COMPUTER NETWORKING

FIRST-STEP

AN INTRODUCTORY GUIDE TO UNDERSTANDING WIRELESS AND CLOUD TECHNOLOGY, BASIC COMMUNICATIONS SERVICES AND NETWORK SECURITY FOR BEGINNERS.

NORMAN LAURENCE

COMPUTER NETWORKING

FIRST-STEP

AN INTRODUCTORY GUIDE TO UNDERSTANDING WIRELESS AND CLOUD TECHNOLOGY, BASIC COMMUNICATIONS SERVICES AND NETWORK SECURITY FOR BEGINNERS.

NORMAN LAURENCE

Computer Networking First-Step:

An Introductory Guide to Understanding Wireless and Cloud Technology, Basic Communications Services and Network Security for Beginners

written consent and can in no way be considered an endorsement from the trademark holder.

Table of Contents

Introduction

Congratulations on purchasing *Computer Networking First-Step: An Introductory Guide to Understanding Wireless and Cloud Technology, Basic Communications Services and Network Security for Beginners* and thank you for doing so.

The following chapters will discuss the basics of computer networking. In today's world where the internet is ruling on top of everything, it is important for you to know the basics otherwise; you won't be able to stay ahead of others. Although it has been 40 years or so since the advent of the internet, wireless standards are attaining great heights even today. The purpose of this book is to provide you with a concise overview of what the world of computer networking is like and some of the major topics that will help you get started.

You will learn about a variety of transmission methods and also some of the common security threats that need to be dealt with. This is quite a fascinating field and I have tried to place it all in a way that it doesn't seem jargon to you. When it comes to establishing new infrastructure in the world of networking, wireless networks have a big role to play and you will understand it once you read the entire book. This particular sector of computer networking has received a considerable amount of attention from the R & D sectors as well.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible, please enjoy!

Chapter 1: Introduction to Wireless Technology

The present time might have let you allowed to be familiar with the term wireless technology. The term “wireless technology” has a wide circumference to cover in. However, in short, it can be described as connecting people or devices to communicate with each other or transfer data or power without any cable or wire, the technology is called wireless technology. So, to begin with, this new technology, let’s know about its brief history over the past decades.

Small History of Wireless Technology

The root of wireless technology was contained with Heinrich Hertz, a German physicist’s discovery of electromagnetic waves. When he was experimenting with electromagnetic waves between 1885 and 1889, he observed the following:

- the length and velocity of the wave and

- the nature of vibration and susceptibility of the wave to reflection and refraction were similar to that of the heat and light waves.

With his findings, he proved that heat and light are electromagnetic waves. This electromagnetic wave was called the Hertzian wave after the name of Heinrich Hertz and later on, it was told as a radio wave.

The First Wireless Communication

Alexander Graham Bell and Charles Sumner Tainter invented the first photophone in 1880. The photophone was a type of telephone which was conducted through modulated light beams to communicate audio conversation.

Wireless Telegraphy with Long-distance Radio transmission

Italian electrical engineer, Guglielmo Marconi is a pioneer, who worked for a long-time on the long-distance radio transmission. Finally, Marconi worked with German physicist Karl Ferdinand Braun and developed their milestone invention of long-distance wireless telegraphy and they jointly shared the Nobel Prize in 1909.

The Radio, Television, and Satellite

With the development of Marconi’s long-distance radio transmission, the radio has emerged at the beginning of the 20th century. Later on, television has come which receives the broadcasted audio-visual communication without any wire. Satellite is also an example of wireless technology.

Wireless Technology in Today’s Era

Wireless technology today has become a part of everybody’s life. If you ask anyone what they know about wireless technology, they will answer you exemplifying the use of a smartphone, tablet, laptop, modem, etc. However, today, wireless technology is used under two broad categories. They are:

- **Wi-Fi Technology** – Wi-Fi technology connects two devices through radio frequencies (RF) or radio waves. It is commonly used to attach internet router with devices like laptops, tablets, computers, mobile phones to communicate with each other. In fact, Wi-Fi technology is a wireless local area network (WLAN) that runs 802.11 protocols which are developed by the Institute of Electrical and Electronics Engineers (IEEE). The specification that the "802.11 families" use is the Ethernet protocol and the protocol shares its path by following Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CA) mechanism.

Wi-Fi can use both 2.4GHz UHF (Ultra High Frequency) and 5GHz SHF (Super High Frequency). You will be wondering to know that wherever you go, for example, your club, coffee shop, the marketplace, or even you stay at home, you are surrounded and succumbed to the radio waves. Whatever gadget you are using, that may be a cell phone, a Bluetooth earpiece, a baby monitor, a car door opener, a garage opener all are run by the radio frequency and the magnitude of frequency is 2.4GHz. so, you are living your life within 2.4GHz RF.

Now the question is what the number 2.4GHz signifies? It is the frequency of the radio wave that is broadcasted by the cell phone service provider to your handset. The number refers to the oscillation of wave or in other words, it can be said number of times that a wave oscillates in one second. In the case of the computer, it tells you about the speed of the computer's processor or clock's rate. In the case of your television set, it refers to the rate at which your TV set refreshes its screen.

5GHz is a part of the SHF radio spectrum that has been allotted internationally to the amateur radio and satellite users on a secondary basis. Although the user must accept its harmful interference from the Industrial, Scientific, and Medical (ISM) bands. However, it is included in the IEEE C Band spectrum.

Both the band 2.4GHz and 5GHz do not need any license to run from the FCC (Federal Communications Commission) to operate in the

USA.

- **Cellular Networks or Cell Phone Networks** – A cellular network is a network that connects two electronic devices over a long distance to communicate with each other or transfer data. Due to covering a long-distanced frequency re-use is necessary. Usually, the network services are provided with the help of a number of base stations. Each base station covers a small area called a cell. The limited power of a station makes possible to re-use the same frequency from a cell which is located a few cells away from the base station and that too becomes possible without any interference. The cell size differs based on the number of users and traffic per user in the area.

The Market for Wireless Technology

The wireless technology market is widespread and it includes fixed wireless, mobile wireless, portable wireless, IR wireless. When you use wireless technology in your office or your home, you mainly use fixed wireless to connect equipment or devices to get access to the internet through a modem. People use mobile wireless in vehicles, PCS (personal communication services) and cell phones. Portable wireless devices include battery-powered cell phone and personal communication system (PCS). IR (Infrared) wireless is used to transfer data in a controlled system.

What are the Industrial Applications of Wireless Technologies?

Maybe you have been using wireless devices during the last two decades but in industry, it has been using over three decades. First, such an application has been used to crane and Automated Guided Vehicle (AGV) to get flexible controllable access to industrial vehicles. However, the standardized protocol of RF like WLAN (IEEE802.11, IEEE802.15.4) and Bluetooth technology (IEEE802.15.1) have now been playing the most dominating role in the industry. The advantages of wireless technology over industrial applications include:

Chapter 2: Wireless Network Components

By now, you probably might have come to know that a wireless network needs several supporting and compatible components to work on the system properly. Although the system is called wireless, some components in the network are there which are connected by wire in the network. So, a question may come to your mind about why the system is called a wireless network. The answer to this question is a wireless network system is an augmentation of the wired network rather than replacing the wire. The purpose of such an augmented wired network is to extend a wireless network between end-users. By and large, the end users like you are the most important target users of the entire wireless infrastructure. The network as a whole uses radiofrequency to work on either to transmit or receive data through the air. That is why the last few steps of the wireless infrastructure are free of wire connectivity. This procedure gives freedom to the user to get access to the internet at any time at any place. So, to start the discussion with the components used or required in a wireless network system let’s begin with the role and importance of the users in the system.

Role and Importance of End-User

A user in a wireless network refers to either a person or an entity. However, it is generally referring to a person. Suppose you are a businessman who travels frequently for business purposes. While you are waiting at the airport for your flight, you need to access the internet to check some urgent mail. What will you do then? You must access the airport's public wireless LAN to check and reply to the mail. Here, you are a user of the airport's wireless network. Many times, the user may not be a human being. Suppose you are using the public wireless network of the airport to send an instruction to your central server. According to your instruction, the central server of your office uses the wireless network settings in your office. The server forwards the same instruction to your manufacturing unit where a robot receives that signal and it acts according to the message sent. Here, the user is a robot. So, the main purpose of the wireless network is to provide services to its end-users. Now perhaps it is clear that the user is one of the major components of the wireless network that gets benefits from the system. That is why the user is one of the important parts of the wireless network infrastructure.

The user is the final authority to decide when to use the wireless network and when terminate it. So, that makes sense of the appropriateness of the term end-user. Generally, as a user, you can use a computer to perform various activities by using different application software in addition to a specific wireless network interface. Different application software helps you to perform your job on a computer and wireless network interface helps you to communicate both ways from server to the client and vice versa. So, as a user of a wireless network interface, your role here is a communicator.

A user of a wireless network may be mobile or stationary. A mobile network is ideal if you need to travel a lot. Suppose you are in the seminar, and you need to receive e-mails and send reply-mails through your PDA. Here, you need continual support of the wireless network interface.

Sometimes, a user may need a portable wireless network interface. Suppose you are in a conference, and you need to discuss an analytical project using a wireless network for a particular time. Here, you can use a laptop and discuss the project before the audience with the help of a wireless network.

Other users of the wireless network are stationary. It means the people who sit in a particular place say an office and work from there and use the wireless network for an unspecified time. Suppose, you work on a BPO where you access wireless network platform for 24x7 hours. So, here the network is stationary. The main difference between a mobile and a stationary wireless network is roaming functionality. A stationary network does not need any sort of roaming function.

Computer Device

Do you know that computer devices can be used in different ways in a wireless network system? Many times, it can be used as a client-server computing system in a wireless network infrastructure. In a client-server computing concept both the client and server computers interface each other. Generally, the client computer sends a request to the server computer to share the resources it needs. There may be several client computers attached to the server computer to get access to the shareable resources. So, a server computer serves multiple client computers connected to it. The wireless network infrastructure acts as a liaison between the client and server computers. The best example of a client-server network system is a web server that returns the demanded web pages to its clients according to their requests.

Unlike the client-server computing system, many times a computer is used as an end system within the same wireless network infrastructure. It includes websites, servers, databases. For example, you can see news of your preferred news channel accessing it from a public wireless LAN from a railway station, airport lounge, or a hotel. Similarly, a staff sitting in the office can access the warehouse management procedure to interface with the staff of the warehouse using the wireless network. The warehouse computer system here acts as an end system.

As a user, you can also install a computer device like a network interface card (NIC) in your laptop to work and interface in a wireless network environment. A computer or a laptop can use an operating system like LINUX, Windows XP, or MAC OS as a software platform to run the wireless network application. Some of the OSs provide built-in features to

access wireless networks. Windows XP is one of the OSs that can work on the wireless network by identifying the wireless LAN.

Network Devices

As the wireless network grows to become larger, the network performance goes down. This is happened due to heavy traffic congestion in the network. Congestion in the network is caused due to the transmission of too many data packets. The network performances may even degrade to no transfer of data. So, to avoid such incidents, a huge network is fragmented into several segments of a small network. Breaking off such a large network into several small network segments is defined as subnetting. Subnetting is done by using different network devices like the hub, bridge, switch, and router. Let's get into each part to know more detail.

- **Hub** : It is a basic device used to bring every computer to be connected to a network. Computers are connected to the ports of the hub and work like a single segment of the network. The hub transfers all data to the computers that are connected to it. The hub has no own intelligence to work on. So, the function of a hub is as simple as to transfer the data that reaches it to the computers attached to it.

All the computers that are connected to a hub can find each other. That is why the chances of data collision in the network increase with the increase of several ports available in the hub and if all the ports are connected to computers. When a hub works on layer 1 network of the Open Systems Interconnection (OSI) model, the hub can detect the error due to the collision of data.

- **Bridge** : A bridge, unlike a hub has a single source and a single destination to send the data packets that it receives. So, a bridge is a two-way interface device. On receiving the data from a particular network interface, it transfers the same to another network interface which is, of course, connected to it. Therefore, a bridge generates two separate collision domains. Based on the features of a bridge's functionality it is sometimes defined as a

smart hub that can detect the target point at which the data has to be sent.

The work of the bridge may be best explained with the example of emails. An email is only delivered at the email address of its recipient and not in any other recipient's account else. For example, if you send an email to your friend at John@xyz.com , the wireless network system will search the email on the web. If that email ID exists, the system will deliver the same at that particular email address else it will fail to deliver. Such is the function of a bridge in the network system.

- **Switch** : A switch acts as a hub but performs the job intelligently. When a switch receives a request for the first time, it delivers the data to all computers that are connected to it. As soon as a computer responds to that data, the switch locates the port in which that computer is connected. At the same time, the switch instantly learns the media access control (MAC) address of the computer along with its port that responds. As a result, in case of any subsequent request received from the same source computer the switch responds directly because the switch already knows the source computer with its MAC address.

For instance, three computers named Computer X, Y, and Z are connected to the switch. The switch receives a request which is destined for the computer X. The switch transfers the data requested to all three computers named X, Y, and Z. The moment at which the Computer X responds to the data, the switch keeps the path in its memory and sends data to Computer X in all future references which are destined for the Computer X.

The switch performs this function on a network layer 1 of the Open Systems Interconnection (OSI) model. However, the switch creates many collision domains of its own on each port of the same network segment.

- **Router** : A router possesses the highest level of intelligence among any other network devices so far available in the market.

It is one of the most efficient devices that can be preset to transfer the data to the destination computers. The routers are used to operate on a layer 3 network of the Open System Interconnection (OSI) model. A router is also able to transfer the data from a network to another network by detecting the IP address of the target computer. However, a router does not forward anything by default.

The router creates a distinct segment for its every port and also creates a distinct collision domain. So, a router has several segments and as well as several collision domains. However, although a router creates distinct collision domains, it acts within the same domains.

A router’s functions include detecting the path, filtering the packet for each path, switching each packet, and work on the internet. For doing such function, routers consider all devices separately and break broadcasting domains from segment to segment. This implies that when a message is sent to a segment, the devices connected to that particular segment can get that message without intervening in other segments within that network. The routers do the packet filtering by using the access list and logical addressing to switch the packet to work on the internet. It also creates a map of the internetwork, selects the path, and sends the data packets to several remote networks.

NICs

A network interface card (NIC) typically functions as a liaison between wireless network infrastructure and a computer device. A NIC is attached with a computer device whereas a network adopter is plugged in externally outside the computer device. Now, you may think, how the NIC works. NIC works by following the standard protocol that has been set by the American Institute of Electrical and Electronics Engineers (IEEE). Suppose the NIC which will implement the IEEE 802.11b standard implies That the NIC will be able to interact with the wireless infrastructure that complies only with the protocol of the IEEE 802.11b standard. Therefore, as a user, you must check to make sure if the specification of NIC chosen matches the specification of the wireless network infrastructure that you need to access.

Apart from the NICs that work internally, there are NICs that can be set externally to a computer called external NICs. An external NIC is suitable for a stationary computer though it has some sort of mobility too in some wireless applications.

Wireless Network Infrastructures

The main purpose of wireless network infrastructure is to establish and ensure a flawless interconnection between its users and its end systems. The infrastructure consists of four components viz, 1) base stations, 2) access controllers, 3) application connectivity software, and 4) distribution system which help to enhance wireless communications.

- **Base Stations** : Basically, a base station is an infrastructural component that enables the users to access network services like web browsers, emails, database applications, etc. It contains the same technology found in a wireless NIC. Here, the base station interfaces the communication signals from one access point to another access point that moves through the air.

- **Access Controllers** : As the name suggests, the access controllers control the traffic between the resources and the open side of the wireless network. It is a hardwired device put between an access point and the open side of the network connected through a wire. It strengthens the wireless system by providing a centralized intelligent solution to the access control mechanism. Access controller also allows its administrator to arrange a per-user basis application to ensure access to a particular port or block the port. For instance, when you put your user ID and password to browse a web page, the access controller verifies, authenticates, and validates your identity through a server.

- **Application Connectivity Software** : The connectivity in network infrastructure, in general, defines the ability to connect an application software or a system else you cannot access the required database or any application. It implies, when you try to access a database or application software that hosts on a system

through your computer, you need an application connectivity software that can interface between your computer and the host server.

The application programs are generally written in several separate programming languages. On the other hand, the processors run several separate operating systems and may be located in different places. Here, application connectivity software plays a key role in establishing the communications between a computer of the user and a server that hosts the database or application software. The access points and the controllers are as well required along with application connectivity software to facilitate the communication system between the two ends.

- **Distribution System** : The wireless network itself functions without any wire but its infrastructure needs wire to bind its distribution system that includes server, access controller, and access point to hold together. However, the distribution system is defined as an interconnection made between an access point and a Wireless LAN following the standard protocol of IEEE 802.11.

For a large network that is necessary for a multi-floored building or to connect two or more offices, an ethernet hub plays the role of a medium that connects all the computers in the wireless infrastructure. The hub enables multiple domains to improve effective transmission performances among users.

Management System

Like any other infrastructure, wireless network infrastructure also needs an effective management procedure that can ensure that the wireless network skeleton and the people involved in it can meet the need of the users.

- **Security** : Security management comprises safety measures of the network components and resources. It enforces the security policy related to the configuration of the network infrastructure to encounter various issues that may compromise the wireless signals. The security policy should include strong encryption to

protect the system from the mischievous persons let not allow to steal the data of the users. Else the users will lose their trust in the access point of the wireless network infrastructure.

- **Help desk** : Helping the users in case of any primary problem associated with a wireless connection is the main objective of a help desk. So, a help desk must have a communicative interface to reach the users' needs.

- **Configuration Management** : An enterprise must have a prominent policy in place to review the wireless network skeleton that comprises, access points, channels of RF, security settings, etc. Configuration management must ensure prompt and dynamic action towards any updating or up-gradation of the skeleton system and configure the system accordingly whenever necessary.

- **Network Monitoring** : Monitoring of wireless network infrastructure is a huge task and it needs a proactive plan to manage the network functions successfully. The key role of a network monitoring management is to ensure mitigating the risk involved in accessing the user's data at the access point. The monitoring management further demands the user's growth to the access point of the network traffic without compromising the security of the network and users as well. The monitoring simplifies the operation support system and provides coverage for the overlapping of the base stations that might result in lower performance at the access point.

- **Reporting** : The reporting system includes various important factors of the wireless network performances including its data usage statistics and notifications of a security breach. These factors are responsible for deciding on any operational change that requires encountering the potential threat to the access point and its utilization. This information must be made available to all the support teams like help desk, engineers, and maintenance.

- **Engineering** : An engineering team is essentially important at the time of installation of wireless network backbone but their role does not remain restricted to the installation only. The necessity of an engineering team is essentially more important to keep the system run effectively and flawlessly. To run a network system smoothly the engineers should be a vigil on the structural design and functional design of the network skeleton. They should continuously monitor the performance of the network system and develop newer technology to increase the traffic flow with effective security measures based on zero compromises with any security threat.

- **Maintenance** : The maintenance part of the wireless network infrastructure deals with the repair of different components like antennae, channel points. The maintenance team evaluates RF propagation, install extra access point wherever and whenever it is necessary. So, the maintenance team acts as an extended support team of the engineering team.

Chapter 3: What is the Internet?

The internet, in simple words, is a global network of computers. It provides communication facilities and other facilities like the sharing of information. The skeleton of the global network is interconnected using a standard communication protocol. It works as a network of all networks in which all web servers of the globe are interconnected to form an international network. For example, you are working on your computer or laptop which is functioning on a network. You can get any information, message, and data from another computer which is working on a separate network. This sharing of information can take place if you have accessibility to a network of someone else computer.

The concept of the internet was first conceived in 1969 by the Defense Advanced Research Projects Agency (DARPA) under the US Government's Department of Defense. The agency aimed to set a network to transfer messages from one computer to another computer of the defense system in case of any military attack or such destruction.

However, the facility has now been spread worldwide and accessible to all citizens from all corners of the globe.

History of the Internet

After DARPA's revolutionary invention of the internet in 1969, the use of it was confined within the defense system of the USA. Nearly one and half decades later, in 1983, a new technology of network protocol was evolved as open network protocol termed as TCP/IP. TCP/IP stands for Transmission Control Protocol/Internet Protocol which consists of a set of standard protocol used in an open suit. National Science Foundation Network (NSFN) in 1985 developed a new design of network which enables all computer science departments to connect their computers countrywide. Internet communications were improved largely in 1989 when the HyperText Transfer Protocol (HTTP) was developed.

The development of HTTP had brought a sea change in the internet world. It provided the connectivity ability of various computer platforms to the same site on the internet. The internet network was further expanded in 1993 when the web browser Mosaic had evolved.

However, the internet has been continually developed its powerful existence all over the world. Internet Protocol version 6 (IPv6), for instance, has been developed by the Internet Engineering Task Force (IETF) that enables packet switching of data. Data switching eases data receiving and sending between two computers in a network.

The development of the internet had opened the necessity of its commercialization and competitiveness. At the beginning of the 1980s, however, some vendors had incorporated TCP/IP for their business product lines. This was happened not because the vendors wanted to initiate the networking but because the customers who approached the networking. Thus, the vendors' organization also approached to the networking of consumer products. Meeting the demand of both consumers forum and vendors organization, however, made possible in 1988 when the Interop trade show was started to begin. Commercialization of the internet has made it a commodity and now it has begun the backbone of information sharing and support commercial activities across the globe.

How Does the Internet Work?

The function of the internet has two parts. One is physical and the other one is technical. The physical part of the internet works on the principle of the prevailing telecommunication process. The technical part deals with TCP/IP which uses a set of data transmission guidelines.

When you dig deep into the internet, you will find two main components that act as pillars of the entire internet infrastructure. The first such pillar is the network protocols and the second one is the hardware. The first component, the network protocol like TCP/IP comprises a set of rules that directs a device carries out to accomplish the task. Without these common sets of rules, a machine would not carry out the task.

The purpose of using the sets of protocols is to translate the alphabetic, numeric, and other symbols used in data into the electronic signals. Those electronic signals are transmitted across the internet. Then, finally, the signals are retranslated to its original text form when it reaches to its end-user.

The second pillar of the internet infrastructure is its hardware part. It includes a smartphone, computer to even a cable that transfers information between the devices. There are some other types of hardware such as servers, routers, satellites, cell phone towers, radios, etc.

All the above hardware is somehow connected to the network. The devices like smartphones, computers, laptops, etc. are called clients, or endpoints. While a machine that provides a program for the functioning of other devices termed as “clients” is called a server. This client-server architecture distributes overall computation across multiple devices. The communication lines responsible for exchanging the data across the internet may be of two types. One is wireless signals that have been sent either through cell phone towers or satellites. The other one may be a physical connection like fiber optics through which the signals can be sent.

Data transfer from a device to another device relies on a connectionless network called packet switching. Packet switching of data occurs between senders and receivers. Whenever you try to connect the internet through your computer, a unique IP address is allotted to your computer to identify it for all future reference. Similarly, when you try to send some data to

someone over the internet, your data is managed in the form of packets. Each such packet is allotted a number called the port number which is used to connect the receiver of it.

So, a packet of your data has two features. One is its unique IP address and another one is its port number. Both unique IP address and port number are translated from their alpha-numeric text into the electronic signals. Now the signals pass between the layers of the Open System Interconnection (OSI) model of communication. The signals move from the top of the application layer to the bottom of the physical layer. Then the message is transferred over the internet where the signals are received by the router of the Internet Service Provider (ISP). The router examines the receiver's address that has been allotted to every packet and determines the path for sending the packet. After reaching the data packet to the client the reverse process is executed to translate the signals into an alpha-numeric text form of the original data. The process begins when the signal moves from the bottom of the lower layer to the top of the upper layer of the OSI communication model. During the process, the alpha-numeric data is stripped from the data packet by detecting the IP address and port number and this way complete the data transmission process.

Uses of the Internet

While almost everyone from across the globe is using the internet, it is pertinent to know the purposes for which the internet can be used for. It is generally used for the sharing of information from one place to another place that may be across the world. However, some important examples of uses of the internet are mentioned below:

- Accessibility for instant messaging, emails, internet relay chat, telephony, video conferencing, social media;
- Attainability for online educational programs for acquiring a degree, attending workshops and different skill development training;
- Opportunity for the job from both ends, for instance, an employer posts job opportunity, a job applicant can apply for the

position vacant. Both recruiters and applicants can find themselves in a common social media platform like LinkedIn;
- Scalability of research work and downloading of files;
- Capability to develop forums for online group discussion;
- Ability to read magazines, newspapers, and journals;
- Facility for online shopping, online gaming, and online dating.

Difference between the Terms the Internet and the WWW (World Wide Web)

Two terms the “Internet” and the “World Wide Web” are often confusingly defined to be the same thing. They are neither synonymous nor perform the same activity. Internet is the network of networks functioning across the globe and it is continually become larger due to the rapid growth of different networks. The term World Wide Web or simply Web is defined as a system of collecting documents and information which you can access over the internet. So, the internet, in other words, can be explained as an infrastructure of the network and the Web provides the services on the top of the infrastructure.

The Web covers a large part of the Internet’s uses. The most extraordinary feature of the Web is its hypertext. Hypertext is a software that allows an extensive cross-referencing between its related portions of the text and the material of the associated graphic. Most of the websites use some specific phrases or words that appear on their page in a separate color in contrast with that of the rest part of the content. Also, differently colored texts are made underlined. When you click on the selected colored text, that webpage will transfer you to a separate page or site related to that colored text. This enables a user to get more information about the colored text. Image, part of an image, button, etc. are used as a hyperlink.

Now the Web has come up with billions of varied information pages to the people for their access. So, to navigate through or browse those web pages you need a browser. A browser is a software application program that helps you to find a way to enter the Web and look at your required page into it and interact with the information provided on that page. Browsing on the

World Wide Web may include Web pages, images, videos, etc. Google Chrome, Internet Explorer, Firefox are the most popular browsers amongst all other Web browsers. However, the looks of a specific Web page may vary a little based on the browser you are using.

Security and the Internet

Accumulation of information that may be private or public is increasingly becoming huge day by day across the Internet. This enormity of the Internet has brought two threats to its users. One is a threat of data breaches and another one is a security threat. Both threats are associated with different risks.

A data breach is a definite occurrence of accessing or disclosing a user's personal confidential or sensitive information in an unauthorized or illegal manner. It may involve accessing a user's personal identification or personally identifiable information (PII), user's personal health information (PHI), intellectual property, trade secrets and many more. Some common examples of data breaches are the Social Security Number (SSN), credit card number, health care information, etc.

The security of the Internet is the defense system of the digital world from either internal or external, malicious or accidental threats. The primary objective of the defense system is to detect the threats on a continuous basis. The second stage of the defense system is to prepare a security policy to respond and counter the threats to prevent the system from malfunctioning with the help of information technology and software tools. Here are some advisable security steps that you can follow to protect your own privacy:

- Install antivirus and antimalware
- Create a strong and varied password and change it periodically in a varied way

- Try to use a virtual private network (VPN) or a private browser like Google Chrome that creates a safe and encrypted connection
- Use only HTTPS
- Make all social media network account private
- Deactivate the auto fill options
- Turn off your device’s GPS
- Update cookies, so that you will be notified whenever it is installed
- Log out an account before leaving it just closing the window or tab
- Do not open a document from an unknown source or download it from there
- Use cation for spam emails
- Use caution while accessing hotspot or public Wi-Fi

Social Impact of the Internet

Like many other scientific achievements, the Internet has also a dialectic impact on society. Some people are on the negative side of the Internet. They argue for the behavior of a particular generation that they never have seen before. Some of such allegations are alienation, detachment from the society, increasing emotional reaction like fear of missing out (FOMO) of a particular generation. While the people on the positive side of the Internet express their opposite opinion on the use of the Internet. They argue that the Internet stretches the boundary of civic engagement, intensifies the relationship within the like-minded people, provides more sociable stability, develops a larger community going beyond the core group of families, friends, and colleagues, focus on individual’s growth by sharing other people’s value, projects, and interests. Some of the social networking sites such as Facebook, Instagram, Twitter, and LinkedIn are the most preferred platform where everyone starting from an individual to corporate is getting an opportunity to interact with each other for the benefit of their own and the society as a whole.

Chapter 4: Wireless Network Applications

Coined in the 19th century, the term wireless communications has left a huge impact on the world and over the years, the technology has undergone several major changes which have, in turn, made it even more developed. When it comes to transferring information from one device to another, the importance of the wireless medium is indispensable and it has also acquired the position of being the most important medium of transmission as well. As you must already know, in wireless communication, the information is not transferred with the help of any physical object but through air and no electronic conductors are required. Astonishing, right? The only thing that is used is the electromagnetic waves like RF, IR, and satellite.

In today's era, wireless communication is not limited to a few devices but has expanded itself over a plethora of items from computers to smartphones, laptops, tabs and so on. Bluetooth technology is also a part of it. In this chapter, you will get an overview of the various applications of the wireless network in today's world and how hugely it has impacted our

day-to-day work. When it comes to communicating from remote operated areas, wireless communication comes of great help.

Types of Wireless Communication

Here are some of the common types of wireless communication and a brief intro of what they are.

Satellite Communication

Being one of the most advanced forms of telecommunication infrastructure, satellite communication is a self-contained technology. With this technology, you can be connected to anyone you want and also anywhere on this planet. This is a type of communication that operates universally. Those who rely on this type of communication usually take the help of a commercial vendor who has a geostationary satellite in his or her reach. Now you must be wondering what geostationary satellites are. Well, they are a type of satellite that matches the rotational velocity of the earth thus having the same orbital period. It is because of this that the satellites always remain at the same point in the sky.

A beam of modulated microwave acts as the signal in this type of communication and when the signal comes in proximity to the satellite, it gets amplified. Then that amplified signal will be sent to the respective antenna whose location is somewhere on the earth. Thus there are two main segments of the satellite communication. One is located on the ground and the other in the space. Mobile or fixed transmission, ancillary equipment, and reception are all a part of the ground segment whereas the space segment consists mainly of the satellite. The pace and pattern of world communications have undergone a complete change after the advent of satellite communications.

Infrared Communication

Next, we come to infrared wireless communications whose basic component is the IR radiations. For those who are not aware of what IR is, it is a type of electromagnetic energy whose wavelength is more than that of red light. The communication of this category can happen between a fixed

device and a portable device and also between two portable devices. There are two basic types of infrared communication which are explained below –

- **Diffuse Point –** A line of sight between the receiver and transmitter is not required in this case and the link maintenance is done by bouncing or reflecting of signals. This is done through surfaces like roofs or ceilings. A very common example of this system is wireless LAN communication.
- **Point to Point –** In this case, a line of sight becomes mandatory. This means that the receiver and the transmitter should be placed or arranged in a way that they point towards each other and in between them, care should be taken that there are no obstacles present. Remote control communication is a common example of this type of infrared communication.

If you are wondering what the advantages of infrared communication are, then let me elaborate that to you –

- For starters, the high directionality of infrared communication is its biggest advantage. The various sources involved here do not emit the same radiation but different ones with differing frequencies and thus, identifying the source becomes way easier. So, any risk involving the diffusion of information is eliminated.
- There is no chance of harm to human beings from infrared radiation and thus, you do not have to think twice before using it at someplace.
- If you are sending video signals or anything that requires high-speed communication, then you should definitely go for infrared communication as the transfer speeds can go as high as 1Gbps.

Broadcast Radio

Do you want to know what the first wireless communication technology was? Well, it was open radio communication. It was quite widespread and even nowadays has its own audience. The multichannel radios allow short-distance communication between users whereas there is a different category of radios known as band and maritime radios which are used by sailors for communication services. Then there are ham radio enthusiasts who, during

disasters, can share emergency communication aids by implementing their strong broadcasting gear and they can even send digital information through their system.

Radio waves are what carry the sound of radio through air. A transmitter is used which sends the data to the receiving antenna. Radio waves are also categorized as electromagnetic signals and they belong to an entirely different set of frequency segments. If you want to obtain a particular audio signal, then you have to change your frequency segment accordingly.

Microwave Communication

This type of communication also uses the help of radio waves and these waves are measured in the range of centimeters. There are two methods through which information or data can be transferred in this type of communication. One is the terrestrial method and the other is the satellite method.

In the case of the satellite method, as you might have already guessed, the satellite is used which performs the task of receiving signals sent from stations on earth. The frequency of these signals ranges between 11-14 GHz. The transmission speed ranges anywhere between 1 to 10 Mbps. Then there is the terrestrial method. Here, a clear line of sight is a prerequisite between two microwave towers. You should be guaranteed that there is no obstruction between these two towers. The range of frequency for this type of microwave communication usually ranges between 4-6 GHz and the speed of transmission is the same as the satellite method. But there is a major disadvantage in the case of microwave communication and that is, they can be hugely impacted in case of bad weather conditions.

Wi-Fi

One of the biggest advantages of Wi-Fi is that it is a type of low power communication in the wireless category. Various types of devices can use Wi-Fi and all these devices are commonly used in the day-to-day life of people. For example, laptops, mobile phones and so on. The role of the communication hub in this category of wireless communication is played by the router. But in order to stay connected to the router, you have to be in

close proximity to the system and you cannot engage in transmission over long distances as was the case in the types of wireless communication mentioned above. For the purpose of security, wireless networks need to be properly secured by setting appropriate passwords.

Mobile Communications System

With each generation, the growth of mobile communications has increased by leaps and bounds. With the help of mobile phones, people can communicate across a single frequency band. Cordless and cellular phones are the two common examples in this category. The coverage of the mobile communications system is huge owing to the various networks available. But in the case of cordless phones, the range is, however, limited. Also, you will find certain devices that use satellites to connect to other devices.

Bluetooth Technology

This is also a form of wireless communication system that allows you to transfer files between two devices. The most common application of this is today's world is when the different devices like earphones, wireless keyboard, and mouse are connected to the mobile phone with the help of this same Bluetooth technology. There are various functionalities associated with this particular technology.

Wireless Communications Gives Internet Access

Among all other viable reasons for which you should get a wireless communication, the most compelling and important one is that it will allow you to access the internet and also share that high-speed internet with others. Thus, all the members of your family or your company can share the same high-speed internet connection. Thus, it will save you a lot of money and is also highly convenient. Everybody will then be able to get access to that high-speed internet and also roam about the building without worrying about losing the connection.

The flexibility also increases because you can go on adding workstations without having to sort the problems related to cables which, in turn, could have created a lot of mess. Also, you can relocate any of your devices anywhere you want without any wires interfering in the process. This also enables the relocation of servers and printers and any other accessory device and makes the entire process hassle-free.

There is another benefit that comes with wireless communications. For example, you have a guest or any client visiting you at your office. Then you can allow him/her to quickly connect to the internet connection without having the need to go through any elaborate configuration settings. Thus, productivity is enhanced to a great extent. Any visitor to your property can simply turn their device on and connect to your network in order to do some work on the web or access their email.

Wireless Network in Inventory Control

Your dealership can suffer a bad hit if you are not up to date with your equipment inventory data. But if you are using wireless network technology, it will be a highly convenient and mobile solution to integrate into your company. You will gain better control over the various sectors of your inventory the moment you integrate the wireless network inventory control services. One of the major benefits that you will enjoy is that this will considerably lower your overall costs. When you establish a LAN connection, your main control systems are connected with your manufacturing equipment through a wireless mode. Thus, the assembly process can then be reconfigured at any point of time and from any place you want.

You can update your inventory and also track it any time you want. This increases accuracy and efficiency to dramatic levels. If you are considering a retail environment, whenever a product is stocked or purchased, the inventory can be updated in real-time with a wireless management solution. If you consider the manufacturing setting, all the statistics that are related to the finished products, as well as the raw materials can be kept up-to-date. If you give your employees the wireless-enabled bar code scanners, then they can change or check the prices or even find out the number in stock.

There is literally a chain reaction of benefits associated with implementing a wireless network in inventory management. If you think about it with a clear mind, you will understand that the clerks possess the handheld scanners and thus the information is being directly inputted into the system. So, there is no paperwork to deal with. Thus, you can steer clear of the chances of human error in the process. Your financial records will become way accurate than before. This aspect of a business is highly important because if you do not have correct financial records, you would not be able to pay your taxes accurately and keep fines to a minimum.

Wireless Network in Health Care

Wireless networks are now being deployed by more and more hospitals and other healthcare institutions because of one sole reason and that is – convenience. Whenever hospitals have a high patient traffic area, the deployment of a wireless LAN network makes everything more manageable. This includes critical care wards, emergency rooms, doctor's offices, nursing stations and even waiting rooms. Better care for patients is synonymous with better communication and for that installing a wireless network is necessary. Patients can be diagnosed and treated more accurately and faster when communication is clearer.

The use of a wireless network ensures that the clinicians can get access to the lab results as soon as they are ready and they do not have to wait upon someone else to bring it to them. They also get access to the vast medical database through their mobile devices, smartphones or laptops. All of this together improves patient outcomes.

The quality of communication between a doctor and a patient can be considerably improved by using suitable videos. Then there is mobile video conferencing which is really a boon for patients who seek treatment from the comfort of their own house.

When it comes to healthcare, the importance of accurate records cannot be explained in words. Mistakes, no matter how small or big they are, can sometimes even cost a patient's life and so no mistake can be tolerated. But in the absence of a wireless network, everything from recording

pharmaceutical orders to keeping test results has to be done through paper and all that paperwork can easily get messy increasing the chances of error. This entire process is overwhelming too and takes the maximum time away from the day. But when you install a wireless connection, everything can be directly logged into the central database and can be wirelessly transmitted. This also enhances the visibility of the data to everyone and thus anyone in need of particular information can access it without disturbing someone else.

Nurses and doctors have to cater to the needs of so many patients in a day and they constantly keep running from one room to the other. When there is a wireless network, they can view, input or edit any patient's records from where they are standing. Thus the speed of delivering health care is highly increased. The tracking of pharmaceuticals also becomes hassle-free. Scanning devices and handheld bar code printing have proved to be a boon in this respect. Drug transactions become more accurate and you can keep a proper track of the expiration dates as well. Also, whether the right drug is being administered to the right patient at the right time or not can be easily monitored.

Wireless Network in Education

When it comes to school education systems, the importance of wireless networks is quite obvious. Faculty members, students and staff are wanting boundless access to the network starting from the general classrooms, meeting rooms, and even auditoriums and common hallways. Installing wireless LANs in elementary schools and colleges can be quite beneficial to the students. Students are, thus, able to do a lot of things like surfing the web, accessing their emails, checking grades, accessing the various school applications or even view the transcripts from anywhere they want. This increases the overall efficiency of the students. They can make much better use of their time.

On the other hand, if you want to establish a computer lab, it can not only be expensive but the students also often have to wait in line to get access to a single computer. This cuts off their time from other activities. But when you start a wireless LAN, the students are then able to get access to the

network from anywhere in the campus by using their own laptops. They can do this even after the computer lab has closed. Thus the network can then be distributed among all students equally and evenly. This increases the efficiency of teaching too and the school can cut off some considerable costs of setting up a huge computer lab.

Wireless Network in Real Estate

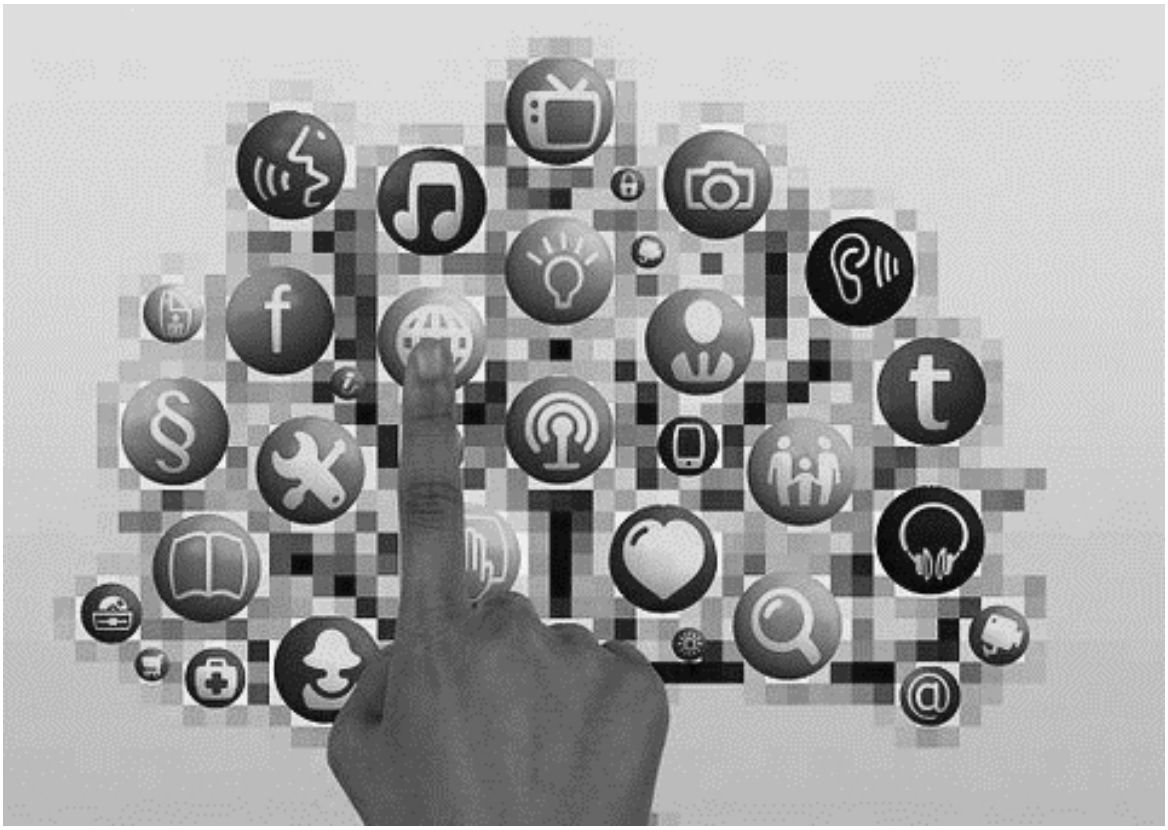
Salespeople in the world of real estate do a large amount of work while they are out of their physical office. They spend half of their time talking with the various buyers and sellers of the property in question that is being sold or rented. Now, before the salesperson meets the potential buyers, he/she has to get the MLS or Multiple Listing Service printed which will have a few sites on it which can be shown to the buyer. But in case the buyer is not satisfied with the sites that are present on the MLS, the salesperson will then have to again drive back to his/her office and then get more listings, which have no guarantee of being approved once again. Also, even if suppose the buyer agrees with one property, then the salesperson will have to again come back to the office to complete the rest of the paperwork which again is quite extensive. Thus, the entire process wastes a lot of time.

But, if you implement a wireless network with a central database, then the process becomes efficient. So, the real estate agent can then access that database no matter where he is simply by using a laptop, mobile or tablet. In order to produce contracts or other such documents, the agent can take the help of a portable printer.

Thus, as you must have understood by now, the location of any person can be shown in a central location and thus location-based services become way easier to handle. There are several corporate applications to wireless networks being used to build a public network. Users can enjoy a constant mobile connectivity irrespective of the place they are in. This ensures a high level of performance. These systems are very common in railways stations, airports, restaurants, and hotels. Thus, the need to stay connected to the internet has risen over the years and rightfully so because almost all types of work are now somehow related to the web.

So, if something can ensure your constant connection to the web without the hassle of any dangling wires, then it gives you freedom and mobility as the network is no longer dependent on your location. So, the application of wireless network has completely changed the face of all sectors.

Chapter 5: Wireless Communication Technology



In the previous chapter, I had given you a brief introduction to the different types of wireless communication technology that exists. Here, I am going to explain to you in detail what are the different aspects of wireless communication technologies and what special characters do they have. It all started with the invention of the radio and now, wireless communication has attained great heights. The society has been transformed with the power of instant communication even over long distances. The world has now literally become a much small place.

Advantages of Wireless Communication

The list of advantages for wireless communication is endless but I have tried to mention all of them in a concise way here –

Mobility

There is a great deal of mobility associated with types of wireless network. They do not face any barriers because communication is done in the form of various waves through air. There are no wires involved. For example, you can listen to your radio while you are driving your car through the woods. Yes, there are certain factors that can affect the signal strength but in any case, there is no question about the extent of mobility you are getting.

Convenience

For the wired connections to work, the presence of a physical connection becomes necessary and this, in turn, can create a lot of hassle. On the other hand, wireless communication does not require any such physical object. The signal strength is the only deciding factor. If that is working, you do not need to worry about anything else. All you need is a password to protect your network and you can instantly connect your devices to the network without worrying about any hackers.

Flexibility

Wireless networks operate through thin air and thus they can penetrate walls. You do not have to think twice about the location of installation. You can install them anywhere you want and they will still be performing efficiently. The flexibility is definitely one of the greatest advantages of a wireless network.

Cost-Effective

Installing a wireless network can save huge costs on your side. It is very cheap to install especially when you compare it with wired systems. In the case of wired systems, the cable cost is huge and you have to pay for it in terms of per-foot wire required. This also involves separate labor and time for the complete installations which, in turn, incurs additional charges. Also, if you want any changes to the plan of wiring for installing these cables, that will fetch you even more costs. But yes some small amount of wiring is sometimes required to set up wireless connections on a large scale but that is way less than that of wired systems.

Basic Elements Present in a Wireless Communication System

There are typically three elements present in most wireless communication systems and these are as follows –

- Transmitter
- Channel
- Receiver

Transmission Path

Some of the parts of a transmissions path in case of wireless communication are as follows – multiplexing, modulation, encryption, and encoder. The Source Encoder is through which the signal originating from a source is passed through. In order to make the signal processing techniques work, a suitable form is created from the signal and that is done with the help of the source encoder itself.

If the signal contains any redundant information, then that is immediately removed. This ensures that the maximum utilization of resources is done. Then comes the work of the Encryption Standard which is responsible for the signal encryption. This ensures that everything is transmitted in a secure form and no type of unauthorized access is entertained.

All types of impairments in a signal like interference, noise and so on are all removed from the signal the moment you make it go through channel encoding. There is another thing that is done during this process, that is, in order to make the signal strong against noise, there is an introduction of a small amount of redundancy. Then, a suitable technique of modulation like FSK, PSK or QPSK is used. This enables the signal to be transmitted with the help of an antenna.

Then comes the role of various multiplexing techniques like FDM or Frequency Division Multiplexing and TDM or Time Division Multiplexing and they help in the sharing of the valuable bandwidth.

The Channel

As you must have understood from the term itself, a channel in the case of a wireless communication network is the medium of transmission which, in this case, is open space. This can be highly variable and unpredictable in nature. It is also quite random. This channel suffers from a lot of things like scattering, noise, distortion, interference and so on. The result is that several errors begin cluttering in the signal.

The Reception Path

The collection of the signal from a particular channel is the task of the receiver. Then that same signal is reproduced to serve as the source signal. Demultiplexing demodulation is a part of the reception path in the case of a wireless communication system. Some other parts include source decoding, decryption, and channel decoding. Now, if you study these aspects carefully, you will understand that the task of the receiver and the transmitter are completely opposite to that of each other.

The demultiplexer is the one that is responsible for receiving the signal from the channel. That particular signal is also separated from all other signals. The various demodulation techniques are then implemented to demodulate the individual signals. After all this, the original signal is finally recovered. The channel decoder then removed any or all of the redundant bits from the signal.

Now, you must understand that the message you receive is in encrypted formatted so decryption has to be done as well. Thus, the security measures are removed and a simple sequence is extracted from that encrypted signal. Then the source decoder comes into play and the signal after decryption is given to it. Finally, the original transmitted message is retrieved.

Wireless Signal

Before we go into the details, you first need to understand what a wireless signal is. The wireless signals are those who are responsible for the transfer of video, audio or any other form of data and they do it all without the presence of any kind of wires. But one thing that is universal to all types of wireless signals is that they are all electromagnetic waves that travel through air. Now, you must be wondering how these waves form. Well,

when some type of metal is used for the transfer of electric energy, then there are waves that are generated around that piece of metal. These waves are known by the term of electromagnetic waves. Depending on what the strength of that energy is, the waves can travel certain distances.

Now, we come to the different types of wireless signals that exist. There are some you must be pretty familiar with and they have been already discussed in gist in the previous chapter – television, AM and FM radio, Bluetooth, Wi-Fi and satellite connections. But all of them are different from each other in some form or the other.

Frequency

So, we start with some of the common aspects of wireless communication because, in order to fully understand it, you need to start with the basics. There is a specific spectrum assigned to every wireless signal. This spectrum is of a wide range which is calculated in terms of frequencies. But in simpler terms, the rate of vibration of a signal is termed to be its frequency. The signal is said to be of a low frequency if it vibrates very softly or almost negligibly. But consequently, the signal is said to have a high frequency, if it vibrates with greater energy.

The measurement of frequency is done in Hertz and by this amount, you will come to know how quickly that particular signal is changing. Or, to put it simply, a signal changes every second but the frequency will help you understand how the signal has changed. An example should make it clearer to you. In the case of radio, FM signals have been proved to vibrate for over 100 million times per day. And in most cases, the frequency of wireless communication is mentioned in such high frequencies. This makes the process of stating the frequencies in their actual state a bit difficult because of so many zeros attached. Thus, they are abbreviated and thus, there is a term called Gigahertz. It is of greater value.

Modulation

The way in which a wireless network conveys information is also different from signal to the other. In order for you to send a message, this wireless signal often needs to be changed of modulated other you will not be able to send information to someone. Among the different types of modulation available, people can use any of them that suit their specifications. The two of them are known as FM and AM and in both these cases, the M stands for modulation. Both of them are different from each other based on the type of modulation they undergo.

In the case of AM, the M is modulation but the A stands for amplitude. This means that it will depend upon the energy of the signal or its strength that is operating on a single frequency. Then there is the FM where again M stands for modulation but F stands for frequency. This means that the modulation is done with respect to the vibration of the wave per second. The different types of modulations implemented by the different technologies usually differ and are sometimes not compatible.

Think about the satellite equipment. Can it speak directly to your phone or laptop? No, right? Your phone or laptop uses Wi-Fi in order to receive or send information. This is because various devices have certain fixed frequencies and modulations that they can listen to and not anything else.

For example, you will get certain broadcast radio receivers that can switch between the FM and AM signals and this is done for two reasons. The first and the obvious one is that two frequencies are being used for transmission and secondly, the modulation type used is also different. If a radio is in FM mode and you try to listen to an AM signal through it, it won’t be giving you anything. The same is the case when you try to listen to an FM signal when, in fact, the radio is in AM mode. The receiver won’t be able to make sense of anything when the signals are so conflicting. Thus, the usage of the same frequencies as well as modulation types between receivers and transmitters is essential for the communication to be done effectively. Nearly every device that you have in your daily life has some different types of modulation and frequency. Thus, the conclusion is clear. Most devices can understand a very specific range of signals and not anything else.

Receivers and Transmitters

A transmitter is a device which is sending out the signal. But when another device understands that signal after picking it up, it is called the receiver. There is use of only a single transmitter in the case of FM radio. This transmitter is not only operated by the radio station but is also owned by them. But there are many receivers and that is what the people use to listen to the radio. But there is another term of which you might not be aware of and that is the transceiver. This is a device that has both a receiver and a transmitter. Do you know an example of such a device? It is quite simple – routers. Routers can do both tasks. They can receive as well as transmit and that is why when it comes to building networks, it is the routers that are used.

Wi-Fi Signals

Now, we come to the topic of Wi-Fi signals. This technology is something that is immensely popular in today's world when it comes to building a network. But they also have some unique properties which I have discussed here.

Based on the frequencies that the Wi-Fi signals have, they are of two types –

- **2.4 GHz –** This is the lower one among the two frequencies but this is also the one that is more commonly found in use in case of Wi-Fi technologies. There are so many devices in the market that are using this frequency. There is a disadvantage to it as well. The more the number of devices utilizing a particular frequency, the more crowded it becomes. Thus, there is interference in signal transmission and thus it is not always faster. But it can easily pass through walls and windows.
- **5 GHz –** Next we come to the higher one among the two frequencies. This frequency is not so popular as the previous one and is thus used by much fewer devices. So, if some device is using this frequency, it can achieve greater speeds because of a lesser crowd. But there is a disadvantage and that is, this

frequency is not efficient in passing through walls and windows as the previous one. That is why the technology of 5GHz is limited.

Wi-Fi can thus be categorized into two types of bands or frequency bands. There are several different channels in each of the frequency bands of Wi-Fi. You can think of these channels as separate rooms in a house where a party is happening. When there are too many people in one room, you cannot really conduct a conversation there. That is when you have to go to another room but after some time, that room can get crowded as well. Very soon, you will find that the entire building is becoming crowded and that is when you finally give up on initiating a conversation simply because it is no longer possible in that crowded place.

2.4 GHz Band – First, we will discuss this band of Wi-Fi. There are a total of 14 channels in this band but not all these channels are unique or separate. There are several of them which are overlapping and can you guess the consequence of it? Well, they cannot be used at the same time. If you are thinking about setting up a mesh network, there is something that you should know about it. The same channel has to contain all of the mesh links. Depending on your location in the world, the available channel number will vary. For example, if you are from the US, then channels 14, 13 and 12 are not available for the use of Wi-Fi because they are used for the purpose of satellite and TV services. So, in order to build a network, you can use channels anywhere between 1 and 11. For the rest of the world, the channels between 1 and 13 are usually available for building a network but there are some places where you can even use channel 14.

Apart from what I have mentioned above, in the 2.4 GHz band, the channels that are the best for use in the US are those of 1, 6 and 11. There are certain partially overlapping Wi-Fi signals but if you stick to these channels, you will face very little interference.

You should also keep in mind that using other channels for your network is totally fine as long as they are 5 channels away from each other, for example, 3, 8, 13. But this is not an optimal option as channel 13 is not a viable option for many places around the world and you are not putting Channels 1 and 2 to use. No matter where you are in the world, do a small

research and you will get to know about the channels that are mostly used in that region and then you need to plan accordingly so that your network is not overlapping.

5 GHz Band – Since this is of a higher frequency, it is much wider than the 2.4 GHz band. Consequently, it holds a greater number of channels too. The best thing is that these channels are not overlapping as in the case of the 2.4 GHz band and so there is nothing such as a non-standard channel. With the presence of so many channels, choosing a channel that doesn't cause any interference is pretty easy in this case. The channels available for building a mesh network in the US are those of 165, 161, 157, 153, 149, 48, 44, 40 and 36. But apart from these, the other channels are available for other forms of community networks or access points but when it comes to a mesh network, those channels are not going to work. You can check online for what works in your area and what doesn't.

Antennas

Next, we come to the antennas. There are different types of antennas in use by wireless routers. But in some of the routers, the antennas are not always separate because they are built-in. On the other hand, there are other types of routers where the choice will be yours regarding what type of antenna you want to attach. Antennas can be of many types but if you consider the basics, then there are three and they are explained below –

- **Omnidirectional Antennas –** The term itself signifies the type of antennas this is. It is responsible for sending out signals in all directions but equally. With these antennas, the creation of a connection in any direction is possible.
- **Directional Antennas –** The main difference with that of omnidirectional antennas is that these send out signals only in one direction. The benefit of these antennas is that you can increase the distance the signal has to travel. They can be further classified into two –

- *Focused Antenna* – This type of antennas sends out a signal in the form of a narrow beam which is usually between 5 to 10 degrees in width.
- *Sector Antenna* – These send out signals in the form of a wedge. They can be as high as 120 degrees in width.

Chapter 6: Mobile Communication System

Mobile communication technology allows you to communicate with others using a wireless network system. Radio waves are used within a radiotelephone creating a mobile communication system. This system involves different types of facilities. Public land mobile radio, a mobile two-way radio, amateur radio, and mobile phone are examples of different types of mobile communication systems.

Public land mobile radio is used in fire agencies, police and municipal agencies including a two way FM (Frequency Modulation) radio system. The capability of this system is restricted within a small geographical area.

A mobile two-way radios help to create a one-to-many communication system to operate within a half-duplex mode. CB (citizen band) radio is one of the most common examples of this type of radios and it utilizes AM (amplitude modulation) to operate within the frequency ranging from 26.271 MHz to 10 kHz involving 40 channels. It utilizes a press-to-talk switch as it is not a commercial service. It may be available as amplitude modulated with a single-sideband or double sideband suppressed carrier.

Amateur (HAM) radios can cover a broad frequency band ranging from 1.8 MHz to 30 MHz including CW (continuous wave), FM, AM, HF slow-scan still picture TV, facsimile, radio teleprinter, UHF or VHF slow scan or fast-scan TV, amplitude-shift keying and frequency-shift keying.

The mobile telephone provides full-duplex transmission. It involves a one-to-one system to permit two simultaneous transmissions. Every mobile unit includes a specific number to maintain privacy.

Recent and Previous Mobile Communication

From the year of 1983, the commercial application of AMPS (advanced mobile phone system) has enhanced the growth of the mobile communication system. The cellular concept was a great breakthrough.

Cellular Concept

The advent of cellular operation has developed exponential growth within the personal communication system involving different advancements such as wireless access, integrated circuits, digital signal processing, increased battery life, and so on. The cellular system acts by following the steps below.

- An available frequency spectrum is separated into discrete channels to assign within groups to the geographic area where cellular service will cover.
- The discrete channels have the capability to be reused within different cells ranging from 2 km. to 50 km.
- An RF (radio frequency) transmitter is used within the service area when adjacent cells avoid interference by the operation on different frequencies.

The Cellular telephone had stated involving two-ways analogue, communication system with frequency modulation due to the involvement of transporting voice and frequency-shift keying to control transportation and signal information. Examples of another end of the cellular system are cordless telephony, a digital cellular system, paging, and satellite mobile.

Analogue cellular system is considered as the 1G (1st generation) category of cellular concept. The digital cellular low-power wireless is considered as 2G (2nd generation) category of cellular concept.

Analogue Cellular Phone: In New Jersey, Bell Labs placed a proposal for a cellular telephone considering as an AMPS (advanced mobile phone system) within the year 1970. The operation of AMPS was started on 13th October 1983 as standard cellular telephone service. It utilizes narrow land FM including usable 300-3 kHz audio frequency band and positive and negative 12 kHz maximum frequency deviation for 100 percent modulation. It corresponds to 3 kHz considering Carson's rule.

AMPS utilizes FDMA (frequency direction multiple access) within the area where transmission is divided within the frequency domain. A pair of voice channels involving forward as well as reverse for the duration of the call is allowed to the subscribers. Analogue cellular channels include both voices utilizing digital signaling information and FM by following binary FSK.

Digital Cellular System : It allows development within both performance and capacity. FDMA utilizes a frequency canalization approach to manage spectrum whereas time-division multiple access (TDMA) uses an approach of time-division. The complete available cellular RF spectrum is divided into subdivision classes within narrow-based channels and these are utilized between base stations and mobile points as a one-way communication link.

Multiple Access Technologies Followed in Cellular Systems

A specific amount of frequency spectrum is usually issued to a cellular system. A user can share easily the available spectrum as multiple access methods are utilized. Multiplexing can be followed by three dimensions for wireless communication and these three dimensions are TDMA (time-dimension multiple access), CDMA (Code-dimension multiple access) and FDMA (frequency-dimension multiple access) and its various OFDMA.

The available spectrum is separated into frequency channels or narrow frequency bands within TDMA. These are also separated within many time slots. Each frequency channel of frequency 30 kHz is separated within three slots according to American digital cellular standard IS 136. On the other hand, each frequency channel of 200 kHz is separated within eight-time slots according to the European digital cellular system. GSM Guard bands are essential both time slots and frequency channels.

The users share the available spectrum within a frequency band within FDMA named traffic channels. Different users are allotted different channels considering frequency band contains the user's signal power. All the analogue cellular systems involve FDMA. A data stream is followed involving several lower-rate subcarrier tones within a multi-cellular transmission method named OFDM. The mobile communication system includes OFDM to control hostile frequency selective fading. Wireless network standard is also maintained by incorporating OFDM.

OFDM offers the advantages of OFDM modulation and coherent identification. It also has several qualities that are complicated for high-speed transmission in the future. The need for electrical bandwidth can be decreased to a great extent by involving up-down conversion for the OFDM transceiver. It is very effective for high-speed design as electrical bandwidth involves the cost. Moreover, the advantages of an effective algorithm of FFT (fast Fourier transform) or inverse FFT are established when signal processing is involved within the OFDM transceiver.

Digital Modulation Keying

Generally, communication systems have modulation of a carrier to create a band pass waveform. A digital signal can help to modulate the frequency amplitude or phase of the sinusoidal carrier making three different digital modulation forms such as FSK (frequency-shift keying), ASK (amplitude-shift keying) and PSK (phase-shift keying). Additionally, some modulation schemes are also involved in engaging a combination of phase modulation and amplitude modulation. It is also important to note PSK transmission is polar whereas the ASK signal is non-polar. PSK represents a non-linear

modulation scheme whereas ASK represents a linear modulation. PSK works better than Ask.

QPSK (Quadrate Phase-Shift Keying)

The above-mentioned methods of digital modulation are not spectrally efficient as the available channel bandwidth is not completely utilized. OPSK helps to improve spectral efficiency. It involves two types of message sources. In this method, modulation carriers create the output waveform by combining within the quadrature phase. In QPSK, modulation gains and the amplitude of the modulator waveform are formed about equally.

DPSK (Differential Phase-Shift Keying)

There is no need to involve synchronous carrier for identification of PSK signals within OPSK modification of PS. It is an igneous method in which the derivation of carrier reference is made from the received waveform within the foregoing bit interval by an application of a 1-bit delay.

Data Transmission Involving Pack Switching

The supply of different addressed packets with interconnection for having a conversation is done by the packet switching process.

SMS (Short Message Service)

Digital cellular networks such as GSM, EDGE, IS-136 and PDC (packet data service) support short message service which is one of the most common packet services. It represents a store-and-forward or packet mode service and it offers inter-working involving the different services and applications within a fixed network. Signaling and control channels are usually utilized for data transmission due to message transfer between applicable network services.

GPRS (General Packet Radio Service)

GPRS is very important to represent add-on capabilities regarding the basic voice-optimized cellular network system to handle important properties of radio-access technology.

EDGE (Enhanced Data Rates for GSM Evolution)

You will have to modify the radio-access part when you want to enhance the capabilities for the data handling of 2G service. EDGE is the form of modification and it has evolved in Europe. It helps to adopt a mechanism for link selecting the best modulation combination and encoding schemes considering the time varying quality of the link. EDGE concept involves both packet mode as well as circuit mode and is also enough generic to use within other digital cellular systems. It acts within the bandwidth of 200 kHz including at least one high-level modulation scheme and specific efficient coding systems.

Spread Spectrum

A spread spectrum is a specific communication method that involves more radio frequency purposefully than the essential transmission of a signal. It is essential to improve the signal-to-noise ratio. It helps to prevent intentional jamming and to secure communication.

Two methods to Perform Speed Spectrum

Frequency Hopping

In the frequency hopping method, the transmitted frequency is converted pre-assigned channel by spreading the narrowband signal as a function of time. The pre-assigned channels are identified by following the order of pseudo-random.

Direct Sequence

In the direct sequence method, the signal is expanded over a broadband part of the radio band to spread the signal. It encodes for being the transmission of digital data by using PN (pseudo noise) code generated locally.

Spread spectrum signals have a large number of different signaling formats and they are used to communicate data symbols. As a result of this, although the receiver can identify one of these formats, it fails to detect any other formats through a single message. The spread spectrum is known as the multiplicity factor of a communication link as it contains many formats.

CDMA (Code Division Multiple Access)

CDMA is a type of direct sequence involving spread spectrum technology. It helps many users to engage the same frequency and time allocations within a mentioned space band. CDMA differentiates signals from different signals within the same spectrum by assigning unique spreading code for each user to layout base band data before transference. Considering this platform, 2G and 3G services have been made. Chip rate represents a signal spreading rate. CDMA offers more analogue capacity than AMPS and more calling capacity than TDMA and GSM systems.

PCS (Personal Communication System)

PCS involves a combination of intelligent networks and cellular networks. It represents SST (super simple transfer) into office protocol. It helps to distinguish physical components of switching networks such as signal control point, signal service point and signal transfer point from the services which SST network offers. As the North American implementation, PCS follows the European GSM standard. GSM involves its own TDMA techniques and offers expanded capacity and specific services such as call forwarding, caller ID and short messaging. A critical quality was roaming seamlessly allowing subscribers to move across the boundaries of the provider. A secondary frequency band was specialized in 1990. This band comprises two domains ranging from 1710 MHz to 1785 MHz and from 1805 MHz to 1880 MHz respectively.

DECT (Digital Enhanced Cordless Telecommunication)

ETSI (European Telecommunication Standards Institute) had developed DECT which is a type of PCS. It was developed as a PABX data LAN of wireless communication. It requires minimal access to open cordless representing a closed environment. It involves a TDD or TDMA frame structure using 24 slots equally allocating to operate uplink and downlink. It helps to specify both duplex and simplex operation. It utilizes multilevel modulation to achieve a high level of data rates.

GSM (Global System Mobile Communication)

The Group Special Mobile developed GSM and it is considered an initiative of the CEPT (Conference of European Post and Telecommunication) administration. The primary band of GSM involves 900 MHs band including two sub-bands of 25 MHz. GSM systems, such as ICO, Globalstar, and Iridium utilize LEO (low-earth orbit) constellations or MEO (medium-earth orbit) satellites and continue operations for spreading networks for existing PCS networks and cellular networks. These systems extend the network services to any location of the earth’s surface utilizing dual-mode.

PCSS (personal communication satellite service) incorporates QPSK modulation and both TDMA and FDMA to utilize LEO satellite repeaters. The international roaming and features such as frequency hopping, short message service, privacy and encryption, and discontinuous transmission are the major advantages of GSM. Other benefits are waiting, forwarding, hold, barring and teleconferencing. The basic architecture includes base station sub-system, system interworking, network sub-system, mobile stations, and system interfaces. The activation and operation of a GSM terminal require SIM (subscriber identity module).

New Developments of Mobile Communication

GPS (Global Positioning System)

GPS helps in reliable navigation within any position of the earth and the operation is allowed within all kinds of weather conditions of a day.

Airborne, marine and land users can utilize the GPs system which was developed in 1983. It includes three segments such as space segment, user segment, and control segment.

Space Segment

GPS involves 24 NAVSTAR satellites including three spare satellites that are positioned within the orbit at a distance of 20,200 km. considering six circular orbital planes involving a 12 hour orbital period for each orbit. These satellites broadcast continuously navigational signals named coarse acquisition code by operating an L1 band with 1.5 GHz frequency. Anyone can receive these codes to decode and find navigational parameters such as latitude, velocity, longitude and time.

Control Segment

The control segment has an MCS (master control system) and many smaller earth stations named monitoring stations positioned at various places within the world. MCS receives measured data which is delivered by monitoring stations by tracking satellites. MCS returns satellite parameters to the satellite by computing them. As a result of this, all GPs receivers get broadcast service.

User Segment

The user segment includes all stationary and moving objects along with GPS receivers. As GPS receiver computes its velocity and position in every second as it is a multi-channel satellite.

Bluetooth

Bluetooth technology can be compared to WLAN technology. It aims to piconets that are within the local-area network involving limited coverage and eliminating the requirement of infrastructure. A collection of Bluetooth devices termed as piconet and synchronized to the same hopping sequence. One Bluetooth device within the piconet performs as master and all other Bluetooth devices perform under it. The master device selects the hopping pattern and other Bluetooth devices synchronized to the selected pattern. The master device uses the device ID, which 48 bit a unique identifier in the

world, to select the hopping pattern. It also assigns the address of a 3-bit active member for all active devices.

All parked devices utilize the address of an 8-bit parked member and there is no need for an address when the devices are in standby mode. The aim of Bluetooth development was to utilize a low-cost, single-chip and radio-based technology for wireless networks for headsets, laptops, notebooks, and so on. Bluetooth operates within the ISM band with 2.4 GHz. For modulation, Bluetooth transceivers utilize Gaussian FSK and they are categorized within three power classes such as Class 1 with a maximum power of 100mW, Class with a maximum power of 2.5mW and Class 3 with a maximum power of 1mW.

Development of 1G to 4G

1G System

In 1990, the 1G feature was released for use in GSM. 1G system represents analogue systems like AMPS which divides the bandwidth by using FDM within significant frequencies for being assigned to individual calls.

2G System

The 2G system represents a second-generation digital mobile system utilizing either CDMA or TDMA method. Digital cellular systems have many benefits over analogue by utilizing digital modulation. They also include more privacy, better application of bandwidth and incorporation of error identification and correction.

2.5G System

By adding the latest bandwidth technology, the 2G system has been converted into a 2.5G system. It allows the transmission of high-data-rate for Web browsing and it also allows WAP (wireless application protocol) which is a new format language of browsing. The various upgrade paths include GPRS, HSCSD (high-speed circuit-switched data) and EDGE.

HSCSD develops the data rate of available application to 14.4 kbps comparing to available data rate GSM to 9.6 kbps. HSCSD can offer a raw transmission rate maximum of 57.6 kbps to individual users.

EDGE represents 8-PSK which is a new digital modulation and involves octal phase-shift keying. It is famous as a coding scheme and multiple modulations by allowing nine various air interface formats including the changeable degree of error control as well as protection. These formats are quickly and automatically selectable. The coverage range of EDGE is smaller than GRPS and HSCSD.

3G System

The 3G system has been developed to overcome the defects of the 2G system and 2.5G system. It involves a wideband wireless network to offer developed clarity within conversations. Different countries within the world are recently selecting new radio spectrum bands for the accommodation of the 3G network system. ITU has built 1700 to 1855 MHz, 2500 to 2690 MHz and 806 to 960 MHz bands. In this system, 2 Mbps is the targeted data rate. Packet switching is used to send data and circuit switching is used to interpret voice calls.

3G W-CDMA (UMTS)

UMTS (universal mobile telecommunication system) or W-CDMA convinces backward compatibility by using TDMA technologies of 2G and 2.5G. W-CDMA has been made for packet-based always-on wireless network service maintaining an air interface standard. As a result of this, computers and entertainment devices can share and a similar wireless network system and make a connection to the internet system anywhere and anytime. W-CDMA allows a data rate maximum of 2.048 Mbps when the user is in a stationary position and allowing high-level data, streaming audio, multimedia, and broadcast type services to the consumers.

The time slots within W-CDMA help in periodic function but don’t help to separate users. The range of bandwidth per W-CDMA channel is from 4.4 MHz to 5 MHz. The 3G system is used within multimedia communication

devices and personal mobile phones. It allows video conferencing and also helps in position-based services.

3.5G System

The 3.5G system helps in speed and high-level of through-put at packet data rates of 14.4 Mbps to support the high-level of data requirements of consumers.

4G System

Chapter 7: Wi-Fi And Internet Troubleshooting

Wi-Fi is an essential technological development of the modern period. It is a wireless network technology to connect a wide range of digital devices, hardware and accesses points involving a radio transmission technology. It is convenient to use for any consumers. It actives over more distance than infrared or Bluetooth and is also below the power of unobtrusive technology. It is compatible with many operating systems, advanced printers, and your devices. It is a perfect option for portable devices such as smartphones, laptops, tablets, and so on to connect the internet.

Wi-Fi Alliance is an association manufacturer and they regulate standard definition and product certification and they also govern Wi-Fi. There are many levels of Wi-Fi network services involving different power

requirements and speeds. The earliest level of the Wi-Fi network system was 802.11b. Then, it was upgraded to 802.11a and 802.11g. The latest standard of the Wi-Fi network system is 802.11n.

How Does Wi-Fi Work?

Wi-Fi network involves radio waves to transmit data or information across a network system. The computer will have to include a wireless adapter to translate data sent within a radio signal. This same signal will be transmitted using an antenna to a decoder named as the router. Then, the data or information will be delivered to the internet by using a wired Ethernet connection. As Wi-Fi serves for two-way traffic, the received data from the internet will pass by using the router to be coded within a radio signal for being accepted by the wireless adapter of the computer. Wi-Fi makes a network within your office or home where your computers will get broadband internet.

How Can You Set Up Wi-Fi?

There is need specific equipment if you want to use Wi-Fi and these are a wireless transmitter named WAP (Wireless Access Point) and a Wi-Fi adapter. There are many ISPs (Internet Service Providers) who set up new customers including Wi-Fi facilities from the outset. If you want to set up Wi-Fi at home, you will have to need a wireless router and you will also have to access the admin management pages of the router to arrange the perfect setting such as password, Wi-Fi channel and network name. Sometimes, wireless adapter built-in is not available within the device and you can purchase a Wi-Fi USB adapter. You can make a wireless hotspot from your computer to share the internet connection with the other devices. Wi-Fi connection is widely used within airports, cafes and many public buildings.

10 Steps for Troubleshooting of Wireless Networking Issues

There are various factors related to wireless networking issues. 1o Steps for troubleshooting of wireless networking issues have been explained here.

Before pointing it within the proper direction, turn it on: Sometimes, it is difficult to find out the most obvious reason of trouble within the network system. Most of the time, faulty assumptions are made. When your Wi-Fi network connection doesn't work, it will be the best option to follow the absolute basics and these are:

- You should check whether the wireless adapter is connected without thinking about the type of device that you are using.
- You should ensure that your tablet or phone is not in Airplane Mode.
- There are many WLAN environments that involve multiple service set identifiers and all of them will not help you to reach your desired place. When your Wi-Fi network connection is active, you will not get any option to check whether you have selected the right network services to reach your desired location. Some wireless internet connection involves dead ends for specific purpose dead ends where internet connection is not available.
- Sometimes, it is essential to take coordinated permission for using Wi-Fi considering the type of network services which you want to connect. If you over-look this condition to follow this step at the time of making a network connection, you will not get network service.

Try to Understand the Level of The Issue: If you want to solve the issues for your network connection, you will have to understand how far the issues have been spread. You should follow the steps below to understand it.

- Do you have a connected relative device? For example, can you make a connection using your laptop, but not using your smartphone? Can you relate your network connection with anyone closer to you?
- If you understand that the issue is related to the user, single device or password, you can take the assistance of the help desk to get arrangements properly.
- Devices of any client or ant accounts of a user may have the issues whether you are using a high-quality Apple product or

you are working as a C-level employee, everyone usually faces Wi-Fi networking issues.
- When multiple users face network problems, you can give more explanations to IT and you will get the solution within a faster way.

Follow the basic diagnostics : When your Wi-Fi network connection doesn't work, smartphones, laptops, and tablets can display and help you to get information on a basic level. But, you will have to understand what you are trying to find out. Don't make decisions by considering scant information.

- The signal bar usually indicates the network connection strength. If the signal bar is not visible or too weak, it represents that there are some issues within your network connection.
- Sometimes, the users' devices are not perfect at roaming. You can get a poor network connection signal due to the poor performance of your device.
- To ping, a destination is one of the most effective network troubleshooting steps. It will help you to understand whether the target device is active to maintain both directions network connection path between the destination and the source. But, ping may be inactive for many reasons starting from the firewall setting of the host to filtering throughout the networking path.
- You can include DNS (Domain Name System) test to find out DNS issues. DNS test is an easy procedure and explains lots of things for troubleshooting.
- Most standard network systems include labeling system. If you have an issue for the access point, you will note down the specification of labeling and the visible LED color when you are reporting for the issue.

Try to Understand the framework of Failure Point: Most of the framework of WLAN is complicated than a Wi-Fi network connection. But, if you understand common high-standard failure points regarding the framework of the connection. Different types of automated tools help to offer a well-administered network connection.

- Wireless network access points get failure and stop working for different reasons. The network connection component can be failed due to physical damage or firmware corruption.
- Sometimes, the access point of wireless internet connection can be overwhelmed due to high client counts or using high bandwidth applications by a few clients. Otherwise, when you are trying to get an internet connection within a crowded access point, your internet connection may be slow or inactive.
- Your network connection can be slow or hampered when there is a problem within a switch that supplies power to many access points.
- Sometimes, many access points are managed by a controller. When the controller gets damaged or fails to do work, there create big issues within the network system.

Try to Measure the Number of Application Issues and Hazard to Reach Destination : Sometimes, you are not able to work using a specific application although you are properly connected to the Wi-Fi network connection. Or, you are trying to open a website page, but you are getting an error message. Generally, this condition may occur due to other conditions of network system than a Wi-Fi network connection. When you hit a roadblock, you will try to measure the quantity that is acting properly or what is inactive. Specifically, this type of fault is related to the WLAN if some significant destination protocol is blocked within a firewall setting. By using radiofrequency and access point of the network system, you will collect information which is essential for troubleshooting by the administrator.

Try to Untangled the Complicated Issues of the Client device : When everything is arranged properly, a specific device may be problematic to run within the network system. You will have to find out the mistake to untangle the complicated issues of the client device. You will leave the device alone and otherwise, there will create a bigger issue. You should watch out that specific device and allow it to be scrutinized involving the help desk. Generally, hardware drivers are not automatically refreshed although the Windows updated is turned on. You should examine the

hardware driver for your wireless network connection adapter, a chipset for freshness and basic input or output system within the network.

The company secured internet connection is more complex than using only a pre-shared key or password. Sometimes, it is essential to arrange several settings before connecting the specific device. Generally, business internet connections are concerned with strong encryption, authentication and details logging for each connection for troubleshooting as well as auditing. This creates complexity when you join a specific device within your internet connection. You should check whether the administrator of your internet connection has provided any written instruction or arrangement tool to fix any specific device within your internet connection.

Sometimes, there may be required to change occasionally password of your internet connection system. You should check whether the Caps Lock is not active before entering the password to connect your device with the network system.

Make a Report for Issues Involving Good Information: Usually, a business WLAN has many components which support to supply the network connection properly. You can get a solution quickly for issues within the network when good information is conveyed regarding the issues to the IT person who handles the issues or formal help desk. Some important questions and information are giving below for troubleshooting wireless network connection issues.

- What is the location of the issue? If it is a room, did the network connection issues follow you to a floor, different room or a building?
- If many devices are connected with the network system, did they all involve with the issues? If the answer is negative, you will have to mention which devices are working well or which devices are not working.
- You should mention when the network connection issues have been started.
- You will explain your experience when your network system is failed to connect your devices.

- You will mention whether you have got an IP address or not. You also mention if you have done the DNS test for your network connection.
- You will try to provide specific information when you are reporting about your network connection issues.

Follow up the Symptoms of Code Bugs: There is much latest AI-driven analytics dashboard and they will not inform you about the code bugs which can attack your Wi-Fi network connection. The administrator of the network connection usually takes responsibility for resolving code bugs. Some symptoms of code bugs are given below.

- Continuous rebooting for different access points, from a few to thousands.
- APS will prevent the client's accessibility.
- Significant features will become inactive.
- Some general subsets within the client's devices will face the same issues whether some other client's devices are fine.
- The network connection pattern for access points or Wi-Fi clients will be erratic.

Use Your Network Connection Properly : Presently, wireless network connections are usually integrated and complicated involving several numbers of components to develop a larger internet connection. There is an effective response within the tools, documentation, training, and monitoring when an issue hits the networking system. It is essential that the supporting team of your internet connection will involve the significant software and wireless-specific skills and also equipment for the test to eliminate the fog due to respond to the issues.

A standard network framework, access points, switches, well-labeled cables, and latest call lists can influence to resolve the network connection issues quickly. Periodically replacement of tools and occasional training of staff are essential to reduce the chances of creating any issue within your network system. Maintenance of the framework accurately and labeling of everything are required time, but these are advantageous for troubleshooting quickly.

Select the Gadgets or Devices Properly : You should choose properly the gadgets or devices supported by internet connection. Sometimes, your Wi-Fi connection may not support when you purchase big expensive devices. There are many reasons for which this type of purchase may not fit for the network system at home. There are some products or devices which are not featured with proper security.

Slow Internet Connection

Sometimes, you may find issues to upload files or to open any website page due to a slow internet connection. Five common issues, which can result in a slow internet connection, have been explained here.

Internet Thieves: Wi-Fi is one of the easiest options to get an internet connection. Sometimes, other people can use your internet connection unlawfully when it is not secured properly. If you choose a simple password for network connection or if you don’t set any password for internet connection, other people can easily access your internet connection. You can utilize a free program named Wi-Fi History View to analyze each device connected to your network and check IP addresses that are unknown to you. You should change the router’s password to protect your internet connection. You can take the help of the Router Password website to locate the default password of the manufacturer. By creating a complex password, you can maintain your network security.

Outdated Equipment: You will have to upgrade the equipment of your network connection. Wi-Fi routers are available in different categories. “AC” routers have more features and have better functionality than the older “B” and “G” router models and even “N” router model. It increases bandwidth allowing more data for transmission without slow down your internet connection.

Congestion : There are too many people within an apartment and crowded neighborhood and they may have the same Wi-Fi channel. When they use the internet connection at the same time, the speed of the internet connection can be slow during peak hours. You can solve this issue by selecting various channels for your Wi-Fi router. Generally, you can choose

11 channels for having a router of 2.4 gigahertz frequency. You can try other channels rather than recommended channels such as 6,1 and 11 to get more speed within your network connection. Otherwise, you can purchase a more powerful router such as the 5 gigahertz frequency router.

Security Settings of Your Router : Sometimes, usage of unauthorized bandwidth to protect your network connection can cause less speed within your network connection. If your network connection is not secured or you are using WEP, you must replace your network security system instantly. The reason is that anyone can easily use your open network system by stealing your Wi-Fi connection. On the other hand, the hackers can easily hack your network connection secured with old WEP. You can use WPA2 with AES to protect your network system as well as high speed for your network system.

Positioning at Out of Router's Range : The transmitted signal of a router is useful for a limited distance. So, there may be the existence of a dead zone or hot spots. You can use a tool named Heat Mapper to identify the most powerful Wi-Fi signal zone. After identifying the problem area within your home, you can buy a Wi-Fi extender to enhance the range of the router's transmission. You can get different ranges of Wi-Fi extenders and you can choose according to your requirement.

You can buy a mesh system as a second option to develop the coverage area of your network connection. A mesh system comprises a series of the small-sized router to sync with one another to enhance the coverage area of your network connection. It will help you to get the perfect speed of network connection throughout your home or your desired position.

If you inform your ISP to find out the reason for the slow internet connection, hey will make lots of inquiries before solving your problems. You can follow some internet troubleshooting checklists which have been listed here to save your time.

Reset Your Internet Connection Adaptor: You will select troubleshooting by making right-click on the internet access icon within your device Window Taskbar. Then, Windows will act automatically to reset your

internet connection adaptor to improve the speed of your internet connection.

Restart Your Router and Modem : Firstly, you will ensure for power down of your modem and then power down the router. After waiting for ten seconds, you will plug in the modem. You will power up the router when the modem becomes completely operational.

Apply Internet Speed Test : You will get many resources for online speed test and they will help to know the accurate speed of your internet connection. Then, you can compare the available speed of your network connection to the mentioned speed of network connection within the contract of your ISP. You can contact your ISP to upgrade the speed of your network connection.

Contact Your ISP for Assistance : If there is no improvement for the speed of your network connection after applying many fixation procedures to speed up your network connection, you should contact ISP for checking the issues and the right solution.

Install a Dual-Band Router or Choose a LAN Connection : There are many conditions when you can install a Dual-Band Router or choose a LAN connection to improve the speed of your network connection. One of these conditions is when you are using network connection within an apartment building area depending on a Wi-Fi modem, your ISP may be failed to provide the services for boosting the speed of your internet connection.

Another condition for slow down your internet connection is when there are several Wi-Fi network connections within the same location, there creates a competition among the different Wi-Fi connections for a free channel. It results in the less speed of your internet connection.

You can install a Dual-Band Router to solve the above-mentioned issues. Otherwise, you can choose a LAN connection to build an internet connection directly to your PC.

Chapter 8: Network Services

In this chapter, you will learn about network services and their explanation including examples, uses, and benefits. You will get a comprehensive knowledge of network services after studying this lesson. The network is applicable in many areas whether these areas are known to you or not. Modern society likes technology-based applications of networking which play a significant role in daily life. For example, a wide range of networking is used in phone calls and messaging and it allows us to get several benefits within different areas.

You can apply network services in different levels of work to get more benefits than basic functions. It is an effective way to contribute a high level of services by using the least amount of dependability, performance and specific security.

What is a Network?

A network explains a system that interconnects devices to build communication for exchanging resources and services by utilizing some common standards. For example, the network plays an important role in achieving professional success. The internet is a great application of

networks to build communication within the world. The network is one of the easiest ways to spread your network to create or maintain relationships with your family, relatives, friends, colleagues and desired persons.

Types of Networking Services

Types of networking services are as follows.

WAN (wide area network) optimization: Sometimes, the company's WANs face performance issues due to constraints of bandwidth and latency. WAN optimization services involve different techniques to prevent them by including protocol optimization, reduplication, local coaching, compression, and traffic shaping. Generally, WAN services help to connect computers placed at a large distance and even miles apart. WAN service can be owned by multiple owners and can be administered to the public globally.

WAN can include the connections involving the company's headquarters, cloud services, branch offices, benefits of colocation and other benefits. WANs are not limited to the same geographical position. The company WANs support users for sharing services, access to applications and other types of resources that are centrally located. WAN connections can include wireless and wired technologies. Wireless technology of WAN connection can involve cellular data networks such as Fi, 4G LTE or satellite network services. The expanded security is essential and it depends on where the end-users are working. The end-users of WAN should use antivirus software and firewalls to resist unauthorized compromises or access to their devices.

Interconnection: If you want to exchange data, resources or digital information directly, privately and securely within your business, interconnection strategy is the perfect option for you. When companies need to make a connection with customers, clients, and employees for collaboration or exchanging data globally to create value within their business, they choose many-to-many connectivity which exists within interconnection services. It helps them to make a connection with different resources and devices simultaneously and instantly. It results in a smooth and fast transaction according to their business needs.

Interconnection involves one-to-one or one-to-many connection, direct and personal connections to deliver the most secure and the best performance.

By creating digital ecosystem density, an interconnection provides many-to-many connectivity when the parties are located within proximity. Interconnection is essential at exchange points of distribution of company, networks service providers and so on as they want to collect and create personal and low-latency connections by using their clouds, digital ecosystem, users, data repositories, employee's and whatever their essential to run their business.

SD-WAN (Software-Defined Wide Area Network) : It is a virtual WAN technology. It helps to distribute network service across WAN by using SDN (software-defined networking) which helps to find out automatically the most advantageous method to route traffic within the data center sites and branch offices. Companies choose SD-WAN services to hold any combinations of transferring services such as LTE, MPLS and broadband internet connection between users and applications. By using a centralized control function, SD-WAN services direct data and resources with security and intelligence. It develops application performance, by increasing business productivity, user experience and reducing IT cost.

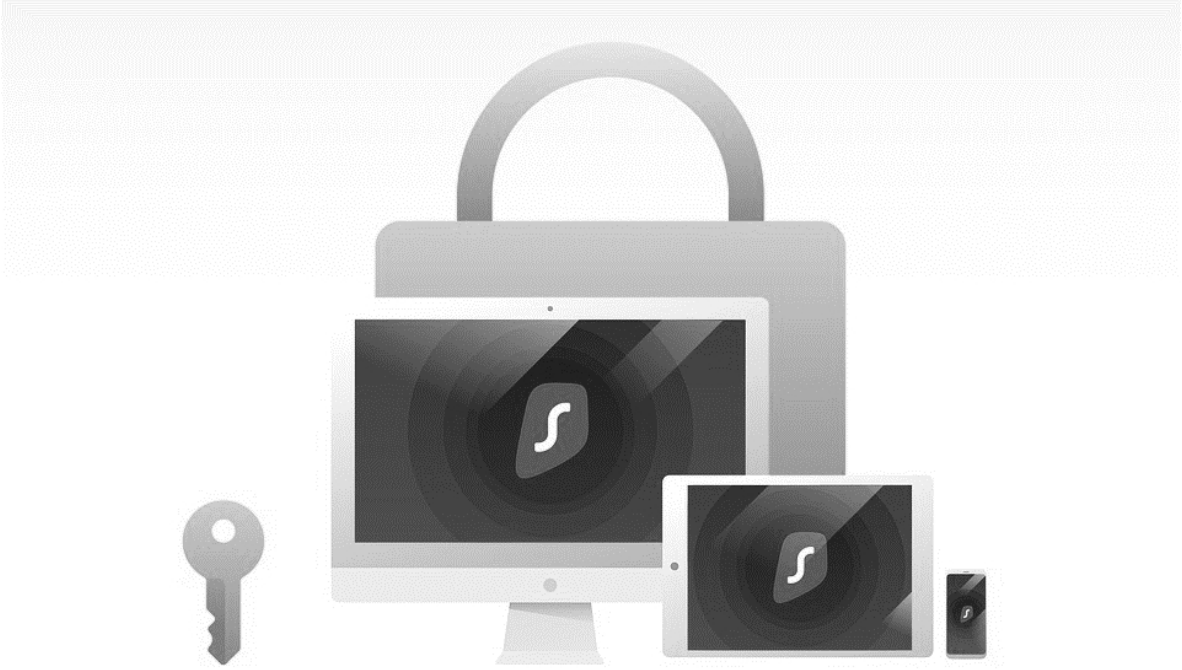
MPLS (Multiprotocol Label Switching): It helps to speed up and shape network traffic flows. The companies can forward data buckets t layer 2 the switching level rather than passing to layer 3 router level when they choose MPLS services. In late 1990, MPLS was made as a more effective option than traditional IP (Internet Protocol) routing. When the companies and service providers want to define LSPs for the implementation of QoS (Quality of Service), they apply MPLS.

MPLS can fulfill specific service level agreements related to downtime, traffic latency, and jitter packet loss. MPLS also assists in classifying traffic and also to make VPN (Virtual Private Network), virtual leased lines and virtual private LAN (Local Area Network). Moreover, it is not tied to any specific transport medium or protocol. It assists in transferring services over Ethernet, IP, ATM (Asynchronous Transfer Mode) and frame relay or any of these agreements to make an LSP (Local Strategic Partnership). GMPLS (Generalized Multiprotocol Label Switching) develops the MPLS services to handle lambda switching, TDM (Time-Division Multiplexing) and other kinds of switching technologies.

Ethernet Private Line Network : You can choose EPL (Ethernet Private Line) network services as high efficiency and cost-effective solution if you have businesses within two or more different locations. It helps to replace traditional TDM (Time Division Multiplexing) by connecting CPE (Customer Premises Equipment) with UNI (User-to-Network Interface) which is cost-effective. It doesn’t traverse the public internet. EPL service is a close date transferring service maintaining security inherently involving no encryption needed. You can use it within a bandwidth speed ranging from 10 Mbps to 10 Gbps.

EPL gives a unique QoS (Quality of Service) without sharing services and always following the direct network path. It is used within the business by providing reliability and security for different applications such as file sharing, video conferencing, credit card processing, Ethernet VOIP and data back-up. It can be structured to carry video, internet, voice and data services collectively over the same connection of EPL services. EPL service also termed as Metro Ethernet, Point-to-point Ethernet or Carrier Ethernet Service.

Chapter 9: Network Security



Network security is a method to involve physical as well as software-based preventive measures for the protection of underlying networking configuration against misuse, modification, malfunction, destruction, unauthorized access, and improper disclosure. Presently, most people depend on the internet to perform their social, professional and personal activities. Some dishonest people attempt to violate the privacy of others by destroying internet-connected computers. Network security is executed by using tasks and tools to resist unauthorized programs and people to access your devices and networks connected to them.

Sometimes, hackers make public mistrust and negative image of an organization by stealing detail information of a customer and sell them to be applied within a fraud case. The attackers mainly target on the data and communication of users within a network system. They also manipulate the system to get facilities by physical access or damage the device of the users.

Basics of Network Security

Basics of network security follow the strategies of protection, detection, and reaction. You should structure your system of the network as accurately as possible when you follow the strategy of protection. You will have to keep the ability to detect any changes in your structured network or the indication of network traffic issues when you will follow the strategy of detection. You will have to respond instantly and arrange a safe state as soon as possible after the detection of security issues. Basics of network security services are followed to secure data, resources or information from any type of malicious use and to provide protection to information, data or resources within your personal computer or laptop used as personal or public domain network area.

Why do You Need Network Security?

When you connect your device with the internet or other network services, you will get opportunities to be connected with different possibilities within the world. You will be able to utilize the opportunities without keeping permanently within your device. You also can allow others to be connected with you to work jointly or other purposes. But, there are lots of hackers and attackers who are always active in misuse or access within an unauthorized way. There are many reasons to use network security services and these are as follows.

- It protects data, resources or information from being a misuse
- It provides safeguard information or data from being unnecessarily delayed within the route followed for the delivery of data to the required place within the desired time.
- It protects the data from any unwanted change.
- It prohibits a specific user within the network to send messages or e-mail hiding the identification of the real sources of the sender.
- It protects hardware such as laptops, hard disk of PC and laptop from being attacked by viruses or malware to destroy the system or to corrupt or delete all of the stored data and content within the devices.

Types of Network Security

There are several specific types of network security and some of these types of network security are as follows.

Access control

It helps you to prevent unauthorized devices and users from accessing your network. It only allows users who have permission to access a limited set of resources authentically. Access control systems act to identify the authentication and authorization of the users. It also helps to reduce the risk of unauthorized users by controlling the fundamental elements of a security program which help to ensure whether the policies of access control and security technology are in the right place for the protection of secret information such as customer details.

Generally, the companies have configuration and process which restrict assess of network application, computer, system, file and confidential data such as intellectual property and personal information for identification. In the case of large businesses there are lots of employees and it is difficult to identify an employee. Then, the access control system helps to prevent strangers and to allow the employees. Moreover, it allows a business to restrict access to specific areas. It reduces accidents and thefts within the business by increasing safety.

Anti-malware

Anti-malware software resists infections caused by different types of malware such as all kinds of viruses, ransomware, rootkits, and spyware. It can be used in personal computing devices, network appliances or gateway servers. It is also useful for cloud services. Moreover, it scans all incoming network data used in malicious software and it also blocks any threat if it can detect. It can identify malware of advanced level and provides significant protection from the attack of ransomware. It resists users to visit websites that are known for spreading malicious code. It also resists the distribution of malware viruses when one device gets infected. It creates and follows up metrics about the quantity of infection and the required time to clear those infections. Sometimes, it assists the administrators to understand in what way the malware has attacked the compromised network or device.

Application security

It explains security measures when you apply it aiming to resist code or data within the app from being hijacked or stolen. It is a method of improving, adding and checking security features within applications to resist vulnerabilities. Presently, applications are frequently available within different networks and connected to the cloud. As a result of this, threats and breaches of security increase within the applications. Checking of application security can find out weakness at the level of the application by assisting to resist attacks of hackers. There are several types of application security such as authentication, encryption, authorization, logging, and application security testing. Application security of authentication helps to identify authorized users. The user will have to provide a user name and password at the time of logging in to a specific application.

Behavioral Analytics

It involves software tools to identify a pattern of unauthorized data transferring within a network. Tools of behavioral analytics follow up and report anomalies to judge considering the basics of normal behavior. A software product of behavioral analytics security can be marked as BTA (behavior threat analysis) product or UBA (user behavior analysis) product. Some products involve behavioral biometrics features for mapping significant behavior such as typing style. It has software to scan the deviation from the normal baseline. It also helps to decide intelligently whether an anomaly can be harmful or not.

Data Loss Prevention (DLP)

It includes a set of procedures and tools to be sure that confidential data is not misused, lost or accessed by unauthorized users. DLP software of network security helps to classify confidential, regulated and business-critical data and to detect policy violations termed by companies or within an already defined policy pack. Generally, DLP is advantageous for mainly three objectives and these are compliance, IP (intellectual property) safeguard, personal information safeguard, and data visibility. It controls and monitors the flow of sensitive information within a network. Some

sensitive data of business are source code, product design reports, process documentation, financial reports, and so on.

Email Security

It explains different techniques to keep confidential data within email communication and also prevents unauthorized access, compromise or loss. Email is a common medium to expand spam, malware and phishing attacks. Generally, phishing attacks aim to the business department which maintains confidential data or financial information. Sometimes, email messages sent by malware may be destructive. A phishing email can contain malware within attachments structured to appear like valid documents. A phishing email can include hyperlinks of websites that act as malware. Moreover, phishing emails target to steal information by asking recipients for confirmation of their passwords, login information, bank account number, social security number, and even credit card data.

Firewalls

It monitors outgoing and incoming network traffic and blocks or stops or allows data packets considering several security rules. It builds a barrier between oncoming traffic sourced externally and your internal network services. It also resists malicious traffic such as hackers and viruses. Packet-filtering firewalls are one of the most common firewalls. They help to check packets and prevent them from passing through the network services if they mismatch considering security rules. It can be classified into two types such as stateful and stateless. Stateful firewalls keep information within their memory about passed packets in the past. Stateless firewalls check packets separately lack context which can be easily hacked. It blocks Trojan horses from the outset before getting a chance to harm your computer.

Intrusion Detection

It monitors suspicious performance and issues alerts of network traffic due to the identification of these types of performances. It scans network services for policy breaching and harmful performance. If you set up properly the system of intrusion detection, it will help you to identify what normal traffic within the network appears as compared to malicious

performance. The intrusion detection system can be categorized into NIDS (Network Intrusion Detection System) and HIDS (Host Intrusion Detection System). NIDS observes passing traffic within the whole subnet and checks their behavior. HIDS monitors outgoing and incoming packets when malicious performance or suspicious activities are identified. Usually, it is used in critical machines.

Network Segmentation

It helps to divide a computer network system into smaller parts improving network security and performance. It can be used within large bank networking services. Network segmentation services can prevent traffic from all branches to reach the financial system by enforcing network segmentation services. It decreases network congestion. It restricts the spreading area of an attack by improving cyber security.

Network segmentation can prevent harmful traffic from reaching unprotected devices within the network services causing an attack. Moreover, it limits the in-scope system numbers to reduce the cost of regulatory compliance. It helps to improve the performance of network services including fewer hosts per subnet to minimize local traffic. It allows for separating broadcast traffic to the local subnet. It has quality access control by allowing users for only accessing important network resources.

Security Information and Event Management (SIEM)

It offers a holistic view to explain the happenings within network services at the right moment and assists IT teams in being more proactive in the fight against network security threats. The application of the SIEM system is advantageous to protect companies of any size. It helps to increase the efficiency of network services. It also resists potential network security threats. Additionally, it reduces costs and the effect of network security breaches. It helps to make better reports, retention and log analysis.

VPN

It builds an encrypted and safe connection to protect less secured network connections such as public internet. It involves tunneling protocols. There are several types of protocols are used in VPN and these are IP security,

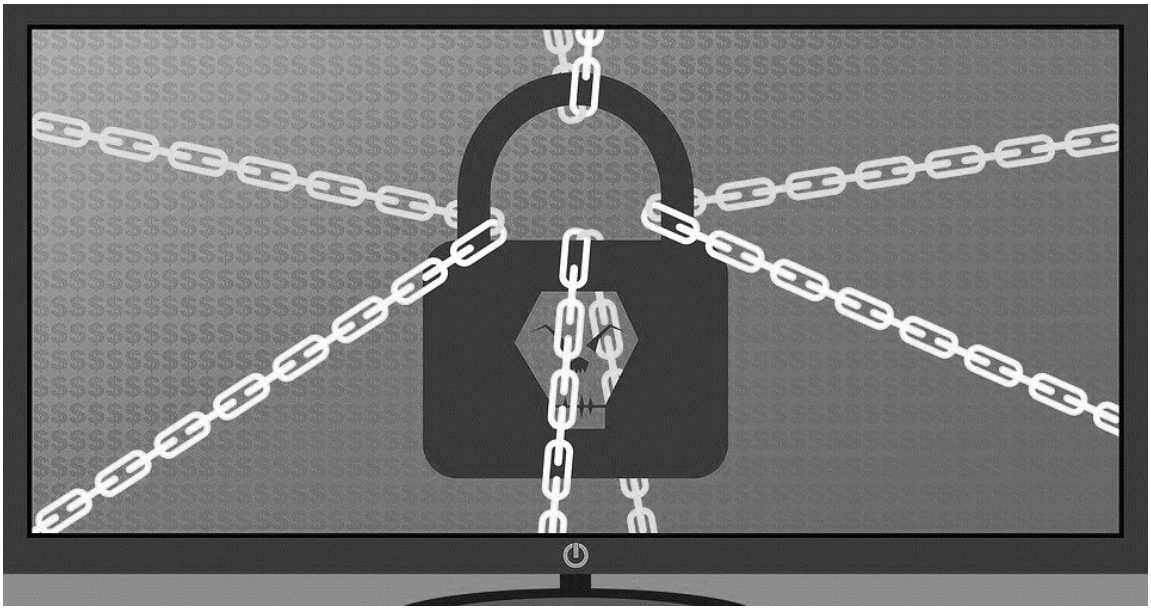
point-to-point tunneling protocol, secure sockets layer, layer 2 tunneling protocol, transport layer security, and open VPN. If you want to use a limited resource by using a VPN, you will have to be authorized for using the VPN app and you will also have to submit one or more documents such as biometric data, password, or security token. Anyone can protect data transferring on their mobile devices or can visit geographically limited websites by using VPN apps. It is advantageous for remote corporate employees, business travelers, and freelance workers. There are several types of VPN and these are remote access VPN, mobile VPN, site-to-site VPN, hardware VPN, dynamic multipoint virtual private network, and VPN appliance.

Web Security

It involves protocols and protection measures for the protection of web applications or websites. It prevents hackers or unauthorized users from entering or using your websites or web applications. There are various types of technologies are used to maintain high-levels of security. Some common technical solutions to check, build and prevent threats involve Fuzzing tools, Web application firewalls, password cracking tools, black box testing tools, security or vulnerability scanners, and white box testing tools.

The security of websites and web applications can be hampered by using several services for threatening web security. Some of these services are password breach, data breach, code injection, SQL injection, remote file inclusion, cross-site scripting and so on. Most efficient web developers maintain the standard or OWASP and close observation on the web hacking incidents database to understand how, why and when the hackers hack different network services and websites.

Chapter 10: How To Secure Your Network?



A wireless network usually needs a connection between an internet access point such as a DSL modem or a cable and a wireless router to send a signal within a fixed range through the air. Any device for being within the range of router can pull the signal present on-air and can use the internet. You will have to take preventive measures so that anyone staying near-by you will not be able to access your internet connection.

Make Your Wireless Network Encrypted

You will have to encrypt or scramble by using different tools so that anyone can’t read it. Presently, most wireless devices are available with a different scheme such as WEP (Wired Equipment Privacy), WPA (Wi-Fi Protected Access) or WPA 2.

WEP: It is an old method to protect network services. It includes the fir generation equipment wireless networking services. Generally, old routers are supported by WEP.

WPA : Wi-Fi alliance develops WPA to give more data encryption sophistically than WEP. It involves the TKIP (Temporal Key Integrity Protocol). TKIP has a message integrity check, per-packet mixing function, a rekeying mechanism, and an extended initialization vector. WPA offers

supportive use authentication involving 802.1 x and EAP (Extensible Authentication Protocol). It also authenticates each user by considering a central authentication server such as RADIUS.

WPA2 : It involves AES (Advanced Encryption Standard) algorithms and CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) replacing TKIP. Generally, the WPA2 system requires a longer password to use network services than WPA. It offers an additional layer of protection and helps to secure public networks potentially. WPA2 is available in two versions such as WPA2-Personal and WPA2-Enterprise. The company's Wi-Fi system doesn't use WPA or WPA2-Personal as the difference exists in the shared password. By choosing WPA2-Enterprise, the company can avoid a shared password and can assign specific credentials to each worker and device. It protects a company from being damaged by a departing employee. Privileged accounts of any financial company should be always strengthened by longer as well as a stronger password and it is also essential to change the password frequently.

Your Default Home Network Name Should be changed

By changing the name of the Wi-Fi network of your home, you can make a better-secured network service at home. The malicious attackers will feel difficulties to understand the type of router used by you when you will change Wi-Fi's default name. If the hackers get information about your router manufacturer's name, they will be able to detect the vulnerabilities involved within the model of your router. Then, they will try to utilize them.

There are many reasons when people change the default Wi-Fi name and some of these reasons are as follows.

- Sometimes, you and your neighbor can use the same default Wi-Fi's name and you may confuse about your router and network services. To avoid your confusion, you can change the default name of Wi-Fi.

- It helps to enhance the security of your home network services. By choosing a customer name, you can discourage the network attackers. It will specify that your router is being administered conscientiously using generic defaults. The hackers generally target the weakest network within a residential neighborhood having several home networks.
- It is advantageous to keep your home network services. If anyone wants to use the network by scanning Wi-Fi signals from their mobile devices or phone, they will see SSID staying within the nearby network services.

Access to Your Network should be Limited

If you want to maintain network security, the NAC (Network Access Security) is one of the perfect solutions. Activation of a NAC system depends on that who or what has permission authentically to use the network. When a network follows a NAC system, it will include an access management system and designated identity. There will be a predetermined set of policies and parameters within the network system to allow or prevent the user from network access. There are many reasons for using a NAC system and some of these reasons are as follows.

- It helps to build a network connection for authentication, authorization, and accounting (AAA).
- It includes specific policies to maintain containment and continuity of valuable property.
- It helps to handle assets and identity.
- It controls users, applications of past authentication or device based on their functions.
- It helps the administrators to explain multiple access schemes to govern users as well as devices connected to the network services based on significant conditions such as device type, user profile, and location.
- When the company follows a NAC system on end-user and compute devices, it starts constantly checking and evaluation of the right software application and also about using of an updated version of devices or patching with the management. In case of

failure of these requirements, the end-user will not be able to access the network without an appropriate update of devices.

- A NAC system allows the guests only to access the limited area of network services of the company.
- In many industries such as healthcare and manufacturing, there is a great demand for the administrator to get a complete view of the ant device used within the network.
- The NAC system includes the application of security analytics and machine learning to identify malicious behavior that may lead to attacks by hackers or stolen credentials within the network services.
- A NAC system is advantageous to find out all devices connected within the network including fingerprints and profiles related to them. As a result of this, IT administrators get a global view of happenings within the network services.

Your Password Should be Unique

The selection of passwords for network services plays an important role in building network security. The password helps a user to prove his or her authentication for using a computing device within network services. You should follow some key points to set up a password reducing the chances of the hacking network by hackers. Some of these key points are as follows.

- By choosing a long and complex password, you can maintain network security.
- When you choose a long and complex password, it will take more effort and time to guess by the hackers.
- You should select a password including at least ten characters combining with letters, numbers, commas, percentage signs, and so on.
- You should not use the same password to handle different devices as it will be easy to take control of other devices if a hacker can find out the password of one device.
- You should avoid writing down the password as it can create the chances of hacking your password.

- You should not set a password-based on common things such as your last name, your pet’s name, your kid’s name, your hobby, and so on. The reason is that this type of password can be fused by others easily.

Your PC Should Have Antivirus Software

You will get antivirus software to protect your device within the network services. Usually, free antivirus software offers a simple scanning procedure by using the detection of your signature to locate already detected malware. On the other hand, paid antivirus software usually involves heuristic to catch kind of threat by utilizing a genetic signature to detect even new types of existing virus codes through the used files with the virtual atmosphere. It will also help to measure malicious behavior within the network. You can get several types of protections by using antivirus software and some of these protections are as follows.

Protection of Your Network System from Spyware, Viruses, and Trojans

There are so many people who know the term Trojan, but they don’t know how to manage them. Trojans represent a malicious computer program involving deceitful techniques to hack the network system. Generally, Trojans spread by using social engineering and it is not easy to identify as they usually look like legitimate software. If you click an email or link attachment an assumed source, Trojans will get the chance to unauthorized access your files. Viruses are harmful and they can destroy your system by replicating and infecting multiple programs. It is extremely difficult to identify viruses. You can eliminate efficiently by using special antivirus software. Malware spies are basically structured to take out categorized files which can destroy a business’s integrity.

Protection for File Sharing

Many businesses use USB drives, hard drives and another kind of file sharing device to share their files. External drives are in danger to the virus spreading specifically auto-run viruses and shortcut viruses. Virus

protection programs help to prevent any malicious virus causing infection within your network system.

Protection for Email Virus

Email antivirus software intercepts inbounds emails by body, header, and attachment including scanning upon system remain running and startup. Antivirus can identify any suspicious by analyzing independent email components for encrypted files and dangerous objects so that harmful viruses can not destroy your business security.

Protection by Making Diagnostic Report

The antivirus software is advantageous to make a performance report of statistically and broken down graphs to understand easily. A thorough diagnosis of network system offers essential configuration of companies including hardware issues, system response time and performance ratings.

Antivirus software ensures your business protection. It helps in real-time scanning for identification of any malicious entity and also removal of suspicious codes.

Turn On the Firewall

A firewall creates a barrier or shield for giving protection to your phone, PC, laptop, or any devices connected with internet services. Firewalls monitor data exchange within your computer, router, and servers to ensure network security. Most devices are featured with a built-in firewall and you will have to know the procedure of setting up for the built-in firewall of the devices. There several benefits for using a firewall and some of these benefits are as follows.

- You can avoid unauthorized remote access to your computer by involving firewalls.
- You can prevent messages linking to unwanted content by using a firewall.
- The firewall provides protection for your personal directories by blocking harmful or unsuitable content.
- The firewall helps to play online games safely.

Generally, four types of firewalls are used and these are:

- Packet Filtering Firewall: It is a basic level of firewall and provides protection for the internal network by creating separation between internal network and external network. You will have to maintain set up involving some values such as IP Protocol ID, Source IP address, IP Options settings, Fragmentation flags, Destination IP Address, ICMP Message type, and so on.
- Application Proxy Firewall: It is considered as the best and a high-quality firewall. It involves seven layers of the protocol to handle the traffic coming from the server.
- Network Address Translation Firewall: The router involves NAT firewall for distributing internet connections to the different devices.
- Circuit Level Gateway Firewall: It actives between the proxy server and the internal user. When any internal client makes a request to the proxy server, it goes by using Circuit Level Gateway Firewall.

Use VPN

VPN (Virtual Private Network) helps to connect your network over an unsecured, public and unencrypted network personally. There specific encryption versions to support VPN tools for providing protection to your data. It gives protection for the data which you send from your mobile device to an internet gateway. It encrypts the user's web session completely. It provides security for any bank or financial websites. You can get more access to your date by using VPN as it compresses all information to the server before sending you. VPN helps to maintain your privacy as it resists for tracking a person's identity.

Turn Off the Router When Not in Use

The router has dedicated software and hardware to forward data within the usage of an integrated addressing system. The router helps to build a

connection between the two different internet connections to forward information and data. It also allows us to make a flexible cross-network connection and also to build a larger network system. It also comprises of combination including other devices to strengthen the features of a firewall.

There are several advantages to turn off the router when not in use and these advantages are as follows.

- **Improve security:** By powering off your device, you can improve your network security. Wi-Fi war drivers or hackers fail to hack the devices which are offline.
- **Cost-effective:** You can save money by turning down your router, modem, and computers.
- **Surge Protection:** If you unplug a network device, it will provide protection for causing damage by electric power surges. It also protects your device from major power such as lightning.
- **Reduce Wireless Interference:** Sometimes, when major devices are running by using the router, the other devices can be weakened or unusable. But, they can be active when you turn down the router.

The Admin Credentials of Your Router Should be Changed

You can install a Wi-Fi router within your home to get internet access including your family. By using the password of your Wi-Fi connection, anyone can connect their devices to your network service. Your router’s signal is available within a certain limit of the surrounding area of your home. It is difficult to detect who is accessing your network when the password of your Wi-Fi connection gets out within the world. It is essential to implement some changes to protect your network services from intruders, hackers, and snoopers. You will have to control who is accessing your network. By following some important tips, you can maintain your network security and these tips are as follows.

- You should choose a complicated router password. If you share the password of your network service, anyone can enter your

network to access it. You can choose a password by selecting letters randomly including numbers and special characters. Fixing a password made by involving 20 characters is an ideal option to maintain your network security.

- You should maintain a limitation for using the password of your network service.
- You can maintain your network security by changing the password frequently.
- You can replace the password of the admin account by choosing random letters and numbers to build the security of your network service.

Turn Off The Plug ‘n Play

The plug ‘n play procedure allows devices to detect the network within your home and connect to the manufacturer for supplies and firmware updates. UPnP (Universal Plug ‘n Play) is an important element to create things related to the internet. It is advantageous to make the smart household appliance. UPnP is also advantageous to make a channel for hacking. UPnP helps to build cooperation between networking supported smart household gadgets and router. The hackers can hack or infect your household devices by including them within botnets which direct the access requests. You should turn off the plug ‘n play when you do not use the devices. As a result of this, you can maintain network security for the devices.

Change Your Default IP Address

An IP address is essential when you connect any device to the internet including the router. The router also has another IP address to connect the devices which use the internet through the router. There are some conditions when changing IP addresses is essential and these conditions are as follows.

- When the user of network services accidentally configures invalid IP address such as the setting of static IP addresses involving the wrong numeric range.
- If you install a new router and reconfigure your home network by using its default IP address range, you will have to change your default IP Address.

There are mainly two types of IP addresses such as static IP address and dynamic address. There are many advantages to static IP addresses. By using a static IP address, your computer can locate the server from anywhere. Moreover, it helps different computers to run different operating systems to access the host systems and to find out the same address every time. You can assign and handle the static IP address easily.

Disable File Sharing on Other Networks

After connecting to the internet using Dial-Up networking, you will be able to share files and printers on the TCP (Transmission Control Protocol) or IP (Internet Protocol) connection to the internet. You can prevent unauthorized access to your printers, files, and network by disabling file sharing. You will not be sure that online sourced files are malware-free. Generally, hackers target file-sharing application and infect them by using malware. When you download these contents, there may be a risk of security. It results in many security breaches if you have not strong protection for security. Sometimes, file sharing interfaces reveal the computer directory of the users without knowing them. As a result of this, hackers can get information for hacking.

There are many techniques for file-sharing and some of the file-sharing techniques are as follows.

- Removal storage media: It involves removable storage devices such as memory sticks, memory cards, optical disks, removable hard disks and so on. A user of removable storage media can share files to another person and the receiver can connect the services to transfer files.
- FTP (File Transfer Protocol): It helps to share files through the internet. All modern operating systems are available including

built-in networks. You will have to fix a valid login and password when you will want to access it.

- Peer-to-peer network: It is a very popular way to share files mainly for music and videos. The examples of peer-to-peer software are uTorrent and Bit Torrent.
- Online storage websites or file hosting services: Google Drive and Drop-box are examples of online storage websites or file hosting services. A member can upload documents, photos and so on by using a web browser.

Sometimes, your computer may be infected by malware through a malware-infected system when you connect removable storage media for your computer. If you transfer official files using FTP, your computer data can be exposed and create security risk as FTP doesn't include encryption for transferring data. Sometimes, when users of file hosting services are not vigilant and they keep confidential data within publicly accessible folders. By disabling file sharing on another network can help you to avoid above mentioned issues or risks.

Disable DHCP

DHCP (Dynamic Host Configuration Protocol) offers automatic, quick and central management for sharing IP addresses within a network service. DHCP helps to configure the default gateway, subnet mask and DNS (Domain Name System) server information on the devices. Usually, in homes or small businesses, the router plays the role of DHCP. When a user requests an IP address through a router, the host allots an available IP address and helps the user to communicate by using network services.

When a device with DHCP server is turned on and communicated to a network with DHCP server, it helps for sending a request to the server named a DHCPDISCOVER request. After receiving the DISCOVER packet, the DHCP server keeps to an IP address to be used by the device. Then, it provides the user the IP address with the DHCP server including DHCPREQUEST to accept it. The server confirms the user for having a specific IP address by sending an ACK (acknowledgment code) and also explains the range of time which the user of the device can use. DHCP

helps to manage the network easily. The user of the device can achieve IP address automatically and the user of the can move freely within the network set up facilitated with DHCP.

Upgrade Your Router’s Firmware From Time To Time

Router’s firmware upgrade is essential to upgrade your device’s firmware. An upgrade firmware provides new features and advanced security. There are different types of router, but the upgrading procedure of the router’s firmware is nearly the same. You should always check the user manual available on the manufacturer’s website for specific instructions to upgrade the router according to your device model. Sometimes, router owners have to face threats from malware users or hackers. When any device is created, the design of hardware and its development is the primary phase. The firmware confirms that the hardware components are functioning properly. Generally, the system performance of the device is degraded due to the running of multiple programs through the device at a time. It will also degrade the speed of operation and people think to replace the worn-out hardware component by using new parts. Upgrade of router’s firmware helps to speed up the device performance.

If you want to upgrade the router’s firmware, you will determine the router model. You can check the manufacturer’s website by using the model number of your router to get the available procedure to update the router. Generally, the update of the router is downloaded by using the router’s admin panel. If you can download the updates firmware file, you will download it and save it within your desktop. Otherwise, you will have to use the admin panel to update the router from your computer. You will also have to know your router’s IP address. Sometimes, the routers have an automatic firmware update.

Amped wireless router is one of the most favorite routers for gamers. You can update the amped wireless router’s firmware conveniently. You can visit the support section for an amped wireless website to update the firmware of the amped wireless router. By clicking on the drop-down menu, you will have to select the model number of your router. Then, click on the

download option and select firmware. You can choose the Linksys router or TP-Link router which involves update firmware automatically.

Conclusion

Thank you for making it through to the end of *Computer Networking First-Step: An Introductory Guide to Understanding Wireless and Cloud Technology, Basic Communications Services and Network Security for Beginners* , let's hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

The next step is to take in all this knowledge and start thinking about it deeply. Once you have completely understood all the chapters, only then should you move on to the next book otherwise you can easily get overwhelmed with such an immense pool of knowledge. The meaning of networking is quite simple in the world of computers and that is the linking of separate devices together in order to transmit messages. A particular combination of hardware and software can together form one network. There are some books in the market which are so technical that it becomes almost impossible for a beginner to understand all of it. That is why my main aim in this book was to help you get a hold of the world of computer networking so that you can take the next step with confidence.

In this book, I have tried breaking down the topics of computer networking into their simplest forms and if you have gone through all the chapters and understood them completely, then you are definitely ready for the next book.

Finally, if you found this book useful in any way, a review on Amazon is always appreciated!