an approach to Internet and Networking.....

# COMPUTER NETWORK AND INTERNET

DR.SUNIL KUMAR VATS

# Computer Network and Internet

**First Edition**

Dr. Sunil Kumar Vats


**IJRTS Publications**

**Crescent ParC, Sector 92, Gurgaon-122001**

**ISBN:** 978-93-5265-353-9

**Price:** 180

Published by Dr. Vipin Mittal for IJRTS Publications, Crescent ParC, Sector 92, Gurgaon-122001

Printed in India

by Manyu Cyber Cafe

Bound in India

By Twarit Print Solution

***Dedicated to my grandparents Late Sh. Radha Krishan & Smt. Bharpi Devi***
***An inspiring source of motivation for me…***

# From the desk of Author…….

Network has a vital role in accessing internet which has played a key and directive role in bringing the international boundaries closer and has proved to be a magnificent medium to turn the earth into a global village. It has revolutionised the dimensions of information technology which with its nano form and rapid accessibility bestows man with immense powers to create more micro and refined media to cater to the prospective generations. When information accompanied with latest technology is channelized in a sophisticated manner, it overcomes the constraints of time and space and helps in accomplishing more challenging assignments and defying enterprises..

My aim in getting this work published is to make huge universe of learners to acquire and be aware of 'Kinley concepts' of IT, Network Security more easily.

**Dr. Sunil Kumar Vats**

# DISCLAIMER

While every effort has been made to ensure that the book is free of error, it is inevitable that some errors still remain. Please report any errors, suggestions or questions to the authors at the following email address.

sunilvats1981@gmail.com

sunilvats27@yahoo.com

# Preface

Networking is one of the most significant steps in the electronic evolution since the invention of the PC. A computer network is a group of connected computers that allow the sharing of information and peripherals. The most basic network is made up of two computers connected by some kind of cable in order to exchange information more quickly and efficiently. A standalone computer is very useful to many businesses, but without a network, those businesses would have to spend twice the amount of money on computerization than they would have to by implementing a network.

A network allows many computers to share peripheral devices such as printers and facsimile machines. The two primary benefits of computer networks are sharing of devices and data. There are two basic types of networks: peer-to-peer and server-based. On a peer-to-peer network, any computer can act as a server to share resources with other machines and as a client to access these resources. On the other hand, server-based networks require a server computer whose job is to respond to requests for services or resources from clients elsewhere on the network. Server-based networks are used in most organizations today. This book help the user to understand the concept, use and security of the Network over Internet. Finally, you'll learn about the conventions used in this book for pointing out special helps like notes, tips, cautions, and references to the data files.

Chapter 1-7 consists of about Network and security on Internet and Glossary is included in the form of Chapter 7.

I would like to thank whole the staff of Jawahar Navodaya Vidyalaya, Mohindergarh for allowing me the chance to teach the computer classes and giving me the freedom I needed to develop these notes. I would also like to acknowledge the influence of my colleagues. The most beautiful proofs and ideas grew out of material that I learned from them.

There are times in such projects when the clock beats you time and again and you run out of energy and you just want to finish it once and for ever. My parents Sh. Pawan Kumar & Smt. Savitari Devi made me endure such times with their unfailing humor and warm wishes with full of mental support and love.

To my wife Smt. Savita Sharma, I owe more than what I can mention. Unintentional love & support of my brother, sister and my twin chaps Abhishek, Abhinav and all other kids helped me profoundly in making this coding script even livelier.

This acknowledgement would not be completed without extending my thanks to my role model Sh. Birbal Singh Dahiya, who helped me clear any doubts that arose during my writing.

Any and all remaining errors or inconsistencies are mine. I will gladly take reader and user feedback to correct them, along with other suggestions to improve the text.

Dr. Sunil Kumar Vats *(MCA, PhD)*

PGT Computer Science

Jawahar Navodaya Vidyalaya

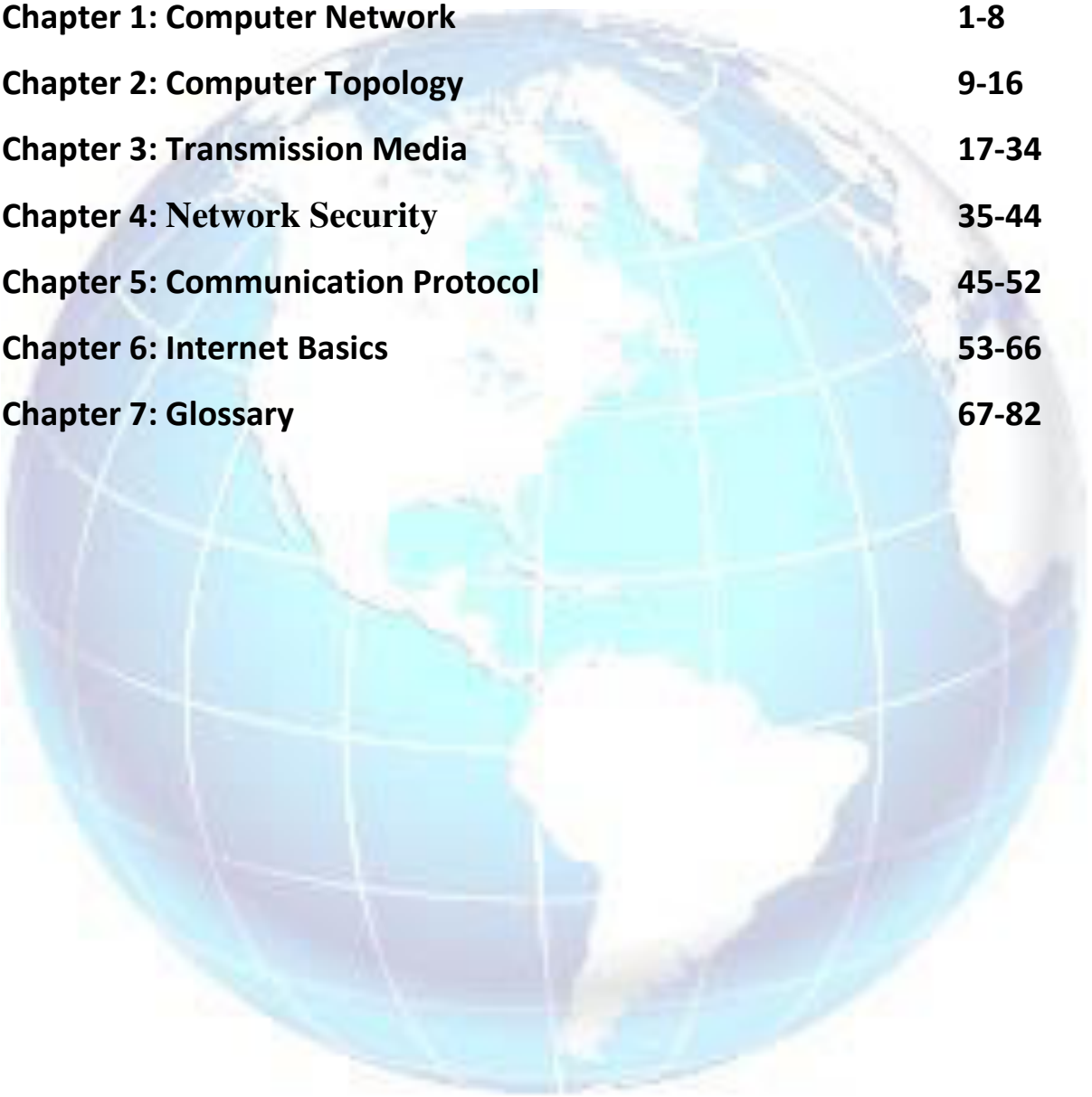
Mohindergarh, Haryana

**e**: sunilvats1981@gmail.com

**t**: +91-941 6266 966

# Contents





# CHAPTER-1
# COMPUTER NETWORK

A system (Collection of Interrelated component, which are designed to achieve a specific goal) of interconnected computers (Node) and other expensive devices which are able to communicate with each other and share hardware and software resources. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

## Classification of Computer Networks

Computer networks can be classified on their geographical area, connectivity and architecture.

## Network Architecture

Computer networks can be discriminated into various types such as Client-Server, peer-to-peer or hybrid, depending upon its architecture.

- There can be one or more systems acting as Server. Other being Client, requests the Server to serve requests. Server takes and processes request on behalf of Clients.
- Two systems can be connected Point-to-Point, or in back-to-back fashion. They both reside at the same level and called peers.
- There can be hybrid network which involves network architecture of both the above types.

## Network Applications

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- Resource sharing such as printers and storage devices
- Exchange of information by means of e-Mails and FTP
- Information sharing by using Web or Internet
- Interaction with other users using dynamic web pages
- IP phones
- Video conferences
- Parallel computing
- Instant messaging

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

## Personal Area Network

A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.

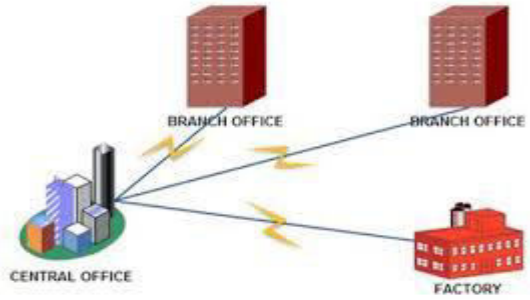
## Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization, schools, colleges or universities. Number of systems connected in LAN may vary from two to as much as 16 million. LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers. LANs are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally. LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.

## Metropolitan Area Network

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI). Metro Ethernet is a service which is provided by ISPs. This service

enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city. Backbone of MAN is high-capacity and high-speed fibre optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

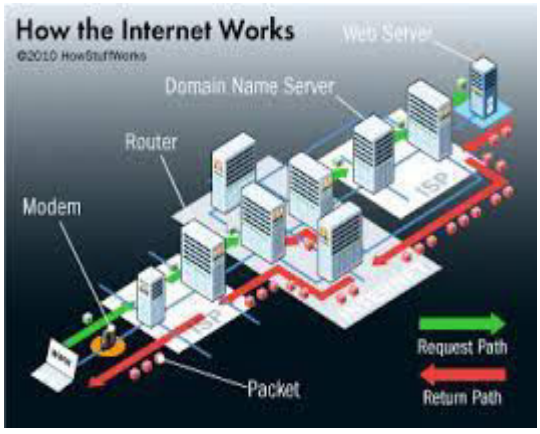



## Wide Area Network

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment. WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administration.

## Internetwork

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet. The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6. Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio and video streaming etc. At huge level, internet works on Client-Server model. Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.



Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very low.

Internet is serving many proposes and is involved in many aspects of life. Some of them are:

- Web sites
- E-mail
- Instant Messaging
- Blogging
- Social Media
- Marketing
- Networking
- Resource Sharing
- Audio and Video Streaming

Let us go through various LAN technologies in brief:

## Ethernet

Ethernet is a widely deployed LAN technology. This technology was invented in the year 1970. It was standardized in IEEE (Institute of Electrical and Electronics Engineers) 802.3 in 1980.

Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions..

Traditional Ethernet uses 10BASE-T specifications. The number 10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5 twisted pair cable with RJ-5 connector. Ethernet follows star topology with segment length up to 100 meters. All devices are connected to a hub/switch in a star fashion. We can also get the idea of different type of Ethernet, cable and maximum length through the given table.

## Fast-Ethernet

To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100 MBPS. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 twisted pair cable. It uses CSMA/CD technique for wired media sharing among the Ethernet hosts and CSMA/CA (CA stands for Collision Avoidance) technique for wireless Ethernet LAN.

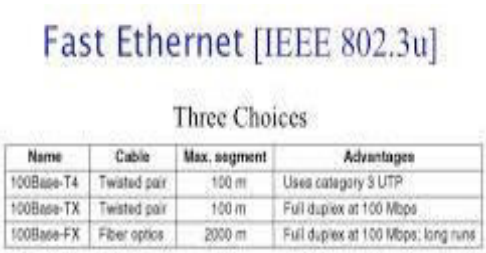



Figure 4-21.The original fast Ethernet cabling.

## Giga-Ethernet

After being introduced in 1995, Fast-Ethernet could enjoy its high speed status only for 3 years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardize Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.

| Speed | Common Name | Informal Name | Formal IEEE Name | Cable and Max. Length |
|---|---|---|---|---|
| 10 Mbps | Ethernet | 10BASE-T | 802.3 | Copper, 100 m |
| 100 Mbps | Fast Ethernet | 100BASE-T | 802.3u | Copper, 100 m |
| 1000 Mbps | Gig Ethernet | 1000BASE-LX | 802.3z | Fiber, 5000 m |
| 1000 Mbps | Gig Ethernet | 1000BASE-T | 802.3ab | Copper, 100 m |
| 10 Gbps | 10 Gig Ethernet | 10GBASE-T | 802.3an | Copper, 100 m |

## Virtual LAN

LAN uses Ethernet which in turn works on shared media. Shared media in Ethernet create one single Broadcast domain and one single Collision domain. Introduction of switches to Ethernet has removed single collision domain issue and each device connected to switch works in its separate collision domain. But even Switches cannot divide a network into separate Broadcast domains. Virtual LAN is a solution to divide a single Broadcast domain into multiple Broadcast domains. Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into the same VLAN.

## How to Make an Ethernet Cable

Purchasing Ethernet cables can be quite expensive and pre-made lengths are not always the length you need. Making Ethernet cables is easy with a

box of bulk Category 5e Ethernet cable and RJ-45 connectors that are attached to the cut ends of your preferred cable length.

**Bulk Ethernet Cable - Category 5e or CAT5e**

You may also use Category 6 or CAT6 cabling which has higher performance specifications and is about 20% more expensive than CAT5e.

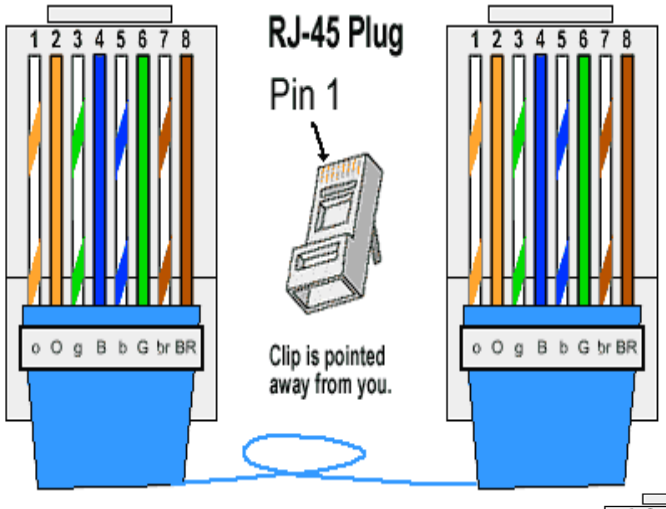
**Bulk RJ45 Crimp able Connectors for CAT-5e**

**or**

**Bulk RJ45 Crimp able Connectors for CAT-6**

**RJ Crimping Tool**

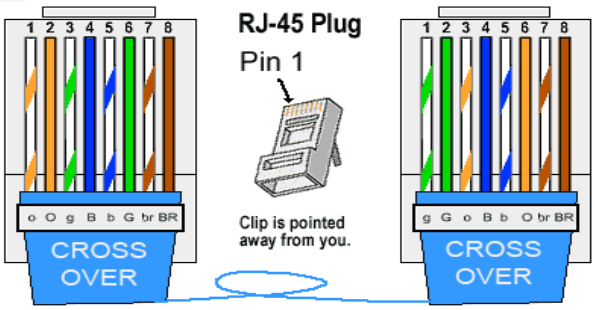
There are two kinds of Ethernet cables you can make, **Straight Through** and **Crossover**.




STRAIGHT THROUGH Ethernet cables are the standard cable used for almost all purposes, and are often called "patch cables". It is highly recommend you duplicate the color order as shown on the left. Note how the green pair is not side-by-side as are all the other pairs. This configuration allows for longer wire runs.

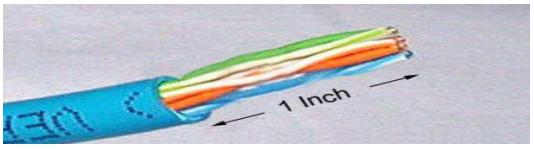
**CROSSOVER CABLES**

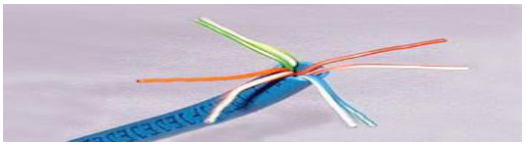
The purpose of a Crossover Ethernet cable is to directly connect one computer to another computer (or device) without going through a router, switch or hub.



Here's how to make a standard cable:

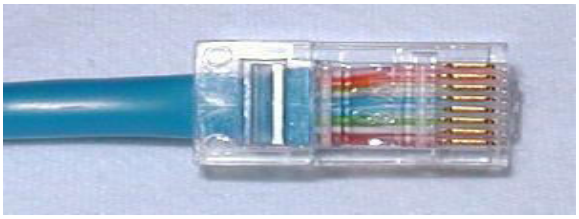
Cut into the plastic sheath about **1 inch** (2.5 cm) from the end of the cut cable. The crimping tool has a razor blade that will do the trick with practice. Unwind and pair the similar colors.



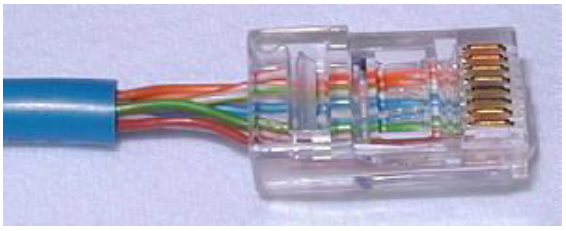
Pinch the wires between your fingers and straighten them out as shown. The color order is important to get correct. Use scissors to make a straight cut across the 8 wires to shorten them to **1/2 Inch** (1.3 cm) from the cut sleeve to the end of the wires.

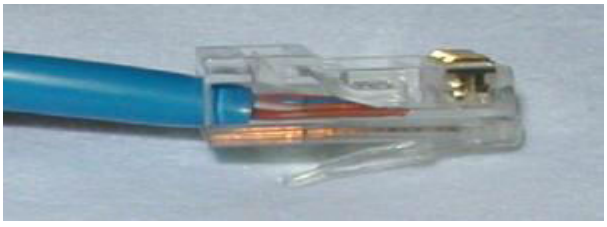
Carefully push all 8 colored wires into the connector. Note the position of the blue plastic sleeve. Also note how the wires go all the way to the end.



A view from the top. All the wires are all the way in. There are no short wires.

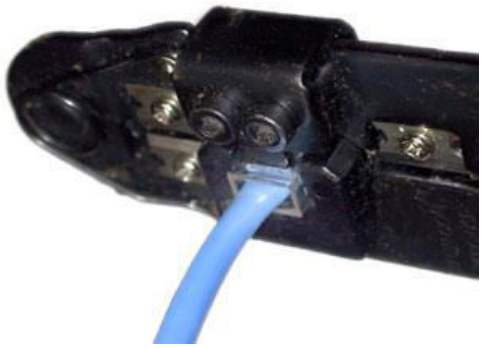
WRONG WAY - Note how the blue plastic sleeve is not inside the connector where it can be locked into place. The wires are too long. The wires should extend only 1/2 inch from the blue cut sleeve.





WRONG WAY - Note how the wires do not go all the way to the end of the connector.

## CRIMPING THE CABLE



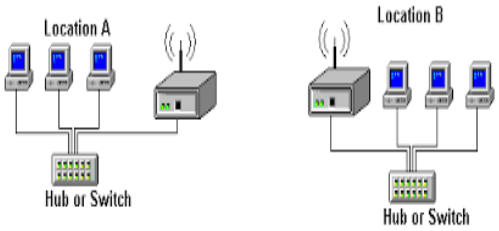
During the crimping of the cable carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is also a locking tab that holds the blue plastic sleeve in place for a tight compression fit. When you remove the cable from the crimper, that end is ready to use.

# CHAPTER-2

# NETWORK TOPOLOGY

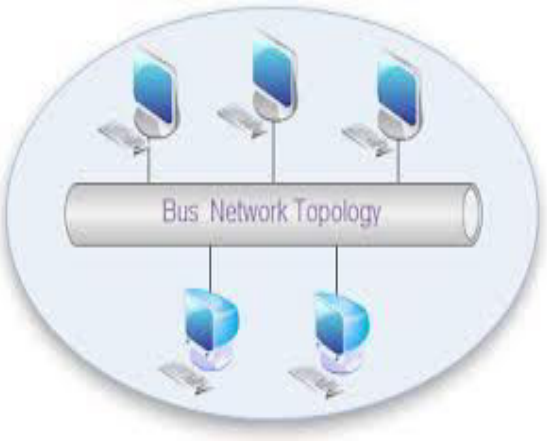
A Network Topology is the arrangement of computer systems or network devices which are connected to each other. Topologies may be defined as physical and logical aspect of the network. Logical and physical topologies could be same or different in a same network.

## Point-to-Point



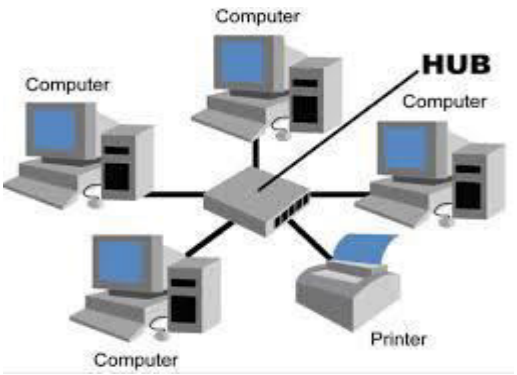

Point-to-point networks contains exactly two nodes such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one node is connected to sending end of the other and vice-versa.

## Bus Topology




In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple nodes sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one node 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. Data in this topology is unidirectional. As soon as it reached at the end, terminator removes it from the line.

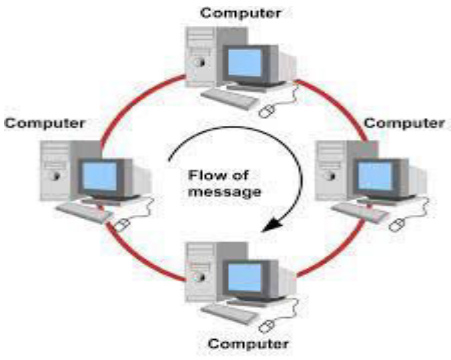
## Star Topology




All nodes 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 nodes and hub. The hub device can be hub, repeater, switch, bridge, router or gateway. As in Bus topology, hub acts as single point of failure, if hub is fail, connectivity with all nodes fails. Every communication between nodes, takes place through only the hub. Star topology is not

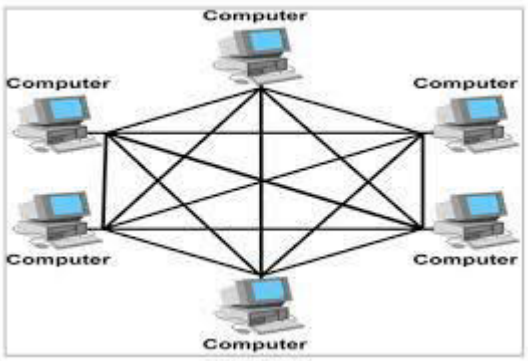
expensive as to connect one more node, only one cable is required and configuration is simple.

## Ring Topology

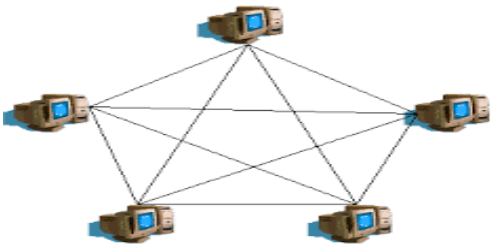



In ring topology, each node machine connects to exactly two other machines, creating a circular network structure. In this topology flow of data is also unidirectional. When one node tries to communicate or send message to a node which is not adjacent to it, the data travels through all intermediate nodes. Failure of any node 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.

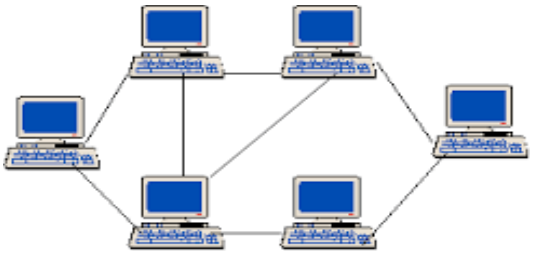
## Mesh Topology




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

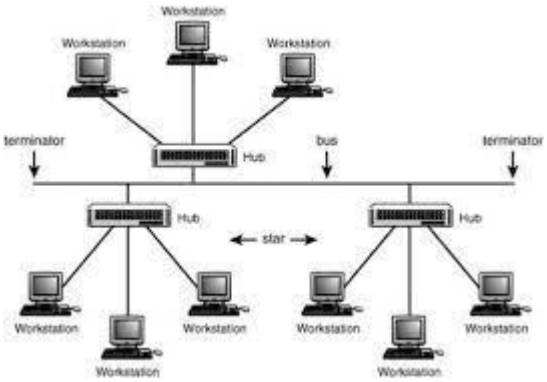


- **Full Mesh**: All nodes have a point-to-point connection to every other node in the network. Thus for every new node n (n-1)/2 connections are required. It provides the most reliable network structure among all network topologies. But it is also expensive one.



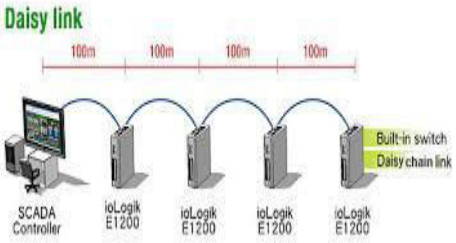
- **Partially Mesh**: All nodes have Not point-to-point connection to every other node. Nodes connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some nodes out of all.

## Tree Topology



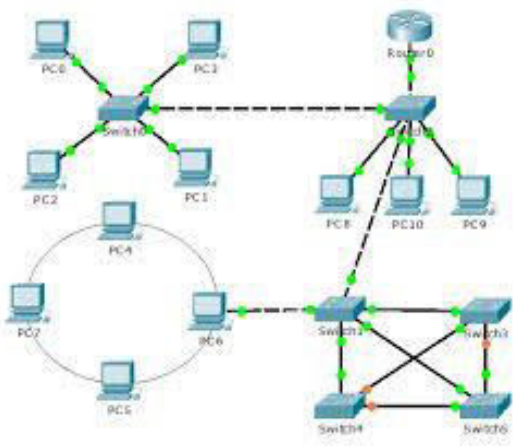

Tree topology also known as Hierarchical Topology, this is the most common form of network topology in modern era. This topology is the follow up of Star topology and inherits properties of bus topology.This topology divides the network in to multiple levels of network. Mainly in LANs, a network is divided into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and which is the root of the tree from where all nodes separate.

## Daisy Chain




This topology connects all the nodes in a linear fashion. Similar to Ring topology, all nodes are connected to two nodes only, except the end nodes. Means, if the end nodes in daisy chain are connected then it represents Ring topology. Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate node works as relay for its immediate nodes.

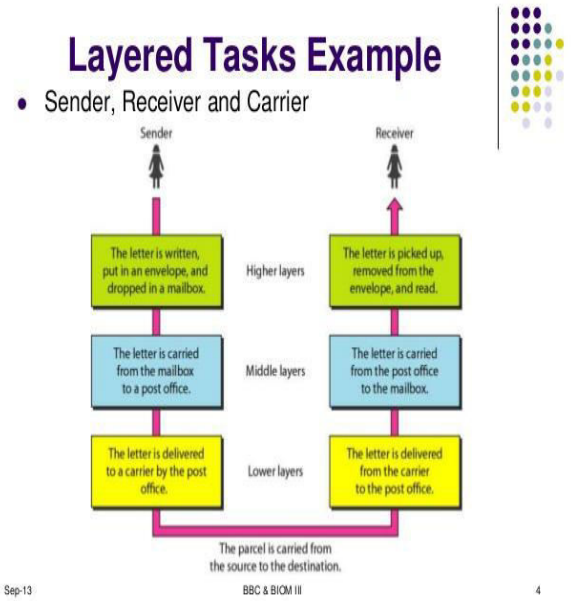
## Hybrid Topology



A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology

## Layered Tasks

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work. One layer of a node deals with the task done by its peer layer at the same level on the remote node. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.




## OSI Model

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers:

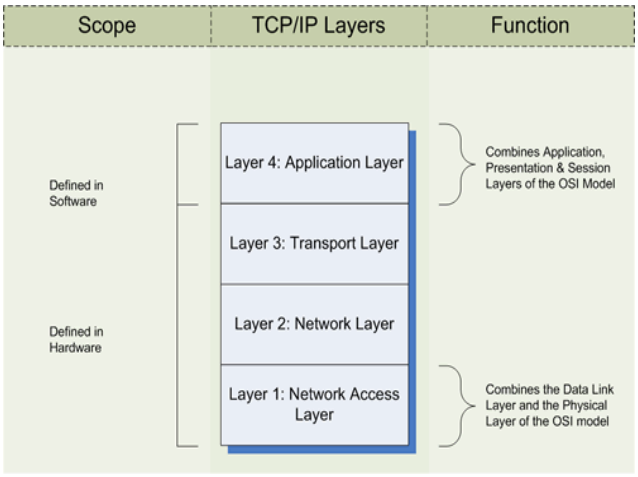
| Layer | Function | Example |
|---|---|---|
| Application (7) | Services that are used with end user applications | SMTP, |
| Presentation (6) | Formats the data so that it can be viewed by the user<br>Encrypt and decrypt | JPG, GIF, HTTPS, SSL, TLS |
| Session (5) | Establishes/ends connections between two hosts | NetBIOS, PPTP |
| Transport (4) | Responsible for the transport protocol and error handling | TCP, UDP |
| Network (3) | Reads the IP address form the packet. | Routers, Layer 3 Switches |
| Data Link (2) | Reads the MAC address from the data packet | Switches |
| Physical (1) | Send data on to the physical wire. | Hubs, NICS, Cable |

- **Application Layer**: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer**: This layer formats the data so that it can be viewed by the user.
- **Session Layer**: This layer establish or end the connection between two hosts. For example, once user/password authentication is done, the remote node maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer**: This layer is responsible for transport protocol and error handling as it is shown in the picture.
- **Network Layer**: This layer is responsible for address assignment and uniquely addressing nodes in a network.

- **Data Link Layer**: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer:** This layer defines the hardware, cabling wiring, power output, pulse rate etc.

## Internet Model

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what the internet uses for all its communication. The internet is independent of its underlying network architecture so is its Model. This model has the following layers:




- **Application Layer**: This is the top most layer of four layer. This layer defines the protocol which enables user to interact with the network. This layer combines the Application, Presentation and session layer of the OSI Model.
- **Transport Layer**: This layer defines how data should flow between nodes. Major protocol at this layer is Transmission Control Protocol (TCP). This layer ensures data delivered between nodes is in-order and is responsible for end-to-end delivery.
- **Network or Internet Layer**: Internet Protocol (IP) works on this layer. This layer facilitates node addressing and recognition. This layer defines routing.
- **Data Link Layer**: This layer provides mechanism of sending and receiving actual data. Unlike its OSI Model counterpart, this layer is independent of underlying network architecture and hardware.

When all networks merged together and formed internet, the data used to travel through public transit network. Common people may send the data that can be highly sensitive such as their bank credentials, username and passwords, personal documents, online shopping details, or confidential documents. All security threats are intentional i.e. they occur only if intentionally triggered. Security threats can be divided into the following categories:

- **Interruption**

  Interruption is a security threat in which availability of resources is attacked. For example, a user is unable to access its web-server or the web-server is hijacked.

- **Privacy-Breach**

  In this threat, the privacy of a user is compromised. Someone, who is not the authorized person is accessing or intercepting data sent or received by the original authenticated user.

- **Integrity**

  This type of threat includes any alteration or modification in the original context of communication. The attacker intercepts and receives the data sent by the sender and the attacker then either modifies or generates false data and sends to the receiver. The receiver receives the data assuming that it is being sent by the original Sender.

- **Authenticity**

  This threat occurs when an attacker or a security violator, poses as a genuine person and accesses the resources or communicates with other genuine users.

For the authenticity the most widely used technique is Cryptography. Cryptography is a technique to encrypt the plain-text data which makes it difficult to understand and interpret. There are several cryptographic algorithms available present day as described below:

- Secret Key
- Public Key
- Message Digest

## Secret Key Encryption

Both sender and receiver have one secret key. This secret key is used to encrypt the data at sender's end. After the data is encrypted, it is sent on the public domain to the receiver. Because the receiver knows and has the Secret Key, the encrypted data packets can easily be decrypted.

Example of secret key encryption is Data Encryption Standard (DES). In Secret Key encryption, it is required to have a separate key for each node on the network making it difficult to manage.

## Public Key Encryption

In this encryption system, every user has its own Secret Key and it is not in the shared domain. The secret key is never revealed on public domain. Along with secret key, every user has its own but public key. Public key is always made public and is used by Senders to encrypt the data. When the user receives the encrypted data, he can easily decrypt it by using its own Secret Key.

## Message Digest

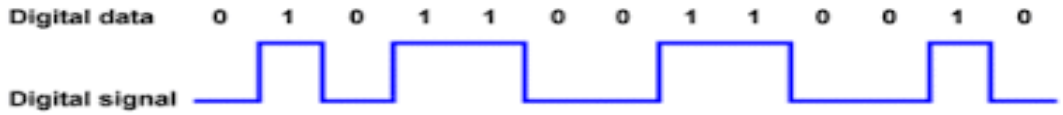
In this method, actual data is not sent, instead a hash value is calculated and sent. The other end user, computes its own hash value and compares with the one just received. If both hash values are matched, then it is accepted otherwise rejected. It is mostly used in authentication where user password is cross checked with the one saved on the server.

## Signals

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voice, or digital such as file on the disk. Both analog and digital data can be represented in digital or analog signals.

- **Digital Signals**

  Digital signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry of a computer system.




- **Analog Signals**

  Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.


## Transmission Impairment

When signals travel through the medium they tend to deteriorate. This may have many reasons as given:

- **Attenuation**

  For the receiver to interpret the data accurately, the signal must be sufficiently strong. When the signal passes through the medium, it tends to get weaker. As it covers distance, it loses strength.

- **Dispersion**

  As signal travels through the media, it tends to spread and overlaps. The amount of dispersion depends upon the frequency used.

- **Delay distortion**

  Signals are sent over media with pre-defined speed and frequency. If the signal speed and frequency do not match, there are possibilities that signal reaches destination in arbitrary fashion. In digital media, this is very critical that some bits reach earlier than

the previously sent ones.

- **Noise**

  Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Noise can be characterized in one of the following class:

  - **Thermal Noise**

    Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable.

  - **Intermodulation**

    When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.

  - **Crosstalk**

    This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.

  - **Impulse**

    This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

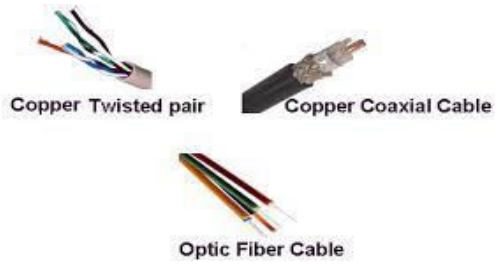
# CHAPTER-3

# Transmission Media

Computer Network is considered the backbone of today's world. By using Computer Network we can sent or receive data at long distance. The kind of media, which is used to send or receive the data on Network is called Transmission media. Transmission Media is further sub divided in two sub categories.

## Guided Media

The kind of transmission, where transmission can be made using physical (wires/cable) connection between the nodes are called guided media, such as UTP, coaxial cables, and fiber Optics.

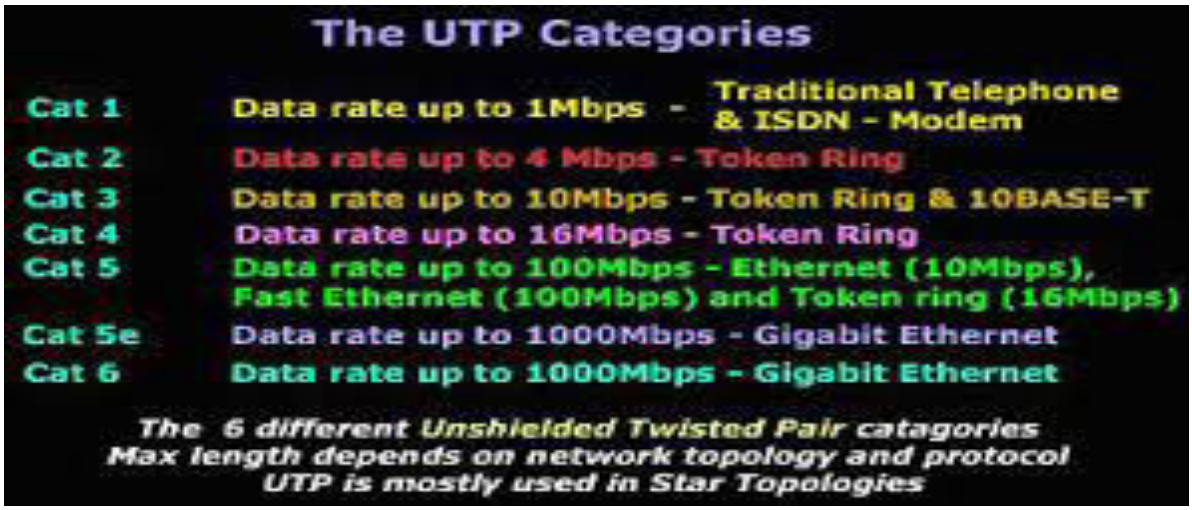



## Twisted Pair Cable

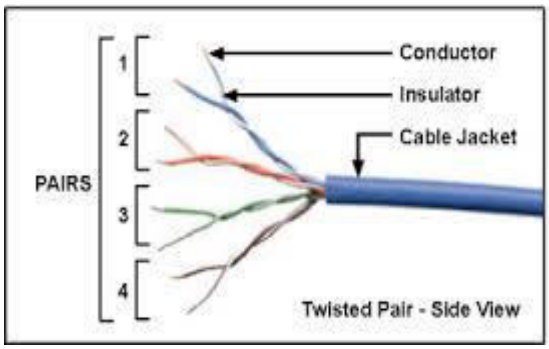
- This is probably the most widely used cable for creating small computer networks. It contains four twisted pairs covered in an outer shield. These pairs are colour coded. An RJ-45 connecter is used to connect this cable to a computer. It is of two types:
- Shielded Twisted Pair (STP) Cable
- Unshielded Twisted Pair (UTP) Cable

**UTP (Unshielded Twisted Pair)**

As the name suggests in UTP cables individual pairs are not shielded. UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

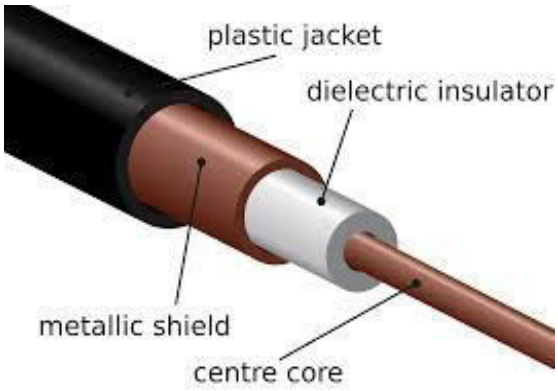


**Shielded Twisted Pair (STP)**

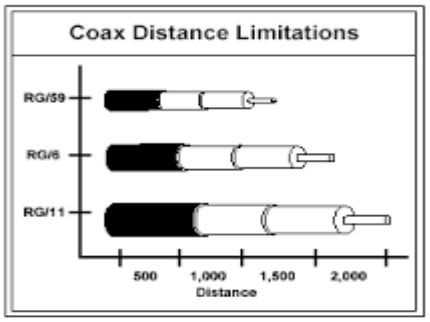



Cables comes with twisted wire pair covered in metal foil. This makes it more indifferent to noise and crosstalk. STP is a special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground.

## Coaxial Cable




Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor. The core is enclosed in an insulating sheath. The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath. This all is covered by plastic cover. Because of its structure, the coax cable is capable of carrying high frequency signals than that of twisted pair cable. The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.




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

Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.

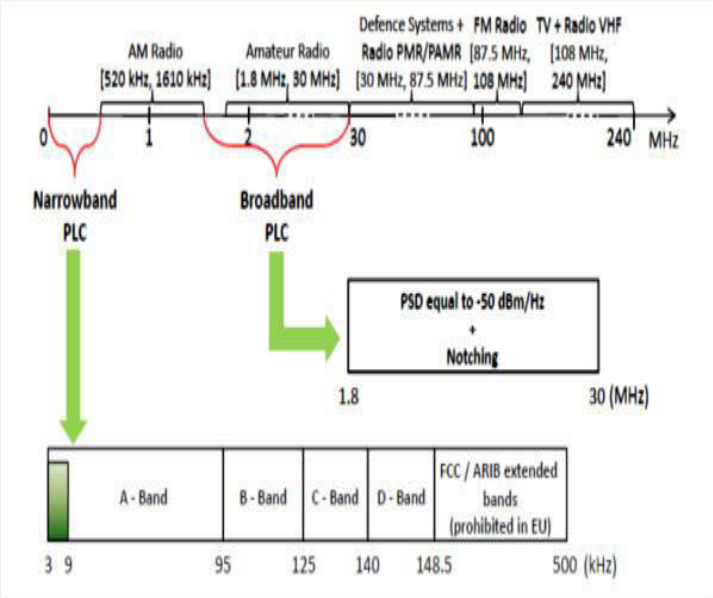
## Power Lines

Power Line communication (PLC) is Layer-1 (Physical Layer) technology which uses power cables to transmit data signals in PLC, modulated data is sent over the cables. The receiver on the other end de-modulates and interprets the data.

Because power lines are widely deployed, PLC can make all powered devices controlled and monitored. PLC works in half-duplex.

There are two types of PLC:

- Narrow band PLC
- Broad band PLC




Narrow band PLC provides lower data rates up to 100s of kbps, as they work at lower frequencies (3-5000 kHz).They can be spread over several kilometres.

Broadband PLC provides higher data rates up to 100s of Mbps and works at higher frequencies (1.8 – 250 MHz).They cannot be as much extended as Narrowband PLC.

## Fiber Optics

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.


Fiber Optic provides the highest mode of speed. It comes in two modes, one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.

Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.

## Unguided Media

In this kind of media data can be transmitted through air or wireless is said to be unguided media, because there is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information.

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data. A little part of electromagnetic spectrum can be used for wireless transmission.

## Radio Transmission

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike. Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Low Frequency) to 300 GHz (High Frequency). Radio frequencies are sub-divided into six bands.

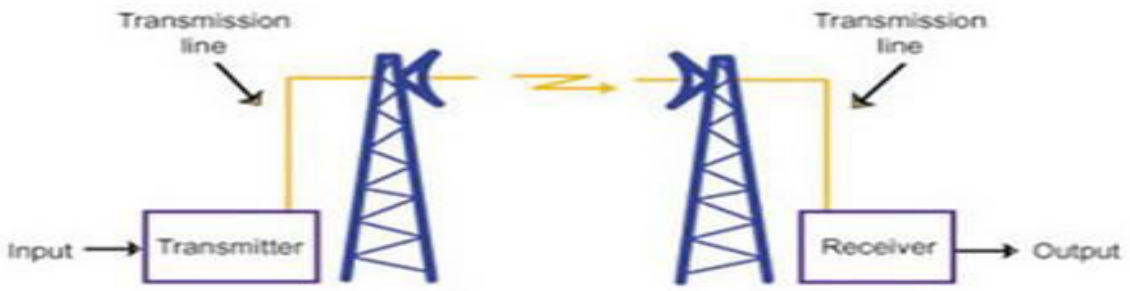
Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back. The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers over the earth's surface.

Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.

## Microwave Transmission

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over



them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight. Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.

Microwave antennas concentrate the waves making a beam of it. As shown in picture above, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles. Microwave transmission depends highly upon the weather conditions and the frequency it is using.

## Infrared Transmission


Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz. Infrared wave is used for very short range communication purposes such as television and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

## Light Transmission

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signalling. This is achieved by means of LASER. Because of frequency light uses, it tends to travel strictly in straight line. Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector needs to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source. Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles such as walls, rain, and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature, or variation in temperature in the path. Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

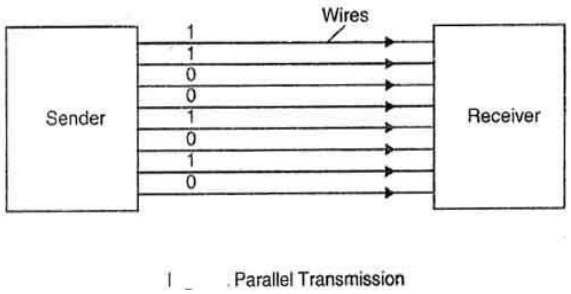
## Transmission Modes

The transmission mode decides how data is transmitted between two computers. The binary data in the form of 1s and 0s can be sent in two different modes which is known as

Parallel and Serial transmission.

### Parallel Transmission

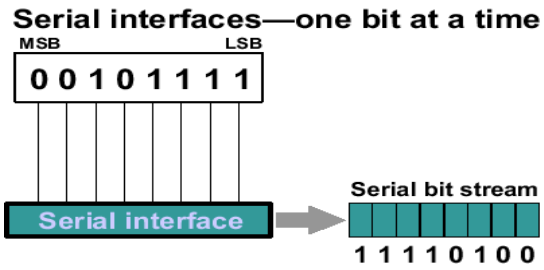
The binary bits are organized in-to groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines. Because the data lines are equal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




Parallel Transmission

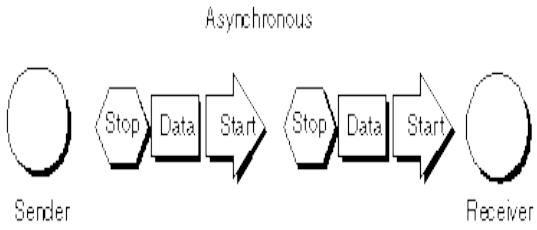
### Serial Transmission

In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel. Serial transmission can be either asynchronous or synchronous.



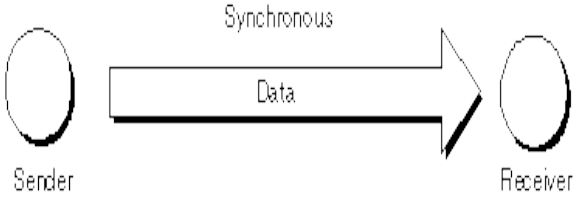

### Asynchronous Serial Transmission

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




### Synchronous Serial Transmission

Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits. There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes. Therefore, timing



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

## Channel Capacity

The speed of transmission of information between the nodes is said to be the channel capacity. We count it as data rate in digital world. It depends on numerous factors such as:

**Bandwidth:** In computer networking, the term "bandwidth" refers to the data rate supported by a network interface. Bandwidth represents the capacity of a network connection for supporting data transfers. Higher network bandwidth often translates to better performance, although overall performance also depends on other factors.

The term derives from the field of electrical engineering, where bandwidth represents the total distance or range between the highest and lowest signals on a communication channel (band).

## Measuring Network Bandwidth

Computer network bandwidth is measured in units of bits per second (bps). Most modern network devices support data rates of thousands and often millions or even billions of bps (units of Kbps, Mbps and Gbps). Network devices each possess a bandwidth rating according to the maximum data rate they are physically capable of supporting. For example old V.90 dialup modems were rated as 56 Kbps devices. 802.11g Wi-Fi devices as 54 Mbps, and Fast Ethernet links as 100 Mbps.

## Measuring Throughput versus Bandwidth

People sometimes use the terms "throughput" and "bandwidth" interchangeably. Technically, throughput represents the actual amount of useful data transferred over a network connection compared to bandwidth that measures a theoretical maximum.

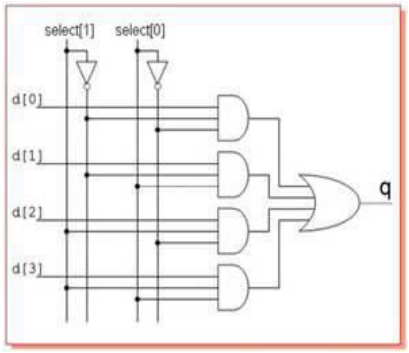
Due to network communication overheads (packing and unpacking of messages, collisions, errors and retries), throughput typically rates significantly lower than bandwidth.

**Error-rate:** In digital transmission, the number of **bit errors** is the number of received bits of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors. The **bit error rate** (**BER**) is the number of bit errors per unit time. The **bit error ratio** (also **BER**) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage

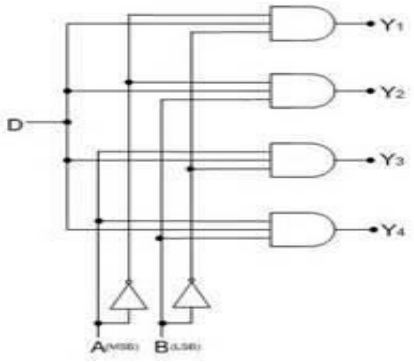
**Encoding:** The number of levels used for signalling.

## Multiplexing

Multiplexing is a technique to mix and send multiple data streams over a single medium. This technique requires system hardware called multiplexer (Takes multiple input and generate Single output) for multiplexing the streams and sending them on a medium, and de-multiplexer (takes single line input and generate multiple output) which takes information from the medium and distributes to different destinations.




MULTIPLEXER




DEMULTIPLEXER

In this technique analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams. When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

### Frequency Division Multiplexing

When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.

### Time Division Multiplexing

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot. TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously. When channel A transmits its

frame at one end the De-multiplexer provides media to channel A on the other end. As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

### Wavelength Division Multiplexing

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.

Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

### Code Division Multiplexing

Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals.

Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth. The receiver knows in advance the chip code signal it has to receive.

### Switching

Switching is a technique to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

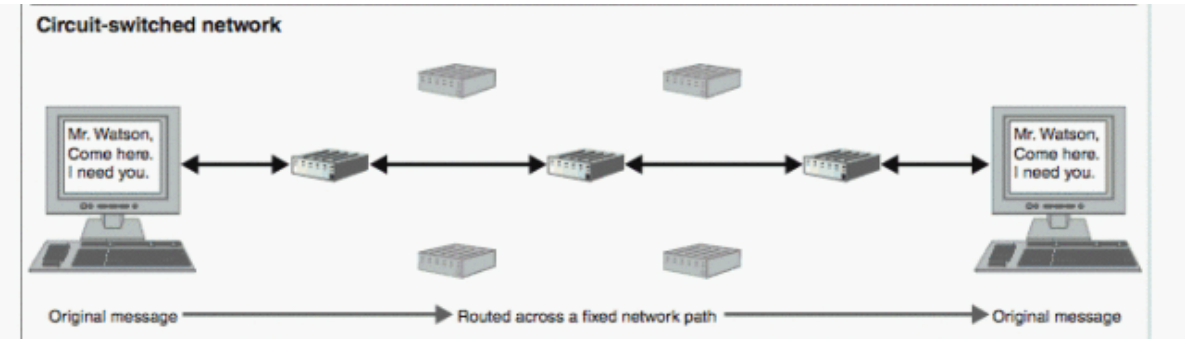
### Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There is a need of pre-specified route from which data will travels

and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

- Establish a circuit
- Transfer the data
- Disconnect the circuit




Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and caller is established over the network.

### Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits. This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

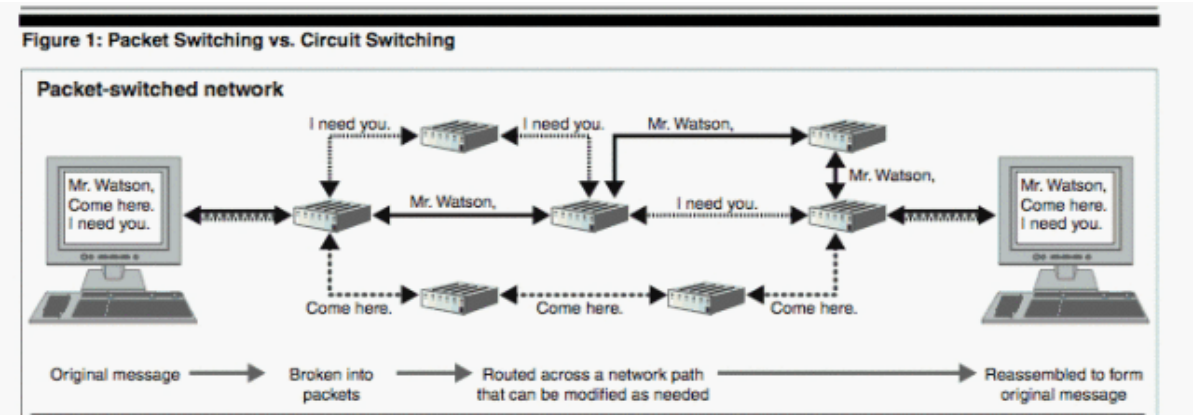
- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

### Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The

entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches. Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.




Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two nodes which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple nodes on single collision domain. Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

## Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are:

- **Framing**

  Data-link layer takes packets from Network Layer and encapsulates them into Frames.

Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

- **Addressing**

  Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

- **Synchronization**

  When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

- **Error Control**

  Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

- **Flow Control**

  Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

- **Multi-Access**

  When node on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

## Types of Errors

There may be three types of errors:

- **Single bit error**


In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**


Frame is received with more than one bits in corrupted state.

- **Burst error**


Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

## Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

## Parity Check

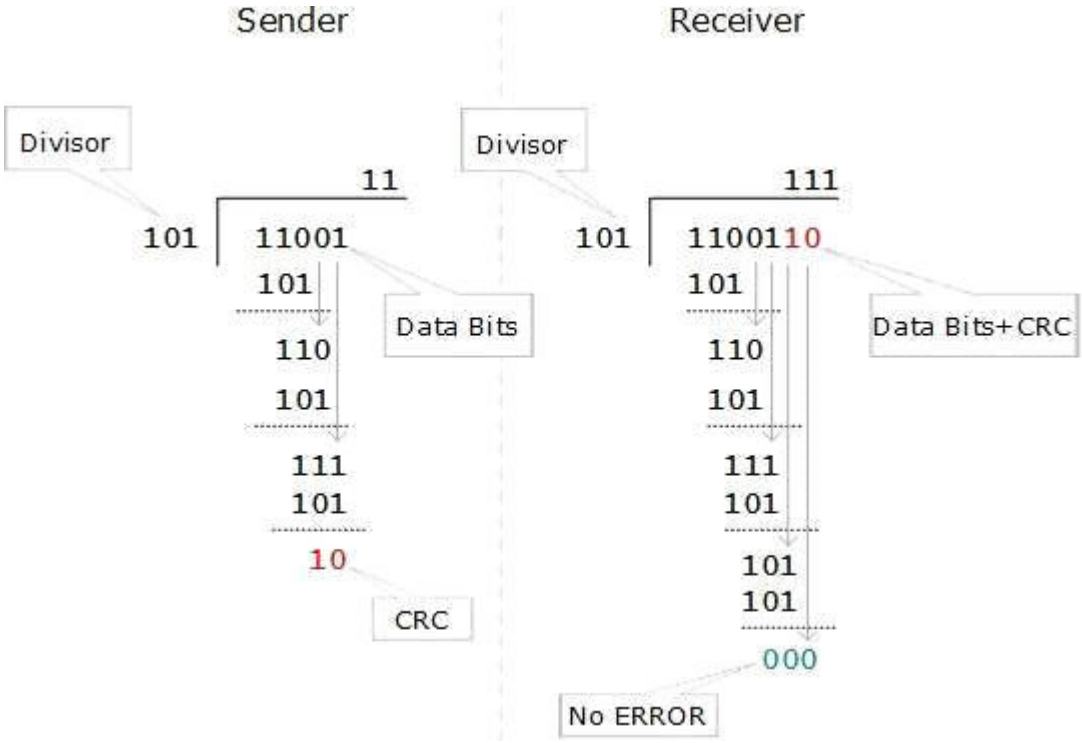
One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity. The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1 remains even, if the number of 1 is odd, to make it even a bit with value 1 is added.


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erro neous, then it is very hard for the receiver to detect the error.

## Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.




At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered

as there some data corruption occurred in transit.

## Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

## Flow Control

When a data frame (Layer-2 data) is sent from one node to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- **Stop and Wait**

  This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.

- **Sliding Window**

  In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

## Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

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

## Digital-to-Digital Conversion

How to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

## Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s. Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available.

### Uni-polar Encoding

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

## Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values.

### Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.

### Block Coding

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding. Block coding is represented by slash notation, mB/nB.Means, m-bit block is substituted with n-bit block where n > m.

### Analog-to-Digital Conversion

Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion. Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).

PCM is one of the most commonly used method to convert analog data into digital form.

### Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data. An analog signal is characterized by its amplitude, frequency, and phase.

### Analog-to-Analog Conversion

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

- **Amplitude Modulation**

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

- **Frequency Modulation**

  In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data). The amplitude and phase of the carrier signal are not altered.

- **Phase Modulation**

  In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage of analog data signal. Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier signal is changed to reflect voltage change in the amplitude of modulating signal.

# Chapter-4

# Network Security

**Network security** consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users can choose or assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs. Conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

## Network security concepts

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name, this is sometimes termed one-factor authentication. Second with two-factor authentication, something the user can use a security token or, an ATM card, or a mobile phone and with other type of authenticating three-factor authentication, something the user also used fingerprint or retinal scan.

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis.

## Network Security

The network security (or information security) is to provide protection to the computer system from the hackers (intruders). Network security focuses on protecting data resources

from external attack and also from simple mistakes made by the users within an organization. Network security also designs computer network infrastructure, policies and rules adopted by the network administrator to protect the network and the network-shareable resources from. The security system also monitor consistently and continuously the effectiveness of all the security measure.

## File Access Permission

In a computer network or even in the internet, some files or documents are made shareable and some are made public. The protected sharable files and documents are shared among few users or even by a group having the access rights. Access rights are generally decided and given by the owner of the file or the network administrator. Thus the three types of users can access a file or a folder i.e. Owner, user having access rights, or all other users.

## Firewall

A firewall is a technique used in a secured computer system or network to block unauthorized access and allow only the authorized user. Firewalls can be implemented in either hardware or software, or a combination of both. It is a device or set of devices or software running on a computer, which is configured to permit or deny computer applications and set of other software based upon a set of rules and other criteria designed by the network administrator. It also inspects network traffic passing through it, and denies or permits passage. It is normally placed between a protected network (usually a LAN) and an unprotected network (usually WAN or Internet) and acts like a gate to protect all resources to ensure that nothing goes out without permission and nothing unwanted comes in into the system. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. In case of Cyber Crime, a digital signature plays a significant role to ensure authenticity and thus protect security of a computer system. A digital signature is a method for proving the authenticity of a message or document or attachment or software sent through email. Digital signatures are commonly used for software distribution, financial

## Digital Certificate

A digital certificate (also known as a public key certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key or password required for decode and encoded document with an authentic identity such as the name of a

person or an organization, their phone numbers or address, and so forth. The certificate can be used to verify that a public key belongs to an authorized individual or organization.

## Cookies

A cookie (also known as a web cookie, browser cookie, and HTTP cookie) is a small bit of text or a file that accompanies requests and pages as they go between the web server and browser. The cookie is sent as header by a web server to a web browser and then sent back by the browser each time it accesses that server. Cookies help web sites to store information about visitors. Some cookies thus may violate privacy concerns. For example, when a user visits your site, you can use cookies to store user preferences or other information like password, address, date of birth etc.(Many sites ask first-time visitors to fill in a form about themselves before they get access to the site). When the user visits your web site another time, the application can retrieve the information it stored earlier. A cookie can also be used for authentication, session tracking (state maintenance), storing site preferences, shopping cart contents, the identifier for a server based session, or anything else that can be accomplished through storing textual data. As text, cookies are not executable. Since they are not executed, they cannot replicate themselves and not harm the computer directly. However, due to the fact that the browser reads and sends cookies to the web server, they can be used as spyware. Today, most of the browsers ask users whether to accept cookies or not, but rejecting cookies makes some websites unusable.

## Cyber Crime

Cyber Crime (or Computer crime) refers to any crime wherein the computer is either a tool or a target or both. Some forms of the Cyber Crime are:

- Creating and distributing Spam Mails
- Hacking
- Fraud through Internet or intranet
- Sending Obscene or Offensive messages
- Creating Websites with Obscene or Offensive content
- Harassment through emails and web messages
- Drug trafficking through internet and intranet
- Cyber terrorism

The propagation of a virus, worm or Trojan is one of the common means of making cyber-crime. What is the legal aspect in such situations of cyber-crimes and how to counter them? First of all, like traditional crimes such as theft, fraud, forgery, defamation and mischief, cyber-

crimes are also treated criminal in nature and are subject of the Indian Penal Code. Information Technology Act (or The IT Act) is a set of recent legal enactments, currently existing in India, which provide legal support to the computer users against the cyber-crime. These laws have been described as "paper laws" for "paperless environment".

Internet crime is crime committed on the Internet, using the Internet and by means of the Internet. Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes.

With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. This is why Internet crime has now become a growing problem in the United States. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.

Such new crimes devoted to the Internet are email “phishing”, hijacking domain names, virus imitation, and cyber vandalism. A couple of these crimes are activities that have been exposed and introduced into the world. People have been trying to solve virus problems by installing virus protection software and other software that can protect their computers. Other crimes such as email “phishing” are not as known to the public until an individual receives one of these fraudulent emails. These emails are cover faced by the illusion that the email is from your bank or another bank. When a person reads the email he/she is informed of a problem with he/she personal account or another individual wants to send the person some of their money and deposit it directly into their account. The email asks for your personal account information and when a person gives this information away, they are financing the work of a criminal. Every year billions of dollars are lost in this crime through online banking (i.e. through debit/credit card etc.).

## Stopping the problem

Device and Computer Fraud and Abuse Act of 1984, the government has been trying to track down and stop online criminals. The FBI has tried many programs and investigations in order to deter Internet crime. The reality is that Internet criminals are rarely caught. One reason is that hackers will use one computer in one country to hack another computer in another country. Another eluding technique used is the changing of the emails, which are involved in virus attacks and “phishing” emails so that a pattern cannot be recognized. An individual can

do their best to protect themselves simply by being cautious and careful. Internet users need to watch suspicious emails, use unique passwords, and run anti-virus and anti-spyware software. Do not open any email or run programs from unknown sources.

## Cyber Lawyering

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly on the Internet. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

## Jurisdiction and Sovereignty

The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet. As such, a single transaction may involve the laws of at least three jurisdictions:

- The laws of the state/nation in which the user resides
- Laws of the state/nation that apply where the server hosting the transaction is located.
- Laws of the state/nation which apply to the person or business with whom the transaction takes place.

So a user in one of the United States conducting a transaction with another user in Britain through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have extra-territorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application, and such questions are generally a matter of conflict of laws, particularly private international law. An example would be where the contents of a web site are legal in one country and illegal in another. In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue.

## Net Neutrality

Another major area of interest is net neutrality, which affects the regulation of the infrastructure of the Internet. Though not obvious to most Internet users, every packet of data

sent and received by every user on the Internet passes through routers and transmission infrastructure owned by a collection of private and public entities, including telecommunications companies, universities, and governments, suggesting that the Internet is not as independent as Barlow and others would like to believe. This is turning into one of the most critical aspects of cyber law and has immediate jurisdictional implications, as laws in force in one jurisdiction have the potential to have dramatic effects in other jurisdictions when host servers or telecommunications companies are affected.

## Internet Regulation of different Countries

While there is some United States law that does restrict access to materials on the internet, it does not truly filter the internet. Many Asian and Middle Eastern nations use any number of combinations of code-based regulation to block material that their governments have deemed inappropriate for their citizens to view. China and Saudi Arabia are two excellent examples of nations that have achieved high degrees of success in regulating their citizens access to the Internet.

## Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.

- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and cause losses, damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

## Sides of INDIAN Cyber Law or IT Act of INDIA

Cyber laws are meant to set the definite pattern, some rules and guidelines that defined certain business activities going on through internet legal and certain illegal and hence punishable. The IT Act 2000, the cyber law of India, gives the legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. Let's have an overview of the law where it takes a firm stand and has got successful in the reason for which it was framed.

a) The E-commerce industry carries out its business via transactions and communications done through electronic records. It thus becomes essential that such transactions be made legal. Keeping this point in the consideration, the IT Act 2000 empowers the government departments to accept filing, creating and retention of official documents in the digital format. The Act also puts forward the proposal for setting up the legal framework essential for the authentication and origin of electronic records / communications through digital signature.

b) The Act legalizes the e-mail and gives it the status of being valid form of carrying out communication in India. This implies that e-mails can be duly produced and approved in a court of law, thus can be a regarded as substantial document to carry out legal proceedings.
c) The act also talks about digital signatures and digital records. These have been also awarded the status of being legal and valid means that can form strong basis for launching litigation in a court of law. It invites the corporate companies in the business of being Certifying Authorities for issuing secure Digital Signatures Certificates.
d) The Act now allows Government to issue notification on the web thus heralding e-governance.
e) It eases the task of companies of the filing any form, application or document by laying down the guidelines to be submitted at any appropriate office, authority, body or agency owned or controlled by the government. This will help in saving costs, time and manpower for the corporates.
f) Also the law sets up the Territorial Jurisdiction of the Adjudicating Officers for cyber crimes and the Cyber Regulations Appellate Tribunal.
g) The law has also laid guidelines for providing Internet Services on a license on a non-exclusive basis.

The IT Law 2000, though appears to be self-sufficient, it takes mixed stand when it comes to many practical situations. It losses its certainty at many places like:

1. The law misses out completely the issue of Intellectual Property Rights, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. The law even doesn't talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.
2. The law even stays silent over the regulation of electronic payments gateway and segregates the negotiable instruments from the applicability of the IT Act , which may have major effect on the growth of e-commerce in India . It leads to make the banking and financial sectors irresolute in their stands.
3. The act empowers the Deputy Superintendent of Police to look up into the investigations and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the context of Corporate India as companies have public offices which would come within the ambit of "public place" under the Act. As a result, companies will not be able to escape potential harassment at the hands of the DSP.

4. Internet is a borderless medium. It spreads to every corner of the world where life is possible and hence is the cyber-criminal. Then how come is it possible to feel relaxed and secured once this law is enforced in the nation?

The Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time

## IT Act of India 2000

The cyber police work as a detector to detect the cyber-crime. They have the right in respect of all the offences committed under TITA (The Information Technology Act 2000) Central Act.No.21 of 2000 or crime related to Intellectual property rights.

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. ***Then again the Information technology Act 2000 has been substantially amended through the Information Technology Amendment Act 2008 which was passed by the two houses of the Indian Parliament on December 23, and 24, 2008. It got the Presidential assent on February 5, 2009 and was notified for effectiveness on October 27, 2009.***

This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.

The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. Some highlights of the Act are listed below:

**Chapter-II** of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

**Chapter-III** of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference. It also include the legal recognition details of Digital Signatures.

**Chapter-IV** of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

**Chapter-VII** of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

**Chapter-IX** of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

**Chapter-X** of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

**Chapter-XI** of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

# Chapter-5

# Communication Protocol

In telecommunications, a **communications protocol** is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. These are the rules or standard that defines the syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.

Communicating systems use protocol for exchanging messages. Each message has an exact meaning intended to response from a range of possible responses pre-determined for that particular situation.

## Internet Protocol (IP)

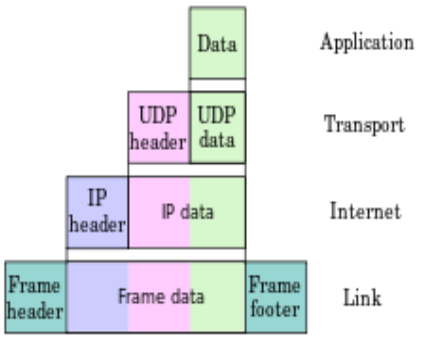
The **Internet Protocol** (**IP**) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries and establishing the Internet Connection. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. Every Packets have the unique address with source and destination address.

## History

IP was the connectionless datagram service in the original *Transmission Control Program* introduced by Vint Cerf and Bob Kahn in 1974. The other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP. IP versions 0 to 3 were experimental versions, used between 1977 and 1979. The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).

## Function

The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system that has two functions: identifying hosts; and providing a logical location service.



## Hyper Text Transfer Protocol (HTTP)

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses hyperlinks between nodes containing text. HTTP is the protocol to exchange or transfer hypertext. The standards development of HTTP was coordinated by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), culminating in the publication of a series of Requests for Comments (RFCs).

## History

The term hypertext was coined by Ted Nelson in 1965, which was in turn inspired by Vannevar Bush's vision (1930s) of the microfilm-based information retrieval and management "memex" system described in his essay As We May Think (1945). Tim Berners-Lee and his team at CERN are credited with inventing the original HTTP along with HTML and the associated technology for a web server and a text-based web browser. Berners-Lee first proposed the "WorldWideWeb" project in 1989 — now known as the World Wide Web. The first version of the protocol had only one method, namely GET, which would request a page from a server. The response from the server was always an HTML page.

The first documented version of HTTP was **HTTP V0.9** (1991). Dave Raggett led the HTTP Working Group (HTTP WG) in 1995 and wanted to expand the protocol with extended operations, extended negotiation, richer meta-information, tied with a security protocol which became more efficient by adding additional methods and header fields. RFC 1945 officially introduced and recognized HTTP V1.0 in 1996. The first definition of HTTP/1.1, the version of HTTP in common use, occurred in RFC 2068 in 1997, although this was obsoleted by RFC 2616 in 1999. A later version, the successor HTTP/2, was standardized in 2015, then supported by major web browsers and already supported by major web servers.

## File Transfer Protocol (FTP)

The **File Transfer Protocol** (**FTP**) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password. The first FTP client applications were command-line programs developed before operating systems

had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications.

### History

The original specification for the File Transfer Protocol was written by Abhay Bhushan born on 23 November 1944, in Allahabad, INDIA and published as RFC 114 on 16 April 1971. Until 1980, FTP run on Network Control Program (middle layers of the protocol stack running on host computers of the ARPANET), the predecessor of TCP/IP. The protocol was later replaced by a TCP/IP version, RFC 765 (June 1980) and RFC 959 (October 1985), the current specification. Several proposed standards amend RFC 959, for example RFC 2228 (June 1997) proposes security extensions and RFC 2428 (September 1998) adds support for IPv6 and defines a new type of passive mode.

### Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP node addressing mechanism. IP addressing enables every node on the TCP/IP network to be uniquely identifiable. IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of nodes. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for node addressing
- **Class B** - it uses first two octets for network addresses and last two for node addressing
- **Class C** - it uses first three octets for network addresses and last one for node addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses and Public address.

### Internet Protocol Version 6 (IPv6)

IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Node Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the nodes can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

- Dual stack implementation
- Tunneling
- NAT-PT

Next Layer in OSI Model is recognized as Transport Layer (Layer-4). All modules and procedures pertaining to transportation of data or data stream are categorized into this layer. As all other layers, this layer communicates with its peer Transport layer of the remote node.

Transport layer offers peer-to-peer and end-to-end connection between two processes on remote nodes. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.

## Functions

- This Layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments. It numbers every byte in the segment and maintains their accounting.
- This layer ensures that data must be received in the same sequence in which it was sent.
- This layer provides end-to-end delivery of data between nodes which may or may not belong to the same subnet.
- All server processes intend to communicate over the network are equipped with well-known Transport Service Access Points (TSAPs) also known as port numbers.

## End-to-End Communication

A process on one node identifies its peer node on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.

The two main Transport layer protocols are:

- **Transmission Control Protocol**

  It provides reliable communication between two nodes.

- **User Datagram Protocol**

  It provides unreliable communication between two nodes.

## Transmission Control Protocol (TCP)

The **Transmission Control Protocol** (**TCP**) is a protocol of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. Major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on TCP. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability.

## History

In May 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper titled "*A Protocol for Packet Network Intercommunication.*" The paper's authors, Vint Cerf and Bob Kahn, described an internetworking protocol for sharing resources using packet-switching among the nodes. A central control component of this model was the *Transmission Control Program* that incorporated both connection-oriented links and datagram services between hosts. The monolithic Transmission Control Program was later divided into a modular architecture consisting of the *Transmission Control Protocol* at the connection-oriented layer and the *Internet Protocol* at the internetworking (datagram) layer. The model became known informally as *TCP/IP*, although formally it was henceforth called the *Internet Protocol Suite*.

## Function

The Transmission Control Protocol provides a communication service between an application program and the Internet Protocol. It provides host-to-host connectivity at the Transport Layer of the Internet model.

At the lower levels of the protocol stack, due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets may be lost, duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost data, rearranges out-of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. If the data still remains undelivered, its source is notified of this failure. Once the TCP receiver has reassembled the sequence of packets originally transmitted, it passes them to the receiving application. Thus, TCP abstracts the application's communication from the underlying networking details. TCP is optimized for accurate delivery rather than timely delivery, and therefore, TCP sometimes incurs relatively long delays (on the order of seconds) while waiting for out-of-order messages or retransmissions of lost messages.

TCP is a reliable stream delivery service which guarantees that all bytes received will be identical with bytes sent and in the correct order. Since packet transfer over many networks is not reliable, a technique known as **positive acknowledgment** with **retransmission** is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgment message as it receives the data. The sender keeps **a record** of each packet it sends. The sender also maintains a **timer** from when the packet was sent, and retransmits a packet if the timer expires before the message has been acknowledged.

## Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.

- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**

## User Datagram Protocol

The **User Datagram Protocol** (**UDP**) is one of the core members of the Internet protocol suite. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768. UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network protocol. There is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

With UDP, computer applications can send messages, in this case referred to as *datagrams*, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. UDP is suitable for purposes where error checking and correction is either not necessary or is performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system. If error correction facilities are needed at the network interface level, an application may use the Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose.

## Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

## UDP application

Here are few applications where UDP is used to transmit data:

- Domain Name Services

- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

Application layer is the top most layer in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

A user may or may not directly interacts with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote node.

When an application layer protocol wants to communicate with its peer application layer protocol on remote node, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.

# Chapter-5

# INTERNET BASICS

The internet, is known and loved by everyone and it is the biggest growth area in Technology at the moment. The Internet is an international Network of Computers

The Internet is basically a very big Wide Area Network (WAN). It was originally developed by the US Government to improve communication between its military computers. If a cable is cut down, the information will take another path. It has since grown into what we all know today.

## To Connect Internet following steps are adopted:

- Most people access the Internet using a PC connected to a normal telephone line. Computers are attached to a telephone line via another piece of kit called a ADSL modem or DSL modem or usually called router.
- To connect to the Internet, you use your modem-router to connect to an Internet Service Provider (ISP) — these companies have computers permanently connected to the Internet. All the information sent from your PC goes via the ISP.

- The two most important pieces of software you need are a web browser to display web pages, and an e-mail client, which transmits and receives e-mail from a PC. Web browsers sometimes need plug-ins small programs — before they can play certain types of multimedia files, like videos, audio or text. The speed of an Internet connection is measured in Megabits per second – Mbps Three things determine the speed of access:

**Modem-Router Speed:** Modern domestic modem-routers are able to work to 6Mb. There is a technology that make modems run at 100Mbits per second.

**Telephone line:** In some cases, the line between home and the ISP server is an old copper cable with slow electronic controllers, so data goes very slow. In big cities, they use optic fibres so the line allows data to “move faster”.

**Volume of traffic:** The more people using the Internet, the slower the speed of access. In the UK the Internet is slower in the afternoon because that's when it's morning in the USA. In Spain, Mondays are horrible for internet traffic.

**Router**

Router essentially shares your Internet connection among multiple devices. A typical router is now a wireless router, and it creates and hosts a Wi-Fi network multiple devices can connect to. It likely has multiple Ethernet ports, too, allowing you to connect multiple devices. The router then connects to the Internet through the modem and the router itself receives a single public IP address on the Internet. Servers on the Internet communicate with your router, and the router routes that traffic to the appropriate devices on your home network. But, with just a router, you can't actually connect to the Internet. The router must be plugged into the Internet via an Ethernet cable. You need a modem to do so.

**Modem**

Your modem communicates with your Internet service provider's network. If it's a cable modem, it plugs into your cable provider's infrastructure via a coaxial cable. If it's a DSL modem, it plugs into your telephone line.

The modem communicates with your Internet service provider, and you'll need the correct type of modem that will work with your ISP's infrastructure.

The modem plugs into whatever type of infrastructure you have — cable, telephone, satellite, or fiber — and gives you a standard Ethernet cable output that you can plug into any router (or a single computer) and get an Internet connection.


**Combined Routers and Modems**

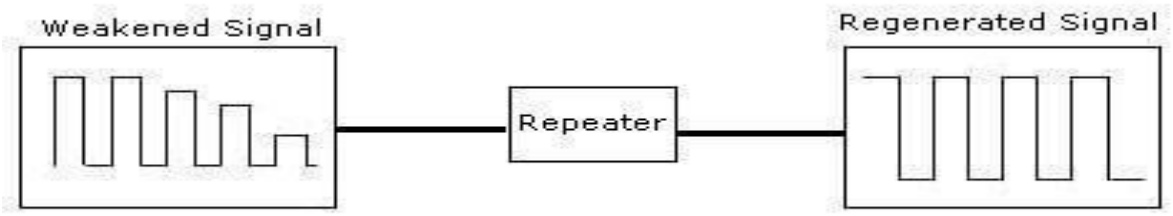
Some Internet service providers offer a modem and router in a single box. That box has the electronics and software in it to provide both functions, acting as a modem that communicates with your ISP and functioning as a router to create a home Wi-Fi network.

ISPs like offering all-in-one devices like these, but there's no reason you have to use one in the same box.

**Repeaters**

As signals travel along a network cable (or any other medium of transmission), they degrade and become distorted in a process that is called attenuation. If a cable is long enough, the attenuation will finally make a signal unrecognizable by the receiver.

A Repeater enables signals to travel longer distances over a network. Repeaters work at the OSI's Physical layer. A repeater regenerates the received signals and then retransmits the regenerated (or conditioned) signals on other segments.

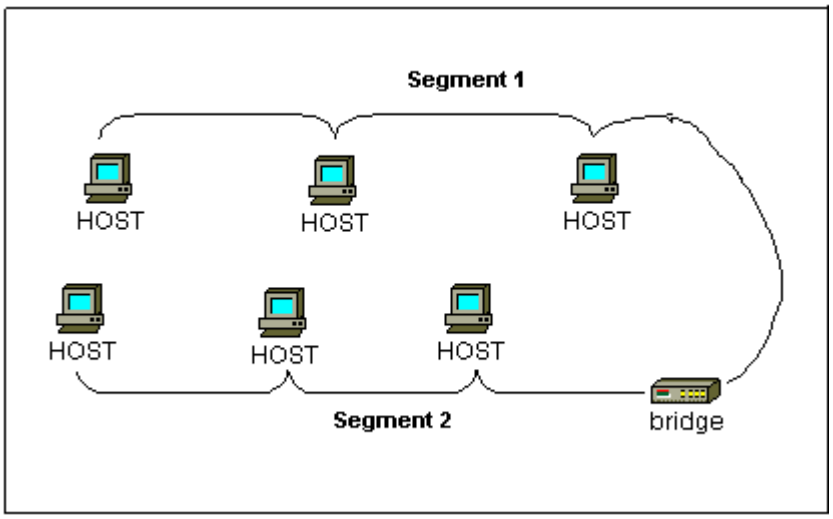



To pass data through the repeater in a usable fashion from one segment to the next, the packets and the Logical Link Control (LLC) protocols must be the same on the each segment. This means that a repeater will not enable communication, for example, between an 802.3 segment (Ethernet) and an 802.5 segment (Token Ring). That is, they cannot translate an Ethernet packet into a Token Ring packet. In other words, repeaters do not translate anything.

**Bridges**

Like a repeater, a bridge can join segments or workgroup LANs. However, a bridge can also divide a network to isolate traffic or problems. For example, if the volume of traffic from one or two computers or a single department is flooding the network with data and slowing down entire operation, a bridge can isolate those computers or that department.

In the following figure, a bridge is used to connect two segment (segment 1 and segment 2).



Bridges can be used to:

- Expand the distance of a segment.
- Provide for an increased number of computers on the network.
- Reduce traffic bottlenecks resulting from an excessive number of attached computers.

Bridges work at the Data Link Layer of the OSI model. Because they work at this layer, all information contained in the higher levels of the OSI model is unavailable to them. Therefore, they do not distinguish between one protocol and another.

Bridges simply pass all protocols along the network. Because all protocols pass across the bridges, it is up to the individual computers to determine which protocols they can recognize.

A bridge works on the principle that each network node has its own address. A bridge forwards the packets based on the address of the particular destination node.

As traffic passes through the bridge, information about the computer addresses is then stored in the bridge's RAM. The bridge will then use this RAM to build a routing table based on source addresses.

**Routers**

In an environment consisting of several network segments with different protocols and architecture, a bridge may not be adequate for ensuring fast communication among all of the segments. A complex network needs a device, which not only knows the address of each segment, but also can determine the best path for sending data and filtering broadcast traffic to the local segment. Such device is called a Router.

Routers work at the Network layer of the OSI model meaning that the Routers can switch and route packets across multiple networks. They do this by exchanging protocol-specific information between separate networks. Routers have access to more information in packets than bridges, and use this information to improve packet deliveries. Routers are usually used in a complex network situation because they provide better traffic management than bridges and do not pass broadcast traffic.

Routers can share status and routing information with one another and use this information to bypass slow or malfunctioning connections.

Routers do not look at the destination node address; they only look at the network address. Routers will only pass the information if the network address is known. This ability to control the data passing through the router reduces the amount of traffic between networks and allows routers to use these links more efficiently than bridge

**Gateways**

Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data.

A gateway repackages information to match the requirements of the destination system. Gateways can change the format of a message so that it will conform to the application program at the receiving end of the transfer.

A gateway links two systems that do not use the same:

- Communication protocols
- Data formatting structures
- Languages
- Architecture

For example, electronic mail gateways, such as X.400 gateway, receive messages in one format, and then translate it, and forward in X.400 format used by the receiver, and vice versa.

To process the data, the gateway:

Decapsulates incoming data through the networks complete protocol stack. Encapsulates the outgoing data in the complete protocol stack of the other network to allow transmission.

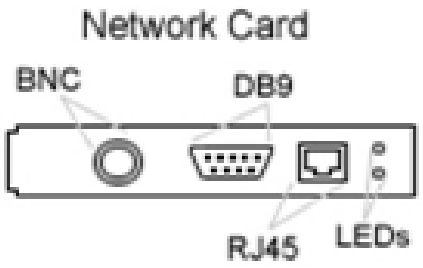
**NIC**

A NIC or Network Interface Card is a circuit board or chip, which allows the computer to communicate to other computers on a Network. This board when connected to a cable or other method of transferring data such as infrared can share resources, information and computer hardware. Local or Wide area networks are generally used for large businesses as well as are beginning to be found in homes as home users begin to have more than one computer. Utilizing network cards to connect to a network allow users to share data such as companies being able to have the capability of having a database that can be accessed all at the same time send and receive e-mail internally within the company or share hardware devices such as printers. **Connectors:**

Network cards have three main types of connectors. Below is an example of what a network card may look like.

- **BNC connector**

  As illustrated in the above picture the BNC connector is a round connector, which is used for thin net or 10Base-2 Local Area Network.



- **DB9 (RJ45 JACK)**

  The DB9 connector not to be confused with the Serial Port or sometimes referred to as the RJ45 JACK not to be confused with the RJ45 connection is used with Token Ring networks.

- **DB15 Connector**

  The DB15 connector is used for a Thick net or 10Base-5 Local area network.

- **RJ45 connector**

  Today one of the most popular types of connections used with computer networks. RJ45 looks similar to a phone connector or RJ11 connector however is slightly larger.

- **LED**

  The LED's as shown in the above illustration indicates if it detects a network generally by a green light which may flash as it communicates and then a red light which indicates collisions which will generally flash or not flash at all.

## WANs are long range Networks

WAN is short for Wide Area Network. They are used when the computers that need to be connected together are in different places. Like LANs, WANs need servers to operate the network, but users connect up to the network using modems, usually connected to the telephone system. Wireless technology such as microwaves or satellite can also be used. WANs are used by companies who have employees working away from the firm's main sites. A good example would be oil exploration engineers who work in remote parts of the world. They're also used by firms who have a lot of teleworkers.


## Advantage of using networks:

- Peripherals such as printers can be shared amongst many different users.
- Terminals are cheaper than stand-alone PCs
- Software can be shared amongst different users

- Communication across the network is cheaper and fast

**Disadvantages of using networks**

- Cabling can be expensive to install and replace
- A fault with the server will prevent the whole network from working.
- Security measures are needed to restrict access to the network.
- WANs are vulnerable to hackers and viruses.

**WLAN – Wireless network**

Wireless (WIFI) networks are just like fixed LANs but instead of using cables, devices are linked by radio waves. Each computer in a wireless network requires a wireless network interface card (MC). These can be built in or you can use plug-in adaptors. These allow each component in the network to communicate with a wireless access point (AP) to create a wireless local area network (WLAN).

The AP operates like a router in a fixed LAN. It also provides a bridge which plugs into the hub of a fixed LAN allowing both fixed and wireless users to talk to each other. If your LAN is connected to the Internet, the WLAN can also use it. If not, you can connect the WLAN to the Internet via an ADSL or cable modem.

**Advantages of a wireless Network:**

You don't need cabling. In older buildings, it can be expensive to install cables and access points. With WiFi, one access point can cover an entire floor or even a building. You can work anywhere within range of the access point. On a sunny day, you could work outside. You can make any room in the house your study. There are now WiFi hotspots in hotels, libraries and airports so you can link to a network away from home or your office.

**Disadvantages of a wireless Network:**

Fixed LANs can run at 1000 Mbps. Wireless networks are much slower and the further you are from an access point, the slower the rate. Although there are savings on the cost of cabling, wireless NICs are a bit more expensive than the wired versions. Then there is the problem of interference, if a neighbour is using the same channel and security. Other users may be able to intercept your data. Encryption programs like Wired Equivalent Privacy (WEP) can help.

**Web Browser**

The internet is the global network of computers which are all connected allowing us to share information and communicate with each other.

The World Wide Web is the series of web pages and files which are stored on the internet. You don't always use the World Wide Web when you're on the internet. For example, you might be making a Skype call or playing an online game. You're still using the internet but you're not using the World Wide Web as you're not looking at web pages or files which are stored on the internet. Each time you type WWW or see it in your browser, this is when you are using the World Wide Web.

A web browser is a piece of software for converting the code in which web pages are written in to things you can see and understand. The web browser displays the text, images and video which are contained on the internet in to a clear structure so they can be browsed and viewed easily. Without a web browser you would still be able to look at web pages, but they might not make any sense since they will be written in code which has not been translated.

**E-mail**

Electronic mail, or email, has become one of the most popular forms of communication. Not only does email save time and money, it can also be a great tool for personal as well as business communications. A basic email message is made up of seven parts

**Recipient's Address**

The first thing you need to enter when composing an email is the recipient's address. This is entered before you compose the body of the email. This field is usually found in one of the spaces above the message. An example of an email address is: johndoe@email.com. When sending a message to multiple recipients be sure to separate all addresses with a comma.

**Cc and Bcc**

Another option when sending a message to multiple recipients is to use the Cc, or carbon copy, and Bcc, blind carbon copy fields. When using the Cc feature, all recipients can see the email addresses of everyone the message was sent to. If you want your communication to be more private, choose the Bcc and the identities of the other recipients will not be shown.

**Date and Time Stamp**

The date and time an email was sent is usually included automatically somewhere in the message.

**Subject Line**

The subject line is the first part of your email that the recipient will see. When entering the subject line be sure to include important information such as what the email is about. If you are too vague or don't include any subject line at all, your message could be mistaken for spam and deleted without ever being read.

**Body**

The body is where you actually write the message that you want sent. Your message can be anything from a professional memo to a note to friend or family member. Try to avoid writing too much in an email and keep it limited to one screen's length. If you have a lot of information that needs to be sent include it as an attached file.

Attachments

Attachments are similar to enclosures in traditional mail. If you have files that you want to share with your recipient's you can include them as attachments to the email. Use caution when opening attachments sent to you as they can contain viruses, and never open an attachment from somebody you don't know.

Signature

Some email systems allow you to enter a signature that will appear automatically at the bottom of every message you send. This feature is optional and can be turned off and on as needed.

## KEEPING DATA SAFE FROM ACCIDENTAL DAMAGE

Accidental damage is a huge risk to your data if you do not take measures to prevent it. It can cause the loss of important documents and files, or even entire servers of information. Accidents which affect data loss could include fires, natural, disasters like floods and accidental deletion. There are several ways to prevent accidental damage:

- Always keep a backup - The most fundamental way to prevent loss from accidents is to keep all of your data backed up on a different hard drive. While this may not prevent accidents it does mean that if one happens, you haven't lost everything. It's important to back up your data frequently and keep the backup copy in a different location from the original as it will then not be affected by a fire or flood.
- **Find the right environment -** Storing data is all about making sure that it's safe from damage. An easy way to do this is to make sure that the location where it is kept is well ventilated, has appropriate safety systems like sprinklers and it an appropriate temperature.
- **Use a good filing system** - Data is often accidentally deleted by a user because they think it is not important. This could be because it has not been named correctly or kept in the correct location. Calling a document Untitled1 and saving it to your desktop is not a safe way of working.
- **Train your staff -** Proper training on how to use the computer system if you own a company could prevent people from accidentally deleting data through lack of

understanding. Make sure all of your staff know the correct way of dealing with the computer.

**KEEPING DATA SAFE FROM UNAUTHORISED ACCESS**

Perhaps an even more worrying scenario is someone getting access to your data who should have access to it. This can be a huge problem for well-known companies and government organisations who constantly find themselves the target of cyber-attacks. The following steps can prevent this or at least reduce the risk:

- **Change passwords frequently -** Changing your password can stop people who have discovered your password from having access for an extended length of time. Doing this every day would mean that the person who had found your password would only have a maximum of 24 hours to access your files.
- **Password protect documents -** As well as having a password for the user accounts, it's also a good idea to password protect each document. This means that even if someone gets access to an account they won't be able to look at the information. You might also want to let people look at documents but not edit them. Many software packages have functionality for this which prevents people accidentally changing things.
- **Keep a backup** - Although this won't prevent people from looking at the documents, it can mean that if they delete them, they are not lost forever. Again though, you have to make sure you backup frequently otherwise you will not have the newest documents on your backup drive.

**THE DIFFERENT TYPES OF OPERATING SYSTEM**

- **Real-Time** - A real time operating system is an operating system which has a goal of transferring information in a specific time frame. They are often used in machinery and manufacturing processes where timing is extremely important — for example when producing something where several aspects of a process have to work together seamlessly. The operating system usually comes from the creator installed on the system and does not easily allow changes or have added utilities.
- **Single-user, single task** - As the name implies, this operating system is designed to manage the computer so that one user can effectively do one thing at a time. The Palm OS for Palm handheld computers is a good example of a modern single-user, single-task operating system.
- **Single-user, multi-tasking** - This is the type of operating system most people use on their desktop and laptop computers today. Microsoft's Windows and Apple's Mac OS

platforms are both examples of operating systems that will let a single user have several programs in operation at the same time. For example, it's entirely possible for a Windows user to be writing a note in a word processor while downloading a file from the Internet while printing the text of an e-mail message.

- **Multi-user** - A multi-user operating system allows many different users to take advantage of the computer's resources simultaneously. The operating system must make sure that the requirements of the various users are balanced, and that each of the programs they are using has sufficient and separate resources so that a problem with one user doesn't affect the entire community of users. Unix, VMS and mainframe operating systems, such as *MVS,* are examples of multi-user operating systems.

**Secure Socket Layer (SSL)**

We've looked at keeping things safe on your own computer system, but what about if you're sending things over the internet. How can you prevent people from intercepting them? Every day millions of transactions take place online, and credit card numbers, bank account details and addresses are transferred without a thought for how they might be protected. The key to protecting these is an encryption system called SSL. SSL stands for Secure Socket Layer (although the newer version is called TSL - Transport Socket Layer).

SSL is way of 'encrypting' your data online. This means that instead of transferring your bank details, your computer turns them in to an unreadable code before it sends them using a complex system of encryption. The receiving computer knows how to unscramble the code but doesn't share this information with anyone else. They unscramble the code and use the bank details to make the transaction. This means that if someone steals the bank details on the way to their destination, they can't read them.

**PUBLIC KEY AND PRIVATE KEY ENCRYPTION**

To encrypt data you need to have a 'key'. A key just means the method that you use to make the code secret or to turn it back in to a readable piece of information. You may have used encryption before to create coded messages in school. A simple method is to move every letter up a certain number of times. For example, replace all Cs with Fs, all Js with Ms etc. This is called private key encryption. The way that the code is created has to be kept private otherwise someone will easily be able to unscramble the sentence. If I were to tell you the key of my code was moving all the letters up 3 places in the alphabet you'd know exactly what I was writing.

The problem with using private key encryption online is that as well as sending your encrypted information to the place you're buying things, you also have to send the key (the method of unscrambling the data) otherwise they won't be able to read it. This means that any hackers intercepting information will be able to get the key as you send it

To overcome this problem, SSL uses something called public key encryption. This means that the method of encrypting your data (making it secret) is different from the method used to decrypt it (make it readable again). When you are ready to send your bank details, the receiving computer will send you a code to use to encrypt your information. This is called the public key. The public key can only be used to encryp and not decrypt. The receiving computer then uses their private key which they never give out to decrypt the bank details you sent. Imagine a door which has two keys, the public key locks the door but only the private key can unlock it.

This might sound impossible - if I replace all Fs with Js to make the code, how can it be a different system to turn it back. The answer is that public key encryption like SSL uses two keys which are mathematically linked by using prime numbers. This means that by knowing the way to encrypt the code, you don't know the way to decrypt the code. For example, I could tell you that my public key was 54 but you wouldn't know that my private key was 48+6 as it could be a large combination of possible products.

By using public key encryption it means that if someone gets hold of the public key all they can do is encrypt things. The private key is never sent out and remains safe on the server of the receiving computer.

**KEY LENGTH**

How strong public key encryption is is based on how long the 'key' is. The length of the key relates to how many possible combination there are.

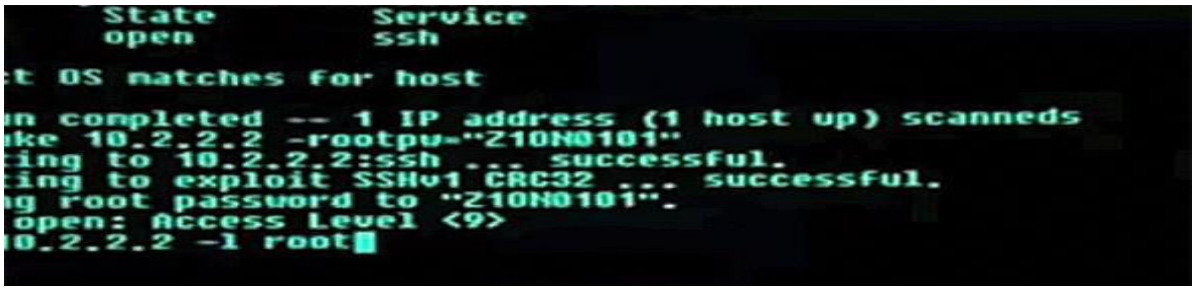
For example, a key length of two would mean that there are only two possible combinations for the code. This obviously wouldn't take long as you only have to try a maximum of two methods to crack the code.

On computers, key sizes are measured in bits. For example, 128 bit encryption means that there are 128 0s and 1s in the key. Therefore there are 2 to the power of 128 possible combinations. This is 340,282,366,920,938,463,463,374,607,431,768,211,456 possibilities. With this many possible combinations it would take a long, long time to figure out the key just by trying different combinations.

It is possible to use massive key lengths like 1024 bit. However, it's pointless simply because a computer would never be able to figure out a key length of half that size.

## HOW HACKERS WORK

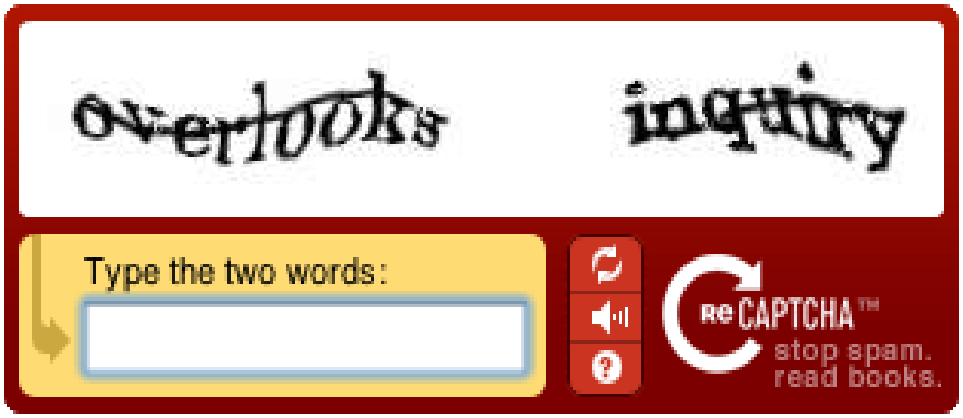
The main reason we use any of the systems above is to prevent hackers. Hacking is to unlawfully gain access to a computer system, and there are many ways of doing it, as you will




see. Below is a table showing the most popular methods hackers use to gain access to our information, and how you can prevent them

### Brute Forcing

Using a program called a brute forcing bot (short for robot) to try a large combination of passwords to gain access to a system. The program has a list of possible passwords (or a dictionary) and tries each one in turn at a very high speed. This is the reason some websites as you to pass a 'captcha' when you enter a password - to prove you are not a robot program.




Make sure you have a long and complicated password which contains both letters and numbers. Also, website developers can ensure they use systems like captcha to prevent bots.

### Port Scanning

A port is a virtual connection from the internet to your computer. There are several ports which are assigned to programs so that they can have access to the internet so that they can run automatic updates and download features. Sometimes these ports are left 'open' meaning that anyone get access to your computer using them. A port scanning program issued to find these prevention.

Make sure you have a firewall installed on your computer. A firewall is a piece of software which scans each incoming and outgoing connection to a computer to make sure they are safe.

## War Driving

War driving is simply the act of driving around and looking for unsecure WIFI networks. These can then be used to access the internet to hack without being traceable. Always have a complex password for your WIFI connection and change it regularly.

## Password Cracking

A website or program which asks you for a password has been programmed to do this in the code. Hackers are sometimes able to find this code and change it so that it no longer asks for password. Software cracking means finding the part of the code which gets a user to register or pay and removing it to access the software for free.

A firewall will again prevent people from gaining access to your computer to change things. Also make sure that you use a reputable web host to host your website who have proper security in place.

## Social Engineering

Some hackers are able to find passwords and access systems without even using a computer themselves. Social engineering means to psychologically manipulate a person in to giving you their password or network access. For example a hacker may pretend to be from technical support.

# Chapter-6

# Glossary

**10Base2** - Ethernet specification for thin coaxial cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 185 meters per segment.

**10Base5** - Ethernet specification for thick coaxial cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 500 meters per segment.

**10BaseF** - Ethernet specification for fiber optic cable, transmits signals at 10 Mbps (megabits per second) with a distance limit of 2000 meters per segment.

**10BaseT** - Ethernet specification for unshielded twisted pair cable (category 3, 4, or 5), transmits signals at 10 Mbps (megabits per second) with a distance limit of 100 meters per segment.

**100BaseT** - Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 100 Mbps (megabits per second) with a distance limit of 100 meters per segment.

**1000BaseTX** -Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 1 Gbps (gigabits per second) with a distance limitation of 220 meters per segment.

**Algorithm -** A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

**AppleTalk** - Apple Computer's network protocol originally designed to run over LocalTalk networks, but can also run on Ethernet and Token Ring. **Applet -**Java programs, an application program that uses the clients web browser to provide a user interface.

**ARPANET -** Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

**Asynchronous Transfer Mode (ATM)** - A network protocol that transmits data at a speed of 155 Mbps and higher. It is most often used to interconnect two or more local area networks.

**AUI Connector** (Attachment Unit Interface) - A 15 pin connector found on Ethernet cards that can be used for attaching coaxial, fiber optic, or twisted pair cable.

**Access Control -** Access Control ensures that resources are only granted to those users who are entitled to them.

**Authentication -** Authentication is the process of confirming the correctness of the claimed identity.

**Authenticity -** Authenticity is the validity and conformance of the original information.

**Authorization -** Authorization is the approval, permission, or empowerment for someone or something to do something.

**Availability -** Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

**Backbone** - A cable to which multiple nodes or workstations are attached.

**Bandwidth -** Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

**Banner -** A banner is the information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use.

**Basic Authentication -** Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.

**BIND -** BIND stands for Berkeley Internet Name Domain and is an implementation of DNS. DNS is used for domain name to IP address resolution.

**Biometrics -** Biometrics use physical characteristics of the users to determine access.

**Bit -** The smallest unit of information storage; a contraction of the term "binary digit;" one of two symbols "0" (zero) and "1" (one) - that are used to represent binary numbers.

**BNC Connector -** Standard connector used to connect 10Base2 coaxial cable.

**Boot Record Infector -** A boot record infector is a piece of malware that inserts malicious code into the boot sector of a disk.

**Bridge** - Devices that connect and pass packets between two network segments that use the same communications protocol.

**Broadcast -** To simultaneously send the same message to multiple recipients. One host to all hosts on network.

**Broadcast Address -** An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

**Browser -** A client computer program that can retrieve and display information from servers on the World Wide Web.

**Byte -** A fundamental unit of computer storage. Usually holds eight bits.

**Cable** - Transmission medium of copper wire or optical fiber wrapped in a protective cover.

**Cache -** Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an

independent high-speed storage device. Two types of caching are commonly used in personal computers. Memory caching and disk caching.

**Cell -** A cell is a unit of data transmitted over an ATM network.

**Ciphertext -** Ciphertext is the encrypted form of the message being sent.

**Client -** A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

**Coaxial Cable** - Cable consisting of a single copper conductor in the center surrounded by a plastic layer for insulation and a braided metal outer shield.

**Collision -** A collision occurs when multiple systems transmit simultaneously on the same wire.

**Computer Network -** A collection of host computers together with the sub-network or inter-network through which they can exchange data.

**Concentrator** - A device that provides a central connection point for cables from workstations, servers, and peripherals. Most concentrators contain the ability to amplify the electrical signal they receive.

**Cron -** Cron is a Unix application that runs jobs for users and administrators at scheduled times of the day.

**Crossover Cable -** A crossover cable reverses the pairs of cables at the other end and can be used to connect devices directly together.

**CSMA/CA** - Carrier Sense Multiple Access Collision Avoidance is a network access method in which each device signals its intent to transmit before it actually does so. This prevents other devices from sending information, thus preventing collisions from occurring between signals from two or more devices. This is the access method used by LocalTalk.

**CSMA/CD** - Carrier Sense Multiple Access Collision Detection is a network access method in which devices that are ready to transmit data first check the channel for a carrier. If no carrier is sensed, a device can transmit. If two devices transmit at once, a collision occurs and each computer backs off and waits a random amount of time before attempting to retransmit. This is the access method used by Ethernet.

**Cut-Through -** Cut-Through is a method of switching where only the header of a packet is read before it is forwarded to its destination.

**Cyclic Redundancy Check (CRC) -** Sometimes called "cyclic redundancy code." A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

**Data Encryption Standard (DES) -** A widely-used method of data encryption

using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

**Data Mining -** Data Mining is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business.

**Data Owner -** A Data Owner is the entity having responsibility and authority for the data.

**Data Warehousing -** Data Warehousing is the consolidation of several previously independent databases into one location.

**Decryption -** Decryption is the process of transforming an encrypted message into its original plaintext.

**Denial of Service -** The prevention of authorized access to a system resource or the delaying of system operations and functions.

**Digital Envelope -** A digital envelope is an encrypted message with the encrypted session key.

**Digital Signature -** A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message that changed since transmission.

**DIN** - A plug and socket connector consisting of a circular pattern of pins in a metal sleeve. This type of connector is commonly seen on keyboards.

**Distance Vector -** Distance vectors measure the cost of routes to determine the best route to all known networks.

**Distributed Scans -** Distributed Scans are scans that use multiple source addresses to gather information.

**Domain -** On the Internet, a domain consists of a set of network addresses. In Windows NT and Windows 2000, a domain is a set of network resources

**Domain Name -** A domain name locates an organization or other entity on the Internet..

**Domain Name System (DNS) -** The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember for an Internet address.

**Dumb Terminal** - Refers to devices that are designed to communicate exclusively with a host (main frame) computer. It receives all screen layouts from the host computer and sends all keyboard entry to the host. It cannot function without the host computer.

**Dynamic Link Library -** A collection of small programs, any of which can be called when needed by a larger program that is running in the computer.

**E-mail** - An electronic mail message sent from a host computer to a remote computer.

**Eavesdropping -** Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.

**End User** - Refers to the human executing applications on the workstation.

**Ethernet** - A network protocol invented by Xerox Corporation and developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps (megabits per second).

**Expansion Slot** - Area in a computer that accepts additional input/output boards to increase the capability of the computer.

**Event -** An event is an observable occurrence in a system or network.

**Fast Ethernet** - An Ethernet standard that supports 100 Mbps using category 5 twisted pair or fiber optic cable.

**Fiber Distributed Data Interface (FDDI)** - A network protocol that is used primarily to interconnect two or more local area networks, often over large distances.

**Fiber Optic Cable** - A cable, consisting of a center glass core surrounded by layers of plastic, that transmits data using light rather than electricity. It has the ability to carry more information over much longer distances.

**File Server** - A computer connected to the network that contains primary files/applications and shares them as requested with the other computers on the network. If the file server is dedicated for that purpose only, it is connected to a client/server network. An example of a legacy client/server network is Novell Netware. All the computers connected to a peer-to-peer network are capable of being the file server. Most modern operating systems can operate as servers or as clients, greying the distinction in the server architecture.

**File Transfer Protocol (FTP) -** A TCP/IP protocol specifying the transfer of text or binary files across the network.

**Filter -** A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

**Firewall** - A security device which inspects traffic entering and leaving a network, and allows or disallows the traffic, depending on rules describing acceptable use of the network, by filtering out unwanted packets. The firewall is usually positioned as the gateway device to another network, such as the internet. Many routers now contain firewalls. A personal firewall is usually software that runs on a workstation or server to filter unwanted traffic at the individual machine.

**Fragmentation -** The process of storing a data file in several "chunks" or fragments

rather than in a single contiguous sequence of bits in one place on the storage medium.

**Frames -** Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data.

**Full Duplex -** A type of duplex communications channel which carries data in both directions at once. Communications in which both sender and receiver can send at the same time.

**Fully-Qualified Domain Name -** A Fully-Qualified Domain Name is a server name with a hostname followed by the full domain name.

**Gateway -** A network point that acts as an entrance to another network.

**Gigabit Ethernet** - An Ethernet protocol that raises the transmission rates to 1 Gbps (gigabits per second). Most school, corporate, and household networks provide gigabit ethernet to the workstations via cabled connections.

**Gigabyte** (GB) - One billion bytes of information. One thousand megabytes.

**GNU -** GNU is a Unix-like operating system that comes with source code that can be copied, modified, and redistributed. The GNU project was started in 1983 by Richard Stallman and others, who formed the Free Software Foundation.

**Gnutella -** An Internet file sharing utility. Gnutella acts as a server for sharing files while simultaneously acting as a client that searches for and downloads files from other users.

**Header -** A header is the extra information in a packet that is needed for the protocol stack to process the packet.

**Host -** Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

**HTTP Proxy -** An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

**Hub -** A hub is a network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub.

**Hyperlink -** In hypertext or hypermedia, an information object that points to related information that is located elsewhere and can be retrieved by activating the link.

**Hypertext Markup Language (HTML) -** The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

**Hypertext Transfer Protocol (HTTP) -** The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

**Hub** - A hardware device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat but merely split signals sent through them).

**Infrared** - Electromagnetic waves whose frequency range is above that of microwaves, but below that of the visible spectrum.

**Integrity -** Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

**Internet -** A term to describe connecting multiple separate networks together.

**Internet Message Access Protocol (IMAP) -** A protocol that defines how a client should fetch mail from and return mail to a mail server. IMAP is intended as a replacement for or extension to the Post Office Protocol.

**Internet Protocol (IP) -** The method or protocol by which data is sent from one computer to another on the Internet.

**Intranet -** A computer network, especially based on Internet technology that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

**Intrusion Detection -** A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

**IP Address -** A computer inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

**IP Spoofing -** The technique of supplying a false IP address.

**ISO -** International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

**Kernel -** The essential center of a computer operating system, the core that provides basic services for all other parts of the operating system. A synonym is nucleus. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. Kernel and shell are terms used more frequently in Unix and some other operating systems than in IBM mainframe systems.

**LAN** (Local Area Network) - A network connecting computers in a relatively small area such as a building.

**Linear Bus** - A network topology in which each node attaches directly to a common cable.

**LocalTalk** - Apple Corporation proprietary protocol that uses CSMA/CA media access scheme and supports transmissions at speeds of 230 Kbps (Kilobits per second).

**Logic Gate -** A logic gate is an elementary building block of a digital circuit. Most logic gates have two inputs and one output. As digital circuits can only understand binary, inputs and outputs can assume only one of two states, 0 or 1.

**MAN** (Metropolitan Area Network) - A network connecting computers over a large geographical area, such as a city or school district.

**MAU** (Multistation Access Unit) - A Token Ring wiring hub.

**Modem** (Modulator/Demodulator) - Devices that convert digital and analog signals. Modems allow computer data (digital) to be transmitted over voice-grade telephone lines (analog).

**Multiplexer** - A device that allows multiple logical signals to be transmitted simultaneously across a single physical channel.

**MAC Address -** A physical address, a numeric value that uniquely identifies that network device from every other device on the planet.

**Malicious Code -** Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

**Malware -** A generic term for a number of different types of malicious code.

**Multiplexing -** To combine multiple signals from possibly disparate sources, in order to transmit them over a single path.

**Network Modem** - A modem connected to a Local Area Network (LAN) that is accessible from any workstation on the network.

**Network Interface Card** (NIC) - A board that provides network communication capabilities to and from a computer.

**Network Mapping -** To compile an electronic inventory of the systems and the services on your network.

**Network Operating System** (NOS) - Operating system designed to pass information and communicate between more than one computers. Examples include Linux/Unix and Windows Server.

**Node** - End point of a network connection. Nodes include any device attached to a network such as file servers, printers, or workstations.

**Node Devices** - Any computer or peripheral that is connected to the network.

**Octet -** A sequence of eight bits. An octet is an eight-bit byte.

**Packet -** A piece of a message transmitted over a packet-switching network. One of

the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

**Packet Switched Network -** A packet switched network is where individual packets each follow their own paths through the network from one endpoint to another.

**Partitions -** Major divisions of the total physical hard disk space.

**Password Authentication Protocol (PAP) -** Password Authentication Protocol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear.

**Password Cracking -** Password cracking is the process of attempting to guess passwords, given the password file information.

**Password Sniffing -** Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

**Patch -** A patch is a small update released by a software manufacturer to fix bugs in existing programs.

**Patching -** Patching is the process of updating software to a different version.

**PCMCIA** - (later versions were **PCMCIA2** and **PC Card**) An expansion slot found in many laptop computers. Largely replaced by USB in the 2000-2010 period.

**Peer-to-Peer Network** - A network in which resources and files are shared without a centralized management source.

**Penetration Testing -** Penetration testing is used to test the external perimeter security of a network or facility.

**Personal Firewalls -** Personal firewalls are those firewalls that are installed and run on individual PCs.

**Phishing -** The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

**Physical Topology** - The physical layout of the network; how the cables are arranged; and how the computers are connected.

**Plaintext -** Ordinary readable text before being encrypted into ciphertext or after being decrypted.

**Point-to-Point** - A direct link between two objects in a network.

**Point-to-Point Protocol (PPP) -** A protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. It packages your computer TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

**Point-to-Point Tunneling Protocol (PPTP) -** A protocol (set of communication rules) that allows corporations to extend

their own corporate network through private "tunnels" over the public Internet.

**Polymorphism -** Polymorphism is the process by which malicious software changes its underlying code to avoid detection.

**Ports** - A connection point for a cable.

**Possession -** Possession is the holding, control, and ability to use information.

**Post Office Protocol, Version 3 (POP3) -** An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client.

**Proprietary Information -** Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

**Protocol** -A formal description of a set of rules and conventions that govern how devices on a network exchange information.

**Protocol Stacks (OSI) -** A set of network protocol layers that work together.

**Proxy Server -** A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

**Public Key -** The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

**RAID** (Redundant Array of Inexpensive Disks) - A configuration of multiple disks designed to preserve data after a disk casualty.

**RAM** (Random Access Memory) - The working memory of a computer where data and programs are temporarily stored. RAM only holds information when the computer is on.

**Registry -** he Registry in Windows operating systems in the central set of settings and information required to run the Windows computer.

**Regression analysis -** The use of scripted tests which are used to test software for all possible input is should expect. Typically developers will create a set of regression tests that are executed before a new version of a software is released.

**Repeater** - A device used in a network to strengthen a signal as it is passed along the network cable

**Request for Comment (RFC) -** A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if

it gains enough interest, it may evolve into an Internet standard.

**RJ-45** - Standard connectors used for unshielded twisted-pair cable.

**Root -** Root is the name of the administrator account in Unix systems.

**Rootkit -** A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

**Router -** Routers interconnect logical networks by forwarding information to other networks based upon IP addresses.

**SCSI (Small Computer Serial Interface)** - An interface controller that allows several peripherals to be connected to the same port on a computer.

**Segment** - Refers to a section of cable on a network. In Ethernet networks, two types of segments are defined. A populated or trunk segment is a network cable that has one or more nodes attached to it. A link segment is a cable that connects a computer to an interconnecting device, such as a repeater or concentrator, or connects a interconnecting device to another interconnecting device.

**Security Policy -** A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

**Segment -** Segment is another name for TCP packets.

**Server-**A system entity that provides a service in response to requests from other system entities called clients.

**Session -** A session is a virtual connection between two hosts by which network traffic is passed.

**Shell -** A Unix term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter. A shell usually implies an interface with a command syntax (think of the DOS operating system and its "C:>" prompts and user commands such as "dir" and "edit").

**Signature -** A Signature is a distinct pattern in network traffic that can be identified to a specific tool or exploit.

**Sneaker-Net** - Refers to a manual method of sharing files in which a file is copied from a computer to a floppy disk, transported to a second computer by a person physically walking (apparently wearing sneakers) to the second computer, and manually transferring the file from floppy disk to the second computer.

**Socket -** The socket tells a host's IP stack where to plug in a data stream so that it connects to the right application.

**Software -** Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be

dynamically written or modified during execution.

**Source Port -** The port that a host uses to connect to a server. It is usually a number greater than or equal to 1024. It is randomly generated and is different each time a connection is made.

**Spam -** Electronic junk mail or junk newsgroup postings.

**Speed of Data Transfer** - The rate at which information travels through a network, usually measured in megabits per second.

**Spoof -** Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

**Star Topology** - LAN topology in which each node on a network is connected directly to a central network hub or concentrator.

**Star-Wired Ring** - Network topology that connects network devices (such as computers and printers) in a complete circle.

**Sub Network -** A separately identifiable part of a larger network that typically represents a certain limited number of host computers, the hosts in a building or geographic area, or the hosts on an individual local area network.

**Subnet Mask -** A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.

**Switch -** A switch is a networking device that keeps track of MAC addresses attached to each of its ports so that data is only transmitted on the ports that are the intended recipient of the data.

**Switched Network -** A communications network, such as the public switched telephone network, in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. Any network providing switched communications service.

**Synchronization -** Synchronization is the signal made up of a distinctive pattern of bits that network hardware looks for to signal that start of a frame.

**Syslog -** Syslog is the system logging facility for Unix systems.

**System Security Officer (SSO) -** A person responsible for enforcement or administration of the security policy that applies to the system.

**System-Specific Policy -** A System-specific policy is a policy written for a specific system or device**Switch** - A "intelligent" type of hub, in that it sends packets only to the intended ports, rather than all computers on the network.

**T1, T3 -** A digital circuit using TDM (Time-Division Multiplexing).

**Tamper -** To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

**Tape Back-Up** - A common server or network peripheral which allows copying data and programs from a computer system to magnetic tape. On tape, data is stored sequentially. When retrieving data, the tape is searched from the beginning of tape until the data is found.

**TCP Full Open Scan -** TCP Full Open scans check each port by performing a full three-way handshake on each port to determine if it was open.

**TCP Half Open Scan -** TCP Half Open scans work by performing the first half of a three-way handshake to determine if a port is open.

**TCP Wrapper -** A software package which can be used to restrict access to certain network services based on the source of the connection; a simple tool to monitor and control incoming network traffic.

**TCP/IP -** A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

**TELNET -** A TCP-based, application-layer, Internet Standard protocol for remote login from one host to another.

**Terminator** - A device that provides electrical resistance at the end of a transmission line. Its function is to absorb signals on the line, thereby keeping them from bouncing back and being received again by the network.

**Threat -** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

**Thicknet** - A thick coaxial cable that is used with a 10Base5 Ethernet LAN.

**Thinnet** - A thin coaxial cable that is used with a 10Base2 Ethernet LAN.

**Token** - A special packet that contains data and acts as a messenger or carrier between each computer and device on a ring topology. Each computer must wait for the messenger to stop at its node before it can send data over the network.

**Token Ring** - A network protocol developed by IBM in which computers access the network
through token-passing. Usually uses a star-wired ring topology.

**Topology** - There are two types of topology: physical and logical. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Logical topology is the method used to pass the information

between workstations. Issues involving logical topologies are discussed on the Protocol chapter

**Transceiver** (Transmitter/Receiver) - A Device that receives and sends signals over a medium. In networks, it is generally used to allow for the connection between two different types of cable connectors, such as AUI and RJ-45.

**Transmission Control Protocol (TCP) -** A set of rules (protocol) used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

**Transport Layer Security (TLS) -** A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

**Tree Topology** - LAN topology similar to linear bus topology, except that tree networks can contain branches with multiple nodes.

**Trojan Horse -** A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

**Trunking -** Trunking is connecting switched together so that they can share VLAN information between them.

**Trust -** Trust determine which permissions and what actions other systems or users can perform on remote machines.

**Tunnel -** A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a logical point-to-point link

**Twisted Pair** - Network cabling that consists of four pairs of wires that are manufactured with the wires twisted to certain specifications. Available in shielded and unshielded versions.

**UDP Scan -** UDP scans perform scans to determine which UDP ports are open.

**Unicast -** Broadcasting from host to host.

**Uniform Resource Identifier (URI) -** The generic term for all types of names and

addresses that refer to objects on the World Wide Web.

**Uniform Resource Locator (URL) -** The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, http://www.pcwebopedia.com/index.html .

**Unix -** A popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s. Created by just a handful of programmers, Unix was designed to be a small, flexible system used exclusively by programmers.

**USB/ USB2 Port** - A hardware interface for peripherals from keyboards to hard drives, widely used on all computers.

**User -** A person, organization entity, or automated process that accesses a system, whether

**User Datagram Protocol (UDP) -** A communications protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network.

**Virtual Private Network (VPN) -** A restricted-use, logical computer network that is constructed from the system resources of a relatively public, physical network, often by using encryption and often by tunneling links of the virtual network across the real network.

**Virus -** Vital Information Resources Under Seize. A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting

**WAN** (Wide Area Network) - A network connecting computers within very large areas, such as states, countries, and the world.

**Web Server -** A software process that runs on a host computer connected to the Internet to respond to HTTP requests for documents from client web browsers.

**WHOIS -** An IP for finding information about resources on networks.

**Windump -** Windump is a freeware tool for Windows that is a protocol analyzer that can monitor network traffic on a wire.

**World Wide Web ("the Web", WWW, W3) -** The global, hypermedia-based collection of information and services that is available on Internet servers and is accessed by browsers using Hypertext Transfer Protocol and other information retrieval mechanisms.

**Worm -** A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

**Workstation** - A computer connected to a network at which users interact with software stored on the network.

**Workgroup** - A collection of workstations and servers on a LAN that are designated to communicate and exchange data with one another.

**Zombies -** A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

..previous publications


ISBN.....