AJSP
المجلة العربية للنشر العلمي
العدد السادس والعشرون
تاريخ الإصدار: 2 – كانون الأول – 2020 م
www.ajsp.net
ISSN: 2663-5798

"The Network Performance for Public Users"

By Researchers:

Ahmed Algahtani and Ghada Shawly

Graduate Projec / Master of Applied and Science

Major: Information Technology Management

Missouri Western State University

St. Joseph, Missouri

2016

العدد السادس والعشرون
تاريخ الإصدار: 2 – كانون الأول – 2020 م
www.ajsp.net
ISSN: 2663-5798

Abstract:

Network improve the way people communicate with each other by offering speed and availability. Network allow us to communicate with individuals from around the world from offices and homes. However, network have inherent limitations; third world countries lack the infrastructure to offer high-speed internet and networking services. The speed, security, and bandwidth are the critical characteristics of networks on the internet and these items also have the greatest impact on network performance. Therefore, our article will discuss the current issues effecting the availability of networks solutions, and will highlight the way these issues impact public networks at universities and public airport. It will also suggest solutions and technologies to improve network performance.

Introduction

Back to 1930, when Telex messaging network or as it was known as Teletypewriter was used in the United Kingdom and some other countries in European, and that was the first network communication that human knew. It was very basic communication and limited used. The way that the network communication worked is there was an operator who made the communication between two people (Meyers, Comp TIA Network+ Exam N10-005 , 2012). For example, if someone his name is Ahmed, and he wants to call another person who is name Mohammed in different location. Ahmed picks up the phone and talk to the operator asking for Mohammed. Mohammed has a unique address that Ahmed should know because he needs to give it to the operator. Then the operator will connect Ahmed's line to Mohammed's line using the switchboard to make the connection between them. The switchboard acted like a circuit switch when connected two lines together. The people in that time used for postal, telegraph, and telephone services. However, the number of people had been increased, and control so many lines became an issue.

Figure 1 Old time telephone operator.

The problem of many telephone wires was solved by using a box called multiplexers. This multiplexer works like an organizer. There are many inputs; however, only output from this box will be the selected input. For example, if I have lines A, B, C, and D, and I select line C to be the output, I will have only line C as output from this box.

ISSN: 2663-5798

Figure 2 AN/FCC-3 TTY Multiplexer in 1958

Over time, there were many local exchanges over the United States. Local exchanges were a characterized gathering of individual telephone circuits assisted by a single multiplexer. A central office is a term that called for a place that has one or more exchanges. In early 1950, dial-up started to show up, and many people who worked as operators got fired. The rest of them had their job because local calls were handled physically; however, central offices' connection were taken care of by particular multiplexed trunk lines.

The old fashioned of trunk lines were amazing. They could care many of voice calls on one single cable, and to keep them separate, people used frequency. The rang of this cable frequency was between 350 Hz – 4000 Hz, and enough of people could use part of this range for their talking. To make everyone's frequency unique, the multiplexer added small part of frequency that different from one to another to people's frequency. This operation is called Frequency Division Multiplexing (FDM).

Using manually connection for long distance was something that had to be changed. Because at every intersection of these line cables an operator got to attach these calls together. Once one call got been connected, the two people who were on their phones could talk, and the circuit that is between these two phones is called circuit switching.

This system of connection which was analog network was working fine until 1950 when telephones became popular, and many people in the United State wanted to have this service. Transferring this signals (analog signals) for long distance is difficult because the signal is needed to recreate and sent again, and that can't be happened. Here is when digital signal was discovered. Digital signal can be recreated by a device called a repeater, and resend the signal for a long distance by using repeaters. Moreover, digital signals have opened the way in front of people to use this signal to transfer data more than voice (Meyers, Comp TIA Network+ Exam N10-005, 2012).

ISSN: 2663-5798

Figure 3 Repeater for digital signal

Since 1930, the network has gone throw several levels of developments. In recent time, the network has several layers (Application, Presentation, Session, Transport, Network, Data Link, Physical), and Physical layer which is the wire that connect devices with each others is the most important for this research.

Because if the end user wants to have a grate connection to the network, there should be in the Physical layer a good technology that is offer by the providers. For example, there are three of more suffusion cables in the network areas DSL, coaxial, and Fiber Optic.

1. Network Topology

To connect different computers or networks together, there are many ways. Some of them are old technic, and the others are modern. There are seven networks topologies bus, ring, and star those are previous topologies while hybrid, mesh, point to multipoint, and point to point are the prevailing (Meyers, Comp TIA Network+ Exam N10-005, 2012) print.

a. Bus Topology

The idea of this topology is all computers and servers are connected in a line single cable, and when a computer send data to another computer or server, the data will travel in the whole network until it arrives to its destination; however, travelling data from a PC to another PC over the cable can cause duplicate data because the data can arrive to end of the cable and return again to the network. Therefore, there has to be terminator which is a device in the both side of network to end the data from reflecting (Sparrow, 2013).

There are two sorts of transport topology: Linear Bus Topology and Distributed Bus Topology. In Linear Bus Topology, all hubs of the system are associated with a typical transmission medium which has precisely two endpoints. Appropriated Bus in which the greater part of the hubs of the system are associated with a typical transmission medium which has more than two endpoints that are made by adding branches to the primary area of the transmission medium.

There are some advantages and disadvantages in this topology. Moreover, bus topology has limitation of use. Bus systems do best with a predetermined number of gadgets. On the off chance that more than constrained PCs are added to a transport, execution issues will be result. In the event that the spine link comes up short, the whole system successfully gets to be unusable (UKessays, 2015).

ISSN: 2663-5798

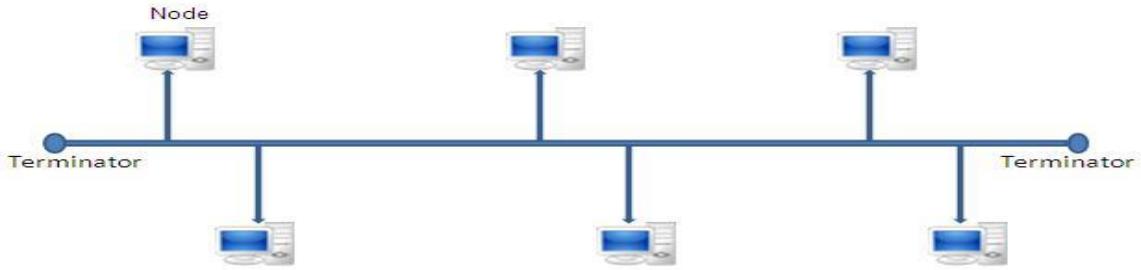


Figure 4 Bus Topology

The advantages of bus network centered in being cheap because it does not need many cables, easy to setup, and easy to link another computer to the network. The disadvantages are when there is a cut in the main cable the whole network will be shutdown, terminator is an important thing without it the network won't work, it is hard to find the problem in the network if there is, and if the business becomes larger, this topology can't be used because bus network is only for small businesses (Edraw, Network Topology Diagrams).

b. Ring Topology

This topology works as the bus network, but the different is that the ring topology is connected in a circle; therefore, it does not need to termination in the end of cable, but data needs to travel over the whole network. The way that ring topology works is the sign is exchanged through a token for one station to the following. A token is a special series of bits that travels around a token-ring network (Knowledge Systems Institute). Each network has only one token. At the point when a station needs to transmit, it snatches the token, connects information and a location to it. And afterward courses it around the ring. The token goes along the ring till achieves the destination address. The getting PC answers an affirmation to the sender source. The sender then discharges the token for use by another PC. Every station on the ring has rise to get to yet one and only station can utilize token at once. To permit an organized access to the ring, a solitary electronic token goes starting with one PC then onto the next around the ring. A PC can just transmit information when it catches the token (UKessays, 2015).

The advantages and disadvantages of ring network are the same of bus topology.

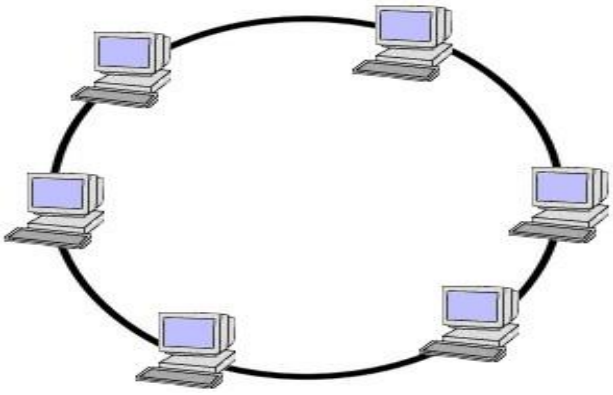


Figure 5 Ring Topology

c. Star Topology

ISSN: 2663-5798

A star system is a neighborhood (LAN) in which all hubs (workstations or different gadgets) are straightforwardly associated with a typical focal PC. Each workstation is by implication associated with each other through the focal PC. In some star arranges, the focal PC can likewise work as a workstation (Techtarget, 2006).

New gadgets or hubs can without much of a stretch be added to the Star Network by simply developing a link from the center. As a result of the center point controls everything, the expansion or evacuation of gadgets are done utilizing the center. On the off chance that the center includes a gadget, for example, a printer or a fax machine, the various PCs on the system can get to that new gadget by getting to the center. The gadget is no should be introduced on every one of the PCs in the whole system. The focal capacity is financially savvy and less demanding to keep up. The star system topology requires more link than the typical Bus topology. A typical link that is utilized as a part of star system is the UTP or the unshielded curved pair link. Another regular link that is utilized as a part of star systems is the RJ45 or the Ethernet links (UKessays, 2015).

In the event that one PC falls flat in the system, it doesn't influence whatever other PC in the system and the reasons for this PC can be effortlessly changed to the following PC effectively utilizing the controls of center. In a Star Network Topology, it is conceivable to have all the critical information reinforcements on the center in a private envelope so in the event that one PC falls flat, it can at present use information utilizing the following PC as a part of the system and getting to the reinforcement records on the center point (UKessays, 2015).

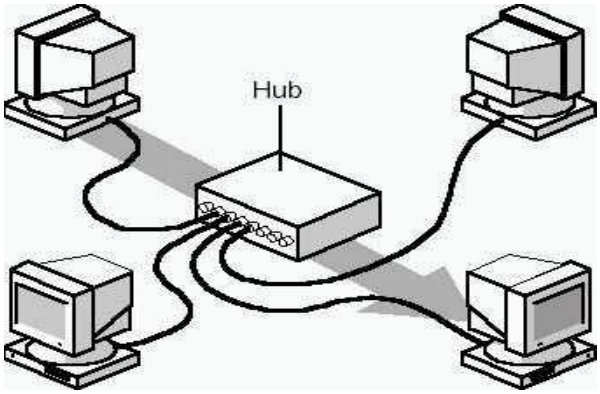


Figure 6 Star Topology
The advantages of this topology are:

A. The topology offers effortlessness of operation.

B. It additionally accomplishes detachment of every gadget in the system.

C. Adding or expelling system hubs is simple, and should be possible without influencing the whole system.

D. It is anything but difficult to distinguish deficiencies in the system gadgets.

E. As the examination of activity is simple, the topology postures lesser security hazard.

F. Data bundles don't need to go through numerous hubs, as on account of a ring system. In this manner, with the utilization of a high-limit focal center point, activity burden can be taken care of at genuinely tolerable rates.

The disadvantages are:

A. Network operation relies on upon the working of the focal center point. Subsequently, focal center point disappointment prompts disappointment of the whole system.

B. Also, the quantity of hubs that can be included, relies on upon the limit of the focal center point.

C. The setup expense is very high (Oak Manali, 2016).

d. Hybrid Topology

Aside from these essential sorts of system topologies, there are cross breed system topologies, which have a blend of two or more fundamental system structures. Figure 7 Hybrid Topology demonstrates a mix of bus, star, and ring topologies (Oak Manali, 2014).

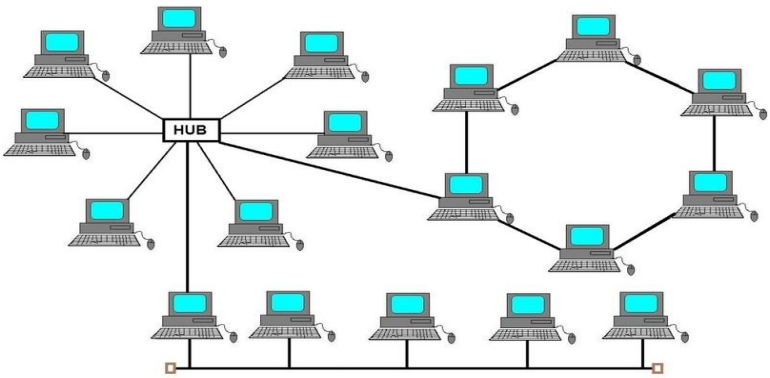


Figure 7 Hybrid Topology

The pros and cons of this topology:

As a crossover topology results from a blend of two or more topologies, it has both the preferences and burdens of the topologies included. The primary favorable position of a half breed system is that two divergent topologies can be joined without exasperating the current design of a system. The utilization of half and half advances makes a system effortlessly expandable (Oak Manali, 2014).

العدد السادس والعشرون
تاريخ الإصدار: 2 – كانون الأول – 2020 م
www.ajsp.net
ISSN: 2663-5798

e. Mesh Topology

There are two types of mesh topologies. First one is when each computer is linked to anther in the network, and that is called fully meshed Figure 8 Fully Mesh Topology.

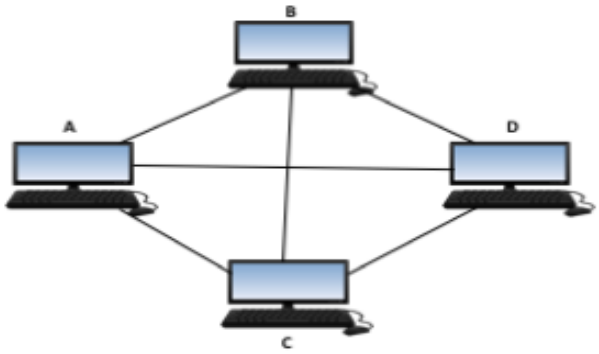


Figure 8 Fully Mesh Topology

Fully meshed gives every computer link to another computer that is in the network. Therefore, if there is no connection in one way, data can go to its distention because of many ways that sender has (Knowledge Systems Institute). For instance, according to Figure 8 Fully Mesh Topology, computer B has three ways to send and receive data. If computer B wants to communicate to computer C, and the link that is between computer B and C is down then computer B has two other ways. It has link that goes throw computer A, and another link that goes over computer D. This network can garnet for computer B to send and receive data three times than any other network. Fully mesh topology consider as the best topology for the network, but it is expensive to be setted up. Moreover, this network can be independent because every computer in the network has its own way to communicate.

Another meshed is called partially, and this method does not give every computer link to another computer in the network. However, some computers need to go over other computers to communicate. For example, there are four computers A, B, C, and D, and these four computers are connected using partially meshed. Computer A is connected to computer B, and computer B is linked to computer C, and D. At the same time, computers C and D are connected to each other. The view of this network looks like the Figure 9 Partially Mesh Topology.

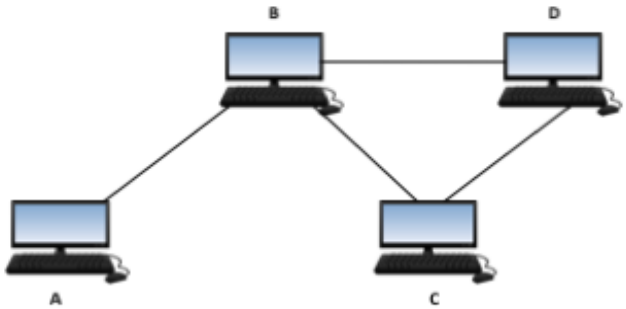


Figure 9 Partially Mesh Topology

ISSN: 2663-5798

When computer A wants to talk to computer C or D, it needs to pass computer B. As a result, if computer B is down, then computer A will be insulated from the network. This topology which is partially mesh can be described as dependent network because computer A depends on computer B to communicate with computers C and D.

Pros and cons of mesh topology are expensive to be built up compressing to other networks; however, it covers most computers in the network that if it does not cover all computers in the system. Data can be transmitted from various gadgets all the while. This topology can withstand high activity, but there are high odds of excess in a significant number of the system associations. Extension and adjustment in this topology should be possible without upsetting different hubs; whoever, set-up and upkeep of this topology is extremely troublesome. Indeed, even organization of the system is intense (Sparrow, 2011).

f. Point to Multipoint Topology

Point-to-multipoint (PMP) correspondence alludes to correspondence that is expert through a particular and particular type of one-to-numerous associations, offering a few ways from one single area to different areas. Point-to-multipoint is for the most part shortened as PTMP, P2MP or PMP. PMP correspondence is generally utilized as a part of information transfers. Figure 10 shows the topology of point to multipoint.

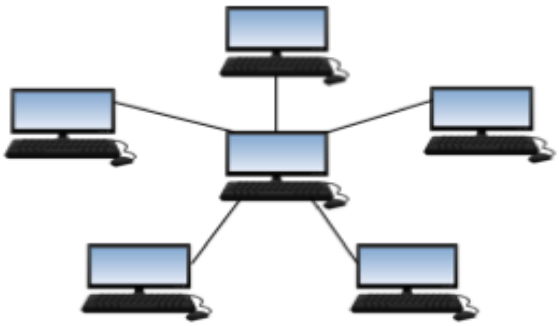


Figure 10 Point to Multipoint Topology

PMP is normally utilized for building up private endeavor availability to workplaces in remote areas, long-extend remote backhaul answers for different locales, and last-mile broadband access. In that capacity, it is broadly utilized as a part of IP telephony and remote Internet by method for gigahertz radio frequencies. These PMP systems are utilized in dissemination courtesies, enormous corporate grounds, school areas, open wellbeing applications.

The point-to-multipoint topology comprises of a focal base station that backings a few supporter stations. These offer system access from a solitary area to different areas, allowing them to utilize the same system assets between them. The scaffold situated at the focal area is known as the base station extension or root span. All information that goes between the remote extension customers ought to at first go by means of the root span.

A point-to-multipoint system can be effortlessly sent when contrasted with the organization of a point-to-point system on the grounds that the hardware must be conveyed just at the new endorser's site. The main condition is that all the

remote destinations must come surprisingly close to the base station. Slopes, trees and different sorts of checks make point-to-multipoint gestures unacceptable for office and private scope.

PMP frameworks are classified into single framework and bi-directional frameworks. A point-to-multipoint system is reasonable for either clients or backhaul operations that need a fast, dependable association, however agonized over paying for unused committed limit. The downside of point-to-multipoint hub topology is its failure to interconnect with different hubs as a result of the directional radio wire (TechopediA, Point to Multipoint Communication).

The advantage and disadvantage of PMP:

While including a recipient site in a PMP system, the required gear just should be conveyed to the supporter's area, and the framework is set up and extended. It is essential to note, in any case, that remote locales must be inside deceivability and scope of a base station. On account of a PMP hub innovation, hubs can't interface with different hubs because of the directional receiving wire. The cooperation of fringe remotes in a PTMP connection is additionally constrained to the Main Point however never among remotes (TechopediA, Point to Multipoint Communication).

g. Point to Point Topology (Tree Topology)

A tree topology is a kind of system topology that incorporates no less than three particular levels in a topology pecking order. Tree topologies are esteemed for their versatility and openness for investigating.

Every hub in a chain of command level has point-to-point joins with each neighboring hub on its beneath level. Every single optional hub has point-to-point connections to the tertiary hubs in their ward, and the essential hub has a point-to-point association with every auxiliary hub. At the point when seen outwardly, these frameworks seem like a tree structure (TechopediA, Tree Topology). Moreover, when there are two computers are connected to each other directly, this topology is called point to point. The connection between these two devices can be wire or wireless. The topology of wireless Networks is concentrated on using central radio base stations (BSs) and several exterior antennas communicating with each other. Figure 11 Point to Point Topology.y.

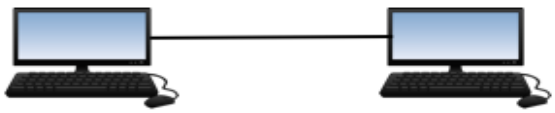


Figure 11 Point to Point Topology.
The pros of point to point topology:

A. The tree topology is valuable in situations where a star or transport can't be executed independently. It is most-suited in systems administration various bureaus of a college or organization, where every unit (star portion) works independently, and is likewise associated with the fundamental hub (root hub).

B. The upsides of centralization that are accomplished in a star topology are acquired by the individual star fragments in a tree system.

C. Each star fragment gets a devoted connection from the focal transport. In this way, coming up short of one portion does not influence whatever remains of the system.

D. Fault distinguishing proof is simple.

E. The system can be extended by the expansion of optional hubs. In this way, adaptability is accomplished (Sparrow, 2012).

The cons are:

A. As various portions are associated with a focal transport, the system depends vigorously on the transport. Its disappointment influences the whole system.

B. Owing to its size and many-sided quality, support is difficult and expenses are high. Likewise, design is troublesome in contrast with that in different topologies.

C. Though it is adaptable, the quantity of hubs that can be included depends the limit of the focal transport and on the link sort.

h. Wireless Infrastructure Topology

The framework remote topology is ordinarily used to extend a wired LAN to incorporate remote gadgets. Remote gadgets speak with the wired LAN through a base station known as an entrance point (AP) or remote access point (WAP).

The AP frames an extension between a remote and wired LAN, and all transmissions between remote stations, or between a framework and a wired system customer, experience the AP.

APs are not versatile and need to stay associated with the wired system; in this manner, they turn out to be a piece of the wired system base in this manner the name. In base remote systems, there may be a few access focuses giving remote scope to an extensive range or just a solitary access point for a little territory, for example, a solitary home or little building (Brain Bell, Wireless Topology).

ISSN: 2663-5798

i. Ad hoc Network Topology

In a remote specially appointed topology, gadgets convey specifically between themselves without utilizing an entrance point. This distributed system configuration is ordinarily used to interface a little number of PCs or remote gadgets. As an illustration, a specially appointed remote system might be set up briefly between portable workstations in a meeting room or to interface with frameworks in a home rather than a wired arrangement. The specially appointed remote outline gives a snappy strategy to share records and assets between a little number of frameworks (S. Toumpis, 2006).

To connect multiple computers, servers, or computers with servers together, we need to have wired cables or wireless devises. Moreover, there must be a modem in each end of the cable. This chapter is going to discuss Digital Subscriber Line (DSL) and Fiber Optic technologies. In additional, it is going to explain a modem, and how it works.

2. Wired Networks

There are two technologies of wired cables: twisted copper which is DSL and the fiber optic cable. Twisted copper is the old technology of network cable and the fiber optic cable is the new one. These cables are set up for an entire city. After that, the city will be connected with another city, and these two cities are going to be connected by wired cables.

a. DSL Concept

Digital Subscriber Line (DSL) is twisted copper which allows for subscribers to send and receive data over phone line cable. Moreover, it allows for users to send voice frequency through this cable. In 1999, there were 882,000 of subscribers over the world who used this technology. However, four years later this number grow to become 63,840,000 subscribers. That shows how important is the transfer data for people.

b. DSL Advantages

It is able to take the existing telephone infrastructure for voice and data while many other broadband, such as satellite and fiber can't do that. Moreover, DSL provides the requirement that users' need. For instance, home users, small and medium businesses, and school. However, DSL needs a modem because the existing infrastructure.

ISSN: 2663-5798

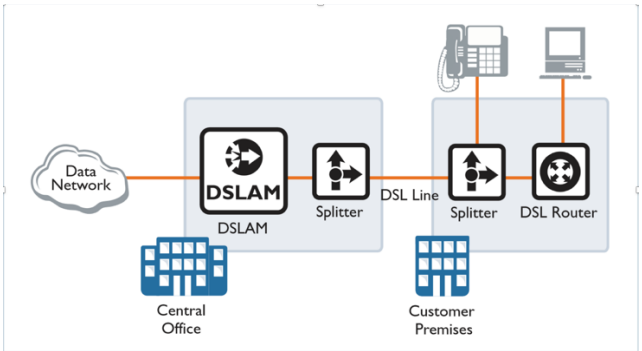


Figure 12 DSL connection setup.

DSL has three types: symmetric, asymmetric, and both symmetric and asymmetric.

c. Symmetric DSL Concept

Symmetric DSL is the rates of the transmission data for the downstream and upstream are the same. There are three kinds of the symmetric (High data rate Digital Subscriber Line (HDSL), Symmetric Digital Subscriber Line (SDSL), and Symmetric High bit rate Digital Subscriber Line (SHDSL)), and the difference between them is in speed and distance. In HDSL, the whole transmission rate of this type is 1.544 Mbps. However, when data is transferred over twisted wire, the signal is splatted into two twisted wire pairs to become 784 Kbps for each twisted wire. SHDSL is the same as HDSL but the speed is different; it has 2.3 Mbps in one line and 4.6 Mbps in two lines. SDSL uses single telephone line to transmit data in speed 2.3 Mbps. HDSL has a maximum wire length which is 3.7 Km while it is 3 Km in SDSL and 5 Km in SHDSL.

d. Asymmetric DSL

There are five types of Asymmetric DSL (Asymmetric Digital Subscriber Line (ADSL), ADSL lite, ADSL 2, ADSL 2+, ADSL 2++ or 4), and they have high speed in downstream than upstream. All these five give a connection to the user's end; however, the different is only in speed. For example, ADSL gives 10 Mbps of the transmit data in downstream and 1 Mbps in upstream while in ADLS 4 the speed reach 52 Mbps in downstream.

e. Both Symmetric and Asymmetric

Very high bit rate Digital Subscriber Line (VDSL) works as asymmetric over short distance, and it gives high rate of transmit up to 52 Mbps. But also it can be configured to work as symmetric to give 10 Mbps for both directions downstream and upstream.

العدد السادس والعشرون
تاريخ الإصدار: 2 – كانون الأول – 2020 م
www.ajsp.net
ISSN: 2663-5798

f. The Way DSL Works and a Modem

Computers use digital signals to share information, and subscribers need to have a modem to convert this signal to analogue and the other way around in order to send and receive this signal over the network. The signal could be voice or digital data frequency. In order to disperse between the voice signal and digital data signal, the copper wire is able to support 1 MHz of frequencies approximately to separate between voice and data frequencies. Therefore, the signals that are below 4 KHz are back to the voice. On the other hand, the signals that are above 25 KHz refer to data.

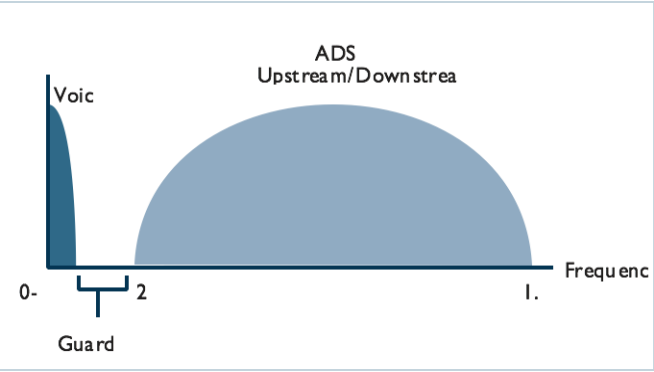


Figure 13 splitting the frequencies.

As a result, ADSL uses a splitter to collect the voice signals and digital signals to pass them over the copper wire then divide them in the other side. When they spread in the other side, the voice frequency goes to telephone exchange, and digital data frequency is sent to the Digital Subscriber Line Access Multiplexor (DSLAM). (DSLAM) is a step before the signal goes to the service provider. Therefore, the digital data can't never switch to go to telephone exchange, nor voice signal can go to Internet Service Provider (ISP).

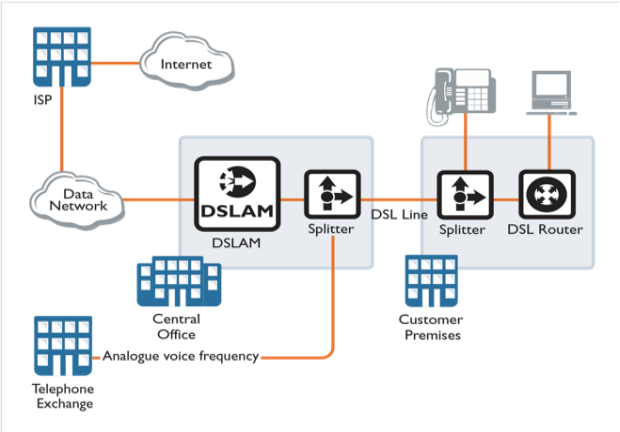


Figure 14 ADSL network setup.

ADSL is important and different than others DSL connections. ADSL can send and receive data at the same time. When most of the bandwidth is downstream, there is small bandwidth can be upstream to the server provider.

DSLAM: it is a device that get the high speed of digital data from many subscribers and aggregates it onto a single high-capacity connection (ATM or Gigabit Ethernet line) to the Internet Service Provider and vice versa. DSLAMs are generally flexible and can support a number of different DSL connections as well as different protocol and modulation technologies in the same type of DSL. (Allied Telesis, 2007).

g. History of Fiber Optics

The idea of sending a message from tower to another tower using light was invented by the French Chappe brothers in 1790s.

After 50 years of inventing this idea, Daniel Collodon and Jacques Babinet found that light could go as the water rushes out of taps. However, John Tyndall the one who could approve that light could be bent by water in 1854. Since that time people were thinking about light and how they can use it in deferent thing. Until 1880 became, and William Wheeler invented a system that made light separated around his home using pipes to do that. The first try of invented a television was in 1895 when the engineering Henry Saint-Rene designed a system depending on the idea that was came by doctors Roth and Reuss. The idea was bent glass rods for illuminate body cavities. He used the bent glass rods for direct light images.

After twenty-five years from first attempt of invent the television, John Logie Baird came with the idea that used arrays of transparent rods to transmit images to get a television while Clarence Hansell did as John did but it was for facsimiles.

In 1930 was the first bundle of optical fiber used for transmit an image and that was by Heinrich Lamm. The laser was presented in 1958 as a productive wellspring of light. The idea was presented by Charles Townes and Arthur Schawlow to demonstrate that masers could be made to work in optical and infrared areas. Fundamentally, light is reflected forward and backward in an invigorated medium to produce enhanced light instead of energized atoms of gas intensified to create radio waves, just like the case with the maser. Laser stands for "light intensification by animated discharge of radiation." Helium neon gas laser which is the first constantly operating is made-up and examined in 1960. That was in the same year which an operable laser was created. The operable laser made-up a pulse of light.

One year after the helium neon was invented, Elias Snitzer had a theoretical explanation that was about single mode fibers. The core of this single mode could be so small to carry light with just one wave-guide mode. Moreover, Elias had the ability to approve that a leaser pointed within a thin glass fiber; however, this idea was possible for medical application not for communication application because losing light was very large.

In 1964, Charles Kao and George Hockham could approve that theoretically, losing light in the glass fibers could be got over by eliminating impurities. Six years later, scientists at Corning Glass Works had a goal of creating single mode fibers with decrease fewer then 20 dB/km, and he succeeded of doing it. This was accomplished through doping silica glass with titanium.

In the same year 1970, Morton Panish and Izuo Hayashi of Bell Laboratories, alongside a gathering from the Ioffe Physical Institute in Leningrad, exhibited a semiconductor diode laser fit for emanating consistent waves at room temperature. After that, Bell Laboratories, in 1973, urbanized an altered substance vapor affidavit prepare that warms synthetic vapors and oxygen to shape ultra-straightforward glass that can be mass-created into low-misfortune optical fiber. This procedure still remains the standard for fiber-optic link producing.

In 1975, the Dorset (UK) police connection non-trial fiber optic link. Two years later, Long Beach in California had the principal live telephone traffic through fiber optics. Next, between end 1970 and beginning 1980, telephone companies started to procedure fiber widely in their set-up communications. The erbium-doped fiber enhancer, which lessened the expense of long-separation fiber frameworks by killing the requirement for optical-electrical-optical repeaters, was imagined in 1986 by David Payne of the University of Southampton and Emmanuel Desurvire at Bell Labratories. In view of Desurvire's improved laser intensification innovation, the main transoceanic phone link went into operation in 1988.

In 1991, Desurvire and Payne exhibited optical intensifiers that were incorporated with the fiber-optic link itself. The all-optic framework could convey 100 times more data than link with electronic intensifiers. Additionally, in 1991, photonic precious stone fiber was created. This fiber manages light by method for diffraction from an intermittent structure rather then aggregate inside reflection which permits energy to be conveyed all the more productively then with ordinary strands in this manner enhancing execution. The principal all-optic fiber link, TPC-5, that uses optical speakers was laid over the Pacific Ocean in 1996. The next year the Fiber Optic Link Around the Globe (FLAG) turned into the longest single-link system on the planet and gave the framework to the up and coming era of Internet applications. (Timbercon, Web).

Since that time, people have developed the way of sending a message using the light until it became the best technology of transferring data over the network. This technology now is calling fiber optic. The fiber optic uses a leaser instead of light to send and receive data.

h. Cables of Fiber Optics

Fiber optic cable is made from glasses, and it is a new technology of transmit data over the network. The backbone of the network is cabling because without it there is no connection at all between two or more computers, and there are two types of fiber optic cables (single mode and multimode). The different between them in the core of the cable. In single mode, the core is so narrow. The size of this core usually come between 8 – 10 µm while the cladding that covers the core is 125 µm. The last layer of the fiber optic cable is coating, and this layer cover the cladding in size 250 µm. In the other hand, there is multimode cable, and it has the same sizes of cladding and coating that single mode has. However, the difference is in the core. The core size is 50 or 62.5 µm (Meridian Technologies, 2008).

ISSN: 2663-5798

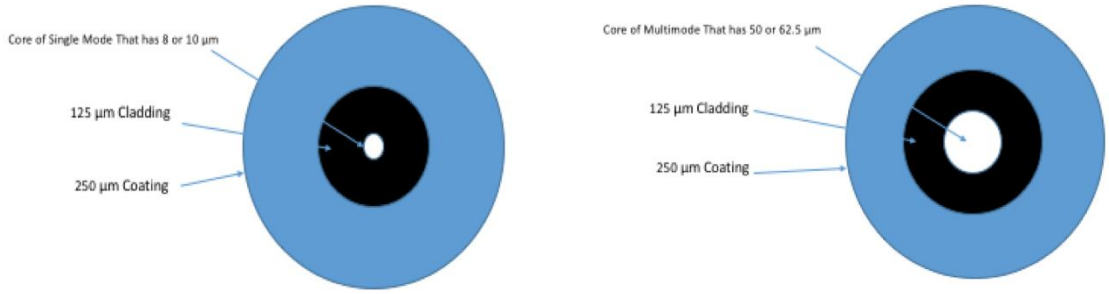


Figure 15 Core of Single Mode and Core of Multimode.

i. The Pros and Cons between Single Mode and Multimode:

Everything has some advantages and disadvantages, and single mode and multimode cables have pros and cons.

First of all, single mode of fiber optic cable characterized in high quality of seeped in transmit data. In additional,

, and everyone has its won used. Therefore, it can be seen all these kinds of fiber optic cables uses such as, LANs network, datacom, telecommunications, CATV, test equipment, gigabit Ethernet, video multimedia, medical, military, asynchronous transmission mode (ATM), active device transceiver, interconnections for O/E modules.

3. Wireless Networks

Using the wireless networks, we can move data from a place to another without the needs of using cables. The wireless networks are standing by to the wired networks, and they are better than the wired networks because the wireless required less infrastructure and they cover large areas almost everywhere. The wireless networks are also less expensive than using the wired networks because there is no need to using cable links between each site. In some situations that are related to the physical and the environmental necessity it is difficult to use wired networks such as in the historical buildings, trading floors, concrete buildings and warehouses. People can use laptops, smart phones and tablets to access the wireless networks. The media of transmission network in the wireless networks is called radio frequency signals. This gives the user's freedom from cables gives more network flexibility. Moreover, this network allows users to place different wireless enabled devices in convenient places throw out homes and offices. It also allows users to move their devices between places as long as the device is within the signal.

ISSN: 2663-5798

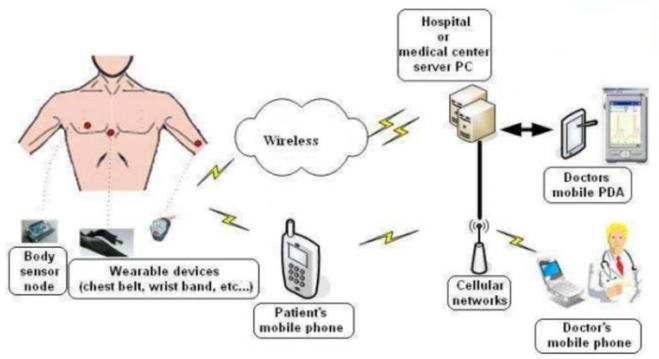
a. Radio Frequency Concept

The frequency can be used to measure the rate of waves, such as radio waves or light waves. Therefore, the radio frequency has different standards and those standards have been published by an organization called IEEE which is the world's largest professional association advancing innovation and technological excellence for the benefit of humanity. IEEE and its members inspire a global community to innovate for a better tomorrow through its highly-cited publications, conferences, technology standards, and professional and educational activities. IEEE is the trusted "voice" for engineering, computing and technology information around the globe. (Crow, 1997)

b. Wireless Body Area Networks (WBAN)

It is usually used in the health care organizations. It connects health care devices such as the medical devices and pagers using Radio Frequency Identification (RFID). The RFID systems consist of small transponders, or tags, attached to physical objects. RFID tags may soon become the most pervasive microchip in history. When wirelessly interrogated by RFID transceivers, or readers, tags respond with some identifying information that may be associated with arbitrary data records. Paper: RFID (Radio Frequency Identification): Principles and Applications. Stephen A. Weis.

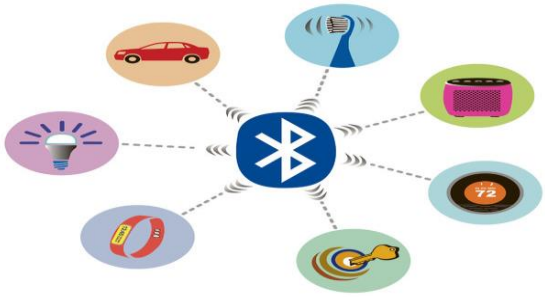
Near Field Communication (NFC) is also used in the wireless body networks. NFC is a set of communication protocols that allows two electronic devices to establish communication within 4 cm of each other. The data transferred in the wireless body area networks are very low in the range and in the distance for example the data transferred is 1 Mbps in 1 meter. (Kumbhare, 2015)



An example about the wireless body area networks can be happened every day at hospitals. Patients usually are required to use some wearable devices such as chest belt or wrist band to measure the heart rate or the blood pressure. The outputs from these devices are sending throw the wireless networks to the medical center computer and then to the doctor mobile. (Kumbhare, 2015)

c. Wireless Personal Area Networks (WPAN)

It connects cellphones and headphones within few meters with a data speed up to 1 Mbps. The PAN standers are differentiated by the Bluetooth (IEEE 802.15.1) which is a specification that describe how mobile phones and computers can be easily interconnected using short range wireless connection. Using this technology, users can get quickly synchronized with information in a lap top with a printer to print out some files, the Universal Wireless Broadband (IEEE 802.15.3) such as the wireless router, and the ZigBee Alliance (IEEE 802.15.4) which is the new language of connected lighting in homes and business. It is in innovative products that provide new ways to use light, improve comfort and convenience, and save energy. (Park, 2007)



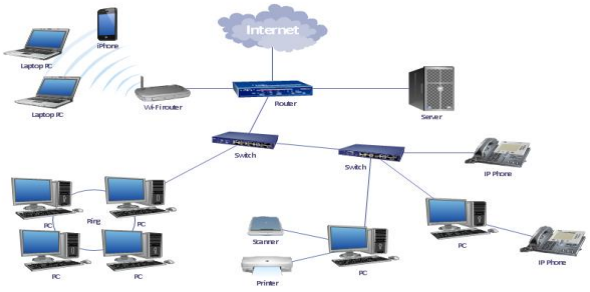
The fitness watches such as Fitbit and Garmin are perfect examples about the wireless personal area networks. The watch calculates your steps and your calories lost and send the data to your mobile phone using Bluetooth techniques, to give you more details about your fitness progress.

d. Wireless Local Area Networks (WLAN) IEEE 802.11

It is used inside big buildings such as universities or companies. The transaction's speed of this type of wireless networks is ranged between 10 to 66 GHz, and it provides up to 54 Mbps of data transmission with the range 100 meters. Nowadays the wireless spectrum is available as a new technique which consists of electromagnetic radiation which is a form of energy that is all around us and takes many forms, such as radio waves, microwaves, X-rays and gamma rays. Sunlight is also a form of EM energy, but visible light is only a small portion of the EM spectrum, which contains a broad range of electromagnetic wavelengths.

These electromagnetic radiations are combined with and frequency bands which is is a specific range of frequencies in the radio frequency spectrum, which is divided among ranges from very low frequencies to extremely high frequencies. Each band has a defined upper and lower frequency limit. The countries can choose their own wireless spectra with ranges up to 300 GHz. This would help the organizations to specify the frequency ranges according to the purpose of using wireless networks and who uses them.

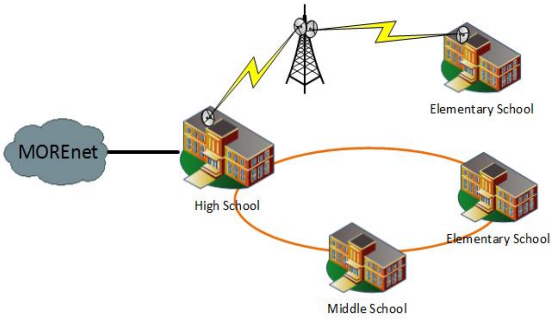
However, there are still a lot of challenges related with this extensive spectrum because of the short wavelengths. The current spectrum frequencies are lowered to be between 2-11 GHz band (including both licensed and license exempt spectra) and this will provide lower data rates and less expensively for more customers in their homes. (Crow, 1997)



To give an example about wireless local area networks we can see that they are implemented between offices in hospitals or inside companies. The previous figure shows that different topologies can be used to provide wireless local area networks.

e. Wireless Metropolitan Area Networks (WMAN)

This stander is defined by IEEE 802.16 and it provides data rate up to 100 Mbps using one single base station that connects to the modem and has the gateway address to the Internet. The WMAN covers area up to 10 Kilometers. It is called Worldwide Interoperability of Microwave Access (WiMax Standard).

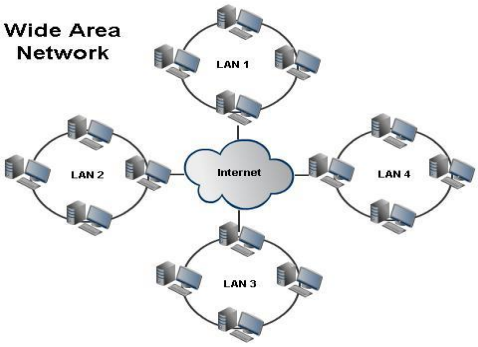


The wireless Man can be implemented between the different bank branches in a city or in a metropolitan area such as buildings inside universities.

f. Wireless Wide Area Networks (WWAN)

It is a developed type of the previous WiMax and it is defined by IEEE 802.16e. It adds mobility to the IEEE 802.16 and it is more accurate. Wide area networking (WAN) is about linking networks to allow wider file sharing or connectivity. Within organisations, this refers to linking multiple internal sites (typically geographically distributed), whilst, externally, the most common use is to allow connection to the Internet via an internet service provider (ISP).(reference WAN paper). The best example about the Wireless WAN is implemented wireless cables between cities and countries. (Seyedzadegan, 2013)

ISSN: 2663-5798



4. General Challenges in the Networks

Everything that human has created is not perfect even in the network area. Therefore, there are some limitations in the three technologies that we talked about previously (DSL, fiber optics, and wireless). In this part, we are going to talk about the limitations and the disadvantages of network. Moreover, we will discus the way that we could improve the fiber optics, and wireless.

Some limitations that IT people can face are speed because end users want to have fast network. Users feel bored when they need to wait until they get their data or send them. As a result, I visited two companies who provide the service of internet in Saudi Arabia to see the things that can affect on speed of transferring data.

When I visited a side of Saudi Telecommunication Company (STC) and Mobily Company, I talked to technical people as I talked to a manger in Mobily Company to see how they set up the fiber optics technology.

a. Limitations in DSL, fiber optics, and wireless

When people started to use DSL, fiber optic, and wireless as first time, these things

had some issues. Some of these problems has been solved while the others still in the focus of IT people. These technologies are not completely strong enough to get people's satisfied because they have some limitations. For example, DSL uses analog signal to send and receive data over cables. These signals do not travel as fast as fiber optics because fiber optics uses lightwave to communicate throw its cobles. When people started to use DSL, they thought it is the fastest way to communicate. However, fiber optics shows the different; fiber optics has the faster way to transfer data than DSL. From this example, we can see there is no limit for speed. As a result, the speed in fiber optics could be faster than what end users have now.

Data travels for a long distance and goes throw several steps. For example, user A want to send a massage to user B. The signal of this request goes out from user A's computer to his/her modem then the modem will change the digital signals to analog signals. This changing will take some times depending on user A's modem, and that cause slow down on the speed of user A's sending massage if user A does not have a good modem. Next, the analog signals move to the user

Optical Distribution Point (ODP). Inside the ODP there is a splitter which is a device that is used to spread the signal to number of users. The splitter has one input and many output that will be given to the end users. Figure 16 is showing the splitter that has one input in one side and many output in the other side.

Figure 16 splitter of fiber optics.

Therefore, Internet Service Provider (ISP) is used the splitter to give user A more connections in case there are more than one apartment or users in user A's home. After that, data will go out from ODP to another box which is Fiber Distribution Terminal (FDT) in the neighborhood of user A. Figure 17 shows the ODP of STC and presents the splitter that inside the ODP, and how it gives five connections from one cable.

Figure 17 STC's box for ODP and the splitter inside the box.

In the other side, there is an exchange that is linked to another exchange in deferent area or city using Optical Line Terminal (OLT). However, because ISP can't give ever user a cable from OLT; therefore, they use Optical Splitter Frame (OSF) in the exchange to give them more connections to spread them to the Optical Distribution Frame (ODF). Figure 18 is a picture for the OSF, and there are many fiber optics cables are coming out from it.

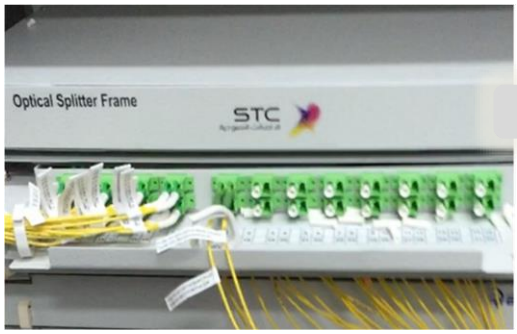


Figure 18 Optical Splitter Frame in exchange

ODF has patch panel to organize the cable output. Every group of cables goes to the FDT that is in the user A's neighborhood. The fiber optical cables that are coming from ODP in user A's home and the exchange are linked together in

ISSN: 2663-5798

the FDT. There are three levels in the FDT (Feeder/OLT, splitter, and ODF). Every single cable that is coming from the exchange is connected to level one which is the Feeder, and the Feeder can be consider as OLT in the exchange. The cable that is coming from the Feeder will be linked to the splitter to give us more connectors. Level three is ODF has the same function that ODF in the exchange has which is organize the output. Figure 19 is a picture for the FDT, and there are OLT in the first box down and ODF in the rest of boxes; however, in the medial, we have the splitters, and there are many cables come from them.

Figure 19 Fiber Distribution Terminal (FDT)

This was the first connection that end user can have, but there are two more links that ISPs in Saudi Arabia can serve for business companies, Institutions government, and end users. First connection is a link between FDT and user's modem directly; there is no splitter in ODP that divides the cable to many connections in user's home. Another line is between the exchange and user's home straightly; there is no ODP or FDT between the user and the exchange. Figure 20 shows the different between the three types of connections.

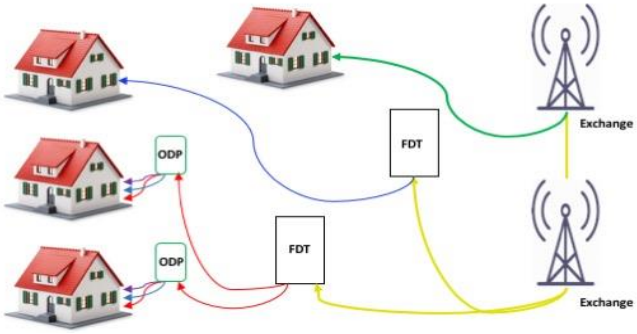


Figure 20 shows the different between the three types of connections.

The red line in Figure 20 describes the first connection that has three splitters, and the blue line is the link that has two splitters that is between the FDT and user's home. The last connection is the green line that is attached between the exchange and user's modem, and that has one splitter in the exchange. The different between the three connections is the power that is coming from the exchange. Every ISP has its own rang of power light, and STC has their own rang as same

as Mobily company has. The rang of power that STC uses 20 db to 25 db. If the power of fiber optics does not in this rang, there won't be connection, or the speed will be low.

As a result, we have two things that can affect on the speed of the network. The first one is a modem because the modem paly an important role in the speed of the network. It changes the signal that is sent over the network to analog signal and reverses it changes it back to digital signal when the modem receives data. Having the high quality of modem is necessary to get high speed of transmit data, and that will cause adding more money to have like this modem. A good modem starts with $100 to $400, and Figure 21 shows the Linksys modem that costs $309.98.

Figure 21 Linksys WRT1900ACS Dual-Band Smart Wi-Fi Gigabit Router.

Another thing that can cause slow down or disconnect to the network is the power of light. To measure the power, we use db unit, and the device that measures the power is called Optical Power Meter (OPM). Figure 22 optical power meter (OPM).

Figure 22 optical power meter (OPM).

There are some things can change or affect on the power of fiber optics. Bending the cable of fiber optics more than needed can cause loss power or db, or if there is a cut into the cable, that can lose connection to the network. Therefore, ISPs take care of fiber optics' cable carefully because any mistake in these cable can cause a problem to the end user.

When I visited Mobily company, they showed me how they fix and take care of these cables. If there is cut into the core that has the glasses of fiber optics, they use a special machine to fix this cut because it can't be done by human hands. This device called Fiber Optic Splicing Machine. But before splice the two ends of cores, they need to clean the cores because if there is a mistake in splicing or cleaning the core, that will cause lose of db. Figure 23 is a picture that has

the splicing machine, the OPM with the cleaning equipments, and fiber optics kit tools, and that shows the serious of taking care of this technology.

Figure 23 tools that are used to fix the fiber cable.

When I tried to fix the two ends of cores in Mobily company, I succeed; however, I have estimation loss 0.02 db which is misalignment of the two ends, air, or dust, and that considers as a good splicing. Figure 24 is showing my fifth attempt of splicing the two ends of cores and the result of splicing.

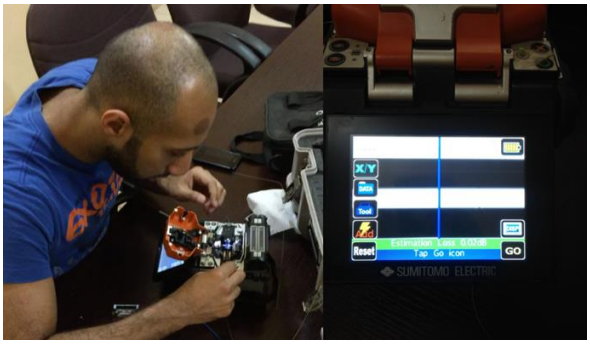


Figure 24 splicing the two ends of cores in Mobily Company.

Therefore, fiber optics cable is very sensitive and needs to trainers people to fix and take care of this cable.

After we got some information about DSL and fiber optics, there are some disadvantages in these technologies. In DSL, there are inconveniences of utilizing an advanced supporter line. One noteworthy weakness of DSL Internet is that most suppliers require that you utilize their modem. This makes it very expensive and badly designed on the off chance that you need to change to an alternate DSL supplier. Luckily, in any case, gear institutionalization will be a reality sooner rather than later.

Another detriment of a DSL association is that it is influenced by separation. The motivation behind why DSL is not accessible in all regions is that clients must be near the server or the system to have the capacity to appreciate a fast association. This causes constrained accessibility, particularly in under populated zones (At&t, The Basics of DSL Internet Service).

Fiber optics disadvantages are summarized in six points:

1. Fiber is costlier than copper link.
2. Interfacing filaments together ("joining") is more troublesome.
3. The mind boggling gadgets at both closures of the line has a tendency to be costlier.
4. Needs master skill to lay fiber and numerous installers are more acquainted with copper link.
5. Fiber can't convey power as it is made of glass. Copper link can convey both flag and power in the meantime.
6. Disappointment can be more cataclysmic than a copper link since you may have packed numerous administrations over a solitary link - they all come up short as a result of a solitary link disappointment (Teach-ICT, Fiber optic communication).

Moving to wireless technology, when we take a look to the places that are in cities or buildings, and these areas are needed to have access to the network, we have two choices to get the signal to the end user wire or wireless. However, sometimes, it is difficult to extend a cable to every place, or users want to have more flexibility to move around with their devices without setting in one place using the network. As a result, we have another choice which is wireless technology to get the signal easily to everywhere, but wireless has some disadvantages that can disrupt the end user.

a. It can require additional expenses and gear to set up, albeit progressively switches have worked in remote ability, as do gadgets, for example, portable workstations, handheld gadgets, present day DVD players, and TVs.

b. Setting up a remote system can once in a while be troublesome for individuals who are not experienced with PCs. (In spite of the fact that there are issues with setting up a wired system as well, off base!)

c. Document imparting exchange velocities are ordinarily slower to remote systems than they are with cabled. The velocities can likewise differ impressively as indicated by your area in connection to the system.

d. The general velocity of a remote connection is likewise normally much slower than a wired one. The connection additionally deteriorates the more distant you are from the router, which can be an issue in a huge building or space.

e. Remote connection can be impeded by regular family unit things and structures, for example, dividers, roofs, and furniture.

f. Remote systems are by and large less secure. There can likewise be issues with neighbors taking data transfer capacity, if the system hasn't been set up to be secret word secured. Data is additionally less secure as well and can be less demanding to hack into (Turbofuture, 2015).

b. Improving in Wireless and Fiber Optics

Improving and fixing the limitations and disadvantages in wireless and fiber optics are important because users want a better network in the future. Our world has been changed in many things, and network needs to be improved to keep up with the time for people needed. Users want to have high speed of transferring data with long distance in wireless and fiber optics, and that is possible with the limitations that the network has.

To improve the connection of wireless, we need to consider the disadvantages of wireless, and work on them. The distance between end user and router is most issue that can face many users. As a result, universities and big buildings set up many repeaters or routers to get the signal to end users in everywhere, and that of course consumes a lot of money and effort. Another thing that we could do is to use users' device to extend the signal of wireless. In iPhone devices, there is hotspot that shares signal with other users. Therefore, we could edit the algorithm of hotspot to make the user's device as a repeater and repeats the signal to other users, so more users use the network more distance the network will go.

Walls, ceilings, and buildings can prevent the signal of wireless to go through them. These things can decrease the distance of wireless significantly, or loss the signal of the wireless. Most routers can send signal in about 100 feet in all ways around the routers. As a result, users need to find a good place in the medial of building or house to put their routers. That will help to spread the signal around users' homes Figure 25 shows how the walls can affect on the wireless signal.

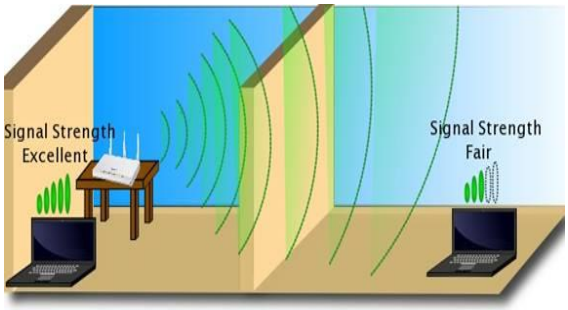


Figure 25 walls affects on the WiFi signal

Another thing that can help to improve the wireless signal is to clear the room from the electronic devices that have wave signals such as, microwave, wireless phones, cellphones, TVs because these devices will make the strength of signal poor (W. Rothman, Wi-Fi Versus Your Walls).

Fiber optics cables can be improved to be faster than what we have now. According to the article of Maddie Stone, "*engineers just broke the capacity limit for fiber optic transmission*". Because the laser of fiber optics won't be able to transfer data if there is a lot of boost of light power. The signal will turn out to be distorted to the point that it can't be decoded at the flip side (Maddie Stone, 2015).

Nikola Alic of the Qualcomm Institute has a nice explanation for this issue. He said "*Today's fiber optic systems are a little like quicksand. With quicksand, the more you struggle, the faster you sink. With fiber optics, after a certain point, the more power you add to the signal, the more distortion you get, in effect preventing a longer reach."* Then he added *"Our approach removes this power limit, which in turn extends how far signals can travel in optical fiber without needing a repeater."*

c. Security Weaknesses

While the wireless networks are preferred than the wired networks, there still are some challenges in the current wireless networks which are listed bellow:

A. Security- it is difficult to secure the wireless networks because the access to the network is not limited and it can be from any place in the world. On the other hand, the wired networks are more secured because the access to the network is controlled easily and it can be physically secured. However, there are some security's solutions that may reduce the performance and increase the cost of the networks such as the encryption techniques.

B. Frequency Allocation- the government should allocate and manage the frequency bands for different users by approving and licensing them. However, operating the wireless network frequency bands will be a time consuming process due to the high demand for available radio frequency spectrum.

C. Figure 26 shows an example of the frequency allocations in United States.

D. Power Consumption- the wireless devices, are meant to be portable and/or mobile, and are typically battery powered. Therefore, devices must be designed to be very energy efficient, resulting in "sleep" modes and low-power displays, causing users to make cost versus performance and cost versus capability trade-off (Crow, 1997)

E. Reliability- the collisions can be happened between two frequencies when two sources started their data transmission at the same time. Collisions are also can be caused when a station send data in a busy channel by mistake because it appeared that the channel is idle to transfer data.

ISSN: 2663-5798

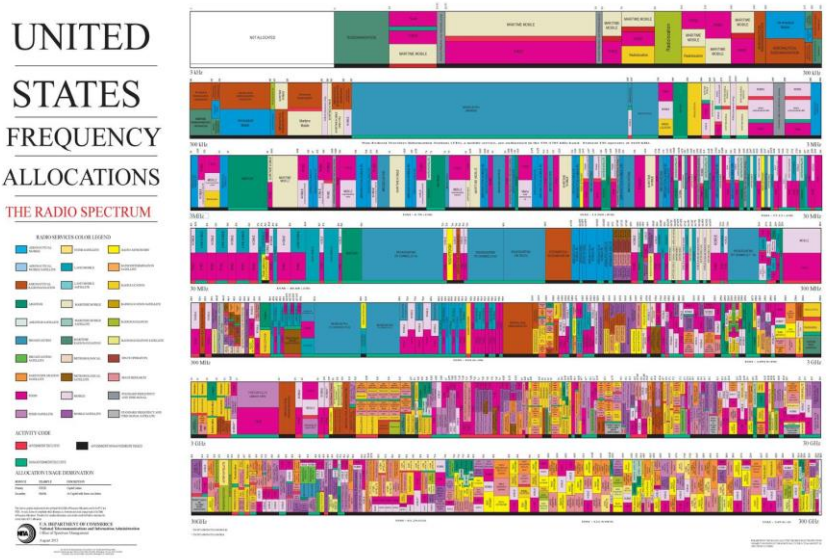


Figure 26 United States Frequency Allocations.

d. Security Weaknesses in DSL

The weaknesses of the networks usually are related to the speed, the security. As ever before, all technologies have been subject security problems the DSL, fiber optics and wireless networks have no exchange.

Do you have a "Always on" Internet connection? It's anything but difficult to imagine that nobody could be occupied with your PC, yet that is essentially not the situation. Having a quick Internet association that is "Always on" when you need to surf the Web is incredible for you, but on the other hand it's extraordinary for programmers from around the globe who clear through a large number of irregular IP addresses searching for PCs that they can misuse. What's more, what they can do is truly very startling. With no noticeable sign or cautioning, programmers can penetrate your framework to get individual data about you or to utilize your PC to camouflage themselves when they assault different PCs.

It has always been assumed that the ability of DSL users to stay logged in for as long as they want to be a convenience. However, it is the same feature that leads to one of the biggest security flaws of DSL. The first thing that should be taken into consideration is the “law of averages”. The “law of averages” is the law that simply implies that if someone stays online for a long period of time, then they increase the likeliness of being attacked. This is an assertion that cannot be disputed. Security risks are always minimal when a person is not connected to the internet. This is basically because when someone is offline then there is no way through which hackers can reach their computers and devices, and access the content without permission. At the end of the day it will be seen that a person offline will have the security that a person online does not have. (Amin, 2012)

Apart from the “law of averages”, it should be noted that if someone is logged in for as long period of time continuously then they will be using the same IP address for the whole period. An IP address is a network address accorded to any device that accesses the internet. When the IP address is static attackers have the privilege of a fixed address. This is a risk that is based on the common knowledge that a moving target will generally be harder to hit as compared to a target that is stationary. Many DSL providers offer DHCP address assignment that makes sure that users get new IP addresses every time they login. This is a feature that helps users in changing the address that is meaning that they are not constant subjects. This is an implication that they would have reduced the possibility of falling prey to online attackers. (Mohan, 2011)

Another weakness can be as a result of the bugs that are sometimes found in the DSL routers. Many computer users usually go a long way in making sure that their computers are secured from various vulnerabilities. However, such people usually forget about the vulnerability of the DSL routers that they use. There are a number of cases where DSL routers have been discovered to have bugs that online attackers can easily take advantage of in their endeavors. In such cases it will be discovered that online users will assume that they are on legitimate sites or platforms while in real sense they are not on the platforms of sites. This might lead to a scenario where a DSL network user is left vulnerable for a very long period of time without them noticing that they are actually being exploited because they assume that they are on a legitimate website.

e. Improving Security in DSL

One of the ways through which a DSL user might enhance security is through reduction of the period when the computer being used for connection to the internet is actually physically connected to the internet. This would involve actions such as shutting down the computer or unplugging the interknitted connection whenever one does not need to use the internet but need to use the computer. If a person makes sure that their computer is shut down when they are not using them, then it implies that the period when they are not using them they will not be facing any security risks because they will be unavailable to the online attackers. The same applies to unplugging the internet connection because it will be a way through which the computer can be inaccessible online even when the computer is actually on. It should be noted that both shutting down and unplugging of the internet connection is advantageous because every time the user goes online again they will be accorded a new IP address. With regard to the allocation of a new IP address it should be noted that even simply logging off without unplugging or shutting down the computer has the same effect. Moreover, it is recommended to turn sharing off on all your devices and printers. You have to set a password on your devices that is connecting with LAN.

There are some computer settings that can also minimize the vulnerability when connected to the internet through DSL. There are a number of windows settings that have proved to be of some degree of importance in protecting computers from network attacks. A good example of such settings is the firewall activation.

It is usually recommendable for computer users, especially those who access the internet through DSL to make sure that they have up-to-date security fixes for their programs and operating systems. This is a way through which they can always make sure that they have the latest versions of their programs and operating systems. It should be noted that when using the latest versions of programs and operating systems there is always less vulnerability as compared to the previous versions.

Given the fact that some routers have been observed to have bug and other forms of vulnerability, it is important to make sure that for any DSL user, the type of router that is bought is one that has been approved to be free of bugs and vulnerabilities. This is a way through which DSL users can make sure that they are not attacked curtsy of the type of router that they are using.

f. Security Weaknesses in Fiber Optics

According to some networking engineers, insecurity of using fiber optic for internet connectivity comes from the fact that tapping of fiber optics is possible. It has been observed that the best places that attackers can be able to tap fiber optics are at the repeater stations. The repeaters stations refer to the junction boxes where splicing of the cables take place. The splicing makes the junction boxes the most appropriate places for such activities to take place. As a result, it will be seen that the information going through the fiber optic can be easily accessed by unauthorized persons. Initially, people had the opinion that tapping of fiber optic would be an impossibility given the fact that most of it is undersea. However, the little that is not under the seas brings the vulnerability to the use of fiber optic to connect to the internet.

Splicing a fiber optic cable is another usual way that is used globally to recover the fiber optic cable from scratching and to extend the length of the fiber optic cables. It is also a common practice where people tend to bend the cable in a manner that enough light can be extracted so as stealing of data is possible. The little cylindrical devices that are used for this purpose can be easily found on e-bay at a price of $100. The cable is then run round the cylindrical device resulting to a slight bending of the cable. The bending leads to light emission that might amount to 2 or 1 decibels. The emitted light can be fed into a receiver, and then later turned into data. What makes this method effective for data stealing is the fact that it does not interfere with the data transfer flow. This is an implication that an attacker will be able to read everything going through the optical fiber without anyone noticing that they are doing so. Even if someone notices the loss, it is usually so small that many people are likely to assume that it is as a result of loss of connection along the line. The data that will have been accessed or stolen as a result might be used in various ways in illegal activities.

There are many different ways to interrupt the data in the fiber optics cables. Intruders who want to interrupt the connection can get access to the fiber optic cables using simple stuff such as the fiber tapping machine, packet sniffer software such as Wireshark software optical/ electrical converter and a laptop, Figure 27 shows the Fiber Tapping Machine.

Figure 27 Optical Fiber Tapping.

Furthermore, it has been noted that tapping of optic fiber under the sea is also a possibility. This is a factor that is supported by the evidence that emerged after evidence supporting the speculation that the NSA has been tapping data that is being transmitted through the optic fiber. What makes matters even worse is the fact that the illegal access of information and data going through optic fiber can be done with the use of equipment that can be legally accessed from various parts of the world. This means that there is a high level of vulnerability of data that is shared by optical fibers that many people might not be able to realize because of the nature of the process that leads to the illegal access of information form the optical fiber network.

In the years 2003 was discovered that optical fibers were also vulnerable to eavesdropping. This is an assertion

that resulted from the discovery that was made by security forces in the United States of America in the same year. An illegally installed optic fiber eavesdropping device had been discovered on an optical fiber network in Verizon. This in an indication that technology has surpassed the perceived security of fiber optic as technology has availed devices that can breach the security measure that have been put in place without being noticed.

A simple scenario for this security problem could comes as following:

If someone send a confidential information throw unencrypted email, and the data will pass via the server and throw the optical fiber. The intruder can cut the protective coating to expose the bare optical fiber and a simple tap is attached, the transferred information can be downloaded easily and freely and the key words will be visible and clear. Less than 1% of light, gives 100% of the transferred data.mproving Security in Fiber Optics

The security in fiber optic can be enhanced through a number of ways. For instance, given the fact that the junction boxes have been identified to be a weak-link, it is only advisable for the relevant parties to make sure that the security around the junction boxes is enhanced. This would be a way through which the involved parties would be able to make sure that the junction boxes are less exposed to security threats. There are a number of ways through which this can be achieved. One of the ways through which this can be achieved is through making sure that physical security around the places where junction boxes are placed is enhanced.

Research has also revealed that the security of fiber optic can be enhanced through running a continuous strand of fiber. This is a discovery that is supported by the fact that running continuous strands of fiber optics will imply that there are reductions of the number of junction boxes that are needed for the network. Given the fact that the junction boxes are sued as illegal data access point, their reduction will imply that there will be a reduction of the channels through which illegal access of data that is carried in the optical fiber can take place. (Mohan, 2011)

There should also be the introduction of technologies that can ensure that attackers have a hard time when trying to illegally access information on the optical fiber. A technology such as OTDR can be effective for continuous monitoring of activities that take place in the physical space. The technology will also be effective in intrusion shut down. This can also be made better if there is an introduction of automatic re-routing traffic to an alternative fiber path whenever there is any detection or suspense that there is an unauthorized access to a given optic fiber path. Moreover, there are another professional ways to secure the fiber optics transactions such as:

A. The encryption method:

Encrypting the transmitted data is very helpful way to secure the transaction. The end user can also use a physical method that changes the light signal to avoid the attacks.

B. Foptic Secure Link:

A new technology developed by the Australian Firm Future of Fiber Technologies. This technology is used for sensing the physical disturbance of light. It uses a technology that can concurrently make use of a fiber optic communications cable as a tampering-alert, intrusion-alert, or integrity-testing sensing cable. It monitors in real-time any physical disturbances, such as clamping or bending. One key advantage to using this technique is that it is not necessary for optical losses to occur in order for the technique to sense disturbances.

C. Using photons to encrypt data:

A transmitter sends photons that are specifically directed at given intervals through a fiber optic cable. The receiver then analyzes the arrival of the photons at the given intervals. When a matching segment of the transmission pattern, which is

advertised on a separate wavelength by a transmitter, is received, the receiver will then utilize this "key" and authenticate the unlocking of the data from the stream. The light beam passage is so weak that any alteration would be immediately observed; any intruder snooping or injecting would inevitably disturb the photons pattern. The receiver's device would detect the change in pattern, ending the transmission and sounding the alarm. The article goes on to mention that since the signals are weak, the range is about 60 miles and this method would require its own freestanding fiber optic network. (Witcher, 2005)

D. WaveSense intrusion prevention technology:

This technology is used by Opterna's FiberSentinel System. It is used to monitor the fiber connections and it reportedly detects all physical intrusions immediately cancels all transmissions by using the artificial intelligence and optical digital signature recognition. At the time of intrusion detection this continuous real time monitoring system will switch the data transmission to an alternate fiber path and alerts the network operator.

E. Oyster Optics, Inc. reports that it has developed an optical security, monitoring, intrusion detection solution that is protocol independent. The system uses a secure phase modulation of the optical signal to impress data on the optical carrier. If data is intercepted, the intruder will not be able to gain access to captured data unless they happen to have a receiver provided by Oyster Optics' that is synchronized to the transmitter at power up. Oyster Optics' provides a unique transmitter and receiver by using a non-pseudo-random manufacturing process that cannot be replicated. This system will also reroute data transmissions to a backup system when an intrusion is detected. There solutions can be implemented as a stand-alone device or at the transceiver card level. (Witcher, 2005)

g. Security Weaknesses in Wireless

One of the security threats that face wireless networks is hidden rogue APs. hidden rogue APs can effectively offer attackers a privilege that can be equal to a RJ45 jack in the parking lot. This is a factor that makes it easier to attack systems that are connected to wireless networks. Technologies such as Bluetooth have been highly appreciated by consumers of information technology products and services. However, Bluetooth is the root for wireless network security threats. However, attackers have also taken advantage of the situation and have been able to identify security vulnerabilities of Bluetooth technologies and have highly taken advantage of the same. Bluetooth attacks always lead to crimes such as unauthorized access of information, disclosure of personal and secret information, manipulation of communication devices, and eavesdropping. This leads to a situation whereby many users of wireless networks end up losing or sharing their personal, secret, and important information to people that they would not have wanted to share the information with. What makes this worse is the fact that the loss of information in wireless networks through Bluetooth is hardly detectable. Most people would go on with their activities as if nothing was wrong.

Mobile devices such as PDAs and smartphones have also been observed to have multiple weaknesses. One thing about these devices is that they need wireless connectivity in order to function. In most cases it is asserted that that the embedded platforms in these devices are the reason for some of the security risks that are associated to the use of wireless networks. This is an assertion that is supported by the fact that the operating systems in these devices do not get regular patch updates for the flaws that some of the applications might have. In most cases it is observed that organizations and individuals are incapable of upgrading the applications and operating systems that come with the mobile devices because the patches will have to be certified by the application vendors before the upgrade takes place. This means that these devices are left vulnerable to attack for a majority of the time they are used.

There are some attacks that are executed through wireless networks that do not target the devices themselves, but the wireless drivers. This is a weakness that does not affect just a single wireless card producer, but a weakness that has been observed to affect most of the major wireless producers.

h. Improving Security in Wireless

One of the ways through which the security of wireless networks can be enhanced is through frequently changing the proxies and passwords. This is an action that can ensure that even when such details get to the wrong hands, they will not be able to use them for long. This is an implication that the network will not remain vulnerable for a long period of time.

It has also been commonly advised that wireless network managers or organizations using the same should make sure that they avoid the use of common Service Set Identification (SSID). However, this method is argued to be ineffective in stopping competent hackers from accessing wireless networks.

Most organizations have opted for wireless routers that have the ability of showing the number of devices that are connected to a wireless network at a given time. The most recent devices have the ability of giving more detailed information, including the type of device that is connected to the network apart from being able to show the IP address, the hostname, and the MAC address. These routers have the ability of giving an alert whenever a new device is connected. The end result is a situation where the network managers will be able to notice whenever there is any activity that is out of normal or suspicious. This is a way through which suspicious activities within a wireless network can be responded to before the damage is done. (STUART McCLURE, 2001)

Some organization has taken disallowing admin access from wireless network as a way through which insecurity that involves using wireless networks can be minimized. However, it should not be assumed that this is a mover that can be able to completely keep hackers away. Nevertheless, it is still important given the fact that it makes it hard for hackers to access an organization's system. The fact that hackers are becoming harder to inhibit everyday does not mean that people should make their work easier by creating an environment whereby hackers will have no obstacle in achieving their goals. (Westhoff, 2006)

Turning the network name broadcasting off, especially for cases where private networks are involved because it hides some of the identity details of the network from the public. This is a step that gets a wireless network closer to being safe from hacker and other unscrupulous people.

5. Case study: The Public Networks

This network is usually user designed and uses principles which are not technically related. The public network has no security placed into it. This makes it vulnerable to threats occurring on the internet. In terms of addressing issues and authentication of the system the public network is different from the private network in a very big way. The hardware and the infrastructure used in creating the system is similar to the one which is used in the creation of the private networks. Its design is very simple to create. Since the network is very open to individuals various security protocols need to be implemented to counter threats and the malicious activities taking place in this network type. Various individuals try to use that advantage of the openness of the network by infiltrating the systems of users who are not keen about the system. This network has been used by hackers in most coffee shops to steal information from top executives in many organizations.

a. Weaknesses in the public networks

A public network is a network which can be used by anyone to connect to the internet or to any other network. This is contrasted to the private network whereby there are restrictions of access to this type of network. The public networks can be accessed by all but the private network are limited to a selected few in the society since it's locked through passwords. Since the public networks are usually open, the users of this network need to be keen when using this type of network since it might provide security threats which cannot be easily eliminated.

The coverage of a network refers to the distance which a network covers. The extent to which the network covers depends on its strength and the type of router used in offering the public networks. The coverage of this network is usually limited. This network can cover a few feet only from the source it's been offered. Most of these cover 30 feet from the original router where the network is being provided. This limits a lot of people from accessing this network since the more the distance from the main router, the lower the strength of the network. A person seated outside a coffee shop won't be able to access the network, especially in times when the shops are full of clients. (Rubalcaba, 2013)

Reliability of a network refers to how the network is resourceful to its clients. The public network should be made reliable to make it accessible to everyone without problems. This network cannot be reliable since many users try to maximize on its usage. This makes this type of network weak. When there are many users logged on to this network, many of the connectors suffer from the low connections. This can cause booting off from the network which is a serious problem especially when you are working on important documents and information. Booting off of the network makes many people not to trust the network since all clients like working with a reliable network system which enables them to browse effectively and non-stop.

This network makes many phones or devices to use a lot of power as compared to connections which are standard wired. This causes a lot of power losses in the devices which might be a disadvantage to the users if they want to use their devices and the network for long. Whatever causes this network to use a lot of power for the machines and the user phones is the fact that most of the Wi-Fi connections need a lot of processing by the machines used or phones therefore the power is consumed at a high rate. Another weakness of this system is that it is majorly used by major companies to advice their products or services. Most of these ads are fake and a few others are legitimate. The fake ones can cause a threat to the security of your device when they are accessed. Many hackers use these ads to send viruses to most devices owned by the users of the network. This is one of the most occurring weaknesses of this kind of a network system.

The network is not encrypted, which makes it unsafe as compared to the hard wired connections. This makes it easy for hackers to access passwords to social networks of the users easily. This makes it easy to leak important information of the users easily to the various networks. The unencrypted network makes it easy for many users of the network to lose trust in the network because a lot of important data is lost through the malicious hackers in most of these public network spots.

b. Speed limitation

There are many users who are subscribed to using the public networks. This makes the speed of transfer of information or data very slowly. The bandwidth of the network is usually slowed down as many users subscribe to this kind of network. Many users also use this network system to spread viruses to many devices which makes it possible to slow the bandwidth of this network and also causing a lot of risks to the users of this network.

c. Security limitation

This network is tailored to be used by many users at the same time. This makes many users who want to do harm to your device take advantage of this network to spread viruses to the various users subscribed to this network. When the firewalls to the public networks are not properly set, this can cause leaking of different passwords and bank account information of the various users of this system. Not only this information, also are the folders which are shared through this kind of network easily accessible and easy to hack.

d. Improving the public networks

In making sure that you do not run out of battery due to the usage of this network, the users of this network are advised to have a backup battery in order to increase the length of accessing this kind of network. Apart from the back up batteries, the users of this network are advised to have a power banks which enables automatic charging of the phones used very fast and efficiently. Most of the coffee shops also have the charging booths whereby the users of this network are allowed to charge their devices at a very affordable price. Charging the devices can take only 10 minutes.

The users of this network should make sure that they have the best software's which will enable them to protect their devices against the malicious attacks. Viruses send by hackers and the hackers themselves may not be easy to prevent but having the appropriate software to protect the machine can make the information stored in your machine inaccessible to the general public. The Software's which can be used in carrying out this activity include 'web root secures anywhere' software and 'SOS online backup' which automatically back-up your files to a secure cloud.

e. Improving speed in public networks

The speed in the access of public Wi-Fi can be amplified through the use of a high end, high performance router which enables the machine to be efficient in terms of downloads at higher megabytes per second. This can also improve the performance of this network with little hanging. To get good routers which can provide high performance public networks needs one to be keen in the selection. Refurbished routers can cut down the cost of buying and also this kind of routers can be from the best brands at a lower cost. Speed of a public network is very important to the users because it makes the public networks very efficient to the users. This makes it very reliable in using by the users.

f. Improving the security in public networks

The security of a public network access can be improved by owning a very safe anti-malware and firewall protection software's. To prevent hackers from accessing the information on your computer and keeping the computer in top conditions, there are software's which are availed to different users which enable protection from viruses which cause harm to the users of the public networks. A good option which can be used is the 'bit defender total security' which has the features of antitheft which help in keeping the identity of the users of the public networks very safe from malicious attacks. Most of the antivirus software's also provide security against malicious attacks which makes them also very important to be used in curbing security threats to the system.

Apart from the software's present in the internet, there are other security options which can be used by many users in making sure that the devices are well protected against malicious attacks. This include blocking of installation of new software's in the devices without authorization of the user. This makes it very easy for the users to decide which software to install and which to reject. Also with the computers, it has options in the window firewalls which protects the machines also from malicious attacks from the hackers. Updating it makes the computer not to be vulnerable with the malicious attacks by the hackers.

g. Study the network environment at King Saud University (KSU):

King Saud University is in Jeddah, Saudi Arabia. It is just for Health of science, nursing,

and medicine. It has around 7000 students and around 450 staffs. To give a good connection to the network for all students and staffs, there should be high speed of internet and great quality of equipment.

Looking to the network that IT department has approved, there is a MDF room in each building and one or two rooms of BDF in each floor. These two rooms are connected together by using fiber optics cable. Into BDF room, there is many switches which are linked together, and these rooms are secured with access card and key as same as MDF rooms. There are many cables that are connected between users' computers and wireless devices to the switches. These cables are twisted pair cables, and they are organized very well to the patch panel to easily identify which cable is linked to which computer; however, transferring many users' data from BDF to MDF needs to have high speed, and fiber optics is the best choose in this cause. After that, there is another connection between data center to all MDF rooms, and the link that is used to connect data center to MDF is fiber optics as well. In data center, there are the all servers and firewalls, and the only way for users to go to the WAN is through data center.

IT department at KSU gives the priority for accessing to the network to KSU's staffs because they want to get the employees high performance to use the internet. As a result, there is a limit of IPs that can be signed to students who want to have access to the network. IT department has configured their routers by selected a range of subnet to allow certain students to use the Internet. That shows large number of users can affect on the speed of network.

F. Conclusion

Communication over the network is something that has old history. Although, people have more than one kind of connection to the network such as DSL, fiber optics, and wireless, they are looking for high quality of transmitting data. The latest technology of network is fiber optics, but it still has some limitation.

The public network is easily accessible to many people and its easier accessibility makes people to use it more often. This network has attracted many people which have made the hackers easily access information from which enables most individuals using this system vulnerable. However, there are various solutions which can be used in solving these threats in the public networks. These solutions can be easily integrated into the computers of people carrying important information of different firms. The public networks or Wi-Fi will then be safe to access by different users if these security protocols are implemented.

G. Reference:

Meyers Mike. (2012). Comp TIA Network+ Exam N10-005. pp. 55-465 print.

P. Sparrow. (2011). Bas Topology: advantages and disadvantages. From http://www.ianswer4u.com/2011/05/bus-topology-advantages-and.html#axzz4F3fz7UgS.

P.Sparrow. (2011). Wireless Network Design. From

http://www.ianswer4u.com/2011/05/mesh-topology-advantages-and.html#axzz4BXbRxWmF.

P.Sparrow. (2012). Tree Topology: advantages and disadvantages. From

http://www.ianswer4u.com/2012/01/tree-topology-advantages-and.html#axzz4F3fz7UgS.

Oak Manali. (2014). Type of Network Topologies. From http://www.buzzle.com/articles/types-of-network-topologies.html.

Oak Manali. (2016). Advantages and Disadvantages of Different Network Topologies. From http://www.buzzle.com/articles/advantages-and-disadvantages-of-different-network-topologies.html.

TechopediA. Point-to-Multipoint Communication. From https://www.techopedia.com/definition/26762/point-to-multipoint-communication-pmp.

TechopediA. Tree Topology. From

https://www.techopedia.com/definition/24206/tree-topology.

Ukessays. (2015). History of The Bus Topology Information Technology Essay. From

https://www.ukessays.com/essays/information-technology/history-of-the-bus-topology-information-technology-essay.php.

Edraw. Network Topology Diagrams. From https://www.edrawsoft.com/Network-Topologies.php.

Tech Target. (2006). Star Network. From http://searchnetworking.techtarget.com/definition/star-network.

One UK Ltd. Point to multipoint communication. From http://www.one-uk.net/one-wireless-solutions/point-to-multipoint/.

Brain Bell. Wireless topology. From http://www.brainbell.com/tutorials/Networking/Infrastructure_Wireless_Topology.html.

S. Toumpis, D. Toumpakaris. (2006). Wireless ad hoc networks and related topologies: applications and research challenges. Vol. 123. Pp. 232-241. From http://link.springer.com/article/10.1007/s00502-006-0348-9.

Timbercon. History of fiber optics. From http://www.timbercon.com/history-of-fiber-optics/.

Meridian Technologies. (2008). Multimode vs. Singlemode – Fiber Fundamentals. From http://www.meridian-tech.com/downloads/articles/Fiber%20Fundamentals%20(MM%20vs.%20SM).pdf.

At&t. The basics of DSL internet service. From http://www.att-services.net/att-internet-resources/digital-subscriber-line.html.

Teach-ICT. Fiber optic communication. From

http://www.teach-ict.com/as_a2_ict_new/ocr/A2_G063/333_networks_coms/optical_wireless/miniweb/pg3.htm.

Turbofuture. (2015). Wireless Network vs Wired Network: Advantages and Disadvantages. From https://turbofuture.com/computers/Wireless-Network-vs-Wired-Network-Advantages-and-Disadvantages.

Maddie Stone. (2015). Engineers Just Broke the Capacity Limit for Fiber Optic Transmission. From http://gizmodo.com/engineers-just-broke-the-capacity-limit-for-fiber-optic-1714070706.

W. Rothman. Wi-Fi Versus Your Walls. From http://www.thisoldhouse.com/toh/article/0,,1094325,00.html

Allied Telesis. (2007). DSL White paper. From http://www.alliedtelesis.com/media/pdf/dsl_wp.pdf.

Knowledge Systems Institute Graduate School of Computer and Information Sciences. Lesson3: Network Topology. From http://pluto.ksi.edu/~cyh/cis370/ebook/ch01d.htm.

Crow, B. Fujitsu, I. Kim, J. Sakai, P. 1997. "IEEE 802.11 wireless local area networks. " *Communications Magazine, IEEE*, vol. 35, no. 9, pp. 116-126.

Kumbhare, Y. Rangaree, P. 2015. "Patient Health Monitoring Using Wireless Body Area Sensor Network. " *International Journal of Engineering and Advanced Technology.* vol. 4, no. 3,

Park. 2007. "Short-range wireless communications for next-generation networks: UWB, 60 GHz millimeter-wave WPAN, and ZigBee. " *Wireless Communications, IEEE.* vol. 14, no. 4, pp. 70-78

Seyedzadegan, M. Othman, M. 2013. "IEEE 802.16: WiMAX Overview. WiMAX Architecture. " *International Journal of Computer Theory and Engineering*, vol. 5, no. 5, p. 784.

Amin, S. 2012 . "Smart grid—Safe, secure, self-healing. " *IEEE Power Energy Mag*, vol. 10, no. 1, pp. 33-40.

Mohan. 2011. "A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment,".

Witcher, K. 2005 ."Fiber Optics and Its Security Vulnerabilities. " *University MARY Washington.*

K. STUART McCLURE. 2001. Hacking Exposed: Network Security Secrets and Solutions, Third Edition, Corel VENTURA™ Publisher.

A. Westhoff. 2006. "Security solutions for wireless sensor networks," *NEC Journal of Advanced Technology*, vol. 59, no. 2.

L. Rubalcaba. 2013. Public\Private Innovation Networks in Services, Edward Elgar Publishing.