CHAPTER ONE
Data communication Basics

1.1. Data communication

Data communication is the process of sharing ideas, information and messages with others in a particular time and place. 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").

It refers to the exchange of data between two or more parties. Parities may refer to person' s organization or devices or machines. Computer communication is a process in which two or more computers or devices transfer or transmit data, instructions, and information. In other words, computer data communications is the movement of computer information from one point to another by means of electrical or optical transmission systems (called networks).

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

Data communication is a subset of telecommunication involving the transmission of data to and from computers and components of computer systems. More specifically, data Communication is the exchange of data (in the form of 0' s and 1' s) between two or more devices (computers) via some form of the transmission medium such as wires, coaxial cables, fiber optics, or radiated electromagnetic waves such as broadcast radio, infrared light, microwaves, and satellites.

For data communication to occur, the communicating devices must be a part of a communication system made up of some specific kind of hardware and software. This type of a system is known as a data communication system. The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

i. **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.
ii. **Accuracy**. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
iii. **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.
iv. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components of Data Communication System

A data communications system has five components as it is shown on Fig 1.1.

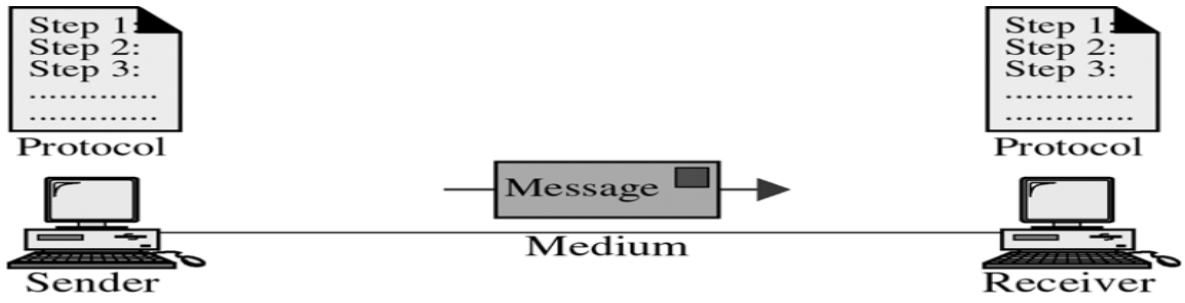


Fig 1.1 Five components of data communication

a. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
b. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
c. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
d. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
e. 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.

A modified communication system

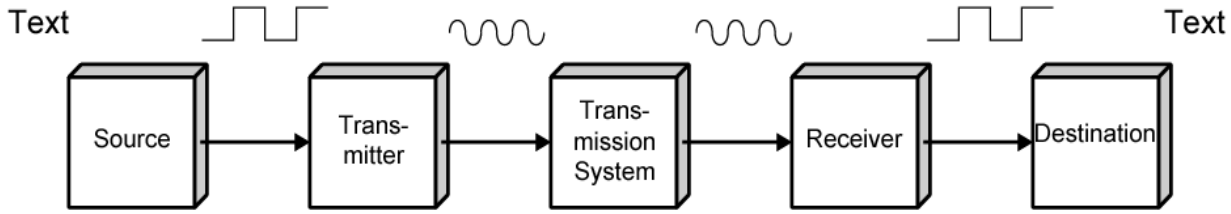


Fig 1.2 Elements of a modified communication system

1.2. Data representation

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

Text: In data communications, text is represented as a bit pattern, a sequence of bits (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. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

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

Images: Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution.* After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black-and-white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.

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. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

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

Data flow

Communication between two devices can be simplex, half-duplex, or full-duplex.

In **simplex mode,** the communication is unidirectional. Only one of the two devices on a link can transmit; the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction. An example of simplex transmission is the signal sent from the cable TV station to the home television.

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. 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. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

In **full-duplex mode** (also called *duplex*), both stations can transmit and receive simultaneously. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions. One common example of full-duplex communication is the 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. The capacity of the channel, however, must be divided between the two directions.

1.3. Digital data transmission

In communication system, data is transmitted from one point to another by means or form of electrical signal 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. For transmission, data needs to be changed to signals.

There are two types of signals that can travel over varies transmission media. These signals are: Analog signals and Digital signals.

Analogue signal: - is continuously varying electromagnetic waves that may be propagated over a variety of media and what we encounter every day of our life. Speech is analogue signal, and varies in amplitude (volume) and frequency (pitch). Main characteristics of analogue signals are amplitude, frequency and phase.

Digital signal: - are the languages of modern day computers. Digital signals normally comprise only two states. These are expressed as on or off, 1 or 0 respectively.

Data or information can be stored in two ways, analog and digital. For a computer to use that data is must be in discrete digital form. To transmit data digitally or analogically it needs to be first converted to digital or analog form.

1.4. Signal Encoding Techniques

Basic terminologies

Data rate/bit rate - defines the number of data elements (bits) sent in 1s. The unit is bits per second (bps).
Signal rate- the number of signal elements sent in 1s. The unit is the baud. The signal rate is sometimes called the **pulse rate,** the **modulation rate,** or the **baud rate.**
Amplitude refers to the strength of a signal, usually measured in volts.
Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.
Frequency refers to the number of periods in 1 s. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverse of period i.e. ***f=1/T and T=1/f.*** Frequency is formally expressed in Hertz (Hz), which is cycle per second. 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.
Phase/phase shift - describes the position of the signal relative to time 0. If we think of the signal 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.
Bandwidth- The range of frequencies contained in a composite signal is its bandwidth**.** The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 − 1000, or 4000Hz.
One goal in data communications is to increase the data rate while decreasing the signal rate. Increasing the data rate increases the speed of transmission; decreasing the signal rate decreases the bandwidth requirement.
Bandpass channel —a channel with a bandwidth that does not start from zero. This type of channel is more available than a low-pass channel. If the available channel is a bandpass channel, we cannot send the digital signal directly to the channel; we need to convert the digital signal to an analog signal before transmission.
Low-pass channel – is a channel that passes frequencies between 0 and *f*.
Baseband transmission-is a transmission of digital or analog signal without modulation, using a low-pass channel.
Broadband transmission- is a transmission of signals using modulation of a higher frequency signal. The term implies a wide-bandwidth data combined from different sources.

1.4.1. Digital data to digital signal conversion

In this part we are going to see how to convert digital data into digital signals. It can be done in three ways; line coding, block coding and scrambling. For all communications, line coding is necessary whereas block coding and scrambling are not mandatory.

A. Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in digital format, which is a binary bit. It is represented (stored) internally as series of 1s and 0s. At the sender, digital data are encoded into a digital signal; at the receiver, the digital data are recreated by decoding the digital signal.

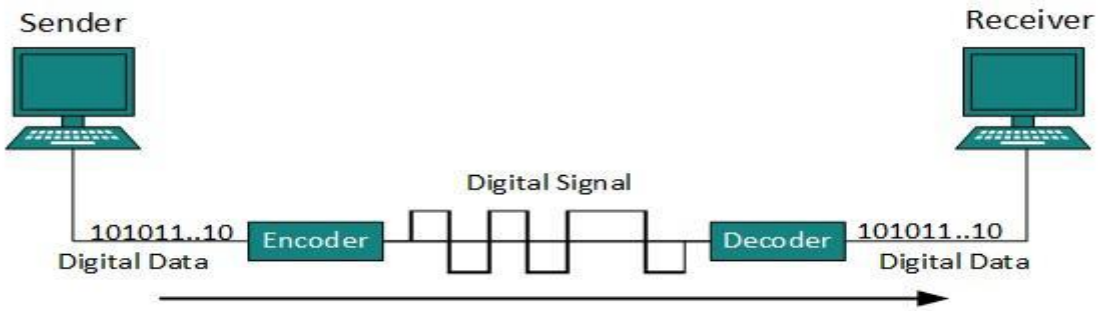


Fig 1.3 Line coding and decoding

Digital signals which represents digital data, represented as discrete signals. Three types of line coding schemes are available: unipolar, polar and bi-polar.

i. Unipolar encoding

Unipolar encoding scheme uses single voltage level to represent data. In this case, to represent binary 1 high voltage is transmitted and to represent 0 no voltage is transmitted. It is also called Unipolar-Non-Return-to-Zero, because there is no rest condition i.e. it either represents 1 or 0.

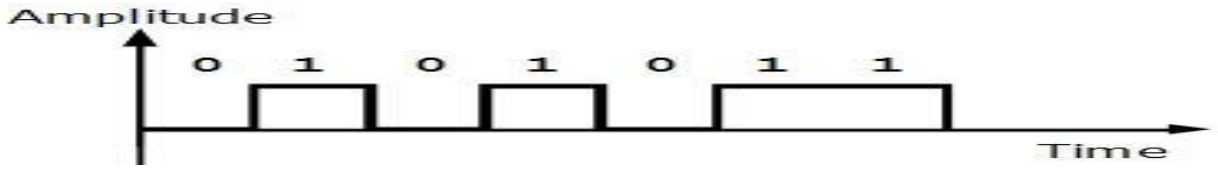


Fig 1.4 Unipolar NRZ Encoding

ii. Polar encoding

In polar encoding schemes multiple voltage levels are used to represent binary values. Polar encodings are available in four types:

a. Polar-NRZ (Non-Return to Zero)

It uses two different voltage levels to represent binary values, generally positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition. NRZ scheme has two variants: NRZ-L and NRZ-I.

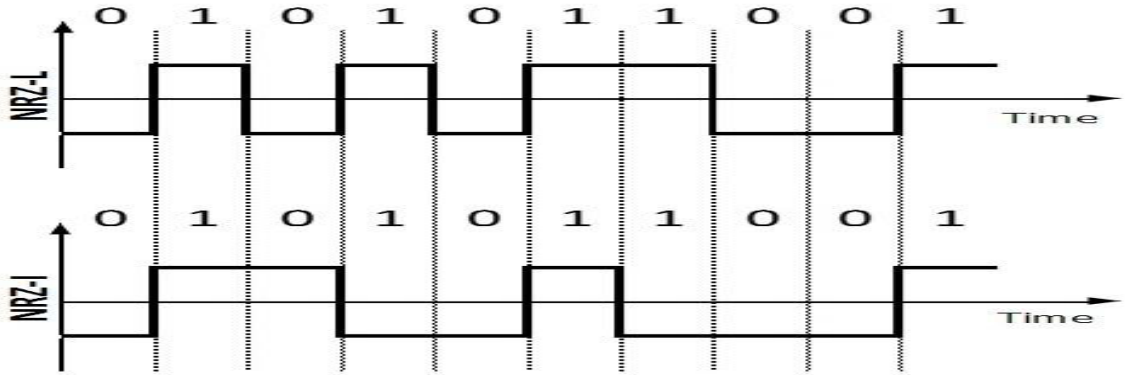


Fig 1.5 Polar-NRZ schemes: NRZ-L and NRZ-I

NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

b. RZ (Return to Zero)

Problem with NRZ was the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receive is clock are not synchronized.

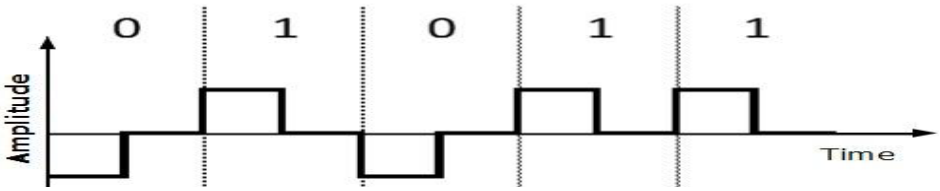


Fig 1.6 Return-to-Zero Encoding

RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

c. Manchester

This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. There is always a transition at the middle of the bit and changes phase when a different bit is encountered.

d. Differential Manchester

This encoding scheme is a combination of RZ and NRZ-I. There is a transition at the middle of the bit but changes phase only when 1 is encountered.

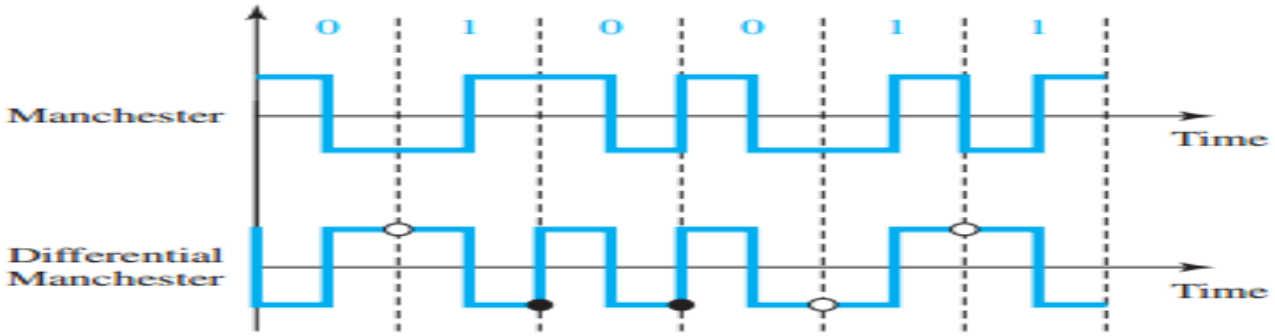


Fig 1.7 Manchester and Differential Manchester encoding

iii. Bipolar encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. There are two schemes available for bipolar encoding: AMI and Pseudoternary.

a. AMI (Alternate Mark Inversion)

Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.

b. Pseudoternary

Zero voltage represents binary 1 and bit 0 is represented by altering positive and negative voltages.

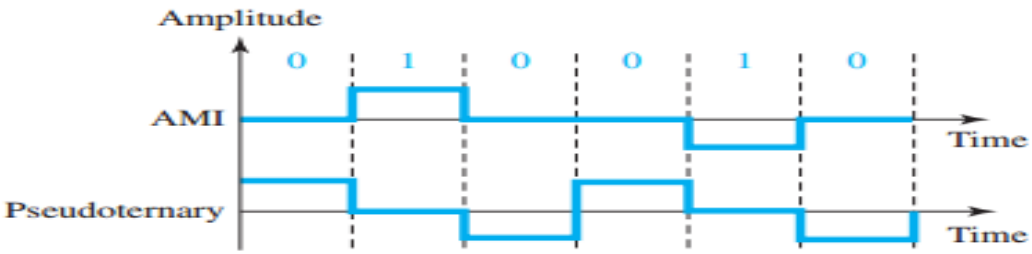


Fig 1.8 Bipolar schemes: AMI and Pseudoternary

B. Block Coding

To ensure accuracy of data frame received, redundant bits are used. For example, in even parity one parity bit is added to make the count of 1s in the frame even. This way the original numbers of bits are increased. It is called Block Coding. Block coding is represented by slash notation, mB/nB, that is m-bit block is substituted with n-bit block where n > m. Block coding involves three steps: division, substitution and combination. After block coding is done it is line coded for transmission.

1.4.2. Analog data to digital data conversion

Microphones creates analog voice and camera creates analog videos, which here in our case is treated is analog data. To transmit this analog data over digital signals we need an analog to digital conversion. Analog data is waveform continuous stream of data whereas digital data is discrete. To convert analog wave into digital data we use Pulse Code Modulation and Delta Modulation.

A. Pulse Code Modulation

It is one of the most commonly used methods to convert analog data into digital form. It involves three steps: Sampling, Quantization and Encoding.

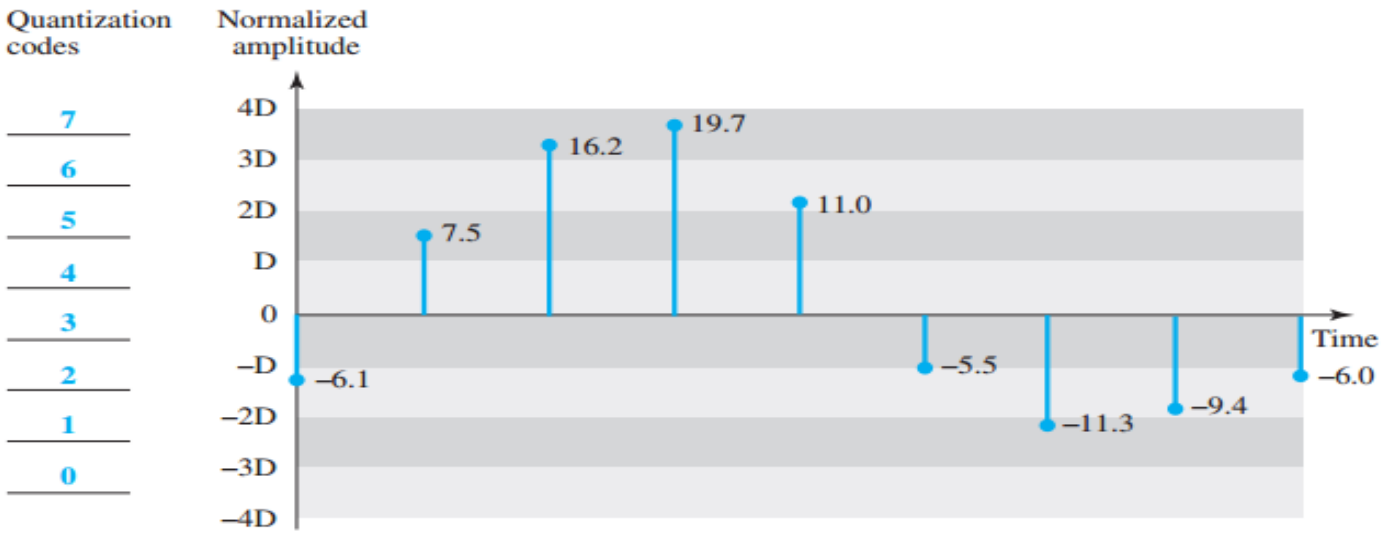
Sampling: The analog signal is sampled every T interval. Most important factor in sampling is the rate on which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal. To elaborate the theorem, first, we can sample a signal only if the signal is band-limited. In other words, a signal with an infinite bandwidth cannot be sampled. Second, the sampling rate must be at least 2 times the highest frequency, not the bandwidth. If the analog signal is low-pass, the bandwidth and the highest frequency are the same value. If the analog signal is bandpass, the bandwidth value is lower than the value of the maximum frequency. Nyquist sampling rate: $f_s=2f$*; where f is the highest frequency.*

Quantization: is a method of assigning integral values in a specific range to sampled instances. The result of sampling is a series of pulses with amplitude values between the maximum and minimum amplitudes of the signal. The set of amplitudes can be infinite with non integral values between the two limits. These values cannot be used in the encoding process. The following are the steps in quantization:

1. We assume that the original analog signal has instantaneous amplitudes between Vmin and Vmax.
2. We divide the range into L zones, each of height Δ (delta). $\Delta=(V\text{max} - V\text{min})/L$
3. We assign quantized values of 0 to $L-1$ to the midpoint of each zone.
4. We approximate the value of the sample amplitude to the quantized values.

As a simple example shown in Fig 1.9, assume that we have a sampled signal and the sample amplitudes are between −20 and +20 V. We decide to have eight levels (L = 8). This means that Δ = 5V.

Encoding: In encoding, each approximated value is then converted into binary format.



Normalized PAM values	–1.22	1.50	3.24	3.94	2.20	–1.10	–2.26	–1.88	–1.20
Normalized quantized values	–1.50	1.50	3.50	3.50	2.50	–1.50	–2.50	–1.50	–1.50
Normalized error	–0.38	0	+0.26	–0.44	+0.30	–0.40	–0.24	+0.38	–0.30
Quantization code	2	5	7	7	6	2	1	2	2
Encoded words	010	101	111	111	110	010	001	010	010

Fig 1.9 Quantization and encoding of a sampled signal

- Normalized PAM values=(Actual amplitude/Δ)
- Normalized quantized values=quantization value from the middle of each zone
- Normalized error= Normalized quantized values- Normalized PAM values

(Read Behrouz A. Forouzan.(2013).Data communication and networkings,5th edition. Section 4.2.1)

B. Delta Modulation

PCM is a very complex technique whereas DM is the simplest modulation technique. PCM finds the value of the signal amplitude for each sample; DM finds the change from the previous sample.

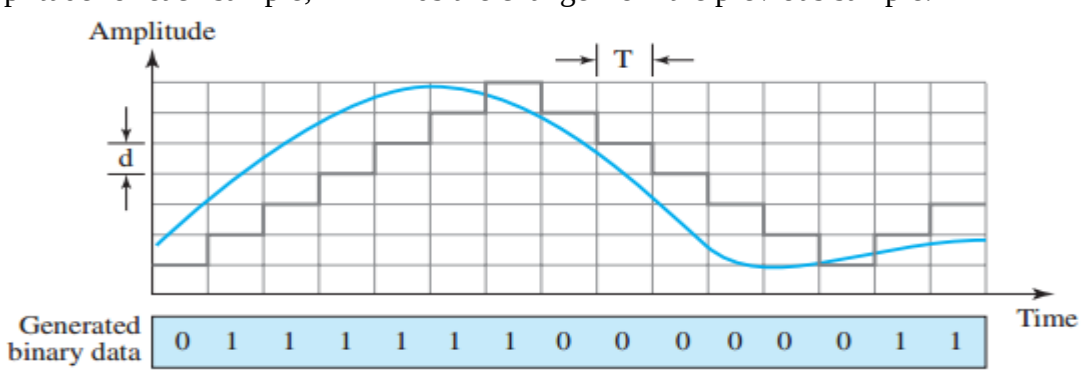


Fig 1.10 Delta modulation

1.4.3. Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data, i.e. binary data. An analog is characterized by its amplitude, frequency and phase. There are three kinds of digital-to-analog conversions possible:

A. Amplitude shift keying

In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.

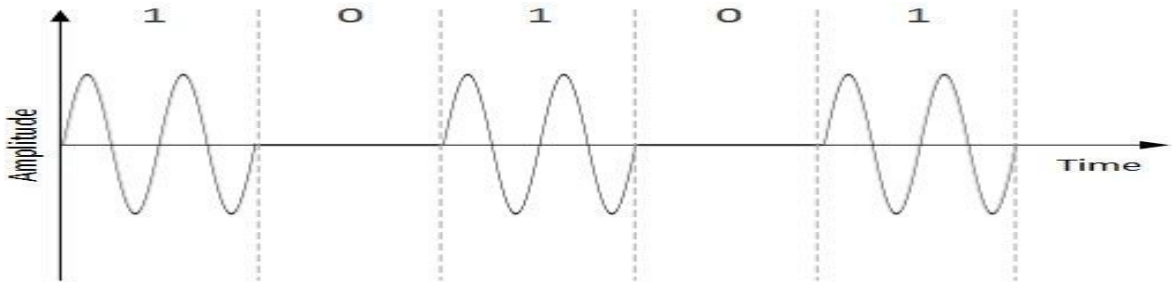


Fig 1.11 Amplitude Shift Keying

When binary data represents digit 1, the amplitude is held otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

B. Frequency shift keying

In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.

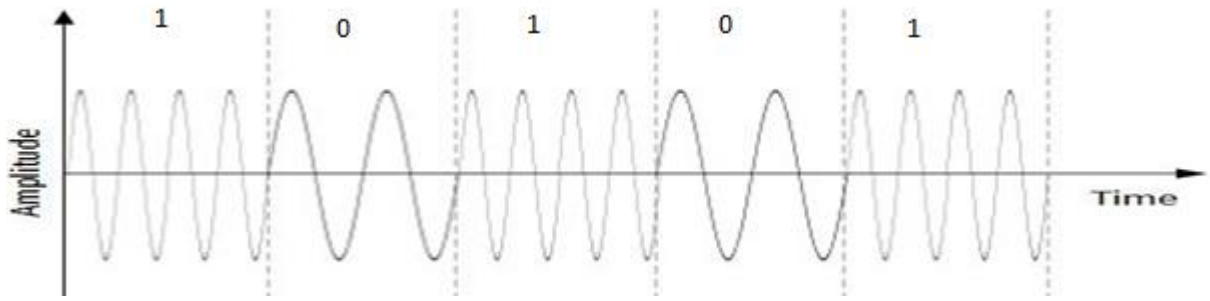


Fig 1.12 Frequency shift keying

This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

C. Phase shift keying

In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.

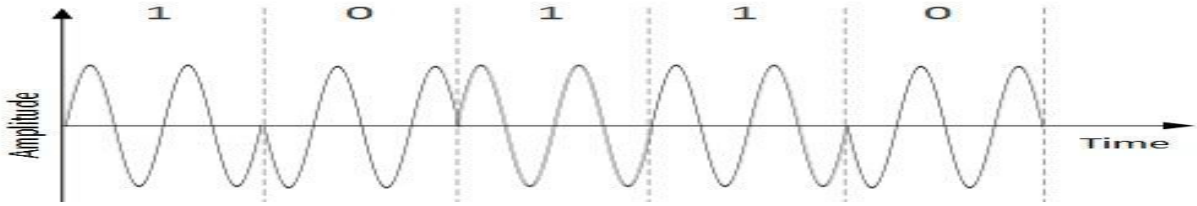


Fig 1.13 Phase shift keying

When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

D. Quadrature phase shift keying

QPSK alters the phase to reflect 2 binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

1.4.4. Analog-to-analog conversion

Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways: Amplitude, frequency and phase modulation.

A. Amplitude modulation

In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.

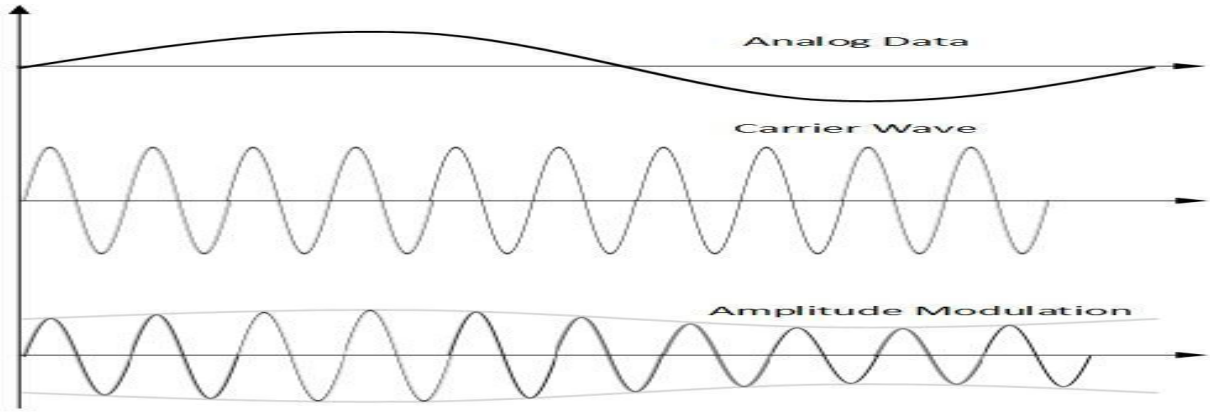


Fig 1.14 Amplitude Modulation

Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data. The frequency and phase of carrier signal remain unchanged.

B. Frequency modulation

In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).

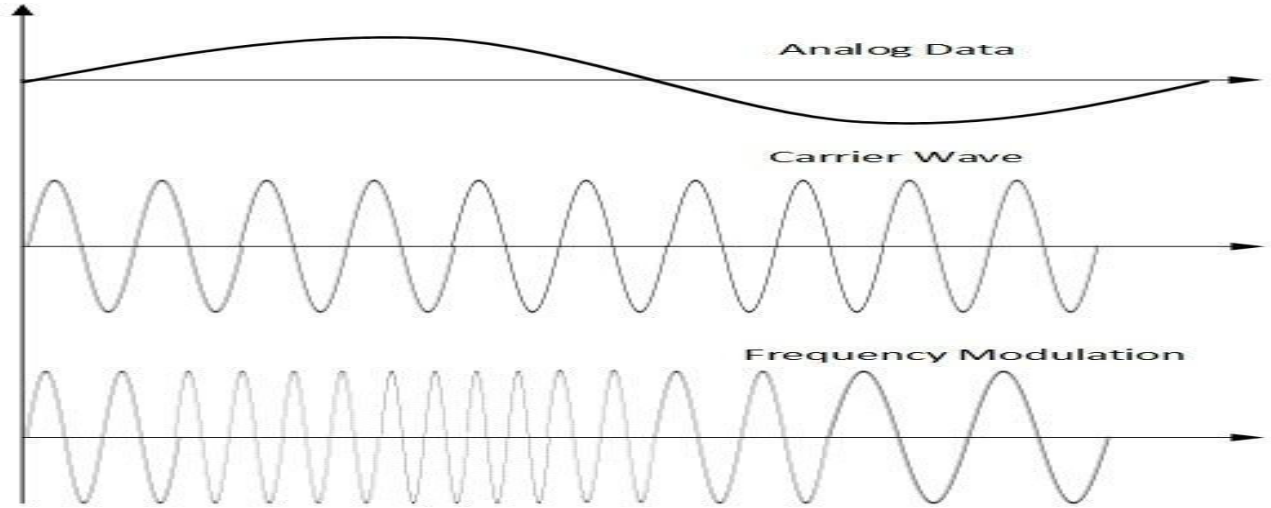


Fig 1.15 Frequency Modulation

The amplitude and phase of the carrier signal are not altered.

C. Phase modulation

In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.

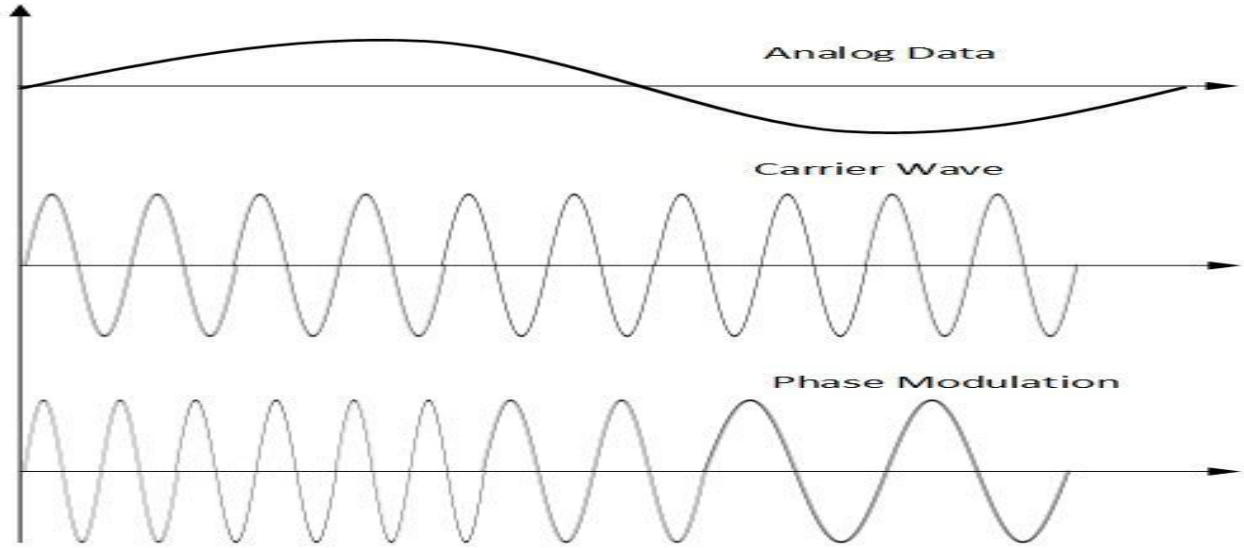


Fig 1.16 Phase Modulation

Phase modulation practically is similar to Frequency Modulation, but in Phase modulation, frequency of the carrier signal is not increased. Frequency in carrier signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

1.5. Modes of Data Transmission

Data transmission means movement of the bits over a transmission medium connecting two devices. How data is to be transferred between to computer is decided by the type of data transmission they are using. Binary data i.e. 1s and 0s can be sent in two different ways: Parallel transmission and Serial transmission.

A. Parallel transmission

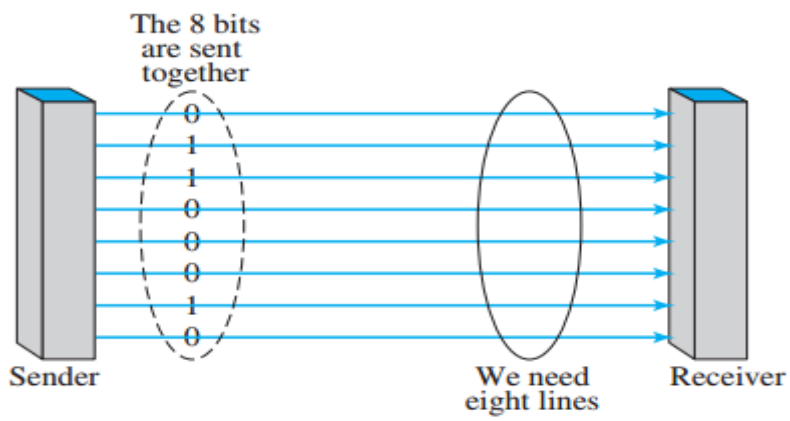


Fig 1.17 Parallel Transmission

The binary bits are organized into groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines. Because data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go. Advantage of parallel transmission is speed and disadvantage is the cost of wires, as it is equal to the number of bits needs to send parallelly.

Generally, in this type of transmission all the bits of a *byte* are transmitted simultaneously on separate wires. And it is practicable if two devices are close to each other. E.g. Computer to Printer, Communication within the Computer.

B. Serial transmission

In serial transmission, bits are sent one after another in a queue manner or in a continuous line. Serial transmission requires only one communication channel as oppose parallel transmission where communication lines depends upon bit word length.

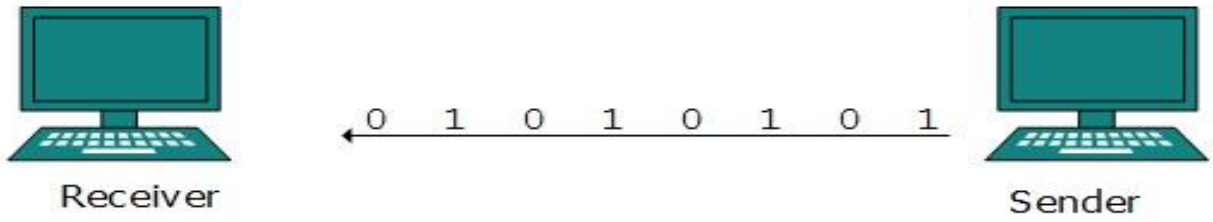
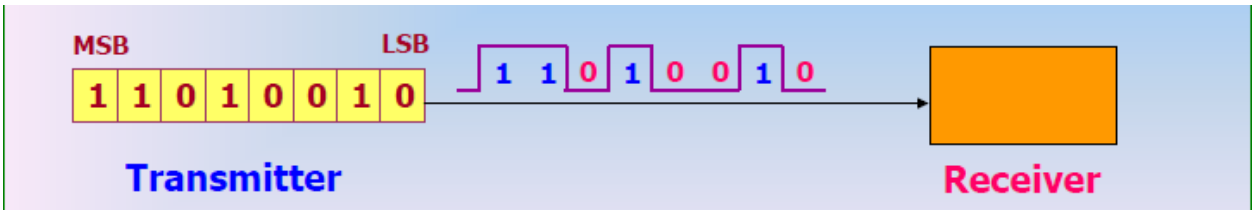


Fig 1.18 Serial Transmission

In serial transmission bits are transmitted one after the other. Usually the Least Significant Bit (LSB) has been transmitted first. Serial transmission requires only one circuit interconnecting two devices and it is much faster than parallel because of way bits processed (e.g. USB and SATA drives). It is suitable for transmission over Long distance.



Note: Received signal is never same as transmitted. Clock signal samples & regenerates the original bits as it was transmitted. Received signal should be sampled at right instant. Otherwise it will cause bit error.

There are two types of serial transmissions.

A. Asynchronous serial transmission

It is named so because there is no importance of timing. Data-bits have specific pattern and helps receiver recognize when the actual data bits start and where it ends. For example, a 0 is prefixed on every data byte and one or more 1s added at the end. Two continuous data-frames (bytes) may have gap between them.

In asynchronous serial transmission

- Sending end commences the transmission of bits at any instant of time.
- Uses stop/ start bits.
- No time relation between the consecutive bits.
- During idle condition Signal ‘ 1’ is transmitted.
- “ Start bit” before the byte and “ Stop bit” at the end of the byte for Start/Stop synchronization.
- Most common type of serial data transfer.
- Allows packet switching.
- Allows sharing of bandwidth (i.e. talk on phone while another person is using internet).

B. Synchronous serial transmission

It is up to the receiver to recognize and separate bits into bytes. The advantage of synchronous transmission is speed and it has no overhead of extra header and footer bits as in asynchronous transmission.
In synchronous serial transmission

- is carried out under the control of the timing source
- no Start/Stop bits
- continuous block of Data are encapsulated with Header & Trailer along with Flags

Why Not use parallel transmission instead of serial transmission?

- Due to inconsistencies on channels data arrives at different times
- Because of the way it is transmitted packet switching cannot be used
- The above two points makes parallel slower than serial and requires higher bandwidth.

Parallel transmissions are rarely used anymore.

1.6. Data transmission error detection and correction

Introduction

Networks must be able to transfer data from one device to another with complete accuracy. A system that cannot guarantee that the data received by one device is identical to the data transmitted by another device is essentially useless. Anytime the data is transmitted from source to destination, it gets corrupted on the way. Many factors including noise can alter or wipe out one or more bits of a given data unit. Reliable systems must have a mechanism for detecting and correcting such errors. Error detection and Correction is implemented either at the data link layer or at the transport layer.

1.6.1. Type of errors

There are two types of error: single-bit and burst errors. Whenever an electromagnetic signal flows from one point to the other, it is subject to unpredictable interference from heat, magnetism and other forms of electricity. This interference can change the shape or timing of the signal. If the signal is carrying encoded binary data, such changes can alter the meaning of the data.

Single Bit error

In a single-bit error, a 0 is changed to a 1 or a 1 to a 0. For example, a 0.01 second burst of impulse noise on a transmission with a data rate of 1200 bps might change all or some of 12 bits of information.

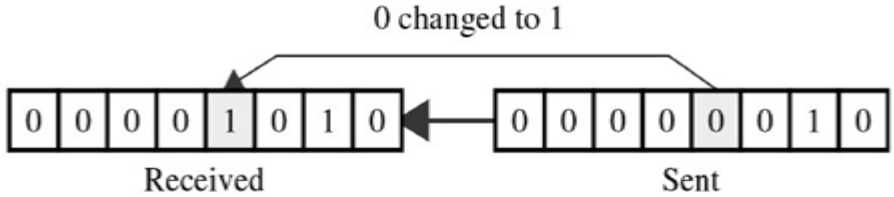


Fig 1.19 Single bit error

The term single bit error means that only one bit of a given data unit (such as a byte, character, or a packet) is changed from 1 to 0 or from 0 to 1. Figure shows the effect of a single bit error on a data unit. Single bit errors are the least likely type of error in serial data transmission. To see why, imagine a sender sends data at 1Mbps. This means that each bit lasts only 1/1,000,000 seconds or 1 microsecond. For single bit error to occur the noise must have duration of 1 microsecond which is very rare, noise lasts much longer than that. However, single bit error can occur if we are sending data using parallel transmission. For example, if 8 wires are used to send all of the eight bits of a byte at the same time and one of the wires is noise, one bit can be corrupted in each byte.

Burst Errors

The term burst error means that two or more bits in the data unit have changed from 1 to 0 or from 0

to 1.

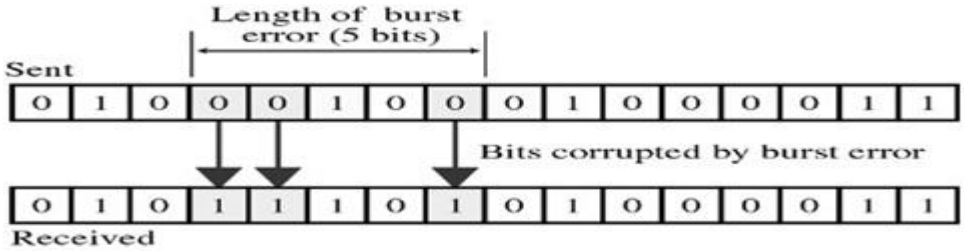


Fig 1.20 Burst error

The above figure shows the effect of a burst error on a data unit. In this case 0100010001000011 was sent but 0101110101000011 was received. Note that a burst error does not necessarily mean that error 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. Burst error is most likely to happen in a serial transmission. The duration of the noise is normally longer than the duration of a bit which means that when noise affects data, it affects a set of bits. The number of bits affected depends on the data rate and duration of noise.

For example, if we are sending data at 1 Kbps, a noise of 1/100 seconds can affect 10 bits. If we are sending data at 1 Mbps, the same noise can affect 10,000 bits.

1.6.2. Error detection/Redundancy

An error detection technique in which a shorter group of bits may be appended to the end of each data unit is called redundancy. This is because the extra bits are redundant to the information and are discarded as soon as the accuracy of transmission has been determined.

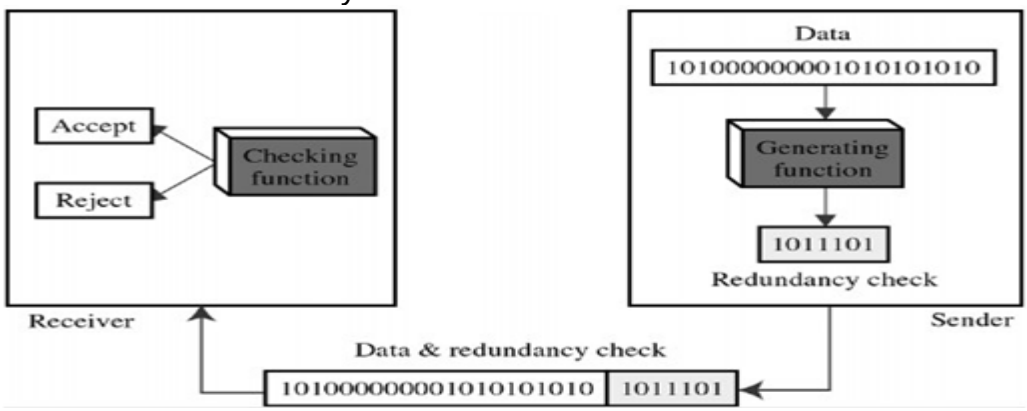


Fig 1.21 Redundancy

The figure shows the process of using redundant bits to check the accuracy of data unit. Once the data stream has been generated, it passes through a device that analyzes it and adds on an appropriately coded redundancy check. The data unit now enlarged by several bits (7) travels over the link to the receiver. The receiver puts the entire stream through a checking function. If the received bit stream passes the checking criteria, the data portion of the data unit is accepted and the redundant bits are discarded.

Types of Redundancy Checks

There are 4 types of redundancy checks used in data communication:

- Vertical Redundancy Check (VRC)
- Longitudinal Redundancy Check (LRC)
- Cyclic Redundancy Check (CRC)
- Checksum

A. Vertical Redundancy Check (VRC)

- Most common and least expensive
- Also called Parity Check

A redundant bit called parity bit is appended to every data unit so that total number of 1' s in the unit becomes even including the parity bit

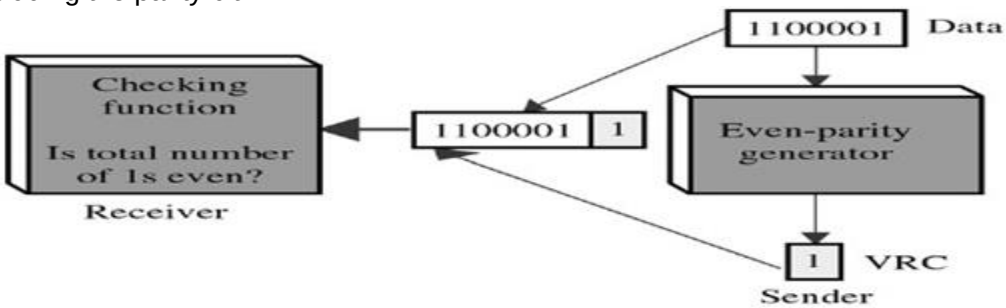


Fig 1.22 Even partiy checking

As it is shown on the figure above, we want to transmit the binary data unit 1100001. Adding together the number of 1' s gives us 3, an odd number. Before transmitting, we pass the data unit through a parity generator, which counts the 1' s and appends the parity bit (1) to the end. The total number of 1' s is now 4, an even number. The system now transfers the entire expanded across the network link. When it reaches its destination, the receiver puts all 8 bits through an even parity checking function. If the receiver sees 11100001, it counts four ones, an even number and the data unit passes. Instead of 11100001, if receiver sees 11100101, then the parity checker counts the 1' s, it gets 5 an odd number and therefore rejects the whole unit. Some systems may also use odd parity checking. The principal is the same as even parity.

B. Longitudinal Redundancy Check (LRC)

In LRC, a block of bits is organized in a table (rows and columns). For example instead of sending 32 bits, we organize them in a table made of 4 rows and 8 columns.

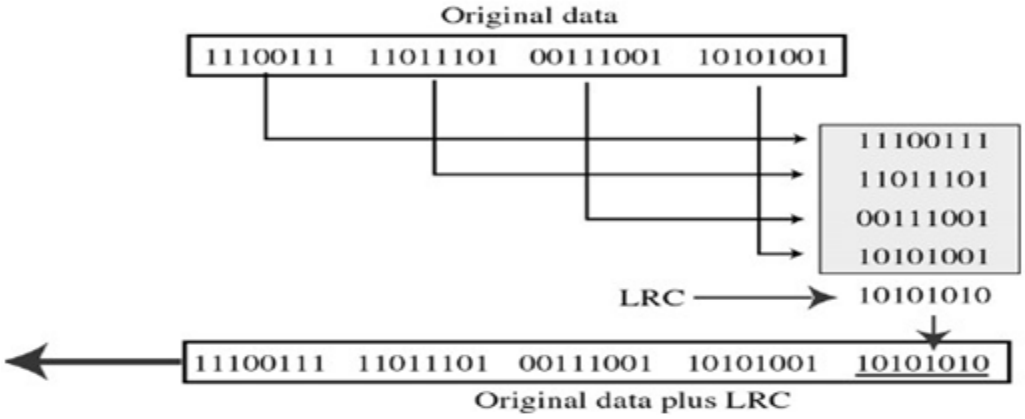


Fig 1.23 Longtidunal Redundancy Checking

We then calculate the Parity bit for each column and create a new row of 8 bits which are the parity bits for the whole block. Note that the first parity bit in the 5th row is calculated based on all the first bits. The second parity bit is calculated based on all the second bits and so on. We then attach the 8 parity bits to the original data and send them to the receiver.

C. Cyclic Redundancy Check (CRC)

- Most powerful of checking techniques
- VRC and LRC are based on Addition
- CRC is based on Binary Division

A sequence of redundant bits called CRC or CRC remainder is appended to the end of the data unit, so that the resulting data unit becomes exactly divisible by a second predetermined binary number. At its destination, the data unit is divided by the same number. At this step, if there is no remainder, the incoming data unit is assumed to be intact and is therefore accepted. Otherwise, a remainder indicates that a data unit has been damaged and therefore must be rejected.

Fig 1.24 Cyclic Redundancy Checking

First a string of n 0' s is appended to the data unit. The number ' n' is one less than the number of bits in the predetermined divisor, which is " n+1" bits. Secondly, newly elongated data unit is divided by the divisor using a process called binary division. The remainder resulting from this division is the CRC. Third, the CRC of ' n' bits replaces the appended 0' s at the end of the data unit. Note that CRC may consist of all zeros. The data unit arrives at the receiver followed by the CRC.

The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder. If string arrives without an error, the CRC checker yields a remainder of zero and data unit passes. If the string has been changed in transit, the division yields a non-zero remainder and the data unit does not pass.

D. CHECKSUM

- Error detection method used by the Higher Layers
- Like VRC, LRC, CRC, Checksum is also based on the concept of redundancy

One' s Complement

Finding one' s complement

- Invert every 1 to 0 and 0 to 1
- A and – A are one' s complement of each other
- +A = 1010 → -A = 0101
- +0 = 0000 → -0 = 1111

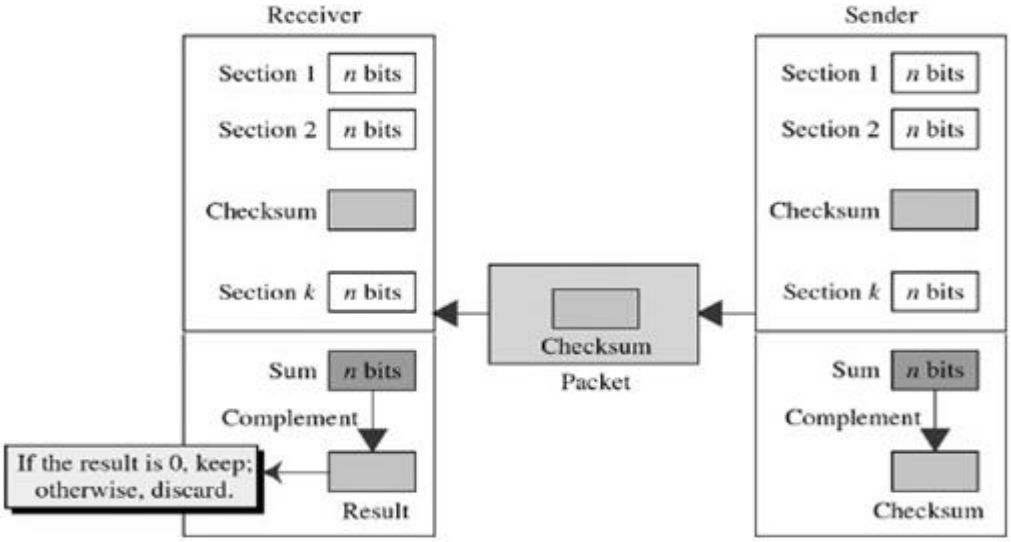


Fig 1.25 CHECKSUM Generator

The sender subdivides data units into equal segments of 'n' bits (16 bits). These segments are added together using one's complement. The total (sum) is then complemented and appended to the end of the original data unit as redundancy bits called CHECKSUM. The extended data unit is transmitted across the network. The receiver subdivides data unit as above and adds all segments together and complement the result. If the

intended data unit is intact, total value found by adding the data segments and the checksum field should be zero. If the result is not zero, the packet contains an error & the receiver rejects it.

1.6.3. Error correction

Error correction locates the invalid bit or bits. Error correction can be done in two ways:

– Receiver can ask sender for retransmission.

– Receiver can use an error-detecting code, which automatically correct certain errors

Error correcting codes are more sophisticated than error detecting codes. They require more redundancy bits and the number of bits required to correct multiple – bit or burst error is so high that in most cases it is inefficient. Error correction is limited to 1, 2 or 3 bit.

Redundancy bit (r)

- r must be able to indicate at least m+r+1 states
- m+r+1 states must be discoverable by r bits
- Therefore, $2^r \geq m+r+1$
- If m=7, r=4 as $2^4 \geq 7+4+1$

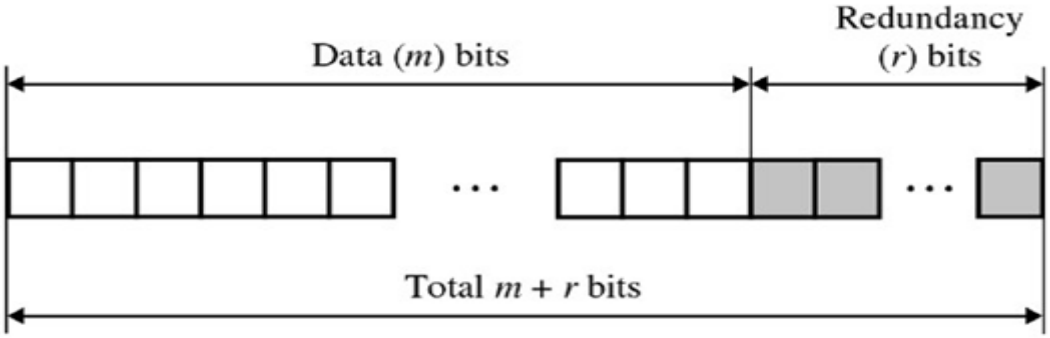
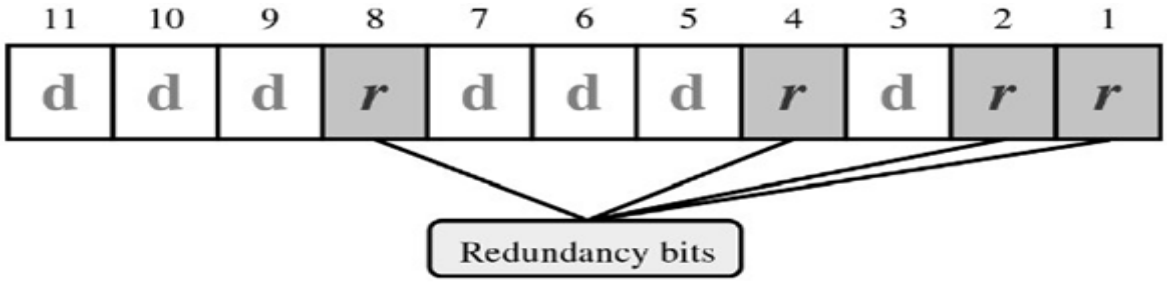
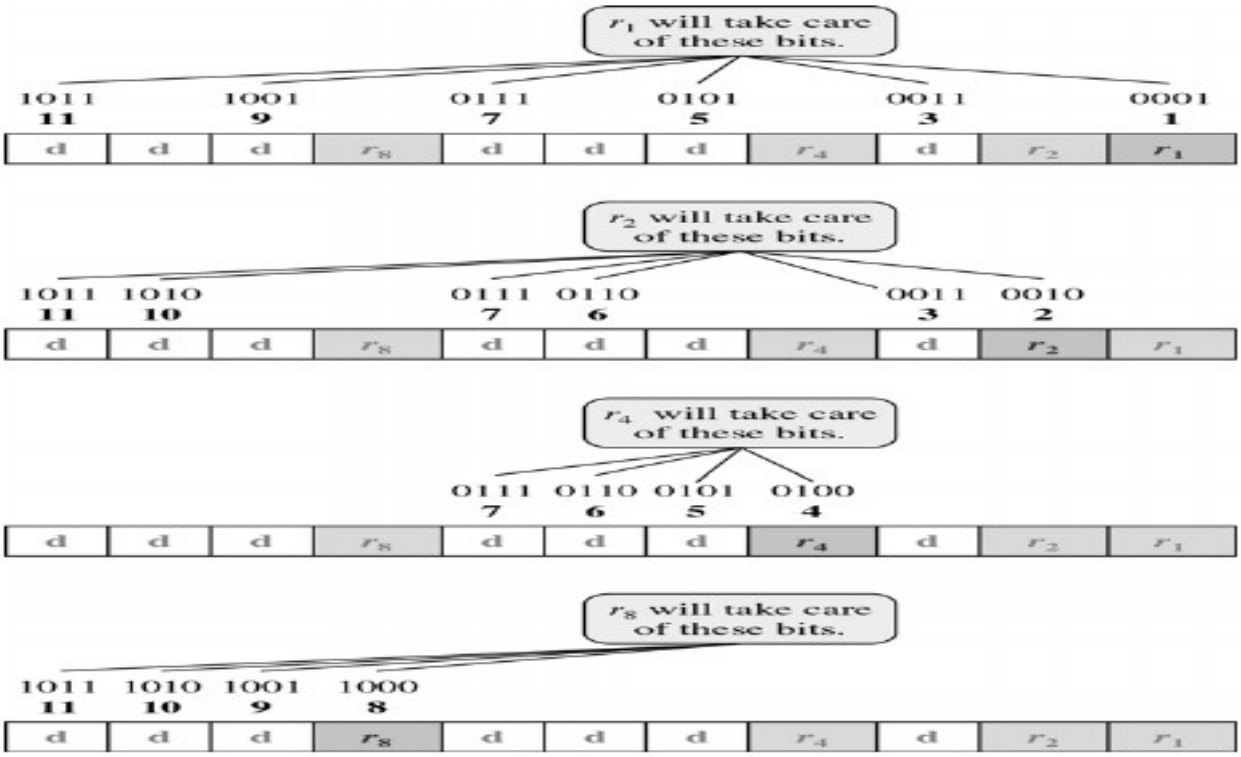


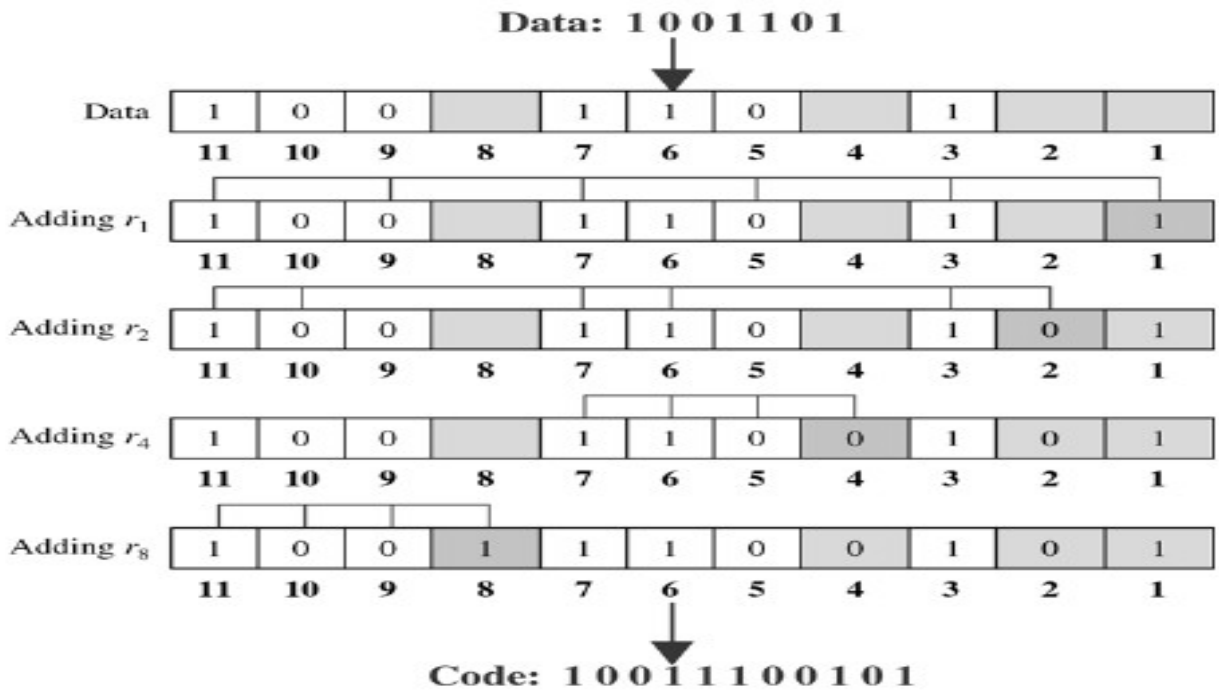
Fig 1.26 Data plus Redundancy bits

Hamming Code

Each r bit is the VRC bit for one combination of data bits. r1(r2) bit is calculated using all bit positions whose binary representation includes a 1 in the first(second) position, and so on.




r1 will take care of these bits.
1011 11
1001 9
0111 7
0101 5
0011 3
0001 1
d d d r8 d d d r4 d r2 r1
r2 will take care of these bits.
1011 11
1010 10
0111 7
0110 6
0011 3
0010 2
d d d r8 d d d r4 d r2 r1
r4 will take care of these bits.
0111 7
0110 6
0101 5
0100 4
d d d r8 d d d r4 d r2 r1
r8 will take care of these bits.
1011 11
1010 10
1001 9
1000 8
d d d r8 d d d r4 d r2 r1


Data: 1 0 0 1 1 0 1
Data 1 0 0 1 1 0 1
11 10 9 8 7 6 5 4 3 2 1
Adding r1 1 0 0 1 1 0 1
11 10 9 8 7 6 5 4 3 2 1
Adding r2 1 0 0 1 1 0 1 0 1
11 10 9 8 7 6 5 4 3 2 1
Adding r4 1 0 0 1 1 0 0 1 0 1
11 10 9 8 7 6 5 4 3 2 1
Adding r8 1 0 0 1 1 1 0 0 1 0 1
11 10 9 8 7 6 5 4 3 2 1
Code: 1 0 0 1 1 1 0 0 1 0 1

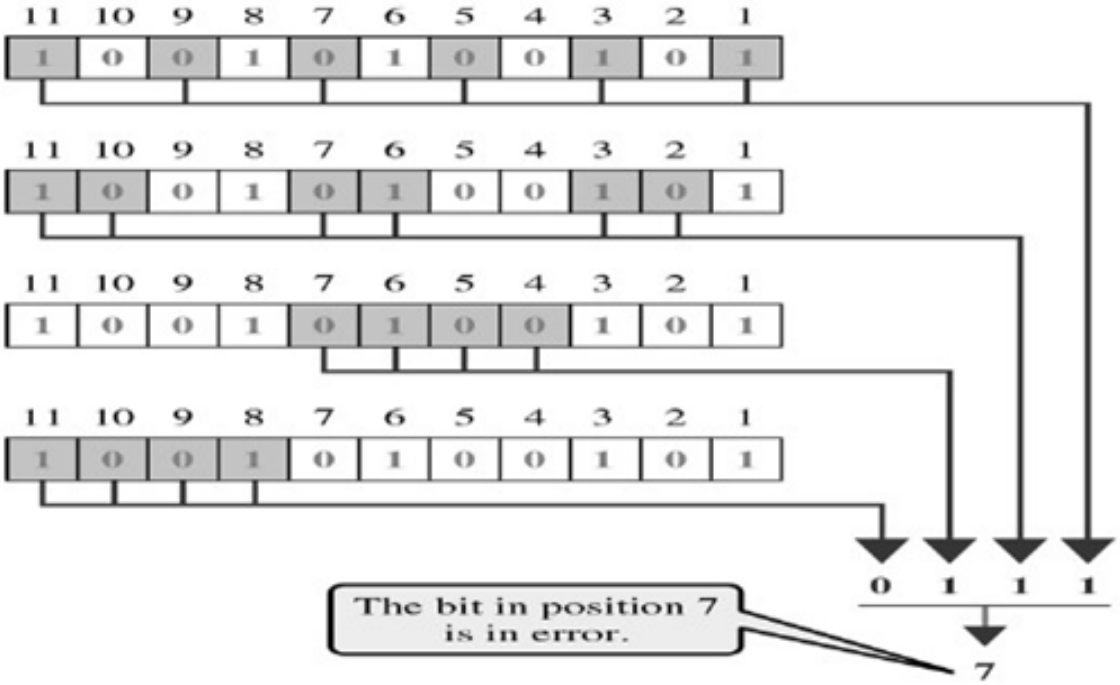


Fig 1.27 Hamming code recovering a single-bir error

CHAPTER TWO

Introduction to Computer Networks

2.1. Computer network and its application

2.1.1. What is a computer network?

A computer network is a system in which a number of independent computers are linked together to share resources. Resource may be file, folder, printer, disk drive or just about anything else that exists on a computer. In the modern world, computer networks have become almost indispensable. All major businesses and governmental and educational institutions make use of computer networks to such an extent that it is now difficult to imagine a world without them.

A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and other tasks with networks and network technologies. Usually, the connections between computers in a network are made using physical wires or cables. However, some connections are wireless, using radio waves or infrared signals.

2.1.2. Applications & Uses of Networks

In the short time they have been around, data communication networks have become an indispensable part of business, industry, and entertainment. Some of the network applications in different fields are the following:

- **Marketing and sales.**

Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data relating to customer needs and product development cycles. Sales applications include teleshopping, which uses order entry computers or telephones connected to an order-processing network, and on-line reservation services for hotels, airlines, and so on.

- **Financial services**

Today's financial services are totally dependent on computer networks. Applications include credit history searches, foreign exchange and investment services, and electronic funds transfer (EFT), which allows a user, to transfer money without going into a bank (an automated teller machine is a kind of electronic funds transfer; automatic paycheck deposit is another).

- **Manufacturing**

Computer networks are used today in, many aspects of manufacturing, including the manufacturing process itself. Two applications that use networks to provide essential services are computer-assisted design (CAD) and computer-assisted manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.

- **Electronic messaging**

Probably the most widely used network application is electronic mail (e-mail).

- **Directory services**

Directory services allow lists of files to be stored in a central location to speed worldwide search operations.

- **Information services**

Network information services include bulletin boards and data banks. A World Wide Web site offering the technical specifications for a new product is an information service.

- **Electronic data interchange (EDI)**

EDI allows business information (including documents such as purchase orders and invoices) to be transferred without using paper.

- **Teleconferencing**

Teleconferencing allows conferences to occur without the participants being in the same place. Applications include simple text conferencing (where participants communicate through their keyboards and computer monitors), voice conferencing (where participants at a number of locations communicate simultaneously over the phone) and video conferencing (where participants can see as well as talk to one another).

- **Cellular telephone**

In the past two parties wishing to use the services of the telephone company had to be linked by a fixed physical connection. Today's cellular networks make it possible to maintain wireless phone connections even while traveling over large distances.

- **Cable television**

Future services provided by cable television networks may include video on request, as well as the same information, financial, and communications services currently provided by the telephone companies and computer networks.

Disadvantages of computer network

Making important and sensitive information available to every user of the network is not normally desirable. For example, information about employees' salaries should not be freely available for anybody to look at. Data security is therefore an important concern in a networked environment. Secondly, the danger of computer viruses entering the network is greatly increased. A virus can infect any of the computers on the network, and can quickly spread throughout the network causing significant damage. Equipment malfunctions and system failures are also the risks of computer networks.

2.2. **Types of networks**

Depending on one's perspective, we can classify networks in different ways.

- Based on network size: LAN, MAN and WAN
- Based on management method: Peer-to-peer and Client/Server

2.2.1. Types of network based on network size (coverage)

i. LANs

Computer networks can be classified into one of two groups, depending on their size and function. A local area network (LAN) is the basic building block of any computer network. A LAN can range from simple (two computers connected by a cable) to complex (hundreds of connected computers and peripherals throughout a major corporation). A local-area network (LAN) can connect many computers in a relatively small geographical area such as a home, an office, or a campus. The distinguishing feature of a LAN is that it is confined to a limited geographic area.

In a typical LAN configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On most LANs, cables are used to connect the network interface cards in each computer. A LAN connects network devices over a relatively short distance. Occasionally a LAN will span a group of nearby buildings.

In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

ii. Metropolitan Area Network (MAN)

It is a network that transmits data and information over city wide distance.

- ✓ A Metropolitan Area Network (MAN) is a network that is utilized across multiple buildings.
- ✓ Is larger than a LAN, but smaller than a WAN.
- ✓ Is also used to mean the interconnection of several LANs by bridging them together. This sort of network is also referred to as a campus network.

iii. Wide area network (WAN)

A wide area network (WAN), on the other hand, has no geographical limit. It can connect computers and other devices on opposite sides of the world. A WAN is made up of a number of interconnected LANs. Perhaps the ultimate WAN is the Internet. LANs typically have much higher transmission rates than WAN. Most LANs are able to transmit data at around 100Mbps (million bits per second), whereas WANs generally transmit at less than 10Mbps. Another difference is the error rates in transmission: the likely number of errors in data transmission is higher for a WAN than for a LAN. WAN is typically slower and less reliable than a LAN.

This distinction between LANs and WANs is made because of the locality principle. The locality principle in computer networking states that computers are much more likely to want to communicate with other computers that are geographically close, than with those that are distant. For example, if you want to request a printout from your PC, it makes much more sense to use the printer in the next room rather than one that is hundreds of kilometers away. Because of the locality principle network designers tend to use higher performance hardware within a LAN compared to the connections between different LANs that form a WAN.

2.2.2. Types of networks based on node relationship

Based on the role each node on the network has, networks are divided into two broad categories:

- Peer-to-peer networks
- Server-based networks

i. Peer-to-peer networks

In a peer-to-peer network, there are no dedicated servers, and there is no hierarchy among the computers. All the computers are equal and therefore are known as peers. Each computer functions as both a client and a server, and there is no administrator responsible for the entire network. The user at each computer determines what data on that computer is shared on the network. Peer-to-peer networks are also sometimes called workgroups.

Peer-to-peer networks are relatively simple. Because each computer functions as a client and a server, there is no need for a powerful central server or for the other components required for a high-capacity network. Peer-to-peer networks can be less expensive than server-based networks. Also, the networking software does not require the same standard of performance and level of security as the networking software designed for dedicated servers.

In typical networking environments, a peer-to-peer implementation offers the following advantages:

- Computers are located at users' desks
- Users act as their own administrators and plan their own security
- They are cheap and easy to set up and administer for small groups of users

Peer-to-peer networks are good choices for environments where:

- There are 10 users or fewer
- Users share resources, such as printers, but no specialized servers exist
- Security is not an issue
- The organization and the network will experience only limited growth within the foreseeable future

Where these factors apply, a peer-to-peer network will probably be a better choice than a server-based network.

ii. Server-based networks

In an environment with more than 10 users, a peer-to-peer network will probably not be adequate. Therefore, most networks have dedicated servers. A dedicated server is one that functions only as a server and is not used as a client or workstation. Servers are described as "dedicated" because they are not themselves clients, and because they are optimized to service requests from network clients quickly and to ensure the security of files and directories. Server-based networks have become the standard models for networking.

When the networks increase in size (as the number of connected computers and the physical distance and traffic between them grows), more than one server is usually needed. Spreading the networking tasks among several servers ensures that each task will be performed as efficiently as possible. Servers must perform varied and complex tasks. Servers for large networks have become specialized to accommodate the expanding needs of users. For example, a network may have separate servers for file storage, printing, email and for storing and running application software.

Although it is more complex to install, configure, and manage, a server-based network has many advantages over a simple peer-to-peer network.

- Server-based data sharing can be centrally administered and controlled. Because these shared resources are centrally located, they are easier to find and support than resources on individual computers.
- Security is often the primary reason for choosing a server-based approach to networking. In a server-based environment, one administrator who sets the policy and applies it to every user on the network can manage security.
- Backups can be scheduled several times a day or once a week depending on the importance and value of the data. Server backups can be scheduled to occur automatically, according to a predetermined schedule, even if the servers are located on different parts of the network.
- A server-based network can support thousands of users. This type of network would be impossible to manage as a peer-to-peer network.

2.3.Network Topologies

The term topology, or more specifically, network topology, refers to the arrangement or physical layout of computers, cables, and other components on the network. Topology defines the structure of the network. This includes the physical topology which is the actual layout of the physical components such as computer, media etc., and the logical topology which is how the media is accessed by the hosts, how data is transmitted between nodes or how the network message is travel from one node to another. "Topology" is the standard term that most network professionals use when they refer to the network's basic design. In addition to the term "topology," you will find several other terms that are used to define a network's design: Physical layout, Design, Diagram or Map.

A network's topology affects its capabilities. The choice of one topology over another will have an impact on the:

- Type of equipment that the network needs
- Capabilities of the network
- Growth of the network

- Way the network is managed

Developing a sense of how to use the different topologies is a key to understanding the capabilities of the different types of networks.

Before computers can share resources or perform other communication tasks they must be connected. Most networks use cable to connect one computer to another. However, it is not as simple as just plugging a computer into a cable connecting to other computers. Different types of cable—combined with different network cards, network operating systems, and other components—require different types of arrangements. To work well, a network topology takes planning. For example, a particular topology can determine not only the type of cable used but also how the cabling runs through floors, ceilings, and walls. Topology can also determine how computers communicate on the network. Different topologies require different communication methods, and these methods have a great influence on the network.

There are four basic types of computer topology: bus, star, ring and mesh.

i. Bus Topology

The bus topology is often referred to as a "linear bus" because the computers are connected in a straight line. This is the simplest and most common method of networking computers. The figure below shows a typical bus topology. It consists of a single cable called a trunk (also called a backbone or segment) that connects all of the computers in the network in a single line.

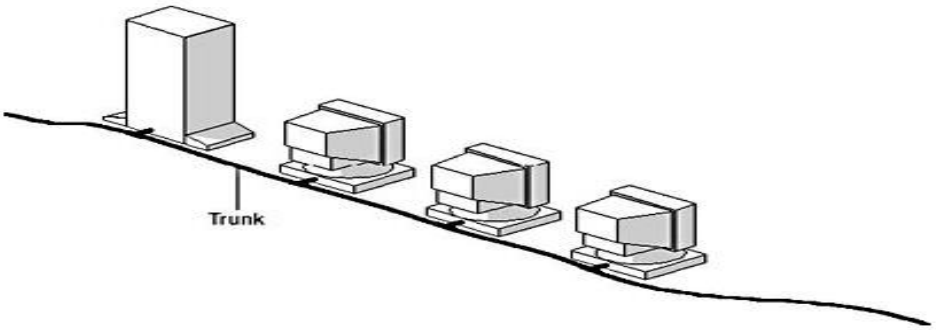


Fig 2.1 The bus topology

Computers on a bus topology network communicate by addressing data to a particular computer and sending out that data on the cable as electronic signals. To understand how computers communicate on a bus, you need to be familiar with three concepts: Sending the signal, Signal bounce and Terminator.

a. Sending the signal

When sending a signal from one computer on the network to another, network data in the form of electronic signals is in fact sent to all the computers on the network. However, only the computer whose address matches the address encoded in the original signal accepts the information. All other computers reject the data. Because only one computer at a time can send data on a bus network, the number of computers attached to the bus will affect network performance. The more computers there are on a bus, the more computers will be waiting to put data on the bus and, consequently, the slower the network will be. Computers on a bus either transmit data to other computers on the network or listen for data from other computers on the network. They are not responsible for moving data from one computer to the next. Consequently, if one computer fails, it does not affect the rest of the network.

b. Signal bounce

Because the data, or electronic signal, is sent to the entire network, it travels from one end of the cable to the other. If the signal is allowed to continue uninterrupted, it will keep bouncing back and forth along the cable

and prevent other computers from sending signals. Therefore, the signal must be stopped after it has had a chance to reach the proper destination address.

c. Terminator

To stop the signal from bouncing, a component called a terminator is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data.

In a bus topology, if a break in the cable occurs the two ends of the cable at the break will not have terminators, so the signal will bounce, and all network activity will stop. This is one of several possible reasons why a network will go "down." The computers on the network will still be able to function as stand-alone computers; however, as long as the segment is broken, they will not be able to communicate with each other or otherwise access shared resources.

ii. Star topology

In the star topology, cable segments from each computer are connected to a centralized component called a hub, making it very easy to add a new workstation. Figure below shows four computers and a hub connected in a star topology. Signals are transmitted from the sending computer through the hub to all computers on the network.

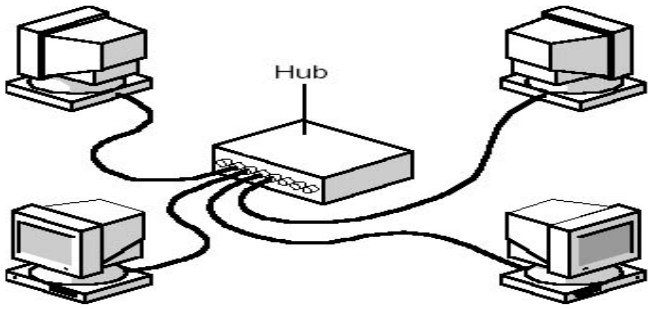


Fig 2.2 The star topology

Because each computer is connected to a central point/device, this topology requires a great deal of cable in a large network installation. Also, if the central point/device fails, the entire network goes down. If one computer or the cable that connects it to the hub fails on a star network, only the failed computer will not be able to send or receive network data. The rest of the network continues to function normally.

Star topologies are more expensive to install than bus networks, because there are several more cables that need to be installed, plus the cost of the hubs that are needed.

iii. Ring topology

The ring topology connects computers on a single circle of cable. Each node is connected to the two nearest nodes so the entire network forms a circle. Unlike the bus topology, there are no terminated ends. The signals travel around the loop in one direction and pass through each computer, which can act as a repeater to boost the signal and send it on to the next computer. The figure below shows a typical ring topology with one server and four workstations. The failure of one computer can have an impact on the entire network. One method for passing data on ring networks is token passing.

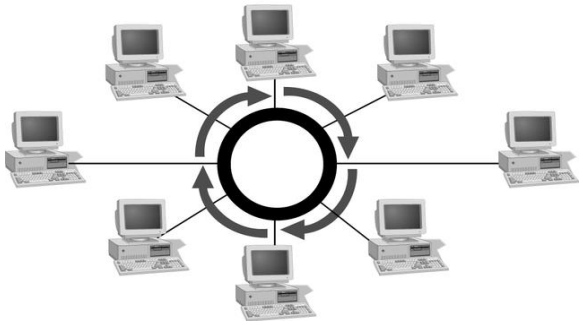


Fig 2.3 The ring topology

Ring topology is easier to manage; easier to locate a defective node or cable problem. It also well-suited for transmitting signals over long distances by handling high-volume network traffic on a LAN. In short ring topology enables reliable communication. However, this topology has the following limitations. Expensive, requires more cable and network equipment at the start, not used as widely as bus topology (i.e. fewer equipment options and fewer options for expansion to high-speed communication.)

iv. Mesh topology

A mesh topology network offers superior redundancy and reliability. In a mesh topology, each computer is connected to every other computer by separate cabling. (See the figure below) This configuration provides redundant paths throughout the network so that if one cable fails, another will take over the traffic. While ease of troubleshooting and increased reliability are definite benefits, these networks are expensive to install because they use a lot of cabling. Often, a mesh topology will be used in conjunction with other topologies to form a hybrid topology.

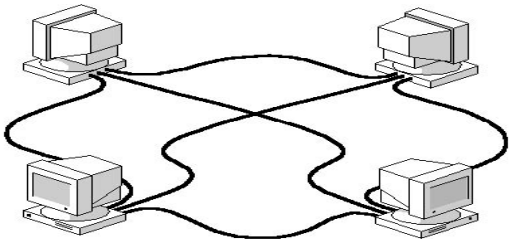


Fig 2.4 The mesh topology

The mesh topology is the simplest logical topology in terms of data flow, but it is the most complex in terms of physical design. In this physical topology, each device is connected to every other device. This topology is rarely found in LANs, mainly because of the complexity of the cabling. If there are x computers, there will be $(x \times (x–1)) \div 2$ cables in the network. For example, if you have five computers in a mesh network, it will use $5 \times (5 – 1) \div 2$, which equals 10 cables. This complexity is compounded when you add another workstation. For example, your five computers, 10 cable network will jump to 15 cables just by adding one more computer.

v. Hybrid topologies

Many working topologies are hybrid combinations of the bus, star, ring, and mesh topologies. Two of the more common are described below.

A. Star bus topology

The star bus is a combination of the bus and star topologies. In a star-bus topology, several star topology networks are linked together with linear bus trunks. The figure below shows a typical star-bus topology.

If one computer goes down, it will not affect the rest of the network. The other computers can continue to communicate. If a hub goes down, all computers on that hub are unable to communicate. If a hub is linked to other hubs, those connections will be broken as well.

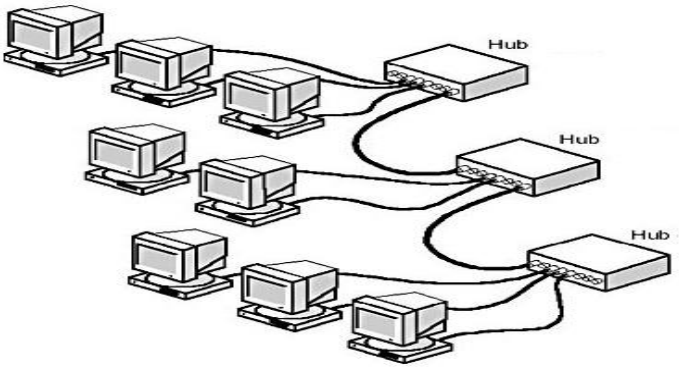


Fig 2.5 The star bus hybrid topology

B. Star ring topology

The star ring (sometimes called a star-wired ring) appears similar to the star bus. Both the star ring and the star bus are centered in a hub that contains the actual ring or bus. The figure below shows a star-ring network. Linear-bus trunks connect the hubs in a star bus, while the hubs in a star ring are connected in a star pattern by the main hub.

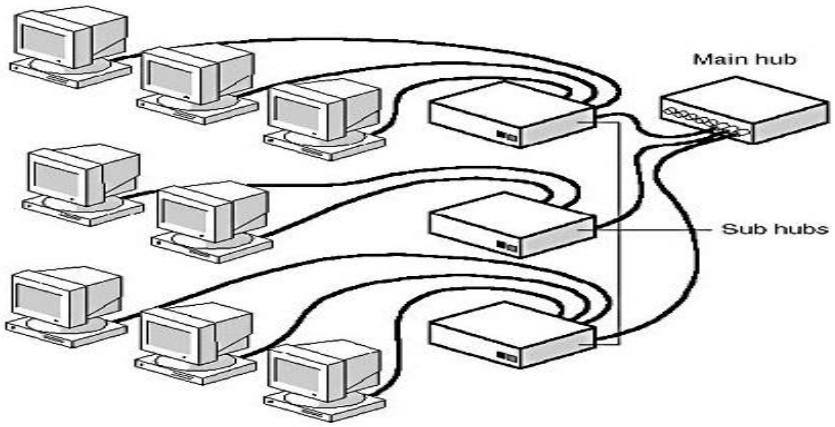


Fig 2.6 The star ring hybrid topology

Until now we have assumed that the word topology is used to refer only to the physical layout of the network. In fact, we can talk about two kinds of topology: physical and logical. A network's physical topology is the wire itself. A network's logical topology is the way it carries signals on the wire.

2.4.Computer network components

The components required to operate a network can be divided into two major categories: Hardware and software.

The hardware components of a network consist of all physical parts that we can see and touch. The following five items are good examples to be mentioned.

- Server
- Workstation/Client
- Transmission media
- Network Interface Cards (NIC)
- A concentrator/network connectivity devices/internetworking devices, or wiring center

The software necessary to operate a network consists of:

- Network operating system (NOS)
- The operating system of the workstation
- Server software
- Client software

2.4.1. Hardware network components

A. The Server

The server functions as the central repository resources/services the network provides. Usually the server is also responsible for controlling which users on which computers in the network are granted access to a service.

B. Workstations/Clients

Almost all the user computers connected to a network are called workstations or clients. A typical workstation is a computer that is configured with a network interface card, networking software, and the appropriate cables.

C. Transmission media

It is either a wired or wireless medium through which information usually moves from one network device to another. (To be covered in details on the next chapter)

D. Network Interface Card (NIC)

The NIC is located in every workstation on the LAN as well as in the server. It is a board that plugs into one of the expansion slots on the motherboard of a workstation and the server, thereby providing a connector on the back to hook to some sort of transmission media (including wireless media). NIC acts as a "transmitter" and "receiver" – transceiver.

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Some computers use external boxes.

Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

E. The Concentrator – Network connectivity or Internetworking devices

Every workstation on the LAN must be connected to the server across some sort of transmission media. However, it is virtually impossible to have every workstation on the LAN actually attached to at the file server, since the file server usually has only one NIC.

To accommodate multiple workstations, a hub or central data collecting area is often used, although certain network architectures such as linear bus structures do not use hubs or concentrators. On certain networks, a hub allows for multiple connections or splitting of the network cable.

i. Hub

A hub acts as the central component in a star topology, and typically contains 4, 8, 16 or even more different ports for connecting to computers or other hubs. It is similar in operation to a repeater, except that it broadcasts data received by any of the ports to all other ports on the hub. Hubs can be active, passive or hybrid. Most hubs are active; that is, they regenerate and retransmit signals in the same way as a repeater does. Because hubs usually have eight to twelve ports for network computers to connect to, they are sometimes called multiport repeaters. Active hubs require electrical power to run. Some types of hubs are passive. They act as connection points and do not amplify or regenerate the signal; the signal passes through the hub. Passive hubs do not require electrical power to run. Advanced hubs that will accommodate several different types of cables are called hybrid hubs.

ii. Switch

A concentrator is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central switch/hub. Most

switches are active, that is they electrically amplify the signal as it moves from one device to another. Switches no longer broadcast network packets as hubs did in the past, they memorize addressing of computers and send the information to the correct location directly. Switches are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or star-wired ring topology
- Sold with specialized software for port management

iii. Repeaters

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

iv. Bridges

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. Bridges can be used to connect different types of cabling, or physical topologies. They must, however, be used between networks with the same protocol.

v. Routers

A router translates information from one network to another; it is similar to a super intelligent bridge. Routers select the best path to route a message, based on the destination IP address. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even "listen" to the entire network to determine which sections are busiest -- they can then redirect data around those sections until they clear up.

If you have a school LAN that you want to connect to the Internet, you will need to purchase a router. In this case, the router serves as the translator between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet. Routers can:

- Direct signal traffic efficiently
- Route messages between any two protocols
- Route messages between linear bus, star, and star-wired ring topologies
- Route messages across fiber optic, coaxial, and twisted-pair cabling

vi. Gateway

A gateway is a translation tool. It is a server that acts as an intermediary for some other server. Unlike a proxy, a gateway receives requests as if it were the original server for the requested resource; the requesting client may not be aware that it is communicating with a gateway. The best way to explain it is with our restaurant example. Let's say you want to order a hamburger, but they don't understand the word hamburger in Russia. A gateway would tell the waiter or waitress that you want a piece of cooked ground beef on bread.

In networking, a gateway translates messages between computers using different topologies. In order to connect your FDDI backbone to your Ethernet network, you must have a gateway installed in order to allow the two to understand each other.

2.4.2. Software network components

A. The Network Operating System

Unlike operating systems, such as DOS and Windows that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly. The network operating system is the software that resides on the server. It controls virtually all the activity on the network. It also manages access to the resource on the server and handles security of the resource on the server.

Network operating system provides true multi-user capabilities and is probably the most important part of the network.

The two major types of network operating systems are: Peer-to-Peer and Client/Server.

Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source. Windows for Workgroup is an example of programs that can function as peer-to-peer network operating systems.

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers. It provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Red Hat 7, Fedora, Windows 2008 and Windows 2012 Server are examples of client/server network operating systems.

B. The server software

Server software usually loaded on the server. They provide an interface through the service is given to clients. Most popular ones are web server, mail server, print server, file server, database server etc.

C. The client software

They are software's that used to access the service given by the server software on the server. They are capable of interfacing with server software. E.g. web browsers, e-mail clients etc.

2.5.Computer network design and management

2.5.1. Network Design

The decision that we make in laying the foundation upon which our network will be built can make our life easier or come back to haunt us. Whenever we start to design a network for an organization, we should clearly identify the organizational objective and the goal of the network to be developed. A general network goal that can work for most organizations can be to install an economical computer network that will bring up-to-date communication technology and be flexible enough to allow for future expansion.

The most typical technical goals in an enterprise LAN/WAN design include scalability, availability, performance, and security.

Scalability: Scalability is the ability of a network to continue to function well as it is changed in size or volume to meet new enterprise traffic or application requirements. Typically, the rescaling is to a larger size or volume. In today's dynamic and rapid changing business environment, enterprises are rapidly adding users, various applications, opening new branch offices, and connecting with external partners to meet new business challenges. Therefore, scalability is always the biggest concern, and the primary technical goal for an enterprise network design.

Availability*:* The second most important technical goal every enterprise network requires is high availability. This refers to the amount of up time the network is available to end users. It can be expressed as a percent of uptime per year, month, week, day, or hour, compared to the total time in that period. For example, a network kept up and running for 165 hours in one week (7 x 24 = 168 hours), means that the availability in that week is 98.21 percent.

Performance*:* Network performance is a very broad and complicated topic. The requirement for it could be a very vague definition stated by the client. They could say something like, "as long as the users have no complaints" or it could be a scientific one like, "I want to see a LAN throughput of at least 1000 PPS (packets per second)." In the former case, you have to work out more specific goals for the client to achieve the performance they really need. In general, network performance can be specified in very scientific and precise terms. Parameters such as capacity utilization, throughput, and delay are just some of the terms that indicate the health of an enterprise network. There are many management tools available to collect and analyze these data.

Security*:* Among all the technical goals, security is becoming more important as enterprises keep connecting their private internetworks to the Internet as well as their partners and remote workers. Therefore, security concerns should be carefully integrated into every step of the network design and planning. The first and most important step to achieve good security for your client is to come up with a thorough corporate security policy. You and your client should jointly make these policies. Ask as many questions as possible to understand the risks associated with not implementing a secure network. Determine how sensitive is the data and where will it be stored.

The first decision we need to make in designing new network is whether it should be a peer-to-peer or a server-based network. The factors we need to examine include the:

- Size of the network.
- Level of security.
- Type of business.
- Level of administrative support available.
- Amount of network traffic.
- Needs of the network users.
- Network budget.

Selecting a Logical Network Topology

A topology pictorially describes the configuration or arrangement of a conceptual network, including all the network nodes and connecting lines. During this phase, identify the network segments and interconnection points between segments, size and scope of networks, and the types of required internetworking devices; for example, hub, switch, or router. You do not have to decide which devices just yet. One of the best practices when designing an enterprise LAN/WAN network is to develop a layered and hierarchical design model, which is recommended by most network design experts. Compared to other design models — such as flat — the hierarchical model allows an internetwork to be designed in three discrete layers, each focusing on specific functions. Modularity in network design allows designers to create elements that can be replicated as the

network grows and changes. As each element changes, the cost and complexity of making the upgrade is constrained to a small subset of the overall network. Therefore, the hierarchical design model provides us the best network scalability.

A typical hierarchical network topology includes the following three layers:

- A core layer consisting of high-end routers and switches that are optimized for availability and performance
- A distribution layer of routers and switches that implement network policies
- An access layer that connects users via hubs, switches, and other interconnection devices

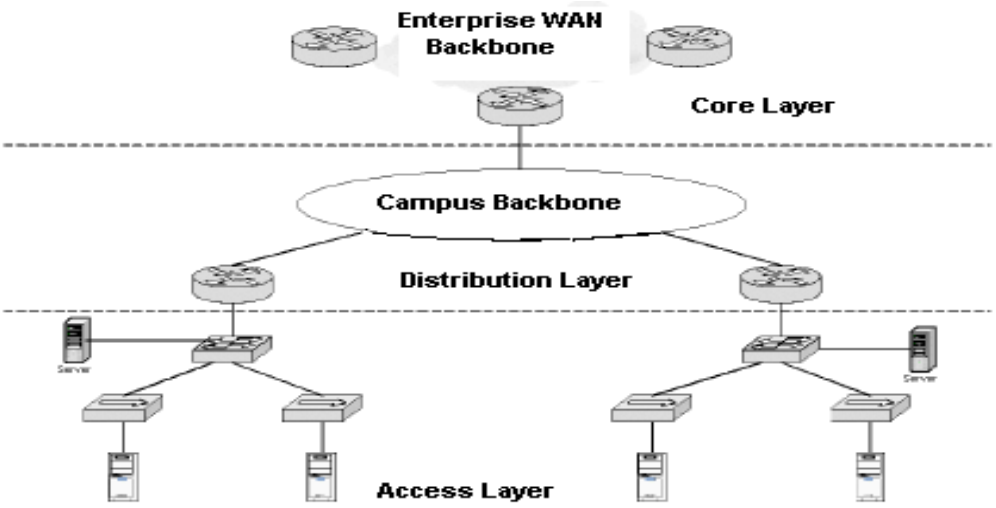


Fig 2.7 Three-Layered Hierarchical Network Design Model.

1) ***The core layer design***. Some refer to the core layer as "the backbone" of the network. This is because it is always a high-speed switching backbone and should be designed to switch packets as fast as possible. This layer should not perform any packet manipulation, such as access list filtering that slows down packet switching. Also, neither servers nor end-user machines should be attached to the core layer. When configuring routers in this layer, you should maximize the packet switching throughput and optimize the core for low latency and good manageability.

2) The distribution layer design. This layer is the demarcation point between the access and core layers and helps define and differentiate the core layer. Its purpose is to provide boundary definition; it's also where packet manipulation can take place.

When designing an enterprise LAN/WAN network, you can include the following functions into the distribution layer:

- Address or area aggregation
- Departmental or workgroup access
- Broadcast/multicast domain definition
- VLAN routing
- Any media transitions that need to occur
- Security policies

3) The access layer design. The access layer is the point where local end users are connected directly into the network. This layer may also use access lists or filters to further optimize the needs of a particular set of users. In an enterprise campus environment, access layers can be designed to have the following functions:

- Shared bandwidth
- Switched bandwidth
- MAC layer filtering
- Micro segmentation

In the non-campus environment, the access layer can give remote sites access to the corporate network via wide-area technology, such as frame relay, ISDN, or leased lines.

Requirements of the Network

After you have examined the existing facility and equipment, you need to define the requirements of your network. You'll then match these requirements to the existing hardware, software, and telecommunications features available and determine what steps need to be taken to develop the network. At a minimum, you should consider the following:

- The size of the facility (located on a single floor vs. multiple floors)
- The number of users
- Whether the LAN will be extended to several buildings
- The environment (office, manufacturing, out-of-doors)
- The current network media, if any
- The technical competence of users
- The amount of network traffic (initially, and anticipated for the future)
- The level of security

2.5.2. Network Management

Proper network management is a critical component of an efficient network. Network administrators need tools to monitor the functionality of the network devices, the connections between them, and the services they provide. Simple network Management Protocol (SNMP) has become the de facto standard for use in network management solutions and is tightly connected with remote monitoring (RMON) and Management Information Bases (MIB). Each managed device in the network has several variables that quantify the state of the device. You can monitor managed devices by reading the values of these variables, and you can control managed devices by writing values into these variables.

2.5.2.1. Network Management Architecture

The network management architecture consists of the following:

- **Network management system (NMS)**: A system that executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources that are required for network management.
- **Network management protocol**: A protocol that facilitates the exchange of management information between the NMS and managed devices, including SNMP, MIB, and RMON.
- **Managed devices**: A device (such as a router) managed by an NMS.
- **Management agents**: Software, on managed devices, that collects and stores management information, including SNMP agents and RMON agents.
- **Management information**: Data that is of interest to a device's management, usually stored in MIBs.

A variety of network management applications can be used on a network management system; the choice depends on the network platform (such as the hardware or operating system). The management information

resides on network devices; management agents that reside on the device collect and store data in a standardized data definition structure known as the *MIB*.

The network management application uses SNMP or other network management protocols to retrieve the data that the management agents collect.

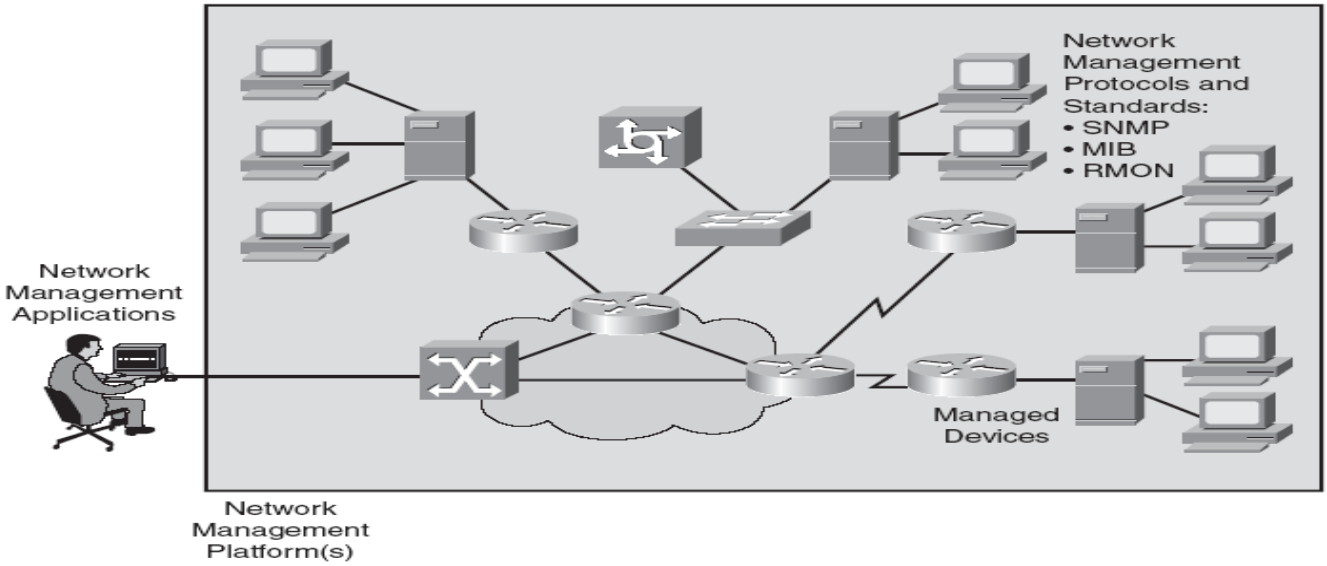


Fig 2.8 Network management protocol

2.5.3. ***Protocols and Standards***

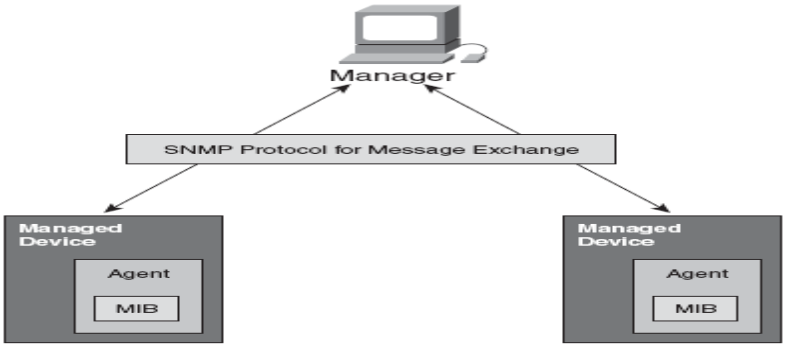
Several protocols are used within the network management architecture. SNMP is the simplest network management protocol. SNMP version 1 (SNMPv1) was extended to SNMP version 2 (SNMPv2) with its variants, which were further extended with SNMP version 3 (SNMPv3). RMON is an extension of the MIB. The MIB typically provides only static information about the managed device; the RMON agent collects specific groups of statistics for long-term trend analysis.

i. SNMP

SNMP has become the de facto standard for network management. SNMP is a simple solution that requires little code to implement, which enables vendors to easily build SNMP agents for their products. In addition, SNMP is often the foundation of the network management architecture. SNMP defines how management information is exchanged between network management applications and management agents. The terms used in SNMP are described as follows:

- **Manager**: The manager, a network management application in an NMS, periodically polls the SNMP agents that reside on managed devices for the data, thereby enabling information to be displayed using a GUI on the NMS. A disadvantage of periodic SNMP polling is the possible delay between when an event occurs and when it is collected by the NMS; there is a trade-off between polling frequency and bandwidth usage.
- **Protocol**: SNMP is a protocol for message exchange. It uses the User Datagram Protocol (UDP) transport mechanism to send and retrieve management information, such as MIB variables.
- **Managed device**: A device (such as a router) managed by the manager.
- **Management agents**: SNMP management agents reside on managed devices to collect and store a range of information about the device and its operation, respond to the manager's requests, and generate traps to inform the manager about certain events. SNMP traps are sent by management agents to the NMS when certain events occur.

- **MIB**: The management agent collects data and stores it locally in the MIB, a database of objects about the device. Community strings, which are similar to passwords, control access to the MIB. To access or set MIB variables, the user must specify the appropriate read or write community string; otherwise, access is denied.



SNMPv1

The initial version of SNMP, SNMPv1 is defined in RFC 1157, *Simple Network Management Protocol (SNMP)*. The protocol's simplicity is apparent by the set of operations that are available. SNMP messages is which the manager uses to transfer data from agents that reside on managed devices. These messages are described as follows:

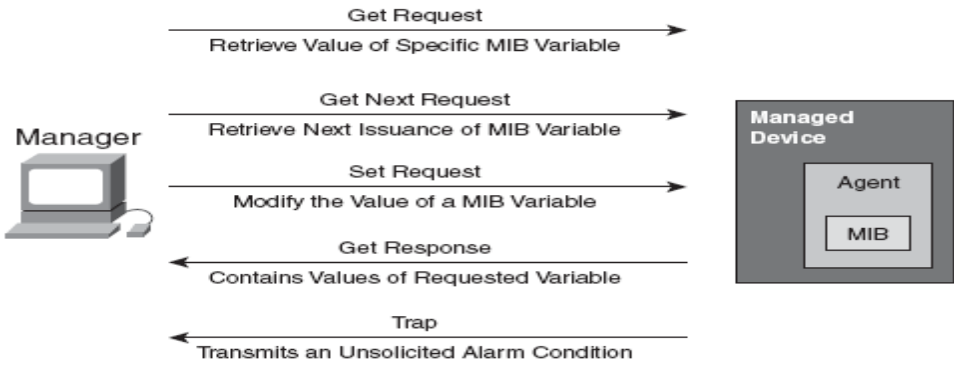
- **Get Request**: Used by the manager to request a specific MIB variable from the agent.
- **Get Next Request**: Used after the initial get request to retrieve the next object instance from a table or list.
- **Set Request**: Used to set a MIB variable on an agent.
- **Get Response**: Used by an agent to respond to a manager's Get Request or Get Next Request message.
- **Trap**: Used by an agent to transmit an unsolicited alarm to the manager. A Trap message is sent when specific conditions occur, such as a change in the state of a device, a device or component failure, or an agent initialization or restart.

SNMPv2

SNMPv2 is a revised protocol that includes performance and manager-to-manager communication improvements to SNMP. SNMPv2 changes include the introduction of the following two new message types:

- **GetBulk message type**: Used for retrieving large amounts of data, such as tables. This message reduces repetitive requests and replies, thereby improving performance.
- **InformRequest**: Used to alert the SNMP manager of a specific condition. Unlike unacknowledged trap messages, InformRequest messages are acknowledged. A managed device sends an InformRequest to the NMS; the NMS acknowledges the receipt of the message by sending a Response message back to the managed device.

Another improvement of SNMPv2 over SNMPv1 is the addition of new data types with 64-bit counters because 32-bit counters were quickly overflowed by fast network interfaces.



MIB

A MIB is a collection of managed objects. A MIB stores information, which is collected by the local management agent, on a managed device for later retrieval by a network management protocol.

Each object in a MIB has a unique identifier that network management applications use to identify and retrieve the value of the specific object. The MIB has a tree-like structure in which similar objects are grouped under the same branch of the MIB tree. For example, different interface counters are grouped under the MIB tree's interfaces branch.

MIB-II

MIB-II is an extension of the original MIB (which is now called *MIB-I*) and is defined by RFC 1213. MIB-II supports a number of new protocols and provides more detailed, structured information. It remains compatible with the previous version, which is why MIB-II retains the same object identifier as MIB-I (1.3.6.1.2.1).

Although the MIB-II definition is an improvement over MIB-I, the following unresolved issues exist:

- MIB-II is still a *device-centric* solution, meaning that its focus is on individual devices, not the entire network or data flows.
- MIB-II is *poll-based*, meaning that data is stored in managed devices and a management system must request (poll) it via the management protocol; the data is not sent automatically.

RMON

RMON is a MIB that provides support for proactive management of LAN traffic.

The RMON standard allows packet and traffic patterns on LAN segments to be monitored. RMON tracks the following items:

- Number of packets
- Packet sizes
- Broadcasts
- Network utilization
- Errors and conditions, such as Ethernet collisions
- Statistics for hosts, including errors generated by hosts, busiest hosts, and which hosts communicate with each other

Without RMON, a MIB could be used to check the device's network performance. However, doing so would lead to a large amount of bandwidth required for management traffic. By using RMON, the managed device itself (via its RMON agent) collects and stores the data that would otherwise be retrieved from the MIB frequently.

RMON agents can reside in routers, switches, hubs, servers, hosts, or dedicated RMON probes. Because RMON can collect a lot of data, dedicated RMON probes are often used on routers and switches instead of enabling RMON agents on these devices. Performance thresholds can be set and reported on if the threshold is breached; this helps reduce management traffic. RMON provides effective network fault diagnosis, performance tuning, and planning for network upgrades.

RMON1

RMON1 works on the data link layer (with MAC addresses) and provides aggregate LAN traffic statistics and analysis for remote LAN segments. Because RMON agents must look at every frame on the network, they might cause performance problems on a managed device. The agent's performance can be classified based on processing power and memory.

RMON1 and RMON2

RMON1 only provides visibility into the data link and the physical layers; potential problems that occur at the higher layers still require other capture and decode tools. Because of RMON1's limitations, RMON2 was developed to extend functionality to upper-layer protocols.

RMON2 is not a replacement for RMON1, but an extension of it. RMON2 extends RMON1 by adding nine more groups that provide visibility to the upper layers. With visibility into the upper-layer protocols, the network manager can monitor any upper-layer protocol traffic for any device or subnet in addition to the MAC layer traffic.

RMON2 allows the collection of statistics beyond a specific segment's MAC layer and provides an end-to-end view of network conversations per protocol. The network manager can view conversations at the network and application layers. Therefore, traffic generated by a specific host or even a specific application (for example, a Telnet client or a web browser) on that host can be observed.

ii. NetFlow

Cisco NetFlow is a measurement technology that measures flows that pass through Cisco devices. NetFlow was originally implemented only on larger devices; it is now available on other devices, including ISRs.

NetFlow answers the questions of what, when, where, and how traffic is flowing in the network. NetFlow data can be exported to network management applications to further process the information, providing tables and graphs for accounting and billing or as an aid for network planning. The key components of NetFlow are the NetFlow cache or data source that stores IP flow information and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector, such as the NetFlow Collection Engine.

NetFlow-collected data serves as the basis for a set of applications, including network traffic accounting, usage-based network billing, network planning, and network monitoring.

iii. CDP

CDP is a Cisco-proprietary protocol that operates between Cisco devices at the data link layer. CDP information is sent only between directly connected Cisco devices; a Cisco device never forwards a CDP frame.

CDP enables systems that support different network layer protocols to communicate and enables other Cisco devices on the network to be discovered. CDP provides a summary of directly connected switches, routers, and other Cisco devices.

CDP is a media- and protocol-independent protocol that is enabled by default on each supported interface of Cisco devices (such as routers, access servers, and switches).

iv. Syslog

It alerts you when something goes wrong or down in your network. Syslog is an excellent tool for system monitoring and is almost always included in your distribution.

Level	Keyword	Description

0	emergencies	System is unusable
1	Alerts	Immediate action is needed
2	Critical	Critical conditions exist
3	Errors	Error conditions exist
4	Warnings	Warning conditions exist
5	Notification	Normal, but significant, conditions exist
6	Informational	Informational messages
7	Debugging	Debugging messages

CHAPTER THREE
Transmission media

3.1. Introduction

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. Transmission media are actually located below the physical layer and are directly controlled by the physical layer. We could say that transmission media belong to layer zero of OSI reference model. Figure 3.1 shows the position of transmission media in relation to the physical layer.

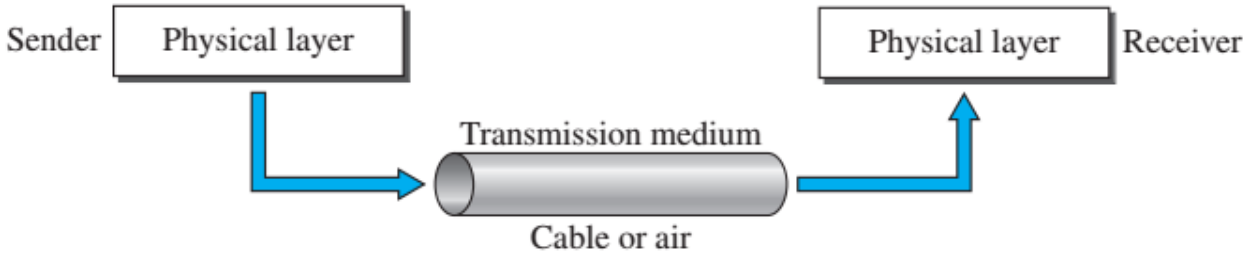


Figure 3.1 Transmission media and physical layer

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

3.2. Guided transmission Media

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

3.2.1. Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure 3.2.

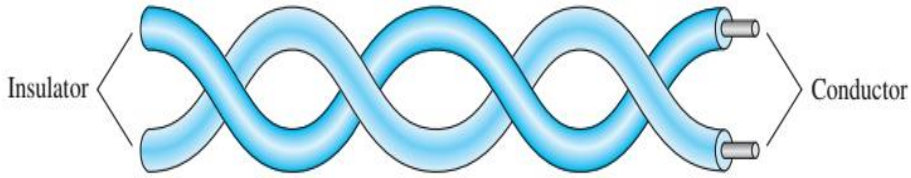


Figure 3.2 Twisted-pair cable Transmission media

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther). This results in a difference at the receiver.

By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out.

From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable. Twisted-pair cables can be unshielded and shielded.

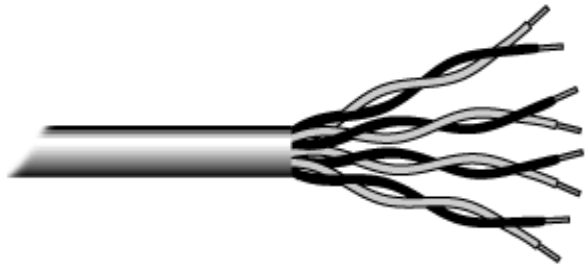
Unshielded *Versus* Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). UTP is cheap and easy to use. However, its performance over long distances is not as good as coaxial cable. The maximum cable length segment of UTP is 100 meters. Most telephone systems use UTP cable (with the RJ11 connector), and many LANs nowadays also use UTP (with the RJ45 connector). IBM has also produced a version of twisted-pair cable for its use, called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive. Our discussion focuses primarily on UTP because STP is seldom used outside of IBM.

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Each EIA category is suitable for specific uses. Table 3.1 shows these categories.

Category	Specification	Data rate (Mbps)	Use
1	Unshielded twisted-pair used in telephone	<0.1	Telephone
2	Unshielded twisted-pair originally used in T lines	2-4	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	16-20	LANs
5	Cable wire is normally with a jacket and outside sheath	100	LANs
5e	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Table 3.1 Categories of unshielded twisted-pair cables



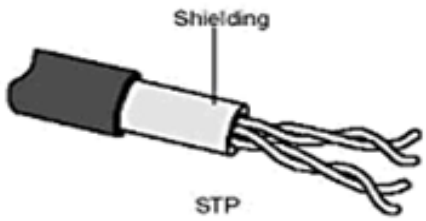


Figure 3.3 (a) Unshielded Twisted-Pair (b) Shielded Twisted-Pair

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a telephone-style connector (RJ-11). 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.

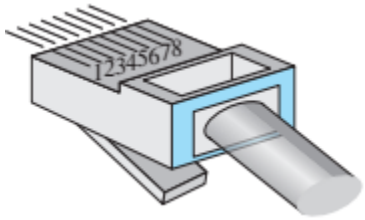


Figure 3.4 RJ-45 connector

UTP connections

The transmit pin of the source device needs to ultimately connect to the receiving pin of the destination device. There are three types of connections that are used to connect different devices.

- Straight through cables
- Crossover Cables
- Rollover cables

1. **Straight through cables**

They are used to connect dissimilar devices.

- Switch/Hub to PC
- Switch/Hub to Router

2. **Cross over cable**

The crossover cable can be used to connect similar devices

- Hub to hub
- Switch to switch
- Hub to switch
- PC to PC
- PC to Router

3. **Console (Rolled) Cable**

Although rolled cable isn't used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a PC to a router console serial communication (com) port (used to connect a PC with console port of a router). If you have a Cisco router or switch, you would use this cable to connect your PC running HyperTerminal to the Cisco hardware.

3.2.2 Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

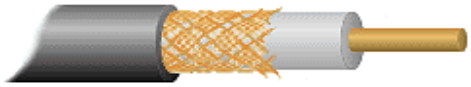


Figure 3.5 Coaxial cable

Although coaxial cabling is difficult to install, it is more resistant to signal interference and attenuation than twisted-pair cabling. The stranded, protective sleeve absorbs stray electronic signals so that they do not affect data being sent over the inner copper cable. For this reason, coaxial cabling is a good choice for longer distances (i.e. it can support greater cable lengths between network devices than twisted pair cable). The two types of coaxial cabling are: Thicknet coaxial and Thinnet coaxial.

Thicknet coaxial cable

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters (can carry a signal for 500 meters). Due to this, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Thicknet cabling is thicker, and a better choice for longer distances, but is more expensive and more difficult to work with.

Thinnet coaxial cable

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. In other word, thinnet coaxial cable can carry a signal for a distance of up to approximately 185 meters before the signal starts to suffer from attenuation.

Thicknet	Thinnet
Has larger diameter	Smaller diameter
Good noise rejection characteristics	Relatively flexible, easier to lay the cable
Longer cable run	Poor noise rejection
Difficult to lay the cable	Supports lower bandwidth
It is rarely used in LANs	No longer in use

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.

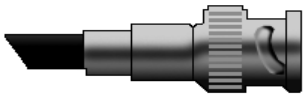


Figure 3.6. BNC connector

3.2.3 Fiber Optic Cable

In fiber-optic cable, optical fibers carry digital data signals in the form of modulated pulses of light. This is a relatively safe way to send data because, unlike copper-based cables that carry data in the form of electronic signals, no electrical impulses are carried over the fiber-optic cable. This means that fiber-optic cable cannot be tapped, and its data cannot be stolen.

Fiber-optic cable is good for very high-speed, high-capacity data transmission because of the purity of the signal and lack of signal attenuation.

An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. Center (core) is made of glass or plastic fibers.

The fibers are sometimes made of plastic. Plastic is easier to install, but cannot carry the light pulses for as long a distance as glass.

Because each glass strand passes signals in only one direction, a cable includes two strands in separate jackets. One strand transmits and the other receives. A reinforcing layer of plastic surrounds each glass strand, and Kevlar fibers provide strength. The Kevlar fibers in the fiber-optic connector are placed between the two cables. Just as their counterparts (twisted-pair and coaxial) are, fiber-optic cables are encased in a plastic coating for protection. 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.

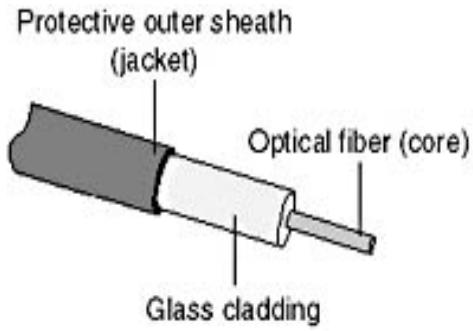


Figure 3.7 Fiber-optic cable

3.2.3.1 Propagation Modes

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics.

A. Multimode

Multimode is so named because multiple beams from a light source move through the core in different paths. Multimode can be implemented in two forms: step-index or graded-index.

Figure 3.8 Multimode (a) Step Index (b) Graded Index

B. Single-Mode

Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber.

Figure 3.9 Single mode

3.2.3.2 Fiber Optic Connector

There are three types of connectors for fiber-optic cables, as shown in Figure 3.10. The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is the same size as RJ45.

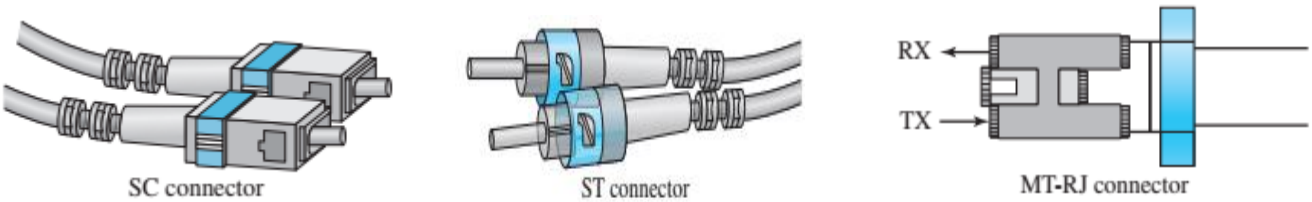


Figure 3.10 Fiber-Optic connectors

3.2.3.3 Advantages and disadvantages of optical fiber cable

Advantages

Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

- Higher bandwidth: Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
- Less signal attenuation: Fiber-optic transmission distance is significantly greater than that of other guided media.
- Immunity to electromagnetic interference: Electromagnetic noise cannot affect fiber-optic cables.
- Resistance to corrosive materials: Glass is more resistant to corrosive materials than copper.
- Light weight: Fiber-optic cables are much lighter than copper cables.
- Greater immunity to tapping: Fiber-optic cables are more immune to tapping than copper cables.

Disadvantages

There are some disadvantages in the use of optical fiber.

- Installation and maintenance: Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- Unidirectional light propagation: Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- Cost: The cable and the interfaces are relatively more expensive than those of other guided media.

3.2.4 Cable Specifications

The three parameters required for cable specification are:

- Speed
- Transmission Type – Digital (Baseband) or Analog (Broadband)
- Maximum Length – determines how far the signal can travel before getting attenuated.

The following are examples of Ethernet specifications relate to cable type:

Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100 meters
10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Fiber Optic	2000 meters
100BaseT	Unshielded Twisted Pair	100 meters
100BaseTX	Unshielded Twisted Pair	220 meters

3.3 Unguided transmission Medias

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Figure 3.11 shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

Unguided signals can travel from the source to the destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure 3.12.

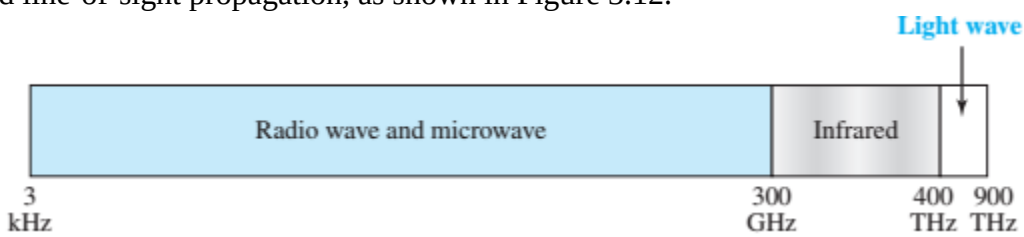


Figure 3.11 Electromagnetic spectrum for wireless communication

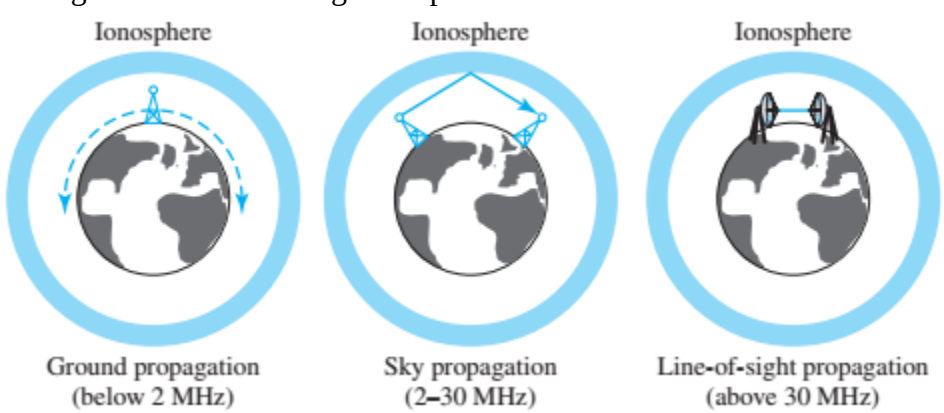


Figure 3.12 Propagation methods

In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance.

In sky propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.

In line-of-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not

to be affected by the curvature of the earth. Line-of sight propagation is tricky because radio transmissions cannot be completely focused.

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

3.3.1. Radio waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves.

Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

Radio waves, particularly those of low and medium frequencies, can penetrate walls. Using any part of the radio wave band requires permission from the authorities.

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

3.3.2. Microwaves

Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. Repeaters are often needed for long distance communication. Very high-frequency microwaves cannot penetrate walls. Use of certain portions of microwave band requires permission from authorities. Two types of antennas are used for microwave communications: the parabolic dish and the horn.

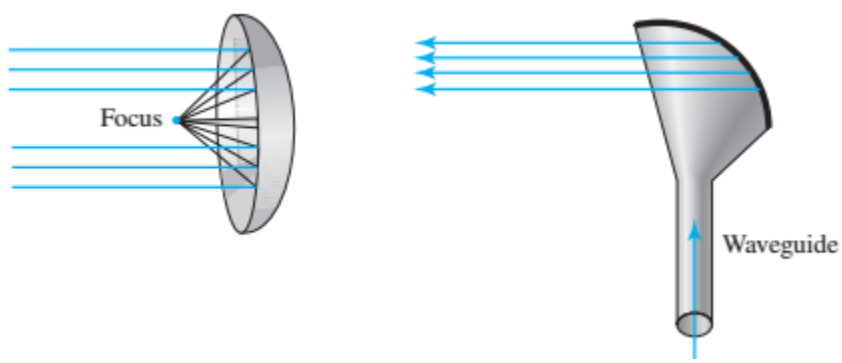


Figure 3.13 Unidirectional antennas (a) Parabolic dish (b) The horn

A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus.

Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.

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

3.3.3. Infrared waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. However, this same characteristic makes infrared signals useless

for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication. Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

3.4 Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Chapter four

The OSI and TCP/IP communication models

4.1. Open Systems Interconnection (OSI) model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. 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. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network. An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

4.1.1 Layered Architecture

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).

The following figure 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. In this case the intermediate node is a router.

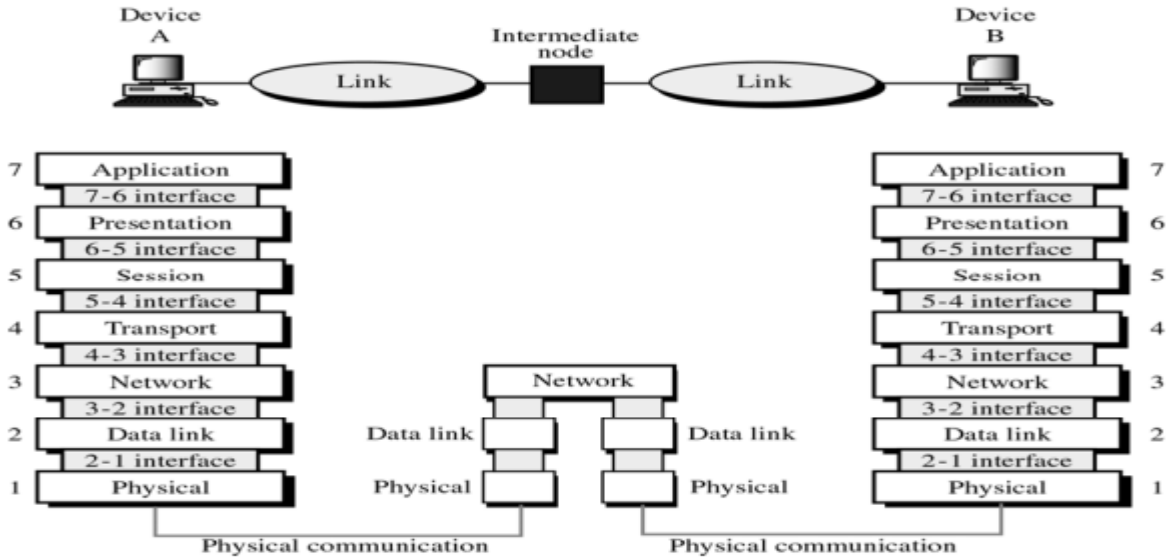


Figure 5.1 Sending message from device A to device B

In developing the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x* on one machine communicates with layer *x* on another machine. This communication is

governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

4.1.2. Organization of the Layers

The seven layers can be thought of as belonging to three subgroups. 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.

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 or optical signal and transported along a physical link.

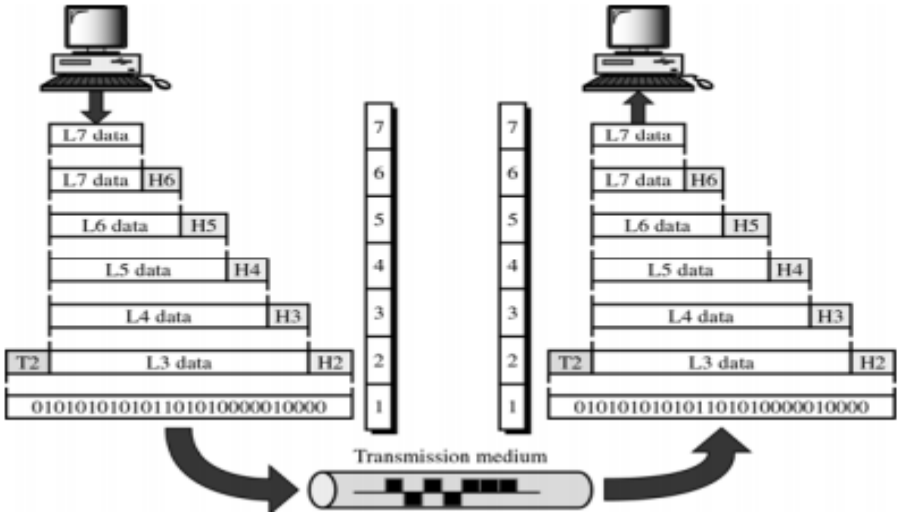


Figure 5.2 Headers and Trailer

Encapsulation

Figure 5.2 reveals another aspect of data communications in the OSI model: encapsulation. 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.

In other words, 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.

4.1.3. Layers in the OSI model

i. Physical Layer

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 5.3 shows the position of the physical layer with respect to the transmission medium and the data

link layer.

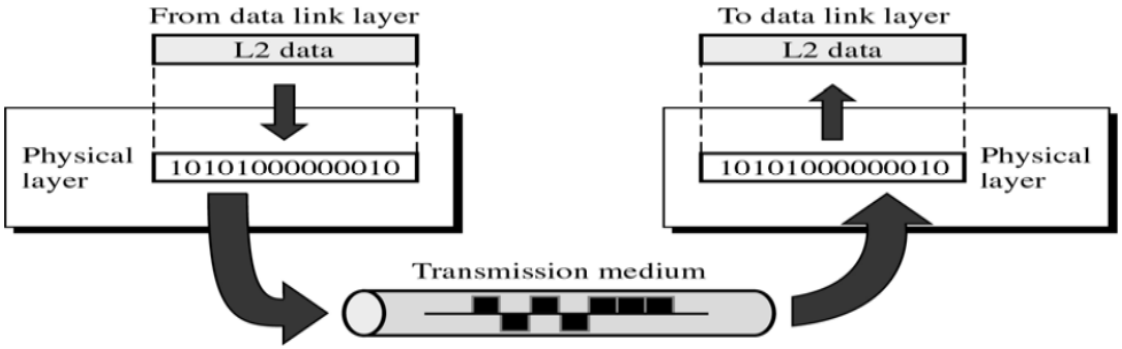


Figure 5.3 Physical Layer

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

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. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
- 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, a star topology, a ring topology, a bus topology, or a hybrid topology.
- Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

ii. Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Figure 5.4 shows the relationship of the data link layer to the network and physical layers.

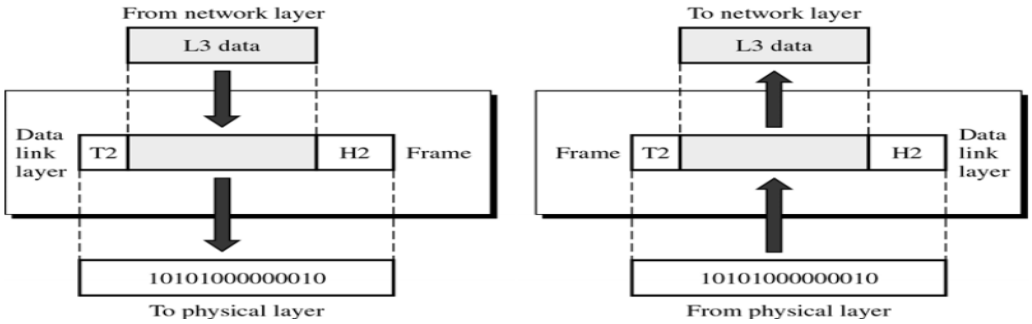


Figure 5.4 Data link layer

The data link layer is responsible for moving frames from one hop (node) to the next.

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.

iii. Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure 5.5 shows the relationship of the network layer to the data link and transport layers.

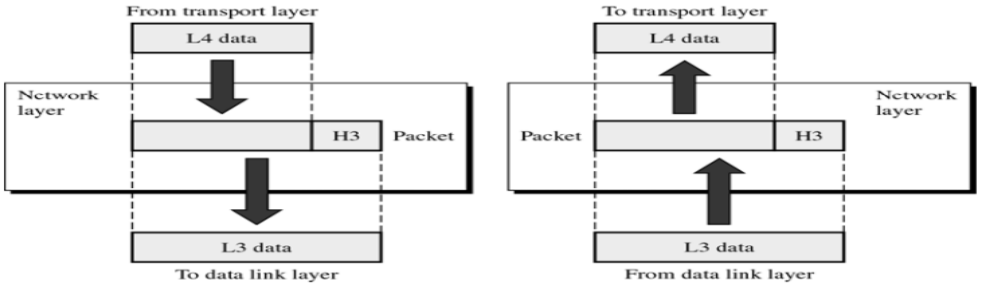


Figure 5.5 Network Layer

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

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.

iv. Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Figure 5.6 shows the relationship of the transport layer to the network and session layers.

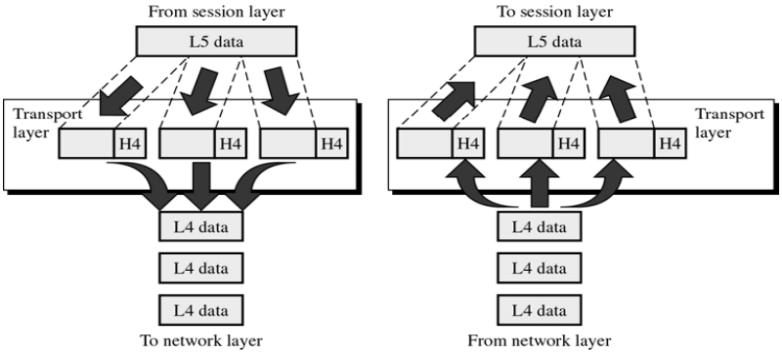


Figure 5.6 Transport Layer

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

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.

v. Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the interaction among communicating systems.

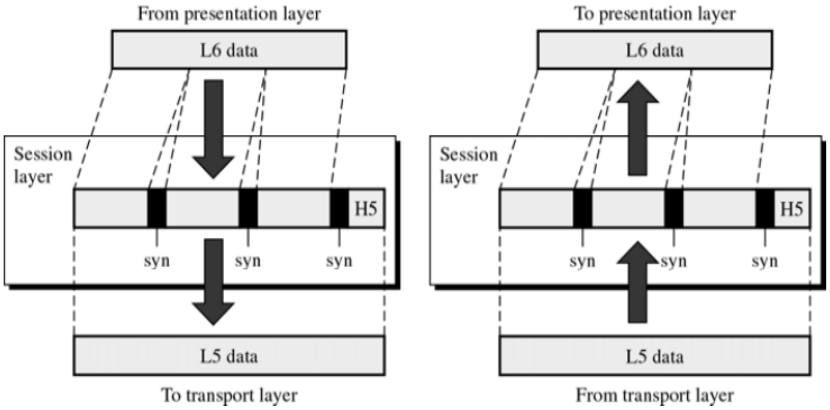


Figure 5.7 Session Layer

The session layer is responsible for dialog control and synchronization.

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.

vi. Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Figure 5.8 shows the relationship between the presentation layer and the application and session layers.

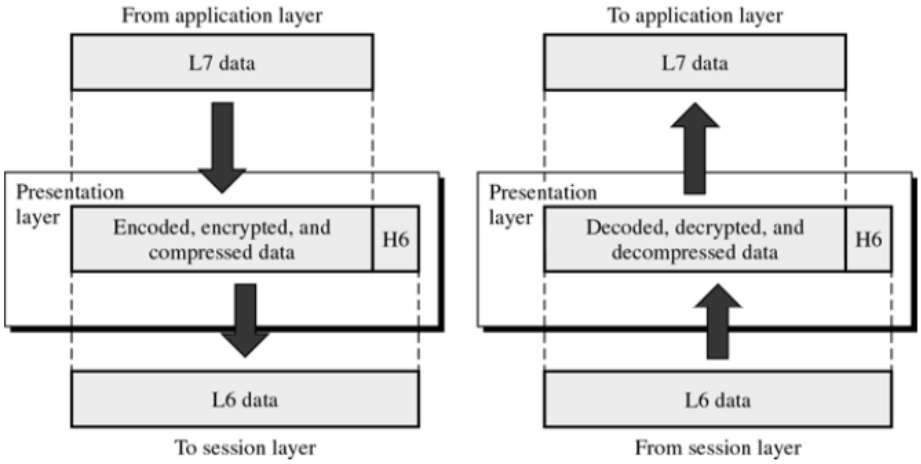


Figure 5.8 Presentation Layer

The presentation layer is responsible for translation, compression, and encryption.

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.

vii. Application Layer

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 5.9 shows the relationship of the application layer to the user and the presentation layer. Of the many application services available, the figure shows only three: *X.400* (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs X.400 to send an e-mail message.

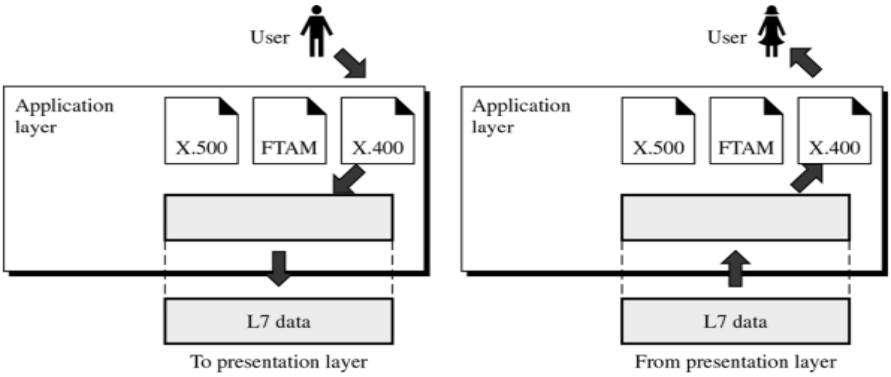


Figure 5.9 Application Layer

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

Specific services provided by the application layer include the following:

- 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.

4.2. TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP

protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network (Hardware), internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer. So in this course, we assume that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and 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 top most layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.

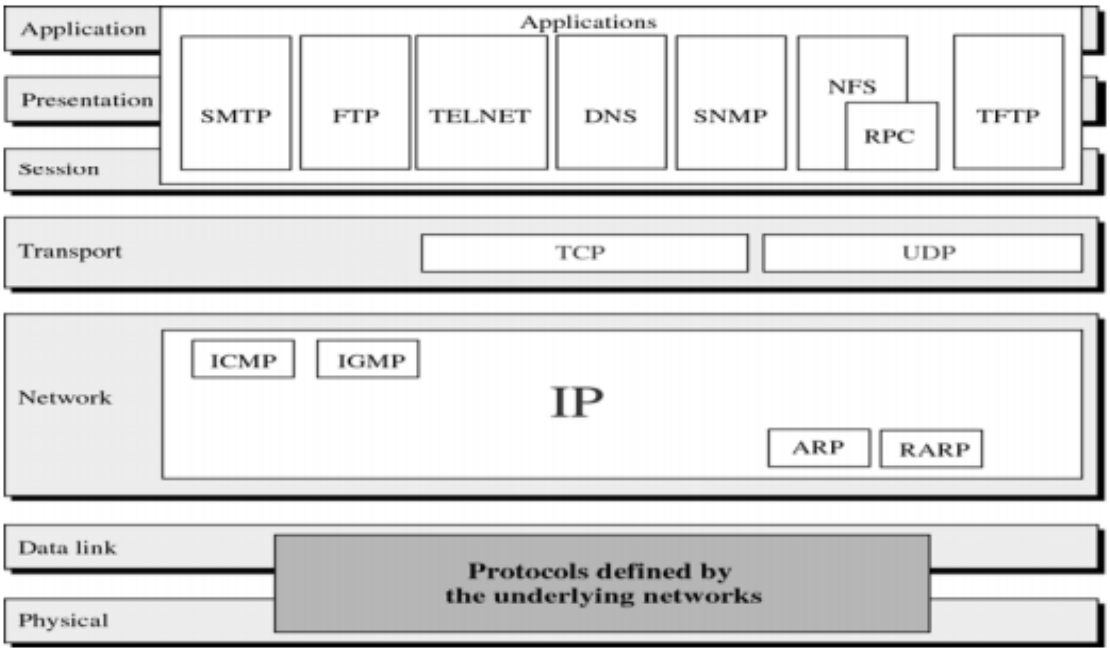


Figure 5.10 TCP/IP Protocol suites

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the *TCP/IP* protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term *hierarchical* means that each upper-level protocol is supported by one or more lower-level protocols.

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. Now, let us see a brief description of each Layers of TCP/IP model.

1. **Physical and Data Link Layers**

At the physical and data link layers, *TCP/IP* does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a *TCP/IP* internetwork can be a local-area network or a wide-area network.

2. **Network Layer**

At the network layer (or, more accurately, the internetwork layer), *TCP/IP* supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP. Each of these protocols is described in the previous chapter (Chapter Four).

Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. 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 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

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.

The limited functionality of IP should not be considered a weakness, however. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

3. Transport Layer

Traditionally the transport layer was represented in *TCP/IP* by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP 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.

4. Application Layer

The *application layer* in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer.

Unit 5

Network Addressing, subnetting and masking

Introduction

In the mid-1990's, the Internet is a dramatically different network than when it was first established in the early 1980's. Today, the Internet has entered the public consciousness as the world's largest public data network, doubling in size every nine months. This is reflected in the tremendous popularity of the World Wide Web (WWW), the opportunities that businesses see in reaching customers from virtual storefronts, and the emergence of new types and methods of doing business. It is clear that expanding business and social awareness will continue to increase public demand for access to resources on the Internet.

There is a direct relationship between the value of the Internet and the number of sites connected to the Internet. As the Internet grows, the value of each site's connection to the Internet increases because it provides the organization with access to an ever expanding user/customer population.

An overview of IP (Internet Protocol) address

An IP address is a logical address of a computer which is expressed as a four 8-bit group of bits (a total of 32 bits) separated by periods. Each 8-bit group of bits can be represented by a 4-digit decimal that spans between 0 and 255. For example 196.27.22.42 is a typical IP address of the DNS server of the Ethiopian Telecommunication Corporation (ETC). The total number of distinct addresses one can have from this 32 bit addressing scheme is 2^{32} = 4,294,967,296.

A host needs an IP address to participate on the Internet. The IP address is a logical network address that identifies a particular host. It must be properly configured and unique in order to communicate with other devices on the Internet.

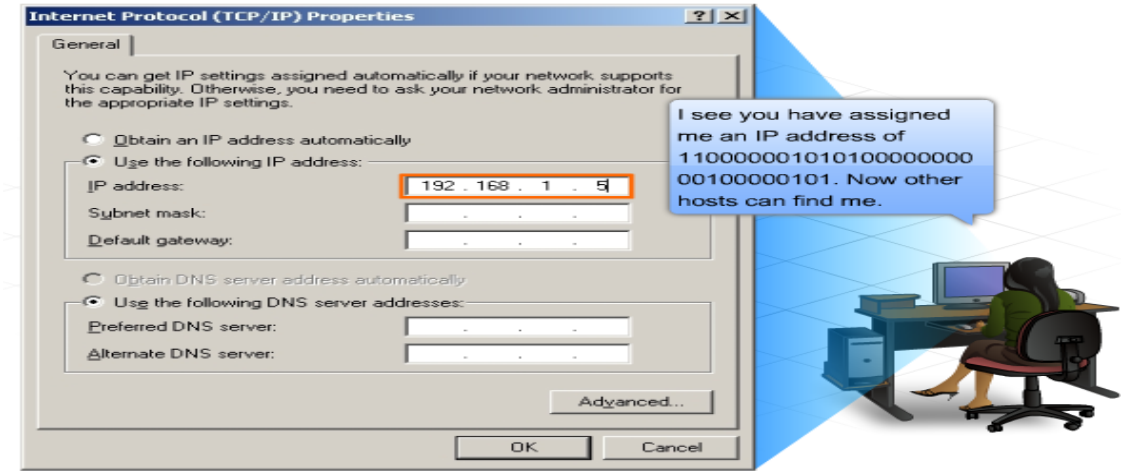
Structure of IP address

An IP address is simply a series of 32 binary bits (ones and zeros). It is very difficult for humans to read a binary IP address. For this reason, the 32 bits are grouped into four 8-bit bytes called octets. An IP address in this format is hard for humans to read, write and remember. To make the IP address easier to understand, each octet is presented as its decimal value, separated by a decimal point or period. This is referred to as dotted-decimal notation.

When a host is configured with an IP address, it is entered as a dotted decimal number such as 192.168.1.5. Imagine if you had to enter the 32-bit binary equivalent of this- 11000000101010000000000100000101. If just

one bit was mistyped, the address would be different and the host may not be able to communicate on the network.

The 32-bit IP address is defined with IP version 4 (IPv4) and is currently the most common form of IP address on the Internet. There are over 4 billion possible IP addresses using a 32-bit addressing scheme.



When a host receives an IP address, it looks at all 32 bits as they are received by the NIC. Humans, on the other hand, need to convert those 32 bits into their four octet decimal equivalent. Each 4 octet is made up of 8 bits and each bit has a value. The four groups of 8 bits have the same set of values. The rightmost bit in an octet has a value of 1 and the values of the remaining bits, from right to left, are 2, 4, 8, 16, 32, 64 and 128.

Determine the value of the octet by adding the values of positions wherever there is a binary 1 present.

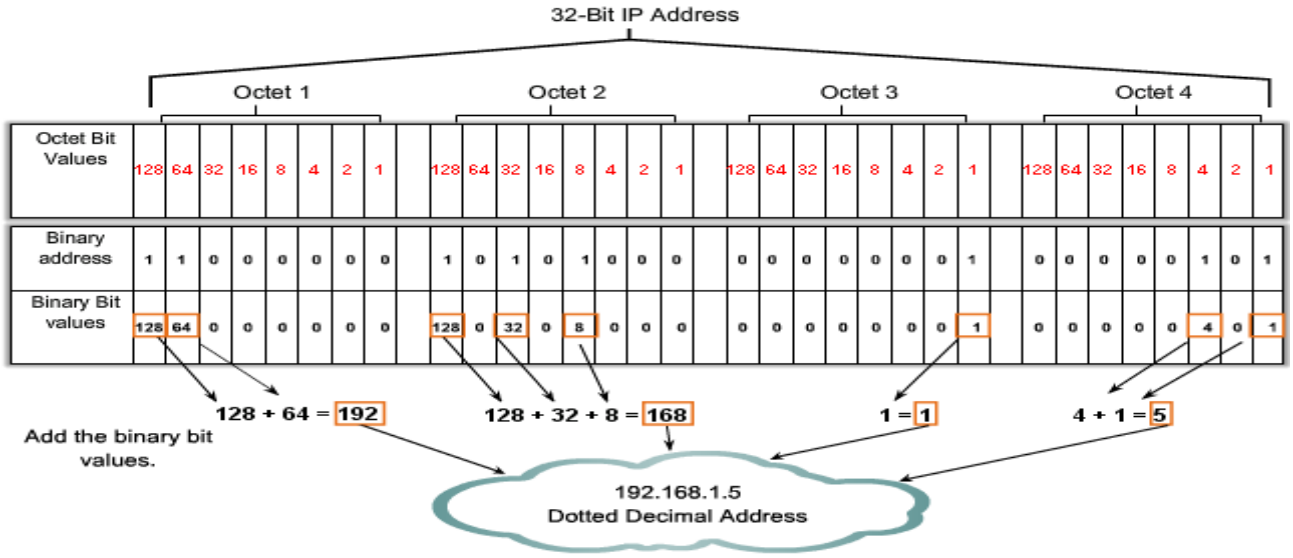
If there is a 0 in a position, do not add the value.

If all 8 bits are 0s. 00000000 the value of the octet is 0.

If all 8 bits are 1s, 11111111 the value of the octet is 255 (128+64+32+16+8+4+2+1).

If the 8 bits are mixed, such as the example 00100111, the value of the octet is 39 (32+4+2+1).

So the value of each of the four octets can range from 0 to a maximum of 255.

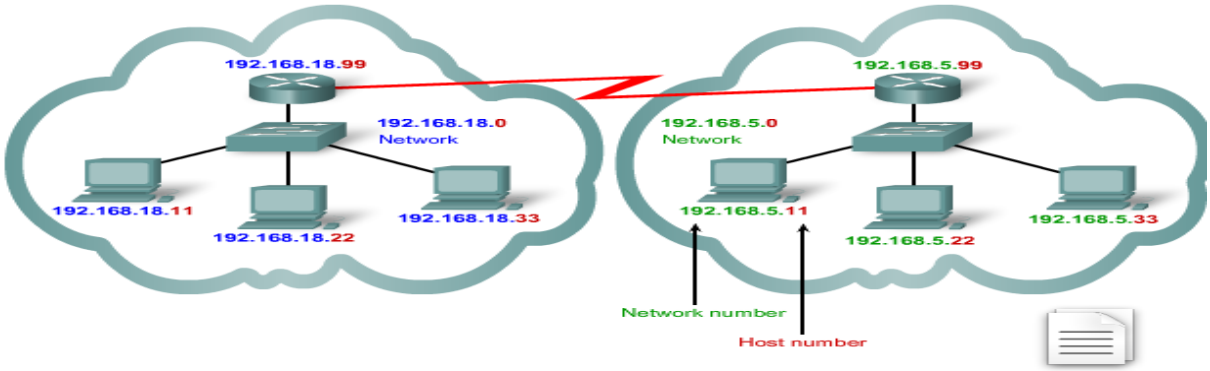


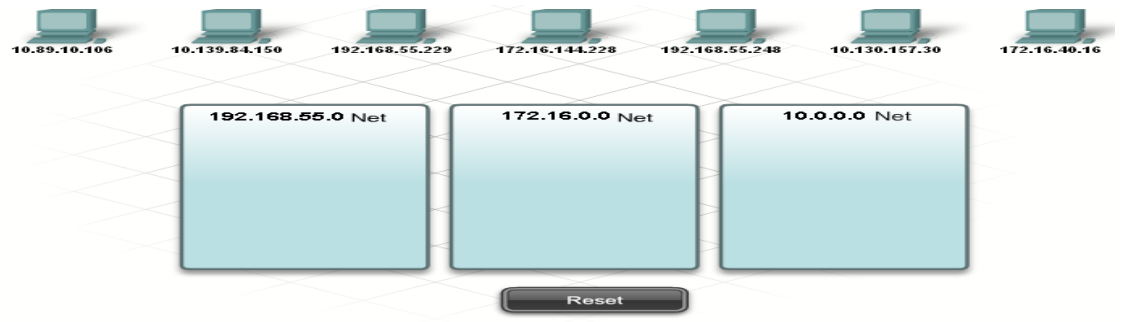
Parts of IP address

The logical 32-bit IP address is hierarchical and is made up of two parts. The first part identifies the *network* and the second part identifies *a host* on that network. Both parts are required in an IP address.

As an example, if a host has IP address 192.168.18.57 the first three octets (i.e. 192.168.18) identify the network portion of the address, and the last octet (i.e. 57) identifies the host. This is known as hierarchical addressing because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each network, rather than needing to know the location of each individual host.

Another example of a hierarchical network is the telephone system. With a telephone number, the country code, area code and exchange represent the network address and the remaining digits represent a local phone number.





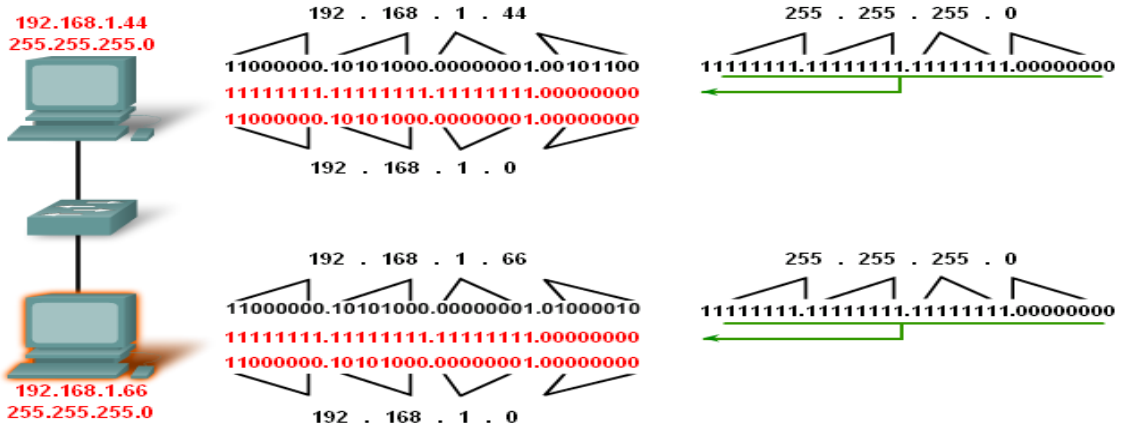
How IP address and Subnet mask Interact

There are two parts to every IP address. How do hosts know which portion is the network and which is the host? This is the job of the subnet mask.

When an IP host is configured, a subnet mask is assigned along with an IP address. Like the IP address, the subnet mask is 32 bits long. The subnet mask signifies which part of the IP address is network and which part is host.

The subnet mask is compared to the IP address from left to right, bit for bit. The 1s in the subnet mask represent the network portion; the 0s represent the host portion. In the example shown, the first three octets are network, and the last octet represents the host.

When a host sends a packet, it compares its subnet mask to its own IP address and the destination IP address. If the network bits match, both the source and destination host are on the same network and the packet can be delivered locally. If they do not match, the sending host forwards the packet to the local router interface to be sent on to the other network.



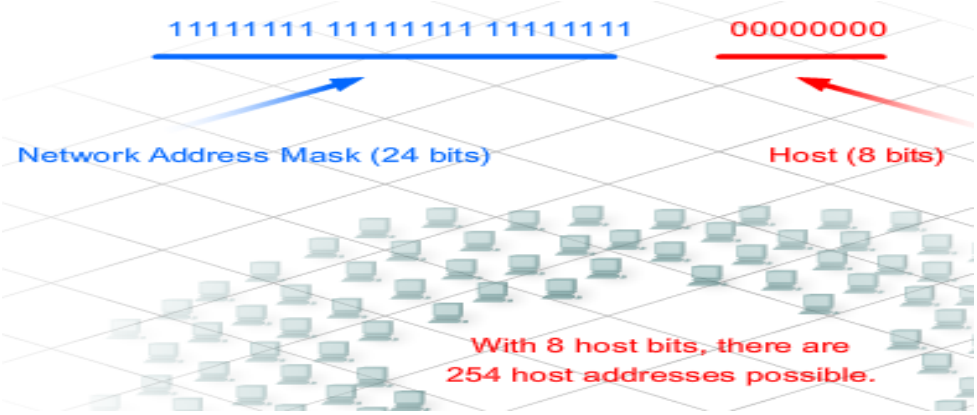
The subnet masks we see most often with home and small business networking are: 255.0.0.0 (8-bits), 255.255.0.0 (16 bits) and 255.255.255.0 (24 bits). A subnet mask of 255.255.255.0 (decimal) or

11111111.11111111.1111111.00000000 (binary) uses 24 bits to identify the network number which leaves 8 bits to number the hosts on that network.

To calculate the number of hosts that can be on that network, take the number 2 to the power of the number of host bits (2^8 = 256). From this number, we must subtract 2 (256-2). The reason we subtract 2 is because all 1s within the host portion of an IP address is a broadcast address for that network and cannot be assigned to a specific host. All 0s within the host portion indicates the network ID and again, cannot be assigned to a specific host.

Another way to determine the number of hosts available is to add up the values of the available host bits (128+64+32+16+8+4+2+1 = 255). From this number, subtract 1 (255-1 = 254), because the host bits cannot be all 1s. It is not necessary to subtract 2 because the value of all 0s is 0 and is not included in the addition.

With a 16-bit mask, there are 16 bits (two octets) for host addresses and a host address could have all 1s (255) in one of the octets. This might appear to be a broadcast but as long as the other octet is not all 1s, it is a valid host address. Remember that the host looks at all host bits together, not at octet values.

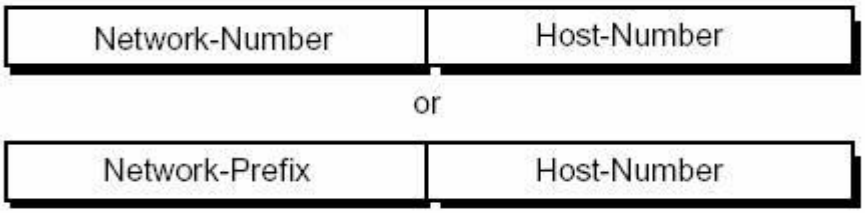


Standard IP Address Classes

Classful IP Addressing

When IP was first standardized in September 1981, the specification required that each system attached to an IP based internet be assigned a unique, 32-bit Internet address value. Some systems, such as routers which have interfaces to more than one network, must be assigned a unique IP address for each network interface.

The first part of an Internet address identifies the network on which the host resides, while the second part identifies the particular host on the given network. This created the two level addressing hierarchy which is illustrated in the figure below.

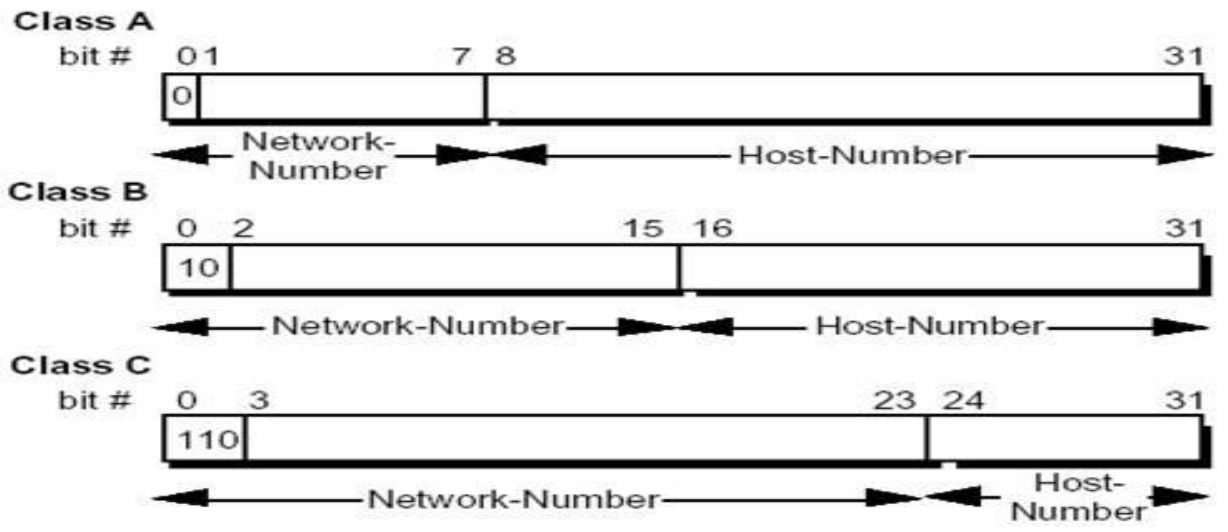


Two level IP address structure

In recent years, the network number field has been referred to as the "network-prefix" because the leading portion of each IP address identifies the network number. All hosts on a given network share the same network-prefix but must have a unique host-number. Similarly, any two hosts on different networks must have different network-prefixes but may have the same host-number.

Primary Address Classes

In order to provide the flexibility required to support different size networks, the designers decided that the IP address space should be divided into three different address classes - Class A, Class B, and Class C. This is often referred to as "classful" addressing because the address space is split into three predefined classes, groupings, or categories. Each class fixes the boundary between the network-prefix and the host number at a different point within the 32-bit address. The formats of the fundamental address classes are illustrated in the figure below.



Principle/Standard classful IP address formats

Class	Initial Bits	Available Nodes/Hosts	Starting Address	Remark
A B C	0xxxxxxx. 10xxxxxx. 110xxxxx.	2^{24} = 16,777,214 2^{16} = 65,536 2^{8} = 256	0 – 126 128 – 191 192 - 223	127 is reserved for network testing (Loopback)
D	1110xxxx.		224-239	Reserved for Multicast
E	1111xxxx.		240 - 255	Reserved for research

The table above displays the range of dotted-decimal values that can be assigned to each of the three principle address classes. The "xxx" represents the host-number field of the address which is assigned by the local network administrator.

One of the fundamental features of classful IP addressing is that each address contains a self-encoding key that identifies the dividing point between the network-prefix and the host-number. For example, if the first two bits of an IP address are 1-0, the dividing point falls between the 15th and 16th bits. This simplified the routing system during the early years of the Internet because the original routing protocols did not supply a "deciphering key" or "mask" with each route to identify the length of the network-prefix.

Class A Networks (/8 Prefixes)

Each Class A network address has an 8-bit network-prefix with the highest order bit set to 0 and a seven-bit network number, followed by a 24-bit host-number. Today, it is no longer considered 'modern' to refer to a Class A network. Class A networks are now referred to as "/8s" (pronounced "slash eight" or just "eights") since they have an 8-bit network-prefix.

A maximum of 126 (2^7-2) /8 networks can be defined. The calculation requires that the 2 is subtracted because the /8 network 0.0.0.0 is reserved for use as the default route and the /8 network 127.0.0.0 (also written 127/8 or 127.0.0.0/8) has been reserved for the "loopback" function. Each /8 supports a maximum of 16,777,214 (2^{24}-2) hosts per network. The host calculation requires that 2 is subtracted because the all-0s ("this network") and all-1s ("broadcast") host-numbers may not be assigned to individual hosts. Since the /8 address block contains 2^{31} (2,147,483,648) individual addresses and the IPv4 address space contains a maximum of 2^{32} (4,294,967,296) addresses, the /8 address space is 50% of the total IPv4 unicast address space.

Class B Networks (/16 Prefixes)

Each Class B network address has a 16-bit network-prefix with the two highest order bits set to 1-0 and a 14-bit network number, followed by a 16-bit host-number. Class B networks are now referred to as"/16s" since they

have a 16-bit network-prefix. A maximum of 16,384 (2^{14}) /16 networks can be defined with up to 65,534 (2^{16}-2) hosts per network. Since the entire /16 address block contains 2^{30} (1,073,741,824) addresses, it represents 25% of the total IPv4 unicast address space.

Class C Networks (/24 Prefixes)

Each Class C network address has a 24-bit network-prefix with the three highest order bits set to 1-1-0 and a 21-bit network number, followed by an 8-bit host-number. Class C networks are now referred to as "/24s" since they have a 24-bit network-prefix. A maximum of 2,097,152 (2^{21}) /24 networks can be defined with up to 254 (2^{8}-2) hosts per network. Since the entire /24 address block contains 2^{29} (536,870,912) addresses, it represents 12.5% (or 1/8th) of the total IPv4 unicast address space.

Other Classes

In addition to the three most popular classes, there are two additional classes. Class D addresses have their leading four-bits set to 1-1-1-0 and are used to support IP Multicasting. Class E addresses have their leading four-bits set to 1-1-1-1 and are reserved for experimental use.

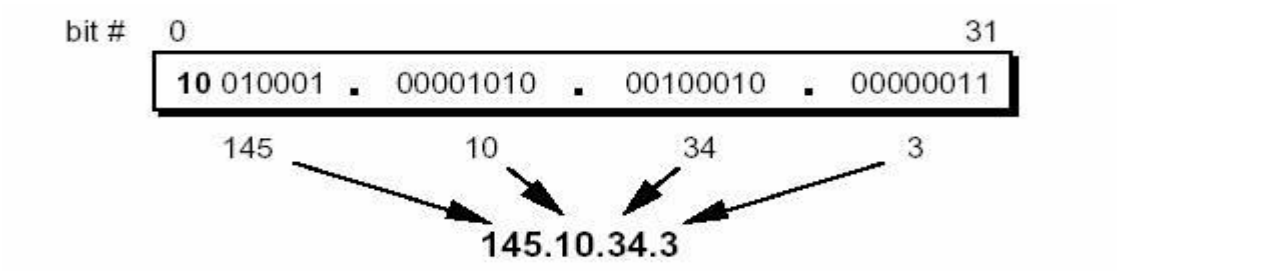
IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits don't change)	Network (N) and Host (H) parts of an address	Default subnet mask (decimal and binary)	Numbers of possible networks and hosts per network
A	1 - 127	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 nets (2^7-2) 16,777,214 hosts per net (2^24-2)
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16,382 nets (2^14-2) 65,534 hosts per net (2^16-2)
C	192 - 223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.11111111.00000000	2,097.150 nets (2^21-2) 254 hosts per net (2^8-2)
D	224 - 239	11100000 - 11101111	Not for commercial use as a host		
E	240 - 255	11110000 - 11111111	Not for commercial use as a host		

Dotted-Decimal Notation

To make Internet addresses easier for human users to read and write, IP addresses are often expressed as four decimal numbers, each separated by a dot. This format is called *"dotted-decimal notation*." Dotted-decimal notation divides the 32-bit Internet address into four 8-bit (byte) fields and specifies the value of each field

independently as a decimal number with the fields separated by dots. Figure below shows how a typical /16 (Class B) Internet address can be expressed in dotted decimal notation.



Dotted-decimal-notation

Types of IP address

Public and Private IP Addresses

All hosts that connect directly to the Internet require a unique public IP address. Because of the finite number of 32-bit addresses available, there is a risk of running out of IP addresses. One solution to this problem was to reserve some private addresses for use exclusively inside an organization. This allows hosts within an organization to communicate with one another without the need of a unique public IP address. RFC 1918 is a standard that reserves several ranges of addresses within each of the classes A, B and C. As shown in the table, these private address ranges consist of a single Class A network, 16 Class B networks and 256 Class C networks. This gives a network administrator considerable flexibility in assigning internal addresses.

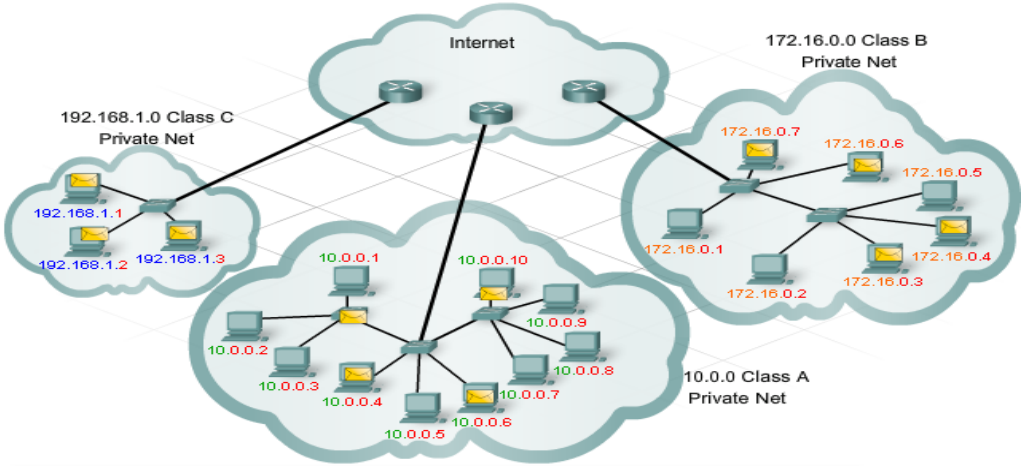
A very large network can use the Class A private network, which allows for over 16 million private addresses. On medium size networks, a Class B private network could be used, which provides over 65,000 addresses per network. Home and small business networks typically use a single class C private address, which allows up to 254 hosts per network.

The Class A network, the 16 Class B networks, or the 256 Class C networks can be used within any size organization. Typically, many organizations use the Class A private network.

Calss	Network Address	Number of Networks	Number of Addresses
A	10.0.0.0-10.255.255.255	1	16,777,216
B	172.16.0.0 – 172.31.255.255	16	1,048,576
C	192.168.0.0 – 192.168.255.255	256	65,536

Private addresses can be used internally by hosts in an organization as long as the hosts do not connect directly to the Internet. Therefore, the same set of private addresses can be used by multiple organizations. Private addresses are not routed on the Internet and will be quickly blocked by an ISP router.

The use of private addresses can provide a measure of security since they are only visible on the local network, and outsiders cannot gain direct access to the private IP addresses.



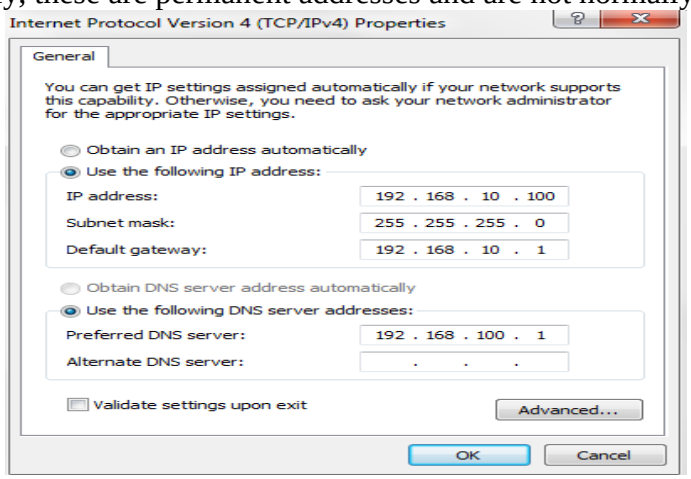
IP Address Assignment

IP addresses can be assigned for devices either statically or dynamically.

1. ***Static IP Address Assignment***

With a static assignment, the network administrator must manually configure the network information for a host. At a minimum, this includes the host IP address, subnet mask and default gateway. Static addresses have some advantages. For instance, they are useful for printers, servers and other networking devices that need to be accessible to clients on the network. If hosts normally access a server at a particular IP address, it would not be good if that address changed. Static assignment of addressing information can provide increased control of network resources, but it can be time consuming to enter the information on each host. When entering IP addresses statically, the host only performs basic error checks on the IP address. Therefore, errors are more likely to occur.

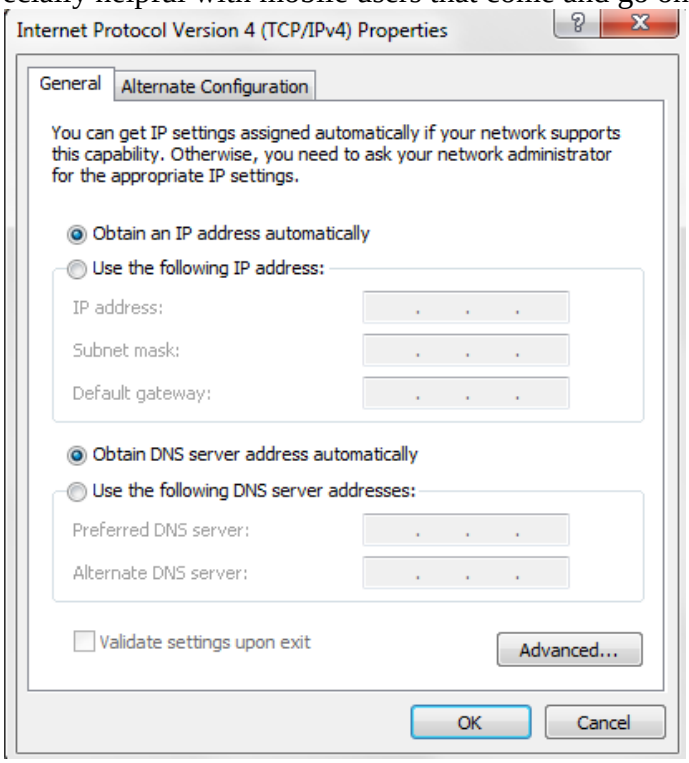
When using static IP addressing, it is important to maintain an accurate list of which IP addresses are assigned to which devices. Additionally, these are permanent addresses and are not normally reused.



2. ***Dynamic IP Address Assignment***

On local networks it is often the case that the user population changes frequently. New users arrive with laptops and need a connection. Others have new workstations that need to be connected. Rather than have the network administrator assign IP addresses for each workstation, it is easier to have IP addresses assigned automatically. This is done using a protocol known as Dynamic Host Configuration Protocol (DHCP). DHCP provides a mechanism for the automatic assignment of addressing information such as IP address, subnet mask, default

gateway, and other configuration information. DHCP is generally the preferred method of assigning IP addresses to hosts on large networks since it reduces the burden on network support staff and virtually eliminates entry errors. Another benefit of DHCP is that an address is not permanently assigned to a host but is only leased for a period of time. If the host is powered down or taken off the network, the address is returned to the pool for reuse. This is especially helpful with mobile users that come and go on a network.

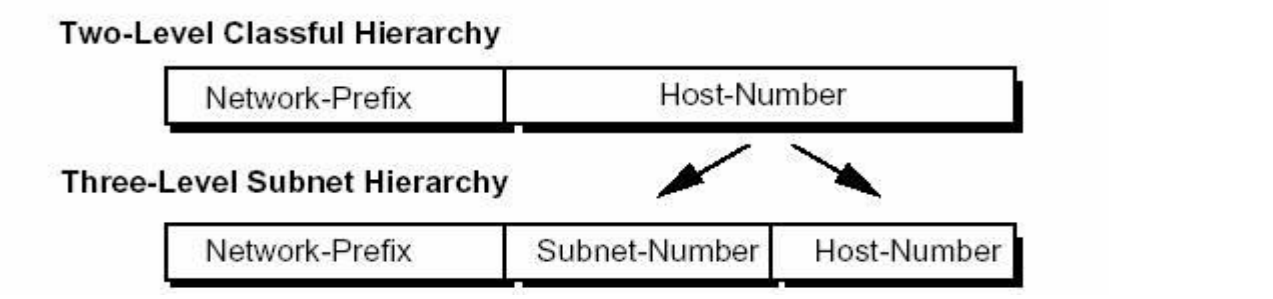


Subnetting

In 1985, RFC 950 defined a standard procedure to support the subnetting, or division, of a single Class A, B, or C network number into smaller pieces. Subnetting was introduced to overcome some of the problems that parts of the Internet were beginning to experience with the classful two-level addressing hierarchy:

- Internet routing tables were beginning to grow.
- Local administrators had to request another network number from the Internet before a new network could be installed at their site.

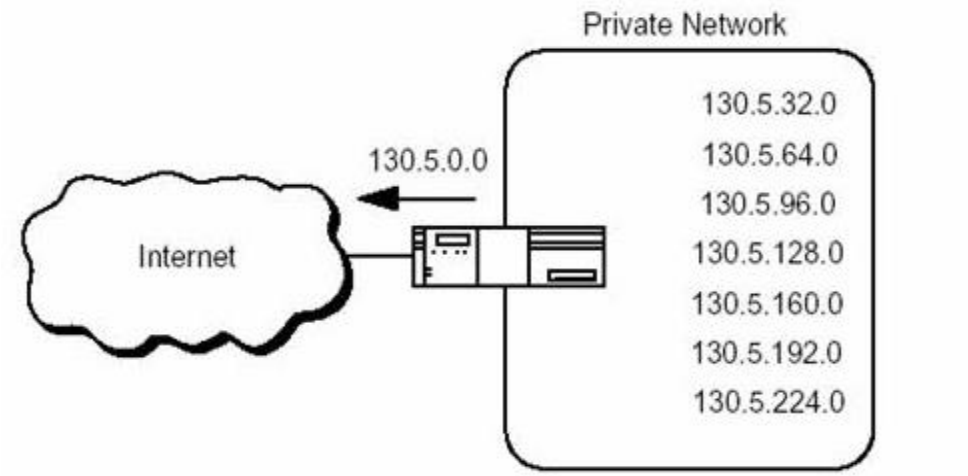
Both of these problems were attacked by adding another level of hierarchy to the IP addressing structure. Instead of the classful two-level hierarchy, subnetting supports a three-level hierarchy. The figure below illustrates the basic idea of subnetting which is to divide the standard classful *host-number field* into two parts - the subnet-number and the host number on that subnet.



Subnet address hierarchy

Subnetting attacked the expanding routing table problem by ensuring that the subnet structure of a network is never visible outside of the organization's private network. The route from the Internet to any subnet of a given IP address is the same, no matter which subnet the destination host is on. This is because all subnets of a given network number use the same network-prefix but different subnet numbers. The routers within the private organization need to differentiate between the individual subnets, but as far as the Internet routers are concerned, all of the subnets in the organization are collected into a single routing table entry. This allows the local administrator to introduce arbitrary complexity into the private network without affecting the size of the Internet's routing tables.

Subnetting overcame the registered number issue by assigning each organization one (or at most a few) network number(s) from the IPv4 address space. The organization was then free to assign a distinct subnetwork number for each of its internal networks. This allows the organization to deploy additional subnets without needing to obtain a new network number from the Internet.



Subnetting reduces the routing requirements of the internet

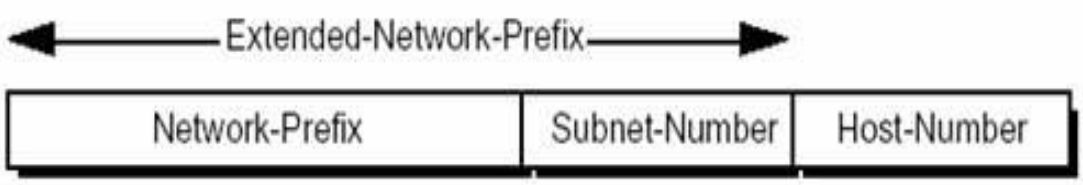
In figure above, a site with several logical networks uses subnet addressing to cover them with a single /16 (Class B) network address. The router accepts all traffic from the Internet addressed to network 130.5.0.0, and

forwards traffic to the interior subnetworks based on the third octet of the classful address. The deployment of subnetting within the private network provides several benefits:

- The size of the global Internet routing table does not grow because the site administrator does not need to obtain additional address space and the routing advertisements for all of the subnets are combined into a single routing table entry.
- The local administrator has the flexibility to deploy additional subnets without obtaining a new network number from the Internet.
- Route flapping (i.e., the rapid changing of routes) within the private network does not affect the Internet routing table since Internet routers do not know about the reachability of the individual subnets - they just know about the reachability of the parent network number.

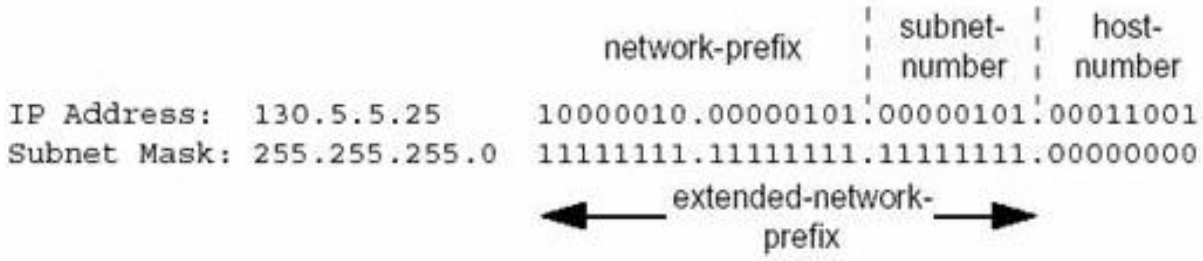
Extended-Network-Prefix

Internet routers use only the network-prefix of the destination address to route traffic to a subnetted environment. Routers within the subnetted environment use the extended-network- prefix to route traffic between the individual subnets. The extended-network-prefix is composed of the classful network-prefix and the subnet-number.



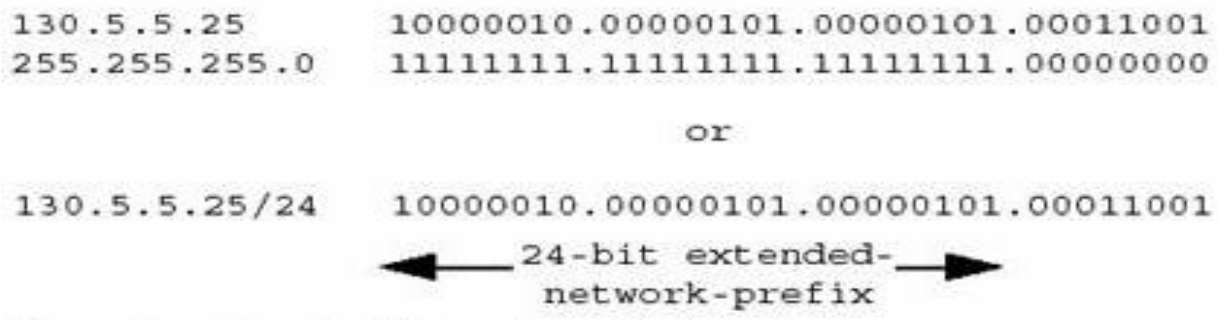
Extended-Network-Prefix

The extended-network-prefix has traditionally been identified by the subnet mask. For example, if you have the /16 address of 130.5.0.0 and you want to use the entire third octet to represent the subnet-number, you need to specify a subnet mask of 255.255.255.0. The bits in the subnet mask and the Internet address have a one-to-one correspondence. The bits of the subnet mask are set to 1 if the system examining the address should treat the corresponding bit in the IP address as part of the extended-network-prefix. The bits in the mask are set to 0 if the system should treat the bit as part of the host-number. This is illustrated in the following figure.



Subnet mask

The standards describing modern routing protocols often refer to the extended-network-prefix-length rather than the subnet mask. The prefix length is equal to the number of contiguous one-bits in the traditional subnet mask. This means that specifying the network address 130.5.5.25 with a subnet mask of 255.255.255.0 can also be expressed as 130.5.5.25/24. The /<prefix-length> notation is more compact and easier to understand than writing out the mask in its traditional dotted-decimal format. This is illustrated in the figure below.



Extended-Network-Prefix Length

However, it is important to note that modern routing protocols still carry the subnet mask. There are no Internet standard routing protocols that have a one-byte field in their header that contains the number of bits in the extended-network prefix. Rather, each routing protocol is still required to carry the complete four-octet subnet mask.

Subnet Design Considerations

The deployment of an addressing plan requires careful thought on the part of the network administrator. There are two key questions that must be answered before any design should be undertaken:

1) How many total subnets does the organization need today and in the future?

2) How many hosts are there on the organization's largest subnet today and in the future?

Steps in IP address subnetting

The first step in the planning process is to take the maximum number of subnets required and round up to the nearest power of two. For example, if a organization needs 9 subnets, 2^3 (or 8) will not provide enough subnet addressing space, so the network administrator will need to round up to 2^4 (or 16). When performing this assessment, it is critical that the network administrator always allow adequate room for future growth. For example, if 14 subnets are required today, then 16 subnets might not be enough in two years when the 17th subnet needs to be deployed. In this case, it might be wise to allow for more growth and select 2^5 (or 32) as the maximum number of subnets.

The second step is to make sure that there are enough host addresses for the organization's largest subnet. If the largest subnet needs to support 50 host addresses today, 2^5 (or 32) will not provide enough host address space so the network administrator will need to round up to 2^6 (or 64).

The final step is to make sure that the organization's address allocation provides enough bits to deploy the required subnet addressing plan. For example, if the organization has a single /16, it could easily deploy 4-bits for the subnet-number and 6-bits for the host number. However, if the organization has several /24s and it needs to deploy 9 subnets, it may be required to subnet each of its /24s into four subnets (using 2 bits) and then build the internet by combining the subnets of 3 different /24 network numbers. An alternative solution would be to deploy network numbers from the private address space (RFC 1918) for internal connectivity and use a Network Address Translator (NAT) to provide external Internet access.

Private Address Space

There are two types of IP addresses: - public and private. The private address space is used to communicate in a local (Intranet) network where the computers are not visible to the global network (the Internet). Whereas public IP addresses are visible to the Internet. Private IP addresses can be used in any network as long as they are unique in the specific Intranet.

These blocks of private IP addresses that are reserved by the Internet Assigned Numbers Authority (IANA) for private networks are shown in table below.

	Starting Address	Ending Address	Remark
1	10.0.0.0	10.255.255.255	We can have 2^{24} private IP addresses
2	172.16.0.0	172.31.255.255	We can have 2^{20} private IP addresses
3	192.168.0.0	192.168.255.255	We can have 2^{16} private IP addresses

Private IP address space

Subnetting Example #1

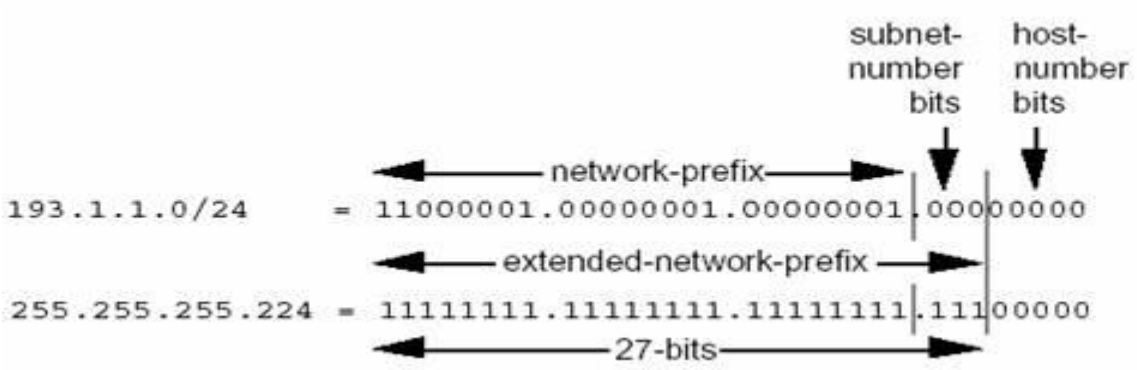
Given

An organization has been assigned the network number 193.1.1.0/24 and it needs to define six subnets. The largest subnet is required to support 25 hosts.

Defining the Subnet Mask / Extended-Prefix Length

The first step is to determine the number of bits required to define the six subnets. Since a network address can only be subnetted along binary boundaries, subnets must be created in blocks of powers of two [2 (2^1), 4 (2^2), 8 (2^3), 16 (2^4), etc.]. Thus, it is impossible to define an IP address block such that it contains exactly six subnets. For this example, the network administrator must define a block of 8 (2^3) and have two unused subnets that can be reserved for future growth.

Since 8 = 2^3, three bits are required to enumerate the eight subnets in the block. In this example, the organization is subnetting a /24 so it will need three more bits, or a /27, as the extended-network-prefix. A 27-bit extended-network-prefix can be expressed in dotted-decimal notation as 255.255.255.224. This is illustrated in the figure below.



Defining the subnet mask/Extended-Prefix Length

A 27-bit extended-network-prefix leaves 5 bits to define host addresses on each subnet. This means that each subnetwork with a 27-bit prefix represents a contiguous block of 2^5 (32) individual IP addresses. However, since the all-0s and all-1s host addresses cannot be allocated, there are 30 (2^5 -2) assignable host addresses on each subnet.

Defining Each of the Subnet Numbers

The eight subnets will be numbered 0 through 7. In this paper, the XXX_2 notation indicates the binary representation of the number. The 3-bit binary representation of the decimal values 0 through 7 are: 0 (000_2), 1 (001_2), 2 (010_2), 3 (011_2), 4 (100_2), 5 (101_2), 6 (110_2), and 7 (111_2).

In general, to define Subnet #n, the network administrator places the binary representation of n into the bits of the subnet-number field. For example, to define Subnet #6, the network administrator simply places the binary representation of 6 (110_2) into the 3-bits of the subnet-number field.

The eight subnet numbers for this example are given below. The underlined portion of each address identifies the extended-network-prefix, while the bold digits identify the 3- bits representing the subnet-number field:

```
Base Net: 11000001.00000001.00000001 .00000000 = 193.1.1.0/24
Subnet #0: 11000001.00000001.00000001. 000 00000 = 193.1.1.0/27
Subnet #1: 11000001.00000001.00000001. 001 00000 = 193.1.1.32/27
Subnet #2: 11000001.00000001.00000001. 010 00000 = 193.1.1.64/27
Subnet #3: 11000001.00000001.00000001. 011 00000 = 193.1.1.96/27
Subnet #4: 11000001.00000001.00000001. 100 00000 = 193.1.1.128/27
Subnet #5: 11000001.00000001.00000001. 101 00000 = 193.1.1.160/27
Subnet #6: 11000001.00000001.00000001. 110 00000 = 193.1.1.192/27
Subnet #7: 11000001.00000001.00000001. 111 00000 = 193.1.1.224/27
```

An easy way to check if the subnets are correct is to ensure that they are all multiples of the Subnet #1 address. In this case, all subnets are multiples of 32: 0, 32, 64, 96...

Defining Host Addresses for Each Subnet

According to Internet practices, the host-number field of an IP address cannot contain all 0-bits or all 1-bits. The all-0s host-number identifies the base network (or subnetwork) number, while the all-1s host-number represents the broadcast address for the network (or subnetwork).

In our current example, there are 5 bits in the host-number field of each subnet address. This means that each subnet represents a block of 30 host addresses (2^5-2 = 30, note that the 2 is subtracted because the all-0s and the all-1s host addresses cannot be used). The hosts on each subnet are numbered 1 through 30.

In general, to define the address assigned to Host #n of a particular subnet, the network administrator places the binary representation of n into the subnet's host-number field. For example, to define the address assigned to Host #15 on Subnet #2, the network administrator simply places the binary representation of 15 (01111_2) into the 5-bits of Subnet #2's host-number field.

The valid host addresses for Subnet #2 in our example are given below. The underlined portion of each address identifies the extended-network-prefix, while the bold digits identify the 5-bit host-number field:

```
Subnet #2: 11000001.00000001.00000001.010 00000 = 193.1.1.64/27
Host #1: 11000001.00000001.00000001.010 00001 = 193.1.1.65/27
Host #2: 11000001.00000001.00000001.010 00010 = 193.1.1.66/27
Host #3: 11000001.00000001.00000001.010 00011 = 193.1.1.67/27
Host #4: 11000001.00000001.00000001.010 00100 = 193.1.1.68/27
Host #5: 11000001.00000001.00000001.010 00101 = 193.1.1.69/27
.
.
Host #15: 11000001.00000001.00000001.010 01111 = 193.1.1.79/27
Host #16: 11000001.00000001.00000001.010 10000 = 193.1.1.80/27
```

.
.
Host #27: 11000001.00000001.00000001.010 **11011** = 193.1.1.91/27
Host #28: 11000001.00000001.00000001.010 **11100** = 193.1.1.92/27
Host #29: 11000001.00000001.00000001.010 **11101** = 193.1.1.93/27

Host #30: 11000001.00000001.00000001.010 **11110** = 193.1.1.94/27

The valid host addresses for Subnet #6 are given below. The underlined portion of each address identifies the extended-network-prefix, while the bold digits identify the 5-bit host-number field:

Subnet #6: 11000001.00000001.00000001.110 **00000** = 193.1.1.192/27

Host #1: 11000001.00000001.00000001.110 **00001** = 193.1.1.193/27

Host #2: 11000001.00000001.00000001.110 **00010** = 193.1.1.194/27

Host #3: 11000001.00000001.00000001.110 **00011** = 193.1.1.195/27

Host #4: 11000001.00000001.00000001.110 **00100** = 193.1.1.196/27

Host #5: 11000001.00000001.00000001.110 **00101** = 193.1.1.197/27

.
.
Host #15: 11000001.00000001.00000001.110 **01111** = 193.1.1.207/27

Host #16: 11000001.00000001.00000001.110 **10000** = 193.1.1.208/27

.
.
Host #27: 11000001.00000001.00000001.110 **11011** = 193.1.1.219/27

Host #28: 11000001.00000001.00000001.110 **11100** = 193.1.1.220/27

Host #29: 11000001.00000001.00000001.110 **11101** = 193.1.1.221/27

Host #30: 11000001.00000001.00000001.110 **11110** = 193.1.1.222/27

Defining the Broadcast Address for Each Subnet

The broadcast address for Subnet #2 is the all 1's host address or:

11000001.00000001.00000001.010 **11111** = 193.1.1.95

Note that the broadcast address for Subnet #2 is exactly one less than the base address for Subnet #3 (193.1.1.96). This is always the case - the broadcast address for Subnet #n is one less than the base address for Subnet # (n+1). The broadcast address for Subnet #6 is simply the all 1's host address or: 11000001.00000001.00000001.110 **11111** = 193.1.1.223

Again, the broadcast address for Subnet #6 is exactly one less than the base address for Subnet #7 (193.1.1.224).

Subnetting Example #2

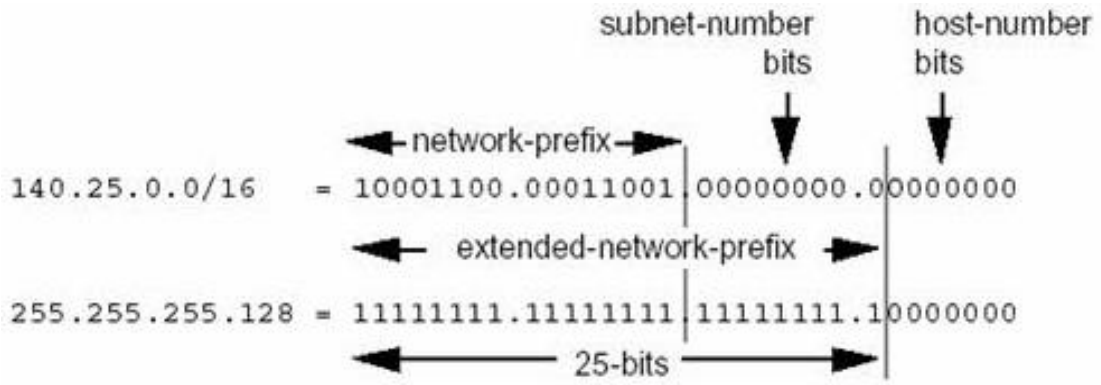
Given

An organization has been assigned the network number 140.25.0.0/16 and it needs to create a set of subnets that supports up to 60 hosts on each subnet.

Defining the Subnet Mask / Extended-Prefix Length

The first step is to determine the number of bits required to define 60 hosts on each subnet. Since a block of host address can only be assigned along binary boundaries, host address blocks can only be created in powers of two. This means that it is impossible to create a block that contains exactly 60 host addresses. To support 60 hosts, the network administrator must define a minimum address block of 62 (2^6-2) host addresses. However, this choice would only provide two unused host addresses on each subnet for future growth. Since this does not appear to be adequate to support additional growth, the network administrator elects to define a block of 126 (2^7-2) host addresses and has 66 addresses on each subnet for future growth. A block of 126 host addresses requires 7-bits in the host-number field.

The next step is to determine the subnet mask/extended-prefix length. Since 7-bits of the 32-bit IP address are required for the host-number field, the extended-prefix must be a /25 (2^5 = 32-7). A 25-bit extended-network-prefix can be expressed in dotted-decimal notation as 255.255.255.128. This is illustrated in the figure below.



Defining the subnet mask/Extended-Prefix Length

The figure above shows that the 25-bit extended-prefix assigns 9-bits to the subnet number field. Since 2^9 = 512, nine bits allow the definition of 512 subnets. Depending on the organization's requirements, the network administrator could have elected to assign additional bits to the host-number field (allowing more hosts on each subnet) and reduce the number of bits in the subnet-number field (decreasing the total number of subnets that can be defined).

Although this example creates a rather large number of subnets, it provides an interesting example because it illustrates what happens to the dotted-decimal representation of a subnet address when the subnet-number bits

extend across an octet boundary. It should be mentioned that the same type of confusion can also occur when the host-number bits extend across an octet boundary.

Defining Each of the Subnet Numbers

The 512 subnets will be numbered 0 through 511. The 9-bit binary representation of the decimal values 0 through 511 are: 0 (000000000_2), 1 (000000001_2), 2 (000000010_2), 3 (000000011_2), ..., 511 (111111111_2). To define subnet #3, the network administrator places the binary representation of 3 (000000011_2) into the 9-bits of the subnet-number field.

The 512 subnet numbers for this example are given below. The underlined portion of each address identifies the extended-network-prefix, while the bold digits identify the 9- bits representing the subnet-number field:

```
Base Net: 10001100.00011001 .00000000.00000000 = 140.25.0.0/16
Subnet #0: 10001100.00011001. 00000000 . 0 0000000 = 140.25.0.0/25
Subnet #1: 10001100.00011001. 00000000 . 1 0000000 = 140.25.0.128/25
Subnet #2: 10001100.00011001. 00000001 . 0 0000000 = 140.25.1.0/25
Subnet #3: 10001100.00011001. 00000001 . 1 0000000 = 140.25.1.128/25
Subnet #4: 10001100.00011001. 00000010 . 0 0000000 = 140.25.2.0/25
Subnet #5: 10001100.00011001. 00000010 . 1 0000000 = 140.25.2.128/25
Subnet #6: 10001100.00011001. 00000011 . 0 0000000 = 140.25.3.0/25
Subnet #7: 10001100.00011001. 00000011 . 1 0000000 = 140.25.3.128/25
Subnet #8: 10001100.00011001. 00000100 . 0 0000000 = 140.25.4.0/25
Subnet #9: 10001100.00011001. 00000100 . 1 0000000 = 140.25.4.128/25
.
.
Subnet #510: 10001100.00011001. 11111111 . 0 0000000 = 140.25.255.0/25
Subnet #511: 10001100.00011001. 11111111 . 1 0000000 = 140.25.255.128/25
```

Notice how sequential subnet numbers do not appear to be sequential when expressed in dotted-decimal notation. This can cause a great deal of misunderstanding and confusion since everyone believes that dotted-decimal notation makes it much easier for human users to understand IP addressing. In this example, the dotted-decimal notation obscures rather than clarifies the subnet numbering scheme!

Defining Hosts Addresses for Each Subnet

In this example there are 7 bits in the host-number field of each subnet address. As discussed earlier, this means that each subnet represents a block of 126 host addresses. The hosts on each subnet will be numbered 1 through 126.

The valid host addresses for Subnet #3 are given below. The underlined portion of each address identifies the extended-network-prefix, while the bold digits identify the 7-bit host-number field:

```
Subnet #3: 10001100.00011001.00000001.1 0000000 = 140.25.1.128/25

Host #1: 10001100.00011001.00000001.1 0000001 = 140.25.1.129/25

Host #2: 10001100.00011001.00000001.1 0000010 = 140.25.1.130/25

Host #3: 10001100.00011001.00000001.1 0000011 = 140.25.1.131/25

Host #4: 10001100.00011001.00000001.1 0000100 = 140.25.1.132/25

Host #5: 10001100.00011001.00000001.1 0000101 = 140.25.1.133/25

Host #6: 10001100.00011001.00000001.1 0000110 = 140.25.1.134/25
.
.
Host #62: 10001100.00011001.00000001.1 0111110 = 140.25.1.190/25
Host #63: 10001100.00011001.00000001.1 0111111 = 140.25.1.191/25

Host #64: 10001100.00011001.00000001.1 1000000 = 140.25.1.192/25

Host #65: 10001100.00011001.00000001.1 1000001 = 140.25.1.193/25
.
.
Host #123: 10001100.00011001.00000001.1 1111011 = 140.25.1.251/25
Host #124: 10001100.00011001.00000001.1 1111100 = 140.25.1.252/25

Host #125: 10001100.00011001.00000001.1 1111101 = 140.25.1.253/25

Host #126: 10001100.00011001.00000001.1 1111110 = 140.25.1.254/25
```

Defining the Broadcast Address for Each Subnet

The broadcast address for Subnet #3 is the all 1's host address or: `10001100.00011001.00000001.1` **1111111** = `140.25.1.255`

As is true in general, the broadcast address for Subnet #3 is exactly one less than the base address for Subnet #4 (`140.25.2.0`)

Some protocols used with IP

Address Resolution Protocol

In order for devices to communicate, the sending devices need both, the IP addresses and the MAC addresses, of the destination devices. When they try to communicate with devices whose IP addresses they know, they must determine the MAC addresses. The TCP/IP suite has a protocol, called ARP that can automatically obtain the MAC address. ARP enables a computer to find the MAC address of the computer that is associated with an IP address

Suppose you are on system 128.6.4.194 and you want to connect to system 128.6.4.7. Your system will first verify that 128.6.4.7 is on the same network, so it can talk directly via Ethernet. Then it will look up 128.6.4.7

in its ARP table (A table mapping IP addresses to MAC addresses), to see if it already knows the Ethernet address. If so, it will stick on an Ethernet header, and send the packet. But suppose this system is not in the ARP table. There is no way to send the packet, because you need the Ethernet address. So it uses the ARP protocol to send an ARP request. Essentially an ARP request says "I need the Ethernet address for 128.6.4.7". Every system listens to ARP requests. When a system sees an ARP request for itself, it is required to respond. So 128.6.4.7 will see the request, and will respond with an ARP reply saying in effect "128.6.4.7 is 8:0:20:1:56:34". (Recall that Ethernet addresses are 48 bits. This is 6 octets. Ethernet addresses are conventionally shown in hex, using the punctuation shown.) Your system will save this information in its ARP table, so future packets will go directly. Most systems treat the ARP table as a cache, and clear entries in it if they have not been used in a certain period of time.

Note by the way that ARP requests must be sent as "broadcasts". There is no way that an ARP request can be sent directly to the right system. After all, the whole reason for sending an ARP request is that you don't know the Ethernet address. So an Ethernet address of all ones is used, i.e. ff:ff:ff:ff:ff:ff. By convention, every machine on the Ethernet is required to pay attention to packets with this as an address. So every system sees every ARP requests. They all look to see whether the request is for their own address. If so, they respond. If not, they could just ignore it. (Some hosts will use ARP requests to update their knowledge about other hosts on the network, even if the request isn't for them.) Note that packets whose IP address indicates broadcast (e.g. 255.255.255.255 or 128.6.4.255) is also sent with an Ethernet address that is all ones.

Dynamic Host Configuration protocol (DHCP)

DHCP is a mechanism to assign unique IP addresses to DHCP clients automatically. Under DHCP, a computer is designated as the DHCP server. All of the other computers on the network - at least, those that need an IP address - will be DHCP clients (computers that already have a permanently set IP address don't need to participate). The network administrator needs to initially configure the DHCP server. Part of that configuration process involves assigning the DHCP server a block of IP address numbers that it can dispense to nodes that need IP addresses.

When a new node comes onto the network - assuming it is capable of being a DHCP client - it will broadcast a request for an IP address. Simply put, the DHCP server will respond by checking its table of address assignments, selecting the next available address, and sending a response back to the requesting node.

The actual process is more complex than that, as the requesting client must first find a DHCP server. Also, the protocol is constructed so that a client may negotiate with more than one DHCP server.

Here's how it works: A DHCP client that is in need of configuration broadcasts a *dhcpdiscover* packet in search of servers. This packet will contain the hardware address of the requesting client, for example, its Ethernet or Token Ring address. It might also contain a suggested IP address. Next, one or more DHCP servers will evaluate the request and respond with a *dhcpoffer* packet, which contains an offer of a specific IP address, together with a "lease period" (the length of time the client may use the address).

The client then selects one from among the dhcpoffer packets it receives. (The client's selection will depend on its design; it may seek the longest lease, for example.) The client then issues a dhcprequest packet, which contains the address of the server that issued the dhcpoffer it prefers.

The chosen server then issues an acknowledgment packet (*dhcpack*), which closes the negotiations. The dhcpack packet contains the IP address and lease period that have been agreed upon. The server now marks this address as committed; it cannot be assigned to any other client for the duration of the lease. The client configures itself to use its new assigned address and begins normal network operation.
Note that more than one DHCP server may respond to a dhcpdiscover with a dhcpoffer. The client must pick one offer, responding with a dhcprequest packet containing the server identifier for the server it has chosen. The other servers monitor the dhcprequest packet and infer from the server identifier that their offers were not chosen; they then know that the IP addresses they offered are still available for assignment to another client.

The Future IP (IPv6)

Motivation:

- *Limited address space* - at the current growth of the Internet, all the possible network prefixes will soon be assigned.
- *Need for Quality of service (QoS) guarantees* for emerging real-time applications.

Characteristics of IPv6

- IP retains many of the design features of the existing IPv4.
- The new features of IP v6 can be grouped into 5 main categories:
- *Address size:* 128-bit addresses instead of 32 bits.
- *Header format:* almost every field in the header has been changed.
- *Extension Headers:* IPv6 encodes info into separate headers, instead of using a single header.

- *QoS offerings:* includes a mechanism which allows for differentiated quality of service for applications.
- *Extensible protocol:* IPv6 does not specify all possible protocol features. Instead, it allows a sender to add additional information to a datagram. This makes IPv6 more flexible and new features can be added to the protocol as needed.

IPv6 Address Format

- The dotted decimal format used in IPv4 would be too cumbersome for a 128-bit address.
- To help reduce the number of characters used to write an address, the *Colon Hexadecimal Notation* is used.
- Each group of 16 bits is written in hexadecimal with a colon separating groups. E.g. 69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF
- Zero compression can be used to further reduce the size of the address. i.e. a sequence of zeros is replaced with two colons:

Chapter Six

LAN and WAN Technologies

Routing Technologies

- **Routing** is the process of determining the route or path through the network that a message will travel from the sending computer to the receiving computer.
- Routing is done by special devices called routers.
- Have the function of storing, forwarding, path-finding
- **Routers** are usually found at the edge of subnets because they are the devices that connect subnets together and enable messages to flow from one subnet to another as the messages move through the network from sender to receiver.
- Every router has a routing table that specifies how messages will travel through the network.
- The routing table is a two-column table. The first column lists every network or computer that the router knows about and the second column lists the interface that connects to it.

- A router uses its routing table to decide where to send the messages it receives.
- Router check the destination address of the packet, and choose the next hop based on the information in route table.
- Route table is stored in RAM

Route table composition

- Destination address （Dest）
- Mask （Mast）
- Next hop address (Gw)
- Forwarding physical interface （interface）
- Source of the information (Owner)
- Route priority （pri）
- metric（metric）

Example

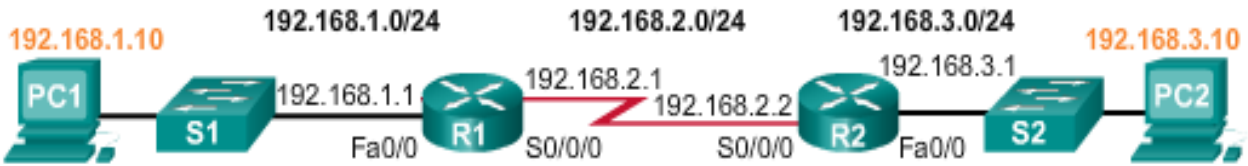
Dest	Mask	Gw	Interface	Owner	pri	metric
172.16.8.0	255.255.255.0	1.1.1.1	fei_1/1	static	1	0

172.16.8.0 -- Destination network address
255.255.255.0 -- Destination network mask
1.1.1.1 -- Next hop address
fei_1/1 -- Route learning interface and forwarding interface
static -- how does router learns this entry
1 -- route priority
0 -- Metric

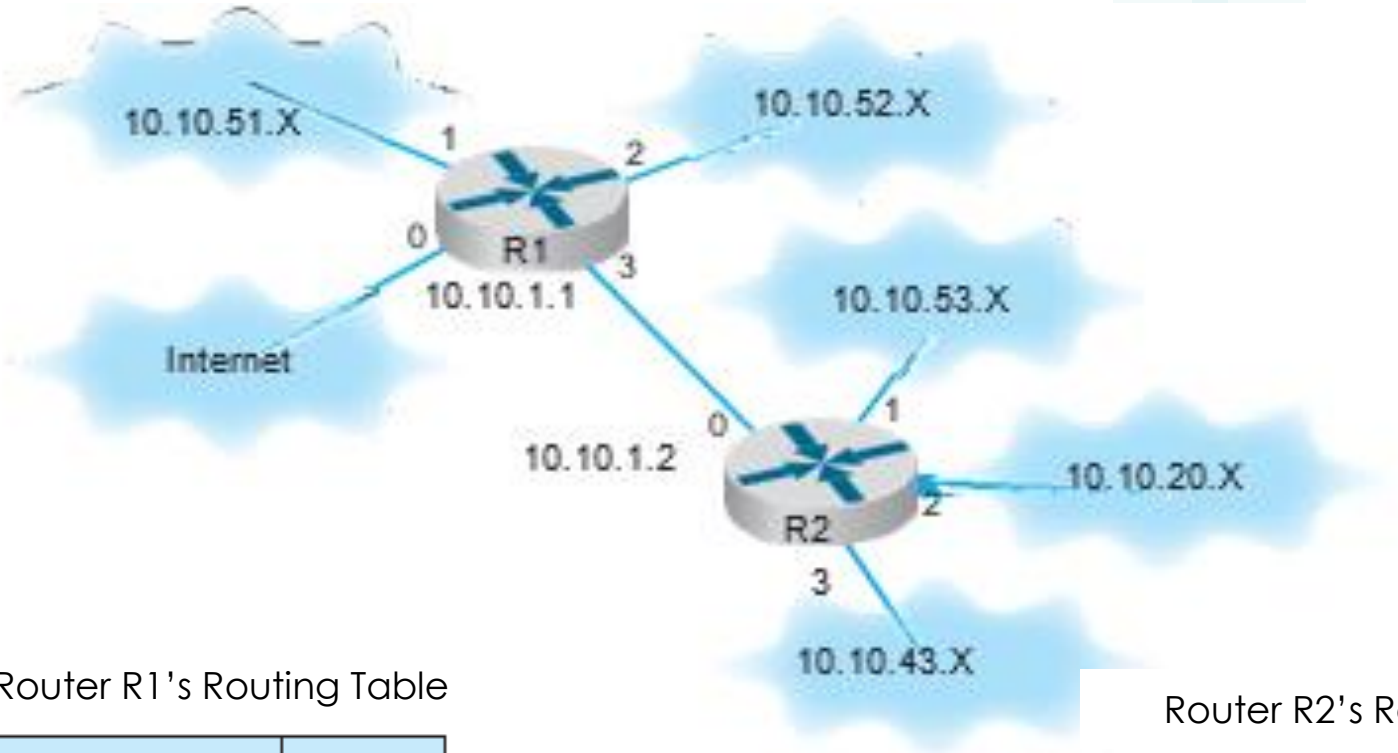
Document Network Addressing

Network Documentation should include at least the following in a topology diagram and addressing table:

- Device names
- Interfaces
- IP addresses and subnet mask
- Default gateways



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1



Router R1's Routing Table

Network Address	Interface
10.10.51.0 to 10.10.51.255	1
10.10.52.0 to 10.10.52.255	2
10.10.53.0 to 10.10.53.255	3
10.10.20.0 to 10.10.20.255	3
10.10.43.0 to 10.10.43.255	3
10.10.1.2	3
All other addresses	0

Router R2's Routing Table

Network Address	Interface
10.10.1.1	0
10.10.53.0 to 10.10.53.255	1
10.10.20.0 to 10.10.20.255	2
10.10.43.0 to 10.10.43.255	3
All other addresses	0

Types of Routing

- centralized routing
- static routing
- dynamic routing

Centralized routing.

- all routing decisions are made by one central router.
- commonly used in host-based networks, and in this case, routing decisions are rather simple.
- All computers are connected to the central router, so any message that needs to be routed is simply sent to the central router

Static routing

- Static routing is decentralized, which means that all routers in the network make their own routing decisions following a formal routing protocol.
- In MANs and WANs, the routing table for each computer is developed by its individual network manager
- Most decentralized routing protocols are self-adjusting, meaning that they can automatically adapt to changes in the network configuration
- routing decisions are made in a fixed manner by individual routers.
- commonly used in networks that have few routing options that seldom change.

Dynamic Routing

- Called *adaptive routing; decisions* are made in a decentralized manner by individual computers.
- This approach is used when there are multiple routes through a network, and it is important to select the best route.
- Dynamic routing attempts to improve network performance by routing messages over the fastest possible route, away from busy circuits and busy computers.
- An initial routing table is developed by the network manager but is continuously updated by the routers themselves to reflect changing network conditions.

Routing Protocols

- A routing protocol is a protocol that is used to exchange information among routers to enable them to build and maintain their routing tables.
- When new paths are added or paths are broken and cannot be used, messages are sent among routers using the routing protocol.
- Dynamic routing protocols become impractical because of the amount of network traffic they generate, this creates autonomous systems of networks.
- An **autonomous system** is a network operated by one organization that runs one part of the Internet.
- Each part of the Internet or each large organizational network connected to the Internet can be a separate autonomous system

- If an autonomous system grows too large, it can be split into smaller parts. The routing protocols used inside an autonomous system are called **interior routing protocols.**
- Protocols used between autonomous systems are called **exterior routing protocols**.
- Interior routing protocols are usually designed to provide detailed routing information about all or most routers inside the autonomous systems
- exterior protocols are designed to be more careful in the information they provide.
- exterior protocols provide information about only the preferred or the best routes rather than all possible routes

LAN Technologies

- Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet.
- All of these LANs used a media-access method to solve the problem of sharing the media. (CSMA/CD)

Logical Link Control (LLC)

The data link control handles framing, flow control, and error control. In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sub layer called the logical link control (LLC). Framing is handled in both the LLC sub layer and the MAC sub layer.

Media Access Control (MAC)

- IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.
- For example, it defines CSMA/CD as the media access method for Ethernet LANs and defines the token-passing method for Token Ring and Token Bus LANs.

Ethernet Evolution

- LAN has gone through four generations:
  - Standard Ethernet (10 Mbps)
  - Fast Ethernet (100 Mbps)
  - Gigabit Ethernet (1 Gbps)
  - 10 Gigabit Ethernet (10 Gbps)

Standard Ethernet

- provides a connectionless service, which means each frame sent is independent of the previous or next frame.
- Ethernet has no connection establishment or connection termination phases.
- The sender sends a frame whenever it has it; the receiver may or may not be ready for it.
- Since the network that uses the standard Ethernet protocol is a broadcast network, we need to use an access method to control access to the sharing medium. The standard Ethernet chooses CSMA/CD.

Fast Ethernet

Ethernet made a big jump by increasing the transmission rate to 100 Mbps, and the new generation was called the Fast Ethernet.

- compatible with the Standard Ethernet.
- The MAC sublayer was left unchanged
- transmission rate, access method, and implementation had to be reconsidered.
  - Upgrade the data rate to 100 Mbps.
  - Make it compatible with Standard Ethernet.
  - Keep the same 48-bit address.
  - Keep the same frame format
- A new feature added to Fast Ethernet is called auto-negotiation. It allows a station or a hub a range of capabilities.
- Autonegotiation allows two devices to negotiate the mode or data rate of operation.
- It was designed particularly to allow incompatible devices to connect to one another.

Gigabit Ethernet

- The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps)
- The goals of the Gigabit Ethernet were to upgrade the data rate to 1 Gbps, but keep the address length, the frame format, and the maximum and minimum frame length the same.
  - Upgrade the data rate to 1 Gbps.
  - Make it compatible with Standard or Fast Ethernet.
  - Use the same 48-bit address.
  - Use the same frame format.
  - Keep the same minimum and maximum frame lengths.
- has two distinctive approaches for medium access: half-duplex and full duplex.
- No collision, CSMA/CD is not used

10 Gigabit Ethernet

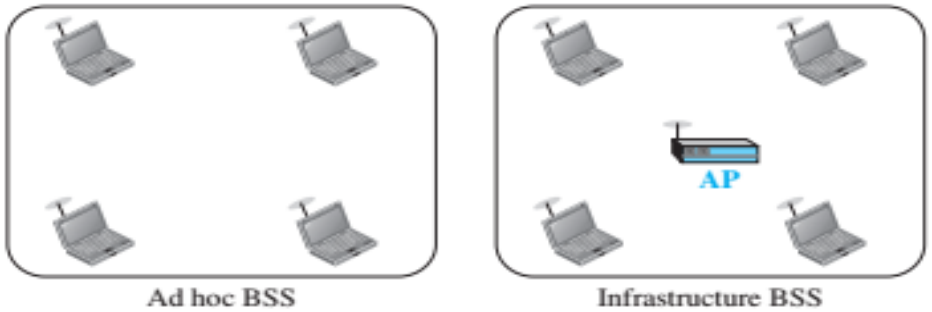
- The goals of the 10 Gigabit Ethernet design can be summarized as
  - upgrading the data rate to 10 Gbps,
  - keeping the same frame size and format,
  - allowing the interconnection of LANs, MANs, and WAN possible.
- possible only with fiber-optic technology at this time.
- 10 Gigabit Ethernet operates only in full-duplex mode
- CSMA/CD is not used in 10 Gigabit Ethernet.

Wireless LAN (WLAN)

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers.
- It is sometimes called wireless Ethernet.
- The standard defines two kinds of services:
  - basic service set (BSS)
  - extended service set (ESS)

basic service set (BSS)

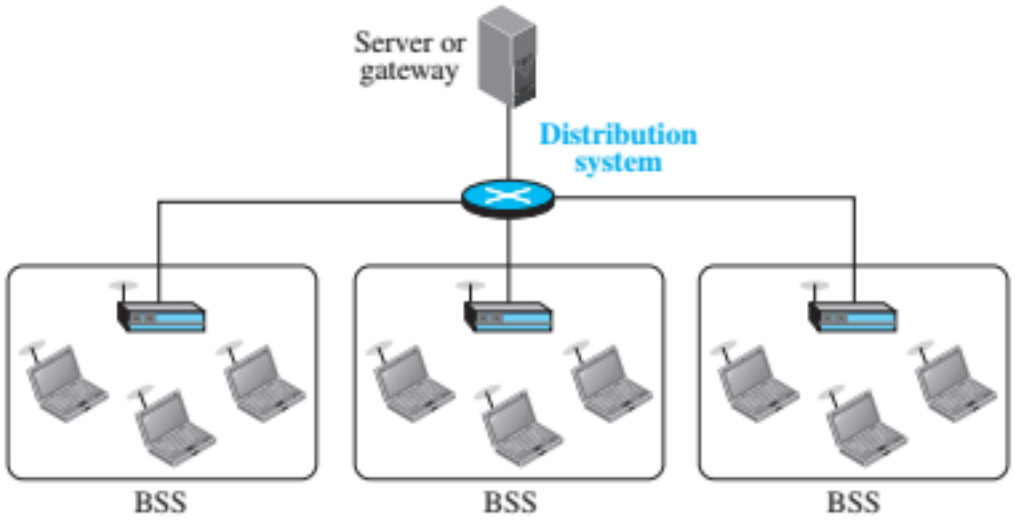
- IEEE 802.11 defines the basic service set (BSS) as the building blocks of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and central base station, known as the access point (AP).
  - ad hoc architecture(no need of AP)
  - infrastructure BSS



- Uses AP to control who can talk and when
- Individual STAs can not communicate directly with each other.
- To communicate each device must obtain permission from the AP
- The AP ensures that all STAs have equal access to the medium
- The area covered by a single AP is known as Basic Service Set (BSS) or cell

Extended Service Set

- An extended service set (ESS) is made up of two or more BSSs with Aps
- the BSSs are connected through a distribution system, which is a wired or a wireless network
- uses two types of stations: mobile and stationary.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.



Types of Wireless Ethernet

- Wi-Fi is one of the fastest changing areas in networking.
- The four amendments of IEEE 802.11 standard that describe different characteristics for wireless communication are

802.11a

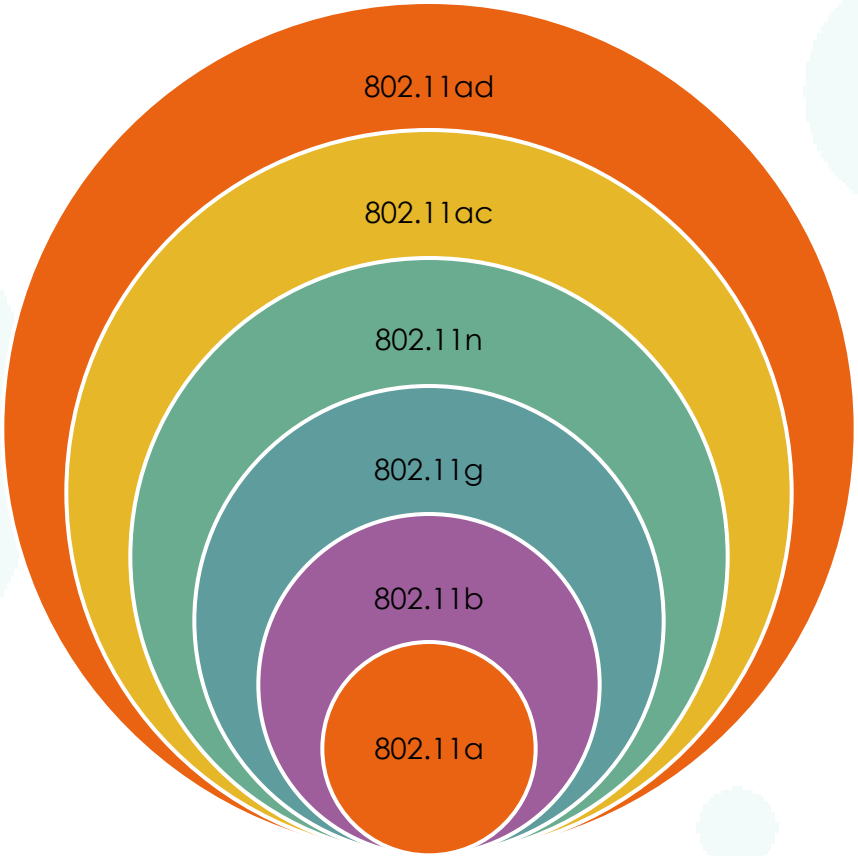
802.11b

802.11g

802.11n

802.11ac

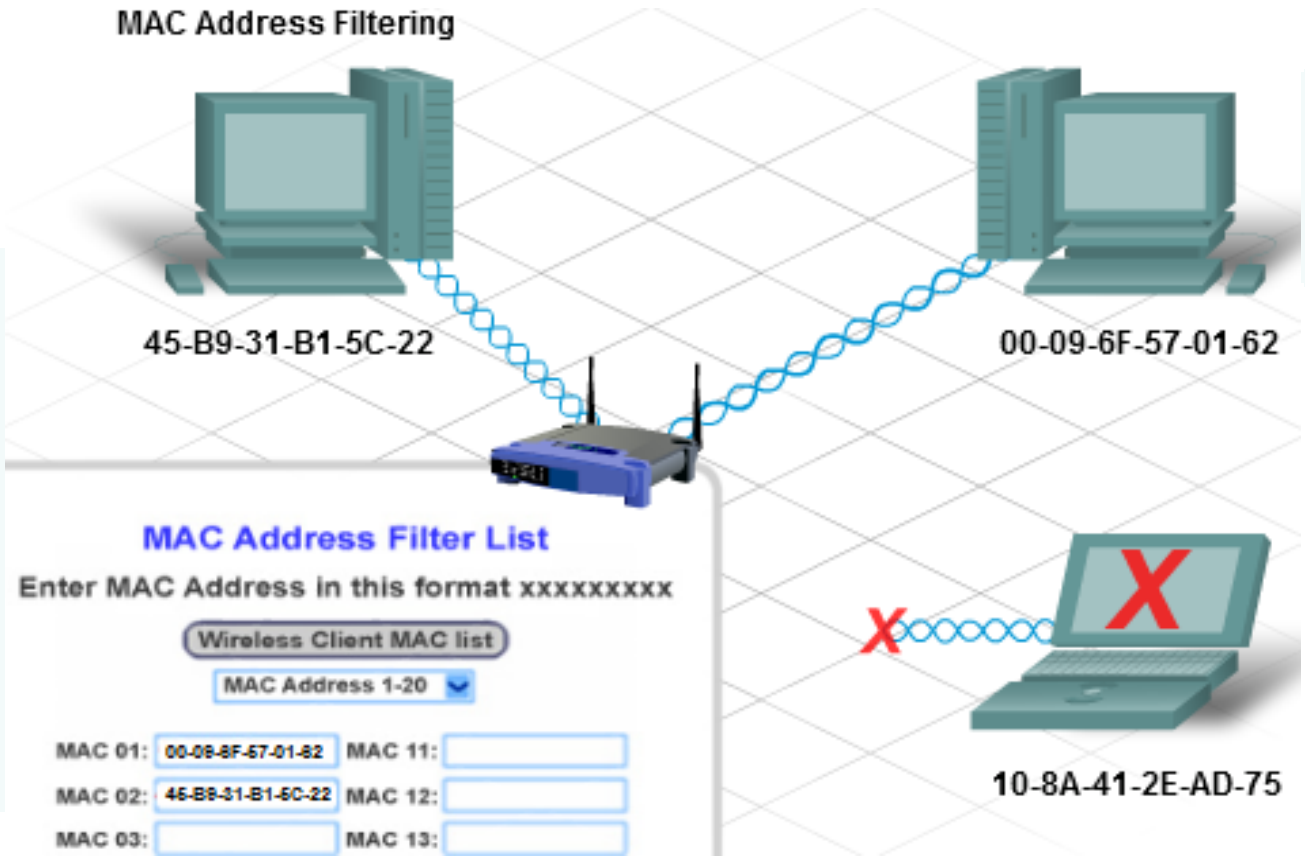
802.11ad



Standard	Frequency	Maximum Speed	Backwards compatibility	Chanel
802.11	2.4 GHz	2 Mbps	-	
802.11a	5 GHz	54 Mbps	-	8
802.11b	2.4 GHz	11 Mbps	-	3
802.11g	2.4 GHz	54 Mbps	802.11b	3
802.11n	2.4 and 5 GHz	600 Mbps	802.11a/b/g	3
802.11ac	5 GHz	1300 Mbps	802.11a/n	
802.11ad	2.4 GHz, 5 GHz and 60 GHz	7 Gbps	802.11a/b/g/n/ac	

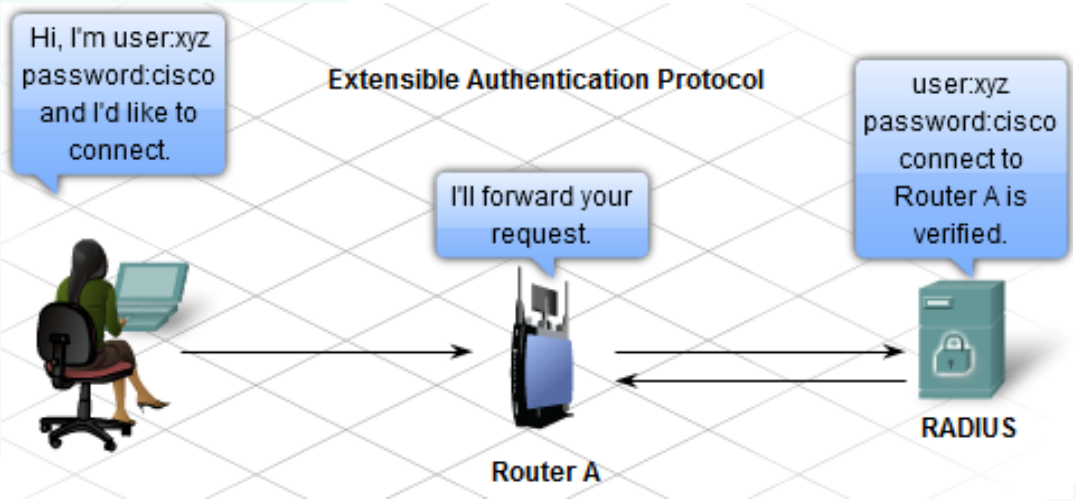
WLAN Security

- **MAC Address Filtering**
  - If MAC filtering is enabled, the STAs send MAC information to the AP, the information will be matched with the preconfigured MAC list and will be allowed or denied access accordingly



Extensible Authentication Protocol (EAP)

- EAP provides mutual, or two-way, authentication as well as user authentication
- Uses a backend server called RADIUS (Remote Authentication Dial-in User Service)
- the user, not just the host, must provide a username and password which is checked against the RADIUS database for validity



Wired Equivalency Protocol (WEP)

- security feature that encrypts network traffic
- uses pre-configured keys to encrypt and decrypt data
- A WEP key is entered as a string of numbers and letters and is generally 64 bits or 128 bits or 256bits long
- many devices include a Passphrase option to simplify creating the key
- every wireless device allowed to access the network must have the same WEP key

Intrusion monitoring: Intrusion monitoring is necessary to prevent the potential damage that an attacker could cause

- Wireless Intrusion Detection System(WIDS)

immediately alerts a systems administrator whenever a rogue access point is detected

- Wireless Intrusion Prevention System(WIPS)
- can automatically take countermeasures

Wi-Fi Protected Access (WPA)

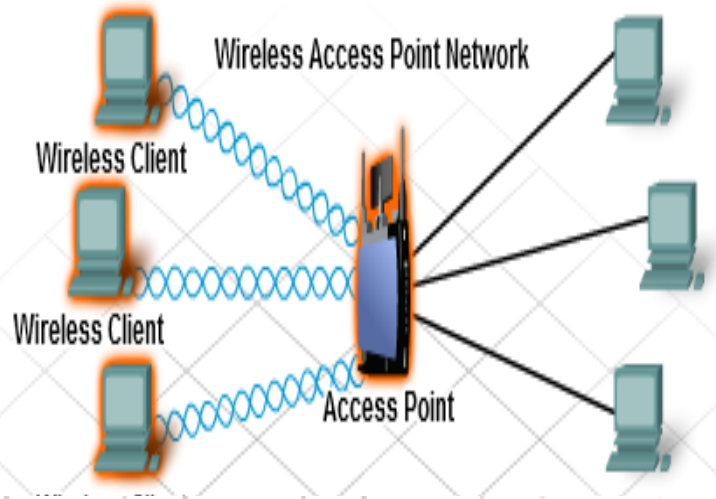
- uses encryption keys from 64 bits up to 256 bits
- Generates new keys each time a client establishes a connection with the AP
- more secure than WEP because it is significantly more difficult to crack

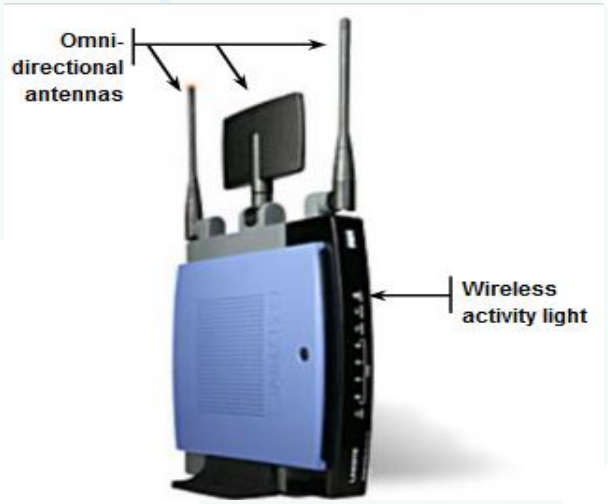
Traffic Filtering on a WLAN

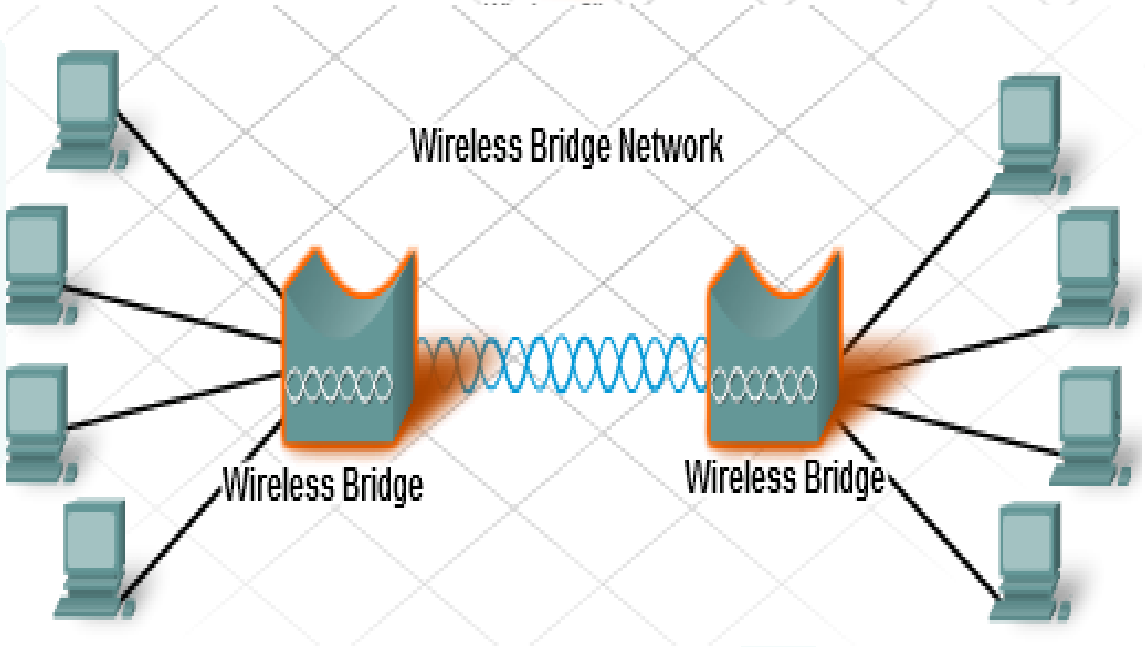
- Blocking undesirable traffic from entering or leaving the wireless network
- done by the AP as traffic passes through it

WAN Components

- components that must be considered in a WLAN include:
  - a wireless client or STA,
  - an Access Point,
  - a Wireless Bridge and
  - an antenna.
  - Wireless network interface card







The end!