Introduction

Signals need something to travel though. The electromagnetic spectrum is filled with many different kinds of energies. The low frequencies are mostly used for power transmission, and voice (0-3kHz). Mid-range frequencies are used for radio (TV), microwaves, satellite. At around 300Ghz, energy becomes infrared light. Visible light is 430-750THz. That is then followed by Ultraviolet light, X rays, Gamma rays, etc.

In any case, the important thing is that we have different things to worry about depending on which frequencies we are dealing with.

There are two primary ways of getting signals from place to place, by using the **guided or unguided media**.

1. Transmission Media

To exchange information between people separated by a distance has been a necessity throughout the history of mankind. Long ago, people used fire for communicating over a limited distance; they used birds and messengers for long distance communication. The postal system still provides an excellent means of sending written communication across the globe Communication over long distances, not just through written text but using other media such as voice and video,it has been achieved through electrical communication. This means a conversion of information into electrical signals and transmitting them over a distance through a transmission medium. Free space (or radio) communication particularly provides the unique advantage of support for mobility—the user can communicate while on the move (in a car or an airplane). However, the radio spectrum is a precious natural resource and has to be used efficiently.

Guided Media

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

1. Twisted Pair

is a pair of copper wires, One popular form of wire is the twisted pair. These are usually broken up into two major categories: Unshielded Twisted Pair (UTP), and Shielded Twisted Pair (STP).

The UTP wire is the cheapest and most common wire, which would explain why most LANs use UTP. There are several “categories” of UTP cable that have been standardized.

1. Category 1: Basic twisted pair; used for the old telephone system. Unsuitable for data communications (unless very low-speed).

2. Category 2: Better than Category 1. Suitable for data communications up to Mbps3

3. Category : Required to have at least 3 twists per foot, and can be used for data communications up to 10Mbps. Modern telephone wire.

4. Category 4: Improved version of Category 3, can be used for data communications up to 16Mbps.

5. Category 5: Can be used for data transmission of up to 100Mbps.

The STP cable has a foil of metal mesh covering the pair of wires, eliminating crosstalk

2. COAXIAL CABLE

Commonly known as coax carries a signal at much higher frequencies than twisted pair. Instead of having two wires, there is a primary ‘core’ wire in the center, with an insulator, and an outer conductor that serves as a shield and insulator.

Coaxial cable is used for cable TV distribution, long-distance telephone trunks, and LANs. The cross section of a coaxial cable used in an Ethernet local area network .

Coaxial cable can support a maximum data rate of 500Mbps for a distance of about 500 meters. Repeaters are required every 1 to 10 kilometers.

Based on the speed of transmission and the distance (length of the cable), the propagation delay can be calculated using the formula

Delay = distance/speed

For example, if the distance is 10 kilometers, the propagation delay is

Delay = 10,000/(2.3 × 108) seconds = 43.48 microseconds.

3. OPTICAL FIBER

Optical fiber is now being deployed extensively and is the most preferred medium for all types of networks because of the high data rates that can be supported. Light in a glass medium can carry more information over large distances, as compared to electrical signals in a copper cable or a coaxial cable.

Optical fiber is the most attractive transmission medium because of its support for very high data rates and low attenuation

The challenge in the initial days of research on fiber was to develop glass so pure that at least 1% of the light would be retained at the end of 1 kilometer. This feat was achieved in 1970. The recent advances in fiber have been phenomenal; light can traverse 100km without any amplification, thanks to research in making purer glass. With the state of the art, the loss will be about 0.35dB/km for 1310 nanometers and 0.25dB/ km for 1550nm.

Light transmission in the fiber works on the principle that the light waves are reflected within the core and guided to the end of the fiber, provided the angle at which the light waves are transmitted is controlled. Note that if the angle is not proper, the light is refracted and not reflected. The fiber medium has a core and cladding, both pure solid glass and protected by acrylate coating that surrounds the cladding.

There are two types of fiber: **single mode and multimode**. **Single mode** fiber has a small core and allows only one ray (or mode) of light to propagate at a time. **Multimode fiber**, the first to be commercialized, has a much larger core than single mode fiber and allows hundreds of rays of light to be transmitted through the fiber simultaneously. The larger core diameter allows low-cost optical transmitters and connectors and hence is cheaper.

2. Unguided Media

Unguided media is still ‘media’ (stuff that signal travels though). The trick is that the media is usually not directional, like air, space, etc. Because the effect is usually much wider than with guided media, there have been a lot of regulation, licensing, and standardization of transmissions via unguided media. The range spans:

1. VLF, 3kHz-30kHz, Very Low Frequency. Used for surface propagation.
2. LF, 30kHz-300kHz, Low Frequency. Used for surface propagation.
3. MF, 300kHz-3MHz, Middle Frequency. Used for Tropospheric propagation.
4. HF, 3MHz-30MHz, High Frequency. Used for Ionospheric propagation.
5. VHF, 30MHz-300MHz, Very High Frequency. Used for Space and Line-of-sight propagation.
6. UHF, 300Mhz-3GHz, Ultra High Frequency. Used for Space and Line-of-sight propagation.
7. SHF, 3GHz-30GHz, Super High Frequency. Used for Space propagation.
8. EHF, 30GHz-300GHz, Extremely High Frequency. Used for Space propagation.

Depending on the frequency used, there are different propagation modes.

- Surface Propagation: The transmission travels near the ground, hugging the earth.
- Tropospheric Propagation: Either line of sight, or bounding off the signal via Ionosphere.
- Ionospheric Propagation: Bouncing off the signal off Ionosphere.
- Line-of-sight Propagation.
- Space Propagation: signals are sent from ground to satellites, which then relay them back to earth.

1. TERRESTRIAL RADIO

Free space as the medium has the main advantage that the receiver can be fixed or mobile. Free space is called an unguided medium because the electromagnetic waves can travel freely in all directions. Depending on the frequency of the radio waves, the propagation characteristics vary, and different frequencies are used for different applications, based on the required propagation characteristics. Radio is used for broadcasting extensively because a central station can transmit the program to be received by a large number of receivers spread over a large geographical area.

In this case, the transmitter transmits at a specific frequency, and all the receivers tune to that frequency to receive the program.

Radio as a transmission medium has the main advantage that it supports mobility. In addition, installation and maintenance of radio systems are very easy.

In two-way communication systems such as for voice, data, or video, there is a base station located at a fixed place in the area of operation and a number of terminals. A pair of frequencies is used for communication—one frequency for transmitting from the base station to the terminals (the downlink) and one frequency from the terminal to the base station (the uplink). This frequency pair is called the *radio channe*l

Note A radio channel consists of a pair of frequencies—one frequency is used for uplink and one frequency is used for downlink. However, in some radio systems, a single frequency is used in both directions.

Radio as the transmission medium has special characteristics that also pose special problems.

Path loss: As the distance between the base station and the terminal increases, the received signal becomes weaker and weaker, even if there are no obstacles between the base station and the terminal. The higher the frequency, the higher the path loss. Many models are available (such as Egli's model and Okomura-Hata model) to estimate path loss. To compensate for path loss, we need to use high-gain antennas and also develop receivers of high sensitivity.

Note Path loss causes a heavy attenuation of the radio signal. Hence, the radio receiver should be capable of receiving very weak signals. In other words, the receiver should have high sensitivity.

Fading: Where there are obstacles between the base station and the terminal (hills, buildings, etc.), the signal strength

goes down further, which is known as fading. In densely populated urban areas, the signal can take more than one path —one signal path can be directly from the base station to the terminal and another path can be from the base station to a building and the signal reflected from the building and then received at the terminal. Sometimes, there may not be a

line of sight between the base station and terminal antennas, and hence the signals received at the terminals are from different paths. The received signal is the sum of many identical signals that differ only in phase. As a result, there will be fading of the signal, which is known as multi-path fading or Raliegh fading.

Note Multi-path fading is predominant in mobile communication systems. The mobile phone receives the signals

that traverse different paths.

Rain attenuation: The rain affects radio frequency signals. Particularly in some frequency bands, rain attenuation is greater. When designing radio systems, the effect of rain (and hence the path loss) needs to be taken into consideration.

The radio spectrum is divided into different frequency bands, and each band is used for a specific application.

Note Radio wave propagation is very complex, and a number of mathematical models have been developed to study the propagation in free space.

2. SATELLITE RADIO

Arthur C. Clarke proposed the concept of communication satellites. A communication satellite is a relay in the sky. If the satellite is placed at a distance of about 36,000 km above the surface of the earth, then it appears stationary with respect to the earth because it has an orbital period of 24 hours. This orbit is called a geostationary orbit, and the satellites are called geostationary satellites.

On Earth, we need satellite antennas (which are a part of the Earth stations) that point toward the satellite for communication. A pair of frequencies is used for communication with the satellite—the frequency used from Earth station to the satellite is called the uplink frequency, and the frequency from the satellite to the Earth station is called the downlink frequency. The signals transmitted by an Earth station to the satellite are amplified and then relayed back to the receiving Earth stations.

The main attraction of communication satellites is distance insensitivity. To provide communication facilities across the continents and also to rural and remote areas where laying cables is difficult, satellite communication will be very attractive. However, satellite communication has a disadvantage—delay. The propagation time for the signal to travel all the way to the satellite and back is nearly 240 msec. Also, because the signal has to travel long distances, there will be signal attenuation, and high-sensitivity receivers are required at both the satellite and the Earth stations.

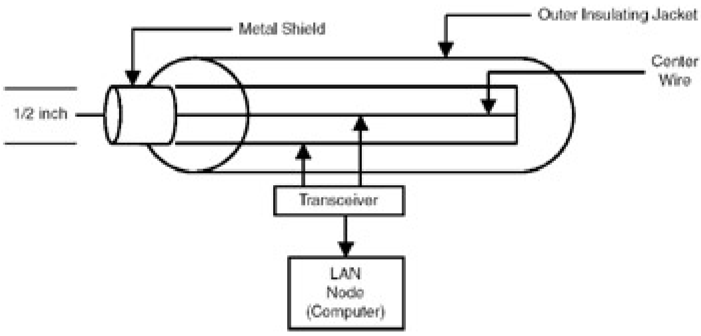


Figure 1.1: Coaxial cable used in Ethernet LAN.

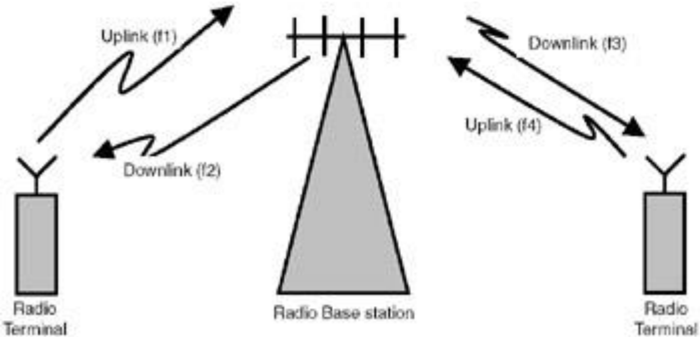


Figure 1.2: Two-way communication using radio

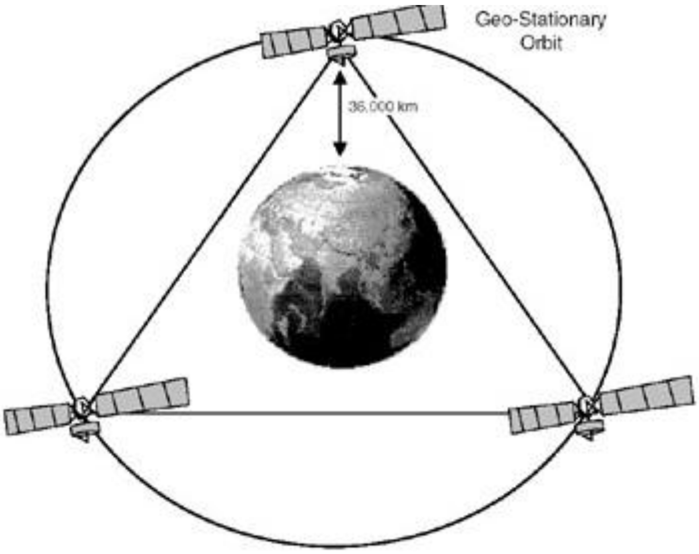


Figure 1.3: Three geostationary satellites covering the entire earth.

TYPES OF COMMUNICATION

Based on the requirements, the communications can be of different types:

Point-to-point communication: In this type, communication takes place between two end points. For instance, in the case of voice communication using telephones, there is one calling party and one called party. Hence the communication is point-to-point.

Point-to-multipoint communication: In this type of communication, there is one sender and multiple recipients. For example, in voice conferencing, one person will be talking but many others can listen. The message from the sender has to be *multicast* to many others.

Broadcasting: In a broadcasting system, there is a central location from which information is sent to many recipients, as in the case of audio or video broadcasting. In a broadcasting system, the listeners are passive, and there is no reverse communication path.

Simplex communication: In simplex communication, communication is possible only in one direction. There is one sender and one receiver; the sender and receiver cannot change roles.

Half-duplex communication: Half-duplex communication is possible in both directions between two entities
(computers or persons), but one at a time. A walkie-talkie uses this approach. The person who wants to talk presses a talk button on his handset to start talking, and the other person's handset will be in receive mode. When the sender finishes, he terminates it with an over message. The other person can press the talk button and start talking. These types of systems require limited channel bandwidth, so they are low cost systems.

Full-duplex communication: In a full-duplex communication system, the two parties—the caller and the called—can communicate simultaneously, as in a telephone system. However, note that the communication system allows simultaneous transmission of data, but when two persons talk simultaneously, there is no effective communication! The ability of the communication system to transport data in both directions defines the system as full-duplex.

In simplex communication, the communication is one-way only. In half-duplex communication, communication is both ways, but only in one direction at a time. In full-duplex communication, communication is in both directions simultaneously.

Depending on the type of information transmitted, we have voice communication, data communication, fax communication, and video communication systems. When various types of information are clubbed together, we talk of multimedia communications. Even a few years ago, different information media such as voice, data, video, etc. were transmitted separately by using their own respective methods of transmission. With the advent of digital communication and "convergence technologies," this distinction is slowly disappearing, and multimedia communication is becoming the order of the day.

TRANSMISSION IMPAIRMENTS

While the electrical signal is traversing over the medium, the signal will be impaired due to various factors. These
transmission impairments can be classified into three types:
a. Attenuation distortion
b. Delay distortion
c. Noise
The amplitude of the signal wave decreases as the signal travels through the medium. This effect is known as *attenuation distortion*. Delay distortion occurs as a result of different frequency components arriving at different times in the guided media such as copper wire or coaxial cable. The third type of impairment—noise—can be divided into the following categories:

- Thermal noise
- Intermodulation
- Crosstalk
- Impulse noise

Thermal noise: Thermal noise occurs due to the thermal agitation of electrons in a conductor. This is distributed uniformly across the spectrum and hence called *white noise*. This noise cannot be eliminated and hence, when designing telecom systems, we need to introduce some method to overcome the ill effects of thermal noise. Thermal noise for a bandwidth of 1 Hz is obtained from the formula:

No=KT

where No is noise power density, watts per Hz
K is the Boltzman's constant 1.3803 x 10^{-23} j/k
T is temperature, k.
Thermal noise for a bandwidth of B Hz is given by

N= kTB(watts)

If N is expressed in dB (decibels)
N=10log k+10log T+ 10 log B dB watts
=-228.6 +10 log T + 10 log B

Using this formula, thermal noise for a given bandwidth is calculated.

Note Thermal noise for a bandwidth of B Hz is given by N = kTB (watts) where k is Boltzmann's constant and T is temperature. N is generally expressed in decibels.

Inter modulation noise: When two signals of different frequencies are sent through the medium, due to nonlinearity of
the transmitters, frequency components such as f1 + f2 and f1 – f2 are produced, which are unwanted components and need to be filtered out.

Crosstalk: Unwanted coupling between signal paths is known as crosstalk. In the telephone network, this coupling is quite common. As a result of this, we hear other conversations. Crosstalk needs to be eliminated by using appropriate design techniques.

Impulse noise: This is caused by external electromagnetic disturbances such as lightning. This noise is unpredictable.
When the signal is traversing the medium, impulse noise may cause sudden bursts of errors. This may cause a temporary disturbance in voice communication. For data communication, appropriate methods need to be devised whereby the lost data is retransmitted.

Note Impulse noise occurs due to external electromagnetic disturbances such as lightning. Impulse noise causes burst of errors.
Noise is the source of bread and butter for telecom engineers! If there were no noise, there would be no need for telecom engineers—for we can then design perfect communication systems. Telecom engineering is all about overcoming the effects of noise.

Lecture three

3. Error Detection & Error correction

In a digital communication system, totally error-free transmission is not possible due to transmission impairments. At the receiving end, there should be a mechanism for detection of the errors and if possible for their correction. In this chapter, we will study the various techniques used for error detection and correction.

3.1 NEED FOR ERROR DETECTION AND CORRECTION

Consider a communication system in which the transmitted bit stream is

1 0 11 0 111 0

The transmitted electrical signal corresponding to this bit stream and the received waveform are shown in Figure 3.1.

Due to the noise introduced in the transmission medium, the electrical signal is distorted. By using a threshould, the receiver determines whether a 1 is transmitted or a 0 is transmitted. In this case, the receiver decodes the bit stream as

1 0 1 0 0 1 0 1 0

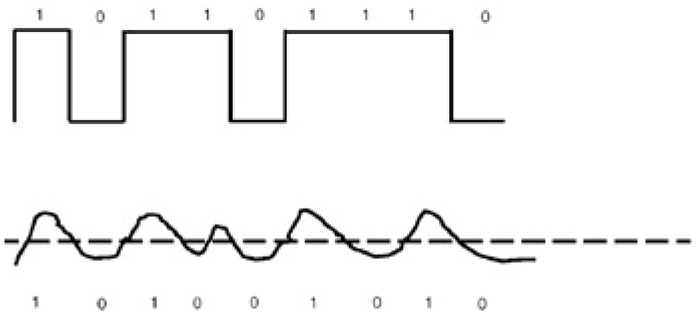


Figure 3.1: Errors introduced by transmission medium.

In a digital communication system, some bits are likely to be received in error due to the noise in the communication channel. As a result, 1 may become 0 or 0 may become 1. The Bit Error Rate (BER) is a parameter used to characterize communication systems.

At two places, the received bit is in error—1 has become 0 in both places.

How many errors can be tolerated by a communication system? It depends on the application. For instance, if English text is transmitted, and a few letters are received in error, it is tolerable. Studies indicate that even if 20% of the letters are missing, human beings can understand the text.

Suppose the communication system is used to transmit digitized voice from one place to another. Studies indicate that even if the Bit Error Rate is 10□3, the listener will be able to understand the speech. In other words, a voice communication system can tolerate one error for every 1000 bits transmitted.

Note The performance of a communication system can be characterized by the Bit Error Rate (BER). If BER is 10□3, there is one error per 1000 bits.
Errors can be classified as

- Random errors
- Burst errors

Random errors occur at random places in the bit stream. Burst errors occur due to sudden disturbances in the medium, caused by lightning, sudden interference with the nearby devices, etc. Such disturbances result in a sequence of bits giving errors.
Detection and correction of errors is done through channel coding. In channel coding, additional bits are added at the transmitter end, and these additional bits are used at the receiving end to check whether the transmitted data is received correctly or not and, if possible, to correct the errors.

3.2 ERROR DETECTION

The three widely used techniques for error detection are parity, checksum, and cyclic redundancy check (CRC). These techniques are discussed in the following sections.

3.2.1 Parity

Parity is used in serial communication protocols whereby we transmit one character at a time. For example, if the information bits are
1 0 1 1 0 1 0
then an additional bit is added, which is called a parity bit. The parity bit can be added in such a way that the total number of ones becomes even. In such a case, it is called *even parity*. In the above bit stream, already there are four ones, and hence a 0 is added as the parity bit. The bit stream transmitted is
1 0 1 1 0 1 0 0
In case of odd parity, the additional bit added will make the total number of ones odd. For odd parity, the additional bit added in the above case is 1 and the transmitted bit stream is
1 0 1 1 0 1 0 1
At the receiving end, from the first 7 bits, the receiver will calculate the expected parity bit. If the received parity and the calculated parity match, it is assumed that the character received is OK.
The various parities can be even, odd or none. In the case of none parity, the parity bit is not used and is ignored.
It is very easy to verify that parity can detect errors only if there is an odd number of errors; if the number of errors is 1, 3, or 5, the error can be detected. If the number of errors is even, parity bit cannot detect the error.

3.2.2 Block Codes

The procedure used in block coding is shown in Figure 3.2. The block coder takes a block of information bits (say 8000 bits) and generates additional bits (say, 16). The output of the block coder is the original data with the additional 16 bits. The additional bits are called checksum or cyclic redundancy check (CRC). Block codes can detect errors but cannot correct errors.

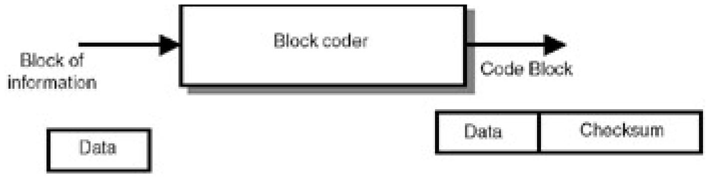


Figure 3.2: Block coder.

Checksum

Suppose you want to send two characters, C and U.
The 7-bit ASCII values for these characters are
C 1 0 0 0 0 1 1
U 1 0 1 0 1 0 1
In addition to transmitting these bit streams, the binary representation of the sum of these two characters is also sent. The value of C is 67 and the value of U is 85. The sum is 152. The binary representation of 152 is 1 0 0 1 1 0 0 0. This bit stream is also attached to the original binary stream, corresponding to C and U, while transmitting the data.

Checksum of information bits is calculated using simple binary arithmetic. Checksum is used extensively because its computation is very easy. However, checksum cannot detect all errors.
So, the transmitted bit stream is

1 0 0 0 0 1 1 1 0 1 0 1 0 1 1 0 0 1 1 0 0 0

At the receiving end, the checksum is again calculated. If the received checksum matches this calculated checksum, then the receiver assumes that the received data is OK. The checksum cannot detect all the errors. Also, if the characters are sent in a different order, i.e., if the sequence is changed, the checksum will be the same and hence the receiver assumes that the data is correct.
However, checksum is used mainly because its computation is very easy, and it provides a reasonably good error detection capability.
Note Checksum is used for error detection in TCP/IP protocols to check whether packets are received correctly.
Different algorithms are used for calculation of checksum.

3.2.3 Cyclic Redundancy Check

CRC is a very powerful technique for detecting errors. Hence, it is extensively used in all data communication systems.

Additional bits added to the information bits are called the CRC bits. These bits can be 16 or 32. If the additional bits are 16, the CRC is represented as CRC-16. CRC-32 uses 32 additional bits.

Error detection using CRC is very simple. At the transmitting side, CRC is appended to the information bits. At the receiving end, the receiver calculates CRC from the information bits and, if the calculated CRC matches the received CRC, then the receiver knows that the information bits are OK.

Note In CRC calculation, a standard polynomial is used. This polynomial is different for CRC- 16 and CRC-32. The bit stream is divided by this polynomial to calculate the CRC bits.

Using error detection techniques, the receiver can detect the presence of errors. In a practical communication system, just detection of errors does not serve much purpose, so the receiver has to use another mechanism such as asking the transmitter to resend the data. Communication protocols carry out this task.

Listing 3.2 gives the C program to calculate CRC-32. In this program the message for which CRC has to be calculated is "Hello World". The message bit stream is

01001000 01100101 01101100 01101100 01101111 00100000 01010111
01101111 01110010 01101100 01100100 00000000 00000000 00000000 00000000
The calculated CRC is 0x31d1680c.

Note In CRC calculation, a standard polynomial is used. This polynomial is different for CRC- 16 and CRC-32. The bit stream is divided by this polynomial to calculate the CRC bits.

Using error detection techniques, the receiver can detect the presence of errors. In a practical communication.

Listing 3.1

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
long CRC = 0x0000;
long GenPolynomial = 0x8005; //Divisor for CRC-16 Polynomial
void bitBybit(int bit);
int main()
{
unsigned int MsgLength;
int i=0,j=0;
char SampleMsg[] = "Hello World";
char tempBuffer[100];
MsgLength = sizeof(SampleMsg)-1;
printf("\nActual Message: %s\n",SampleMsg);
strcpy(tempBuffer, SampleMsg);
tempBuffer[MsgLength] = 0x00;
tempBuffer[MsgLength+1] = 0x00;
tempBuffer[MsgLength+2] = '\0';
printf("\nAfter padding 16 0-bits to the Message:");
for(i=0;i<MsgLength+2;++i)
{
unsigned char ch = tempBuffer[i];
unsigned char mask = 0x80;
for(j=0;j<8;++j)
{
bitBybit(ch&mask);
mask>>=1;
}
printf(" ");
}
printf("\n\nCalculated CRC:0x%x\n\n",CRC);
return 0;
}
void bitBybit(int bit)
{
long firstBit = (CRC & 0x8000);
CRC = (CRC << 1);
if(bit)
{
CRC = CRC ^ 1;
printf("1");
}
else
{
CRC = CRC ^ 0;
printf("0");
}
if(firstBit)
{
CRC = (CRC^GenPolynomial);
}
}
```

In this listing, the actual message to be transmitted is "Hello World". The message is padded with sixteen 0 bits, and
the message bit stream is

```
01001000 01100101 01101100 01101100 01101111 00100000 01010111
01101111 01110010 01101100 01100100 00000000 00000000
```

The calculated CRC value in hexadecimal notation is 0x303f70c3.

Program for calculation of CRC-32

Program for calculation of CRC-32.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
long CRC = 0x00000000L;
long GenPolynomial = 0x04c11db7L; //Divisor for CRC-32 Polynomial
void bitBybit(int bit);
int main()
{
unsigned int MsgLength;
int i=0,j=0;
char SampleMsg[] = "Hello World";
char tempBuffer[100];
MsgLength = sizeof(SampleMsg)-1;
printf("\nActual Message: %s\n",SampleMsg);
strcpy(tempBuffer, SampleMsg);
tempBuffer[MsgLength] = 0x00;
tempBuffer[MsgLength+1] = 0x00;
tempBuffer[MsgLength+2] = 0x00;
tempBuffer[MsgLength+3] = 0x00;
tempBuffer[MsgLength+4] = '\0';
printf("\nAfter padding 32 0-bits to the Message:");
for(i=0;i<MsgLength+4;++i)
{
unsigned char ch = tempBuffer[i];
unsigned char mask = 0x80;
for(j=0;j<8;++j)
{
bitBybit(ch&mask);
mask>>=1;
}
printf(" ");
}
printf("\n\nCalculated CRC:0x%x\n\n",CRC);
return 0;
}
void bitBybit(int bit)
{
long firstBit = (CRC & 0x80000000L);
CRC = (CRC << 1);
if(bit)
{
CRC = CRC ^ 1;
printf("1");
}
else
{
CRC = CRC ^ 0;
printf("0");
}
if(firstBit)
{
CRC = (CRC^GenPolynomial);
}
}
```

Lecture Four

4. Introduction to Multiplexing

In a communication system, the costliest element is the transmission medium. To make the best use of the medium, we have to ensure that the bandwidth of the channel is utilized to its fullest capacity. *Multiplexing* is the technique used to combine a number of channels and send them over the medium to make the best use of the transmission medium.

4.1 MULTIPLEXING AND DEMULTIPLEXING

Use of multiplexing technique is possible if the capacity of the channel is higher than the data rates of the individual data sources. Consider the example of a communication system in which there are three data sources. As shown in Figure 4.1, the signals from these three sources can be combined together (multiplexed) and sent through a single transmission channel. At the receiving end, the signals are separated (demultiplexed).

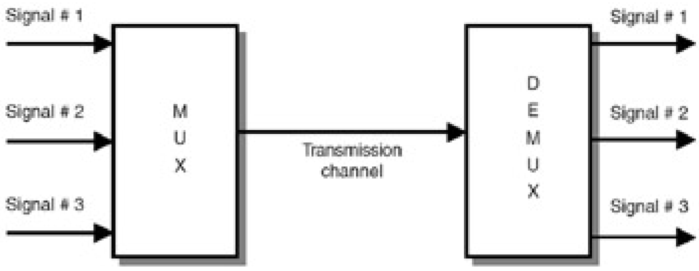


Fig.4.1 Multipler & Demultiplexer

At the transmitting end, equipment known as a multiplexer (abbreviated to MUX) is required. At the receiving end, equipment known as a demultiplexer (abbreviated to DEMUX) is required. Conceptually, multiplexing is a very simple operation that facilitates good utilization of the channel bandwidth. The various multiplexing techniques are described in the following sections.

A multiplexer (MUX) combines the data of different sources and sends it over the channel. At the receiving end, the demultiplexer (DEMUX) separates the data of the different sources. Multiplexing is done when the capacity of the channel is higher than the data rates of the individual data sources.

4.2 FREQUENCY DIVISION MULTIPLEXING

In frequency division multiplexing (FDM), the signals are translated into different frequency bands and sent over the medium. The communication channel is divided into different frequency bands, and each band carries the signal corresponding to one source.

Consider three data sources that produce three signals as shown in Figure 4.2. Signal #1 is translated to frequency band #1, signal #2 is translated into frequency band #2, and so on. At the receiving end, the signals can be demultiplexed using filters. Signal

#1 can be obtained by passing the multiplexed signal through a filter that passes only frequency band #1.

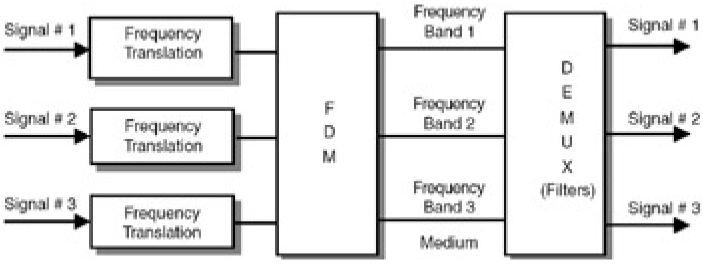


Figure 4.2: FDM

FDM is used in cable TV transmission, where signals corresponding to different TV channels are multiplexed and sent through the cable. At the TV receiver, by applying the filter, a particular channel's signal can be viewed. Radio and TV transmission are also done using FDM, where each broadcasting station is given a small band in the frequency spectrum. The center frequency of this band is known as the *carrier frequency*.

NOTE

In FDM, the signals from different sources are translated into different frequency bands at the transmitting side and sent over the transmission medium. In cable TV, FDM is used to distribute programs of different channels on different frequency bands. FDM is also used in audio/video broadcasting

4.3 TIME DIVISION MULTIPLEXING

In synchronous time division multiplexing (TDM), the digitized signals are combined and sent over the communication channel. Consider for ex. the case of a communication system, three data sources produce data at 64kbps using pulse code modulation (PCM). Each sample will be 8 bits, and the time gap between two successive samples is 125 microseconds. The job of the MUX is to take the 8-bit sample value of the first channel and the 8 bits of the second channel and then the 8 bits of the third channel. Again, go back to the first channel. Since no sample should be lost, the job of the MUX is to complete scanning all the channels and obtain the 8-bit sample values within 125 microseconds. This combined bit stream is sent over the communication medium. The MUX does a scanning operation to collect the data from each data source and also ensures that no data is lost. This is known as time division multiplexing. The output of the MUX is a continuous bit stream, the first 8 bits corresponding to Channel 1, the next 8 bits corresponding to Channel 2, and so on.

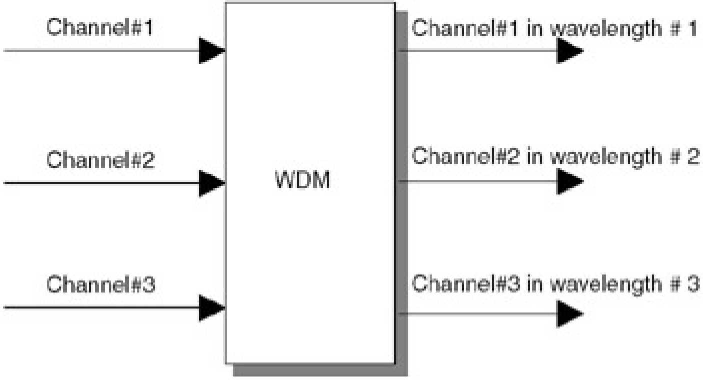
4.4 WAVE DIVISION MULTIPLEXING

Wave division multiplexing (WDM) is used in optical fibers. In optical fiber communication, the signal corresponding to a channel is translated to an optical frequency (generally expressed in wavelength) and transmitted. This optical frequency is expressed by its equivalent wavelength and denoted by □□(lambda).

Instead of transmitting only one signal on the fiber, if two (or more) signals are sent on the same fiber at different frequencies (or wavelengths), it is called WDM. In 1994, this was demonstrated—signal frequencies had to be separated widely, typically 1310 nm and 1550 nm. Therefore, just using the two wavelengths can double the fiber capacity.

As shown in Figure 4.3, the wave division multiplexer takes signals from different channels, ranslates them to different wavelengths, and sends them through the optical fiber. Conceptually, it is the same as FDM.

Figure 4.3:


Channel#1
Channel#2
Channel#3
WDM
Channel#1 in wavelength # 1
Channel#2 in wavelength # 2
Channel#3 in wavelength # 3

Wave Division Multiplexing is used in optical fibers. Data of different sources is sent through the fiber using different wavelengths. The advantage of WDM is that the full capacity of an already laid optical fiber can be used.

Lecture 5

5.1 Introduction

5.1.1 Data Link Layer

The open systems interconnection(OSI) model is a reference tool for understanding data communications between any two networked systems. It divides the communications processes into seven layers. Each layer both performs specific functions to support the layers above it & offers a service to the layer below it. The three lowest layers focus on passing traffic through the network to an end system. The top four layers come into play in the end system to complete the process.

The second layer of OSI model provides the following function:-

1. allows a dev. To access the network to send & receive messages
2. offers a physical address so a dev.'s data can be sent on the network.
3. works with dev.'s networking s/w when sending & receiving messages.
4. provides error detection capability.

Common networking components that function at layer 2 includes

- network interface card.
- Ethrent & token ring switches
- Bridges

Bridges & switches function is a similar fashion, bridging is normally a s/w program on a cpu , while switches use application specific integrated circuit(ASICs) to perform the task in dedicated H/W which is much faster.

5.2 link layer protocol

A link is the physical communication channels that connect either two host, two routers or a host-router pair. The **link-layer protocol** defines the format of the units of data (**frames**) exchanged between the nodes at the ends of the link, as well as the actions taken by these nodes when sending and receiving these data units. Each link-layer frame typically encapsulates one network layer datagram.

A link-layer protocol has the node-to-node job of moving a network-layer datagram over a *single link* in the path. An important characteristic of the link layer is that a datagram may be handled by different link- layer protocols, offering different services, on the different links in the path.

Possible services that can be offered by a link- layer protocol include:

•**Framing and link access**. Almost all link- layer protocols encapsulate each network-layer datagram within a network-layer datagram is inserted, and a number of header fields. A data- link protocol specifies the structure of the frame, as well as a channel access protocol that specifies the rules by which a frame is transmitted onto the link. the channel access protocol serves to coordinate the frame transmissions of the many nodes link-layer frame before transmission onto the link. A frame consists of a data field, in which the frame headers also often include fields for **physical address,** which is completely *distinct* from the node's network layer (for example, IP) address.

•**Reliable delivery**. When a link-layer protocol provides reliable-delivery service, it guarantees to move each network-layer datagram across the link without error. This is achieved with acknowledgments and retransmissions. A link- layer reliable-delivery service is often used for links that are prone to high error rates, such as a wireless link, with the goal of correcting an error locally,

on the link where the error occurs, rather than forcing an end-to-end retransmission of the data by a transport- or application- layer protocol. However, link-layer reliable delivery can be considered an unnecessary overhead for low bit-error links, including fiber, coax, and many twisted-pair copper links. For this reason, many of the most popular link- layer protocols do.

link layer services are:-

- ➢ **Flow Control:**

1. pacing between sender and receivers

- ➢ **□Error Detection:**

1. **□errors caused by signal attenuation, noise.**
2. **□receiver detects presence of errors:**
3. **signals sender for retransmission or drops frame**

- ➢ **□Error Correction:**

1. □receiver identifies and corrects bit error without resorting to retransmission

- ➢ **□Half-duplex and full-duplex**

Multiple Access Links and Protocols

Three types of “links”:

□□point-to-point (single wire, e.g. PPP, SLIP)

□□broadcast (shared wire or medium; e.g, Ethernet, Waveland, etc.)

□□switched (e.g., switched Ethernet, ATM etc)

Multiple Access protocols

❒ single shared communication channel

❒ two or more simultaneous transmissions by nodes: Interference

only one node can send successfully at a time

Blah,
zzzz
shared wire
(e.g. Ethernet)
shared wireless
(e.g. Wavelan)
satellite
coc

❒ multiple access protocol:

□□distributed algorithm that determines how stations share channel, i.e., determine when station can transmit

□□communication about channel sharing must use channel itself!

□□what to look for in multiple access protocols:

- synchronous or asynchronous
- information needed about other stations
- robustness (e.g., to channel errors)
- performance

There are three broad classes:

❒ Channel Partitioning

❍ divide channel into smaller “pieces” (time slots, frequency)

□□allocate piece to node for exclusive use

❒ Random Access

❍ allow collisions

□□“recover” from collisions

❒ **“Taking turns”**

❍ tightly coordinate shared access to avoid collisions

5.3 LAN Technologies

Multiple access protocols are extensively used in local area networks(LANs). A LAN is a broadcast channel, which provides to its host access to the Internet through a router. The LAN is a single "link" between each user host and the router, where each node sends frames to each other over a broadcast channel; it therefore uses a link- layer protocol, part of which is a multiple access protocol. The transmission rate, *R*, of most LANs is very high (up to 1Gbps).

➢ in general a node in the LAN doesn't want to send a frame to *all* of the other LAN nodes but instead wants to send to some *particular* LAN node. Therefore, the nodes need LAN addresses (in reality the is adapters has a LAN address) and the link- layer frame needs a field to contain such a destination address.

➢ In this manner, when a node receives a frame, it can determine whether the frame was intended for it or for some other node in the LAN. Note that, with the introduction of layer 2 addresses, broadcast must be explicitly addressed. Additionally, some LANs needs to be interconnected together, and this can be obtained with different type of devices: repeaters, hubs, bridges, switches.

➢ This interconnection takes place at layer 2. Finally, several geographically distant LANs can be interconnected only at physical layer and “virtually” interconnected at layer 2in a so called virtual LAN.

HUB
The simplest way to interconnect LANs is to use a hub. A **hub** is a simple device that takes an input (that is, a frame's bits) and retransmits the input on the hub's outgoing ports. Hubs are essentially repeaters, operating on bits.
They are thus physical- layer devices. When a bit comes into a hub interface,the hub simply broadcasts the bit on all the other interfaces. All nodes belong to the same **collision domain,** that is, whenever two or more nodes on the LAN segments transmit at the same time, there will be a collision and all of the transmitting nodes will enter exponential back off.

Bridges – layer 2

❒ Link Layer devices: operate on Ethernet frames, examining frame header and selectively forwarding frame based on its destination

❒ Bridge isolates collision domains since it buffers frames

❒ When frame is to be forwarded on segment, bridge uses CSMA/CD to access segment and transmit ❒ Can connect different type Ethernet since it is a buffering device

❒ two bridges protocols: transparent bridge and spanning tree protocol

Bridges vs. Routers

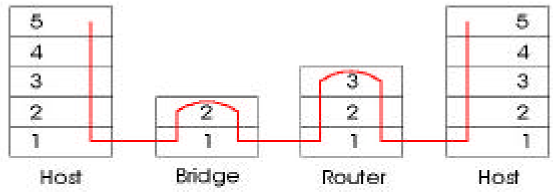
❒ both store-and-forward devices

❍ routers: network layer devices (examine network layer headers)

❍ bridges are Link Layer devices

❒ routers elaboration ~ 10 times bridges elaboration

❒ bridges are plug-and-play



5.4 Address Resolution Protocol(ARP)

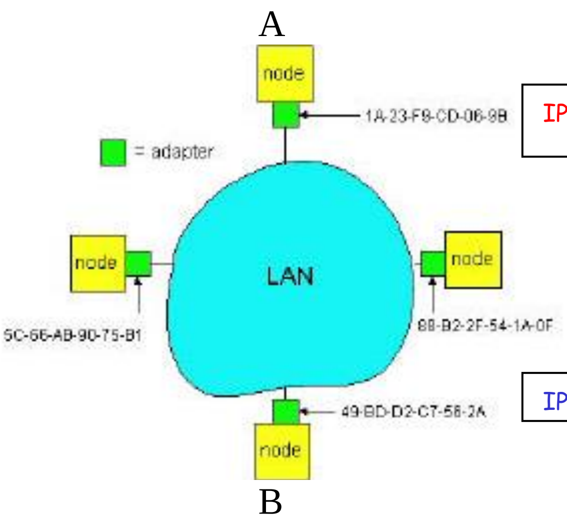
The Address Resolution Protocol is a request and reply protocol that runs encapsulated by the line protocol. It is communicated within the boundaries of a single network, never routed across internet work nodes. This property places ARP into the link layer of the internet protocol suite while in the (OSI) model, it is often described as residing between Layers 2 and 3, being encapsulated by Layer 2 protocols. However, ARP was not developed in the OSI framework.

Every Internet host and router on a LAN has an **ARP module.** ARP resolves an IP address to a LAN address ***only* for nodes on the same LAN**. The ARP module in each node has a table in its RAM called an **ARP table**. This table contains the mappings of IP addresses to LAN addresses.

For each address mapping the table also contains a time-to- live (TTL) entry, which indicates when the entry will be deleted from the table (typically 20 mintues)

If the table does not contain the MAC address of the destination, the source constructs a special packet called an **ARP packet.** An ARP packet has several fields, including the sending and receiving IP and LAN addresses. Both ARP query and response packets have the same format. The purpose of the ARP query packet is to query all the other nodes on the LAN to determine the LAN

address corresponding to the IP address that is being resolved. If the MAC address is returned, the querying node can then update its ARP table and send its IP datagram.

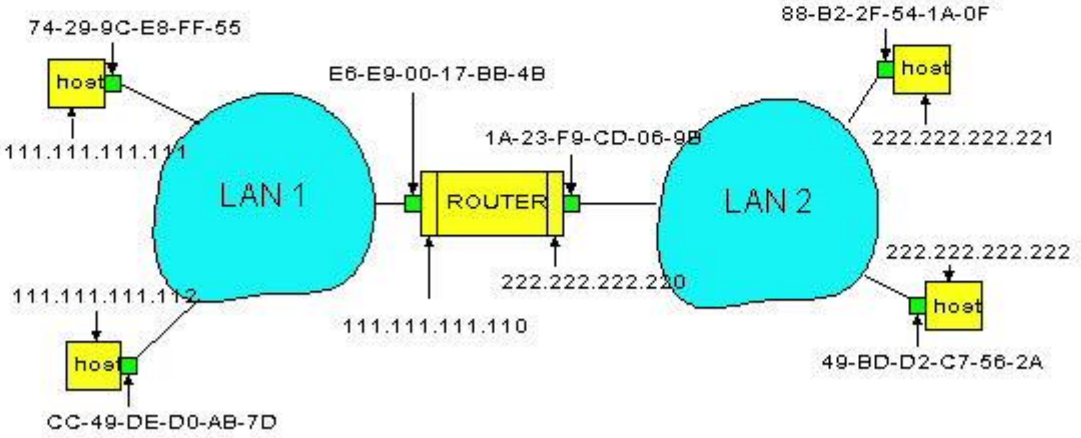


IP dest| IP source|MAC source

IP dest| IP source|MAC source| MAC

Routing to another LAN

walkthrough: routing from A to B via R



❒ In routing table at source Host, find router 111.111.111.110

❒ In ARP table at source, find MAC address E6-E9-00-17-BB-4B, etc

Note

ARP operates when a node wants to send a datagram to another node *on the same LAN*. The situation is more complex when a node on a LAN wants to send a network-layer datagram to a node *off the LAN*. All of the interfaces connected to LAN 1 have addresses of the form 111.111.111.xxx and all of the interfaces connected to LAN 2 have the form 222.222.222.xxx.

Now suppose that host 111.111.111.111 wants to send an IP datagram to host 222.222.222.222. The sending host passes the datagram to its adapter, as usual. However, it is not able to indicate an appropriate destination LAN address. Even if known, the MAC address of the destination cannot be used in this case: none of the adapters on LAN 1 would bother to pass the IP datagram up to its network layer, since the frame's destination address would not match the LAN address of any adapter on LAN 1. And the datagram would die. Indeed, the route of the datagram is decided at network layer. It has to pass through the router R, that will the forward it to the LAN2. Therefore, the MAC address that has to be used is the one of the next step, that is the one of the interface on LAN1 of R. In R the packet is passed up to the network layer, where the next routing step is considered. When in the LAN2 (e.g. at the interface of R on LAN2) R uses ARP to get the destination physical layer address. Finally, R creates the frame containing source-to-destination IP datagram sends to destination A

5.5 Telnet

Telnet provides a method to monitor printer activities over a TCP/IP network. Printer activities such as status, media type, ribbon type, print queues, and progress messages can be viewed via Telnet.

From most computer systems, a Telnet connection is established by typing:

telnet hostname *or* **IP Address**

- The user will be prompted for a login name and password. When those are entered, a command line prompt, #, will be displayed. The user is now logged into the printer.
- A user can login as **root** to the printer. There is no password initially on root. Being logged in as root gives the user superuser privileges. A password can be installed for the root login by typing, **passwd**. This command will prompt you for a password, and then make you retype. If you forget the password the printer can be returned to factory state by performing a Level -0 Reset.
- Progress messages are displayed to your Telnet session from the different programs running when an image is processed and printed.

- The status login displays the operating status of the printer. This special login is provided so that anyone can inquire about the root status of the printer without needing root privileges.

Telnet into the printer using:

telnet hostname *or* **IP Address**
login: **status**

The information displayed is printer status, date and time, media installed, ribbon installed,
printer ID, Ethernet address, print jobs in image processing queue and print queue, captions installed, keys installed, and image parameters.

5.6 DNS(Domain Name System)

- DNS provides a name lookup facility that is similar to a standard telephone directory. To perform lookups, DNS relies on a distributed system of name servers and a standardized language to query these servers. Each name server stores a portion of the overall name space, and can contact other name servers to lookup names outside its name space.

The three main components of a DNS system are:

- Domain Name Space: defines the overall naming structure of the Internet.
- Name Server: maintains a portion of the domain name spaces, resolves lookups, and maintains a cache .
- Domain Name Resolution: maps a domain name to an IP address

An effective Domain Name System (DNS) is critical to Internet access speeds. The bandwidth of your Internet connection is irrelevant if the DNS system is slow.

- DNS supports high performance, availability, and scalability through the use of data hierarchies, data replication, and caching.

- The domain name space defines the overall naming structure of the Internet.
- The name space is consists of a tree structure of domain names, with a root domain at the top. Immediately below the root domain are the major domains such as .com, .net, and .org. From these domains, the name space can branch into multiple paths, with each intersection point called a node and labeled with a simple name
- DNS processes a domain name from right to left, with the highest-level node represented at the far right, and the lowest level node at the far left. The node labels are separated by dots.
- The domain name of any node in the tree is the sequence of node labels leading from that node all the way up to the root domain.

The top-level node (appearing farthest to the right) identifies the geography or purpose (for example, the nation covered by the domain, such as .uk, or a company category, such as .com). The second-level node (appearing second from the right) identifies a unique place within the top-level domain.

Domain names can contain up to 255 characters consisting of: characters A to Z, 0 to 9, and/or “-”; 63 characters per node; and up to 127 node levels. To ensure that each node is uniquely identified, DNS requires that sibling nodes - nodes that are “children” of the same “parents” - be uniquely named. For example, these “absolute” names are unique: beckett.incognito.com and beckett.af.mil.

Zones

- the name space tree is sub-divided into zones. A zone consists of a group of linked nodes served by an authoritative DNS name server (the final authority in providing information about a set of domains).

- A zone contains domain names starting at a particular point in the tree ("Start Of Authority") to the end node or to a point in the tree where another host has authority for the names.

For example, the top-level .gov domain has the sub domains wa.gov, tx.gov, co.gov, for the states Washington, Texas and Colorado. The .gov zone file contains pointers to the sources of data for tx.gov, co.gov and wa.gov.

Similarly, if the wa.gov domain delegated authority for dol.co.gov to the information system section of the Washington State Department of Licensing, the zone file for wa.gov only contains a pointer to the data source for dol.wa.gov.

- There are two types of name servers: primary and secondary. Every zone MUST have its data stored on both a primary and a secondary name server.
- Primary name servers hold "authoritative" information about set of domains, as well as cached data about domains previously requested from other servers.
- Secondary name servers can download a copy of zone information from a primary name server using a process called a "zone transfer."
- Zone transfers allow secondary name servers to download complete copies of zones.

5.7 UDP: User Datagram Protocol

- UDP is a connectionless transport layer (layer 4) protocol in OSI model, which provides a simple and unreliable message service for transaction-oriented services. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another.

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine, and some way to make sure replies get routed to the correct application on the source computer. This is accomplished through the use of the UDP "port numbers". For example, if a station wished to use a Domain Name

- System (DNS) on the station 128.1.123.1, it would address the packet to station 128.1.123.1 and insert destination port number 53 in the UDP header. The source port number identifies the application on the local station that requested domain name server, and all response packets generated by the destination station should be addressed to that port number on the source station. Details of UDP port numbers could be found in the TCP/UDP Port Number document and in the reference. Unlike the TCP , UDP adds no reliability, flow-control, or error-recovery functions to IP.
- Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP.
- UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control, or real time data transportation is required.
- UDP is the transport protocol for several well-known application-layer protocols,

including Network File System (NFS) , Simple Network Management Protocol (SNMP) , Domain Name System (DNS) , and Trivial File Transfer Protocol (TFTP).

Protocol Structure - UDP User Datagram Protocol Header

16	**32 bit**
Source port	**Destination port**
Length	**checksum**
Data	

- Source port - Source port is an optional field. When used, it indicates the port of the sending process and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.
- Destination port - Destination port has a meaning within the context of a particular Internet destination address
- Length - It is the length in octets of this user datagram, including this header and the data. The minimum value of the length is eight.
- Checksum -- The sum of a pseudo header of information from the IP header, the UDP header and the data, padded with zero octets at the end, if necessary, to make a multiple of two octets.
- Data - Contains upper-level data information.