DEFINITION OF TELECOMMUNICATION

Telecommunication is the transmission of data (voice, audio, facsimile, image, video etc.) over significant distances by use of electronic technologies like telephones (wired and wireless), microwave communications, fiber optics, satellites, radio and television broadcasting, and the internet. Electronic communications including but not limited to emails, instant messages and phone calls are examples of data communications.

ROLE OF TELECOMMUNICATIONS IN BUSINESS

Enable effective Communication

Communication plays a vital role in the operations of a business. Telecom services provide the platform necessary for data to be exchanged electronically either through wired or wireless means. It enables companies to communicate effectively with customers and deliver high standards of customer service. Telecommunications can help main communication capability for employees working in remote locations or at home. With high-speed internet, mobile apps, VoIP and other means of communication, employees can now exchange information such as documents, analytics, reports, emails, participate in teleconference conversations etc., in real time and reach out to prospective clients regardless of location. From web browsing to cell phone calling to instant messaging, telecommunications have become increasingly integrated into how we work. This has helped businesses to streamline workflow and productivity. Businesses can leverage mobile communication to streamline workflow and productivity. For instance, VoIP (Voice over Internet Protocol) or IP telephony services bring together email, audio and video calls, texting and other telecom solutions. Users can conduct conference calls in multiple cities or countries at the same time, hold virtual meetings and record calls. Moreover, VoIP solutions are more affordable than traditional phone and internet services.

Businesses are able to reach more customers and provide quality services

Telecommunications technology empowers businesses to reach more customers with fewer resources and manpower. It has enabled direct conversations with clients and colleagues hence building business relationships. The absence of proper business relationships, hurdles business growth. Businesses all over the world are getting connected as a result of embracing telecommunications technology thus extending their services. Being able to access the internet 24/7 has

helped many businesses in delivering high-quality customer service. How your business communicates with customers (and potential customers) will reinforce brand loyalty, help your team build better relationships with prospects and clients, and increase retention. Such technologies include; telephony and video conferencing, broadcast and interactive television, instant messaging, email, distributed electronic collaboration, and a range of web- and Internet-based communications and data transmissions. Clients are served regardless of time zone and distance. Through calls and texts, clients can be attended to without any delays. Any assistance with fixing issues is quick, thanks to telecommunications. Employees can now assist clients by being present there virtually, with video calls and tele-immersions. Telecommunication methods of advertising and marketing include telephone marketing calls, social network marketing and online advertising. These types of campaigns expose a business's services and products to a wider audience which helps the business in generating more sales and expanding its customer base.

Reduces costs associated with transactions

Telecommunications have reduced the financial costs, time and efforts associated with business transactions. Promotion of business, broadcasting information and services is just a click away. Your business can be recognized across the boundaries overnight. Shipping operations have been made smoother by automating the basic processes that people once handled. The cost of acquiring information through research and development has also reduced since vast amounts of information are available to employees. Telecommunications allow more employees to access and use information and make decisions upon it. This helps to free up valuable time to allow for more productivity. This technology helps coordinate and dispatch roaming employees to sites as needed, eliminating the need for a central-based office. Businesses spend a substantial amount of money and time in training, traveling, and communicating with customers. Through telecommunication methods such as teleconferencing, costs and limitations are reduced. Teleconferencing involves the use of an Internet connection and a phone line to communicate with people in other locations. Teleconferencing enables businesses to make decisions more quickly, especially if businesses have overseas partnerships, because customers and business partners involved have instant face-to-face communication to exchange information without having to travel far or wait too long for correspondence. Faster decision making means a business can progress and implement its operations on time.

Increase employee productivity and satisfaction

Telecommunications can help a company improve its performance through increased collaboration, flexibility and direct communication. Telecommunication and remote work go hand in hand. Connectivity is a critical element for the modern workplace. It helps companies stay competitive and relevant by making sure they have access to critical information and the ability to foster deeper relationships with their customers. As a manager, you can provide your team with access to VoIP services, file sharing tools, collaboration software, and other services that allow them to work on the go. This may result in higher job satisfaction and productivity. You may also find it easier to attract and retain talent, especially millennials and other groups that prefer newer communication tools. *A May 2020 survey by Harvard Business Review assessed the implications of working from home amid COVID-19. The study was conducted on more than 600 white-collar employees. Half of the respondents said they were able to maintain a 10-hour workday in the first few weeks of the lockdown. Later on, their workdays were still 10 to 20 percent longer than before the lockdown began. Employees also reported fewer task conflicts and less stress while working from home. Their mental focus and self-efficacy increased by about 10 percent. They also said they had a better work-life balance, shorter meetings, and more time for the tasks at hand. Virtual meetings, videoconferencing and other telecom solutions allowed them to do business as usual and eased their transition to remote work. Their job satisfaction improved, too.* Telecommunications give companies the opportunity to introduce more flexible working by allowing employees to work efficiently from home or other, more remote locations.

Improve Collaboration

In today's business world, many organizations employ cross-functional teams for product development, customer relationship management, corporate initiatives, marketing campaigns etc. Telecommunications can improve collaboration between teams and departments. Smartphones, laptops and tablets connected to cellular phone services or Wi-Fi hotspots give employees the ability to connect with each other at any time, virtually anywhere in the world. Mobile phones, videoconferencing, messaging and other telecom services enable employees to brainstorm ideas, share data, and work together on projects from anywhere in the world. Social media and real-time messaging streamline collaboration, allowing companies to create a digital workplace. Employees can work on the same report or sales proposal by using services like Microsoft OneDrive or Google Drive. This allows them to see everyone else's contributions to the document in real time.

Software systems like Basecamp, online chat software and video-conferencing apps (such as zoom, skype) give business people the opportunity to work as if they were side-by-side, regardless of where they are in the world. The introduction of 5G wireless systems will make things like video calls faster, of higher quality and more accessible to everyone. With the above, company teams are able to get more done in less time and make faster decisions.

DATA COMMUNICATIONS

Data communications is the transmission of data signals across distances, between two or more devices using various transmission media that may either be wired or wireless.

FUNDAMENTAL CHARACTERISTICS OF DATA COMMUNICATIONS

Delivery: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user. This characteristic includes the security of the system, that is; the protection of data.

Accuracy: Data must be delivered to the receiver without being altered or damaged. The receiver should receive the exact same data which was sent by the sender. The protocol might require to alter the sent data to protect and optimize the process. However, the protocol should also reverse and restore the data back to its original form before representing it to the receiver. The accuracy must be maintained otherwise data that has been altered in transmission and left uncorrected is unusable.

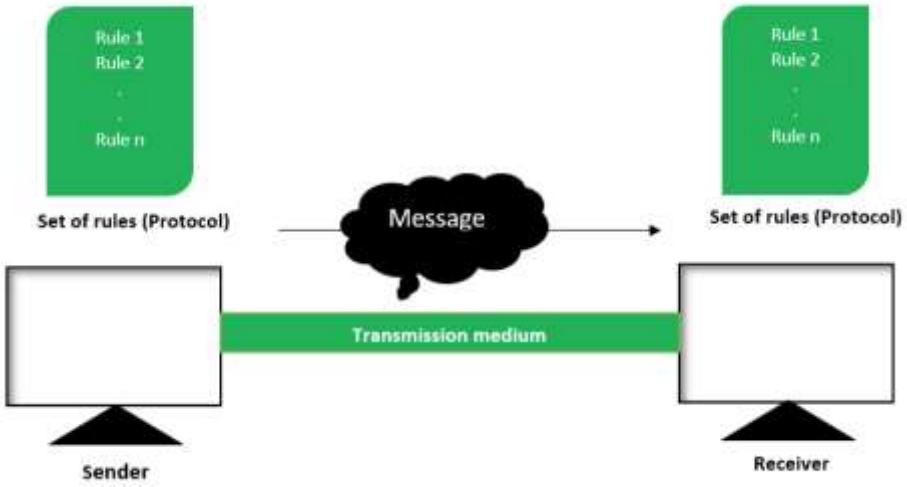
Timeliness: Data must deliver data in a timely manner. Delayed delivery can make the data useless to the receiver. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

Jitter- Jitter refers to the variation in the packet arrival time. Data is sent as packets, that is, a chunk of the whole data is sent in each turn. These packets get re-joined back in the target device to represent the complete data as it is. Each packet is sent with a predefined delay or acceptable amount of delay. If packets are sent without maintaining the predefined delay, then an uneven quality in the data may result. For example, in case of a video, let us assume that video packets

are sent every 3D-ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, the quality of the video when streaming may be affected.

Throughput and Bandwidth: Throughput is an actual measure of how much data is successfully transferred from source to destination, and bandwidth is a theoretical measure of how much data could be transferred from source to destination. Throughput measures speed while bandwidth is only indirectly related to speed. Bandwidth makes your internet connection perceptually faster, but not technically faster.

COMPONENTS OF DATA COMMUNICATIONS



Message: Communication of data means a message or data will be transmitted from one device and will be received in the destination or target device. Hence the first component in a data communication network is data or message that needs to be delivered and received. The data or message can be in any form such as text, audio, video, image or combinations of these forms etc.

Sender: A source must send the message to a destination. This source is the sender (the device that sends the data to the destination or target). It can be a computer, workstation, cell phone, laptop, video camera etc.

Receiver: The destination of a transmitted message is the receiver that will receive the message. The device that receives the message is the receiver. A

receiver can again be a computer, workstation, cell phone, laptop, video camera etc.

Transmission medium: The transmission medium is the physical path for the message to travel to its destination. The sender will send the message from one end of this path and the receiver will receive the message from another end of the path. The transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves etc.

Protocol: A protocol is a set of rules that applies on the full data communication procedure. It represents some kind of agreement between the networked devices to successfully communicate with each other. For example, how to send the data, how the data will be traveling, how to ensure that full data is received, how to handle errors in transmission etc. The communicating devices must follow the same set of rules or protocol so that they understand each other. A typical example of a data communication system is sending an e-mail. The user who wants to send an email acts as a sender, the message is the information contained in the email, the receiver is the who the user wants to send the message to, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send and receive email.

DATA COMMUNICATIONS SYSTEM TASKS

Signal Generation: To transmit the data over the transmission system, communicating device must be able to generate and receive these signals. They system ensures that the resultant signal generated can be acceptable by the transmission mediums.

Interface: Devices must interact or connect with the transmission system to communicate or transfer the data over network.

Data Synchronization: It is the process of establishing consistency among data from a source to destination devices and vice versa and continuous harmonization of the data over time.

Error Detection and Correction: In any communication system transmitted data is prone to error. Either it is because of transmitted signal getting distorted in the

transmission medium leading to misinterpretation of signal or errors introduced by the intermediate devices.

Flow Control: At the time of transmission of data, source computer is generating data faster than receiver device capable to receive it. To handle such problem, there must be some kind of flow control mechanism used to ensure that the source does not overwhelm the destination by sending data faster than it can be processed by the receiver.

Addressing and Routing: When more than two devices share a transmission facility, a source system must indicate the identity or address of the destination and can choose a specific route through the network. This will ensure that the data is sent to the appropriate destinations.

Recovery: The system ensures that interrupted transactions resume activity at the point of interruption or to condition prior to the beginning of the exchange.

Security: Security is a very important issue in a data communication system. The sender needs to be assured that; only the intended receiver receives the data, data is delivered unaltered.

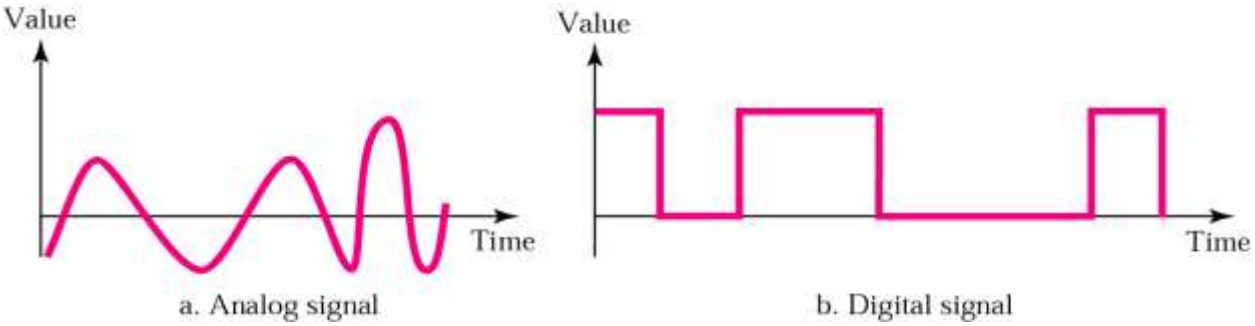
Network management: Network management capabilities are needed to configure the system, monitor its status, react to failures and overloads and plan intelligently for future growth.

Exchange management: The system ensures that if the data needs to be exchanged in both directions over a period of time, both parties must cooperate as follow; whether both devices must transmit simultaneously or take turns, amount of data to be sent at one time, format of the data, what to do when an error arises.

Transmission system utilization: The system must ensure efficient use of transmission facilities that are shared among a number of communicating devices. For example; techniques like multiplexing to allow multiple users to share total capacity of a transmission medium, congestion control to ensure that the transmission system is not overwhelmed by traffic.

DATA COMMUNICATION SIGNALS

A signal is an electromagnetic current or light wave that is used for carrying data from one device or network to another through a communication medium. It is the key component behind virtually all: Communication, Computing, Networking, Electronic devices. A signal can be either *analog* or *digital*



a. Analog signal b. Digital signal

ANALOG SIGNALS

These are continuous time-varying signals in form of waves. Temperature sensors, FM radio signals, photocells, light sensor, resistive touch screen are examples of analog signals.

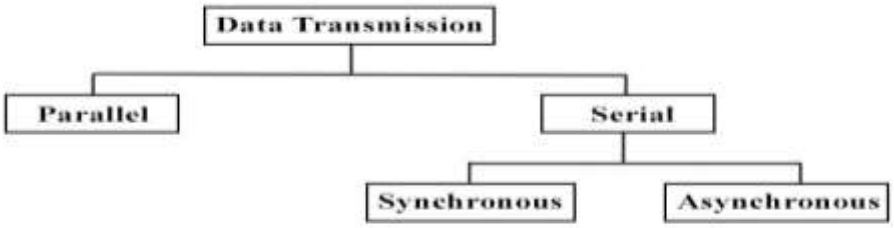
DIGITAL SIGNALS

A digital signal is a signal that is used to represent data as a sequence of separate values at any point in time. It can only take on one of a fixed number of values. For example, HDTV uses digital signals to broadcast high quality video signals.

DATA TRANSMISSION METHODS

Data transmission methods are ways in which digital or analog data is sent and received between two or more electronic devices over a communication medium.

TYPES OF DATA TRANSMISSION



PARALLEL DATA TRANSMISSION

This is a method of transmitting multiple binary digits simultaneously using multiple lines (8, 16, 32, 64). Parallel data transmission enables data to be sent much faster. It can be used when a large amount of data is being sent, data being sent is time sensitive or when the data needs to be sent quickly. An example of parallel mode transmission is a connection established between a computer and a printer. Most printers are within 6 meters (about 20 feet) from the transmitting computer, and the slight cost for extra wires is offset by the added speed gained through parallel transmission of data.

SERIAL DATA TRANSMISSION

Serial data transmission is the process of sending data one bit at a time, sequentially, over a communication channel or computer bus. It is a very reliable method; as new signals don't be sent until the previous ones are received. Pulse of a 1 byte is transmitted in a block of 8 bits from sender to destination. This method is suitable when there's long distance data transfer and the amount of data being sent is relatively small. An example of serial data transmission is the transfer of bits from the computer to the modem for transmission over the phone.

Major categories of serial data transmission are;

- Asynchronous serial transmission
- Synchronous serial transmission

ASYNCHRONOUS SERIAL TRANSMISSION

Asynchronous Transmission is a communication interface in which the data is transmitted as a continuous stream of bytes separated by start and stop bits. The signals used are not synchronized to each other using a common clock signal. Instead, start and stop bits are used to indicate the beginning and end of a data message. The start and stop bits ensure that the data is transmitted correctly.

Without the use of these bits, the sending and receiving systems will not know where one character ends and another begins. Examples where its applicable include email, forums etc.

SYNCHRONOUS SERIAL TRANSMISSION

Synchronous data transmission is a data transfer method in which a continuous stream of data signals is accompanied by timing signals (generated by an electronic clock) to ensure that the transmitter and the receiver are in step (synchronized) with one another. The data is sent in blocks (called frames or packets) spaced by fixed time intervals. This method is used when large amounts of data must be transferred very quickly from one location to the other. The speed of the synchronous connection is attained by transferring data in large blocks instead of individual characters. Examples where its applicable include chat rooms, telephone conversations, video conferencing, VOIP.

DATA TRANSMISSION MODES

Data transmission modes also known as communication modes; define the direction of signal flow between two linked communication devices in a computer network. It is important to control the direction of signal flow as it leads to successful communication over the network and minimizes errors. Data transmission modes are categorized into;

- Simplex mode
- Duplex mode

SIMPLEX MODE

In this mode, is transmitted in one direction only i.e. from the sender to the receiver. Example; transfer of data from computer to printer, radio and television broadcasts, keyboard, mouse etc.

DUPLEX MODE

In this mode, two or more connected devices can communicate with one another in both directions. This mode is further categorized into;

- Half Duplex
- Full Duplex

HALF DUPLEX MODE

In this mode, data is transmitted in both directions but not simultaneously i.e. not at the same time. The sender and receiver can both send and receive information, but only one is allowed to send at any given time. That means, when one device is sending, the other can only receive, and vice versa. Example; communication using walkie-talkies.

FULL DUPLEX MODE

In this mode, data is transmitted in both directions simultaneously. The sender and receiver can both transmit and receive at the same time. Example; Broadband phone connection.

DATA COMMUNICATION CHANNELS

The physical path by which data signals are transmitted from one computer to another. Communication channels are categorized into;

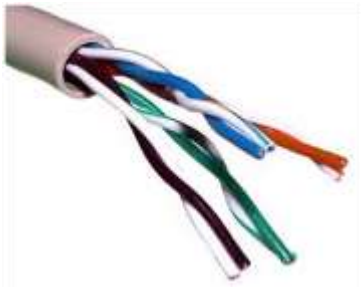
- Guided (Wired) channels
- Unguided (Wireless) channels

GUIDED (WIRED) CHANNELS

It is also referred to as wired or bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. There are three major types of guided media;

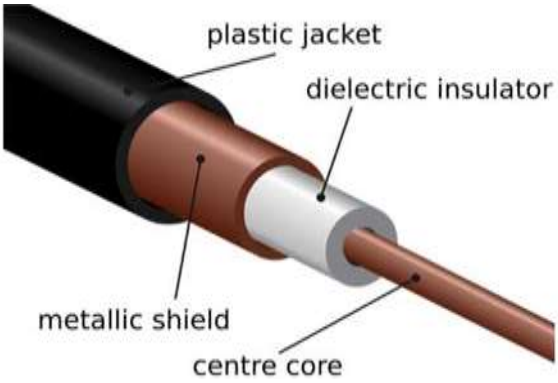
- Twisted-Pair cable
- Coaxial cable
- Fibre-Optic cable

Twisted-Pair cable; It consists of 2 separately insulated conductor wires intertwined together. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types: *Unshielded twisted pair (UTP)*, which has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

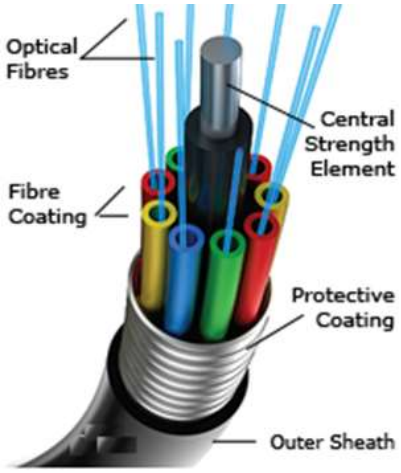


Shielded twisted pair (STP), which consists of a special jacket to block external interference. It is used in fast data rate Ethernet and in voice and data channels of telephone lines.

Coaxial cable; It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode (dedicated cable bandwidth) and broadband mode (cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use coaxial cables.



Fibre-Optic cable; It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by less dense glass or plastic covering called cladding. Digital signals are sent as light pulses which are translated back into electronic signals. It is used for the transmission of large volumes of data.



UNGUIDED (WIRELESS) CHANNELS

It is also referred to as wireless or unbounded transmission media. These transmit electromagnetic waves without using a physical medium hence being referred to as wireless transmission. Signals are normally broadcast through space and they are available to anyone who has a device capable of receiving them. There are 3 types of signals transmitted through unguided media;

- Radiowaves
- Microwaves
- Infrared

Radiowaves; These are low frequency signals and can travel a long distance. They are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range: 3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission. They are further categorized as (i) Terrestrial and (ii) Satellite.

Microwaves; It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. They have a higher frequency than radio waves. Frequency Range:1GHz – 300GHz. They are majorly used for telephone communication, mobile phones, television distribution etc.

Infrared; Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, VCRs etc.

PROTOCOLS AND STANDARDS

Network *Protocols* are a set of rules governing exchange of information in an easy, reliable and secure way. Rules of network protocols include guidelines that regulate the following characteristics of a network; access method, allowed physical topologies, types of cabling and speed of data transfer.

Network *Standards* define the rules for data communications that are needed for interoperability of networking technologies and processes. The primary reason for standards is to ensure that hardware and software produced by different vendors can work together. The use of standards makes it much easier to develop software and hardware that link different networks.

TYPES OF PROTOCOLS

Many different types of network protocols and standards are required to ensure that an electronic device (no matter which operating system, network card, or application it's using) can communicate with another electronic device located near or far away. The protocols listed below are a few of the more well-known;

File Transfer Protocol (FTP); Allows users to transfer files form one electronic device to another. Types of files may include program files, multimedia files, text files and documents etc.

Simple Mail Transfer Protocol; Is an internet standard for electronic mail (email) transmission. It is designed to send and distribute outgoing E-mail.

Hyper Text Transfer Protocol (HTTP); Is an application for distributed, collaborative, and hypermedia information systems. It is the foundation of data communication for the World Wide Web. HTTP is designed for transferring hypertext among two or more systems. HTML tags are used for creating links. These Links may be in any form like text or images.

Hyper Text Transfer Protocol Secure (HTTPS); Is an adaptation of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network, and is widely used on the internet. The secure version is encrypted, meaning that all the data will be encrypted as it is sent from the client to the server. It can be defined as a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. Https thwart hackers from interpretation or modification of data throughout the transfer of packets.

Transmission Control Protocol; TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination. It is one of the main protocols of the internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating by an IP network. Major Internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP.

Internet Protocol (IP); IP is designed explicitly as an addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.

TYPES OF STANDARDS

Standards are of two types;

- **De facto −** These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP had started as a de facto standard.
- **De jure −** These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

Some of the noted standards organizations are;

- International Standards Organization (ISO)
- International Telecommunication Union (ITU)
- Institute of Electronics and Electrical Engineers (IEEE)
- American National Standards Institute (ANSI)
- Internet Research Task Force (IETF)
- Electronic Industries Association (EIA)

NETWORK SECURITY BEST PRACTICES

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

The steps below will guide on how to secure a business network.

1. **Perform a Network Audit;** A thorough network audit is recommended in order to assess the networks weaknesses that need to be combated in order to tighten and improve network security. The goal of the audit is to identify and assess;

- Possible security vulnerabilities
- Unused or unnecessary applications running in the background
- Open ports
- Overall strength of your firewall
- Anti-virus/anti-malware software
- The overall health of servers, software, and applications
- Backups

After the audit, a detailed report is made and reviewed with the business' IT expert with an intention to make improvements.

2. **Disable file sharing;** File sharing might seem like a great and convenient collaborative method, but it can also put your business' network security at risk. However, file sharing means that any user that is accessing the same public network can access your files. Therefore, it's a good idea to disable file sharing on all employee devices, except on your independent, private servers.

3. **Update your Anti-Virus/Anti-Malware Software;** In many cases, businesses will purchase desktop computers for their offices or laptops with the latest version of anti-virus and anti-malware software. However, over time, that software becomes outdated. Most cases, users never update their software again. By taking the time to ensure that your anti-virus and anti-malware is up to date, you are also ensuring that your devices are running software with the most recent bug fixes and security updates.

4. **Set up a Firewall;** If you don't currently have a firewall, then make this a priority. Not only should you install firewalls on your devices, but also set up a web application firewall (WAF). This is especially important if you are an eCommerce business and sell products online and store customers' confidential information. Installing a WAF will help protect all your stored data.

5. **Invest in a VPN;** A Virtual Private Network (VPN) encrypts your network to ensure online privacy for all your users. A VPN blocks your activities, data, browsing history, communications and other personal information from hackers. It also protects your files and information while using a public Wi-Fi network. If your employees frequently travel or work remotely, then a VPN is a good investment for your business.

6. **Secure your Router;** it is essential to secure you router. Believe it or not, a security breach or other security event can occur by simply hitting the reset button on your network router. Therefore, if your router is in an open or common location in your office, consider moving it to a more secure location, such as in a locked room or closet. You can also take security one step further and investing in video surveillance equipment and installing it in your server or network router room.

7. **Update router information periodically;** In addition to moving your router to a more secure location, update the login information on a semi-regular basis. Most routers are initially set up with a default username and password, such as "admin". It is not wise to leave your username and password as "admin". There is actually a list of usernames and passwords that are easiest to hack, and "admin" tops the list.Therefore, set a complex password combination that contains at least 8 characters, a number, and a special symbol. Be sure to also schedule a reminder to change the router information once a month, or once a quarter, whatever you think might be appropriate.

8. **Update the Name of your network;** Again, similar to updating your network router's username and password on a regular basis, you might also want to update your network name on a regular basis—and keep your router's make and model confidential. For example, many default network names are the name of your provider. This tells a potential hacker that you don't follow best network security practices, which makes your business a prime target.

9. **Use a private IP address;** In order to prevent unauthorized users or devices to access your network, consider assigning private IP addresses to specific devices on your network. Therefore, when you or your IT administrator check your router logs, you will see any and all attempts of unauthorized

users or devices connecting to your network or any other suspicious activity.

10. **Establish a Network security maintenance system;** Depending on the size of your business, you may have an in-house IT team, or you might be a DIY solopreneur. Regardless of size, network security is still important. Therefore, take the time to establish a network security maintenance system that involves processes such as:

    - Performing regular backups
    - Running activity reports
    - Keeping software up to date
    - Setting up a schedule for changing your network name and passwords

    Depending on the size and complexity of your business, your network security maintenance system may involve additional or fewer steps. The overarching goal here is to be proactive and establish a process for monitoring and maintaining network security. Once you have established a network security maintenance system with the necessary steps that make sense to your business, document it and circulate it to your team.

11. **Create a Network Security-Centered Culture;** In addition to taking specific network security measures and adopting a network security protocol, the other steps involve educating and training your staff on the importance of network security and how they can do their part. By creating a culture devoted to network security, you can ensure that your team will better understand the implications and risks of lack of network security, and what they can do to help.

12. **Train employees in network security practices;** Even though you have put thought, effort, and time into documenting your network security practices and process, unfortunately, most team members and employees will skim through your documentation. In an effort to build a network security-centered culture, it is also important to follow up with a network security training session for your employees. For example, in addition to educating team members on good versus poor network security practices, you can also engage them with interactive activities, such as having them identify phishing emails, quality versus unsecured password combinations, and what to do if they notice any suspicious activity on any of their devices.