Unit-III

Introduction to Computer Network: Introduction, importance of Computer Network, LAN, MAN, WAN, Networking Devices, World Wide Web, Web Browser, viruses, worms, malware, Use of Antivirus software, Good Computer Security Habits.

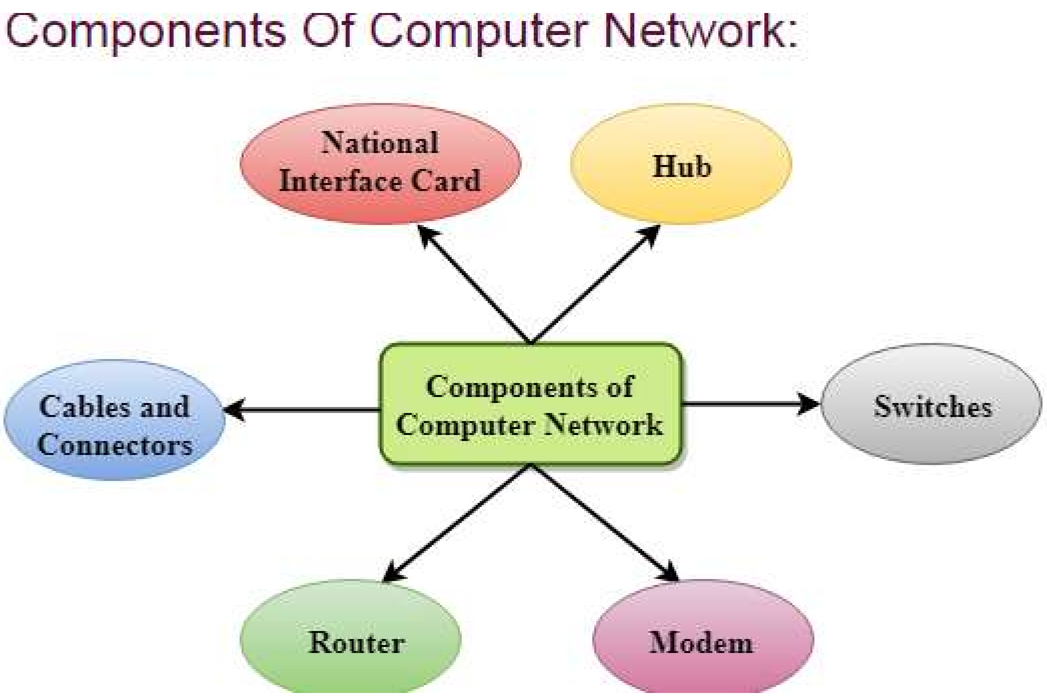
What is Computer Network?

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

Computer Network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task.

- **Computer Network** is a group of computers connected with each other through wires, optical fibres 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.

Components Of Computer Network:



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.

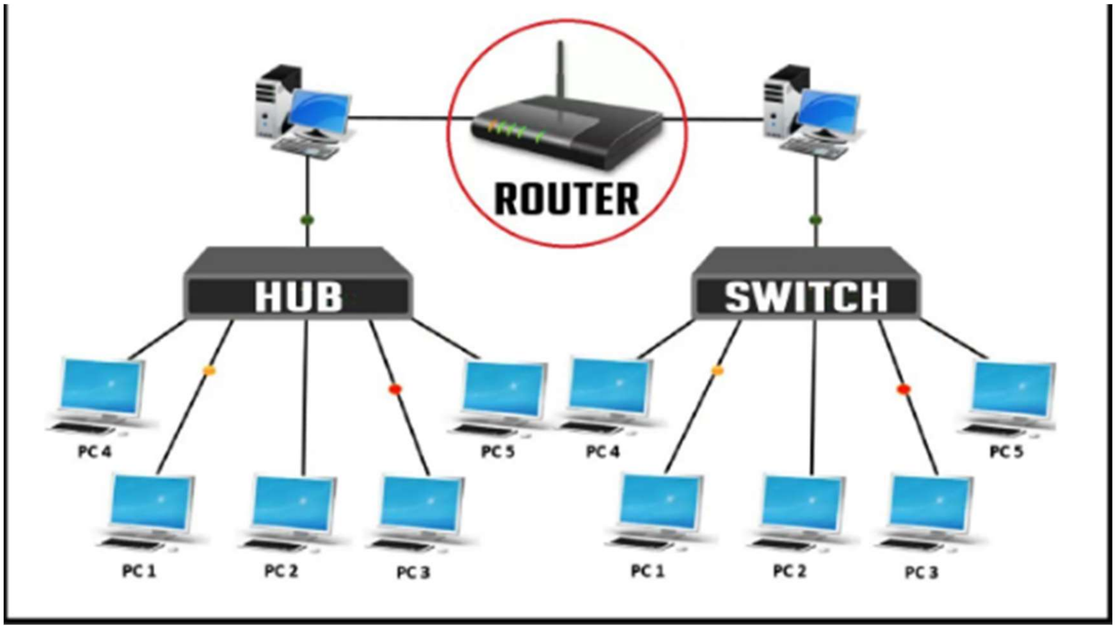
- **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.
- **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

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

Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

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.

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.

Features Of Computer network

A list Of Computer network features is given below.

- Communication speed
- File sharing
- Back up and Roll back is easy
- Software and Hardware sharing
- Security
- Scalability
- Reliability

Communication speed

Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.

File sharing

File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.

Back up and Roll back is easy

Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

Backward Skip 10sPlay VideoForward Skip 10s

Software and Hardware sharing

We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

Security

Network allows the security by ensuring that the user has the right to access the certain files and applications.

Scalability

Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But, it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.

Reliability

Computer network can use the alternative source for the data communication in case of any hardware failure.

Computer Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

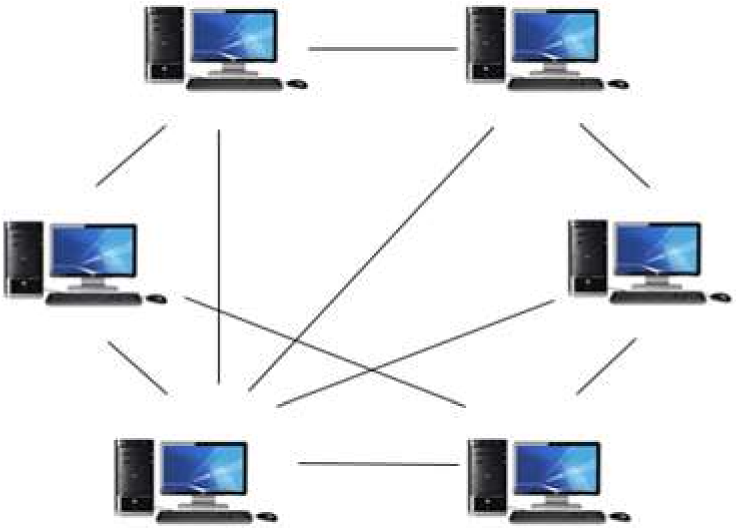
The two types of network architectures are used:

- Peer-To-Peer network

- Client/Server network

Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network:

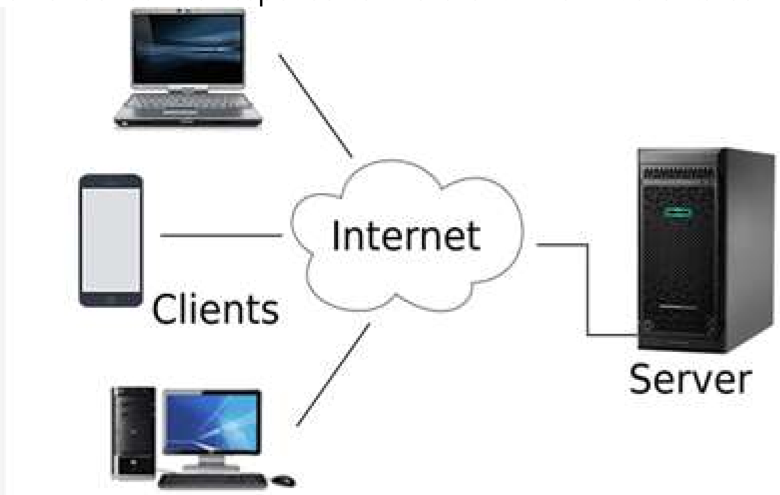
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Computer Network Types

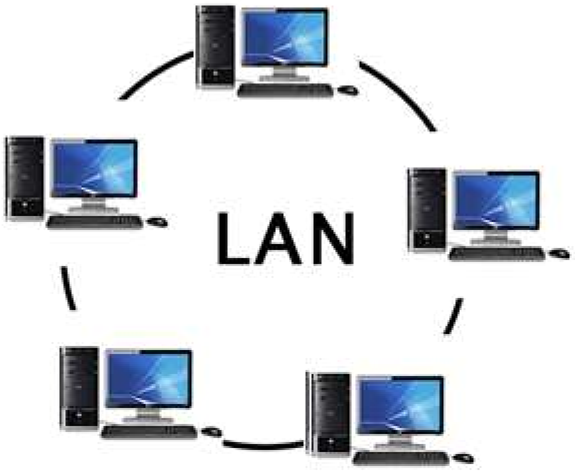
A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

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)

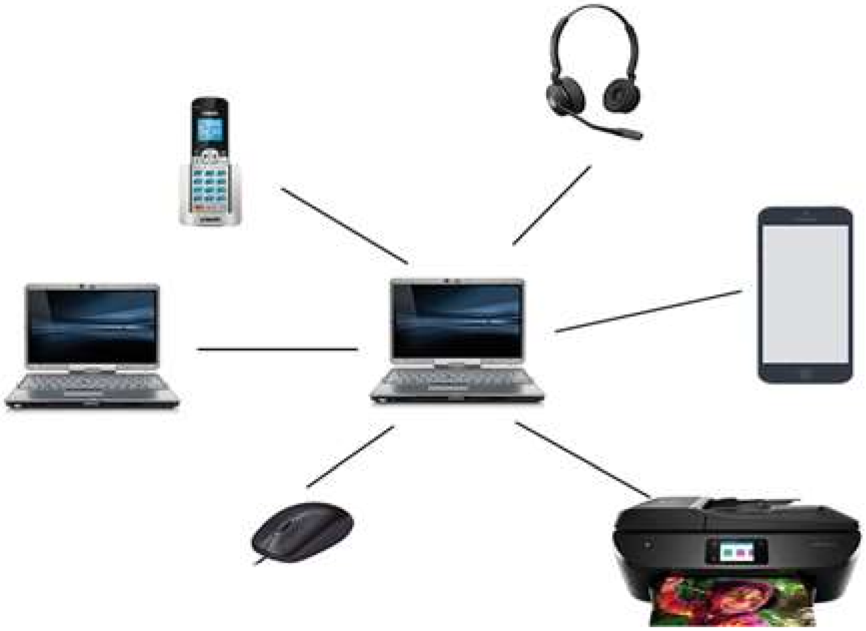
LAN(Local Area Network)

- 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.



There are two types of Personal Area Network:

- Wired Personal Area Network
- Wireless Personal Area Network

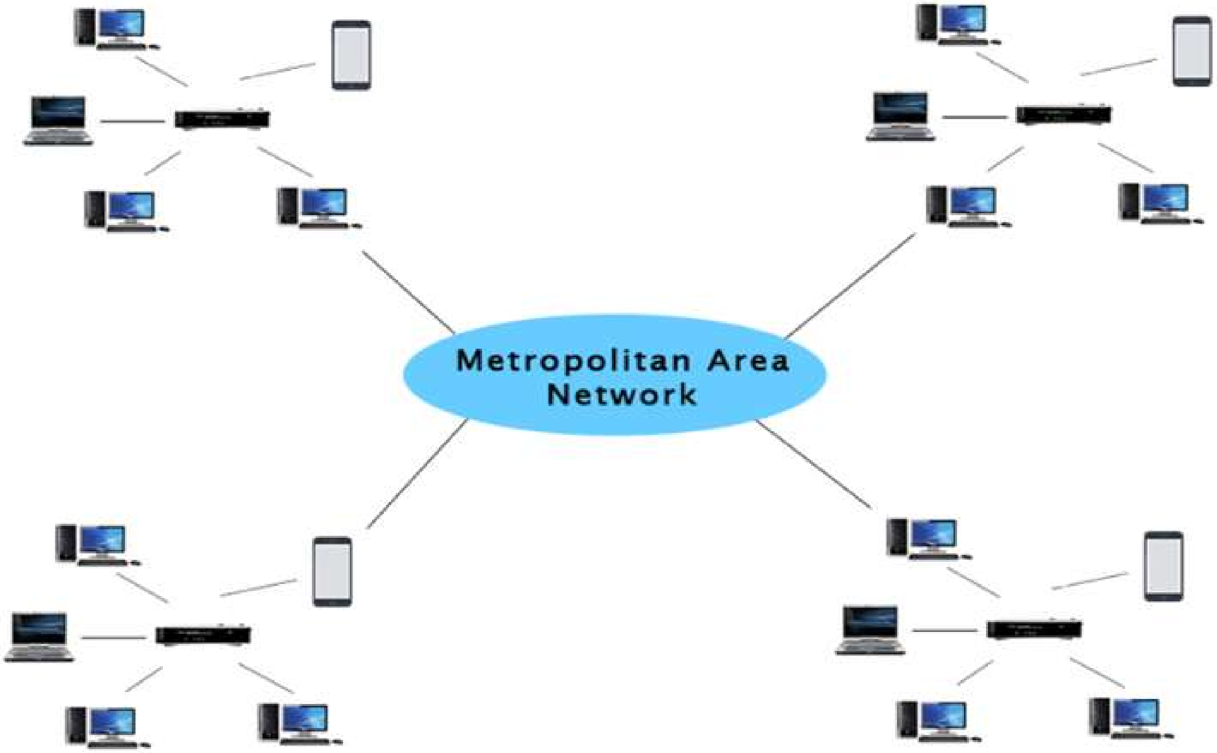
Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

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

MAN(Metropolitan Area Network)

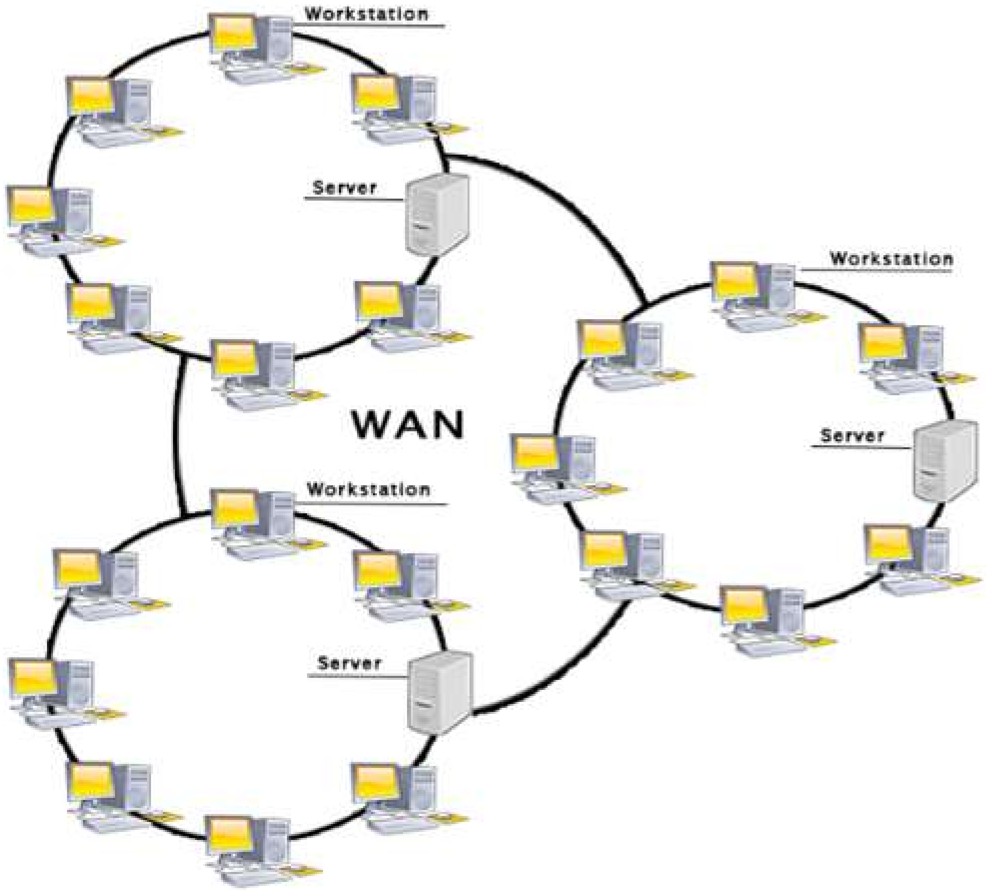
- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.

- In MAN, various LANs are connected to each other through a telephone exchange line.
- It has a higher range than Local Area Network(LAN).



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



What is World Wide Web?

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP. These links are electronic connections that link related pieces of information so that users can access the desired information quickly. Hypertext offers the advantage to select a word or phrase from text and thus to access other pages that provide additional information related to that word or phrase.

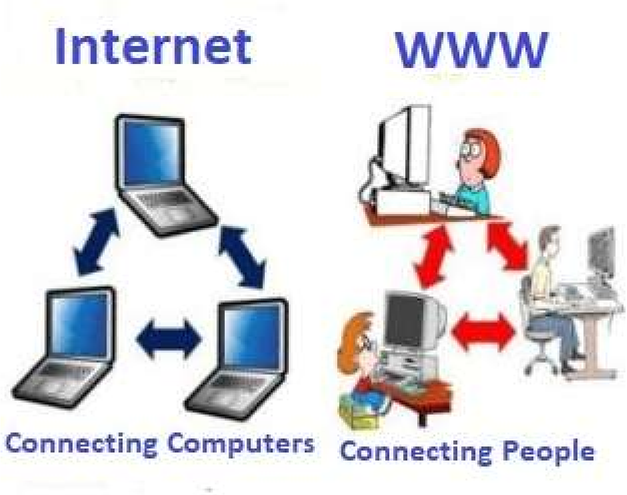
A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., *www.facebook.com*, *www.google.com*, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

Small websites store all of their WebPages on a single server, but big websites or organizations place their WebPages on different servers in different countries so that when users of a country search their site they could get the information quickly from the nearest server.

So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web.

Difference between World Wide Web and Internet:

Some people use the terms 'internet' and 'World Wide Web' interchangeably. They think they are the same thing, but it is not so. Internet is entirely different from WWW. It is a worldwide network of devices like computers, laptops, tablets, etc. It enables users to send emails to other users and chat with them online. For example, when you send an email or chatting with someone online, you are using the internet.



But, when you have opened a website like google.com for information, you are using the World Wide Web; a network of servers over the internet. You request a webpage from your computer using a browser, and the server renders that page to your browser. Your computer is called a client who runs a program (web browser), and asks the other computer (server) for the information it needs.

Good Security Habits

There are some simple habits you can adopt that, if performed consistently, may reduce the chances that the information on your computer will be lost or corrupted.

- **Improve password security.** Passwords are one of the most vulnerable cyber defenses. Improve your password security by doing the following
  - **Create a strong password.** Use a strong password that is unique for each device or account. Longer passwords are more secure. An option to help you create a long password is using a passphrase—four or more random words grouped together and used as a password. To create strong passwords, the National Institute of Standards and Technology (NIST) suggests using
  - **Use security questions properly.** For accounts that ask you to set up one or more password reset questions, use private information about yourself

that only you would know. Answers that can be found on your social media or facts everyone knows about you can make it easier for someone to guess your password.

    - **Create unique accounts for each user per device.** Set up individual accounts that allow only the access and permissions needed by each user. When you need to grant daily use accounts administrative permissions, do so only temporarily. This precaution reduces the impact of poor choices, such as clicking on phishing emails or visiting malicious websites.
- **Choose secure networks.** Use internet connections you trust, such as your home service or Long-Term Evolution connection through your wireless carrier. Public networks are not very secure, which makes it easy for others to intercept your data. If you choose to connect to open networks, consider using antivirus and firewall software on your device or using a Virtual Private Network service, which allows you to connect to the internet securely by keeping your exchanges private. When setting up your home wireless network, use Wi-Fi Protected Accessed 3 (WPA3) encryption. All other wireless encryption methods are outdated and more vulnerable to exploitation. (See Securing Wireless Networks.)
- **Keep all of your personal electronic device software current.** Manufacturers issue updates as they discover vulnerabilities in their products. Automatic updates make this easier for many devices—including computers, phones, tablets, and other smart devices—but you may need to manually update other devices. Only apply updates from manufacturer websites and built-in application stores—third-party sites and applications are unreliable and can result in an infected device. When shopping for new connected devices, consider the brand's consistency in providing regular support updates.
- **Be suspicious of unexpected emails.** Phishing emails are currently one of the most prevalent risks to the average user. The goal of a phishing email is to gain information about you, steal money from you, or install malware on your device. Be suspicious of all unexpected emails. (See Avoiding Social Engineering and Phishing Attacks.)

In computer systems, the security of data is always a major concern because there are some unidentified people (known as hackers) who always try to steal or harm the personal data or information of the users using viruses, worms, trojans, etc. So, to protect computer systems from these viruses or any other harmful activity, software is developed and that software is known as Antivirus software.

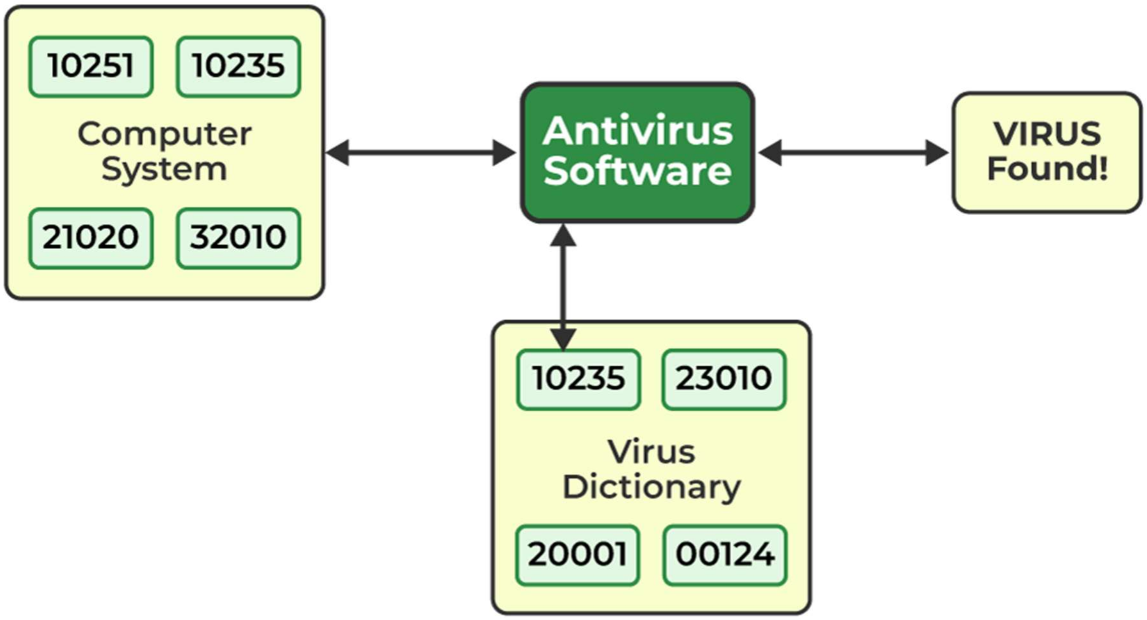
What is Antivirus Software?

Antivirus software (computer protection software) is a program(s) that is created to search, detect, prevent and remove software viruses from your system that can harm your system. Other harmful software such as worms, adware, and other threats can also be detected and removed via antivirus. This software is designed to be used as a proactive approach to cyber security, preventing threats from entering your computer and causing issues. Most antivirus software operates in the background once installed, providing real-time protection against virus attacks.

While you may believe that your computer is safe as long as you don't visit questionable websites, hackers have far more sophisticated methods of infecting your computer, which is why you need a powerful antivirus to stay to secure your data and system. The implications of a virus getting into your computer might be fatal. Viruses can cause a wide range of malicious behaviour. They can crash your device, monitor your accounts, or spy on you through your webcam. So, always use antivirus software.

How Antivirus Works?

Antivirus software works by comparing your computer applications and files to a database of known malware kinds. Because hackers are continually creating and disseminating new viruses, they will also check systems for the presence of new or undiscovered malware threats. The antivirus checks files, programs, and applications going in and out of your computer to its database to identify matches. Similar and identical matches to the database are segregated, scanned, and eliminated.



How Antivirus Works?

Most Antivirus programs will employ these four types of detection techniques:

- **Signature detection** is a method by which an antivirus keenly scans files that are brought into a system to analyze more likely hazardous files.
- **Specific detection**, which looks for known parts or types of malware or patterns that are linked by a common codebase
- **A genericthe detection** is a type of detection that looks for known parts or types of malware or patterns that are related to a common codebase.
- **Heuristic detection** is a type of virus detection that looks for unknown infections by spotting suspicious file structures.

To learn more about computer security threats, please see this article

Examples of Antivirus Software

The antivirus software is available in 2 types:

(i) Free: Free anti-virus software provides basic virus protection

(ii) Paid: commercial anti-virus software provides more extensive protection.

The following are some commonly used antivirus software:

1. Bitdefender: Bitdefender Total Security is a comprehensive security suite that protects against viruses and dangerous malware of all varieties. This user-friendly antivirus software is compatible with all four major operating systems and smart homes, and it also includes a free VPN with a daily limit of 200MB, parental controls, camera protection, a password manager, etc. This security suite is reasonably priced and will protect up to five devices 24 hours a day, seven days a week.

2. AVAST: This is a free antivirus available. All you have to do to obtain top-notch protection on your computer, emails, downloads, and instant messages in the free version is register (for free) once a year. It includes a sophisticated heuristics engine that enables it to detect viruses**.**

3. Panda: It can detect viruses, trojans, spyware, adware, worms, and malware at the same level as other antiviruses do. It is different from others because using this software, when you scan your computer, it doesn't consume any of your computer's resources instead, it runs in the cloud, allowing your machine to continue to function normally.

Benefits of Antivirus Software

- **Spam and advertisements are blocked:** Viruses exploit pop-up advertising and spam websites as one of the most common ways to infect your computer and destroy your files. Antivirus acts against harmful virus-infected adverts and websites by denying them direct access to your computer network.
- **Virus protection and transmission prevention:** It identifies any possible infection and then attempts to eliminate it.
- **Hackers and data thieves are thwarted:** Antivirus do regular checks to see if there are any hackers or hacking-related apps on the network. As a result, antivirus offers complete security against hackers.
- **Protected against devices that can be detached:** Antivirus scans all removable devices for potential viruses, ensuring that no viruses are transferred.
- **To improve security from the** to**web, restrict website access:** Antivirus restricts your online access in order to prevent you from accessing unauthorized networks. This is done to ensure that you only visit websites that are safe and non-harmful to your computer.

- **Password Protection:** Using antivirus, you should consider using a password manager for added security.

Disadvantages of Antivirus programs

- **Slows down system's speed:** When you use antivirus programs, you're using a lot of resources like your RAM and hard drive. As a result, the computer's overall speed may be significantly slowed.
- **Popping up of Advertisements:** Apart from commercial antivirus applications, free antivirus must make money in some way. One approach to attaining these is through advertising. Many times these advertisements degrade the user experience by popping up every time.
- **No customer care service:** There will be no customer service provided unless you pay for the premium version. If an issue arises, the only method to solve it is to use forums and knowledge resources.

Computer Virus

Computer viruses are unwanted software programs or pieces of code that interfere with the functioning of the computer. They spread through contaminated files, data, and insecure networks. Once it enters your system, it can replicate to produce copies of itself to spread from one program to another program and from one infected computer to another computer. So, we can say that it is a self-replicating computer program that interferes with the functioning of the computer by infecting files, data, programs, etc.

There are many antiviruses, which are programs that can help you protect your machine from viruses. It scans your system and cleans the viruses detected during the scan. Some of the popular antiviruses include Avast, Quickheal, McAfee, Kaspersky, etc.

Symptoms of a Computer Virus:

There are many warning signs or symptoms which show that a computer is infected with a virus, some of which are as follows:

- **Slow computer performance:** The machine may work slowly, e.g., it will take more time to open or shut down the computer or while opening a file, document, computer application, etc. The operating system and internet speed may get slow.
- **Frequent pop-ups:** A virus may cause unusual frequent pop-ups on your window.

- **Hard Drive issue:** The hard drive may exhibit unusual high activity even when it is not in use. It may cause unwanted changes to your hard drive and may freeze or crash this device.
- **Frequent crashes:** One may experience frequent sudden system crashes while playing games, watching videos, or doing some other work using the infected system. A blue screen appears when it crashes.
- **Unknown programs:** Unwanted programs may open or start automatically when you start your computer. You can see these programs in your computer's list of active applications. Sometimes, the window shuts down unexpectedly without any reason.
- **Unusual activities:** Your machine may perform differently, such as you may not be able to log into your accounts, to delete the corrupt files, and Blue Screen of Death (BSOD) may appear frequently, and more. Furthermore, the hardware, software, or OS may start malfunctioning leading to crashing the system abruptly.
- **Impaired security solutions:** Sometimes, security measures taken by you, such as antivirus may not work smoothly due to virus attack on your computer.
- **Network issue:** Sometimes, you experience high network activity even if you are not connected to the internet and vice versa.
- **Unnecessary advertisement:** We often see advertisements while browsing, but if you see them even when you are not browsing, it may indicate a virus on your computer.
- **Display problems:** You may experience different colors in your display if your computer is affected by a virus.
- **Affected Applications:** Some viruses are developed to affect specific applications. Consequently, some applications may not work on your computer if it is infected.
- **Blocked by Antivirus Sites:** An antivirus site may deny access to a computer that is infected by a virus.
- **Dialog Boxes:** Many dialog boxes keep appearing suddenly on your screen.
- **Printer Issues:** A printer attached to an infected computer may print documents without getting any command or in an inappropriate manner.
- **Changed Homepage:** Your home page may get changed without any effort from your side. For example, you may see a new toolbar on your screen, and you may be redirected to a different web address instead of the page visited by you initially.

- **Strange messages:** One may see strange messages on a computer screen such as error messages, e.g., "cannot rename "folder" as a folder already exists with this name"

VIRUS: Vital Information Resources Under Seize

A **computer virus** is *a computer program or a piece of code* that is loaded onto your computer without your knowledge and run against your consent. Virus has a property to replicate itself and spread itself from one computer to another computer. It can affect the data files, boot sector of hard drive etc. when its replication succeeds. The affected area is said infected.

Viruses are human made programs generally write to access private information, corrupt data, to display political and humorous messages on the user's screen. They insert themselves into host programs and spread on the execution of infected programs.

Computer viruses cause damage of billions of dollars worth every year. The majority of viruses target systems running Microsoft window. To counter with viruses, programmers created anti-virus programs.

Harmful Effects of Computer Viruses

- Can corrupt your system file and slow down your computer system
- Can make some programs corrupt or faulty
- Can damage computer's boot sector
- Can steal your computer's information and send it to another person
- Can delete your complete hard drive
- Can display irrelevant and annoying messages on your computer screen
- Can change the power rating of your computer which may cause of blast

Types of Computer Viruses

This is a list of common types of computer viruses.

1. Boot sector viruses
2. Program viruses

3. Multipartite viruses
4. Stealth viruses
5. Macro viruses
6. Polymorphic viruses
7. Active X viruses
8. Browser hijacker
9. Resident viruses
10. File infector viruses

List of malwares which are generally categorized as computer viruses:

- Computer Worms
- Trojan horse
- Spam virus
- Spyware
- Zombies

Difference between Virus, Worm, and Trojan horse

When discussing computer viruses, the most common problem is to refer to a ***worm*** or ***trojan horse*** as a ***virus***. However, the phrases Trojan, worm, and virus are sometimes interchangeable, and they are not identical. Malicious software like viruses, worms, and trojan horses may damage the computer system. Before diving into the differences between viruses, worms, and Trojan horses, you should be familiar with the term **"*Malware*"**. Malware is a malicious program that is mainly designed to damage or harm systems. The term **"*malware*"** is an abbreviation for **"*malicious software*"**.

In this article, you will learn about the difference between viruses, worms, and Trojan horses. But before discussing the differences, you must know about ***viruses, worms***, and ***trojan horses***.

What is Virus?

A ***virus*** is a computer program that connects to another computer software or program to harm the system. When the legitimate program runs, the virus may execute any function, like deleting a file. The main task of a virus is that when an infected software or program is run, it would first run the virus and then the legitimate program code will run. It may also affect the other programs on the computer system.

After damaging all files on the current user's computer, the virus spreads and sends its code via the network to the users whose e-mail addresses are stored on the current user's computer system. Specific events may also trigger a virus. Several types of viruses include parasitic, polymorphic, stealth, boot sector, memory resident, and metamorphic viruses. Infection with a virus can be avoided by blocking the entry of a virus.

What is Worm?

A ***worm*** is a form of a ***malicious program (virus)*** that replicates itself as it moves from one system to another and leaves copies of itself in the memory of each system. A worm discovers vulnerability in a computer and spreads like an infection throughout its related network, continuously looking for more holes. E-mail attachments spread the worms from reliable senders. Worms are spread to a user's contacts through an address book and e-mail account.

Some worms reproduce before going dormant, while others cause harm. In such circumstances, the code of the worm's virus is known as the ***payload***.

What is a Trojan horse?

The ***Trojan horse*** gets its name from the well-known story of the ***Trojan War***. It is a malicious piece of code with the ability to take control of the system. It is intended to steal, damage, or do some other harmful actions on the computer system. It attempts to deceive the user into loading and running the files on the device. Once it executes, it permits cybercriminals to execute various tasks on the user's system, like modifying data from files, deleting data from files, etc. The trojan horse cannot replicate itself, unlike many viruses or worms.

A Trojan virus spreads by spamming a huge number of users' inboxes with genuine-looking e-mails and attachments. If cybercriminals induce users to download malicious software, it may affect the users' devices. Malicious malware could be hidden in pop-up ads, banner adverts, or website links.

Some well-known Trojan horses' instances are ***Beast, Back Orifice, Zeus, and The Blackhole Exploit Kit***.

Key differences between the Virus, Worm, and Trojan horse

There are various key differences between ***Viruses, Worms***, and ***Trojan horses***. Some of the key differences between Viruses, Worm, and Trojan horses are as follows:

The main differences between Viruses, Worms, and Trojan horses are as follows:

Features	Virus	Worm	Trojan horse
Definition	Viruses are computer programs that connect to other software or programs to harm the system.	A worm is a malware program similar to a virus that doesn't interact with other system applications but instead multiplies and executes itself to slow down and harm the system's performance.	A Trojan Horse is a type of malware that steals sensitive data from a user's system and delivers it to a different location on the network.
Replication	It replicates itself.	It also replicates itself.	It doesn't replicate itself.
Execution	It relies on the transfer.	It replicates itself without human action and utilizes a network to embed itself in other systems.	It is downloaded as software and executed.

Remotely Controlled	A virus could not be remotely controlled.	It may be remotely controlled.	It may also be remotely controlled.
Infection	Viruses spread through executable files.	Worms take advantage of system flaws.	The Trojan horse runs as a program and is interpreted as utility software.
Rate of Spreading	Viruses spread at a moderate rate.	Worms spread at a quicker rate than viruses and Trojan horses.	In addition, the spread rate of Trojan horses is slower than that of viruses and worms.
Purpose	It is primarily utilized to modify or erase system data.	These are utilized to excessive using system resources and slow it down.	It may be utilized to steal user data to obtain access to the user's computer system.

What is a Worm?

Worms are the type of virus that can self-replicate and travel from device to device using a computer network. That means worms don't need any host to spread. They are standalone computer malware that doesn't even require human support to execute. Usually, worms use computer networks by exploiting vulnerabilities, and that makes them spread more quickly.

Besides, worms stay within the memory of an infected computer, making a computer think they are part of the system files. This helps worms to avoid any suspicious detection. Unlike a typical virus, worms don't harm the system data. Instead, they tend to consume system resources like CPU, memory, or network bandwidth and make the entire system or network crash. Because of self-replicating nature, worms can even disrupt systems in a series worldwide using a network.

How does a worm spread?

Unlike viruses, worms don't require host files to spread. This means that worms do not attach themselves with executable files or programs. Instead, worms find a weak spot in the system and enter through a vulnerability in the network. Before we detect and remove worms from our system, they replicate and spread automatically and consume all the network bandwidth. This can result in the failure of the entire network and web servers. Because worms can spread automatically, their spreading speed is comparatively faster than other malware.

Apart from this, worms can also reach other networks that are attached to the infected system. The most dangerous thing is that the worms can send themselves into other systems using email services.

Key Differences between Virus and Worm

Few key differences between Virus and Worm are listed below:

- Worms usually spread using a computer network, whereas viruses use executable files to spread from one system to others.
- Worms can automatically replicate to different systems, while viruses require human action to replicate.
- The spreading speed of viruses is comparatively slower than worms. Because worms can replicate automatically, they spread at a much faster speed.
- The viruses are designed to corrupt, delete, or modify the target devices' data or software, whereas worms don't harm the stored data but aim to harm the resources.
- Viruses are found in executable files or can attach themselves to executable files to operate on target devices, whereas worms remain independent in an infected device's memory.
- The viruses require hosts to spread from one device to another. Worms, on the other side, don't need any host.
- Viruses usually destroy and damage the stored data, whereas worms can harm the entire network by using maximum resources. For example- by consuming bandwidth, sending mass emails, or deleting or copying files in bulk.

Major Differences between Virus and Worm

The other major differences between a virus and a worm can be explained in a tabulated form, as below:

Attributes	Virus	Worm
Nature	The virus is a malicious program attached to the executable files so that it can spread from one system to another.	A worm is a program made up of malicious code that replicates itself and propagates itself from device to device using a network.
Human Action	Human action is required for viruses. Without human help, they cannot execute and spread.	Human action is not required for the worms. They are designed and developed in such a way that they can automatically execute and spread.
Speed of Spread	The virus spreads at a relatively slower speed than a Worm.	Worms spreading speed is fast, and they can infect multiple devices or networks quickly.
Host Requirement	The host is required to spread viruses. Viruses connect themselves to the host and travel with the host. They spread into devices where the host reaches.	The host is not necessary for the worms to replicate from one device to another. Worms exploit the vulnerability of a network to spread.
Protection Method	To protect the devices from viruses, the user must have installed trusted antivirus software.	To protect the devices from worms, the user is required to use antivirus software and a firewall. Many modern antivirus software come with an in-built firewall system.
Malware Removal	To clean the virus's infection or stop spreading it further, the user must scan the device using antivirus software and remove the infected files. Sometimes, formatting an entire system is the only option to remove the infection completely.	To remove the worm's infection, the user needs a virus removal tool. Also, users must allow only trusted software through a firewall to eliminate the chances of spreading worms. In a complex situation, formatting the system is the best option.
Consequences	Viruses can corrupt, alter, or delete the stored files or programs in the infected device.	Worms do not harm stored files or software; instead, they consume system resources and increase the system's load. This eventually

		leads to slow processing and system crashes. Also, it can result in network failures.

****