

Data Communication and Computer Network



Government of Nepal
Ministry of Education, Science and Technology
Curriculum Development Centre
Sanothimi, Bhaktapur

Phone : 5639122/6634373/6635046/6630088
Website : www.moecdc.gov.np



**Technical and Vocational Stream
Learning Resource Material**

**DATA COMMUNICATION AND COMPUTER NETWORK
(Grade 12)**

**Secondary Level
Computer Engineering**



Government of Nepal
Ministry of Education, Science and Technology
Curriculum Development Centre
Sanothimi, Bhaktapur

Publisher : Government of Nepal

Ministry of Education, Science and Technology

Curriculum Development Centre

Sanothimi, Bhaktapur

© Publisher

Layout by Khados Sunuwar

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any other form or by any means for commercial purpose without the prior permission in writing of Curriculum Development Centre.

Preface

The curriculum and curricular materials have been developed and revised on a regular basis with the aim of making education objective-oriented, practical, relevant and job oriented. It is necessary to instill the feelings of nationalism, national integrity and democratic spirit in students and equip them with morality, discipline and self-reliance, creativity and thoughtfulness. It is essential to develop in them the linguistic and mathematical skills, knowledge of science, information and communication technology, environment, health and population and life skills. It is also necessary to bring in them the feeling of preserving and promoting arts and aesthetics, humanistic norms, values and ideals. It has become the need of the present time to make them aware of respect for ethnicity, gender, disabilities, languages, religions, cultures, regional diversity, human rights and social values so as to make them capable of playing the role of responsible citizens with applied technical and vocational knowledge and skills. This Learning Resource Material for Computer Engineering has been developed in line with the Secondary Level Computer Engineering Curriculum with an aim to facilitate the students in their study and learning on the subject by incorporating the recommendations and feedback obtained from various schools, workshops and seminars, interaction programs attended by teachers, students and parents.

In bringing out the learning resource material in this form, the contribution of the Director General of CDC Dr. Lekhnath Poudel, Pro, Dr. Subarna Shakya, Bibha Sthapit, Kumar Prasun, Yogesh Parajuli, Dr. Romakanta Pandey, Dinesha Khatri, Bimal Thapa, Jonshan Khadka is highly acknowledged. The book is written by Satyaram Suwal and the subject matter of the book was edited by Badrinath Timalina and Khilanath Dhamala. CDC extends sincere thanks to all those who have contributed in developing this book in this form.

This book is a supplementary learning resource material for students and teachers. In addition they have to make use of other relevant materials to ensure all the learning outcomes set in the curriculum. The teachers, students and all other stakeholders are expected to make constructive comments and suggestions to make it a more useful learning resource material.

Content

1.	Communication System and Transmission Media	1
2.	Multiplexing and Switching	26
3.	Modulation Scheme	42
4.	Computer Network and Topology	46
5.	Reference Model	57
6.	IP Addressing	65
7.	Router Configuration	76
8.	Network Cabling	92
9.	Network Troubleshoot	115

Unit: 1

Communication System and Transmission Media

Objective

After completion of this unit students will be able

- To explain the concept of Analog and Digital Signal
- To elaborate different types of transmission media
- To distinguish between Simplex, Half-Duplex and Full Duplex

Learning process and support material

- Class demonstration with Pictures and Lecture method
- Group discussion and Questionnaire

Content's Elaboration

Analogue Communication

An **analog signal** is a continuous wave denoted by a sine wave (pictured below) and may vary in signal strength (amplitude) or frequency (time). The sine wave's amplitude value can be seen as the higher and lower points of the wave, while the frequency (time) value is measured in the sine wave's physical length from left to right. There are many examples of analog signals around us. The sound from a human voice is analog, because sound waves are continuous, as is our own vision, because we see various shapes and colors in a continuous manner due to light waves. Even a typical kitchen clock having its hands moving continuously can be represented as an analog signal.

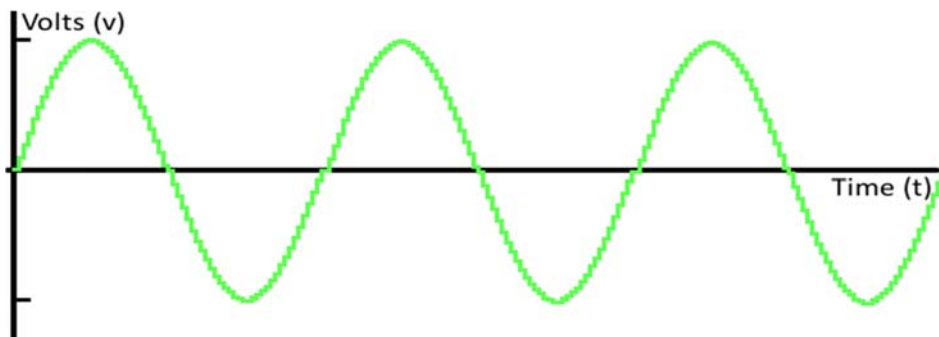


Fig: Analog Signal

Block diagram of Analog Communication

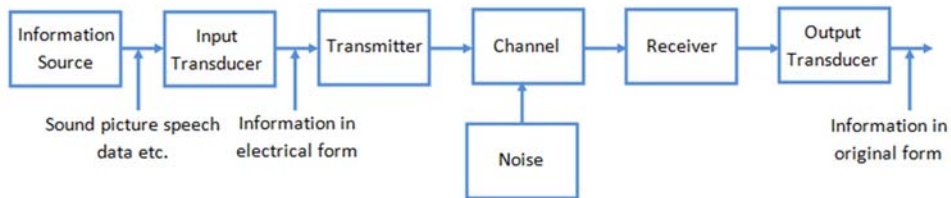


Fig: Basic analog communication system

- The elements of basic analog communication system are input signal or information, input transducer, transmitter, channel, noise, receiver, output transducer.

1. Information or Input signal

- The information is transmitted from one place to another.
- This information can be in the form of a sound signal like speech, or it can be in the form of pictures or it can be in the form of data information.

2. Input transducer

- The information in the form of sound, picture or data signals cannot be transmitted as it is.
- First it has to be converted into a suitable electrical signal.
- The input transducer block does this job.
- The commonly used input transducers used are microphones, TV etc.

3. Transmitter

- The function of the transmitter is to convert the electrical equivalent of the information to a suitable form so that it can transfer over long distance.
- Basic block in transmitter are: Amplifier, Oscillator, Mixer.

4. Channel

- The communication channel is the medium used for transmission of electrical signal from one place to other.
- The communication medium can be conducting wires, cables, optical fibers or free space.

- Depending on the type of communication medium, two types of communication system exist.
- Line communication: The line communication systems uses the communication medium like the simple wires or cables or optical fibers. E.g. Telephone, Cable TV.
- Radio communication : The radio communication systems uses the free space as their communication medium. The transmitted signal is in the form of electromagnetic waves. e.g. Mobile communication, satellite communication.

5. Noise

- Noise is an unwanted electrical signal which gets added to the transmitted signal when it is travelling towards the receiver.
- Due to noise quality of information gets degraded.
- Once added the noise cannot be separated out from the information

6. Receiver

- The receiver always converts the modulated signal into original signal which consists of Amplifier, Oscillator, Mixer.

7. Output transducer

- Output transducer converts electrical signal into the original form i.e. sound or TV pictures etc.
e.g. loudspeaker, data and image convertor.

Digital Signal

A **digital signal** a must for computer processing, is described as using binary (0s and 1s), and therefore, cannot take on any fractional values. As illustrated in the graphic below, digital signals retain a uniform structure, providing a constant and consistent signal. Because of the inherent reliability of the digital signal, technology using it is rapidly replacing a large percentage of analog applications and devices. For example, the wristwatch, showing the time of day, with its minute, hour, and sweeping second hands, is being replaced by the digital watch, which offers the time of day and other information using a numerical display. A typical digital signal is represented below. Note the equally dispersed 1s and 0s.

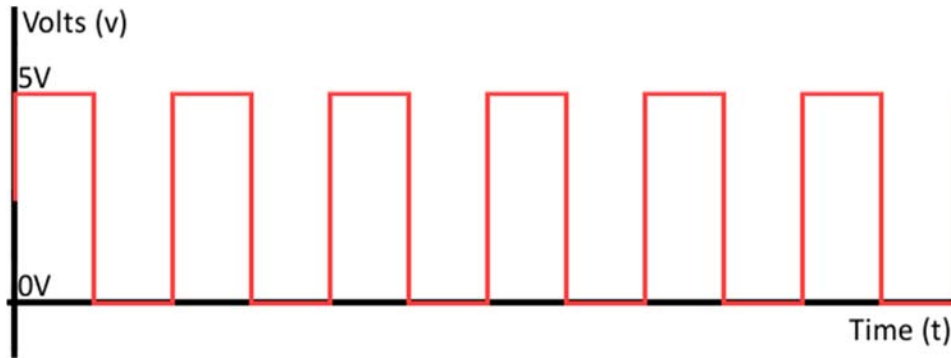


Fig: Digital Signal

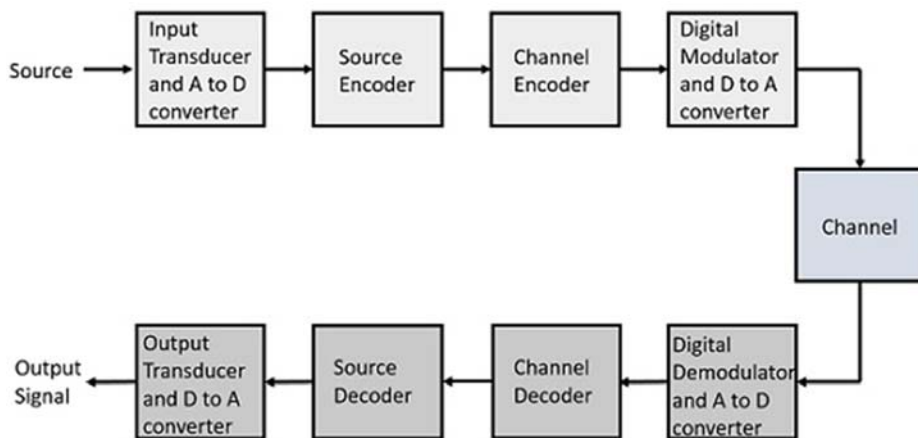
Advantages of Digital Signals

As the signals are digitized, there are many advantages of digital communication over analog communication, such as—

- The effect of distortion, noise, and interference is much less in digital signals as they are less affected.
- Digital circuits are more reliable.
- Digital circuits are easy to design and cheaper than analog circuits.
- The hardware implementation in digital circuits, is more flexible than analog.
- The occurrence of cross-talk is very rare in digital communication.
- The signal is un-altered as the pulse needs a high disturbance to alter its properties, which is very difficult.
- The probability of error occurrence is reduced by employing error detecting and error correcting codes.
- Spread spectrum technique is used to avoid signal jamming.
- Combining digital signals using Time Division Multiplexing (TDM) is easier than combining analog signals using Frequency Division Multiplexing (FDM).
- The configuring process of digital signals is easier than analog signals.
- Digital signals can be saved and retrieved more conveniently than analog signals.

Block Diagram of Digital Communication

The elements which form a digital communication system is represented by the following block diagram for the ease of understanding.



Basic Elements of a Digital Communication System

Following are the sections of the digital communication systems :

Source

The source can be an **analog** signal. **Example:** A sound signal

Input Transducer

This is a transducer which takes a physical input and converts it to an electrical signal (**Example:** microphone). This block also consists of an **analog to digital** converter where a digital signal is needed for further processes. A digital signal is generally represented by a binary sequence.

Source Encoder

The source encoder compresses the data into minimum number of bits. This process helps in effective utilization of the bandwidth. It removes the redundant bits (unnecessary excess bits, i.e., zeroes).

Channel Encoder

The channel encoder, does the coding for error correction. During the transmission of the signal, due to the noise in the channel, the signal may get altered and hence to avoid this, the channel encoder adds some redundant bits to the transmitted data.

These are the error correcting bits.

Digital Modulator

The signal to be transmitted is modulated here by a carrier. The signal is also converted to analog from the digital sequence, in order to make it travel through the channel or medium.

Channel

The channel or a medium, allows the analog signal to transmit from the transmitter end to the receiver end.

Digital Demodulator

This is the first step at the receiver end. The received signal is demodulated as well as converted again from analog to digital. The signal gets reconstructed here.

Channel Decoder

The channel decoder, after detecting the sequence, does some error corrections. The distortions which might occur during the transmission, are corrected by adding some redundant bits. This addition of bits helps in the complete recovery of the original signal.

Source Decoder

The resultant signal is once again digitized by sampling and quantizing so that the pure digital output is obtained without the loss of information. The source decoder recreates the source output.

Output Transducer

This is the last block which converts the signal into the original physical form, which was at the input of the transmitter. It converts the electrical signal into physical output (**Example**: loud speaker).

Output Signal

This is the output which is produced after the whole process. **Example**: The sound signal received. This unit has dealt with the introduction, the digitization of signals, the advantages and the elements of digital communications. In the coming chapters, we will learn about the concepts of Digital communications, in detail.

Transmission Media:

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to move from one point to another (from sender to receiver). Electromagnetic energy (includes electrical and magnetic fields) consists of power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication (Networks OSI Seven layer) model is dedicated to the transmission media, we will study the OSI Model later.

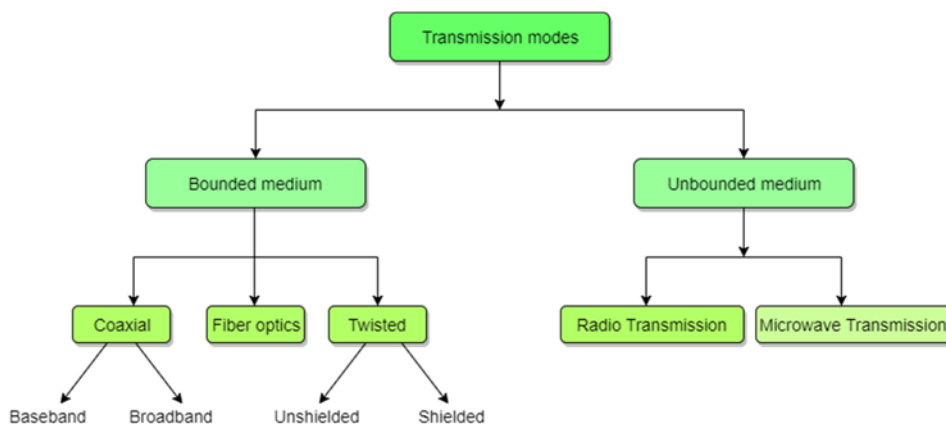


Fig: Types of transmission media

Factors to be considered while selecting a Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances

Bounded or 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 travelling 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.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points:

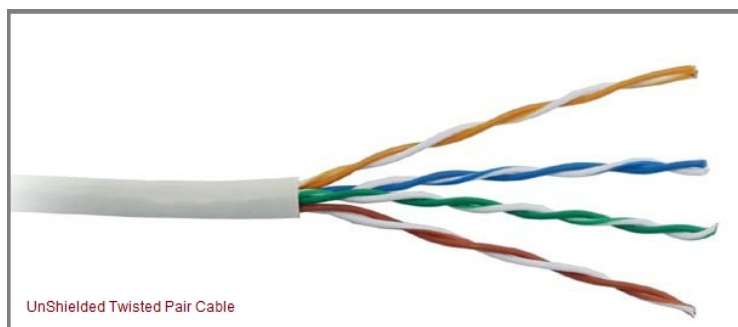
- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km@1kHz.
- Typical delay is 50 μ s/km.
- Repeater spacing is 2km.

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as 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. This results in a difference at the receiver.

Twisted Pair is of two types

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

Unshielded Twisted Pair Cable



It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own color plastic insulator. Identification is the reason behind colored plastic insulation. UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.

Advantages of Unshielded Twisted Pair Cable

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100-meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

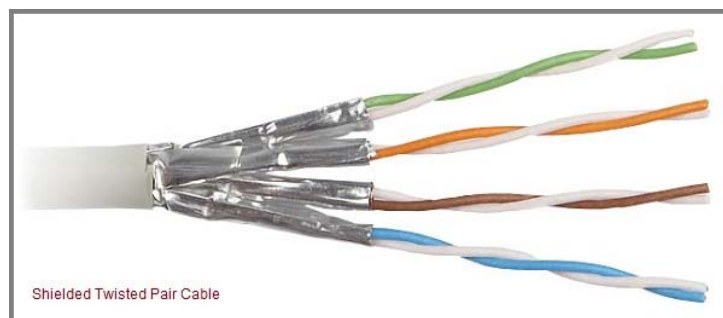
Disadvantages of Unshielded Twisted Pair Cable

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.



Advantages of Shielded Twisted Pair Cable

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signaling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of Shielded Twisted Pair Cable

- Difficult to manufacture
- Heavy

Performance of Shielded Twisted Pair Cable

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. As shown in the below figure, a twisted-pair cable can pass a wide range of frequencies. However, with increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100kHz. Note that gauge is a measure of the thickness of the wire.

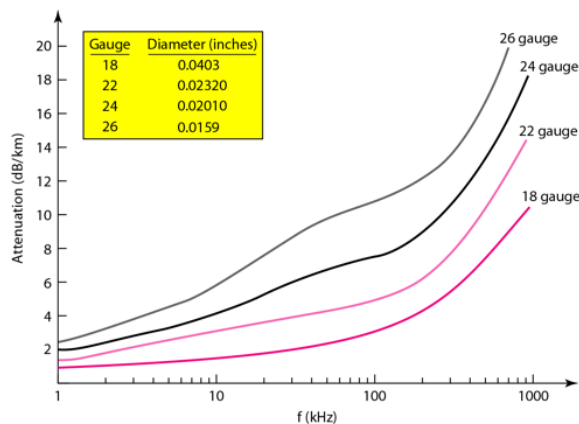


Fig: Performance graph of Shielded Twisted Pair Cable

Applications of Shielded Twisted Pair Cable

- In telephone lines to provide voice and data channels. The DSL lines that are

used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

- Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as center conductor which can be a solid wire or a standard one. It is surrounded by PVC insulation, a sheath which is encased in an outer conductor of metal foil, braid or both. Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here are the most common coaxial standards.

- 50-Ohm RG-7 or RG-11: used with thick Ethernet.
- 50-Ohm RG-58: used with thin Ethernet
- 75-Ohm RG-59: used with cable television
- 93-Ohm RG-62: used with ARCNET.

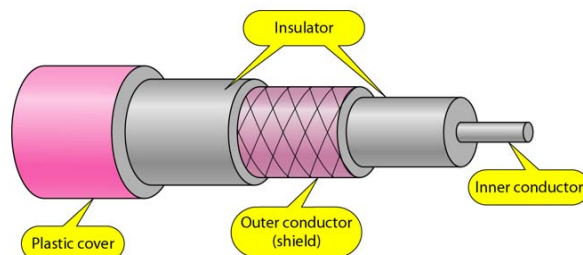


Fig: Coaxial Cable

Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector. The below figure shows 3 popular types of these connectors: the BNC Connector, the BNC T connector and the BNC terminator.

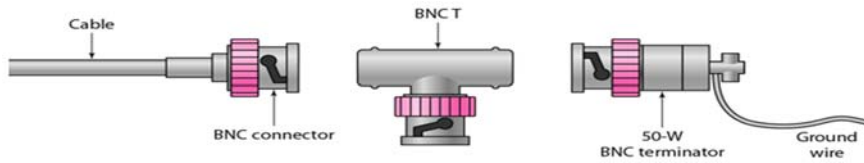


Fig: Coaxial cable connectors

The BNC connector is used to connect the end of the cable to the device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

There are two types of Coaxial cables

1. Baseband

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

2. Broadband

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signals using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages of Coaxial Cable

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages of Coaxial Cable

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Performance of Coaxial Cable

We can measure the performance of a coaxial cable in same way as that of Twisted Pair Cables. From the below figure, it can be seen that the attenuation is much higher in coaxial cable than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

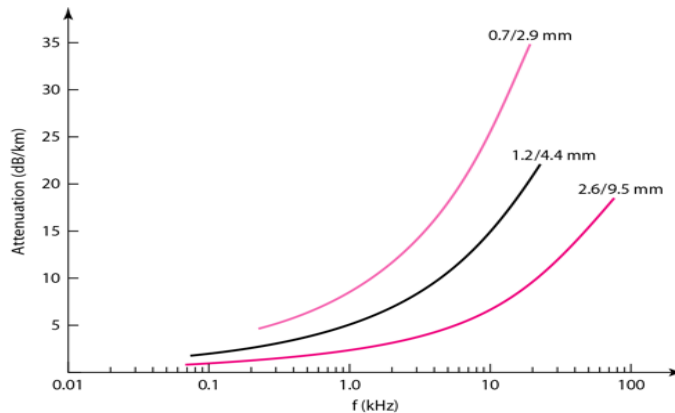


Fig: Performance graph of Coaxial Cable

Applications of Coaxial Cable

- Coaxial cable was widely used in analog telephone networks, where a single coaxial network could carry 10,000 voice signals.
- Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Cable TV uses RG-59 coaxial cable.
- In traditional Ethernet LANs, because of its high bandwidth, and consequence high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10Mbps with a range of 185 m.

Fiber Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. For better understanding we first need to explore several aspects of the **nature of light**.

Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction.

The below figure shows how a ray of light changes direction when going from a denser to a less dense substance.

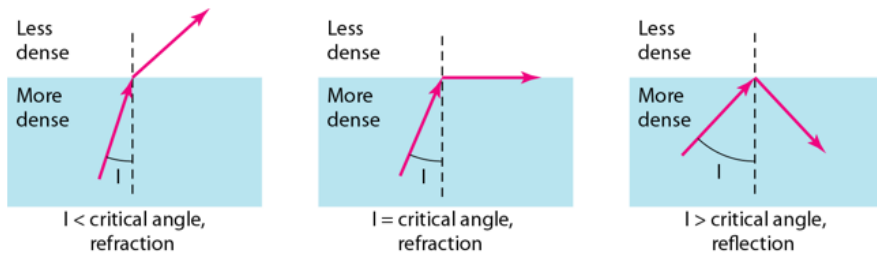


Fig: Light changes direction

Bending of a light ray

As the figure shows:

- If the **angle of incidence I** (the angle the ray makes with the line perpendicular to the interface between the two substances) is **less** than the **critical angle**, the ray **refracts** and moves closer to the surface.
- If the angle of incidence is **greater** than the critical angle, the ray **reflects** (makes a turn) and travels again in the denser substance.
- If the angle of incidence is **equal** to the critical angle, the ray refracts and **moves parallel** to the surface as shown.

Note: The critical angle is a property of the substance, and its value differs from one substance to another.

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

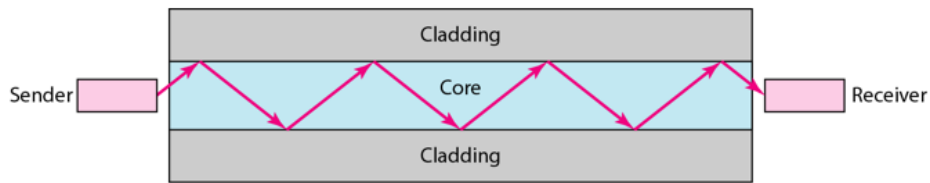
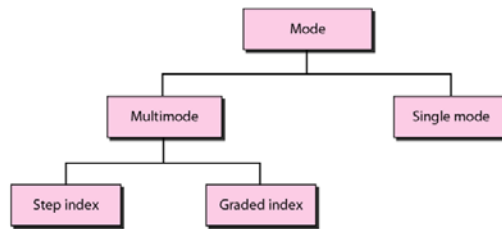


Fig: Internal view of an Optical fiber

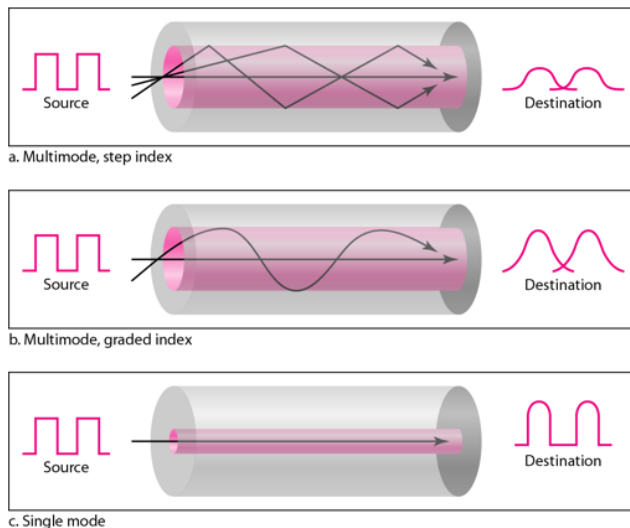
Propagation Modes of Fiber Optic Cable

Current technology supports two modes (**Multimode** and **Single mode**) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: **Step-index** and **Graded-index**.



Multimode Propagation Mode

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core as shown in the below figure.



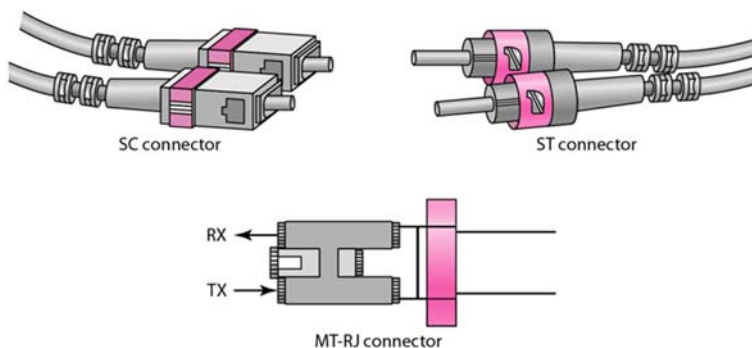
- In **multimode step-index fiber**, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. The term step-index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.
- In **multimode graded-index fiber**, this distortion gets decreases through the cable. The word index here refers to the index of refraction. This index of refraction is related to the density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.

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, and with substantially lower density. The decrease in density results in a critical angle that is close enough to 90 degrees to make the propagation of beams almost horizontal.

Fiber Optic Cable Connectors

There are three types of connectors for fiber-optic cables, as shown in the figure below.



The **Subscriber Channel(SC)** connector is used for cable TV. It uses push/pull locking system. The **Straight-Tip(ST)** connector is used for connecting cable to the networking devices. MT-RJ is a connector that is the same size as RJ45.

Advantages of fiber Optic Cable

Fiber optic has several advantages over metallic cable:

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

Disadvantages of fiber Optic Cable

There are some disadvantages in the use of optical fiber:

- Installation and maintenance
- Unidirectional light propagation
- High Cost

Performance of fiber Optic Cable

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer (actually one tenth as many) repeaters when we use the fiber-optic cable.

Applications of fiber Optic Cable

- Often found in backbone networks because its wide bandwidth is cost-effective.
- Some cable TV companies use a combination of optical fiber and coaxial cable thus creating a hybrid network.
- Local-area Networks such as 100Base-FX network and 1000Base-X also use fiber-optic cable.

Unbounded or Unguided Transmission Media

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.

The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

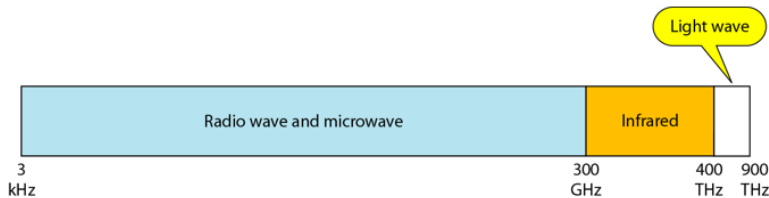
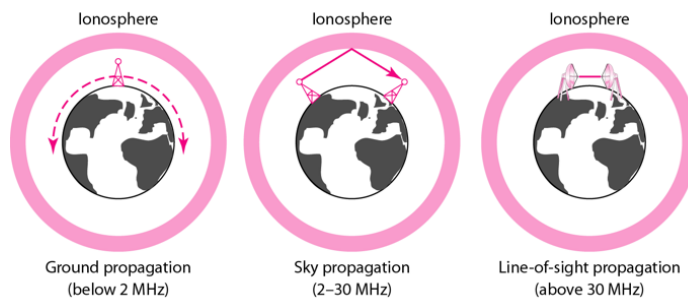


Fig: Electromagnetic Spectrum

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 below figure.



Propagation Modes

- **Ground Propagation:** In this, 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.
- **Sky Propagation:** In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.
- **Line-of-sight Propagation:** in this type, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

We can divide wireless transmission into three broad groups:

- Radio waves
- Micro waves

- Infrared waves

Radio Waves

Electromagnetic waves ranging in frequencies between 3kHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Omnidirectional Antenna for Radio Waves

Radio waves use omnidirectional antennas that send out signals in all directions.



Fig: Radio Wave Antena

Applications of Radio Waves

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

Micro Waves

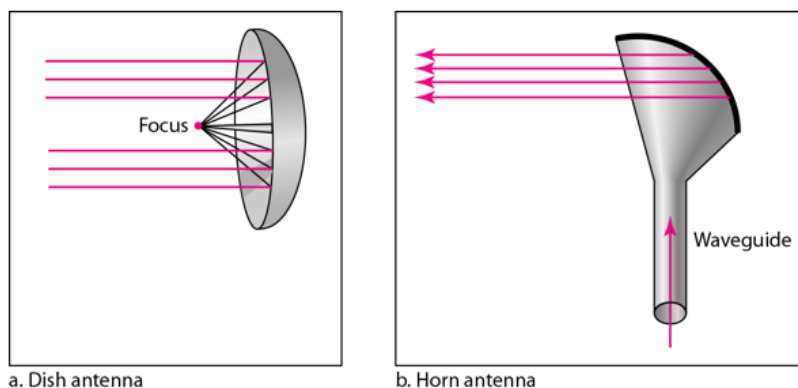
Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

The following describes some characteristics of microwaves propagation:

- 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.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna for Micro Waves

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: **Parabolic Dish** and **Horn**.



A parabolic antenna works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications of Micro Waves

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.

There are 2 types of Microwave Transmission:

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

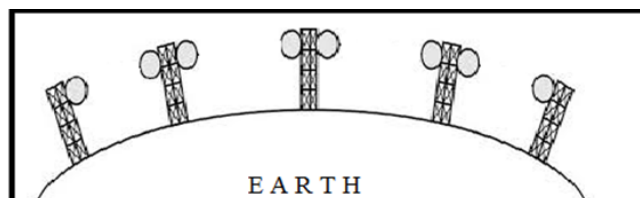
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is very costly

Terrestrial Microwave

For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna. The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world

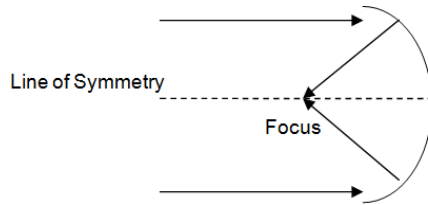


There are **two types of antennas** used for terrestrial microwave communication:

1. Parabolic Dish Antenna

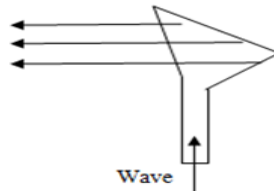
In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on

geometry of parabola.



2. Horn Antenna

It is like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 36000 Km above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geosynchronous orbit, it is stationary relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.

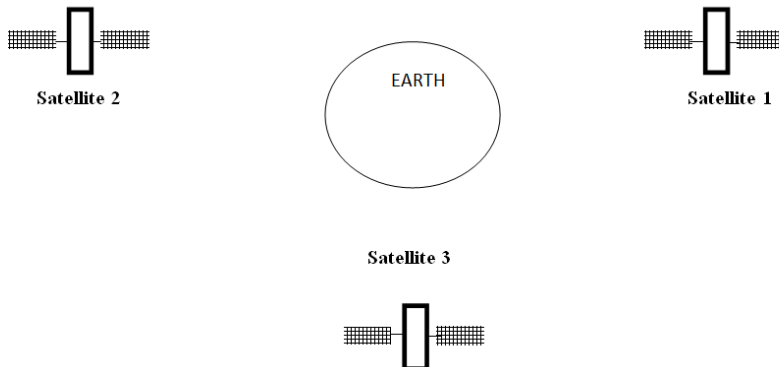


Fig: Satellite above earth surface

Features of Satellite Microwave

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

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.

When we use infrared remote control, we do not interfere with the use of the remote by our neighbors. 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.

Applications of Infrared Waves

- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for

communication between devices such as keyboards, mouse, PCs and printers.

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Transmission Modes:

Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode: -

- Simplex-Mode
- Half-Duplex Mode
- Full-Duplex Mode

Simplex Mode

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

Example: Keyboard, Television, Radio and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.

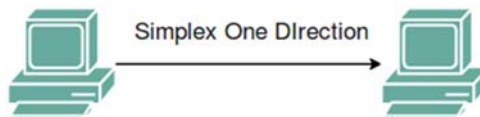


Fig: Simplex mode

Half-Duplex Mode

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. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

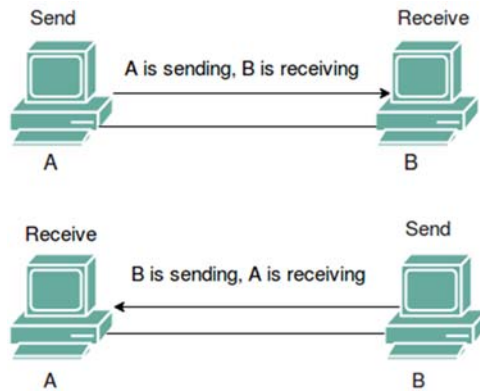


Fig: Half Duplex

Full-Duplex Mode

In full-duplex mode, 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 other direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and other for receiving Or the capacity is divided between signals travelling in both directions.
- Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two directions.

Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

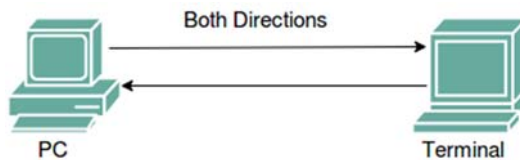


Fig: Full Duplex

Unit: 2

Multiplexing and Switching

Objectives

- To identify different multiplexing techniques.
- To elaborate different types of switching techniques.

Learning Process and support material

- Class demonstration with chart paper drawings.
- Case Study

Content's Elaboration

Multiplexing

In general, a medium can carry only one signal at any moment in time. For multiple signals to share one medium, the medium must somehow be divided, giving each signal a portion of the total bandwidth. Multiplexing (also known as MUX-ing) is a method by which multiple analog message signals or digital data streams are combined into one signal over a shared medium. The basic aim of the Multiplexing is to share an expensive resource by putting-up multiple signals on the same channel. For example, in telecommunications, several telephone calls may be carried using one wire. Multiplexing originated in telegraphy in the 1870s and is now widely applied in different streams of communications. When several communication channels are needed between the same two points, significant economies may be realized by sending all the messages on one transmission facility – called multiplexing. As shown in Figure, 'n' number of signals from the low speed channels have been combined to one high speed link using a n:1 multiplexer. Whereas the opposite process is carried out at the other end, where the signals are further separated into n number of low speed channels. This opposite process is referred as demultiplexing.



Fig: Multiplexing and De-Multiplexing

Thus, Multiplexing refers to the ability to transmit data coming from several pairs of equipment (transmitters and receivers) called low-speed channels on a single physical medium (called the high-speed channel). Whereas, a multiplexer is the multiplexing device that combines the signals from the different transmitters and sends them over the high-speed channel. A demultiplexer is the device which separates signal received from a high-speed channel into different signal and sends them to receivers. There are four basic multiplexing techniques:

- Frequency division multiplexing (FDM)
- Time division Multiplexing (TDM)
- Code division Multiplexing (CDM)
- Space-division Multiplexing (SDM)
- Frequency division Multiplexing: Bandwidth is divided into different smaller frequency bands (range)
- Time division Multiplexing (TDM) (Time slots are allocated to message signals in non-overlapping manner in the time domain so that individual messages can be recovered from time synchronized switches)
- Quadrature Carrier/amplitude Multiplexing (QAM): Two message signals are transmitted in the same frequency band. The recovery is possible due to the carrier signals being orthogonal) High Speed Link n-Channels (Low Speed Channels) n-Channels (Low Speed Channels) ` 43 Multiplexing and Switching
- Code division Multiplexing (CDM) users occupy the same frequency band but modulate their messages with different codes TDMA FDMA CDMA when used for multiple access TDMA, FDMA, e.g., GSM, FM, AM, Wireless network.

Frequency-division multiplexing

Frequency division multiplexing (FDM) is the technique used to divide the available bandwidth into a number of smaller independent logical channels with each channel having a small bandwidth. The method of using a number of carrier frequencies each of which is modulated by an independent speech signal is in fact frequency division multiplexing. The following Figure depicts the basic process of frequency division multiplexing, in which the total bandwidth has been divided into n-number of different channels and each one of them working with a specific bandwidth. The following figure 2 depicts how three voice-grade telephone channels are multiplexed using FDM. When many channels are multiplexed together, 4000Hz is allocated to each channel to keep them well separated. First the voice channels are raised in frequency, each by a different amount. Then they can be combined, because no two channels can occupy the same portion of the spectrum. Notice that even though there are gaps (guard bands) between the channels, there is some overlap between adjacent channels, because the filters do not have sharp edges. This overlap means that a strong spike at the edge of one channel will be felt in the adjacent one as non-thermal noise.

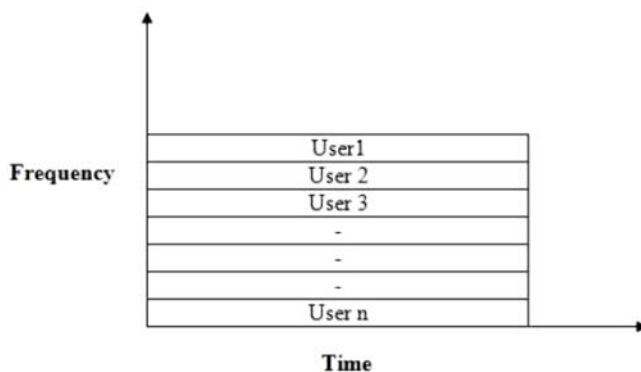


Fig: FDM

In the telecommunication technology, the total bandwidth available in a communication medium is divided into a series of non-overlapping frequencies sub bands using the frequency division multiplexing. Each one of these sub-bands then carries a separate signal. This allows a single transmission medium such as a cable or optical fiber to be shared by many signals.

An example of a system using FDM is cable television, in which many television channels are carried simultaneously on a single cable. FDM is also used by telephone systems to transmit multiple telephone calls through high capacity trunk lines, communications satellites to transmit multiple channels of data on uplink and downlink radio beams, and broadband DSL modems to transmit large amounts of computer data through twisted pairs telephone lines, among many other uses. Frequency-division multiplexing works best with low-speed devices. The frequency division multiplexing schemes used around the world are very standardized. A wide spread standard is 12, 4000-Hz each voice channels (3000Hz for user, plus two guard bands of 500Hz each) multiplexed into the 60 to 108 kHz band. Many carriers offer a 48 to 56 kbps leased line service to customers, based on the group. The frequency band division has been illustrated in the Figure taking some example frequencies.

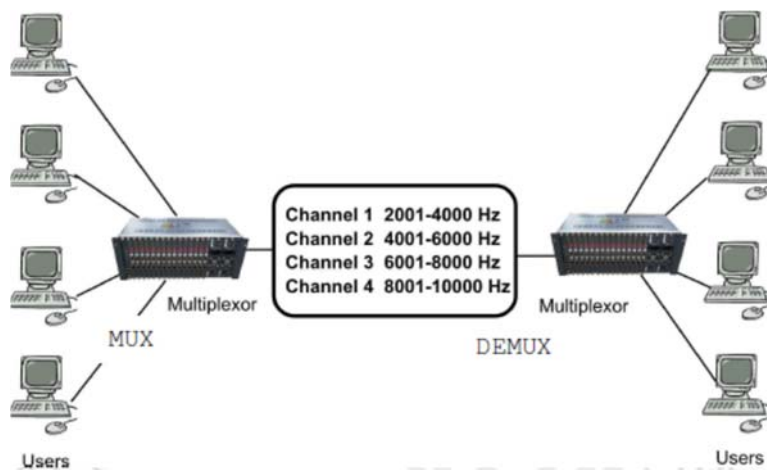


Fig:Illustration of FDM using four different channels.

In Telephony, the most widely used method of modulation in FDM is single sideband modulation, which, in the case of voice signals, requires a bandwidth that is approximately equal to that of the original voice signal. Each voice input is usually assigned a bandwidth of 4 KHz. The bandpass filters following the modulators are used to restrict the band of each modulated signal to its prescribed range. The resulting bandpass filter outputs are combined in parallel to form the input to the common channel. At the receiving terminal, a bank of band pass filters,

with their inputs connected in parallel, is used to separate the message signals on a frequencyoccupancy basis. The original message signals are recovered by individual demodulators Frequency division multiplexing (FDM) is also referred as the Wavelength division multiplexing (WDM),where we are using the optical communications focusing on the wavelength rather than the frequency.

Advantages of FDM

1. The users can be added to the system by simply adding another pair of transmitter modulator and receiver demodulators.
2. FDM system support full duplex information (Both side simultaneous Communication) flow which is required by most of application.

Disadvantages of FDM

1. In FDM system, the initial cost is high. This may include the cable between the two ends and the associated connectors for the cable.
2. A problem with one user can sometimes affect the others.
3. Each user requires a precise carrier frequency for transmission of the signals.

Time-division multiplexing

Time Division Multiplexing (TDM) is another popular method of utilizing the capacity of a physical channel effectively. Each user of the channel is allotted a small time interval during which it may transmit a message. Thus, the total time available in the channel is divided and each user is allocated a time slot. Data from each user is multiplexed into a frame which is transmitted over the channel. In TDM, user's messages are buffered as they received and read from the buffer during its time slot to make a frame. Therefore, each user can use the full channel bandwidth. The channel capacity is fully utilized in TDM by interleaving a number of messages belonging to different users into one long message. This message sent through the physical channel must be separated at the receiving end. Individual chunks of message sent by each user should be reassembled into a full message. The process of the Time division multiplexing has been shown in Figure.

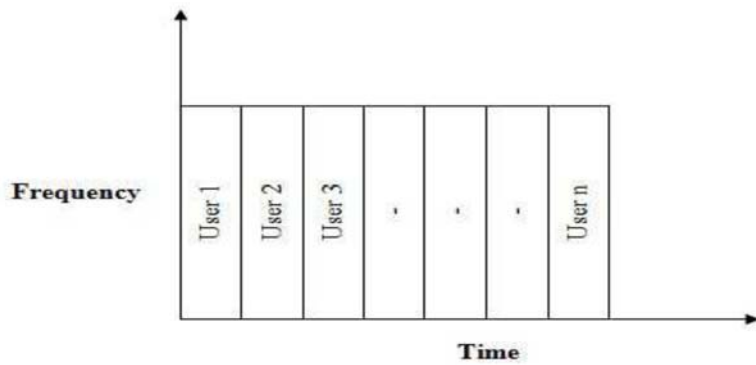


Fig: Time Division Multiplexing

Sharing of the signal is accomplished by dividing available transmission time on a medium among users. For example, in some countries, the individual stations have two logical sub channels: music and advertising. These two alternates in time on the same frequency first a burst of music, then a burst of advertising, then more music and so on. This situation is time division multiplexing. Unfortunately, TDM can only be used for digital data multiplexing. Since local loops produce analog signals, a conversion is needed from analog to digital in the end office. Where all the individual local loops come together to be combined onto outgoing trucks. The TDM process is further illustrated in Figure with the digital data stream.

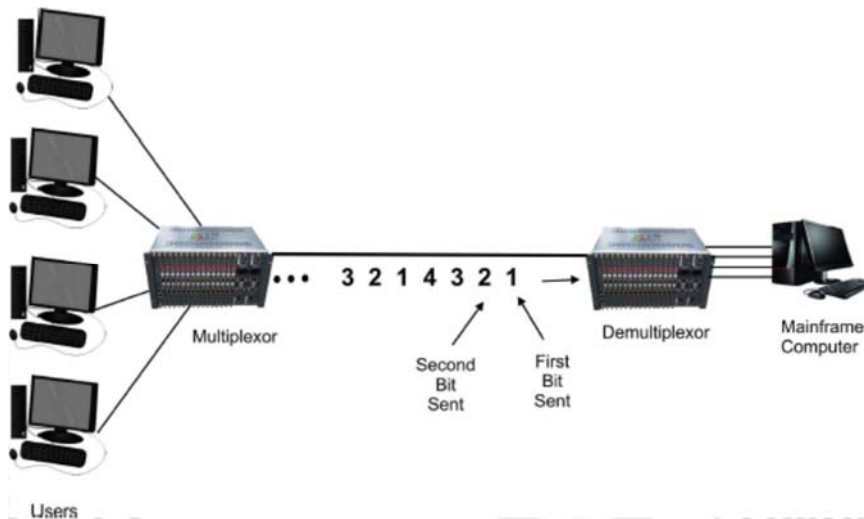


Fig:Digital Transmission using TDM

Applications of TDM

- The PDH (Plesiochronous Digital Hierarchy) system, also known as the PCM (Pulse Code Modulation) systems
- The synchronous digital hierarchy (SDH) / synchronous optical networking (SONET) network transmission standards.
- TDM can be further extended into the time division multiple Channel (TDMA) scheme, where several stations connected to the same physical medium, for example sharing the same frequency channel, can communicate. Application examples include the widely used GSM telephone system

Advantages of TDM

1. It uses a single link
2. It does not require precise carrier matching at both end of the links.
3. Use of the channel capacity is high.
4. Ease to expand the number of users on a system at a low cost.
5. There is no need to include identification of the traffic stream on each packet.

Disadvantages of TDM

1. The sensitivity to other user is very high and causes problems
2. Initial cost is high
3. Technical complexity is more

Space division multiplexing

When we want to transmit multiple messages through any of the communication media, the ultimate goal is to maximize the use of the given resources (e.g. time and frequency in general). It involves grouping many separate wires into a common cable enclosure. A cable that has, for example, 50 twisted pairs inside it can support 50 channels. SDM has the unique advantage of not requiring any multiplexing equipment. It is usually combined with other multiplexing techniques to better utilize the individual physical channels. For example, if there are six persons in the office and all of them want to talk at the same time, this will give rise to interference between the conversations. To reduce the interference, they may divide themselves into three groups of two, such that the conversation is between each pair of people.

If the pairs continue talking while sitting next to each other, the interference would still be present. The best way for each pair to converse with minimal interference would be to sit a few feet away from the other pairs (within the same room) and converse. They would still be sharing the same medium for their conversations but the physical space in the room would be divided for each conversation. This is the simplest example of Space Division Multiplexing. The concept of SDM has been illustrated in Figure

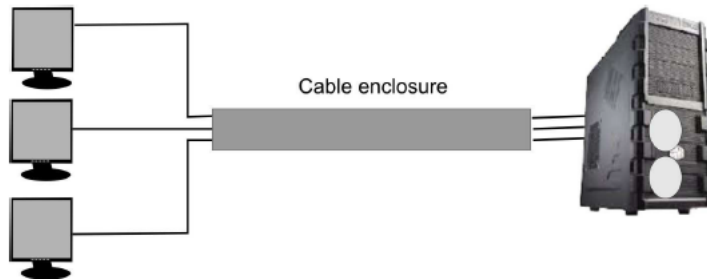


Fig:Space Division Multiplexing

Space Division Multiplexing is the multiplexing technique in which both the time and frequency can be reused by transmitting our information through a parallel set of channels. In wired communication, space-division multiplexing simply implies different point to-point wires for different channels. Examples include an analogue stereo audio cable, with one pair of wires for the left channel and another for the right channel, and a multi pair telephone cable usually employed to provide PSTN connections in different homes. Another example is a switched star network such as the analog telephone access network (although inside the telephone exchange or between the exchanges, other multiplexing techniques are typically employed). In wireless communication, space-division multiplexing is achieved by multiple antenna elements forming a phased array antenna. Examples are multiple-input and multiple-output (MIMO), single-input and multiple-output (SIMO) and multiple-input and single output (MISO) multiplexing

Wavelength Division Multiplexing (WDM)

Wavelength division multiplexing (WDM) is a technology or technique modulating numerous data streams, i.e. optical carrier signals of varying wavelengths (colors) of laser light, onto a single optical fiber. WDM enables bi-directional

communication as well as multiplication of signal capacity. WDM is actually frequency division multiplexing (FDM) but referencing the wavelength of light as opposed to the frequency of light. However, since wavelength and frequency have an inverse relationship (shorter wavelength means higher frequency), the WDM and FDM terms actually describe the same technology – light in optical cable used to carry data and communication signals.

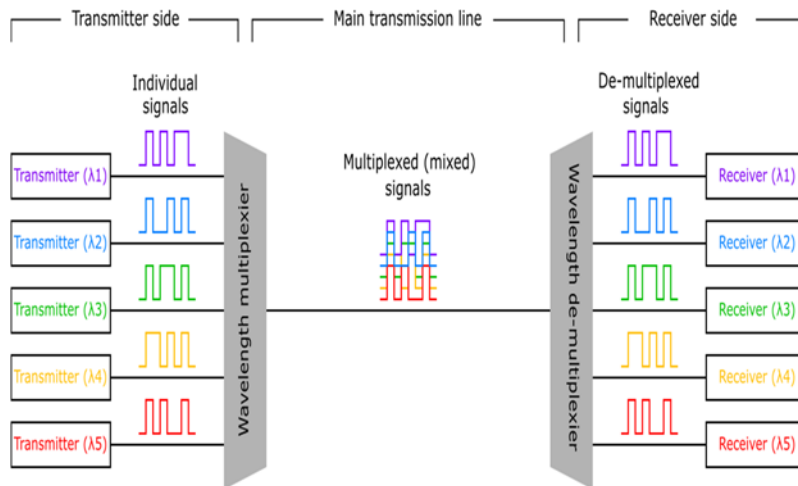


Fig: Wavelength Division Multiplexing

Typical WDM systems use single-mode optical fiber (SMF); this is optical fiber for only a single ray of light and having a core diameter of 9 millionths of a meter (9 μm). Other systems with multi-mode fiber cables (MM Fiber; also called premises cables) have core diameters of about 50 μm . Standardization and extensive research have brought down system costs significantly.

WDM systems are divided according to wavelength categories, generally coarse WDM (CWDM) and dense WDM (DWDM). CWDM operates with 8 channels (i.e., 8 fiber optic cables) in what is known as the “C-Band” or “erbium window” with wavelengths about 1550 nm (nanometers or billionths of a meter, i.e. 1550×10^{-9} meters). DWDM also operates in the C-Band but with 40 channels at 100 GHz spacing or 80 channels at 50 GHz spacing. Even newer technology, called Raman amplification, is using light in the L-Band (1565 nm to 1625 nm), approximately doubling these capacities.

Message Switching

Switched communication networks are those in which data transferred from source to destination is routed between various intermediate nodes. Switching is the technique by which nodes control or switch data to transmit it between specific points on a network. There are 3 common switching techniques

1. Circuit Switching
2. Packet Switching
3. Message Switching

Switching

Message switching was a technique developed as an alternate to circuit switching, before packet switching was introduced. In message switching, end users communicate by sending and receiving *messages* that included the entire data to be shared. Messages are the smallest individual unit. Also, the sender and receiver are not directly connected. There are a number of intermediate nodes transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems.

They provide two distinct and important characteristics

1. **Store and forward**– The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise it'll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.
2. **Message delivery** – This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.

Message switching network consists of transmission links (channels), store-and-forward switch nodes and end stations as shown in the following picture:

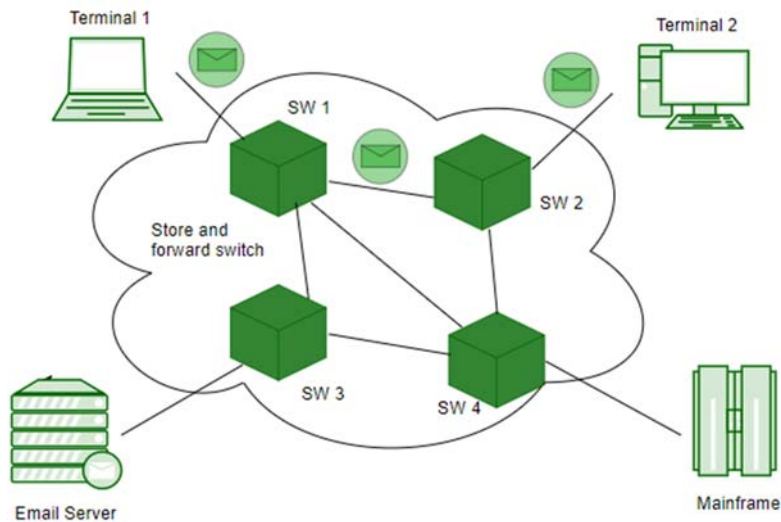


Fig: Message Delivery

Characteristics of message switching

Message switching is advantageous as it enables efficient usage of network resources. Also, because of the store-and-forward capability of intermediary nodes, traffic can be efficiently regulated and controlled. Message delivery as one unit, rather than in pieces, is another benefit.

However, message switching has certain disadvantages as well. Since messages are stored indefinitely at each intermediate node, switches require large storage capacity. Also, these are pretty slow. This is because at each node, first there is wait till the entire message is received, then it must be stored and transmitted after processing the next node and links to it depending on availability and channel traffic.

Hence, message switching cannot be used for real time or interactive applications like video conference.

Applications

The store-and-forward method was implemented in telegraph message switching centers. Today, although many major networks and systems are packet-switched or circuit switched networks, their delivery processes can be based on message switching. For example, in most electronic mail systems the delivery process is

based on message switching, while the network is in fact either circuit-switched or packet-switched.

Packet switching

Packet switching is a method of transferring the data to a network in a form of packets. In order to transfer the file fast and efficient manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**. At the destination, all these small-parts (packets) have to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed.

Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first stores that packet then forwards. This technique is very beneficial because packets may get discarded at any hop due to some reasons. More than one path is possible between a pair of source and destination. Each packet contains source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some paths, packets are allowed to choose different paths possible over existing network.

Packet-Switched networks were designed to overcome the *weaknesses* of Circuit-Switched networks since circuit-switched networks are not very effective for small messages.

Advantage of Packet Switching

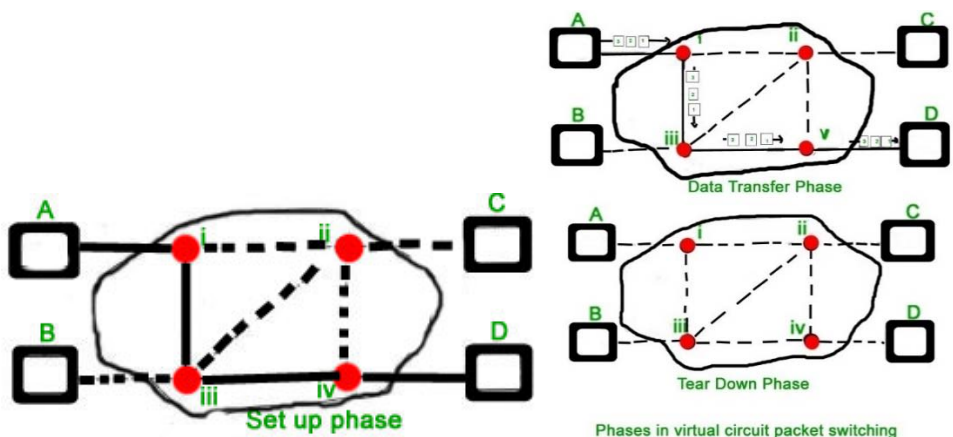
- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as destination can detect the missing packet.
- More fault tolerant because packets may follow different path in case any link is down, Unlike Circuit Switching.
- Cost effective and comparatively cheaper to implement.

Disadvantage of Packet Switching

- Packet Switching don't give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers to each packet.
- Complexity is more at each node because of the facility to follow multiple path.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bulky data (large messages) Circuit Switching is better.

Modes of Packet Switching:

1. **Connection-oriented Packet Switching (Virtual Circuit):-** Before starting the transmission, it establishes a logical path or virtual connection using signaling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence number. Overall, three phases take place here- Setup, data transfer and tear down phase.

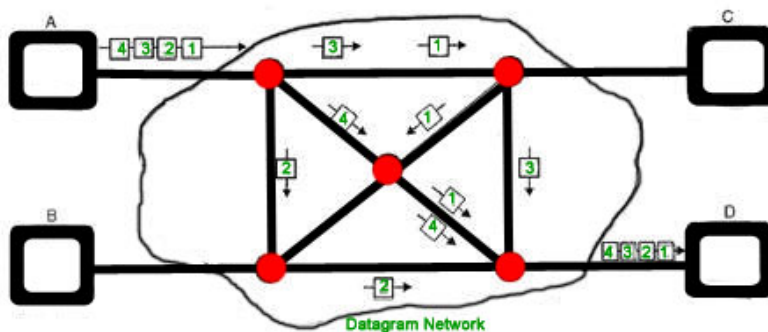


All address information is only transferred during setup phase. Once the route to destination is discovered, entry is added to switching table of each intermediate

node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number etc.

Connection-oriented switching is very useful in switched WAN. Some popular protocols which use Virtual Circuit Switching approach are X.25, Frame-Relay, ATM and MPLS (Multi-Protocol Label Switching).

1. **Connectionless Packet Switching (Datagram):** Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.
2. Packet delivery is not guaranteed in connectionless packet switching, so the reliable delivery must be provided by end systems using additional protocols.



Datagram Packet Switching

Delays in Packet switching:

1. Transmission Delay
2. Propagation Delay
3. Queuing Delay
4. Processing Delay

Transmission Delay

Time taken to put a packet onto link. In other words, it is simply time required to put data bits on the wire/communication medium. It depends on length of packet and bandwidth of network.

$$\text{Transmission Delay} = \text{Data size} / \text{bandwidth} = (L/B) \text{ second}$$

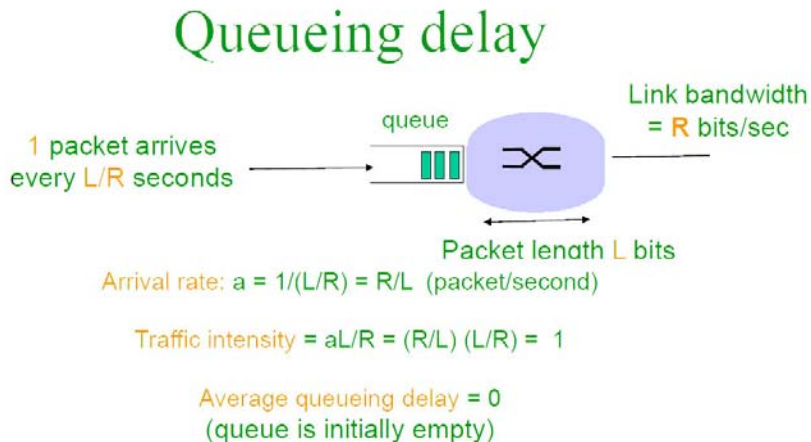
Propagation delay:

Time taken by the first bit to travel from sender to receiver end of the link. In other words, it is simply the time required for bits to reach the destination from the start point. Factors on which Propagation delay depends are Distance and propagation speed.

$$\text{Propagation delay} = \text{distance}/\text{transmission speed} = d/s$$

Queuing Delay:

Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time difference between when the packet arrived Destination and when the packet data was processed or executed. It may be caused by mainly three reasons i.e. originating switches, intermediate switches or call receiver servicing switches.



$$\text{Average Queuing delay} = (N-1)L/(2*R)$$

where N = no. of packets

L = size of packet

R=bandwidth

Processing Delay:

Processing delay is the time it takes routers to process the packet header. Processing of packets helps in detecting bit-level errors that occur during transmission of a packet to the destination. Processing delays in high-speed routers are typically on the order of microseconds or less. In simple words, it is just the time taken to process packets.

Circuit Switching

In circuit switching network resources (bandwidth) is divided into pieces and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established. Telephone system network is the one of example of Circuit switching.

Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM) are two methods of multiplexing multiple signals into a single carrier.

- **Frequency Division Multiplexing:** *Divides into multiple bands*

Frequency Division Multiplexing or FDM is used when multiple data signals are combined for simultaneous transmission via a shared communication medium. It is a technique by which the total bandwidth is divided into a series of non-overlapping frequency sub-bands, where each sub-band carry different signal. Practical use in radio spectrum & optical fiber to share multiple independent signals.

- **Time Division Multiplexing:** *Divides into frames*

Time-division multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line. TDM is used for long-distance communication links and bears heavy data traffic loads from end user. Time division multiplexing (TDM) is also known as a digital circuit switched.

Unit: 3

Modulation Scheme

Objective

To Illustrate AM and FM modulation schemes with suitable circuit diagrams

Learning Process and Study Materials

- Class demonstration and practical
- Question/Answer
- Group discussion

Content's Elaboration

Modulation

A message carrying a signal has to get transmitted over a distance and for it to establish a reliable communication, it needs to take the help of a high frequency signal which should not affect the original characteristics of the message signal. The characteristics of the message signal, if changed, the message contained in it also alters. Hence, it is a must to take care of the message signal. A high frequency signal can travel up to a longer distance, without getting affected by external disturbances. We take the help of such high frequency signal which is called as a **carrier signal** to transmit our message signal. Such a process is simply called as Modulation. Modulation is the process of changing the parameters of the carrier signal, in accordance with the instantaneous values of the modulating signal.

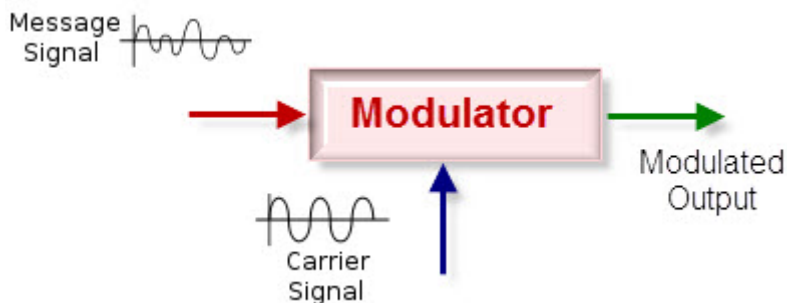


Fig: Modulation Process

Need for Modulation

Baseband signals are incompatible for direct transmission. For such a signal, to travel longer distances, its strength has to be increased by modulating with a high frequency carrier wave, which doesn't affect the parameters of the modulating signal.

Advantages of Modulation

The antenna used for transmission, had to be very large, if modulation was not introduced. The range of communication gets limited as the wave cannot travel a distance without getting distorted. Following are some of the advantages for implementing modulation in the communication systems.

- Reduction of antenna size
- No signal mixing
- Increased communication range
- Multiplexing of signals
- Possibility of bandwidth adjustments
- Improved reception quality

Analog Modulation:

$$A_c \cos(2\pi f_c t + \phi)$$

The diagram shows the equation $A_c \cos(2\pi f_c t + \phi)$ with three red arrows pointing to its components: 'Amplitude' points to A_c , 'Frequency' points to $2\pi f_c$, and 'Phase' points to ϕ . A large black curly bracket underneath the $2\pi f_c t + \phi$ term is labeled 'Angle' with the text '(Frequency = Rate of Change of Angle)' below it.

Analog Modulation

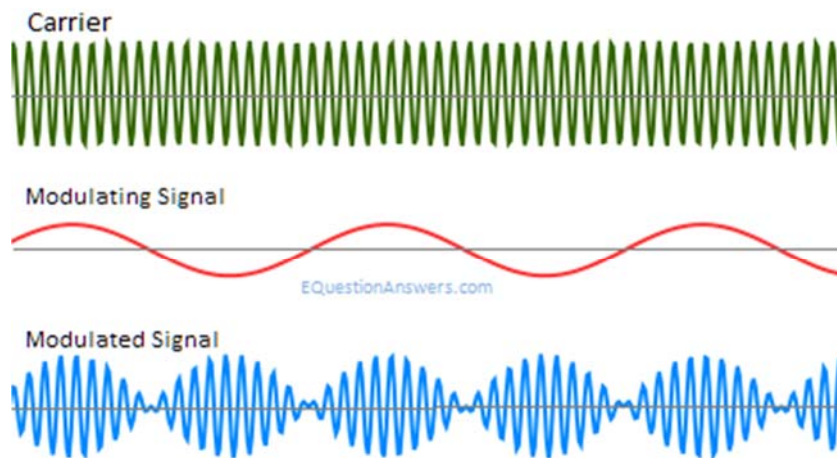
In this modulation, a continuously varying sine wave is used as a carrier wave that modulates the message signal or data signal. The Sinusoidal wave's general function is shown in the figure below, in which, three parameters can be altered to get modulation – they are amplitude, frequency and phase, so the types of analog modulation are:

- Amplitude modulation (AM)

- Frequency modulation (FM)
- Phase modulation (PM)

Amplitude Modulation

In **amplitude modulation**, the amplitude of the carrier wave is varied in proportion to the message signal, and the other factors like frequency and phase remain constant. The modulated signal is shown in the below figure, and its spectrum consists of lower frequency band, upper frequency band and carrier frequency components. This type of modulation requires greater band width, more power. Filtering is very difficult in this modulation.



Amplitude Modulation

Fig: AM Modulation

Frequency Modulation:

Frequency modulation (FM) varies the frequency of the carrier in proportion to the message or data signal while maintaining other parameters constant. The advantage of FM over AM is the greater suppression of noise at the expense of bandwidth in FM. It is used in applications like radio, radar, telemetry seismic prospecting, and so on. The efficiency and bandwidths depend on modulation index and maximum modulating frequency.

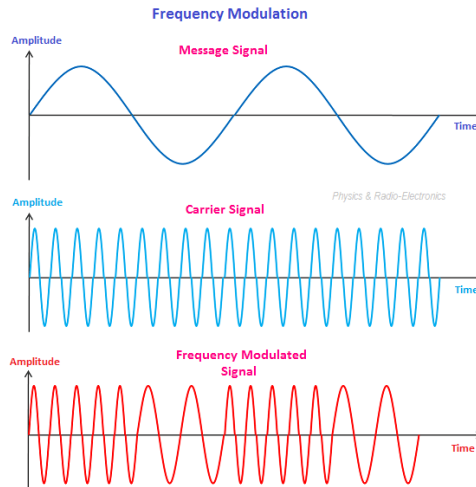


Fig: Frequency Modulation

Phase Modulation:

In **phase modulation**, the carrier phase is varied in accordance with the data signal. In this type of modulation, when the phase is changed it also affects the frequency, so this modulation also comes under frequency modulation.

Analog modulation (AM, FM and PM) is more sensitive to noise. If noise enters into a system, it persists and gets carried till the end receiver. Therefore, this drawback can be overcome by the digital modulation technique.

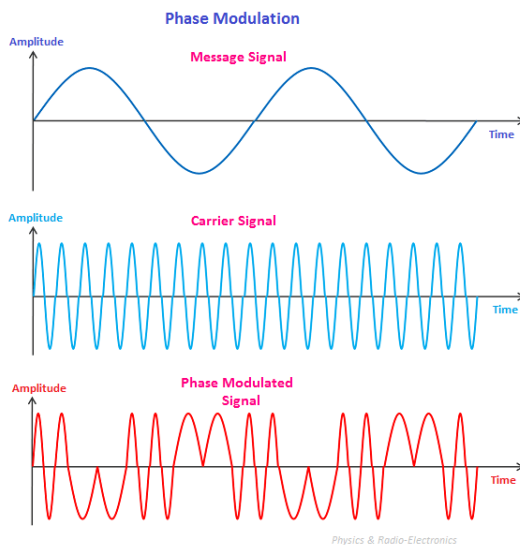


Fig: Phase Modulation

Unit: 4

Computer Network and Topology

Objective

- To identify different types of network architecture and their applications.
- To identify different types of network topologies and their applications

Learning Process and Study Materials

- Class demonstration and practical
- Field Visit
- Project work

Content's Elaboration

Computer Network

A system of interconnected computers and computerized peripherals such as printers is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

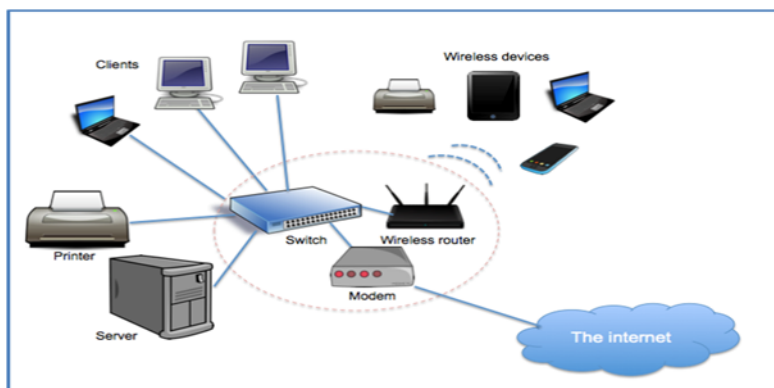


Fig: Computer Network

Advantages of computer network

Every technology and system provide merits and demerits. Similarly, computer network also possesses, several advantages and few disadvantages. Some of them are discussed below.

- **Resource sharing**

Resource sharing is the main advantage of the computer network. The goal is to provide all the programs, data and hardware to everyone on the network without regard to the physical location of the resource and the users.

- **Inexpensive system**

Installing networking software on the device would not cost too much, as it is assured that it lasts and can effectively share information to the peers. Also, there is no need to change the software regularly, as mostly it is not required to do so.

- **Powerful communication medium**

Computer network helps people who live or work apart to report together. So, when one user prepared some documentation, he can make the document online enabling other to read and convey their opinions.

- **Increases system security**

Only authorized user can access resource in a computer network. Users are authenticated by their user name and password. Hence it is not possible to access the data unauthorized persons.

- **Storage Capacity**

Computer network is used to share information, files and resources to other people and ensures that all data and content are properly stored in the system. With the help of computer technology, we can do all of this without any problem, while having all the space we need for storage.

Disadvantages of Computer Networking

1. It lacks independence

Computer networking involves a process that is operated using computers, so people will be relying more of computer work, instead of exerting an effort for their tasks at hand. Aside from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.

2. It poses security difficulties

Because there would be a huge number of people who would be using a computer

network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.

3. It lacks robustness.

As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.

4. It allows for more presence of computer viruses and malware

There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.

5. Its light policing usage promotes negative acts

It has been observed that providing users with internet connectivity has fostered undesirable behavior among them. Considering that the web is a minefield of distractions—online games, humor sites and even porn sites—workers could be tempted during their work hours. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters. While many organizations draw up certain policies on this, they have proven difficult to enforce and even engendered resentment from employees.

6. It requires an efficient handler:

For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

7. It requires an expensive set-up

Though computer networks are said to be an inexpensive system when it is already running, its initial set up cost can still be high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. Aside from these, it would also need network interface cards (NICs) for workstations in case they are not built in.

Types of Networks

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose. The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe. Some of the different networks based on size are:

- Personal area network, or PAN
- Local area network, or LAN
- Metropolitan area network, or MAN
- Wide area network, or WAN

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

- Storage area network, or SAN
- Enterprise private network, or EPN
- Virtual private network, or VPN

Personal Area Network

A **personal area network**, or **PAN**, is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices.

If multiple individuals use the same network within a residence, the network is

sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device. This type of network provides great flexibility. For example, it allows you to:

- Send a document to the printer in the office upstairs while you are sitting on the couch with your laptop.
- Upload a photo from your cell phone to your desktop computer.
- Watch movies from an online streaming service to your TV.

If this sounds familiar to you, you likely have a PAN in your house without having called it by its name.

Local Area Network (LAN)

Local Area Network (LAN) connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

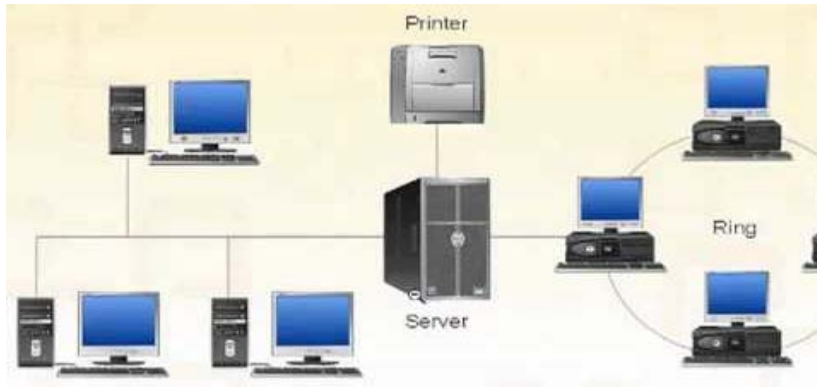


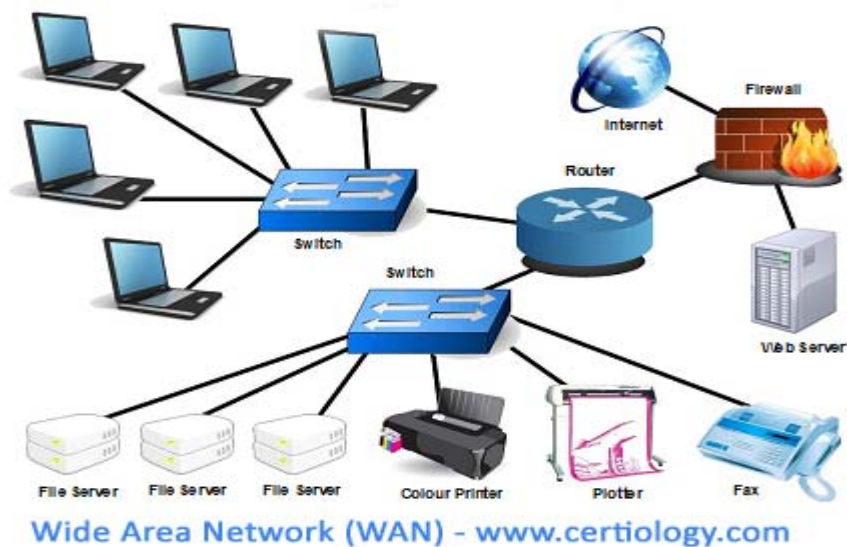
Fig: LAN

Early LAN's had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example: A bunch of students playing Counter Strike in the same room (without internet).

Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.



Wide Area Network (WAN)

Wide Area Network (WAN) is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

WAN's data rate is slow about a 10th LAN's speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for transmission of data through WAN are:

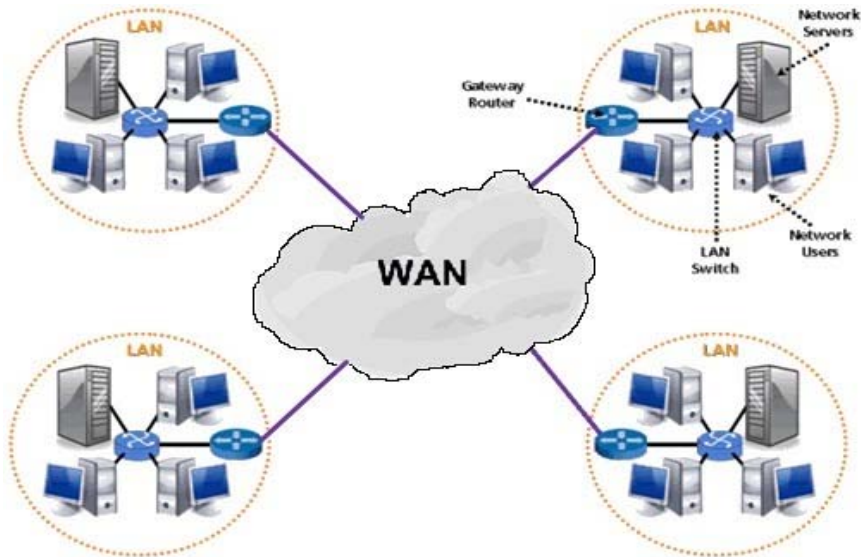


Fig: WAN

Optic wires, Microwaves and Satellites. Example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet.

Network Topology

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Bus Topology

In case of bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

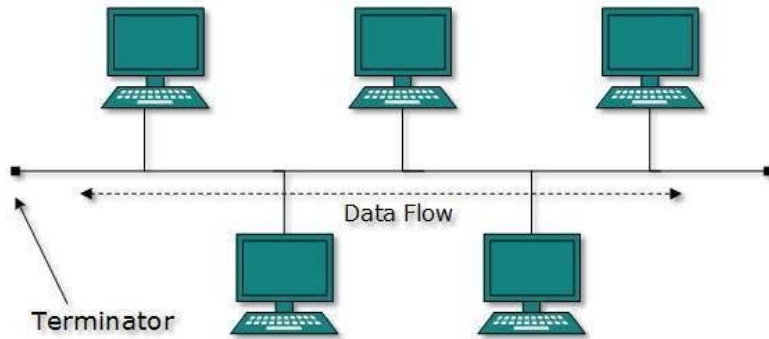


Fig: Bus Topology

Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star Topology

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

- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway

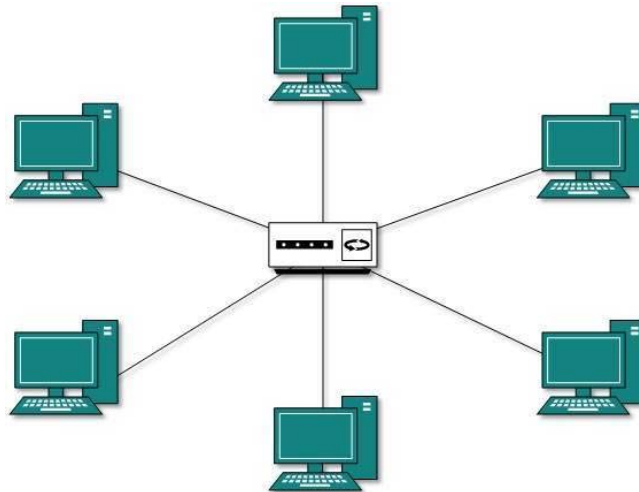


Fig: Star Topology

As in bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable. Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

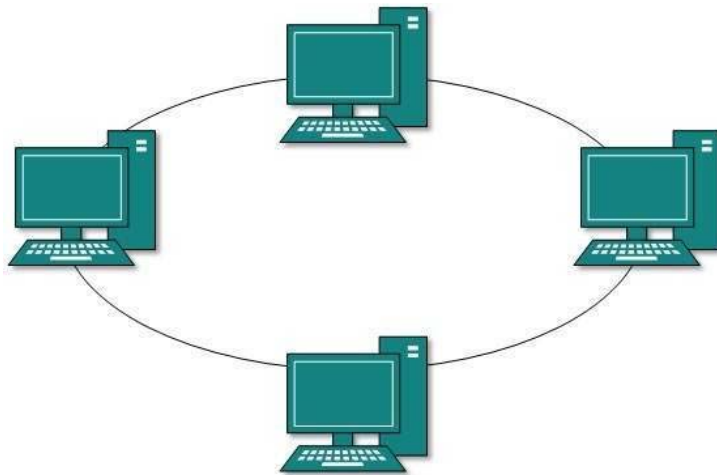


Fig: Ring Topology

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only. Hosts in mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

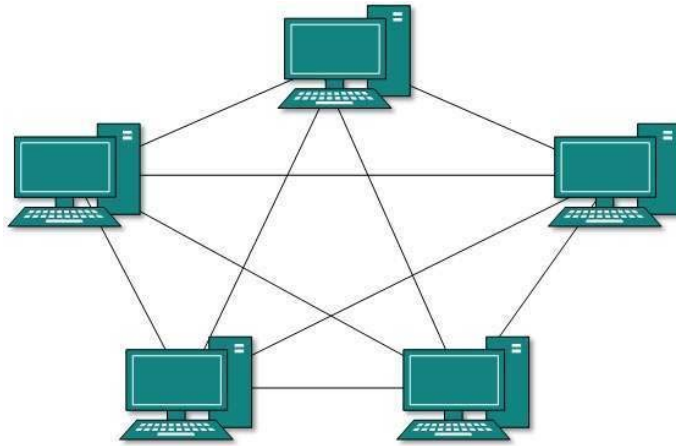


Fig: Mesh Topology

- **Full Mesh:** All hosts have a point-to-point connection to every other host in the network. Thus, for every new host $n(n-1)/2$ connections are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh:** Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

Unit: 5

Reference Model

Objectives:

- To explain OSI and TCP/IP reference model.
- To compare OSI and TCP/IP Model.

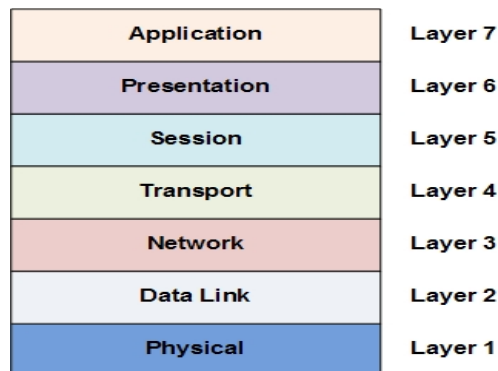
Learning Process and Study Materials

- Class demonstration and practical
- Group discussion
- Project work

Content's Elaboration:

OSI (Open Systems Interconnection):

OSI (Open Systems Interconnection) model was created by the International Organization for Standardization (ISO), an international standard-setting body. It was designed to be a reference model for describing the functions of a communication system. The OSI model provides a framework for creating and implementing networking standards and devices and describes how network applications on different computers can communicate through the network media. It has seven layers, with each layer describing a different function of data traveling through a network.



Below we have the complete representation of the OSI model, showcasing all the layers and how they communicate with each other

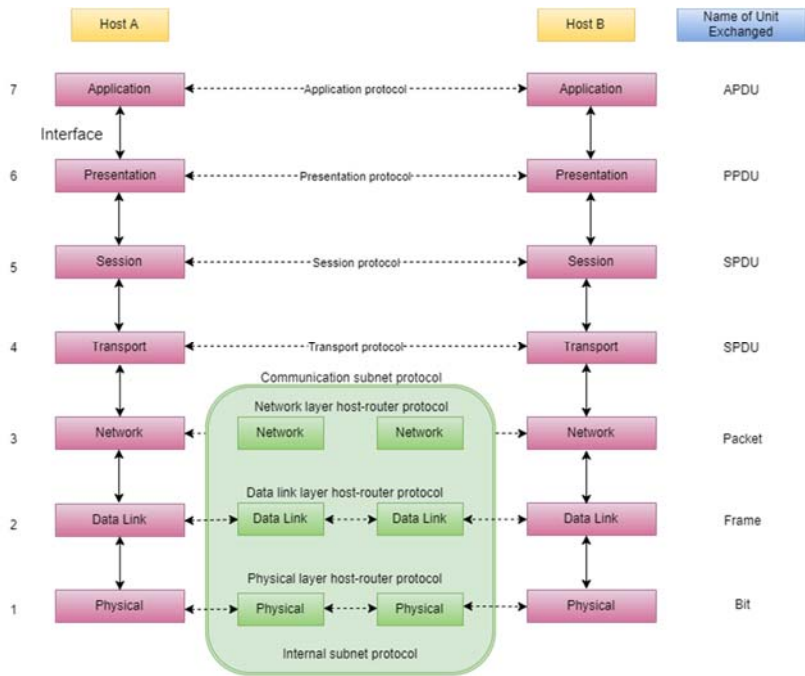


Fig: OSI layer

In the table below, we have specified the **protocols** used and the **data unit** exchanged by each layer of the OSI Model.

Layer	Name of Protocol	Name of Unit exchanged
Application	Application Protocol	APDU - Application Protocol Data Unit
Presentation	Presentation Protocol	PPDU - Presentation Protocol Data Unit
Session	Session Protocol	SPDU - Session Protocol Data Unit
Transport	Transport Protocol	TPDU - Transport Protocol Data Unit
Network	Network layer host-router Protocol	Packet
Data Link	Data link layer host-router Protocol	Frame
Physical	Physical layer host-router Protocol	Bit

Table: Protocol use in OSI layer

The Physical Layer (Layer 1)

Layer 1 of the OSI model is named the physical layer because it is responsible for the transmission and reception of wire level data. For example, the physical layer is where it is dictated how bits are represented across a specific networking medium.

Regardless of whether the networking medium is electrical or optical in construction, the physical layer handles how data is physically encoded and decoded; examples of this would include whether a specific voltage on an electrical medium represents a 1 or 0 or another example would be how a light received at a specific wavelength would be interpreted. Standards examples include IEEE 802.3 (Ethernet), IEEE 802.11 (Wireless Ethernet) and Synchronous optical networking (SONET) among others.

The Data Link Layer (Layer 2)

Layer 2 of the OSI model is named the data link layer and is responsible for link establishment and termination, frame traffic control, sequencing, acknowledgment, error checking, and media access management. The most familiar standards used at the data link layer include IEEE 802.3 (Ethernet) Media Access Control (MAC) and Logical Link Control (LLC) sub layers. The LLC acts as an interface between the physical layer and the MAC sub layer, and the MAC sub layer provides the ability for multiple terminals (computers) to communicate over the same physical medium. Other standards examples include Asynchronous Transfer Mode (ATM), High-Level Data Link Control (HDLC), Frame Relay and the Point to Point Protocol (PPP)

The Network Layer (Layer 3)

Layer 3 of the OSI model is named the network layer and is where routing of network traffic begins. The network layer not only makes the traffic routing decisions but also provides traffic control, fragmentation, and logical addressing (Internet Protocol (IP) addresses). The most common network layer protocol is IP, but other commonly used protocols include the Internet Control Message Protocol (ICMP) and Internet Group Message Protocol (IGMP).

The Transport Layer (Layer 4)

Layer 4 of the OSI model is named the transport layer and is responsible for message segmentation, acknowledgement, traffic control, and session multiplexing. The transport layer also has the ability to perform error detection and correction (resends), message reordering to ensure message sequence, and reliable message

channel depending on the specific transport layer protocol used. The most common of the used transport layer protocols include the Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

The Session Layer (Layer 5)

Layer 5 of the OSI model is named the session layer and is responsible for session establishment, maintenance and termination (the ability to have multiple devices use a single application from multiple locations). Common examples of session layer protocols are Named Pipes and NetBIOS.

The Presentation Layer (Layer 6)

Layer 6 of the OSI model is named the presentation layer and is responsible for character code translation (i.e. ASCII vs. EBCDIC vs. Unicode), data conversion, compression, and encryption. Some common examples include Multipurpose Internet Mail Extensions (MIME), Transport Layer Security (TLS) and Secure Sockets Layer (SSL).

The Application Layer (Layer 7)

Layer 7 of the OSI model is named the application layer and is responsible for a number of different things depending on the application; some of these things include resource sharing, remote file access, remote printer access, network management, and electronic messaging (email). There are a large number of application layer protocols that are familiar to the common Internet user, including the File Transfer Protocol (FTP), Domain Name Service (DNS), Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP).

TCP/IP Model

Like the OSI model, the TCP/IP model is layered and is used in the same fashion as the OSI model but with fewer layers. As the modern internet and most communications use the Internet Protocol (IP), the TCP/IP model is technically more in line with modern network implementations. As stated before, the layers within the TCP/IP model are considered less rigid than that of the OSI model, which basically means that many protocols implemented can be considered in grey areas between one area and another. The TCP/IP protocol suite (often referred to as the

TCP/IP protocol) contains the same protocols referenced in the earlier OSI model sections. Figure below shows a representation of the TCP/IP model:

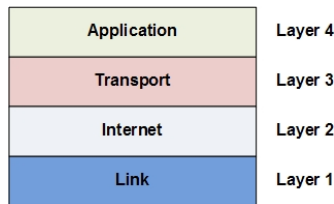


Fig: TCP/IP Model

The Link Layer

The link layer is the lowest layer of the TCP/IP model; it is also referred to in some texts as the *network interface* layer. The link layer combines the physical and data link layer functions into a single layer. This includes frame physical network functions like modulation, line coding and bit synchronization, frame synchronization and error detection, and LLC and MAC sublayer functions. Common protocols include Address Resolution Protocol (ARP), Neighbor Discovery Protocol (NDP), IEEE 802.3 and IEEE 802.11.

The Internet Layer

The internet layer is the next layer up from the link layer and is associated with the network layer of the OSI model. Functions include traffic routing, traffic control, fragmentation, and logical addressing. Common protocols include IP, ICMP and IGMP.

The Transport Layer

The transport layer is the next layer and is typically related directly with the same named layer in the OSI model. Functions include message segmentation, acknowledgement, traffic control, session multiplexing, error detection and correction (resends), and message reordering. Common protocols include Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

The Application Layer

The application layer is the highest layer in the TCP/IP model and is related to the session, presentation and application layers of the OSI model. The application layer

of the TCP/IP model is used to handle all process-to-process communication functions; these functions were carried out by multiple different layers when referencing the OSI model. There are a number of different functions which are carried out by this layer, including session establishment, maintenance and termination, character code translations, data conversion, compression and encryption, remote access, network management and electronic messaging to name a few. Common protocols include Named Pipes, NetBIOS, MIME, TLS, SSL, FTP, DNS, HTTP, SMTP and many others.

Similarities between OSI and TCP / IP Reference Models

1. Both the reference models are based upon layered architecture.
2. The layers in the models are compared with each other. The physical layer and the data link layer of the OSI model correspond to the link layer of the TCP/IP model. The network layers and the transport layers are the same in both the models. The session layer, the presentation layer and the application layer of the OSI model together form the application layer of the TCP/IP model.
3. In both the models, protocols are defined in a layer-wise manner.
4. In both models, data is divided into packets and each packet may take the individual route from the source to the destination.

TCP/IP Model vs. OSI Model

The TCP/IP model is older than the OSI model. The following figure shows corresponding relationship of their layers.

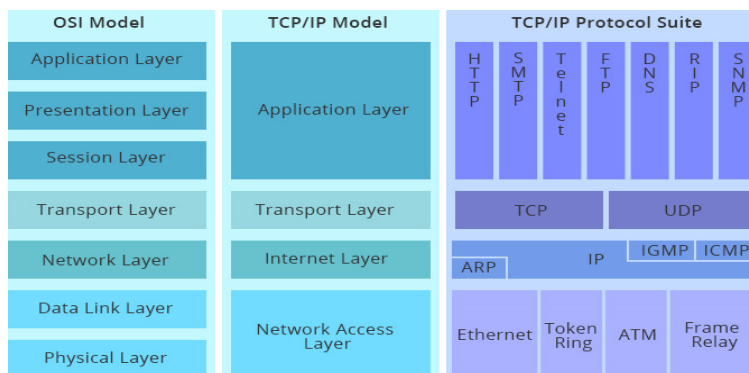


Fig: OSI model vs. TCP/IP model, and TCP/IP protocol suite

Comparing the layers of the TCP/IP model and the OSI model, the application layer of the TCP/IP model is similar to the OSI layers 5, 6, 7 combined, but TCP/IP model does not have a separate presentation layer or session layer. The transport layer of TCP/IP encompasses the responsibilities of the OSI transport layer and some of the responsibilities of the OSI session layer. The network access layer of the TCP/IP model encompasses the data link and physical layers of the OSI model. Note that the Internet layer of TCP/IP does not take advantage of sequencing and acknowledgment services that might be present in the data link layer of OSI model. The responsibility is of the transport layer in TCP/IP model.

Considering the meanings of the two reference models, the OSI model is just a conceptual model. It is mainly used for describing, discussing, and understanding individual network functions. However, TCP/IP is firstly designed to solve a specific set of problems, not to function as a generation description for all network communications as OSI model. OSI model is generic, protocol independent, yet most protocols and systems adhere to it, while TCP/IP model is based on standard protocols which the Internet has developed. Another thing should be noted in OSI model is that not all layers are used in simpler applications. While the layers 1, 2, 3 are mandatory for any data communication, the application may use some unique interface layer to the application instead of the usual upper layers in the model.

Differences between OSI and TCP / IP Reference Models

1. OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.
2. OSI model distinguishes the three concepts, namely, services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three.
3. OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
4. In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.
5. The OSI has seven layers while the TCP/IP has four layers.

1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally, it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers
OSI (Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)

Fig:Comparison Table of OSI and TCP/IP model

Unit: 6

IP Addressing

Objectives:

- To understand the IPV4 internet protocol and explain the addressing schemes.
- To introduce the basics of IPV6

Learning Process and Study Materials

- Class demonstration and practical
- Group discussion
- Project work

Content's Elaboration

IP Address

Every machine on a network has a unique identifier. Just as you would address a letter to send in the mail, computers use the unique identifier to send data to specific computers on a network. Most networks today, including all computers on the internet, use the TCP/IP protocol as the standard for how to communicate on the network. In the TCP/IP protocol, the unique identifier for a computer is called its IP address. There are two standards for IP addresses: IP Version 4 (IPv4) and IP Version 6 (IPv6). All computers with IP addresses have an IPv4 address, and many are starting to use the new IPv6 address system as well.

IPv4 Address

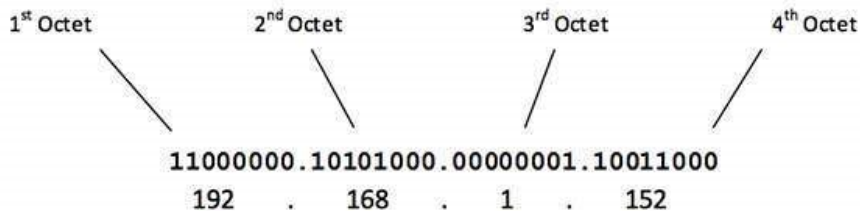
IPv4 uses 32 binary bits to create a single unique address on the network. An IPv4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number, also called an octet. For example: 216.27.61.137

At the dawn of IPv4 addressing, the internet was not the large commercial sensation it is today, and most networks were private and closed off from other networks around the world. When the internet exploded, having only 32 bits to identify a unique internet address caused people to panic that we'd run out of IP addresses. Under IPv4, there are 232 possible combinations, which offers just under 4.3 billion

unique addresses. IPv6 raised that to a panic-relieving 2128 possible addresses

A static address is one that you configure yourself by editing your computer's network settings. This type of address is rare, and it can create network issues if you use it without a good understanding of TCP/IP. Dynamic addresses are the most common. They're assigned by the Dynamic Host Configuration Protocol (DHCP), a service running on the network. DHCP typically runs on network hardware such as routers or dedicated DHCP servers.

Dynamic IP addresses are issued using a leasing system, meaning that the IP address is only active for a limited time. If the lease expires, the computer will automatically request a new lease. Sometimes, this means the computer will get a new IP address, too, especially if the computer was unplugged from the network between leases. This process is usually transparent to the user unless the computer warns about an IP address conflict on the network (two computers with the same IP address). An address conflict is rare, and today's technology typically fixes the problem automatically. The IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP address. The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



The number of networks and the number of hosts per class can be derived by this formula:

$$\text{Number of networks} = 2^{\text{network_bits}}$$

$$\text{Number of Hosts/Network} = 2^{\text{host_bits}} - 2$$

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus, the first octet ranges from 1 – 127, i.e.

00000001 - 01111111
1 - 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts ($2^{24}-2$).

Class A IP address format is:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 - 10111111
128 - 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 ($2^{16}-2$) Host addresses.

Class B IP address format is:

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000000 - 11011111
192 - 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses.

Class C IP address format is:

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

$$\begin{array}{c} \mathbf{1110}0000 - \mathbf{1110}1111 \\ 224 - 239 \end{array}$$

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

IPv4 addresses represent four eight-digit binary numbers. That means that each number could be 00000000 to 11111111 in binary, or 0 to 255 in decimal (base-10). In other words, 0.0.0.0 to 255.255.255.255. However, some numbers in that range are reserved for specific purposes on TCP/IP networks. These reservations are recognized by the authority on TCP/IP addressing, the Internet Assigned Numbers Authority (IANA). Four specific reservations include the following:

- **0.0.0.0** -- This represents the default network, which is the abstract concept of just being connected to a TCP/IP network.
- **255.255.255.255** -- This address is reserved for network broadcasts, or

messages that should go to all computers on the network.

- **127.0.0.1** -- This is called the loopback address, meaning your computer's way of identifying itself, whether or not it has an assigned IP address.
- **169.254.0.1 to 169.254.255.254** -- This is the Automatic Private IP Addressing (APIPA) range of addresses assigned automatically when a computer's unsuccessful getting an address from a DHCP server.

Subnet masks

A single IP address identifies both a network, and a unique interface on that network. A subnet mask can also be written in dotted decimal notation and determines where the network part of an IP address ends, and the host portion of the address begins. When expressed in binary, any bit set to one means the corresponding bit in the IP address is part of the network address. All the bits set to zero mark the corresponding bits in the IP address as part of the host address. The bits marking the subnet mask must be consecutive ones. Most subnet masks start with 255 and continue on until the network mask ends. A Class C subnet mask would be 255.255.255.0. Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of

second octet and added to Network address, it creates two Subnets ($2^1=2$) with ($2^{23}-2$) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and ($2^{16}-2$) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may

ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator has 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology, the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step - 1

Make a list of Subnets possible.

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step - 2

Sort the requirements of IPs in descending order (Highest to Lowest).

- Sales 100
- Purchase 50
- Accounts 25
- Management 5

Step - 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step - 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step - 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step - 6

Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So, this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used CIDR.

IPv6 address

An IPv6 address is a 128-bit alphanumeric string that identifies an endpoint device in the Internet Protocol Version 6 (IPv6) addressing scheme. In more precise terms, an IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are

separated by colons. Here's an example of a full IPv6 address:

FE80:CD00:0000:0CDE:1257:0000:211E:729C

That address can be shortened, however, because the addressing scheme allows the omission of any leading zero, as well as any sequences consisting only of zeroes. Here's the short version: FE80:CD00:0:CDE:1257:0:211E:729C

It has been a concern for some time that the IPv4 addressing scheme was running out of potential addresses. The IPv6 format was created to enable the trillions of new IP addresses required to connect not only an ever-greater number of computing devices but also the rapidly expanding numbers of items with embedded connectivity. In the Internet of Things (IoT) scenario, objects, animals and people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction. IPv6 expands the available address space sufficiently to enable anything conceivable to have an IP address. The number of potential IPv6 addresses has been calculated as: 340,282,366,920,938,463,374,607,431,768,211,456

According to Computer History Museum docent Dick Guertin, that number allows an IPv6 address for each atom on the surface of the planet-- with enough left over for more than 100 more similar planets.

The Benefits of IPv6

While increasing the pool of addresses is one of the most often-talked about benefit of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol:

- No more NAT (Network Address Translation)
- Auto-configuration
- No more private address collisions
- Better multicast routing
- Simpler header format
- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"

- Built-in authentication and privacy support
- Flexible options and extensions
- Easier administration (say good-bye to DHCP)

The Difference Between IPv4 and IPv6 Addresses

An IP address is binary numbers but can be stored as text for human readers. For example, a 32-bit numeric address (IPv4) is written in decimal as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address. IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

Unit: 7

Router Configuration

Objectives:

- To understand the basics of Routing.
- To apply Cisco Simulator

Learning Process and Study Materials

- Class demonstration and practical
- Group discussion
- Project work

Content's Elaboration

Introduction to Routing

Routing is the process of forwarding packets from one network to the destination address in another network. Router, a packet forwarding device between two networks, is designed to transmit packets based on the various routes stored in routing tables. Each route is known as a routing entry.

We have seen switches and you have learned that they “switch” based on MAC address information. The only concern for our switch is to know when an Ethernet frame enters one of its interfaces where it should send this Ethernet frame by looking at the destination MAC address. Switches make decisions based on Data Link layer information (layer 2).

Routers have a similar task but this time we are going to look at IP packets and as you might recall IP is on the Network layer (layer 3). Routers look at the destination IP address in an IP packet and send it out the correct interface.

Why don't we use MAC addresses everywhere and switch? Why do we need to look at IP addresses and route? Both MAC addresses and IP addresses are unique per network device. Good question and I'm going to show you a picture to answer this:

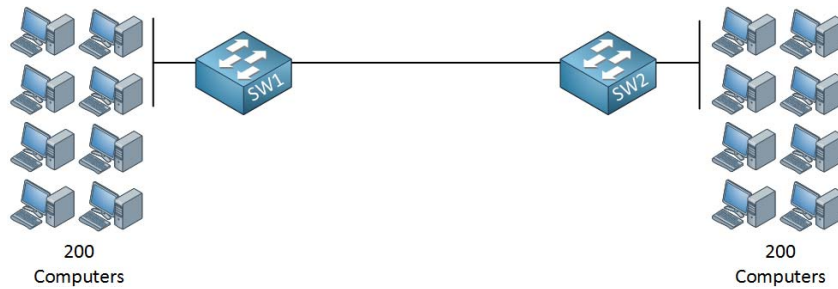
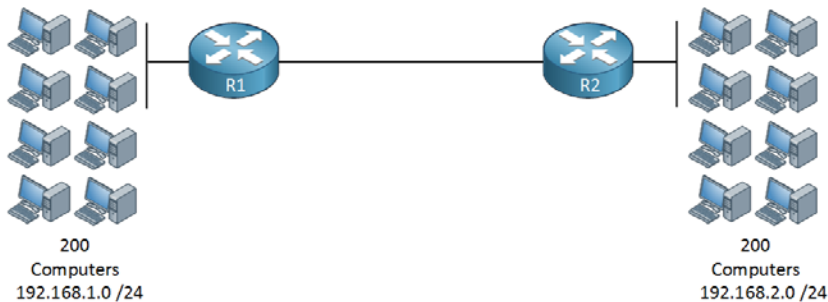


Fig: Network to Network communication

We can see two switches in figure each switch there are 200 computers connected. Now if all 400 computers want to communicate with each switch has to learn 400 MAC addresses. The need to know the MAC addresses of the computers on the left and right side.

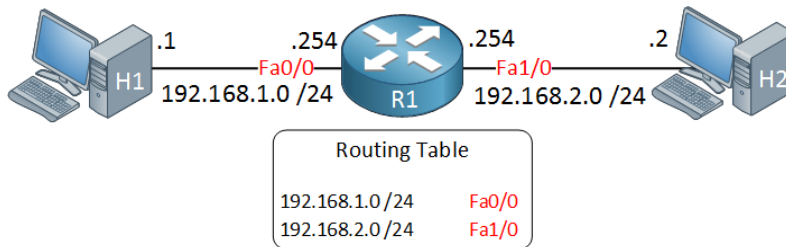
Now think about a really large network...for example the internet. There are millions of devices! Would it be possible to have millions of entries in your MAC-address table? For each device on the Internet? No way! The problem with switching is that it's not scalable; we don't have any hierarchy just flat 48-bit MAC addresses. Let's look at the same example but now we are using routers.



What we have here is our 200 computers on the left are connected to R1 and in the 192.168.1.0 /24 network. R2 has 200 computers behind it and the network we use over there is 192.168.2.0 /24. Routers “route” based on IP information, in our example R1 only has to know that network 192.168.2.0 /24 is behind R2. R2 only needs to know that the 192.168.1.0 /24 network is behind R1. Are you following me here?

Instead of having a MAC-address-table with 400 MAC addresses we now only need a single entry on each router for each other's networks. Switches use mac address

tables to forward Ethernet frames and routers use a routing table to learn where to forward IP packets to. As soon as you take a brand new router out of the box It will build a routing table but the only information you'll find are the directly connected interfaces. Let's start with a simple example:



Above there are one router and two computers:

- H1 has IP address 192.168.1.1 and has configured IP address 192.168.1.254 as its default gateway.
- H2 has IP address 192.168.2.2 and has configured IP address 192.168.2.254 as its default gateway.
- On our router we have configured IP address 192.168.1.254 on interface Fast Ethernet 0/0 and IP address 192.168.2.254 on interface Fast Ethernet 1/0.
- Since we also configured a subnet mask with the IP addresses our router knows the network addresses and will store these in its routing table.

There are 3 types of routing:

1. Static routing

Static routing is a process in which we have to manually add routes in routing table.

Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

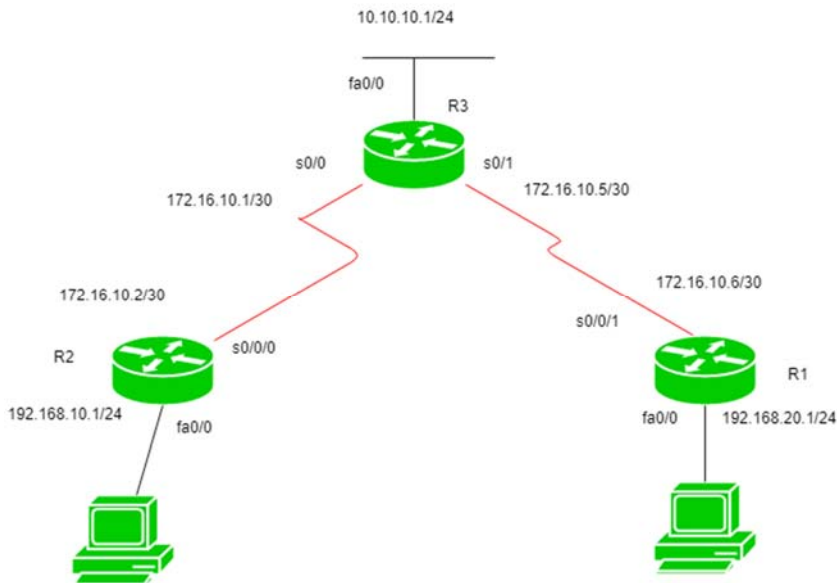
Disadvantage

- For a large network, it is a hectic task for administrator to manually add each

route for the network in the routing table on each router.

- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Configuration



R1 having IP address 172.16.10.6/30 on s0/0/1, 192.168.10.1/24 on fa0/0.
R2 having IP address 172.16.10.2/30 on s0/0/0, 192.168.20.1/24 on fa0/0.
R3 having IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.

Now configuring static routes for router R3:

```
R3(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.2
```

```
R3(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.6
```

Here, provided the route for 192.168.10.0 network where 192.168.10.0 is its network I'd and 172.16.10.2 and 172.16.10.6 are the next hop address.

Now, configuring for R2:

```
R2(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.1
```

```
R2(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.1
```

```
R2(config)#ip route 172.16.10.4 255.255.255.0 172.16.10.1
```

Similarly, for R1:

```
R1(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.5
```

```
R1(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.5
```

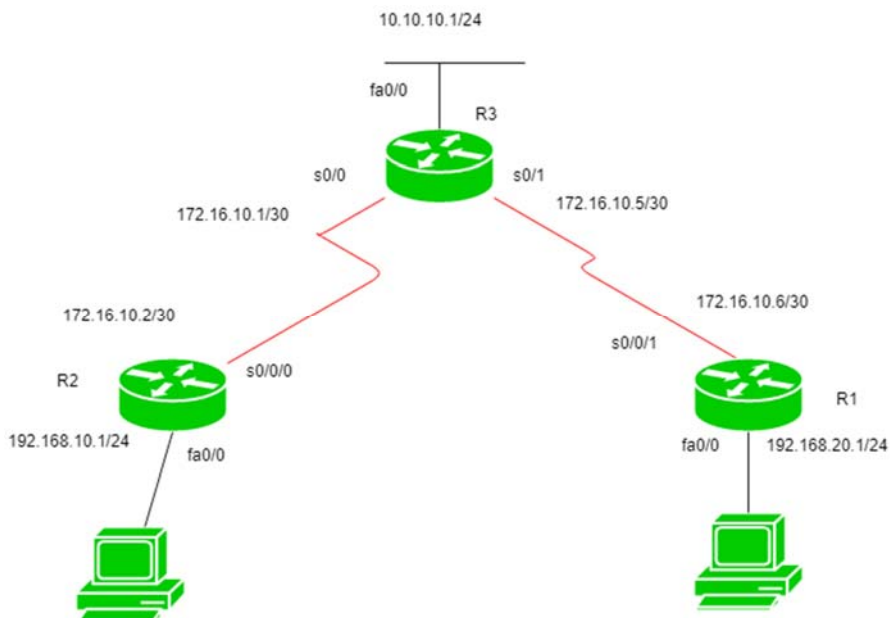
```
R1(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.5
```

1. Default Routing

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.

2. Configuration

Using the same topology which we have used for the static routing before.



In this topology, R1 and R2 are stub routers so we can configure default routing for both these routers.

Configuring default routing for R1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.5
```

Now configuring default routing for R2:

```
R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.1
```

3. Dynamic Routing

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

A dynamic protocol has following features:

1. The routers should have the same dynamic protocol running in order to exchange routes.
2. When a router finds a change in the topology then router advertises it to all other routers.

Advantages

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation program that allows students to experiment with network behavior and ask “what if” questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts.

Packet Tracer supplements physical equipment in the classroom by allowing students to create a network with an almost unlimited number of devices, encouraging practice, discovery, and troubleshooting. The simulation-based learning environment helps students develop 21st century skills such as decision making, creative and critical thinking, and problem solving. Packet Tracer complements the Networking Academy curricula, allowing instructors to easily teach and demonstrate complex technical concepts and networking systems design.

The Packet Tracer software is available free of charge to Networking Academy instructors, students, alumni, and administrators who are registered NetSpace users.

Cisco packet tracer is network simulator software, basically it is used for practicing labs for Cisco exams. With the help of this tool we can build our own network topology and can practice different scenarios. Also, you can use it for testing purpose. Suppose, if we want to deploy any change in our production network, we can use packet tracer to first test the required changes and if everything is working fine then we can deploy that changes into production. Packet tracer has limited features, if we want advance features then we can use GNS3 network simulator. It is a great tool.

Use of Cisco Simulator

Step1: Download the software first. Click on the link below.

Step2: Install it like the other regular software.

Step3: Open/ Start the software.

Step4: If you have Neta cad username password then use those credentials to login Other wise if you don't have any username & password then click on the GUEST LOGIN. Wait few seconds then click on confirmed Guest for logging in.

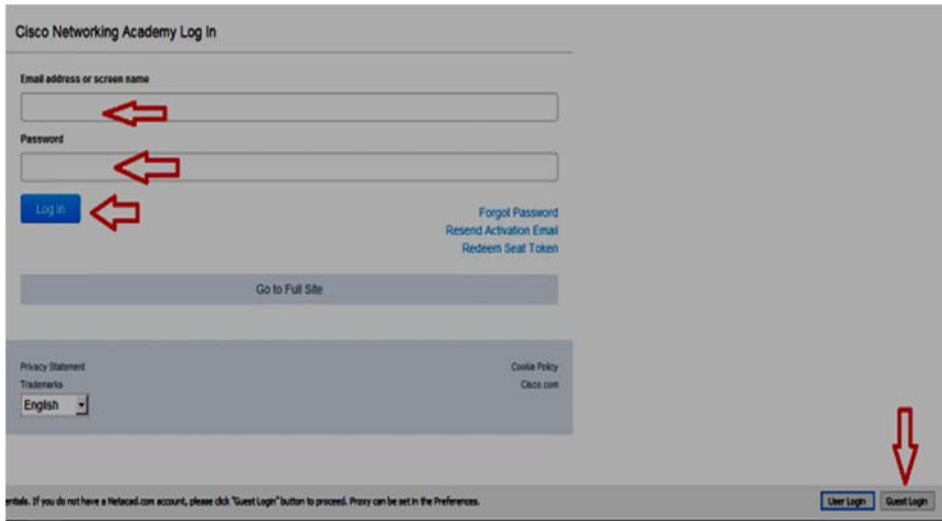


Figure: Cisco Packet tracer login

Now the first look for the simulator will be like this

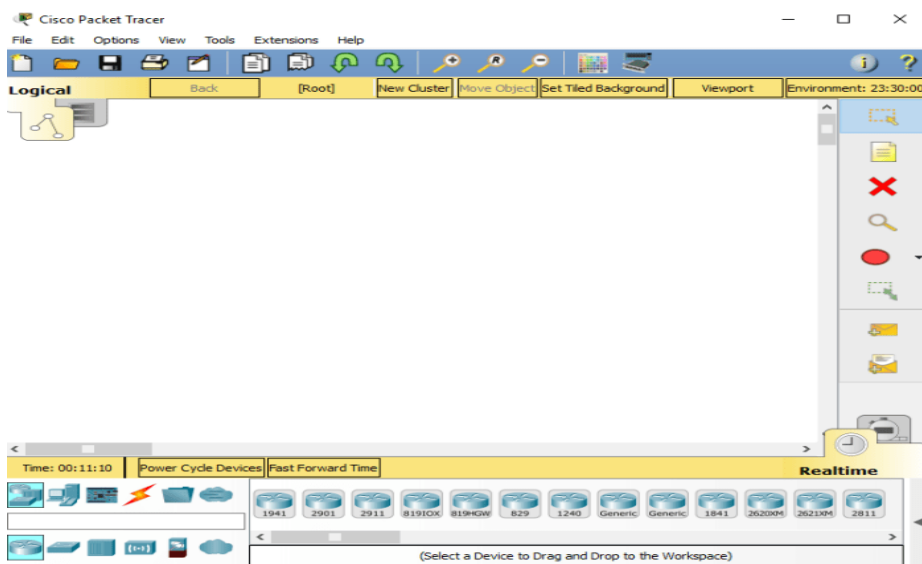
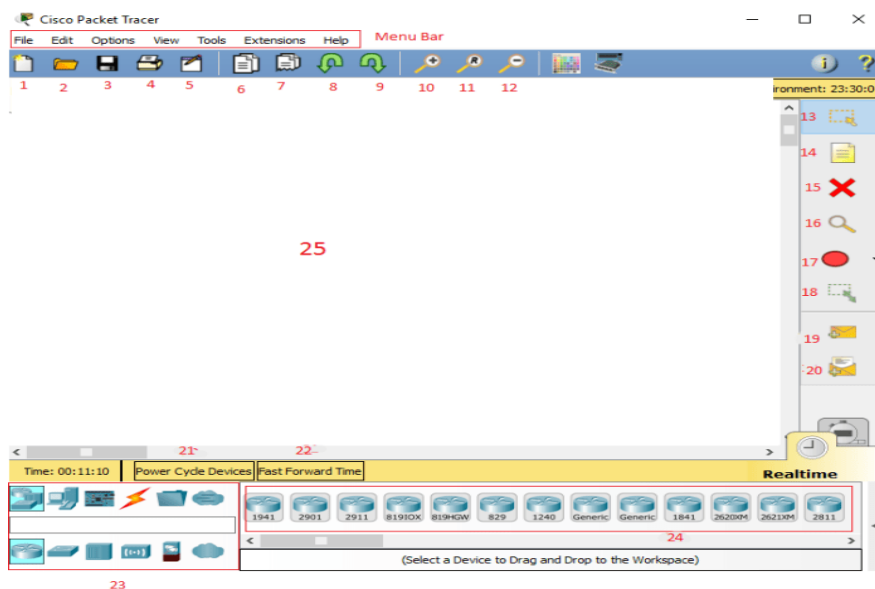


Figure: First look of the cisco packet tracer Simulator

Now let's get introduced to the Simulator's components and good features.

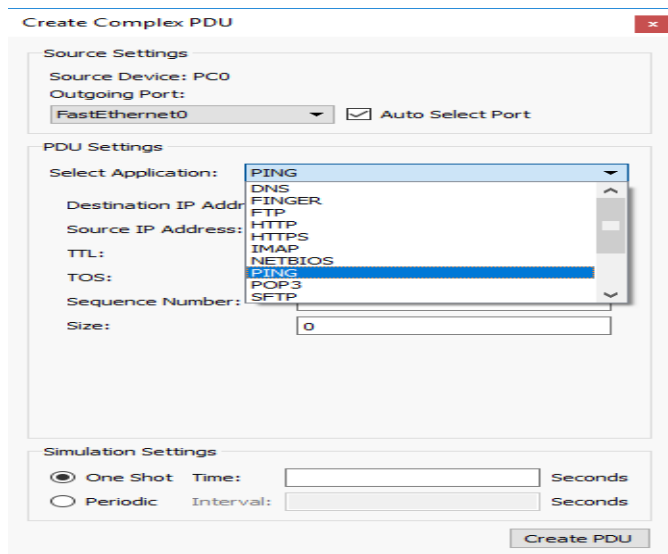


Menu Bar : Menu bar holds all the common menus like File,edit, option, help etc.

To understand the other tools and feature please check above image and information given below:

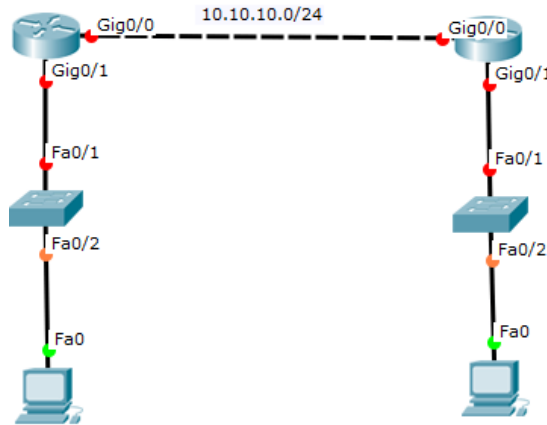
1. New File: Creates a new file
2. Open: Opens a Saved file. You have to select your previously saved packet tracer file.
3. Save: Saves your existing topology.
4. Print: Prints your existing topology
5. Activity Wizard: Allows an instructor to create a scenario with instructions and answers.
6. Copy: Copy and Object or group of objects
7. Paste: Paste the copied objects
8. Undo: Performs the undo task
9. Redo: Performs redo task
10. Zoom in
11. Zoom reset
12. Zoom out
13. Select / cursor

14. Place Note
15. Delete
16. Inspect
17. Drawing tools
18. Resize shape
19. Add a simple PDU: Used to ping 1 time only in simulation to test connectivity
20. Add a complex PDU: Used to check connectivity or service. Complex PDU has more options than Simple PDU. Check the image below:
21. Power Cycle: Used to restart a device



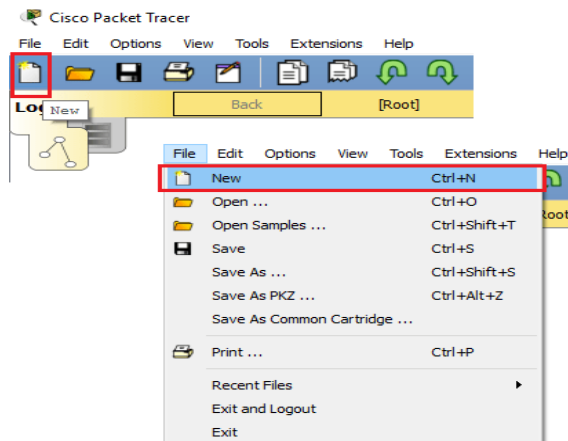
22. Fast Forward: Used to fast forward any task. For example, Fast forwarding Device Boot procedure. It just saves time during work.
23. Inventory: Device inventory. User has to select device types from here
24. Device List: Device list shows all the devices of inventory. If you have selected Routers from inventory then all the router's list will be showed in the device list. A user has to select a Specific device from the device list to use in the simulator.
25. Workspace: The place where you work or build your topology.

Now let's Make a topology using Cisco Packet tracer: So we are going to make a topology like the below one.

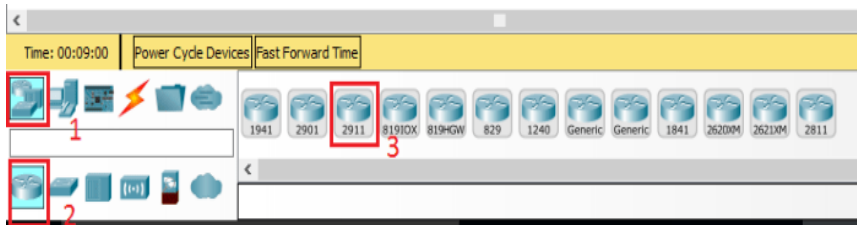


So, to make this topology we have to do the following tasks:

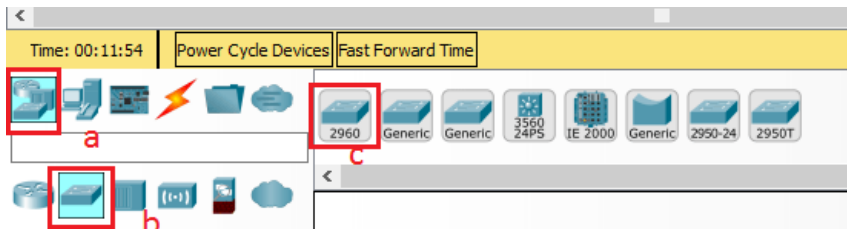
1. Create a new file
2. Get the devices
3. Connect cables
4. Puts some textsSaves the topology**Create a New File:** Click on File Menu and Select New or Simply click on “NEW” [check above]



5. Get the devices:
6. Click on the device types
7. Click on Router.
8. Select Cisco 2911 router then Click on the white workspace. So, a router will be placed on the work-space.
9. Do the same thing again to place the 2nd router.



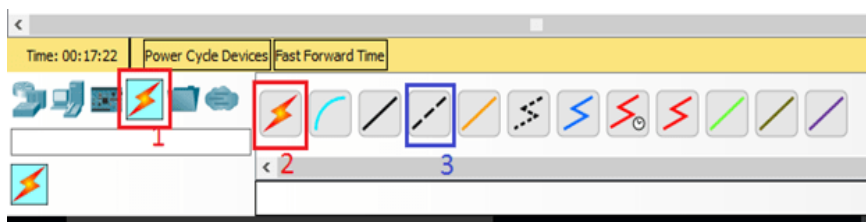
Now select Switch from the device inventory: Select switch and then select 2960 switch from right side device list. Then Click on the workspace. Do it 2 times.



Now Select 2 Desktop PC: Select End user list. Select PC from the right-side device list. Now click on workspace. Do this 2 times.



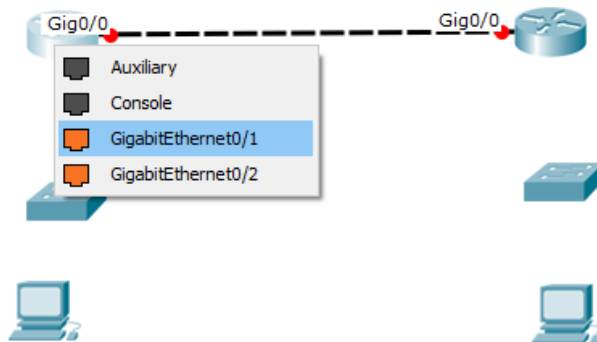
Cable Connection: Go to the cable option. Select cables, select Auto cable first.



Auto Cable Connection: Now after selecting auto cable click on the left router first. The cable will be automatically connected. Then move the mouse cursor to the 2nd router and click on it. Cable will be automatically connected.

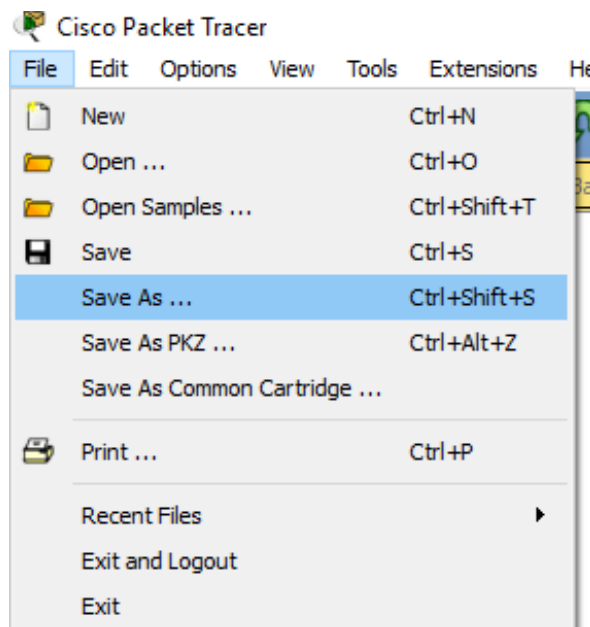
Manual Cable connection: to perform this step please select appropriate cable like for same type of devices use cross cable and for different type of cable use straight cable. Here for switch to router connection we will use straight cable:

1. Select Straight cable
2. Click on the router > select interface G0/1
3. Click on the selection.
4. Then move your mouse cursor/pointer to the switch and click on the switch
5. Select interface G0/1 and click on it.
6. So, cable will be connected.

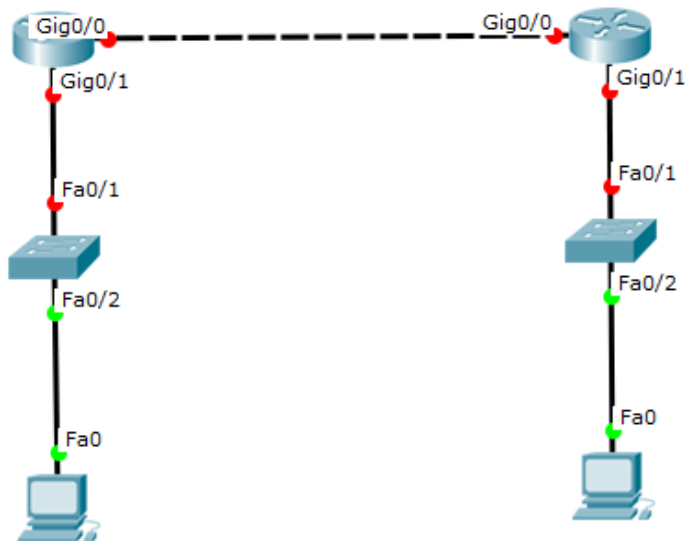


Perform these steps to connect the remaining cabling:

Save the file: Click on File>Click on Save as >Select a location in your HDD> Provide a File name> Click on Save.

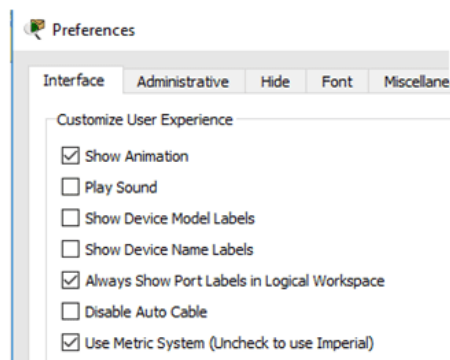
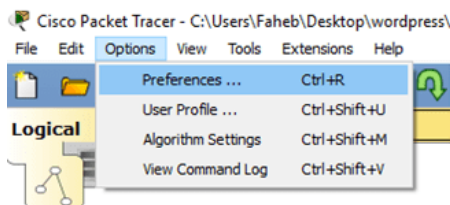


So after completing everything our topology will look like this :



Note: The Red Circle confirms that the link is inactive. The Green circle indicates that the link is active. Now if you don't see the interface number labels on the link then do as following:

1. Click on Option > preference
 2. Enable the "Always show port labels...."
- You may also enable or disable the "Show device model label" and "Show device name label"



Now for any new change save the file again.

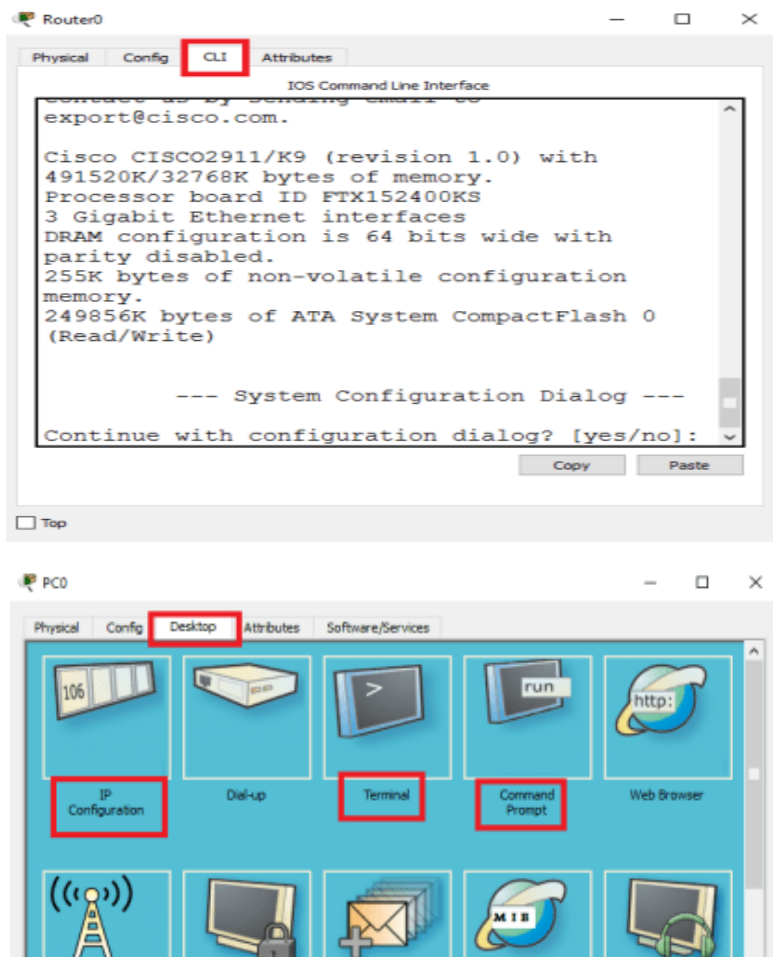
1. Click on File>Save

Now Starting Configuring a Device:

To start configuring a device click on the device:

For Router or Switch: Click on the CLI to get the Command Line Interface(CLI)

For Desktop or LAPTOP: Click on the Desktop. from there you will find your necessary options.



That's all for today, lets cook some typologies and practice to enhance the skills

Let's practice some configuration, to do that please check Network Fundamental Page. To go there click on the link below:

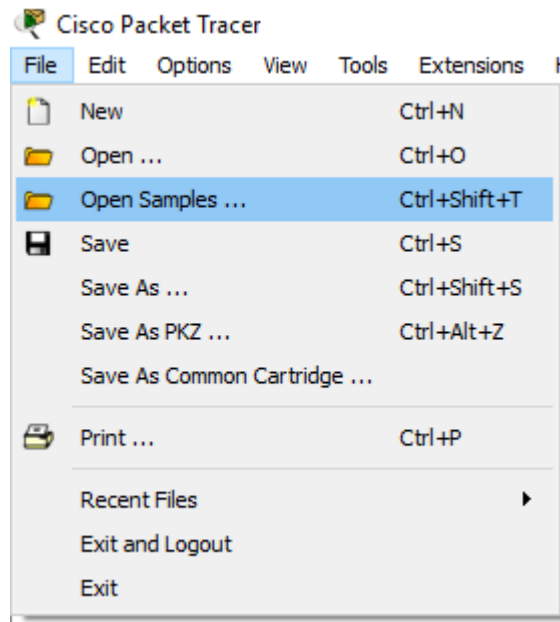
Network fundamental

In the packet tracer simulator there are some sample configurations for practice purpose. you can also open those configurations to practice some tasks if you want to. to do this do the following:

Step1: GO to File Menu>Open Samples

Step2: Select The sample from the folders

Step3: Click on Open.



If you find this post helpful then please do not hesitate to rate this post.

Unit: 8

Network Cabling

Objectives

- To explain the types of media used in networks
- To justify the physical layer in the networking system
- To identify the disaster recovery strategies and apply them

Learning Process and Study Materials

- Lecture basis
- Class demonstration and practical
- Field Visit
- Project work

Content's Elaboration

Network Media

Whatever type of network is used, some type of network medium is needed to carry signals between computers. Two types of media are used in networks: cable-based media, such as twisted pair, and the media types associated with wireless networking, such as radio waves.

In networks using cable-based media, there are three basic choices:

- Twisted pair
- Coaxial
- Fiber-optic

Twisted pair and coaxial cables both use copper wire to conduct the signal electronically; fiber-optic cable uses a glass or plastic conductor and transmits the signals as light.

For many years, coaxial was the cable of choice for most LANs. Today, twisted pair has proven to be far and away the cable medium of choice, thus retiring coaxial to the confines of storage closets. Fiber-optic cable has also seen its popularity rise, but because of cost it has been primarily restricted to use as a

network backbone where segment length and higher speeds are needed. That said, fiber is now increasingly common in server room environments as a server-to-switch connection method, and in building-to-building connections in what are called metropolitan area networks (MANs). For more information on MANs, see Chapter 1, “Introduction to Networking.”

The following sections summarize the characteristics of each of these cable types.

Twisted-Pair Cabling

Twisted-pair cabling has been around for a very long time. It was originally created for voice transmissions and has been widely used for telephone communication. Today, in addition to telephone communication, twisted pair is the most widely used medium for networking.

The popularity of twisted pair can be attributed to the fact that it is lighter, more flexible, and easier to install than coaxial or fiber-optic cable. It is also cheaper than other media alternatives and can achieve greater speeds than its coaxial competition. These factors make twisted pair the ideal solution for most network environments.

Two main types of twisted-pair cabling are in use today:

Unshielded Twisted Pair

(UTP) and Shielded Twisted Pair (STP). UTP is significantly more common than STP and is used for most networks. Shielded twisted pair is used in environments in which greater resistance to EMI and attenuation is required. The greater resistance comes at a price, however. The additional shielding, plus the need to ground that shield (which requires special connectors), can significantly add to the cost of a cable installation of STP. STP provides the extra shielding by using an insulating material that is wrapped around the wires within the cable. This extra protection increases the distances that data signals can travel over STP but also increases the cost of the cabling. Figure 2.1 shows STP and UTP cabling.



FIGURE 2.1 STP and UTP cabling. (Reproduced with permission from Computer Desktop Encyclopedia. 1981–2005. The Computer Language Company, Inc. All rights reserved.)

There are several categories of twisted-pair cabling. The early categories are most commonly associated with voice transmissions. The categories are specified by the Electronic Industries Association/Telecommunications Industry Association (EIA/TIA). EIA/TIA is an organization that focuses on developing standards for electronic components, electronic information, telecommunications, and Internet security. These standards are important to ensure uniformity of components and devices.

EIA/TIA has specified a number of categories of twisted-pair cable:

Category 1: Voice-grade UTP telephone cable. Due to its susceptibility to interference and attenuation and its low bandwidth capability, Category 1 UTP is impractical for network applications.

Category 2: Data-grade cable that can transmit data up to 4 Mbps. Category 2 cable is too slow for network applications. It is unlikely that you will encounter Category 2 on any network today.

Category 3: Data-grade cable that can transmit data up to 10 Mbps with a possible bandwidth of 16 MHz. For many years, Category 3 was the cable of choice for twisted-pair networks. As network speeds pushed the 100 Mbps speed limit, Category 3 became ineffective.

Category 4: Data-grade cable that has potential data throughput of 16 Mbps. Category 4 cable was often implemented in the IBM Token-Ring Network. Category 4 cable is no longer used.

Category 5: Data-grade cable that typically was used with Fast Ethernet operating at 100 Mbps with a transmission range of 100 meters. Although

Category 5 was a popular media type, this cable is an outdated standard. Newer implementations use the 5e standard. Category 5 provides a minimum of 100MHz of bandwidth. Category 5, despite being used primarily for 10/100 Ethernet networking, can go faster. The IEEE 802.11ae standard specifies 1000Mbps over Category 5 cable. Chapter 6, “WAN Technologies and Internet Access,” provides more information on IEEE standards.

Category 5e: Data-grade cable used on networks that run at 10/100Mbps and even up to 1000Mbps. Category 5e cabling can be used up to 100 meters, depending on the implementation and standard used. Category 5e cable provides a minimum of 100 MHz of bandwidth.

Category 6: High-performance UTP cable that can transmit data up to 10Gbps. Category 6 has a minimum of 250 MHz of bandwidth and specifies cable lengths up to 100 meters with 10/100/1000Mbps transfer, along with 10Gbps over shorter distances. Category 6 cable typically is made up of four twisted pairs of copper wire, but its capabilities far exceed those of other cable types. Category 6 twisted pair uses a *longitudinal separator*, which separates each of the four pairs of wires from each other. This extra construction significantly reduces the amount of cross talk in the cable and makes the faster transfer rates possible.

Category 6a: Also called augmented 6. Offers improvements over Category 6 by offering a minimum of 500MHz of bandwidth. It specifies transmission distances up to 100 meters with 10Gbps networking speeds.

Coaxial

Coaxial cable, or *coax* as it is commonly called, has been around for a long time. Coax found success in both TV signal transmission and network implementations. As shown in Figure 2.2, coax is constructed with a copper core at the center that carries the signal, plastic insulation, braided metal shielding, and an outer plastic covering. Coaxial cable is constructed in this way to add resistance to *attenuation* (the loss of signal strength as the signal travels over distance), *cross talk* (the degradation of a signal, caused by signals from

other cables running close to it), and EMI. Two types of coax are used in networking: thin coax, also known as thinnet, and thick coax, also known as thicknet. Neither is particularly popular anymore, but you are most likely to encounter thin coax. Thick coax was used primarily for backbone cable. It could be run through plenum spaces because it offered significant resistance to EMI and crosstalk and could run in lengths up to 500 meters. Thick coax offers speeds up to 10Mbps, far too slow for today's network environments.

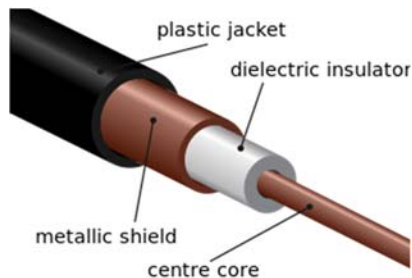


Fig: 2.2 Coaxial cabling.

Thin Coax

Thin coax is much more likely to be seen than thick coax in today's networks, but it isn't common. Thin coax is only .25 inches in diameter, making it fairly easy to install. Unfortunately, one of the disadvantages of all thin coax types is that they are prone to cable breaks, which increase the difficulty when installing and troubleshooting coaxial-based networks.

Several types of thin coax cable exist, each of which has a specific use.

Fiber-Optic Cable

In many ways, fiber-optic media addresses the shortcomings of copper-based media. Because fiber-based media use light transmissions instead of electronic pulses, threats such as EMI, crosstalk, and attenuation become nonissues. Fiber is well suited for the transfer of data, video and voice transmissions. In addition, fiber-optic is the most secure of all cable media. Anyone trying to access data signals on a fiber-optic cable must physically tap into the medium. Given the composition of the cable, this is a particularly difficult task.

Unfortunately, despite the advantages of fiber-based media over copper, it still

does not enjoy the popularity of twisted-pair cabling. The moderately difficult installation and maintenance procedures of fiber often require skilled technicians with specialized tools. Furthermore, the cost of a fiber-based solution limits the number of organizations that can afford to implement it. Another some- times hidden drawback of implementing a fiber solution is the cost of retro- fitting existing network equipment. Fiber is incompatible with most electronic network equipment. This means that you have to purchase fiber-compatible network hardware.

As shown in Figure 2.3, fiber-optic cable is composed of a core glass fiber surrounded by *cladding*. An insulated covering then surrounds both of these within an outer protective sheath.

Fiber-opticCable:

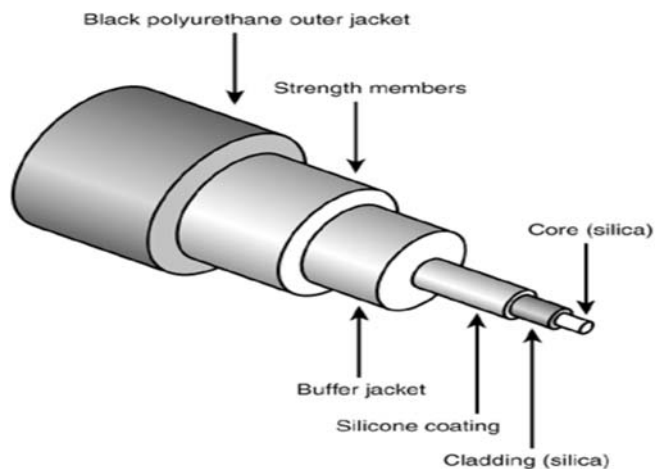


Fig: Fiber Optic Cabling...

Two types of fiber-optic cable are available:

Multi-

modefiber: Many beams of light travel through the cable, bouncing off the cable walls. This strategy actually weakens the signal, reducing the length and speed at which the data signal can travel.

Single-modefiber: Uses a single direct beam of light, thus allowing for greater distances and increased transfer speeds.

Some of the common types of fiber-optic cable include the following:

- 62.5-micron core/125-micron cladding multimode
- 50-micron core/125-micron cladding multimode
- 8.3-micron core/125-micron cladding single mode

In the ever-increasing search for bandwidth that will keep pace with the demands of modern applications, fiber-optic cables are sure to play a key role

Definition of Baseband Transmission

Baseband transmission uses whole frequency spectrum of the medium for the transmission. That is the reason frequency division multiplexing cannot be used in the transmission but time division multiplexing is used in this transmission as in TDM the link is not divided into multiple channels instead it provides each input signal with a time slot, in which the signal utilizes whole bandwidth for a given time slot. The signals are carried by wires in the form of electrical pulse.

Signals transmitted at point propagated in both the directions hence it is bidirectional. The expansion of baseband signal is limited to shorter distances because at high frequency the attenuation of the signal is most strong and the pulse blur out, causing the large distance communication completely impractical.

Definition of Broadband Transmission

The **Broadband transmission** employs analog signals which include optical or electromagnetic wave form of signal. The signals are sent into multiple frequencies permitting multiple signals to be sent simultaneously. Frequency division multiplexing is possible in which the frequency spectrum is divided into multiple sections of bandwidth. The distinct channels can support different types of signals of varying frequency ranges to travel simultaneously (at the same instance).

The signals propagated at any point are unidirectional in nature, in simple words the signal can be travelled at only one direction, unlike baseband transmission. It requires two data path that are connected at a point in the network refer to as head end. The first path is used for signal transmission from the station to the head end. And the other path is used for receiving propagated signals.

Difference between Baseband and Broadband Transmission



1. Baseband transmission utilizes digital signaling while broadband transmission uses analog signaling.
2. Bus and tree topologies, both work well with the broadband transmission. On the other hand, for the baseband transmission bus topology is suitable.
3. Baseband involves Manchester and differential Manchester encoding. In contrast, broadband does not make use of any digital encoding instead it uses PSK (Phase shift keying) encoding.
4. The signals can be travelled in both the direction in baseband transmission whereas in broadband transmission the signals can travel in only one direction.
5. In baseband transmission, the signals cover shorter distances because at higher frequencies the attenuation is most pronounced which make a signal to travel short distances without reducing its power. As against, in broadband signals, the signals can be travelled at longer distances.

Wireless networks

Wireless networks use radio waves to connect devices such as laptops to the Internet, the business network and applications. When laptops are connected to Wi-Fi hot spots in public places, the connection is established to that business's wireless network.

There are four main types of wireless networks:

- Wireless Local Area Network (LAN): Links two or more devices using a wireless distribution method, providing a connection through access points to the wider Internet.
- Wireless Metropolitan Area Networks (MAN): Connects several wireless

LANs.

- Wireless Wide Area Network (WAN): Covers large areas such as neighboring towns and cities.
- Wireless Personal Area Network (PAN): Interconnects devices in a short span, generally within a person's reach.
- Here is simple explanation of how it works, let say you have 2 computers each equipped with wireless adapter and you have set up wireless router. When the computer send out the data, the binary data will be encoded to radio frequency and transmitted via wireless router. The receiving computer will then decode the signal back to binary data.
- It doesn't matter you are using broadband cable/DSL modem to access internet, both ways will work with wireless network. If you heard about **wireless hotspot**, that means that location is equipped with wireless devices for you and others to join the network.
- The two main components are **wireless router or access point** and **wireless clients**.
- If you have not set up any wired network, then just get a wireless router and attach it to cable or DSL modem. You then set up wireless client by adding wireless card to each computer and form a simple wireless network. You can also cable connect computer directly to router if there are switch ports available.

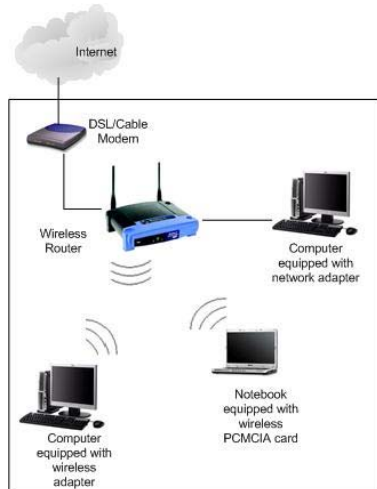


Fig: Wireless Networks

- If you already have wired Ethernet network at home, you can attach a wireless access point to existing network router and have wireless access at home.

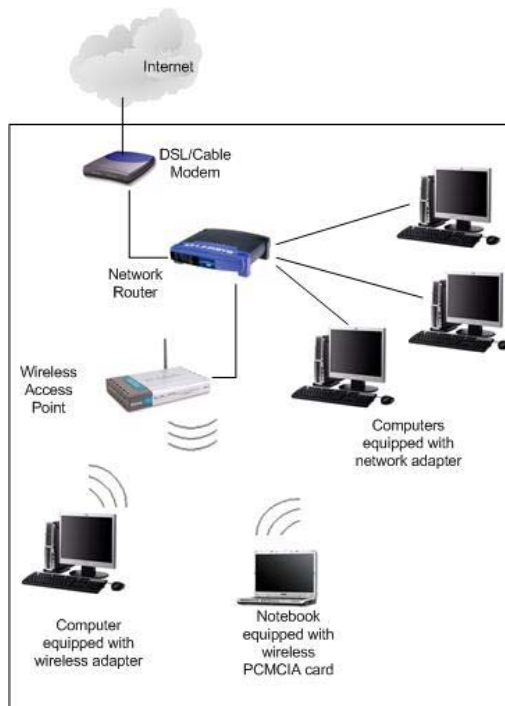


Fig: Wireless Access

- Wireless router or access points should be installed in a way that maximizes coverage as well as throughput. The coverage provided is generally referred to as the coverage cell. Large areas usually require more than one access point in order to have adequate coverage. You can also add access point to your existing wireless router to improve coverage.

Physical Layer Device

Hub

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.



Fig: Hub

Types of Hub

- **Active Hub:** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
- **Passive Hub:** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.
- **Repeater:** A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.



Fig: Repeater

- **Switch** – A switch is a multi-port bridge with a buffer and a design that can boost its efficiency (large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.



Fig: Switch

Disaster recovery (DR)

Disaster recovery (DR) is an area of security planning that aims to protect an organization from the effects of significant negative events. DR allows an organization to maintain or quickly resume mission-critical functions following a disaster.

A disaster can be anything that puts an organization's operations at risk, from a cyberattack to equipment failures to natural disasters. The goal with DR is for a business to continue operating as close to normal as possible. The disaster recovery process includes planning and testing and may involve a separate physical site for restoring operations.

The importance of disaster recovery: RPO and RTO

As businesses have become more reliant on high availability, the tolerance for downtime has decreased. A disaster can have a devastating effect on a business. Studies have shown that many businesses fail after experiencing a significant data loss, but DR can help. Recovery point objective (RPO) and recovery time objective (RTO) are two important measurements in disaster recovery and downtime. RPO is the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster. The recovery point objective determines the minimum frequency of backups. For example, if an organization has an RPO of four hours, the system must back up at least every four hours.

RTO is the maximum amount of time, following a disaster, for an organization to recover files from backup storage and resume normal operations. In other words, the recovery time objective is the maximum amount of downtime an organization can handle. If an organization has an RTO of two hours, it cannot be down for longer than that. The RPO and RTO help administrators choose optimal disaster

recovery strategies, technologies and procedures.

Meeting tighter RTO windows requires positioning secondary data so that it can be accessed faster. Recovery-in-place is one method of restoring data more quickly. This technology moves backup data to a live state on the backup appliance, eliminating the need to move data across a network. It can protect against storage system and server failure. Before using recovery-in-place, an organization needs to consider the performance of the disk backup appliance, the time needed to move data from a backup state to a live state, and failback. Since recovery-in-place can take up to 15 minutes, an organization may need to perform replication if it wants a quicker recovery time.

Preparing for a disaster requires a comprehensive approach that encompasses hardware and software, networking equipment, power, connectivity and testing that ensures DR is achievable within RTO and RPO targets. While implementing a thorough DR plan isn't a small task, the potential benefits are significant.

Disaster recovery planning and strategy

A disaster recovery plan provides a structured approach for responding to unplanned incidents that threaten a company's IT infrastructure, including hardware and software, networks, procedures and people. The plan provides step-by-step disaster recovery strategies for recovering disrupted systems and networks to minimize negative impacts to company operations. A risk assessment identifies potential threats to the IT infrastructure; the DR plan outlines how to recover the elements that are most important to the company. According to independent consultant Paul Kirvan, the components needed in a DR plan include the following:

- A disaster recovery policy statement, plan overview and main goals of the plan.
- Key personnel and DR team contact information.
- Description of emergency response actions immediately following an incident.
- A diagram of the entire network and recovery site.
- Directions for how to reach the recovery site.

- A list of software and systems that will be used in the recovery.
- Sample templates for a variety of technology recoveries, including technical documentation from vendors.
- Tips for dealing with the media.
- Summary of insurance coverage.
- Proposed actions for dealing with financial and legal issues.
- Ready-to-use forms to help complete the plan.

According to Kirvan, the development team should include the following activities when creating their DR plan:

- Meet with the internal technology team and network administrator to establish the scope of the plan, and then brief senior management on the meeting.
- Gather all of the relevant network infrastructure documents.
- Identify the most serious threats and vulnerabilities to the infrastructure.
- Review the previous history of outages and disruptions and how the business handled them.
- Identify the most critical IT assets and determine their maximum outage time.
- Identify the emergency response team and its capabilities.
- Have management review the plan.
- Test the plan and update it if necessary.
- Schedule the next review/audit of disaster recovery capabilities.

An organization should consider its disaster recovery plan a living document. The DR plan needs scheduled reviews and updates to ensure it is accurate and will work if a recovery is required. The plan should also be updated whenever there are changes in the business that could affect disaster recovery.

Risk of Data

Organizations in current times are competing in a global market where time and distance have no meaning. Competition being intense, companies have got to ensure that they delivery top line performance all the time and not risk any kind of failures. Disaster Recovery and Business Continuity planning concept has come of age in the new world.

The concepts of risk analysis and mitigation are relevant to all areas of business and scales of organizations. However, the concept has gained ground more in the IT and service industry where in the risk of failure of IT systems can be disastrous for the company.

Every Organization big or small engages in a lot of IT systems and Communication tools. From desktops, laptops, servers to all sorts of other peripheral equipments, softwares, applications, databases as well as extensive Email and communication networks make up the operational backbone of each and every company.

The data that the Companies have in their system including customer details, financial data as well as other operational data including sales, purchase, inventory and other operations is invaluable. Any loss of data can seriously hamper the business operations and cause huge losses to the Organization.

IT systems are known to possess very high risk of failure. The causes of systems failures can be many. The equipment's being highly sensitive to power fluctuations, any disruption or fluctuation of power can cause damage or destroy the data. Imagine a bank losing the data of the transactions in their accounts. Imagine an Organization losing its financial data. These are unthinkable but probable.

Types of Risks to IT Systems:

IT systems can fall prey to several categories of risks. Some of the common areas of disaster are:

1. Virus attack - Inadequate protection in terms of firewall and other barriers to the internal systems can make the entire system vulnerable to virus attacks through the internet which can harm the internal systems and destroying or corrupting data.
2. Risk of systems failure and communication network failure due to power fluctuations and absence of effective UPS protection.
3. Hardware or LAN Failure.
4. Loss of data due to inadequate backup facility or procedure.
5. Poorly trained, poorly skilled IT staff that lack sufficient knowledge.
6. Overdependence on outsourced vendor and their staff.

7. Poor IT management practices and lack of proper processes for storage and backup of data in all areas of business.
8. Inadequate use of anti-virus package for protection.
9. Lack of facilities and keeping IT systems in poor environments that are not conducive to the system hardware and performance.

Apart from the above, there can be several and many more risks that are associated with IT systems failures. Of the above, the power related failures and the over dependence upon outsourced vendors and manpower happen to be the most common occurrence events resulting in loss of data in Organizations. In many organizations there seems to be a general lack of seriousness in planning and keeping regular backups in place.

Whatever be the nature of the risk or occurrence, the data loss can create major impact on the business of the Organization. Companies like credit card companies, banks and other service organizations cannot afford to lose any data. Therefore, protecting their data calls for adequate investments in protection methods as well as in planning and maintaining a good Disaster Recovery backup plan.

Backup methods devices and media

Data is essential for running an organization, and it is certainly the central component of any business continuity plan. Without immediate and constant access to data, your business will come to a grinding halt. Worse still, in the event of a disaster you could risk losing valuable data if you don't have a backup strategy in place. Backing up data should be at the top of your list of priorities, so here are some devices you can use to protect your data. There's no one-size-fits-all solution when it comes to data backups. You'll want to consider the pros and cons of each of the backup devices below before making a purchase.

USB stick

USB flash drives are basically miniature hard drives that you connect to your computer using a USB port. The drives are extremely cheap, with prices depending on their capacity. They're also portable and can be used to backup information from several computers to the same drive. Although, USB sticks are highly convenient,

they're still not a complete backup solution, and are best suited for intermediate backups, such as storing file recovery programs or critical business documents.

External hard drive

An external hard drive is perfect when used as backup storage media. It has the lowest cost per gigabyte when compared to the other backup devices out there. External hard drives use the same plug-and-play functionality as USB sticks, so you can plug the drive into your computer and immediately start selecting the files you want to backup. The transfer rate is also very fast, and you can backup a large amount of data within seconds. One of the evident drawbacks of using an external hard drive is that you'll need to update your backups on a regular basis, or else new files won't be included. There's also the risk of the device being stolen or misused. For instance, a colleague may take your drive when you're away from your desk, or a disgruntled employee may copy all of your important business files and take it with them when quitting.

Network attached storage

Network attached storage, or NAS for short, is a dedicated device with its own IP address. It can be used as a multimedia server and can function as an email or lightweight database server. NAS offers data redundancy, meaning it will generate a backup of your backups, so you can ensure your files are fully protected.

The main downside of NAS is its inability to scale beyond the limits of the system; you have to purchase additional hard drive bays when you need more capacity. You also have to take full responsibility for data security if you're implementing NAS.

Cloud storage

Cloud storage is becoming more and more popular among businesses of all sizes, due to its many benefits such as allowing users to access data anywhere on smartphone devices, as well as enabling you to work with the most current hardware and up-to-date software. It is also affordable, since you'll only have to pay for what you use. What's more, cloud computing is very convenient, because your service provider will take care of the installation, management, and maintenance processes. On the downside, some cloud service providers don't employ sufficient

security measures on their systems, so your data could be exposed to potential cybersecurity threats. This means that it is not always the ideal solution for companies dealing with very sensitive data – medical practices and law firms, for example. Predicting costs can also be hard; if your business is growing rapidly, then you might find you have not adequately planned for incremental costs. Choosing the best system for backup is a critical decision that will impact your business on a daily basis. There are trade-offs among backup devices, which is why you need to choose the solution – or solutions – best suited to your business. Contact us today and our experts will assess your company’s needs and provide the best backup solutions for you.

Backup Schedule

The backup schedule determines how often your data is backed up and the backup media you will require. Each hardware type has a different group of rotation schemes to select from, including industry standard strategies. Each scheme can also be customized once the job has been created. Customization includes scheduling differential, incremental and transaction log backups. Depending on the backup type you have selected, you can configure your job to run multiple times each day. This is useful if your data changes frequently throughout the day and you want to be able to restore from multiple points in time.

New Agent Backup Job

Schedule
Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Job Mode Run the job automatically

Name Daily at this time: 10:00 PM Everyday Days...
 Monthly at this time: 10:00 PM Fourth Saturday Months...
 Periodically every: 1 Hours Schedule...
 After this job: Windows Servers Backup (Backup Job for Windows Servers)

Automatic retry

Retry failed items processing: 3 times
 Wait before each retry attempt for: 10 minutes

Backup window

Terminate job if it exceeds allowed backup window Window...
 If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

< Previous Apply Finish Cancel

We recommend choosing a schedule that will give you a rich backup history with multiple points of restore, as well as off-site storage. Usually, after data loss, the most recent backup available is used. All good rotation schemes should allow you to restore from the previous working day. Sometimes, however, data loss may not be discovered for days or weeks after it occurs. To allow for this your schedule should allow you to restore data from previous weeks, months and even years. This is best achieved by archiving your data. Archived data is stored permanently, preferably offsite in a secure location, on portable media (external HDD, tape, etc) that is never overwritten. For example, we recommended that yearly and quarterly media be archived; that way, data will be available for many years to come.

Typically, the better protection a scheme provides, the more backup media you will require. You can choose from a variety of backup schemes depending on your requirements and the backup media you have available. Once the scheme has been selected and configured, you can view the Calendar to confirm that the correct schedule has been set up.

1. Select a scheme from the left-hand menu under **Select scheme**.
2. A media pool diagram will appear to the right of the screen which outlines what the selected rotation strategy involves.



- Portable media example (tape, external hard drive, optical disc, REV, and so on):
- The media pool diagram for the *Professional* scheme shows that a total of 14 separate backup tapes are required: 4 daily, 4 weekly, 2 monthly, 3 quarterly, and 1 yearly.

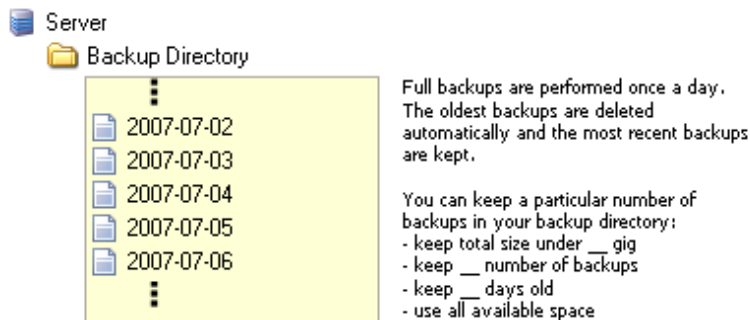
An icon at the top-right of each colored square indicates how the media should be rotated and stored (e.g. Monthly tapes (in the green square) should be stored offsite after the backup completes and be brought onsite when next required; a yearly tape, however, should be permanently stored offsite after being backed up to and a new

tape should be purchased for the following yearly backup).

The label for each tape is indicated on the diagram (e.g. Tuesday, Week 2, Month 2) and these labels should be physically written on each tape so that they can be readily identified when required.

- **Fixed destination example (NAS, local folder, etc.):**

The media pool diagram for the *Most Recent Full* NAS rotation scheme shows how backup files will be bestored on the NAS. The diagram indicates that a separate backup file, with a date-based filename, will be written to the backup directory each day. During the next step of the job creation you can define how storage space is managed on the backup destination.



- **Mirror example (File Replication/Rsync jobs only)**

When creating a File Replication or Rsync job, depending on the destination you have selected you can select the **Mirror** scheme, which will create an exact replica of your selected files and folders on your backup device each time the backup runs. Only a single mirror will be kept on the backup device. Choose a different scheme if you want to create a series of mirrors to will ensure that you have a greater backup history with multiple restore points.



Once you have selected an appropriate scheme you can specify the time of the day

that the backup should run. If you have multiple jobs scheduled, any jobs that are scheduled to start while another is already running will be placed in a queue and executed as soon as the job currently running finishes.

Data recovery

Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible. In enterprise IT, data recovery typically refers to the restoration of data to a desktop, laptop, server or external storage system from a backup.

Causes of data loss

Most data loss is caused by human error, rather than malicious attacks, according to U.K. statistics released in 2016. In fact, human error accounted for almost two-thirds of the incidents reported to the U.K. Information Commissioner's Office. The most common type of breach occurred when someone sent data to the wrong person. Other common causes of data loss include power outages, natural disasters, equipment failures or malfunctions, accidental deletion of data, unintentionally formatting a hard drive, damaged hard drive read/write heads, software crashes, logical errors, firmware corruption, continued use of a computer after signs of failure, physical damage to hard drives, laptop theft, and spilling coffee or water on a computer.

How data recovery works

The data recovery process varies, depending on the circumstances of the data loss, the data recovery software used to create the backup and the backup target media. For example, many desktop and laptop backup software platforms allow users to restore lost files themselves, while restoration of a corrupted database from a tape backup is a more complicated process that requires IT intervention. Data recovery services can also be used to retrieve files that were not backed up and accidentally deleted from a computer's file system, but still remain on the hard disk in fragments. Data recovery is possible because a file and the information about that file are stored in different places. For example, the Windows operating system uses a file allocation table to track which files are on the hard drive and where they are

stored. The allocation table is like a book's table of contents, while the actual files on the hard drive are like the pages in the book.

When data needs to be recovered, it's usually only the file allocation table that's not working properly. The actual file to be recovered may still be on the hard drive in flawless condition. If the file still exists -- and it is not damaged or encrypted -- it can be recovered. If the file is damaged, missing or encrypted, there are other ways of recovering it. If the file is physically damaged, it can still be reconstructed. Many applications, such as Microsoft Office, put uniform headers at the beginning of files to designate that they belong to that application. Some utilities can be used to reconstruct the file headers manually, so at least some of the file can be recovered.

Most data recovery processes combine technologies, so organizations aren't solely recovering data by tape. Recovering core applications and data from tape takes time, and you may need to access your data immediately after a disaster. There are also risks involved with transporting tapes.

In addition, not all production data at a remote location may be needed to resume operations. Therefore, it's wise to identify what can be left behind and what data must be recovered.

Data recovery techniques

Instant recovery, also known as *recovery in place*, tries to eliminate the recovery window by redirecting user workloads to the backup server. A snapshot is created so the backup remains in a pristine state and all user write operations are redirected to that snapshot; users then work off the backup virtual machine (VM) and the recovery process begins in the background. Users have no idea the recovery is taking place, and once the recovery is complete, the user workload is redirected back to the original VM.

One way to avoid the time-consuming and costly process of data recovery is to prevent the data loss from ever taking place. Data loss prevention (DLP) products help companies identify and stop data leaks and come in two versions: stand-alone and integrated.

- Stand-alone DLP products can reside on specialized appliances or be sold as

software.

- Integrated DLP products are usually found on perimeter security gateways and are useful for detecting sensitive data at rest and in motion.

Unlike stand-alone data loss prevention products, integrated DLP products usually do not share the same management consoles, policy management engines and data storage.

Unit: 9

Network Troubleshoot

Objectives

- To identify the basic tools network troubleshoot and apply them.

Learning Process and Study Materials

- Class demonstration and practical
- Group discussion
- Project work

Content's Elaboration

Network Troubleshoot

The process of troubleshooting your network involves a methodology that starts with cabling and works through the OSI model to the application layer. The network devices have a network cable that terminates at a wired switch. Cabling is a source of a lot of network problems.

The key with troubleshooting is to determine what has changed. Sometimes it is hardware that isn't working or some change was made such as new software, configured equipment or additional employees stressing the network. It could be a specific issue or several problems. Start with the client adapter, determine the specific symptoms and go from there.

The following is a series of questions that can be used as a guideline during the troubleshooting process:

1. Can you ping the switch IP address?
2. Can you ping the router?
3. Can you ping the DHCP server?
4. Does the client obtain an IP address?
5. Is the WAN circuit available?
6. Has new software been installed on the client or server?
7. Do all clients experience the problem?

8. Is it random or a specific pattern?
9. Is the problem server specific or application specific?
10. Is the DNS server IP address setting correct?
11. Is there a firewall that is filtering traffic?
12. Ran trace route and examined routing behavior?

Tools

1. Windows control panel shows network adapter settings, firewall configuration etc.
2. Ping and traceroute will verify that network routing is working.
3. Examine the ARP table on the desktop, switch and router confirming the device MAC address is there.
4. Network packet sniffers examine packet information such as protocols, filtered programs or errors with applications.
5. Verify change management activities and determine what if any device was changed and how.
6. Show interfaces at the router will reveal any interface errors pointing to a cable or hardware problem.
7. Examine router interface utilization patterns.

Working from the cable level and determining if the problem is affecting a single user, a department, building or city wide is a good place to start. A citywide problem sometimes indicates a data center outage. A building sometimes points to a circuit, router or primary switch. A department can indicate a problem with their network switch or fiber cabling. The single user problem could be a myriad of issues from a bad cable to network permissions. Because companies have in some cases hundreds of applications, network switches and routers the problem becomes more complex when it is a cross department issue. Not all employees have the same network permissions and use a variety of applications across departments, cities and countries.

Determining who is affected by the problem can be a key factor in resolving the issue. The ping is a popular tool since it verifies to the network layer all is working. In that case you're then focusing on application issues although not always.

Traceroute verifies how packets are traveling between source and destination. You could have packets using non-optimal routing paths that are causing performance problems.

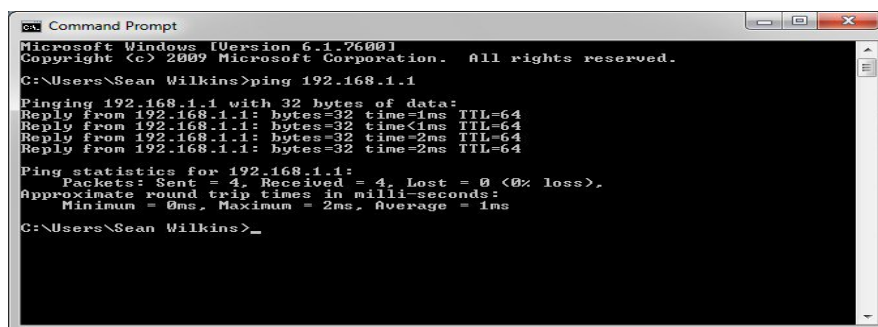
Some Basics Tools use in Network Troubleshoot

Network troubleshooting tools are a necessity for every network administrator. When getting started in the networking field, it is important to amass a number of tools that can be used to troubleshoot a variety of different network conditions.

While it is true that the use of specific tools can be subjective and at the discretion of the engineer, the selection of tools in this article has been made based on their generality and common use. This article reviews the top 10 basic tools that can help you troubleshoot most networking issues.

1. Ping

The most commonly used network tool is the ping utility. This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host. Simply stated, if the requesting host receives a response from the destination host, this host is reachable. This utility is commonly used to provide a basic picture of where a specific networking problem may exist. For example, if an Internet connection is down at an office, the ping utility can be used to figure out whether the problem exists within the office or within the network of the Internet provider. Figure 1 below shows an example of the ping utility being used to obtain the reachability status of the locally connected router.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Sean Wilkins>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

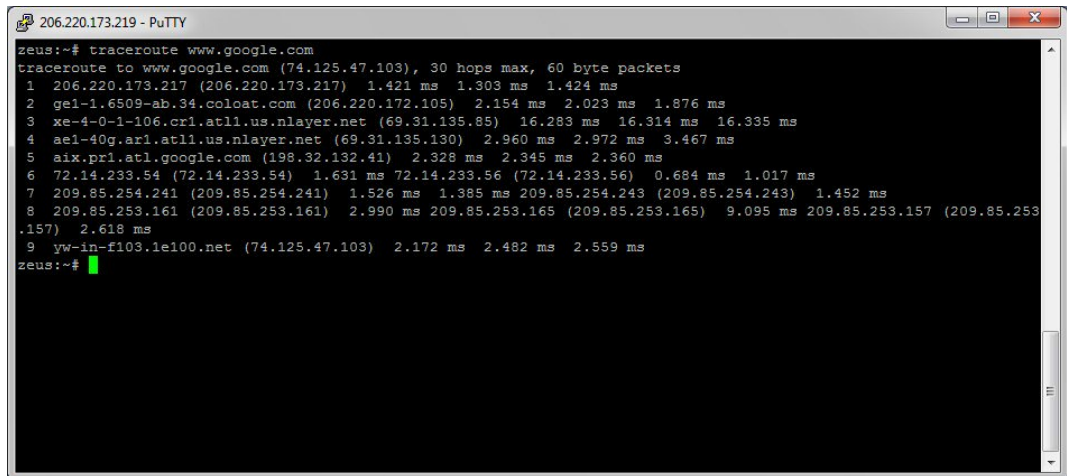
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\Sean Wilkins>_
```

Fig: Ping utility

2. Tracert/traceroute

Typically, once the ping utility has been used to determine basic connectivity, the tracert/traceroute utility can be used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts. Figure 2 below shows an example of the tracert utility being used to find the path from a host inside an office to www.google.com. The tracert utility and traceroute utilities perform the same function but operate on different operating systems, Tracert for Windows machines and traceroute for Linux/*nix-based machines.



```
206.220.173.219 - PuTTY
zeus:~# traceroute www.google.com
traceroute to www.google.com (74.125.47.103), 30 hops max, 60 byte packets
 1 206.220.173.217 (206.220.173.217)  1.421 ms  1.303 ms  1.424 ms
 2  ge1-1.6509-ab.34.coloat.com (206.220.172.105)  2.154 ms  2.023 ms  1.876 ms
 3  xe-4-0-1-106.crl.atl1.us.nlayer.net (69.31.135.85)  16.283 ms  16.314 ms  16.335 ms
 4  ae1-40g.ar1.atl1.us.nlayer.net (69.31.135.130)  2.960 ms  2.972 ms  3.467 ms
 5  aix.prl.atl1.google.com (198.32.132.41)  2.328 ms  2.345 ms  2.360 ms
 6  72.14.233.54 (72.14.233.54)  1.631 ms  72.14.233.56 (72.14.233.56)  0.684 ms  1.017 ms
 7  209.85.254.241 (209.85.254.241)  1.526 ms  1.385 ms  209.85.254.243 (209.85.254.243)  1.452 ms
 8  209.85.253.161 (209.85.253.161)  2.990 ms  209.85.253.165 (209.85.253.165)  9.095 ms  209.85.253.157 (209.85.253.157)  2.618 ms
 9  yw-in-f103.1e100.net (74.125.47.103)  2.172 ms  2.482 ms  2.559 ms
zeus:~#
```

Fig: Tracert/traceroute utility

3. Ipconfig/ifconfig

One of the most important things that must be completed when troubleshooting a networking issue is to find out the specific IP configuration of the variously affected hosts. Sometimes this information is already known when addressing is configured statically, but when a dynamic addressing method is used, the IP address of each host can potentially change often. The utilities that can be used to find out this IP configuration information include the ipconfig utility on Windows machines and the ifconfig utility on Linux/*nix based machines. Figure 3 below shows an example of the ifconfig utility showing the IP configuration information of a queries host.

```
zeus:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:84:63
         inet addr:206.220.173.219  Bcast:206.220.173.223  Mask:255.255.255.248
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:1114578  errors:0  dropped:0  overruns:0  frame:0
         TX packets:1008426  errors:0  dropped:0  overruns:0  carrier:0
         collisions:0  txqueuelen:1000
         RX bytes:389028395 (371.0 MiB)  TX bytes:610687218 (582.3 MiB)

eth0:1    Link encap:Ethernet  HWaddr 08:00:27:59:84:63
         inet addr:206.220.173.220  Bcast:206.220.173.223  Mask:255.255.255.248
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0:2    Link encap:Ethernet  HWaddr 08:00:27:59:84:63
         inet addr:206.220.173.221  Bcast:206.220.173.223  Mask:255.255.255.248
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         UP LOOPBACK RUNNING  MTU:16436  Metric:1
         RX packets:2392075  errors:0  dropped:0  overruns:0  frame:0
         TX packets:2392075  errors:0  dropped:0  overruns:0  carrier:0
         collisions:0  txqueuelen:0
         RX bytes:1471173328 (1.3 GiB)  TX bytes:1471173328 (1.3 GiB)

zeus:~#
```

Fig: ifconfig utility

4. Nslookup

Some of the most common networking issues revolve around issues with Dynamic Name System (DNS) address resolution issues. DNS is used by everyone using the Internet to resolve commonly known domain names (i.e. google.com) to commonly unknown IP addresses (i.e. 74.125.115.147). When this system does not work, most of the functionality that people are used to goes away, as there is no way to resolve this information. The nslookup utility can be used to lookup the specific IP address(es) associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue. Along with simple lookup, the nslookup utility is able to query specific DNS servers to determine an issue with the default DNS servers configured on a host. Figure 4 below shows an example of how the nslookup utility can be used to query the associated IP address information.

```
zeus:~# nslookup www.google.com
Server:      127.0.0.1
Address:     127.0.0.1#53

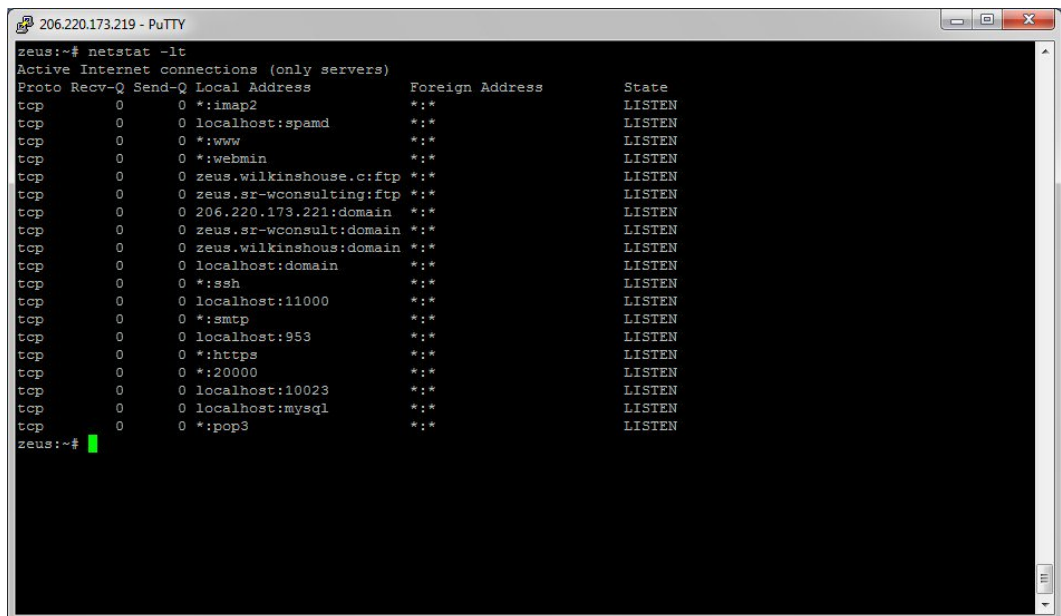
Non-authoritative answer:
www.google.com canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 74.125.47.99
Name:   www.l.google.com
Address: 74.125.47.103
Name:   www.l.google.com
Address: 74.125.47.104
Name:   www.l.google.com
Address: 74.125.47.105
Name:   www.l.google.com
Address: 74.125.47.106
Name:   www.l.google.com
Address: 74.125.47.147

zeus:~#
```

Fig: Nslookup utility

5. Netstat

Often, one of the things that are required to be figured out is the current state of the active network connections on a host. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port. It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports. Figure 5 below shows an example of the netstat utility being used to display the currently active ports on a Linux machine.



```
zeus:~# netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 *:imap2                 **                       LISTEN
tcp      0      0 localhost:spamd         **                       LISTEN
tcp      0      0 *:www                   **                       LISTEN
tcp      0      0 *:webmin                 **                       LISTEN
tcp      0      0 zeus.wilkinshouse.c:ftp **                       LISTEN
tcp      0      0 zeus.sr-wconsulting:ftp **                       LISTEN
tcp      0      0 206.220.173.221:domain **                       LISTEN
tcp      0      0 zeus.sr-wconsult:domain **                       LISTEN
tcp      0      0 zeus.wilkinshous:domain **                       LISTEN
tcp      0      0 localhost:domain       **                       LISTEN
tcp      0      0 *:ssh                    **                       LISTEN
tcp      0      0 localhost:11000         **                       LISTEN
tcp      0      0 *:smtp                   **                       LISTEN
tcp      0      0 localhost:953           **                       LISTEN
tcp      0      0 *:https                  **                       LISTEN
tcp      0      0 *:20000                  **                       LISTEN
tcp      0      0 localhost:10023         **                       LISTEN
tcp      0      0 localhost:mysql         **                       LISTEN
tcp      0      0 *:pop3                   **                       LISTEN
zeus:~#
```

Fig: Netstat utility

6. PuTTY/Tera Term

When connecting to a variety of different types of equipment, a telnet, SSH or serial client is required; when this is required both the puTTY and Tera Term programs are able to provide these functionalities. The selection of one over the other is strictly a personal preference. Figures 6 and 7 below show both puTTY and Tera Term being used to connect to a host via SSH.

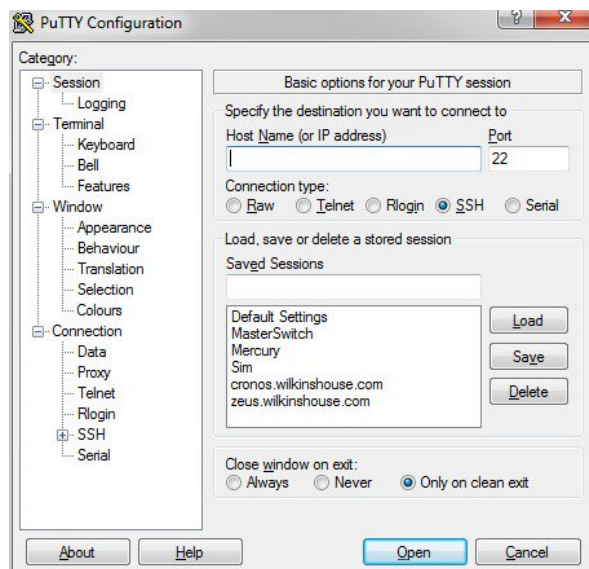


Fig: PuTTY

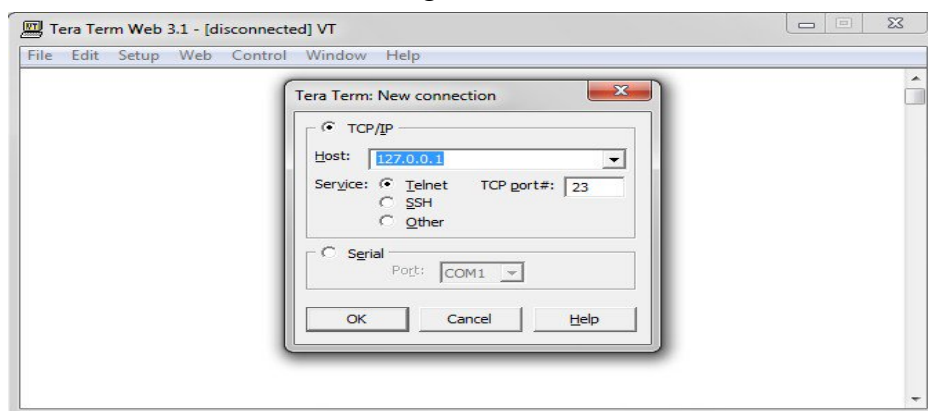


Fig: Tera Term

7. Subnet and IP Calculator

One of the most important tools in the belt of a junior network engineer is an IP network calculator. These can be used to ensure a correct IP address selection and with this a correct IP address configuration. While this type of tool is used by senior level network engineers, much of the information obtained from the tool becomes simpler to calculate the longer and more experience you have in the field. Two of the more commonly used free IP calculators include Wildpackets (Bitcricket) Network Calculator and SolarWinds Advanced Subnet Calculator which can be found at the links below.

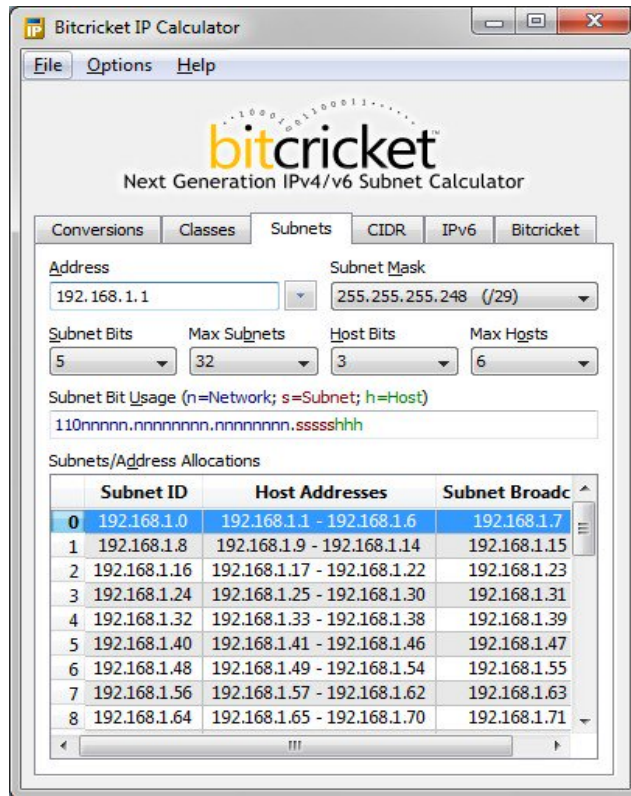


Fig:Subnet calculator

8. Speedtest.net/pingtest.net

A very easy test that can be used to both determine the Internet bandwidth available to a specific host and to determine the quality of an Internet connection is the use of the tools available at the speedtest.net and pingtest.net websites. The speedtest.net site provides the ability to determine the amount of bandwidth that is available to a specific host at a specific point in time; this is often a good tool to use when measuring how long it is going to take to upload or download information from a local to remote host. This measurement can also be used to determine whether the connection is offering the amount of bandwidth that was purchased from the Internet provider; keep in mind however that some amount of bandwidth difference is expected between the quoted bandwidth purchased and the measured bandwidth. The pingtest.net website is used to determine the quality of the connection by measuring the ping response times and jitter amounts over a short

period of time. This information can be used to determine a likelihood of how well the measured connection will deal with certain types of high demand traffic like Voice over IP (VoIP) or gaming. Figure 9 and 10 below show example output from both of these sites.

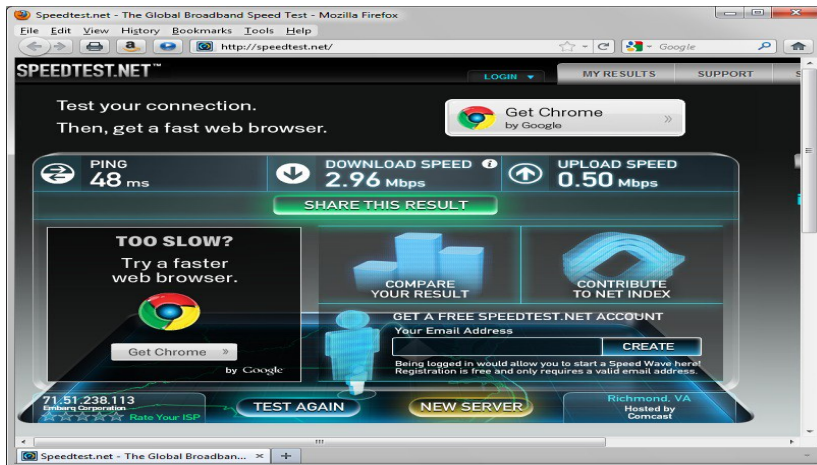


Fig: Speedtest



Fig: PingTest

9. Pathping/mtr

In an effort to take advantage of the benefits of both the ping and tracert/traceroute commands, the pathping and mtr utilities were developed. Both of these tools take the functionality and information that can be obtained from these types of tools and provide a more detailed single picture of the path characteristics from a specific host to a specific destination. Figure 11 and 12 below show examples of these two tools and what information they provide.

```

C:\Users\Sean Wilkins>pathping www.google.com
Tracing route to www.l.google.com [74.125.93.105]
over a maximum of 30 hops:
 0  seansdell [192.168.1.101]
 1  192.168.1.1
 2  192.168.100.2
 3  10.10.10.1
 4  nc-71-52-136-1.dhcp.embarqhsd.net [71.52.136.1]
 5  nc-69-69-52-245.sta.embarqhsd.net [69.69.52.245]
 6  host.lightcore.net [208.110.248.125]
 7  bb-rcntncxa-jx9-02-ae0.core.centurytel.net [208.110.248.66]
 8  bb-asbnvacv-jx9-02-ae3.0.core.centurytel.net [208.110.248.170]
 9  bb-asbnvacv-jx9-01-ae0.0.core.centurytel.net [208.110.248.117]
10  72.14.219.254
11  216.239.48.112
12  209.85.248.75
13  209.85.254.237
14  64.233.175.14
15  qw-in-f105.1e100.net [74.125.93.105]

Computing statistics for 375 seconds...
Source to Here          This Node/Link
Hop  RTT      Lost/Sent = Pct      Lost/Sent = Pct      Address
 0          0/ 100 = 0%          0/ 100 = 0%          seansdell [192.168.1.101]
 1    5ms     0/ 100 = 0%          0/ 100 = 0%          192.168.1.1
 2   17ms    0/ 100 = 0%          0/ 100 = 0%          192.168.100.2
 3   20ms    0/ 100 = 0%          0/ 100 = 0%          10.10.10.1
 4   91ms    0/ 100 = 0%          0/ 100 = 0%          |
 5  [71.52.136.1] 0/ 100 = 0%          0/ 100 = 0%          nc-71-52-136-1.dhcp.embarqhsd.net
 6  [69.69.52.245] 0/ 100 = 0%          0/ 100 = 0%          nc-69-69-52-245.sta.embarqhsd.net
 7   96ms    0/ 100 = 0%          0/ 100 = 0%          |
 8   101ms   0/ 100 = 0%          0/ 100 = 0%          host.lightcore.net [208.110.248.125]
 9   108ms   0/ 100 = 0%          0/ 100 = 0%          |
10   114ms   0/ 100 = 0%          0/ 100 = 0%          bb-rcntncxa-jx9-02-ae0.core.centurytel.net [208.110.248.66]
11   119ms   0/ 100 = 0%          0/ 100 = 0%          |
12   112ms   0/ 100 = 0%          0/ 100 = 0%          bb-asbnvacv-jx9-02-ae3.0.core.centurytel.net [208.110.248.170]
13   114ms   0/ 100 = 0%          0/ 100 = 0%          |
14   121ms   0/ 100 = 0%          0/ 100 = 0%          bb-asbnvacv-jx9-01-ae0.0.core.centurytel.net [208.110.248.117]
15   116ms   0/ 100 = 0%          0/ 100 = 0%          |
16          0/ 100 = 0%          0/ 100 = 0%          72.14.219.254
17          0/ 100 = 0%          0/ 100 = 0%          216.239.48.112
18          0/ 100 = 0%          0/ 100 = 0%          209.85.248.75
19          0/ 100 = 0%          0/ 100 = 0%          |
20          0/ 100 = 0%          0/ 100 = 0%          209.85.254.237
21          0/ 100 = 0%          0/ 100 = 0%          |
22          0/ 100 = 0%          0/ 100 = 0%          64.233.175.14
23          0/ 100 = 0%          0/ 100 = 0%          |
24          0/ 100 = 0%          0/ 100 = 0%          qw-in-f105.1e100.net [74.125.93.105]
  
```

Fig: Pathping

```

206.220.173.219 - PuTTY
My traceroute [v0.80]
zeus.wilkinshouse.com (0.0.0.0) Sun May 29 21:41:06 2011
Help Display mode Restart statistics Order of fields quit

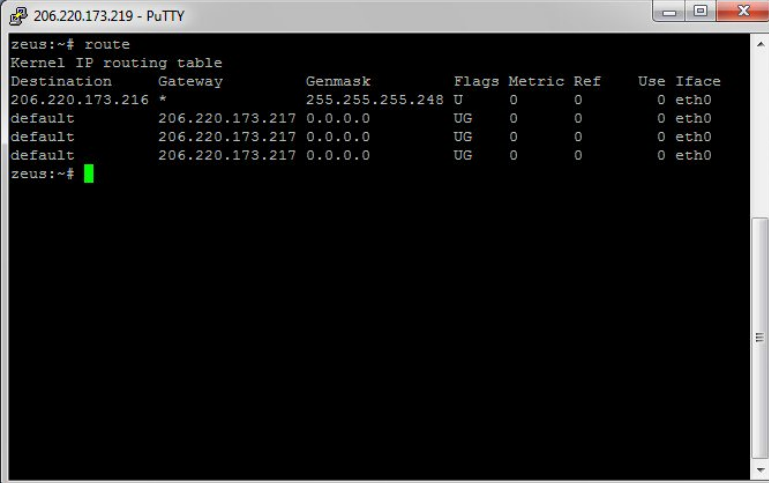
Host
1. 206.220.173.217
2. gcl-1.6509-ab.34.coload.com
3. xe-4-0-1-106.cri.atl1.us.nlayer.net
4. ae1-407.cri.atl1.us.nlayer.net
5. aik.pri.atl1.google.com
6. 72.14.233.56
7. 209.85.254.241
  209.85.254.243
8. 209.85.253.157
  209.85.253.161
  209.85.253.169
  209.85.253.165
9. yw-in-f105.1e100.net

Packets          Pings
Loss% Snt  Last  Avg Best Wrst StDev
1. 0.0% 30  2.0  1.0 0.6 3.0 0.6
2. 0.0% 30  1.2  1.1 0.7 5.7 0.9
3. 0.0% 30  0.9  3.2 0.6 53.1 9.8
4. 0.0% 30  2.4  3.3 2.1 20.0 1.7
5. 0.0% 30  0.8  3.8 0.6 42.4 9.5
6. 0.0% 30 13.3  6.8 0.9 113.4 20.8
7. 0.0% 30  1.3  3.2  1.2 40.9  7.4
8. 0.0% 29  1.5  6.2  1.5 15.9  4.4
9. 0.0% 29  1.7  1.7  1.5  2.4  0.2
  
```

Fig: Mtr

10. Route

The last of the tools covered in this article is the route utility. This utility is used to display the current status of the routing table on a host. While the use of the route utility is limited in common situations where the host only has a single IP address with a single gateway, it is vital in other situations where multiple IP address and multiple gateways are available. Figure 13 below shows an example of the route utility being used on a Windows machine.



```
zeus:~# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
206.220.173.216 * 255.255.255.248 U 0 0 0 eth0
default 206.220.173.217 0.0.0.0 UG 0 0 0 eth0
default 206.220.173.217 0.0.0.0 UG 0 0 0 eth0
default 206.220.173.217 0.0.0.0 UG 0 0 0 eth0
zeus:~#
```

Fig: Route Utility

Key points

As with any job, the type of tools that are quickly available can greatly influence the amount of time that it takes to complete a job. When troubleshooting a networking issue, the amount of time that it takes to find and fix a problem directly affect the wasted costs that it causes to any system relying on the network. This article has taken a look at the 10 most commonly used tools that can help in ensuring that the time that it takes to find and fix a problem is as short as possible. I hope the information in this article can be helpful in future troubleshooting.

References

<https://www.elprocus.com/different-types-of-modulation-techniques-in-communication-systems/>

<https://www.pluralsight.com/blog/it-ops/network-troubleshooting-tools>

<http://www.bitcricket.com/downloads/IPCalculator.msi>

<http://downloads.solarwinds.com/solarwinds/Release/FreeTool/SolarWinds-Subnet-Calculator.zip>

References:

<https://study.com/academy/lesson/types-of-networks-lan-wan-wlan-man-san-pan-eqn-vpn.html>

<https://www.geeksforgeeks.org/computer-network-types-routing/>

<https://networkchefbd.com/introduction-cisco-packet-tracer-simulator/>

<https://www.managementstudyguide.com/risk-of-data-loss-and-it-system-failures.htm>

<https://searchdisasterrecovery.techtarget.com/definition/data-recovery>