# 15CS34T- COMPUTER NETWORK

**Note: This is only Basic Information for students. Please refer "Reference Books" prescribed as per syllabus**

# UNIT- 1: Introduction to Data Communication

### 1.1 Introduction

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").

The word **data** refers to information presented in whatever form is agreed upon by the parties creating and using the data.

**Data communications** are the exchange of data between two devices via some form of transmission medium such as a wire cable.

- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).
- The effectiveness of a data communications system depends on four fundamental characteristics:
    1. delivery,
    2. accuracy,
    3. timeliness, and
    4. 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 ackets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

## 1.2Components

A data communications system has five components (see Figure 1.1).

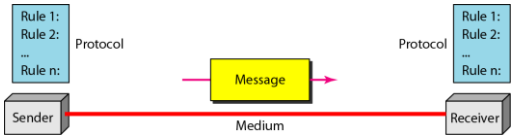



Figure 1.1 Five components of data communication

**Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

**Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

**Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

**Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver.

Examples: twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

**Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

## 1.3 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 (0s or 1s).
- 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**.
- 2 standards for representing **letters** and **numbers** are:
  - ASCII - **American Standard Code for Information Interchange**
    - 7 bit code
    - $8^{th}$ bit is unused
    - $2^7$=128 codes
  - **Unicode** – Extended version of ASCII
    - 16 bit code
    - $2^{16}$ = over 65 thousand codes
- 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.

**Numbers**

- Numbers are also represented by bit patterns.
- 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.
- Co lour is expressed in a computer as an RGB(red-green-blue)value, which is actually a three numbers (255,255,255)

**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. Therefore it is necessary to convert analog signals to digital form.
- In particular, samples of the sound will have to be taken and each sample will have to be quantized to the nearest binary code in the digital representation.

**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. Again we can change video to a digital or an analog signal.

## 1.4 Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1.2.

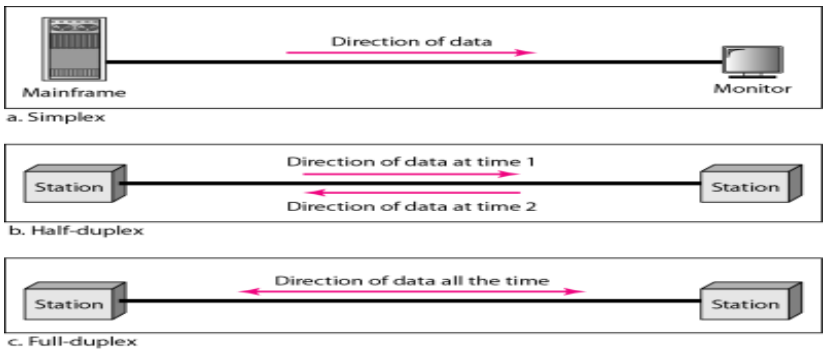



Figure 1.2 Data flow (simplex, half-duplex, andfull-duplex)

**Simplex**

- In simplex mode, the communication is unidirectional, as on a one-way street.
- Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a).
- The simplex mode can use the entire capacity of the channel to send data in one direction
- Ex: Keyboards and traditional monitors. The keyboard can only introduce input; the monitor can only accept output.

**Half-Duplex**

- In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see Figure 1.2b).
- The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

**Full-Duplex**

- In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c).
- The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time.
- In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction.
- Ex:Telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

- The full-duplex mode is used when communication in both directions is required all the time.

https://www.youtube.com/watch?v=Ii3d_QB5nYw

## 1.5 Categories of Networks

- The three primary categories of networks are:
    1. Local-area networks (LAN )
    2. Metropolitan Area Network (MAN)
    3. Wide-area networks (WAN)
- These categories depending on various factors like size of the network, the distance it covers and the type of link used in interconnection.

### 1.5.1 Local Area Network (LAN)

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus of up to few kilometers in size(see Figure 1.10).
- LANs are designed to allow resources to be shared between personal computers or workstations.
    - The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.
    - A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.
- Usually, LANs offers a bandwidth of 10 to 100 mpbs.
- In general, LAN will use only one type of transmission medium.
- The most common LAN topologies are bus, ring, and star.

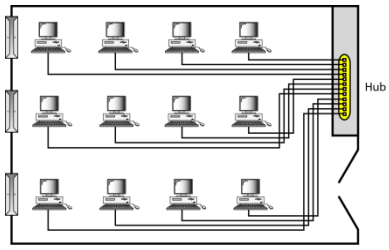



Figure 1.10 An isolated IAN connecting 12 computers to a hub in a closet

### 1.5.2 Metropolitan Area Networks (MAN)

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
- It normally covers the area inside a town or a city.
- It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.
- A good **example** of a MAN is the part of the **telephone company network** that can provide a high-speed DSL line to the customer.
- Another **example** is the cable **TV network** that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

### 1.5.3 Wide Area Network (WAN)

- A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.
- WANs are designed to serve an area of hundreds or thousands miles.
- A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN (Figure 1.11).
    - The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.
    - The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often used to provide Internet access.

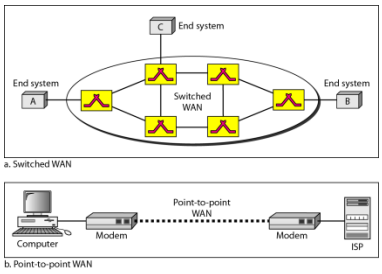



Figure 1.11 WANs: a switched WAN and a point-to-point WAN

https://www.youtube.com/watch?v=aQScX7B3ntY

## 1.6 Interconnection of Networks: Internetwork

- When two or more networks are connected, they become an internetwork, or internet.
- It may consist of several local, metropolitan or wide area networks interconnected via a LAN, MAN or WAN oriented communication technology.

- Individual networks are joined into internet works by using internetworking devices like bridges, routers and gateways.
- Common form of internet is a collection of LANs connected by a WAN.
- There exist 3 classes of internetworks for most of particle and analytical purposes:
  - The Global public internetwork: The Internet
  - The owned /private internetworks: Intranets
  - The hybrid internetwork :Extranets
- As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle and needs to have control over the company from her horne. To create a backbone WAN for connecting these three entities (two LANs and the president's computer), a switched WAN (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modern line offered by a cable TV provider as shown in Figure 1.12.

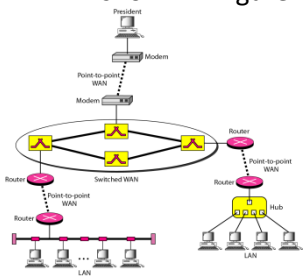



Figure 1.12 A heterogeneous network made of four WANs and two LANs

https://www.youtube.com/watch?v=i5oe63pOhLI

**THE INTERNET**

- The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.
- The Internet is a structured, organized system.
- The Internet has revolutionized many aspects of our daily lives.
- It has affected the way we do business as well as the way we spend our leisure time.
- Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or maybe you researched a medical topic, booked a hotel reservation, chatted with a fellow Trekkie, or comparison-shopped for a car.

**A Brief History**

- Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet.

- Millions of people are users. Internet this extraordinary communication system only came into being in 1969.

- In the mid-1960s, mainframe computers in research organizations were standalone devices.
- Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

- In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.
- The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.
- By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network.
- Software called the Network Control Protocol (NCP) provided communication between the hosts.

- In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Projec1.
- Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets.
- This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

- Shortly thereafter, authorities made a decision to split TCP into two protocols:
- Transmission Control Protocol (TCP) and Internetworking Protocol (IP).
- IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection.
- The internetworking protocol became known as TCPIIP.

**The Internet Today**

- The Internet has come a long way since the 1960s.
- The Internet today is not a simple hierarchical structure.
- It is made up of many wide-and local-area networks joined by connecting devices and switching stations.
- It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.
- Today most end users who want Internet connection use the services of Internet service providers (ISPs).
- There are

- international service providers,
- national service providers,
- regional service providers, and
- Local service providers.

- The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.

**International Internet Service Providers**

At the top of the hierarchy are the international service providers that connect nations together.

**National Internet Service Providers**

- The national Internet service providers are backbone networks created and maintained by specialized companies.
- To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs).
- A national ISP is a business that provides Internet access in cities and towns nation wide.

**Regional Internet Service Providers**

- Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs.
- They are at the third level of the hierarchy with a smaller data rate.
- A regional ISP usually provides Internet access to specific geographic area.

**Local Internet Service Providers**

- Local Internet service providers provide direct service to the end users.
- The local ISPs can be connected to regional ISPs or directly to national ISPs.

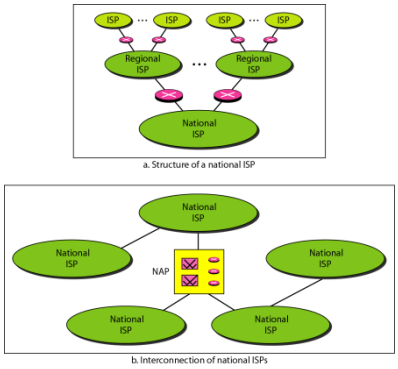



Figure 1.13 Hierarchical organization of the Internet

**PROTOCOLS**

**Protocols**

- **A protocol** is a set of rules that govern data communications.

- A protocol defines what is communicated, how it is communicated, and when it is communicated.
- The key elements of a protocol are
  - syntax,
  - semantics, and
  - timing.

**Syntax**

- The term syntax refers to the structure or format of the data, meaning the order in which they are presented.
- For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

**Semantics**

- The word semantics refers to the meaning of each section of bits.
- How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- For example, does an address identify the route to be taken or the final destination of the message?

**Timing**

- The term timing refers to two characteristics: when data should be sent and how fast they can be sent.
- For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

## 1.7 Data and Signals

One of the major functions of the physical layer is to move data in the form of **electromagnetic signals** across a transmission medium. Whether you are collecting numerical statistics from another computer, sending animated pictures from a design workstation, or causing a bell to ring at a distant control center, you are working with the transmission of data across network connections.

Generally, the data usable to a person or application are not in a form that can be transmitted over a network. For example, a photograph must first be changed to a form that transmission media can accept. Transmission media work by conducting energy along a physical path.

**To be transmitted, data must be transformed to electromagnetic signals.**

### 1.6.1 Analog and Digital Signals

Signals can be either analog or digital.

- **Analog signals** can have an infinite number of values in a range
- 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.

- **Digital signals** can have only a limited number of defined values.
- Although each value can be any number, it is often as simple as 1 and 0.

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 3.1 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, demonstrate the sudden jump that the signal makes from value to value.

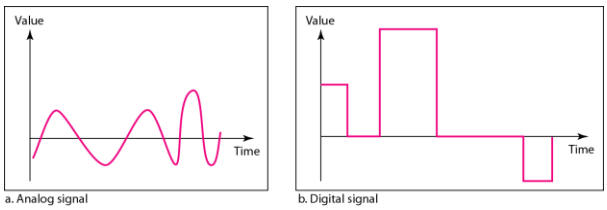



Figure 3.1 Comparison ofanalog and digital signals

### 1.7.2 Periodic and Nonperiodic Signals

- **A periodic signal** completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.
- **A nonperiodic signal** changes without exhibiting a pattern or cycle that repeats over time.

- Both analog and digital signals can be periodic or nonperiodic.
- In data communications, we commonly use periodic analog signals (because they need less bandwidth) and nonperiodic digital signals (because they can represent variation in data).

### 1.7.3 PERIODIC ANALOG 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.

### 1.7.4 Sine Wave

- The sine wave is the most fundamental form of a periodic analog signal.
- It is a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow.
- Figure 3.2 shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.
- A sine wave can be represented by three parameters: **the peak amplitude, the frequency, and the phase**.

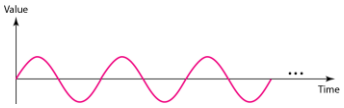



Figure 3.2 A sine wave

### 1.7.5 Peak Amplitude

- The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries.
- For electric signals, peak amplitude is normally measured in **volts**.
- Figure 3.3 shows two signals and their peak amplitudes.

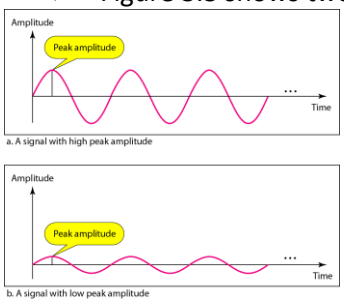



Figure 3.3 Two signals with the same phase and frequency, but different amplitudes

### 1.7.6 Period and Frequency

- **Period** refers to the amount of time, in seconds, a signal needs to complete 1 cycle.
- **Frequency** refers to the number of periods in 1s.
- Frequency and period are the inverse of each other. The following formulas show this.
- Figure 3.4 shows two signals and their frequencies

$$f = \frac{1}{T} \quad \text{and} \quad T = \frac{1}{f}$$

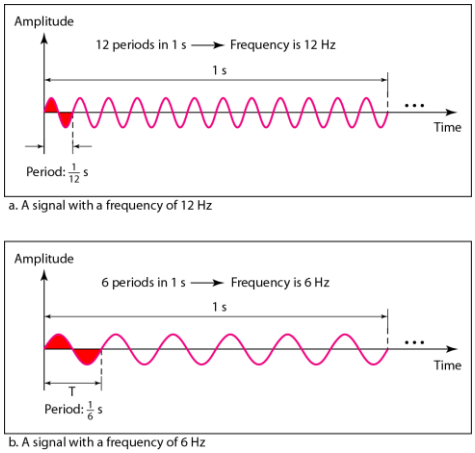



Figure 3.4 Two signals with the same amplitude and phase, but different frequencies

- Period is formally expressed in **seconds**.
- Frequency is formally expressed in **Hertz** (Hz), which is cycle per second.
- Units of period and frequency are shown in Table 3.1.

| *Unit* | *Equivalent* | *Unit* | *Equivalent* |
|---|---|---|---|
| Seconds (s) | 1 s | Hertz (Hz) | 1 Hz |
| Milliseconds (ms) | $10^{-3}$ s | Kilohertz (kHz) | $10^{3}$ Hz |
| Microseconds (µs) | $10^{-6}$ s | Megahertz (MHz) | $10^{6}$ Hz |
| Nanoseconds (ns) | $10^{-9}$ s | Gigahertz (GHz) | $10^{9}$ Hz |
| Picoseconds (ps) | $10^{-12}$ s | Terahertz (THz) | $10^{12}$ Hz |

Table 3.1 Units of period and frequency

**More about Frequency**

- Frequency is the rate of change with respect to time.
- Change in a short span of time means high frequency.
- Change over a long span of time means low frequency.

Two Extremes

- If a signal does not change at all, its frequency is zero. - If signal does not change at all, it never completes a cycle, so its frequency is a 0 Hz.
- If a signal changes instantaneously, its frequency is infinite. - In other words, when a signal changes instantaneously, its period is zero; since frequency is the inverse of period, in this case, the frequency is 1/0, or infinite

**1.7.7 Phase**

- The term phase describes the position of the waveform relative to time 0.
- If we think of the wave as something that can be shifted backward or forward along the time axis**, phase describes the amount of that shift. It indicates the status of the first cycle.**
- Phase is measured in **degrees or radians**.
    - A phase shift of 360° corresponds to a shift of a complete period; a phase shift of 180° corresponds to a shift of one-half of a period; and a phase shift of 90° corresponds to a shift of one-quarter of a period (see Figure 3.5).

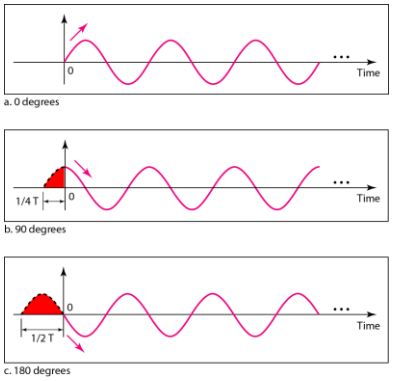



Figure 3.5 Three sine waves with the same amplitude and frequency, but different phases

Looking at Figure 3.5, we can say that

1. A sine wave with a phase of 0° starts at time 0 with a zero amplitude. The amplitude is increasing.

2. A sine wave with a phase of 90° starts at time 0 with a peak amplitude. The amplitude is decreasing.

3. A sine wave with a phase of 180° starts at time 0 with a zero amplitude. The amplitude is decreasing.

Another way to look at the phase is in terms of shift or offset. We can say that

1. A sine wave with a phase of 0° is not shifted.

2. A sine wave with a phase of 90° is shifted to the left by 1/4 cycle. However, note that the signal does not really exist before time 0.

3. A sine wave with a phase of 180° is shifted to the left by ½ cycle. However, note that the signal does not really exist before time 0.

### 1.7.8 Wavelength

- The wavelength is the distance a simple signal can travel in one period.
- Wavelength is another characteristic of a signal traveling through a transmission medium.
- Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium (see Figure 3.6).
- The wavelength depends on both the frequency and the medium.
- Wavelength is a property of any type of signal.

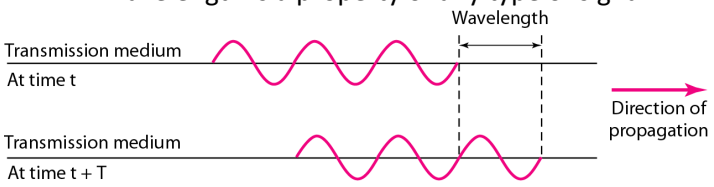



Figure 3.6 Wavelength and period

In data communications, we often use **wavelength to describe the transmission of light in an optical fiber**. Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. However, since period and frequency are related to each other, if we represent wavelength by y, propagation speed by c (speed of light), and frequency by f, we get

**Wavelength =propagation speed x period**

**= propagation speed/frequency**

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal. For example, in a vacuum, light is propagated with a speed of 3 x $10^8$ mls. That speed is lower in air and even lower in cable.

The wavelength is normally measured **in micrometers (microns) instead of meters.**

### 1.7.9 Composite Signals

- A composite signal is made of many simple sine waves.
- In data communications; we need to send a composite signal.
- A composite signal can be periodic or nonperiodic.
- **A periodic composite signal** can be decomposed into a series of simple sine waves with discrete frequencies -frequencies that have integer values (1, 2, 3, and so on).

- **A nonperiodic composite signal** can be decomposed into a combination of an infinite number of simple sine waves with continuous frequencies, frequencies that have real values.
- Figure 3.9 shows a periodic composite signal with frequency f.

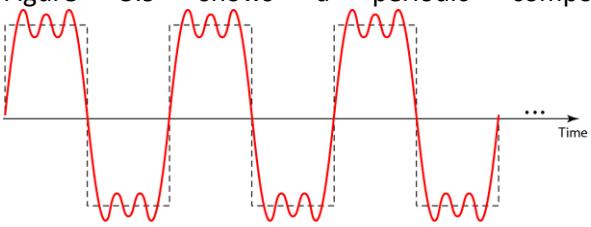



Figure 3.9 A composite periodic signal

- It is very difficult to manually decompose this signal into a series of simple sine waves.
- However, there are tools, both hardware and software, that can help us do the job.
- Figure 3.10 shows the result of decomposing the above signal in both the time and frequency domains.
- The amplitude of the sine wave with frequency f is almost the same as the peak amplitude of the composite signal.
- The amplitude of the sine wave with frequency 3f is one-third of that of the first, and the amplitude of the sine wave with frequency 9f is one-ninth of the first.
- The frequency of the sine wave with frequency f is the same as the frequency of the composite signal; it is called the fundamental frequency, or first harmonic.
- The sine wave with frequency 3f has a frequency of 3 times the fundamental frequency; it is called the third harmonic.
- The third sine wave with frequency 9f has a frequency of 9 times the fundamental frequency; it is called the ninth harmonic.
- Note that the frequency decomposition of the signal is discrete; it has frequencies f, 3f, and 9f.
- Because f is an integral number, 3f and 9f are also integral numbers. There are no frequencies such as 1.2for 2.6f .
- The frequency domain of a periodic composite signal is always made of discrete spikes.

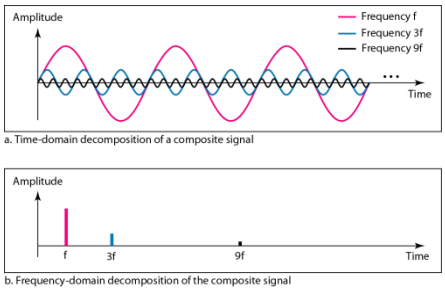



Figure 3.10 Decomposition of a composite periodic signal in the time and frequency domains

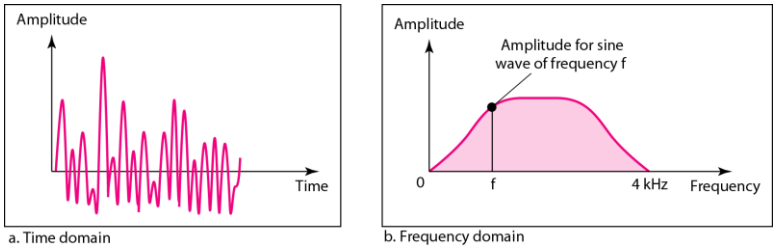



Figure 3.11 The time and frequency domains of a nonperiodic signal

- Figure 3.11 shows a nonperiodic composite signal.
- It can be the signal created by a microphone or a telephone set when a word or two is pronounced.
- In this case, the composite signal cannot be periodic, because that implies that we are repeating the same word or words with exactly the same tone.

## 1.7.10 Bandwidth

- **The range of frequencies contained in a composite signal is its bandwidth.**
- **The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal**.
- For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 -1000, or 4000.
- Figure 3.12 shows the concept of bandwidth.
- The figure depicts two composite signals, one periodic and the other nonperiodic.
- The bandwidth of the periodic signal contains all integer frequencies between 1000and5000(1000, 100I, 1002, ...).
- The bandwidth of the nonperiodic signals has the same range, but the frequencies are continuous.

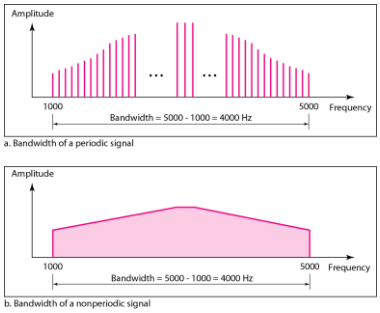



Figure 3.12 The bandwidth of periodic and nonperiodic composite signals

## 1.8 DIGITAL SIGNALS

- 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.
- Figure 3.16 shows two signals, one with two levels and the other with four.
- We send 1 bit per level in part a of the figure and 2 bits per level in part b of the figure. In general, if a signal has L levels, each level needs log2L bits.

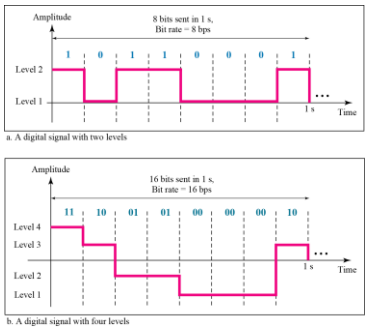



Figure 3.16 Two digital signals: one with two signal levels and the other with four signal levels

### 1.8.1 Bit Rate

- bit rate (instead of fjrequency)-is used to describe digital signals.
- **The bit rate is the number of bits sent in 1s, expressed in bits per second (bps).**
- Figure 3.16 shows the bit rate for two signals.

### 1.8.2 Bit Length

- The bit length is the distance one bit occupies on the transmission medium.

**Bit length = propagation speed x bit duration**

### 1.8.3 PERFORMANCE

One important issue in networking is the performance of the network-how good is it?

The parameter used to measures the performance are

1. Bandwidth
2. Throughput
3. Latency
4. Bandwidth delay product

5. Jitter

### 1.8.3.1 Bandwidth

The term can be used in two different contexts with two different measuring values:

bandwidth in hertz and

bandwidth in bits per second.

**Bandwidth in Hertz**

- Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass.
- For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

**Bandwidth in Bits per Seconds**

- The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit.
- For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

**Relationship**

There is an explicit relationship between the bandwidth in hertz and bandwidth in bits per seconds. Basically, an increase in bandwidth in hertz means an increase in bandwidth in bits per second.

The relationship depends on whether we have baseband transmission or transmission with modulation.

### 1.8.3.2 Throughput

**The throughput is a measure of how fast we can actually send data through a network.**

- The bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

- For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

### 1.8.3.3 Latency (Delay)

- The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.
- latency is made of four components:
    1. propagation time,
    2. transmission time,
    3. queuing time and
    4. processing delay.

**Latency=propagation time + transmission time + queuing time + processing delay**

### 1.8.3.4 Propagation Time

- Propagation time measures the time required for a bit to travel from the source to the destination.
- The propagation time is calculated by dividing the distance by the propagation speed.

**Propagation time = Distance/Propagation speed**

### 1.8.3.5 Transmission Time

- In data communications we don't send just 1 bit, we send a message. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time. However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later.
- The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

**Transmission time =Message size /Bandwidth**

### 1.8.3.6 Queuing Time

- The queuing time, the time needed for each intermediate or end device to hold the message before it can be processed.
- The queuing time is not a fixed factor; it changes with the load imposed on the network.
- When there is heavy traffic on the network, the queuing time increases.

- An intermediate device, such as a router, queues the arrived messages and processes them one by one. If there are many messages, each message will have to wait.

**Bandwidth-Delay Product**

- Bandwidth and delay are two performance metrics of a link.
- What is very important in data communications is the product of the two, the bandwidth-delay product. We elaborate on this issue, using two hypothetical cases as examples.

**Case 1:** Figure 3.31 shows case 1.

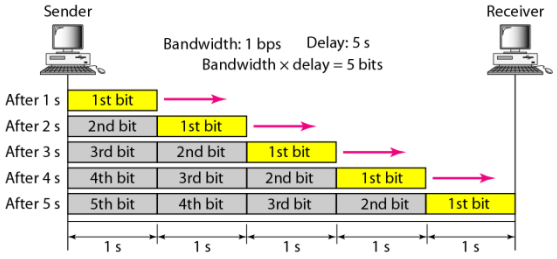



Figure 3.31 Filling the link with bits for case 1

- Let US assume that we have a link with a bandwidth of 1 bps (unrealistic, but good for demonstration purposes).
- We also assume that the delay of the link is 5 s (also unrealistic).
- We want to see what the bandwidth-delay product means in this case. Looking at figure, we can say that this product 1 x 5 is the maximum number of bits that can fill the link.
- There can be no more than 5 bits at any time on the link.

**Case 2:** Now assume we have a bandwidth of 4 bps.

Figure 3.32 shows that there can be maximum 4 x 5 =20 bits on the line.

The reason is that, at each second, there are 4 bits on the line; the duration of each bit is 0.25 s.

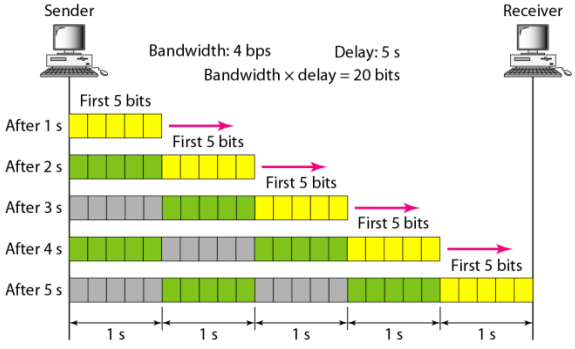


Figure 3.32 Filling the link with bits in case 2

- **The above two cases show that the product of bandwidth and delay is the number of bits that can fill the link.**
- **This measurement is important if we need to send data in bursts and wait for the acknowledgment of each burst before sending the next one.**

### 1.8.3.7 Jitter

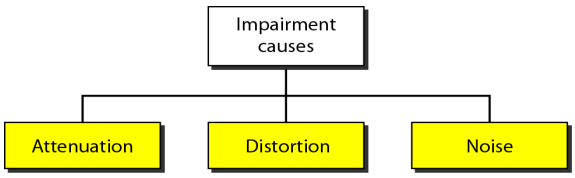
- **Jitter** is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example).
- If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

## 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

1. attenuation,
2. distortion, and
3. noise




### 1.9.1 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. That is why a wire carrying **electric signals** gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, **amplifiers** are used to amplify the signal. Figure 3.26 shows the effect of attenuation and amplification.

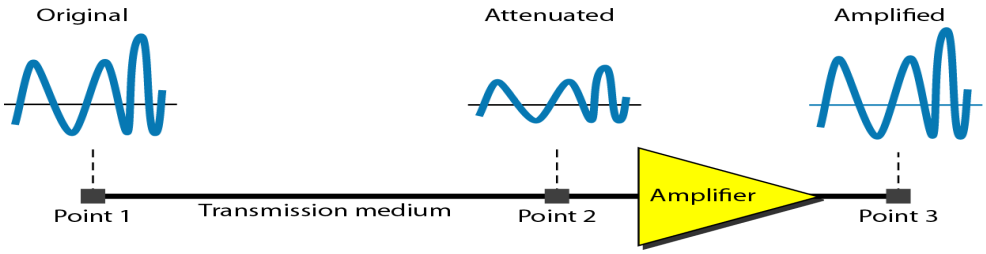



Figure 3.26 Attenuation

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. Note that some engineering books define the decibel in terms of voltage instead of power. In this case, because power is proportional to the square of the voltage, the formula is dB = 20 log 10 (V2IV1). In this text, we express dB in terms of power.

### 1.9.2 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. Figure 3.28 shows the effect of distortion on a composite signal.

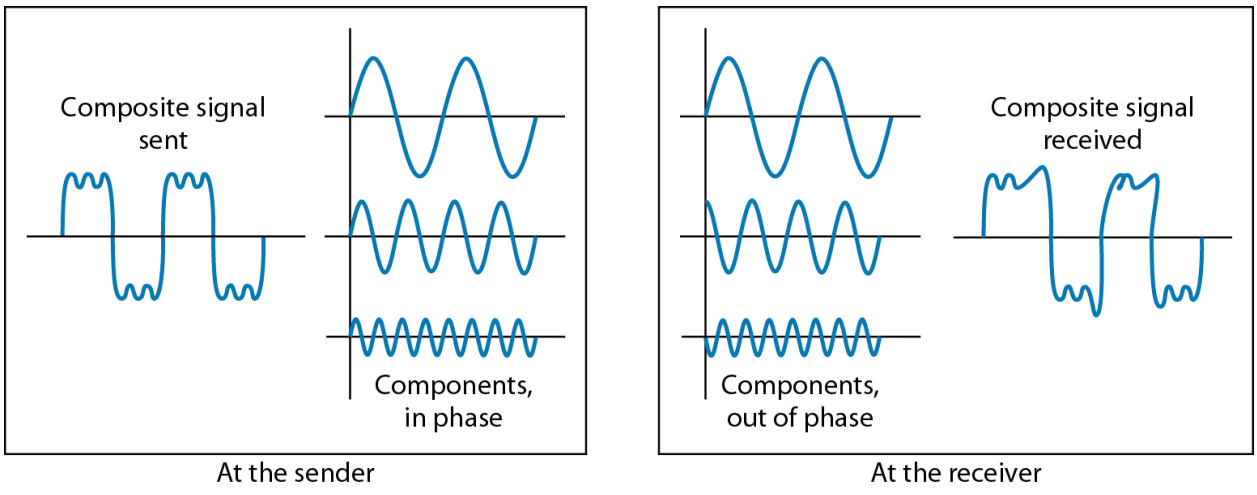



Figure 3.28Distortion

### 1.9.3 Noise

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

**Thermal noise** is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.

**Induced noise** comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

**Crosstalk** is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.

**Impulse noise** is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on

. Figure 3.29 shows the effect of noise on a signal.

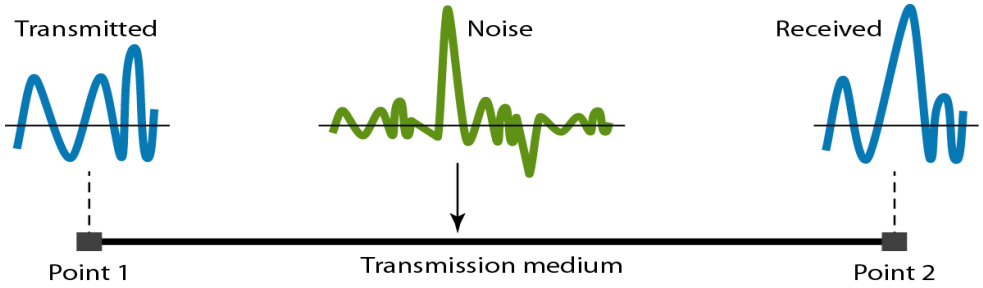



Figure 3.29 Noise

## 1.10 TRANSMISSION MODES

The transmission of binary data across a link can be accomplished in either parallel or serial mode.

In **parallel mode**, multiple bits are sent with each clock tick.

In **serial mode**, 1 bit is sent with each clock tick. While there is only one way to send parallel data, there are **three** subclasses of serial transmission:

1. asynchronous,
2. synchronous, and
3. isochronous

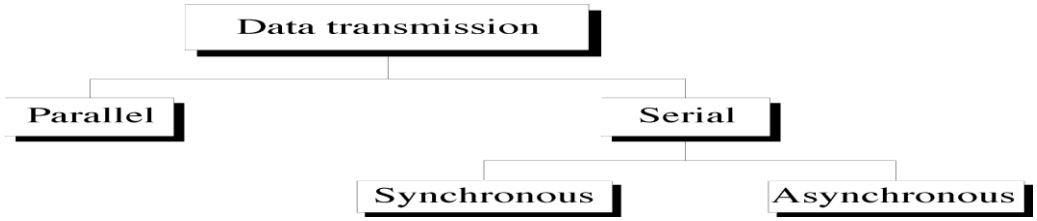



Figure 4.31 Data transmission and modes

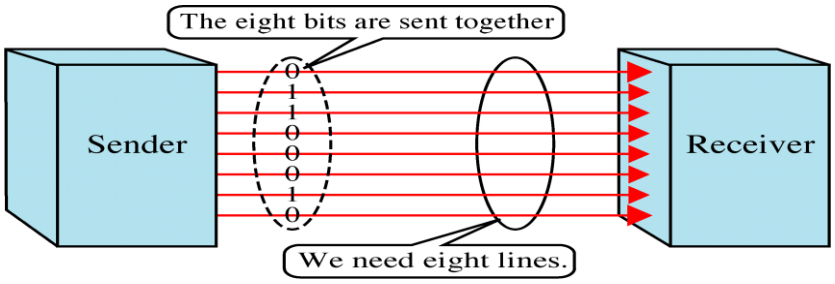
### 1.10.1 Parallel Transmission

Binary data, consisting of 1s and 0s, may be organized into groups of n bits each. Computers produce and consume data in groups of bits much as we conceive of and use spoken language in the form of words rather than letters. By grouping, we can send data n bits at a time instead of 1. This is called parallel transmission.

The mechanism for parallel transmission is a conceptually simple one: Use n wires to send n bits at one time. That way each bit has its own wire, and all n bits of one group can be transmitted with each clock tick from one device to another. Figure 4.32 shows how parallel transmission works for n = 8. Typically, the eight wires are bundled in a cable with a connector at each end.

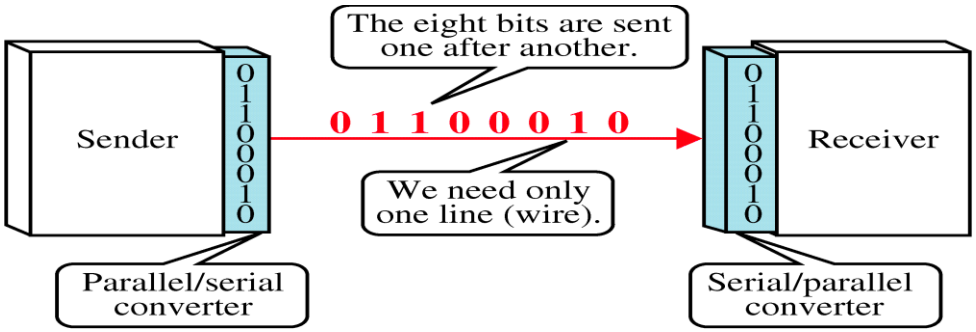
The **advantage** of parallel transmission is **speed**. All else being equal, parallel transmission can increase the transfer speed by a factor of n over serial transmission. We need eight lines

But there is a significant **disadvantage**: **cost**. Parallel transmission requires n communication lines (wires in the example) just to transmit the data stream. Because this is expensive, parallel transmission is usually limited to short distances.




### 1.10.2 Serial Transmission

In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices (see Figure 4.33).




**Note: This is only Basic Information for students. Please refer "Reference Books" prescribed as per syllabus**

Figure 4.33 Serial transmission

The **advantage** of serial over parallel transmission is that with only one communication channel, serial transmission **reduces the cost** of transmission over parallel by roughly a factor of n.

Since communication within devices is parallel, **conversion devices** are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-to-parallel).

Serial transmission occurs in one of **three** ways:

1. asynchronous,
2. synchronous, and
3. isochronous.

https://www.youtube.com/watch?v=PJ_bS7meE7s

**1.10.2.1Asynchronous Transmission**

Asynchronous transmission is so named because **the timing of a signal is unimportant**. Instead, information is received and translated by **agreed upon patterns**. As long as those patterns are followed, the receiving device can retrieve the information without regard to the rhythm in which it is sent. Patterns are based on grouping the bit stream into bytes. **Each group, usually 8 bits, is sent along the link as a unit.** The sending system handles each group independently, relaying it to the link whenever ready, without regard to a timer.

To alert the receiver to the arrival of a new group, therefore, an extra bit is added to the beginning of each byte. This bit, usually a 0, is called the **start bit**. To let the receiver know that the byte is finished, 1 or more additional bits are appended to the end of the byte. These bits, usually Is, are called **stop bits**. By this method, each byte is increased in size to at least 10 bits, of which 8 bits is information and 2 bits or more are signals to the receiver. In addition, the transmission of each byte may then be followed by a gap of varying duration. This **gap can be represented either by an idle channel or by a stream of additional stop bits**.

**In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (Is) at the end ofeach byte. There may be a gap between each byte.**

The start and stop bits and the gap alert the receiver to the beginning and end of each byte and allow it to synchronize with the data stream. This mechanism is called asynchronous because, at the byte level, the sender and receiver do not have to be synchronized..

Figure 4.34 is a schematic illustration of asynchronous transmission. In this example, the start bits are as, the stop bits are 1s, and the gap is represented by an idle line rather than by additional stop bits.

The addition of stop and start bits and the insertion of gaps into the bit stream make asynchronous transmission **slower** than forms of transmission that can operate without the addition of control information. But it is **cheap and effective**, two **advantages** that make it an attractive choice for situations such as low-speed communication. For **example**, the connection of a **keyboard to a computer** is a natural application for asynchronous transmission. A user types only one character at a time, types extremely slowly in data processing terms, and leaves unpredictable gaps of time between each character.

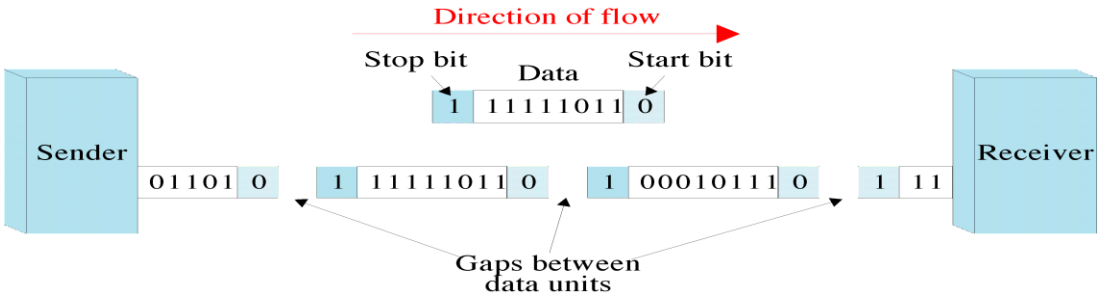



Figure 4.34 Asynchronous transmission

**1.10.2.2 Synchronous Transmission**

In synchronous transmission, the bit stream is combined into longer "**frames,**" which may **contain multiple bytes**. Each byte, however, is introduced onto the transmission link without a gap between it and the next one. It is left to the receiver to separate the bit stream into bytes for decoding purposes. In other words, data are transmitted as an unbroken string of 1s and 0s, and the receiver separates that string into the bytes, or characters, it needs to reconstruct the information.

**In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits**.

Figure 4.35 gives a schematic illustration of synchronous transmission. We have drawn in the divisions between bytes. In reality, those divisions do not exist; the sender puts its data onto the line as one long string. If the sender wishes to send data in separate bursts, the gaps between bursts must be filled with a special sequence of Os and Is that means idle. The receiver counts the bits as they arrive and groups them in 8-bit units.

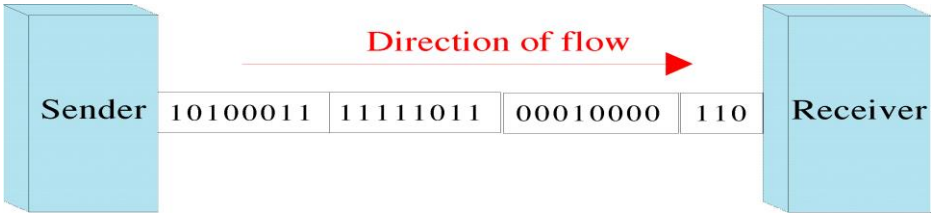



Figure 4.35 Synchronous transmission

Without gaps and start and stop bits, there is no built-in mechanism to help the receiving device adjust its bit synchronization midstream. **Timing** becomes very important, therefore, because the accuracy of the received information is completely dependent on the ability of the receiving device to keep an accurate count of the bits as they come in.

The **advantage** of synchronous transmission is **speed**. With no extra bits or gaps to introduce at the sending end and remove at the receiving end, and, by extension, with fewer bits to move across the link, synchronous transmission is **faster than asynchronous transmission**. For this reason, it is more **useful for high-speed applications** such as the **transmission of data from one computer to another.** Byte synchronization is accomplished in the data link layer.

**1.10.2.3 Asynchronous**

In real-time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails. For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If each image is sent by using one or more frames, there should be no delays between frames. For this type of application, synchronization between characters is not enough; the **entire stream of bits must be synchronized**. The **asynchronous transmission guarantees that the data arrive at a fixed rate**.

https://video.search.yahoo.com/search/video?fr=tightropetb&p=synchronous+and+asynchronous+data+transmission+videos#id=1&vid=0c6b812c33eb7d3c0ccd6b1149d9b1fb&action=click

## Questions:

1. Define Data Communication?

2. Explain data communication Components with a diagram?

3. Define a Protocol?

4. Explain how text, audio, video, and images data are represented?

5. Explain different modes of data transmission?

6. Define a Network?

7. Explain LAN, WAN and MAN?

8. Define a internet?

9. Write a note of internet Today?

10. Differentiate LAN and WAN?

11. Differentiate Analog signal and Digital signal?

12 Differentiate periodic and non periodic signals?

13. Explain the characteristics of sign wave signal?

14. Explain characteristics of digital signal?

15. Define bit rate and bit length?

16. Write a note on transmission impairments?

17. Define the following terms?

a. Data communication.
b. Phase.
c. Wavelength.
d. Bandwidth.
e. Throughput.

18. Explain the different categories of networks
19. Mention and explain the fundamental characteristics of data communication system
20. Illustrate different types of data flow.
21. Define data transmission mode. Give the classification of transmission modes
22. Differentiate serial and parallel transmission
23. Define the following terms?

a. Periodic signal.
b. Non-periodic signal.
c. Latency.
d. Jitter.
e. Bit rate

24. Differentiate synchronous and asynchronous transmission

## Activities

1.Both station can transmit and receive data simultaneously in

A. simplex mode.
B. Half duplex mode.
C. Full duplex mode.
D. None of Above.

Ans is C

2.Data communications are transfer of data through some

A. transmission medium.
B. linear medium.
C. Network LAN.
D. Protocols.

Ans is A

3.Keyboard and traditional monitors are examples of

A. Simplex devices.
B. Duplex devices.
C. Half Duplex devices.
D. Full Duplex devices.

Ans is A

4.One big disadvantage of a star topology is, if one hub goes down whole system is

A. Effects one Hub.
B. Remains unharm.
C. Dead.
D. Don't know.

Ans is C

5.Protocols are, set of rules to govern

A. Communication.
B. Maintain standards.
C. Metropolitan communication.
D. None of Above.

Ans is A

6.Parameter that refers to uneven delay of data packets in delivery is

A. Jitter.
B. Timelessness.
C. Accuracy.
D. Delivery.

Ans is C

7. Mode in which each station can send and receive data but not at same time is called

A. Half Duplex.
B. Simplex.
C. Full Duplex.
D. Duplex.

Ans is A

8.In mesh topology, every device has a dedicated topology of

A. Multipoint linking.
B. Point to point linking.
C. None of Above.
D. Both a and b.

Ans is A

9.Performance, reliability, and security are criteria of

A. Efficient network.
B. intranet.
C. protocols.
D. None of Above.

Ans is A

10.Effectiveness of a data communications system depends on four fundamental characteristics

A. delivery, accuracy.
B. timeliness and jitter.
C. jitter and delivery.

D. both a and b.

Ans is D

11.An internet is a

A. Collection of WANS.
B. Network of networks.
C. collection of LANS.
D. Collection of identical LANS and WANS.

Ans is B

12. Mode that is like a two way street with traffic flowing in both direction simultaneously is

A. Simplex.
B. Full Duplex.
C. Half Duplex.
D. None of above.

Ans is B

# UNIT- 2: Introduction to Networking and Topologies

## 2.1 Overview of Networking

**A computer network is** an interconnection of various computers to share software, hardware, resources and data through a communication medium between them.

A Computer Networking is a set of autonomous computers that permits distributed processing of the information and data and increased Communication of resources.

Any Computer Networking communication need a sender, a receiver and a communication medium to transfer signal or Data from sender to the receiver. We need sender, receiver, communication channel, protocols and operating system to establish a computer networking.

A network is a group of two or more computers that intelligently share hardware or software devices with each other. A network can be as small and simple as two computers that share a printer or as complex as the world's largest network: the Internet. A shared printer, on the other hand, can be controlled remotely and can store print jobs from different computers on the print server's hard disk. Users can change the sequence of print jobs, hold them, or cancel them. And, sharing of the device can be controlled through passwords, further differentiating it from a switchbox.

You can share or access many different types of devices over a network, but the most common devices include the following : Printers , Storage drives ,Modems, Cameras, Media players/recorders ,Game consoles

In addition to reducing hardware costs by sharing expensive printers and other peripherals among multiple users, networks provide additional benefits to users:

- A single Internet connection can be shared among multiple computers.
- Electronic mail (email) can be sent and received.
- Multiple users can share access to software and data files.
- Files and folders can be backed up to local or remote shares.
- Audio and video content can be streamed to multiple devices.
- Multiple users can contribute to a single document using collaboration features

## 2.2 Need for Networking

Networks are used for a simplified but worthwhile description of the uses of computer networks might be as follows:

• Sharing of hardware: For example, several PCs might be networked together in a wired or wireless local area network (LAN) to share a printer

. • Sharing of information: Distributed databases, e-mail, the World Wide Web and so on are examples of this. Here the sharing involves both LANs and wide area networks (WANs), especially the latter.

Some of features of networking can help our business

- Speed: Networks provides a very rapid method for sharing and transferring files.
- File sharing: a network makes it easy for everyone to access the same file and prevents people from accidentally creating different versions.
- Printer sharing: with a network several computers can share the same printer.
- Communication and collaboration: a network allows employees to share files, view other peoples work and exchange ideas more efficiently. you can use email and instant messaging tools to communicate quickly and store messages for future use.
- Remote Access: users are able to access the same files, data and messages even they are not in the office.
- Data Backup: a network makes it easier to back up all of your company's data on an offsite server, a set of tapes, CDs or other backup systems.
- Data security: only the authorized and unauthorized users can access data.
- Cost: sharing on a network allows for easier upgrading of the programs when compared to buying individually licensed copies

## 2.3 Hardware and Software components

### 2.3.1 Hardware Componets

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers.

**Network interface cards**

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses.

Each network interface card has its unique id. This is written on a chip which is mounted on the card.

**Repeaters**

A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation.

Bridges

A network bridge connects multiple network segments at the data link layer of the OSI model. Bridges broadcast to all ports except the port on which the broadcast was received. However, bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address to that port only.

Bridges come in three basic types:

- Local bridges: Directly connect local area networks (LANs)
- Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
- Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

**Switches**

A network switch is a device that forwards and filters OSI layer 2 datagrams (chunks of data communication) between ports (connected cables) based on the MAC addresses in the packets. A switch is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches. Some switches are capable of routing based on Layer 3 addressing or additional logical levels; these are called multi-layer switches. The term switch is used loosely in marketing to encompass devices including routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier).

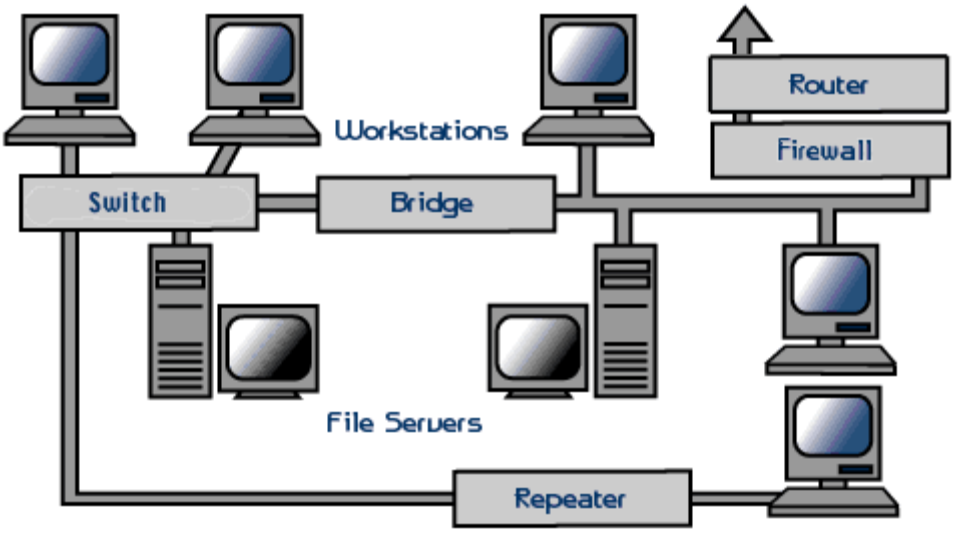
**Routers**

A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).

**Firewalls**

Firewalls are the most important aspect of a network with respect to security. A firewalled system does not need every interaction or data transfer monitored by a human, as automated processes can be set up to assist in rejecting access requests from unsafe sources, and

allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in 'cyber' attacks for the purpose of stealing/corrupting data, planting viruses, etc.




### 2.3.2 Software components

Software components of a Network

- Protocols:_**A protocol** is a set of rules that govern data communications over the network.Network protocols are TCP/IP,Novell IPX
- Device Drivers:a device driver is a program that controls the functionality of the hardware devices. Ex:NIC driver controls the functionality of the NIC,which act as the interface through which a computer connects to the network.
- Network operating Systems for Servers. Ex:Novel Netware6.5Microsoft windows NT,Windows 2000 Server etc.
- Network operating Systems for clients(PCs/workstations).Ex:NovellNetware 6.5 client,Microsoft windows XP, Windows 2000 Server.
- Application softwares : Ex:Internet Web browsers and E-mail clients.

## 2.4 Network Communication Standards

## PROTOCOLS AND STANDARDS

**Protocols**

- **A protocol** is a set of rules that govern data communications.
- A protocol defines what is communicated, how it is communicated, and when it is communicated.
- The key elements of a protocol are
  - syntax,
  - semantics, and
  - timing.

**Syntax**

- The term syntax refers to the structure or format of the data, meaning the order in which they are presented.
- For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

**Semantics**

- The word semantics refers to the meaning of each section of bits.
- How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- For example, does an address identify the route to be taken or the final destination of the message?

**Timing**

- The term timing refers to two characteristics: when data should be sent and how fast they can be sent.
- For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

**Standards**

- **Standards** provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- Data communication standards fall into two categories:

  de facto (meaning "by fact" or "by convention") and

  de jure (meaning "by law" or "by regulation").

**De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

**De jure.** Those standards that have been legislated by an officially recognized body are de jure standards.

**Standards Organizations**

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

**Standards Creation Committees**

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

1. **International Organization for Standardization (ISO).** The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
2. **International Telecommunication Union-Telecommunication Standards Sector (ITU-T).** This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular.
3. **American National Standards Institute (ANSI).** Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government
4. **Institute of Electrical and Electronics Engineers (IEEE).** It aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.
5. **Electronic Industries Association (EIA).** Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns.

**Forums**

- **Forums are special-interest groups that quickly evaluate and standardize new technologies.**
- Forums are special-interest groups made up of representatives from interested corporations.
- The forums work with universities and users to test, evaluate, and standardize new technologies which are to be used in the telecommunications community.

**Regulatory Agencies**

- All communications technology is subject to regulation by government agencies such as the Federal Communications Commission (FCC) in the United States.

- The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications.
- The FCC has authority over interstate and international commerce as it relates to communications.

**Internet Standards**

- **An Internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet.**
- It is a formalized regulation that must be followed.
- There is a strict procedure by which a specification attains Internet standard status.
- A specification begins as an Internet draft.
- An Internet draft is a working document (a work in progress) with no official status and a 6-month lifetime.
- Upon recommendation from the Internet authorities, a draft may be published as a Request for Comment (RFC).
- Each RFC is edited, assigned a number, and made available to all interested parties.
- RFCs go through maturity levels and are categorized according to their requirement level.

## 2.5 THE OSI MODEL

- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model.
- It was first introduced in the late 1970s.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- OSI model allows computers from different manufacturers to communicate with each other without requiring any logic changes to the hardware and software.
- The OSI model is a layered framework.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2.2).

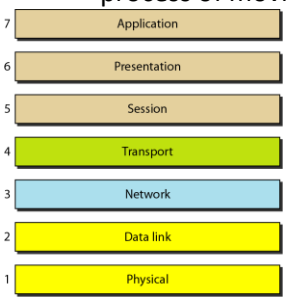



Figure 2.2 Seven layers of the OSI model

**Layered Architecture**

- Grouping of the communication function into related and manageable sets called layers.
- Each layer defines a family of functions distinct from those of the other layers. This layered architecture simplifies the network design

- The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7).
- Figure 2.3 shows the layers involved when a message is sent from device A to device B.
- As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.
- Within a single machine, each layer calls upon the services of the layer just below it.
- For example Layer 3, uses the services provided by layer 2 and provides services for layer 4.

**Peer-to-Peer Processes**

- Between machines, layer x on one machine communicates with layer x on another machine.
- The processes on each machine that communicate at a given layer are called **peer-to-peer processes**.
- This communication is governed by an agreed-upon series of rules and conventions called **protocols**.

**Interfaces Between Layers**

- The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.
- Each interface defines the information and services a layer must provide for the layer above it.
- Well-defined interfaces and layer functions provide modularity to a network.

- In Figure 2.3, device A sends a stream of bits to device B (through intermediate nodes).
- At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers.
- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
- At layer 1 the entire package is converted to a form that can be transmitted to the receiving device.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.
- For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

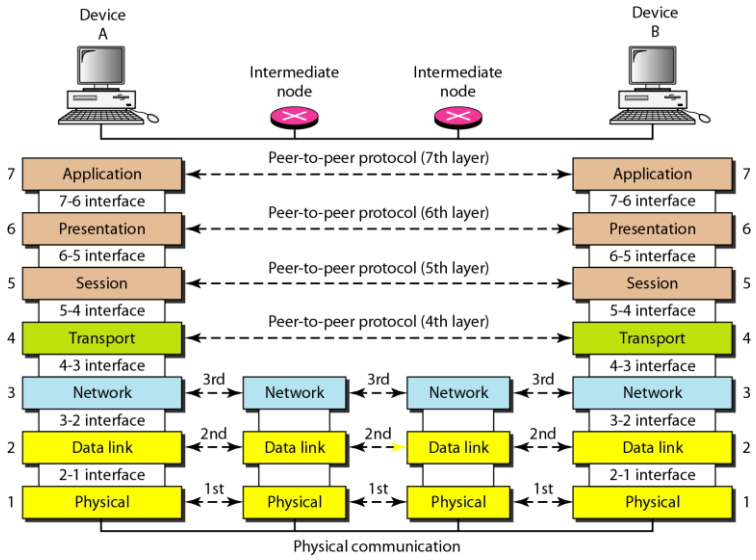



Figure 2.3 The interaction between layers in the OSI model

**Organization of the Layers**

- Layers 1, 2, and 3-physical, data link, and network-are the **network support layers**; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).
- Layers 5, 6, and 7-session, presentation, and application-can be thought of as the **user support layers**; they allow interoperability among unrelated software systems.
- Layer 4, the transport layer, **links** the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.
- The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

https://www.youtube.com/watch?v=O_rsqVtaloI

**Exchange of information**

- In Figure 2.4, which gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on.
- The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order.
- At each layer, a header, or possibly a trailer, can be added to the data unit.
- Commonly, the trailer is added only at layer 2.
- When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.
- Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form.

- The data units then move back up through the OSI layers.
- As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken.
- By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

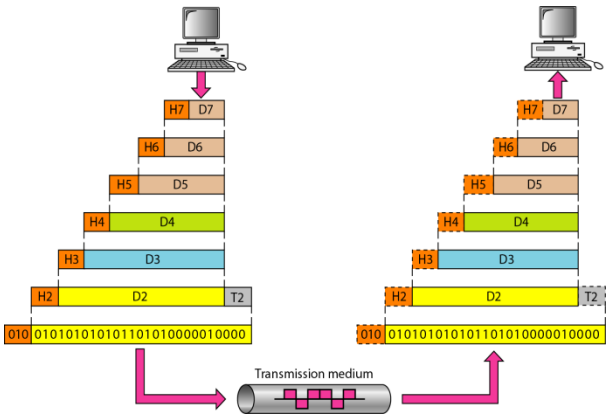



Figure 2.4 An exchange using the OSI model

**Encapsulation**

The data portion of a packet at level N -1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called **encapsulation**; level N -1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level N -1, the whole packet coming from level N is treated as one integral unit.

In Figure 2.3 A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.

**LAYERS IN THE OSI MODEL**

In this section we briefly describe the functions of each layer in the OSI model.

**Physical Layer**

- The physical layer is responsible for movements of individual bits from one hop (node) to the next.

- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.
- Figure 2.5 shows the position of the physical layer with respect to the transmission medium and the data link layer.

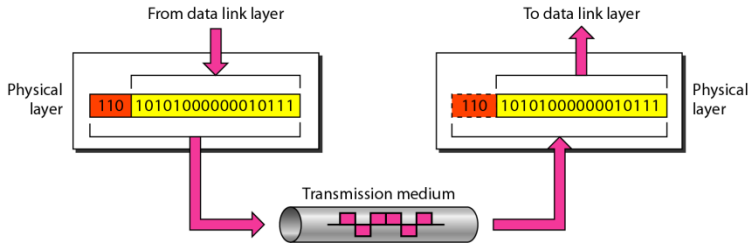



Figure 2.5 Physical layer

The physical layer is also concerned with the following:

- **Physical characteristics of interfaces and medium:** The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- **Representation of bits:** The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of **encoding** (how 0s and 1s are changed to signals).
- **Data rate:** The transmission rate-the number of bits sent each second-is also defined by the physical layer.
- **Synchronization of bits:** The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
- **Line configuration:** The physical layer is concerned with the connection of devices to the media. In a **point-to-point configuration,** two devices are connected through a dedicated link. In a **multipoint configuration,** a link is shared among several devices.
- **Physical topology:** The physical topology defines how devices are connected to make a network. Devices can be connected by using a **mesh topology** (every device is connected to every other device), a **star topology** (devices are connected through a central device), a **ring topology** (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a **hybrid topology** (this is a combination of two or more topologies).
- **Transmission mode:** The physical layer also defines the direction of transmission between two devices: **simplex, half-duplex, or full-duplex.** In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

**Data Link Layer**

- The data link layer is responsible for moving frames from one hop (node) to the next.
- Figure 2.6 shows the relationship of the data link layer to the network and physical layers.

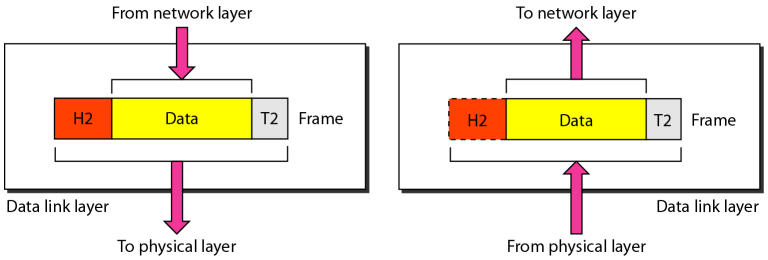



Figure 2.6 Data link layer

Other responsibilities of the data link layer include the following:

- **Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing**. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control.** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a **trailer** added to the end of the frame.
- **Access control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.
-

**Network Layer**

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- The network layer ensures that each packet gets from its point of origin to its final destination.
- Figure 2.8 shows the relationship of the network layer to the data link and transport layers.

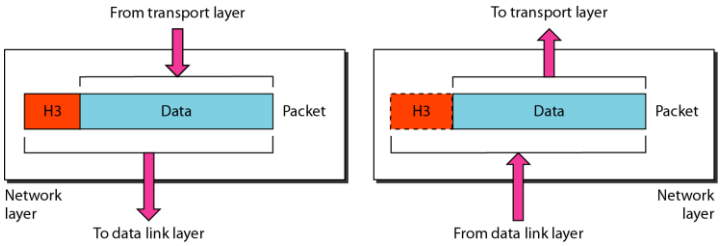



Figure 2.8 Network layer

Other responsibilities of the network layer include the following:

- **Logical addressing:** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing:** When independent networks or links are connected to create intemetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

**Transport Layer**

- The transport layer is responsible for the delivery of a message from one process to another.
  - A process is an application program running on a host.
- The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.
- Figure 2.10 shows the relationship of the transport layer to the network and session layers.

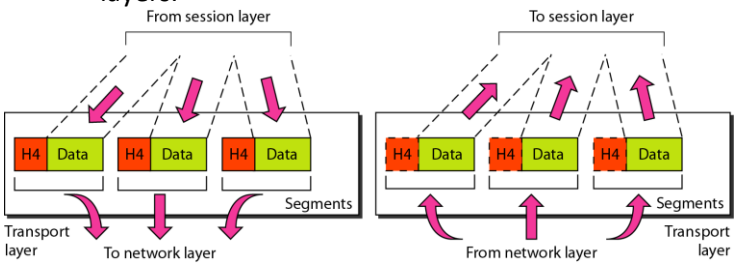



Figure 2.10 Transport layer

Other responsibilities of the transport layer include the following:

- **Service-point addressing:** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must

therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

- **Segmentation and reassembly:** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- **Connection control:** The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- **Flow control**: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control:** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.
- Figure 2.11 illustrates process-to-process delivery by the transport layer.

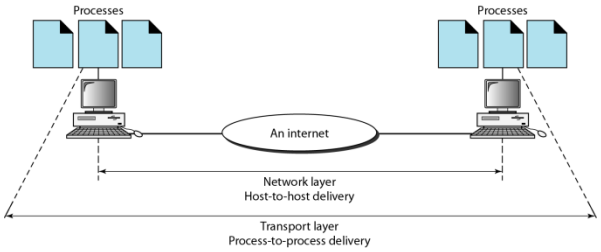



Figure 2.11 Reliable process-to-process delivery ofa message

**Session Layer**

- The session layer is responsible for dialog control and synchronization.
- The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

Specific responsibilities of the session layer include the following:

- **Dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization:** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash

happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

- Figure 2.12 illustrates the relationship of the session layer to the transport and presentation layers.

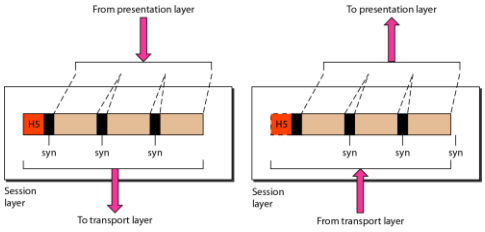



Figure 2.12 Session layer

**Presentation Layer**

- The presentation layer is responsible for translation, compression, and encryption.
- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- Figure 2.13 shows the relationship between the presentation layer and the application and session layers.

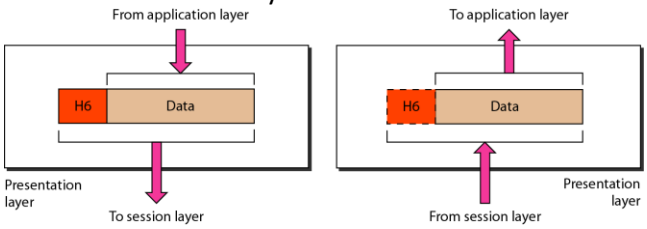



Figure 2.13 Presentation layer

Specific responsibilities of the presentation layer include the following:

- **Translation:** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- **Encryption:** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression:** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

**Application Layer**

- The application layer is responsible for providing services to the user.
- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Figure 2.14 shows the relationship of the application layer to the user and the presentation layer

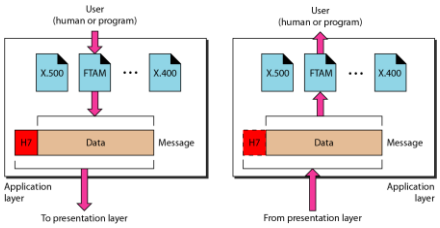



Figure 2.14 Application layer

Specific services provided by the application layer include the following: o

- **Network virtual terminal:** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management:** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services:** This application provides the basis for e-mail forwarding and storage.
- **Directory services:** This application provides distributed database sources and access for global information about various objects and services.

**Summary of Layers**

Figure 2.15 shows a summary of duties for each layer.

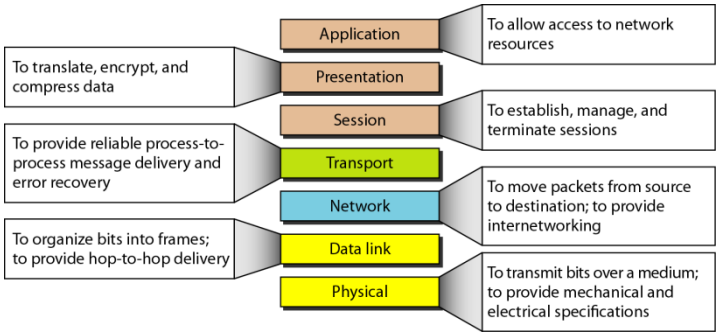



Figure 2.15 Summary of layers

## 2.6 TCP/IP PROTOCOL SUITE /INTERNET MODEL

- The TCPIIP protocol suite was developed prior to the OSI model.
- The TCPIIP protocol suite is made of **five layers**:
    1. physical,
    2. data link,
    3. network,
    4. transport, and
    5. application
- The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCPIIP by a single layer called the application layer (see Figure 2.16).

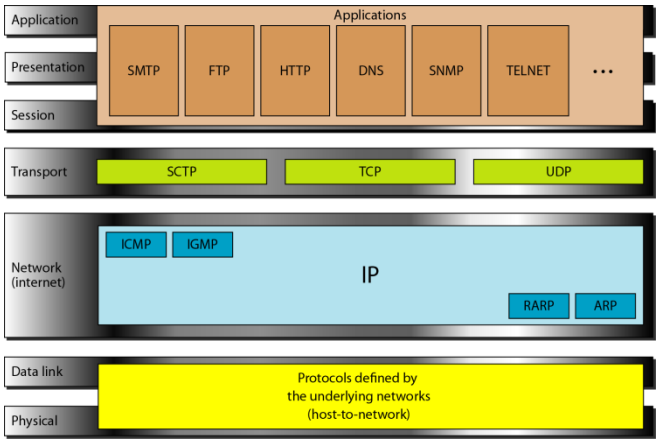



Figure 2.16 TCPIIP and OSI model

- At the transport layer, TCP/IP defines three protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).
- At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

**Physical and Data Link Layers (Host-to-network)**

- At the physical and data link layers, TCP/IP does not define any specific protocol.
- It supports all the standard and proprietary protocols.

**Network Layer (Internet)**

- At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol(IP).
- IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

**Internetworking Protocol (IP)**

- It is an unreliable and connectionless protocol -a best-effort delivery service. The term best effort means that IP provides no error checking or tracking.
- IP transports data in packets called datagrams, each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

**Address Resolution Protocol**

- The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address.
- On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). **ARP is used to find the physical address of the node when its Internet address is known.**

**Reverse Address Resolution Protocol**

- The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

**Internet Control Message Protocol**

- The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
- ICMP sends query and error reporting messages.

**Internet Group Message Protocol**

- The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

**Transport Layer**

- Totally the transport layer was represented in TCP/IP by 3 protocols: TCP, UDP and SCTP.
- UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process

**User Datagram Protocol**

- The User Datagram Protocol (UDP) is the simpler of the two standard TCPIIP transport protocols.
- It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

**Transmission Control Protocol**

- The Transmission Control Protocol (TCP) provides full transport-layer services to applications.
- TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.
- At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received.
- Segments are carried across the internet inside of IP datagrams.
- At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

**Stream Control Transmission Protocol**

- The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet.
- It is a transport layer protocol that combines the best features of UDP and TCP.

**Application Layer**

- The application layer in TCPIIP is equivalent to the combined session, presentation, and application layers in the OSI model.
- Many protocols like SNMP, HTTP, FTP, TELNET,…etc are defined at this layer.

**2.7 ADDRESSING**

Four levels of addresses are used in an internet employing the TCP/IP protocols: (see Figure 2.17).

1. physical (link) addresses,
2. logical (IP) addresses,
3. port addresses, and
4. specific addresses

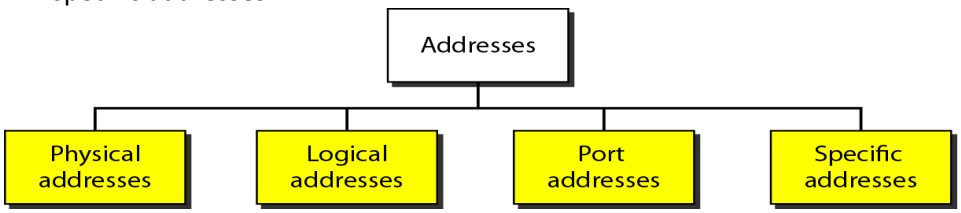



Figure 2.17 Addresses in TCPIIP

Each address is related to a specific layer in the TCPIIP architecture, as shown in Figure 2.18.

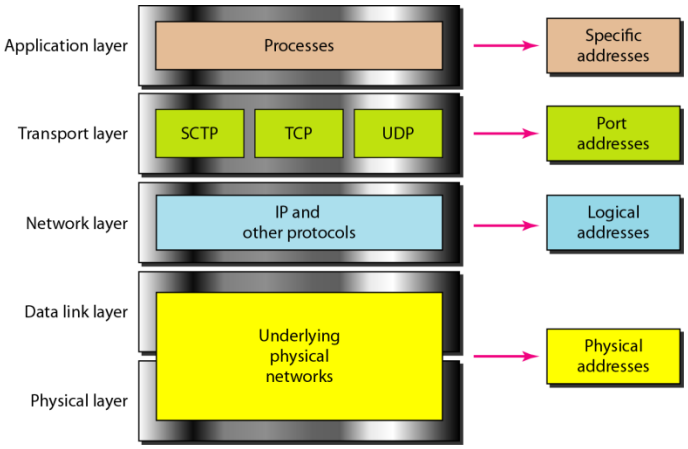



Figure 2.18 Relationship of layers and addresses in TCPIIP

**Physical Addresses**

- The physical address, also known as the **link address(MAC address or NIC address)**, is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer.
- It is the lowest-level address.
- The physical addresses have authority over the network (LAN or WAN).
- The size and format of these addresses vary depending on the network.
  - For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).
  - LocalTalk (Apple), however, has a 1-byte dynamic address that changes each time the station comes up.
- ***most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:***

**07:01:02:01:2C:4B**

**Logical Addresses**

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.
- **A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.**
- No two publicly addressed and visible hosts on the Internet can have the same IP address.
- ***Logicaladdress is a 32-bit address represented by 4 decimal number separated by 3 dots as shown***

**172.20.20.01**

**Port Addresses**

- A port address in TCPIIP is 16 bits in length.
- Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.
  - For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses.
- In the TCP/IP architecture, the label assigned to a process is called a port address.
- ***port address is a 16-bit address represented by one decimal number as shown***

**753**

**Specific Addresses**

- Some applications have user-friendly addresses that are designed for that specific address.
- Examples include the e-mail address (**for example, forouzan@fhda.edu)** and the Universal Resource Locator (URL) (for **example, www.mhhe.com**).

The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer

https://www.youtube.com/watch?v=e5DEVa9eSN0

https://www.youtube.com/watch?v=upQ6OujD6qA

## 2.8 Overview of network topologies

**Type of Connection**

- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.
- For visualization purposes, it is simplest to imagine any link as a line drawn between two points.
- There are two possible types of connections:
  - Point-to-point and
  - Multipoint.

**Point-to-Point**

- A point-to-point connection provides a dedicated link between two devices.
- The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1.3a).
- When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

**Multipoint**

- A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b).
- In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
- If several devices can use the link simultaneously, it is a spatially shared connection.
- If users must take turns, it is a timeshared connection.

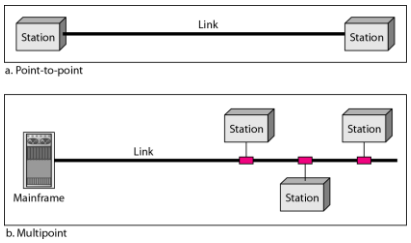



**Figure 1.3 Types *of connections: point-to-point and multipoint***

**Physical Topology**

- The term physical topology refers to the way in which a network is laid out physically. Or Topology refers to the physical or logical arrangement of a network.
- **The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.**
- There are four **basic topologies** possible:
    1. mesh,
    2. star,
    3. bus, and
    4. ring

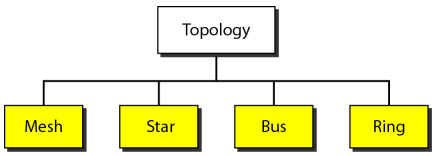



Figure 1.4 Categories of topology

**Mesh Topology**

- In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.
- In a mesh topology, we need n(n -1) /2 duplex-mode links.
- Ex: the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

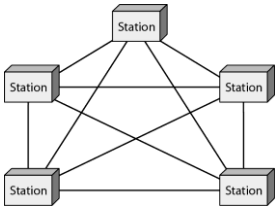



Figure 1.5 A fully connected mesh topology (five devices)

**Advantages:**

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-point links make fault identification and fault isolation easy.

**Disadvantages** of a mesh are related to the amount of cabling and the number of I/O ports required.

1. Installation and reconnection are difficult, because every device must be connected to every other device.
2. The bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. The hardware required to connect each link (I/O ports and cable) can be expensive.

**Star Topology**

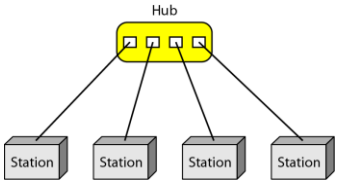



Figure 1.6 A star topology connecting four stations

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another.
- A star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 1.6) .
- The star topology is used in local-area networks (LANs). High-speed LANs often use a star topology with a central hub.

**Advantages**

1. A star topology is less expensive than a mesh topology.
2. Easy to install and reconfigure. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
3. Star topology is robust. If one link fails, only that link is affected. All other links remain active.
4. **Fault identification and fault isolation** is easy.

**Disadvantage**

1. Disadvantage of a star topology is the dependency of the whole topology on one single point, the **hub**. If the hub goes down, the whole system is dead.
2. Cabling cost is more
3. The cost of the hub makes the network expensive as compared to bus and ring topology.

**Bus Topology**

- A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.7).
- When one computer sends a message, all computer on the network receive the information, but one with the address that matches the one encoded in the message accepts the information while all others reject the message.
- Speed is slow because only one computer can send a message at a time. A computer must wait until the bus is free before it can transmit.
- Requires a proper termination at both the ends of the cable.

- Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular now.

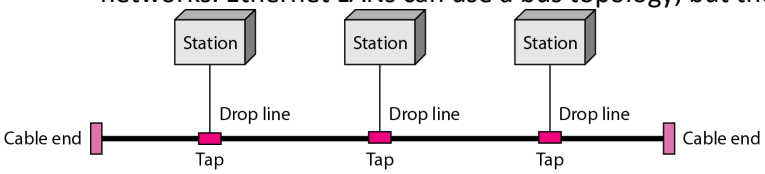



Figure 1.7 A bus topology connecting three stations

**Advantages**

1. Easy to understand, install and use for small networks.
2. Cabling cost is less because a bus uses less cabling than mesh or star topologies.
3. Easy to expand by joining 2 cables with connector.

**Disadvantages**

1. Difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
2. Signal reflection at the taps can cause degradation in quality.
3. Adding new devices may therefore require modification or replacement of the backbone.
4. A fault or break in the bus cable stops all transmission.
5. Requires a proper termination at both the ends of the backbone cable.

**Ring Topology**

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from 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 (see Figure 1.8).

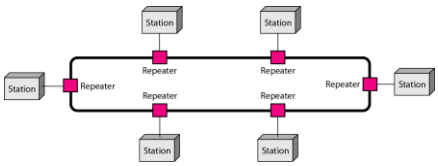



Figure 1.8 A ring topology connecting six stations

**Advantages**

1. A ring topology is easy to install and reconfigure.
2. Fault isolation is simplified.

Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

**Disadvantages**

1. Unidirectional traffic can be a disadvantage. Failure in any cable or node on the ring can affect the whole network.
   In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

2. It is difficult to troubleshoot the ring.
3. Adding or removing the computers disturbs the network activity.

**Hybrid Topology**

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure 1.9.

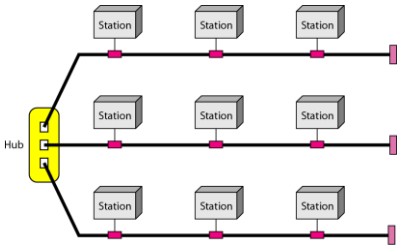



Figure 1.9 A hybrid topology: a star backbone with three bus networks

https://www.youtube.com/watch?v=kUdw7XulC5Y

## Questions

**1.** Explain the need for networking.

2. Explain the function of physical and data link layers of OSI model.

3. Define network communication standards. List different standards

4. Explain the function of transport layer and session layer of OSI model

5. Explain the function of presentation and application layers of OSI model

6. Explain the function of network layer

6. Explain TCP/IP reference model.

7. List different network topologies. Explain with a diagram Ring Topology.

8. Classify types of hardware and software network components.

9. Explain OSI reference model with neat diagram.

10. Compare OSI and TCP/IP Reference Models.

11. Compare Bus and Star Topologies with diagram.

12. Compare Mesh topology and Hybrid topology

## Objective Questions

1. A set of rules that governs all aspects of information communication is called

A. Server

B. Internet

C Protocol

D OSI Model

2. Which of the following is not network support layer

A. Transport layer

B. Network layer

C. Data link layer

D. Physical layer

3. The Process of each machine that communicate at a given layer is called

A. UDP process

B. Intranet process

C. Server technology

D. Peer to Peer process

4. The Duration of time it takes to send a message from one end of a network to the other and back is called

A. Round trip time

B. Full duplex time

C. circle trip time

D. Data travelling time

5. In TCP/IP the error detection is done by

A. Bit sum

B. Data sum

C. Error

D. Check sum

6. The amount of data send from one place to another place in a period of time

A. Limitation

B. Scope

C. Bandwidth

D. Capacity

7. Which of the following is not the possible way of data exchange?

A. Multiplex

B. Half Duplex

C. Full Duplex

D. Simplex

8. How many layers does OSI model has?

A. 4

B. 5

C. 3

D. 7

9.. How many layers does TCP/IP model has?

A. 4

B. 5

C. 3

D. None of above

10. Which of the following provides reliable communication?

A. IP

B. UDP

C. TCP

D. All the above

11. What is the benefits of networking?

A. File Sharing

B. Easier accesses to resources

C Easier backup

D. All of the Above

12. What is the size of Host Bit is Class B of IP address

A. 32

B. 8

C. 16

D. 4

13. What is the size of Network Bit is Class B of IP address

A. 14

B. 8

C. 16

D. 4

14. What is the Maximum Header size of an IP address

A. 60 bytes

B. 32 bytes

C. 16 bytes

D. 64 bytes

# UNIT- 3: Error Detection and Correction

Networks must be able to transfer data from one device to another with acceptable accuracy. For most applications, a system must guarantee that the data received are identical to the data transmitted. Any time data are transmitted from one node to the next, they can become corrupted in passage. Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting errors.

Some applications can tolerate a small level of error. For example, random errors in audio or video transmissions may be tolerable, but when we transfer text, we expect a very high level of accuracy.

## 3.1 INTRODUCTION

Let us first discuss some issues related, directly or indirectly, to error detection and correction.

## 3.2 Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal.

### Single-Bit Error

- The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.
- Figure 10.1 shows the effect of a single-bit error on a data unit.
- In Figure 10.1, 00000010 (ASCII STX) was sent, meaning start of text, but 00001010 (ASCII LF) was received, meaning line feed.
- Single-bit errors are the **least likely type of error** in serial data transmission.

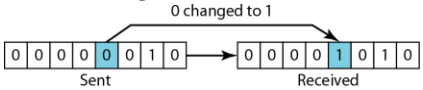



Figure 10.1 Single-bit error

### Burst Error

- The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.
- Figure 10.2 shows the effect of a burst error on a data unit. In this case, 0100010001000011 were sent, but 0101110101100011 were received.
- Note that a burst error does not necessarily mean that the errors occur in consecutive bits.

- The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.
- A burst error is **more likely to occur** than a single-bit error.
- The duration of noise is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits.

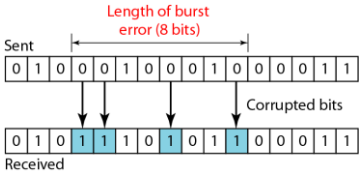



Figure 10.2 Burst error of length 8

### 3.3 Redundancy

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some **extra (redundant) bits** with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.

### 3.4 Detection versus Correction

The correction of errors is more difficult than the detection.

- In **error detection**, we are looking only to see if any error has occurred. The answer is a simple yes or no.We are not even interested in the number of errors.
- In **error correction**, we need to know the exact number of bits that are corrupted and more importantly, their location in the message.
  - The number of the errors and the size of the message are important factors.
  - If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities.

### 3.5 Forward Error Correction Versus Retransmission

There are two main methods of error correction.

- **Forward error correction** is the process in which the receiver tries to guess the message by using redundant bits. This is possible if the number of errors is small.

- **Correction by retransmission** is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free

### 3.6 Coding

- Redundancy is achieved through various **coding schemes**.
- The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits.
- The receiver checks the relationships between the two sets of bits to detect or correct the errors.
- Figure 10.3 shows the general idea of coding.
- We can divide coding schemes into **two broad categories: block coding and convolution coding.**
- we concentrate on only **block coding**

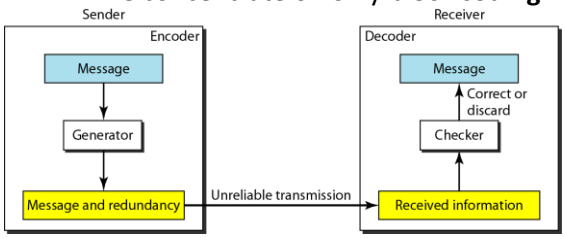



Figure 10.3 The structure of encoder and decoder

### 3.7 BLOCK CODING

- In block coding, we divide our message into blocks, each of k bits, called **datawords.**
- We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called **codewords.**
- We have a set of datawords, each of size k, and a set of codewords, each of size of n.
- With k bits, we can create a combination of $2^k$ datawords; with n bits, we can create a combination of $2^n$ codewords. Since n > k, the number of possible codewords is larger than the number of possible datawords.
- The block coding process is one-to-one; the same dataword is always encoded as the same codeword.
- This means that we have $2^n - 2^k$ codewords that are not used. We call these codewords invalid or illegal.
- Figure 10.5 shows the situation.

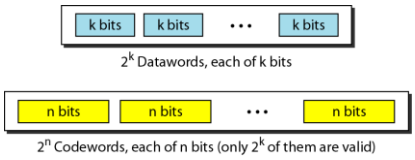



Figure 10.5 Datawords and codewords in block coding

### 3.8 Error Detection

How can errors be detected by using block coding? If the following two conditions are met, the receiver can detect a change in the original codeword.

1. The receiver has (or can find) a list of valid codewords.
2. The original codeword has changed to an invalid one.

Figure 10.6 shows the role of block coding in error detection.

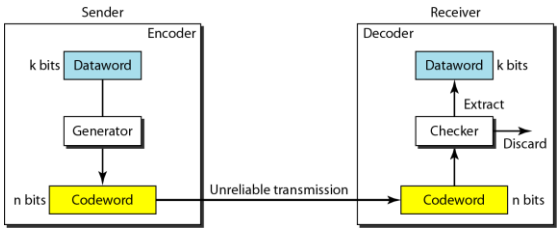



Figure 10.6 Process oferror detection in block coding

The sender creates codewords out of datawords by using a generator that applies the rules and procedures of encoding (discussed later). Each codeword sent to the receiver may change during transmission. If the received codeword is the same as one of the valid codewords, the word is accepted; the corresponding dataword is extracted for use. If the received codeword is not valid, it is discarded. However, if the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected. This type of coding can detect only single errors. Two or more errors may remain undetected.

### 3.9 Error Correction

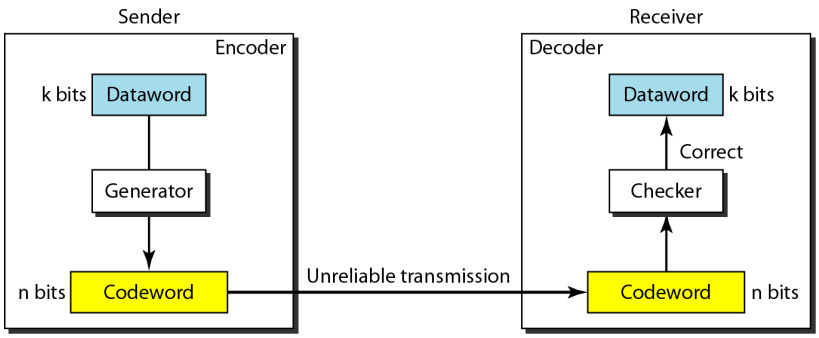



Figure 10.7 Structure of encoder and decoder in error correction

- Error correction is much more difficult than error detection. In error correction the receiver needs to find (or guess) the original codeword sent. We need more redundant bits for error correction than for error detection.
- Figure 10.7 shows the role of block coding in error correction.
- We can see that the idea is the same as error detection but the checker functions are much more complex.

### 3.10 CYCLIC CODES

- In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.
- For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword.

### 3.10.1 Cyclic Redundancy Check

- We can create cyclic codes to correct errors.
- Cyclic redundancy check (CRC) is used in networks such as LANs and WANs.
- Table 10.6 shows an example of a CRC code. We can see both the linear and cyclic properties of this code.
- Figure 10.14 shows one possible design for the encoder and decoder.

| *Dataword* | *Codeword* | *Dataword* | *Codeword* |
|---|---|---|---|
| 0000 | 0000000 | 1000 | 1000101 |
| 0001 | 0001011 | 1001 | 1001110 |
| 0010 | 0010110 | 1010 | 1010011 |
| 0011 | 0011101 | 1011 | 1011000 |
| 0100 | 0100111 | 1100 | 1100010 |
| 0101 | 0101100 | 1101 | 1101001 |
| 0110 | 0110001 | 1110 | 1110100 |
| 0111 | 0111010 | 1111 | 1111111 |

Table 10.6 A CRC code with C(7, 4)

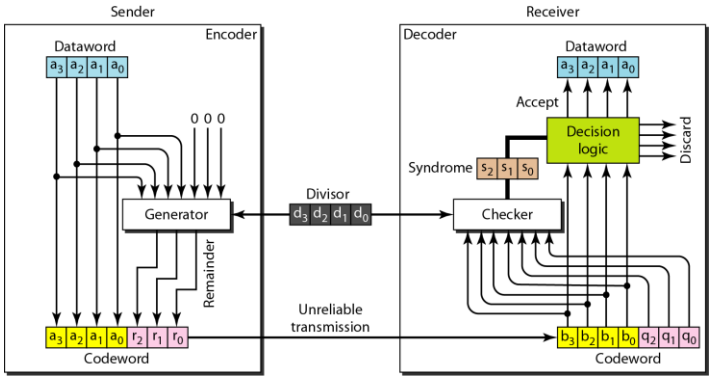



Figure 10.14 CRC encoder and decoder

- In **the encoder**, the dataword has k bits (4 here); the codeword has n bits (7 here).

- The size of the dataword is augmented by adding n -k (3 here) 0s to the right-hand side of the word.
- The n-bit result is fed into the generator.
- The generator uses a divisor of size n -k + 1 (4 here), predefined and agreed upon.
- The generator divides the augmented dataword by the divisor (modulo-2 division).
- The quotient of the division is discarded; the remainder (r2 rl r0) is appended to the dataword to create the codeword.

- **The decoder** receives the possibly corrupted codeword.
- A copy of all n bits is fed to the checker which is a replica of the generator.
- The remainder produced by the checker is a syndrome of n -k (3 here) bits, which is fed to the decision logic analyzer. The analyzer has a simple function. If the syndrome bits are all 0s, the 4 leftmost bits of the codeword are accepted as the dataword (interpreted as no error); otherwise, the 4 bits are discarded (error).

**Encoder**

- Let us take a closer look at the encoder.
- The encoder takes the dataword and augments it with n -k number of 0s.
- It then divides the augmented dataword by the divisor, as shown in Figure 10.15.

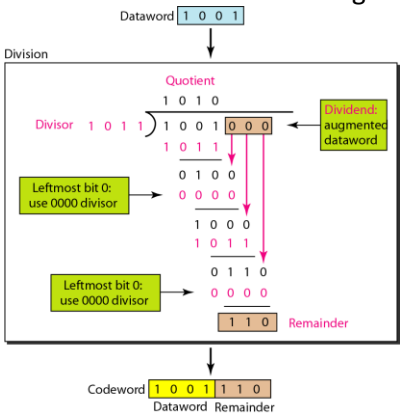



Figure 10.15 Division in CRC encoder

**Dataword Remainder**

- The process of modulo-2 binary division is the same as the familiar division process we use for decimal numbers. However, in this case addition and subtraction are the same. We use the XOR operation to do both.
- As in decimal division, the process is done step by step. In each step, a copy of the divisor is XORed with the 4 bits of the dividend.
- The result of the XOR operation (remainder) is 3 bits (in this case), which is used for the next step after 1 extra bit is pulled down to make it 4 bits long.
- There is one important point we need to remember in this type of division. If the leftmost bit of the dividend (or the part used in each step) is 0, the step cannot use the regular divisor; we need to use an all-0s divisor.
- When there are no bits left to pull down, we have a result.

- The 3-bit remainder forms the check bits (r2' rl' and r0). They are appended to the dataword to create the codeword.

**Decoder**

- The codeword can change during transmission.
- The decoder does the same division process as the encoder.
- The remainder of the division is the **syndrome**.
- If the syndrome is all 0s, there is no error; the dataword is separated from the received codeword and accepted. Otherwise, everything is discarded.
- Figure 10.16 shows two cases: The left hand figure shows the value of syndrome when no error has occurred; the syndrome is 000. The right-hand part of the figure shows the case in which there is one single error. The syndrome is not all 0s (it is 011).

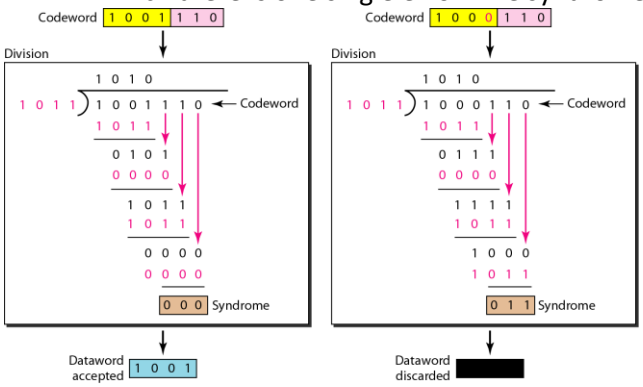



Figure 10.16 Division in the CRC decoder for two cases

**Advantages of Cyclic Codes**

- Cyclic codes have a very good performance in detecting single-bit errors, double errors, an odd number of errors, and burst errors.
- They can easily be implemented in hardware and software.
- They are especially fast when implemented in hardware. This has made cyclic codes a good candidate for many networks.

**3.10.2 Polynomials**

- A better way to understand cyclic codes and how they can be analyzed is to represent them as polynomials.
- A pattern of 0s and 1s can be represented as a polynomial with coefficients of 0 and 1.
- The power of each term shows the position of the bit; the coefficient shows the value of the bit.
- Figure 10.21 shows a binary pattern and its polynomial representation. In Figure 10.21a we show how to translate a binary pattern to a polynomial; in Figure 10.21b we show how the polynomial can be shortened by removing all terms with zero coefficients and replacing $x^1$ by x and $x^0$ by 1.
- Figure 10.21 shows one immediate benefit; a 7-bit pattern can be replaced by three terms.

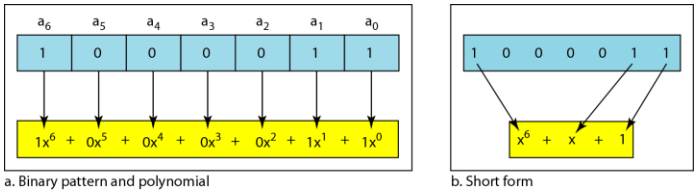



Figure 10.21 A polynomial to represent a binary word

**Degree of a Polynomial**

- The degree of a polynomial is the **highest power** in the polynomial.
- For example, the degree of the polynomial $x^6 + x + 1$ is 6. Note that the degree of a polynomial is 1 less that the number of bits in the pattern. The bit pattern in this case has 7 bits.

**Adding and Subtracting Polynomials**

- Adding and subtracting polynomials in mathematics are done by adding or subtracting the coefficients of terms with the same power.
- In our case, the coefficients are only 0 and 1, and adding is in modulo-2.
- This has two consequences. First, addition and subtraction are the same.
- Second, **adding or subtracting is done by combining terms and deleting pairs of identical terms.**
  - For example, adding $x^5 + x^4 + x^2$ and $x^6 + x^4 + x^2$ gives just $x^6 + x$. The terms $x^4$ and $x^2$ are deleted.

**Multiplying or Dividing Terms**

- In this arithmetic, multiplying a term by another term is very simple; we just **add the powers**.
  - For example, $x * x^4$ is $x^5$,
- For dividing, we just **subtract the power of the second term from the power of the first**.
  - For example, $x^5/x^2$ is $x^3$.

**Shifting**

- A binary pattern is often shifted a number of bits to the right or left.
- Shifting to the **left means adding extra 0s** as rightmost bits; shifting to the **right means deleting some rightmost bits.**
  - Shifting left 3 bits: 10011 becomes 10011000 $x^4 + x + 1$ becomes $x^7 + x^4 + x^3$
  - Shifting right 3 bits: 10011 becomes 10 $x^4 + x + 1$ becomes $x$
- When we augmented the dataword in the encoder of Figure 10.15, we actually shifted the bits to the left. Also note that when we concatenate two bit patterns, we shift the first polynomial to the left and then add the second polynomial.

**Cyclic Code Encoder Using Polynomials**

- Figure 10.22 is the polynomial version of Figure 10.15. We can see that the process is shorter.
- The dataword 1001 is represented as $x^3 + 1$. The divisor 1011 is represented as $x^3 + x + 1$.
- To find the augmented dataword, we have left-shifted the dataword 3 bits (multiplying by x The result is $x^6 + x$.)
- Division is straightforward. We divide the first term of the dividend, x, by the first term of the divisor, x. The first term of the quotient is then $x^6/x^3$, or x. Then we multiply $x^3$ by the divisor and subtract (according to our previous definition of subtraction) the result from the dividend. The result is $x^4$, with a degree greater than the divisor's degree; we continue to divide until the degree of the remainder is less than the degree of the divisor.

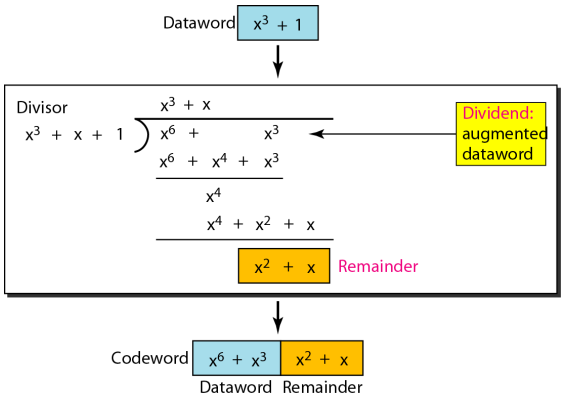



Figure 10.22 CRC division using polynomials

https://www.youtube.com/watch?v=aNqiTCZ-nko

https://www.youtube.com/watch?v=x6RfdZigBOI

### 3.11 FLOW AND ERROR CONTROL

Data communication requires at least two devices working together, one to send and the other to receive. Even such a basic arrangement requires a great deal of coordination for an intelligible exchange to occur. *The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as* ***data link control.***

#### 3.11.1 Flow Control

- Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.
- The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending

device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a **buffer**, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

### 3.11.2 Error Control

- Error control is both error detection and error correction.
- It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender.
- Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called **automatic repeat request (ARQ).**
- Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

### 3.12 Multiple Access

We can consider the data link layer as two sub layers. The upper sub layer is responsible for data link control, and the lower sublayer is responsible for resolving access to the shared media. Figure 12.1 shows these two sublayers in the data link layer.

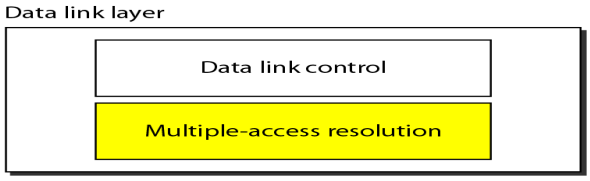



Figure 12.1 Data link layer divided into two functionality-oriented sub layers

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link. The problem of controlling the access to the medium is similar to the rules of speaking in an assembly. The procedures guarantee that the right to speak is upheld and ensure that two people do not speak at the same time, do not interrupt each other, and do not monopolize the discussion, and so on.

Many formal protocols have been devised to handle access to a shared link. We categorize them into three groups. Protocols belonging to each group are shown in Figure 12.2.

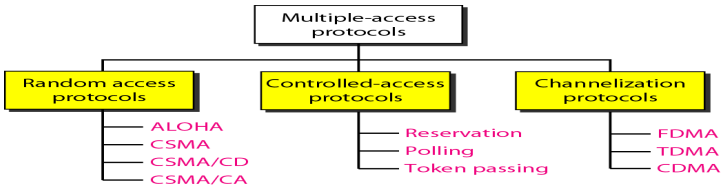



Figure 12.2 Taxonomy of multiple-access protocols discussed in this chapter

**RANDOM ACCESS**

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send..

**3.12.1 Carrier Sense Multiple Access (CSMA)**

CSMA is based on the principle "sense before transmit" or "listen before talk."

CSMA can reduce the possibility of collision, but it cannot eliminate it.

**Persistence Methods**

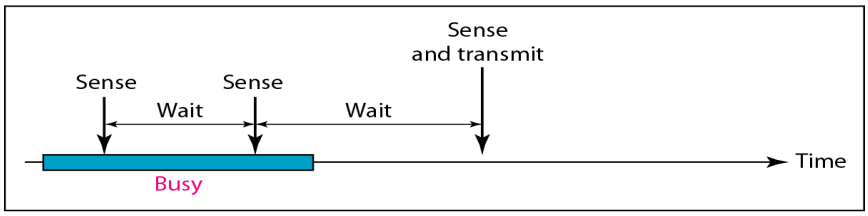
What should a station do if the channel is busy? What should a station do if the channel is idle?

**Three** methods have been devised to answer these questions:

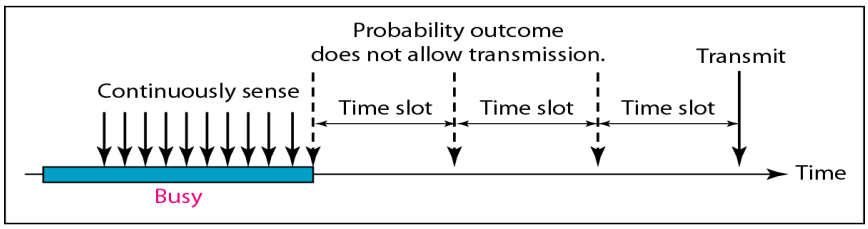
1. 1-persistent method,
2. Nonpersistent method, and
3. p-persistent method.

Figure 12.10 shows the behavior of three persistence methods when a station finds a channel busy.


a. 1-persistent

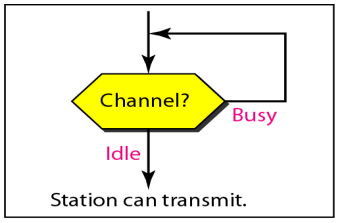



b. Nonpersistent

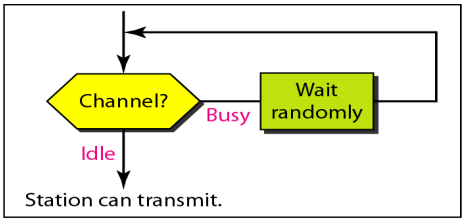



c. p-persistent

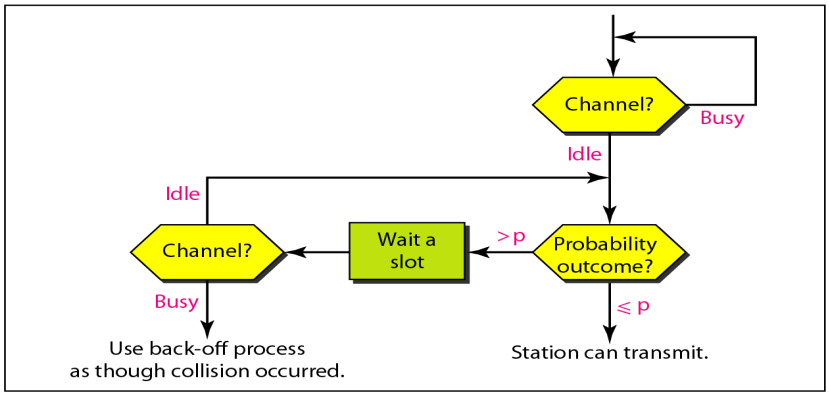
Figure 12.10 Behavior of three persistence methods




a. 1-persistent




b. Nonpersistent




c. p-persistent

Figure 12.11 shows the flow diagrams for these methods.

**1-Persistent**In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).

Advanta

The 1-persistent method is **simple and straightforward**.

This method has the **highest chance of collision** because two or more stations may find the line idle and send their frames immediately.

**Non-persistent** In the non-persistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, **it waits a random amount of time** and then senses the line again.

The non-persistent approach **reduces the chance of collision** because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.

However, this method **reduces the efficiency of the network** because the medium remains idle when there may be stations with frames to send.

**c. p-persistent** The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.

The p-persistent approach combines the advantages of the other two strategies.

It reduces the chance of collision and improves efficiency.

In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.

2. With probability q =1-p, the station waits for the beginning of the next time slotand checks the line again.

a. If the line is idle, it goes to step 1.

b.Ifthe line is busy, it acts as though a collision has occurred and uses the backoff procedure.

Figure 12.11 Flow diagram for three persistence methods

https://www.youtube.com/watch?v=R3UmGs0Bht0

### 3.12.2 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Carriers sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

**Procedure**

Now let us look at the flow diagram for CSMA/CD in Figure 12.14. It is similar to the one for the ALOHA protocol, but there are differences.

The **first difference** is the addition of the persistence process. We need to sense the channel before we start sending the frame by using one of the persistence processes we discussed previously (non persistent, 1-persistent, or p-persistent). The corresponding box can be replaced by one of the persistence processes shown in Figure 12.11.

The **second difference** is the frame transmission. In CSMA/CD, transmission and collision detection is a continuous process. We do not send the entire frame and then look for a collision. The station transmits and receives continuously and simultaneously (using two different ports). We use a loop to show that transmission is a continuous process. We constantly monitor in order to detect one of two conditions: either transmission is finished or a collision is detected. Either event stops transmission. When we come out of the loop, if a collision has not been detected, it means that transmission is complete; the entire frame is transmitted. Otherwise, a collision has occurred.

The **third difference** is the sending of a short jamming signal that enforces the collision in case other stations have not yet sensed the collision.

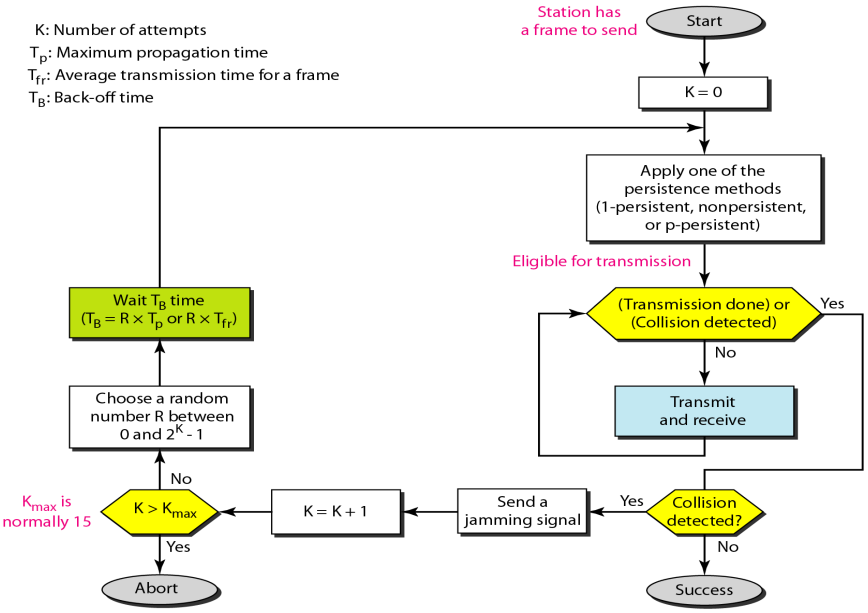



Figure 12.14 Flow diagram for the CSMA\CD

https://www.youtube.com/watch?v=LzGSZufwMCc

### 3.13 CONTROLLED ACCESS

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss three popular controlled-access methods.

#### 3.13.1 Reservation

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval. Ifthere are N stations in the system, there are exactly N reservation minislots in the reservation frame. Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame.

Figure 12.18 shows a situation with five stations and a five-minislot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

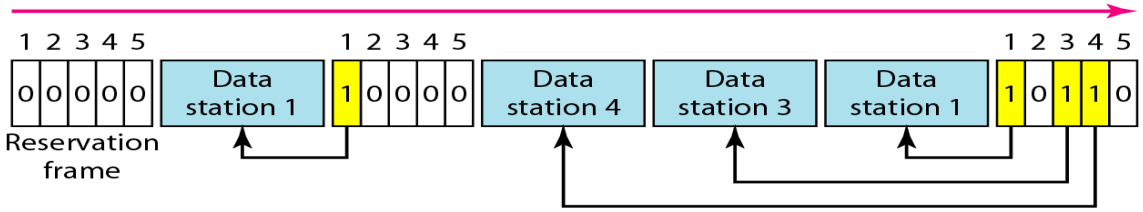



Figure 12.18 Reservation access method

### 3.13.2 Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session (see Figure 12.19).

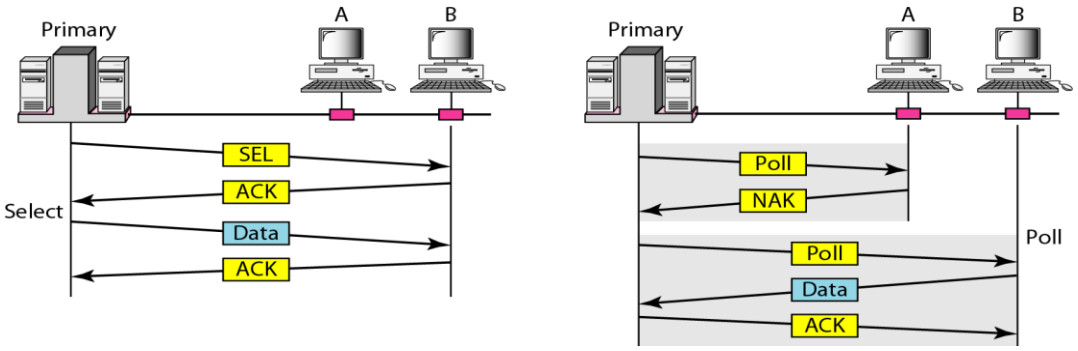



Figure 12.19 Select and poll functions in polling access method

Ifthe primary wants to receive data, it asks the secondaries if they have anything to send; this is called **poll function**. If the primary wants to send data, it tells the secondary to get ready to receive; this is called **select function**.

#### Select

The select function is used whenever the primary device has something to send. So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the

secondary's ready status. Before sending data, the primary creates and transmits a **select (SEL) frame**, one field of which includes the address of the intended secondary.

**Poll**

The poll function is used by the primary device to ask for transmissions from the secondary devices. When the primary is ready to receive data, it must ask **(poll)** each device in turn if it has anything to send. When the first secondary is approached, it responds either with a **NAK frame** if it has nothing to send or with data (in the form of a data frame) if it does. If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (**ACK frame),** verifying its receipt.

**3.13.3 Token Passing**

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The **predecessor** is the station which is logically before the station in the ring; the **successor** is the station which is after the station in the ring. The **current station** is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

In this method, **a special packet called a token** circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.

**Logical Ring**

In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one. Figure 12.20 show four different physical topologies that can create a logical ring.

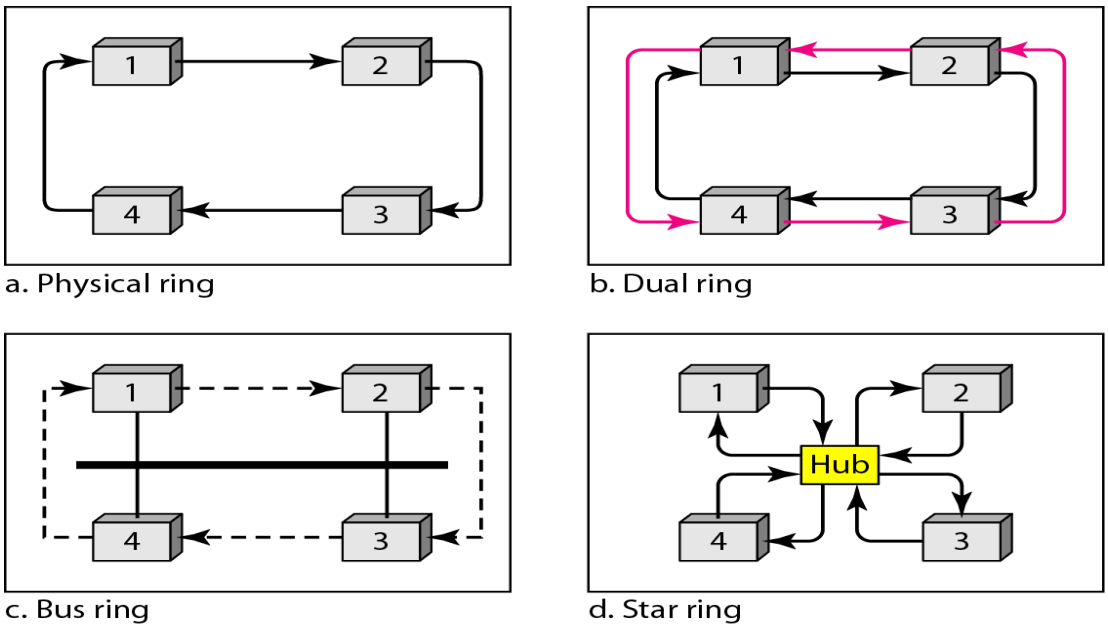



Figure 12.20 Logical ring and physical topology in token-passing access method

In the **physical ring topology**, when a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line. This means that the token does not have to have the address of the next successor. The problem with this topology is that if one of the links-the medium between two adjacent stationsfails, the whole system fails.

The **dual ring** topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring. The second ring is for emergencies only (such as a spare tire for a car). If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring. After the failed link is restored, the auxiliary ring becomes idle again..

In the **bus ring** topology, also called a token bus, the stations are connected to a single cable called a bus. They, however, make a logical ring, because each station knows the address of its successor (and also predecessor for token management purposes). When a station has finished sending its data, it releases the token and inserts the address

of its successor in the token. Only the station with the address matching the destination address of the token gets the token to access the shared media.

In a **star ring** topology, the physical topology is a star. There is a hub, however, that acts as the connector. The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections. This topology makes the network less prone to failure because if a link

goes down, it will be bypassed by the hub and the rest of the stations can operate. Also adding and removing stations from the ring is easier.

**Activities**

1. How many bits in data unit has changed in single bit error

A. only 1.
B. two bits.
C. three bits.
D. four bits.

Ans A

2. Cyclic codes are fast when these are implemented in

A. software.
B. hardware.
C. Local area network.
D. Wide area network.

Ans is B

3.In block coding, we divide our message into blocks, is called

A. code blocks.
B. packet blocks.
C. code words.
D. datawords.

Ans is D

4.Process of modulo-2 binary division is same as the

A. multiplication.
B. division.

C. addition.
D. subtraction.

Ans B

5.Traditionally, Internet checksum is

A. 8-bit.
B. 16-bit.
C. 24-bit.
D. 32-bit.

Ans B

6. If value of checksum is 0, then message is

A. accepted.
B. rejected.
C. sent back.
D. resend.

Ans A

7 .CRC stands for

A. combine resistance check.
B. cyclic redundancy cod.
C. combine redundancy code.
D. cyclic redundancy check.

Ans is D

8. A pattern of 0s and 1s can be represented as a

A. bits.
B. modulo-2.
C. polynomial.

D. coefficient.

Ans is C

9. Forward error correction is possible when number of errors is

A. zero.
B. small.
C. large.
D. infinity.

Ans is B

10. Single-bit errors are least likely type of error in

A. parallel data transmission.
B. serial data transmission..
C. unidirectional transmission.
D. bidirectional transmission.

Ans is B

11. In a cyclic code, decoder is failed to detect any error, when syndrome is

A. zero.
B. non zero.
C. infinity.
D. negative value.

Ans is A

12. In a cyclic code, generator polynomial is normally called the

A. multiplier.
B. divisor.
C. addition.
D. subtraction.

Ans is B

http://in.mcqslearn.com/cs/computer-networks/mcq/error-detection-correction-mcqs-test.php?page=6

**Questions**

1.Explain the terms –

a. Error detection.
b. Error correction.
c. Redundancy.
d. Forward error correction.
e. Re-transmission.

2. Illustrate with examples different types of errors.

3 . Illustrate block coding with example.

4 . Mention some standard CRC Polynomials.

5. Discuss the advantages of Cyclic Codes.

6. Explain briefly CSMA protocol

7. Write a note on CSMA/CD.

8 . Explain with a diagram and an example, the process of error detection using block coding method.

9. With a diagram and an example, explain the structure of encoder and decoder in error correction.

10 .Illustrate with a block diagram process of error detection in block coding.

11. Explain the design of CRC encoder and decoder, with an example.

12. With an example, explain CRC division with polynomials.

13. Discuss Controlled Access methods.

# UNIT- 4: LAN Components and Protocols

## 4.1 Introduction

To establish a connection between two computers or devices, we need hardware as well as software components. The hardware components are usually cables, hubs, Network Interface Cards (NICs), and switches. The software components are protocols such as Ethernet, Token Ring, and TCP/IP. The hardware components of a LAN are devices operating at the physical layer or the data link layer and are responsible for transmission of electrical signals from one device to another. To transmit electrical signals, the following devices are commonly used in LANs.

- Cables
- Repeaters
- Hubs
- Switches
- Network Interface Cards

## 4.2 Cables

Transmission medium is the means by which a communication signal is carried from one system to another. Basically, a transmission medium is the cable, a wire capable of transmitting signals from one device to another. When transmitting signals from one device to another, the following factors must be considered: bandwidth, distance.

### 4.2.1 Bandwidth

Bandwidth is a widely used term that usually refers to the data-carrying capacity of a cable. It indicates the maximum amount of data that can be transmitted from one point to another in a unit of time. For example, a bandwidth of 10Mbps (10 Megabits per second) indicates that the cable can transfer 10 million bits of data per second.

Throughput is the amount of data that is actually transferred between two computers or network devices. Throughput is affected by the length of communication medium i.e. the distance between the computers to be connected. In the above example, if the length of the cable exceeds a particular value, the actual throughput may be less than 10Mbps.

### 4.2.2 Distance

The bandwidth of a cable is limited by the distance over which the medium needs to transmit the signal. If the distance between the computers is greater, the bandwidth decreases because the signal needs to travel over a greater distance

**Attenuation**

Signal attenuation is one of the most difficult problems faced by network administrators when connecting computers and devices in a network. When a signal is transmitted across a cable, the cable offers resistance to this transmission. This resistance consumes a part of the signal strength, and as a result, the signal strength decreases. If the length of the cable is too great, almost all of the signal strength is used to overcome the resistance. As a result, the destination computer or device does not receive any data.

Attenuation is overcome in LANs by using:

- Short length cables – The amount of resistance offered by the cable is less, and, therefore, attenuation is also less.
- Amplifiers – in practice, it is not possible to use short cable lengths in a LAN. In such cases, devices such as repeaters, active hubs, and switches are used to amplify the attenuated signal so that the destination computer or device can receive the signal.

Figure 4.1 shows the use of amplifier or repeater to amplify the signals.

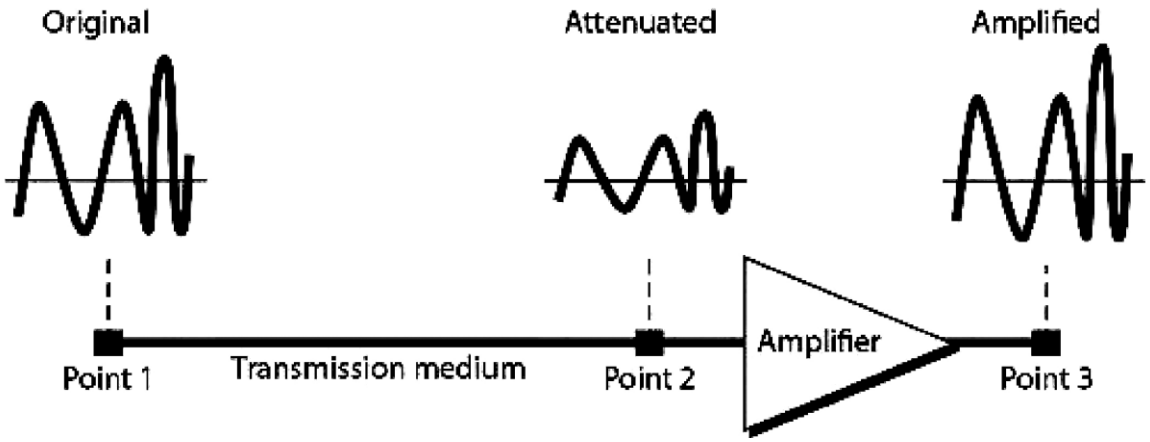



**Figure 4.1 Amplifier or Repeater used to amplify signal strength**

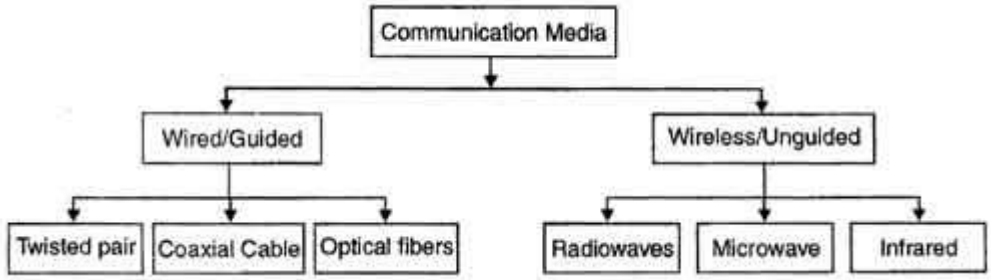
**Distortion**

Unlike attenuation, which decrease the signal strength, distortion modifies the signal itself. When a signal is modified, the data transmitted by the signal becomes corrupt. As a result, the destination computer or device may not be able to interpret the signal and obtain the correct data. The following methods are used to prevent distortion:

- The possible causes and the effect of EMI or RFI in the network are analyzed and communication media that are resistant of interference are used.
- Cables are not passed through regions of high interference.
- Network protocols capable of detecting signal corruption are sued to check errors during transmission.

Transmission media is broadly classified into two groups.

1. Wired or Guided Media or Bound Transmission Media
2. Wireless or Unguided Media or Unbound Transmission Media




In guided media, the sender and receiver are directly connected and the information is send (guided) through it.

There are three common types of cable media that can be used to connect devices to a network and they are coaxial cable, twisted-pair cable, and fiber-optic cable.

**4.3 Coaxial Cable**

At one time, coaxial cable was the most widely used network cabling. There were a couple of reasons for coaxial cable's wide usage: it was relatively inexpensive, and it was light, flexible, and easy to work with.

In its simplest form, *coaxial cable* consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover. Figure 4.2 shows the various components that make up a coaxial cable.

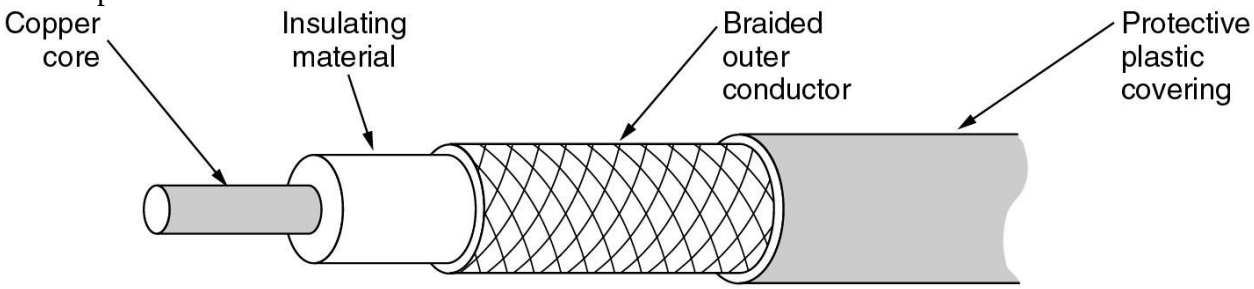



**Figure 4.2 Coaxial Cable**

The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. If the core is solid, it is usually copper. Surrounding the core is a dielectric insulating layer that separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk. The conducting core and the wire mesh must always be kept separate from each other. A non-conducting outer shield usually made of rubber, Teflon, or plastic surrounds the entire cable. Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling. Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable.

The two types of coaxial cabling are thick coaxial and thin coaxial.
They are also called as thicknet or 10Base5 and thinnet or 10Base2 respectively.

Thinnet is a flexible coaxial cable about 0.25 inch thick. Thinnet is used for short-distance. Thinnet connects directly to a workstation's network adapter card using a British Naval Connector (BNC). The maximum length of thinnet is 185 meters.

Thicknet coaxial is thicker cable than thinnet. Thicknet cable is about 0.5 inch thick and can support data transfer over longer distances than thinnet. Thicknet has a maximum cable length of 500 meters and usually is used as a backbone to connect several smaller thinnet-based networks.

There are three categories of coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG stands for Radio Government.

### 4.4 Twisted-Pair Cables

A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk. Crosstalk is the undesired signal noise generated by the Electro-Magnetic fields of the adjacent wires. Twisted pair may be used to transmit both analog and digital signals. For analog signals, amplifiers are required about every 5 to 6 km. For digital signals, repeaters are required every 2 or 3 km.

The construction of twisted pair cable has been shown in Figure 4.3. This is the most commonly used medium and it is cheaper than the co-axial cable.

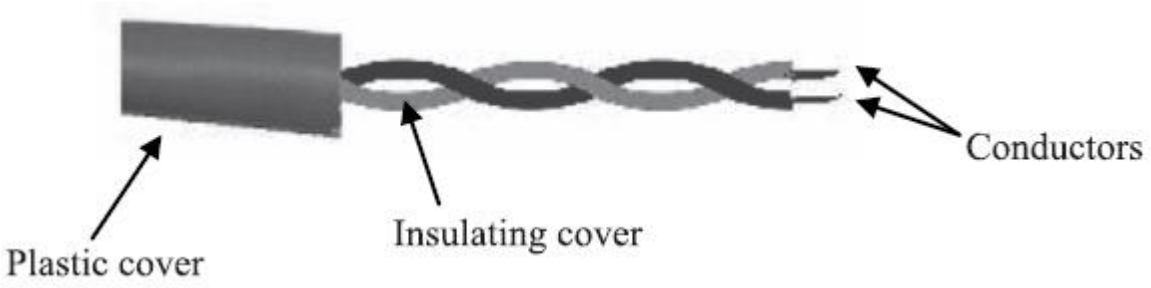



**Figure 4.3 Construction of twisted pair cable**

A twisted pair consists of two insulated conductor twisted together in the spiral form. Twisting of wires will reduce the effect of noise or external interference. One of the wires is used to carry signals to the receiver and the other is used only as a ground reference. By twisting the cable balance is maintained. The number of twists per unit length will determine the quality of the cable. More twists means better quality. It can be shielded or unshielded.
The most common twisted pair cables used in communication are:

- Unshielded twisted pair (UTP)
- Shielded twisted pair (STP)

### 4.4.1 Unshielded Twisted Pair Cable (UTP)

Unshielded twisted-pair (UTP) cable is the most common networking media. Unshielded twisted-pair (UTP) consists of four pairs of thin, copper wires covered in color-coded plastic insulation that are twisted together. The wire pairs are then covered with a plastic outer jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.

The unshielded twisted pair cables are very cheap and easy to install. Therefore, UTP is the most popular and is generally the best option for school networks. But they are badly affected by the noise interference. Colors used for Twisted Pair wires are Orange, Orange-White, Blue, Blue-White, Green, Green-White, Brown and Brown-White. . Following Figure 4.4 shows a dissected Unshielded Twisted Pair cable.

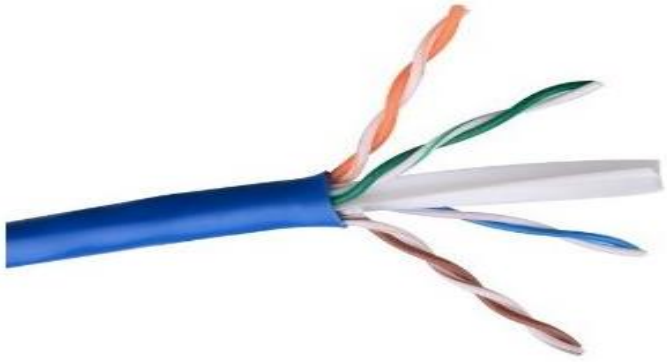


**Figure 4.4 Unshielded twisted pair cable**

UTP cabling has different categories. Each category of UTP cabling was designed for a specific type of communication or transfer rate. The most popular categories in use today is 5e and 6, which can reach transfer rates of over 1000 Mbps (1 Gbps). Unshielded Twisted

Pair cables support a maximum distance of 100 Meters (from NIC Card to Switch Port), without signal distortion.
The following table shows different UTP categories and corresponding transfer rate.

| UTP Categories - Copper Cable | | | | |
|---|---|---|---|---|
| **UTP Category** | **Data Rate** | **Max. Length** | **Cable Type** | **Application** |
| **CAT1** | Up to 1Mbps | - | Twisted Pair | Old Telephone Cable |
| **CAT2** | Up to 4Mbps | - | Twisted Pair | Token Ring Networks |
| **CAT3** | Up to 10Mbps | 100m | Twisted Pair | Token Rink & 10BASE-T Ethernet |
| **CAT4** | Up to 16Mbps | 100m | Twisted Pair | Token Ring Networks |
| **CAT5** | Up to 100Mbps | 100m | Twisted Pair | Ethernet, FastEthernet, Token Ring |
| **CAT5e** | Up to 1 Gbps | 100m | Twisted Pair | Ethernet, FastEthernet, Gigabit Ethernet |
| **CAT6** | Up to 10Gbps | 100m | Twisted Pair | GigabitEthernet, 10G Ethernet (55 meters) |
| **CAT6a** | Up to 10Gbps | 100m | Twisted Pair | GigabitEthernet, 10G Ethernet (55 meters) |
| **CAT7** | Up to 10Gbps | 100m | Twisted Pair | GigabitEthernet, 10G Ethernet (100 meters) |

Firewall.cx
Routing Information & Expertise To Network Professionals

### 4.4.2 Shielded Twisted Pair Cable (STP)

This shielded twisted pair (STP) provides better performance at lower data rates. However, it is more expensive and more difficult to work with than unshielded twisted pair.
The term STP can include a number of different cable types which all include a shielding mechanism. Some cable types include a shield only between the different twisted pairs within the cable and others include various shielding types both around the pairs and the whole cable; the specifics will not be covered here. Figure 4.5 shows an example of an STP cable that has a shield between the pairs and the whole cable:

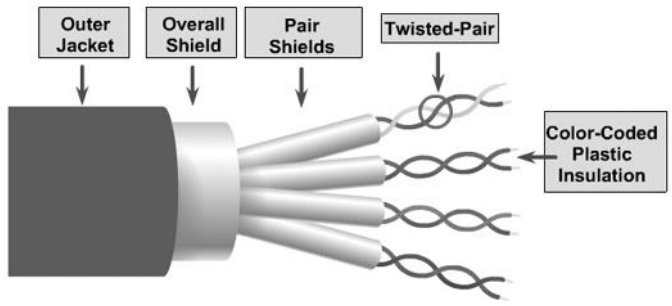



**Figure 4.5 Shielded twisted pair cable**

Shielded Twisted Pair (STP) is suitable for environments with electrical interference. STP cable has a metal foil or braded mesh to cover each pair of insulating conductors. This is known as the metal shield. It reduces the interference of the noise but makes the cable bulky and expensive. So, practically UTP is more used than STP.
The following summarizes the features of STP cable:

- Speed and throughput—10 to 100 Mbps
- Average cost per node—Moderately expensive

- Media and connector size—Medium to large
- Maximum cable length—100 m (short)

**4.5 Optical Fiber Cable**

Fiber-optic cables use optical fibers that carry digital data signals in the form of modulated pulses of light. An optical fiber is a thin (2 to 125 pm), flexible medium capable of conducting an optical ray. Various glasses and plastics can be used to make optical fibers.

An optical fiber cable has a cylindrical shape and consists of three concentric sections:

the core,

the cladding, and

the jacket (See Figure 4.6)

The *core* is the innermost section and consists of one or more very thin strands, or fibers, made of glass or plastic. Each fiber is surrounded by its own *cladding,* a glass or plastic coating that has optical properties different from those of the core. The outermost layer, surrounding one or a bundle of cladded fibers, is the *jacket.* The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers. There are two fibers per cable – one to transmit and one to receive.

It transmits light rather than electronic signals eliminating the problem of electrical interference.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

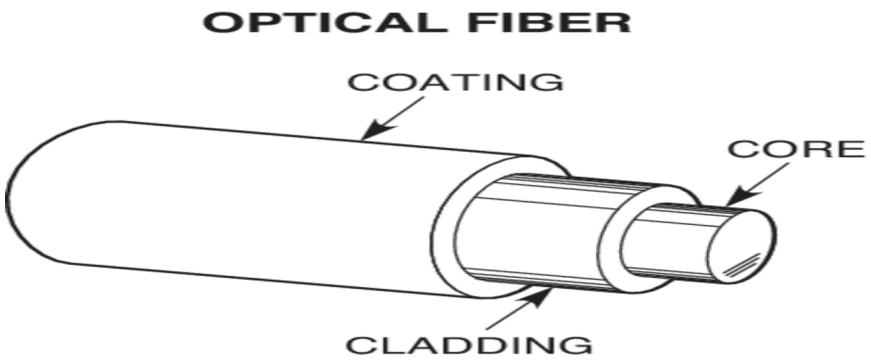



**Figure 4.6 optical fiber cable**

Fiber optic cable transmits light signals which are converted from electrical to light with the help of devices like Light Emitting Diodes (LEDs) or Light Amplification by Stimulated Emitted Radiations (LASERs). Each fiber has an inner core of glass or plastic that conducts light. The inner core is surrounded by *cladding*, a layer of glass or plastic that reflects the light back into the core instead of refraction. Figure 4.7 shows the path of a light.

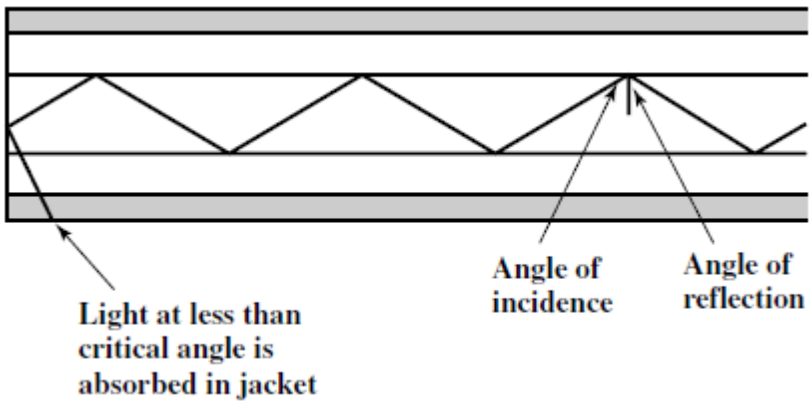



**Figure 4.7 Propagation of light in optical fibers**

The principle of optical fiber transmission is as follows. Light from a source enters the cylindrical glass or plastic core. Rays at shallow angles are reflected and propagated along the fiber; Other rays are absorbed by the surrounding material.
There are two types of fiber-optic cables:
single-mode fiber (SMF) and
multimode fiber (MMF).
A mode is defined as the angle at which a ray of light enters the core of the optical fiber cable. If the light enters the core at different angles, it is called multimode transmission.

**Multimode Fiber (MMF)** – Uses multiple rays of light (modes) simultaneously, with each ray of light running at different reflection angle to carry the transmission over short distances. MMF cables use a larger internal core diameter (typically, 50 µm or 62.5 µm) and can utilize lower cost LEDs for transmission. While the larger core diameter offers a cable that supports multiple modes and a cable that is easier to work with (light coming into the cable is allowed to come in at multiple angles). An LED is not a concentrated light source, and, therefore, the rays of the light beam disperse after traveling a certain distance through the fiber.

**Figure 4.8 Multimode transmission**

The disadvantages of multimode transmission are:

- For a given signal, the dispersed light beams arrive later than the un-dispersed ones, a delay which can result in slower transmission rates.
- The collision of light beams due to dispersion and reflection. These collisions weaken the signal strength, resulting in attenuation.

MMF cables are typically only used for connections that are less than 2 kilometers in length; this also makes it a very common cable in LAN deployments.

**Single-mode Fiber (SMF) –** Uses a single ray of light, known as a mode to carry the transmission over long distances. Like Multi-Mode Fiber (MMF), Single Mode Fibers (SMF) transmits signals via light and is not subject to electrical interference. The difference between SMF and MMF is in their physical characteristics; a MMF cable has a large core diameter

and is able to accept a number of different modes that come into the cable from multiple angles, SMF has a much smaller core diameter (typically 8-10 µm) and accepts signals coming in from a specific angle and on a specific mode. In single-mode transmission, an ILD (Injection Laser Diode) is used to emit a light beam (laser) that carries data. ILD is an extremely concentrated light source, and, therefore, the laser beams do not disperse when traveling through the fiber. As a result, all the light beams reach the destination at the same time. In addition, the beams do not collide, thereby preventing any attenuation of the light signals.

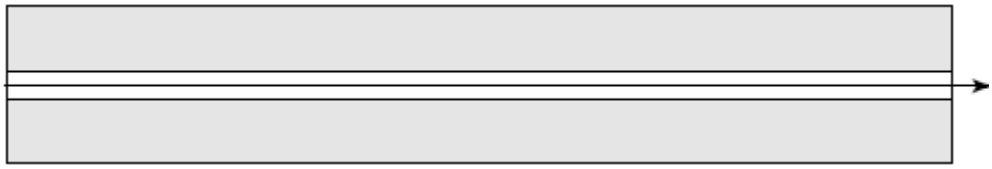


**Figure 4.9 Single mode transmission**

MMF is typically used for shorter cable runs (up to 2 km typically) and SMF can be used for cable runs of very long distances (typically up to ~40 miles without repeaters depending on wavelength).

### 4.6 LAN Connectors

Connectors act as interface between NIC of the computer and the  that transmits the signals. The type of connector depends on type of cable of used to connect computers or devices on the network.

### 4.6.1 Coaxial Cable Connectors

To connect coaxial cable to the device, we need coaxial cable connector. The most common type of connector used for coaxial cables is the Bayone-Neill-Concelman or BNC connectors. BNC connectors are available in three different forms:

1. BNC Cable Connector
2. BNC –T Connector
3. BNC Terminator

Figure 4.8 shows the various types of BNC connectors


**Figure 4.8 Coaxial Cable Connectors**

The BNC cable connector is either soldered or crimped to the end of a cable. The BNC connector is used to connect the coaxial cable to the T-connector, which is plugged into the NIC of the computer.  That is, the BNC-T connector is used in Ethernet networks for branching out a cable for connection to a computer or other devices. The BNC terminator is

used at the end of the cable to prevent the reflection of the signal. It absorbs or destroy any signals that are not received by the computers in the network.

### 4.6.2 Twisted Pair Cable Connectors

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See figure 4.9) attached to UTP cable. This type of connector resembles the older RJ11 connectors that most people are familiar with from wired telephones. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

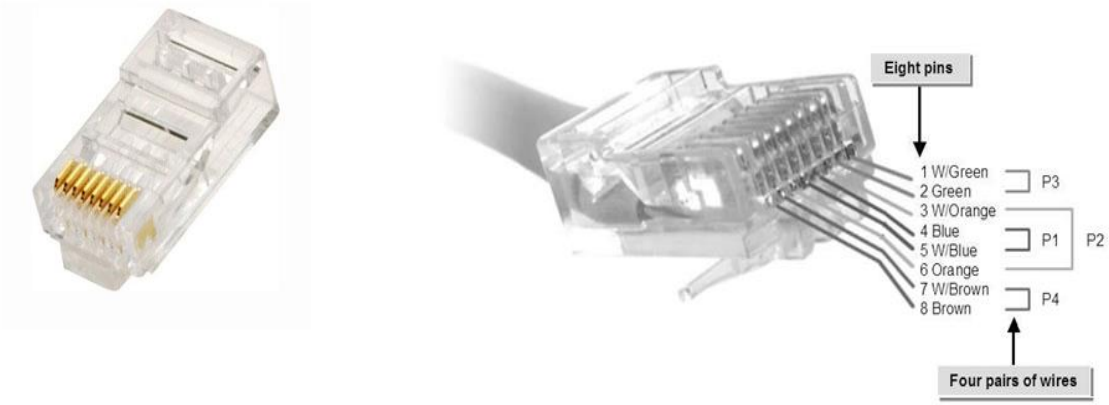



**Figure 4.9 RJ-45 connector**

The connector used on a UTP cable is called as RJ-45 (Registered Jack 45) connector. Below picture shows an RJ45 jack, attached to UTP cable. Eight color-coded wires inside Twisted-Pair cable is attached to eight pins in a RJ45 jack as shown above. Each wire in the Twisted Pair cable is crimped into 8 pins in the RJ45 jack.

To prepare a UTP network cable, it is necessary to crimp two RJ45 connectors as shown below.

**Figure 4.10 UTP network cable**

One end of the Unshielded Twisted Pair cable with RJ45 jack attached is plugged in to computer's Ethernet NIC card port and other end is plugged to the NIC card port of another

computer to connect only two computers or to the port in the hub have a network of more than two computers.

**Pinout for Ethernet**

Although used for a variety of purposes, the RJ-45 connector is probably most commonly used for 10Base-T and 100Base-TX Ethernet connections.

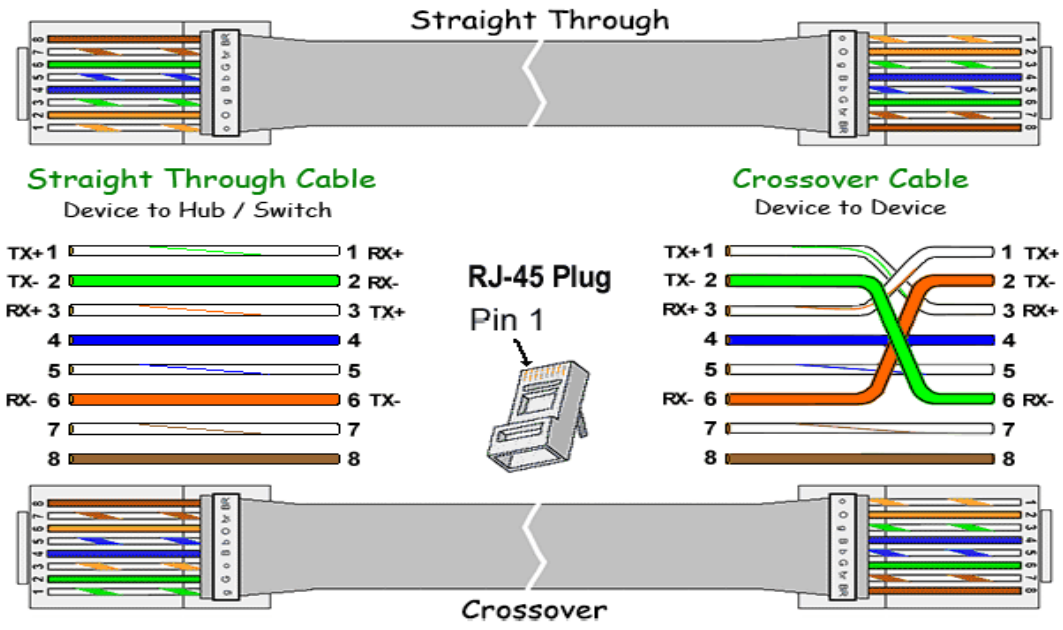
There are two types of cabling: straight-through cabling and crossover cabling. Straight-through cable is used for connecting a computer to the hub/switch. Whereas crossover cable is used for connecting two computers or two hubs/switches. Each cable requires two connectors.

**Straight-through Cable:**

| **Connector 1** | | **Connector 2** | |
|---|---|---|---|
| **Pin** | **Color** | **Pin** | **Color** |
| 1 | White/Green | 1 | White/Green |
| 2 | Green | 2 | Green |
| 3 | White/Orange | 3 | White/Green |
| 4 | Blue | 4 | Blue |
| 5 | White/Blue | 5 | White/Blue |
| 6 | Orange | 6 | Orange |
| 7 | White/Brown | 7 | White/Brown |

**Crossover Cable:**

| **Connector 1** | | **Connector 2** | |
|---|---|---|---|
| **Pin** | **Color** | **Pin** | **Color** |
| 1 | White/Green | 1 | White/ Orange |
| 2 | Green | 2 | Orange |
| 3 | White/Orange | 3 | White/Green |
| 4 | Blue | 4 | Blue |
| 5 | White/Blue | 5 | White/Blue |
| 6 | Orange | 6 | Green |
| 7 | White/Brown | 7 | White/Brown |




**4.6.3 Optical Fiber Connectors**

There are several types of fiber optic connectors available today. The most common are: ST, SC, FC, MT-RJ and LC style connectors. All of these types of connectors can be used with either multimode or singlemode fiber.

**Straight Tip (ST)**

The ST connector was one of the first connector types widely implemented in fiber optic networking applications. Originally developed by AT&T, it stands for Straight Tip connector. ST connections use a 2.5mm ferrule with a round plastic or metal body. Available in single-mode and multimode, the ST connector features reliable and durable field installation Figure 4.11below shows an example of a ST connector:

**Figure 4.11 Straight Tip (ST) Connector**

**Subscriber Connector (SC)**

SC connectors also use a round 2.5mm ferrule to hold a single fiber. They use a push-on/pull-off mating mechanism which is generally easier to use than the twist-style ST connector when in tight spaces. The connector body of an SC connector is square shaped, and two SC connectors are usually held together with a plastic clip (this is referred to as a duplex connection). The Subscriber Connector (SC) can be seen commonly on MMF or SMF. Figure 4.12 below shows an example of an SC connector:

**Figure 4.12 Subscriber Connector (SC)**

**Lucent Connector (LC)**

One popular Small Form Factor (SFF) connector is the LC type. This interface was developed by Lucent Technologies (hence, Lucent Connector). It uses a retaining tab mechanism, similar to a phone or RJ45 connector, and the connector body resembles the squarish shape of SC connector. LC connectors are normally held together in a duplex configuration with a plastic clip. The ferrule of an LC connector is 1.25mm. Unlike the SC and ST connectors, the LC connector is always duplex connecting a pair of fibers at a time. Figure 4.15 below shows an example of a LC connector:

**Figure 4.13 Lucent Connector (LC)**

**Multi-fiber Push On (MPO)**

The Multi-fiber Push On (MPO) connector is another duplex connector that offers an easy options for connection.. It is often also referred to as Multi-fiber Termination Push-on (MTP); the MTP connector is a brand name (US Conec). Figure 4.14 below shows an example of an MPO connector:

**Figure 4.14 Multi-fiber Push On (MPO) Connector**

**MU Connector**

The MU connector is designed for high-density connections. This small single-fiber connector has a high level of performance, providing more than double the packaging density of the SC connector. The following Figure 4.15 shows the MU connector.

**Figure 4.15 MU connector**

### 4.7 Comparison of Coaxial, Twisted pair, and Optical Fiber cables

| Sl No | Twisted pair cable | Co-axial cable | Optical fiber |
|---|---|---|---|
| 1 | Transmission of signals takes place in the electrical form over the metallic conducting wires | Transmission of signals takes place in the electrical form over the inner conductor of the cable | Signal transmission takes place in an optical form over a glass or plastic fiber |
| 2 | Noise immunity is low. Therefore more distortion | Higher noise immunity than the twisted pair cable due to the presence of shielding conductor | Higher noise immunity as the light rays are unaffected by the electrical noise |
| 3 | Affected due to external magnetic field | Less affected due to external magnetic field | Not affected by the external magnetic field |
| 4 | Short circuit between two conductors is possible | Short circuit between two conductors is possible | Short circuit is not possible |
| 5 | Cheapest | Moderately expensive | Expensive |
| 6 | Supports low data rates | Moderately high data rates | Very high data rates |
| 7 | Low bandwidth | Moderately high bandwidth | Very high bandwidth |
| 8 | Attenuation is very | Attenuation is low | Attenuation is very low |

| | | | |
|---|---|---|---|
| | high | | |
| 9 | Installation is easy | Installation is fairly easy | Installation is difficult |
| 10 | Electromagnetic interference (EMI) can take place | EMI is reduced due to shielding | EMI is not present |

**4.8 LAN Devices**

In previous sections, we learn about different types of cables that can be used to transmit data in the form of signals from one computer to another. However, the cables cannot transmit the signal beyond a certain distance. In addition, there may be multiple computers present in a network, and to connect these computers, we need a central concentrator. A concentrator is a device with two or more ports through which computers and devices can be connected. The following are the two main functions of a concentrator:

- To boost the signal to restore its original strength
- To provide an interface to connect multiple computers and devices in a network

**4.8.1 Repeaters**

Repeaters are used to increase the usable length of the cable. Repeaters amplify a weak signal so that the signal stays as strong as the original one. For example, consider a network in which two computers about 300m apart are connected with a coaxial cable. If one computer sends a signal to the other, the signal starts attenuating, and after distance of 185m, the signal strength falls to such an extent that the second computer may not receive a signal at all. In such cases, you can use a repeater every 185m between the computers to boost the signal.

Repeaters can also be used to connect two segments of the same network. Segments refer to logical sections of the same network. For example, suppose an organization has offices on the first floor and fifth floor of a building, and the computers on both the floors are connected in the same network. In this case, computers in the first floor form one segment, and the computers on the fifth floor form another segment. A repeater can be used on one of the intermediate floors to connect the segments.

Repeaters do not have any capability of directing network traffic or deciding what particular route that certain data should take, they are simply devices that sit on the network and boost the data signal that they receive. The problem with repeaters is that they amplify the entire signal that they receive, including any line noise.

Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay, which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. *Repeaters work at the physical layer of the Internet model*. The role of repeater is shown in Figure 4.16.

Repeaters were most commonly associated with coaxial network configurations. Because coaxial networks have now fallen out of favor, and because the functionality of repeaters has been built in to other devices, such as hubs and switches, repeaters are rarely used.

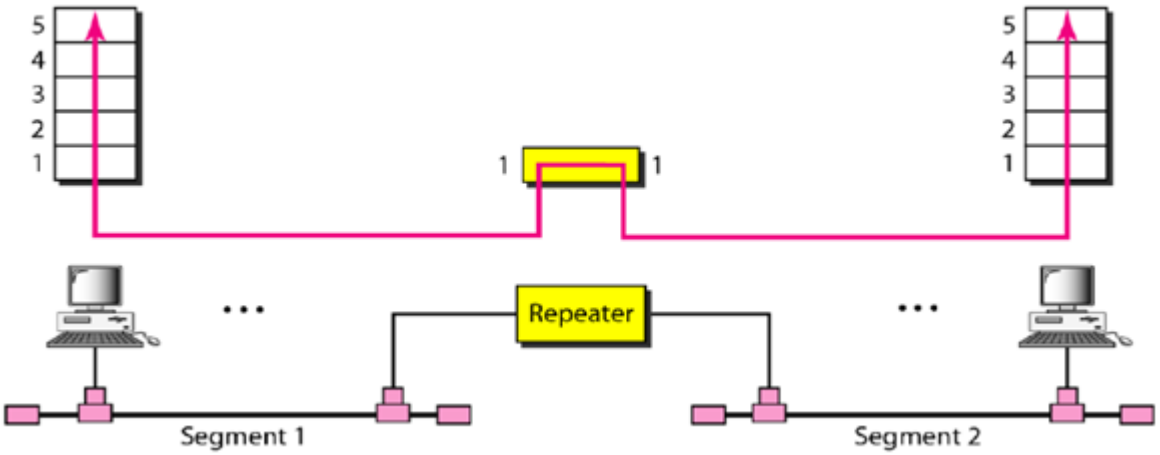



**Figure 4.16 A repeater connecting two segments of a LAN**

**4.8.2 Hubs**

A hub is like a repeater but with multiple ports. That is, a hub is simply a multiport repeater. There is usually no software to load, and no configuration required (i.e. network administrators don't have to tell the device what to do). Hubs operate very much the same way as a repeater. They amplify and propagate signals received out all ports, with the exception of the port from which the data arrived. A hub works at physical layer and hence connects networking devices physically together. Hubs are fundamentally used in networks that use **twisted pair cabling** to connect devices.

Hubs can be used to connect multiple segments of the same network and transfer data from one segment to another. Also, hubs are used to connect computers to a server in networks that use star topology. Figure 4.17 shows a typical hub used in LANs.

**Figure 5.17 Hub with 12 ports**

Based on their functions, hubs can be classified as follows:

- **Active Hubs -** Active hubs amplify/regenerate a signal before forwarding it to all the ports on the device, as does a different type of dedicated network device called a repeater. Active hubs require a power supply. Active hubs are the most common types of hubs used in networks. They are useful when the segments of the network are not close to one another and the signals require amplification.

- **Passive Hubs** – A passive hubs do not amplify/regenerate signals. They act as interface between two segments of a network or between two computers in a network.

A passive hub is used when the network is divided into multiple segments, but the segments are sufficiently close and the signals require no amplification.

- **Intelligent Hubs** – An intelligent hub is an active hub with additional features such as network monitoring capabilities. For example, an intelligent hub supporting Simple Network Management Protocol (SNMP) can provide information about such things as activity on each port. In addition, an intelligent hub can also be used to prevent unauthorized computers from connecting to the segments of the network. Active hubs are more expensive than passive hubs as they provide additional features.

Hubs do not read any of the data passing through them and are not aware of their source or destination. Regeneration of the signal aside, the basic function of a hub is to take data from one of the connected devices and forward it to all the other ports on the hub. This method of operation is inefficient because, in most cases, the data is intended for only one of the connected devices. You can see a representation of how a hub works in Figure 4.18.

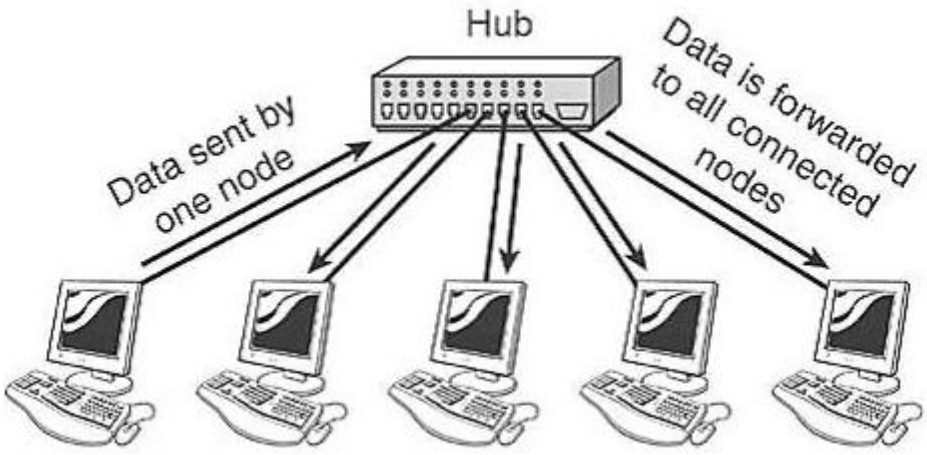



**Figure 4.18 How a hub works**

Due to the inefficiencies of the hub system and the constantly increasing demand for more bandwidth, hubs are slowly but surely being replaced with switches. If the hub is intended for a small network with very little traffic, this should not be a problem. However, if the network is large or expected to expand, a switch is a better option. Hubs run in only half duplex mode.

### 4.8.3 Switches

Like hubs, switches also connect computers in a network or different segments of the same network. Unlike hubs, which work at the physical layer, switches work at the data link layer of the OSI reference model. Therefore, switches treat data in the form of frames and not as signals, which is the case with physical layer devices like hubs. Figure 4.19 shows an example of a 32-port Ethernet switch.

**Figure 4.19 A 32-port Ethernet Switch**

Just as in hub, devices in switches are connected to ports through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. Hub works by sending the data to all the ports on the device whereas a switch transfers it only to that port which is connected to the destination device as shown in Figure 4.20. A switch does so by having an in-built learning of the MAC address of the devices connected to it. A *MAC address* is a unique number that is stamped into every NIC. By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically. In effect, the switch literally channels (or *switches*, if you prefer) data between the ports. For this purpose, switches maintain a list of MAC addresses and the port number associated with each MAC address.

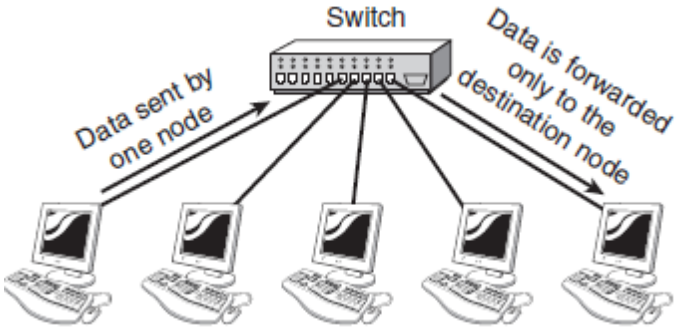



**Figure 4.20 How a switch works**

The following methods are used to transmit data via switches:

- **Cut-through transmission**: It allows the packets to be forwarded as soon as they are received. The switch reads the destination MAC address of a data frame and immediately forwards the frame to the respective port.
- **Store and forward**: In this switching environment all the data frames are received and 'checked' for integrity and errors before being forwarded ahead. If the frames are found error free, the switch forwards them to the respective port. If the frames are corrupt, they are not forwarded to the destination, and the source device has to resend the frames. The errors are thus eliminated before being propagated further. The downside of this process is that error checking takes relatively longer time consequently making it a bit slower in processing and delivering.

Depending on the requirements of the network, one can select an appropriate method of switching. For example, if the speed of network is the primary concern, you can select cut-through switching. Most switches have the ability to select an appropriate switching method depending on the network conditions. Initially, the switch uses cut-through switching, but if it finds that the number of corrupt data frames is high, it automatically selects store and forward switching. After sometime, if the switch observes that the number of corrupt data frames is lower, the switch reverts back to cut-through switching. This is called as auto switching.

### 4.8.4 Network Interface Cards (NICs)

Network Interface Cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus.

Many NIC adapters comply with plug-and-play specifications. On these systems, NICs are automatically configured without user intervention, while on non-plug-and-play systems, configuration is done manually through a set-up program and/or DIP switches.

NICs work at both the data link layer and physical layers of the OSI reference model. At the data link layer, NIC converts the data packets into data frames and adds the MAC address to the data frame. At the physical layer, it is responsible for converting the data into signals, and transmitting them across the communication medium. A MAC address is a unique hardware number present on the NIC and is specified by the NIC manufacturer. MAC addresses are globally unique.

When a computer needs to send data, the NIC receives data packets from the computer, converts them into data frames, and passes them across the cable as signals. The role of NIC in most PC environments can be divided into the following tasks:

- **Host-to-card communication** – The NIC communicates with the computer using IRQ (Interrupt Request) and receives data present in the memory of the computer for transmission.
- **Buffering** – The data received from the computer is not immediately transmitted. Instead, all the data is buffered, or stored temporarily on the NIC before transmission. Buffering ensures that the NIC has the complete data packet before converting it into frames, thus preventing incomplete data transmissions.
- **Frame Creation** – Once the NIC has all the data that needs to be transmitted, it divides the data into frames. A frame has three parts: header, data, and trailer. The header contains the source and destination MAC addresses; the data part contains the actual data being transmitted across the network; and the trailer contains error checking information such as Cyclic Redundancy Check (CRC).
- **Parallel-to-Serial conversion** – The NIC receives data from the computer in parallel form. For example, a PCI card receives 32 or 64 bits simultaneously. The number of bits depends on the motherboard bus architecture. However, the data must be converted into serial form because LANs generally transmit data bit after bit, and not multiple bits at a time.
- **Encoding** – The serial bits are converted into electrical signals for transmission across the cable.

After performing these tasks, the NIC accesses the cable and transmits the signals.

Unlike other network devices such as hubs or switches, that perform independently, the performance of NIC depends on the configuration of the computer. The following factors affect the performance of an NIC.

- **Bus speed** – The type of an expansion slot on the motherboard determines the bus speed. For example, ISA slots work at a speed of 8 or 16 KBps, whereas PCI slots have a speed of 32 or 64 KBps. Therefore, a PCI network card offers better performance than an ISA network card.
- **Memory** – Memory affects the overall performance of a computer to an extent. Therefore, NICs on computers with more memory perform better than those on computers with less memory.
- **Memory access Methods** – The NIC can access the main memory using different methods such as Direct Memory Access(DMA) or Input/Output (I/O). In I/O, the NIC requests the information from the main memory. This request should be accepted by the processor, and then the NIC can access the data. In DMA, the DMA controller present on the motherboard allows the NIC to access the main memory directly. Therefore, NICs that use DMA are faster than NICs that use I/O.

### 4.9 Wireless LANs (WLANs)

WLANs as the name suggests, do not use a physical medium to connect computers and devices on the network. Instead, wireless media such as radio and infrared signals are used. Therefore, in a WLAN, the computers or devices have an infrared port or an NIC that supports wireless communication. The popular technologies used for wireless communication are radio waves, infrared and Bluetooth. Multiple computers in a WLAN are connected with the help of an Access Point (AP). An AP performs the same function as the hub as shown in Figure 4.21.

*Wireless access points*, referred to as either *WAPs* or *wireless APs*, are a transmitter and receiver
(*transceiver*) device used for wireless LAN (WLAN) radio signals. A WAP is typically a separate network device with a built-in antenna, transmitter, and adapter. WAPs use the wireless
infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. WAPs also typically have several ports allowing a way to expand the network to support additional clients. Each WAP is limited by a transmissions range, the distance a client can be from a WAP and still get a useable signal. The actual distance depends on the wireless standard being used and the obstructions and environmental conditions between the client and the WAP.

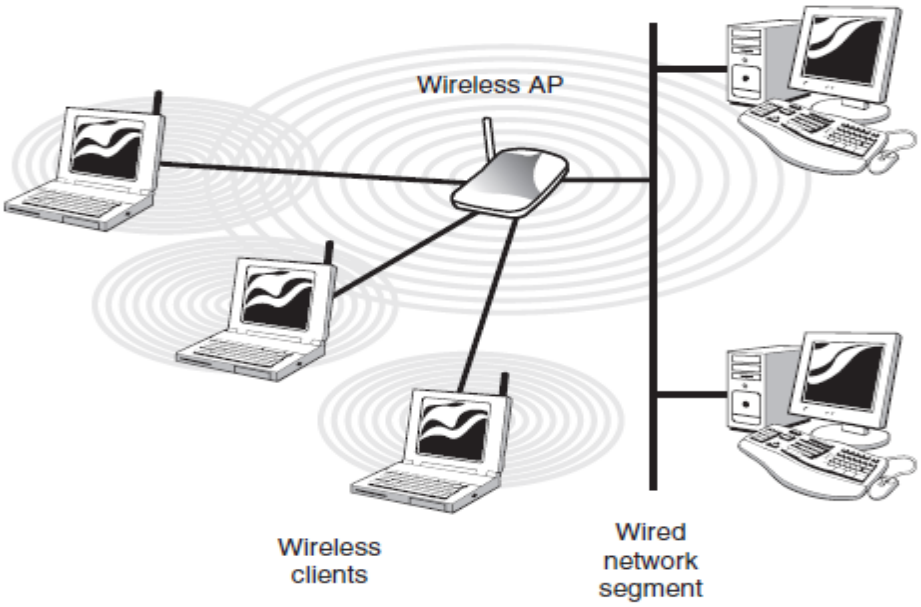



**Figure 4.21 WLAN using a WAP**

An access point (AP) performs the following three functions:

- Receives data frames from computers and devices connected to it.
- Buffers the data frames and checks their integrity.
- Transmits the data frames to the destination computer or device.

WLANs were first developed in the early 1990s. WLANs offer the following benefits over conventional LANs that use physical connectivity:

- **Resistance to EMI/RFI** – WLANs use radio or infrared waves to transmit data and are therefore resistant to signal attenuation and distortion due to EMI and RFI.
- **Easy Installation** – The absence of physical media to connect computers greatly reduce the time required to install a LAN. Also, the time required to configure the

devices and APs is nearly the same as that required to configure computers in a conventional LAN.

- **Mobility** – The absence of physical connectivity provides users the flexibility to move computers and devices within the network. This is helpful for employees who may need to access up-to-date data in meetings and conferences.
- **Flexibility** – WLANs can connect computers and devices in areas where cabling is not possible. For example, in factories that have heavy machinery, UTP cables cannot be used because they are prone to EMI. A WLAN can be implemented in such cases.
- **Expansion** – A conventional LAN can be expanded with the help of an WAP. Most WAPs support transfer of data between a conventional LAN and a WLAN. Therefore, LANs can be expanded to accommodate more computers without incurring any additional cabling cost.

Due to these advantages, WLANs are very popular. The common use of WLANs is in the following areas.

- **Home users** – Most home users are not comfortable with installation of cables. WLANs provide an easy way to connect multiple devices and setup a home network.
- **General access** – Nowadays, travelling employees of organizations need to access their corporate network from places such as airport, a hotel, or an auditorium hall. Most of these buildings are built without a provision for connecting computers. It is not practical to provide connectivity by installing cables in such locations. As a result, WLANs are preferred.
- **WAN connectivity** – Wireless technologies such as radio waves, infrared waves, and microwave are popular options to connect LANs in situations where connectivity options such as leased lines or ISDN are not available.

### 4.10 LAN Protocols

In a LAN, there are multiple computers that need to communicate with one another. For example, consider the network shown in Figure 4.22 in which computer are connected by using a switch.

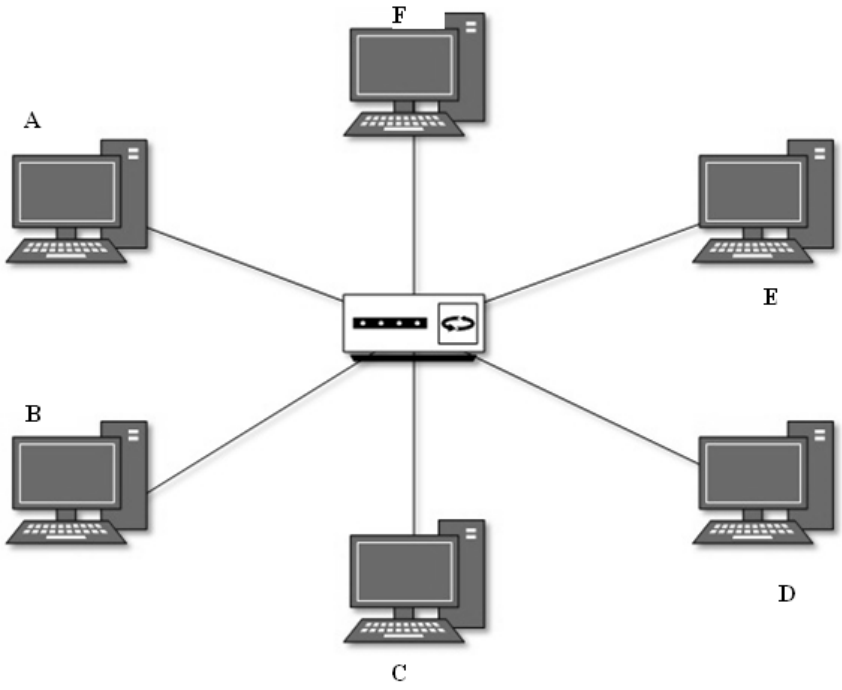



Figure 4.22 Network using a switch

A network protocol is defined as the set of rules or communication formats for exchanging information over a network. Both sender and receiver must agree upon a protocol. Without a protocol, two devices may be connected but not communicating. In other words, protocol is a standard procedure and format that two data communication devices must understand, accept and use to be able to talk to each other. Network protocols mainly define the following aspects of communication.

- Addressing method used by the devices – For example, in Figure 4.23, the computers can address each other by their names or by the address assigned to each computer. Node A can be addressed as 1, node B as 2, node C as 3 and so on.
- Data format – Computers and devices on a network should send and receive data in a format that can be understood by one another.
- Reliability of data transfer – Network protocols ensure that data transfers on a network are reliable.
- Speed of communication – Network protocols play an important role in determining the speed of data transfer on the network.

As network protocols need to perform multiple tasks, it is practically impossible to develop a single protocol that can manage all these tasks. Therefore, different protocols have been defined to operate at various layers of the OSI reference modelBased on the layers at which the protocols operate, network protocols are broadly classified as :

- Lower layer protocols
- Middle layer protocols
- Higher layer protocols

### 4.11.1 Lower Layer Protocols

Lower layer protocols operate at the physical and data link layers of the OSI reference model and perform the following tasks.

- Transmitting data between two devices on a network
- Ensuring that data transmission between devices is error free

Note that ensuring that the data transmission is error free is not an essential function of a lower layer protocol. Transmission errors are usually detected and corrected at the transport layer. However, most lower layer protocols used in LANs include the ability to detect transmission errors.

Following are the common lower layer protocols used in LANs.

- ARCnet
- Ethernet
- Token Ring
- Fiber Distributed Data Interface (FDDI)

**4.11.1.1 ARCnet**

ARCnet or Attached Resource Computer Network is one of the oldest lower layer protocols used in LANs. ARCnet was developed by principal development engineer John Murphy at Datapoint Corporation in 1976 and announced in 1977 ARCnet used to support data transmission rate up to 2.5 Mbps. Latere, however, ARCnet supported speeds of up to 10 Mbps.

Each device on an ARCnet network is assigned a *node number*. This number must be unique on

each network and in the range of 1 to 255.

ARCnet uses the token passing scheme to provide media access to the devices on the network. The LAN server continuously circulates empty message frames on a medium . When a device wants to send a message, it inserts a "token" (this can be as simple as setting a token bit to 1) in an empty frame in which it also inserts the message. When the destination device or LAN server reads the message, it resets the token to 0 so that the frame can be reused by any other device. The scheme is very efficient when traffic increases since all devices are afforded the same opportunity to use the shared network.

The token (permission to speak on the network) is passed from the lowest number node to higher number nodes in ascending order. Lower numbered addresses get the token before the higher numbered addresses.

The frame format used by ARCnet to transmit data can be broadly divided into the following three parts:

- Header – Contains information about the source and destination nodes
- Data – Contains information about the size of data and the actual data
- Trailer – Contains Cyclic Redundancy Checks (CRC) for error detection

The following Figure 5.24 shows different parts of an ARCnet DATA frame.

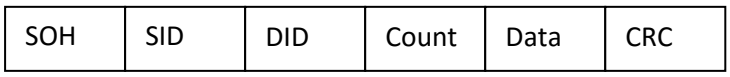



Figure 4.23 ARCnet DATA Frame

The header consists of three components: SOH (Start Of Header), SID (Source ID), and DID (Destination ID). To a destination device, the SOH includes the beginning of the header. The SID contains the address of the source device, whereas the DID contains the address of the destination device.

Data part consists of two components, Count and Data. The Count component contains information about the size of data while the Data component contains the actual information to be transmitted. The destination devices use the information in the Count field to check whether the entire data is received.

The trailer consists of CRCs to detect any errors encountered during the transmission. If errors are detected, the destination computer sends a negative acknowledgement frame to the source node. A negative acknowledgement (NACK) frame indicates that the data received was corrupt. The source node resends the frame until it receives an acknowledgement (ACK) frame indicating correct receipt of data in response.
Following are the main features of ARCnet:

- ARCnet supports coaxial and twisted pair cables as well as optical fiber cables.
- ARCnet supports the star, bus, and ring topologies. Depending on the requirement of the network, an appropriate topology can be selected, thereby optimizing cable lengths.
- ARCnet uses token passing mechanism, which prevents collisionson the network. As a result, there is no loss of data due to collisions.

**Disadvantages of ARCnet:**

- The maximum frame size supported by ARCnet is 508 bytes. Therefore, multiple data frames need to be generated if the amount of data to be transferred is large. For example, to transfer a 20 KB file, ARCnet generates approximately 40 frames.
- ARCnet requires an ACK frame in response to every data frame. If the amount of data transferred is large, the number of ACK frames is also high, resulting in an increased network traffic. In addition, the time required for a data transfer increases because the source node releases the token only after it receives the ACK frames for all data frames sent.
- The maximum number of nodes supported in a single ARCnet LAN is 255.
- ARCnet supports a maximum data transfer speed of 10 Mbps.

The disadvantages of ARCnet severely affect the network performance if the amount of data transferred is high. Therefore, newer protocols such as Ethernet and Token Ring are preferred over ARCnet.

**4.11.1.2 Ethernet**

Ethernet is the most popular lower layer protocol used in LANs. Ethernet is a family of technologies that provides data-link and physical specifications for controlling access to a shared network medium. It has emerged as the dominant technology used in LAN networking. Ethernet was originally developed by Xerox Palo Alto Research (PARC) in the 1970s and operated at 2.94Mbps. The original 802.3 Ethernet operated at 10Mbps, and successfully supplanted competing LAN technologies, such as Token Ring. Ethernet was initially designed to run over coaxial cables, but a typical Ethernet LAN now uses special grades of twisted pair cables, or fiber optical cabling.
Ethernet has several benefits over other LAN technologies:

- Simple to install and manage
- Inexpensive
- Flexible and scalable
- Easy to interoperate between vendors

**CSMA/CD and Half-Duplex Communication**

Ethernet was originally developed to support a **shared media** environment.This allowed two or more hosts to use the same physical network medium. There are two methods of communication on a shared physical medium:

- **Half-Duplex –** hosts can transmit or receive, but *not simultaneously*

- **Full-Duplex –** hosts can both transmit and receive simultaneously

On a half-duplex connection, Ethernet utilizes **Carrier Sense Multiple Access with Collision Detect (CSMA/CD)** to control media access. *Carrier sense* specifies that a host will monitor the physical link, to determine whether a *carrier* (or *signal)* is currently being transmitted. The host will *only* transmit a frame if the link is **idle**, and the Interframe Gap has expired. If two hosts transmit a frame simultaneously, a **collision** will occur. This renders the collided frames unreadable. Once a collision is detected, both hosts will send a **32-bit jam sequence** to ensure all transmitting hosts are aware of the collision. The collided frames are also discarded. Both devices will then wait a *random* amount of time before resending their respective frames, to reduce the likelihood of another collision. This is controlled by a **backoff** timer process.

**Full-Duplex Communication**

Unlike half-duplex, **full-duplex** Ethernet supports simultaneously communication by providing separate transmit and receive paths. This effectively *doubles* the throughput of a network interface. Full-duplex Ethernet was formalized in IEEE 802.3x, and *does not use CSMA/CD* or slot times. Collisions should *never* occur on a functional full-duplex link. Greater distances are supported when using full-duplex over half-duplex.

Full-duplex is only supported on a point-to-point connection between two devices. Thus, a bus topology using coax cable *does not* support full-duplex.

Only a connection **between two hosts** or between **a host and a *switch*** supports full-duplex. A host connected to a *hub* is limited to half-duplex. Both hubs and half-duplex communication are mostly deprecated in modern networks.

**Ethernet Communication**

In Ethernet LANs, the source node sends data to all the nodes on the network and not only to the destination node. This process is called as *broadcasting*. All the nodes check the destination MAC address on the data frame. The device with the corresponding MAC address accepts the data while the other devices ignore it.

Figure 4.24 shows the process of broadcasting in an Ethernet network.

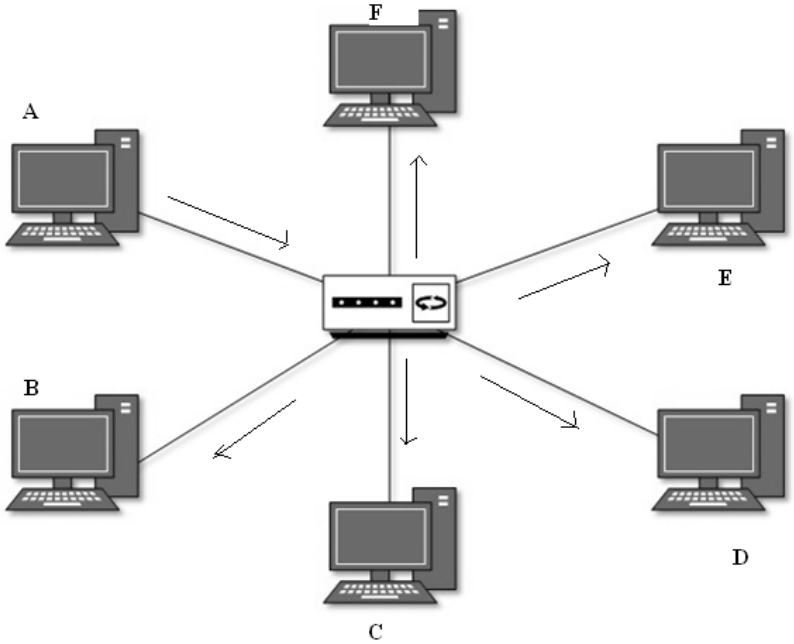



Figure 4.24 Data frames broadcast in Ethernet

In the above figure, node A needs to send data to node B. Node A creates a data frame and includes the destination MAC address of node B in the frame and broadcasts the frame across

the network. All the nodes check the destination MAC address of the data frame. As the destination MAC address corresponds to node B, only node B accepts the data.

**Categories of Ethernet**

The original 802.3 Ethernet standard has evolved over time, supporting faster transmission rates, longer distances, and newer hardware technologies. These *revisions* or *amendments* are identified by the letter appended to the standard, such as 802.3*u* or 802.3*z*.

Major categories of Ethernet have also been organized by their speed:

- **Ethernet** (10Mbps)
- **Fast Ethernet** (100Mbps)
- **Gigabit Ethernet**
- **10 Gigabit Ethernet**

The *physical* standards for Ethernet are often labeled by their transmission rate, signaling type, and media type. For example, *100baseT* represents the following:

- The first part (*100*) represents the transmission rate, in Mbps.
- The second part (*base)* indicates that it is a baseband transmission.
- The last part (*T)* represents the physical media type (*twisted-pair)*.

Ethernet communication is **baseband**, which dedicates the entire capacity of the medium to one signal or channel. In **broadband**, multiple signals or channels can share the same link, through the use of *modulation* (usually frequency modulation).

**Ethernet (10 Mbps)**

Ethernet is now a somewhat generic term, describing the entire family of technologies. However, Ethernet traditionally referred to the original 802.3 standard, which operated at **10 Mbps**. Ethernet supports coax, twisted-pair, and fiber cabling. Ethernet over twisted-pair uses **two** of the four pairs. Both 10baseT and 10baseF support full-duplex operation, effectively doubling the bandwidth to 20 Mbps.

**Fast Ethernet (100 Mbps)**

In 1995, the IEEE formalized **802.3u**, a **100 Mbps** revision of Ethernet that became known as **Fast Ethernet.** Fast Ethernet supports both twisted-pair copper and fiber cabling, and supports both half-duplex and full-duplex.

100baseT4 was never widely implemented, and only supported half-duplex operation. 100baseTX is the dominant Fast Ethernet physical standard. 100baseTX uses **two** of the four pairs in a twisted-pair cable, and requires Category 5 cable for reliable performance.

Fast Ethernet is backwards-compatible with the original Ethernet standard. A device that supports both Ethernet and Fast Ethernet is often referred to as a *10/100* device.

**Gigabit Ethernet**

Gigabit Ethernet operates at 1000 Mbps, and supports both twisted-pair **(802.3ab)** and fiber cabling **(802.3z)**. Gigabit over twisted-pair uses **all four pairs**, and requires Category 5e cable for reliable performance. Gigabit Ethernet is backwards-compatible with the original Ethernet and Fast Ethernet. A device that supports all three is often referred to as a 10/100/1000 device. Gigabit Ethernet supports both half-duplex or full-duplex operation. Full-duplex Gigabit Ethernet effectively provides 2000 Mbps of throughput. In modern network equipment, Gigabit Ethernet has replaced both Ethernet and Fast Ethernet.

**10 Gigabit Ethernet**

10 Gigabit Ethernet operates at 10000 Mbps, and supports both twisted-pair **(802.3an)** and fiber cabling **(802.3ae)**. 10 Gigabit over twisted-pair uses **all four pairs**, and requires Category 6 cable for reliable performance. 10 Gigabit Ethernet is usually used for high-speed connectivity within a datacenter, and is predominantly deployed over fiber.

Ethernet is the most popular protocol used in LAN for the following reasons:

- Supports coaxial, twisted –pair, and optical fiber cables.
- Supports bus and star network topologies.
- Easy to install, maintain, troubleshoot and expand
- Costs less to setup than ARCnet, Token Ring or FDDI LANs.
- In most LANs, devices need to transmit data intermittently and not on a continuous basis. The CSMA/CD method of providing media access is best suited for this situation.
- Newer standards such as Fast Ethernet and Gigabit Ethernet can be used on network where speed is important

Following are the .disadvantages of Ethernet:

- It is impossible to predict the exact amount of time a node needs to wait before it can start transmitting data. Therefore, Ethernet cannot be used in LANs where the delays can be predicted.
- Nodes in an Ethernet LAN broadcast data across network, resulting in an increase of network traffic. In networks with a large number of computers, broadcasting significantly increases the network traffic. The network needs to be divided into multiple broadcast domains to overcome this issue. This issue is usually overcome with the help of switches for interconnecting nodes and segments.
- Priority bases communication is not possible.

### 4.11.2 Token Ring

Token ring local area network (LAN) technology is a communications protocol for local area networks. It uses a special three-byte frame called a "token" that travels around a logical "ring" of workstations or servers. This token passing is a channel access method providing fair access for all stations, and eliminating the collisions of contention-based access methods.
Token Ring, although not as widely used as Ethernet, is still a very popular networking technology. Like ARCnet, Token Ring also uses the token passing scheme to provide media access to the network devices. Token passing is a Media Access Control, or MAC, protocol which determines how stations transmit data to the network and when they can do so. It is a very "low level" protocol built in to every Token Ring device and operates automatically, with no user setup or intervention required.
A token passing network operates in the following manner. One station on the network generates a special frame called a token and transmits it to the network. The network is an electrical ring and the next node receives the token. If that station has any data to transmit, it does not repeat the token, but begins sending its data instead. The station may continue to transmit data until a timer called a Token Holding Timer expires. This timer begins when the token is captured, and when it expires, the station must stop sending data and send a new token to the network. The next station in the ring will see the token, and either capture it and send its own data or it may simply repeat the token. The process continues until the token has made a complete trip around the ring.

Every Token Ring network is built in a star wired ring topology. The network is physically wired with all nodes connecting to a device called a Multistation Access Unit (MSAU) in a star topology. The MSAUs are connected together in a ring topology. Figure 4.25 shows the physical layout of a Token Ring network.

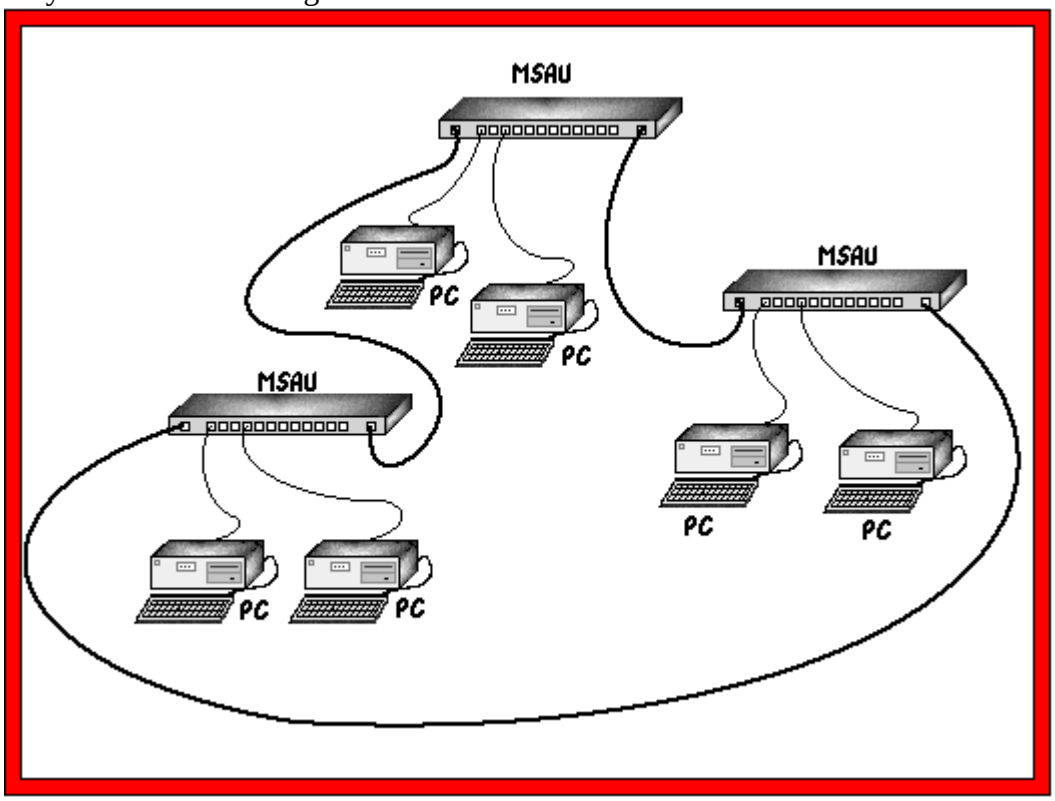
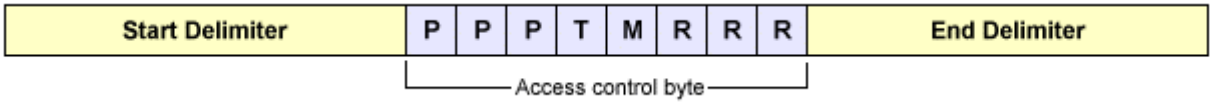



**Figure 4.25 Token Ring Physical Topology**

Token Ring networks provide a priority system that allows administrators to designate specific stations as having a higher priority than others, allowing those stations to use the network more frequently by setting the priority level of the token so that only stations with the same priority or higher can use the token (or reserve the token for future use).

**Token Ring Frame Format**

Two basic frame types are used - tokens, and data/command frames. The token is three bytes long and consists of a *start delimiter(one byte)* , an *access control byte*, and an *end delimiter(bne byte)*. The format of the token is shown below.




- **Start delimiter** – Indicates the beginning of the token.
- **Access Control Field** – Defines the access of devices to the tokens. This field in turn contains other fields. Access Control Format is:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| P | P | P | T | M | R | R | R |

**P=Priority field**

Priority Bits indicate tokens priority, and therefore, which devices are allowed to use it. Device can transmit if its priority is at least as high as that of the token. Contains a value between 000 and 111 which is set by the device that releases the token in the

network.

**T=Token field (**T = 0 for Token, T = 1 for data Frame) When a device with a Frame to transmit detects a token which has a priority equal to or less than the Frame to be transmitted, it may change the token to a start-of-frame (1) sequence and transmit the Frame.

**M=Monitor field**

The monitor bit is used to prevent a token whose priority is greater than 0 or any frame from continuously circulating on the ring. If an active monitor detects a frame or a high priority token with the monitor bit equal to 1, the frame or token is aborted. This bit shall be transmitted as 0 in all frame and tokens. The active monitor inspects and modifies this bit. All other stations shall repeat this bit as received.

**R =Request Priority field**

On a network there may be devices that may to send high priority information. Such devices can use this field to get faster access to the token. A device can change the Request Priority field to its priority value and inform the device that is releasing the token to increase the value of the Priority field to equal to its priority. Thus, intermediate devices with lower priority cannot use this token.

- **Ending Delimiter:** Indicates the end of delimiter.

**Data Frame Format**

The basic format of a Token Ring data frame is shown in Figure 4.26 and described in the table that follows.

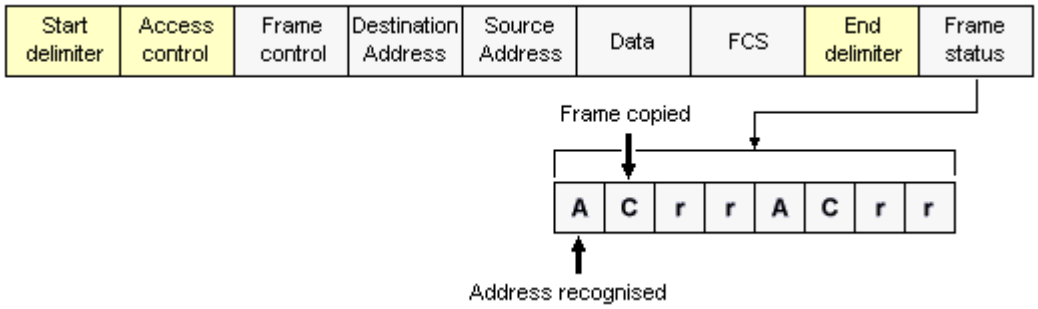



Figure 4.26 Token Ring Data Frame

| Frame field | Description |
|---|---|
| Start delimiter | Indicates start of the frame |
| Access control | Indicates the frame's priority and whether it is a token or a data frame |
| Frame control | Contains either Media Access Control information for all computers or "end station" information for only one computer |
| Destination address | Indicates the address of the computer to receive the frame |
| Source address | Indicates the computer that sent the frame |
| Information, or data | Contains the data being sent |
| Frame check sequence | Contains CRC error-checking information |
| End delimiter | Indicates the end of the frame |
| Frame status | Tells whether the frame was recognized, copied, or whether the destination address was available |

**Fault Management and Tolerance**

Fault management refers to the techniques used to monitor and troubleshoot networks, and fault tolerance refers to the ability of the network to function smoothly in spite of faults such as device or link failures. In token Ring LANs, fault management and fault tolerance are accomplished by designing a computer as an active monitor. The first computer to come online is assigned by the Token Ring system to monitor network activity. The monitoring computer makes sure that frames are being delivered and received correctly. It does this by checking for frames that have circulated the ring more than once and ensuring that only one token is on the network at a time. Usually frames circulate on the network more than once when the device that has to accept the frames fails.

In addition to an active monitor, Token Ring LAN also have a standby monitor. The standby monitor continuously checks whether the Active monitor is working correctly. If it detects that the Active monitor has failed, the standby monitor performs the functions of the Active monitor. The active monitor and Standby monitor perform fault management in a Token Ring LAN. Fault tolerance, is achieved with the help of a process called *beaconing.*

The process of monitoring is called *beaconing*. To understand the process of beaconing, consider the Token Ring LAN shown in Figure 4.27.

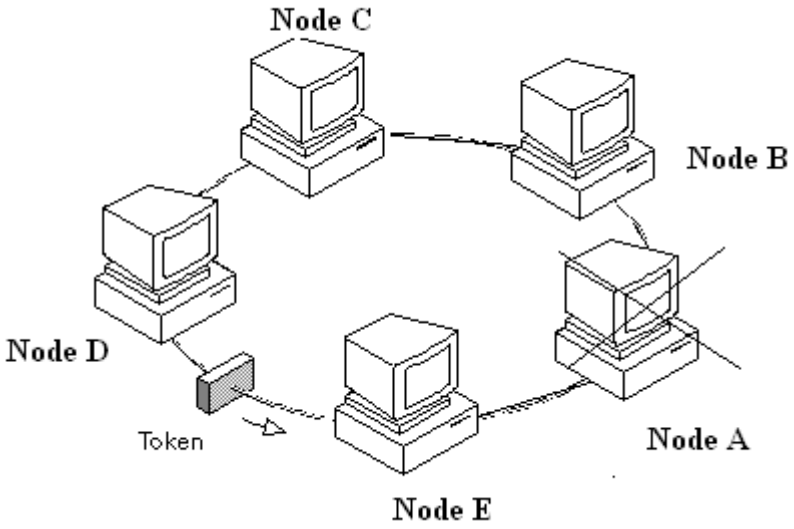



**Figure 4.27 Token Ring LAN**

If Node A fails, any frames addressed to Node A continue to circulate on the network because Node A is not available to accept the frame. The frame circulates on the network more than once, and is therefore, detected by the Active monitor. The Active monitor first checks the integrity of the data frame to make sure that the frame is not corrupted. It then checks the destination address and interprets that Node A is not available to accept data. The active monitor sends a beacon frame containing the information about the device failure to all the devices on the network.

From this information, the ring attempts to diagnose the problem and make a repair without disrupting the entire network resulting in autoreconfiguration.

Autoreconfiguration is a process by which devices on the network eliminate the malfunctioning device and form a ring as shown in Figure 4.28

Devices that receive a beacon frame perform diagnostic procedures and attempt to reconfigure the network around the failed areas. Much of this reconfiguration process can be handled internally by the MSAU. The MSAU contains relays that switch a computer into the ring when it is turned on, or out of the ring when the computer is powered off. A MSAU has a number of ports to which network devices can be connected, a *ring-out* port allowing the

unit to be connected to another MSAU, and a *ring-in port* that can accept an incoming connection from another MSAU. A number of MSAUs can thus be connected together in daisy-chain fashion to create a larger network. The ring-out port of the last MSAU in the chain must be connected back to the ring-in port of the first MSAU.

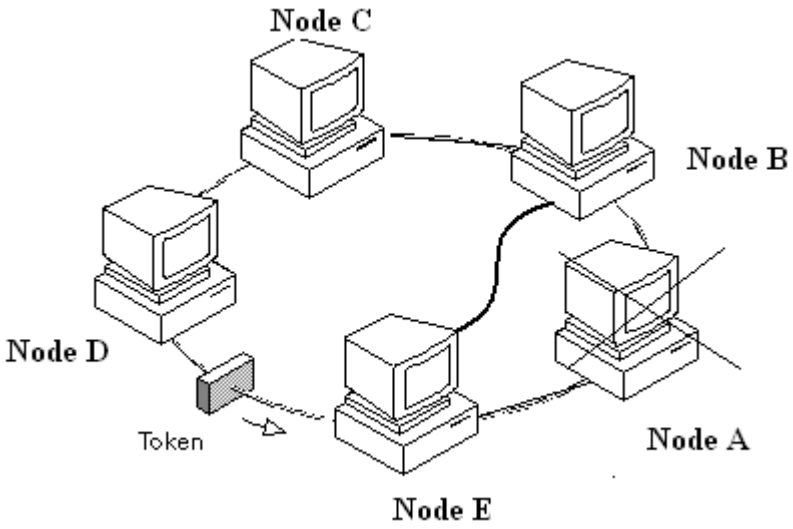



**Figure 4.28 Autoreconfiguration after device failure**

In a pure token-passing network, a computer that fails stops the token from continuing. This in turn brings down the network. MSAUs were designed to detect when a NIC fails, and to disconnect from it. This procedure bypasses the failed computer so that the token can continue on.

**Advantages of Token Ring**

- Token Ring networks are deterministic in nature.
- Token Ring employs fault tolerance systems and is therefore, extremely resistant to device failures

**Disadvantages of Token Ring**

- The cost of setting up a Token Ring LAN is higher than that for an Ethernet LAN.
- Token Ring LANs are more difficult to install and maintain than Ethernet LANs.
- The maximum speed offered by Token Ring LAN is 16 Mbps, compared to 1000 Mbps offered by Ethernet.
  https://www.youtube.com/watch?v=qeTSiGHPNDQ

### 4.11.3 Fiber Distributed Data Interface (FDDI)

FDDI stands for Fiber Distributed Data Interface. FDDI is a 100 Mbps LAN technology which can run over fiber optic. It is the oldest 100 Mbps network type commonly available, and is widely used as a backbone technology to interconnect several smaller Ethernet or Token Ring networks. The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users. FDDI is frequently used on the backbone for a wide area network (WAN).

The FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles).

FDDI uses a dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating). The dual-rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. The primary purpose of the dual rings, as will be discussed in detail later in this chapter, is to provide superior reliability and robustness. Figure 4.29 shows the counter-rotating primary and secondary FDDI rings

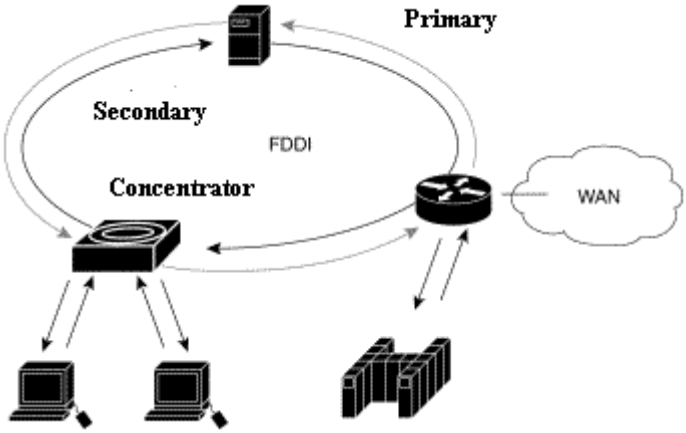



Figure 4.29 FDDI LAN

https://www.youtube.com/watch?v=Ltt4R_TtAqA

There are two main ways of interconnecting nodes in an FDDI network. The first way is called Single Attachment Station, or SAS for short. The other is called Dual Attached Station, or DAS.

- **Single Attachment Station (SAS )**
  A Single Attachment Station (SAS) FDDI network consists of each node having only one cable connecting it to a concentrator. Each node only connects to the primary ring in this configuration, and operation at 200 Mbps is not possible. The concentrator handles any situation where the primary ring needs to be wrapped back to the secondary ring.

- **Dual Attachment Station (DAS )**
  A Dual Attachment Station (DAS) FDDI network consists of each node having two connections. These connections can be node to node, both between one node and one concentrator, or one node to two concentrators.

Following are the advantages of FDDI:

- **High Speed And Deterministic Technology**
- **Long Distance**
- **Fault Tolerance**
- **Management**
- **Flexibility**

The disadvantages of FDDI are:

- **Cost**
  FDDI equipment costs more than other 100 Mbps network technologies. This is due to the complexity of the token passing protocol and certain royalties which must be paid for every piece of equipment manufactured.

### 4.12 Middle Layer Protocols

Middle layer protocols are network protocols that operate at the network and transport layers of the OSI reference model. Middle layer protocols are responsible for ensuring reliable transfer of data between two devices on a network. The transport layer protocols ensure reliable delivery of data whereas the network layer protocols are responsible for correct addressing of the data.

The common middle layer protocols used in LAN are:

- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)
- NetBios Enhanced User Interface (NETBEUI)

In this section, the TCP/IP protocol is covered. The other two are out of this syllabus.

### 4.12.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

TCP/IP reference model was developed based on the operation of the different protocols that are part of TCP/IP protocol suite. TCP/IP protocol suite or the Internet protocol suite is a set of communications protocols which is used on the Internet and similar networks. It is referred to as TCP/IP because of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). Those two protocols were the first networking protocols defined in this standard. The TCP/IP protocol suite has five abstraction layers (in contrast to OSI model which has 7), each with its own protocols. From highest to lowest the layers are:

- **Application layer** – handles application-based interaction on a process-to-process level between communicating Internet hosts
- **Transport layer** – handles host-to-host communication
- **Internet layer** – connects different networks
- **Link layer** – Provides a framing service to the Internet layer
- **Physical layer -** Provides an electrical signal bit transmission service to the network

At the Internet layer, TCP/IP contains protocols that are responsible for addressing data, converting the data into packets, and routing the data packets. The protocols that operate at this layer are:

- **IP (Internet Protocol)** – IP is responsible for addressing of sender and receiver on the network and routing the packets to the destination. Every computer on the network has to have its own unique address known as the IP address. Every packet sent will contain an IP address showing where it is supposed to go. A packet may go through a number of computer routers before arriving at its final destination and IP controls the process of getting everything to the designated computer. IP as a protocol is responsible for the following:
    - Fragmenting of IP datagrams if the Network Interface layer MTU demands it
    - Reassembly of IP fragments
    - Making the IP datagram routing decision
- **Address Resolution Protocol (ARP)** – Translates the network address of a computer to a MAC address.
- **Internet Control Message Protocol (ICMP)** – Provides diagnostic capabilities such as error reporting and delivery conditions for the data packets, it defines a small number of messages used for diagnostic and management purposes.

- **Internet Group Management Protocol (IGMP)** – Used when a single data packet needs to be sent to computers located in different networks. . IGMP allows us to take a single message and send it out to multiple hosts throughout the network

The transport layer is responsible for ensuring reliable delivery of data from source device to a destination device. TCP/IP consists of the following protocols at the transport layer.

- **Transmission Control Protocol (TCP)** – TCP provides a connection-oriented, guaranteed, reliable transport service. A connection oriented protocol responsible for sequencing and acknowledgement of the data packets. Connection oriented means that two hosts - one a client, the other a server - must establish a connection before any data can be transferred between them. On the sender side, TCP breaks the data into multiple packets and sent it to the destination. These packets may not be sent in correct sequence. On the receiver side, TCP ensures that the packets are assembled in correct sequence before passing them to the higher layer. In addition, TCP requires an acknowledgement from the destination device for data that has been sent. This ensures reliability and integrity of data during transmission. It also ensures that no packets got lost in transmission. TCP provides reliability. An application that uses TCP knows that data it sends is received at the other end, and that it is received correctly. TCP uses checksums on both headers and data. When data is received, TCP sends an acknowledgement back to the sender. If the sender does not receive an acknowledgement within a certain timeframe the data is re-sent. It also implements flow control, so a sender cannot overwhelm a receiver with data."
- **User Datagram Protocol** – A connectionless protocol less reliable than TCP. This protocol is used together with IP when small amount of data are to be transferred. It is simpler than TCP and lacks the flow control and error recovery functions of TCP. A unit of data sent using UDP is called a datagram.

The application layer protocols provide the user with an interface to access the services of other layers in the TCP/IP reference model. The most common application layer protocols are:
Hyper Text Transport Protocol (HTTP),
File Transport Protocol (FTP),
Simple Mail Transfer Protocol (SMTP),
Simple Network Management Protocol (SNMP )and
Telnet.

https://www.youtube.com/watch?v=QyYqruaoKKo

**4.13 Higher Layer Protocols**

Higher layer protocols operate at the session, presentation and application layers of the OSI reference model. The higher layer protocols provide users with an interface to access network data and resources. The common higher layer protocols used are: HTTP,FTP, SMTP, and IMAP.

**4.13.1 Hyper Text Transfer Protocol (HTTP)**

Hypertext Transfer Protocol (HTTP) is a method used to transfer information on the World Wide Web. HTTP protocol works in a client and server model like many other protocols. A web browser using which a request is initiated is called as a client and a web server software which respond's to that request is called as a server. HTTP is a request/response protocol between clients and servers. The protocol actually identifies how the browser submits a request to the

server that holds the website, and how the server formats that data to return it back to the browser, and then how the browser displays the information. HTTP can be described as an information requesting and responding protocol. HTTP uses port number 80 by default and predominately uses TCP as the transport protocol, although it can use UDP also.

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote 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 a status line, such as "HTTP/1.1 200 OK", and a message of its own, the body of which is perhaps the requested file, an error message, or some other information.

Resources to be accessed by HTTP are identified using Uniform Resource Locators (URLs) using the http:// or https:// schemes.

### 4.13.2 File Transfer Protocol (FTP)

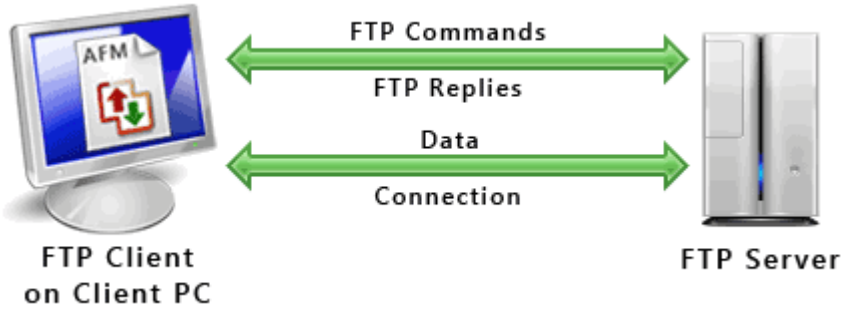
File transfers over the Internet use special techniques, of which one of the oldest and most widely-used is FTP. FTP, short for "File Transfer Protocol," can transfer files between any computers that have an Internet connection, and also works between computers using totally different operating systems.

Transferring files from a client computer to a server computer is called "uploading" and transferring from a server to a client is "downloading".

The File Transfer Protocol allows a user to transfer files between local and remote host computers. FTP (File Transfer Protocol), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

FTP can transfer both binary and text files, including HTML, to another host. FTP URLs are preceded by ftp:// followed by the DNS name of the FTP server. To log in to an FTP server, use ftp://username@servername.

FTP uses one connection for commands and the other for sending and receiving data. FTP has a standard port number on which the FTP server "listens" for connections. A port is a "logical connection point" for communicating using the Internet Protocol (IP). The standard port number used by FTP servers is 21 and is used only for sending commands. Since port 21 is used exclusively for sending commands, this port is referred to as a command port. For example, to get a list of folders and files present on the FTP server, the FTP Client issues a "LIST" command. The FTP server then sends a list of all folders and files back to the FTP Client. So what about the internet connection used to send and receive data? The port that is used for transferring data is referred to as a data port (usually 20).




https://www.youtube.com/watch?v=hiQrYptlZ08

**4.13.3 SMTP (Simple Mail Transfer Protocol)**

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving Email. SMTP is used between email servers and clients on each end that need to send mail. SMTP is used by email clients to send mail to the mail server. Then it's used between mail servers to send mail from one server to the next. SMTP uses TCP transport protocol on port 25.

However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or IMAP that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending E-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server.

POP and IMAP (Internet Mail Access Protocol) deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet. You send e-mail with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP.

**4.13.4 Post Office Protocol (POP)**

POP is short for **P***ost* **O***ffice* **P***rotocol*, a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an *e-mail client*) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

POP, which is an abbreviation for Post Office Protocol, is the widespread method of receiving email. Much like the physical version of a post office clerk, POP receives and holds email for an individual until they pick it up. And, much as the post office does not make copies of the mail it receives, when an individual downloaded email from the server into their email program, there were no more copies of the email on the server; POP automatically deleted them.

POP makes it easy for anyone to check their email from any computer in the world, provided they have configured their email program properly to work with the protocol.

There are two versions of POP. The first, called *POP2*, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP

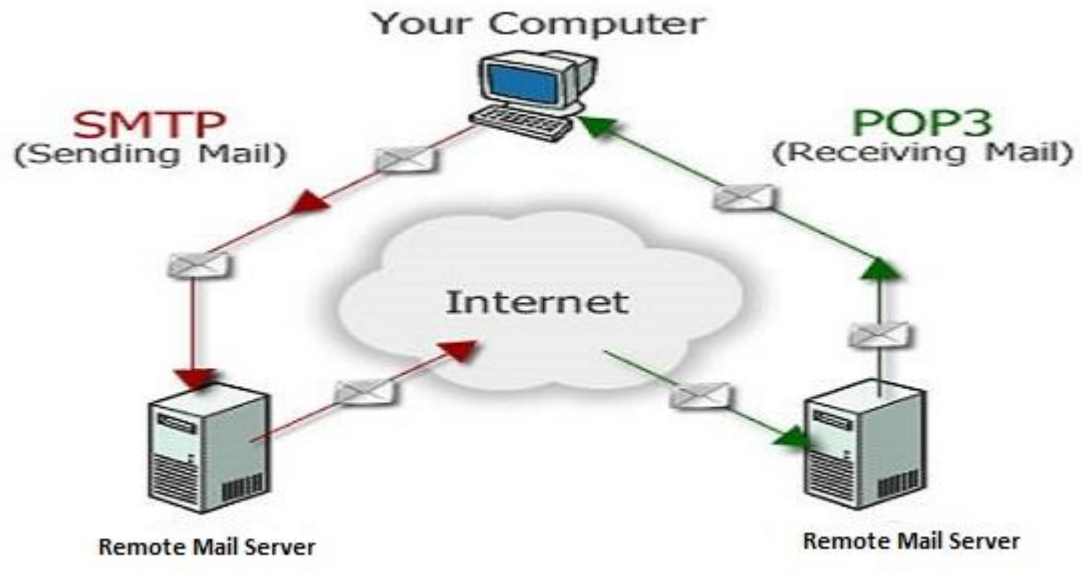
Normally, messages are downloaded to your computer and then deleted from the mail server. The mil retrieved from the server is stored on the local computer and can be accessed any number of times in the future. Retrieving emails from the mail server and storing them on the local computer offers the following advantages:

- The emails can be organized according to the preferences of the users, thereby facilitating easy retrieval in future.
- Mailboxes present on the servers usually have limited storage space typically 1 MB or 5 MB. The server handles multiple mail boxes. Leaving all the mails on the server may take up a significant disk storage space on the server. This problem can be solved by continually retrieving mails from the server.
- POP downloads the emails onto the local computer and therefore the user need not remain connected to the mail server to read the messages. The ability to read and modify mails without remaining connected to the internet is the main advantage.

POP, however has the following disadvantages:

- POP was designed for, and works best in, the situation where you use only a single computer to access your email.
- If you choose to work with your POP mail on more than one machine, you may have trouble with email messages getting downloaded on one machine that you need to work with from another machine; for example, you may need a message at work that was downloaded to your machine at home.
- You have to take care of your own backups of the mail downloaded to your computer. Unless you backup your mail frequently and regularly, this increases your risk of losing email due to hard disk problems, computer theft, etc.
- POP uses five default folders to handle emails: Inbox, Outbox, Drafts, Sent Items, and Deleted. POP does not allow users to create any customized folders for sorting email messages on the mail server.
- If you choose the POP option 'keep mail on server', your POP 'inbox' can grow large and unwieldy, and email operations can become inefficient and time-consuming.
- POP does not allow to search emails.

The functions of the SMTP and POP3 are shown in the following figure.



https://www.youtube.com/watch?v=1MZPSIU9Bf8

### 4.13.5 Internet Mail Access Protocol (IMAP)

As its name implies, IMAP allows you to access your email messages wherever you are; much of the time, it is accessed via the Internet. Basically, email messages are stored on servers. Whenever you check your inbox, your email client contacts the server to connect you with your messages. When you read an email message using IMAP, you aren't actually downloading or storing it on your computer; instead, you are reading it off of the server. As a result, it's possible to check your email from several different computers without missing a thing.

IMAP is an alternative to POP3 (Post Office Protocol 3), works in some fundamentally different ways, and makes a few fundamentally different assumptions.

Unlike POP, IMAP allows you to access, organize, read and sort your email messages without having to download them first. As a result, IMAP is very fast and efficient. The server also keeps a record of all of the messages that you send, allowing you to access your sent messages from anywhere. IMAP does not move messages from the server to your computer; instead, it copies the messages if you download them. It synchronizes the email that's on your computer with the email that's on the server. If the user has downloaded and modified emails, synchronizing ensures that the emails on the server also contain updated information.

IMAP allows users to access email messages from the mail server in any of the following modes:

- Online – The email messages exist on the mail server and the user can access mails from a remote computer.
- Offline – The user downloads email messages from the server to the local computer and the email messages are deleted from the server.
- Disconnected – The user downloads the messages from the server to the local computer. However, a copy of the messages is retained on the server. Every time the user connects to the server, the messages on the server are synchronized with the messages on the local computer.

**Advantages of IMAP**

There are several advantages to using IMAP.

- It allows you to access your email messages from anywhere, via as many different computers as you want.
- It only downloads a message when you click on it. As a result, you do not have to wait for all of your new messages to download from the server before you can read them.
- Attachments are not automatically downloaded with IMAP. As a result, you're able to check your messages a lot more quickly and have greater control over which attachments are opened.
- IMAP can be used offline just like POP - you can basically enjoy the benefits of both protocols in one.
- IMAP enables the users to search the e-mails.

**Disadvantages of IMAP**

- Using the online mode to access email messages my use a considerable amount of disk space on the mail server.

- IMAP is useful only if the user needs to access emails from multiple locations. If only a single computer is used, the advantages of IMAP are not felt.

**IMAP versus POP**

If you think that IMAP and POP are interchangeable, think again. POP works by contacting your email server and downloading all of your new messages from it. Once they are downloaded, they disappear from the server. If you decide to check your email from a different device, the messages that have been downloaded previously will not be available to you. POP works fine for those who generally only check their email messages from a single device; those who travel or need to access their email from various devices are much better off with IMAP-based email service.

**Review Questions**

1. List the devices used in LAN.
2. Explain the coaxial cable used in networking with a diagram
3. Differentiate thinnet nd thicknet coaxial cables
4. Differentiate UTP and STP.
5. Explain different categories of UTP cables available for networking
6. Explain STP cable with its advantages over UTP
7. Write a note on OFC
8. List different coaxial cable connectors
9. Explain connectors used with twisted pair cables
10. List different connectors used with optical fiber cable
11. Explain the role of repeater in LAN
12. Define Hub? Where is it used?
13. List and explain different types of hubs
14. Differentiate hub and switch
15. What is NIC? Define its role in LAN.
16. Explain functions of NIC
17. Explain working of WLAN
18. Bring out advantages of WLAN over LAN
19. Define a protocol
20. List lower layer protocols
21. List the main features of ARCnet
22. List the disadvantages of ARCnet
23. What is Ethernet protocol?
24. Explain Ethernet communication
25. Explain Ethernet categories
26. What are the advantages of Token Ring over Ethernet?
27. Explain fault management and tolerance in Token Ring
28. Explain working of Token Ring
29. List advantages and disadvantages of Token Ring
30. Explain working of FDDI
31. List the advantages of FDDI
32. Explain the functions of TCP and IP protocols
33. Write a note on http
34. Differentiate between http and https
35. Explain FTP

36. Explain the role of SMTP and POP in email messaging
37. Differentiate POP and IMAP

## Objective Questions:

1. Coaxial cables are widely used on
   A telephone networks
   B cable TV networks
   C broadband networks
   D none of these above

   Answer: Option [B]

2. The effective bandwidth of a signal is the
   A width of the spectrum
   B width of range of frequencies
   C band of frequencies containing most of the energy in the signal
   D width of the channel

   Answer: Option [C]

3. Twisting of wire reduces
   A interference
   B impulse noise
   C low frequency interference
   D none of these above

   Answer: Option [C]

4. The transmission of digital signal at the original frequency without modulation is called

   A baseband signaling
   B broadband signaling
   C digital signaling
   D none of these

   Answer: Option [A]

5. Which of the following transmission is concerned with content of the data ?
   A Analog transmission
   B Digital transmission
   C Both analog and digital transmission
   D None of these above

   Answer: Option [B]

6. The loss of power a signal suffers as it travels from the transmitting computer to a receiving computer is :

A. Echo
B. Jitter
C. Spiking
D. Attenuation

Answer: Option [D]

7. An effective way to prevent attenuation is :
A adding repeaters or amplifiers to a circuit
B compressing a circuit
C shielding wires
D none of these above

Answer: Option [A]

8. The core of an optical fiber has a
A. Lower refracted index than air
B. Lower refractive index than the cladding
C. Higher refractive index than the cladding
D. Similar refractive index with the cladding

Answer: Option [C]

9. Which of the following cabling techniques is considered best between buildings for establishing LANs ?
A 10Base5
B 10Base-F
C 10Base2
D None of these

Answer: Option [B]

10. Connector that is used for connecting cable to networking devices is called
A. Subscriber channel (SC).
B. Straight-tip (ST).
C. MT-RJ.
D. None of them.

Answer: Option [B]

11. Most common unshielded twisted pair connector is
A. RG-45.
B. RG-59.
C. RG-58.
D. RG-ll
Answer: Option [A]

12. Twisted pair cable in which metal casing improves penetration of noise or crosstalk is called
A. Fiber optic cable.
B. Shielded twisted pair cable.

C. Unshielded twisted pair cable.
D. Microwave.

Answer: Option [B]

13. Optical Fibers use reflection to guide light through a
A. Channel.
B. Metal.
C. Light.
D. Plastic.

Answer: Option [A]

14. Super High frequency (SHF) is used in
A. FM radio.
B. Satellite communication.
C. AM radio.
D. Cellular phones.

Answer: Option [B]

15. 1000Base-LX has used two wires for long wave are
A.STP Cable.
B. UTP Cable.
C. Fiber Optic.
D. Coaxial Cable.

Answer: Option [A]

16. Protocol Data Unit (PDU) is similar to
A. LLC.
B. HDLC.
C. MAC.
D. DSAP.

Answer: Option [B]

17. Terms that control flow and errors in full duplex switched Ethernet is called
A. LLC Sub layer.
B. MAC Sub layer.
C. LLC Control Layer.
D. MAC Control Layer.

Answer: Option [D]

18. NIC stands for
A. Network Interface Card.
B. National interface code.
C. Network international card.
D. Network international code.

Answer: Option [A]

19. Simple mail transfer protocol (SMTP) utilizes ____ as the transport layer protocol for electronic mail transfer.

A. TCP
B. UDP
C. DCCP
D. SCTP

Answer: Option [A]

20. SMTP connections secured by SSL are known as

A. SMTPS
B. SSMTP
C. SNMP
D . None of the mentioned

Answer: Option [A]

# UNIT- 5: Network Addressing

## 5.1 Introduction

Each computer on the network has an address that is unique within the network. Any computer that is willing to sent the data to the another device that includes the address of the Destination computer, this is sent to all the computer on the networks. The computer whose address matches with the destination address of data accepts the data while all other devices ignore it. If the destination address of the data does not match with the address of any computer on the network, it is forwarded usually with the help of Router to a different network where a computer with a destination address exits. The middle layer protocols uses on the network are responsible for providing a unique address to each computer on the network

https://sites.google.com/site/cprorgrams https://sites.google.com/site/cprorgrams

## 5.2 TCP/IP Addressing Scheme:

TCP/IP uses a 32 bit addressing scheme to identify the devices on a network. These 32 bits are divided into four octets, of eight bits each. Each of these four octets is represented in a decimal form, and separated by a dot.

For example, 198.172.168.10 is an IP address. This format of representing IP address is called the dotted decimal format.

The octets in an IP address can take a decimal value from 9 to 255 because the largest decimal value that can be represented by eight binary bits is 255(11111111 in binary).

For example, the 32 bit binary address 11000110.10101100.1010100.0001010 represents the IP address 198.172.168.10.

The addressing provided by a network layer protocol to a device is called its network address.

For example, 198.172.168.10 is the network address of a device. This is different from the MAC address which is the hardware address of the NIC or the device (routers or switch). The network addresses in a TCP/IP network are also known as IP addresses. Therefore, 198.172.168.10 is also known as the IP address.

## 5.3 Components of IP Address:

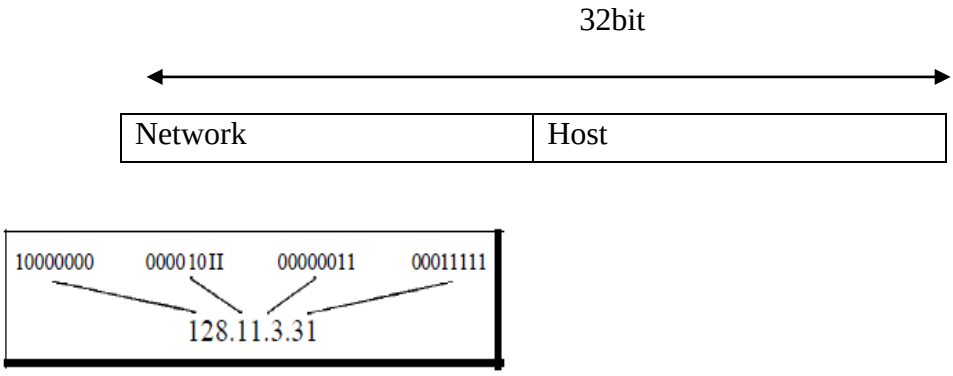
For continence sake we use IP address dotted-decimal notation, while the computer converts this into binary. However, even though these sets of 32 bits are considered a single “entity”, they have an internal structure containing two components:

1. **Network Address (Network ID):** A certain number of bits, starting from the left-most bit, is used to identify the network where the host or other network interface is located.

This is also sometimes called the network prefix or even just the prefix. This is the address of the network itself, and is used by other networks to identify this network.

2. **Host Address (Host ID):** The remainder of the bits is used to identify the host on the network. This is the address of the device with in the network.

The fundamental division of the bits of an IP address is into a network ID and host ID. Here, the network ID is 8 bits long and the host ID is 24 bits in length.




### 5.4 IP Addressing Classes

The IP header has 32 bits assigned for addressing a desired device on the network. An IP address is a unique identifier used to locate a device on the IP network. To make the system scalable, the address structure is subdivided into the *network* ID and the *host* ID. The network ID identifies the network the device belongs to; the host ID identifies the device. This implies that all devices belonging to the same network have a single network ID. Based on the bit positioning assigned to the network ID and the host ID, the IP address is further subdivided into classes A, B, C, D (multicast), and E (reserved), as shown in Figure 5.2

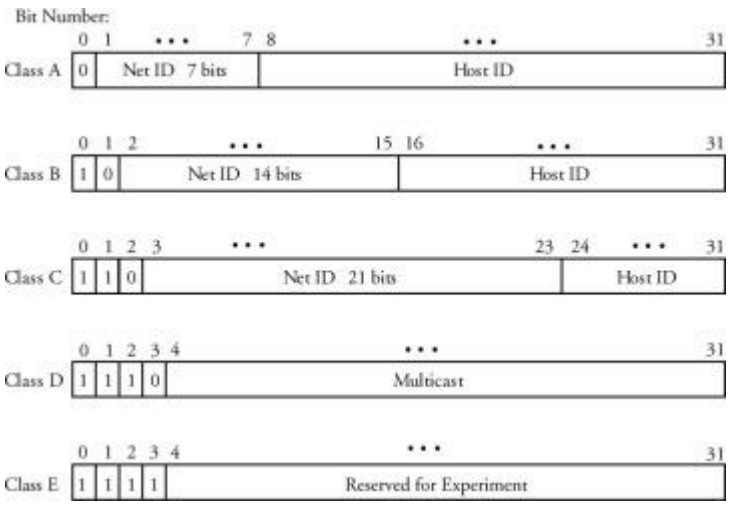



Figure 5.2 Classes of IP addresses

Consider the lengths of corresponding fields for each class shown in this figure:

Class A starts with 0 followed by 7 bits of network ID and 24 bits of host ID.

Class B starts with 10 followed by 14 bits of network ID and 16 bits of host ID.

Class C starts with 110 followed by 21 bits of network ID and 8 bits of host ID.

Class D starts with 1110 followed by 28 bits. Class D is used only for multicast addressing by which a group of hosts form a multicast group and each group requires a multicast address. Chapter 6 is entirely dedicated to multicast techniques and routing.

Class E starts with 1111 followed by 28 bits. Class E is reserved for network experiments only.

For ease of use, the IP address is represented in *dot-decimal* notation. The address is grouped into four dot-separated bytes. For example, an IP address with 32 bits of all 0s can be shown by a dot-decimal form of 0.0.0.0 where each 0 is the representation of 00000000 in a logic bit format.

Table 1.1 Comparison of IP addressing schemes

| Class | Bits to Start | Size of Network ID Field | Size of Host ID Field | Number of Available Network Addresses | Number of Available Host Addresses per Network | Start Address | End Address |
|---|---|---|---|---|---|---|---|
| A | 0 | 7 | 24 | 126 | 16,777,214 | 0.0.0.0 | 127.255.255.255 |
| B | 10 | 14 | 16 | 16,382 | 65,534 | 128.0.0.0 | 191.255.255.255 |
| c | 110 | 21 | 8 | 2,097,150 | 254 | 192.0.0.0 | 223.255.255.255 |
| D | 1110 | N/A | N/A | N/A | N/A | 224.0.0.0 | 239.255.255.255 |
| E | 1111 | N/A | N/A | N/A | N/A | 240.0.0.0 | 255.255.255.255 |

Example. A host has an IP address of 10001000 11100101 11001001 00010000. Find the class and decimal equivalence of the IP address.

**IP CLASSES**

Class A

Class A addresses always have the first bit of their IP addresses set to "0". Since Class A networks have an 8-bit network mask, the use of a leading zero leaves only 7 bits for the network portion of the address, allowing for a maximum of 128 possible network numbers, ranging from 0.0.0.0 – 127.0.0.0. Number 127.x.x.x is reserved for loopback, used for internal testing on the local machine.

Class B

Class B addresses always have the first bit set to "1" and their second bit set to "0". Since Class B addresses have a 16-bit network mask, the use of a leading "10" bit-pattern leaves 14 bits for the network portion of the address, allowing for a maximum of 16,384 networks, ranging from 128.0.0.0 – 181.255.0.0.

Class C

Class C addresses have their first two bits set to "1" and their third bit set to "0". Since Class C addresses have a 24-bit network mask, this leaves 21 bits for the network portion of the address, allowing for a maximum of 2,097,152 network addresses, ranging from 192.0.0.0 – 223.255.255.0.

Class D

Class D addresses are used for multicasting applications. Class D addresses have their first three bits set to "1" and their fourth bit set to "0". Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address space, since all the hosts within a group share the group's IP address for receiver purposes.

Class E

Class E addresses are defined as experimental and are reserved for future testing purposes. They have never been documented or utilized in a standard way.

### 5.5 Limitations of IP Address classes

The limitations of IP address classes are

1**. Inefficient use of address space**: A large number IP addresses are wasted because of using IP address classes The existence of only three address class(Class A, Class B, Class C) leads to waste of IP address space. It means that there are too few choices in the sizes of networks available. The gaps between the sizes of enormous, and the sizes don't match with the organizations requirement in the real world

2. **Poor network performance**: The IP address classes provide the flexibility of selecting a class depending on the number of computers, the performance of the network goes down if all the computers are connected to the same network

3. **Decreased router performance**: if the number of computers on a networks is more the routing table will become large. More and more entries are required for routers to handle the routing of packets, which causes performance problems for routers. The larger these tables, the more time it takes for routers to make routing decisions.

4. **Difficult to administer**: Since Class A and Class B supports huge number of host for network this leads to difficulty in managing a network

### 5.6 IP Subnetting:

Sub netting is the process of breaking down an IP network into smaller sub-networks called "subnets." Each subnet is a non-physical description (or ID) for a physical sub-network (usually a switched network of host containing a single router in a multi-router network).

In many cases, subnets are created to serve as physical or geographical separations similar to those found between rooms, floors, buildings, or cities.

There could be more than one definition for sub netting but perhaps the best explanation is that by default a network id has only one broadcast domain. Sub netting is a process of segmentation of a network id into multiple broadcast domains.

Sub netting originally referred to the subdivision of a class-based network into many sub networks, but now it generally refers to the subdivision of a CIDR block in to smaller CIDR blocks. Sub netting allows single routing entries to refer either to the larger block or to its individual constituents. This permits a single routing entry to be used though most of the Internet, more specific routes only being required for routers in the subnetted block.

Most modern subnet definitions are created according to **3 main factors.** These include:

The number of hosts that needs to exist on the subnet now and in the future.

The necessary security controls between networks.

The performance required for communications between hosts.

There are two forms of subnet notation,

1.subnet mask notation

2.CIDR (Classless Internet Domain Routing) notation

standard notation and CIDR (Classless Internet Domain Routing) notation. Both versions of notation use a base address (or network address) to define the network's starting point, such as 192.168.1.0. This means that the network begins at 192.168.1.0 and the first possible host IP address on this subnet would be 192.168.1.1.

**1.subnet mask notation**

In standard subnet mask notation, a four octet numeric value is used as with the base address, for example 255.255.255.0. The standard mask can be calculated by creating four binary values for each octet, assigning the binary digit of .1. to the network portion, and assigning the binary digit of .0. to the host portion. In the example above this value would be 11111111.11111111.11111111.00000000. In combination with the base address is a subnet definition. In this case the subnet in standard notation would be 192.168.1.0 255.255.255.0.

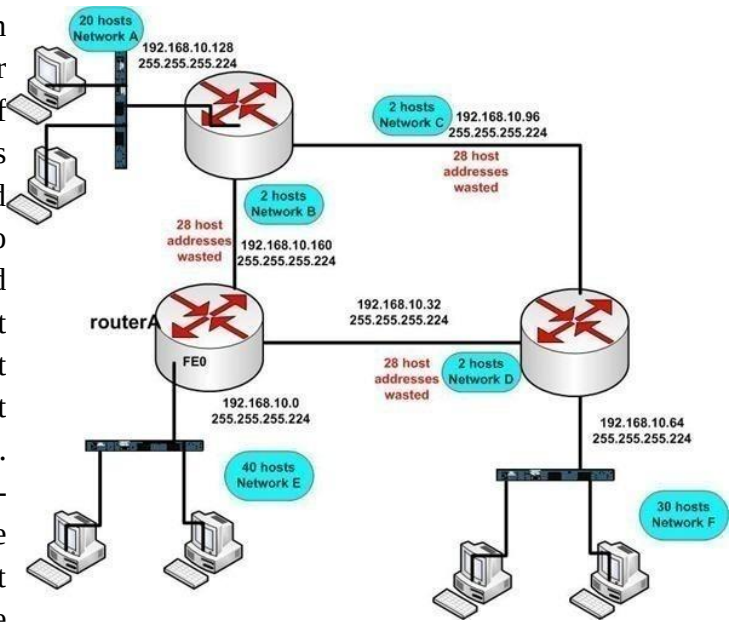
**2.CIDR notation**

In CIDR notation, the number of 1.s in the mask's binary version is counted from the left and that number is appended to the end of the base address following a slash (/). In the example here, the subnet would be listed in CIDR notation as 192.168.1.0/24.

### 5.6.1 Creating subnets in networks

**Network Subnetting**

In a subnetted network, there is an extended network portion. For example, a subnet mask of 255.255.255.0 would subnet a class B IP address space using its third byte. Using this scheme, the first two octets of an IP address would identify the class B network, the next octet would identify the subnet within that network, and the last octet would select an individual host. Since subnet masks are used or bit-by-bit bases, masks like 255.255.224.0 (three bits of subnet and thirteen bits of host) are perfectly normal.




There are several restrictions applied in a traditional subnetted network. Many of these restrictions have been lifted by CIDR, VLSM and more flexible IP routing protocols such as EIGRP and OSPF. However, if other routing protocols such as IGRP and RIP are used, the two restrictions must still be observed are as follow:

All subnet masks must be of a fix length. Since IGRP and RIP routing updates do not include subnet mask information, a router must assume that the subnet mask with which it has been configured is valid for all subnets. Therefore, a single mask must be used for all the subnets of a given classful network and different subnet masks can be used for different classful network addresses. This rule is referred to as the rule of FLSM (Fixed Length SubnetMask). Based on the assumption of FLSM, router can exchange subnet route with other routers within the network. Since the subnet masks are identical across the network, the routers will interpret these routes in the same manner. However, routers not attached to the subnetted network cannot interpret these subnet routes, since they lack the subnet mask. Therefore, subnet route are not relayed to router on other networks. This leads to second restriction.

A subnetted network cannot be split into isolated portions. All the subnets must be contiguous, since subnet routing information cannot be passed to non-members. All the subnets must be able to reach all other subnets with in a network without passing traffic through other networks.

**Class C Subnetting**

The Class C subnetting is less complicated then the other two classes of IP Addresses. There is comparatively less calculations you have to do in this type of subnetting. For example your company is using a single class C network of 192.168.0.0 with a default subnet mask of 255.255.255.0. The company has six departments of 30 hosts each and the requirement of your company is to segment them and broke the single broadcast domain for security reasons and to increase the maximum availability of bandwidth. You have to do three bits of subnetting using the formula 2n -2 where n is the value of subnet bits. The subnet bits would change the host portion of the subnet mask which is now 255.255.255.224 after subnetting. This can also be written in bit count format such as 192.168.0.0/27.

A common subnetwork environment is too inflexible when you require various types of subnet mask for the same network address. For example, consider a large organization with a single class C address of 192.168.0.0. Its headquarters site is made up of one subnet with 120 hosts on this subnet. The same organization has three regional offices, with a single LAN with less than 30 hosts each. Finally, this organization has six field offices. Each field office has a single segment with less than five hosts each. Which of the following subnet mask is best for this organization?

A 25 bit subnet mask yielding 2 subnets with each subnet yields 128 valid host addresses each (255.255.255.128).

A 26 bit subnet mask yielding 4 subnets with each subnet yields 62 valid host addresses each (255.255.255.192).

A 29 bit subnet mask yielding 30 subnets with each subnet yields 6 valid host addresses each (255.255.255.248).

The answer is the 25 bit subnet mask can be deployed at the central site. The 26 bit subnet mask can be deployed at the branch offices while the 29 bit mask can be deployed at the field offices. This is an example of a Variable Length Subnet Mask. However, the FLSM environment cannot accommodate deploying all of these different length subnet masks for a single classful network prefix.

There are two types of subnetted environment

1. Fixed Length Subnet Mask (FLSM)

2. Variable Length Subnet Mask (VLSM). The selection of routing protocol also determines whether you are stuck with a FLSM environment or whether you can deploy VLSM.

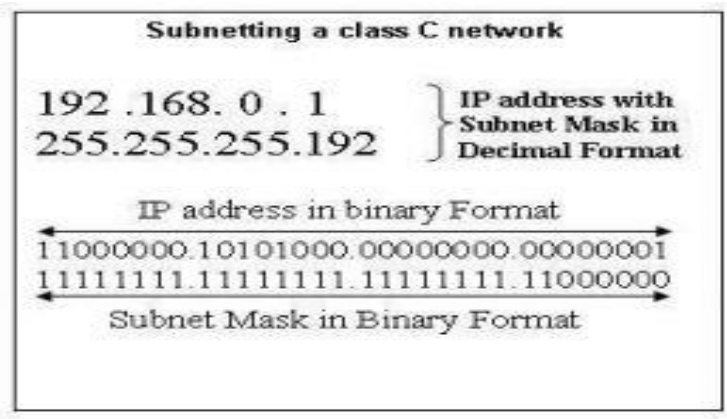
**How to Compute the Maximum Number of Hosts for a Subnet Mask**

To compute the maximum number of hosts for a subnet mask, take two and raise it to the amount of bits allocated to the subnet (count the number of 0.s in the subnet mask binary value) and subtract two. Subtract two from the resulting value because the first value in the IP address range (all 0s) is reserved for the network address and the last value in the IP address range (all 1s) is reserved for the network broadcast address. For example, DSL networks commonly use 8 bits for their subnets. The amount of allowable hosts for such a DSL network could be computed by the following formula: max hosts = (2^8)-2 = 254 hosts.

As users subnet networks, the number of bits that the subnet mask represents will decrease. Decrease the octets in order starting from the rightmost value and proceed left toward a zero value. Mask values decrease by a power of two each time a network is split into more subnets. Values are 255, 254*, 252, 248, 240, 224, 224, 192, 128. Each decrease indicates that an additional bit has been allocated. After 128, the next bit allocated will reduce the fourth octet to 0, and the third octet will follow same 8-number progression.

For instance, a subnet mask dotted decimal number of 255.255.255.255 indicates that no bits have been allocated and that the maximum number of hosts is 1 (0^1=1). The subnet mask 255.255.255.128 indicates that the maximum number of hosts is 128. And the subnet mask 255.255.128.0 indicates that the maximum number of hosts is 32,786.

* 254 is not a valid number for the fourth octet because no addresses are available for hosts. i.e. (2^1)-2 = 0.




### 5.6.2 Communication across subnets

Implementing Subnetting

The **Important factors** that should be clarified when determining the requirements of your subnetting scheme are:

The number of required network IDs. A network ID is needed for each subnet, and for each WAN connection.

The number of required host IDs. A host ID is needed for each TCP/IP based network device

Using the information above, you can create

A subnet mask for the network.

A subnet ID for every physical network segment

A range of host IDs for every unique subnet

You can implement subnetting by assigning a subnet address to each machine on a particular physical network. While you cannot change the network address segment of an IP address, you can change the host address segment. With subnetting, you take part of the host address and reuse it as a subnet address. This is done by taking bit positions from the host ID and then changing it to the subnet identifier. The number of host IDs are therefore reduced when you implement subnetting.

When you start the subnetting process, the bit position taken from the host ID reduces the number of hosts by a factor of 2. For instance, in a Class B network, you can have 65,534 possible host addresses or IDs. If you start subnetting the number of hosts which you can have is about half that figure. This is calculated as 65,534 / 2.

If the network has been subnetted, you can use the following equation to determine the number of host IDs you can have for each subnet:

2x – 2

x = number of bits in the host ID

Legacy Subnets

Legacy subnets were not flexible because they had predefined limitations on their size and numbers. These were called "classful" networks because each network could be easily identified and placed into a specific class, A to E. Shown below is a table containing the original "classful" definitions for IP addresses:

| IP Address Range | CIDR Equivalent | Purpose | RFC | Class | Total # of Addresses |
|---|---|---|---|---|---|
| 0.0.0.0 – 0.255.255.255 | 0.0.0.0/8 | Zero Addresses | 1700 | A | 16,777,216 |
| 10.0.0.0 – 10.255.255.255 | 10.0.0.0/8 | Private IP addresses | 1918 | A | 16,777,216 |
| 127.0.0.0 – 127.255.255.255 | 127.0.0.0/8 | Localhost Loopback Address | 1700 | A | 16,777,216 |
| 169.254.0.0 – 169.254.255.255 | 169.254.0.0/16 | Zeroconf / APIPA | 3330 | B | 65,536 |
| 172.16.0.0 – 172.31.255.255 | 172.16.0.0/12 | Private IP addresses | 1918 | B | 1,048,576 |
| 192.0.2.0 – 192.0.2.255 | 192.0.2.0/24 | Documentation and Examples | 3330 | C | 256 |
| 192.88.99.0 – 192.88.99.255 | 192.88.99.0/24 | IPv6 to IPv4 relay Anycast | 3068 | C | 256 |
| 192.168.0.0 – 192.168.255.255 | 192.168.0.0/16 | Private IP addresses | 1918 | C | 65,536 |
| 198.18.0.0 – 198.19.255.255 | 198.18.0.0/15 | Network Device Benchmark | 2544 | C | 131,072 |

| | | | | | |
|---|---|---|---|---|---|
| 224.0.0.0 – 239.255.255.255 | 224.0.0.0/4 | Multicast | 3171 | D | 268,435,456 |
| 240.0.0.0 – 255.255.255.255 | 240.0.0.0/4 | Reserved | 1700 | E | 268,435,456 |

https://www.4shared.com/video/z6ZvxSpSce/22_-_Routing_-_Creating_Subnet.htm?

**Classless Inter-Domain Routing(CIDR)**

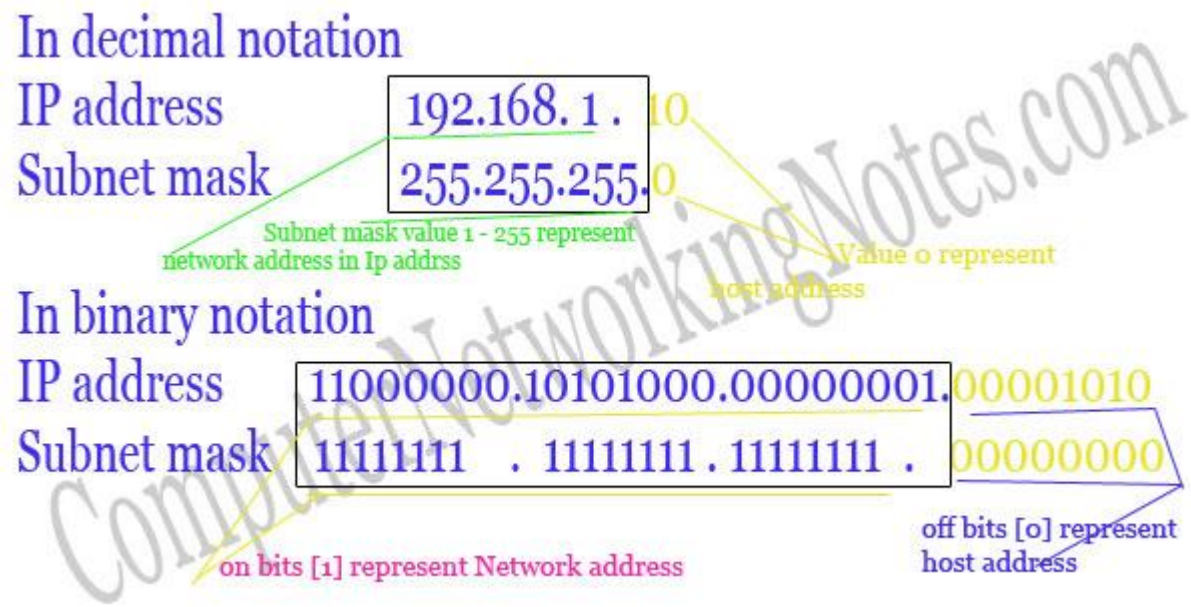
Classless IP Addresses

With the advent of CIDR (Classless Inter-Domain Routing), the "classful" definition of subnet divisions was lifted. Any network address could be defined just as any of the "classful" subnet of the past could be defined. All that is required is enough neighboring address space to cover all the IP addresses needed. Classless addresses also assist in reducing the overall size of the global routing tables on network devices.

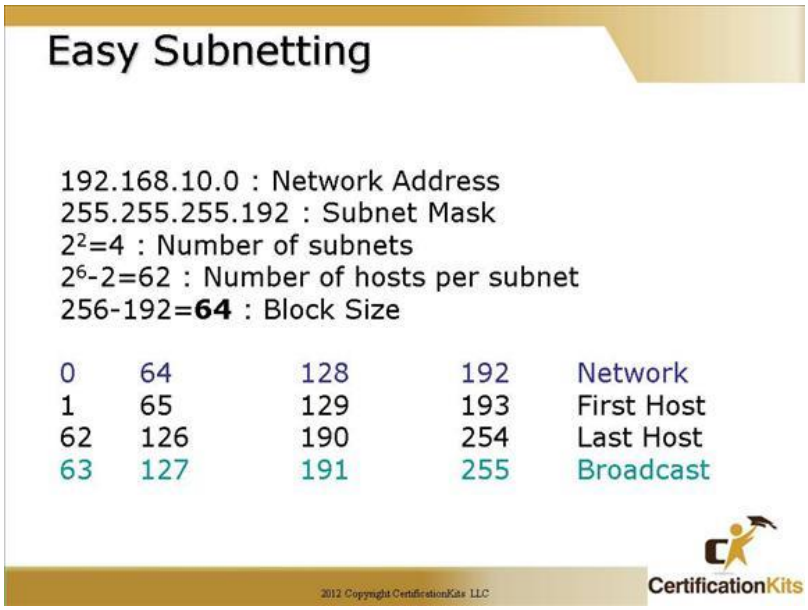
**When is Subnetting Used?**

The advantages associated with subnettng a network are summarized below:

- Through subnetting, you can reduce network traffic and thereby improve network performance. You only allow traffic that should move to another network (subnet) to pass through the router and to the other subnet.
- Subnettiing can be used to restrict broadcast traffic on the network.
- Subnetting facilitates simplified management. You can delegate control of subnets to other administrators.
- Troubleshooting network issues is also simpler when dealing with subnets than it is in one large network.
- A subnet is usually composed of a network router, a switch or hub, and at least one host.




| IP Class | Default Subnet | Network bits | Host bits | Total hosts | Valid hosts |
|---|---|---|---|---|---|
| A | 255.0.0.0 | First 8 bits | Last 24 bits | 16, 777, 216 | 16, 777, 214 |
| B | 255.255.0.0 | First 16 bits | Last 16 bits | 65,536 | 65,534 |
| C | 255.255.255.0 | First 24 bits | Last 8 bits | 256 | 254 |




**Note: This is only Basic Information for students. Please refer "Reference Books" prescribed as per syllabus**

## 5.7 Subnetting considerations:

Following factors are to be considered before dividing a network in to subnets

1. Number of subnets required: Computers on a network are usually grouped in to subnets on a common factor. For example consider a company with four departments and each departments has 20 computers the network administrators wants each department to remain segmented to facilitate network management. A router is used between each department it is logical create four subnets one for each department, because computers required within the department we need to communicate more frequently with one another than with the computers with other departments.

2. Number of subnets required in the future: When the computer network is designed it is necessary to ensure that the network can accommodate additional computers in future and therefore be expandable.

3. Number of host in the largest subnet:

We know that the some of the bits reserved for host address by the IP address are used for the subnet address therefore; the maximum number of hosts possible in a subnet is determined by the number of bits stolen from the host address part. For example In a class C network , the number of host in the largest subnet is 32. Therefore 5 bits of the last octet are required for the host address and only 3 bits are available for the subnet address. So maximum number of subnets on the network is 8.

## 5.8 Subnetting Limitations:

1. All the subnets created cannot be used at a time but can be reserved for the further expansion

2. It is not possible to allocate IP address proportionately per subnet. This leads to wastage of addresses in subnets

3. Subnetting leads to limitations on the number of hosts that can be accommodated in a single subnet

## 5.9 IPv6

Every device on the Internet is assigned a unique IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect devices than the IPv4 address space had available. By 1998, the Internet Engineering Task Force (IETF) had formalized the successor protocol. IPv6 uses a 128-bit address, theoretically allowing $2^{128}$, or approximately $3.4\times10^{38}$ addresses. The actual number is

slightly smaller, as multiple ranges are reserved for special use or completely excluded from use. The total number of possible IPv6 addresses is more than $7.9\times10^{28}$ times as many as IPv4, which uses 32-bit addresses and provides approximately 4.3 billion addresses. The two protocols are not designed to be interoperable, complicating the transition to IPv6. However, several IPv6 transition mechanisms have been devised to permit communication between IPv4 and IPv6 hosts.

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 also known as IPng (Internetworking Protocol next generation)
- IPv6 is an **"Internet layer"** protocol for a packet switched internetworking and provides end-to-end datagram transmission across multiple networks.

**Advantages –**

The following are the some of the advantages over the IPv4.

**Larger Address space -** An IPv6 address is 128-bit long compared to IPv4 i.e. 32-bit

**Better header format -** IPv6 uses a new header format in which option are separated from header.

**New options -** IPv6 has new options to allow for additional functionalities.

**Allowance for extension -** IPv6 is designed to allow the extension of the protocol, if required by new application.

**Support for resource allocation -** IPv6 uses new mechanism for avoiding traffic such as real-time audio and video

**Security -** The encryption and authentication option in IPv6 provides confidentially and integrity.

| Borrowed Bits | Number of Subnets | Number of Usable Hosts | Subnet Mask | Prefix |
|---|---|---|---|---|
| 0 | 0 (default) | $2^{16} - 2 = 65,534$ | 255.255.0.0 | /16 |
| 1 | $2^1 = 2$ | $2^{15} - 2 = 32,766$ | 255.255.128.0 | /17 |
| 2 | $2^2 = 4$ | $2^{14} - 2 = 16,382$ | 255.255.192.0 | /18 |
| 3 | $2^3 = 8$ | $2^{13} - 2 = 8,190$ | 255.255.224.0 | /19 |
| 4 | $2^4 = 16$ | $2^{12} - 2 = 4,094$ | 255.255.240.0 | /20 |
| 5 | $2^5 = 32$ | $2^{11} - 2 = 2,046$ | 255.255.248.0 | /21 |

**Activities**

1. 1 .14.23.120.8 address lies in which class

A. class A.
B. class B.
C. class D.
D. class E.

Answer is A

2. First 3 classes of addresses are

A. multicast.
B. reserved.
C. Unicast.
D. None.

Answer is C

3. Class C lies between

A. 0 to 127.
B. 1128-19111.
C. 1192-22311.
D. 1240-25511.

Answer is C

4. Network addresses are very important concepts of

A. Routing.
B. Mask.
C. IP Addressing.
D. Classless Addressing.

Answer is C

5. First address in block can be found by setting rightmost 32- n bits to

A. Os..
B. 1s.
C. combination of 0 and 1s.
D. None.

Answer is A

6. First address in a block is used as network address that represents the

A. Class Network.
B. Entity.
C. Organization.
D. Codes.

Answer is C

7. Packets of data that is transported by IP is called

A. datagram's.
B. Frames.
C. Segments.
D. Encapsulate.

Answer is A

8. Size and format of physical addresses vary depending on the

A. Receiver.
B. Message.
C. Sender.
D. Network.

Answer is A

9.Default network mask for CLASS B is

A. 255.0.0.0
B. 255.255.0.0
C. 255.255.255.0
D. 255.255.255.255

Answer is B

9.Default network mask for CLASS A is

A. 255.0.0.0
B. 255.255.0.0
C. 255.255.255.0
D. 255.255.255.255

Answer is A

10. What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask

A. 14
B. 15
C. 30
D. 62

Answer is C

11. To test the IP stack on your local host, which IP address will you ping

A. 127.0.0.0
B. 1.0.0.127
C. 127.0.0.1
D. 255.255.255.0

Answer is C

12. You need to subnet a network that has 5 subnets, each with at least 16 hosts. Which can be your choice?

A. 255.255.255.192
B. 255.255.255.224
C. 255.255.255.240
D. 255.255.255.248

Answer is B

# UNIT- 6: Wide Area Networks

## 6.1 Overview of WAN

To overcome the geographical limitations of LAN, Wide Area Network (WAN) is used.

A Wide Area Network (WAN) is a network that connects computers spread across a large geographical area. It can connect computers spread across a country, a continent, or the earth. Basically, WANs are interconnection of LANs. If a LAN is setup in only one branch office of an organization, only the computers in that branch office can share data and resources. However, by setting up LANs in all branch offices, and interconnecting these LANs, the data and resources can be shared among computers of all branch offices. The ability to share data over vast geographical areas is the most important benefit of WAN. Internet is a WAN that is spread across the earth. That is, Internet is a world-wide WAN.

WANs use facilities provided by a service provider, or carrier, such as a telephone or cable company, to connect the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. WANs provide network capabilities to support a variety of mission-critical traffic such as voice, video, and data.

Following are some of the important differences between LAN and WAN technologies:

- **Geographical Spread –** LAN covers local areas only (e.g., homes, offices, schools). WANs cover large geographic areas (e.g., cities, states, nations).
- **Ownership** – LANs are generally owned and maintained by a single person or small organization. WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management over long distances.
- **Connectivity** – The devices in a LAN are connected using coaxial cables, twisted pair cables, or optical fiber cables. In WAN, to connect devices and computers, connectivity options such as POTS, leased lines, ISDN, VSAT, Microwave, and Infrared are used.
- **Hardware** – Hardware devices used to establish connection in WAN are different from those used in LAN. Computers in a LAN are connected by devices such as hubs, switches, and repeaters. The devices such as routers, bridges, and gateways are used to establish connectivity in a WAN.
- **Protocols** – Protocols used in LAN for communication among computers are Ethernet, Token Ring or FDDI. Computers in a WAN use protocols such as Frame Relay, ATM, or X.25 for communication.
- **Speed** – Local Area Network (LAN) has higher bandwidth rates. Current Local Area Networks (LANs) run on bandwidths of 100 Mbps, 1 Gbps or 10 Gbps. Wide Area Network (WAN) has lower bandwidth rates compared with Local Area Network (LAN) because of the distance involved and technologies used between the locations.. Current Wide Area Networks run on bandwidths of 2 Mbps, 4 Mbps, 8 Mbps, 20 Mbps, 50 Mbps or 100 Mbps.
- **Fault Tolerance -** LANs tend to have fewer problems associated with them, as there are smaller numbers of systems to deal with. WANs tend to be fewer fault tolerant as they consist of large number of systems.
- **Security -** Since Local Area Networks (LANs) are private networks, managed by dedicated local network administrators, Local Area Networks (LANs) are more reliable and secure than Wide Area Networks (WANs). Since Wide Area Networks (WANs) involve 3rd party service providers, WAN networks are less reliable and secure.
- **Congestion -** Wide Area Networks (WANs) are more congested than Local Area Networks (LANs).

**6.2 WAN Connectivity**

In case of WAN, the cost of connectivity is high. For example, consider an organization having branch offices at Bengaluru, Mumbai, Delhi, and Hyderabad. Each branch office has its own LAN. The cost of cables used to connect these LANs would be high. Therefore, connectivity in WAN is not owned by the organization but obtained from service providers for a fee, known as access charges. The access charges mainly depend on the following:

- Data transfer speed (or bandwidth)
- Type of connectivity (leased lines, switched circuits, or ISDN)
- Distance between the locations to be connected (for example, a leased line between Bengaluru and Delhi would cost more than the one between Bengaluru and Hyderabad).
- WAN protocols
- Additional services offered by the service provider, such as security

In addition to being expensive, the connectivity options in WAN are different from those used in LAN because WANs spread across a vast geographical area.

The following are some of the popular connectivity methods used to setup a WAN.

- POTS
- Leased Lines
- ISDN
- VSAT
- Microwave
- Radio
- Infrared

Figure 6.2 provides a high-level view of the various WAN link connection options:

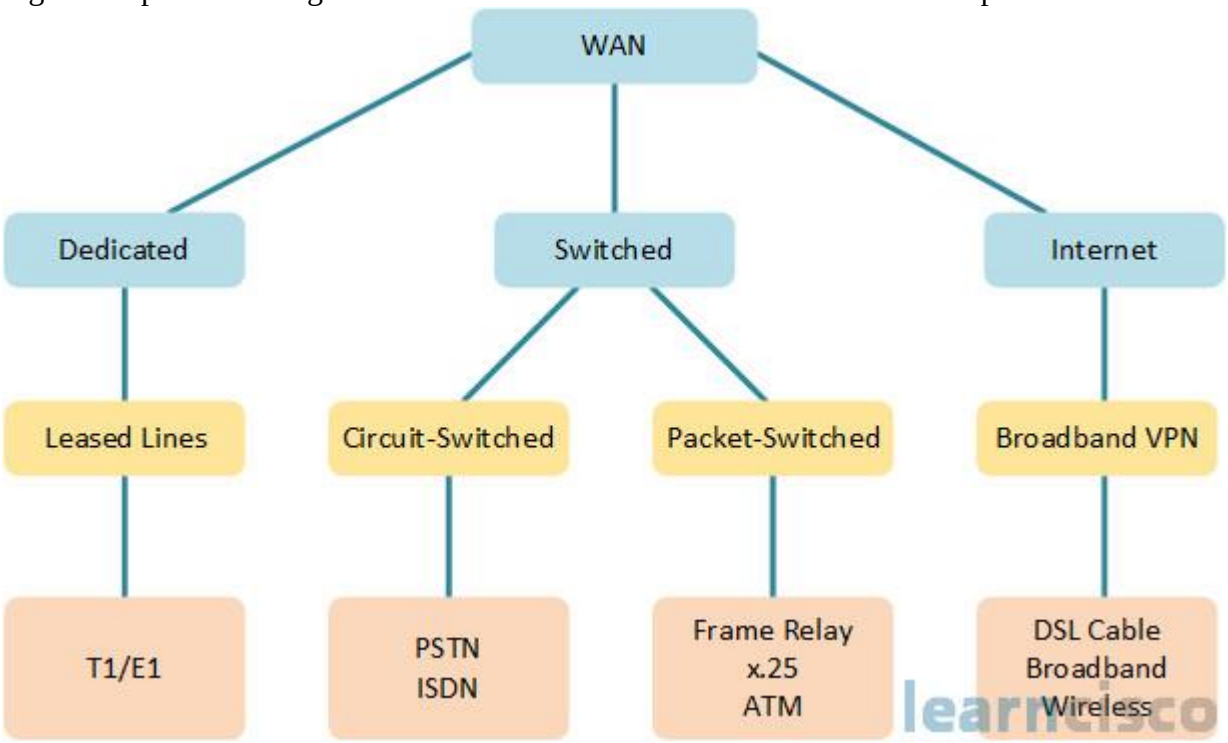



**Figure 6.2 WAN Link Connection Options**

https://www.youtube.com/watch?v=AoGqbQXRBAo

**Note: This is only Basic Information for students. Please refer "Reference Books" prescribed as per syllabus**

### 6.3 POTS (Plain Old Telephone System)

Dial-up connection uses POTS (Plain Old Telephone System). POTS is also called as PSTN (Public Switched Telephone Network). POTS is an analog technology that provides data transfer rates of 33.6 Kbps or 56 Kbps. In POTS, the connection among different LANs is established with the help of telephone lines. This connection between LANs is called a circuit. The circuit is made available for the LANs for communication and terminated when the communication ends. This process of making the circuit available only when the LANs communicate is called circuit switching.

Circuit switching works exactly in the same manner as the telephone system for voice communication. When two LANs communicate, a circuit is established between them. The circuit is dedicated as long as the communication is in progress. After the communication ends, the circuit is made available for other LANs to communicate.

Figure 6.1 shows an analog dialup connection between two LANs with the help of POTS.

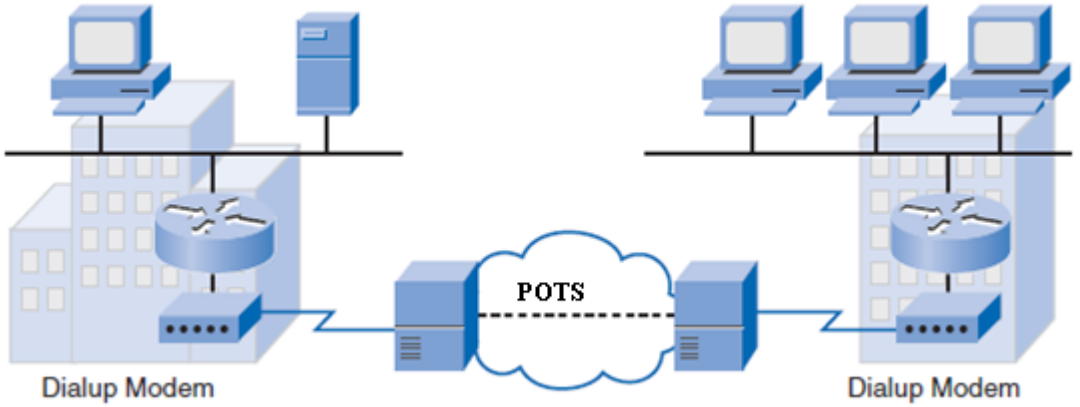



**Figure 6.1 WAN Built with an Intermittent Connection Using a Modem and the Voice Telephone Network POTS**

Traditional ***telephony*** uses a copper cable, called the local loop, to connect the telephone handset in the subscriber premises to the CO. The signal on the local loop during a call is a continuously varying electronic signal that is a translation of the subscriber analog voice signal.

https://www.youtube.com/watch?v=MansIEKvTNs

### 6.4 Leased Lines

Leased lines are also known as dedicated lines or private lines. When permanent dedicated connections are required, point-to-point lines are used with various capacities that are limited only by the underlying physical facilities and the willingness of users to pay for these dedicated lines. A point-to-point link provides a pre-established WAN communications path from the customer premises through the provider network to a remote destination. Point-to-point lines usually are leased from a carrier and are also called leased lines. Figure 6.3 shows a T3 and E3 circuit. This section describes how enterprises use leased lines to provide a dedicated WAN connection.

Leased lines are available in different capacities. They generally are priced based on the bandwidth required and the distance between the two connected points.

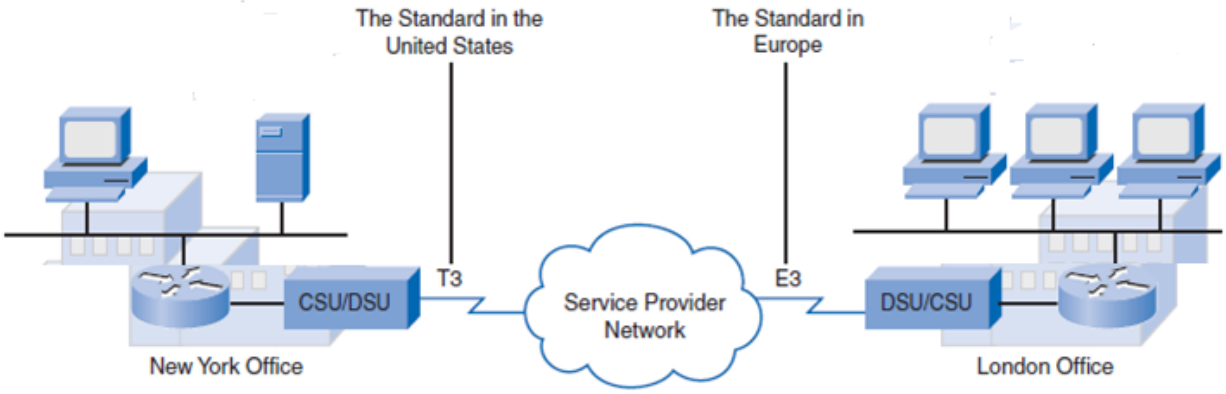



**Figure 6.3 Networks connected by Leased Lines**

The following table lists the available leased-line types and their bit-rate capacities.

| Line Type | Bit Rate Capacity | Line Type | Bit Rate Capacity |
|---|---|---|---|
| 56 | 56 kbps | OC-9 | 466.56 Mbps |
| 64 | 64 kbps | OC-12 | 622.08 Mbps |
| T1 | 1.544 Mbps | OC-18 | 933.12 Mbps |
| E1 | 2.048 Mbps | OC-24 | 1244.16 Mbps |
| J1 | 2.048 Mbps | OC-36 | 1866.24 Mbps |
| E3 | 34.064 Mbps | OC-48 | 2488.32 Mbps |
| T3 | 44.736 Mbps | OC-96 | 4976.64 Mbps |
| OC-1 | 51.84 Mbps | OC-192 | 9953.28 Mbps |
| OC-3 | 155.54 Mbps | OC-768 | 39,813.12 Mbps |

Point-to-point links usually are more expensive than shared services such as Frame Relay. The cost of leased-line solutions can become significant when they are used to connect many sites over increasing distances. However, sometimes the benefits outweigh the cost of the leased line. The dedicated capacity removes latency and jitter between the endpoints. Constant availability is essential for some applications, such as VoIP and video over IP.

A router serial port is required for each leased-line connection. A CSU/DSU and the actual circuit from the service provider are also required. A CSU/DSU is a digital interface device used to connect a data terminal equipment (DTE), such as a router, to digital circuit, such as a Digital Signal 1 (T1) line. A CSU/DSU converts a digital data frame from the communications technology used on a LAN into a frame appropriate to a WAN and vice versa.

Leased lines provide several advantages with respect to other WAN technologies. Leased lines provide dedicated bandwidth with very little latency or jitter and constant network availability. This makes leased lines very attractive for mission critical and business transaction data. Leased lines require minimal expertise to install and maintain and offer a high Quality of Service (QoS). Leased line bandwidth is limited only by the physical nature

of communications medium and the price users are willing to pay for the dedicated bandwidth.

Leased lines have several disadvantages when contrasted with other WAN technologies. First, leased lines are the most expensive type of WAN access. The cost of leased lines depends on the required bandwidth, QoS and distance of the connection. Second, an organization's bandwidth usage and needs are intuitively variable. Leased lines provide fixed capacity that results in wasted bandwidth when network traffic is minimal. Leased lines offer limited flexibility since the carriers provide a fixed and limited network capacity.

https://www.youtube.com/watch?v=34AHD-Osrpc

**6.5 Integrated Services Digital Network (ISDN)**

Integrated Services for Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. This technology uses ISDN adapters in place of modems and provides very fast speed up. ISDN requires adapters at both ends of the transmission.

Integrated Services Digital Network (ISDN) is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher-capacity switched connections.

ISDN changes the internal connections of the PSTN from carrying analog signals to time-division multiplexed (TDM) digital signals. TDM allows two or more signals or bit streams to be transferred as subchannels in one communication channel. The signals appear to transfer simultaneously, but physically they take turns on the channel. A data block of subchannel 1 is transmitted during time slot 1, subchannel 2 during time slot 2, and so on. One TDM frame consists of one time slot per subchannel.

ISDN connections are considerably faster than regular modem connections. To access ISDN, a special phone is required. To establish an ISDN connection, you dial the number associated with the receiving computer, much as you do with a conventional phone line call or modem dialup connection. A conversation between sending and receiving devices is then established. The connection is dropped when one end disconnects or hangs up. The line pick up of ISDN is very fast, allowing a connection to be established or brought up much more quickly than a a conventional phone line.

**Features of ISDN**

ISDN is a network architecture in which digital technology is used to convey information from multiple networks to the end user. This information is end-to-end digital.

Some of the features of ISDN are:

1. Offers point-to-point delivery
2. Network access and network interconnection for multimedia.
3. Different data rates from 64 Kbps up to 2 Mbps are commercially available which can meet many needs for transporting multimedia and is four to many times more than today's analog modems
4. Call set-up times are under one second. ISDN can dramatically speed up transfer of information over the Internet or over a remote LAN connection, especially rich media like graphics, audio or video or applications that normally run at LAN speeds.

ISDN turns the local loop into a TDM digital connection. This change enables the local loop to carry digital signals that result in higher-capacity switched connections. The connection uses 64-kbps ***bearer (B) channels*** to carry voice or data and a ***signaling***, ***delta channel*** for call setup and other purposes.

There are two types of ISDN interfaces:

- **Basic Rate Interface (BRI)**: provides an ISDN user with simultaneous access to two 64 Kbps data channels using the existing twisted pair copper telephone cable. Each data channel is referred to as a B-channel and can carry voice or data. Another channel, the D-channel, operates at 16 Kbps and is used for signaling between user devices and the ISDN. The total data rate of BRA is therefore 144 Kbps. The two B-channels and the single signaling channel give rise to the term 2B+D ISDN is intended for low capacity usage, such as that required for small businesses.
- **Primary Rate Interface (PRI)**: ISDN is also available for larger installations. PRI delivers 23 B channels with 64 kbps and one D channel with 64 kbps in North America, for a total bit rate of up to 1.544 Mbps. This includes some additional overhead for **synchronization**. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and one D channel, for a total bit rate of up to 2.048 Mbps, including synchronization overhead

Figure 6.4 illustrates the various differences between ISDN BRI and PRI lines.

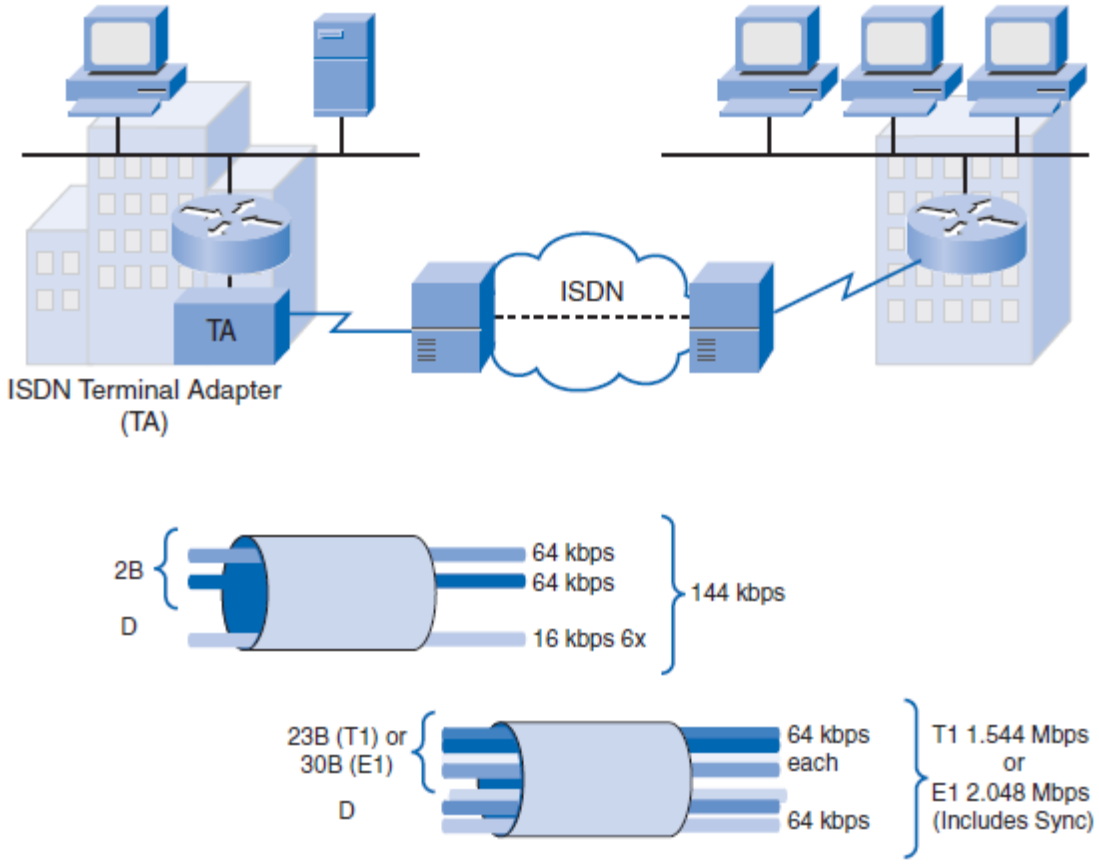



**Figure 6.4 ISDN Network Infrastructure and PRI/BRI Line Capacity**

https://www.youtube.com/watch?v=mTFE-So38GE

### 6.6 Very Small Aperture Terminal (VSAT)

VSAT (Very Small Aperture Terminal) refers to a small fixed earth station. VSATs provide the vital communication link required to setup a satellite based communication network. VSATs can support any communication requirement be it voice, data, or video conferencing. IT is a satellite communications system that serves home and business users. It is an earthbound station used in satellite communications of data, voice and video signals, excluding broadcast television.These are small stations with antenna diameters 0.6 to 3.8 meters, hence the name 'small aperture' which refers to the area of the antenna.

#### 6.6.1 VSAT Devices

The VSAT consists of two modules – an outdoor unit and an indoor unit. The outdoor unit consists of an antenna and radio frequency transceiver (RFT). The antenna size is typically 1.8 meter or 2.4 meter in diameter, although smaller antennas are also in use. The transceiver is to receive and send satellite signals. The indoor unit functions as a modem and also interfaces with the end user equipment like stand alone PCs, LANs, or telephones. One end of the indoor unit is connected to the computers and other devices in the network. The other end of the indoor unit is connected to the outdoor unit.

VSAT devices are categorized into two types depending on their operational capabilities: receive only devices and bi-directional devices. Receive-only VSAT devices can only receive data from the network but cannot send any data whereas bi-directional devices can receive as well as send data to the network.

#### 6.6.2 VSAT Networks

A typical VSAT network consists of three components: a central hub that is connected to the main earth station, the satellite that transmits data across different earth stations, and the VSAT earth stations located in different geographical areas.

A VSAT hub is a huge earth station that is responsible for controlling & monitoring all the activities of the geographical spread of VSATs. The hub station has a larger antenna size than that of a VSAT, say 4 m to 11 m, resulting in a higher gain than that of a typical VSAT antenna, and is equipped with a more powerful transmitter. As a result of its improved capability, the hub station is able to receive adequately all carriers transmitted by the VSATs, and to convey the desired information to all VSATs by means of its own transmitted carriers. The architecture of the network becomes *star-shaped* as shown in Figure 6.5. The links from the hub to the VSAT are named *outbound links*. Those from the VSAT to the hub are named *inbound links*. Both inbound and outbound links consist of two links, uplink and downlink, to and from the satellite.

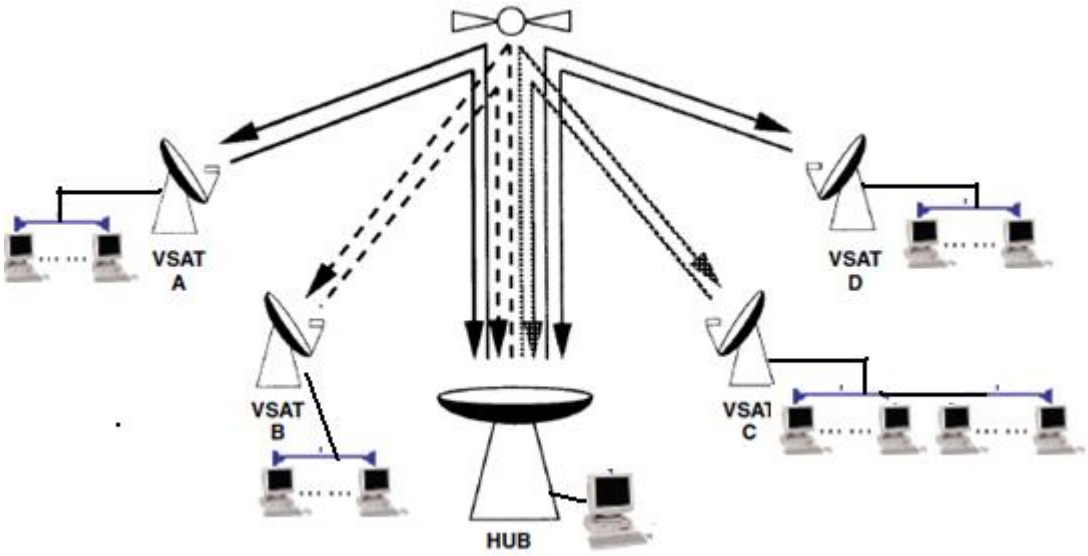



Figure 6.5 Two-way star-shaped VSAT network with four VSATs

The hub controls the entire operation of the network. For one end user to communicate with another, each transmission has to first go to the hub station that then retransmits it via the satellite to the other end user's VSAT. VSAT can handle up to 56 Kbps.

There are two types of star-shaped VSAT network:

- Two-way networks (Figure 6.5), where VSATs can transmit and receive. Such networks support interactive traffic;
- One-way networks (Figure 6.6), where the hub transmits carriers to receive-only VSATs. This configuration supports broadcasting services from a central site where the hub is located to remote sites where the receive-only VSATs are installed.

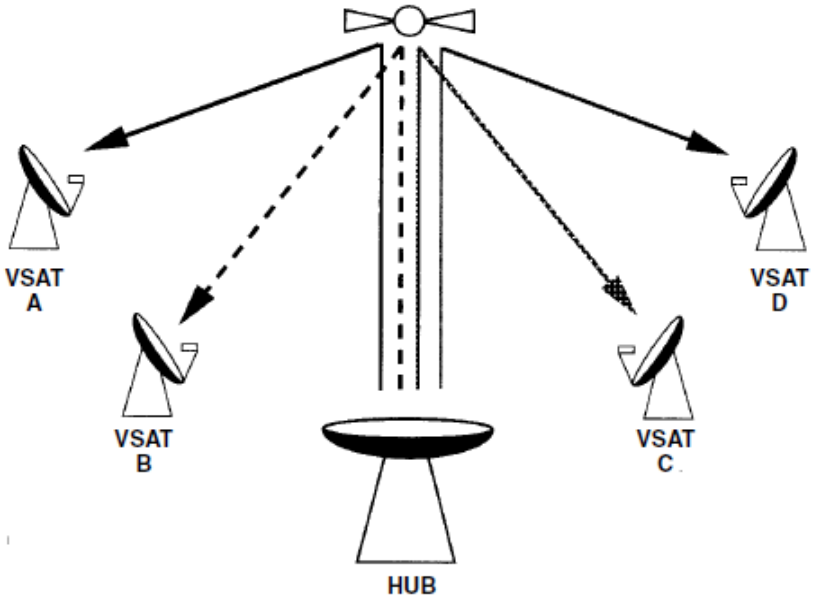



Figure 6.6 One-way star shaped VSAT network

**https://www.youtube.com/watch?v=bw3tB98HWs0**

**6.6.3 VSAT Network Architectures**

The following architectures are popularly used to set up VSAT networks:

- Single Channel Per Carrier (SCPC) – In SCPC, the VSAT service provider offers a single permanent channel between the locations required by the user; SCPC has the flexibility of adding additional channels between the user locations. However, each additional channel needs to have a separate VSAT device, and therefore, increasing the number of channels increases the equipment cost. SCPC is preferred when the user exactly knows the amount of data to be transmitted over the VSAT network.
- Multi Channels Per Carrier (MCPC) – IN MCPC, the VSAT service provider offers multiple permanent channels between the user locations, resulting in higher data transfer rates between the locations. However, the user is charged for all the channels irrespective of how much data is actually transferred. MCPC is used when transmitting data pertaining to applications that require higher bandwidth.
- Time Division Multiple Access (TDMA) – In TDMA, the VSAT link between the user locations is offered on a sharing basis. TDMA works in a similar manner as switched circuits. The VSAT link is made available when the VSAT devices need to communicate and the link is terminated at the end of the communication.

### 6.6.4 VSAT Access Technologies

The commonly used VSAT access technologies are:

- Pre Assigned Multiple Access (PAMA) - PAMA is an access scheme where in when 2 VSATs want to communicate with each other a bandwidth is assigned to them exclusively. This assigned bandwidth will be available between the source and destination VSAT stations on a permanently basis. This link can either be a symmetric and asymmetric link. It is nothing but a point to point connectivity. PAMA works in a similar manner as that of leased lines, and therefore the user needs to pay for the entire link irrespective of the actual duration for which it was used.
- Demand Assigned Multiple Access (DAMA) – The DAMA scheme is very similar to a telephone connection. Whenever, there is a need to talk to someone, you dial a number. The call lands at the telephone exchange, and the telephone exchange connects you to the dialed number. The role of the telephone exchange is to connect you to the desired number. This is exactly how a DAMA network operates. The HUB plays the role of a telephone exchange, between any two VSAT's. The connection is made available as long as the communication is in progress and terminated at the end of the communication. The access charges are based on the actual time for which the VSAT link was used.

### 6.6.5 VSAT Advantages

Some of the advantages of using VSATs are:

a. VSATs are highly reliable of all the wireless connectivity options.
b. VSAT also offers high uptimes as high as 99.5% as compared to uptime rates of approximately 85% offered by leased lines or ISDN.
c. Since VSATs use a satellite to communicate geographical boundaries or terrain is not a constraint.
d. A centrally managed network, which reduces a lot of logistics cost for the customer.
e. VSAT offers the same bandwidth as the leased lines.
f. In case of a failure the Mean Time to Repair is in the order of a few Hours.
https://www.youtube.com/watch?v=GBh-ljtaS3w

## 6.7 MICROWAVE TRANSMISSION

Microwave transmission is the transmission of information by electromagnetic waves whose wavelengths are measured in small numbers of centimeter; these are called microwaves. Microwave transmission is a wireless technology that can be used to transmit digital information between two computers that can be around 15 kilometers apart. It is possible to use repeaters, or amplifiers to boost the signal strength so that computers as far as 40 kilometers or more apart can communicate. In order to communicate using microwave, each computer or network needs to have a microwave device installed. A typical microwave device consists of the following:

- Digital Modem – It receives the microwave signals, converts them into digital signals and passes it on to the computer and vice versa.
- Radio Frequency (RF) unit – The RF unit converts the signal from the modem into a microwave signal and transmits the signal across the microwave network and vice versa.
- Antenna – The antenna transmits and receives the microwave signals. The antennas of the terminals must maintain a line of sight for the microwave communication to work.

Figure 6.7 represents two networks connected with the help of microwave.

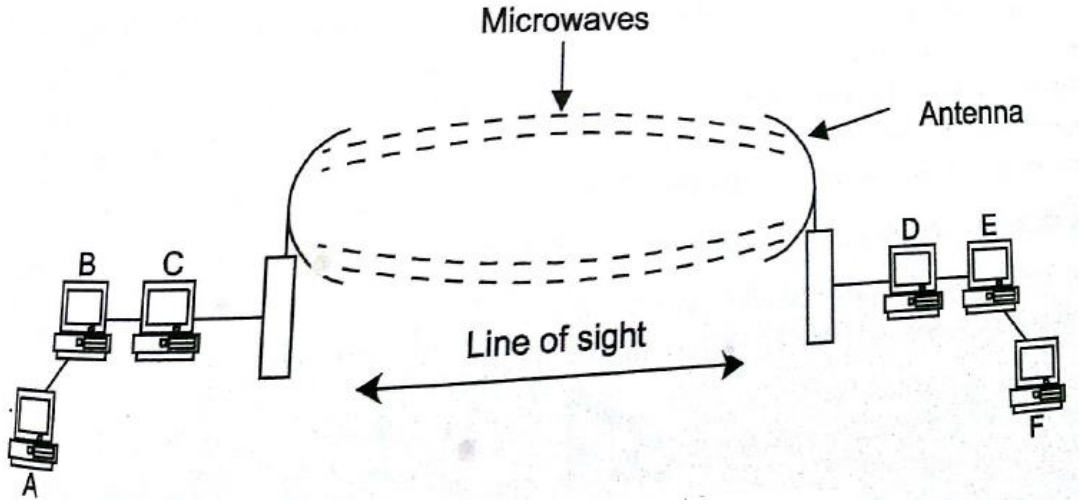



Figure 6.7 Networks connected with microwaves

In the above figure, when Network A needs to transmit data to Network B, the data reaches the digital modem, which converts the data into digital signals. These signals reach the RF unit where the signals are converted to microwaves and are transmitted with the help of the antenna from Network A. the antenna on Network B receives the microwaves and passes them on to the RF unit where the microwaves are converted to digital signals. The digital signals are then passed through the digital modem to the Network B.

**Advantages:**

- Microwave offers several advantages over terrestrial connectivity options as well as VSAT.
- As there are no cables involved, the time required to setup as microwave network is very low.
- The connectivity between microwave devices can be established without a service provider and there are no access charges.
- Microwave supports higher bandwidth and data transfer speeds compared to VSAT, and leased lines while providing a reliable means of data transfer.

**Disadvantages:**

The antennas should maintain a line of sight. Therefore, microwave networks are effective only if the networks are spread over a smaller geographical area. Therefore, microwave network finds limited use in setting up WANs.

https://www.youtube.com/watch?v=FrvgWhsQka4

## 6.8 RADIO TRANSMISSION

In this method, radio waves are used to wirelessly connect LANs or computers. Radio waves are also used only when terrestrial connectivity options are not available. The computers or networks that need to communicate using radio waves should have an antenna. The antenna converts outgoing data packets into radio waves and transmits them. The antenna also converts the incoming radio waves into data packets and passes them onto the network. Figure 6.8 shows two networks connected with the help of radio waves.

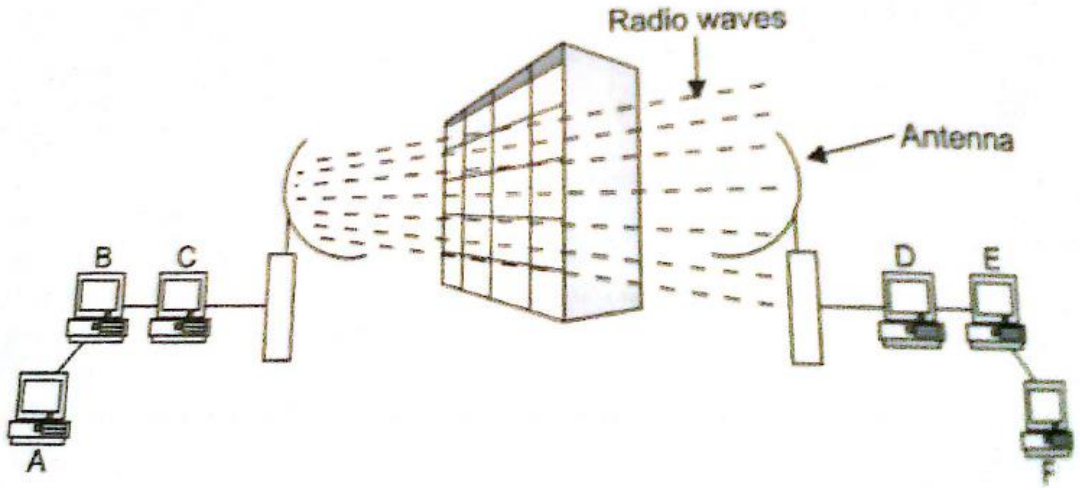



Figure 6.8 Networks connected with radio waves

Assume that Network A sends data to Network B. the data from Network A reaches the antenna where it is converted to radio waves and transmits them. These waves are received by the antenna on Network B, which converts the waves into data and passes them onto the computers in the network.

The antennas in the networks need to maintain line of sight, and the distance between the antennas or networks depends on the capacity of the transmitter used by the antenna. With a powerful transmitter, the devices can be as far as one kilometer apart.

Similar to microwaves, the time to setup a radio wave network is very less due to the absence of cabling. In addition, the cost of antenna used to transmit and receive radio waves is lesser than the cost of microwave device. However, the data transfer rates provided by radio waves is lesser than those of microwave.

https://www.youtube.com/watch?v=gLMC5R5Me9c

## 6.9 INFRARED TRANSMISSION

Infrared technology allows devices with infrared ports to communicate with each other, and share data. Infrared transports data through light, which is invisible to human eye. The infrared light is usually in the frequency range of 1000GHz.

The networks that wish to communicate using infrared need to satisfy the following criteria:

- The networks should have devices with infrared ports
- The devices should maintain a direct line of sight

- The distance between the devices should not be more than three yards

Figure 6.9 shows two networks connected using infrared devices.

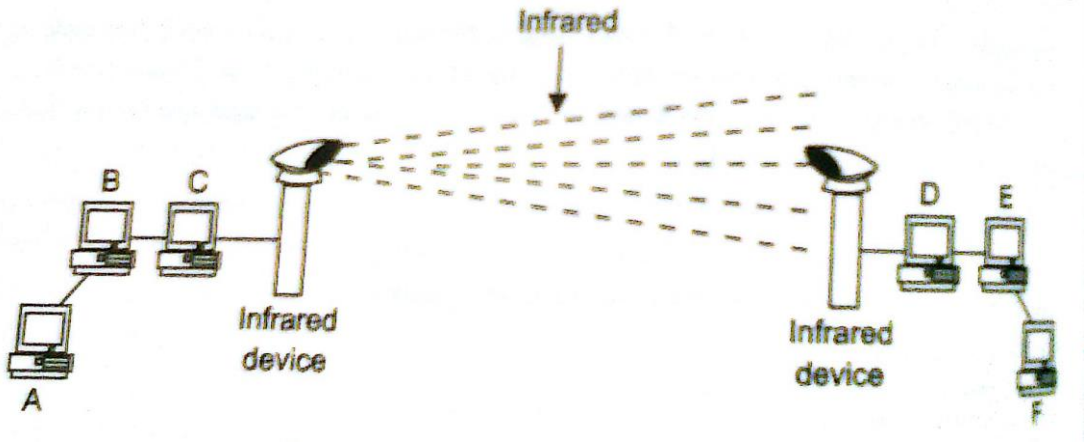



Figure 6.9 Networks connected with Infrared

In practice, however, the networks and the devices are usually farther than three yards, and also may not maintain a direct line of sight. To overcome these drawbacks, infrared mirrors are used. An infrared mirror focuses the infrared signal into a tight beam, boosts the signal, and then transmits it. With the help of an infrared mirror, devices as far apart as four kilometers can communicate. Infrared is generally used to connect networks close to one another and in cases where a line of sight is maintained. For example two networks present in adjacent buildings.

**http://study.com/academy/lesson/infrared-waves-definition-uses-examples.html**

### 6.10 VIRTUAL PRIVATE NETWORKS (VPNs)

VPN is a secure, private communication tunnel between two (or more) devices across a public network (like the Internet). A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private tunnel. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network as shown in Figure 6.10.

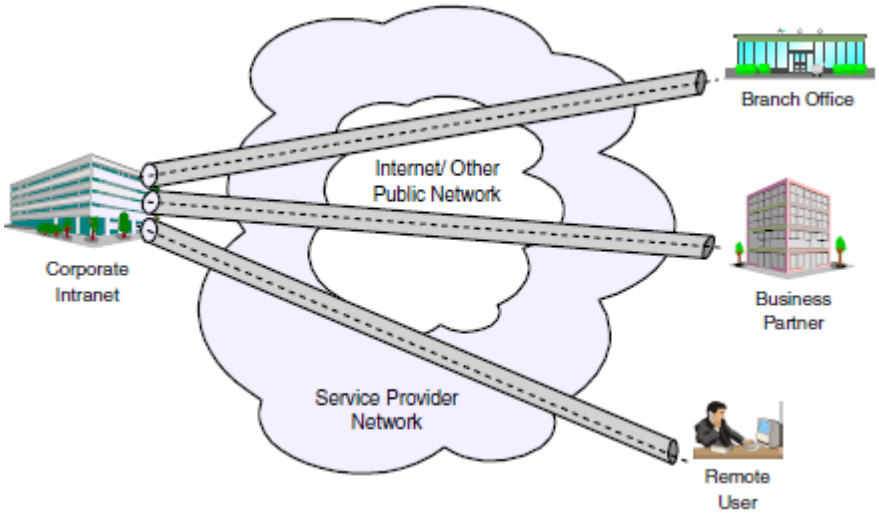



Figure 6.10 Virtual Private Network (VPN)

Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive, leased lines, long-distance calls, and toll-free telephone numbers.

**It is Virtual** - Virtual means not real or in a different state of being. In most cases it also means that the physical network is not owned by the user of a VPN but is a public network shared with many other users.

**It is Private** - Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them.

**It is a Network** - A network consists of two or more devices that can freely and electronically communicate with each other via cables and wire. A VPN is a network. It can transmit information over long distances effectively and efficiently.

Simply put, a VPN, Virtual Private Network, is defined as a network that uses public network paths but maintains the security and protection of private networks.

VPNs use the existing connectivity options in a WAN to provide a cost-effective, flexible, and reliable method of accessing private networks. VPN extends the benefits offered by WANs without compromising on the security of data.

VPN is also advantageous in cases where a single computer needs to connect to a WAN. Assume that the sales manager of the organization has travelled to another place on a one week business visit. The sale manager needs to access the corporate network for important information updates. It is practically impossible to use connectivity options such as leased lines, ISDN, VSAT, or microwave for this purpose. In this case, the VPN can be used by the sales manager to connect to the corporate network. In fact, VPN is a popular option used by mobile users to connect to their corporate networks.

A typical VPN is shown in Figure 6.11.

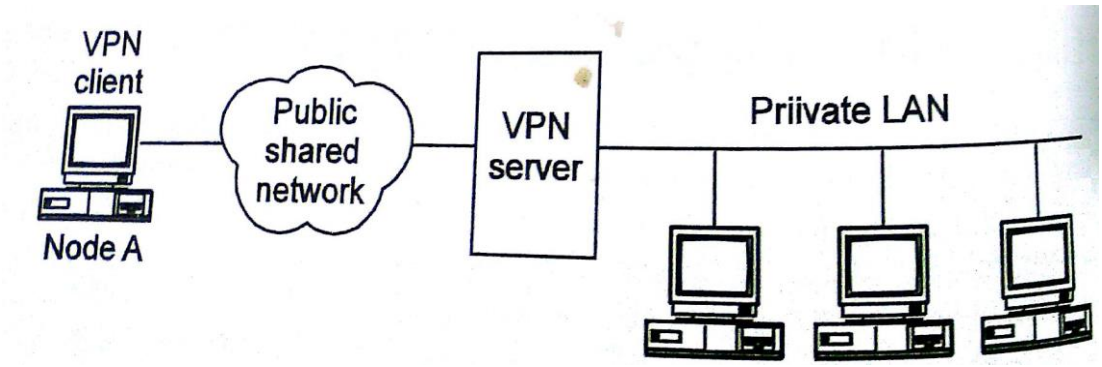



Figure 6.11 Virtual Private Network

Node A is the VPN client. A VPN client is either a computer that needs to access a private network, or a server in a network that needs to access another private network. VPN Clients are most often software based, and have the ability to "call" VPN servers, logon and communicate as they're on the same "virtual" network. Node A connects to the VPN server of the private network over the Internet. The VPN server is computer in the private network that accepts incoming VPN connections. The VPN server authenticates the user information

provided by Node A, and connects Node A to the network. VPN servers are hardware or software that listens for incoming connections, and acts as a gateway into a local network (or a single computer).

VPNs transmit important data over the internet, and therefore, need to ensure that data integrity is maintained. Therefore, the three main functions of a VPN are:

- Security -- The VPN should protect data while it's traveling on the public network. If intruders attempt to capture the data, they should be unable to read or use it.
- Reliability -- Employees and remote offices should be able to connect to the VPN with no trouble at any time (unless hours are restricted), and the VPN should provide the same quality of connection for each user even when it is handling its maximum number of simultaneous connections.
- Scalability -- As a business grows, it should be able to extend its VPN services to handle that growth without replacing the VPN technology altogether.
- To transfer data across networks that may be using different protocols

### 6.10.1 Working of VPN

VPN performs the following functions to ensure that the data transmitted over a VPN is secure:

- Authentication – The VPN client requesting access to a private network is authenticated to ensure that the client is trusted one. Authentication is done with the help of a user name and password.
- Encryption – The data transmitted across the Internet is encrypted so that the packets cannot be read by unauthorized sources.
- Data integrity – To prevent accidental loss of data packets over the Internet. VPNs employ several data integrity checks to ensure that the data packets reach the destination correctly

### 6.10.2 VPN Protocols

VPN protocols are responsible for encrypting and encapsulating data packets that travel over the Internet. Commonly used VPN protocols are:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Internet Protocol Security (IPSec)

**Point-to-Point Tunneling Protocol (PPTP)**

One of the more "established" techniques for remote connection is the Point-to-Point Tunneling Protocol (PPTP). PPTP is a vendor solution that meets the requirements for a VPN. It has been implemented by Microsoft on the Windows NT, Windows 98 and Windows 95 (OSR2) platforms. Supports 40-bit and 128-bit encryption and any authentication scheme supported by PPP.

PPTP allows users to establish a low cost connection to a corporate or private network over the Internet. Following are the important features of PPTP:

- PPTP is an extension of the basic PPP protocol. It is due to this fact that PPTP does not support multipoint connections, connections must be point-to-point.
- PPTP supports only IP, IPX, NetBIOS and NetBEUI.
- PPTP does not change the PPP protocol. PPTP only defines a new way, a tunneled way, of transporting PPP traffic.
- PPTP works at Layer 2 of the OSI reference model

- PPTP uses Extensible Authentication Protocol (EAP), Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), and Password Authentication Protocol (PAP) to authenticate user before granting access to network resources in a VPN
- The encryption protocol used by PPTP is Microsoft Point-to-Point Encryption (MPPE).
- MPPE provides only link encryption between the VPN client and the VPN server.

**Layer 2 Tunneling Protocol (L2TP)**

Layer Two Tunneling Protocol (L2TP) is a combination of PPTP and Layer 2 Forwarding (L2F), a technology developed by Cisco Systems, Inc.L2F developed by Cisco; uses any authentication scheme supported by PPP. Rather than having two incompatible tunneling protocols competing in the marketplace and causing customer confusion, the Internet Engineering Task Force (IETF) mandated that the two technologies be combined into a single tunneling protocol that represents the best features of PPTP and L2F. Combines features of PPTP and L2F and fully supports IPSec.

L2TP encapsulates PPP frames to be sent over IP, X.25, frame relay, or ATM networks. When sent over an IP network, L2TP frames are encapsulated as User Datagram Protocol (UDP) messages. L2TP can be used as a tunneling protocol over the Internet or over private intranets.

L2TP allows a remote user to connect to a corporate network with the help of two devices: L2TP Access Concentrator(LAC), and L2TP Network Server (LNS). Figure 6.12 shows a typical VPN implemented with the help of L2TP.

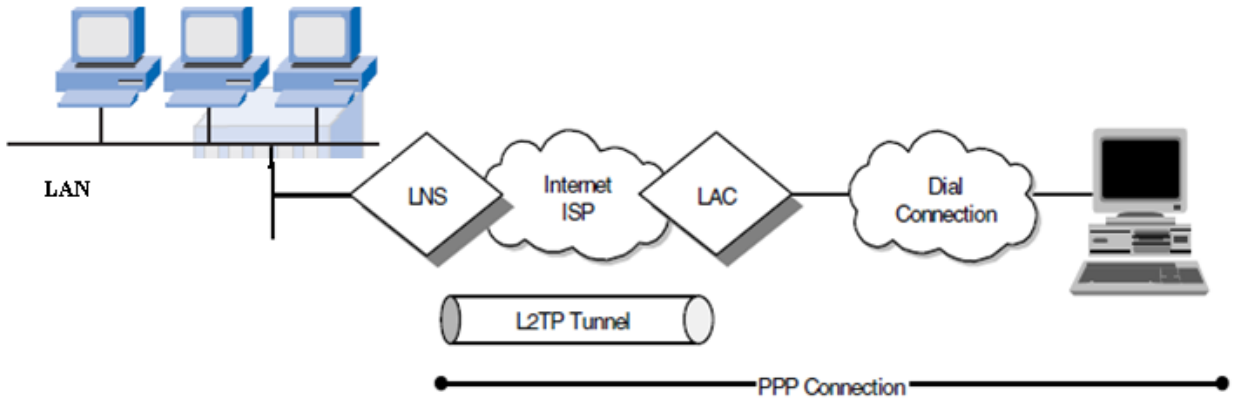



Figure 6.12 VPN using L2TP

The LAC is located at the ISP's POP (Point of Presence) to provide the physical connection of the remote user. The remote user connects to the ISP using PPP. When the user contacts the ISP, the LAC contacts the LNS to authenticate the user. If the user is authenticated, access is granted to the corporate network, and an L2TP tunnel is created between the LAC and the LNS. The data traveling through the L2TP tunnel is encapsulated and encrypted.

https://www.youtube.com/watch?v=4Q7bj3dNbR8

**Internet Protocol Security (IPSec)**

IPSec works at layer 3 of the OSI reference model, and is designed to provide enhanced security for data that is transmitted over the Internet. IPSec is a widely used protocol for securing traffic on IP networks, including the Internet. IPSec can encrypt data between various devices, including router to router, firewall to router, desktop to router, and desktop to server.

IPSec consists of three components:

- **Encapsulated Security Payload** (**ESP**) encrypts the packet's payload (the data it's transporting) with a symmetric key. Encapsulating Security Protocol (ESP) ensures privacy and integrity.
- **Authentication Header** (**AH**). It provides authentication of the data origin, checks for data integrity, and provides protection against replay. Authentication Header (AH) ensures data integrity and authenticity
- Internet Security Association and key management protocol(ISAKMP). It provides a method of automatically setting up security associations to encrypt and decrypt data.

Networked devices can use IPSec in one of two encryption modes. In **transport mode**, devices encrypt the data traveling between them but not encapsulated. In **tunnel mode**, the devices encrypt the data as well as build a virtual tunnel between two networks.

## 6.11 WAN DEVICES

Tthe following devices are used to interconnect LANs.i e WAN devices.

- Bridges
- Routers
- Gateways

### 6.11.1 Bridges

The device that can be used to interconnect two separate LANs is known as a *bridge*. It is commonly used to connect two similar or dissimilar LANs as shown in Figure 6.13. The bridge operates in layer 2, that is data-link layer and that is why it is called *level-2 relay* with reference to the OSI model. It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations. The flow of information through a bridge is shown in Figure 6.14. Use of bridges offer a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage. But, it is desirable that the quality of service (QOS) offered by a bridge should match that of a single LAN. Key features of a bridge are mentioned below:

- A bridge operates both in physical and data-link layer
- A bridge uses a table for filtering/routing
- A bridge does not change the physical (MAC) addresses in a frame

Bridges use MAC addresses stored by Layer 2 protocols to transmit data across networks. The primary use of a bridge to connect two networks that use different Layer 2 protocols.

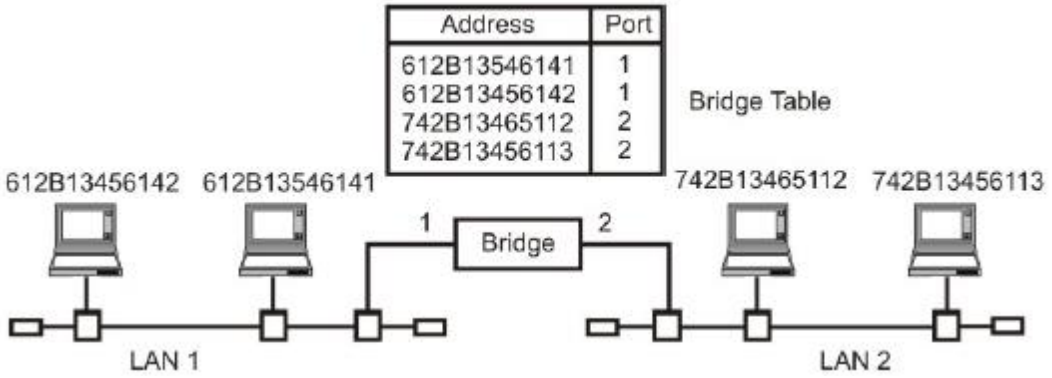



Figure 6.13 A bridge connecting two separate LANs

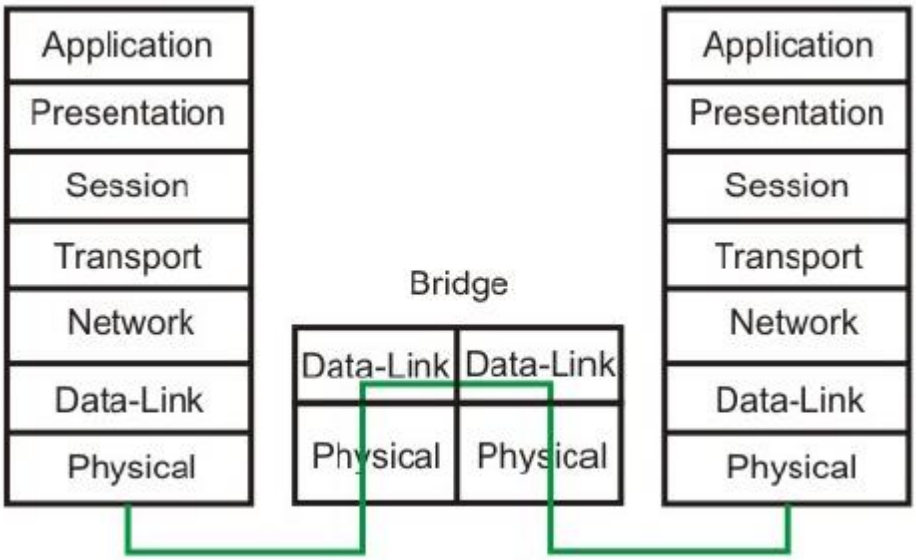



Figure 6.14 Information flow through a bridge

**Types of Bridges**

Bridges can be grouped into categories based on various product characteristics. Using one popular classification scheme, bridges are either

- Local Bridge
- Remote Bridge

Local bridges provide a direct connection between multiple LAN segments in the same area. Remote bridges connect multiple LAN segments in different areas, usually over telecommunications lines/Internet. Figure 6.15 illustrates these two configurations.

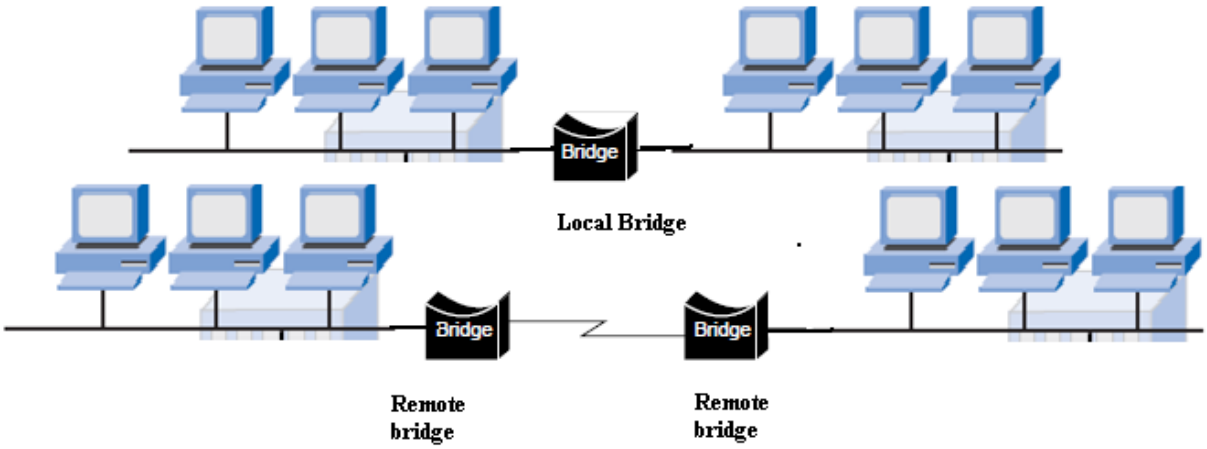



Figure 6.15 Local and Remote bridges

Depending on the manner in which bridges transmit data among networks, they are divided into two types:

- Transparent bridges
- Source route bridges.

**Transparent Bridges**

A transparent bridge is a device, in which the stations are completely unaware of the bridge is existence.

The transparent bridges must meet three criteria. They are

1. **Forwarding** - Frames must be forwarded from one station to another
2. **Learning** – The Bridge has using the dynamic table instead of static table. The dynamic table maps addresses to port automatically by learning from the frame movements.

The figure 11.6 illustrates the process of learning.

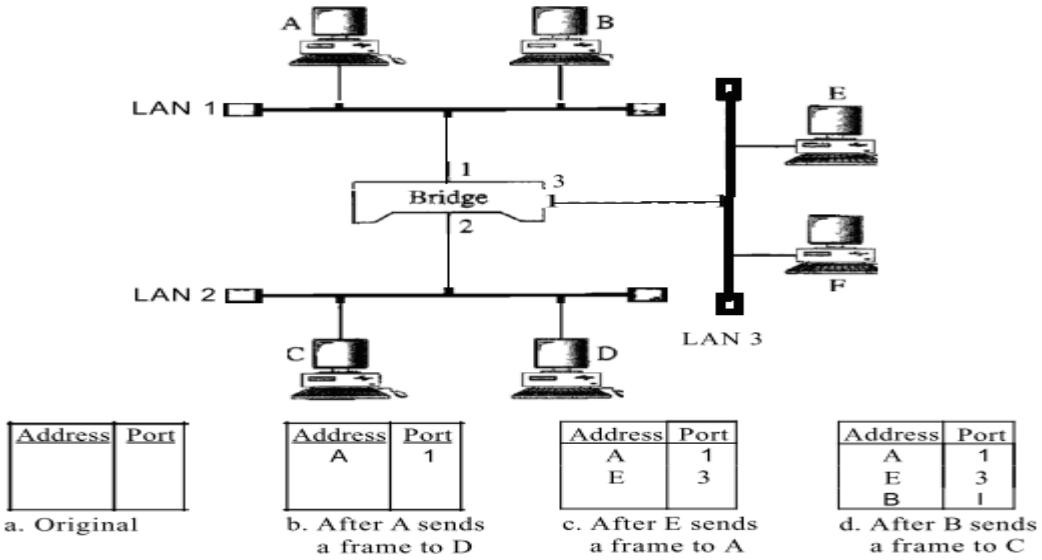



Figure 11.6 A learning bridge and the process of learning

- When station A sends a frame to station D, the bridge does not have any entry for either A or D. The frame floods the network by looking the source address and bridge leans that station A must be located on the LAN connected to port 1. It means that

frames destined for A. In future, must be sent out through port 1. The bridge adds this entry to its table.

- When station E sends a frame to station A, the bridge has an entry for A so it forwards the frame from port 1. It uses the source address of E to add a second entry to the table.
- When station B send a frame to C, the bridge has no entry for C, it floods the network and adds one more entry to the table
- The process of learning continues as the bridge forwards frames.

3. **Looping** - Loops in the system must be prevented.

The transparent-bridge algorithm fails when multiple paths of bridges and local-area networks (LANs) exist between any two LANs in the internetwork. The figure 11.7 illustrates the Bridging Loops can Result in inaccurate Forwarding and Learning in Transparent Bridging Environments.

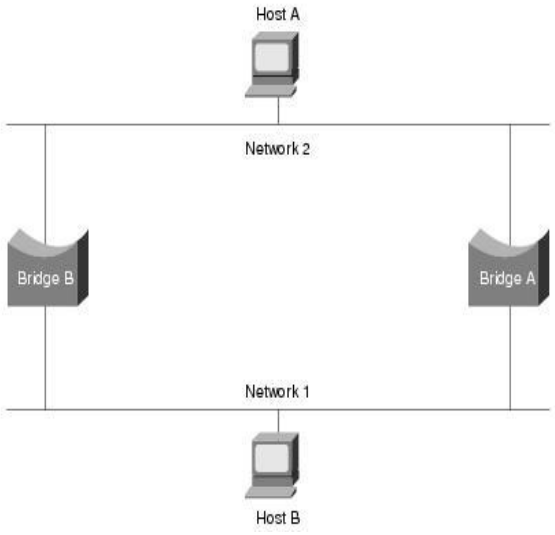



Figure 11.7 Loop problems in transparent bridge

Suppose that Host A sends a frame to Host B. Both bridges receive the frame and correctly learn that Host A is on segment 2. Each bridge then forwards the frame onto segment 1. Unfortunately, not only will Host B receive two copies of the frame (once from bridge 1 and once from bridge 2), but each bridge now believes that Host A resides on the same segment as Host B. When Host B replies to Host A's frame, both bridges will receive and subsequently filter the replies because the bridge table will indicate that the destination (Host A) is on the same network segment as the frame's source.

https://www.youtube.com/watch?v=dM32iiY4hiQ

**Source Route Bridges (SRBs)**

SRBs are so named because they assume that the complete source-to-destination route is placed in all inter-LAN frames sent by the source. SRBs store and forward the frames as indicated by the route appearing in the appropriate frame field. Figure 6.23 illustrates a sample SRB network. In Figure 6.23, assume that Host X wants to send a frame to Host Y. Initially, Host X does not know whether Host Y resides on the same or a different LAN. To determine this, Host X sends out a test frame. If that frame returns to Host X without a positive indication that Host Y has seen it, Host X must assume that Host Y is on a remote segment.

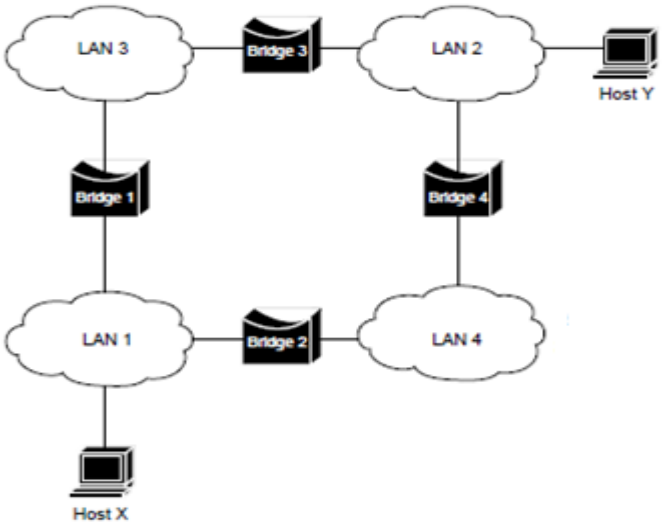



Figure 6.23 An SRB network contains LANs and bridges.

To determine the exact remote location of Host Y, Host X sends an *explorer* frame. Each bridge receiving the explorer frame (Bridges 1 and 2, in this example) copies the frame onto all outbound ports. Route information is added to the explorer frames as they travel through the internetwork. When Host X's explorer frames reach Host Y, Host Y replies to each individually, using the accumulated route information. Upon receipt of all response frames, Host X chooses a path based on some predetermined criteria.

In the example in Figure 25-1, this process will yield two routes:

- LAN 1 to Bridge 1 to LAN 3 to Bridge 3 to LAN 2
- LAN 1 to Bridge 2 to LAN 4 to Bridge 4 to LAN 2

Host X must select one of these two routes. The IEEE 802.5 specification does not mandate the criteria Host X should use in choosing a route, but it does make several suggestions, including the following:

- First frame received
- Response with the minimum number of hops
- Response with the largest allowed frame size
- Various combinations of the preceding criteria

In most cases, the path contained in the first frame received is used.

After a route is selected, it is inserted into frames destined for Host Y in the form of a *routing information field* (RIF). A RIF is included only in those frames destined for other LANs. The presence of routing information within the frame is indicated by setting the most significant bit within the Source Address field, called the *routing information indicator* (RII) bit.

Source-route bridging occurs primarily in Token Ring environments.

Source route bridging provides a more flexible routing scheme compared to the spanning tree algorithm used in transparent bridge, because the source node can select an appropriate path for the data to travel. However, source routing increases the traffic because of routing information generated by each source node whenever it wishes to send data across the networks. Higher network traffic decreases the network performance.

Bridges works at the data link layer and cannot be used across networks that use different network layer protocols. In addition, bridges cannot select an alternate path that the data packet should take if the original path encounters problems such as a device failure. Also, bridges cannot be used to selectively filter network traffic. For example, a bridge cannot be

used to prevent traffic from a particular node from entering a different network. These drawbacks are overcome by routers.

### 6.11.2 ROUTERS

A router is considered as a layer-3 relay that operates in the network layer, that is , it acts on network layer frames. Routers can connect two networks that use a common network layer protocol. For example, a router can connect two networks that use TCP/IP. Routers operate at the network layer of the OSI reference model. Some routers can be used to link two dissimilar LANs. These router incorporate the functionality of a bridge, and are called brouters. A router isolates LANs in to subnets to manage and control network traffic. However, unlike bridges it is not transparent to end stations. A schematic diagram of the router is shown on Figure 6.24. A router has four basic components: Input ports, output ports, the routing processor and the switching fabric. The functions of the four components are briefly mentioned below.

- Input port performs physical and data-link layer functions of the router.
- Output ports perform the same functions as the input ports, but in the reverse order.
- The routing processor performs the function of the network layer. The process involves table lookup.
- The switching fabric moves the packet from the input queue to the output queue by using specialized mechanisms. The switching fabric is realized with the help of multistage interconnection networks.
- Communication of a frame through a router is shown in Figure 6.25.

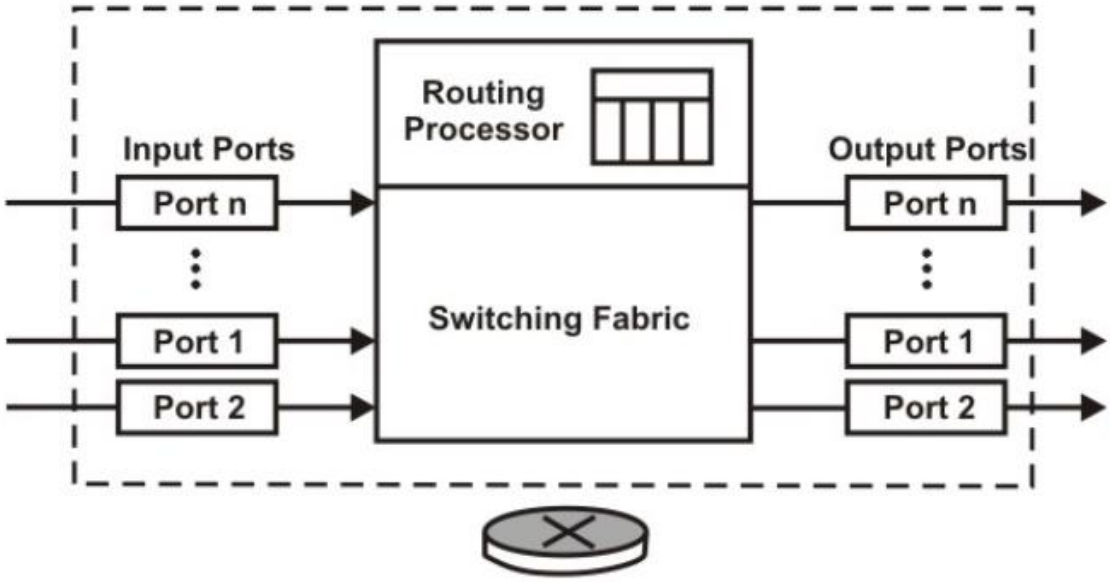



Figure 6.24 Schematic diagram of a router

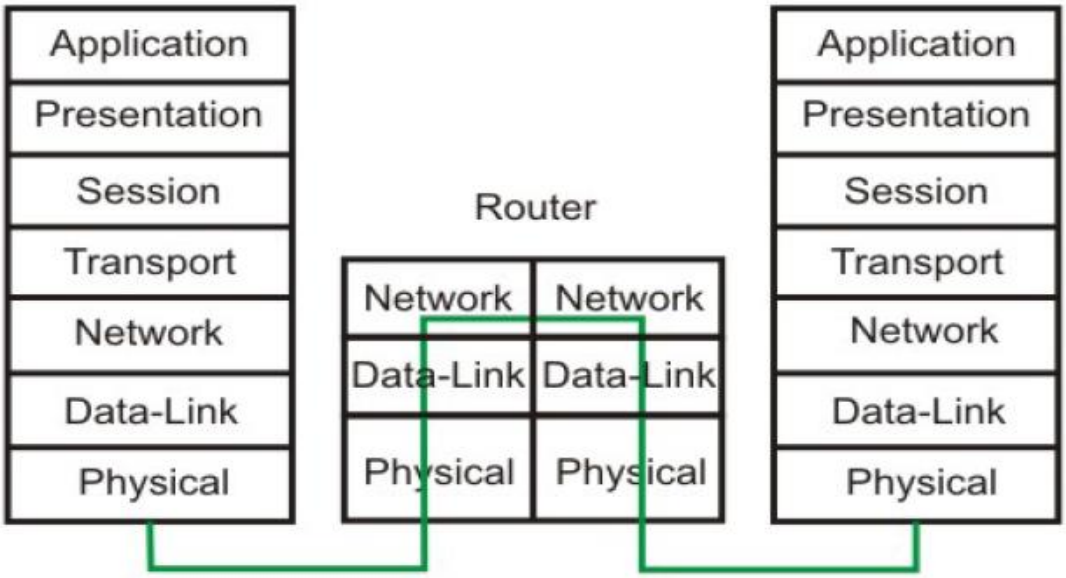



Figure 6.25 Communication through a router

Like bridges, routers also filter and forward information among different networks. However, routers work at network layer (layer 3), so they use the network addresses for filtering and forwarding information. In addition, routers can also provide additional features such as the ability to determine the best route for a destination and filtering information from a particular node.

Routers store the network addresses of computers in different networks in a table, called the routing table. In addition to the network addresses, the routing table also contains information on the path that should be used to transmit data, and any rules that have been defined for filtering network traffic. Whenever a router receives a packet, it checks for the network address of the destination. If the destination address is in a different network than the source address, it checks the routing table for the path the packet needs to take to reach the destination. If a route is found, the packet is forwarded to the specified path. Otherwise the data packet is filtered.

https://www.youtube.com/watch?v=JMEdUxYDVlo

**6.11.2.1 Routing Mechanics**

When multiple paths exist to transmit data across networks, the most appropriate path is selected either by the source node or the router. If the source node selects the path, the process is called node based routing. If the router determines the path, the process is called router based routing. The most appropriate path is usually the lowest cast path. The cost of the path is determined by using metrics, such as number of hops, percentage of data loss, or the network traffic on that route. The network administrator specifies the metrics for a route. The lowest-cast path is the route with the least metric value.

**a) Node-based Routing**

In node-based routing, the source node determines the path to be taken by the data packet to reach the destination node. This type of routing is also called source-based routing. Before sending the data packet, the source node compares the internetwork address of the destination node against the entries in its internal routing table to check if the destination node is part of the same network. If the destination node is in the same network, the source node directly sends data to the destination.

If the destination node is outside the network, the source node sends a packet to the destination node to trace the entire route. After obtaining the route information, the source node provides the entire path that should be taken by the data packet to reach the destination. In case of node-based routing, the routers perform a function similar to bridges. The routers do not decide the path of the data packets but forward the data packets depending on the path information included with the packet.

**b) Router-based Routing**

In this method of routing, the source node checks if the destination node is present in the same network. If the destination is not in the same network, the source node forwards the data packet to the router. The router than decides on the path to be taken by the data packet to reach the destination. The path is decided based on the entries in the routing table.

### 6.11.2.2 Routing Table

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

As illustrated in Figure 6.28, entries in the routing table usually consist of the following fields:

**Network ID** - The Network ID field contains the identification number for a network route or an internetwork address for a host route. **Network address** and **subnetmask** together describe the **Network id**. For example, destination **192.168.0.0** and submask **255.255.255.0** can be written as network id **192.168.0.0/24**.

**Forwarding (Next hop) Address** - The Forwarding Address field contains the address to which the packet is to be forwarded. The forwarding address can be a network interface card address or an internetwork address. For network IDs to which the end system or router is directly attached, the Forwarding Address field may be blank.

**Interface** - The Interface field indicates the network interface that is used when forwarding packets to the network ID. This is a port number or other type of logical identifier. For example, the interface for a 3COM EtherLink III network interface card may be referred to as ELNK3 in the routing table.

**Metric** - The Metric field indicates the cost of a route. If multiple routes exist to a given destination network ID, the metric is used to decide which route is to be taken. The route with the lowest metric is the preferred route.

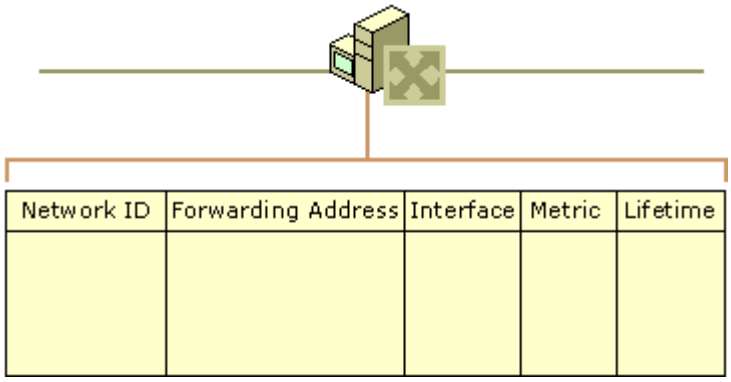
Metrics can indicate different ways of expressing a route preference:

- **Hop Count** - A common metric. Indicates the number of routers (hops) in the path to the network ID.
- **Delay** - A measure of time that is required for the packet to reach the network ID. Delay is used to indicate the speed of the path—local area networks (LAN) links have a low delay, wide area network (WAN) links have a high delay—or a congested condition of a path.
- **Throughput** - The effective amount of data that can be sent along the path per second. Throughput is not necessarily a reflection of the bit rate of the link, as a very

busy Ethernet link may have a lower throughput than an unutilized 64-Kbps WAN link.

- **Reliability** - A measure of the path constancy. Some types of links are more prone to link failures than others. For example, with WAN links, leased lines are more reliable than dial-up lines.

**Lifetime** - The Lifetime field indicates the lifetime that the route is considered valid. When routes are learned through the exchange of information with other routers, this is an additional field that is used. Learned routes have a finite lifetime..




https://www.youtube.com/watch?v=aMVu7WzZXIQ

**Figure 6.28 Routing Table Structure**

**Note** : The Lifetime field is typically not visible in routing tables.This list of fields is a representative list in the routing tables. Actual fields in the routing tables for different routable protocols may vary.

The routing tables are present on the nodes in a network, as well as the routers. There are two basic methods of building a routing table:

- **Static Routing** - A static routing table is created, maintained, and updated by a network administrator, *manually*. A static route to *every* network must be configured on *every* router for full connectivity. This provides a granular level of control over routing, but quickly becomes impractical on large networks. Routers will *not* share static routes with each other, thus reducing CPU/RAM overhead and saving bandwidth. However, static routing is *not fault-tolerant*, as any change to the routing infrastructure (such as a link going down, or a new network added) requires manual intervention. Routers operating in a purely static environment cannot seamlessly choose a better route if a link becomes unavailable.
- **Dynamic Routing** - A dynamic routing table is created, maintained, and updated by a *routing protocol* running on the router. Examples of routing protocols include RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and OSPF (Open Shortest Path First). Routers *do* share dynamic routing information with each other, which increases CPU, RAM, and bandwidth usage. However, routing protocols are capable of dynamically choosing a different (or better) path when there is a change to the routing infrastructure.

**Static vs. Dynamic Routing**

The following briefly outlines the advantages and disadvantages of static routing:

Advantages of Static Routing

- Minimal CPU/Memory overhead
- No bandwidth overhead (updates are not shared between routers)

- Granular control on how traffic is routed

Disadvantages of Static Routing

- Infrastructure changes must be manually adjusted
- No "dynamic" fault tolerance if a link goes down
- Impractical on large network

The following briefly outlines the advantages and disadvantages of dynamic routing:

Advantages of Dynamic Routing

- Simpler to configure on larger networks
- Will dynamically choose a different (or better) route if a link goes down
- Ability to load balance between multiple links

Disadvantages of Dynamic Routing

- Updates are shared between routers, thus consuming bandwidth
- Routing protocols put additional load on router CPU/RAM
- The choice of the "best route" is in the hands of the routing protocol, and not the network administrator

https://www.youtube.com/watch?v=Sa5XuO9H29M

**6.11.2.3 Routing Protocols**

A routing protocol is the language a router speaks with other routers in order to share information about the reachability and status of network. It includes a procedure to select the best path based on the reachability information it has and for recording this information in a route table. Regarding to select the best path, a routing metric will be applied and it is computed by a routing algorithm. The most commonly used routing protocols are:

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)

**Routing Information Protocol**

RIP is a standardized vector distance routing protocol and uses a form of distance as hop count metric. It is a distance vector. Through limiting the number of hop counts allowed in paths between sources and destinations, RIP prevents routing loops. Typically, the maximum number of hops allowed for RIP is 15. However, by achieving this routing loop prevention, the size of supporting networks is sacrificed. Since the maximum number of hop counts allowed for RIP is 15, as long as the number goes beyond 15, the route will be considered as unreachable.

RIP has four basic timers:

**Update Timer (default 30 seconds)** - defines how often the router will send out a routing table update.

**Invalid Timer (default 180 seconds)** - indicates how long a route will remain in a routing table before being marked as invalid, if no new updates are heard about this route.

**Hold-down Timer (default 180 seconds)** - specifies how long RIP will keep a route from receiving updates when it is in a hold-down state. In a hold-down state, RIP will not receive any new updates for routes until the hold-down timer expires. A route will go into a hold-down state for the following reasons:

- The invalid timer has expired
- An update has been received from another router; route goes into a 16 metric (or unreachable).
- An update has been received from another router; route goes into a higher metric than what it is currently using.

**Flush Timer (default 240 seconds)** -When no new updates are received about this route, flush timer indicates how long a route can remain in a routing table before getting flushed out

**Open Shortest Path First**

OSPF is a link state route exchange protocol that was standardized by the Internet Engineering Task Force to support scalable, resilient networks. A primary goal of OSPF is to reduce the frequency of update traffic. Another goal is fast convergence. Meeting these two goals results in a tradeoff, that OSPF consumes more memory and CPU resources on the router than distance vector protocols.

**SPF calculation**

Before running the calculation, it is required that all routers in the network to know about all the other routers in the same network and the links among them. The next step is to calculate the shortest path between each single router. For all the routers they exchange link-states which would be stored in the link-state database. Every time a router receives a link-state update, the information stores into the database and this router propagate the updated information to all the other routers. Below is a simple model of how the SPF algorithm works.

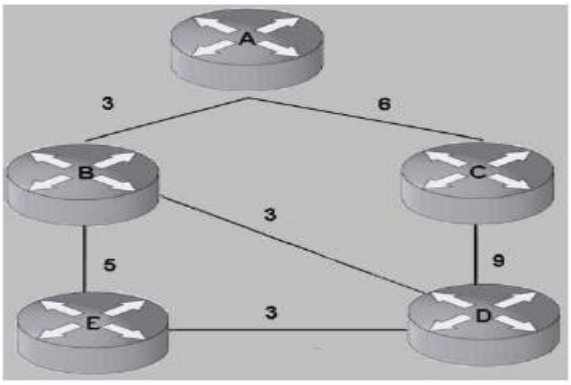



Figure 6.29 Simple structure of OSPF

A simple network formed by five routers; all the routers know about all the other routers and links. After all the paths are figured out, the path information are stored in the link database. The link database for the above model is : [A, B, 3], [A, C, 6], [B, A, 3], [B, D, 3], [B, E, 5], [C, A, 6], [C, D, 9], [D, C, 9], [D, B, 3], [D, E, 3] , [E, B, 5] and [E, D, 3]. Each term is referred to the originating router, the router connected to and the cost of the link between the two routers. Once the database of each router is finished, the router determines the Shortest Path Tree to all the destinations. (The shortest path in the SPF algorithm is called the Shortest Path Tree). The Dijkstra Shortest Path First is then running to determine the shortest path from a specific router to all the other routers in the network. Each router is put at the root of the Shortest Path Tree and then the shortest path to each destination is calculated. The accumulated cost to reach the destination would be the shortest path.

The cost (metric) of OSPF is the cost of sending packets across a certain interface. The formula to calcite the cost is: cost= 10000 0000 /bandwidth in bps. If the bandwidth is wider, the cost would be lower.

When the Shortest Path Tree is completed, the router will work on the routing table.

https://www.youtube.com/watch?v=hH8Fmlv5gOM

**6.11.3 GATEWAYS**

Gateway is a generic term used to represent devices that connect two dissimilar networks. Gateways can be hardware devices, software running on a computer, or a combination. Depending on the manner in which a gateway connects the networks, the following types of gateways are defined:

- Network gateways
- Protocol gateways
- Tunneling gateways

Network gateways connect different networks that use the same network layer protocols. Network gateways are usually routers, which contain routes to reach nodes outside the network to which the router is connected.

Protocol gateways connect networks that use different network layer protocols. For example, a protocol gateway can transmit data between a network that uses IPX/SPX and another network that uses TCP/IP protocol gateways convert the addressing format of the data packet from the source network to match the addressing format used in the destination network.

Protocol gateways are usually computers running protocol conversion software. The protocol conversion feature is inbuilt in the Microsoft Windows 2000 and Microsoft Windows NT 4.0 operating systems. Therefore, computers running these operating systems can be configured as protocol gateways.

Tunneling gateways encapsulate the data packet of the source network in a protocol that is recognized by the destination network. For example, if the source network uses IPX/SPX, and the destination network uses TCP/IP, the gateway encapsulates or wraps the IPX/SPX data with TCP/IP headers and trailers so that the destination network can recognize the data packet. The router on the destination network unwraps the data packet to retrieve the original data, which is then transmitted to the destination node. Gateways used in Virtual Private Networks are examples of tunneling gateways. Figure 6.30 shows a tunneling gateway transferring information between two networks.


Figure 6.30 Dissimilar networks connected tunneling gateways

### 6.12 WAN PROTOCOLS

WAN communication is significantly different from LAN communication largely due to the difference in the geographical area covered. In WANs the possibility of data getting corrupted, or being read by unauthorized sources is very high, so reliability is the primary concern. To ensure reliability of the data, the following Layer 2 protocols are commonly used in WAN:

- Point-to-Point Protocol (PPP)
- X.25
- Frame Relay
- Asynchronous Transfer Mode (ATM)

#### 6.12.1 Point-to-Point Protocol (PPP)

PPP originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP was originally devised as an encapsulation protocol for transporting IP traffic between two peers. It is a data link layer protocol (layer 2 in the OSI model) in the TCP-IP protocol suite. PPP also established a standard for the assignment and management of IP

addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link-quality testing, error detection, and option negotiation for such capabilities as network layer address negotiation and data compression negotiation. PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities. The broadband connection type used determine the use of Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA).
PPP is comprised of the following main components:

- **Link Control Protocol** - The LCP provided by PPP is versatile and portable to a wide variety of environments. The LCP is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link.
- **Network Control Protocol** - An extensible Link Control Protocol (LCP) for establishing, configuring, and testing and managing the data-link connections.
- **High Level Data Link Control (HDLC) Protocol** - The High Level Data Link Control (HDLC) protocol, an ISO data link layer protocol based on the IBM SDLC, ensures that data passed up to the next layer has been received exactly as transmitted (i.e. error free, without loss and in the correct order).

### 6.12.2 X.25

X.25 is a standard for WAN communications that defines how connections between user devices and network devices are established and maintained. X.25 is designed to operate effectively regardless of the type of systems connected to the network. It is typically used in the packet-switched networks (PSNs) of common carriers, such as the telephone companies. Subscribers are charged based on their use of the network. The devices used in an X.25 connection can be divided into the following categories:

- Data Terminal Equipment (DTE) – These are end systems that communicate across the X.25 network. They are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers.
- Data Circuit terminating Equipment (DCE) – Data communication Equipments (**DCEs)** are communications devices, such as modems and packet switches that provide the interface between DTE devices and a PSE, and are generally located in the carrier's facilities
- Packet Switching Exchange (PSE) – PSE is a term used to refer the equipment used by the telecommunications carrier to transmit information across different networks. **PSEs** are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another through the X.25 PSN.

In addition to these devices, another type of device called a Packet Assembler/Disassembler (PAD) is used if the DTE is not capable of implementing the X.25 protocol. PADs are located between DTE and DCE. The main functions of PAD are buffering, packet assembly, and packet disassembly. The PAD buffers data sent to or from the DTE device. It also assembles outgoing data into packets and forwards them to the DCE device. Finally, the PAD disassembles incoming packets before forwarding the data to the DTE.

Figure 6.31 shows an X.25 network illustrating relationships among DTE, DCE, and PSE.

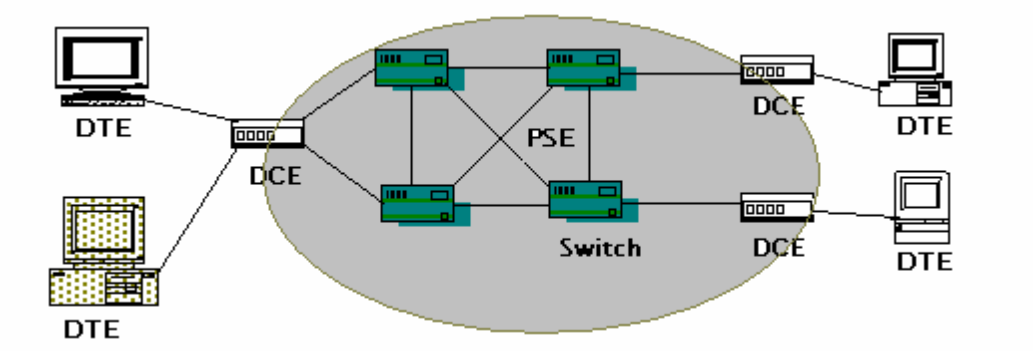



Figure 6.31 X.25 Network

X.25 protocol suite consists of the following protocols:

- **Packet Layer Protocol (PLP)** - The Packet Layer Protocol (PLP): describes the data transfer protocol in the packet switched network at the network layer (layer 3). PLP manages packet exchanges between DTE devices across virtual circuits.. The PLP operates in five distinct modes: call setup, data transfer, idle, call clearing, and restarting.
- **Link Access Procedure, Balanced (LAPB) Protocol** - Link Access Procedure, Balanced (LAPB) is a data link layer protocol used to manage communication and packet framing between data terminal equipment (DTE) and the data circuit terminating equipment (DCE) devices in the X.25 protocol stack.
- **X.21bis** – X.21bis operates at Layer 1 of the OSI reference model. X.21bis defines the electrical and mechanical procedures to use the physical medium.

### 6.12.3 FRAME RELAY

Frame Relay is an example of a packet-switched technology. It is an enhancement of the features offered by the X.25 protocol. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. It employs the following two packet techniques: a) Variable-length packets and

b) Statistical multiplexing.

It does not guarantee data integrity and discard packets when there is network congestion. In reality, it still delivers data with high reliability.

Frame Relay networks are typically deployed as a cost-effective replacement for point-to point private line, or leased line, services. The Frame Relay frame is transmitted to its destination through virtual circuits, which are logical paths from an originating point in the network to a destination point. Virtual circuits provide bidirectional communication paths from one terminal device to another and are uniquely identified by a data-link connection identifier (DLCI). A virtual circuit can pass through any number of intermediate switches located within the Frame Relay packet switched network.

**Frame Relay Devices**

Devices attached to a Frame Relay WAN fall into the following two general categories:

- Data terminal equipment (DTE)
- Data circuit-terminating equipment (DCE)

DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. In most cases, these are packet switches.

**Virtual Circuits**

Packet-switched networks may establish routes through the switches for particular end-to end connections. These routes are called virtual circuits (VC). A VC is a logical circuit created within a shared network between two network devices. Two types of VCs exist:

- **Permanent virtual circuit (PVC)**: A permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with establishing and terminating VCs, but they increase costs because of constant virtual circuit availability. PVCs generally are configured by the service provider when an order is placed for service.
- **Switched virtual circuit (SVC)**: A VC that is dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the VC between the source and destination devices, with SVC entries stored in lookup tables held in memory. Data transfer involves transmitting data between the devices over the VC, and the circuit termination phase involves tearing down the VC between the source and destination devices.

Figure 6.32 shows the components of a Frame Relay Network.

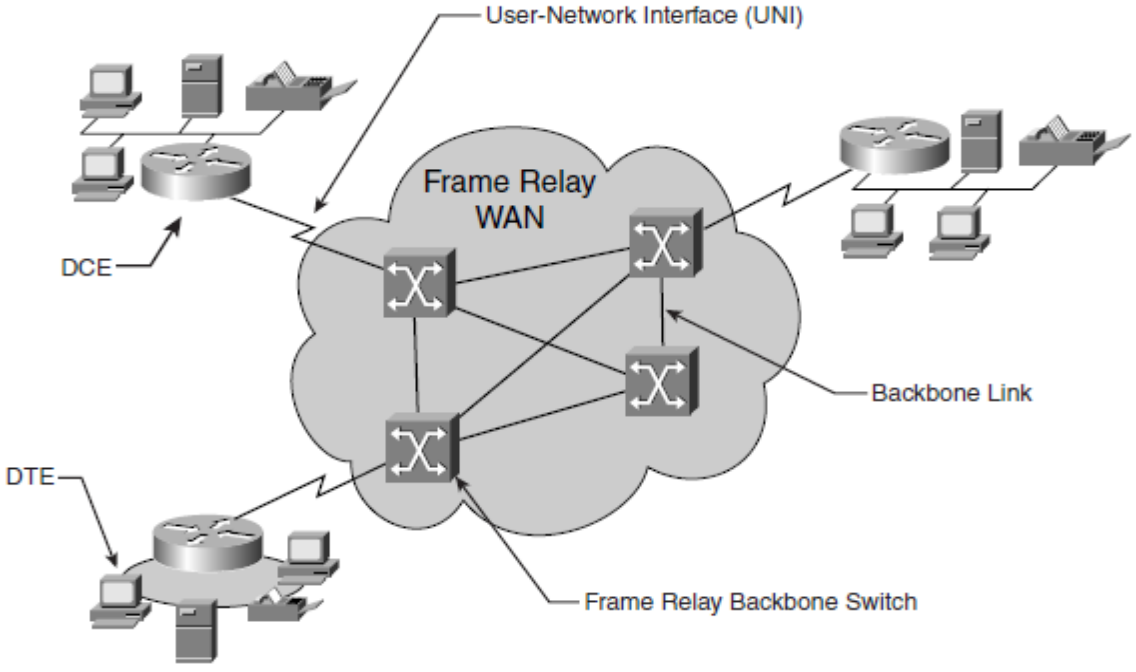



Figure 6.32 Frame Relay WAN

### 6.12.4 Asynchronous Transfer Mode (ATM)

ATM is a packet switching protocol that enables encoding of data traffic into small predetermined sized cells. The Asynchronous Transfer Mode (ATM) comprises a protocol

suite under the ATM reference model which establishes a mechanism to carry all traffic on a stream of fixed 53-byte packets (cells). A fixed-size packet can ensure that the switching and multiplexing function could be carried out quickly and easily. This protocol is based on connection-oriented technology. It operates by establishing between two end points, a virtual circuit even before exchange of data commences.

ATM is a connection-oriented technology, in which a connection is established between the two endpoints before the actual data exchange begins.

Asynchronous Transfer Mode (ATM) technology can transfer voice, video, and data through private and public networks. It is built on a cell based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes.

Like frame relay, ATM is a circuit-based network technology that also uses PVCs and SVCs. Figure 6.32 shows an ATM network.

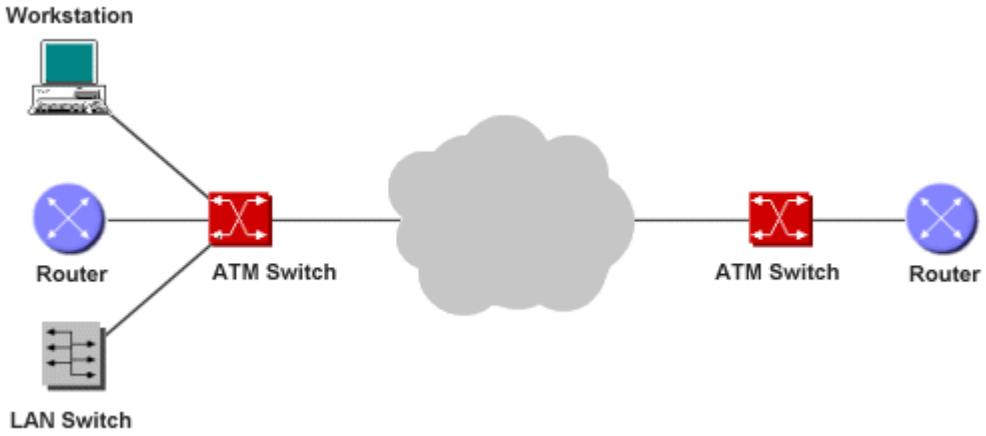



Figure 6.32 ATM Network

An ATM network is made up of an ATM switch and ATM endpoints. An ATM switch is responsible for cell transit through an ATM network. The job of an ATM switch is well defined. It accepts the incoming cell from an ATM endpoint or another ATM switch. It then reads and updates the cell header information and quickly switches the cell to an output interface towards its destination. An ATM endpoint (or end system) contains an ATM network interface adapter. Examples of ATM endpoints are workstations, routers, digital service units (DSUs), LAN switches, and video coder-decoders (Codec's).

**ATM Reference Model**

The ATM reference model is divided into three layers:

the ATM adaptation layer (AAL),

the ATM layer, and

the physical layer as shown in Figure 6.33.

The AAL interfaces the higher layer protocols to the ATM Layer, which relays ATM cells both from the upper layers to the ATM Layer and vice versa. When relaying information received from the higher layers, the AAL segments the data into ATM cells. When relaying information received from the ATM Layer, the AAL must reassemble the payloads into a format the higher layers can understand. This is called Segmentation and Reassembly (SAR). Different AALs are defined in supporting different types of traffic or service expected to be used on ATM networks.

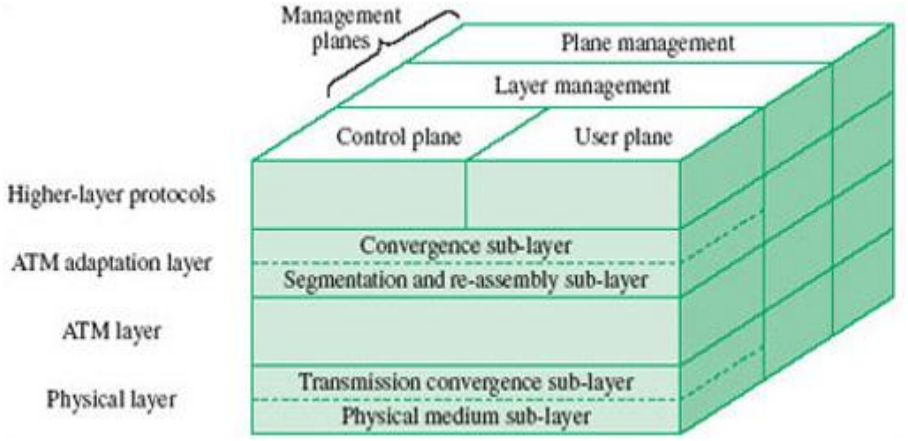



Figure 6.33 Layers of ATM reference model

The ATM layer is responsible for relaying cells from the AAL to the physical layer for transmission and from the physical layer to the AAL for use at the end systems. It determines where the incoming cells should be forwarded to, resets the corresponding connection identifiers and forwards the cells to the next link, buffers cells and handles various traffic management functions such as cell loss priority marking, congestion indication, and generic flow control access. It also monitors the transmission rate and conformance to the service contract (traffic policing).

The physical layer of ATM defines the bit timing and other characteristics for encoding and decoding the data into suitable electrical/optical waveforms for transmission and reception on the specific physical media used. In addition, it also provides a frame adaptation function, which includes cell delineation, header error check (HEC) generation and processing, performance monitoring, and payload rate matching of the different transport formats used at this layer.

https://www.youtube.com/watch?v=6x5WqEJCfIw

**6.13 Internet Tools and Services**

Following are the Internet Services:

- Domain Name System (DNS)
- Windows Internet Naming Service (WINS)
- Dynamic Host Configuration Protocol (DHCP)

**6.13.1 Domain Name System (DNS)**

Domain Name System (DNS) enables you to use hierarchical, friendly names to easily locate computers and other resources on an IP network. Although TCP/IP uses IP addresses to locate and connect to hosts (computers and other TCP/IP network devices), users typically prefer to use friendly names. IP addresses are hard to remember.

DNS is an Internet service that translates *domain names* into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to *198.105.232.4*.

Domain names are alphanumeric names for IP addresses for example www.dte.kar.nic.in, www.google.com, www.facebook.com.

The DNS client sends a request to the DNS server to map the host name to the corresponding IP address. The DNS server maps the host name to the corresponding IP address in its database and returns the IP address in its response.

- An application program on a host accesses the domain system through a DNS client, called the resolver. The part of the system sending the queries is called the resolver and is the client side of the configuration.
- Resolver contacts DNS server, called name server. The name server answers the queries.
- DNS server returns IP address to resolver, which passes the IP address to application.

**DNS Hierarchy**

The naming system on which DNS is based is a hierarchical and logical tree structure called the *domain namespace*. Organizations can also create private networks that are not visible on the Internet, using their own domain namespaces. Figure 6.34 shows part of the Internet domain namespace, from the root domain and top-level Internet DNS domains, to the second level domains.

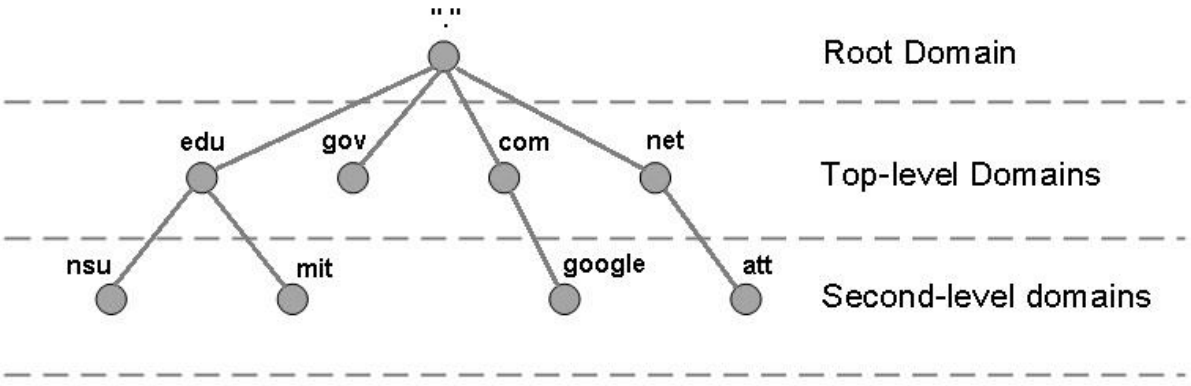



Figure 6.34 Domain Name Space

Each node in the DNS tree represents a DNS name. Some examples of DNS names are DNS domains, computers, and services. A DNS domain is a branch under the node.

Subdividing is an important concept in DNS. Creating subdivisions of the domain namespace and private TCP/IP network DNS domains supports new growth on the Internet and the ability to continually expand name and administrative groupings. Subdivisions are generally based on departmental or geographic divisions. For example, the reskit.com DNS domain might include sites in North America and Europe. A DNS administrator of the DNS domain reskit.com can subdivide the domain to create two subdomains that reflect these groupings: noam.reskit.com. and eu.reskit.com. Figure 6.35 shows an example of these subdomains.

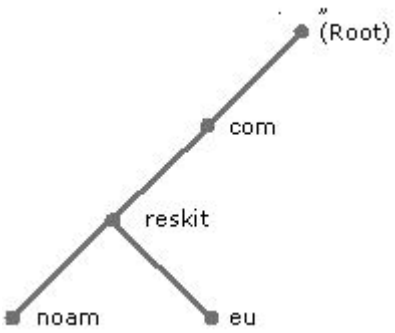



Figure 6.35 Subdomains

The most commonly used top-level DNS name components for organizations are:

| Top level name component | Descrption |
|---|---|
| .com | Commercial organizations |
| .edu | Educational Institutions |
| .gov | Government Institutions |
| .int | International organizations |
| .mil | Military groups |
| .net | Network support centers |
| .org | Nonprofit organizations |
| .arpa | Temporary ARPANET domain (obsolete |

**How does DNS work?**

DNS uses a client/server model in which the DNS server maintains a static database of domain names mapped to IP addresses. The DNS client, known as the resolver, performs queries against the DNS servers. DNS resolves domain names to IP address using these steps.

**Step 1.** A client (or "resolver") passes its request to its local name server. For example, the URL term www.idgbooks.com typed into Internet Explorer is passed to the DNS server identified in the client TCP/IP configuration. This DNS server is known as the local name server.

**Step 2.** If, as often happens, the local name server is unable to resolve the request, other name servers are queried to satisfy the resolver.

**Step 3.** If all else fails, the request is passed to more and more higher-level name servers until the query resolution process starts with the far-right term (for instance, com) or at the top of the DNS tree with root name servers.

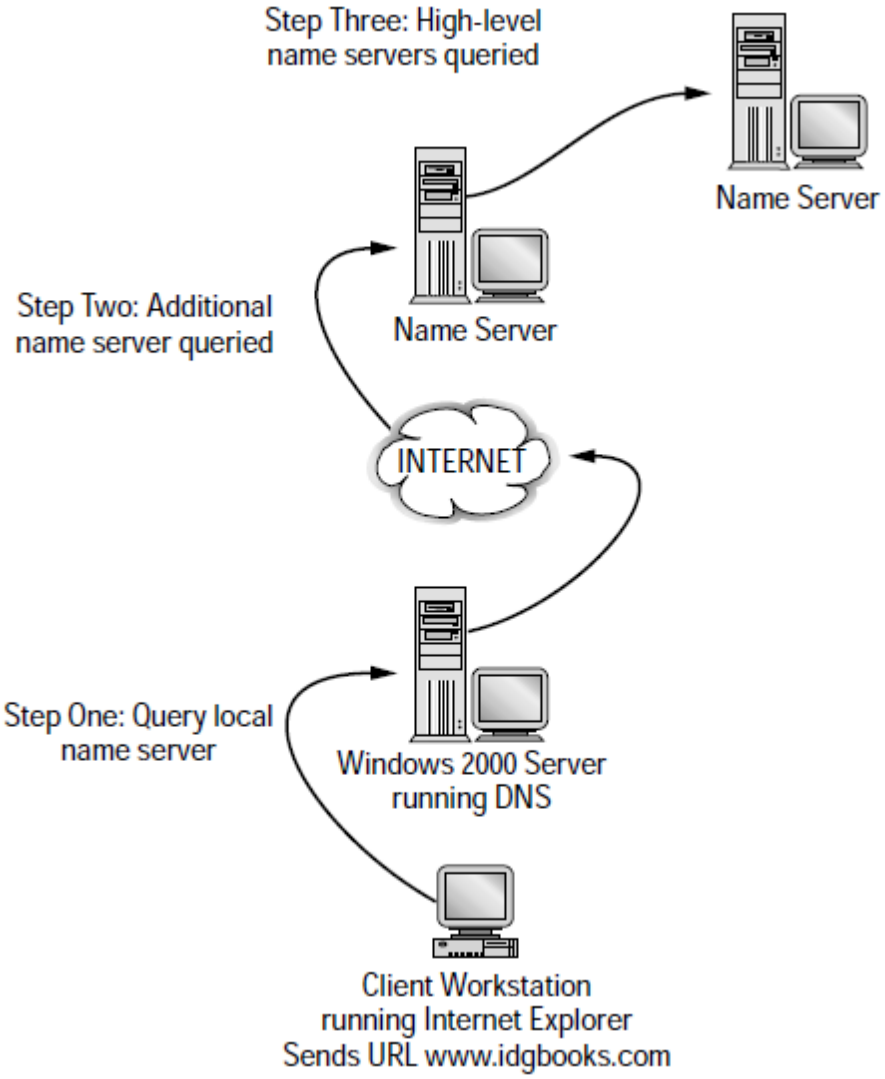



Figure 6.38 How DNS works

https://www.youtube.com/watch?v=72snZctFFtA

### 6.13.2 Windows Internet Naming Service (WINS)

WINS is used to map computer name or group name on the network to an IP address. Windows Internet Name Service (WINS) provides a distributed database for registering and querying dynamic mappings of NetBIOS names for computers and groups used on your network. WINS maps NetBIOS names to IP addresses and was designed to solve the problems arising from NetBIOS name resolution in routed environments. WINS is the best choice for NetBIOS name resolution in routed networks that use NetBIOS over TCP/IP. WINS was designed specifically to support NetBIOS over TCP/IP (NetBT). A NetBIOS (Network Basic Input/Output System) name is a unique identifier up to 15 characters long with a 16$^{th}$ character type identifier, that NetBIOS services use to identify resources on a network running NetBIOS over TCP/IP (NetBT). That is, a NetBIOS name is a 16-byte address that is used to identify a NetBIOS resource on the network.

WINS is designed to eliminate broadcasts and maintain a dynamic database by providing computer name-to-IP address mappings. A WINS system has two components: servers and clients.

- **WINS servers** - WINS servers maintain the database that maps a WINS Client IP address to its NetBIOS computer name. Broadcasts for NetBIOS type name resolutions are eliminated (or at least reduced) because the database on the WINS server may be consulted for immediate name resolution.
- **WINS clients.** A WINS client is a workstation that is configured with the WINS server(s) IP address(es). At system startup, the WINS client registers its name and IP address with the WINS server. When a WINS client needs a name resolved, the WINS server and its database are consulted. This results in fast and efficient name resolution.

**How Does WINS Work?**

In a typical scenario, the following occurs:

1. ClientA, which uses NetBIOS and is a WINS client, sends a name registration request to its configured WINS server (WINSA) when it starts up and joins the network. WINSA adds ClientA's NetBIOS name and IP address to the WINS database.
2. When ClientB needs to connect to ClientA by its name, it requests the IP address from the WINS server.
3. The WINS server locates the corresponding entry in its database and replies with ClientA's IP address.

**Name Registration**

Name registration is a WINS client requesting the use of a NetBIOS name on the network. When the WINS client starts, it sends a request to the WINS server. The request contains the NetBIOS name and the IP address of the client. The WINS server sends a successful registration message if no other WINS client is registered with the same NetBIOS name. The message includes:

- Registered NetBIOS name
- Time To Live (TTL)

If the NetBIOS name is already registered the WINS database checks whether the registration is still active or not. If the requesting NetBIOS name is registered in the database, then the WINS server sends a negative reply to the WINS client. However, if the NetBIOS name is not registered with the WINS server, a positive reply is sent to the WINS client.

As illustrated in the following Figure 6.39, a WINS client (HOST-C) sends a Name Registration Request directly to its configured WINS server, WINS-A.

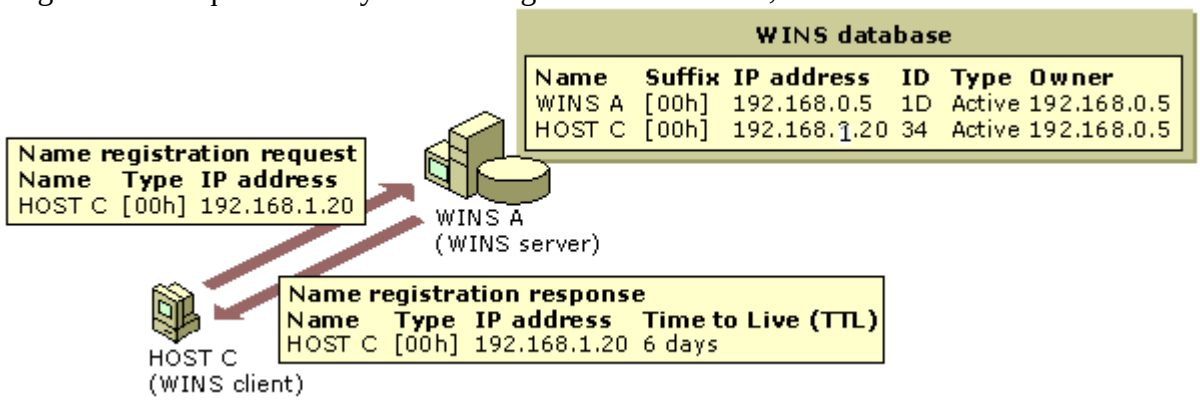



Figure 6.39 Name Registration

WINS-A can accept or reject the name registration request by issuing either a positive or negative name registration response to HOST-C. The action taken by WINS-A depends on several factors:

- Whether the name already exists in the server database at WINS-A
- If a record of the name exists, the state in the server database of the record at WINS-A might make a difference. Also, if the recorded IP address for the name is the same or different from the IP address of the requesting client, HOST-C.

**Renewing Names**

Periodic name renewal is required for WINS client computers to renew their NetBIOS name registrations with the WINS server. The WINS server treats name renewal requests similarly to new name registrations.

When a client computer first registers with a WINS server, the WINS server returns a message with a TTL value that indicates when the client registration expires or needs to be renewed. If renewal does not occur by that time, the name registration expires on the WINS server and the name entry is eventually removed from the WINS database. However, static WINS name entries do not expire, and therefore do not need to be renewed in the WINS server database.

The default **Renew interval** for entries in the WINS database is six days. Renewal occurs every three days for most WINS clients because WINS clients attempt to renew their registrations when 50 percent of the TTL value has elapsed.

A name must be refreshed before this interval ends, or it will be released. Names are refreshed by sending a name refresh request to the WINS server, as shown in Figure 6.40.

It is the responsibility of the client (HOST-C) to refresh its name before the Renew interval expires. If the WINS server, WINS-A, does not respond to the refresh request, the client, HOST-C, can increase the rate at which it attempts to refresh its name.

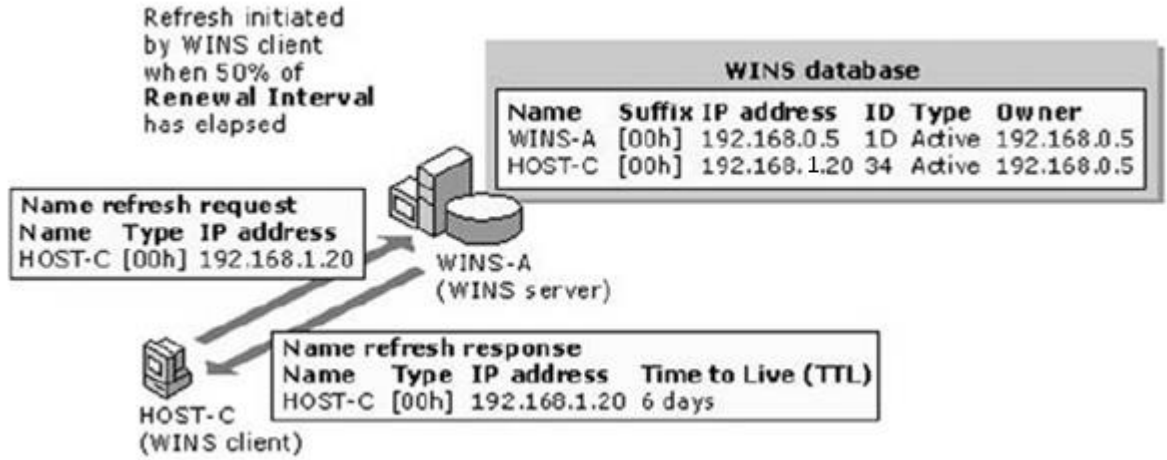



Figure 6.40 How clients refresh name in WINS

**Releasing Names**

Name release occurs when a WINS client computer finishes using a particular name, when a proper shutdown occurs. In releasing its name, a WINS client notifies its WINS server (or potentially other computers on the network) that it is no longer using its registered name.

As shown in the following Figure 6.41, when a WINS-enabled client (HOST-C) releases its name, the following steps occur:

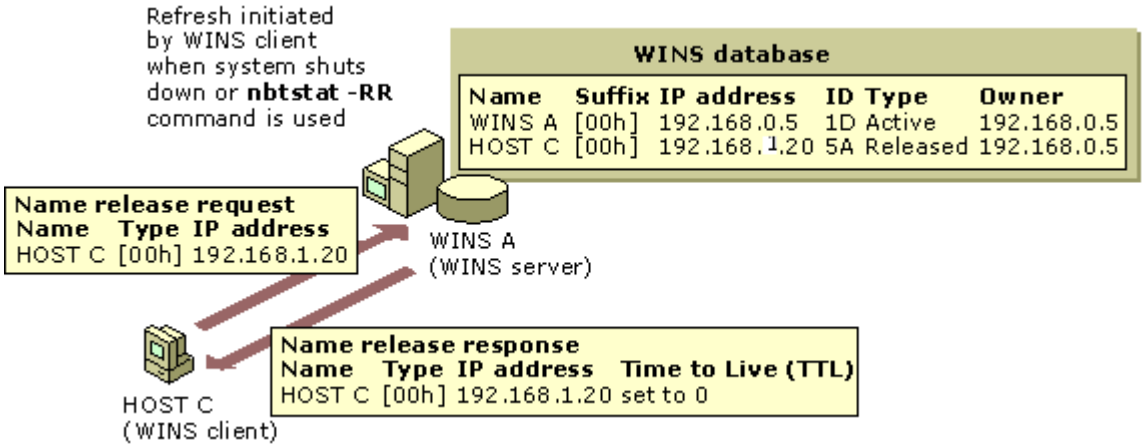



Figure 6.41 Releasing Names

1. The computer named HOST-C either shuts down properly or a user enters command initiating a name release request to be sent to the WINS server, WINS-A.
2. WINS-A marks the related database entry for HOST-C as *released*. If the entry remains released for a period of time, WINS-A marks the entry as *tombstoned*, updates the version ID for the entry, and notifies other WINS servers of the change.
3. WINS-A returns a release confirmation message to the WINS client, HOST-C.

**Comparison of WINS and DNS**

WINS and DNS are both name resolution services for TCP/IP networks. While WINS resolves names in the NetBIOS namespace, DNS resolves names in the DNS domain namespace. WINS primarily supports clients that run older versions of Windows and applications that use NetBIOS. Windows 2000, Windows XP, and Windows Server 2003 use DNS names in addition to NetBIOS names. Environments that include some computers that use NetBIOS names and other computers that use domain names must include both WINS servers and DNS servers.

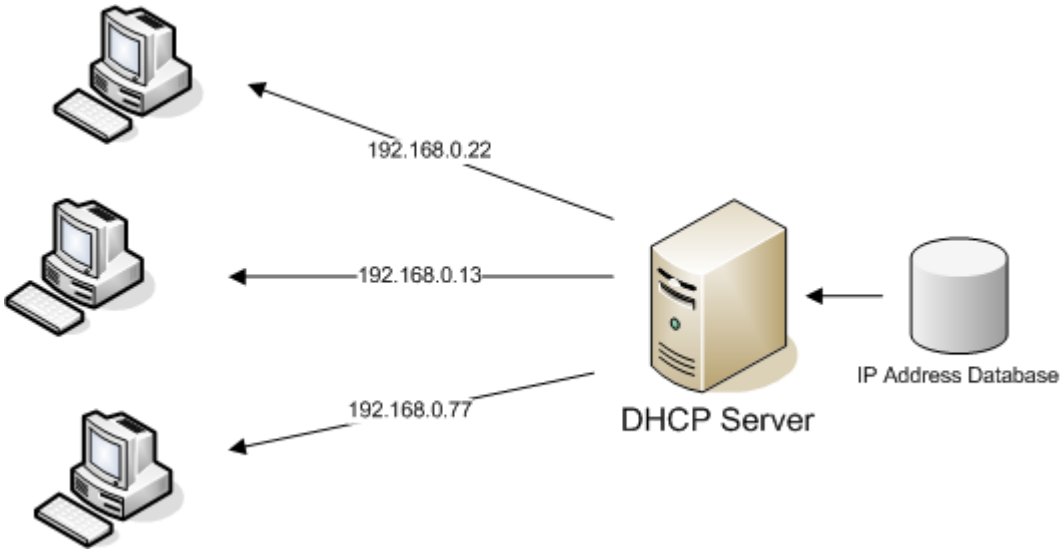
https://www.youtube.com/watch?v=b3t6CxZSwrk

### 6.13.3 Dynamic Host Configuration Protocol (DHCP)

To communicate on the Internet and private TCP/IP network, all hosts defined on the network must have IP addresses. DHCP uses a client-server model of communication.

Dynamic Host Configuration Protocol (DHCP) enables hosts on an IP network, called DHCP clients, to lease a temporary IP address from a DHCP server. DHCP functions at the application layer of the TCP/IP protocol stack. One of the primary tasks of the protocol is to *automatically assign IP addresses to DHCP clients*. A server running the DHCP service is called a DHCP server. The DHCP protocol automates the configuration of TCP/IP clients because IP addressing occurs through the system. You can configure a server as a DHCP server so that the DHCP server can automatically assign IP addresses to DHCP clients, and with no manual intervention. IP addresses that are assigned via a DHCP server are regarded as *dynamically assigned IP addresses*. The DHCP server assigns IP addresses from a predetermined IP address range(s), called a scope.

The implementation of DHCP is shown below




The functions of the DHCP server are outlined below:

- Dynamically assign IP addresses to DHCP clients.
- Allocate the following TCP/IP configuration information to DHCP clients:
  - Subnet mask information.
  - Default gateway IP addresses.
  - Domain Name System (DNS) IP addresses.
  - Windows Internet Naming Service (WINS) IP addresses.

DHCP uses User Datagram Protocol (UDP) as its transport protocol. DHCP messages that a client sends to a server are sent to well-known port 67 (UDP—Bootstrap Protocol and DHCP). DHCP Messages that a server sends to a client are sent to port 68.

**The DHCP Lease Process**

The DHCP lease process, also known as the DHCP negotiation process, is a fairly straight forward process. A lease is defined as the time period for which a DHCP server allocates a network address to a client. The lease might be extended (renewed) upon subsequent requests. If the client no longer needs the address, it can release the address back to the server before the lease is up. The server is then free to assign that address to a different client if it has run out of unassigned addresses.

A DHCP client initiates a conversation with a DHCP server when it is seeking a new lease. The DHCP conversation consists of a series of DHCP messages passed between the DHCP client and DHCP servers. The following Figure 6.42 shows an overview of this process when the DHCP server and DHCP client are on the same subnet.

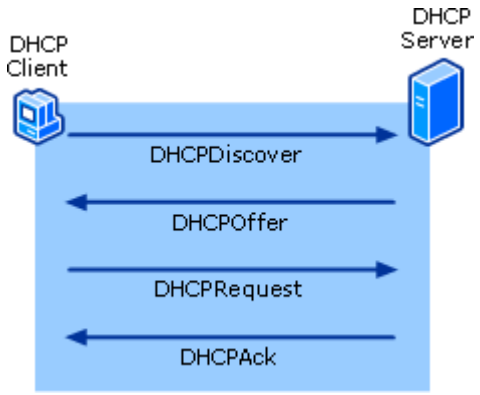



Figure 6.42 DHCP Lease process

The DHCP lease process is described below:

1. The *DHCPDiscover message* is sent from the client to the DHCP server. This is the message used to request an IP address lease from a DHCP server. The message is sent when the client boots up. The DHCP Discover message is a broadcast packet that is sent over the network, requesting for a DHCP server to respond to it.
2. The DHCP servers that have a valid range of IP addresses, sends an offer message to the client. The *DHCPOffer message* is the response that the DHCP server sends to the client. The DHCP Offer message informs the client that the DHCP server has an available IP address. The *DHCPOffer message* includes the following information:
   - IP address of the DHCP server which is offering the IP address.
   - MAC address of the client.
   - Subnet mask.
   - Length of the lease.
3. The client sends the DHCP server a *DHCPRequest message*. This message indicates that the client accepted the offer from the first DHCP server which responded to it. It also indicates that the client is requesting the particular IP address for lease. The client broadcasts the acceptance message so that all other DHCP servers who offered addresses
   can withdraw those addresses. The message contains the IP address of the DHCP server which it has selected.
4. The DHCP server sends the client a *DHCPAck message*. The DHCP Acknowledge message is actually the process of assigning the IP address lease to the client.
   https://www.youtube.com/watch?v=CgsRdy0iCiE

**Review Questions**

1. Differentiate LAN and WAN
2. List different WAN connectivity options
3. Explain how POTS is used to interconnect LANs
4. Explain leased lines WAN connectivity option
5. Explain ISDN
6. Differentiate BRI and PRI ISDN interfaces
7. Explain VSAT WAN connectivity option
8. Differentiate PAMA and DAMA VSAT access technologies
9. Explain microwave WAN connectivity

10. Explain radio wave transmission WAN connectivity
11. Write a note on VPN
12. Explain the working of VPN
13. List and explain different VPN protocols
14. Explain the role of bridges in WAN
15. List different types of bridges
16. Explain the role of a router in WAN
17. Explain routing mechanics
18. Define routing table. Explain its contents
19. Differentiate static and dynamic routing
20. Explain OSPF routing protocol
21. Write a note on gateways
22. List different WAN protocols
23. In brief explain PPP
24. In brief explain X.25 protocol
25. In brief explain frame relay protocol
26. In brief explain ATM protocol
27. Write a note on DNS
28. Explain working of DNS
29. Define WINS
30. Explain working of WINS
31. Explain WINS name registration process
32. Explain WINS name release process
33. Define DHCP. List its advantages
34. Explain DHCP lease process

## Activities

1. When setting up Frame Relay for point-to-point subinterfaces, which of the following must not be configured?

**A.** The Frame Relay encapsulation on the physical interface

**B.** The local DLCI on each subinterface

**C.** An IP address on the physical interface

**D.** The subinterface type as point-to-point

Answer is C

2 .A default Frame Relay WAN is classified as what type of physical network?

**A.** Point-to-point

**B.** Broadcast multi-access

**C.** Non-broadcast multi-access

Non-broadcast multipoint

Answer is C

3.ATM technology supports different types of connections between two

A. fields.
B. switches.
C. end users.
D. cells.

Answer is C

4.Technology that can be easily adapted for expansion in an organization is

A. ATM.
B. ATM LAN.
C. ATM WAN.
D. ATM MAN.

Answer is B

5.Data communication system spanning states, countries, or the whole world is
A.LAN
B.WAN
C.MAN
D .None of the mentioned
Answer is B

6..Name of domain is domain name of node at top of the

A. Sub Tree.
B. Main Tree.
C. Last Tree.

D. Bottom Tree.

Answer is A

7.Term that define registered hosts according to their generic behavior, is called

A. Generic Domains.
B. Main Domains.
C. Small Domains.
D. Sub-Domains.

Answer is A

8.100BASE-FX runs over which of the following media types?

A. Category 5e cable

B. UTP (Unshielded Twisted Pair) cable

C. MMF (Multimode Fiber) optic cable

D. RG-58 (Radio Grade) coaxial cable

**Answer is C**

9.Which one of the following topologies does FDDI (Fiber Distributed Data Interface) use?

A. Star

B. Bus

C. Mesh

D. Ring

**Answer is D**

10.Which of the following access methods does Ethernet use?

A. Token passing

B. Full duplex

C. CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance)

D. CSMA / CD (Carrier Sense Multiple Access / Collision Detection)

**Answer is D**

11. All of the following represents fault-tolerant strategies except:

A. Link redundancy

B. UPS (Uninterrupted Power Suplly)

C. Fail over

D. X 25

**Answer is D**

12. What should be used to automatically configure host computers for IP (Internet Protocol)?

A. DNS (Domain Name Service)

B. SNMP (Simple Network Management Protocol)

C. SMTP (Simple Mail Transfer Protocol)

D. DHCP (Dynamic Host Configuration Protocol)

**Answer is D**

13. In a Windows Server 2003 AD (Active Directory) network, which server stores information about resource objects?

A. Domain master

B. Domain tree

C. Domain controller

D. Domain configuration

**Answer: C**

14. A home user has enforced HTTPS (Hypertext Transfer Protocol Secure) access to a web server. After HTTPS is enforced, the web server is no longer accessible from the Internet, but can still be accessed by internal network users. What is causing this problem?

A. The users DNS (Domain Name Server) server is down.

B. The users web server IP (Internet Protocol) address has changed.

C. The users Internet router is blocking port 389.

D. The users Internet router is blocking port 443.

**Answer: D**

15. One of the purposes of a VLAN (Virtual Local Area Network) is to:

A. enforce better security

B. add more users

C. limit the network bandwidth

D. reduce the number of subnets

**Answer: A**

16.What is the purpose of the DHCP server?

A - to provide storage for email

B - to translate URLs to IP addresses

C - to translate IPv4 addresses to MAC addresses

D - to provide an IP configuration information to hosts

Answer**: D**

17.how is the message sent from **PC2** attempts to contact the DHCP Server when its first powers on?

A - Layer 3 unicast

B - Layer 3 broadcast

C - Layer 3 multicast

D - Without any Layer 3 encapsulation

Answer **is B**

18. Frame Relay networks offer an option called

A. Voice Over For Relay.
B. Voice Over Fine Relay.
C. Voice On Frame Relay.
D. Voice Over Frame Relay.

Answer**: D**

19. Domain, which is used to map an address to a name is called

A. Generic Domains.
B. Inverse Domain.
C. Small Domains.
D. Sub-Domains.

Answer **is B**

20.VSAT stands for

A. Very Small Aperture Terminal
B. Varying Size Aperture Terminal
C. Very Small Analog Terminal
D. None of the above

Answer **is A**