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 ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – I DATA COMMUNICATION AND NETWORKING – SEC1306

UNIT I DATA COMMUNICATION- BASICS

I. INTRODUCTION

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media.

Digital data is information stored on a computer system as a series of 0's and 1's in a binary language. Information is stored on computer disks and drives as a magnetically charged switch which is in either a 0 or 1 state.

A digital signal refers to an electrical signal that is converted into a pattern of bits. Unlike an analog signal, which is a continuous signal that contains time-varying quantities, a digital signal has a discrete value at each sampling point. The precision of the signal is determined by how many samples are recorded per unit of time.

Bit rate describes the rate at which bits are transferred from one location to another. In other words, it measures how much data is transmitted in a given amount of time. Bit rate is commonly measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps).

Bit length is the distance one bit occupies on the transmission medium

$$Bit\ Length = Prpogation\ Speed\ X\ Bit\ \text{Duration} \tag{1.1}$$

1.1 EFFECTIVENESS OF A DATA COMMUNICATIONS

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

Delivery: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

Accuracy: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

Timeliness: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

1.2 DATA REPRESENTATION

Information today comes in different forms such as text, numbers, images, audio, and video.

Text: In data communications, text is represented as a bit pattern, a sequence of bits (Os or Is). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin. Appendix A includes part of the Unicode.

Numbers: Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images: Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image. After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only blackand-white dots (e.g., a chessboard), a I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio: Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete.

Video: Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

1.3 NETWORKS

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

1.3.1 Distributed Processing

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computer (usually a personal computer or workstation) handle a subset.

1.3.2 Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance: Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability: In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1.4 ANALOG AND DIGITAL

1.4.1 Analog and Digital Data

Both data and the signals that represent them can be either analog or digital in form. Analog and Digital Data. Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states. For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous. On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06. Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal. Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

1.4.2 Analog and Digital Signals

Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and O. The simplest way to show signals is by plotting them on a pair of perpendicular axes. The vertical axis represents the value or strength of a signal. The horizontal axis represents time. Figure 1.1 illustrates an analog signal and a digital signal. The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal, however, demonstrate the sudden jump that the signal makes from value to value.

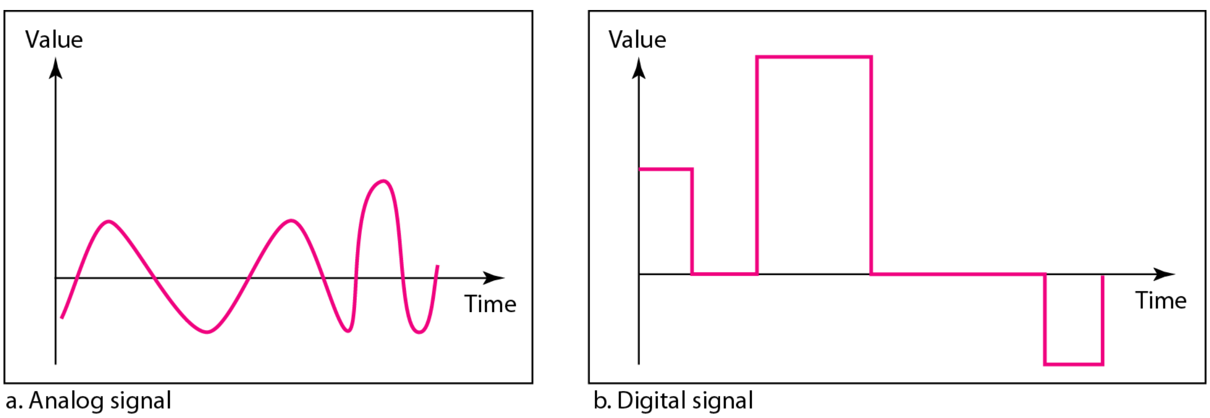


Fig. 1.1 ***Comparison of analog and digital signals***

1.5 TIME DOMAIN CONCEPTS

Continuous signal - Infinite number of points at any given time

Discrete signal - Finite number of points at any given time; maintains a constant level then changes to another constant level

Periodic signal - Pattern repeated over time

Aperiodic (non-periodic) signal - Pattern not repeated over time

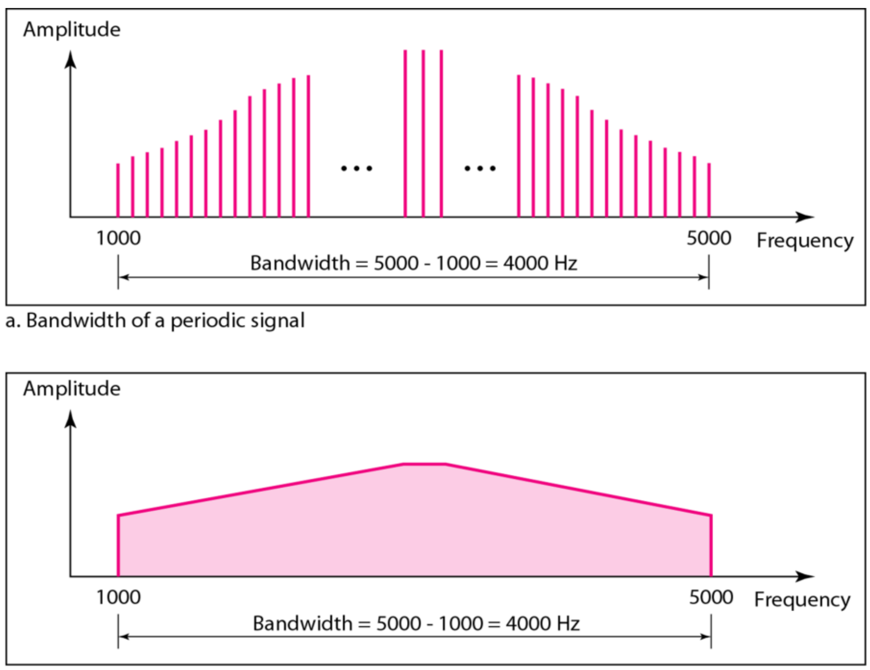
- In data communications, we commonly use periodic analog signals and nonperiodic digital signals.
- Periodic analog signals can be classified as simple or composite.
- A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals.
- A composite periodic analog signal is composed of multiple sine waves.

1.6 BANWIDTH

The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.

Note: each frequency is identifiable

Note: frequencies are all over the place



a. Bandwidth of a periodic signal

b. Bandwidth of a nonperiodic signal

Fig. 1.2 The bandwidth of periodic and non-periodic composite signals

EXAMPLE 1.1

If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is its bandwidth? Draw the **spectrum** ***(range of frequencies), assuming all components have maximum amplitude of 10 V.***

Solution

Let f_h be the highest frequency, f_l the lowest frequency, and B the bandwidth. Then The spectrum has only five spikes, at 100, 300, 500, 700, and 900 Hz

$$B = f_h - f_l = 900 - 100 = 800 \text{ Hz}$$

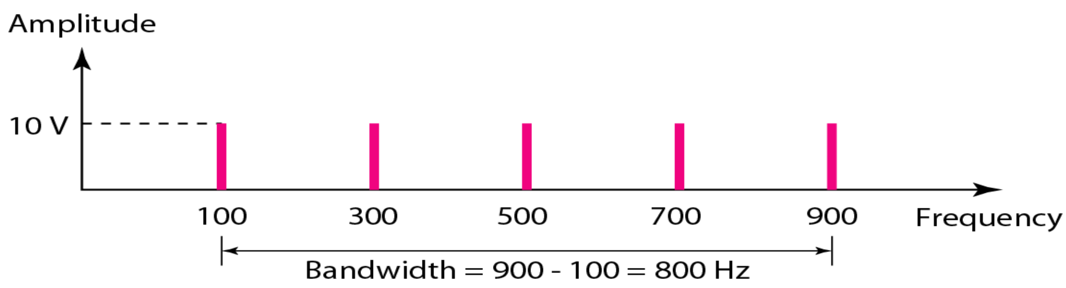


Fig. 1.3 The bandwidth for Example 1.1

1.7 DIGITAL SIGNALS

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level.

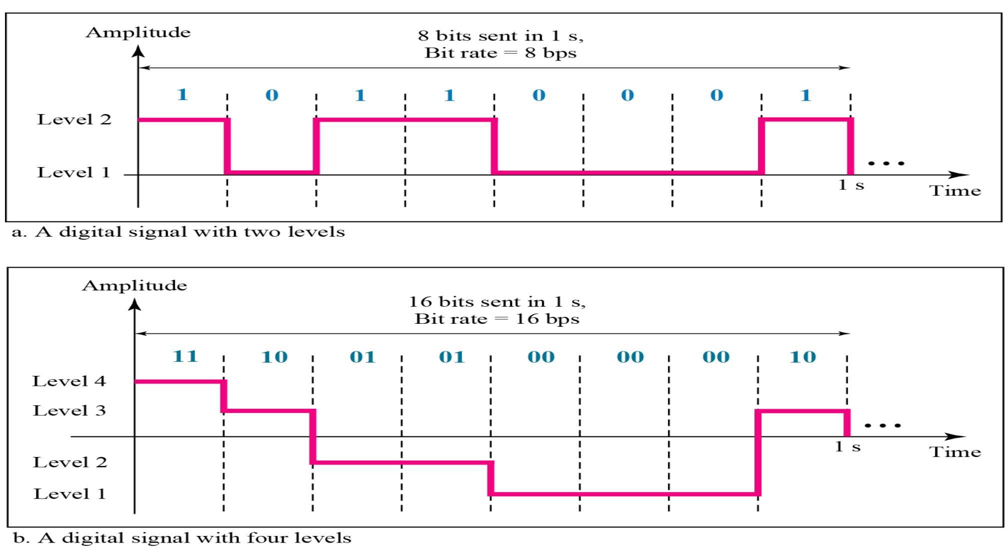


Fig 1.4 Two digital signals: one with two signal levels and the other with four signal levels

1.7.1 Bit rate

- Rate at which bits are transferred from one location to another.
- Measures how much data is transmitted in a given amount of time
- Measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps).
- A good rule of thumb is for the bitrate of your stream to use no more than 50% of your available upload bandwidth capacity on a dedicate d line.
- For example, if the result you get from a speed test shows that you have 2Mbps of upload speed available, your combined audio and video bit rate should not exceed 1Mbps.

1.7.2 Bit rate, Bit Length, Baud rate

Estimation of Bit rate

Frequency × bit depth × channels = bit rate.

44,100 samples per second × 16 bits per sample × 2 channels = 1,411,200 bits per second (or 1,411.2 kbps)

Baud Rate: Baud Rate is the number of signal unit transmitted per second. Thus Baud Rate is always less than or equal to bit rate.

Bit Length: The Bit Length is the distance of one Bit occupies on the transmission medium.

Bit Length = Propagation speed * Bit duration

EXAMPLE 1.2

A digital signal has eight levels. How many bits are needed per level? We calculate the number of bits from the formula

Solution

$$\text{Number of bits per level} = \log_2 8 = 3$$

Each signal level is represented by 3 bits.

EXAMPLE 1.3

Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel?

Solution

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits, the bit rate is

$$100 \times 24 \times 80 \times 8 = 1{,}636{,}000 \text{ bps} = 1.636 \text{ Mbps}$$

EXAMPLE 1.4

A digitized voice channel, as we will see in Chapter 4, is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits. What is the required bit rate?

Solution

$$2 \times 4000 \times 8 = 64{,}000 \text{ bps} = 64 \text{ kbps}$$

EXAMPLE 1.5

What is the bit rate for high-definition TV (HDTV)?

Solution

HDTV uses digital signals to broadcast high quality video signals. The HDTV screen is normally a ratio of 16 : 9. There are 1920 by 1080 pixels per screen, and the screen is renewed 30 times per second. Twenty-four bits represents one color pixel. The TV stations reduce this rate to 20 to 40 Mbps through compression.

$$\boxed{1920 \times 1080 \times 30 \times 24 = 1{,}492{,}992{,}000 \text{ or } 1.5 \text{ Gbps}}$$

1.7.3 BANDWIDTH REQUIREMENTS FOR VARIOUS BITRATE

A good rule of thumb is for the bitrate of your stream to use no more than 50% of you r available upload bandwidth capacity on a dedicated line. For example, if the result you get from a speed test shows that you have 2Mbps of upload speed available, your combined audio and video bit rate should not exceed 1Mbps.

Table 1.1 Bandwidth Requirements

Bit Rate	Harmonic 1	Harmonics 1, 3	Harmonics 1, 3, 5
n = 1 kbps	B = 500 Hz	B = 1.5 kHz	B = 2.5 kHz
n = 10 kbps	B = 5 kHz	B = 15 kHz	B = 25 kHz
n = 100 kbps	B = 50 kHz	B = 150 kHz	B = 250 kHz

EXAMPLE 1.6

If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is its bandwidth?

Solution

Let f h be the highest frequency, f l the lowest frequency, and B the bandwidth.

Then $B = f_h - f_l = 900 - 100 = 800$ ***Hz.***

EXAMPLE 1.7

A periodic signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency?

Solution

Let f_h be the highest frequency, f_l the lowest frequency, and B the bandwidth. Then

$B = f_h - f_l = 20$; $20 = 60 - f_l$; $f_l = 40$ Hz.

EXAMPLE 1.8

A non-periodic composite signal has a bandwidth of 200 kHz, with a middle frequency of 140 kHz and peak amplitude of 20V. Find the lowest and highest frequency.

Solution

Bandwidth B = 200 kHz Middle Frequency is 140 kHz

fh = middle frequency + (B/2) = 140 + 100 = 240 kHz

fl = middle frequency - (B/2) = 140 -100 = 40 kHz

1.8 TRANSMISSION CHANNEL

Physical Transmission Medium - Connection over a multiplexed channel - Radio Channel

Types of Transmission Media

Guided Media - Twisted Pair Cable Coaxial Cable Optical Fibre Cable

Unguided Media - Radiowaves Microwaves Infrared

1.8.1 Transmission of Digital Signals

Baseband Transmission

- Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal.
- In baseband transmission, the required bandwidth is proportional to the bit rate; if we need to send bits faster, we need more bandwidth.

Note: Baseband transmission of a digital signal that preserves the shape of the digital signal is possible only if we have a low-pass channel with an infinite or very wide bandwidth.

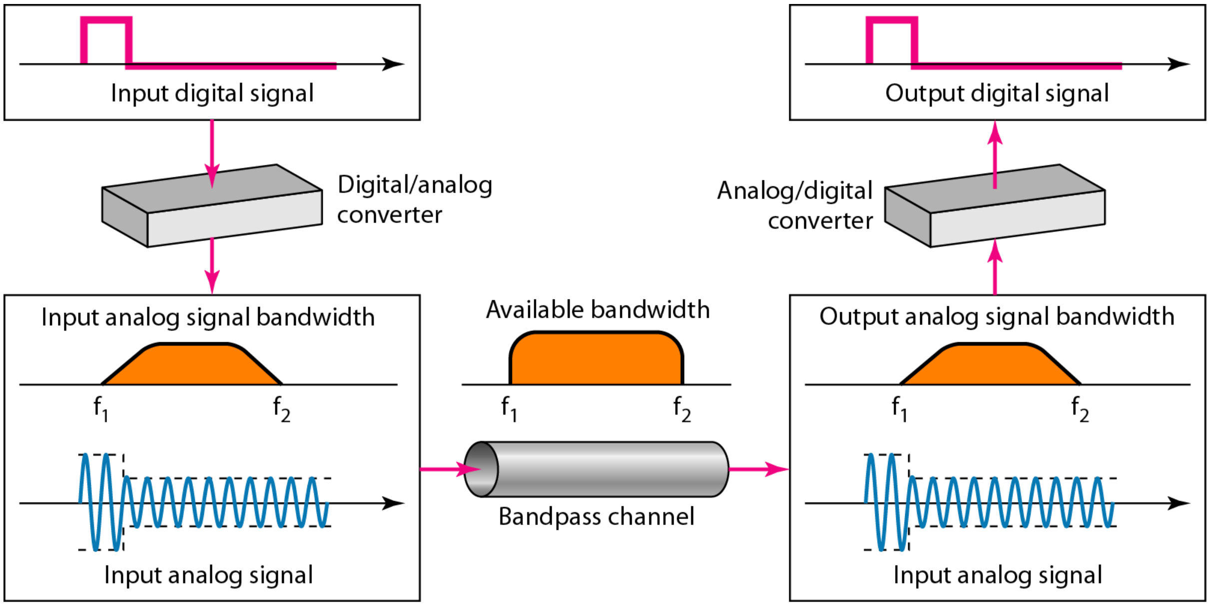


Fig. 1.5 Modulation of a digital signal for transmission on a bandpass channel

Broadband Transmission (or) Modulation

- Broadband transmission or modulation means changing the digital to analog signal for transmission
- It uses a band pass channel - a channel with a bandwidth that does not start with zero

  Examples: internet data through telephone line using MODEMs, Modulation in cellular mobile networks, etc.,

1.9 TRANSMISSION IMPAIRMENT

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

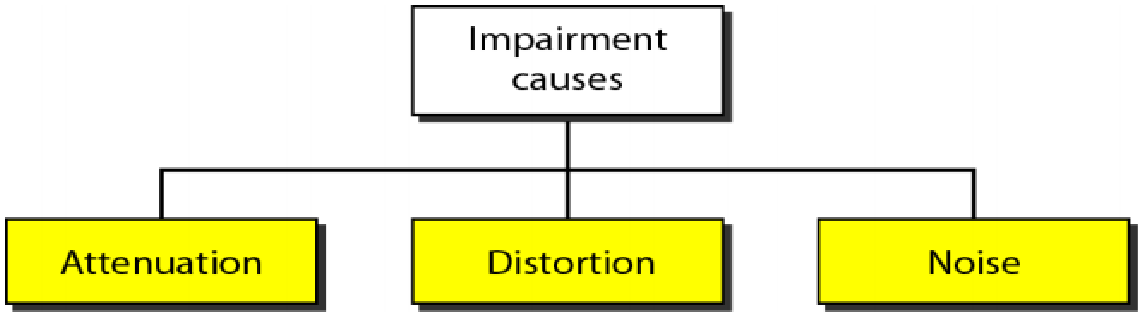


Fig. 1.6 Various causes for Impairment

Attenuation

- ✓ Attenuation means a loss of energy.
- ✓ When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium.
- ✓ Some of the electrical energy in the signal is converted to heat.
- ✓ To compensate for this loss, amplifiers are used to amplify the signal.

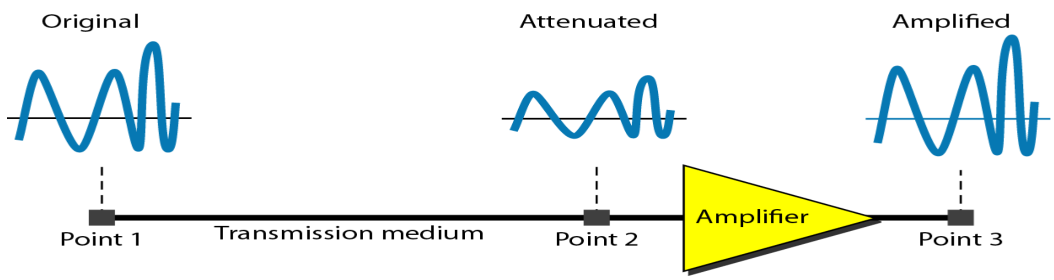


Fig. 1.7 Attenuation

Decibel

- ✓ To show that a signal has lost or gained strength, engineers use the unit of the decibel
- ✓ The decibel (dB) measures the relative strengths of two signals or one signal at two different points.
- ✓ Note that the decibel is negative if a signal is attenuated and positive if a signal is amplified.
- ✓ Variables PI and P2 are the powers of a signal at points 1 and 2, respectively.

$N_{dB} = 10 \times \log_{10} (P2 / P1)$

P2 = ending power level in watts

P1 = beginning power level in watts

Distortion

- ✓ Distortion means that the signal changes its form or shape.
- ✓ Distortion can occur in a composite signal made of different frequencies.
- ✓ Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination.
- ✓ Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.
- ✓ In other words, signal components at the receiver have phases different from what they had at the sender.
- ✓ The shape of the composite signal is therefore not the same.

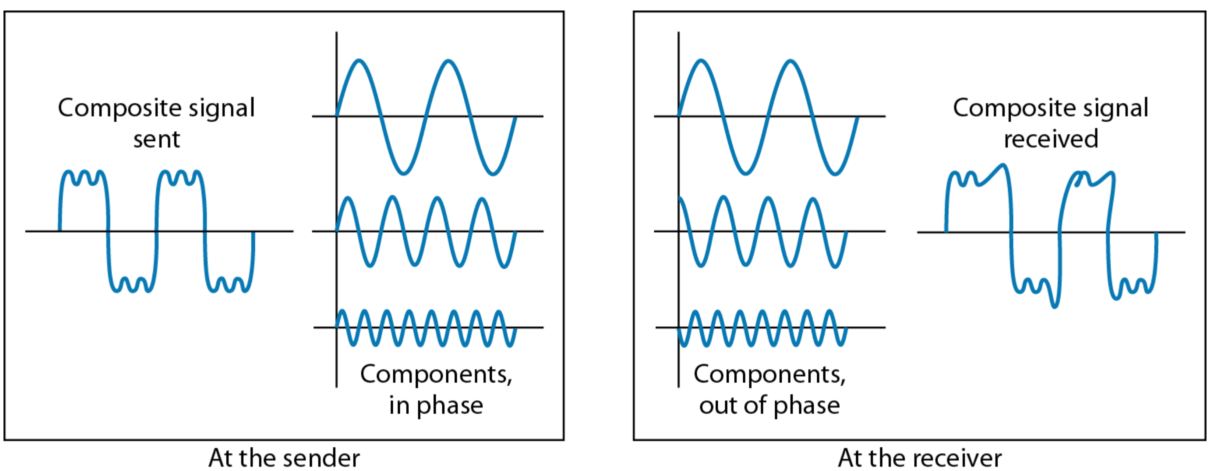


Fig. 1.8 Distortion

Noise

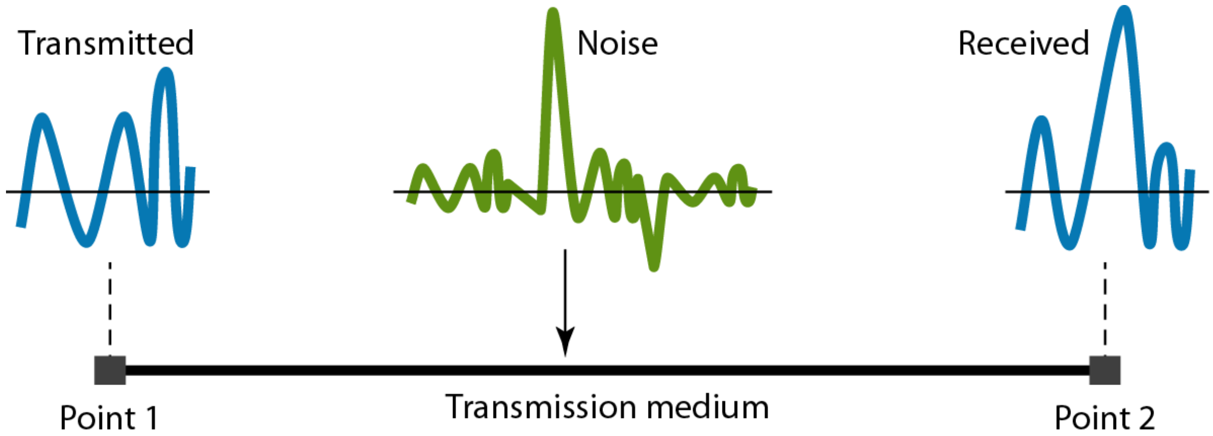


Fig. 1.9 noise

1.10 SWITCHING TECHNIQUES

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks. The number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time. Other topologies employing multipoint connections, such as a bus, areruled out because the distances between devices and the total number of devices increase beyond the capacities of the media and equipment.

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. Figure 1.10 shows a switched network.

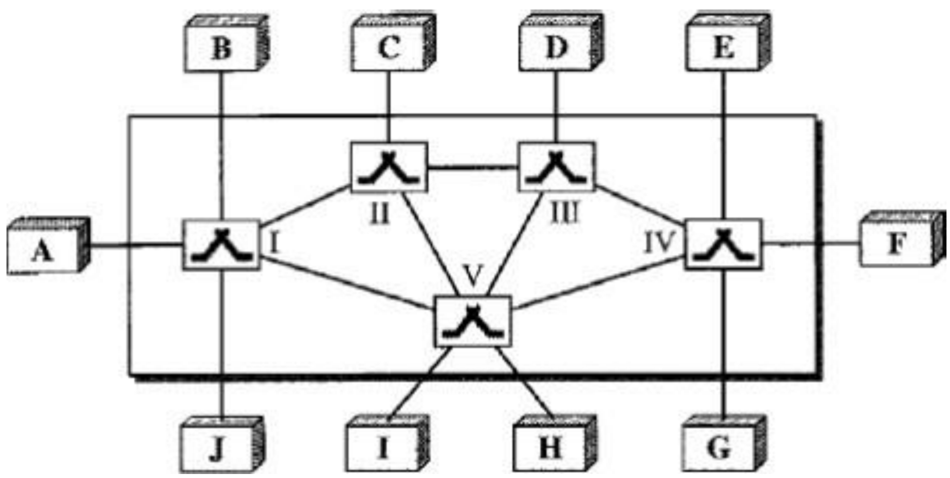


Fig.1.10 switched network

The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

Taxonomy of switched networks

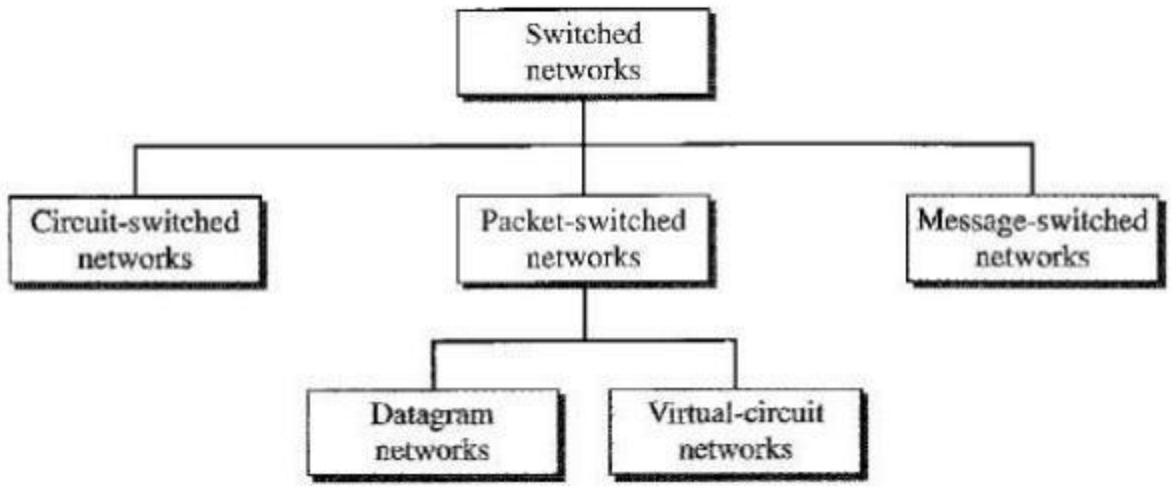


Fig.1.11 Taxonomy of Switched Networks

CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM

Figure 1.12 shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.

A trivial circuit-switched network

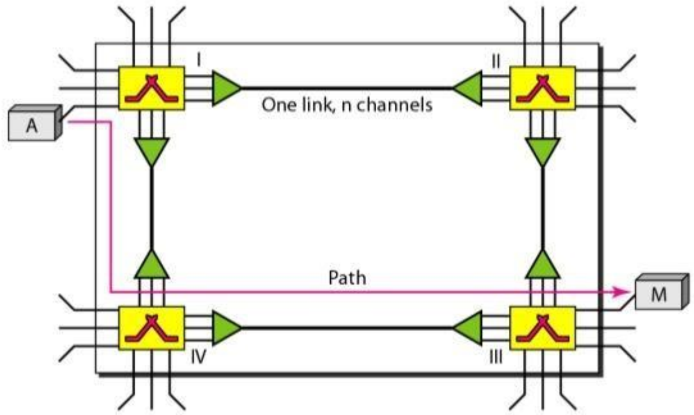


Fig 1.12 trivial circuit-switched network

Three Phases

The actual communication in a circuit-switched network requires three phases:

1. Connection setup

2. Data transfer,

3. Connection teardown

1. Setup Phase:

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, in Figure 1.2, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose.

Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established. Note that end-to-end addressing is required for creating a connection between the two end systems. These can be, for example, the addresses of the computers assigned by the administrator in a TDM network, or telephone numbers in an FDM network.

2. Data Transfer Phase:

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

3. Teardown Phase: When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency:

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation. However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time. In this case, allowing resources to be dedicated means that other connections are deprived.

Delay: Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

Figure 1.13 shows the idea of delay in a circuit switched network when only two switches are involved. As Figure shows, there is no waiting time at each switch. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

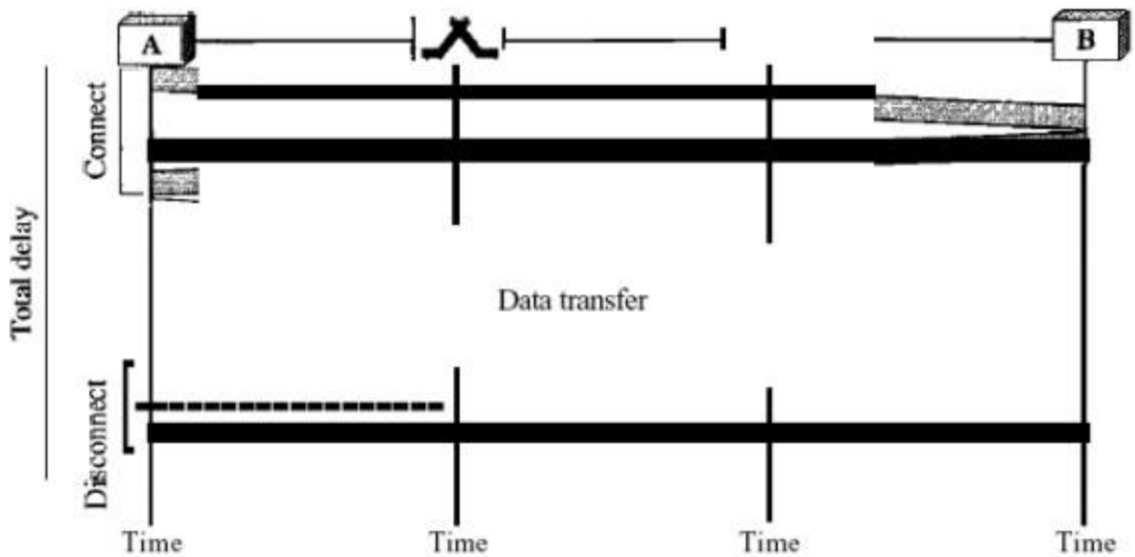


Fig 1.13 delay in a circuit switched network

The delay caused by the setup is the sum of four parts: the propagation time of the source computer request (slope of the first gray box), the request signal transfer time (height of the first gray box), the propagation time of the acknowledgment from the destination computer (slope of the second gray box), and the signal transfer time of the acknowledgment (height of the second gray box).

The delay due to data transfer is the sum of two parts: the propagation time (slope of the colored box) and data transfer time (height of the colored box), which can be very long. The third box shows the time needed to tear down the circuit. We have shown the case in which the receiver requests disconnection, which creates the maximum delay.

DATAGRAM NETWORKS

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer. Figure 1.14 shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. That is why we use a different symbol for the switches in the figure.

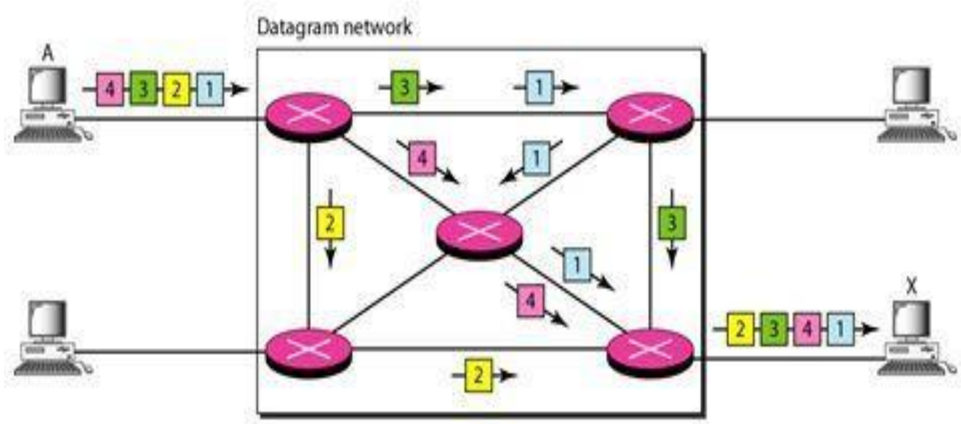


Fig 1.14 datagram network

In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources.

In most protocols, it is the responsibility of an upperlayer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application. The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

Routing Table:

If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network? In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over. Figure 1.15 shows the routing table for a switch.

Destination address	Output port
1232	1
4150	2
.	.
9130	3

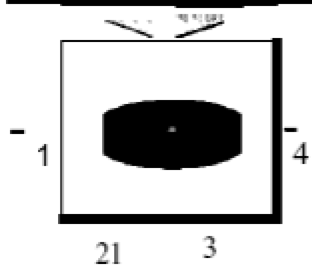


Fig 1.15 Routing table in a datagram network

Destination address:

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual circuit-switched network, remains the same during the entire journey of the packet.

Efficiency:

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

Delay:

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

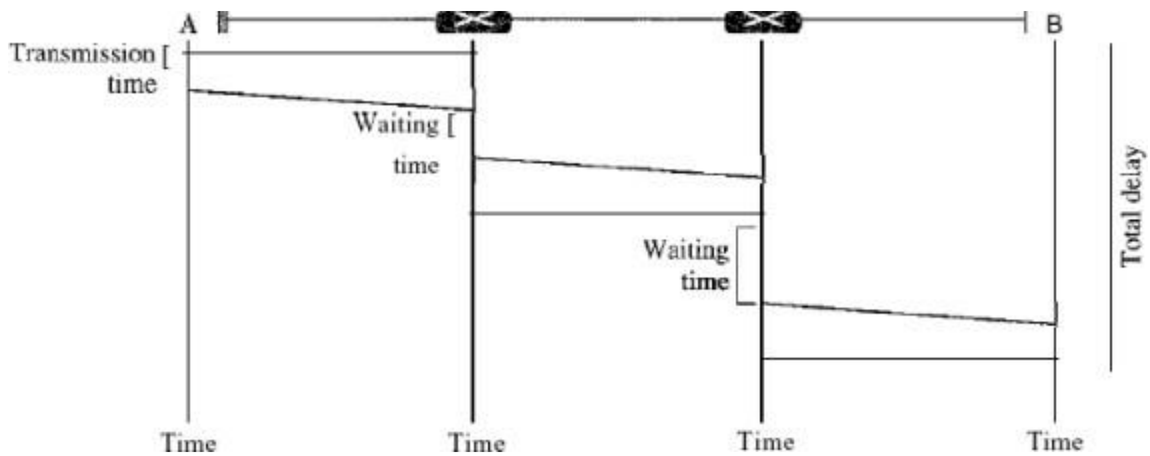


Fig 1.16 Delay in a datagram network

The packet travels through two switches. There are three transmission times (3T), three propagation delays (slopes 3't of the lines), and two waiting times (WI + w2)' we ignore the processing time in each switch.

The total delay is Total delay =3T + 3t + WI + W2

VIRTUAL-CIRCUIT NETWORKS:

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being canied), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no

final destination address carried by a packet. The answer will be clear when we discuss virtual circuit identifiers in the next section.

4. As in a circuit-switched network, all packets follow the same path established during the connection.

5. A virtual-circuit network is normally implemented in the data link layer, while a circuit switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future. Figure 1.17 is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

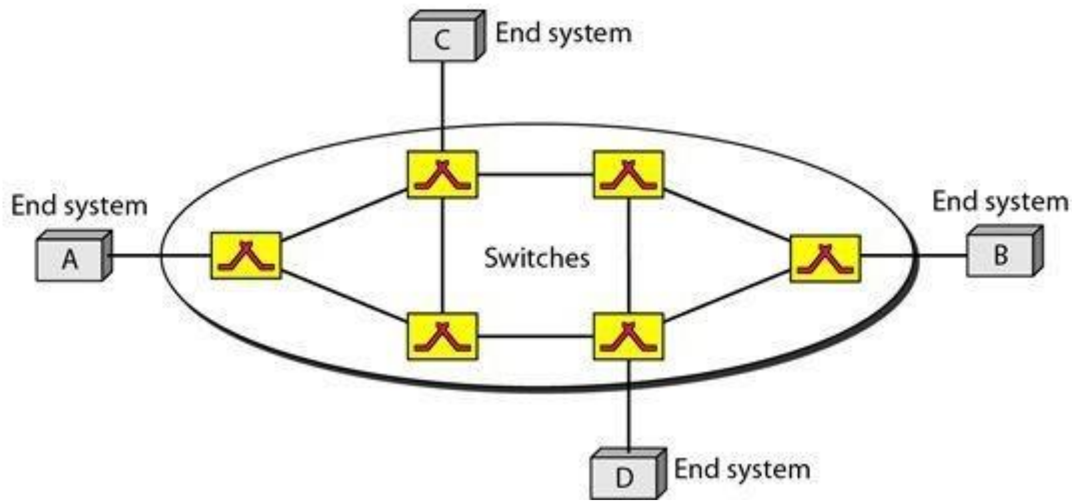


Fig 1.17 Virtual-circuit network

Addressing

In a virtual-circuit network, two types of addressing are involved:

Global and local (virtual-circuit identifier).

Global Addressing: A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

Virtual-Circuit Identifier: The identifier that is actually used for data transfer is called the virtual circuit identifier (Vel). A vel, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl. Figure 1.18 shows how the VCI in a data frame changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCls.

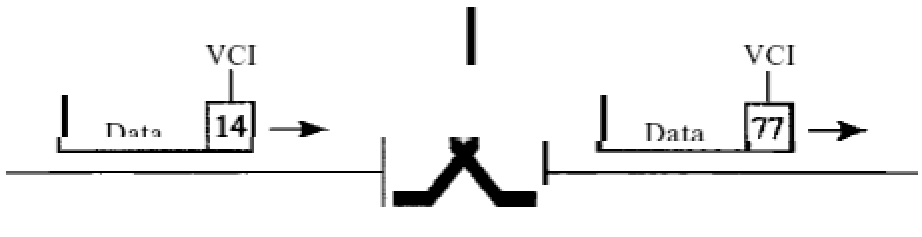


Fig 1.18 Virtual-circuit identifier

Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.

In the setup phase,

The source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete the corresponding entry. Data transfer occurs between these two phases. We first discuss the data transfer phase, which is more straightforward; we then talk about the setup and teardown phases.

Data Transfer Phase:

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. We show later how the switches make their table entries, but for the moment we assume that each switch has a table with entries for all active virtual circuits. The process creates a virtual circuit, not a real circuit, between the source and destination.

Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment

Efficiency

As we said before, resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays. There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it. Consider a family that wants to dine at a restaurant. Although the restaurant may not accept reservations (allocation of the tables is on demand), the family can call and find out the waiting time. This can save the family time and effort.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Below Figure 1.19 shows the delay for a packet traveling through two switches in a virtual circuit network.

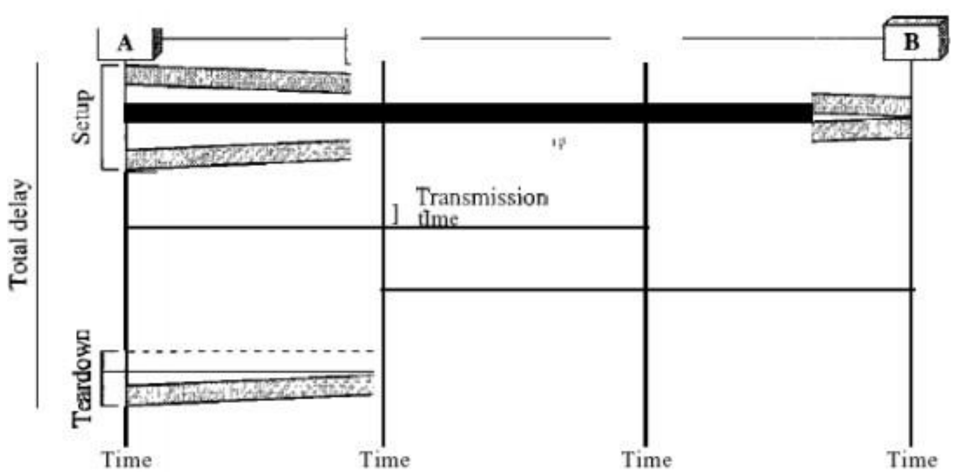


Fig 1.19 Delay in a virtual-circuit network

The packet is traveling through two switches (routers). There are three transmission times (3T), three propagation times (3't), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction). We ignore the processing time in each switch.

The total delay time is Total delay = 3T+ 3't + setup delay + teardown delay

Differences between Virtual Circuits & Datagram Networks

Virtual Circuits-

1. It is connection-oriented simply meaning that there is a reservation of resources like buffers, CPU, bandwidth,etc. for the time in which the newly setup VC is going to be used by a data transfer session.
2. First packet goes and reserves resources for the subsequent packets which as a result follow the same path for the whole connection time.
3. Since all the packets are going to follow the same path, a global header is required only for the first packet of the connection and other packets generally don’t require global headers.
4. Since data follows a particular dedicated path, packets reach inorder to the destination.
5. From above points, it can be concluded that Virtual Circuits are highly reliable means of transfer.
6. Since each time a new connection has to be setup with reservation of resources and extra information handling at routers, its simply costly to implement Virtual Circuits.

Datagram Networks:

1. It is connectionless service. There is no need of reservation of resources as there is no dedicated path for a connection session.
2. All packets are free to go to any path on any intermediate router which is decided on the go by dynamically changing routing tables on routers.

3. Since every packet is free to choose any path, all packets must be associated with a header with proper information about source and the upper layer data.

4. The connectionless property makes data packets reach destination in any order, means they need not reach in the order in which they were sent.

5. Datagram networks are not reliable as Virtual Circuits.

6. But it is always easy and cost efficient to implement datagram networks as there is no extra headache of reserving resources and making a dedicated each time an application has to communicate.

ISO / OSI MODEL:

ISO refers International Standards Organization was established in 1947, it is a multinational body dedicated to worldwide agreement on international standards. OSI refers to Open System Interconnection that covers all aspects of network communication. It is a standard of ISO. Here open system is a model that allows any two different systems to communicate regardless of their underlying architecture. Mainly, it is not a protocol it is just a model.

1.11 OSI MODEL

The open system interconnection model is a layered framework. It has seven separate but interrelated layers. Each layer having unique responsibilities.

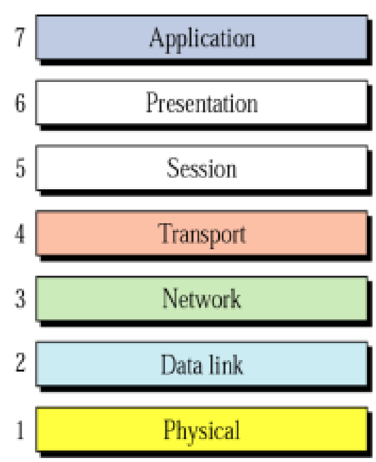


Fig 1.20 OSI Model

The OSI model shown in figure 1.20 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. It consists 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.

Layered Architecture :

The OSI model is composed of seven layers: Physical, Data link, Network, Transport, Session, Presentation, Application layers.

Figure 1.21 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 governed by 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.

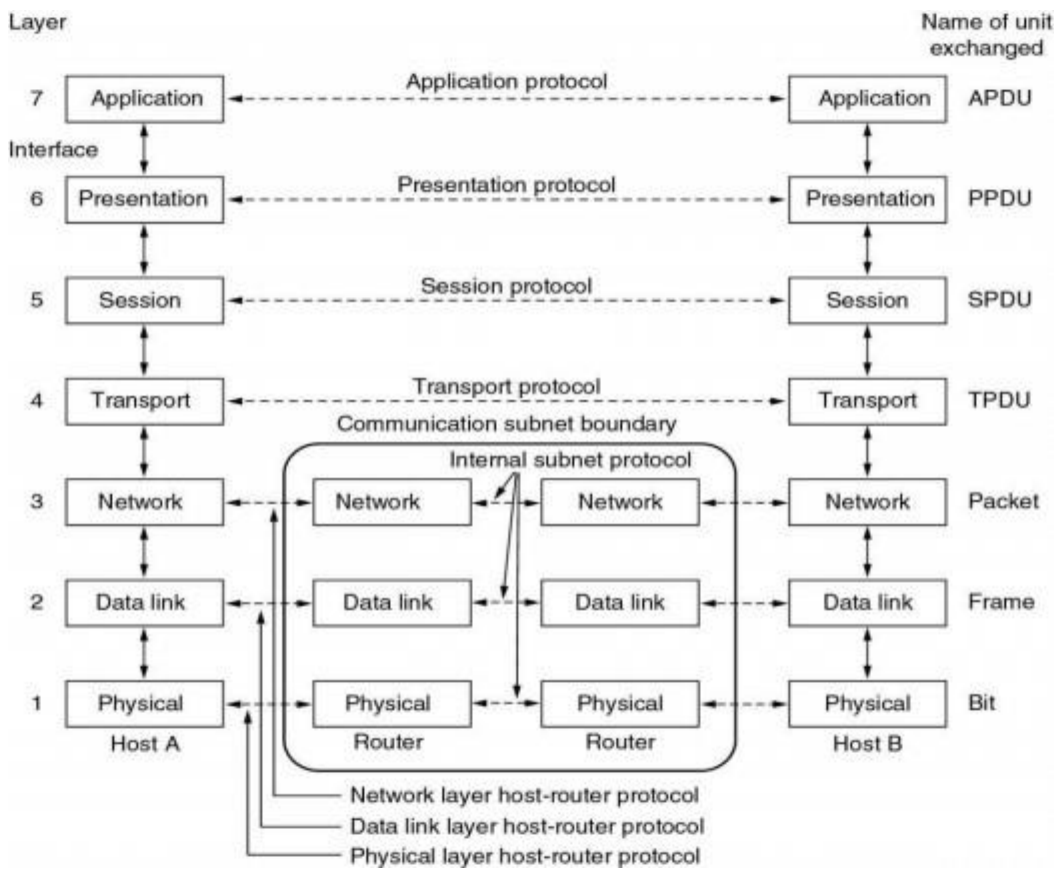


Fig 1.21 interaction between layers in the OSI model

ORGANIZATION OF LAYERS

The seven layers are arranged by three sub groups.

1. Network Support Layers

2. User Support Layers

3. Intermediate Layer

Network Support Layers:

Physical, Datalink and Network layers come under the group. They deal with the physical aspects of the data such as electrical specifications, physical connections, physical addressing, and transport timing and reliability.

User Support Layers:

Session, Presentation and Application layers comes under the group. They deal with the interoperability between the software systems.

Intermediate Layer:

The transport layer is the intermediate layer between the network support and the user support layers.

FUNCTIONS OF THE LAYERS

PHYSICAL LAYER

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and the transmission medium.

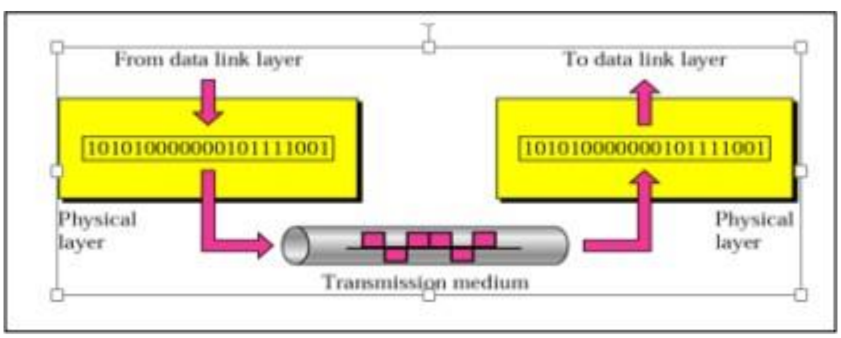


Fig 1.22 Physical Layer

The functions are,

1. Physical Characteristics of Interfaces and Media: It defines the electrical and mechanical characteristics of the interface and the media. It defines the types of transmission medium

2. Representation of Bits: To transmit the stream of bits they must be encoded into signal. It defines the type of encoding weather electrical or optical.

3. Data Rate: It defines the transmission rate i.e. the number of bits sent per second.

4. Synchronization of Bits: The sender and receiver must be synchronized at bit level.

5. Line Configuration: It defines the type of connection between the devices.

Two types of connection are

1. Point to point 2. Multipoint

6. Physical Topology: It defines how devices are connected to make a network.

Five topologies are,

1. mesh 2. star 3. tree 4. bus 5. ring

7. Transmission Mode It defines the direction of transmission between devices.

Three types of transmission are, 1. simplex 2. half duplex3. full duplex

DATALINK LAYER

Datalink layer responsible for node-to-node delivery

The responsibilities of Datalink layer are,

1. Framing: It divides the stream of bits received from network layer into manageable data units called frames.

2. Physical Addressing: It adds a header that defines the physical address of the sender and the receiver. If the sender and the receiver are in different networks, then the receiver address is the address of the device which connects the two networks.

3. Flow Control: It imposes a flow control mechanism used to ensure the data rate at the sender and the receiver should be same.

4. Error Control: To improve the reliability the Datalink layer adds a trailer which contains the error control mechanism like CRC, Checksum etc

5. Access Control: When two or more devices connected at the same link, then the Datalink layer used to determine which device has control over the link at any given time.

NETWORK LAYER

When the sender is in one network and the receiver is in some other network then the network layer has the responsibility for the source to destination delivery.

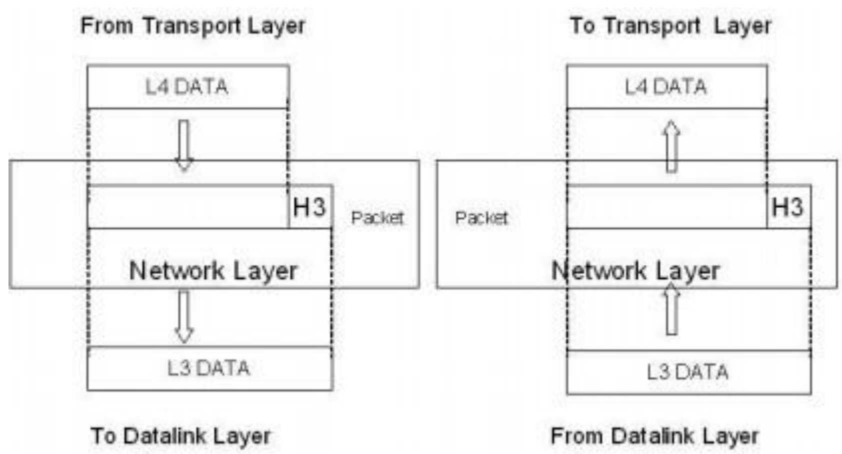


Fig 1.23 Network Layer

The responsibilities are,

1. Logical Addressing: If a packet passes the network boundary that is when the sender and receiver are places in different network then the network layer adds a header that defines the logical address of the devices.

2. Routing: When more than one networks connected and to form an internetwork, the connecting devices route the packet to its final destination. Network layer provides this mechanism.

TRANSPORT LAYER

The network layer is responsible for the end to end delivery of the entire message. It ensures that the whole message arrives in order and intact. It ensures the error control and flow control at source to destination level.

Fig 1.23 Network Layer

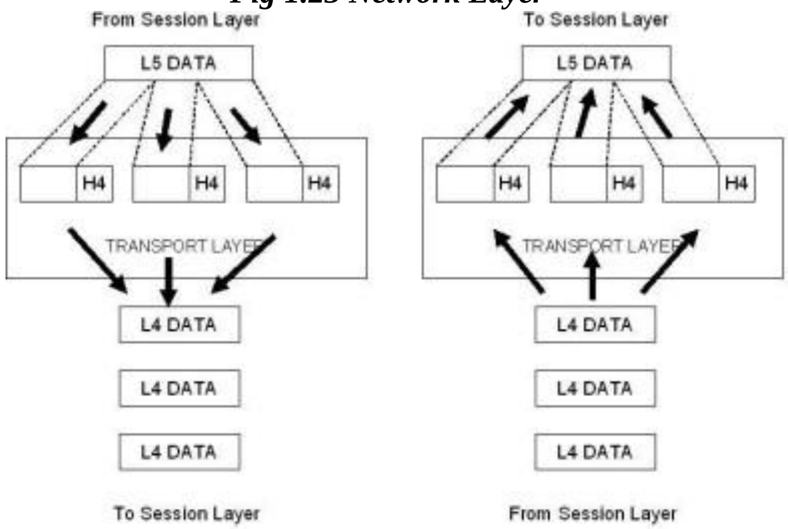


Fig 1.24 Transport Layer

The responsibilities are,

1. Service point Addressing: A single computer can often run several programs at the same time. The transport layer gets the entire message to the correct process on that computer. It adds a header that defines the port address which used to identify the exact process on the receiver.

2. Segmentation and Reassembly: A message is divided into manageable units called as segments. Each segment is reassembled after received that information at the receiver end. To make this efficient each segment contains a sequence number.

3. Connection Control: The transport layer creates a connection between the two end ports. It involves three steps. They are,

1. Connection establishment

2. Data transmission

3. Connection discard

4. Flow Control Flow control is performed at end to end level

5. Error Control Error control is performed at end to end level.

SESSION LAYER

It acts as a dialog controller. It establishes, maintains and synchronizes the interaction between the communication devices.

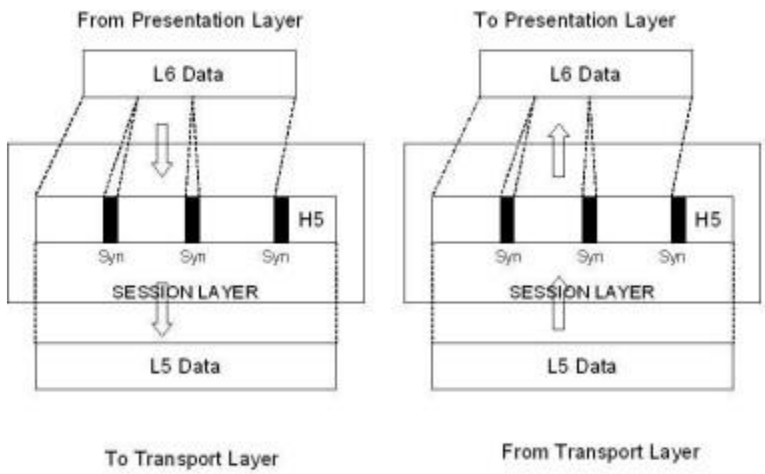


Fig 1.25 Session Layer

The responsibilities are,

1. Dialog Control: The session layer allows two systems to enter into a dialog. It allows the communication between the devices.

2. Synchronization: It adds a synchronization points into a stream of bits.

PRESENTATION LAYER

The presentation layer is responsible for the semantics and the syntax of the information exchanged.

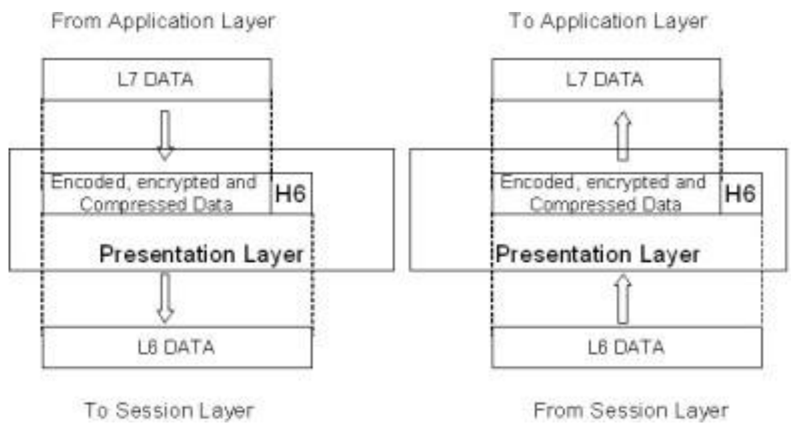


Fig 1.26 Presentation Layer

1. Translation: Different systems use different encoding systems. The presentation layer is responsible for interoperability between different systems. The presentation layer t the sender side translates the information from the sender dependent format to a common format. Likewise, at the receiver side presentation layer translate the information from common format to receiver dependent format.

2. Encryption: To ensure security encryption/decryption is used. Encryption means transforms the original information to another form. Decryption means retrieve the original information from the encrypted data

3. Compression: It used to reduce the number of bits to be transmitted.

APPLICATION LAYER

The application layer enables the user to access the network. It provides interfaces between the users to the network.

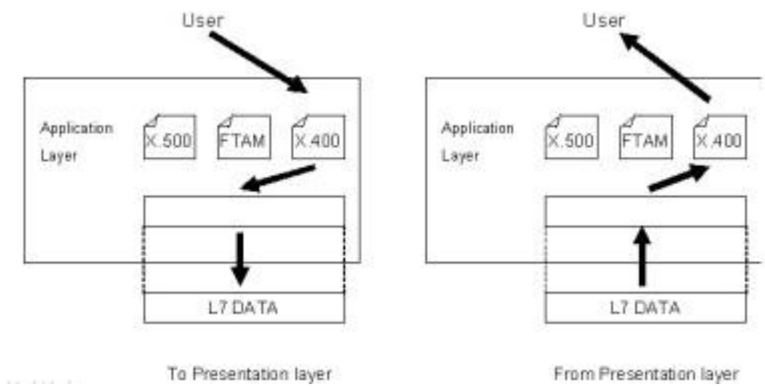


Fig 1.27 Application Layer

The responsibilities are,

1. Network Virtual Terminal: It is a software version of a physical terminal and allows a user to log on to a remote host.

2. File Transfer, Access, and Management: It allows a user to access files in a remote computer, retrieve files, and manage or control files in a remote computer.

3. Mail Services: It provides the basis for e-mail forwarding and storage.

4. Directory Services: It provides distributed database sources and access for global information about various objects and services.

1.12 TCP/IP REFERENCE MODEL

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.

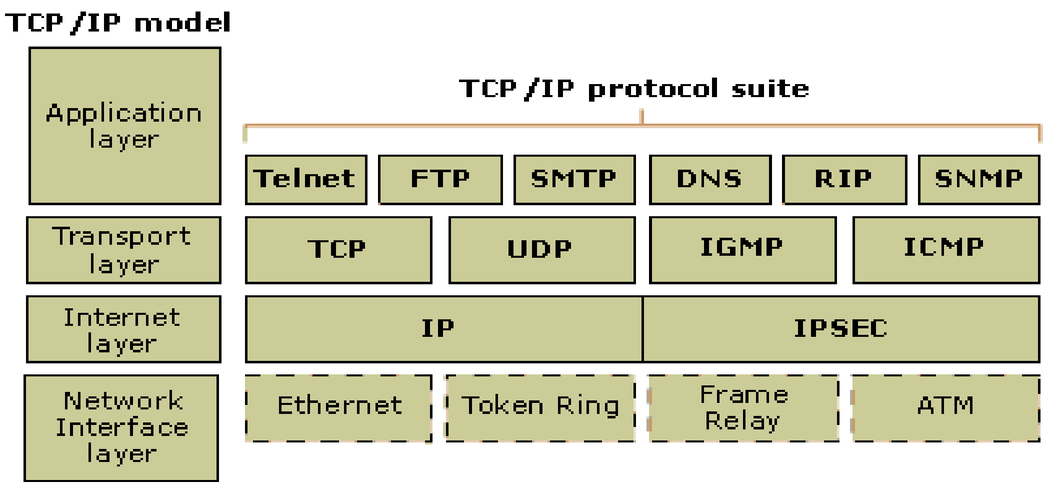


Fig 1.28 TCP/IP Model

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

6. The various functions performed by the Internet Layer are:
   - Delivering IP packets
   - Performing routing
   - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
   - **TCP (Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.

- **UDP (User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

TEXT / REFERENCE BOOKS

1. Andrew S Tanenbaum “Computer Networks” 5th Edition. Pearson Education/PH I/2011.

2. Behrouz A. Forouzan, “Data Communications and Networking” Fourth Edition, Mc GrawHill HIGHER Education 2007.

3. Michael A.Gallo, William Hancock.M, Brooks/Cole Computer Communications and Networking Technologies,2001

4. Richard Lai and Jirachief pattana, “Communication Protocol Specification and Verification”, Kluwer Publishers, Boston, 1998.

5. Pallapa Venkataram and Sunilkumar S.Manvi, “Communication protocol Engineering”, PHI Learning, 2008

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 ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – II DATA COMMUNICATION AND NETWORKING – SEC1306

UNIT II NETWORKING

2.1 NETWORK TOPOLOGIES

The term topology refers to the way a network is laid out, either physically or logically.

- Two or more devices connect to a link; two or more links form topology.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices to each other.
- There are five basic topologies possible :

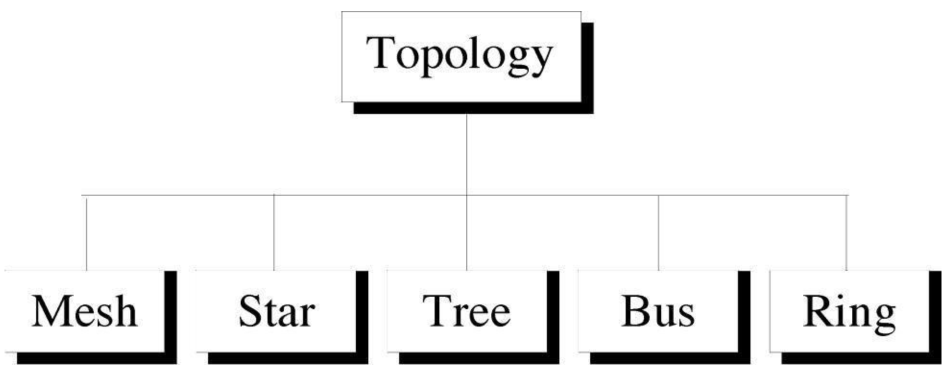


Fig 2.1 Types of Topologies

Mesh topology

- In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only

- Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

  - **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.

  - **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

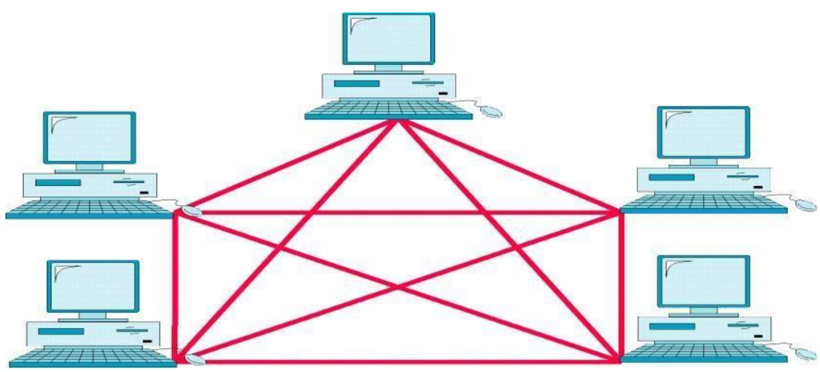


Fig 2.2 Partial Mesh Topology

Star topology

- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

  - Layer-1 device such as hub or repeater

  - Layer-2 device such as switch or bridge

  - Layer-3 device such as router or gateway

- As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails.

- Every communication between hosts, takes place through only the hub.
- Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

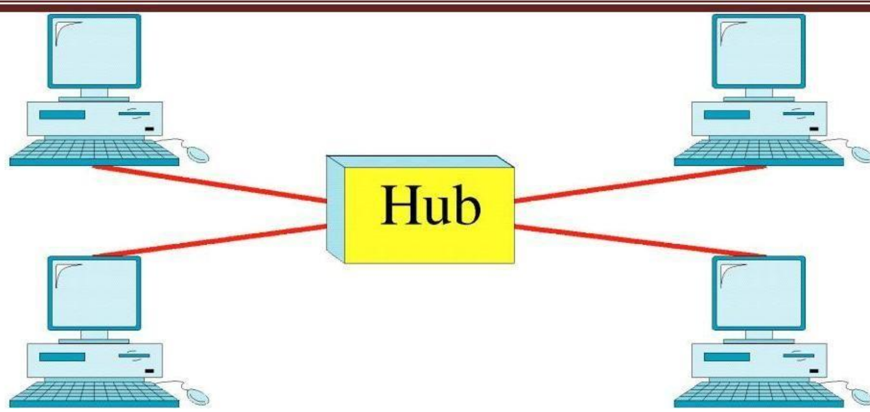


Fig 2.3 Star Topology

Tree Topology

- Nodes in a tree are linked to central hub that controls the traffic to the network.
- Not every device plugs directly to the central hub
- Majority of devices connected to secondary hub, that in turns connect to the central hub.
- The central hub in the tree is an active hub
- An active hub contains repeater
- The secondary hub may be active or passive
- A passive hub provides a simple physical connection between two attached devices.

- Repeater which is a hardware device that regenerates the received bit pattern before sending them out

- Repeating strengthens transmission and increases the distance a signal can travel.

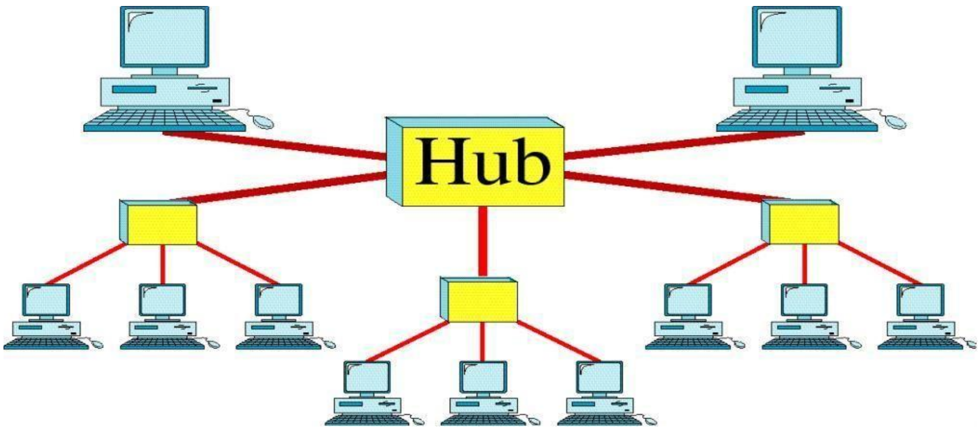


Fig 2.4 Tree Topology

Bus topology

- The bus topology is an example of multipoint configurations.

- One long cable acts as backbone, links all devices in the network.

- Nodes are connected to the bus cable by drop line and taps.

- A drop line is a connection running between the devices and the main cable.

- A tap is a connector that either splices in to the main cable or punctures the sheathing of a cable to create a contact with the metallic core

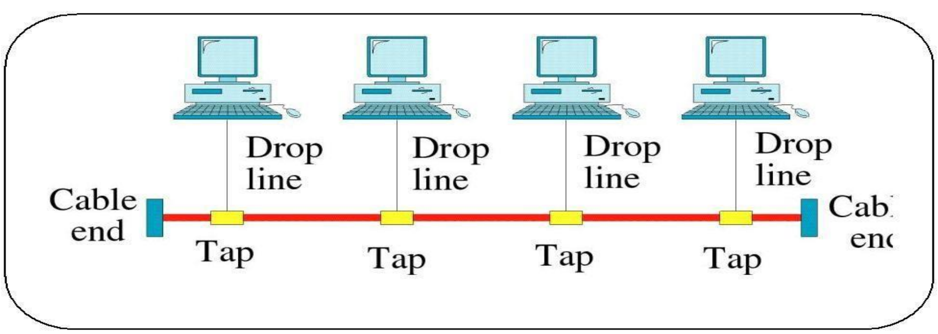


Fig 2.5 Bus Topology

Ring topology

- In a ring topology ,each device has a dedicated point-to-point line configuration only with the two devices on either side of it.

- A signal is passed along the ring in one direction, from a device to device, until it reaches its destination

- Each device in the ring incorporates a repeater .when a device receives a signal intended for another device ,its repeater regenerates the bits and passes them along

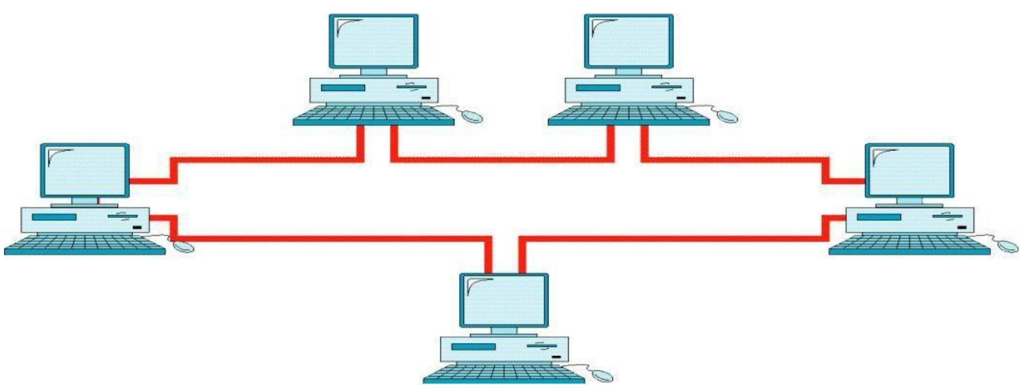


Fig 2.6 Ring Topology

2.2 STANDARDS IN NETWORKING

Standards are necessary in networking to ensure interconnectivity and interoperability

-

between various networking hardware and software components. Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.

Concept of Standard

Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity. Data communications standards are classified into two categories:

De facto Standard

These are the standards that have been traditionally used and mean **by fact** or **by convention** These standards are not approved by any organized body but are adopted by widespread use.

De jure standard

It means by **law** or **by regulation.** These standards are legislated and approved by an body that is officially recognized.

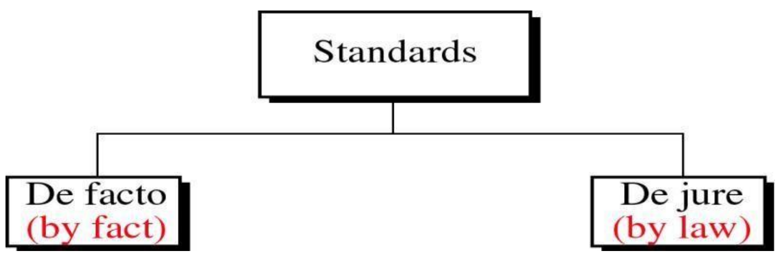


Fig 2.7 various standards

Standard Organizations in field of Networking

- Standards are created by standards creation committees, forums, and government regulatory agencies.

- **Examples of Standard Creation Committees** :
    1. International Organization for Standardization(ISO)

    2. International Telecommunications Union –

Telecommunications Standard (ITU-T)

3. American National Standards Institute (ANSI)

4. Institute of Electrical & Electronics Engineers (IEEE)

5. Electronic Industries Associates (EIA)

Examples of Forums

1. ATM Forum
2. MPLS Forum
3. Frame Relay Forum

Examples of Regulatory Agencies:

1. Federal Communications Committee (FCC)

IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks. More specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. By contrast, in cell relay networks data is transmitted in short, uniformly sized units called cells. Isochronous networks, where data is transmitted as a steady stream of octets, or groups of octets, at regular time intervals, are also out of the scope of this standard. The number 802 was simply the next free number IEEE could assign, though ―802‖ is sometimes associated with the date the first meeting was held — February 1980. The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named logical link control (LLC) and media access control (MAC), so the layers can be listed like this:

- Data link layer
    - LLC sublayer
    - MAC sublayer
- Physical layer

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual working group provides the focus for each area.

Wireless LAN and IEEE 802.11

A wireless LAN (WLAN or WiFi) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired network and a group of client computers, giving these users wireless access to the full resources and services of the corporate network across a building or campus setting. The widespread acceptance of WLANs depends on industry standardization to ensure product compatibility and reliability among the various manufacturers.

The 802.11 specification as a standard for wireless LANS was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in the year 1997. This version of 802.11 provides for 1 Mbps and 2 Mbps data rates and a set of fundamental signaling methods and other services. Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels the ISO model, the physical layer and link layer (see figure below). Any LAN application, network operating system, protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

The major motivation and benefit from Wireless LANs is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere.The other advantages for WLAN include cost-effective network setup for hard-to-wire locations such as older buildings and solid-wall structures and reduced cost of ownership-particularly in dynamic environments requiring frequent modifications, thanks to minimal wiring and installation costs per device and user. WLANs liberate users from dependence on hard-wired access to the network backbone, giving them anytime, anywhere network access. This freedom to roam offers numerous user benefits for a variety of work environments, such as:

- Immediate bedside access to patient information for doctors and hospital staff
- Easy, real-time network access for on-site consultants or auditors
- Improved database access for roving supervisors such as production line managers, warehouse auditors, or construction engineers
- Simplified network configuration with minimal MIS involvement for temporary setups such as trade shows or conference rooms

- Faster access to customer information for service vendors and retailers, resulting in better service and improved customer satisfaction
- Location-independent access for network administrators, for easier on-site troubleshooting and support
- Real-time access to study group meetings and research links for students

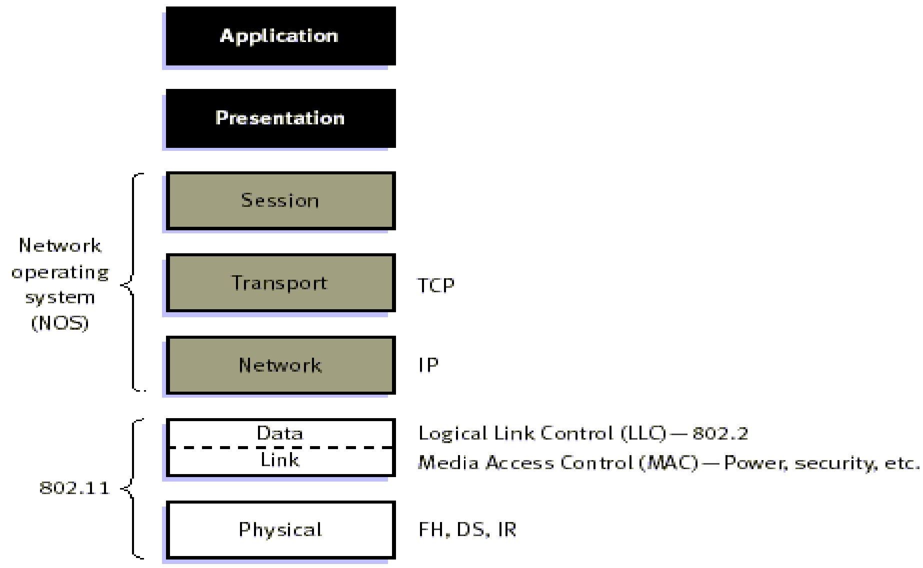


Fig 2.8 IEEE 802.11 and the ISO Model

Wireless sensor network (**WSN**) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on.

These are similar to **wireless ad hoc networks** in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. Sometimes they are called **dust networks**, referring to minute sensors as small as dust. **Smart dust** is a U C Berkeley project sponsored by DARPA. Dust Networks Inc., is one of the early companies that produced wireless sensor network products. WSNs are spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main locations. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

\

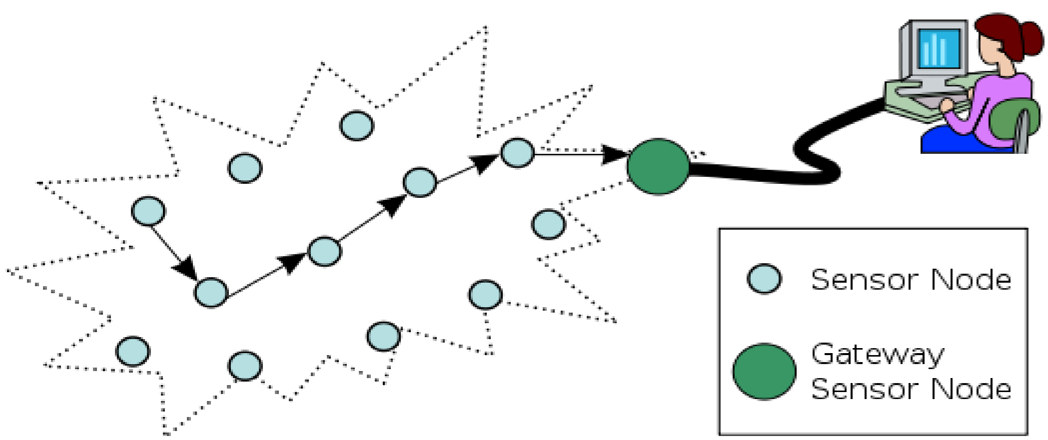


Fig 2.9 Layout WSN

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, SenSys, and EWSN.

Wireless Sensor Networks (WSNs)

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.WSN is a wireless network that consists of base stations and numbers of nodes (wireless sensors).These networks are used to monitor physical or environmental conditions like sound, pressure, temperature and co-operatively pass data through the network to a main location as shown in the figure.

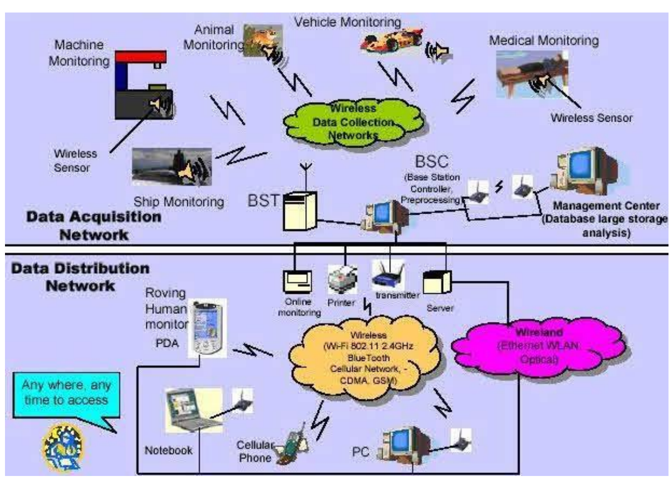


Fig 2.10 Applications

On the environment, the types of networks are decided so that those can be deployed underwater, underground, on land, and so on. Different types of WSNs include:

1. Terrestrial WSNs
2. Underground WSNs
3. Underwater WSNs
4. Multimedia WSNs
5. Mobile WSNs

1. Terrestrial WSNs

Terrestrial WSNs are capable of communicating base stations efficiently, and consist of hundreds to thousands of wireless sensor nodes deployed either in unstructured (ad hoc) or structured (Preplanned) manner. In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane. The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models.

In this WSN, the battery power is limited; however, the battery is equipped with solar cells as a secondary power source. The Energy conservation of these WSNs is achieved by using low duty cycle operations, minimizing delays, and optimal routing, and so on.

2. Underground WSNs

The underground wireless sensor networks are more expensive than the terrestrial WSNs in terms of deployment, maintenance, and equipment cost considerations and careful planning. The WSNs networks consist of a number of sensor nodes that are hidden in the ground to monitor underground conditions. To relay information from the sensor nodes to the base station, additional sink nodes are located above the ground.

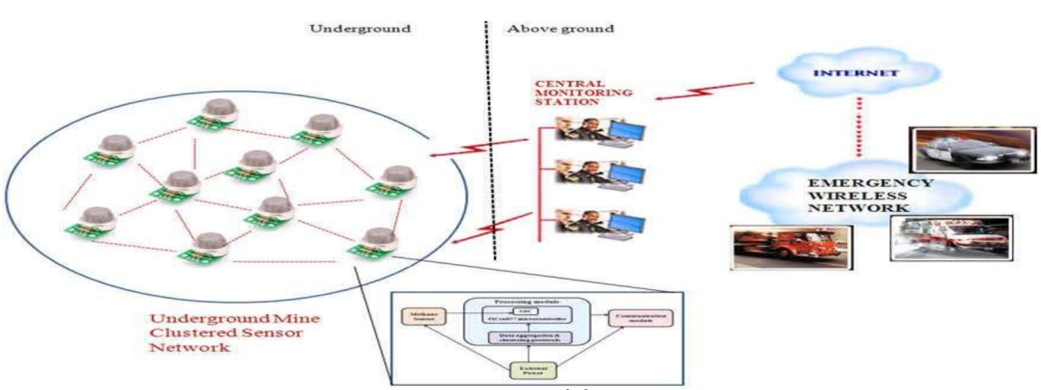


Fig2 .10 Underground WSN

The underground wireless sensor networks deployed into the ground are difficult to recharge. The sensor battery nodes equipped with a limited battery power are difficult to recharge. In addition to this, the underground environment makes wireless communication a challenge due to high level of attenuation and signal loss.

3. Under Water WSNs

More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Autonomous underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, and bandwidth and sensor failures.

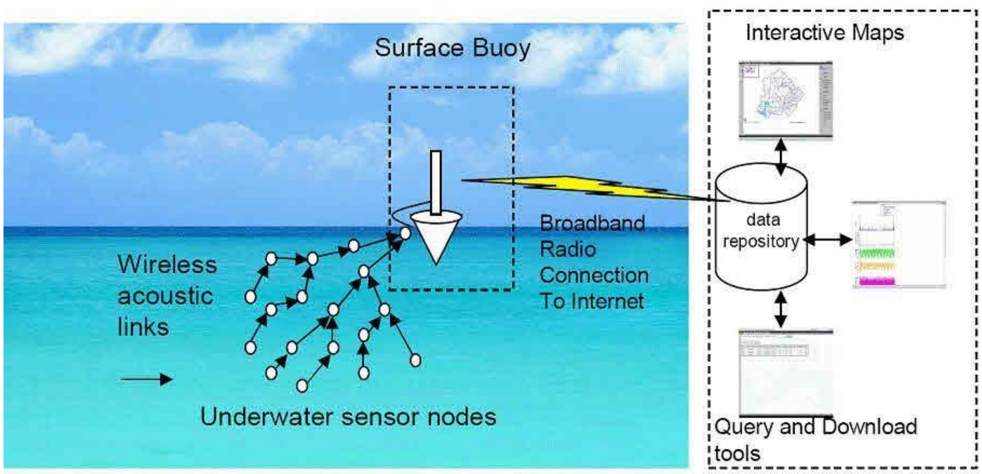


Fig 2.10 Underwater WSN

Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy conservation for under water WSNs involves the development of underwater communication and networking techniques.

4. Multimedia WSNs

Muttimedia wireless sensor networks have been proposed to enable tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio. These networks consist of low-cost sensor nodes equipped with micrpphones and cameras.These nodes are interconnected with each other over a wireless connection for data compression, data retrieval and correlation.

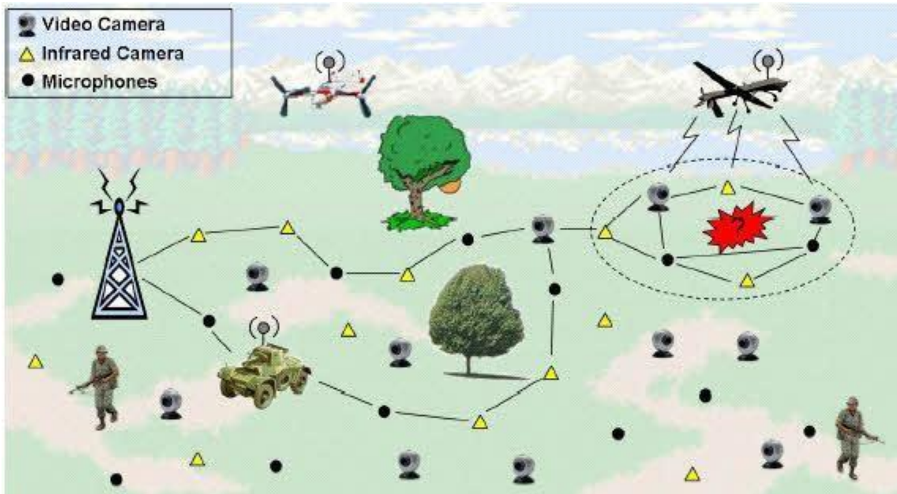


Fig 2.11 MultimediaWSN

The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.

5. Mobile WSNs

These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate.

The mobile wireless sensor networks are much more versatile than the static sensor networks. The advantages of MWSN over the static wireless sensor networks include better and improved coverage, better energy efficiency, superior channel capacity, and so on.

Limitations of Wireless Sensor Networks

1. Possess very little storage capacity – a few hundred kilobytes
2. Possess modest processing power-8MHz
3. Works in short communication range – consumes a lot of power
4. Requires minimal energy – constrains protocols
5. Have batteries with a finite life time

6. Passive devices provide little energy

2.3 UMTS ARCHITECTURE

The UMTS architecture is required to provide a greater level of performance to that of the original GSM network. However as many networks had migrated through the use of GPRS and EDGE, they already had the ability to carry data. Accordingly many of the elements required for the WCDMA / UMTS network architecture were seen as a migration. This considerably reduced the cost of implementing the UMTS network as many elements were in place or needed upgrading.

With one of the major aims of UMTS being to be able to carry data, the UMTS network architecture was designed to enable a considerable improvement in data performance over that provided for GSM.

UMTS network constituents

The UMTS network architecture can be divided into three main elements:

1. ***User Equipment (UE):*** The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. The new name was chosen because the considerably greater functionality that the UE could have. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.
2. ***Radio Network Subsystem (RNS):*** The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface for the overall network.
3. ***Core Network:*** The core network provides all the central processing and management for the system. It is the equivalent of the GSM Network Switching Subsystem or NSS.

The core network is then the overall entity that interfaces to external networks including the public phone network and other cellular telecommunications networks.

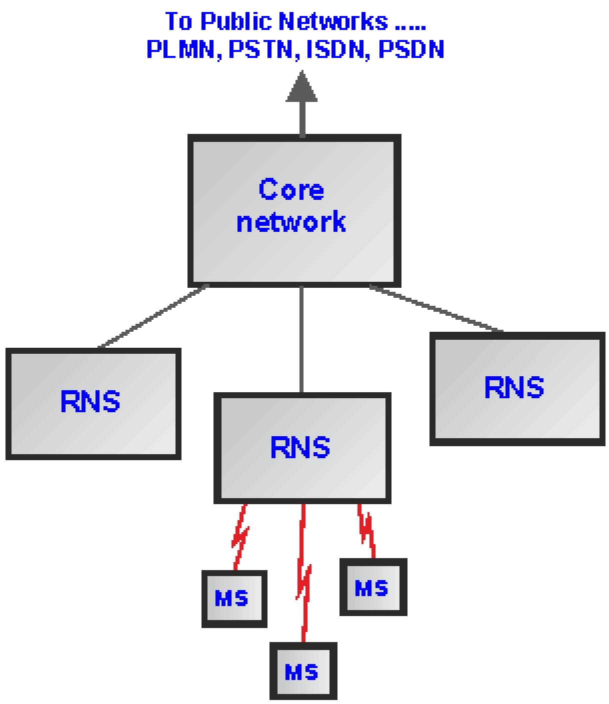


Fig 2.12 UMTS Network Architecture Overview

User Equipment, UE

The USER Equipment or UE is a major element of the overall 3G UMTS network architecture. It forms the final interface with the user. In view of the far greater number of applications and facilities that it can perform, the decision was made to call it a user equipment rather than a mobile. However it is essentially the handset (in the broadest terminology), although having access to much higher speed data communications, it can be much more versatile, containing many more applications. It consists of a variety of different elements including RF circuitry, processing, antenna, battery, etc.

There are a number of elements within the UE that can be described separately:

- ***UE RF circuitry:*** The RF areas handle all elements of the signal, both for the receiver and for the transmitter. One of the major challenges for the RF power amplifier was to reduce the power consumption. The form of modulation used for W-CDMA requires the use of a linear amplifier. These inherently take more current than non linear amplifiers which can be used for the form of modulation used on GSM. Accordingly to maintain battery life, measures were introduced into many of the designs to ensure the optimum efficiency.

- ***Baseband processing:*** The base-band signal processing consists mainly of digital circuitry. This is considerably more complicated than that used in phones for previous generations. Again this has been optimised to reduce the current consumption as far as possible.
- ***Battery:*** While current consumption has been minimised as far as possible within the circuitry of the phone, there has been an increase in current drain on the battery. With users expecting the same lifetime between charging batteries as experienced on the previous generation phones, this has necessitated the use of new and improved battery technology. Now Lithium Ion (Li-ion) batteries are used. These phones to remain small and relatively light while still retaining or even improving the overall life between charges.
- ***Universal Subscriber Identity Module, USIM:*** The UE also contains a SIM card, although in the case of UMTS it is termed a USIM (Universal Subscriber Identity Module). This is a more advanced version of the SIM card used in GSM and other systems, but embodies the same types of information. It contains the International Mobile Subscriber Identity number (IMSI) as well as the Mobile Station International ISDN Number (MSISDN). Other information that the USIM holds includes the preferred language to enable the correct language information to be displayed, especially when roaming, and a list of preferred and prohibited Public Land Mobile Networks (PLMN).

  The USIM also contains a short message storage area that allows messages to stay with the user even when the phone is changed. Similarly "phone book" numbers and call information of the numbers of incoming and outgoing calls are stored.

The UE can take a variety of forms, although the most common format is still a version of a "mobile phone" although having many data capabilities. Other broadband dongles are also being widely used.

UMTS Radio Network Subsystem

This is the section of the 3G UMTS / WCDMA network that interfaces to both the UE and the core network. The overall radio access network, i.e. collectively all the Radio Network Subsystem is known as the UTRAN UMTS Radio Access Network.

The radio network subsystem is also known as the UMTS Radio Access Network or UTRAN.

3G UMTS Core Network

The 3G UMTS core network architecture is a migration of that used for GSM with further elements overlaid to enable the additional functionality demanded by UMTS.

In view of the different ways in which data may be carried, the UMTS core network may be split into two different areas:

- ***Circuit switched elements:*** These elements are primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.
- ***Packet switched elements:*** These network entities are designed to carry packet data. This enables much higher network usage as the capacity can be shared and data is carried as packets which are routed according to their destination.

Some network elements, particularly those that are associated with registration are shared by both domains and operate in the same way that they did with GSM.

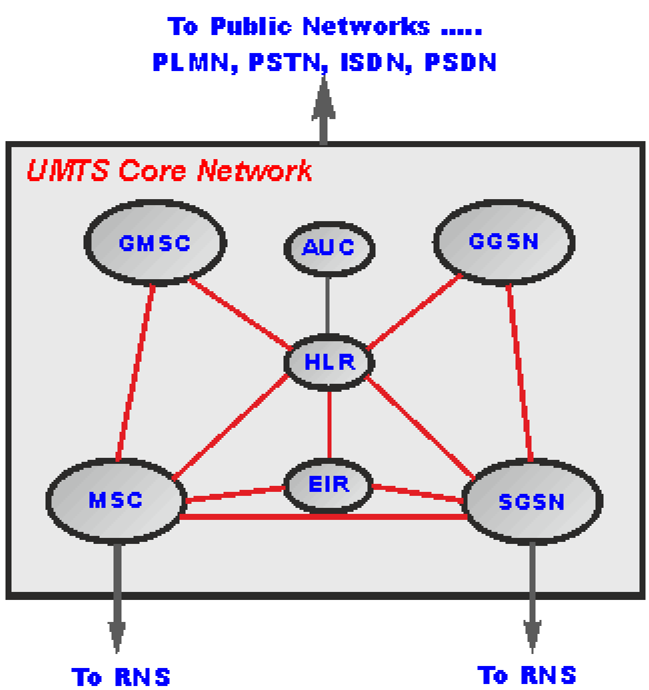


Fig 2.13 UMTS Core Network

Circuits witched elements

The circuit switched elements of the UMTS core network architecture include the following network entities:

- ***Mobile switching centre (MSC):*** This is essentially the same as that within GSM, and it manages the circuit switched calls under way.

- ***Gateway MSC (GMSC):*** This is effectively the interface to the external networks.

Packet switched elements

The packet switched elements of the 3G UMTS core network architecture include the following network entities:

- ***Serving GPRS Support Node (SGSN):*** As the name implies, this entity was first developed when GPRS was introduced, and its use has been carried over into the UMTS network architecture. The SGSN provides a number of functions within the UMTS network architecture.
    - Mobility management When a UE attaches to the Packet Switched domain of the UMTS Core Network, the SGSN generates MM information based on the mobile's current location.
    - Session management: The SGSN manages the data sessions providing the required quality of service and also managing what are termed the PDP (Packet data Protocol) contexts, i.e. the pipes over which the data is sent.
    - Interaction with other areas of the network: The SGSN is able to manage its elements within the network only by communicating with other areas of the network, e.g. MSC and other circuit switched areas.
    - Billing: The SGSN is also responsible billing. It achieves this by monitoring the flow of user data across the GPRS network. CDRs (Call Detail Records) are generated by the SGSN before being transferred to the charging entities (Charging Gateway Function, CGF).
- ***Gateway GPRS Support Node (GGSN):*** Like the SGSN, this entity was also first introduced into the GPRS network. The Gateway GPRS Support Node (GGSN) is the central element within the UMTS packet switched network. It handles inter-working between the UMTS packet switched network and external packet switched networks, and can be considered as a very sophisticated router. In operation, when the GGSN receives data addressed to a specific user, it checks if the user is active and then forwards the data to the SGSN serving the particular UE.

Shared elements

The shared elements of the UMTS core network architecture include the following network entities:

- **Home location register (HLR):** This database contains all the administrative information about each subscriber along with their last known location. In this way, the UMTS network is able to route calls to the relevant RNC / Node B. When a user switches on their UE, it registers with the network and from this it is possible to determine which Node B it communicates with so that incoming calls can be routed appropriately. Even when the UE is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position with their current or last known location on the network.
- **Equipment identity register (EIR):** The EIR is the entity that decides whether a given UE equipment may be allowed onto the network. Each UE equipment has a number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration.
- **Authentication centre (AuC) :** The AuC is a protected database that contains the secret key also contained in the user's USIM card.

IEEE STANDARDS

The relationship of the 802 Standard to the traditional OSI model is shown in the figure. The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.

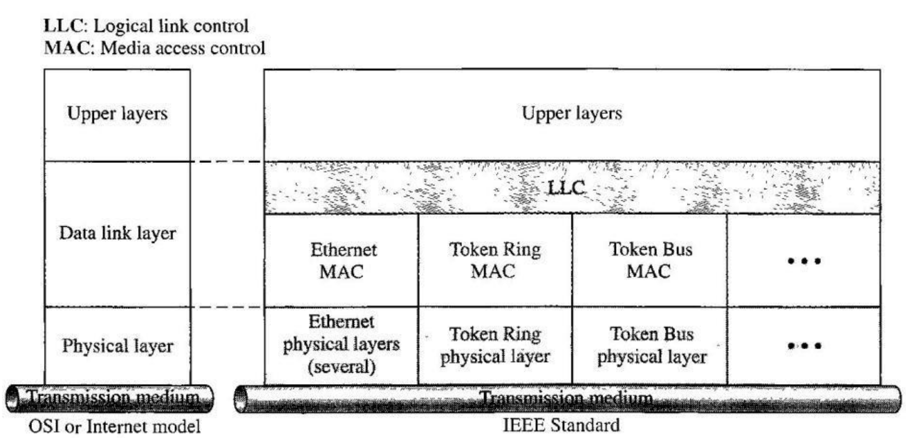


Fig 2.14 IEEE Standards

Data Link Layer

The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

Logical Link Control (LLC)

In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MACsublayer.

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

Framing LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source Gif

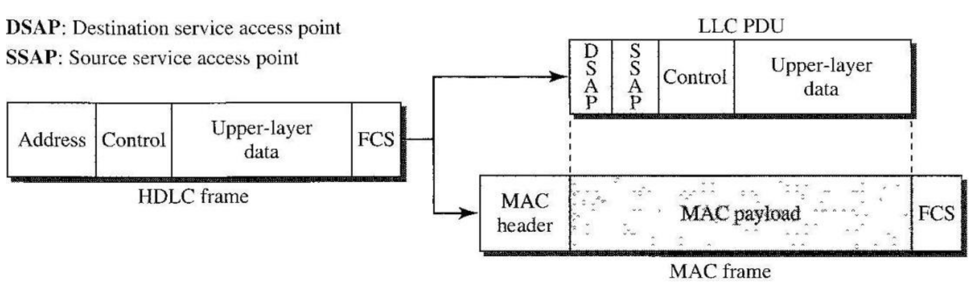


Fig 2.14 Framing

service access point (SSAP). The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in figure.

Need for LLC The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper-layer protocols such as IP, do not use the services of LLC.

Media Access Control (MAC)

IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token-passing method for Token Ring and Token Bus LANs. Part of the framing function is also handled by the MAC layer.In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

Physical Layer

The physical layer is dependent on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there is only one MAC sublayer for Standard Ethernet, there is a different physical layer specification for each Ethernet implementations.

Key features of LANs are summarized below:

- Limited geographical area – which is usually less than 10 Km and more than 1 m.
- High Speed – 10 Mbps to 1000 Mbps (1 Gbps) and more
- High Reliability – 1 bit error in 10^{11} bits.
- Transmission Media – Guided and unguided media, mainly guided media is used; except in a situation where infrared is used to make a wireless LAN in a room.
- Topology – It refers to the ways in which the nodes are connected. There are various topologies used.
- Medium-Access Control Techniques –Some access control mechanism is needed to decide which station will use the shared medium at a particular point in time. In this lesson we shall discuss various LAN standards proposed by the IEEE 8.2 committee with the following goals in mind:

- To promote compatibility

- Implementation with minimum efforts
- Accommodate the need for diverse applications

For the fulfillment of the abovementioned goals, the committee came up with a bunch of LAN standards collectively known as IEEE 802 LANs as shown in Fig. 5.3.1. To satisfy diverse requirements, the standard includes CSMA/CD, Token bus, Token
Ring medium access control techniques along with different topologies. All these standards differ at the physical layer and MAC sublayer, but are compatible at the data link layer.

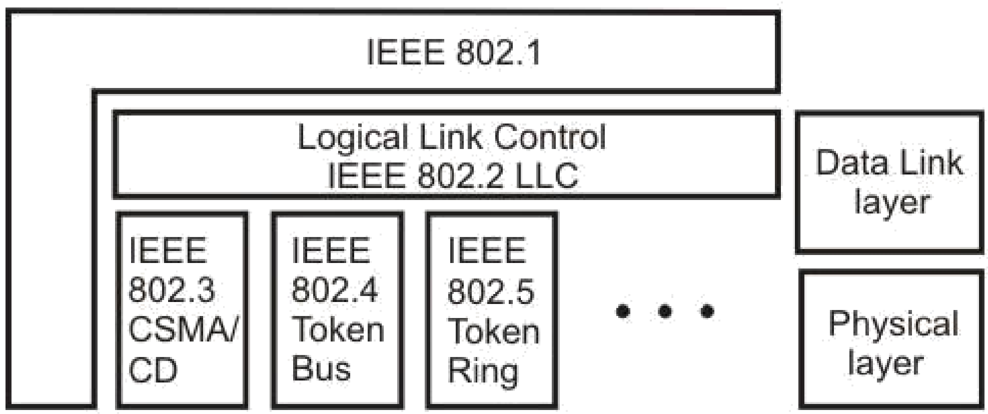


Figure 2.15 IEEE 802 Legacy LANs

The **802.1** sublayer gives an introduction to set of standards and gives the details of the interface primitives. It provides relationship between the OSI model and the 802 standards. The **802.2** sublayer describes the **LLC** (logical link layer), which is the upper part of the data link layer. LLC facilitate error control and flow control for reliable communication. It appends a header containing sequence number and acknowledgement number. And offers the following three types of services:

- Unreliable datagram service
- Acknowledged datagram service
- Reliable connection oriented service

The standards 802.3, 802.4 and 802.5 describe three LAN standards based on the CSMA/CD, token bus and token ring, respectively. Each standard covers the physical layer and MAC sublayer protocols. In the following sections we shall focus on these three LAN standards.

IEEE 802.3 and Ethernet

Ethernet - A Brief History

The original Ethernet was developed as an experimental coaxial cable network in the 1970s by Xerox Corporation to operate with a data rate of 3 Mbps using a carrier sense multiple access collision detection (CSMA/CD) protocol for LANs with sporadic traffic requirements. Success with that project attracted early attention and led to the 1980 joint development of the 10-Mbps Ethernet Version 1.0 specification by the three-company consortium: Digital Equipment Corporation, Intel Corporation, and Xerox Corporation.

The original IEEE 802.3 standard was based on, and was very similar to, the Ethernet Version 1.0 specification. The draft standard was approved by the 802.3 working group in 1983 and was subsequently published as an official standard in 1985 (ANSI/IEEE Std.

802.3-1985). Since then, a number of supplements to the standard have been defined to take advantage of improvements in the technologies and to support additional network media and higher data rate capabilities, plus several new optional network access control features. From then onwards, the term *Ethernet* refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps—10Base-T Ethernet
- 100 Mbps—Fast Ethernet
- 1000 Mbps—Gigabit Ethernet

Ethernet has survived as the major LAN technology (it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations) because its protocol has the following characteristics:

- It is easy to understand, implement, manage, and maintain
- It allows low-cost network implementations
- It provides extensive topological flexibility for network installation
- It guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer

Ethernet Architecture

Ethernet architecture can be divided into two layers:

➢ **Physical layer:** this layer takes care of following functions.

- Encoding and decoding
- Collision detection
- Carrier sensing
- Transmission and receipt

➢ **Data link layer:** Following are the major functions of this layer.

- Station interface
- Data Encapsulation /Decapsulation
- Link management
- Collision Management

STANDARD ETHERNET

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (10 t Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps), as shown in the figure:

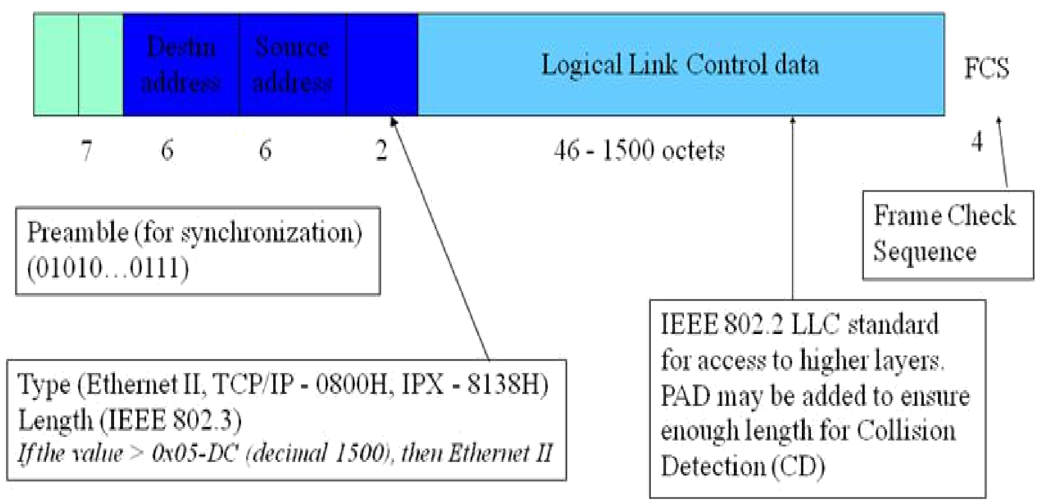


Figure 2.16 IEEE 802 Legacy LANs

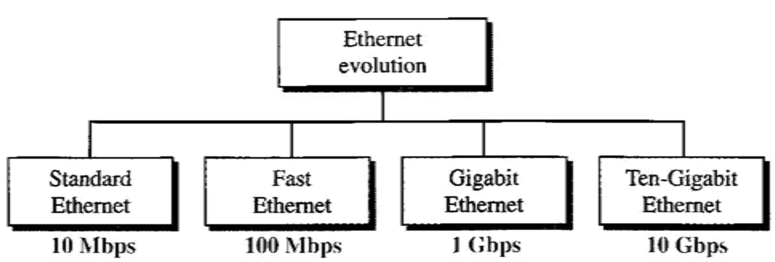


Fig 2.17 Ethernet Evolution

MAC Sublayer

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

Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.

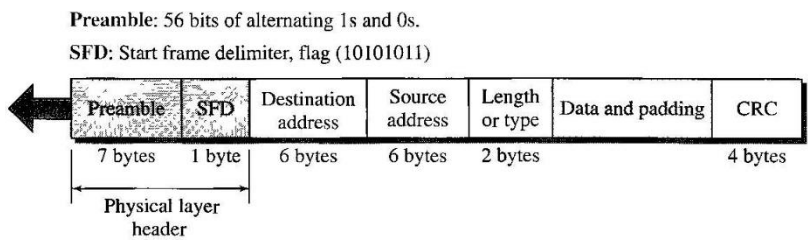


Fig 2.18 Frame Format

Acknowledgments must be implemented at the higher layers. The format of the MAC frame is shown in the figure.

- **Preamble**. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.
- **Destination address (DA)**. The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Source address (SA)**. The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **Length or type**. This field is defined as a type field or length field. The original Ethernet

used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field.

- **Data**. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

- **CRC**. The last field contains error detection information, in this case a CRC-32.

Frame Length

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

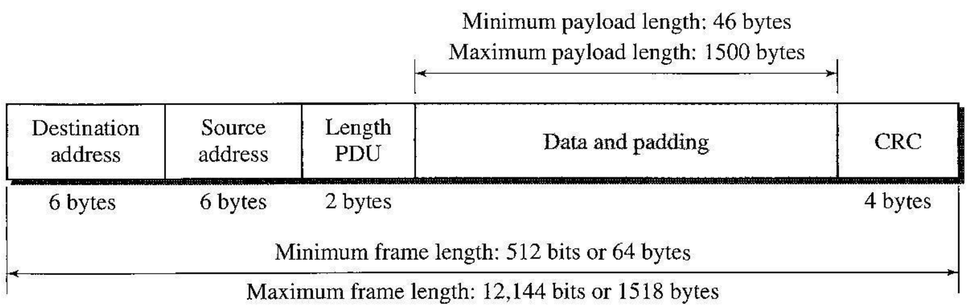


Fig 2.18 Frame Length

The minimum length restriction is required for the correct operation of CSMA/CD. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Addressing

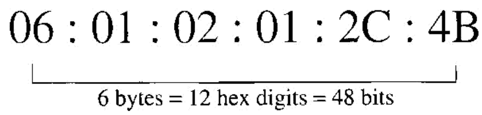


Fig 2.19 Addressing

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

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

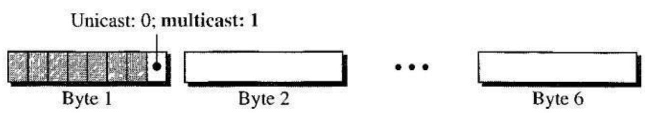


Fig 2.20 Frame Format

A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one4o-many. The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight

Access Method: CSMA/CD

Standard Ethernet uses 1-persistent CSMA/CD

Slot Time In an Ethernet network, the round-trip time required for a frame to travel from one end of a maximum-length network to the other plus the time needed to send the jam sequence is called the slot time.

Slot time = round-trip time + time required to send the jam sequence

The slot time in Ethernet is defined in bits. It is the time required for a station to send 512 bits. This means that the actual slot time depends on the data rate; for traditional 10-Mbps Ethernet it is 51.2μs.

Slot Time and Collision The choice of a 512-bit slot time was not accidental. It was chosen to allow the proper functioning of CSMA/CD. To understand the situation, let us consider two cases.

In the first case, we assume that the sender sends a minimum-size packet of 512 bits. Before the sender can send the entire packet out, the signal travels through the network and reaches the end of the network. If there is another signal at the end of the network (worst case), a collision occurs. The sender has the opportunity to abort the sending of the frame and to send a jam sequence to inform other stations of the collision. The roundtrip time plus the time required to send the jam sequence should be less than the time needed for the sender to send the minimum frame, 512 bits. The sender needs to be aware of the collision before it is too late, that is, before it has sent the entire frame.

In the second case, the sender sends a frame larger than the minimum size (between 512 and 1518 bits). In this case, if the station has sent out the first 512 bits and has not heard a

$$\text{MaxLength} = \text{PropagationSpeed} \times \frac{\text{SlotTime}}{2}$$

$$\text{MaxLength} = (2 \times 10^{8}) \times (51.2 \times 10^{-6} / 2) = 5120\text{ m}$$

collision, it is guaranteed that collision will never occur during the transmission of this frame. The reason is that the signal will reach the end of the network in less than one-half the slot time. If all stations follow the CSMA/CD protocol, they have already sensed the existence of the signal (carrier) on the line and have refrained from sending. If they sent a signal on the line before one-half of the slot time expired, a collision has occurred and the sender has sensed the collision. In other words, collision can only occur during the first half of the slot time, and if it does, it can be sensed by the sender during the slot time. This means that after the sender sends the first 512 bits, it is guaranteed that collision will not occur during the transmission of this frame. The medium belongs to the sender, and no other station will use it. In other words, the sender needs to listen for a collision only during the time the first 512 bits are sent.

Slot Time and Maximum Network Length There is a relationship between the slot time and the maximum length of the network (collision domain). It is dependent on the propagation speed of the signal in the particular medium. In most transmission media, the signal propagates at 2 x

108 m/s (two-thirds of the rate for propagation in air). For traditional Ethernet, we calculate Of course, we need to consider the delay times in repeaters and interfaces, and the time required to send the jam sequence. These reduce the maximum-length of a traditional Ethernet network to 2500 m, just 48 percent of the theoretical calculation.

MaxLength = 2500 m

Physical Layer

The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in figure.Because Ethernet devices implement only the bottom two layers of the OSI protocol stack, they are typically implemented as network interface cards (NICs) that plug into the host device's motherboard, or presently built-in in the motherboard. Various types cabling supported by the standard are shown in Fig. 5.3.2. The naming convention is a concatenation of three terms indicating the transmission rate, the transmission method, and the media type/signal encoding. Consider for example, 10Base-T. where 10 implies transmission rate of 10 Mbps, Base represents that it uses baseband signaling, and T refers to twisted-pair cables as transmission media. Various standards are discussed below:

Encoding and Decoding

All standard implementations use digital signaling (baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data. The figure shows the encoding scheme for Standard Ethernet.

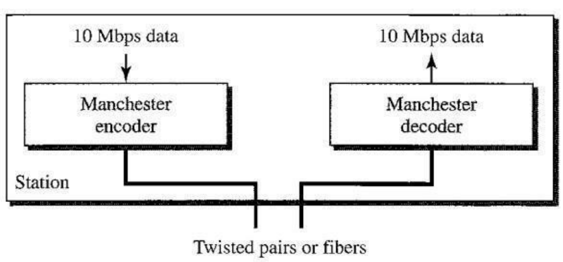


Fig 2.21 Encoding and Decoding

10Base5: Thick Ethernet

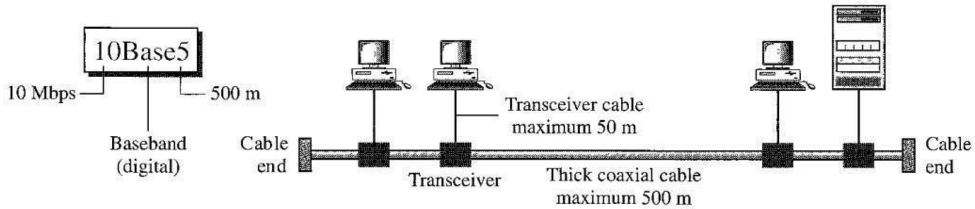


Fig 2.22 Thick Ethernet

10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable. The transceiver is responsible for transmitting, receiving, and detecting collisions.The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive degradation of the signal. If a length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

10Base2: Thin Ethernet

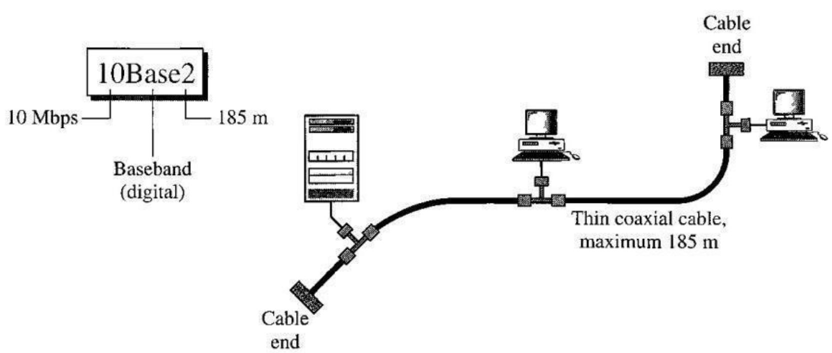


Fig 2.23 Thin Ethernet

10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

10Base- T: Twisted-Pair Ethernet

The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.

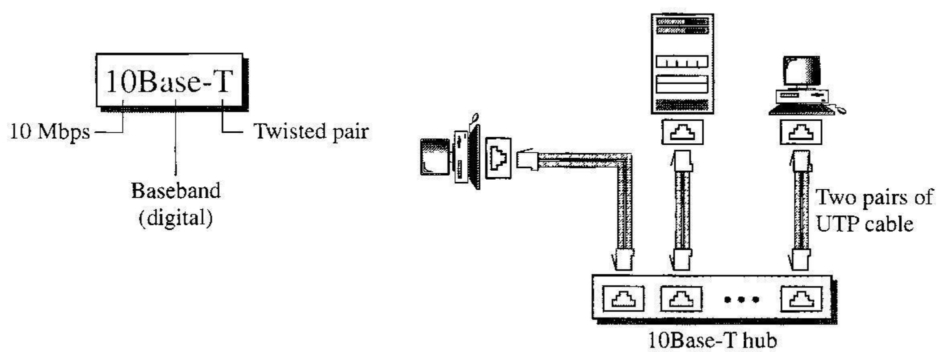


Fig 2.24 Twisted Pair Ethernet

Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

10Base-F: Fiber Ethernet

10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables.

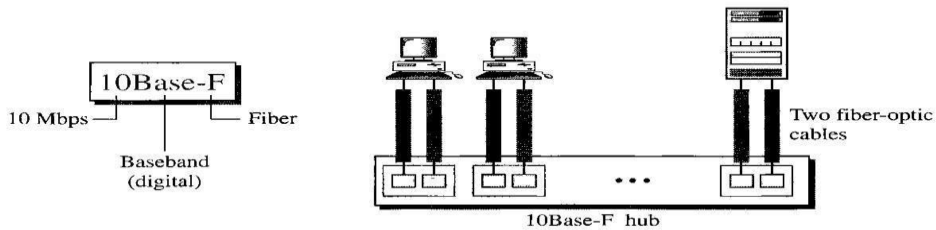


Fig 2.25 Fibre Ethernet

No Need for CSMA/CD

In full-duplex switched Ethernet, there is no need for the CSMA/CD method. In a full- duplex switched Ethernet, each station is connected to the switch via two separate links. Each station or switch can send and receive independently without worrying about collision. Each link is a point-to-point dedicated path between the station and the switch. There is no longer a need for carrier sensing; there is no longer a need for collision detection. The job of the MAC layer becomes much easier. The carrier sensing and collision detection functionalities of the MAC sublayer can be turned off.

MAC Control Layer

Standard Ethernet was designed as a connectionless protocol at the MAC sublayer. There is no explicit flow control or error control to inform the sender that the

frame has arrived at the destination without error. When the receiver receives the frame, it does not send any positive or negative acknowledgment.

To provide for flow and error control in full-duplex switched Ethernet, a new sublayer, called the MAC control, is added between the LLC sublayer and the MAC sublayer.

□

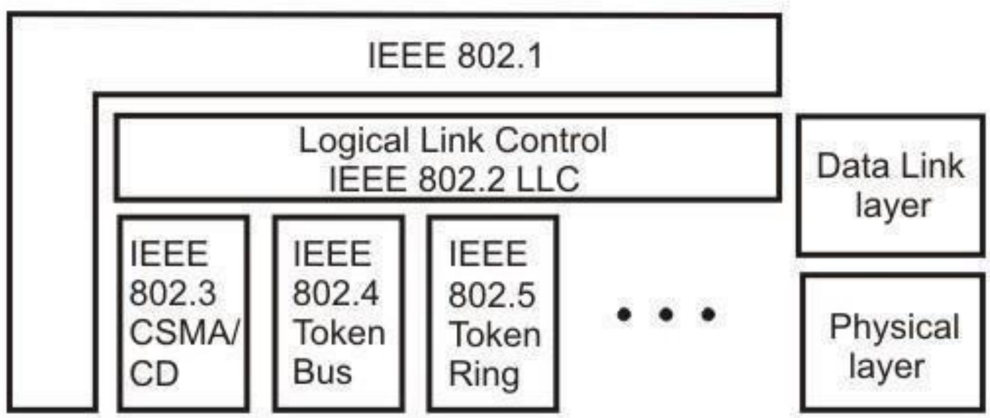


Fig2.26 IEEE 802 Legacy LANs

Token Ring (IEEE 802.5)

Token Ring: A Brief History

Originally, IBM developed Token Ring network in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and on the same lines. The term *Token Ring* is generally used to refer to both IBM's Token Ring network and IEEE 802.5 networks.

Before going into the details of the Token Ring protocol, let's first discuss the motivation behind it. As already discussed, the medium access mechanism used by Ethernet (CSMA/CD) may results in collision. Nodes attempt to a number of times before they can actually transmit, and even when they start transmitting there are chances to encounter collisions and entire transmission need to be repeated. And all this become worse one the traffic is heavy i.e. all nodes have some data to transmit. Apart from this there is no way to predict either the occurrence of collision or delays produced by multiple stations attempting to capture the link at the same time. So all these problems with the Ethernet gives way to an alternate LAN technology, Token Ring.

Token Ring and IEEE802.5 are based on token passing MAC protocol with ring topology. They resolve the uncertainty by giving each station a turn on by one. Each node takes turns sending the data; each station may transmit data during its turn. The technique that coordinates this turn mechanism is called Token passing; as a Token is passed in the network and the station that gets the token can only transmit. As one node transmits at a time, there is no chance of collision. We shall discuss the detailed operation in next section.

Stations are connected by point-to-point links using repeaters. Mainly these links are of shielded twisted-pair cables. The repeaters function in two basic modes: Listen mode, Transmit mode. A disadvantage of this topology is that it is vulnerable to link or station failure. But a few measures can be taken to take care of it.

TEXT / REFERENCE BOOKS

1. Andrew S Tanenbaum "Computer Networks" 5th Edition. Pearson Education/PH I/2011.
2. Behrouz A. Forouzan, "Data Communications and Networking" Fourth Edition, Mc GrawHill HIGHER Education 2007.
3. Michael A.Gallo, William Hancock.M, Brooks/Cole Computer Communications and Networking Technologies,2001
4. Richard Lai and Jirachief pattana, "Communication Protocol Specification and Verification", Kluwer Publishers, Boston, 1998.
5. Pallapa Venkataram and Sunilkumar S.Manvi, "Communication protocol Engineering", PHI Learning, 2008

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 ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – III DATA COMMUNICATION AND NETWORKING – SEC1306

UNIT III PHYSICAL LAYER AND DATALINK LAYER

Design Factors for Transmission Media

Bandwidth: All other factors remaining constant, the greater the band-width of a signal, the higher the data rate that can be achieved.

Transmission impairments: Limit the distance a signal can travel.

Interference: Competing signals in overlapping frequency bands can distort or wipe out a signal.

Number of receivers: Each attachment introduces some attenuation and distortion, limiting distance and/or data rate.

TYPES OF TRANSMISSION MEDIA

1. **Conducted or Guided Media** :

Use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver.

2. **Wireless or Unguided Media**:

Use radio waves of different frequencies and do not need a wire or cable conductor to transmit signals.

Guided Transmission Media

Guided media includes everything that 'guides' the transmission. That usually takes the form of some sort of a wire. Usually copper, but can also be an optical fiber.

Transmission capacity depends on the distance and on whether the medium is point-to-point or multipoint. Ex: twisted pair wires, coaxial cables, optical fiber

Twisted Pair Wires

A transmission medium consisting of pairs of twisted copper wires arranged in a regular spiral pattern to minimize the electromagnetic interference between adjacent pairs .Often used at customer facilities and also over distances to carry voice as well as data communications .Low frequency transmission medium.

We can transmit 1 Mbps over short distances (less than 100m). They are mainly used to transmit analog signals, but they can be used for digital signals.

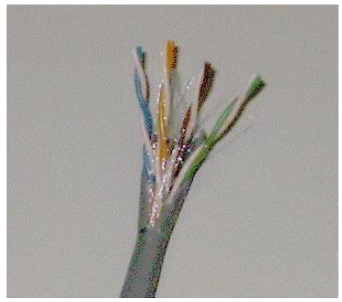


Figure 3.1 Twisted pair Cable

Twisted Pair Advantages

- Inexpensive and readily available Flexible and light weight
- Easy to work with and install

Twisted Pair Disadvantages

- Susceptibility to interference and noise Attenuation problem
- For analog, repeaters needed every 5-6km
- For digital, repeaters needed every 2-3km relatively low bandwidth (3000Hz)

Applications

They are used in telephone lines to provide voice and data channels. Local area networks, such as 10 Base-T and 100 Base-T also use twisted-pair cables.

Coaxial Cable (or Coax)

- In its simplest form, coaxial consists of a core made of solid copper surrounded by insulation, a braided metal shielding, and an outer cover.
- A transmission medium consisting of thickly insulated copper wire, which can transmit a large volume of data than twisted wire.

Coax Advantages

Higher bandwidth

- to 600MHz

- up to 10,800 voice conversations

Much less susceptible to interference than twisted pair

Coax Disadvantages

High attenuation rate makes it expensive over
long distance Bulky

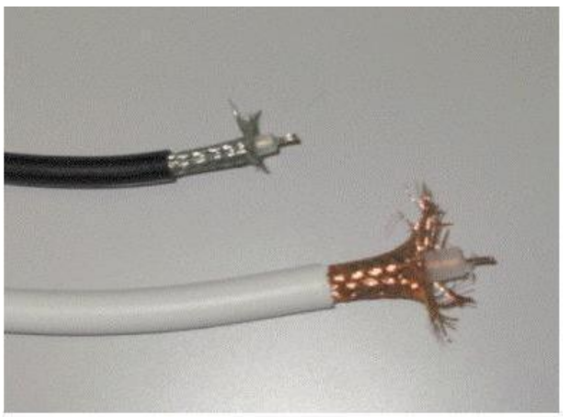


Figure 3.2 Coaxial Cable

Applications

- It is used in cable TV networks
- It is used in traditional Ethernet LANs.

Fiber Optic Cable

Relatively new transmission medium used by telephone companies in place of long-distance trunk lines also used by private companies in implementing local data communications networks

Require a light source with injection laser diode (ILD) or light-emitting diodes (LED) Optical fiber consists of a glass core, surrounded by a glass cladding with slightly lower refractive index.

In most networks fiber-optic cable is used as the high-speed backbone, and twisted wire and coaxial cable are used to connect the backbone to individual devices.

Fiber Optic Advantages

- Greater capacity (bandwidth of up to 2 Gbps). Smaller size and lighter weight.
- Lower attenuation.
- Immunity to environmental interference.
- Highly secure due to tap difficulty and lack of signal radiation.

Fiber Optic Disadvantages

- expensive over short distance
- requires highly skilled installers
- adding additional nodes is difficult

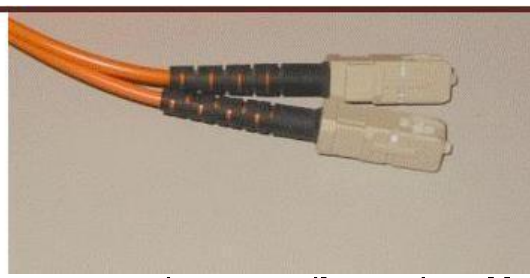


Figure 3.3 Fiber Optic Cable

Applications

- The fiber optic cable is often found in backbone networks because its bandwidth is cost effective.
- Used in TV companies.
- LAN such as 100 Base-FX Network

Wireless (Unguided Media) Transmission

Transmission and reception are achieved by means of an antenna directional

- transmitting antenna puts out focused beam
- transmitter and receiver must be aligned omni directional
- signal spreads out in all directions
- can be received by many antennas

Wireless Examples

Terrestrial microwave, satellite microwave, broadcast radio ,infrared

Microwaves

Electromagnetic waves having frequency between 1 and 300 GHz are called as Micro waves.

- Micro waves are unidirectional.
- Microwave propagation is line of sight.
- Very high frequency Micro waves cannot penetrate walls.
- The microwave band is relatively wide, almost 299 GHz

Terrestrial Microwave

- Used for long-distance telephone service.
- Uses radio frequency spectrum, from 2 to 40 Ghz.
- Parabolic dish transmitter, mounted high.
- Used by common carriers as well as private networks.
- Requires unobstructed line of sight between source and receiver.
- Curvature of the earth requires stations (repeaters) ~30 miles apart.

Satellite Microwave

A microwave relay station in space can relay signals over long distances geostationary satellites

- remain above the equator at a height of 22,300 miles (geosynchronous orbit)
- travel around the earth in exactly the time the earth takes to rotate

Applications

- They are used in Cellular phones.
- They are used in satellite networks.
- They are used in wireless LANs.

Radio Waves Application

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

PSTN

The public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing most telephones to communicate with each other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core network and includes mobile and other networks, as well as fixed telephones. The technical operation of the PSTN adheres to the standards created by the ITU-T. These standards allow different networks in different countries to interconnect seamlessly. The E.163 and E.164 standards provide a single global address space for telephone numbers. The combination of the interconnected networks and the single numbering plan allow telephones around the world to dial each other.

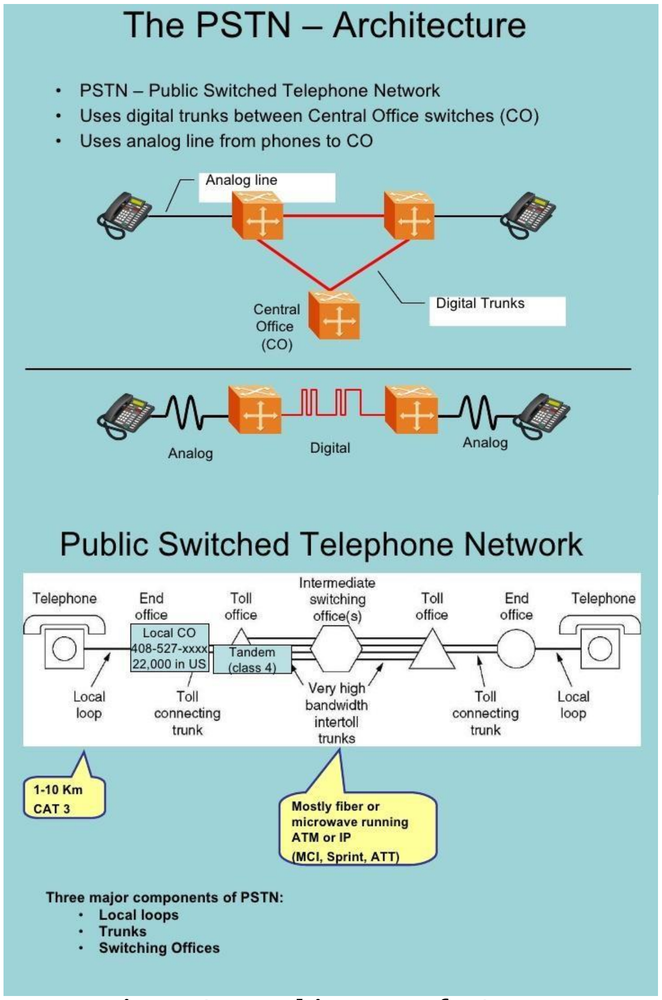


Figure 3.4 Architecture of PSTN

Data-Link Protocols

Data-Link Protocol Functions

Line discipline – coordinates hop-to-hop data delivery where a hop is a computer, a network controller, or some type of network-connecting device, such as router.It determines which device is transmitting and which is receiving at any point in time

Flow control – the rate at which data is transported over a link.

- It provides an acknowledgement mechanism that data is received at the destination.
- It regulate flow of data from sender to receiver

Error control – detects and corrects transmission errors

Framing – recognizing beginning and end of frames (blocks, packets).Communications requires at least two devices, one to send and one to receive. If both devices are ready to send some information and put their signals on the link then the two signals collides each other and became nothing. To avoid such a situation the data link layer use a mechanism called line discipline.

Line discipline coordinates the link system. It determines which device can send and when it can send. It answers the question, who should send now? Line discipline can serve in two ways:

1. enquiry / acknowledgement (ENQ / ACK)
2. poll / select (POLL / SELECT)

ENQ / ACK:

This method is used in peer to peer communications. That is where there is a dedicated link between two devices. The initiator first transmits a frame called an enquiry (ENQ) asking I the receiver is available to receive data. The receiver must answer either with an acknowledgement (ACK) frame if it ready to accept or with a negative acknowledgement (NAK) frame if it is not ready. If the response is positive, the initiator is free to send its data. Otherwise it waits, and try again. Once all its data have been transmitted, the sending system finishes with an end of transmission (EOT) frame.

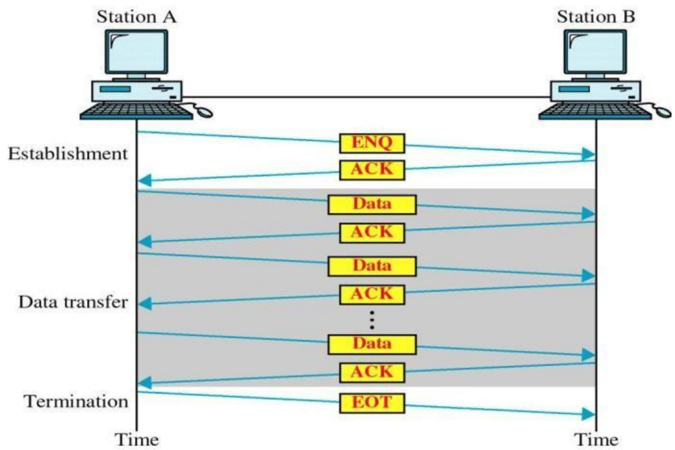


Figure 3.5 Line discipline

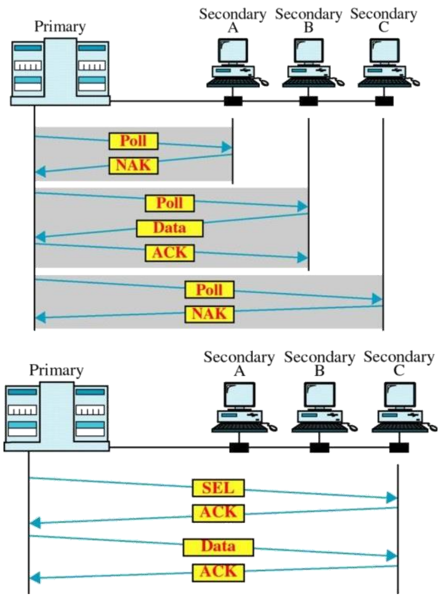


Figure 3.6 Poll/Select

Flow control

Stop-and-Wait flow control

- Source transmits frame
- Destination receives frame and replies with acknowledgement
- Source waits for ACK before sending next frame
- Destination can stop flow by not send ACK
- Works well for a few large frames

It refers to a set of procedures used to restrict the amount of data flow between sending and receiving stations. It tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver. There are two methods are used. They are,

1. stop and wait
2. sliding window

STOP AND WAIT

In this method the sender waits or acknowledgment after every frame it sends. Only after an acknowledgment has been received, then the sender sends the next frame.

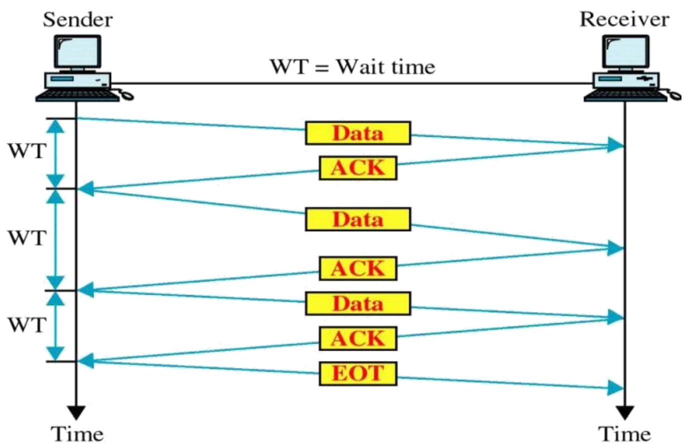


Figure 3.7 Stop-and-Wait flow control

The advantage is simplicity. The disadvantage is inefficiency

SLIDING WINDOW:

In this method, the sender can transmit several frames before needing an acknowledgment. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

The sliding window refers to imaginary boxes at both the sender and receiver. This window provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement. To identify each frame the sliding window scheme introduces the sequence number.

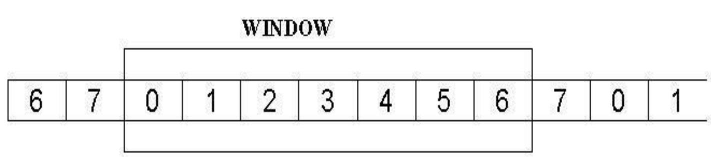


Figure 3.8 Sliding window flow control

The frames are numbered as 0 to n-1. And the size of the window is n-1. Here the size of the window is 7 and the frames are numbered as 0,1,2,3,4,5,6,7.

SENDER WINDOW

At the beginning the sender's window contains n-1 frames. As frames are sent out the left boundary of the window moves inward, shrinking the size of the window. Once an ACK receives the window expands at the right side boundary to allow in a number of new frames equal to number of frames acknowledged by that ACK.

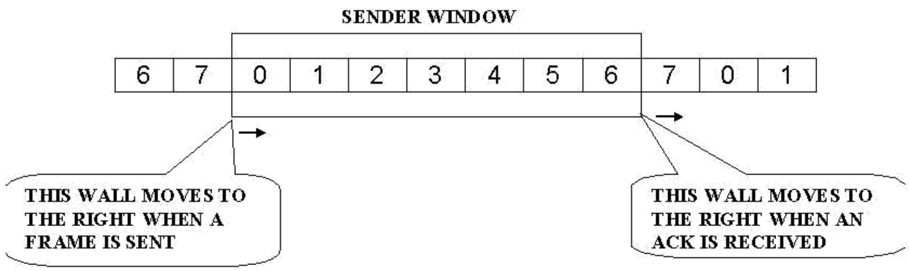


Figure 3.9 Sender Window

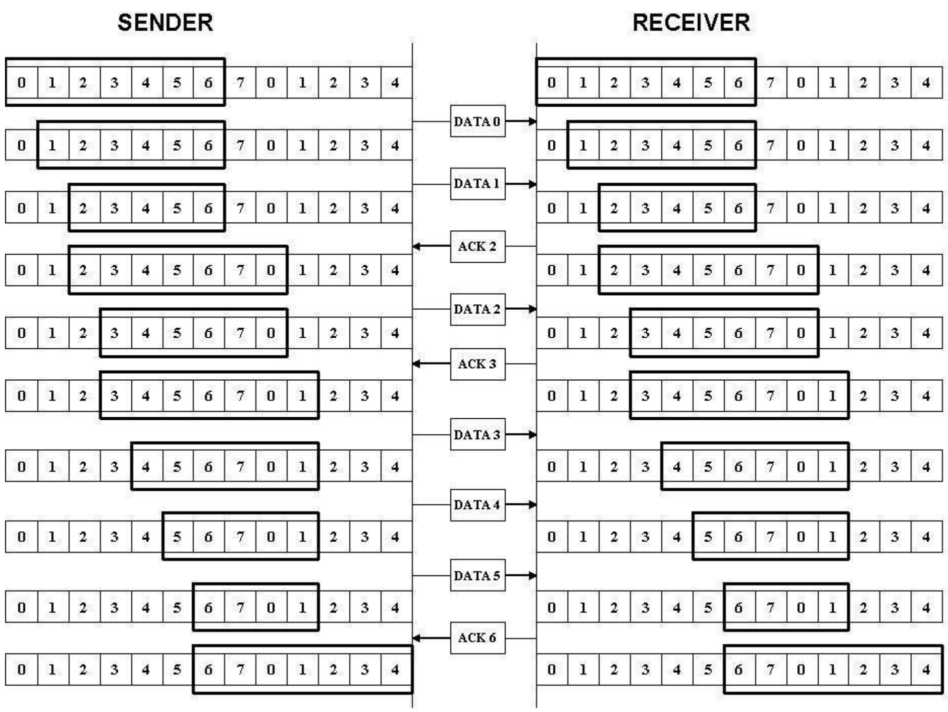


Figure 3.10 Sender and Receiver Window

ERROR CONTROL

Detection and correction of errors Lost frames

Damaged frames

Techniques for error control (Automatic repeat request)

--Error detection

--Positive acknowledgment

--Retransmission after timeout

--Negative acknowledgement and retransmission

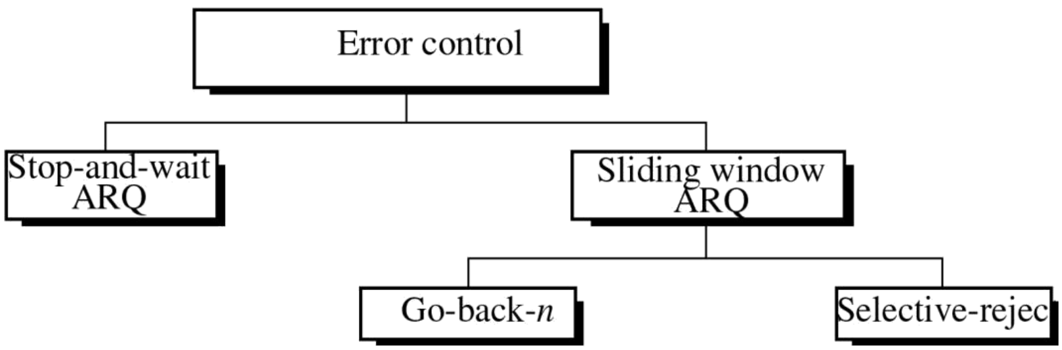


Figure 3.11 Classification of Error Control

Error control is implemented in such a way that every time an error is detected, a negative acknowledgement is returned and the specified frame is retransmitted. This process is called **automatic repeat request (ARQ).**The error control is implemented with the flow control mechanism. So there are two types in error control. They are,

1. stop and wait ARQ
2. sliding window ARQ

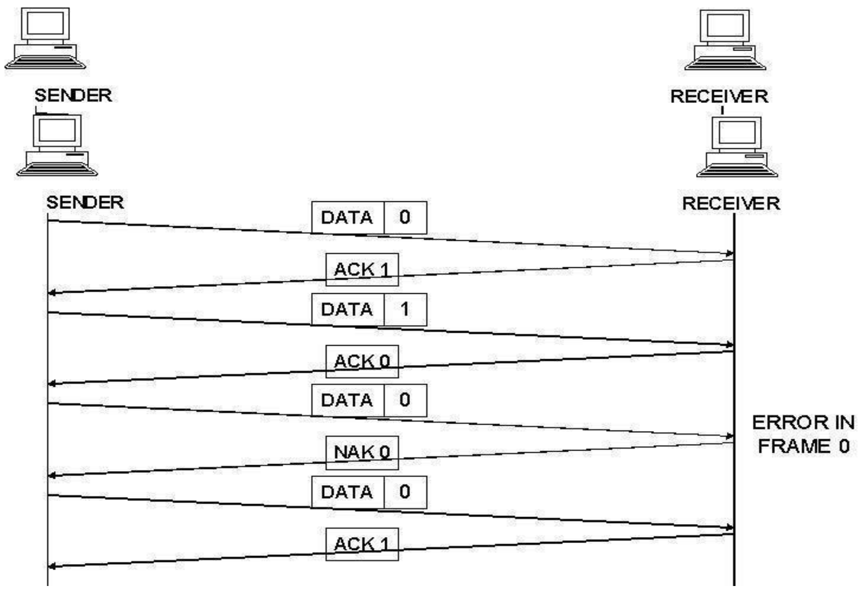
STOP AND WAIT ARQ:

It is a form of stop and wait flow control, extended to include retransmission of data in case of lost or damaged frames.

DAMAGED FRAME:

When a frame is discovered by the receiver to contain an error, it returns a NAK frame and the sender retransmits the last frame.

Figure 3.12 Damaged Frame in stop and wait ARQ



LOST DATA FRAME:

The sender is equipped with a timer that starts every time a data frame is transmitted. If the frame lost in transmission the receiver can never acknowledge it. The sending device waits for an ACK or NAK frame until its timer goes off, then it tries again. It retransmits the last data frame.

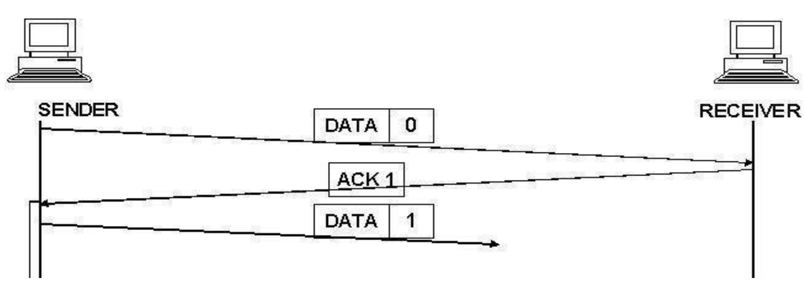


Figure 3.13 Lost Data Frame in stop and wait ARQ

LOST ACKNOWLEDGEMENT:

The data frame was received by the receiver but the acknowledgement was lost in transmission. The sender waits until the timer goes off, then it retransmits the data frame. The receiver gets a duplicated copy of the data frame. So it knows the acknowledgement was lost so it discards the second copy.

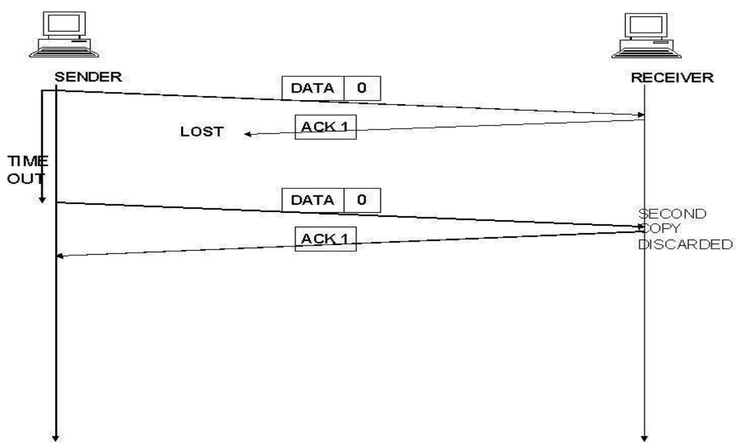


Figure 3.14 Lost Acknowledgement in stop and wait ARQ

SLIDING WINDOW ARQ

It is used to send multiple frames per time. The number of frame is according to the window size. The sliding window is an imaginary box which is reside on both sender and receiver side. It has two types. They are,

1. go-back-n ARQ
2. selective reject ARQ

GO-BACK-N ARQ:

In this method, if one frame is lost or damaged, all frames sent since the last frame acknowledged or retransmitted.

DAMAGED FRAME:

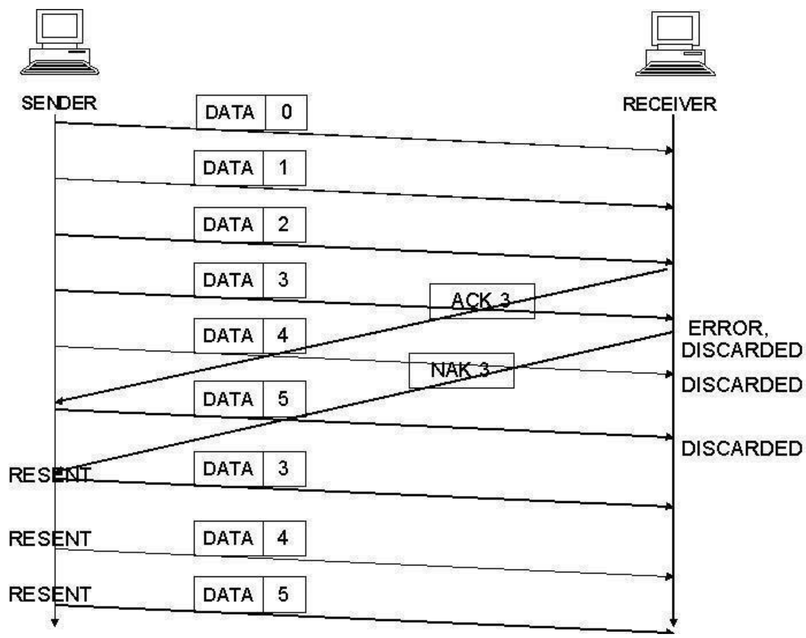


Figure 3.15 Damaged Frame in go back N ARQ

LOST FRAME:

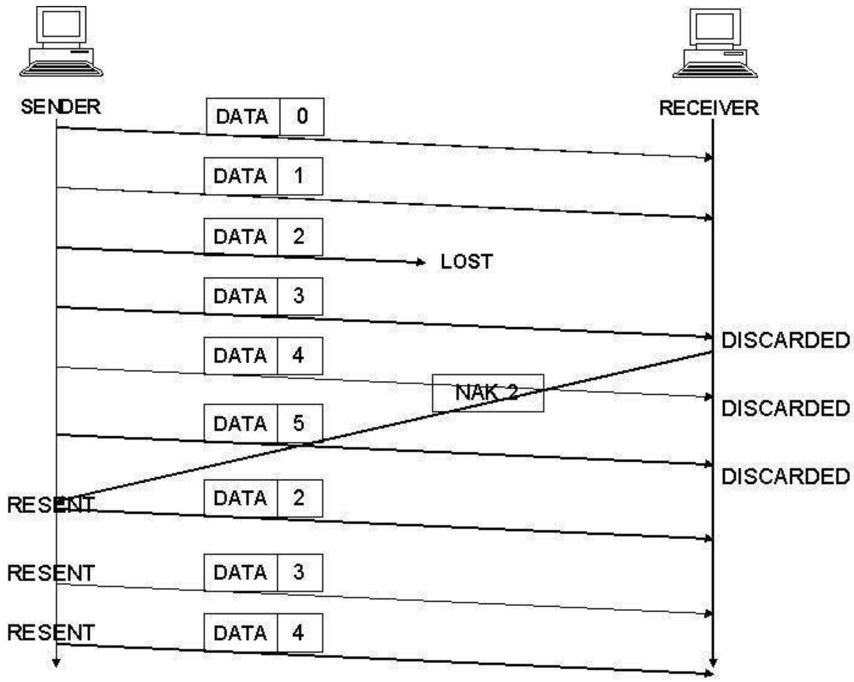


Figure 3.15 Lost Frame in go back N ARQ

LOST ACK:

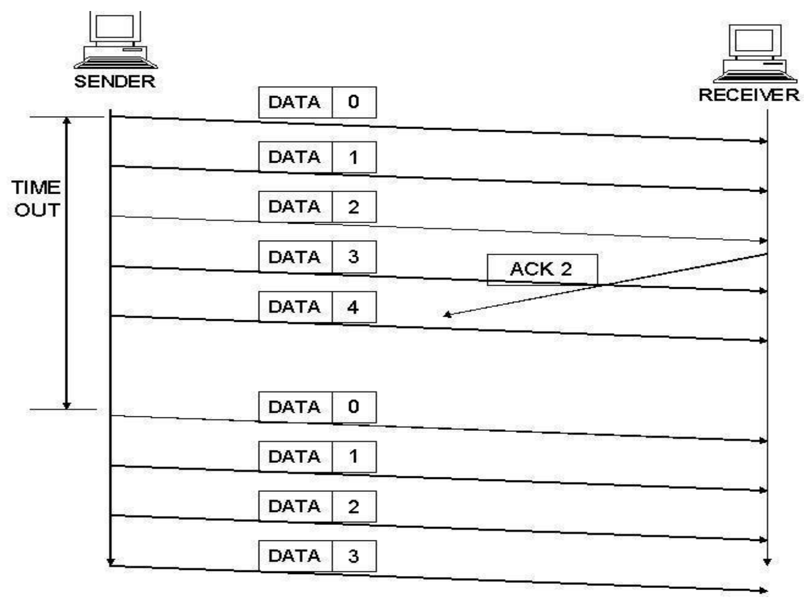


Figure 3.16 Lost Acknowledgement in go back N ARQ

SELECTIVE REPEAT ARQ

Selective repeat ARQ re transmits only the damaged or lost frames instead of sending multiple frames. The selective transmission increases the efficiency of transmission and is more suitable for noisy link. The receiver should have sorting mechanism.

DAMAGED FRAME

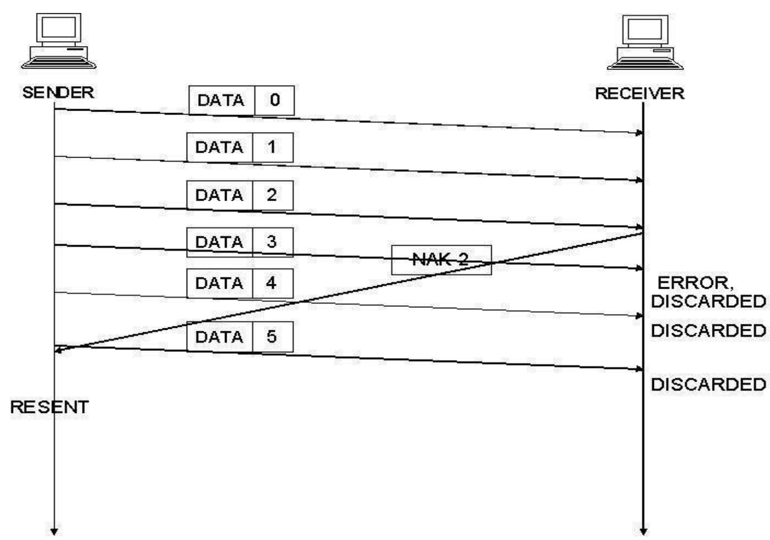


Figure 3.17 Damaged Frame in Selective Repeat ARQ

LOST FRAME

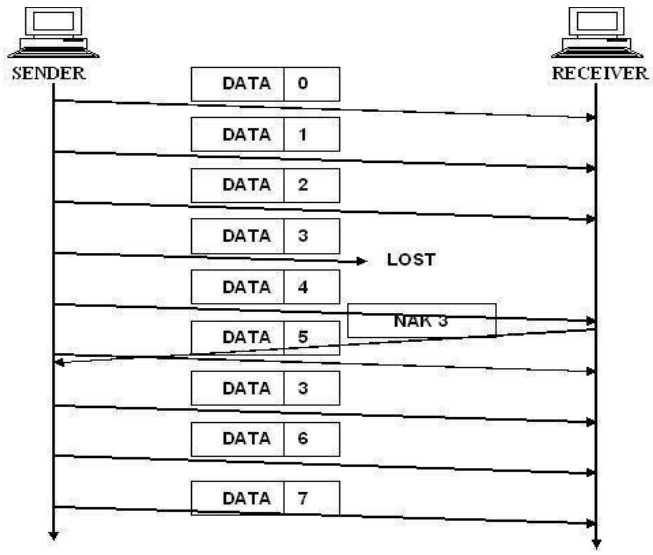


Figure 3.18 Lost Frame in Selective Repeat ARQ

LOST ACK

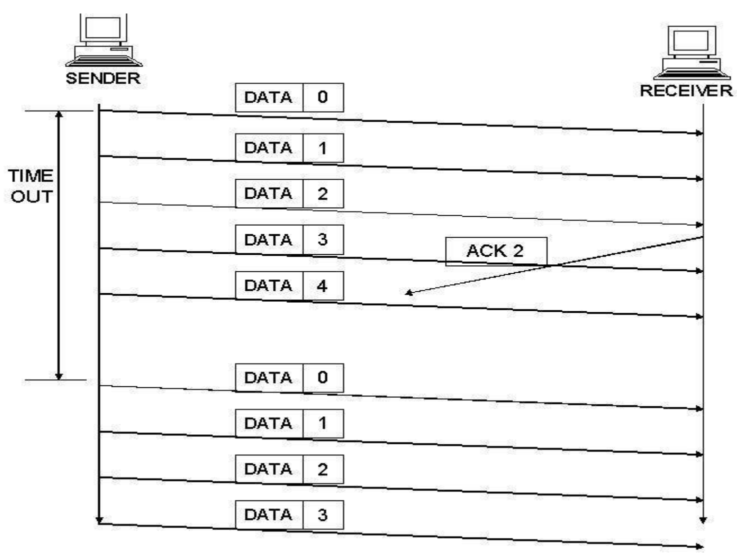


Figure 3.19 Lost Acknowledgement in Selective Repeat ARQ

HDLC

HDLC is a bit-oriented protocol. It was developed by the International Organization for Standardization (ISO). It falls under the ISO standards ISO 3309 and ISO 4335. It specifies a packitization standard for serial links. It has found itself being used throughout the world. It has been so widely implemented because it supports both half-duplex and full-duplex communication lines, point-to-point (peer to peer) and multi-point networks, and switched or non-switched channels. HDLC supports several modes of operation, including a simple sliding-window mode for reliable delivery. Since Internet provides retransmission at higher levels (i.e., TCP), most Internet applications use HDLC's unreliable delivery mode, Unnumbered Information.

Other benefits of HDLC are that the control information is always in the same position, and specific bit patterns used for control differ dramatically from those in representing data, which reduces the chance of errors. It has also led to many subsets. Two subsets widely in use are Synchronous Data Link Control (SDLC) and Link Access Procedure-Balanced (LAP-B).

HDLC Stations and Configurations

HDLC specifies the following three types of stations for data link control:

- Primary Station
- Secondary Station
- Combined Station

Primary Station

Within a network using HDLC as its data link protocol, if a configuration is used in which there is a primary station, it is used as the controlling station on the link. It has the responsibility of controlling all other stations on the link (usually secondary stations). A primary issues *commands* and secondary issues *responses*. Despite this important aspect of being on the link, the primary station is also responsible for the organization of data flow on the link. It also takes care of error recovery at the data link level (layer 2 of the OSI model).

Secondary Station

If the data link protocol being used is HDLC, and a primary station is present, a secondary station must also be present on the data link. The secondary station is under the control of the primary station. It has no ability, or direct responsibility for controlling the link. It is only activated when requested by the primary station. It only responds to the primary station. The secondary station's frames are called responses. It can only send response frames when requested by the primary station. A primary station maintains a separate logical link with each secondary station.

Combined Station

A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link. Each combined station is in full control of itself, and does not rely on any other stations on the link. No other stations can control any combined station. May issue both commands and responses. HDLC also defines three types of configurations for the three types of stations. The word configuration refers to the relationship between the hardware devices on a link. Following are the three configurations defined by HDLC:

- Unbalanced Configuration
- Balanced Configuration
- Symmetrical Configuration

Unbalanced Configuration

The unbalanced configuration in an HDLC link consists of a primary station and one or more secondary stations. The unbalanced condition arises because one station controls the other stations. In an unbalanced configuration, any of the following can be used:

- Full-Duplex or Half-Duplex operation
- Point to Point or Multi-point networks

An example of an unbalanced configuration can be found below

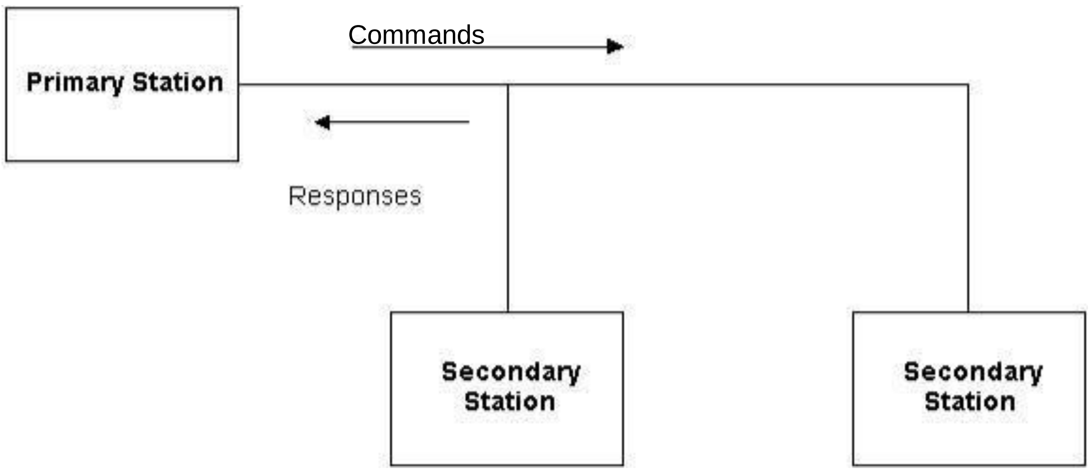


Figure 3.20 Unbalanced configuration

Balanced Configuration

The balanced configuration in an HDLC link consists of two or more combined stations.Each of the stations has equal and complimentary responsibility compared to each other.Balanced configurations can use only the following:

- Full - Duplex or Half - Duplex operation
- Point to Point networks

An example of a balanced configuration can be found below.

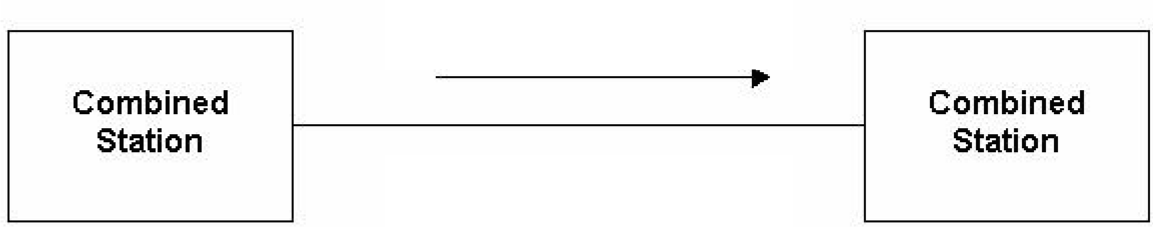


Figure 3.21 Balanced configuration

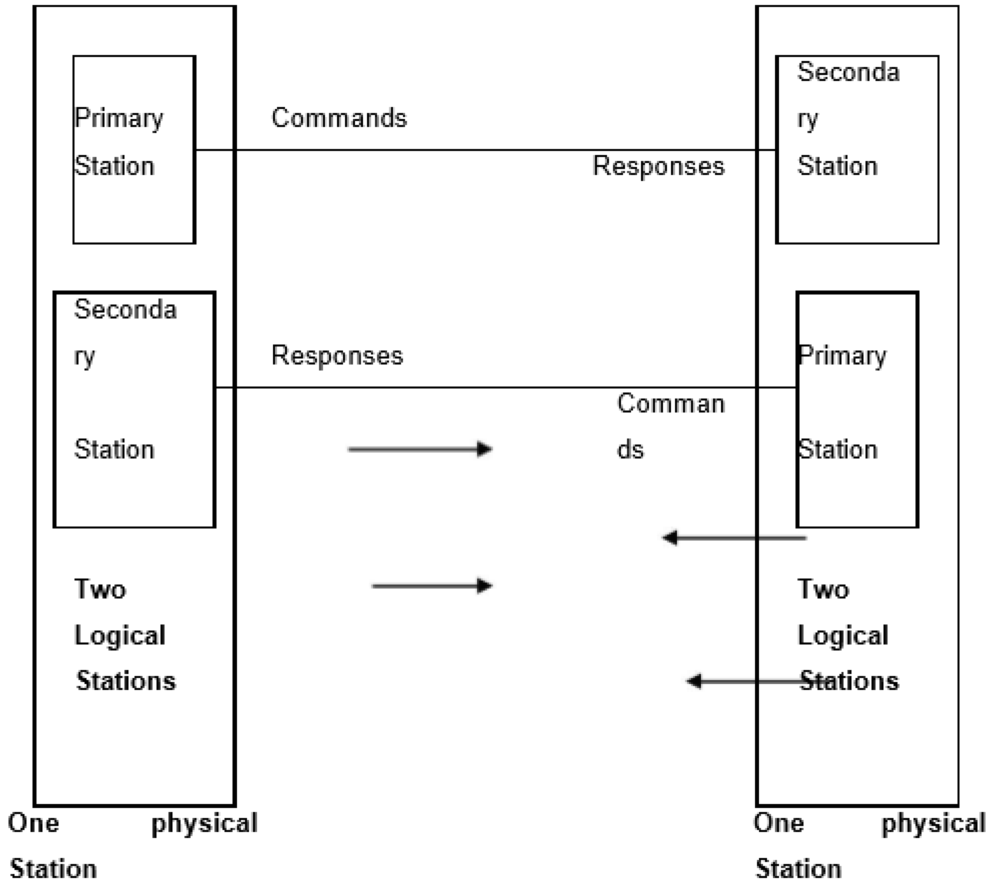


Figure 3.22 Symmetric configuration

Symmetrical Configuration

This third type of configuration is not widely in use today. It consists of two independent point-to- point, unbalanced station configurations as shown in Figure. In this configuration, each station has a primary and secondary status. Each station is logically considered as two stations

HDLC Operational Modes

A mode in HDLC is the relationship between two devices involved in an exchange; the mode describes who controls the link. Exchanges over unbalanced configurations are always conducted in normal response mode. Exchanges over symmetric or balanced configurations can be set to specific mode using a frame design to deliver the command. HDLC offers three different modes of operation. These three modes of operations are:

- Normal Response Mode (NRM)
- Asynchronous Response Mode (ARM)
- Asynchronous Balanced Mode (ABM)

Normal Response Mode

This is the mode in which the primary station initiates transfers to the secondary station. The secondary station can only transmit a response when, and only when, it is instructed to do so by the primary station. In other words, the secondary station must receive explicit permission from the primary station to transfer a response. After receiving permission from the primary station, the secondary station initiates its transmission. This transmission from the secondary station to the primary station may be much more than just an acknowledgment of a frame. It may in fact be more than one information frame. Once the last frame is transmitted by the secondary station, it must wait once again from explicit permission to transfer anything, from the primary station. Normal Response Mode is only used within an unbalanced configuration.

Asynchronous Response Mode

In this mode, the primary station doesn't initiate transfers to the secondary station. In fact, the secondary station does not have to wait to receive explicit permission from the primary station to transfer any frames. The frames may be more than just acknowledgment frames. They may contain data, or control information regarding the status of the secondary station. This mode can reduce overhead on the link, as no frames need to be transferred in order to give the secondary station permission to initiate a transfer. However, some limitations do exist. Due to the fact that this mode is asynchronous, the secondary station must wait until it detects and idle channel before it can transfer any frames. This is when the ARM link is operating at half-duplex. If the ARM link is operating at full duplex, the secondary station can transmit at any time. In this mode, the primary station still retains responsibility for error recovery, link setup, and link disconnection.

Synchronous Balanced Mode

This mode is used in case of combined stations. There is no need for permission on the part of any station in this mode. This is because combined stations do not require any sort of instructions to perform any task on the link.Normal Response Mode is used most frequently in multi- point lines, where the primary station controls the link. Asynchronous Response Mode is better for point-to-point links, as it reduces overhead. Asynchronous Balanced Mode is not used widely today. The "asynchronous" in both ARM and ABM does not refer to the format of the data on the link. It refers to the fact that any given station can transfer frames without explicit permission or instruction from any other station.

HDLC Non-Operational Modes

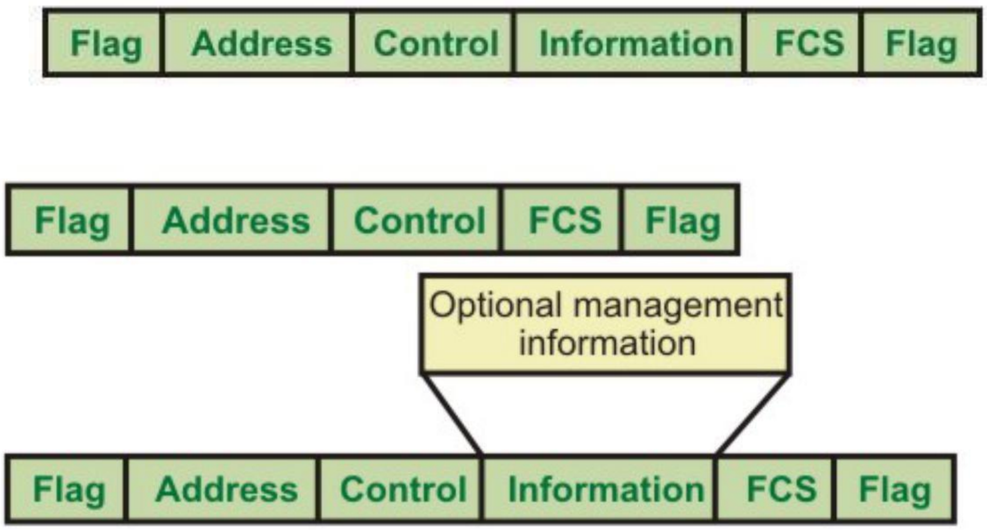
HDLC also defines three non-operational modes. These three non-operational modes are:

- Normal Disconnected Mode (NDM)
- Asynchronous Disconnected Mode (ADM)
- Initialization Mode (IM)

The two disconnected modes (NDM and ADM) differ from the operational modes in that the secondary station is logically disconnected from the link (note the secondary station is not physically disconnected from the link). The IM mode is different from the operations modes in that the secondary station's data link control program is in need of regeneration or it is in need of an exchange of parameters to be used in an operational mode.

HDLC Frame Structure

There are three different types of frames as shown in Fig. and the size of different fields are shown Table



I-Frame

S-Frame

U-Frame

Figure 3.23 Different types of Frames in HDLC

Table 3.1 Size of different fields

Field Name	Size(in bits)
[redacted]	[redacted]
Flag Field(F)	8 bits
Address Field(A)	8 bits
Control Field(C)	8 or 16 bits
Information Field(I) OR Data	Variable; Not used in some frames
Frame Check Sequence(FCS)	16 or 32 bits
Closing Flag Field(F)	8 bits

The Flag field

Every frame on the link must begin and end with a flag sequence field (F). Stations attached to the data link must continually listen for a flag sequence. The flag sequence is an octet looking like 01111110. Flags are continuously transmitted on the link between frames to keep the link active. Two other bit sequences are used in HDLC as signals for the stations on the link. These two bit sequences are:

- Seven 1's, but less than 15 signal an abort signal. The stations on the link know there is a problem on the link.
- 15 or more 1's indicate that the channel is in an idle state.

The time between the transmissions of actual frames is called the **interframe time fill**. The interframe time fill is accomplished by transmitting continuous flags between frames. The flags may be in 8 bit multiples.

HDLC is a code-transparent protocol. It does not rely on a specific code for interpretation of line control. This means that if a bit at position N in an octet has a specific meaning, regardless of the other bits in the same octet. If an octet has a bit sequence of 01111110, but is not a flag field, HLDC uses a technique called bit-stuffing to differentiate this bit sequence from a flag field as we have discussed in the previous lesson.

At the receiving end, the receiving station inspects the incoming frame. If it detects 5 consecutive 1's it looks at the next bit. If it is a 0, it pulls it out. If it is a 1, it looks at the 8^{th} bit. If the 8^{th} bit is a 0, it knows an abort or idle signal has been sent. It then proceeds to inspect the following bits to determine appropriate action. This is the manner in which HDLC achieves code- transparency. HDLC is not concerned with any specific bit code inside the data stream. It is only concerned with keeping flags unique.

The Address field

The address field (A) identifies the primary or secondary stations involvement in the frame transmission or reception. Each station on the link has a unique address. In an unbalanced configuration, the A field in both commands and responses refer to the secondary station. In a balanced configuration, the command frame contains the destination station address and the response frame has the sending station's address.

The Control field

HDLC uses the control field (C) to determine how to control the communications process. This field contains the commands, responses and sequences numbers used to maintain the data flow accountability of the link, defines the functions of the frame and initiates the logic to control the movement of traffic between sending and receiving stations. There three control field formats:

- **Information Transfer Format**: The frame is used to transmit end-user data between two devices.
- **Supervisory Format**: The control field performs control functions such as acknowledgment of frames, requests for re-transmission, and requests for temporary suspension of frames being transmitted. Its use depends on the operational mode being used.

- **Unnumbered Format**: This control field format is also used for control purposes. It is used to perform link initialization, link disconnection and other link control functions.

The Poll/Final Bit (P/F)

The 5th bit position in the control field is called the **poll/final bit, or P/F bit**. It can only be recognized when it is set to 1. If it is set to 0, it is ignored. The poll/final bit is used to provide dialogue between the primary station and secondary station. The primary station uses P=1 to acquire a status response from the secondary station. The P bit signifies a poll. The secondary station responds to the P bit by transmitting a data or status frame to the primary station with the P/F bit set to F=1. The F bit can also be used to signal the end of a transmission from the secondary station under Normal Response Mode.

The Information field or Data field

This field is not always present in a HDLC frame. It is only present when the Information Transfer Format is being used in the control field. The information field contains the actually data the sender is transmitting to the receiver in an I-Frame and network management information in U- Frame.

The Frame check Sequence field

This field contains a 16-bit, or 32-bit cyclic redundancy check bits. It is used for error detection as discussed in the previous lesson.

Error Detecting Codes

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

Some popular techniques for error detection are:

1. Vertical Redundancy Check(VRC)
2. Longitudinal Redundancy Check(VRC)

3. Checksum

4. Cyclic redundancy check

1. Vertical Redundancy Check (VRC)

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 odd number of 1's, and
- 0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.

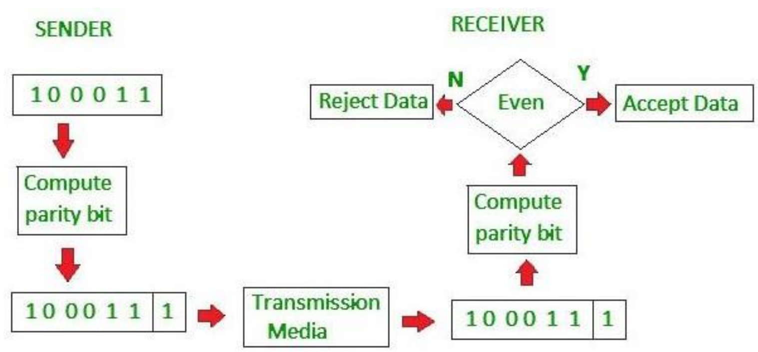
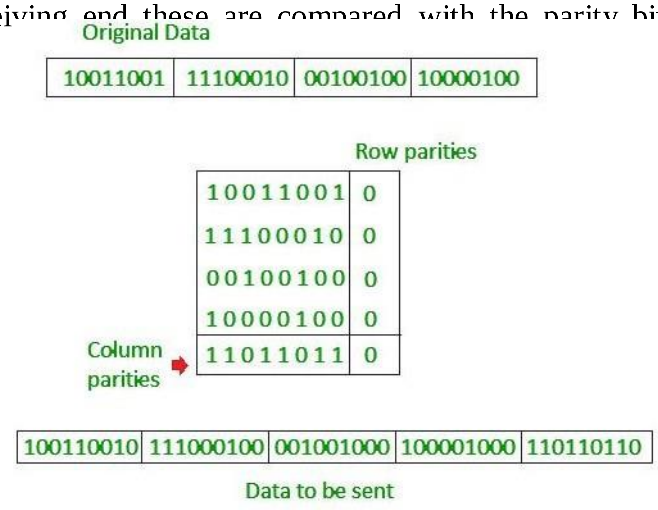


Figure 3.24 Vertical Redundancy Check

2. Longitudinal Redundancy Check (VRC)

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.



3. Checksum

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

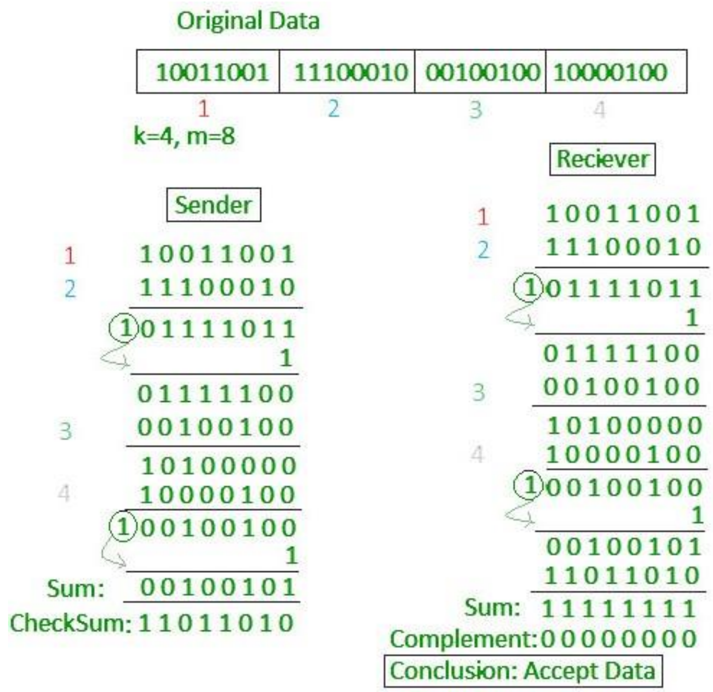


Figure 3.26 Checksum

4. Cyclic redundancy check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

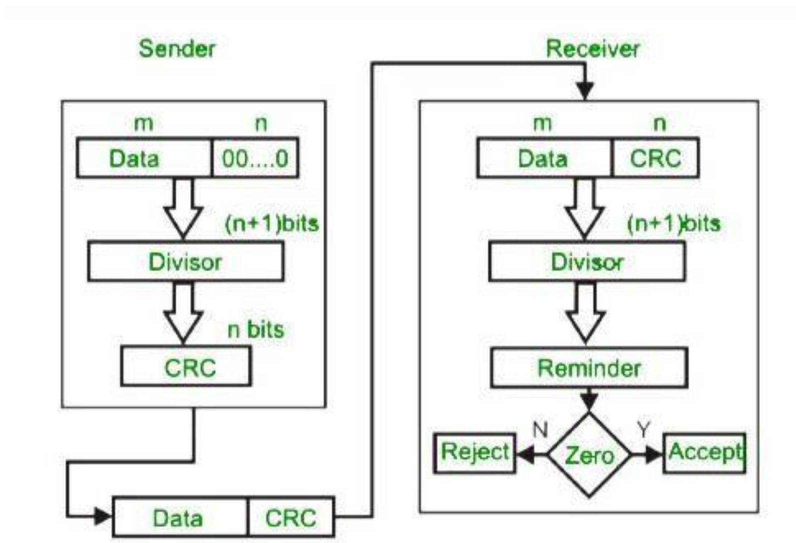


Figure 3.27 Algorithm of Cyclic redundancy check

Example :

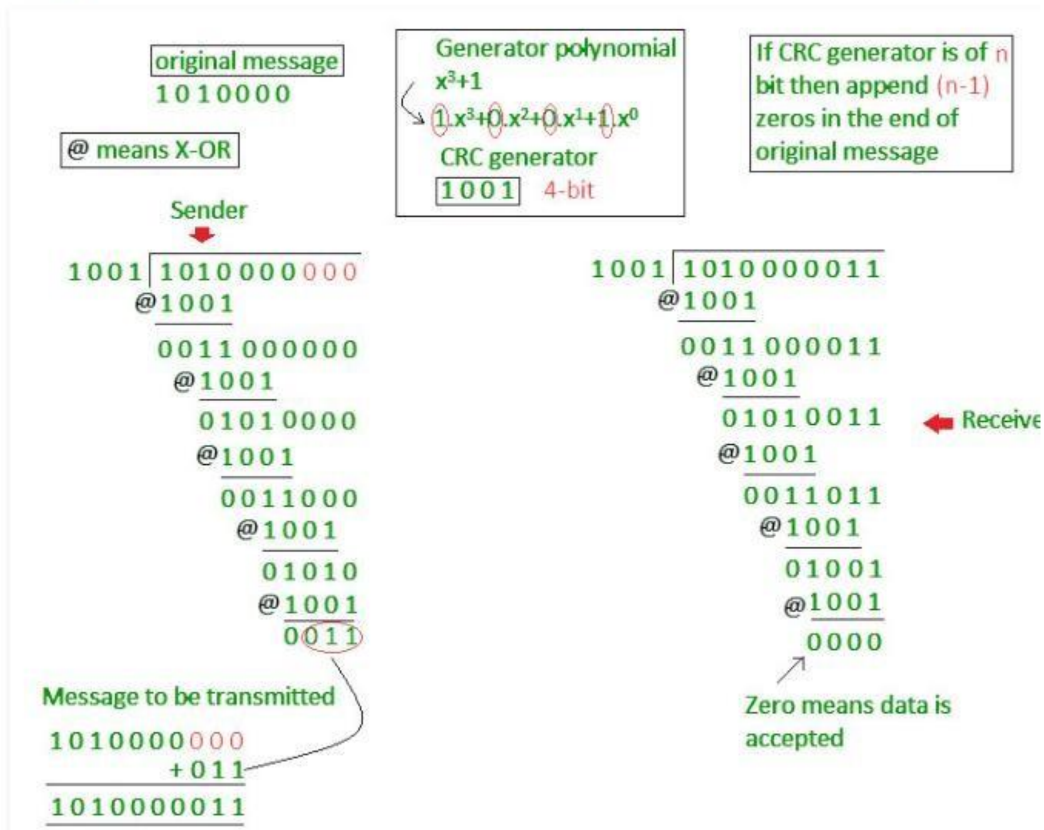


Figure 3.27 Example of Cyclic redundancy check

TEXT / REFERENCE BOOKS

1. Andrew S Tanenbaum “Computer Networks” 5th Edition. Pearson Education/PH I/2011.
2. Behrouz A. Forouzan, “Data Communications and Networking” Fourth Edition, Mc GrawHill HIGHER Education 2007.
3. Michael A.Gallo, William Hancock.M, Brooks/Cole Computer Communications and Networking Technologies,2001
4. Richard Lai and Jirachief pattana, “Communication Protocol Specification and Verification”, Kluwer Publishers, Boston, 1998.

5. Pallapa Venkataram and Sunilkumar S.Manvi, “Communication protocol Engineering”, PHI Learning, 2008

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 ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATON ENGINEERING

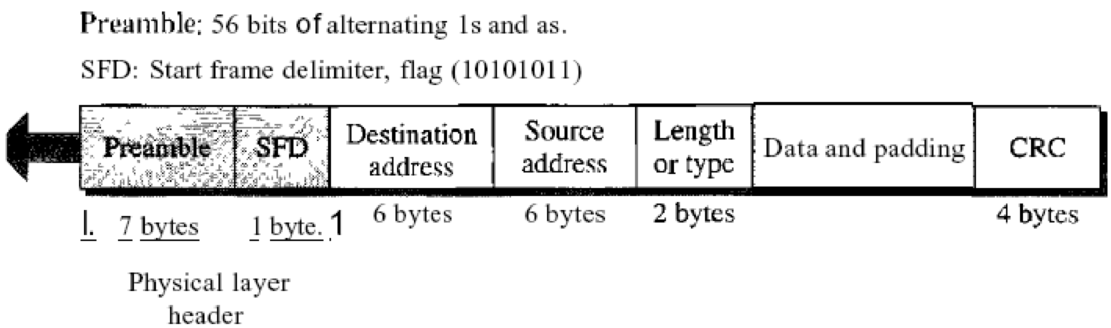
Data Communication and Networking – SEC1306

IV. MAC Sub Layer and Network Layer

IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token passing method for Token Ring and Token Bus LANs. As we discussed in the previous section, part of the framing function is also handled by the MAC layer. In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

802.3 MAC Frame

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRe. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.



Preamble: Alerts the receiving system to the coming frame and enables it to synchronize its input timing
Start frame delimiter (SFD): The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address
Destination address (DA): This field is 6 bytes and contains the physical address of the destination stations to receive the packet.
Source address (SA): The SA field is also 6 bytes and contains the physical address of the sender of the packet.
Length or type: The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field.
Data: This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes
CRC: This field contains error detection information

Addressing:

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). 6-byte physical address in hexadecimal notation.

Types of Address: Unicast , Multicast and Broadcast

A source address is always a unicast. The frame comes from only one station.

The broadcast destination address is a special case of the multicast address in which all bits are 1s.

Transmission of Address : The address 47:20:1B:2E:08:EE is sent out on line as, left-to-right, byte by byte; for each byte, it is sent right-to-left, bit by bit

Exercise:

Define the type of destination address a) 1A:01 A2:B0 10:06

b) 27:09 54:C2 23:2B c) FF:FF FF:FF FF:FF

Solution

a) LSB is 0 – A : 1010 (even); Unicast

b) LSB is 1 – 7 : 0111 (odd); Multicast

c) All bits are FF’s : all 1’s; Broadcast

The network layer is concerned with getting packets from the source all the way to the destination. Getting to the destination may require making many hops at intermediate routers along the way. This function clearly contrasts with the function of the data link layer. The data link layer is concerned with only moving frames from one end of a wire to the other. Thus, the network layer is the lowest layer that deals with end-to-end transmission. To achieve its goals, the network layer must know about the topology of the network (i.e., the set of all routers and links). It should also choose appropriate paths through the network, even if it is large. It must also take care when choosing routes to avoid overloading some of the communication lines and routes while leaving others idle. It must also handle problems when source and destination are in different networks. It is up to the network layer to deal with them.

Network designers should grapple with certain design issues. These issues include the service provided to the transport layer and the internal design of the network.

SERVICES PROVIDED TO THE TRANSPORT LAYER

Network layer provides its services to the transport layer at the network layer/transport layer interface.
What kind of services the network layer provides to the transport layer?

The services need to be carefully 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.

SERVICES PROVIDED TO THE TRANSPORT LAYER

These goals allow a lot of freedom to the network layer designers in writing detailed specifications of the services to be offered to the transport layer. Conflicts of opinions arise among various factions of designers. The debate centers on whether the network layer should provide connection oriented or connectionless service. Internet community argues that the routers’ job is moving packets around and nothing else. In this view the network is inherently unreliable. So the hosts should accept this fact and do errors control themselves. It leads to the conclusion that the network service should be connectionless.

SERVICES PROVIDED TO THE TRANSPORT LAYER

No packet ordering and flow control should be done, as the hosts are going to do that anyway. This reasoning is an example of the end-to-end argument. Moreover, each packet must carry the full destination address, as each packet is carried independently of its predecessors. Another camp argues that the network should provide a reliable, connection-oriented service. This camp is represented by the telephone companies. They view quality of service (QoS) as the dominant factor. They view that QoS is difficult to achieve without connections.

IMPLEMENTATION OF CONNECTIONLESS SERVICE:

Packets are injected into the network individually and routed independently of each other. Any advance setup is not required. Packets are called datagrams in this context (in analogy with telegrams). The network is called a datagram network.

IMPLEMENTATION OF CONNECTION-ORIENTED SERVICE:

The idea behind VCs is to avoid having to choose a new route for every packet sent. When a connection is established a route between source and destination is chosen and stored within the tables inside the routers. That route is used for all traffic flowing over the connection. This is exactly similar to the telephone system. When the connection is released, VC is also terminated. With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.

ALOHA:

In the 1970s, Norman Abramson and his colleagues at the University of Hawaii devised a new and elegant method to solve the channel allocation problem. Their work has been extended by many researchers since then (Abramson, 1985). Although Abramson's work, called the ALOHA system, used ground-based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel. There are two versions of ALOHA: pure and slotted. They differ with respect to whether time is divided into discrete slots into which all frames must fit. Pure ALOHA does not require global time synchronization; slotted ALOHA does.

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 in a way that can lead to conflicts are widely known as contention systems.

A sketch of frame generation in an ALOHA system is given in Fig.1. We have made the frames all the same length because the throughput of ALOHA systems is maximized by having a uniform frame size rather than by allowing variable length frames.

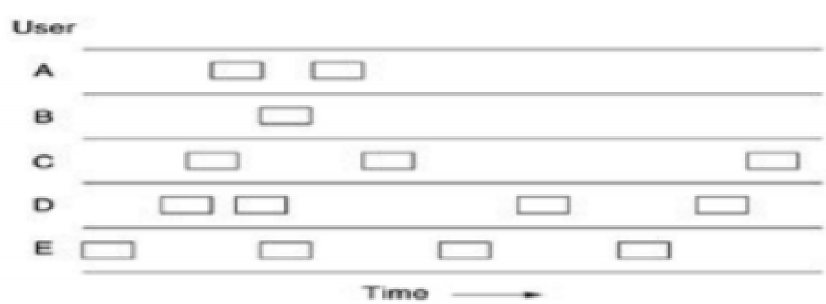


Figure.1 Pure ALOHA

Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled. If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later. The checksum cannot (and should not) distinguish between a total loss and a near miss. Let the "frame time" denote the amount of time needed to transmit the standard, fixed length frame (i.e., the frame length divided by the bit rate). At this point we assume that the infinite population of users generates new frames according to a Poisson distribution with mean N frames per frame time. (The infinite-population assumption is needed to ensure that N does no decrease as users become blocked.) If N > 1, the user community is generating frames at a higher rate than the channel can handle, and nearly every frame will suffer a collision.

For reasonable throughput we would expect 0 < N < 1. In addition to the new frames, the stations also generate retransmissions of frames that previously suffered collisions. Let us further assume that the probability of k transmission attempts per frame time, old and new combined, is also Poisson, with mean G per frame time. Clearly, G≥N. At low load (i.e., N 0), there will be few collisions, hence few retransmissions, so G N. At high load there will be many collisions, so G > N. Under all loads, the throughput, S, is just the offered load, G, times the probability, P0, of a transmission succeeding—that is, S = GP0, where P0 is the probability that a frame does not suffer a collision.

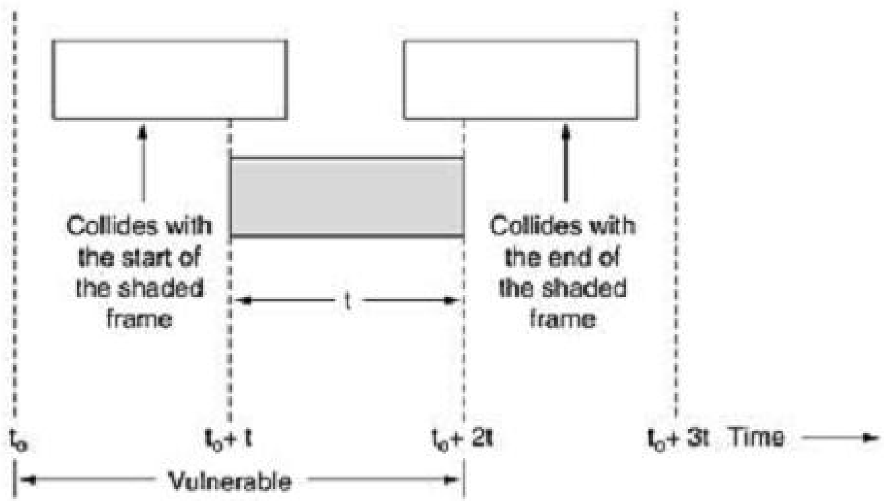


Figure 2. Vulnerable period

A frame will not suffer a collision if no other frames are sent within one frame time of its start, as shown in Figure 2.

Under what conditions will the shaded frame arrive undamaged? Let t be the time required to send a frame. If any other user has generated a frame between time t0 and t0+tr, the end of that frame will collide with the beginning of the shaded one. In fact, the shaded frame's fate was already sealed even before the first bit was sent, but since in pure ALOHA a station does not listen to the channel before transmitting, it has no way of knowing that another frame was already underway. Similarly, any other frame started between t0+t and t0+2t will bump into the end of the shaded frame. The probability that k frames are generated during a given frame time is given by the Poisson distribution:

$$\Pr[k] = \frac{G^k e^{-G}}{k!}$$

The probability of zero frames is just e-G. In an interval two frame times long, the mean number of frames generated is 2G. The probability of no other traffic being initiated during the entire vulnerable period is thus given by P0 = e -2G. Using S = GP0, we get

$$S = Ge^{-2G}$$

The relation between the offered traffic and the throughput is shown in Fig.3. The maximum throughput occurs at G = 0.5, with S = 1/2e, which is about 0.184. In other words, the best we can hope for is a channel utilization of 18 per cent. This result is not very encouraging, but with everyone transmitting at will, we could hardly have expected a 100 per cent success rate.

Slotted ALOHA: In 1972, Roberts published a method for doubling the capacity of an ALOHA system (Robert, 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.

As it can be seen from Fig.3, slotted ALOHA peaks at G = 1, with a throughput of S=1/e or about 0.368, twice that of pure ALOHA. If the system is operating at G = 1, the probability of an empty slot is 0.368. The best we can hope for using slotted ALOHA is 37 percent of the slots empty, 37 percent successes, and 26 percent collisions. Operating at higher values of G reduces the number of empties but increases the number of collisions exponentially.

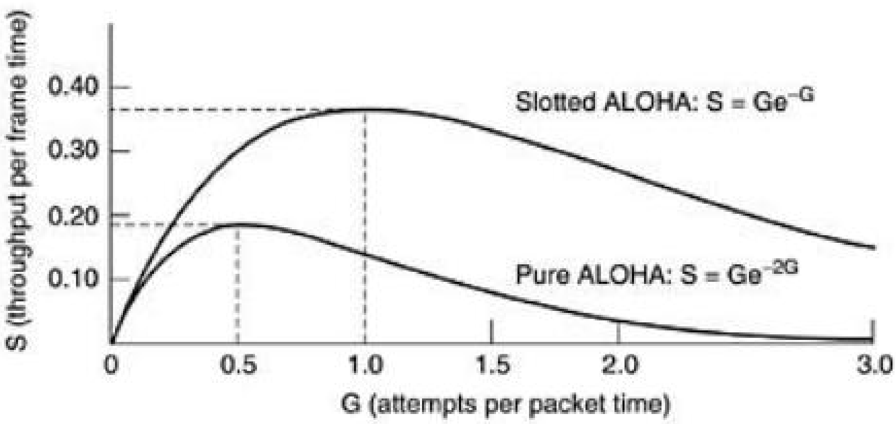


Figure.3 Throughput versus offered traffic for ALOHA systems

To see how this rapid growth of collisions with G comes about, consider the transmission of a test frame. The probability that it will avoid a collision is e-G, the probability that all the other users are silent in that slot. The probability of a collision is then just 1 – e-G. The probability of a transmission requiring exactly k attempts, (i.e., k – 1 collisions followed by one success) is ;

$$P_k = e^{-G}(1 - e^{-G})^{k-1}$$

The expected number of transmissions, E, per carriage return typed is then,

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-G}(1 - e^{-G})^{k-1} = e^G$$

As a result of the exponential dependence of E upon G, small increases in the channel load can drastically reduce its performance.

Carrier Sense Multiple Access Protocols:

With slotted ALOHA the best channel utilization that can be achieved is 1/e. This is hardly surprising, since with stations transmitting at will, without paying attention to what the other stations are doing, there are bound to be many collisions. In local area networks, however, it is possible for stations to detect what other stations are doing, and adapt their behaviour accordingly. These networks can achieve a much better utilization than 1/e. In this section we will discuss some protocols for improving performance. Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called carrier sense protocols. A number of them have been proposed. Kleinrock and Tobagi (1975) have analysed several such protocols in detail. Below we will mention several versions of the carrier sense protocols.

Persistent CSMA:

The first carrier sense protocol that we will study here is called **1-persistent CSMA** (Carrier Sense Multiple Access). When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment. If the channel is busy, the station waits until it becomes idle. When the station detects an idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1- persistent because the station transmits with a probability of 1 when it finds the channel idle.

The first carrier sense protocol that we will study here is called **1-persistent CSMA** (Carrier Sense Multiple Access). When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment. If the channel is busy, the station waits until it becomes idle. When the station detects an idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1- persistent because the station transmits with a probability of 1 when it finds the channel idle.

The propagation delay has an important effect on the performance of the protocol. There is a small chance that just after a station begins sending, another station will become ready to send and sense the channel. If the first station's signal has not yet reached the second one, the latter will sense an idle channel and will also begin sending, resulting in a collision. The longer the propagation delay, the more important this effect becomes, and the worse the performance of the protocol. Even if the propagation delay is zero, there will still be collisions. If two stations become ready in the middle of a third station's transmission, both will wait politely until the transmission ends and then both will begin transmitting exactly simultaneously, resulting in a collision. If they were not so impatient, there would be fewer collisions. Even so, this protocol is far better than pure ALOHA because both stations have the decency to desist from interfering with the third station's frame. Intuitively, this approach will lead to a higher performance than pure ALOHA. Exactly the same holds for slotted ALOHA.

Non-persistent CSMA:

A second carrier sense protocol is **nonpersistent CSMA**. In this protocol, a conscious attempt is made to be less greedy than in the previous one. Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself. However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

The last protocol is p-persistent CSMA. It applies to slotted channels and works as follows. When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p. With a probability q = 1 - p, it defers until the next slot. If that slot is also idle, It either transmits or defers again, with probabilities p and q. This process is repeated until either the frame has been transmitted or another station has begun transmitting. In the latter case, the unlucky station acts as if there had been a collision (i.e., it waits a random time and starts again). If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm. Figure 4 shows the computed throughput versus offered traffic for all three protocols, as well as for pure and slotted ALOHA.

CSMA with Collision Detection:

Persistent and nonpersistent 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 saves time and bandwidth.

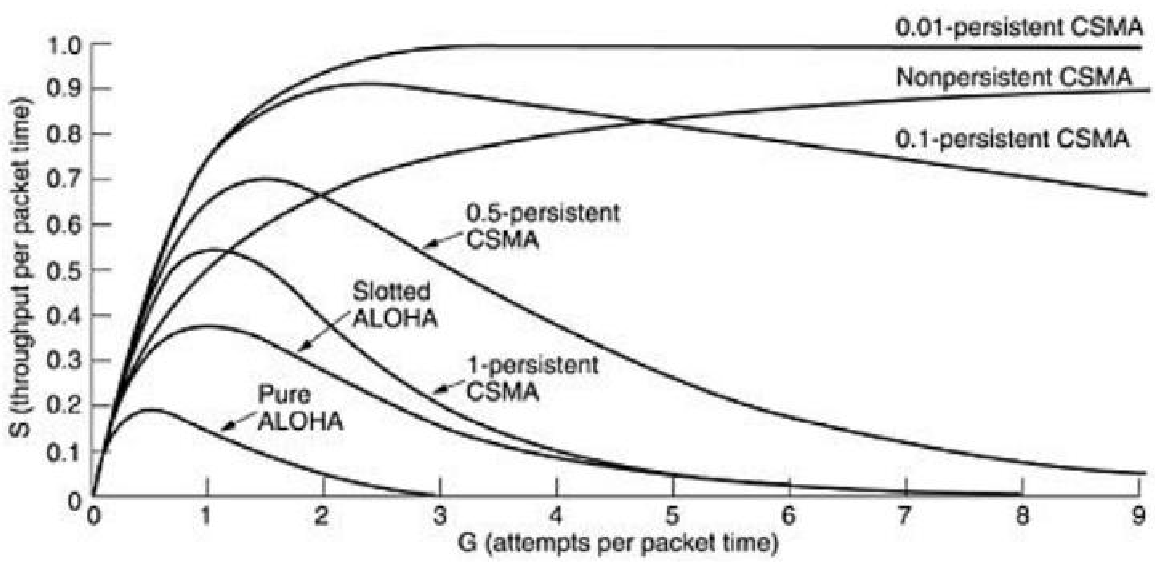


Figure.4 Comparison of the channel utilization versus load for various random access protocols

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 of Figure.5. At the point marked t0, 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.

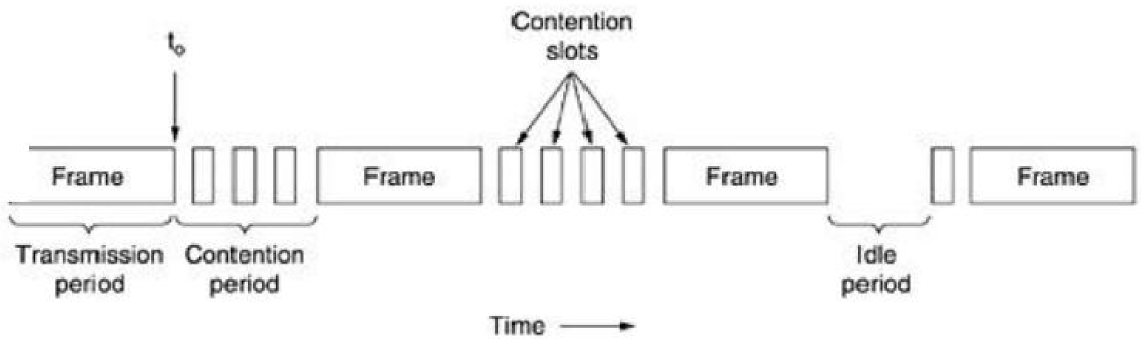


Figure.5. CSMA/CD can be in one of three states: contention, transmission, or idle After a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime. Therefore, our model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet (e.g., for lack of work).

The physical layer is dependent on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there is only one MAC sublayer for Standard Ethernet, there is a different physical layer specifications for each Ethernet implementations.

Standard Ethernet

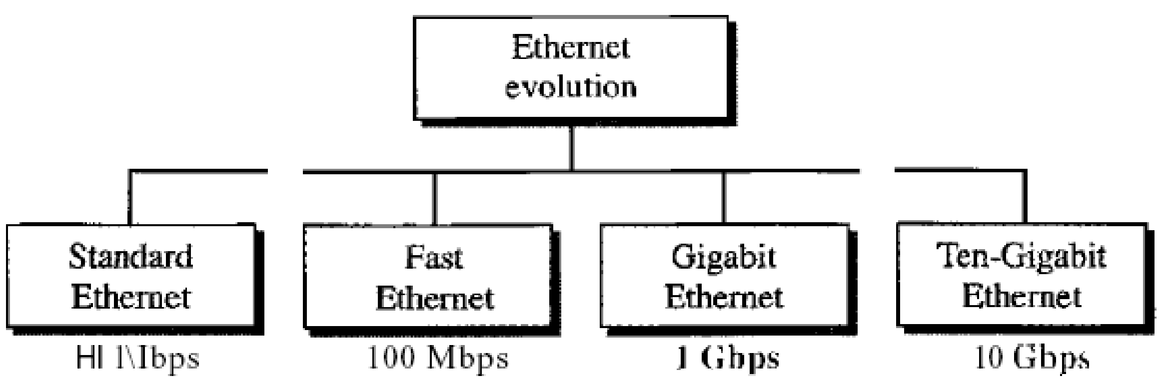


Figure 6 Ethernet evolution through four generations

Encoding and Decoding

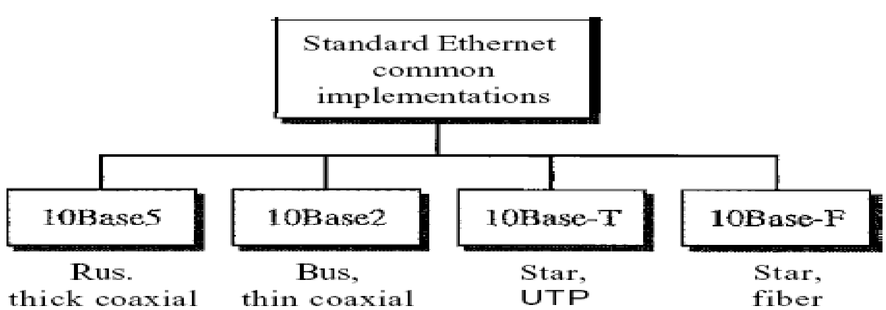


Figure 7. Implementation of Ethernet

Fast Ethernet

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.

The goals of Fast Ethernet can besummarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

Logical Link Control (LLC)

It was known that data link control handles framing, flow control, and error control. In IEEE Project 802, flow control, error control,and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer.

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent. Figure 1 shows one single LLC protocol serving several MAC protocols. Framing LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP). The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in Figure 6.

Need for LLC The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper-layer protocols such as IP, do not use the services of LLC.

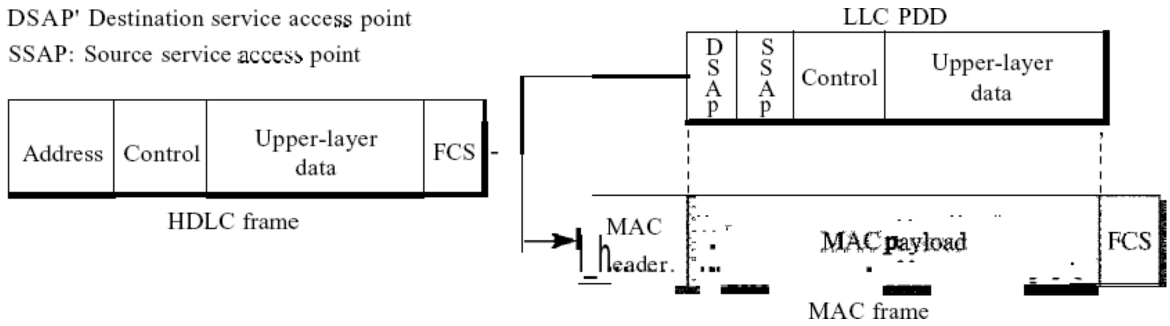


Figure 8 ***HDLC frame compared with LLC and MAC frames***

Network Layer Design Issues

1. Store-and-forward packet switching 2. Services provided to transport layer 3. Implementation of connectionless service 4. Implementation of connection-oriented service 5. Comparison of virtual-circuit and datagram networks

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 ISP. The packet is stored there until it has fully arrived and the link has finished its processing by verifying the checksum. Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching.

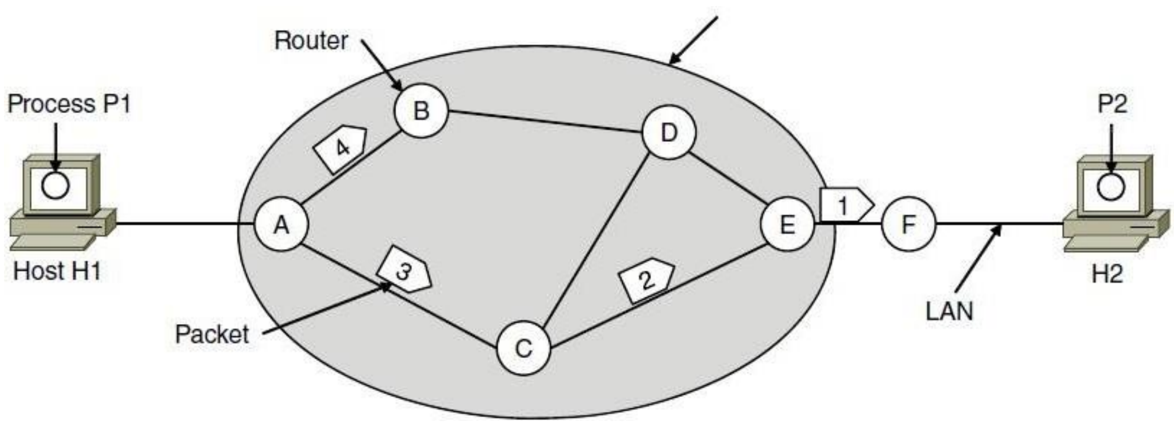
Services provided to transport layer

The network layer provides services to the transport layer at the network layer/transport layer interface. The services need to be carefully designed with the following goals in mind:

1. Services independent of router technology.
2. Transport layer shielded from number, type, topology of routers.
3. Network addresses available to transport layer use uniform numbering plan even across LANs and WANs

Implementation of connectionless service

If connectionless service is offered, packets are injected into the network 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 network is called a d**atagram network**.



A's table (initially) A's table (later) C's Table E's Table

A	⊠
B	B
C	C
D	B
E	C
F	C

Dest. Line

A	⊠
B	B
C	C
D	B
E	D
F	D

A	A
B	A
C	⊠
D	E
E	E
F	E

A	C
B	D
C	C
D	D
E	⊠
F	F

Figure 9. Datagram Network

Let us assume for this example that the message is four times longer than the maximum packetsize,sothenetwork layerhastobreakitintofourpackets,1,2,3,and4,andsendeach of them in turn to router *A*.

Every router has an internal table telling it where to send packets for each of thepossible

destinations. Each table entry is a pair(destination and the outgoing line). Only directly connected lines can be used.

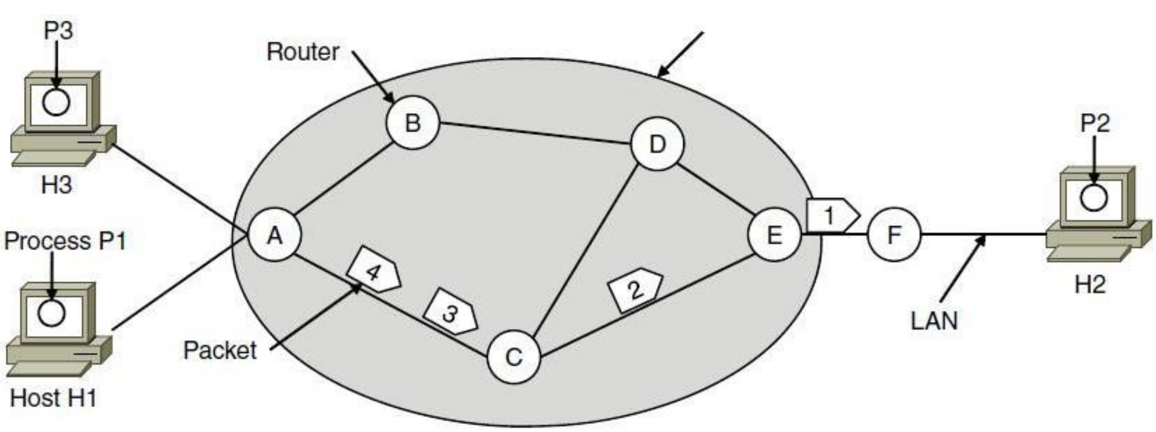
A's initial routing table is shown in the figure under the label ''initially.''

At *A*, packets 1, 2, and 3 are stored briefly, having arrived on the incoming link. Then each packet is forwarded according to *A*'s table, onto the outgoing link to *C* within a new frame. Packet 1 is then forwarded to *E* and then to *F*.

However, something different happens to packet 4. When it gets to *A* it is sent to router *B*, even though it is also destinedfor*F*.Forsomereason(trafficjamalongACEpath),*A* decided to send packet 4 via a different route than that of the first three packets. Router A 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**.

Implementation of connection-oriented service



A'stable C'sTable E's Table

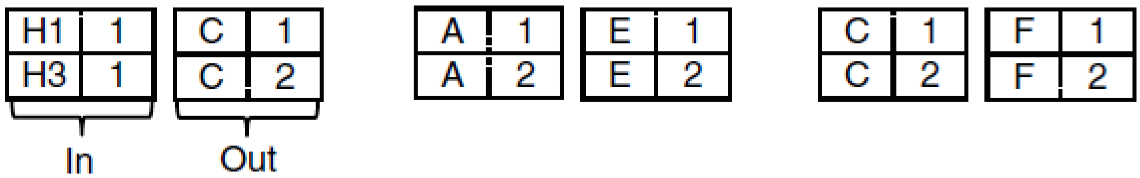


Figure 10. Implementation of connection-oriented service

If connection-oriented service is used, a path from the source router all the way to the destination router must be established before any data packets can be sent. This connection is called a **VC** (**virtual circuit**), and the network is called a **virtual-circuit network**

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.

Table 1 : Datagram Network versus Virtual-circuit Network

Issue	Datagram network	Virtual-circuit network
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

As an example, consider the situation shown in Figure. Here, host *H1* has established connection 1 with host *H2*. This connection 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 1.

Now let us consider what happens if *H3* also wants to establish a connection to *H2*. It chooses connection identifier 1 (because it is initiating the connection and this is its only connection) and tells the network 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.

Comparison of virtual-circuit and datagram networks

Routing Algorithms

The main function of NL (Network Layer) is routing packets from the source machine to the destination machine.

There are two processes inside router:

a) One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing table. This process is forwarding.
b) The other process is responsible for filling in and updating the routing tables. That is where the routing algorithm comes into play. This process is routing.

Regardless of whether routes are chosen independently for each packet or only when new connections are established, certain properties are desirable in a routing algorithm **correctness, simplicity, robustness, stability, fairness, optimality**

Routing algorithms can be grouped into two major classes:

1) Nonadaptive (Static Routing)

---

2) Adaptive. (Dynamic Routing)

Nonadaptive algorithm do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J is computed in advance, off line, and downloaded to the routers when the network is booted. This procedure is sometimes called static routing.

Adaptive algorithm, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well.

Adaptive algorithms differ in

1) Where they get their information (e.g., locally, from adjacent routers, or from all routers),
2) When they change the routes (e.g., every ΔT sec, when the load changes or when the topology changes), and

3) What metric is used for optimization (e.g., distance, number of hops, or estimated transit time).
This procedure is called dynamic routing

Different Routing Algorithms

- Optimality principle
- Shortest path algorithm
- Flooding
- Distance vector routing
- Link state routing

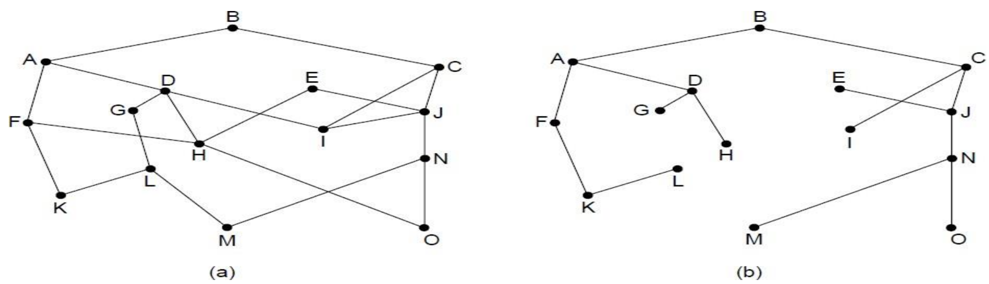
- Hierarchical Routing

The Optimality Principle

One can make a general statement about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle.

It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same

As a direct consequence of the optimality principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a **sink tree**. The goal of all routing algorithms is to discover and use the sink trees for all routers.



a) A network. (b) A sink tree for router *B.*

Figure 11. Implementation of connection-oriented service

Shortest Path Routing(Dijkstra's)

The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line or link.

To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph

1. Start with the local node (router) as the root of the tree. Assign a cost of 0 to this node and make it the first permanent node.
2. Examine each neighbor of the node that was the last permanent node.
3. Assign a cumulative cost to each node and make it tentative
4. Among the list of tentative nodes
   a. Find the node with the smallest cost and make it Permanent
   b. If a node can be reached from more than one route then select the route with the shortest cumulative cost.
5. Repeat steps 2 to 4 until every node becomes permanent

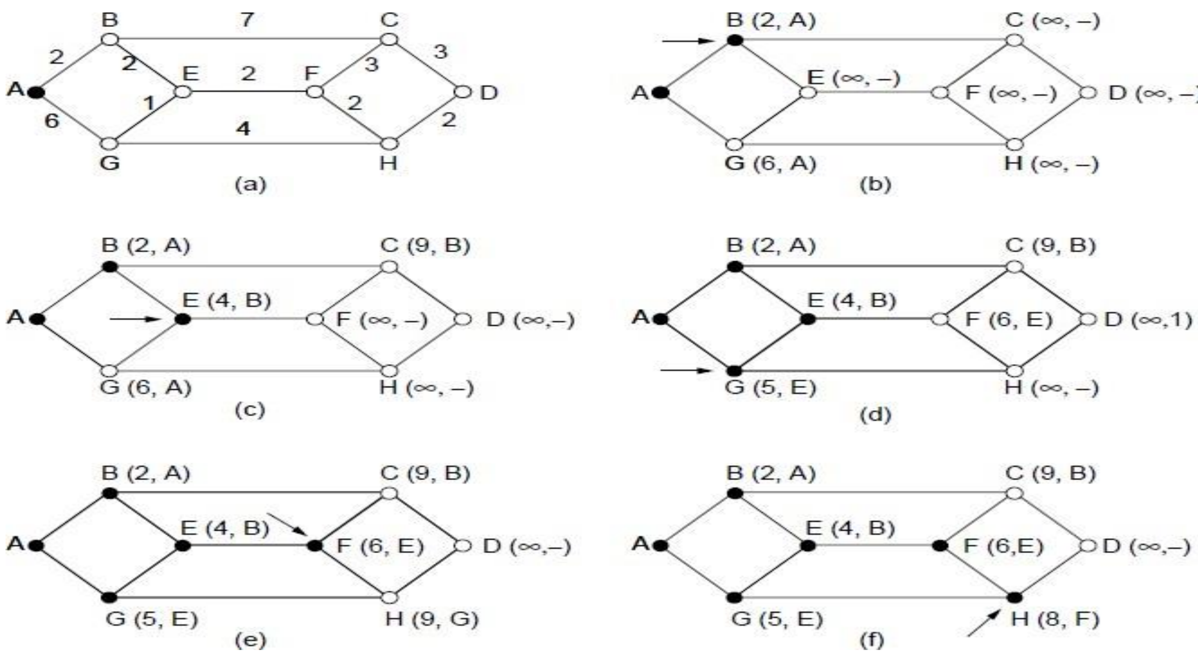
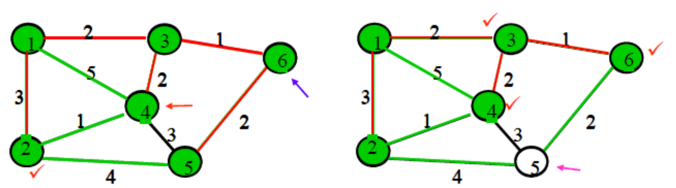


Figure 12. Implementation of connection-oriented service

Execution of Dijkstra's algorithm



Iteration	Permanent	tentative	D_2	D_3	D_4	D_5	D_6
Initial	{1}	{2,3,4}	3	2 ✓	5	∞	∞
1	{1,3}	{2,4,6}	3 ✓	2	4	∞	3
2	{1,2,3}	{4,6,5}	3	2	4	7	3 ✓
3	{1,2,3,6}	{4,5}	3	2	4 ✓	5	3
4	{1,2,3,4,6}	{5}	3	2	4	5 ✓	3
5	{1,2,3,4,5,6}	{}	3	2	4	5	3

Flooding

- Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on.
- Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.
- One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero. Ideally, the hop counter should be initialized to the length of the path from source to destination.
- A variation of flooding that is slightly more practical is **selective flooding**. In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction.
- Flooding is not practical in most applications.

Intra- and Inter domain Routing

An autonomous system (AS) is a group of networks and routers under the authority of a single administration.

Routing inside an autonomous system is referred to as intra domain routing. (DISTANCE VECTOR, LINK STATE)

Routing between autonomous systems is referred to as inter domain routing. (PATH VECTOR) Each autonomous system can choose one or more intra domain routing protocols to handle routing inside the autonomous system. However, only one inter domain routing protocol handles routing between autonomous systems.

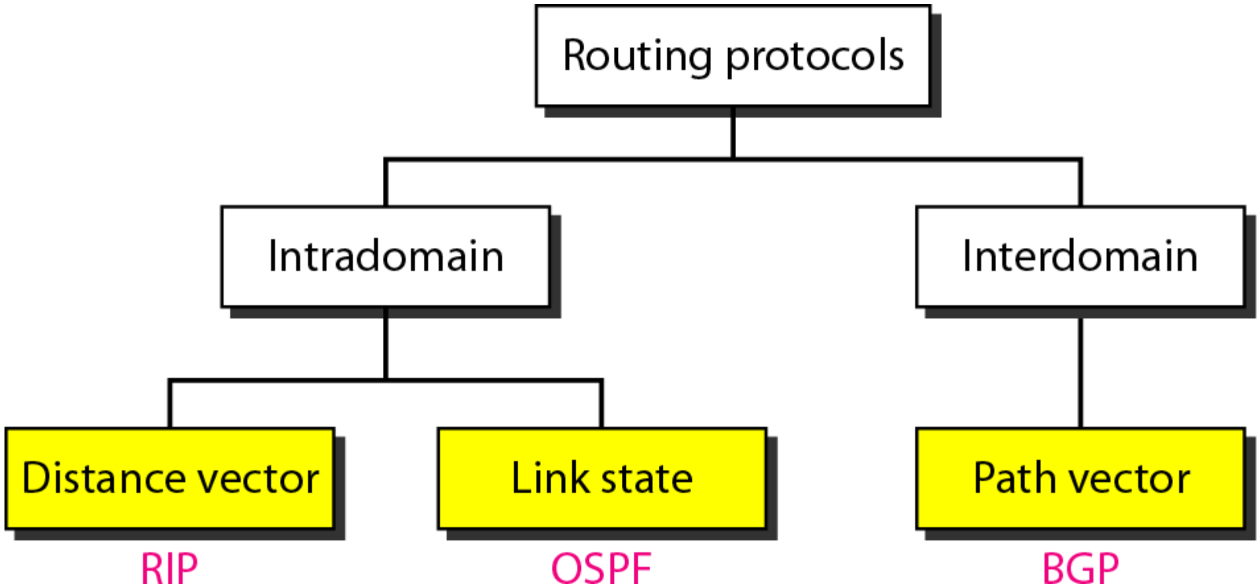


Figure 13. Routing Protocols

Distance Vector Routing

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.

Mainly 3 things inthis

Initialization
Sharing Updating

Initialization

Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. Below fig shows the initial tables for each node. The distance for any entry that is not a neighbor is marked as infinite(unreachable).

Initialization of tables in distance vector routing

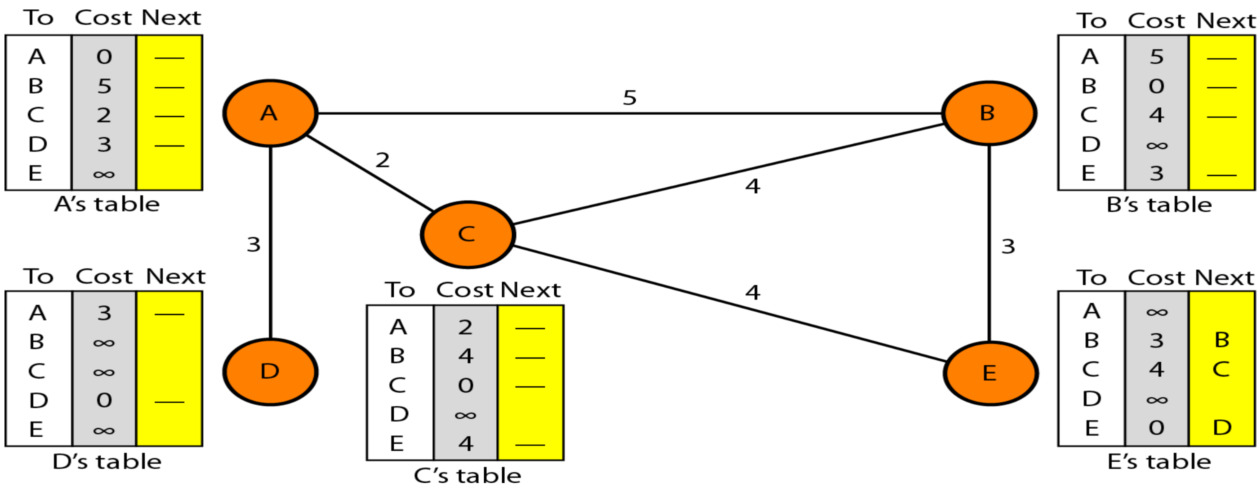


Figure 14. Distance Vector Routing Algorithm working

<u>Sharing</u>

The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

NOTE: In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change

Updating

When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. (x+y)
2. If the receiving node uses information from any row. The sending node is the next node in the route.
3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.
    a. If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
    b. If the next-node entry is the same, the receiving node chooses the new row.

For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller. The old route does not exist anymore. The new route has a distance of infinity.

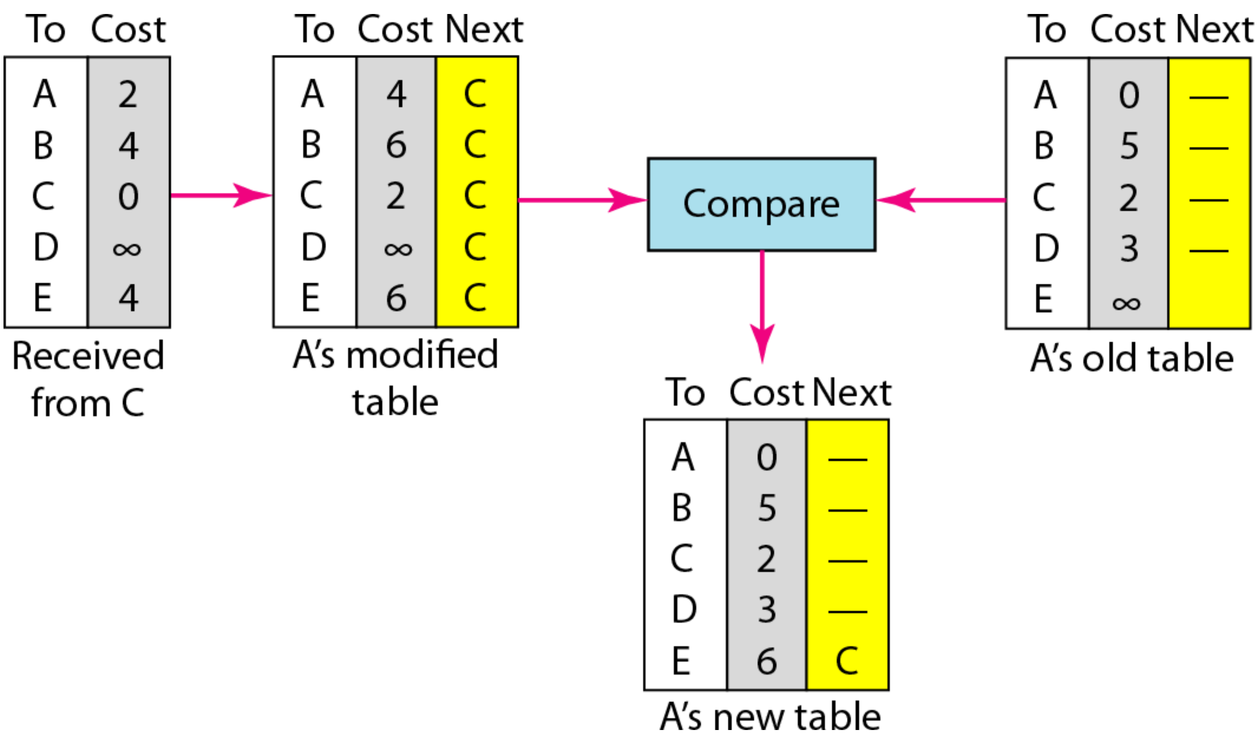


Figure 15. Updating in distance vector routing

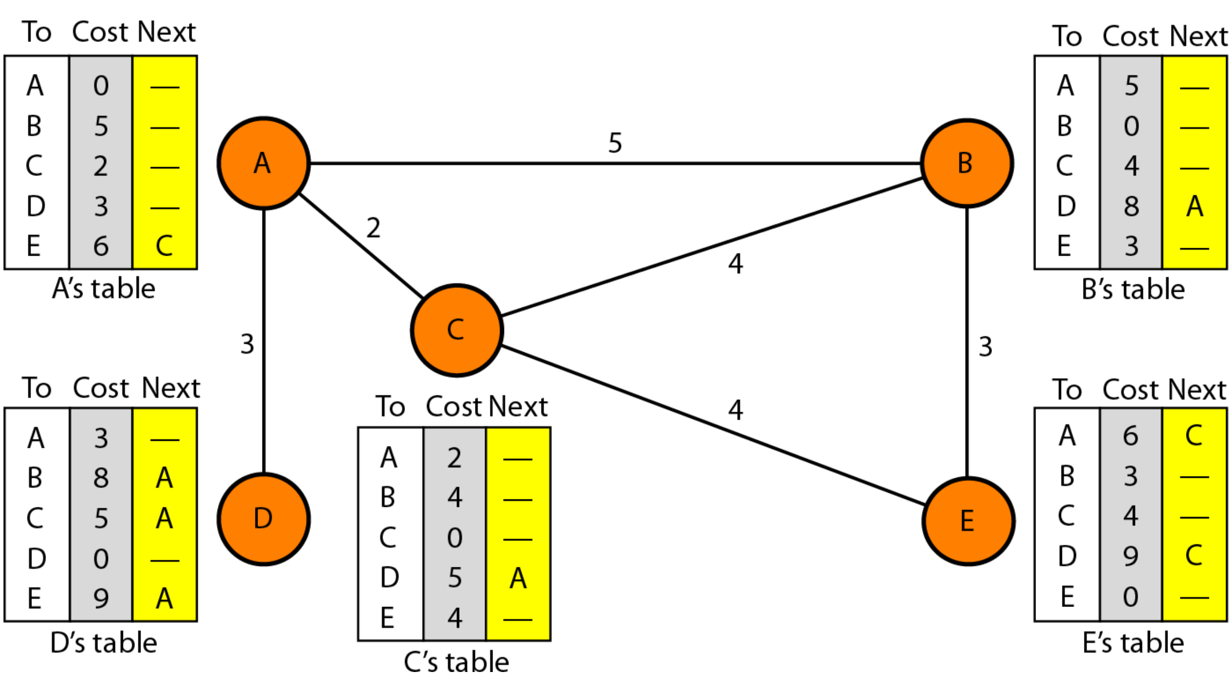


Figure 16. Final Diagram

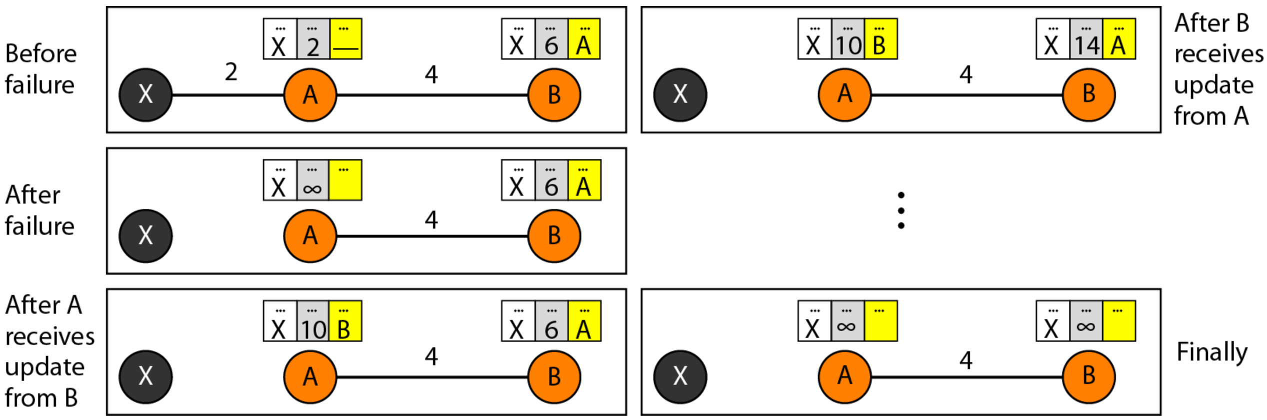
When to Share :

The question now is, When does a node send its partial routing table (only two columns) to all its immediate neighbors? The table is sent both periodically and when there is a change in the table.

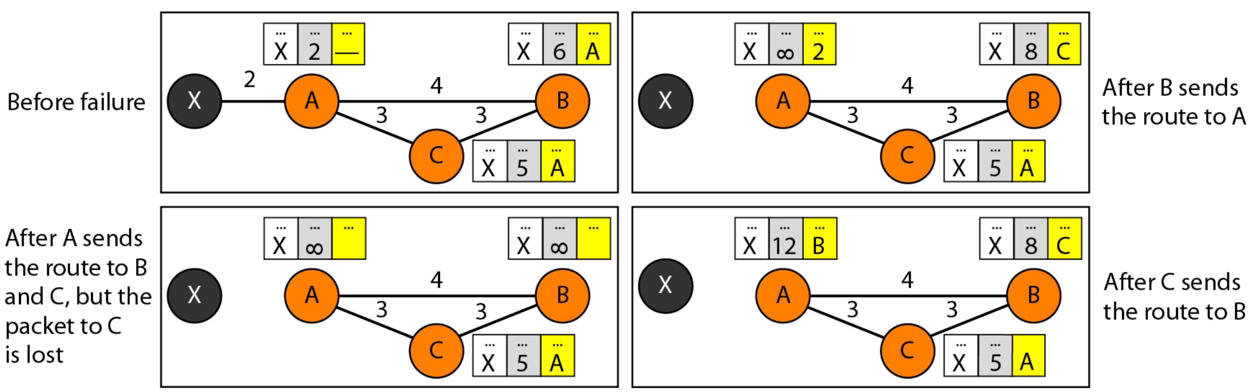
Periodic Update A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

Triggered Update A node sends its two-column routing table to its neighbors anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

1. A node receives a table from a neighbor, resulting in changes in its own table after updating.
2. A node detects some failure in the neighboring links which results in a distance change to infinity.



Two-node instability



Three-node instability

Figure 17. Node Instability

SOLUTIONS FOR INSTABILITY

1. **Defining Infinity:** redefine infinity to a smaller number, such as 100. For our previous scenario, the system will be stable in less than 20 updates. As a matter of fact, most implementations of the distance vector protocol define the distance between each node to be 1 and define 16 as infinity. However, this means that the distance vector routing cannot be used in large systems. The size of the network, in each direction, cannot exceed 15 hops.

2. **Split Horizon:** In this strategy, instead of flooding the table through each interface, each node sends **only part of its table** through each interface. If, according to its table, node B thinks that the optimum route to reach X is via A, it does not need to advertise this piece of information to A; the information has come from A (A already knows). Taking information from node A, modifying it, and sending it back to node A creates the confusion. In our scenario, node B eliminates the last line of its routing table before it sends it to A. In this case, node A keeps the value of infinity as the distance to X. Later when node A sends its routing table to B, node B also corrects its routing table. The system becomes stable after the first update: both node A and B know that X is not reachable.

3. **Split Horizon and Poison Reverse** Using the split horizon strategy has one drawback. Normally, the distance vector protocol uses a timer, and if there is no news about a route, the node deletes the route from its table. When node B in the previous scenario eliminates the route to X from its advertisement to A, node A cannot guess that this is due to the split horizon strategy (the source of information was A) or because B has not received any news about X recently. The split horizon strategy can be combined with the poison reverse strategy. Node B can still advertise the value for X, but if the source of information is A, it can replace the distance with infinity as a warning: "Do not use this value; what I know about this route comes from you."

The Count-to-Infinity Problem

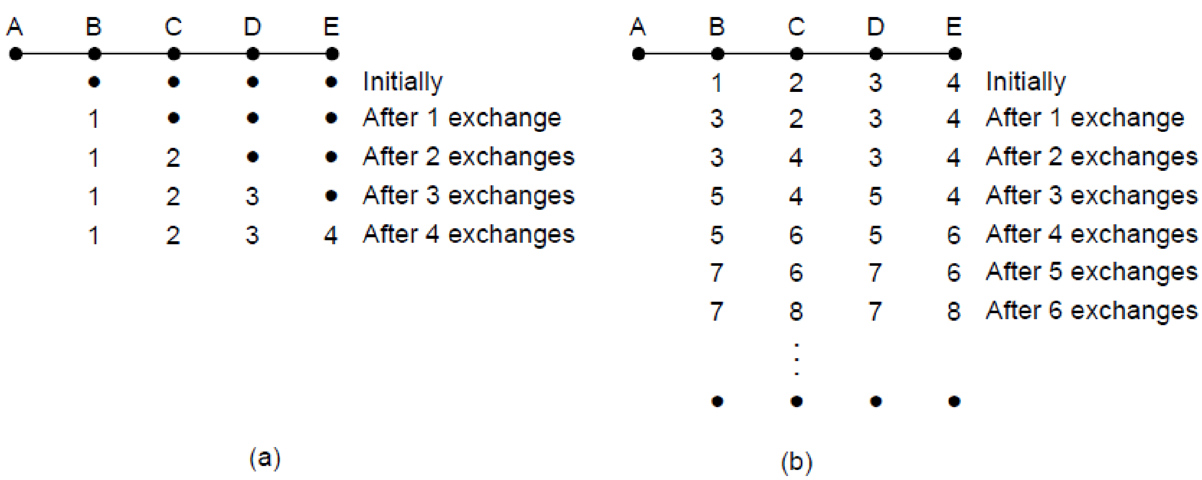


Figure 18. Count to Infinity Problem

Link State Routing

Link state routing is based on the assumption that, although the global knowledge about the topology is not clear, each node has partial knowledge: it knows the state (type, condition, and cost) of its links. **In other words, the whole topology can be compiled from the** partial knowledge of each node

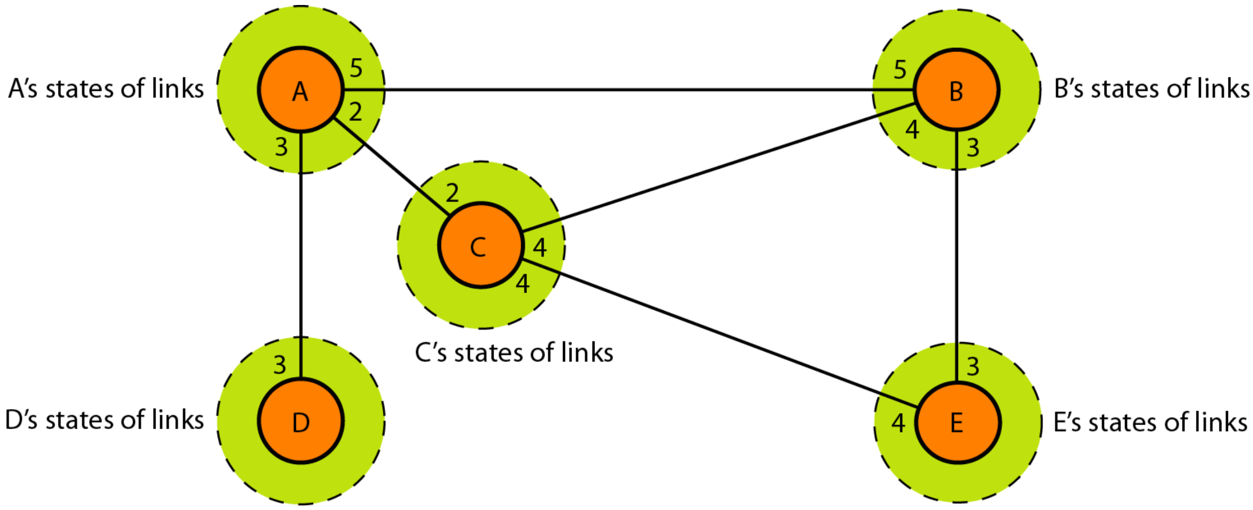


Figure 19. Link State Routing

Building Routing Tables

1. Creation of the states of the links by each node, called the link state packet (LSP).
2. Dissemination of LSPs to every other router, called **flooding, in an efficient and** reliable way.
3. Formation of a shortest path tree for each node.
4. Calculation of a routing table based on the shortest path tree

I. **Creation of Link State Packet (LSP)** A link state packet can carry a large amount of information. For the moment, we assume that it carries a minimum amount of data: the node identity, the list of links, a sequence number, and age. The first two, node identity and the list of links, are needed to make the topology. The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones. The fourth, age, prevents old LSPs from remaining in the domain for a long time.
LSPs are generated on two occasions:

   1. When there is a change in the topology of the domain
   2. on a periodic basis: The period in this case is much longer compared to distance vector. The timer set for periodic dissemination is normally in the range of **60 min or 2 h** based on the implementation. A longer period ensures that flooding does not create too much traffic on the network.

II. **Flooding of LSPs:** After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbors. The process is called flooding and based on the following

   1. The creating node sends a copy of the LSP out of each interface

2. A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. If it is newer, the node does the following:

a. It discards the old LSP and keeps the new one.

b. It sends a copy of it out of each interface except the one from which the packet arrived. This guarantees that flooding stops somewhere in the domain (where a node has only one interface).

Formation of Shortest Path Tree: Dijkstra Algorithm

A shortest path tree is a tree in which the path between the root and every other node is the shortest.

The Dijkstra algorithm creates a shortest path tree from a graph. The algorithm divides the nodes into two sets: **tentative and permanent.** It finds the neighbors of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent.

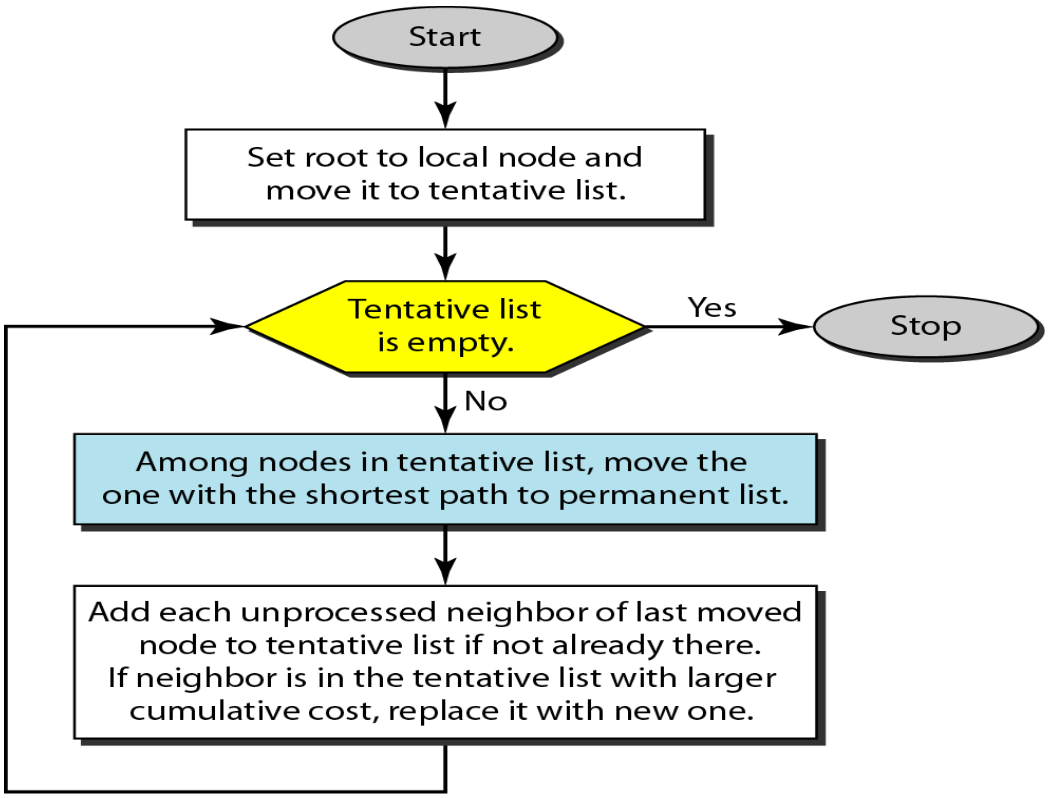


Figure 20. Dijkstra Algorithm

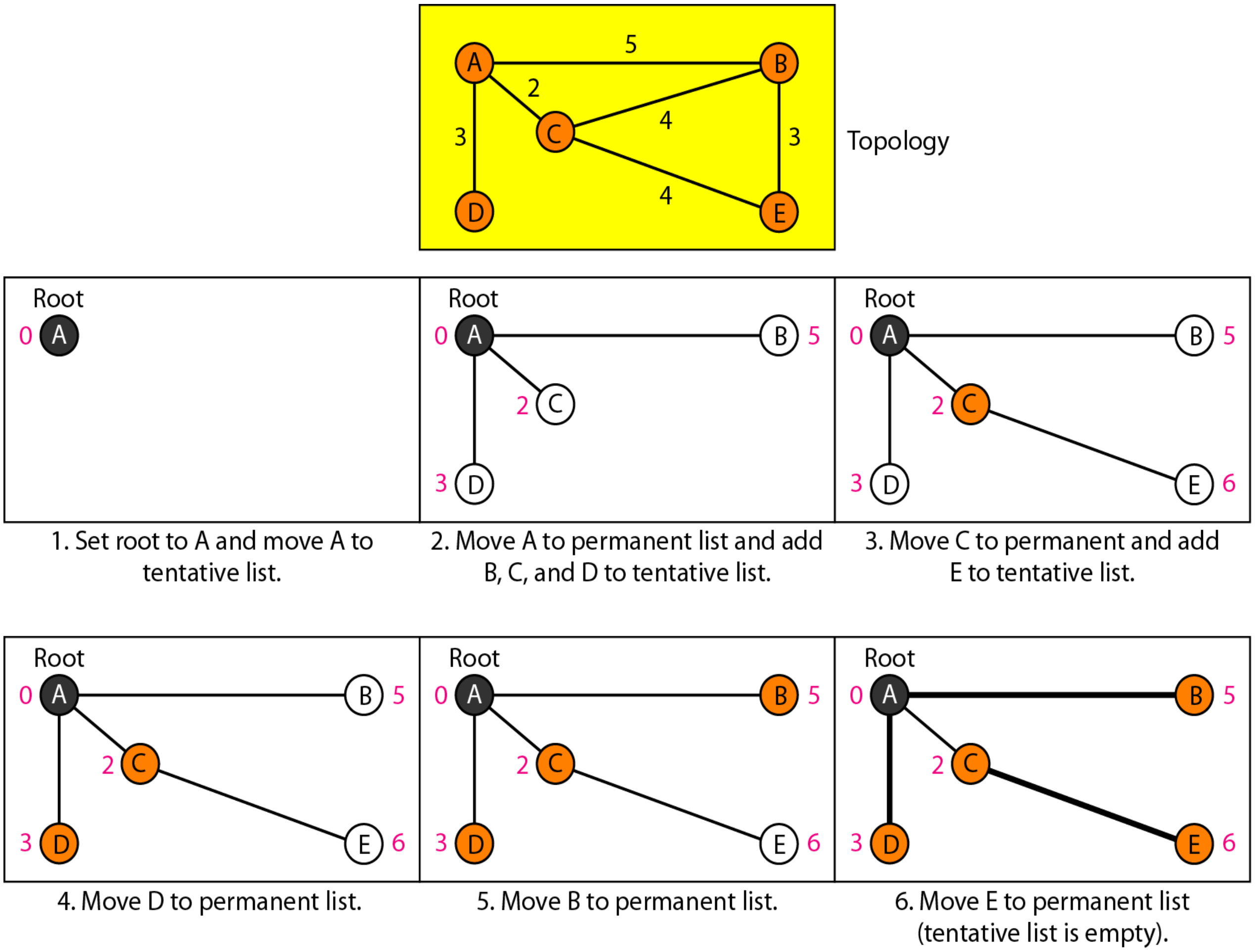


Figure 20. (a) Dijkstra Algorithm

III. Calculation of a routing table

Node	*Cost*	*Next Router*
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

Figure 21 . Routing table for node A

Path Vector Routing

Distance vector and link state routing are both intra domain routing protocols. They can be used inside an autonomous system, but not between autonomous systems. These two protocols are not suitable for inter domain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. **Distance vector routing is subject to instability** in the domain of operation. **Link state routing needs a huge amount of resources** to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.

Path vector routing proved to be useful for inter domain routing. The principle of path vector routing is similar to that of distance vector routing. **In path vector routing, we assume that there is one node** (there can be more, but one is enough for our conceptual discussion) **in each AS** that acts on behalf of the entire AS. Let us call it the **speaker node**. The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs. The idea is the same as for distance vector routing except that only speaker nodes in each AS can communicate with each other. However, what is advertised is different. A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems

Initialization

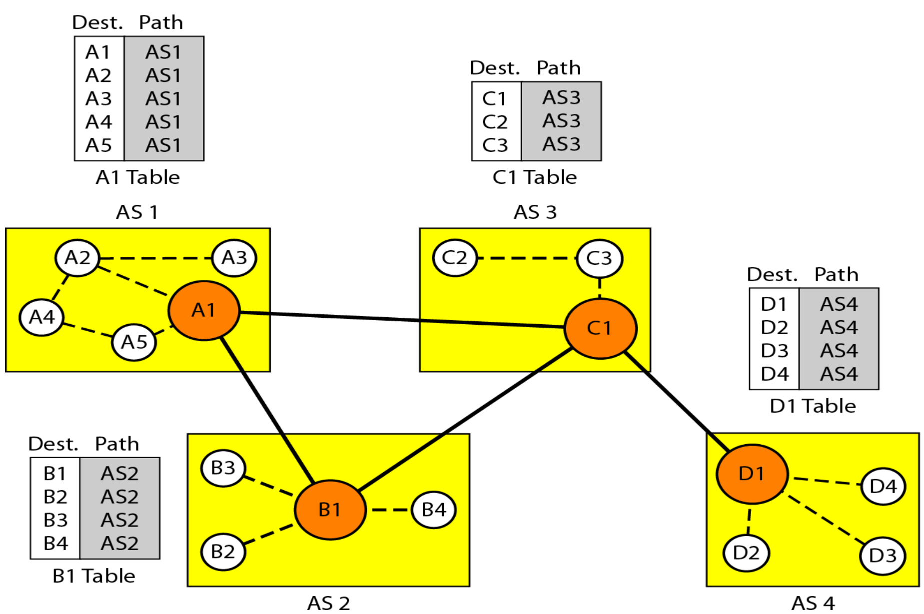


Figure 22 . Initial routing tables in path vector routing

Sharing

Just as in distance vector routing, in path vector routing, a speaker in an autonomous system shares its table with immediate neighbors. In Figure, node A1 shares its table with nodes B1 and C1. Node C1 shares its table with nodes D1, B1, and A1. Node B1 shares its table with C1 and A1. Node D1 shares its table with C1.

Dest.	Path
A1 … A5	AS1 … AS1
B1 … B4	AS1-AS2 … AS1-AS2
C1 … C3	AS1-AS3 … AS1-AS3
D1 … D4	AS1-AS2-AS4 … AS1-AS2-AS4

A1 Table

Dest.	Path
A1 … A5	AS2-AS1 … AS2-AS1
B1 … B4	AS2 … AS2
C1 … C3	AS2-AS3 … AS2-AS3
D1 … D4	AS2-AS3-AS4 … AS2-AS3-AS4

B1 Table

Dest.	Path
A1 … A5	AS3-AS1 … AS3-AS1
B1 … B4	AS3-AS2 … AS3-AS2
C1 … C3	AS3 … AS3
D1 … D4	AS3-AS4 … AS3-AS4

C1 Table

Dest.	Path
A1 … A5	AS4-AS3-AS1 … AS4-AS3-AS1
B1 … B4	AS4-AS3-AS2 … AS4-AS3-AS2
C1 … C3	AS4-AS3 … AS4-AS3
D1 … D4	AS4 … AS4

D1 Table

Figure 23 . Sharing information

<u>Updating</u>

When a speaker node receives a two-column table from a neighbor, it updates its own table by adding the nodes that are not in its routing table and adding its own autonomous system and the autonomous system that sent the table. After a while each speaker has a table and knows how to reach each node in other Ass

a) **Loop prevention**. The instability of distance vector routing and the creation of loops can be avoided in path vector routing. When a router receives a message, it checks to see if its AS is in the path list to the destination. If it is, looping is involved and the message is ignored.

b) **Policy routing**. Policy routing can be easily implemented through path vector routing. When a router receives a message, it can check the path. If one of the AS listed in the path is against its policy, it can ignore that path and that destination. It does not update its routing table with this path, and it does not send this message to its neighbors.

c) **Optimum path.** What is the optimum path in path vector routing? We are looking for a path to a destination that is the best for the organization that runs the AS. One system may use RIP, which defines hop count as the metric; another may use OSPF with minimum delay defined as the metric. In our previous figure, each AS may have more than one path to a destination. For example, a path from AS4 to ASI can be AS4-AS3-AS2-AS1, or it can be AS4- AS3-ASI. For the tables, **we chose the one that had the smaller number of ASs,** but this is not always the case. Other criteria, such as security, safety, and reliability, can also be applied

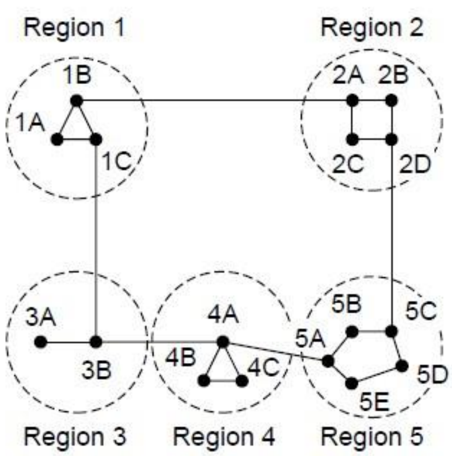
Hierarchical Routing

As networks grow in size, the router routing tables grow proportionally. Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them and more bandwidth is needed to send status reports about them.

At a certain point, the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically, as it is in the telephone network.

When hierarchical routing is used, the routers are divided into what we will call regions. Each router knows all the details about how to route packets to destinations within its own region but knows nothing about the internal structure of other regions.

For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regionsintoclusters,the clustersintozones,thezonesintogroups,andsoon,untilwerunout of names foraggregations



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Figure 24 . Hierarchical Routing

When a single network becomes very large, an interesting question is ‘‘how many levels

should the hierarchy have?’’

Forexample,consideranetworkwith720routers.Ifthereisnohierarchy,eachrouterneeds 720 routing tableentries.

If the network is partitioned into 24 regions of 30 routers each, each router needs 30 local entries plus 23 remote entries for a total of 53 entries.

If a three-level hierarchy is chosen, with 8 clusters each containing 9 regions of 10 routers, each router needs 10 entries for local routers, 8 entries for routing to other regions within its own cluster, and 7 entries for distant clusters, for a total of 25 entries

Kamoun and Kleinrock (1979) discovered that the optimal number of levels for an *N router network is ln N, requiring a total of e ln N entries per router*

CONGESTION CONTROL ALGORITHMS

Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called **congestion.**

The network and transport layers share the responsibility for handling congestion. Since congestion occurs within the network, it is the network layer that directly experiences it and must ultimately determine what to do with the excess packets.

However, the most effective way to control congestion is to reduce the load that the transport layer is placing on the network. This requires the network and transport layers to work together. In this chapter we will look at the network aspects of congestion.

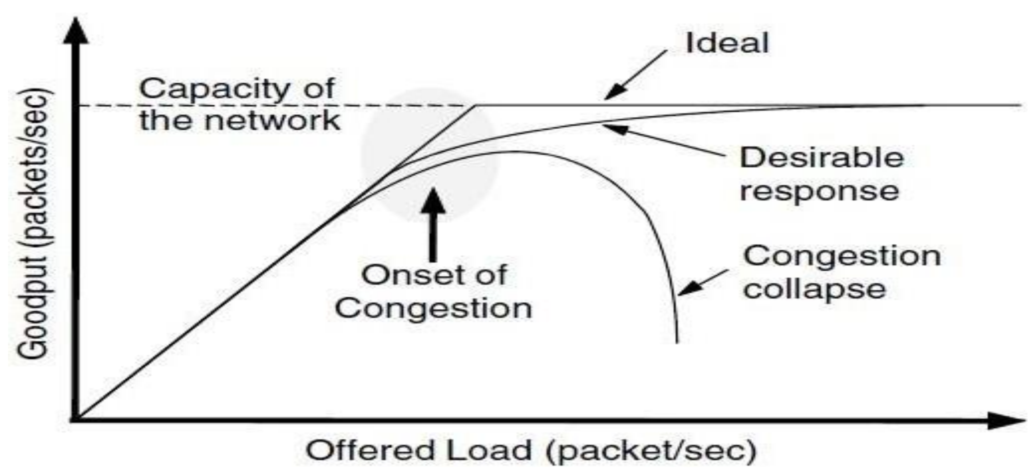


Figure 25 . Congestion Scenario

When too much traffic is offered, congestion sets in and performance degrades sharply

Above Figure depicts the onset of congestion. When the number of packets hosts send into the network is well within its carrying capacity, the number delivered is proportional to the number sent. If twice as many are sent, twice as many are delivered. However, as the offered load approaches the carrying capacity, bursts of traffic occasionally fill up the buffers inside routers and some packets are lost. These lost packets consume some of the capacity, so the number of delivered packets falls below the ideal curve. The network is now congested. Unless the network is well designed, it may experience a **congestion collapse**

<u>difference between congestion control and flow control</u>.

Congestion control has to do with making sure the network is able to carry the offered traffic. It is a global issue, involving the behavior of all the hosts and routers.

Flow control, in contrast, relates to the traffic between a particular sender and a particular receiver. Its job is to make sure that a fast sender cannot continually transmit data faster than the receiver is able to absorb it.

To see the difference between these two concepts, consider a network made up of 100-Gbps fiber optic links on which a supercomputer is trying to force feed a large file to a personal computer that is capable of handling only 1 Gbps. Although there is no congestion (the network itself is not in trouble), flow control is needed to force the supercomputer to stop frequently to give the personal computer a chance to breathe.

At the other extreme, consider a network with 1-Mbps lines and 1000 large computers, half of which are trying to transfer files at 100 kbps to the other half. Here, the problem is not that of fast senders overpowering slow receivers, but that the total offered traffic exceeds what the network can handle.

The reason congestion control and flow control are often confused is that the best way to handle both problems is to get the host to slow down. Thus, a host can get a ‘‘slow down’’ message either because the receiver cannot handle the load or because the network cannot handle it.

Several techniques can be employed. These include:

1. Warning bit
2. Choke packets
3. Load shedding
4. Random early discard
5. Traffic shaping

The first 3 deal with congestion detection and recovery. The last 2 deal with congestion avoidance

Warning Bit

1. A special bit in the packet header is set by the router to warn the source when congestion is detected.
2. The bit is copied and piggy-backed on the ACK and sent to the sender.
3. The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly.

Choke Packets

1. A more direct way of telling the source to slow down.
2. A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow.
3. The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.
4. An example of a choke packet is the ICMP Source Quench Packet. Hop-by-Hop Choke Packets

1. Over long distances or at high speeds choke packets are not very effective.
2. A more efficient method is to send to choke packets hop-by-hop.
3. This requires each hop to reduce its transmission even before the choke packet arrive at the source

Load Shedding

1. When buffers become full, routers simply discard packets.
2. Which packet is chosen to be the victim depends on the application and on the error strategy used in the data link layer.
3. For a file transfer, for, e.g. cannot discard older packets since this will cause a gap in the received data.
4. For real-time voice or video it is probably better to throw away old data and keep new packets.
5. Get the application to mark packets with discard priority.

Random Early Discard (RED)

1. This is a proactive approach in which the router discards one or more packets *before* the buffer becomes completely full.
2. Each time a packet arrives, the RED algorithm computes the average queue length, ***avg***.
3. If *avg* is lower than some lower threshold, congestion is assumed to be minimal or non- existent and the packet is queued.
4. If *avg* is greater than some upper threshold, congestion is assumed to be serious and the packet is discarded.
5. If *avg* is between the two thresholds, this might indicate the onset of congestion. The probability of congestion is then calculated.

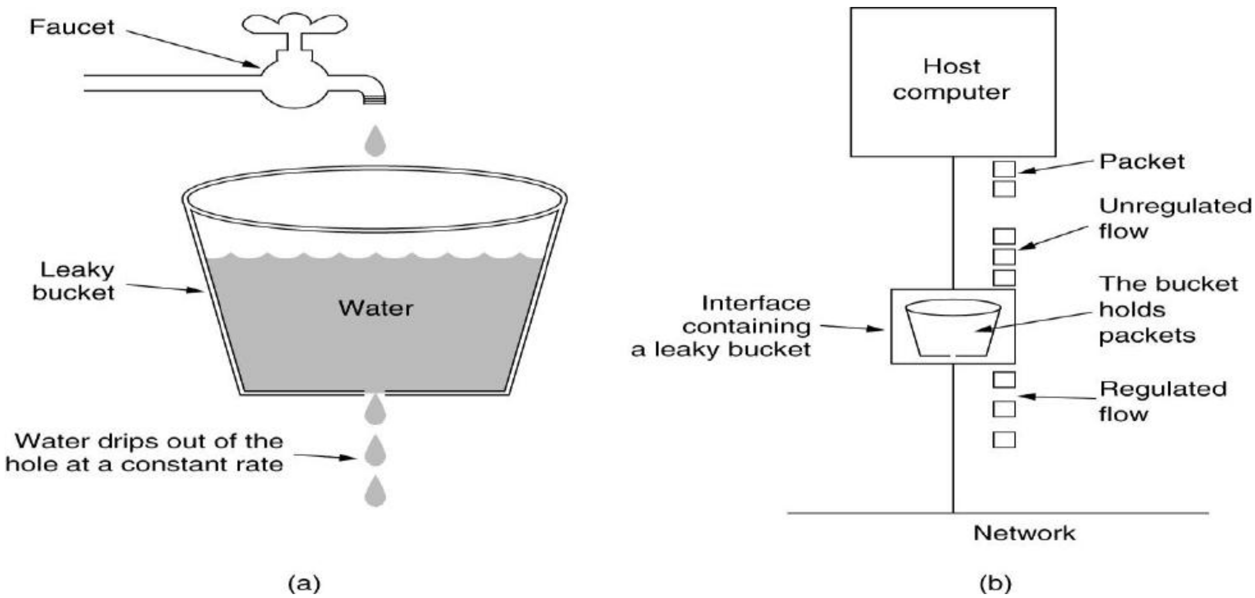
Traffic Shaping

1. Another method of congestion control is to "shape" the traffic before it enters the network.
2. Traffic shaping controls the *rate* at which packets are sent (not just how many). Used in ATM and Integrated Services networks.
3. At connection set-up time, the sender and carrier negotiate a traffic pattern (shape).

Two traffic shaping algorithms are:

Leaky Bucket Token
Bucket

The **Leaky Bucket Algorithm** used to control rate in a network. It is implemented as a single- server queue with constant service time. If the bucket (buffer) overflows then packets are discarded.



(a) A leaky bucket with water. (b) a leaky bucket with packets.

Figure 26 . Leaky Bucket Algorithm

1. The leaky bucket enforces a constant output rate (average rate) regardless of the burstiness of the input. Does nothing when input is idle.
2. The host injects one packet per clock tick onto the network. This results in a uniform flow of packets, smoothing out bursts and reducing congestion.
3. When packets are the same size (as in ATM cells), the one packet per tick is okay. For variable length packets though, it is better to allow a fixed number of bytes per tick. E.g. 1024 bytes per tick will allow one 1024-byte packet or two 512-byte packets or four 256- byte packets on 1 tick

Token Bucket Algorithm

1. IncontrasttotheLB,theTokenBucketAlgorithm,allowstheoutput ratetovary, depending on the size of the burst.
2. IntheTBalgorithm,thebucketholdstokens.Totransmitapacket,thehostmust capture and destroy onetoken.
3. Tokens are generated by a clock at the rate of one token every □t sec.
4. Idlehostscancaptureandsaveuptokens(uptothemax.sizeofthebucket)in orderto send larger burstslater.

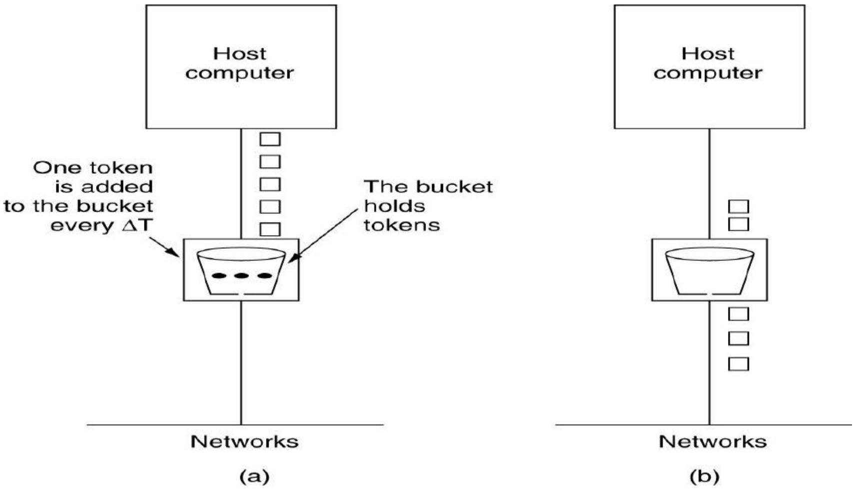


Figure 27 . Token Bucket Algorithm a) Before (b) After.

Leaky Bucket vs. Token Bucket

1. LB discards packets; TB does not. TB discards tokens.
2. WithTB,apacketcanonlybetransmittedifthereareenoughtokenstocoverits lengthin bytes.
3. LBsendspacketsatanaveragerate.TBallowsforlargeburststobesentfasterby speeding up the output.
4. TBallowssavinguptokens(permissions)tosendlargebursts.LBdoesnotallowsaving.

Network layer in the Internet

The Mobile IP allows for location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home.

The main aim of the **Network Layer** the source-to- destination delivery of a packet across multiple networks (links). Whereas the data link **layer** oversees the delivery of a packet between two systems on the same **network** (links), the **network layer** ensures that each packet gets from its source to its final destination address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the tunnel.

Researchers create support for mobile networking without requiring any pre-deployed infrastructure as it currently is required by MIP. One such example is Interactive Protocol for Mobile Networking (IPMN) which promises supporting mobility on a regular IP network just from the network edges by intelligent signalling between IP at end-points and application layer module with improved quality of service.

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4. In December 1998, IPv6 became a Draft Standard for the IETF,who subsequently ratified it as an Internet Standard on 14 July 2017.

IPv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol. IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4). In addition to offering more addresses, IPv6 also implements features not present in IPv4. It simplifies aspects of address configuration, network renumbering, and router announcements when changing network connectivity providers. It simplifies processing of packets in routers by placing the responsibility for packet fragmentation into the end points. The IPv6 subnet size is standardized by fixing the size of the host identifier portion of an address to 64 bits.

Changes in IPv6 for Mobile IPv6

- A set of mobility options to include in mobility messages
- A new Home Address option for the Destination Options header
- A new Type 2 Routing header
- New Internet Control Message Protocol for IPv6 (ICMPv6) messages to discover the set of home agents and to obtain the prefix of the home link
- Changes to router discovery messages and options and additional Neighbor Discovery options
- Foreign Agents are no longer needed

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 ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – V DATA COMMUNICATION AND NETWORKING – SEC1306

UNIT V TRANSPORT LAYER AND APPLICATION LAYER

5.1 TRANSPORT LAYER

The Transport layer (also known as the Host-to-Host Transport layer) provides the Application layer with session and datagram communication services. The Transport layer encompasses the responsibilities of the OSI Transport layer. The core protocols of the Transport layer are TCP and UDP. TCP provides a one-to-one, connection-oriented, reliable communications service. TCP establishes connections, sequences and acknowledges packets sent, and recovers packets lost during transmission. In contrast to TCP, UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when an application developer does not want the overhead associated with TCP connections, or when the applications or upper-layer protocols provide reliable delivery. TCP and UDP operate over both IPv4 and IPv6 Internet layers.

Note The Internet Protocol (TCP/IP) component of Windows contains separate versions of the TCP and UDP protocols than the Microsoft TCP/IP Version 6 component does. The versions in the Microsoft TCP/IP Version 6 component are functionally equivalent to those provided with the Microsoft Windows NT® 4.0 operating systems and contain all the most recent security updates. The existence of separate protocol components with their own versions of TCP and UDP is known as a dual stack architecture. The ideal architecture is known as a dual IP layer, in which the same versions of TCP and UDP operate over both IPv4 and IPv6 (as Figure 2-1 shows). Windows Vista has a dual IP layer architecture for the TCP/IP protocol components.

Application Layer

The Application layer allows applications to access the services of the other layers, and it defines the protocols that applications use to exchange data. The Application layer contains many protocols, and more are always being developed. The most widely known Application layer protocols help users exchange information: The Hypertext Transfer Protocol (HTTP) transfers files that make up pages on the World Wide Web. The File Transfer Protocol (FTP) transfers individual files, typically for an interactive user session.

The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments.

Additionally, the following Application layer protocols help you use and manage TCP/IP networks: The Domain Name System (DNS) protocol resolves a host name, such as www.microsoft.com, to an IP address and copies name information between DNS servers. The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network.

The Simple Network Management Protocol (SNMP) collects and exchanges network management information between a network management console and network devices such as routers, bridges, and servers. Windows Sockets and NetBIOS are examples of Application layer interfaces for TCP/IP applications.

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

IP addressing

The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.

Host-to-host communications – IP determines the path a packet must take, based on the receiving system's IP address.

ARP Protocol

The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers.ARP assists IP in directing datagram's to the appropriate receiving system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:

Dropped packets – Packets that arrive too fast to be processed Connectivity failure – A destination system cannot be reached

Transport Layer

The TCP/IP transport layer ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets.

This type of communication is known as end-to-end. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service.
UDP provides unreliable datagram service.

TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by- character fashion, rather than as discrete packets. This transmission consists of the following:

SCTP Protocol

It is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP. Moreover, SCTP can support connections between systems that have more than one address, or multihued.The SCTP connection between sending and receiving system is called an association.

Application Layer

The application layer defines standard Internet services and network applications that anyone can use. These services work with the transport layer to send and receive data. Many application layer protocols exist.The following list shows examples of application layer protocols: 1.Standard TCP/IP services such as the ftp, tftp, and telnet commands

- **Node-to-node delivery**: At the data-link level, delivery of frames take place between two nodes connected by a point-to-point link or a LAN, by using the data-link layers address, say MAC address.
- **Host-to-host delivery**: At the network level, delivery of datagrams can take place between two hosts by using IP address.

From user's point of view, the TCP/IP-based internet can be considered as a set of application programs that use the internet to carry out useful communication tasks. Most popular internet applications include Electronic mail, File transfer, and Remote login. IP allows transfer of IP datagrams among a number of stations or hosts, where the datagram is routed through the internet based on the IP address of the destination. But, in this case, several application programs (processes) simultaneously running on a source host has to communicate with the corresponding processes running on a remote destination host through the internet. This requires an additional mechanism called *process-to-process delivery*, which is implemented with the help of a transport -level protocol. The transport level protocol will require an additional address, known as *port number*, to select a particular process among multiple processes running on the destination host. So, there is a requirement of the following third type of delivery system.

- **Process-to-process delivery**: At the transport level, communication can take place between processes or application programs by using port addresses

  Basic communication mechanism is shown in Fig. 6.3.1. The additional mechanism needed to facilitate multiple application programs in different stations to communicate with each other simultaneously can be provided by a transport level protocol such as UDP or TCP, which are discussed in this lesson.

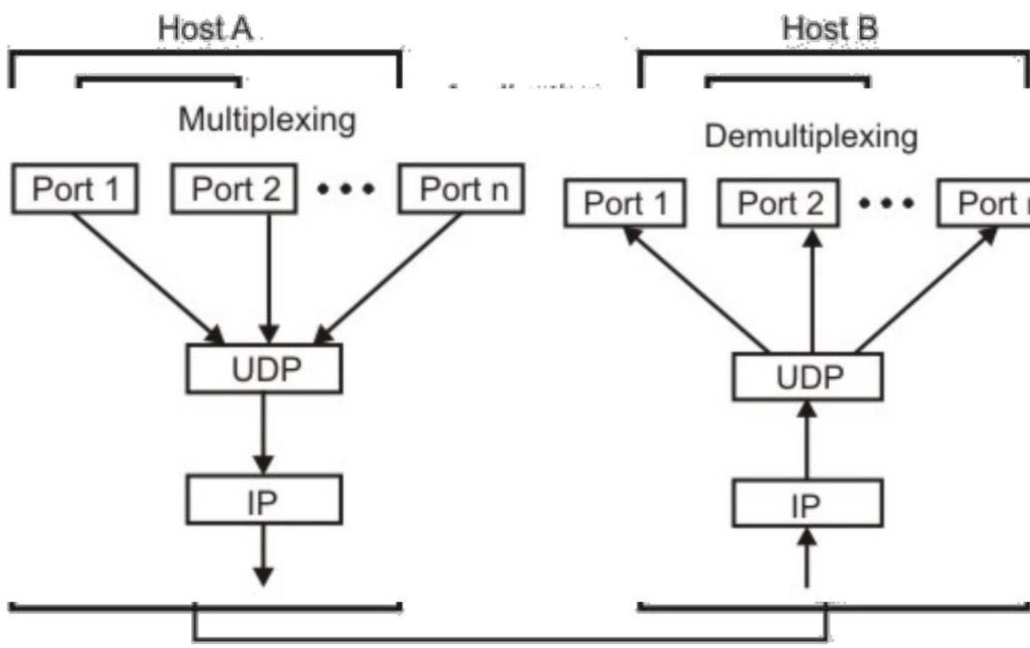


Fig 5.1 Communication mechanism through the internet

User Datagram protocol (UDP)

UDP is responsible for differentiating among multiple source and destination processes within one host. Multiplexing and demultiplexing operations are performed using the port mechanism as depicted in Fig

UDP Datagram

A brief description of different fields of the datagram are given below:

- Source port (16 bits): It defines the port number of the application program in the host of the sender

- Destination port (16 bits): It defines the port number of the application program in the host of the receiver
- Length: It provides a count of octets in the UDP datagram, minimum length = 8

- Checksum: It is optional, 0 in case it is not in use Characteristics of the UDP

- Key characteristics of UDP are given below:
- UDP provides an unreliable connectionless delivery service using IP to transport messages between two processes

- UDP messages can be lost, duplicated, delayed and can be delivered out of order

- UDP is a thin protocol, which does not add significantly to the functionality of IP

- It cannot provide reliable stream transport service

The above limitations can be overcome by using connection-oriented transport layer protocol known as *Transmission Control Protocol* (TCP), which is presented in the following section.

Transmission Control Protocol (TCP)

TCP provides a connection-oriented, full -duplex, reliable, streamed delivery service using IP to transport messages between two processes.

Reliability is ensured by:

- Connection-oriented service

- Flow control using sliding window protocol

- Error detection using checksum
- Error control using go-back-N ARQ technique
- Congestion avoidance algorithms; multiplicative decrease and slow-start

TCP Datagram

The TCP datagram format is shown in Figure. A brief explanation of the functions of different fields are given below:

- Source port (16 bits): It defines the port number of the application program in the host of the sender
- Destination port (16 bits): It defines the port number of the application program in the host of the receiver
- Sequence number (32 bits): It conveys the receiving host which octet in this sequence comprises the first byte in the segment
- Acknowledgement number (32 bits): This specifies the sequence number of the next octet that receiver expects to receive
- HLEN (4 bits): This field specifies the number of 32-bit words present in the TCP header
- Control flag bits (6 bits): URG: Urgent pointer
- ACK: Indicates whether acknowledge field is valid
- PSH: Push the data without buffering
- RST: Resent the connection
- SYN: Synchronize sequence numbers during connection establishment
- FIN: Terminate the connection
- Window (16 bits): Specifies the size of window
- Checksum (16 bits): Checksum used for error detection.

- User pointer (16 bits): Used only when URG flag is valid

- Options: Optional 40 bytes of information

The well-known ports used by TCP are given in Table 6.3.2 and the three types of addresses used in TCP/IP are shown in Fig. 6.3.5. TCP establishes a virtual path between the source and destination processes before any data communication by using two procedures, *connection establishment* to start reliably and *connection termination* to terminate gracefully, as discussed in the following subsection.

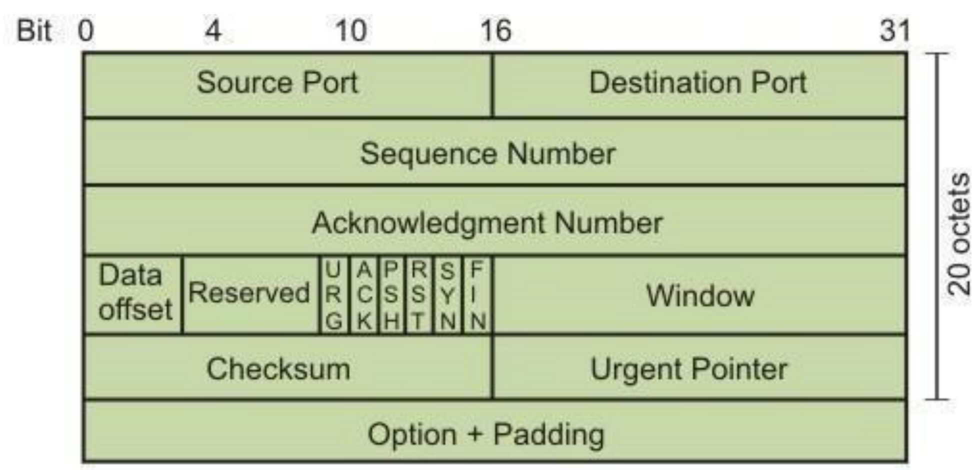


Fig 5.2 The TCP datagram format

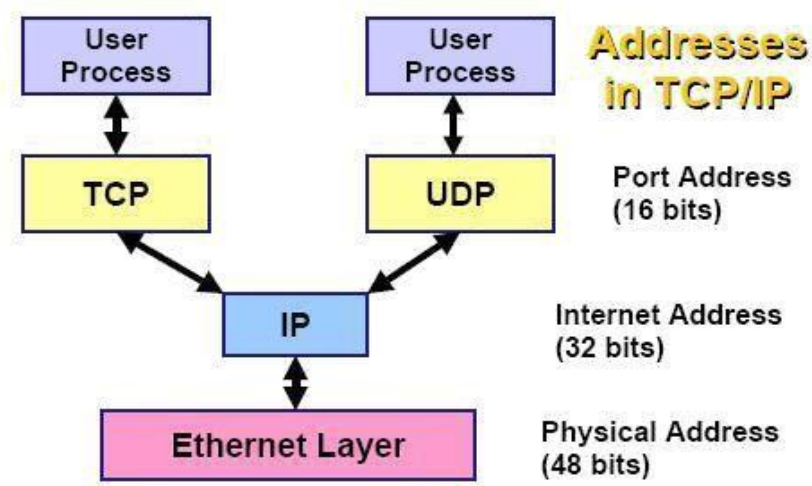


Fig 5.3 Three types of addresses used in TCP/IP

Table 5.1 Well-known ports used by TCP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connections)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	BOOTP Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Electronic Mail

Simple Mail Transfer Protocol (**SMTP**) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a Transmission Control Protocol (TCP) connection. An SMTP session consists of commands originated by an SMTP client (the initiating agent, sender, or transmitter) and corresponding responses from the SMTP server (the listening agent, or receiver) so that the session is opened, and session parameters are exchanged. A session may include zero or more SMTP transactions. An SMTP transaction consists of three command/reply sequences (see example below.) They are:

1. MAIL command, to establish the return address, a.k.a. Return-Path, 5321.From, m from, or envelope sender. This is the address for bounce messages.

2. RCPT command, to establish a recipient of this message. This command can be issued multipletimes, one for each recipient. These addresses are also part of the envelope.

3. DATA to send the message text. This is the content of the message, as opposed to its envelope.

4. It consists of a message header and a message body separated by an empty line. DATA is actually a group of commands, and the server replies twice: once to the DATA command proper, to acknowledge that it is ready to receive the text, and the second time after the end-of-data sequence, to either accept or reject the entire message.

Electronic mail is among the most widely available application services. Each user, who intends to participate in email communication, is assigned a mailbox, where out-going and incoming messages are buffered, allowing the transfer to take place in the background. The message contains a header that specifies the sender, recipients, and subject, followed by a body that contains message. The TCP/IP protocol that supports electronic mail on the internet is called *Simple Mail Transfer Protocol* (SMTP), which supports the following:

- Sending a message to one or more recipients
- Sending messages that include text, voice, video, or graphics

A software package, known as *User Agent*, is used to compose, read, reply or forward emails and handle mailboxes. The email address consists of two parts divided by a @ character. The first part is the local name that identifies mailbox and the second part is a domain name.

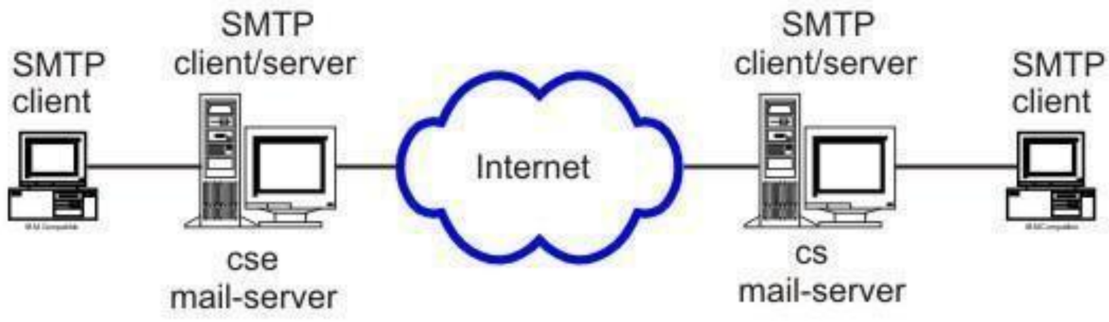


Fig 5.4 Simple Mail Transfer Protocol (SMTP)

TELNET

Telnet is a simple remote terminal protocol that provides a remote log-on capability, which enables a user to log on to a remote computer and behaves as if it is directly connected to it. The following three basic services are offered by TELNET:

- It defines a network virtual terminal that provides a standard interface to remote systems
- It includes a mechanism that allows the client and server to negotiate options from a standard set
- It treats both ends symmetrically

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a TCP/IP client -server application for transfer files between two remote machines through internet. A TCP connection is set up before file transfer and it persists throughout the session. It is possible to send more than one file before disconnecting the link. A control connection is established first with a remote host before any file can be transferred. Two connections required are shown in Fig. 6.3.15. Users view FTP as an interactive system

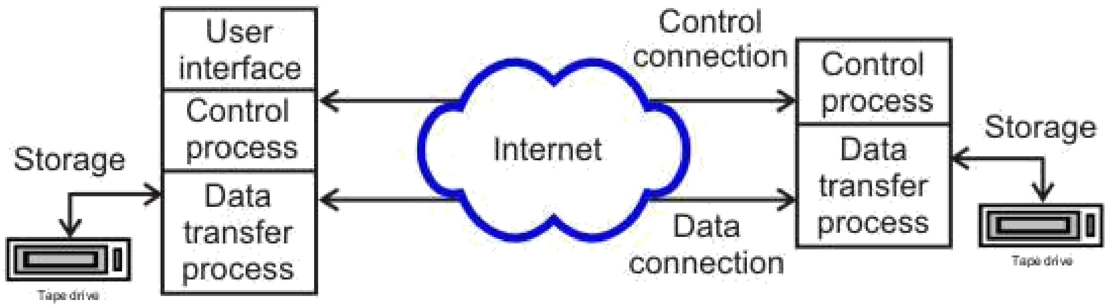


Fig 5.5 File Transfer Protocol (FTP)

Simple Network Management Protocol (SNMP)

Network managers use network management software that help them to locate, diagnose and rectify problems. Simple Network Management Protocol (SMTP) provides a systematic way for managing network resources. It uses transport layer protocol for communication. It allows them to monitor switches, routers and hosts. There are four components of the protocol:

- Management of systems
- Management of nodes; hosts, routers, switches
- Management of Information Base; specifies data items a host or a router must keep and the operations allowed on each (eight categories)
- Management of Protocol; specifies communication between network management client program a manager invokes and a network management server running on a host or router

HTTP (HyperText Transfer Protocol) The WEB

Internet (or The Web) is a massive distributed client/server information system as depicted in the following diagram.Many applications are running concurrently over the Web, such as web browsing/surfing, e-mail, file transfer, audio & video streaming, and so on. In order for proper communication to take place between the client and the server, these applications must agree on a specific application-level protocol such as HTTP, FTP, SMTP, POP, and etc.

HyperText Transfer Protocol (HTTP)

HTTP (Hypertext Transfer Protocol) is perhaps the most popular application protocol used in the Internet (or The WEB).

The WEB

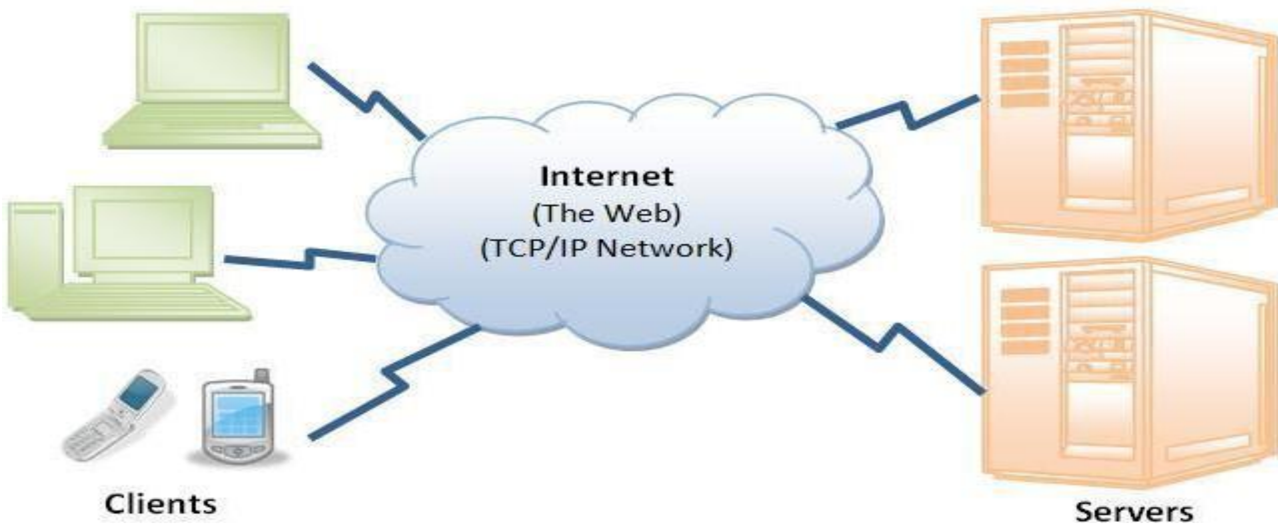


Fig 5.5 Layout of WEB

Internet (or The Web) is a massive distributed client/server information system as depicted in the following diagram.

Many applications are running concurrently over the Web, such as web browsing/surfing, e-mail, file transfer, audio & video streaming, and so on. In order for proper communication to take place between the client and the server, these applications must agree on a specific application-level protocol such as HTTP, FTP, SMTP, POP, and etc.

Hyper Text Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is communications protocol of the TCP/IP Suit. It is used for retrieving inter-linked text documents (hypertext). HTTP led to the establishment of the World Wide Web.HTTP's development was coordinated by the World Wide Web Consortium and the Internet Engineering Task Force (IETF), resulting in the publication of a series of Request for Comments (RFCs), most notably RFC 2616 (June 1999), which defines HTTP/1.1, the version of HTTP in common use.

HTTP is a request/response standard between a client and a server. The end-user client making a HTTP request—using a web browser typically—is referred to as the **user agent**. The responding server—which serves resources such as HTML files and images—is called the **origin server**.

Typically, an HTTP client initiates a request. It establishes a Transmission Control Protocol (TCP) connection to a particular port on a host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message. Upon receiving the request, the server sends back the requested resource. Resources to be accessed by HTTP are identified using Uniform Resource Identifiers (URIs) (or, more specifically, Uniform Resource Locators (URLs)) using the http: or https: URI schemes.

Here is how HTTP works:

- You type a website's URL, for example, www.ustudy.in in your favorite browser (IE, Firefox, Opera, Safari)

- Your web browser looks up the IP address of www.ustudy.in using DNS services - it is resolved as 202.54.158.131.

- Your web browser then establishes a TCP connection to the IP address 202.54.158.131 on port

The web browser's packets are transported to the Ustudy.in server over the internet using IP. The server for UStudy.in successfully receives the packet and acknowledges a connection. On seeing it is for port 80, delivers it to the web server software (apache, IIS etc.).

HTTP (Hypertext Transfer Protocol) is perhaps the most popular application protocol used in the Internet (or The WEB).

HTTP is an *asymmetric request-response client-server* protocol as illustrated. An HTTP client sends a request message to an HTTP server. The server, in turn, returns a response message. In other words, HTTP is a*pull protocol*, the client *pulls* information from the server (instead of server *pushes* information down to the client).

HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.

HTTP permits negotiating of data type and representation, so as to allow systems to be built independently of the data being transferred.

Quoting from the RFC2616: "The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers."

Browser

Whenever you issue a URL from your browser to get a web resource using HTTP, e.g. http://www.nowhere123.com/index.html, the browser turns the URL into a *request message* and sends it to the HTTP server. The HTTP server interprets the request message, and returns you an appropriate response message, which is either the resource you requested or an error message.

Uniform Resource Locator (URL)

A URL (Uniform Resource Locator) is used to uniquely identify a resource over the web. URL has

protocol://*hostname*:*port*/*path-and-file-name*

the following syntax:

There are 4 parts in a URL:

1. *Protocol*: The application-level protocol used by the client and server, e.g., HTTP, FTP, and telnet.
2. *Hostname*: The DNS domain name (e.g., www.nowhere123.com) or IP address (e.g., 192.128.1.2) of the server.
3. *Port*: The TCP port number that the server is listening for incoming requests from the clients.
4. *Path-and-file-name*: The name and location of the requested resource, under the server document base directory.

HTTP is an *asymmetric request-response client-server* protocol as illustrated. An HTTP client sends a request message to an HTTP server. The server, in turn, returns a response message. In other words, HTTP is a *pull protocol*, the client *pulls* information from the server (instead of server *pushes* information down to the client).

HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests. HTTP permits negotiating of data type and representation, so as to allow systems to be built independently of the data being transferred.

Quoting from the RFC2616: "The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers."

World Wide Web (WWW)

The **World Wide Web** (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

Each site holds one or more documents, referred to as *Web pages*. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers.

Client (Browser)

A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocol, and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described previously such as FTP or HTTP (described later in the chapter). The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

Server

The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk. A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.

TEXT / REFERENCE BOOKS

1. Andrew S Tanenbaum "Computer Networks" 5th Edition. Pearson Education/PH I/2011.
2. Behrouz A. Forouzan, "Data Communications and Networking" Fourth Edition, Mc GrawHill HIGHER Education 2007.
3. Michael A.Gallo, William Hancock.M, Brooks/Cole Computer Communications and Networking Technologies,2001
4. Richard Lai and Jirachief pattana, "Communication Protocol Specification and Verification", Kluwer Publishers, Boston, 1998.
5. Pallapa Venkataram and Sunilkumar S.Manvi, "Communication protocol Engineering", PHI Learning, 2008