University of ADRAR

Faculty of Science and Technology

Department of Electrical Engineering

Local Computer Networks

C O U R S E

H A N D O U T

Full Local Computer Networks Course

Level: **3rd YEAR LICENCE** (LMD) in **ELECTRONIC**

Semester: 5th semester (**S5**)

Dr. KADDI Mohammed

Associate Professor

University of ADRAR - ALGERIA

Foreword

This handout, a crucial resource, is specifically designed for third-year LMD students in the Electronic field. It serves as a comprehensive course manual for the subject "Local Computer Networks", aiming to introduce the fundamental notions of local computer networks.

This handout is structured into five chapters as follows:

Chapter 1. Notions on data transmission.

Chapter 2. Local networks.

Chapter 3. Ethernet network.

Chapter 4. The TCP/IP protocol.

Chapter 5. Wireless local area networks (WIF).

Table of contents

Chapter 1. Notions on data transmission

Introduction: Signals

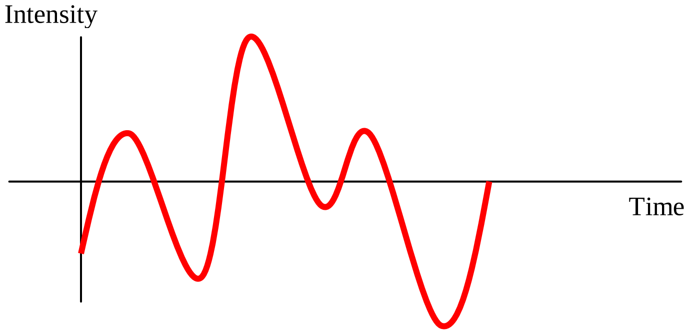
I- Analog and Digital:

1- Analog data and digital data:

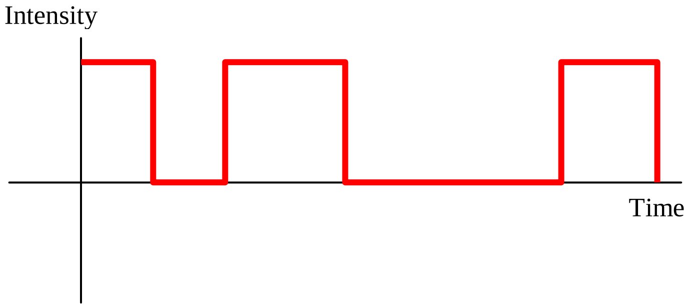
- Data can be analog or digital.
- Analog data are of continuous form.
- Example: Human voice, video clips, ...
- Digital data are of discontinuous form.
- Example: text files, memory bits, ...
- Both analog and digital data can be converted to signals to be transmitted [1] [2].

2- Analog signal and digital signal:

- Signals are the conversion of data when transmitted through a transmission medium.
- Signals can be either digital or analog.
- Analog signals have (theoretically) infinite levels of intensity over a period of time.



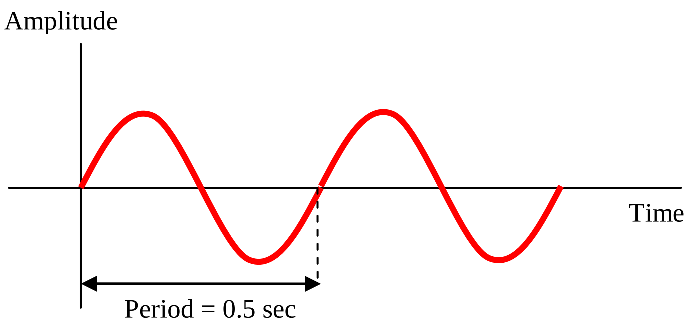
- Digital signals have limited number of defined values, as simple as 0 and 1 [2][3].



II- Analog Signals [4][5]:

1- Sine Wave:

- Analog signals can be simple or composite.
- Sine waves are an example of simple signals: they cannot get decomposed to other signals; they are elementary.



- A sine wave is periodic; it repeats itself after each period of time. Others are aperiodic.
- A sine wave is mathematically described as: $s(t) = A\sin(2\pi ft + \phi)$

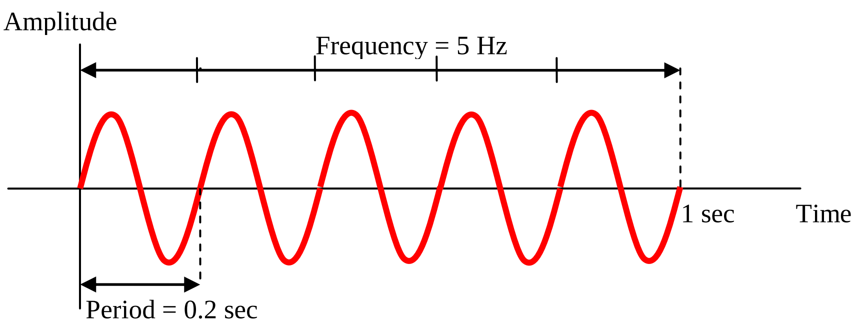
  where s is the amplitude at time t, A the peak amplitude, f the signal frequency, and ϕ the phase.

2- Peak:

- The highest amplitude a signal can take.
- For electric signals, the amplitude represents the voltage.

3- Period and frequency:

- The period is the amount of time that takes a signal to complete a cycle.
- The frequency is the number of cycles or periods that a signal takes in one second.
- $frequency = \dfrac{1}{period}$.



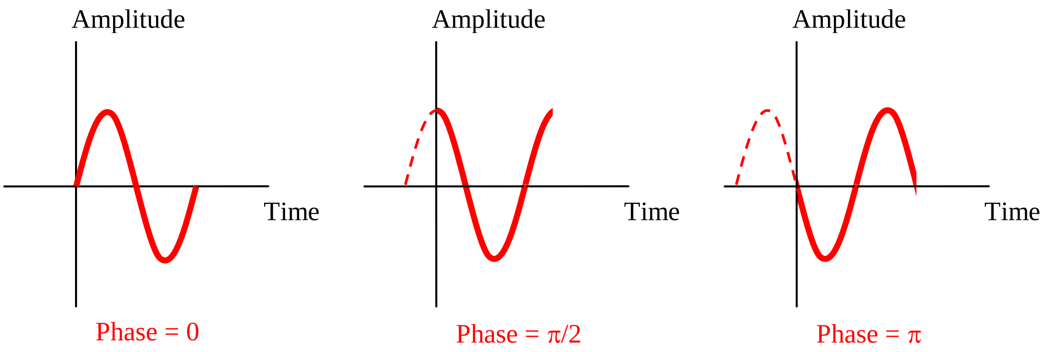
Unit	Equivalent	Unit	Equivalent
Seconds	1 s	hertz (Hz)	1 Hz

Milliseconds (ms)	10^{-3} s	kilohertz (KHz)	10^{3} Hz
Microseconds (μs)	10^{-6} s	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

- Frequency is rate of change with respect to time. The more changes the higher the frequency. The lesser changes the lower the frequency.
- Reception devices can distinguish different signals from the rate of changes in a second: the frequency.

4- Phase:

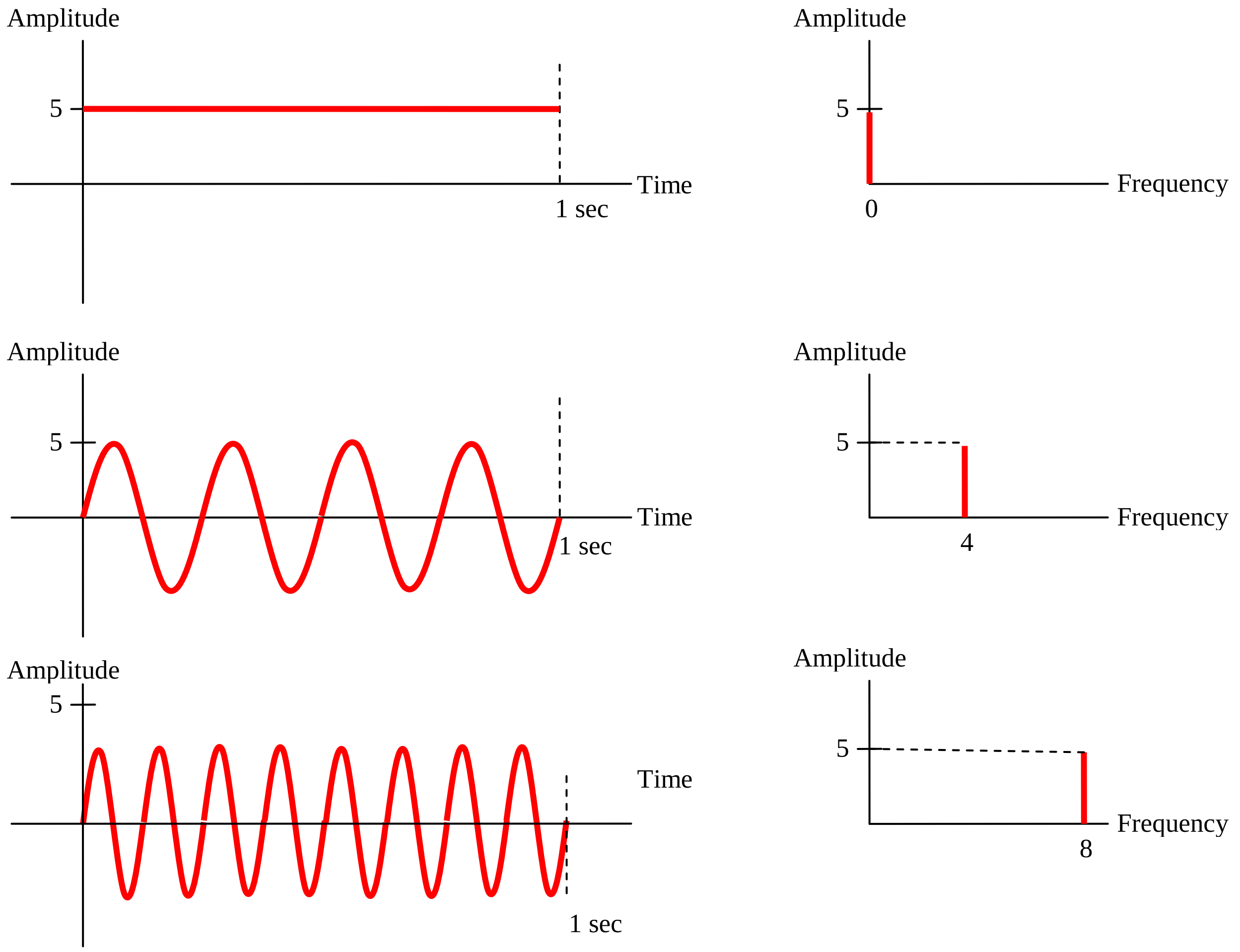
- The phase describes the position of the waveform relative to time zero.



5- Time domain and Frequency domain:

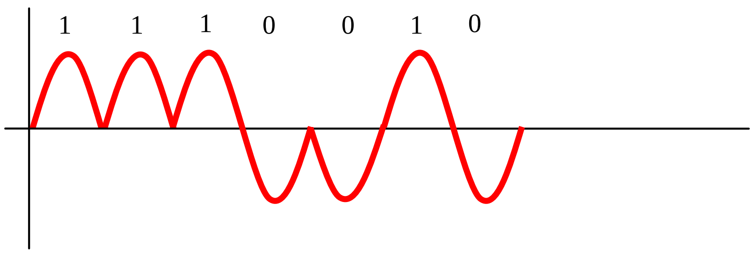
- Time domain is the signal representation through the relation between amplitude and time.
- Frequency domain is the signal representation through the relation between amplitude and frequency.
- An analog signal is best represented in frequency domain.

Time Domain | **Frequency Domain**

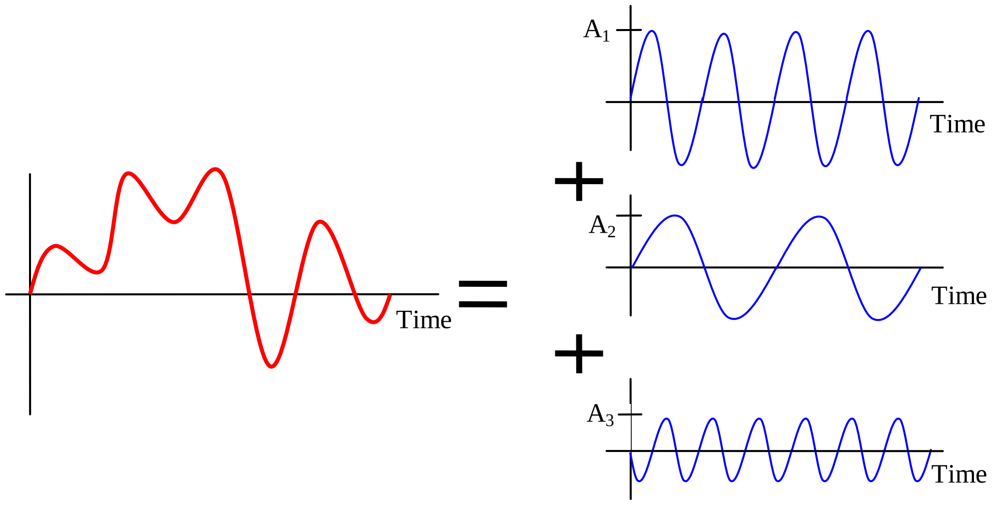


6- Composite signals:

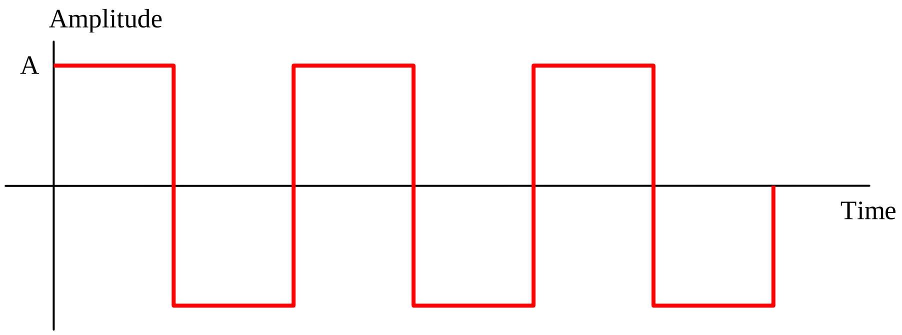
- A simple sine wave signal cannot transmit any information we need to send. For instance, if we use high amplitude to encode 1 and low amplitude to encode 0, then the only info we can send is a series of 1's and 0's : 101010101010.
- On the other hand, other signals (composite signals) can easily transmit any kind of encoded information:



- Based on Fourier analysis, any composite signal can be decomposed into the sum of several sine waves: $s(t) = A_1\sin(2\pi f_1 t + \phi_1) + A_2\sin(2\pi f_2 t + \phi_2) + \ldots$



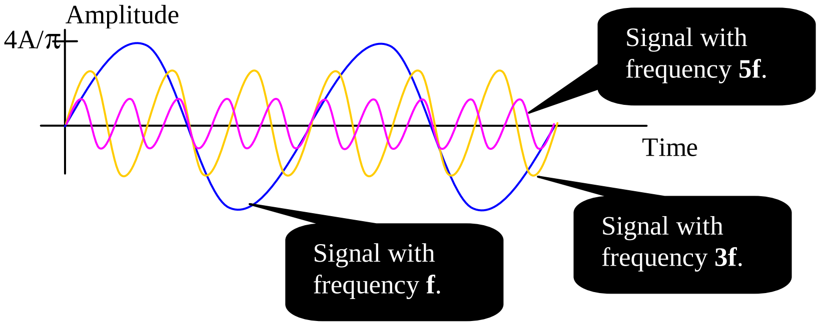
- Since most information we transmit is of digital form, or encoded digitally, let's see the example of a square wave signal:



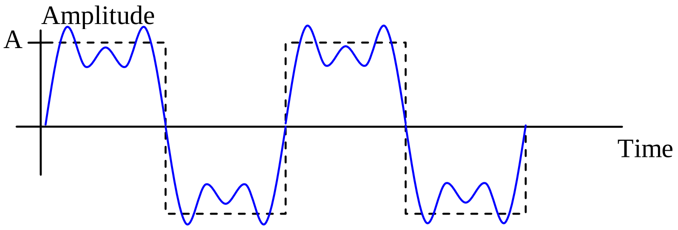
- Using Fourier analysis, we can prove that the above signal is of the form:

  $s(t) = \dfrac{4A}{\pi}\sin 2\pi ft + \dfrac{4A}{3\pi}\sin 2\pi(3f)t + \dfrac{4A}{5\pi}\sin 2\pi(5f)t + \ldots$

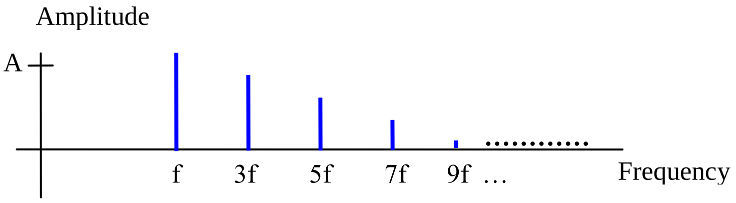
- The square wave s(t) is formed of a series of sine waves with frequencies f, 3f, 5f, … and amplitudes $4A/\pi$, $4A/3\pi$, $4A/5\pi$.
- The term with frequency f is considered as the fundamental frequency.
- The term with frequency 3f is called the third harmonic.
- The term with frequency 5f is called the fifth harmonic, and so on.



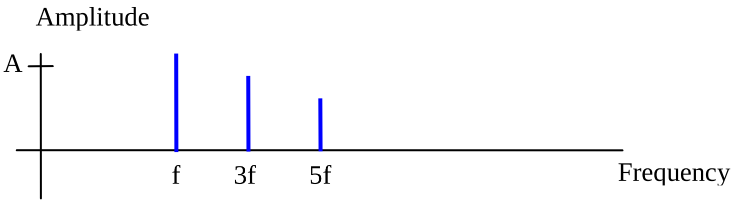
- Composition of the first 3 harmonics



- As we mentioned above, a signal can be best described using the frequency domain. The frequency spectrum of a signal is its description in the frequency domain:



Frequency spectrum of a square wave

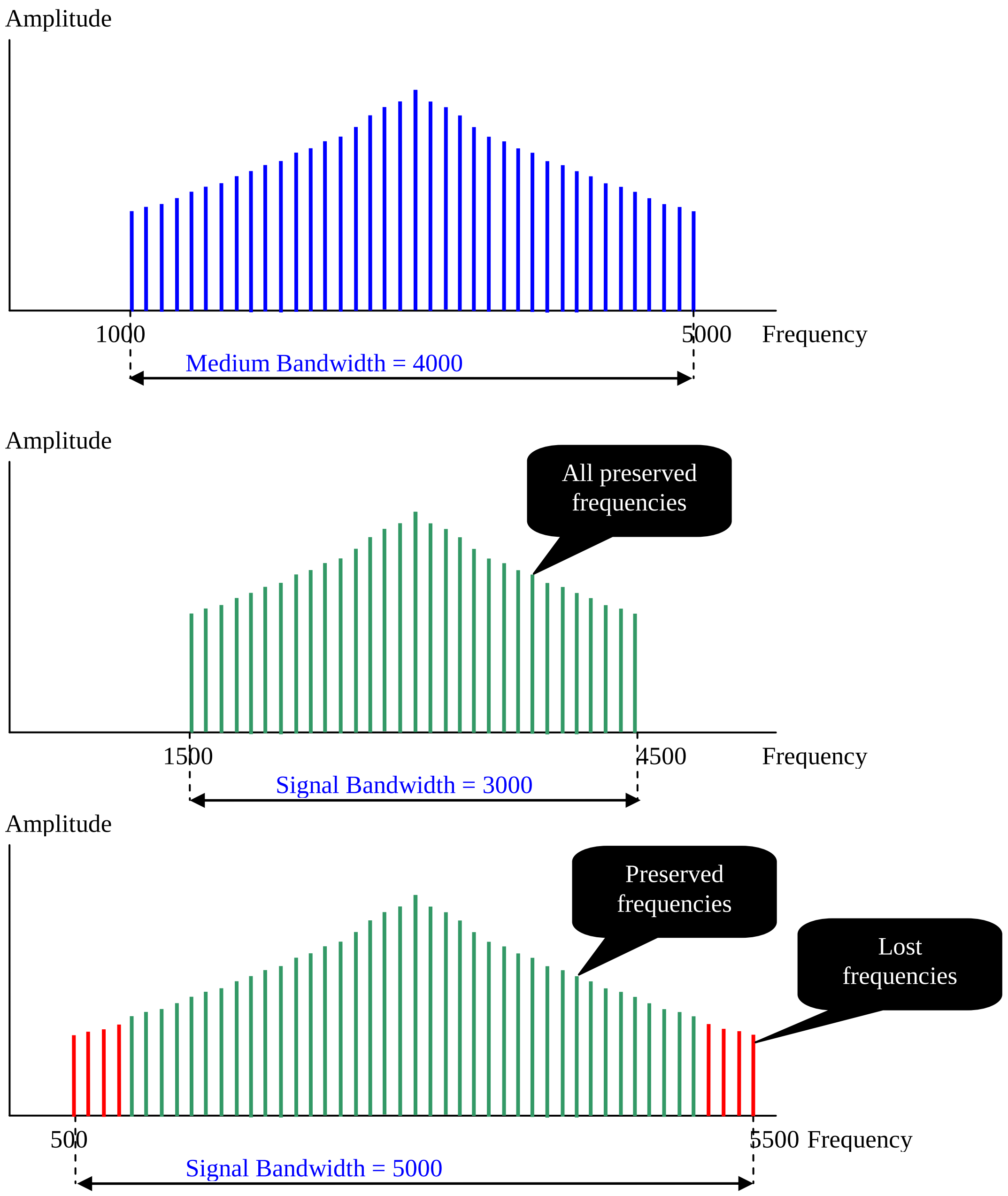


Frequency spectrum of an approximation with only three harmonics

7- Bandwidth:

- When a signal passes through a medium of transmission, usually it loses some of its quality.
- Each transmission medium has a low and a high frequency that allows passing through it.
- The composite signal frequencies that are not in the range of low-high frequency are filtered out (lost).

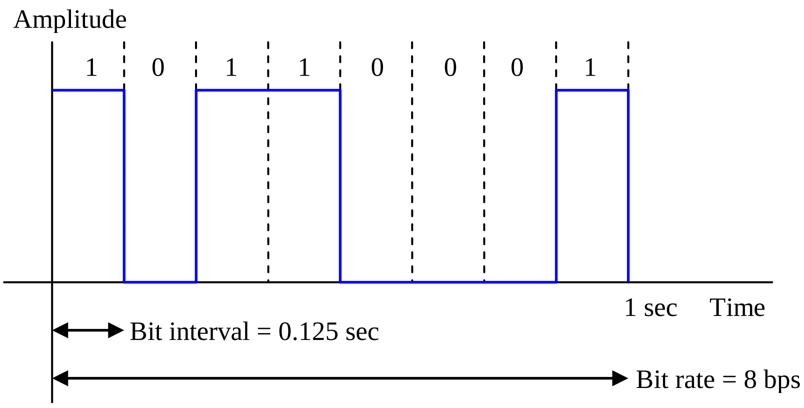
- The range of frequencies that can pass through a medium is called the bandwidth.
- Example: a coaxial cable allows frequencies between 1000 Hz and 5000 Hz to pass. So the bandwidth is 4000 Hz.
- Even though the bandwidth is related to a medium, you can also hear the term signal bandwidth; it refers to the medium bandwidth that let pass all that signal frequencies.
- The signal bandwidth is the difference between its highest and its lowest frequency.


Amplitude
1000
5000
Frequency
Medium Bandwidth = 4000
Amplitude
All preserved frequencies
1500
4500
Frequency
Signal Bandwidth = 3000
Amplitude
Preserved frequencies
Lost frequencies
500
5500
Frequency
Signal Bandwidth = 5000

II- Digital Signals [1] [3][4][5]:

1- Bit interval and bit rate:

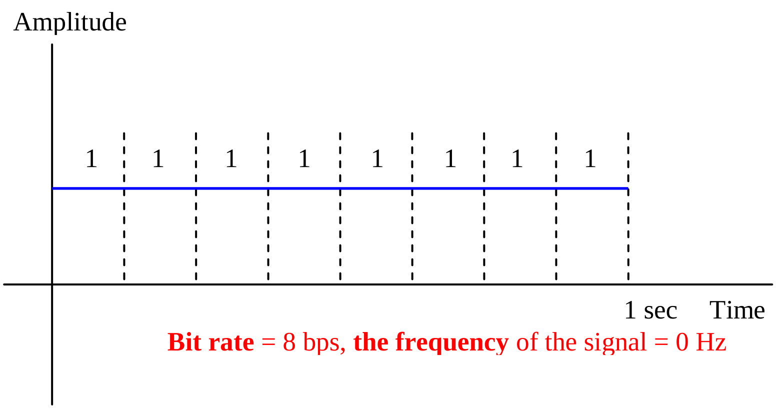
- Data can be represented using digital signal.
- Most digital are aperiodic. Thus, they don't have a specific frequency or a period.



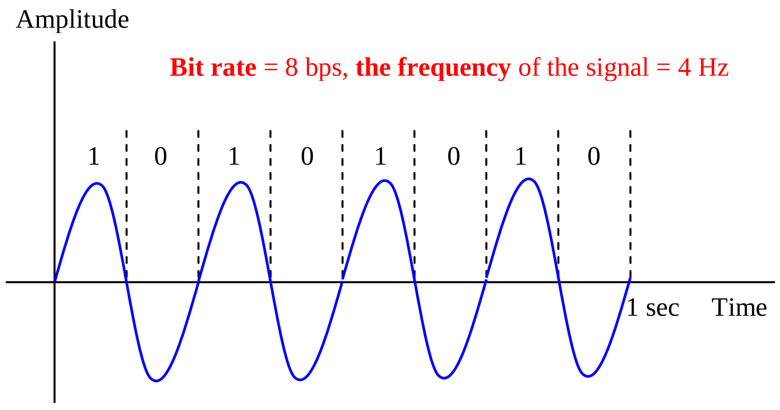
- Bit interval is the time required to send one single bit.
- Bit rate is the number of bits (intervals) sent per second.
- As we mentioned above, a digital signal is composed of infinite number of sine waves. Thus, it requires an infinite bandwidth to be fully reconstructed at the receiver site.

2- Required Bandwidth:

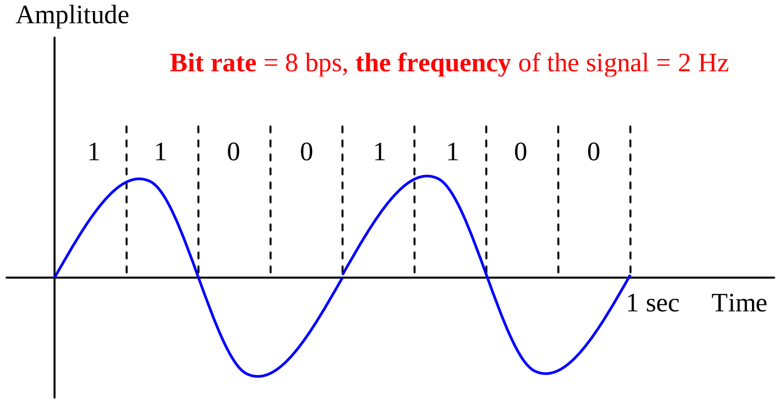
- The required bandwidth to transmit a digital signal is related to the desired bit rate.
- For instance, if we want a bit rate of 8bps, in the best case we can use a signal of frequency 0 to represent the set 11111111.



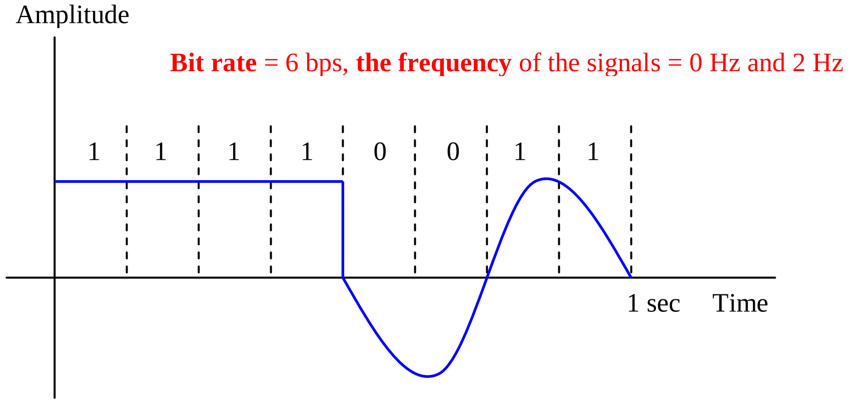
- In the worst case, we can use a signal of frequency 4 Hz to transmit the set 10101010:



- In a normal case, we can use a signal of frequency 2 Hz to transmit the set 11001100:



- In another normal case, we can use two signals of frequency 0Hz and 2Hz to transmit the set 11110011:



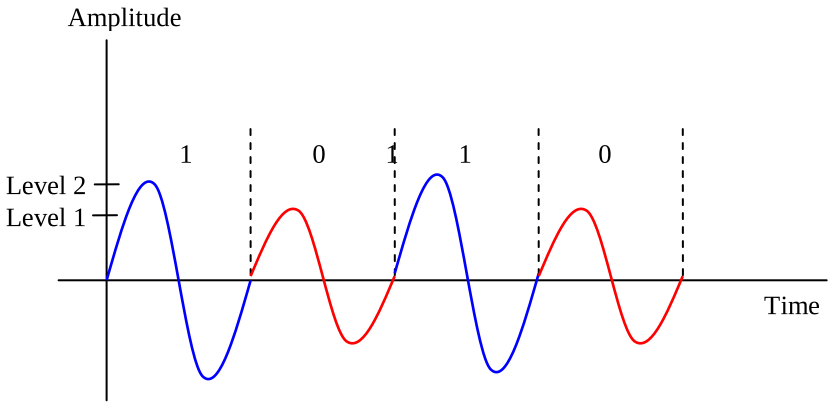
- Therefore, in order to handle all cases, we need a bandwidth of (4Hz – 0Hz) = 4Hz in order to transmit at bit rate of 8 bps.
- In general, using one harmonic, the required bandwidth B = n/2, where n is the bit rate.

- If we want to enhance the quality of the signal, we can use more harmonics: 1st and 3rd harmonic corresponds to a bandwidth B = 3n/2 Hz. Using the 1st, 3rd and 5th harmonics requires a bandwidth B = 5n/2 Hz. So, in general, B >= n/2.

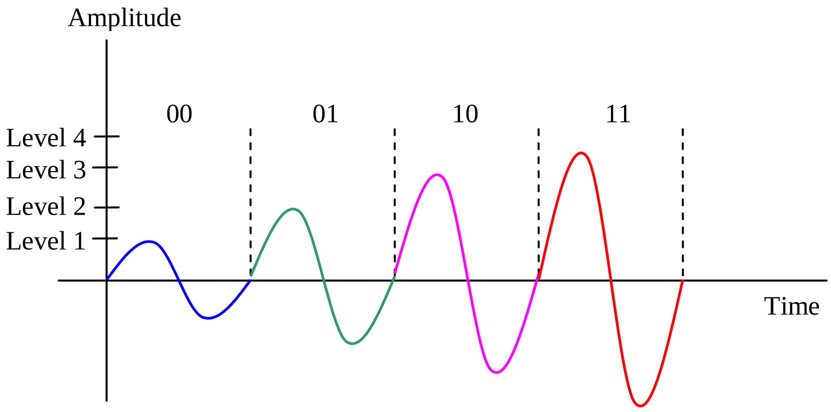
Bit Rate	**1st harmonic**	**1st and 3rd harmonics**	**1st, 3rd, and 5th harmonics**	**1st, 3rd, 5th, and 7th harmonics**
n = 1 Kbps	B = 500 Hz	B = 1.5 KHz	B = 2.5 KHz	B = 3.5 KHz
n = 10 Kbps	B = 5 KHz	B = 15 KHz	B = 25 KHz	B = 35 KHz
n = 100 Kbps	B = 50 KHz	B = 150 KHz	B = 250 KHz	B = 350 KHz

3- Data Rate Limits:

- When transmitting data over a channel, the data rate capacity depends on 3 factors:
  - The available bandwidth.
  - The levels of signals we can use.
  - The quality of the channel (degree of the noise)
- For each frequency in the bandwidth, we can encode one bit using 2 levels of a signal:



- For each frequency in the bandwidth, we can also encode two bits using 4 levels of a signal:



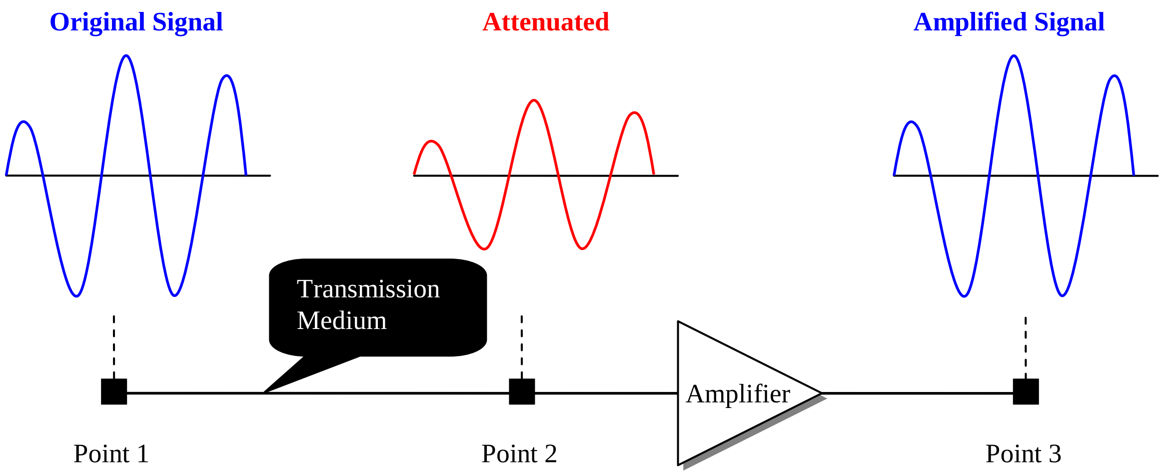
- For Noiseless channels, Nyquist defined a theoretical formula to calculate the data rate limit of the channel: Bit Rate = 2 x Bandwidth x Log_2 (signal levels).
- For instance, if we have a noiseless channel that have a bandwidth of 2 MHz, and uses 4 levels of transmission signals, than the (theoretical) bit rate = 2 x 2 MHz x $Log_2(4)$ = 8 Mbps.
- For Noisy channels, which is a realistic phenomenon, Shannon defined the channel capacity following the quality of the channel vis-à-vis the noise. He used the SNR, i.e., the signal-to-noise ratio, usually measured in dB.
- Capacity = Bandwidth x $\log_2(1 + SNR)$, regardless of how many levels of transmission signal we are using.
- For instance, if we have a noisy channel with SNR = 31 and a bandwidth of 2 MHz then the channel capacity = 2 MHz x $Log_2(1 + 31)$ = 10 Mbps.
- In practice, we use both Nyquist and Shannon formula as upper limits for the channel capacity.

III- Transmission Impairment [1][6]:

- When signals travel through transmission medium, they usually arrive in different shape than the originally generated signal.
- Three types of impairments are distinguished: Attenuation, Distortion, and Noise.

1- Attenuation:

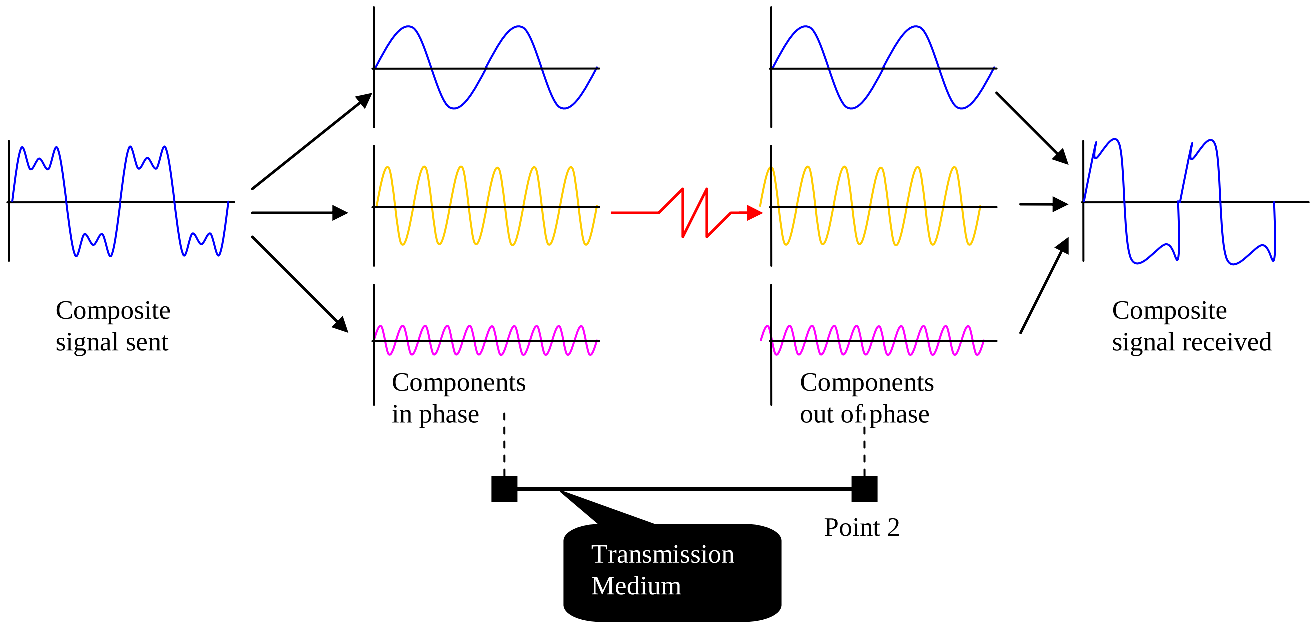
- It means loss of energy.
- The transmission medium is considered as a resistance to the transmitted signals. Some wires get warm or even hot due to signal energy that passes through.
- The loss of energy is usually regained through amplifiers. Amplifiers are basic components in repeaters, switches, bridges, routers, …



- Engineers used the term decibel to measure the relative strengths of two signals.
- If a signal had a power P_1 at the sender, and arrived attenuated or amplified with power P_2 at the receiver, then the decibel is: $dB = 10\log_{10}(P_2/P_1)$.
- If dB is negative then the signal has attenuated.
- If dB is positive then the signal has been amplified.
- Example: a signal travels through a transmission medium and loses half of its energy, compute the attenuation. $dB = 10\log_{10}(0.5P/P) = 10\log_{10}(0.5) = 10(-0.3) = -3$ dB.
- Example: a signal passes through an amplifier in order to gain 10 times. Compute the amplification. $dB = 10\log_{10}(10P/P) = 10\log_{10}(10) = 10(1) = 10$ dB.
- Property: the decibels of cascaded attenuations and amplifications can be added to get the global decibel. Attenuation (-3 dB) + Amplification (8 dB) + Attenuation (-4 dB) = Amplification (1 dB).

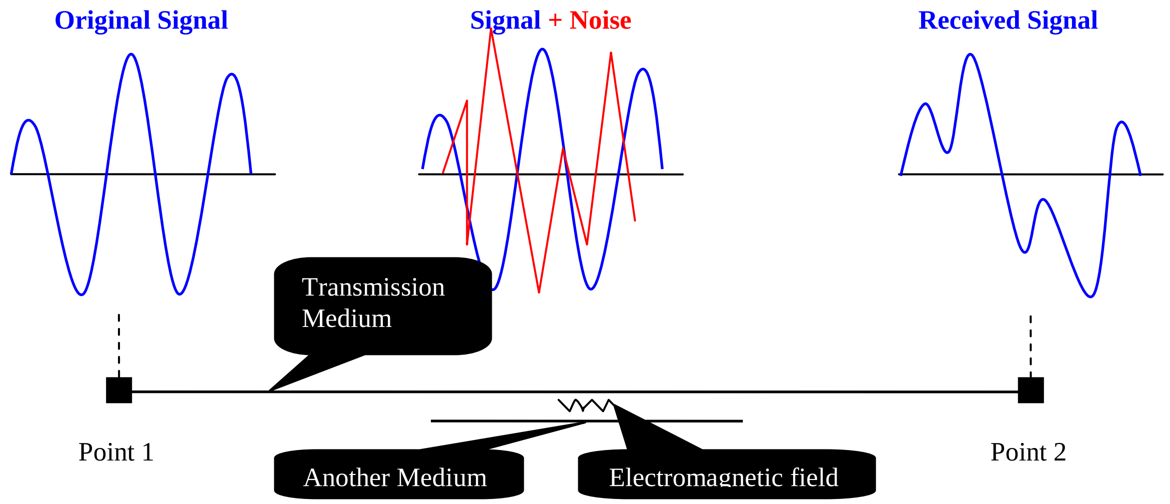
2- Distortion:

- When a composite signal is sent over a transmission medium, its components (simple signals) might arrive with different latencies. This will change totally the shape of the composite signal at the receiver:



3- Noise:

- The energy of the transmitted signal might get affected by the environment.
- Electromagnetic fields, nuclear fields, thermal noise and crosstalk may corrupt the signal.



- The noise signal is simply another signal that affects the original signal.
- The Signal-to-noise ratio (SNR) is the ratio between the signal and the noise:

  SNR = Signal Power / Noise Power , $SNR_{dB} = 10 \, Log_{10}(SNR)$, then $SNR = 10^{SNRdb/10}$.

III- Other Measurements [1][5]:

1- Throughput:

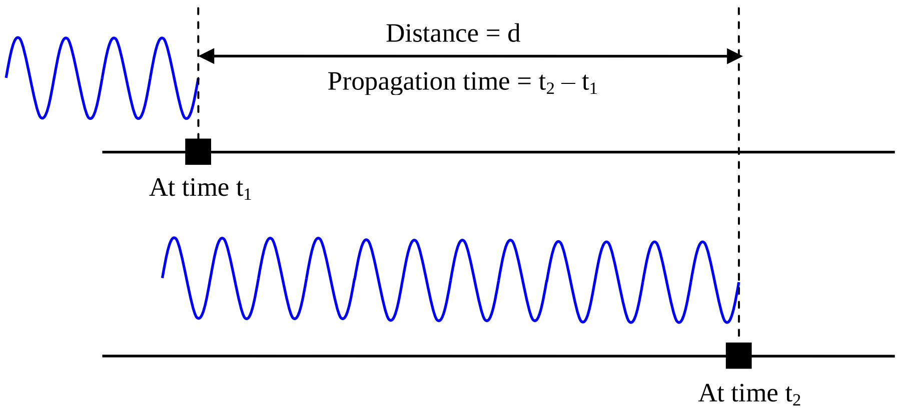
- In order to measure the data rate coming out of a device (router, firewall,…) or an algorithm (compression, encryption,…) we use the term throughput, which means how many bits are released in a second.

2- Propagation speed:

- Measures how fast a signal or bits are transmitted.
- It depends on the medium of transmission; in vacuum, light propagate faster than air, which is faster than in fiber optic.

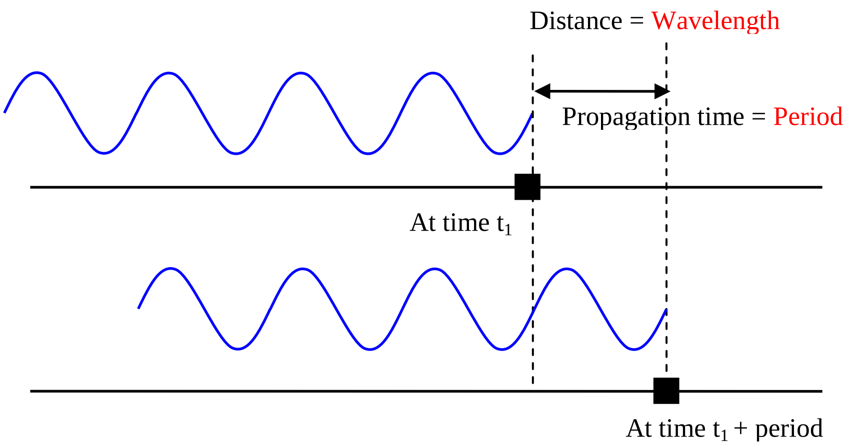
3- Propagation time:

- Measures how long a signal or bits are transmitted.
- If signal is transmitted for a distance, with certain propagation speed, then the propagation time is: propagation time = distance / propagation speed



4- Wavelength:

- Measures the distance that a signal travels in a time of one cycle (the period).

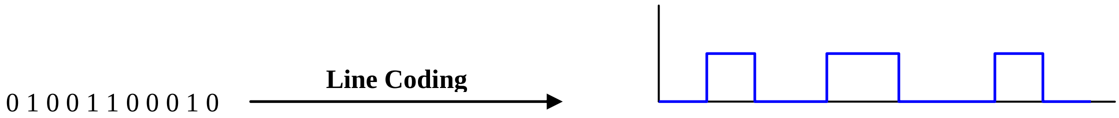


- The frequency is a characteristic of a signal, but the wavelength is a characteristic of signal that travels in a medium.
- Wavelength = Propagation Speed x Period = Propagation Speed/frequency.
- Example: The wavelength of red light (frequency = 4×10^{14} Hz) that travels in vacuum is: Wavelength = $3 \times 10^{8} / (4 \times 10^{14}) = 0.75 \times 10^{-6} = 0.75\ \mu$m.

Digital transmission systems

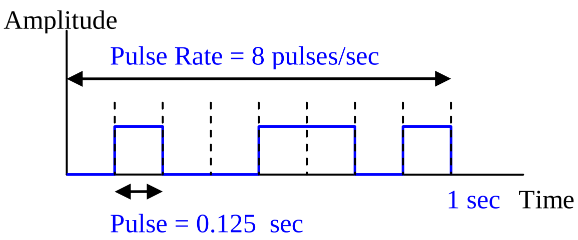
I- Line Coding:

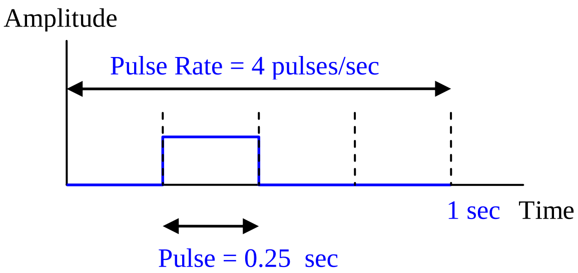
- Digital data are represented by sequences of bits.
- Digital data are converted to digital signals in order to be transmitted.
- Line coding is the process of converting bits into signals.



1- Pulse Rate and Bit Rate [3]:

- A pulse is the amount of time required to transmit information. In digital transmission, a pulse is the minimum time that a signal can maintain one level of a signal before changing it to another level.
- The pulse rate defines the number of pulses per second.

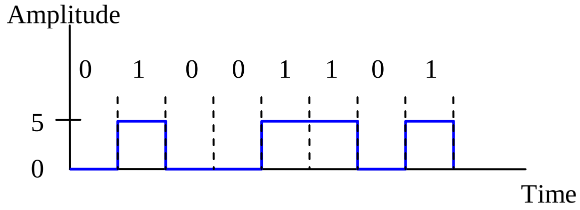




- The bit rate is related to the pulse rate and the number of signal level.
- Bite rate = Pulse Rate x Log_2 (Number of Levels).
- Example 1: A signal has two levels (0, 5) with pulse duration of 1 ms. What is the bit rate?

  Pulse rate = 1/(pulse duration) = 1000 pulse/sec.

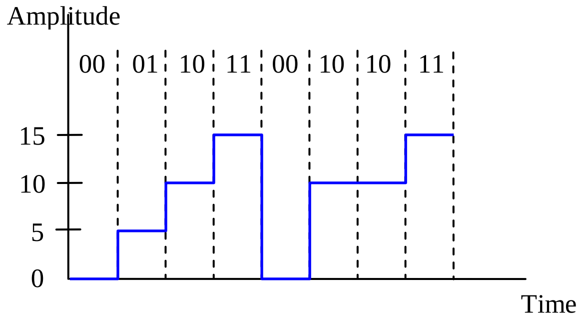
  Bit rate = Pulse rate x Log_2(2 levels) = 1000 bps.



- Example 2: A signal has four levels (0, 5, 10, 15) with pulse duration of 1 ms. What is the bit rate?

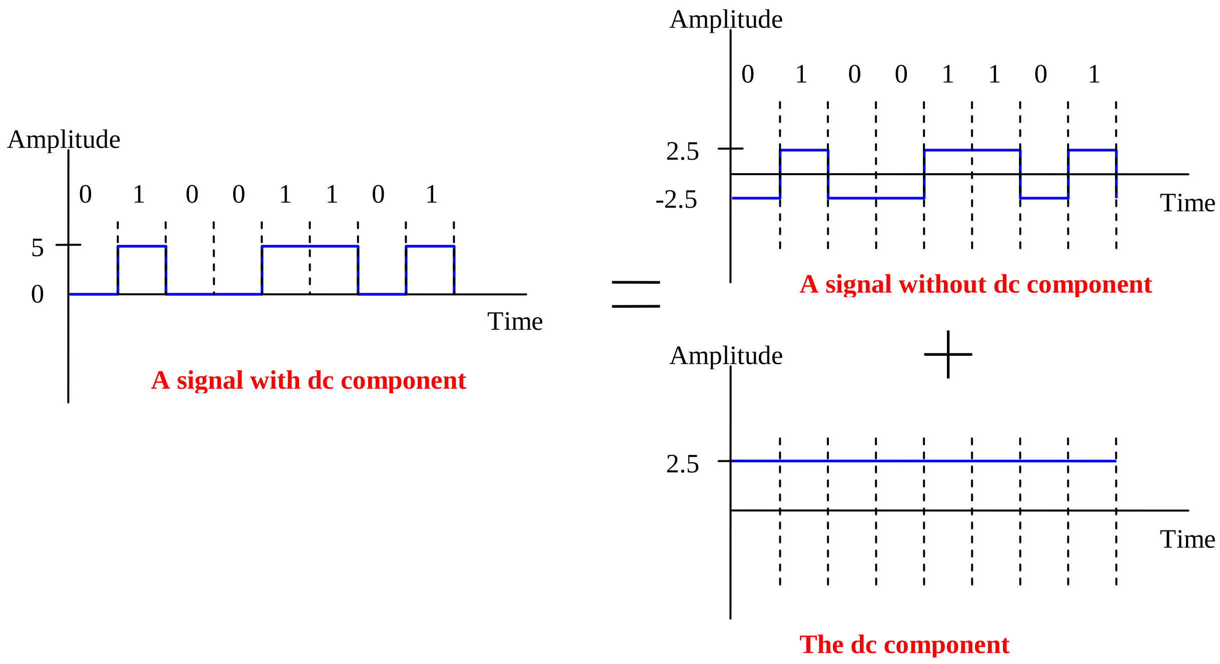
  Pulse rate = 1/(pulse duration) = 1000 pulse/sec.

  Bit rate = Pulse rate x Log_2(4 levels) = 2000 bps.

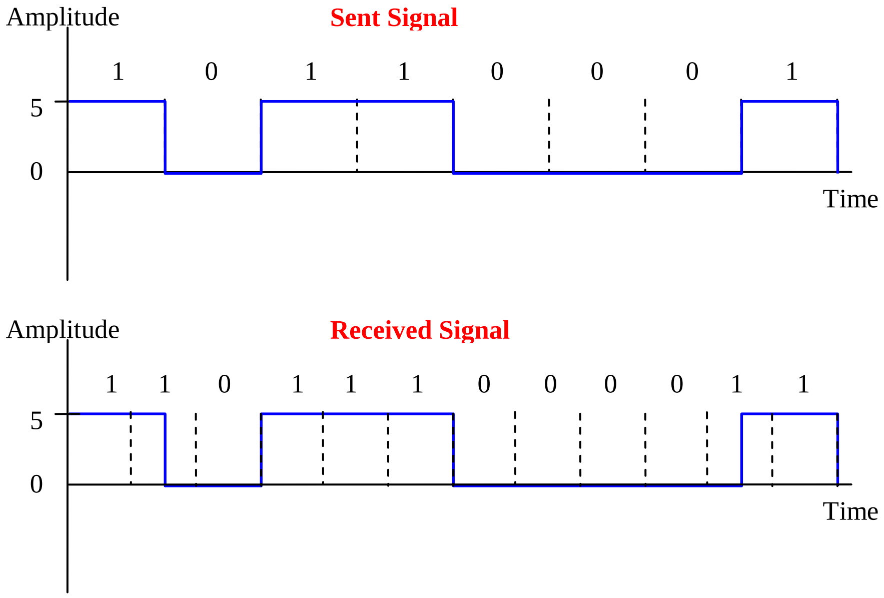


2- Coding that causes transmission problems [1][6]:

- The DC (direct-courant) component, the simple signal of frequency 0 is undesirable for two reasons.
- 1^{st} Reason: it accumulates energy in the transmission medium, which render useless after sometime.
- 2^{nd} Reason: it always requires a low-pass medium (with 0 frequency), which is not possible all the time.



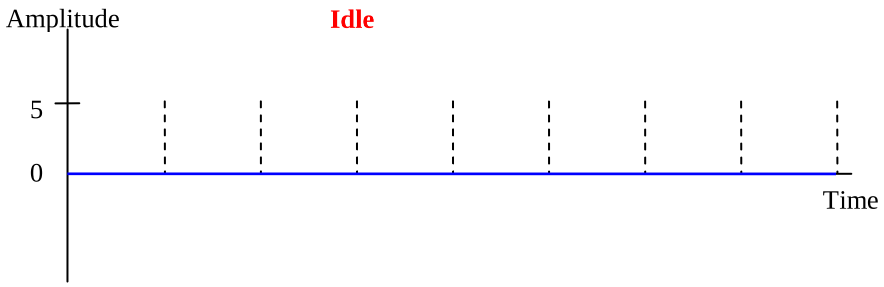
- Lack of self-synchronization: if the two clocks of the sender and the receiver are not in synch then the received signal might be interpreted differently than the sender.

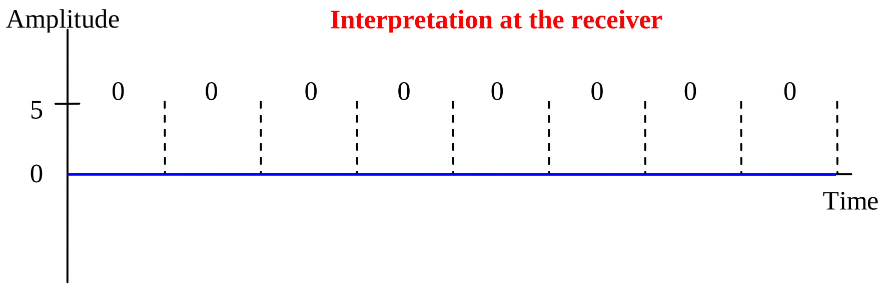


- Example: if the receiver clock is 0.1 % faster than the sender clock, how many extra bits per second does the receiver receive if the data rate is 1 Kbps?

  1000 bits sent $\rightarrow$ 1001 bits receives $\rightarrow$ 1 extra bit.

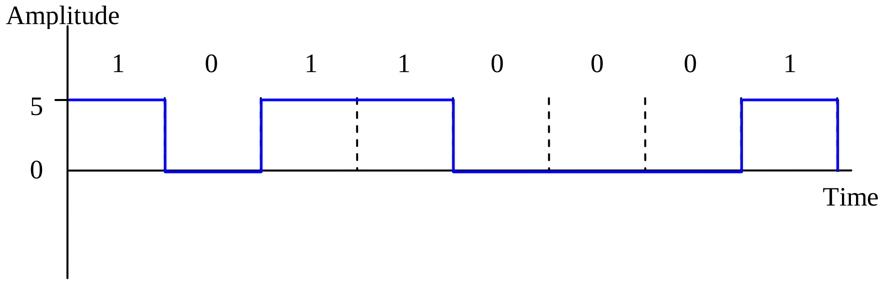
- Also, when the sender is down, the transmission medium is idle. The receiver might interpret it as a low signal, and encode information based on the used coding method:





3- Unipolar Coding [1][6]:

- Very simple and very primitive, so it is obsolete today.
- It uses one polarity to encode 1, and the null value to encode 0.
- Disadvantages: dc component, lack of synchronization.

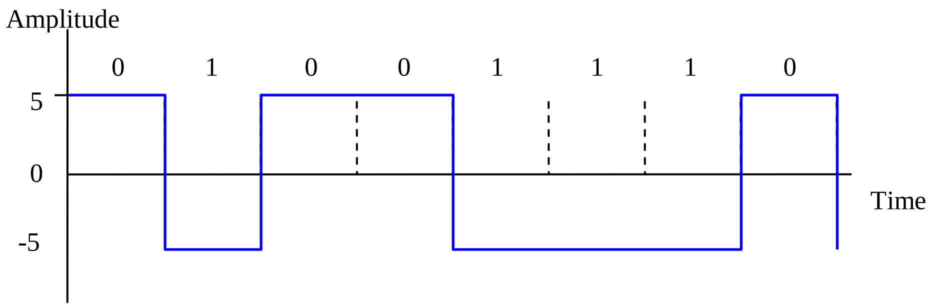


4- Polar Coding [1][7]:

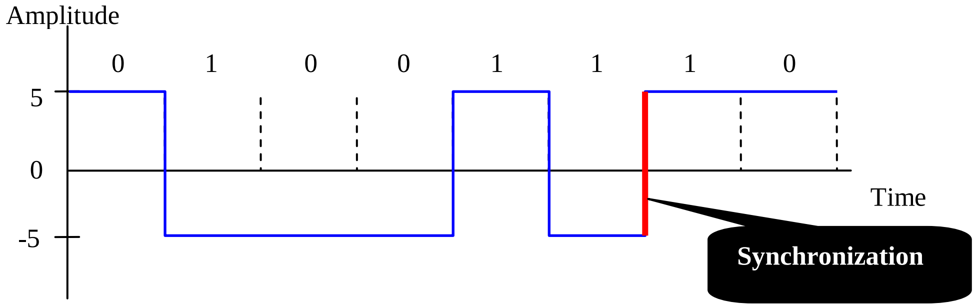
- Characterized by the use of two polar levels of voltages: positive and negative.
- There are several schemes of polar coding:

4-1- Non return to zero encoding (NRZ):

- The transmission signal is either positive or negative, not null (0).
- Two popular forms of NRZ: NRZL and NRZI.
- In NRZL (NRZ Level), the level of the signal depends on the state of the bit to be sent: positive for 0, negative for 1, or vice-versa.



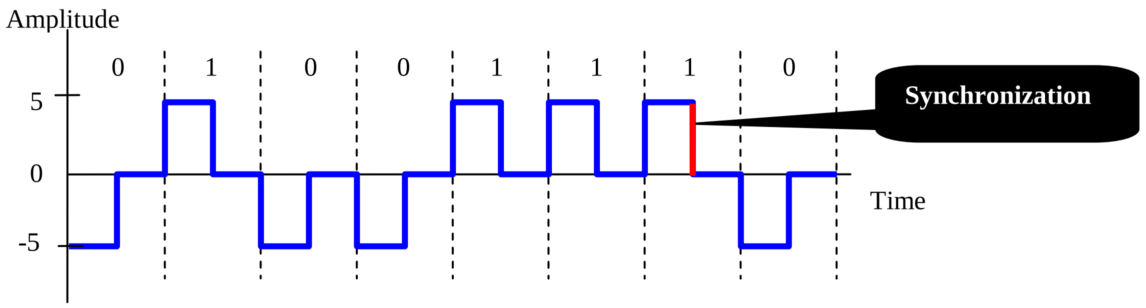
- Advantages: No dc component (in general).
- Disadvantages: Lack of synchronization.
- In NRZI (NRZ Invert), the level of the signal is inversed once a state of a bit is encountered (1); otherwise, it stays steady (0). So, 1 refers to a change in the signal level, 0 refers to no change.



- The receiver may adjust its internal clock whenever a change in the signal is received (1); thus self-synchronizing with the sender.
- The levels are meaningless to the receiver: only at the beginning of the pulse, the receiver looks at the signal for any possible changes to convert it to 1. Otherwise, it keeps converting to zeros following the internal clock.
- Advantages: No dc component (in general), synchronization (in general).
- Disadvantages: A long stream of 0s (not as likely) may cause a dc component and lack of synchronization.

4-2- Return to zero encoding (RZ):

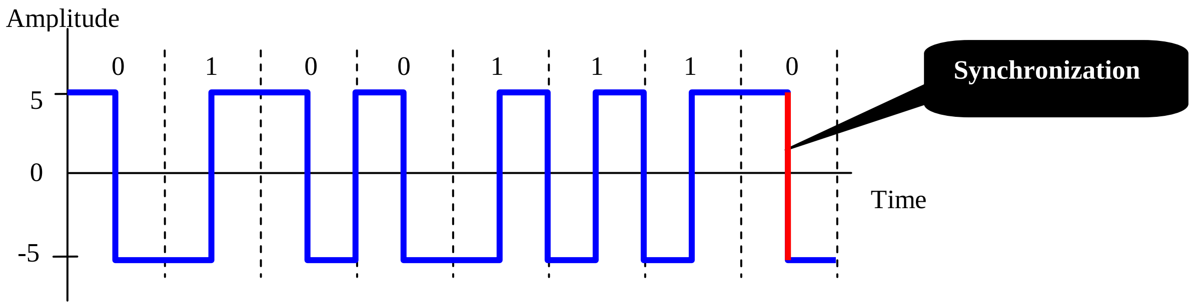
- The transmission signal is either positive or negative, but it returns to 0 for certain period.
- The signal always changes during bit duration: 0 is encoded by two changes: "zero to negative and then negative to zero"; 1 is otherwise.
- The receiver may adjust its internal clock in each bit duration; thus self-synchronizing with the sender.



- Advantages: No dc component (in general), full synchronization.
- Disadvantages: Requires more bandwidth (two changes per bit). Also, if the number of 0s and 1s are different, then it may cause a dc component.

4-3- Manchester encoding:

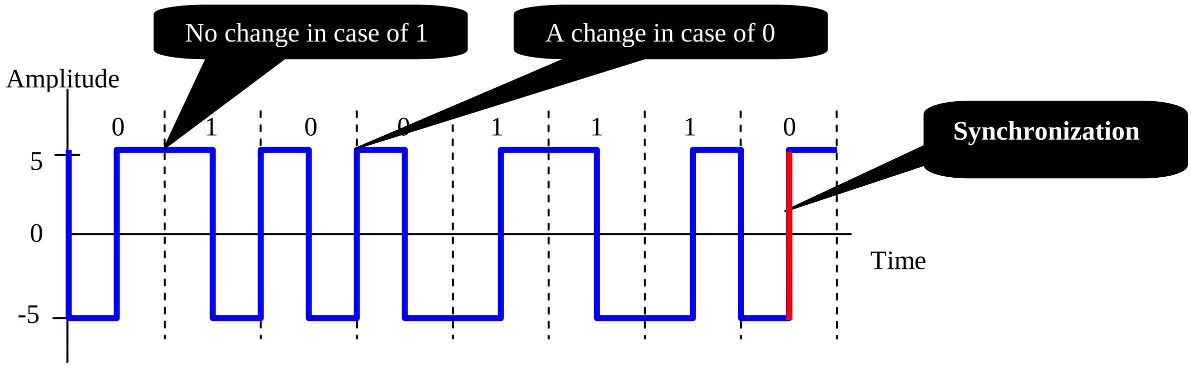
- Uses a signal inversion in the middle of the bit duration.
- An inversion from positive to negative encodes 0; otherwise, 1.



- Advantages: No dc component at all, full synchronization, requires lesser bandwidth than RZ (one change per bit for non consecutive streams of bits).
- Disadvantages: Requires more bandwidth than NRZ (two changes per bit for consecutive 1's or 0's).

4-4- Differential Manchester encoding:

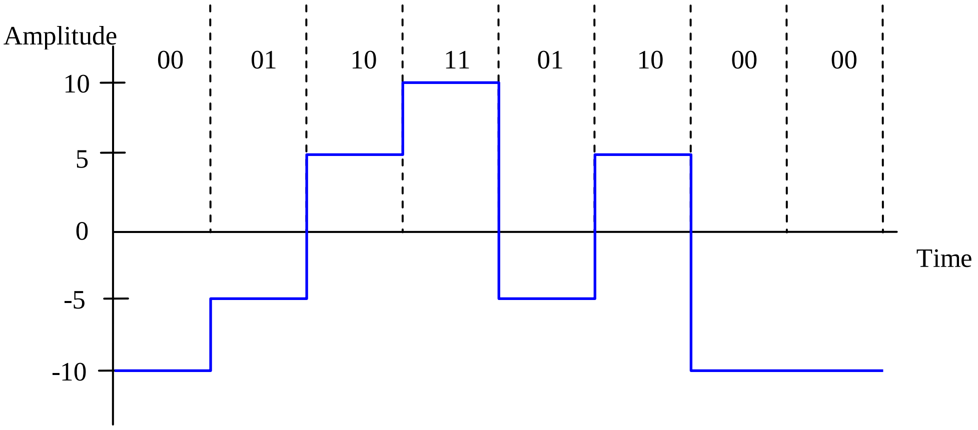
- Uses a signal inversion in the middle of the bit duration.
- An inversion at the beginning of the bit duration encodes 0; otherwise, 1.
- The levels are meaningless to the receiver: only at the beginning of the pulse, the receiver looks at the signal for any possible changes to convert it to 0. Otherwise, it keeps converting to zeros following the internal clock.



- Advantages & Disadvantages: Same as Manchester.
- When compared to Manchester, Differential Manchester cares only about the signal changes in the beginning of the bit interval, which is easier than testing the signal levels.
- On the other hand, with differential Manchester encoding we cannot use more levels to encode more bits.

4-5- Other schemes of encoding:

- 2B1Q (2 binary 1 quaternary) is similar to NRZL where 4 voltage levels are used to encodes 2 bits per pulse.



II- Block Coding [1][6][7]:

- Block coding handle a sequence of bits instead on separate ones.
- It passed through three steps: Division, Substitution, and Line Coding.

1- Division:

- First of all the sequence of bits to be sent is divided into groups of m bits. For instance, in 4B/5B encoding, the original stream of bits is divided into groups of 4 bits.

2- Substitution:

- Then, depending on the encoding scheme, a map table is used to substitute the m bits with n bits. For instance, in 4B/5B encoding, each group of 4 bits has its corresponding sequence of 5 bits following the 4B/5B map table.

3- Line coding:

- Last, the sequence of n bits are encoded using one of the previous line coding schemes (RZ, NRZ, …).

4- 4B/5B Block Coding:

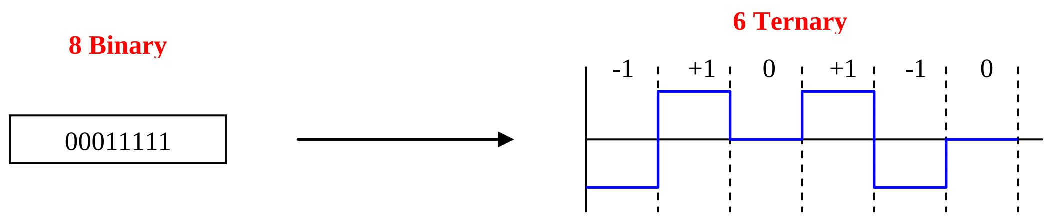
Data Sequence (4 bits)	Encoded Sequence (5 bits)	Data Sequence (4 bits) Used for Control	Encoded Sequence (5 bits)
0000	11110	Q (Quiet)	00000
0001	01001	I (Idle)	11111
0010	10100	H (Halt)	00100
0011	10101	J (start delimiter)	11000
0100	01010	K (start delimiter)	10001
0101	01011	T (end delimiter)	01101
0110	01110	S (Set)	11001
0111	01111	R (Reset)	00111
1000	10010		
1001	10011		
1010	10110		
1011	10111		
1100	11010		
1101	11011		
1110	11100		
1111	11101		

- With 4 bits, we can have 16 possible groups of 4 bits, whereas with 5 bits, we can generate 32 possible substituting groups of 5 bits. 4B/5B selects the best sequences of 5 bits to be sent over the transmission medium.
- When data are transmitted, 4B/5B guarantees that no more than 3 consecutive 0's are in sequence, and also no more than 8 consecutive 1's.
- 4B/5B gives the possibility of sending control symbol for better synchronization.

- Advantages: with simple line coding (NRZL), 4B/5B ensures synchronization, with alleviation of the dc component in some cases.
- Disadvantages: loss of 20% of the bit rate (bit rate < pulse rate) (an overhead of 1 bit in every 5 bits sent). Also, dividing and substitution time overhead.

4- 8B/6T Block Coding:

- In this block coding, each sequence of 8 bits ($2^8 = 256$ cases) is substituted by a sequence of 6 ternary code ($3^6 = 729$ cases). In the ternary code, three units are used (+1, 0, and -1 V).
- So not all the 729 codes will be used. 8B/6T selects the best sequences for data, and reserves other sequences for control.
- 8B/6T ensures, in most cases, that the substituting signal of 6 ternary codes or levels of voltage has no dc component: the signal leaves zero energy level in the transmission medium.



Data Sequence (8 bits)	Encoded Sequence (6 ternary signal)
00000000	−+00−+
00000001	0−+−+0
…	…
11111111	00+−0+

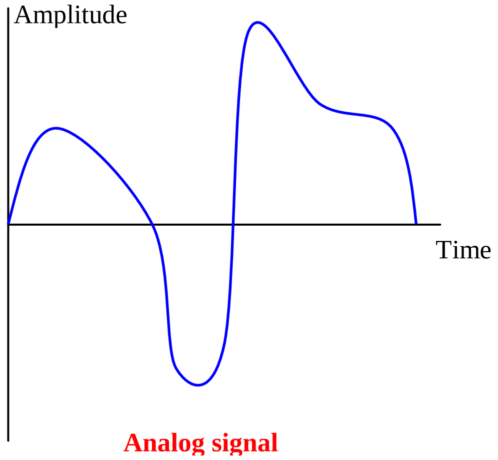
- Advantages: 8B/6T ensures synchronization, and better alleviation of the dc component in most cases. Also, no overhead in the bit rate (bit rate > pulse rate).
- Disadvantages: Use of 3 levels of voltages. Also, dividing and substitution time overhead.

III- Sampling [1][6][8]:

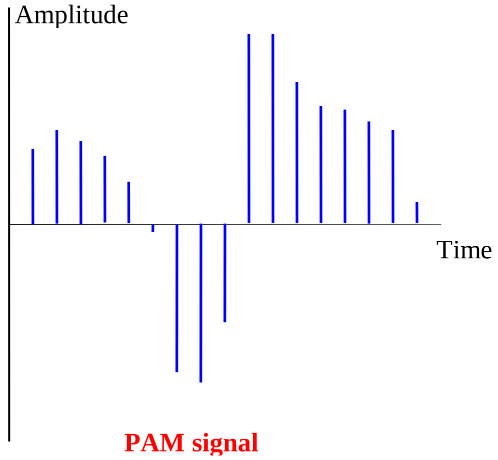
- If we want to convert analog data (voice, video, …) into digital signals, analog data are first changed into digital data through the process of sampling.
- Sampling a signal means measuring the amplitude of that signal at equal intervals.

1- PAM:

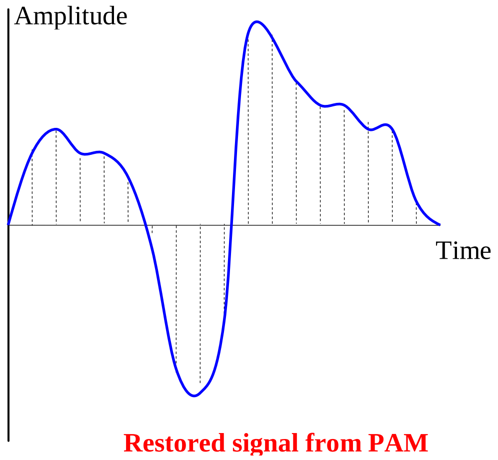
- PAM (pulse amplitude modulation) is a sampling technique based on sampling and briefly holding the signal.
- The result of PAM is a series of pulses or samples of amplitudes that looks like the original signal.



Analog signal



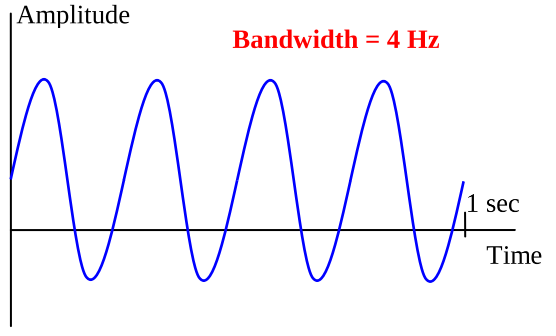
PAM signal



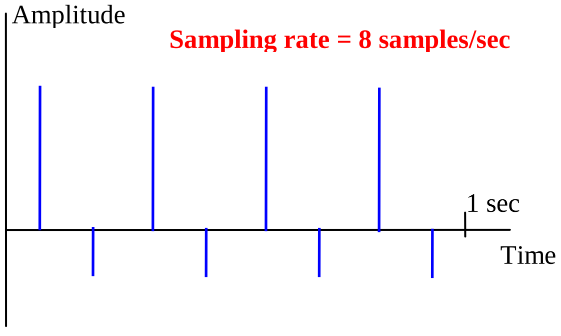
Restored signal from PAM

- There are two extremes in sampling: the more sampling the better quality of the restored signal. Yet, the lesser sampling, the lesser bandwidth needed to transmit the PAM signal. So what's the perfect sampling rate that makes it possible to restore the most significant characteristics of the original signal?
- Based on Nyquist theorem, we need to sample at a rate of twice the highest frequency of the signal in order to ensure a good quality of the restored signal. In case that a signal has components of frequency 0 then we need to sample a rate of twice the bandwidth.

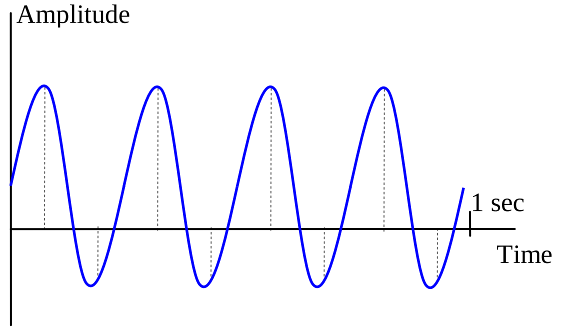
- Example: if we have a signal composed of a wave signal that has a frequency of 4 Hz and a dc signal (0 Hz), which needs a bandwidth of 4 – 0 = 4 Hz, then we need to sample that signal 8 times (4 x 2) in order to be able to restore back the original signal.



Original sine wave signal



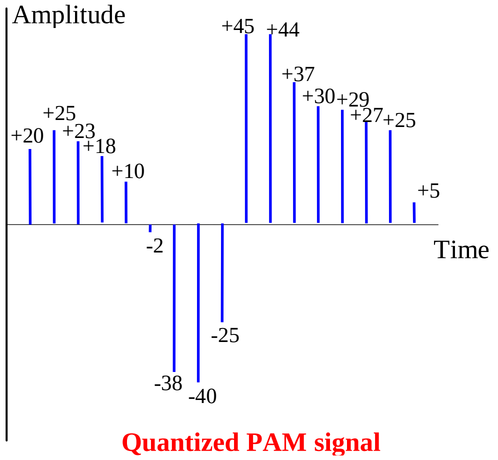
PAM signal



Restored signal

2- PCM:

- PCM (pulse code modulation) convert the pulses created by PAM into binary codes in order to be transmitted digitally.
- PCM is made of 4 processes: PAM, quantization, binary encoding, and line coding.
- PAM converts analog data into samples of pulse.
- Quantization is the process of associating numerical values to the PAM pulses.

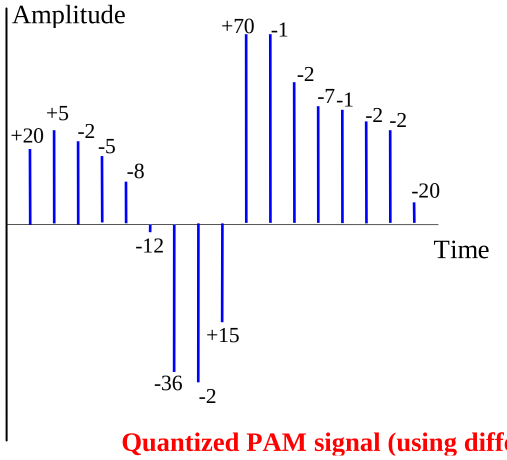


Quantized PAM signal

- Binary encoding the process of converting the quantization numerical values into binary codes: +20 : 00010100, -2: 10000010. The number of bits used per sample depends on the range of quantization numerical values. Then, the bit rate can be easily calculated as:
  Bit rate = (Sampling rate) x (bits per sample)
- Example: When sampling a human voice, the quantization process emerged values between (-128 and 127). If the human voice contains frequencies between 0 and 4000 Hz, what's the bit rate required to transmit digitally a human voice?
  Sampling rate = 4000 x 2 = 8000 samples/sec.
  256 values need 8 bits to be encoded.
  Then, the required bit rate is (8000 samples/sec) x 8 (bits/sample) = 64 Kbps.
- In line coding, one the above mentioned techniques (NRZ, RZ, Manchester, …) is used to convert binary code into digital signal.

3- Differential PCM:

- In Differential PCM, the quantization deals with the differences between samples values rather than the values themselves.

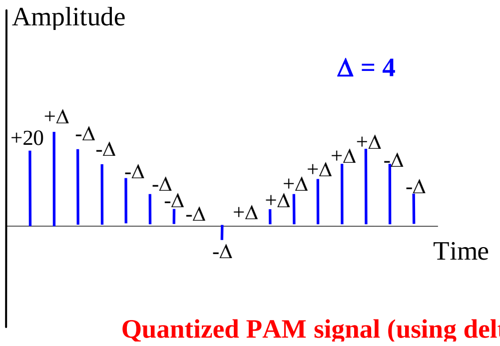


Quantized PAM signal (using differences)

- For instance, the range of differences between samples is between -4 and +3, then 3 bits only are needed to encode the quantized values.
- Advantages: Lesser bits per sample, if the differences between samples are considerably small.

4- Delta PCM:

- In Delta PCM, only one bit is used in encoding to mention higher pulse (1) or lower (0) than the previous one. In this technique, a fixed amplitude value (Δ) is either added (1) or subtracted (0) to get the value of the new sample:



Quantized PAM signal (using delta)

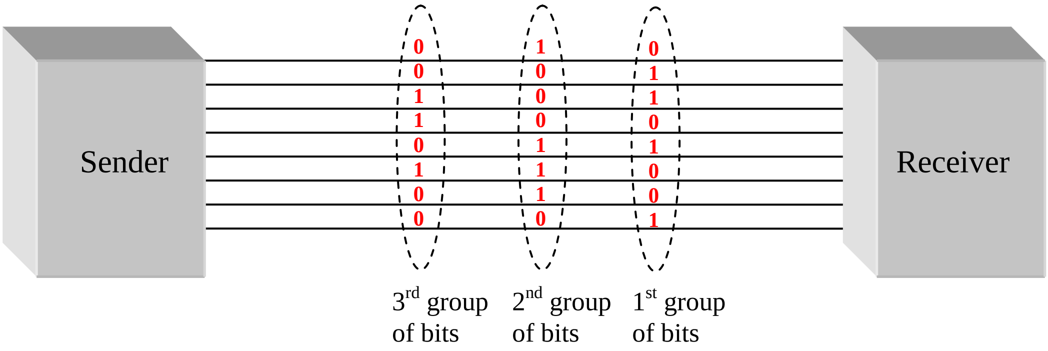
- Advantages: Only one bit per sample.
- Disadvantages: does not work for signals with sharp variations.

IV- Transmission Mode [6]:

- We recognize two types of transmission modes: Parallel and Serial.

1- Parallel transmission:

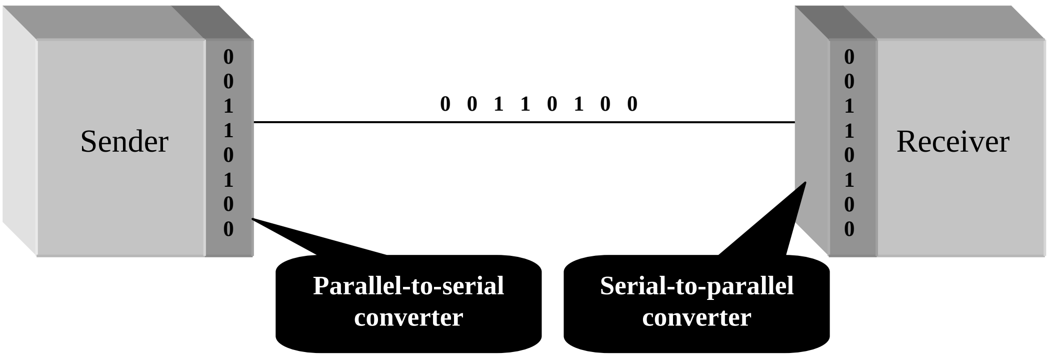
- Instead of transmitting bits sequentially, a group of n bits are sent simultaneously. Therefore, *n* links or wires are required for transmission.



- Advantages: Bit rate is enhanced n times.
- Disadvantages: Expensive. Therefore, parallel transmission is usually used in short distances.

2- Serial transmission:

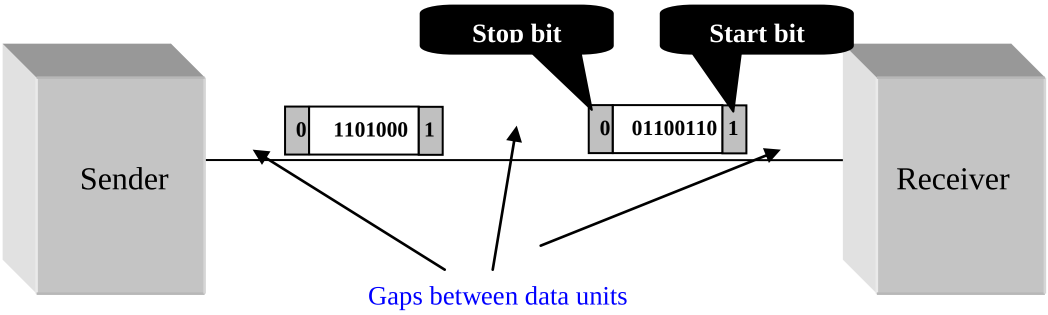
- In serial transmission, only one link is used for data communication.
- If data is originally packed in groups of bits, the sender needs to rearrange then in a sequence of bits in order to be sent over the serial link.
- The receiver collects the arrived bits and then regroups them in their original structure.



- Advantages: widely used (cheaper).
- Disadvantages: not as fast as parallel transmission.

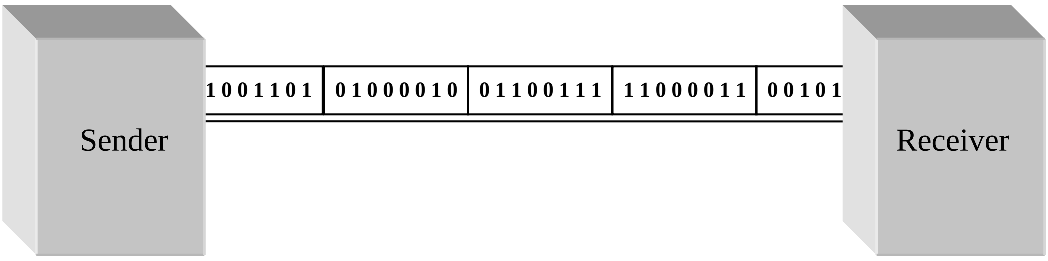
3- Asynchronous Serial transmission:

- It's a serial transmission, where bytes are sent asynchronously; the receiver has no idea about the next time the sender is sending data.
- When a byte is transmitted, at least two bits are added as a header (start bit) and a trailer (stop bit) in order to handle the byte synchronization between the sender and the receiver. So this mode is asynchronous outside the byte level, but synchronous inside the byte level.
- This mode is used in slow and asynchronous communication, like the keyboard where the user might type few words and stop for a while to think what to write next.



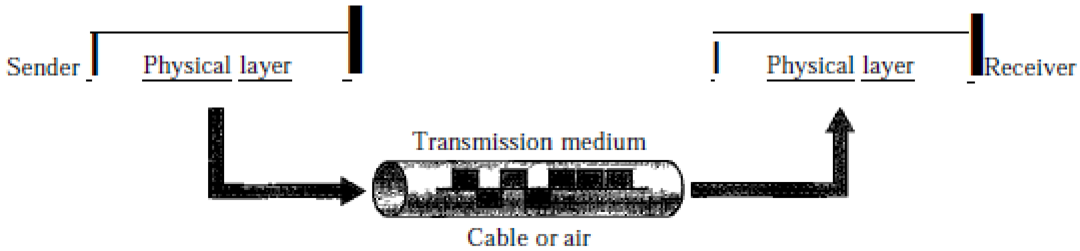
4- Synchronous Serial transmission:

- It's also a serial transmission, where a collection of bytes are sent together in a frame with no gaps in between.
- It is synchronous because the sender and the receiver are basically communicating all the time of transmission. This mode is used for faster transmissions, thus no header or trailers are added to bytes.
- The line is then filled-up with bits, and the bytes' divisions do not appear while in transmission.
- The receiver regroups the bit back into bytes and restores their original structure.
- In case the sender has nothing to send, then it sends the idle message (like 11111 in 4B/5B) instead of leaving gaps.



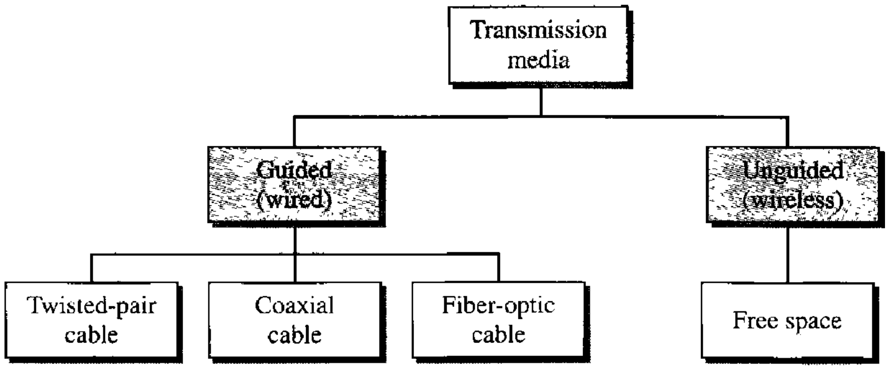
Transmission Media

- A **transmission medium** can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane [1].
- In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form [1][9].



I- Classes of transmission media [1][10] [11]:

- In telecommunications, transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

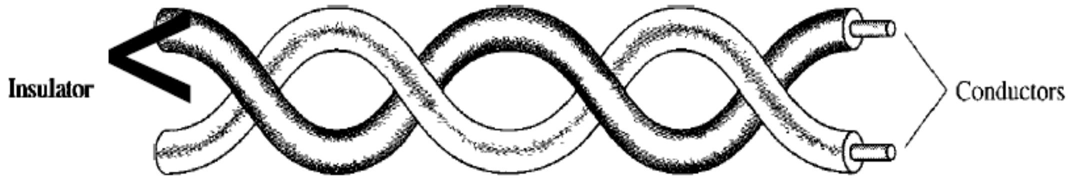


1- GUIDED MEDIA:

- Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.

- Optical fiber is a cable that accepts and transports signals in the form of light.

1.1- Twisted-Pair Cable:

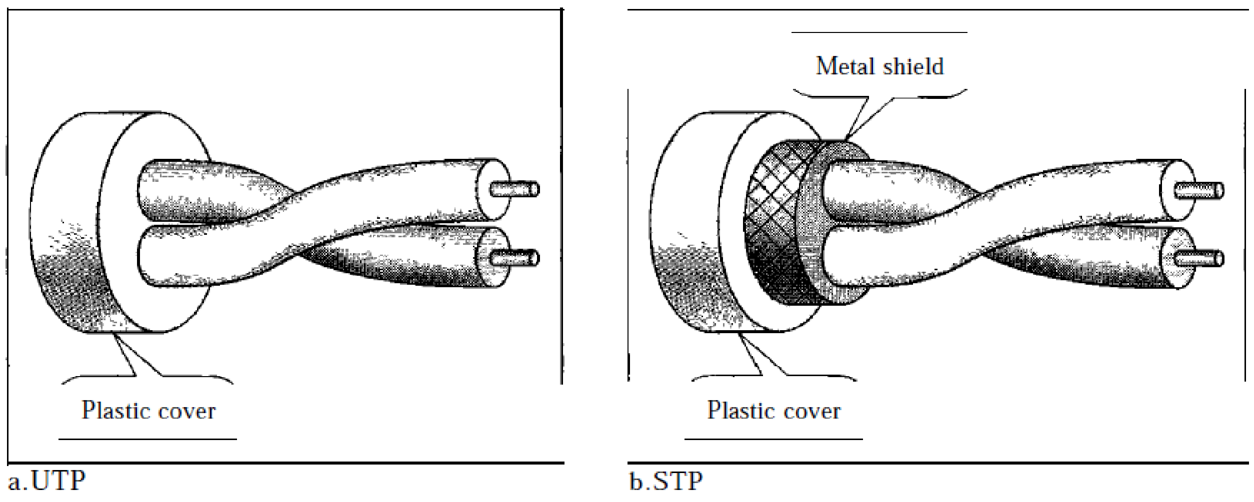


- A twisted pair consists of two conductors (normally copper), each with its own plasticinsulation, twisted together.

a) Unshielded Versus Shielded Twisted-Pair Cable:

- The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP).
- IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP).
- STP cable has a metal foil or braidedmesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it isbulkier and more expensive.
- The following figure shows the difference between UTP and STP.

UTP and STP cables



b) Categories:

- The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories.
- Categories are determined by cablequality, with 1 as the lowest and 7 as the highest.
- Each EIA category is suitable forspecific uses.
- The following table shows these categories.

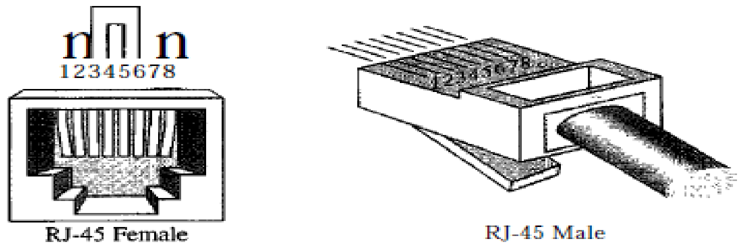
Table *Categories ofunshielded twisted-pair cables*

Category	*Specification*	*Data Rate (Mbps)*	*Use*
I	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-llines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
SE	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk: and increases the data rate.	600	LANs

c) Connectors:

- The most common UTP connector is RJ45 (RJ stands for registered jack).
- The RJ45 is a keyed connector, meaning the connector can be inserted inonly one way.

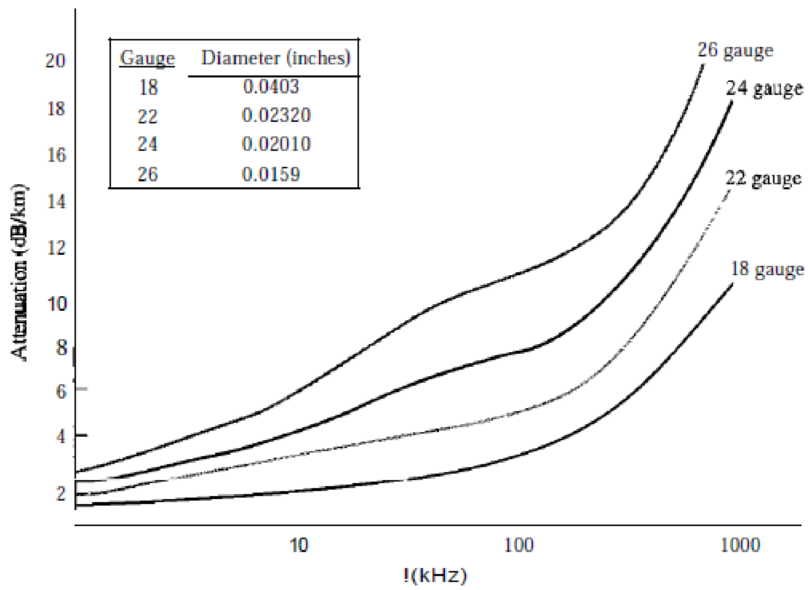
UTP connector



d) Performance:

- One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance.
- A twisted-pair cable can pass a wide range of frequencies.
- However, with increasing frequency, the attenuation, measured indecibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz.
- Notethat gauge is a measure of the thickness of the wire.

UTP performance



e) Performance:

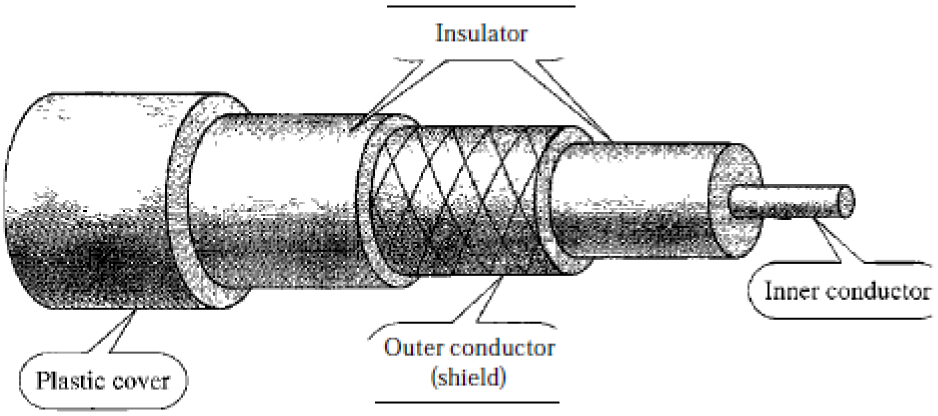
- Twisted-pair cables are used in telephone lines to provide voice and data channels.
- Thelocal loop-the line that connects subscribers to the central telephone office---commonlyconsists of unshielded twisted-pair cables.
- The DSL lines that are used by the telephone companies to provide high-data-rateconnections also use the high-bandwidth capability of unshielded twisted-pair cables.

- Local-area networks, such as lOBase-T and lOOBase-T, also use twisted-pair cables.

1.2- Coaxial Cable:

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twistedpaircable, in part because the two media are constructed quite differently.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Coaxial cable



a) Coaxial Cable Standards:

- Coaxial cables are categorized by their radio government (RG) ratings.
- Each RG number denotes a unique set of physical specifications, including the wire gauge of theinner conductor, the thickness and type of the inner insulator, the construction of theshield, and the size and type of the outer casing. Each cable defined by an RG rating isadapted for a specialized function.

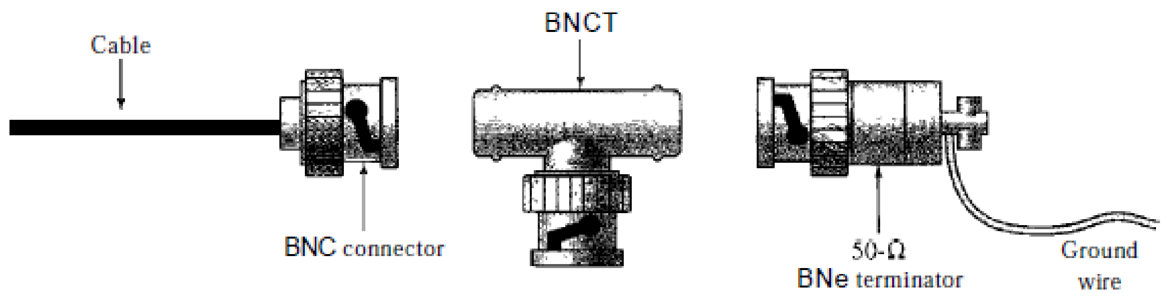
Table *Categories of coaxial cables*

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

b) Coaxial Cable Connectors:

- To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNe), connector.
- There are three popular types of these connectors: the BNC connector, the BNC T connector, andthe BNC terminator.
- The BNC connector is used to connect the end of the cable to a device, such as aTV set.
- The BNC T connector is used in Ethernet networks to branchout to a connection to a computer or other device.
- The BNC terminator is used at theend of the cable to prevent the reflection of the signal.

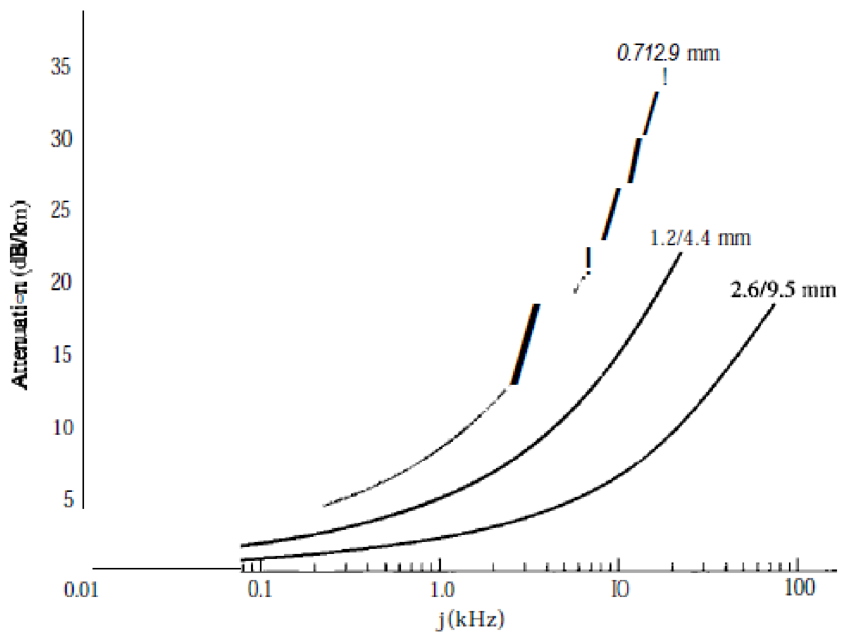
BNC connectors



c) Performance:

- As we did with twisted-pair cables, we can measure the performance of a coaxial cable.
- We notice that the attenuation is much higher in coaxial cables than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Coaxial cable pelformance



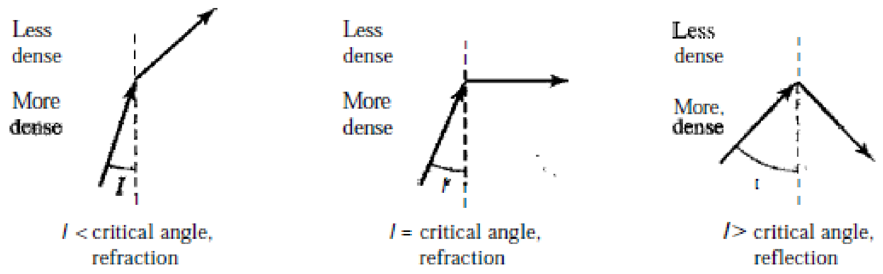
d) Applications:

- Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
- Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps.
- However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable.
- Cable TV networks also use coaxial cables. In the traditional cableTV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.
- Another common application of coaxial cable is in traditional Ethernet LANs. Because of its high bandwidth, and consequently high data rate, coaxialcable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or ThinEthernet, uses RG-58 coaxial cable with BNe connectors to transmit data at 10 Mbpswith a range of 185 m. The lOBase5, or Thick Ethernet, uses RG-11 (thick coaxial cable)to transmit 10 Mbps with a range of 5000 m. Thick Ethernet has specialized connectors.

1.3- Fiber-Optic Cable:

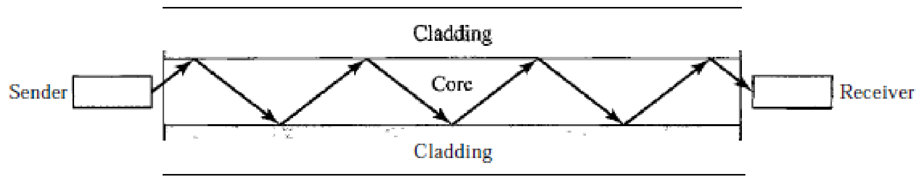
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.To understand optical fiber, we first need to explore several aspects of the nature of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.If a ray of light traveling through one substance suddenly enters another substance(of a different density), the ray changes direction.
- The following figure shows how a ray of lightchanges direction when going from a more dense toa less dense substance.

Bending oflight ray



- As the figure shows, if the angle of incidence I (the arIgle the ray makes with theline perpendicular to the interface between the two substances) is less than the criticalangle, the ray refracts and moves closer to the surface. If the angle of incidence isequal to the critical angle, the light bends along the interface. If the angle is greater thanthe critical angle, the ray reflects (makes a turn) and travels again in the denser substance.Note that the critical angle is a property of the substance, and its value differsfrom one substance to another.
- Optical fibers use reflection to guide light through a channel. A glass or plastic coreis surrounded by a cladding of less dense glass or plastic. The difference in density of thetwo materials must be such that a beam of light moving through the core is reflected offthe cladding instead of being refracted into it.

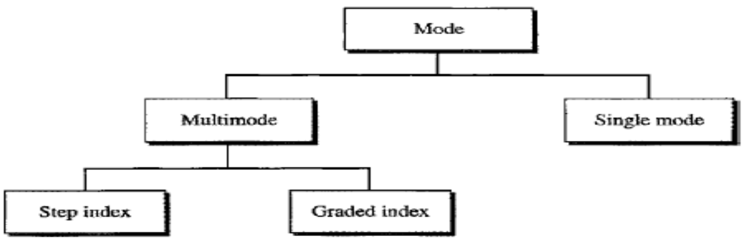
Opticaljiber



a) Propagation Modes:

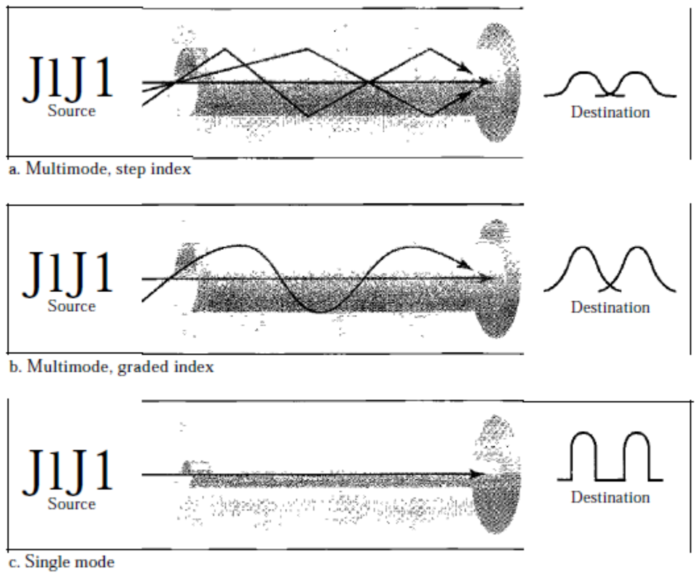
- Current technology supports two modes (multimode and single mode) for propagating lightalong optical channels, each requiring fiber with different physical characteristics.
- **Multimode**can be implemented in two forms: step-index or graded-index.

Propagation modes



- Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core.

Modes



- In multimode step-index fiber, the density of the core remains constant from thecenter to the edges. A beam of light moves through this constant density in a straightline until it reaches the interface of the core and the cladding. At the interface, there isan abrupt change due to a lower density; this alters the angle of the beam's motion. Theterm step index refers to the suddenness of this change, which contributes to the distortionof the signal as it passes through the fiber.
- A second type of fiber, called multimode graded-index fiber, decreases this distortionof the signal through the cable. The word index here refers to the index of refraction.
- The index of refraction is related to density. A graded-index fiber,therefore, is one with varying densities. Density is highest at the center of the core anddecreases gradually to its lowest at the edge.
- **Single-mode** uses step-index fiber and a highly focused source of lightthat limits beams to a small range of angles, all close to the horizontal.
- The singlemodefiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction).
- The decrease in densityresults in a critical angle that is close enough to 90° to make the propagation of beamsalmost horizontal. In this case, propagation of different beams is almost identical, anddelays are negligible. All the beams arrive at the destination "together" and can berecombined with little distortion to the signal.

b) Fiber Sizes:

- Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers.
- Note that the last size listed is for single-mode only.
- The common sizes are shown in the following table.

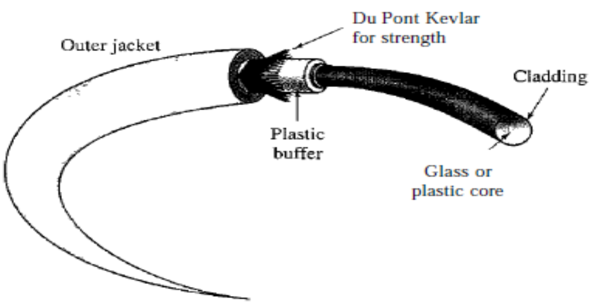
Table *Fiber types*

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
501125	50.0	125	Multimode, graded index
62.51125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

c) Cable Composition:

- The following figure shows the composition of a typical fiber-optic cable. The outer jacket is madeof either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is anotherplastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists ofcladding and core.

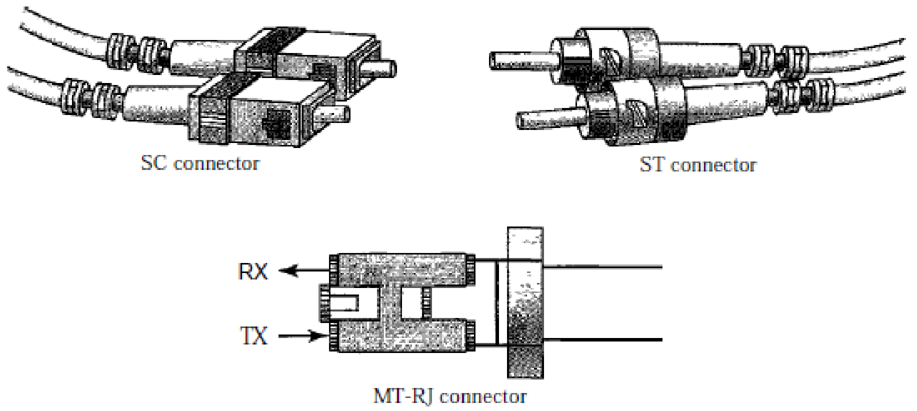
Fiber construction



d) Fiber-Optic Cable Connectors:

- There are three types of connectors for fiber-optic cables.

Fiber-optic cable connectors

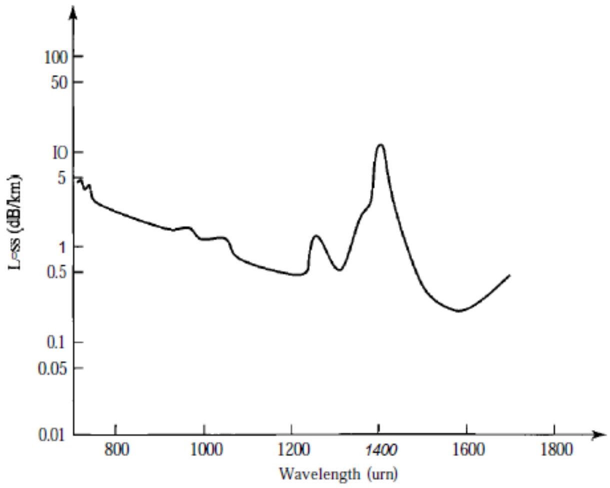


- The subscriber channel (SC) connector is used for cable TV. It uses a push/pulllocking system.
- The straight-tip (ST) connector is used for connecting cable tonetworking devices. It uses a bayonet locking system and is more reliable than SC.
- MT-RJ is a connector that is the same size as RJ45.

e) Performance:

- Theplot of attenuation versus wavelength in the following figure shows a very interestingphenomenon in fiber-optic cable.

Optical fiber performance



- Attenuation is flatter than in the case of twisted-paircable and coaxial cable.
- The performance is such that we need fewer (actually 10 timesless) repeaters when we use fiber-optic cable.

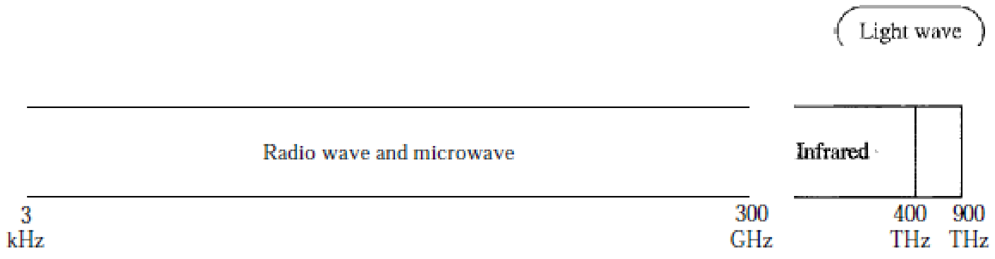
f) Applications:

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps. The SONET network that we discuss in Chapter 17 provides such a backbone.
- Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises. This is a cost-effective configuration since the narrow bandwidth requirement at the user end does not justify the use of optical fiber.
- Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

2- UNGUIDED MEDIA: WIRELESS [1][12][13]:

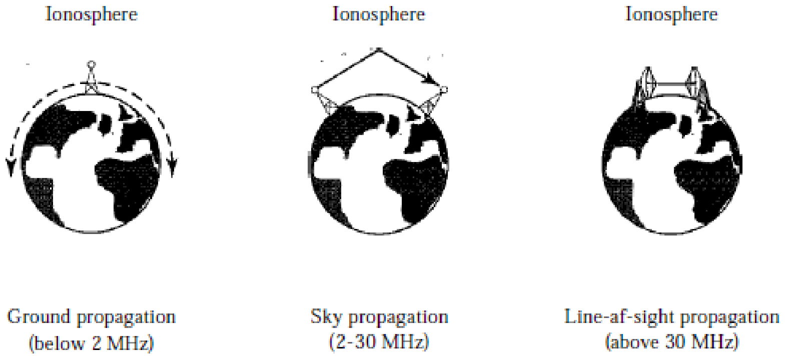
- Unguided media transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication.
- Signalsare normally broadcast through free space and thus are available to anyone who has adevice capable of receiving them.
- The following figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to900 THz, used for wireless communication.

Electromagnetic spectrum for wireless communication



- Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in the following figure.

Propagation methods



- In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth.
- These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
- Distance depends on the amount of power in the signal: The greater the power, the greater the distance. In sky propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth.
- This type of transmission allows for greater distances with lower output power.
- In line-or-sight propagation, very high-frequency signals are transmitted in straightlines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

- The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called bands, each regulated by government authorities.These bands are rated from very low frequency (VLF) to extremely highfrequency (EHF).
- The following table lists these bands, their ranges, propagation methods, and some applications.

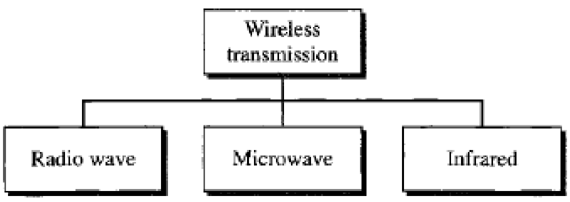
Table *Bands*

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3-30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30-300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz-3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3-30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30-300 GHz	Line-of-sight	Radar, satellite

2- 1 Wireless transmission groups:

- We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves.

Wireless transmission waves



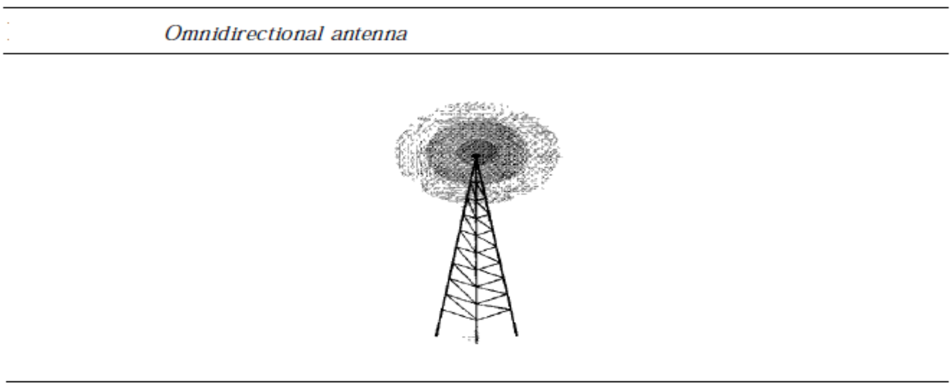
2- 1-1 Radio Waves:

- Although there is no clear-cut demarcation between radio waves and microwaves, electromagneticwaves ranging in frequencies between 3 kHz and 1 GHz are normally calledradio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves.However, the behavior of the waves, rather than the frequencies, is a bettercriterion for classification.

- Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has a disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into subbands, the subbands are also narrow, leading to a low data rate for digital communications.
- Almost the entire band is regulated by authorities (e.g., the FCC in the United States). Using any part of the band requires permission from the authorities.

a) Omnidirectional Antenna:

- Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas.



Radio waves are used for multicast communications, such as radio and television, and paging systems.

b) Applications:

- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

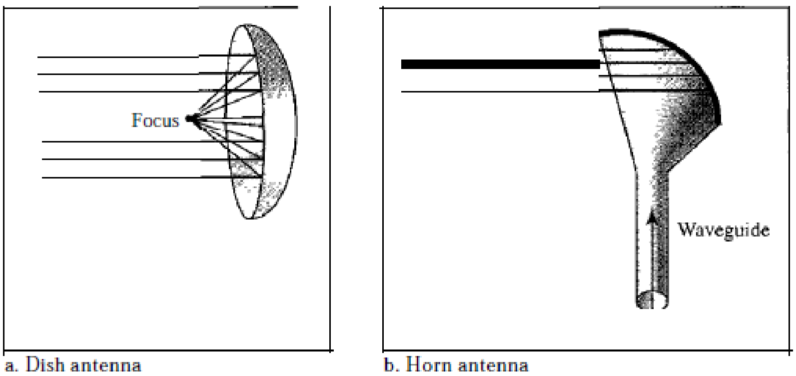
2- 1-2 Microwaves:

- Electromagnetic waves having frequencies between I and 300 GHz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. The following describes some characteristics of microwave propagation:
    - ✓ Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long distance communication.
    - ✓ Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
    - ✓ The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible.
    - ✓ Use of certain portions of the band requires permission from authorities.

a) Unidirectional Antenna:

- Microwaves need unidirectional antennas that send out signals in one direction.
- Two types of antennas are used for microwave communications: the parabolic dish and the horn.

Unidirectional antennas



a. Dish antenna   b. Horn antenna

- A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-pointreceiver.

- Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.
- A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

b) Applications:

- Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks, and wireless LANs.

2- 1-3 Infrared:

- Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mmto 770 nm), can be used for short-range communication. Infrared waves, having highfrequencies, cannot penetrate walls.
- This advantageous characteristic prevents interferencebetween one system and another; a short-range communication system in one roomcannot be affected by another system in the next room.
- When we use our infrared remotecontrol, we do not interfere with the use of the remote by our neighbors.
- However, thissame characteristic makes infrared signals useless for long-range communication.
- Inaddition, we cannot use infrared waves outside a building because the sun's rays containinfrared waves that can interfere with the communication.

a) Applications:

- The infrared band, almost 400 THz, has an excellent potential for data transmission.
- Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association (IrDA), an association for sponsoring the use of infraredwaves, has established standards for using these signals for communication betweendevices such as keyboards, mice, PCs, and printers.
- For example, some manufacturersprovide a special port called the IrDA port that allows a wireless keyboard to communicatewith a PC. The standard originally defined a data rate of 75 kbps for a distanceup to 8 m. The recent standard defines a data rate of 4 Mbps.Infrared signals defined by IrDA transmit through line of sight; the IrDA port onthe keyboard needs to point to the PC for transmission to occur.

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Chapter 2. Local networks

1- Network Standardization [1][9]

- Networking standards define the rules for data communications that are needed for interoperability of networking technologies and processes.
- Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.
- During data communication, a number of standards may be used simultaneously at the different layers. The commonly used standards at each layer are:
  - ✓ **Application layer** – HTTP, HTML, POP, H.323, IMAP
  - ✓ **Transport layer** – TCP, SPX
  - ✓ **Network layer** –IP, IPX
  - ✓ **Data link layer** – Ethernet IEEE 802.3, X.25, Frame Relay
  - ✓ **Physical layer** –RS-232C (cable), V.92 (modem)

1.1- Types of Standards

- Standards are of two types:
  - ✓ **De facto:** These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP had started as a de facto standard.
  - ✓ **De jure:** These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

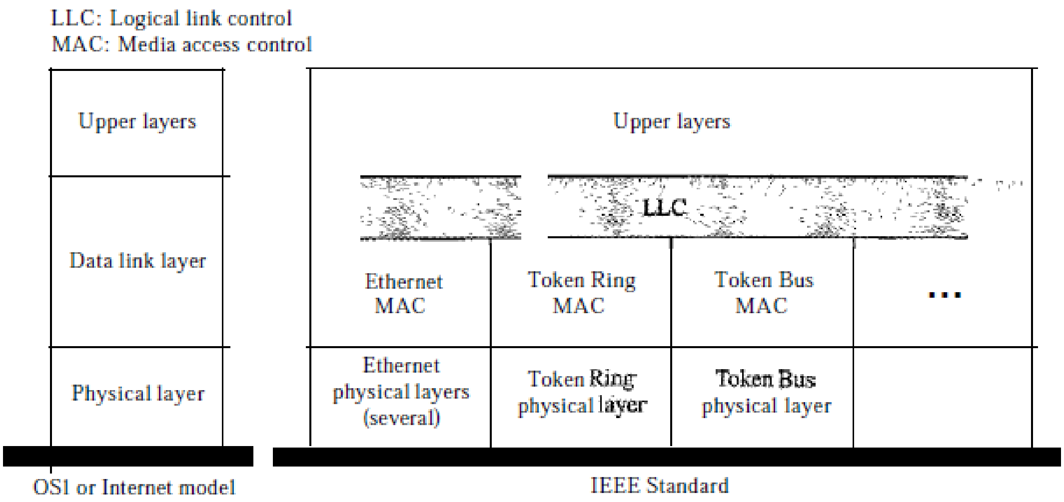
1.2- Standards Organizations

- Some of the noted standards organizations are:
  - ✓ International Standards Organization (ISO)
  - ✓ International Telecommunication Union (ITU)
  - ✓ Institute of Electronics and Electrical Engineers (IEEE)
  - ✓ American National Standards Institute (ANSI)
  - ✓ Internet Research Task Force (IETF)
  - ✓ Electronic Industries Association (EIA)

2- IEEE Standards [1][9][14]:

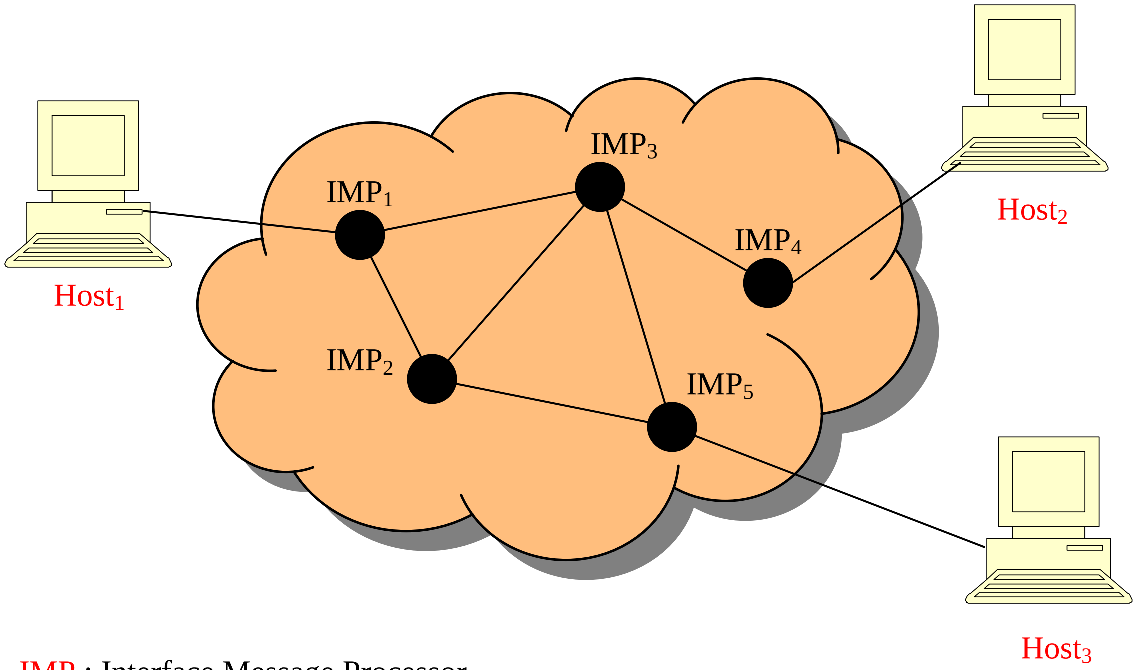
- In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.
- The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802.
- The relationship of the 802 Standard to the traditional OSI model is shown in Figure 13.1. The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.

IEEE standardfor LANs



3- Why Computer Networks? [1][13]

- Exchanging ideas.
- Separating data from physical storage.
- Convenience: without computer networks everybody needs a huge “super computer”.
- Mobility: it is hard to move a super computer while traveling.
- Robustness: a sudden damage to one or few machines should not affect the entire system.
- Concurrency: Different machines can be used in processing distributed computing applications.



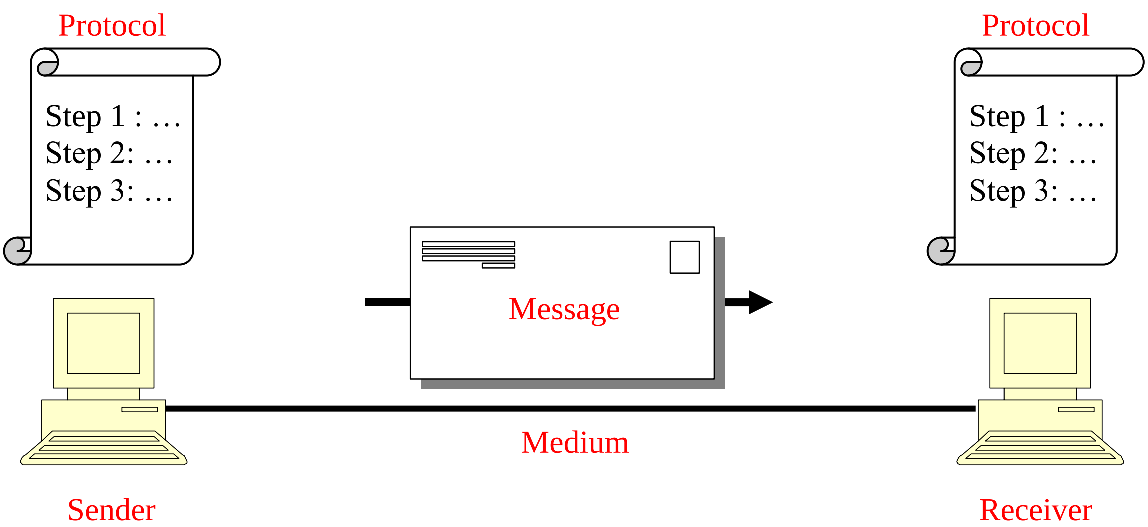
IMP : Interface Message Processor.

4- Network Effectiveness [1][11]:

The effectiveness of any computer network system depends on 3 fundamental characteristics:

1. Delivery: The network must deliver data to the correct destination.
2. Accuracy: The network must deliver data without alteration in transmission.
3. Timeliness: The network must deliver data in time schedule. Some data are asynchronous: email, file transmission, thus they don't require high quality service of transmission. On the other hand, live TV or radio transmission needs a nearly immediate broadcasting.

5- Data Communication Components[1][13]:



- Message: The information to be communicated such as text, sound, image, video, …
- Sender: The device that sends the message such as a computer, a server, a video camera, …
- Receiver: The device that receives the message.
- Medium: The physical path by which a message travels from a sender to a receiver, e.g., twisted-pair wire, coaxial cable, fiber optic cable, radio waves, …
- Protocol: The set of rules that governs data communications.

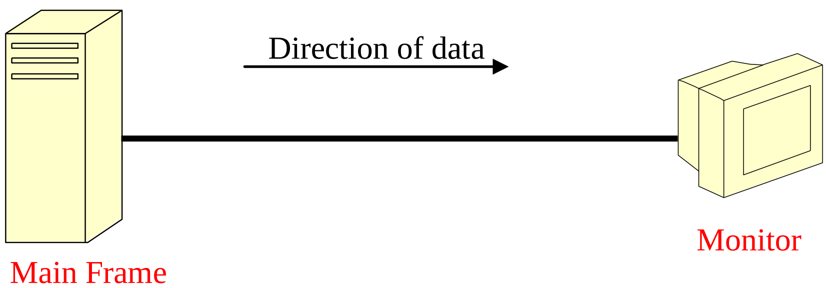
Example of a protocol:

At the sender side	At the receiver side
- Put the message in an envelop. - Stick a stamp on the envelop. - Go outside and post it (slide it into a posting box).	- Check your PO box for new mail. - Open the envelop and throw it away. - Read the message

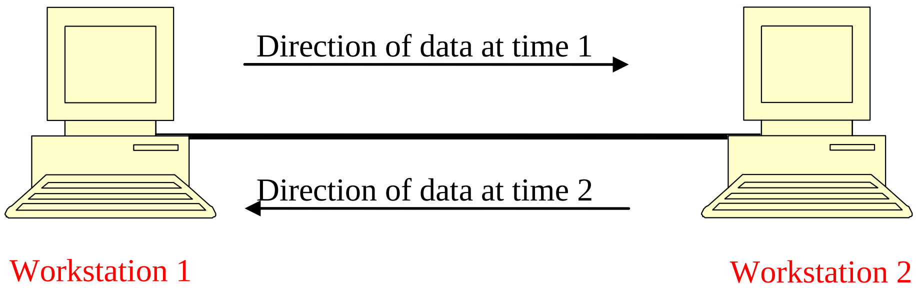
6- Direction of Data Flow[13][15][16]:

Data flow has three modes of direction:

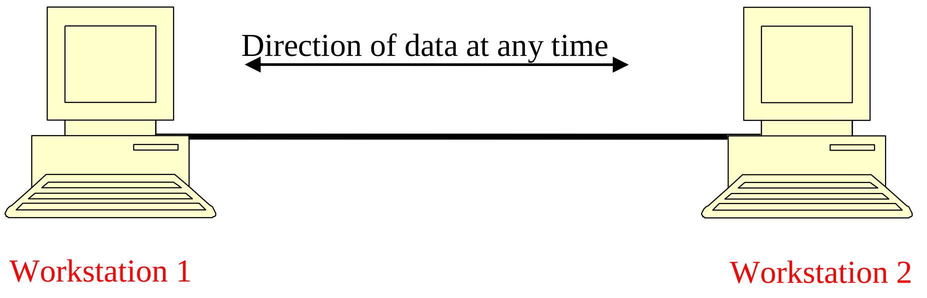
- Simplex: In this mode, information are transmitted in one-way direction only: The sender can only send information while the receiver can only receive it.



- Half-Duplex: In this mode, both stations can send and receive information but not at the same time: When a station is sending the other receives, and vice versa. Walkie-Talkie conversations are an example of half-duplex communications.



- Full-Duplex: In this mode, both stations can send and receive information simultaneously. Phone communications are full duplex since both persons can speak at the same time!!!

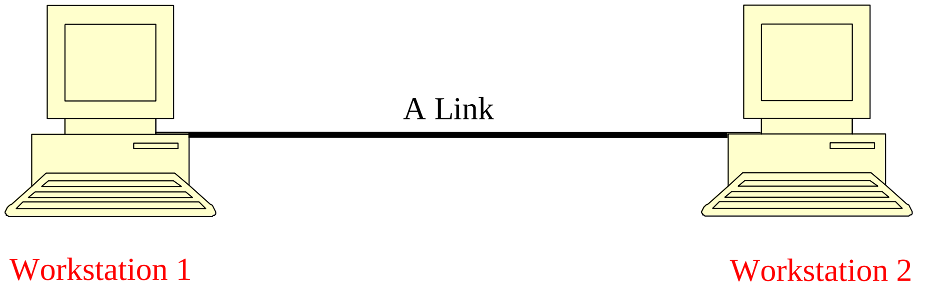


7- Types of Connections [1][6]:

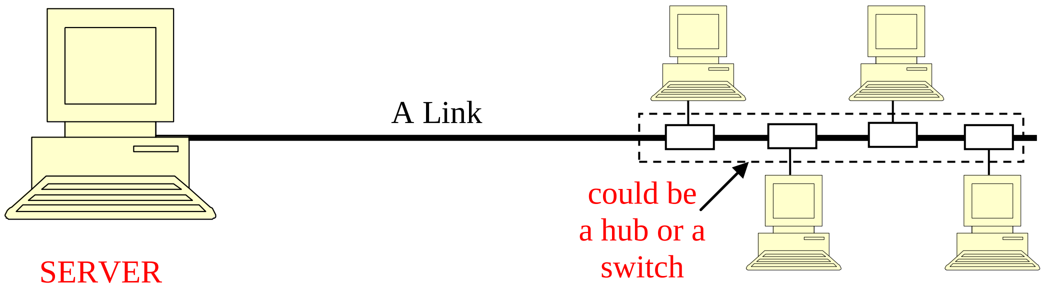
A network is two or more devices connected together through links. A links is communication pathway that is able to transfer data from one device to another.

In order for two devices to be able to communicate, they need to be connected to the same link at the same time. There are two types of connections:

- Point-to-Point connection: in this type, a dedicated link is provided between two devices. When you change a TV channel, the infrared connection between the remote control and the TV set is point-to-point.



- Multipoint connection: in this type, a link is shared between many communicating devices, either spatially or temporally:



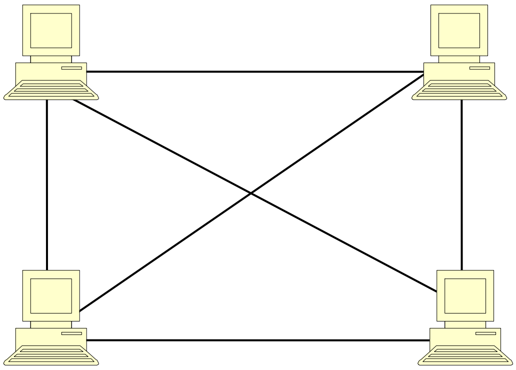
When the link is shared spatially, two or more devices can use some of the link capacity. Let's say that the link has a bandwidth of 10 Mbps (Mega bits per second), then 5 workstations can download simultaneously using 2 Mbps.

On the other hand, devices can share the link temporally: each device uses the entire bandwidth for certain moment.

8- Types of Topologies [1][17][18]:

A network topology refers to the way in which the devices are connected physically. We can distinguish 4 types of topologies:

- **8.1. Mesh topology:** in this topology, each station has a dedicated point-to-point link to every other device. Therefore, for n stations we need n(n-1)/2 links to complete the connections a fully connected network.



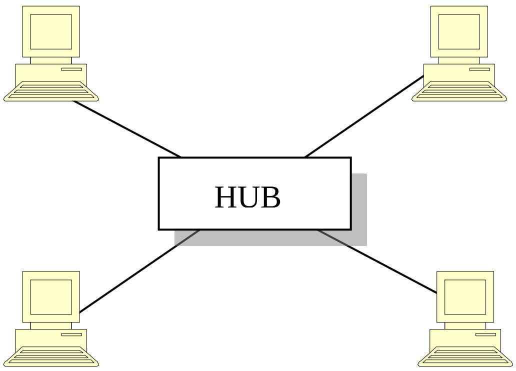
Advantages:

- Robust.
- Security and privacy.
- Fast response (1 hop).
- Fault detection.

Disadvantages:

- Very Expensive: the number of links and ports is quadratic to the number of devices.

- **8.2. Star topology:** in this topology, each station has a dedicated point-to-point link only to central controller, usually called a hub. Hence, the traffic between any two stations takes two hops:



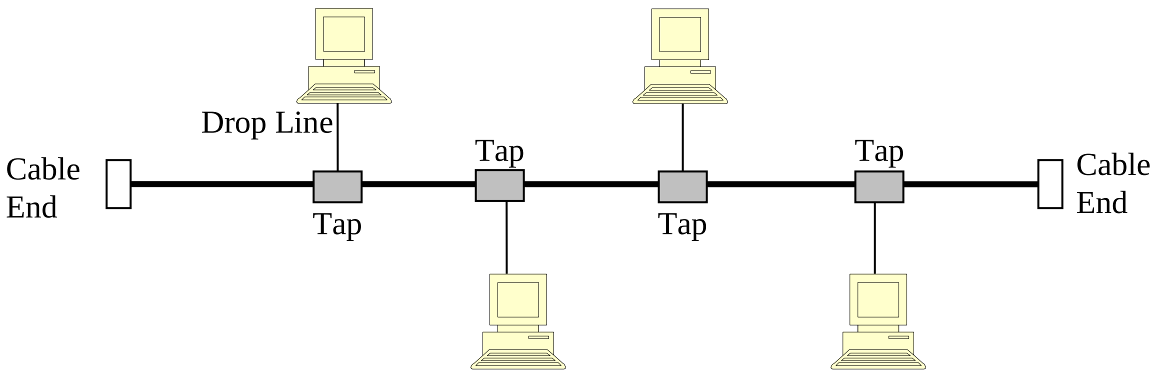
Advantages:

- Only one link and one port per station.
- Robust (when a device is down).
- Fast response (2 hops).
- Fault detection.

Disadvantages:

- Not robust: when the hub is down, the entire network is disabled.
- The Hub must have as ports as the number of connecting stations.
- No privacy.

- **8.3. Bus topology:** this topology is a multipoint connection where each station is connection through a tap (using a drop line) to a backbone cable:



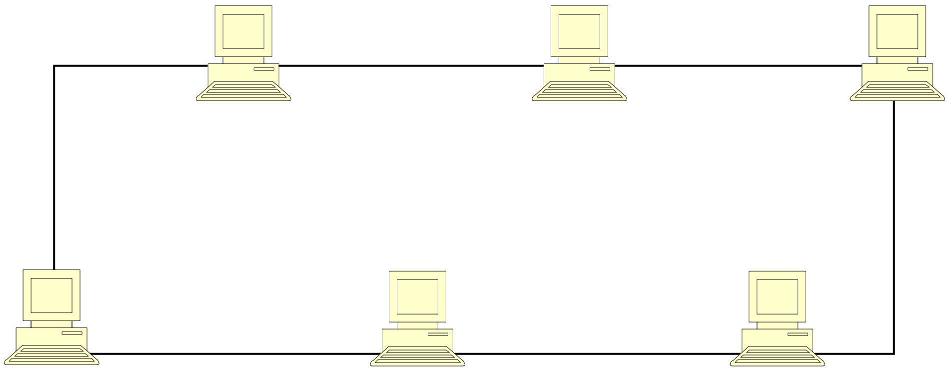
Advantages:

- Drop lines are proportionally shorter than links in ring topology. Only the backbone cable can extend to reach all stations.
- Easy installation: Backbone cable can be built-in offices walls.
- Robust (when a device is down).

Disadvantages:

- Fault detection is difficult.
- Connections are limited: adding more stations weakens the signal transmission.
- Not robust when the backbone cable is damaged.
- No privacy.

- **8.4. Ring topology:** in this topology, each station has two dedicated point-to-point links to stations on the right and left sides. So, data are transmitted from one station to another until it reaches the destination:



Advantages:

- Easy to install: two ports and two links per station.

Disadvantages:

- Considerable amount of hops.
- Not Robust.
- No Privacy.

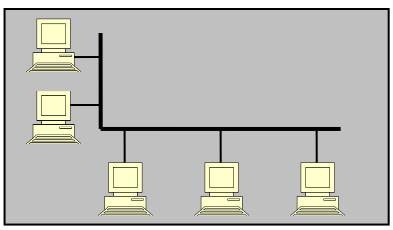
Networks: Categories and Models

I- Network Categories [1][8][9]:

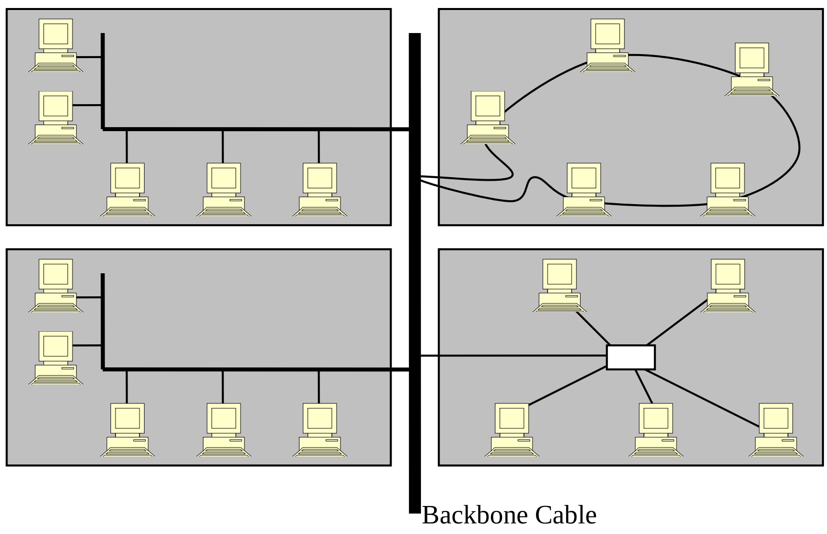
Networks are classified into three categories: LAN, MAN, and WAN

1- Local Area Networks (LAN):

- Privately owned.
- Links devices in a single building, or multiple buildings.
- Example: connecting two PCs and a printer in a house.
- Example: connecting 100 workstations and a server in an institute.
- Goals: sharing local resources (printer, …) , client/server applications
- Topologies: Ring, Bus, Star.
- Size: up to 1 KM.
- Speed: up to 100 Mbps.



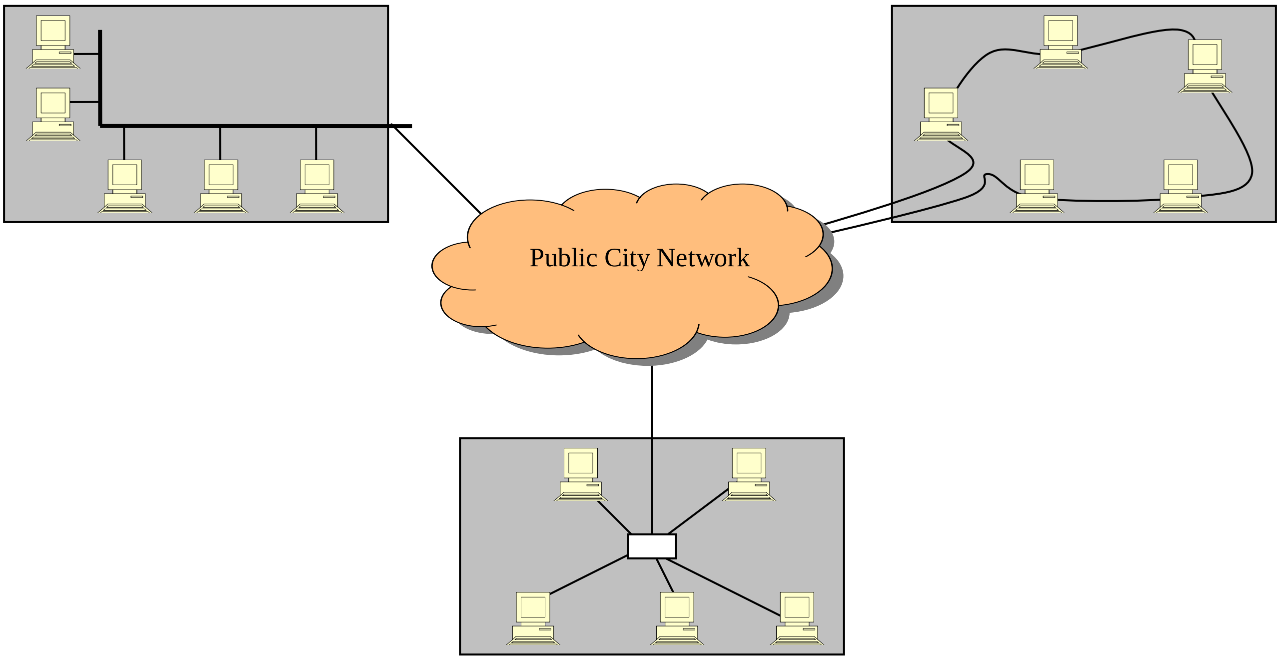
Single-building
LAN



Multiple-building
LAN

2- Metropolitan Area Networks (MAN):

- Extends over a city.
- Owned by a public/private company.
- Size: up to 10 km (city size)
- Speed: up to 10 Gbps.

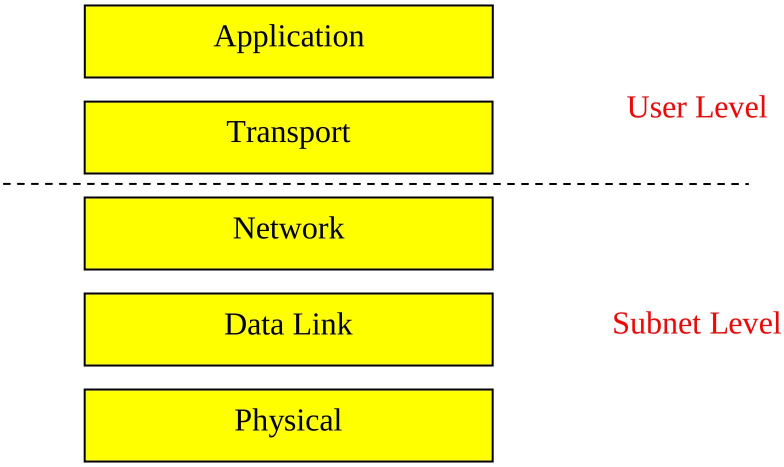


3- Wide Area Networks (WAN):

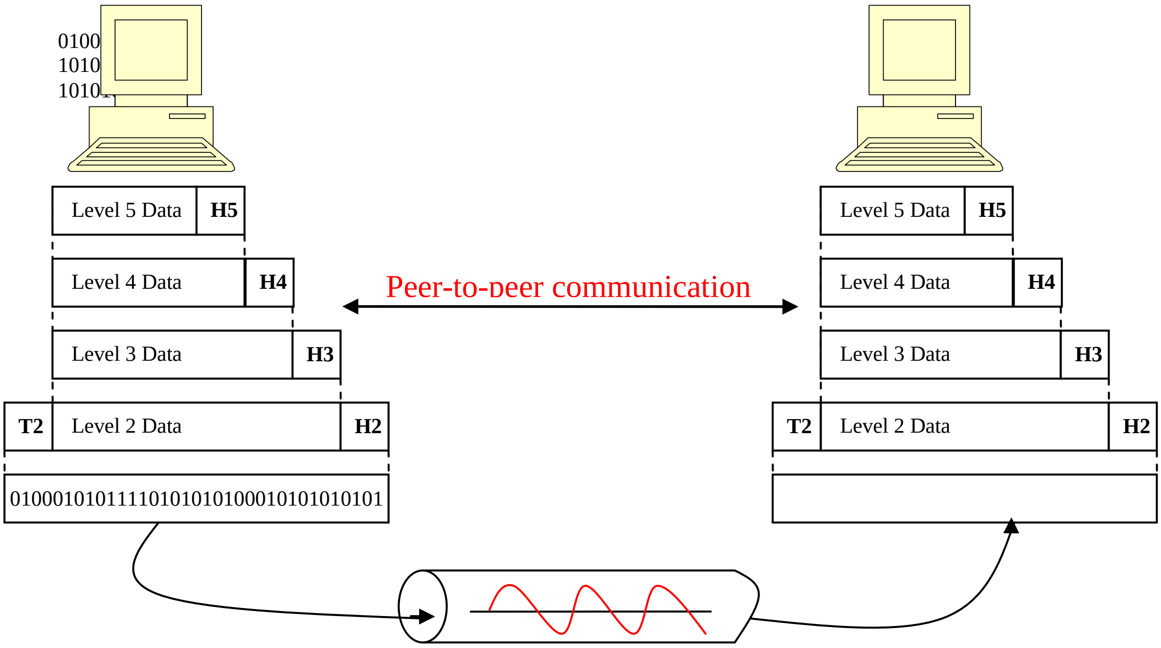
- Extends over a country or a continent.
- Provides long distance transmissions: large bandwidths, high quality and capacity of transmission medium.
- Utilizes public resources.

II- Network Models: Internet Model [1][19][20]

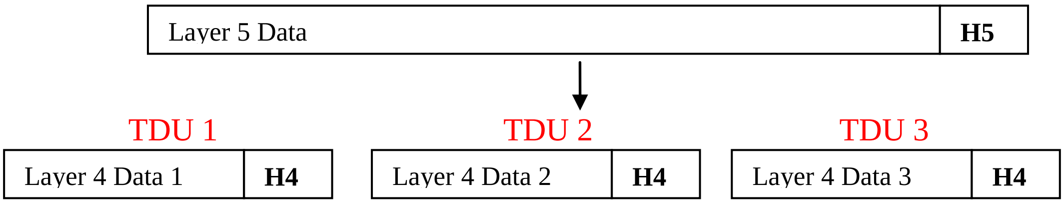
The Internet model is a layered protocol stack that dominates data communications and networking today. It is basically composed of 5 layers:



- A layer represents some functions that are mostly related.
- Functions of different layers are of different abstraction level.
- Headers and trailers might be attached to data units to serve protocol application.



- When data is passed from one layer to another, it might be divided into segments that we called data units: transport data units (TDU), network data units (packets), data link data units (frames).

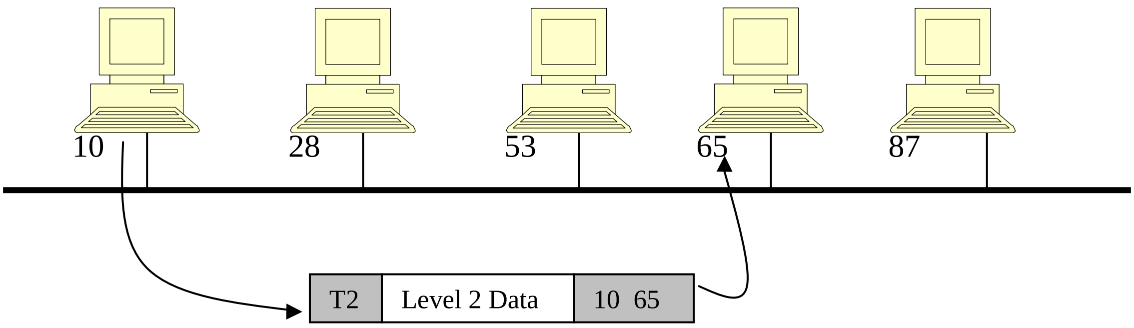


1- Physical Layer:

- Raw data transmission over communication channel.
- Data rate transmission.
- Voltage level, representation of bits.
- Simplex, half-duplex, duplex connections.
- Modulation, encoding, decoding.
- Transmission media.
- Transmission techniques: analog, digital.

2- Data Link Layer:

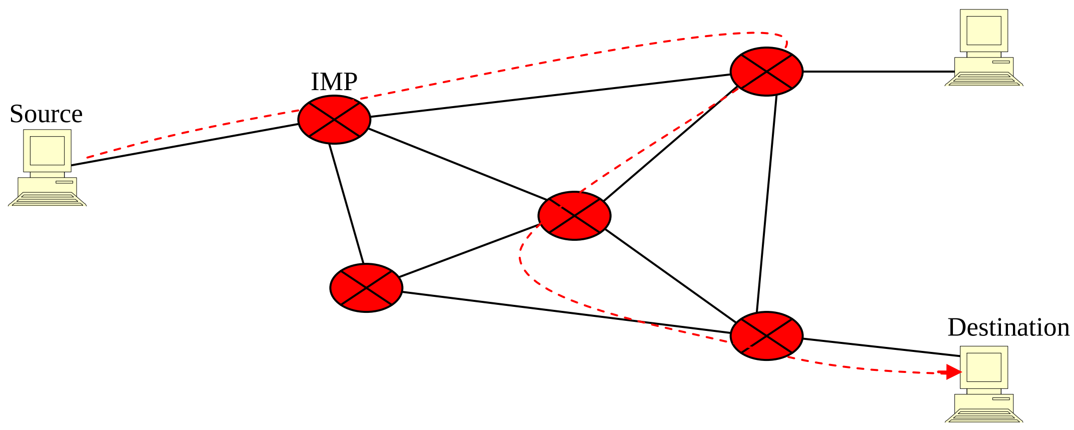
- Responsible for (local) node-to-node delivery of frames (information).
- Since noise might hit the transmitted signal at the physical layer, the data link layer detect and correct these errors at the receiver site before passing data to the network layer.
- At the sender site, the data link layer divides the network data units into frames of manageable sizes.
- Each frame has an attached header that contains the physical address of the sender and the receiver.



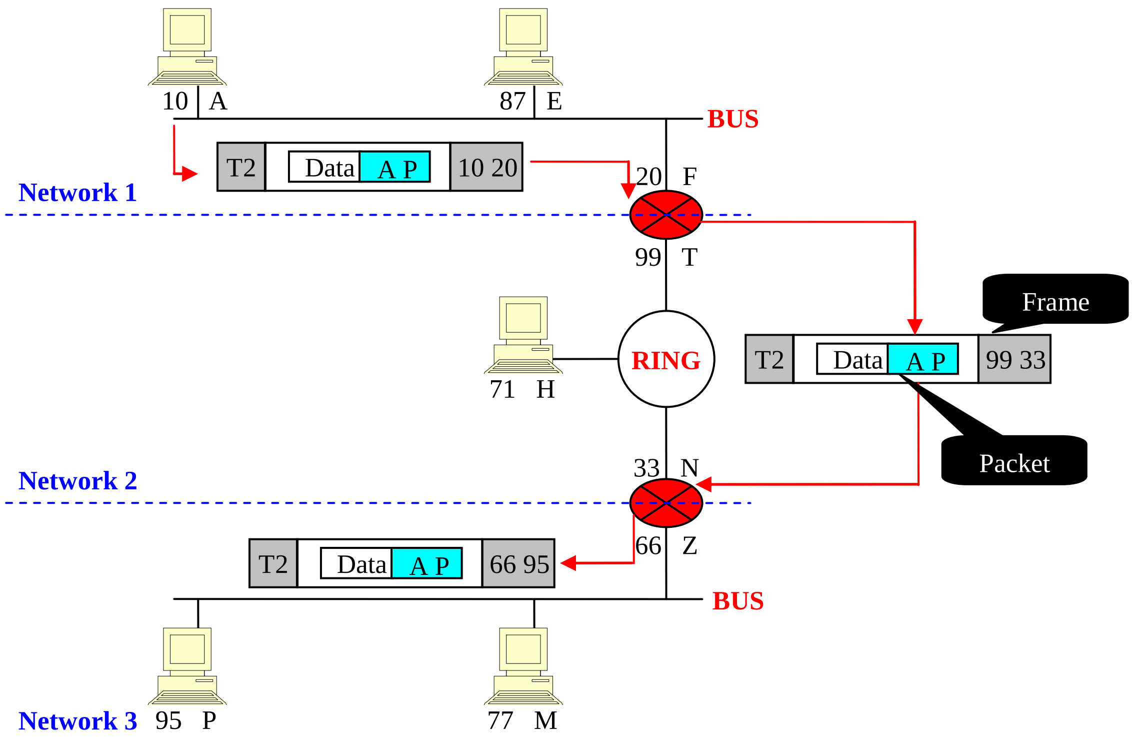
- If the receiver is outside the sender's network, the frame's header should contain the address of the bridge that connects the local network to the outside.
- Flow control: fast computers connected to slow ones.
- Access control: in multipoint connection for instance, data link protocols solve collision problems.

3- Network Layer:

- Responsible for (global) source-to-destination delivery of packets (information).
- When two systems belong to the same network, there is no need for a network layer. However, in order to be able to send a packet between two systems of different networks, routing algorithms are necessary to route packet through the grid of IMPs (Routers, switches, …).



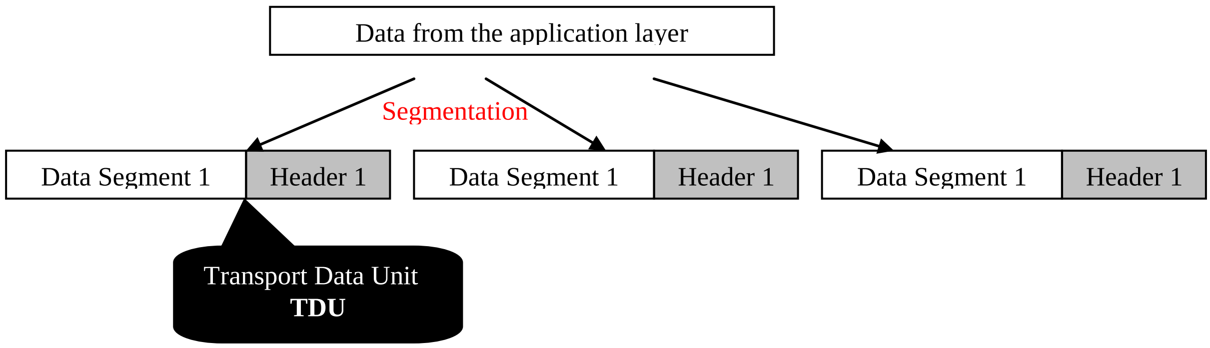
- The physical address is used in the same network to handle local problems (data link layer). The logical address (e.g., IP address) is attached to any machine logically, and can be changed any time. It serves as a universal address in internetworks.



- IMPs have usually two or more interfaces, each directed to the connected network. Therefore an IMP has more than one physical and logical address.
- When the frame is passed from a network to another, the physical addresses stored in the header are changed based on the logical addresses that are kept in the network packet inside the frame.

4- Transport Layer:

- Responsible for process-to-process delivery of the entire sent message.
- They could be many processes that communicate between two systems. The transport layer organizes the communication through port numbers, each correspond to an application or a service (process).
- Port numbers are stored in the header of the transport data unit TDU.



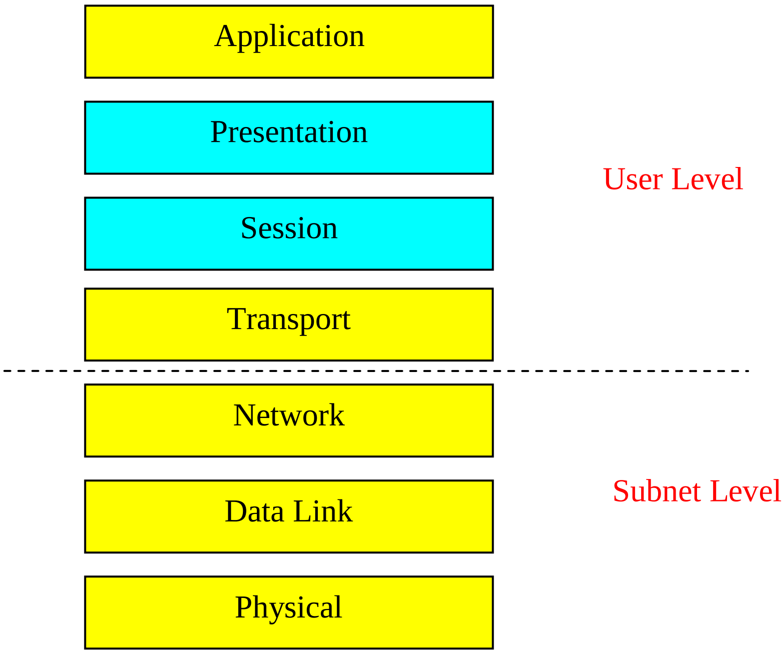
- The transport layer is responsible for segmentation and reassembly of the data coming from the application layer.
- TDUs can be sent in different paths (connectionless service) or a dedicated path (connection oriented service). In connectionless mode, sequence numbers of the TDUs must be added to the header in order to arrange them back in case they arrived in different order.
- The transport layer is also concerned with the flow control between end systems.
- Error control is also handled by the transport layer: if a TDU is lost (never arrived) the destination usually asks the source to retransmit it.

5- Application Layer:

- Serves as the interface between network and the user.
- Provides support for services like email, web access, remote login, file transfer.

III- Network Models: OSI Model [1][17][18]

The OSI model (Open Systems Interconnections), designed by ISO (International Organization for standardization), and has two more layers compared to the internet model: the presentation and the session layers:



1- Presentation layer:

- Designed to handle syntax and semantics of the exchanged information.
- Character sets: ASCII, extended ASCII, Unicode, ISO, …
- Compression and decompression.
- Encryption and decryption.

2- Session layer:

- Sessions Establishment, Session ending.
- Dialog controller.

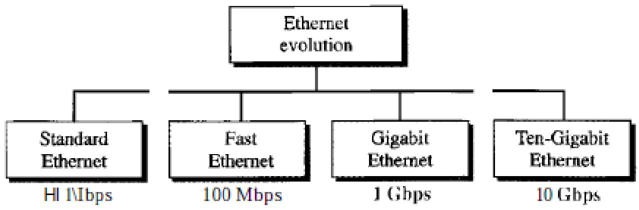
Chapter 3. Ethernet network

Local Area Networks: Ethernet

I- Standard Ethernet [1][21]:

- The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC).
- Since then, it has gone through four generations: Standard Ethernet (lot Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (l Gbps), and Ten-Gigabit Ethernet (l0 Gbps).

Ethernet evolution through four generations

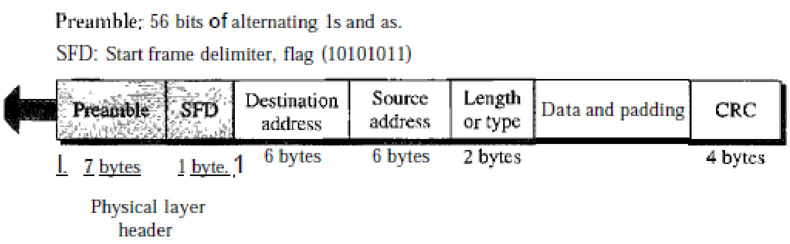


- In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

1- Frame Format

- The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRe.
- Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers.
- The format of the MAC frame is shown in the following figure.

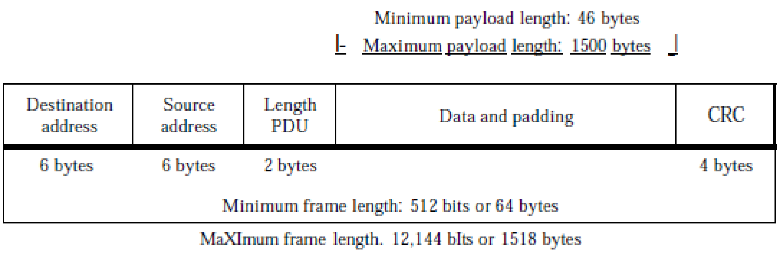
802.3 MAC frame



2- Frame Length

- Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame, as shown in the following figure.

Minimum and maximum lengths



3- Addressing

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address.
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

Example ofan Ethernet address in hexadecimal notation

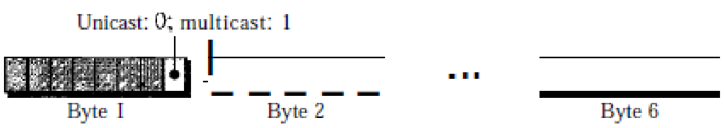
06:01 :02:01:2C:4B

6 bytes = 12 hex digits = 48 bits

4- Unicast, Multicast, and Broadcast Addresses

- A source address is always a unicast address-the frame comes from only one station.
- The destination address, however, can be unicast, multicast, or broadcast.
- The following figure shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

Unicast and multicast addresses



The least significant bit of the first byte defines the type of address.
If the bit is 0, the address is unicast; otherwise, it is multicast.

- A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one.
- A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many.
- The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight Is.

Example 01:

Define the type of the following destination addresses:

a. 4A:30:10:21:1O:1A

b. 47:20:1B:2E:08:EE

c. FF:FF:FF:FF:FF:FF

Solution:

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010 (even).

b. This is a multicast address because 7 in binary is 0111 (odd).

c. This is a broadcast address because all digits are F's.

The way the addresses are sent out on line is different from the way they are written in hexadecimal notation. The transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last. This means that the bit that defines an address as unicast or multicast arrives first at the receIver.

Example 02:

Show how the address 47:20:1B:2E:08:EE is sent out on line.

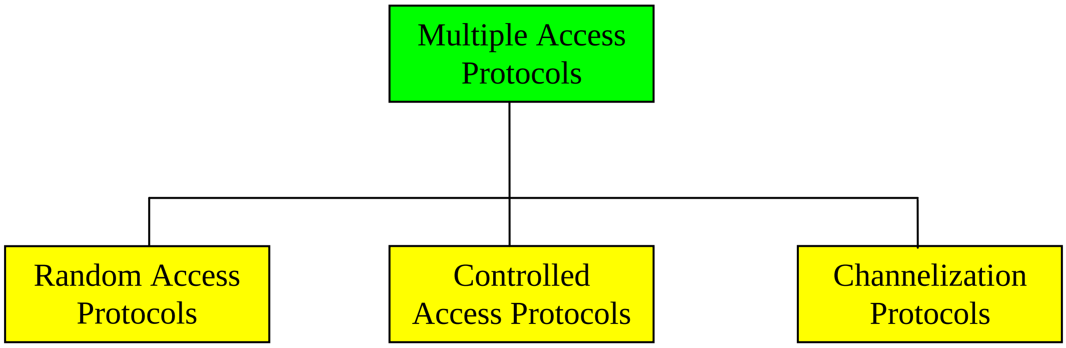
Solution:

The address is sent left-to-right, byte by byte; for each byte, it is sent right-to-Ieft, bit by bit, as shown below:

← 11100010 00000100 11011000 01110100 00010000 01110111

II- Multiple Access Protocols [1][21][22]:

- With Point-to-Point links, access control protocols are not needed since collisions cannot happen.
- When stations are connected using a common link (multipoint or broadcast), we need a protocol to coordinate access to the link.
- Many protocols have been developed to handle access to shared links:



- MA
- CSMA
- CSMA/CD
- CSMA/CA

- Reservation
- Polling
- Token passing

- FDMA
- TDMA
- CDMA

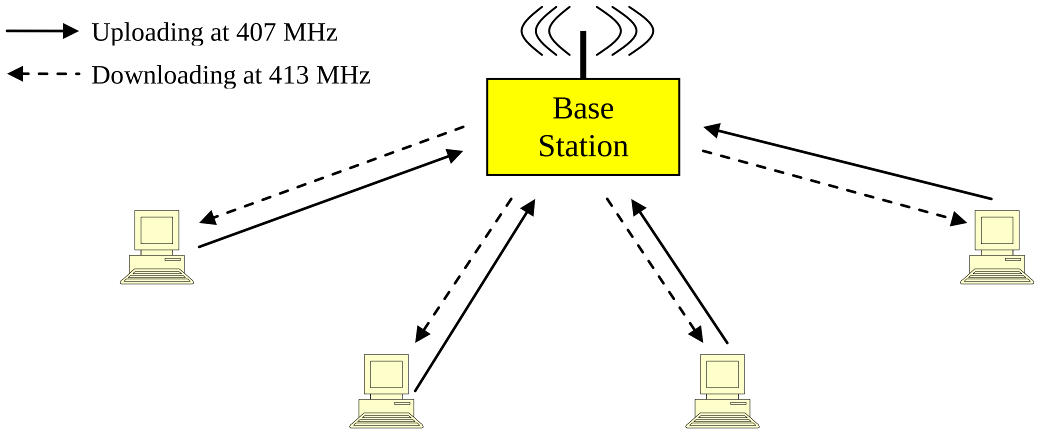
III- Random Access Protocols [1][23]:

- Each station has the right to access the shared medium without being controlled by any other station.
- When two or more stations start sending at the same time, their frames will collide so that they will be damaged. Then the protocol should be able to solve collision situation.
- The random access protocol should be able to answer the following questions:

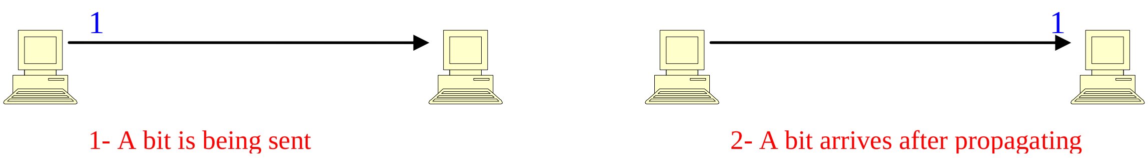
  - When can a station access the medium?
  - What can the station do if the medium is busy?
  - How can the station determine the success or failure of the transmission?
  - What can the station do in case of a collision?

1- MA (Multiple Access):

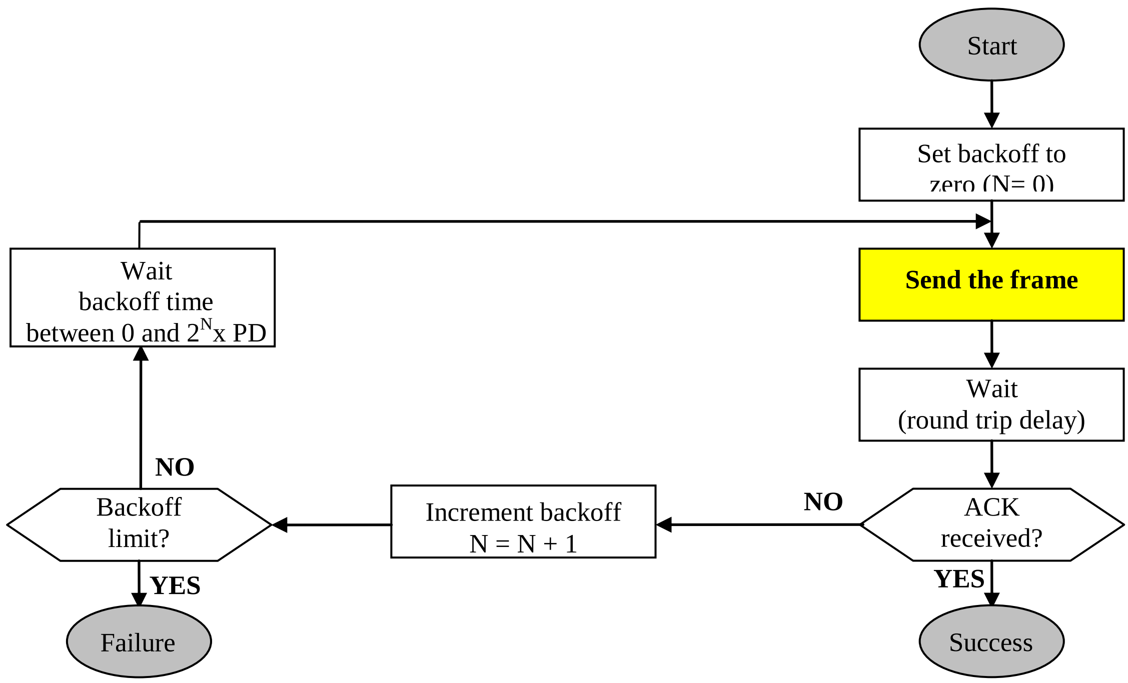
- The earliest and simple method of random access, originally known as ALOHA, developed in the University of Hawaii (1970).
- ALOHA was designed for radio LANs: stations can communicate through a central base station using one carrier frequency for uploading (407 MHz), and another carrier frequency for downloading (413 MHz).
- The base station plays the role of a hub, not a controller to organize the shared medium(air).

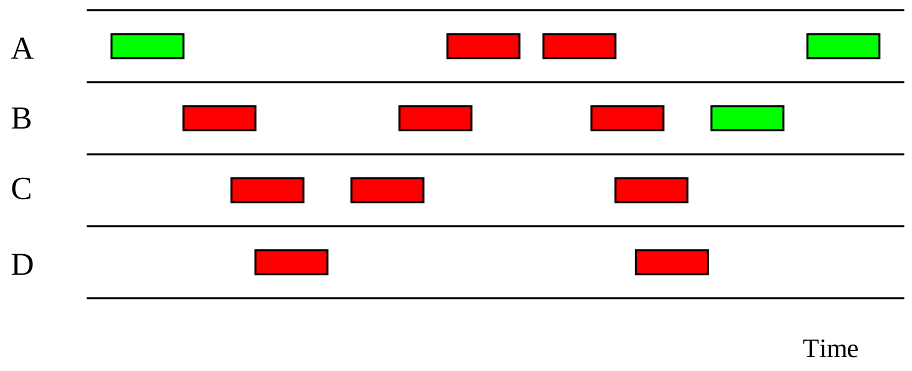


- In this protocol, a station can send frame whenever it's ready.
- In case of collision, the station waits for the some time related to the propagation delay.
- The propagation delay is the time that takes one bit to arrive to the receiver.



- If the link was idle, then the sending station should receive an ACK after a round trip delay.
- The round trip delay includes the propagation delay from the sender to receiver, and the time of frame processing (error control, flow control, …), and the propagation delay from the receiver to the sender for acknowledgement.
- If the link was busy, then the sending station will never get an ACK. In this case, the sending station should wait for some random time before resending the damaged frame.
- The random time is based on the exponential backoff mechanism: the station should wait for certain time between 0 and 2^N x (maximum propagation delay), where N is the number of attempted transmissions, initialized at 0.



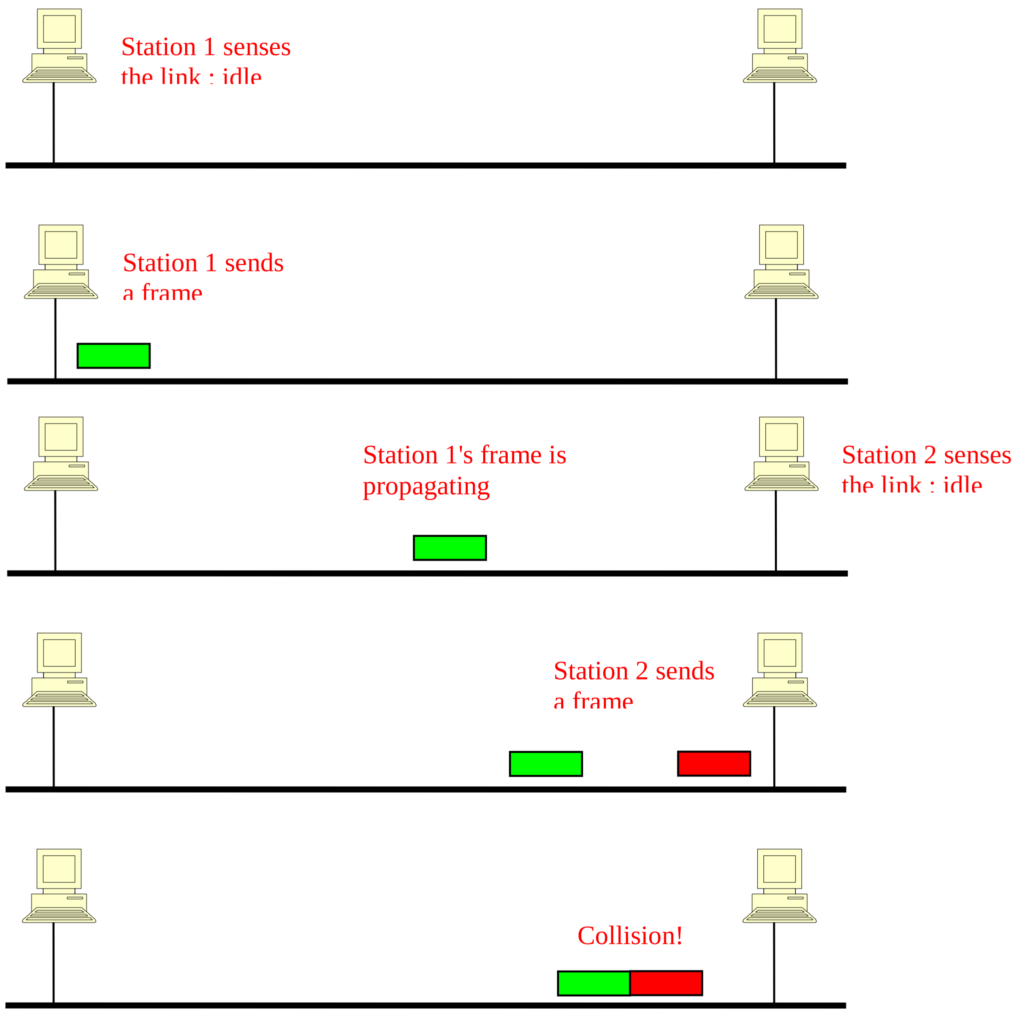


- Let's say that the maximum propagation delay is 1 ms. In case of a first collision, the sender should backoff for certain time between 0 and 2 ms. Then the sender attempts for the second time to send its frame. In case of a second collision, it should wait for certain time between 0 and 4 ms, and so on (0 and 8 ms, 0 and 16 ms, …) until reaching the maximum number of attempts, where the sender recesses.
- So, when 4 stations want to send frames at the same time, collision happens. Then each station waits for random time between 0 and 2 ms. Let's say that before 2nd attempt of sending frames, station 1 waits for 0 ms, station 2 waits for 1 ms, station 3 waits for 0 ms and station 4 waits for 2 ms. In this case, frames of station 1 and station 3 collides, while frames 2 and frames 4 are safe.

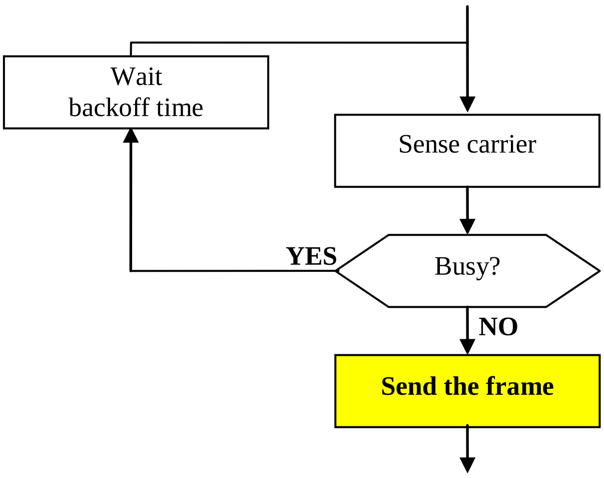
2- CSMA (Carrier Sense Multiple Access):

- In order to minimize the chance for collisions, the CSMA method was developed.

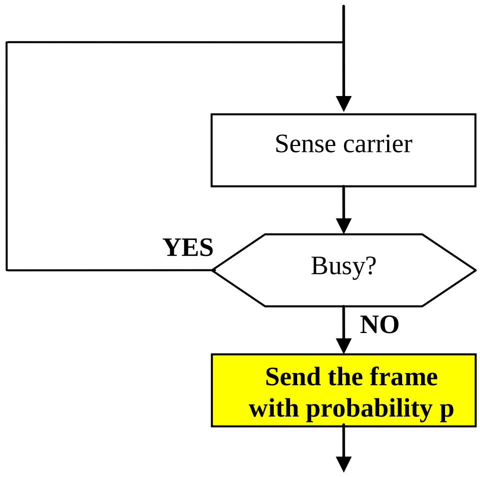
- The CSMA is based on sensing the carrier before utilizing it. The station can send frames only when the carrier (link) is idle.
- The CSMA reduces the possibility of collision, but it cannot eliminate it. Suppose that two stations sense the carrier at the same time and find it idle. Then, both of them start sending frames also at the same time.
- Even when two stations do not send frames at the same time, it is still possible for them to collide if the difference between sending time is less than the propagation time of each.



- The CSMA uses two strategies: Non-persistent and persistent.
- In Non-persistent strategy, it a station senses the link and finds it busy, then it waits for some random time before re-sensing it. This will reduce the chance of collisions.



- In persistent strategy, it a station senses the link and finds it idle, it sends a frame with probability *p*.

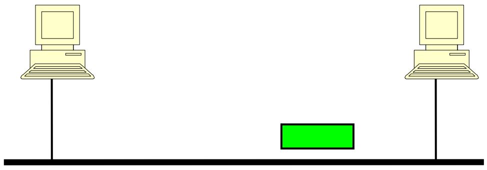


- When $p = 1$, the strategy is called 1-persistent, which means that a station sends a frame as soon as it finds the carrier idle.
- When $p \neq 1$, the strategy is called p-persistent, which means that a station sends a frame as soon as it finds the carrier idle, but with probability p. For instance, if $p = 0.2$, then the station sends frames only in 20% of the times only when the link is idle. The station can simply choose randomly a number between 0 and 100. If the result is less than or equal 20, then it can send a frame when the link is idle. Otherwise, it waits for certain time.

3- CSMA/CD (CSMA with Collision Detection):

- The CSMA method does not define the procedure for collision.
- CSMA/CD adds a procedure to handle collision. CSMA/CD is used in traditional Ethernet.
- The collision is detected through a burst signal (> 24 mAmp for coax) different that the sent one (between 18 and 20 mAmp), and arrives at time less than or equal 2τ, where τ is the maximum propagation delay (between the two farthest stations).

1- Station 1 sends a packet at time 0

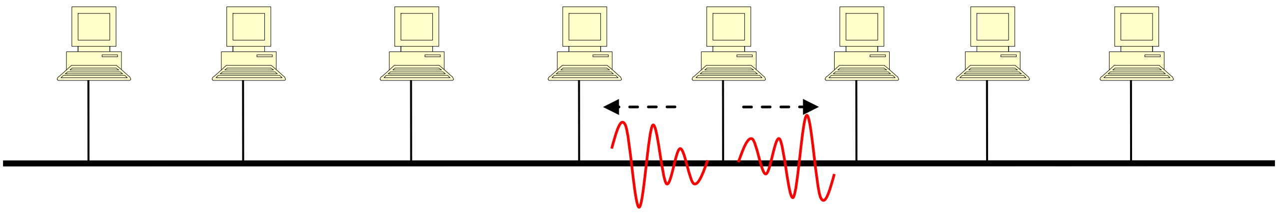


2- Packet at time $\tau - \varepsilon$

3- Station 2 sends a frame t at time τ: a burst signal is created.

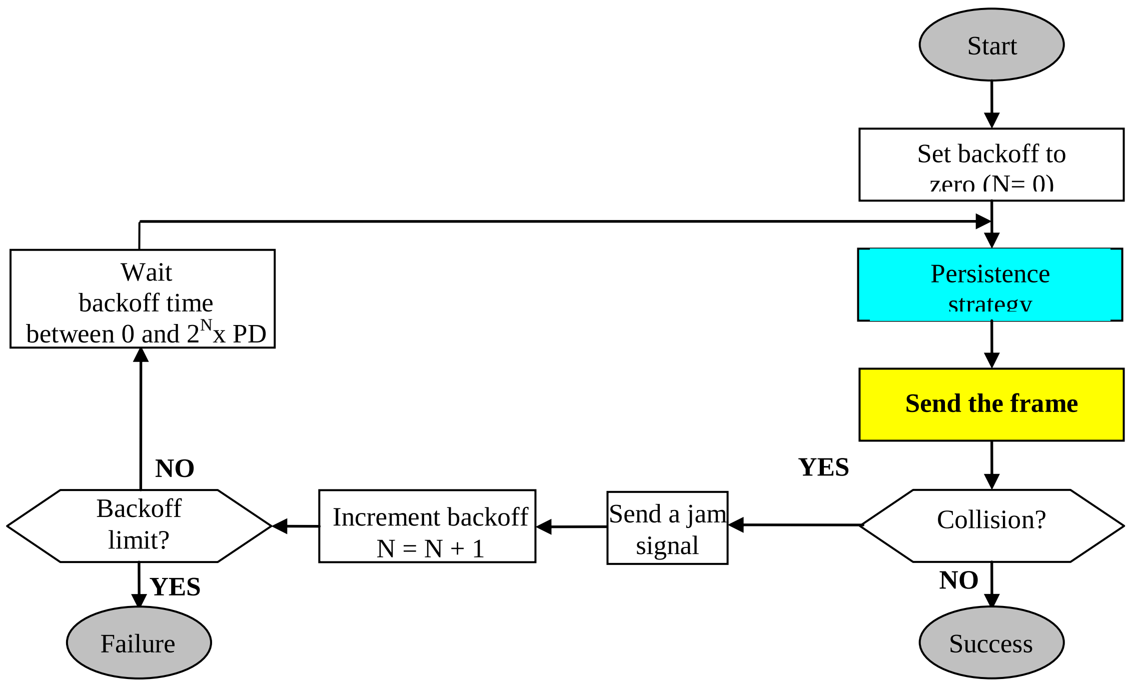
4- The burst signal arrives at station 1 at time 2τ

- Once a collision is detected by the sending station, the latter sends a jam signal informing other station of a collision situation. Note that, in a LAN, all stations receive the sent frame and the burst signal, so the jam signal inform them to ignore what they have received.



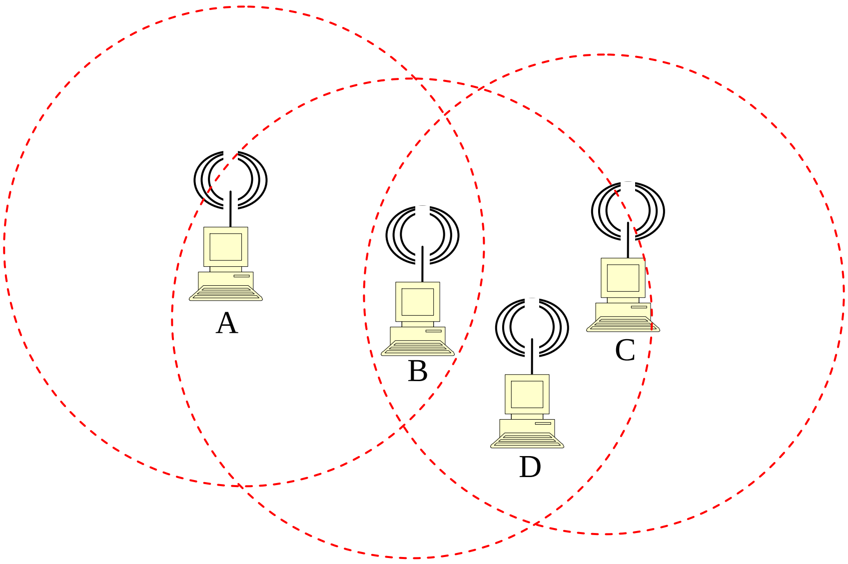
Sending a jam signal to all stations

- The CSMA/CD applies the exponential backoff whenever a frame is damaged due to collision.

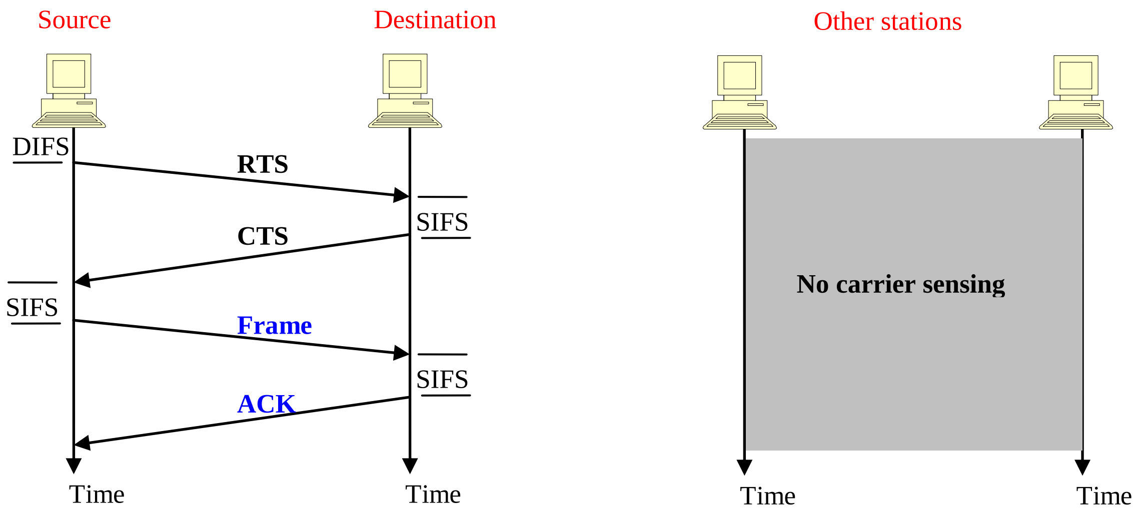

Start
Set backoff to zero (N= 0)
Persistence strategy
Send the frame
Collision?
YES
NO
Success
Send a jam signal
Increment backoff
N = N + 1
Backoff limit?
NO
YES
Failure
Wait
backoff time
between 0 and 2^N x PD

4- CSMA/CA (CSMA with Collision Avoidance):

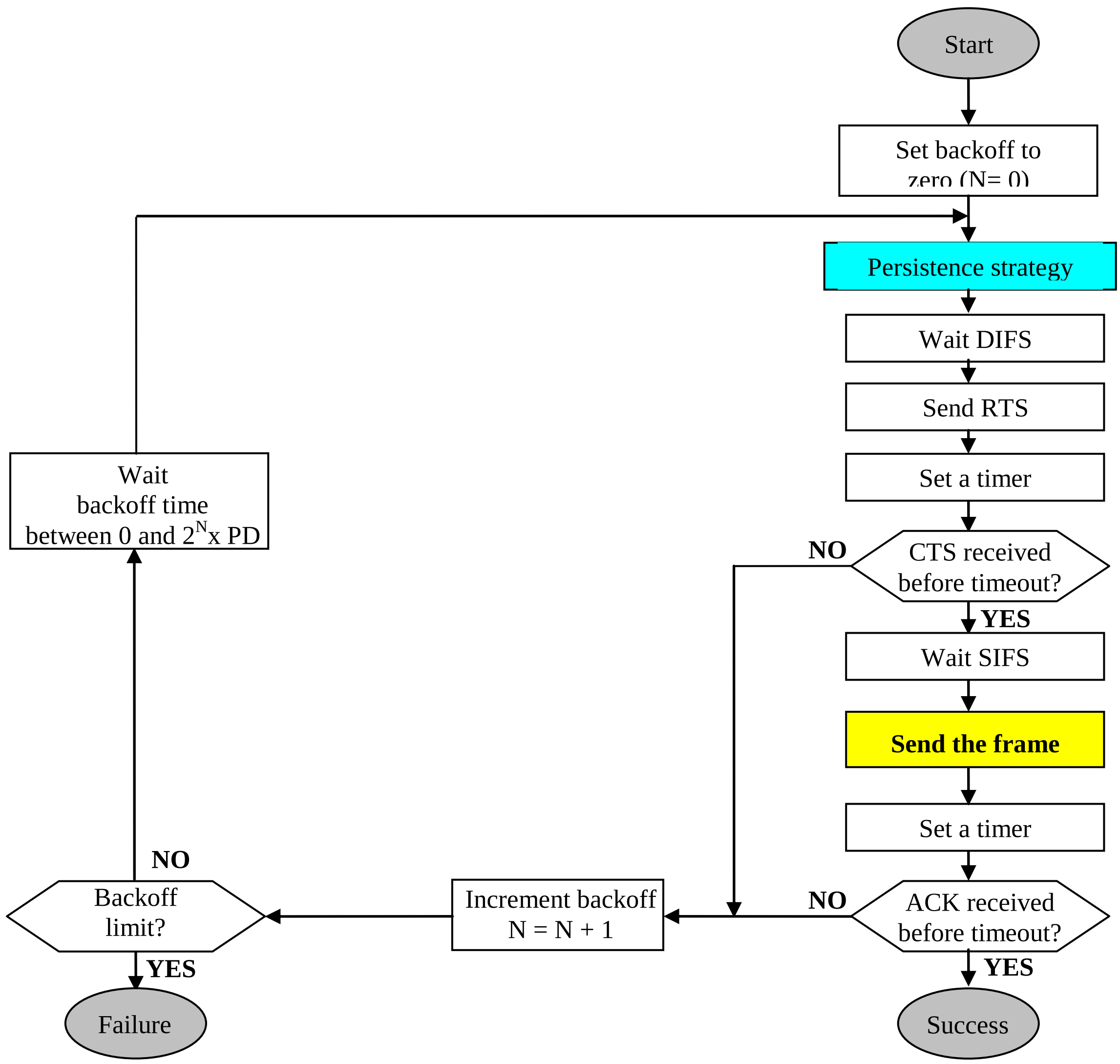
- The CSMA/CD is used in wired networks due to the ability that if a collision happen it will propagate to all stations.
- The CSMA/CD also requires that a station should be able to send a frame and receive collision signal at the same time which require more bandwidth.
- In wireless networks, stations of the same LAN are not necessarily in the same range. This problem is called the hidden terminal problem where a station A can never sense if a station B is sending a frame to a station C.



- The IEEE 802.11 standard (wireless) uses the CSMA/CA where the collision is avoided as much as possible.
- Before start sending a frame, the sender waits for some time DIFS (distributed interframe space) and then sends a RTS frame (request to send) to the receiver. Then the receiver replies with a CTS frame (clear to send) after a short time called SIFS (short interframe space).
- In order to avoid collision while receiving data, the source/destination station sends a NAV (network allocation vector) to all stations in its range. The NAV shows the time that other stations should stay idle before sensing the channel. So the stations freeze their timers until NAV time is expired.



- Next is a flowchart describing the CSMA/CA in IEEE802.11:

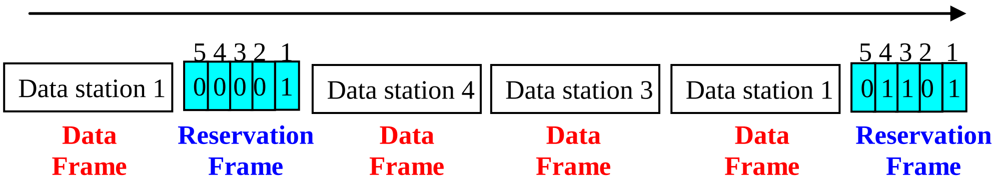


IV- Controlled Access Protocols [1][20]:

- In controlled access protocols, stations consult each other before sending/receiving data.
- A station cannot send a frame unless it has been authorized by other stations.

1- Reservation:

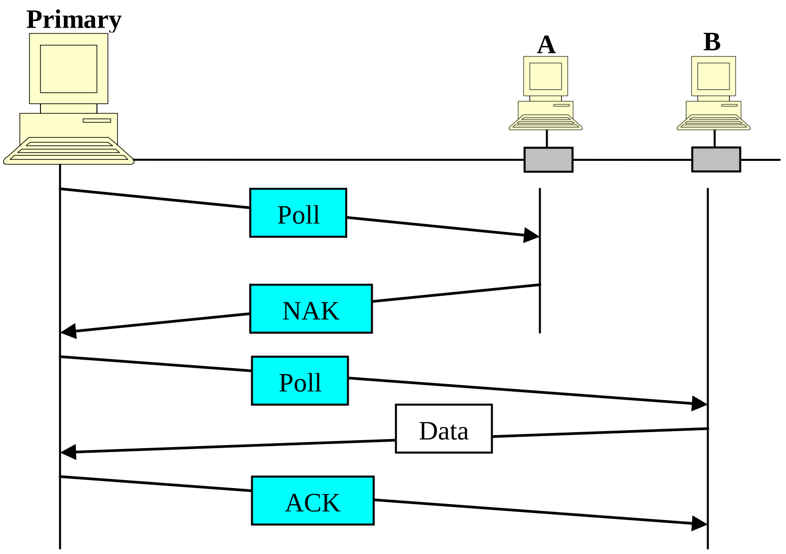
- In the reservation access method, a station needs to make a reservation before sending data.
- Usually, a reservation frame, divided into N slots, is used to make reservations for N stations. Each slot is 1 bit long: 0 for not reserved, 1 for reserved.



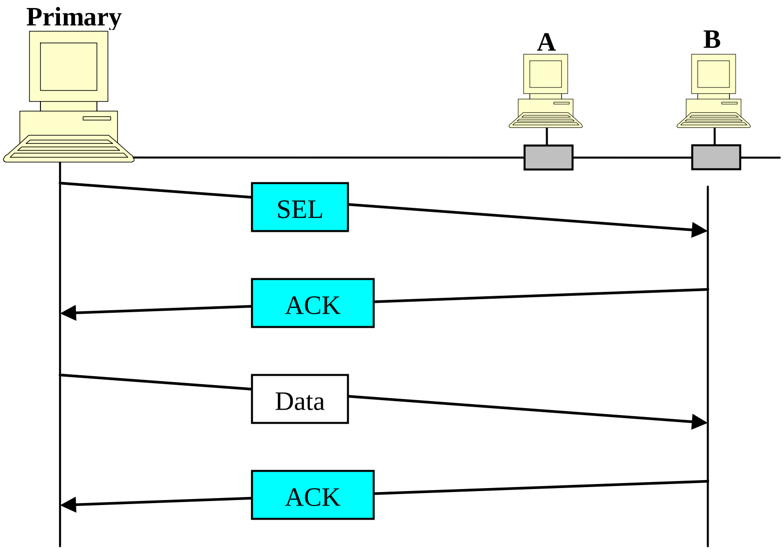
- In the above example, station 1 and 3 and 5 made reservations and sends their frames in order. Then only station 1 had data to be sent, so it made a reservation and sends its data.

2- Polling:

- It is used in topologies with primary and secondary stations.
- All data exchange must go through the primary station. So if two secondary stations need to communicate, the first one should send data to the primary, and then the primary forwards it to the second station.
- There are two modes in this protocol: polling and selecting.
- In poll mode, the primary station asks the secondary station if it has data to send. The secondary station replies either with data to send, or a NAK saying that it has nothing to send. The primary station relies with an ACK in case it receives data from the secondary station.



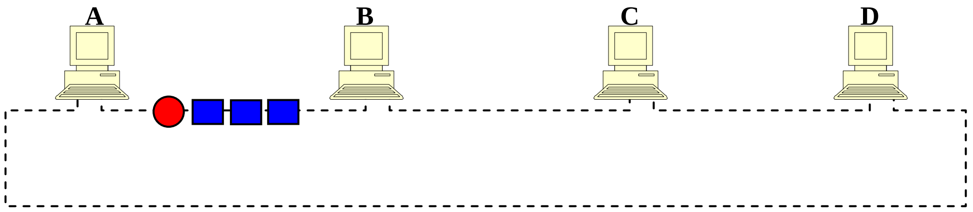
- In select mode, the primary station has some data to send to a secondary station. So, the primary sends a SEL frame to ask the secondary whether it's ready or not. The secondary replies with an ACK or NAK. In case the secondary is ready, the primary sends data and the secondary replies with an ACK.



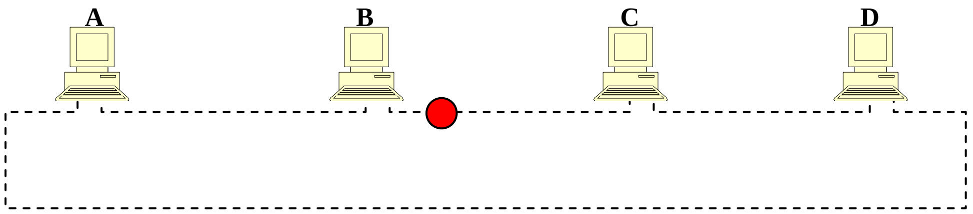
2- Token Passing:

- In token passing, a station is authorized to send data only when it receives a special frame called a token.
- Stations are organized in a ring. The token is passed from one station to another in a circular way.

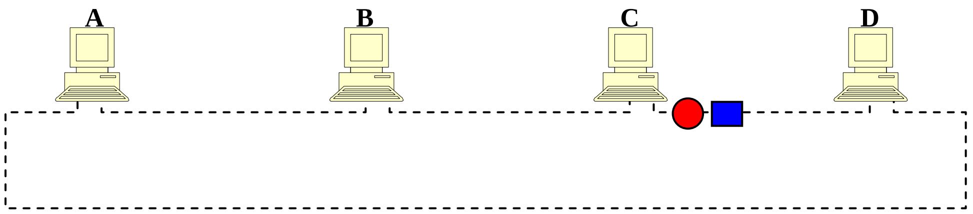
1- Station A sends three data frames and then releases the token



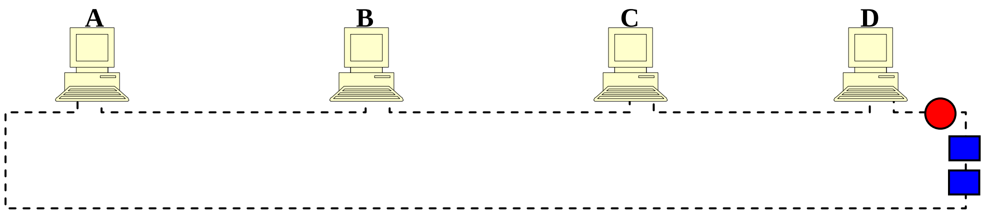
2- Station B has nothing to send, so it releases the token



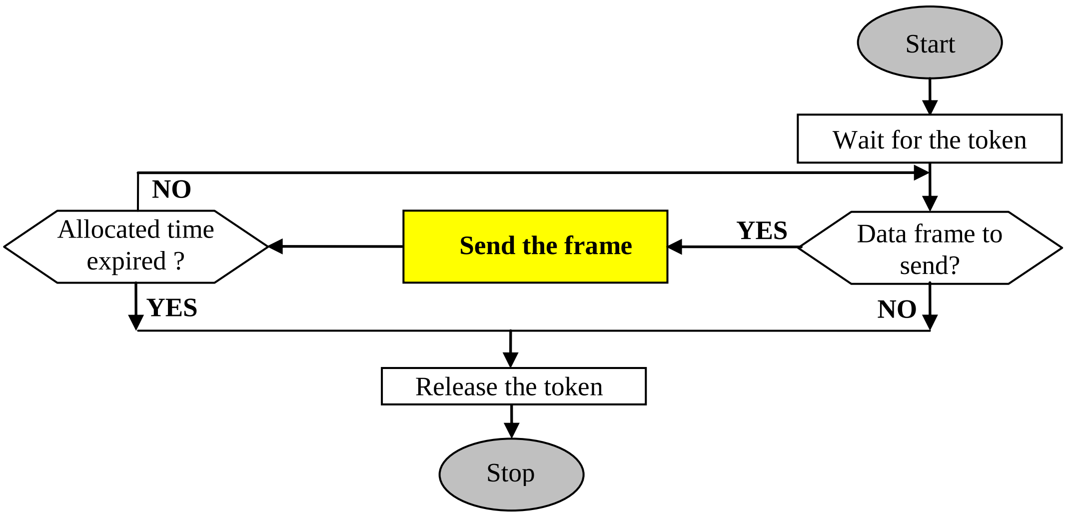
3- Station C sends one data frames and then releases the token



4- Station C sends 2 data frames and then releases the token



- Once a station gets hold of the token, it can send data as long as its allocated time is not expired.



V- Channelization [1] [14][16][21]:

- Unlike random access and controlled access method, some channelization methods allow multiple access to the shared link.

1- FDMA:

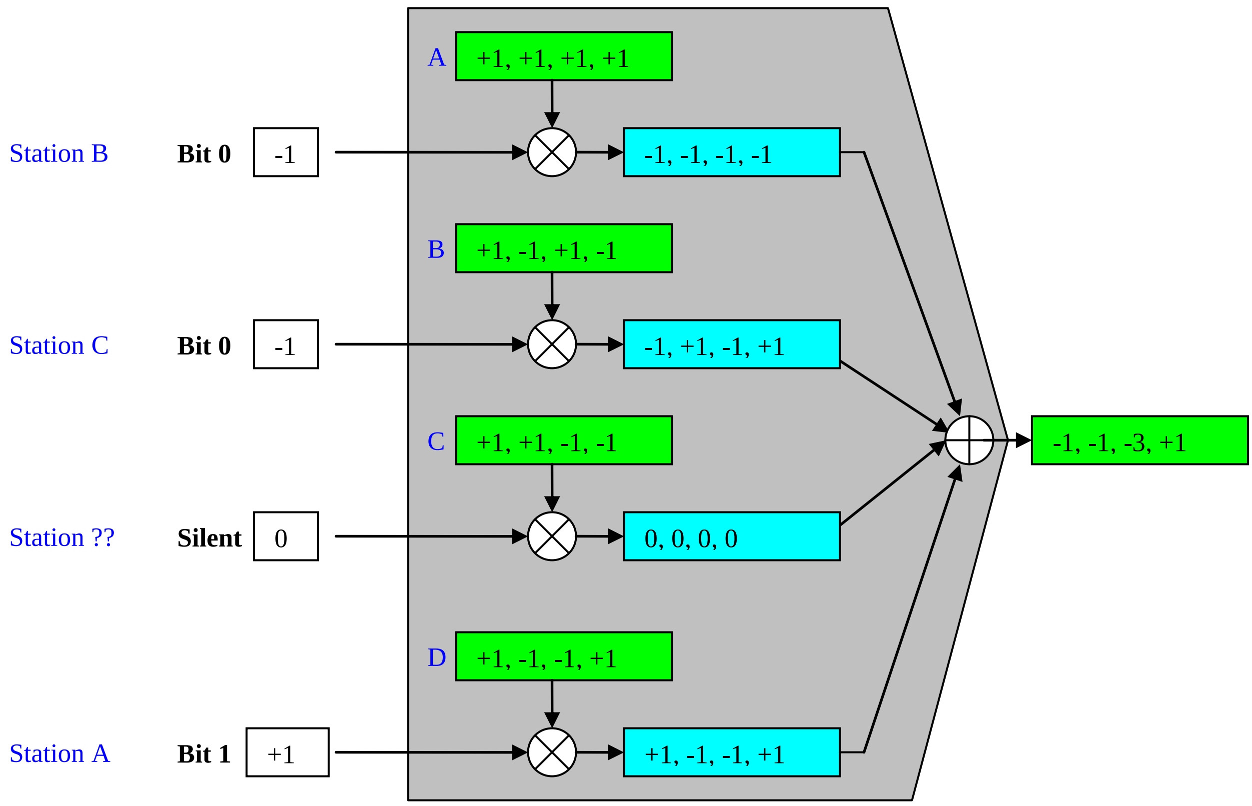
- In FDMA (frequency division multiple access), the available bandwidth is shared between all stations.
- Each band is reserved for a specific station.
- Each station uses its allocated band to send its data.
- FDMA in the data link layer uses FDM at the physical layer.

2- TDMA:

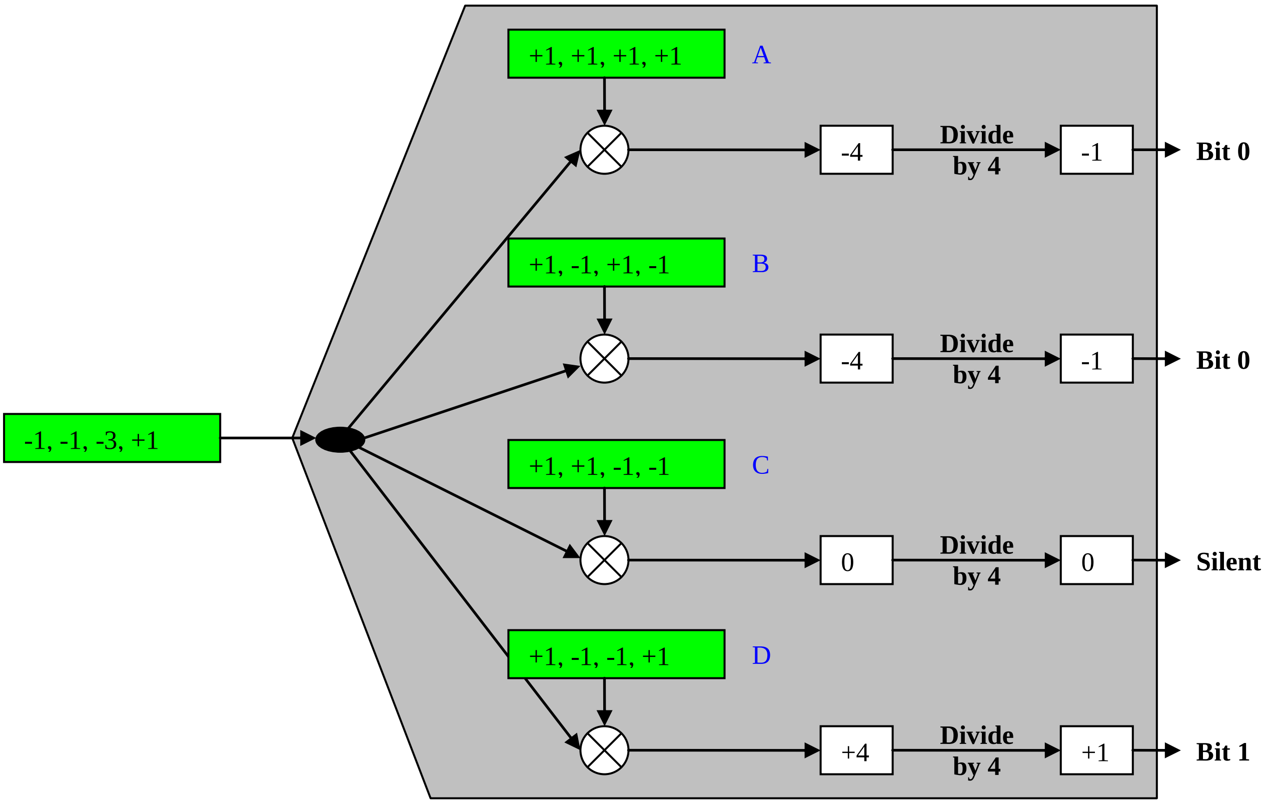
- In TDMA (time division multiple access), the entire bandwidth is allocated to one station at a time.
- Each station is allocated a time slot during which it can send data.
- TDMA in the data link layer uses TDM at the physical layer.

3- CDMA:

- In CDMA (code division multiple access) all stations can send data at the same time without the need to specify a band for each station.
- Each station is allocated a code called chips. Suppose we have 4 stations A, B, C, D that are respectively allocated the chips (+1, +1, +1, +1), (+1, -1, +1, -1), (+1, +1, -1, -1), (+1, -1, -1, +1).
- The chips are orthogonal vectors: the scalar product of each pair of chips is null:
  (+1, +1, +1, +1) x (+1, -1, +1, -1) = 1 - 1 + 1 – 1 = 0, …
- There is an encoding rule when a bit is needed to be send: 0 is encoded -1, 1 is encoded +1. If the station is silent, it sends code 0.
- The CDMA has a multiplexer that multiply the encoded bit of each sending station by the corresponding chip vector of the receiving station, then adds up all the results into one vector to be sent.



- The demultiplexer receives the sent code vector and multiplies it (scalar) by the chip vector of each receiving station, resulting in a d, $-d$, or 0, where d is the dimension of the chip vectors. This result is divided by d to get the code +1, -1, or 0, which will be decoded into bit 1, bit 0, or silent, respectively.



VI- Fast Ethernet and Gigabit Ethernet [1][21]:

1- Fast Ethernet

- Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled).
- IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:
  - ✓ Upgrade the data rate to 100 Mbps.
  - ✓ Make it compatible with Standard Ethernet.
  - ✓ Keep the same 48-bit address.
  - ✓ Keep the same frame format.
  - ✓ Keep the same minimum and maximum frame lengths.
- **Fast Ethernet implementations:**

Table *Summary ofFast Ethernet implementations*

Characteristics	*lOOBase-TX*	*lOOBase-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100m	100m	100m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

2- Gigabit Ethernet

- The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:
    - ✓ Upgrade the data rate to 1 Gbps.
    - ✓ Make it compatible with Standard or Fast Ethernet.
    - ✓ Use the same 48-bit address.
    - ✓ Use the same frame format.
    - ✓ Keep the same minimum and maximum frame lengths.
    - ✓ To support autonegotiation as defined in Fast Ethernet.
- **Gigabit Ethernet implementations:**

Table *Summary ofGigabit Ethernet implementations*

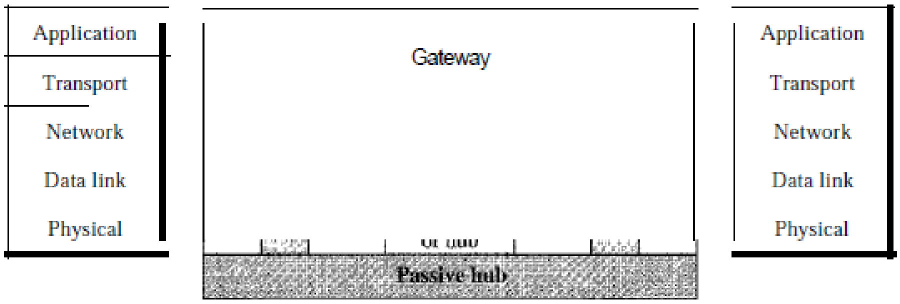
Characteristics	*lOOOBase-SX*	*lOOOBase-LX*	*lOOOBase-CX*	*lOOOBase-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550m	5000m	25m	100m
Block encoding	8B/lOB	*8B/lOB*	8B/lOB	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Connecting Devices

I- Connecting Devices [1][9][10]

- LANs do not normally operate in isolation. They are connected to one another or to the Internet. To connect LANs, or segments ofLANs, we use connecting devices.
- Connectingdevices can operate in different layers of the Internet model.
- Connecting devices divided into five different categories based on the layer in which they operate in a network.

Five categories ofconnecting devices



- The five categories contain devices which can be defined as:
  - ✓ Those which operate below the physical layer such as a **passive hub**.
  - ✓ Those which operate at the physical layer (**a repeater or an active hub**).
  - ✓ Those which operate at the physical and data link layers (a **bridge** or a **two-layer switch**).
  - ✓ Those which operate at the physical, data link, and network layers (a **router** or a **three-layer switch**).
  - ✓ Those which can operate at all five layers (a **gateway**).

1- Passive Hubs

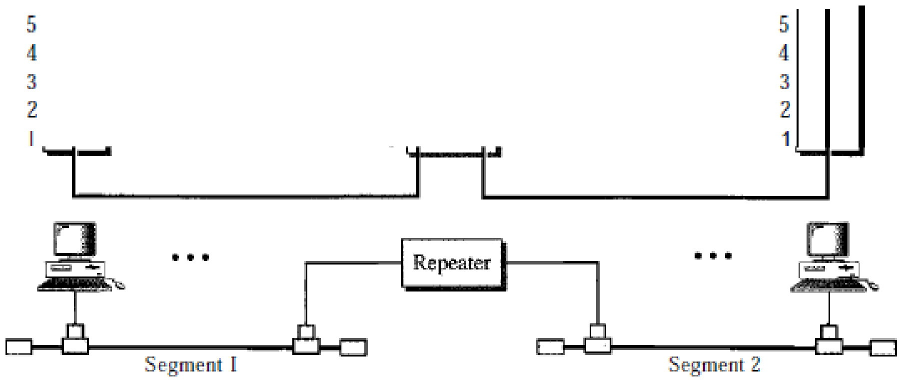
- A passive hub is just a connector. It connects the wires coming from different branches.
- In a star-topology Ethernet LAN, a passive hub is just a point where the signals comingfrom different stations collide; the hub is the collision point.
- This type of a hub is partof the media; its location in the Internet model is below the physical layer.

2- Repeaters

- A repeater is a device that operates only in the physical layer.

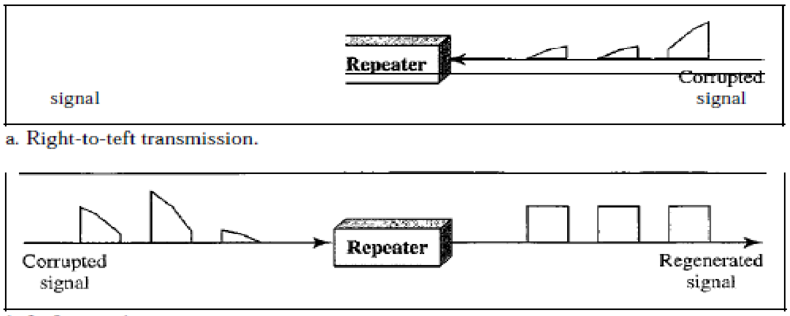
- Signals that carry information within a network can travel a fixed distance before attenuation endangers theintegrity of the data.
- A repeater receives a signal and, before it becomes too weak orcorrupted, regenerates the original bit pattern.
- The repeater then sends the refreshedsignal. A repeater can extend the physical length of a LAN.

A repeater connecting two segments ofa LAN



- A repeater does not actually connect two LANs; **it connects two segments of the same LAN**. The segments connected are still part of one single LAN. A repeater is not a device that can connect two LANs of different protocols.
- A repeater can overcome the 10Base5 Ethernet length restriction. In this standard, the length of the cable is limited to 500 m. To extend this length, we divide the cable into segments and install repeaters between segments. Note that the whole network is still considered one LAN, but the portions of the network separated by repeaters are called segments. The repeater acts as a two-port node, but operates only in the physical layer. When it receives a frame from any of the ports, it regenerates and forwards it to the other port.
- **A repeater forwards every frame; it has no filtering capability.**
- **A repeater is a regenerator, not an amplifier.**

Function ofa repeater



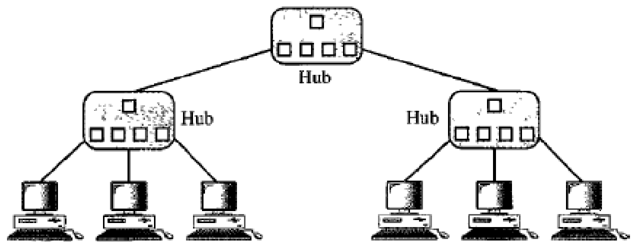
a. Right-to-teft transmission.

b. Left-to-right transmission.

3- Active Hubs

- An active hub is actually a multipart repeater.
- It is normally used to create connections between stations in a physical star topology.
- We have seen examples of hubs in some Ethernet implementations (lOBase-T, for example).
- However, hubs can also be used to create multiple levels of hierarchy.
- The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).

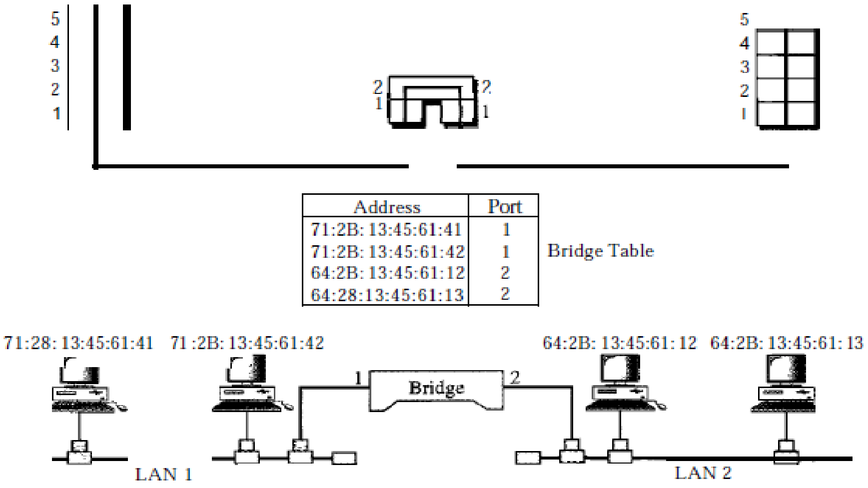
A hierarchy ofhubs



4- Bridges

- A bridge operates in both the physical and the data link layer.
- As a physical layer device, it regenerates the signal it receives.
- As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.
- **Filtering:**One may ask, What is the difference in functionality between a bridge and a repeater?
  - ✓ A bridge has filtering capability. It can check the destination address of a frame anddecide if the frame should be forwarded or dropped. If the frame is to be forwarded, thedecision must specify the port. A bridge has a table that maps addresses to ports.
  - ✓ **A bridge has a table used in filtering decisions.**
- A bridge connecting two LANs

A bridge connecting two LANs



- A bridge does not change the physical addresses contained in the frame.

4- Two-Layer Switches

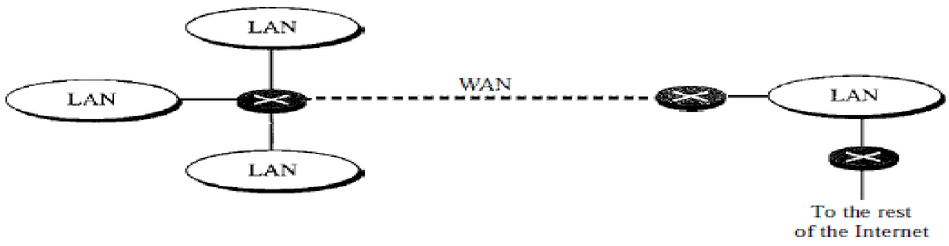
- When we use the term switch, we must be careful because a switch can mean two different things. We must clarify the term by adding the level at which the device operates.
- We can have a two-layer switch or a three-layer switch.
- A three-layer switch is used atthe network layer; it is a kind of router.
- The two-layer switch performs at the physicaland data link layers.
- A two-layer switch is a bridge, a bridge with many ports and a design that allowsbetter (faster) performance.
- A bridge with a few ports can connect a few LANstogether.
- A bridge with many ports may be able to allocate a unique port to each station,with each station on its own independent entity. This means no competing traffic (nocollision, as we saw in Ethernet).
- A two-layer switch, as a bridge does, makes a filtering decision based on the MAC address of the frame it received. However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing. It can have a switching factor that forwards the frames faster. Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.

5- Routers

- A router is a three-layer device that routes packets based on their logical addresses(host-to-host addressing).

- A router normally connects LANs and WANs in the Internetand has a routing table that is used for making decisions about the route.
- The routingtables are normally dynamic and are updated using routing protocols.

Routers connecting independent LANs and WANs



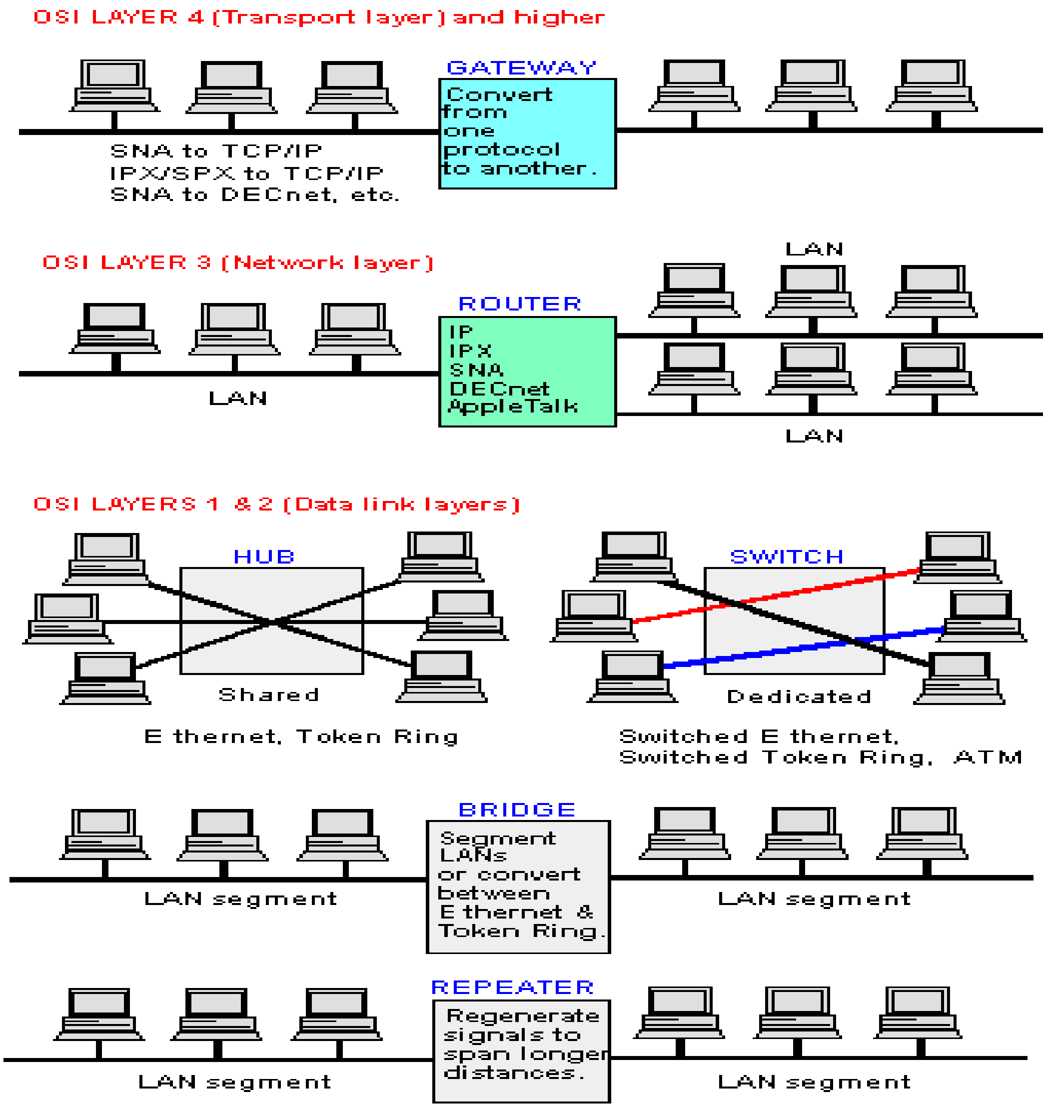
5- Three-Layer Switches

- A three-layer switch is a router, but a faster and more sophisticated.
- The switching fabricin a three-layer switch allows faster table lookup and forwarding.

6- Gateway

- Although some textbooks use the terms gateway and router interchangeably, most of theliterature distinguishes between the two.
- A gateway is normally a computer that operatesin all five layers of the Internet or seven layers of OSI model. A gateway takes anapplication message, reads it, and interprets it. This means that it can be used as aconnecting device between two internetworks that use different models. For example,a network designed to use the OSI model can be connected to another network usingthe Internet model. The gateway connecting the two systems can take a frame asit arrives from the first system, move it up to the OSI application layer, and remove themessage.
- Gateways can provide security. The gateway is used to filter unwanted application-layer messages.

II- Connecting Devices Vs. OSI layers [1][7] [8][10]


OSI LAYER 4 (Transport layer) and higher
GATEWAY
Convert from one protocol to another.
SNA to TCP/IP
IPX/SPX to TCP/IP
SNA to DECnet, etc.
OSI LAYER 3 (Network layer)
ROUTER
IP
IPX
SNA
DECnet
AppleTalk
LAN
LAN
LAN
OSI LAYERS 1 & 2 (Data link layers)
HUB
Shared
Ethernet, Token Ring
SWITCH
Dedicated
Switched Ethernet,
Switched Token Ring, ATM
BRIDGE
Segment LANs or convert between Ethernet & Token Ring.
LAN segment
LAN segment
REPEATER
Regenerate signals to span longer distances.
LAN segment
LAN segment

Chapter 4. TCP/IP protocol

Network Layer: Addressing

- Global logical addresses are logical: they are easily organized, controlled and modified as we need.
- Addressing in network layer is essential for routing.
- We need to uniquely identify devices on the Internet to allow global communication.
- It is analogous to the telephone system where each phone in the world is associated to a unique number[1].

I- Addressing in Internet[1]:

- The internet address is called the IP address.
- An IP address is a 32-bit address that uniquely and universally defines a connection of a host or a router in the internet.
- An address can never be shared by two devices or hosts. However, a host, especially a router can have more than one address.

1- Notation[1][9]:

- The Internet address has two notations: The dotted-decimal notation and the binary notation.
- In the binary notation, a 32-bit string is displayed in 4-byte format:

  01110101 10010101 00011101 11101010
- In the dotted-decimal, the address is written in decimal for better readability.
- In this format, 4 decimals between 0 and 255 are separated by a dot ".":

  128.11.3.31

2- Sections[1][7]:

- The IP address is divided into two sections: The Net ID and the Host ID.
- The Net ID represents the address of the network that a host belongs to.
- The Host ID represents the local address of a host inside a network.
- As an analogy, if we look at the phone number 049-96-40-51 which is in 4-decimal format, we can consider that 049-96 is the netid of the wilaya of Adrar, where 40-51 is the host id of Salim who lives in Adrar. We can also consider that 049-96-40 is the netid of Ouled Brahim, and 51 is still the host id of Salim who lives in Adrar, but specifically in Ouled Brahim.

3- Classification [1][17]:

- IP addresses are classified into 5 classes: A, B, C, D, and E.

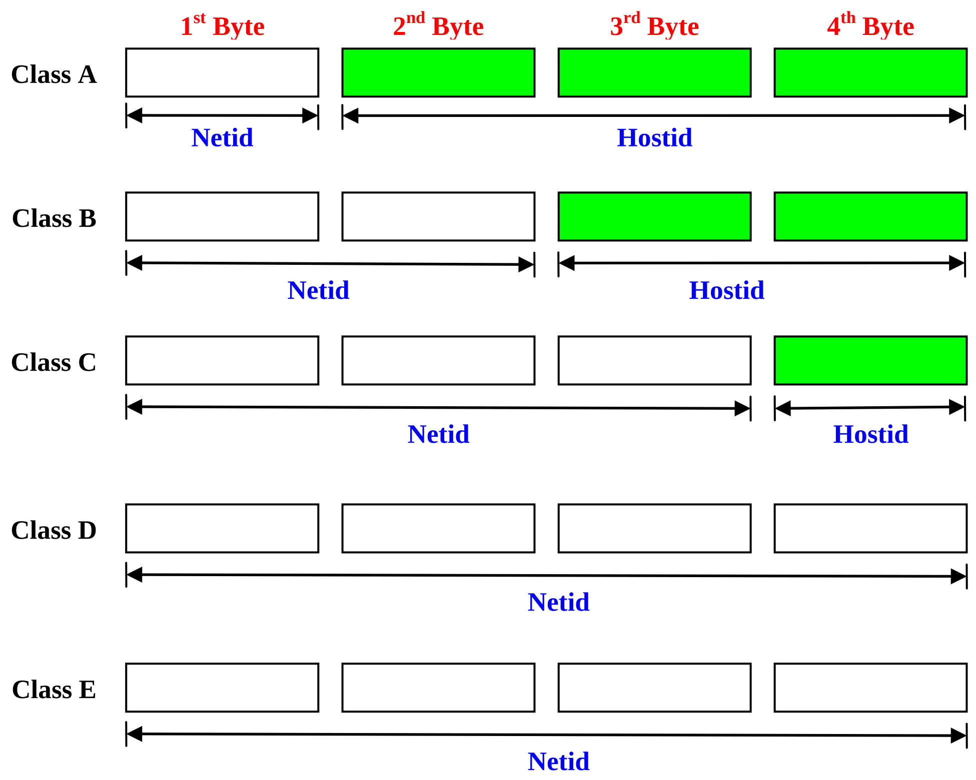
- Classification is based on the value of the first byte of the address.

	1st Byte	2nd Byte	3rd Byte	4th Byte
Class A	**0 to 127**			
Class B	**128 to 191**			
Class C	**192 to 223**			
Class D	**224 to 239**			
Class E	**240 to 255**			

- The binary notation shows an easier way to distinguish classes:

	1st Byte	2nd Byte	3rd Byte	4th Byte
Class A	**0…………….**			
Class B	**10...………….**			
Class C	**110………….**			
Class D	**1110………..**			
Class E	**1111………..**			

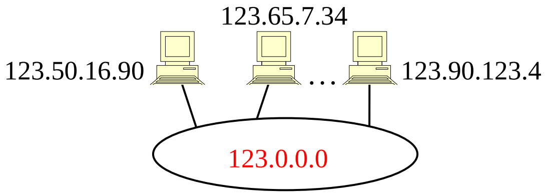
- IP address classes are also distinguished by the size of the netid and the hostid they use:



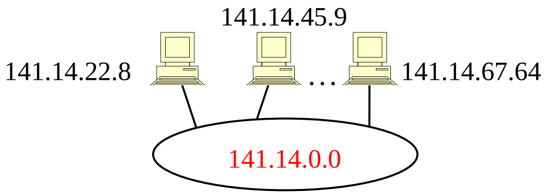
- Class A organizes the internetwork into 128 networks (netid) with 2^{24} = 16,777,216 possible hosts inside each network. Class A was designed for large organizations with a large number of hosts or routers. Yet, 16,777,216 hosts is larger than most organizations need.
- Class B organizes the internetwork into 64×2^8 = 16384 networks (netid) with 2^{16} = 65536 possible hosts inside each network. Class B was designed for midsize organizations, but still many addresses are wasted inside each network.
- Class C organizes the internetwork into 32×2^{16} = 2,097,152 networks (netid) with 2^8 = 256 possible hosts inside each network. Class C was designed for regular organizations, that happens to need more than 256 hosts inside each network. Yet, it is possible for an organization to get attributed two or more blocks of networks to fit its needs.
- IP addresses in classes A, B, and C are unicast addresses, where a host is able to send data to only a unique host.
- Classes D and E organizes the internetwork into networks only (net id). There is no specification of a host. IP addresses in Class D are multicast addresses, where a host can use only one destination address to broadcast a message to a group of hosts that is characterized by a class D address. Of course, a multicast address is used only as a destination address.
- Class E addresses are reserved for future use.

4- Network Address [1][18]:

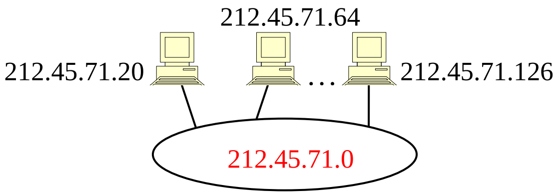
- The network address is an address that is assigned to an entire network, not a host.
- A network address is an address with all hostid bytes equal to 0.
- The network address defines the network to the rest of the world. The router can route a packet based on the network address.



Class A

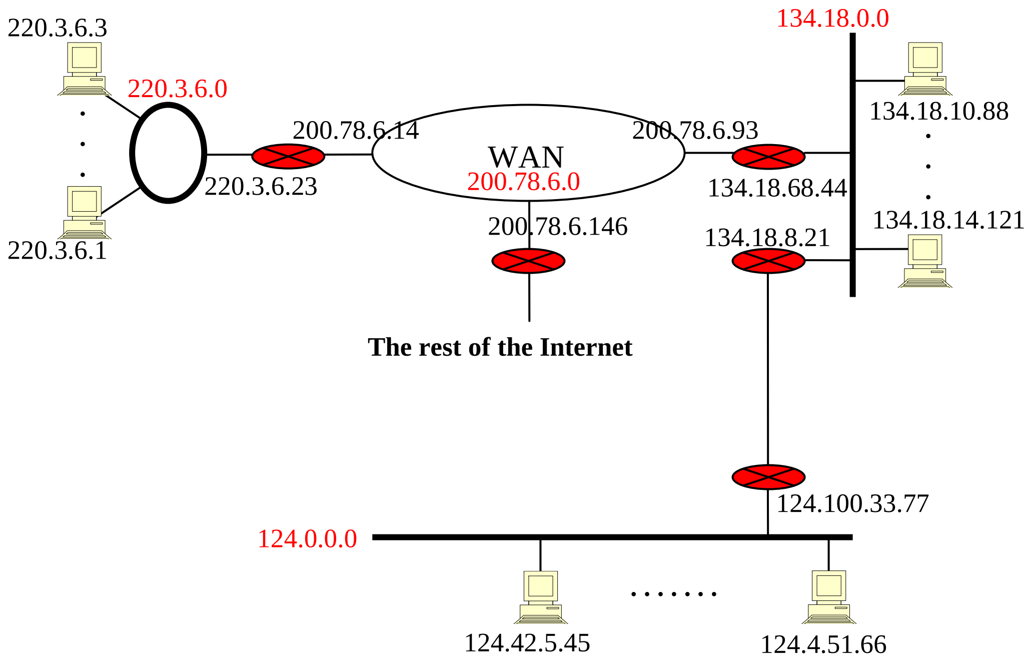


Class B



Class C

- Here is an example of internetwork with different types of addresses:



5- The Mask [17][18]:

- Although the size of the netid and the hosted is predetermined in classful addressing, we can use a mask that extracts the network address from an IP address.
- The Mask is also a 32-bit string, which is ANDed with the IP address to get the network address.

Class	Default Mask In Binary	Default Mask In Dotted-Decimal	Default Mask Using Slash
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- In slash notation, the used number corresponds to the number of 1's in the mask.
- Example: What is the network address corresponding to 100.50.150.200?
- Answer: Since the first byte equals to 100 then this address is of class A.
-
```
    IP address     01100100 00110010 1001011011001000 AND
    Mask           11111111 00000000 00000000 00000000
    Net. Address   01100100 00000000 00000000 00000000
```

  So, the network address is 100.0.0.0

6- Classless Addressing [1][7]:

- The classification of addresses led to addresses depletion despite the large space of 2^{32} addresses.
- The depletion is due to the wasting of addresses.
- In classless addressing, there is no need to classify addresses.
- Each organization is granted addresses quite as much as it needs.
- There are some restrictions about the granted addresses:

  1- they need to be contiguous.

  2- they need to be power of 2 (2, 4, 8, 16, …).

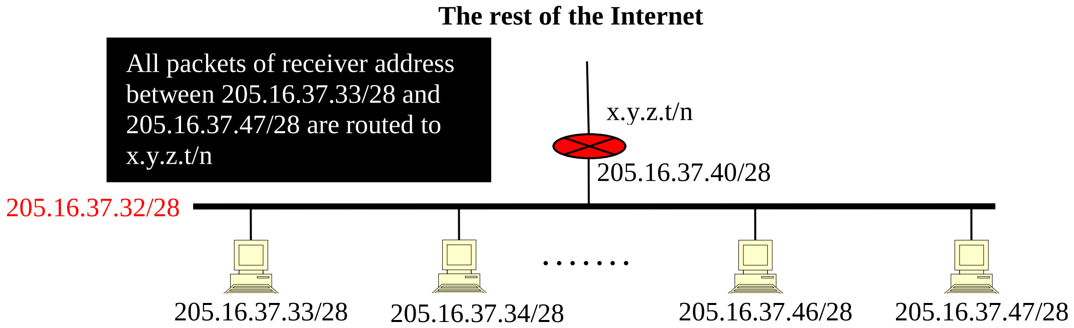
  3- the first address should have a number of rightmost 0's as much as $\log_2$(the number of addresses).
- The first address of the block is usually considered as the network address.
- The mask of a network in classless addressing is composed of 32 bits where the leftmost (32 – m) bits are all 1's and the rest of n bits is all 0's, and m is $\log_2$(the number of addresses).
- Example: An organization is granted 16 addresses as follows:

```
205.16.37.32       11001101 00010000 0010010100100000
205.16.37.33       11001101 00010000 0010010100100001
...                ...
205.16.37.47       11001101 00010000 00100101 00101111

The mask
255.255.255.240    11111111 11111111 11111111 11110000 (/28)
```

- We saw that in classful addressing it is easy to get block of addresses from the network address. In classless addressing we need to use the slash notation which corresponds to the mask of the network: `205.16.37.32/28`
- The first address is gotten by ANDing the given address with the mask. The last address is gotten by ORing the given address with the 1's complement of the mask.
- Example: the address `205.16.37.45/28` means that this address IP belongs to a network:

```
IP address      11001101 00010000 00100101 00100001      AND
Mask            11111111 11111111 11111111 11110000
First Address   11001101 00010000 00100101 00100000  (net. Add)

IP address      11001101 00010000 00100101 00100001      OR
Mask's Comp.    00000000 00000000 00000000 00001111
Last Address    11001101 00010000 00100101 00101111
```

- So, in classless addressing each host is identified by the notation x.y.z.t/n where x.y.z.t is the IP address and /n is the slash notation of the network mask. The IP address by itself is not enough, since routing is based on the network address which is not obvious in classless addressing.



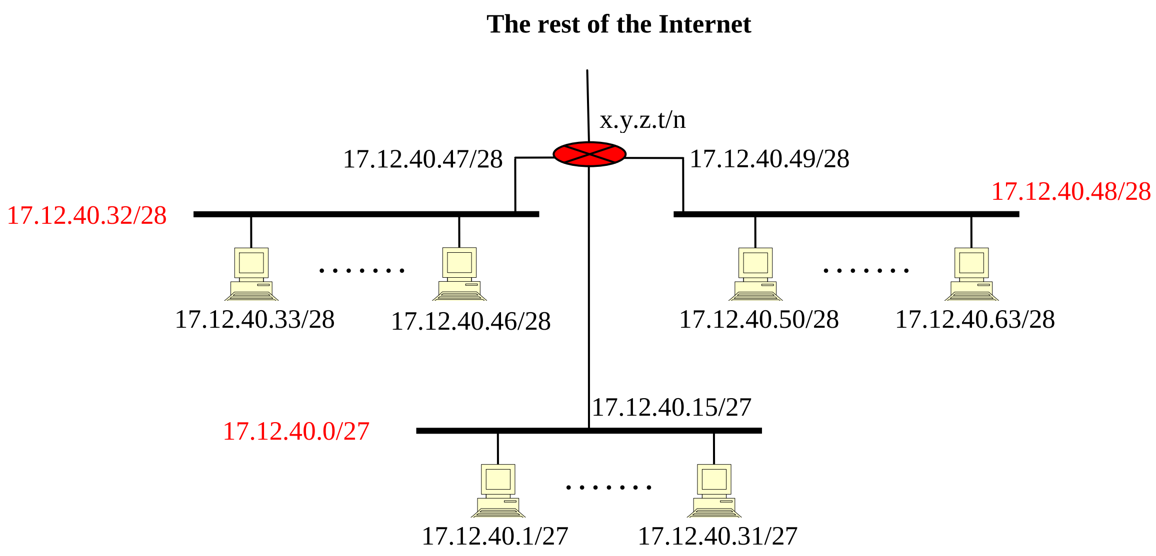
7- Subnetting [1][22]:

- When an organization is granted a large block of addresses, it can organize them into clusters of subnets.
- The outside networks always see the organization as one network; but internally there are another hierarchy of networks.
- Let's say for instance that an organization is granted the block 17.12.40.0/26. This block contains 64 addresses (from 17.12.40.0/26 to 17.12.40.63/26). The organizations like to create a subnet for each of its 3 offices: 32 hosts for one office and 16 hosts for each of the other offices. Of course the organization needs to acquire an internal router for these subnets.
- The organization mask is /26 which is know to the rest of the world. Yet, the internal subnets should have their specific internal masks: /27, /28, and /28 for office 1, 2 and 3 respectively:

`Subnet 1 (32 addresses)`

```
        First Address   17.12.40.0
        Last Address    17.12.40.31
        Mask            255.255.255.224      (224 = (11100000)2)
    Subnet 2 (16 addresses)
        First Address   17.12.40.32
        Last Address    17.12.40.47
        Mask            255.255.255.240      (240 = (11110000)2)
    Subnet 3 (16 addresses)
        First Address   17.12.40.48
        Last Address    17.12.40.63
        Mask            255.255.255.240      (240 = (11110000)2)
```

- So the internal router alters the packets going in or out of the network by changing the mask. For instance, if host `17.12.40.31/27` issues a packet outside the network, then the router replaces the sender's address to `17.12.40.31/26`. Also, if a packet is received with the address of `17.12.40.50/26` then the router replaces the receiver's address by `17.12.40.50/28` and routes it to the third subnet.



8- Address Allocation[1][17][18]:

- The ultimate responsibility of address allocation is given to a global authority called theInternet Corporation for Assigned Names and Addresses (ICANN).

- However, ICANNdoes not normally allocate addresses to individual organizations. It assigns a large blockof addresses to an Internet Service Provider (ISP). Each ISP, in turn, divides its assigned block into smaller subblocksand grants the subblocks to its customers.
- The structure of classless addressing does not restrict the number of hierarchical levels.
- A national ISP can divide a granted large block into smaller blocksand assign each of them to a regional ISP. A regional ISP can divide the block receivedfrom the national ISP into smaller blocks and assign each one to a local ISP. A local ISPcan divide the block received from the regional ISP into smaller blocks and assign eachone to a different organization. Finally, an organization can divide the received blockand make several subnets out of it.
- An ISP receives one large blockto be distributed to its Internet users. This is called address aggregation: many blocks of addresses are aggregated in one block and granted to one ISP.
- Example:An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISPneeds to distribute these addresses to three groups of customers as follows:

  a. The first group has 64 customers; each needs 256 addresses.

  b. The second group has 128 customers; each needs 128 addresses.

  c. The third group has 128 customers; each needs 64 addresses.

  Design the subblocks and find out how many addresses are still available after these allocations.
- Solution:

Group 1:

For this group, each customer needs 256 addresses, so 8 bits are reserved for hostid and 24 bits for netid. Then:

1^{st} Customer: 190.100.0.0/24to190.100.0.255/24

2^{nd}Customer: 190.100.1.0/24to190.100.1.255/24

…

64^{th}Customer: 190.100.63.0/24 to190.100.63.255/24

Total =64 x 256 =16,384 addresses

Group2:

For this group, each customer needs 128 addresses, so 7 bits areneeded to define each host and 25 bits for each net. Then:

1^{st}Customer: 190.100.64.0/25to190.100.64.127/25

2^{nd}Customer: 190.100.64.128/25to190.100.64.255/25

…

128^{th}Customer: 190.100.127.128/25 to190.100.127.255/25

Total =128 x 128 = 16,384 addresses

Group3:

For this group, each customer needs 64 addresses, so 6 bits are needed for each hostid and 26 bits for each netid. So, the addresses are:

1st Customer: 190.100.128.0/26to190.100.128.63/26

2nd Customer: 190.100.128.64/26to190.100.128.127/26

3rd Customer: 190.100.128.128/26to190.100.128.191/26

4th Customer: 190.100.128.192/26to190.100.128.255/26

…

128th Customer: 190.100.159.192/26 to190.100.159.255/26

Total =128 x 64 =8192 addresses

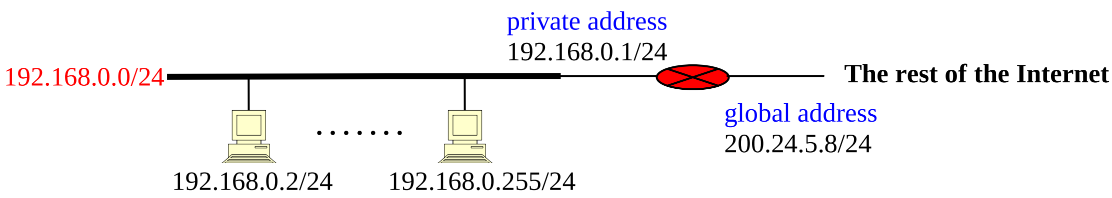
- Number of granted addresses to the ISP: 65,536
- Number of allocated addresses by the ISP: 16,384 + 16,384 + 8,192 = 40,960
- Number of available addresses: 24,576

9- Network Address Translation (NAT) [1][17][18]:

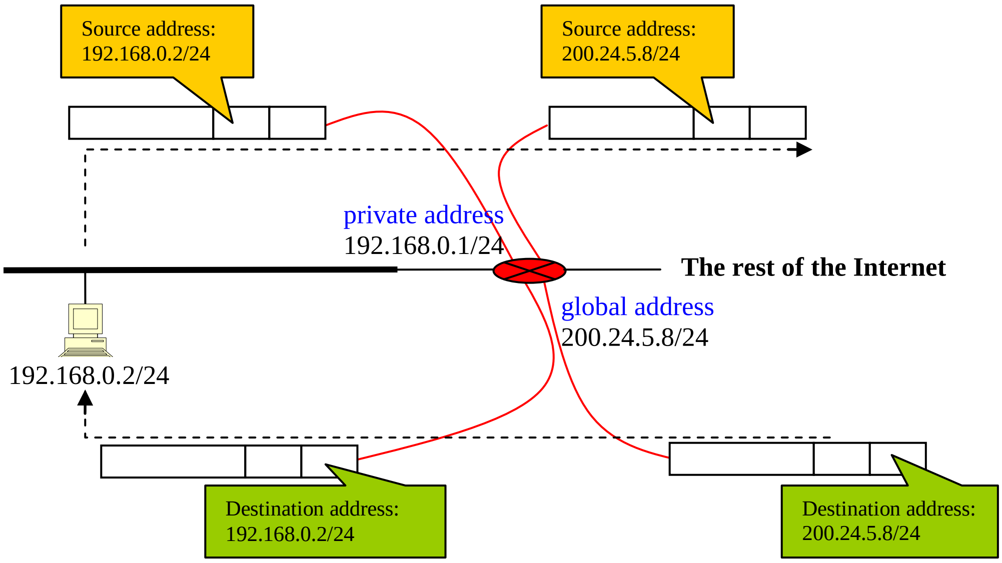
- Home users and small businesses can be connected by an ADSL line or cable modem, but many are not happy with one address; many have created small networks with several hosts and needan IP address for each host.
- To separate the addresses used inside the home or business and the ones used forthe Internet, the Internet authorities have reserved three sets of addresses as privateaddresses:

Range		Total
10.0.0.0	to 10.255.255.255	2^{24}
172.16.0.0	to 172.31.255.255	2^{20}
192.168.0.0	to 192.168.255.255	2^{16}

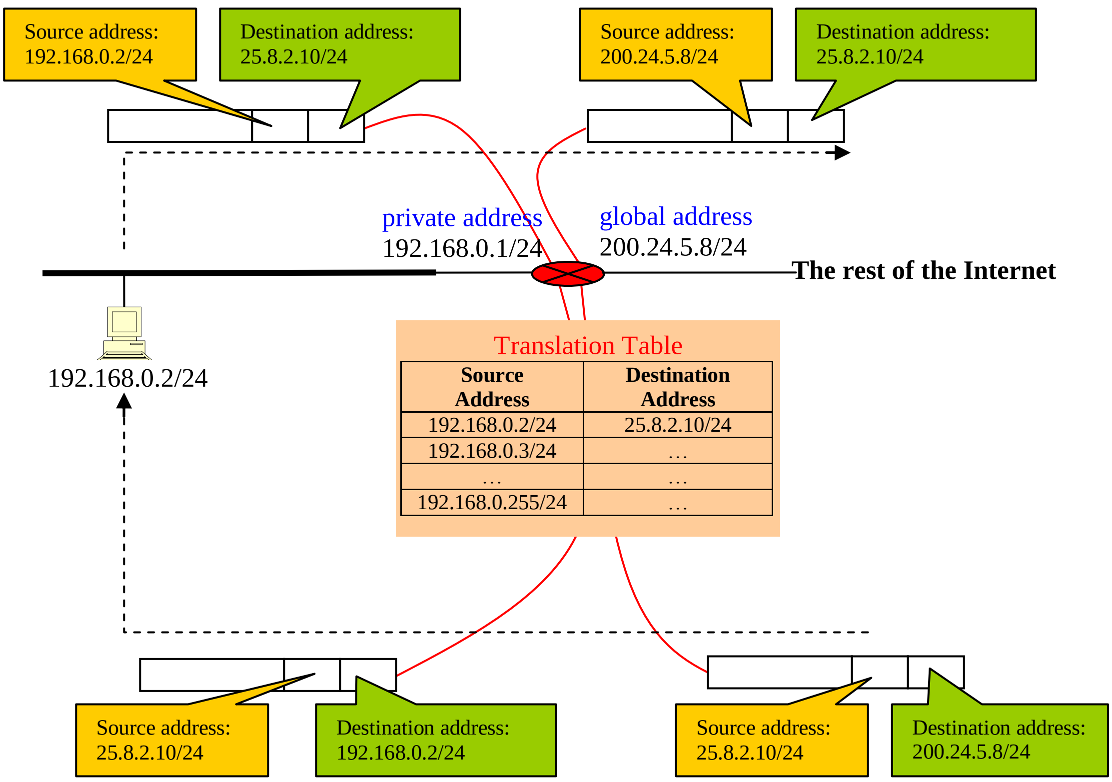
- Any organization can use an address out of this set without permission from theInternet authorities. Everyone knows that these reserved addresses are for private networks.
- These are unique inside the organization, but they are not unique globally. Norouter (except NAT router) will forward a packet that has one of these addresses as the destination address.
- The NAT router thatconnects the private network to the global address uses one private address and one globaladdress. The private network is transparent to the rest of the Internet; the rest of theInternet sees only the NAT router with the global address.



- All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.
- All incoming packets also pass through the NAT router, which replaces the destination addressin the packet (the NAT router global address) with the host private address.



- The replacement of source addresses at the NAT router is straight forward. However, it is not obvious to replace destination addresses in incoming packets. There are 3 proposed solutions:
- The first solution consists of using one IP address for the entire organization. The NAT router maintains a translation table with two columnsin order to save the source address (private) and the destination address(global) of the outgoing packet. When the receiver replies back, the NAT router looks up at the table and replaces the destination address (NAT global address) with the one associated to the receiver's address.



- This strategy has two major disadvantages: 1- Only one host of the organization site can connect to a specific host outside the site. 2- Communication is initiated only by a host inside the site; an internal host can access a web server (http) outside the site, but the organization cannot implement a web server on one of its hosts.
- In order to overcome the first disadvantage, a pool of global addresses is used to identify the NAT router. In this case, multiple hosts can connect to one specific location as much as the global addresses allocated to the NAT router.
- For instance, let's say that a NAT router is associated 4 global addresses: 200.24.5.8/24, 200.24.5.9/24, 200.24.5.10/24, and 200.24.5.11/24. In this case, 4 different hosts inside the private network can connect to the same location (google.com):
- Example of a translation table using a pool of NAT addresses:

Source Address	Destination Address	Used NAT Address
192.168.0.2/24	25.8.2.10/24	200.24.5.8/24
192.168.0.3/24	25.8.2.10/24	200.24.5.9/24
192.168.0.4/24	25.8.2.10/24	200.24.5.10/24
192.168.0.5/24	25.8.2.10/24	200.24.5.11/24
…	…	…

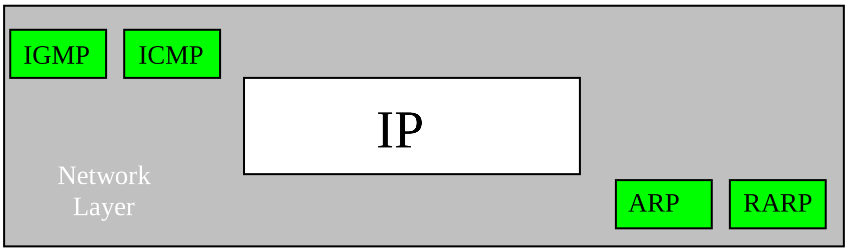
- In this strategy, an internal host is allowed only one connection (at a time) outside the site (htpp, ftp, …).
- The third solution uses port numbers to identify incoming packets. Port numbers are used in the transport layer to distinguish different processes running on a machine. Different servers have also different port numbers (web server port = 80, …).
- So in this strategy, an internal host is considered as process of the NAT router, and then, each internal host is associated a separate port number.
- Example of a translation table using port numbers:

Private Address	**Private Port #**	**External Address**	**External Port #**	**Transport Protocol**
192.168.0.2/24	1400	25.8.2.10/24	80 (http)	UDP
192.168.0.2/24	1401	25.8.2.10/24	21 (ftp)	TCP
192.168.0.3/24	1402	25.8.2.10/24	80 (http)	UDP
…	…	…	…	…

-

Network Layer: Protocols - ARP

- In the Internet network model, there are five network layer protocols: ARP, RARP, IP, ICMP, IGMP.
- The main protocol is IP, which is responsible for host-to-host delivery. But IP needs other protocols in order to accomplish its task.
- The current version of IP is called IPv4. There is a new version called IPv6 which came to extend the existing IPv4 in terms of addresses' space and network services.
- ARP is needed to find the physical MAC addressgiven an IP address. RARP, or Reverse ARP does exactly the opposite job.
- ICMP is needed to handle unusual situations like errors.
- Since IP is designed for unicast transmissions, IGMP is needed to handle multicasting transmissions [1][11].



I- ARP (Address Resolution Protocol):

- The internet address is universal; it does not depend on the type of the physical network (Ethernet, Token ring, Wireless, …).
- The network layer is responsible for packet delivery from host-to-hostbased on an IP address. Yet, this delivery is based on multiple hop-to-hop delivery that happens at the data link layer based on a MAC address.
- In order to be able to deliver a packet to a host or a router, we need to have a protocol that maps an IP address to its corresponding MAC address.
- There are two types of mapping in ARP: Static mapping and dynamic mapping [1].

1- Static Mapping [1][24]:

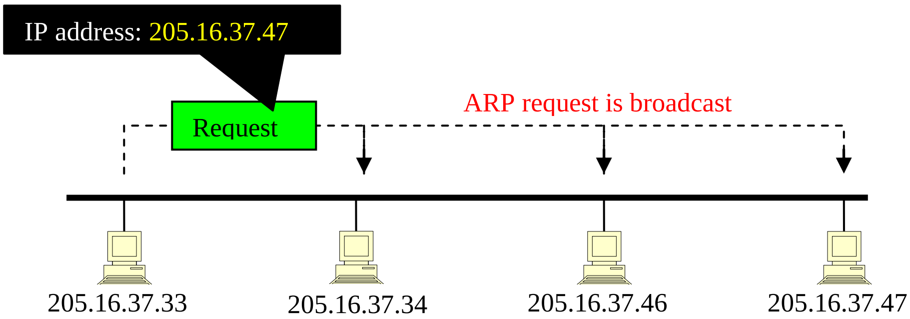
- In static mapping, each machine in the physical network stores a table that associates the IP address of each machine of the network with its corresponding MAC address.

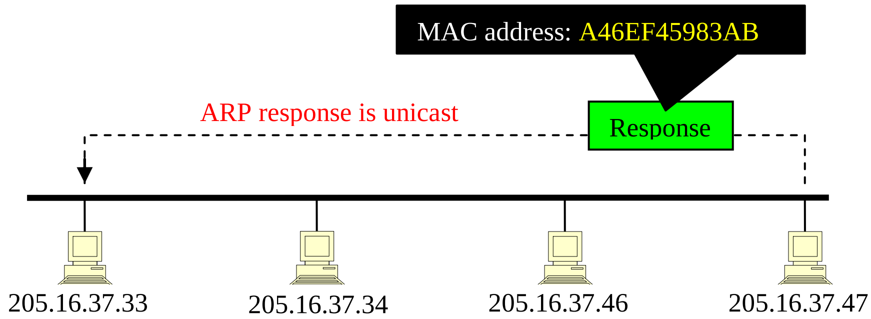
IP Address	MAC Address
141.23.56.1	A46EF45983AB
…	…

- Since there is no guarantee that the machine will not change its MAC address (network card) or its IP address, the mapping table should be maintained periodically, which affects the network performance.

2- Dynamic Mapping[1][24][25]:

- In dynamic mapping, the host or the router sends an ARP query packet that includes the physical and IP addresses of the sender and the IP address of the receiver.
- Because the sender does not know the physical address of the receiver, the query is broadcasted over the physical network.
- Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet that contains the recipient's IP and physical addresses.





- The mapping is saved in a cache memory for 20 to 30 minutes. This might save the overhead of requesting again MAC addresses, especially if the communication with the destination is needed for more than once.

3- ARP Packet Format[1][24]:

<table>
<tr><td colspan="2">Hardware Type
16 bits</td><td>Protocol Type
16 bits</td><td></td></tr>
<tr><td>Hardware Length8 bits</td><td>Protocol Length8 bits</td><td>Operation16 bits
Request 1, Reply 2</td><td></td></tr>
<tr><td colspan="3">Sender Hardware Address
6 bytes for Ethernet</td><td></td></tr>
<tr><td colspan="3">Sender ProtocolAddress
4 bytes for IPv4</td><td></td></tr>
<tr><td colspan="3">Target Hardware Address
6 bytes for Ethernet</td><td>← Not filled in a request</td></tr>
<tr><td colspan="3">Target ProtocolAddress
4 bytes for IPv4</td><td></td></tr>
</table>

- Hardware Type: (16 bits) this field defines the type of physical network. Each LAN is assigned a value. For example Ethernet is given type 1, token ring… ARP is not dependent on a specific type of network.
- Protocol Type: (16 bits) this field defines the type of the protocol using ARP. For example IPv4 is given type 0800_{16}. ARP can be used with different protocols.
- Hardware length: (8 bits) this field defines the length of the address at the physical network. For example, Ethernet MAC address is of 6 bytes.
- Protocol length: (8 bits) this field defines the length of the network (IP) address. For example, IPv4 address is of 4 bytes.
- Operation: (16 bits) this field defines the type of the ARP packet: 1 for request, 2 for reply.
- Sender's hardware address: (variable length) this field contains the MAC address of the requesting host. For Ethernet, this field is 6 bytes long.
- Sender's protocol address: (variable length) this field contains the network address of the requesting host. For IPv4, this field is 4 bytes long.
- Target's hardware address: (variable length) this field contains the MAC address of the target host.
- Target's protocol address: (variable length) this field contains the network address of the target host.

4- Packet Encapsulation [25]:

- An ARP packet is encapsulated in a data link frame as data.
- The type field of the frame mentions the type of the encapsulated data which is ARP.

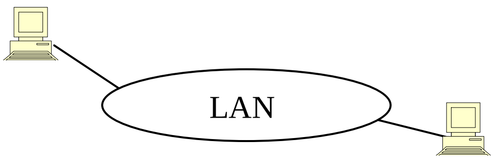
Preamble and SFD	Destination Address	Source Address	Type	Data (ARP Packet)	CRC
8 bytes	6 bytes	6 bytes	2 bytes	(variable)	4 bytes

Encapsulation of an ARP
packet inside an Ethernet frame

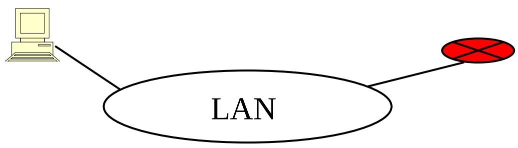
5- ARP Operation (steps) [26]:

- **1.** The sender knows the IP address of the target and wants to send a datagram (data) to a target.
- **2.** IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0's.
- **3.** The message is passed to the data link layer where it is encapsulated in a frame by using the physical address of the sender as the source address and the physical broadcast address as the destination address.
- **4.** Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes its IP address.
- **5.** The target machine replies with an ARP reply message that contains its physical address. The message is unicast.
- **6.** The sender receives the reply message. It now knows the physical address of the target machine.
- **7.** The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

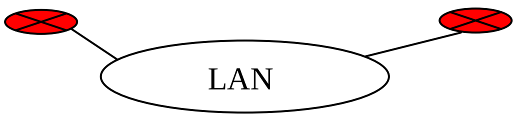
6- ARP Operation (cases) [1][27]:



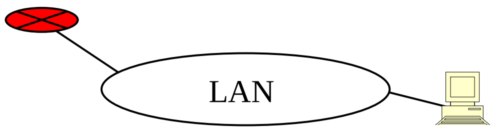
Host-to-host



Host-to-router



Router-to-router



Router-to-host

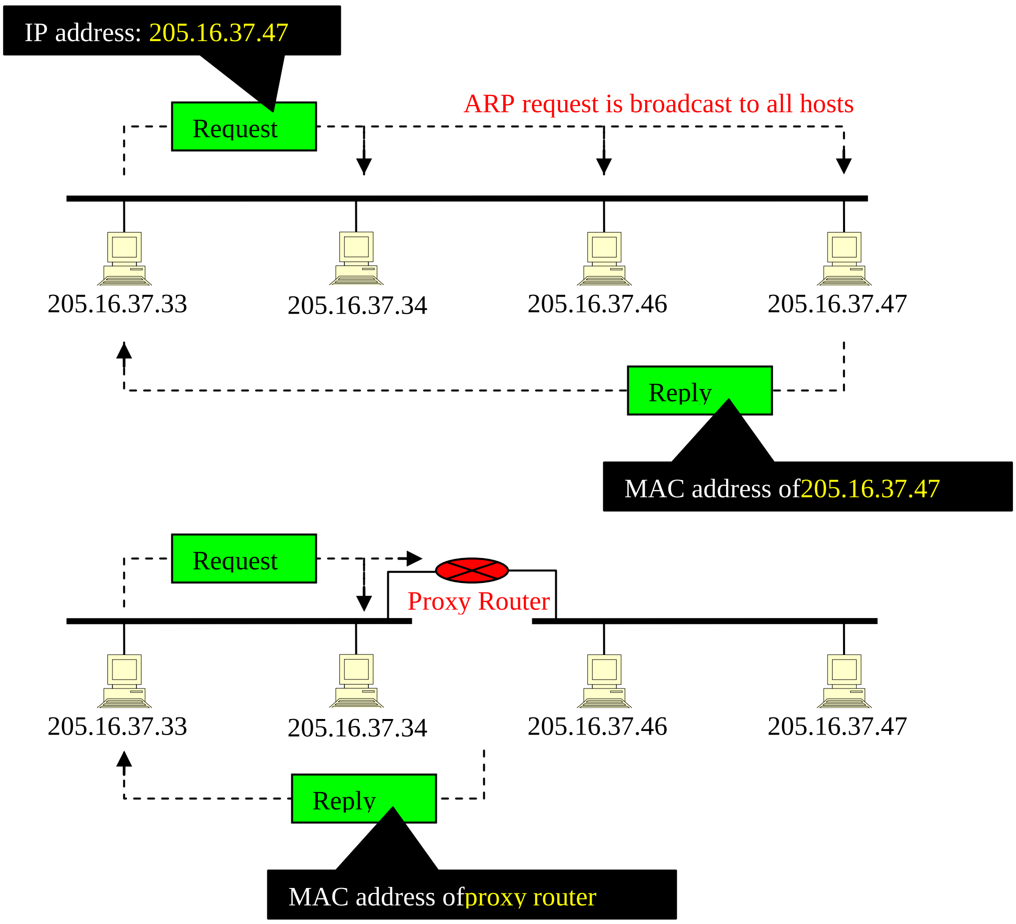
- **Case 1.** The sender is a host and wants to send a packet to another host on the same network. In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.
- **Case 2.** The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop router for this destination. If it does not have a routing table, it looks for the IP address of the default router. The

IP address of the router becomes the logical address that must be mapped to a physical address. Notice that the sender host does not need to know the MAC address of the receiving host.

- **Case 3.** The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of the next router. The IP address of the next router becomes the logical address that must be mapped to aphysical address.
- **Case 4.** The sender is a router that has received a datagram destined for a host on the samenetwork. The destination IP address of the datagram becomes the logical addressthat must be mapped to a physical address.

7- Proxy ARP [1][24]:

- A proxy ARP is an ARP that acts on behalf of a set of hosts that constitute a subnet.
- Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts (its protégés), the router sends an ARP reply announcing its own MAC address. After the router receives the actual IP packet, it sends the packet to the appropriate host or router.



Protocols – RARP, BOOTP and DHCP

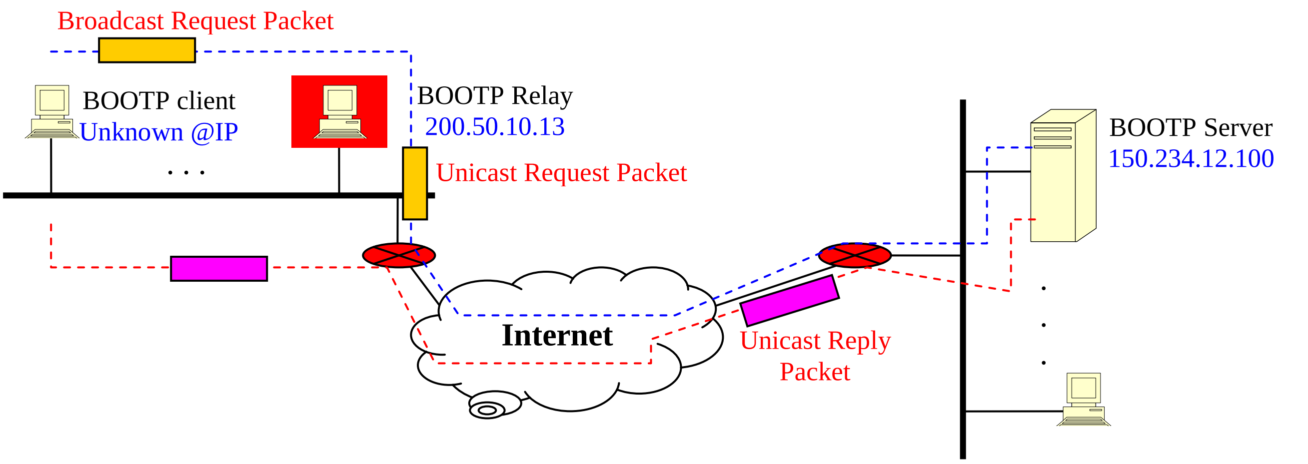
- There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases.
- A station can find its physical address by checking its interface, but it does not know its IP address.
- An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease [1][8].

I- RARP (Reverse Address Resolution Protocol):

- The machine can locally get its physical address which is unique. It can then use the physical address to get the logical address by using the RARP protocol.
- A RARP request is created (RARP client) and broadcast on the local network.
- Another machine (RARP server) on the local network that knows all the IP addresses will respond with a RARP reply.
- There is a serious problem with RARP: Broadcasting is done at the data link layer. The physical broadcast address, all 1's in the case of Ethernet, does not pass the boundaries of a physical network.
- This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet. This is the reason that RARP is almost obsolete.
- Two protocols, BOOTP and DHCP, are replacing RARP[1][25][26].

II- BOOTP (Boot Strap Protocol)[1][22]:

- The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping, especially for diskless machines.
- A diskless machine usually boots from an external ROM (like CDROM) where it cannot save a logical address. Then there should be another machine (server) that saves the mapping of physical addresses to logical addresses for an entire network.
- The administrator may put the client and the server on the same network or on different networks.
- Unlike RARP, BOOTP is an application layer protocol.
- BOOTP messages (Application) are encapsulated in a UDP data unit (Transport), and the UDP data unit itself is encapsulated in an IP packet (Network).



- The BOOTP request is broadcast (frame with destination address all 1's in Ethernet) because the client does not know the IP address of the server, but this packet cannot go out of the local network.
- To solve the problem, one of the hosts (or a router that can be configured to operate at the application layer) can be used as a relay. The host in this case is called a relay agent.
- The relay agent knows the unicast address of a BOOTP server. When it receives this type of packet, it encapsulates the message in a unicast packet and sends the request to the BOOTP server.
- The BOOTP server checks the translation table for the client's logical address (given its physical address) and sends it back to the relay agent.
- The relay agent, after receiving the reply, sends it to the BOOTP client.

III- DHCP (Dynamic Host Configuration Protocol) [1][9] [11][24]::

- The address mapping in BOOTP is static: the client has a fixed logical address that the network administrator has manually stored it in a BOOTP server.
- BOOTP is not suitable for networks that need to lease logical addresses for certain time. In other words, if an organization provides a set of logical addresses that are less than the existing host machines, then it needs to allocate on demand these addresses dynamically to its hosts.
- BOOTP is also not suitable for a host that changes networks like mobile hosts.
- The Dynamic Host Configuration Protocol (DHCP) is designed to enhance the BOOTP.
- The DHCP has been devised to provide static and dynamic address allocation that can be manual or automatic.
- The DHCP acts in the static mode as in BOOTP: The DHCP server checks first its translation table for an entry that has the physical address of the requester. This table is maintained manually by the network administrator.

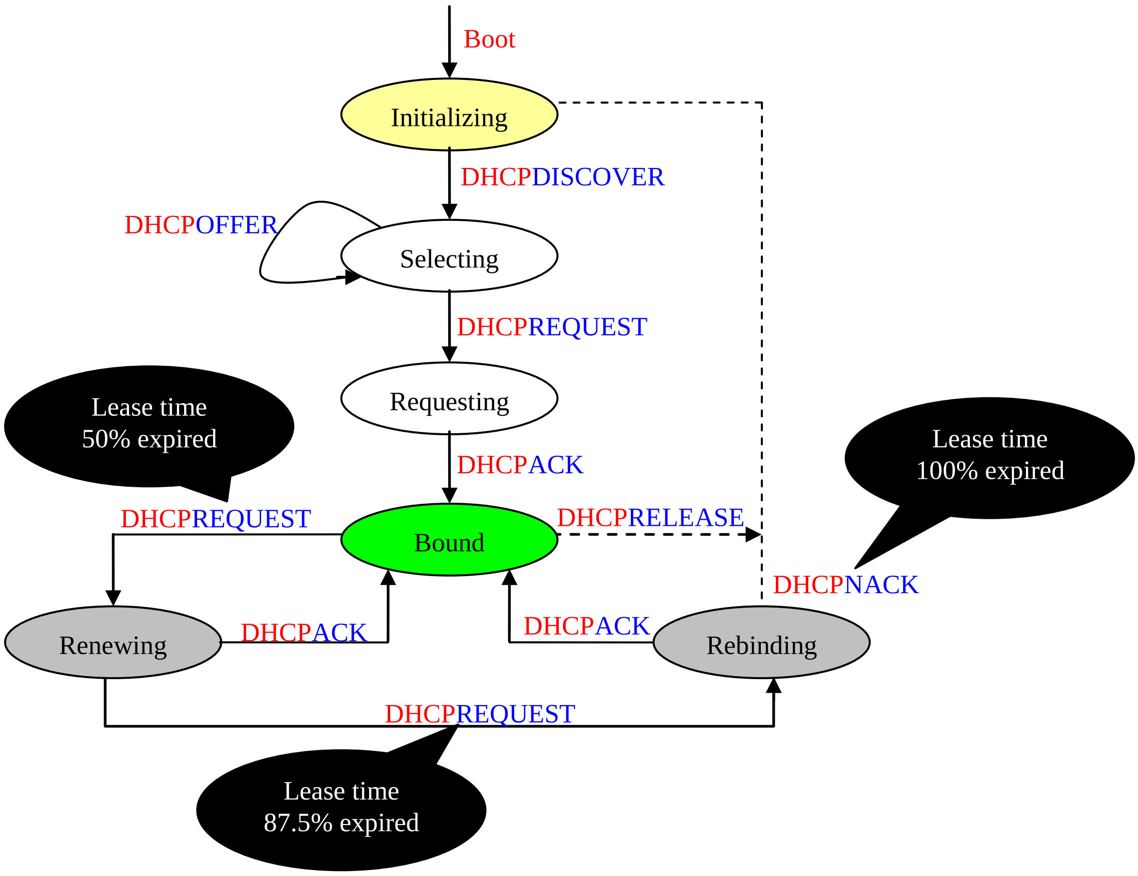
- In dynamic mode, the DHCP server leases automatically addresses for hosts on demand.

1- Leasing:

- In dynamic mode, the addresses assigned from the pool are temporary addresses.
- The DHCP server issues a lease for a specific period of time.
- When the lease expires, the client needs to renew it or it must stop using the address.

2- Transition States:

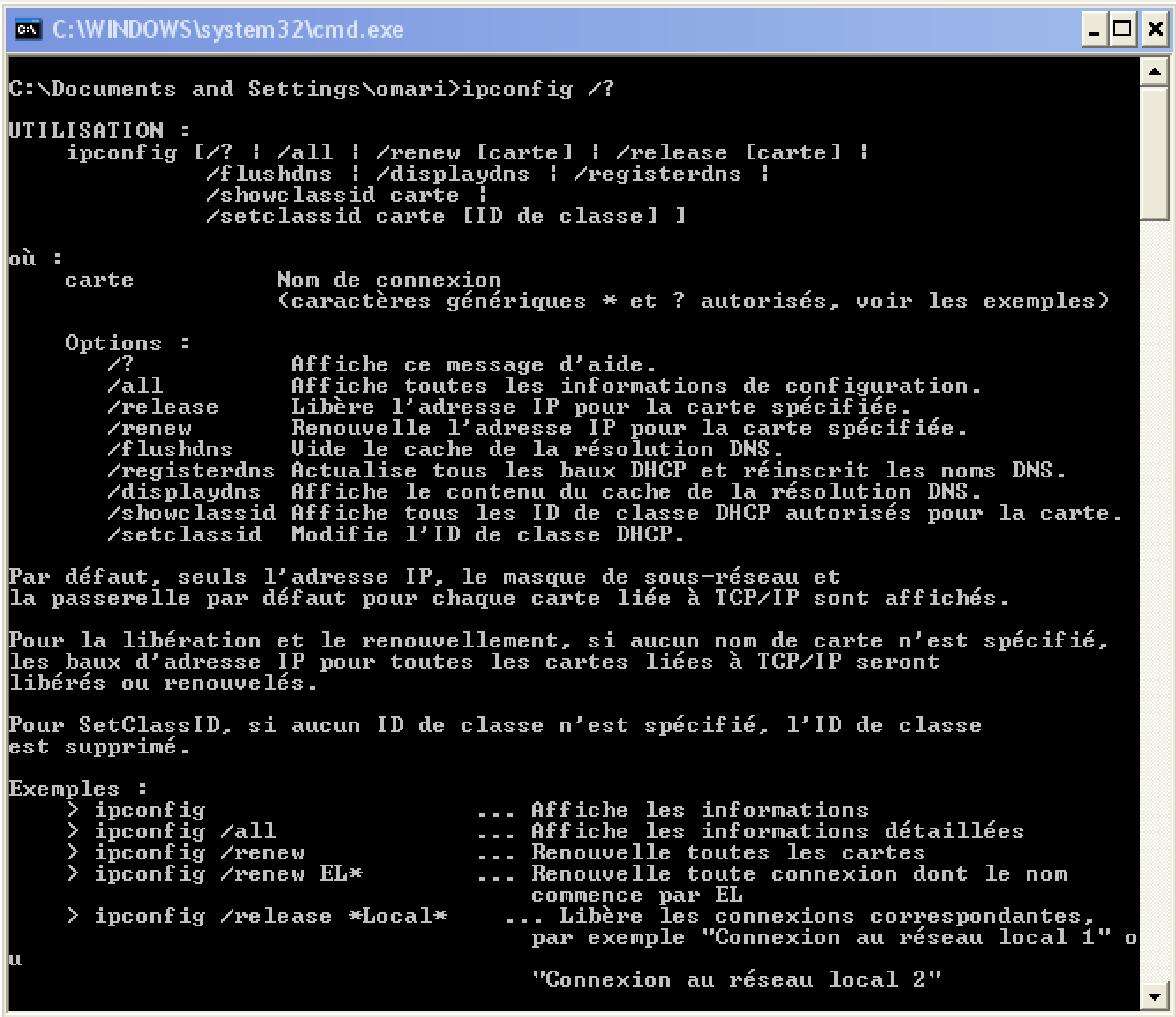
- The DHCP client transitions from one state to another.



- DHCPDISCOVER: a message sent by the client to any server that runs DHCP in order to request an offer for leasing an address.
- DHCPOFFER: the client might receive more than one offer from different servers.
- DHCPREQUEST: a client selects one of the offers and request leasing an address.
- DHCPACK: a message sent from the server with the allocated address.
- DHCPNACK: a message sent from the server denying the request. The server might reject the request simply because the pool of addresses is entirely in use.
- DHCPRELEASE: once a client is finish with the address, it sends this message to release the binding.

3- IPCONFIG command:

- Both windows and Unix operation systems provide the "ipconfig" command for dynamic allocation of ip addresses.
- ipconfig /? displays help for the command.

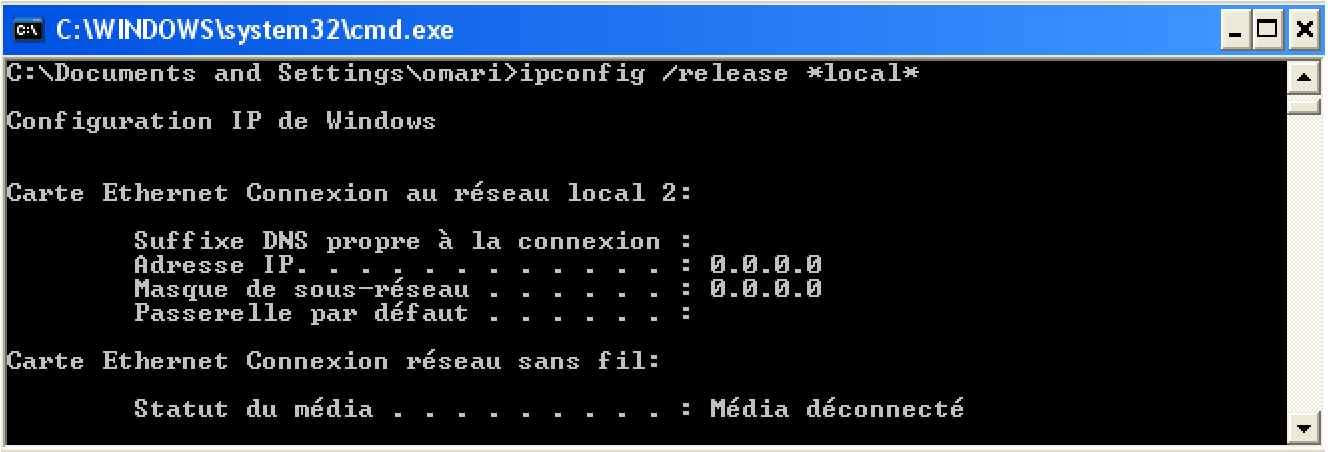


```
C:\Documents and Settings\omari>ipconfig /?

UTILISATION :
    ipconfig [/? | /all | /renew [carte] | /release [carte] |
              /flushdns | /displaydns | /registerdns |
              /showclassid carte |
              /setclassid carte [ID de classe] ]

où :
    carte           Nom de connexion
                    (caractères génériques * et ? autorisés, voir les exemples)

    Options :
       /?           Affiche ce message d'aide.
       /all         Affiche toutes les informations de configuration.
       /release     Libère l'adresse IP pour la carte spécifiée.
       /renew       Renouvelle l'adresse IP pour la carte spécifiée.
       /flushdns    Vide le cache de la résolution DNS.
       /registerdns Actualise tous les baux DHCP et réinscrit les noms DNS.
       /displaydns  Affiche le contenu du cache de la résolution DNS.
       /showclassid Affiche tous les ID de classe DHCP autorisés pour la carte.
       /setclassid  Modifie l'ID de classe DHCP.

Par défaut, seuls l'adresse IP, le masque de sous-réseau et
la passerelle par défaut pour chaque carte liée à TCP/IP sont affichés.

Pour la libération et le renouvellement, si aucun nom de carte n'est spécifié,
les baux d'adresse IP pour toutes les cartes liées à TCP/IP seront
libérés ou renouvelés.

Pour SetClassID, si aucun ID de classe n'est spécifié, l'ID de classe
est supprimé.

Exemples :
    > ipconfig                   ... Affiche les informations
    > ipconfig /all              ... Affiche les informations détaillées
    > ipconfig /renew            ... Renouvelle toutes les cartes
    > ipconfig /renew EL*        ... Renouvelle toute connexion dont le nom
                                     commence par EL
    > ipconfig /release *Local*    ... Libère les connexions correspondantes,
                                     par exemple "Connexion au réseau local 1" o
u
                                     "Connexion au réseau local 2"
```

- ipconfig /all displays detailed information about physical and logical addresses.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\omari>ipconfig /all

Configuration IP de Windows

        Nom de l'hôte . . . . . . . . . . : 287959d5023540f
        Suffixe DNS principal . . . . . . :
        Type de n?ud . . . . . . . . . . : Inconnu
        Routage IP activé . . . . . . . . : Oui
        Proxy WINS activé . . . . . . . . : Non

Carte Ethernet Connexion réseau sans fil:

        Statut du média . . . . . . . . . : Média déconnecté
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 3945ABG Networ
k Connection
        Adresse physique . . . . . . . . .: 00-18-DE-A4-AD-AF

Carte Ethernet Connexion au réseau local 2:

        Suffixe DNS propre à la connexion :
        Description . . . . . . . . . . . : Broadcom 440x 10/100 Integrated Cont
roller
        Adresse physique . . . . . . . . .: 00-15-C5-3E-BC-17
        DHCP activé. . . . . . . . . . . : Non
        Adresse IP. . . . . . . . . . . . : 192.168.0.171
        Masque de sous-réseau . . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . . : 192.168.0.1
        Serveurs DNS . . . . . . . . . .  : 192.168.0.1

Carte PPP FAWRI :

        Suffixe DNS propre à la connexion :
        Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Adresse physique . . . . . . . . .: 00-53-45-00-00-00
        DHCP activé. . . . . . . . . . . : Non
        Adresse IP. . . . . . . . . . . . : 41.201.103.103
        Masque de sous-réseau . . . . . . : 255.255.255.255
        Passerelle par défaut . . . . . . : 41.201.103.103
        Serveurs DNS . . . . . . . . . .  : 208.67.222.222
                                            208.67.220.220
        NetBIOS sur TCPIP. . . . . . . .  : Désactivé

C:\Documents and Settings\omari>
```

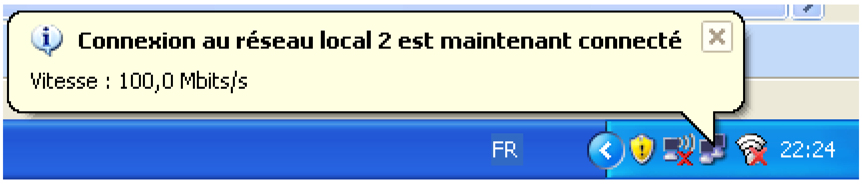
- ipconfig /release releases the binding with the logical address.



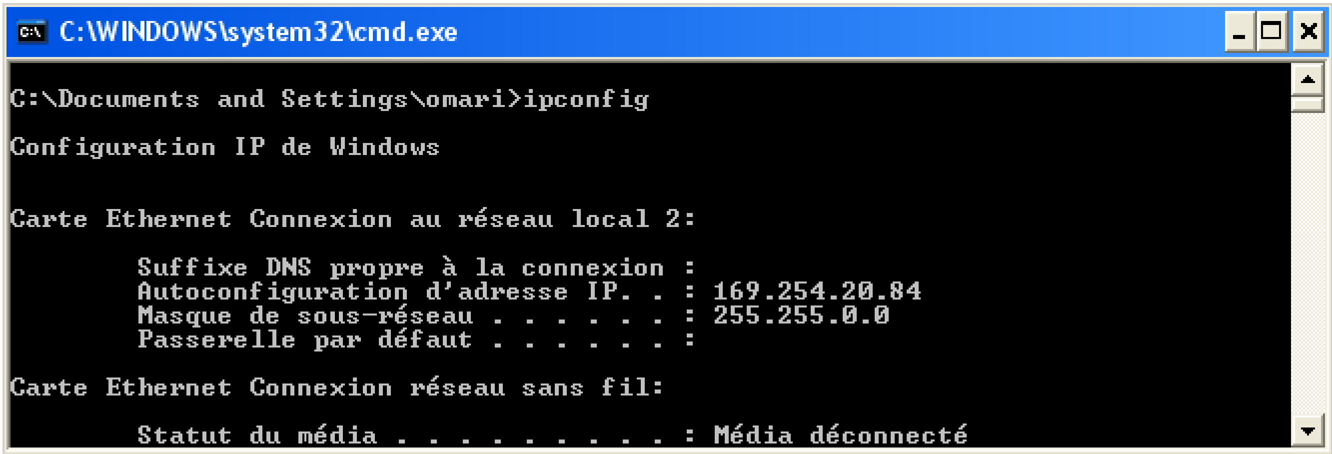
```
C:\Documents and Settings\omari>ipconfig /release *local*

Configuration IP de Windows


Carte Ethernet Connexion au réseau local 2:

        Suffixe DNS propre à la connexion :
        Adresse IP. . . . . . . . . . . . : 0.0.0.0
        Masque de sous-réseau . . . . . . : 0.0.0.0
        Passerelle par défaut . . . . . . :

Carte Ethernet Connexion réseau sans fil:

        Statut du média . . . . . . . . . : Média déconnecté
```

- ipconfig /release releases the binding with the logical address. The system contacts a DHCP server for an ip address.
- ipconfig /renew rebinds the physical address with a new ip address.

The server replies with an ip address



And the binding is done.

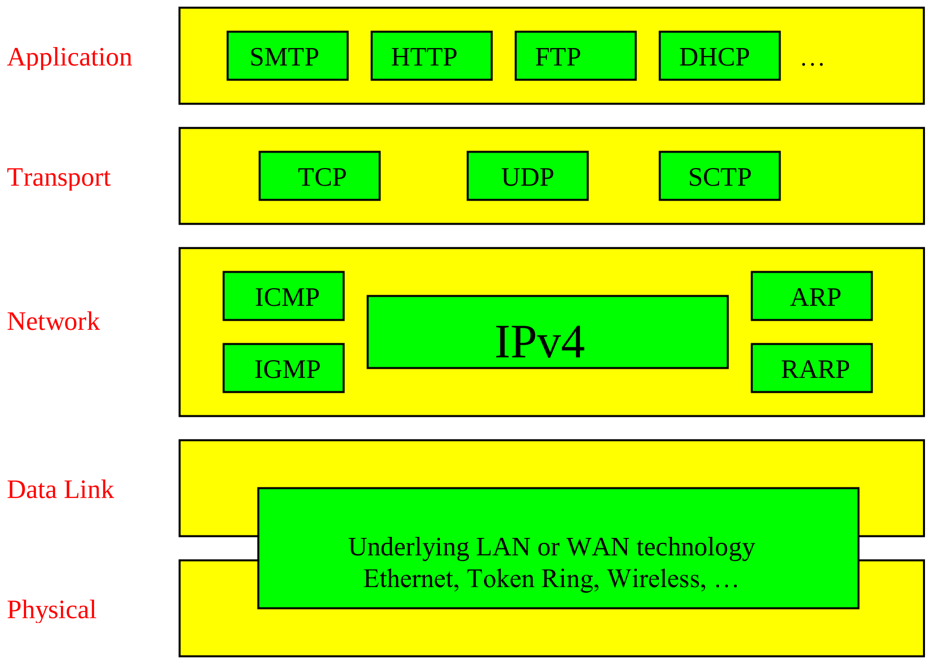


```
C:\Documents and Settings\omari>ipconfig

Configuration IP de Windows


Carte Ethernet Connexion au réseau local 2:

        Suffixe DNS propre à la connexion :
        Autoconfiguration d'adresse IP. . : 169.254.20.84
        Masque de sous-réseau . . . . . . : 255.255.0.0
        Passerelle par défaut . . . . . . :

Carte Ethernet Connexion réseau sans fil:

        Statut du média . . . . . . . . . : Média déconnecté
```

Protocols – IPv4, IPv6

I- IPv4 (Internet Protocol):

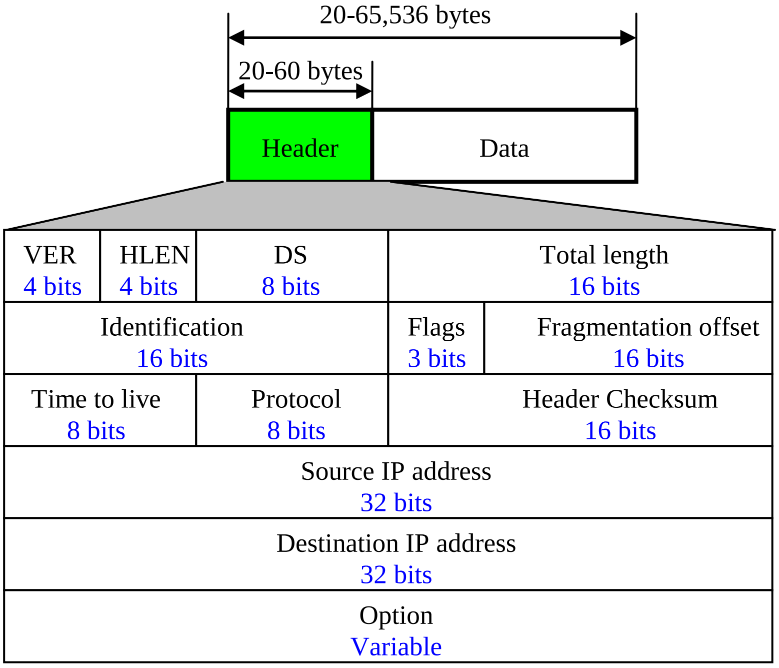
- The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols[1][25].



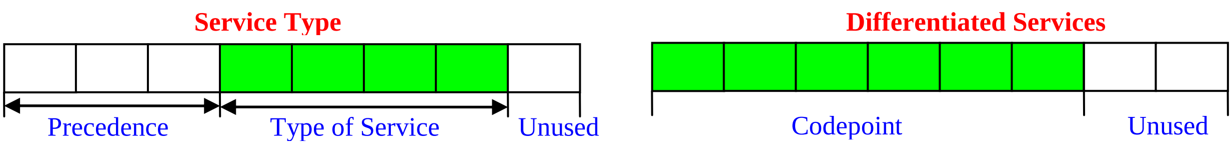
- IPv4 is an unreliable and connectionless datagram protocol that provides a best-effort delivery service.
- The term best-effort means that IPv4 provides no error control or flow control (except for error detection on the header).
- IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.
- If reliability is important, IPv4 must be paired with a reliable protocol such as TCP.
- IPv4 is also a connectionless protocol for a packet-switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transmission[1][26].

A- Datagram:

- Packets in the IPv4 layer are called datagrams.



- **1- Version (VER):** This 4-bit field defines the version of the IP protocol. Currently the version is 4. However, version 6 (or IPv6) may totally replace version 4 in the future.
- **2- Header length (HLEN)[1][25]:** This 4-bit field defines the total length of the datagram header, in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes). When there are no options, the header length is 20 bytes, and the value of this field is 5 (5 x 4 = 20). When the option field is at its maximum size, the value of this field is 15 (15 x 4 = 60).
- **3- Differentiated Services (DS)[1][27]**: The interpretation and name of this 8-bit field has been changed. This field, previously called service type, is now called differentiated services. We show both interpretations.



- In the service type interpretation, the first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits, and the last bit is not used.
- Precedence is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary). The precedence defines the priority of the datagram in issues such as congestion. If a router is congested and needs to discard some datagrams, those datagrams with lowest precedence are discarded first. Some datagrams in the Internet are more important than others. For example, a datagram used for

network management is much more urgent and important than a datagram containing optional information for a group.

- TOS bits is a 4-bit subfield with each bit having a special meaning. Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram. With only 1 bit set at a time, we can have five different types of services.

TOS bits	Description
0000	Normal (Default)
0001	Minimize Cost
0010	Maximize Reliability
0100	Maximize Throughput
1000	Minimize Delay

- Application programs can request a specific type of service. The defaults for some applications are shown as follows:

Protocol	TOS bits	Description
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize Cost
SNMP	0010	Maximize Reliability
TELNET	1000	Minimize Delay
FTP (Data)	0100	Maximize Throughput
FTP (control)	1000	Minimize Delay
SMTP (Data)	0100	Maximize Throughput
SMTP (Command)	1000	Minimize Delay

- It is clear from the table above that interactive activities, activities requiring immediate attention, and activities requiring immediate response need minimum delay. Those activities that send bulk data require maximum throughput. Management activities need maximum reliability. Background activities need minimum cost.
- In the second interpretation (Differentiated Services), the first 6 bits make up the codepoint subfield, and the last 2 bits are not used.
- The codepoint subfield can be used in two different ways.
- When the 3 rightmost bits are 0's, the 3 leftmost bits are interpreted the same as the precedence bits in the service type interpretation. In other words, it is compatible with the old interpretation.

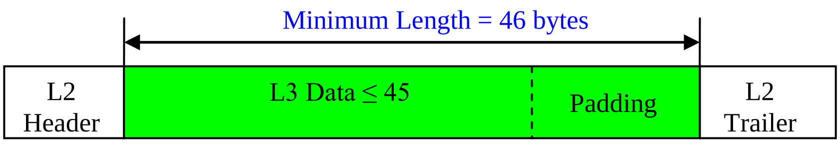
- When the 3 rightmost bits are not all 0's, the 6 bits define 64 services based on the priority assignment by the Internet or local authorities according to the next table. The first category contains 32 service types; the second and the third each contain 16.
- The first category (numbers 0, 2, 4, ... ,62) is assigned by the Internet authorities. The second category (3, 7, 11, 15, …, 63) can be used by local authorities (organizations). The third category (1, 5, 9, …,61) is temporary and can be used for experimental purposes.

Category	Codepoint	Assigning Authority
1	XXXXX0	Internet Authority
2	XXXX01	Local
3	XXXX11	Temporary or Experimental

- **4- Total length [1][14]:** This is a 16-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.

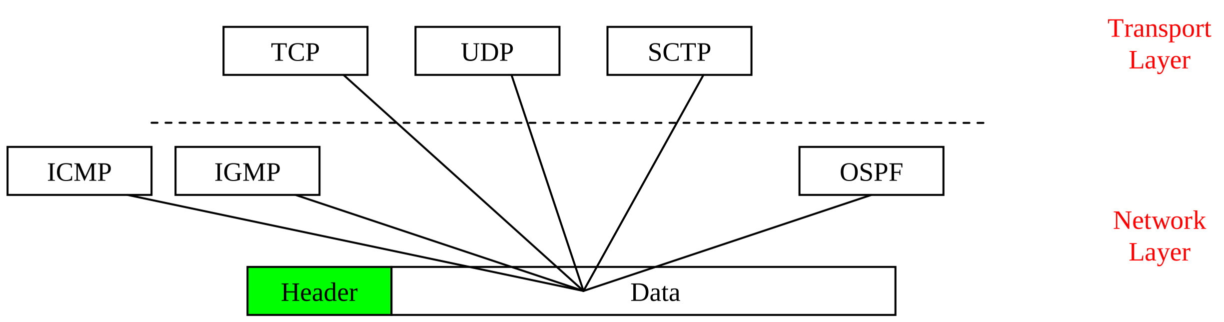
  Length of data = Total length - Header length

- Since the field length is 16 bits, the total length of the IPv4 datagram is limited to 65,535 (2^{16} - 1) bytes, of which 20 to 60 bytes are the header and the rest is data from the upper layer.
- Though a size of 65,535 bytes might seem large, the size of the IPv4 datagram may increase in the near future as the underlying technologies allow even more throughput (greater bandwidth). Yet, when we discuss fragmentation next, we will see that some physical networks are not able to encapsulate a datagram of 65,535 bytes in their frames. The datagram must be fragmented to be able to pass through those networks.
- One may ask why we need the total length field. When a machine (router or host) receives a frame, it drops the header and the trailer, leaving the datagram. There are occasions in which the datagram is not the only thing encapsulated in a frame; it may be that padding has been added. For example, the Ethernet protocol has a minimum and maximum restriction on the size of data that can be encapsulated in a frame (46 to 1500 bytes).



- If the size of an IPv4 datagram is less than 46 bytes, some padding will be added to meet this requirement. In this case, when a machine decapsulates the datagram, it needs to check the total length field to determine how much is really data and how much is padding.

- **5- Identification [1]:** This field is used in fragmentation to link separate fragments to the original packet.
- **6- Flags [1]:** This field is used in fragmentation to show the status fragmentation.
- **7- Fragmentation offset [1]:** This field is used in fragmentation to identify the order of the fragment in the original packet.
- **8- Time to live [1][13]:** This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero. However, for this scheme, all the machines must have synchronized clocks which practically impossible.
- Today, this field stores the maximum number of hops (routers) visited by the datagram. Each router that processes the datagram decrements this number by 1. If this value, after being decremented, is zero, the router discards the datagram.
- This field is needed because routing tables in the Internet can become corrupted. A datagram may travel in a loop of routers without ever getting delivered to the destination host.
- Another use of this field is to limit the journey of a datagram. For instance, if the field is set to 1, then the datagram circulates locally; when the packet reaches the next router it will be discarded.
- **9- Protocol [1][27]:** This 8-bit field defines the protocol that uses the services of the IPv4 layer. It could be a network layer protocol such as ICMP (value = 1) and IGMP (value = 2), or a transport layer protocol like TCP (value = 6) and UDP (value = 17).



- **10- Checksum [1][16]:** The implementation of the checksum in the IPv4 packet follows the same principles of the usual checksum. First, the value of the checksum field is set to zero. Then the entire header is divided into 16-bit sections and added together. The result (sum) is complemented and inserted into the checksum field.
- The checksum in the IPv4 packet covers only the header, not the data, because all higher-level protocols that encapsulate data in the IPv4 datagram have a checksum field that covers the whole packet. Also, the header of the IPv4 packet changes with each visited router, but the data do not.

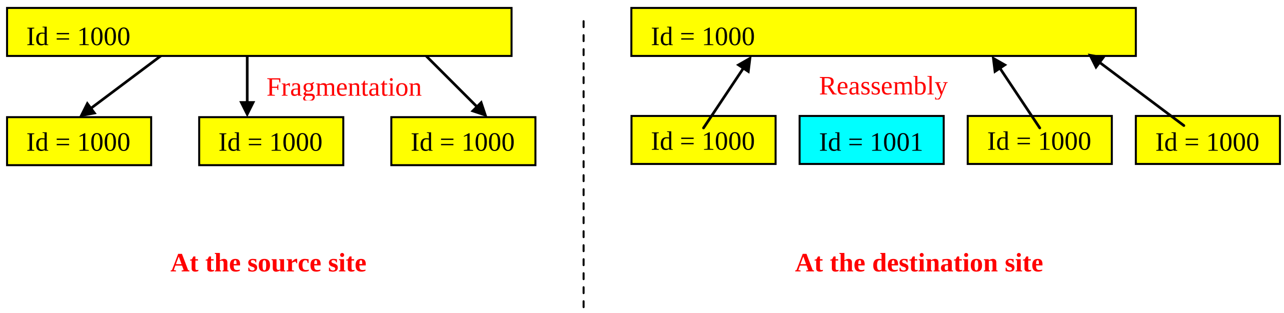
- **11- Source address [1][17]:** This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
- **12- Destination address [1][18]:** This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

B- Fragmentation[1][15]:

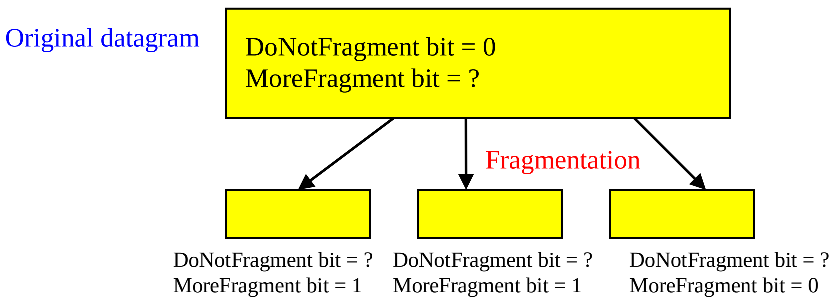
- A datagram can travel through different networks. Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the frame depend on the protocol used by the physical network through which the frame has just traveled and also the network that is going to travel.
- In most protocols, each data link layer protocol has its own frame format that defines the MTU (maximum transfer unit) or the maximum size of the data field.

Network or Protocol	MTU
Hyperchannel	65,535
Token Ring	17,914
Token Bus	4,464
FDDI	3,352
Ethernet	1,500
X.25	576
PPP	296

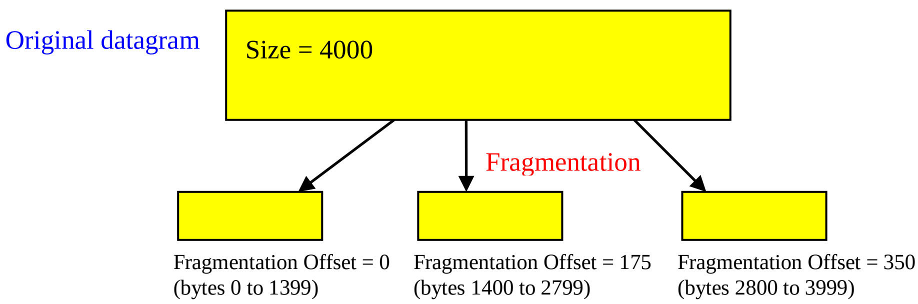
- In order to keep the IPv4 independent of the physical network, the maximum size of a datagram is set to 65,535 bytes. On the other hand, when the datagram size is greater than the MTU of the data link layer, then the packet needs to be fragmented into smaller packets.
- When a datagram is fragmented, most parts of the header must be copied by all fragments. The host or router that fragments a datagram must change the values of four fields: flags, fragmentation offset, total length, and checksum.
- **Identification:** This 16-bit field identifies a datagram originating from the source. The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host. The identification number helps the destination in reassembling the datagram. It knows that all fragments having the same identification value must be assembled into one datagram.



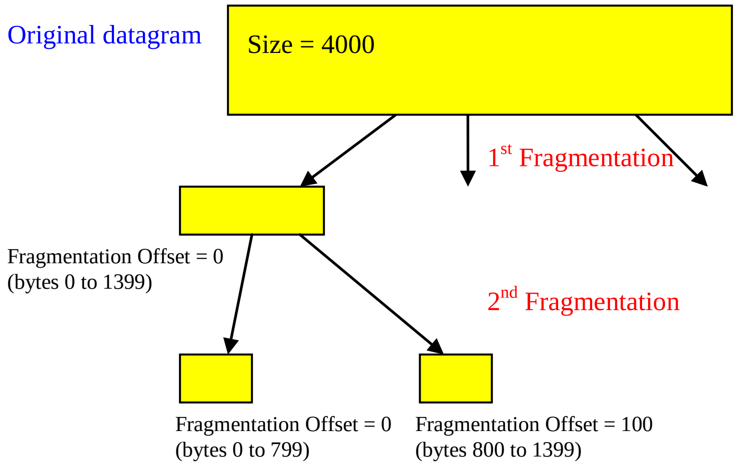
- **Flags:** This is a 3-bit field. The first bit is reserved. The second bit is called the DoNotFragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary.
- The third bit is called the MoreFragment bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment.



- **Fragmentation offset:** This 13-bit field shows the relative position of this fragment with respect to the whole datagram. The offset is measured in units of 8 bytes.
- For instance, when a datagram with a data size of 4000 bytes is fragmented into three fragments, the first fragment carries bytes 0 to 1399. The offset for this new datagram is 0/8 = 0. The second fragment carries bytes 1400 to 2799; the offset value for this fragment is 1400/8 = 175. Finally, the third fragment carries bytes 2800 to 3999. The offset value for this fragment is 2800/8 =350.



- A fragment can further be fragmented. In this case the value of the offset field is always relative to the original datagram.

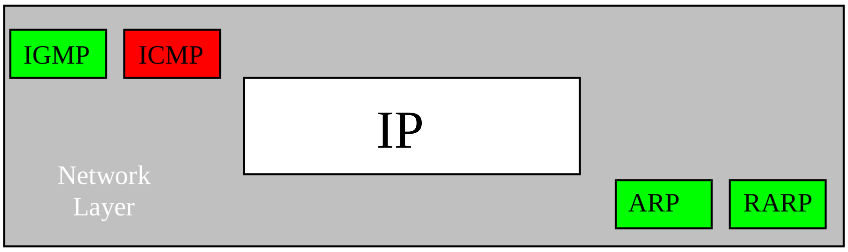


- It is recommended that the reassembly of the fragment is done at the destination only for better performance.

Protocols – ICMP, IGMP

I- ICMP (Internet Control Message Protocol) [1][25] [26]:

- The IP provides unreliable and connectionless datagram delivery. It was designed this way to make efficient use of network resources.
- The IP protocol has two deficiencies: lack of error control and lack of assistance mechanisms.
- The IP protocol has no error-reporting or error-correcting mechanism, e.g., a router discards a datagram because it cannot find a router to the final destination, or because the time-to-live field has a zero value. Another case is when the final destination host must discard all fragments of a datagram because it has not received all fragments within a predetermined time limit.
- The IP protocol also lacks a mechanism for host and management queries like determining if a router or another host is alive.
- The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies.



- There are two types of ICMP messages: Error-reporting messages and Query messages.

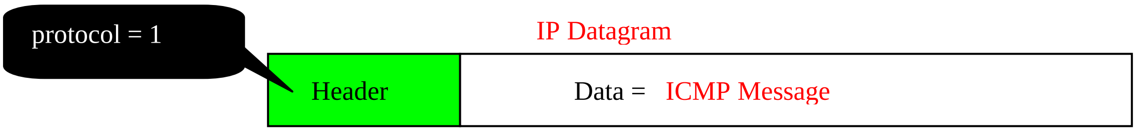
1- ICMP Messages:

- An ICMP message is composed of a header and a data section. The header has a type field that defines the type of the ICMP message. The code field is used to specify reasons for some messages. The checksum field is used to control errors of the entire ICMP message.

ICMP Message

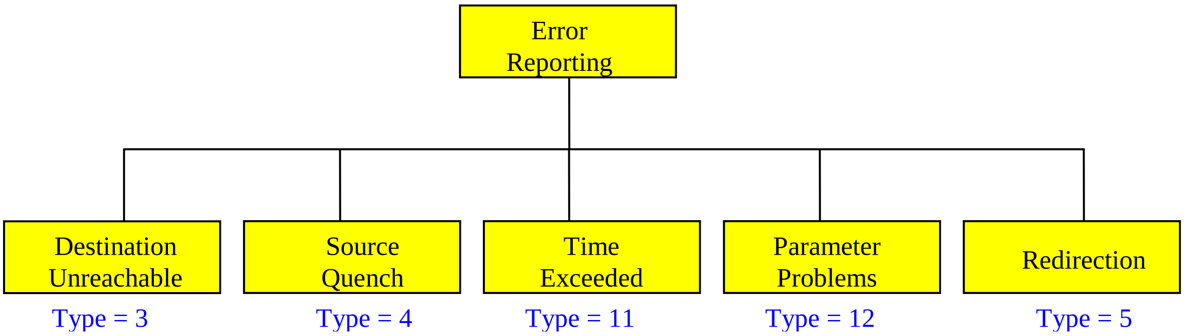
Type 8 bits	Code 8 bits	Checksum 16 bits
Rest of Header…		
Data		

- An ICMP message is encapsulated as data in an IP datagram.

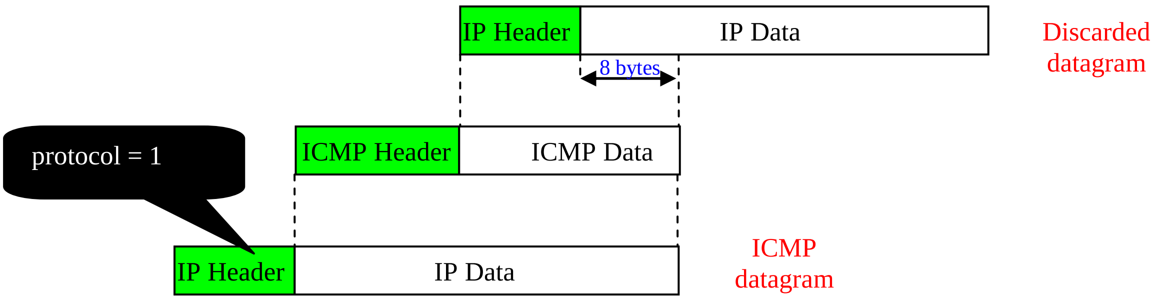


1- Error Reporting Messages [1][24]:

- ICMP always reports error messages to the original source.
- ICMP does not correct errors: it simply reports them.
- Five types of errors are handled: destination unreachable, source quench, time exceeded, parameter problems, and redirection.

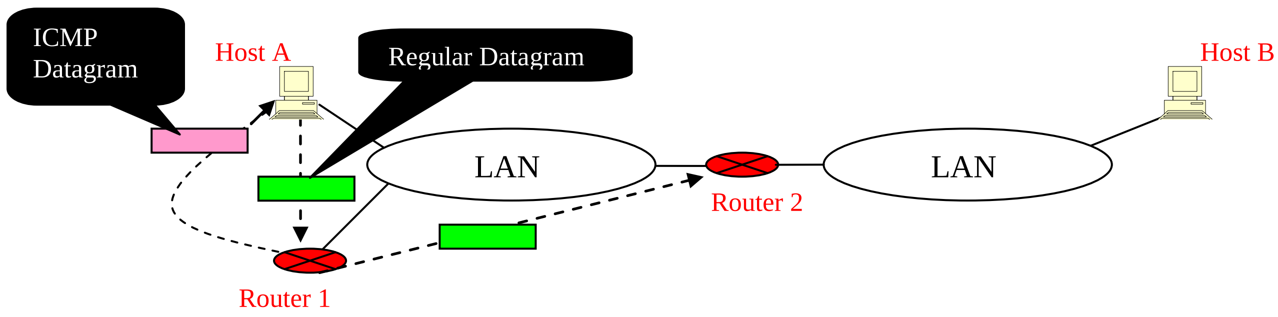


- Most error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram.
- The original datagram header is added to give the original source, which receives the error message, information about the datagram itself (identification, fragmentation, …).
- The first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCP or UDP) about the error.
- ICMP forms an error packet, which is then encapsulated in an IP datagram.



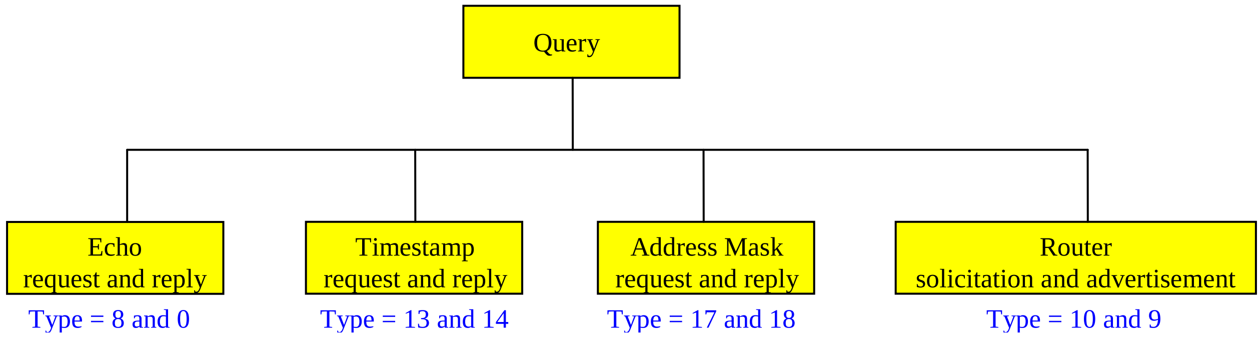
- **A- Destination Unreachable:** When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message (type = 3) back to the source host that initiated the datagram.

- **B- Source Quench:** The IP protocol is a connectionless protocol: it does not have an embedded flow control mechanism which creates a major problem in communication: congestion.
- The source host never knows if the routers or the destination host has been overwhelmed with datagrams.
- The source host never knows if it is producing datagrams faster than can be forwarded by routers or processed by the destination host.
- The source-quench message in ICMP was designed to add a kind of flow control to the IP. When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram. This message informs the source that the datagram has been discarded, and warns it (the source) that there is congestion somewhere in the path. Therefore, the source may slow down in sending data to the destination.
- **C- Time Exceeded:** The time-exceeded message is generated in case of discarding a datagram by a router when the value of the time-to-live field is equal to zero. Then, a time-exceeded message must be sent by the router to the original source.
- Another case where a time-exceeded message is also generated is when not all fragments that make up a message arrive at the destination host within a certain time limit.
- **D- Parameter Problem:** Any ambiguity in the header part of a datagram can create serious problems as the datagram travels through the Internet.
- For instance, we know that if a noise hits the datagram packet, there is a possibility that the checksum mechanism cannot catch it.
- If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.
- **E- Redirection:** When a packet is destined for another network, a host must have a routing table to find the address of the router or the next router. In dynamic routing, routers take part in the routing update process; however, for efficiency, hosts do not take part in the routing update process because there are many more hosts in an internet than routers. Therefore, hosts usually use static routing.
- For this reason, the host may send a datagram, which is destined for another network, to the wrong router. In this case, the router that receives the datagram will forward the datagram to the correct router. However, to update the routing table of the host, it sends a redirection message to the host.

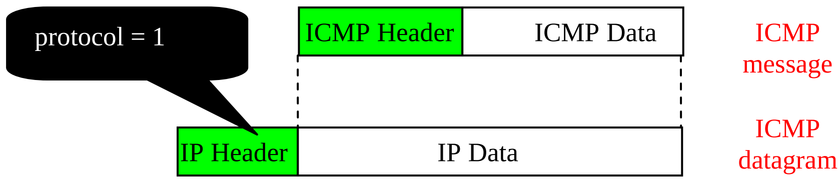


2- Query Messages [1][28]:

- In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through some query messages: Echo, timestamp, address mask, router solicitation and advertisement.



- In query mode, a node sends a message that is answered in a specific format by the destination node. A query message is encapsulated in an IP packet.



- **A-Echo Request and Reply:** The echo-request and echo-reply messages are designed for diagnostic purposes.
- The echo-request and echo-reply messages can be used to determine if there is communication at the IP level. The exchange of these messages is a proof that the intermediate routers are receiving, processing, and forwarding IP datagrams.
- Today, most systems provide a version of the ping command that can create a series of echo-request and echo-reply messages, providing statistical information.

```
$ ping thda.edu
PING thda.edu (153.18.8.1) 56 (84) bytes of data.
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=0    Ttl=62   time=1.91 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=1    ttl=62   time=2.04 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=2    ttl=62   time=1.90 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=3    ttl=62   time=1.97 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=4    ttl=62   time=1.93 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=5    ttl=62   time=2.00 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=6    ttl=62   time=1.94 ms
```

```
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=7    ttl=62   time=1.94 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=8    ttl=62   time=1.97 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=9    ttl=62   time=1.89 ms
 64 bytes from tiptoe.thda.edu (153.18.8.1): icmp_seq=10   ttl=62   time=1.98 ms

--- thda.edu ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10103ms
rtt min/avg/max = 1.899/1.955/2.041 ms
```

- The ping program sends messages with sequence numbers starting from 0. For each probe it gives us the RTT time (round trip time). The TTL (time to live) field in the IP datagram that encapsulates an ICMP message has been set to 62, which means the packet cannot travel more than 62 hops.
- The traceroute program in UNIX or tracert in Windows can be used to trace the route of a packet from the source to the destination.
- The program elegantly uses two ICMP messages, time exceeded and destination unreachable, to find the route of a packet. This is a program at the application level that uses the services of UDP at the transport layer.

```
$ traceroute xerox.com
traceroute to xerox.com (13.1.64.93), 30 hops max, 38 byte packets

1 Dcore.fbda.edu (153.18.31.254)      0.622 ms      0.891 ms      0.875 ms
2 Ddmz.fbda.edu (153.18.251.40)       2.132 ms      2.266 ms      2.094 ms
3 Cinic.fhda.edu (153.18.253.126)     2.110 ms      2.145 ms      1.763 ms
4 cenic.net (137.164.32.140)          3.069 ms      2.875 ms      2.930 ms
5 cenic.net (137.164.22.31)           4.205 ms      4.870 ms      4.197 ms
...
14 snfc21.pbi.net (151.164.191.49)    7.656 ms      7.129 ms      6.866 ms
15 sbcglobaLnet (151.164.243.58)      7.844 ms      7.545 ms      7.353 ms
16 pacbell.net (209.232.138.114)      9.857 ms      9.535 ms      9.603 ms
17 209.233.48.223 (209.233.48.223)    10.634 ms     10.771 ms     10.592 ms
18 alpha.Xerox.COM (13.1.64.93)       11.172 ms     11.048 ms     10.922 ms
```

- The *traceroute* program uses the following steps to find the address of the first router R_1 and the round-trip time between host A and router R_l.
- **a.** The *traceroute* application at host A sends a packet to destination B using UDP; the message is encapsulated in an IP packet with a TTL value of 1. The program notes the time the packet is sent.
- **b.** Router R_1 receives the packet and decrements the value of TTL to 0. It then discards the packet (because TTL is 0). The router, however, sends a time-exceeded ICMP message (type: 11, code: 0) to show that the TTL value is 0 and the packet was discarded.
- **c.** The *traceroute* program receives the ICMP messages and uses the source address of the IP packet encapsulating ICMP to find the IP address of router Rl. The program also makes note of the time the packet has arrived. The difference between this time and the time at step **a** is the round-trip time.
- The traceroute program repeats steps a to c three times to get a better average round-trip time. The first trip time may be much longer than the second or third because it takes time for the ARP program to find the physical address of router R_1.
- The *traceroute* program repeats the previous steps to find the address of the next router R_2 and the round-trip time between host A and router R_2. However, in this step, the value of TTL is set to 2.

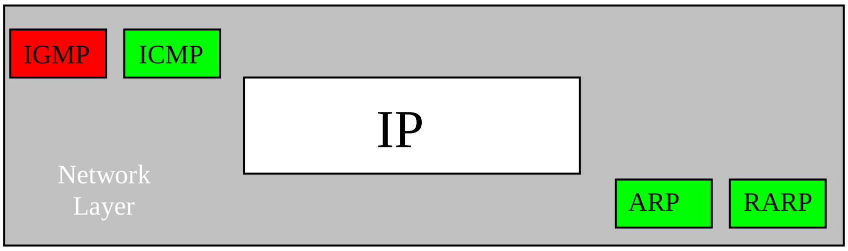
So router R_1 forwards the message, while router R2 discards it and sends a time-exceeded ICMP message. The same process is repeated for the rest of the routers but with different TTLs.

- The *traceroute* finds the address of host B and the round-trip time between host A and host B using the same technique. But host B does not discard the message since it has reached its final destination, which means that no ICMP message is generated due to time-exceeded event. The *traceroute* program uses a different strategy here. The destination port of the UDP packet is set to one that is not supported by the UDP protocol. When host B receives the packet, it cannot find an application program to accept the delivery. It discards the packet and sends an ICMP destination-unreachable message (type: 3, code: 3) to host A. Receiving the destination-unreachable message with a code value 3 is an indication that the whole route has been found and there is no need to send more packets.
- **B- Timestamp Request and Reply:** Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them.
- It can also be used to synchronize the clocks in two machines.
- **C- Address-Mask Request and Reply:** A host may know its IP address, but it may not know the corresponding mask.
- To obtain its mask, a host sends an address-mask-request message to a router on the LAN. If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message.
- The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host.
- **D- Router Solicitation and Advertisement:** A host that wants to send data to a host on another network needs to know the address of routers connected to its own network, and must know if the routers are alive and functioning.
- In this case, a host broadcasts (or multicasts) a router-solicitation message. The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message.
- A router can also periodically (dynamic routing) send router-advertisement messages even if no host has solicited. Then, it announces not only its own presence but also the presence of all routers on the network of which it is aware.

II- IGMP (Internet Group Management Protocol) [1][25][26]:

- The IP protocol can be involved in two types of communication: unicasting and multicasting.

- Unicasting is the communication between one sender and one receiver.
- However, some processes sometimes need to send the same message to a large number of receivers simultaneously. This is called multicasting, which is a one-to-many communication.
- For example, multiple stockbrokers can simultaneously be informed of changes in a stock price, or travel agents can be informed of a plane cancellation, or multiple users watching video-on-demand movies.
- The Internet Group Management Protocol (IGMP) is one of the necessary protocols that is involved in multicasting. IGMP is a companion to the IP protocol.

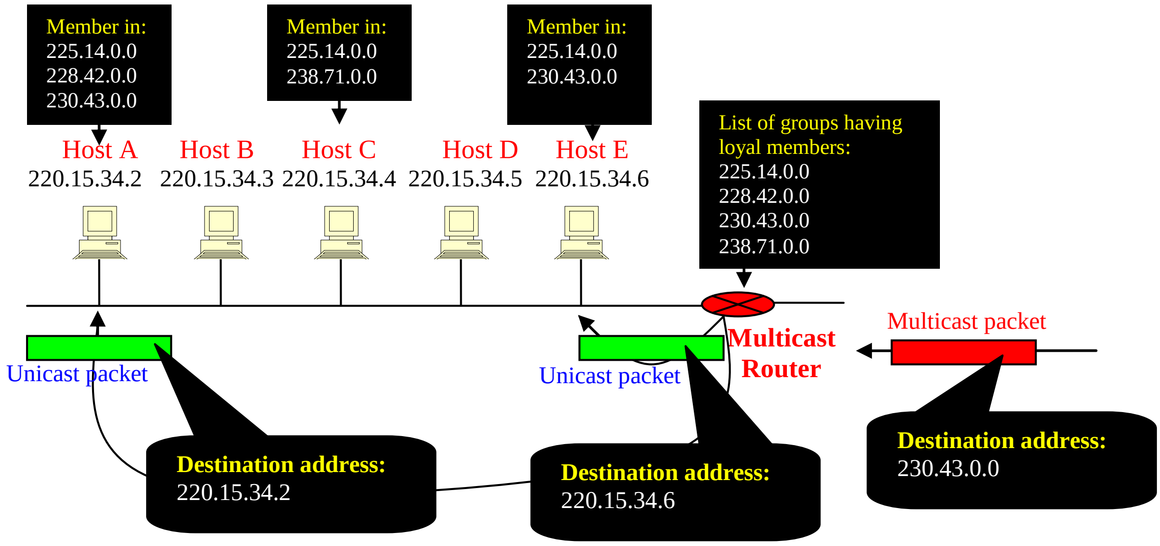


1- Group Management:

- IGMP is not a multicasting routing protocol; it is a protocol that manages group membership.
- In any network, there are one or more multicast routers that distribute multicast packets to hosts or other routers. The IGMP protocol gives the multicast routers information about the membership status of hosts (routers) connected to the network.
- In multicasting, a group of identified by an IP address of class D.

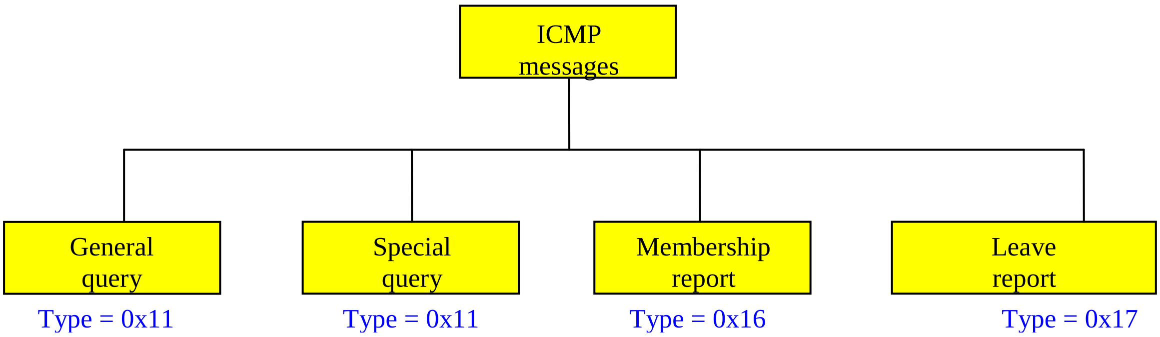
	1st Byte	2nd Byte	3rd Byte	4th Byte
Class D	**224 to 239**			

- A multicast router may receive thousands of multicast packets every day for different groups. If a router has no knowledge about the membership status of the hosts, it must broadcast all these packets which creates a lot of traffic and consumes bandwidth.
- A better solution is to keep a list of groups in the network for which there is at least one loyal member. The main role of the IGMP is to help the multicast router create and update this list.



2- IGMP Messages

- IGMP (version 2) has three types of messages: the query (general and special), the membership report, and the leave report.



3- Message Format

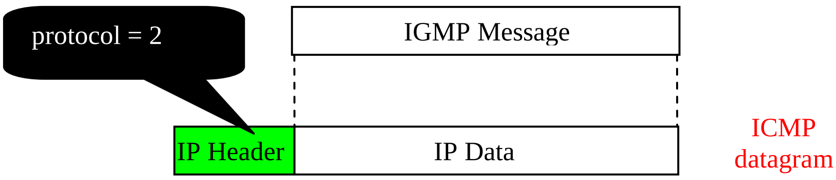
8 bits	8 bits	16 bits
Type	Maximum response time	Checksum
- All 0s for general query. - Group multicast address for special query, membership report and leave report.		

- Type: This 8-bit field defines the type of message: 0x11 for query, 0x16 for membership report, 0x17 for leave report.
- Maximum response time: This 8-bit field defines the amount of time in which a query must be answered. The value is in 100 milliseconds; for example, if the value is 100, it means 10 s.
- The value is nonzero in the query message; it is set to zero in membership report and leave report messages.

- Checksum: This is a 16-bit field carrying the checksum. The checksum is calculated over the 8-byte message.
- Group address: The value of this field is 0 for a general query message. The value defines the groupid (multicast address of the group) in the special query, the membership report, and the leave report messages.

4- Encapsulation:

- Let us recall that the IGMP is not responsible for the delivery of multicast packet. The IGMP helps the routers to keep track of memberships of local hosts.
- Once an IGMP message is created, it is encapsulated in an IP datagram. The protocol field in the IP header is set to 2.



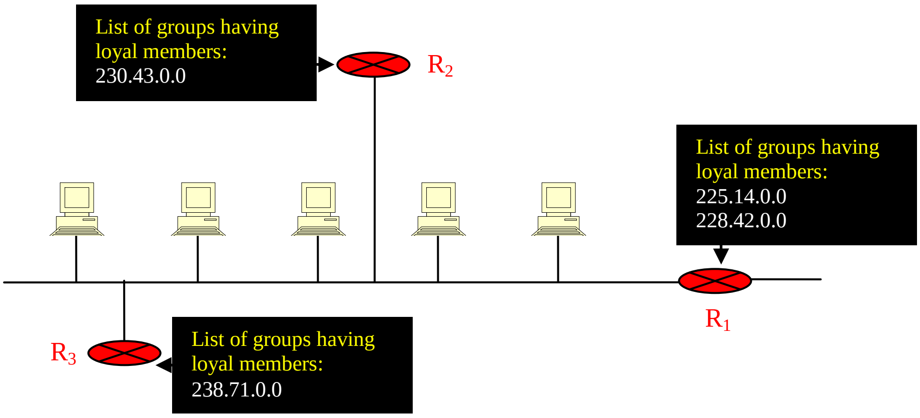
- When the message is encapsulated in the IP datagram, the value of TTL must be 1. This is required because the domain of IGMP is local. No IGMP message must travel beyond the LAN. A TTL value of 1 guarantees that the message does not leave the LAN since this value is decremented to 0 by the next router and, consequently, the packet is discarded.
- The destination address of the IP datagram that encapsulates the IGMP message varies depending on the type of the IGMP message:

Type	Destination IP Address
Query (general and special)	224.0.0.1 (all systems {hosts + routers} on this subnet)
Membership Report	Multicast address of the group
Leave Report	224.0.0.2 (all routers on this subnet)

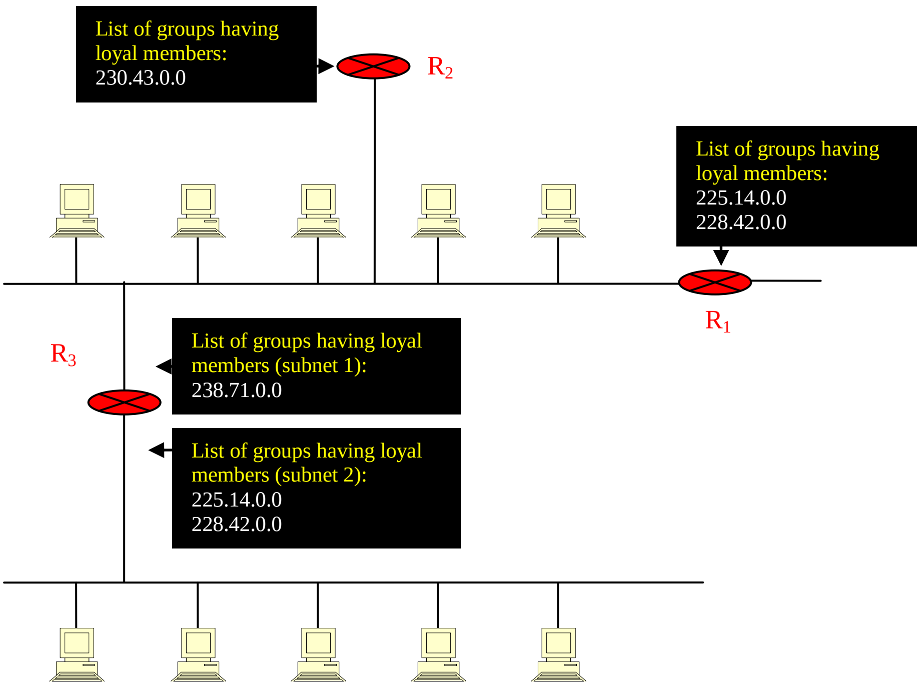
- A query message is multicast by using the multicast address 224.0.0.1. All hosts and all routers will receive the message.
- A membership report is multicast using a destination address equal to the multicast address being reported (groupid). Every station (host or router) that receives the packet can immediately determine (from the header) the group for which a report has been sent.
- This address is duplicated in a packet; it's part of the message itself and also a field in the IP header. The duplication prevents errors.
- A leave report message is multicast using the multicast address 224.0.0.2 (all routers on this subnet) so that routers receive this type of message. Hosts receive this message too, but disregard it.

5- IGMP Operation:

- IGMP operates locally. A multicast router connected to a network has a list of multicast addresses of the groups with at least one loyal member in that network.
- For each group there is one router only that has the duty of distributing the multicast packets destined for that group. This means that if there are many multicast routers connected to a network, their lists of groupids are mutually exclusive.

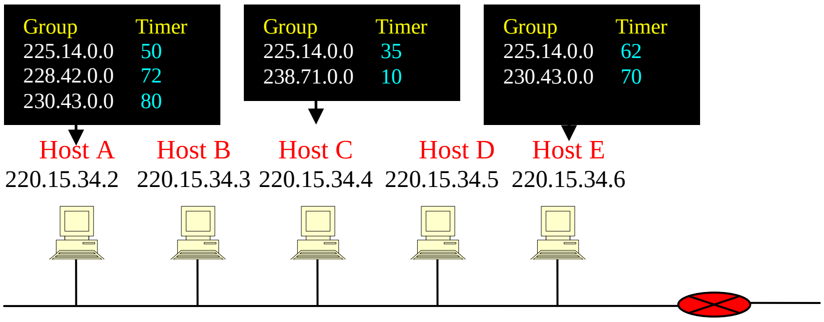


- For example, in the above figure only router R_1 distributes packets with the multicast address of 225.70.8.20.
- A router can have membership in a group. When a router has membership, it means that a network connected to one of its other interfaces receives these multicast packets. We say that the router has an interest in the group. In this case, the router keep a list of groupids and relay their interest to the distributing router.



- For example, in the above figure, router R_1 is the distributing router. There are two other multicast routers (R_2 and R_3) could be the recipients of router R in this network. Routers R_2 and R_3 may be distributors for some of these groups in other networks, but not on this network.
- **A- Joining a Group:** A host or a router can join a group. A host maintains a list of processes or applications that have membership in a group. When a process wants to join a new group, it sends its request to the host. If this is the first entry for this particular group, the host sends a membership report message. If this is not the first entry, there is no need to send the membership report since the host is already a member of the group.
- The IGMP protocol requires that the membership report be sent twice, one after the other within a few moments. In this way, if the first one is lost or damaged, the second one replaces it.
- **B- Leaving a Group:** When a host sees that no process is interested in a specific group, it sends a leave report. Similarly, when a router sees that none of the networks connected to its interfaces is interested in a specific group, it sends a leave report about that group.
- However, when a multicast router receives a leave report, it cannot immediately purge that group from its list because the report comes from just one host or router; there may be other hosts or routers that are still interested in that group.
- To make sure, the router sends a special query message and inserts the groupid, or multicast address, related to the group. The router allows a specified time for any host or router to respond. If, during this time, no interest (membership report) is received, the router assumes that there are no loyal members in the network and purges the group from its list.
- **C- Monitoring Membership:** A host or router can join a group by sending a membership report message. It can leave a group by sending a leave report message. However, sending these two types of reports is not enough. Consider the situation in which there is only one host interested in a group, but the host is shut down or removed from the system. The multicast router will never receive a leave report. To handle this situation, the multicast router is responsible for monitoring all the hosts or routers in a LAN to see if they want to continue their membership in a group.
- The router periodically (by default, every 125 s) sends a general query message. In this message, the group address field is set to 0.0.0.0. This means the query for membership continuation is for all groups in which a host is involved, not just one.
- The router expects an answer for each group in its group list; even new groups may respond. The query message has a maximum response time of 10 s. When a host or router receives the general query message, it responds with a membership report if it is interested in a group.
- However, if there is a common interest (two hosts, for example, are interested in the same group), only one response is sent for that group to prevent unnecessary traffic.

- This is called a delayed response.
- **D- Delayed Response:** To prevent unnecessary traffic, IGMP uses a delayed response strategy. When a host or router receives a query message, it does not respond immediately; it delays the response.
- Each host or router uses a random number to create a timer, which expires between 1 and 10s. A timer is set for each group in the list. For example, the timer for the first group may expire in 2 s, but the timer for the third group may expire in 5 s. Each host or router waits until its timer has expired before sending a membership report message.
- During this waiting time, if the timer of another host or router, for the same group, expires earlier, that host or router sends a membership report.
- Because the report is broadcast, the waiting host or router receives the report and knows that there is no need to send a duplicate report for this group; thus, the waiting station cancels its corresponding timer.

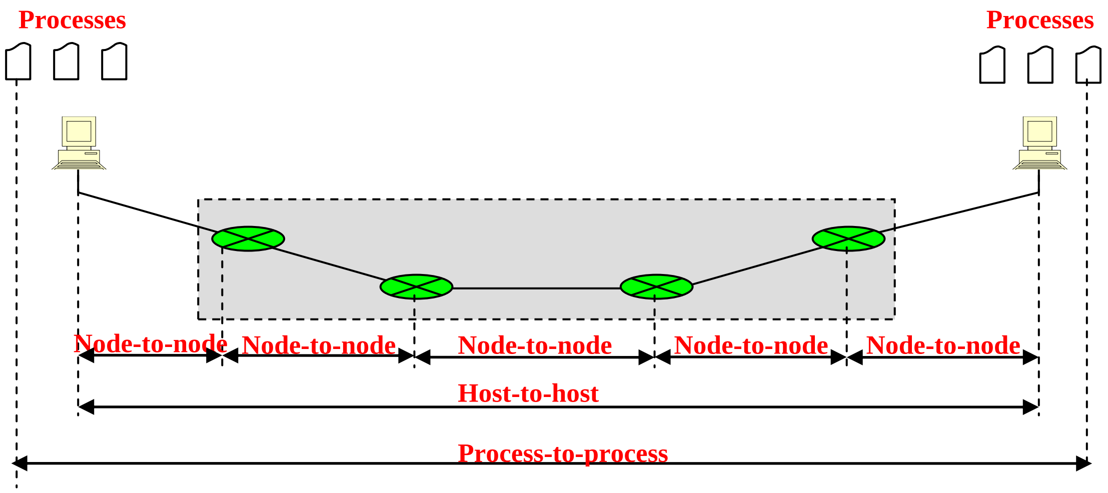


- **E- Query Router:** Query messages may create a lot of responses. To prevent unnecessary traffic, IGMP designates one router as the query router for each network. Only this designated router sends the query message, and the other routers are passive (they receive responses and update their lists).

UDP

I- Introduction:

- The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called node-to-node delivery.
- The network layer is responsible for delivery of datagrams between two hosts. This is called host-to-host delivery.
- Communication on the Internet is not defined as the exchange of data between two nodes or between two hosts. Real communication takes place between two processes (application programs). We need process-to-process delivery.
- We need a mechanism to deliver data from one of the processes running on the source host to the corresponding process running on the destination host.
- The transport layer is responsible for process-to-process delivery. Two processes communicate in a client/server relationship [1][13].

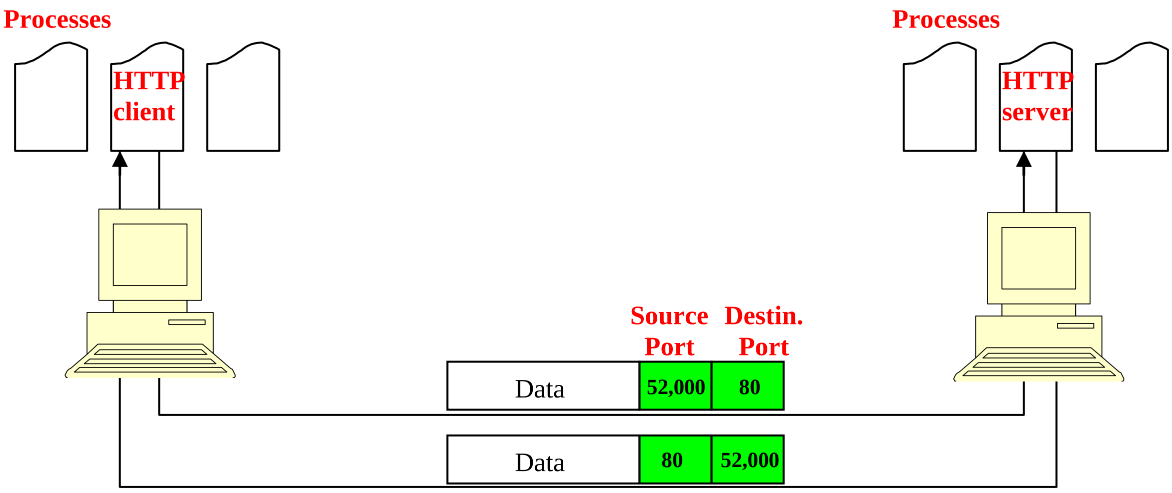


1- Client/Server Paradigm[1][5]:

- The most common way to achieve process-to-process delivery is the client/server paradigm. A process on the local host, called a client, needs services from a process usually on the remote host, called a server.
- Both processes (client and server) have the same name. For example, to get a web page from a remote machine, we need an HTTP client process running on the local host and an HTTP server process running on a remote machine.
- Operating systems today support both multiuser and multiprogramming environments.
- A remote computer can run several server programs at the same time, just as local computers can run one or more client programs at the same time.

2- Addressing[1][6]:

- Whenever we need to deliver something to one specific destination among many, we need an address.
- At the data link layer, we need a MAC address to choose one node among several nodes if the connection is not point-to-point.
- At the network layer, we need an IP address to choose one host among millions.
- At the transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host.
- In the Internet model, the port numbers are 16-bit integers between 0 and 65,535.
- The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral port number.
- The server process must also define itself with a port number. This port number, however, cannot be chosen randomly.
- The Internet has decided to use universal port numbers for servers; these are called well-known port numbers.
- There are some exceptions to this rule; for example, there are clients that are assigned well-known port numbers. Every client process knows the well-known port number of the corresponding server process. For example, while the HTTP client process, discussed above, can use an ephemeral (temporary) port number 52,000 to identify itself, the HTTP server process must use the well-known (permanent) port number 80.



3- IANA Ranges[1][7]:

- The IANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well known, registered, and dynamic (or private).
- 1- Well-known ports: The ports ranging from 0 to 1023 are assigned and controlled by IANA.

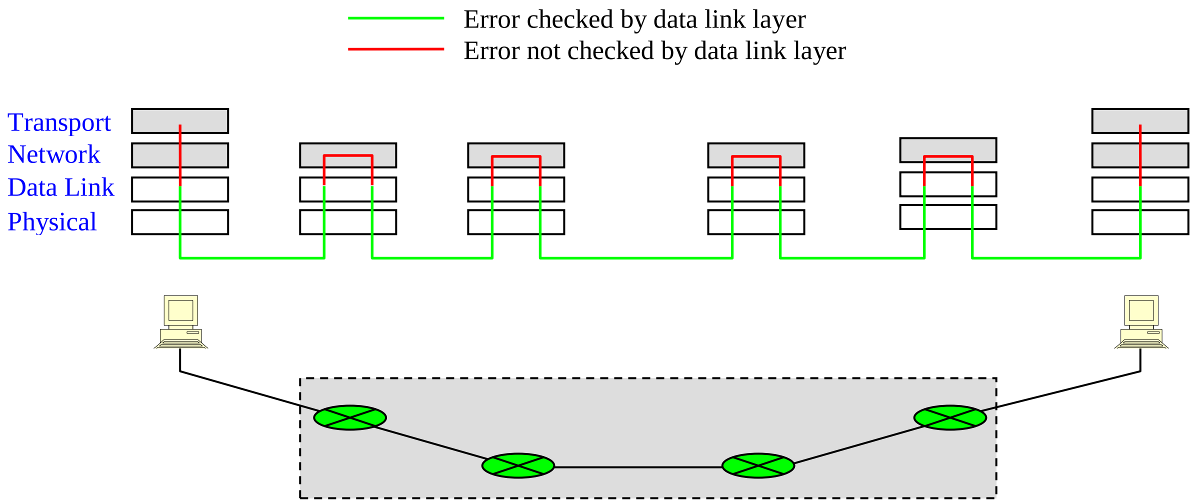
- 2- Registered ports: The ports ranging from 1024 to 49,151 are not assigned or controlled by IANA. They can only be registered (on demand) with IANA to prevent duplication.
- 3- Dynamic ports: The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process. These are the ephemeral ports.

4- Connectionless Versus Connection-Oriented Service[1][8]:

- A transport layer protocol can either be connectionless or connection-oriented.
- In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release. The packets may be delayed or lost or may arrive out of sequence. There is no acknowledgment either.
- UDP, is connectionless.
- In a connection-oriented service, a connection is first established between the sender and the receiver. Data are transferred in order. At the end, the connection is released.
- TCP and SCTP are connection-oriented protocols.

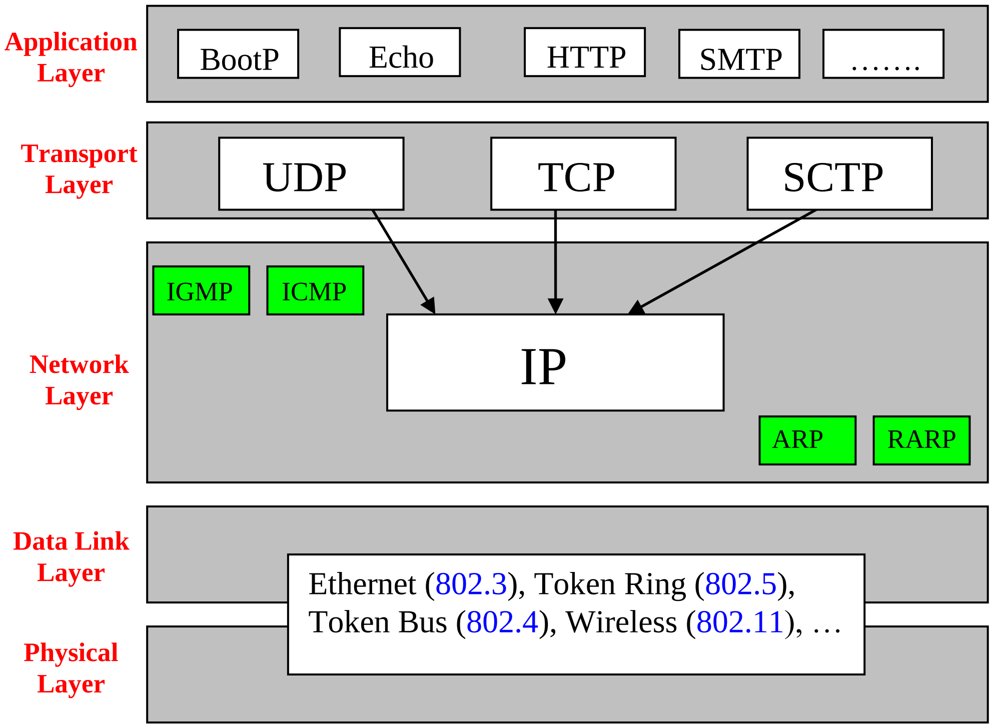
5- Reliable Versus Unreliable[1][12]:

- The transport layer service can be reliable or unreliable.
- If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer. This means a slower and more complex service.
- On the other hand, if the application program does not need reliability because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used.
- In the Internet, there are three common different transport layer protocols: UDP is connectionless and unreliable; TCP and SCTP are connection oriented and reliable.
- Why do we need error and flow control in the transport layer if the data link layer is reliable and has flow and error control? The answer is because the network layer in the Internet is unreliable (best-effort delivery).



6- Three Protocols[1][25][26][27]:

- The original TCP/IP protocol suite specifies two protocols for the transport layer: UDP and TCP. A new transport layer protocol, SCTP, has been designed.



II- USER DATAGRAM PROTOCOL (UDP) [1][18][25][26]:

- The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It performs very limited error checking.

- UDP is a very simple protocol using a minimum of overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP. Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP or SCTP.

1- Well-Known Ports for UDP:

- The next table shows some well-known port numbers used by UDP. Some port numbers can be used by both UDP and TCP.

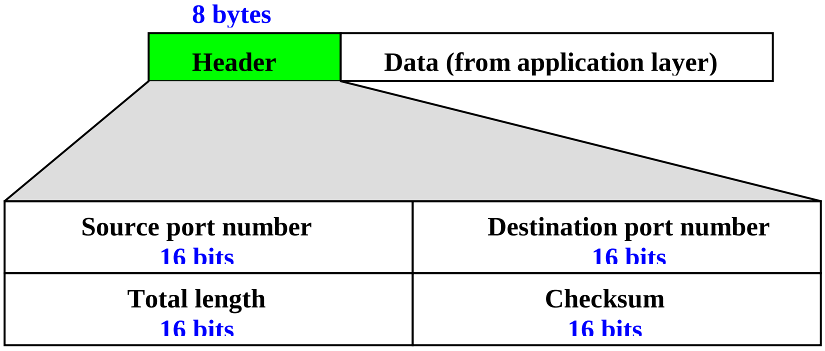
Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
11	Users	Active users
13	Daytime	Returns the date and the time
53	Nameserver	Domain Name Service
67	Bootps	Server port to download bootstrap information
68	Bootpc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
123	NTP	Network time protocol

- In LUNIX operating systems, the well-known ports are stored in a file called /etc/services. Each line in this file gives the name of the server and the well-known port number. We can use the grep utility to extract the line corresponding to the desired application. The following shows the port for FTP and HTTP. Note that FTP (or HTTP) can use port 21 (or 80) with either UDP, TCP or SCTP.

```
$grep ftp /etc/services
ftp         21/tcp
ftp         21/udp
ftp         21/sctp
…
$grep http /etc/services
http        80/tcp
http        80/udp
…
$grep sctp /etc/services
ftp         21/sctp
ssh         22/sctp
…
```

2- User Datagram

- UDP packets, called user datagrams, have a fixed-size header of 8 bytes.



- Source port number: This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535. If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.
- Destination port number: This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet.
- Length: This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be much less because a UDP user datagram is encapsulated in an IP datagram with a total length of 65,535 bytes.
- The length field in a UDP user datagram is actually not necessary because there is a field in the IP datagram that defines the total length and another field in the IP datagram that defines the length of the header (of IP datagram). So if we subtract the header length from the total length, we can deduce the length of a UDP datagram that is encapsulated in an IP datagram.
- However, the designers of the UDP protocol felt that it was more efficient for the destination UDP to calculate the length of the data from the information provided in the UDP user datagram rather than ask the IP software to supply this information.
- Checksum: This field is used to detect errors over the entire user datagram (header plus data).

3- UDP Operation:

1- Connectionless Services:

- UDP provides a connectionless service. This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program.
- The user datagrams are not numbered.

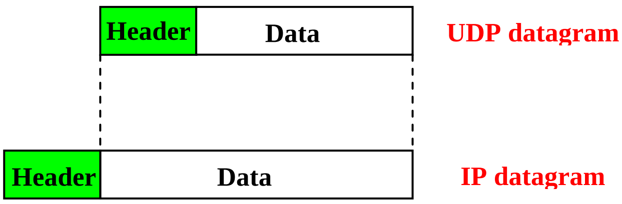
- Also, there is no connection establishment and no connection termination, as is the case for TCP. This means that each user datagram can travel on a different path.
- One of the ramifications (disadvantages) of being connectionless is that the process that uses UDP cannot send a stream of data to UDP and expect UDP to chop them into different related user datagrams. Instead each request must be small enough to fit into one user datagram. Only those processes sending short messages should use UDP.

2- Flow and Error Control:

- UDP is a very simple, unreliable transport protocol. There is no flow control and hence no window mechanism. The receiver may overflow with incoming messages.
- There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded.
- The lack of flow control and error control means that the process using UDP should provide these mechanisms.

3- Encapsulation and Decapsulation

- To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram.



4- Use of UDP:

- UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as ftp that needs to send bulk data.
- UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.
- UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
- UDP is used for management processes such as SNMP.
- UDP is used for some route updating protocols such as Routing Information Protocol (RIP).

Transport Layer: TCP

I- Introduction:

- The second transport layer is called Transmission Control Protocol (TCP).
- TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers.
- Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data.
- In addition, TCP is reliable; it uses flow and error control mechanisms at the transport level[1][25][26][27].

II- TCP Services [1][25][26][27]:

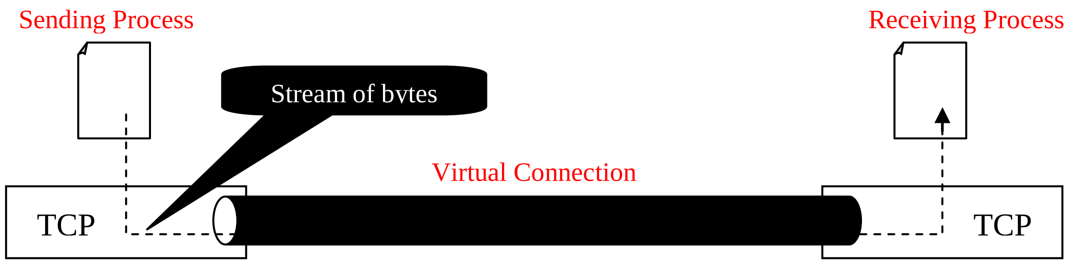
1- Process-to-Process Communication:

- Like UDP, TCP provides process-to-process communication using port numbers. The next table lists some well-known port numbers used by TCP:

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
11	Users	Active users
13	Daytime	Returns the date and the time
20	FTP (data)	File Transfer Protocol (data connection)
21	FTP (control)	File Transfer Protocol (control connection)
53	DNS	Domain Name Service
67	Bootp	port to download bootstrap information
80	HTTP	Hypertext Transfer Protocol

2- Stream Delivery Service:

- TCP, unlike UDP, is a stream-oriented protocol. In UDP, each message is called a user datagram and becomes, eventually, one IP datagram. Neither IP nor UDP recognizes any relationship between the datagrams.
- TCP, on the other hand, allows the sending process to deliver data as a stream of bytes (not segments) and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet.



2-1 Buffering:

- Because the sending and the receiving processes may not write or read data at the same speed, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction. These buffers are also necessary for flow and error control mechanisms used by TCP.

2-2 Segments:

- The IP layer, as a service provider for TCP, needs to send data in packets, not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment.
- TCP adds a header to each segment (for control purposes) and delivers the segment to the IP layer for transmission. The segments are encapsulated in IP datagrams and transmitted.
- This entire operation is transparent (not aware) to the receiving process. The segments may be received out of order, lost, or corrupted and resent. All these are handled by TCP with the receiving process unaware of any activities.

3- Full-Duplex Communication:

- TCP offers full-duplex service, in which data can flow in both directions at the same time. Each TCP then has a sending and receiving buffer, and segments move in both directions.

4- Connection-Oriented Service:

- TCP, unlike UDP, is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:

  1. The two TCPs establish a connection between them.

  2. Data are exchanged in both directions.

  3. The connection is terminated.

- Note that this is a virtual connection, not a physical connection. The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then resent. Each may use a different path to reach the destination.
- TCP creates a stream-oriented environment in which it accepts the responsibility of delivering the bytes in order to the other site.

5- Reliable Service:

- TCP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe and sound arrival of data.

III- TCP Features [1][25][26][27]:

- To provide the services mentioned in the previous section, TCP has several features that are discussed next.

1- Numbering System:

- Although the TCP software keeps track of the segments being transmitted or received, there is no field for a segment number value in the segment header. Instead, there are two fields called the sequence number and the acknowledgment number.

1-1 Byte Number:

- TCP numbers all data bytes that are transmitted in a connection. Numbering is independent in each direction.
- The numbering does not necessarily start from 0. Instead, TCP generates a random number between 0 and 2^{32} - 1 for the number of the first byte. For example, if the random number happens to be 1057 and the total data to be sent are 6000 bytes, the bytes are numbered from 1057 to 7056. The byte numbering is used for flow and error control.

1-2 Sequence Number:

- After the bytes have been numbered, TCP assigns a sequence number to each segment that is being sent. The sequence number for each segment is the number of the first byte carried in that segment.
- Example: Suppose a TCP connection is transferring a file of 5000 bytes. The first byte is numbered 10,00l. What are the sequence numbers for each segment if data are sent in five segments, each carrying 1000 bytes?

```
Segment 1 Sequence Number: 10,001 (range: 10,001 to 11,000)
Segment 2 Sequence Number: 11,001 (range: 11,001 to 12,000)
Segment 3 Sequence Number: 12,001 (range: 12,001 to 13,000)
Segment 4 Sequence Number: 13,001 (range: 13,001 to 14,000)
Segment 5 Sequence Number: 14,001 (range: 14,001 to 15,000)
```

2-3 Acknowledgment Number:

- Each party (sender or receiver) uses an acknowledgment number to confirm the bytes it has received.
- The acknowledgment number defines the number of the next byte that the party expects to receive.
- The acknowledgment number is cumulative, which means that the party takes the number of the last byte that it has received, safe and sound, adds 1 to it, and announces this sum as the acknowledgment number.
- Example: if a party uses 5643 as an acknowledgment number, it has received all bytes from the beginning up to 5642. Note that this does not mean that the party has received 5642 bytes because the first byte number does not have to start from 0.

2- Flow Control:

- TCP, unlike UDP, provides flow control. The receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overwhelmed with data. The numbering system allows TCP to use a byte-oriented (not segment-oriented) flow control.

3- Error Control:

- To provide reliable service, TCP implements an error control mechanism. Although error control considers a segment as the unit of data for error detection (loss or corrupted segments), error control is byte-oriented.

4- Congestion Control:

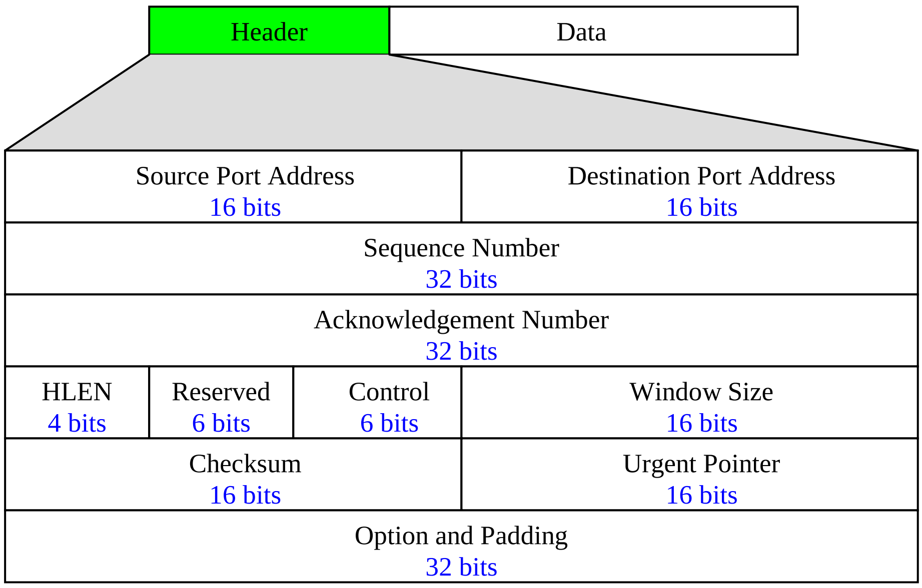
- TCP, unlike UDP, takes into account congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control), but is also determined by the level of congestion in the network.

IV- Segment[1][24][26][27]:

- The segment consists of a 20- to 60-byte header, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options.

1- Format:

- The format of a segment is shown as follows:



- Source port address: This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP header.
- Destination port address: This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP header.
- Sequence number: This 32-bit field defines the number assigned to the first byte of data contained in this segment.
- Acknowledgment number: This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number x from the other party, it defines x + 1 as the acknowledgment number. Acknowledgment and data can be piggybacked together.
- Header length: This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 (5 x 4 =20) and 15 (15 x 4 =60).
- Reserved: This is a 6-bit field reserved for future use.
- Control: This field defines 6 different control bits or flags. These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP.

Flag	Description
URG (bit # 1)	The value of the urgent pointer field is valid
ACK (bit # 2)	The value of the acknowledgement field is valid
PSH (bit # 3)	Push the data
RST (bit # 4)	Reset the connection
SYN (bit # 5)	Synchronize sequence numbers during connection
FIN (bit # 6)	Terminate the connection

- Window size: This field defines the size of the window, in bytes, that the other party must maintain. Note that the length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes. This value is normally referred to as the receiving window (rwnd) and is determined by the receiver. The sender must obey the dictation of the receiver in this case.
- Checksum: This 16-bit field contains the checksum. The calculation of the checksum for TCP follows the same procedure as the one described for UDP (header + data). However, the inclusion of the checksum in the UDP datagram is optional, whereas the inclusion of the checksum for TCP

is mandatory. In addition, the only action taken in UDP in case of an error is discarding the datagram while in TCP an error control mechanism is launched.

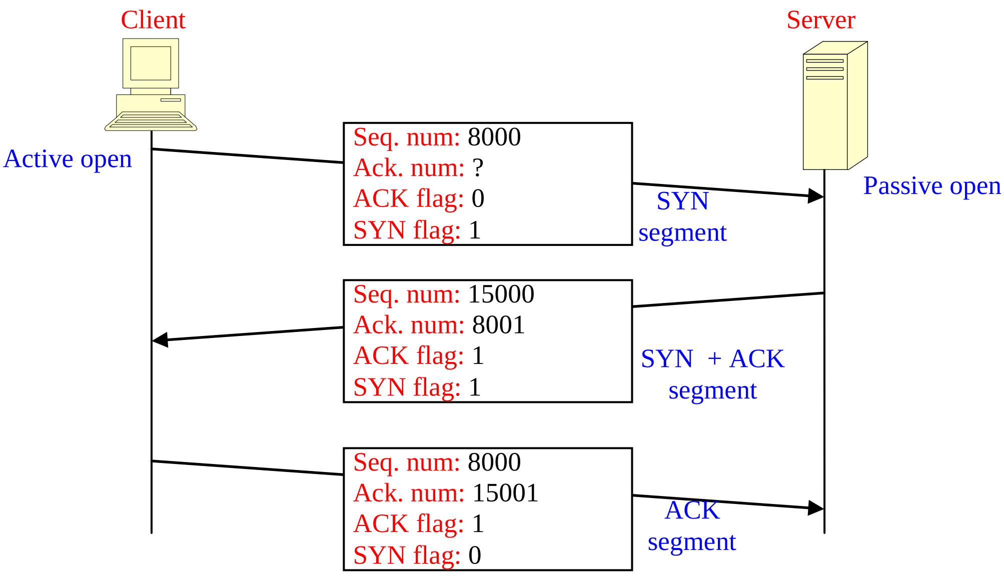
- Urgent pointer: This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.
- Options: There can be up to 40 bytes of optional information in the TCP header.

V- A TCP Connection[1][25][26][27]:

- TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgment process as well as retransmission of damaged or lost frames.
- How TCP, which uses the services of IP, a connectionless protocol, can be connection-oriented. The point is that a TCP connection is virtual, not physical. TCP operates at a higher level. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted.
- Unlike TCP, IP is unaware of this retransmission. If a segment arrives out of order, TCP holds it until the missing segments arrive; IP is unaware of this reordering.
- In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.

1- Connection Establishment:

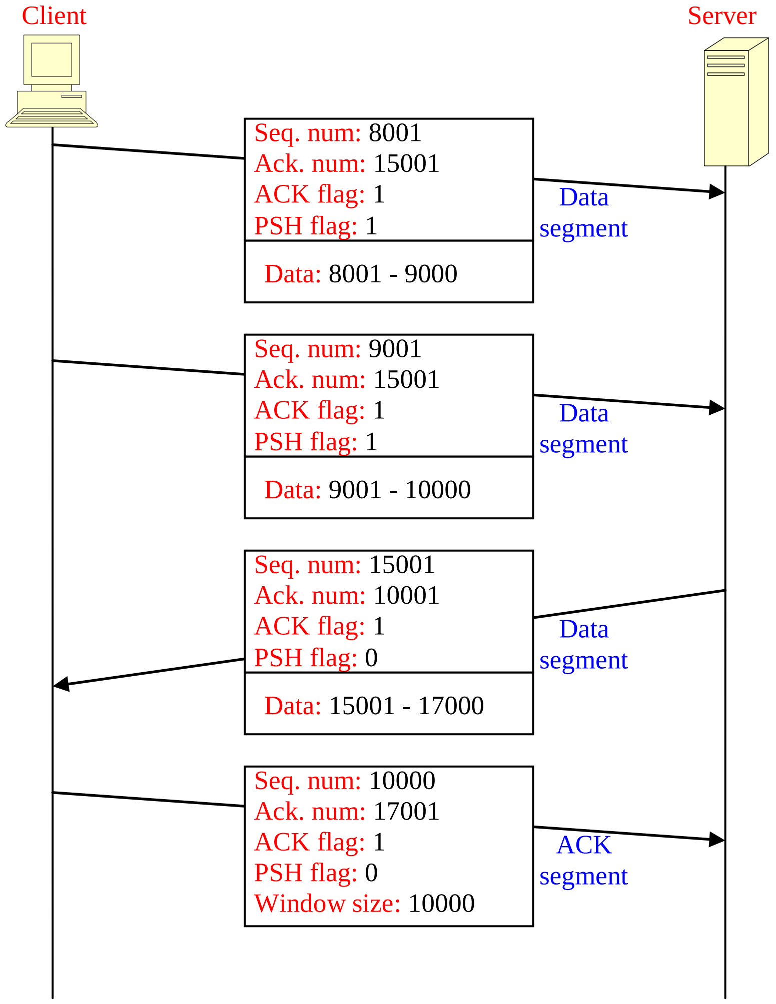
- TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.
- The connection establishment in TCP is called three way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.
- The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a passive open. Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection itself.
- The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process as shown next.



- Step 1: The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing 1 imaginary byte.
- Step 2: The server sends the second segment, a SYN +ACK segment, with 2 flag bits set: SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgment for the received SYN segment. It consumes one sequence number.
- Step 3: The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers.
- SYN Flooding Attack: The connection establishment procedure in TCP is susceptible to a serious security problem called the SYN flooding attack. This happens when a malicious attacker sends a large number of SYN segments to a server, pretending that each of them is corning from a different client by faking the source IP addresses in the datagrams.
- The server, assuming that the clients are issuing an active open, allocates the necessary resources, such as creating communication tables and setting timers. The TCP server then sends the SYN +ACK segments to the fake clients, which are lost. During this time, however, a lot of resources are occupied without being used. If, during this short time, the number of SYN segments is large, the server eventually runs out of resources and may crash. This SYN flooding attack belongs to a type of security attack known as a denial-of-service attack, in which an attacker monopolizes a system with so many service requests that the system collapses and denies service to every request.

2- Data Transfer [1][13][14]

- After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgments. We will study the rules of
- The acknowledgment is piggybacked with the data.



- In the example above, after connection is established (not shown in the figure), the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment.
- The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there are no more data to be sent. Note the values of the sequence and acknowledgment numbers. The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.
- The segment from the server, on the other hand, does not set the push flag. Most TCP implementations have the option to set or not set this flag.
- Pushing Data: We saw that the sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The receiving TCP

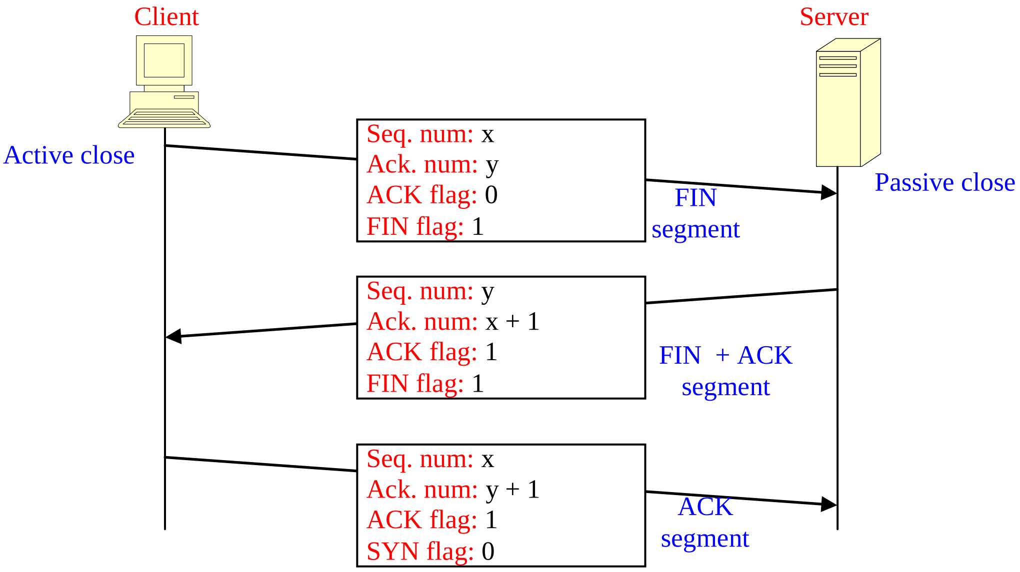
also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP.

- However, on occasion the application program has no need for this flexibility. For example, consider an application program that communicates interactively with another application program on the other end. The application program on one site wants to send a keystroke to the application at the other site and receive an immediate response. Delayed transmission and delayed delivery of data may not be acceptable by the application program.
- TCP can handle such a situation. The application program at the sending site can request a push operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.
- Urgent Data: On occasion an application program needs to send urgent bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program. As an example, suppose that the sending application program is sending data to be processed by the receiving application program. When the result of processing comes back, the sending application program finds that everything is wrong. It wants to abort the process, but it has already sent a huge amount of data. If it issues an abort command (control +C), these two characters will be stored at the end of the receiving TCP buffer. It will be delivered to the receiving application program after all the data have been processed.
- The solution is to send a segment with the URG bit set. The sending application program tells the sending TCP that the piece of data is urgent. The sending TCP creates a segment and inserts the urgent data at the beginning of the segment. The rest of the segment can contain normal data from the buffer. The urgent pointer field in the header defines the end of the urgent data and the start of normal data.
- When the receiving TCP receives a segment with the URG bit set, it extracts the urgent data from the segment, using the value of the urgent pointer, and delivers them, out of order, to the receiving application program.

3- Connection Termination[1][13][14]:

- Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client.
- Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

3-1 Three-Way Handshaking:

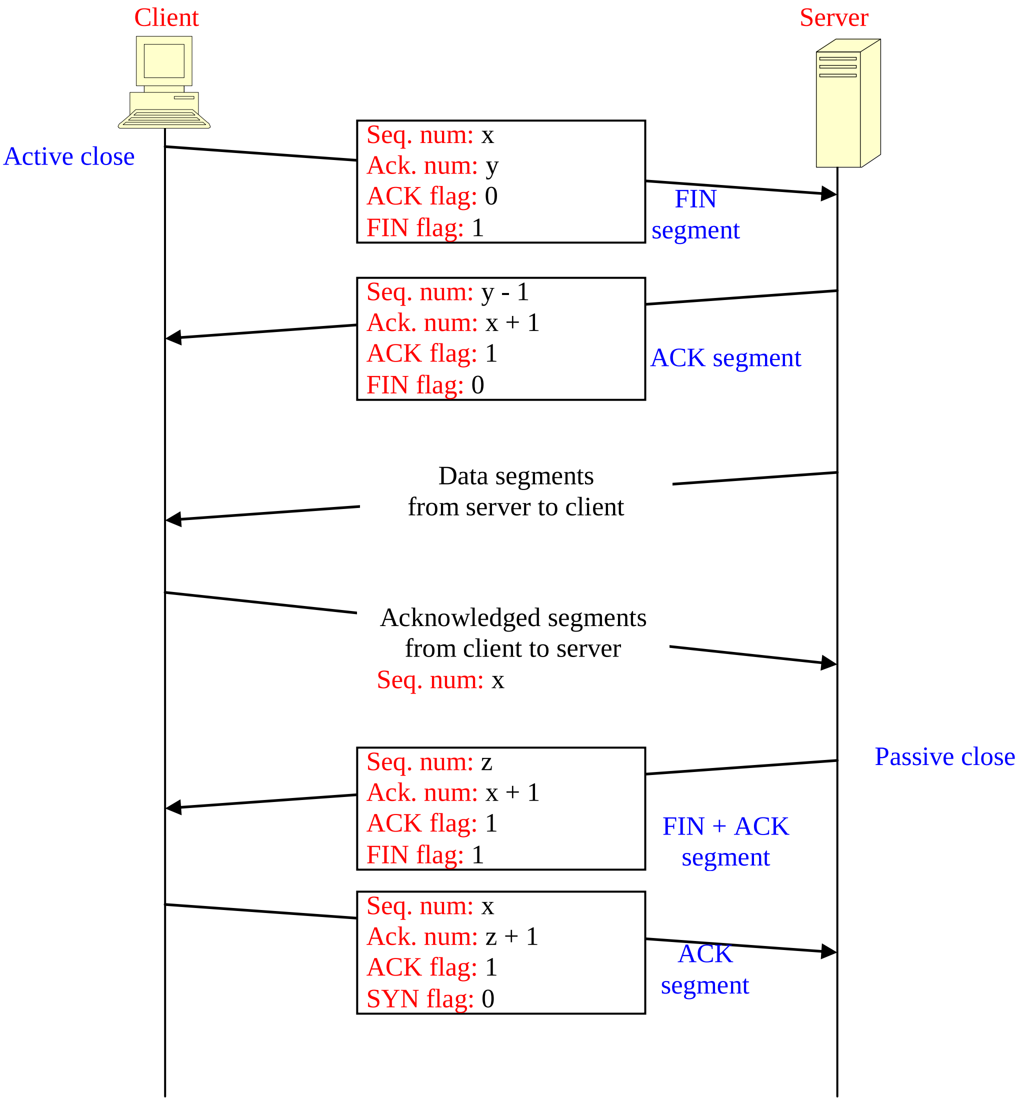


- Step 1: In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set.
- Note that a FIN segment can include the last chunk of data sent by the client, or it can be just a control segment. If it is only a control segment, it consumes only one sequence number.
- Step 2: The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.
- Step 3: The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers.

3-2 Half-Close :

- In TCP, one end can stop sending data while still receiving data. This is called a half-close. Although either end can issue a half-close, it is normally initiated by the client. It can occur when the server needs all the data before processing can begin.
- A good example is sorting. When the client sends data to the server to be sorted, the server needs to receive all the data before sorting can start. This means the client, after sending all the data, can close the connection in the outbound direction. However, the inbound direction must remain open to receive the sorted data.

- The server, after receiving the data, still needs time for sorting; its outbound direction must remain open.



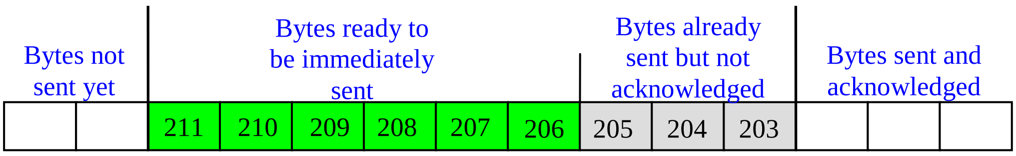
- Step 1: The client half-closes the connection by sending a FIN segment.
- Step2: The server accepts the half-close by sending the ACK segment.
- Step 3: The data transfer from the client to the server stops. The server, however, can still send data. When the server has sent all the processed data, it sends a FIN segment, which is acknowledged (Step 4) by an ACK from the client.
- After half-closing of the connection, data can travel from the server to the client and acknowledgments can travel from the client to the server. The client cannot send any more data to the server.
- Note the sequence numbers we have used. The second segment (ACK) consumes no sequence number. Although the client has received sequence number y - 1 and is expecting y, the server sequence number is still y - 1.

- When the connection finally closes, the sequence number of the last ACK segment is still x, because no sequence numbers are consumed during transmission in that direction.

3- Flow Control [1][24]

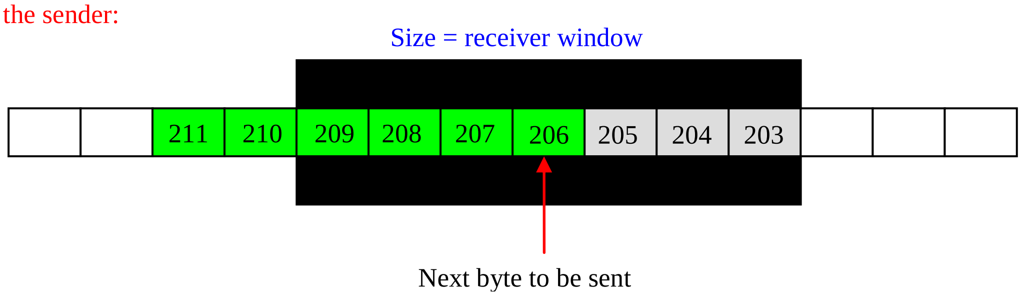
- TCP uses a sliding window to handle flow control.
- The sliding window protocol used by TCP, however, is something between the Go-Back-N and Selective Repeat sliding window.
- The sliding window protocol in TCP looks like the Go-Back-N protocol because it does not use NAKs.
- It looks like Selective Repeat because the receiver holds the out-of-order segments until the missing ones arrive.
- There are two big differences between this sliding window and the one we used at the data link layer. First, the sliding window of TCP is byte-oriented; the one we discussed in the data link layer is frame-oriented. Second, the TCP's sliding window is of variable size; the one we discussed in the data link layer was of fixed size.

At the sender:



- The sender window is always less than or equal to the receiver window.
- The window spans a portion of the buffer containing bytes received from the process. The bytes inside the window are the bytes that can be in transit; they can be sent without worrying about acknowledgment.

At the sender:



3-1 Deciding the receiver window:

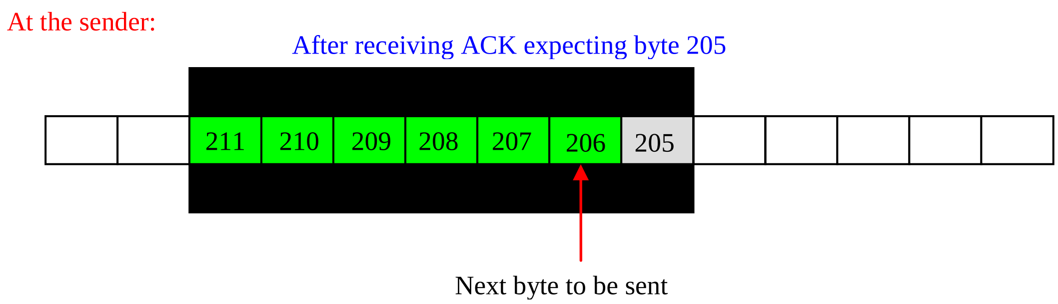
- The receiver window is variable. It depends on two factors: the size of the buffer and the processed bytes:
- Receiver window size = buffer size – unprocessed data.
- Example: What is the value of the receiver window (rwnd) for host A if the receiver, host B, has a buffer size of 5000 bytes and 1000 bytes of received and unprocessed data?
- Solution: The value of rwnd =5000 - 1000 = 4000. Host B can receive only 4000 bytes of data before overflowing its buffer. Host B advertises this value in its next segment to A.

3-2 Deciding the sender window:

- We know that the sender's window is always lesser than the receiver window. Yet, another factor must be taken in consideration: congestion. The sender can get information about congestion in the network and decide its window size.
- Sender window size = minimum (receiver window size, congestion window size).

3-3 Sliding the sender window:

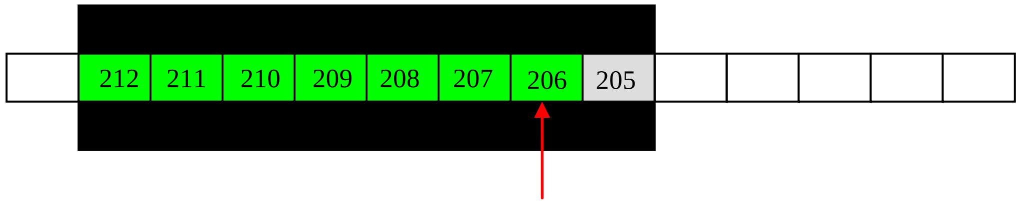
- Once the receiver verifies the integrity of the received bytes, it sends an acknowledgement (could be piggybacked) to the sender with the number of the expected byte.



3-4 Expanding the sender window:

- If the receiver process consumes data faster than it receives, the size of the receiver window expands.
- In this case, the receiver updates the window size field in the TCP header with the new size and sends it to the sender in the next TCP segment.

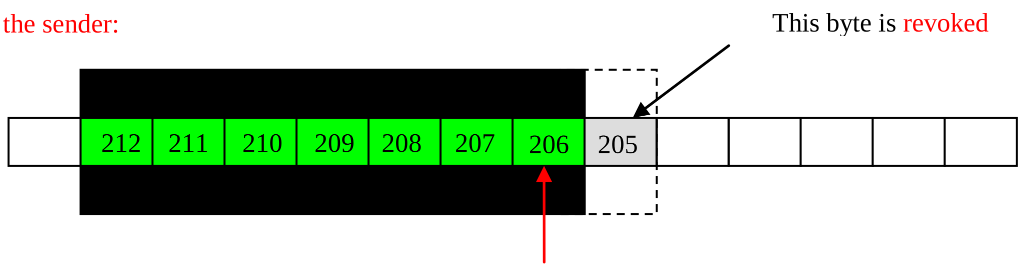
At the sender:



3-5 Shrinking the sender window:

- If the receiver process consumes data slower than it receives, the size of the receiver window shrinks.
- In this case, the receiver updates the window size field in the TCP header with the new size and sends it to the sender in the next TCP segment.
- Shrinking is not recommended since some bytes can be revoked from being acknowledged:

At the sender:



3-2 Closing the sender window:

- If the buffer of the receiver is full, it sets the window size to be zero and informs the sender. In this case the sender recess sending bytes until receiving a non-zero window size.

4- Error Control [1][24][27]:

- TCP is reliable: it handles error control using timers, acknowledgements and retransmissions.
- TCP has no negative acknowledgement.
- There are three cases

4-1 Lost or corrupted segment and lost acknowledgment:

- Once the receiver checks the integrity of a segment and finds it corrupted, it simply discards it.
- The sender sets a timer for each segment. If an acknowledgement is received for this segment or for any of its successors than the timer is destroyed and the segment is considered safe.
- If the timer goes off before receiving an acknowledgement, the sender consider that the segment was lost or corrupted. In this case, it retransmits the segment and sets its timer.

- On the other hand, if an acknowledgement is lost, then the sender's timer goes off and the corresponding segment is retransmitted.

4-2 Duplicate segment and acknowledgement:

- If an acknowledgement for a segment is delayed and arrived after retransmitting the segment, the sender consider it as the real acknowledgment, and ignore any other duplicates.
- In this case, the receiver also might receive a duplicate segment of bytes. Then, by checking the sequence number of the segment, it knows that it has been already acknowledged, so it simply discards it.

4-3 Out-of-order segments:

- TCP used an unreliable IP service that guarantees no order of the transmitted datagrams.
- TCP handles this problem by delaying the acknowledgement of a segment until receiving its predecessors.

Chapter 5. Wireless local area networks (WIF)

Wireless LANs

- Wireless communication is one of the fastest-growing technologies.
- The demand for connecting devices without the use of cables is increasing everywhere.
- Wireless LANs can be found on college campuses, in office buildings, and in many public areas.
- **IEEE 802.11 wireless LANs** is one of the promising wireless technologies for LANs [1][29].

I- IEEE 802.11[1][29]:

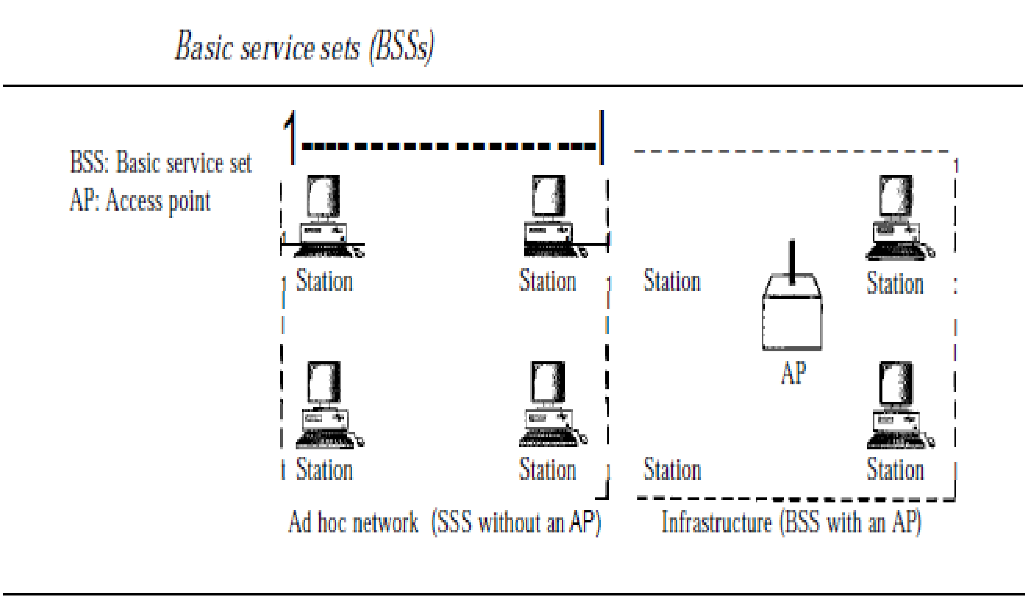
- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

1- Architecture [1][30]:

- The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

a) Basic Service Set:

- IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). The following figure shows two sets in this standard.



- The BSS without anAP is a stand-alone network and cannot send data to other BSSs.It is called an ad hoc architecture. In this architecture, stations can form a networkwithout the need of an AP;

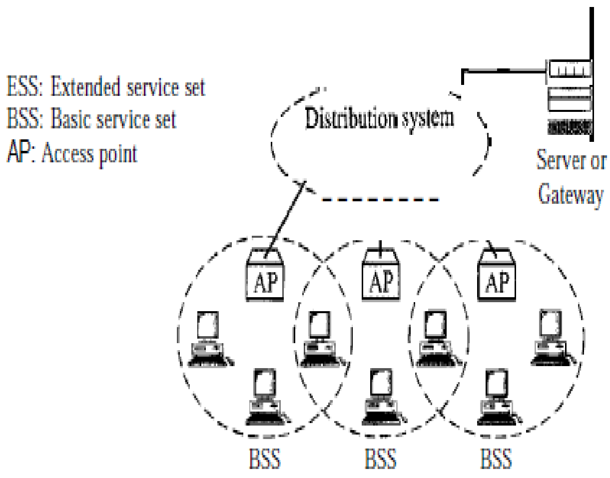
they can locate one another and agree to be part of a BSS. ABSS with an AP is sometimes referred to as an infrastructure network.

- A BSS without an AP is called an ad hoc network;
- A BSS with an AP is called an infrastructure network.

b) Extended Service Set:

- An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.
- The following figure shows an ESS.

Extended service sets (ESSs)



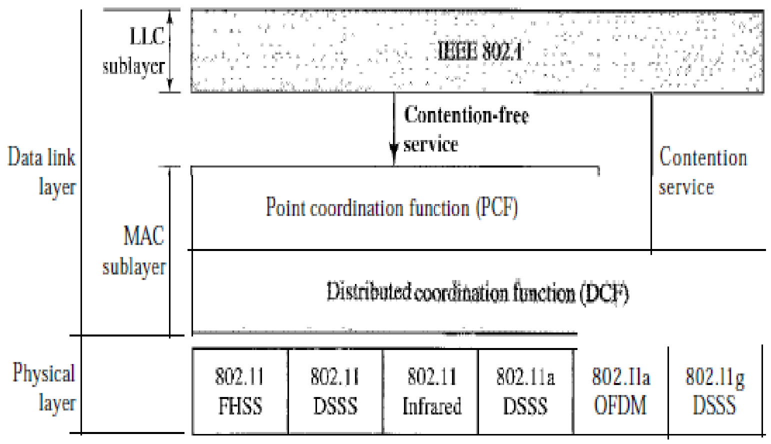
- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

2- MAC Sublayer [1][30][31][32]:

- IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).

- The following figure shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer.

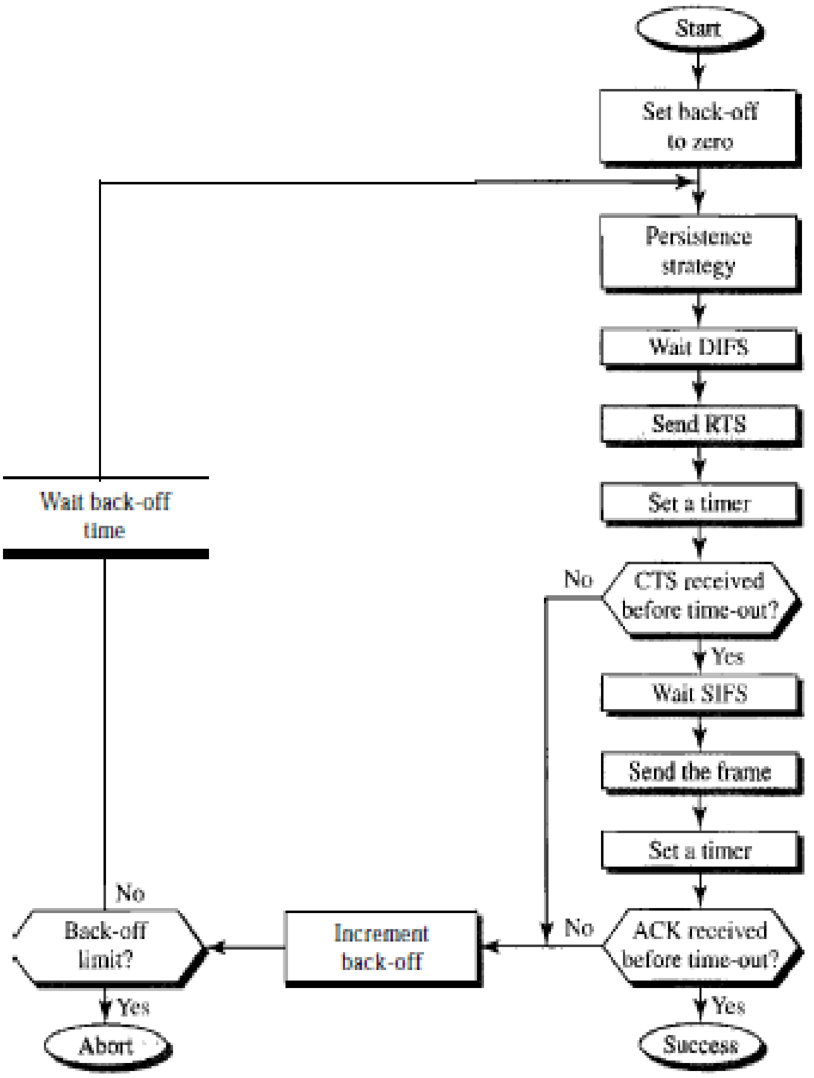
MAC layers in IEEE 802.11 standard



a) Distributed Coordination Function:

- One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses CSMAICA as the access method. Wireless LANs cannot implement CSMAfCD for three reasons:
  - ✓ For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.
  - ✓ Collision may not be detected because of the hidden station problem.
  - ✓ The distance between stations can be great. Signal fading could prevent a station atone end from hearing a collision at the other end.
- The following figure shows the process flowchart for CSMAICA as used in wireless LANs.

CSMAICA flowchart



- ✓ 1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

  a. The channel uses a persistence strategy with back-off until the channel is idle.

  b. After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

- ✓ 2. After receiving the RTS and waiting a period of time called the short interframespace (SIFS), the destination station sends a control frame, called the clear tosend (CTS), to the source station. This control frame indicates that the destinationstation is ready to receive data.

- ✓ 3. The source station sends data after waiting an amount of time equal to SIFS.
- ✓ 4. The destination station, after waiting an amount of time equal to SIFS, sends anacknowledgment to show that the frame has been received. Acknowledgment isneeded in this protocol because the station does not have any means to check forthe successful arrival of its data at the destination. On the other hand, the lack ofcollision in CSMA/CD is a kind of indication to the source that data have arrived.

II- Medium Access Control Protocols [1][33][34]:

- Schedule-based: Establish transmission schedules statically or dynamically.
  - ✓ TDMA
  - ✓ FDMA
  - ✓ CDMA
- Contention-based:
  - ✓ Let the stations contend for the channel
  - ✓ Random access protocols
- Reservation-based:
  - ✓ Reservations made during a contention phase
  - ✓ Size of packet in contention phase much smaller than a data Packet
  - ✓ CDMA
- Space-division multiple access:
  - ✓ Serve multiple users simultaneously by using directional antennas

1- Schedule-based access methods:

- FDMA (Frequency Division Multiple Access).
  - ✓ assign a certain frequency to a transmission channel between a sender and a receiver.
  - ✓ permanent (e.g., radio broadcast), slow hopping (e.g., GSM), fast hopping (FHSS, Frequency Hopping Spread Spectrum).
- TDMA (Time Division Multiple Access)
  - ✓ assign the fixed sending frequency to a transmission channel between a sender and a receiver for a certain amount of time.
- CDMA (Code Division Multiple Access)
  - ✓ signals are spread over a wideband using pseudo-noise sequences.
  - ✓ codes generate signals with “good-correlation” properties.
  - ✓ signals from another user appear as “noise”.
  - ✓ the receiver can “tune” into this signal if it knows the pseudo random number, tuning is done via a correlation function.

2- Contention-based protocols

- Aloha
- CSMA (Carrier-sense multiple access)
- MACA (Multiple access collision avoidance)
- MACAW
- CSMA/CA and IEEE 802.11

III- Ingredients of MAC Protocols [1][30][35][36]:

- Carrier sense (CS)
  - ✓ Hardware capable of sensing whether transmission taking place in vicinity.
- Collision detection (CD)
  - ✓ Hardware capable of detecting collisions
- Collision avoidance (CA)
  - ✓ Protocol for avoiding collisions
- Acknowledgments
  - ✓ When collision detection not possible, link-layer mechanism for identifying failed transmissions
- Backoff mechanism
  - ✓ Method for estimating contention and deferring transmissions

1- Carrier Sense Multiple Access

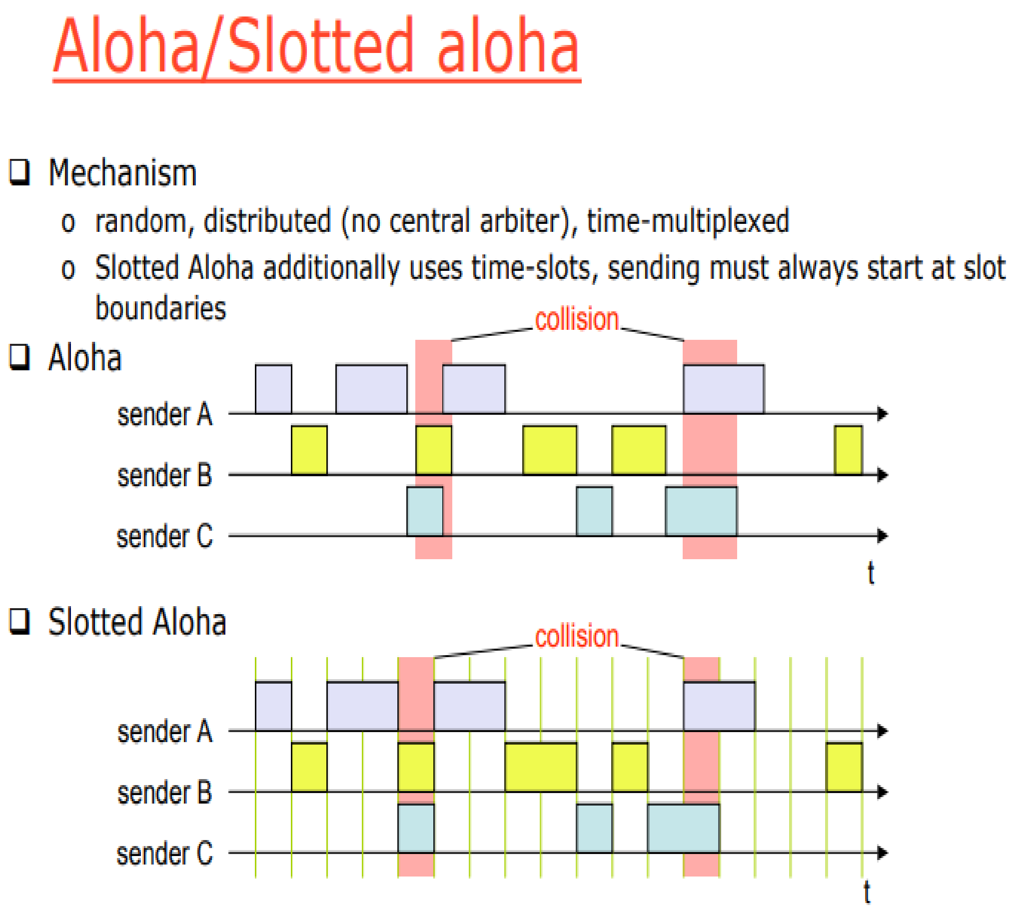
- Every station senses the carrier before transmitting
- If channel appears free
  - ✓ Transmit (with a certain probability)
- Otherwise, wait for some time and try again
- Different CSMA protocols:
  - ✓ Sending probabilities
  - ✓ Retransmission mechanisms

2- Aloha

- Proposed for packet radio environments where every node can hear every other node
- Assume collision detection
- In Slotted Aloha, stations transmit at the beginning of a slot
- If collision occurs, then each station waits a random number of slots and retries

- ✓ Random wait time chosen has a geometric distribution
- ✓ Independent of the number of retransmissions

- Analysis in standard texts on networking theory



IV- WLAN topology [1][30][31]:

- **Wireless Local Area Network (WLAN) topology** refers to the arrangement or structure of interconnected devices and their communication paths within a wireless network.

1- Infrastructure Mode:

- In infrastructure mode, wireless clients connect via an **Access Point (AP)**.
- **Key terminology:**
  a. **Basic Service Set (BSS):** A single AP interconnecting all associated wireless clients.
  b. **Basic Service Area (BSA):** The area covered by an AP's signal.
  c. **Basic Service Set Identifier (BSSID):** Unique identifier for the AP (usually derived from its MAC address).
  d. **Service Set Identifier (SSID):** Human-readable identifier used by the AP to advertise its wireless service.

e. **Distribution System (DS):** Wired connection (e.g., Ethernet) between APs and the network infrastructure.

f. **Extended Service Set (ESS):** Multiple BSSs interconnected via a common DS.

2- Independent Basic Service Set (IBSS) (Ad Hoc Mode):

- IBSS connects two devices wirelessly in a peer-to-peer manner without an AP.
- No other wireless devices are needed.
- Not suitable for large-scale networks (limited scalability).

3- Mesh Topology:

- Common in modern WLANs.
- APs form a mesh network, allowing dynamic routing and redundancy.
- No central AP; each AP communicates with neighboring APs.
- Useful for large coverage areas and self-healing networks.

References

[1] B. A. Forouzan, Data Communications and Networking (McGraw-Hill Forouzan Networking). McGraw-Hill Higher Education, 2007.

[2] R. K. Rao Yarlagadda, Analog and Digital Signals and Systems, Springer Nature, 2010

[3] Bellamy, J. Digital Telephony. New York, NY: Wiley, 2000.

[4] Bergman, J. Digital Baseband Transmission and Recording. Boston, MA: Kluwer, 1996.

[5] Couch, L. Digital and Analog Communication Systems. Upper Saddle River, NJ: Prentice Hall, 2000.

[6] Blahut, R. Algebraic Codes for Data Transmission. Cambridge, UK: Cambridge University Press, 2003.

[7] Comer, D. Computer Networks. Upper Saddle River, NJ: Prentice Hall, 2004.

[8] Kurose, 1. and Ross, K. Computer Networking. Reading, MA: Addison-Wesley, 2005.

[9] orouzan, B. Local Area Networks. New York, NY: McGraw-Hill, 2003.

[10] Perlman, R. Interconnection: Bridges, Routers, Switches, and Intemet-working Protocols. Reading, MA: Addison-Wesley, 2000.

[11] Peterson, L., and Davie B. Computer Networks: A Systems Approach. San Francisco, CA: Morgan, Kaufmans, 2000.

[12] Pieprzyk, J., Hardjono, T, and Seberry, J, Fundamentals of Computer Security. Berlin, Germany: Springer, 2003.

[13] Stallings, W. Data And Computer Communications. Upper Saddle River, NJ: Prentice Hall, 2004.

[14] Pearson, J. Basic Communication Theory. Upper Saddle River, NJ: Prentice Hall,' 1992.

[15] Drozdek, A. Elements of Data Compression. Brooks/Cole Thomson Learning, 2003.

[16] Wittmann, R. and Zitterbart, M. Multicast Communication. San Francisco, CA: Morgan, Kaufmans, 2001.

[17] Andrew S. Tanenbaum, Computer Networks. Pearson, Third edition, 1996

[18] Andrew S. Tanenbaum, Computer Networks. Prentice Hall, Fourth edition, 2002
[19] Cheswick, W., Bellovin, S., and Rubin, A. Firewalls and Internet Security. Reading, MA: Addison-Wesley, 2003.
[20] Comer, D. Internetworking with TCPlIp, Volume 1: Principles, Protocols, and Architecture. Upper Saddle River, NJ: Prentice Hall, 2000.
[21] Sauders, S. Gigabit Ethernet Handbook. New York, NY: McGraw-Hill, 1998.
[22] Black, U. QoS In Wide Area Network. Upper Saddle River, NJ: Prentice Hall,2000.
[23] Warland, J. and Varaiya, P. High Peiformance Communication Networks. San Francisco, CA: Morgan, Kaufmans, 2000.
[24] Bishop, M. Computer Security. Reading, MA: Addison-Wesley, 2003.
[25] Forouzan, B. TCPIIP Protocol Suite. New York, NY: McGraw-Hill, 2006.
[26] Stevens, W. TCPIIP Illustrated, Volume 1. Upper Saddle River, NJ: Prentice Hall, 2000.
[27] Stevens, W. TCPIIP Illustrated, Volume 3. Upper Saddle River, NJ: Prentice Hall, 2000.
[28] Albitz, P. and Liu, C. DNS and BIND. Sebastopol, CA: O'Reilly, 1998.
[29] Agrawal D. and Zeng, Q. Introduction to Wireless and Mobile Systems. Pacific Grove, CA, NJ: Brooks/Cole Thomson Learning, 2003.
[30] Schiller, B. Mobile Communications. Reading, MA: Addison-Wesley, 2003.
[31] Stallings, W. Wireless Communications and Networks. Upper Saddle River, NJ: Prentice Hall, 2002.
[32] Barr, T, Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall, 2002
[33] Doraswamy, H. and Harkins, D. IPSec. Upper Saddle River, NJ: Prentice Hall,2003.
[34] Dutcher, D. The NAT Handbook. New York, NW: Wiley, 2001.
[35] Mao, W. Modem Cryptography. Upper Saddle River, NJ: Prentice Hall, 2004.
[36] Maxwell, K. Residential Broadband. New York, NY: Wiley, 2003.