SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ECE

COMPUTER COMMUNICATION – SCSA1305

COURSE OBJECTIVES

- ➢ To understand the basics of communication
- ➢ To impart knowledge on basics of analog and digital communication.
- ➢ To analyze the data communication models and understand how to employ.
- ➢ To explore the various layers and its functionalities in data communication model.

UNIT I BASICS OF COMMUNICATION 9Hrs.

Introduction to Communication systems – basic model, point to point, broadcast communication; modulation-need for modulation, types of modulation, Base band and Pass band transmission; Demodulation (detection) – Coherent and Non-coherent detection; Noise – types of noise; Analog to Digital Conversion (ADC) process– Sampling , Quantization and Coding; Sampling theorem, types of sampling – ideal, natural and flat –top sampling; nyquist rate, Signal reconstruction, types of quantization, Quantization noise, Aliasing.

UNIT 2 ANALOG AND DIGITAL COMMUNICATION 9Hrs.

Amplitude modulation – types of amplitude modulation- Standard AM with Full Carrier, Comparison of different amplitude modulations; Angle modulation (FM and PM), FM generation using PM, PM generation using FM, Comparison of Narrowband and Wideband FM, Comparison of AM,FM and PM.

Analog pulse modulation – PAM, PWM, PPM; Digital pulse modulation – Pulse Code Modulation (PCM), Delta modulation (DM), Adaptive Delta modulation (ADM), Multiplexing – Frequency Division Multiplexing (FDM), Time Division Multiplexing.

UNIT 3 INTRODUCTION TO DATA COMMUNICATION AND OSI MODEL 9Hrs.

Introduction to computer communication: Transmission modes - Switching: circuit switching and packet switching, OSI model, Layers in OSI model, TCP/IP protocol suite.

Physical Layer: Guided and unguided transmission media (Co-axial cable, UTP,STP, Fiber optic cable), Data Link

Layer: Framing, Flow control (stop and wait , sliding window flow control) ,Error control, HDLC, Media access control: Ethernet (802.3), CSMA/CD, Logical link control, Wireless LAN (802.11), CSMA/CA.

UNIT 4 NETWORK LAYER COMPONENTS AND FUNCTIONS 9Hrs.

Network Layer Logical addressing: IPv4 & IPV6, Subnetting, DHCP, Virtual LAN, Networking devices (Hubs, Bridges

& Switches), Network topologies.

Routing: Routing and Forwarding, Static routing and Dynamic routing, Routing Algorithms: Distance vector routing algorithm, Link state routing (Dijkstra's algorithm), Routing Protocols: Routing Information protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), MPLS.

UNIT 5 TRANSPORT, SESSION AMD APPLICATION LAYER 9Hrs.

Transport Layer –UDP, TCP, Congestion Control & Quality of Service – Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics, Application Layer – DNS, Remote Logging (Telnet), SMTP, FTP, WWW, HTTP, POP3, MIME, SNMP

Total : 45 Hrs.

COURSE OUTCOME

CO1: Describe the essential basics of communication

CO2: Classify different types of analog and digital modulation schemes

CO3: Comprehend the need of data communication models

CO4: Identify the required network layer components and functions

CO5: Analyze the various protocols required in various layers

CO6: Acquire the needs for building a communication mod

TEXT / REFERENCE BOOKS:

1. William Stallings, Data and Computer Communications, 10th Edition, Pearson, 2014.

2. Wayne Thomasi, "Advanced Electronic Communication Systems", 6th Edition, PHI Publishers, 2003.

3. Simon Haykins, “Communication Systems” John Wiley, 5th Edition, March 2009.

4. John G. Proakis, MasoudSalehi, “Digital Communication”, McGraw Hill 5th edition November 6, 2007.

5. Bernard Sklar, “Digital Communication, Fundamentals and Application”, Pearson Education Asia, 2nd

Edition, Jan. 21, 2001.

6. Behrouz A. Forouzen, “Data communication and Networking”, Fourth Edition, Tata McGraw – Hill, 2011.

7. Andrew S.Tanenbaum, “Computer Networks”, 5th Edition, Pearson, 2011.

END SEMESTER EXAM QUESTION PAPER PATTERN

Max. Marks : 100 Exam Duration : 3 Hrs.

PART A : 10 Questions of 2 marks each-No choice **20 Marks**

PART B :2 Questions from each unit with internal choice, each carrying 16 Marks **80 Marks**

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ECE

UNIT1-BASICS OF COMMUNICATION – SCSA1305

UNIT I BASICS OF COMMUNICATION

Introduction to Communication systems basic model, point to point, broadcast communication; modulation-need for modulation, types of modulation, Base band and Pass band transmission; Demodulation (detection) - Coherent and Noncoherent detection; Noise types of noise; Analog to Digital Conversion (ADC) process Sampling , Quantization and Coding; Sampling theorem, types of sampling ideal, natural and flat top sampling; nyquist rate, Signal reconstruction, types of quantization, Quantization noise, Aliasing.

1.1 Introduction to Electronic Communication Systems

•Communication is the process of establishing connection or link between two points for information exchange or Communication is simply the basic process of exchanging information.

•The electronic equipment which are used for communication purpose, are called communication equipment. Different communication equipment when assembled together form a communication system.

•Typical example of communication system are line telephony and line telegraphy, radio telephony and radio telegraphy, radio broadcasting, point-to-point communication and mobile communication, computer communication, radar communication, television broadcasting, radio telemetry, radio aids to navigation, radio aids to aircraft landing etc.

1.1 Block Diagram of Communication System

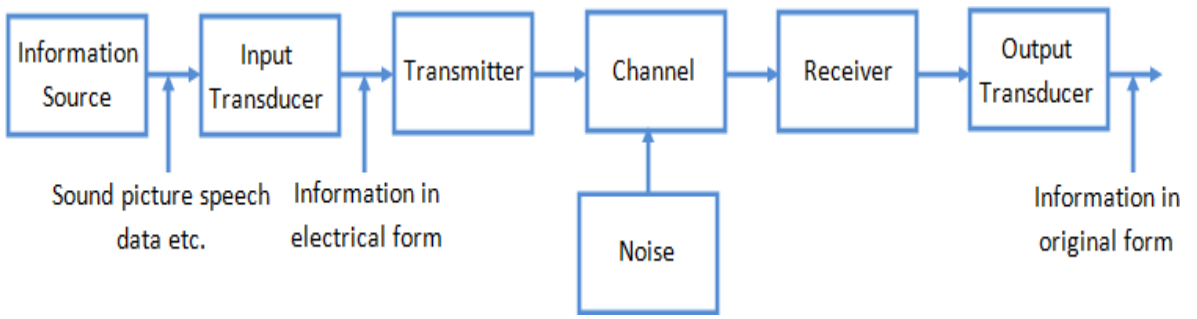


Figure 1.1 ***Block Diagram of Communication System***

Information Source

As we know, a communication system serves to communicate a message or information. This information originates in the information source.

- In general, there can be various messages in the form of words, group of words, code, symbols, sound signal etc. However, out of these messages, only the desired message is selected and communicated.
- Therefore, we can say that the function of information source is to produce required message which has to be transmitted.

Input Transducer

- A transducer is a device which converts one form of energy into another form. The message from the information source may or may not be electrical in nature.
- In a case when the message produced by the information source is not electrical in nature, an input transducer is used to convert it into a time- varying electrical signal.
- For example, in case of radio-broadcasting, a microphone converts the information or massage which is in the form of sound waves into corresponding electrical signal.

Transmitter.

- The function of the transmitter is to process the electrical signal from different aspects. It does modulation and amplification of the signal to be transmitted.
- In the modulation process, some parameter of the carrier wave (such as amplitude, frequency or phase) is varied in accordance with the modulating signal . This modulated signal is then transmitted by the transmitter. The modulating signal is nothing but the baseband signal or information signal while the carrier is a high frequency sinusoidal signal. In the process of modulation the carrier wave actually carries the information signal from the transmitter to receiver .
- For example in radio broadcasting the electrical signal obtained from sound signal, is processed to restrict its range of audio frequencies (upto 5 kHz in amplitude modulation radio broadcast) and is often amplified, modulated and then given to antenna for radiation in to space. In wire telephony, no real processing is needed. However, in long-distance radio communication, signal amplification is necessary before modulation.
- Modulation is the main function of the transmitter. In modulation, the message signal is superimposed upon the high-frequency carrier signal. All these processing of the message signal are done just to ease the transmission of the signal through the channel.

Channel and the Noise

- The term channel means the medium through which the message travels from the transmitter to the receiver. In other words, we can say that the function of the channel is to provide a physical connection between the transmitter and the receiver. There are two types of channels, namely point-to-point channels and broadcast channels.
- Example of point-to-point channels is wire lines, microwave links and optical fibres. Wire-lines operate by guided electromagnetic waves and they are used for local telephone transmission. In case of microwave links, the transmitted signal is radiated as an electromagnetic wave in

free space. Microwave links are used in long distance telephone transmission.

- An optical fibre is a low-loss, well-controlled, guided optical medium. Optical fibres are used in optical communications. Although these three channels operate differently, they all provide a physical medium for the transmission of signals from one point to another point. Therefore, for these channels, the term point-to-point is used.
- On the other hand, the broadcast channel provides a capability where several receiving stations can be reached simultaneously from a single transmitter. An example of a broadcast channel is a satellite in geostationary orbit, which covers about one third of the earth‟s surface.
- Noise is an unwanted signal which tends to interfere with the required signal During the process of transmission and reception the signal gets distorted due to noise introduced in the system.. Noise signal is always random in character. Noise may interfere with signal at any point in a communication system. However, the noise has its greatest effect on the receiver.

Receiver

- The main function of the receiver is to reproduce the message signal in electrical form from the distorted received signal. This reproduction of the original signal is accomplished by a process known as the demodulation or detection. Demodulation is the reverse process of modulation carried out in transmitter.

Destination

- Destination is the final stage which is used to convert an electrical message signal into its original form. For example in radio broadcasting, the destination is a loudspeaker which works as a transducer i.e. converts the electrical signal in the form of original sound signal.

Types of Communication

- Broadcast
- Point-to-point

Broadcast:

A method of sending a signal where multiple parties may hear a single sender. Radio stations are a good example of every day life "Broadcast Network". In this example, you can see a single station is broadcasting a message to multiple locations that may or may not be able to hear it, and if they are able to hear it, may choose to listen or not.

Point-to-point:

A method of communication where one "point" (person orentity) speaks to another entity.

1.2 Periodic signals in the time and frequency domain

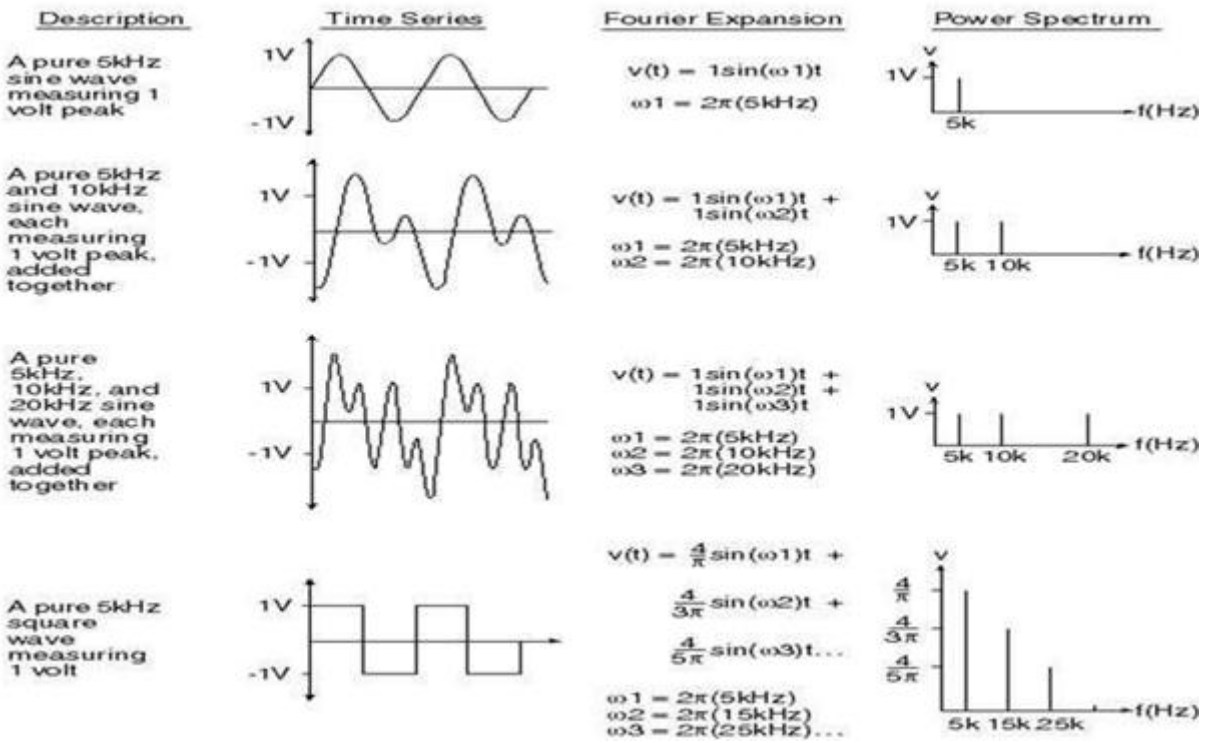


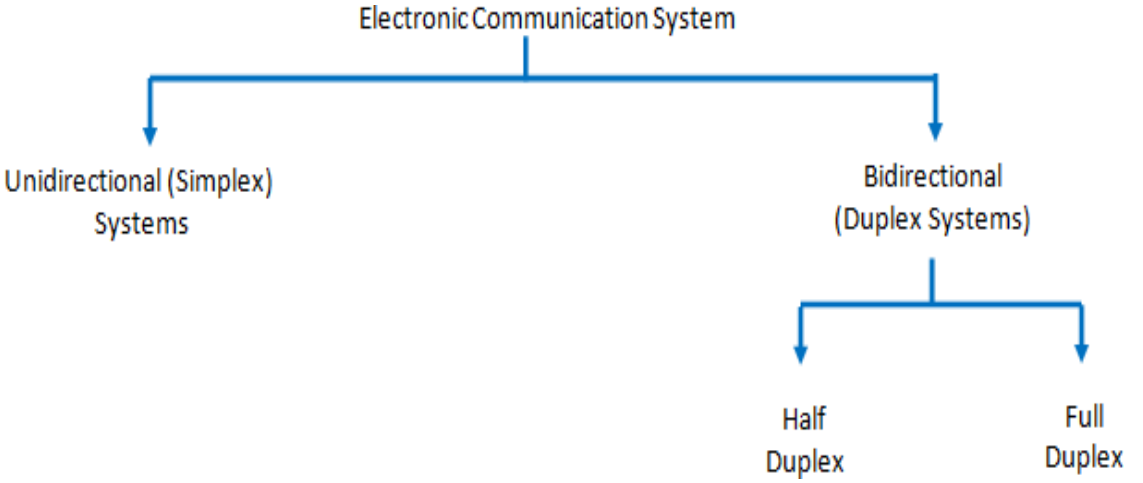
Figure 1.2 ***Periodic signals in the time and frequency domain***

Classification Based on Direction of Communication

- Based on whether the system communicates only in one direction or otherwise
- The communication systems are classified as under:
  - Simplex System
  - Half duplex System
  - Full duplex System

Fundamental Limitations in Communications

Limitations Due to Technological Problems



•Hardware availability

•Economic factors

•International and national regulating norms

Fundamental Physical Limitations

•Available transmission bandwidth, level of noise generated in the electronic system, atmospheric conditions and maximum capacity of the channel used for communication puts a limit of the rate of information exchange. The impact of each of these factors are given below

Transmission Bandwidth(B)

Limits the spectrum of the transmitted signal, i.e. the maximum speed of variation of the transmitted signal. The time required for transmission of a given amount of information is inversely proportional to the transmission bandwidth B.

Noise

Noise is generated in all conductors and in electronic devices as well. Noises generated in electronic systems(Thermal, shot, flicker, popcorn, avalanche noise) degrades the signal quality or fidelity in analog communication systems and produces errors in digital communications. Noise generation limits the weakest transmitted signal. Its impact is significant in long-distance communications when the signal attenuation is large. A measure of noise level is Signal-to-noise ratio (S/N) given by

Channel capacity (C) Hartley-Shannon law or channel capacity theorem states that the rate of information transmission cannot exceed the channel capacity C.

$C=B \log(1+S/N)$

Modulation and Demodulation

In the modulation process, some parameter of the carrier wave (such as amplitude, frequency or phase) is varied in accordance with the modulating signal . This modulated signal is then transmitted by the transmitter. The modulating signal is nothing but the baseband signal or information signal while the carrier is a high frequency sinusoidal signal. In the process of modulation the carrier wave actually carries the information signal from the transmitter to receiver .The receiver demodulates the received modulated signal and gets the original information signal back. Thus, demodulation is exactly opposite to modulation .

Terms to remember:

•Modulating signal – represents the message.

•Carrier wave – High frequency signal on which message is imposed through modulation process. Usually the modulating signal is much slower than the carrier wave.

•Modulation – altering one or more of the parameters (amplitude, frequency, phase, pulse width) of the carrier in correspondence with the modulating signal.

•Demodulation – extraction of modulating signal from modulated signal;

reverse operation to modulation.

•Continuous wave modulation – when the carrier is sinusoidal

•Pulse modulation – the carrier is pulse train

Analog and Digital Communications

Analog

•In analog communication systems, the message signals are transmitted in analog form itself. AM, FM and PM are common analog modulation schemes which uses sinusoidal carrier signal.

•In pulse modulation systems such as PAM, PWM and PPM, the carrier signal is a pulse train but the message signal is in analog form.

•Therefore PAM, PWM and PPM are also called as analog modulation schemes. They are generally not used for wireless communications.

Digital

•In digital communication systems, the analog information is converted to digital binary data (ones and zeros) using Analog to digital convertor ICs.

•Then the binary data is modulated with a sinusoidal carrier and transmitted. Amplitude shift keying (ASK), Frequency shift keying (FSK) and Phase shift keying(PSK) are some digital modulation schemes.

Advantages of Digital Communication over analog communication

1.Digital is more robust than analog to noise and interference†

2.Digital is more viable to using regenerative repeaters

3.Digital hardware more flexible by using microprocessors and VLSI

4.Can be coded to yield extremely low error rates with error correction

5.Easier to multiplex several digital signals than analog signals

6.Digital is more efficient in trading off SNR for bandwidth

7.Digital signals are easily encrypted for security purposes

8.Digital signal storage is easier, cheaper and more efficient

9.Reproduction of digital data is more reliable without deterioration

10.Cost is coming down in digital systems faster than in analog systems and DSP algorithms are growing in power and flexibility

Need for modulation

The answer is that the baseband transmission has many limitations which can be overcome using modulation . It is explained below.

Advantages of Modulation

The process of modulation provides the following benefits:

- Reduction in the height of antenna
- Avoids mixing of signals
- Increases the range of communication
- Multiplexing is possible
- Improves quality of the signal

1.Reduction in the height of antenna

For the transmission of radio signals, the antenna height must be multiple of

$\lambda/4$,where λ is the wavelength .

$\lambda = c / f$

where c : is the velocity of light

f: is the frequency of the signal to be transmitted.

2.Avoids mixing of signals

If the baseband sound signals are transmitted without using the modulation by more than one transmitter, then all the signals will be in the same frequency range i.e. 0 to 20 kHz . Therefore, all the signals get mixed together and a receiver cannot separate them from each other. Hence, if each baseband sound signal is used to modulate a different carrier then they will occupy different slots in the frequency domain (different channels). Thus, modulation avoids mixing of signals.

Example : FM stations broadcasting at different carrier frequencies.

3.Increase the Range of Communication

The frequency of baseband signal is low, and the low frequency signals cannot travel long distance when they are transmitted. They get heavily attenuated. The attenuation reduces with increase in frequency of the transmitted signal, and they travel longer distance. The modulation process increases the frequency of the signal to be transmitted. Therefore, it increases the range of communication.

4.Multiplexing is possible

Multiplexing is a process in which two or more signals can be transmitted over the same communication channel simultaneously. This is possible only with modulation. The multiplexing allows the same channel to be used by many signals.

Hence, many TV channels can broadcast simultaneously without getting mixed with each other as they use different carrier frequencies. It is referred to as frequency division multiplexing.

5.Improves Quality of Reception

With frequency modulation (FM) and the digital communication techniques such as PCM, the effect of noise is reduced to a great extent. This improves quality of reception.

Analog signal

•An analog signal is any continuous signal for which the time-varying feature (variable) of the signal is a representation of some other time- varying quantity, i.e., analogous to another time-varying signal

•Examples of analog signals are Human voice, Thermometer, Analog phones etc

•An analog communication system is a communication system where the information signal sent from point A to point B can only be described as an analog signal.

•An example of this is ALICE speaking to BOB over the telephone

1.3 MODULATION

Modulation is performed at the transmitting end of the communication system.At the receiving end of the system we usually require the original baseband signal to be restored, this is usually accomplished by using a process known as demodulation which is the reverse process of the modulation. In basic signal processing terms, we thus find that the transmitter of an analog communication system consists of a modulator and the receiver consists of a demodulator

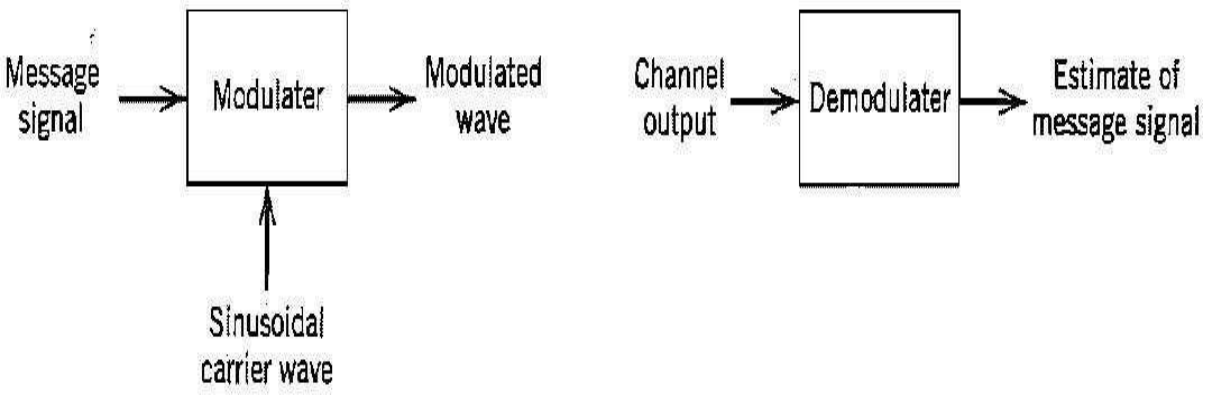


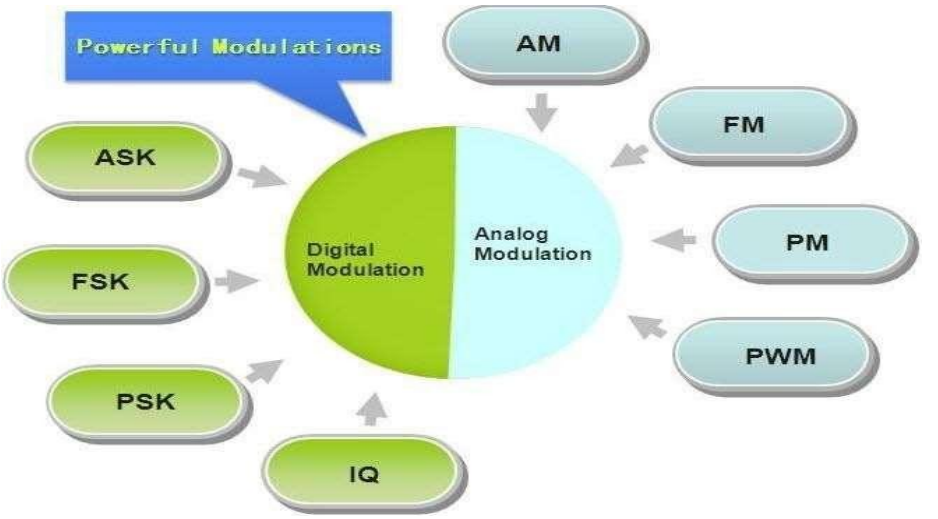
Figure 1.3 ***MODULATION BLOCK DIAGRAM***

Types of modulation

•There are various types of modulation techniques used for transmitting information. If the carrier is sinusoidal, then its amplitude, frequency or phase is changed in accordance with the modulating signal to obtain AM, FM or PM respectively. These are continuous wave modulation systems.

•Analog modulation can be pulsed modulation as well. Here the carrier is in the form of rectangular pulse. The amplitude, width or position of the carrier pulses is varied in accordance with the instantaneous value of modulating signal to obtain the PAM, PWM or PPM outputs.

•Some commonly used analog and digital modulation techniques are outlined below in figure 13, 14 and15. AM, FM, PM, PAM, PWM and PPM are analog modulation schemes. ASK, FSK and PSK are digital modulation schemes.



1.4 Frequency modulation

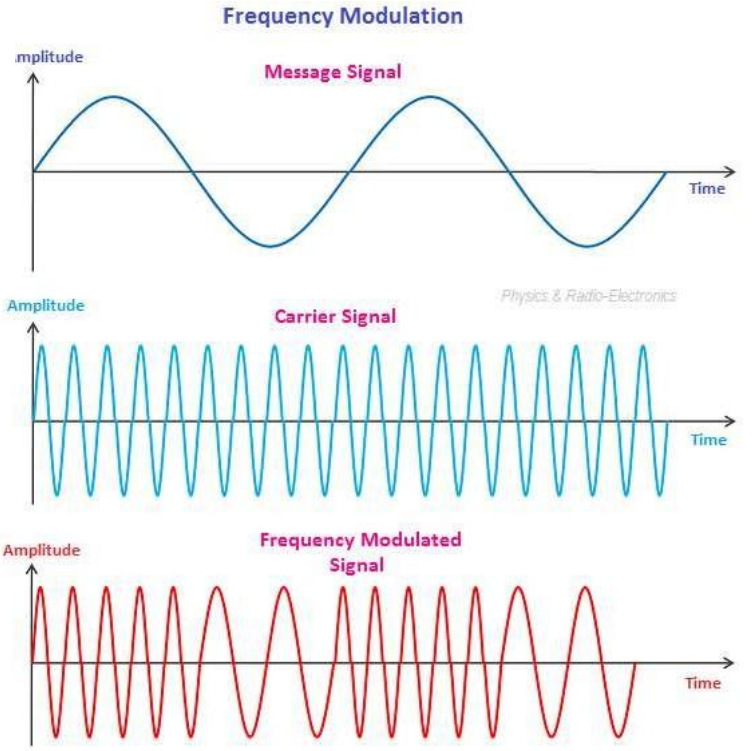
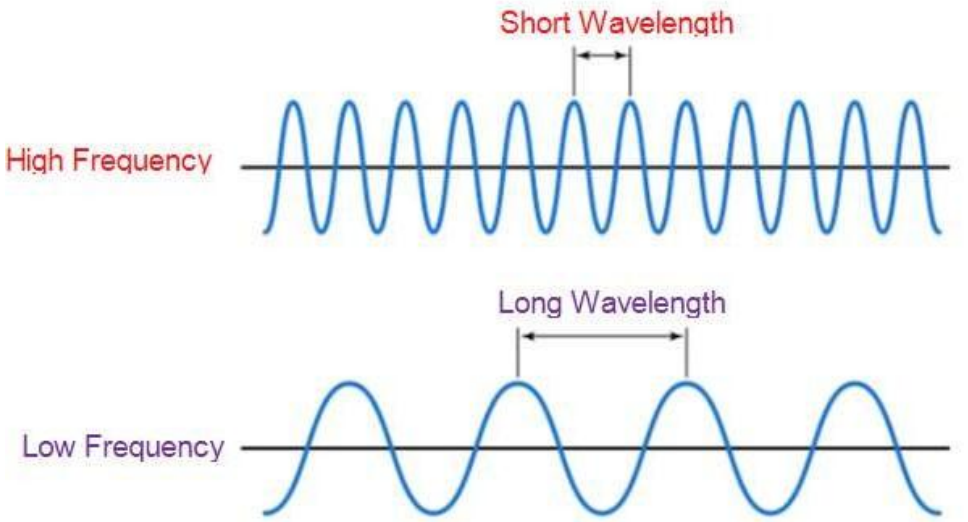


Figure 1.4 ***FREQUENCY MODULATION***

Short Wavelength = High Frequency (More Waves In The Same Time Frame



$$\text{Wavelength} = \frac{\text{Speed of light}}{\text{Frequency}}$$

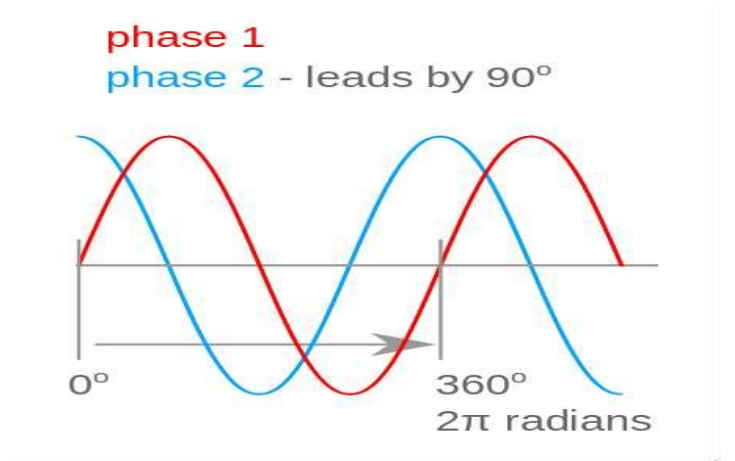


Figure 1.5 Amplitude Modulation

1.6 Phase Modulation

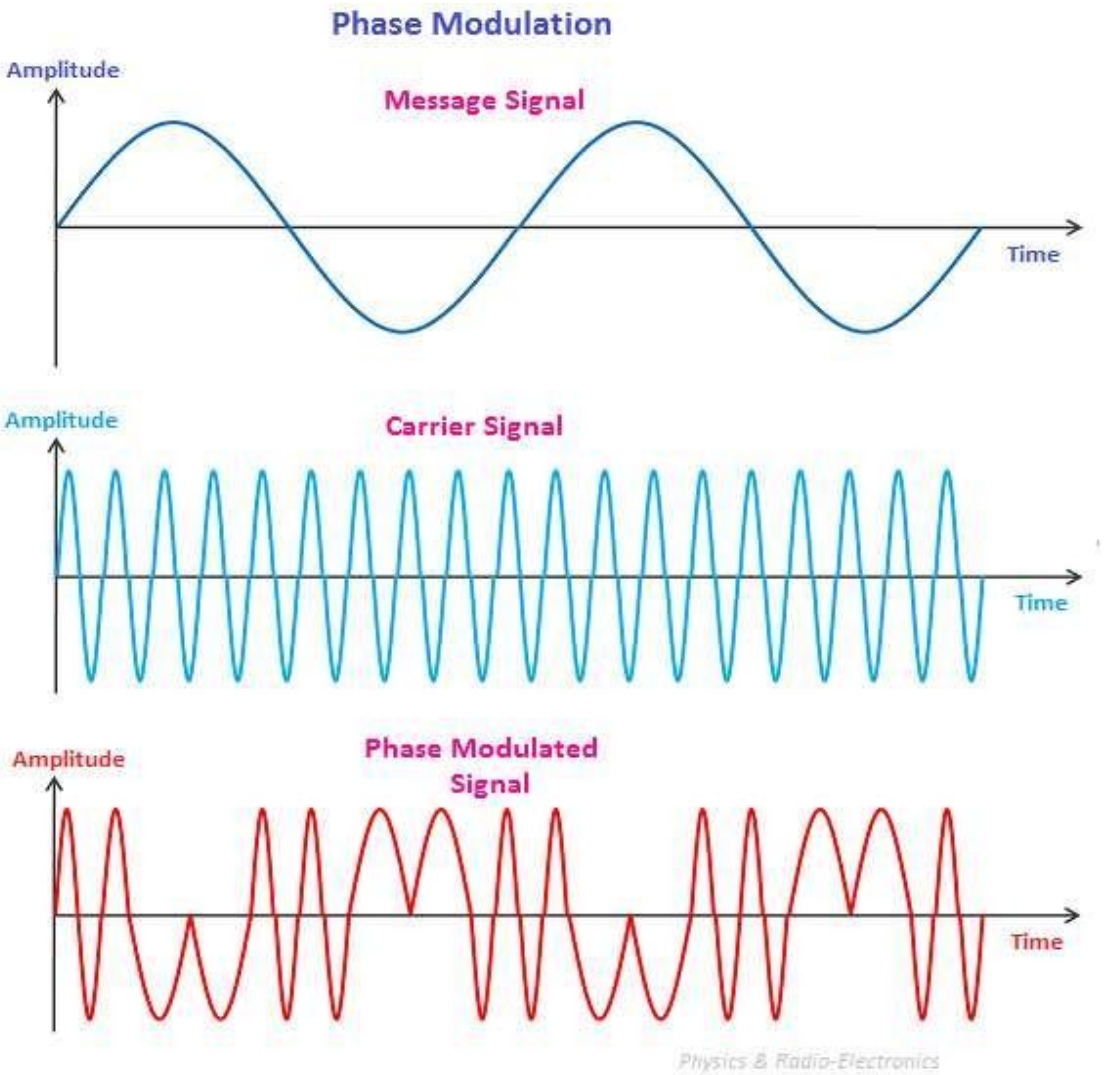


Figure 1.6 Phase Modulation

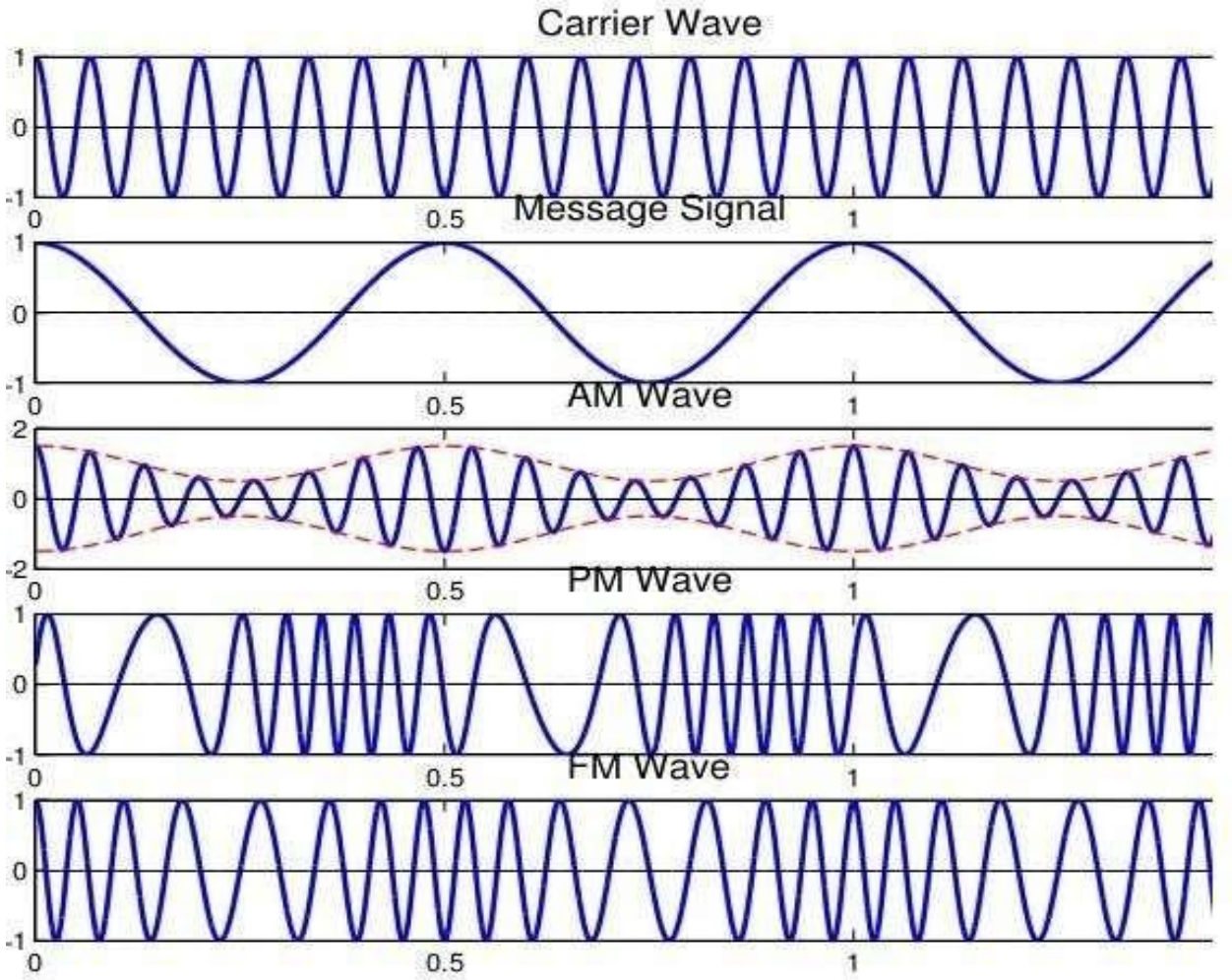


Figure 1.7 Examples of the basic continuous modulation schemes(AM,PM,FM).

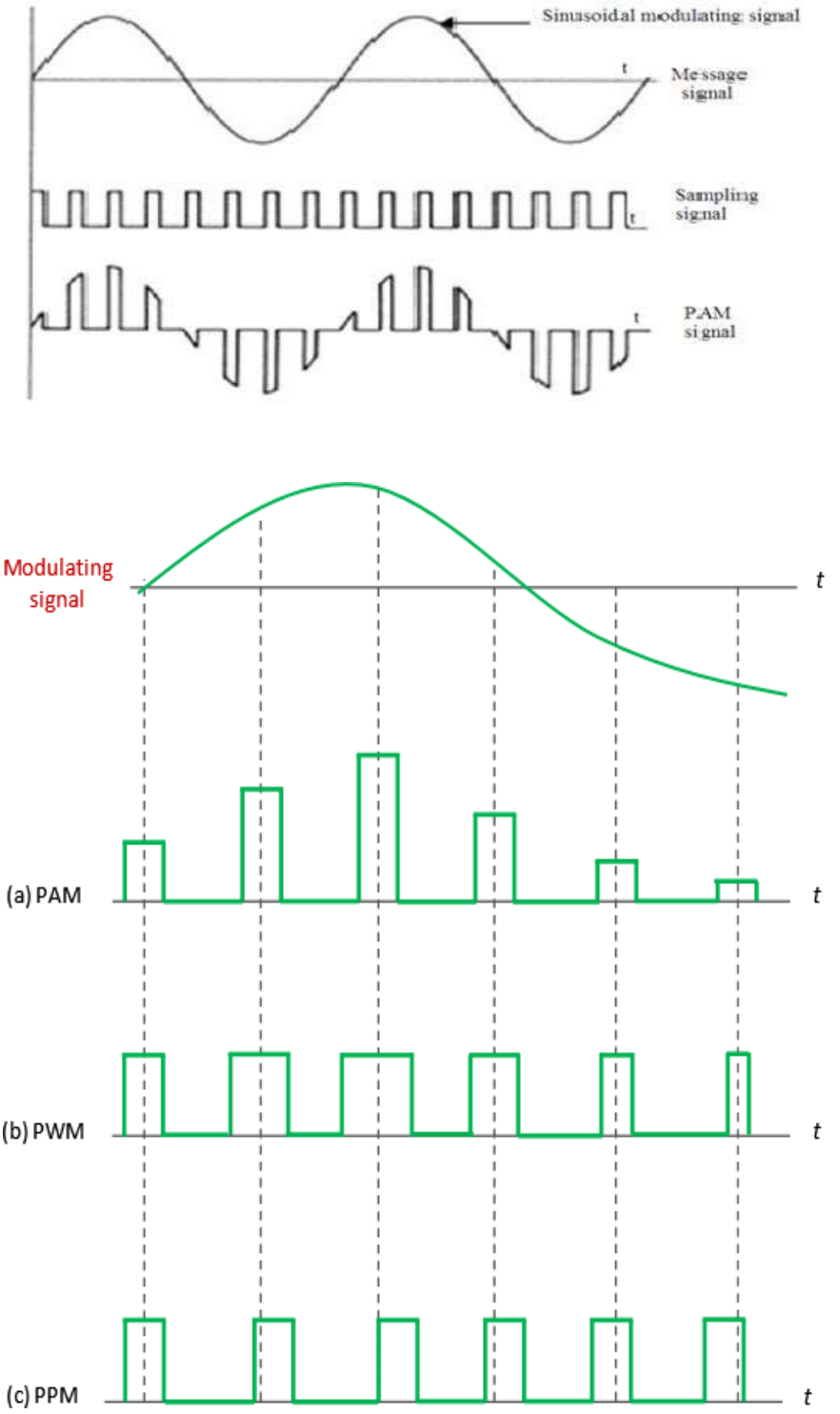


Figure 1.8 Examples of the basic pulse modulations

Advantages of analog communication

•Transmitters and receivers are simple

•Low bandwidth requirement

•FDM (Frequency division multiplexing) can be used

Drawbacks of analog communication

•Noise affects the signal quality

•It is not possible to separate noise and signal

•Repeaters cannot be used between transmitter and receiver

•Coding is not possible

•It is not suitable for the transmission of secret information

Applications

•Radio broadcasting (AM and FM)

•TV broadcasting(AM for video and FM for audio)

Amplitude Modulation

•Amplitude Modulation is the process of changing the amplitude of a relatively high frequency carrier signal in accordance with the amplitude of the modulating signal (Information).

•Application of AM - Radio broadcasting, TV pictures (video), facsimile transmission

•Frequency range for AM - 535 kHz – 1600 kHz

•Bandwidth - 10 kHz

Baseband and Pass band transmission

Baseband transmission is transmission of the encoded signal using its own baseband frequencies; i.e. without any shift (up-converting) to higher frequency ranges, while pass band transmission is the transmission after shifting the baseband frequencies to some higher frequency range (called pass band) using modulation

Demodulation

The process of extracting an original message signal from the modulated wave is known as detection or demodulation. The circuit, which demodulates the modulated wave is known as the demodulator.

Coherent and non-coherent detection

Coherent systems need carrier phase information at the receiver and they use matched filters to detect and decide what data was sent , while noncoherent systems do not need carrier phase information and use methods like square law to recover the data.

Noise

Noise can be defined as an unwanted signal that interferes with the communication or measurement of another signal. A noise itself is a signal that conveys information regarding the source of the noise. It is even present and limits the performance of communication and measurement systems. Therefore the removal of the effects of noise has been at the core of the theory and practice of communications and signal processing.

With reference to an electrical system, noise may be defined as any unwanted form of energy which tends to interfere with proper reception and reproduction of wanted signal. Many disturbances of an electrical nature produce noise in receivers, modifying the signal in an unwanted manner. In radio receivers, noise may produce hiss in the loudspeakers output. In television receivers ‘snow’ or ‘confetti’ (colored snow) becomes superimposed on the picture. In pulse communication systems, noise may produce unwanted pulses or perhaps cancel out the wanted ones. It may cause serious mathematical errors. Noise can limit the range of systems, for a given transmitted power. It affects the sensitivity of receivers, by placing a limit on the weakest signals that can be amplified. It may sometimes even force a reduction in the bandwidth of a system

1.9 Classification Of Noise

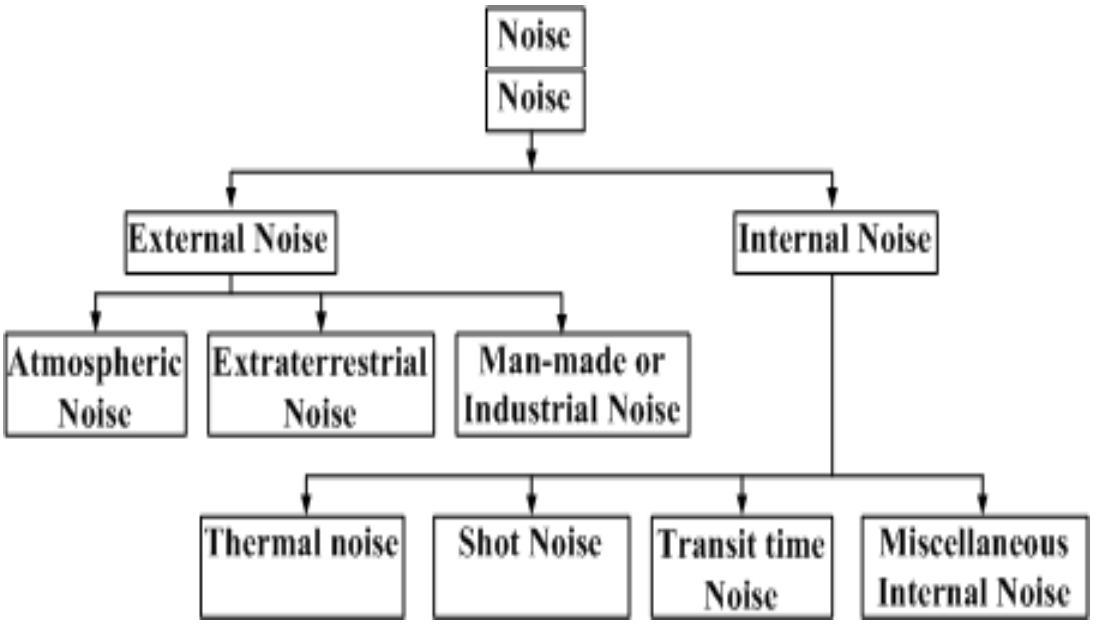
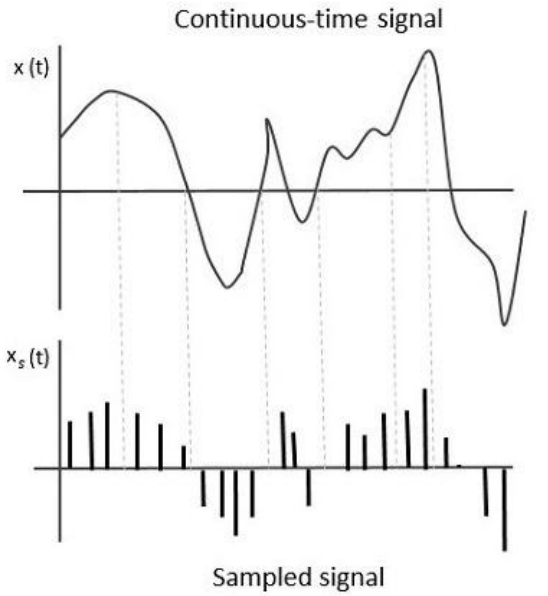


Figure 1.9 Classification Of Noise Block Diagram



A sampling signal is a periodic train of pulses, having unit amplitude, sampled at equal intervals of time T_s, which is called as sampling time. This data is transmitted at the time instants T_s and the carrier signal is transmitted at the remaining time.

Sampling Rate

To discretize the signals, the gap between the samples should be fixed. That gap can be termed as the sampling period T_s. Reciprocal of the sampling period is known as sampling frequency or sampling rate f_s.

Mathematically, we can write it as

f_s= \frac{1}{T_s}

Where,

f_s is the sampling frequency or the sampling rate

T_s is the sampling period

SAMPLING THEOREM

The sampling rate should be such that the data in the message signal should neither be lost nor it should get over-lapped. The sampling theorem states that, "a signal can be exactly reproduced if it is sampled at the rate f_s, which is greater than or equal to twice the maximum frequency of the given signal W."

•It states that a continuous time signal can be recovered from its discrete samples if and only if the sampling frequency is greater than or equal to twice the highest frequency of the continuous time signal.

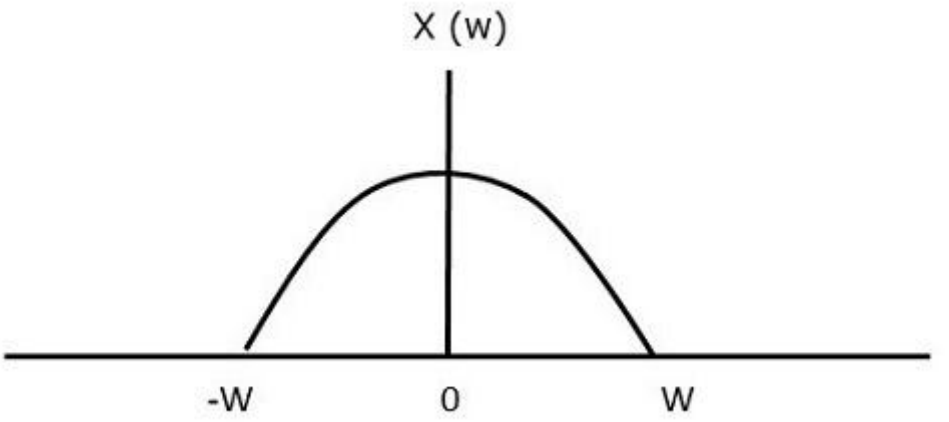
fs - Sampling frequency;

fm-maximum frequency of the message signal

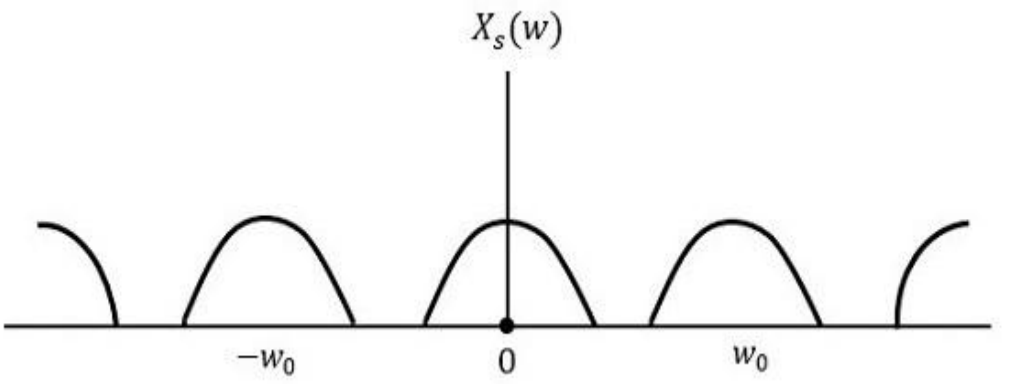
If the sampling rate is equal to twice the maximum frequency of the given signal W, then it is called as Nyquist rate.

The sampling theorem, which is also called as Nyquist theorem, delivers the theory of sufficient sample rate in terms of bandwidth for the class of functions that are band limited.

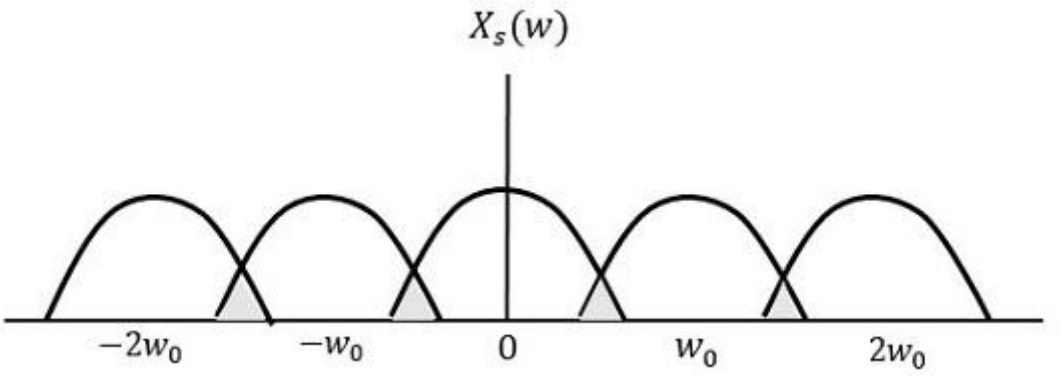
For continuous-time signal x(t), which is band-limited in the frequency domain is represented as shown in the following figure.



If the signal is sampled above Nyquist rate, then the original signal can be recovered. The following figure explains a signal, if sampled at a higher rate than 2w in the frequency domain



If the same signal is sampled at a rate less than 2w, then the sampled signal would look like the following figure.

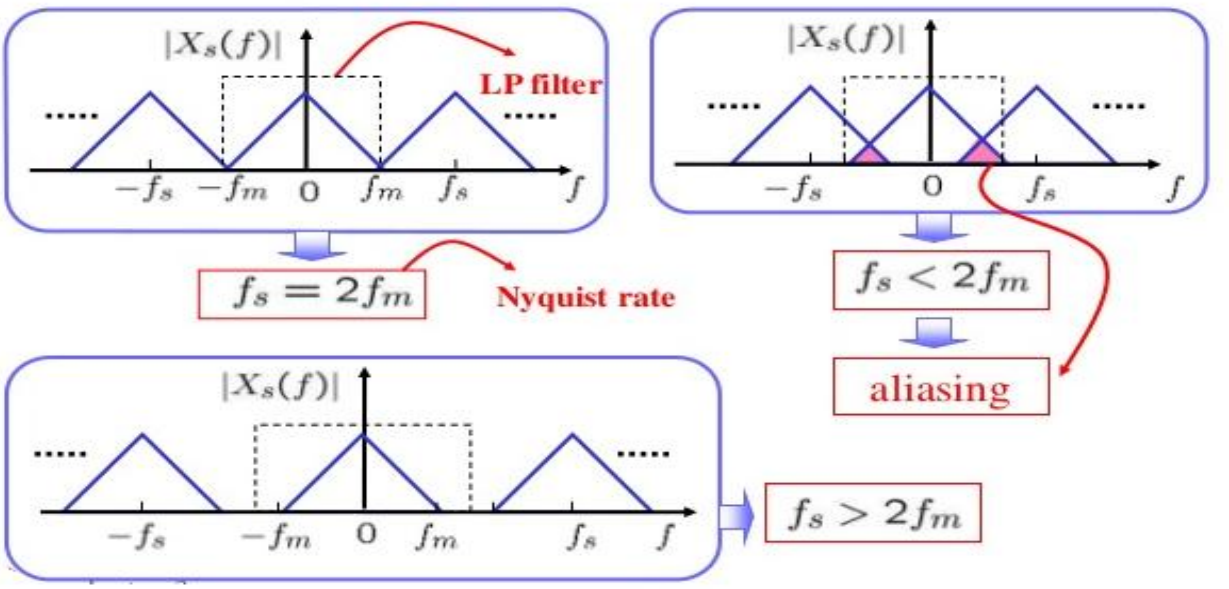


ALIASING EFFECT

We can observe from the above pattern that there is over-lapping of information, which leads to mixing up and loss of information. This unwanted phenomenon of over-lapping is called as Aliasing.

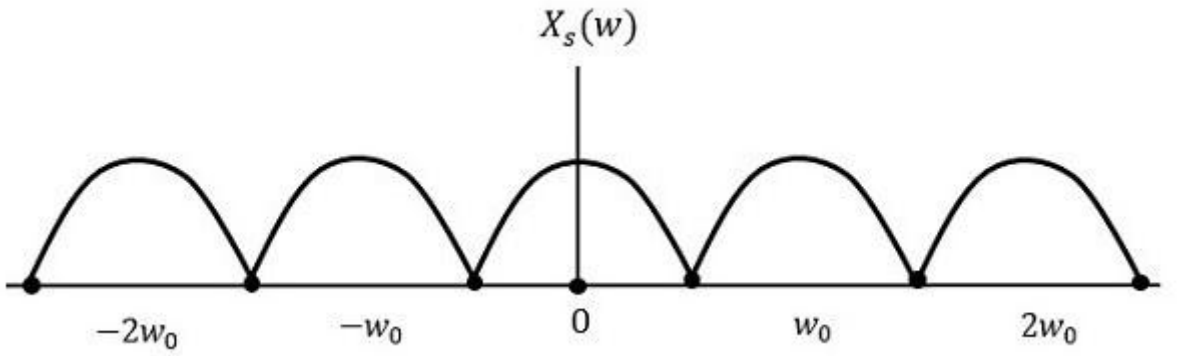
If fs<2fm, low pass filtered signal contains some high frequency components along with message signal due to spectral overlapping.

The presence of high frequency signal in the reconstructed signal causes distortion. This is called as Aliasing effect.



Aliasing can be referred to as "the phenomenon of a high-frequency component in the spectrum of a signal, taking on the identity of a low-frequency component in the spectrum of its sampled version."

Hence, the sampling rate of the signal is chosen to be as Nyquist rate. If the sampling rate is equal to twice the highest frequency of the given signal W, then the sampled signal would look like the following figure



In this case, the signal can be recovered without any loss. Hence, this is a good sampling rate.

There are three types of sampling techniques:

Impulse sampling.

Natural sampling.

Flat Top sampling.

1.10 Impulse sampling

Ideal Sampling is also known as Instantaneous sampling or Impulse Sampling.Train of impulse is used as a carrier signal for ideal sampling. In this sampling technique the sampling function is a train of impulses and the principle used is known as multiplication principle.

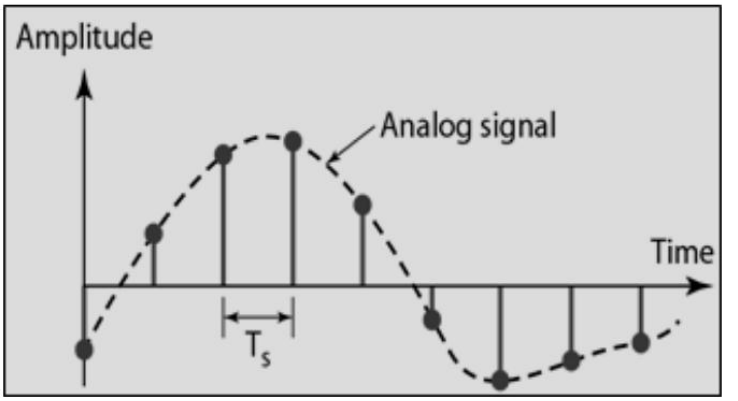


Figure 1.10 Impulse Sampling

1.11Natural Sampling

Natural Sampling is a practical method of sampling in which pulse have finite width equal to τ. Sampling is done in accordance with the carrier signal which is digital in nature.Natural Sampling is a practical method of sampling in which pulse have finite width equal to τ. ... With the help of functional diagram of a Natural sampler, a sampled signal g(t) is obtained by multiplication of sampling function c(t) and the input signal x(t).

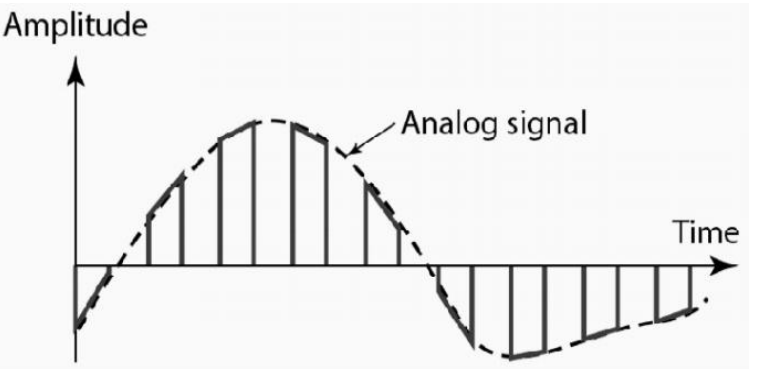


Figure 1.11 Natural Sampling

1.12 Flat Top Sampling

During transmission, noise is introduced at top of the transmission pulse which can be easily removed if the pulse is in the form of flat top. Here, the top of the samples are flat i.e. they have constant amplitude. Hence, it is called as flat top sampling or practical sampling. Flat top sampling makes use of sample and hold circuit.

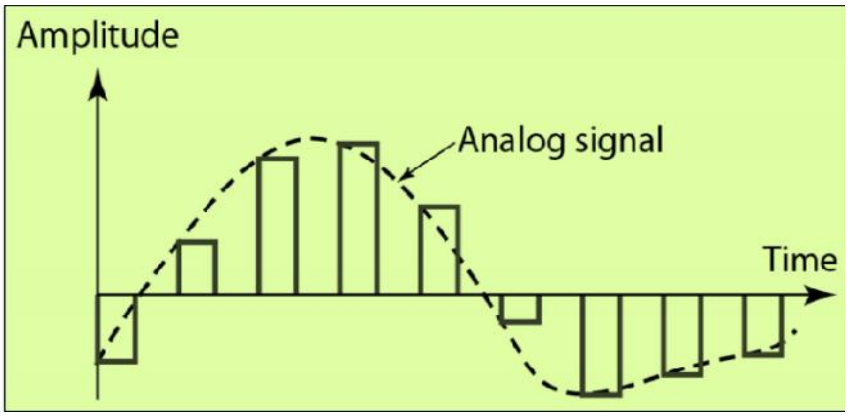


Figure 1.12 Flat-Top Sampling

1.13 Pulse-code modulation (PCM) is used to digitally represent sampled analog signals. It is the standard form of digital audio in computers, CDs, digital telephony and other digital audio applications. The amplitude of the analog signal is sampled at uniform intervals and each sample is quantized to its nearest value within a predetermined range of digital levels.

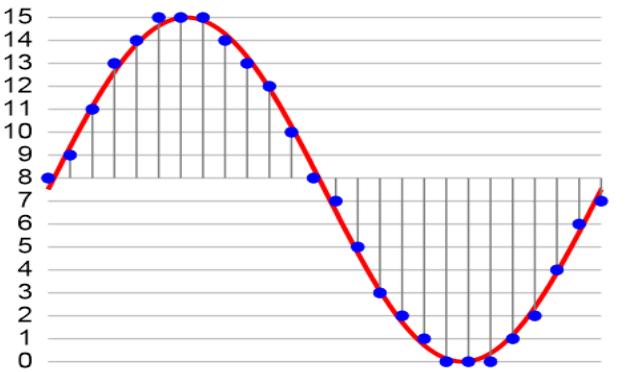


Figure 1.13 Pulse code modulatiojn

1.14 Analog To Digital Conversiom

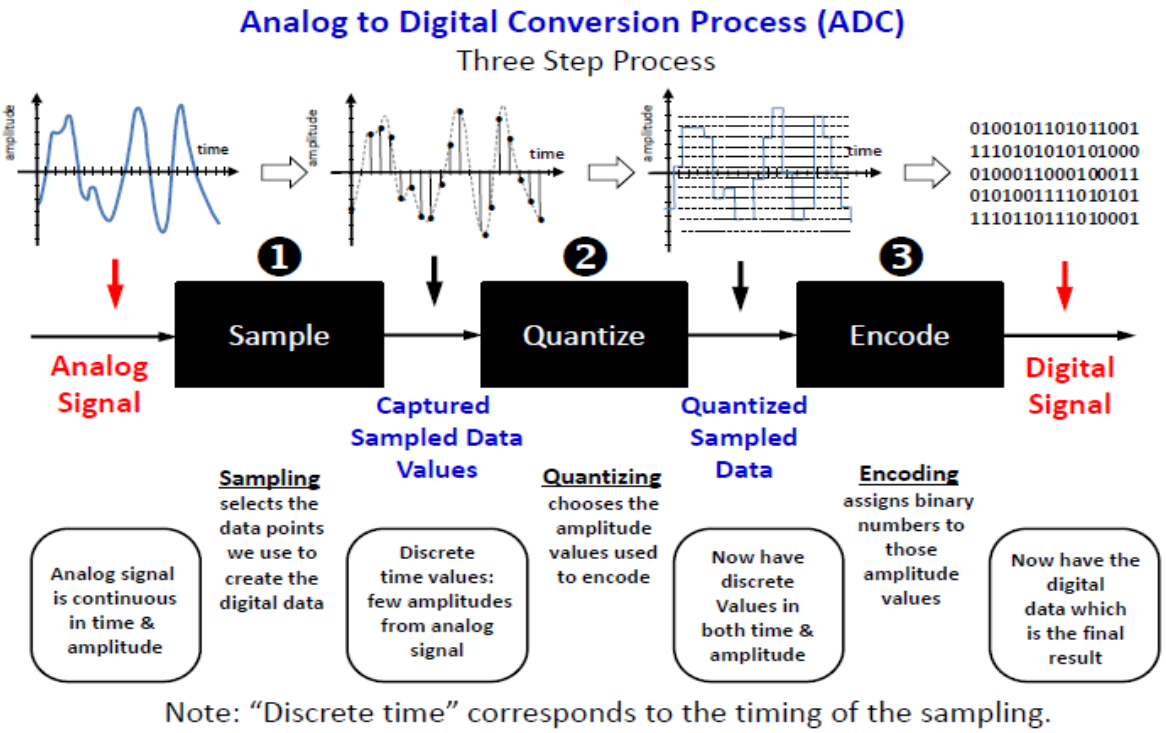


Figure 1.14 Analog To Digital Conversiom

Effect of Under sampling: ALIASING

It is the effect in which overlapping of a frequency components takes place at the frequency higher than Nyquist rate. Signal loss may occur due to aliasing effect. We can say that aliasing is the phenomena in which a high frequency component in the frequency spectrum of a signal takes identity of a lower frequency component in the same spectrum of the sampled signal.

Because of overlapping due to process of aliasing, sometimes it is not possible to overcome the sampled signal x(t) from the sampled signal g(t) by applying the process of low pass filtering since the spectral components in the overlap regions . hence this causes the signal to destroy.

TEXT / REFERENCE BOOKS:

1. William Stallings, Data and Computer Communications, 10th Edition, Pearson, 2014.

2. Wayne Thomasi, "Advanced Electronic Communication Systems", 6th Edition, PHI Publishers, 2003.

3. Simon Haykins, “Communication Systems” John Wiley, 5th Edition, March 2009.

4. John G. Proakis, MasoudSalehi, “Digital Communication”, McGraw Hill 5th edition November 6, 2007.

5. Bernard Sklar, “Digital Communication, Fundamentals and Application”, Pearson Education Asia, 2nd

Edition, Jan. 21, 2001.

6. Behrouz A. Forouzen, “Data communication and Networking”, Fourth Edition, Tata McGraw – Hill, 2011.

7. Andrew S.Tanenbaum, “Computer Networks”, 5th Edition, Pearson, 2011.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ECE

UNIT II ANALOG AND DIGITAL COMMUNICATION – SCSA1305

UNIT 2 ANALOG AND DIGITAL COMMUNICATION

Amplitude modulation types of amplitude modulation- Standard AM with Full Carrier ,Comparison of different amplitude modulations; Angle modulation (FM and PM), FM generation using PM, PM generation using FM, Comparison of Narrowband and Wideband FM, Comparison of AM,FM and PM. Analog pulse modulation PAM,PWM,PPM; Digital pulse modulation Pulse Code Modulation (PCM), Delta modulation (DM), Adaptive Delta modulation (ADM), Multiplexing Frequency Division Multiplexing (FDM), Time Division Multiplexing.

NOTES

Communication is the process of establishing connection or link between two points for information exchange or Communication is simply the basic process of exchanging information.

• The electronic equipment which are used for communication purpose, are called communication equipment. Different communication equipment when assembled together form a communication system.

• Typical example of communication system are line telephony and line telegraphy, radio telephony and radio telegraphy, radio broadcasting, point-to-point communication and mobile communication, computer communication, radar communication, television broadcasting, radio telemetry, radio aids to navigation, radio aids to aircraft landing etc.

Standard AM with Full Carrier

Amplitude Modulation is the process of changing the amplitude of a relatively high frequency carrier signal in accordance with the amplitude of the modulating signal (Information). ϖ Application of AM - Radio broadcasting, TV pictures (video), facsimile transmission ϖ Frequency range for AM - 535 kHz – 1600 kHz ϖ Bandwidth - 10 kHz

Modulation is the process of changing the parameters of the carrier signal, in accordance with the instantaneous values of the modulating signal.

Parameters ◊ Amplitude, Frequency, Phase

¬ Message signal is low frequency signal, Carrier signal is High frequency signal ¬ Modulated signal is high frequency signal ¬ Converting low frequency signal into radio wave signal ¬ Multiplication Process

2.1 Amplitude Modulation Types

1.Double-Sideband Full carrier (DSB-FC) AM or (Conventional Amplitude Modulation)

2. Double-Sideband Suppressed Carrier (DSB-SC) AM

3. Single-Sideband Suppressed Carrier (SSB-SC) AM

4. Vestigial Sideband (VSB) AM

Representation of DSB FC -AM

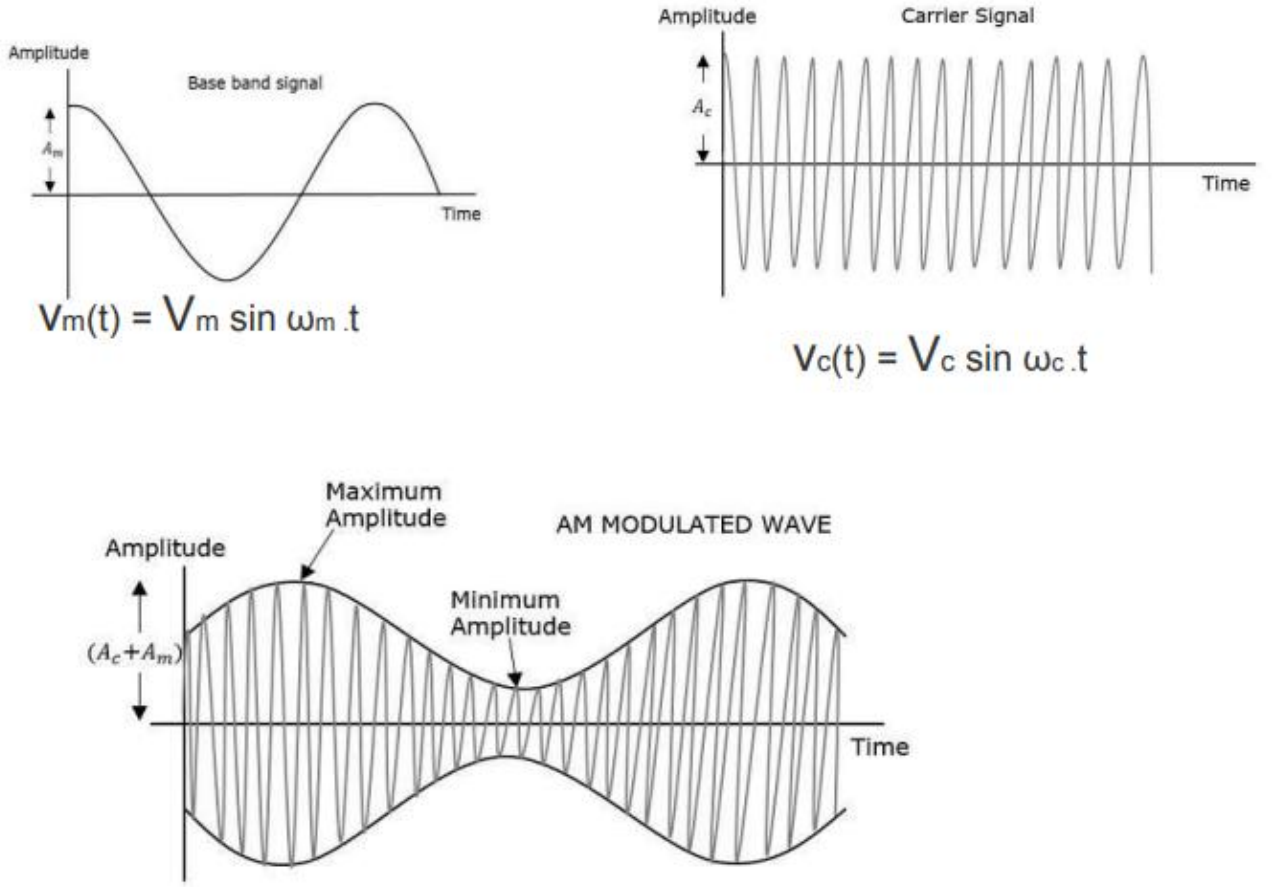


Figure 2.1 Amplitude modulation types

Advantages:

- AM has the advantage of being usable with very simple modulators and demodulators.
- AM is a relatively inexpensive.
- AM wave can travel a long distance

. Disadvantages:

- Poor performance in the presence of noise.
- Inefficient use of transmitter power.
- It needs larger bandwidth.

Applications:

- Low quality form of modulation that is used for commercial broadcasting of both audio and video signals
- Two-way mobile radio communications such as citizens band (CB) radio.
- Aircraft communications in the VHF frequency range.

Comparison of different types of AM

S.No	Parameter	DSBFC	DSBSC	SSB	VSB
1	Carrier Suppression	NA	Fully	Fully	NA
2	Sideband Suppression	NA	NA	One SB completely	One SB suppressed partially
3	Bandwidth	2fm	2fm	fm	fm < BW >2fm
4	Transmission efficiency	Min (33.3%)	Moderate (66.7%)	Max (83.3%)	Moderate
5	Total Power	$P_c\left[1+\left(\frac{m_a^2}{2}\right)\right]$	$P_c\left(\frac{m_a^2}{2}\right)$	$P_c\left(\frac{m_a^2}{4}\right)$	Between DSBSC and SSB
6	Applications	Radio Broadcasting	Radio Broadcasting	Point to point mobile comm	TV

Table 2.1.1

Features of angle modulation:

•It can provide a better discrimination (robustness) against noise and interference than AM

•This improvement is achieved at the expense of increased transmission bandwidth

•In case of angle modulation, channel bandwidth may be exchanged for improved noise performance

•Such trade- off is not possible with AM

Basic definitions:

The other type of modulation in continuous-wave modulation is **Angle Modulation**. Angle Modulation is the process in which the frequency or the phase of the carrier signal varies according to the message signal.

The standard equation of the angle modulated wave is

$$s(t) = A_c \cos \theta_i(t)$$

Where,

AcAc is the amplitude of the modulated wave, which is the same as the amplitude of the carrier signal θi(t)θi(t) is the angle of the modulated wave

Angle modulation is further divided into frequency modulation and phase modulation.

- **Frequency Modulation** is the process of varying the frequency of the carrier signal linearly with the message signal.
- **Phase Modulation** is the process of varying the phase of the carrier signal linearly with the message signal.

Now, let us discuss these in detail.

2.2 Frequency Modulation

In amplitude modulation, the amplitude of the carrier signal varies. Whereas, in **Frequency Modulation (FM)**, the frequency of the carrier signal varies in accordance with the instantaneous amplitude of the modulating signal.

Hence, in frequency modulation, the amplitude and the phase of the carrier signal remains constant. This can be better understood by observing the following figures.

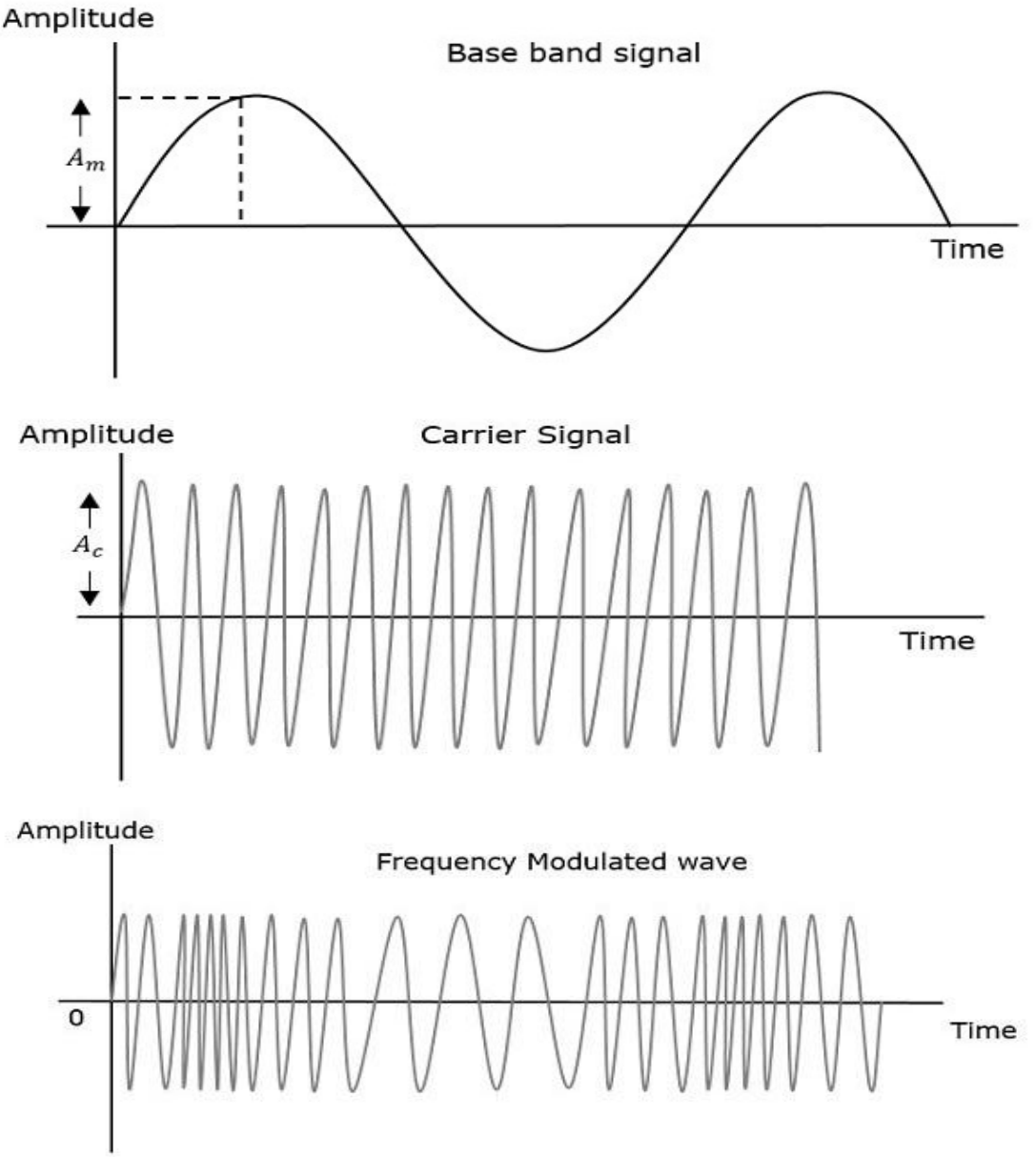


Figure 2.2 Frequency Modulation

The frequency of the modulated wave increases, when the amplitude of the modulating or message signal increases. Similarly, the frequency of the modulated wave decreases, when the amplitude of the modulating signal decreases. Note that, the frequency of the modulated wave remains constant and it is equal to the frequency of the carrier signal, when the amplitude of the modulating signal is zero.

- There is yet another way of modulation namely the angle modulation in which the angle of the carrier wave changes in accordance with the signal
- In this method of modulation the amplitude of the carrier wave is maintained constant
- The advantage is it can show better discrimination against noise and interference than amplitude modulation

FREQUENCY MODULATION INDEX

The frequency modulation index is the equivalent of the modulation index for AM , but obviously related to FM. In view of the differences between the two forms of modulation, the FM modulation index is measured in a different way.

The FM modulation index is equal to the ratio of the frequency deviation to the modulating frequency.

$$m = \frac{Frequency\ deviation}{Modulation\ frequency}$$

FM deviation ratio

Accordingly the FM deviation ratio can be defined as: the ratio of the maximum carrier frequency deviation to the highest audio modulating frequency.

$$m = \frac{Max\ frequency\ deviation}{Max\ modulation\ frequency}$$

There are two main classifications for frequency modulated signals and these can be related to the modulation index and deviation ratio.

Wideband FM:

For NBFM, the FM modulation index must be less than 0.5, although a figure of 0.2 is often used. For NBFM the audio or data bandwidth is small, but this is acceptable for this type of communication. Wideband FM is typical used for signals where the FM modulation index is above about 0.5. For these signals the sidebands beyond the first two terms are not insignificant. Broadcast FM stations use wide-band FM which enables them to transmit high quality audio, as well as other facilities like stereo, and other facilities like RDS, etc.

The wide bandwidth of wide band FM is enables high quality broadcast transmissions to be made, combining a wide frequency response with low noise levels. Once the signal is sufficiently strong, the audio signal to noise ratio is very good.

Sometimes high fidelity FM tuners may use a wide-band filter for strong signals to ensure the optimum fidelity and performance. Here the quieting effect of the strong signal will allow for wide-band reception and the full audio bandwidth. For for lower strength signals they may switch to a narrower filter to reduce the noise level, although this will result in the audio bandwidth being reduced. However on balance the narrower bandwidth will give a more pleasing sound when the received signal is low.

Narrowband FM:

Narrow band FM, NBFM, is used for signals where the deviation is small enough that the terms in the Bessel function is small and the main sidebands are those appearing at ± modulation frequency. The sidebands further out are negligible.

Narrowband FM is widely used for two way radio communications. Although digital technologies are taking over, NBFM is still widely used and very effective. Many two way radios or walkie talkies use NBFM, especially those which conform to the licence-free standards like PMR446 and FRS radio communications systems.

2.3 Phase Modulation

In frequency modulation, the frequency of the carrier varies. Whereas, in **Phase Modulation (PM)**, the phase of the carrier signal varies in accordance with the instantaneous amplitude of the modulating signal.

So, in phase modulation, the amplitude and the frequency of the carrier signal remains constant. This can be better understood by observing the following figures.

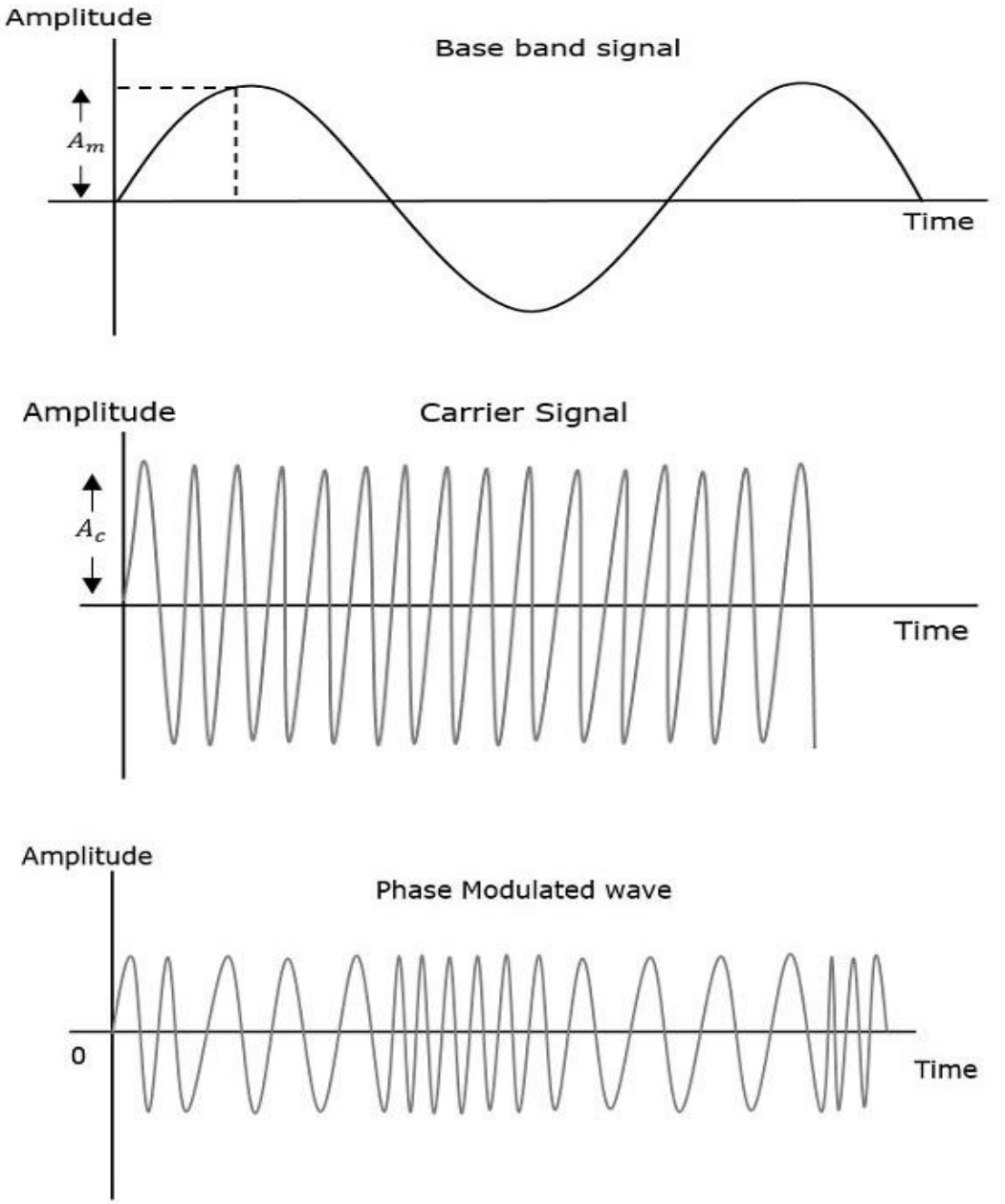
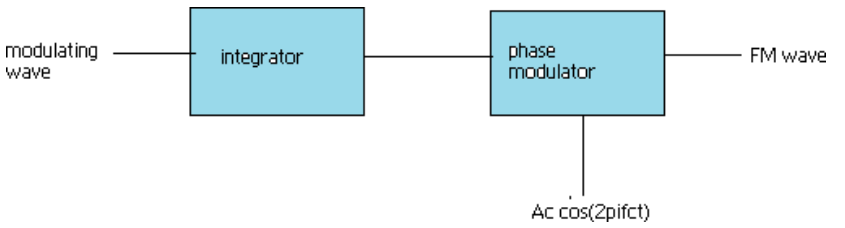


Figure 2.3 phase modulation

The phase of the modulated wave has got infinite points, where the phase shift in a wave can take place. The instantaneous amplitude of the modulating signal changes the phase of the carrier signal. When the amplitude is positive, the phase changes in one direction and if the amplitude is negative, the phase changes in the opposite direction.

Phase Modulation:



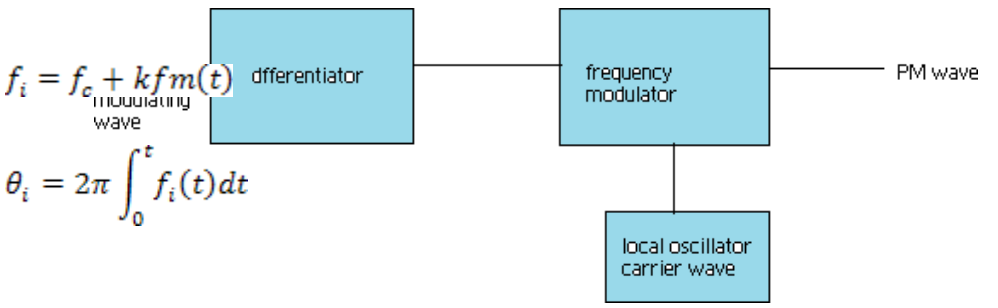
Phase modulation is that form of angle modulation in which the angle $\theta_i(t)$ is varied linearly with the message signal m(t)

$$\theta_i(t) = 2\pi fct + kpm(t)$$

- The term $2^{\pi fct}$ represents the angle of the unmodulated carrier wave and constant Kp is the phase sensitivity of the modulator expressed in radian per volt
- We have assumed that the angle of the unmodulated carrier is zero at time t =0
- The phase –modulated signal s(t) is thud described in the time domain by

$$s(t) = A_c \cos 2\pi fct + Kpm(t)]$$

FREQUENCY MODULATION :



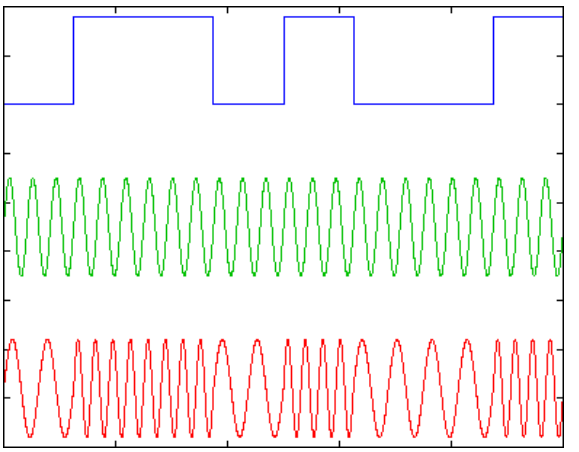
Frequency modulation is that form of angle modulation in which the instantaneous frequency if(t) is varied linearly with the message signal m(t)

$$\theta_i = 2\pi fct + 2\pi kf \int_0^t m(t)dt$$

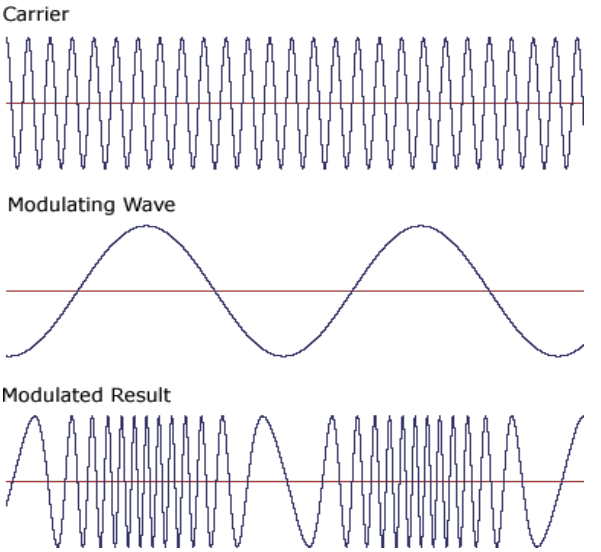
$$s(t) = A_c \cos[2\pi fct + 2\pi kf \int_0^t m(t)dt$$

]

Frequency of the carrier varies with the signal mathematically in the above equation

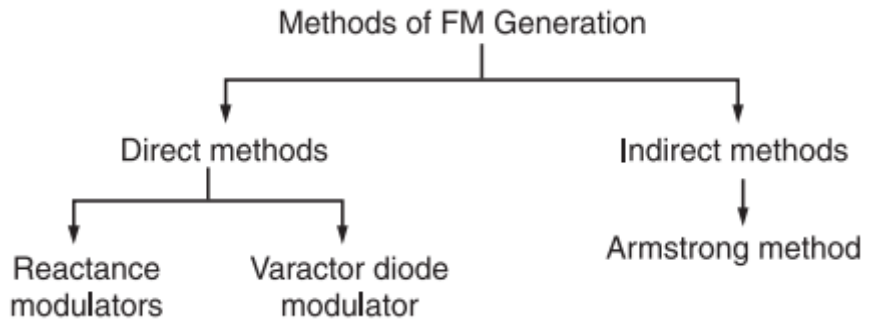


- Comparison between phase and frequency modulated equations frequency modulated signal is the same as phase modulation with the message signal integrated
- The variation of the frequency is discrete differing from the sinusoidal modulated wave where the frequency changes constantly
- There will be a phase discontinuity in case of phase modulation when message is a square wave
- There is a phase reversal in the phase modulation and the visualization is easier



Note: The FM wave is a non linear function of the modulating wave m(t)

Generation of fm waves:



There are two types
Direct method and indirect method
In the indirect method of producing a narrow band FM is generated then frequency multiplied to obtain wide band frequency modulated wave

2.4 VARACTOR DIODE MODULATOR

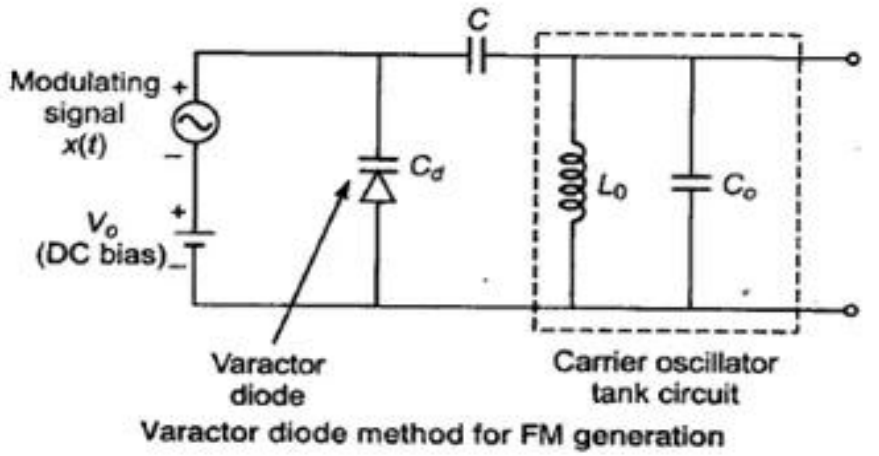


Figure 2.4 VARACTOR DIODE MODULATOR

A varactor diode is a semiconductor diode whose junction capacitance varies linearly with the applied bias andThe varactor diode must be reverse biased.

Working Operation

The varactor diode is reverse biased by the negative dc source $-V_b$.
The modulating AF voltage appears in series with the negative supply voltage. Hence, the voltage applied across the varactor diode varies in proportion with the modulating voltage.This will vary the junction capacitance of the varactor diode.The varactor diode appears in parallel with the oscillator tuned circuit.Hence the oscillator frequency will change with change in varactor dioide capacitance and FM wave is produced.The RFC will connect the dc and modulating signal to the varactor diode but it offers a very high impedance at high oscillator frequency. Therefore, the oscillator circuit is isolated from the dc bias and modulating signal.

2.5 ARMSTRONG METHOD OF FM GENERATION

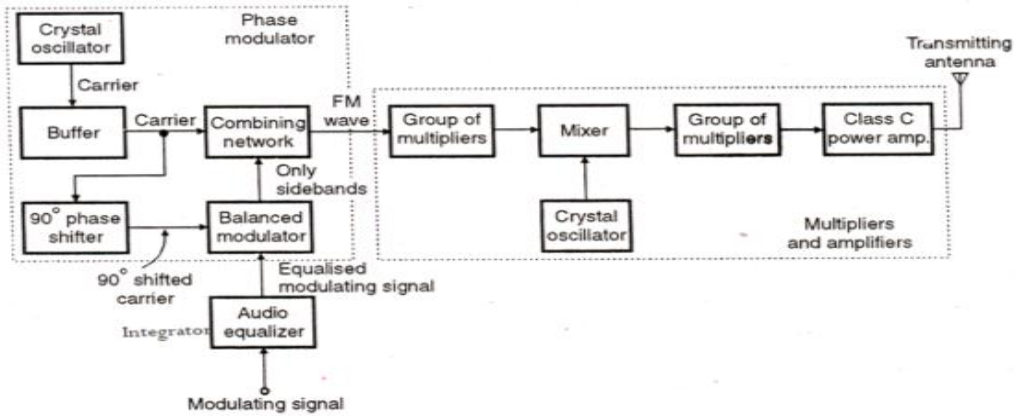


Figure 2.5 ARMSTRONG METHOD OF FM GENERATION

The crystal oscillator generates the carrier at low frequency typically at 1MHz. This is applied to the combining network and a 90° phase shifter.

- The modulating signal is passed through an audio equalizer to boost the low modulating frequencies .The modulating signal is then applied to a balanced modulator.
- The balanced modulator produced two side bands such that their resultant is 90° phase shifted with respect to the unmodulated carrier.
- The unmodulated carrier and 90° phase shifted sidebands are added in the combining network.
- At the output of the combining network we get *Fm* wave. This wave has a low carrier frequency *fc* and low value of the modulation index *mf.*
- *The carrier frequency and the modulation index are then raised by passing the FM wave*

through the first group of multipliers. The carrier frequency is then raised by using a mixer and then the fc and mf,both are raised to required high values using the second group of multipliers.

- *The FM signal with high fc and high mf is then passed through a class C power amplifier to raise the power level of the FM signal.*

- *The Armstrong method uses the phase modulation to generate frequency modulation. This method can be understood by dividing it into four parts as follows:*

2.6 INDIRECT METHOD:

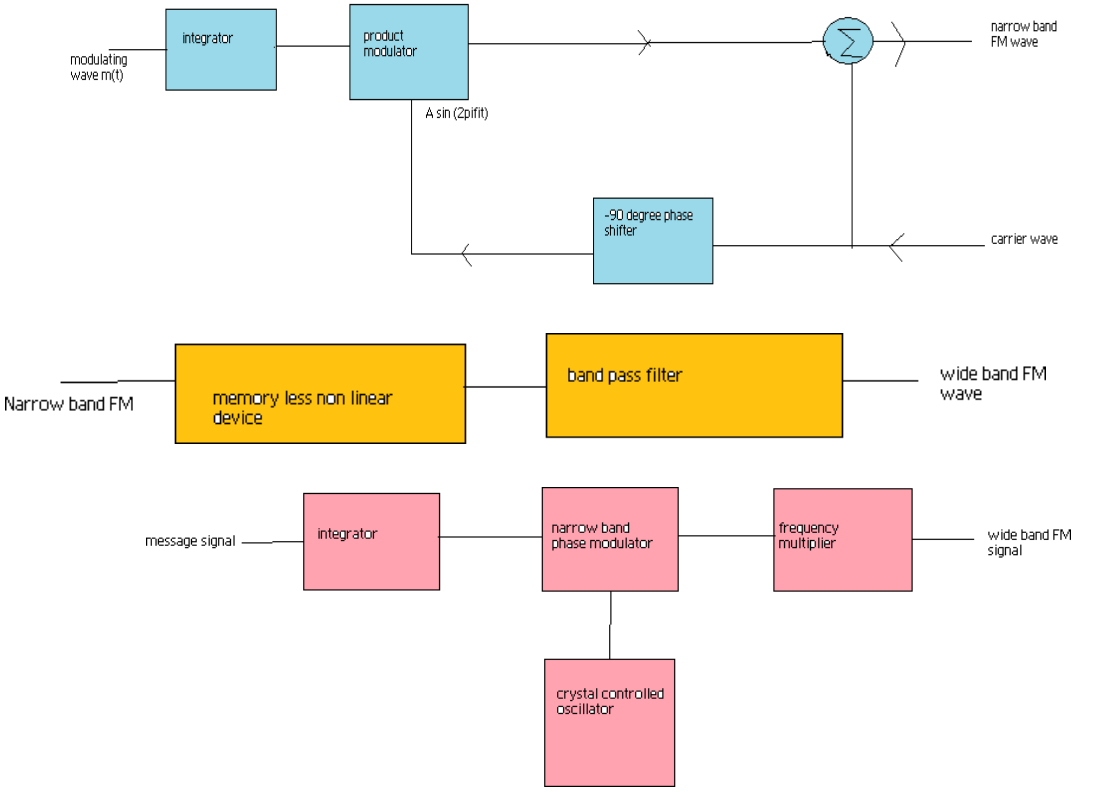


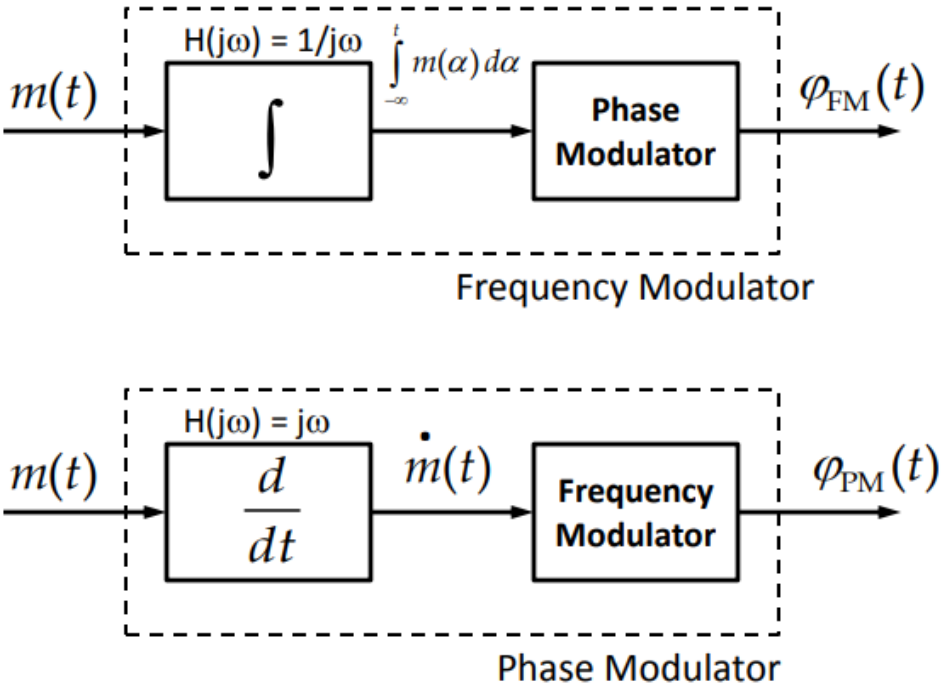
Figure 2.6 Indirect method block diagram

FM modulation : The amplitude of the modulated carrier is held constant and the time derivative of the phase of the carrier is varied linearly with the information signal.HenceTherefore NBFM signal can be generated using phase modulator circuit as shown.

To obtain WBFM signal, the output of the modulator circuit (NBFM) is fed into frequency multiplier circuit and the mixer circuit.

The function of the frequency multiplier is to increase the frequency deviation or modulation index so that WBFM can be generated.The instantaneous value of the carrier frequency is increased by N times.

2.7 CONVERSION OF FM TO PM AND PM TO FM



We require that H(jω) be a reversible (or invertible) operation so that m(t) is recoverable.

2.7 CONVERSION OF FM TO PM AND PM TO FM

FM signals can be **generated** using either direct or indirect frequency modulation: Direct **FM** modulation can be achieved by directly feeding the message into the input of a voltage-controlled oscillator. For indirect **FM** modulation, the message signal is integrated to **generate** a phase-modulated signal.

Phase modulation (**PM**) is a modulation pattern for conditioning communication signals for transmission. It encodes a message signal as variations in the instantaneous phase of a carrier wave. Phase modulation is one of the two principal forms of angle modulation, together with frequency modulation.The phase of a carrier signal is modulated to follow the changing signal level (amplitude) of the message signal. The peak amplitude and the frequency of the carrier signal are maintained constant, but as the amplitude of the message signal changes, the phase of the carrier changes correspondingly.Phase modulation is widely used for transmitting radio waves and is an integral part of many digital transmission coding schemes that underlie a wide range of technologies like Wi-Fi, GSM and satellite television.PM is used for signal and waveform generation in digital synthesizers, such as the Yamaha DX7, to implement FM synthesis. A related type of sound synthesis called phase distortion is used in the Casio CZ synthesizers.

The change in phase, changes the frequency of the modulated wave. The frequency of the wave also changes the phase of the wave. ... Phase modulation is an indirect method of producing **FM**. The amount of frequency shift, **produced** by a phase modulator increases with the modulating frequency.

2.8 COMPARISON BETWEEN AM AND FM

Sr. No.	FM	AM
1	FM receivers are immune to noise	AM receivers are not immune to noise
2	It is possible to decrease noise by increasing deviation	This feature is absent in AM
3	Bandwidth is higher and depends on modulation index	Bandwidth is lower compared to AM but independent of modulation index
4	FM transmission and reception equipment are more complex	FM transmission and reception equipment are less complex
5	All transmitted power is useful	Carrier power and one sideband power is useless

Table 2.8.1

#	Frequency Modulation (FM)	Phase Modulation (PM)
1	Frequency deviation is proportional to modulating signal $m(t)$	Phase deviation is proportional to modulating signal $m(t)$
2	Noise immunity is superior to PM (and of course AM)	Noise immunity better than AM but not FM
3	Signal-to-noise ratio (SNR) is better than in PM	Signal-to-noise ratio (SNR) is not as good as in FM
4	FM is widely used for commercial broadcast radio (88 MHz to 108 MHz)	PM is primarily for some mobile radio services
5	Modulation index is proportional to modulating signal $m(t)$ as well as modulating frequency f_m	Modulation index is proportional to modulating signal $m(t)$

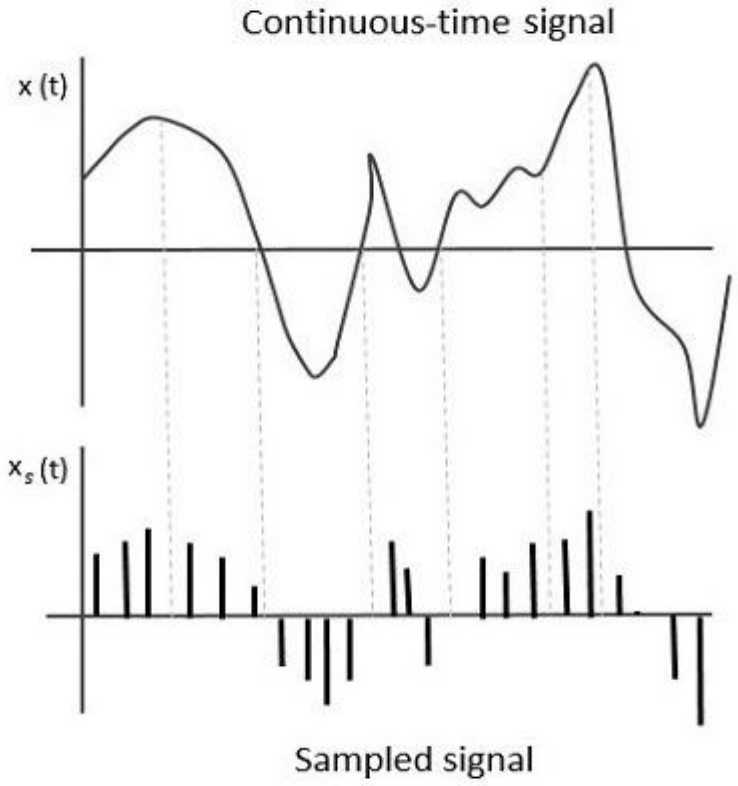
Table 2.8.2

SAMPLING

These pulse modulation techniques deal with discrete signals. So, now let us see how to convert a continuous time signal into a discrete one.

The process of converting continuous time signals into equivalent discrete time signals, can be termed as **Sampling**. A certain instant of data is continually sampled in the sampling process.

The following figure shows a continuous-time signal **x(t)** and the corresponding sampled signal $\mathbf{x_s(t)}$. When **x(t)** is multiplied by a periodic impulse train, the sampled signal $\mathbf{x_s(t)}$ is obtained.



A **sampling signal** is a periodic train of pulses, having unit amplitude, sampled at equal intervals of time T_s, which is called as **sampling time**. This data is transmitted at the time instants T_s and the carrier signal is transmitted at the remaining time.

Sampling Rate

To discretize the signals, the gap between the samples should be fixed. That gap can be termed as the sampling period T_s. Reciprocal of the sampling period is known as **sampling frequency** or **sampling rate** f_s.

Mathematically, we can write it as

$$f_s= \frac{1}{T_s}$$

Where,

f_s is the sampling frequency or the sampling rate
T_s is the sampling period

SAMPLING THEOREM

The sampling rate should be such that the data in the message signal should neither be lost nor it should get over-lapped. The **sampling theorem** states that, "a signal can be exactly reproduced if it is sampled at the rate f_s, which is greater than or equal to twice the maximum frequency of the given signal **W**."

- It states that a continuous time signal can be recovered from its discrete samples if and only if the sampling frequency is greater than or equal to twice the highest frequency of the continuous time signal.

$$f_s \geq 2 f_m$$

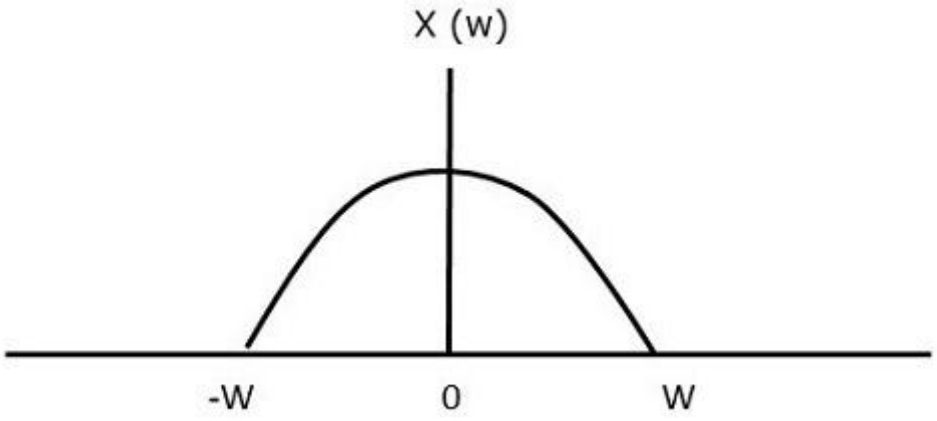
fs - Sampling frequency;

fm-maximum frequency of the message signal

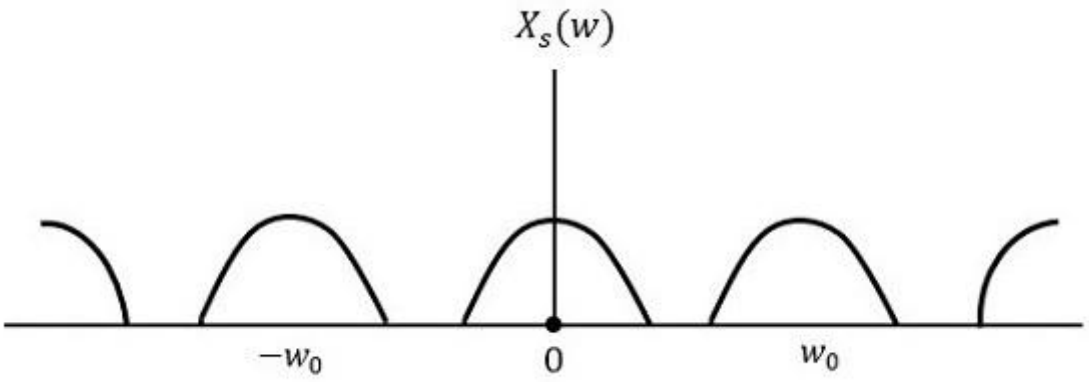
If the sampling rate is equal to twice the maximum frequency of the given signal W, then it is called as **Nyquist rate**.

The sampling theorem, which is also called as **Nyquist theorem**, delivers the theory of sufficient sample rate in terms of bandwidth for the class of functions that are bandlimited.

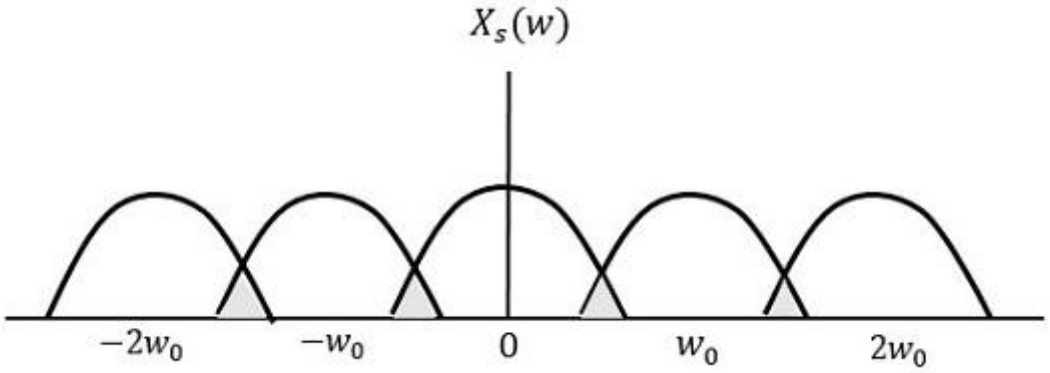
For continuous-time signal **x(t)**, which is band-limited in the frequency domain is represented as shown in the following figure.



If the signal is sampled above Nyquist rate, then the original signal can be recovered. The following figure explains a signal, if sampled at a higher rate than **2w** in the frequency domain.



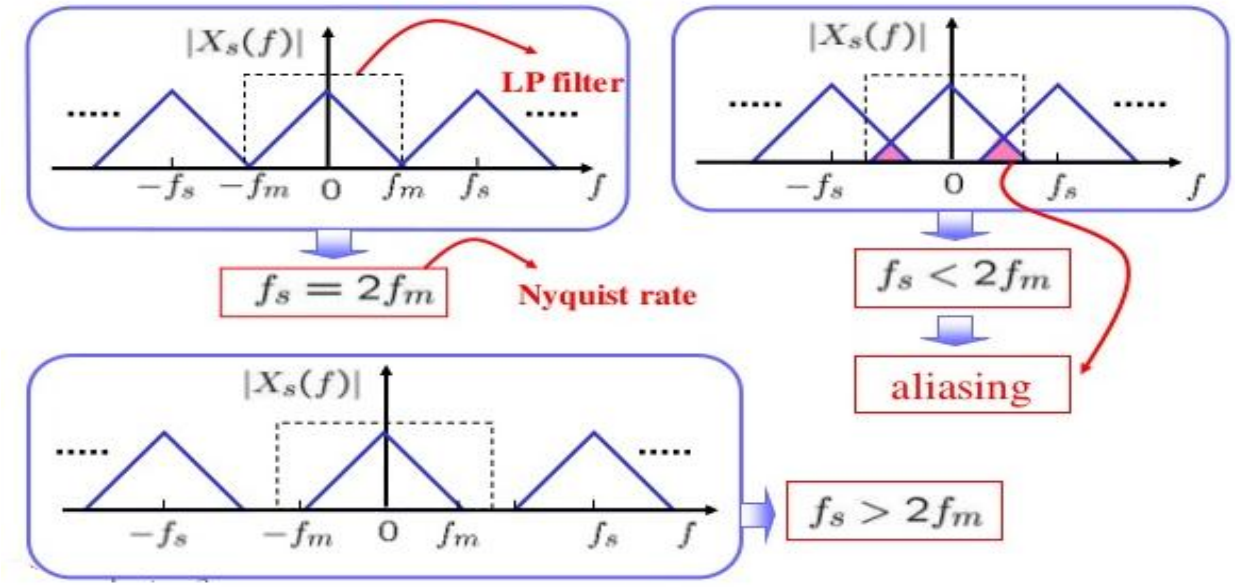
If the same signal is sampled at a rate less than **2w**, then the sampled signal would look like the following figure.



ALIASING EFFECT

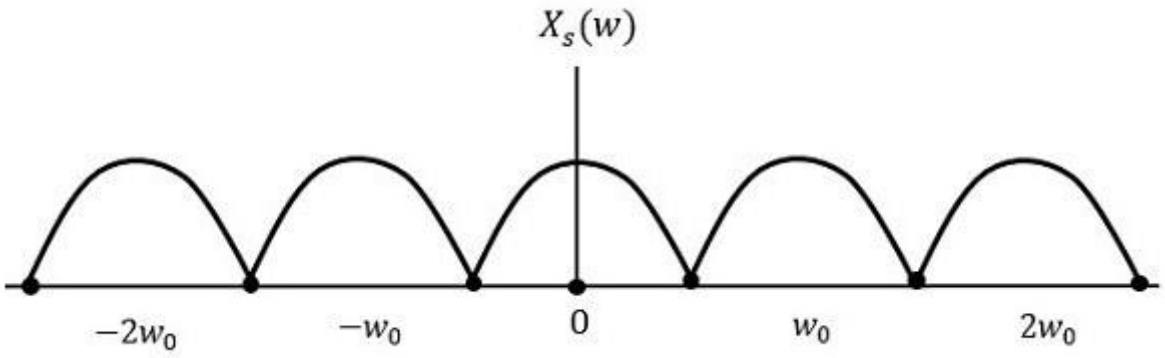
We can observe from the above pattern that there is over-lapping of information, which leads to mixing up and loss of information. This unwanted phenomenon of over-lapping is called as **Aliasing**.

- If fs<2fm, low pass filtered signal contains some high frequency components along with message signal due to spectral overlapping.
- The presence of high frequency signal in the reconstructed signal causes distortion. This is called as **Aliasing effect**.



Aliasing can be referred to as "the phenomenon of a high-frequency component in the spectrum of a signal, taking on the identity of a low-frequency component in the spectrum of its sampled version."

Hence, the sampling rate of the signal is chosen to be as Nyquist rate. If the sampling rate is equal to twice the highest frequency of the given signal **W**, then the sampled signal would look like the following figure.



In this case, the signal can be recovered without any loss. Hence, this is a good sampling rate.

2.9 PULSE AMPLITUDE MODULATION

Pulse Amplitude Modulation (PAM) is an analog modulating scheme in which the amplitude of the pulse carrier varies proportional to the instantaneous amplitude of the message signal.

The pulse amplitude modulated signal, will follow the amplitude of the original signal, as the signal traces out the path of the whole wave. In natural PAM, a signal sampled at the Nyquist rate is reconstructed, by passing it through an efficient **Low Pass Frequency (LPF)** with exact cutoff frequency

The following figures explain the Pulse Amplitude Modulation.

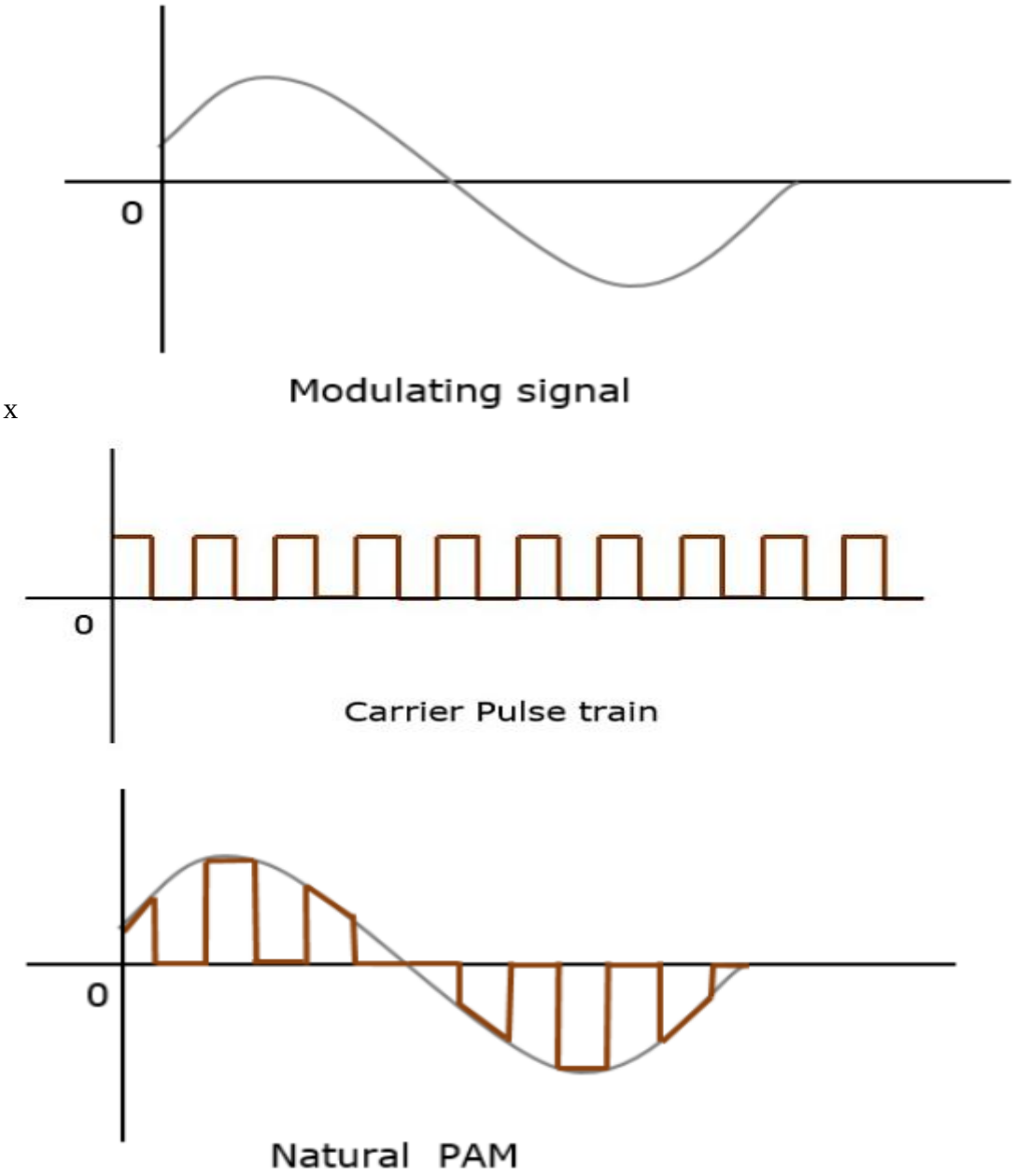
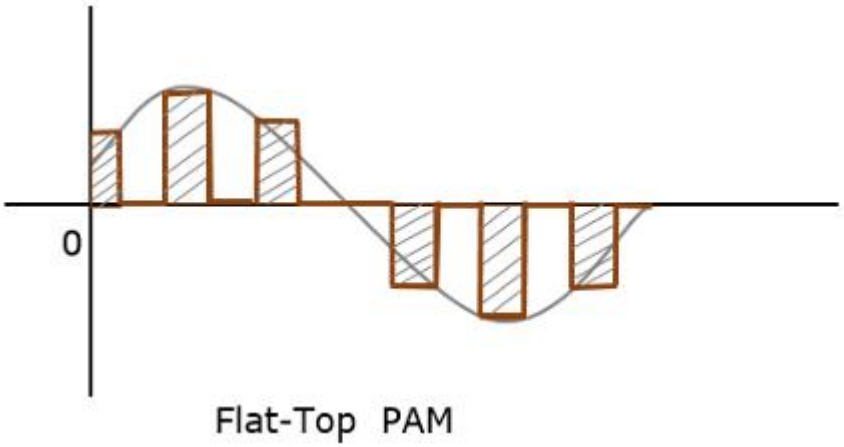


Figure 2.9 pulse amplitude modulation

Though the PAM signal is passed through an LPF, it cannot recover the signal without distortion. Hence to avoid this noise, flat-top sampling is done as shown in the following figure.



Flat-top sampling is the process in which sampled signal can be represented in pulses for which the amplitude of the signal cannot be changed with respect to the analog signal, to be sampled. The tops of amplitude remain flat. This process simplifies the circuit design.

2.10 PULSE WIDTH MODULATION

Pulse Width Modulation (PWM) or **Pulse Duration Modulation (PDM)** or **Pulse Time Modulation (PTM)** is an analog modulating scheme in which the duration or width or time of the pulse carrier varies proportional to the instantaneous amplitude of the message signal.

The width of the pulse varies in this method, but the amplitude of the signal remains constant. Amplitude limiters are used to make the amplitude of the signal constant. These circuits clip off the amplitude, to a desired level and hence the noise is limited.

The following figures explain the types of Pulse Width Modulations.

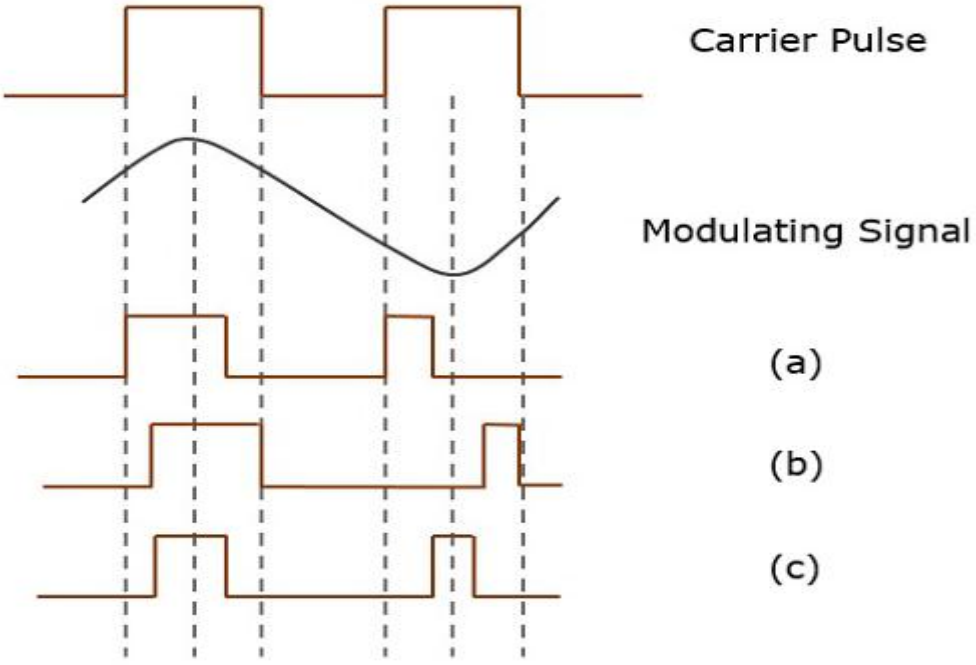


Figure 2.10 pulse width modulation

There are three variations of PWM. They are −

- The leading edge of the pulse being constant, the trailing edge varies according to the message signal.
- The trailing edge of the pulse being constant, the leading edge varies according to the message signal.
- The center of the pulse being constant, the leading edge and the trailing edge varies according to the message signal.

2.11 PULSE POSITION MODULATION

Pulse Position Modulation (PPM) is an analog modulating scheme in which the amplitude and width of the pulses are kept constant, while the position of each pulse, with reference to the position of a reference pulse varies according to the instantaneous sampled value of the message signal.

The transmitter has to send synchronizing pulses (or simply sync pulses) to keep the transmitter and receiver in synchronism. These sync pulses help maintain the position of the pulses. The following figures explain the Pulse Position Modulation.

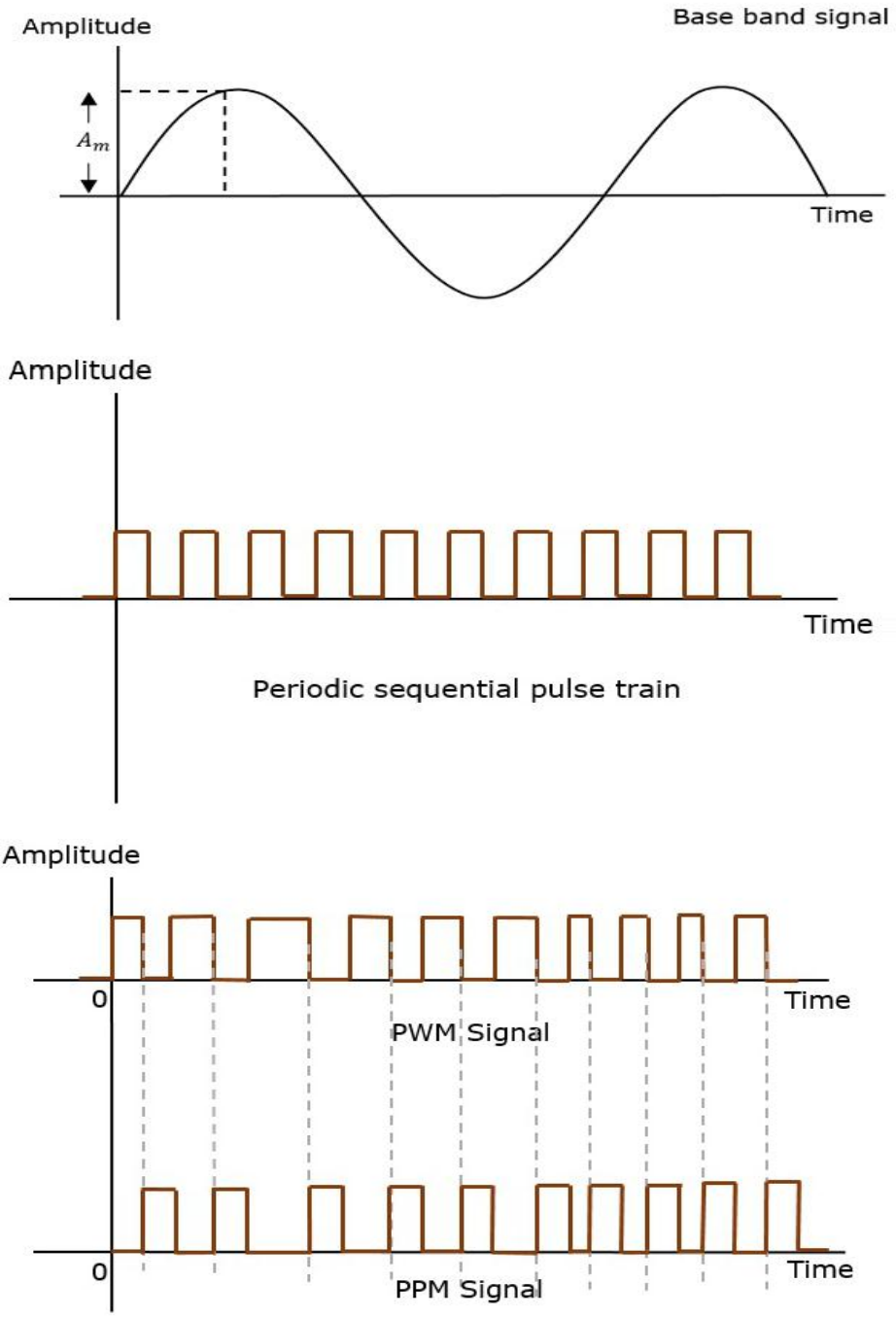


Figure 2.11 pulse position modulation

Pulse position modulation is done in accordance with the pulse width modulated signal. Each trailing of the pulse width modulated signal becomes the starting point for pulses in PPM signal. Hence, the position of these pulses is proportional to the width of the PWM pulses.

Advantage

As the amplitude and width are constant, the power handled is also constant.

Disadvantage

The synchronization between transmitter and receiver is a must

2.12 Comparison between PAM, PWM, and PPM

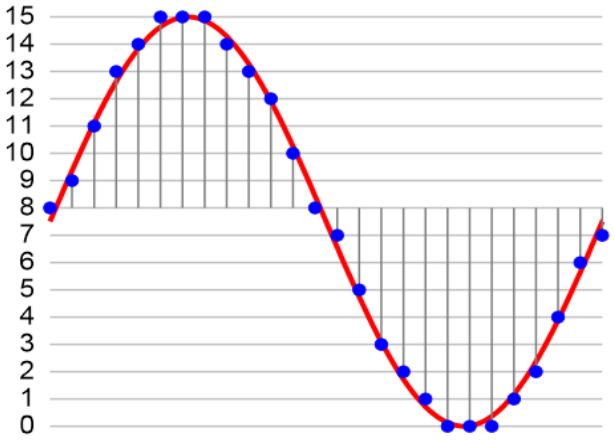
The comparison between the above modulation processes is presented in a single table.

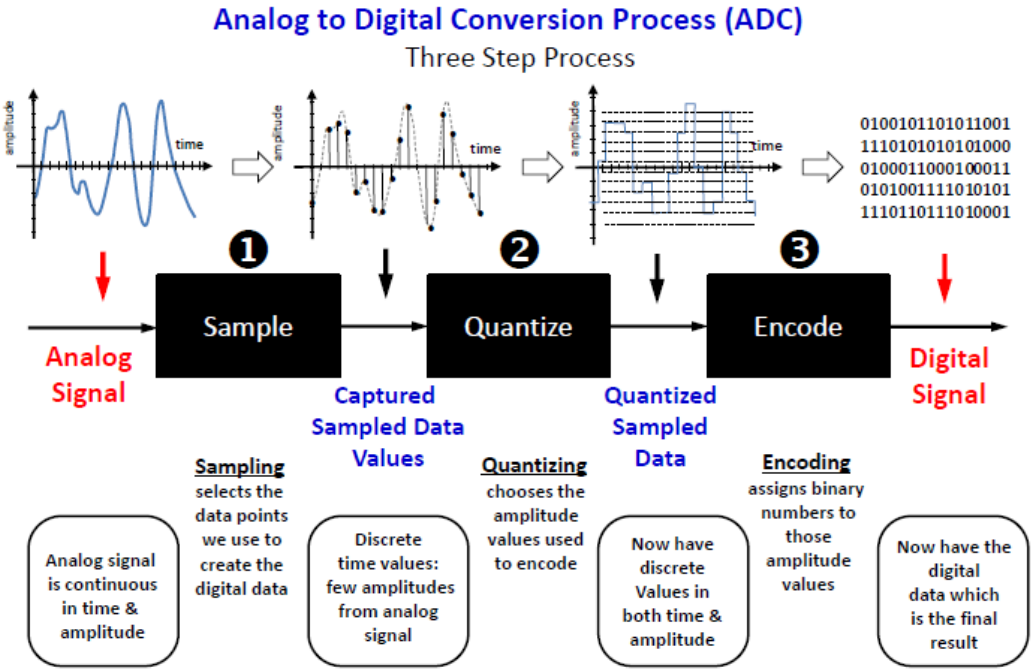
PAM	PWM	PPM
Amplitude is varied	Width is varied	Position is varied
Bandwidth depends on the width of the pulse	Bandwidth depends on the rise time of the pulse	Bandwidth depends on the rise time of the pulse
Instantaneous transmitter power varies with the amplitude of the pulses	Instantaneous transmitter power varies with the amplitude and width of the pulses	Instantaneous transmitter power remains constant with the width of the pulses
System complexity is high	System complexity is low	System complexity is low
Noise interference is high	Noise interference is low	Noise interference is low
It is similar to amplitude modulation	It is similar to frequency modulation	It is similar to phase modulation

Table 2.12

Pulse-code modulation (PCM)

Pulse-code modulation (PCM) is used to digitally represent sampled analog signals. It is the standard form of digital audio in computers, CDs, digital telephony and other digital audio applications. The amplitude of the analog signal is sampled at uniform intervals and each sample is quantized to its nearest value within a predetermined range of digital levels.





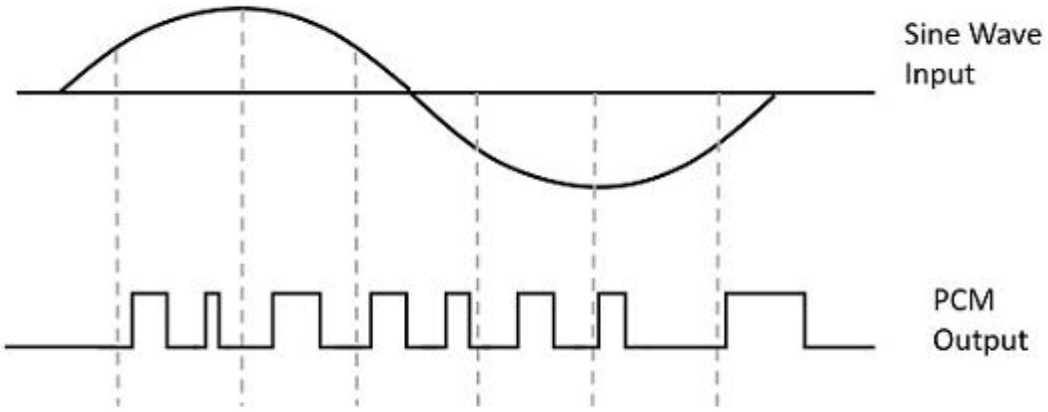
Note: "Discrete time" corresponds to the timing of the sampling.

Modulation is the process of varying one or more parameters of a carrier signal in accordance with the instantaneous values of the message signal.

The message signal is the signal which is being transmitted for communication and the carrier signal is a high frequency signal which has no data, but is used for long distance transmission.

There are many modulation techniques, which are classified according to the type of modulation employed. Of them all, the digital modulation technique used is **Pulse Code Modulation** PCMPCM.

A signal is pulse code modulated to convert its analog information into a binary sequence, i.e., **1s** and **0s**. The output of a PCM will resemble a binary sequence. The following figure shows an example of PCM output with respect to instantaneous values of a given sine wave.



Instead of a pulse train, PCM produces a series of numbers or digits, and hence this process is called as **digital**. Each one of these digits, though in binary code, represent the approximate amplitude of the signal sample at that instant.

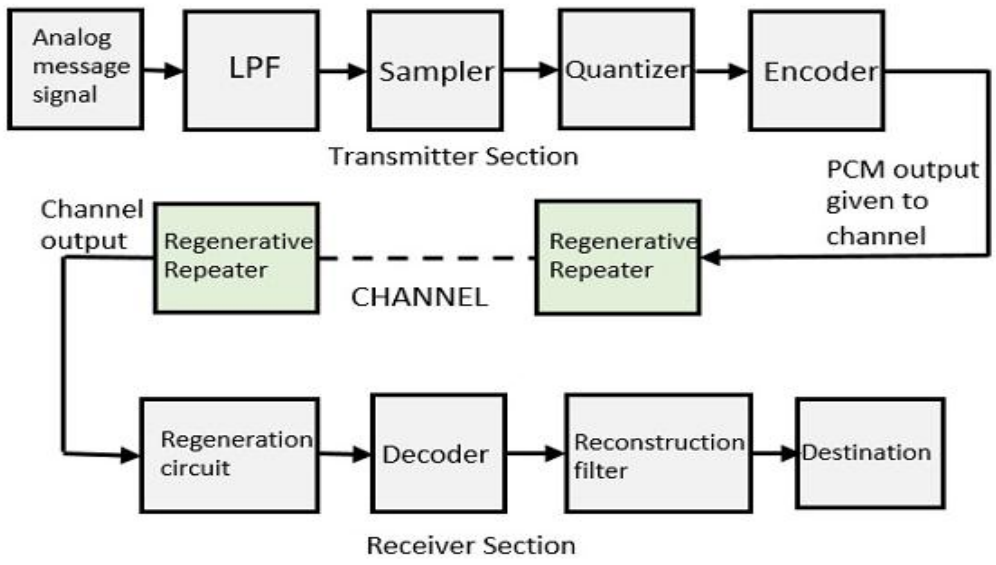
In Pulse Code Modulation, the message signal is represented by a sequence of coded pulses. This message signal is achieved by representing the signal in discrete form in both time and amplitude.

2.13 Basic Elements of PCM

The transmitter section of a Pulse Code Modulator circuit consists of **Sampling, Quantizing** and **Encoding**, which are performed in the analog-to-digital converter section. The low pass filter prior to sampling prevents aliasing of the message signal.

The basic operations in the receiver section are **regeneration of impaired signals, decoding,** and **reconstruction** of the quantized pulse train. Following is the block diagram of PCM which represents the basic elements of both the transmitter and the receiver sections.

Figure 2.13 Block Diagram



Low Pass Filter

This filter eliminates the high frequency components present in the input analog signal which is greater than the highest frequency of the message signal, to avoid aliasing of the message signal.

Sampler

This is the technique which helps to collect the sample data at instantaneous values of message signal, so as to reconstruct the original signal. The sampling rate must be greater than twice the highest frequency component **W** of the message signal, in accordance with the sampling theorem.

Quantizer

Quantizing is a process of reducing the excessive bits and confining the data. The sampled output when given to Quantizer, reduces the redundant bits and compresses the value.

Encoder

The digitization of analog signal is done by the encoder. It designates each quantized level by a binary code. The sampling done here is the sample-and-hold process. These three sections LPF,Sampler,andQuantizerLPF,Sampler,andQuantizer will act as an analog to digital converter. Encoding minimizes the bandwidth used.

Regenerative Repeater

This section increases the signal strength. The output of the channel also has one regenerative repeater circuit, to compensate the signal loss and reconstruct the signal, and also to increase its strength.

Decoder

The decoder circuit decodes the pulse coded waveform to reproduce the original signal. This circuit acts as the demodulator.

Reconstruction Filter

After the digital-to-analog conversion is done by the regenerative circuit and the decoder, a low-pass filter is employed, called as the reconstruction filter to get back the original signal.

Hence, the Pulse Code Modulator circuit digitizes the given analog signal, codes it and samples it, and then transmits it in an analog form. This whole process is repeated in a reverse pattern to obtain the original signal.

The sampling rate of a signal should be higher than the Nyquist rate, to achieve better sampling. If this sampling interval in Differential PCM is reduced considerably, the sampleto-sample amplitude difference is very small, as if the difference is **1-bit quantization**, then the step-size will be very small i.e., **Δ** deltadelta.

Delta Modulation

The type of modulation, where the sampling rate is much higher and in which the stepsize after quantization is of a smaller value **Δ**, such a modulation is termed as **delta modulation**.

Features of Delta Modulation

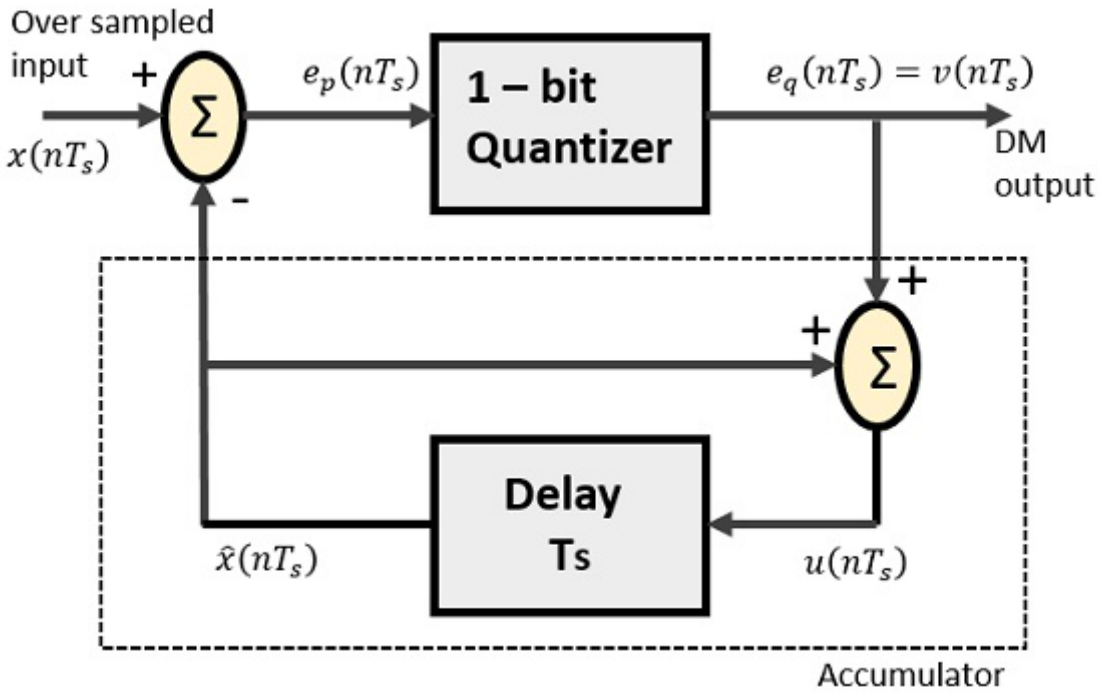
Following are some of the features of delta modulation.

- An over-sampled input is taken to make full use of the signal correlation.
- The quantization design is simple.
- The input sequence is much higher than the Nyquist rate.
- The quality is moderate.
- The design of the modulator and the demodulator is simple.
- The stair-case approximation of output waveform.
- The step-size is very small, i.e., **Δ** deltadelta.
- The bit rate can be decided by the user.
- This involves simpler implementation.

Delta Modulation is a simplified form of DPCM technique, also viewed as **1-bit DPCM scheme**. As the sampling interval is reduced, the signal correlation will be higher.

Delta Modulator

The Delta Modulator comprises of a 1-bit quantizer and a delay circuit along with two summer circuits. Following is the block diagram of a delta modulator.



The predictor circuit in DPCM is replaced by a simple delay circuit in DM.

From the above diagram, we have the notations as −

- x(nTs)x(nTs) = over sampled input
- ep(nTs)ep(nTs) = summer output and quantizer input
- eq(nTs)eq(nTs) = quantizer output = v(nTs)v(nTs)
- xˆ(nTs)x^(nTs) = output of delay circuit
- u(nTs)u(nTs) = input of delay circuit

The present input of the delay unit is given by

ThepreviousoutputofthedelayunitThepreviousoutputofthedelayunit + thepresentquantizeroutputthe presentquantizeroutput

Delay unit output is an Accumulator output lagging by one sample.

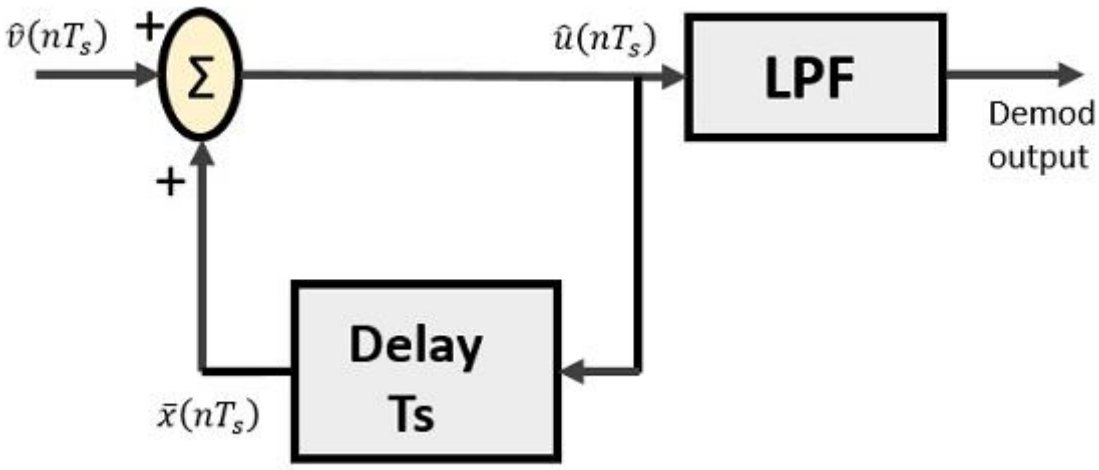
From equations 5 & 6, we get a possible structure for the demodulator.

A Stair-case approximated waveform will be the output of the delta modulator with the step-size as delta (**Δ**). The output quality of the waveform is moderate.

Delta Demodulator

The delta demodulator comprises of a low pass filter, a summer, and a delay circuit. The predictor circuit is eliminated here and hence no assumed input is given to the demodulator.

Following is the diagram for delta demodulator.



From the above diagram, we have the notations as −

- v^(nTs)v^(nTs) is the input sample
- u^(nTs)u^(nTs) is the summer output
- x¯(nTs)x¯(nTs) is the delayed output

A binary sequence will be given as an input to the demodulator. The stair-case approximated output is given to the LPF.

Low pass filter is used for many reasons, but the prominent reason is noise elimination for out-of-band signals. The step-size error that may occur at the transmitter is called **granular noise**, which is eliminated here. If there is no noise present, then the modulator output equals the demodulator input.

Advantages of DM Over DPCM

- 1-bit quantizer
- Very easy design of the modulator and the demodulator

However, there exists some noise in DM.

- Slope Over load distortion (when **Δ** is small)
- Granular noise (when **Δ** is large)

Applications

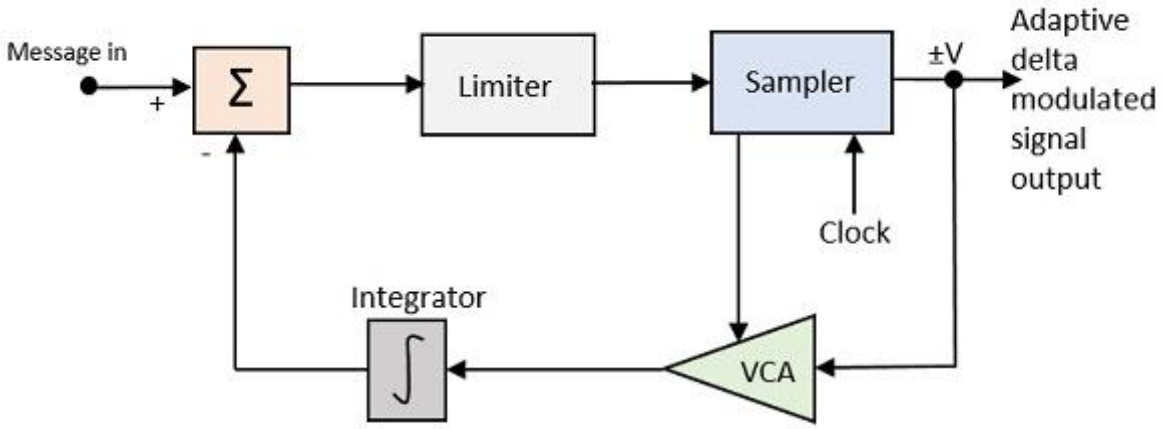
Delta Modulation is most useful in systems where timely data delivery at the receiver is more important than the data quality. This **modulation** is applied to ECG waveform for database reduction and real-time signal processing. For analog-to-PCM encoding, this **Modulation** method is used. It is widely used in radio communication devices and digital voice storage and voice information transmission where signal quality is less important.

Adaptive Delta Modulation ADM

In digital modulation, we have come across certain problem of determining the step-size, which influences the quality of the output wave.

A larger step-size is needed in the steep slope of modulating signal and a smaller stepsize is needed where the message has a small slope. The minute details get missed in the process. So, it would be better if we can control the adjustment of step-size, according to our requirement in order to obtain the sampling in a desired fashion. This is the concept of **Adaptive Delta Modulation**.

Following is the block diagram of Adaptive delta modulator.



Adaptive delta modulator

The gain of the voltage controlled amplifier is adjusted by the output signal from the sampler. The amplifier gain determines the step-size and both are proportional.

ADM quantizes the difference between the value of the current sample and the predicted value of the next sample. It uses a variable step height to predict the next values, for the faithful reproduction of the fast varying values.

Applications of Adaptive Delta Modulation

- It is effectively used in audio communications.
- It can be used in systems that require improved voice quality.
- It is used in voice coding.
- It is used in television signal transmission.

Multiplexing

Multiplexing is the process of combining multiple signals into one signal, over a shared medium. If the analog signals are multiplexed, then it is called as **analog multiplexing**. Similarly, if the digital signals are multiplexed, then it is called as **digital multiplexing**.

Multiplexing was first developed in telephony. A number of signals were combined to send through a single cable. The process of multiplexing divides a communication channel into several number of logical channels, allotting each one for a different message signal or a data stream to be transferred. The device that does multiplexing can be called as **Multiplexer** or **MUX**.

The reverse process, i.e., extracting the number of channels from one, which is done at the receiver is called as **de-multiplexing**. The device that does de-multiplexing can be called as **de-multiplexer** or **DEMUX**.

The following figures illustrates the concept of MUX and DEMUX. Their primary use is in the field of communications.

Multiplexing and Demultiplexing

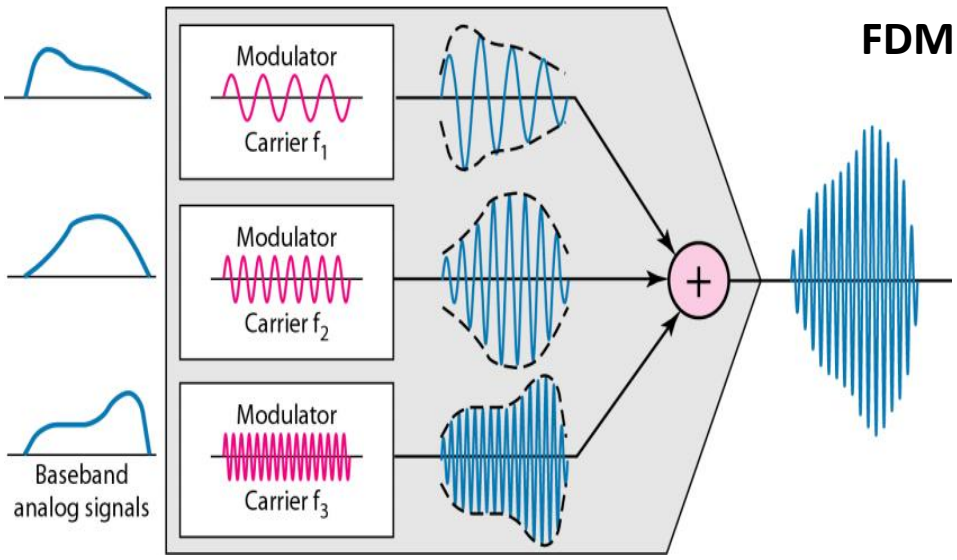
Types of Multiplexers

There are mainly two types of multiplexers, namely analog and digital. They are further divided into

- Frequency Division Multiplexing (FDM),
- Time Division Multiplexing (TDM).
- Quadrature carrier multiplexing (QCM)

2.14 Frequency Division Multiplexing(FDM)

- FDM is an analog multiplexing technique that combines different signals by modulating each analog signal with a different carrier frequency.



Demultiplexing FDM signal

Demultiplexing is the processing of recovering the individual baseband signals from the multiplexed signal

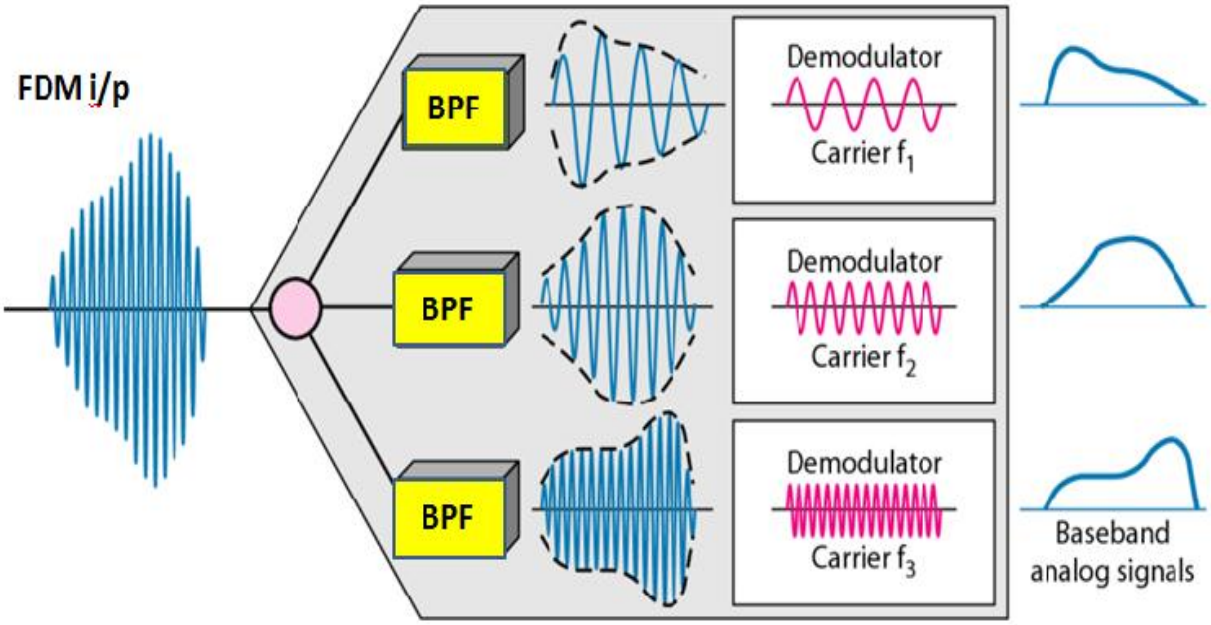
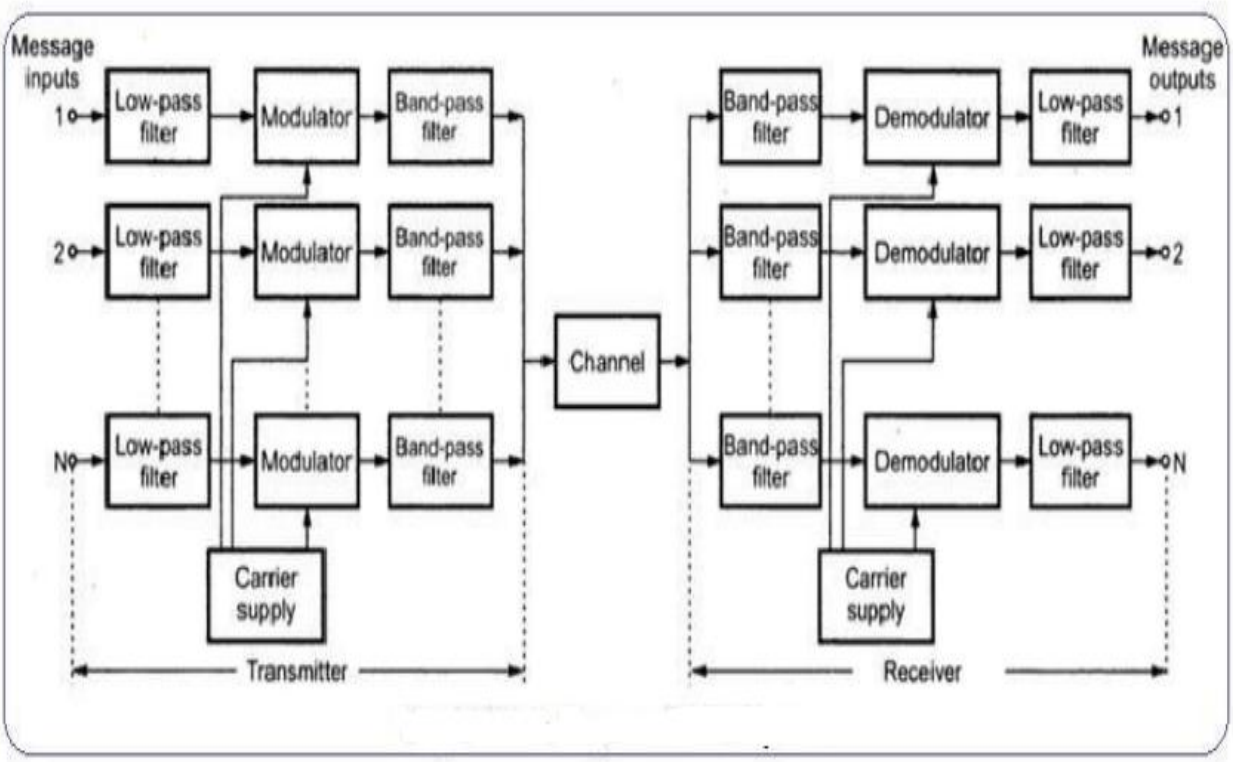
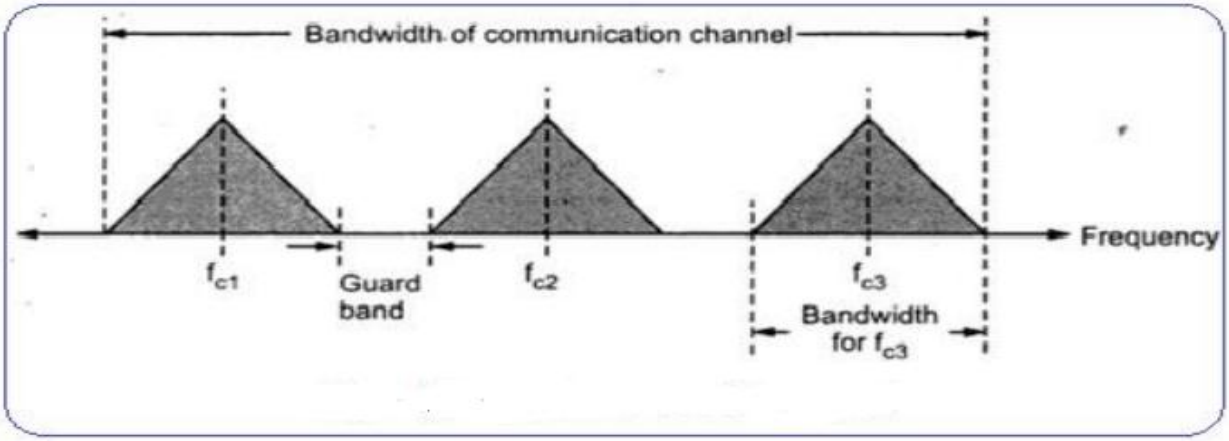


Figure 2.14 Block Diagram of FDM System



Spectrum of FDM

- Spectrum of FDM signal shows that each subcarrier modulated signal is separated by a **small frequency band** to prevent inter-channel interference or cross talk. These unused frequency band between each successive channel are known as **guard bands**.If the channels are very close to one other, it leads to inter-channel cross talk.



Merits and Demerits of FDM

Advantages of FDM

i. The frequency division multiplexing does not need synchronization between its transmitter and receiver for proper operation.
ii. A large number of signals (channels) can be transmitted simultaneously.
iii. Due to slow narrow band fading only a single channel gets affected.
iv. The Demodulation process of frequency division multiplexing is easy.

Disadvantages of FDM

i. All the frequency division multiplexing channels get affected due to wideband fading.
ii. A large number of modulators and filters are required.
iii. The communication channel must have a very large bandwidth.
iv. The frequency division multiplexing suffers from the problem of crosstalk.
v. Intermodulation distortion takes place.

Applications of FDM

i. FDM is commonly used in TV networks.
ii. FDM is used for FM & AM radio broadcasting.
iii. First generation cellular telephone also uses FDM.

2.15 Time division Multiplexing

- TDM is a multiplexing technique in which each signal is assigned a

different time slot for transmission. TDM requires synchronization between the switching unit at Transmitter and Receiver.

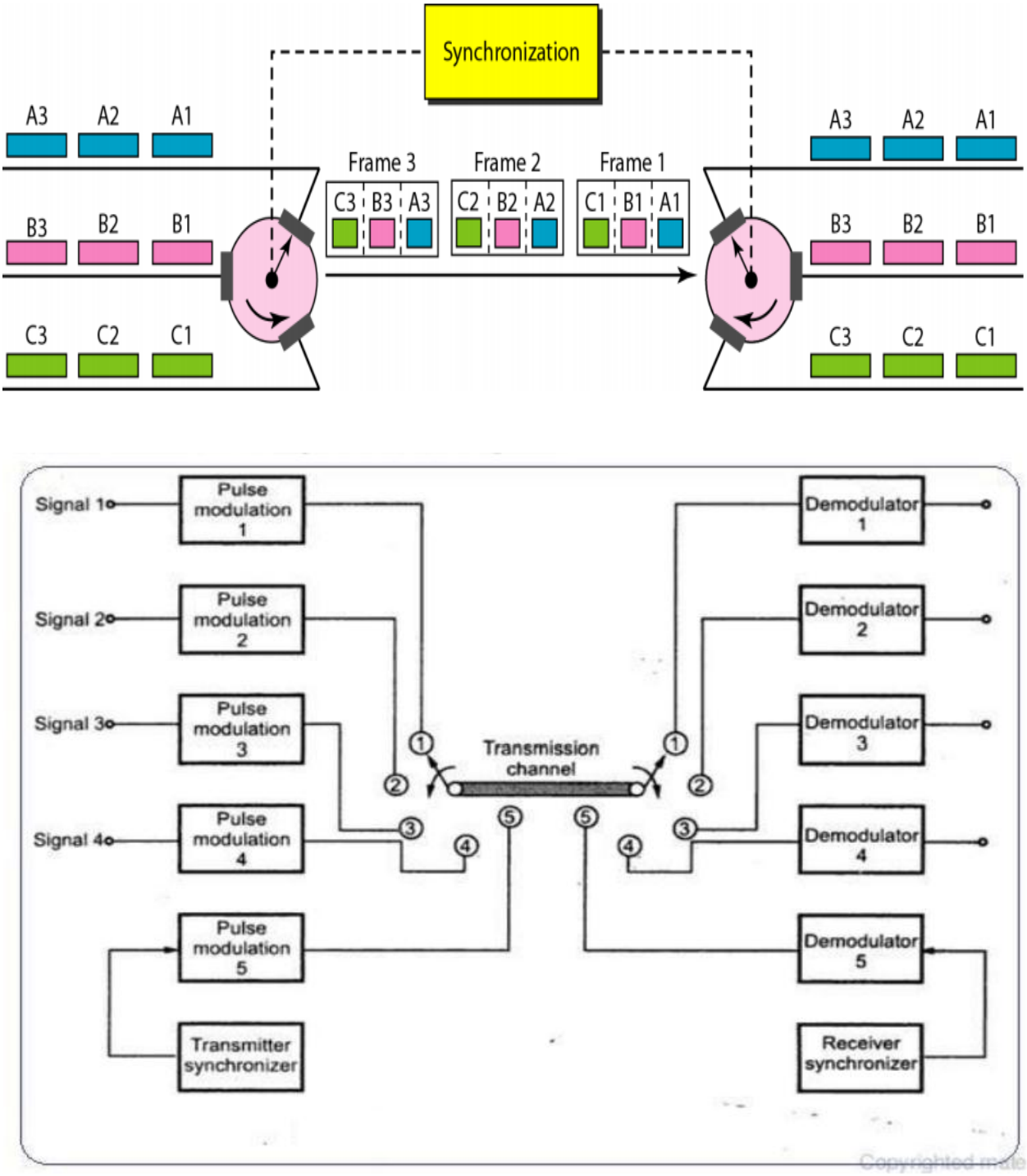


Figure 2.15 Block diagram of TDM system

Merits and Demerits of TDM

Advantages:

- Time division multiplexing circuitry is not complex.
- Problem of cross talk is not severe.
- Full available channel bandwidth can be utilized for each channel.

Disadvantage:

- Synchronization is required in time division multiplexing.

Applications:

- It used in ISDN (Integrated Services Digital Network) telephone lines.
- It is used in PSTN (public switched telephone network).

TEXT / REFERENCE BOOKS:

1. William Stallings, Data and Computer Communications, 10th Edition, Pearson, 2014.
2. Wayne Thomasi, "Advanced Electronic Communication Systems", 6th Edition, PHI Publishers, 2003.
3. Simon Haykins, “Communication Systems” John Wiley, 5th Edition, March 2009.
4. John G. Proakis, MasoudSalehi, “Digital Communication”, McGraw Hill 5th edition November 6, 2007.
5. Bernard Sklar, “Digital Communication, Fundamentals and Application”, Pearson Education Asia, 2nd Edition, Jan. 21, 2001.
6. Behrouz A. Forouzen, “Data communication and Networking”, Fourth Edition, Tata McGraw – Hill, 2011.
7. Andrew S.Tanenbaum, “Computer Networks”, 5th Edition, Pearson, 2011.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ECE

UNIT III INTRODUCTION TO DATA COMMUNICATION AND OSI MODEL - SCSA1305

UNIT 3 INTRODUCTION TO DATA COMMUNICATION AND OSI MODEL

Introduction to computer communication: Transmission modes - Switching: circuit switching and packet switching, OSI model, Layers in OSI model, TCP/IP protocol suite. Physical Layer: Guided and unguided transmission media (Co-axial cable, UTP,STP, Fiber optic cable), Data Link Layer: Framing, Flow control (stop and wait , sliding window flow control) ,Error control, HDLC, Media access control: Ethernet (802.3), CSMA/CD, Logical link control, Wireless LAN (802.11), CSMA/CA.

3.1 THE OSI MODEL

The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.

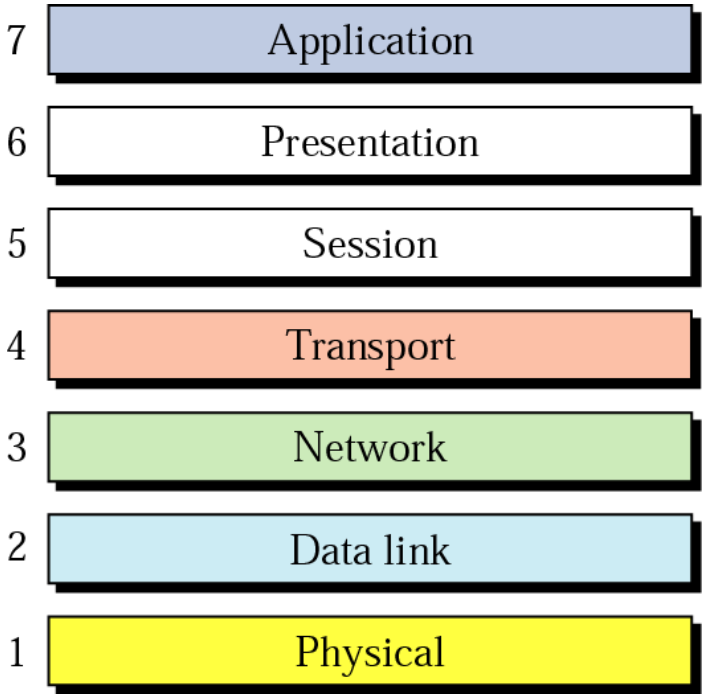


Figure 3.1 The seven layers of OSI model

The OSI model shown in fig. is based on the proposal developed by the International Standards Organization (ISO) as a first step towards international standardization of the protocols used in the various layers. The model is called the OSI (Open System Interconnection) reference model because it deals with connecting open systems, i.e., systems that are open for communication with other systems. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model

for understanding and designing a network architecture that is flexible, robust and interoperable. The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. Itconsists of seven separate but related layers, each of which defines a part of the process of moving information across a network. The principles that were applied to arrive at the seven layers are as follows:

* A layer should be created where a different level of abstraction is needed.

* Each layer should perform a well-defined function.

* The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

* The layer boundaries should be chosen to minimize the information flow across the interfaces.

* The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

3.2 Layered Architecture:

The OSI model is composed of seven layers: Physical, Data link, Network, Transport, Session, Presentation, Application layers. Fig 1.26 shows the layers involved when a message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes involve only the first 3 layers of the OSI model. Within a single machine, each layer calls upon the services of the layer just below it, layer 3 for ex. Uses the services provided by layer 2 & provides services for layer 4. Between machines, layer X on one machine communicates with layer X on another machine. This communication is governedby an agreed upon series of rules & Conventions called protocols. The processes on each machine that communicate at a given layer are called peer — to — peer processes. Communication between machines is therefore a peer — to –peer process using the protocols appropriate to a given layer.

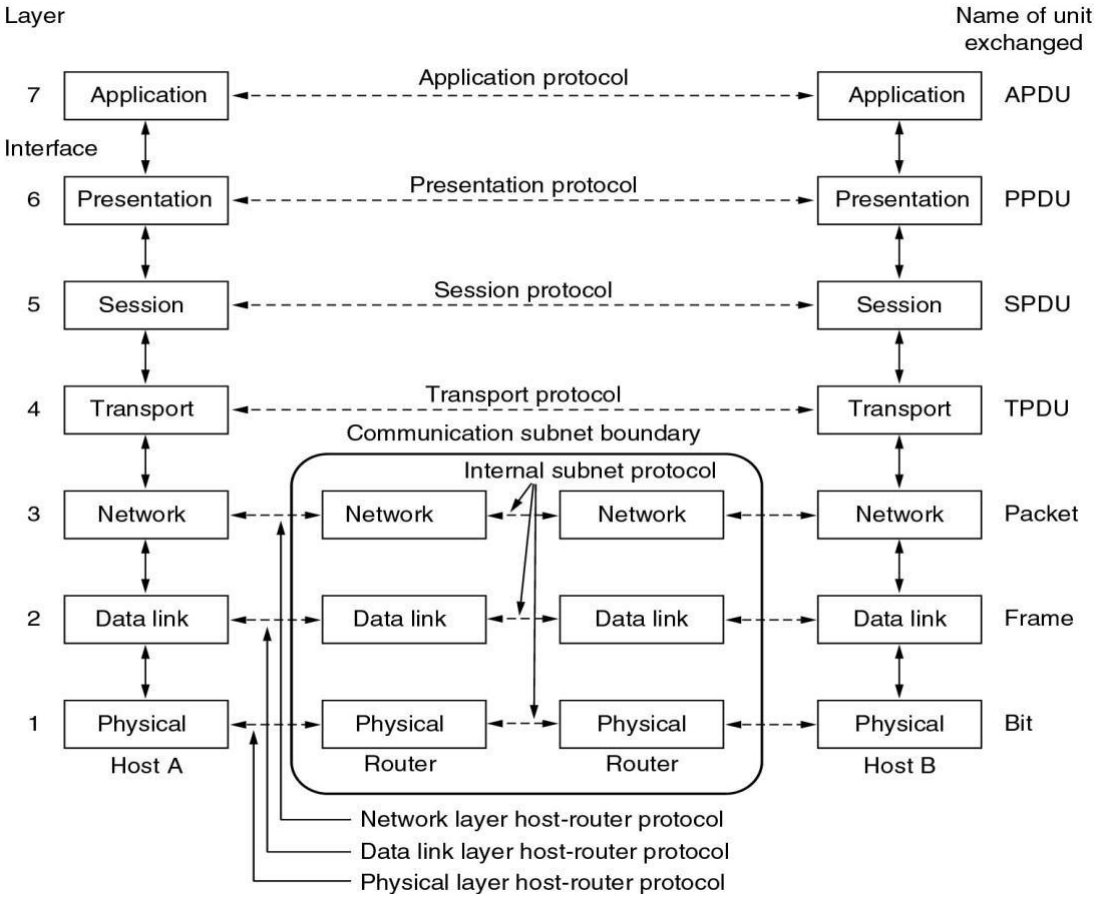


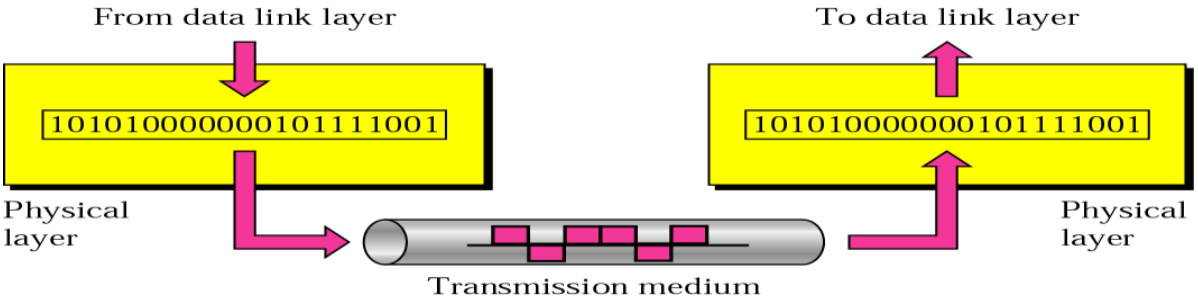
Figure 3.2 Interaction between the layers in the model

Layers in the OSI model:

i) Physical Layer:

The physical layer has as a main function to transmit bits over a communication channel as well as to establish and terminate a connection to a communications medium. It is also responsible to make sure that when one side sends a '1' bit the other side will receive '1' bit and not '0' bit.

Physical Layer is responsible for movements of individual bits from one node to the next



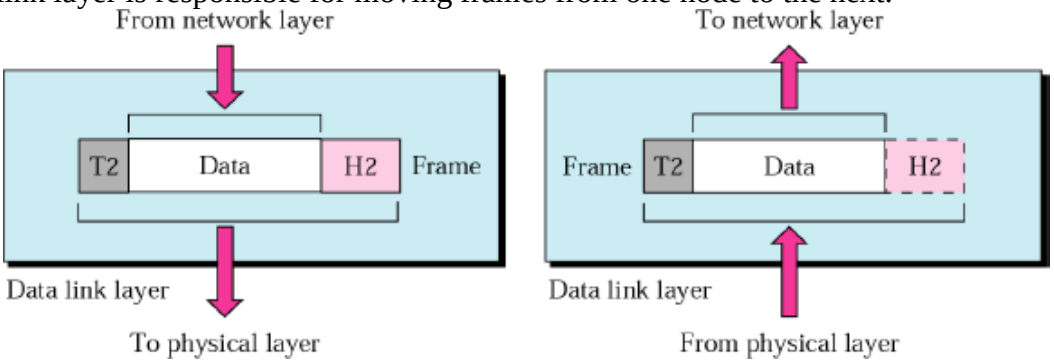
Physical characteristics of interfaces & medium, type of transmission medium.

- Representation of bits.
- Data rate.
- Synchronization of bits.
- Line configuration.
- Physical topology – Mesh, Star, Ring, Bus, Hybrid.
- Transmission mode – Simplex, Half-duplex, Full-duplex.

ii) Data Link Layer:

Data link layer provides means to transfer data between network entities. At the source machine it takes the bit streams of data from the Network Layer breaks into frames and passes them to the physical layer. At the receiving end data link layer detects and possibly corrects the errors that may occur during the transmission and passes the correct stream to the network layer. It's also concerned with flow control techniques.

Data link layer is responsible for moving frames from one node to the next.

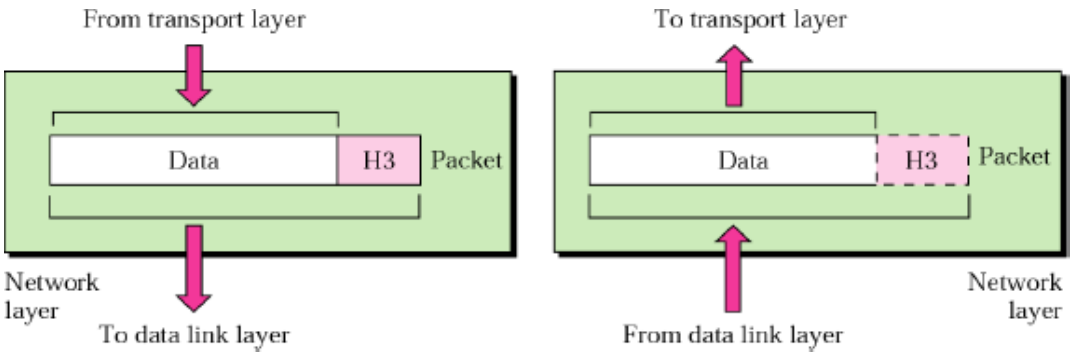


• Framing.
• Physical addressing.
• Flow control.
• Error control.
• Access control.

iii) Network Layer:

Network layer is responsible for the delivery of individual packets from the source host to the destination host.

This layer performs network routing, flow control and error control functions. Network routing simply means the way packets are routed from source to destination and flow control .prevents the possibility of congestion between packets which are present inthe subnet simultaneously and form bottlenecks.

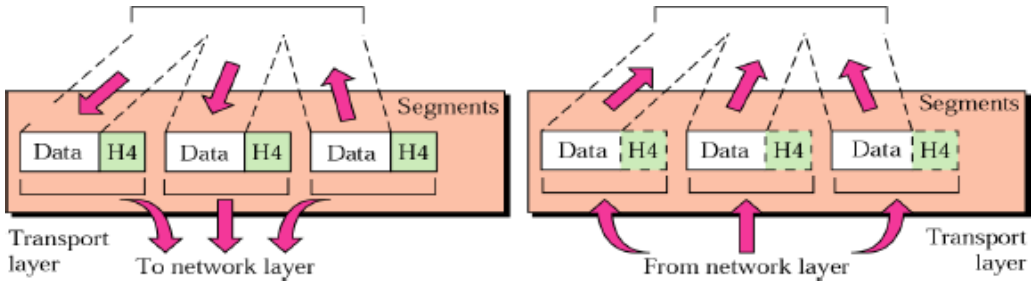


• Logical addressing.
• Routing.

Transport Layer:

The Transport Layer has as a main task to accept data from the Session layer, split them up into smaller units and passes them to the Network layer making sure that all the pieces arrive correctly to the destination. It is the first end-to-end layer all the way from source machine to destination machine unlike the first three layers which are chained having their protocols between each machine. This is shown clearly in the diagram above.

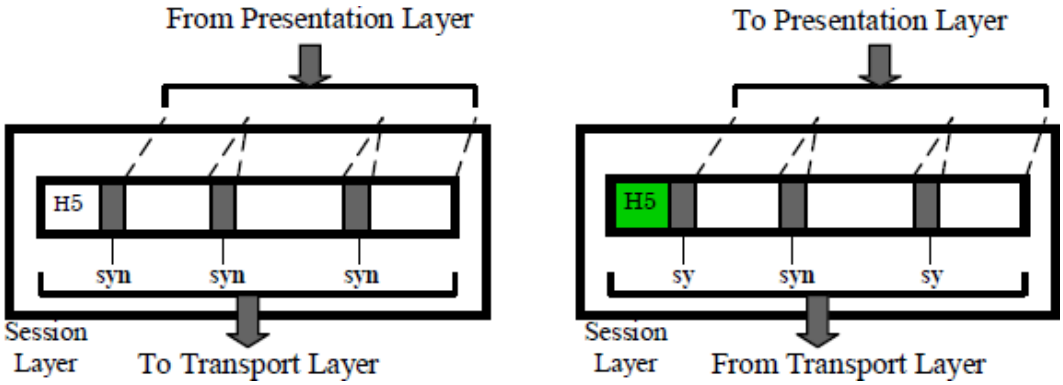
Transport layer is responsible for the delivery of a message from one process to another.



• Service-point addressing.
• Segmentation and reassembly.
• Connection control.
• Flow control.
• Error control.

iv)Session Layer:

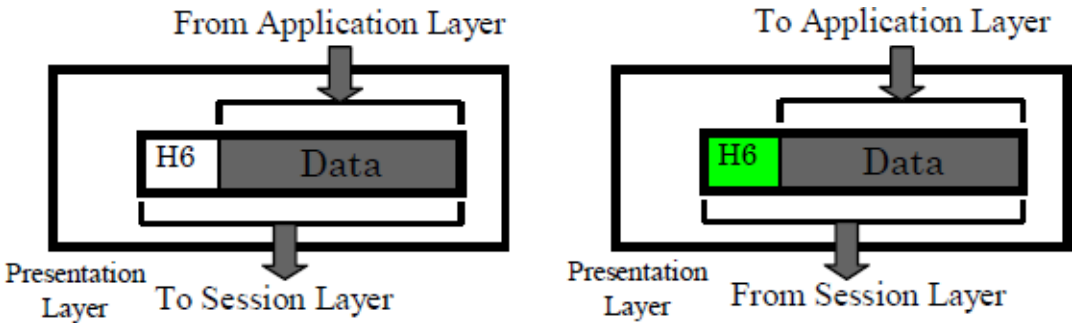
The session layer is responsible for dialog control and synchronization.



v) Presentation Layer:

It is responsible to translate different data formats from the representation used inside the computer (ASCII) to the network standard representation and back. Computersuse different codes for representing character strings so a standard encoding must be used and is handled by the presentation layer. Generally in a few words this layer is concerned

with the syntax and semantics of the informationtransmitted.

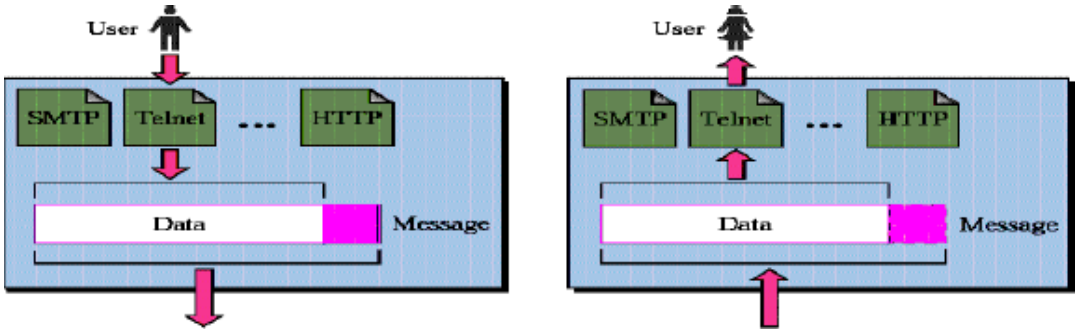


• Concerned with syntax and semantics of the information.
• Translation.
• Encryption.
• Compression.

vi) Application Layer:

The upper layer of this model performs common application service for the application processes meaning that software programs are written in the application layer to handle the many different terminal types that exist and map the virtual terminal software ontothe real terminal. It contains a variety of protocols and is concerned with file transfer as well as electronic mail, remote job entry and various other services of general interest.

The Application layer is responsible for providing services to the user.



• Network virtual terminal.
• File transfer, access, and management.
• Mail services.
• Directory services.

3.3 TCP/IP Protocol suite:

The TCP/IP protocol suite has four layers as shown in figure 1.27.

- Host – to – Network
- Internet
- Transport
- Application.

Comparing TCP/IP to OSI model: the Host — to — Network layer is equivalent to the combination of physical and data link layers, the Internet layer is equivalent to the network layer, the Transport layer in TCP/IP taking care of part of the duties of the session layer, and the application layer is roughly doing the job of the session, presentation, & application layers.

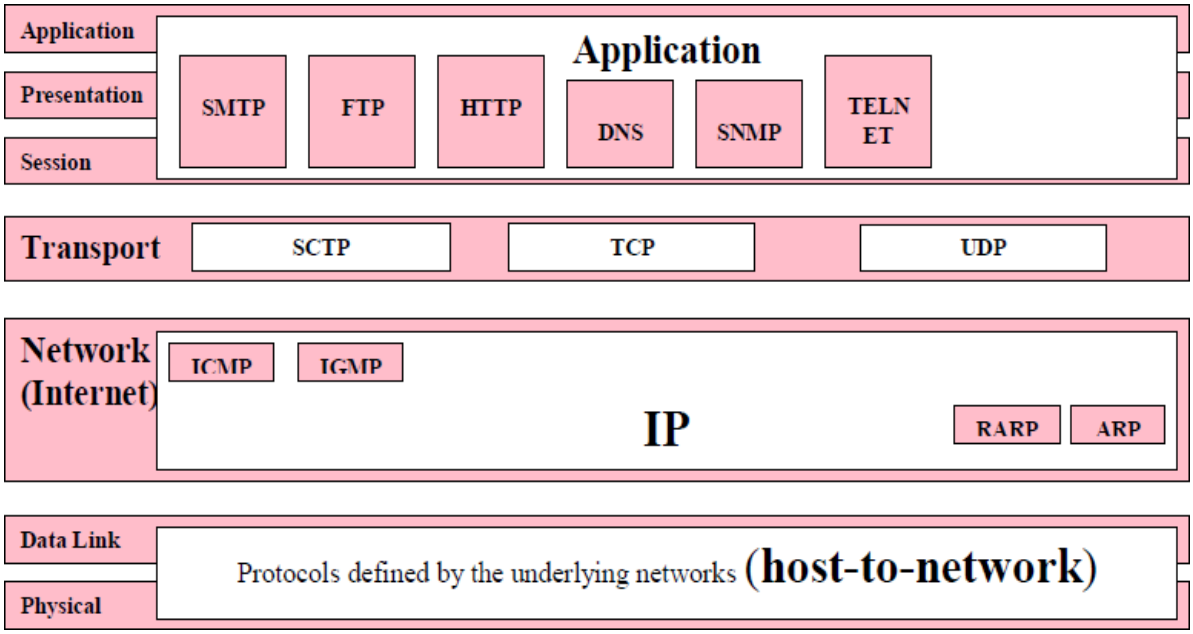


Figure 3.3 TCP/IP protocol suite

TCP/IP reference model was named after its two main protocols: TCP (Transmission Control Protocol) and IP (Internet Protocol). This model has the ability to connect multiple networks together in a way so that data transferred from a program in one computer are delivered safely to a similar program on another computer. The four layers are discussed as follows

(i) ***Host-to-Network Layer:*** It translates data and addresses information into format appropriate for an Ethernet Network or Token Ring Network. It uses a protocol (not specified due to lack of information concerned with this layer) in order for the host to connect to the network. Through this layer communication is achieved with physical links such as twisted pair or fiber optics carrying 1's and 0's.

(ii) ***Internet Layer:*** This layer is a connectionless internetwork layer and defines a connectionless protocol called IP. Its concerned with delivering packets from source to destination. These packets travel independently each taking a different route so may arrivein a different order than they were send. Internet layer does not care about the order the packets arrive at the destination as this job belongs to higher layers.

(iii) ***Transport Layer:*** It contains two end-to-end protocols. **TCP** is a connection oriented

(iv) protocol and is responsible for keeping track of the order in which packets are sent and reassemble arriving packets in the correct order. It also ensures that a byte stream originating on one machine to be delivered without error on any other machine on the internet. The incoming byte stream is fragmented into discrete messages and is passed to the internet layer. With an inverse process, at the destination, an output stream is produced by reassembling the received massage.

(v) ***UDP*** is the second protocol in this layer and it stands for User Datagram Protocol. In contrast to TCP, UDP is a connectionless protocol used for applications operating on its own flow control independently from TCP. It is also an unreliable protocol and is widely used for applications where prompt delivery is more important than accurate delivery such as transmitting speech or video.

(vi) ***Application Layer:*** Is the upper layer of the model and contains different kindsof protocols used for many applications. It includes virtual terminal, TELNET for remote accessing on a distance machine, File Transfer Protocol FTP and e-mail (SMTP). It also contains protocols like HTTP for fetching pages on the www and others.

3.4 Addressing:

Four levels of addresses are used in an internet employing the TCP/IP Protocols shown infigure 1.28

i) Physical addresses
ii) Logical addresses

iii) Port addresses

iv) Specific addresses

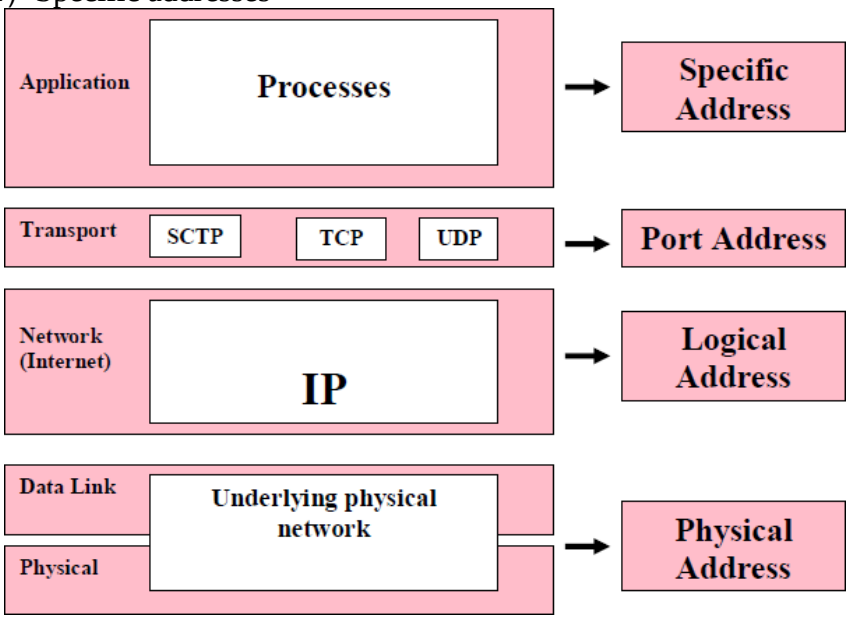


Figure 3.4 Four level of addressing schemes

3.5 Point to Point Networks

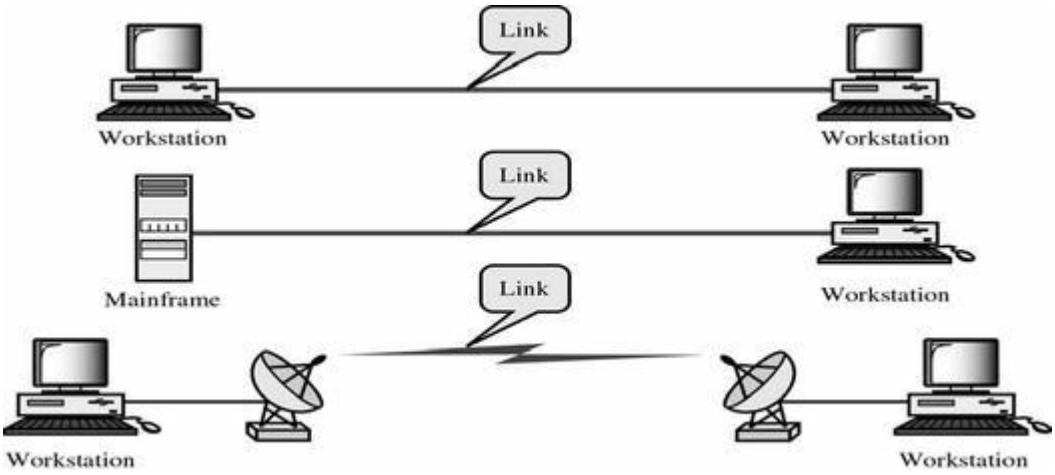


Fig 3.5.1 Point to Point Networks

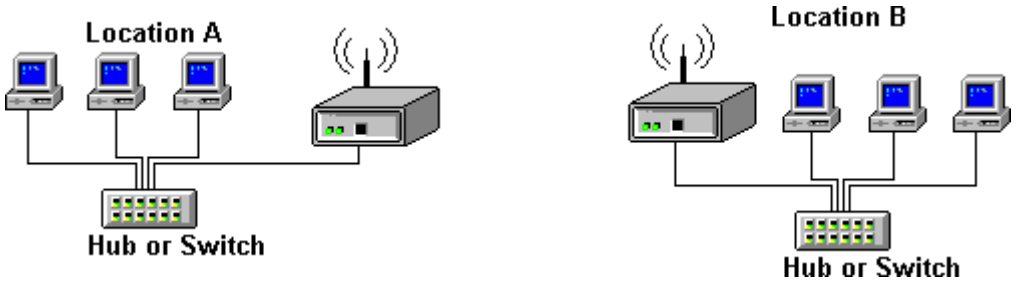


Fig 3.5.2 Point to Point Networks scenario

Point to point networks is used to connect one location to one other location. The above diagram shows two connected multi-user networks (using a Hub or Switch). Either location (A or B) may be configured as direct (without a Hub or Switch).

Application:

Internet, Intranet or Extranet configurations. ISP access networks (bridged or routed). LAN to LAN applications (bridged or routed see below). Remote data capture (Telemetry or SCADA). Remote Control. Remote Monitoring. Security.

Bridged or Routed

In a bridged connection the traffic sent from location A to Location B AND from Location B to Location A consists of:

- Traffic for a PC or system on the remote network
- Broadcast traffic (e.g. network management)
- Multicast traffic

In effect the two locations operate as a single, fully transparent LAN. Where both LANs consist of many systems the broadcast traffic can be considerable and consideration should be given to a routed network.

In a routed connection the traffic sent from location A to Location B AND from Location B to Location A consists of:

- Traffic for a PC or system on the remote network only

In this case the two LANs operate independently but communication is enabled between them.

3.6 Routing and Flow Control: The two main functions performed by a routing algorithm are the selection of routes for various origin-destination pairs and the delivery of messages to their correct destination once the routes are selected. The second function is conceptually straightforward using a variety of protocols and data structures (known as routing tables), someof which will be described in the context of practical networks in Section 5.1.2. The focus will be on the first function (selection of routes) and how it affects network performance. There are two main performance measures that are substantially affected by the routing algorithm-throughput (quantity of service) and average packet delay (quality of service). Routing interacts with flow control in detaining these performance measures

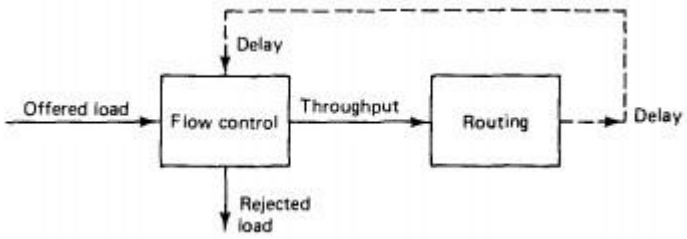


Figure 3.6 Interaction of routing and flow control. As good routing keeps delay low, flow control allows more traffic into the network.

by means of a feedback mechanism shown in Fig. 2.3. When the traffic load offered by the external sites to the subnet is relatively low, it will be fully accepted into the network, that is,

Throughput = offered load

When the offered load is excessive, a portion will be rejected by the flow control algorithm and throughput = offered load - rejected load The traffic accepted into the network will experience an average delay per packet that will depend on the routes chosen by the routing algorithm. However, throughput will also be greatly affected (if only indirectly) by the routing algorithm because typical flow control schemes operate on the basis of striking a balance between throughput and delay (i.e., they start rejecting offered load when delay starts getting excessive). Therefore, as the routing algorithm is more successful in keeping delay low, the flow control algorithm allows more traffic into the network. While the precise balance between delay and throughput will be determined by flow control, the effect of good routing under high offered load conditions is to realize a more favorable delay-throughput curve along which flow control operates, as shown in Fig. 2.4. The following examples illustrate the discussion above:

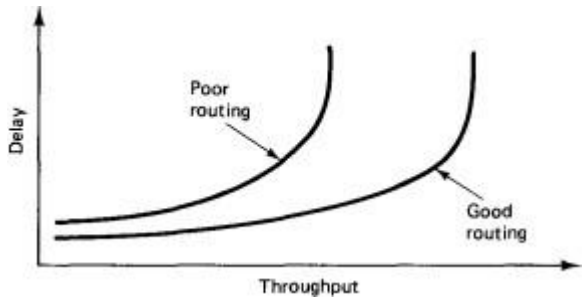


Figure 3.6 Delay-throughput operating curves for good and bad routing

Flow Control Sender does not flood the receiver, but maximizes throughput Sender throttled until receiver grants permission

Packet Switching Networks

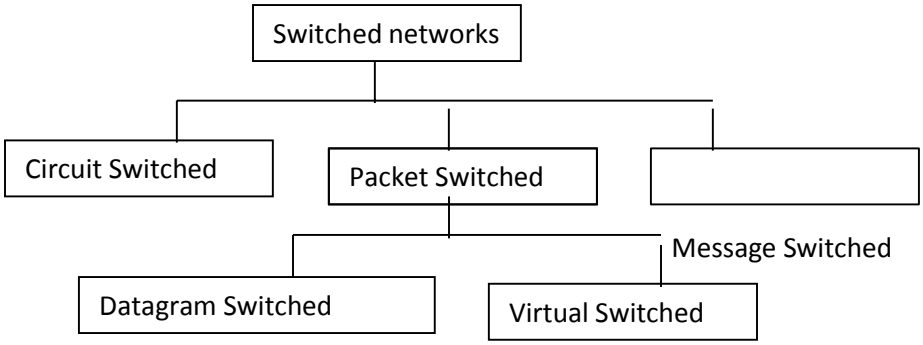
What is a Computer Network? • Communication Networks: "Sets of nodes that are interconnected to allow the exchange of information such as voice, sound, graphics, pictures, video, text, data, etc…" • Telephone Networks: " The first well established and most widely used communication networks which are used for voice transmission" – Telephone networks originally used analog transmission as a transmission technology for the information. However, digital transmission started to evolve replacing a lot of the analog transmission techniques used in telephone networks. • Computer Networks: "Collection of autonomous computers interconnected by a technology to allow exchange of information" A network is a series of connected devices. Whenever we have many devices, the interconnection between them becomes more difficult as the number of devices increases. Some of the conventional ways of interconnecting devices are

a. Point to point connection between devices as in mesh topology.

b. Connection between central device and every other device – as in star topology

c. Bus topology-not practical if the devices are at greater distances. The solution to this interconnectivity problem is switching. A switched network consists of a series of interlinked nodes called switches. A switch is a device that creates temporary connections between two or more systems. Some of the switches are connected to end systems (computers and telephones) and others are used only for routing.

Taxonomy of switched networks



Circuit switching

• Traditional telephone networks operate on the basis of circuit switching

• In conventional telephone networks, a circuit between two users must be established for a communication to occur

• Circuit switched networks requires resources to be reserved for each pair of end users

• The resources allocated to a call cannot be used by others for the duration of the call

The reservation of the network resources for each user results in an inefficient use of bandwidth for applications in which information transfer is bursty or if the information is small

Packet Switching

• Packet switched networks are the building blocks of computer communication systems in which data units known as packets flow across the networks.

• It provides flexible communication in handling all kinds of connections for a wide range ofapplications e.g. telephone calls, video conferencing, distributed data processing etc...

• Packet switched networks with a unified, integrated data infrastructure known as the Internet can provide a variety of communication services requiring different bandwidths.

• To make efficient use of available resources, packet switched networks dynamically allocate resources only when required.

• The form of information in packet switched networks is always digital bits.

Differences between Circuit Switching and Packet Switching

Circuit switching	**Packet switching**
1. Call set up is required.	1. Call setup is not required.
2. Dedicated connection between two Hosts.	2. No dedicated connection between two Hosts.
3. Connection/Communication is lost, if any link in the path between the Hosts is broken.	3. Connection/Communication could continue between the Hosts since data have many routes between the Hosts.
4. Information take the same route between the connected Hosts	4. Information could take different routes to reach the destination Host.
5. Information always arrives in order.	5. Information could arrive out of order to the destination
6. Bandwidth available is fixed.	6. Bandwidth available is variable.
7. Congestion is call based.	7. Congestion is packet based.
8. Bandwidth utilization is partial.	8. Bandwidth utilization is full.
9. It does not uses store-and-forward transmission.	9. It uses store-and forward transmission.
10. It is Transparent.	10. Not transparent.
11. Charging is time based.	11. Charging is packet based.

Packet networks can be viewed from two perspectives:

• ***External view of network :-*** It is Concerned with the services that the network provides to the transport layer

• Internal operation of the network.

Network service can be Connection-oriented service or connectionless service Connectionless service:

• Connectionless service is simple with two basic interactions (1) a request to network layer thatit send a packet (2) an indication from the network layer that a packet has arrived

• It puts total responsibility of error control, sequencing and flow control on the end system transport layer

Connection-oriented service:

The Transport layer cannot request transmission of information until a connection is established between end systems

Network layer must be informed about the new flow

Network layer maintains state information about the flows it is handling

During connection set up, parameters related to usage and quality of services may benegotiated and network resources may be allocated

Connection release procedure may be required to terminate the connection It is also possible fora network layer to provide a choice of services to the user of network like:

Best-effort connectionless servicesLow delay connectionless services

Connection oriented reliable stream services

Connection oriented transfer of packets with guaranteed delay and bandwidth

Physical Layer

Physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as 1 bit and not as 0 bit. In physical layer we deal with the communication medium used for transmission.

Types of Medium

Medium can be classified into 2 categories.

1. ***Guided Media:*** Guided media means that signals is guided by the presence of physical media i.e. signals are under control and remains in the physical wire. For eg. copper wire.
2. ***Unguided Media:*** Unguided Media means that there is no physical path for the signal to propagate. Unguided media are essentially electro-magnetic waves. There is no control on flow of signal. For eg. Radio waves.

Communication Links

In a network nodes are connected through links. The communication through links can be classified as

1. **Simplex :** Communication can take place only in one direction. eg. T.V broadcasting.
2. **Half-duplex :** Communication can take place in one direction at a time. Suppose node A and B are connected then half-duplex communication means that at a time data can flow from A to B or from B to A but not simultaneously. eg. two persons talking to each other such that when speaks the other listens and vice versa.
3. **Full-duplex :** Communication can take place simultaneously in both directions. eg. A discussion in a group without discipline.

Links can be further classified as

1. **Point to Point :** In this communication only two nodes are connected to each other. When a node sends a packet then it can be recieved only by the node on the other side and none else.
2. **Multipoint** : It is a kind of sharing communication, in which signal can be recieved by all nodes. This is also called broadcast.

Generally two kind of problems are associated in transmission of signals.

1. **Attenuation :** When a signal transmitts in a network then the quality of signal degrades as the signal travels longer distances in the wire. This is called attenuation. To improve quality of signal amplifiers are used at regular distances.
2. **Noise :** In a communication channel many signals transmits simultaneously, certain random signals are also present in the medium. Due to interference of these signals our signal gets disrupted a bit.

Bandwidth

Bandwidth simply means how many bits can be transmitted per second in the communication channel. In technical terms it indicates the width of frequency spectrum.

Transmission Media

- **Guided**
- Transmission
- **Media**

In Guided transmission media generally two kind of materials are used.

- Copper
- Coaxial Cable
- Twisted Pair
- Optical Fiber

3.7 Coaxial Cable: Coaxial cable consists of an inner conductor and an outer conductor which are seperated by an insulator. The inner conductor is usually copper. The outer conductor is covered by a plastic jacket. It is named coaxial because the two conductors are coaxial.Typical

diameter of coaxial cable lies between 0.4 inch to 1 inch. The most application of coaxial cable is cable T.V. The coaxial cable has high bandwidth, attenuation is less.

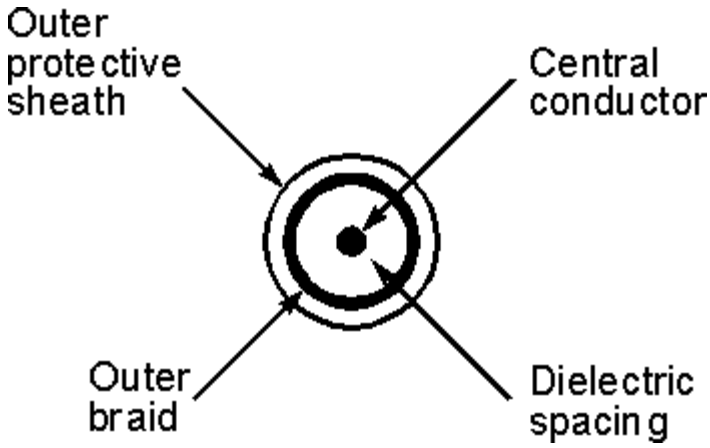


Figure 3.7 Coaxial Cable

3.8 Twisted Pair: A Twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form the purpose of twisting is to reduce cross talk interference between several pairs. Twisted Pair is much cheaper then coaxial cable but it is susceptible to noise and electromagnetic interference and attenuation is large.

Figure 3.8 Twisted Pair

Twisted Pair can be further classified in two categories:
Unshielded twisted pair: In this no insulation is provided, hence they are susceptible to interference.
***Shielded twisted pair*:** In this a protective thick insulation is provided but shielded twisted pair is expensive and not commonly used.

The most common application of twisted pair is the telephone system. Nearly all telephones are connected to the telephone company office by a twisted pair. Twisted pair can run several kilometers without amplification, but for longer distances repeaters are needed. Twisted pairs can be used for both analog and digital transmission. The bandwidth depends on the thicknessof wire and the distance travelled. Twisted pairs are generally limited in distance, bandwidth and data rate.

Optical Fiber: In optical fiber light is used to send data. In general terms presence of light is taken as bit 1 and its absence as bit 0. Optical fiber consists of inner core of either glassor plastic. Core is surrounded by cladding of the same material but of different refractive index. This cladding is surrounded by a plastic jacket which prevents optical fiber from electromagnetic interference and harsh environments. It uses the principle of total internal reflection to transfer data over optical fibers. Optical fiber is much better in bandwidth as compared to copper wire, since there is hardly any attenuation or electromagnetic interference in optical wires. Hence thereare fewer requirements to improve quality of signal, in long distance transmission. Disadvantage of optical fiber is that end points are fairly expensive. (eg. switches)

Differences between different kinds of optical fibers:

Depending on material

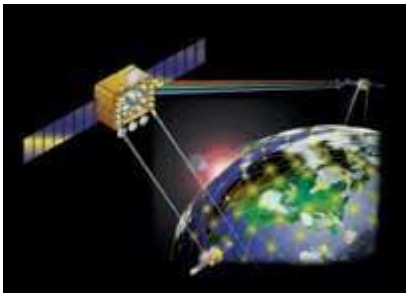
- Made of glass
- Made of plastic.
- Depending on radius
- Thin optical fiber
- Thick optical fiber
- Depending on light source
- LED (for low bandwidth)
- Injection laser diode (for high bandwidth)

Wireless Transmission

1. ***Radio:*** Radio is a general term that is used for any kind of frequency. But higher frequencies are usually termed as microwave and the lower frequency band comes under radio frequency. There are many application of radio. For eg. Cordless keyboard, wireless LAN, wireless Ethernet.
2. ***Terrestrial microwave:*** But it is limited in range to only a few hundred meters. Depending on frequency radio offers different bandwidths.
3. ***Terrestrial microwave:*** In terrestrial microwave two antennas are used for communication. A focused beam emerges from an antenna and is received by the other antenna, provided that antennas should be facing each other with no obstacle in between. For this reason antennas are situated on high towers. Due to curvature of earth terrestrial microwave can be used for long

distance communication with high bandwidth. Telecom department is also using this for long distance communication. An advantage of wireless communication is that it is not required to lay down wires in the city hence no permissions are required.

4. ***Satellite* communication:** Satellite acts as a switch in sky. On earth VSAT(Very Small Aperture Terminal) are used to transmit and receive data from satellite. Generally one station on earth transmits signal to satellite and it is received by many stations on earth. Satellite communication is generally used in those places where it is very difficult to obtain line of sight i.e. in highly irregular terrestrial regions. In terms of noise wireless media is not as good as the wired media. There are frequency band in wireless communication and two stations should not be allowed to transmit simultaneously in a frequency band. The most promising advantage of satellite is broadcasting. If satellites are used for point to point communication then they are expensive as compared to wired media.

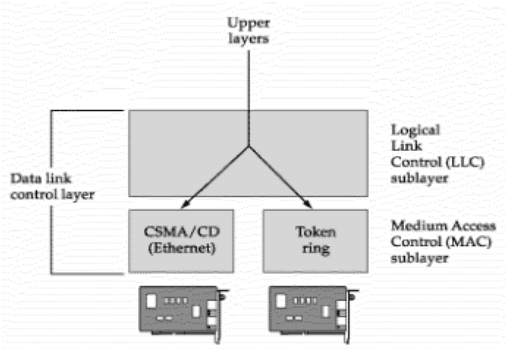


Data Link Layer

Data Link Layer Design Issues

This layer provides reliable transmission of a packet by using the services of the physical layer which transmits bits over the medium in an unreliable fashion. This layer is concerned with :

- Framing : Breaking input data into frames (typically a few hundred bytes) and caring about the frame boundaries and the size of each frame.
- Acknowledgment : Sent by the receiving end to inform the source that the frame was received without any error.
- Sequence Numbering : To acknowledge which frame was received.
- Error Detection : The frames may be damaged, lost or duplicated leading to errors.The error control is on **link to link** basis.
- Retransmission : The packet is retransmitted if the source fails to receive acknowledgment.
- Flow Control : Necessary for a fast transmitter to keep pace with a slow receiver.



Error Detecting Codes

Basic approach used for error detection is the use of redundancy, where additional bits are added to facilitate detection and correction of errors. Popular techniques are:

• Simple Parity check

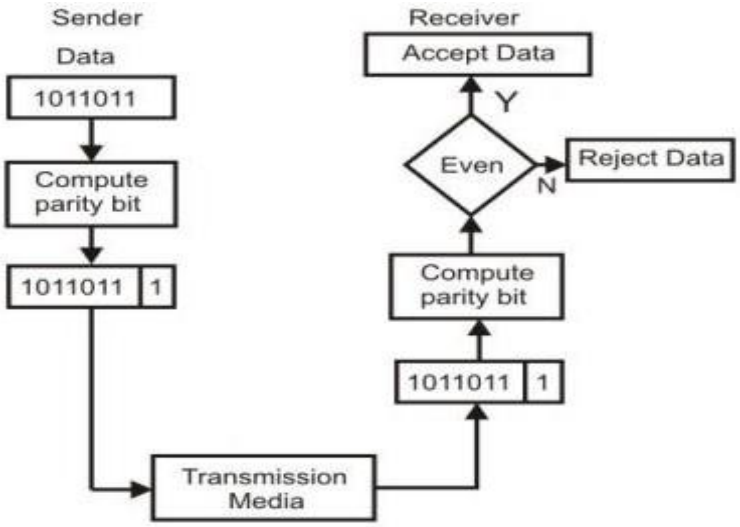
• Two-dimensional Parity check

• Checksum

• Cyclic redundancy check

Simple Parity Checking or One-dimension Parity Check The most common and least expensive mechanism for error- detection is the simple parity check. In this technique, a redundant bit called parity bit, is appended to every data unit so that the number of 1s in the unit (including the parity becomes even). Blocks of data from the source are subjected to a check bit or Parity bit generator form, where a parity of 1 is added to the block if it contains an odd number of 1's (ON bits) and 0 is added if it contains an even number of 1's. At the receiving end the parity bit is computed from the received data bits and compared with the received parity bit, as shown in

Fig2.8This scheme makes the total number of 1's even, that is why it is called even parity checking. Considering a 4-bit word, different combinations of the data words and the corresponding code words are given in Table



Even-parity checking scheme

Table : Possible 4-bit data words and corresponding code words

Decimal value	Data Block	Parity bit	Code word
0	0000	0	00000
1	0001	1	00011
2	0010	1	00101
3	0011	0	00110
4	0100	1	01001
5	0101	0	01010
6	0110	0	01100
7	0111	1	01111
8	1000	1	10001
9	1001	0	10010
10	1010	0	10100
11	1011	1	10111
12	1100	0	11000
13	1101	1	11011
14	1110	1	11101
15	1111	0	11110

Note that for the sake of simplicity, we are discussing here the even-parity checking, where the number of 1's should be an even number. It is also possible to use odd-parity checking, where the number of 1's should be odd.

Performance

An observation of the table reveals that to move from one code word to another, at least two

data bits should be changed. Hence these set of code words are said to have a minimum distance (hamming distance) of 2, which means that a receiver that has knowledge of the code word set can detect all single bit errors in each code word. However, if two errors occur in the code word, it becomes another valid member of the set and the decoder will see only another valid code word and know nothing of the error. Thus errors in more than one bit cannot be detected. In fact it can be shown that a single parity check code can detect only odd number of errors in a code word.

Error-Correcting Codes:

Network designers have developed two basic strategies for dealing with errors. One way is to include enough redundant information along with each block of data sent, to enable the receiver to deduce what the transmitted data must have been. The other way is to include only enough redundancy to allow the receiver to deduce that an error occurred, but not which error, and haveit request a retransmission. The former strategy uses error-correcting codes and the latter uses error-detecting codes. The use of error-correcting codes is often referred to as forward error correction.
Each of these techniques occupies a different ecological niche. On channels that are highly reliable, such as fiber, it is cheaper to use an error detecting code and just retransmit the occasional block found to be faulty. However, on channels such as wireless links that make many errors, it is better to add enough redundancy to each block for the receiver to be able to figure out what the original block was, rather than relying on a retransmission, which itself maybe in error.
To understand how errors can be handled, it is necessary to look closely at what an error reallyis. Normally, a frame consists of m data (i.e., message) bits and r redundant, or check, bits. Let the total length be n (i.e., n = m + r). An n-bit unit containing data and check bits is often referred to as an n-bit codeword.
Given any two code words, say, 10001001 and 10110001, it is possible to determine how many

Corresponding bits differ. In this case, 3 bits differ. To determine how many bits differ, just exclusive OR the two code words and count the number of 1 bits in the result, for example:

The number of bit positions in which two code words differ is called the Hamming distance. Its significance is that if two codeword's are a Hamming distance d apart, it will require d single-bit errors to convert one into the other.
In most data transmission applications, all 2m possible data messages are legal, but due to the way the check bits are computed, not all of the 2n possible code words are used. Given the algorithm for computing the check bits, it is possible to construct a complete list of the legal codeword's, and from this list find the two codeword's whose Hamming distance is minimum.This distance is the Hamming distance of the complete code. The error-detecting and error correcting properties of a code depend on its Hamming distance. To detect d errors, you need a distance d + 1 code because with such a code there is no way that d single-bit errors can changea valid codeword into another valid codeword. When the receiver sees an invalid codeword, itcan tell that a transmission error has occurred. Similarly, to correct d errors, you need a distance 2d + 1 code because that way the legal codewords are so far apart that even with d changes, theoriginal codeword is still closer than any other codeword, so it can be uniquely determined. As a simple example of an error-detecting

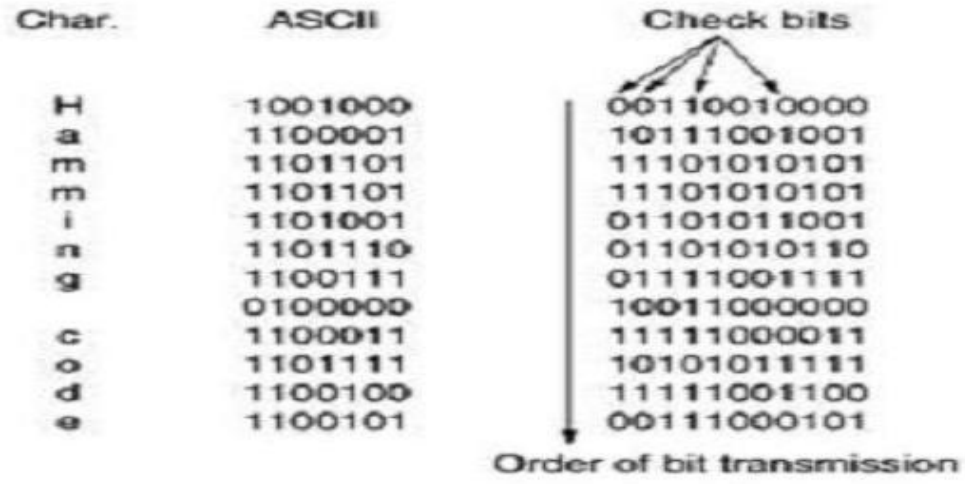
code, consider a code in which a single parity b appended to the data. The parity bit is chosen so that the number of 1 bits in the codeword is even (or odd).For example, when 1011010 is sent in even parity, a bit is added to the end to make it 10110100.With odd parity 1011010 becomes 10110101. A code with a single parity bit has a distance 2, since any single-bit error produces a codeword with the wrong parity. It can be used to detect single errors.

As a simple example of an error-correcting code, consider a code with only four valid codewords: 0000000000, 0000011111, 1111100000, and 1111111111

This code has a distance 5, which means that it can correct double errors. If the codeword 0000000111 arrives, the receiver knows that the original must have been 0000011111. If,however, a triple error changes 0000000000 into 0000000111, the error will not be corrected properly.

Imagine that we want to design a code with m message bits and r check bits that will allow all single errors to be corrected. Each of the 2m legal messages has n illegal codewords at a distance 1 from it. These are formed by systematically inverting each of the n bits in the n-bit codeword formed from it. Thus, each of the 2m legal messages requires n + 1 bit patterns dedicated to it. Since the total number of bit patterns is 2n, we must have $(n + 1)2m \leq 2n$. Using $n = m + r$, this requirement becomes $(m + r + 1) \leq 2r$. Given m, this puts a lower limit on

the number of check bits needed to correct single errors. This theoretical lower limit can, in fact, be achieved using a method due to Hamming (1950). The bits of the codeword are numbered consecutively, starting with bit 1 at the left end, bit 2 to its immediate right, and so on. The bits that are powers of 2 (1, 2, 4, 8, 16, etc.) are check bits. The rest (3, 5, 6, 7, 9, etc.) are filled up with the m data bits. Each check bit forces the parity of some collection of bits, including itself, to be even (or odd). A bit may be included in several parity computations. To see which check bits the data bit in position k contributes to, rewrite k as a sum of powers of 2.For example, 11 = 1 + 2 + 8 and 29 = 1 + 4 + 8 + 16. A bit is checked by just those check bits occurring in its expansion (e.g., bit 11 is checked by bits 1, 2, and 8). When a codeword arrives, the receiver initializes a counter to zero. It then examines each check bit, k (k = 1, 2, 4, 8 ...), to see if it has the correct parity. If not, the receiver adds k to the counter. If the counter is zero after all the check bits have been examined (i.e., if they were all correct), the codeword is accepted as valid. If the counter is nonzero, it contains the number of the incorrect bit. For example, if check bits 1, 2, and 8 are in error, the inverted bit is 11, because it is the only one checked by bits 1, 2, and 8. Figure 4.1 shows some 7-bit ASCII characters encoded as 11-bit code words using a Hamming code. Remember that the data are found in bit positions 3, 5, 6, 7, 9, 10, and 11.



Use of a Hamming code to correct burst errors

Hamming codes can only correct single errors. However, there is a trick that can be used to permit Hamming codes to correct burst errors. A sequence of k consecutive code words is arranged as a matrix, one codeword per row. Normally, the data would be transmitted one codeword at a time, from left to right. To correct burst errors, the data should be transmitted one column at a time, starting with the leftmost column. When all k bits have been sent, the second column is sent, and so on, as indicated in Fig2.9 When the frame arrives at the receiver, the matrix is reconstructed, one column at a time. If a burst error of length k occurs, at most 1 bit in each of the k codeword will have been affected, but the Hamming code can correct one error per codeword, so the entire block can be restored. This method uses kr check bits to make blocks of km data bits immune to a single burst error of length k or less.

Error-Detecting Codes

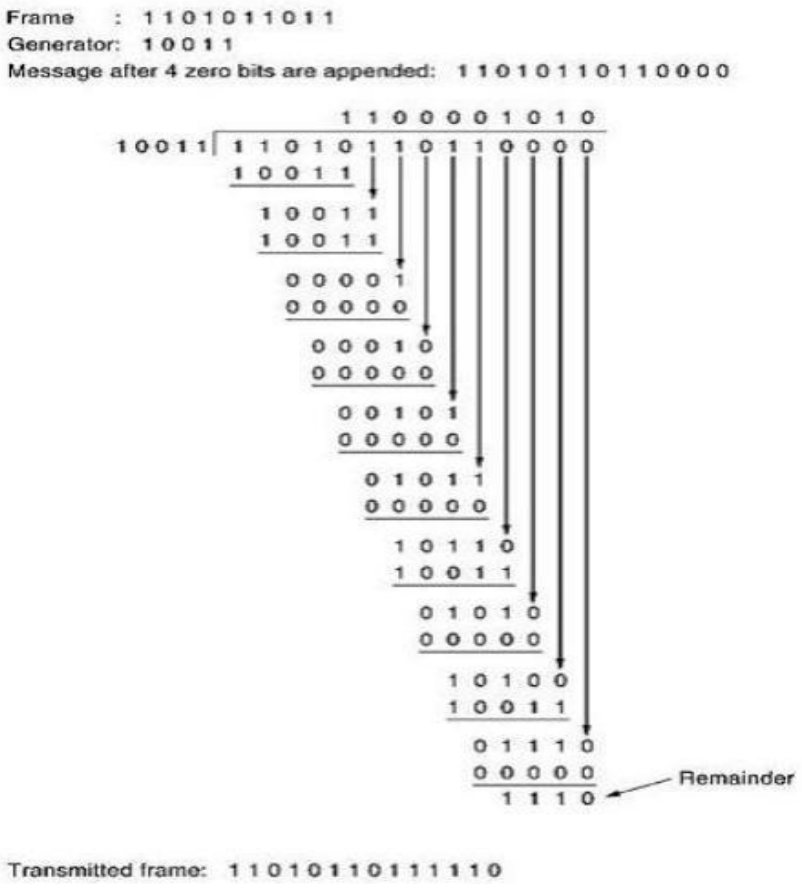
Error-correcting codes are widely used on wireless links, which are notoriously noisy and error prone when compared to copper wire or optical fibers. Without error-correcting codes, it would be hard to get anything through. However, over copper wire or fiber, the error rate is much lower, so error detection and retransmission is usually more efficient there for dealing with the occasional error. As a simple example, consider a channel on which errors are isolated and the error rate is 10-6 per bit. Let the block size be 1000 bits. To provide error correction for 1000-bit blocks, 10 check bits are needed; a megabit of data would require 10,000 check bits. To merely detect a block with a single 1-bit error, one parity bit per block will suffice. Once every 1000 blocks, an extra block (1001 bits) will have to be transmitted. The total overhead for the error detection + retransmission method is only 2001 bits per megabit of data, versus 10,000 bits for a Hamming code.
If a single parity bit is added to a block and the block is badly garbled by a long burst error, the

probability that the error will be detected is only 0.5, which is hardly acceptable.
The odds can be improved considerably if each block to be sent is regarded as rectangular matrix n bits wide and k bits high, as described above. A parity bit is computed separately for each column and affixed to the matrix as the last row. The matrix is then transmitted one row at atime. When the block arrives, the receiver checks all the parity bits. If any one of them is wrong, the receiver requests a retransmission of the block. Additional retransmissions are requested as needed until an entire block is received without any parity errors. This method can detect a singleburst of length n, since only 1 bit per column will be changed. A burst of length n + 1 will pass undetected, however, if the first bit is inverted, the last bit is inverted, and all the other bits are correct. (A burst error does not imply that all the bits are wrong; it just implies that at least thefirst and last are wrong.) If the block is badly garbled by a long burst or by multiple shorter bursts,the probability that any of the n columns will have the correct parity, by accident, is 0.5, so the probability of a bad block being accepted when it should not be is 2-n. Although the above scheme may sometimes be adequate, in practice, another method is in widespread use: the polynomial code, also known as a CRC (Cyclic Redundancy Check).
Polynomial codes are based upon treating bit strings as representations of polynomials with coefficients of 0 and 1 only. A k-bit frame is regarded as the coefficient list for a polynomial with kterms, ranging from xk-1 to x0. Such a polynomial is said to be of degree k - 1. The high order (leftmost) bit is the coefficient of xk-1; the next bit is the coefficient of xk-2, and so on. For example, 110001 has 6 bits and thus represent a six-term polynomial with coefficients 1, 1, 0, 0, 0, and 1: x5 + x4 + x0.
Polynomial arithmetic is done modulo 2, according to the rules of algebraic field theory. There are no carries for addition or borrows for subtraction. Both addition and subtraction are identicalto exclusive OR. For example: Long division is carried out the same way as it is in binary except that the subtraction is done modulo 2, as above. A divisor is said "to go into" a dividend if the dividend has as many bits as the divisor. When the polynomial code method is employed, the sender and receiver must agree upon a generator polynomial, G(x), in advance. Both the high- and low-order bits of the generator must be 1. To compute the checksum for some frame with m bits, corresponding to the polynomial M(x), the frame must be longer than the generator polynomial. The idea is to append a checksum to the end of the frame in such a way that the polynomial represented by the check summed frame is divisible by G(x). When the receiver gets the check summed frame, it tries dividing it by G(x). If there is a remainder, there has been a transmission error.
The algorithm for computing the checksum is as follows:
1. Let r be the degree of G(x). Append r zero bits to the low-order end of the frame so it now contains m + r bits and corresponds to the polynomial xr M(x).

2. Divide the bit string corresponding to G(x) into the bit string corresponding to xr M(x), using modulo 2 divisions.

3. Subtract the remainder (which is always r or fewer bits) from the bit string corresponding to xr M(x) using modulo 2 subtractions. The result is the check summed frame to be transmitted. Call its polynomial T(x).

Figure 2.10 illustrates the calculation for a frame 1101011011 using the generator G(x) = x4 + x+ 1.



Calculation of the polynomial code checksum

Elementary Data Link Layer

ProtocolsAn Unrestricted Simplex

Protocol:

As an initial example we will consider a protocol that is as simple as it can be. Data are transmitted in one direction only. Both the transmitting and receiving network layers are always ready. Processing time can be ignored. Infinite buffer space is available. And best of all, the communication channel between the data link layers never damages or loses frames. This thoroughly unrealistic protocol, which we will nickname "utopia" .

The protocol consists of two distinct procedures, a sender and a receiver. The sender runs in the

data link layer of the source machine, and the receiver runs in the data link layer of thedestination machine. No sequence numbers or acknowledgements are used here, so MAX_SEQ is not needed. The only event type possible is frame arrival (i.e., the arrival of an undamaged frame).
The sender is in an infinite while loop just pumping data out onto the line as fast as it can. The body of the loop consists of three actions: go fetch a packet from the (always obliging) network layer, construct an outbound frame using the variable s, and send the frame on its way. Only the info field of the frame is used by this protocol, because the other fields have to do with error and flow control and there are no errors or flow control restrictions here. The receiver is equally simple. Initially, it waits for something to happen, the only possibility being the arrival of an undamaged frame. Eventually, the frame arrives and the procedure wait_for_event returns, with event set to frame_arrival (which is ignored anyway). The call to from_physical_layer removes the newly arrived frame from the hardware buffer and puts it in the variable r, where the receiver code can get at it. Finally, the data portion is passed on to the network layer, and the data link layer settles back to wait for the next frame, effectively suspending itself until the frame arrives.

3.9 A Simplex Stop-and-Wait Protocol:

- **Stop and Wait**

  This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received shown in Fig 2.11

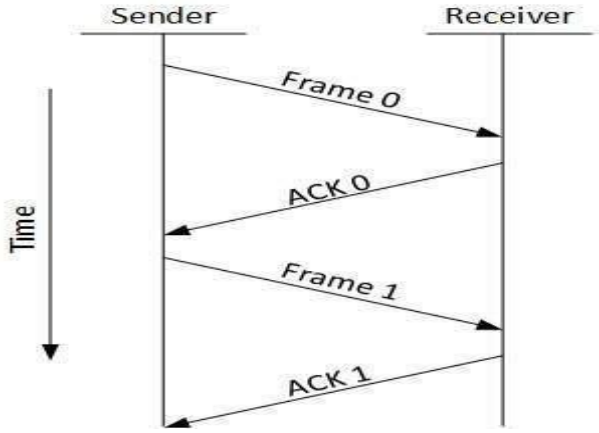


Figure 3.9 Stop and wait protocol

Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data- frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data- frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

- ***Error detection*** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- ***Positive ACK*** - When the receiver receives a correct frame, it should acknowledge it.
- ***Negative ACK*** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- ***Retransmission:*** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

3.10 Stop-and-wait ARQ

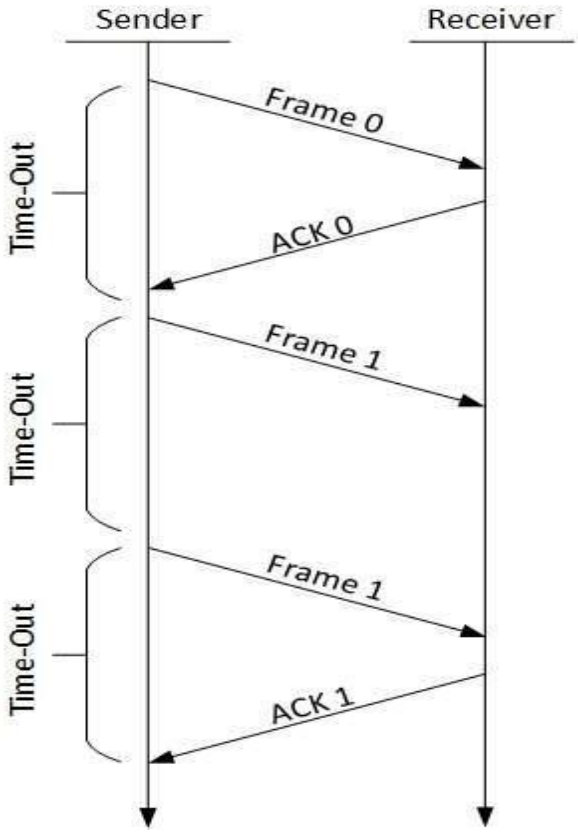


Figure 3.10 Stop-and-Wait ARQ

The following transition may occur in Stop-and-Wait ARQ as shown in fig 2.12

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

3.11 Go-Back-N ARQ

Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method as shown in fig Go-Back-N ARQ

, both sender and receiver maintain a window.

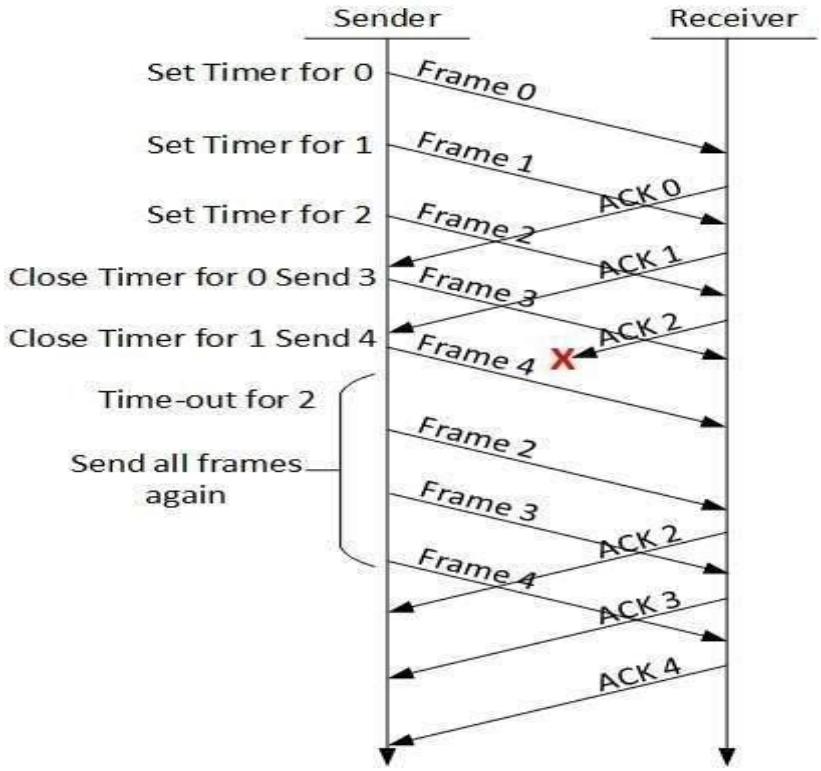


Figure 3.11 Go-Back-N ARQ

The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not

receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

3.12 Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.

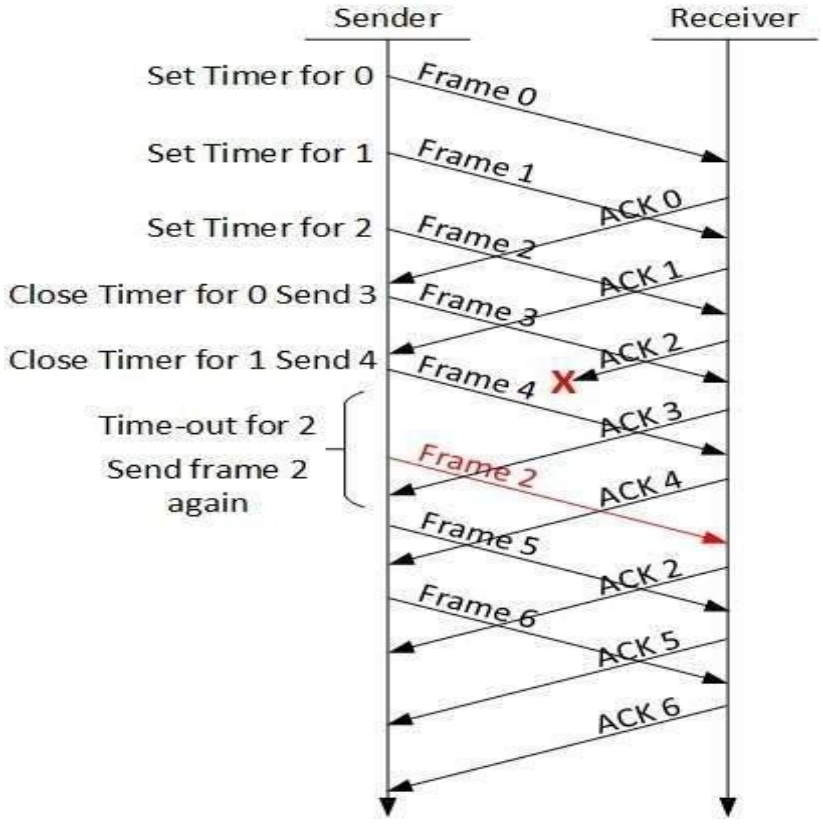


Figure 3.12 Selective-Repeat ARQ

In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers,buffers the frames in memory and sends NACK for only frame which is missing or damaged.
The sender in this case, sends only packet for which NACK is received.

3.13 HDLC—High-Level Data Link Control:

These are a group of closely related protocols that are a bit old but are still heavily used. They are

all derived from the data link protocol first used in the IBM mainframe world: SDLC (Synchronous Data Link Control) protocol. After developing SDLC, IBM submitted it to ANSI and ISO for acceptance as U.S. and international standards, respectively. ANSI modified it to become ADCCP (Advanced Data Communication Control Procedure), and ISO modified it to become HDLC (High-level Data Link Control). CCITT then adopted and modified HDLC for its LAP (Link Access Procedure) as part of the X.25 network interface standard but later modified it again to LAPB, to make it more compatible with a later version of HDLC. The nice thing about standards is that you have so many to choose from. Furthermore, if you do not like any of them, you can just wait for next year's model. These protocols are based on the same principles. Allare bit oriented, and all use bit stuffing for data transparency. They differ only in minor, but nevertheless irritating, ways. The discussion of bit-oriented protocols that follows is intended as ageneral introduction. For the specific details of any one protocol, please consult the appropriate definition.

All the bit-oriented protocols use the frame structure shown in Fig.2.15. The Address field is primarily of importance on lines with multiple terminals, where it is used to identify one of the terminals. For point-to-point lines, it is sometimes used to distinguish commands from responses.

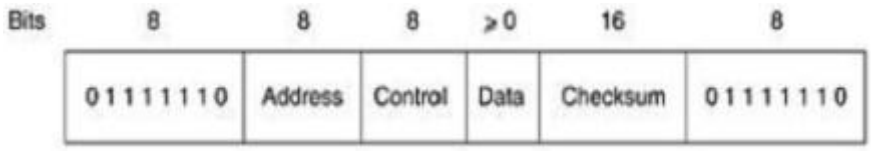
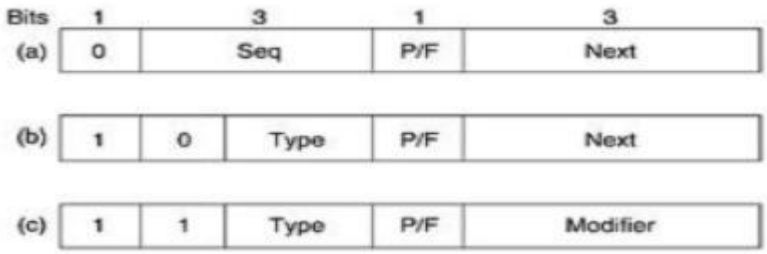


Figure 3.13 High-Level Data Link Control

Frame format for bit-oriented protocols

The Control field is used for sequence numbers, acknowledgements, and other purposes, as discussed below.
The Data field may contain any information. It may be arbitrarily long, although the efficiency of the checksum falls off with increasing frame length due to the greater probability of multiple burst errors. The Checksum field is a cyclic redundancy code. The frame is delimited with another flag sequence (01111110). On idle point-to-point lines, flag sequences are transmitted continuously. The minimum frame contains three fields and totals 32 bits, excluding the flags on either end.
There are three kinds of frames: Information, Supervisory, and Unnumbered.

The contents of the Control field for these three kinds are shown in Fig.2.16 The protocol uses a sliding window, with a 3-bit sequence number. Up to seven unacknowledged frames may be outstanding at any instant. The Seq field in Fig 2.16 (a) is the frame sequence number. The Next field is a piggybacked acknowledgement. However, all the protocols adhere to the convention that instead of piggybacking the number of the last frame received correctly, they use the number of the first frame not yet received (i.e., the next frame expected). The choice of using the last frame received or the next frame expected is arbitrary; it does not matter which convention isused, provided that it is used consistently



Control field of (a) an information frame, (b) a supervisory frame, (c) an unnumbered frame

The P/F bit stands for Poll/Final. It is used when a computer (or concentrator) is polling a group of terminals. When used as P, the computer is inviting the terminal to send data. All the frames sent by the terminal, except the final one, have the P/F bit set to P. The final one is set to F. In some of the protocols, the P/F bit is used to force the other machine to send a Supervisory frame immediately rather than waiting for reverse traffic onto which to piggyback the window information. The bit also has some minor uses in connection with the unnumbered frames.

The various kinds of Supervisory frames are distinguished by the Type field. Type 0 is an acknowledgement frame (officially called RECEIVE READY) used to indicate the next frame expected. This frame is used when there is no reverse traffic to use for piggybacking.

Type 1 is anegative acknowledgement frame (officially called REJECT). It is used to indicate that atransmission error has been detected. The Next field indicates the first frame in sequence not received correctly (i.e., the frame to be retransmitted). The sender is required to retransmit all Outstanding frames starting at Next. This strategy is similar to our protocol 5 rather than our protocol 6.

Type 2 is RECEIVE NOT READY. It acknowledges all frames up to but not including next, just as RECEIVE READY does, but it tells the sender to stop sending. RECEIVE NOT READY is intended to signal certain temporary problems with the receiver, such as a shortage of buffers, and not as an alternative to the sliding window flow control. When the condition has been repaired, the receiver sends a RECEIVE READY, REJECT, or certain control frames.

Type 3 is the SELECTIVE REJECT. It calls for retransmission of only the frame specified. In this sense it is like our protocol 6 rather than 5 and is therefore most useful when the sender's window size is half the sequence space size, or less. Thus, if a receiver wishes to buffer out- of-sequence frames for potential future use, it can force the retransmission of any specific frame using Selective Reject. HDLC and ADCCP allow this frame type, but SDLC and LAPB do not allow it (i.e., there is no Selective Reject), and type 3 frames are undefined.

The third class of frame is the unnumbered frame. It is sometimes used for control purposes but can also carry data when unreliable connectionless service is called for. The various bit-oriented protocols differ considerably here, in contrast with the other two kinds, where they are nearly identical. Five bits are available to indicate the frame type, but not all 32 possibilities are used.

PPP-The Point-to-Point Protocol:

The Internet needs a point-to-point protocol for a variety of purposes, including router-to-router traffic and home user-to-ISP traffic. This protocol is PPP (Point-to-Point Protocol), which is defined in RFC 1661 and further elaborated on in several other RFCs (e.g., RFCs 1662 and 1663). PPP handles error detection, supports multiple protocols, allows IP addresses to be negotiated at connection time, permits authentication, and has many other features.

PPP provides three features:

1. A framing method that unambiguously delineates the end of one frame and the start of the next one. The frame format also handles error detection.

2. A link control protocol for bringing lines up, testing them, negotiating options, and bringing them down again gracefully when they are no longer needed. This protocol is called LCP (Link Control Protocol). It supports synchronous and asynchronous circuits and byte-oriented and bit-oriented encodings.

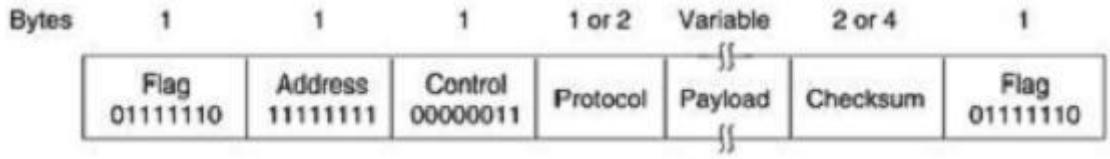
3. A way to negotiate network-layer options in a way that is independent of the network layer protocol to be used. The method chosen is to have a different NCP (Network Control Protocol) for each network layer supported.

To see how these pieces fit together, let us consider the typical scenario of a home user calling up an Internet service provider to make a home PC a temporary Internet host. The PC first calls the provider's router via a modem. After the router's modem has answered the phone and established a physical connection, the PC sends the router a series of LCP packets in the payload field of one or more PPP frames. These packets and their responses select the PPP parameters to be used.

Once the parameters have been agreed upon, a series of NCP packets are sent to configure the network layer. Typically, the PC wants to run a TCP/IP protocol stack, so it needs an IP address

There are not enough IP addresses to go around, so normally each Internet provider gets a blockof them and then dynamically assigns one to each newly attached PC for the duration of its login session. If a provider owns n IP addresses, it can have up to n machines logged in simultaneously, but its total customer base may be many times that. The NCP for IP assigns the IP address. At this point, the PC is now an Internet host and can send and receive IP packets, just as hardwired hosts can. When the user is finished, NCP tears down the network layer connection and frees up the IP address. Then LCP shuts down the data link layer connection. Finally, the computer tells the modem to hang up the phone, releasing the physical layerconnection.

1. The PPP frame format was chosen to closely resemble the HDLC frame format, since there was no reason to reinvent the wheel. The major difference between PPP and HDLC is that PPP is character oriented rather than bit oriented. In particular, PPP uses byte stuffing on dial-upmodem lines, so all frames are an integral number of bytes. It is not possible to send a frame consisting of 30.25 bytes, as it is with HDLC. Not only can PPP frames be sent over dialup telephone lines, but they can also be sent over SONET or true bit-oriented HDLC lines (e.g., for router-router connections). The PPP frame format is shown in Fig.2.17.



The PPP full frame format for unnumbered mode operation

All PPP frames begin with the standard HDLC flag byte (01111110), which is byte stuffed if it occurs within the payload field. Next comes the Address field, which is always set to the binary value 11111111 to indicate that all stations are to accept the frame. Using this value avoids the issue of having to assign data link addresses.

The Address field is followed by the Control field, the default value of which is 00000011. This value indicates an unnumbered frame. In other words, PPP does not provide reliable transmission using sequence numbers and acknowledgements as the default. In noisy environments, such as wireless networks, reliable transmission using numbered mode can be used. The exact details are defined in RFC 1663, but in practice it is rarely used. Since the Address and Control fields are always constant in the default configuration, LCP provides the necessary mechanism for the two parties to negotiate an option to just omit them altogether and save 2 bytes per frame.

The fourth PPP field is the Protocol field. Its job is to tell what kind of packet is in the Payload field. Codes are defined for LCP, NCP, IP, IPX, AppleTalk, and other protocols. Protocolsstarting with a 0 bit are network layer protocols such as IP, IPX, OSI CLNP, XNS. Those starting with a 1 bit are used to negotiate other protocols. These include LCP and a different NCP for each network layer protocol supported. The default size of the Protocol field is 2 bytes, but it can be negotiated down to 1 byte using LCP. The Payload field is variable length, up to some negotiated maximum. If the length is not negotiated using LCP during line setup, a default length of 1500 bytes is used. Padding may follow the payload if need be. After the Payload field comes the Checksum field, which is normally 2 bytes, but a 4-byte checksum can be negotiated.

In summary, PPP is a multiprotocol framing mechanism suitable for use over modems,HDLC bit-serial lines, SONET, and other physical layers. It supports error detection, option negotiation, header compression, and, optionally, reliable transmission using an HDLC type frame format.

3.14 Framing:

To provide service to the network layer, the data link layer must use the service provided to it by the physical layer. What the physical layer does is accept a raw bit stream and attempt to deliver it to the destination. This bit stream is not guaranteed to be error free. The number of bits received may be less than, equal to, or more than the number of bits transmitted, and they may have different values. It is up to the data link layer to detect and, if necessary, correct errors. The usual approach is for the data link layer to break the bit stream up into discrete frames and compute the checksum for each frame. When a frame arrives at thedestination, the checksum is recomputed. If the newly computed

checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it (e.g., discarding the bad frame and possibly also sending back an error report). Breaking the bit stream up into frames is more difficult than it at first appears. One way to achieve this framing is to insert time gaps between frames, much like the spaces between words in ordinary text. However, networks rarely make any guarantees about timing, so it is possible these gaps might be squeezed out or other gaps might be inserted during transmission. Since itis too risky to count on timing to mark the start and end of each frame, other methods have been devised. We will look at four methods: 1. Character count. 2. Flag bytes with byte stuffing. 3. Starting and ending flags, with bit stuffing. 4. Physical layer coding violations. The first framing method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is. This technique is shown in Fig.2.18(a) for four framesof sizes 5, 5, 8, and 8 characters, respectively.

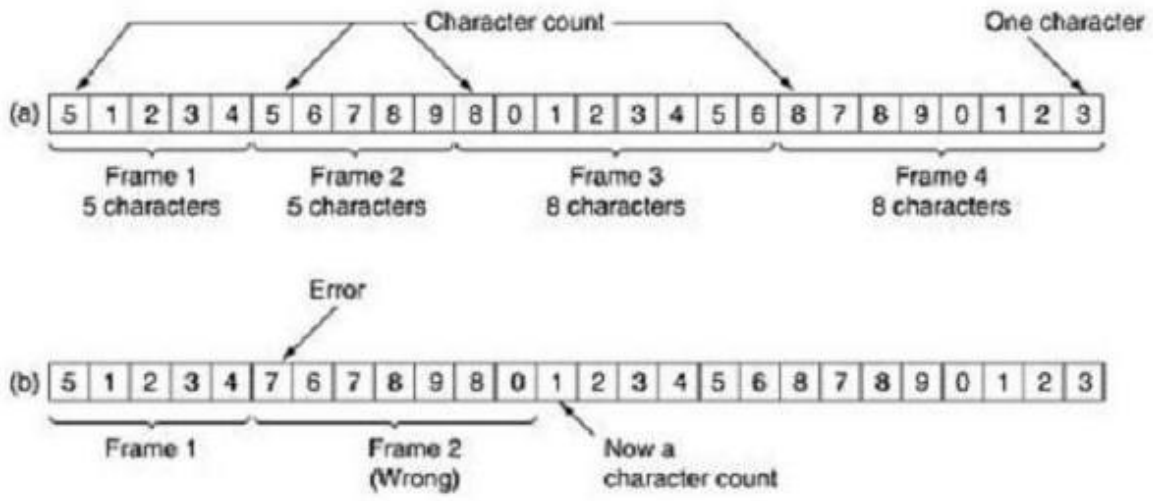


Figure 3.14 Framing

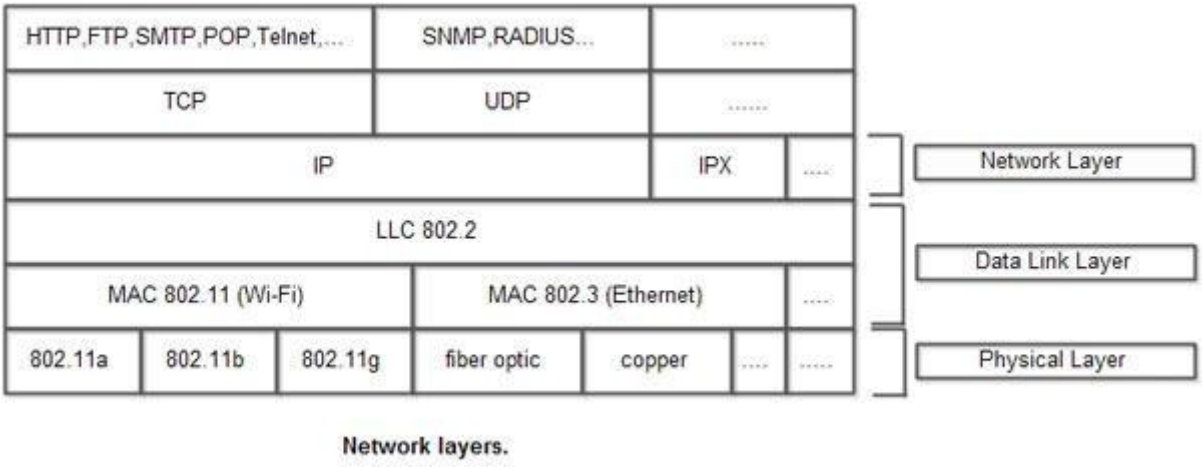
The Media Access Control (MAC) data communication Networks protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the data link layer specified in the seven-layer OSI model. The medium access layer was made necessary bysystems that share a common communications medium. Typically these are local area networks. The MAC layer is the "low" part of the second OSI layer, the layer of the "data link". In fact, the IEEE divided this layer into two layers "above" is the control layer the logical connection(Logical Link Control, LLC) and "down" the control layer The medium access (MAC).

The LLC layer is standardized by the IEEE as the 802.2 since the beginning 1980 Its purpose is

to allow level 3 network protocols (for eg IP) to be based on a single layer (theLLC layer) regardless underlying protocol used, including WiFi, Ethernet or Token Ring, for example. All WiFi data packets so carry a pack LLC, which contains itself packets from the upper network layers. The header of a packet LLC indicates the type of layer 3 protocol in it: most of the time, it is IP protocol, but it could be another protocol, such as IPX (Internet Packet Exchange) for example. Thanks to the LLC layer, it is possible to have at the same time, on the same network, multiple Layer 3 protocols.

In LAN nodes uses the same communication channel for transmission. The MAC sub-layer has two primary responsibilities:

Data encapsulation, including_frame assembly before transmission, and frame parsing/error detection during and after reception. Media access control, including initiation of frame transmission and recovery from transmission failure.



Network layers.

MAC layer protocol stack

The channel allocation problem

The traditional way of allocating a single channel, such as a telephone trunk, among multiple competing users is Frequency Division Multiplexing (FDM). If there are *N* users, the bandwidth is divided into *N* equal-sized portions each user being assigned one portion. Since each user has a private frequency band, there is no interference between users. When there is only a small and constant number of users, each of which has a heavy (buffered) load of traffic (e.g., carriers' switching offices), FDM is a simple and efficient allocation mechanism.

However, when the number of senders is large and continuously varying or the traffic is

bursty, FDM presents some problems. If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. If more than N users want to communicate, some of them will be denied permission for lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever transmit or receive anything.

$$T_{\text{FDM}} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT \tag{3.1}$$

$$T = \frac{1}{\mu C - \lambda} \tag{3.2}$$

However, even assuming that the number of users could somehow be held constant at N, dividing the single available channel into static subchannels is inherently inefficient. The basic problem is that when some users are quiescent, their bandwidth is simply lost. They are not using it, and no one else is allowed to use it either. Furthermore, in most computer systems,data traffic is extremely bursty (peak traffic to mean traffic ratios of 1000:1 are common). Consequently, most of the channels will be idle most of the time.

The poor performance of static FDM can easily be seen from a simple queueing theory calculation. Let us start with the mean time delay, T, for a channel of capacity C bps, with an arrival rate of λ frames/sec, each frame having a length drawn from an exponential probability density function with mean $1/\mu$ bits/frame. With these parameters the arrival rate is λ frames/sec and the service rate is μC frames/sec. From queueing theory it can be shown that for Poisson arrival and service times,

For example, if C is 100 Mbps, the mean frame length, $1/\mu$, is 10,000 bits, and the frame arrival rate, λ, is 5000 frames/sec, then $T = 200$ μsec. Note that if we ignored the queueing delay and just asked how long it takes to send a 10,000 bit frame on a 100-Mbps network, we would get the (incorrect) answer of 100 μsec. That result only holds when there is no contention for the channel.

Now let us divide the single channel into N independent subchannels, each with capacity C/N bps. The mean input rate on each of the subchannels will now be λ/N. Recomputing T we get

The mean delay using FDM is N times worse than if all the frames were somehow magically arranged orderly in a big central queue.

Precisely the same arguments that apply to FDM also apply to time division multiplexing (TDM). Each user is statically allocated every Nth time slot. If a user does not use the allocated slot, it just lies fallow. The same holds if we split up the networks physically. Using our previous

example again, if we were to replace the 100-Mbps network with 10 networks of 10 Mbps each and statically allocate each user to one of them, the mean delay would jump from 200 μsec to 2 msec.

Since none of the traditional static channel allocation methods work well with bursty traffic, we will now explore dynamic methods.

Dynamic Channel Allocation in LANs and MANs

Before we get into the first of the many channel allocation methods to be discussed in this chapter, it is worthwhile carefully formulating the allocation problem. Underlying all the work done in this area are five key assumptions, described below.

Station Model. The model consists of N independent **stations** (e.g., computers, telephones, or personal communicators), each with a program or user that generates frames for transmission. Stations are sometimes called **terminals**. The probability of a frame being generated in an interval of length Δt is $\lambda \Delta t$, where λ is a constant (the arrival rate of new frames). Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

Single Channel Assumption. A single channel is available for all communication. All stations can transmit on it and all can receive from it. As far as the hardware is concerned, all stations are equivalent, although protocol software may assign priorities to them.

Collision Assumption. If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is called a **collision**. All stations can detect collisions. A collided frame must be transmitted again later. There are no errors other than those generated by collisions.

4a. Continuous Time. Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.

4b. Slotted Time. Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

5a. Carrier Sense. Stations can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.

5b. No Carrier Sense. Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

Some discussion of these assumptions is in order. The first one says that stations are independent and that work is generated at a constant rate. It also implicitly assumes that each

station only has one program or user, so while the station is blocked, no new work is generated. More sophisticated models allow multi programmed stations that can generate work while a station is blocked, but the analysis of these stations is much more complex.

The single channel assumption is the heart of the model. There are no external ways to communicate. Stations cannot raise their hands to request that the teacher call on them.

The collision assumption is also basic, although in some systems (notably spread spectrum), this assumption is relaxed, with surprising results. Also, some LANs, such as token rings, pass a special token from station to station, possession of which allows the current holder to transmit a frame. But in the coming sections we will stick to the single channel with contentionand collisions model.

Two alternative assumptions about time are possible. Either it is continuous (4a) or it is slotted (4b). Some systems use one and some systems use the other, so we will discuss and analyze both. For a given system, only one of them holds.

Similarly, a network can either have carrier sensing (5a) or not have it (5b). LANsgenerally have carrier sense. However, wireless networks cannot use it effectively because not every station may be within radio range of every other station. Stations on wired carrier sense networks can terminate their transmission prematurely if they discover that it is colliding with another transmission. Collision detection is rarely done on wireless networks, for engineering reasons. Note that the word "carrier" in this sense refers to an electrical signal on the cable and has nothing to do with the common carriers (e.g., telephone companies) that date back to the Pony Express days.

MULTIPLE ACCESS PROTOCOLS

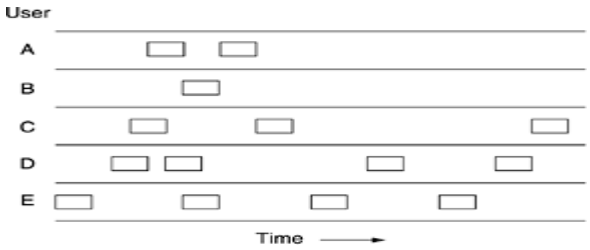
Following Protocols are used by Medium Access Layer:

ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication channel. It was developed in the 1970s at the University of Hawaii. The original system used terrestrial radio broadcasting, but the system has been implemented in satellite communication systems. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time.

PURE ALOHA

The basic idea of an ALOHA system is simple: let users transmit whenever they have data to be sent. There will be collisions, of course, and the colliding frames will be damaged. However, due to the feedback property of broadcasting, a sender can always find out whether its frame was destroyed by listening to the channel, the same way other users do. With a LAN, the feedback is immediate; with a satellite, there is a delay of 270 msec before the sender knows if the transmission was successful. If listening while transmitting is not possible for some reason, acknowledgements are needed. If the frame was destroyed, the sender just waits a random amount of time and sends it again. The waiting time must be random or the same frames will collide over and over, in lockstep. Systems in which multiple users share a common channel ina way that can lead to conflicts are widely known as **contention** systems.

In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.



Frames are transmitted at completely arbitrary times

SLOTTED ALOHA

In 1972, Roberts published a method for doubling the capacity of an ALOHA system (Roberts, 1972). His proposal was to divide time into discrete intervals, each interval corresponding to one frame. This approach requires the users to agree on slot boundaries. One way to achieve synchronization would be to have one special station emit a pip at the start of each interval, like a clock.

In Roberts' method, which has come to be known as slotted ALOHA, in contrast to Abramson's pure ALOHA, a computer is not permitted to send whenever a carriage return is typed. Instead, it is required to wait for the beginning of the next slot. Thus, the continuous pure

ALOHA is turned into a discrete one. Since the vulnerable period is now halved, the probability of no other traffic during the same slot as our test frame is e-G which leads to

$$S = Ge^{-G}$$

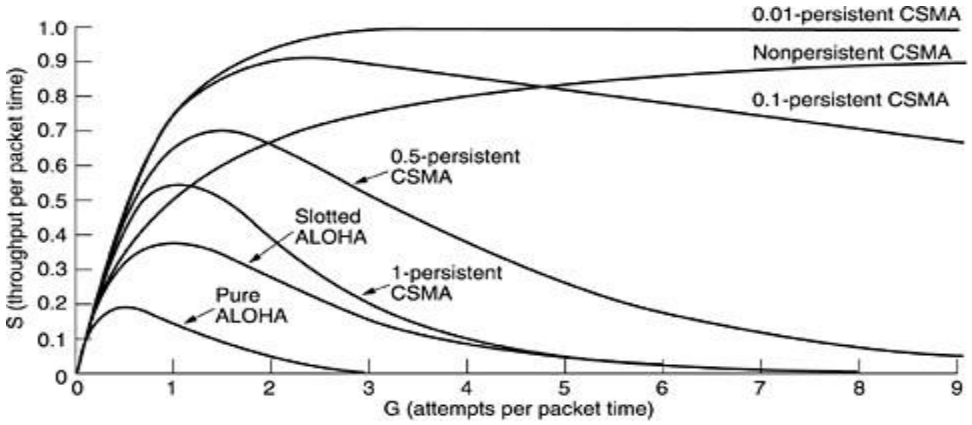
***Carrier* Sensed Multiple Accesses (CSMA):** CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cableeven though another has already just accessed it. There are two methods for avoiding these so- called collisions, listed here:

CSMA/CD (Carrier Sense Multiple Access/Collision Detection): CD (collision detection) defines what happens when two devices sense a clear channel, and then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, and then retransmit. This is the technique used to access the 802.3 Ethernet network channel.

This method handles collisions as they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must beless than 40 percent of the bus capacity for the network to operate efficiently. If distances are long, time lags occur that may result in inappropriate carrier sensing, and hence collisions.

***CSMA*/CA (Carrier Sense Multiple Access/Collision Avoidance):** In CA collision avoidance), collisions area voided because each node signals its intent to transmit before actually doing so. This method is not popular because it requires excessive overhead that reduces performance.



Performance comparison of various MAC protocols

3.15 CSMA WITH COLLISION DETECTION

Persistent and non-persistent CSMA protocols are clearly an improvement over ALOHA because they ensure that no station begins to transmit when it senses the channel busy. Another improvement is for stations to abort their transmissions as soon as they detect a collision. In other words, if two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately. Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the collision is detected. Quickly terminating damaged frames savestime and bandwidth. This protocol, known as **CSMA/CD** (**CSMA with Collision Detection**) is widely used on LANs in the MAC sublayer. In particular, it is the basis of the popular Ethernet LAN, so it is worth devoting some time to looking at it in detail.

CSMA/CD, as well as many other LAN protocols, uses the conceptual model. At the point marked t_0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.

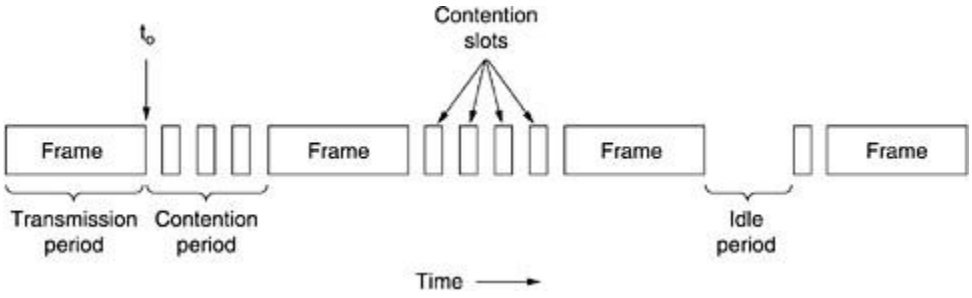


Figure 3.15 CSMA/CD can be in one of three states: contention, transmission, or idle.

COLLISION-FREE PROTOCOLS

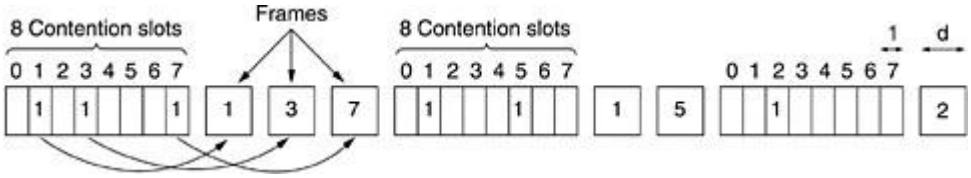
Although collisions do not occur with CSMA/CD once a station has unambiguously captured the channel, they can still occur during the contention period. These collisions adversely affect the system performance, especially when the cable is long (i.e., large τ) and the frames are short. And CSMA/CD is not universally applicable. In this section, we will examine some protocols that resolve the contention for the channel without any collisions at all, not even duringthe contention period. Most of these are not currently used in major systems, but in a rapidly changing field, having some protocols with excellent properties available for future systems is often a good thing.

In the protocols to be described, we assume that there are exactly *N* stations, each with a unique

address from 0 to *N* - 1 "wired" into it. It does not matter that some stations may be inactive part of the time. We also assume that propagation delay is negligible.

A BIT-MAP PROTOCOL

In our first collision-free protocol, the **basic bit-map method**, each contention period consists of exactly *N* slots. If station 0 has a frame to send, it transmits a 1 bit during the zeroth slot. No other station is allowed to transmit during this slot. Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 during slot 1, but only if it has a frame queued. In general, station *j* may announce that it has a frame to send by inserting a 1 bit into slot *j*. After all *N* slots have passed by, each station has complete knowledge of which stations wish to transmit. At that point, they begin transmitting in numerical order



Basic bit-map protocol

Since everyone agrees on who goes next, there will never be any collisions. After the last ready station has transmitted its frame, an event all stations can easily monitor, another *N* bit contention period is begun. If a station becomes ready just after its bit slot has passed by, it is out of luck and must remain silent until every station has had a chance and the bit map has come around again. Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.

3.16 WAVELENGTH DIVISION MULTIPLE ACCESS PROTOCOLS

A different approach to channel allocation is to divide the channel into subchannels using FDM, TDM, or both, and dynamically allocate them as needed. Schemes like this are commonly used on fiber optic LANs to permit different conversations to use different wavelengths (i.e., frequencies) at the same time. In this section we will examine one such protocol (Humblet et al., 1992).

A simple way to build an all-optical LAN is to use a passive star coupler. In effect, two fibers from each station are fused to a glass cylinder. One fiber is for output to the cylinder and one is for input from the cylinder. Light output by any station illuminates the cylinder and can be detected by all the other stations. Passive stars can handle hundreds of stations.

To allow multiple transmissions at the same time, the spectrum is divided into channels (wavelength bands). In this protocol, **WDMA** (**Wavelength Division Multiple Access**), each station is assigned two channels. A narrow channel is provided as a control channel to signal the station, and a wide channel is provided so the station can output data frames.

Each channel is divided into groups of time slots, as shown in. Let us call the number of slots in the control channel *m* and the number of slots in the data channel *n* + 1, where *n* of these are for data and the last one is used by the station to report on its status (mainly, which slots on both channels are free). On both channels, the sequence of slots repeats endlessly, with slot 0 being marked in a special way so latecomers can detect it. All channels are synchronized by a single global clock.

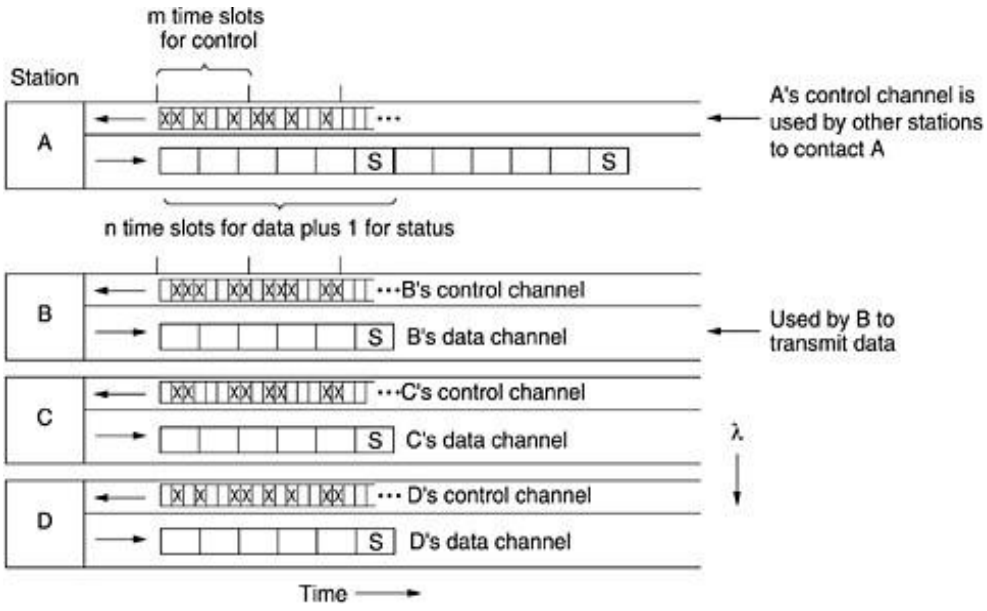


Figure 3.16 Wavelength division multiple access

ETHERNET:

- **IEEE 802.3 Local Area Network (LAN) Protocols:** Ethernet protocols refer to thefamily of local-area network (LAN) covered by the IEEE 802.3. In the Ethernet standard, there are two modes of operation: half-duplex and full-duplex modes. In the half duplex mode, data are transmitted using the popular Carrier-Sense Multiple Access/Collision Detection (CSMA/CD) protocol on a shared medium.

- The main disadvantages of the half-duplex are the efficiency and distance limitation, in which the link distances, is limited by the minimum MAC frame size. This restriction reducesthe efficiency drastically for high-rate transmission. Therefore, the carrier extension technique is used to ensure the minimum frame size of 512 bytes in Gigabit Ethernet to achieve a reasonable link distance. Four data rates are currently defined for operation over optical fiber and twisted-pair cables :

10 Mbps - 10Base-T Ethernet (IEEE 802.3)

100 Mbps - Fast Ethernet (IEEE 802.3u)

1000 Mbps - Gigabit Ethernet (IEEE

802.3z)

10-Gigabit - 10 Gbps Ethernet (IEEE 802.3ae).

The **Ethernet System** consists of three basic elements:

(1) The physical medium used to carry Ethernet signals between computers,

(2) a set of medium access control rules embedded in each Ethernet interface that allowmultiple computers to fairly arbitrate access to the shared Ethernet channel, and

(3) an Ethernet frame that consists of a standardized set of bits used to carry data over the system.

As with all IEEE 802 protocols, the ISO data link layer is divided into two IEEE 802 sub-layers, the Media Access Control (MAC) sub-layer and the MAC-client sub-layer. The IEEE
802.3 physical layer corresponds to the ISO physical layer.

Each Ethernet-equipped computer operates independently of all other stations on the network: there is no central controller. All stations attached to an Ethernet are connected to a shared signaling system, also called the medium. To send data a station first listens to the channel, and

when the channel is idle the station transmits its data in the form of an Ethernet frame, or packet.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface located in each station. The medium access control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

As each Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the destination address. If the destination address of the frame matches with the interface address, the frame will be read entirely and be delivered to the networking software running on that computer. All other network interfaces will stop reading the frame when they discover that the destination address does not match their own address.

IEEE 802.4 Token Bus: In token bus network station must have possession of a token before it can transmit on the network. The IEEE 802.4 Committee has defined token bus standards as broadband networks, as opposed to Ethernet's baseband transmission technique. The topology of the network can include groups of workstations connected by long trunk cables.

These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance. IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cableusing a bus topology. The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring. The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at oneend of the cable and station 2 might be at the other, with station 3 in the middle.

While token bus is used in some manufacturing environments, Ethernet and token ring standards have become more prominent in the office environment.

IEEE 802.5 Token Ring: Token ring is the IEEE 802.5 standard for a token-passing ring network with a star-configured physical topology. Internally, signals travel around the network from one

station to the next in a ring. Physically, each station connects to a central hub called a MAU (multistation access unit). The MAU contains a "collapsed ring," but the physical configuration is a star topology. When a station is attached, the ring is extended out to the station and then back to the MAU.

If a station goes offline, the ring is reestablished with a bypass at the station connector. Token ring was popular for an extended period in the late 1980s and 1990s, especially in IBM legacy system environments. IBM developed the technology and provided extensive support for connections to SNA systems. More recently, Ethernet, Fast Ethernet, and Gigabit Ethernet technologies have pushed token ring and other LAN technologies to the sidelines.

Historically, **10Base5** cabling, popularly called **thick Ethernet,** came first. It resembles a yellow garden hose, with markings every 2.5 meters to show where the taps go. (The 802.3

standard does not actually *require* the cable to be yellow, but it does *suggest* it.) Connections to it are generally made using **vampire taps**, in which a pin is *very* carefully forced halfway into the coaxial cable's core. The notation 10Base5 means that it operates at 10 Mbps, uses baseband signaling, and can support segments of up to 500 meters. The first number is the speed in Mbps. Then comes the word "Base" (or sometimes "BASE") to indicate baseband transmission. There used to be a broadband variant, 10Broad36, but it never caught on in the marketplaceand has since vanished. Finally, if the medium is coax, its length is given rounded to units of100 m after "Base."

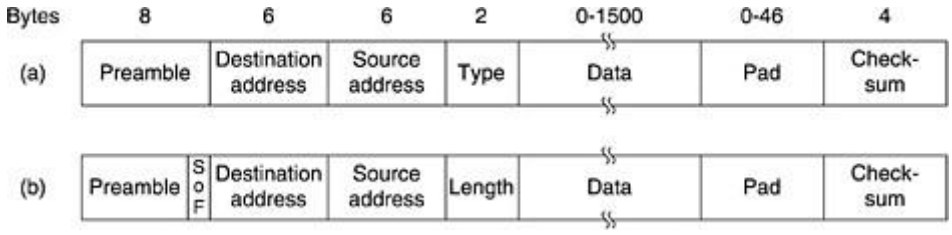
Historically, the second cable type was **10Base2**, or **thin Ethernet,** which, in contrast to the garden-hose-like thick Ethernet, bends easily. Connections to it are made using industry- standard BNC connectors to form T junctions, rather than using vampire taps. BNC connectors are easier to use and more reliable. Thin Ethernet is much cheaper and easier to install, but it can run for only 185 meters per segment, each of which can handle only 30 machines.

Detecting cable breaks, excessive length, bad taps, or loose connectors can be a major problem with both media. For this reason, techniques have been developed to track them down. Basically, a pulse of known shape is injected into the cable. If the pulse hits an obstacle or the end of the cable, an echo will be generated and sent back. By carefully timing the interval between sending the pulse and receiving the echo, it is possible to localize the origin of the echo. This technique is called **time domain reflectometry**.

The problems associated with finding cable breaks drove systems toward a different kind of wiring pattern, in which all stations have a cable running to a central **hub** in which they are all connected electrically (as if they were soldered together). Usually, these wires are telephone

company twisted pairs, since most office buildings are already wired this way, and normally plenty of spare pairs are available. This scheme is called **10Base-T**. Hubs do not buffer incoming traffic. We will discuss an improved version of this idea (switches), which do buffer incoming traffic later.

For 10Base5, a **transceiver** is clamped securely around the cable so that its tap makes contact with the inner core. The transceiver contains the electronics that handle carrier detection and collision detection. When a collision is detected, the transceiver also puts a special invalid signal on the cable to ensure that all other transceivers also realize that a collision has occurred.



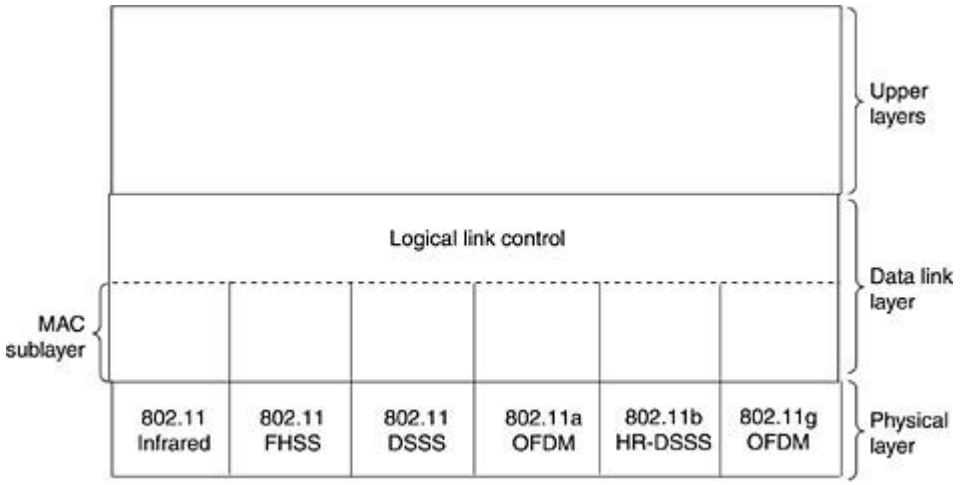
Frame formats. (a) DIX Ethernet. (b) IEEE 802.3

Types:

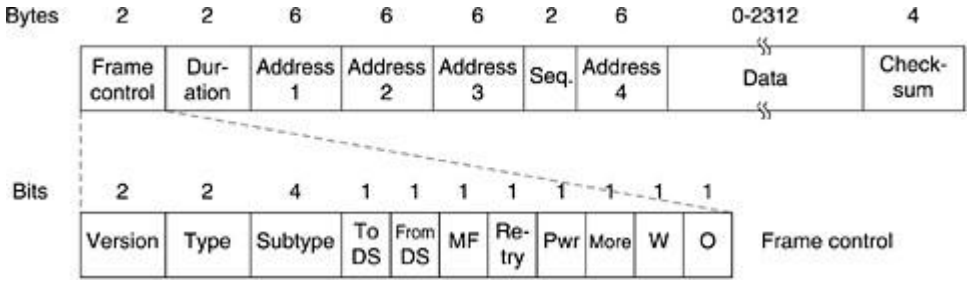
- Fast Ethernet
- Gigabit Ethernet
- Ten- Gigabit Ethernet

Wireless LANs

- IEEE 802.11, the Working Group Setting the Standards for Wireless LANs.
- WiFi Alliance
- IEEE 802.11x and 802.11aa IEEE standards for authentication
- Wi-Fi Planet News and hype about IEEE 802.11 wireless LANs
- IEEE 802.11 Wikipedia article
- ZigBee versus other wireless networking standards A comparison with Bluetooth, 802.11, etc.



The 802.11 Protocol Stack



Frame Format

The protocol starts when *A* decides it wants to send data to *B*. It begins by sending an RTS frame to *B* to request permission to send it a frame. When *B* receives this request, it may decide to grant permission, in which case it sends a CTS frame back. Upon receipt of the CTS, *A* now sends its frame and starts an ACK timer. Upon correct receipt of the data frame, *B* respondswith an ACK frame, terminating the exchange. If *A*'s ACK timer expires before the ACK gets back to it, the whole protocol is run again.

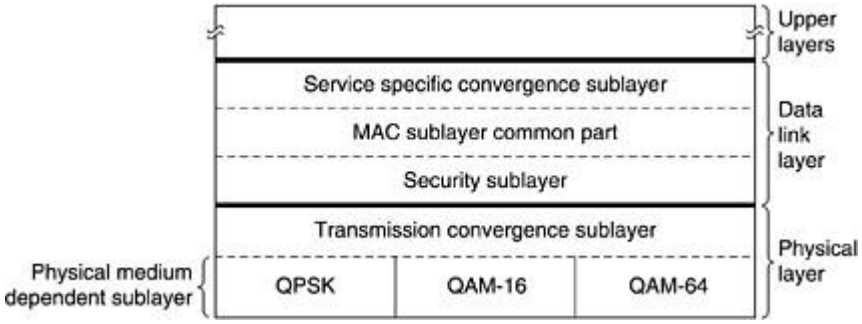
Now let us consider this exchange from the viewpoints of *C* and *D*. *C* is within range of *A*, so it may receive the RTS frame. If it does, it realizes that someone is going to send data soon, so for the good of all it desists from transmitting anything until the exchange is completed. From the information provided in the RTS request, it can estimate how long the sequence will take, including the final ACK, so it asserts a kind of virtual channel busy for itself, indicated by **NAV** (**Network Allocation Vector**)

BROADBAND WIRELESS

- IEEE 802.16 (Wireless MAN) Fixed broadband (MMDS and LMDS)
- Wireless broadband Wikipedia article
- IEEE 802.16 Wikipedia article
- WiMAX Wikipedia article
- WiMAX Forum Industry news, press releases, white papers, etc.

Running fiber, coax, or even category 5 twisted pair to millions of homes and businesses is prohibitively expensive.

The answer is broadband wireless. Erecting a big antenna on a hill just outside of town and installing antennas directed at it on customers' roofs is much easier and cheaper than digging trenches and stringing cables. Thus, competing telecommunication companies have a great interest in providing a multimegabit wireless communication service for voice, Internet, movies on demand, etc.



Protocol stack

Many people in the industry realized that having a broadband wireless standard was the key element missing, so IEEE was asked to form a committee composed of people from keycompanies and academia to draw up the standard. The next number available in the 802 numbering space was **802.16**, so the standard got this number. Work was started in July 1999, and the final standard was approved in April 2002. Officially the standard is called "Air Interface for Fixed Broadband Wireless Access Systems." However, some people prefer to call it a **wireless MAN (Metropolitan Area Network)** or a **wireless local loop**. We regard all these terms as interchangeable.

Like some of the other 802 standards, 802.16 was heavily influenced by the OSI model, including the (sub) layers, terminology, service primitives, and more. Unfortunately, also like OSI, it is fairly complicated. In the following sections we will give a brief description of some of the highlights of 802.16, but this treatment is far from complete and leaves out many details. For additional information about broadband wireless in general, see (Bolcskei et al., 2001; and Webb, 2001). For information about 802.16 in particular, see (Eklund et al., 2002).

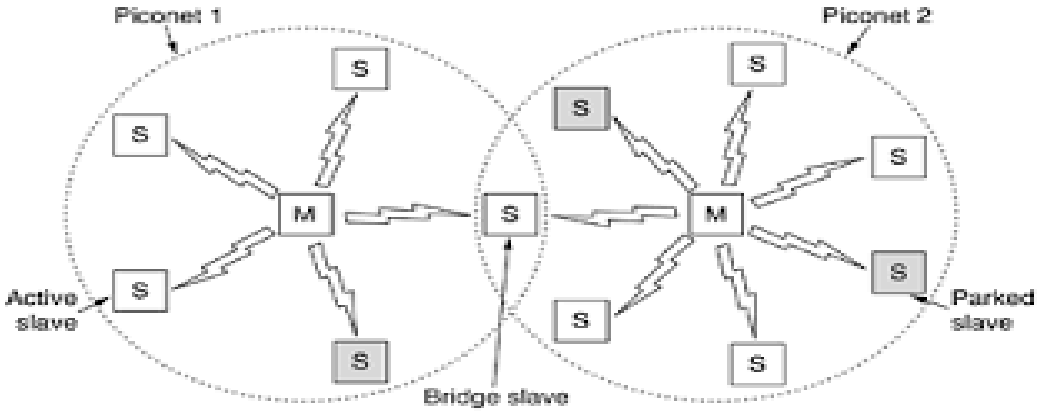
BLUETOOTH

- Bluetooth is to allow very different (portable and fixed) devices located in each other's proximity to exchange information:
- Let very different portable devices (PDA, cellular phone, notebook) set up
    - Connections.
    - Replace many of the existing cables (headset, keyboard, mouse, printer) Provide better wireless connection (handsfree solutions)
    - Provide wireless access to Internet entry points Relatively high bandwidth: 1 Mbit/second
- Also referred to as IEEE 802.15.1
- It's named after a Viking king who unified Denmark and Norway (940-981) Paolo Costa04 - MAC Sublayer Bluetooth 53

Bluetooth Architecture

Piconet: Group of devices with one master and multiple slaves. There can as much as 7 active slaves, but a total of 255 parked ones (i.e., in a power-saving state).

Scatternet: An interconnected collection of piconets A piconet is a centralized TDM system with the master determining which device gets to communicate the connection procedure for a non-existent piconet is initiated by any of the devices, which then becomes the master The master-slave design facilitates the implementation of Bluetooth chips for under 5$ Paolo Costa 04 - MAC Sublayer Bluetooth

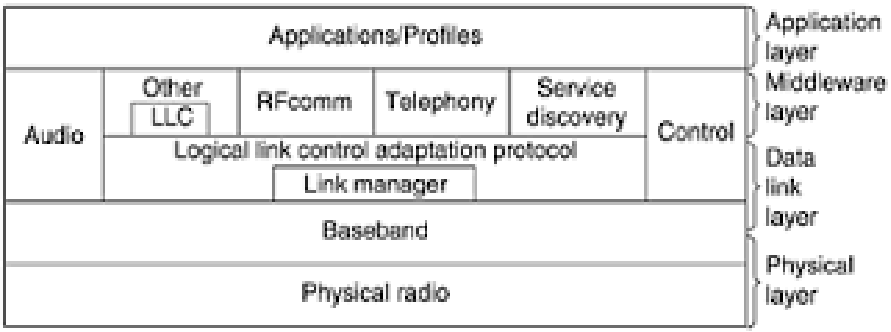


Two piconets can be connected to form a scatternet

Bluetooth Protocol Stack (1/2)

Radio: it uses frequency hopping (2.4 GHz band):

- Take data signal and modulate it with a carrier signal that changes frequency in hops.
- Good to minimize interference from other devices (microwave ovens!) hops for Bluetooth:fixed at 2402 + k MHz, k = 0, 1. . . 78.
- Modulation is frequency shift keying with 1 bit / Hertz ⇒ 1Mbps data rate but much of this isconsumed as overhead
- Baseband: Core of the data link layer.
  - Determines timing, framing, packets, and flow control.
  - Provides synchronous and asynchronous data communication.
  - Error correction can be used to provide higher reliability



802.15 version of the Bluetooth protocol architecture

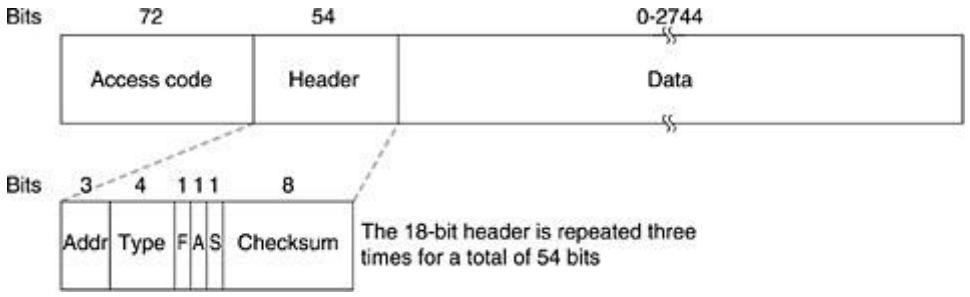
Bluetooth Protocol Stack (2/2)

Link manager: Manages connections, power management

Logical link control: Multiplexing of higher-level protocols, segmentation and reassembly of large packets, device discovery

Audio: Handles streaming for voice-related applications

RFCOMM: Emulate serial cable based on GSM protocol



Data Link Layer Switching

- LAN Switching LAN switching tutorial from Cisco
- Multiprotocol Label Switching (MPLS) Wikipedia article
- Virtual LANs
  - IEEE 802.1Q Home Page Many 802.1Q links
  - Virtual LAN s Links to articles about VLANs
  - VLAN Tutorial everything about VLANs, from Computer-Network.net

- VLAN Basics Tutorial A brief tutorial on VLANs.
- Virtual LAN Wikipedia Article
- Multiprotocol Label Switching article at Cisco

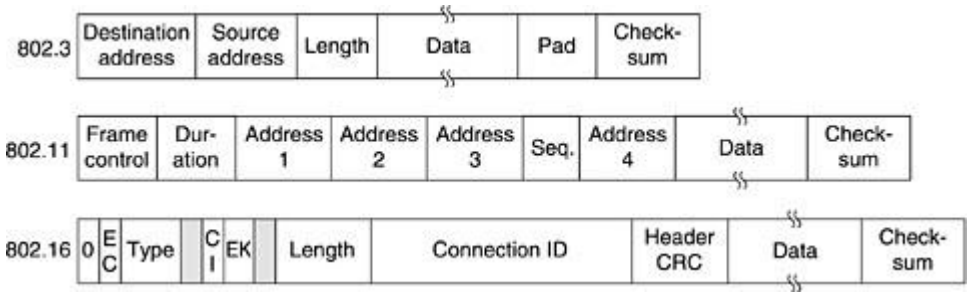
Many organizations have multiple LANs and wish to connect them. LANs can be connected by devices called **bridges**, which operate in the data link layer. Bridges examine the data layer link addresses to do routing. Since they are not supposed to examine the payload field of the frames they route, they can transport IPv4 (used in the Internet now), IPv6 (will be used in the Internet in the future), AppleTalk, ATM, OSI, or any other kinds of packets. In contrast, *routers* examine the addresses in packets and route based on them. Although this seems like a clear division between bridges and routers, some modern developments, such as the advent of switched Ethernet, have muddied the waters, as we will see later. In the following sections we will look at bridges and switches, especially for connecting different 802 LANs. For a comprehensive treatment of bridges, switches, and related topics, see (Perlman, 2000).

Before getting into the technology of bridges, it is worthwhile taking a look at some common situations in which bridges are used. We will mention six reasons why a single organization may end up with multiple LANs.

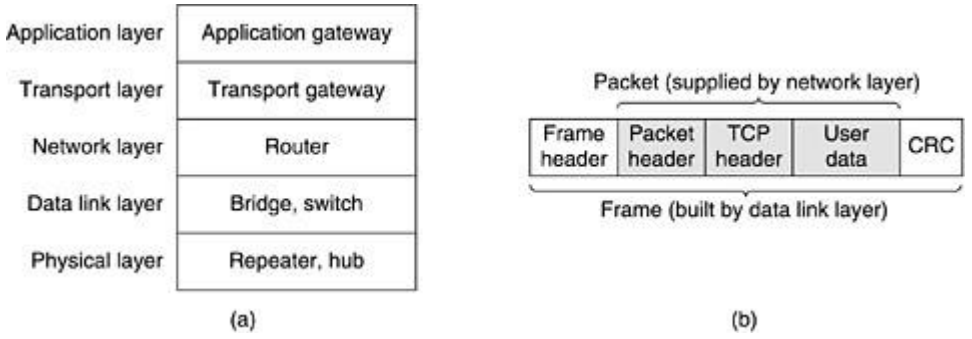
First, many university and corporate departments have their own LANs, primarily to connect their own personal computers, workstations, and servers. Since the goals of the various departments differ, different departments choose different LANs, without regard to what other departments are doing. Sooner or later, there is a need for interaction, so bridges are needed. In this example, multiple LANs came into existence due to the autonomy of their owners.

Second, the organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANs in each building and connect them with bridges and laser links than to run a single cable overthe entire site.

Third, it may be necessary to split what is logically a single LAN into separate LANs to accommodate the load. At many universities, for example, thousands of workstations are available for student and faculty computing. Files are normally kept on file server machines and are downloaded to users' machines upon request. The enormous scale of this system precludes putting all the workstations on a single LAN—the total bandwidth needed is far too high. Instead, multiple LANs connected by bridges are used, as shown in Fig 3.14. Each LAN contains a cluster of workstations with its own file server so that most traffic is restricted to a single LAN and does not add load to the backbone.



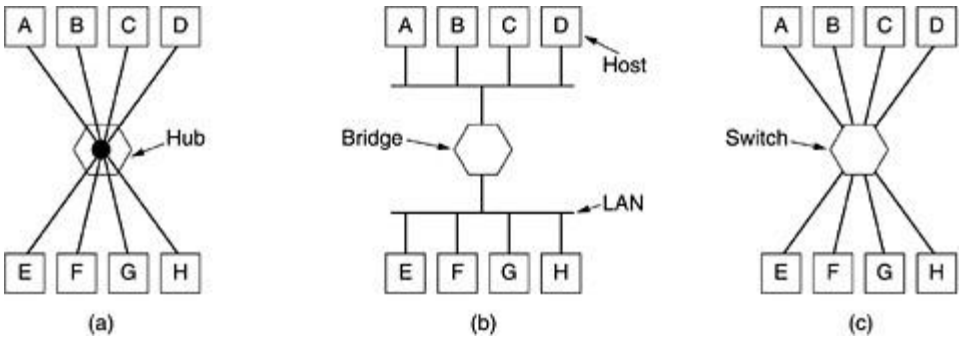
The IEEE 802 frame formats



(a) Which device is in which layer. (b) Frames, packets, and headers.

Now let us look at the switching devices and see how they relate to the packets and frames. At the bottom, in the physical layer, we find the repeaters. These are analog devices that are connected to two cable segments. A signal appearing on one of them is amplified and put outon the other. Repeaters do not understand frames, packets, or headers. They understand volts. Classic Ethernet, for example, was designed to allow four repeaters, in order to extend the maximum cable length from 500 meters to 2500 meters.

Next we come to the hubs. A hub has a number of input lines that it joins electrically.Frames arriving on any of the lines are sent out on all the others. If two frames arrive at the same time, they will collide, just as on a coaxial cable. In other words, the entire hub forms a single collision domain. All the lines coming into a hub must operate at the same speed. Hubs differ from repeaters in that they do not (usually) amplify the incoming signals and are designed to hold multiple line cards each with multiple inputs, but the differences are slight. Like repeaters, hubs do not examine the 802 addresses or use them in any way.



(a) A hub. (b) A bridge. (c) A switch

Network Layer

Network Layer Design Issues

3.17 Store-and-Forward Packet Switching

The major components of the system are the carrier's equipment (routers connected by transmission lines), shown inside the shaded oval, and the customers' equipment, shown outside the oval.

Host H1 is directly connected to one of the carrier's routers, A, by a leased line. In contrast, H2 is on a LAN with a router, F, owned and operated by the customer. This router also has a leased line to the carrier's equipment.

·We have shown F as being outside the oval because it does not belong to the carrier, but in terms of construction, software, and protocols, it is probably no different from the carrier's routers.

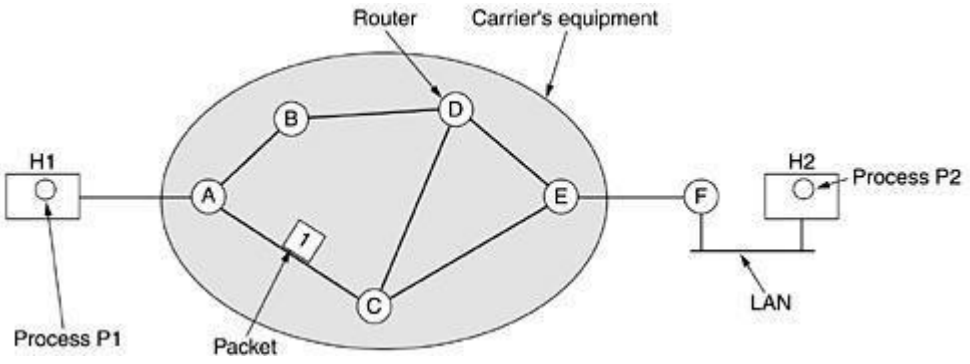


Figure 3.17 The environment of the network layer protocols.

This equipment is used as follows. A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier. The packet is storedthere until it has fully arrived so the checksum can be verified.

·Then it is forwarded to the next router along the path until it reaches the destination host, whereit is delivered. This mechanism is store-and-forward packet switching.

Services provided to the Transport Layer

The network layer provides services to the transport layer at the network layer/transport layer interface. An important question is what kind of services the network layer provides to the transportlayer.

The network layer services have been designed with the following goals in mind.

1.The services should be independent of the router technology.

2.The transport layer should be shielded from the number, type, and topology of the routers present.

3.The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

Given these goals, the designers of the network layer have a lot of freedom in writing detailed specifications of the services to be offered to the transport layer. This freedom often degenerates into a raging battle between two warring factions.

The other camp argues that the subnet should provide a reliable, connection-oriented service. They claim that 100 years of successful experience with the worldwide telephone system is an

excellent guide. In this view, quality of service is the dominant factor, and without connections in the subnet, quality of service is very difficult to achieve, especially for real-time traffic such as voice and video.

These two camps are best exemplified by the Internet and ATM. The Internet offers connectionless network-layer service; ATM networks offer connection-oriented network-layer service. However, it is interesting to note that as quality-of-service guarantees are becoming more and more important, the Internet is evolving.

3.18 Implementation of Connectionless Service

Two different organizations are possible, depending on the type of service offered. If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed.

In this context, the packets are frequently called datagrams (in analogy with telegrams) and the subnet is called a datagram subnet. If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent.

This connection is called a VC (virtual circuit), in analogy with the physical circuits set up by the telephone system, and the subnet is called a virtual-circuit subnet. In this section we will examine datagram subnets; in the next one we will examine virtual-circuit subnets.

Let us now see how a datagram subnet works. Suppose that the process P1 in Fig. 3-18 has a long message for P2. It hands the message to the transport layer with instructions to deliver it to process P2 on host H2.

The transport layer code runs on H1, typically within the operating system. It prepends a transport header to the front of the message and hands the result to the network layer, probably just another procedure within the operating system.

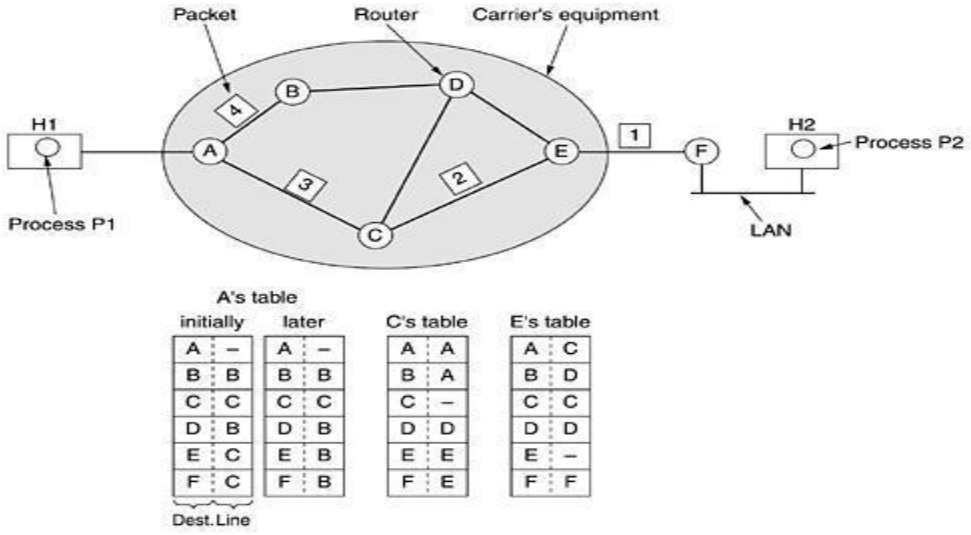


Figure 3.18 Routing within a datagram subnet.

Let us assume that the message is four times longer than the maximum packet size, so the network layer has to break it into four packets, 1, 2, 3, and 4 and sends each of them in turn to router A using some point-to-point protocol, for example, PPP.

At this point the carrier takes over. Every router has an internal table telling it where to send packets for each possible destination. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination.

Only directly-connected lines can be used. A has only two outgoing lines—to B and C—so every incoming packet must be sent to one of these routers, even if the ultimate destination is some other router. A's initial routing table is shown in the figure under the label "initially."

However, something different happened to packet 4. When it got to A it was sent to router B, even though it is also destined for F. For some reason, A decided to send packet 4 via a different route than that of the first three.

Perhaps it learned of a traffic jam somewhere along the ACE path and updated its routing table, as shown under the label "later." The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

3.19 Implementation of Connection-Oriented Service

For connection-oriented service, we need a virtual-circuit subnet. The idea behind virtual circuits

is to avoid having to choose a new route for every packet sent, as in Fig.

Instead, when a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers. That route is used for all traffic flowing over the connection, exactly the same way that the telephone system works.

When the connection is released, the virtual circuit is also terminated. With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to. As an example, consider the situation of Fig. 3-3. Here, host H1 has established connection 1 with host H2.

It is remembered as the first entry in each of the routing tables. The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1. Similarly, the first entry at C routes the packet to E, also with connection identifier

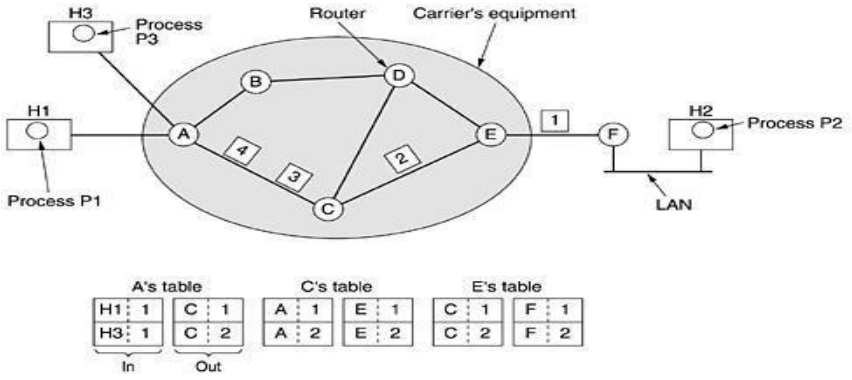


Figure 3-19. Routing within a virtual-circuit subnet.

Now let us consider what happens if H3 also wants to establish a connection to H2. It chooses connection identifier 1 and tells the subnet to establish the virtual circuit. This leads to the second row in the tables.

Note that we have a conflict here because although A can easily distinguish connection 1 packets from H1 from connection 1 packets from H3, C cannot do this. For this reason, A assigns a different connection identifier to the outgoing traffic for the second connection.

Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets. In some contexts, this is called label switching.

3.20 Comparison of Virtual-Circuit and Datagram Subnets

Both virtual circuits and datagrams have their supporters and their detractors. We will now attempt to summarize the arguments both ways. The major issues are listed in ,although purists could probably find a counterexample for everything in the figure.

Table 3.20.1

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Inside the subnet, several trade-offs exist between virtual circuits and datagrams. One trade-off is between router memory space and bandwidth. Virtual circuits allow packetsto contain circuit numbers instead of full destination addresses.If the packets tend to be fairly short, a full destination address in every packet may represent a significant amount of overhead and hence, wasted bandwidth. The price paid for using virtual circuits internally is the table space within the routers.

Depending upon the relative cost of communication circuits versus router memory, oneor the other may be cheaper. Another trade-off is setup time versus address parsing time. Using virtual circuits requires a setup phase, which takes time and consumes resources.

However, figuring out what to do with a data packet in a virtual-circuit subnet is easy: the router just uses the circuit number to index into a table to find out where the packet goes. In a datagram subnet, a more complicated lookup procedure is required to locate the entry for the destination.

For transaction processing systems (e.g., stores calling up to verify credit card purchases), the overhead required to set up and clear a virtual circuit may easily dwarf the use of the circuit. If the majority of the traffic is expected to be of this kind, the use of virtual circuits inside the subnet makes little sense.

On the other hand, permanent virtual circuits, which are set up manually and last for months or years, may be useful here. Virtual circuits also have a vulnerability problem. If a router crashes and loses its memory, even if it comes back up a second later, all the virtual circuits passing through it will have to be aborted.

In contrast, if a datagram router goes down, only those users whose packets were queued in the router at the time will suffer, and maybe not even all those, depending upon whether they have already been acknowledged.

The loss of a communication line is fatal to virtual circuits using it but can be easily compensated for if datagrams are used. Datagrams also allow the routers to balance the traffic throughout the subnet, since routes can be changed partway through a long sequence of packet transmissions.

TEXT / REFERENCE BOOKS:

1. William Stallings, Data and Computer Communications, 10th Edition, Pearson, 2014.
2. Wayne Thomasi, "Advanced Electronic Communication Systems", 6th Edition, PHI Publishers, 2003.
3. Simon Haykins, “Communication Systems” John Wiley, 5th Edition, March 2009.
4. John G. Proakis, MasoudSalehi, “Digital Communication”, McGraw Hill 5th edition November 6, 2007.
5. Bernard Sklar, “Digital Communication, Fundamentals and Application”, Pearson Education Asia, 2nd Edition, Jan. 21, 2001.
6. Behrouz A. Forouzen, “Data communication and Networking”, Fourth Edition, Tata McGraw – Hill, 2011.
7. Andrew S.Tanenbaum, “Computer Networks”, 5th Edition, Pearson, 2011.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ECE

UNIT IV NETWORK LAYER COMPONENTS AND FUNCTIONS - SCSA1305

UNIT 4 NETWORK LAYER COMPONENTS AND FUNCTIONS

Network Layer Logical addressing: IPv4 & IPV6, Subnetting, DHCP, Virtual LAN, Networking devices (Hubs, Bridges & Switches), Network topologies. Routing: Routing and Forwarding, Static routing and Dynamic routing, Routing Algorithms: Distance vector routing algorithm, col (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), MPLS.

What is Network Layer?

The network layer is concerned with getting packets from the source all the way to the destination. The packets may require to make many hops at the intermediate routers while reaching the destination. This is the lowest layer that deals with end to end transmission. In order to achieve its goals, the network layer must know about the topology of the communication network. It must also take care to choose routes to avoid overloading of some of the communication lines while leaving others idle. The network layer-transport layer interface frequently is the interface between the carrier and the customer, that is the boundary of the subnet. The functions of this layer include :

1. Routing - The process of transferring packets received from the Data Link Layer of the source network to the Data Link Layer of the correct destination network is called routing. Involves decision making at each intermediate node on where to send the packet next so that it eventually reaches its destination. The node which makes this choice is called a router. For routing we require some mode of addressing which is recognized by the Network Layer. This addressing is different from the MAC layer addressing.
2. Inter-networking - The network layer is the same across all physical networks (such as Token-Ring and Ethernet). Thus, if two physically different networks have to communicate, the packets that arrive at the Data Link Layer of the node which connects these two physically different networks, would be stripped of their headers and passed tothe Network Layer. The network layer would then pass this data to the Data Link Layer of the other physical network..
3. Congestion Control - If the incoming rate of the packets arriving at any router is morethan the outgoing rate, then congestion is said to occur. Congestion may be caused by many factors. If suddenly, packets begin arriving on many input lines and all need the same output line, then a queue will build up. If there is insufficient memory to hold all of them, packets will be lost. But even if routers have an infinite amount of memory, congestion gets worse, because by the time packets reach to the front of the queue, they have already timed out (repeatedly), and duplicates have been sent. All these packets are dutifully forwarded to the next router, increasing the load all the way to the destination. Another reason for congestion are slow processors. If the router's CPUs are

slow at performing the bookkeeping tasks required of them, queues can build up, even though there is excess line capacity. Similarly, low-bandwidth lines can also cause congestion.

The main functions performed by the network layer are as follows:

- Routing
- Congestion Control
- Internetwokring

Routing

Routing is the process of forwarding of a packet in a network so that it reaches its intendeddestination. The main goals of routing are:

1. ***Correctness:*** The routing should be done properly and correctly so that the packets may reach their proper destination.
2. ***Simplicity:*** The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.
3. ***Robustness:*** Once a major network becomes operative, it may be expected to run continuously for years without any failures. The algorithms designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.
4. ***Stability:*** The routing algorithms should be stable under all possible circumstances.
5. ***Fairness:*** Every node connected to the network should get a fair chance of transmitting their packets. This is generally done on a first come first serve basis.
6. ***Optimality:*** The routing algorithms should be optimal in terms of throughput and minimizing mean packet delays. Here there is a trade-off and one has to choose depending on his suitability.

Classification of Routing Algorithms

The routing algorithms may be classified as follows:

1. ***Adaptive Routing Algorithm:*** These algorithms change their routing decisions to reflect changes in the topology and in traffic as well. These get their routing information from adjacent routers or from all routers. The optimization parameters are the distance, number of hops and estimated transit time. This can be further classified as follows:
    1. ***Centralized:*** In this type some central node in the network gets entire information about the network topology, about the traffic and about other nodes. This then transmits this information to the respective routers. The advantage of this is that only one node is required to keep the information. The disadvantage isthat if the

central node goes down the entire network is down, i.e. single point of failure.

2. ***Isolated:*** In this method the node decides the routing without seeking information from other nodes. The sending node does not know about the status of a particular link. The disadvantage is that the packet may be send through acongested route resulting in a delay. Some examples of this type of algorithm for routing are:
    - ***Hot Potato:*** When a packet comes to a node, it tries to get rid of it as fast as it can, by putting it on the shortest output queue without regard to where that link leads. A variation of this algorithm is to combine static routing with the hot potato algorithm. When a packet arrives, the routing algorithm takes into account both the static weights of the links and the queue lengths.
    - ***Backward Learning:*** In this method the routing tables at each node gets modified by information from the incoming packets. One way toimplement backward learning is to include the identity of the source node in each packet, together with a hop counter that is incremented on each hop. When a node receives a packet in a particular line, it notes down the number of hops it has taken to reach it from the source node. If the previous value of hop count stored in the node is better than the current one then nothing is done but if the current value is better then the value is updated for future use. The problem with this is that when the best route goes down then it cannot recall the second best route to a particular node. Hence all the nodes have to forget the stored informations periodically and start all over again.
3. ***Distributed:*** In this the node receives information from its neighbouring nodes and then takes the decision about which way to send the packet. The disadvantage is that if in between the the interval it receives information and sends the paket something changes then the packet may be delayed.

2. ***Non-Adaptive Routing Algorithm:*** These algorithms do not base their routing decisions on measurements and estimates of the current traffic and topology. Insteadthe route to be taken in going from one node to the other is computed in advance, off- line, and downloaded to the routers when the network is booted. This is also known as static routing. This can be further classified as:
    1. ***Flooding:*** Flooding adapts the technique in which every incoming packet is sent on every outgoing line except the one on which it arrived. One problem with this method is that packets may go in a loop. As a result of this a node may receive several copies of a particular packet which is undesirable. Some techniques adapted to overcome these problems are as follows:
        - ***Sequence Numbers:*** Every packet is given a sequence number. When a node receives the packet it sees its source address and sequence number. If the node finds that it has sent the same packet earlier then it will not transmit the packet and will just discard it.
        - ***Hop* Count:** Every packet has a hop count associated with it. This is decremented(or incremented) by one by each node which sees it. When the hop count becomes zero(or a maximum possible value) the packet is dropped.

- **Spanning Tree:** The packet is sent only on those links that lead to the destination by constructing a spanning tree routed at the source. This avoids loops in transmission but is possible only when all the intermediatenodes have knowledge of the network topology.

Flooding is not practical for general kinds of applications. But in cases wherehigh degree of robustness is desired such as in military applications, flooding isof great help.

2. ***Random Walk:*** In this method a packet is sent by the node to one of its neighbours randomly. This algorithm is highly robust. When the network is highly interconnected, this algorithm has the property of making excellent use of alternative routes. It is usually implemented by sending the packet onto the least queued link.

Delta Routing

Delta routing is a hybrid of the centralized and isolated routing algorithms. Here each node computes the cost of each line (i.e some functions of the delay, queue length, utilization, bandwidth etc) and periodically sends a packet to the central node giving it these values which then computes the **k** best paths from node **i** to node **j**. Let **Cij1** be the cost of the best **i-j** path, **Cij2** the cost of the next best path and so on.If **Cijn - Cij1 < delta**, (**Cijn** - costof **n'th** best**i-j** path, **delta** is some constant) then path **n** is regarded equivalent to the best **i-j** path since their cost differ by so little. When **delta -> 0** this algorithm becomes centralized routing and when **delta -> infinity** all the paths become equivalent.

Multipath Routing

In the above algorithms it has been assumed that there is a single best path between any pair of nodes and that all traffic between them should use it. In many networks however there are several paths between pairs of nodes that are almost equally good. Sometimes in order to improve the performance multiple paths between single pair of nodes are used. This techniqueis called multipath routing or bifurcated routing. In this each node maintains a table with one row for each possible destination node. A row gives the best, second best, third best, etc outgoing line for that destination, together with a relative weight. Before forwarding a packet, the node generates a random number and then chooses among the alternatives, using the weights as probabilities. The tables are worked out manually and loaded into the nodes before the network is brought up and not changed thereafter.

Hierarchical Routing

In this method of routing the nodes are divided into regions based on hierarchy. A particular node can communicate with nodes at the same hierarchial level or the nodes at a lower level and directly under it. Here, the path from any source to a destination is fixed and is exactly one if the heirarchy is a tree.

Non-Hierarchical Routing

In this type of routing, interconnected networks are viewed as a single network, where bridges, routers and gateways are just additional nodes.

- Every node keeps information about every other node in the network
- In case of adaptive routing, the routing calculations are done and updated for all the nodes.

The above two are also the disadvantages of non-hierarchical routing, since the table sizes and the routing calculations become too large as the networks get bigger. So this type of routing is feasible only for small networks.

Hierarchical Routing

This is essentially a 'Divide and Conquer' strategy. The network is divided into different regions and a router for a particular region knows only about its own domain and other routers. Thus, the network is viewed at two levels:

1. The Sub-network level, where each node in a region has information about its peers in the same region and about the region's interface with other regions. Different regionsmay have different 'local' routing algorithms. Each local algorithm handles the traffic between nodes of the same region and also directs the outgoing packets to the appropriate interface.
2. The Network Level, where each region is considered as a single node connected to its interface nodes. The routing algorithms at this level handle the routing of packets between two interface nodes, and is isolated from intra-regional transfer.

Networks can be organized in hierarchies of many levels; e.g. local networks of a city at one level, the cities of a country at a level above it, and finally the network of all nations.

In Hierarchical routing, the interfaces need to store information about:

- All nodes in its region which are at one level below it.
- Its peer interfaces.

- At least one interface at a level above it, for outgoing packages.

Advantages :

- Smaller sizes of routing tables.
- Substantially lesser calculations and updates of routing tables.

Disadvantage :

- Once the hierarchy is imposed on the network, it is followed and possibility of direct paths is ignored. This may lead to sub optimal routing.

Source Routing

Source routing is similar in concept to virtual circuit routing. It is implemented as under:

- Initially, a path between nodes wishing to communicate is found out, either by flooding or by any other suitable method.
- This route is then specified in the header of each packet routed between these two nodes. A route may also be specified partially, or in terms of some intermediate hops.

Advantages:

- Bridges do not need to lookup their routing tables since the path is already specified in the packet itself.
- The throughput of the bridges is higher, and this may lead to better utilization of bandwidth, once a route is established.

Disadvantages:

- Establishing the route at first needs an expensive search method like flooding.
- To cope up with dynamic relocation of nodes in a network, frequent updates of tables are required, else all packets would be sent in wrong direction. This too is expensive.

Policy Based Routing

In this type of routing, certain restrictions are put on the type of packets accepted and sent. e.g.. The IIT- K router may decide to handle traffic pertaining to its departments only, and reject packets from other routes. This kind of routing is used for links with very low capacity or for security purposes.

Shortest Path Routing

Here, the central question dealt with is 'How to determine the optimal path for routing ?' Various algorithms are used to determine the optimal routes with respect to some predetermined criteria. A network is represented as a graph, with its terminals as nodes and the links as edges. A 'length' is associated with each edge, which represents the cost of using the link for transmission. Lower the cost, more suitable is the link. The cost is determined depending upon the criteria to be optimized. Some of the important ways of determining the cost are:

- ***Minimum number of hops:*** If each link is given a unit cost, the shortest path is the one with minimum number of hops. Such a route is easily obtained by a breadth first search method. This is easy to implement but ignores load, link capacity etc.
- ***Transmission and Propagation Delays*****:** If the cost is fixed as a function of transmission and propagation delays, it will reflect the link capacities and the geographical distances. However these costs are essentially static and do not consider the varying load conditions.
- ***Queuing Delays:*** If the cost of a link is determined through its queuing delays, it takes care of the varying load conditions, but not of the propagation delays.

Ideally, the cost parameter should consider all the above mentioned factors, and it should be updated periodically to reflect the changes in the loading conditions. However, if the routes are changed according to the load, the load changes again. This feedback effect between routing and load can lead to undesirable oscillations and sudden swings.

Routing Algorithms

As mentioned above, the shortest paths are calculated using suitable algorithms on the graph representations of the networks. Let the network be represented by graph G (V, E) and let the number of nodes be 'N'. For all the algorithms discussed below, the costs associated with the links are assumed to be positive. A node has zero cost w.r.t itself. Further, all the links are assumed to be symmetric, i.e. if $d_{i,j}$ = cost of link from node i to node j, then $d_{i,j} = d_{j,i}$. The graph is assumed to be complete. If there exists no edge between two nodes, then a link of infinite cost is assumed. The algorithms given below find costs of the paths from all nodes to a particular node; the problem is equivalent to finding the cost of paths from a source to all destinations.

Bellman-Ford Algorithm

This algorithm iterates on the number of edges in a path to obtain the shortest path. Since the number of hops possible is limited (cycles are implicitly not allowed), the algorithm terminates giving the shortest path.

Notation:

$d_{i,j}$ = Length of path between nodes i and j, indicating the cost of the link.
h = Number of hops.
D[i,h] = Shortest path length from node i to node 1, with upto 'h' hops.D[1,h] = 0 for all h .

Algorithm :

Initial condition : D[i, 0] = infinity, for all i (i != 1)

Iteration : D[i, h+1] = min { $d_{i,j}$ + D[j,h] } over all values of j

.Termination : The algorithm terminates when

D[i, h] = D [i, h+1] for all i .

Principle:

For zero hops, the minimum length path has length of infinity, for every node. For one hop the shortest-path length associated with a node is equal to the length of the edge between that node and node 1. Hereafter, we increment the number of hops allowed, (from h to h+1) and find out whether a shorter path exists through each of the other nodes. If it exists, say through node 'j', then its length must be the sum of the lengths between these two nodes (i.e. $d_{i,j}$) and the shortest path between j and 1 obtainable in upto h paths. If such a path doesn't exist, then

the path length remains the same. The algorithm is guaranteed to terminate, since there are utmost N nodes, and so N-1 paths. It has time complexity of O (N^3) .

Dijkstra's Algorithm

Notation:

D_i = Length of shortest path from node 'i' to node 1.
$d_{i,j}$ = Length of path between nodes i and j .

Algorithm

Each node j is labeled with Dj, which is an estimate of cost of path from node j to node 1. Initially, let the estimates be infinity, indicating that nothing is known about the paths. We now iterate on the length of paths, each time revising our estimate to lower values, as we obtain them. Actually, we divide the nodes into two groups ; the first one, called set P contains the nodes whose shortest distances have been found, and the other Q containing all the remaining nodes. Initially P contains only the node 1. At each step, we select the node that has minimum cost path to node 1. This node is transferred to set P. At the first step, this corresponds to shifting the node closest to 1 in P. Its

minimum cost to node 1 is now known. At the next step, select the next closest node from set Q and update the labels corresponding to each node using
:

$$D_j = \min [D_j , D_i + d_{j,i}] \quad (3.4)$$

Finally, after N-1 iterations, the shortest paths for all nodes are known, and the algorithm terminates.

Principle

Let the closest node to 1 at some step be i. Then i is shifted to P. Now, for each node j , the closest path to 1 either passes through i or it doesn't. In the first case Dj remains the same. In the second case, the revised estimate of D_j is the sum $D_i + d_{i,j}$. So we take the minimum of these two cases and update D_j accordingly. As each of the nodes get transferred to set P, the estimates get closer to the lowest possible value. When a node is transferred, its shortest path length is known. So finally all the nodes are in P and the D_j 's represent the minimum costs. The algorithm is guaranteed to terminate in N-1 iterations and its complexity is $O(N^2)$.

The Floyd Warshall Algorithm

This algorithm iterates on the set of nodes that can be used as intermediate nodes on paths. This set grows from a single node (say node 1) at start to finally all the nodes of the graph. At each iteration, we find the shortest path using given set of nodes as intermediate nodes, so that finally all the shortest paths are obtained.

Notation

$D_{i,j}[n]$ = Length of shortest path between the nodes i and j using only the nodes 1,2,.....n as intermediate nodes.

Initial Condition

$Di,j[0] = d_{i,j}$ for all nodes i,j .

Algorithm

Initially, n = 0. At each iteration, add next node to n. i.e. For n = 1,2, ...N-1 ,

$$Di,j[n + 1] = \min \{ D_{i,j}[n] , D_{i,n+1}[n] + D_{n+1,j}[n] \} \quad (3.5)$$

Principle

Suppose the shortest path between i and j using nodes 1,2,...n is known. Now, if node n+1 is allowed to be an intermediate node, then the shortest path under new conditions either passes through node n+1 or it doesn't. If it does not pass through the node n+1, then $D_{i,j}[n+1]$ is same

as $D_{i,j}[n]$. Else, we find the cost of the new route, which is obtained from the sum, $D_{i,n+1}[n]$ + $D_{n+1,j}[n]$. So we take the minimum of these two cases at each step. After adding all the nodes to the set of intermediate nodes, we obtain the shortest paths between all pairs of nodes together. The complexity of Floyd-Warshall algorithm is O (N^3).

It is observed that all the three algorithms mentioned above give comparable performance, depending upon the exact topology of the network.

Address Resolution Protocol

If a machine talks to another machine in the same network, it requires its physical or MAC address. But ,since the application has given the destination's IP address it requires some mechanism to bind the IP address with its MAC address.This is done through Address Resolution protocol (ARP).IP address of the destination node is broadcast and the destination node informs the source of its MAC address.

1. Assume broadcast nature of LAN
2. Broadcast IP address of the destination
3. Destination replies it with its MAC address.
4. Source maintains a cache of IP and MAC address bindings

But this means that every time machine A wants to send packets to machine B, A has to sendan ARP packet to resolve the MAC address of B and hence this will increase the traffic load too much, so to reduce the communication cost computers that use ARP maintains a cache of recently acquired IP_to_MAC address bindings, i.e. they dont have to use ARP repeatedly. ARP Refinements Several refinements of ARP are possible: When machine A wants to send packets to macine B, it is possible that machine B is going to send packets to machine A in the near future.So to avoid ARP for machine B, A should put its IP_to_MAC address binding in the special packet while requesting for the MAC address of B. Since A broadcasts its initial request for the MAC address of B, every machine on the network should extract and store in its cache the IP_to_MAC address binding of A When a new machine appears on the network (e.g. when an operating system reboots) it can broadcast its IP_to_MAC address binding so that all other machines can store it in their caches. This will eliminate a lot of ARP packets by all other machines, when they want to communicate with this new machine.

Example displaying the use of Address Resolution Protocol:

Consider a scenario where a computer tries to contact some remote machine using pingprogram, assuming that there has been no exchange of IP datagrams previously between the two machines and therefore arp packet must be sent to identify the MAC address of the remote machine.

The arp request message (who is A.A.A.A tell B.B.B.B where the two are IP addresses) is broadcast on the local area network with an Ethernet protocol type 0x806. The packet isdiscarded

by all the machines except the target machine which responds with an arp response message (A.A.A.A is hh:hh:hh:hh:hh:hh where hh:hh:hh:hh:hh:hh is the Ethernet source address). This packet is unicast to the machine with IP address B.B.B.B. Since the arp request message included the hardware address (Ethernet source address) of the requesting computer, target machine doesn't require another arp message to figure it out.

Reverse Address Resolution Protocol

RARP is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. This is needed since the machine may not have permanently attacded disk where it can store its IP address permanently. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Medium Access Control - MAC) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Both the machine that issues the request and the server that responds use physical network addresses during their brief communication. Usually, the requester does not know the physical address. So, the request is broadcasted to all the machines on the network. Now, the requester must identify istelf uniquely to the server. For this either CPU serial number or the machine's physical network address can be used. But using the physical address as a unique id has two advantages.

- These addresses are always available and do not have to be bound into bootstrap code.
- Because the identifying information depends on the network and not on the CPU vendor, all machines on a given network will supply unique identifiers.

Request:

Like an ARP message, a RARP message is sent from one machine to the another encapsulatedin the data portion of a network frame. An ethernet frame carrying a RARP request has the usual preamle, Ethernet source and destination addresses, and packet type fields in front of the frame. The frame conatins the value 8035 (base 16) to identify the contents of the frame as a RARP message. The data portion of the frame contains the 28-octet RARP message. The sender braodcasts a RARP request that specifies itself as both the sender and target machine, and supplies its physical network address in the target hardware address field. All machines on the network receive the request, but only those authorised to supply the RARP services process the request and send a reply, such machines are known informally as RARP servers. For RARP to succeed, the network must contain at least one RARP server.

Reply:

Servers answers request by filling in the target protocol address field, changing the message type from request to reply, and sending the reply back directly to the machine making the request.

Timing RARP Transactions

Since RARP uses the physical network directly, no other protocol software will time the response or retransmit the request. RARP software must handle these tasks. Some workstations that rely on RARP to boot, choose to retry indefinitely until the receive a response. Other implementations announce failure after only a few tries to avoid flooding the network with unnecessary broadcast.

Mulitple RARP Servers Advantage: More reliability. Diadvantage: Overloading may result when all servers respond. So, to get away with disadvantage we have primary and secondary servers. Each machine that makes RARP request is assigned a primary server. Normally, the primary server responds but if it fails, then requester may time out and rebroadcast the request.Whenever a secondary server receives a second copy of the request within a short time of the first, it responds. But, still there might be a problem that all secondary servers respond, thus overloading the network. So, the solution adopted is to avoid having all secondary servers transmit responses simultaneously. Each secondary server that receives the request computes a random delay and then sends a response.

Drawbacks of RARP

- Since it operates at low level, it requires direct addresss to the network which makes it difficult for an application programmer to build a server.
- It doesn't fully utilizes the capability of a network like ethernet which is enforced to send a minimum packet size since the reply from the server contains only one small piece of information, the 32-bit internet address.

RARP is formally described in RFC903.

Congestion Control Algorithms

As Internet can be considered as a Queue of packets, where transmitting nodes are constantly adding packets and some of them (receiving nodes) are removing packets from the queue. So, consider a situation where too many packets are present in this queue (or internet or a part of internet), such that constantly transmitting nodes are pouring packets at a higher rate than receiving nodes are removing them. This degrades the performance, and such a situationis termed as Congestion. Main reason of congestion is more number of packets into the networkthan it can handle. So, the objective of congestion control can be summarized as to maintain thenumber of packets in the network below the level at which performance falls off dramatically.The nature of a Packet switching network can be summarized in following points:

• A network of queues

• At each node, there is a queue of packets for each outgoing channel

• If packet arrival rate exceeds the packet transmission rate, the queue size grows without bound

• When the line for which packets are queuing becomes more than 80% utilized, the queue length grows alarmingly

When the number of packets dumped into the network is within the carrying capacity, they all are delivered, expect a few that have too be rejected due to transmission errors). And then the number delivered is proportional to the number of packets sent. However, as traffic increases too far, the routers are no longer able to cope, and they begin to lose packets. This tends to make matter worse. At very high traffic, performance collapse completely, and almost no packet is delivered. In the following sections, the causes of congestion, the effects of congestion and various congestion control techniques are discussed in detail

Causes Of Congestion

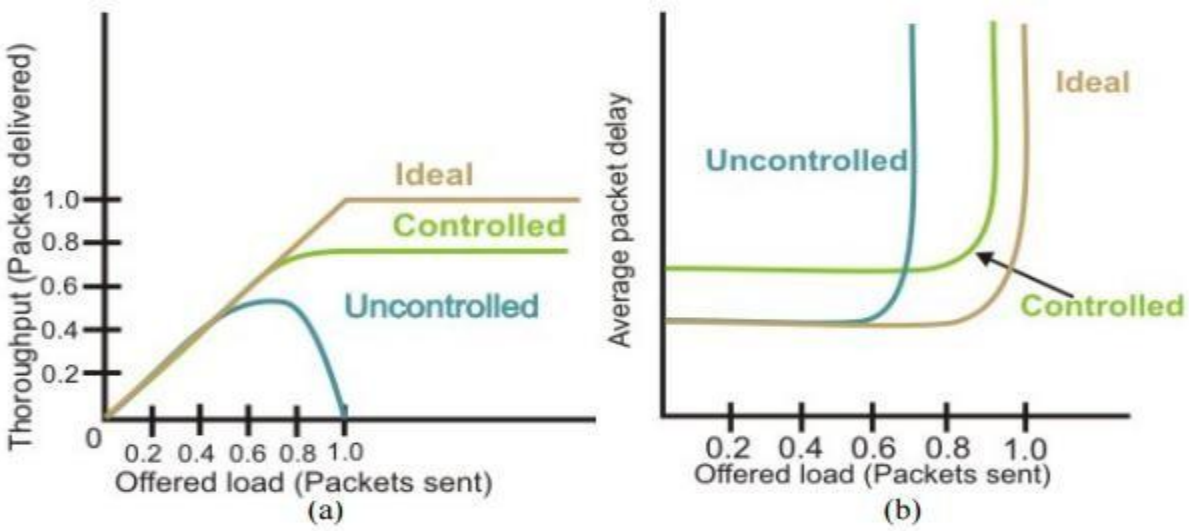
Congestion can occur due to several reasons. For example, if all of a sudden a streamof packets arrive on several input lines and need to be out on the same output line, then a long queue will be build up for that output. If there is insufficient memory to hold these packets, then packets will be lost (dropped). Adding more memory also may not help in certain situations. If router have an infinite amount of memory even then instead of congestion being reduced, it getsworse; because by the time packets gets at the head of the queue, to be dispatched out to the output line, they have already timed-out (repeatedly), and duplicates may also be present. All the packets will be forwarded to next router up to the destination, all the way only increasing the load to the network more and more. Finally when it arrives at the destination, the packet will be discarded, due to time out, so instead of been dropped at any intermediate router (in case memory is restricted) such a packet goes all the way up to the destination, increasing the network load throughout and then finally gets dropped there. Slow processors also causeCongestion. If the router CPU is slow at performing the task required for them (Queuing buffers, updating tables, reporting any exceptions etc.), queue can build up even if there is excess ofline capacity. Similarly, LowBandwidth lines can also cause congestion. Upgrading lines but not changing slow processors, or vice-versa, often helps a little; these can just shift the bottleneckto some other point. The real problem is the mismatch between different parts of the system. Congestion tends to feed upon itself to get even worse. Routers respond to overloading by dropping packets. When these packets contain TCP segments, the segments don't reach their destination, and they are therefore left unacknowledged, which eventually leads to timeout and retransmission. So, the major cause of congestion is often the bursty nature of traffic. If the hosts could be made to transmit at a uniform rate, then congestion

problem will be less commonand all other causes will not even led to congestion because other causes just act as anenzyme which boosts up the congestion when the traffic is bursty (i.e., other causes just add on to make the problem more serious, main cause is the bursty traffic). This means that when a device sends a packet and does not receive an acknowledgment from the receiver, in most the cases it can be assumed that the packets have been dropped by intermediate devices due to congestion. By detecting the rate at which segments are sent and not acknowledged, the sourceor an intermediate router can infer the level of congestion on the network. In the followingsection we shall discuss the ill effects of congestion.

Effects of Congestion

Congestion affects two vital parameters of the network performance, namely throughput and delay. In simple terms, the throughput can be defined as the percentage utilization of the network capacity. Figure shows how throughput is affected as offered loadincreases. Initially throughput increases linearly with offered load, because utilization of the network increases.

However, as the offered load increases beyond certain limit, say 60% of the capacity of the network, the throughput drops. If the offered load increases further, a point is reached when nota single packet is delivered to any destination, which is commonly known as deadlock situation. There are three curves in Fig. the ideal one corresponds to the situation when all the packets introduced are delivered to their destination up to the maximum capacity of the network. The second one corresponds to the situation when there is no congestion control. The third one is the case when some congestion control technique is used. This prevents the throughput collapse, but provides lesser throughput than the ideal condition due to overhead of the congestion control technique. The delay also increases with offered load, as shown in Fig.. And no matter what technique is used for congestion control, the delay grows without bound as the load approaches the capacity of the system. It may be noted that initially there is longer delay when congestion control policy is applied. However, the network without any congestion control will saturate at a lower offered load



(a) Effect of congestion on throughput (b) Effect of congestion on delay

4.1 Congestion Control Techniques

Congestion control refers to the mechanisms and techniques used to control congestion and keep the traffic below the capacity of the network. As shown in Fig., the congestion control techniques can be broadly classified two broad categories:

• Open loop: Protocols to prevent or avoid congestion, ensuring that the system (or network under consideration) never enters a Congested State.

• Close loop: Protocols that allow system to enter congested state, detect it, and remove it

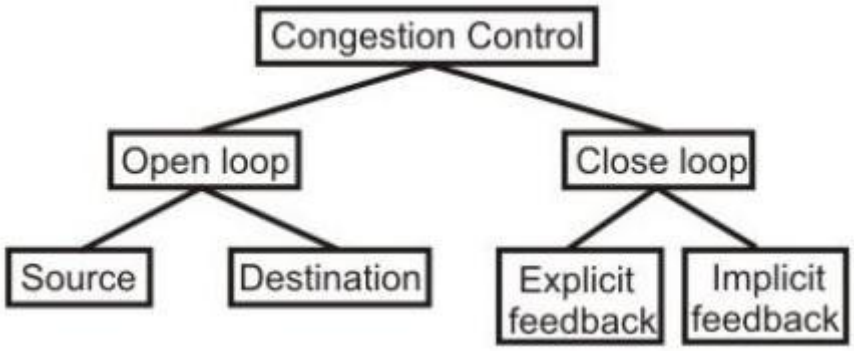


Figure 4.1 Congestion control categories

The first category of solutions or protocols attempt to solve the problem by a good design, at first, to make sure that it doesn't occur at all. Once system is up and running midcourse corrections are not made. These solutions are somewhat static in nature, as the policies to control congestion don't change much according to the current state of the system. SuchProtocols are also known as Open Loop solutions. These rules or policies include deciding uponwhen to accept traffic, when to discard it, making scheduling decisions and so on. Main point here is that they make decision without taking into consideration the current state of the network. The open loop algorithms are further divided on the basis of whether these acts on source versus that act upon destination. The second category is based on the concept of feedback. During operation, some system parameters are measured and feed back to portionsof the subnet that can take action to reduce the congestion. This approach can be divided into 3 steps:

• Monitor the system (network) to detect whether the network is congested or not and what's the actual location and devices involved.

• To pass this information to the places where actions can be taken

• Adjust the system operation to correct the problem.

These solutions are known as Closed Loop solutions. Various Metrics can be used to monitor the network for congestion. Some of them are: the average queue length, number of packetsthat are timed-out, average packet delay, number of packets discarded due to lack of buffer space, etc. A general feedback step would be, say a router, which detects the congestion send special packets to the source (responsible for the congestion) announcing the problem. These extra packets increase the load at that moment of time, but are necessary to bring down the congestion at a later time. Other approaches are also used at times to curtail down the congestion. For example, hosts or routers send out probe packets at regular intervals to explicitly ask about the congestion and source itself regulate its transmission rate, if congestion is detected in the network. This kind of approach is a pro-active one, as source tries to get knowledge about congestion in the network and act accordingly.

Yet another approach may be where instead of sending information back to the source an intermediate router which detects the congestion send the information about the congestion to rest of the network, piggy backed to the outgoing packets. This approach will in no way put an extra load on the network (by not sending any kind of special packet for feedback). Once the congestion has been detected and this information has been passed to a place where the actionneeded to be done, then there are two basic approaches that can overcome the problem. These are: either to increase the resources or to decrease the load. For example, separate dial-uplines or alternate links can be used to increase the bandwidth between two points, where congestion occurs. Another example could be to decrease the rate at which a particular senderin transmitting packets out into

the network. The closed loop algorithms can also be divided into two categories, namely explicit feedback and implicit feedback algorithms. In the explicit approach, special packets are sent back to the sources to curtail down the congestion. While in implicit approach, the source itself acts pro-actively and tries to deduce the existence of congestion by making local observations. In the following sections we shall discuss about some of the popular algorithms from the above categories.

4.2 Leaky Bucket Algorithm

Consider a Bucket with a small hole at the bottom, whatever may be the rate of water pouring into the bucket, the rate at which water comes out from that small hole is constant. This scenario is depicted in figure Once the bucket is full, any additional water entering it spills over the sides and is lost (i.e. it doesn't appear in the output stream through the hole underneath). The same idea of leaky bucket can be applied to packets, as shown in Fig. Conceptually each network interface contains a leaky bucket. And the following steps are performed:

• When the host has to send a packet, the packet is thrown into the bucket.

• The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

• Bursty traffic is converted to a uniform traffic by the leaky bucket.

• In practice the bucket is a finite queue that outputs at a finite rate. This arrangement can be simulated in the operating system or can be built into the hardware. Implementation of this algorithm is easy and consists of a finite queue. Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded.

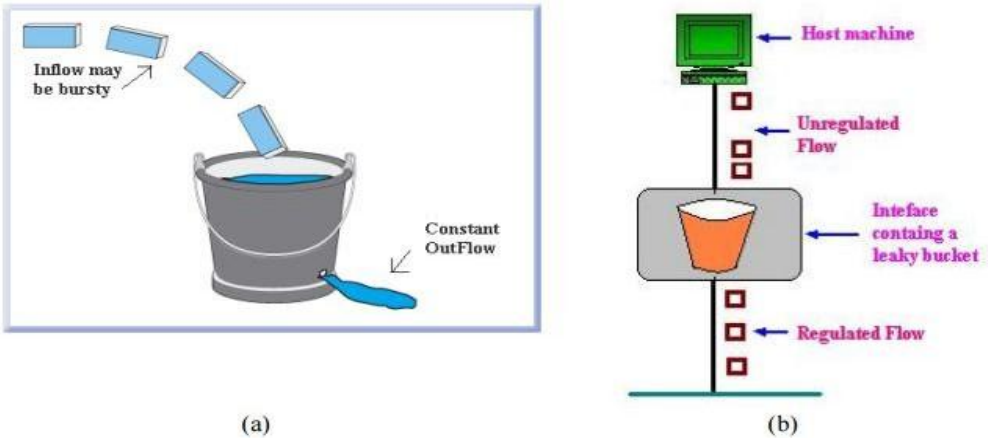


Figure 4.2 (a) Leaky bucket (b) Leaky bucket implementation

4.3 Token Bucket Algorithm

The leaky bucket algorithm described above, enforces a rigid pattern at the output stream, irrespective of the pattern of the input. For many applications it is better to allow the output to speed up somewhat when a larger burst arrives than to loose the data. Token Bucket algorithm provides such a solution. In this algorithm leaky bucket holds token, generated at regularintervals. Main steps of this algorithm can be described as follows: *ƒ* In regular intervals tokens are thrown into the bucket. *ƒ* The bucket has a maximum capacity. *ƒ* If there is a ready packet,a token is removed from the bucket, and the packet is send. *ƒ* If there is no token in the bucket, the packet cannot be send. Figure shows the two scenarios before and after the tokens present in the bucket have been consumed. In the bucket holds two tokens, and three packets are waiting to be sent out of the interface, in Fig. two packets have been sent out by consuming two tokens, and 1 packet is still left. The token bucket algorithm is less restrictive than the leaky bucket algorithm, in a sense that it allows bursty traffic. However, the limit of burst is restricted by the number of tokens available in the bucket at a particular instant of time. The implementation of basic token bucket algorithm is simple; a variable is used just to countthe tokens. This counter is incremented every t seconds and is decremented whenever a packetis sent. Whenever this counter reaches zero, no further packet is sent out as shown

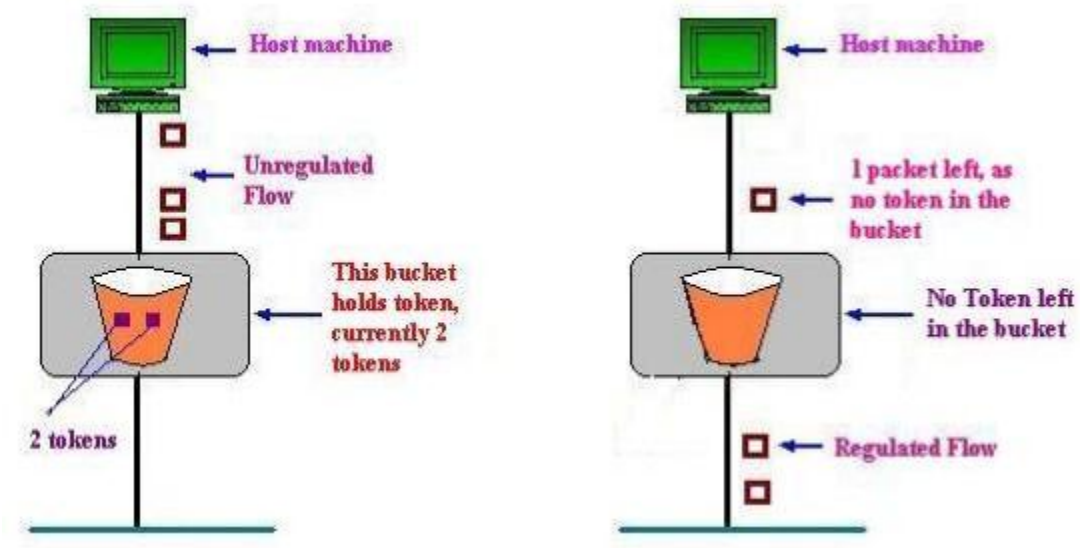


Fig 4.3.1 Token bucket holding two tokens, before packets are send out, (b) Token bucket after two packets are send, one packet still remains as no token is left

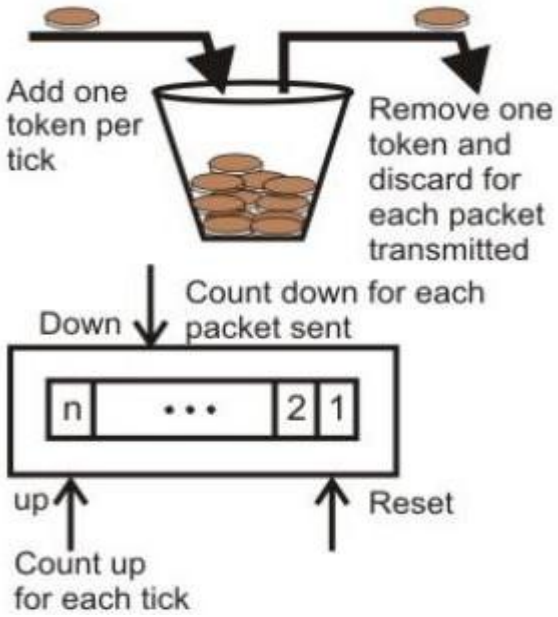


Figure 4.3.2 Implementation of Token bucket algorithm

Congestion control in virtual Circuit

Till now we have discussed two open loop algorithms, where the policy decisions are made in the beginning, irrespective of the current state. Both leaky bucket algorithm and token bucket algorithm are open loop algorithms.

In this section we shall have a look at how the congestion is tackled in a virtual circuit network. Admission control is one such closed-loop technique, where action is taken once congestion is detected in the network. Different approaches can be followed:

• Simpler one being: do not set-up new connections, once the congestion is signaled. This type of approach is often used in normal telephone networks. When the exchange is overloaded, then no new calls are established.

• Another approach, which can be followed is: to allow new virtual connections, but route these carefully so that none of the congested router (or none of the problem area) is a part of this route.

• Yet another approach can be: To negotiate different parameters between the host and the network, when the connection is setup. During the setup time itself, Host specifies the volume and shape of traffic, quality of service, maximum delay and other parameters, related to the traffic it would be offering to the network. Once the host specifies its requirement, the resources needed are reserved along the path, before the actual packet follows.

4.4 Choke Packet Technique

The choke packet technique, a closed loop control technique, can be applied in both virtual circuit and datagram subnets. Each router monitors its resources and the utilization at each ofits output line. There is a threshold set by the administrator, and whenever any of the resource utilization crosses this threshold and action is taken to curtail down this. Actually each outputline has a utilization associated with it, and whenever this utilization crosses the threshold, the output line enters a ―warning‖ state. If so, the router sends a choke packet back to the source, giving it a feedback to reduce the traffic. And the original packet is tagged (a bit is manipulatedin the header field) so that it will not generate other choke packets by other intermediate router, which comes in place and is forwarded in usual way. It means that the first router (along the wayof a packet), which detects any kind of congestion, is the only one that sends the choke packets. When the source host gets the choke packet, it is required to reduce down the traffic send out to that particular destination (choke packet contains the destination to which the original packet was send out). After receiving the choke packet the source reduces the traffic by a particular fixed percentage, and this percentage decreases as the subsequent choke packets are received. Figure depicts the functioning of choke packets. For Example, when source A receives a choke packet with destination B at first, it will curtail down the traffic to destination B by 50%, and if again after affixed duration of time interval it receives the choke packet again for the same destination, it will further curtail down the traffic by 25% more and so on. As stated above that a source will entertain another subsequent choke packet only after a fixed interval of time, not before that. The reason for this is that when the first choke packet arrives at that pointof time other packets destined to the same destination would also be there in the network and they will generate other choke packets too, the host should ignore these choke packets which refer to the same destination for a fixed time interval.

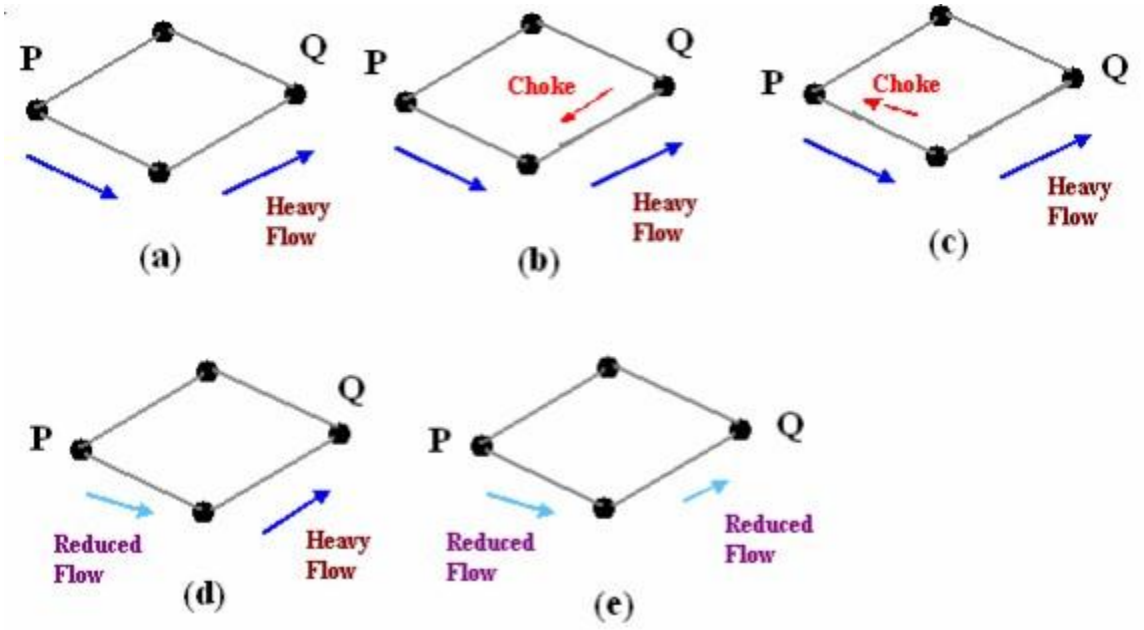


Figure 4.4 Depicts the functioning of choke packets, (a) Heavy traffic between nodes P and Q, (b) Node Q sends the Choke packet to P, (c) Choke packet reaches P, (d) P reduces the flow and send a reduced flow out, (e) Reduced flow reaches node Q

4.5 Hop-by Hop Choke Packets

This technique is an advancement over Choked packet method. At high speed over longdistances, sending a packet all the way back to the source doesn't help much, because by the time choke packet reach the source, already a lot of packets destined to the same original destination would be out from the source. So to help this, Hop-by-Hop Choke packets are used. In this approach, the choke packet affects each and every intermediate router through which it passes by. Here, as soon as choke packet reaches a router back to its path to the source, it curtails down the traffic between those intermediate routers. In this scenario, intermediate nodesmust dedicate few more buffers for the incoming traffic as the outflow through that node will be curtailed down immediately as choke packet arrives it, but the input traffic flow will only be curtailed down when choke packet reaches the node which is before it in the original path. This method is illustrated in Fig.. As compared to choke packet technique, hop-by-hop choke packet algorithm is able to restrict the flow rapidly. As can been seen from Figures and one-step reduction is seen in controlling the traffic, this single step advantage is because in our example there is only one intermediate router. Hence, in a more complicated network, one can achieve a significant advantage by using hop-by-hop choke packet method.

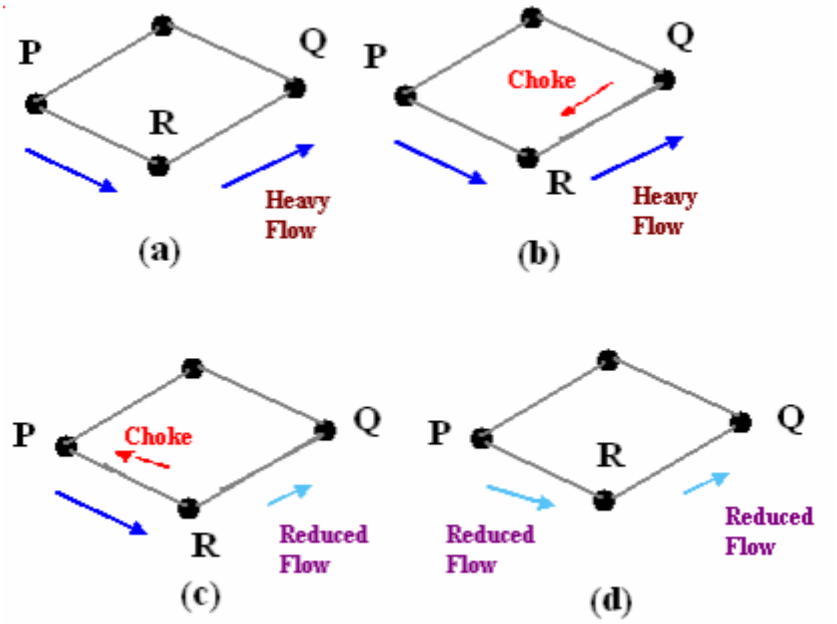


Figure 4.5 Depicts the functioning of Hop-by-Hop choke packets, (a) Heavy traffic between nodes P and Q, (b) Node Q sends the Choke packet to P, (c) Choke packet reaches R, and the flow between R and Q is curtail down, Choke packer reaches P, and P reduces the flow out

Load Shedding

Another simple closed loop technique is Load Shedding; it is one of the simplest and more effective techniques. In this method, whenever a router finds that there is congestion in the network, it simply starts dropping out the packets. There are different methods by which a host can find out which packets to drop. Simplest way can be just choose the packets randomly which has to be dropped. More effective ways are there but they require some kind of cooperation from the sender too. For many applications, some packets are more important than others. So, sender can mark the packets in priority classes to indicate how important they are. If such a priority policy is implemented than intermediate nodes can drop packets from the lower priority classes and use the available bandwidth for the more important packets.

Slow Start - a Pro-active technique

This is one of the pro-active techniques, which is used to avoid congestion. In the original implementation of TCP, as soon as a connection was established between two devices, they could each go ―hog wild‖, sending segments as fast as they liked as long as there was room in the other devices receive window. In a busy internet, the sudden appearance of a large amount of new traffic could aggravate any existing congestion. To alleviate this, modern TCP devices are restrained in

the rate at which they initially send segments. Each sender is at first restricted to sending only an amount of data equal to one ―full-sized‖ segment——that is, equal to the MSS (maximum segment size) value for the connection. Each time an acknowledgment is received, the amount of data the device can send is increased by the size of another full-sized segment. Thus, the device ―starts slow‖ in terms of how much data it can send, with the amount it sends

increasing until either the full window size is reached or congestion is detected on the link. In the latter case, the congestion avoidance feature is used. When potential congestion is detected on a TCP link, a device responds by throttling back the rate at which it sends segments. A special algorithm is used that allows the device to drop the rate at which segments are sent quickly when congestion occurs. The device then uses the Slow Start algorithm just above to gradually increase the transmission rate back up again to try to maximize throughput without congestion occurring again.

Flow Control versus Congestion control

Flow control is a very important part of regulating the transmission of data between devices, but it is limited in a way that it only considers what is going on within each of the devices on the connection, and not what is happening in devices between them. It relates to the point-point traffic between a given sender and a receiver. Flow control always involves some kind of feedback from receiver to sender to tell sender how things are at other end of the network. Since we are dealing with how TCP works between a typical server and client at layer four, we don't worry about how data gets between them; that's the job of the Internet Protocol at layer three. In practice, what is going on at layer three can be quite important. Considered from an abstract point of view, our server and client may be connected ―directly‖ using TCP, but all the packets we transmit are carried across an internet and routers between different networks. These networks and routers are also carrying data from many other connections and higher- layer protocols. If the internet becomes very busy, the speed at which segments are carried between the endpoints of our connection will be reduced, and they could even be dropped. This is called congestion control. Congestion control has to do with making sure that subnet carry theoffered traffic. It is the global issue, involving the behavior of all the hosts, router, link, store and forward mechanism between them in the entire subnet or internet

4.6 Quality of Service

Requirements • Techniques for Achieving Good Quality of Service • Integrated Services • Differentiated Services • Label Switching and MPLS

Requirements

How stringent the quality-of-service requirements are

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Table 4.6.1

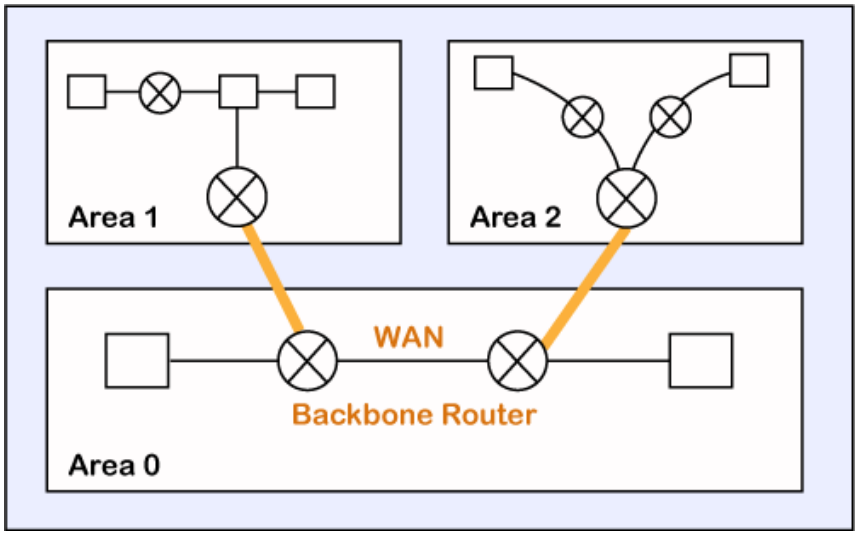
Techniques for Good QoS

- Over provisioning
- Buffering
- Traffic shaping
- The leak bucket algorithm
- Token bucket algorithm
- Resource reservation
- Admission control
- Proportional routing
- Packet scheduling

OSPF Protocol:

The OSPF stands for **Open Shortest Path First**.
It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network.
It is an interior gateway protocol that has been designed within a single autonomous system.
These LSAs contain information about every router, subnet, and other networking information.
Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB.
The main goal is to have the same information about every router in an LSDBs.

OSPF Areas:



Types of links in OSPF:

A link is basically a connection, so the connection between two routers is known as a link.

There are four types of links in OSPF:

1. ***Point-to-point link:*** The point-to-point link directly connects the two routers without any host or router in between.
2. ***Transient link:*** When several routers are attached in a network, they are known as a transient link.
   The transient link has two different implementations:
   Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.
   Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.
3. ***Stub link:*** It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.
4. ***Virtual link:*** If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

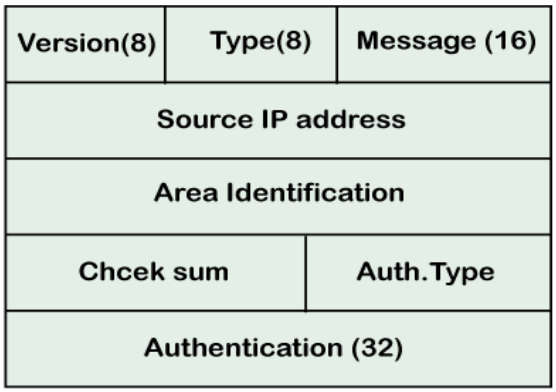
OSPF States

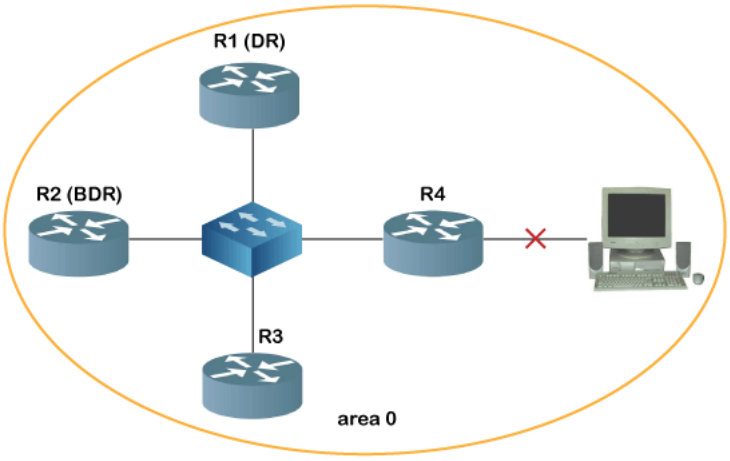
The device running the OSPF protocol undergoes the following states:

- **Down:** If the device is in a down state, it has not received the HELLO packet. Here, down does not mean that the device is physically down; it means that the OSPF process has not been started yet.
- **Init:** If the device comes in an init state, it means that the device has received the HELLO packet from the other router.
- **2WAY:** If the device is in a 2WAY state, which means that both the routers have received the HELLO packet from the other router, and the connection gets established between the routers.
- **Exstart:** Once the exchange between the routers get started, both the routers move to the Exstart state. In this state, master and slave are selected based on the router's id. The master controls the sequence of numbers, and starts the exchange process.
- **Exchange:** In the exchange state, both the routers send a list of LSAs to each other that contain a database description.
- **Loading:** On the loading state, the LSR, LSU, and LSA are exchanged.
- **Full:** Once the exchange of the LSAs is completed, the routers move to the full state.

OSPF Message Format

The following are the fields in an OSPF message format:





Example.

R1 is chosen as the DR, while R2 is chosen as the BDR as R1 has the highest router ID, whereas the R2 has the second-highest router ID. If the link fails between R4 and the system, then R4 updates only R1 and R4 about its link failure. Then, DR updates all the non-DR and non-BDR about the change, and in this case, except R4, only R3 is available as a non-DR and non-BDR.

Border Gateway Protocol:

It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

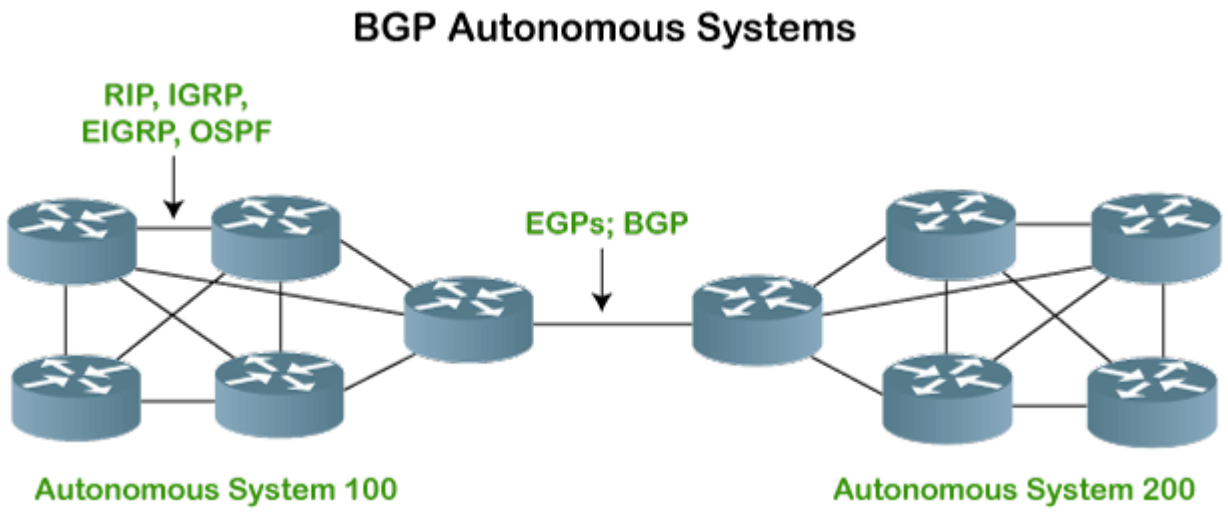
As we know that Border Gateway Protocol works on different autonomous systems, so we should know the history of BGP, types of autonomous systems, etc.

There are many versions of BGP, such as:

- BGP version 1: This version was released in 1989 and is defined in RFC 1105.
- BGP version 2: It was defined in RFC 1163.

- BGP version 3: It was defined in RFC 1267.
- BGP version 4: It is the current version of BGP defined in RFC 1771.

BGP Autonomous Systems



Multi-Protocol Label Switching (MPLS):

Multiprotocol Label Switching (MPLS) is a routing technique that augments speed and control of the network traffic by directing data from one node to the next node based on short path labels.

Instead of being routed using long network addresses, the data packets are routed through path labels that identify virtual paths between the nodes rather than endpoints.

MPLS is a scalable and protocol-independent routing technique. It works with Internet Protocol (IP), Ethernet, Frame Relay and Asynchronous Transport Mode (ATM).

Despite the advent of newer technologies, it remains relevant due to its features like security, flexibility and traffic engineering.

Working Principle

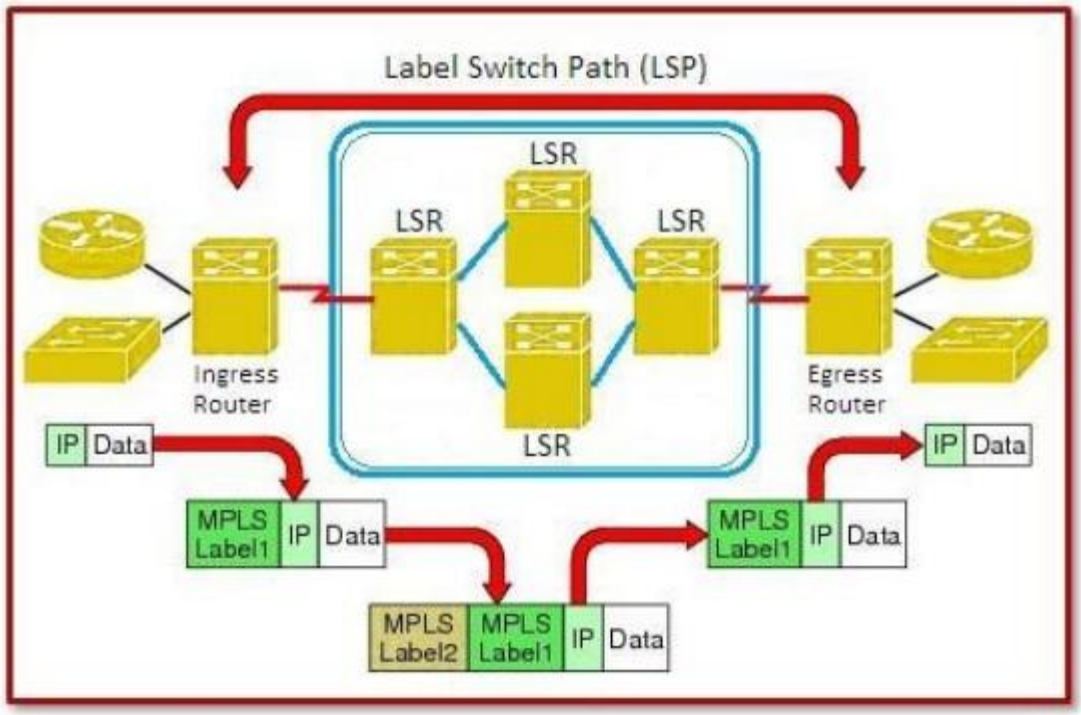
MPLS works by prefixing 32-bit labels with the MPLS header. The 32-bit label contains four fields −

- Label value field of 20-bits
- Traffic class field of 3-bits for QoS (quality of service)
- Bottom of stack flag of 1-bit (1 value denotes that the current label is the last one in the stack)
- TTL (time to live) field of 8-bits

When an IP packet enters the MPLS network, the 32-bit MPLS label is added by the ingress router, which is a label edge router (LER). LER decides the virtual path called label-switched path (LSP) that the packet will follow until it reaches its destination.

The subsequent label-switching routers (LSRs) along the LSP, forwards the packet based upon only the MPLS labels. They do not look beyond the MPLS label to the IP header.

When the packet reaches the egress router (also an LER), the MPLS labels are removed and the original IP packet is forwarded towards the final destination. The mechanism is depicted in the following diagram −



Distance Vector Routing Algorithm

- ***The Distance vector algorithm is iterative, asynchronous and distributed.***
    - ***Distributed:*** It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
    - ***Iterative*****:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
    - ***Asynchronous*****:** It does not require that all of its nodes operate in the lock step with each other.
- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as **Vector**.
- Three Keys to understand the working of Distance Vector Routing Algorithm:
- ***Knowledge about the whole network:*** Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.
- ***Routing only to neighbors*****:** The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.
- ***Information sharing at regular intervals:*** Within 30 seconds, the router sends the information to the neighboring routers.
- Let $d_x(y)$ be the cost of the least-cost path from node x to node y. The least costs are related by Bellman-Ford equation,
- $d_x(y) = \min_v\{c(x,v) + d_v(y)\}$
- **Where** the minv is the equation taken for all x neighbors. After traveling from x to v, if we consider the least-cost path from v to y, the path cost will be $c(x,v)+d_v(y)$. The least cost from x to y is the minimum of $c(x,v)+d_v(y)$ taken over all neighbors.
- **With the Distance Vector Routing algorithm, the node x contains the following routing information:**

    - For each neighbor v, the cost c(x,v) is the path cost from x to directly attached neighbor, v.
    - The distance vector x, i.e., $D_x = [\ D_x(y) : y \text{ in } N\ ]$, containing its cost to all destinations, y, in N.

TEXT / REFERENCE BOOKS:

1. William Stallings, Data and Computer Communications, 10th Edition, Pearson, 2014.

2. Wayne Thomasi, "Advanced Electronic Communication Systems", 6th Edition, PHI Publishers, 2003.

3. Simon Haykins, “Communication Systems” John Wiley, 5th Edition, March 2009.

4. John G. Proakis, MasoudSalehi, “Digital Communication”, McGraw Hill 5th edition November 6, 2007.

5. Bernard Sklar, “Digital Communication, Fundamentals and Application”, Pearson Education Asia, 2nd

Edition, Jan. 21, 2001.

6. Behrouz A. Forouzen, “Data communication and Networking”, Fourth Edition, Tata McGraw – Hill, 2011.

7. Andrew S.Tanenbaum, “Computer Networks”, 5th Edition, Pearson, 2011.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ECE

UNIT V TRANSPORT, SESSION AND APPLICATION LAYER

UNIT 5 TRANSPORT, SESSION AMD APPLICATION *LAYER*

Transport Layer UDP, TCP, Congestion Control & Quality of Service Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics, Application Layer DNS, Remote Logging (Telnet), SMTP, FTP, WWW, HTTP, POP3, MIME, SNMP.

Transport protocol

- In computer networking, the transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack in the Internet Protocol Suite and the Open Systems Interconnection (OSI). The protocols of the layer provide host-to-host communication services for applications.[1] It provides services such as connection-oriented data stream support, reliability, flow control, and multiplexing.
- The details of implementation and semantics of the Transport Layer of the TCP/IP model (RFC 1122),[2] which is the foundation of the Internet, and the Open Systems Interconnection (OSI) model of general networking, are different. In the OSI model the transport layer is most often referred to as Layer 4 or L4, while numbered layers are not used in TCP/IP.
- The best-known transport protocol of TCP/IP is the Transmission Control Protocol (TCP), and lent its name to the title of the entire suite. It is used for connection- oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions. TCP is the more complex protocol, due to its stateful design incorporating reliable transmission and data stream services. Other prominent protocols in this group are the Datagram Congestion Control Protocol (DCCP) and the Stream Control Transmission Protocol (SCTP).

Transport Service

Transport layer services are conveyed to an application via a programming interface to the transport layer protocols. The services may include the following features:

- Connection-oriented communication: It is normally easier for an application to interpret a connection as a data stream rather than having to deal with the underlying connection- less models, such as the datagram model of the User Datagram Protocol (UDP) and of the Internet Protocol (IP).
- Same order delivery: The network layer doesn't generally guarantee that packets of data will arrive in the same order that they were sent, but often this is a desirable feature. This is usually done through the use of segment numbering, with the receiver passing them to the application in order. This can cause head-of-line blocking.
- Reliability: Packets may be lost during transport due to network congestion and errors. By means of an error detection code, such as a checksum, the transport protocol may check that the data is not corrupted, and verify correct receipt by sending an ACK or NACK message to the sender. Automatic repeat request schemes may be used to

retransmit lost or corrupted data.

- Flow control: The rate of data transmission between two nodes must sometimes be managed to prevent a fast sender from transmitting more data than can be supported by the receiving data buffer, causing a buffer overrun. This can also be used to improve efficiency by reducing buffer under run.
- Congestion avoidance: Congestion control can control traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. For example, automatic repeat requests may keep the network in a congested state; this situation can be avoided by adding congestion avoidance to the flow control, including slow-start. This keeps the bandwidth consumption at a low level in the beginning of the transmission, or after packet retransmission.
- Multiplexing: Ports can provide multiple endpoints on a single node. For example, the name on a postal address is a kind of multiplexing, and distinguishes between different recipients of the same location. Computer applications will each listen for information on their own ports, which enables the use of more than one network service at the same time. It is part of the transport layer in the TCP/IP model, but of the session layer in the OSI model.

- The transport layer is responsible for delivering data to the appropriate applicationprocess on the host computers. This involves statistical multiplexing of data from different application processes, i.e. forming data packets, and adding source and destination port numbers in the header of each transport layer data packet. Together with the source and destination IP address, the port numbers constitutes a network socket, i.e. an identification address of the process-to-process communication. In the OSI model, this function is supported by the session layer.
- Some transport layer protocols, for example TCP, but not UDP, support virtual circuits, i.e. provide connection oriented communication over an underlying packet oriented datagram network. A byte-stream is delivered while hiding the packet mode communication for the application processes. This involves connection establishment, dividing of the data stream into packets called segments, segment numbering and reordering of out-of order data.

  Finally, some transport layer protocols, for example TCP, but not UDP, provide end-to-end reliable communication, i.e. error recovery by means of error detecting code and automatic repeat request (ARQ) protocol. The ARQ protocol also provides flow control, which may be combined with congestion avoidance.

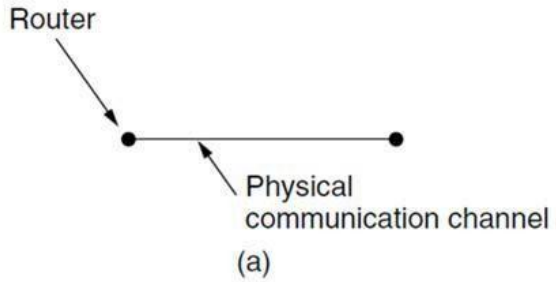
- UDP is a very simple protocol, and does not provide virtual circuits, nor reliable communication, delegating these functions to the application program. UDP packets are called datagrams, rather than segments.
- TCP is used for many protocols, including HTTP web browsing and email transfer. UDP may be used for multicasting and broadcasting, since retransmissions are not possible to

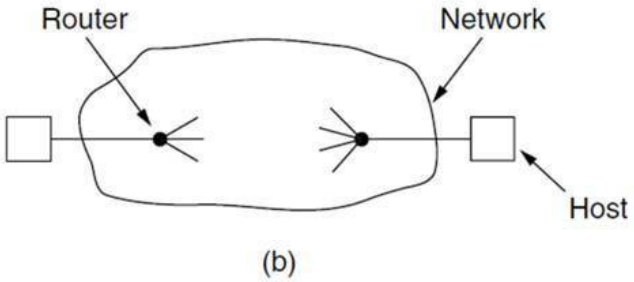
a large amount of hosts. UDP typically gives higher throughput and shorter latency, and is therefore often used for real-time multimedia communication where packet loss occasionally can be accepted, for example IP-TV and IP-telephony, and for online computer games.

- Many non-IP-based networks, such as X.25, Frame Relay and ATM, implement the connection-oriented communication at the network or data link layer rather than the transport layer. In X.25, in telephone network modems and in wireless communication systems, reliable node-to-node communication is implemented at lower protocol layers.
- The OSI connection-mode transport layer protocol specification defines five classes of transport protocols: TP0, providing the least error recovery, to TP4, which is designed for less reliable networks.

Elements of transport protocol

- Transport protocol similar to data link protocols
- Both do error control and flow control
- However, significant differences exist



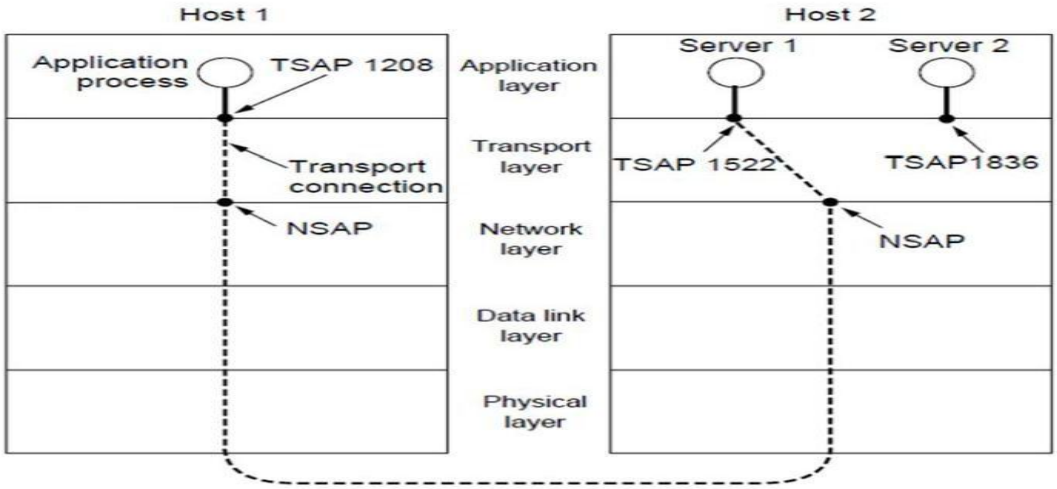


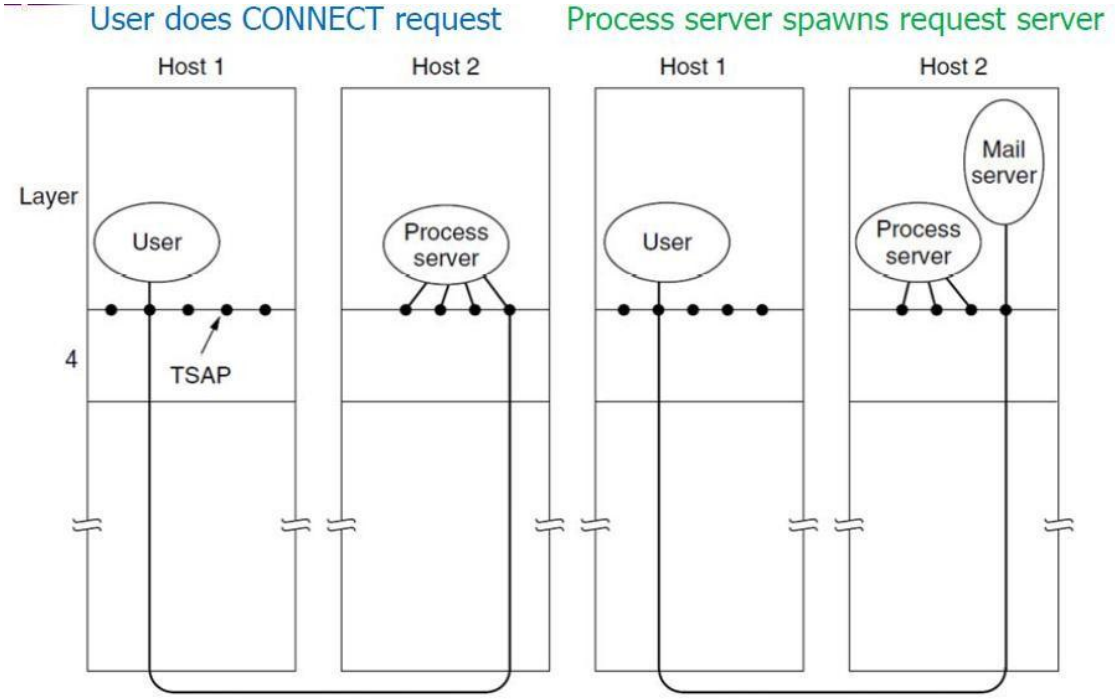
Environment of the data link layer

Environment of the transport layer

Addressing

- Specify which host process to connect to
- TSAP: Transport Service Access Point
- In TCP, UDP, called ports
- Analogy: NSAP. Example: IP address
- Client or server app attaches to TSAP
- Connections run through NSAP
- TSAP to distinguish endpoints sharing NSAP


Host 1
Host 2
Application process
TSAP 1208
Transport connection
NSAP
Application layer
Transport layer
Network layer
Data link layer
Physical layer
Server 1
Server 2
TSAP 1522
TSAP1836
NSAP


User does CONNECT request
Process server spawns request server
Host 1
Host 2
Host 1
Host 2
Layer
User
Process server
User
Process server
Mail server
4
TSAP

Connection Establishment

- Sounds easy; surprisingly tricky!
- Just send REQUEST, wait for
- ACCEPTED?Can lose, delay, corrupt,
- duplicate packets Duplicate may transfer
- bank money again! Protocols must work
- correct all cases Implemented efficiently in
- common cases Main problem is delayed duplicates

  Cannot prevent; must deal with (reject)

Solutions for delayed duplicates

- Not reuse transport address (TSAP)
- difficult to connect to process
- Give each connection unique ID
- seq # chosen by initiating party
- update table listing obsolete connections
- check new connections against table
- requires maintain certain amount of history

  if machine crashes, no longer identify old con

- To simplify problem, restrict packet lifetime
- restricted network design: prevent looping
- hop counter in each packet: - 1 at each hop
- timestamp in each packet: clock must be synced
- Must also guarantee ACKs are dead
- Assume a value T of max packet lifetime
- T sec after packet sent, sure traces are gone
- In the Internet, T is usually 120 seconds.

New method with packet lifetime bounded

- Label segments with seq # not reused in T
- T and packet rate determine size of seq #s 1
- packet w given seq # may be outstanding
- Duplicates may still occur, but discarded dst
- Not possible to have delayed duplicate old packet with same seq # accepted at dest

How to deal with losing memory after crash?

- Each host has time- of- day clock
- clocks at different host need not be synced
- binary counter increments uniform intervals
- no. of bits must be ≥ of seq #
- clock must be running even if host goes down
- Initial seq # (k- bits) ← low k- bits of
- clock Seq space must be so large
- by time # wrap, old pkts w same # are long gone

Clock method work within connection

- Host don't remember # across connections
- Can't know if CONN REQUEST with initial

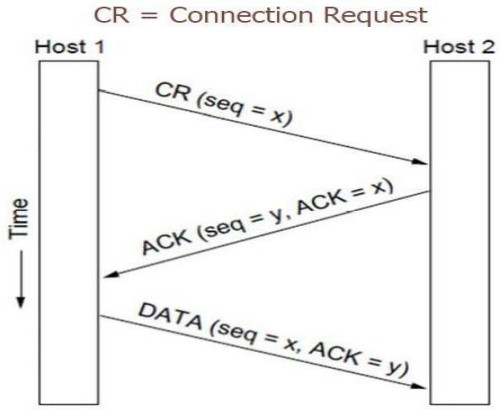
seq # is a duplicate of a recent connection

- To solve this, use three- way
- handshake
- Check with other peer that con req is current
- Used in TCP, with 32- bit seq #

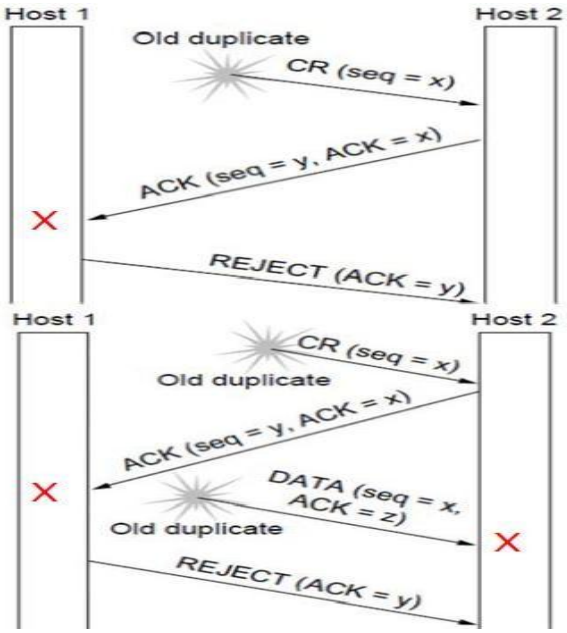
Clock not used in TCP; attacker can predict

Normal Procedure

- H1 choses initial s# x
- H2 replies
- ACKs x
- announce own s# y
- H1replies
- ACKs y
- with 1st data segment

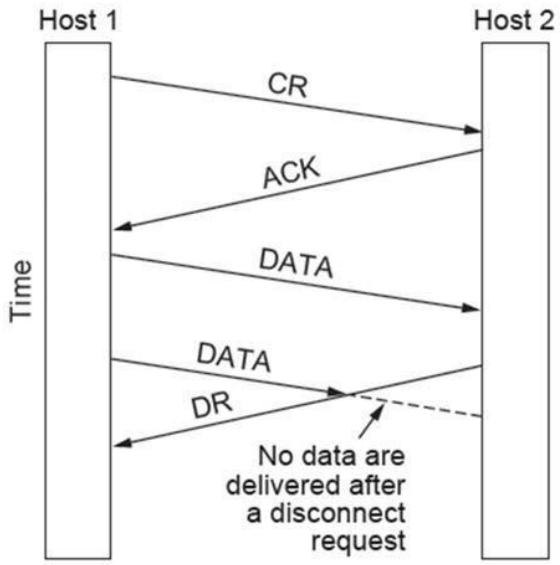


Abnormal situations
 Delayed duplicate CR
 H2 sends ACK to H1
 H1 rejects
 H2 knows it was tricked16
 Worst case
DD CR, old ACK floating
 H2 gets delayed CR, replies
 H1 rejects
 H2 gets old DATA, discards(z received instead of y)



Connection Release

- Easier than establish
- However, some pitfalls
- Asymmetric release
- each con term separately
- abrupt; may cause data loss
- better protocol needed



Symmetric release

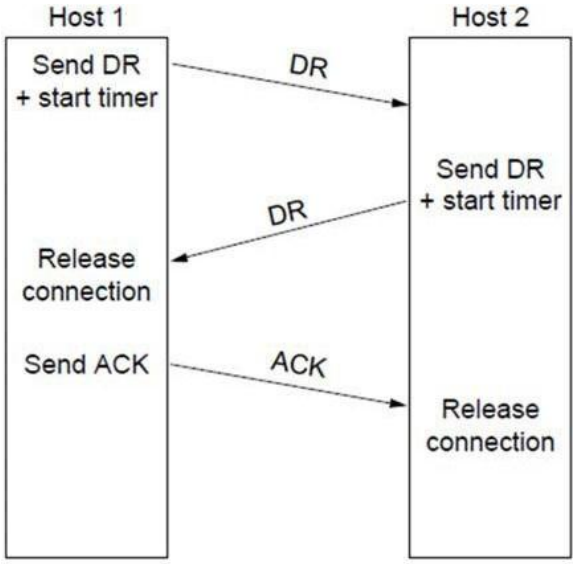
- Each direction is released independently
- Can receive data after sending DISCONNECT
- H1: I am done, are you done too?
- H2: I am done too, goodbye
- Two- army problem: unreliable channel

- Two army problem

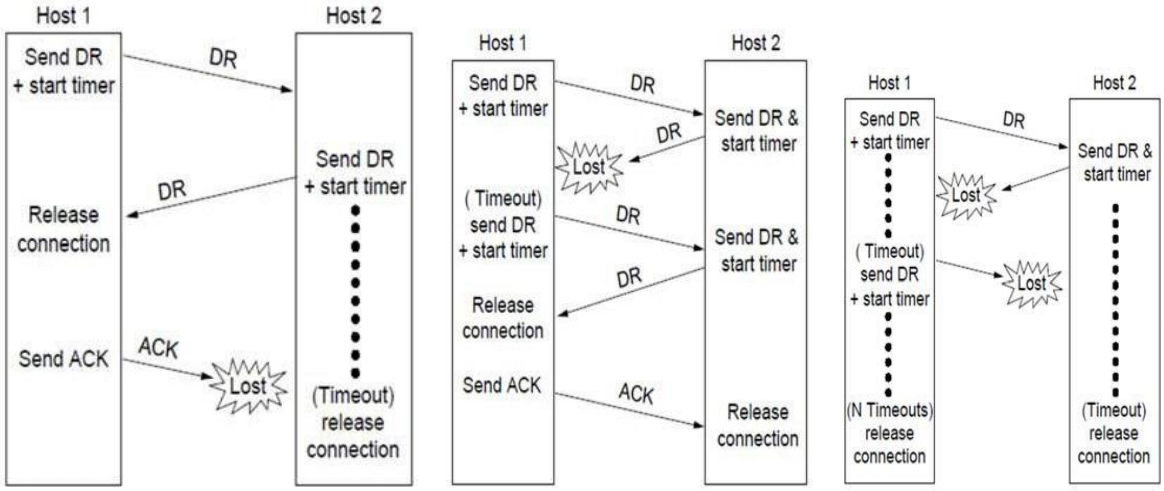
- each blue army < white army, but together are larger
- need to sync attack
- however, only com channel is the valley
- (unreliable)3- way handshake? B1 can't know
- ACK arrived making 4- way handshake doesn't
- help either

Let each side independently decide its done
Easier to solve

Normal release sequence H1
- send DR, start timer H2
- responds with DR when
- H1 recv DR, release
- when H2 recv ACK, release



Error cases, handled by timers, retransmissions



Final ACK lost:
Many lost DRs
Host 2 times out

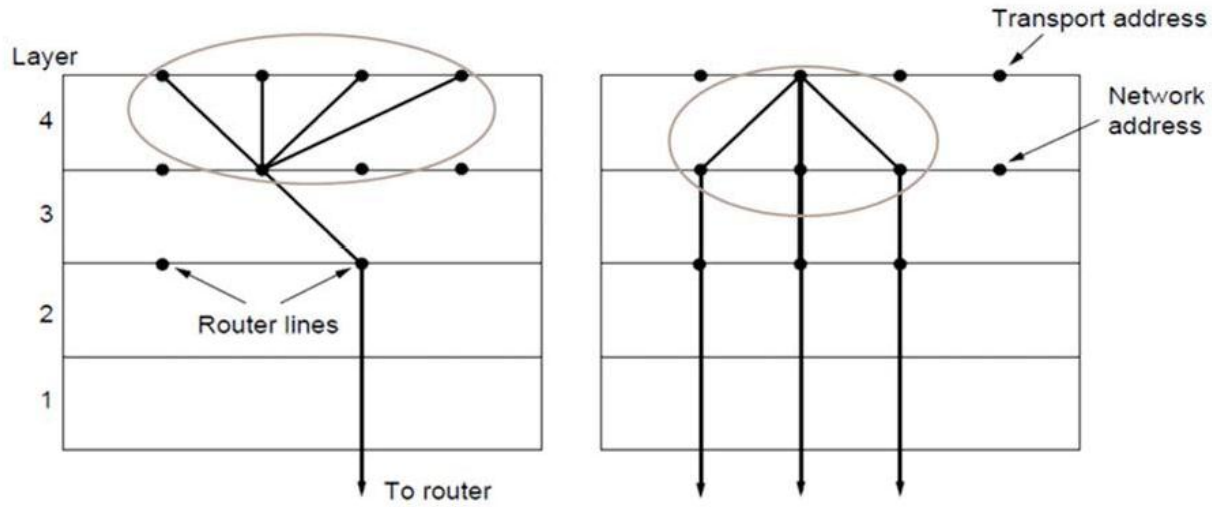
Lost DR:H1 starts over

Extreme:
both release after N

- Protocol usually suffices; can fail in theory
- after N lost attempts; half open connection
- Not allowing give up, can go on forever
- To kill half open connections, automatically disconnect if no received segments in X sec
- Must have timer reset after each segment
- Send dummy segments to keep con alive TCP
- normally does symmetric close, with each side independently close ½ con w FIN

Multiplexing

- Transport, network sharing can either be:
- Multiplexing: connections share a network address
- Inverse multiplexing: addresses share a connection



Domain Name System (DNS)

The Domain Name System (DNS) provides translation between symbolic names and IPaddresses

Structure of DNS names

Each name consists of a sequence of alphanumeric components separated by periods

Examples:

www.eg.bucknell.edu

www.netbook.cs.purdue.edu

charcoal.eg.bucknell.edu

Names are hierarchical, with most-significant component on the right

Left-most component is computer name top level domains (right-most components; also knownas TLDs) defined by global authority

Domain Name	Assigned To
com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military group
net	Major network support center
org	Organization other than those above
arpa	Temporary ARPA domain (still used)
int	International organization
country code	A country

Organizations apply for names in a top-level

domain:bucknell.edu

macdonalds.com

Organizations determine own internal structure

eg.bucknell.

edu

cs.purdue.ed

u

Geographic structure

Top-level domains are US-centric

Geographic TLDs used for organizations in other countries:

TL D | Country

.uk	United Kingdom
.fr	France
.ch	Switzerland
.in	India

Countries define their own internal hierarchy: ac.uk and .edu.au are used for academicorganizations in the United Kingdom and Australia

Domain names within an organization

Uniqueness of TLD and organization name guarantee uniqueness of any internal name (muchlike file names in your directories)

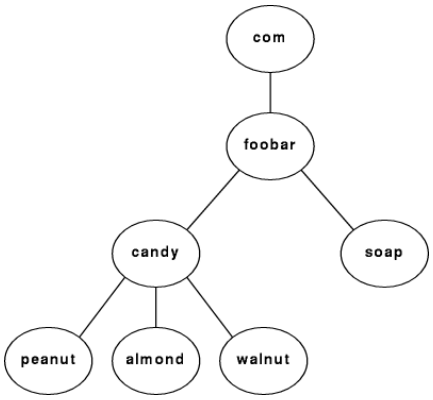
All but the left-most component of a domain name is called the domain for that name:

Name	Domain
www.netbook.cs.purdue.edu	netbook.cs.purdue.edu
regulus.eg.bucknell.edu	eg.bucknell.edu
coral.bucknell.edu	bucknell.edu

Authority for creating new subdomains is delegated to each domain

Administrator of bucknell.edu has authority to create eg.bucknell.edu and need not contact anycentral naming authority

Example DNS hierarchy



DNS domains are logical concepts and need not correspond to physical location oforganizations

DNS domain for an organization can span multiple

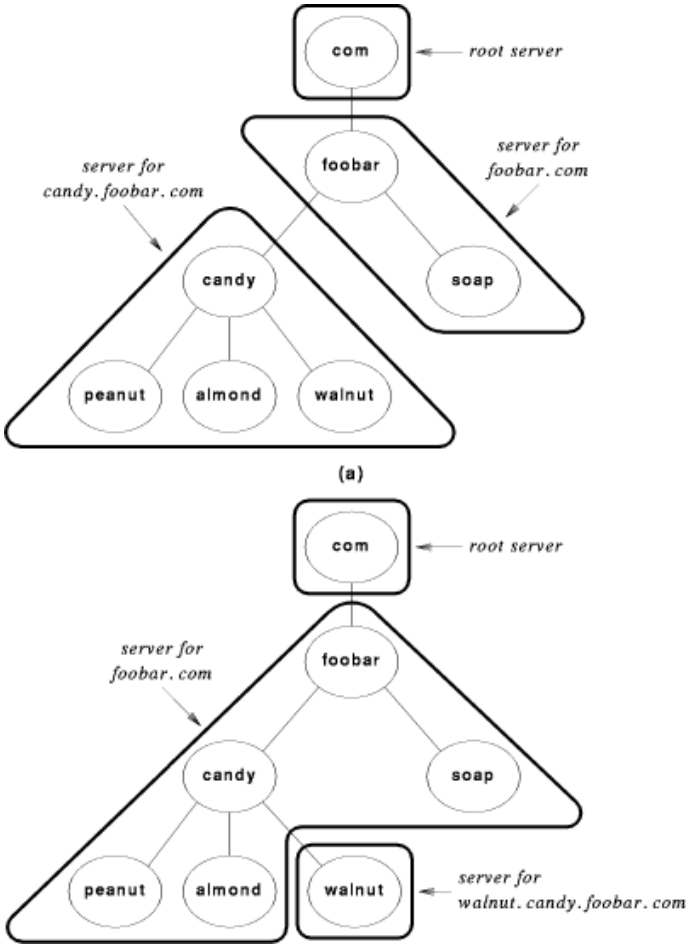
networksbucknell.edu covers all networks at Bucknell

www.netbook.cs.purdue.edu is in 318 Dana

laptop.eg.bucknell.edu could be connected to a network in California

DNS and client-server computing

- DNS names are managed by a hierarchy of DNS servers
- Hierarchy is related to DNS domain hierarchy



- Root server at top of tree knows about next level servers
- Next level servers, in turn, know about lower level

serversChoosing DNS server architecture

- Small organizations can use a single server
  - Easy to administer
  - Inexpensive
- Large organizations often use multiple servers
  - Reliability through redundancy
  - Improved response time through load-sharing
  - Delegation of naming authority
- Locality of reference applies - users will most often look up names of computers withinsame organization

Name resolution

Resolver software typically available as library procedures

- Implement DNS application protocol
- Configured for local servers
- Example - UNIX gethostbyname

- Calling program is *client*
  - Constructs DNS protocol message - a *DNS request*
  - Sends message to local DNS server

- DNS *server* resolves name
  - Constructs DNS protocol message - a *DNS reply*
  - Sends message to client program and waits for next request
    - DNS messages
    - DNS request contains name to be resolved
    - DNS reply contains IP address for the name in the request
    - Using DNS servers
    - DNS request is forwarded to root server, which points at next server to use
    - Eventually, authoritative server is located and IP address is returned
    - DNS server hierarchy traversal is called iterative resolution
    - Applications use recursive iteration and ask DNS server to handle traversal

DNS caching

- DNS resolution can be very inefficient
- Every host referenced by name triggers a DNS request
- Every DNS request for the address of a host in a different organization goesthrough the root server
- Servers and hosts use caching to reduce the number of DNS requests
- Cache is a list of recently resolved names and IP addresses
- Authoritative server include time-to-live with each reply

Electronic mail

- Many user applications use client-server architecture
- Electronic mail client accepts mail from user and delivers to server on destinationcomputer
- Many variations and styles of delivery

- Many user applications use client-server architecture
- Electronic mail client accepts mail from user and delivers to server on destinationcomputer
- Many variations and styles of delivery

- E-mail users have an electronic mailbox into which incoming mail is deposited. User then accesses mail with a mail reader program. Usually associated with computer account; one user may have a different electronic mailboxes. Electronic mailbox is identified by an e-mail address.Typically user's account ID, although not always .On non-networked multi-user computer, e-mail address is just account ID (no need to identify computer)

Networked e-mail addresses

- Mail delivery among networked computers is more complicated
- Must identify computer as well as mailbox
- Syntactically, e-mail address is composed of computer name and mailbox name
- Common example - user@host
- Other:
  - host1!host2!host!user
  - host%user

- User portion is site-specific
  - droms
  - Ralph_E._Droms
  - 578.4309
- Host portion is domain name
- Source mail client
  - Resolves destination name using DNS (MX, if available)
  - Contacts mail delivery server at destination
  - Copies mail to server
- Destination mail server
  - Interprets user name according to local mailbox addresses
  - Places mail in appropriate mailbox
- Simple two-part format:
  - Header includes delivery information
  - Body carries text of message
- Header and body separated by blank line
- Lines of text in format keyword: information
- keyword identifies information; information can appear in any order
- Essential information:
  - To: list of recipients
  - From: sender
  - Cc: list of copy recipients
- Useful information:
  - Reply-to: different address than From:
  - Received-by: for debugging
- Frivolous information:

    - Favorite-drink: lemonade
    - Phase-of-the-moon: gibbous
- Mail software passes unknown headers unchanged.Some software may interpret vendor-specific information.Original Internet mail carried only 7-bit ASCII data.Couldn't
  contain arbitrary binary values; e.g., executable program.Techniques for encoding binarydata allowed transport of binary data
- uuencode: 3 8-bit binary values as 4 ASCII characters (6 bits each)
    - Also carries file name and protection information
    - Incurs 33% overhead
    - Requires manual intervention

5.1 Mail transfer

- E-mail communication is really a two-part process:
- User composes mail with an e-mail interface program
- Mail transfer program delivers mail to destination
- Waits for mail to be placed in outgoing message queues
- Picks up message and determines recipient(s)
- Becomes client and contacts server on recipient's computer
- Passes message to server for delivery

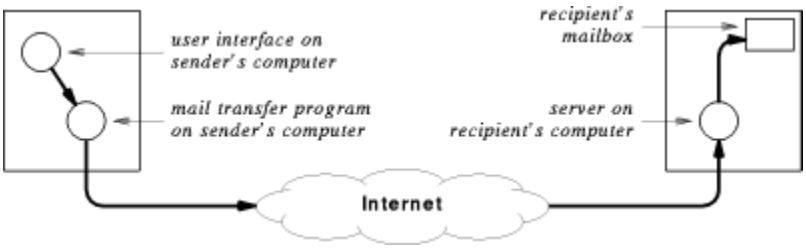


Figure 5.1 Mail Transfer

5.2 World wide Web (WWW)

The World Wide Web (**WWW**) can be viewed as a huge distributed system consisting of millions of clients and servers for accessing linked documents. Servers maintain collections of documents, while clients provide users an easyto- use interface for presenting and accessing those documents. The Web started as a project at CERN, the European Particle Physics Laboratory in Geneva, to let its large and geographically dispersed group of researchers provide access to shared documents using a simple hypertext system. A document could be anything that could be displayed on a user's computer terminal, such as personal notes, reports, figures, blueprints, drawings, and so on. By linking documents to each other, it became easy to integrate documents from different projects into a new document without the necessity for centralized changes. The only thing needed was to construct a document providing links to other relevant documents (see also Berners-Lee et al., 1994). The Web gradually grew worldwide encompassing sites other than high energy physics, but popularity really increased when graphical user interfaces became available, notably Mosaic (Vetter et al., 1994). Mosaic provided an easy-to-use interface to present and access documents by merely clicking the mouse. A document was fetched from a server, transferred to a client, and presented on the screen. To a user, there was conceptually no difference between a document stored locally or inanother part of the world. In this sense, distribution was transparent. Since 1994, Web developments are primarily initiated and controlled by the World Wide Web Consortium, a collaboration between CERN and M.I.T. This consortium is responsible for standardizing protocols, improving interoperability, and further enhancing the capabilities of the Web. Its homepage can be found at http://www.w3.org/.

The WWW is essentially a huge client-server system with millions of servers distributed worldwide. Each server maintains a collection of documents; each document is stored as a file (although documents can also be generated on request). A server accepts requests for fetchinga document and transfers it to the
client. In addition, it can also accept requests for storing new documents. The simplest way torefer to a document is by means of a reference called a Uniform Resource Locator (URL). A URL is comparable to an IOR in CORBA and a contact address in Globe. It specifies where adocument is located, often by
embedding the DNS name of its associated server along with a file name by which the server can look up the document in its local file system. Furthermore, a URL specifies the application- level protocol for transferring the document across the network. There are different protocols available, as we explain below. A client interacts with Web servers through a special applicationknown as a browser. A browser is responsible for properly displaying a document. Also, a browser accepts input from a user mostly by letting the user select a reference to another document, which it then subsequently fetches and displays.

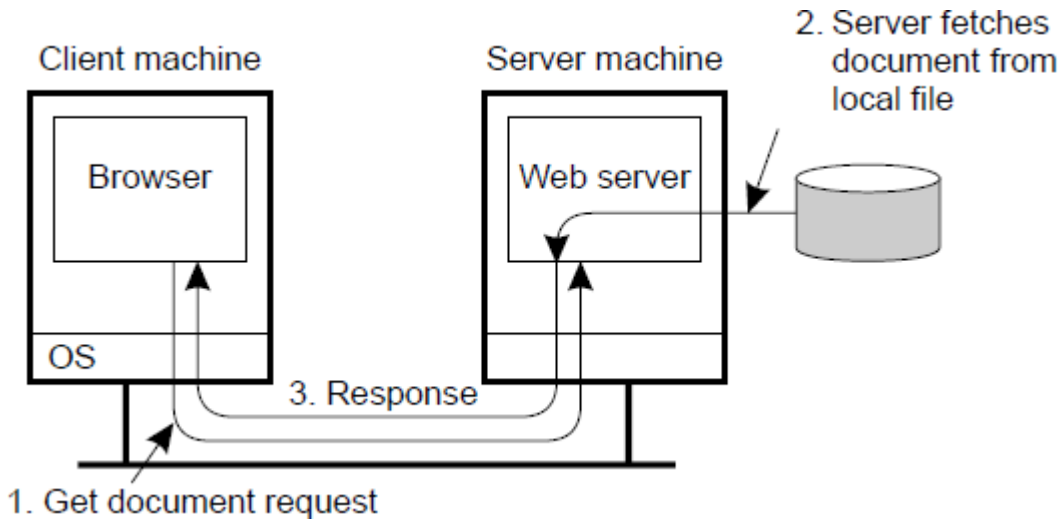


Figure 5.2 The overall organization of WWW

The Web has evolved considerably since its introduction some 10 years ago. By now, there is a wealth of methods and tools to produce information that can be processed by Web clients and Web servers. In the following text, we will go into detail on how the Web acts as a distributed system. However, we skip most of the methods and tools to actually construct Web documents, as they often have no direct relationship to the distributed nature of the Web. A good and thorough introduction on how to build Web-based applications can be found in (Deitel and Deitel, 2000).

Document Model

Fundamental to the Web is that all information is represented by means of documents. There are many ways in which a document can be expressed. Some documents are as simple as an ASCII text file, while others are expressed by a collection of scripts that are automatically executed when the document is downloaded into a browser.However, most important is that a document can contain references to other
documents. Such references are known as hyperlinks. When a document is displayed in a browser, hyperlinks to other documents can be shown explicitly to the user. The user can then select a link by clicking on it. Selecting a hyperlink results in a request to fetch the document that is sent to the server where the referenced document is stored. From there, it is subsequently transferred to the user's machine and displayed by the browser. The new document may either replace the current one or be displayed in a new pop-up window.

Most Web documents are expressed by means of a special language called HyperText

Markup anguage or simply HTML. Being a markup language means that HTML provides keywords to structure a document into different sections.For example, each HTML document is divided into a heading section and a main body. HTML also distinguishes headers, lists, tables,and forms. It is also possible to insert images or animations at specific positions in a document. Besides these structural elements, HTML provides various keywords to instruct the browserhow to present the document. For example, there are keywords to select a specific font or font size, to present text in italics or boldface, to align
parts of text, and so on.HTML is no longer what it used to be: a simple markup language. By now, it
includes many features for producing glossy Web pages. One of its most powerful features is the ability to express parts of a document in the form of a script. To give a simple example, consider the HTML document.

```
<HTML>                                          <!-- Start of HTML document      -->
<BODY>                                          <!-- Start of the main body      -->
<H1>Hello World</H1>                            <!-- Basic text to be displayed  -->
<P>                                             <!-- Start of new paragraph      -->
<SCRIPT type = "text/javascript">               <!-- Identify scripting language -->
    document.writeln("<H1>Hello World</H1>");   // Write a line of text
</SCRIPT>                                       <!-- End of scripting section    -->
</P>                                            <!-- End of paragraph section    -->
</BODY>                                         <!-- End of main body            -->
</HTML>                                         <!-- End of HTML section         -->
```

Figure 4.14 A simple Web page embedding a script written in JavaScript.

When this Web page is interpreted and displayed in a browser, the user will see the text ‘‘Hello World’’ twice, on separate lines. The first version of this text is the result of interpreting the HTML line

<H1>Hello World</H1>

The second version, however, is the result of running a small script written in JavaScript, a Java-like scripting language. The script consists of a single line of code document.

Writeln ("<H1>Hello World</H1>");

Although the effect of the two versions is exactly the same, there is clearly an important difference. The first version is the result of directly interpreting the HTML commands to properly display the marked up text. The second version is the result of executing a script that was downloaded into the browser as part of the document. In other words, we are faced with a form of mobile code.When a document is parsed, it is internally stored as a rooted tree, called a parse tree, in which each node represents an element of that document. To achieve portability,

the representation of the parse tree has been standardized. For example,each node canrepresent only one type of element from a predefined collection of element types. Similarly, each node is required to implement a standard interface containing methods for accessing its content, returning references to parent and child nodes, and so on. This standard representationis also known as the Document Object Model or DOM (le Hors et al., 2000). It is also often referred to as dynamic HTML. The DOM provides a standard programming interface to parsed Web documents.The interface is specified in CORBA IDL, and mappings to various scripting languages such as JavaScript have been standardized. The interface is used by the scripts embedded in a document to traverse the parse tree, inspect and modify nodes, add and delete nodes, and so on. In other words, scripts can be used to inspect and modify the document that they are part of.Clearly, this opens a wealth of possibilities to dynamically adapt a document. Although most Web documents are still expressed in HTML, an alternative language that also matches the DOM is XML, which stands for the Extensible Markup Language (Bray et al., 2000). Unlike HTML, XML is used only to structure a document; it contains no keywords to format a document such as centering a paragraph or presenting text in italics. Another important difference with HTML is that XML can be used to define arbitrary structures. In other words, it provides the means to define different document types.

```
(1)   <!ELEMENT article (title, author+, journal)>
(2)   <!ELEMENT title (#PCDATA)>
(3)   <!ELEMENT author (name, affiliation?)>
(4)   <!ELEMENT name (#PCDATA)>
(5)   <!ELEMENT affiliation (#PCDATA)>
(6)   <!ELEMENT journal(jname, volume, number?, month?, pages, year)>
(7)   <!ELEMENT jname (#PCDATA)>
(8)   <!ELEMENT volume (#PCDATA)>
(9)   <!ELEMENT number (#PCDATA)>
(10)  <!ELEMENT month (#PCDATA)>
(11)  <!ELEMENT pages (#PCDATA)>
(12)  <!ELEMENT year (#PCDATA)>
```

Defining a document type requires that the elements of that document are declared first. As anexample, the XML definition of a simple general reference to a journal article is show above (The line numbers are not part of the definitions.) An article reference is declared in line 1 to bea document consisting of three elements: a title, an author element, and a journal. The ‘‘+’’ signfollowing the author element indicates that one or more authors are given.In line 2, the title element is declared to consist of a series of characters
(referred to in XML by the primitive #PCDATA data type). The author element is subdivided intotwo other elements: a name and an affiliation. The ‘‘?’’ indicates that the affiliation element is optional, but cannot be provided more than once per author in an article reference.

Likewise, inline 6, the journal element is also subdivided into smaller elements.

Remote Logging (Telnet):

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
- A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

5.3 THERE ARE TWO TYPES OF TELNET:

5.3.1 Local Login:

- When a user logs into a local computer, then it is known as local login.
- When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.
- However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters have special meanings such as control character with "z" means suspend. Such situations do not create any problem as the terminal driver knows the meaning of such characters. But, it can cause the problems in remote login.

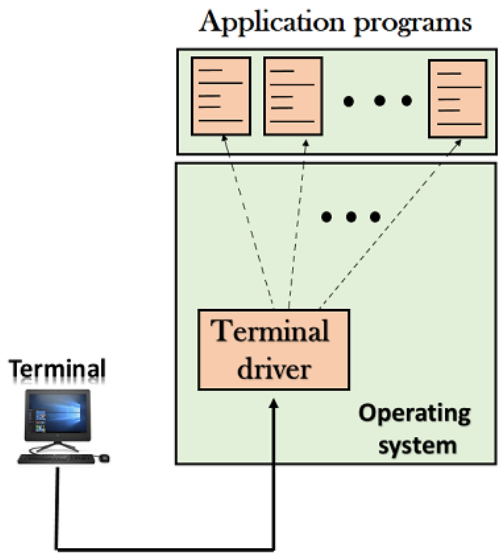


Figure 5.3.1 Local Login

5.3.2 Remote login:

- When the user wants to access an application program on a remote computer, then the user must perform remote login.

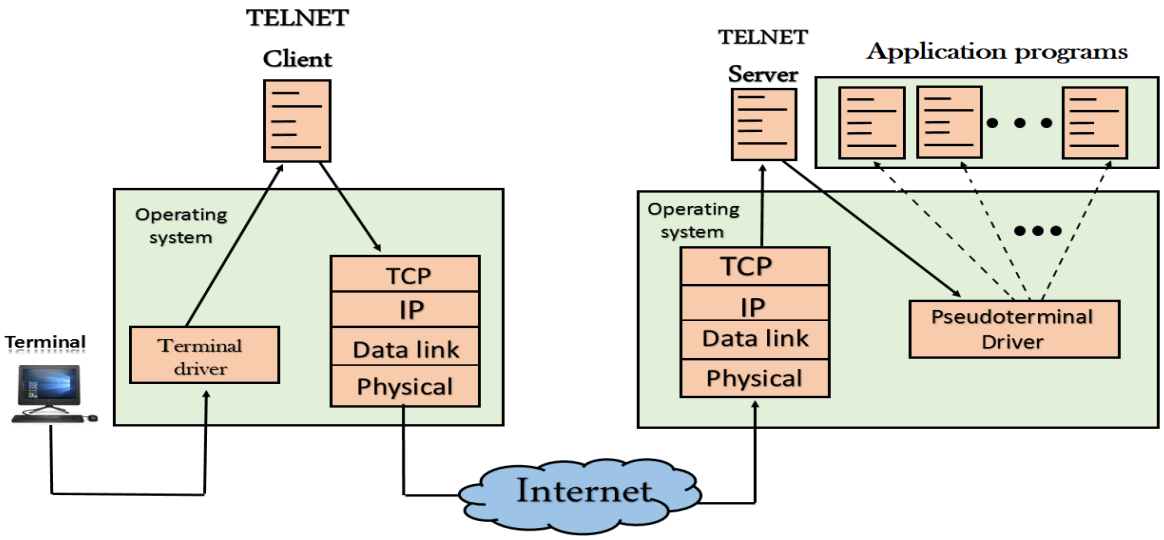


Figure 5.3.2 Remote Login

5.4 SMTP:

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It provides a mail exchange between users on the same or different computers, and it also supports:
    - It can send a single message to one or more recipients.
    - Sending message can include text, voice, video or graphics.
    - It can also send the messages on networks outside the internet.The main purpose of SMTP is used to set up communication rules between servers.

For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

Components of SMTP:

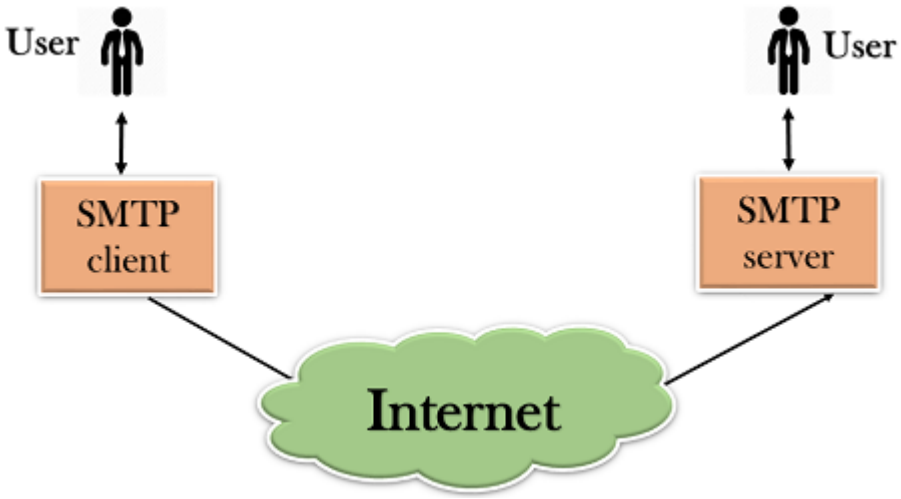


Figure 5.4.1 components of STMP

- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.

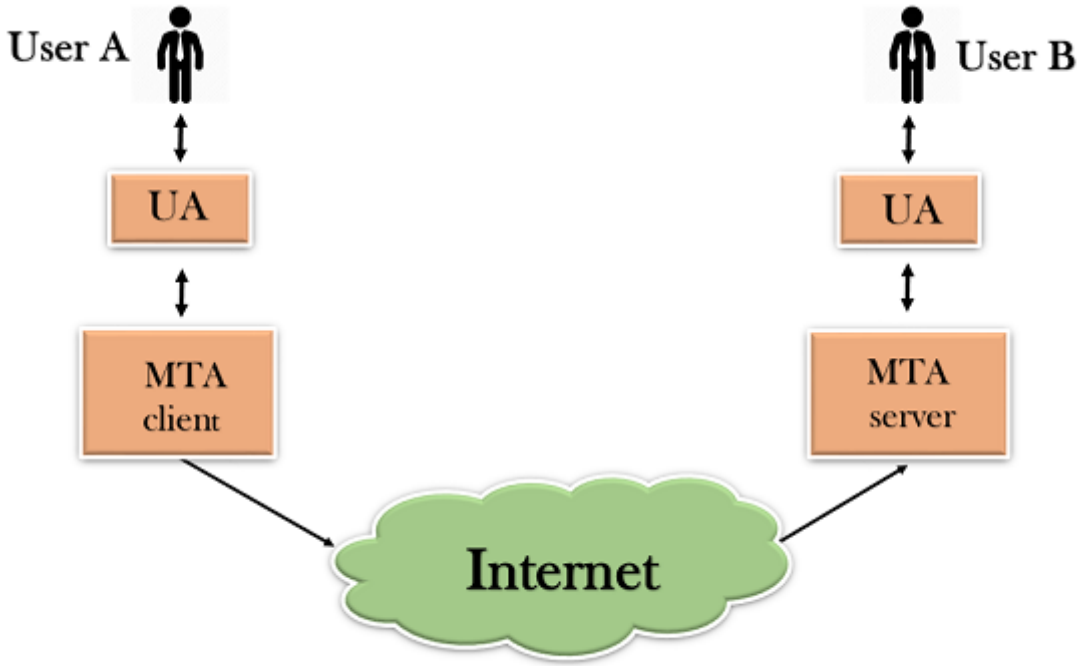


Figure 5.4.2

- SMTP allows a more complex system by adding a relaying system. Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.

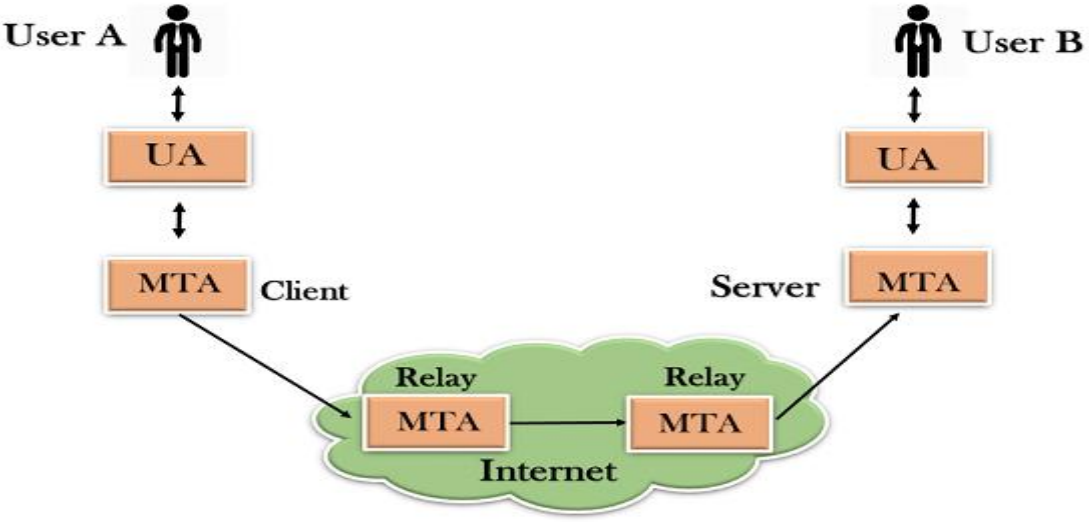


Figure 5.4.3

- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.

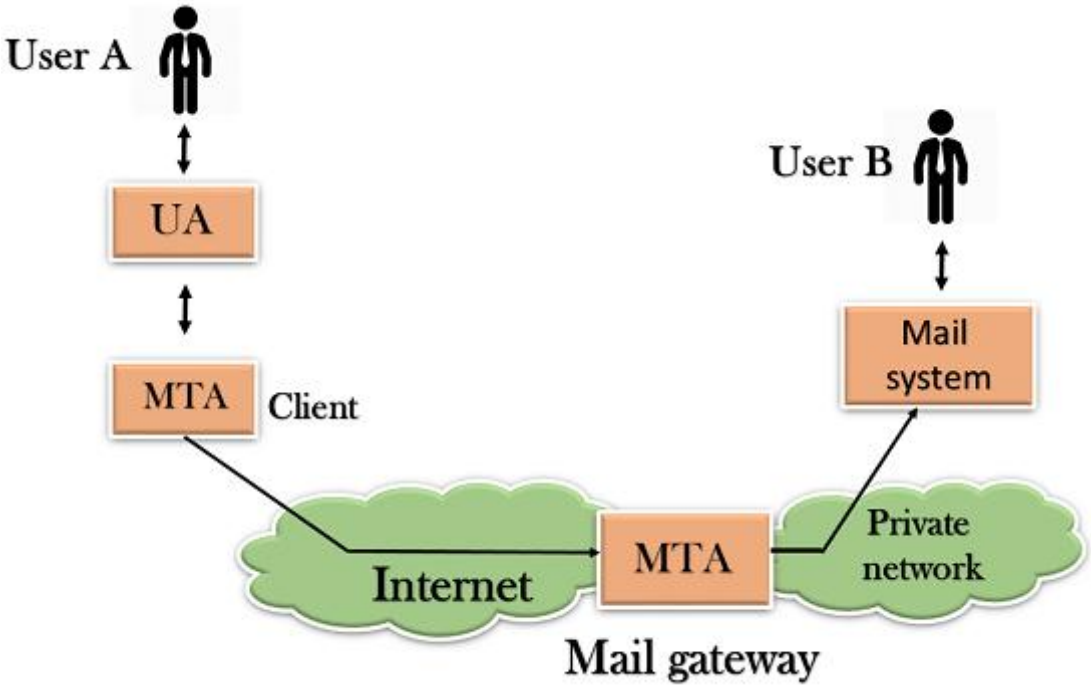


Figure 5.4.4

5.5 FTP:

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

There are two types of connections in FTP:

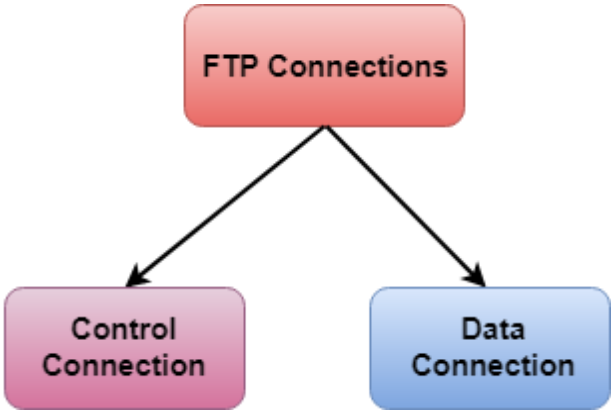


Figure 5.5 FTP types

- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

5.6 Mechanism of FTP:

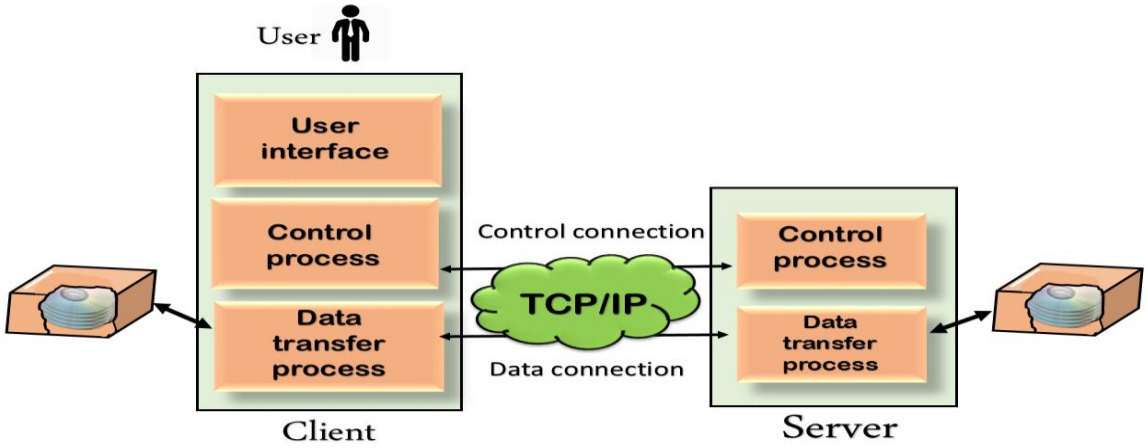


Figure 5.6 Mechanics of FTP

the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.

POP Protocol:

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent.

When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server.

5.7 understand the working of the POP3 protocol.

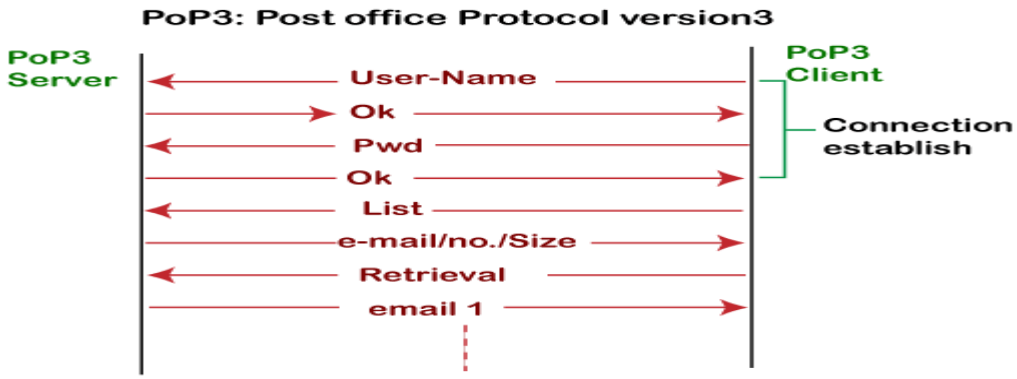


Figure 5.7 working of POP3

Advantages of POP3 protocol:

- It provides easy and fast access to the emails as they are already stored on our PC.
- There is no limit on the size of the email which we receive or send.
- It requires less server storage space as all the mails are stored on the local machine.
- There is maximum size on the mailbox, but it is limited by the size of the hard disk.
- It is a simple protocol so it is one of the most popular protocols used today.
- It is easy to configure and use.

Disadvantages of POP3 protocol:

- If the emails are downloaded from the server, then all the mails are deleted from the server by default. So, mails cannot be accessed from other machines unless they are configured to leave a copy of the mail on the server.
- Transferring the mail folder from the local machine to another machine can be difficult.
- Since all the attachments are stored on your local machine, there is a high risk of a virus attack if the virus scanner does not scan them. The virus attack can harm the computer.

5.8 MIME Protocol:

MIME stands for Multipurpose Internet Mail Extensions.

It is used to extend the capabilities of Internet e-mail protocols such as SMTP.

It does not operate independently, but it helps to extend the capabilities of e-mail in collaboration with other protocols such as SMTP.

Since MIME was able to transfer only text written file in a limited size English language with the help of the internet.

At present, it is used by almost all e-mail related service companies such as Gmail, Yahoo-mail, Hotmail.

Working diagram of MIME Protocol

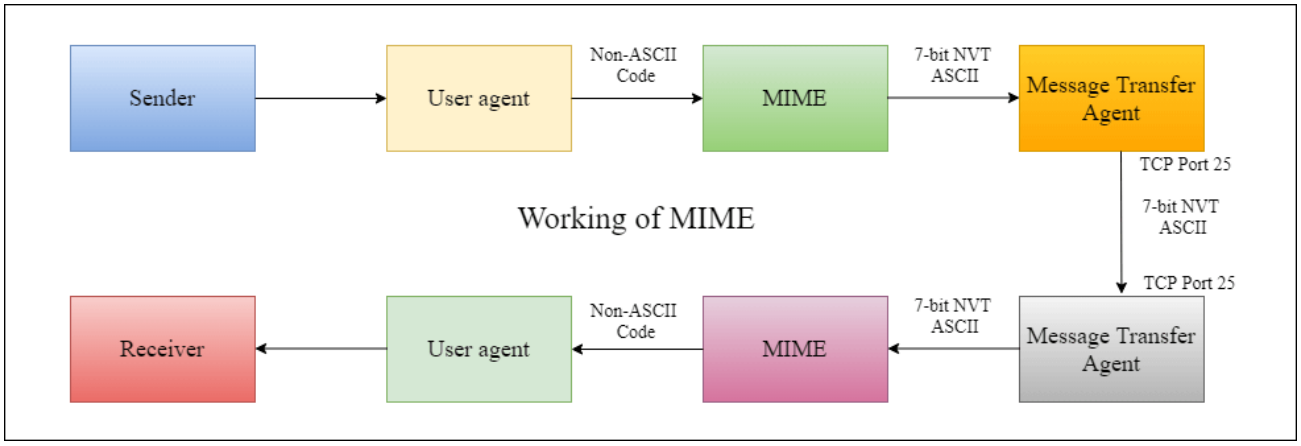


Figure 5.8 Block Diadram of MIME

MIME Header

MIME adds five additional fields to the header portion of the actual e-mail to extend the properties of the simple email protocol. These fields are as follows:

1. MIME Version
2. Content Type
3. Content Type Encoding
4. Content Id
5. Content description

1. MIME Version

It defines the version of the MIME protocol. This header usually has a parameter value 1.0, indicating that the message is formatted using MIME.

2. *Content Type*

It describes the type and subtype of information to be sent in the message. These messages can be of many types such as Text, Image, Audio, Video, and they also have many subtypes such that the subtype of the image can be png or jpeg. Similarly, the subtype of Video can be WEBM, MP4 etc.

3. Content Type Encoding

In this field, it is told which method has been used to convert mail information into ASCII or Binary number, such as 7-bit encoding, 8-bit encoding, etc.

4. *Content Id*

In this field, a unique "Content Id" number is appended to all email messages so that they can be uniquely identified.

5. *Content description*

This field contains a brief description of the content within the email. This means that information about whatever is being sent in the mail is clearly in the "Content Description". This field also provides the information of name, creation date, and modification date of the file.

Example of Content description

```
Content-Description: attachment; filename = javatpoint.jpeg; modification-date = "Wed, 12 Feb 1997 16:29:51 -0500";
```

SNMP:

- SNMP stands for **Simple Network Management Protocol**.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.

5.9 SNMP Concept

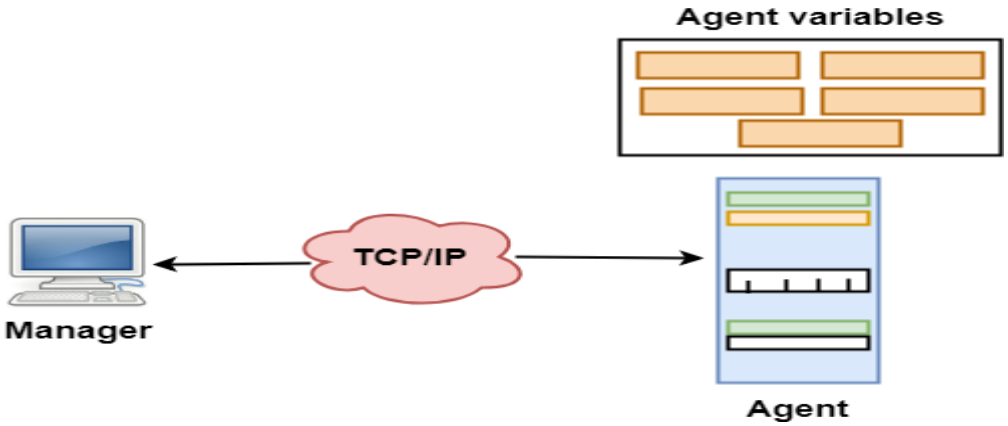


Figure 5.9 SNMP

- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.

Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

5.10 Management Components

- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).

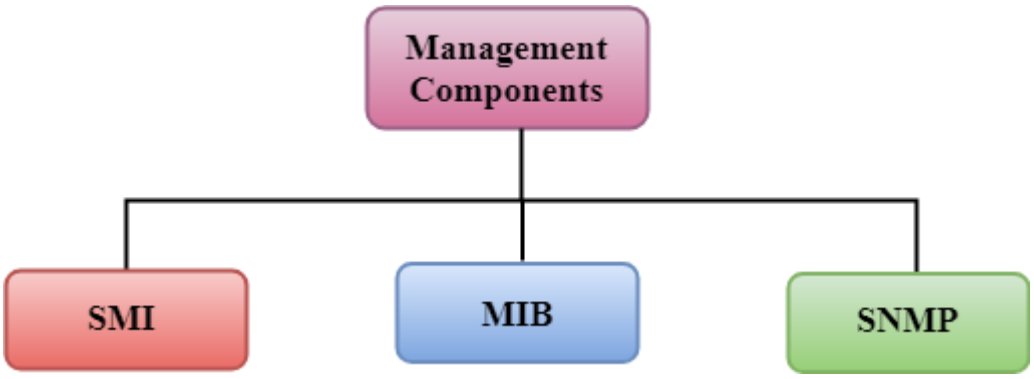


Figure 5.10 Management Components

SMI

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

5.11 MIB

- The MIB (Management information base) is a second component for the network management.
- Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.

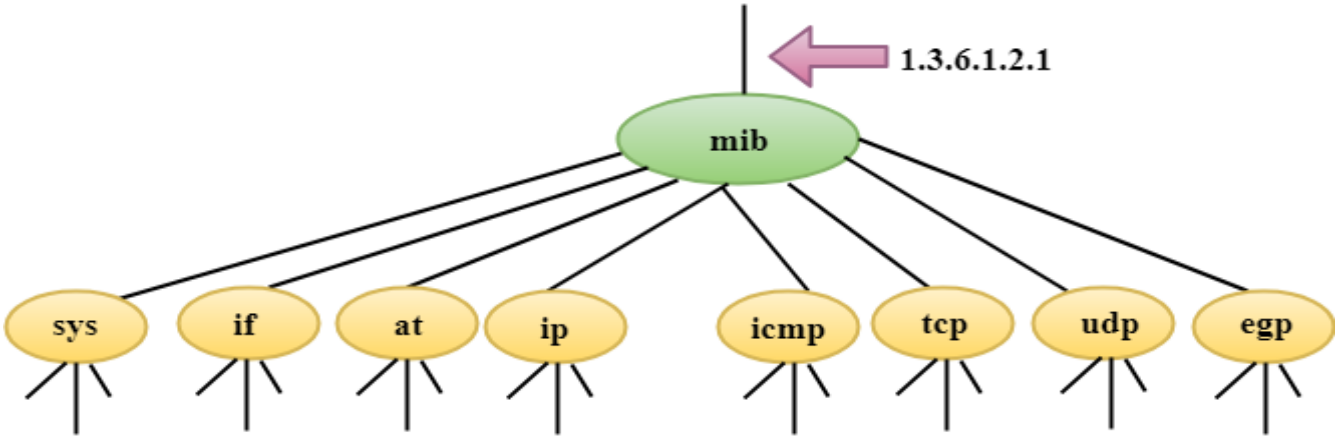


Figure 5.11 MIE

5.12 SNMP

SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.

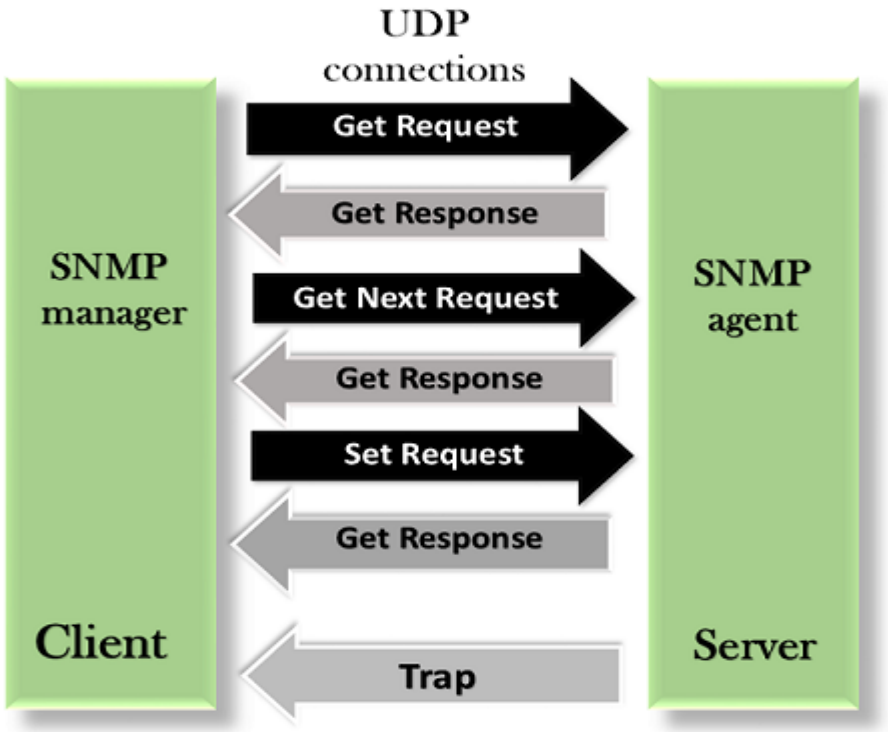


Figure 5.12 Block Diagram of SNMP

GetRequest: The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.

GetNextRequest: The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. In such situations, GetNextRequest message is used to define an object.

GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.

***SetRequest*:** The SetRequest message is sent from a manager to the agent to set a value in a variable.

Trap: The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

TEXT / REFERENCE BOOKS:

1. William Stallings, Data and Computer Communications, 10th Edition, Pearson, 2014.

2. Wayne Thomasi, "Advanced Electronic Communication Systems", 6th Edition, PHI Publishers, 2003.

3. Simon Haykins, “Communication Systems” John Wiley, 5th Edition, March 2009.

4. John G. Proakis, MasoudSalehi, “Digital Communication”, McGraw Hill 5th edition November 6, 2007.

5. Bernard Sklar, “Digital Communication, Fundamentals and Application”, Pearson Education Asia, 2nd

Edition, Jan. 21, 2001.

6. Behrouz A. Forouzen, “Data communication and Networking”, Fourth Edition, Tata McGraw – Hill, 2011.

7. Andrew S.Tanenbaum, “Computer Networks”, 5th Edition, Pearson, 2011.