This module was prepared by the Wolaita Sodo University School of informatics

Department of information systems

Module on Computer networking

and

Information security

Developed By:

Hailye Teklesilassie (MSc.)

Admasu Desalegn (MSc.)

Mukrem Mubarek (BSc.)

Henok Alemneh (BSc.)

Compiled & Edited By: Hailye Teklesilassie (MSc)

February 2023

Module Preface

This resource module is designed and developed in support of the Computer networking and information security It provides learning resources and teaching ideas. Dear students, in chapter one you have been studied about the network, Over view of network, elements and characteristics of network, network architectures, computer network & human network.

In chapter two, Data communication in chapter three, network types in chapter four, protocols, in chapter five, OSI reference model, in chapter six, Switching & Multiplexing, in chapter seven, Introduction to IP Addressing and Subnetting, in chapter eight, Data Security and Integrity, in chapter nine, system and network administration, in chapter ten, information Systems security.

Table of Contents

Chapter 1

Introduction

1. What is network

Computer networking as we know it today may be said to have gotten its start with the Arpanet development in the late 1960s and early 1970s. Prior to that time there were computer vendor "networks" designed primarily to connect terminals and remote job entry stations to a mainframe?

Year	Event
1961	The idea of ARPANET, one of the earliest computer networks, was proposed by Leonard Klein rock in 1961, in his paper titled "Information Flow in Large Communication Nets."
1965	The term "packet" was coined by Donald Davies in 1965, to describe data sent between Computers over a network.
1969	ARPANET was one of the first computer networks to use packet switching. Development of ARPANET started in 1966, and the first two nodes, UCLA and SRI (Stanford Research Institute), were connected, officially starting ARPANET in 1969.
1969	The first RFC surfaced in April 1969, as a document to define and provide information About computer communications, network protocols, and procedures.
1969	The first network switch and IMP (Interface Message Processor) was sent to UCLA on August 29, 1969. It was used to send the first data transmission on ARPANET.
1969	The Internet was officially born, with the first data transmission sent between UCLA and SRI on October 29, 1969, at 10:30 p.m.
1970	Steve Crocker and a team at UCLA released NCP (NetWare Core Protocol) in 1970. NCP is a file sharing protocol for use with NetWare.
1971	Ray Tomlinson sent the first e-mail in 1971.
1971	ALOHA net, a UHF wireless packet network, is used in Hawaii to connect the islands Together. Although it is not Wi-Fi, it helps lay the foundation for Wi-Fi.

1973	Ethernet is developed by Robert Metcalfe in 1973 while working at Xerox PARC.
1973	The first international network connection, called SATNET, is deployed in 1973 by ARPA.
1973	An experimental VoIP call was made in 1973, officially introducing VoIP technology And capabilities. However, the first software allowing users to make VoIP calls was not Available until 1995.
1974	The first routers were used at Xerox in 1974. However, these first routers were not Considered true IP routers.
1976	Ginny Strazisar developed the first true IP router, originally called a gateway, in 1976.
1978	Bob Kahn invented the TCP/IP protocol for networks and developed it, with help from Vint Cerf, in 1978.
1981	Internet Protocol version 4, or IPv4, was officially defined in RFC 791 in 1981. IPv4 was the first major version of the Internet protocol.
1981	BITNET was created in 1981 as a network between IBM mainframe systems in the United States.
1981	CSNET (Computer Science Network) was developed by the U.S. National Science Foundation in 1981.
1983	ARPANET finished the transition to using TCP/IP in 1983.
1983	Paul Mockapetris and Jon Postel implemented the first DNS in 1983.
1986	The NSFNET (National Science Foundation Network) came online in 1986. It was a backbone for ARPANET, before eventually replacing ARPANET in the early 1990s.
1986	BITNET II was created in 1986 to address bandwidth issues with the original BITNET.
1988	The first T1 backbone was added to ARPANET in 1988.
1988	WaveLAN network technology, the official precursor to Wi-Fi, was introduced to The market by AT&T, Lucent, and NCR in 1988.
1988	Details about network firewall technology was first published in 1988. The published paper discussed the first firewall, called a packet filter firewall, that was developed by Digital Equipment Corporation the same year.
1990	Kalpana, a U.S. network hardware company, developed and introduced the first network

	Switch in 1990.
1996	IPv6 was introduced in 1996 as an improvement over IPv4, including a wider range of IP Addresses, improved routing, and embedded encryption.
1997	The first version of the 802.11 standard for Wi-Fi is introduced in June 1997, providing transmission Speeds up to 2 Mbps.
1999	The 802.11a standard for Wi-Fi was made official in 1999, designed to use the 5 GHz band and provide transmission speeds up to 25 Mbps.
1999	802.11b devices were available to the public starting mid-1999, providing transmission speeds up to 11 Mbps.
1999	The WEP encryption protocol for Wi-Fi is introduced in September 1999, for use with 802.11b.
2003	802.11g devices were available to the public starting in January 2003, providing transmission speeds Up to 20 Mbps.
2003	The WPA encryption protocol for Wi-Fi is introduced in 2003, for use with 802.11g.
2003	The WPA2 encryption protocol is introduced in 2004, as an improvement over and replacement For WPA. All Wi-Fi devices are required to be WPA2 certified by 2006.
2009	The 802.11n standard for Wi-Fi was made official in 2009. It provides higher transfer speeds Over 802.11a and 802.11g, and it can operate on the 2.4 GHz and 5 GHz bandwidths.
2018	The Wi-Fi Alliance introduced WPA3 encryption for Wi-Fi in January 2018, which includes Security enhancements over WPA2.

1.1 Over view of network

A computer network is comprised of connectivity devices and components. ... To share data and resources between two or more computers is known as networking. There are different types of a computer network such as LAN, MAN, WAN and wireless network.

How did network start?

ARPANET began the networking long ago. In 1957, when SPUTNIK Satellite was launched by Russia. An agency named ADVANCED RESEARCH PROJECT AGENCY (ARPA) was started by American, and its first satellite was launched within 18 months after establishment. Then they used ARPANET to share the information on another computer.

What types of network?

A computer network is mainly of four types:

- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

Which is the first network

The Arpanet

Switched on in late October 1969, the **Arpanet** is the first large-scale, general-purpose computer network to connect different kinds of computers together.

What are the basic concept of networking?

The foundations of **networking**: switches, routers, and wireless access points. Switches, routers, and wireless access points are the **essential networking basics**. Through them, devices connected to your **network** can communicate with one another and with other **networks**, like the Internet.

1.2 Networks in Our Daily Lives

Among all of the essentials for human existence, the need to interact with others ranks just below

Our need to sustain life. Communication is almost as important to us as our reliance on air, water,

Food, and shelter.

The methods that we use to communicate are constantly changing and evolving. Whereas we were

once limited to face-to-face interactions, breakthroughs in technology have significantly extended

The reach of our communications. From cave paintings to the printing press to radio and television,

each new development has improved and enhanced our ability to connect and communicate with Others.

The creation and interconnection of robust data networks has had a profound effect on communication, and has become the new platform on which modern communications occur.

Networks connect people and promote unregulated communication.

Networks are the platforms on which to run businesses, to address emergencies, to inform individuals, and to support education, science, and government.

The Internet is the largest network in existence. In fact, the term Internet, means a network of networks. It is actually a collection of interconnected private and public networks. It is incredible how quickly the Internet has become an integral part of our daily routines.

1.3 Network as a plat form

A **network**-based **platform** is a piece of technology or software that connects users with other members of a community to create mutually beneficial opportunities. ... The usefulness of the **platform** snowballs as more and more members join the **network**. This phenomenon is known as the **Network** Effect

1.4 What are the elements of a network?

Networks are comprised of four basic **elements**: hardware, software, protocols and the connection medium. All data **networks** are comprised of these **elements**, and cannot function without them.

What are the 3 basic elements of a network?

Basic elements of a **computer network** include **hardware**, software, and **protocols**. The interrelationship of these basic elements constitutes the infrastructure of the network.

1.5 What are the characteristics of network architectures?

As networks evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations:

- **Fault tolerance**. Is the process of working of a system in a proper way in spite of the occurrence of the failures in the system? ... Hence, systems are designed in such a way that in case of error availability and failure, system does the work properly and given correct result.
- **Scalability**. Is the measure of a system's ability to increase or decrease in performance and cost in response to changes in application and system processing demands? ... Enterprises that are growing rapidly **should** pay special attention to **scalability** when evaluating hardware and software.
- **QoS**. **Quality of service** (**QoS**) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on a network. **QoS** controls and manages network resources by setting priorities for specific types of data on the network.
- **Security**. The quality or state of being **secure**: such as.
- A: freedom from danger: safety.
- B: freedom from fear or anxiety.
- C: freedom from the prospect of being laid off job **security**.

1.6 Computer Networks versus Human Network

Both of them have memory, both of them use electrical signals, both of them **can** retrieve and transmit data, both of them have partitions and both of them connect data in order to reach to conclusions which are logical and working

The difference between Human network and Computer network is explained in the following points:

HUMAN NETWORK:

1. They possess **Biological neurons or nerve cells**.
2. The Neuron size is approximately **10 m to 6 m**.
3. They consume the energy of about **6-10 joule per operation per second**.
4. Moreover, they possess **high Learning capability**.

COMPUTER NETWORK:

1. Network is made up of **Silicon transistors**.
2. The size of a Single transistor is about **10 m to 9 m**.
3. It consumes Energy between the range of **10-16 joules per operation per second**.
4. Possesses **high Programming Capability**.

Chapter 2:

2. Data Communications

2.1. What is communication?

The root of the word "communication" in Latin is *communicare,* which means to share, or to make common (Weakley, 1967). Communication is defined as the process of understanding and sharing meaning (Pearson & Nelson, 2000).

At the center of our study of communication is the relationship that involves interaction between participants. This definition serves us well with its emphasis on the process, which we'll examine in depth across this text, of coming to understand and share another's point of view effectively.

The first key word in this definition is process. A process is a dynamic activity that is hard to describe because it changes (Pearson & Nelson, 2000). Imagine you are alone in your kitchen thinking. Someone you know (say, your mother) enters the kitchen and you talk briefly. What has changed? Now, imagine that your mother is joined by someone else, someone you haven't met before—and this stranger listen intently as you speak, almost as if you were giving a speech. What has changed? Your perspective might change, and you might watch your words more closely. The feedback or response from your mother and the stranger (who are, in essence, your audience) may cause you to reevaluate what you are saying. When we interact, all these factors—and many more—influence the process of communication.

The second key word is understanding: "To understand is to perceive, to interpret, and to relate our perception and interpretation to what we already know." (McLean, 2003) If a friend tells you a story about falling off a bike, what image comes to mind? Now your friend points out the window and you see a motorcycle lying on the ground. Understanding the words and the concepts or objects they refer to is an important part of the communication process.

Next comes the word sharing. Sharing means doing something together with one or more people. You may share a joint activity, as when you share in compiling a report; or you may benefit jointly from a resource, as when you and several coworkers share a pizza. In communication, sharing occurs when you convey thoughts, feelings, ideas, or insights to others. You can also

share with yourself (a process called intrapersonal communication) when you bring ideas to consciousness, ponder how you feel about something, or figure out the solution to a problem and have a classic “Aha!” moment when something becomes clear.

Finally, meaning is what we share through communication. The word “bike” represents both a bicycle and a short name for a motorcycle. By looking at the context the word is used in and by asking questions, we can discover the shared meaning of the word and understand the message.

Eight Essential Components of Communication

In order to better understand the communication process, we can break it down into a series of eight essential components:

- Source
- Message
- Channel
- Receiver
- Feedback
- Environment
- Context
- Interference

Each of these eight components serves an integral function in the overall process. Let’s explore them one by one.

✓ **Source**

The source imagines, creates, and sends the message. In a public speaking situation, the source is the person giving the speech. He or she conveys the message by sharing new information with the audience. The speaker also conveys a message through his or her tone of voice, body language, and choice of clothing. The speaker begins by first determining the message—what to say and how to say it. The second step involves encoding the message by choosing just the right order or the perfect words to convey the intended meaning. The third step is to present or send the information to the receiver or audience. Finally, by watching for the audience’s reaction, the source perceives how well they received the message and responds with clarification or supporting information.

- ✓ **Message**

"The message is the stimulus or meaning produced by the source for the receiver or audience." (McLean, 2005) When you plan to give a speech or write a report, your message may seem to be only the words you choose that will convey your meaning. But that is just the beginning. The words are brought together with grammar and organization. You may choose to save your most important point for last. The message also consists of the way you say it—in a speech, with your tone of voice, your body language, and your appearance—and in a report, with your writing style, punctuation, and the headings and formatting you choose. In addition, part of the message may be the environment or context you present it in and the noise that might make your message hard to hear or see.

Imagine, for example, that you are addressing a large audience of sales reps and are aware there is a World Series game tonight. Your audience might have a hard time settling down, but you may choose to open with, "I understand there is an important game tonight." In this way, by expressing verbally something that most people in your audience are aware of and interested in, you might grasp and focus their attention.

- ✓ **Channel**

"The channel is the way in which a message or messages travel between source and receiver." (McLean, 2005) For example, think of your television. How many channels do you have on your television? Each channel takes up some space, even in a digital world, in the cable or in the signal that brings the message of each channel to your home. Television combines an audio signal you hear with a visual signal you see. Together they convey the message to the receiver or audience. Turn off the volume on your television. Can you still understand what is happening? Many times you can, because the body language conveys part of the message of the show. Now turn up the volume but turn around so that you cannot see the television. You can still hear the dialogue and follow the story line.

Similarly, when you speak or write, you are using a channel to convey your message. Spoken channels include face-to-face conversations, speeches, telephone conversations and voice mail messages, radio, public address systems, and voice over Internet protocol (VoIP). Written

channels include letters, memorandums, purchase orders, invoices, newspaper and magazine articles, blogs, e-mail, text messages, tweets, and so forth.

- ✓ **Receiver**

"The receiver receives the message from the source, analyzing and interpreting the message in ways both intended and unintended by the source." (McLean, 2005) To better understand this component, think of a receiver on a football team. The quarterback throws the football (message) to a receiver, who must see and interpret where to catch the ball. The quarterback may intend for the receiver to "catch" his message in one way, but the receiver may see things differently and miss the football (the intended meaning) altogether.

As a receiver you listen, see, touch, smell, and/or taste to receive a message. Your audience "sizes you up," much as you might check them out long before you take the stage or open your mouth. The nonverbal responses of your listeners can serve as clues on how to adjust your opening. By imagining yourself in their place, you anticipate what you would look for if you were them. Just as a quarterback plans where the receiver will be in order to place the ball correctly, you too can recognize the interaction between source and receiver in a business communication context. All of this happens at the same time, illustrating why and how communication is always changing.

- ✓ **Feedback**

When you respond to the source, intentionally or unintentionally, you are giving feedback. Feedback is composed of messages the receiver sends back to the source. Verbal or nonverbal, all these feedback signals allow the source to see how well, how accurately (or how poorly and inaccurately) the message was received. Feedback also provides an opportunity for the receiver or audience to ask for clarification, to agree or disagree, or to indicate that the source could make the message more interesting. As the amount of feedback increases, the accuracy of communication also increases (Leavitt & Mueller, 1951).

For example, suppose you are a sales manager participating in a conference call with four sales reps. As the source, you want to tell the reps to take advantage of the fact that it is World Series season to close sales on baseball-related sports gear. You state your message, but you hear no replies from your listeners. You might assume that this means they understood and agreed with

you, but later in the month you might be disappointed to find that very few sales were made. If you followed up your message with a request for feedback ("Does this make sense? Do any of you have any questions?") you might have an opportunity to clarify your message, and to find out whether any of the sales reps believed your suggestion would not work with their customers.

- ✓ **Environment**

"The environment is the atmosphere, physical and psychological, where you send and receive messages." (McLean, 2005) The environment can include the tables, chairs, lighting, and sound equipment that are in the room. The room itself is an example of the environment. The environment can also include factors like formal dress, that may indicate whether a discussion is open and caring or more professional and formal. People may be more likely to have an intimate conversation when they are physically close to each other, and less likely when they can only see each other from across the room. In that case, they may text each other, itself an intimate form of communication. The choice to text is influenced by the environment. As a speaker, your environment will impact and play a role in your speech. It's always a good idea to go check out where you'll be speaking before the day of the actual presentation.

- ✓ **Context**

"The context of the communication interaction involves the setting, scene, and expectations of the individuals involved." (McLean, 2005) A professional communication context may involve business suits (environmental cues) that directly or indirectly influence expectations of language and behavior among the participants.

A presentation or discussion does not take place as an isolated event. When you came to class, you came from somewhere. So did the person seated next to you, as did the instructor. The degree to which the environment is formal or informal depends on the contextual expectations for communication held by the participants. The person sitting next to you may be used to informal communication with instructors, but this particular instructor may be used to verbal and nonverbal displays of respect in the academic environment. You may be used to formal interactions with instructors as well, and find your classmate's question of "Hey Teacher, do we have homework today?" as rude and inconsiderate when they see it as normal. The nonverbal

response from the instructor will certainly give you a clue about how they perceive the interaction, both the word choices and how they were said.

Context is all about what people expect from each other, and we often create those expectations out of environmental cues. Traditional gatherings like weddings or quinceañeras are often formal events. There is a time for quiet social greetings, a time for silence as the bride walks down the aisle, or the father may have the first dance with his daughter as she is transformed from a girl to womanhood in the eyes of her community. In either celebration there may come a time for rambunctious celebration and dancing. You may be called upon to give a toast, and the wedding or quinceañera context will influence your presentation, timing, and effectiveness.

✓ **Interference**

Interference, also called noise, can come from any source. “Interference is anything that blocks or changes the source’s intended meaning of the message.”(McLean, 2005) For example, if you drove a car to work or school, chances are you were surrounded by noise. Car horns, billboards, or perhaps the radio in your car interrupted your thoughts, or your conversation with a passenger.

2.2. The platform for communication

What is a Communication Platform? A **communication platform**

Is a cloud-based **platform** that allows organizations to add **communication** services like **messaging**, voice and video to their business applications and processes?

Types of Communication Software

- Instant Messaging Apps. Instant messaging is a preferred form of **communication** for consumers and companies. ...
- Collaboration Tools. ...
- Video Conferencing. ...
- Customer Relationship Management. ...
- Tech Support. ...
- Brosix. ...
- Dropbox.
- Google Drive.

The **main platform to communicate** is social media. In past, they using letters and telephone while in the present they using a social media, emails, etc.

2.2.1. Communicating the Message

2.3. Data transmission

What is data transmission?

Data transmission refers to the process of transferring data between two or more digital devices. Data is transmitted from one device to another in analog or digital format. Basically, data transmission enables devices or components within devices to speak to each other.

How does data transmission work between digital devices?

Data is transferred in the form of bits between two or more digital devices. There are two methods used to transmit data between digital devices: serial transmission and parallel transmission. Serial data transmission sends data bits one after another over a single channel. Parallel data transmission sends multiple data bits at the same time over multiple channels.

What is serial transmission?

When data is sent or received using serial data transmission, the data bits are organized in a specific order, since they can only be sent one after another. The order of the data bits is important as it dictates how the transmission is organized when it is received. It is viewed as a reliable data transmission method because a

Serial transmission has two classifications: asynchronous and synchronous.

Asynchronous Serial Transmission

Data bits can be sent at any point in time. Stop bits and start bits are used between data bytes to synchronize the transmitter and receiver and to ensure that the data is transmitted correctly. The time between sending and receiving data bits is not constant, so gaps are used to provide time between transmissions.

The advantage of using the asynchronous method is that no synchronization is required between the transmitter and receiver devices. It is also a more cost effective method. A disadvantage is that data transmission can be slower, but this is not always the case.

Synchronous Serial Transmission

Data bits are transmitted as a continuous stream in time with a master clock. The data transmitter and receiver both operate using a synchronized clock frequency; therefore, start bits, stop bits, and gaps are not used. This means that data moves faster and timing errors are less frequent because the transmitter and receiver time is synced. However, data accuracy is highly dependent on timing being synced correctly between devices. In comparison with asynchronous serial transmission, this method is usually more expensive.

When is serial transmission used to send data?

Serial transmission is normally used for long-distance data transfer. It is also used in cases where the amount of data being sent is relatively small. It ensures that data integrity is maintained as it transmits the data bits in a specific order, one after another. In this way, data bits are received in-sync with one another.

What is parallel transmission?

When data is sent using parallel data transmission, multiple data bits are transmitted over multiple channels at the same time. This means that data can be sent much faster than using serial transmission methods.

Advantages and Disadvantages of Using Parallel Data Transmission

The main advantages of parallel transmission over serial transmission are:

- it is easier to program;
- and data is sent faster.

Although parallel transmission can transfer data faster, it requires more transmission channels than serial transmission. This means that data bits can be out of sync, depending on transfer distance and how fast each bit loads. A simple of example of where this can be seen is with a voice over IP (VOIP) call when distortion or interference is noticeable. It can also be seen when there is skipping or interference on a video stream.

2.3.1. Concepts and Terminology

• **Transmission terminology** – Transmission from transmitter to receiver goes over some transmission medium using electromagnetic waves Guided media. Waves are guided along a physical path; twisted pair, optical fiber, coaxial cable unguided media. Waves are not guided; air waves, radio direct link. Signal goes from transmitter to receiver with no intermediate devices, other than amplifiers and repeaters Point-to-point link. Guided media with direct link between two devices, with those two devices being the only ones sharing the medium Multipoint guided configuration.

More than two devices can share the same medium – Simplex, half duplex, and full duplex transmission

• Frequency, spectrum, and bandwidth – Signal is generated by a transmitter and transmitted over a medium – Signal is a function of time or frequency (components of different frequency) – Time-domain concepts Continuous signal. Signal intensity varies in a smooth fashion over time; no breaks or discontinuities in signal Discrete signal. Signal intensity can take one of two prespecified values for any amount of time Periodic signal. Same signal pattern repeats over time; signal is said to be periodic if $s(t + T) = s(t) - \infty < t < \infty$ T is the period of the signal; sine wave Aperiodic signal. Signal that is not periodic Peak amplitude.

Maximum signal intensity over time; typically measured in volts Frequency f. Rate at which signal repeats; measured in cycles per second or Hz Period T. Amount of times required for one repetition of signal $T = 1$ f Phase. Measure of relative position in time within a single period of a signal ∗ For a periodic signal f(t), phase is fractional part t p of the period P through which t has advanced relative to an arbitrary origin

General sine wave can be written as $s(t) = A \sin(2\pi f t + \varphi)$ Wavelength λ.

Distance occupied by a single cycle ∗ Consider a signal traveling at velocity v ∗ Wavelength is related to period as

2.3.2. Analog and Digital Data Transmission

• Analog vs digital (continuous vs discrete)

• Data – Entities that convey information

• Signaling – Physical propagation of signal along suitable medium

• Transmission – Communication of data by propagation and processing of signals

Two forms of transmission:

• digital transmission: data transmission using square waves

• analog transmission: data transmission using all other waves Four possibilities to consider:

• analog data via analog transmission → "as is" (e.g., radio)

• analog data via digital transmission → sampling (e.g., voice, audio, video)

• digital data via analog transmission → broadband & wireless

• digital data via digital transmission → baseband (e.g., Ethernet)

Why consider digital transmission?

Common to both: problem of attenuation.

• Decrease in signal strength as a function of distance

• Increase in attenuation as a function of frequency Rejuvenation of signal via amplifiers (analog) and repeaters (digital)

Delay distortion: different frequency components travel at different speeds. Most problematic: effect of noise −→ thermal, interference,

• Analog: Amplification also amplifies noise—filtering out just noise, in general, is a complex problem.

• Digital: Repeater just generates a new square wave; more resilient against ambiguity.

Analog transmission of digital data

Three pieces of information to manipulate: amplitude, frequency, phase.

• Amplitude modulation (AM): encode bits using amplitude levels.

• Frequency modulation (FM): encode bits using frequency differences.

• Phase modulation (PM): encode bits using phase shifts

2.3.3. Transmission Impairments

• Attenuation

– To reduce the amplitude of an electrical signal with little or no distortion

– Logarithmic in nature for guided media; expressed as a constant number of decibels per unit distance

– For unguided media, complex function of distance and atmospheric conditions

– Three considerations for transmission engineer

1. Received signal must have sufficient strength to enable detection

2. Signal must maintain a level sufficiently higher than noise to be received without error

3. Attenuation is an increasing function of frequency

– Signal strength must be strong but not too strong to overload the circuitry of transmitter or receiver, which will cause distortion

– Beyond a certain distance, attenuation becomes large to require the use of repeaters or amplifiers to boost the signal

– Attenuation distorts the received signal, reducing intelligibility

∗ Attenuation can be equalized over a band of frequencies

∗ Use amplifiers than can amplify higher frequencies more than low frequencies

• Delay distortion

– Peculiar to guided transmission media

– Caused by the fact that the velocity of signal propagation through a guided medium varies with frequency

∗ In bandlimited signal, velocity tends to be highest near the center frequency and falls off

towards the two edges of band

∗ Varying frequency components arrive at the receiver at different times, resulting in phase

shifts between different frequencies

– In digital data transmission, some signal components of one bit position will spill over into other bit positions, causing intersymbol interference

– May be reduced by using equalization techniques

• Noise

– Undesired signals that are inserted into the real signal during transmission

– Four types of noise

1. Thermal noise

∗ also called white noise

∗ Occurs due to thermal agitation of electrons

∗ Function of temperature and present in all electronic devices

∗ Uniformly distributed across frequency spectrum

∗ cannot be eliminated and places an upper bound on system performance

∗ Thermal noise in a bandwidth of 1 Hz in any device or conductor is

$$N0 = kT \text{ W/Hz}$$

Where N0 = Noise power density in watts per 1 Hz of bandwidth

k = Boltzmann's constant = 1.3803×10^{-23} J/◦K

T = temperature in degree kelvin

∗ At room temperature, T = 17◦C, or 290◦K, and the thermal noise power density is

$$N0 = 1.3803 \times 10^{-23} \times 290$$
$$= 4 \times 10^{-21} \text{ W/Hz}$$
$$= -204 \text{ dBW/Hz}$$

∗ Noise is assumed to be independent of frequency ·

Thermal noise in a bandwidth of B Hz can be expressed as

$$N = kT B$$

Or, in decibel-watts

$$N = 10 \log k + 10 \log T + 10 \log B$$
$$= -228.6 + 10 \log T + 10 \log B \text{dBW}$$

Given a receiver with an effective noise temperature of 100◦ K and a 10 mhz bandwidth, thermal noise level at the output is

$$N = -228.6 + 10 \log 102 + 10 \log 107$$
$$= -228.6 + 20 + 70$$
$$= -138.6 \text{dBW}$$

2. Intermodulation noise

   ∗ Signals at different frequencies share the same transmission medium

   ∗ May result in signals that are sum or difference or multiples of original frequencies

   ∗ Occurs when there is some nonlinearity in the transmitter, receiver, or intervening transmission system · Nonlinearity may be caused by component malfunction or excessive signal strength

3. Crosstalk

   ∗ Unwanted coupling between signal paths

   ∗ Occurs due to electric coupling between nearby twisted pairs, multiple signals on a coaxial cable, or unwanted signals picked up by microwave antennas

   ∗ Typically same order of magnitude or less than thermal noise

4. Impulse noise

   ∗ Noncontiguous noise, consisting of irregular pulses or noise spikes of short duration and high amplitudes

   ∗ May be caused by lightning, or flaws in communications system

   ∗ Not a major problem for analog data but can be significant for digital data ·

   A spike of 0.01 s will not destroy any voice data but will destroy 560 bits being transmitted at 56 kbps

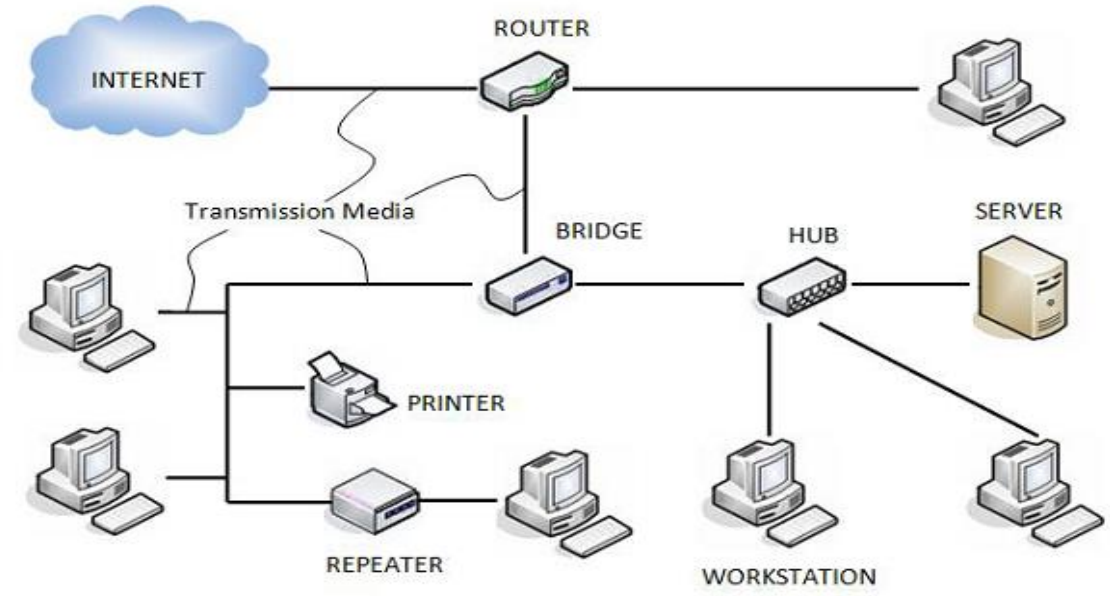
2.4. Components of the network

What is a Computer Network?

- **Computer Network** is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the sharing of resources among various devices.
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.

Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.

The following figure shows a network along with its component



COMPUTER NETWORK COMPONENTS

Hardware Components

- **Server's** −Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they

give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.

- **Clients** − Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers** − Peers are computers that provide as well as receive services from other peers in a workgroup network.
- **Transmission Media** − Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.
- **Connecting Devices** − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

2.4.1. End Devices & their role

Major components of a computer network are:

NIC (National interface card)

NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

- **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.
- **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

Hub

Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.

Switches

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

Cables and connectors

Cable is a transmission media that transmits the communication signals.

There are three types of cables:

- **Twisted pair cable:** It is a high-speed cable that transmits the data over **1Gbps** or more.
- **Coaxial cable:** Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.
- **Fibre optic cable:** Fibre optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

Router

What is a Router? The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**, etc. Some important points of routers are given below:

- A router is used in **LAN** (Local Area Network) and **WAN** (Wide Area Network) environments. For example, it is used in **offices** for connectivity, and you can also establish the connection between distant networks such as from **Bhopal** to
- It shares information with other routers in networking.
- It uses the routing protocol to transfer the data across a network.
- Furthermore, it is more **expensive** than other networking devices like switches and hubs.

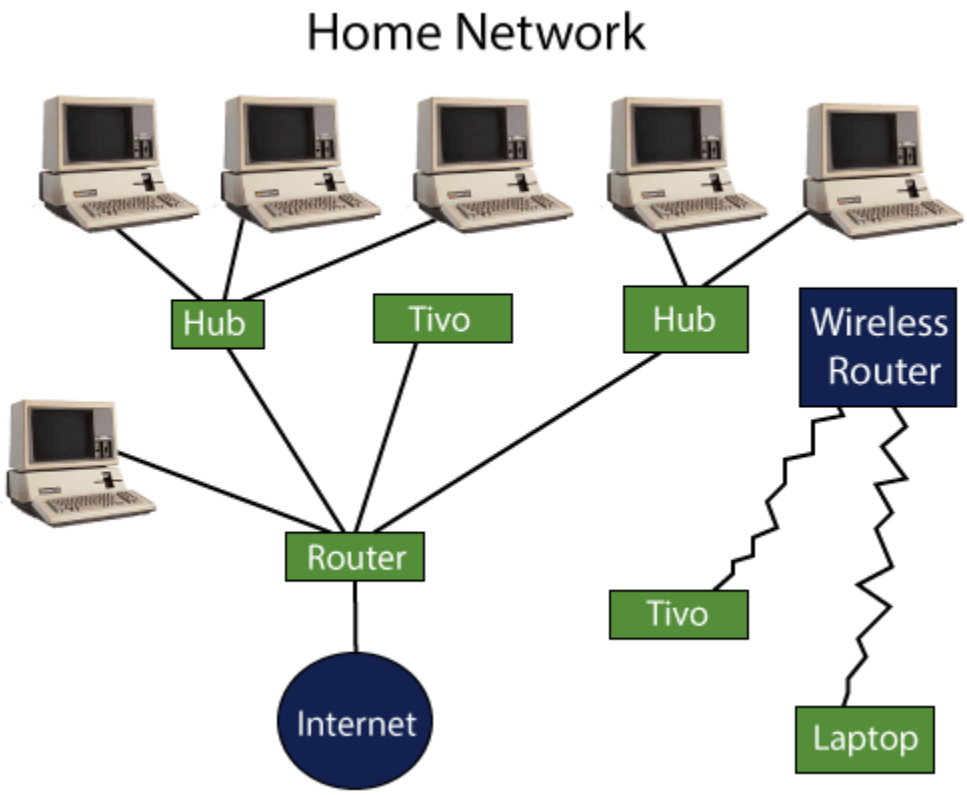
A router works on the **third layer** of the OSI model, and it is based on the IP address of a computer. It uses protocols such as ICMP to communicate between two or more networks. *It is also known as an **intelligent device** as it can calculate the best route to pass the network packets from source to the destination automatically.*

A virtual router is a software function or software-based framework that performs the same functions as a physical router. It may be used to increase the reliability of the network by virtual router redundancy protocol, which is done by configuring a virtual router as a default gateway. A virtual router runs on commodity servers, and it is packaged with alone or other network functions, like load balancing, firewall packet filtering, and wide area network optimization capabilities.

Why Routers?

A router is more capable as compared to other network devices, such as a hub, switch, etc., as these devices are only able to execute the basic functions of the network. For example, a hub is a basic networking device that is mainly used to forward the data between connected devices, but it cannot analyze or change anything with the transferring data. On the other hand, the router has the capability to analyze and modify the data while transferring it over a network, and it can send

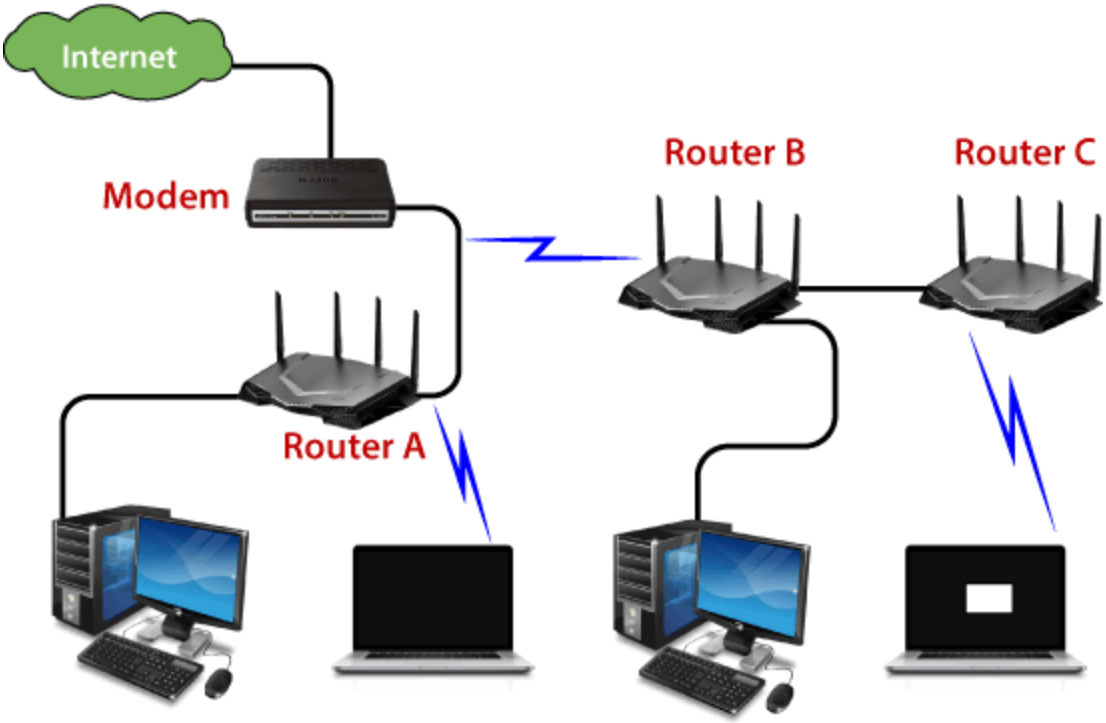
it to another network. For example, generally, routers allow sharing a single network connection between multiple devices.



How does Router work?

A router analyzes a destination IP address of a given packet header and compares it with the routing table to decide the packet's next path. The list of routing tables provides directions to transfer the data to a particular network destination. They have a set of rules that compute the best path to forward the data to the given IP address.

Routers use a **modem** such as a cable, fiber, or DSL modem to allow communication between other devices and the internet. Most of the routers have several ports to connect different devices to the internet at the same time. It uses the **routing tables** to determine where to send data and from where the traffic is coming.



A routing table mainly defines the default path used by the router. So, it may fail to find the best way to forward the data for a given packet. For example, the office router along a single default path instructs all networks to its internet services provider.

There are two types of tables in the router that are **static and dynamic**. The static routing tables are configured manually, and the dynamic routing tables are updated automatically by dynamic routers based on network activity.

Features of Router

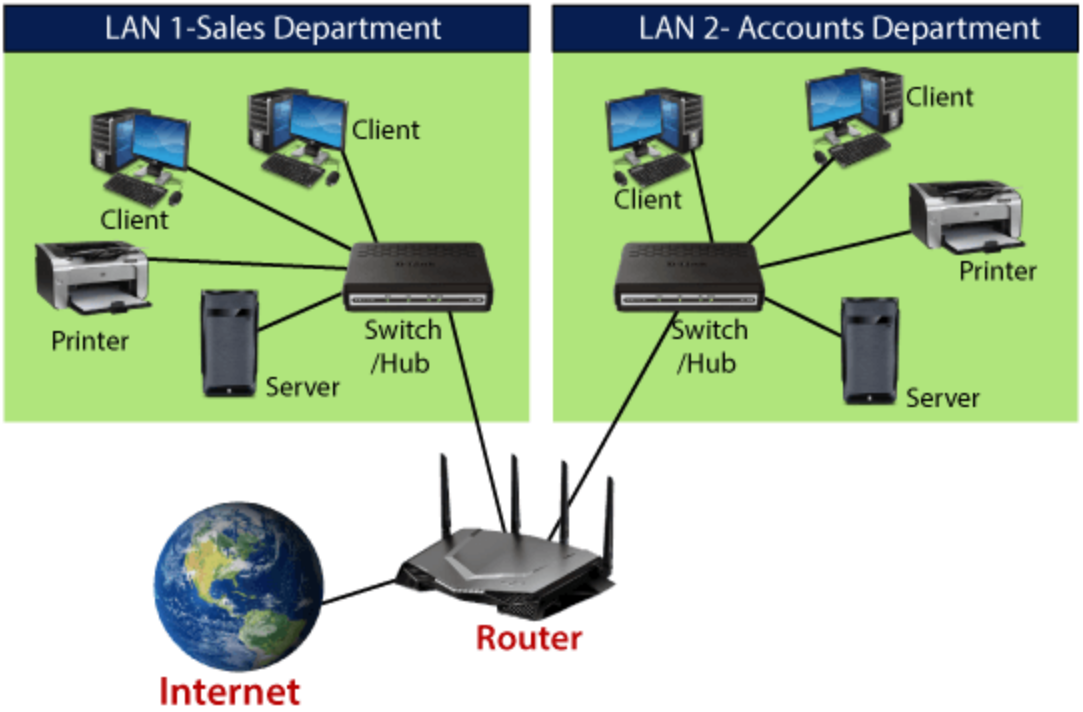
- A router works on the 3rd layer (Network Layer) of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
- A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
- It allows the users to configure the port as per their requirements in the network.
- Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.

- Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
- Routers filter out the unwanted interference, as well as carry out the data encapsulation and DE capsulation process.
- Routers provide the redundancy as it always works in master and slave mode.
- It allows the users to connect several LAN and WAN.
- Furthermore, a router creates various paths to forward the data.

Applications of Routers

There are various areas where a router is used:

- Routers are used to connect hardware equipment with remote location networks like **BSC, MGW, IN, SGSN**, and other servers.
- It provides support for a fast rate of data transmission because it uses high STM links for connectivity; that's why it is used in both wired or wireless communication.
- Internet service providers widely use routers to send the data from source to destination in the form of e-mail, a web page, image, voice, or a video file. Furthermore, it can send data all over the world with the help of an IP address of the destination.
- Routers offer access restrictions. It can be configured in a way that allows for few users to access the overall data and allows others to access the few data only, which is defined for them.
- Routers are also used by software testers for WAN communications. For example, the software manager of an organization is located in Agra, and its executive is located at a different place like Pune or Bangalore. Then the router provides the executive the method to share his software tools and other applications with the manager with the help of routers by connecting their PCs to the router using WAN architecture.
- In wireless networks, by configuring VPN in routers, it can be used in the client-server model, which allows sharing the internet, video, data, voice, and hardware resources. As shown in the below picture:



- In modern times, routers have the facility of inbuilt USB ports within the hardware. They have enough internal storage capacity. External storage devices can be used with routers to store and share data.
- Routers are used to set up the operation and maintenance center of an organization, which is known as the NOC center. All equipment at a distant location are connected by routers on optical cable at a central location, which also offer redundancy through the main link and protection link topology.

Types of Routers

There are various types of routers in networking; such are given below:

1. Wireless Router: Wireless routers are used to offer Wi-Fi connectivity to laptops, smartphones, and other devices with Wi-Fi network capabilities, and it can also provide standard ethernet routing for a small number of wired network systems.

Wireless routers are capable of generating a wireless signal in your home or office, and it allows the computers to connect with routers within a range, and use the internet. If the connection is

indoors, the range of the wireless router is about 150 feet, and when the connection is outdoors, then its range is up to 300 feet.

Furthermore, you can make more secure wireless routers with a password or get your IP address. Thereafter, you can log in to your router by using a user ID and password that will come with your router.

2. Brouter: A brouter is a combination of the bridge and a router. It allows transferring the data between networks like a bridge. And like a router, it can also route the data within a network to the individual systems. Thus, it combines these two functions of bridge and router by routing some incoming data to the correct systems while transferring the other data to another network.

3. Core router: A core router is a type of router that can route the data within a network, but it is not able to route the data between the networks. It is a computer communication system device and the backbone of networks, as it helps to link all network devices. It is used by internet service providers (ISPs), and it also provides various types of fast and powerful data communication interfaces.

4. Edge router: An edge router is a lower-capacity device that is placed at the boundary of a network. It allows an internal network to connect with the external networks. It is also called as an access router. It uses an External BGP (Border Gateway Protocol) to provides connectivity with remote networks over the internet.

There are two types of edge routers in networking:

- **Subscriber edge router**
- **Label edge router**

The **subscriber edge router** belongs to an end-user organization, and it works in a situation where it acts on a border device.

The **label edge router** is used in the boundary of Multiprotocol Label Switching (MPLS) networks. It acts as a gateway between the LAN, WAN, or the internet.

5. Broadband routers: Broadband routers are mainly used to provide high-speed internet access to computers. It is needed when you connect to the internet through phone and use voice over IP technology (VOIP).

All broadband routers have the option of three or four Ethernet ports for connecting the laptop and desktop systems. A broadband router is configured and provided by the internet service provider (ISP). It is also known as a **broadband modem**, asymmetric digital subscriber line (**ADSL**), or digital subscriber line (**DSL**) modem.

Benefits of Router

There are so many benefits of a router, which are given below:

- **Security:** Router provides the security, as LANs work in broadcast mode. The information is transmitted over the network and traverses the entire cable system. Although the data is available to each station, but the station which is specifically addressed reads the data.
- **Performance enhancement:** It enhances the performance within the individual network. For example, if a network has 14 workstations, and all generate approximately the same volume of traffic. The traffic of 14 workstations runs through the same cable in a single network. But if the network is divided into two sub-networks each with 7 workstations, then a load of traffic is reduced to half. As each of the networks has its own servers and hard disk, so fewer PCs will need the network cabling system.
- **Reliability:** Routers provide reliability. If one network gets down when the server has stopped, or there is a defect in the cable, then the router services, and other networks will not be affected. The routers separate the affected network, whereas the unaffected networks remain connected, without interrupting the work and any data loss.
- **Networking Range:** In networking, a cable is used to connect the devices, but its length cannot exceed 1000 meters. A router can overcome this limitation by performing the function of a repeater (Regenerating the signals). The physical range can be as per the requirement of a particular installation, as long as a router is installed before the maximum cable range exceeds.

Routing Protocols

Routing protocols specify a way for the router to identify other routers on the network and make dynamic decisions to send all network messages. There are several protocols, which are given below:

Open Shortest Path First (OSPF): It is used to calculate the best route for the given packets to reach the destination, as they move via a set of connected networks. It is identified by the Internet Engineering Task Force **(IETF)** as Interior Gateway Protocol.

Border Gateway Protocol (BGP): It helps manage how packets are routed on the internet via exchange of information between edge routers. It provides network stability for routers if one internet connection goes down while forwarding the packets, it can adapt another network connection quickly to send the packets.

Interior Gateway Routing Protocol (IGRP): It specifies how routing information will be exchanged between gateways within an independent network. Then, the other network protocols can use the routing information to determine how transmissions should be routed.

Enhanced Interior Gateway Routing Protocol (EIGRP): In this protocol, if a router is unable to find a path to a destination from the tables, it asks route to its neighbors, and they pass the query to their neighbors until a router has found the path. When the entry of routing table changes in one of the routers, it informs its neighbors only about the changes, but do not send the entire table.

Exterior Gateway Protocol (EGP): It decides how routing information can be exchanged between two neighbor gateway hosts, each of which has its own router. Additionally, it is commonly used to exchange routing table information between hosts on the internet.

Routing Information Protocol (RIP): It determines how routers can share information while transferring traffic among connected group of local area networks. The maximum number of hops that can be allowed for RIP is 15, which restricts the size of networks that RIP can support.

2.4.2. Intermediary Devices & their role

Difference between Bridge and Router

Bridge	Router
A bridge is a networking device that is used to connect two local area networks (LANs) by using media access control addresses and transmit the data between them.	A router is also a networking device that sends the data from one network to another network with the help of their IP addresses.
A bridge is able to connect only two different LAN segments.	A router is capable of connecting the LAN and WAN.
A bridge transfers the data in the form of frames.	A router transfers the data in the form of packets.
It sends data based on the MAC address of a device.	It sends data based on the IP address of a device.
The bridge has only one port to connect the device.	The router has several ports to connect the devices.
The bridge does not use any table to forward the data.	The router uses a routing table to send the data.

Difference between Hub, Switch, and Router

There are three primarily networking devices that connect the computers from one to another. These devices are hub, switch, and router. These all have the ability to connect one computer to another, but there is some difference between them. The difference between a hub, switch, and router are given below:

Hub: A hub is a basic networking device that is used to connect computers or other networking devices together. A hub does not use any routing table to send the data to the destination. Although it can identify basic errors of networks like collisions, it can be a security risk to broadcast all information to the multiple ports. As the hub is a dumb device, it does not need an IP address. Furthermore, Hubs are cheaper than a switch or router.

Switch: A switch is a hardware device that also connects computers to each other. A switch is different as compared to a hub in that way; it handles packets of data. Whenever a switch receives a packet, it decides the device to which the packet can be sent, and sends it to that device only. A hub broadcasts the packet to all computers, but the switch does not circulate the packet to all devices, which means bandwidth is not shared with the network, and thus it increases the efficiency of the network. That's why switches are more preferred as compared to a hub.

Router: A router is more different from a switch or hub. It is mainly used to route the data packets to another network instead of transmitting the data to the local networks only. A router is commonly found in homes and offices as it allows your network to communicate with other networks through the internet. Basically, a router provides more features to your networks like firewall, VPN, QoS, traffic monitoring, etc.

What is Routing Table in Router?

A routing table determines the path for a given packet with the help of an IP address of a device and necessary information from the table and sends the packet to the destination network. The routers have the internal memory that is known as Random Access Memory (RAM). All the information of the routing table is stored in RAM of routers.

For example:

Destination (Network ID)	Subnet mask	Interface
200.1.2.0	255.255.255.0	Eth0
200.1.2.64	255.255.255.128	Eth1
200.1.2.128	255.255.255.255	Eth2
Default		Eth3

A routing table contains the following entities:

- It contains an IP address of all routers which are required to decide the way to reach the destination network.
- It includes extrovert interface information.
- Furthermore, it is also contained IP addresses and subnet mask of the destination host.

Network Element in Router

There are two types of a network element in the router which are as follows:

Control plane: A router supports a routing table that determines which path and physical interface connection should be used to send the packet. It is done by using internal pre-configured directives, which are called static routes, or by learning routes with the help of routing protocol. A routing table stores the static and dynamic routes. Then the control-plane logic eliminates the unnecessary directives from the table and constructs a forwarding information base that is used by the forwarding plane.

Forwarding plane: A router sends data packets between incoming and outgoing interface connections. It uses information stored in the packet header and matches it to entries in the FIB, which is supplied by the control plane; accordingly, it forwards the data packet to the correct network type. It is also called the user plane or data plane.

How to buy a Router?

There are many points to keep in mind while buying a router:

1. **Type of Connection:** Which kind of router should you buy depends on the type of connection you have. For example, if you want to use the internet connection from your telephone services providers like BSNL or MTNL, you will need an ADSL router. In this router, you have to use the hardware that is provided to you with your connection. Although this router may have limited functionalities on some fronts. Alternatively, you can purchase an advanced router that allows you sharing storage, including printer over a wireless connection. If you use the connection provided by the local cable operator, you will need a non-ADSL router.
2. **Standard:** The routers support standards like 802.11ac, 802.11n, etc. The routers that support 802.11ac standard, enhances the speed to transfer the data more than three times the speed of 802.11n standard routers. It uses the 5GHz frequency band, which is less crowded as compared to the regular 2.4GHz band. Furthermore, it also provides better network performance for file transfers and streaming media content. The routers that support 802.11ac standard are beneficial as they are compatible with 'n' standard, by which your older devices can also work without any problem.Alternatively; you can save some money and full fill your requirements by purchasing 'n' standard routers.
3. **Dual-band:** Most of 'n' standard routers operate in the 2.4GHz frequency, but a dual-band router is better as it supports the 5GHz band. Furthermore, it can also connect with smartphones and laptops on 5GHz, while other routers can operate over 2.4GHz only.
4. **USB port:** Routers with USB ports allow you to plug flash drives, including printers, to share these resources over the network. These functions are suitable for a small area as they can be used within the wireless network without using the internet. Some routers provide backup internet by 3G data dongles when your main connection goes down. But these routers work with specific brands only. So, before purchasing a router, check if it supports the dongle you are using.

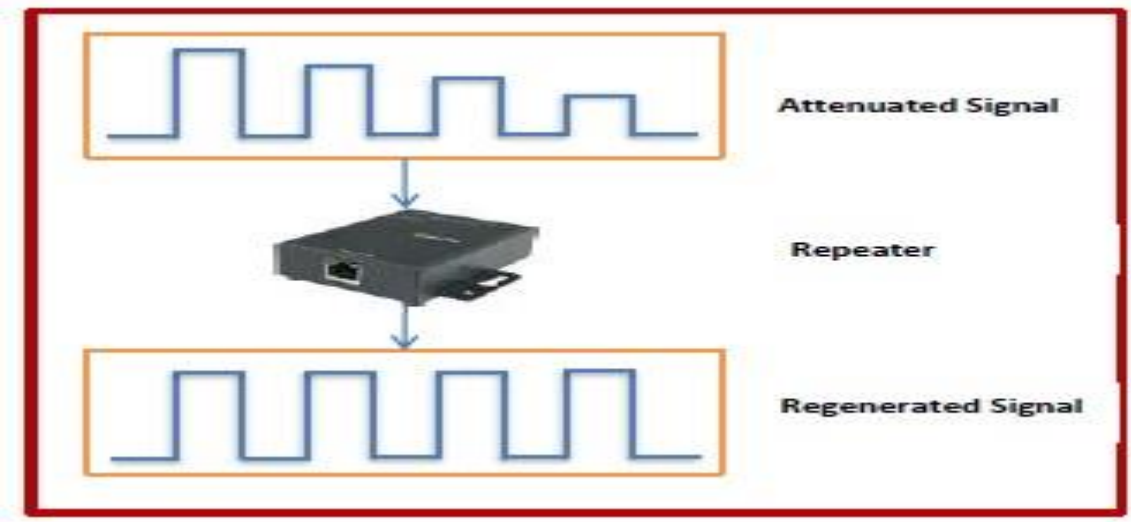
5. **Multiple antennas:** External antennas are strong enough to increase the overall range of your router as well as are suitable for environments where you need signals across multiple walls or doors.

Modem

Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard. A modem is a separate part on the PC slot found on the motherboard.

Repeaters

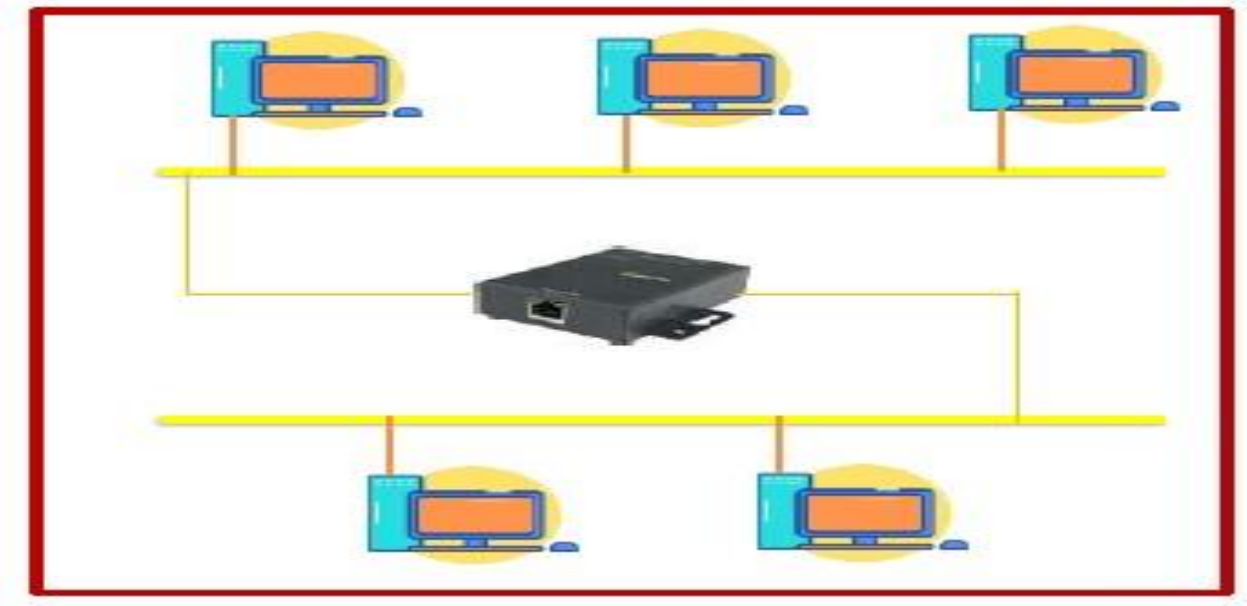
Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals. Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.

So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN. This is shown in the following diagram −



Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- **Analog Repeaters** − They can only amplify the analog signal.
- **Digital Repeaters** − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types

- **Wired Repeaters** − they are used in wired LANs.
- **Wireless Repeaters** − they are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- **Local Repeaters** − they connect LAN segments separated by small distance.
- **Remote Repeaters** − they connect LANs that are far from each other.

Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don’t require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

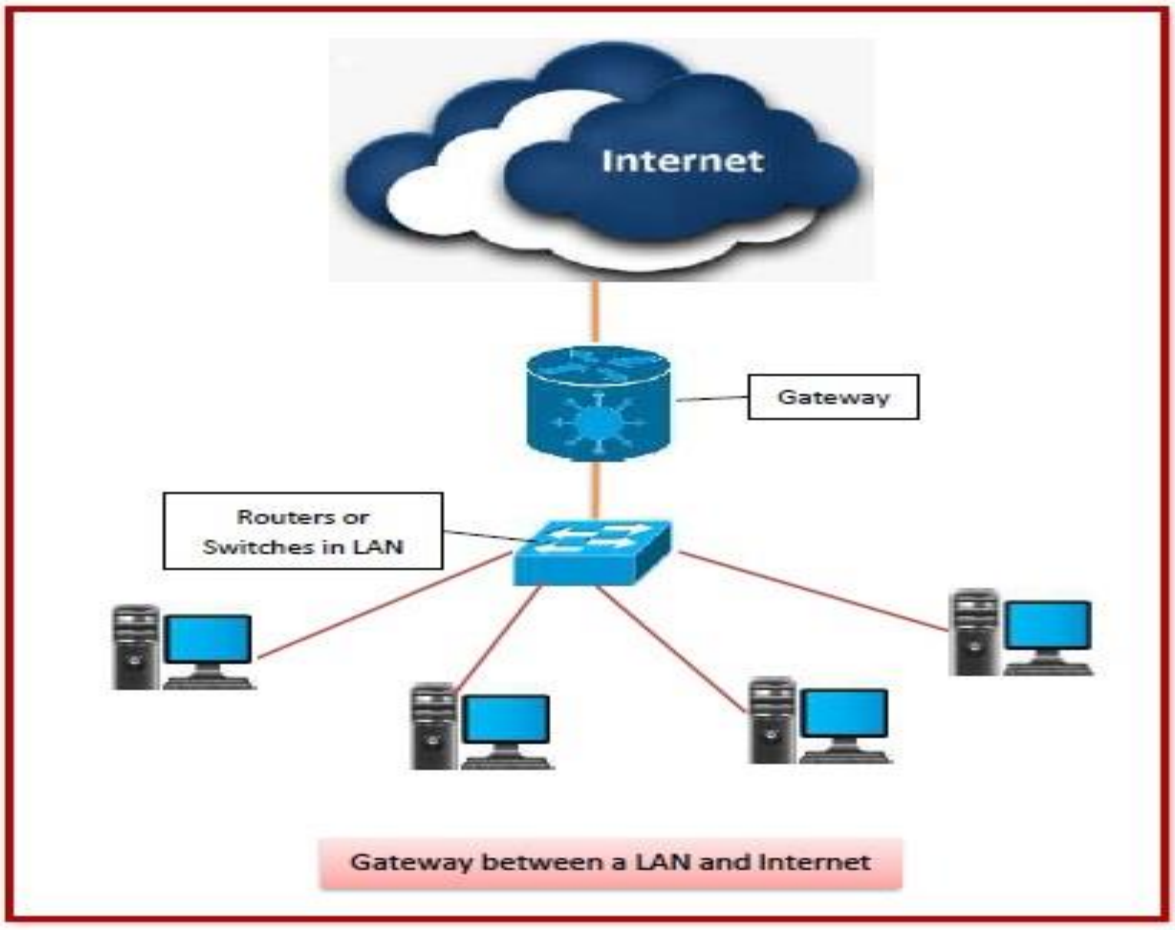
Disadvantages of Repeaters

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

Gateways

A gateway is a hardware device that acts as a "gate" between two networks. It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network.
While a gateway protects the nodes within network, it also a node itself. The gateway node is considered to be on the "edge" of the network as all data must flow through it before coming in or going out of the network. It may also translate data received from outside networks into a format or protocol recognized by devices within the internal network.
A router is a common type of gateway used in home networks. It allows computers within the local network to send and receive data over the Internet. A firewall is a more advanced type of gateway, which filters inbound and outbound traffic, disallowing incoming data from suspicious or unauthorized sources. A proxy server is another type of gateway that uses a combination of hardware and software to filter traffic between two networks. For example, a proxy server may only allow local computers to access a list of authorized websites.

NOTE: Gateway is also the name of a computer hardware company founded in the United States in 1985. The company was acquired by Acer in 2007 but still sells computers under the Gateway name.



Features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or out flows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.

- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses packet switching technique to transmit data across the networks.

Types of Gateways

On basis of direction of data flow, gateways are broadly divided into two categories −

- **Unidirectional Gateways** − they allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
- **Bidirectional Gateways** − they allow data to flow in both directions. They can be used as synchronization tools.

On basis of functionalities, there can be a variety of gateways, the prominent among them are as follows −

- **Network Gateway** − This is the most common type of gateway that provides as interface between two dissimilar networks operating with different protocols. Whenever the term gateway is mentioned without specifying the type, it indicates a network gateway.
- **Cloud Storage Gateway** − It is a network node or server that translates storage requests with different cloud storage service API calls, such as SOAP (Simple Object Access Protocol) or REST (Representational State Transfer).It facilitates integration of private cloud storage into applications without necessitating transfer of the applications into any public cloud, thus simplifying data communication.
- **Internet-To-Orbit Gateway (I2O)** − It connects devices on the Internet to satellites and spacecraft orbiting the earth. Two prominent I2O gateways are Project HERMES and Global Educational Network for Satellite Operations (GENSO).

- **IoT Gateway** − IoT gateways assimilates sensor data from IoT (Internet of Things) devices in the field and translates between sensor protocols before sending it to the cloud network. They connect IoT devices, cloud network and user applications.
- **VoiP Trunk Gateway** − It facilitates data transmission between plain old telephone service (POTS) devices like landline phones and fax machines, with VoIP (voice over Internet Protocol) network.

Switches

What is a network switch?

A network switch is a device that operates at the Data Link layer of the OSI model—Layer 2. It takes in packets being sent by devices that are connected to its physical ports and sends them out again, but only through the ports that lead to the devices the packets are intended to reach. They can also operate at the network layer--Layer 3 where routing occurs.

Switches are a common component of networks based on Ethernet, Fibre Channel, Asynchronous Transfer Mode (ATM), and InfiniBand, among others. In general, though, most switches today use ether net

How does a network switch work?

Once a device is connected to a switch, the switch notes its media access control (MAC) address, a code that's baked into the device's network-interface card (NIC) that attaches to an ethernet cable that attaches to the switch. The switch uses the MAC address to identify which attached device outgoing packets are being sent from and where to deliver incoming packets.

So the MAC address identifies the physical device as opposed to the network layer (Layer 3) IP address, which can be assigned dynamically to a device and change over time.

When a device sends a packet to another device, it enters the switch and the switch reads its header to determine what to do with it. It matches the destination address or addresses and sends the packet out through the appropriate ports that leads to the destination devices.

To reduce the chance for collisions between network traffic going to and from a switch and a connected device at the same time, most switches offer full-duplex functionality in which

packets coming from and going to a device have access to the full bandwidth of the switch connection. (Picture two people talking on a cell phone as opposed to a walkie-talkie).

While it's true that switches operate at Layer 2, they can also operate at Layer 3, which is necessary for them to support virtual LANs (VLAN), logical network segments that can span subnets. In order for traffic to get from one subnet to another it must pass between switches, and this is facilitated by routing capabilities built into the switches.

2.4.3. Network Media

Uses Of Computer Network

- **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
- **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Software Components

- **Networking Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −
    - a. OSI Model (Open System Interconnections)
    - b. TCP / IP Model

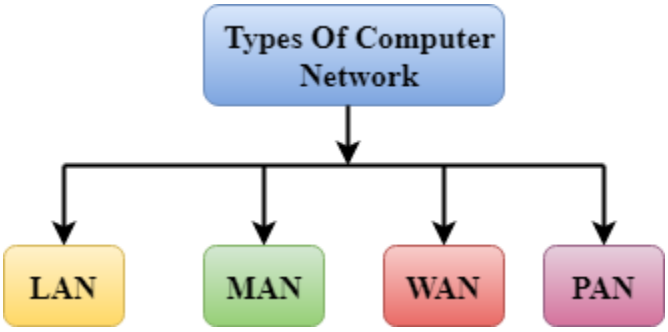
Chapter 3:

3. Network Types

3.1 Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

3.1. LANs, WANs and Internetworks

LAN(Local Area Network)

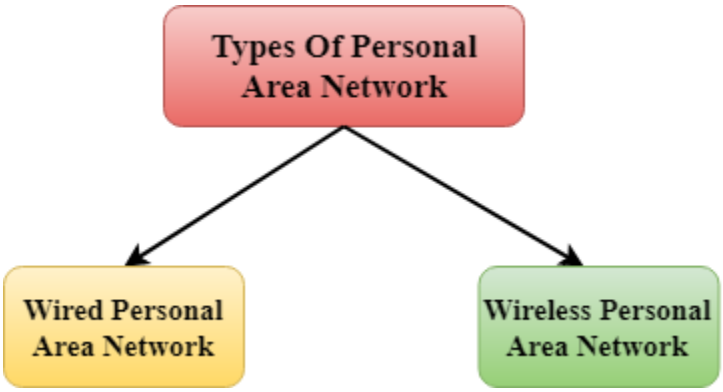
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.

- Local Area Network provides higher security.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:



- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

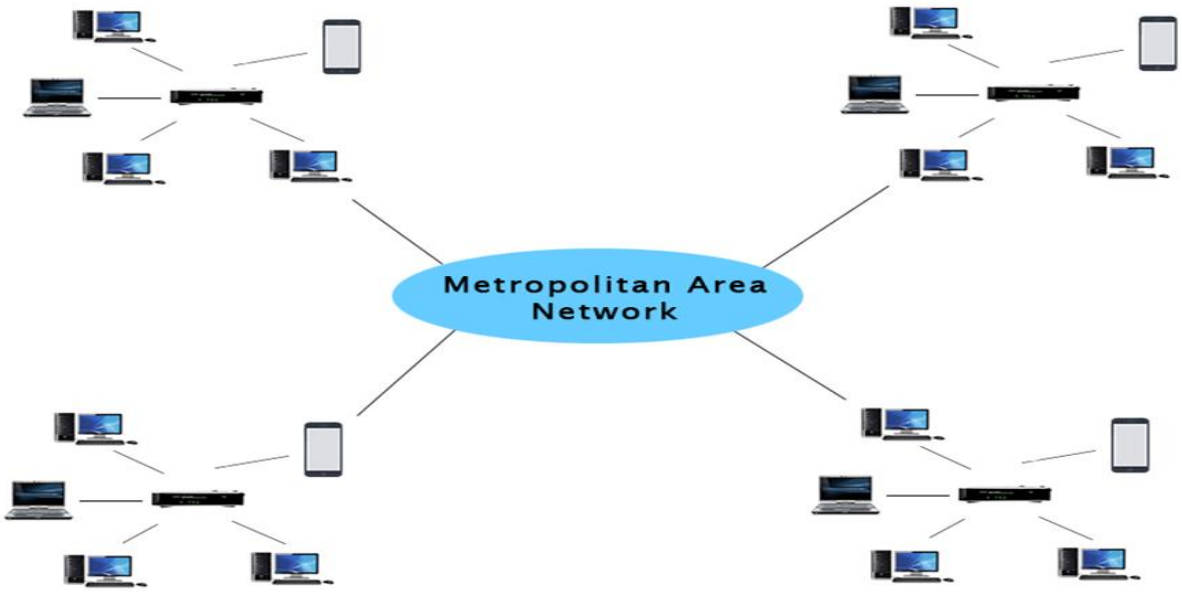
Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN (Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

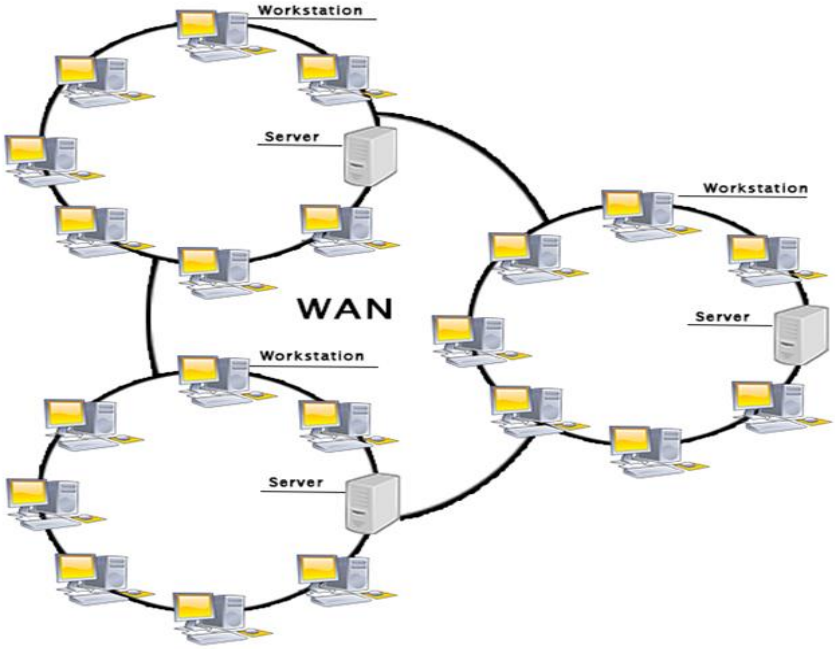


Uses **of** Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN (Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.

- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.

- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
- **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
- **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
- **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

3.2. Peer to peer versus Server based Networks

The two major types of network operating systems are:

- Peer-to-Peer
- Client/Server

Nearly all modern networks are a combination of both. The networking design can be considered independent of the servers and workstations that will share it.

Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source (See fig. 1). In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. Nearly all modern desktop operating systems, such as Macintosh OSX, Linux, and Windows, can function as peer-to-peer network operating systems.

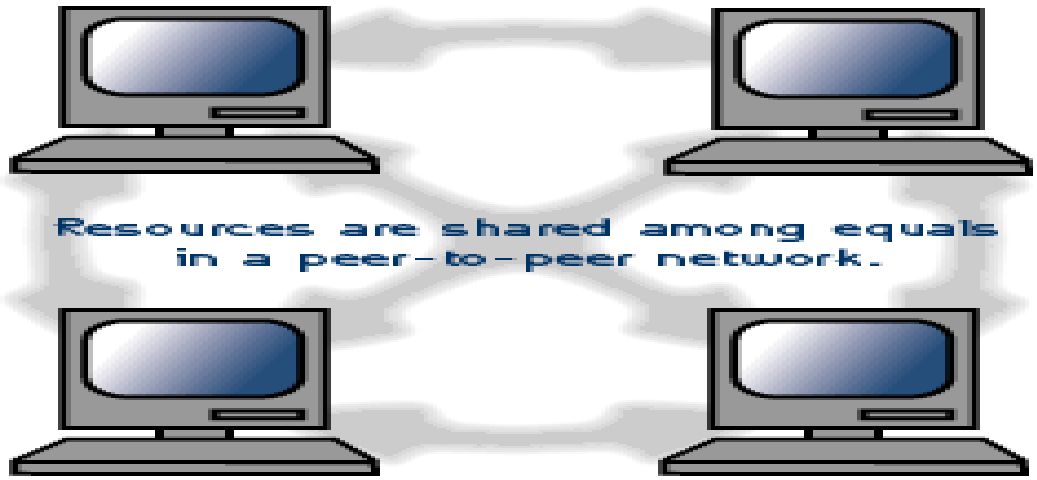


Fig. 1. Peer-to-peer network

Advantages of a peer-to-peer network:

- Less initial expense - No need for a dedicated server.
- Setup - An operating system (such as Windows XP) already in place may only need to be reconfigured for peer-to-peer operations.

Disadvantages of a peer-to-peer network:

- Decentralized - No central repository for files and applications.
- Security - Does not provide the security available on a client/server network.

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers. The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. UNIX/Linux and the Microsoft family of Windows Servers are examples of client/server network operating systems.

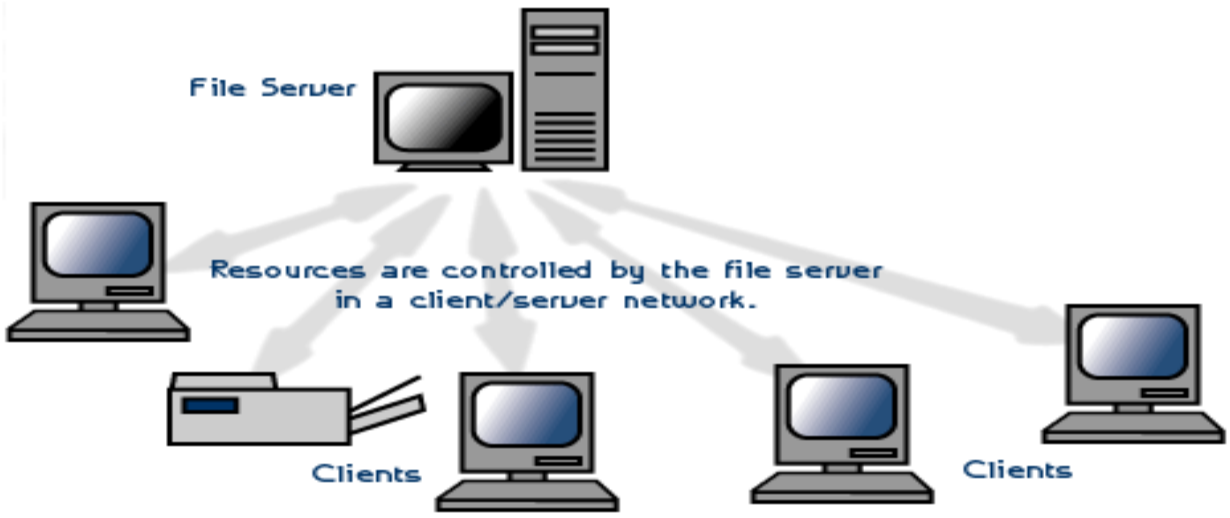


Fig. 2. Client/server network

Advantages of a client/server network:

- Centralized - Resources and data security are controlled through the server.
- Scalability - Any or all elements can be replaced individually as needs increase.
- Flexibility - New technology can be easily integrated into system.
- Interoperability - All components (client/network/server) work together.
- Accessibility - Server can be accessed remotely and across multiple platforms.

Disadvantages of a client/server network:

- Expense - Requires initial investment in dedicated server.
- Maintenance - Large networks will require a staff to ensure efficient operation.
- Dependence - When server goes down, operations will cease across the network.

3.3. Packet-switched and Circuit switched networks

What is Circuit Switching?

Circuit switching is defined as the method of switching which is used for establishing a dedicated communication path between the sender and the receiver. The link which is established between the sender and the receiver is in the physical form. Analog telephone network is a well-

known example of circuit switching. Bandwidth is fixed in this type of switching. Let us know in detail about the advantages and disadvantages of circuit switching.

Advantages and Disadvantages of Circuit Switching

Advantages

- The bandwidth used is fixed.
- The quality of communication is increased as a dedicated communication channel is used.
- The rate at which the data is transmitted is fixed.
- While switching, no time is wasted in waiting.
- It is preferred when the communication is long and continuous.

Disadvantages

- Since dedicated channels are used, the bandwidth required is more.
- The utilization of resources is not full.
- Since a dedicated channel has been used, the transmission of other data becomes impossible.
- The time taken by the two stations for the establishment of the physical link is too long.
- Circuit switching is expensive because every connection uses a dedicated path establishment.
- The link between the sender and the receiver will be maintained until and unless the user terminates the link. This will also continue if there is no transfer of data taking place.

What is Packet Switching?

Packet switching is defined as the connectionless network where the messages are divided and grouped together and this is known as a packet. Each packet is routed from the source to the destination as individual packets. The actual data in these packets are carried by the payload. When the packet arrives at the destination, it is the responsibility of the destination to put these packets in the right order. Let us know in detail about the advantages and disadvantages of packet switching.

Advantages and Disadvantages of Packet Switching

Advantages

- There is no delay in the delivery of the packets as they are sent to the destination as soon as they are available.
- There is no requirement for massive storage space as the information is passed on to the destination as soon as they are received.
- Failure in the links does not stop the delivery of the data as these packets can be routed from other paths too.
- Multiple users can use the same channel while transferring their packets.
- The usage of bandwidth is better in case of packet switching as multiple sources can transfer packets from the same source link.

Disadvantages

- Installation costs of packet switching are expensive.
- The delivery of these packets becomes easy when complicated protocols are used.
- High-quality voice calls cannot use packet switching as there is a lot of delay in this type of communication.
- Connectivity issues may lead to loss of information and delay in the delivery of the information.

You may also want to check out these topics given below!

- Components of Basic Electric Circuit
- Circuit Diagram
- Types of Switches

Let us understand the difference between circuit and switching packet switching.

Circuit Switching Vs Packet Switching

Circuit switching is referred to as the technology of data transfer that utilizes sending messages from one point to another. This involves sending messages from the receiver to the sender and back simultaneously. A physical connection gets established during this process along with the

receiver; a dedicated circuit is always present to handle data transmissions, through which data is sent. Packet switching can be used as an alternative to circuit switching. In the packet-switched networks, data is sent in discrete units that have variable length.

Difference between Circuit Switching and Packet Switching	
Circuit Switching	**Packet Switching**
A circuit needs to be established to make sure that data transmission takes place.	Each packet containing the information that needs to be processed goes through the dynamic route.
A uniform path is followed throughout the session.	There is no uniform path that is followed end to end through the session.
It is most ideal for voice communication, while also keeping the delay uniform.	It is used mainly for data transmission as the delay is not uniform.
Without a connection, it cannot exist, as the connection needs to be present on a physical layer.	A connection is not necessary, as it can exist without one too. It needs to be present on a network layer.
Data to be transmitted is processed at the source itself.	Data is processed and transmitted at the source as well as at each switching station.

Thus, this explains the Circuit Switching and Packet Switching differences.

3.4. Network cabling & Topologies

What is Network Cabling?

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a

network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides
- Wireless LANs
- Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

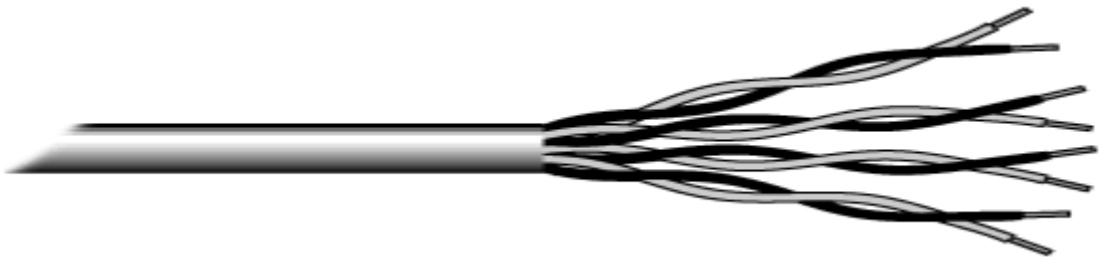


Fig.1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Categories of Unshielded Twisted Pair

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

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

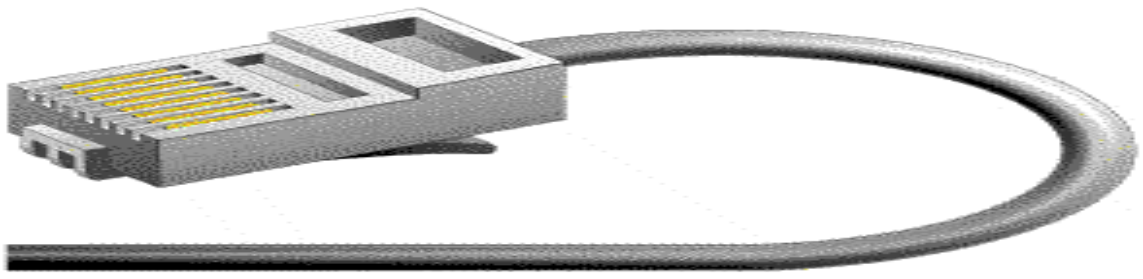


Fig. 2. RJ-45 connector

Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

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

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

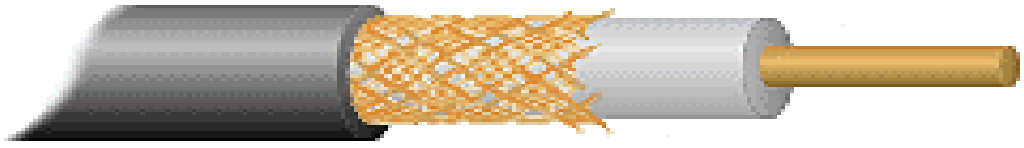


Fig. 3. Coaxial cable

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

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

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

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

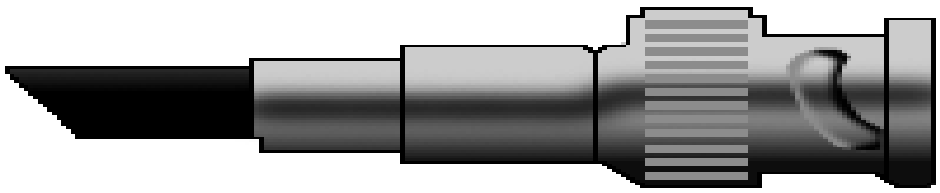


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

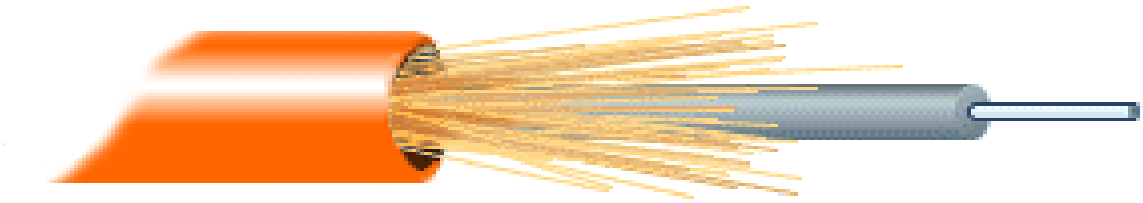


Fig. 5. Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Specification	**Cable Type**
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic

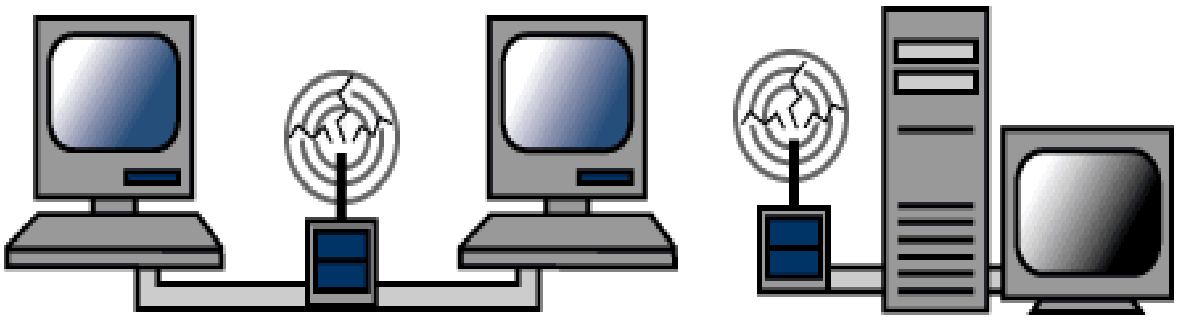
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

Installing Cable - Some Guidelines

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

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

Wireless LANs



More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations, servers, or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless standards and speeds

The Wi-Fi Alliance is a global, non-profit organization that helps to ensure standards and interoperability for wireless networks, and wireless networks are often referred to as WiFi (Wireless Fidelity). The original Wi-Fi standard (IEEE 802.11) was adopted in 1997. Since then many variations have emerged (and will continue to emerge). Wi-Fi networks use the Ethernet protocol.

Standard	Max Speed	Typical Range
802.11a	54 Mbps	150 feet

802.11b	11 Mbps	300 feet
802.11g	54 Mbps	300 feet
802.11n	100 Mbps	300+ feet

Wireless Security

Wireless networks are much more susceptible to unauthorized use than cabled networks. Wireless network devices use radio waves to communicate with each other. The greatest vulnerability to the network is that rogue machines can "eves-drop" on the radio wave communications. Unencrypted information transmitted can be monitored by a third-party, which, with the right tools (free to download), could quickly gain access to your entire network, steal valuable passwords to local servers and online services, alter or destroy data, and/or access personal and confidential information stored in your network servers. To minimize the possibility of this, all modern access points and devices have configuration options to encrypt transmissions. These encryption methodologies are still evolving, as are the tools used by malicious hackers, so always use the strongest encryption available in your access point and connecting devices.

A NOTE ON ENCRYPTION: As of this writing WEP (Wired Equivalent Privacy) encryption can be easily hacked with readily-available free tools which circulate the internet. WPA and WPA2 (WiFi Protected Access versions 1 and 2) are much better at protecting information, but using weak passwords or passphrases when enabling these encryptions may allow them to be easily hacked. If your network is running WEP, you must be very careful about your use of sensitive passwords or other data.

Three basic techniques are used to protect networks from unauthorized wireless use. Use any and all of these techniques when setting up your wireless access points:

Encryption.

Enable the strongest encryption supported by the devices you will be connecting to the network. Use strong passwords (strong passwords are generally defined as passwords containing symbols, numbers, and mixed case letters, at least 14 characters long).

Isolation.

Use a wireless router that places all wireless connections on a subnet independent of the primary private network. This protects your private network data from pass-through internet traffic.

Hidden SSID.

Every access point has a Service Set IDentifier (SSID) that by default is broadcast to client devices so that the access point can be found. By disabling this feature, standard client connection software won't be able to "see" the access point. However, the eves-dropping programs discussed previously can easily find these access points, so this alone does little more than keep the access point name out of sight for casual wireless users.

Advantages of wireless networks:

- Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free WiFi access ("Hot spots").
- Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.
- Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.
- Expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

Disadvantages of wireless networks:

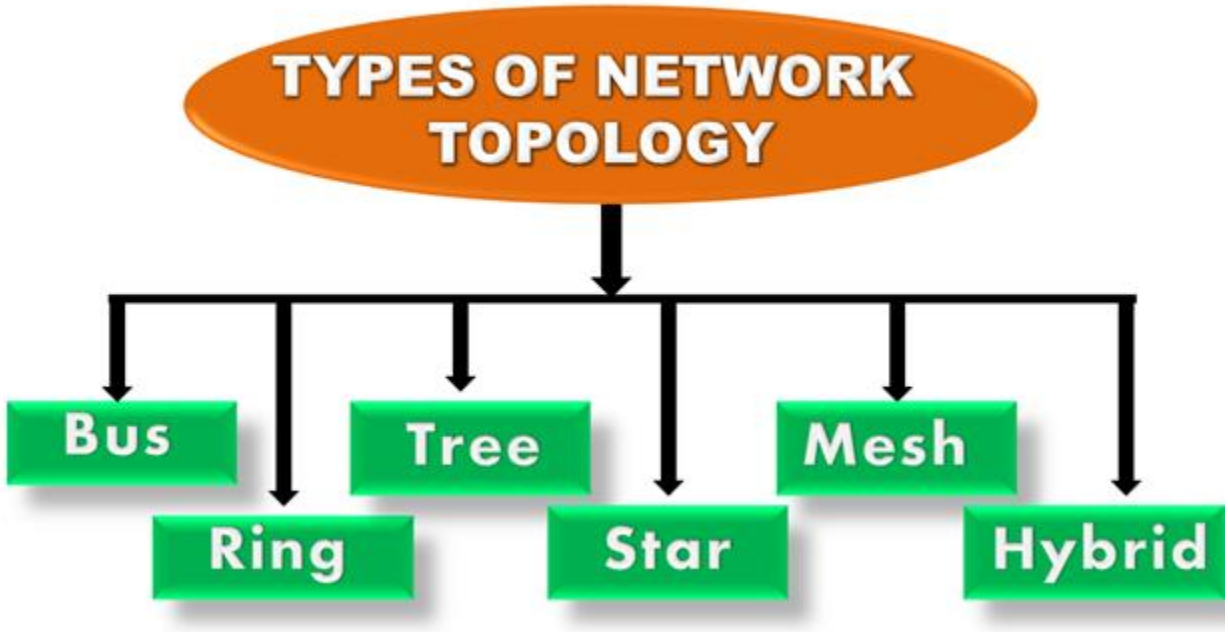
- Security - Be careful. Be vigilant. Protect your sensitive data with backups, isolated private networks, strong encryption and passwords, and monitor network access traffic to and from your wireless network.

- Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
- Inconsistent connections - How many times have you hears "Wait a minute, I just lost my connection?" Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
- Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. If you are only using wireless for internet access, the actual internet connection for your home or school is generally slower than the wireless network devices, so that connection is the bottleneck. If you are also moving large amounts of data around a private network, a cabled connection will enable that work to proceed much faster.

What is Topology?

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Physical topology is the geometric representation of all the nodes in a network.



Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".

- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
    - **Token passing:** It is a network access method in which token is passed from one node to another node.
    - **Token:** It is a frame that circulates around the network.

Working of Token passing

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.

- In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.

- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

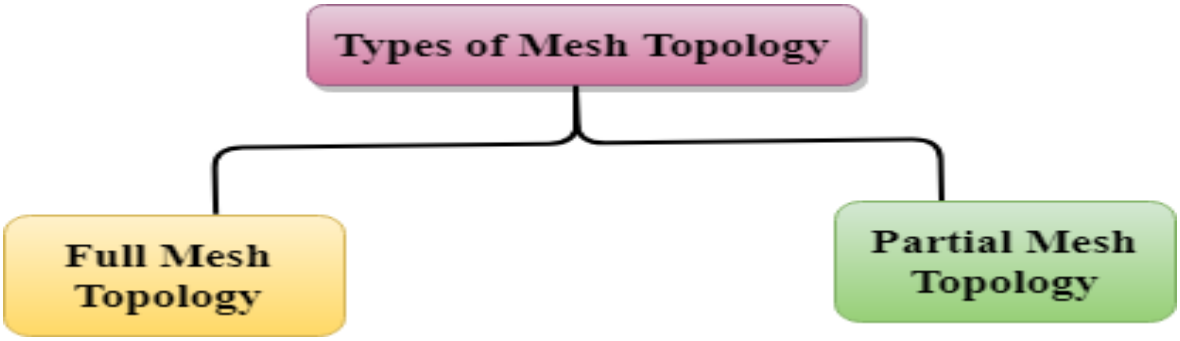
Mesh topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:
  Number of cables = (n*(n-1))/2;

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology



- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

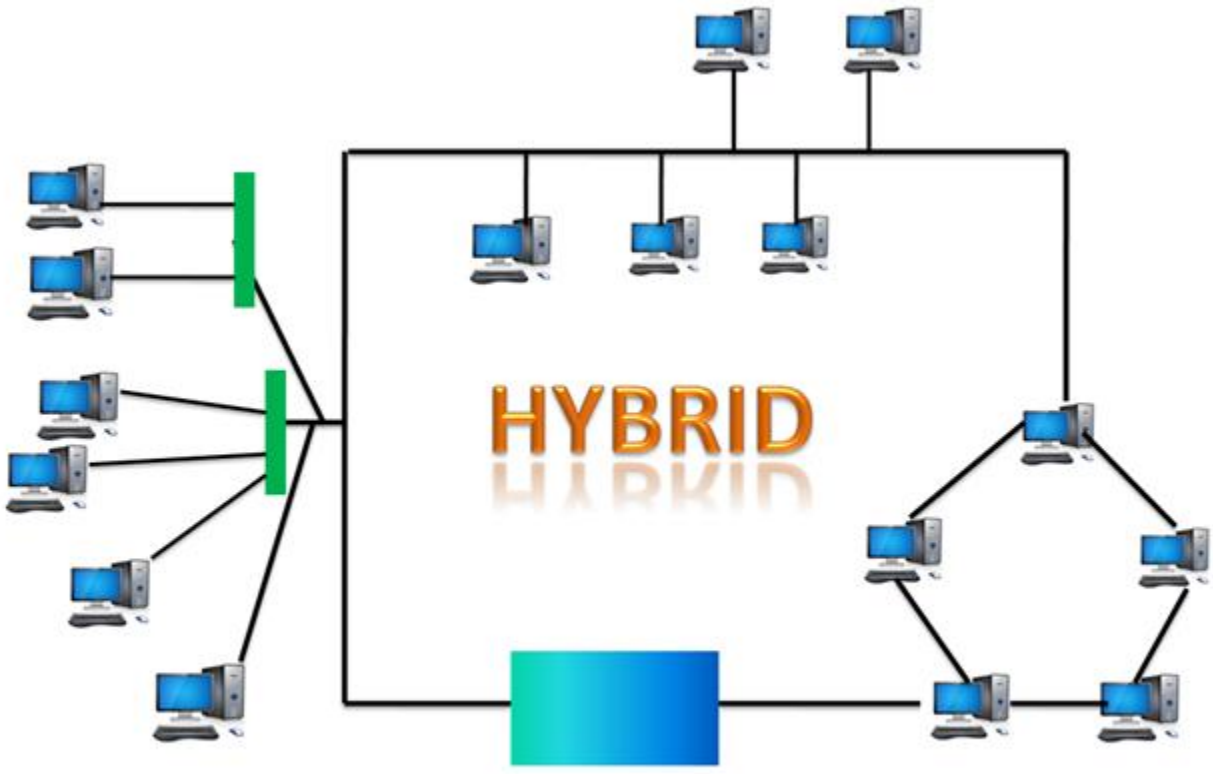
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Chapter 4

4. Protocols

4.1 Network protocols

Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. In other words, network protocols can be equated to languages that two devices must understand for seamless communication of information, regardless of their infrastructure and design disparities.

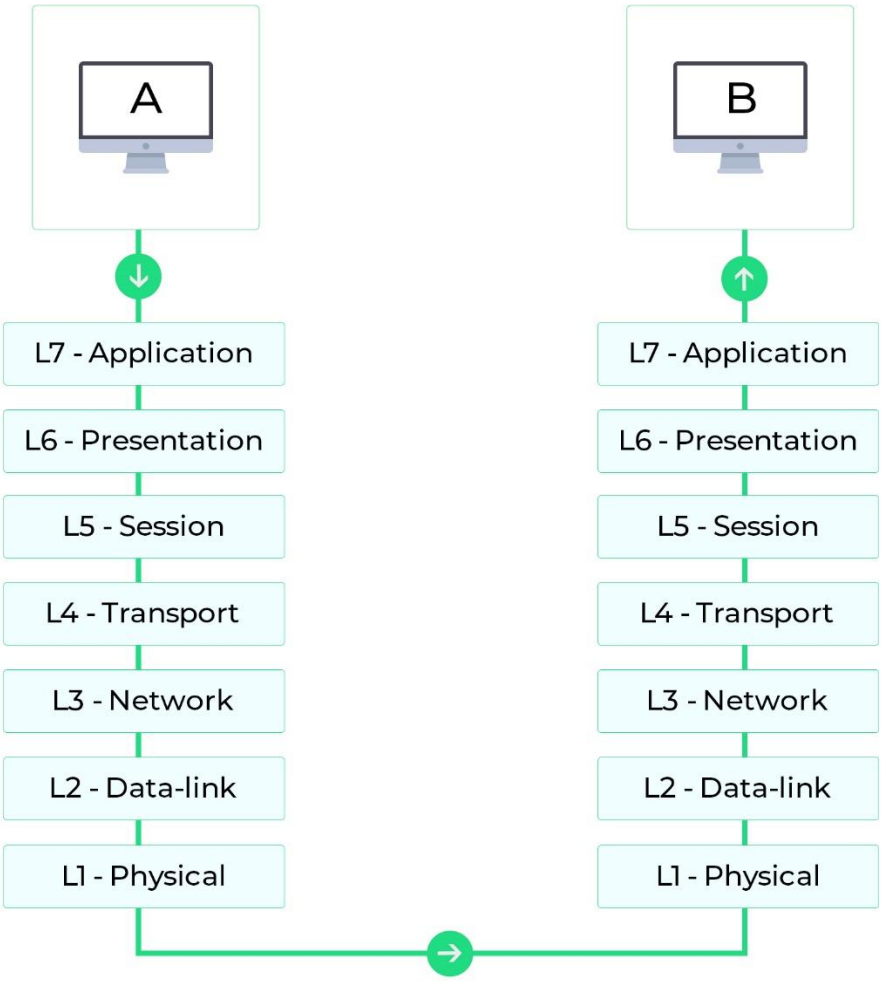
4.1. Rules & Network Protocols

The OSI model: How network protocols work

To understand the nuances of network protocols , it's imperative to know about the Open Systems Interconnection (OSI) model first. Considered the primary architectural model for internet working communications, the majority of network protocols used today are structurally based on the OSI model.

The OSI model splits the communication process between two network devices into 7 layers. A task or group of tasks is assigned to each of these 7 layers. All the layers are self-contained, and the tasks assigned to them can be executed independently.

To put this into context, here is a representation of the communication process between two network devices following the OSI model:



The seven layers in the OSI model can be divided into two groups: upper layers, including layers 7, 6, and 5, and lower layers, including layers 4, 3, 2, and 1. The upper layers deal with application issues, and the lower layers deal with data transport issues.

Network protocols divide the communication process into discrete tasks across every layer of the OSI model. One or more network protocols operate at each layer in the communication exchange.

Following are the detailed descriptions of the functioning of network protocols in each layer of the OSI model:

Layer 7: Application layer network protocols	Provides standard services such as virtual terminal, file, and job transfer and operations.
Layer 6: Presentation layer network protocols	Masks the differences in data formats between dissimilar systems. Encodes and decodes data, encrypts and decrypts data, and compresses and decompresses data.
Layer 5: Session layer network protocols	Manages user sessions and dialogues. Establishes and terminates sessions between users.
Layer 4: Transport layer network protocols	Manages end-to-end message delivery in networks. Renders reliable and sequential packet delivery through error recovery and flow control mechanisms.
Layer 3: Network layer protocols	Routes packets according to unique network device addresses. Renders flow and congestion control to prevent network resource depletion.
Layer 2: Data link layer network protocols	Frames packets. Detects and corrects packet transmit errors.
Layer 1: Physical layer network protocols	Interfaces between network medium and devices. Defines optical, electrical, and mechanical characteristics.

Though some say the OSI model is now redundant and less significant than the Transmission Control Protocol (TCP)/IP network model, there are still references to the OSI model even today as the model's structure helps to frame discussions of protocols and contrast various technologies.

Protocol suites & Industry Standards

Classification of network protocols

Now that you know how the OSI model works, you can dive straight into the classification of protocols. The following are some of the most prominent protocols used in network communication.

Application layer network protocols

1. DHCP: Dynamic Host Configuration Protocol

DHCP is a communication protocol that enables network administrators to automate the assignment of IP addresses in a network. In an IP network, every device connecting to the internet requires a unique IP. DHCP lets network admins distribute IP addresses from a central point and automatically send a new IP address when a device is plugged in from a different place in the network. DHCP works on a client-server model.

Advantages of using DHCP

Centralized management of IP addresses.

Seamless addition of new clients into a network.

Reuse of IP addresses, reducing the total number of IP addresses required.

Disadvantages of using DHCP

Tracking internet activity becomes tedious, as the same device can have multiple IP addresses over a period of time.

Computers with DHCP cannot be used as servers, as their IPs change over time.

2. DNS: Domain Name System protocol

The DNS protocol helps in translating or mapping host names to IP addresses. DNS works on a client-server model, and uses a distributed database over a hierarchy of name servers.

Hosts are identified based on their IP addresses, but memorizing an IP address is difficult due to its complexity. IPs are also dynamic, making it all the more necessary to map domain names to IP addresses. DNS helps resolve this issue by converting the domain names of websites into numerical IP addresses.

Advantages

DNS facilitates internet access.

Eliminates the need to memorize IP addresses.

Disadvantages

DNS queries don't carry information pertaining to the client who initiated it. This is because the DNS server only sees the IP from where the query came from, making the server susceptible to manipulation from hackers.

DNS root servers, if compromised, could enable hackers to redirect to other pages for phishing data.

3. FTP: File Transfer Protocol

File Transfer Protocol enables file sharing between hosts, both local and remote, and runs on top of TCP. For file transfer, FTP creates two TCP connections: control and data connection. The control connection is used to transfer control information like passwords, commands to retrieve and store files, etc., and the data connection is used to transfer the actual file. Both of these connections run in parallel during the entire file transfer process.

Advantages

- Enables sharing large files and multiple directories at the same time.
- Let’s you resume file sharing if it was interrupted.
- Let’s you recover lost data, and schedule a file transfer.

Disadvantages

- FTP lacks security. Data, usernames, and passwords are transferred in plain text, making them vulnerable to malicious actors.
- FTP lacks encryption capabilities, making it non-compliant with industry standards.

4. HTTP: Hyper Text Transfer Protocol

HTTP is an application layer protocol used for distributed, collaborative, and hypermedia information systems. It works on a client-server model, where the web browser acts as the client. Data such as text, images, and other multimedia files are shared over the World Wide Web using HTTP. As a request and response type protocol, the client sends a request to the server, which is then processed by the server before sending a response back to the client.

HTTP is a stateless protocol, meaning the client and server are only aware of each other while the connection between them is intact. After that, both the client and server forget about each other's existence. Due to this phenomenon, the client and server can't both retain information between requests.

Advantages

- Memory usage and CPU usage are low because of lesser concurrent connections.
- Errors can be reported without closing connections.
- Owing to lesser TCP connections, network congestion is reduced.

Disadvantages

- HTTP lacks encryption capabilities, making it less secure.
- HTTP requires more power to establish communication and transfer data.

5. IMAP and IMAP4: Internet Message Access Protocol (version 4)

IMAP is an email protocol that lets end users access and manipulate messages stored on a mail server from their email client as if they were present locally on their remote device. IMAP follows a client-server model, and lets multiple clients access messages on a common mail server concurrently. IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and removing flags; and much more. The current version of IMAP is version 4 revision 1.

Advantages

- As the emails are stored on the mail server, local storage utilization is minimal.
- In case of accidental deletion of emails or data, it is always possible to retrieve them as they are stored on the mail server.

Disadvantages

- Emails won't work without an active internet connection.
- High utilization of emails by end users requires more mailbox storage, thereby augmenting costs.

6. POP and POP3: Post Office Protocol (version 3)

The Post Office Protocol is also an email protocol. Using this protocol, the end user can download emails from the mail server to their own email client. Once the emails are downloaded locally, they can be read without an internet connection. Also, once the emails are moved locally, they get deleted from the mail server, freeing up space. POP3 is not designed to perform extensive manipulations with the messages on the mail server, unlike IMAP4. POP3 is the latest version of the Post Office Protocol.

Advantages

- Read emails on local devices without internet connection.
- The mail server need not have high storage capacity, as the emails get deleted when they're moved locally.

Disadvantages

If the local device on which the emails were downloaded crashes or gets stolen, the emails are lost.

7. SMTP: Simple Mail Transfer Protocol

SMTP is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a push protocol and is used to send the email, whereas POP and IMAP are used to retrieve emails on the end user's side. SMTP transfers emails between systems, and notifies on incoming emails. Using

SMTP, a client can transfer an email to another client on the same network or another network through a relay or gateway access available to both networks.

Advantages

- Ease of installation.
- Connects to any system without any restriction.
- It doesn't need any development from your side.

Disadvantages

- Back and forth conversations between servers can delay sending a message, and also increases the chance of the message not being delivered.
- Certain firewalls can block the ports used with SMTP.

8. Telnet: Terminal emulation protocol

Telnet is an application layer protocol that enables a user to communicate with a remote device. A Telnet client is installed on the user's machine, which accesses the command line interface of another remote machine that runs a Telnet server program.

Telnet is mostly used by network administrators to access and manage remote devices. To access a remote device, a network admin needs to enter the IP or host name of the remote device, after which they will be presented with a virtual terminal that can interact with the host.

Advantages

- Compatible with multiple operating systems.
- Saves a lot of time due to its swift connectivity with remote devices.

Disadvantages

- Telnet lacks encryption capabilities and sends across critical information in clear text, making it easier for malicious actors.
- Expensive due to slow typing speeds.

9. SNMP: Simple Network Management Protocol

SNMP is an application layer protocol used to manage nodes, like servers, workstations, routers, switches, etc., on an IP network. SNMP enables network admins to monitor network performance, identify network glitches, and troubleshoot them. SNMP protocol is comprised of three components: a managed device, an SNMP agent, and an SNMP manager.

The SNMP agent resides on the managed device. The agent is a software module that has local knowledge of management information, and translates that information into a form compatible with the SNMP manager. The SNMP manager presents the data obtained from the SNMP agent, helping network admins manage nodes effectively.

Currently, there are three versions of SNMP: SNMP v1, SNMP v2, and SNMP v3. Both versions 1 and 2 have many features in common, but SNMP v2 offers enhancements such as additional protocol operations. SNMP version 3 (SNMP v3) adds security and remote configuration capabilities to the previous versions.

Presentation layer network protocols

LPP: Lightweight Presentation Protocol

The Lightweight Presentation Protocol helps provide streamlined support for OSI application services in networks running on TCP/IP protocols for some constrained environments. LPP is designed for a particular class of OSI applications, namely those entities whose application context contains only an Association Control Service Element (ACSE) and a Remote Operations Service Element (ROSE). LPP is not applicable to entities whose application context is more extensive, i.e., contains a Reliable Transfer Service Element.

Session layer network protocols

RPC: Remote Procedure Call protocol

RPC is a protocol for requesting a service from a program in a remote computer through a network, and can be used without having to understand the underlying network technologies. RPC uses TCP or UDP for carrying the messages between communicating programs. RPC also works on client-server model. The requesting program is the client, and the service providing program is the server.

Advantages

- RPC omits many protocol layers to improve performance.
- With RPC, code rewriting or redeveloping efforts are minimized.

Disadvantages

- Not yet proven to work effectively over wide-area networks.
- Apart from TCP/IP, RPC does not support other transport protocols.

Transport layer network protocols

1. TCP: Transmission Control Protocol

TCP is a transport layer protocol that provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgement. TCP is a connection-oriented protocol, as it requires a connection to be established between applications before data transfer. Through flow control and acknowledgement of data, TCP provides extensive error checking. TCP ensures sequencing of data, meaning the data packets arrive in order at the receiving end. Retransmission of lost data packets is also feasible with TCP.

Advantages

- TCP ensures three things: data reaches the destination, reaches it on time, and reaches it without duplication.
- TCP automatically breaks data into packets before transmission.

Disadvantages

- TCP cannot be used for broadcast and multicast connections.

2. UDP: User Datagram Protocol

UDP is a connection-less transport layer protocol that provides a simple but unreliable message service. Unlike TCP, UDP adds no reliability, flow control, or error recovery functions. UDP is useful in situations where the reliability mechanisms of TCP are not necessary. Retransmission of lost data packets isn't possible with UDP.

Advantages

- Broadcast and multicast connections are possible with UDP.

- UDP is faster than TCP.

Disadvantages

- In UDP, it's possible that a packet may not be delivered, be delivered twice, or not be delivered at all.
- Manual disintegration of data packets is needed.

Network layer protocols

1. IP: Internet Protocol (IPv4)

IPv4 is a network layer protocol that contains addressing and control information, which helps packets be routed in a network. IP works in tandem with TCP to deliver data packets across the network. Under IP, each host is assigned a 32-bit address comprised of two major parts: the network number and host number. The network number identifies a network and is assigned by the internet, while the host number identifies a host on the network and is assigned by a network admin. The IP is only responsible for delivering the packets, and TCP helps puts them back in the right order.

Advantages

- IPv4 encrypts data to ensure privacy and security.
- With IP, routing data becomes more scalable and economical.

Disadvantages

- IPv4 is labor intensive, complex, and prone to errors.

2. IPv6: Internet Protocol version 6

IPv6 is the latest version of the Internet Protocol, a network layer protocol that possesses addressing and control information for enabling packets to be routed in the network. IPv6 was created to deal with IPv4 exhaustion. It increases the IP address size from 32 bits to 128 bits to support more levels of addressing.

Advantages

- More efficient routing and packet processing compared to IPv4.

- Better security compared to IPv4.

Disadvantages

- IPv6 is not compatible with machines that run on IPv4.
- Challenge in upgrading the devices to IPv6.

3. ICMP: Internet Control Message Protocol

ICMP is a network layer supporting protocol used by network devices to send error messages and operational information. ICMP messages delivered in IP packets are used for out-of-band messages related to network operation or disoperation. ICMP is used to announce network errors, congestion, and timeouts, as well assist in troubleshooting.

Advantages

- ICMP is used to diagnose network issues.

Disadvantages

- Sending a lot of ICMP messages increases network traffic.
- End users are affected if malicious users send many ICMP destination unreachable packets.

Data link layer network protocols

1. ARP: Address Resolution Protocol

The Address Resolution Protocol helps map IP addresses to physical machine addresses (or a MAC address for Ethernet) recognized in the local network. A table called an ARP cache is used to maintain a correlation between each IP address and its corresponding MAC address. ARP offers the rules to make these correlations, and helps convert addresses in both directions.

Advantages

- MAC addresses need not be known or memorized, as the ARP cache contains all the MAC addresses and maps them automatically with IPs.

Disadvantages

- ARP is susceptible to security attacks called ARP spoofing attacks.
- When using ARP, sometimes a hacker might be able to stop the traffic altogether. This is also known as ARP denial-of-services.

2. SLIP: Serial Line IP

SLIP is used for point-to-point serial connections using TCP/IP. SLIP is used on dedicated serial links, and sometimes for dial-up purposes. SLIP is useful for allowing mixes of hosts and routers to communicate with one another; for example, host-host, host-router, and router-router are all common SLIP network configurations. SLIP is merely a packet framing protocol: It defines a sequence of characters that frame IP packets on a serial line. It does not provide addressing, packet type identification, error detection or correction, or compression mechanisms.

Advantages

- Since it has a small overhead, it is suitable for usage in microcontrollers.
- It reuses existing dial-up connections and telephone lines.
- It's easy to deploy since it's based on the Internet Protocol.

Disadvantages

- SLIP doesn't support automatic setup of network connections in multiple OSI layers at the same time.
- SLIP does not support synchronous connections, such as a connection created through the internet from a modem to an internet service provider (ISP).

4.3. Layered Models

- By breaking the network communication process into manageable layers, the industry can benefit in the following ways:
- Defines common terms that describe the network functions to those working in the industry and Allows greater understanding and cooperation.
- Fosters competition because products from different vendors can work together.

- ❖ Provides a common language to describe networking functions and capabilities.
- ❖ Assists in protocol design, because protocols that operate at a specific layer, have defined

Information that they act upon and a defined interface to the layers above and below.

4.3. Layered Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

Layered Architecture

The main aim of the layered architecture is to divide the design into small pieces.

Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.

- ➢ It provides modularity and clear interfaces, i.e., provides interaction between subsystems.

It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.

The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.

The basic elements of layered architecture are services, protocols, and interfaces.

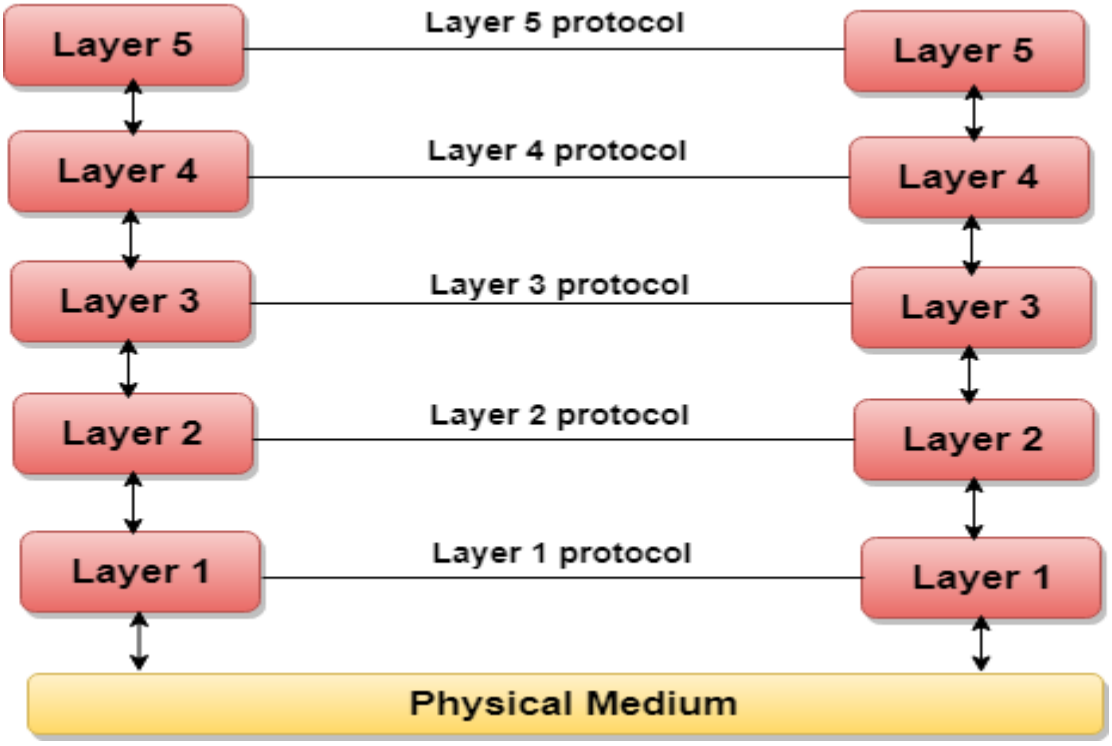
Service: It is a set of actions that a layer provides to the higher layer.

Protocol: It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.

Interface: It is a way through which the message is transferred from one layer to another layer.

In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

Let's take an example of the five-layered architecture.



In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.

Below layer 1 is the physical medium through which the actual communication takes place.

In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.

The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among

different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.

A set of layers and protocols is known as network architecture.

4.3.1. The TCP/IP Model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Internet Layer

- ✓ An internet layer is the second layer of the TCP/IP model.
- ✓ An internet layer is also known as the network layer.
- ✓ The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

IP Addressing: This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.

Host-to-host communication: It determines the path through which the data is to be transmitted.

Data Encapsulation and Formatting: An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

Fragmentation and Reassembly: The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.

Routing: When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

ARP stands for **Address Resolution Protocol**.

ARP is a network layer protocol which is used to find the physical address from the IP address.

The two terms are mainly associated with the ARP Protocol:

ARP request: When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

ARP reply: Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

ICMP stands for Internet Control Message Protocol.

It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

An ICMP protocol mainly uses two terms:

ICMP Test: ICMP Test is used to test whether the destination is reachable or not.

ICMP Reply: ICMP Reply is used to check whether the destination device is responding or not.

The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.

ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

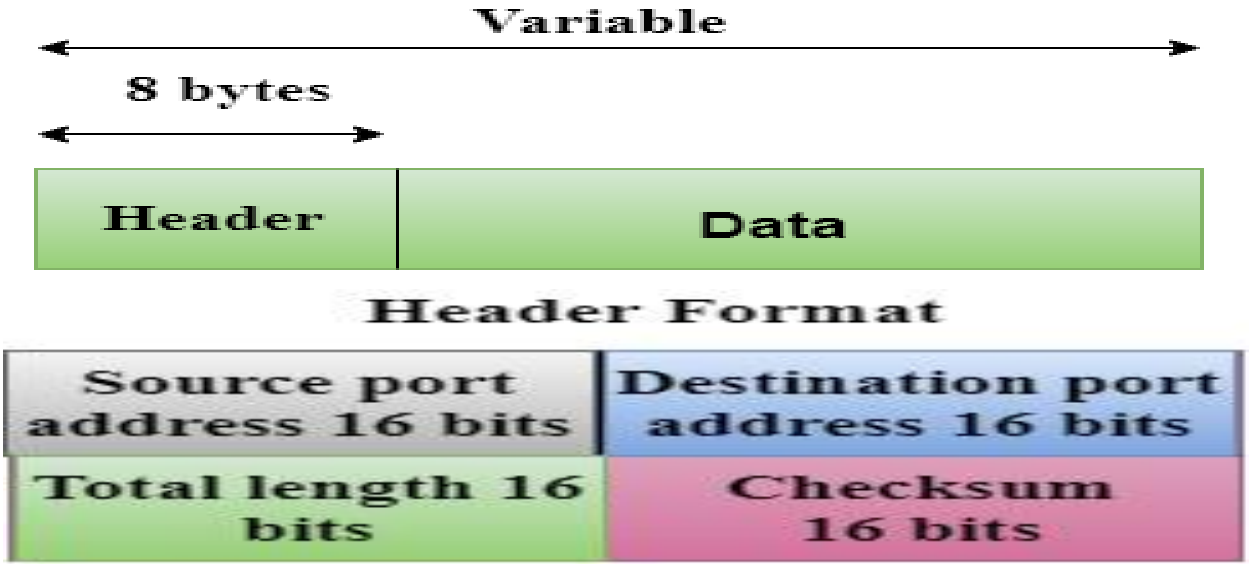
UDP consists of the following fields:

Source port address: The source port address is the address of the application program that has created the message.

Destination port address: The destination port address is the address of the application program that receives the message.

Total length: It defines the total number of bytes of the user datagram in bytes. **Checksum:** The checksum is a 16-bit field used in error detection.

UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- ✓ An application layer is the topmost layer in the TCP/IP model.
- ✓ It is responsible for handling high-level protocols, issues of representation.
- ✓ This layer allows the user to interact with the application.
- ✓ When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- ✓ There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

HTTP: HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

SNMP: SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

SMTP: SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

DNS: DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

TELNET: It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

FTP: FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer

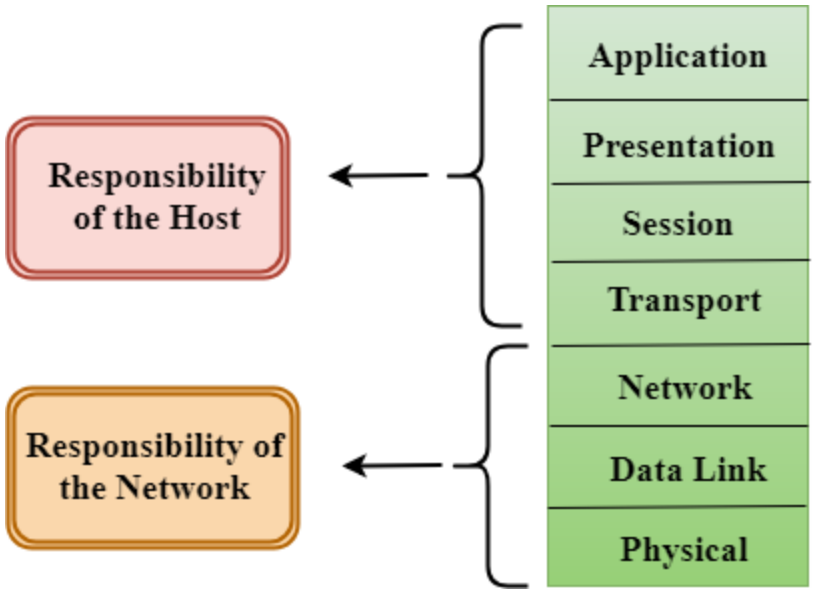
4.3.2. The OSI Model

OSI Model

OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

- ✓ OSI consists of seven layers, and each layer performs a particular network function.
- ✓ OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- ✓ OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- ✓ Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



The OSI model is divided into two layers: upper layers and lower layers.

The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

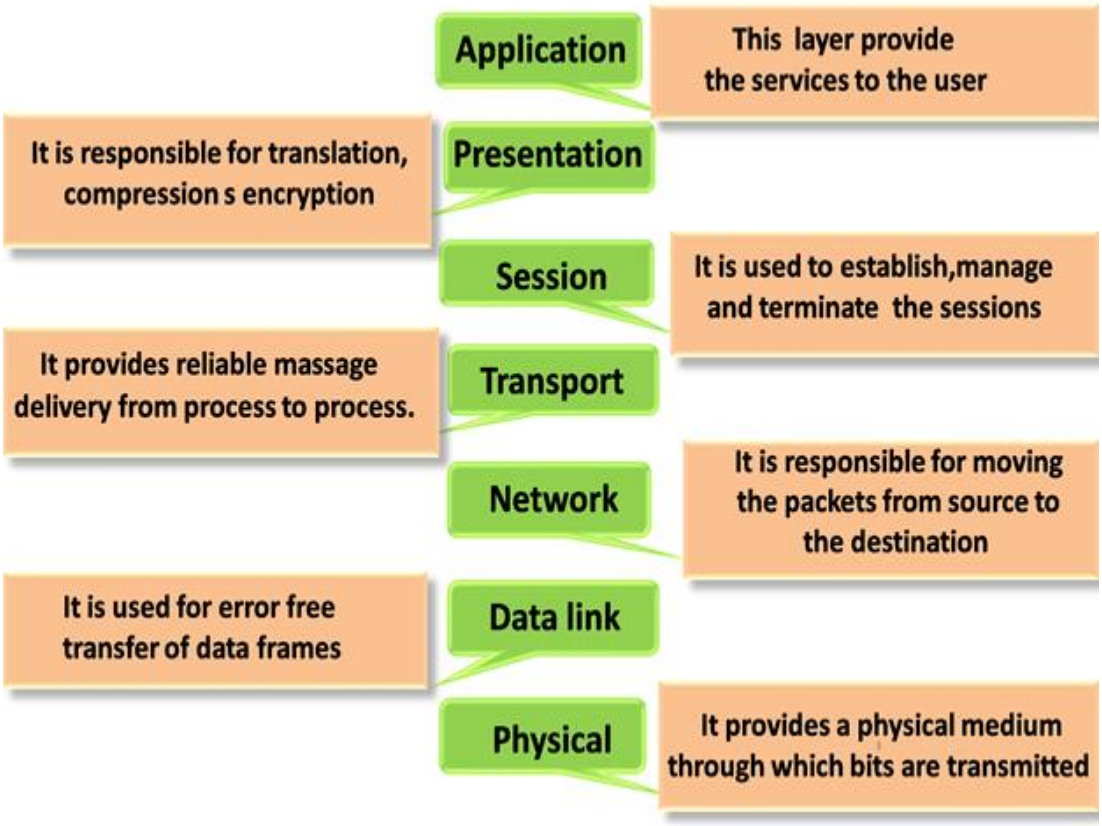
The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers

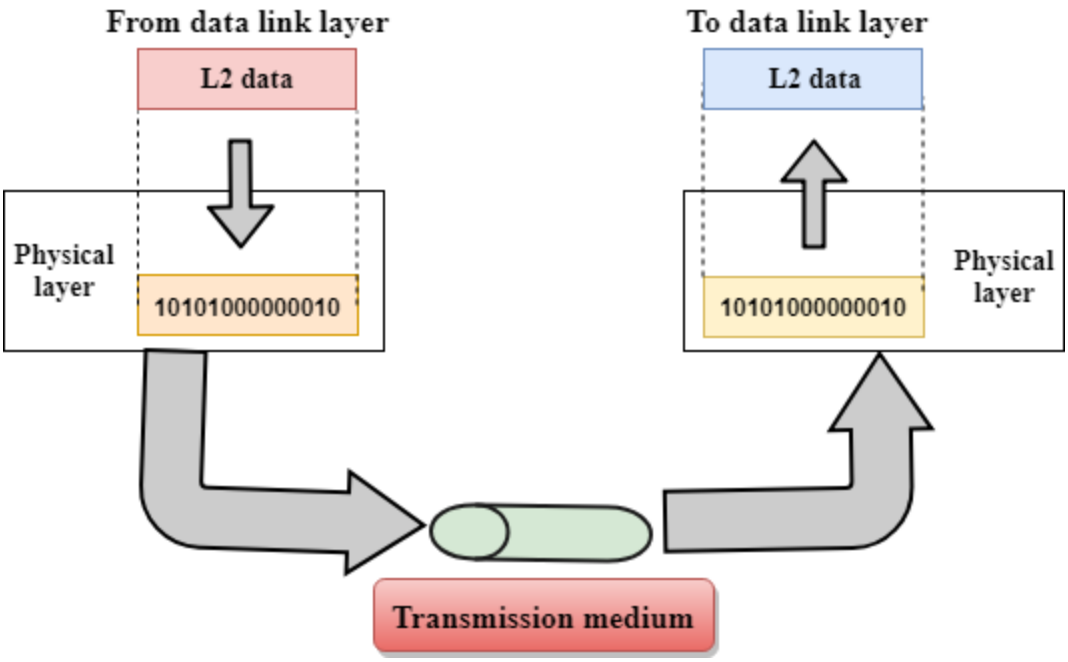
There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

- ✓ Physical Layer
- ✓ Data-Link Layer
- ✓ Network Layer
- ✓ Transport Layer
- ✓ Session Layer
- ✓ Presentation Layer

- ✓ Application Layer



Physical layer



The main functionality of the physical layer is to transmit the individual bits from one node to another node.

- ✓ It is the lowest layer of the OSI model.
- ✓ It establishes, maintains and deactivates the physical connection.
- ✓ It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

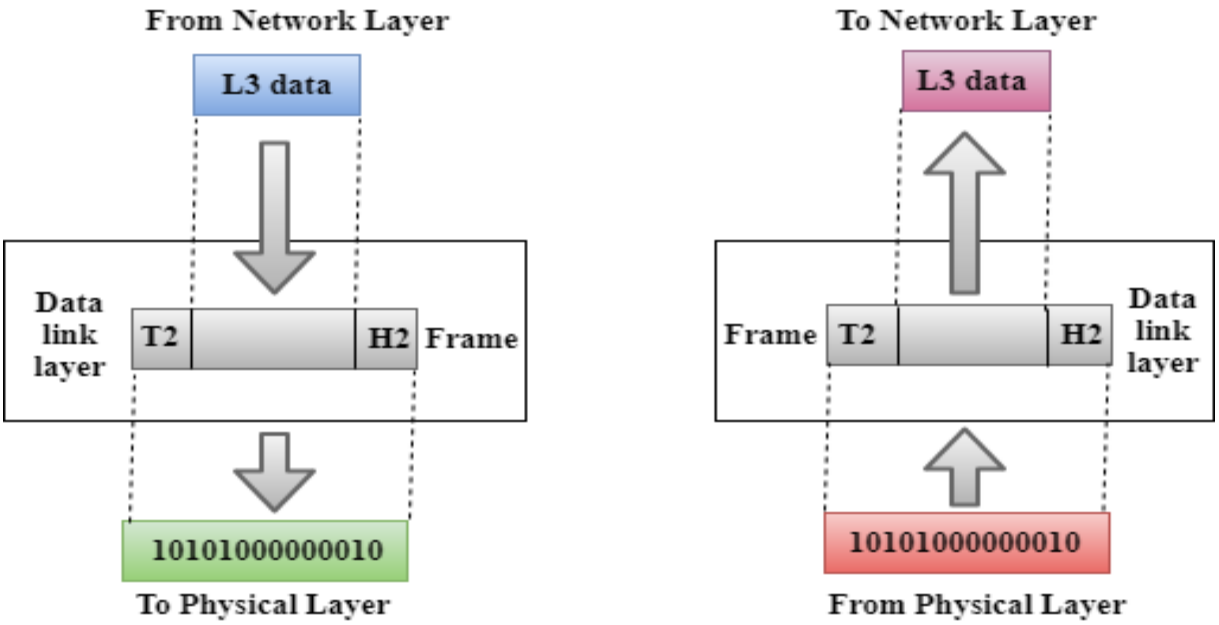
Line Configuration: It defines the way how two or more devices can be connected physically.

Data Transmission: It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

Topology: It defines the way how network devices are arranged.

Signals: It determines the type of the signal used for transmitting the information.

Data-Link Layer



This layer is responsible for the error-free transfer of data frames.

- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:

Logical Link Control Layer

- It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
- It identifies the address of the network layer protocol from the header.
- It also provides flow control.

Media Access Control Layer

- A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
- It is used for transferring the packets over the network.

Functions of the Data-link layer

Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

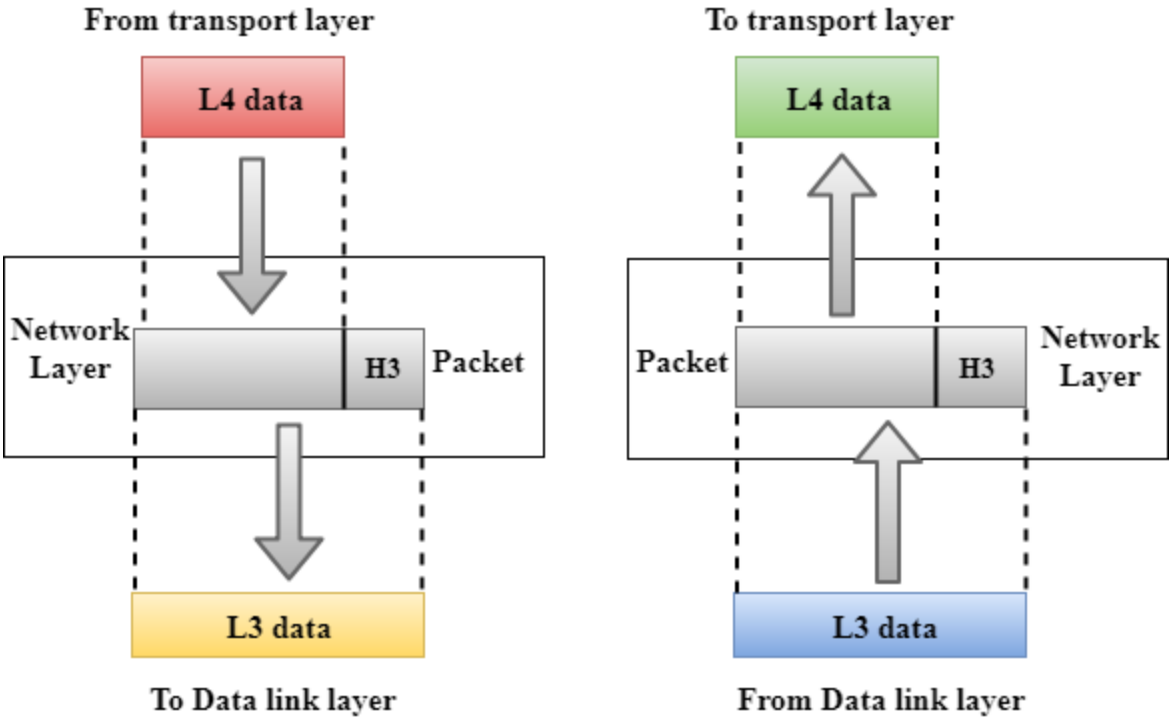
Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.

Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer



- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

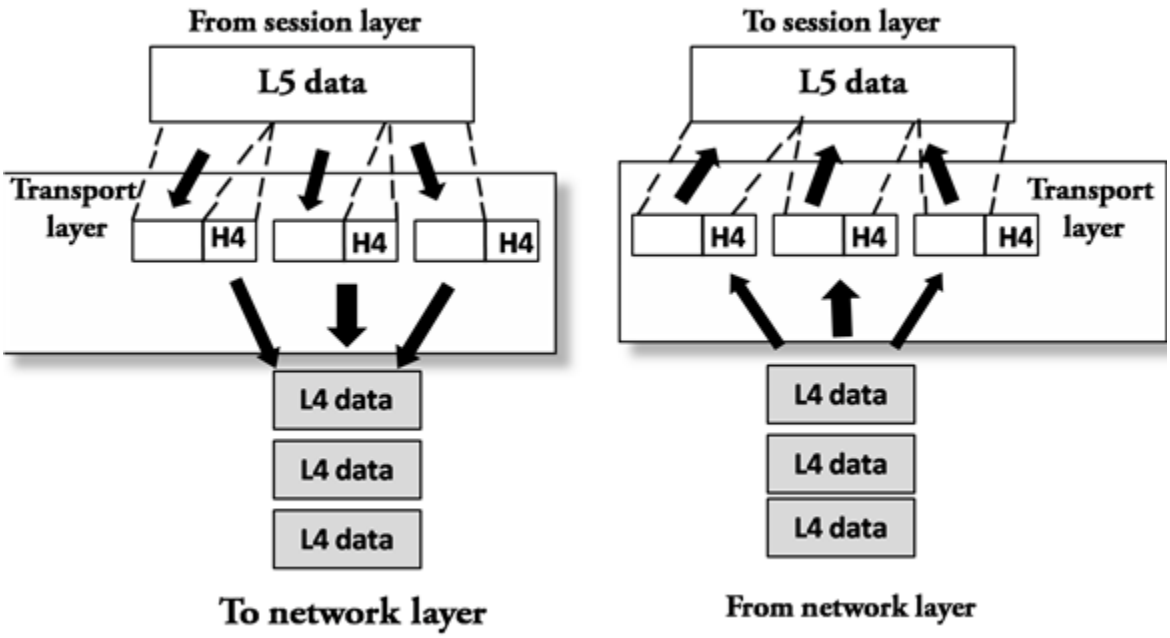
Internetworking: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.

Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

Packetizing: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

Transmission Control Protocol

- It is a standard protocol that allows the systems to communicate over the internet.
- It establishes and maintains a connection between hosts.

When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

User Datagram Protocol

- User Datagram Protocol is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

Service-point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

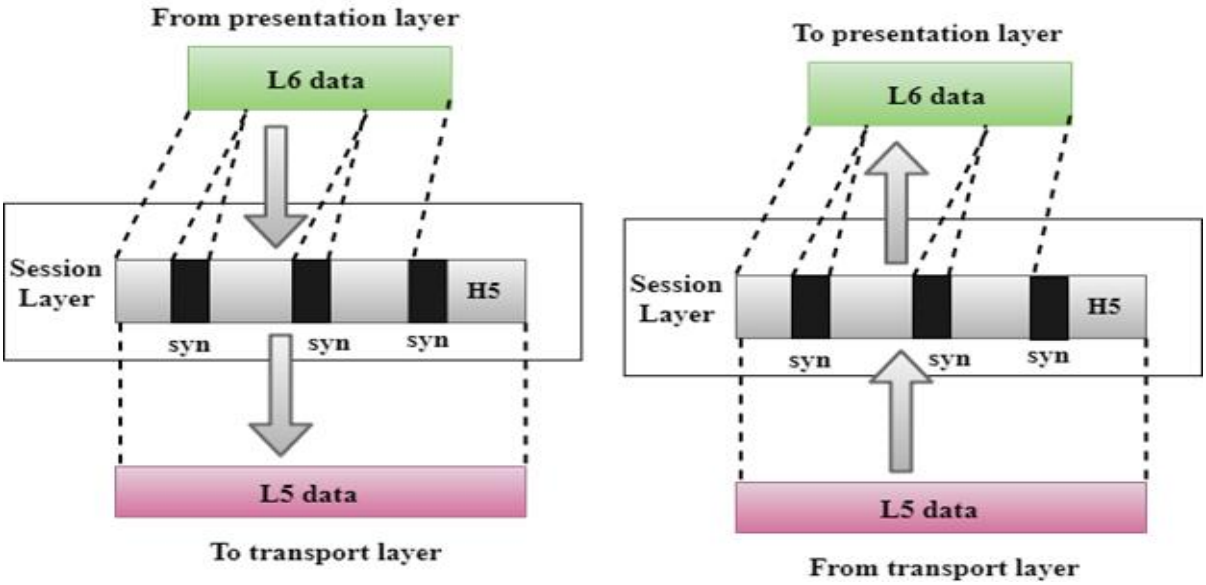
Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a

connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

Flow control: The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer



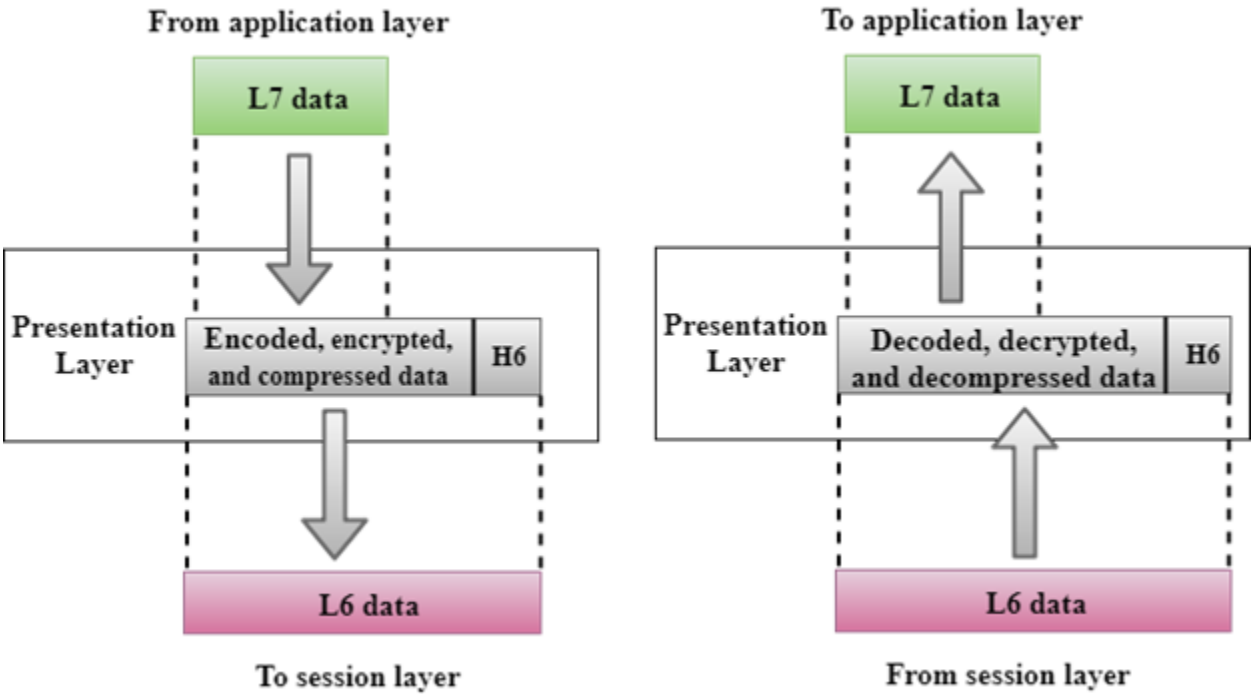
- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer



- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

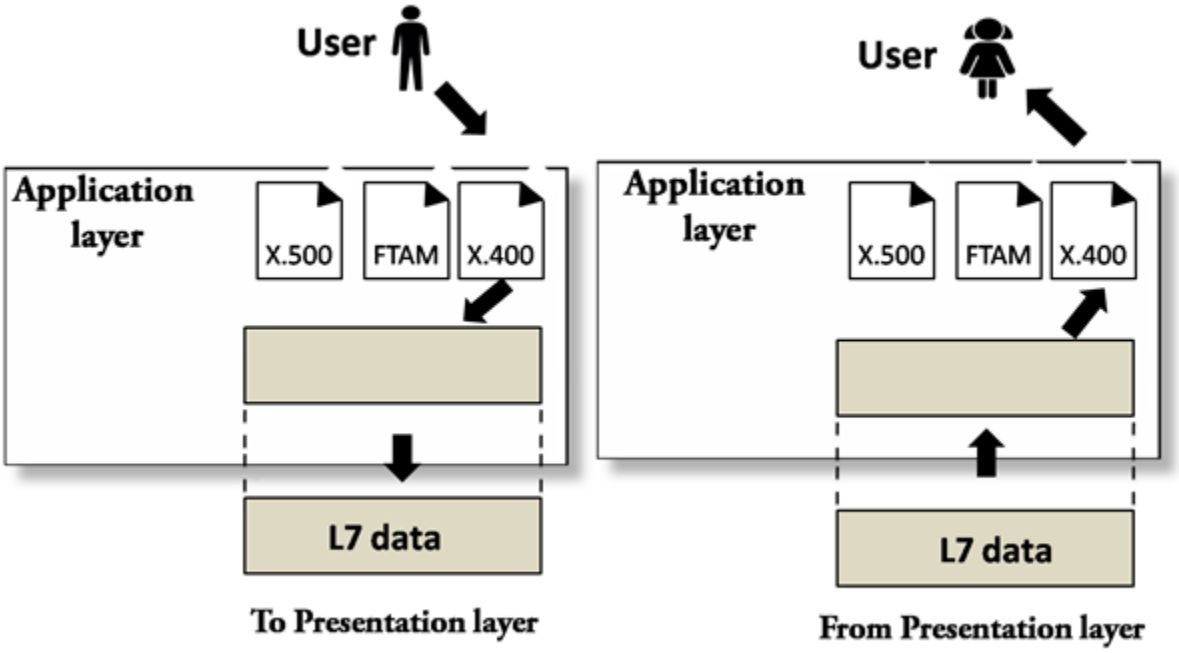
Translation: The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data

from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

Encryption: Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

Compression: Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

File transfer, access, and management (FTAM): An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

Mail services: An application layer provides the facility for email forwarding and storage.

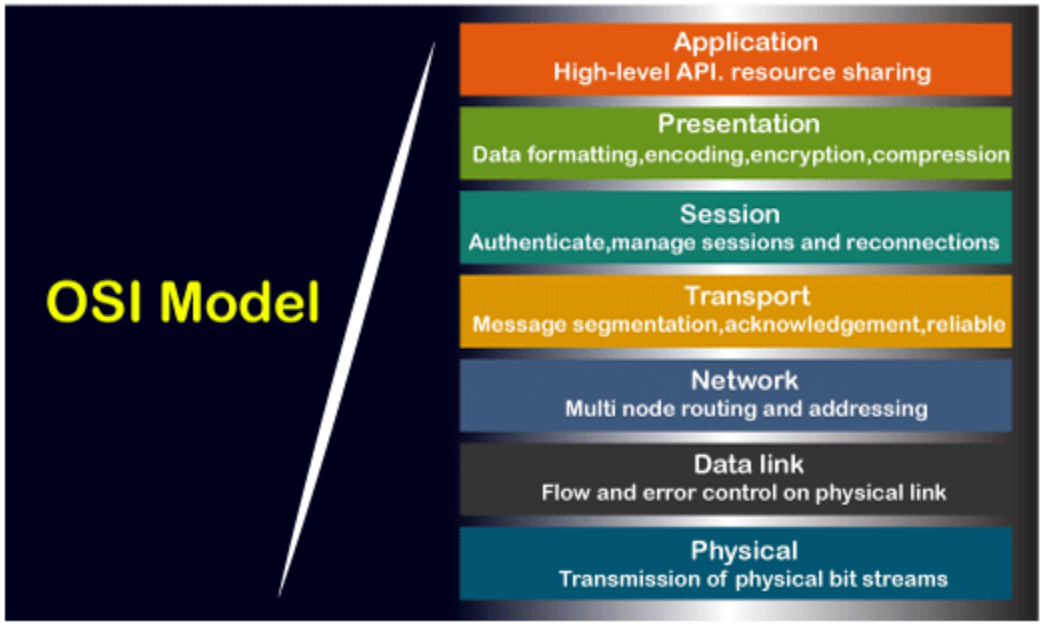
Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

4.3.3. Comparing OSI Model with TCP/IP Model

OSI vs TCP/IP

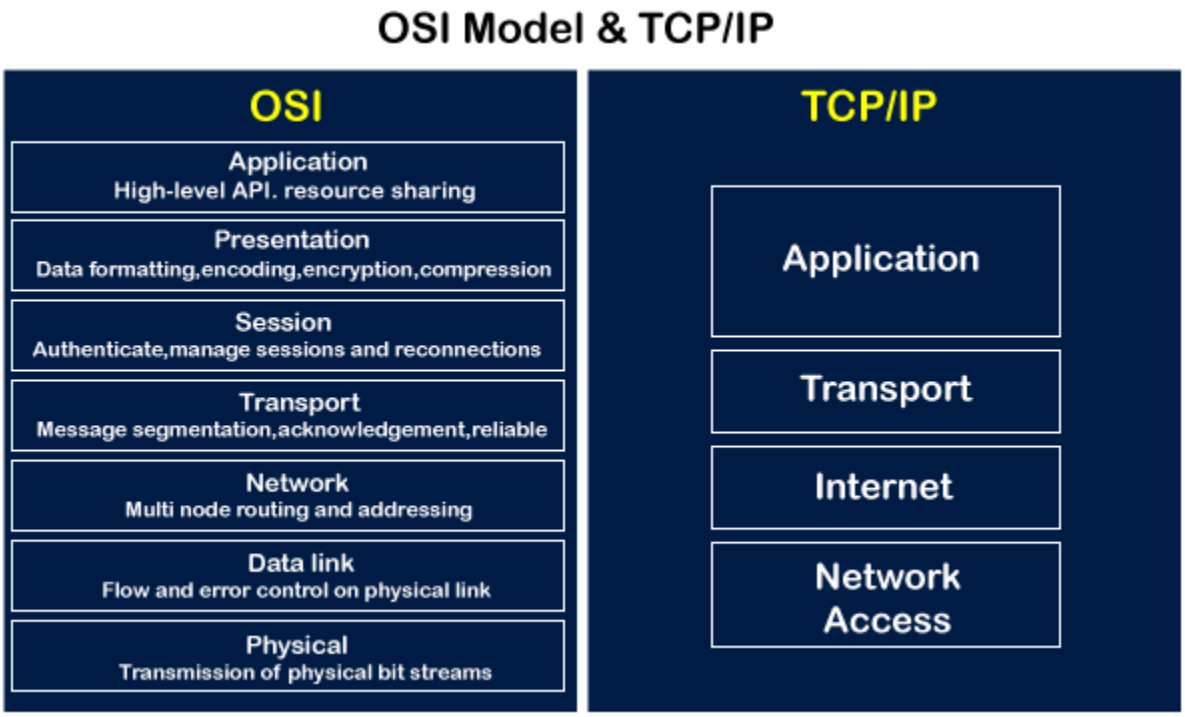
What is OSI model?

The OSI stands for Open System Interconnection, which was developed in 1980s. It is a conceptual model used for network communication. It is not implemented entirely, but it is still referenced today. This OSI model consists of seven layers, and each layer is connected to each other. The data moves down the OSI model, and each layer adds additional information. The data moves down until it reaches the last layer of the OSI model. When the data is received at the last layer of the OSI model, then the data is transmitted over the network. Once the data is reached on the other side, then the process will get reversed.



What is TCP/IP model?

The TCP model stands for **Transmission Control Protocol,** whereas IP stands for **Internet Protocol**. A number of protocols that make the internet possibly comes under the TCP/IP model. Nowadays, we do not hear the name of the TCP/IP model much, we generally hear the name of the IPv4 or IPv6, but it is still valid. This model consists of 4 layers. Now, we will look at the diagrammatic representation of the TCP/IP model.



As shown in the above diagram, the TCP/IP model has 4 layers, while the OSI model consists of 7 layers. Diagrammatically, it looks that the 4 layers of the TCP/IP model exactly fit the 7 layers of the OSI model, but this is not reality. The application layer of the TCP/IP model maps to the first three layers, i.e., application, session, and presentation layer of the OSI model. The transport layer of the TCP maps directly to the transport layer of the OSI model. The internet layer of the TCP/IP model maps directly to the network layer of the OSI model. The last two layers of the OSI model map to the network layer of the TCP/IP model. TCP/IP is the most widely used model as compared to the OSI model for providing communication between computers over the internet.

Similarities between the OSI and TCP/IP model

The following are the similarities between the OSI and TCP/IP model:

Share common architecture

Both the models are the logical models and having similar architectures as both the models are constructed with the layers.

Define standards

Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.

Simplified troubleshooting process

Both models have simplified the troubleshooting process by breaking the complex function into simpler components.

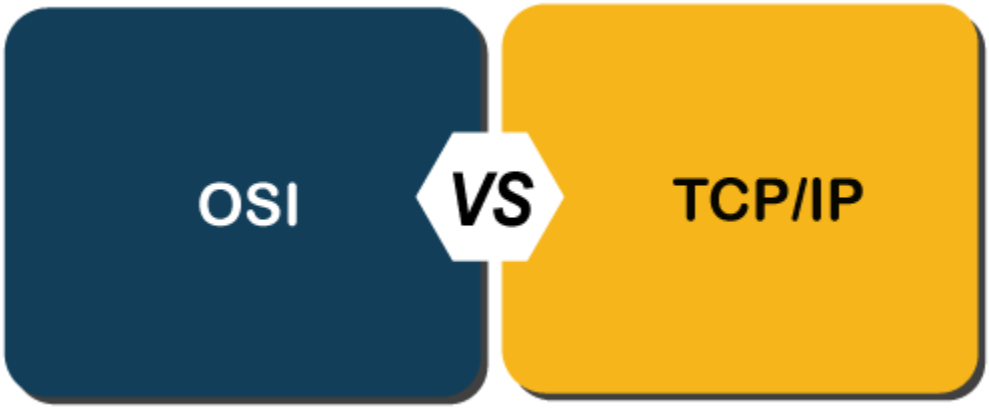
Pre-defined standards

The standards and protocols which are already pre-defined; these models do not redefine them; they just reference or use them. For example, the Ethernet standards were already defined by the IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.

Both have similar functionality of 'transport' and 'network' layers

The function which is performed between the **'presentation'** and the **'network'** layer is similar to the function performed at the **transport** layer.

Differences between the OSI and TCP/IP model



Let's see the differences between the OSI and TCP/IP model in a tabular form:

OSI Model	TCP/IP Model
It stands for **Open System Interconnection.**	It stands for **Transmission Control Protocol.**
OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).
It is an independent standard and generic protocol used as a communication gateway between the network and the end	It consists of standard protocols that lead to the development of an Internet. It is a communication protocol that provides the connection Among the hosts.

user.	
In the OSI model, the transport layer provides a guarantee for the delivery of the packets.	The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.
This model is based on a vertical approach.	This model is based on a horizontal approach.
In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool.	It is an implemented model of an OSI model.
In this model, the network layer provides both connection-	The network layer provides only connectionless service.

oriented and connectionless service.	
Protocols in the OSI model are hidden and can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.
It consists of 7 layers.	It consists of 4 layers.
OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.	In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.
The usage of this model is very low.	This model is highly used.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.

Chapter 5:

OSI Reference Model

The Open Systems Interconnection (OSI) model was developed by the International Organization for Standardization (ISO), and formalized in 1984. It provided the first framework governing how information should be sent across a network.

5.1. Layered Framework of OSI

The OSI model consists of seven layers, each corresponding to a specific network function:

- Application
- Presentation
- Session
- Transport
- Network
- Data-link
- Physical

Note that the bottom layer is Layer 1. Various mnemonics make it easier to remember the order of the OSI model's layers:

7 Application	All	Away
6 Presentation	People	Pizza
5 Session	Seem	Sausage
4 Transport	To	Throw
3 Network	Need	Not
2 Data-link	Data	Do
1 Physical	Processing	Please

ISO further developed an entire protocol suite based on the OSI model; however, the OSI protocol suite was never widely implemented.

The OSI model itself is now somewhat deprecated – modern protocol suites, such as the TCP/IP suite, are difficult to fit cleanly within the OSI model's seven layers. This is especially true of the upper three layers.

The bottom (or lower) four layers are more clearly defined, and terminology from those layers is still prevalently used. Many protocols and devices are described by which lower layer they operate at.

OSI Model - The Upper Layers

The top three layers of the OSI model are often referred to as the upper layers:

- Layer-7 - Application layer
- Layer-6 - Presentation layer
- Layer-5 - Session layer

Protocols that operate at these layers manage application-level functions, and are generally implemented in software.

The function of the upper layers of the OSI model can be difficult to visualize. Upper layer protocols do not always fit perfectly within a layer, and often function across multiple layers.

5.2. Overview & functions of each layer

OSI Model - The Application Layer

The Application layer (Layer-7) provides the interface between the user application and the network. A web browser and an email client are examples of user applications.

The user application itself does not reside at the Application layer - the protocol does. The user interacts with the application, which in turn interacts with the application protocol.

Examples of Application layer protocols include:

- FTP, via an FTP client
- HTTP, via a web browser
- POP3 and SMTP, via an email client

Telnet

The Application layer provides a variety of functions:

- Identifies communication partners
- Determines resource availability
- Synchronizes communication

The Application layer interacts with the Presentation layer below it. As it is the top-most layer, it does not interact with any layers above it.

OSI Model - The Presentation Layer

The Presentation layer (Layer-6) controls the formatting and syntax of user data for the application layer. This ensures that data from the sending application can be understood by the receiving application.

Standards have been developed for the formatting of data types, such as text, images, audio, and video.

Examples of Presentation layer formats include:

- Text - RTF, ASCII, EBCDIC
- Images - GIF, JPG, TIF
- Audio - MIDI, MP3, WAV
- Movies - MPEG, AVI, MOV

If two devices do not support the same format or syntax, the Presentation layer can provide conversion or translation services to facilitate communication.

Additionally, the Presentation layer can perform encryption and compression of data, as required. However, these functions can also be performed at lower layers as well. For example, the Network layer can perform encryption, using IPSec.

OSI Model - The Session Layer

The Session layer (Layer-5) is responsible for establishing, maintaining, and ultimately terminating sessions between devices. If a session is broken, this layer can attempt to recover the session.

Sessions communication falls under one of three categories:

- Full-Duplex – simultaneous two-way communication
- Half-Duplex – two-way communication, but not simultaneous
- Simplex – one-way communication

Many modern protocol suites, such as TCP/IP, do not implement Session layer protocols. Connection management is often controlled by lower layers, such as the Transport layer.

The lack of true Session layer protocols can present challenges for highavailability and failover. Reliance on lower-layer protocols for session management offers less flexibility than a strict adherence to the OSI model.

OSI Model - The Lower Layers

The bottom four layers of the OSI model are often referred to as the lower layers:

- Layer-4 – Transport layer
- Layer-3 – Network layer
- Layer-2 – Data-Link layer
- Layer-1 – Physical layer

Protocols that operate at these layers control the end-to-end transport of data between devices, and are implemented in both software and hardware.

OSI Model - The Transport Layer

The Transport layer (Layer-4) does not actually send data, despite its name. Instead, this layer is responsible for the reliable transfer of data, by ensuring that data arrives at its destination error-free and in order.

Transport layer communication falls under two categories:

Connection-oriented – requires that a connection with specific agreed-upon parameters be established before data is sent.

Connectionless – requires no connection before data is sent.

Connection-oriented protocols provide several important services:

Segmentation and sequencing – data is segmented into smaller pieces for transport. Each segment is assigned a sequence number, so that the receiving device can reassemble the data on arrival.

Connection establishment – connections are established, maintained, and ultimately terminated between devices.

Acknowledgments – receipt of data is confirmed through the use of acknowledgments. Otherwise, data is retransmitted, guaranteeing delivery.

Flow control (or windowing) – data transfer rate is negotiated to prevent congestion.

The TCP/IP protocol suite incorporates two Transport layer protocols:

Transmission Control Protocol (TCP) – connection-oriented

User Datagram Protocol (UDP) – connectionless

OSI Model - The Network Layer

The Network layer (Layer-3) controls internetwork communication, and has two key responsibilities:

Logical addressing – provides a unique address that identifies both the host, and the network that host exists on.

Routing – determines the best path to a particular destination network, and then routes data accordingly.

Two of the most common Network layer protocols are:

Internet Protocol (IP)

Novell's Internetwork Packet Exchange (IPX).

IPX is almost entirely deprecated. IP version 4 (IPv4) and IP version 6 (IPv6) are covered in nauseating detail in other guides.

OSI Model - The Data-Link Layer

While the Network layer is concerned with transporting data between networks, the Data-Link layer (Layer-2) is responsible for transporting data within a network.

The Data-Link layer consists of two sublayers:

- Logical Link Control (LLC) sublayer
- Media Access Control (MAC) sublayer

The LLC sublayer serves as the intermediary between the physical link and all higher layer protocols. It ensures that protocols like IP can function regardless of what type of physical technology is being used.

Additionally, the LLC sublayer can perform flow-control and errorchecking, though such functions are often provided by Transport layer protocols, such as TCP.

The MAC sublayer controls access to the physical medium, serving as mediator if multiple devices are competing for the same physical link. Datalink layer technologies have various methods of accomplishing this - Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD), and Token Ring utilizes a token.

OSI Model - The Data-Link Layer (continued)

The Data-link layer packages the higher-layer data into frames, so that the data can be put onto the physical wire. This packaging process is referred to as framing or encapsulation.

The encapsulation type will vary depending on the underlying technology. Common Data-link layer technologies include following:

Ethernet – the most common LAN data-link technology

Token Ring – almost entirely deprecated

FDDI (Fiber Distributed Data Interface)

802.11 Wireless

Frame-Relay

ATM (Asynchronous Transfer Mode)

The data-link frame contains the source and destination hardware (or physical) address. Hardware addresses uniquely identify a host within a network, and are often hardcoded onto physical network interfaces. However, hardware addresses contain no mechanism for differentiating one network from another, and can only identify a host within a network.

The most common hardware address is the Ethernet MAC address.

OSI Model - The Physical Layer

The Physical layer (Layer-1) controls the signaling and transferring of raw bits onto the physical medium. The Physical layer is closely related to the Data-link layer, as many technologies (such as Ethernet) contain both datalink and physical functions.

The Physical layer provides specifications for a variety of hardware:

- Cabling
- Connectors and transceivers
- Network interface cards (NICs)
- Wireless radios
- Hubs Physical-layer devices and topologies are covered extensively in other guides.

Chapter 6

Switching & Multiplexing

6.1. Switching Concept and Types

Switching

Fully connected networks don't scale well, but you still need to let any possible pair of nodes communicate.

Switching is the idea that you can dynamically configure a network which is less than fully connected in order to join any two nodes for communication.Two ways to switch: you can establish your own dedicated path (circuit switching) or you can take whatever path is available at the time you send data (packet switching).

Circuit switching

Circuit switching maintains the idea of dedicated connections between two end points, but allows for sharing of channels within the network, and hence is much more saleable.

Circuit switching takes advantage of the fact that while everybody needs to be able to talk to everybody else, they aren't likely to all do so at the same time.

The telephone network is based on circuit switching. To make a phone call you ask the PSTN to establish a dedicated circuit for you. It does this by finding unused channels all along the way through the network and dedicates them to your call. When you actually start exchanging data (talking) all of your data follows the same path or circuit through the network. If you pause in your conversation the circuit you're using is idle, wasting bandwidth. But you never lose data because you have a guaranteed, reserved circuit, so it is impossible for the system to be too busy to handle your data.

6.2. Multiplexing Concepts and Types

Multiplexing and De-multiplexing

- To combine multiple signals (analog or digital) for transmission over a single line or media.
- A common type of multiplexing combines several low-speed signals for transmission over a single high-speed connection.
- Multiplexing is done by using a device called Multiplexer (MUX) that combines n input lines to generate one output line i.e. (many to one). Therefore multiplexer (MUX) has several inputs and one output.
- At the receiving end, a device called DE multiplexer (DEMUX) is used that separates signal into its component signals. So DEMUX has one input and several outputs.

Concept of Multiplexing

- Input lines and diverts them to single output line.
- The signal from 4 different devices is combined and carried by this single line.
- At the receiving side, a DE multiplexer takes this signal from a single line & breaks it into the original signals and passes them to the 4 different receivers.

Advantages of Multiplexing

- If no multiplexing is used between the users at two different sites that are distance apart, then separate communication lines would be required.
- This is not only costly but also become difficult to manage. If multiplexing is used then, only one line is required. This leads to the reduction in the line cost and also it would be easier to keep track of one line than several lines.
- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

Why to use Multiplexing?

• If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth.

• For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.

• When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.

Types of Multiplexing

Frequency Division Multiplexing (FDM)

- Frequency-Division Multiplexing (FDM) is a scheme in which numerous signals are combined for transmission on a single communications line or channel.
- It is analog technique. Each signal is assigned a different frequency (sub channel) within the main channel.
- FDM requires that the bandwidth of a link should be greater than the combined bandwidths of the various signals to be transmitted. Thus each signal having different frequency forms a particular logical channel on the link and follows this channel only. These channels are then separated by the strips of unused bandwidth called guard bands.
- In FDM, signals to be transmitted must be analog signals. Thus digital signals need to be converted to analog form, if they are to use FDM.
- A typical analog Internet connection via a twisted pair telephone line requires approximately three kilohertz (3 kHz) of bandwidth for accurate and reliable data transfer.
- Twisted-pair lines are common in households and small businesses. But major telephone cables, operating between large businesses, government agencies, and municipalities, are capable of much larger bandwidths.

FDM Process

In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link.

- Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal.
- These bandwidth ranges are the channels through which the various signals travel.
- Channels can be separated by strips of unused bandwidth guard bands to prevent signals from overlapping.

Wavelength-Division Multiplexing

- Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber-optic cable.
- The optical fiber data rate is higher than the data rate of metallic transmission cable, but using a fiber-optic cable for a single line wastes the available bandwidth.
- WDM is conceptually the same as FDM, except that the multiplexing and DE multiplexing involve optical signals transmitted through fiber-optic channels. The difference is that the frequencies are very high.
- WDM is an analog multiplexing technique.
- In WDM different signals are optical or light signals that are transmitted through optical fiber.

Time Division Multiplexing (TDM):

- TDM is the digital multiplexing technique.
- In TDM, the channel/link is divided on the basis of time.
- Total time available in the channel is divided between several users. Each user is allotted a particular a time interval called time slot or time slice during which the data is transmitted by that user.
- Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time.
- Each user is allotted a particular time interval called time slot or slice.
- In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices.
- All the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one. Thus each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel.
- The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing.
- The TDM signal in the form of frames is transmitted on the common communication medium

Chapter 7

7. Introduction to IP Addressing and Subnetting

An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

- IP Address is a unique identification given to Host, network device, server for data communication.
- IP Address stand for Internet Protocol address, it is an addressing scheme used to identify a system on a network.
- It is a unique address that certain electronic devices currently use to communicate with each other on a network using internet protocol.
- IPV4 is a 32 bit number represented in 4 decimal numbers, where each decimal number is of 8 bit (an octet), where each octet is separated by a dot in between. Thus the representation is known as Dotted Decimal Notation. An IPV4 address is divided into 2 parts with Network ID and Host ID. It allows 232 addresses.
- IPV4 has Unicast, Broadcast & Multicast addresses. Routing Protocols that supports IPV4 addressing are RIPV1, V2, IGRP, OSPF & EIGRP.

Two device on the internet can never have the same address at the same time.

- A protocol such as IPv4 that defines address has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses N bits to define an address space is 2N because each bit can have two different values (0 or 1) and N bits can have 2N values
- IPv4 uses a 32 bit address, which means the address space is 232 or 4,294,967,296.

IP Addressing

There are four forms of IP addressing, each with its own unique properties.

1. **Unicast:** The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. E It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. E Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient

2. **Broadcast:** In IPv4 it is possible to send data to all possible destinations ("all-hosts broadcast"), which permits the sender to send the data only once, and all receivers receive a copy of it.

3. **Multicast**: A multicast address is associated with a group of interested receivers.

4. **Any cast:** Like broadcast and multicast, any cast is a one-to-many routing topology. However, the data stream is not transmitted to all receivers, just the one which the router decides is logically closest in the network.

7.1 Classful & Classless Addressing

Classful IP Addressing

- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.
- Each class occupies some part of the address space
- We can find the class of an address
- When given the address in binary notation the first few bits can be immediately tell us the class of the address
- If the address is given in dotted decimal notation , the first byte describes the class Systems that have interfaces to more than one network require a unique IP address for each network interface.
- The first part of an Internet address identifies the network on which the host resides.
- The second part identifies the particular host on the given network

Class A Networks (/8 Prefix)

- Each Class A network address has an 8-bit network prefix, with thehighest order bit set to 0 (zero) and a 7-bit network number, followed by a 24-bit host number.
- Today, Class A networks are referred to as "/8s" (pronounced "slash eight" or just "eights") since they have an 8- bit network prefix.
- A maximum of 126 (2 7-2) /8 networks can be defined.
- The calculation subtracts two because the /8 network 0.0.0.0 is reserved for use as the default route and the /8 network 127.0.0.0 (also written 127/8 or 127.0.0.0/8) is reserved for the "loopback" function.
- Each /8 supports a maximum of 2 24 -2 (16,777,214) hosts per network. The host calculation subtracts two because the all-0s (all zeros or "this network") and all-1s (all ones or "broadcast") host numbers may not be assigned to individual hosts.
- Since the /8 address block contains 2 31 (2,147,483,648) individual addresses and the IPv4 address space contains a maximum of 2 32 (4,294,967,296) addresses, the /8 address space is 50 percent of the total IPv4 unicast address space.

Class B Networks (/16 Prefixes)

- Each Class B network address has a 16-bit network prefix, with the two highest order bits set to 1-0 and a 14-bit network number, followed by a 16- bit host number.
- Class B networks are now referred to as "/16s" since they have a 16-bit network prefix.
- A maximum of 16,384 (2 14) /16 networks can be defined with up to 65,534 (216-2) hosts per network. Since the entire /16 address block contains 230 (1,073,741,824) addresses, it represents 25 percent of the total IPv4 unicast address space.

Class C Networks (/24 Prefixes)

- Each Class C network address has a 24-bit network prefix, with the three highest order bits set to 1-1-0 and a 21-bit network number, followed by an 8-bit host number.
- Class C networks are now referred to as "/24s" since they have a 24-bit network prefix.

- A maximum of 2,097,152 (2 21) /24 networks can be defined with up to 254 (28-2) hosts per network. Since the entire /24 address block contains 229 (536,870,912) addresses, it represents 12.5 percent (or 1/18 th) of the total IPv4 unicast address space.

Class D Networks

- Class D network addresses are not assigned to devices on a network.
- These addresses are used for special-purpose, multicast applications (such as video and audio-streaming applications).
- These addresses all need to be registered with IANA to be used globally.
- Addresses in this class have the first bits of the first octet set to 1110, yielding addresses in the first octet ranging from 11100000 to 11101111, or 224 to 239.
- These addresses are not defined by a normal subnet mask; instead, each address is used for a specific purpose. And because each address is individually used, it uses a 255.255.255.255 mask. 20

Class E Networks

- If Class D is special, Class E addresses are even more special.
- There is no defined use for this address class.
- Officially, it is listed as reserved for usage and testing by IANA and the Internet Research Task Force (IRTF). In fact, as of RFC3330 in 2002, Class E was updated to "reserved for future use."
- Class E comprises absolutely all valid addresses with 240 or higher in the first octet.
- The first bits of the first octet is 1111, which yields addresses from 11110000 to 11111110 — or technically, 11111111 — which, in decimals, are 240 to 254 — or 255. Because this address class is not being used for address allocation, you cannot know what the network ID, which defines the valid addresses in a range. So the inclusion of 255 at the end of the range is moot because this address range is not available for you to use. All you need to know is that by definition Class E includes all valid addresses higher than Class D.

Classless Addressing

- During the 1990s, ISP (Internet Service Provider)s came into prominence.

- ❖ An ISP is an organization that provides Internet access for individuals, small business, and mid-size organization
- ❖ An ISP can be granted several class B or class C blocks and then subdivide the range of addresses(in groups of 2,4,8, or 16 addresses)
- ❖ The customers are connected via a dial-up modem, DSL, or capable modem to the ISP
- ❖ To facilitate this evolution, in 1996, the Internet authorities announced a new architecture called classless addressing that would eventually render classful addressing obsolete.
- ❖ To simplify the handling of addresses, the internet authorities impose three restriction on classless address blocks
- ❖ The address in a block must be contiguous, one after another
- ❖ The number of addresses in a block must be a power of 2(1, 2, 4, 8, 16…)
- ❖ The first address must be evenly divisible

Example: A classless IP address assigned to a small organization with only 16 IP Addresses 205.16.37.32 205.16.37.33 . . .

205.16.37.4

- ✓ A better way to define a block of address in classless addressing is to select any address in the block and mask it.
- ✓ A mask is a 32bit number in which the n left most bits are 1s and the 32-n rightmost bits are 0s.
- ✓ The mask can take a value from 0 to 32
- ✓ IN IPV4 classless addressing a block of addresses can be defined as x.y.z.t/n in which x.y.z.t defines one of the addresses and the /n defines the mask
- ✓ The address and /n notation completely define the whole block (the first address, the last address, and the number of addresses).
- ✓ The first address in the block can be found by setting the 32-n right most bits in the binary notation of the address 0.
- ✓ The last address in the block can be found by setting the rightmost 32-n bits to 1s.
- ✓ The number of address in the block can be found by using the formula 232-n

Example: Find the first address, the last address and the number of addresses in the following classless block 205.16.37.39/28

Solution

Step 1: Convert the dotted decimal representation into binary

Representation 11001101.00010000.00100101.00100111

Step 2: To find the first address in the block convert the 32-28 right most bits to 0. 11001101.00010000.00100101.00100000=205.16.37.32.

Step 3: To find the last address in the block convert the 32-28 right most bits to 1. 11001101.00010000.00100101.00101111=205.16.37.47.

Step 4: The number of address

Network Masks

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node.

Class A, B, and C networks have default masks, also known as natural masks, as shown here: Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

An IP address on a Class A network that has not been subnetted would have an address/mask pair similar to: 8.20.15.1 255.0.0.0.

In order to see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.

8.20.15.1

= 00001000.00010100.00001111.00000001 255.0.0.0

= 11111111.00000000.00000000.00000000

Once you have the address and the mask represented in binary, then identification of the network and host ID is easier.

1. Any address bits which have corresponding mask bits set to 1 represent the network ID.

2. Any address bits that have corresponding mask bits set to 0 represent the node ID(Host ID).

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000 ---------- net id | host id net id = 00001000 = 8 host id = 00010100.00001111.00000001 = 20.15.1

The Network Address

- ✓ When an IPv4 packet is created or forwarded, the destination network address must be extracted from the destination address.
- ✓ This is done by a logic called AND
- ✓ The IPv4 host address is logically AND end with its subnet mask to determine the network address to which the host is associated
- ✓ When this AND ing between the address and the subnet mask is performed, the result yields the network address Anding operation:

1 AND 1 = 1 1 AND 0 = 0 0 AND 1 = 0 0 AND 0 = 0 32Cont… Using the subnet mask to determine the network address for the host 172.16.132.70/20 Convert binary network address to decimal

7.2 Subnetting and Variable Length Subnet Masking (VLSM)

7.2.1 Subnetting

- ✓ Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network.
- ✓ If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic. But what are the implications of dividing networks for the network planners?

Dividing the Network into right size:

- ✓ Every network within the internetwork of a corporation or organization is designed to accommodate a finite number of hosts.
- ✓ Some networks, such as point-to-point WAN links, only require a maximum of two hosts.
- ✓ Other networks, such as a user LAN in a large building or department, may need to accommodate hundreds of hosts.
- ✓ Network administrators need to devise the internetwork addressing scheme to accommodate the maximum number of hosts for each network

Network Administrators must Consider the following points:

- Determine the Total Number of Hosts This includes end user devices, servers, intermediate devices, and router interfaces
- Determine the Number and Size of the Nets based on common groupings of hosts We subnet our network to overcome issues with location, size, and control.
- Grouping based on common geographic location
- Grouping hosts used for specific purposes
- Grouping based on ownership 35How to create subnet In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID.

For each bit borrowed, we double the number of sub networks available.

For example, if we borrow 1 bit, we can define 2 subnets, If we borrow 2 bits, we can have 4 subnets.

• Example: if we borrow one bit

√ 11111111.11111111.11111111.00000000 – Subnet 1

√ 11111111.11111111.11111111.10000000 -- Subnet 2

• If we borrow two bit

√ 11111111.11111111.11111111.00000000 – Subnet 1

√11111111.11111111.11111111.01000000--Subnet2

√11111111.11111111.11111111.10000000–Subnet3

√ 11111111.11111111.11111111.11000000 -- Subnet4

However, with each bit we borrow, fewer host addresses are available per subnet

Calculating Addresses

Example#1: Router A in the figure above has two interfaces to interconnect two networks. Given an address block of 192.168.1.0 /24, we need to create two subnets.

- We borrow one bit from the host portion by using a subnet mask of 255.255.255.128, instead of the original 255.255.255.0 mask.
- The most significant bit in the last octet is used to distinguish between the two subnets.
- For one of the subnets, this bit is a "0" and for the other subnet this bit is a "1".
- Formula for calculating subnets we can create by borrowing bits of host address

√ 2 n where n = the number of bits borrowed

In this example, the calculation looks like this:

√ 2 1 = 2 subnets

Formula for calculating the number of hosts in the subnet

2n - 2 where n = the number of bits left for hosts

Applying this formula, (2 7 - 2 = 126) shows that each of these subnets can have 126 hosts.

For each subnet, examine the last octet in binary.

The values in these octets for the two networks are:

Subnet 1: 00000000 = 0

Subnet 2: 10000000 = 12

Defining the Subnet Numbers

Subnet Example #2 Given: An organization is assigned the network number 193.1.1.0/24 and it needs to define six subnets. The largest subnet is required to support 25 hosts.

- Since a network address can only be subnetted along binary boundaries, subnets must be created in blocks of powers of two [2 (21), 4 (22), 8 (23), 16 (24), and so on]. Thus, it is impossible to define an IP address block such that it contains exactly six subnets.

For this example, the network administrator must define a block of 8 (23) and have two unused subnets that can be reserved for future growth.

In this example, the organization is subnetting a /24 so it will need three more bits, or a /27, as the extended network prefix.

- A 27-bit extended network prefix mask can be expressed in dotted- decimal notation as 255.255.255.224.
- A 27-bit extended network prefix leaves 5 bits to define host addresses on each subnet. This means that each subnetwork with a 27-bit prefix represents a contiguous block of 2 5 (32) individual IP addresses.

However, since the all-0s and all-1s host addresses cannot be allocated, there are 30 (2 5-2) assignable host addresses on each subnet.

The eight subnet numbers for this example are listed in the following code sample. The underlined portion of each address identifies the extended network prefix, while the bold digits identify the 3 bits representing the subnet number field:

Base Net: 11000001.00000001.00000001 .00000000 = 193.1.1.0/24

1. Subnet #0: 11000001.00000001.00000001.000 00000 = 193.1.1.0/27

2. Subnet #1: 11000001.00000001.00000001.001 00000 = 193.1.1.32/27

3. Subnet #2: 11000001.00000001.00000001.010 00000 = 193.1.1.64/27

4. Subnet #3: 11000001.00000001.00000001.011 00000 = 193.1.1.96/27

5. Subnet #4: 11000001.00000001.00000001.100 00000 = 193.1.1.128/27

6. Subnet #5: 11000001.00000001.00000001.101 00000 = 193.1.1.160/27

7. Subnet #6: 11000001.00000001.00000001.110 00000 = 193.1.1.192/27

8. Subnet #7: 11000001.00000001.00000001.111 00000 = 193.1.1.224/27

Defining Host Addresses for Each Subnet

- According to Internet practices, the host number field of an IP address cannot contain all 0-bits or all 1-bits.
- The all-0s host number identifies the base network (or subnetwork) number, while the all-1s host number represents the broadcast address for the network (or subnetwork).
- In our current example, there are 5 bits in the host number field of each subnet address. This means that each subnet represents a block of 30 host addresses (25 -2 = 30, note that the 2 is subtracted because the all-0s and the all-1s host addresses cannot be used). The hosts on each subnet are numbered 1 through 30.
- In general, to define the address assigned to Host #N of a particular subnet, the network administrator places the binary representation of N into the subnet' s host number field. For example, to define the address assigned to Host #15 on Subnet #2, the network administrator simply places the binary representation of 15 (011112) into the 5-bits of Subnet #2' s host number field.
- The valid host addresses for Subnet #2 in this example are listed in the following sample code. The underlined portion of each address identifies the extended network prefix, while the bold digits identify the 5-bit host number field:

Subnet #2: 11000001.00000001.00000001.010 00000 = 193.1.1.64/27

Host #1: 11000001.00000001.00000001.010 00001 = 193.1.1.65/27

Host #2: 11000001.00000001.00000001.010 00010 = 193.1.1.66/27

Host #3: 11000001.00000001.00000001.010 00011 = 193.1.1.67/27

Host #4: 11000001.00000001.00000001.010 00100 = 193.1.1.68/27

Host #5: 11000001.00000001.00000001.010 00101 = 193.1.1.69/27

Host #15: 11000001.00000001.00000001.010 01111 = 193.1.1.79/27

Host #16: 11000001.00000001.00000001.010 10000 = 193.1.1.80/27

Host #27: 11000001.00000001.00000001.010 11011 = 193.1.1.91/27

Host #28: 11000001.00000001.00000001.010 11100 = 193.1.1.92/27

Host #29: 11000001.00000001.00000001.010 11101 = 193.1.1.93/27

Host #30: 11000001.00000001.00000001.010 11110 = 193.1.1.94/27

7.2.2 Variable Length Subnet Masking (VLSM)

- VLSM is a technique that network administrators employ in order to use their IP subnet(s) in a more effective manner.
- By using VLSM, a long mask can be used on a network that has a few hosts and a short net mask on subnets that have a large number of hosts.
- To use VLSM, however, a routing protocol that supports it has to be used. Cisco routers support the concept with the following protocols: Integrated IS-IS (Integrated Intermediate System to Intermediate System), EIGRP (Enhanced Interior Gateway Routing Protocol), RIPv2, Open Shortest Path First (OSPF), and static routing.
- VLSM allows networks to have different subnet masks if the routing protocol on the network on which it is employed supports it.
- VLSM also allows more than one subnet mask within the same network address space, which is also referred to as “sub netting a subnet.”

Example

- In all of the previous examples of Subnetting, notice that the same subnet mask was applied for all the subnets. This means that each subnet has the same number of available host addresses.
- You can need this in some cases, but, in most cases, having the same subnet mask for all subnets ends up wasting address space.

For example, in the Subnet

Example #3 section, a class C network was split into eight equal-size subnets; however, each subnet did not utilize all available host addresses, which results in wasted address space.

VLSM allows you to use different masks for each subnet, thereby using address space efficiently.

Given the same network and requirements as in Subnet Example #3 develop a subnetting scheme with the use of VLSM, given:

1. net A: must support 14 hosts
2. netB: must support 28 hosts
3. netC: must support 2 hosts
4. netD: must support 7 hosts
5. netE: must support 28 host.

Determine what mask allows the required number of hosts.

1. netA: requires a /28 (255.255.255.240) mask to support 14 hosts
2. netB: requires a /27 (255.255.255.224) mask to support 28 hosts
3. netC: requires a /30 (255.255.255.252) mask to support 2 hosts
4. netD*: requires a /28 (255.255.255.240) mask to support 7 hosts
5. netE: requires a /27 (255.255.255.224) mask to support 28 hosts * a /29 (255.255.255.248) would only allow 6 usable host addresses therefore netD requires a /28 mask.

The easiest way to assign the subnets is to assign the largest first.

For example, you can assign in this manner:

1. netB: 204.15.5.0/27 host address range 1 to 30
2. netE: 204.15.5.32/27 host address range 33 to 62
3. netA: 204.15.5.64/28 host address range 65 to 78
4. netD: 204.15.5.80/28 host address range 81 to 94
5. netC: 204.15.5.96/30 host address range 97 to 98

Chapter 8

8. 1.Data Security and Integrity

1. Data Security:

Data security refers to the prevention of data from unauthorized users. It is only allowed to access the data to the authorized users. In database, the DBA or head of department can access all the data. Some users are only allowed to retrieve data, whereas others are allowed to retrieve as well as to modify the data.

2. Data Integrity:

Data integrity is defined as the data contained in the database is both correct and consistent. For this purpose, the data stored in the database must satisfy certain types of procedures (rules). The data in a database must be correct and consistent. So, data stored in the database must satisfy certain types of procedure (rules). DBMS provides different ways to implement such types of constraints (rules). This improves data integrity in a database.

8.1. Fundamentals of secure networks; cryptography

Top 5 fundamentals of network security

These network security fundamentals are vital to downtime prevention, government regulation compliance, reduced liability and reputation protection:

1. Keep patches and updates current

Cyber criminals exploit vulnerabilities in operating systems, software applications, web browsers and browser plug-ins when administrators are lax about applying patches and updates.

In particular, verify that office computers are running current versions of these much used programs:

- Adobe Acrobat and Reader
- Adobe Flash
- Oracle Java
- Microsoft Internet Explorer

- Microsoft Office Suite

Keep an inventory to make sure each device is updated regularly, including mobile devices and network hardware. And make sure Windows and Apple computers have automatic updating enabled.

2. Use strong passwords

By now, most users know not to write their passwords on Post-It Notes that are plastered to their monitors. But there's more to keeping passwords secure than keeping them out of plain sight.

The definition of a strong password is one that's difficult to detect by humans and computers, is at least 6 characters, preferably more, and uses a combination of upper- and lower-case letters, numbers and symbols.

Symantec gives additional suggestions:

- Don't use any words from the dictionary. Also avoid proper nouns or foreign words.
- Don't use anything remotely related to your name, nickname, family members or pets.
- Don't use any numbers someone could guess by looking at your mail like phone numbers and street numbers, and
- Choose a phrase that means something to you, take the first letters of each word and convert some into characters.

The SANS Institute recommends passwords be changed at least every 90 days, and that users not be allowed to reuse their last 15 passwords. They also suggest that users be locked out of their accounts for an hour and a half after eight failed log-on attempts within a 45-minute period.

Train users to recognize social engineering techniques used to trick them into divulging their passwords. Hackers are known to impersonate tech support to get people to give out their passwords or simply look over users' shoulders while they type in their passwords.

3. Secure your VPN

Data encryption and identity authentication are especially important to securing a VPN. Any open network connection is a vulnerability hackers can exploit to sneak onto your network. Moreover, data is particularly vulnerable while it is traveling over the Internet. Review the

documentation for your server and VPN software to make sure that the strongest possible protocols for encryption and authentication are in use.

Multi-factor authentication is the most secure identity authentication method. The more steps your users must take to prove their identity, the better. For example, in addition to a password, users could be required to enter a PIN. Or, a random numerical code generated by a key-fob authenticator every 60 seconds could be used in conjunction with a PIN or password.

- It is also a good idea to use a firewall to separate the VPN network from the rest of the network.
- Other tips include:
- Use cloud-based email and file sharing instead of a VPN.
- Create and enforce user-access policies. Be stingy when granting access to employees, contractors and business partners.
- Make sure employees know how to secure their home wireless networks. Malicious software that infects their devices at home can infect the company network via an open VPN connection, and
- Before granting mobile devices full access to the network, check them for up-to-date anti-virus software, firewalls and spam filters.

4. Actively manage user access privileges

Inappropriate user-access privileges pose a significant security threat. Managing employee access to critical data on an ongoing basis should not be overlooked. More than half of 5,500 companies recently surveyed by HP and the Ponemon Institute said that their employees had access to "sensitive, confidential data outside the scope of their job requirements." In reporting on the study's findings, eWeek.com said "general business data such as documents, spreadsheets, emails and other sources of unstructured data were most at risk for snooping, followed by customer data." When an employee's job changes, make sure the IT department is notified so their access privileges can be modified to fit the duties of the new position.

5. Clean up inactive accounts

Hackers use inactive accounts once assigned to contractors and former employees to gain access and disguise their activity. The HP/Ponemon Institute report did find that the companies in the

survey were doing a good job deleting accounts once an employee quit or was laid off. Software is available for cleaning up inactive accounts on large networks with many users.

Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word *kryptos*, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging. Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers.

When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other plain-text messages. The simplest method uses the symmetric or "secret key" system. Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption. The problem? If the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the asymmetric or "public key" system. In this case, every user has two keys: one public and one private. Senders request the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient's private key will decode it — meaning theft is of no use without the corresponding private key.

Best Practices

Users should always encrypt any messages they send, ideally using a form of public key encryption. It's also a good idea to encrypt critical or sensitive files — anything from sets of family photos to company data like personnel records or accounting history. Look for a security solution that includes strong cryptography algorithms along with an easy-to-use interface. This helps ensure the regular use of encryption functions and prevents data loss even if a mobile device, hard drive or storage medium falls into the wrong hands.

8.2. Encryption and privacy

Encryption can help protect data you send, receive, and store, using a device. That can include text messages stored on your smartphone, running logs saved on your fitness watch, and banking information sent through your online account.

Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information.

Vast amounts of personal information are managed online and stored in the cloud or on servers with an ongoing connection to the web. It's nearly impossible to do business of any kind without your personal data ending up in an organization's networked computer system, which is why it's important to know how to help keep that data private.

Encryption plays an essential role.

How does encryption work?

Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format — called "cipher text." This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet.

- When the intended recipient accesses the message, the information is translated back to its original form. This is called decryption.
- To unlock the message, both the sender and the recipient have to use a "secret" encryption key — a collection of algorithms that scramble and unscramble data back to a readable format.

Symmetric and asymmetric encryption: What's the difference?

An encryption key is a series of numbers used to encrypt and decrypt data. Encryption keys are created with algorithms. Each key is random and unique.

There are two types of encryption systems: symmetric encryption and asymmetric encryption. Here's how they're different.

- Symmetric encryption uses a single password to encrypt and decrypt data.

- Asymmetric encryption uses two keys for encryption and decryption. A public key, which is shared among users, encrypts the data. A private key, which is not shared, decrypts the data.

Types of Encryption

There are several types of encryption, each developed with different needs and security needs in mind. Here are the most common examples of encryption.

Data Encryption Standard (DES)

Data Encryption Standard is considered a low-level encryption standard. The U.S. government established the standard in 1977. Due to advances in technology and decreases in the cost of hardware, DES is essentially obsolete for protecting sensitive data.

Triple DES

Triple DES runs DES encryption three times. Here's how it works: It encrypts, decrypts, and encrypts data — thus, "triple." It strengthens the original DES standard, which became regarded as too weak a type of encryption for sensitive data.

RSA

RSA takes its name from the familial initials of three computer scientists. It uses a strong and popular algorithm for encryption. RSA is popular due to its key length and therefore widely used for secure data transmission.

Advanced Encryption Standard (AES)

Advanced Encryption Standard is the U.S. government standard as of 2002. AES is used worldwide.

TwoFish

Two fish is considered one of the fastest encryption algorithms and is free for anyone to use. It's used in hardware and software.

Using encryption via SSL

Most legitimate websites use what is called "secure sockets layer" (SSL), which is a form of encrypting data when it is being sent to and from a website. This keeps attackers from accessing that data while it is in transit.

- Look for the padlock icon in the URL bar, and the "s" in the "https://" to make sure you are conducting secure, encrypted transactions online.
- It's a good idea to access sites using SSL when:
- You store or send sensitive data online. If you use the internet to carry out tasks such as filing your taxes, making purchases, renewing your driver's license, or conducting any other personal business, visiting sites using SSL is a good idea.
- Your work requires it. Your workplace may have encryption protocols, or it may be subject to regulations that require encryption. In these cases, encryption is a must.

3 reasons why encryption matters

Why is encryption important? Here are three reasons:

1. Internet privacy concerns are real

- Encryption helps protect your online privacy by turning personal information into "for your eyes only" messages intended only for the parties that need them — and no one else.
- You should make sure that your emails are being sent over an encrypted connection, or that you are encrypting each message.
- Most email clients come with the option for encryption in their Settings menu, and if you check your email with a web browser, take a moment to ensure that SSL encryption is available.

2. Hacking is big business

- Cybercrime is a global business, often run by multinational outfits.
- Many of the large-scale data breaches that you may have heard about in the news demonstrate that cybercriminals are often out to steal personal information for financial gain.

3. Regulations demand it

- The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers to implement security features that help protect patients' sensitive health information online.
- Institutions of higher learning must take similar steps under the Family Education Rights and Privacy Act (FERPA) to protect student records.
- Retailers must contend with the Fair Credit Practices Act (FCPA) and similar laws that help protect consumers.
- Encryption helps businesses stay compliant with regulatory requirements and standards. It also helps protect the valuable data of their customers.

8.3. Authentication protocols

User authentication is the first most priority while responding to the request made by the user to the software application. There are several mechanisms made which are required to authenticate the access while providing access to the data. In this blog, we will explore the most common authentication protocols and will try to explore their merits and demerits.

Types of authentication protocols

1. Kerberos :

Kerberos is a protocol that aids in network authentication. This is used for validating clients/servers during a network employing a cryptographic key. It is designed for executing strong authentication while reporting to applications. The overall implementation of the Kerberos protocol is openly available by MIT and is used in many mass-produced products.

Some advantages of Kerberos:

- It supports various operating systems.
- The authentication key is shared much efficiently than public sharing.

Some disadvantages of Kerberos:

- It is used only to authenticate clients and services used by them.
- It shows vulnerability to soft or weak passwords.

2. Lightweight Directory Access Protocol (LDAP) :

- LDAP refers to Lightweight Directory Access Protocol. It is a protocol that is used for determining any individuals, organizations, and other devices during a network regardless of being on public or corporate internet. It is practiced as Directories-as-a-Service and is the grounds for Microsoft building Activity Directory.

Some advantages of LDAP:

- It is an automated protocol which makes it modernizing easier.
- It supports existing technologies and allows multiple directories.

Some disadvantages of LDAP:

- It requires the experience of deployment.
- The directory servers are required to be LDAP obedient for deployment.

3. OAuth2 :

OAuth as the name suggests it is an authorization framework that promotes granting limited access to the user on its account through an HTTP service. When a user requests access to resources an API call is made and after the authentication token is passed.

Some advantages of OAuth2 :

- It is a simple protocol and is easy to implement.
- It provides server-side authorization of code.

Some disadvantages of OAuth2 :

- It is vulnerable to manage different sets of code.
- It shows serious effects on sites connected to another affected system.

4. SAML :

SAML stands for Security Assertion Markup Language which is based on XML-based authentication data format which provides the authorization between an identity provider and service provider. It serves as a product of the OASIS Security Services Technical Committee.

Some advantages of SAML :

- It reduced the administrative costs for the end-users.

- It provides a single sign-in for authenticating across service providers.

Some disadvantages of SAML:

- It is dependent on the identity provider.
- All the data is managed in a single XML format.

5. RADIUS :

RADIUS stands for Remote Authentication Dial-In User Service. It is a network protocol that provides sufficient centralized Authentication, Accounting, and Authorization for the users that use and network services. The functioning of the protocol occurs when the user requests access to network resources, where the RADIUS server encrypts the credentials which are entered by the user. After this, the user credentials are mapped through the local database and provide access.

Some advantages of RADIUS :

- It is a great mechanism for providing multiple access for Admins.
- It provides a unique identity to each user in a session.

Some disadvantages of RADIUS :

- Initial implementation for this mechanism is hard on hardware.
- It has a variety of models that may require a special team which is cost consuming.
- Differentiating between the protocols will not make justice to the protocols because it depends on the use of the application and for what purpose it is being used.

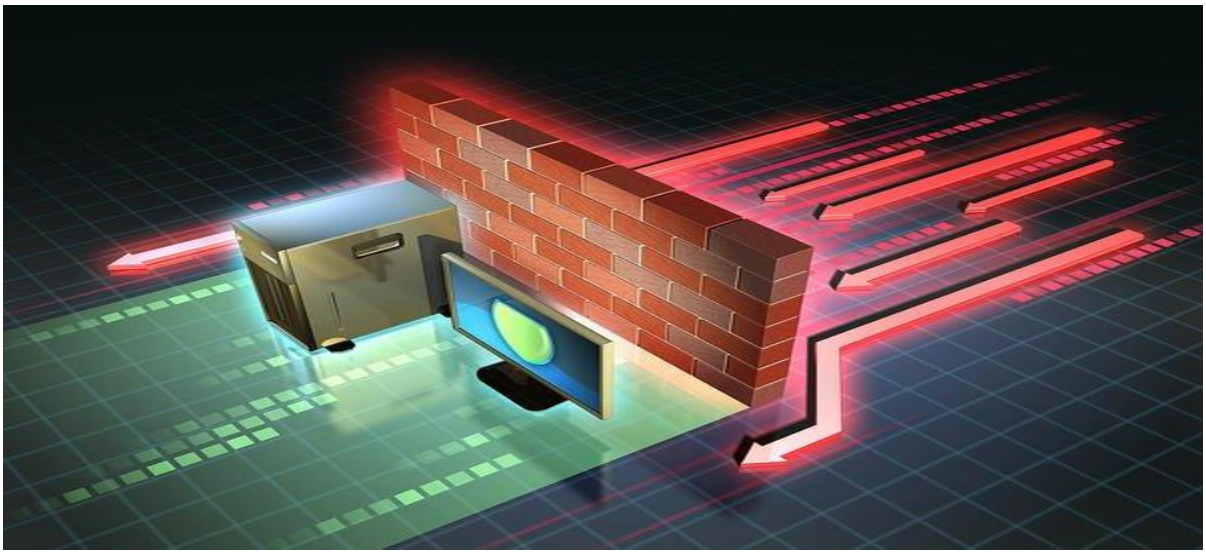
8.4. Firewalls

What is a Firewall?

A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

8 Types of Firewalls



Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (a.k.a. proxy firewalls)
- Next-gen firewalls
- Software firewalls
- Hardware firewalls
- Cloud firewalls

Note: The last three bullets list methods of delivering firewall functionality, rather than being types of firewall architectures in and of themselves.

- How do these firewalls work? And, which ones are the best for your business' cybersecurity needs?
- Here are a few brief explainers:

Packet-Filtering Firewalls

As the most “basic” and oldest type of firewall architecture, packet-filtering firewalls basically create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.

- If the information packet doesn’t pass the inspection, it is dropped.
- The good thing about these firewalls is that they aren’t very resource-intensive. This means they don’t have a huge impact on system performance and are relatively simple. However, they’re also relatively easy to bypass compared to firewalls with more robust inspection capabilities.

Circuit-Level Gateways

As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the

transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.

While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware, but had the right TCP handshake, it would pass right through. This is why circuit-level gateways are not enough to protect your business by themselves.

Stateful Inspection Firewalls

These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone.

However, these firewalls do put more of a strain on computing resources as well. This may slow down the transfer of legitimate packets compared to the other solutions.

Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source—hence, the name "application-level gateway." These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.

This check is similar to the stateful inspection firewall in that it looks at both the packet and at the TCP handshake protocol. However, proxy firewalls may also perform deep-layer packet inspections, checking the actual contents of the information packet to verify that it contains no malware.

Once the check is complete, and the packet is approved to connect to the destination, the proxy sends it off. This creates an extra layer of separation between the "client" (the system where the packet originated) and the individual devices on your network—obscuring them to create additional anonymity and protection for your network.

If there's one drawback to proxy firewalls, it's that they can create significant slowdown because of the extra steps in the data packet transferal process.

Next-Generation Firewalls

Many of the most recently-released firewall products are being touted as “next-generation” architectures. However, there is not as much consensus on what makes a firewall truly next-gen.

Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.

The issue is that there is no one definition of a next-generation firewall, so it’s important to verify what specific capabilities such firewalls have before investing in one.

Software Firewalls

Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware (or a cloud server). The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.

However, maintaining individual software firewalls on different devices can be difficult and time-consuming. Furthermore, not every device on a network may be compatible with a single software firewall, which may mean having to use several different software firewalls to cover every asset.

Hardware Firewalls

Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.

The major weakness of a hardware-based firewall, however, is that it is often easy for insider attacks to bypass them. Also, the actual capabilities of a hardware firewall may vary depending on the manufacturer—some may have a more limited capacity to handle simultaneous connections than others, for example.

Cloud Firewalls

Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or firewall-as-a-service (FaaS). Cloud firewalls are considered synonymous with proxy firewalls by many, since a cloud server is often used in a proxy firewall setup (though the proxy doesn't necessarily *have* to be on the cloud, it frequently is).

The big benefit of having cloud-based firewalls is that they are very easy to scale with your organization. As your needs grow, you can add additional capacity to the cloud server to filter larger traffic loads. Cloud firewalls, like hardware firewalls, excel at perimeter security.

Which Firewall Architecture is Right for Your Company?

So, which firewall architecture is the right one for your business?

- The simple packet filtering or circuit-level gateway, which provides basic protection that has minimal performance impact?
- The stateful inspection architecture that combines the capabilities of both of the previous two options, but has a larger performance impact? Or

- A proxy or next-gen firewall that offers far more robust protection in exchange for additional expenses and an even higher performance impact?

The real question is “why would you only use one?”

No one protection layer, no matter how robust, will ever be enough to protect your business. To provide better protection, your networks should have multiple layers of firewalls, both at the perimeter and separating different assets on your network. For example, you could have a hardware or cloud firewall at the perimeter of your network, then individual software firewalls on each of your network assets.

- Having additional firewalls helps to make your network tougher to crack by creating additional defense-in-depth that isolates different assets—making it so attackers have to perform extra work to reach all of your most sensitive information.
- The particular firewalls that you will want to use will depend on the capabilities of your network, relevant compliance requirements for your industry, and the resources you have in place to manage these firewalls.
- Need help finding the ideal firewall architecture for your business’ needs? Consider starting with a security policy audit and assessment first. This can help you identify all of the assets on your network that need protecting so you can better optimize your firewall implementation.

Or, contact Compuquip Cybersecurity to get more assistance with perfecting your company’s cybersecurity strategy.

8.5. Virtual private networks

What is VPN? How It Works, Types of VPN

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

What are the benefits of a VPN connection?

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

- **Secure encryption:** To read the data, you need an *encryption key* . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.

- **Disguising your whereabouts** : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.
- **Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing** , you can switch to a server to another country and effectively "change" your location.
- **Secure data transfer:** If you work remotely, you may need to access important files on your company's network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Why should you use a VPN connection?

- Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.
- Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.
- This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.

What should a good VPN do?

You should rely on your VPN to perform one or more tasks. The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

- ✓ **Encryption of your IP address:** The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.
- ✓ **Encryption of protocols:** A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.
- ✓ **Kill switch:** If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.
- ✓ **Two-factor authentication:** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

The history of VPNs

Since humans have been using the internet, there has been a movement to protect and encrypt internet browser data. The US Department of Defense already got involved in projects working on the encryption of internet communication data back in the 1960s.

The predecessors of the VPN

Their efforts led to the creation of **ARPANET** (Advanced Research Projects Agency Network), a packet switching network, which in turn led to the development of the Transfer Control Protocol/Internet Protocol (TCP/IP).

The **TCP/IP** had four levels: **Link, internet, transport and application**. At the internet level, local networks and devices could be connected to the universal network – and this is where the risk of exposure became clear. In 1993, a team from Columbia University and AT&T Bell Labs

finally succeeded in creating a kind of first version of the modern VPN, known as swIPe: Software IP encryption protocol.

In the following year, Wei Xu developed the IPSec network, an internet security protocol that authenticates and encrypts information packets shared online. In 1996, a Microsoft employee named Gurdeep Singh-Pall created a Peer-to-Peer Tunneling Protocol (PPTP).

Early VPNs

Contiguous to Singh-Pall developing PPTP, the internet was growing in popularity and the need for consumer-ready, sophisticated security systems emerged. At that time, anti-virus programs were already effective in preventing malware and spyware from infecting a computer system. However, people and companies also started demanding encryption software that could hide their browsing history on the internet.

The first VPNs therefore started in the early 2000s, but were almost exclusively used by companies. However, after a flood of security breaches, especially in the early 2010s, the consumer market for VPNs started to pick up.

VPNs and their current use

According to the ***GlobalWebIndex***, the number of VPN users worldwide increased more than fourfold between 2016 and 2018. In countries such as Thailand, Indonesia and China, where internet use is restricted and censored, **one in fiveinternet users** uses a VPN. In the USA, Great Britain and Germany, the proportion of VPN users is **lowerat around 5%**, but is growing.

One of the biggest drivers for VPN adoption in recent years has been the increasing demand for content with geographical access restrictions. For example, video streaming services such as Netflix or YouTube make certain videos available only in certain countries. With contemporary VPNs, you can encrypt your IP address so that you appear to be surfing from another country, enabling you to access this content from anywhere.

Here’s how to surf securely with a VPN

A VPN encrypts your surfing behavior, which can only be decoded with the help of a key. Only your computer and the VPN know this key, so your ISP cannot recognize where you are surfing. Different VPNs use different encryption processes, but generally function in three steps:

Once you are online, start your VPN. The VPN acts as a secure tunnel between you and the internet. Your ISP and other third parties cannot detect this tunnel.

Your device is now on the local network of the VPN, and your IP address can be changed to an IP address provided by the VPN server.

You can now surf the internet at will, as the VPN protects all your personal data.

What kind of VPNs are there?

There are many different types of VPNs, but you should definitely be familiar with the three main types:

SSL VPN

Often not all employees of a company have access to a company laptop they can use to work from home. During the corona crisis in Spring 2020, many companies faced the problem of not having enough equipment for their employees. In such cases, use of a private device (PC, laptop, tablet, mobile phone) is often resorted to. In this case, companies fall back on an **SSL-VPN** solution, which is usually implemented via a corresponding hardware box.

The prerequisite is usually an HTML-5-capable browser, which is used to call up the company's login page. HTML-5 capable browsers are available for virtually any operating system. Access is guarded with a username and password.

Site-to-site VPN

A **site-to-site VPN** is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources.

A site-to-site VPN is useful if you have multiple locations in your company, each with its own local area network (LAN) connected to the WAN (Wide Area Network). Site-to-site VPNs are also useful if you have two separate intranets between which you want to send files without users from one intranet explicitly accessing the other.

Site-to-site VPNs are mainly used in large companies. They are complex to implement and do not offer the same flexibility as SSL VPNs. However, they are the most effective way to ensure communication within and between large departments.

Client-to-Server VPN

Connecting via a **VPN client** can be imagined as if you were connecting your home PC to the company with an extension cable. Employees can dial into the company network from their home office via the secure connection and act as if they were sitting in the office. However, a VPN client must first be installed and configured on the computer.

This involves the user not being connected to the internet via his own ISP, but establishing a direct connection through his/her VPN provider. This essentially shortens the tunnel phase of the VPN journey. Instead of using the VPN to create an encryption tunnel to disguise the existing internet connection, the VPN can automatically encrypt the data before it is made available to the user.

This is an increasingly common form of VPN, which is particularly useful for providers of insecure public WLAN. It prevents third parties from accessing and compromising the network connection and encrypts data all the way to the provider. It also prevents ISPs from accessing data that, for whatever reason, remains unencrypted and bypasses any restrictions on the user's internet access (for instance, if the government of that country restricts internet access).

The advantage of this type of VPN access is greater efficiency and universal access to company resources. Provided an appropriate telephone system is available, the employee can, for example, connect to the system with a headset and act as if he/she were at their company workplace. For example, customers of the company cannot even tell whether the employee is at work in the company or in their home office.

How do I install a VPN on my computer?

Before installing a VPN, it is important to be familiar with the different implementation methods:

VPN client

Software must be installed for standalone VPN clients. This software is configured to meet the requirements of the endpoint. When setting up the VPN, the endpoint executes the VPN link and connects to the other endpoint, creating the encryption tunnel. In companies, this step usually requires the entry of a password issued by the company or the installation of an appropriate

certificate. By using a password or certificate, the firewall can recognize that this is an authorized connection. The employee then identifies him/herself by means of credentials known to him/her.

Browser extensions

VPN extensions can be added to most web browsers such as Google Chrome and Firefox. Some browsers, including Opera, even have their own integrated VPN extensions. Extensions make it easier for users to quickly switch and configure their VPN while surfing the internet. However, the VPN connection is only valid for information that is shared in this browser. Using other browsers and other internet uses outside the browser (e.g. online games) cannot be encrypted by the VPN.

While browser extensions are not quite as comprehensive as VPN clients, they may be an appropriate option for occasional internet users who want an extra layer of internet security. However, they have proven to be more susceptible to breaches. Users are also advised to choose a reputable extension, as ***data harvesters*** may attempt to use fake VPN extensions. Data harvesting is the collection of personal data, such as what marketing strategists do to create a personal profile of you. Advertising content is then personally tailored to you.

Router VPN

If multiple devices are connected to the same internet connection, it may be easier to implement the VPN directly on the router than to install a separate VPN on each device. A router VPN is especially useful if you want to protect devices with an internet connection that are not easy to configure, such as smart TVs. They can even help you access geographically restricted content through your home entertainment systems.

A router VPN is easy to install, always provides security and privacy, and prevents your network from being compromised when insecure devices log on. However, it may be more difficult to manage if your router does not have its own user interface. This can lead to incoming connections being blocked.

Company VPN

A company VPN is a custom solution that requires personalized setup and technical support. The VPN is usually created for you by the company's IT team. As a user, you have no administrative influence from the VPN itself and your activities and data transfers are logged by your company. This allows the company to minimize the potential risk of data leakage. The main advantage of a corporate VPN is a fully secure connection to the company's intranet and server, even for employees who work outside the company using their own internet connection.

Can I also use a VPN on my smartphone or other devices?

Yes, there are a number of VPN options for smartphones and other internet-connected devices. A VPN can be essential for your mobile device if you use it to store payment information or other personal data or even just to surf the internet. Many VPN providers also offer mobile solutions - many of which can be downloaded directly from Google Play or the Apple App Store, such as Kaspersky VPN Secure Connection.

Is a VPN really so secure?

It is important to note that VPNs do not function like comprehensive anti-virus software. While they protect your IP and encrypt your internet history, a VPN connection does not protect your computer from outside intrusion. To do this, you should definitely use anti-virus software such as Kaspersky Internet Security . Because using a VPN on its own does not protect you from Trojans, viruses, bots or other malware.

Once the malware has found its way onto your device, it can steal or damage your data, whether you are running a VPN or not. It is therefore important that you use a VPN together with a comprehensive anti-virus program to ensure maximum security.

Selecting a secure VPN provider

It is also important that you choose a VPN provider that you can trust. While your ISP cannot see your internet traffic, your VPN provider can. If your VPN provider is compromised, so are you. For this reason, it is crucial that you choose a trusted VPN provider to ensure both the concealment of your internet activities and ensure the highest level of security.

How to install a VPN connection on your smartphone

- ✓ As already mentioned, there are also VPN connections for Android smartphones and iPhones. Fortunately, smartphone VPN services are easy to use and generally include the following:
- ✓ The installation process usually only downloads one app from the iOS App Store or Google Play Store. Although free VPN providers exist, it's wise to choose a professional provider when it comes to security.
- ✓ The setup is extremely user-friendly, as the default settings are already mostly designed for the average smartphone user. Simply log in with your account. Most apps will then guide you through the key functions of the VPN services.
- ✓ Switching on the VPN literally works like a light switch for many VPN apps. You will probably find the option directly on the home screen.
- ✓ Server switching is usually done manually if you want to fake your location. Simply select the desired country from the offer.
- ✓ Advanced setup is available for users requiring a higher degree of data protection. Depending on your VPN, you can also select other protocols for your encryption method.
- ✓ Diagnostics and other functions may also be available in your app. Before you subscribe, learn about these features to find the right VPN for your needs.

In order to surf the internet safely from now on, all you have to do is first activate the VPN connection through the app.

But keep the following in mind: A VPN is only as secure as the data usage and storage policies of its provider. Remember that the VPN service transfers your data to their servers and these servers connect over the internet on your behalf. If they store data logs, make sure that it is clear for what purpose these logs are stored. Serious VPN providers usually put your privacy first and foremost. You should therefore choose a trusted provider such as Kaspersky Secure Connection .

Remember that only internet data is encrypted. Anything that does not use a cellular or Wi-Fi connection will not be transmitted over the internet. As a result, your VPN will not encrypt your standard voice calls or texts.

Conclusion

A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks. That's because only you can access the data in the encrypted tunnel – and nobody else can because they don't have the key. A VPN allows you to access regionally restricted content from anywhere in the world. Many streaming platforms are not available in every country. You can still access them using the VPN. VPN solutions from Kaspersky are available for both Windows PCs and Apple Macs.

There are now also many providers of VPN connections for smartphones which keep mobile data traffic anonymous. You can find certified providers in the Google Play Store or the iOS App Store. However, remember that only your data traffic on the internet is anonymized and protected by using a VPN. The VPN connection does not protect you from hacker attacks, Trojans, viruses or other malware. You should therefore rely on an additional trusted anti-virus software.

What security solutions include VPN protection?

8.6. Transport layer security

What is Transport Layer Security?

Transport Layer Security (TLS) is an Internet Engineering Task Force (IETF) standard protocol that provides authentication, privacy and data integrity between two communicating computer applications. It's the most widely deployed security protocol in use today and is best suited for web browsers and other applications that require data to be securely exchanged over a network. This includes web browsing sessions, file transfers, virtual private network (VPN) connections, remote desktop sessions and voice over IP (VoIP). More recently, TLS is being integrated into modern cellular transport technologies, including 5G, to protect core network functions throughout the radio access network (RAN).

How does Transport Layer Security work?

- ✓ TLS uses a client-server handshake mechanism to establish an encrypted and secure connection and to ensure the authenticity of the communication. Here's a breakdown of the process:
- ✓ Communicating devices exchange encryption capabilities.
- ✓ An authentication process occurs using digital certificates to help prove the server is the entity it claims to be.
- ✓ A session key exchange occurs. During this process, clients and servers must agree on a key to establish the fact that the secure session is indeed between the client and server -- and not something in the middle attempting to hijack the conversation.

The benefits of Transport Layer Security

The benefits of TLS are straightforward when discussing using versus not using TLS. As noted above, a TLS-encrypted session provides a secure authentication mechanism, data encryption and data integrity checks. However, when comparing TLS to another secure authentication and encryption protocol suite, such as Internet Protocol Security, TLS offers added benefits and is a reason why IPsec is being replaced with TLS in many enterprise deployment situations. These include benefits such as the following:

- ➢ Security is built directly into each application, as opposed to external software or hardware to build IPsec tunnels.
- ➢ There is true end-to-end encryption (E2EE) between communicating devices.
- ➢ There is granular control over what can be transmitted or received on an encrypted session.
- ➢ Since TLS operates within the upper layers of the Open Systems Interconnection (OSI) model, it doesn't have the network address translation (NAT) complications that are inherent with IPsec.
- ➢ TLS offers logging and auditing functions that are built directly into the protocol.

The challenges of TLS

- ➢ There are a few drawbacks when it comes to either not using secure authentication or any encryption -- or when deciding between TLS and other security protocols, such as IPsec. Here are a few examples:

- Because TLS operates at Layers 4 through 7 of the OSI model, as opposed to Layer 3, which is the case with IPsec, each application and each communication flow between client and server must establish its own TLS session to gain authentication and data encryption benefits.

The ability to use TLS depends on whether each application supports it.

- Since TLS is implemented on an application-by-application basis to achieve improved granularity and control over encrypted sessions, it comes at the cost of increased management overhead.
- Now that TLS is gaining in popularity, threat actors are more focused on discovering and exploiting potential TLS exploits that can be used to compromise data security and integrity.

Differences between TLS and SSL

As mentioned previously, SSL is the precursor to TLS. Thus, most of the differences between the two are evolutionary in nature, as the protocol adjusts to address vulnerabilities and to improve implementation and integration capabilities.

Key differences between SSL and TLS that make TLS a more secure and efficient protocol are message authentication, key material generation and the supported cipher suites, with TLS supporting newer and more secure algorithms. TLS and SSL are not interoperable, though TLS currently provides some backward compatibility in order to work with legacy systems. Additionally, TLS -- especially later versions -- completes the handshake process much faster compared to SSL. Thus, lower communication latency from an end-user perspective is noticeable.

Attacks against TLS/SSL

Implementation flaws have always been a big problem with encryption technologies, and TLS is no exception. Even though TLS/SSL communications are considered highly secure, there have been instances where vulnerabilities were discovered and exploited. But keep in mind that the examples mentioned below were vulnerabilities in TLS version 1.2 and earlier. All known vulnerabilities against prior versions of TLS, such as Browser Exploit against SSL/TLS

(BEAST), Compression Ratio Info-leak Made Easy (CRIME) and protocol downgrade attacks, have been eliminated through TLS version updates. Examples of significant attacks or incidents include the following:

The infamous Heartbleed bug was the result of a surprisingly small bug vulnerability discovered in a piece of cryptographic logic that relates to Open SSL's implementation of the TLS heartbeat mechanism, which is designed to keep connections alive even when no data is being transmitted.

Although TLS isn't vulnerable to the POODLE attack because it specifies that all padding bytes must have the same value and be verified, a variant of the attack has exploited certain implementations of the TLS protocol that don't correctly validate encryption padding byte requirements.

The BEAST attack was discovered in 2011 and affected version 1.0 of TLS. The attack focused on a vulnerability discovered in the protocol's cipher block chaining (CBC) mechanism. This enabled an attacker to capture and decrypt data being sent and received across the "secure" communications channel.

An optional data compression feature found within TLS led to the vulnerability known as CRIME. This vulnerability can decrypt communication session cookies using brute-force methods. Once compromised, attackers can insert themselves into the encrypted conversation.

The Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) vulnerability also uses compression as its exploit target, like CRIME. However, the difference between BREACH and CRIME is the fact that BREACH compromises Hypertext Transfer Protocol (HTTP) compression, as opposed to TLS compression. But, even if TLS compression isn't enabled, BREACH can still compromise the session.

Chapter 9

9. Overview

9.1. system and network administration

A system is **a group of interacting or interrelated elements that act according to a set of rules to form a unified whole**. A system, surrounded and influenced by its environment, is

described by its boundaries, structure and purpose and expressed in its functioning. Systems are the subjects of study of systems theory and other systems sciences.

Systems theory is the understanding of the whole being greater than all the parts that comprise it and was created because of the effect behaviorism had on psychology. It addresses the weakness of mechanistic approaches and provides an excellent framework to solve problems because it analyzes the interdependence and wholeness of the system.

Systems theory has negative and positive feedback loops that influence the systems.

Negative feedback loops do not offer change but help to reinforce the system

Positive feedback loops create changes

A few systems theory examples are as follows:

In the case of air travel, many different systems make the whole experience successful. For instance, when someone engages in air travel, they must start by purchasing a ticket and then go through security, having their bags and suitcases scanned in the process. The plane must also go through a safety check, refueling each time before take-off.

In this scenario, the summation of these systems and subsystems gives a high level of safety for each flight and is greater together than they are separate.

Organization is the foundation upon which the whole structure of management is erected. Organization is associated with developing an outline where the overall work is divided into manageable components in order to facilitate the achievement of objectives or goals. Thus, organization is the structure or mechanism that enables living things to work together. In a static sense, an organization is a structure or machinery manned by group of individuals who are working together towards a common goal. Examples of organization are Corporations, governments, non-government organizations, armed forces, non-profit organizations etc.

The term organization has been used in four different senses;

1. **Organization as Framework of Relationships:** Organization refers to the structure and interactions among various job positions which are created to realize certain objectives.
2. **Organization as a process:** Organization is viewed as a dynamic process and a managerial activity which is vital for planning the utilization of company's resources.
3. **Organization as a System:** Organization is also viewed as a system. System concepts recognize that organizations are made up of components, each of which has exclusive properties, abilities and reciprocated associations. The constituent elements of a system are linked together in such complex ways that actions taken by one individual have far reaching effects on others.
4. **Organization as a Group of Persons:** Organization is very often viewed as a group of persons contributing their efforts towards certain goals.

9.1.1. Exercises

Self-test objectives /answer these questions whenever you finished chapter nine

1. What kinds of issues does system administration cover?

2. Is system administration management or engineering?

3. Why does the physical environment play a role in system administration?

4. Describe why ethics and human values are important.

5. Is system administration a science? Why/why not?

6. State the top-most principles that guide network and system administrators.

9.1.2. System theory in organization

Systems theory is a theoretical framework for understanding how organizations work. A system can be defined in different ways, but it's best characterized as an entity that has all the elements necessary to carry out its functions.

Boundaries are another component of communication and interaction within the family. Boundaries have to do with both how information exits and enters the family. For example, some information may be held only inside the family, while others may be shared with non-family

members. Boundaries on information can be tied to the expectations set by the family leaders, such as the parents or caretakers.

Additionally, **homeostasis** argues that family members always try to obtain a balance within their interactions; systems theory can also be thought of in terms of homeostasis and teamwork in a work environment. If a team works very efficiently and accomplishes many tasks, they have achieved a state of homeostasis. However, if the team is easily disrupted by distractions or is inefficient, they have not achieved homeostasis. Adaptation is how a family readjusts to anything that changes within the environment of the family unit.

Systems theory was created because of the effect behaviorism had on psychology. It addresses the weakness of mechanistic approaches and provides an excellent framework to solve problems because it analyzes the interdependence and wholeness of the system.

9.1.3. What are Information systems?

Many organizations work with large amounts of **data**. Data are basic values or facts and are organized in a **database**. Many people think of data as synonymous with **information**; however, information actually consists of data that has been organized to help answer questions and to solve problems. An **information system** is defined as the software that helps organize and analyze data. So, the purpose of an information system is to turn raw data into useful information that can be used for decision making in an organization.

General Purpose vs. Specialized Information Systems

There are some general types of information systems. For example, a **database management system (DBMS)** is a combination of software and data that makes it possible to organize and analyze data. DBMS software is typically not designed to work with a specific organization or a specific type of analysis. Rather, it is a general-purpose information system. Another example is an **electronic spreadsheet**. This is a tool for basic data analysis based on formulas that define relationships among the data. For example, you can use a spreadsheet to calculate averages for a set of values or to plot the trend of a value over time.

In contrast, there are a number of specialized information systems that have been specifically designed to support a particular process within an organization or to carry out very specific

analysis tasks. For example, **enterprise resource planning (ERP)** is an information system used to integrate the management of all internal and external information across an entire organization. Another example is a **geographic information system (GIS)**, which is used to manage and analyze all types of geographical data. **Expert systems** are another example of information system. An expert's system is designed to solve complex problems by following the reasoning of an expert.

Typical Components of Information Systems

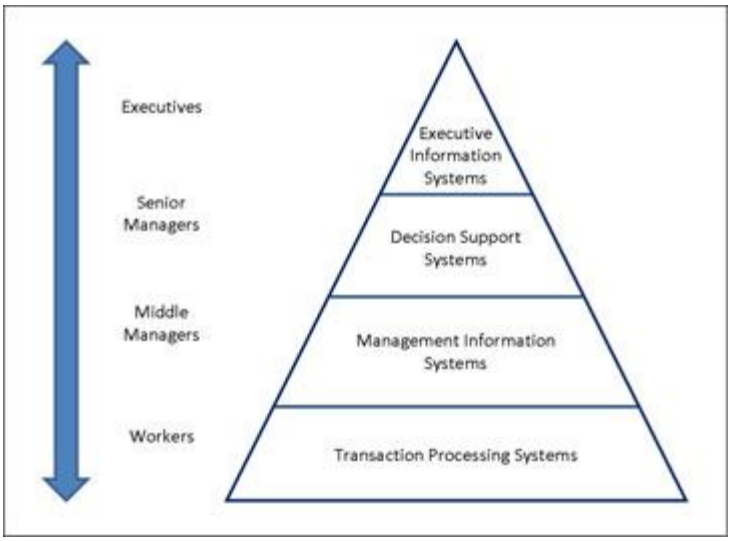
While information systems may differ in how they are used within an organization, they typically contain the following components:

1. **Hardware**: Computer-based information systems use computer hardware, such as processors, monitors, keyboard and printers.
2. **Software**: These are the programs used to organize, process and analyze data.
3. **Databases**: Information systems work with data, organized into tables and files.
4. **Network**: Different elements need to be connected to each other, especially if many different people in an organization use the same information system.
5. **Procedures**: These describe how specific data are processed and analyzed in order to get the answers for which the information system is designed.

The first four components are part of the general **information technology (IT)** of an organization. Procedures, the fifth component, are very specific to the information needed to answer a specific question.

Different Types

The many different types of information systems can be divided into categories based on where they are used in the hierarchy of an organization.



Information management is the process of **collecting, storing, and organizing data in a way that allows for efficient retrieval and use**. Its purpose is to ensure that the right information is available to the right people at the right time, in order to facilitate decision-making and support the efficient operation of an organization.

9.2. Fundamental concepts.

Protocols in the TCP/IP

TCP/IP has 4 layers Application layer. Programs use application layer protocols to access network resources. Application layer protocols include: Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) Server Message Block (SMB)Domain Name System (DNS), Post Office Protocol 3 (POP3), one –way incoming message) Simple Network Management Protocol (SNMP), (two –way incoming message) Simple Mail Transfer Protocol (SMTP).

Transport layer.

Transport layer protocols control data transfer reliability on the network. Transport layer protocols include: Transmission Control Protocol (TCP) User Datagram Protocol (UDP)

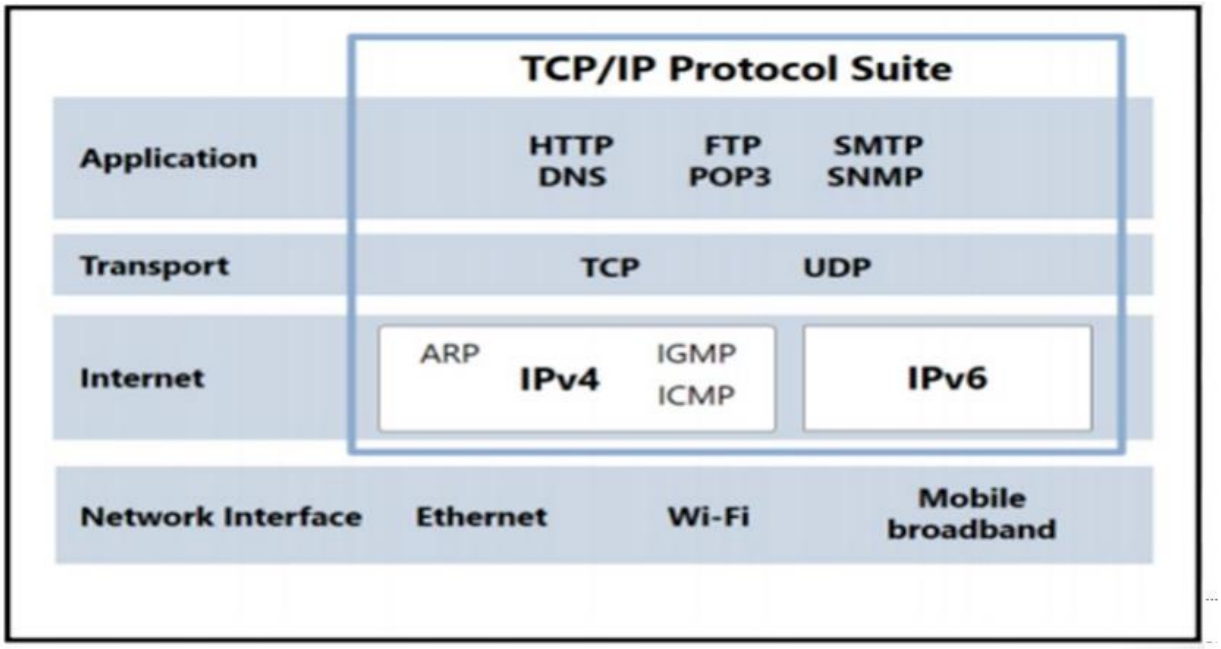
Internet layer.

The Internet layer protocols control packet movement between networks. Internet layer protocols include: Internet protocol (IP) (IPv4 and IPv6) Address Resolution Protocol (ARP) Internet Group Management Protocol (IGMP) Internet Control Message Protocol (ICMP)

Network interface layer.

The network interface layer protocols define how datagrams from the Internet layer are transmitted on the media.

Protocols in the TCP/IP Suite



What is an IP Address?

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

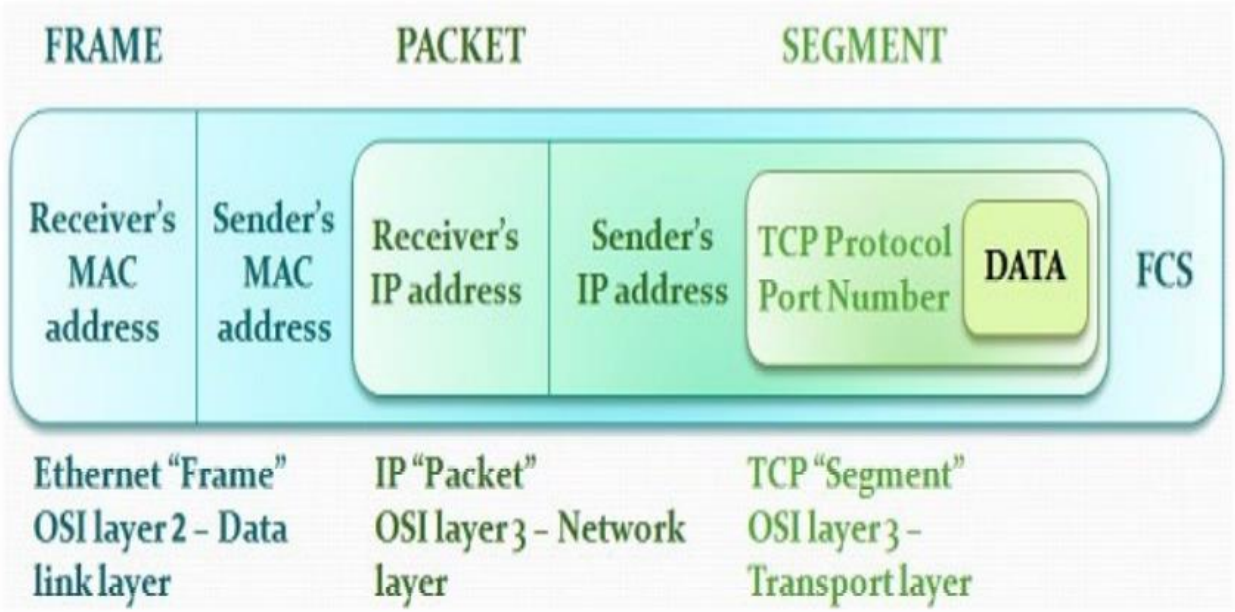
Static addressing

Assign permanent IP address Gives consistency for monitoring Can be laborious for large networks Dynamic addressing IP address assigned during logon Uses the Dynamic Host Configuration Protocol (DHCP).

Default gateway

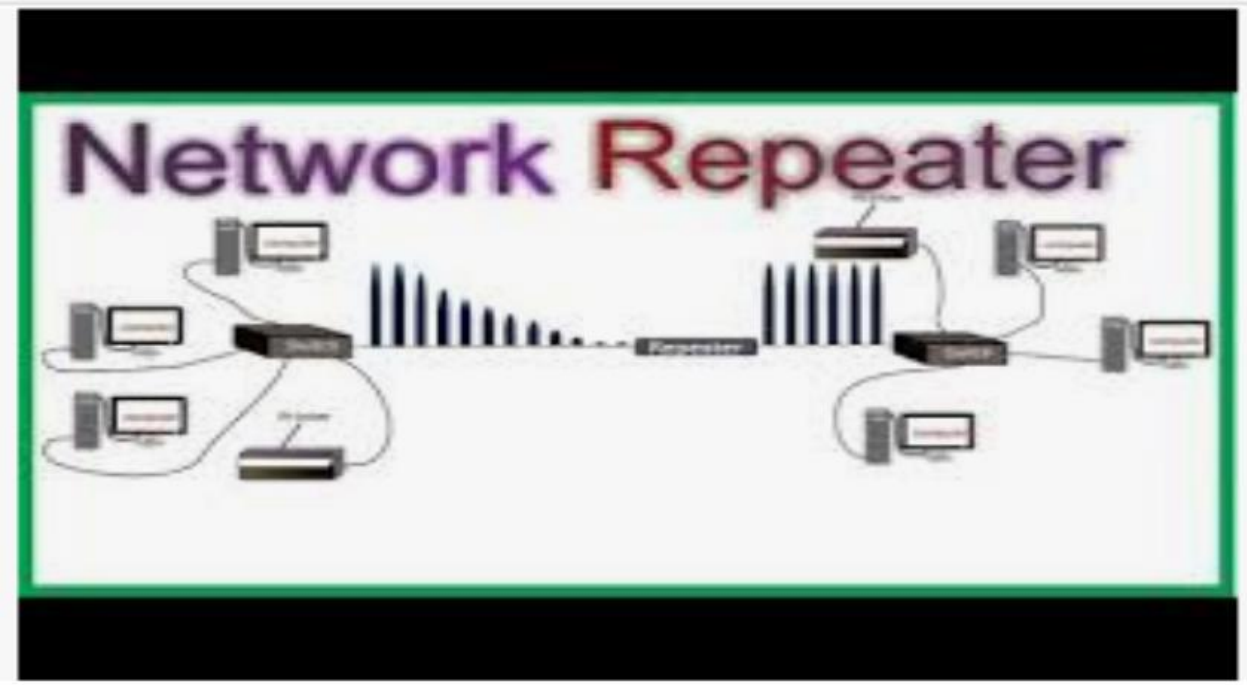
IP address of the router that has a connection to other networks. Name resolution Domain Name System (DNS) translates domain and computer names to IP addresses

frame and packet.



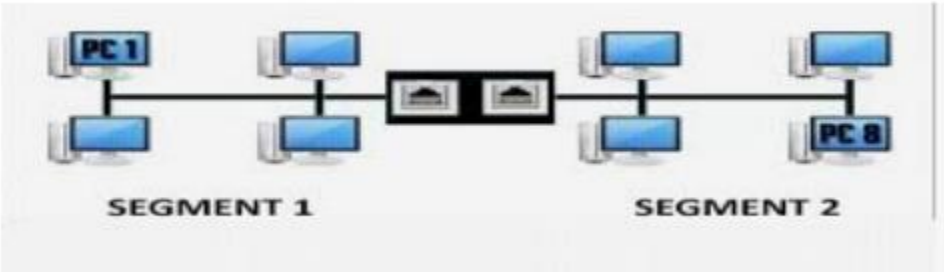
Network Devices

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.



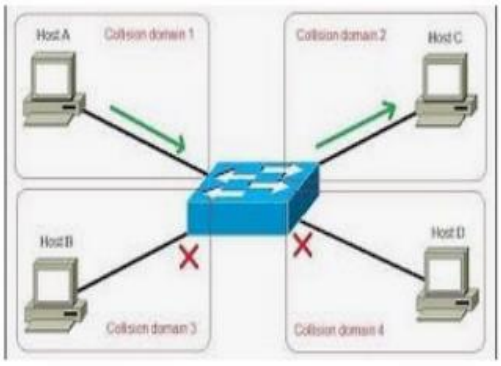
Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.

3.Bridge A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.



4. Switch

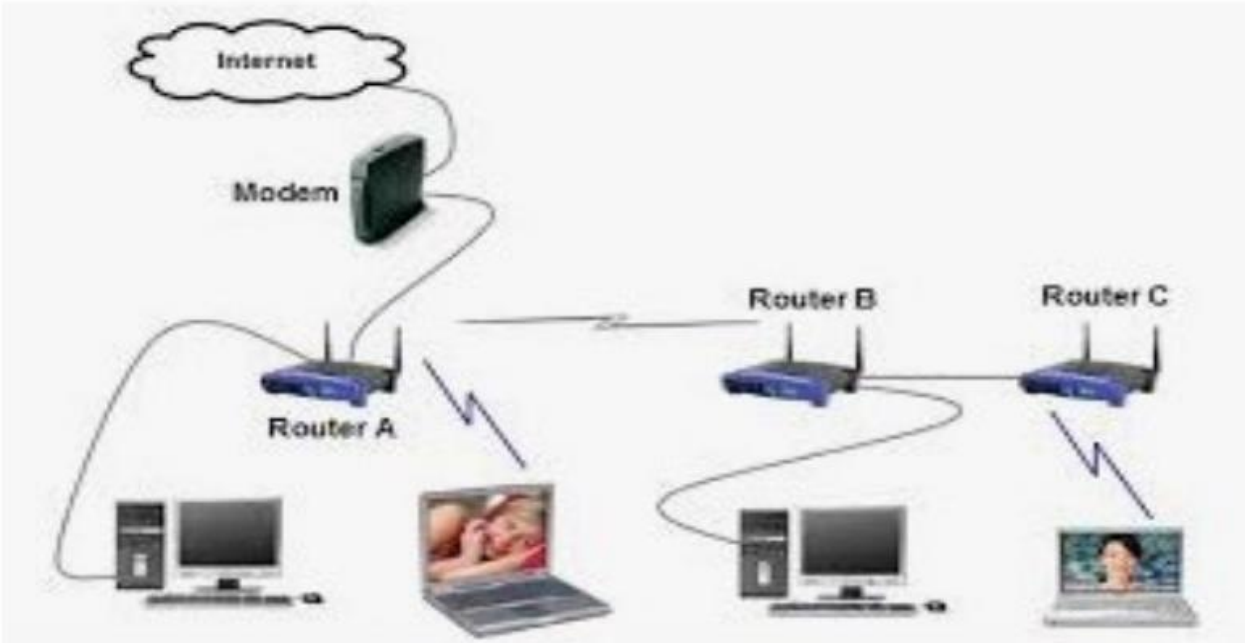
A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device.



5.Routers

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

Wireless router



6.Gateway

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.

IP addressing

An IP address is a number identifying of a computer or another device on the Internet. IPv4 vs IPv6 addresses IPv4 was deployed on ARPANET work (advanced research projects agency NET work) in 1983 and still powers most of the internet.

IPv4 addresses are 32 bits long. Four bytes

The maximum value of a 32-bit number is 2 power 32, or 4,294,967,296. So the maximum number of IPv4 addresses, which is called its address space, is about 4.3 billion.

IPv6

A major advantage of IPv6 is that it uses 128 bits of data to store an address, permitting 2 power 128 unique addresses, or 340,282,366,920,938,463,463,374,607,431,76 8,211,456. or 340 trillion unique address.

IPv6 was developed by the Internet Engineering Task Force (IETF), and was formalized in 1998. 16-byte, addresses that means 340 trillion address. IP addresses are globally managed by Internet Assigned Numbers Authority (IANA) and regional Internet registries (RIR).

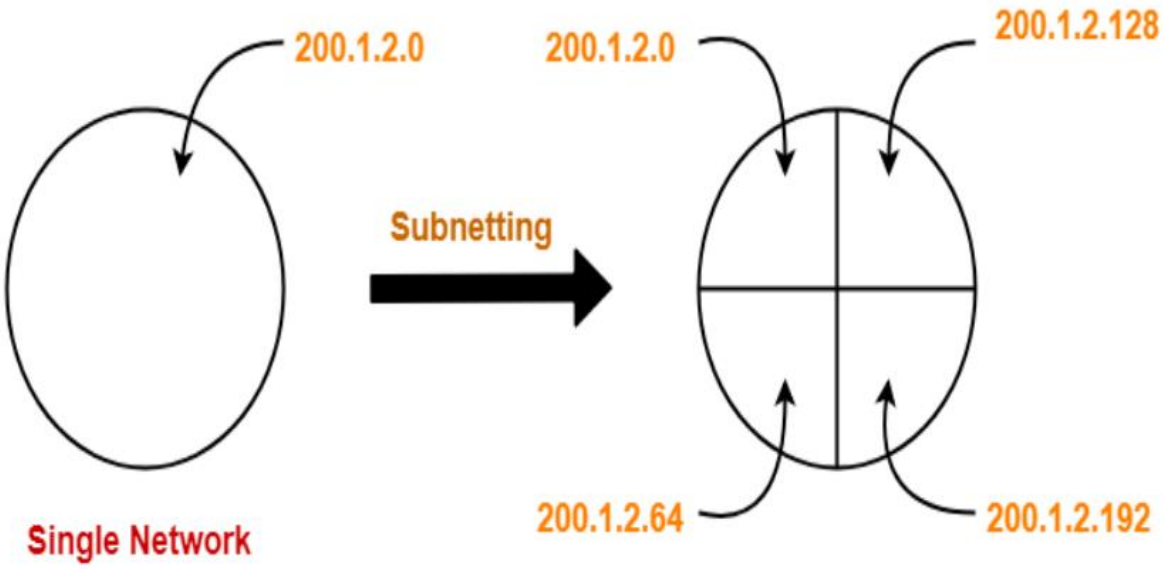
Subnets and Super nets

Subnets provide a way of chopping/slicing up or Splitting large networks into smaller entities. Networks might be split up to segment traffic. Networks might be split up to facilitate better use of an assigned IP address space.

What is IP Subnetting?

IP Subnetting is a process of dividing a large IP network in smaller IP networks. In Subnetting we create multiple small manageable networks from a single large IP network.

Subnetting example



For 1st Subnet-

- IP Address of the subnet = 200.1.2.0
- Total number of IP Addresses = 2^6 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**00**000000, 200.1.2.**00**111111] = [200.1.2.0, 200.1.2.63]
- Direct Broadcast Address = 200.1.2.**00**111111 = 200.1.2.63
- Limited Broadcast Address = 255.255.255.255

For 2nd Subnet-

- IP Address of the subnet = 200.1.2.64
- Total number of IP Addresses = 2^6 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**01**000000, 200.1.2.**01**111111] = [200.1.2.64, 200.1.2.127]
- Direct Broadcast Address = 200.1.2.**01**111111 = 200.1.2.127
- Limited Broadcast Address = 255.255.255.255

For 3rd Subnet-

- IP Address of the subnet = 200.1.2.128
- Total number of IP Addresses = 2^6 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**10**000000, 200.1.2.**10**111111] = [200.1.2.128, 200.1.2.191]
- Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
- Limited Broadcast Address = 255.255.255.255

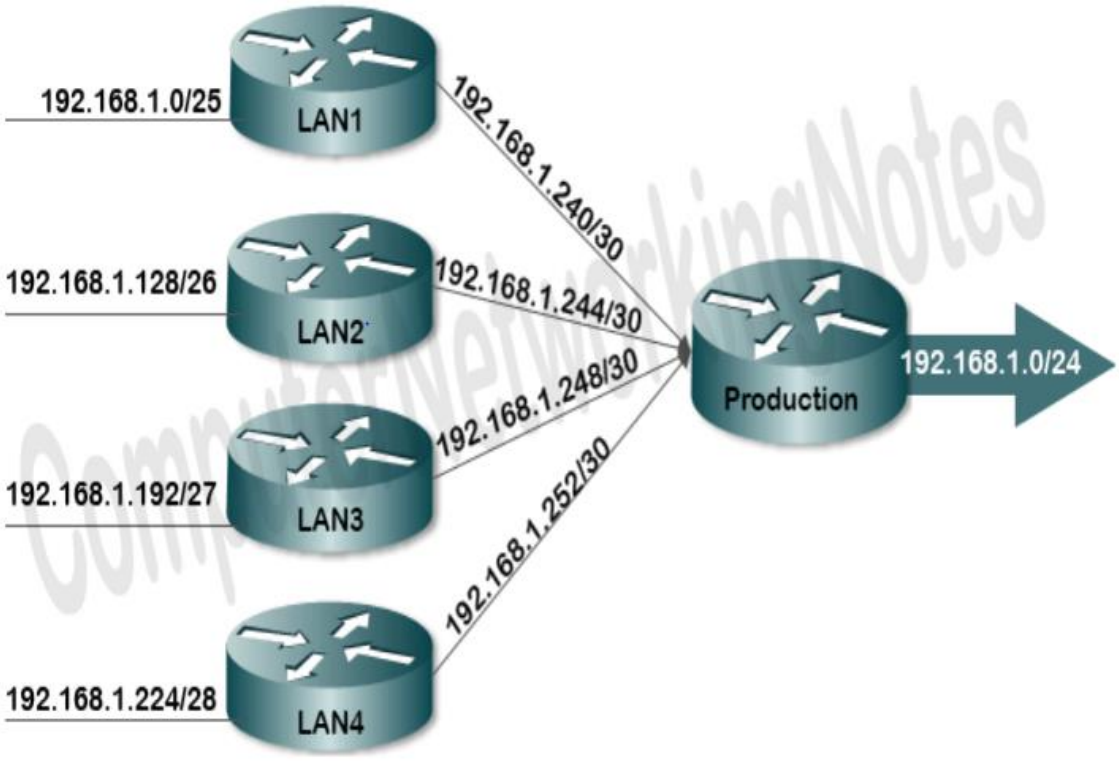
For 4th Subnet-

- IP Address of the subnet = 200.1.2.192
- Total number of IP Addresses = 2^6 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**11**000000, 200.1.2.**11**111111] = [200.1.2.192, 200.1.2.255]
- Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
- Limited Broadcast Address = 255.255.255.255

What is Super netting

Super netting is the process of summarizing a bunch of contiguous Sub netted networks back in a single large network. Super netting is also known as route summarization and route aggregation.

Super netting example



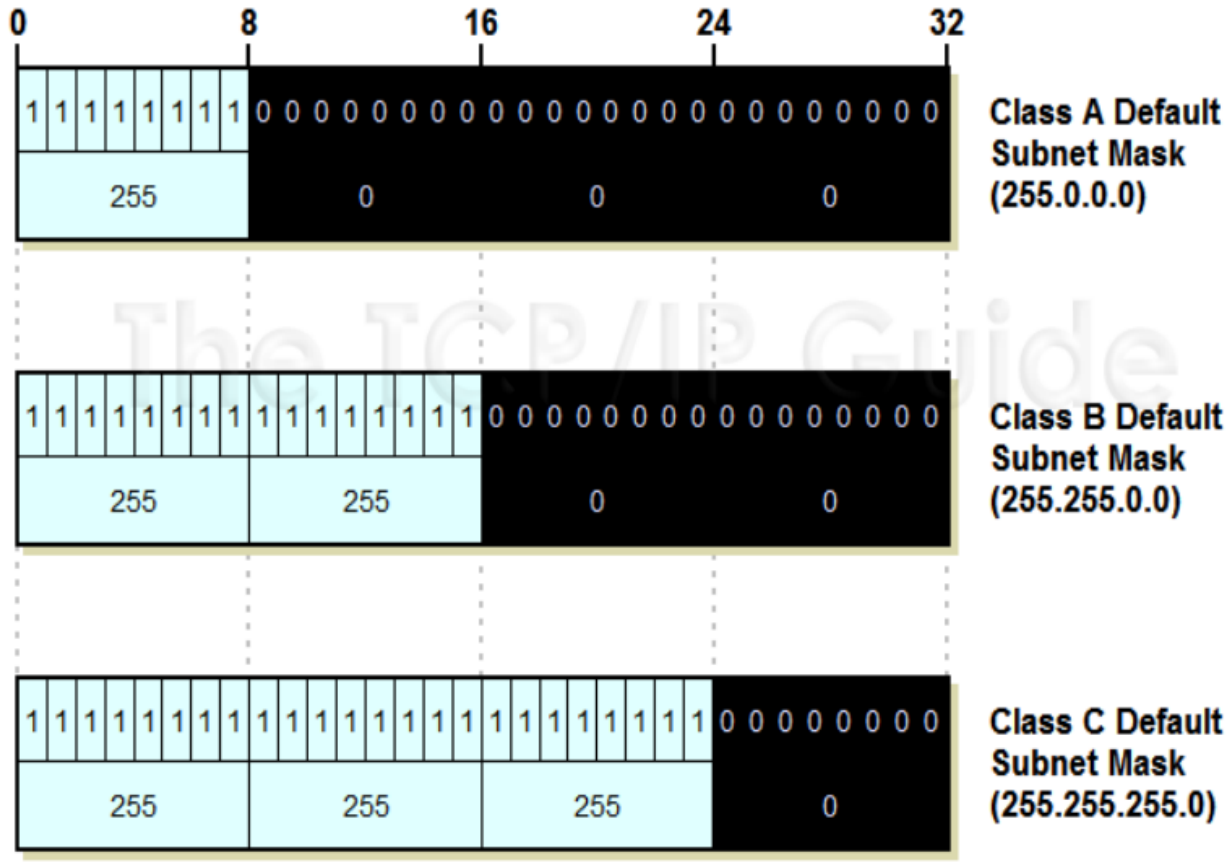
IP address Classes

Class	FIrst octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-

subnet mask

A subnet mask is a number that defines a range of IP addresses available within a network. A subnet mask hides (or masks) the network part of a system's IP address and leaves only the host part as the machine identifier.

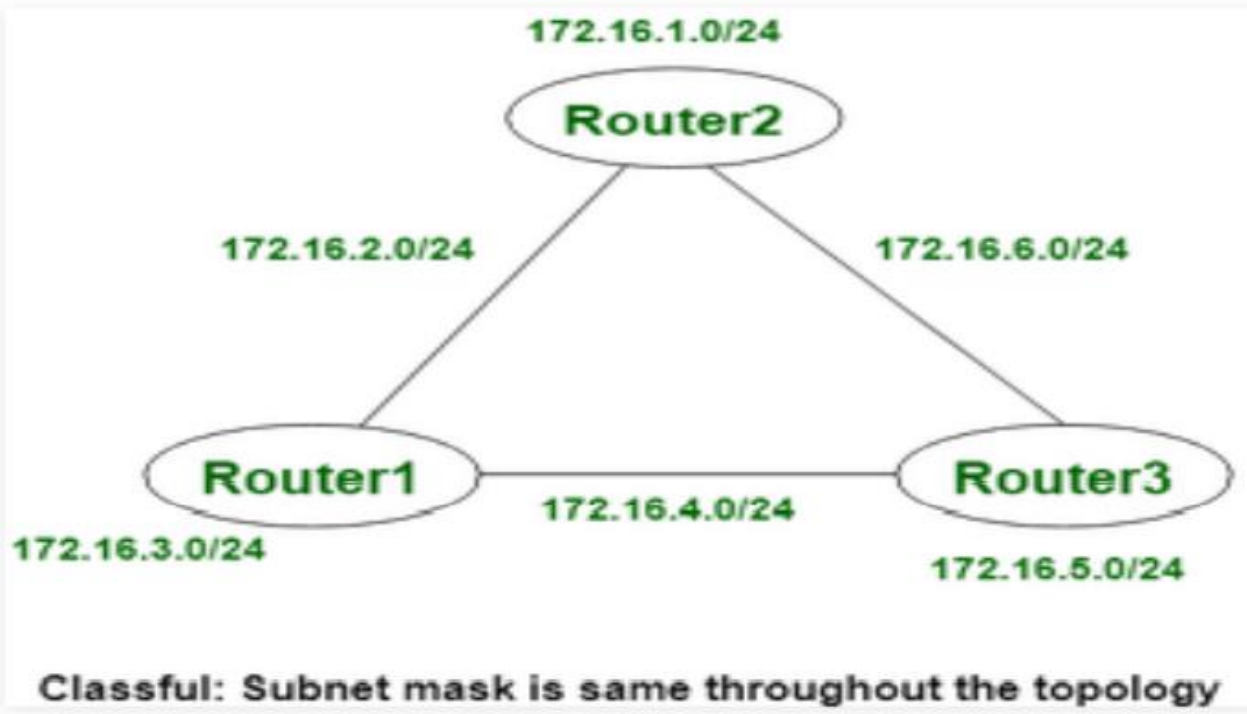
IP Address Class	Total # Of Bits For Network ID / Host ID	Default Subnet Mask			
		First Octet	Second Octet	Third Octet	Fourth Octet
Class A	8 / 24	11111111 (255)	00000000 (0)	00000000 (0)	00000000 (0)
Class B	16 / 16	11111111 (255)	11111111 (255)	00000000 (0)	00000000 (0)
Class C	24 / 8	11111111 (255)	11111111 (255)	11111111 (255)	00000000 (0)



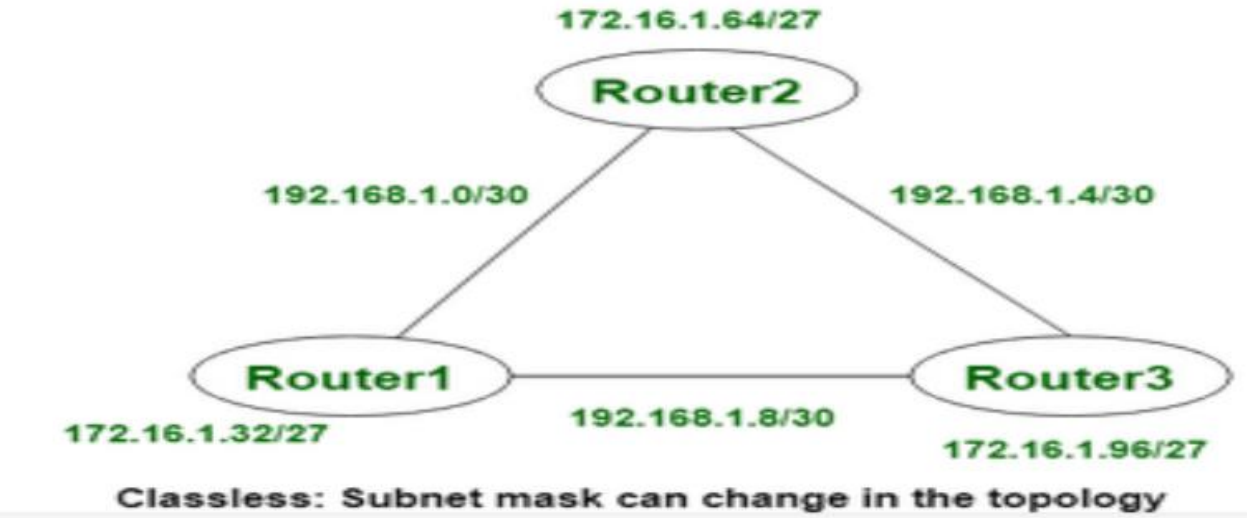
What is Sub netting?

Sub netting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet. Classful IP addressing does not provide any flexibility of having a smaller number of Hosts per Network or more Networks per IP Class. CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet.

Classful /FLSM



CLDR/VLSM



By using subnetting, one single Class A IP address can be used to have smaller subnetworks (128) which provides better network management capabilities.

Class A Subnets

in Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly. For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2 the power of 1 =2) with (2 the power of 23-2) 8388606 Hosts per Subnet.

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254

25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (2 power of 14 (usable) 16384 /65,536 Networks and (2 power of 16-2) 65,534 Hosts. Class B IP Addresses can be sub netted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting.

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of sub netted Class C IP address.

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Example 1 Now that you understand subnetting, put this knowledge to use. In this example, you are given two addresses / mask combinations, written with the prefix/length notation, which have been assigned to two devices. Your task is to determine if these devices are on the same subnet or different subnets. You can use the address and mask of each device in order to determine to which subnet each address belongs. Device A: 172.16.17.30/20 Device B: 172.16.28.15/20 Determine the Subnet for Device A:

172.16.17.30 - 10101100.00010000.00010001.00011110

255.255.240.0 - 11111111.11111111.11110000.00000000

----------| sub|----------

Subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0

Looking at the address bits that have a corresponding mask bit set to one, and setting all the other

address bits to zero (this is equivalent to performing a logical "AND" between the mask and address),

shows you to which subnet this address belongs. In this case, Device A belongs to subnet 172.16.16.0.

Determine the Subnet for Device B:

172.16.28.15 - 10101100.00010000.00011100.00001111

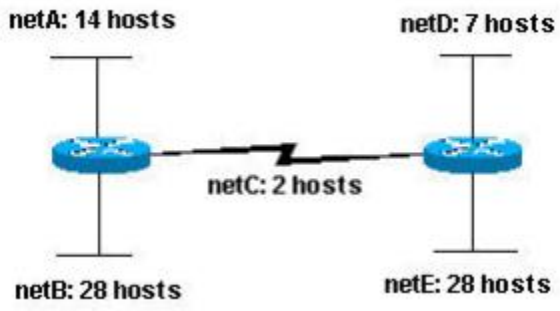
255.255.240.0 - 11111111.11111111.11110000.00000000

----------| sub|----------

Subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0

From these determinations, Device A and Device B have addresses that are part of the same subnet.

Example 2 Given the Class C network of 204.15.5.0/24, subnet the network in order to create the network in the below figure with the host requirements shown.



Looking at the network shown in the above figure, you can see that you are required to create five subnets. The largest subnet must support 28 host addresses. Is this possible with a Class C network? If so, then how? You can start by looking at the subnet requirement. In order to create the five needed subnets, you would need to use three bits from the Class C host bits. Two bits would only allow you four subnets (22).

Since you need three subnet bits that leaves you with five bits for the host portion of the address, how

many hosts do this support? 25

= 32 (30 usable). This meets the requirement.

Therefore, you have determined that it is possible to create this network with a Class C network. An example of how you might assign the subnetworks is:

netA: 204.15.5.0/27 host address range 1 to 30

netB: 204.15.5.32/27 host address range 33 to 62

netC: 204.15.5.64/27 host address range 65 to 94

netD: 204.15.5.96/27 host address range 97 to 126

netE: 204.15.5.128/27 host address range 129 to 158

Example 3

Here is a scenario where subnetting is needed. Pretend that a web host with a Class C network needs to divide the network so that parts of the network can be leased to its customers. Let's assume that a host has a network address of 216.3.128.0. Let's say that we're going to divide the network into 2 and dedicate the first half to itself, and the other half to its customers.

216. 3. 128. (0000 0000) (1st half assigned to the web host)

216. 3. 128. (1000 0000) (2nd half assigned to the customers)

The web host will have the subnet mask of 216.3.128.128 (/25). Now, we'll further divide the 2nd

half into eight blocks of 16 IP addresses.

216. 3. 128. (1000 0000) Customer 1 -- Gets 16 IPs (14 usable)

216. 3. 128. (1001 0000) Customer 2 -- Gets 16 IPs (14 usable)

216. 3. 128. (1010 0000) Customer 3 -- Gets 16 IPs (14 usable)

216. 3. 128. (1011 0000) Customer 4 -- Gets 16 IPs (14 usable)

216. 3. 128. (1100 0000) Customer 5 -- Gets 16 IPs (14 usable)

216. 3. 128. (1101 0000) Customer 6 -- Gets 16 IPs (14 usable)

216. 3. 128. (1110 0000) Customer 7 -- Gets 16 IPs (14 usable)

216. 3. 128. (1111 0000) Customer 8 -- Gets 16 IPs (14 usable)

---

255. 255. 255. (1111 0000) (Subnet mask of 255.255.255.240)

9.4. Wireless LAN

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building.

This gives users the ability to move around within the area and remain connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet

What is a Wi-Fi or wireless network vs. a wired network?

A wireless network allows devices to stay connected to the network but roam untethered (not connected) to any wires. Access points amplify Wi-Fi signals, so a device can be far from a router but still be connected to the network.

When you connect to a Wi-Fi hotspot at a cafe, a hotel, an airport lounge, or another public place, you're connecting to that business's wireless network.

A wired network uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network. A wired network has some disadvantages when compared to a wireless network.

biggest disadvantage is that your device is tied to a router. The most common wired networks use cables connected at one end to an Ethernet port on the network router and at the other end to a computer or other device.

an ad-hoc network

From Latin meaning "for this," an ad-hoc network is a makeshift chain of devices that can connect and communicate directly with one another at the time of need.

Point-to-point (telecommunications)

In telecommunications, a point-to-point connection refers to a communications connection between two communication endpoints or nodes. An example is a telephone call, in which one telephone is connected with one other, and what is said by one caller can only be heard by the other.

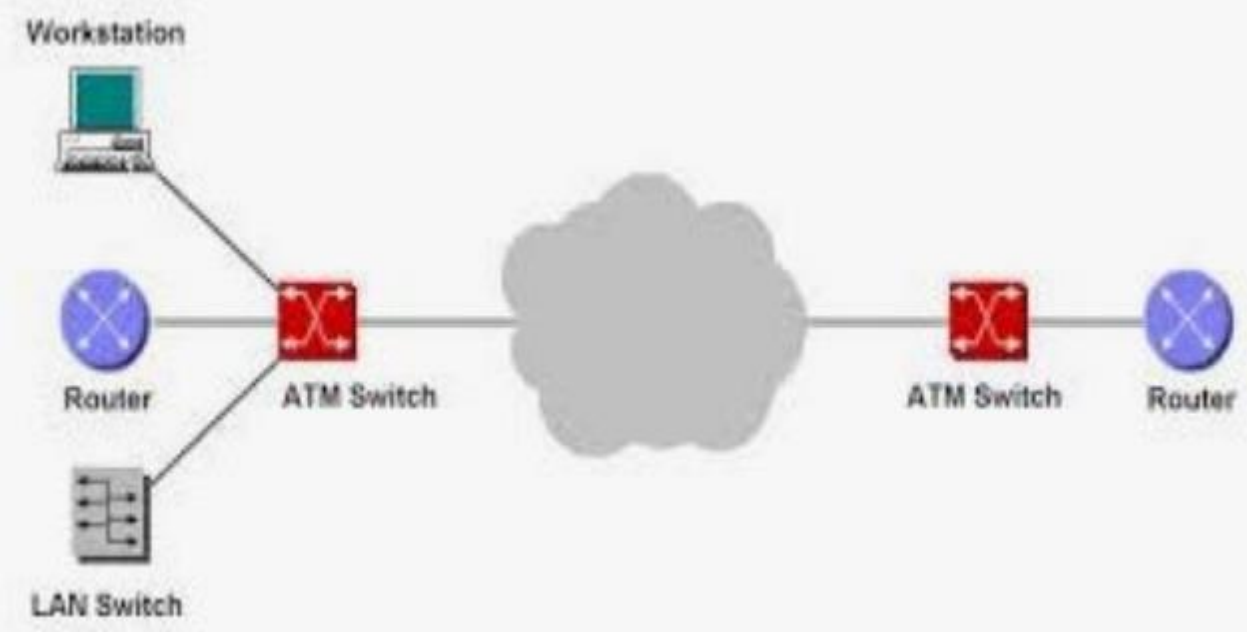
Integrated Services Digital Network (ISDN)

ISDN is a circuit-switched telephone network system, but it also provides access to packet switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s.


ISDN telephone

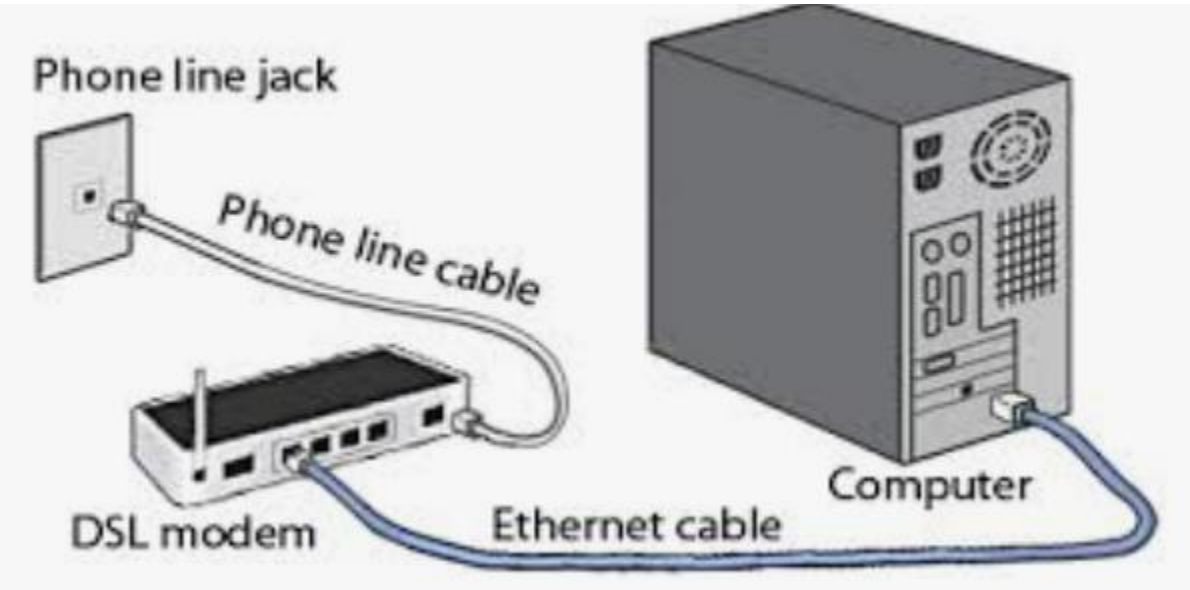
Asynchronous Transfer Mode (ATM)

It is an International Telecommunication Union Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video or voice which is conveyed in small fixed size packets called cells.



DSL (Digital Subscriber Line)

DSL (Digital Subscriber Line) is a modem technology that uses existing telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. DSL provides dedicated, point-to-point, public network access.

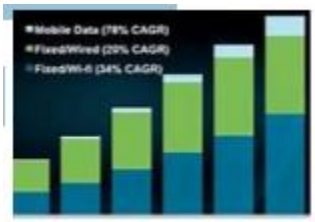


9.3. Network design and implementation

Network design requirements. Most businesses actually have only a few requirements for their network (Scalability, Availability, Security, Manageability): The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.

Network scalability

Scalability is the ability of a network to cope with increasing workloads in a cost-effective and sustainable way, by expanding the network's bandwidth capacity and supporting its physical expansion to new development areas.



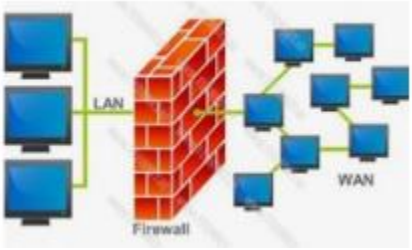
Network availability

Network availability is the amount of uptime in a network system over a specific time interval. Uptime refers to the amount of time a network is fully operational. Network availability is calculated by dividing the uptime by the total time in any period.

The goal is 100% availability, although another commonly referenced goal is known as "five nines," or 99.999% availability. That's the equivalent of only a few minutes of downtime in a year.

Network security

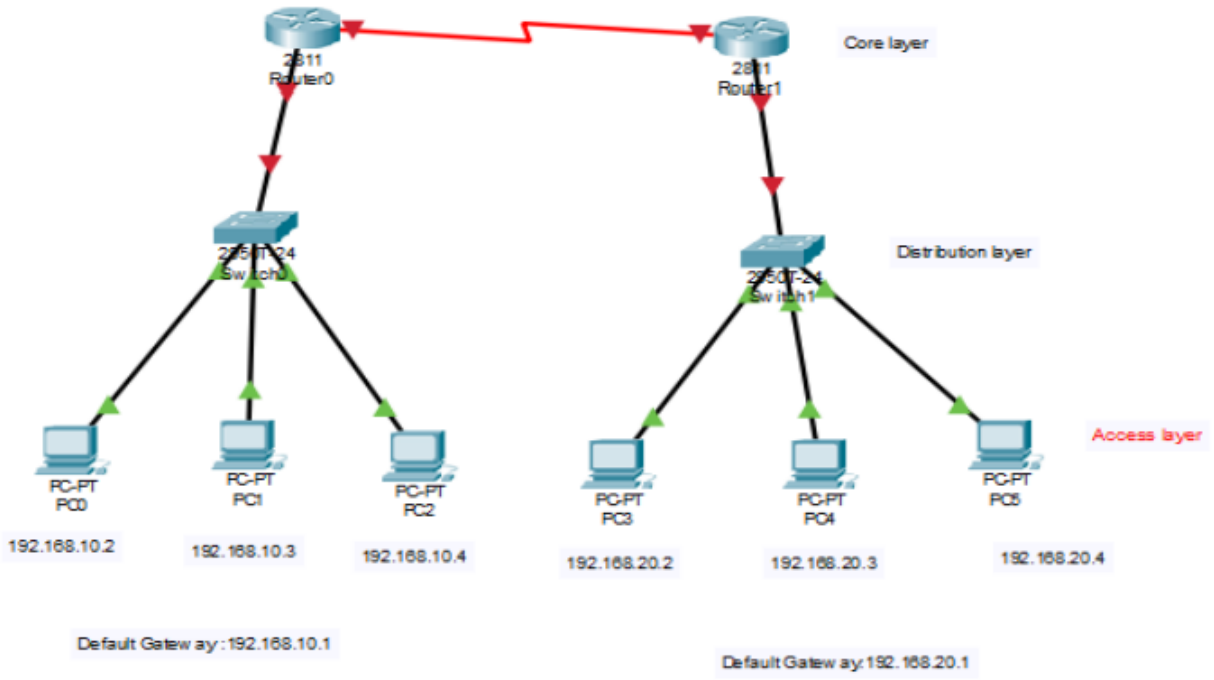
Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.



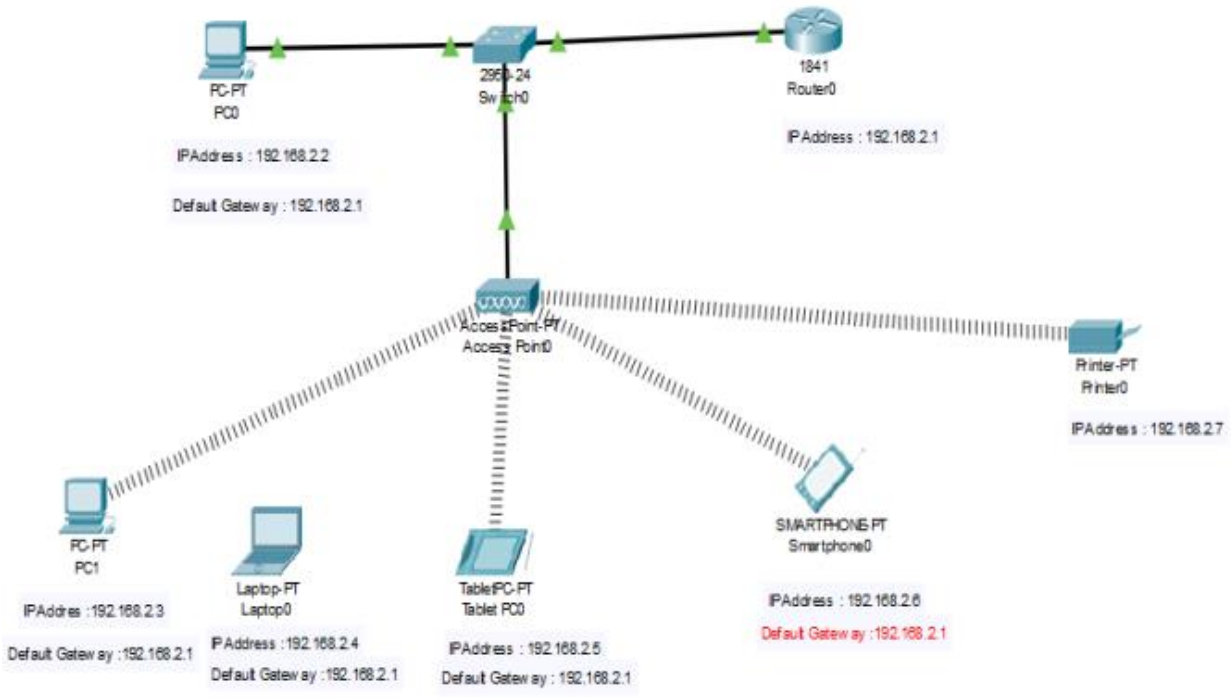
Network manageability

The ability to effectively operate, monitor and control an entire network is the domain of network management. Network management is a multifaceted discipline that provides network administrators with network management tools, protocols and processes to empower optimized network operations.

Router configuration



Wireless network configuration



Hierarchical Network Design

Core Layer - Connects Distribution Layer devices. Also called network backbone. Distribution Layer - Interconnects the smaller local networks Access Layer - Provides connectivity for network hosts and end devices.

Network design methodology

Large network design projects are normally divided into three distinct steps: Step 1: Identify the network requirements. Step 2: Characterize the existing network. Step 3: Design the network topology and solutions.

Identifying Network Requirements

The network designer works closely with the customer to document the goals of the project. Goals are usually separated into two categories: Business goals - Focus on how the network can make the business more successful Technical requirements - Focus on how the technology is implemented within the network.

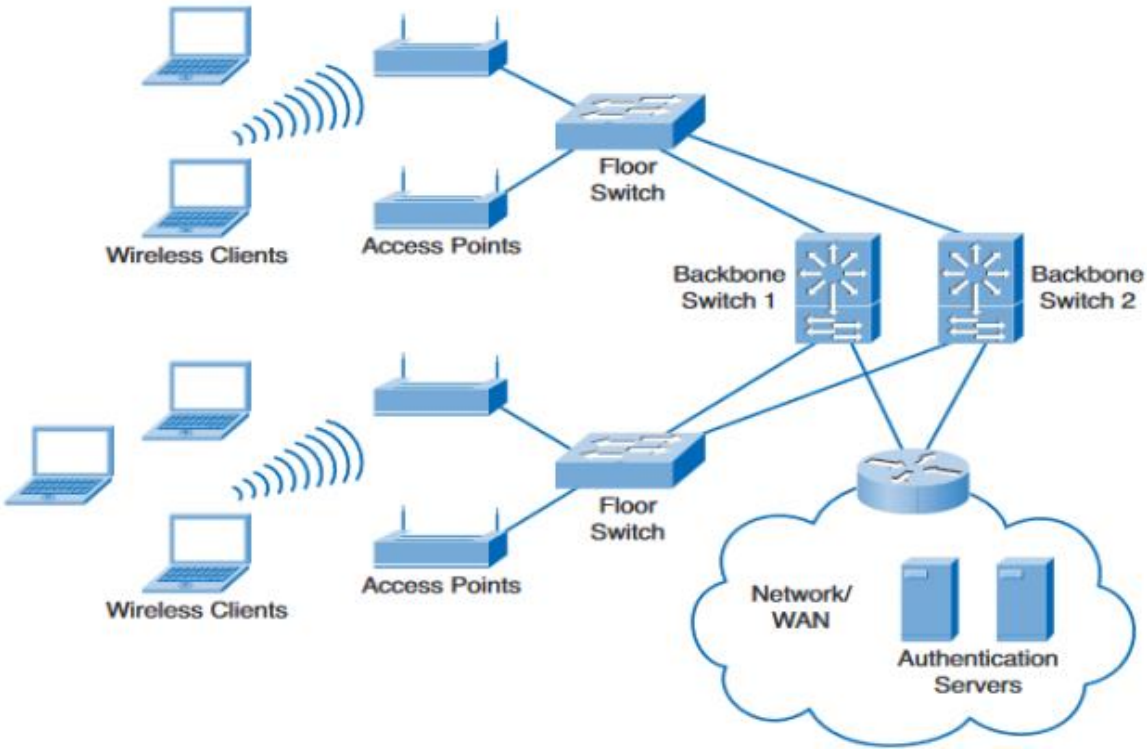
Characterizing the Existing Network

Information about the current network and services is gathered and analyzed. It is necessary to compare the functionality of the existing network with the defined goals of the new project. The designer determines whether any existing equipment, infrastructure, and protocols can be re-used, and what new equipment and protocols are needed to complete the design.

Designing the Network Topology

A common strategy for network design is to take a top-down approach. In this approach, the network applications and service requirements are identified, and then the network is designed to support them. When the design is complete, a prototype or proof of-concept test is performed

WLAN Topology



Determining the Scope of the Project

While gathering requirements, the designer identifies the issues that affect the entire network and those that affect only specific portions. Failure to understand the impact of a particular requirement often causes a project scope to expand beyond the original estimate.

This oversight can greatly increase the cost and time required to implement the new design. The new project can be: Impacting the Entire Network Impacting a Portion of the Network.

The Core Layer includes one or more links to the devices at the enterprise edge in order to support Internet, Virtual Private Networks (VPNs), extranet, and WAN access. Goals of the Core Layer Provide 100% uptime Maximize throughput • Facilitate network growth

Preventing Failures

The network designer must strive to provide a network that is resistant to failures and can recover quickly in the event of a failure. Core routers and switches can contain:

Dual power supplies and fans A modular chassis-based design Additional management modules Reducing Human Error Failures at the Core Layer cause widespread outages. It is critical to have

written policies and procedures in place to govern how changes are approved, tested, installed, and documented.

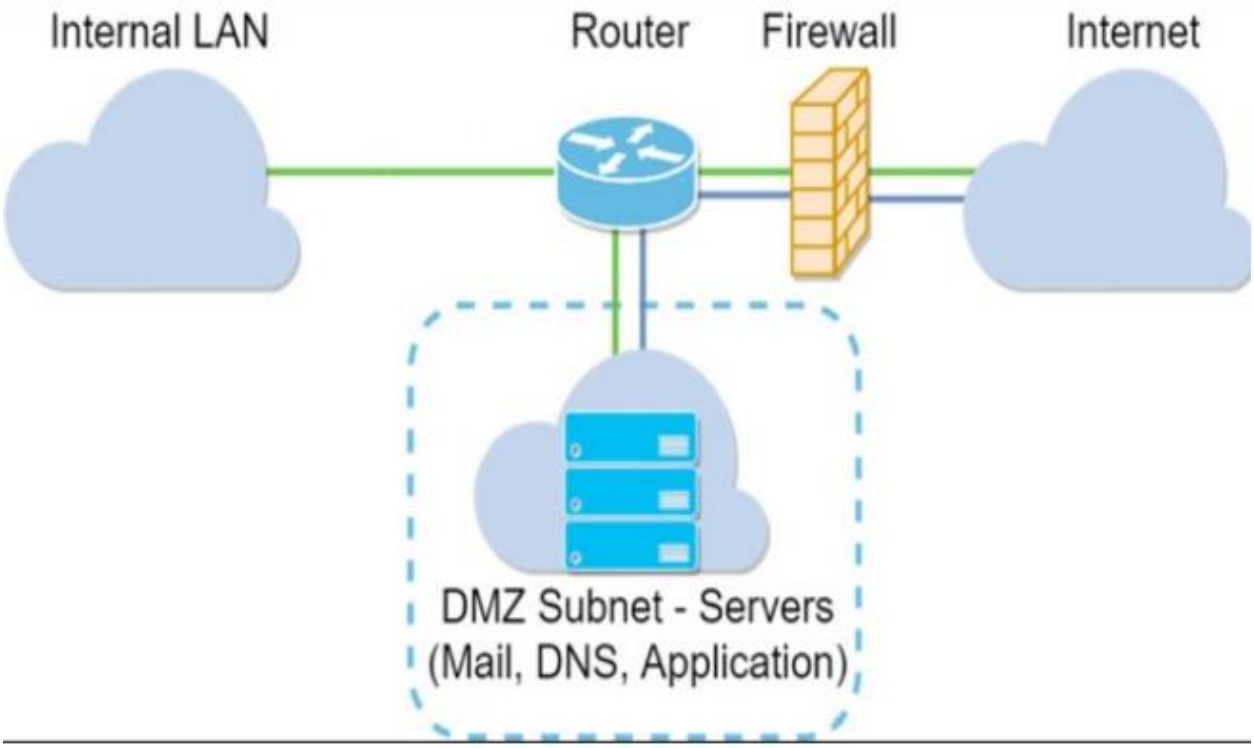
Design Considerations

Most networks contain a combination of dynamic and static routes. Network designers need to consider the number of routes required to ensure that all destinations in the network are reachable.

Large routing tables can take significant time to converge. The design of network addressing and summarization strategies in all layers affects how well the routing protocol can react to a failure.

Demilitarized Zones

In the traditional network firewall design, servers that needed to be accessed from external networks were located on a demilitarized zone (DMZ). LAN users were treated as trusted users and usually had few restrictions imposed when they accessed servers on the DMZ.



Secured Employee Access

To secure employee access, use an entirely separate WLAN infrastructure that does not include guest access. The recommended practice is to separate the internal users on a different VLAN.

Other wireless implementation recommended practices include: Non-broadcast SSID Strong encryption User authentication Virtual private network (VPN) tunneling for sensitive data Firewall and intrusion prevention/IDS

9.4. LINUX SYSTEM AND NETWORK ADMINISTRATION

How to determine risk?

“Risk Assessment” Identify assets Identify threats Identify vulnerabilities Determine likelihood of damage Estimate cost of recovery Estimate cost of defense A risk is the likelihood of a threat successfully exploiting a vulnerability and the estimated cost (or potential damage) both in the short and long term you may incur as a result.

System Security

The thing that makes security difficult is not the software or hardware components. It’s the human component. Users care about usability, not about security, Users will not change their default settings. Giving freedom is easier than taking it away.

System Security

The thing that makes security difficult is not the software or hardware components. It’s the human component. Users care about usability, not about security. Users will not change their default settings. -Giving freedom is easier than taking it away.

Encryption

Encryption can help mitigate some of the risks sometimes. It may provide security in the areas of: 1. Secrecy or Confidentiality Did/could anybody else see (parts of) the message? 2. Accuracy or Integrity Was the message (could it have been) modified before I received it? 3. Authenticity - Is the party I’m talking to actually who I think it is / they claim they are?

UNIX

Unix is a multi-user, multi-tasking operating system You can have many users logged into a system simultaneously, each running many programs. It's the kernel's job to keep each process and user separate and to regulate access to system hardware, including cup, memory, disk and other I/O devices.

What is LINUX

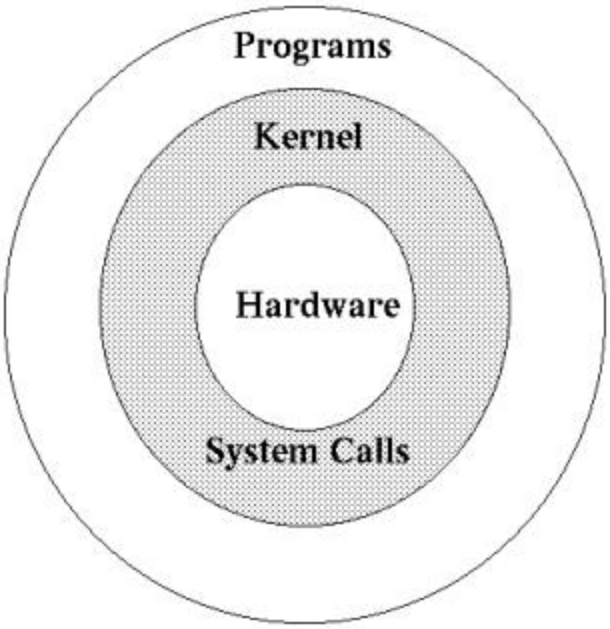
Linux is a free Unix-type operating system originally created by Linus Torvalds with the assistance of developers around the world. It originated in 1991 as a personal project of Linus Torvalds, a graduate student. The Kernel version 1.0 was released in 1994 and today the most recent stable version is 2.6.9 Developed under the GNU General Public License, the source code for Linux is freely available to everyone.

LINUX Distributions

Mandrake: http://www.mandrakesoft.com/ RedHat: http://www.redhat.com/ Fedora: http://fedora.redhat.com/ SuSE/Novell: http://www.suse.com/ Debian: http://www.debian.org/

Red Hat Enterprise Linux is an Enterprise targeted Operating System. It based on mature Open Source technology and available at a cost with one-year Red Hat Network subscription for upgrade and support contract.

UNIX Structure



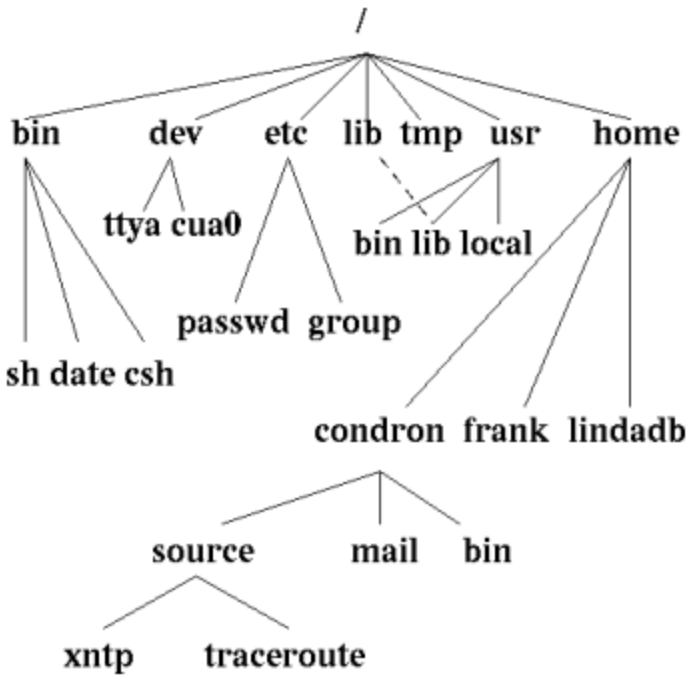
unicast, multicast, broadcast, any cast

A unicast communication originates from one computer and is destined for exactly one other computer (or host). A multicast is destined for a group (of computers). A broadcast is meant for everyone. An anycast signal goes the (geographically) nearest of a well-defined group.

Linux Resource Monitoring & Management

Most Linux distributions are equipped with tons of monitoring. These tools provide metrics which can be used to get information about system activities. You can use these tools to find the possible causes of a performance problem.

UNIX File System



File System

The Unix file system looks like an inverted tree structure. You start with the root directory, denoted by /, at the top and work down through sub-directories underneath it.

Each node is either a file or a directory of files, where the latter can contain other files and directories. You specify a file or directory by its path name, either the full, or absolute, path name or the one relative to a location. The full path name starts with the root, /, and follows the branches of the file system, each separated by /, until you reach the desired file, e.g.: /home/Condron/source/xntp

A relative path name specifies the path relative to another, usually the current working directory that you are at. Two special directories: the current directory the parent of the current directory So if I'm at /home/frank and wish to specify the path above in a relative fashion I could use: /condron/source/xntp This indicates that I should first go up one directory level, then come down through the condron directory, followed by the source directory and then to xntp.

Structure of Standard Directories in Unix/Linux

The ancestor of all directories on the system; all other directories are subdirectories of this directory, either directly or through other subdirectories. Most Linux systems however, follow a general convention for file system organization at the highest level. /(root):- The top level directory referred to as root. Contains all files in the file system. /bin:- Executable files for standard UNIX utilities. /dev:- Files that represent devices. For example, you use the file `/dev/cdrom' to access the CD−ROM drive.

Standard Linux File System

/etc:- Miscellaneous and system administrative files such as the password file and system start up files. – /lib:- UNIX program libraries. – /tmp:- Temporary space that can be used by programs or users. – /usr:-used to store any files that are common to all users on the system.

– /u:- User home directories. – /var:- Variable sized files. – /home:- directory in which every user on the system has his own personal folder for his own personal files. (my documents in window) – /mnt:- it is a mounted device. All storage device is mounted to use in the linux. – /proc:-a deluxe version of the Windows Task Manager. It holds all the information about your system's processes and resources.

Directories, Files and Inodes

Every directory and file is listed in its parent directory. In the case of the root directory, that parent is itself. A directory is a file that contains a table listing the files contained within it, giving file names to the inode numbers in the list. The information about all the files and directories is maintained in INODE TABLE An Inode (Index Nodes) is an entry in the table containing information about a including file permissions, UID, file (metadata) GID, size, time stamp, pointers to files data blocks on the disk etc.

Users, Groups and Access Permissions

In UNIX/LINUX, there is a concept of user and an associated group the system determines whether or not a user or group can access a file or program based on the permissions assigned to them. Apart from all the users, there is a special user called Super User or the root which has permission to access any file and directory.

Access Permissions

There are three permissions for any file, directory or application program. The following lists the symbols used to denote each, along with a brief description: r - Indicates that a given category of user can read a file. w — Indicates that a given category of user can write to a file. x — Indicates that a given category of user can execute the file.

Each of the three permissions are assigned to three defined categories of users. The categories are: owner group — The owner of the file or application. — The group that owns the file or application. others — All users with access to the system.

One can easily view the permissions for a file by invoking a long format listing using the command ls -l. For instance, if the user juan creates an executable file named test, the output of the command ls -l test would look like this: -rwxrwxrwx 1 juan student 0 Sep 26 12:25 test

The permissions for this file are listed at the start of the line, starting with rwx. This first set of symbols define owner access. The next set of rwx symbols define group access the last set of symbols defining access permitted for all other users.

This listing indicates that the file is readable, writable, and executable by the user who owns the file (user juan) as well as the group owning the file (which is a group named student). The file is also world-readable and world- executable, but not world-writable.

Listing the Content of a Directory

ls is used to list the contents of a directory. If the command ls is written with parameter –l then the command lists contents of the working directory with details. Example: $ ls –l

Moving in Directories

cd try_it Changes the directory to try_it pwd Prints present working directory (e.g. /home/smith/try_it) cd .. Move to superior directory pwd : Prints /home/smith cd /home The absolute path pwd : Prints /home cd The system is returned to the user home directory pwd : Print /home/smith.

Make Directory

The command mkdir my_dir makes new directory my_dir (the path is given relative) as a subdirectory of the current directory.

Remove Directory

The command rmdir your_dir removes directory your_dir if it is empty.

Copy File

The command cp file_1 file_2 copies file_1 to file_2. The both files must be in the same working directory. If they are in various directories, the path must be given.

Rename and/or Move the File

The command mv file_1 file_2 moves file_1 to file_2 both files must be in the same working directory. If they are in different directories, the path must be given. The file_1 is removed from the disk.

Remove File

The command rm file_a removes the file_a from the system If you use wildcard. For example, rm h*c you will remove all files beginning with h and ending with c which are in working directory. If you write rm *

you will erase all files from your working directory.

Access Permission of File/Directory

The ownership of the file or directory can be changed using the command chown the group of the file or directory can be changed using the command chgrp The permissions of the file can be changed using chmod command chmod -R ### -R is optional and when used with directories will traverse all the sub-directories of the target directory changing ALL the permissions to ###.

Access Permission of File/Directory

The #'s can be:

0 = Nothing
1 = Execute
2 = Write
3 = Execute & Write (2 + 1)
4 = Read
5 = Execute & Read (4 + 1)
6 = Read & Write (4 + 2)
7 = Execute & Read & Write (4 + 2 + 1)

Linux system Resource and performance Monitoring

Monitoring your Linux system is of paramount importance to **keep it running** in **top condition** and **keep it from catastrophic**.

Some of the basic things we must have to monitor:-

- **The utilization of the hard disk**
- **Memory or RAM**
- **CPU**
- **The running processes**
- **The network traffic**

1. Monitoring the Hard Disk Space

Use a simple command like:

df -h

This results in the **output**:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	22G	5.0G	16G	24%	/
/dev/sda2	34G	23G	9.1G	72%	/home

System and Network Administration

9.5. Network Administration

What is administration?

Merriam Webster: administer, v: to manage or supervise the execution, use, or conduct of something. In this regard, the main issues are the following: System plan and design Resource management (checking and repair) Fault diagnosis handing

System administration

Is a set of functions that: – Provides support services – Ensures reliable operations – Promotes efficient use of the system – Ensures that prescribed service-quality objectives are met • System administration functions includes installation, configuration, and maintenance of network equipment and computer systems. – Network equipment switches, routers, DHCP, DNS servers, etc. – Computer systems database, email server, web server

Is the branch of engineering that is responsible for maintaining reliable computer systems in a multi-user environment A person who works as a system administration is called system administrator, or sys admin.

Systems Administration…

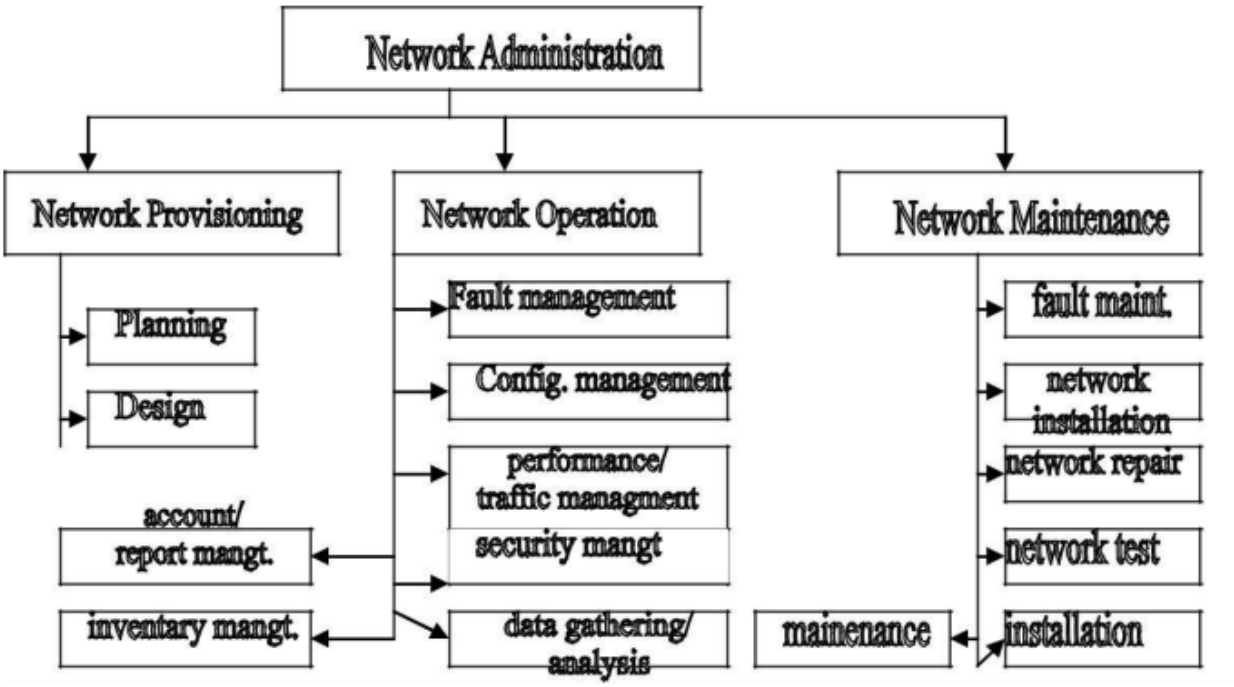
Monitoring of systems/software. Performing backups of data. Installing and configuring new hardware/software. Adding/deleting/creating/modifying user account information, resetting passwords, etc. Automating operations Responsibility for security. Responsibility for documenting the configuration of the system. •System performance tuning. Keeping the network up and running.

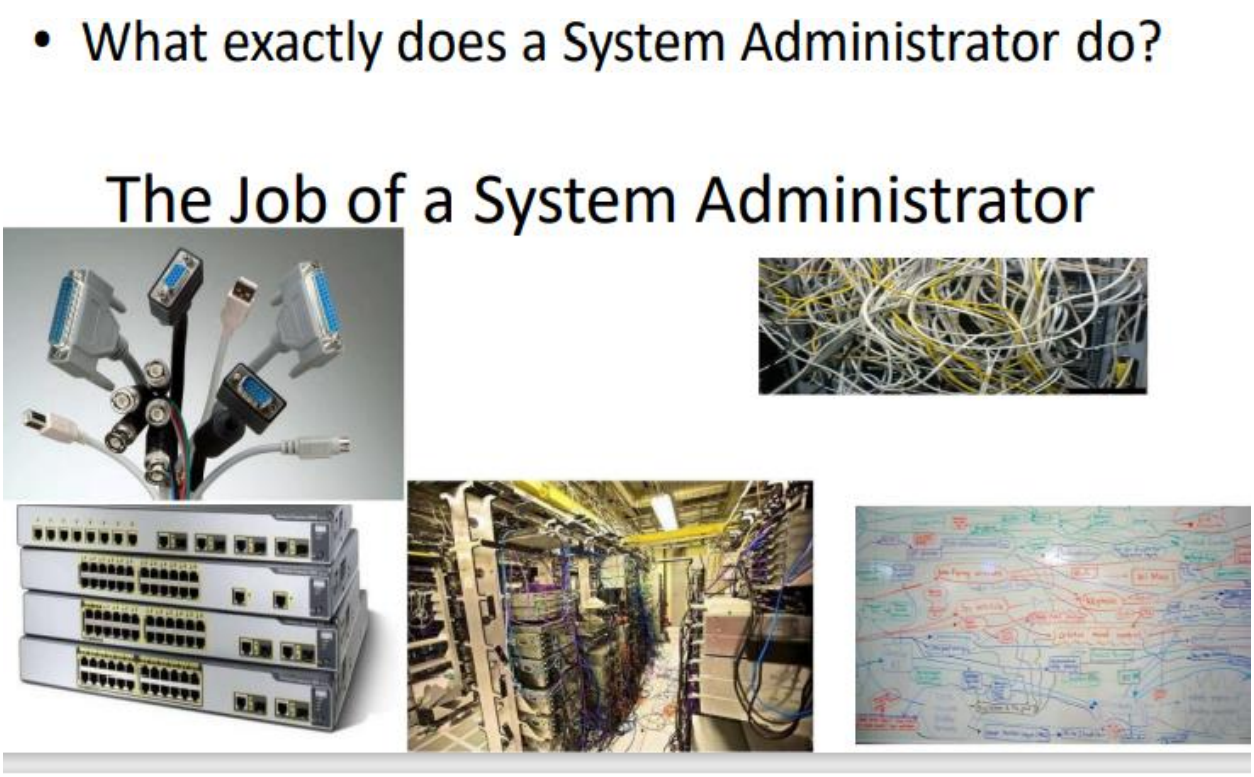
The Goal of System Administration

Ensuring the systems are running efficiently and effectively. Supervise system functionality. Every system must work and be connected to the network. Create backups on media, better if automatic backup. Create and install desktop and servers. – Create users and assign to them customizable Graphical User Interface. Update systems for the maximum performance Share system resources for the maximum network flow share disks between heterogenous systems in the better position share printers to save superfluous investment Systems starts up and shutdowns properly Allocating disks spaces and relocating quotas when the needs grows.

The Goal of Network Administration

Network administration means the management of network infrastructures devices (such as router and switches) Network administration compromises of 3 majors' groups: Network provisioning It consists of planning and design of network which is done by engineer. Network operations it consists of fault, configurations, traffic, all type of management. It is nerve center of network management operations. Network maintenance: it consists of all type of installations and maintenance work.





What exactly does a System Administrator do? no precise job description – often learned by experience "makes things run" often known as IT support, Operator, Network Administrator, System Programmer, System Manager, Service Engineer, Site Reliability Engineer etc.

What sysadmins do?

User account management, Hardware management, perform filesystem backups, restores Install and configure new software and services, keep systems and services operating, Maintain documentation Audit security Help users, performance tuning, and more!

9.4.1. User Management

Is Defining the rights of organizational members to information in the organization Involves a wide range of functionality such as adding/deleting users, controlling user activity through permissions, managing user roles, updating permissions when users change roles, defining authentication policies, managing external user stores and manual/automatic logout, and resetting passwords. Challenge: managing large number of users – Commonly organized into groups (users with similar privileges) E.g. all faculty members in the computer science department

access to mailing list Active directory in windows provides centralized user management and access control for computers.

Any user management system has the following basic components: Users: Users are consumers who interact with your organizational applications, databases, and other systems. A user can be a person, a device, or another application/program within or outside of the organization's network. Because users interact with internal systems and access data, organizations need to define which data and functionality each user can access by assigning permissions.

Permissions: A permission is a delegation of authority or a right that is assigned to a user or a group of users to perform an action on a system. Permissions can be granted to or revoked from a user, user group, or user role automatically or by a system administrator.

User roles: A user role is a grouping of permissions. In addition to assigning individual permissions to users, admins can create user roles and assign those roles to users. For example, you might create user roles called VP, Manager, and Employee, each of which has a different set of permissions, and then assign those roles to users based on their position in the company. Then, if you need to modify the permissions of all your managers, you can simply modify the Manager user role, and all the users with that role will have their permissions updated automatically.

Creating user accounts User Ids, Home directories (quotas, drive capacities) , Default startup files (paths), Permissions, group memberships, accounting and restrictions, Communicating policies and procedures, Disabling / removing user accounts, Consistency requires automation, Username and UID namespace management , Home directory backups and quotas, Removing user accounts Consistency requires automation , Remove everything, not just home dir and passwd.

9.4.2. Hardware Management

Adding and removing hardware, Configuration, cabling, etc. Device driver's installation Scheduling downtimes and notifying users, Hardware evaluation and purchase, System configuration and settings, Capacity planning, How many servers? How much bandwidth, disk space? Data Center management Power, racks, environment (cooling, fire alarm).

9.4.3. Data Backups

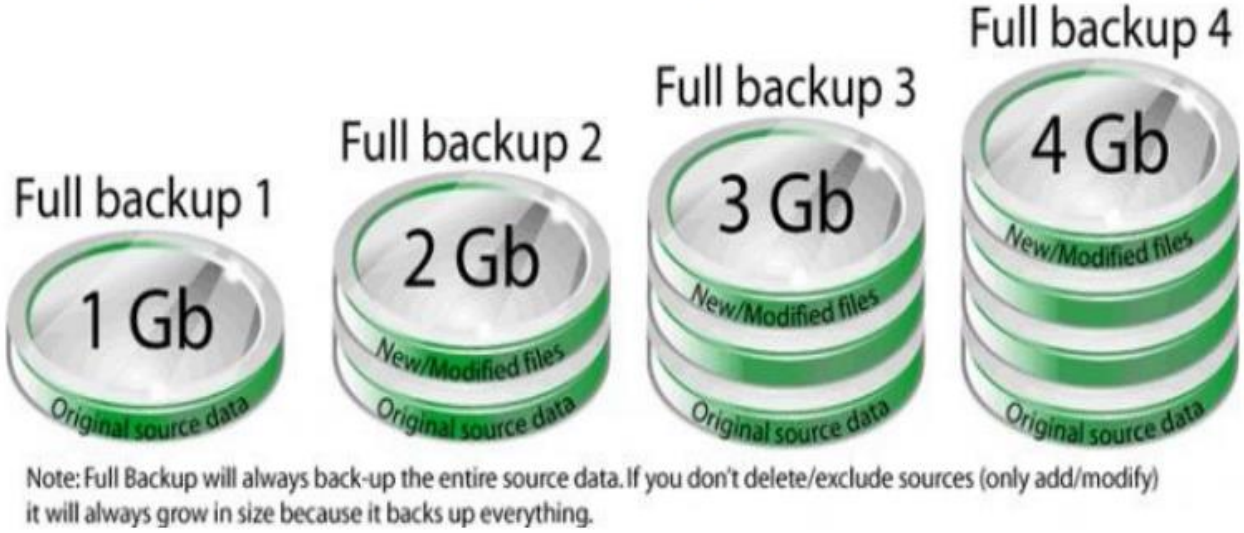
Perhaps most important aspect! Backup strategy and policies, Scheduling: when and how often? –Capacity planning –Location: On-site vs off-site, Installing backup software, Performing backups and restores, Monitoring backups Checking logs, Verifying media, Disaster recovery Onsite/Offsite Periodic testing Multiple copies.

Backup

The process of taking a copy of important data to another partition or disk or secondary site for preservation. The process of backing up data is pivotal to a successful disaster recovery (DR) plan.

Types of Backup

Full Backup:-is a method of backup where all the files and folders selected for the backup will be backed up.



Note: Full Backup will always back-up the entire source data. If you don't delete/exclude sources (only add/modify) it will always grow in size because it backs up everything.

9.4.4. Software Installation and Maintenance

Automated consistent OS installs, Evaluation of software, Finding and building open source software, Purchase of commercial software, Managing software installations Distributing software to multiple hosts Package management Managing multiple versions of a software pkg, Patching and updating software, Scheduling downtimes and notifying users, Maintenance of multiple versions.

9.4.5. Troubleshooting

Problem discovery, diagnosis, and resolution Often difficult, Problem identification By user notification By log files or monitoring programs, Tracking and visibility Ensure users know you're working on problem , Finding the root cause of problems Provide temporary solution if necessary Solve the root problem to permanently eliminate.

9.4.6. Monitoring

Hardware and services functioning and operational, Automatically monitor systems for Problems (disk full, error logs, security) Performance (CPU, memory, disk, network), Log periodic rotation and backups, Provides data for capacity planning – Convince management of need for hardware, Two Kinds: – Reactive: Detecting and analyzing failures after they have occurred, Problem notifications, analyzing logs after failures(e.g. identifying modus operandi, affected system – Proactive: testing a system for specific issues before they occur, Vulnerability scanners(automatically identify/prioritize issues), penetration testing.

9.4.7. Local Documentation

Administrative policies and procedures – Backup media locations – Hardware, Location, Description, configuration, connections – Software, Install media (or download location), Installation, build, and configuration details, Patches installed, Acceptable use policies, Network setting.

9.4.8. Security Concerns

System logging and audit facilities – Evaluation and implementation – Monitoring and analysis – Traps, auditing and monitoring programs, Unexpected or unauthorized use detection, Monitoring of security advisories – Security holes and weaknesses – Live exploits.

9.4.9. Helping Users

Request tracking system – Ensures that you don't forget problems. – Ensures users know you're working on their problem; reduces interruptions, status queries. – Lets management know what you've done. User documentation and training – Acceptable Use Policies – Document software, hardware (printers), etc.

Qualities of a Successful Sysadmin

Customer oriented – Ability to deal with interrupts, time pressure – Communication skills – Service provider, not system police, Technical knowledge – Hardware, network, and software knowledge – Debugging and troubleshooting skills, Time management – Automate everything possible. – Ability to prioritize tasks: urgency and importance.

Implement Strong Security – Less privilege principle, – a role-based security system, – monitoring critical services, – and conducting vulnerability and penetration testing. – Also, watch for any signs of a break-in.

9.5. Network security

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies.

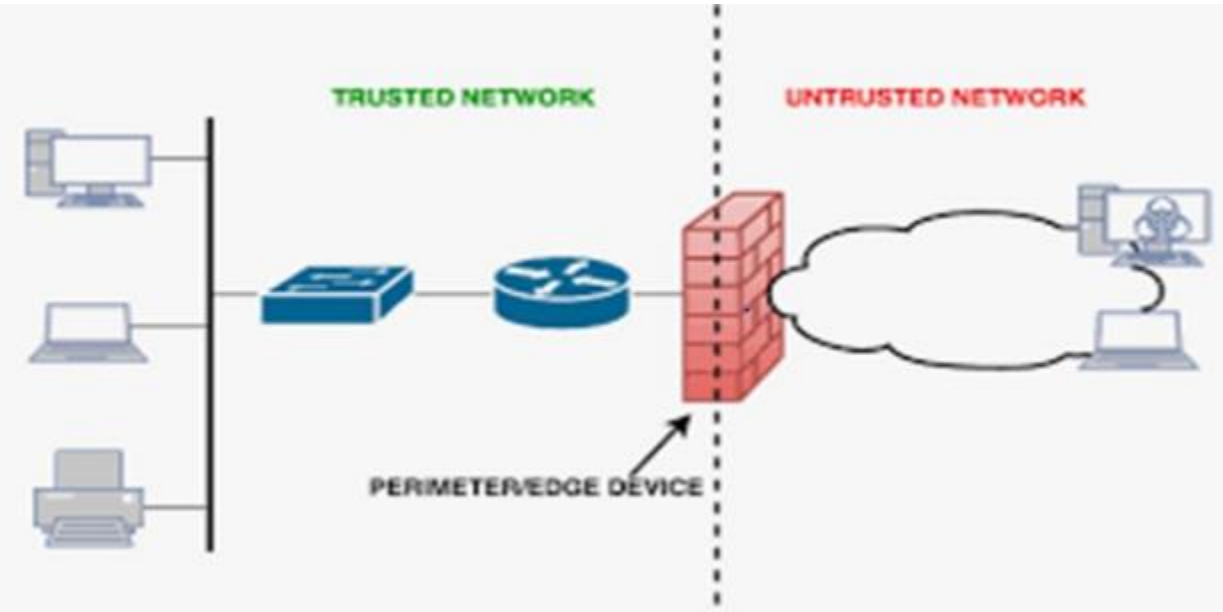
Antivirus and antimalware software

"Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

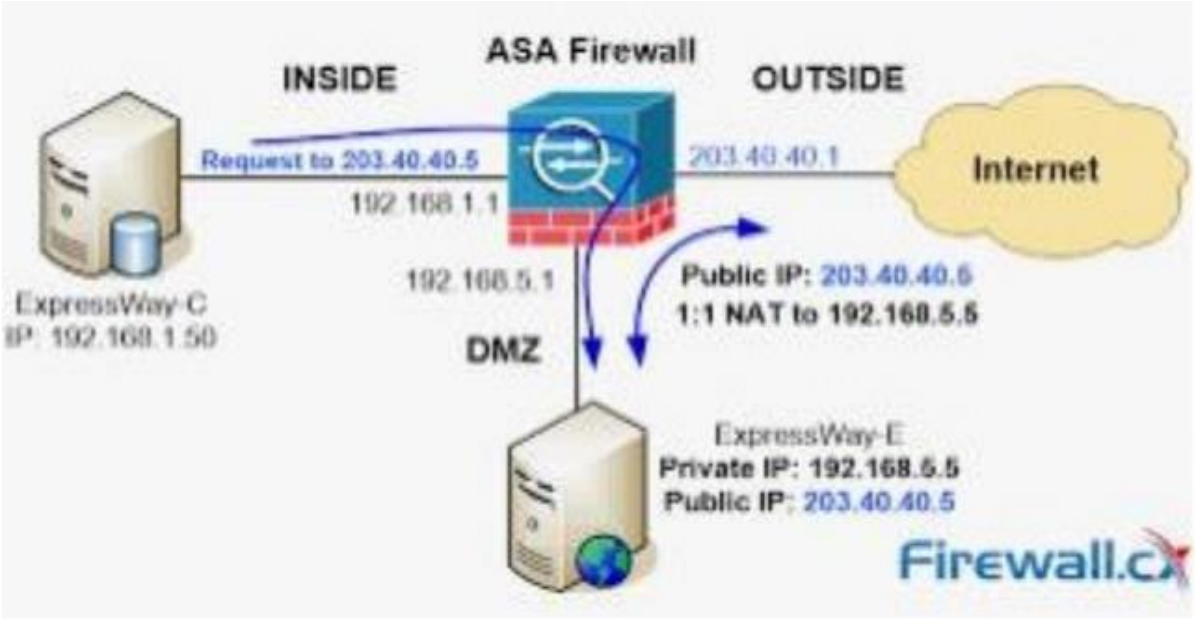
Firewalls

Firewall is a security framework for the network that tracks and regulates incoming and outgoing network traffic. Firewalls are defined as a network-based or host based system that is based on a set of security rules to allow or block, It is also capable of filtering traffic from unsecured or suspicious sources to avoid attacks, such as malicious traffic.

If a firewall filters traffic based on IP address, it operates at the network layer. If a firewall filters traffic based on port number, it operates at the transport layer, and if a firewall inspects protocol states or data, then it operates at the application layer.



DMZ or demilitarized zone



Intrusion prevention systems (IPS/IDS)

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

Virtual private network (VPN)

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

Network security tools (Lab session)

Network Security Monitoring tools, Encryption Tools, Web Vulnerability Scanning tools, Network Defence Wireless Tools, Packet Sniffers, Antivirus Software, Firewall, Snort, Nagios • Wireshark Penetration testing tools • Kali Linux , Nikto, Log360, SiteLock.

9.6. Specials

Information Systems Management are applying computer-base for managing information in organizations for management roles such as interpersonal roles, informational roles and decision-

based roles. Information Systems Management compound of theories of computer science and management science. These theories build systems and program utilization.

Troubleshooting (Hardware, Software, Network)

What is Hardware Troubleshooting? This is a process of analyzing, diagnosing, and discovering operational or mechanical defects within a hardware device or equipment. The main aim is to fix physical and/or logical flaws within the computer hardware. This process is done by a hardware or technical support technician.

Software troubleshooting

Software troubleshooting is the process of scanning, identifying, diagnosing and resolving problems, errors and bugs in software. It is a systematic process that aims to filter out and resolve problems, and restore the software to normal operation. It is a subcategory of IT troubleshooting.

Network troubleshooting

Network troubleshooting in the process of measuring, identifying, and resolving network-related issues. It's also defined as a logical process network engineers follow to improve the overall network operations. Troubleshooting is a repetitive, rigorous, and effective process that involves regular analysis and testing of individual network components to ensure smooth operations.

System requirement

System requirement simply means needs of system to run smoothly and efficiently. It is a structured document that gives a detailed description of system functions, services, and operational constraints. It requires many hardware and software resources.

Systems design

Systems design is an interdisciplinary engineering activity that enables the realization of successful systems. A system may be denned as an integrated set of components that accomplish a defined objective.

System installation

Installation (or setup) of a computer program (including device drivers and plugins), is the act of making the program ready for execution. Installation refers to the particular configuration of a software or hardware with a view to making it usable with the computer.

System configuration

System configuration mainly refers to the specification of a given computer system, from its hardware components to the software and various processes that are run within that system. It refers to what types and models of devices are installed and what specific software is being used to run the various parts of the computer system.

Chapter 10

10.1. overview of information systems security

Information systems security, more commonly referred to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.

It also refers to:

Access controls, which prevent unauthorized personnel from entering or accessing a system.

Protecting information, no matter where that information is, i.e. in transit (such as in an email) or in a storage area.

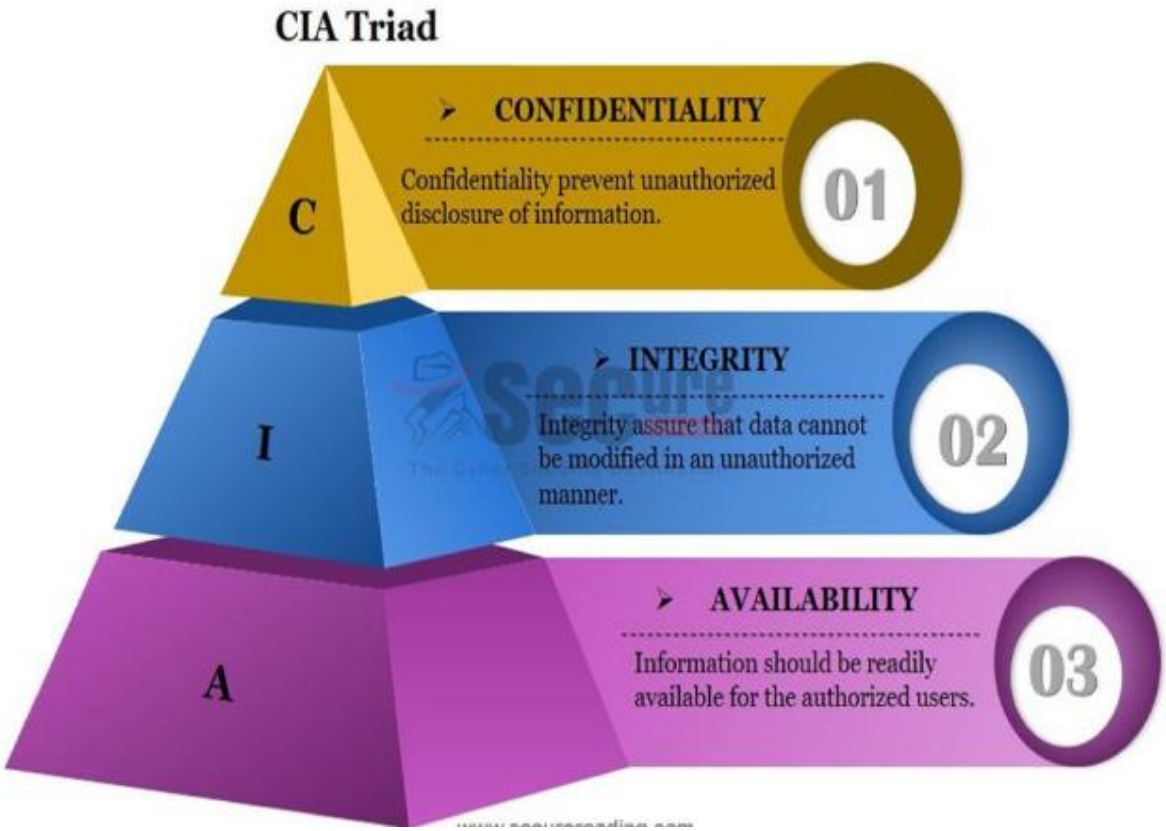
The detection and remediation of security breaches, as well as documenting those events.

As computers and other digital devices have become essential to business and commerce, they have also increasingly become a target for attacks. In order for a company or an individual to use a computing device with confidence, they must first be assured that the device is not compromised in any way and that all communications will be secure. This chapter reviews the fundamental concepts of information systems security and discusses some of the measures that can be taken to mitigate security threats. The chapter begins with an overview focusing on how organizations can stay secure. Several different measures that a company can take to improve security will be discussed. Finally, you will review a list of security precautions that individuals can take in order to secure their personal computing environment.

10.2. Basic Information Security Concepts

Three basic information security concepts important to information are **Confidentiality, Integrity, and Availability.** If we relate these concepts with the people who use that information, then it will be **authentication, authorization, and non-repudiation.**

Information Security is such a broad discipline that it's easy to get lost in a single area and lose perspective. Nevertheless, the classic definition of information security is brief and simple: 'Information security is the confidentiality, integrity, and availability of information also referred as C-I-A triad or information security triad.



Confidentiality

When information is read or copied by someone not authorized to do so, then it will be **"loss of confidentiality".** For sensitive information, confidentiality is a very important criterion. Bank account statements, personal information, credit card numbers, trade secrets, government documents are some examples of sensitive information. This goal of the CIA triad emphasizes the need for information protection. For example, confidentiality is maintained for a computer file, if authorized users are able to view it, while unauthorized persons are blocked from seeing it.

Integrity

Information can be corrupted or manipulated if it's available on an insecure network, and is referred to as "**loss of integrity."** This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting. For example, banks are more concerned about the integrity of financial records, with confidentiality having only second priority. Some bank

account holders or depositors leave ATM receipts unchecked and hanging around after withdrawing cash. This shows that confidentiality does not have the highest priority. In the CIA triad, integrity is maintained when the information remains unchanged during storage, transmission, and usage not involving modification to the information.

Availability

Information can be erased or become inaccessible, resulting in **"loss of availability."** This means that people who are authorized to get information are restricted from accessing. Availability is often the most important attribute in service-oriented businesses that depend on information. Denying access to information has become a very common attack nowadays. Almost every week you can find news about high profile websites being taken down by Denial of Service attacks. The CIA triad goal of availability is the situation where information is available when and where it is rightly needed.

Now let's take a look at other key terms in Information Security – Authorization, Authentication, and Nonrepudiation processes and methods, which are some of the main controls aimed at protecting the C-I-A triad.

The first events in the history of exploiting security date back to the days of telephony. Telephone signals were sent via copper cables. Telephone lines could be tapped and conversations could be heard. In the early days of telephone systems, telephone operators intentionally misdirected calls and eavesdropped on conversations. In the 1970s, a set of people known as phreakers exploited the weakness of digital switching telephone systems for fun. Phreakers discovered the signal frequency at which the numbers are dialed and tried to match the frequency by blowing a whistle and fooling the electronic switching system to make calls for free. Among these phreakers, John Draper found that he could make long-distance calls for free by building an electronic box that could whistle different frequencies.

During the 1960s and 1970s, telephone networks became the dominant mode of communication, connecting millions of users. Given the increasing importance of computers and the advent of time shared systems, it was natural to consider linking the computers on the telephone networks so that information could be shared among geographically distributed networks. Since telephones were analog and computers were digital, modem (modulator and demodulator) devices were used to connect computers over the telephone network. Connecting computers and sharing

information was of major interest during the early days of network computing and the security of the information became weak. Since people already knew how to break and tap into the phone systems, it became a game for them to break into the computer system, which was connected over the telephone networks.

With the creation of Advanced Research Projects Agency Network (ARPANET), a limited form of a system break-in to the network began. ARPANET was originally designed to allow scientists to share data and access remote systems. E-mail applications became the most popular application to allow scientists to collaborate on research projects and discuss various topics over the network. Soon, a bulletin message board was created where people could post a topic and discuss various research topics together. Bulletin boards became the venue of choice for discussing a wide range of topics, including passwords, credit card numbers, and trade tips, which encouraged the bad guys to hack into the system. Some famous bulletin boards include Sherwood Forest and Catch-22.

10.4. WHAT IS ARPANET?

The predecessor of the Internet, the Advanced Research Projects Agency Network (ARPANET) was a large wide-area network created by the United States Defense Advanced Research Project Agency (ARPA). Established in 1969, ARPANET served as a testing ground for new networking technologies, linking many universities and research centers. The first two nodes that formed the ARPANET were UCLA and the Stanford Research Institute, followed shortly thereafter by the University of Utah. Some of the reasons for creating ARPANET include making it easier for people to access computers, to improve computer equipment, and to have a more effective communication method for the military.

In the 1980s, the TCP/IP network protocol Transmission Control Protocol (TCP) and the Internet Protocol (IP), and Personal Computers (PC) brought computing to homes where more and more people connected to the Internet. The 1983 fictional movie, “War Games,” was watched by millions of people and popularized hacking and made it glamorous. In 1981, Ian Murphy broke into AT&T’s computers and changed billing rates of meters. He was later convicted.[1] Kevin Mitnick stole computer manuals of Pacific Bells’ switching center in Los Angeles, California,

and was prosecuted for this crime.[1] Bill Landreth was convicted for breaking into NASA's Department of Defense computers through GTE's e-mail network. In 1988, Kevin Mitnick was held for stealing software that was worth $1 million, and also caused damages of around $4 million.

10.5. Introduction to Cybersecurity Fundamentals

For a few years, the growth of the internet has increased exponentially. A decade back, most of the things were handled offline while these days one can internet for almost of the purpose. Together with the growth of the internet, security has become a point of concern. The attackers are sitting all across the world to breach the system for their personal benefits. Several AI-based complex applications have also been developed these days that make hacking easier. In contrast to that, the cybersecurity auditors have also reinforced their court by using the same complex applications to protect the system. Here in this article, we are going to learn about cybersecurity fundamentals. Cybersecurity is comprised of various components.

10.6. Understanding the Fundamentals of Cybersecurity

Cybersecurity refers to the term which means protecting the system on the internet. It can also be considered as fortifying the systems in order to stay protected against breaches online. Cybersecurity compromise is several modules where every module has is responsible for protecting the system in a particular manner. Eventually, what all the modules take care of is to prevent the system from malicious attacks that could lead to harm to the system. Below are some of the modules of cybersecurity that helps in protecting the system, especially to the systems that are having a public interface.

As the digital era has gifted us a massive technological innovation, organizations and companies have spent the past several decades aggressively increasing their online presence to reach new customers and grow their digital presence. It is not surprising, then, that cybercrime also escalated simultaneously. The omnipresence of the internet and growing access to it have

made it easier than ever before for cybercriminals to target businesses and gain access to personal information about their customers or employees.

The concept of computer security is no longer limited to only safeguarding electronic devices against external threats. To prevent unauthorized credentials of an organization's network, it must also ensure the security of its network. No matter what field you operate in or how secure your data is, there will always be online threats that can put your company's information at risk.

In addition, physical security is also crucial, such as protecting hardware data from events or actions that can cause serious damage to an organization, such as natural disasters, burglaries, floods, theft, fires, vandalism, and many others.

Learning about basic concepts of cybersecurity helps equip individuals with the knowledge they need to safeguard their networks from potential attacks and safely maintain privileged user access. In addition, it is highly beneficial to learn the best online Cybersecurity certificate programs.

History of Cyberthreats Explained

There has been a turbulent history of cyber threats. It was challenging to carry out a cyberattack in an era when technology was limited. Only a few people knew how to operate the giant electronic machines, which weren't networked, therefore, it was virtually not hackable.

John von Neumann proposed storing the program instructions in the same memory as the data in 1945. Stored programs made it easier for computers to reprogram and complete the fetch-decode-execute cycle (FDE). This idea is often called 'Von Neumann' architecture.

In the late 1950s, phone phreaking—hijacking the phone protocols that enabled the 'phreaks' to work remotely on the network without contacting the telecom engineering to make free calls and avoid paying for long-distance calls got popular. Unfortunately, the phone

companies could not control the phreaks due to limited sources and eventually, phone phreaking faded in the 1980s.

In 1979, Kevin Mitnick made copies of the operating systems developed by the Digital Equipment Corporation using the Ark computer. In the following decades, he committed several cyberattacks that led to his arrest and imprisonment. Currently, he serves as the CEO and founder of Mitnick Security Consulting. Since this field has such a rich history, it's not surprising that people are concerned about the recent developments since hackers can easily penetrate increasingly robust security software.

Why is Cybersecurity Critical?

Cybersecurity is a fast-evolving field that continually poses new challenges for companies, government agencies, and individuals. While some may assume that cybersecurity means protecting computers from viruses and other types of malware using anti-virus software or other security programs, this is only one aspect of the subject.

It is more common than ever for data breaches and cyberattacks to occur. They're no longer limited to large corporations with vast resources and sophisticated information security practices. Today, smaller businesses and those operating online marketplace sites or other e-commerce services are also at risk.

It takes one mischievous user with access to a computer or mobile device to break into an organization's network, steal confidential information, cause damage and result in lost revenue and penalties for failing to safeguard assets. They can also expose companies to liability risks. Thus, every organization must understand the basics of information security and why it's essential for their business.

The excellent accessibility of cloud computing also makes it a popular choice for many companies, which can access information anywhere, anytime, and from any location.

There are, however, some risks associated with cloud computing, such as the fact that few services are available in the public domain, and third parties can access these services. Therefore, hackers may be able to hack these services easily. In addition, cloud computing also poses a severe security risk of account hijacking. When information in cloud accounts such as email, bank, social media, etc., is not password protected, it becomes vulnerable, and hackers can access it to perform unauthorized activities.

Important Cybersecurity Fundamentals

The IT Security Fundamentals skill path includes an understanding of computer hardware, software, and network security. The cybersecurity fundamentals course trains you in developing and implementing security solutions for small and large organizations, protecting systems and network infrastructures.

Four Fundamentals of Cybersecurity

1. Device Protection

With the rise in cyber threats, individuals and companies should prioritize device protection. It is crucial to protect devices that connect to the internet using anti-virus software, enables the lock-and-erase options, activate two-factor authentication, and perform a regular automatic update of the system software, whether they are laptops, PCs, mobile phones, AI-based devices (Alexa, smart watches, etc.), iPads, tables, or any device that connects to the internet. Device protection will significantly reduce the risk of attacks on individuals and their devices regardless of their location.

2. Securing Online Connection

Once an individual device is connected online, information transmitted over the Internet requires more defenses. Furthermore, one should use VPNs: Virtual Private Networks as they automatically encrypt internet traffic. By using a VPN, all online transactions are secured, including the user's identity, location, browsing details, and any sensitive information such as passwords and bank details.

3. Securing Email Communication

Cybercriminals often use email to gather sensitive information about individuals or companies. It is highly recommended to encrypt emails to prevent sensitive data from being accessed by anyone other than the intended recipient since they mask the original information. In addition, email encryption often includes one-time password authentication.

4. Protecting and Performing Timely Backups of Files and Documents

Backups fall into two categories: Remote backups (offline) and cloud storage (online). Solutions differ in their advantages and disadvantages.

Remote backup services are convenient and inexpensive, but it is not easily accessible from anywhere. Alternatively, cloud solutions can be accessed from anywhere and are suitable for an organization that operates from different locations.

However, one must ensure that critical documents should have their own digital vault with encryption codes, as anything connected to the internet has a cyber threat risk.

Cyber threats can, however, affect anything connected to the internet. With a database and infrastructure security management system, the cloud computing solution is highly secure, with strong network security, application security, and cloud security. Additionally, strong mobile security enhances cloud computing security.

By implementing a BCDR plan, an organization can recover quickly from unforeseen cloud security situations such as natural disasters, power outages, team member negligence, hardware failure, and cyberattacks, allowing routine operations to resume in less time. Moreover, identity management frameworks provide endpoint security and data security at the highest level.

Key Concept of Cybersecurity

Cybersecurity refers to protecting systems, networks, programs, devices, and data from cyber-attacks using technologies, processes, and controls. The basic cybersecurity concepts involve reducing cyber-attack risks and preventing unauthorized access to systems, networks, and technologies.

Five Primary Key Concepts of Cybersecurity

- Threat identification
- Keeping information safe
- Detecting intrusions and attacks
- Respond to intrusions and attacks
- Rebuild intrusion defenses and recover database security

Basic Terminologies of Cyber Security

Cybersecurity basics for beginners should include these terminologies. Knowing the cybersecurity basics terminology will help you better understand the high-tech world. However, technological advances in cybersecurity are accompanied by the emergence of new jargon.

1. Internet Protocol (IP) Address

Hardware devices on a network are identified by IP addresses (Internet Protocol addresses). On a local network or over the internet, these devices can communicate with each other and transfer data. Numbers are separated by periods in each address. It comprises four digits with a range of 0 to 255. An IP address might look like this: 192.159.1.98

Internet computers, routers, and websites need billions of unique IP addresses to be identified as one cannot repeat them. IPv6 is a new protocol designed to meet the day's needs when the system runs out of unique addresses in the future.

2. VPN - Virtual Private Network

Virtual Private Network, popularly known as VPN, allows users to maintain their privacy and anonymity while browsing the internet. VPNs make online activities virtually untraceable by masking the internet protocol (IP) address.

In addition to providing greater privacy than secured Wi-Fi hotspots, VPN services establish secure and highly encrypted connections. With a VPN, online activity is hidden from cybercriminals, businesses, governments, and other snoopers who tend to lure users into clicking on anonymous links.

3. Firewall

A firewall monitors and filters the system's incoming and outgoing network traffic as per a company’s security policies. Firewalls are a barrier between a private internal network and the Internet at its primary level. A firewall blocks virtual traffic, which looks destructive, and allows secure and non-threatening traffic to flow uninterrupted.

4. Domain Name Server (DNS)

DNS - Domain Name Server operates as the internet’s virtual phone book. As every browser on the internet is known by its IP address which allows users to locate the device, the DNS converts the domain name into an IP address. For instance, the DNS converts the URL of www.mycompany123.com to a numerical IP address 204.0.6.42. Browsers send data to the origin servers on the content delivery network (CDN) using the IP address found by DNS servers.

5. Encryption and Decryption

Encryption is a process of converting plain text (readable message) into codes using an encryption algorithm known as ciphertext. While, Decryption is a process of converting the ciphertext into plain text.

6. Encryption Key

Data that is encrypted is decrypted and unscrambled using an encryption key. Keys are unique and complex to replicate since they are associated with specific encryption codes.

In addition, here are the top 50 cybersecurity terms you should learn to become a pro in cybersecurity.

Common Types of Cyber Attacks

The world today is plagued by a variety of cyberattacks. However, our networks and systems are better protected if we know the types of cyberattacks. Here are the five most common types of cyberattacks:

1. Malware Attack

- **Virus:** A virus is a type of malware that can infect all the files on the network, which is one of the most challenging types to eliminate. A computer virus can replicate itself by inserting its malicious code into other programs.
- **Worm:** Have the power to infect the entire network quickly and require no end-user involvement as the worms can self-replicate.
- **Trojan:** One of the most challenging types of malware to detect is Trojan malware, as it disguises itself as a legitimate program. As soon as the victim executes the malicious code and instructions, the malware can function independently. It is often used as an entry point for other forms of malware.
- **Adware:** End-users are served unwanted advertising (for instance, contact pop-ups) by adware.
- **Spyware:** This type of malware collects sensitive data like user ids and passwords without suspecting the end-user.
- **Ransomware:** Known as one of the most dangerous types of malware attack that infects the system, encrypting files and holding onto the encryption key until the victim pays a ransom. The ransom is mainly in the form of cryptocurrency with a

P2P network. Increasingly, organizations are being attacked by ransomware that costs them millions to restore vital systems as they pay off the attackers to recover them. There are several ransomware families, but Crypto Locker, Petya, and Locky are the most recognized ones.

2. Password Attack

Password attacks most commonly cause data breaches. To gain access to user accounts, the hacker tries to bypass the authentication.

3. Phishing Attack

The hacker can steal user data through phishing attacks, including login credentials, bank account details, and credit card numbers. Attackers use disguises to trick victims into opening emails, instant messages, or text messages that appear to come from trusted entities. After the recipient clicks a malicious link, sensitive information is revealed, and malware is installed.

4. Clickjacking

In clickjacking, the attacker usually uses some sort of ad online to lure the user. They are tricking a user into clicking on buttons or links that open to another page that installs malware into the user's system.

The Adobe Flash plugin settings page is one of the most scandalous examples of clickjacking. This page could be loaded into an invisible iframe and enable an attacker to manipulate the security settings in Flash, allowing the computer’s microphone and camera to be used remotely by Flash animations.

5. Cryptocurrency Hijacking

Cryptocurrency hijacking is a new cyber-attack that grew rigorously after the cryptocurrency was introduced widely. Attackers use crypto jacking to mine cryptocurrency on someone else’s computer.

During the attack, the attacker gains access to the user's computer by infecting their system or manipulating them to click on malicious links. In most cases, the users are unaware of this since the Crypto Mining code works in the background, and the only indication that something is wrong is a delay in the execution.

Cyber Security Job Roles

1. Network Security Engineer

Every organization needs a network security engineer to ensure security systems are in place to stop and counter threats. In addition, Network Security engineers are also responsible for systems maintenance, vulnerability identification, and automation of the system. The engineers also oversee the maintenance of routers, firewalls, switches, and VPNs (virtual private networks).

2. Cybersecurity Analyst

Security measures and controls are planned, implemented, and upgraded by a cybersecurity analyst. Security audits are conducted internally and externally to ensure no loopholes or security lapses. In addition to conducting vulnerability testing, risk analyses, and security assessments, a cybersecurity analyst is also responsible for managing the network. The analyst also trains colleagues in security awareness and procedures to prevent security breaches.

3. Chief Information Security Officer (CISO)

In an organization, the Chief Information Security Officer (CISO) ensures that cybersecurity plans are aligned with the business’s vision, operations, and technologies. Security-related processes are also developed, implemented, and maintained by CISOs in collaboration with their staff.

4. Ethical Hackers

Due to the intuitive knowledge and skills they possess, ethical hackers are a valuable resource for organizations. They tested and picked apart to reveal vulnerabilities. Additionally, ethical

hackers provide high-level cyberattack prevention information that is gaining momentum in the market.

5. Cloud Security Engineer

An organization's cloud-based networks and systems are built and maintained by a cloud security engineer. They manage the organization's cloud computing environments, core infrastructure, and software platforms. In addition to providing security recommendations, they also offer advice on designing and developing secure applications.

Cybersecurity Best Practices

Cyberattacks can be challenging, and keeping up with cybercriminals who constantly seek out innovative methods of exposing security risks is tough. However, one can still prevent cyberattacks in some ways:

1. Updating the Software Regularly

A typical software update includes updated features, bug fixes, and security updates. It is always a good idea to update your software to the latest version to ensure your safety.

2. Making Sure the Computer is Protected from Viruses and Malware

You can't be entirely protected from malware as long as you're connected to the internet. The vulnerability of your computer will be significantly reduced if you install an anti-virus program and at least one anti-malware program.

3. Set up 2-factor Authentication

In addition, web security is strengthened by two-factor authentication because it eliminates the risk of a compromised password immediately. Two-factor authentication is now available on several platforms to keep your accounts safer.

4. Protect your Connections with a VPN

Use a virtual private network (VPN) for a more secure web. Even your internet service provider won’t be able to have a glimpse of your confidential information because VPN will encrypt the connection.

5. Being Careful While Clicking on Links

Whenever you click on random hyperlink messages, make sure you double-check their legitimacy since links can easily be masked as something they are not.

6. Make Sure Bluetooth is Disabled When Not in Use

Hackers can steal your private information via Bluetooth if your devices are on. If you aren't using Bluetooth, please do turn it off.

7. Delete Adware on your Computer

You will receive more targeted ads via adware as it collects information about you. To maintain your privacy, keep your computer free of adware and install an ad blocker.

8. Upgrade your Security System

Make sure to invest in a good security system and upgrades when they are available. Investing in high-grade security is better than paying a huge amount for security breaches.

9. Virus Scan External Storage Devices

In addition to internal storage devices, external storage devices can also be exposed to malware. Infected external devices can spread malware to your computer if you connect them. Therefore, before accessing external devices, scan the device to ensure they are malware-free.

10. Ensure Critical Data is Backed Up

Sensitive information can be lost as a result of security breaches. Highly advisable to take back up of your critical data to the cloud or a local storage device frequently to ensure you are prepared to restore it in the event of a loss. In addition, ensure you store the sensitive files with password protected system.

Some of the cybersecurity fundamentals are given below:

10.7. Network Security

Network security can be defined as protecting the internal network from being attacked by malicious users. The organizations use internal servers that have to stay protected in order to protect the system and business operations. The server has to be configured with the security aspects so that it has the capability to oppose the attack. Network security is also about protecting all the devices connected to the network like computers, printers, routers, switches, etc. The server should have a strong mechanism implemented to detect malicious activity to stop before it harms the network. The main purpose of this network security is to ensure that the network is secure so that the entire system could stay protected. Below are some of the technologies and tools used in network security.

- **IPS & IDS –** These are the tools that are used to detect malicious activity and stop it from being executed. IPS stands **for intrusion prevention system**, and IDS stands for the intrusion detection system.
- **Firewall – Firewall works** are the checking point for all of the requests that hit the ports of the server to get inside the network. It ensures that the ports not in use should be closed or filtered based on the business need.

10.8. Security Compliances

Compliances are the policies that have to be implemented in the organization to protect its system. The compliances comprise a set of rules that define the security measures that the organization must have to take care of to stay protected. All the policies that restrict the users or the employees of the organization from performing particular activities are the outcome of

security compliances. ISO 27001 is one of the most popular compliance is usually practiced by large, mid, and some of the small organizations. Below are some of the compliance that vary industry-wise.

- **PCI DSS:** The compliance is applicable for all of the organizations that accept online payment. It stands for Payment Card Industry Data Security Standard. It is mandatory for all organizations to adopt this compliance before they can bring the functionality of accepting online payment into their system.
- **HIPPA:** It stands for Health Insurance Portability and Accountability Act. This is the compliance that has to be followed by all of the organization that works with patients data. The purpose of this complaint is to ensure that the sensitive data of the patients are protected.

10.9.Web Application Security

Web Application Security may be defined as the term that defines the protection of the web application that the users of that system use in order to interact with them. The web application must be developed by keeping security in mind as attackers can leverage the vulnerability in order to breach the system. Compromising any vulnerability can also make a path for the attacker to attack the organization's network. To make sure that the application is protected from vulnerabilities, there is a mechanism to perform manual and automated checks. There are several tools available that allow cybersecurity analysts to run the scan and check if the web application is vulnerable to any attack. The OWASP Top 10 is the list of commonly found vulnerabilities in any application and are very severe in nature.

Following Top 5 Key Elements of an Information Security

10.8.1. Confidentiality

Data and information assets should be confine to individuals license to access and not be disclose to others; I Confidentiality assurance that the information is accessible those who are authorize to have access. Confidentiality breaches may occur due to improper data handling or a **hacking** attempt. It controls include data classification, data encryption, and proper equipment disposal (i.e. of DVDs, CDs, etc.), Confidentiality is roughly adore privacy. Measures undertaken to confirm confidentiality are design to prevent sensitive data from reaching the

incorrect people. Whereas ensuring the correct people will really get it: Access should be restricted those licensed looks at information in question. It's common for information to be categorize consistent with quantity and kind of injury might be done. It makes up unintended hands. A lot of or less rigorous measures will then be implemented according to those classes.

10.8.2. Integrity

Keeping the information intact, complete and correct, and IT systems operational; Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorize changes the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only the authorized people can update, add, and delete data to protect its integrity). Integrity involves maintaining the consistency, accuracy, and trustworthiness of information over its entire life cycle.

What is Ethical Hacking? & Types of Hacking

Information should not be modified in transit, and steps should be taken to confirm that information can't be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version management maybe won't be able to prevent incorrect changes or accidental deletion by licensed users becoming a problem. Additionally, some means that should be in place to discover any changes in information that may occur as a result of non-human-caused events like an electromagnetic pulse (EMP) or server crash. Some information would possibly include checksum, even cryptographic checksum, for verification of integrity. Backups or redundancies should be offer to revive the affected information to its correct state.

10.8.3. Availability

An objective indicating that data or system is at disposal of license users once require. Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Availability means data is accessible by licensed users.

If AN **attacker** isn't able to compromise the primary components of data security (see above) they'll try and execute attacks like denial of service that will bring down the server, creating the web site unavailable to legitimate users because of lack of availability. Measures to maintain data availability can include redundant systems' disk arrays and clustered Machines, anti-virus

software to stop malware from destroying networks, and distributed denial-of-service (DDoS) prevention systems.

10.8.4. Authenticity

A security policy includes a hierarchical pattern. It means inferior workers is typically certain to not share the small quantity of data they need unless explicitly approved. Conversely, a senior manager might have enough authority to create a choice what information is shared and with whom, which implies that they're not tied down by an equivalent data security policy terms. That the logic demands that ISP ought to address each basic position within the organization with specifications which will clarify their authoritative standing. Authenticity refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine or corrupted. The major role of authentication is to confirm that a user is genuine, one who he / she claims to be. Controls such as bio metrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, or documents.

The user should prove access rights and identity. Commonly, usernames and passwords are used for this method. However, this kind of authentication may be circumvented by hackers. a much better form of authentication is bio metrics, as a result of it depends on the user's presence and biological features (retina or fingerprints). The PKI (Public Key Infrastructure) authentication methodology uses digital certificates to prove a user's identity. Different authentication tools will be key cards or USB tokens. The best authentication threat occurs with unsecured emails that seem legitimate.

10.8.5. Non-Repudiation

It is the assurance that somebody cannot deny the validity of one thing. It may be a legal thought that's widely used in data security and refers to a service that provides proof of the origin of information and also the **integrity** of the information. In different words, non-repudiation makes it very difficult to successfully deny who/where a message came from also as the authenticity of that message.Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.

10.8.6. Questions related to this topic

1. What is confidentiality availability and integrity?
2. What does confidentiality integrity and availability have to do with security?
3. What is confidentiality in information security?

4. What are the 3 principles of information security?
5. What are Top 5 Key Elements of an Information Security?

Information System Security or **INFOSEC** refers to the process of providing protection to the computers, networks and the associated data. With the advent of technology, the more the information is stored over wide networks, the more crucial it gets to protect it from the unauthorized which might misuse the same. Every organisation has the data sets that contain confidential information about its activities.

The major reason of providing security to the information systems is not just one fold but 3 fold:

1. Confidentiality
2. Integrity
3. Availability

An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements.

ISPs should address all data, programs, systems, facilities, infrastructure, authorized users, third parties and fourth parties of an organization.

Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

1. Hardware Vulnerability:

A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.

For examples:

1. Old version of systems or devices
2. Unprotected storage
3. Unencrypted devices, etc.

2. Software Vulnerability:

A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:

1. Lack of input validation
2. Unverified uploads
3. Cross-site scripting
4. Unencrypted data, etc.

3. Network Vulnerability:

A weakness happen in network which can be hardware or software.

For examples:

1. Unprotected communication
2. Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
3. Social engineering attacks
4. Misconfigured firewalls

4. Procedural Vulnerability:

A weakness happen in an organization operational method.

For examples:

1. Password procedure – Password should follow the standard password policy.
2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

Malicious Security Threats

viruses

worms

Trojan horses

Spyware

Basic Information security controls fall into three groups:

Preventive controls, which address weaknesses in your information systems identified by your risk management team before you experience a cybersecurity incident.

- **Detective** controls, which alert you to cybersecurity breach attempts and also warn you when a data breach is in progress, so your cybersecurity staff can begin to limit the damage.

- **Corrective** controls, such as backups used after a cybersecurity incident, to minimize data loss and damage to information systems; and to restore your information systems as quickly as possible.

10.9.6. Social engineering defined

For a social engineering definition, it's the art of manipulating someone to divulge sensitive or **confidential information**, usually through digital communication, that can be used for fraudulent purposes.

Unlike traditional cyberattacks that rely on security vulnerabilities to gain access to unauthorized devices or networks, social engineering techniques target human vulnerabilities. For this reason, it's also considered human hacking.

Cybercriminals who conduct social engineering attacks are called social engineers, and they're usually operating with two goals in mind: to wreak havoc and/or obtain valuables like important information or money.

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing". In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is

known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography: In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events.

Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks. Security is necessary to provide integrity, authentication and availability.

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

In general, web security refers to the protective measures and protocols that organizations adopt to protect the organization from cyber criminals and threats that use the web channel. Web security is critical to business continuity and to protecting data, users and companies from risk.

References

[1] M. Burgess, Principles of Network and System Administration, Oslo University College, Norway: john wiley & sons, LTD, 2004.

[2] M. Burgess, HANDBOOK OF NETWORK AND SYSTEM ADMINISTRATION,

Amsterdam : Elsevier, 2007.

[3] D. T. Sreenivasulu, DATA COMMUNICATIONS & COMPUTER NETWORKS, Delhi: A Division of Visual Soft (India) Pvt. Ltd., 2018.

[4] B.A.Forouzan, Data Communications and Networking, 2003.

[5] J.Kurose, Computer Networking: A Top-Down Approach to the Internet, 2005.

[6] D. Kim, Fundamentals of Information Systems Security, Burlington: Printed in the United States of America, 2023.

[7] B. A., DATA COMMUNICATION AND NETWORKING, New york: Alan R, 2007.

[8] Y. N. ASAFE, DATA COMMUNICATION & NETWORKING, Abuja: ResearchGate, 2015.