Lecture 1 Oct. 2018

Computer Networks

Computer System Dept. – Second Year

Lecturer: Dr. Nadia Ali

1 Definitions

1.1 Computer Network

A computer network consists of a collection of computers, printers and other equipment linked together in order to communicate with each other and share resources. The computers might be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. Fig.1 gives an example of a small home network consist of connecting computers and showing the various links.

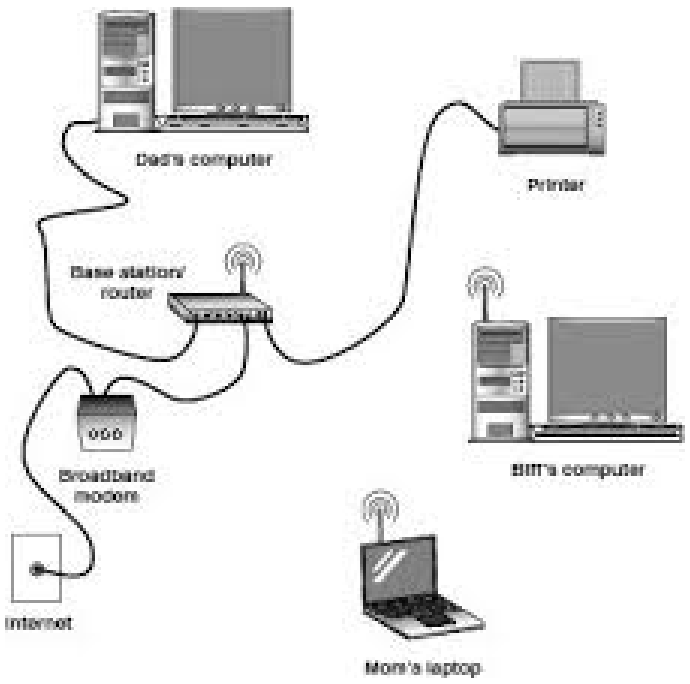

Figure 1: Home computer network.

1.2 Intranet

An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.

1.3 The Internet

sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

1.4 Extranet

An extranet is an intranet with a wider range than one organization - a company and their suppliers, for example.

2 Hierarchal link Idea

Broadly speaking, there are two types of network configuration, peer-to-peer networks and client/server networks.

2.1 Peer-to-peer networks

Peer-to-peer networks are more commonly implemented where less then ten computers are involved and where strict security is not necessary. All computers have the same status, hence the term 'peer', and they communicate with each other on an equal footing. Files, such as word processing or spreadsheet documents, can be shared across the network and all the computers on the network can share devices, such as printers or scanners, which are connected to any one computer. Fig.2 shows a peer to peer network.

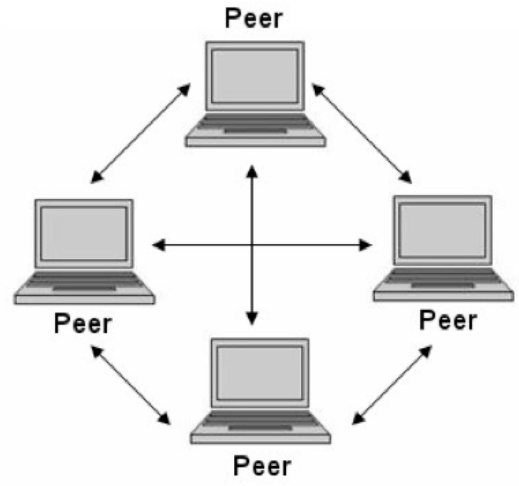

Figure 2: Peer to Peer Networking.

2.2 Client/server networks

Client/server networks are more suitable for larger networks. A central computer, or 'server', acts as the storage location for files and applications shared on the network. Usually the server is a higher than average performance computer. The server also controls the network access of the other computers which are referred to as the 'client' computers. Typically, teachers and students in a school will use the client computers for their work and only the network administrator (usually a designated staff member) will have access rights to the server. Fig.3 gives an example of a client/server network.

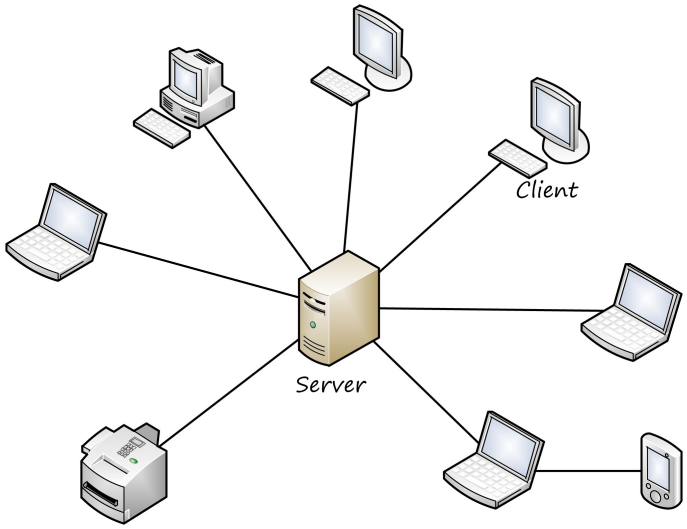

Figure 3: Client - Server Networking.

There are different kinds of servers, the most common are:

1. **Proxy Server**: A proxy server sits between a client program (typically a Web browser) and an external server (typically another server on the Web) to filter requests, improve performance, and share connections.

2. **Mail Server**: mail servers move and store mail over corporate networks (via Local Area Networks (LANs) and Wide Area Networks (WANs) and across the Internet.

3. **List Server**: List servers offer a way to better manage mailing lists, whether they be interactive discussions open to the public or one-way lists that deliver announcements, newsletters or advertising.

4. **Web Server**: a Web server serves static content to a Web browser by loading a file from a disk and serving it across the network to a user's Web browser. This entire exchange is mediated by the browser and server talking to each other using HTTP.

5. **FTP Server**: One of the oldest of the Internet services, File Transfer Protocol makes it possible to move one or more files securely between computers while providing file security and organization as well as transfer control.

6. **Telnet Server**: A Telnet server enables users to log on to a host computer and perform tasks as if they're working on the remote computer itself.

Table 1 provides a summary comparison between Peer-to-Peer and Client/Server Networks.

Peer-to-Peer Networks vs Client/Server Networks	
Peer-to-Peer Networks	**Client/Server Networks**
Easy to set up	More difficult to set up
Less expensive to install	More expensive to install
Can be implemented on a wide range of operating systems	A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking
More time consuming to maintain the software being used (as computers must be managed individually)	Less time consuming to maintain the software being used (as most of the maintenance is managed from the server)
Very low levels of security supported or none at all. These can be very cumbersome to set up, depending on the operating system being used	High levels of security are supported, all of which are controlled from the server. Such measures prevent the deletion of essential system files or the changing of settings
Ideal for networks with less than 10 computers	No limit to the number of computers that can be supported by the network
Does not require a server	Requires a server running a server operating system
Demands a moderate level of skills to administer the network	Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system

Table 1: Peer-to-Peer Networks vs Client/Server Networks.

3 Basic Computer Network Components

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), local operating system(LOS), and the network operating system (NOS).

3.1 Hardware

- **Servers** - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers, to name a few.

- **Clients** - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers(users) of the network, as they request and receive services from the servers.

- **Transmission Media** - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.

- **Network Interface Card** - Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares(formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.

- **Shared printers and other peripherals** - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

- **Hub** - Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer requests information from a network or a specific computer, it sends the request to the hub through a cable.

The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

- **Switch** - Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or port.

  Unlike a hub, switch doesn't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words, switch connects the source and destination directly which increases the speed of the network.

  Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

- **Router** - When we talk about computer network components, the other device that used to connect a LAN with an internet connection is called Router. When you have two distinct networks (LANs) or want to share a single internet connection to multiple computers, we use a Router. In most cases, recent routers also include a switch

which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks. There are two types of Router: wired and wireless. The choice depends on your physical office/home setting, speed and cost.

- **LAN Cable**- A local area Network cable is also known as data cable or Ethernet cable which is a wired cable used to connect a device to the internet or to other devices like other computer, printers, etc.

3.2 Software

- **Local Operating System** - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, Unix, Linux, Windows 2000, Windows 98, Windows XP etc.

- **Network Operating System** - The network operating system is a program that runs on computers and servers, and allows the computers to communicate over the network.

- **Shared data** - Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.
- **Network Management System (NMS)**: is an application or set of applications that lets network engineers manage a network's independent components inside a bigger network management framework and performs several key functions.
- **Network Protocols**: In data communication, network protocols are defined as the formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network.

4 Network Physical Topology

The term physical topology refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.

4.1 Mesh Topology

- In a mesh topology, every device has a dedicated point-to-point link to every other device. Check Fig.4

- The term **dedicated** means that the link carries traffic only between the two devices it connects.

- To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to $n - I$ nodes, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to $n - 1$ nodes. We need $n(n - 1)$ physical links.

  However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need $n(n-1)/2$ duplex-mode links.

- To accommodate that many links, every device on the network must have $n - 1$ input/output (VO) ports to be connected to the other $n - 1$ stations.

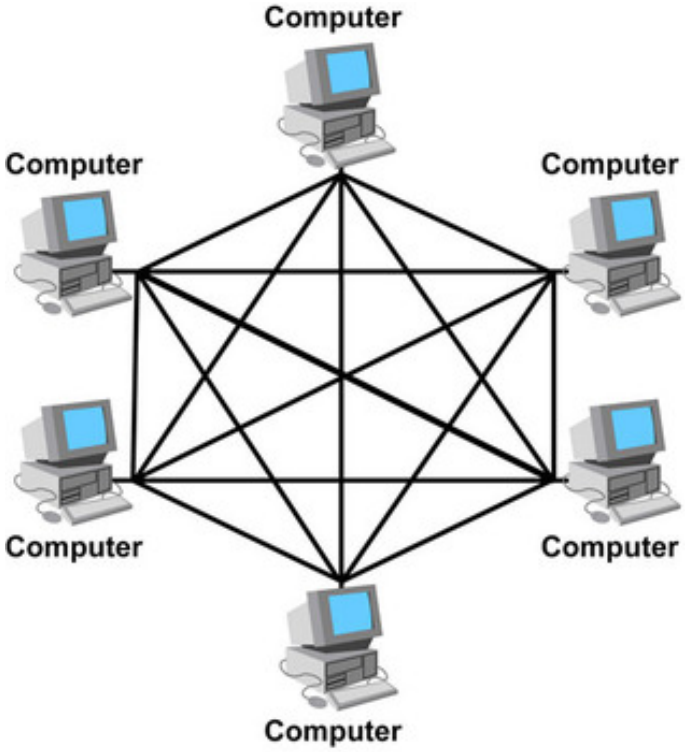

Figure 4: Mesh Topology.

Advantages:

- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

- There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
- Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages:

1. Installation and reconnection are difficult because every device must be connected to every other device.
2. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

4.2 Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices.

The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device. (refer to Fig.5)

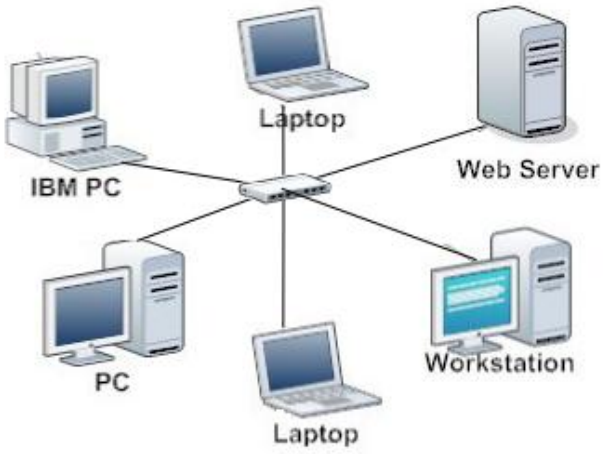

Figure 5: Star Topology.

Advantages:

1. Star topology is less expensive than a mesh topology.
2. In a star, each device needs only one link and one I/O port to connect it to any number of others.
3. easy to install and reconfigure.
4. less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
5. Robustness: If one link fails, only that link is affected. All other links remain active.

Disadvantages:

1. One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
2. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

4.3 Bus Topology

A bus topology is multipoint one long cable acts as a backbone to link all the devices in a network. Nodes are connected to the bus directly Fig.6. Bus topology was the one of the first topologies used in the design of early local area networks.

As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. Therefore, there is a limit on the number of nodes a bus can support and on the distance between those nodes.

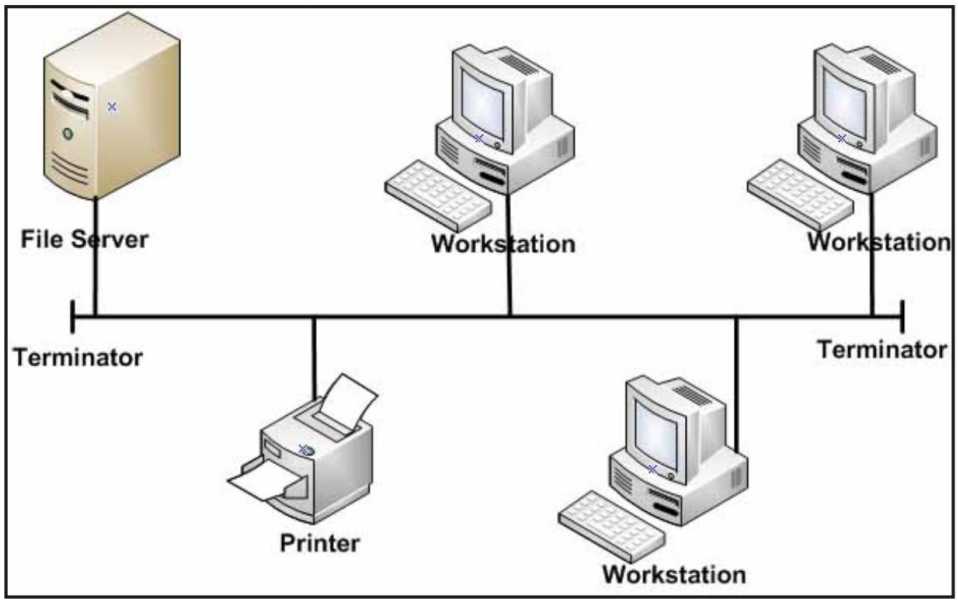

Figure 6: Bus Topology.

Advantages:

1. ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
2. Uses less cabling than mesh or star topologies.
3. Only the backbone cable stretches through the entire facility.

Disadvantages:

1. Difficult reconnection and fault isolation.
2. Difficult to add new devices.
3. Adding new devices may therefore require modification or replacement of the backbone.

4. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.

4.4 Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

Advantages:

1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbours (either physically or logically).
2. To add or delete a device requires changing only two connections.
3. Fault isolation is simplified.

Disadvantages:

1. All data being transferred over the network must pass through each workstation on the network.
2. Slower than a star topology.
3. The entire network will be impacted if one workstation shuts down.
4. The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

4.5 Token Ring Network (Token Passing)

Is a local area network (LAN) in which all computers are connected in a ring or star topology and pass one or more logical tokens from host to host. Only a host that holds a token can send data, and tokens are released when receipt of the data is confirmed. Token ring networks prevent data packets from colliding on a network segment because data can only be sent by a token holder and the number of tokens available is controlled.

The token ring LAN process is delineated by the following sequence of events:

- A token continually circulates inside the token ring LAN.
- To transmit a message, a node inserts a message and destination address inside an empty token.
- The token is examined by each successive node.
- The destination node copies the message data and returns the token to the source with the source address and a data receipt message.
- The source receives the returned token, verifies copied and received data and empties the token.

5 Geographical Coverage

Computer Networks are divided based on their size (geographical coverage) to:

1. **Local-Area Networks (LANs)**: a network in which all nodes are connected with network cables and which occupies a relatively small geographical area. For example: a building, office, or department, or a home. The computers are geographically close together.

2. **Wide-Area Networks (WANs)**: a network consisting of two or more LAN's spread out over a relatively large area. For example: a country or state, or even the world. The networks are sometimes connected using POTs (plain old telephone) technology, but are more likely to use high-speed fiber- optics, microwave dishes, or satellite links.

3. **Campus-Area Networks (CANs)**: The computers are within a limited geographic area, such as a campus or military base.

4. **Metropolitan-Area Networks MANs)**: A data network designed for a town or city.

5. **Home-Area Networks (HANs)**: A network contained within a user's home that connects a person's digital devices.

6 Network Interface Card (NIC)

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to physically access a networking medium. It provides a low-level addressing system through the use of MAC addresses.

Types of Network Interface card are:

1. Ethernet – 10Mbps
2. Fast Ethernet – 100Mbps
3. Gigabit Ethernet – 1000Mbps

Figure 7: Network Interface Cards.

7 Cables Used in the Network

What is Network Cabling? Cable is the medium through which information usually moves from one network device to another.

There are several types of cables which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types.

The type of cable chosen for a network is related to the network's topology, protocol, and size.

Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

- Twisted Pair Cable.
- Coaxial Cable.
- Fiber Optic Cable.

7.1 Twisted Pair Cable

Twisted pair cabling comes in two varieties: shielded (STP) and unshielded (UTP).

1.Unshielded twisted pair (UTP): is the most popular and is generally the best option for school networks (See Fig.8). The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.

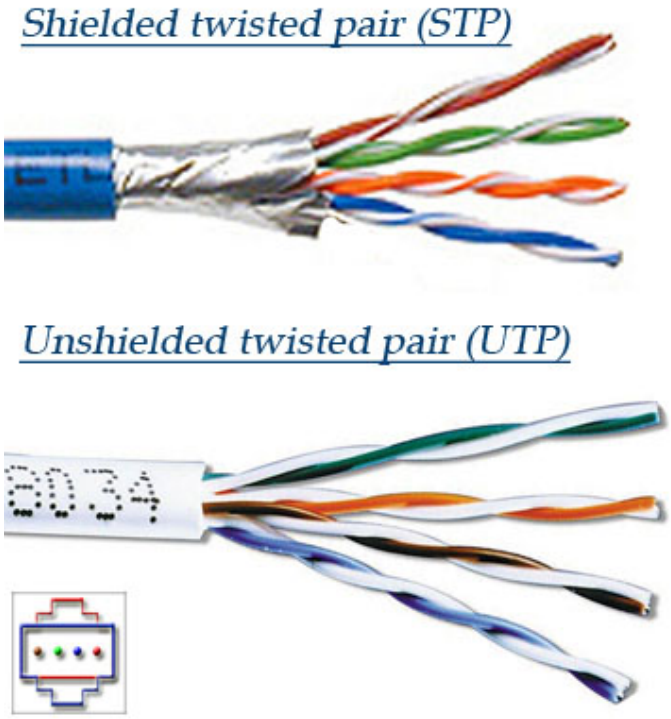

Figure 8: STP and UTP.

The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging). (Table 7.1)

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair) 1000 Mbps (4 pair)	100BaseT Ethernet Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Table 2: Categories of Unshielded Twisted Pair.

2. Shielded twisted pair: Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.).

If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

- Each pair of wires is individually shielded with foil.
- There is a foil or braid shield inside the jacket covering all wires (as a group).
- There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Unshielded Twisted Pair Connector: The standard connector for unshielded twisted pair cabling is an $RJ-45$ connector. This is a plastic connector that looks like a large telephone-style connector (See Fig.9). A slot allows the $RJ-45$ to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

Figure 9: RJ-45 connector.

7.2 Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See Fig. 10). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

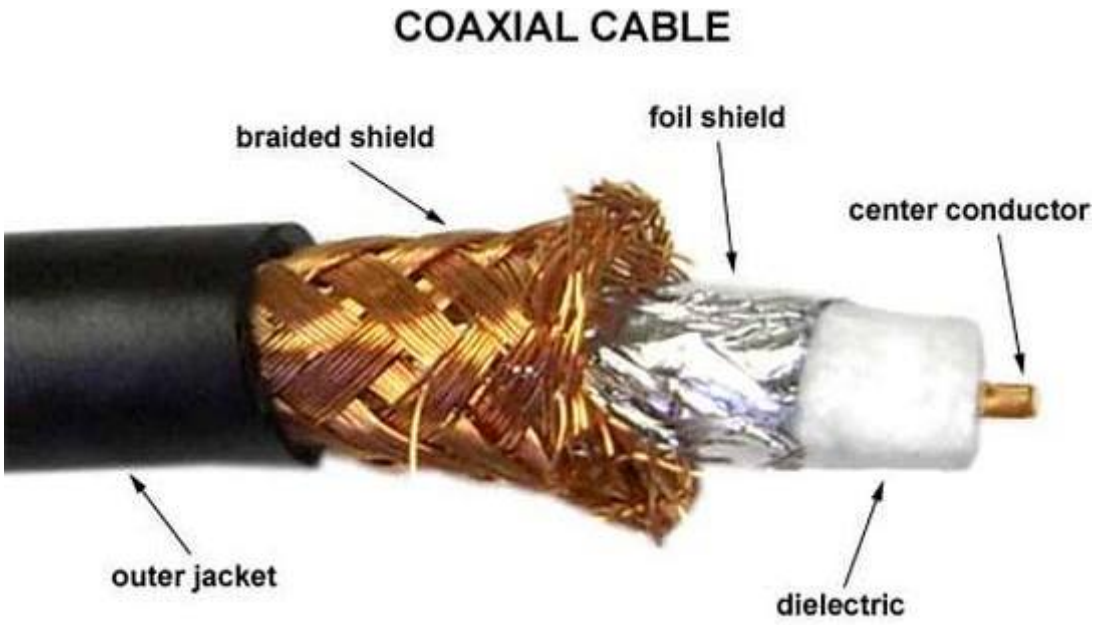

Figure 10: Coaxial Cable.

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors: The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See Fig. 11). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

Figure 11: Coaxial Cable Connector.

7.3 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See Fig.12). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

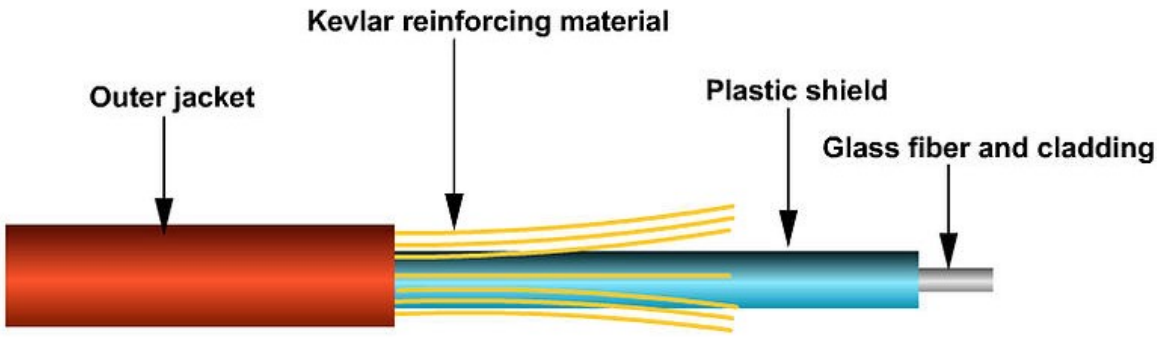

Figure 12: Fiber Optic cable.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services.

The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (See Fig.12). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC. Fig.13 shows various types of fiber connectors.

Figure 13: Fiber Optic cable Connectors.

7.4 Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

8 Wireless Communication

Communication Systems can be Wired or Wireless and the medium used for communication can be Guided or Unguided. In Wired Communication, the medium is a physical path like Co-axial Cables, Twisted Pair Cables and Optical Fiber Links etc. which guides the signal to propagate from one point to other.

If there is no physical medium, then how does wireless communication transmit signals? Even though there are no cables used in wireless communication, the transmission and reception of signals is accomplished with Antennas.

Antennas are electrical devices that transform the electrical signals to radio signals in the form of Electromagnetic (EM) Waves and vice versa. These Electromagnetic Waves propagates through space. Hence, both transmitter and receiver consists of an antenna.

Wireless Communication is the fastest growing and most vibrant technological areas in the communication field. Wireless Communication is a method of transmitting information from one point to other, without using any connection like wires, cables or any physical medium. Generally, in a communication system, information is transmitted from transmitter to receiver that are placed over a limited distance. With the help of Wireless Communication, the transmitter and receiver can be placed anywhere between few meters to few thousand kilometres.

Some of the commonly used Wireless Communication Systems in our day-to-day life are: Mobile Phones, GPS Receivers, Remote Controls, Bluetooth Audio and Wi-Fi etc. (Fig.14)

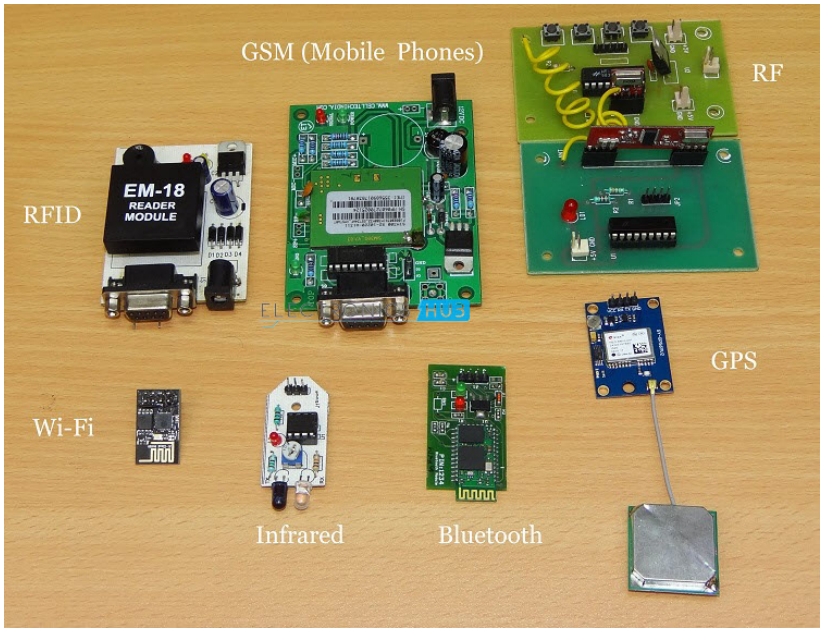

Figure 14: Wireless Devices.

Electromagnetic Waves carry the electromagnetic energy of electromagnetic field through space. Electromagnetic Waves include Gamma Rays (Îş - Rays), X - Rays, Ultraviolet Rays, Visible Light, Infrared Rays, Microwave Rays and Radio Waves. Electromagnetic Waves (usually Radio Waves) are used in wireless communication to carry the signals.

An Electromagnetic Wave consists of both electric and magnetic fields in the form of time varying sinusoidal waves. Both these fields are oscillating perpendicular to each other and the direction of propagation of the Electromagnetic Wave is again perpendicular to both these fields.

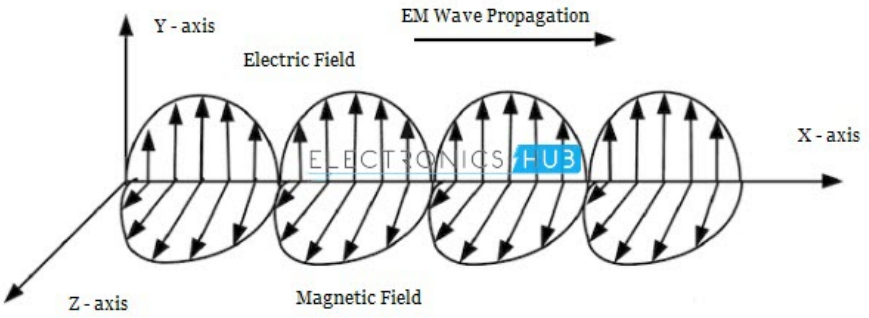

Figure 15: Electromagnetic Wave.

8.1 Advantages of Wireless Communication

There are numerous advantage of Wireless Communication Technology, Wireless Networking and Wireless Systems over Wired Communication like Cost, Mobility, Ease of Installation, and Reliability etc.

Cost: The cost of installing wires, cables and other infrastructure is eliminated in wireless communication and hence lowering the overall cost of the system compared to wired communication system. Installing wired network in building, digging up the Earth to lay the cables and running those wires across the streets is extremely difficult, costly and time consuming job.

In historical buildings, drilling holes for cables is not a best idea as it destroys the integrity and importance of the building. Also, in older buildings with no dedicated lines for communication, wireless communication like Wi-Fi or Wireless LAN is the only option.

Mobility: As mentioned earlier, mobility is the main advantage of wireless communication system. It offers the freedom to move around while still connected to network.

Ease of Installation: The setup and installation of wireless communication networkâĂŹs equipment and infrastructure is very easy as we need not worry about the hassle of cables. Also, the time required to setup a wireless system like a Wi-Fi network for example, is very less when compared to setting up a full cabled network.

Reliability: Since there are no cables and wires involved in wireless communication, there is no chance of communication failure due to damage of these cables which may be caused by environmental conditions, cable splice and natural diminution of metallic conductors.

Disaster Recovery: In case of accidents due to fire, floods or other disasters, the loss of communication infrastructure in wireless communication system can be minimal.

8.2 Disadvantages of Wireless Communication

Even though wireless communication has a number of advantages over wired communication, there are a few disadvantages as well. The most concerning disadvantages are Interference, Security and Health.

Interference: Wireless Communication systems use open space as the medium for transmitting signals. As a result, there is a huge chance that radio signals from one wireless communication system or network might interfere with other signals.

The best example is Bluetooth and Wi-Fi (WLAN). Both these technologies use the 2.4GHz frequency for communication and when both of these devices are active at the same time, there is a chance of interference.

Security: One of the main concerns of wireless communication is Security of the data. Since the signals are transmitted in open space, it is possible that an intruder can intercept the signals and copy sensitive information.

Health Concerns: Continuous exposure to any type of radiation can be hazardous. Even though the levels of RF energy that can cause the damage are not accurately established, it is advised to avoid RF radiation to the maximum.

8.3 Basic Elements of a Wireless Communication System

A typical Wireless Communication System can be divided into three elements: the Transmitter, the Channel and the Receiver. The following image shows the block diagram of wireless communication system. (Fig.16)

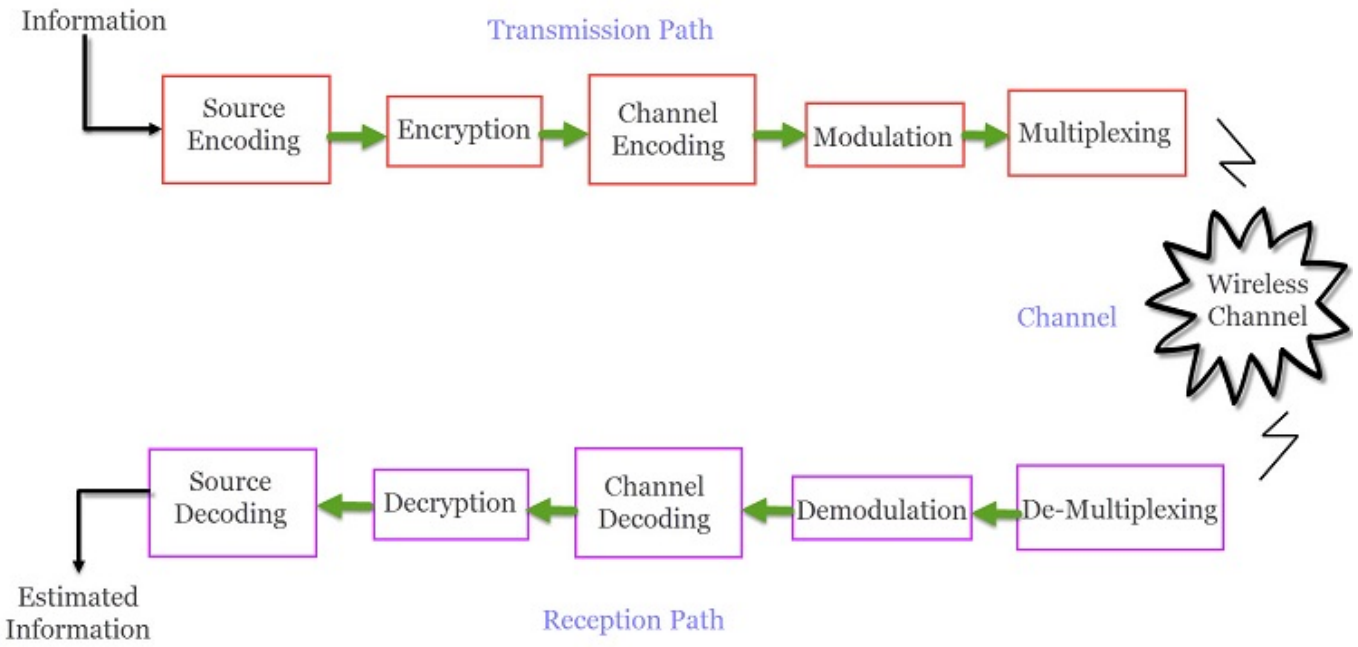

Figure 16: Block Diagram of Wireless Communication System.

9 Bandwidth. Data Rate. Throughput

Latency is the amount of time it takes for data to travel from one point to another. It is dependent on the physical distance that data must travel through cords, networks and the like to reach its destination.

Bandwidth is the rate of data transfer for a fixed period of time. Bandwidth, as its name implies, is the width of a communication band. The wider the communication band, the more data that can flow through it simultaneously. When most people talk about âĂIJinternet speed,âĂİ they usually talk in terms of network bandwidth. Bandwidth can also be interpreted as a traffic number. This is especially true when referencing services such as content delivery networks or web hosts which charge clients based on a combination of inbound/outbound bandwidth.

While bandwidth plays a big role in how fast webpages load, the journey from one machine to another takes time to traverse. No matter how much data you can send and receive at once, it can only travel as fast as latency allows. Of course, this means that websites run slower for some users depending on their physical location. Figuring how to faster reach users from all points of the globe is what reducing latency is all about.

Throughput: Throughput is the amount of data that enters and goes through a system. It is a measure of how many units of information a system can process in a given amount of time. It is applied broadly to systems ranging from various aspects of computer and network systems to organizations. Related measures of system productivity include , the speed with which some specific workload can be completed, and response time, the amount of time between a single interactive user request and receipt of the response.

Data Rate Data rate is the speed at which data is transferred between two devices, measured in mega bits per second (Mbps or mbps)

Example

Bandwidth is the MAXIMUM amount of water that can travel through that hose. Similarly, bandwidth would be the maximum about of data that could be transferred through the RF channel(s)

Throughput is the ACTUAL amount of water that travels through the hose. There are external things that can affect that throughput, a kink in the hose, etc. In the same way that there are external factors for the water hose, there are also real world interferences that can affect the amount of data that is being sent wirelessly. Some typical things that can affect your actual throughput is RF interference and physical obstructions.

10 Modems

10.1 Dial-Up Modems

As previously discussed, a computerâĂŹs digital signals must be converted to analog signals before they are transmitted over standard telephone lines. The communications device that performs this conversion is a modem, sometimes called a dial-up modem. The word, modem, is derived from the combination of the words, modulate, to change into an analog signal, and demodulate, to convert an analog signal into a digital signal.

A modem usually is in the form of an adapter card that you insert in an expansion slot on a com- puterâĂŹs motherboard. One end of a standard telephone cord attaches to a port on the modem card and the other end plugs into a telephone outlet.

10.2 ISDN and DSL Modems

If you access the Internet using ISDN or DSL, you need a communications device to send and receive the digital ISDN or DSL signals. An ISDN modem sends digital data and information from a computer to an ISDN line and receives digital data and information from an ISDN line. A DSL modem sends digital data and information from a computer to a DSL line and receives digital data and information from a DSL line. ISDN and DSL modems usually are external devices.

10.3 Wireless Modems

Some mobile users have a wireless modem that uses the cell phone network to connect to the Internet wirelessly from a notebook computer, a smart phone, or other mobile device (Figure 8-19). Wireless modems, which have an external or built-in antenna, are available as PC Cards, ExpressCard modules, and flash cards.

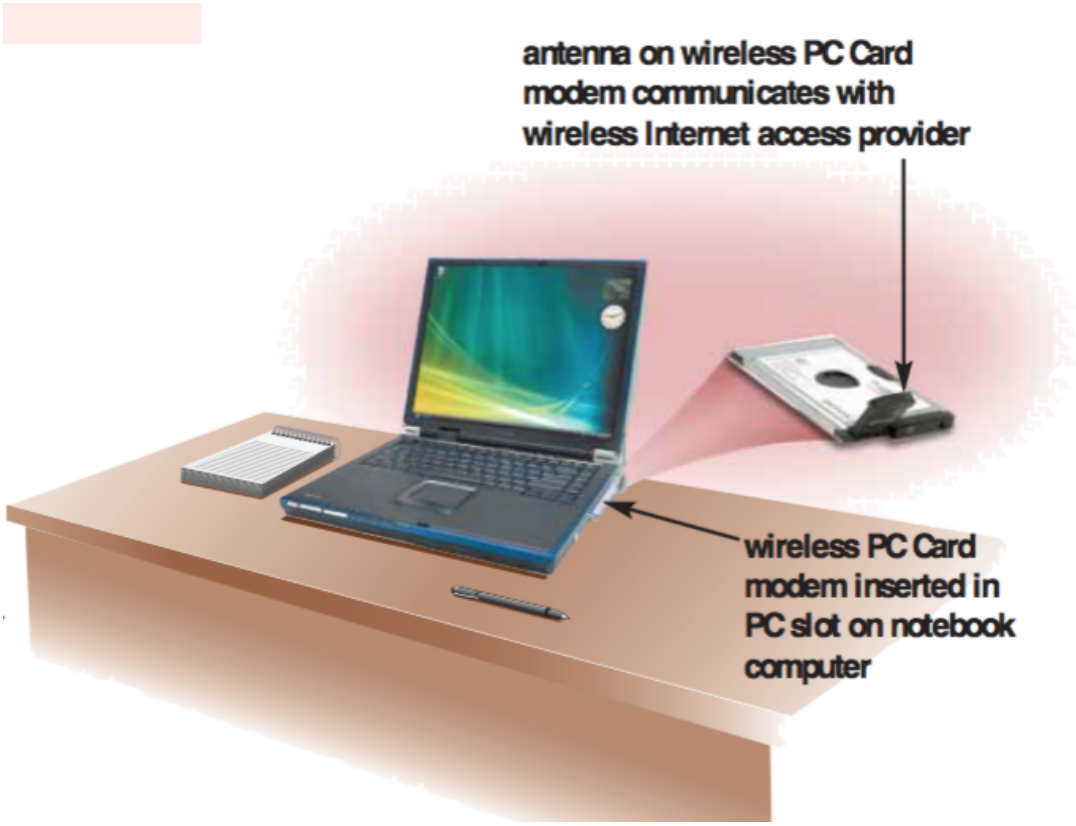

Figure 17: Wireless Modems in the form of PC card.

10.4 Repeaters

In digital communication systems, a repeater is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal along the next leg of the medium. In electromagnetic media, repeaters overcome the attenuation caused by free-space electromagnetic-field divergence or cable loss. A series of repeaters make possible the extension of a signal over a distance.

Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, signals are restrengthened with amplifiers which unfortunately also amplify noise as well as information.

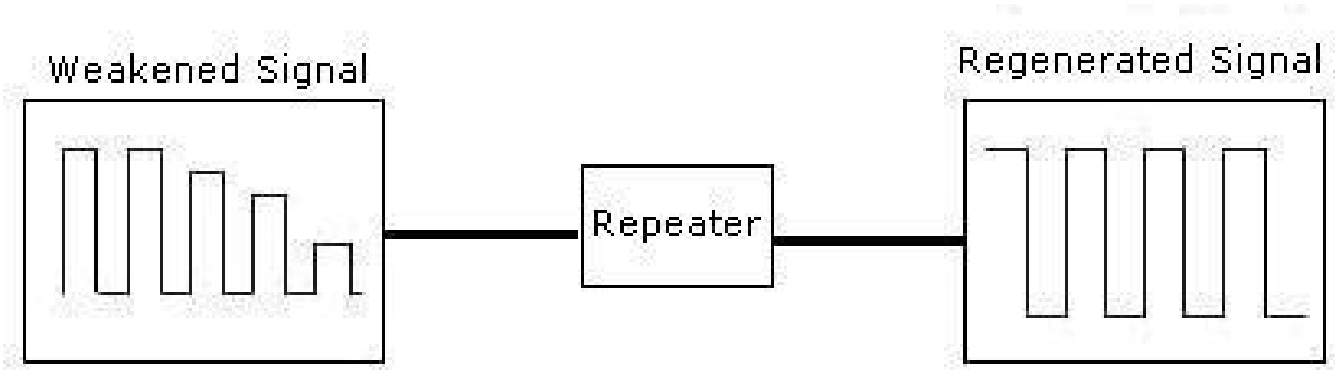

Figure 18: Repeater.

Bridges Bridges are a solution to some of the problems that often occur where a large number of PCs are placed together on one LAN.

Bridges, like repeaters, forward packets from one segment of the network to another. However, bridges have the intelligence to understand the source and destination hardware addresses of network devices; they reduce network utilisation levels by only forwarding relevant packets between network segments.

10.5 Bridges

A bridge intercepts packets coming into the device and identifies their destination. If the destination is on the remote network segment, the bridge forwards the packet out. If the destination is on the same network segment as the source address, the bridge simply discards the packet.

Bridges operate at the Network Access Layer of the TCP/IP-model. This layer has two sublayers, the logical link control (LLC) sublayer and the media access control (MAC) sublayer. All bridges operate at the MAC sublayer. However, some bridges are intelligent enough to link segments containing different topologies, such as Ethernet and Token Ring. These bridges are known as translation bridges. Because network types often handle frames differently (e.g. Ethernet packets are 1500 bytes and Token Ring packets vary from 4000 to 17800 bytes), translation bridges must disassemble and reassemble packets into a different format. Translation bridges therefore also work at the LLC sublayer within the OSI model.

10.6 Gateway

A gateway is used to change network information between different formats. For example, a gateway may connect an IP LAN with a service provider's ATM backbone network.

Gateways vary broadly in their functionality, depending on the specific task they have been installed for. Many gateways handle interconnection between LAN-based clients and mainframe environments. Gateways generally operate at the Transport and Application layers of the TCP/IP- model and as such frequently run on a network server or a dedicated computer.

- **Repeater** : Physical layer relay.
- **Bridge** : Data link layer relay.
- **Router** : Network layer relay.
- **Gateway** : Any relay at higher layer than network layer.

11 Definition

In the context of data communication, network protocols are defined as formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network. However, the model itself does not provide specific methods of communication. Actual communication is defined by various communication protocols. In other words, a protocol is a standard procedure and format that two data communication devices must understand, accept and use to be able to talk to each other.

12 Purpose of Network Protocols

Network protocols serve these basic functions:

- Address data to the correct recipient(s).
- Physically transmit data from source to destination, with security protection if needed.
- Receive messages and send responses appropriately.

Therefore, without protocols the devices would lack the ability to understand the electronic signals they send to each other over network connections. No one protocol exists that supports all the features every kind of computer network needs. Many different kinds of network protocols have been invented over the years, each attempting to support certain kinds of network communication. Three basic characteristics that distinguish one type of protocol from another are:

1. **Simplex vs. duplex.** A simplex connection allows only one device to transmit on a network. Conversely, duplex network connections allow devices to both transmit and receive data across the same physical link.

2. **Connection-oriented or connectionless**. A connection-oriented network protocol exchanges (a process called a handshake) address information between two devices that allows them to carry on a conversation (called a session) with each other. Conversely, connectionfewer protocols deliver individual messages from one point to another without regard for any similar messages sent before or after (and without knowing whether messages are even successfully received).

3. **Layer**. Network protocols normally work together in groups (called stacks because diagrams often depict protocols as boxes stacked on top of each other). Some protocols function at lower layers closely tied to how different types of wireless or network cabling physically works. Others work at higher layers linked to how network applications work, and some work at intermediate layers in between.

13 Types of Network Protocols

As mentioned before, network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication.

Modern protocols for computer networking all generally use packet switching techniques to send and receive messages in the form of packets, messages subdivided into pieces that are collected and re-assembled at their destination. Hundreds of different computer network protocols have been developed each designed for specific purposes and environments, among them are:

13.1 Internet Protocols

The Internet Protocol family contains a set of related (and among the most widely used network protocols. Beside Internet Protocol (IP) , higher-level protocols like TCP, UDP, HTTP, and FTP all integrate with IP to provide additional capabilities. Similarly, lower-level Internet Protocols like ARP and ICMP also co-exist with IP. In general, higher level protocols in the IP family interact more closely with applications like Web browsers while lower-level protocols interact with network adapters and other computer hardware.

13.2 Wireless Network Protocols

Thanks to Wi-Fi, Bluetooth and LTE, wireless networks have become commonplace. Network protocols designed for use on wireless networks must support roaming mobile devices and deal with issues such as variable data rates and network security.

13.3 Network Routing Protocols

Routing protocols are special-purpose protocols designed specifically for use by network routers on the Internet. A routing protocol can identify other routers, manage the pathways (called routes) between sources and destinations of network messages, and make dynamic routing decisions. Common routing protocols include EIGRP, OSPF and BGP.

14 How Network Protocols are Implemented

Modern operating systems contain built-in software services that implement support for some network protocols. Applications like Web browsers contain software libraries that support the high level protocols necessary for that application to function. For some lower level TCP/IP and routing protocols, support is implemented in directly hardware (silicon chipsets) for improved performance.

Each packet transmitted and received over a network contains binary data (ones and zeros that encode the contents of each message). Most protocols add a small header at the beginning of each packet to store information about the message's sender and its intended destination. Some protocols also add footer at the end. Each network protocol has the ability to identify messages of its own kind and process the headers and footers as part of moving data among devices.

A group of network protocols that work together at higher and lower levels are often called a protocol family. We will study the OSI model that conceptually organizes network protocol families into specific layers.

15 Transmission Problems

Distance is a key factor affecting the integrity of data transmission for the following reasons:

1. The greater the distance between the transmitter and the receiver, the longer required for the message to reach the destination.

2. The farther the distance between the transmitter and the receiver, the more scattering affecting the signal, until a certain stage where the signal becomes incomprehensible to the receiver.

3. More distance means extra connection cables, which means extra cost and the cable is more likely to be affected by the electromagnetic noise sources.

Furthermore, the network performance might be affected by the fading, confusion, and delay.

- **Attenuation**: attenuation is a natural consequence of signal transmission over long distances, which can be defined as the loss of transmission signal strength. The loss happened to the volume of the signal without changing its form, which is also called fading.

  Fading is also liable when transmitting the signal in the form of optical waves using optical fiber cables for the following reasons:

  1. Radiation dispersion of the signal away from the fiber axis.
  2. Collision with impurities found in fiberglass. Fading can be reduced by keeping the length of the cable short, or if it is not applicable then the use of special devices such as reinforcements.

- **Distortion**: it is known as an unwanted change in the signal form as it is transmitted across the grid lines, it become unclear and does not reflect the actual data that came from the source. There are several ways to prevent distortion:

  1. Adhering to the instructions provided by the broadcast center. The need to use the appropriate type cables with maintaining an acceptable transmission length.
  2. Manage the expected interference sources and pass the network cables far from them.
  3. Using error detection protocols.

- **Dispersion**: it is one of the problems to which the signal transmitted between the sender and the receiver is exposed because of the type of the medium used in the transmission. Dispersion means the occurrence of the binary symbols sent, which leads to overlap with each other so that it is not possible to distinguish between the beginning and the end of each binary code of data.

- **Jitter**: It can be defined as a loss in the transmitted signal between the transmitter and the receiver, which leads to a difference in the arriving time. The signal may arrive before or after its expected time. This problem can be avoided using a series of clock pulses synchronized with the transmitted signal, whether through the physical entity, the software or the use of protocols to achieve the required synchronization.

- **Collision**: Occurs between two signals transmitted in the carrier medium, were two nodes in the network try to transmit at the same time.

- **Cross Talk**: It is a form of interference resulting from transmitting signals through two adjacent transmission lines, which leads to overlapped signals. This is similar to the case of hearing people talking to each other during telephone call. This phenomenon is avoided by the use of additional protective covers in the cables.

16 TCP/IP (Transmission Control Protocol/Int Protocol)

TCP/IP is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet). TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

TCP/IP uses the client/server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network. Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continuously.

The TCP/IP model differs slightly from the seven-layer Open Systems Interconnection (OSI) networking model designed after it, which defines how applications can communicate over a network.

16.1 TCP/IP Layers

TCP/IP functionality is divided into four layers, each of which includes specific protocols.

- **The application layer** provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).

- **The transport layer** is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

- **The network layer** also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

- **The physical layer** consists of protocols that operate only on a link – the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).

Each layer of the stack depends on the layers below it; that is, each layer services the layer above or below it. When two computers communicate, each computer has its own set of layers. When you send a message to another computer on the network, your information starts at the top layer of your computer, travels down all the layers to the bottom of the stack, and then jumps to the other computer. When your information arrives on the other computer, it starts at the bottom layer and moves up the stack to the application in the top layer.

Each layer has a special function: ***The lower layers are hardware oriented, and the highest layer provides user services***, such as e-mail, file transfers, and general network monitoring.

16.2 Advantages of TCP/IP

- TCP/IP is nonproprietary and, as a result, is not controlled by any single company. Therefore, the internet protocol suite can be modified easily.

- It is compatible with all operating systems, so it can communicate with any other system.

- The internet protocol suite is also compatible with all types of computer hardware and networks.
- TCP/IP is highly scalable and, as a routable protocol, can determine the most efficient path through the network.

16.3 Security and the TCP/IP

Each layer has security mechanisms:

1. **Physical Layer:**
    - Packet Filters – A packet filter is designed to set between the internal and external network. As packets enter or leave the network, they are compared to a set of rules. This determines if they are passed, rejected, or dropped. A router ACL is an example of a packet filter.
    - NAT – NAT (Network Address Translation) is a means of translating addresses. Most residential high speed Internet users use NAT. It provides security as it hides the internal address from external networks.
    - CHAP – CHAP (Challenge Handshake Authentication Protocol) is an authentication protocol that is used as an alternative to passing clear text usernames and passwords

2. **Network Layer:**

   - PPTP – PPTP (Point to Point Tunneling Protocol) was developed by a consortium of vendors including Microsoft and 3Com. Its purpose is to provide data encapsulation. Security for PPTP is provided by Microsoft Point-to-Point Encryption. b) IPsec – IPsec is used to protect IP packets and defend against network attacks. It uses cryptographic-based protection services, security protocols, and dynamic key management.

3. **Transport Layer:**

   - SSL– SSL (Secure Sockets Layer) is a protocol independent technology that enables users to ensure security for data that is exchanged over the Internet.
   - TLS – This protocol is similar to SSL. The TLS (Transport Layer Security) protocol is a layered approach to data security that consists of several sub-protocols.

4. **Application Layer:**

- RADIUS – RADIUS (Remote Authentication Dial-In User Service) is the most widely used dialup authentication protocol in the world. It offers authentication and
- S-MIME – S/MIME (Secure / Multipurpose Internet Mail Extensions) is a protocol designed to secure e-mail. It secures clear-text email by adding digital signatures and encryption.
- Virus scanners – Virus scanners play an important part of security.

17 The OSI (Open Systems Interconnection) Data Model

The OSI model began as a reference model; it was created by the International Organization for Standarization (ISO) to provide a logical framework for how data communication process should interact across networks. There are seven layers in the OSI model. Each layer is responsible for a particular aspect of data communication. During the sending process, each layer (from top to down) will add a specific header to the raw data. At the reception, headers are eliminated conversely until the data arrived to the receiving application.

- Physical layer: ensures a safe and efficient travel of data; consists of electronic circuits for data transmission etc.
- Data link layer: in charge of data encapsulation under the form of packets and their interpretation at the physical layer.
- Network layer: in charge of packets transmission from a source A to a destination B.
- Transport layer: in charge of the delivery of packets from a source A to a destination B.
- Session layer: in charge of the management of network access.

- Presentation layer: determines the format of the data transmitted to applications, data compressing/decompressing, encrypting etc.
- Application layer: contains the applications which are used by the end-user, such as Java, Word etc.