protocols.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

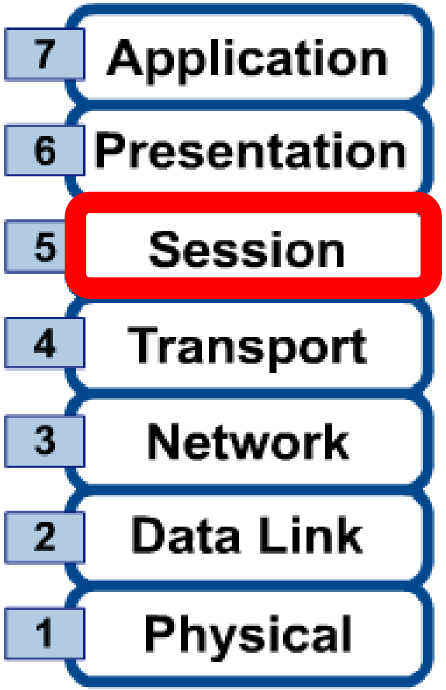
Transport Layer

❖ Connectionless Protocols

- Here, there is no preliminary communication between the two systems before the transmission of application data.
- The sender simply transmits its data to the destination without knowing if the system is ready to receive data, or even if the system exists.
- Usually used for brief transactions that consist only of single requests and responses.
- Connectionless Protocols are fast as compared to connection oriented protocols.
- They have low overhead
- They are not not reliable
- UDP is an example of connectionless Transport layer protocol.

Session Layer

- There are no separate session layer protocols, where Session layer functions are instead integrated into other protocols that also include presentation and application layer functions.
- The session layer establishes, manages, and terminates sessions between two communicating hosts.
- The session layer provides services which are mainly concerned with the ways in which networked systems exchange information (called dialogs). The most important of these services are:
  - Dialog control
  - Dialog separation



Session Layer

- **Dialog Control :-**

  is the selection of a mode that the systems will use to exchange messages. When the dialog is begun, the systems can choose one of two modes:-

  - **Two-way Alternate (TWA) mode:-** (for two communicating computers, only one is permitted to transmit at a time)
  - **Two-way Simultaneous (TWS) mode:-** (is more complex where the two communicating computers, can transmit at the any time, and even simultaneously)

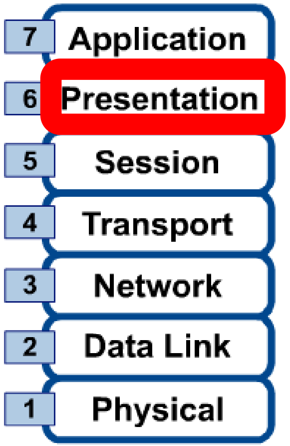
- **Dialog Separation :-**

  Is the process of creating checkpoints in a data stream that enable communicating systems to synchronize their functions.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

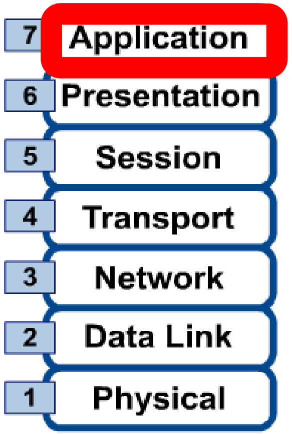
Presentation Layer

- The main function found at the presentation layer: the translation of syntax between different systems from the abstract syntax each system use to a transfer syntax throw the communication process.
- This translation may also include compression and encryption



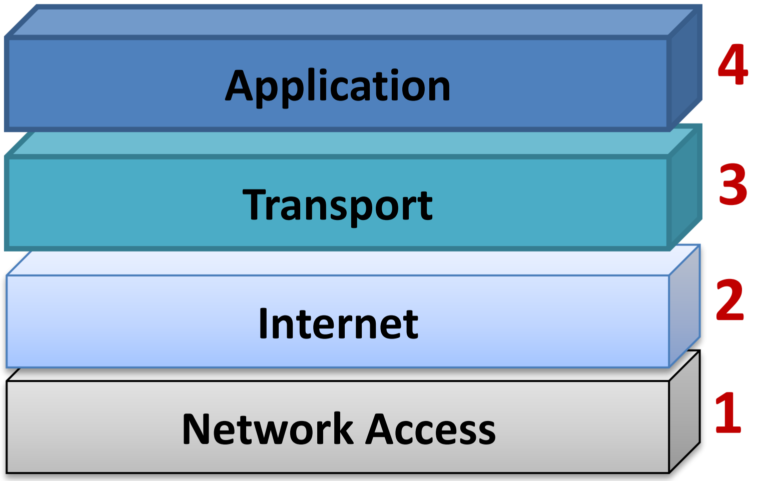
Application Layer

- The application layer is the OSI layer that is closest to the user.
- It provides network services to the user's applications.
- Examples on application layer protocols are:
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)



TCP/IP Model

- It is developed by the DoD (Department of Defense) in USA.
- It created in the 1970s
- It evolved from ARPANET, which was the world's first WAN and a predecessor of the Internet.
- The TCP/IP Model is sometimes called the Internet Model
- It is a four layer model.



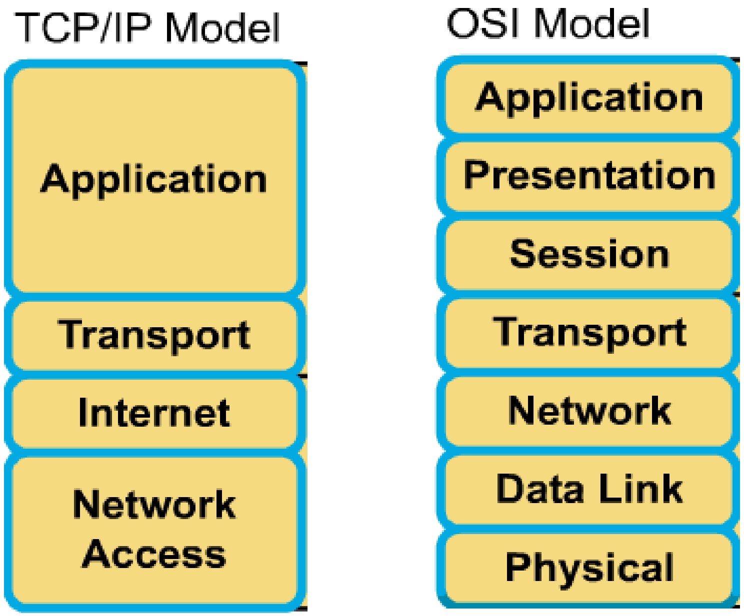
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

TCP/IP Model

❖ TCP/IP & OSI

Similarities

- Both are layered models
- Both have application layers, though they include very different services
- Both have comparable transport and network (internet) layers
- Packet-switched (not circuit-switched) technology is assumed

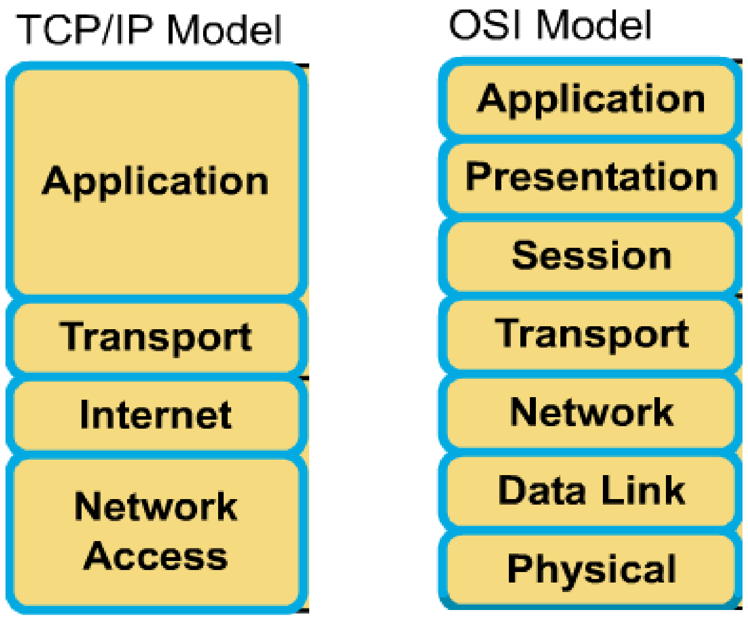


TCP/IP Model

❖ TCP/IP & OSI

Differences

- **TCP/IP combines the presentation and session layer issues into its application layer.**
- **TCP/IP combines the OSI data link and physical layers into one layer**
- **TCP/IP appears simpler because it has fewer layers, however this is a misconception. The OSI reference model, with its less complex and multiple layers, is simpler to develop and troubleshoot.**



???? Quiz ????

TCP/IP model that responsible of data encryption is:

a- Session
b- Presentation
c- Application
d- Transport

One of the followings is a reliable Transport layer protocol

a- Ethernet
b- PDU
c- UDP
d- TCP

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

MAC mechanism is one of the functions of

a- Physical layer in the TCP/IP model.
b- Network access layer in the OSI reference model.
c- Network layer in the TCP/IP model.
d- Network Access layer in the TCP/IP model

One of the followings is an end to end communication protocol

a- IP
b- TCP/IP
c- FDDI
d- RFC

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Lec.#5: *Physical Layer Part II*

By: *Laith W. Abdullah*

Objectives

- Explain the functions of repeaters and hubs as the main physical layer devices.
- Discuss the main types of noise that may affects signals carried by networking mediums .
- Briefly describes the effect of timing issues on signals transmission over the network.
- List the main physical topologies with a brief description for each.
- Gives an idea of losses types in networking cables.
- List the main types of signals modulation.
- Explain the concept of encoding combined with some of line and block encoding schemes.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Physical Layer devices

- **Physical Layer Devices**

The most common examples on Physical Layer devices are :

- Repeaters
- Hubs

- **Repeater**
  - Repeaters are internetworking devices.
  - Repeaters usually two port devices (one input port and one output port).
  - They can increase the distance over which the network can extend (expand the network).
  - Repeaters reshape, regenerate, and retime signals before sending them on along the network.
  - Repeaters cannot filter network traffic.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Physical Layer devices

➢ Hubs

- **Hub is internetworking device.**
- **Connect the nodes of the network in a physically star topology (or extended star topology by interconnecting hubs).**
- **In Ethernet, hub is to provide the crossover circuit that connects the transmit pins to the receive pins for each connection between two computers.**

- **Hubs can be classified according to signal amplification or repetition into two classes:**
  - **Passive hubs:** **they don't do any amplification, but just distributing the signal coming on one port on to the other ports.**
  - **Active Hubs:** **in addition to distribute the incoming signal on one port of the hub on the other ports, active hub takes in the weakened signal, cleans it up, and amplifies it before sending it out (So, they are multiport repeaters).**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Physical Layer devices

Hubs

- Hubs can also classified according to the way they deal the data into two types
  - **Dumb Hubs:** work with the signals native to the network medium, such as electrical voltages, but does not interpret the signals, read the data inside packets, or even recognize that there is data there.
  - **Intelligent Hubs:** include management features that enable them to monitor the operation of each of the hub's ports. In most cases, an intelligent hub uses the Simple Network Management Protocol (SNMP) to transmit periodic reports to a centralized network management console.

Signals

Topics related to signals all lie in the physical layer of the OSI reference model, these includes.

- Noise
- Losses
- Timing
- Modulation
- Encoding

Noise

- Noise is unwanted random signal added to original signal.
- it is important to keep the Signal-to-Noise (S/N) ratio as high as possible.
- Common types of noise:

A-Cross Talk Noise

- Electrical noise on the cable that originates from signals on other wires in the cable.
- Twisting is a good solution to reduce the effect of cross talk noise.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

Noise

B-Thermal Noise

- Thermal noise, is due to the random motion of electrons within the media
- Solution is to give the signals large enough amplitude so that it does not matter.

C- AC Power Noise

Good grounding is a good solution for the AC power noise.

D-Reference Ground Noise

Short and separate signal reference ground cables can decrease the effects of reference ground noise.

E- EMI/RFI

electromagnetic interference (EMI) like lightning, electrical motors , and radio frequency interference (RFI) like radio systems can be avoided by Shielding and good grounding are good solutions to reduce the effect of EMI/RFI noise.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

Losses

Mainly divided according to the type of medium into:

- Copper Losses
- Fiber Optic Losses

A- Copper losses:-

- **Conductor losses:** This is due to the resistance of the copper medium.
- **Radiation losses:** Portion of signal energy is lost as electromagnetic radiation due to the flow of current in the copper conductor.
- **Coupling losses:** Connectors are discontinuities which are locations on which dissimilar materials meet. Discontinuities tend to heat up, radiate energy and dissipate power.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

➢ Losses

B-Fiber optic losses:

- Absorption losses: **Impurities in fiber optic tend to absorb light in the fiber and convert it to heat.**
- Scattering losses: **microscopic irregularities and impurities along the fiber causes the light to be diffracted and spread and out in different directions.**
- Radiation losses: **portion of the light can be radiated out of the core due to bends and kinks in the fiber.**
- Coupling losses: **these losses occurs at the junctions in fiber optics. Junctions are either source-to-fiber, fiber-to-fiber, or fiber-to-photodetector.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

➢ Timing

The most important timing issues are:

- Dispersion
- Jitter
- Latency

A-Dispersion

- Dispersion occurs when the signal broadens in time.
- It is caused by the type of media involved.
- It may cause a bit to interfere with the next bit and confuse it with the bits before and after it.

B- Jitter

- Packets may arrive a little earlier and later than expected.
- It especially affects real time audio or video applications.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

Timing

C-Latency

Latency (or simply the delay) is made of four components.

- Propagation time: signals in different mediums have different propagations speeds. So the propagation time differs according to:

$$\text{Propagation time} = \text{Distance} \;/\; \text{Propagation Speed}$$

- Transfer time: The transfer time depends on the throughput. Where

$$\text{Transfer time} = \text{Packet Size} \;/\; \text{Throughput}$$

- Queuing time: the time needed by each intermediate or device to hold the message before it pass it or process it.
- Processing time: the time needed to process the packet.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

Modulation

Modulation techniques are mainly divided into two brands:

- Analog
- Digital

A- Analog Modulation:

- AM (Amplitude Modulation) - the amplitude, or height, of a carrier sine wave is varied to carry the message
- FM (Frequency Modulation) - the frequency of the carrier wave is varied to carry the message
- PM (Phase Modulation) - the phase, or beginning and ending points of a given cycle, of the wave is varied to carry the message

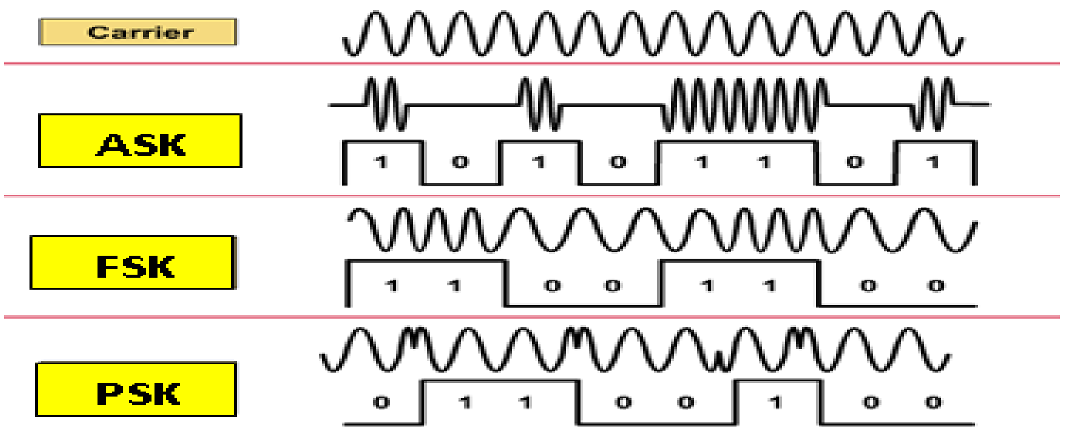
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

➢ Modulation

B- Digital Modulation:

- **ASK (Amplitude Shift Keying) : here the amplitude of the carrier varies between two levels, one for 1's and the other for zeros.**
- **FSK (Frequency Shift Keying): here we have two carriers frequencies, one for 1's and the other for 0's.**
- **PSK (Phase Shift keying) : the phase of the carrier changes between two phases according to the message (1's and 0's).**



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

Encoding

- Encoding means converting 1's and 0's (data) into something real and physical, such as electrical signals and light pulses.
- Encoding methods goal to get one or more of the followings:-
  - Self synchronization techniques.
  - Built in error Detection.
  - Immunity to noise.
  - Better channel usage by maximizing bit rates.
  - Reducing or eliminating low frequency components.
- Generally coding methods are divided into:-
  1. Line coding.
  2. Block coding.

Signals

❖ Line Encoding

- Converting data bits sequentially into signals.
- There are different types of line coding but the most important in computer networks are:

A- Non Return to Zero Level (NRZL)

- NRZL encoding is polar that positive voltage is used to represent a binary 1 and negative voltage to represent a binary 0.
- Non return to zero means that the voltage never returns to a value of zero in the bit interval.
- While and the value of the voltage during a bit time is level.

B- Non Return to Zero Inverted (NRZI)

- NRZI is NRZ polar encoding scheme.
- the main difference here is that a transition at the beginning of the bit time is used to represent a 1 while a 0 is represented by no transition or no change. NRZI
- It offers better power balancing, and immunity to noise than NRZL.

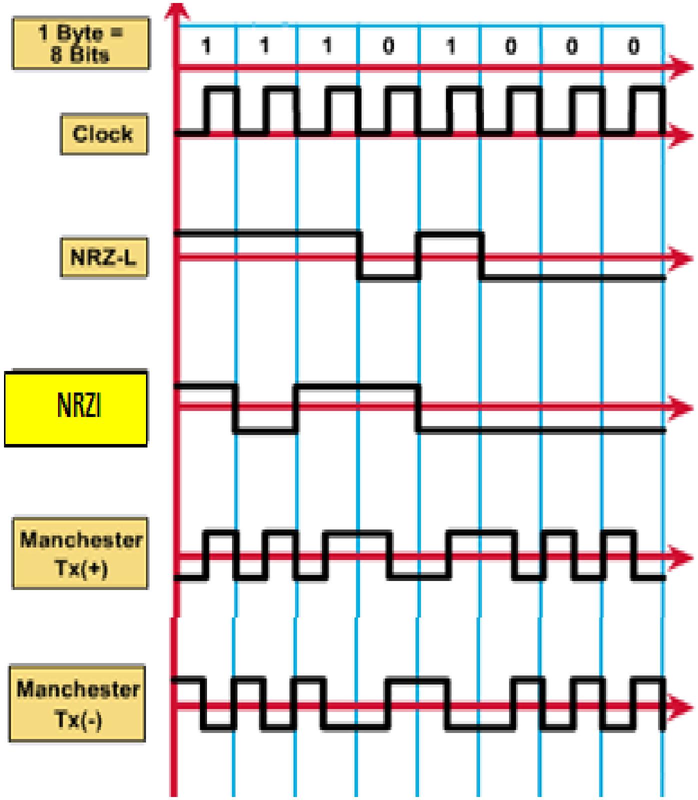
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

❖ Line Encoding

C- Manchester Encoding:-

- Manchester encoding is RZ (Return to Zero) biphase encoding scheme.
- RZ means that that voltage returns to zero in the middle of the bit interval.
- biphase referred to the two phases used to represent a 1 or 0 bit.
- Manchester encoding results in 1 being encoded as a low-to-high transition and 0 being encoded as a high-to-low transition.
- Clock can be effectively recovered at the receiver.
- Manchester encoding is more immune to noise.
- It is better at remaining synchronized
- It results in better elimination of low frequency components.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

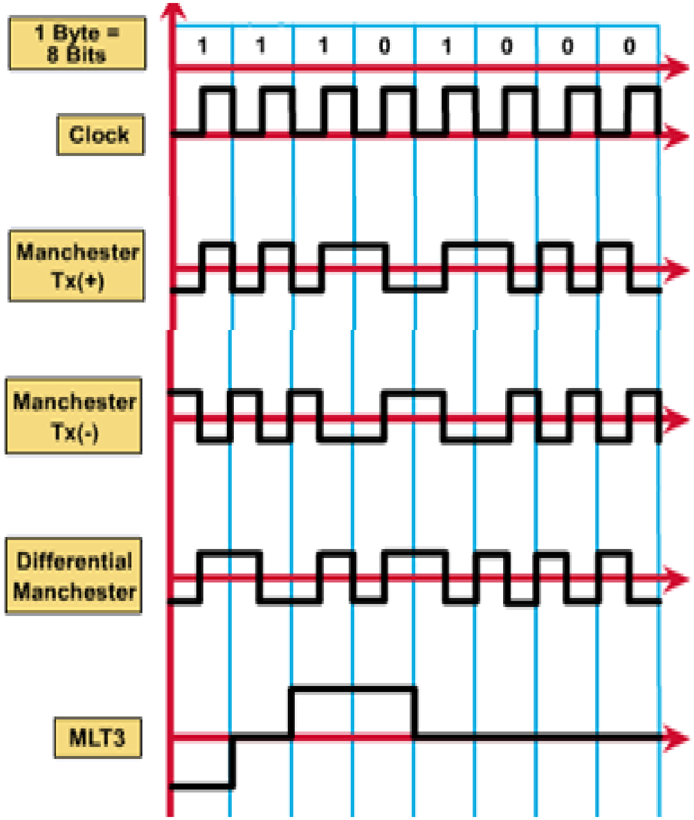
❖ Line Encoding

D- Differential Manchester Encoding:-

- it is a RZ biphase encoding scheme.
- 0 is represented by a transition at the beginning of the bit interval while no change (or transition) is used to represent a 1.

E- Multi-Level Threshold 3 (MLT3):-

- Three levels are used to represent the signal (-1 volt, 0 volt, +1 volt).
- These levels changes in cycle (-1,0,1,-1,0....).
- Logic 1 is represented by a transition to the next level in the cycle while no transition occurs in the case of zero.



Signals

❖ Block Encoding

- Block coding results in better error detection due to redundant codes.
- Specific codes can be used to start and end communication which helps in better synchronization than line coding.
- Block coding normally involves three stages :-
  - Division (dividing the stream of data into m-bit blocks)
  - Substitution (substitute the m-bit into appropriate n-bit block)
  - Combination (n- bit blocks are combined together to form a stream)

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Signals

Block Encoding

4 Binary/5 Binary (4B/5B) :-

- In this block coding method every four bits of data are encoded in a five-bit code.
- The selection of the five-bit code is done so that each code does not contain more than one leading zero and ends with no more than two trailing zeros. (So, no more than three consecutive zeros are encountered).
- 4B/5B block encoder always followed by line encoder (NRZI or MLT3) to maximize bit rate and eliminate low frequency components.

Data code		Definition
4-bits	5-bits	
0000	11110	Data0
0001	01001	Data1
0010	10100	Data2
0011	10101	Data3
0100	01010	Data4
0101	01011	Data5
0110	01110	Data6
0111	01111	Data7
1000	10010	Data8
1001	10011	Data9
1010	10110	DataA
1011	10111	DataB
1100	11010	DataC
1101	11011	DataD
1110	11100	DataE
1111	11101	DataF
	00000	Line is dead
	11111	Line is idle
	00100	Halt, transmission error
	11000	Delimiter for part 1 start of data stream
	10001	Delimiter for part 2 start of data stream
	01101	Delimiter for part 1 end of data stream
	00111	Delimiter for part 1 end of data stream

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The noise resulting from signals in adjacent cables is:

a- Thermal noise
b- AC power noise
c- Cross talk noise
d- None of the previous

Fiber optic losses that may result due to fabrication process is called

a- EMI/RFI loss
b- Absorption loss
c- Coupling loss
d- Conductor loss

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The code 00000 is used in 4B/5B encoding to describe

a- line halt
b- transmission error
c- idle line
d- dead line

One of the followings is not an active hub function

a- Packet filtering
b- Distributing the signal
c- Signal amplification
d- Signal reshape

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#6: Ethernet Part I

By: Laith W. Abdullah

Objectives

- Give a brief historic view of Ethernet evolution
- Present the physical layer specifications of Ethernet.
- Clarifying the format of Ethernet frame.
- Explains the addressing mechanism used by Ethernet
- List MAC address types

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

Till today Ethernet is one of the most popular LAN standards. Although its first document published before more than 30 years, it is still the most dominant LAN protocol mainly due to its simplicity and versions compatibility. Discussing Ethernet we will focus on the followings:

- **Evolution**
- **Physical layer specifications**
- **Frame format**
- **Media Access Control (MAC) mechanism.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

Evolution

- **DIX Ethernet:**
  - The oldest Ethernet standard
  - Work with RG8 coaxial cables
  - Developed by Digital Equipment Corporation, Intel, and Xerox.
  - Also called Thicket or 10Base5
  - first document was published in 1980.
- **The DIX Ethernet II**
  - published in 1982,
  - Use RG-58 coaxial cable.
  - This standard is called thin Ethernet, Thinnet, Cheapernet, or 10Base2.
- **IEEE 802.3**
  - Developed by Electrical and Electronic Engineers (IEEE)
  - published in 1985
  - Defines the previous standards plus other Ethernet physical layer standards including twisted pair and fiber optic cables with different transfer rates

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ Physical Layer Specifications

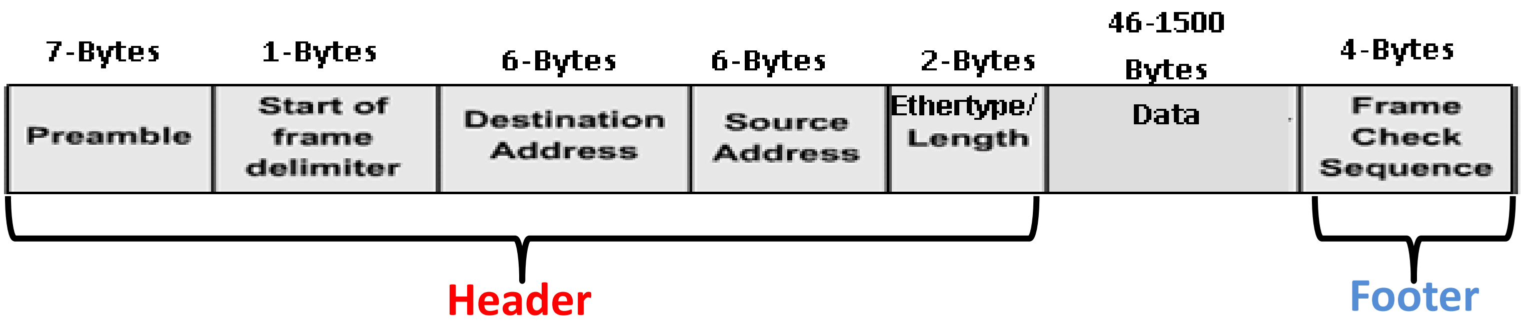
Ethernet (IEEE 802.3) comes in four basic types according to bandwidth, each of these types may specify one or more of Ethernet Desginations

Type	Designation	Cable Type	Physical Topology	Encoding	Maximum Segment Length
Standard Ethernet	10Base5	RG-8 coaxial	Bus	Manchester	500 m
	10Base2	RG-58 coaxial	Bus	Manchester	185 m
	10Base-T	Cat3, cat5 UTP	Star	Manchester	100 m
	10Base-F	Multimode fiber	Star	Manchester	100 m
Fast Ethernet	100Base-TX	Cat5, Cat5e, UTP	Star	4B/5B+MLT3	100 m
	100Base-FX	Multimode fiber	Star	4B/5B+NRZI	100 m
	100Base-T4	Cat3 UTP	Star	8B/6T	100 m
Gigabit Ethernet	1000Base-SX	Multimode fiber	Star	8B/10B+NRZL	550 m
	1000Base-LX	Singlemode fiber	Star	8B/10B+NRZL	5 km
	1000Base-CX	STP	Star	8B/10B+NRZL	25 m
	1000Base-T	Cat5e, Cat6 UTP	Star	4D-PAM5	100 m
10-Gigabit Ethernet	10GBase-S	Multimode fiber	Star	64B/66B	300 m
	10GBase-L	Singlemode fiber	Star	64B/66B	10 km

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ Frame Format



- **Preamble (7 bytes):**

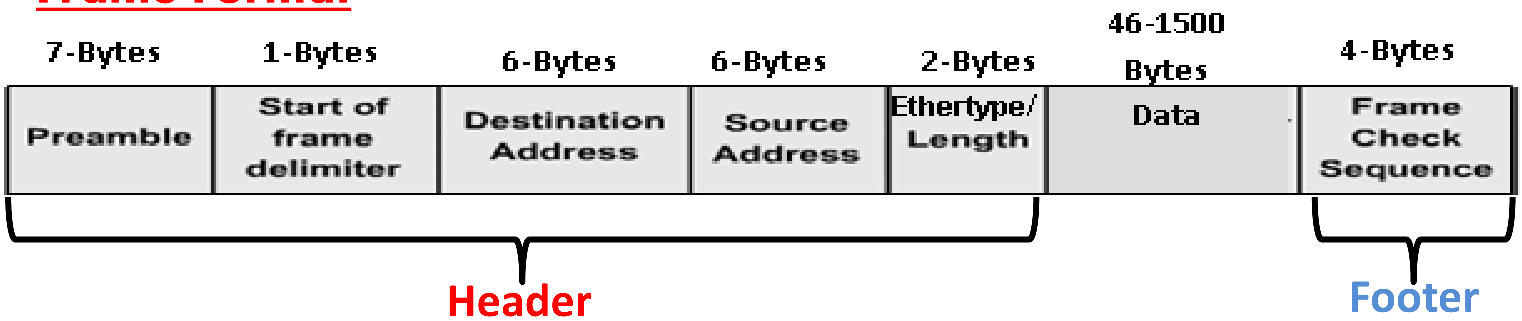
  This field contains 7 bytes of alternating 0s and 1s, which the communicating systems use to synchronize their clock signals.

- **Start Of Frame (1 byte):**

  This field contains 6 bits of alternating 0s and 1s, followed by two consecutive 1s, which is a signal to the receiver that the transmission of the actual frame is about to begin.

Ethernet

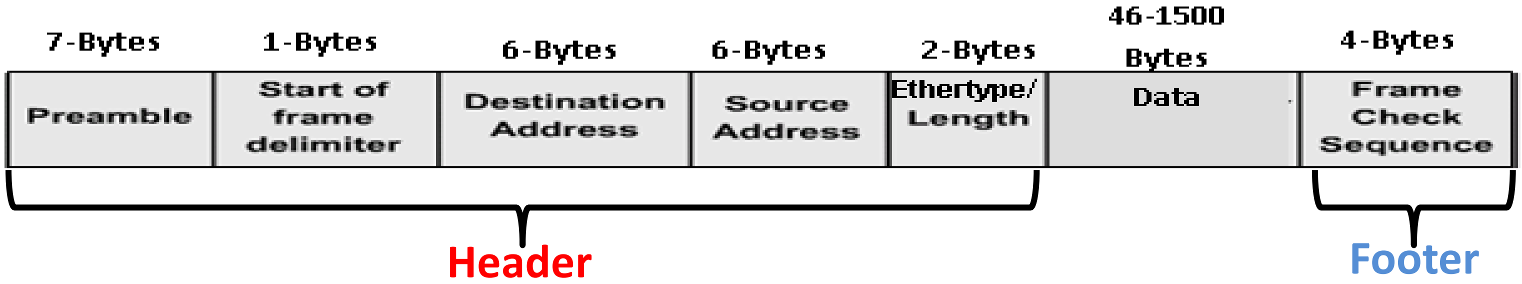
➢ Frame Format



- **Destination Address (6 bytes): This field contains the 6-byte hexadecimal address of the network interface adapter on the local network to which the packet will be transmitted.**
- **Source Address (6 bytes): This field contains the 6-byte hexadecimal address of the network interface adapter in the system generating the packet.**
- **Ethertype/Length (2 bytes): In the DIX Ethernet frame, this field contains a code identifying the network layer protocol for which the data in the packet is intended. In the IEEE 802.3 frame, this field specifies the length of the data field (excluding the pad).**

Ethernet

➢ Frame Format



- **Data And Pad (46 to 1500 bytes): This field contains the data received from the network layer protocol on the transmitting system. Ethernet frames (including the header and footer, except for the Preamble and Start Of Frame Delimiter) must be at least 64 bytes long; so if the data received from the network layer protocol is less than 46 bytes, the system adds padding bytes to bring it up to its minimum length.**
- **Frame Check Sequence (4 bytes): The Frame Check Sequence (FCS) field (4 bytes) is used to detect errors in a frame. It uses a cyclic redundancy check (CRC). The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors.**

Ethernet

Addressing

Regarded to addresses used in Ethernet, we will focus on three topics, these are:

- Address format
- Address transmission
- Addresses types

Address format:

- Each of the Destination Address and Source Address fields use a 6-byte hardware addresses.
- This address coded into network interface adapters to identify systems on the network.
- MAC addresses are written in hexadecimal notation using a hyphen (-) or column (:) to separate bytes from each other.

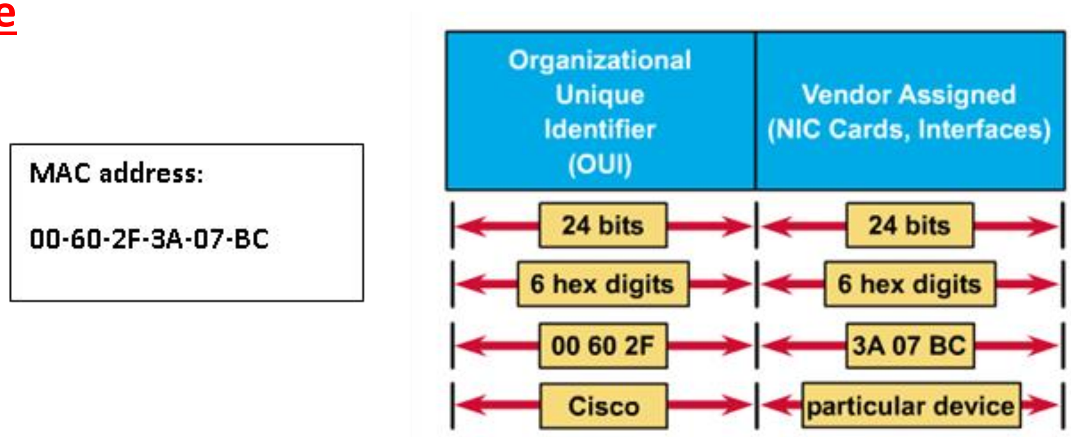
Ethernet

➤ Addressing

❖ Address format:

- Every network interface adapter has a unique hardware address (also called a Media Access Control(MAC) address, which consists of:
    - i. 3-byte (6-hexadecimal characters) value called an Organizationally Unique Identifier (OUI), which is assigned to the adapter's manufacturer by the IEEE
    - ii. 3-byte (6-hexadecimal characters) value assigned by the manufacturer itself.

- Example



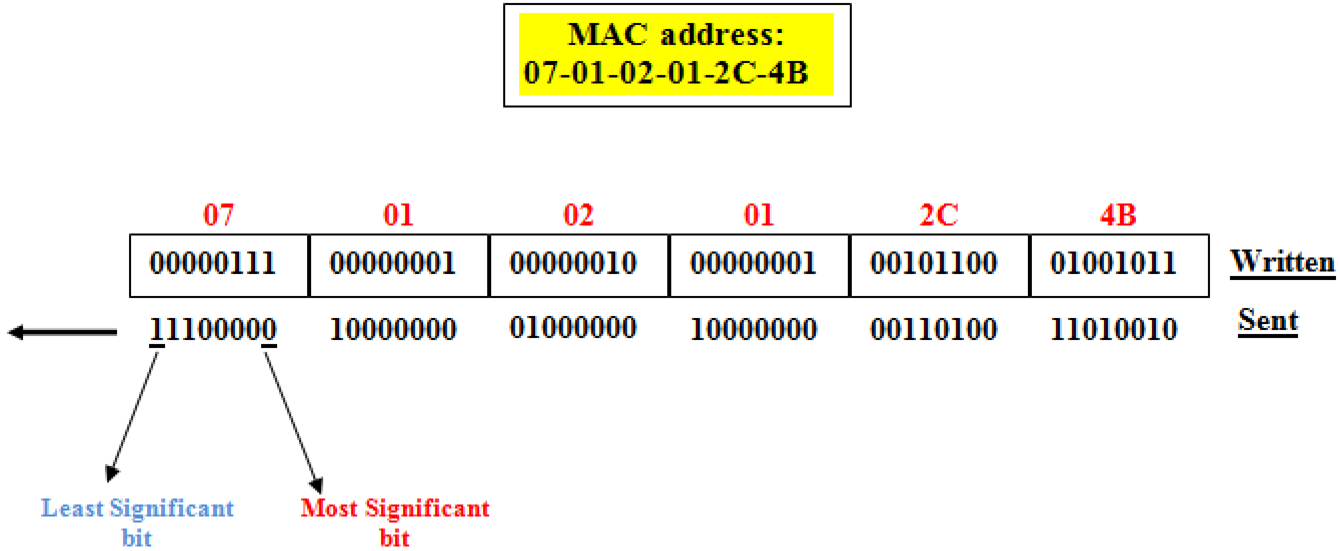
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ Addressing

❖ Address Transmission:

The way MAC addresses are sent is different from the way they are written. The transmission is left to right byte by byte starting with the least significant bit in each byte.



Ethernet

➢ Addressing

❖ Types of addresses

MAC addresses can be divided into unicast, multicast, and braodcast addresses.

- **Unicast address:**

  It is dedicated for single node, source address is of course a unicat address, but destination address can be unicast, multicast or broadcast.

- **Multicast address:**

  Multicast destination address defines a group of nodes. If the first bit to be transmitted is one, the MAC address is multicast.

- **Broadcast address:**

  It a special multicast address consists of 48 ones (FF-FF-FF-FF-FF-FF). in case of broadcast destination address the recipient are the nodes in the network.

Ethernet

➢ Addressing

- **Example**

Multicast MAC address: 07-01-02-01-2C-4B

	07	01	02	01	2C	4B	
	00000111	00000001	00000010	00000001	00101100	01001011	Written
←	11100000	10000000	01000000	10000000	00110100	11010010	Sent

Least Significant bit (the first bit, 1, of 11100000) — Most Significant bit (the last bit, 0, of 11100000)

Unicast MAC address: 06-01-02-01-2C-4B

	06	01	02	01	2C	4B	
	00000110	00000001	00000010	00000001	00101100	01001011	Written
←	01100000	10000000	01000000	10000000	00110100	11010010	Sent

Least Significan bit (the first bit, 0, of 01100000) — Most Significant bit (the last bit, 0, of 01100000)

???? Quiz ????

One of the following is an Ethernet designations that utilizes fiber optics

a- 10BaseT
b- 10Base F
c- 100BaseC
d- 100Base-F

Ethernet station that wants to broadcast a frame

a- uses the address FF:FF:FF:FF:FF:FF for both frame’s source and destination fields.
b- uses the address FF:FF:FF:FF:FF:FF for frame’s source destination field.
c- uses the address FF:FF:FF:FF:FF:FF for both frame’s destination fields.
d- uses the address FF:FF:FF:EE:FF:FF for both frame’s source and destination fields.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Ethertype field used in Ethernet DIX II frame for

a- error detection
b- describe the type of Ethernet.
c- synchronization
d- Identifying network layer protocol

To detect frame's errors, Ethernet depends

a- CRC
b- FEC
c- FFT
d- BER

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#7: *Ethernet Part II*

By: *Laith W. Abdullah*

Objectives

- List the persistence strategies followed in Ethernet MAC mechanism.
- Explain the main phases of CSMA/CD as the MAC mechanism of Ethernet.
- Define time slot concept and how it affects the MAC of Ethernet
- Define Jam signal and the role it plays in collision detection phase.
- Presents the importance of Backoff time and how it can be calculated.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

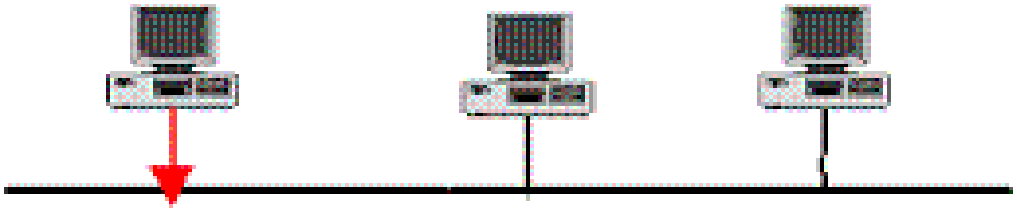
CSMA/CD

- The MAC mechanism followed by Ethernet is called Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
- MAC mechanism defines who and how node can access the medium.
- MAC mechanism is one of the main jobs to be carried out by Data-link layer protocol.
- CSMA/CD is a contention based mechanism means that the stations may compete to access the medium
- As the name implies the MAC mechanism of Ethernet is basically pass through three phases
    - Carrier Sense
    - Multiple Access
    - Collision Detection

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

- **Carrier Sense:**
  - **The station that has data to transmit first listens to the network to see if it is idle, this is the carrier sense phase.**
  - **Upon the case of the network "idle" or "busy" CSMA/CD defines what should the station do in what is called "Persistence strategy".**
  - **Persistence strategies can be divided into three types:**
    - **Non persistence**
    - **1 – persistence**
    - ***p* - Persistence**



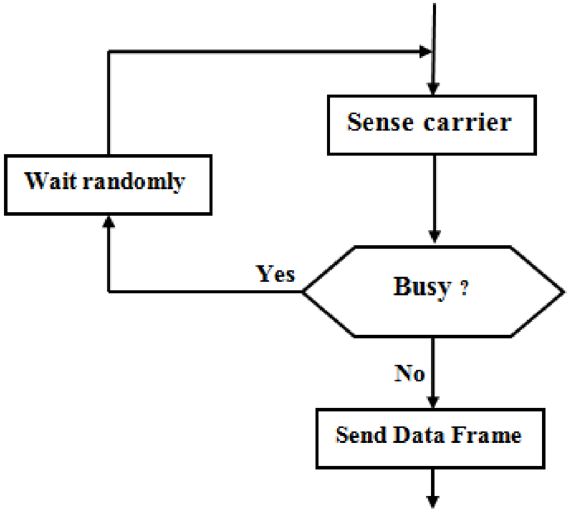
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

➢ Carrier Sense:

❖ Non-persistence:

Here the station senses the line, if it is idle it sends immediately. If the line busy; it waits a random time then senses the line again. Even random wait time reduces the chance of collision but it also reduces network efficiency.



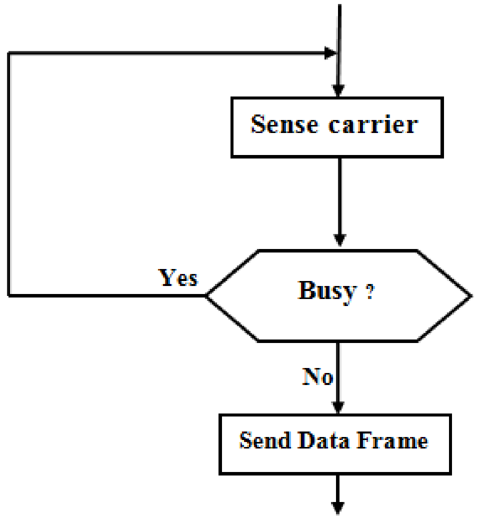
Non-persistence flow diagram

CSMA/CD

➢ Carrier Sense:

❖ 1-Persistence:

here, after the station finds the line idle, it sends its data immediately (with probability 1). This method increases the chance of collision.



1-persistence flow diagram

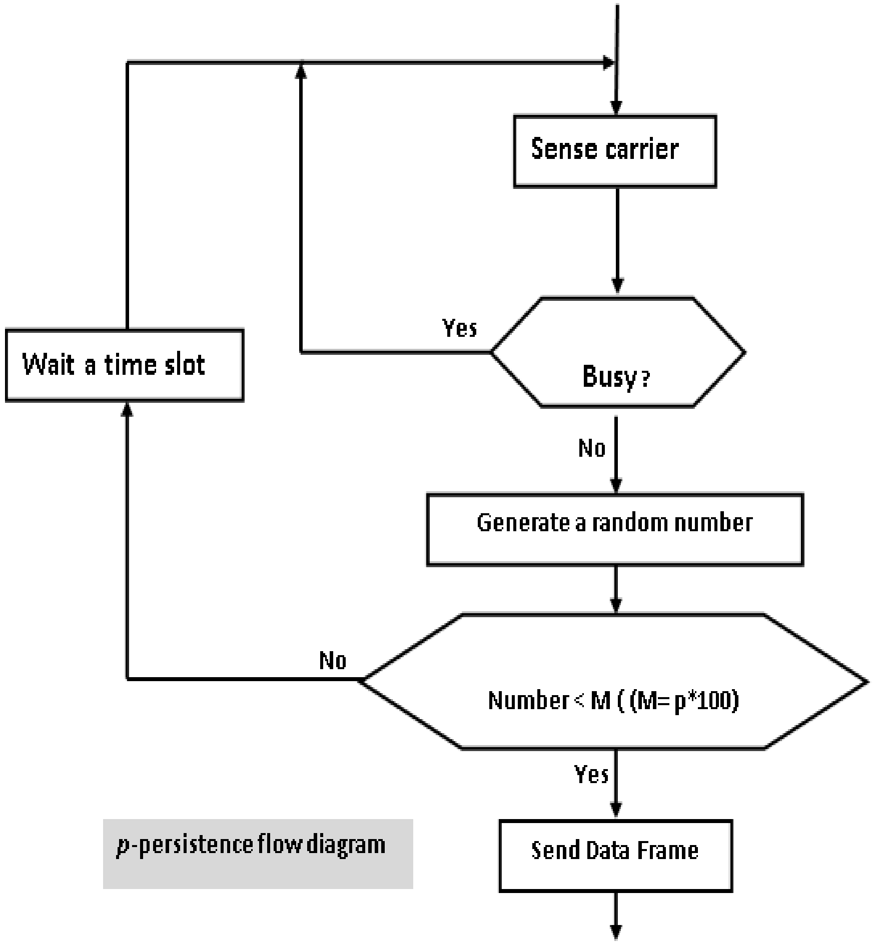
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

➢ Carrier Sense:

❖ *p*-Persistence:

- in this strategy after the station finds the line idle, it may or may not sends its data. Here the probability of sending is defined by ***p*** and probability of refraining is ***(1-p)***.
- This method reduces the chance of collision and increases network efficiency.

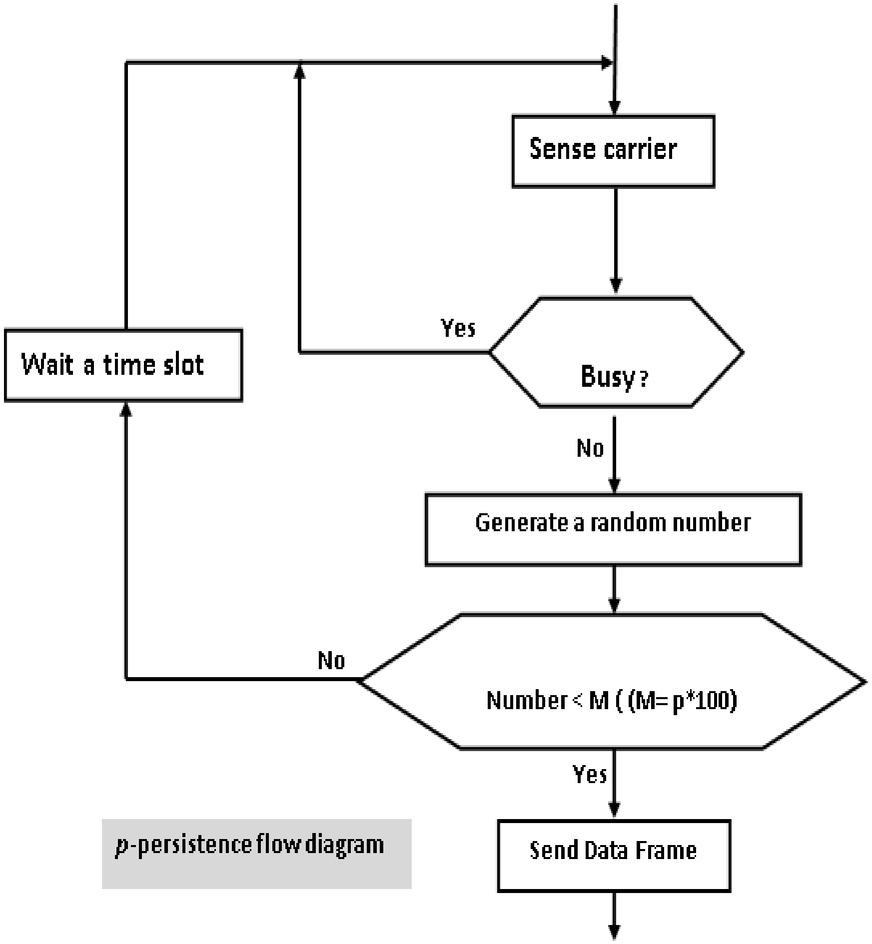


p-persistence flow diagram

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

- *p*-Persistence:
- **Example**:
  - if *p=0.3* ,
  - The station sends with 30% of the time and refrains 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.



p-persistence flow diagram

CSMA/CD

➢ Slot Time:

- This factor plays an important role in the MAC mechanism of Ethernet, this factor affects both carrier sense and collision detection phases
- it is the time occupied by the minimum length of an Ethernet frame (512 bit in standard and fast Ethernet).
- It depends on the bit time, so it varies with the type of Ethernet.

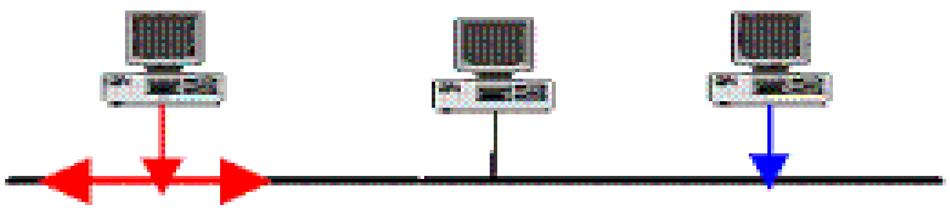
Ethernet type	Bandwidth	bit time	Slot time
Standard Ethernet	10Mbps	100 ns	51.2 micro s
Fast Ethernet	100Mbps	10 ns	5.12 micro s

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

➢ Multiple Access

- CSMA/CD is a contention access method.
- Because all of the stations on the network are contending for access to the same network medium this phase is called the multiple access phase.



➢ Collision Detection

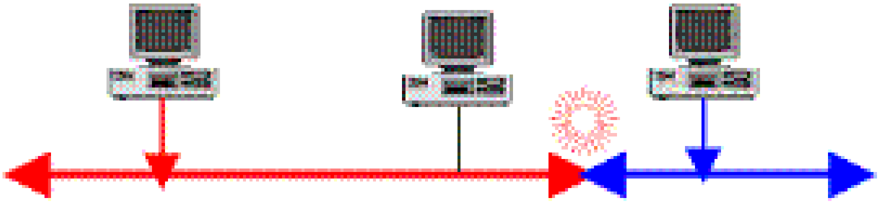
- Even though an initial check is performed during the carrier sense phase, it is still possible for two systems on the network to transmit at the same time, causing a collision.
- If the systems can't tell when their packets collide, corrupted data may reach the destination system and be treated as valid.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

Collision Detection

- As long as a computer is still in the process of transmitting, it is capable of detecting a collision on the network.
  - On a UTP or fiber optic networks
    A computer assumes that a collision has occurred if it detects signals on both its transmit and receive wires at the same time.
  - On a coaxial Ethernet networks
    a voltage spike indicates the occurrence of a collision. If the network cable is too long or if the packet is too short, the probability of collision increased.

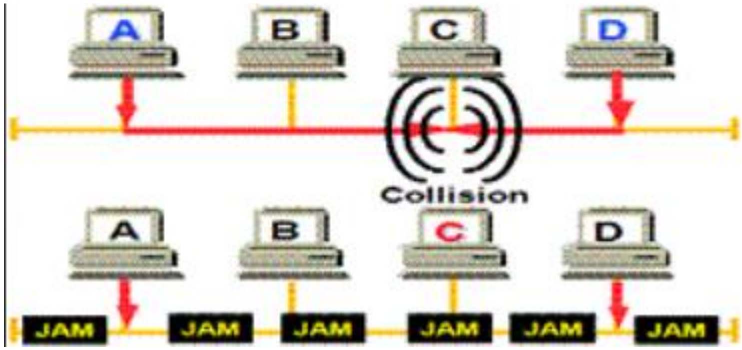


CSMA/CD

Collision Detection

Jam signal

- When a system detects a collision, it immediately stops transmitting data and starts sending a jam pattern instead.
- The jam pattern serves as a signal to each system on the network that a collision has taken place, that it should discard any partial packets it may have received, and that it should not attempt to transmit any data until the network has cleared.
- Jam pattern consists of 32-bit string of alternating 0s and 1s.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

Collision Detection

Backoff time

- After transmitting the jam pattern, the system waits a specified period of time before attempting to transmit again. This is called the Backoff time.
- Both of the systems involved in a collision compute the length of their own backoff periods using a randomized algorithm called "Truncated Binary Exponential Backoff". They do this to try to avoid causing another collision by backing off for the same period of time.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

➢ Collision Detection

❖ Backoff time calculation:

i. Each station wants to transmit set a parameter called backoff parameter "*k*" to zero.

ii. It follows a persistence strategy and if the line is idle the station sends its data.

iii. After sending its data the station keeps monitoring the line. In case of collision the station sends a jam signal, increase *"k"* by one *(k=k+1)*, then calculating backoff period as:

Backoff time= $R \times$ slot time

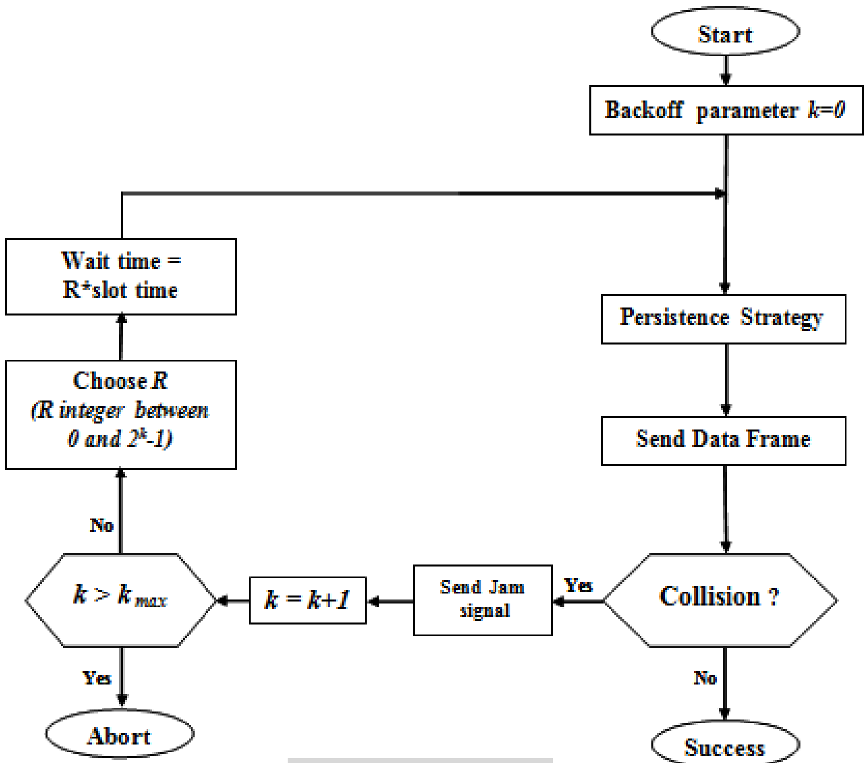
Where R : Random number between *0* and 2^k-1

iv. When the station detects another collision it repeats this procedure until k reaches a predefined value "kmax" (usually $k_{max} = 15$), here the station give up and aborts trying to send its data

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

CSMA/CD

➢ **Collision Detection**



CSMA/CD flow diagram

CSMA/CD

➢ Collision Detection

Example:

In a Standard Ethernet network, a station detects a collision and succeed to send its data after two tries. Find the possible backoff times for each try.

Sol:

- **In Standard Ethernet slot time = 51.2 micro sec**
- **now the backoff time can be calculated as follows:**

Try	k	2^k-1	range	Backoff time (micro sec)
1	1	1	0 to 1	0 or 51.2
2	2	3	0 to 3	0, 51.2, 102.4, or 153.6
3	N/A	N/A	N/A	N/A

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

the persistence strategy by which the Ethernet station sends without any wait is called

a- 1-persistence
b- Wait-persistence
c- p-persistence
d- No-persitence

The time of transmitting 512 bits in Ethernet is called

a- Backoff time
b- slot time.
c- wait time
d- idle time

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

As an Ethernet station that detects a collision it

a- sends its data
b- waits a random time.
c- retransmits its data
d- sends jam pattern

Jam signal is

a- 32 Bytes of alternating 1’s and 0’s
b- 32 Bytes of alternating 1’s
c- 23 Bits of alternating 1’s and 0’s
d- non of the previous

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#8: Ethernet Part III

By: Laith W. Abdullah

Objectives

- Present the main difference in the format of Ethernet DIX II and IEEE 802.3 Ethernet frames.
- Define the LLC and MAC sublayers of the Data-link layer.
- List some of the special packets in Ethernet with their role and format.
- Explain how the value of the FCS field of Ethernet is calculated.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ Identifying Upper Layer Protocol

The 2-byte field after the Source Address field is the primary difference between the DIX Ethernets and IEEE 802.3 standards.

7-Bytes	1-Bytes	6-Bytes	6-Bytes	2-Bytes	46-1500 Bytes	4-Bytes
Preamble	Start of frame delimiter	Destination Address	Source Address	Ethertype/ Length	Data	Frame Check Sequence

❖ For DIX Ethernet II

This field identifies which network layer protocol has generated the data in a particular packet using values like those shown in the following table .

Network Layer Protocol	Ethertype value (hexadecimal)
Internet Protocol (IP)	0800
Internetwork Packet Exchange (IPX)	8137

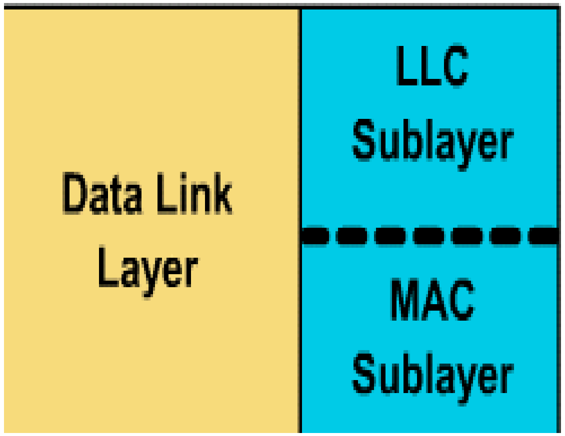
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ Identifying Upper Layer Protocol:

❖ For IEEE 802.3 Ethernet

- This field specifies the length of the data field in the frame.
- Data-link layer is split into two sublayers;
  - MAC (Media Access Control) is the part that contains the elements particular to the IEEE 802.3 specification, such as the Ethernet physical layer options, the frame, and the MAC mechanism.
  - LLC (Logical Link Control) One of the main functions of the LLC sublayer is to define the network layer protocol. LLC is achieved by an additional 8-9 byte subheader that is carried within the Data field. This 8-9 byte subheader contains 2-byte field called Local Code that performs the same function as the Ethertype field in the Ethernet II header



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

- **Special Packets**:

  - **Pause Packet**:
    - **Pause packet is used to slow down the flow of data frames between two devices at the ends of Ethernet full-duplex link.**
    - **This mechanism overcomes a temporary overload condition and not to prevent long or continuous congestion.**
    - **Pause packet depends a simple flow control method called "stop-start“.**
    - **The station sends the pause packet causes the other end station to stop for a period called “wait time”.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ Special Packets:

❖ Pause Packet:

- Even the paused station stops sending its data for the period of "wait time" it can still sending pause packets.
- The last pause packet cancels the previous one. So, the station can ask to increase, decrease, or eliminate wait time.
- Pause Packet Format
  - Code (2 Bytes): it is usually contains the hexadecimal code (0001).
  - Wait parameter (44 Bytes): this field used to find the wait time which is the multiplication of the value in the wait parameter field by the slot time.

2B	44 B
Code	Wait Parameter

Ethernet

- **Special Packets**:

  - **Auto Negotiation**
    - **Auto negotiation is a feature added to fast Ethernet networks.**
    - **End and/or intermediate devices can use auto negotiation to decide the mode of transmission (half-duplex or full duplex) and the bandwidth (10Mbps or 100Mbps).**
  - **Auto negotiation rules:-**
    1) **Two devices should be connected in a point-to-point link.**
    2) **Negotiation covers only the link not the whole network.**
    3) **Negotiation can occur only during link initialization.**
    4) **Negotiation use separate frame format.**
    5) **Each device in the link offers its capabilities for the other device.**
    6) **Decision is based on common capabilities.**

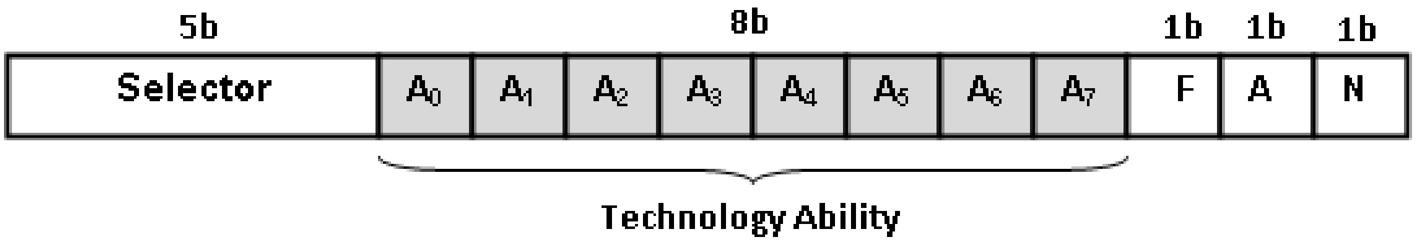
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ **Special Packets**:

❖ **Auto Negotiation**

- **Frame format:**

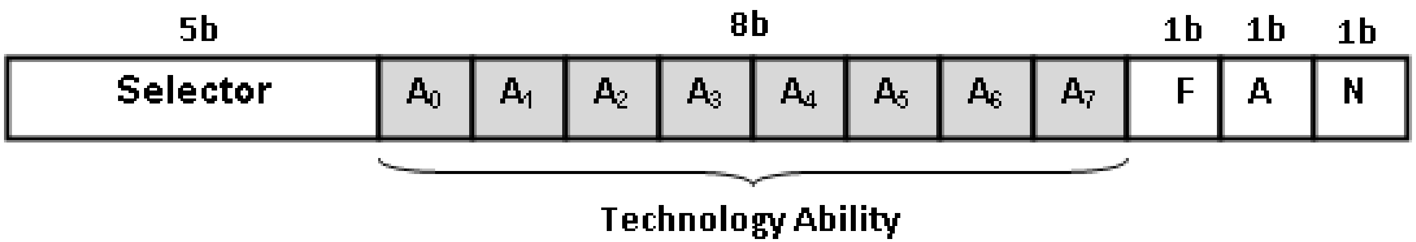


- **Selector (5b): this field used to describe the type of LAN. The code for Ethernet LANs is (10000).**
- **Fault (1b): this bit when set announces that a fault has been occur.**
- **Acknowledged (1b): this bit when set indicates that the auto negotiation frame has received successfully.**
- **Next Page (1b): this bit when set indicates that there is another negotiation frame coming.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

- **Special Packets**:
  - **Auto Negotiation**
  - **Frame format:**



- **Technology Ability (8b):**
  a device advertising its capabilities can set one or more of the bits in this field.

Bit	Supported Technology
A_0	10Base-T
A_1	10Base-T full-duplex
A_2	100Base-TX
A_3	100Base-TX full-duplex
A_4	100Base-T4
A_5	Pause Operation
A_6	Reserved
A_7	Reserved

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

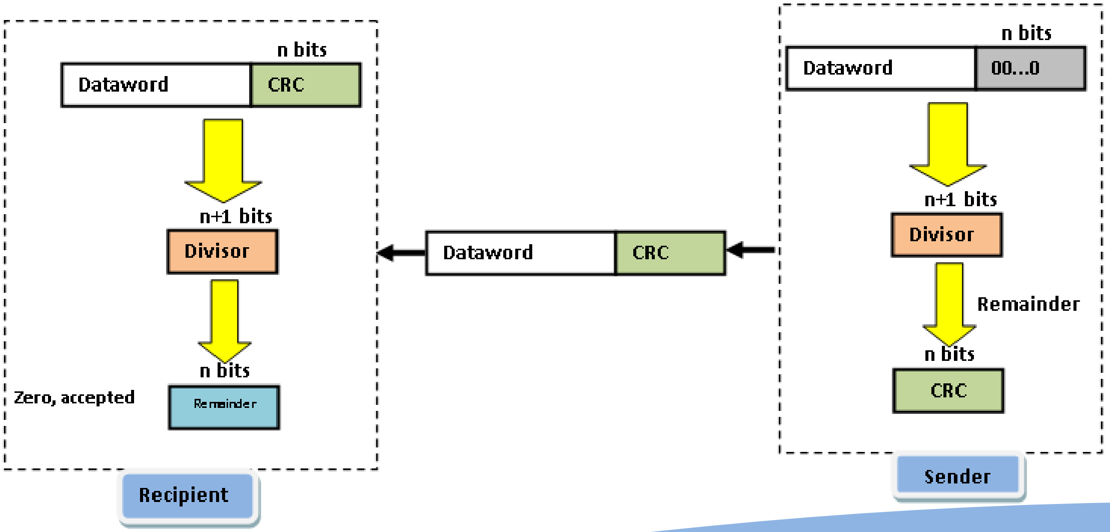
➢ **CRC**:

7-Bytes	1-Bytes	6-Bytes	6-Bytes	2-Bytes	46-1500 Bytes	4-Bytes
Preamble	Start of frame delimiter	Destination Address	Source Address	Ethertype/ Length	Data	Frame Check Sequence

- **It is an error detection method by which a sequence of redundant bits called "CRC" or "CRC remainder" is appended to the end of a data word.**
- **It is used in the footer FCS field in Ethernet.**
- **Even Ethernet station can detect an error, but Ethernet protocol is not capable to ask the sender to retransmit the data. This task is left to upper layer protocols.**
- **Ethernet station that detects an error in received frame simply discards that frame.**

Ethernet

- **CRC**:
  - **CRC calculation**
    - A predetermined divisor called the "generator" is used to achieve the CRC.
    - First the dataword is appended by a specific number of zeros equals the length of the divisor minus one.
    - Then it is divided by the generator.
    - The reminder of the division process is the CRC which is appended to the dataword and sent.



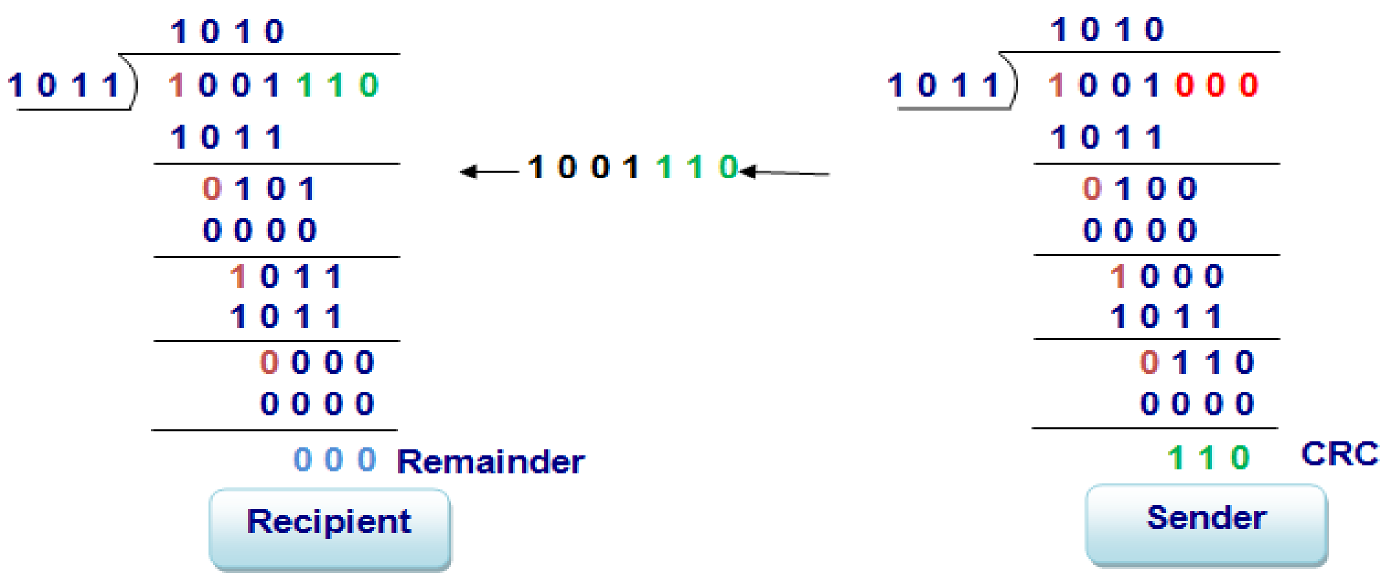
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

- **CRC**:

Example:

Using the generator (1011), the data word (1001), the sender and the recipient handles CRC calculation and checking as follows.



Notes

1- Addition used in CRC generation and CRC verification is module-2 addition.

2- Division used here is binary division.

Ethernet

- **CRC**:

Polynomials

To simplify the process of finding the CRC of binary data word. The data word and the generator can be written as polynomials as follows. As follows

$$b_n x^n + \ldots\ldots\ldots\ldots\ldots + b_2 x^2 + b_1 x^1 + b_0 x^0$$

where b_n can be 0 or 1

it should be noticed that the degree of polynomial to represent n-bit binary word is *(n-1)*.

Note

Ethernet uses CRC-32 , the generator polynomial is

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

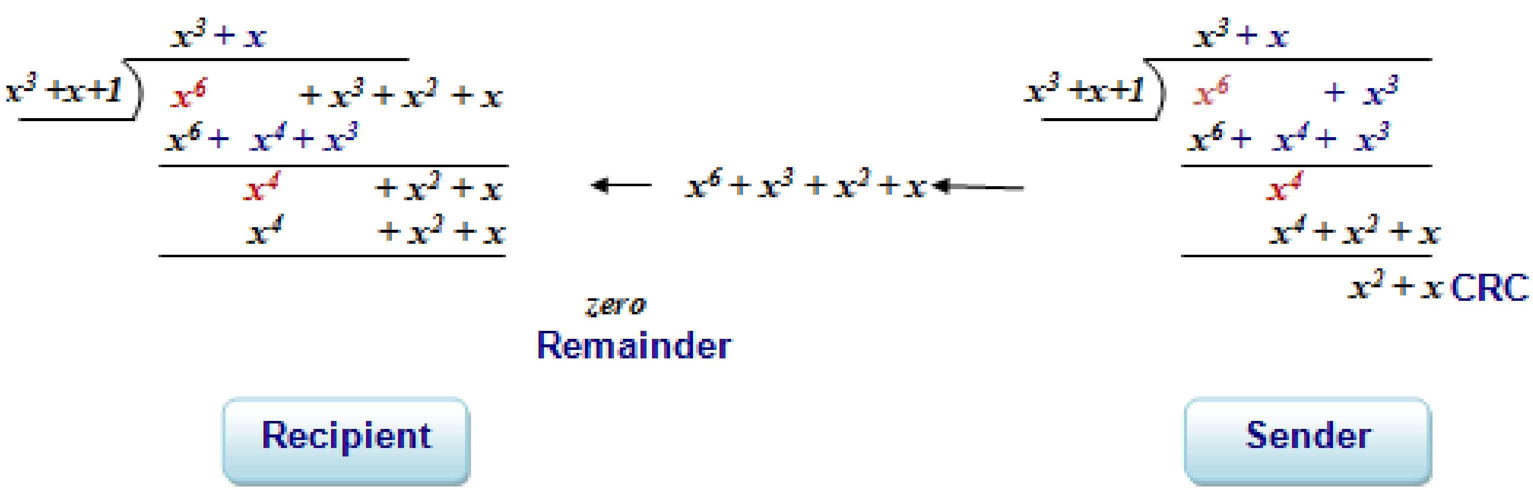
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Ethernet

➢ CRC:

Example: Using the generator (1011), the data word (1001). Find how the sender and the recipient handles CRC calculation in a polynomial form.

Sol : The data word must be appended with three zeros, so it comes(1001000) and it is written in polynomial form (x^6+x^3). The generator is written in the form (x^3+x+1).



???? Quiz ????

the flow control mechanism depended by pause packet is called

a- stop-start
b- wait-stop
c- just stop
d- start-wait

Ethernet frame that is failed in CRC check is

a- acknowledged
b- repeated
c- discarded
d- asked to be re-transmitted

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

the field used to identify upper layer protocol in IEEE802.3 frame is called

a- local code
b- ethertype.
c- IP code
d- LLC code

The rank of polynomial used to calculate CRC in Ethernet is

a- 32
b- 31
c- 8
d- non of the previous

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#9: *WLAN Part I*

By: *Laith W. Abdullah*

Objectives

- List the currently used WLAN standards.
- Explain the architecture of IEEE802.11 WLAN.
- Explain the signaling schemes used in WLANs
- Present Antenna types used in WLANs and Discuss some of the important concepts related to these antennas.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

- The main advantages to use WLANs are:
  - Mobility
  - Low cost
  - Simplicity
- While the main challenges are
  - Security
  - Interference
- The Wireless Local Area Network (WLAN) technology is defined by the IEEE 802.11 family of specifications.
- Currently, the four specifications in use are:
  - IEEE 802.11a
  - IEEE 802.11b
  - IEEE 802.11g
  - IEEE 802.11n

WLAN

➢ Physical Layer Specifications:

❖ Topologies

- **Ad-hoc :**

  The ad- hoc topology is one in which computers equipped with wireless network interface adapters communicate directly with each other;. This type of network is designed to support only a limited number of computers, such as those in a home or small business.

WLAN NIC

- **Infrastructure:**

  it is designed to extend the range and flexibility of a normal cabled network by enabling wireless-equipped computers to connect to it using a specialized module called an access point.

Access Point

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

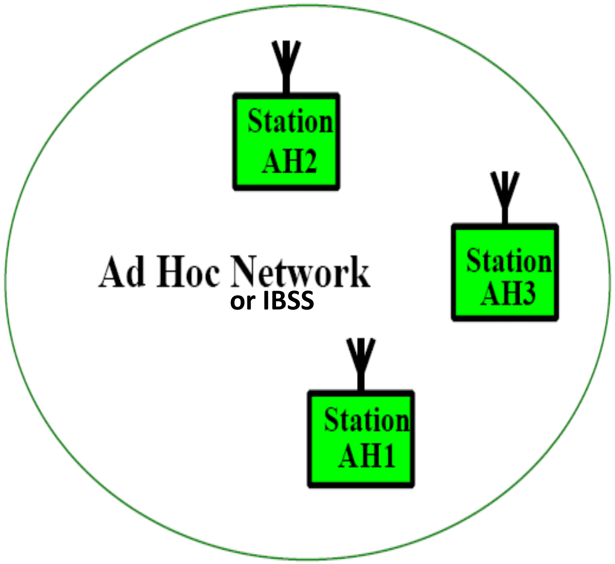
WLAN

➢ Physical Layer Specifications:

❖ Architecture

a- Basic Service Set (BSS)

- Basic Service Set (BSS) consists of two or more wireless nodes, or stations (STAs), which have recognized each other and have established communications.
- BSS can be considered as the fundamental building block of the IEEE 802.11 standards architecture.
- BSS can be independent as in ad hoc networks thus it is called IBSS.
- In most instances BSS operates in the infrastructure topology so the stations are controlled by an access point.
- The geographical area covered by the BSS is known as the Basic Service Area (BSA)



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

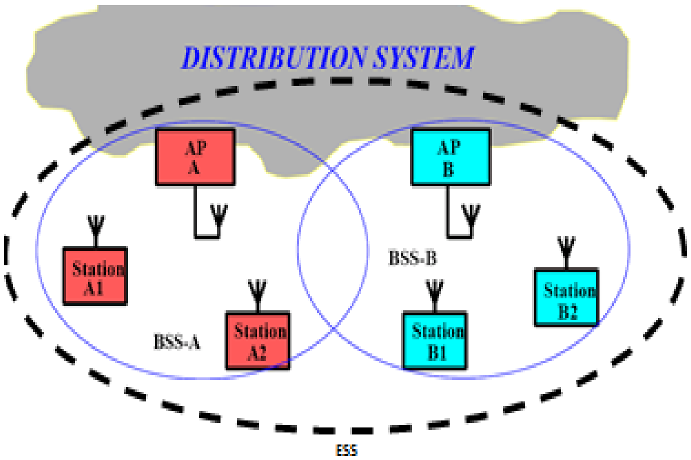
WLAN

➢ Physical Layer Specifications:

❖ Architecture

b- Extended Service Set (ESS)

- **In Infrastructure networks APs covers BSSs. AP also supports range extension by providing connectivity between multiple BSSs, thus forming what is known as Extended Service Set (ESS).**
- **The ESS consists of a series of overlapping BSSs (each containing an AP) connected together by means of a Distribution System (DS).**



c- Distribution System (DS)

- **The DS can be thought of as a backbone network.**
- **The DS, as specified by IEEE 802.11, is implementation independent.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

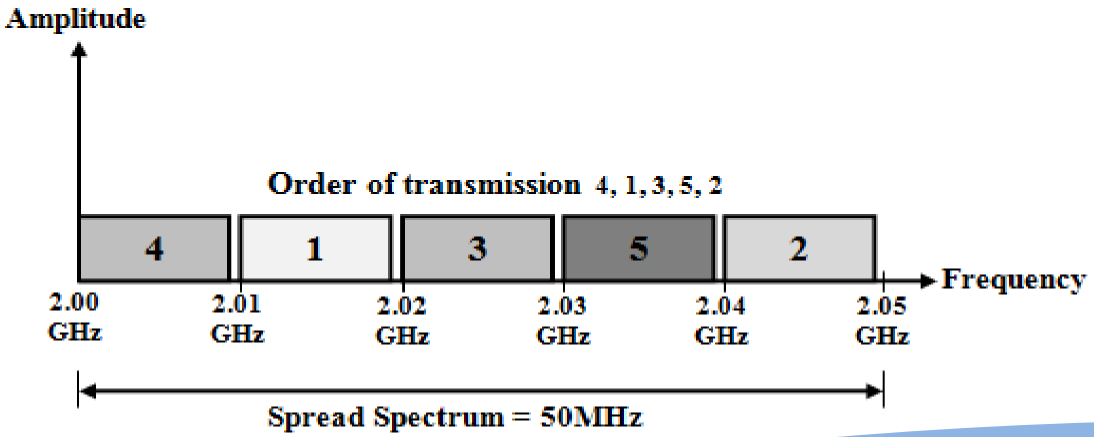
WLAN

➢ Physical Layer Specifications:

❖ Signaling Schemes

a - Frequency Hopping Spread Spectrum (FHSS):

- The transmitter continuously performs rapid frequency shifts or hops according to a preset algorithm.
- Hopping periods are equal and for N hopping periods the cycle is repeated.
- If the bandwidth of the original signal is B, the bandwidth of the new signal is spread to N× B.
- The receiver performs the exact same shifts to read the incoming signals.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

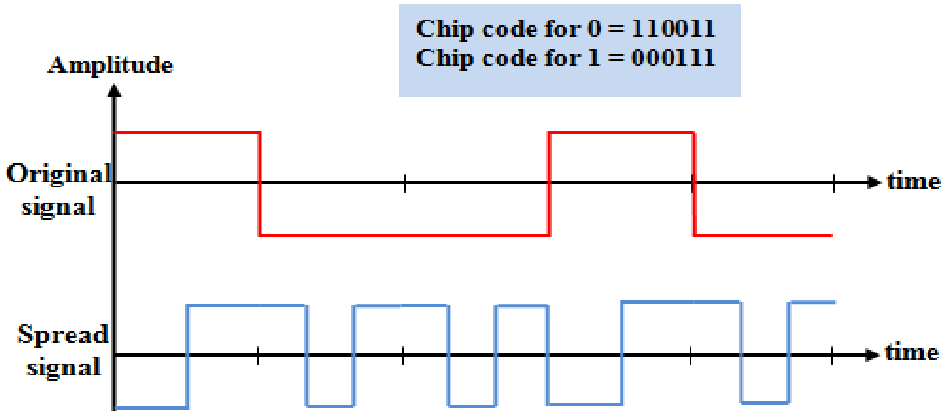
WLAN

➢ **Physical Layer Specifications:**

❖ Signaling Schemes

b - Direct Sequence Spread Spectrum (DSSS):

- The outgoing signals are modulated using a digital code called "chip code".
- The time taken by a bit in the original signal equals the time of the whole chip code.
- if N-bit chip code is used to spread a signal of bandwidth B the new bandwidth needed is N× B.
- WLANs use an 11-bit chipping code called "Barker Sequence".



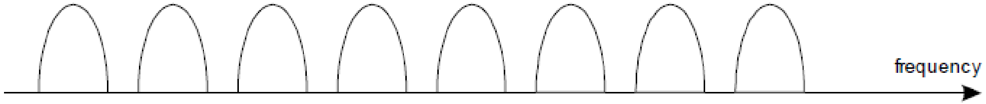
WLAN

Physical Layer Specifications:

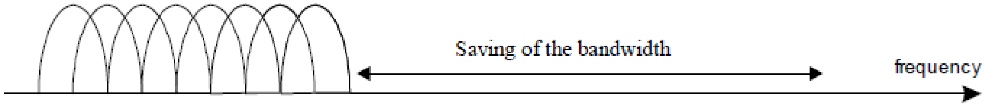
Signaling Schemes

c - Orthogonal Frequency Division Multiplexing (OFDM):

This method effectively squeezes multiple modulated carriers tightly together, reducing the required bandwidth but keeping the modulated signals orthogonal so they do not interfere with each other.



Conventional Frequency Division Multiplex (FDM) multicarrier modulation technique



Orthogonal Frequency Division Multiplex (OFDM) multicarrier modulation technique

d- Infrared (IR):

Infrared communications use high frequencies, just below the visible light spectrum. Infrared is a "line of sight" technology, meaning that the signals cannot penetrate through opaque walls and objects.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

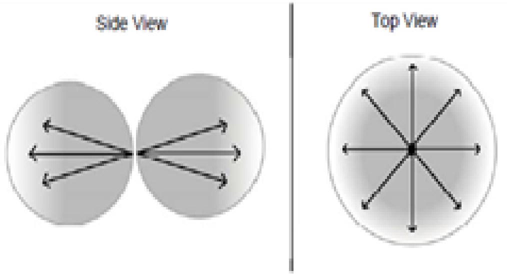
WLAN

➢ Physical Layer Specifications:

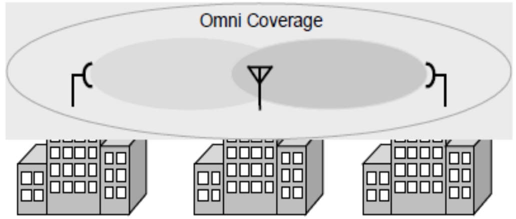
❖ Antenna Types

1- Omni-directional antenna:

- The most common wireless LAN antenna is the omni-directional antenna which is standard equipment on most access points
- Omni-directional antenna, radiates its energy in all directions around its axis.
- Usage:
  - Indoor: in the center of a single floor of a ground or multistory building
  - Outdoor: with an omni-directional antenna being placed on top of a structure (such as a building) in the middle of the coverage area.



Point-to-multipoint link



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

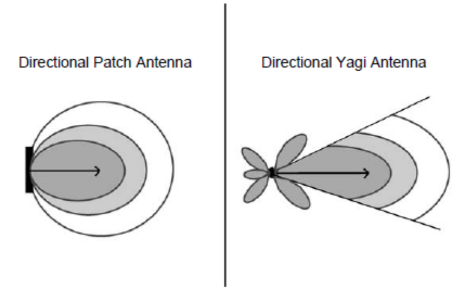
➢ Physical Layer Specifications:

❖ Antenna Types

2- Semi-directional Antennas

- Common semi-directional antennas types frequently used with wireless LANs are
  - Patch
  - Panel
  - Yagi
- These antennas direct the energy from the transmitter significantly more in one particular direction.
- Usage:
  - **Indoor:** In a large indoor space, if the transmitter must be located in the corner or at the end of a building, a corridor, or a large room,
  - **Outdoor:** semi-directional antennas are commonly used outdoor as a point-to-point link between two sites.

Coverage area of a semi-directional antenna



Point-to-point link using semi-directional antennas

WLAN

- **Physical Layer Specifications:**
- Antenna Types

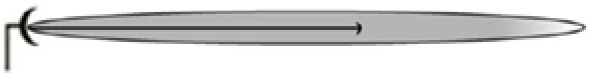
3- Highly-directional Antennas

- Highly-directional antennas emit the most narrow signal beam of any antenna type and have the greatest gain of these three groups of antennas.
- Highly-directional antennas are typically concave devices. Some are:
- parabolic dishes while others are grid antennas
- Usage: These antennas are ideal for long distance, point-to-point wireless links.

Highly-directional Parabolic dish antenn:

Highly-directional Grid antenna

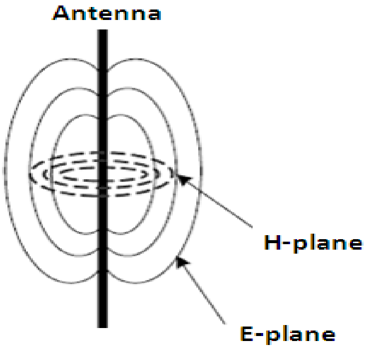
Radiation pattern of a highly-directional antenna



WLAN

Physical Layer Specifications:

Antenna Concepts



a- Polarization:

Antennas that are not polarized in the same way are not able to communicate with each other effectively.

b- Gain:

The higher the antenna gain (measured in dBi), the farther the wave will travel.

c- Free Space Path Loss:

Free Path Loss represents the single greatest source of loss in a wireless system. The formula for Path Loss (in dB) is:

$$PathLoss = 20LOG_{10}\left[\frac{4\Pi d}{\lambda}\right]$$

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

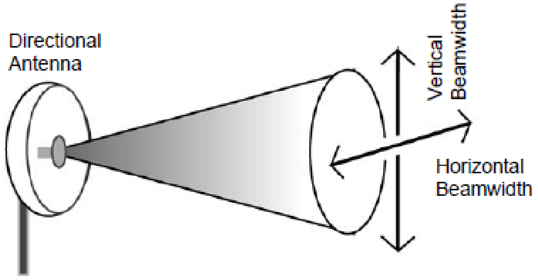
WLAN

➢ Physical Layer Specifications:

❖ Antenna Concepts

e-Beamwidth:

There are two vectors to consider when discussing an antenna's beamwidths (measured in degrees): the vertical and the horizontal.



Antenna Type	Horizontal Beamwidth (in degrees)	Vertical Beamwidth (in degrees)
Omni-directional	360	Ranges from 7-80
Patch/Panel	Ranges from 30-180	Ranges from 6-90
Yagi	Ranges from 30-78	Ranges from 14-64
Parabolic Dish	Ranges from 4-25	Ranges from 4-21

???? Quiz ????

The formal name of ad hoc WLAN

a- IPTP
b- IBSS
c- DSSS
d- IDS

10MHz signal is spreaded by 10-hop FHSS to

a- 1 GHz
b- 100 MHz
c- 10 GHz
d- 1 Gbps

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Omni directional antenna

a- radiates its energy 180 degrees around its axis
b- radiates its energy 360 degrees around its axis
c- usually used for point-to-point links
d- has high directivity in a specific direction

Signaling scheme that gives better usage of available channel bandwidth is

a- FHSS
b- BER
c- OFDM
d- non of the previous

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#10: *WLAN Part II*

By: *Laith W. Abdullah*

Objectives

- classify WLAN stations according to their mobility.
- Define the frequency bands used by IEEE 802.11 family of standards.
- Compare IEEE 802.11 standards in terms of coverage and interference.
- Listing the types of frames used in WLANs, focusing on the format of Data frames and give brief explanation of Control and Mangment frames
- Clarify the Addressing mechnism followed by WLAN standards.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

Physical Layer Specifications:

Station Types

Based on their mobility, IEEE define three types of stations:-

- **No Transition Mobility:**

  Here the station is fixed or mobile only in inside the BSS.

- **BSS-Transition Mobility:**

  The station here can move from a BSS to another, the movement is confined inside one ESS.

- **ESS-Transition Mobility:**

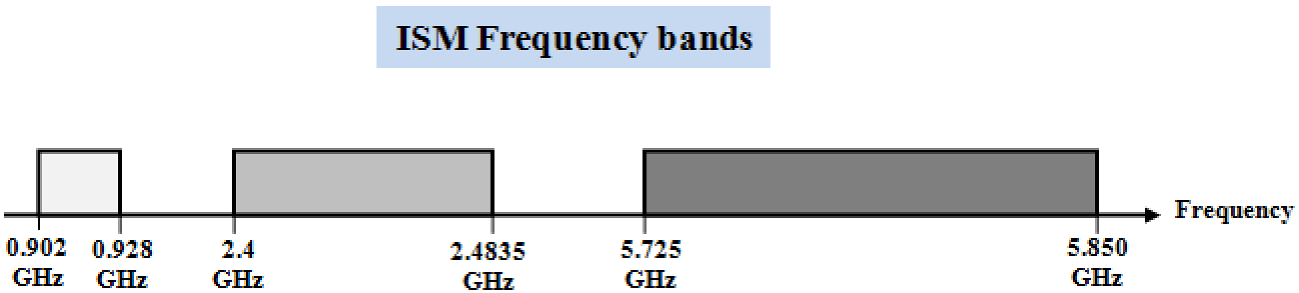
  The satiation in this type can move form one ESS to another.

WLAN

➢ Physical Layer Specifications:

❖ ISM bands

- In 1985, the Federal Communications Commission (FCC) in the United States define the ISM bands to be used by unlicensed devices.



- The 2.4 GHz band is available globally while the other two bands are unlicensed only in USA.

WLAN

➢ Physical Layer Specifications:

Standard	Release Date	Op. Freq. band (GHz)	Bandwidth (Mbps)	Transfer rates (Mbps)	Signaling Scheme	Modulation
IEEE 802.11	1997	2.4	2	1,2	FHSS	FSK
					DSSS	PSK
		Infrared	2	1,2		PPM
IEEE 802.11a	1999	5.725	54	6,9,12,18, 24,36,48,54	OFDM	PSK or QAM
IEEE 802.11b	1999	2.4	11	1,2,5.5,11	DSSS	PSK
IEEE 802.11g	2003	2.4	54	1,2,5.5,11	DSSS	PSK or QAM
				6,9,12,18, 24,36,48,54	OFDM	

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

Physical Layer Specifications:

Interference:

- IEEE 802.11b, IEEE 802.11g use the 2.4 GHz range of the (ISM) band. Because of this choice, 802.11b and 802.11g equipment can incur interference from many other devices using the same band.
- The 802.11a standard uses the 5 GHz band, and is therefore not affected by products operating on the 2.4 GHz band.

Coverage:

- The high carrier frequency restricts the use of 802.11a to almost line of sight, necessitating the use of more access points; it also means that 802.11a cannot penetrate as far as 802.11b or 802.11g since it is absorbed more readily.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ Frames:

❖ Frame types

IEEE 802.11 standards define three types of frames. These types are:

- Data.
- Management.
- Control.

❖ Data Frame:

2 B	2 B	6 B	6 B	6 B	2B	6 B	0-2312 B	4 B
Frame Control	Duration	Address 1	Address 2	Address 3	Seq	Address 4	Frame body	FCS

- **Duration:** indicate the time (in microseconds) the channel will be allocated for successful transmission of layer2 PDU.
- **Address fields (1-4):** contains up to four 6-byte addresses. The usage of each address field is dependent on the "To DS" and "From DS" subfields in the frame control field.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

Frames:

Data Frame

2 B	2 B	6 B	6 B	6 B	2B	6 B	0-2312 B	4 B
Frame Control	Duration	Address 1	Address 2	Address 3	Seq	Address 4	Frame body	FCS

- **Sequence Control:** consists of fragment number and sequence number. It is used to represent the order of different fragments belonging to the same frame.
- **Frame body:** depending on the frame type and subtype, this field contains data or management information.
- **FCS (Frame Check Sequence):** contains a 32-bit Cyclic Redundancy Check (utilizes CRC-32).

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ Frames:

❖ Data Frame :

2 B	2 B	6 B	6 B	6 B	2B	6 B	0-2312 B	4 B
Frame Control	Duration	Address 1	Address 2	Address 3	Seq	Address 4	Frame body	FCS

2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b
Version	Type	subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More data	WEP	Rsvd

- **Frame control:**

it is one of the most important fields in the IEEE 802.11 frame, it consists of several subfields as illustrated bellow:

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ Frames:

❖ Data Frame

Version	Type	subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More data	WEP	Rsvd
2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type
To DS	Regarded to addressing (Defined later in this lecture)
From DS	Regarded to addressing (Defined later in this lecture)
More Frag	Set to "1" for more fragments
Retry	Set to "1" in retransmitted frames
Pwr mgt	Set to "1" when station in power management mode
More data	Set to "1" where the station has other frames to send
WEP	Wired Equivalent Privacy (for encryption)
Rsvd	Reserved for future use

WLAN

➢ Frames:

❖ Control Frames:

RTS, CTS and ACK are three subtypes of control frames. these frames takes an important role in the MAC mechanism of WLANs that will described in the next lecture.

- **Format of RTS Frame**

2 B	2 B	6 B	6 B	4 B
Frame Control	Duration	Address 1	Address 2	FCS

- **Format of CTS and ACK Frames**

2 B	2 B	6 B	4 B
Frame Control	Duration	Address 1	FCS

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

Frames:

Management Frames:

The most important subtypes of management frames are:

- **Association:**
  used by a station to associate itself with an access point.
- **Beaconing:**
  used by an access point periodically to scan if any station needs association.
- **Reassociation:**
  used by a station to associate itself with a new access point when it moves to new BSS.
- **Disassociation:**
  used by an access point or a station to terminate association.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

Addressing:

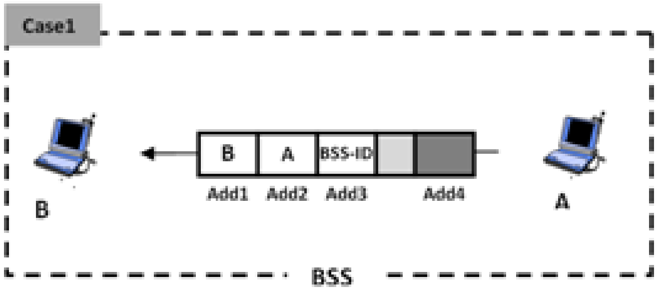
According to the values of the "To DS" and "from DS" subfields in the "frame control" field , IEEE 802.11 addressing mechanism specify four cases:

Case	To DS	From DS	Address 1	Address 2	Address 3	Address 4
1	0	0	Destination	Source	BSS ID	N/A
2	0	1	Destination	Sending AP	Source	N/A
3	1	0	Receiving AP	Source	Destination	N/A
4	1	1	Receiving AP	Sending AP	Destination	Source

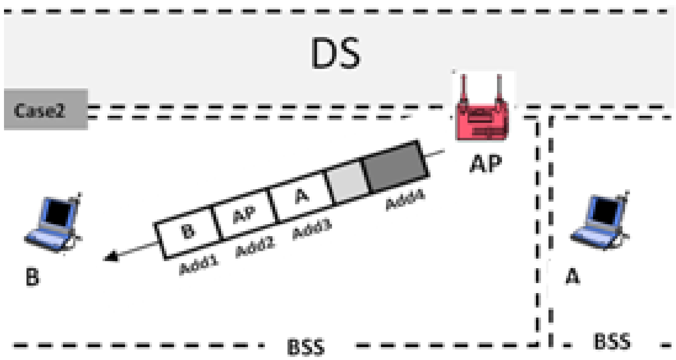
WLAN

Addressing:

- **Case 1 (00):**
  The frame is going from one station in a BSS to another without passing through the distribution system. The ACK frame should be sent to the original sender.



- **Case 2 (01):**
  The frame is coming from an AP and going to a station. The ACK should be sent to the AP. Note that address 3 contains the original sender of the frame (in another BSS).



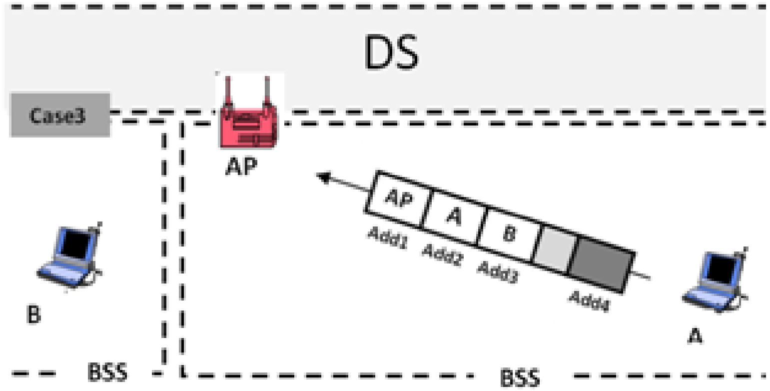
WLAN

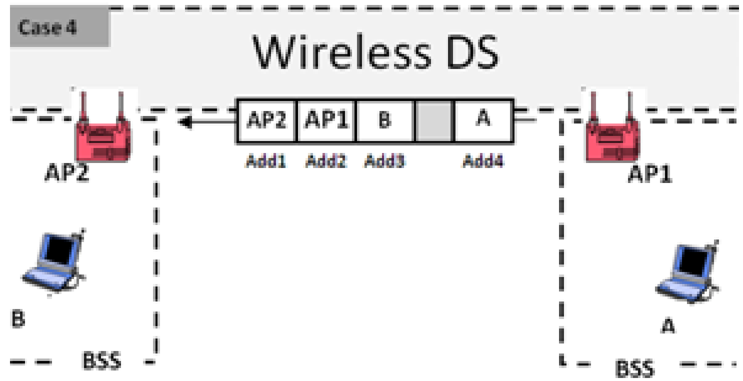
➢ Addressing:

- Case 3 (10):

  The frame is going from a station to an AP. The ACK is sent to the original station. Note that address 3 contains the final destination of the frame (in another BSS).

- Case 4 (11): This is the case in which the distribution system is also wireless. We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame (Ethernet, for example). Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.





???? Quiz ????

The field used to describe the order of fragment in IEEE 802.11 data frame is

a- Frame control
b- Fragment control
c- Access control
d- Sequence control

The third address field is assigned for BSS ID, if

a- the frame is sent form a wireless station to another in the same BSS
b- the frame is sent form a wireless station to another in the same DSS
c- the frame is sent form a wireless station to another in another BSS
d- the frame is sent form a wireless station to another in another ESS

???? Quiz ????

To encrypt its data frame, a wireless station has to set

a- ToDS flag
b- WEP flag
c- ACK flag
d- CTS flag

The frame used by a wireless station to end its exist at a BSS is

a- CTS frame
b- Beacon frame
c- Disassociation frame
d- Pause frame

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#11: *WLAN Part III*

By: *Laith W. Abdullah*

Objectives

- Discuss the phases of CSMA/CA as the MAC mechanism used by WLAN standards
- Define the problem of hidden nodes
- Explain Hand Shaking procedure.
- Discuss the virtual carrier sense mechanisms used in IEEE 802.11 standards

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ CSMA/CA

- Like all of the protocols developed by the IEEE 802 working groups, IEEE 802.11 splits the data-link layer into two sublayers, LLC and MAC.
- IEEE 802.11 uses a MAC mechanism called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

❖ Carrier Sense

CSMA/CA is similar to CSMA/CD in that computers listen to the network to see if it is in use before they send their data, and if the network is free, the transmission proceeds.

❖ Multiple Access

like CSMA/CD, because all of the stations on the network are contending for access to the same network medium, this phase is called the multiple access phase.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

CSMA/CA

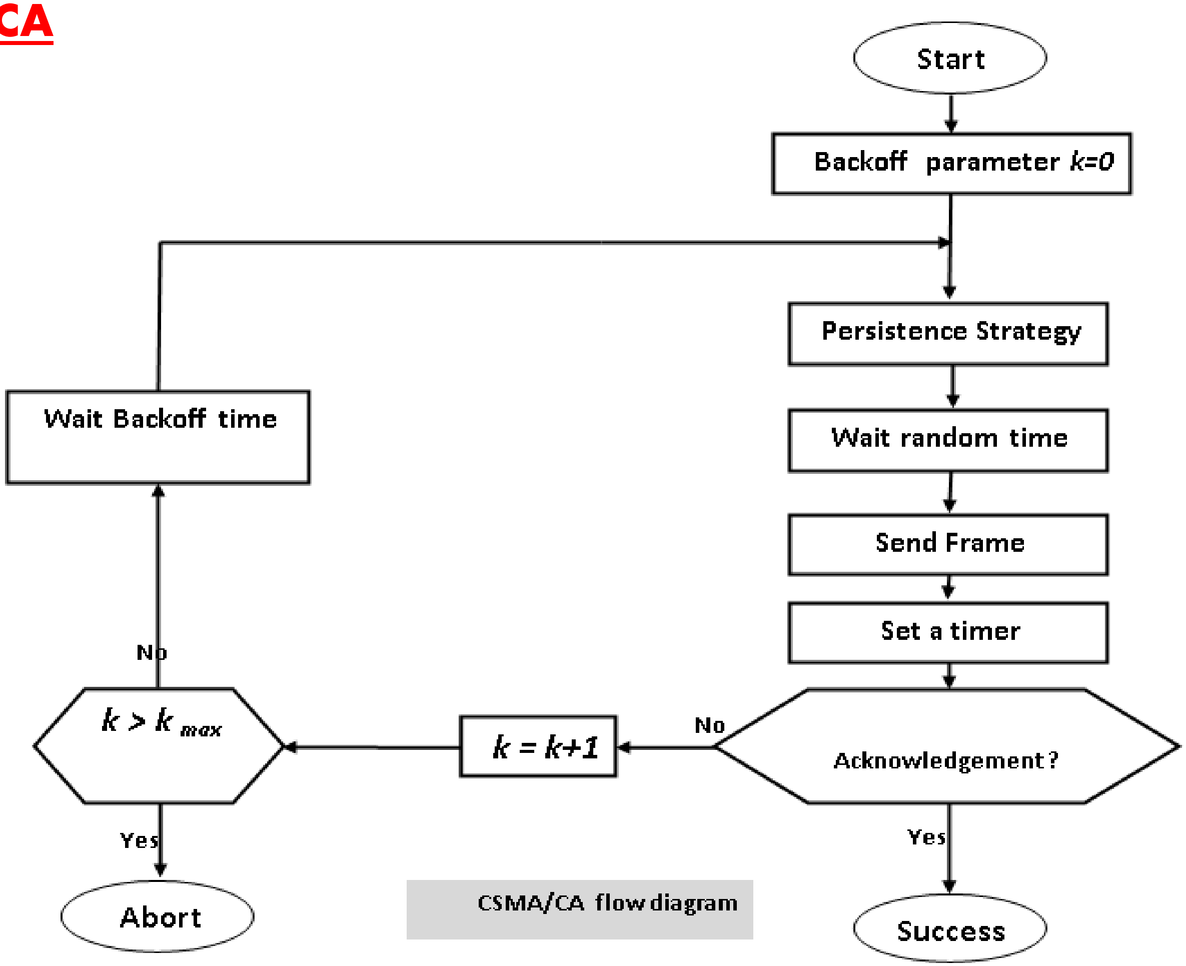
Collision Avoidance:

- Also like CSMA/CD, two computers can transmit at the same time on a CSMA/CA network, causing a collision.
- collision detection mechanism would be impractical, because it would require full-duplex communications.
- Instead of detecting collisions as they occur, the receiving computer on a CSMA/CA network performs a CRC check on the incoming packets and, if no errors are detected, transmits an acknowledgment message to the sender.
- This acknowledgment serves as an indication that no collision has occurred.
- If the sender does not receive an acknowledgment for a particular packet, it automatically retransmits it until it either receives an acknowledgment or times out

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ CSMA/CA



CSMA/CA flow diagram

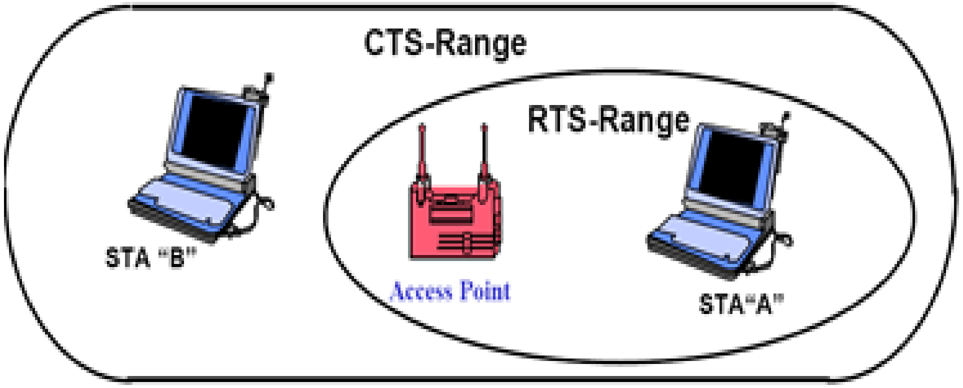
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ CSMA/CA

❖ Hidden Nodes Problem:

- AP is within range of the STA-A, but STA-B is out of range.
- STA-B would not be able to detect transmissions from STA-A, and the probability of collision is greatly increased.
- STA-B is a hidden node to STA-A.



- Physical carrier sense is not useful.
- Virtual carrier sense is implemented to solve hidden node problem via one or both the following access methods.

  - ❖ DCF (Distribution Coordination Function)
  - ❖ PCF (Point Coordination Function)

WLAN

CSMA/CA

DCF

- It is a contention-based access method.
- It is optional in infrastructure WLANs while it is the only access method in ad hoc WLANs.
- DCF is based upon the traditional CSMA/CA but with the use of process known "hand shaking".
- DCF defines two types of IFS (Inter Frame Space), these are:
    - SIFS (Short Inter Frame Space)
      used in high priority situations
    - DIFS(DCF Inter Frame Space)
      used in other situations.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ CSMA/CA

❖ Hand Shaking:

- **In this process two control frames (RTS and CTS) are exchanged between two communicating wireless nodes before the transmission of data frames.**

- **Handshaking procedure:**

  For the previous example where STA-A wants to sends its data to STA-B in an infrastructure WLAN, hand shaking and data transmission process can be explained as follows:-

  1) **STA-A senses the medium, it waits an idle medium to send, then it waits a DIFS to send an RTS frame to the Access Point. The sender reserves the medium for the period defined by the duration field in the RTS frame.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

CSMA/CA

Hand Shaking:

- **Handshaking procedure:**

2) Upon receipt of the RTS, the AP responds with a CTS frame. The CTS gives the green light to STA-A (the requester) to send its data. The CTS frame also contains a duration field specifying the period of time for which the medium is reserved.
3) After receiving the CTS frame, STA-A waits an SIFS to send its data frame(s).
4) To verify that no collision has been occurred, STA-A waits an ACK frame form the Access Point after SIFS.

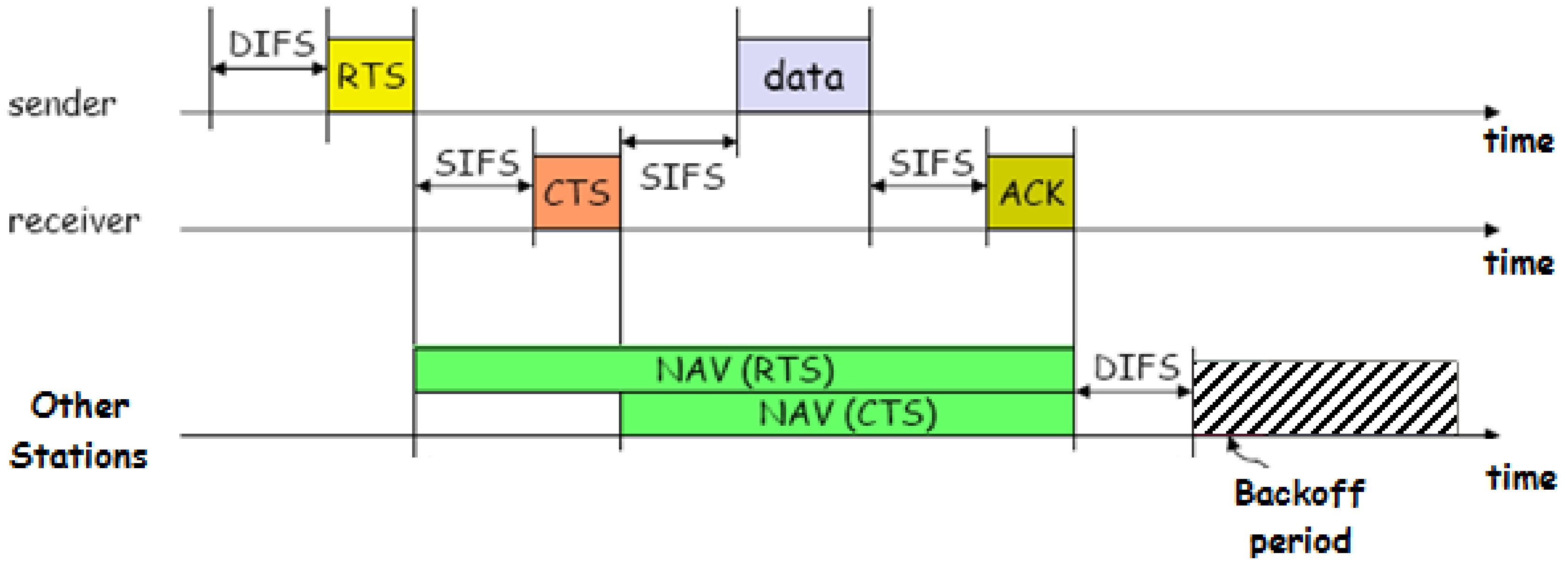
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ CSMA/CA

❖ Hand Shaking:

- **Handshaking procedure:**



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

CSMA/CA

PCF

- It is an optional access method implemented only in infrastructure WLANs
- It is centralized contention-free access method.
- A defined set of stations are polled by the Access Point to see if the stations have any data to send.
- Polling is done by a special software installed in the access point called Point Coordinator (PC).
- PCF defines two types of IFSs.
  - PIFS (PCF IFS)
  - SIFS.
- PIFS is shorter than DIFS. This gives the priority to an Access Point using PCF over a station tries to access the media using DCF.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

WLAN

➢ CSMA/CA

❖ PCF

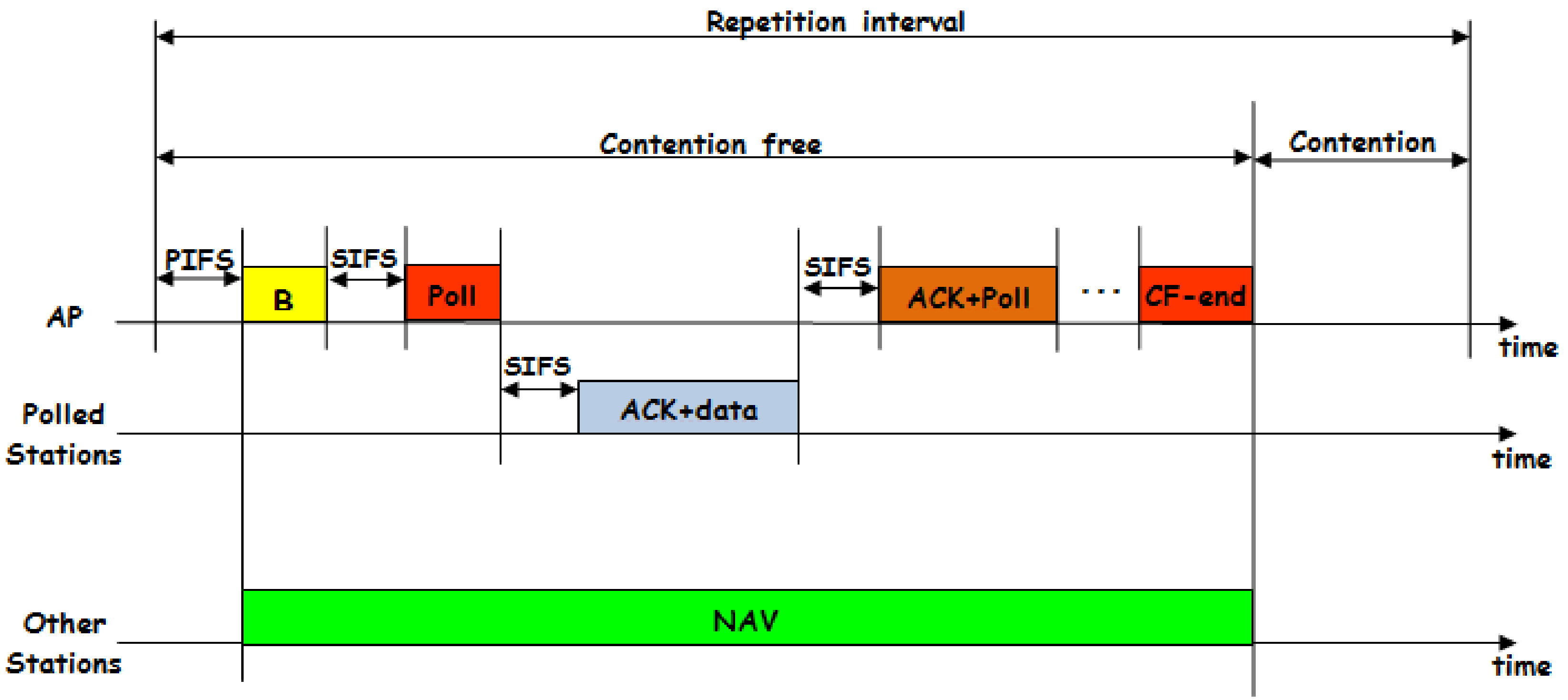
- **Repetition Interval:**
  - A repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF).
  - Repetition interval repeated continuously, starts with a special frame sent by the Access Point called "beacon" frame.
  - Beacon frame contains a duration field that sets the NAV of stations receive that frame to the period of the contention-free interval.
  - After sending the beacon frame, the Access Point sends a "poll" frame to the destination station , receive data, receive an ACK, send an ACK or any combination of these.
  - The Access Point then starts with other polled station and so on.
  - The contention-free interval ends by a CF-end (Contention Free end) frame sent by the Access Point.
  - It is now the time to start the contention based DCF process.

WLAN

➢ CSMA/CA

❖ PCF

- **Repetition Interval:**



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The time interval between CTS and RTS frames in handshaking is defined as

a- DSSS
b- DIFS
c- PPP
d- SIFS

The repetition interval in WLAN starts by

a- Ack frame
b- CTS frame
c- Association frame
d- Beacon frame

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The WLAN station supposes a collision when

a- Ack frame is not received within a specific time
b- No CTS frame detected
c- a beacon frame is not detected
d- AP is pooling other stations

The duration field in the IEEE 802.11 frame affects the time defined by

a- NAV
b- SIFS
c- DIFS
d- PIFS

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Lec.#12: Token Ring *Part I*

By: *Laith W. Abdullah*

Objectives

- Present the physical and logical topologies of Token Ring networks
- Describe and compares mediums supported by Token Ring Protocol.
- List other Physical layer specifications includig digital bandwidth and encoding.
- Clarify the format and role of data and token IEEE 802.5 frames

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

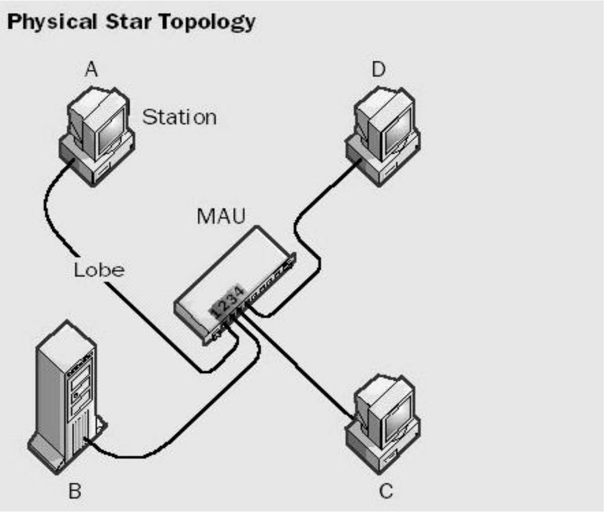
Token Ring

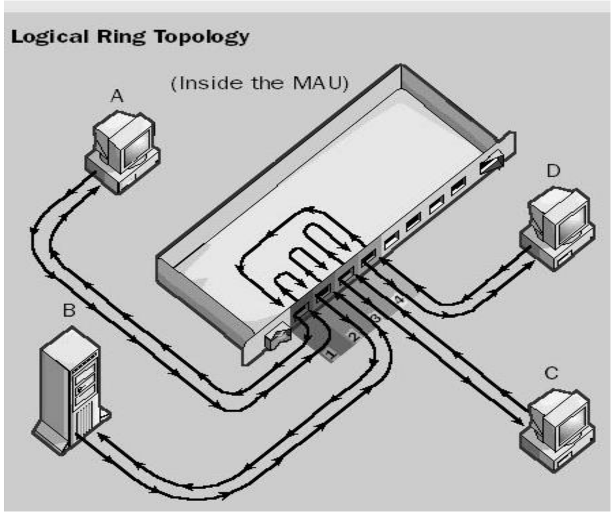
- IBM originally designed Token Ring in 1970s.
- Then it was standardized in the IEEE 802.5 document.

Physical Layer Specifications

Topology

- It is implemented logically as Ring inside the Multistation Access Unit (MAU), the Token Ring equivalent of a hub.
- The network cables take the form of a physical star topology





Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Physical Layer Specifications

❖ Media

Generally there are two options related to Token Ring physical layer specifications; these are called Type 1 and Type 3.

a- Type 1:

- Type 1 is a heavy, shielded twisted pair (STP) cable.
- Connectors:
  - The connector at the MAU end of the cable is a large, proprietary jack called an IBM Data Connector (IDC) or a Universal Data Connector (UDC).
  - The NICs in the computers use standard DB-9 connectors.

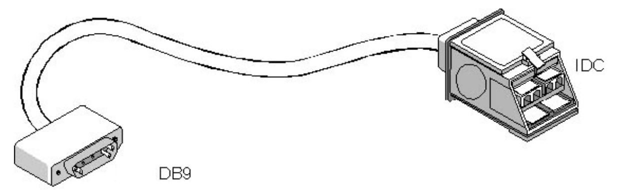
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

Physical Layer Specifications

a- Type 1:

- **Cables:**
  - Cables with one IDC and one DB-9 connector, which are used to connect a computer to a MAU, are called lobe cables.
  - Cables with IDC connectors at both ends, used for connecting MAUs together, are called patch cables.



Token Ring

- **Physical Layer Specifications**

b- Type 3:

- Most Token Ring networks use Category 5 UTP.
- RJ-45 connectors are used at both ends.
- Type 3 networks use the same connectors for both computers and MAUs.

Comparison

- Type 1 lobe cable can be up to 300 meters long, whereas Type 3 cables are limited to 150 meters.
- Type 1 networks can have up to 260 connected workstations, whereas Type 3 networks can have only 72.
- Type 1 is more immune to noise
- Type 3 is easier to install.

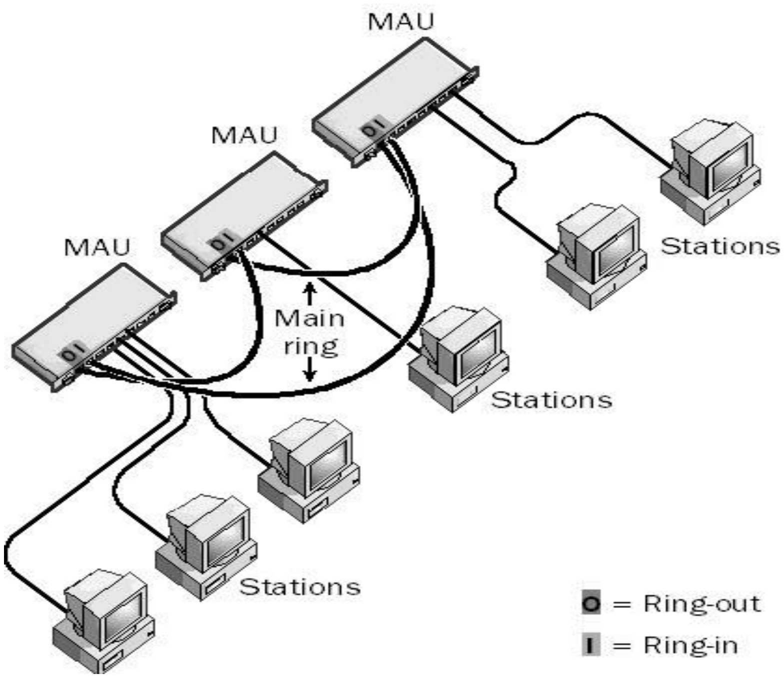
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Physical Layer Specifications

❖ **Network Expansion**:

Patch cables connect MAUs to other adjacent MAUs using "Ring IN" and "Ring OUT" ports



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

Physical Layer Specifications

- **Bandwidth:**
  - Token Ring networks were originally designed to run at 4 Mbps
  - but later implementations increased the speed to 16 Mbps.
  - 16 Mbps is faster than standard Ethernet, but nowhere near the 100-Mbps speed of Fast Ethernet.
- **Encoding:-**
  - Token Ring networks use baseband differential Manchester encoding (a variation of Manchester encoding).
  - While Ethernet uses baseband Manchester encoding.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Frames

Token Ring mainly defines four types of frames

- Data frame
- Token frame
- Command frame
- Abort delimiter frame.

❖ Data Frame

1-Byte	1-Byte	1-Byte	6-Bytes	6- Bytes	Up to 4500 Bytes	4-Bytes	1-Byte	1-Byte
Start Delimiter	Access Control	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status

- **Start Delimiter (1 byte):** This field contains a bit pattern that signals the beginning of the frame to the receiving system. The main usage for this frame is synchronization.

Token Ring

➢ Frames

❖ Data Frame

1-Byte	1-Byte	1-Byte	6-Bytes	6- Bytes	Up to 4500 Bytes	4-Bytes	1-Byte	1-Byte
Start Delimiter	Access Control	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status

3-bits	1-bit	1-bit	3-bits
priority	Token bit	Monitor bit	reservation

- **Access Control (1 byte):** This field contains bits that can be used to prioritize Token Ring transmissions, enabling certain systems to have priority access to the token frame and the network. The access control byte contains the priority and reservation field, and a token and monitor bits.

Token Ring

Frames

Data Frame

Start Delimiter	Access Control	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status
1-Byte	1-Byte	1-Byte	6-Bytes	6- Bytes	Up to 4500 Bytes	4-Bytes	1-Byte	1-Byte

- **Frame Control (1 byte):** This field contains bits that specify whether the frame is a data or a command frame.
- **Destination Address (6 bytes):** This field contains the 6-byte address of the network interface adapter on the local network to which the packet will be transmitted.
- **Source Address (6 bytes):** This field contains the 6-byte address of the network interface adapter in the system generating the packet.
- **Information (up to 4500 bytes):** This field contains the data generated by the network layer protocol, including a standard LLC subheader.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Frames

❖ Data Frame

1-Byte	1-Byte	1-Byte	6-Bytes	6- Bytes	Up to 4500 Bytes	4-Bytes	1-Byte	1-Byte
Start Delimiter	Access Control	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status

- **Frame Check Sequence (4 bytes):** This field contains a 4-byte CRC-32 of the packet (excluding the Start Delimiter, End Delimiter, and Frame Status fields) that the receiving system uses to verify that the packet was transmitted without error.
- **End Delimiter (1 byte):** This field contains a bit pattern that signals the end of the frame, including a bit that specifies if there are further packets in the sequence yet to be transmitted and a bit that indicates that the packet has failed the error check.
- **Frame Status (1 byte):** This field contains bits that indicate whether the destination system has received the frame and copied it into its buffers.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Frames

❖ Token Frame

- The token frame is 3 bytes long and contains only the Start Delimiter, Access Control, and End Delimiter fields.
- The Start Delimiter and End Delimiter fields use the same format as in the data frame,
- the token bit in the Access Control field is set to a value of 1 to distinguish this frame from data frame.
- Monitor bit is used to distinguish a "busy" token from "free" token as will be discussed in "Token Passing" mechanism.

1-Byte	1-Byte	1-Byte
Start Delimiter	Access Control	End Delimiter

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Token Ring maximum transfer rate is

a- 16 MBps
b- 16 Gbps
c- 16000 Kbps
d- 16 KBps

The device used to connect Token Ring in Logical star topology is called

a- MAU
b- MMS
c- NIC
d- AP

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Error detection method depended by Token Ring is

a- FEC
b- CRC
c- Parity Check
d- FFT

One of the following bits is used to distinguish free from busy token

a- monitor bit
b- token bit
c- distinguish bit
d- free bit

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#13: *Token Ring Part II*

By: *Laith W. Abdullah*

Objectives

- Clarify the format and role of Command and Abort-delimiter Frames IEEE 802.5 frames.
- Explain the priority system of IEEE 802.5 networks.
- Define the role of Active Monitor system.
- Detail the modes of MAC mechanism of Token Ring networks.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

Frames

Command Frame

- The command frame uses the same basic format as the data frame, differing only in:
- the value of the Frame Control field
- the contents of the Information field.
- The Information field, contains a 2-byte called "major vector ID", which specifies the control function the packet is performing, followed by the actual control data itself, which can vary in length.

1-Byte	1-Byte	1-Byte	6-Bytes	6- Bytes	Up to 4500 Bytes	4-Bytes	1-Byte	1-Byte
Start Delimiter	Access Control	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

Frames

Common Command Frames

Common control frames with their hexadecimal major vector values are:

- **0010—Beacon:**
  - **Beaconing is a process by which systems on a Token Ring network indicate that they are not receiving data from their Nearest Active Upstream Neighbor (NAUN).**
  - **Beaconing enables a network administrator to more easily locate the malfunctioning computer on the network and also to reconfigure the network so that the malfunctioning station can be removed from the ring.**
- **0100—Ring Purge:**

  This vector ID is used by the active monitor system in the event of an error to clear the ring of unstripped data and to return all of the systems to repeat mode.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Frames

❖ Abort Delimiter Frame

- **The abort delimiter frame consists of only 2 bytes, the same Start Delimiter and End Delimiter fields**
- **it uses the same values for those fields as the data and command frames.**
- **When a problem occurs, such as an incomplete packet transmission, the active monitor system generates an abort delimiter frame to flush all existing data from the ring.**

1-Byte	1-Byte
Start Delimiter	End Delimiter

Token Ring

➢ Priority System

- Token Ring networks use an optional sophisticated priority system that permits certain user-designated, high priority stations to use the network more frequently.
- Token Ring frames have two fields that control priority, the priority field and the reservation field.

3-bits	1-bit	1-bit	3-bits
priority	Token bit	Monitor bit	reservation

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Priority System

- Only stations with a priority equal to, or higher than, the priority value contained in a token can seize that token.
- Once the token has been seized and changed to a data frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next network pass.
- The next token generated includes the higher priority of the reserving station.
- Stations that raise the priority level of a token must reinstate the previous priority when their transmission has been completed.

3-bits	1-bit	1-bit	3-bits
priority	Token bit	Monitor bit	reservation

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

Active Monitor System

This system acts as a centralized source of timing information for other ring stations and performs a variety of ring maintenance functions.
Main functions of active monitor system are:

- **Errant Frame:**

  One of this functions of the station is to remove continuously circulating frames from the ring called "Errant" or "Orphan" frames. The monitor system changes the value of the "monitor" bit in the Access control" field form "0" to "one" in a frame which circulates the ring for the first time. When this frame circulates the ring for the second time, the value of the monitor bit is checked again, if it is "1" this means that this frame is an errant frame and it is drained from the ring.

Token Ring

Active Monitor System

- **No Frame or NoToken:**

  This case occurs when the receiving station crashes after receiving a frame or a token, and thus there is nothing circulating in the ring. It is now the responsibility of the active monitor to generate a new token.

- **Beconing:**

  Removing the a faulty NAUN.

- **Ring purge:**

  Removing unstriped data

- **Generating abort delimiter frame:**

  In case of incomplete Packet transmission.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

Token Passing

- The MAC mechanism of Token Ring networks is called Token Passing
- Token passing is a controlled access method.
- Token passing works by circulating a special packet called a token around the network.
- The token is only 3 bytes long and contains no useful data. Its only purpose is to designate which system on the network is allowed to transmit its data.
- Main phases of Token Passing mechanism are:
  - Repeat Mode
  - Transmit Mode
  - Strip Mode
  - Token Release

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

Token Passing

Repeat Mode

- In their idle state, computers on a Token Ring network are in what is known as repeat mode.
- While in this state, the computer systems receive packets from the network and immediately forward them back to the MAU for transmission to the next port.
- If a system doesn't return the packet, the ring is effectively broken and network communication ceases.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Token Passing

❖ Transmit mode

- When a computer has data to transmit, it must wait for a free token to arrive before it can send its data.
- Because there is only one token, only one system on the network can transmit at any one time. This means that there can be no collisions on a Token Ring network.
- When a computer takes possession of the token, it convert it to a busy token by changing the value of the monitor bit to "one“ and forward it back to MAU.
- other computers that the network can't take possession of the busy token. Immediately after the computer transmits the "network busy" token, it transmits its data packet.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Token Passing

❖ Strip mode

- Data frame circulates around the ring until it reaches the intended destination station, which copies the information for processing.
- The information frame continues around the ring until it reaches the sending station.
- At the same time that the sending computer goes into transmit mode, its receive wire pair goes into stripping mode.
- When the data packet traverses the entire ring and returns to its source, it is the responsibility of the sending computer that generated the packet to strip it from the network.
- The sending station can verify whether the frame was received and copied by the destination.
- The data frame that cannot be removed by its sender is removed by the active monitor system

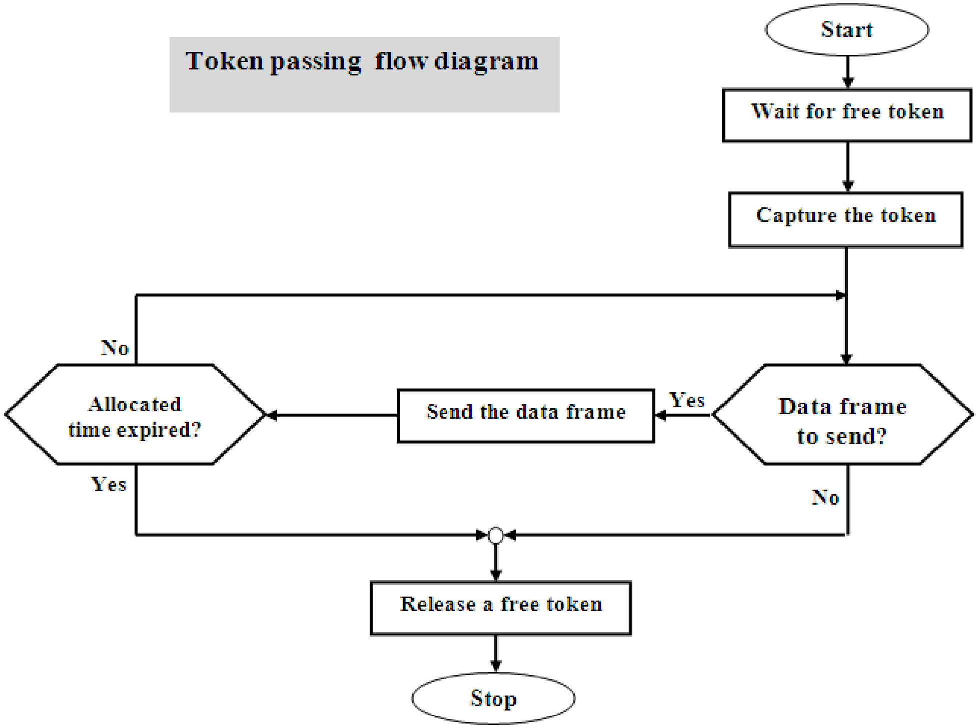
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Token Ring

➢ Token Passing

❖ Token release

The original Token Ring network design calls for the system transmitting its data packet to wait for the last bit of data to arrive back at its source before it generates a new token by modifying the monitor bit in the token frame back to its original value and transmitting it.



???? Quiz ????

Token frame fields that concerns with priority is

a- Frame control
b- Access control
c- Sequence control
d- Frame status

The frame that is used to abort a malfunctioning Token Ring station is called

a- CTS
b- Ring purge
c- Beacon
d- Abort delimeter

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the main functions of active monitor systems is to

a- generate errant frames
b- remove errant frames
c- remove the free token
d- none of the previous

a free token is circulated around the ring in

a- strip mode
b- listen mode
c- transmit mode
d- repeat mode

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#14: *FDDI*

By: *Laith W. Abdullah*

Objectives

- Discuss the topologies of FDDI networks.
- List station types of FDDI networks
- Present other physical layer specifications like mediums, bandwidth, and encoding.
- Detail the format of FDDI data frame.
- Explain the MAC of FDDI network.
- List some of the main features of FDDI networks

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

➢ Physical Layer Specifications

❖ Topology

- FDDI defines two physical topologies , these are:

1- Dual ring :

- FDDI specifies the use of dual rings for physical connections.
- Traffic on each ring travels in opposite directions.
- The outer ring is called the primary ring and the inner ring is called the secondary ring.
- Normally, traffic flows only on the primary ring.
- If primary ring fails, then the data automatically flows onto the secondary ring in the opposite direction. (this called wrapped state)

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

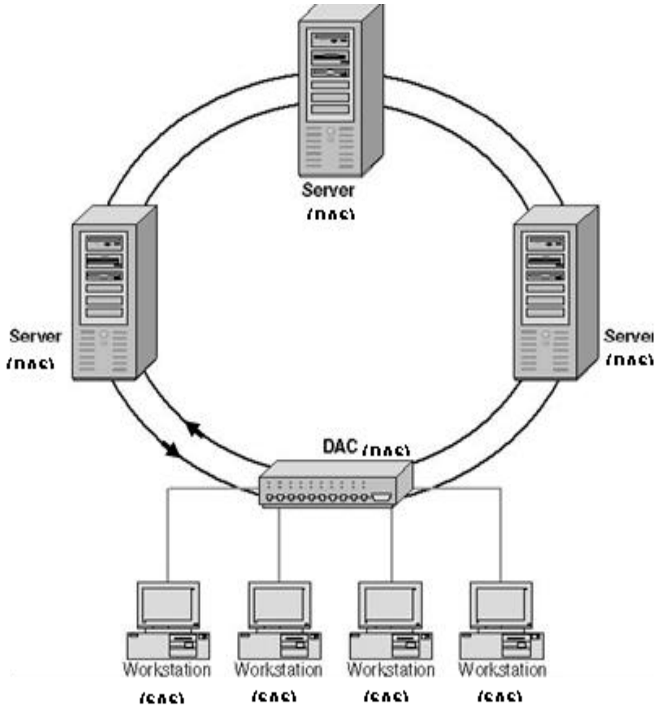
FDDI

Physical Layer Specifications

Topology

2-Star

- It's also possible to cable a FDDI network in a physical star topology using a hub called a Dual Attachment Concentrator (DAC).
- The DAC creates a single logical ring, like a Token Ring MAU.



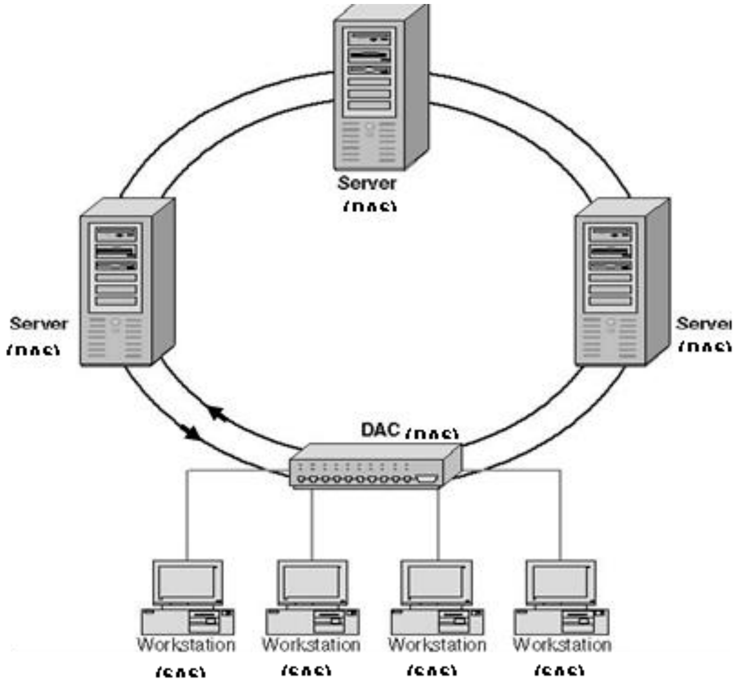
FDDI

Physical Layer Specifications

Stations Types

Computers or stations on a FDDI network are divided into two classes, as follows:

- Class A also called Dual Attachment Station (DAS); here computer or station is connected to both rings, DAC is an example of DAS.
- Class B also called Single Attachment Station (SAS); station here connected to only one ring. Examples on SAS are the stations connected to DAC



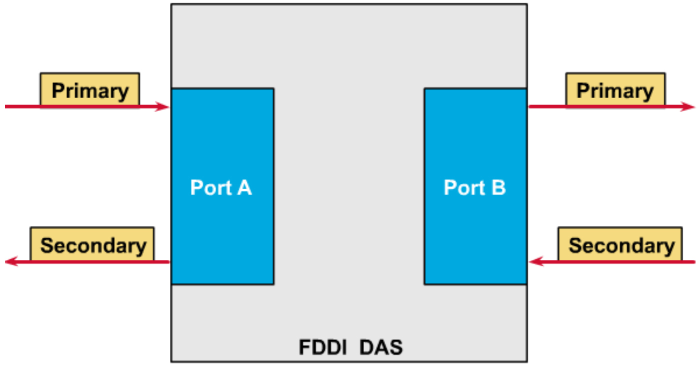
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

Physical Layer Specifications

Stations Types

- **DAS:**
  - **Each FDDI DAS has two ports, designated A and B. These ports connect the station to the dual FDDI ring. Therefore, each port provides a connection for both the primary and the secondary ring.**



  - **The DAS servers have full advantage of the double ring's fault tolerance, as do the DACs. The concentrator ensures that a failure, or power down, of any given SAS, does not interrupt the ring.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

➢ Physical Layer Specifications

❖ Stations Types

FDDI supports several different types of fiber optic cable, including:

- Multimode cable which provides for network segments up to 100 kilometers long with up to 500 workstations placed as far as 2 kilometers apart.
- Singlemode fiber optic cables provide even longer segments, with up to 60 kilometers between workstations.

➢ Bandwidth

- FDDI supports a maximum speed (transfer rate) of 100 Mbps.
- This speed was unprecedented at the time of its introduction (there was the standard Ethernet and Token Ring which operates at maximum speeds of 10 Mbps and 16 Mbps relatively)

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

Physical Layer Specifications

Mediums

FDDI supports several different types of fiber optic cable, including:

- **Multimode** cable which provides for network segments up to 100 kilometers long with up to 500 workstations placed as far as 2 kilometers apart.
- **Singlemode** fiber optic cables provide even longer segments, with up to 60 kilometers between workstations.

Bandwidth

- FDDI supports a maximum speed (transfer rate) of **100 Mbps**.

Encoding

- FDDI uses an encoding scheme called **4B/5B.**
- The signal sources in FDDI transceivers are:
  - LEDs (for multimode fibers)
  - Lasers (for singlemode fibers).

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

Frames

Frames Types

FDDI uses several different types of frames in its communications. these are

1- data frame

2- token frame

3- station management frame

Data Frame:

8-Bytes	1-Byte	1-Byte	6-Bytes	6- Bytes	variable	4-Bytes	4-bits	12-bits
Preamble	Starting Delimiter	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status

- **Preamble (8 bytes):** Contains series of alternating 0s and 1s, used for clock synchronization.
- **Starting Delimiter (1 byte):** Indicates the beginning of the frame.
- **Frame Control (1 byte):** Indicates the type of data found in the Data field.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

Frames

Data Frame:

Preamble	Starting Delimiter	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status
8-Bytes	1-Byte	1-Byte	6-Bytes	6- Bytes	variable	4-Bytes	4-bits	12-bits

- **Destination Address (6 bytes):** Specifies the hardware address of the computers that will receive the frame.
- **Source Address (6 bytes):** Specifies the hardware address of the system sending the frame.
- **Data (variable):** Contains network layer protocol data, or control information depending on the type of the frame.
- **Frame Check Sequence (4 bytes):** Contains a Cyclical Redundancy Check value used for error detection

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

➢ Frames

❖ Data Frame:

8-Bytes	1-Byte	1-Byte	6-Bytes	6- Bytes	variable	4-Bytes	4-bits	12-bits
Preamble	Starting Delimiter	Frame Control	Destination Address	Source Address	Information (Data)	Frame Check Sequence	End Delimiter	Frame Status

- **Ending Delimiter (4 bits): Indicates the end of the frame.**
- **Frame status (12 bits):** Contains three indicators that may be modified by intermediate systems when they retransmit the packet, the functions of which are as follows:
    - **Error** Indicates that an error has been detected.
    - **Acknowledge** Indicates that the intermediate system has determined that the frame's destination address applies to itself.
    - **Copy** Indicates that the intermediate system has successfully copied the contents of the frame into its buffers.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

Frames

Token frame

A three Byte frame that plays the main role in the MAC mechanism of FDDI networks.

4-Bits	1-Byte	1-Byte	4-bits
Preamble	Starting Delimiter	Frame Control	End Delimiter

Station management frame

The third type of frame used on FDDI networks is the station management frame, which is responsible for ring maintenance and network diagnostics.

FDDI

Early Token Release

- The token passing mechanism used by FDDI is virtually identical to that of Token Ring, except that the early token release feature that is optional in Token Ring is standard equipment for the FDDI protocol.
- In this method another system on the network can receive a data packet, take possession of the token, and begin transmitting its own data frame before all of the data from the first packet has returned to its source.
- There are parts of two data frames on the network at the same time, but there is never more than one free token.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

FDDI

FDDI Features

- Collision free: because Token Passing is a controlled MAC mechanism
- Deterministic: where the time the rule is back to the station to transmit can be estimated.
- Fault tolerance: because of using the dual ring.
- Not susceptible to EMI/RFI: where the signals to be transmitted are light pulses with frequencies so far of the RF region.
- High security: due to the use of fiber optics where tapping is not possible as in copper mediums
- Long distances: fiber optics usually can carry signals to far distances as compared with copper mediums where they have less attenuation.
- High speed: low attenuation in fibers enables HW manufacturers to get higher transmission rates

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

A station that is connected to both rings of FDDI is called

a- DAS
b- SAS
c- DSB
d- MAU

Encoding Scheme used by FDDI is called

a- 7B/8B
b- 5B/4B
c- 4B/5B
d- 8B/10B

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the followings is not an FDDI feature

a- high security
b- low interference
c- low cost
d- high speed

Error detection method depended by FDDI is

a- FEC
b- Parity Check
c- RCC
d- CRC

Technical Engineering College / Al-Najaf

Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#15: Data-link Layer Devices

By: Laith W. Abdullah

Objectives

- Discuss the main functions of NIC.
- Describe the role of bridge with detailed explanation of building address tables
- Define the main functions of switches and explain how they can be classified.
- Explain the main role of Access Points.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link layer Devices

NICs

- It is the component that provides the link between a computer and the network of which it is a part.

- NIC Functions:
  - Data encapsulation
  - encoding and decoding
  - Data buffering
  - Serial/parallel conversion
  - Media Access Control (MAC)

- Although NIC performs some of physical layer functions, but it is said that it is a Data-link layer device because it can also perform Data-link layer functions.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link layer Devices

Bridges

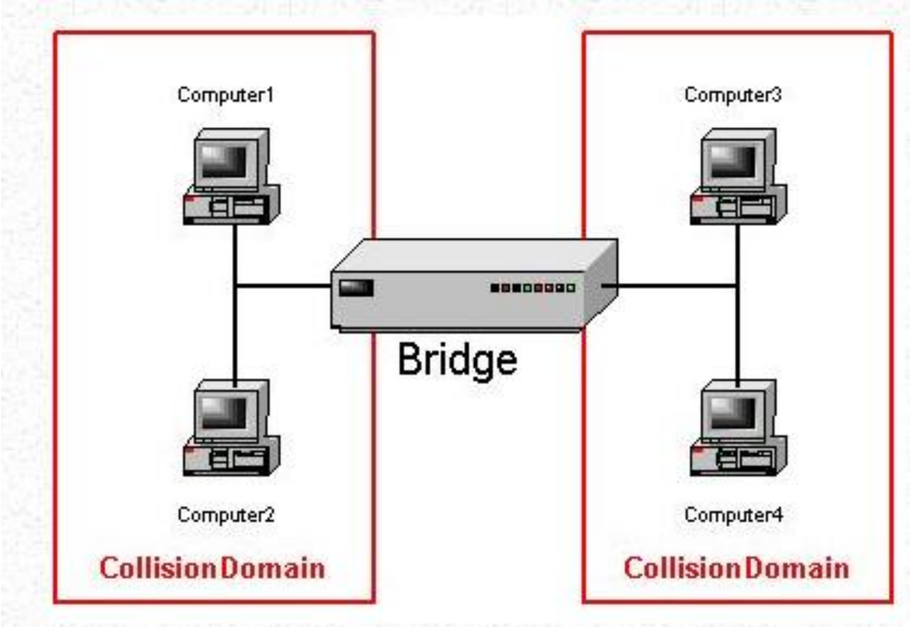
- A bridge is a physical unit, typically a box with two ports.
- It can be used to connect two existing LANs or to split one LAN into two segments.
- it is capable of interpreting the information in the data-link layer protocol header (especially MAC addresses).
- the bridge then reads the destination address in each incoming packet header and decides how to discard or relay the packet.
- The use of the bridge (theoretically) cuts the unnecessary traffic passing over each network segment in half.

Data-link layer Devices

Bridges

- **Collision domains:**

  The bridge splits the collision domain into two collision domains. (collision domain is a network part that is constructed so that when two computers transmit packets at precisely the same time, a collision occurs.



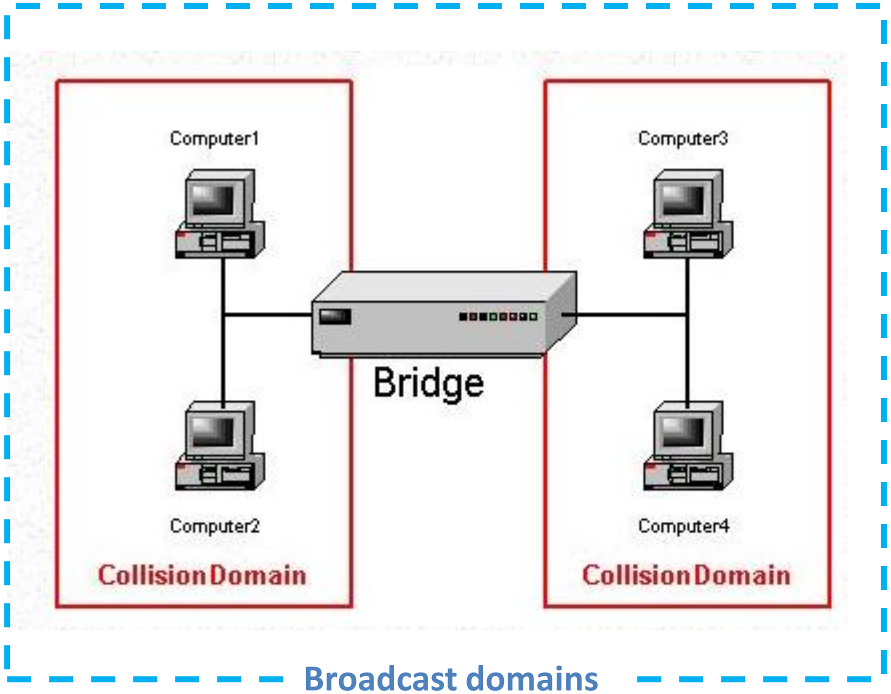
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link layer Devices

➢ **Bridges**

- Broadcast domains

  the segments on either side of the bridge remain part of the same broadcast domain (a broadcast domain is a group of computers that all receive a broadcast message transmitted by any one of the computers in the group.



Data-link layer Devices

- **Bridges**

  - **Bridging Types**

    Bridges can forward or discard incoming packets by maintaining an internal address table that lists the hardware addresses of the computers on both segments.

    The way the bridge builds this address table decides the type of bridging, generally there are two types:

    - **Manual: Originally, network administrators had to manually create the lists of hardware addresses for each segment connected to the bridge and this was obviously an onerous chore.**
    - **Transparent: bridges use a technique called transparent bridging to automatically or dynamically obtain their own address lists.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link layer Devices

Bridges

Transparent Bridging Procedure

- **Learning:**

  When you activate a transparent bridge for the first time, it begins processing packets. For each incoming packet, the bridge reads the source address in the data-link layer protocol header and adds it to the address list for the network segment over which the packet arrived. This process is called learning.

- **Packet filtering:**

  When a sufficient number of packets passes through the bridge to enable the compilation of the address tables, the bridge begins using them to selectively forward or discard packets. This process is known as packet filtering

Data-link layer Devices

Bridges

Transparent Bridging Procedure

- **Aging:**

  A transparent bridge continuously updates its address table. It put a time stamp for each entry in the address table that when expired this entry is removed from the table. This is called aging.

- **Flooding:**

  A frame that it is targeted to all nodes in the network (broadcast frame) or that have a destination address that is not in the address table is forwarded to the other segment, this process is known as flooding.

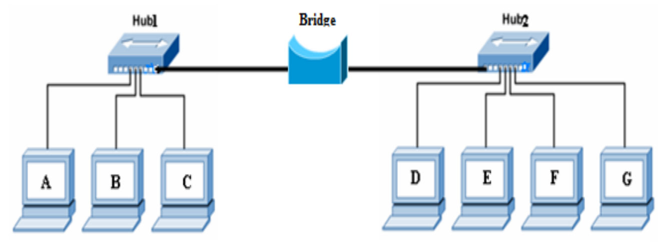
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link layer Devices

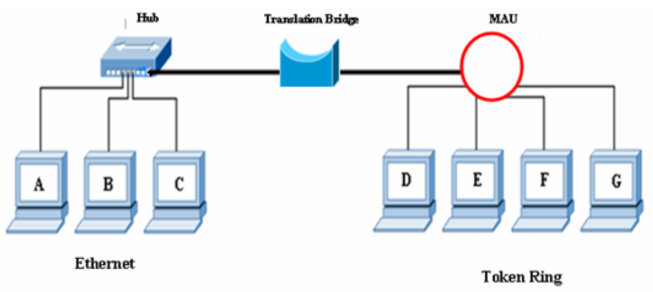
➢ **Bridges**

❖ **Types**

- **Local Bridge:** it is a type of bridge used to connect network segments of the same type at the same location.



- **Translation Bridge:** it connects network segments using different network media or different protocols. This bridge is slower and more complicated than a local bridge



- **Remote Bridge:** is designed to connect two network segments at distant locations using some form of WAN link such as modem connection.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

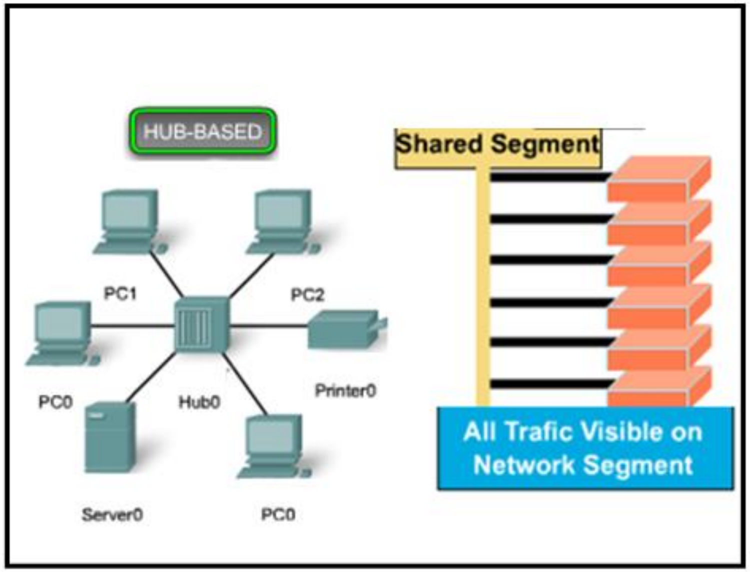
Data-link layer Devices

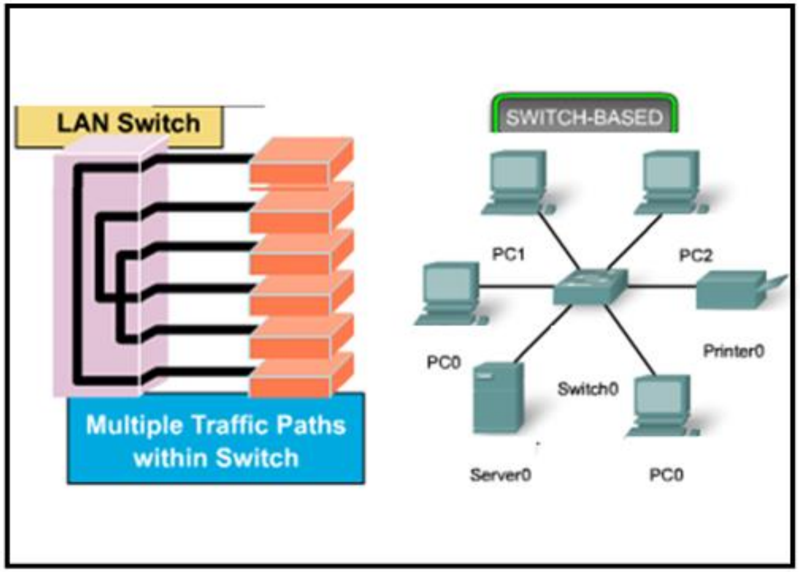
Switches

- Switch indeed is a multiport bridge.
- It does the functions of active hub except that it forwards each incoming packet only to the port that provides access to the destination system.
- Switches split the collision domain and keeping the broad cast domain.
- switches essentially convert the LAN from a shared network medium to a dedicated one.

Data-link layer Devices

- **Switches**





Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link layer Devices

- **Switches**

- **Types :**
  - **Cut-through Switch:** which forwards packets immediately by reading the destination address from their data-link layer protocol headers as soon as they're received and relaying the packets out through the appropriate port with no additional processing.
  - **Store-and-forward Switch:** that waits until an entire packet arrives before forwarding it to its destination.. While the packet is stored in the switch's memory buffers, the switch takes the opportunity to verify the data by performing a CRC. This checking naturally introduces additional latency delay into the packet forwarding process.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Data-link layer Devices

➢ Access Points

- AP connects wireless communication devices together to create a wireless network.
- A wireless access point acts as the network's arbitrator, negotiating when each nearby client device can transmit.
- At the same time Access points are bridges between the wireless world and the wired world.
- As Bridges, all access points have features that one would expect to see on a network bridge.
- Many access points also offer the option of using external antennas to further boost range.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the followings is not a NIC function

a- MAC
b- data-buffering
c- Dialog control
d- Encoding/decoding

The bridge increases network efficiency by

a- splitting the broadcast domain
b- splitting the collision domain
c- directing the data to final destination
d- authorizing user data

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the followings depends source MAC address

a- routing
b- learning
c- packet filtering
d- flooding

8 port switch can theoretically split the network into

a- 8 broadcast domains
b- 4 collision domains
c- 8 collision domains
d- 2 collision domains

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#16: *IPv4* *Part I*

By: *Laith W. Abdullah*

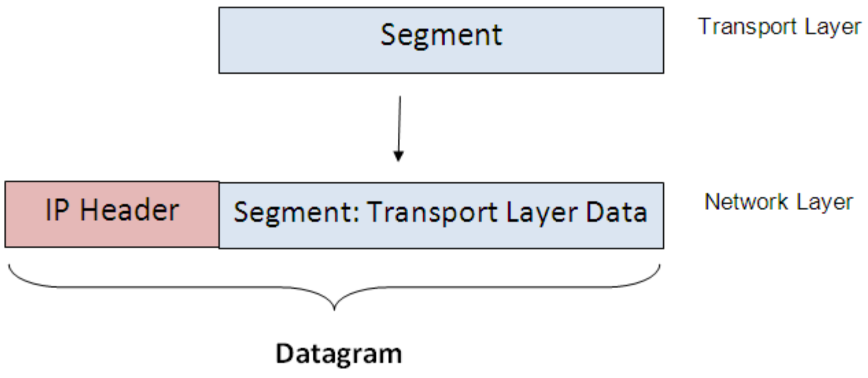
Objectives

- List the main functions of network layer
- Detail the format of IPv4 datagram
- Explain some of the options of IPv4 datagrams
- Specify how IPv4 deals with upper layer protocols

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

- The Internet Protocol (IP) is the cornerstone of the TCP/IP protocol suite.
- IP is the protocol responsible for transmitting data from its source to its final destination.
- IP encapsulates the transport layer PDU (called segment) by adding a header, creating what's known as a datagram.
- During the transportation process, various systems might encapsulate the datagram in different data-link layer protocol headers, but the datagram itself remains intact.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

Network Layer Main Functions

- **Encapsulation:** The packaging of the transport layer data into a datagram
- **Fragmentation:** The division of data into fragments of an appropriate size for transmission over the network
- **Protocol identification:** The specification of the transport layer protocol that generated the data in the datagram
- **Addressing:** The identification of systems in the network using IP addresses
- **Routing:** The identification of the most efficient path to the destination system through the internetwork

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

➢ IPv4

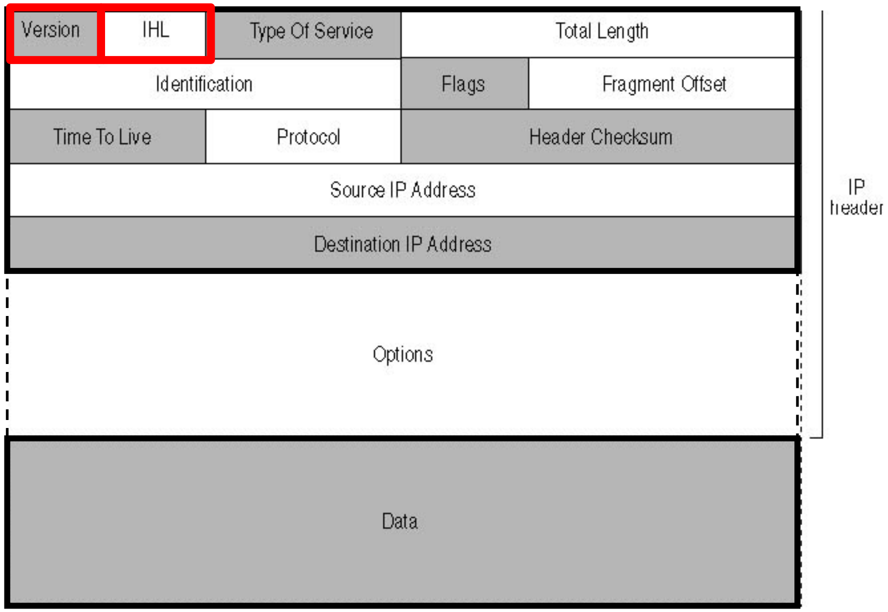
❖ Datagram Format:

- **Version (4 bits):**

  This field specifies the version of the IP protocol used to create the datagram. The version currently in use is 4.

- **Internet Header Length (IHL, 4 bits):**

  This field specifies the length of the datagram's header, in 32-bit (4-byte) words. The minimum length of a datagram header is five words (20 bytes), but if the datagram includes additional options, it can be longer, which is the reason for having this field. However the maximum length of the IPv4 datagram header is 60 Bytes.



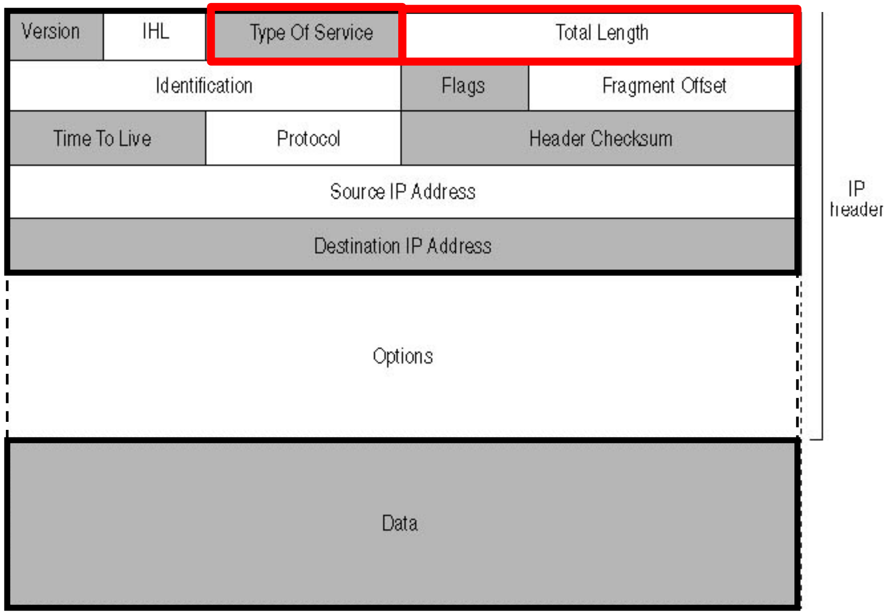
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

Datagram Format:

- **Type Of Service (1 byte):**

  This field contains a code that specifies the priority for the datagram. This is a rarely used feature that enables a system to assign a priority to a datagram that routers observe while forwarding it through an internetwork.



- **Total Length (2 bytes):**

  This field specifies the length of the datagram, including that of the Data field and all of the header fields, in bytes.

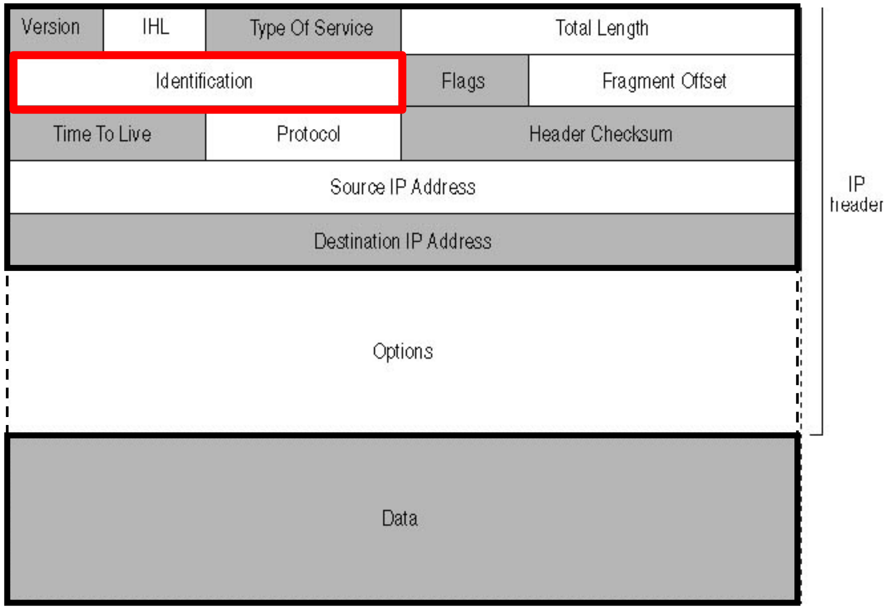
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

➢ IPv4

❖ Datagram Format:

○ **Identification (2 bytes):**

This field in combination with source IP address field uniquely identifies the datagram. IP guarantees that the value in this field is not duplicated for datagrams transmitted from a source host to a specific destination host. The value in this filed is initiated by a number that is incremented by one for each new datagram. Identification value helps to reassemble datagrams that have been fragmented during transmission as will be discussed later.



IPv4

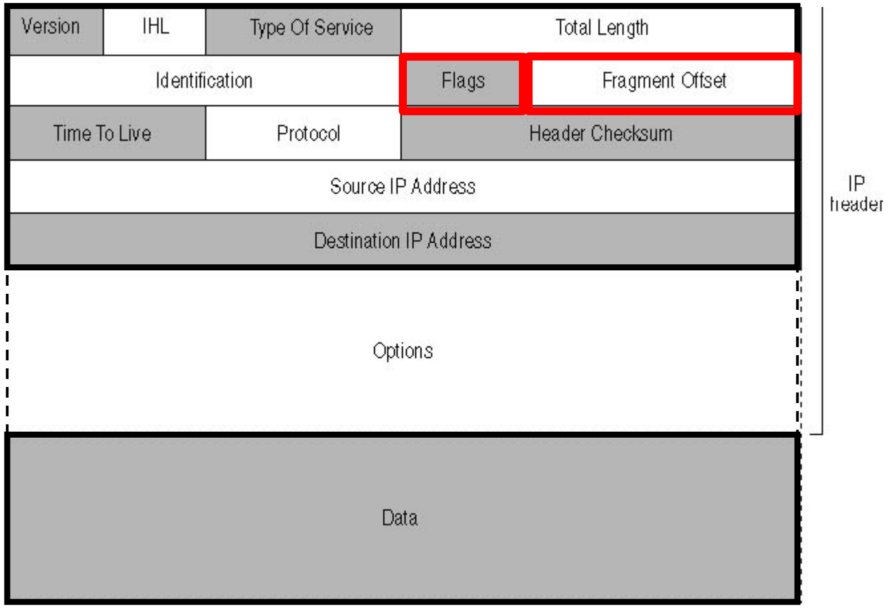
Datagram Format:

- **Flags (3 bits):**

  This field contains bits used to regulate the datagram fragmentation process.

- **Fragment Offset (13 bits):**

  When a datagram is fragmented, the system inserts a value in this field that identifies this fragment's place in the datagram. This will be discussed in more details in fragmentation section of this lecture.



➢ IPv4

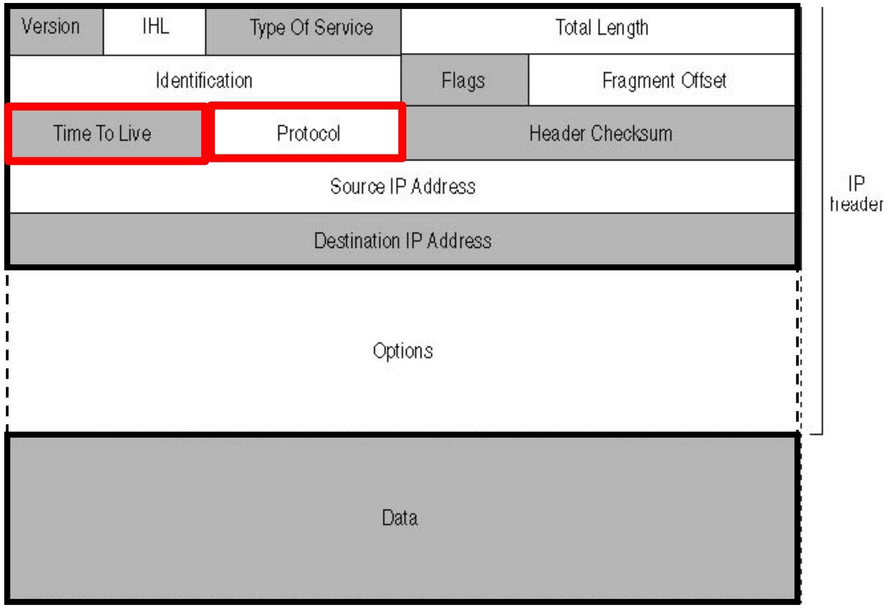
❖ Datagram Format:

- **Time To Live (TTL, 1 byte):**

  This field specifies the number of networks (hops) that the datagram is permitted to travel through on the way to its destination. Each router that processes the datagram reduces the value of this field by one. If the value reaches zero, the datagram is discarded.

- **Protocol (1 byte):**

  This field contains a code that identifies the protocol that generated the information found in the Data field.

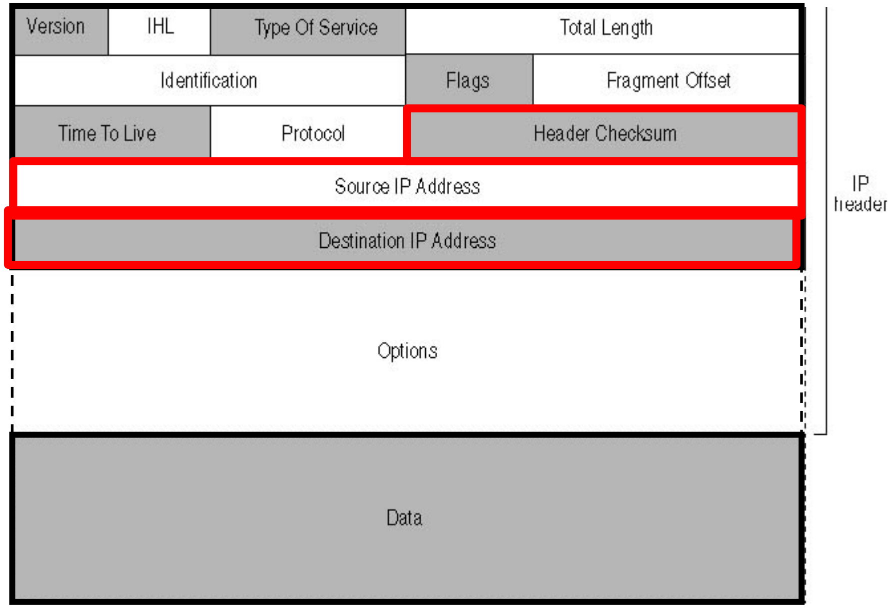


Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

Datagram Format:

- **Header Checksum (2 bytes):**
  This field contains a checksum value computed on the IP header fields only (and not the contents of the Data field) for the purpose of error detection.
- **Source IP Address (4 bytes):**
  This field specifies the IP address of the system that generated the datagram.
- **Destination IP Address (4 bytes):**
  This field specifies the IP address of the system for which the datagram is destined.



IPv4

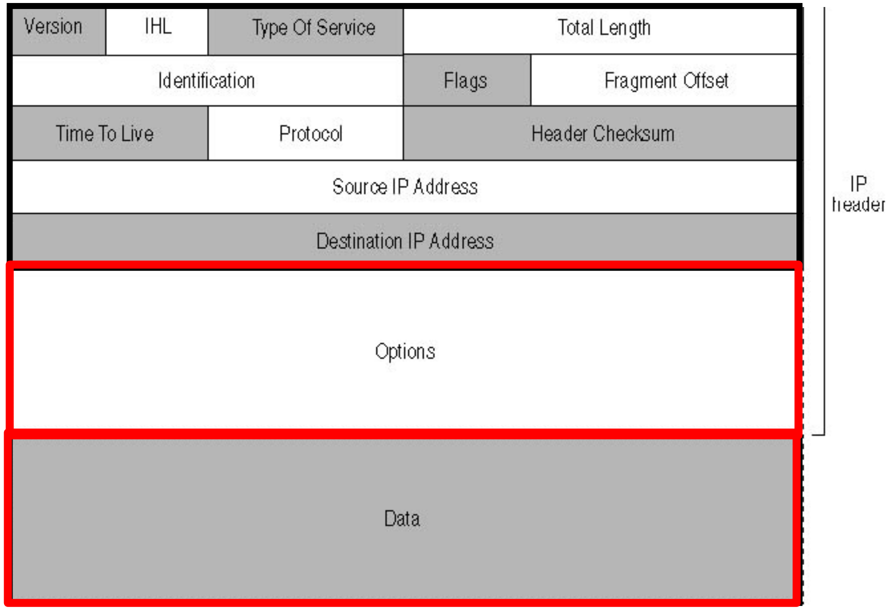
Datagram Format:

- **Options**

  This field is present only when the datagram contains one or more of the 16 available IP options. The size and content of the field depends on the number and the nature of the options and it should never exceed 40 Bytes.

- **Data**

  This field contains the information generated by the protocol specified in the Protocol field. The size of the field depends on the data-link layer protocol used by the network over which the system will transmit the datagram.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

Protocol Identification (2 Bytes)

The most commonly used values for the Protocol field are as follows:

- 6 TCP
- 17 UDP

IP Options (max 40 Bytes)

Some of the options defined in the IP standard are as follows:

- **Loose Source Route:** This option contains a list of router addresses that the datagram can use as it travels through the internetwork. The datagram also can use other routers in addition to those listed.
- **Strict Source Route:** This option contains a complete list of the router addresses that the datagram must use as it travels through the internetwork. The datagram cannot use any routers other than those listed.
- **Record Route:** This option provides an area in which routers can add their IP addresses when they process the datagram.
- **Timestamp:** This option provides an area in which routers can add timestamps indicating when they processed the datagram.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the followings is not a function of Network layer

a- MAC
b- Routing
c- End to End communication
d- Identify upper layer protocol

the Protocol ID field of a datagram that is destinated for UDP carries the hexadecimal code

a- 6
b- 71
c- 17
d- 9

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The field that describes the order of a fragment is:

a- Fragment offset
b- Protocol ID
c- Service Type
d- Fragment type

Header check sum field is used to detect

a- IPv4 data errors
b- IPv4 header errors
c- IPv4 options errors
d- IPv4 datagram errors

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#17: IPv4 Part II

By: Laith W. Abdullah

Objectives

- Detail the concept of fragmentation.
- Explain the role of ID, Flags and Frag. Offset in Fragmentation process.
- Clarify the error detection mechanism followed by IPv4.
- Give detailed examples on Fragmentation and Check sum determination

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

Fragmentation

- In an internetwork, routers are intermediate systems that are used to connect different networks.
- Routers can connect networks that use different media types and different data-link layer protocols.
- Forwarding a packet from an network to another requires re-encapsulating the packet in the outgoing network frame.
- The re-encapsulation process may require splitting the packet into smaller size packets called fragment due to the limited size of the outgoing network Maximum Transmission Unit (MTU).

IPv4

Fragmentation

- Fragments can themselves be split into smaller fragments.
- Once fragmented, the individual parts of a datagram are not reassembled until they reach the end system, which is their final destination.
- IP header fields that concerns fragmentation process are:
    - Identification
    - Flags
    - Fragment Offset.

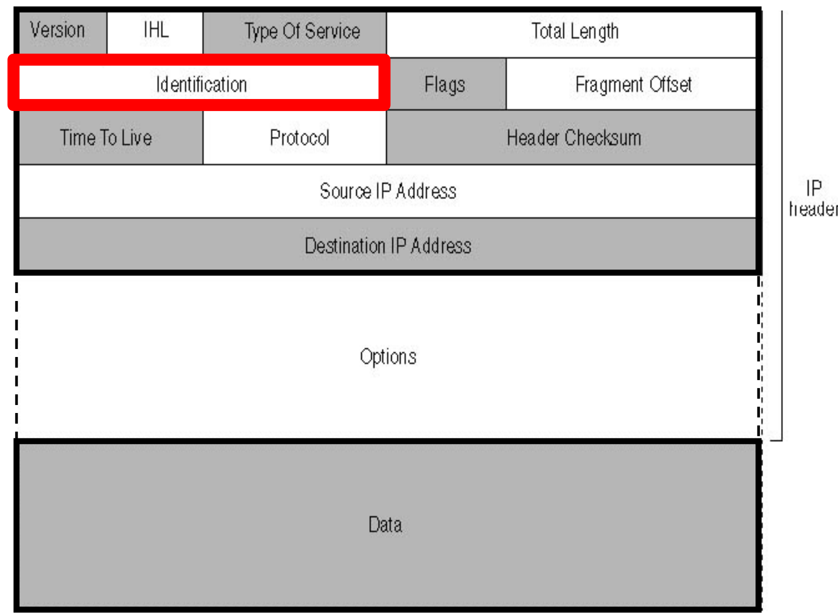
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

➢ Fragmentation

❖ Identification:-

- this field in combination with source IP field uniquely identifies a datagram.
- When this datagram is fragmented, all fragments carry the same value in the identification field.
- This is very important when the datagram need to be reassembled at the final destination to distinguish the fragments of a datagram that may be arrive out of order with respect to other datagrams or fragments.

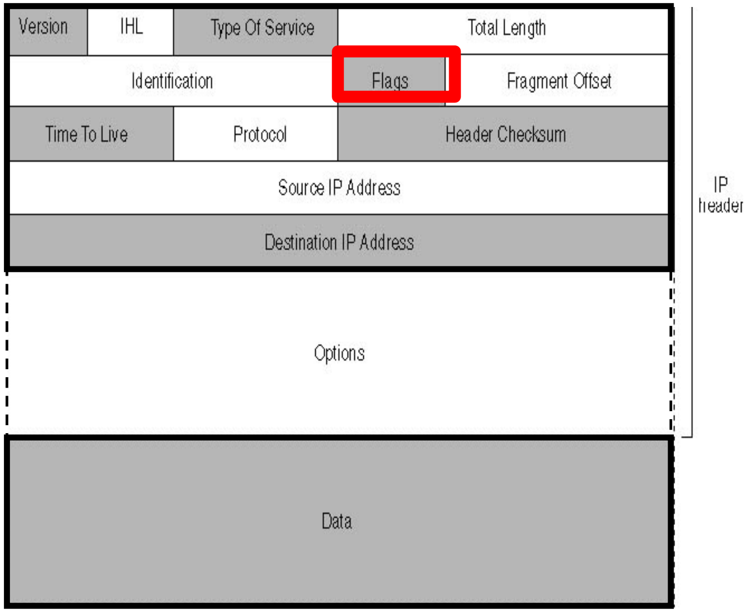


IPv4

➢ Fragmentation

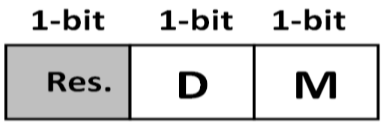
❖ Flags:

- This field consists of three bits.
- The first bit is reserved and it is (0).
- The other two flags (bits) are:



○ **Don't Fragment bit (D):**

When this flag is set (D=1) , the datagram is not allowed to be fragmented. If a router needs to fragment this datagram due MTU limitation of the next data-link network, the router is not allowed to do so and this datagram is discarded.



○ **More Fragment bit (M):**

in a fragmented datagram, this flag is set in all fragments (M=1) in all fragments except the last one. It also should be noted that the value of M equals zero in a non fragmented datagram.

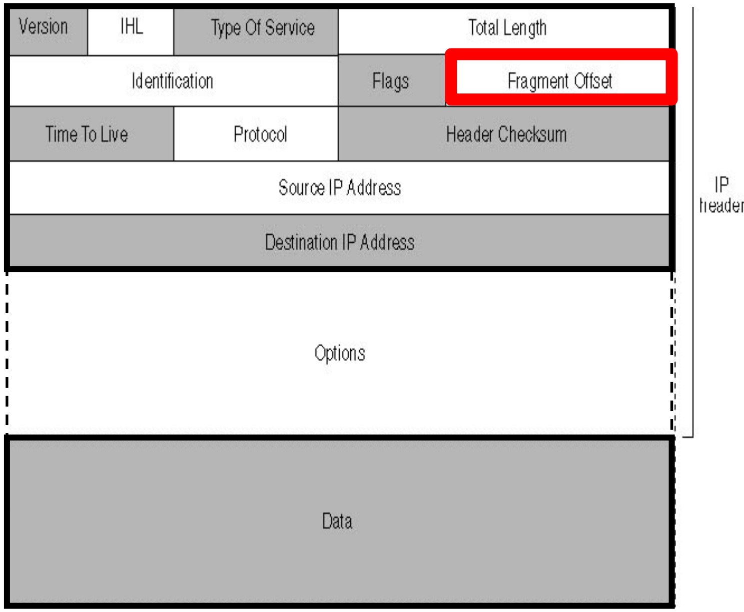
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

➢ Fragmentation

❖ Fragment Offset

- This field contains a value that specifies each fragment's place in the datagram with respect to other fragments.
- The value of this field gives total size of data fields in the previous fragments measured in 8-bytes.
- The first fragment has a value of 0 in this field, and the value in the second fragment is the size of data field in the first fragment. The third fragment's offset value is the size of data fields in the first two fragments, and so forth.



- The destination system uses these values to reassemble the fragments in the proper order.
- It should be noticed that in non fragmented datagram the value of fragment offset filed must be (0).

IPv4

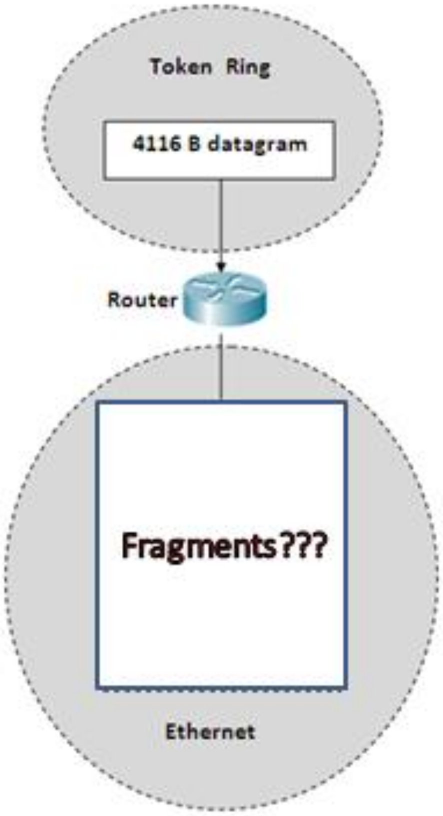
Fragmentation

Example:

Refer to the exhibit, show the fragmentation process of a 4116 Bytes datagram that has no option fields regarding to Total length, Identification, Flags, and Fragment Offset fields.

Solution:

- **The datagram is forwarded by the router from a Token Ring network to an Ethernet network.**
- **The datagram need to be fragmented so that it can encapsulated in Ethernet frames that has MTU equals 1500.**



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

Fragmentation

- The ID field carries the same value for all fragments.
- Don't fragment bit must be "0" that the datagram can be fragmented.
- More fragment bit is "1" in all fragments except the last fragment.
- The original packet carries (4116-20= 4096)B of data, since its header has no options.
- Since the original datagram has no options, all its fragments also have no options.
- Since the MTU of Ethernet is 1500, so the first datagram Total length field has a value of 1500 and it carries (1500-20=1480)B of data.
- The Fragment offset field in the first fragment is 0.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

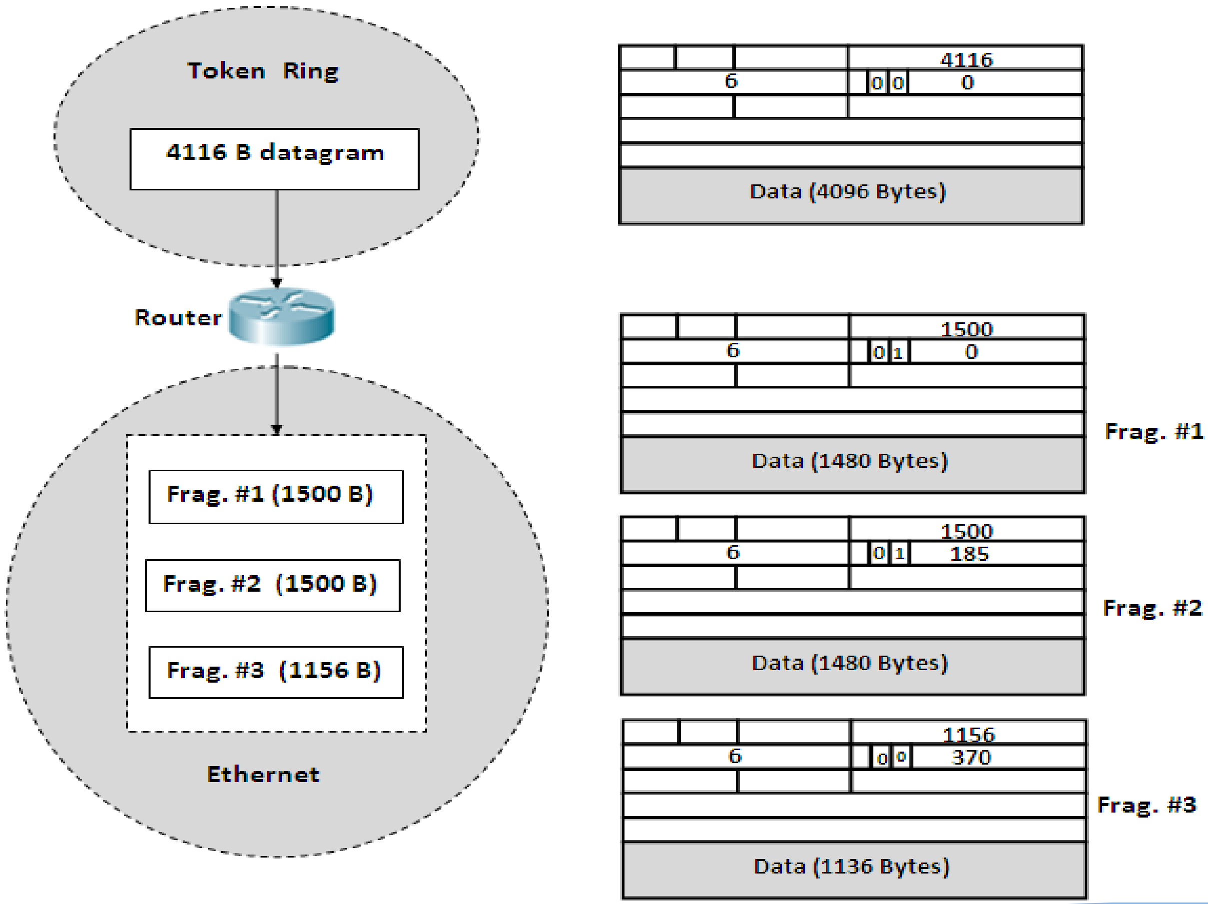
IPv4

Fragmentation

- Since the first fragment carries 1480B of the original 4096B datagram data, so the remaining data need to be fragmented. So, the second fragment which also 1500B total length will carry another 1480B of this data. Fragment offset field in this fragment will be (1480/8=185) which the size of the data in the first fragment divided by 8.
- Since the first and the second fragments carries (1480+1480=2960)B of the original 4096B datagram data, so the remaining data(4096-2960=1136)B does need to be fragmented. It will encapsulated in the third fragment which will have (1036+20=1056) value in total length field. Fragment offset field in this fragment will be (1480+1480/8=370) which the size of the data in the first and second fragments divided by 8.

IPv4

➢ Fragmentation



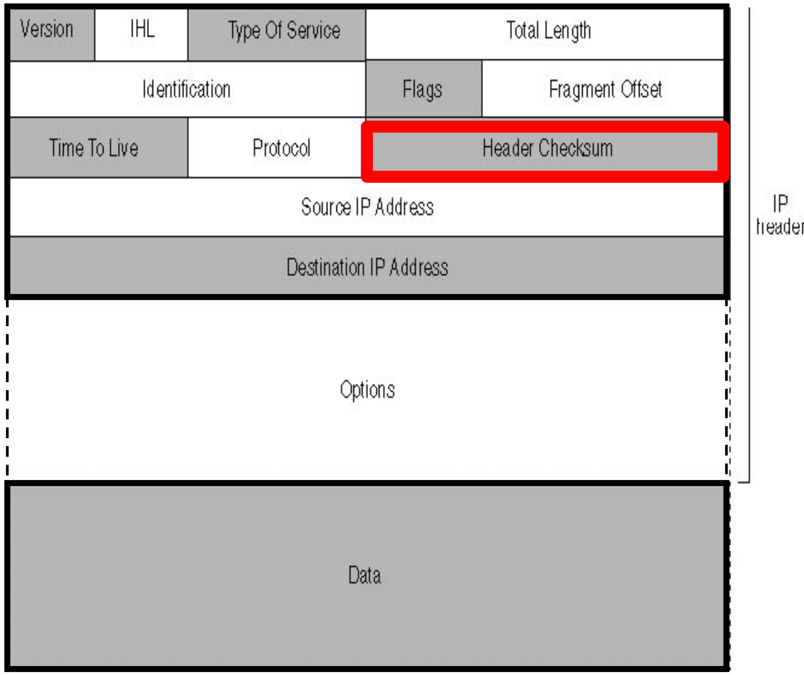
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

➢ Fragmentation

❖ Checksum:

- Header Checksum is the field dedicated in IP for error detection.
- In IP, checksum covers only the header of the datagram. This may be for two reasons:
    - upper layer protocols that delivers data for IP usually have checksums
    - only the header of the datagram may be altered with each router visited by the datagram.
- Checksum is calculated at the original source of the datagram, its final destination and intermediate systems (such as routers).



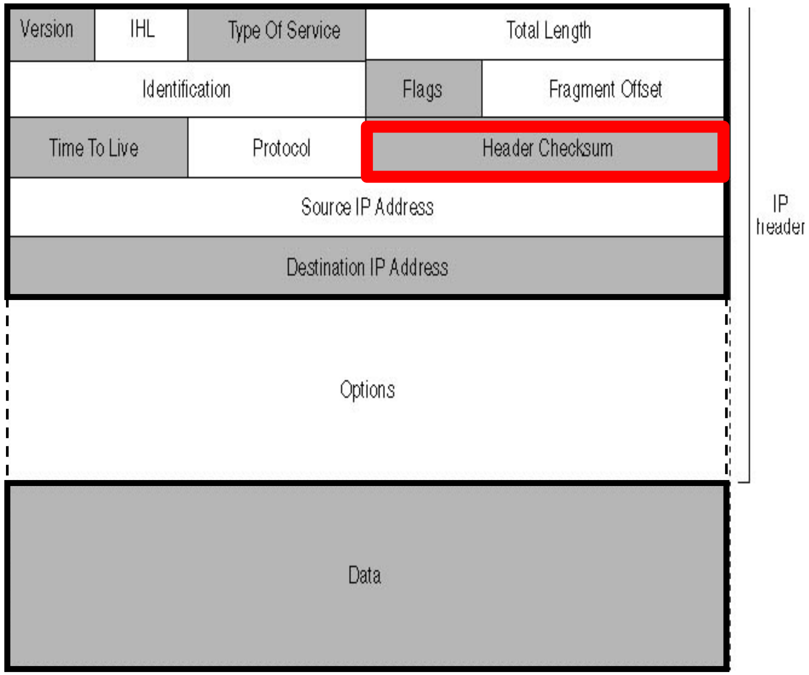
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

Error Detection

Checksum:

- Header Checksum is the field dedicated in IP for error detection.
- In IP, checksum covers only the header of the datagram. This may be for two reasons:
  - upper layer protocols that delivers data for IP usually have checksums
  - only the header of the datagram may be altered with each router visited by the datagram.
- Checksum is calculated at the original source of the datagram, its final destination and intermediate systems (such as routers).



IPv4

Fragmentation

Checksum:

- **Each system sends the datagram calculates the checksum value as follows:**
  - **First, the checksum value is set to (0).**
  - **The header of the datagram is divided into 16-bit sections.**
  - **The 16-bit sections are added together.**
  - **The summation result is complemented and transferred to the checksum field.**
- **While the system receives datagram checks it as follows**
  - **The header of the datagram is divided into 16-bit sections.**
  - **The 16-bit sections are added together.**
  - **The summation result is complemented, the result must be (0) for a correct datagram; else the datagram is rejected.11**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

➢ Error Detection

Example:

For the following datagram that has no option fields; calculate the checksum value.

<table>
<tr><td>4</td><td>5</td><td>0</td><td colspan="2">28</td></tr>
<tr><td colspan="3">1</td><td>0</td><td>0</td></tr>
<tr><td colspan="2">4</td><td>17</td><td colspan="2">Checksum ?</td></tr>
<tr><td colspan="5">10.12.14.5</td></tr>
<tr><td colspan="5">12.6.7.9</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv4

➢ Error Detection

❖ Solution:

4, 5, 0	→	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0
28	→	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0
1	→	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0 , 0	→	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4, 17	→	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1
Checksum (0)	→	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10, 12	→	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	0
14, 5	→	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0	1
12, 6	→	0	0	0	0	1	1	0	0	0	0	0	0	0	1	1	0
7, 9	→	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1
Sum		0	1	1	1	0	1	0	0	0	1	0	0	1	1	1	0
Checksum		1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	1

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the following fields does not engaged in fragmentation process

a- Destination address
b- Identifier
c- Fragment offset
d- Flags

Fragmentation is done due to outgoing network limited

a- MAU
b- MTU
c- CPU
d- UDC

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The datagram cannot be fragmented if

a- More fragment bit is set
b- Monitor bit is set
c- The outgoing network is FDDI
d- Don’t fragment bit is set

one of the following IPv4 header fields is not affected by routers

a- Source address
b- version
c- header checksum
d- Identification

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#18: Classful IPv4 Addressing

By: Laith W. Abdullah

Objectives

- Explain the structure of IPv4 address.
- Compare IPv4 addresses to MAC addresses
- Detail the classes of IPv4 address.
- Present the concepts of network and broadcast addresses.
- Explain the role of subnet mask.
- List the range of private IPv4 addresses and their role.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

- **IP address Assignment:**
  - For systems that are on the Internet, the Internet Assigned Numbers Authority (IANA) assigns network identifiers to ensure that there is no address duplication.
  - When an organization registers its network, it is assigned a network identifier.
  - When you are building a new network and want to obtain a registered network address, you now get one from an ISP, not directly from the IANA.
  - It is then up to the network administrators to assign unique host identifiers to each of the systems on that network.
  - IP addresses are divided into classes mainly for distinguishing the network and the host portion of the IP address. This leads to what is called "Classful IP addressing".
  - Another arrangement that do not depends calssess is adopted later, it is called "Classless IP addressing"

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

IP vs. MAC Addresses

IP addresses

- They define end devices (used for end to end communication)
- IP is 32bit address
- IP address is divided into two potions that defines both the network and the host in the network.
- It is called logical address because it can be assigned and changed by the administrator.

MAC Addresses

- They define local devices (used for node to node communication).
- MAC is 48bit address.
- MAC address is divided into two potions that defines OUI and the S/N of the hardware.
- It is called physical or hardware address because it is burned into the ROM of the NIC cannot be changed by the administrator.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

❖ Classful IP Addressing

- IANA defines five different classes of IP addresses (A,B,C,D and E), which provide support for networks of different sizes.
- Only the first three classes are used commercially (Classes A ,B and C).
- The decimal value of the first octet in the IP address decides the block it belongs to.
- Addresses 0.0.0.0 and 255.255.255.255 cannot be assigned for hosts.
- In class A, address 127.X.X.X is reserved for loopback.

Class	1st Octet Decimal Range	Network / Host ID (N=Network, H=Host)
A	1 - 127*	N.H.H.H
B	128 – 191	N.N.H.H
C	192 – 223	N.N.N.H
D	224 – 239	Reserved for Multicasting
E	240 - 254	Experimental, used for research

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

❖ Classful IP Addressing

- **Network fields and Host fields in A,B and C classes**

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network bits	Host bits	Number of Networks	Hosts per Network (usable addresses)
A	1 – 127	0	8	24	126 (2^7 - 2)	16,777,214 (2^{24} - 2)
B	128 - 191	1 0	16	16	16,384 (2^{14})	65,534 (2^{16} - 2)
C	192 - 223	1 1 0	24	8	2,097,152 (2^{21})	254 (2^8 - 2)

Classful IPv4 Addressing

- **Network and Broadcast addresses:**
  - **Network IP address:**
    - An IP address that ends with binary 0s (zeros) in all host bits.
    - Hosts on a network can only communicate directly with devices that have the same network ID
    - If the destination host has different network Address then it needs router(s) to access this destination.
  - **Broadcast IP address:**
    - it is the IP address that ends with binary 1s in the entire host part of the address (the host field).
    - A broadcast occurs when a host sends out data to all devices on its network.
    - A Broadcast address is used by the sender as a destination IP address when it wants its message to reach all the hosts into its network

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

❖ Network and Broadcast addresses:

Example:

Find the network address and the broadcast address of the host 210.10.12.30.

Solution:

- **The host is class C , that only the last byte is assigned for host bits ,thus**
- **The network address is: 210.10.12.0**
- **The broadcast address is: 210.10.12.255**

Classful IPv4 Addressing

❖ Subnetting :-

- **A subnetwork (subnet) is simply a subdivision of a network address.**
- **subnet addresses are assigned locally, usually by the network administrator. Also, like other IP addresses, each subnet address is unique.**
- **Subnet addresses include the Class A, Class B, or Class C network portion, plus a subnet field and a host field.**
- **The subnet field and the new host field are created from the original host portion for the entire network.**
- **To create a subnet address, a network administrator borrows bits from the host field and designates them as the subnet field.**

Classful IPv4 Addressing

Subnetting

- The minimum number of bits that can be borrowed is 2.
- The maximum number of bits that can be borrowed can be any number that leaves at least 2 bits remaining, for the host number.
- The primary reason for using subnets are:
    - Reducing the size of a broadcast domain, thus increase network efficiency.
    - Better usage of the available addressing space.
    - Better management

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

Subnet ing

- The **subnet mask** determines which part of an IP address is the network field and which part is the host field
- A subnet mask is 32 bits long and has 4 octets, just like an IP address.
- Just like the IP address , subnet mask is either assigned manually or automatically.
- **Expressing subnet in decimal**
- Express the subnet mask in binary form.
  - Replace the network and subnet portion of the address with all 1s.
  - Replace the host portion of the address with all 0s (zeros).
  - Convert the binary expression back to dotted-decimal notation.
- **Default subnet masks** of Class A, B, and C (Classes without subneting) are:

Class	Subnet Mask (binary)	Subnet Mask (decimal)
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111. 11111111.11111111.00000000	255.255.255.0

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

❖ Subnetting:

However, you can create multiple subnets within a given address class by using a different mask. But remember the followings:

- **The minimum number of bits that can be borrowed is 2.**
- **The maximum number of bits that can be borrowed can be any number that leaves at least 2 bits remaining, for the host number.**
- **Number of usable subnets created due to subnetting equals (2^n -2), where n is the number of subnet bits.**
- **Number of usable host addresses per each subnet equals (2^m -2), where m is the number of remaining host bits.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

Subnetting:

Example:

The TCP/IP settings of a host includes the following:

- IP address 200.10.12.10
- Subnet mask 255.255.255.240

What is the number of subnet bits in this network

Solution:

- This is a class C network where the default subnet mask is 255.255.255.0 which is (11111111.11111111.11111111.00000000) in binary.
- The given mask (255.255.255.240) is expressed in binary as (11111111.11111111.11111111.11110000)
- So 4 bits are borrowed from the original host bit field to form the new subnet field

Classful IPv4 Addressing

ANDing Process

- Hosts and routers use the "ANDing" process to determine if a destination host is on the same network or not.
- The ANDing process is done each time a host wants to send a packet to another host on an IP network.
- ANDing process procedure:
  - First the source host will compare (AND) its own IP address to its own subnet mask. The result of the ANDing is to identify the network or subnet where the source host resides. It will then compare the destination IP address to its own subnet mask.
  - The result of the 2nd ANDing will be the network or subnet that the destination host is on.
  - If the source network or subnet address and the destination network or subnet address are the same they can communicate directly.
  - If the results are different then they are on different networks or subnets and will need to communicate through routers or may not be able to communicate at all.

Classful IPv4 Addressing

❖ Private IP Addresses

- There are certain addresses in each class of IP address that are not registered. Network administrator can freely assign these addresses without obtaining them from an ISP or the IANA.
- Private addresses might be used by hosts that use a proxy server, to connect to a public (registered) network.
- They also might be used by hosts that do not connect to the Internet at all.
- By agreement, any traffic with a destination address within one of the private address ranges will not be routed on the Internet.

Class	Network Address
A	10.0.0.0 through 10.255.255.255
B	172.16.0.0 through 172.31.255.255
C	192.168.0.0 through 192.168.255.255

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Number of Class A public addresses is

a- 256
b- 126
c- 125
d- 128

IPv4 address is divided into two parts that defines

a-network ID and host ID
b- OUI and serial number
c- upper protocol and lower protocol
d- TCP and UDP

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Network address is obtained by

a- ANDing host IP address to its subnet mask
b- ANDing host IP address to routers IP address
c- ANDing host IP address to destination subnet mask
d- non of the previous

maximum number of subnets that can be created in the network 200.10.10.0 is

a- 128
b- 256
c- 46
d- 64

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#19: *Classful IPv4 Addressing*

Examples

By: *Laith W. Abdullah*

Classful IPv4 Addressing

Example1:

Your company has been given a 200.10.57.0 network address. You need to divide your network into two subnets (X and Y) using a router, Answer the following questions.

1. What is the network class.
2. How many bits needed to be borrowed form the host field to the subnet field.
3. What is the actual number of hosts per subnet
4. What is the usable number of hosts per subnet
5. What is the subnet mask.
6. What is the IP addresses of the routers NICs at both subnets. Assuming that routers NICs at subnets X and Y takes the first usable host IP addresses at the first and second usable subnets respectively.
7. Explain the ANDing process when a compute named X1 takes the second usable host IP address at subnet X sends a packet to a second computer named Y1 and takes the second usable host IP address at subnet Y.
8. What is the percentage of IP addresses lost due to subnetting

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

1. What is the network class?

Since the first octet in the network address is 200, then the IP address is class C because class C IP addresses 1st octet ranges from 192-223.

2- How many bits needed to be borrowed form the host field to the subnet field?

Since the number of usable subnets =2
Then $2= 2^n-2$
So n=2 , where n is the number of bits to be borrowed from the original host field to the subnet field.

3- What is the actual number of hosts per subnet?

Since the network is class C, and two bits are borrowed to the subnet field, so we have 6 bits remains at the new host field, thus
The actual number of hosts per subnet = 2^6 = 64

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

4- What is the usable number of hosts per subnet?

Since the first and last host addresses per subnet are used for network address and broad cast address respectively. Then

The usable number of hosts per subnet = 2^6-2= 62

5- What is the subnet mask?

We have a class C network with two host bits borrowed from the fourth octet to the the subnet field, so the binary subnet mask can be formed by putting 1's in the network and subnet fields and 0's in the host field as follows:

1st octet	2nd octet	3rd octet	4th octet	
N	N	N	S	H
11111111	11111111	11111111	11	000000

And the decimal subnet mask will be:

255.255.255.192

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

6- What is the IP addresses of the routers NICs at both subnets. Assuming that routers NICs at subnets X and Y takes the first usable host IP addresses at the first and second usable subnets respectively?

Subnet No.	Subnet bits binary value	Host bits binary values	Subnet / Host Decimal range	Usable Hosts IP addresses	Useable subnet
Subnet #0	00	000000 - 111111	0 – 63	200.10.57.1-200.10.57.62	NO
Subnet #1	01	000000 - 111111	64 - 127	200.10.57.65-200.10.57.126	YES
Subnet #2	10	000000 - 111111	128 - 191	200.10.57.129-200.10.57.190	YES
Subnet #3	11	000000 - 111111	192 - 255	200.10.57.193-200.10.57.254	NO

From the table above :

The IP address of the router NIC at subnet X is 200.10.57.65

The IP address of the router NIC at subnet Y is 200.10.57.129

Classful IPv4 Addressing

7- Explain the ANDing process when a compute named X1 takes the second usable host IP address at subnet X sends a packet to a second computer named Y1 and takes the second usable host IP address at subnet Y.

a-X1 ANDing its IP address to the subnet mask

X1 binary IP address:	11001000 . 00001010 . 00111001 . 01000010
Binary subnet mask :	11111111 . 11111111 . 11111111 . 11000000
Binary anding result :	11001000 . 00001010 . 00111001 . 01000000
Decimal ANDing result is:	200.10.57.64

So the subnet to which X1 belongs is 200.10.57.64

b- X1 ANDing Destination (Y1) IP Address to the subnet mask

Y1 binary IP address:	11001000 . 00001010 . 00111001 . 10000010
Binary subnet mask :	11111111 . 11111111 . 11111111 . 11000000
Binary anding result :	11001000 . 00001010 . 00111001 . 10000000
Decimal ANDing result is:	200.10.57.128

So the subnet to which Y1 belongs is 200.10.57.128

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

7- Explain the ANDing process when a compute named X1 takes the second usable host IP address at subnet X sends a packet to a second computer named Y1 and takes the second usable host IP address at subnet Y.

c- from the results of ANDing processes in steps a and b the Host X1 finds that the destination host Y1 lies on another subnet so it forwards the packet to router NIC at the subnet X side. The router then forwards the packet to the router NIC at subnet Y which forwards it to host Y1. (if the result from steps a and b is the same, meaning that source and destination hosts on the same subnet, then the source host directs the packet directly to the destination host)

Classful IPv4 Addressing

8- What is the percentage of IP addresses lost due to subnetting?

a- Actual number of hosts in class C network without subnetting is 256

b- Number of IP addresses lost by unusable subnets in this example is

(2* actual number of hosts/ subnet) = 2*64 = 128

c- number of IP addresses lost in each usable subnet is

(2* number of usable subnets) = 2*2 =4

d- percentage loss of IP addresses = [(c+b) /a]* 100%= (132/256)*100% = 52%

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

Example2:

Your institute is given a network address 150.193.0.0 . This address must be subdivided to get at least 200 host per subnet. Answer the followings.

1. **what is the network class.**
2. **How many bits needed to be borrowed to the subnet filed.**
3. **What is the subnet mask**
4. **What is the IP address of the first host in the fifth usable subnet.**
5. **What is the number of IP addresses lost by subnetting.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

1. what is the network class?

Since the first octet in the network address is 150, then the IP address is class B because class B IP addresses 1st octet ranges from 128-191.

2. How many bits needed to be borrowed to the subnet filed?

Since the number of hosts =200

Then $200 \le 2^m - 2$

So m=8 ,

And since the total number of bits in the original host filed is 16, then the remaining bits to be borrowed to the subnet field is 8.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

3- What is the subnet mask?

We have a class B network with eight host bits borrowed from the 3rd octet to the subnet field, so the binary subnet mask can be formed by putting 1's in the network and subnet fields and 0's in the host field as follows

1st octet	2nd octet	3rd octet	4th octet
N	N	S	H
11111111	11111111	11111111	00000000

And the decimal subnet mask will be 255.255.255.0

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

4- What is the IP address of the first host in the fifth usable subnet?

Subnet No.	Subnet bits (binary value)	Host bits (binary values)	Usable range of Hosts IP addresses	Useable subnet
Subnet #0	00000000	00000000 - 11111111	150.193.0.1-150.193.0.254	NO
Subnet #1	00000001	00000000 - 11111111	150.193.1.1-150.193.1.254	YES
Subnet #2	00000010	00000000 - 11111111	150.193.2.1-150.193.2.254	YES
⋮	⋮	⋮	⋮	⋮
Subnet #5	00000101	00000000 - 11111111	150.193.5.1-150.193.5.254	YES
⋮	⋮	⋮	⋮	⋮
Subnet #254	11111110	00000000 - 11111111	150.193.254.1-150.193.254.254	YES
Subnet #255	11111111	00000000 - 11111111	150.193.255.1-150.193.255.254	NO

So, the first usable host IP address in the 5th subnet 150.193.5.1

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classful IPv4 Addressing

5- What is the number of IP addresses lost by subnetting?

a- Number of IP addresses lost by unusable subnets in this example is

(2* actual number of hosts/ subnet) = 2*256 = 512

b- number of IP addresses lost in each usable subnet is

(2* number of usable subnets) = 2*254 =508

c- IP addresses lost by subnetting = 512+508= 1020

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Lec.#18: Classless IPv4 Addressing
Part I

By: Laith W. Abdullah

Objectives

- Discuss the reasons lead to Classless addressing
- Explain how subnet masks can be expressed in CIDR notation
- Details fixed length subnetting in Classless IPv4 addressing.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

- Since 1996 Internet authorities announce another addressing architecture called classless IP addressing.
- This architecture overcomes the main problem of classful IP addressing (better usage of the available addressing space)
- In IP addressing the address space (2^{32}) is divided into blocks of different sizes. (while the block size is fixed in classfull IP addressing to be a multiple of 256)
- The block belongs to no class and thus this addressing architecture is named classless IP addressing.
- Number of addresses in the block is a power of 2 (2^1, 2^2, 2^3, …).
- The block in classful IP addressing can be subnetted into only fixed length subnets while the subnets in classless IP addressing can be fixed or variable length.
- The first address in the block (block address or network address) must be divisible by the number of addresses in this block.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

Example:

Which of the followings can be used for a block that contains 1024 address:

a- 205.16.37.32 c-17.17.32.0

b- 190.16.42.0 d- 123.45.24.52

Answers:

The decimal number that equals the entire IP address can be found by

(1st octet) x 256^3 + (2nd octet) x 256^2 + (3rd octet) x 256^1 + (4th octet) x 256^0

So for :

a- (205 x256^3 + 16 x 256^2 + 37 x 256 + 32) / 1024 = 3359753.281

b- (190 x256^3 + 16 x 256^2 + 42 x 256 + 0) / 1024 = 3113994.5

c- (17 x256^3 + 17 x 256^2 + 32 x 256 + 0) / 1024 =279624

d- (123 x256^3 + 45 x 256^2 + 24 x 256 + 52) / 1024 = 2018118.051

So, it is clear that only c (17.17.32.0) can be used because it is divisible by 1024.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

CIDR Notation

- Subnet masks can be expressed in another form called CIDR (Classless Inter Domain Routing) notation.
- In this form the mask is expressed as (/ n) where n is the number of bits in the network portion of the IP address.
- So all classless addresses are expressed in the CIDR notation form; which is expressed in general as:

x . y . z . t / n

- prefix and prefix length“: prefix is netid part of the IP address while prefix length is the number of bits in the prefix (it is n in the CIDR notation).
- suffix and suffix length: suffix is the hostid part of the IP address while suffix length equals (32-n).

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ CIDR Notation

Example:

for the block 17.17.32.0 / 22, find:
1- subnet mask.
2-suffix length.

Solution:

1- Since the CIDR notation n=22, then the subnet mask is 255.255.252.0
2- suffix length = 32-n = 10

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ **Finding the block**

- **Block boundaries are clear in classful IP addressing because block sizes are fixed to multiples of 256, while this is not the case in classless IP addressing.**
- **To find the block of addresses in classless addressing. It is necessary to find the followings:**
  - **First address in the block:**

    It can be found by ANDing any address in the block with the subnet mask
  - **Number of addresses in the block:**

    Actual number of addresses in the block is (2^{32-n}). while the useable number of addresses in the block equals the actual number of addresses in the block minus two.
  - **Last address in the block:**

    It can be found by adding the 1st address in the block with the complement of the subnet mask.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Finding the block

Example:

Find the block if one of the addresses is 190.87.140.202 / 29.

a- Finding the first address: is found by ANDing the address (190.87.140.202) with the subnet mask (255.255.255.248).

10111110.01010111.10001100.11001010
11111111.11111111.11111111.11111000
10111110.01010111.10001100.11001000

So, The first address in the block is (190.87.140.200 / 29)

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ **Finding the block**

b- Number of addresses in the block = $2^{32-n} = 2^{32-29} = 2^3 = 8$

c- Last address in the block can be found by adding the 1st address in the block (190.87.140.200) with the complement of the subnet mask (0.0.0.7)

```
 10111110.01010111.10001100.11001000
 00000000.00000000.00000000.00000111
 -----------------------------------
 10111110.01010111.10001100.11001111
```

So, The last address in the block is (190.87.140.207 / 29)

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

Fixed length subnetting

- As in calssful subnetting, sizes of subnets in this method is **fixed.**
- Number of subnets is a power of two and the useable number of subnets in classless addressing is ($2^{\text{number of subnet bits}}$).

Example:

An organization is granted the block 130.34.12.64 /26. The organization use a router to subnet the block into four subnets .

Answer the followings:

1- What is the number of addresses in the original block.

2- What is the last address in the original block.

3- What is the range of useable addresses in the original block.

4- The CIDR notation after subnetting.

5- The useable range of hosts IP addresses in each subnet.

6- What is the number of hosts IP addresses lost due to subnetting.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Fixed length subnetting

Answers:

1- The number of addresses in the block = $2^{32-26} = 2^6 = 64$

2- The last address in the block can be found by adding the 1st address in the block to the number of IP addresses in the block minus one (64 -1= 63)

```
  1 0 0 0 0 0 1 0 . 0 0 1 0 0 0 1 0 . 0 0 0 0 1 1 0 0 . 0 1 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 1 1 1 1 1 1
  -----------------------------------------------------------------------
  1 0 0 0 0 0 1 0 . 0 0 1 0 0 0 1 0 . 0 0 0 0 1 1 0 0 . 0 1 1 1 1 1 1 1
```

So, the last address in the block 130.34.12.127 /26

3- The first and the last address in the block cannot be assigned to hosts, so the range of useable addresses is

130.34.12.65 /26 – 130.34.12.126 /26

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Fixed length subnetting

4- $2^{\text{No. of subnet bits}}$ = no. of subnets

$2^{\text{No. of subnet bits}} = 4$

No. of subnet bits =2

So, the CIDR becomes /28 (instead of /26 in the original block)

5- The range can be determined as follows

Subnet No.	Subnet bits (binary value)	Host bits (binary values)	Useable range of Hosts IP addresses
Subnet #0	00	0000 – 1111	130.34.12.65 /28 -130.34.12.78 /28
Subnet #1	01	0000 – 1111	130.34.12.81 /28 -130.34.12.94 /28
Subnet #2	10	0000 – 1111	130.34.12.97 /28 -130.34.12.110 /28
Subnet #3	11	0000 – 1111	130.34.12.113 /28 -130.34.12.126 /28

6- The number of hosts IP addresses lost due to subnetting=2 x No. of subnets=2 x4 = 8

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

The main reason for classless addressing is

a- better usage of the available addressing space
b- more security by encrypting datagrams
c- more compatibility with upper layers protocols
d- more classes than other types of addressing

One of the followings can be used as block address for an 1024 host network

a-network ID and host ID
b- OUI and serial number
c- upper protocol and lower protocol
d- TCP and UDP

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

Only one of the followings can be assigned as a host address

a- 100.10.50.192 /28
b- 200.60.6.7 /29
c- 100.256.70.10 /24
d- 210.60.50.40 /25

Number of hosts in the block 20.30.50.0 /22 is

a- 1024
b- 2024
c- 1048
d- non of the previous

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#21: Classless IPv4 Addressing
Part II

By: Laith W. Abdullah

Objective

- **Details variable fixed length subnetting in Classless IPv4 addressing.**

Classless IPv4 Addressing

Variable length subnetting:

- in classless addressing subnets can be designed to fit your needs. Subnets can be of different sizes and this gives better usage of hosts IP addresses.
- In variable length subnetting we start with the largest subnet(s) followed by the rest descendingly.
- Larger subnets that are left can further subnetted to obtain smaller subnets and the smaller subnets may subjected to further subnetting.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Variable length subnetting:

Example:

A big company is granted the block 14.24.74.0 /24. The company needs to subnet this block as follows:

a- One subnet with 60 hosts.

b- Two subnets, each with 28 hosts.

c- Three subnets, each with 10 hosts.

d- Two subnets, each with 2 hosts.

Answer the followings:-

1- Can fixed length subnetting used to subnet network.

2- What is the actual range of IP addresses in each subnet.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Variable length subnetting:

Answers:

1- Total number of subnets = 1 + 2 + 3 + 2= 8

So, if we use fixed length subnetting; then

$2^{\text{No. of subnet bits}} \geq 8$ ⇨ No. of subnet bits = 3 which leaves only five host bits in each subnet; and since 5 host-bits gives up to (2^5 -2 =30) hosts in each subnet while the company's needs exceeds this number (60 hosts in the first subnet). So in this example, variable length subnetting must be used.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

2-

i) In variable length subnetting, we start with the largest subnet(s). So we start with the 60-host subnet. In this subnet

$2^{\text{No. of host bits}} - 2 \geq 60$ ➪ No. of host bits = 6

No. of subnet bits = 8 - No. of host bits = 8 - 6 =2

Then the subnet mask is /26

And the actual range is:

Subnet No.	Subnet bits (binary value)	Host bits (binary values)	Actual range of IP addresses	Used /Available
Subnet #0	00	000000 – 111111	14.24.74.0 /26 -14.24.74.63 /26	Used
Subnet #1	01	000000 – 111111	14.24.74.64 /26 -14.24.74.127 /26	Available
Subnet #2	10	000000 – 111111	14.24.74.128 /26 -14.24.74.191 /26	Available
Subnet #3	11	000000 – 111111	14.24.74.192 /26 -14.24.74.255 /26	Available

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

ii) For the next largest subnet(s) (the next two 28-host subnets) , the number of addresses in these two subnets must be at least (28+28+2+2=60) , so we the next available subnet (14.24.74.64 /26) which actually contains (2^6=64) addresses can be used to address these two subnets.

$2^{\text{No. of host bits}} - 2 \geq 28$ ⇨ No. of host bits = 5

No. of subnet bits = 6 - No. of host bits = 6 - 5 =1

Then the subnet mask is /27

And the actual range is:

Subnet No.	Subnet bits (binary value)	Host bits (binary values)	Actual range of IP addresses	Used /Available
Subnet #1.0	01 0	00000 –11111	14.24.74.64 /27 -14.24.74.95 /27	Used
Subnet #1.1	01 1	00000 – 11111	14.24.74.96 /27 -14.24.74.128 /27	Used
Subnet #2	10	000000 – 111111	14.24.74.128 /26 -14.24.74.191 /26	Available
Subnet #3	11	000000 – 111111	14.24.74.192 /26 -14.24.74.255 /26	Available

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Variable length subnetting:

ii) For the next largest subnet(s) (the next two 28-host subnets) , the number of addresses in these two subnets must be at least (28 +28 +2+2 =60) , so we the next available subnet (14.24.74.64 /26) which actually contains (2^6 =64) addresses can be used to address these two subnets.

$2^{\text{No. of host bits}} - 2 \geq 28$ ⇨ No. of host bits = 5

No. of subnet bits = 6 - No. of host bits = 6 - 5 =1

Then the subnet mask is /27

And the actual range is:

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Variable length subnetting:

Subnet No.	Subnet bits (binary value)	Host bits (binary values)	Actual range of IP addresses	Used /Available
Subnet #1.0	01 0	00000 –11111	14.24.74.64 /27 -14.24.74.95 /27	Used
Subnet #1.1	01 1	00000 – 11111	14.24.74.96 /27 -14.24.74.128 /27	Used
Subnet #2	10	000000 – 111111	14.24.74.128 /26 -14.24.74.191 /26	Available
Subnet #3	11	000000 – 111111	14.24.74.192 /26 -14.24.74.255 /26	Available

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Variable length subnetting:

iii) For the next large subnet(s) (the next three 10-host subnets) , the number of addresses in these three subnets must be at least (10 + 10 + 10+2+2+2=36) , so the next available subnet (14.24.74.128 /26) which contains actually contains (64) addresses is further subnetted.

$2^{\text{No. of host bits}} - 2 \geq 10$ ➪ No. of host bits = 4

No. of subnet bits = 6 - No. of host bits = 6 - 4 =2

Then the subnet mask is /28

The range of actual addresses in these subnets is

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Variable length subnetting:

Subnet No.	Subnet bits (binary value)	Host bits (binary values)	Actual range of IP addresses	Used /Available
Subnet #2.0	10 00	0000 –1111	14.24.74.128 /28 -14.24.74.143 /28	Used
Subnet #2.1	10 01	0000 –1111	14.24.74.144 /28 -14.24.74.159 /28	Used
Subnet #2.2	10 10	0000 –1111	14.24.74.160 /28 -14.24.74.175 /28	Used
Subnet #2.3	10 11	0000 –1111	14.24.74.176 /28 -14.24.74.191 /28	Available
Subnet #3	11	000000 – 111111	14.24.74.192 /26 -14.24.74.255 /26	Available

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

❖ Variable length subnetting:

iv) For the rest subnet(s) (the next two 2-host subnets) , the number of addresses in these three subnets must be at least (2 +2+2+2 =8) , so we subnet the next available subnet (14.24.74.176 /28) which actually contains (16) addresses is further subnetted.

$2^{\text{No. of host bits}} - 2 \geq 2$ ⇨ No. of host bits = 2

No. of subnet bits = 4 - No. of host bits = 4 - 2 =2

Then the subnet mask is /30

The range of actual addresses in these subnets is

Classless IPv4 Addressing

❖ Variable length subnetting:

Subnet No.	Subnet bits (binary value)	Host bits (binary values)	Actual range of IP addresses	Used /Available
Subnet #2.3.0	10 11 00	00 –11	14.24.74.176 /30 -14.24.74.179 /30	Used
Subnet #2.3.1	10 11 01	00 –11	14.24.74.180 /30 -14.24.74.183 /30	Used
Subnet #2.3.2	10 11 10	00 –11	14.24.74.184 /30 -14.24.74.187 /30	Available
Subnet #2.3.3	10 11 11	00 –11	14.24.74.188 /30 -14.24.74.191 /30	Available
Subnet #3	11	000000 – 111111	14.24.74.192 /26 -14.24.74.255 /26	Available

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Classless IPv4 Addressing

Note that the ranges in the two available subenets (14.24.74.184 /30) and (14.24.74.88 /30) can be merged into one subnet (14.24.74.184 /29).

So the whole range of addresses in this network

Subnet No.	Actual range of IP addresses	Used /Available
Subnet #0	14.24.74.0 /26 -14.24.74.63 /26	Used
Subnet #1.0	14.24.74.64 /27 -14.24.74.95 /27	Used
Subnet #1.1	14.24.74.96 /27 -14.24.74.128 /27	Used
Subnet #2.0	14.24.74.128 /28 -14.24.74.143 /28	Used
Subnet #2.1	14.24.74.144 /28 -14.24.74.159 /28	Used
Subnet #2.2	14.24.74.160 /28 -14.24.74.175 /28	Used
Subnet #2.3.0	14.24.74.176 /30 -14.24.74.179 /30	Used
Subnet #2.3.1	14.24.74.180 /30 -14.24.74.183 /30	Used
	14.24.74.184 /29 -14.24.74.191 /29	Available
	14.24.74.192 /26 -14.24.74.255 /26	Available

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#22: *IPv6* *Part I*

By: *Laith W. Abdullah*

Objectives

- Present the new features of IPv6 over IPv4.
- Detail the format of IPv6 datagram.
- Compares the formats of IPv6 and IPv4 datagrams.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

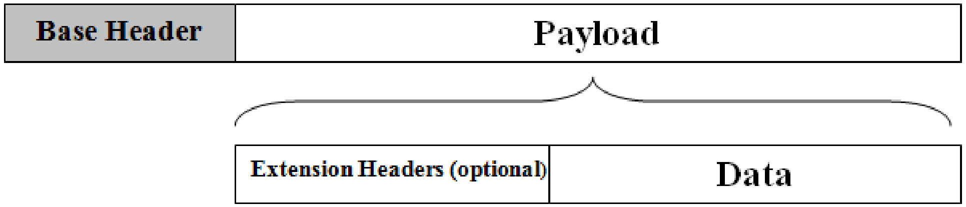
IPv6

❖ What is new in IPv6?

- Larger addressing space
- Supporting real time audio and video applications
- High security.

❖ IPv6 Datagram Format

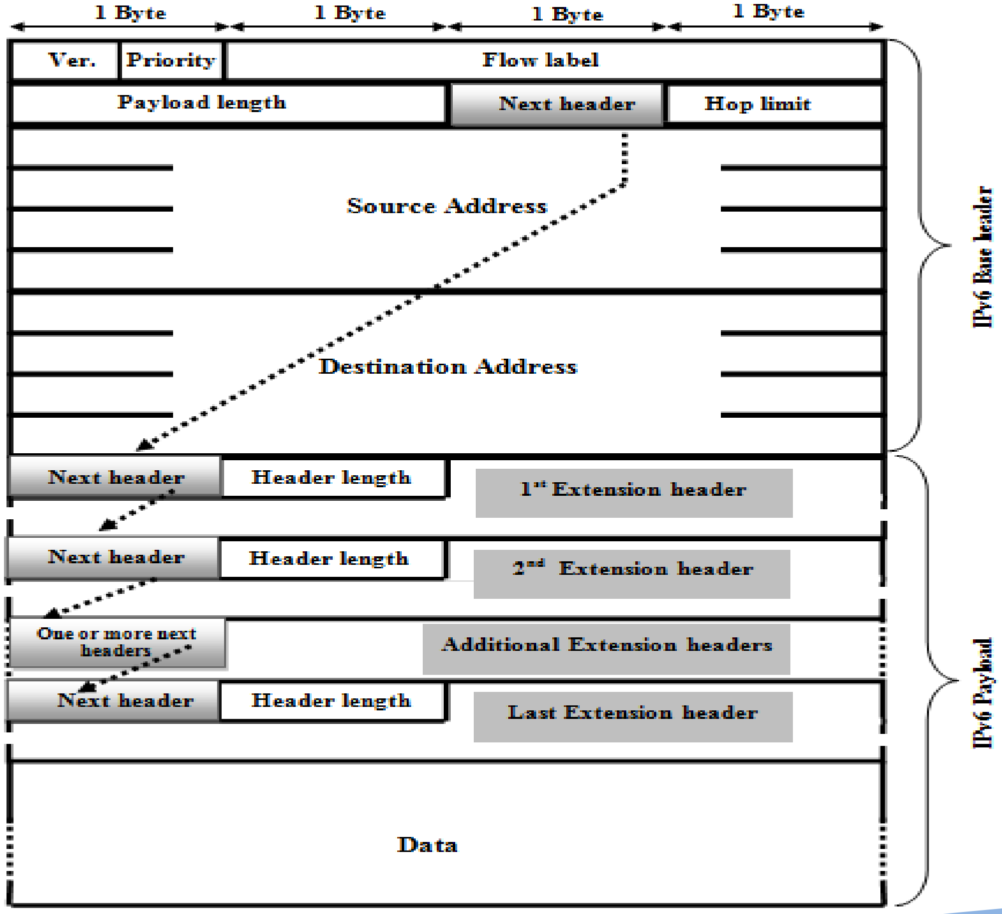
- IPv6 datagram consists of two parts:
  - Base header of 40B.
  - payload up to 65,536B.
- The payload consists of:
  - Extension headers(optional)
  - Upper Layer data.



Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

IPv6 Datagram Format



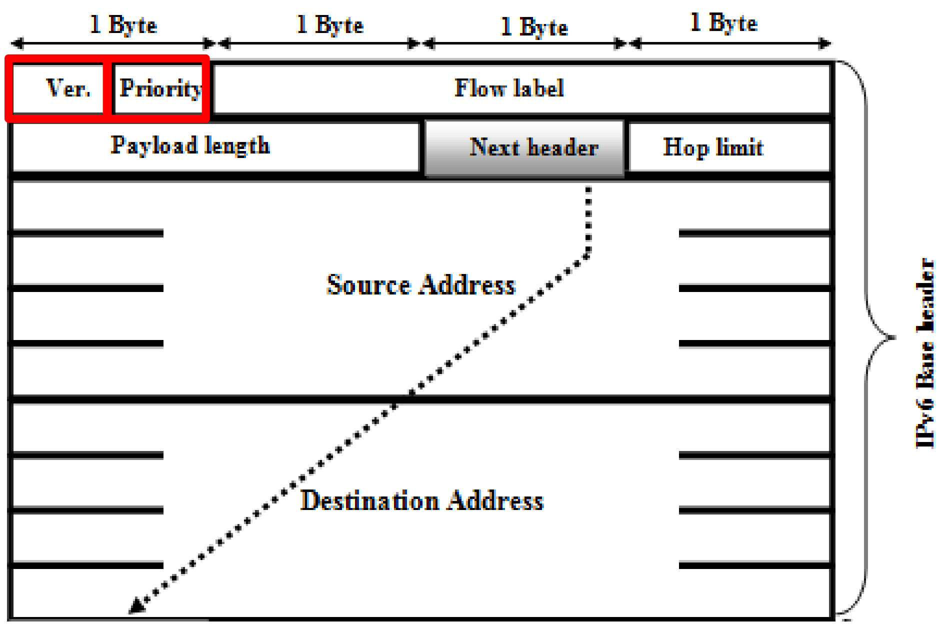
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

❖ IPv6 Datagram Format

➢ Base header

- **Ver. (4 bits):** This field specifies the version of the IP which is 6 for IPv6.
- **Priority (4 bits):** This field defines the priority of the datagram with respect to other datagrams of the same source. The highest value in this field yields the highest priority.

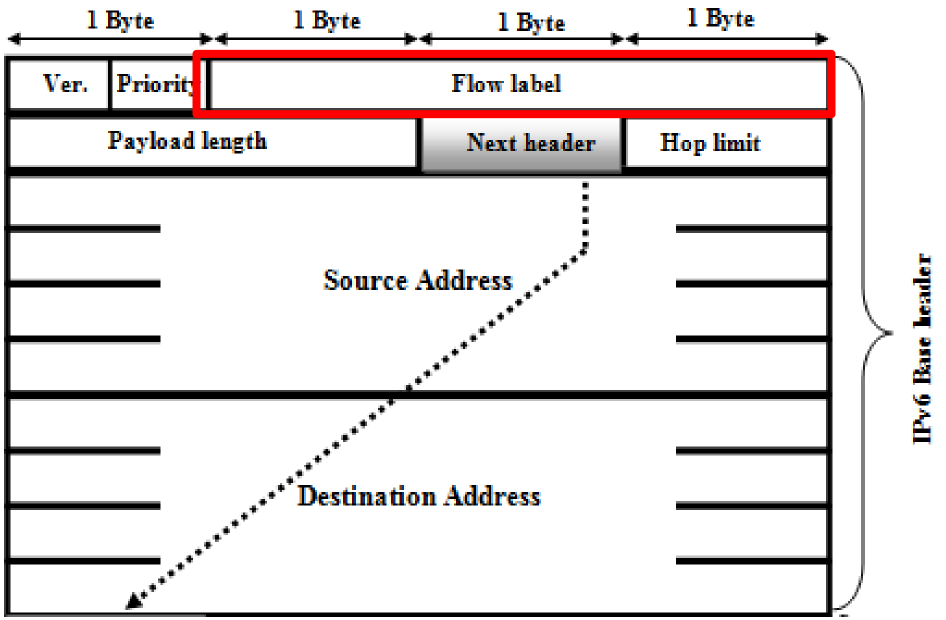


IPv6

❖ IPv6 Datagram Format

➢ **Base header**

- **Flow label (3 byte):** The value of this field in combination with source address used to provide a special handling for a flow of data. The packets belongs to this flow have the same source, same destination, same priority and the same options. Flow label is important to support real time audio and video because it can speed up the processing of data by a router which handles the entire flow in the same way. The datagram that doesn't belong to any flow has the all flow label bits set to zero.



IPv6

❖ IPv6 Datagram Format

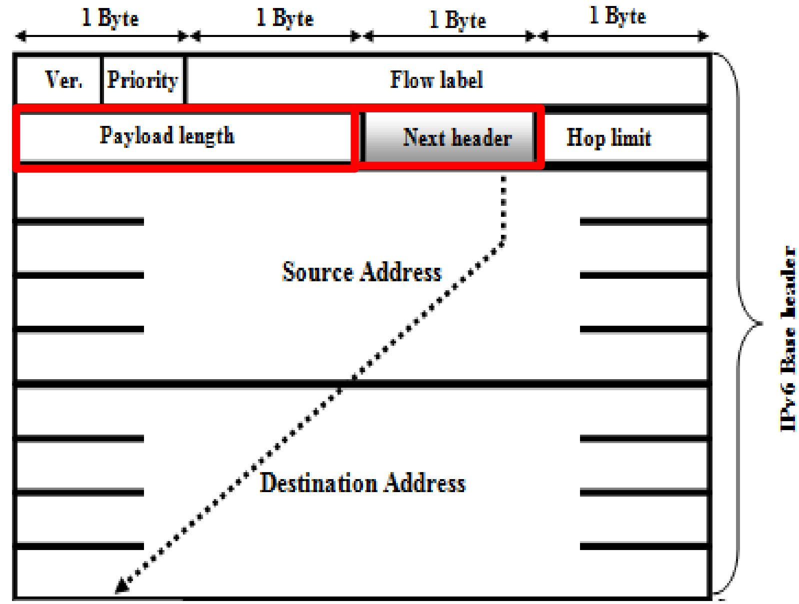
➢ Base header

- **Payload Length (2 bytes):**

  This field specifies the length of the datagram in bytes excluding the length of the base header field.

- **Next header (1 bytes):**

  This field defines the header that immediately follows the base header which is either one of the optional extension headers used by IPv6 or a higher layer protocol header such as TCP or UDP. The followings are some examples of decimal codes used in this field.



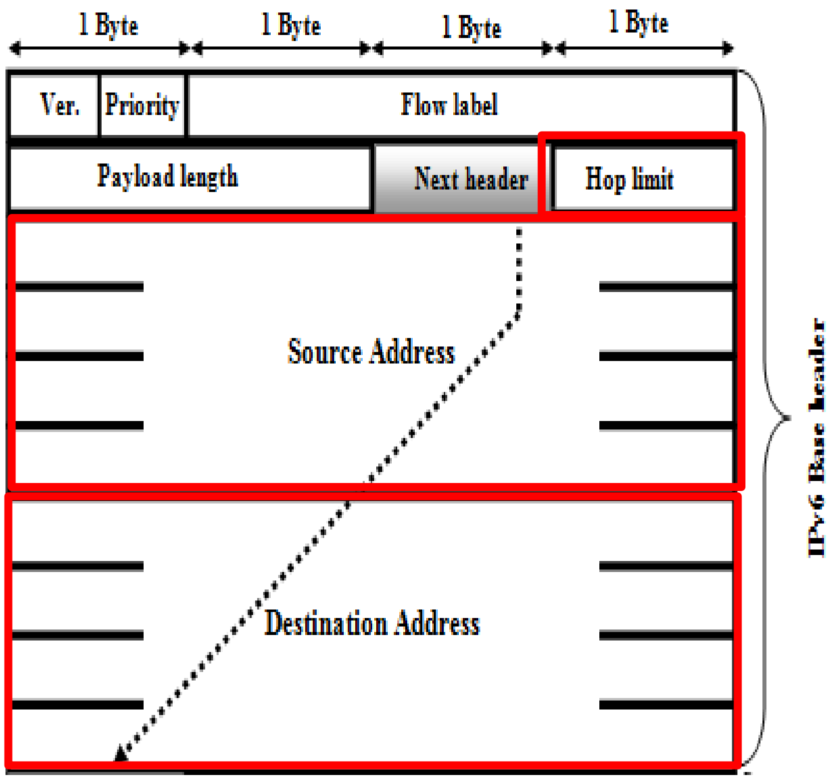
Code	Next header indication
06	TCP (higher layer protocol)
17	UDP (higher layer protocol)
43	Source Route (option)
44	Fragmentation (option)
59	Null header (No additional headers)

IPv6

IPv6 Datagram Format

Base header

- **Hop limit (1 byte):** This field serves the same purpose of TTL field in IPv4.
- **Source address (16 bytes):** this field identifies the Internet Protocol address of the original source of the datagram.
- **Destination address (16 bytes):** This field specifies the Internet Protocol address of the final destination.

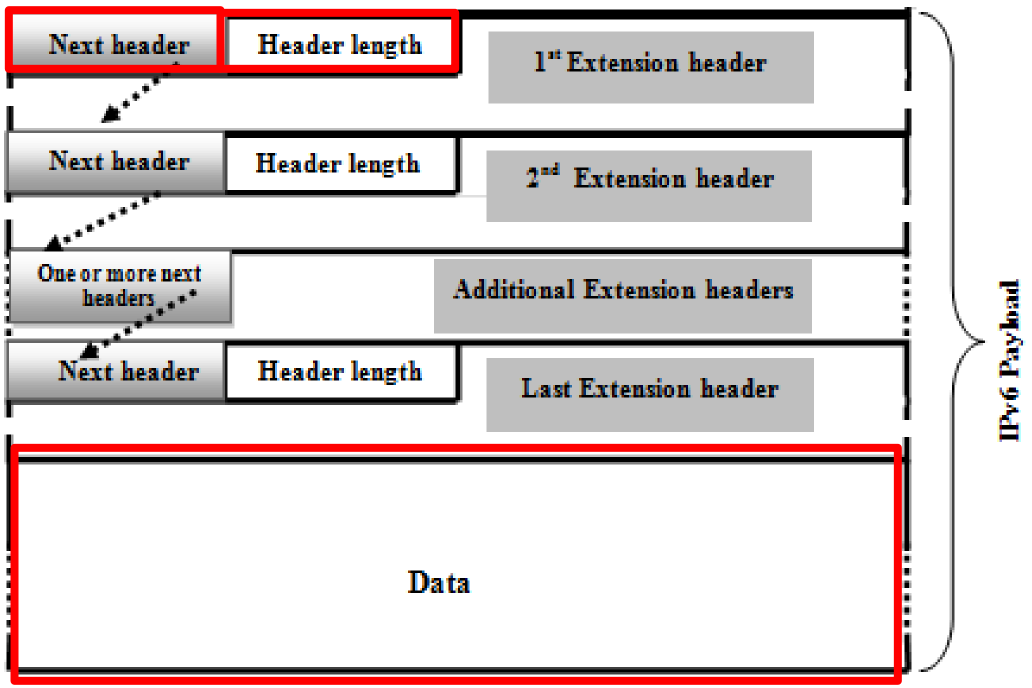


IPv6

❖ IPv6 Datagram Format

➢ Payload

- **Next header (1 byte):**
  this field is used as in the base header.
- **Header length (1 bytes):**
  this field is used to specify the length of this extension header in bytes.
- **Data:**
  This field contains the data generated by the upper layer protocol.



IPv6

IPv6 Datagram Options

- The base header of IPv6 can be followed by up to six extension headers.
- Each extension header can be the header of an upper layer protocol or an IPv6 option. Here are some of the options of IPv6:-
  - Source Routing: this header combines the concepts of strict source route and loose source route options of IPv4.
  - Fragmentation: the concept of fragmentation here is the same as in IPv4 except that IPv6 does fragmentation only on the original source using a technique known as "path MTU discovery" by which the source discovers the smallest MTU in the path and does fragmentation just once depending on this MTU value.
  - Authentication: This header has a dual purpose; it validates message sender as well as ensuring data integrity.
  - Encryption Security Payload ESP: this extension header provides confidentiality and guards against eavesdropping.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

IPv6 Vs. IPv4

- **Larger address space** in IPv6 (2^{128}) compared to (2^{32}) in IPv4.
- **Real time** and **security** are supported by IPv6 extension fields.
- "***Header length***" eliminated in IPv6 because header length is fixed to 40B.
- "***Priority***" and "***Flow label***" fields takes over the function of "***Type of service***" field in IPv4.
- "***Payload length***" field in IPv6 replaces IPv4 "***Total length***" field.
- "***Hop limit***" field in IPv6 does the same work of "***TTL***" field in IPv4.
- "***Next header***" field of IPv6 base header can perform the job of "***Protocol***" field of IPv4.
- Fields regarded to **fragmentation** in IPv4 are eliminated in IPv6 base header and included in an optional extension header.
- "***Checksum***" field is eliminated in IPv6 and left to the upper layer protocol.
- **Option fields** are implemented as extension headers in IPv6.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

IPv6 datagram field that is decremented by one by every router is

a- TTL
b- hop limit
c- protocol ID
d- priority

The binary code in the version field of IPv6 is

a- 6
b- 4
c- 110
d- 0110

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the following hexadecimal codes define IPv6 datagrams that must be delivered to TCP

a- 06
b- 60
c- 17
d- 71

IPv6 defines the source or destination address by

a- 128 B
b- 182 B
c- 16 B
d- non of the previous

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

Technical Engineering College / Al-Najaf
Communications Techniques Eng. Dpt.

Computer Networks-4th Class-2015/2016

Lec.#23: *IPv6* *Part II*

By: *Laith W. Abdullah*

Objectives

- Clarify how IPv6 addresses can be expressed
- Explain IPv6 address allocation
- Detail main IPv6 address types

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

- **IPv6 Addressing Format:-**
  - IPv6 address consists of 128 b (16 B).
  - To make addresses more readable, IPv6 addresses are specified in hexadecimal colon notation.
  - In this notation the address is divided into eight sections each of four hexadecimal characters.

Example:

FDEC : 0074 : 0000 : 0000: 0000 : B0FF : 0000 : FFF1

- **IPv6 Address Abbreviation:-**
  - Consecutive sections consisting of zeros can be abbreviated and replaced by double double-colons.
  - this type of abbreviation is allowed once per address.
  - Zeros at the most left digits of each section can be eliminated.

Example:

IPV6 address 000F : A0B0 : 0000 : 0000 : 0010: FFEE : 0000 : D1C0

Can be abbreviated to F : A0B0 : : FFEE : 0 : D1C0

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

- **IPv6 Addressing Format:-**
- **IPv6 Address Re-Expansion :-**
  - **Aligning the unabbreviated portions.**
  - **Inserting zeros then putting the missing double colons.**

Example:-

The abbreviated address 133 : 15 : : 10 : FDE1 : 0

Can be re-expanded to 0133: 0015 : 0000 : 0000 : 0000 : 0010 : FDE1 : 0000

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

❖ IPv6 Addresses Allocation:-

Each IPv6 address is divided into two parts.

- The first part is called the "type prefix". Type prefix is a variable length code that defines the purpose of the address.
- The second part of the address which as a result is also variable length code represents the remainder of the IPv6 address.

Prefix	Type
0000 0000	Reserved
0000 0001	Reserved
0000 001	NSAP
0000 010	IPX
0000 011	Reserved
0000 100	Reserved
0000 101	Reserved
0000 110	Reserved
0000 111	Reserved
0001	Reserved
001	Reserved
010	Provider-based unicast address
011	Reserved
100	Geographica unicast address
101	Reserved
110	Reserved
1110	Reserved
1111 0	Reserved
1111 10	Reserved
1111 110	Reserved
1111 1110 0	Reserved
1111 1110 10	Link-local address
1111 1110 11	Site-local address
1111 1111	Multicast address

IPv6

❖ IPv6 Address Types:

IPv6 addresses are generally divided into three types; these are:

- **Unicast.**
- **Anycast.**
- **Multicast**

➢ IPv6 Unicast Addresses:

- **Unicast address is unique as it defines a single interface.**
- **Unicast addresses can be used for a source or destination interfaces.**
- **There are several kinds of IPv6 unicast addresses; these include:**
  - **Provider-based**
  - **Special**
  - **Local addresses.**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

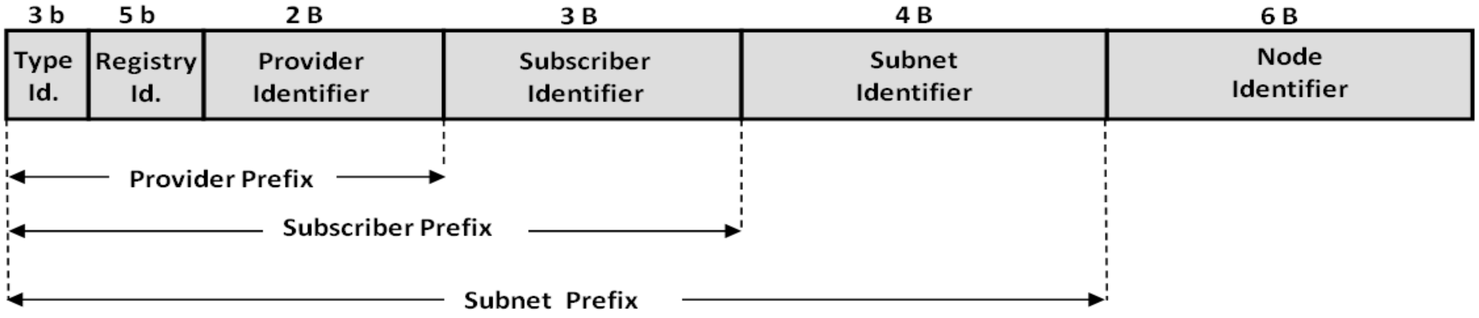
➢ IPv6 Unicast Addresses:

○ Provider-based addresses:

These addresses are used for global communications over the internet.

Provider based address composed of six fields; these are:

1. **Type Identifier:** **It identifies the address as provider-based address by the three bit code (010).**



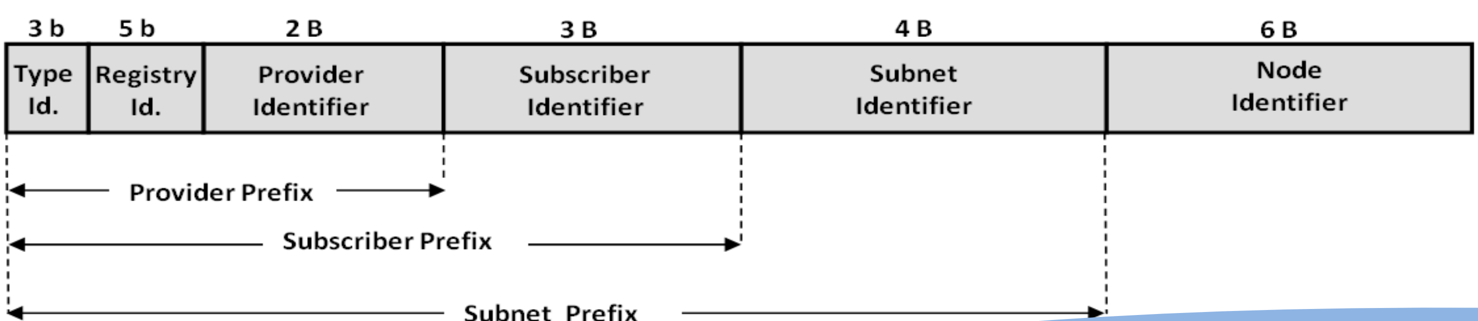
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

- **IPv6 Unicast Addresses:**

- **Provider-based addresses:**

2. **Registry Identifier:** **This field specifies the address of the internet agency that the address is registered with; examples of the currently available agencies are:**
   - **INTERNIC:** **The center of North America specified by the code (11000).**
   - **RIPNIC:** **The center of European registration specified by the code (01000).**
   - **APNIC:** **The center of Asia and Pacific countries specified by the code (10100).**



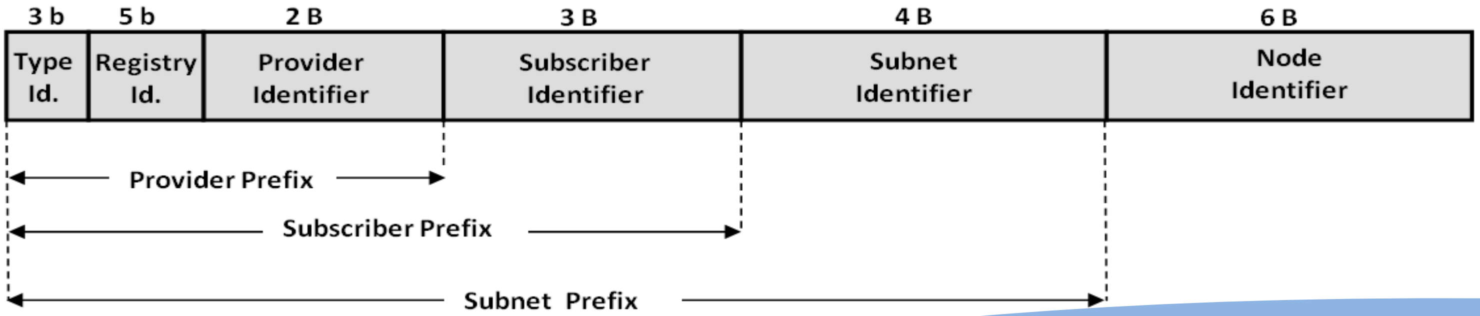
Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

- **IPv6 Unicast Addresses:**

- **Provider-based addresses:**

3. **Provider Identifier: this is usually a 16 bit code which represents the ID assigned by internet agency to each Internet Service Provider (ISP).**
4. **Subscriber Identifier: this field contains a code that is used by an ISP to uniquely identify each of its subscribers.**
5. **Subnet Identifier: it is used to define a subnetwork for a subscriber since the subscriber can have multiple subnets.**
6. **Node Identifier: node identifier field (also called interface identifier) specifies a single device interface within the subnet.**



IPv6

- **IPv6 Unicast Addresses:**
  - **Provider-based addresses:**
    - **IEEE EUI-64**

- **Node is usually identified by 64 bits of the 128 bits of the IPv6 address**
- **Usually the node identifier portion is calculated directly from the MAC address using the IEEE EUI-64**
- **48 bits of these 64 bits are derived from the MAC address of the node**
- **The rest 16 bits are replaced by the code FFFE which is inserted between the two halves of the Mac Address**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

- **IPv6 Unicast Addresses:**
  - **Provider-based addresses:**
    - **IEEE EUI-64**

Example:

What is the IPv6 address of the interface 02:17:95:AD:1A:10 if it is assigned manually the address 2001:8:85A3: : /64.

Answer:

- **From the address above the subnet prefix portion is (2001:8:85A3)**
- **while the rest of the address (the 64-bit that identifies the node) are calculated according to the IEEE EUI-64 and derived from the MAC address**
- **The two parts of the MAC address (the OUI and the vendor assigned) are separated by the code FFFE ,thus it become 0217:95FF:FEAD:1A10**
- **The whole add is 2001:8:85A3::217:95FF:FEAD:1A10**

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

➢ IPv6 Unicast Addresses:

○ Special addresses:

Special addresses are reserved addresses that starts by eight contiguous zeros (00000000). These include; loopback, unspecified, and IPv4 to IPv6 addresses.

i. Loopback address:

- In IPv6 there is only one loopback address.
- It is comprised of 127 0s followed by single 1 (represented in hexadecimal colon notation as " : : 1").
- Loopback address is used by the device to test its own TCP/IP software.
- The datagram sent to a loopback address never leaves the device that originates it whether the device is connected or not connected to a network.

8 b	120 b
Type & Registry	Provider, Subscriber, Subnet, & Node Identifiers
00000000	000000000000000000 ………………………………………………………….............. 00000001

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

➢ IPv6 Unicast Addresses:

○ Special addresses:

ii. Unspecified addresses:

- **It is comprised of 128 0s (represented as " : : ").**
- **It is used when a host sends an inquiry to learn its own IP address.**
- **The inquiry message contains the unspecified IPv6 address in the source address field.**

8 b	120 b
Type & Registry	Provider, Subscriber, Subnet, & Node Identifiers
00000000	000000000000000000 00000000

IPv6

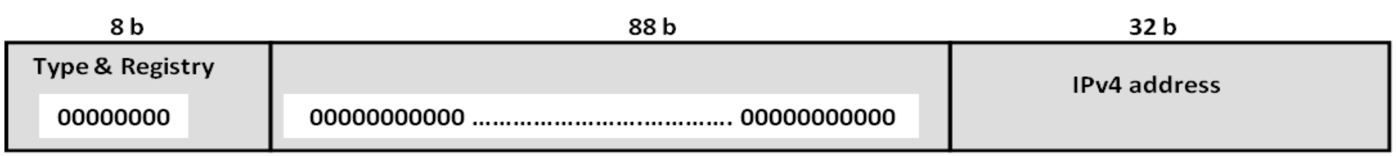
- **IPv6 Unicast Addresses:**
  - **Special addresses:**

iii. IPv4 over IPv6 addresses:

During the transition from IPv4 to IPv6, a device can embed its IPv4 address within an IPv6 address. There are two mechanisms to achieve that:

- **Compatible addresses:**

  This mechanism is used when an IPv6 device sends a datagram to another IPv6 device and the datagram must pass through one or more IPv4 networks.



IPv6

- **IPv6 Unicast Addresses:**
  - **Special addresses:**

iii. **IPv4 over IPv6 addresses:**

- **Mapped addresses:** **They are used when an IPv6 device sends a datagram to an IPv4 device and the datagram passes through one or more IPv6 networks.**

8 b	72 b	16 b	32 b
Type & Registry 00000000	00000000 00000000	1111....... 1111	IPv4 address

Example:

Find the compatible and mapped IPv6 addresses for the IPv4 address (4.12.18.14).

Answer:

- **The compatible IPv6 address is (0::040C:120E)**
- **The mapped IPv6 address is (0::FFFF:040C:120E)**

IPv6

- **IPv6 Unicast Addresses:**

- **Local addresses:**

  - **All IPV6 local addresses starts by the code (11111110) in the type and registry identifier fields.**
  - **A local address is an address with only a local routability scope.**
  - **IPv6 local addresses are divided into two types.**

i. **Link-local addresses:**
They are similar to IPv4 private addresses as they are used in isolated networks, so they do not have global impact. The format of IPv6 link-local address is shown bellow.

10 b	54 b	64 b
11111110 10	000000000000 0000000000000	Node address (16 b fill plus 48 b MAC address)

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

- **IPv6 Unicast Addresses:**

- **Local addresses:**

ii. **Site-local addresses:**

These addresses are used in isolated internetworks that are located in close proximity to each other. Site-local addresses also have no global impact. The format of IPv6 site-local address is illustrated below.

10 b	38 b	16 b	64 b
11111110 11	000000 ……….000000	Subnet address	Node address (16 b fill plus 48 b MAC address)

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

IPv6

- **IPv6 Anycast addresses:**

  They specify a group of devices whose addresses have the same prefix. The datagram that is sent with anycast address onto a physical network must be delivered only to one interface within the group (the physical network). This interface is generally the closest one to the source.

- **IPv6 Multicast addresses:**

  They specify a group of interfaces which do not necessarily share the same prefix (they are not on the same physical network). A datagram sent with a multicast address is delivered to all interfaces in the group.

Note: Anycast and multicast addresses are used only as destination addresses.

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com

???? Quiz ????

One of the followings is not an IPv6 address type

a- Multicast
b- Unicast
c- Anycast
d- Broadcast

IPv6 provider-based address usually defines the node ID by

a- 64 B
b- 64 b
c- 128 B
d- 32 b

???? Quiz ????

One of the followings specifies IEEE EUI-64

a- it is used to define MAC addresses
b- It is an Ethernet standard
c- it derives node ID portion of IPV6 from its MAC address
d- it converts the MAC address into IPv4 address

One of the followings is used by the host to test its TCP /IP software

a- MAC address
b- provider-based address
c- multicast address
d- loopback address

Lecturer: Laith Wajeeh, e-mail: laithwajeeh@ymail.com