Network and telecommunication

**End devices, data transfer devices, transmission medium. Types of networks. Stack protocols: TCP/IP, OSI. IP addressing. Local and wide area networks. Wire and wireless network technologies. DHCP protocol. Technologies of connection to the Internet. Telecommunication technologies.**

Network is a set of devices and systems that are connected to each other (logically or physically) and communicate with each other. These include servers, computers, phones, routers, and so on. The size of this network can be equal to the size of the Internet, or it can consist only two devices connected by a cable.

**End devices, data transfer devices, transmission medium**

The network infrastructure contains three categories of network components:

* End devices
* Intermediary devices
* Network media

Computer Network is an interconnection of two more more computers. Computers enable to communicate and share available resources.

End Devices: Devices that transmit and / or receive any data. It can be computers, telephones, servers, some terminals or thin clients, televisions.

Intermediary devices: These are devices that connect end nodes to each other. These include switches, hubs, modems, routers, Wi-Fi access points.

Network media: These are the media in which direct data transfer occurs. These include cables, network cards, various connectors, air transmission medium.

Modern networks primarily use the following three types of media to interconnect devices and to provide the pathway over which data can be transmitted:

* Metallic wires within cables
* Glass or plastic fibers (fiber-optic cable)
* Wireless transmission

Figure 1 shows examples of the three types of physical media.

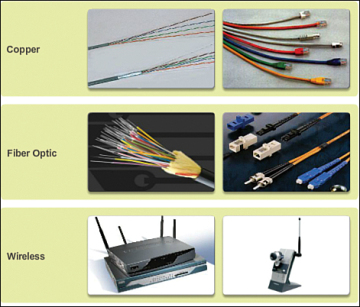


Figure 1 Network Media

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber-optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.

Different types of network media have different features and benefits. Not all network media types have the same characteristics or are appropriate for the same purpose. The criteria for choosing network media are

* The distance the media can successfully carry a signal
* The environment in which the media is to be installed
* The amount of data and the speed at which it must be transmitted
* The cost of the media and installation

Network Representations

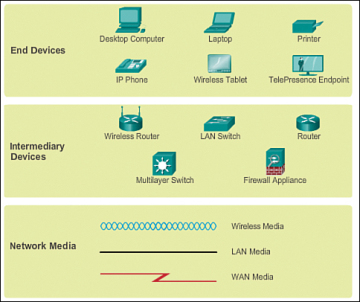


Figure 2 Network Representations

In addition to being able to recognize these representations, you need to understand the specialized terminology that is used when discussing how each of these devices and media connect to each other. Important terms to remember are

* Network interface card (NIC): Provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC (also known as a LAN adapter).
* Physical port: A connector or outlet on a networking device where the media is connected to a host or other networking device.
* Interface: Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.

**What are networks for?**

**Applications:** Using applications we send different data between devices, we open access to shared resources. It can be both console applications and applications with a graphical interface.

**Network resources:** These are network printers, which, for example, are used in the office or network cameras that security monitors while in a remote location.

**Storage:** Using a server or workstation connected to the network, storage is created accessible to others. Many people upload their files, videos, pictures and share them with other users. An example is a google drive, Yandex drive

**Backup:** Often, in large companies, they use a central server, where all computers copy important files for backup. This is necessary for subsequent data recovery if the original is deleted or damaged.

**VoIP:** IP telephony. It is now used everywhere, since it is simpler, cheaper than traditional telephony and every year it supplants it.

**Loaders.** These are FTP, TFTP file managers. A commonplace example is downloading a movie, music, pictures from file hosting or other sources.

**Protocols**

Network protocols are sets of established rules that dictate how to format, transmit and receive [data](https://searchdatamanagement.techtarget.com/definition/data) so computer network devices from [servers](https://whatis.techtarget.com/definition/server) and routers to [endpoints](https://whatis.techtarget.com/definition/endpoint-device) can communicate regardless of the differences in their underlying infrastructures, designs or standards.

A set of cooperating network protocols is called a protocol suite. The [TCP/IP](https://searchnetworking.techtarget.com/definition/TCP-IP) suite includes numerous protocols across layers -- such as the data, network, transport and application layers -- working together to enable internet connectivity. These include:

* Transmission Control Protocol ([TCP](https://searchnetworking.techtarget.com/definition/TCP)), which uses a set of rules to exchange messages with other internet points at the information packet level;
* User Datagram Protocol ([UDP](https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol)), which acts as an alternative communication protocol to TCP and is used to establish low-[latency](https://whatis.techtarget.com/definition/latency) and loss-tolerating connections between applications and the Internet.
* Internet Protocol ([IP](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol)), which uses a set of rules to send and receive messages at the Internet address level;
* additional network protocols that include the Hypertext Transfer Protocol ([HTTP](https://searchwindevelopment.techtarget.com/definition/HTTP)) and File Transfer Protocol ([FTP](https://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol)), each of which has defined sets of rules to exchange and display information.

Below are descriptions of the most popular protocols of this group:

FTP is a standard connection protocol. Powered by TCP Standard port number 21. It is most often used to upload a site to a web hosting and upload it. This is what the application looks like:

TFTP is a simplified version of the FTP protocol that works without establishing a connection using UDP. It is used to load an image with diskless workstations. Especially widely used by Cisco devices for the same image download and backups.

Interactive applications. Applications for interactive exchange. For example, the "man-man" model. When two people, using interactive applications, communicate with each other or carry on a common work. This includes: ICQ, e-mail, a forum where several experts help people solve problems. Or a human-machine model. When a person communicates directly with a computer. This can be a remote configuration of the base, the configuration of the network device. Bandwidth is already more sensitive to delays than downloader applications. For example, with a remote configuration of a network device, it will be difficult to configure it if the response from the command is 30 seconds.

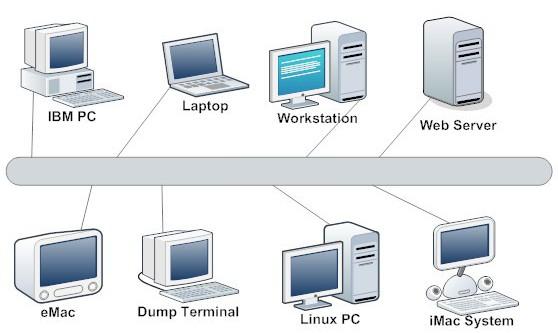
Real-time applications. Applications that allow you to transfer information in real time. Just this group includes IP-telephony, streaming systems, video conferencing. The most sensitive to latency and bandwidth applications. On average, the delay should not exceed 300 ms. This category can include Skype, Lync, Viber (when we make a call).

**Topology**

The topology is divided into 2 large categories: physical and logical. It is very important to understand their difference. So physical topology is what our network looks like. Where are the nodes located, what kind of network intermediate devices are used and where do they stand, what kind of network cables are used, how are they routed

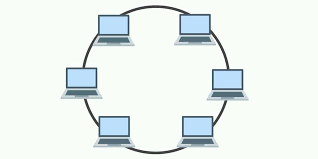
Types of topology

Bus Topology



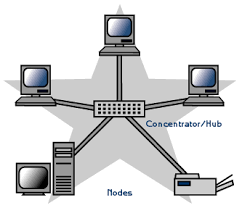
One of the first physical topologies. The bottom line is that all devices are connected to one long cable and a local network is organized. At the ends of the cable are terminators. Its advantage is only in ease of installation. In terms of performance, it was extremely unstable. If a break occurred somewhere in the cable, the entire network remains paralyzed until the cable is replaced.

Ring Topology



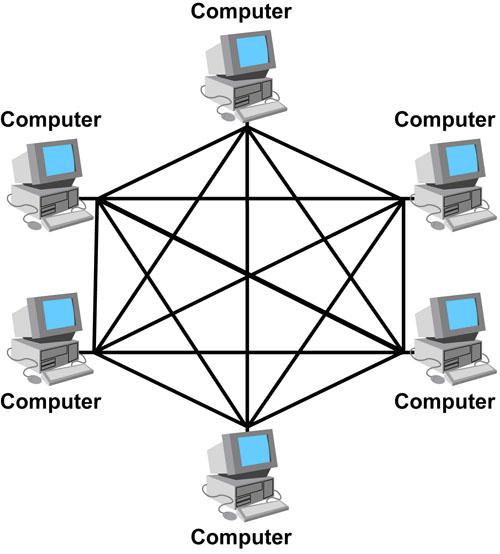
In this topology, each device is connected to 2 neighboring ones. Thus creating a ring. From one end, the computer only accepts, but from the other only sends. That is, it turns out the transmission in a ring and the next computer acts as a signal repeater. Due to this, the need for terminators disappears. Accordingly, if somewhere the cable was damaged, the ring was opened and the network became inoperative.

Star Topology



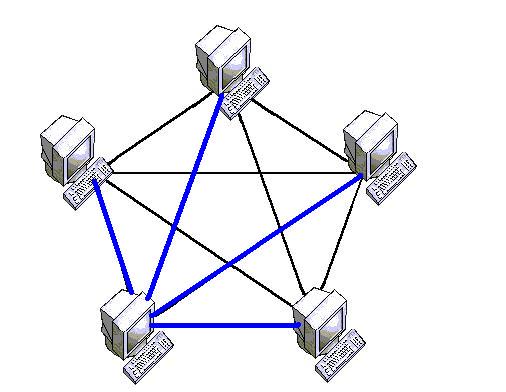
All devices are connected to the central node. This model is used in local networks. Here the fault tolerance is much higher than in the previous two. When a cable breaks, only one device drops out of the network. Everyone else continues to work quietly. However, if the central node fails, the network will become inoperative.

Full-Mesh Topology



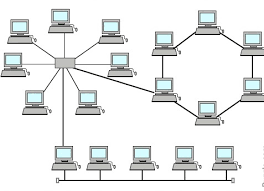
All devices are connected directly to each other. That is, from each to each. This model is perhaps the most fault tolerant, as it does not depend on others. But building networks on this model is difficult and expensive. Since in a network with at least 1000 computers, you will have to connect 1000 cables to each computer.

Partial-Mesh Topology



The connection is built not from each to each, but through additional nodes. That is, node A is directly connected only to node B, and node B is connected to both node A and node C. So, to send node A a message to node C, it must first send to node B, and node B in turn sends this message to node C. Routers work on this topology.

Hybrid Topology

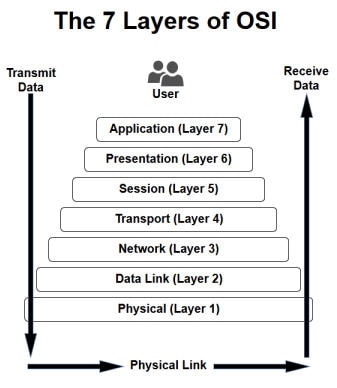


The most popular topology, which combined all the topologies. One of the most fault-tolerant topologies, since if two sites break, then only the connection between them will be paralyzed, and all other combined sites will work faultlessly. Today, this topology is used in all medium and large companies.

ISO Model

Initially, networks did not have common standards. Each vendor used its proprietary solutions that did not work with the technologies of other vendors. Then the International Organization for Standardization (ISO - International Organization for Standartization) created the OSI model, which was released in 1984. But it was developed for 7 years. Currently, the OSI model is not used. It is used only as a training network.

The model include 7 levels and each level performs a specific role and tasks



The OSI model is not used today. While this model was being developed, the TCP / IP protocol stack has become popular.

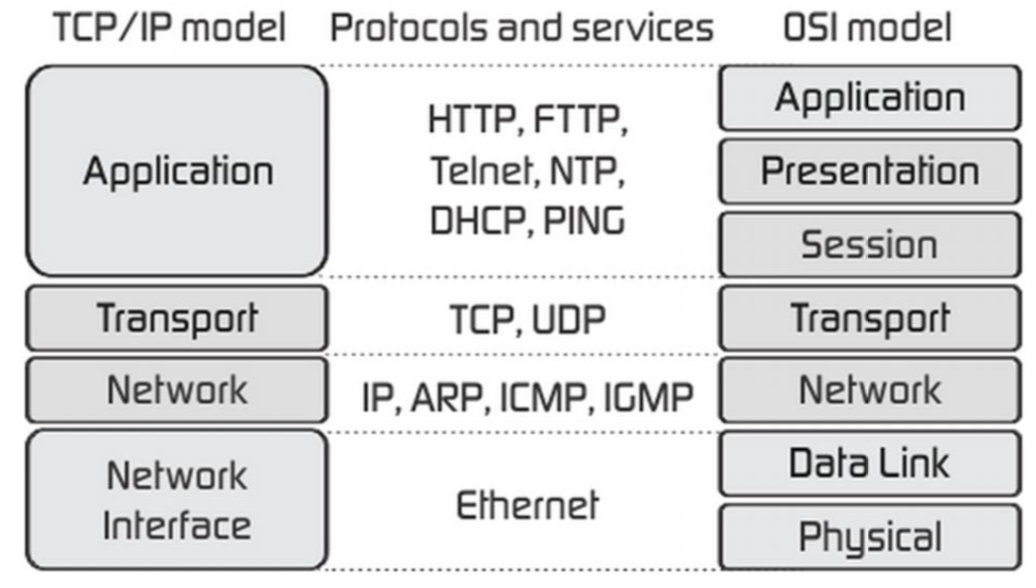
TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at al

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.  
The TCP/IP model has five layers.

1. Application Layer   
2. Transport Layer

3. Internet Layer  
4. Data Link Layer

5. Physical Network



In figure, presentation and session layers are not there in TCP/IP model. Also note that the Network Access Layer in TCP/IP model combines the functions of Data link Layer and Physical Layer.

**IP address, MAC address, Subnet masks**

A MAC address and your IP address are both key components to networking, but they serve different purposes, and are visible in very different ways

**A MAC address** (or Machine Access Control) is a device’s “physical” address**.** It’s hard-coded to the network card from the manufacturer. Represented by a 12-digit, hexadecimal number, every device in the world has a unique MAC address. (In case you were wondering, the 48-bit identifier has 281.5 trillion combinations, so you shouldn’t be worried about duplicates.)

**The IP address is a virtual address** and it changes depending on the network your device connects to, or even every time you reboot your computer. Years ago, you kept the same IP address on your computer, but now IP addresses are usually dynamically assigned. Some websites always have the same IP address, called a **Static IP Address**.

**Subnet masks.** Every IPv4 address has a network portion and a host portion. These parts are defined by the subnet mask that is assigned to the address. A common subnet mask of 255.255.255.0 tells us the first three octets of the address denotes the network portion and the last octet denotes the host portion of the address. With an address of 192.158.3.4 with a 255.25.255.0 mask; 192.168.3.0 is the network and the last octet, .4, is a host on that network.

**Repeater, Hub, Modem, Routers, Switch, Gateway**, **Brouter, Bridge**

**Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

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

**Types of Hub**

* **Active Hub :-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
* **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend distance between nodes.

**Bridge** – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

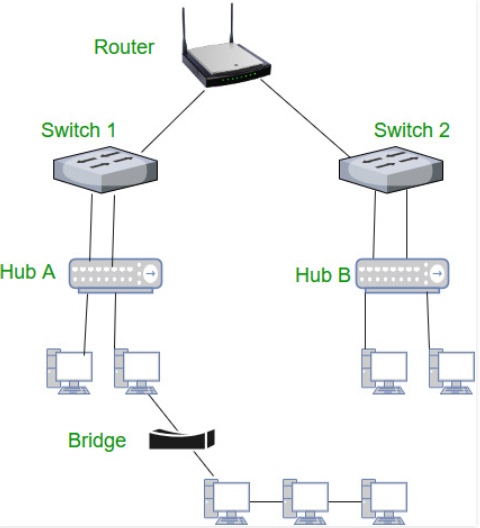
* **Transparent Bridges :-** These are the bridge in which the stations are completely unaware of the  
  bridge’s existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of  
  the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges :-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

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

**Routers** – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

**Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

**Brouter** – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

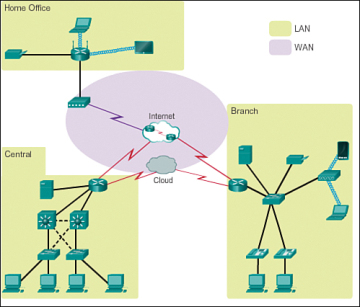


**Types of Networks**

Network infrastructures can vary greatly in terms of

* Size of the area covered
* Number of users connected
* Number and types of services available

Figure 3 illustrates the two most common types of network infrastructures:

* *Local-area network (LAN)*: A network infrastructure that provides access to users and end devices in a small geographical area.
* *Wide-area network (WAN)*: A network infrastructure that provides access to other networks over a wide geographical area.  
    
  Figure 3 LANs Separated by Geographic Distance Connected by a WAN

Other types of networks include

* Metropolitan-area network (MAN): A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). MANs are typically operated by a single entity, such as a large organization.
* *Wireless LAN (WLAN)*: Similar to a LAN but wirelessly interconnects users and endpoints in a small geographical area.
* *Storage-area network (SAN)*: A network infrastructure designed to support file servers and provide data storage, retrieval, and replication. It involves high-end servers, multiple disk arrays (called *blocks*), and Fibre Channel interconnection technology.

**Local-Area Networks**

LANs are a network infrastructure that spans a small geographical area. Specific features of LANs include

* LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
* A LAN is usually administered by a single organization or individual. The administrative control that governs the security and access control policies is enforced on the network level.
* LANs provide high-speed bandwidth to internal end devices and intermediary devices.

**Wide-Area Networks**

WANs are a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet service providers (ISPs).

Specific features of WANs include

* WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
* WANs are usually administered by multiple service providers.
* WANs typically provide slower-speed links between LANs.

**Telecommunication technologies.**

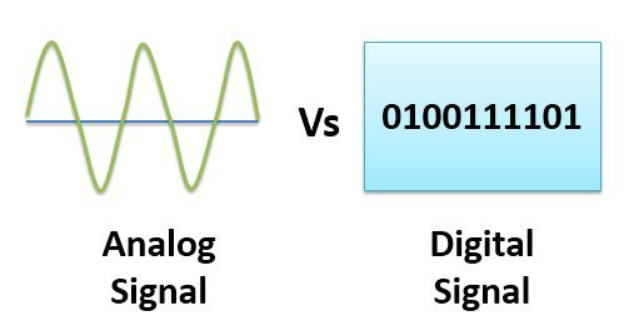
These are [technologies](http://clearlyexplained.com/technology/index.html) for the transfer of information via electrical or light technologies.

Common examples are:

* Visual Light communications ( fires, flashes of light, smoke signals)
* Radio and TV communication
* Telegraph communications
* Telephone communications (partly superseded converged by the , or evolving into the [internet](http://clearlyexplained.com/internet/index.html))

**In telecommunications, there are 2 types of signal:**

Analog and Digital signals



Analog and Digital are the different forms of signals. Signals are used to carry information from one device to another. Analog signal is a continuous wave that keeps on changing over a time period. Digital signal is discrete in nature. The fundamental difference between analog and digital signal is that analog signal is represented by the sine waves whereas, the digital signal is represented by square waves. Lets us learn some more differences between analog and digital signal with the help of comparison chart shown below

Analog signal is a kind of continuous wave form that changes over time. An anlaog 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

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

Difference of the signals

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.