UNIT I DATA COMMUNICATION MODEL

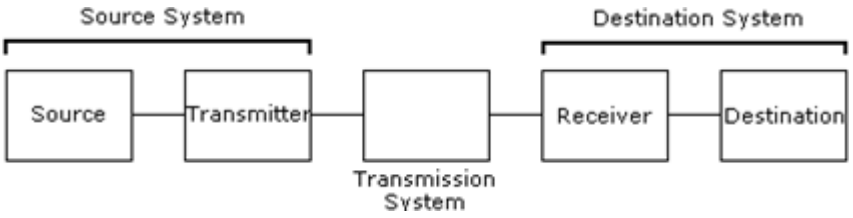
1.1Basic Communication Model

Data Communications is the transfer of data or information between a source and a receiver. The source transmits the data and the receiver receives it. Data communication involved the following like communication networks, different communication services required, the kind of networks available, protocol architectures, OSI models, TCP/IP protocol models etc. Data Communication is interested in the transfer of data, the method of transfer and the preservation of the data during the transfer process.

In Local Area Networks, we are interested in "connectivity", connecting computers together to share resources. Even though the computers can have different disk operating systems, languages, cabling and locations, they still can communicate to one another and share resources.

A Communication model is used to exchange data between two parties. For example: communication between a computer, server and telephone (through modem).

The purpose of Data Communications is to provide the rules and regulations that allow computers with different disk operating systems, languages, cabling and locations to share resources. The rules and regulations are called protocols and standards in Data Communications.



Source
It is the generator of data that will pass on the destination using networks. Without any request source never passes the data to destination. So, if source is passing the data means any of the destinations is requesting for data using some query languages.
Transmitter
It is simply a device used to convert the data as per the destination requirement. For example a modem, converts the analog (telephonic signals) signal to digital (computer signals) signals and alternatively digital to analog also.
Transmission System
To transmit the data on different connected systems we use different transmission systems. Data transmission using transmission system means the physical transfer of data over point-to-point or point-to-multipoint communication channels. Example of such channels are copper wires, optical fibers even wireless communication channels etc.
Receiver
This receives the signals from the transmission system and converts it into a form that is suitable to the destination device. For example, a modem accepts analog signal from a transmission channel and transforms it into digital bit stream which is acceptable by computer system.
Destination
It is simply a device for which source device sends the data.

1.2 Data Communication System Tasks

There are some tasks performed by the communication systems are:

Signal Generation: To transmit the data over the transmission system, communicating device must be able to generate and receive these signals. The generation of the signals should be in such a way that the resultant signal can be acceptable by the transmission mediums.

Interface: Device must interface with the transmission system to communicate or transfer the data over network.
Data Synchronization: It is the process of establishing consistency among data from a source to destination devices and vice versa and continuous harmonization of the data over time.
Exchange Management: For meaningful data transaction there should be some management of data being exchanged. Both the transmitter and receiver should adhere to some common convention about the format of data, amount of data, time required, data format etc.
Transmission System Utilization: Due to the importance of Data transmissions without interruptions or failures the transmission systems is usually well dimensioned and are being operated with margins that minimize the possibility of outages. Various techniques are available to allocate the total capacity of a transmission channel among connected devices like Digital, Analog, Multiplex, Simplex, Duplex, Half-Duplex etc.
Error Detection and Correction: In any communication system transmitted data is prone to error. Either it is because of transmitted signal getting distorted in the transmission medium leading to misinterpretation of signal or errors introduced by the intermediate devices. Error detection and correction is required in cases where there is no scope for error in the data transaction. We can think of file transfer between two computers or even on remote network computers where there is a need for this. But in some cases it may not be very important as in the case of telephonic conversation.
Flow Control: At the time of transmission of data, source computer is generating data faster than receiver device capable to receive it. To handle such problem, there is some kind of flow control mechanism used. Before getting started the transmission of data they have to agree upon between two communication devices.
Addressing: When more than two devices share a transmission facility, a source system must somehow indicate the identity or address of the destination. Addresses are in form of IP or we can say ftp address and there are used lots of credentials.
Routing: Routing means to send data to appropriate destinations. In this process the evolved computer ensures that the data is being sent on destination system only or any other hacking happening. To eliminate such problem developers uses SSL level security.

1.3 Network Types :LAN,MAN,WAN

LAN (Local Area Network)

LAN operate a Broadcast networks have a single communication channel that is shared by all the machines on the network.
Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size.
They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
Six Basic Components of a LAN :
Network Size- LANs are restricted in size, How many computer connect to the each other. It also simplifies network management.
Network Device -Such as workstations,printer,file server which are normally accessed by all other computer.
Network communication Device- That include such as hub,switch,router etc used for network operations. **Switches :** A switch is an equipment responsible for undertaking the forwarding and filtering of data based on the Media Access Control (MAC) address of the network cards involved in communication.
Hubs : This device is similar to a switch, however, it is incapable of filtrating the data packets based on their MAC address, and instead, sends all packets to all devices. It generally has a better performance value on a computer network.

Router -Router is a device that connect two or more networks. They consist of combination of hardware and software. Two software in a router are the operating system and the routing protocol.
Network Interface Card - For each network device required to access the network. Network Operating system- software application required to control the use of the network LAN Standard.
Topology - Various topologies are possible for broadcast LANs .In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending.
IEEE 802.3, popularly called Ethernet, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps . A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted.
As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.
Transmission technology - LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps.

Metropolitan Area Networks (MAN):

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.
Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.

Wide Area Network:

WAN operate a point to point networks consist of many connections between individual pairs of machines . A wide area network, or WAN, spans a large geographical area, often a country or continent.
It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider.
Two Basic Components of a WAN :
Transmission lines Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links.
switching elements Switching elements are specialized computers that connect three or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.
These switching device have been called route r. a host can be connected directly to a router Thecollection of communication lines and routers (but not the hosts) form the subnet. its only meaning was the collection of routers and communication lines that moved packets from the source host to the destination host.
The network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers.
When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store and forward or

packet switched subnet. The principle of a packet switched WAN is so important that it is worth devoting a few more words to it. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession.

The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process.

In this figure, all the packets follow the route ACE, rather than ABDE or ACDE. In some networks all packets from a given message must follow the same route; in others each packet is routed separately. Of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually routed. Routing decisions are made locally. When a packet arrives at router A ,it is up to A to decide if this packet should be sent on the line to B or the line to C. How A makes that decision is called the routing algorithm.

Wireless LAN Components :

Components of a traditional WLAN network include APs, network interface cards (NICs) or client adapters, bridges, repeaters, and antennae. Additionally, an authentication, authorization, and accounting (AAA) server & network management server (NMS) and routers are considered as part of an enterprise WLAN network.

Access point (AP): An AP operates within a specific frequency spectrum and uses an 802.11 standard modulation technique. It also informs the wireless clients of its availability and authenticates and associates wireless clients to the wireless network. An AP also coordinates the wireless clients' use of wired resources. It should be noted that there are several kinds of APs, including single radio and multiple radios, based on different 802.11 technologies.

NIC or client adapter: A PC or workstation uses a wireless NIC or client adapter to connect to the wireless network. The NIC scans the available frequency spectrum for connectivity and associates it to an AP or another wireless client. The NIC is coupled to the PC or workstation operating system (OS) using a software driver.

Bridge: Wireless bridges are used to connect multiple LANs (both wired and wireless) at the Media Access Control (MAC) layer level. Used in buildingtobuilding wireless connections, wireless bridges can cover longer distances than APs. (The Institute of Electrical and Electronics Engineers [IEEE] 802.11 standard specifies one mile as the maximum coverage range for an AP.) Bridges are available for deployment using different 802.11 technologies.

Note

Currently, bridges are not defined in the 802.11 standards; hence, the bridges do not operate on open standards. This means the bridges must be from the same vendor as the WLAN infrastructure.

Workgroup bridge (WGB): A workgroup bridge is a smallerscale bridge that can be used to support a limited number of wired clients.

Antenna: An antenna radiates the modulated signal through the air so that wireless clients can receive it. Characteristics of an antenna are defined by propagation pattern (directional versus omnidirectional), gain, transmit power, and so on. Antennas are needed on the APs, bridges, and clients. The antennas need not be conspicuous at all; for example, many PC manufacturers build the antenna inside the LCD screen.

AAA server: AAA services are needed to secure a WLAN network. The AAA server is used for both user and administrator authentication in a WLAN network. It is used for enterprise networks, not home WLANs. The AAA server can be used to pass policy such as virtual LAN (VLAN) and SSID for clients, to grant different levels of authorization rights to administrative users, and to generate dynamic encryption keys for WLAN users. Furthermore, accounting features of a AAA server can be used to track WLAN user activities.

Network management server (NMS): The NMS is needed to ease the complexity of deployment and management of large WLAN networks. The NMS should support firmware/software management, configuration management, performance trending and reporting, and client association reporting capabilities in a WLAN network. Furthermore, additional capabilities to manage the RF spectrum and detect rogue APs are needed in an enterprise WLAN network. The NMS should be Supported by other normal management systems for sys logs, traps, and so on.

1.4 Wireless LAN

Client-Server Model:

Client/server network is also called as Domain Model.
Client/server is a distributed computing model in which client applications request services from server processes. Clients and servers typically run on different computers interconnected by a computer network.
A client application is a process or program that sends messages to a server via the network. Those messages request the server to perform a specific task, such as looking up a customer record in a database or returning a portion of a file on the server's hard disk. The client manages local resources such as a display, keyboard, local disks and other peripherals.
A client/server environment typically hosts various operating system brands just like (Windows server 2000 ,Windows server 2003, Windows server 2008) and hardware from multiple vendors. Vendor independence and freedom of choice are thus further advantages of the model.
Client/server systems can be scaled up in size more readily than centralized solutions as server functionality can be distributed across more and more server computers, as the number of clients increases.
The drawbacks of the client/server model are that security is more difficult to ensure in a distributed environment than it is in a centralized one, that the administration of distributed equipment can be much more expensive than the maintenance of a centralized system, that data distributed across servers needs to be maintained consistent, and that the failure of one server can render a large client/server system unavailable. If a server fails, none of its clients can make progress any more.

- Domain has central management system
- Domain has a central storage place and that's call ACTIVE DIRECTORY SERVICES in Windows server 2003 & 2008 but Windows server 2000 use for ACTIVE DIRECTORY CERTIFICATION Service.
- In the domain the server domain operating system need : Win Server 2000, 2003, 2008.
- Domain provides the higher security and it's a also not the systematic network systematic network. ile, Folder & User & Group Permission we can assign.
- Windows 2000 & 2003 Server or Advance Support For Server Configuration
- Security of Data, User & Groups.

Peer To Peer Network :

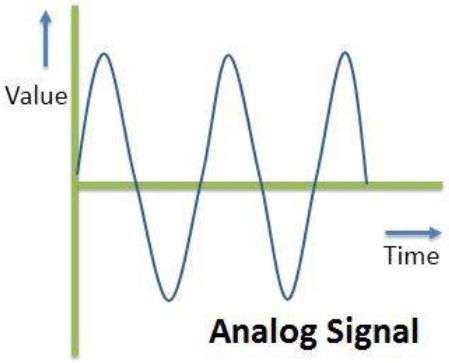
Peer To Peer network is also called as Workgroup Model.
Peer to Peer networks have no central computer (server). Each computer on the network can share its resources and access resources on another computer.The only requirements for building a peer-to-peer network include installing an operating system on the PCs that supports peer-to- peer networking and then physically connecting the Pcs.
Peer-to-peer networking provides a simple, low-cost method for connecting personal computers in situations where you want to share files and other resources such as a printer. Peer-to-peer networking does not require a server, meaning the added expense of a powerful computer to act as a server and a network operating system for the server is avoided in this approach to creating small networks.
A peer computer basically acts as both a client and a server computer. Peer computers can access resources on the network, and they can supply resources to other peer computers.

- Workgroup has no central management system
- There is no need to use the server operating system in the workgroup
- Workgroup has no central storage place

- Workgroup not provides the higher security and its also not the systematic network.
- We can assign permission to drives & folder & files but much security than Domain.
- Basically Windows 98 & XP is going to used in Clients side.
- Not much security for Data, User & Groups. (Depends on Configuration)
- No Server & Client Matter..Each pc reacts like a Client as well as Server.

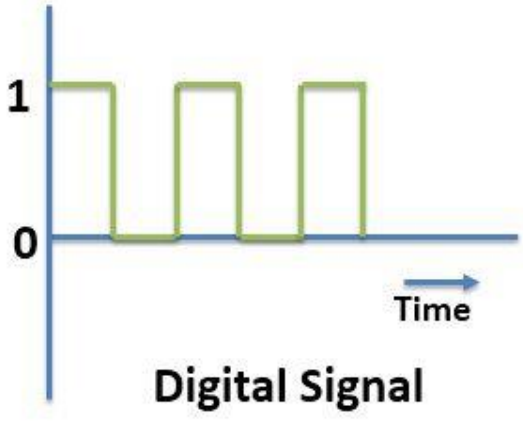
Analog and Digital Signal

Definition of Analog Signal: Analog signal is a kind of continuous wave form that changes over time. An analog signal is further classified into simple and composite signals. A simple analog signal is a sine wave that cannot be decomposed further. On the other hand, a composite analog signal can be further decomposed into multiple sine waves. An analog signal is described using amplitude, period or frequency and phase. Amplitude marks the maximum height of the signal. Frequency marks the rate at which signal is changing. Phase marks the position of the wave with respect to time zero.



An analog signal is not immune to noise hence, it faces distortion and decrease the quality of transmission. The range of value in an analog signal is not fixed.

Definition of Digital Signal: Digital signals also carry information like analog signals but is somewhat is different from analog signals. Digital signal is noncontinuous, discrete time signal. Digital signal carries information or data in the binary form i.e. a digital signal represent information in the form of bits. Digital signal can be further decomposed into simple sine waves that are called harmonics. Each simple wave has different amplitude, frequency and phase. Digital signal is described with bit rate and bit interval. Bit interval describes the time require for sending a single bit. On the other hand, bit rate describes the frequency of bit interval.



A digital signal is more immune to the noise; hence, it hardly

faces any distortion. Digital signals are easier to transmit and are more reliable when compared to analog signals. Digital signal has a finite range of values. The digital signal consists 0s and 1s.

Key Differences Between Analog and Digital Signal.

1. An analog signal represents a continuous wave that keeps changing over a time period. On the other hand, a digital signal represents a noncontinuous wave that carries information in a binary format and has discrete values.
2. An analog signal is always represented by the continuous sine wave whereas, a digital signal is represented by square waves.
3. While talking of analog signal we describe the behaviour of the wave in respect of amplitude, period or frequency, and phase of the wave. On the other hand, while talking of discrete signals we describe the behaviour of the wave in respect of bit rate and bit interval.
4. The range of an anlaog signal is not fixed whereas the range of the digital signal is finite and which can be 0 or 1.
5. An analog signal is more prone to distortion in response to noise, but a digital signal has immunity in response to noise hence it rarely faces any distortion.
6. An analog signal transmits data in the form of wave whereas, a digital signal transmits the data in the binary form i.e. in the form of bits.
7. The best example of an analog signal is a human voice, and the best example of a digital signal is the transmission of data in a computer.

Conclusion:

Digital signal is nowadays replacing the analog signal, but analog signal is still best for audio transmission.