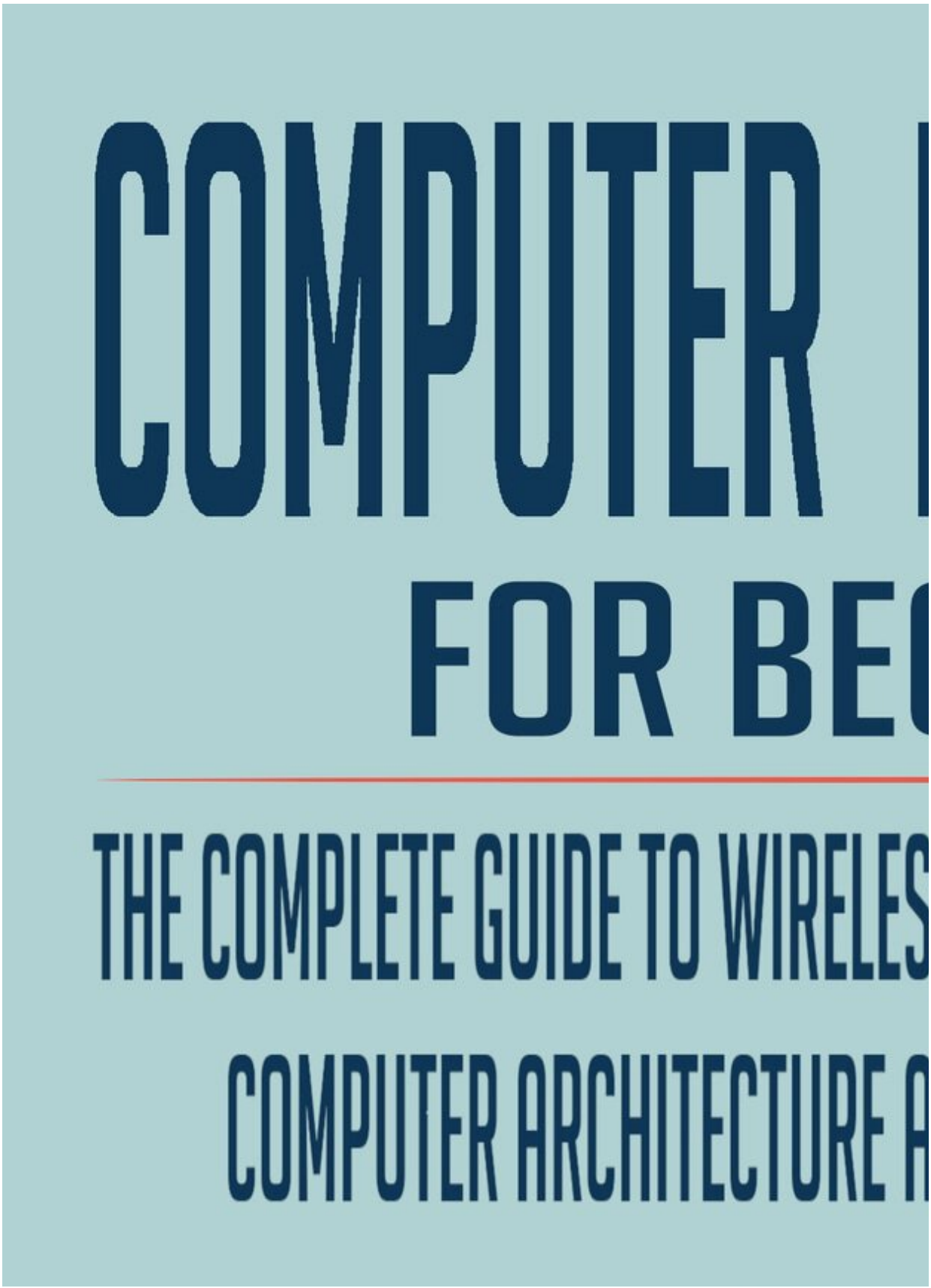
COMPUTER NETWORKING

FOR BEGINNERS

THE COMPLETE GUIDE TO WIRELESS TECHNOLOGY, NETWORK SECURITY COMPUTER ARCHITECTURE AND COMMUNICATIONS SYSTEMS

DR. JOHN HUSH


COMPUTER
FOR BE
THE COMPLETE GUIDE TO WIRELES
COMPUTER ARCHITECTURE A

COMPUTER NETWORKING FOR BEGINNERS

THE COMPLETE GUIDE TO WIRELESS TECHNOLOGY, NETWORK SECURITY, COMPUTER ARCHITECTURE AND COMMUNICATIONS SYSTEMS.

[Dr. John Hush]

Legal & Disclaimer

The information contained in this book and its contents is not designed to replace or take the place of any form of medical or professional advice; and is not meant to replace the need for independent medical, financial, legal or other professional advice or services, as may be required. The content and information in this book has been provided for educational and entertainment purposes only.

The content and information contained in this book has been compiled from sources deemed reliable, and it is accurate to the best of the Author's knowledge, information and belief. However, the Author cannot guarantee its accuracy and validity and cannot be held liable for any errors and/or omissions. Further, changes are periodically made to this book as and when needed. Where appropriate and/or necessary, you must consult a professional (including but not limited to your doctor, attorney, financial advisor or such other professional advisor) before using any of the suggested remedies, techniques, or information in this book.

Upon using the contents and information contained in this book, you agree to hold harmless the Author from and against any damages, costs, and expenses, including any legal fees potentially resulting from the application of any of the information provided by this book. This disclaimer applies to any loss, damages or injury caused by the use and application, whether directly or indirectly, of any advice or information presented, whether for breach of contract, tort, negligence, personal injury, criminal intent, or under any other cause of action.

You agree to accept all risks of using the information presented inside this book.

You agree that by continuing to read this book, where appropriate and/or necessary, you shall consult a professional (including but not limited to your doctor, attorney, or financial advisor or such other advisor as needed)

before using any of the suggested remedies, techniques, or information in this book.

Table of Contents

INTRODUCTION

A computer network is a physical and virtual connection that allows you to share resources both locally and remotely. The connection to a network can be wired or wireless. Wireless transmission takes place over radio waves. Wireless technologies exist in various forms such as infrared technology used in home electronic remote controllers, Bluetooth connection, cordless keyboard, and cellular phones. A wireless network concerns a digital network that connects nodes locally or remotely through infrared, radio waves and microwave technologies to share resources.

Benefits of Wireless Communication

- Reachability: With wireless communication systems, individuals can stay connected and reachable irrespective of your geographical location as long as the area is covered by the wireless signal. Think of cellphones and hotspots.
- Mobility: Through the wireless communications system, individuals can access information beyond their current location without the need for a wired connection.
- Maintainability: The relative cost and time spent to maintain a wireless network system are less compared to wired setup in most cases.
- Simplicity: It is easy and fast to activate wireless communication system compared to a wired network even though the initial setup cost can be high.
- New services: Short message service and multimedia service are some of the smart services that can be deployed on wireless communication systems.
- Roaming services: Through wireless connections, you can offer services anywhere making wireless highly flexible.

We are in the internet age, and therefore, ignorance is not an option. This book enlightens you on the basis that you should know about computer networking.

CHAPTER 1: INTRODUCTION TO WIRELESS TECHNOLOGY

WHAT IS WIRELESS TECHNOLOGY?

Wireless technology is the process of sending information through invisible waves in the air. Data, voice, and video are carried through the radiofrequency.

WHAT ARE WIRELESS DEVICES?

A growing number of devices are also getting the wireless tag. The term, “wireless devices” covers a long list of devices that work without cords or cables. These devices can be used without any physical connection to an object or powered by a cable to be useful. Such devices are collectively taking advantage of the wireless technology concept for operation.

EXAMPLES OF WIRELESS DEVICES

Wherever you turn in the world today, you see wireless devices at work. They can be found in different sectors and are available to perform different functions, ranging from domestic use to industrial use. Some typical examples of wireless devices are TV remote controls, cordless phones, GPS systems, radios, and other devices that will soon hit the shelves as wireless technology is taken to a new height by inventors. Other examples of these devices are wireless mice, PDAs, wireless routers, wireless keyboards, wireless network cards, and any other device that doesn’t depend on the use of physical wire to transmit information. Let me give you a list of some of the most important wireless devices and their functions. These are:

Wireless router

A wireless router is used for accepting incoming Internet connections. It also sends some data in the form of radiofrequency (RF) signals to some

other wireless devices within the proximity of the router. Wireless routers have a wide range of applications. They are used in different devices for an array of uses, such as connecting wireless-enabled computers and other related devices to the Internet. Any network that is set up with a wireless computer is also known as a wireless local area network (WLAN). Many of these routers have some important built-in security features that offer the devices that are connected to the router maximum protection against computer viruses and other malicious attacks.

Wireless adapters

Wireless adapters are hardware devices that are installed in computers to create room for wireless connectivity. Without a wireless adapter, connecting to a router to enable connectivity to the Internet is impossible. Some modern computers come equipped with built-in adapters into their motherboards. You can also physically install wireless adapters to your computer to enable you to activate its wireless capability, especially if the computer doesn’t have a built-in adapter.

Wireless repeater

A wireless repeater is also a wireless networking device used for extending the range of reach of a router. When a repeater receives signals, it amplifies the signals and remits them. When you place a repeater between the computer that is connected to a router and the router, the signal strength will receive a major boost that will automatically result in increased connection speeds. This is a big plus for Internet users as they can enjoy the luxury of using the Internet at an impressive speed with outstanding benefits, such as judicious use of time and fast access to resources over the Internet.

Wireless phones

In the past, phones were connected with cables to enable users to communicate over the phone. However, wireless phones are gradually replacing wired phones. Unlike their predecessors, wireless phones use wireless technology for operation. In this category are cordless and cellular phones. These two are also built on wireless signals and are a deviation from the former phones that used wires for a physical connection before they can be used. Cordless phones are known for their limited range of operation. On the other hand, cell phones boast a larger range than the readily available local wireless networks. The larger range is due to the fact

that cell phone providers provide coverage to their subscribers through large telecommunication towers.
There are also satellite phones. These phones communicate through large signals that they receive from satellites, a principle similar to the one used by the Global Positioning System devices. I will write extensively about Global Positioning Systems later in the course of the book.

Wireless microphone

For years, microphones were built on wired technology such that a cord must connect the microphone to a sound system before it can be used. Well, that was in the past. In this era of wireless technology, wireless microphones are center stage. The last time you attended a concert or went to see your favorite artist play, you probably saw him or her use a wireless microphone. This has drastically increased the mobility of the artist on the stage while entertaining his or her audience. This is in stark difference to some decades ago when a wireless microphone was an unknown concept, a weird concept that had a say on the mobility of the user since a user can only go as far as the attached cord allows it to go. With each passing day, wireless microphone technology keeps advancing with more features added every so often.

Computer peripherals

Computers have played a very important role in the modern society. Wherever you turn — homes, schools, and business establishments — you see computer everywhere. Today, wireless technology has extended its reach to the computer industry. To improve the overall performance of a computer, many computer peripherals are created with different functions that can have a huge positive impact on what services a computer can offer its users. Many computer peripherals are now supported by wireless technology and can be used without being physically connected to the computer. Wireless mice, keyboards, printers, and other computer peripherals have contributed in a big way to the performance of a computer. Thus, you can print documents directly from your computer without connecting directly with the printer via a cable. You can also use your computer with other wireless peripherals according to your needs without having to spend extra money on wires and cables.

Household items

Making the list of wireless devices are some household items. In fact, this list will be incomplete without a mention of the several household items that are powered by wireless technology. In recent years, nearly everyone has a wireless household item or the other. For instance, if you have a television at home, it obviously has a remote control. The same can be said about a DVD player and a remote garage door opener. Recently, wireless baby monitors have also been introduced into homes. These monitors allow parents to monitor a baby's activities in another room without being physically in the vicinity of the baby, which has a lot of benefits. Regardless of the distance between a parent and a baby, the security of the baby can be guaranteed since the parents are aware of the baby's every move. Other wireless devices that can be found in the home include wireless routers, walkie-talkies, wireless adapters, and some video game consoles. All these devices are the product of wireless technology and have turned out to be a perfect alternative to their wireless counterparts.

CHAPTER 2: WIRELESS COMMUNICATION TECHNOLOGY

Wireless access concerning computer networking is built on the IEEE 802.11 standard for wireless connections. Wireless-fidelity is a custom trademark that operationalizes the 802.11 standards. Note that the Wireless-fidelity Alliance has attempted to simplify the naming of IEEE 802.11 standards, for instance, 802.11ax is named as Wireless-fidelity 6 and 802.11 ac is named as Wireless-fidelity 5 including 802.11n as Wireless-fidelity 4. The motivation for this renaming is to create router capabilities and a matching endpoint. Nevertheless, it is critical to stick with IEEE naming conventions. The following are some of the 802.11 standards.

802.11 ac

The 802.11 ac standard is for modern wireless routers and works best in the 5 Giga Heartz rate band. The devices that operationalize 802.11ac have multiple inputs, multiple outputs known as MIMO. The implication is that devices that implement 802.11ac have numerous antennas on receiving and sending end devices of data to help reduce error and enhance speed. The

802.11 ac can reach data rates of 3.46 Gbps. Some routers support lower 802.11 standards such as the 2.4 Giga Heartz rate through 802.11n that accommodate client devices running 802.11 b,g or n radios.

The 802.11n

The standard is among the pioneer standard to specify multiple inputs, multiple outputs and allows for running in tow frequencies, that is 2.4Giga Hertz and 5GHz, and speeds can reach 600Mbps. The technique of delivering data across these two frequencies is known as dual-band.

802.11a

The 802.11a allows for operation in the 5Giga Hertz rate and speeds that can reach 54 Mbps. For emphasis, 802.11a was released after 802.11b which created some confusion.

802.11b

The 802.11b always functions optimally in the 2.4 Giga Hertz rate and can reach a transmission rate of approximately 11 Megabytes per second.

A typical 802.11 network will have a wired connection especially from switches to routers and the radio receiver. The radio receiver is powered by power over Ethernet standard. The radio receiver connects with the satellite signal or nearest base station of an Internet Service Provider. The signal from the Internet Service Provider hits the radio receiver that then distributes it to the main router of the wireless local connection. From the router, the Internet service is distributed to other routers or directly fed to switches for uniform sharing of the bandwidth. The purpose of switches is to break up the collision domain by increasing the collision domain. Switches in a network help segregate nodes within the same network. The router helps interconnects different networks.

A wired local area connection can also be extended as a local wireless connection which is important for organizations that implement Bring-Your-Own-Device policy. Once the main router receives a signal from the radio receiver, then the Internet service will be available via wireless platform if the router has Wireless-fidelity capabilities. Alternatively, the network designer can install access points for a large organization to create Wireless-fidelity hotspots. Typical access points offer a stable connection

to a physical distance of 30 meters. The distance can be extended using Wireless-fidelity extenders which are essentially signal repeaters. It is important to remember that like any network; the more users join a Wireless-fidelity network the lower the Quality of Service if other factors remain constant.

There are challenges when implementing a wireless local area connection. One of the challenges arises when individual end users create more Wireless-fidelity hotspots that are not secured. It is easier for users to create their Wireless-fidelity hotspots using virtual Wireless-fidelity applications or using their small-home office routers. With this in mind, it is imperative that network administrators properly configure the network to ensure that extending Wireless-fidelity or network does not happen without the express intervention by the network manager. The network administrator should also monitor packets on the connection or network using packet analyzers to detect any anomaly.

Additionally, administrators of a network should remember that Wireless Protected Access is mainly encrypting the data transmitted but more needs to be done to prevent active attacks on the entire network structure. For instance, the local router address should be changed from the default address to a custom address only known to the network administrator. The router should not maintain default values unless such default values have zero impact on network usage and network security. It is one of the good practices for the network administrator to update the network map of the organization each time the network is modified even by changing the location of a switch. The network map should be kept confidential as it constitutes part of the security of the wireless local area connection.

CHAPTER 3: APPLICATION OF WIRELESS TECHNOLOGY

Since its introduction into the networking industry, wireless networks have taken the industry by storm. From the real estate to the insurance industry, education to finance, wireless networking has continued to be the go-to technology when considering networking and Internet connectivity. Over the years, wireless networking has come in different forms and applications. Let's consider a couple of these types and applications.

TYPES OF WIRELESS NETWORKS AND THEIR APPLICATIONS

Wireless technology has gradually become an integral part of our daily existence. Most students today have a Personal Digital Assistant (PDA) or a cell phone they use for checking emails, voice communications, and other important uses. Thus, this technology has provided users with incredible opportunities that are too numerous to ignore as well as various beneficial applications.

Some public applications of wireless networks include:

- **Internet access:** Unlimited access to the Internet ranks high among the numerous areas of applications of wireless networks. It is easily the most compelling reason why installing a wireless network becomes a necessity. As earlier highlighted, having free access to the Internet makes job execution faster, is more convenient, and saves money.

- **Voice over wireless:** The incorporation of wireless networks into the transmission of voice conversations is a welcome development and a beneficial solution for individuals who need to constantly be in touch with each other. When wireless networking serves as the center of a combination of data and voice, it provides the users lower operating costs and mobility. This is obviously beneficial to the users. For instance, retail store employees may quickly locate clothes for a customer or check their inventory via a specially-designed wireless LAN phone. With the full support of the wireless LAN in the store, barcode transmission while taking inventory of goods is possible. Pricing with a handheld barcode scanner is also supported by the LAN, making this a cost-saving alternative for retail store owners. In a business setting, a business may similarly deploy their telephone system over a wireless network. Thus, employees can move around with their phones as a cell phone, making it easy for them to accept calls with a single phone within the facility.

- **Inventory control:** Wireless LAN has assisted companies to track and update their inventory without delay. Real-time tracking and updating have enabled accuracy and efficiency to increase in the business sector. For instance, it is possible for a wireless management solution to update an inventory as soon as the clerk stocks a product. The huge impact on the retail store with this new development cannot be overemphasized.

The same can be said of the manufacturing industry. Wireless networks make keeping finished product and raw materials statistics up-to-date easier than it previously was. With wireless-enabled barcode scanners, manufacturing employees' workloads are made simpler because the wireless network allows scanners to handle some functions such as

checking or changing product prices. These scanners can also go through the stock to check the number of available products.

It is noteworthy that the adoption of wireless LAN for managing inventory leads to improved accuracy. The accuracy, on its part, creates tons of benefits. For instance, the clerks don't have to deal with voluminous paperwork since they enter their data via handheld scanners into their main computers. This reduces human error significantly when inputting data and thus, the company can boast of accurate financial records. This is of great importance to manufacturing companies as accurate financial records ensure that they pay their taxes promptly and accurately, preventing the companies from being fined by tax offices for incorrect tax payment.

MEDICAL APPLICATIONS OF WIRELESS NETWORKS

Wireless networks can fully be deployed for many applications that will contribute in a significant way to the efficiency and accuracy of medical examinations, treatments, and others. These are some of the top applications of the wireless network in the medical industry:

1. **Clinical communication:** Better care can be given to patients if medical personnel have access to better communication. Wireless networking makes it possible for clinicians to have access to lab results as soon as the results are ready. They can equally have access to vast medical databases via their tablets, smartphones, and other mobile devices. The availability of patient information ensures that patients get better treatments. For instance, Vocera and some other third-party vendors have developed voice-over wireless phones that make it easy for doctors and nurses to communicate effectively, whether they are in an examination room or on rounds.
2. **Tracking and location:** Tracking and location are very important for effective and prompt medical assistance. When a healthcare institution is aware of the real-time location of its patients, staff, and assets at a particular point in time, it can lead to an improved

workflow, increased staff safety, reduced costs, and increased staff safety. Some services, such as Wi-Fi location, have drastically improved response time and have reduced the loss of valuable assets by giving information about such assets' precise location when needed.

3. **Medical Device Connectivity:** Today, more and more medical devices are connected to LAN. Some examples are electrocardiograms (EKGs), patient monitors, portable CAT scans, and others. This has increased information flow as well as better quality of care for the patients. A typical example of such an application is SecurEdge Networks . This device can provide assistance to numerous medical devices on a single WLAN. In the process, it helps minimize the complexity associated with the network. Thus, it makes it possible for your hospital network to provide the right support for all the wireless mobile devices on your network.

4. **Inventory management:** You can't remove proper inventory management from increased profit in any industry, including the medical industry. A Wireless network can really assist hospitals to manage their inventories properly in order to help them reduce costs. Hospitals can take inventory of their assets to enable them to get the best out of their stock, such as the quantities of used or available prescription drugs. When the pharmacy fills a prescription drug, it will attach a barcode label to the drug's container. This will serve as the link between the prescription drug and the hospital inventory. With a mobile device, a hospital employee can quickly scan the drug barcode to enable him or her to remove the drug

from the inventory and administer the drug to the patient after scanning the patient's wristband barcode.

5. **Cardiovascular diseases treatment:** Cardiovascular diseases can better be treated with the use of smart sensor nodes. These nodes are installed on any patient with this health problem. Medical staff can then prepare treatment in advance as he or she receives important information about heart irregularities and heart rate while the patient's status is kept under proper monitoring. The availability of these pieces of information makes it more convenient for the medical staff to provide the best medical care that will reduce the patient's chances of sudden death that may arise as a result of cardiovascular diseases.

6. **Cancer detection:** Cancer is undoubtedly a monstrous killer. It is currently the second leading killer in the United States and is currently one of the most dreaded killers in the world. However, the increased mortality rate of this dreaded killer can be reduced with a sensor that comes fully equipped with the ability to detect dangerous chemicals emitted by cancer cells. It can also be used for differentiating cancerous cells and other cells in a patient. The isolation of the cancerous cells will go a long way in reducing the time and other resources wasted in isolating these harmful cells through conventional means. Thus, medical personnel can provide a cancer patient with timely life-saving treatments.

7. **Depression, Alzheimer's, and elderly people monitoring:** At the moment, there are an estimated 200 million adults across the globe. These senior citizens are vulnerable to a plethora of health challenges, including depression and Alzheimer's. The health condition of these adults can be better monitored with the assistance of a

wireless sensor network. Elderly people and the homebound who sometimes feel depressed and lonely can be assisted with the sensor network. When it is implanted on the subject, the sensor will detect any abnormal behavior of the victim and promptly alert the family, neighbors, and/or the nearest hospital. The swift reaction of the medical personnel or the family members may make the difference between life and death for the elderly or homebound person.

8. **Preventing medical accidents:** Medical accidents lead to approximately 98,000 deaths annually due to human error. The thousands of lives lost to this human error can be prevented with a sensor network. This network has the ability to accurately maintain the log of all the previous medical accidents. The information will help health practitioners to be wary of repeating such errors and thus save more lives.

9. **Asthma attacks prevention:** This is where a wireless network can also be found handy. Millions of asthma patients can handle this ailment effectively by using a sensor node that can sense any allergic agents that may undermine the patient’s health. The status report will be continuously relayed to the patient as well as the physician. This will help the patient take the right preventive measures to prevent an attack.

10. **Public networks:** The proliferation of PDAs, laptops, and cell phones in recent years has led to a growing need for an interface that can connect mobile devices with corporate applications and the Internet. Users want a platform where they can get constant and easy access to the wide array of resources on the Internet. Wireless networks have come to their aid and provided the infrastructure needed to provide these users high-

performance Internet connectivity for their use, both in the office or at home. With the public wireless network, people can connect with the Internet whenever they want without any undue restrictions. Some public places where wireless LANs can commonly be found include restaurants, hotels, and airports.

11. **Utilities:** Unlike in the past when utility companies had to manually check meters to enable them to calculate bills, they are now employing wireless WANs to support system monitoring and meter reading. Rather than go through the strenuous meter readings that were initially recorded on a sheet of paper before they were later transferred into the computer for processing, WAN allows the periodic data transfer from the meter to the processing computer via the company's wireless connection. This smart move reduces the company's overhead costs and saves time by completely eliminating manual meter readers as well as human meter readers.

12. **Education:** The education sector has also benefited immensely from wireless applications. Today, many elementary schools and colleges have made it a priority to install wireless LANs for the benefit of the students. The goal is to provide the students with the needed mobile network applications that will assist them with their assignments and researches. By targeting students with mobile devices and laptops, these schools want the students to have access to the school resources and the Internet from different locations in the school, such as quads, classrooms, dormitories, and libraries. The students can surf the Web, check e-mail, check their grades, access specialized school applications, and view their transcripts, all from the comfort of their school. The more access to

the Internet and other valuable resources, the more efficient the students will become.

NETWORK TECHNOLOGIES IN THE MEDICAL INDUSTRY

While the application of wireless networking has been found to be very useful in the medical industry, some powerful technologies make these dreams come true. These technologies are behind the application and effectiveness of these areas of application. A good look at some of these technologies will leave you in awe of what can be achieved with wireless technology, especially in the medical field.

1. **HipGuard System:** This is a special design for patients recuperating from hip surgery. The system is designed for monitoring a patient's hip position, their leg, and hip rotation through an embedded wireless sensor. If the system senses false leg or hip rotation or position, it will immediately send a signal to the Wrist Unit of the patient. The HipGuard System can then use this information to provide real-time information that can aid the patient's rehabilitation process.
2. **MobiHealth:** MobiHealth was built on the GPRS/UMTS wireless technology for the purpose of data transfer. The technology was built on the European decision to create a platform where home healthcare can be done with wireless telephony technology and sensor technology. The aim of the technology is to monitor a patient continuously even outside the four walls of the hospital. MobiHealth is out to improve patients' quality of life through the provision of disease diagnosis, disease prevention, physical state monitoring, remote assistance, and clinical research. These value-added services will improve patients' health tremendously. For instance, a patient that is discovered to need short-term monitoring

may not have to be admitted to a hospital before he or she can be monitored. Rather, the patient may live his or her life without movement restriction while the physician can still monitor the patient closely

4. LifeShirt: LifeShirt is a completely non-invasive and comfortable smart garment that was designed for gathering data while a patient goes through his or her daily routine. It can then provide the healthcare researchers and professionals with a complete picture of the wearer's health status. This information will prove valuable as it assists these professionals to have accurate monitoring of over 30 life-sign functions at the patient's workplace and home. LifeShirt carries out the data collection with the help of integrated sensors such as respiratory bands that are designed for measuring the pulmonary activity and an ECG for recording whatever electrical activity occurs in the heart.

Wireless technologies have come to stay. With each passing day, the areas of application of these technologies keep increasing. In the nearest future, these technologies have the potential to change the world for good.

CHAPTER 4: WIRELESS TECHNOLOGY FOR INTERNET

A wide territory organizes (WAN) is a media communications arrange, normally utilized for associating PCs, which traverses a wide land region, for example, between various urban communities, states, or even nations. WANs normally are utilized by partnerships or associations to encourage the trading of information between their PCs in scattered workplaces. Overall enterprises, most enormous organizations with offices at different areas use WANs, and even free organizations with just two local areas logically use WANs. Most WANs interface at any rate two neighborhoods (LANs) and the Internet is on a very basic level an immense WAN.

Even though WANs fill a need like that of LANs, WANs are sorted out and worked out of the blue. The customer of a WAN as a general rule does not have the correspondence lines that interface the remote PC frameworks however rather buys into an administration through a media communications supplier. In contrast to LANs, WANs normally don't connect singular PCs, however rather are used to interface LANs in what are known as internetworks, using devices called switches and remote augmentations.

Even though WANs fill a need like that of LANs, WANs are organized and worked unexpectedly. The client of a WAN, for the most part, does not claim the correspondence lines that associate the remote PC frameworks yet rather buys into an administration through a broadcast communications supplier. In contrast to LANs, WANs ordinarily don't interface singular PCs, yet rather are utilized to connect LANs in what are known as internetworks, utilizing gadgets called switches and remote scaffolds.

WANs additionally transmit information at much more slow speeds than LANs, most regularly at about 1.5 megabits every second (Mbps) or less, rather than the tens, hundreds, or even a huge number of Mbps

accomplished by LANs. WANs are basically like metropolitan zone systems (MANs), yet are ordinarily increasingly slow interchanges joins for separations more noteworthy than 50 kilometers.

WANs have existed for a considerable length of time, yet innovations, administrations, and applications have created throughout the years. WANs were initially created for advanced rented line administrations conveying just voice, instead of information. Accordingly, they associated the private branch trades (PBXs) of remote workplaces of a similar organization. WANs are as yet utilized for voice administrations, however, they are utilized most vigorously for information and, as of late, additionally for pictures, for example, video conferencing. WAN utilization is developing, as more organizations have introduced LANs and as progressively moderate internetworking hardware has turned out to be accessible.

Even though WANs fill a need like that of LANs, WANs are sorted out and worked out of the blue. The customer of a WAN normally does not have the correspondence lines that interface the remote PC structures anyway rather gets tied up with an organization through a media interchanges provider. As opposed to LANs, WANs normally don't associate particular PCs, yet rather are used to interface LANs in what are known as internetworks, using contraptions called switches and remote frameworks. WANs moreover transmit data at significantly more moderate rates than LANs, most for the most part at about 1.5 megabits consistently (Mbps) or less, as opposed to the tens, hundreds, or even a considerable number of Mbps achieved by LANs. WANs are in a general sense like metropolitan zone frameworks (MANs), be that as it may, are conventionally progressively moderate trades joins for partitions more unmistakable than 50 kilometers.

CHAPTER 5: INTRODUCTION TO COMPUTER NETWORKING

How did it start?

If we are going to start talking about computer systems and networks as a career, we have to understand its history and how it became an in-demand job today.

"Information technology," better known as IT, is defined as the technology that involves the development, use and maintenance of computer systems, software and networks for the distribution and processing of data. The term goes way back to 1978.

Computers did exist before 1978, but they were mostly used to perform calculations. Since they started to be used to index and sort written information, the term IT was invented.

Today, IT is a quickly evolving field and that, of course, includes the computer systems and networking career inside this branch.

Computer systems and networking. What exactly is it?

The IT career is based on the upkeep, configurations and reliable operation of the computer system, especially the process of multi-user computers and its networks with other users.

Nowadays, companies rely on their networks for a lot of their work, so any issues must be fixed quickly and entirely.

The computer systems and network administrator keeps the organization's workflow and its lines of communication accessible - at all times necessary. Besides identifying and solving network problems, computer systems administrators also make updates to all hardware and software they manage, so they're always ongoing.

A computer systems administrator is the main point of contact for an organization's network users when they suffer some technical issues. The specialist also needs to guarantee that every connection in the office is working well and supervise the performance of the Internet optimizing their hardware and software.

A computer system and network administrator also make sure that the overall performance and security of the computers they supervise, fulfill the needs of the network users, without surpassing the company's budget.

The person in charge of this job needs to be ready to find new issues each day and needs to get their knowledge optimized to approach them efficiently.

The importance of the field in the current era

Today, companies look at networks and computer systems as their foundation to work optimally. They need their hardware to be highly functional and maintainable, they need their Internet and servers stable, and they need someone to do all the networking and cable installation and check-ups constantly around their offices.

As we said before, they are the ones responsible for the configuration, reliable operation and upkeep of computer systems inside the office. They seek to ensure that the uptime, performance, resources, and security of the computers they manage to meet the needs of all the users.

Today, companies are very dependent on this type of professionals. They need to check the performance of their systems and need a person available almost 24/7 to guarantee that everything is functioning as it should. If one of their servers are down, or they lose Internet connection, they start to lose money very quickly mainly because they stop their production for a certain amount of time, and there is no way to monetize the operation without it working efficiently with the connections and servers.

A computer system administrator or specialist is one of the most critical professionals inside every office nowadays.

The computer systems and networking administrator is also the one in charge to guarantee that the Internet connection is working correctly and that the mail server is running and processing emails that are being sent and received by all staff within the organization.

If this task isn't well-executed, it might lead to a lot of expensive problems for the company such as serious mistakes in the production and handling of

their job to significant money problems and losses.

Here is a list focused on why it is essential to have a computer system and network specialist:

A specialist in this field maintains the operating system of the serves and applications, such as mail services, web services and more. They troubleshoot any hardware, OS or application-related problems to ensure the whole operation of the company itself.

A computer system and network administrator is in charge of maintaining the network infrastructure, such as routers and switches and fixing network-related problems. They attend every single detail about the networks and cables going around the office and how to keep them and the security of people working there.

They are also in charge of one of the most critical jobs inside an organization, and that is keeping the database system used by the company. In bigger organizations, this is a highly essential task, to secure all the data and to keep it optimized and safe from third parties, and possible losses.

This type of specialist is the one that coordinates the daily operation of secure systems. They handle the monitoring systems and the running of regular backups. They set up, delete and manage individual user accounts.

They keep every single system updated and working on its optimal conditions.

An overview of the process to become a computer system network specialist

When wanting to become a computer systems administrator, there is no one single way of learning. Educational requirements commonly include getting a bachelor's degree in computer science, web technology or network administration. Therefore, anyone who wants can become a computer systems administrator by self-learning or on-the-job training.

Some employers may need their administrators on computer systems to hold a certificate or proof of training from some specific software. There are some training methods and certification intended for specific IT fields such as Microsoft training and certification for Microsoft-based systems like Microsoft Windows and SQL. Another certification they might be looking for is a Cisco training certification for Cisco networks.

To become a computer system and network specialist or administrator, the first thing to aim for will be education.

While most employers want their network and computer systems administrators to have a bachelor's degree, others only need a postsecondary certificate.

Many degree programs focus on computer network and system administration. Because administrators work with computer equipment and hardware, a degree in computer engineering or electrical engineering is adequate as well. Programs in this area frequently include classes in networking, computer programming or systems design.

Because this technology is always changing and evolving, administrators need to keep up with all the recent developments.

Many specialists in this field keep taking courses throughout their careers and attend information technology conferences to keep updated with the latest technology as well. Some businesses need that administrators have a master's degree in IT.

Organizations generally want their network and computer systems specialists to be certified in the products they use. Certification programs are usually offered by the vendor or vendor-neutral certification providers. These certifications validate the knowledge and the use of the best methods that are needed by the network computer systems administrators. One of the most standard certifications is the one Microsoft offers.

Network administrators can work and study enough to become computer network architects. They can also advance to managerial jobs in IT departments, like computer and information system managers.

Here is a list of essential qualities everyone who wants to get into this career must have:

- **Analytical Skills** . Every computer system and network administrator or specialist needs to evaluate networks and policies to ensure that they perform reliably and to prepare for new customer's requirements and changing needs.
- **Multitasking skills** . Every computer system and network aspirant will have to work on many problems and tasks at the same time. The ability to deliver an excellent job while multitasking is one of the most important items on this list.
- **Communication skills** . A lot of people overlook this quality when it comes to this career, but its importance relies on the moment when they have to describe the problems and the solutions to non-IT workers.

- **Responsibility** . This is one mind-changing quality everybody should have, but when it comes to a computer system and network specialist, it is crucial. They manage the whole functioning of an entire company and how their production and work is on its optimal condition. Without responsibility, the company can suffer a lot of losses and issues due to a lack of conscience from their IT department.
- **Quick Learning** . As we mentioned many times before, the IT world is always changing and evolving and adding new systems to the list. For a computer system and network administrator, it is crucial to be updated with the software and hardware to ensure the best outcome for the organization.
- **Programming skills** . This is a perfect add-on to every computer system specialist, as sometimes you will need to go a little deeper when it comes to working with a particular server or web technology challenge, and the new knowledge will boost your work.

An overview of what makes an excellent specialist profile

What makes the right specialist for a company these days relies on many things, not only education. It is not a simple profession, but that is what makes it so demanding.

The computer system administrator is a crucial figure in any company, and it has always been a high profile when it comes to knowledge and qualities.

A computer system administrator is an essential part of a big or strong organization IT team. The positions do vary from business to business, but they are all responsible for managing the same things and duties.

These IT professionals must work closely with employees to install updates on computers and provide tech support when the problems appear.

Here are some traits that all excellent computer system and networking specialist must fulfill:

Patience . This is a crucial trait of any good systems administrator. Many times, the employees may be unfamiliar with certain computer functions. When it comes to optimizing or making changes, administrators need to have the patience to lead employees through different challenges.

Especially, when it comes to hardware or software issues, it can take a while for employees to do it the right way. In this case, the user is likely to be angry or irritable because they don't understand what to do with their computer or why it is not working as it should. A good system administrator needs to be able to respond with a patient and understanding manner to help and resolve the problem, to also minimize employee

frustration. Patience goes first when we talk about managing computer issues.

Flexibility. If you are doing a significant company-wide software upgrade and suddenly one of your primary servers fails, a competent system specialist will be able to quickly prioritize and be flexible when a potential hardware crisis arises. They need to know which upgrades to focus on first and which to pause given the current circumstances.

A flexible approach here can help understand the priority route to take when it comes to dealing with your company's problems. When looking for a candidate to take a job like this, it is essential to pick a multitasker. You need someone who is up to the challenges.

Technical Knowledge. Arguably the essential trait of any good systems administrator is a comprehensive understanding of computer equipment, hardware, and software. You need to have the strong technical knowledge to be able to figure out the solutions – especially when things aren't working as they should.

Embedded systems administrators typically have professional experience in an enterprise environment, plus numerous relevant certificates in their field. When hiring or interviewing new candidates, asking them questions related to their technical knowledge will determine how much they know about what they do.

Personable Nature. A computer system and network administrator frequently works with other employees. Operations and network specialists need to know how to communicate clearly and manage difficult personalities while staying calm under pressure and tight deadlines.

How do computer systems and networking improve a company?

When running a growing business, we start to understand that quality IT solutions are crucial to company efficiency. And computer networks are one of the most critical IT solutions. They help the business grow and let employees share ideas rapidly and work more efficiently. It increases their productivity and creates more income for the company.

Excellent computer systems and network administrators also reduce the amount of money that is spent on hardware by creating a computer network and sharing the equipment you already have.

With a professional on your IT team, you also improve storage efficiency and volume, you have the freedom to choose the best computer networking

method for your team to display. Hiring a professional computer system and network specialist also gives you a lot of flexibility.

Information technology has for a long time dominated the industrial segment. Since the inception of microprocessors, this field hasn't witnessed a dark stage. Each year, we witness a significant change in this domain that brings the real world closer to the virtual one. Smartphones, smart televisions, gaming consoles, motion-sensing devices are all wonders of the IT field. IT has become an integral part of our lives and it is difficult to imagine a world without it.

Information Technology and Business – What's the connection?

Information technology is required by companies to reduce costs, increase efficiency as well as gain dominance over the market. From website hosting and storage of data to strategy formulation and social networking, IT offers a wide array of corporate solutions. Strong integration of IT is done by business leaders to accomplish these goals. Nonetheless, there are certain domains under information technology that are trending and expect to grow exponentially shortly.

Why should you be keeping an eye on these trends?

These trends in Information Technology will likely be the point of focus in the coming years. These trends refer to those sectors that allow companies to enhance productivity and make their consumers aware of their range of products and services. Businesses from all over the world will be looking to exploit the potential of these technologies.

Here are the top technology trends that according to analysts will be the game changers shortly.

Private Cloud : The private cloud is an excellent alternative to public cloud computing as it resolves all the security issues posed by the latter. Consumers of information technology demand more from the services it provides. Wouldn't it be great if a business could reduce the time-to-market and operate cost-effectively? Every company will want this. As the private cloud is deployed within the company firewall, all the data can be shared among the employees without having to worry about security breaches.

Cyber Security : This continues to be a cause of serious concern among IT companies all across the globe. It would be dangerous if someone had access to a company's records and data about tenders. Our economies, nations, corporations are all interconnected. Most organizations survive on

the Internet. Compromising with cybersecurity can have a devastating impact on the global economy. This has become increasingly essential as Internet-based attacks will increase in the coming years.

Enterprise Social Networking : This is the next big thing in the corporate world. Every company would want to market its new products and enhance brand awareness. As more and more people are getting onto social websites, it has become easy to connect with them on social networks. In the coming years, it is anticipated that people will become more comfortable with using such websites and carry out business transactions over the Internet. Businesses that succeed in becoming social organizations have a better run on the market.

Gamification : This is one of the leading trends in information technology. Companies that focus on enhancing user experience are more successful. Gamification employs gaming mechanics, interactive media and social networking to accomplish this. Gamification is done to deepen the connection with consumers so that they interact well with the company. Gaming has for a long time been a very profitable domain and leading-edge companies will also be looking to explore its potential.

CHAPTER 6: NETWORK PROTOCOL

Network Protocols

Network protocols in the simplest sense are the policies and standards, including but not limited to, the formats, procedures, and rules that define how devices, two or more, communicate within a network. These policies and standards govern the end-to-end processes involved in communication and ensure the timely, secure delivery of data and network communication. Protocols in a network incorporate the processes, constraints, and even requirements of accomplishing communication between servers, routers, computers, and other devices that may be network-enabled. Normally, these network protocols are installed and confirmed by the receivers and senders so that network and data communication is done, and they apply to both the hardware and software nodes that communicate with each other on a network.

As such, a protocol can be likened to the language through which communication happens on the internet. This is because there is a set of mutually accepted rules that are also implemented as both ends of what is perceived to be the communication channel to ensure proper communication exchange. Two devices can exchange information only if they adopt the rules. We, therefore, cannot even dare communicate over the internet without the use of protocols. Every protocol is defined using unique terms, and each has a different name. Typically, messages travel from the sender to the receiver through a medium just like normal communication does. In this case, the medium refers to the physical path over which the information will travel once it is sent and expected by the receiver. It uses a protocol.

These formats are used among communicating systems to exchange messages, where each has a precise meaning and is intended for a particular

recipient. This recipient then produces a singular response from a pool of all probable responses predetermined for the specific situation being examined. This characteristic is typically autonomous of its intended implementation communication protocols agreed to by the parties involved, and to do this, protocols are developed according to technical standards. This kind of arrangement is also the same for a programming language, and it can, therefore, be said that protocols act to communicate as programming languages do to computations. Different protocols describe different aspects of communication. A group of protocols that have been designed to work in collaboration is known as protocol suites. When protocol suites are implemented in software, they are known as protocol stacks. The Internet Engineering Task Force publishes internet communication protocols, and hence, it handles both wired and wireless networking that has become a prominent part of present-day networking. The International Organization for Standardization, also known as ISO, on the other hand, handles other types of networking. Yet another organization, the ITU-T, handles protocols for telecommunications and public switched telephone network (PSTN) formats. This and internet coverage are uniting over time. As such, the standards are doing the same and are moving towards convergence as well.

Communicating Systems

Between other media and the devices in a network, communication is exchanged in every instance. This type of exchange is administered by predetermined agreements set out in communication protocol specifications. These specifications work to define the state-dependent behaviors, actual data that is exchanged, and the nature of communication. Digitally, in computing systems, the rules are expressed as data structures and algorithms, while in communication, they are expressed as protocols. Operating systems, which we will discuss later in the book, usually contain cooperating processes that work to manipulate the data that has been shared within devices to know what was being communicated. The protocols that govern this communication and protocols are also embedded in the process code. Communicating systems do not have shared memory, and therefore, they have to use a shared transmission medium for communication with each other. Transmission as the way to achieve the ultimate goal of communication may not be reliable. As such, individual systems sometimes end up using different operating systems and different hardware. When implementing a network protocol, software modules for protocols and

frameworks within the operating systems of machines interface. The framework is responsible for implementing the operating system's networking functionality. Protocols are usually expressed in a portable programming language, and when this happens, protocol software and the operating system are made independent of each other. The TCP/IP and OSI models are the most popular frameworks.

A design approach that has been deemed successful is abstraction layering from the days as early as when internet development was taking place. Abstraction layering was a useful design approach for both the operating system and compiler design. There are similarities between communication protocols and programming languages, and this meant that the monolithic networking programs could be broke down into protocols that could work together, giving rise to the concept of layered protocols. As a result of such developments, today, layered protocols are the basis of protocol design. One protocol is generally not enough for systems when transmitting information. Instead, there are sets of protocols that cooperate to ensure transmission, and they are known as protocol suites. Protocols are arranged based on the way they function in groups. To illustrate, take a group of transport protocols, for example. Here, the groups of layers pertain to certain functionalities, where each of the layers solves a particular class of problems that relate to different aspects, such as the internet, application, transport, and network functions. For a message to get transmitted, each layer gives a chosen protocol. The subsequent protocol's selection is attained when the message is drawn-out by a protocol selector in each of the layers.

Basic Requirements for Network Protocols

For data to get across, an entire network is just a small part of the equation when it comes to transmission. Once the data is received, more things happen. For instance, data has to be evaluated so that it can be understood how far the conversation has reached. Protocols, therefore, must be inclusive of rules of engagement that will describe the context. The rules in question express communication syntax. There are other rules as well, and these determine the usefulness of the data that has been transmitted according to the context of the exchange. They are the rules that express the semantics of communication. Communication, in this case, involves semantics and syntax.

There is the sending and receiving of data on communication systems, and protocols define and specify the rules that are responsible for the government of transmission. The aspects described below are, therefore, to be addressed

Data Formats for Exchange of Data

In this sense, there is an exchange of information bit-strings. There is a division of the bit-strings into fields, and every one of these fields carries information that is relevant to the protocol in question. There is a division in the bit-string, so it consists of two parts: the payload and header. The payload is responsible for carrying the actual message, and the header, on the other hand, is responsible for fields that are relevant to the protocol's operation. There is a maximum transmission unit for bit-strings, and sometimes, some bit-strings are longer than this specified minimum. In such cases, the bit-strings end up being divided into smaller appropriate-sized pieces.

Address Formats for the Exchange of Data

Addresses in networking are just like addresses for humans in real life. They identify who the sender of information is and who the intended receiver is. The header area in the bit-string described above contains this information, and this allows the recipients of the message to determine if the bit-strings will be of use to them or not so that they can process or ignore the message therein. There may be a connection between the receiver and the sender, and this is identified using what is known as an address pair. Address pair come with values that have meanings for the

receiver and sender. Sometimes, the addresses come with special values that have meaning. This is what results in a broadcast message in a local network. An addressing scheme is the set of rules that describes the meanings of the address values in the address pair.

Mapping of Addresses

This happens when protocols need to address one scheme to another. For example, when there is a need to translate an application specified logical IP address to an Ethernet Mac address, address mapping must happen so that the address of the first scheme is understood to the second scheme.

Detection of Errors That Occur During Transmission

Data detection is a necessary and important part of the process of data transmission in networks. It is especially necessary in cases where data corruption has occurred. The most common approach to this issue is the attachment of CRCs to the end of packets. When the CRCs are added, then the receiver of data can establish that some differences have occurred as a result of corruption. This gives the receiver a basis for rejecting the packet, and therefore, arrangements are made for retransmission.

Routing

Sometimes, you may find that systems do not connect directly. In such cases, there is the employment of intermediary systems that work to connect the intended receiver with the message. These routers forward the message on behalf of the sender and make it possible for the receiver to get the intended message. “Router” is a term that is used when these connections happen on the internet, and the resulting interconnection of networks is referred to as internetworking, as mentioned earlier.

Acknowledging

When there is the expectation of communication, then acknowledgment that the correct data was received is necessary. The receiver usually sends the acknowledgment to the original sender of the message.

Timeouts and Retries

Interestingly, despite taking all the necessary precautions, packets tend to be lost in networks sometimes. At other times, there may be a simple delay in the delivery of the packets. This is where acknowledgment plays a role because the sender expects that the receiver sends an acknowledgment so that they are sure that the message was received. The acknowledgment is expected in a set amount of time, and this gave rise to the concept of timeout. When the time lapses and the sender has not received an acknowledgment, it becomes a cue that there is a need to retransmit the information. In other cases, links may permanently be broken. In such cases, retransmission usually loses its effect, resulting in a restricted number of retries. When a number of retries exceed that of the limit, then an error follows.

The Direction in Which Information Flows

Sometimes, transmissions occur in one direction as would be on the case of information that flows from one sender at a time or half-duplex. If this happens, then there is a problem that will need to be addressed. This is the root of the concept of media access control as arrangements are made so that the case of contention and collisions are involved. Collisions happen when two senders want to simultaneously send out information, and contention happens when the two senders both wish to transmit data.

Control of Sequences

As we had discussed above, sometimes, bit-strings may need to be transmitted after division into smaller pieces. However, problems may arise as most times, when these bit-strings are sent individually on the network, they may get delayed and sometimes, lost as they may take different routes to reach their destination. In such cases, these pieces of bit-string end up reaching the destination out of sequence. Retransmissions, on the other hand, will result in duplicate pieces, which does not solve the problem. As such, the pieces are marked with sequence information when they are still with the sender. If, therefore, they reach the receiver when out of sequence, the receiver has the right tool to determine what is duplicated and can know what was lost and either reassemble or ask for retransmission as is best seen.

Control of Flow

The flow needs to be controlled when the sender is transmitting packets of data faster than can be received and processed by the intermediate network or receiver. As we have mentioned earlier, the best way to establish flow control is by messaging the sender and receiver.

Defense in Depth Principle

There are threats to every system and several ways an attacker may try to exploit them. When we consider how to secure a system, we need to consider Defense in Depth.

The *Defense in Depth Principle* states that there is no one thing or even two that can completely secure a system. This contention is that if one part of the security solution would have failed then another part should be able to resist or prevent the attack from succeeding.

In practice, this means applying security in layers. For example we could have a firewall and an IPS (Intrusion Prevention System) on the edge of the network, behind the firewall there may be an email scanning service, and on the workstations, there would be antivirus software.

An attacker may try to send some malicious code through email, the firewall and IPS may not be able to pick this up as email is a valid application. In this scenario, we would rely on the email scanner.

But what if the email scanner service is down for whatever reason? Maybe it crashed or maybe it just did not pick up that this email is a threat. In that case, we still have the antivirus software on the workstation to fall back on. This example is a simplified look at the Defense in Depth. This strategy reduces the risk of a successful and possibly very expensive security breach.

A common misconception in network security for beginners is to rely too heavily on the firewall. All too often people think that the firewall should suffice. Unfortunately, that is just not true. Firewalls are only just a piece of a much larger puzzle. A simple firewall uses IP address and ports to allow or deny traffic. An IPS can look into this information further and deeper into the traffic to see if it matches known patterns of attacks. These two are just part of the edge of the network.

What about encrypting traffic with HTTPS, requiring authentication and authorization before accessing secure resources. New security flaws are found regularly, patching these flaws regularly would help with the security

of the network systems. Also, we need to consider our endpoints - workstations, laptops, smartphones, and any other device that connects to the network. This is where we think about antivirus, host-based firewalls, and VPN (Virtual Private Network) connections.

We cannot consider something to be reasonably secured without considering all aspects of the systems. Aside from the technical controls like firewalls and antivirus, but there are also other things to consider like the physical and administrative controls. We need to consider things like the security of the building where the servers or workstations are based, locking the door to the server room, or putting equipment in locked racks or cabinets. When it comes to administrative controls, these relate to policies and procedures. It can start with identifying the proper way to handle data, a big part of this is simply educating the users. Having a controlled set of who can access the data. Reminding the users to use strong passwords, how to avoid social engineering, and how to recognize threats in general.

Security should be applied in layers and these layers are more than just technical controls. Having a contingency plan in the event one of the security layers failed, what actions can be taken to put everything back together and minimize the threat or damage.

Intrusion Prevention Service (IPS)

Intrusion Prevention Service is designed to prevent malicious actions from occurring within the network. For modern implementations, we always deal with IPS than IDS (Intrusion Detection System) since aside from preventing malicious actions, it also logs each incident where malicious actions have been prevented.

IPS can be either network-based (NIPS) or host-based (HIPS). The network-based monitors the entire network for malicious traffic by analyzing all TCP/IP traffic entering the network. The host-based on the other hand monitors a single host for malicious activity, usually for unauthorized changes.

NIPS requires that IPS be installed on a device at the network perimeter. The HIPS requires that IPS be installed on every host that requires protections - usually, it is only installed on specific servers.

IPS detection can be signature-based or anomaly-based. There is always one signature for every exploit that is capable of preventing, the signature works by zeroing in on some unique aspect of the particular exploit that is always present. One of the advantages of this method is the low rate of false-positives. On the other hand, signature-based can only detect exploits for which a signature exists, so signatures must always be updated.

In anomaly-based, the system looks for abnormal traffic and assumes that the abnormal traffic is malicious. The advantage of this method - it requires less maintenance; it does not need to be updated constantly. The only downside with the anomaly-based is the higher rate of false-positives.

Newer IPS systems are primarily signature-based employed in a physical security device. This is highly recommended for the needs of the majority of networks. Signature-based IPS can be put on a physical security client such as a firewall that sits on the perimeter of the network. A subscription is typically needed to be obtained from the vendor to keep the signatures up to date. Generally, the signatures update automatically, daily similar to how antivirus does its updates.

Types of threat:

- DoS (denial of service)
- **Ransomware**
- **Phishing**
- Data theft
- **Tracking**
- **Botnet**

Sources of Threats

Threat actors: Individuals with malicious intent, nation state sponsored groups

Sources of Vulnerabilities

Design problems

When somebody has designed an application or a system and there’s just a fundamental problem with that design

Implementation flaws

The design is fine but actually when that design has been translated into the appropriate code, will probably be at hardware, there’s problem at that stage and there’s resulting in weaknesses

Configuration issues

This is quite common. Systems are insecure when it shouldn’t be, because somebody either misunderstood how to configure the item

Changes over time

Too many changes have been done to the point that the system is no longer secure because the original intent has been lost

Failure to provide security updates

Most of the recent security attacks have been successful purely because people have not applied security updates.

Assumption of trust

Devices that do not belong to the network are plugged to the computer, making it the network system highly vulnerable for phishing scams. Email attachments that we easily open without examining a few details.

Vulnerabilities: Wi-Fi

- Do you control the hardware?
- Do you control the software / firmware?
- Are the protocols broken?

- Who have you given access to? Are their systems secure?
- Whose network have you connected to?

Risk Management

- Apply security in layers
- Know your gear
- Port scanning - a sample program is Nmap
- Firewall logging
- Intrusion Detection and Intrusion Prevention Service

Risk Management: Wi-Fi

- SSID hiding doesn’t work
- WEP is broken
- Don’t use SSIDs that can make you a target

Wireless Security

Most of us had connected to a Wi-Fi network with our laptop, tablet, or our smartphones. To join a network connection with a device, a network name needs to be selected and a password needs to be supplied.

Wi-Fi network can be just open with no password required; in that scenario, it means anybody can join it. However, in the majority of cases, Wi-Fi networks will be secure and will require a password. There are several different protocols for securing a Wi-Fi network.

Wired Equivalent Privacy (WEP)

This protocol was developed in 1999 making it the earliest security protocol that was used for wireless networks. As the term suggests, it is meant to supply an equal level of security to wireless networks as it did for wired networks. However, this turned out not to be 100 percent the case, it was learned that the 40-bit encryption that WEP used was vulnerable and not secure making it easily hackable. This is the main reason why WEP is no

longer used today and modern Wi-Fi routers won't even have it as an option anymore.

Wi-Fi Protected Access (WPA)

After WEP, a better security protocol was needed for wireless networks. WPA is a wireless security protocol that was developed to solve the problems of WEP. WPA uses a stronger encryption method called Temporary Key Integrity Protocol (TKIP). The new encryption method dynamically changes its keys as it is being used that way it ensures the data integrity. Even though WPA is a lot more secure than WEP, even today the WPA is outdated. TKIP did eventually have some vulnerabilities.

WPA2

WPA2 was developed to provide even stronger security than WPA, it does this by requiring the use of a stronger encryption method. While WPA uses TKIP for encryption, WPA2 uses AES which stands for Advanced Encryption Standard. The newer encryption uses asymmetric encryption algorithm which makes it strong enough to resist a brute-force attack. In fact, AES is classified to be secure that the U.S. federal government has adopted to use it, it is being utilized to encrypt sensitive government data.

Now when you log in to the Wi-Fi router's configuration page and proceed to the Wi-Fi security section, this is where you would find the different security protocols that you can choose from to protect your Wi-Fi network. In most routers, there is an option that has both WPA and WPA2 - this is a mixed security option. This option enables WPA and WPA2 at the same time, it will use both TKIP and AES security. The reason for this option is for compatibility purposes because some older devices (dated prior to 2006) may not be compatible with using AES encryption that is being used with WPA2. In this option, older devices will connect to the older WPA protocol, but at the same time, modern devices will connect to WPA2.

Using the mixed option all the time, though it is the most compatible with all devices, with this option while it uses AES it also is utilizing TKIP which is the lesser secure encryption. This leaves your network more vulnerable to a breach.

WPA3

This is the next generation of wireless security; it was introduced in 2018. According to the Wi-Fi Alliance, WPA3 contributes top of the line security

protocols available for commerce. To facilitate further vigorous authentication, additional features were placed to streamline Wi-Fi security. It will also receive increased protection from password guessing attempts. The WPA3 option is available to newer routers.

Wi-Fi Protected Setup (WPS)

This is another type of wireless security method that does not require the user to type in a password. The WPS was designed for people who know a little or novice about wireless networks, to make it easy as possible for their devices to join a wireless network.

There are a couple of different methods that are used with WPS, but by far the most common method is the Push Button method. In this method, the user would just need to press a couple of buttons to be connected to the network.

Most routers today will have a physical WPS button that you can press, and a lot of Wi-Fi printers will also have software or physical WPS button.

For example, you want to connect a printer via WPS, you would need to push and hold the WPS button that is located on the Wi-Fi router and in the span of 120 seconds you would press the WPS button on your printer. After a few seconds, the printer should be connected to the Wi-Fi router.

Another method for WPS is if the client you are using has a WPS pin number. If this is the set-up, the user just needs to enter a pin number to the field provided and within a few seconds, it will connect to the network.

WPS is the easiest way to join a wireless network, a lot of manufacturers have built wireless products with WPS. This is just to make it as simple as possible for the users to join a device to a wireless network.

ACCESS CONTROL

Access Control is called MAC filter in some routers, with this option the network administrator can either allow or block devices from joining a network. Every network adapter has a MAC address (MAC address can be described as the hexadecimal number - numeral system made up of 16 symbols, that exclusively pinpoint the identity of each device that resides on a network) and with Access Control the network administrator can manage the devices that can and cannot connect to the network using the MAC address of the specific device. When a device is blocked, it would exclusively be able to obtain an IP address from the router, but it would not

be able to communicate with any other device and it would not be able to connect to the internet.
The Access Control can be used as an extra layer of security that is in addition to the network’s Wi-Fi password. Access Control also works for wired devices.

CHAPTER 7: WIRELESS TECHNOLOGY SECURITY AND FUTURES

The wide areas of applications of wireless networks in modern times are an indication of what the technology will offer in the future. At the moment, wireless networks have simplified a lot of human activities such as communication, business transactions, and other activities. However, the future is brighter than most people can imagine. The modern wireless network will be easy to use. Let's analyze the main future developments of wireless networks and the huge impact on users. Let me start with Li-Fi.

LI-FI

You obviously are aware of the attributes and usefulness of the Wi-Fi wireless technology. As a reminder, this technology is one of the best things that has ever happened to wireless technology. Wi-Fi has really simplified wireless connection and makes it accessible to millions of users around the world. However, a better version of this wireless network is around the corner. Welcome to the world of Li-Fi. What is Li-Fi?

Li-Fi, Light Fidelity, is the new poster boy of wireless communication technology. This technology carries out data communication through light signals. One of the biggest advantages of this technology is its impressive speed. At the moment, this wireless technology can boast of a speed of 224 gigabits/second. When compared with its predecessor, Wi-Fi, this is a good improvement with tons of benefits for wireless connection users. Professor Harald Hass introduced Li-Fi into the world at a TED Talk in 2011. He had the dream of turning the light bulbs into a better use: wireless routers. Today, he is working towards achieving that dream and may do so in the near future.

HOW DOES IT WORK?

The Li-Fi network works on a very simple principle. First, a LED light bulb is fed with data and subsequently has a signal processing technology interfaced. The data is pulsed by the LED bulb at a high rate to the photodetector. When the photodetector receives the pulses, it interprets the pulse into an electrical signal. The signal is subsequently converted into binary data, the web content we all use.

Thus, the LED lights are later networked to make data accessible to multiple users through a single LED light or shift from a LED light to another while their access remains unaffected by the move. Li-Fi's high speed and spatial limits can be combined with Wi-Fi and cellular technologies as a connectivity option. The technology is very useful for siphoning off heavy traffic from Wi-Fi and cellular networks. For instance, this technology can be made available in sports stadiums, shopping malls, and other densely populated areas to allow users to consume live streaming, videos, and other content-rich media. When people are using Li-Fi, the capacities of Wi-Fi and cellular networks in the area will be freed up. Naturally, uplinks don't use much capacity like the downlinks with its network-straining capability.

One of the biggest challenges that experts are facing about the Internet of Things (IoT) revolution is how to find the huge capacity needed to handle the data. Well, Li-Fi has come to the rescue. It has proven to be an efficient, viable, and secure solution to that problem. An office, a home, or a factory can leverage the power of the Li-Fi technology for running its high capacity network while the public capacity is not affected in any way.

CAR-TO-CAR COMMUNICATION

In the future, a simple wireless technology will take over driving challenges and make our roads safer with reduced accidents. The technology is designed to warn drivers of impending collisions to enable them to prepare in advance to prevent the collision. Known as vehicle-to-vehicle or car-to-car communication, the technology will let cars on the road broadcast their speed, position, brake status, steering-wheel position, and other relevant information to other road users within a couple of meters of the car.
This valuable information will be used by the other cars to have a general view of what is going on around them and notify them of potential troubles that even the most cautious and experienced driver may miss. By building anticipation for the potential collision, the driver is best poised to take all necessary precautions to avoid the accident.

At the moment, many cars are equipped with ultrasound or radar technology for detecting vehicles or obstacles. Despite the usefulness of these technologies, their limited sensor range is a big issue to contend with. Cars equipped with the technology can see beyond the nearest obstruction, making it pale in comparison with the car-to-car wireless technology that will soon take over in the nearest future. With over five million accidents recorded in the United States alone every year, resulting in over 30,000 fatal cases, this technology will be a welcome development. At the moment, Japan and Europe are already testing this technology. It is a matter of time before other countries embrace this amazing wireless and life-saving technology.

THE INTERNET OF THINGS

IoT also comprises micro-electromechanical (MEMS) systems. When MEMS are embedded into an object, it allows you to communicate and interact effectively with the environment. The objects that can be used include controllers in oil refineries and humans with implanted medical devices. Thus, regardless of the numerous definitions of the concept, it is estimated that tens of billions of devices will enjoy Internet connection by 2020. To realize this vision, much is dependent on wireless technology. What happens to the connected billions of devices?

The connected devices have the capacity to generate information and data that Internet users from all walks of life can access regardless of their places

of residence. Therefore, businesses, governments, and individuals are allowed to use the information for making real-time data-driven decisions. In the future, the IoT has tons of areas of applications that will be explored as the technology fully matures. Let's take a look into some of the practical uses of this wireless technology in the future.

MORE CITIES WILL BECOME SMART

At the moment, the IoT wireless technology is embraced mostly by homeowners. This trend is expected to continue in the future, although more cities are expected to adopt this technology. Then, companies and cities will turn to the wireless technology to save time and money in addition to becoming more efficient. The adoption of the technology means that cities can be automated and remotely managed. Useful data can also be collected through video camera surveillance systems, visitor kiosks, taxis, and even bike rental stations.

ARTIFICIAL INTELLIGENT WILL BECOME THE REAL "THING"

Thermostats, home hubs, lighting systems, and others will collect data on your pattern of usage and habits. The voice-controlled devices in your home will record whatever you tell them and store the recordings in the cloud. The data collection has a goal: facilitate machine learning.

Machine learning is an integral part of artificial learning because it is designed to help computers "learn" without being programmed for specific uses. The computers are designed to pay attention to whatever information they collect and use the information to learn. In the future, the machines can really learn your preferences through series of data collection and adjust themselves to meet your preferences.

ROUTERS WILL BECOME MORE "SMARTER" AND SECURE

Routers are mostly used in homes and are vulnerable to attacks because users can't install security software on them. The craze for the adoption of

IoT in the consumer market has placed the necessity on manufacturers to make their products available in the market as soon as possible. The impact is that sometimes these manufacturers pay little or no attention to security in their bid to hit the market before their competitors. The home router becomes handy here.

As previously discussed, the router serves as the Internet's entry point into your home. It is true that the connected devices have no way of self-protection, but the router can provide entry point protection. Although the current routers provide some protection through firewalls, password protection, and the ability to be configured to grant access to some selected devices, they are still prone to attacks because they don't have security software installed on them. Thus, malware can still find a way around the security measures and gain access to a network.

Currently, attackers are focusing on effective ways they can exploit the vulnerabilities in IoT devices. In the future, routers will come fully equipped with built-in security software programs that are more effective at shutting off potential intruders than what the current security measure can offer.

WEARABLES WILL REMAIN A NICHE

It is estimated that by the end of 2018, over 12 million wearables will be sold in the US alone due to the increased adoption of Google Assistant and Amazon Alexa in more devices. The hype surrounding these devices has provided marketers with a new way of dealing with customers. It is expected that the manufacturers and marketers of these devices will not rest on their oars but will build more of these wearables in the future to meet the growing needs for these efficient wireless technologies that have wormed their ways into the hearts of millions of users from all walks of life.

CLOUD COMPUTING

This simply means that you can store and access data over the Internet, rather than on your computer's hard drive. Thus, the cloud is nothing but a metaphor for the Internet. To give you an idea of how cloud computing works, I will give you two typical examples of cloud computing that billions of people are using:

- **Apple iCloud:** This cloud service is offered by Apple. It is primarily used for online backup and storage. You can also use the cloud service for synchronizing your contacts, mail, calendar, and others. Whatever data you need is at your fingertips on your Mac OS, iOS, or Windows device, although Windows users must install the iCloud control panel to use this tool. In addition to all these services, iCloud is also a very important tool for iPhone users. Its “Find My iPhone” feature allows iPhone users to locate their handset when it goes missing.
- **Google Drive:** This is the complete cloud computing service. Google Drive is designed to work with cloud apps such as Google Sheets, Google Docs, and Google Slides. The use of this cloud computing service is not limited to desktop computer users but is also available for smartphone and iPad users. Separate apps are available for Sheets and Docs as well. In a nutshell, most of the services offered by Google is cloud computing such as Google Calendar, Gmail, and Google Maps. Today, cloud computing has served as the platform where many people have put their skills to use. It has also served as the business companion of many entrepreneurs. Some of what you can do with cloud computing are:

- Store your data, back it up, or recover it through cloud.
- Create new services and apps.
- Host blogs and websites.
- Stream video and audio.
- Create and deliver software.
- Data analysis for patterns and predictions.

Cloud computing offers some benefits that make it a very important technology both now and in the future. A couple of its numerous benefits are:

- **Cost effective:** With cloud computing, you have to think less about buying software and hardware, a very expensive thing. You also don't have to bother yourself with setting up and running datacenters and spending a huge sum of money on round-the-clock electricity, racks of servers, and IT experts that will manage the infrastructure. This saves you a huge amount of money.
- **Speed:** Speed is another benefit you can enjoy from using cloud computing. Whatever computing resources you need will be delivered to you within a couple of minutes. You only need a few mouse clicks to access the services. This will give your business the desired flexibility while the pressure of capacity planning will be taken off you.
- **Performance:** A global network of datacenters is used for running cloud computing services; these datacenters are upgraded regularly by using the latest computing hardware that offers speed and efficiency. Thus, you have access to better resources rather than what a single corporate datacenter can ever offer you. It also offers greater economies of scale and reduced network latency.
- **Reliability:** Disaster recovery, data backup, and other related services are less expensive and easier through data computing. This is because the technology allows data to be mirrored.

Many people, including inventors and technology enthusiasts, are optimistic about the future of wireless technology. The availability of the needed

resources and the increasing demand for more wireless devices ensure that inventors will still feed humanity with more technologies that will make life easier and better in the future.

CHAPTER 8: WIRELESS NETWORK COMPUTER ARCHITECTURE

A few strategies for putting away information have developed to adapt to the prerequisite to save data. Here are four key stockpiling models:

Server-joined capacity

System joined capacity

Capacity zone systems

Tape libraries

Server-appended capacity

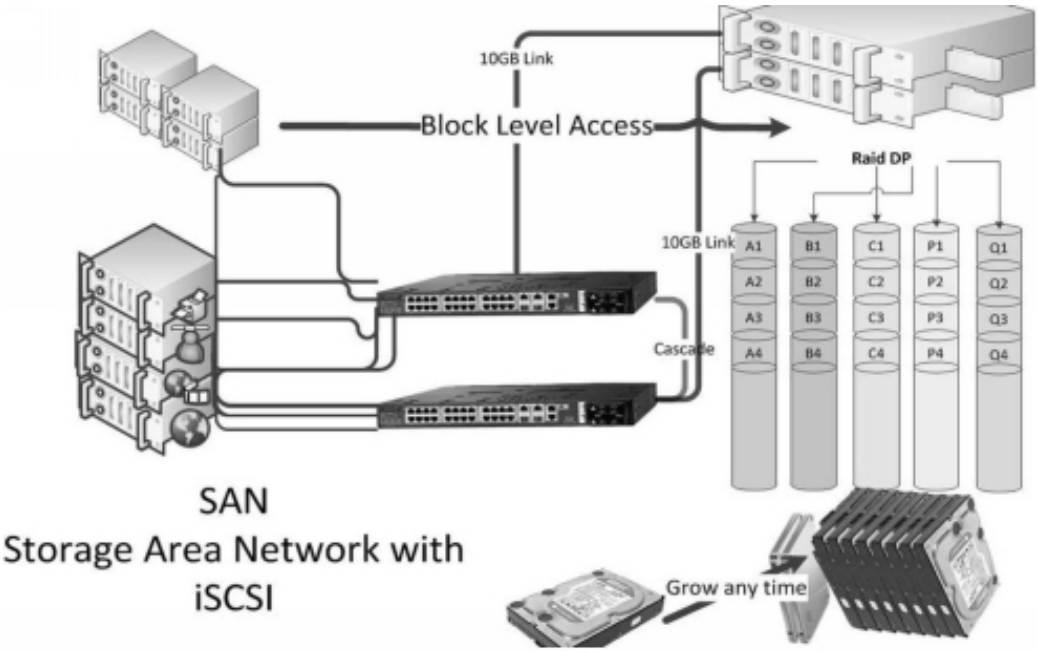
Server-appended capacity is the most widely recognized kind of capacity and has maybe turned into somewhat unfashionable.

As the name suggests, the majority of the circles and gadgets used to store the information are introduced in the server itself, as opposed to in a different gadget. That makes server-appended capacity financially savvy, particularly for little and moderate size organizations (SMBs), because they won't have to purchase some other gadget or framework. This method is increasingly reasonable for little servers that help access to petition for a few PCs or clients in a little office arrange. It is additionally a dependable method to give stockpiling to an application that keeps running on a server. Be that as it may, one test organizations face with server-appended capacity is versatility, as a server can just help such a large number of hard drives. This means, on the off chance that you come up short on space and need new capacity, the main option is to utilize greater plates. Be that as it may, when your organization begins utilizing greatest circles, the movement or

redesign way to a greater stockpiling system turns out to be progressively unpredictable.

Network Attached Storage (NAS)

The essential distinction among NAS and server-joined capacity is its utilization of a committed apparatus to house circle drives. NAS boxes, as they are known, associated with a system and can be gotten to by numerous customer gadgets, for example, PCs or servers. These containers are presently accessible in different sizes extending from single drive units costing a few hundred dollars each, to million-dollar frameworks each pressed with many plates. NAS became a force to be reckoned with in the late 1990s as an approach to enable servers to run applications quicker, easing the server from conveying information documents to clients. This type of capacity design additionally enables organizations to keep documents and information they need now and again in a committed machine. NAS is likewise well known for its capacity to hold different circles, which enables the reflecting of information to guarantee unwavering quality and information security. NAS machines have multiplied into numerous expert structures. In smaller-scale or independent ventures, NAS units are regularly utilized as a substitute for a server. In enormous organizations, master NAS gadgets speed access to information, for example, databases or email chronicles. Bigger organizations use NAS as a spot to store information they use oftentimes, as opposed to producing system traffic that courses through other capacity machines, for example, stockpiling region systems.



Storage Area Network (SAN)

The present most progressive stockpiling choice is a capacity region to arrange (SAN). These capacity systems can include at least one stockpiling gadgets, however, are seen by applications and servers as a solitary wellspring of information. This is significant for clients who need a ton of capacity limit because by joining gadgets into a solitary legitimate substance, SAN bolsters the utilization of various gadgets with various abilities to store information of various significance. These capacity systems are likewise incredible because they enable organizations to more readily control their capacity costs by mixing various kinds of capacity equipment in a solitary coherent unit. Records that are utilized each day, for instance, can be put away on quick, costly plates so clients can get to them instantly. More seasoned information that is just gotten to once a month can be moved off to more established, increasingly slow capacity gadgets. Access to the information here is slower however since the documents are utilized less now and again, client desires can be better overseen. Since these capacity choices live in a solitary SAN, which the working framework oversees as one single unit, organizations can blend and match stockpiling to accomplish higher execution and value proportion. One significant

component organizations must remember is that, with SAN, they should send and deal with a system to associate their capacity gadgets. This system can be executed dependent on Fiber Channel, a convention that is full-grown and broadly conveyed and gives quicker, progressively complex access to information. Be that as it may, this type of system is more costly to obtain and work than an Ethernet arrange. Fiber Channel is all the more expensive because such arrange frameworks sell at much lower volumes than Ethernet. All things considered, there are less prepared specialists fit for working a fiber channel system and this drives up work and in general costs for such organizes. An opponent Ethernet-based standard Internet SCSI (iSCSI), has since developed, giving paces moving toward 10Gbps, contrasted with Fiber Channel's 8Gbps. Whichever stage an association picks, it ought to recall that speed is significant if its representatives frequently get to bigger documents - an undertaking for which SANs are perfect on account of their entrance speed capacities.

Tape and tape libraries

Any of the capacity advancements referenced above are more than equipped for making reinforcements for an organization's information documents. All can be conveyed with Redundant Arrays of Inexpensive Disks (RAID), an innovation that permits the coordinated utilization of at least two hard drives so organizations can achieve better repetition, and henceforth, more prominent execution and information unwavering quality. Be that as it may, long haul information stockpiling on the circle is not a typical practice since plate stockpiling is still nearly more costly than tape. Moreover, plates work inside servers so NASs or SANs expend control at whatever point they are being used, and this can be an exorbitant domain for SMBs to keep up - just as a situation that isn't eco-accommodating for its high vitality utilization. Another contention against the utilization of plate as reinforcement is its cumbersomeness. The tape is, in this way, regularly pushed as the most ideal approach to store reinforcements and long haul documents. Tapes are commonly less expensive than plate since they can be put away on the rack, rather than inside a circle exhibit, and devour less power. Tape additionally has the benefit of being inactive when not being used, which means they break less regularly than plates. An amazing cluster of tape drives is accessible in the market today, going to top-end tape library frameworks that mechanize the capacity and recovery

of tapes, making it simple to get to the tape- - and information - organizations need to recover. Getting to information from tape, notwithstanding, accepts somewhat longer as organizations still need to distinguish and find the suitable piece of tape to recover specific information they need. Circles, on the other hand, take into account the recovery of any record or information inside minutes.

The staff in Internet technology send machines that are a virtual great rate, they unavoidably arrive at the presentation furthest reaches of the turning plates, surpassing most extreme stockpiling IOPS before arriving at the greatest limit. Accordingly, there is a lot of unutilized limits. There are four principal segments of virtualization;

The central processing unit (CPU)

Memory

Circle stockpiling

System

The work of the CPU power is that it keeps on expanding as per Moore's Law, multiplying roughly like clockwork by giving a consistently expanding number of handling centers and clock speeds. We likewise observe memory sizes expanding quickly attributable to ease RAM modules and quicker network, for example, here are 10 gigabit Ethernet, fiber channel 8gb, and Infiniband 40gb.

The majority the said permits, the VMs that are to be sent at expanded degrees of execution. Whilst we take a gander at plate innovation, in any case, great turning circles stay restricted by their involuntary parts, compelling IOPS in this manner the quantity of VMs they can bolster. Even though the SSD innovation may change this association, it is probably not going to move toward becoming standard as essential stockpiling for quite a long while as a result of cost/limit imperatives and unwavering quality concerns. Along these lines, as the IT business' hunger for more noteworthy quantities of VMs develops, it puts a huge weight on the capacity framework an issue that must be tended to by progressively effective plan.

At what time did capacity become so basic?

When you make servers virtual clients, they can separate them in between equipment quickly and with no vacation, while excluding the seen machine for them to be viewed as little than the CPU with the memory and I/O. On the other hand, in a VM domain, the capacity framework develops insignificance, as it turns into the supporting of the whole foundation. In a virtualized domain the customary framework circles are provisioned from the focal stockpiling, including load as well as adding to the randomized information access design the same number of virtual servers simultaneously fight for plate assets.

Think about this model: Admin A requires to solidify and make virtual the framework Let us say they own 25 window servers, MS Exchange, Linux servers, two little SQL databases, ERP framework and also client host indexes. The overseer in this situation will frequently put resources into a few new servers which have radically expanded CPU centers and give memory required yet may disregard to measure the capacity framework appropriately. The issues begin here because numerous elements, including limit, sorts of the RAID levels, and that of drivers as well as irregular execution of I/O should be taken into consideration.

Execution versus limit

Within the exemplary plate coerce showcase, huge limit increments happen at regular intervals. Be that as it may, we don't see a critical increment in turning plate execution. Execution outcomes continue as before. Back then, it might have displayed a test, as circle limit stayed down in that many SAN arrangements involve of 50+ plates to give any helpful limit. This numerous plates gave a lot of IOPS for every GB of limit. In the present innovation atmosphere, a pervasiveness of savvy SATA drives could give a similar limit of a fifth or sixth of the required number of plates contrasted and also SAS drives. The quantity of IOPS diminishes with the utilization of SATA drives which whenever utilized in a requesting irregular I/O condition like an exceptionally value-based file or enormous servers that are virtual, the SATA circles and their IOPS ability will block well prior to as far as possible is come to, except if they are led with strong condition reserve, where it can expand the framework's arbitrary in I/O execution by many times. It's additionally of value taking a gander with the rough manageable cost purposes of various circle innovations: During the IOPS run of 100-3000 run, the SATA drives give a very financially savvy stage, with

estimating as a rule given in terms of per GB dollars. The SAS are generally in automatic innovation, as arriving at this SATA exhibition needs countless shafts or measure of SSD reserving. Elite plates are normally estimated up cost for each GB. In the 10,000+ IOPS run, SSD starts to bode well, as just a small amount of clients general stockpiling requires such degrees of execution. Be that as it may, the best utilization of blaze is as a reserve.

The I/O data Patterns

The example where the request or the host' server peruses information can essentially influence the presentation of the capacity framework. Information examples are normally alluded to as either arbitrary or successive. An irregular information example suggests that the information is composed of arbitrary regions of the circle platter. With these, there are two fundamental impacts on a RAID exhibition framework. First, there is decreasing of the controller reserve viability, with which depends on examples to 'surmise' which information squares will be perused or composed straightaway. In irregular information design, this is beyond the realm of imagination, since an arbitrary grouping of occasions can never be 'speculated' and, accordingly, stored, however, 'hot information' tends to float into the reserve. The second pivotal impact of arbitrary examples is an expanded number of 'looks for': the time when a plate head must move to the following mentioned information square. If this square is haphazardly set, the plate's head and implementor have to go a huge separation in search of the square for every compose. In the circumstance includes overhead that is huge and also lessens execution. For instance, SATA drives, which utilize bigger circle platters, endure under arbitrary outstanding tasks at hand, as they just turn at 7200rpm and also have an extended look for and entry times. There are more qualified SAS drives just for the reason that they have platters that are littler and turn at the rate of 15000rpm, which also they look for in a moment of a fraction of the selected time (3.3ms by and large). Due to lack of moving parts, SSD is an option in the outrageous elite apps which makes it non-existent to look for times.

With an irregular remaining task at hand, turn rate and right to use time are usually vital to turning circle execution. The quicker a circle turns, then the IOPS will be more. On the other hand, one of the structures is successive information and consistency: an instance, information reinforcement as well as video gushing. Within these apps, then the records are normally

enormous and also kept in touch with the plate in nonstop squares and areas. Given this, the RAID controller and plates can all the more effectively 'surmise' and additionally store the looming information squares to expand execution. Moreover, there is no need to move the header and actuator arm of the plate in an incredible separation to look for the mentioned square. Such successive apps are generally planned when within MBs. This structure is infrequently constrained by plate speed and all the more ordinarily restricted by the controller and interconnect. Along these lines, in a capacity structure for consecutive applications, such as SATA, SSD and SAS circles give fundamentally the same as execution levels. The fast decide guideline is that consecutive examples are those with huge or gushing records and are most appropriate to SATA drives. Arbitrary remaining tasks at hand are commonly those with little documents or capacity demands that have no steady structure (virtual servers, virtual work areas, value-based databases, etc) and are most appropriate to SSD or conceivably SAS.

The RAID Effect

The comprehending of information examples, as well as plate kinds, are urgent during planning to stockpile for explicit applications, however, RAID level/type should likewise be considered. The capacity idea of 'equality punishment' alludes to the exhibition cost or effect of securing information through RAID. This punishment is only available on composes, therefore it is essential to recognize whether the earth is composed or perused escalated. These are the RAID insurance equality punishments: Peruses In light of these compose overhead costs, think about the accompanying: SSD drives are intended for irregular outstanding tasks at hand, so they ought to ordinarily be arranged as RAID1+0 to augment execution (except if a domain is 100% perused). SAS drives are additionally gone for execution. Along these lines, there ought to be the utilization of RAID 1+0 or RAID 5.

Enormous limits of SATA drives are usually gone for limit with throughput ought to be arranged as RAID6. RAID6 likewise gives extra security and true serenity during remakes for reinforcement apps where SATA the drives are liked. There can be viewing of RAID 5 when utilizing 2TB drives or littler. RAID1+0 can likewise be believed in exceptionally top-ranked virtual frameworks of about 2000 machines.

Structuring the capacity framework

The good way of structuring a productive stockpiling arrangement is getting application and condition necessities. Building up the information to plan the correct engineering can emerge out of specialized gatherings and talks, remote examination, on-location expert administrations and contemplating apps good practice IOPS control necessities for the SQL, VMware View, Exchange, or different apps explicit to nature. For each situation, the fundamental objective is to decide whether the earth/application is consecutive or arbitrary. Next, find the necessities for limit, IOPS, and MBs. However, there could be necessities used for capacity capacities, for example, depictions and duplication. In any case, the information full detail is inaccessible, basically with knowledge in the working framework and apps will provide you with guidance within the structure. The I/O stat can be used for requesting servers within the client condition can be checked utilizing (Unix) or Perfmon (Windows). At the point when utilized accurately, these implicit instruments can give every one of the information required. Another alternative is to utilize outsider observing applications, for example, VMware Capacity Planner. Such applications will accumulate nitty-gritty execution data and produce stockpiling reports. At last, you may assemble execution measurements from your current stockpiling framework. This information offers a beginning stage for planning the capacity arrangement. In an irregular condition, you will require to adjust and limit IOPS. In a successive domain, the structure will concentrate on limit and throughput or MB/s. Significantly, consecutive stockpiling frameworks are a lot simpler to design, as the MB/s appraisals quite often surpass the prerequisites.

Importance of Data storage

In the beginning, it is necessary to discuss the significance of data. The sheer volume of information combined with the improved investigation abilities accessible today implies that organizations currently can show signs of improvement comprehension of how their clients act in the at various times just as potentially what's to come. This veritable abundance of information can be mined and controlled into noteworthy data that can help take care of key business issues, sell more items or administrations, and everything in the middle. Information examination has turned into a significant focused separation from which most any business can profit.

Importance of storage

Because of its supreme volume, how and where organizations store this consistently developing pool of information has turned out to could easily compare to ever. The IT foundation must most likely scale with development and keep on giving reliable degrees of execution.

However, the truth for some is that server farms are coming up short on space in offices with premium expense per square foot. Moreover, inheritance circle based capacity can't convey reliably against new execution necessities. Putting away information isn't just about how and where, yet also, the speed wherein it very well may be gotten to, controlled, and introduced. For instance, getting to information in 5-10 ms is simply unreasonably delayed for an information-driven business that is reacting progressively to worldwide business openings on a 24×7 premise.

Because of its characteristic innovative favorable circumstances, an flash storage arrangement can illuminate a considerable lot of the present information development and availability issues in a denser, progressively productive, and littler structure factor. This empowers a higher level of capacity combination inside each 42U rack, sparing enormously on server farm space. This expanded rack thickness is balanced by power and cooling investment funds of up to 80% along these lines empowering server farms to remain inside their capacity envelope for each rack on the floor. Also, with progression in glimmer innovation, the descending value bend implies that every single blaze arrangement would now be able to be procured at a similar expense as customary endeavor plate stockpiling.

Simultaneously, streak based capacity conveys higher I/O execution, which is by and large 10-15x quicker than heritage stockpiling. Blaze can recover information in microseconds, as opposed to milliseconds, which is fundamental for constant or other execution delicate remaining burdens. Along these lines, glimmer conveys higher thickness and execution at the practically identical expense.

Virtualization Architecture

The term virtualization extensively depicts the detachment of an asset or solicitation for an administration which comes from the hidden seen conveyance of the administration. Using virtual memory as an example, PC

programming accesses large memory chunk than what is initially introduced, using the foundation exchanging of information to circle stockpiling. Additionally, the virtualization strategies can be connected to other layers of the foundation levels which also include systems, stockpiling, PC or server equipment, working frameworks, and apps. The sending of the virtual foundation is non-problematic since the client encounters are to a great extent unaltered. In any case, the virtual framework gives heads the upside of overseeing pooled assets over the enterprise, enabling IT supervisors to be increasingly receptive to diverse authoritative needs and also all the more likely influence foundation speculations. Utilizing virtual framework arrangements, for example, those from VM ware, venture IT supervisors should be able to attend to difficulties that comprise: Consolidation of server, and also sprawl containment using framework sending which act as virtual machines. This is VMs that can securely run and go straightforwardly crosswise over communal equipment, as well as increment server usage speed which ranges 5-15 to 60-80.

The test and development optimization quickly provides test and improvement servers which include reusing of pre-arranged frameworks and also upgrading designer joint effort and standardizing advancement situations. Advancement of Business- Decreasing of the expense and intricacy of business progression which includes high accessibility and calamity recuperation arrangements) by typifying whole frameworks into single documents that can be imitated and reestablished on any objective server, accordingly limiting vacation. Undertaking the work stations and Desktop Securing unmanaged PCs, where there is no trading off end client self-rule by leveling a safety approach in programming around work area virtual machines.

Virtualization Approaches

Whilst virtualization is a piece of the IT scene for quite a long time, it is as of late that the advantages virtualization were conveyed by VMware to the industry value set stages, which currently structure most of the work area, workstation as well as shipment of servers. A key virtualization advantage involves the capacity to run different working frameworks on a solitary physical framework and offer the fundamental equipment assets known as parceling. Hypervisors can be intended to stay firmly combined with the

working frameworks or else rationalist to working frameworks. Additionally, the last approach furnishes clients with the capacity to execute a nonpartisan of an OS administration worldview, consequently giving further legitimization of the server farm. The parceling of the level of application is yet another methodology, where numerous apps share a solitary working framework, yet this offers less seclusion (and higher hazard) than equipment or programming dividing, and constrained help for heritage applications or heterogeneous conditions. Be that as it may, different dividing methods can be joined, but with expanded unpredictability. Thus, virtualization is a wide IT activity, of which apportioning is only one aspect.

Different advantages incorporate the detachment of the virtual machines and the equipment autonomy that outcomes from the virtualization procedure. One outstanding advantage is the compactness of the virtual machines which can also be shifted and copied to any acceptable standard in the industry equipment stage, paying little heed to the make or model. In this way, virtualization encourages versatile IT asset the board and more noteworthy responsiveness to changing business conditions. To give favorable circumstances past parceling, a few framework assets have to be virtualized and overseen. This includes the Central processing units, I/O and principle memory notwithstanding having a between segment asset the board capacity. While parceling is a helpful capacity for IT associations, a genuine virtual framework conveys business worth well that has past that.

The Virtualization for the Server Consolidation and Containment- Virtual framework activities regularly leap from server farm server union tasks, which spotlight on decreasing existing foundation "box tally", resigning more seasoned equipment expanding inheritance apps. The solidification of server advantages come from a decrease in the general number of frameworks and related repeating costs which involve control, rack space, cooling and so forth. Whilst server solidification tends to the decrease of the present foundation, server control takes a progressively key view, server regulation takes an increasingly vital view, server containment leading to an objective of framework unification. Server containment utilizes a gradual way to deal with outstanding burden virtualization, where new ventures are provided with machines that are virtual instead of the servers that are physical, in this manner conceding equipment buys. It’s essential to take

note of that solidification nor repression ought to be seen as an independent implementation. Either way, the most noteworthy advantages come about because of embracing an all-out expense of-proprietorship (TCO) point of view, with an attention on the progressing, repeating backing and the board costs, notwithstanding onetime, direct costs. Server farm conditions are winding up increasingly mind-boggling and heterogeneous, with correspondingly higher administration costs. Virtual foundation empowers increasingly powerful improvement of IT assets, through the institutionalization of server farm components that should be overseen. Apportioning alone does not convey server union or control, and thus solidification does not liken to full virtual foundation the board. Past segmenting and fundamental part level asset the board, a center arrangement of frameworks the board abilities are required to adequately actualize sensible server farm solutions. These the executive's capacities should incorporate exhaustive framework asset observing (of measurements, for example, CPU action, circle get to, memory usage and system data transmission), mechanized provisioning, high accessibility and the remaining task at hand relocation support. These administration capacities should incorporate extensive framework asset observing (of measurements, for example, CPU action, circle get to, memory use and system data transfer capacity), mechanized provisioning, high accessibility, and outstanding burden relocation hold.

The complementing of virtualization New Generation Hardware Extensive 'scale-out' and multi-level application models are ending up progressively normal, and the appropriation of littler structure factor edge servers is developing significantly. Since the change to edge designs is commonly determined by a longing for a physical combination of IT assets, virtualization is a perfect supplement for cutting edge servers, conveying advantages, for example, asset enhancement, operational effectiveness, and quick provisioning. The most recent age of x86-based frameworks highlight processors with 64-piece augmentations supporting memories with large space. With this, there is the improvement of their ability to have huge, serious memory apps, just as permitting a lot increasingly machines that are virtual to be facilitated by a server that is physically conveyed inside a virtual system. The consistent abatement in the cost of memory costs will further quicken this pattern. In like manner, the approaching double center processor innovation altogether benefits IT associations by drastically

bringing down the expenses of expanded execution. Contrasted with conventional single-center frameworks, frameworks using double center processors will be more affordable since just a large portion of the attachments numbers which are to be needed in a similar number of CPUs.

Essentially, by bringing down the multi-processor expense frameworks, double center innovation will quicken server farm union and virtual foundation ventures. Past these upgrades, the VMware is additionally toiling intimately to guarantee that the technology of the processor of intel and AMD highlights virtual framework to the furthest reaches. Specifically, the new virtualization equipment assists in supporting Intel and AMD and will empower powerful CPU virtualization usefulness. In such equipment virtualization backing does not supplant virtual foundation, however, enables it to run all the more productively.

Paravirtualization - Even though virtualization is quickly getting to be standard technology, the idea has pulled in an enormous measure of premium, and upgrades keep on being explored. One of these is paravirtualization, whereby working framework similarity is exchanged against execution for specific CPU-bound apps which run on frameworks even without virtualization equipment help. There is possible performance in the para-virtualized model and gives advantages when a visitor working framework concerned that it is working inside a virtualized domain, and also adjusted to misuse this. One potential drawback of this methodology is that such adjusted visitors can't ever be relocated back to keep running on physical equipment.

Before actualizing virtualized frameworks, you have to decide the sort of virtualization engineering to use in your datacenter. There are two noteworthy sorts of virtualization engineering: facilitated and exposed metal.

Facilitated Architecture

In facilitated design, a working framework (OS) is introduced on the equipment first. Next programming, a hypervisor or virtual machine screen is introduced. This product is utilized to introduce different visitor activity frameworks, or virtual machines (VMs), on the equipment. Applications are then introduced and kept running on the virtual machines similarly as on a physical machine. Facilitated virtualization engineering is increasingly

helpful for programming advancement, running inheritance applications, and supporting distinctive working frameworks.

Exposed metal Architecture

With the exposed metal design, the hypervisor is introduced straightforwardly on the equipment instead of over a hidden working framework. VMs and their applications are introduced on the hypervisor similarly as with facilitated design. Applications that give constant access or information preparing advantage from uncovered metal virtualization desi.

CHAPTER 9: HOW DO WIRELESS NETWORKS WORK

The wireless network connects computers and other digital devices through the air via radio waves. Wireless networks are commonly called as Wireless Local Area Networks (WLAN), another term that is widely used is “Wi-Fi”.

Wireless networks can be structured in various ways; however, the basic components remain the same.

Access Point (AP) - this is the “heart” of the network and the links connect it to the nodes. This is the wireless router; it provides access to the internet and other to other computers within the network. Typically, a router is hardwired to a modem or in some cases a multipurpose device like the modem - router can be used. Typically, internet access is going through ethernet wires. From this moment on, the network becomes wireless.

Links

These are radio waves instead of wires, it uses one or two bands of the spectrum; 2.4GHz or 5 GHz. The earlier band is shared with microwaves, baby monitors, garage door openers, and many other non-Wi-Fi devices - all of which can cause interference to the network. The 2.4 GHz has a longer range compared to 5 GHz spectrum; however, the latter is extremely less crowded but since it does have a shorter range to extend its range capacity, it might require multiple access points as needed

Nodes

These are the computers or workstations and all other digital devices that can be connected to the Wi-Fi. Laptops and desktops have information cards that receive and send data through radio waves, the mobile devices like a smartphone or a tablet are like two-way radios in the sense that they receive and transmit radio waves to link to the access points

How is a device recognized by the wireless network?

Custom code is being used by the computer, this the Transmission Control Protocol / Internet Protocol. The TCP follows rules to create and assemble packets of information and the IP sends and receives these data. An IP address is assigned to a computer or every digital device while it in the network.

What is the difference between 2.4 GHz and 5 GHz Wi-Fi Routers?

The technology of today lets us have wider options when it comes to devices. This is also true for Wireless Networks. You might have noticed some Wi-Fi routers that have both 2.4GHz and 5 GHz frequency bands.

Overview:

2.4 GHz

· Advantages:

- Farther range
- Can penetrate solid objects

· **Disadvantages**

- Vulnerable to interference
- Slower speed

5GHz

· Advantages:

- Higher transfer speed
- Less vulnerable to interference

· **Disadvantages**

- Shorter range
- Harder time penetrating solid objects

802.11 Channel Access

RF is an openly shared medium since we operate in a license-free space with 802.11 such as 2.4 GHz, portions of the 5 GHz all the way down to 50 GHz for some of the television whitespace and all the way up to 60 GHz with 802.11a/d or Multi-Gigabit (DMG) devices physical layers. There is more frequency space that we use today than ever with 802.11, however, the one thing they all share in common is that they are openly shared medium. Meaning, multiple devices on the same channel must share access and the device cannot detect what is happening somewhere else. There is no way for a transmitting station to know as it is sending information that the receiving station does not have interference or some other factor that might be impacting it there.

Quick Notes:

· RF is an open medium

· Multiple devices in the same channel must share access

· Devices cannot detect what is happening in other locations

· An algorithm is needed to assist in the prevention of collisions (Collision Avoidance)

· Devices should be able to detect signals at the lowest modulation rate within the channel

· This is the primary key to proper WLAN shared access

The wireless technology has helped us to transfer data from one device to another without using wires or cables. Using this technology, we can now establish a network is more flexible, intangible and has ease of access.

The use of smartphones or tablets or any other wireless devices that support Wi-Fi, wireless networking has allowed us to move around an area without hesitation since the device is still connected to the network.

In wires connection, data passes through cables whereas in wireless connection the data is passing through radio frequency (RF) signal.

The frequency of the Radio Frequency or RF signals ranges from 30kHz to 300 GHz, it falls under the category of EM waves or electromagnetic waves. Light is a good example of an electromagnetic wave; however, we can see a light as it passes through, RF signal ,on the other hand, is completely not visible to us.

In radios, FM radio stations use RF signals to broadcast signals. The frequency signal being used is frequently the same as the station name, for example, KIIS-FM 102.7 (the 102.7 in the station name is the frequency it uses).

RF Signal range: 30kHz to 300 GHz

Types of Wireless Network

- Wireless LAN
- Wireless MAN
- Wireless WAN
- Wireless PAN

Wireless LAN (Local Area Network)

This is a network where there are two or more computers or devices connected to the network and it only covers a limited area, for example, a home or small business. The NIC is sed in this type of network, we often call this the Peer-to-Peer Network (P2P). Another form of this is an ad-hoc network which is used temporarily.

Unlike using the switch in a wired network, in the WLAN setup, we use a device called an access point. This is a central device from which the RF

signal is being generated. WLAN which uses the access point is called Basic Service Set (BSS), it acts as the coordinator between different devices within the network.

Wi-Fi

RF signal Frequency: 2.4 GHz or 5 GHz

Range: 100 meters

Wi-Fi products are certified and tested by the Wi-Fi Alliance

Wireless MAN (Wireless Metropolitan Area Network)

Collected unit of many WLANs located at various places

Uses WIMAX technology (Worldwide Interoperability for Microwave Access) which is controlled by WiMAX Forum

Maximum Speed: 1 Gbits/ sec

IEEE 802.16 Standard

WWAN (Wireless Wide Area Network)

This is an extensive network that has been distributed across an immense amount of space. It connects cities together. Mobile phones use WWAN to make communication possible.

The technology in WWAN are subdivided in generations: 2G, 3G,

Time Evolution

In 1G in the 2980s, the only single voice was going from one device to another device. The analog protocol was being utilized during this period. In mid 1980s 2G network has introduced, with it came voice and text capabilities. Both voice and text messages are going from one device to another device with the use of digital standards. The speed from 1G (2.4 kbps) has increased when 2G was invented (16 kbps). In 2003, 3G has evolved from voice and text, with now including data. It uses multimedia technologies and has a speed of up to 2 Mb per second. In 2009 4G was

introduced to the market, this technology allows the voice to go through data. IP protocol is utilized, and the speed can reach up to 100 Mb per second. 5G technology is the next one to hit the market soon, it will have more bandwidth mobility which a key factor for it would be to succeed.

WPAN (Wireless Personal Area Network)

This kind of network is used smaller distance

Technologies that are mostly used for WPAN are Bluetooth and Infrared Data Association

Bluetooth

- Uses ISM band of 2.4 GHz
- Speed of up to 721Kbps
- Range goes anywhere between 10 to 100 meters

If you are using Bluetooth technology, let's say in your headset or keyboard or speakers and it is connected to your smartphone or tablet, this is an example of a personal wireless area network

VLAN (Virtual Local Area Network)

A VLAN is a local area network where the computers, servers, and other network devices are logically connected regardless of their physical location. This means, even if the devices connected to the network are scattered in different places, it would not matter because a VLAN can logically group these devices into separate virtual networks.

The purposes of a VLAN

- Improved security
- Traffic management
- Make a network simpler

A VLAN capable switch can logically create several virtual networks to separate network broadcast traffic. This can be done by designating specific

ports on the switch and assigning those ports to a specific VLAN.

Security Options

Data can be easily hacked in Wireless Networks without using proper security protocols. RF signals can be intercepted by other antennas.

IEEE Standards

The acronym stands for Institute of Electrical and Electronics Engineers.

Since there are various types of technology available for wireless networks, IEEE was established to determine standards for the functioning of wireless networks.

Most networking standards are designed by thr 802 LAN/MAN Standards Committee.

IEEE Wireless Standards

- The first Wireless LAN was successfully made in 1997
- IEEE 802.11 Standard was designed because of WLAN
- Frequency used: 2.4 GHz
- Maximum Speed: 2Mbps
- This is now referred to as 802.11 Legacy

802.11a

Frequency: 5 GHz

Maximum Speed: 54 Mbps

802.11b

Frequency: 2.4 GHz

Maximum Speed: 11 Mbps

These standards were introduced in the same year in the late 1990s

802.11g

Frequency: 2.4 GHz

Maximum Speed: 54 Mbps

Introduced in 2003

802.11n

Frequency: 2.4 GHz and 5 GHz

Maximum Speed: 300 Mbps

Usual drawbacks of Wireless Networking

· RF signal strength gets weaker as the distance increases

· The signal may be affected by structures like concrete walls, big objects, and other similar items

· Unsecured signal can be easily targeted for hacking and can be intercepted

CHAPTER 10: COMMUNICATION SYSTEM AND WIRELESS NETWORKS

A wide territory organizes (WAN) is a media communications arrange, normally utilized for associating PCs, which traverses a wide land region, for example, between various urban communities, states, or even nations. WANs normally are utilized by partnerships or associations to encourage the trading of information between their PCs in scattered workplaces. Overall enterprises, most enormous organizations with offices at different areas use WANs, and even free organizations with just two local areas logically use WANs. Most WANs interface at any rate two neighborhoods (LANs) and the Internet is on a very basic level an immense WAN.

Even though WANs fill a need like that of LANs, WANs are sorted out and worked out of the blue. The customer of a WAN as a general rule does not have the correspondence lines that interface the remote PC frameworks however rather buys into an administration through a media communications supplier. In contrast to LANs, WANs normally don't connect singular PCs, however rather are used to interface LANs in what are known as internetworks, using devices called switches and remote augmentations.

Even though WANs fill a need like that of LANs, WANs are organized and worked unexpectedly. The client of a WAN, for the most part, does not claim the correspondence lines that associate the remote PC frameworks yet rather buys into an administration through a broadcast communications supplier. In contrast to LANs, WANs ordinarily don't interface singular PCs, yet rather are utilized to connect LANs in what are known as internetworks, utilizing gadgets called switches and remote scaffolds.

WANs additionally transmit information at much more slow speeds than LANs, most regularly at about 1.5 megabits every second (Mbps) or less, rather than the tens, hundreds, or even a huge number of Mbps accomplished by LANs. WANs are basically like metropolitan zone systems (MANs), yet are ordinarily increasingly slow interchanges joins for separations more noteworthy than 50 kilometers.

WANs have existed for a considerable length of time, yet innovations, administrations, and applications have created throughout the years. WANs were initially created for advanced rented line administrations conveying just voice, instead of information. Accordingly, they associated the private branch trades (PBXs) of remote workplaces of a similar organization. WANs are as yet utilized for voice administrations, however, they are utilized most vigorously for information and, as of late, additionally for pictures, for example, video conferencing. WAN utilization is developing, as more organizations have introduced LANs and as progressively moderate internetworking hardware has turned out to be accessible.

Even though WANs fill a need like that of LANs, WANs are sorted out and worked out of the blue. The customer of a WAN normally does not have the correspondence lines that interface the remote PC structures anyway rather gets tied up with an organization through a media interchanges provider. As opposed to LANs, WANs normally don't associate particular PCs, yet rather are used to interface LANs in what are known as internetworks, using contraptions called switches and remote frameworks. WANs moreover transmit data at significantly more moderate rates than LANs, most for the most part at about 1.5 megabits consistently (Mbps) or less, as opposed to the tens, hundreds, or even a considerable number of Mbps achieved by LANs. WANs are in a general sense like metropolitan zone frameworks (MANs), be that as it may, are conventionally progressively moderate trades joins for partitions more unmistakable than 50 kilometers.

Point to Point services

The fundamental sort of point-to-point WAN development in North America is TI, which relies upon a strategy for disengaging a propelled line organization with a pace of 1.544 Mbps into 24 channels of 64 Kbps each. By recent rules, this rate is respectably moderate appeared differently concerning LAN advancement and stood out from the extending corporate

solicitations set on LANs. The cost of setting up and leasing a TI (or the snappier T3) addresses a sizable expense for associations. In the mid-1990s pretty much all WANs used Ti or other leased lines, which are leased from a media correspondences transporter, yet this changed rapidly as more affordable and faster alternatives rose. Various onlookers have guessed the sharp lessening of leased line benefits once the system is set up to all the more probable assistance the more exceptional, increasingly moderate alternatives. Other point-to-point organizations open consolidate fragmentary Tl, T3, information telephone automated organizations, traded 56 Kbps, composed organizations propelled framework (ISDN), and digressed propelled endorser line (ADSL). ADSL and practically identical DSL developments drew a great deal of thought from corporate framework chairmen in the late 1990s since they were widely more reasonable than leased lines—as much as 60 percent less and passed on relative or better execution.

Despite their average amazing costs, another drawback to point-to-point arrangements is that they aren't fitting to oblige convenient customers, e.g., business voyagers. Since the organizations are associated exceptionally to unequivocal territories, associations must find elective techniques for framework access for versatile customers. Group traded frameworks organization gives this limit, among various points of interest.

Group Switched Services

WAN advancements that rely upon open frameworks utilizing package trading, a system for encoding data into little, amazingly recognized pieces known as groups, have been logically renowned over the earlier decade. Two of the most noteworthy pack based developments are edge hand-off and non-concurrent move mode (ATM).

Packaging move is the more prepared of the two, coming into general use in the mid-1990s. It was in the colossal segment a substitution to the slower X.25 standard that had been around since the mid-1970s. Most packaging hand-off WANs are encouraged by businesses to sort out chairmen that charge level rates subject to the speed of organization or volume of data required. Supported by decently modest frameworks organization hardware, diagram handoff relies upon structure up a predictable or virtual circuit over a framework with another PC. In packaging hand-off, the groups, or edges,

of data may change in size, and no undertaking is made to address botches. This keeps going part relies upon the assumption that packaging move is continued running over the commonly high gauge, automated frameworks, and the data is less weak to botches. This is like manner improves speed since the framework show isn't endeavoring to address the data. The reliability of this affiliation licenses packaging move master centers to guarantee a particular least level of organization. The close to insignificant exertion and high bore of the organization made edge move one of the most noticeable WAN developments during the 1990s.

ATM organizations, which were introduced monetarily in the mid-1990s, contingent upon relative gauges. Many have touted ATM as a jump forward development, anyway as of the late 1990s it had only an unassuming impact on the WAN market. ATM uses a thought called cell to move to transmit data. Cells are reliably evaluated, little packages of data; by ATM, just 53 bytes each, including a 5-byte header. Then again, a packaging hand-off bundle may range up to a couple of thousand bytes. Correspondingly, similarly as with edge hand-off, ATM moves data over a portrayed virtual path as opposed to empowering groups to seek after any number of approaches to their objectives, as occurs in TCP/IP shows used in Internet applications. This particularly relentless affiliation fits video and various applications that require a reliable, obvious movement of data. The weaknesses to this sureness are that the enduring level of organization may below stood out from various decisions, an ATM may not be all around arranged to regulate transient spikes looked for after for framework resources.

Fiber Optic network

Fiber-optic accessibility for WANs is another huge innovative work in an area. Fiber optics, which incorporate sending light banner through glass or plastic fibers, can reinforce brisk and incredibly astonishing data move. Most fiber-optic frameworks use some sort of group trading advancement, for instance, ATM.

One creating a standard in this field is a synchronous optical framework (SONET), a lot of shows grasped by the American National Standards Institute (ANSI) for high-transmission limit fiber-optic frameworks organization. The all-inclusive easy to SONET is known as the synchronous

modernized pecking request (SDH). While its specific advantages have been recognized by a couple of, others note that the monetary issues of SONET are less captivating. It has exhibited expensive to execute, and a couple of critics promise it wasn't organized properly to manage overpowering data traffic that associations need such benefits for. Regardless, gigantic associations with generous throughput necessities have begun to connect to SONET-based organizations.

A battling, and even more fiscally persuading, standard is thick wavelength division multiplexing (DWDM). DWDM is a system for capably sharing give up the fiber by changing the piece of the light go for each phenomenal stream of data. By using each fiber even more capably, DWDM allows inside and out higher exchange speeds for data than SONET, which relies upon time-division multiplexing (TDM) or conveying time to each unique stream of data on a fixed rotate. This proselyte into extensive cost speculation assets on gear as well. DWDM development was overall rapidly sent by different framework overseers because of such focal points. While the Internet and different frameworks organization progressions have changed the quintessence of WANs and have bargained some progressively prepared kinds of WAN development, different authorities acknowledge they will end up being increasingly huge instead of less, as examples can envision globalization and telecommuting make new enthusiasm for high control long-partition arranging. Enthusiasm for framework information move limit will continue swelling. One advancement measure saw corporate WAN traffic climbing by as much as 30 percent a year through 2002, and a lot of this traffic will dynamically be coordinated through open frameworks using virtual private framework development rather than the shut private previous frameworks.

Advantages of WAN

Brings together IT framework-Many think about this present WAN's top preferred position. A WAN takes out the need to purchase email or record servers for every office. Rather, you just need to set up one at your head office's server farm. Setting up a WAN additionally streamlines server the board, since you won't need to help, back-up, host, or physically secure a few units. Additionally, setting up a WAN gives huge economies of scale by giving a focal pool of IT assets the entire organization can take advantage of.

Lifts your security -Setting up a WAN enables you to impart touchy information to every one of your destinations without sending the data over the Internet. Having your WAN scramble your information before you send it includes an additional layer of insurance for any secret material you might move. With such huge numbers of programmers out there simply kicking the bucket to take delicate corporate information, a business needs all the security it can get from system interruptions.

Expands transmission capacity -Corporate WANS regularly utilize rented lines rather than broadband associations with the structure the foundation of their systems. Utilizing rented lines offers a few pluses for an organization, including higher transfer speeds than your run of the mill broadband associations. Corporate WANS additionally commonly offer boundless month to month information move limits, so you can utilize these connections as much as you can imagine without boosting costs. Improved correspondences increment proficiency as well as lift profitability.

Disposes of Need for ISDN -WANs can slash expenses by wiping out the need to lease costly ISDN circuits for telephone calls. Rather, you can have your WAN convey them. If your WAN supplier "organizes voice traffic," you likely won't perceive any drop off in voice quality, either. You may likewise profit by a lot less expensive call rates when contrasted with calls made utilizing ISDN circuits. A few organizations utilize a half and half approach. They have inbound brings come over ISDN and outbound brings go over the WAN. This methodology won't set aside you like a lot of money, yet it will even now bring down your bill.

Ensured uptime -Many WAN suppliers offer business-class support. That implies you get a particular measure of uptime month to month, quarterly, or yearly as a component of your SLA. They may likewise offer you nonstop help. Ensured uptime is a major in addition to regardless of what your industry. Let's be honest. No organization can bear to be down for any time allotment in the present business condition given the stringent requests of current clients.

Cuts costs, increment benefits -notwithstanding taking out the requirement for ISDN, WANs can enable you to cut expenses and increment benefits in a wide assortment of different ways. For instance, WANS kill or altogether decrease the expenses of social occasion groups

from various workplaces in a single area. Your promoting group in the United States can work intimately with your assembling group in Germany utilizing video conferencing and email. Saving money on the movement costs alone could make putting resources into a WAN a reasonable alternative for you.

Technical support -Notwithstanding offering help for a wide assortment of utilizations and countless terminals, WANs enable organizations to grow their systems through module associations over areas and lift interconnectivity by utilizing portals, scaffolds, and switches. Besides, by bringing together organize the board and observing of utilization and execution, WANS guarantees the greatest accessibility and unwavering quality.

Disadvantages of WAN

High arrangement costs — WANs are confused and complex, so they are fairly costly to set up. Clearly, the greater the WAN, the costlier it is to set up. One reason that the arrangement expenses are high is the need to associate remote zones. In any case, by utilizing open systems, you can set up a WAN utilizing just programming (SD-WAN), which diminishes arrangement costs. Remember additionally that the value/execution proportion of WANs is preferable now over 10 years or so back.

Security Concerns — WANs open the path for particular sorts of inward security breaks, for example, unapproved use, data robbery, and malignant harm to documents. While numerous organizations have some security set up with regards to the branches, they send the majority of their security at their server farms to control and oversee data sent to their areas. This technique decreases the executives' costs yet restrains the organization's capacity to manage security breaks at their areas. A few organizations additionally experience serious difficulties compacting and quickening SSL traffic without fundamentally expanding security vulnerabilities and making new administration challenges.

Support Issues-Maintaining a WAN is a test, no uncertainty about it. Ensuring that your server farm will be up and working every minute of every day is the greatest upkeep challenge of all. Server farm supervisors must most likely distinguish disappointments before they happen and

decrease server farm personal time however much as could reasonably be expected, paying little respect to the reasons.

CHAPTER 11: MOBILE WIRELESS NETWORK

Setting up a computer system network is very useful in every business. It makes communication between the computers an easier job, sharing the necessary data quickly and safely. Depending on the size of the network you want to create, you will need specific elements. Here is a list of the essential items you will need to start:

- Computer systems: You will need to have at least two computer systems to start a network. These can be a desktop or laptop, and they do not necessarily need to be in the same room. Other devices such as notebooks and tablets can be included in the network as computer systems. The network also connects the computer systems with computer accessories like printers, scanners, etc.

- Handy Tools: For some of the installations, you will need to have some tools. The most important one will be a screwdriver. If you can, use an antistatic wrist strap or be sure to have rubber shoes to prevent electric shocks. If it is a wired installation, you will probably need to have a drill to open holes and insert the wires so you can link the computer systems through the rooms.

- Modem with a broadband internet connection: This element is essential for a wireless connection, but it can also be handy for all the different installations. It provides the Internet to the computer systems linked through the network, making it easier to communicate.

- Wireless Router and Ethernet cables: Depending on the kind of installation, you will need wireless routers or Ethernet cables to link the computer systems. For a wireless network, your computers systems should have a wireless network adapter. Most of the portable computing devices already have it installed on their systems, and even some desktops have

one. If not, you need to acquire and install this device on your computer systems.

Types of Network

LAN: A LAN, or Local Area Network, is a network connection that is set in a specific area, like a house, an office or a building. Although computer systems don't need to be close to one another, they have to be inside the specific area. Currently, Virtual LAN is becoming more common when talking about setting up a network; wiring can take time and is more expensive.

Pros

- You can share information with other computers and computer accessories quickly. It makes it easier to send the final product to an output source like an external hard drive for storage, or print it.

- You can keep all the crucial data and information in one computer system. If you need to retrieve data from another computer, you can use a password and log in. It saves space and keeps the information secure.

- You can share a program license without having to buy one for each computer system. You don't even need to install the program on all the computers, connect directly to the main network through your device to use it.

- It is easy to install, and you don't need to be an expert. There are many video tutorials and webpages that explain how to make a Local Area Network.

Cons

- The network is limited to an area. You can’t work from home, or check information outside the building.

- You need to install a particular program to set up a LAN, what you need an administrator to keep everything going. It means it is a significant investment to do.

- If data is corrupted, it will probably be damaged in all the computers. An infected computer can infect the rest of them through the network.

WAN: A Wide Area Network allows you to set a network without the limitation of area. It works excellently for companies that have stores in different regions of the city or other cities. You need to have access to the Internet to set up a WAN.

Pros

- You don't have space limitations. You can have all the pertinent data in a central office, and manage all the other computer systems around the country. It helps communication between other locals, check inventory, and keep order without leaving your workspace or your home.

- It allows more advanced network technologies, setting exclusive passwords and software to make the net more difficult to hack or corrupt.

Cons

- It is costly because it requires specific connection plans, and the installation must be done in every workspace. You will need to pay monthly to have continuous internet service.

- It can be slow because of Internet traffic, and it can be interrupted if there are problems with the antenna that transmit the information.

- It needs continuous maintenance to secure that the software works correctly, and it has to be done by a professional.

MAN: MAN refers to Metropolitan Area Network. It is a net compound by smaller local area networks (LANs) and is used more like a network for a large area like universities. They can connect to the LAN of every building into a central system.

Pros

- It uses a fiber-optic cable and other high-technology bandwidth to allow faster communication between the computer systems. Different departments can share relevant information in a few seconds; a file can be sent to a printer in another building. A massive memo can arrive in all the computer systems connected to the network at the same time.

- It allows economizing in the cost of the Internet and other services, dividing the expenses between the users. At the same time, they all share a

high-quality internet. It is not as fast as the LAN network connection but is faster than the WAN network.

Cons

- It is costly to install, and not all companies can offer this service. The technology it uses is the newest in the market. It can't use older installations, like other networks, so everything has to be installed for the first time, which means breaking walls and changing wires. It is a lot of work.

- You need to install the first several LAN networks in the buildings you wish to connect, so it takes more time and investment to be done.

Setting up each type

Depending on the network, you may have to hire a third party to make part of the installation, while others can be done by yourself. It implies knowledge of hardware installation to the search and setup of specific software.

For LAN:

- Once you have all the elements for the installation mentioned above, you need to select the central computer system. If it is the first time connecting the router to the computer, a "wizard" or installation helper program should appear and ask to create a network. If it is not new, go to Control Panel and look for the Network and Sharing Centre and select the option to set up a new system.

- If you want it to be a virtual LAN or if you're going to share the Internet between the computer settings, you then must set up the Wi-Fi. The manual of the router already has instructions for its installation. If you are not going to share the internet, go to the next step.

- Connect all the computer systems and computer accessories with a wire or through the wireless router. Some of the devices, like the printer, will need further instructions. In Control Panel, you will have to select Devices and Printers and click on the Add Printer.

Now you are ready to start sharing information in your small business or setting a game night with your friends in the house.

For WAN:

- You will need to have broadband Internet service with a company that provides it. These companies already have WAN plans to offer, so check which one would work for the kind of business you have. They will install the equipment in every building that will be connected to the WAN network.

- Connect the router to the WAN. This step usually is already made by the company when they install the service. In case they don't, you must find a router that can connect with that specific WAN circuit.

- Then it is time to connect all the computer systems to the router. You can do it via Wi-Fi, or use Ethernet cables to link the different devices. Do this process in all the stores or buildings that you want to connect to your WAN network, and you will be ready to start your business in other cities.

For MAN:

- To set up a MAN network, you need to have set a LAN network in every building you want to connect into one interface. You will also need to have broadband Internet service, optical fibers, and router devices to link all the LAN networks to a central system.

- Once you have followed the steps of how to install a LAN network in all the buildings, you must select which building will have a central computer system. There you will set the Internet service and the main router that will then interlink with the other routers in the different buildings.

Choosing the network for you

Each computer system network has its advantages and disadvantages. These reside mostly on the distances they can reach and the speed of the connection between the devices.

LAN: The LAN network is the best option for an office building and home installations. It allows setting many different computer systems, computer accessories, and other mobile devices into the same network as long as the

devices are inside the area. You can share information faster than with other networks, link software and programs so the computers can work with it without having to install them in all of them, nor paying a license for each machine. It can be set up without hiring a professional. It can cover up an area from 100 to 1000 meters.

WAN: The Wide Area Network is perfect for business with multiple stores and branch offices. Whether they are in the same city or many cities around the country, it allows them to keep track of the management of each store, so all the offices can offer the same service with the same quality. It can have a slower connection, but the information will arrive, making the communication safer. The range of the WAN can even reach to other countries, as far as 100.000 km.

MAN: The MAN network doesn't reach as far as a WAN, but reaches further than a LAN. It is best for universities or big hospitals, where they need to connect the different buildings and departments into one network. The internet connection is not as good as the LAN, but it is faster than the WAN. The Metropolitan Area Network is the middle option between the other two networks, but it needs LAN networks to work. The range of the Metropolitan Area Network is between 50 meters to 100 km.

CHAPTER 12: NETWORKS AND COMMUNICATION SYSTEMS

PING Utility

The ping command is the most widely used of all network utilities. It is a tool that is used to test issues such as network connectivity and name resolution

In some cases, you might get a result from a ping that says, “request timed out”, this could mean that the host network is down, or it is blocking all the ping requests.

Another message that you might get is “destination host unreachable”, that message is coming from the router, that means that the route to the destination cannot be found.

The ping command can also be used to test DNS name resolution issues. Instead of using the IP address in the ping command, try using the domain name of the website you are trying to reach. For example, type “ping” space, the domain name, then hit enter. If by pinging the domain name, if you get the same successful result as typing the IP address when you ping the same destination, then this would indicate that the name resolution by the DNS is working fine.

If you ping the domain name and it failed, then the next step is typing the ip address instead. If by typing the IP address and the ping is successful this time, then you can isolate the issue to DNS

Trace Route Utility

Tracert is used to find the exact path the data packet is taking on its way to the destination.

For example: to trace a route from one computer to another, key in "tracert" space, then the destination computer's IP address at the command prompt,

then press enter. By doing this, the data packet will find its way to the destination. Each time the data reaches a router on its path, it will report back information about that router such as its IP address and the time it took between each hop.

TraceRT utility is a great tool that can be used to pinpoint where the problem lies within a network if the data cannot reach its destination.

IPCONFIG

This is a useful tool to display network configurations for your computer and this information can be used as part of the problem-solving process.

- Ipconfig – shows the default gateway, the IP address, and the subnet mask
- Ipconfig /all – shows the full TCP/IP configuration
- Ipconfig /renew - releases and renew the IP address lease
- Ipconfig /release - releases the IP address lease

CHAPTER 13: WIRELESS NETWORK TECHNOLOGY

CISCO SYSTEM

CISCO is unarguably the largest networking company in the world. The San Jose, California-based multinational technology conglomerate located in Silicon Valley has proved to be the leader in wireless technology with over three decades of experience in the field. CISCO is reputable for developing, manufacturing, and selling telecommunications equipment, networking hardware, and some other high-technology products and services. Since its acquisition of some subsidiaries such as WebEx, Jasper, OpenDNS, and Jabber, the company has also proved to be an expert in some specific technology markets such as domain security, Internet of Things (IoT), and energy management. Founded in December 1984 by two computer scientists from Stanford University, Sandy Lerner and Leonard Bosack, the company is responsible for pioneering the concept of Local Area Network (LAN). Today, the multibillion-dollar company has continued to set the pace in networking.

CCENT

The Cisco Certified Entry Networking Technicians is the lowest certification level offered by this company. This certification covers the fundamental networking knowledge, and CCENT certified individuals can perform some operations such as installation, management, and troubleshooting on small enterprise networks. They can also carry out some basic network security on such networks as well. Having a CCENT certification is the prerequisite for CCNA certification in order to enable a potential networker to understand the rudiments of networking before dabbling into it. In 2017, the company introduced two new examinations, ICND1 and ICND2, that prepare potential networkers in advance for

CCNA. It also prepares such individuals for CCNA Voice, CCNA Security, and CCNA Wireless.

Another entry level certification is the Cisco Certified Technicians (CCT). This certification empowers technicians certified by the company to diagnose Cisco networking challenges. They can also restore and repair the network after a successful diagnosis. The technicians work in alliance with the Cisco Technical Assistance Center (CTAC) for prompt resolution of support incidents. There are two domains for individuals who are interested in CCT certification. These are:

- CCT Routing and Switching, a program that is valid for 3 years
- CCT Data Center, also valid for 3 years as well

The 3-year validity period requires that certification holders must register for the same level Cisco recertification exams or recertification exams at a higher level and pass the exams every 3 years to retain their certification.

CCNA/CCDA

The CCNA (Cisco Certified Network Associate) certification is an IT-based certification from this networking giant. Over the years, the Cisco exams have been modified. In a 2013 release, the company announced its desire to update this program so that the program “aligns certification and training curricula with evolving industry job roles.”

The modifications to the certification have given rise to several types of CCNA certification. Thus, the certification currently focuses on cloud, security, CCNA Routing and Switching, security operations, collaboration, data center technologies, service providers, industrial plants, design, and wireless.

Out of all these different types, the Routing and Switching sector is the closest to the original purpose of establishing the CCNA program. The certification “covers skills necessary to administer devices on small or medium-sized networks.” Thus, specialists in that field can easily provide networking solutions to networks that are designed for use on a small or medium scale. To get this certification, a potential candidate is expected to

have passed the ICND1 and ICND2 examinations. These exams are designed to serve as a prerequisite to some other certifications such as CCDA, CCNP, CCDP, and other advanced certifications. Like other certifications previously mentioned, CCNA certifications equally have a validity period of 3 years.

CCNP/CCDP

The CCNP is one of the most important professional certification programs for LANs and WANs. The Cisco Certified Network Profession (CCNP) validates the candidate's skills and knowledge required for installing, configuring, and troubleshooting LANs and WANs with up to 500 end-devices. Before you can obtain this certification, you must already have a valid CCNA certification. There are different CCNP certifications as well. Each of these certifications is designed to address a specific networking or cybersecurity issue. On the list of these certifications are:

- **CCNP Security:** This is formerly referred to as Cisco Certified Security Professional (CCSP). The certification program prepares a candidate for the job a Cisco Network Security Engineer. The responsibilities of the Cisco-certified engineer include security in switches, routers, appliances, and networking devices. He is also responsible for choosing firewalls as well as supporting, deploying, and troubleshooting them. He carries out the same operation for VPNs in addition to providing IDS/IPS solutions. A prerequisite to the CCNP Security certification is the CCNA Security or any other related CCIE certification.
- **CCNP Wireless:** The CCNP Wireless certification takes care of all aspects of the principles and theory of wireless networking. Before a candidate can be awarded the CCNP Wireless certification, he or she must have passed these four tests: Wireless Voice Networks, Wireless Mobility Services, Wireless Site Survey, and

Wireless Security. These prerequisites are used instead of the CCNA Wireless certification.

- **CCDP:** There is also the CCDP certification where people are trained to become network professionals. As a professional, you will be trained in the art of discussing, designing, and creating advanced security, data centers, network management, and advanced addressing and routing.

CCIE/CCDE

Next is the Cisco Certified Internetwork Expert. This is the highest certification offered by this company, and the holders are considered as experts with the "most technically advanced IT certification." This is supported by the result of a survey that revealed that CCIE Certification is the "highest salaried certification in IT salary surveys."

Although there are no formal prerequisites for the CCIE exams at the moment, potential candidates are advised to have a minimum of three years of networking experience.

The CCDE certification program runs parallel with the more popular CCIE program and provides a higher skill-set than what the CCIE can offer in some areas. Specifically, the certification focuses on network professionals with commendable network design skills. The network design will be used for translating business requirements into an effective network design that will contribute to network integration and expansion.

CCAR

The competence and experience of network designers are assessed by the Cisco Certified Architect (CCAr). The networkers are groomed to provide the needed support for the ever-increasing number of the complex network of organizations around the globe. They must also possess the skills for effectively translating business strategies directly into technical strategies. Awarding CCAr certification is a complete deviation from the norm. Candidates who apply for this certification are required to propose the perfect architecture solution to some business requirements. While defending their proposal before a board, the candidates may have to make

on-the-spot modifications to the proposal according to a set of requirements provided by the exam board. The prerequisite to this certification includes up to 10 years' experience in the networking industry, a CCDE certification, and acceptance into the certification program through an application process.

As a Cisco Certified Architect, you have these responsibilities:

- Lead the creation and the evolution of architecture for enterprises
- Analyze the relevant technology and the trends in the industry market
- Establishing principles that will govern Enterprise networks
- Selection of the appropriate products and technology for the Enterprise network
- Identification of the resources needed by an organization
- Leading the development of the education and communication plan for the architecture of an enterprise network

The importance of all these certifications will not be lost if you consider the huge importance of networking to wireless communication. It is obvious that the communication cannot be possible if the devices are not connected to each other, a role that experts at Cisco can play well.

CISCO HOME

As a part of its effort to make networking easier and easily applicable to all facets of our lives, Cisco went ahead to incorporate home networking into the industry. This affords a homeowner to fully enjoy the benefits of networking.

CISCO PACKET TRACER

The Cisco Packet Tracer is a very powerful and innovative networking simulation tool. This efficient tool is used for practicing networking and troubleshooting networking problems. Cisco systems designed this tool for creating network topologies as well as imitating the existing computer networks. With this system, you can easily simulate how Cisco switches and routers are created through a command line interface that is equally simulated. Through its drag and drop feature, users can easily remove or add network devices according to their specific needs.

Thus, the tool can be used for stimulating home networking and get mastery over the concept before putting your networking skills to use. The tool will assist you to understand some concepts such as IT essentials, Cybersecurity essentials, Networking essentials, and other networking concepts you learn during your networking classes. This will have a positive impact on your networking skills in the long run as you convert your home into a mini networking project.

CHAPTER 14: WHAT'S HOME NETWORK

A home network simply refers to the internal network you put up in your home to connect your computer and other devices in your home to each other. They are also connected to the Internet via a router, in this case, a wireless router. The home network is a Local Area Network (LAN) that can help you with file sharing, the use of printers, and other valuable uses. The modern networking technology has made it possible to connect everything in your home – thermostats, air-conditioners, garage doors, lights, and what have you – and have all these devices controlled with your mobile device.

The Internet of Things (IoT) is a new technology that makes it pretty easy to have all the electronic devices in your home connected together and controlled by a simple mobile device. Thus, whether you are at home or away from home, you can easily switch on/off the security light, control some of your gadgets, or do some other things that were previously considered impossible. That is the power of networking. You can read more about the Internet of Things to have a better understanding of how this technology works. You can equally increase your knowledge of how home automation works by reading this informative article by Molly Edmonds and Nathan Chandler, "***How Smart Homes Work*** ."

THE COMPONENTS OF A HOME NETWORK

A home network, or home automation, cannot be achieved without the right set of components. Each component plays a significant role in ensuring that the right environment and devices are available for connecting all the devices of a home to make it easy for the homeowner to communicate with these devices without much fuss. This article entitled "***Smart Home Systems: Everything You Need to Know*** " will give you a complete guide on the components of a home network and how the components connect to each other. However, let me give you a brief explanation on this issue. If

you are passionate about building a home network, there are some networking components you can't do without. These components are:

Wireless Access Point: This component is used for connecting Wi-Fi equipped devices in your home to the Internet.

Wireless router: With a router, you can easily connect your home network to the Internet. It serves as a bridge between the Internet and your home. ***Functions and features of routers for home computer networks*** are extensively discussed by Bradley Mitchell. You can equally learn how to set up your home network with a wireless router if you go through this ***network hardware guide*** .

Broadband filters: A broadband filter is a necessity when setting up a home network. Once you activate your line with broadband, it will automatically carry 2 signals: a digital (broadband) and an analog (phone) signal. These signals are not carried at the same frequencies. Thus, in order to receive these signals without quality issues, it is imperative that you connect all your devices into this filter. This will allow you to use the Internet while receiving your faxes or on the phone.

If you fail to connect the devices to the Broadband filters, these are a couple of the problems you have to contend with:

The broadband service will have connection issues.

The Internet connection may drop intermittently.

When you plug in the modem, you may experience a bad or fuzzy telephone connection.

A network bridge: This is useful for connecting different networks such as connecting a wired device to a wireless network.

A network switch: The switch serves as the central networking hub and contains some Ethernet ports that are handy when multiple networked devices are to be connected together.

A broadband modem: The modem can also be used for establishing a connection between the network and the Internet. If you wish, a cable modem that uses a cable Internet connection can be used for this

purpose. Alternatively, you have the DSL modem that uses a phone line at your disposal as well.

This beginner's guide into ***how to set up a home network*** will give you a step-by-step networking approach that will simplify home networking.

WIRELESS SETTINGS

The numerous benefits of a wireless home include the ability to get online from outside your house. This requires giving your home network the right settings to make that possible. Cisco has provided a convenient means of setting up a wireless network. ***Basic Router Configuration Using Cisco Configuration Professional*** is another beautifully written guide by Cisco that will give you a step-by-step wireless set-up procedure you can use for setting up your home network appropriately.

This is another masterpiece from the company you should check out: "***Cisco 1800 Series Integrated Services Routers Software Configuration Guide.*** " These two articles will be of tremendous assistance in setting your home network without much difficulty.

Cisco router configuration: You can configure your router to give you the best output by using ***Cisco configuration method*** . The tutorial provides an easy-to-follow step-by-step configuration guide that takes you through the whole configuration process from the beginning to the end. In a detailed example, you will learn how to erase, secure, set, configure, and carry out some other tasks on the router during the configuration process.

Cisco wireless LAN controller configuration guide: Apart from configuring your router, you can as well configure your LAN controller. There are different LAN controller configuration options as different networking companies attempt to outdo each other. One of the simplest and detailed guides for LAN controller configuration is this simple guide by Cisco. Check out this article: "***Cisco Wireless LAN Controller Configuration Guide*** " for detailed instructions on how to configure your LAN controller without going through too much stress.

CHAPTER 15: WIRELESS NETWORK APPLICATION

Computer networking is an attractive career that many have set their eyes on. It became a field of interest in the early 2000s and has not gone down the ladder of popularity since. The reason why computer networking continues to be popular is that there is a shortage of professionals that can take up jobs in the field, and yet, it can be an easy way for a person in the field to land a relatively lucrative position and scale-up in a fast-growing company. Whatever side of the debate you lie on, there are some things you should know about beginning a career in networking, expanding. Also, we outline some of the things you will need to be keen on when hunting for a job in this field. Luckily, these tips apply for other jobs in technical careers as well.

JOB TITLES IN NETWORKING

There are several positions when it comes to professional computer networking, and each of them comes with a variation in salaries and a high potential for long-term careers. The only disadvantage with this field is that job titles in networking can always be a source of confusion and not just for beginners but experienced people as well. There may be bombastic or bland titles that may fail to capture the essence of the actual work a professional may need to carry out in the field. There are some job titles that should be clearly spelled out as is done below:

- ✓ **Network administrator.** It is only fair, to begin with, that a large chunk of the discussion in the above sections has been focused on network administration. Basically, the job of a network administrator entails managing and configuring WANs and LANs.
- ✓ **Network engineer.** A network engineer is also called a systems engineer. The job role primarily focuses on system upgrades and

evaluation of vendor products. Also, a systems engineer is always responsible for security testing.

- ✓ **Network technician** . Sometimes, network technicians are referred to as service technicians. The job, in this case, tends to give more focus on setting up, troubleshooting, and repairing both software and hardware products. It is not uncommon to find network technicians traveling to remote locations so they can upgrade fields and offer support as needed.

- ✓ **Network analyst** . A network analyst is also known as a network programmer. Their duties revolve around writing software scripts and programs that are useful in network analysis. Network analysis, in this case, involves monitoring of utilities and diagnostics. They also must evaluate third party products and integrate these products and software technologies into the already existing network environment. Conversely, they can easily build new network environments as well.

- ✓ **Network systems manager** . A network systems manager can also be called an information systems manager. Their main duties revolve around supervision of the work of network administrators, technicians, engineers, and programmers. They have a special focus on longer-range planning and make strategy considerations.

It is vital to realize that there are no uniform salaries in networking; in fact, salaries may vary, depending on different factors. These factors include which organization is in question, the market conditions within the locality, and the skill level and experience of the person being hired. This is why it is important to get into networking with a straight face and realistic expectations. Rarely will you find it a smooth walk in the park, but when you have the passion and determination for the job, you will find that your movement upward is a simple task. Advancement up the career ladder will often carry with it more lucrative opportunities when it comes to networking. Read on for more about gaining experience in networking.

GAINING EXPERIENCE WITH NETWORKING

Well, getting a job in networking can be quite an arduous task. This is because most employers are always seeking employees with experience, but

where are you supposed to gain experience when you are fresh out of college? It is not uncommon to hear job seekers lamenting about this reality, and many people complain that the best and only way to gain experience is through getting hired. These sentiments may be true, despite the many promises of a lucrative job in the IT industry. The conditions are increasingly becoming harder and landing an entry-level position in networking can be difficult. However, you can still gain experience in other ways, as will be discussed in the next paragraphs. With these tips, you can have better chances of getting a good job and faster.

One great tip for gaining experience in networking is to pursue a help desk or programming internship full time in the summer months. Alternatively, you can take up a work-study job in these fields as they will work equally well. Internships are not assuring of the best pay, but the work could turn out to be more interesting or uninteresting for some. If the job is not interesting, there is a likelihood that an individual will not finish a substantial project during the limited time they have there. However, there is a clear advantage for you should you manage to complete your work-study or internship. Besides, you will gain hands-on experience, and you will be adequately trained, so you are ready for the market. With you being able to obtain and work well in these jobs, you demonstrate to your future and potential employers that you have an interest in the networking role you are applying for, and that is exactly what they like to see when hiring.

Another useful tip that can help you to gain experience is to self-study. Being handy can pay, albeit in different ways. One thing for sure, however, is that being hands-on can work in your favor as the skills you have can be useful and powerful when you demonstrate something to a potential employer. For instance, you may have just completed a class project recently. Do not stop there, extend the project in some way that will show that you can think out of the box, and show your abilities. You can also create a personal project that you have not been tasked to and complete it. A good way to start would be, for example, to experiment with network administration tools.

Also, earlier on, I mentioned something about home computer networking. This can be quite a useful way to gain experience. You can start with setting up the networks of friends and family and acting as an administrator for the same, for free. While this may not be the best idea for earning income, it

will provide you with a basic understanding of how networks run. Should you find a job in business, however, remember that business computer networking is more complex. Therefore, you should expect that there is a different level of complexity and that you will use different technologies than you did in the home environment.

Also, the field of networking is vast and can be overwhelming for many people who may just be starting . Instead of trying to eat more than you can chew by mastering every language and trying to keep up with every trend, make your life easier. Simply focus on the basic technologies that will be most important as you enter into the market. Over time, you will realize that you keep learning and keeping up if indeed, your interest is in the computer networking industry. Some core technologies that you can build expertise in include TCP/IP, as this will form a foundation for you to learn other specialized new ones in later life.

EDUCATION AND EXPERIENCE

As a person that is interested in venturing into networking, you may wonder the value that education holds when placed against the value of experience. As you may have noticed by now, a lot of employers seek out employees who have completed a four-year degree in university. This may not make sense in some instances, but it is important because they use this as a gauge for your commitment in the industry and field at large. The technology utilized in networking is not constant, and it keeps changing every other day. This is why employers find it important to know that you possess current information when it comes to networking and that you are willing to learn and adapt in the future as technology continues to change. Certifications in networking help prove that you have the basic knowledge base, but college degrees are the real thing; they demonstrate your general ability to learn.

Experience is also important because it demonstrates that you have skills that are needed for the workplace. The more experience you have in the field, the better because it tends to put you in a better position to get a job. However, nothing beats the combination of experience and education when it comes to getting into networking as a career. This is because when you have both experience and education, it sets you apart from individuals who have one of each.

REPRESENTATION OF THE SKILLS AND ABILITIES

I discussed in the earlier sections that to get into network administration, a person should have a great combination of technical and interpersonal skills. I need to emphasize that interpersonal skills are important, and yet often, they are underrated. Also, you need to understand how to explain and exchange information about technical aspects of networking. You will most likely be working in a team and not alone and having the ability to explain yourself verbally and in writing, both email and formal, you have the advantage of getting the chance to enjoy communicating with other networking professionals throughout your life as you seek to build your career.

Before even going further about the importance of communication skills at the networking workplace, let us start with the initial stages. You will need good communication skills during an interview. Your ability to articulate yourself in the work environment is important, and the interviewers will be looking for possible clues into how well you can be understood within the networking environment as you work in a team. Therefore, understand the jargon used in such places and learn to relax when making conversation about such technical subjects. This is not something that will simply come to you in one day, but over time and with practice, you can learn so much that you can answer impromptu questions when asked. You can learn to articulate yourself through many tactics. For instance, you can visit local job fairs and discuss professional subjects with the people you will find there and with your friends. You will find that you gain indispensable knowledge on these subjects.

Some tips have been outlined above that may not work for people who are already in the field of networking. However, they can be used by those who aspire to venture into fields related to networking. Furthermore, some tips can be used no matter where you are in your career, for instance, visiting job fairs to help polish your skills. I hope that the information given can be of help to you, even in the slightest of ways.

CONCLUSION

Technology has gradually shifted from wired to wireless with broad benefits. However, it doesn’t come without some challenges, too, primarily, security issues. This book has covered all these subjects extensively and has highlighted both the benefits and challenges of wireless technologies. It has also given us an insight into what the world stands to gain from wireless technologies in the future.

These are salient points that keep reminding us of what the world holds for us. It is imperative that you and I take full advantage of these technologies and use them to the full. That’s one of the ways we can enjoy life to the fullest; we have the technologies to get things done better, faster, and easier.