BASIC COMPUTER SCIENCE

Topic 1 : Computer History & Fundamentals

The computer was born not for entertainment or email but out of a need to solve a serious number-crunching crisis. By 1880, the U.S. population had grown so large that it took more than seven years to tabulate the U.S. Census results. The government sought a faster way to get the job done, giving rise to punch-card based computers that took up entire rooms.

Today, we carry more computing power on our smartphones than was available in these early models. The following brief history of computing is a timeline of how computers evolved from their humble beginnings to the machines of today that surf the Internet, play games and stream multimedia in addition to crunching numbers.

1801: In France, Joseph Marie Jacquard invents a loom that uses punched wooden cards to automatically weave fabric designs. Early computers would use similar punch cards.
1822: English mathematician Charles Babbage conceives of a steam-driven calculating machine that would be able to compute tables of numbers. The project, funded by the English government, is a failure. More than a century later, however, the world's first computer was actually built.
1890: Herman Hollerith designs a punch card system to calculate the 1880 census, accomplishing the task in just three years and saving the government $5 million. He establishes a company that would ultimately become IBM.
1936: Alan Turing presents the notion of a universal machine, later called the Turing machine, capable of computing anything that is computable. The central concept of the modern computer was based on his ideas.
1937: J.V. Atanasoff, a professor of physics and mathematics at Iowa State University, attempts to build the first computer without gears, cams, belts or shafts.
1941: Atanasoff and his graduate student, Clifford Berry, design a computer that can solve 29 equations simultaneously. This marks the first time a computer is able to store information on its

main memory.

1943-1944: Two University of Pennsylvania professors, John Mauchly and J. Presper Eckert, build the Electronic Numerical Integrator and Calculator (ENIAC**)**. Considered the grandfather of digital computers, it fills a 20-foot by 40-foot room and has 18,000 vacuum tubes.
1946: Mauchly and Presper leave the University of Pennsylvania and receive funding from the Census Bureau to build the UNIVAC, the first commercial computer for business and government applications.
1947: William Shockley, John Bardeen and Walter Brattain of Bell Laboratories invent the transistor. They discovered how to make an electric switch with solid materials and no need for a vacuum.
1953: Grace Hopper develops the first computer language, which eventually becomes known as COBOL. Thomas Johnson Watson Jr., son of IBM CEO Thomas Johnson Watson Sr., conceives the IBM 701 EDPM to help the United Nations keep tabs on Korea during the war.
1954: The FORTRAN programming language, an acronym for FORmula TRANslation, is developed by a team of programmers at IBM led by John Backus, according to the University of Michigan.
1958: Jack Kilby and Robert Noyce unveil the integrated circuit, known as the computer chip. Kilby was awarded the Nobel Prize in Physics in 2000 for his work.
1964: Douglas Engelbart shows a prototype of the modern computer, with a mouse and a graphical user interface (GUI**)**. This marks the evolution of the computer from a specialized machine for scientists and mathematicians to technology that is more accessible to the general public.
1969: A group of developers at Bell Labs produce UNIX, an operating system that addressed compatibility issues. Written in the C programming language, UNIX was portable across multiple platforms and became the operating system of choice among mainframes at large companies and government entities. Due to the slow nature of the system, it never quite gained traction among home PC users.
1970: The newly formed Intel unveils the Intel 1103, the first Dynamic Access Memory (DRAM) chip.
1971: Alan Shugart leads a team of IBM engineers who invent the "floppy disk," allowing data to be shared among computers.
1973: Robert Metcalfe, a member of the research staff for Xerox, develops Ethernet for connecting multiple computers and other hardware.
1974-1977: A number of personal computers hit the market, including Scelbi & Mark-8 Altair, IBM 5100, Radio Shack's TRS-80 — affectionately known as the "Trash 80" — and the Commodore PET.
1975: The January issue of Popular Electronics magazine features the Altair 8080, described as the "world's first minicomputer kit to rival commercial models." Two "computer geeks," Paul Allen and Bill Gates, offer to write software for the Altair, using the new BASIC language. On April 4, after the success of this first endeavor, the two childhood friends form their own software company, Microsoft.
1976: Steve Jobs and Steve Wozniak start Apple Computers on April Fool's Day and roll out the Apple I, the first computer with a single-circuit board, according to Stanford University.
1977: Radio Shack's initial production run of the TRS-80 was just 3,000. It sold like crazy. For the first time, non-geeks could write programs and make a computer do what they wished.
1977: Jobs and Wozniak incorporate Apple and show the Apple II at the first West Coast Computer Faire. It offers color graphics and incorporates an audio cassette drive for storage.

1978: Accountants rejoice at the introduction of VisiCalc, the first computerized spreadsheet program
1981: The first IBM personal computer, code-named "Acorn," is introduced. It uses Microsoft's MS-DOS operating system. It has an Intel chip, two floppy disks and an optional color monitor.

Sears & Roebuck and Computerland sell the machines, marking the first time a computer is available through outside distributors. It also popularizes the term PC.
1983: Apple's Lisa is the first personal computer with a GUI. It also features a drop-down menu and icons. It flops but eventually evolves into the Macintosh. The Gavilan SC is the first portable computer with the familiar flip form factor and the first to be marketed as a "laptop."
1985: Microsoft announces Windows, according to Encyclopedia Britannica. This was the company's response to Apple's GUI. Commodore unveils the Amiga 1000, which features advanced audio and video capabilities.
1985: The first dot-com domain name is registered on March 15, years before the World Wide Web would mark the formal beginning of Internet history. The Symbolics Computer Company, a small Massachusetts computer manufacturer, registers Symbolics.com. More than two years later, only 100 dot-coms had been registered.
1986: Compaq brings the Deskpro 386 to market. Its 32-bit architecture provides as speed comparable to mainframes.
1990: Tim Berners-Lee, a researcher at CERN, the high-energy physics laboratory in Geneva, develops HyperText Markup Language (HTML), giving rise to the World Wide Web.
1993: The Pentium microprocessor advances the use of graphics and music on PCs.
1994: PCs become gaming machines as "Command & Conquer," "Alone in the Dark 2," "Theme Park," "Magic Carpet," "Descent" and "Little Big Adventure" are among the games to hit the market.
1996: Sergey Brin and Larry Page develop the Google search engine at Stanford University.
1997: Microsoft invests $150 million in Apple, which was struggling at the time, ending Apple's court case against Microsoft in which it alleged that Microsoft copied the "look and feel" of its operating system.
1999: The term Wi-Fi becomes part of the computing language and users begin connecting to the Internet without wires.
2001: Apple unveils the Mac OS X operating system, which provides protected memory architecture and pre-emptive multi-tasking, among other benefits. Not to be outdone, Microsoft rolls out Windows XP, which has a significantly redesigned GUI.
2003: The first 64-bit processor, AMD's Athlon 64, becomes available to the consumer market.
2004: Mozilla's Firefox 1.0 challenges Microsoft's Internet Explorer, the dominant Web browser. Facebook, a social networking site, launches.
2005: YouTube, a video sharing service, is founded. Google acquires Android, a Linux-based mobile phone operating system.
2006: Apple introduces the MacBook Pro, its first Intel-based, dual-core mobile computer, as well as an Intel-based iMac. Nintendo's Wii game console hits the market.
2007: The iPhone brings many computer functions to the smartphone.
2009: Microsoft launches Windows 7, which offers the ability to pin applications to the taskbar and advances in touch and handwriting recognition, among other features.
2010: Apple unveils the iPad, changing the way consumers view media and jumpstarting the dormant tablet computer segment.
2011: Google releases the Chromebook, a laptop that runs the Google Chrome OS.

2012: Facebook gains 1 billion users on October 4
2015: Apple releases the Apple Watch. Microsoft releases Windows 10.
2016: The first reprogrammable quantum computer was created. "Until now, there hasn't been any quantum-computing platform that had the capability to program new algorithms into their system. They're usually each tailored to attack a particular algorithm," said study lead author Shantanu Debnath, a quantum physicist and optical engineer at the University of Maryland, College Park.
2017: The Defense Advanced Research Projects Agency (DARPA) is developing a new "Molecular Informatics" program that uses molecules as computers.

Generation in computer terminology is a change in technology a computer is/was being used. Initially, the generation term was used to distinguish between varying hardware technologies. Nowadays, generation includes both hardware and software, which together make up an entire computer system.

There are five computer generations known till date. Each generation has been discussed in detail along with their time period and characteristics. In the following table, approximate dates against each generation has been mentioned, which are normally accepted.

Sl No	Generation & Description
1	**First Generation** The period of first generation: 1946-1959. Vacuum tube based.
2	**Second Generation** The period of second generation: 1959-1965. Transistor based.
3	**Third Generation** The period of third generation: 1965-1971. Integrated Circuit based.
4	**Fourth Generation** The period of fourth generation: 1971-1980. VLSI microprocessor based.
5	**Fifth Generation** The period of fifth generation: 1980-onwards. ULSI microprocessor based.

Functionalities of a Computer

If we look at it in a very broad sense, any digital computer carries out the following five functions:

- Step 1 - Takes data as input.
- Step 2 - Stores the data/instructions in its memory and uses them as required.
- Step 3 - Processes the data and converts it into useful information.
- Step 4 - Generates the output.
- Step 5 - Controls all the above four steps.

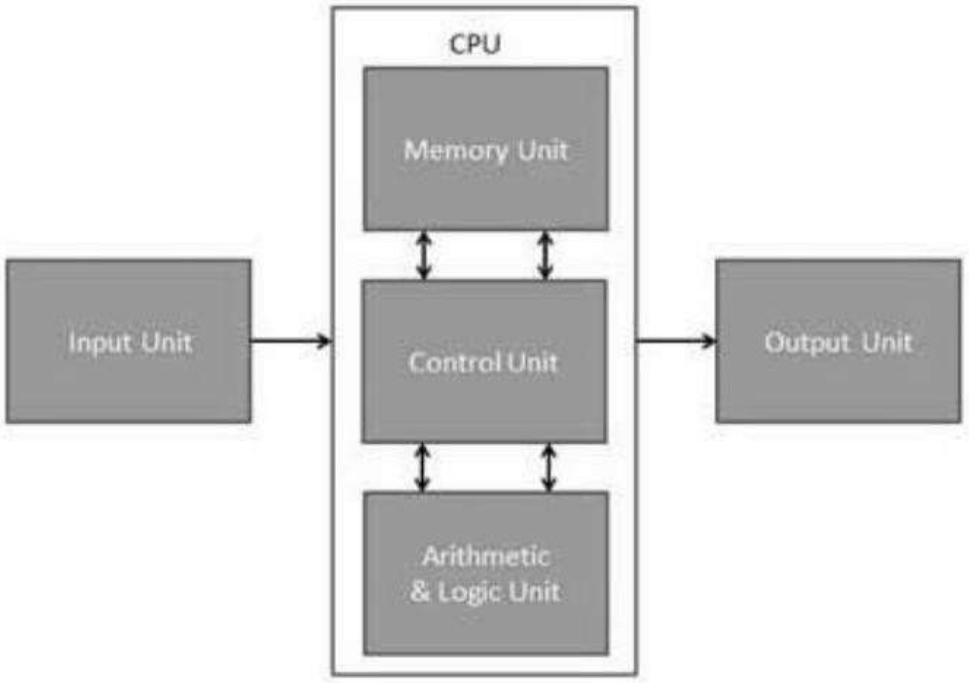
Computers can be broadly classified by their speed and computing power.

Sr. No.	Type	Specifications
1	PC (Personal Computer)	It is a single user computer system having moderately powerful microprocessor
2	Workstation	It is also a single user computer system, similar to personal computer however has a more powerful microprocessor
3	Mini Computer	It is a multi-user computer system, capable of supporting hundreds of users simultaneously.
4	Main Frame	It is a multi-user computer system, capable of supporting hundreds of users simultaneously. Software technology is different from minicomputer.
5	Supercomputer	It is an extremely fast computer, which can execute hundreds of millions of instructions per second.

Fundamentals of a Computer:

All types of computers follow the same basic logical structure and perform the following five basic operations for converting raw input data into information useful to their users.

Sr. No.	Operation	Description
1	Take Input	The process of entering data and instructions into the computer system.
2	Store Data	Saving data and instructions so that they are available for processing as and when required.
3	Processing Data	Performing arithmetic, and logical operations on data in order to convert them into useful information.
4	Output Information	The process of producing useful information or results for the user, such as a printed report or visual display.
5	Control the workflow	Directs the manner and sequence in which all of the above operations are performed.



Input Unit

This unit contains devices with the help of which we enter data into the computer. This unit creates a link between the user and the computer. The input devices translate the information into a form understandable by the computer.

CPU (Central Processing Unit)

CPU is considered as the brain of the computer. CPU performs all types of data processing operations. It stores data, intermediate results, and instructions (program). It controls the operation of all parts of the computer.

CPU itself has the following three components:

- ALU (Arithmetic Logic Unit)
- Memory Unit
- Control Unit

Output Unit

The output unit consists of devices with the help of which we get the information from the computer. This unit is a link between the computer and the users. Output devices translate the computer's output into a form understandable by the users.

TOPIC 2: Operating System

What is an operating system?

An operating system is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of its software and hardware. It also allows you to communicate with the computer without knowing how to speak the computer's language. Without an operating system, a computer is useless.

The operating system's job

Your computer's operating system (OS) manages all of the software and hardware on the computer. Most of the time, there are several different computer programs running at the same time, and they all need to access your computer's central processing unit (CPU), memory, and storage. The operating system coordinates all of this to make sure each program gets what it needs.

Types of operating systems

Operating systems usually come pre-loaded on any computer you buy. Most people use the operating system that comes with their computer, but it's possible to upgrade or even change operating systems. The three most common operating systems for personal computers are Microsoft Windows, macOS, and Linux.Modern operating systems use a graphical user interface, or GUI (pronounced gooey). A GUI lets you use your mouse to click icons, buttons, and menus, and everything is clearly displayed on the screen using a combination of graphics

and text.

Microsoft Windows

Microsoft created the Windows operating system in the mid-1980s. There have been many different versions of Windows, but the most recent ones are Windows 10 (released in 2015), Windows 8 (2012), Windows 7 (2009), and Windows Vista (2007). Windows comes pre-loaded on most new PCs, which helps to make it the most popular operating system in the world.

macOS

macOS (previously called OS X) is a line of operating systems created by Apple. It comes preloaded on all Macintosh computers, or Macs. Some of the specific versions include Mojave (released in 2018), High Sierra (2017), and Sierra (2016).

According to StatCounter Global Stats, macOS users account for less than 10% of global operating systems—much lower than the percentage of Windows users (more than 80%). One reason for this is that Apple computers tend to be more expensive. However, many people do prefer the look and feel of macOS over Windows.

Linux

Linux (pronounced LINN-ux) is a family of open-source operating systems, which means they can be modified and distributed by anyone around the world. This is different from proprietary software like Windows, which can only be modified by the company that owns it. The advantages of Linux are that it is free, and there are many different distributions—or versions—you can choose from.

According to StatCounter Global Stats, Linux users account for less than 2% of global operating systems. However, most s ervers run Linux because it's relatively easy to customize.

Following are some of important functions of an operating System.

- Memory Management
- Processor Management
- Device Management
- File Management
- Security
- Control over system performance
- Job accounting
- Error detecting aids
- Coordination between other software and users

Applications of Operating System

Following are some of the important activities that an Operating System performs −

- **Security** − By means of password and similar other techniques, it prevents unauthorized access to programs and data.
- **Control over system performance** − Recording delays between request for a service and response from the system.

- **Job accounting** − Keeping track of time and resources used by various jobs and users.
- **Error detecting aids** − Production of dumps, traces, error messages, and other debugging and error detecting aids.
- **Coordination between other softwares and users** − Coordination and assignment of compilers, interpreters, assemblers, and other software to the various users of the computer systems.

Types of Operating Systems :

Operating systems are there from the very first computer generation and they keep evolving with time. In this chapter, we will discuss some of the important types of operating systems which are most commonly used.

Batch operating system

The users of a batch operating system do not interact with the computer directly. Each user prepares his job on an off-line device like punch cards and submits it to the computer operator. To speed up processing, jobs with similar needs are batched together and run as a group. The programmers leave their programs with the operator and the operator then sorts the programs with similar requirements into batches.

The problems with Batch Systems are as follows −

- Lack of interaction between the user and the job.
- CPU is often idle, because the speed of the mechanical I/O devices is slower than the CPU.
- Difficult to provide the desired priority.

Time-sharing operating systems

Time-sharing is a technique which enables many people, located at various terminals, to use a particular computer system at the same time. Time-sharing or multitasking is a logical extension of multiprogramming. Processor's time which is shared among multiple users simultaneously is termed as time-sharing.

The main difference between Multiprogrammed Batch Systems and Time-Sharing Systems is that in case of Multiprogrammed batch systems, the objective is to maximize processor use, whereas in Time-Sharing Systems, the objective is to minimize response time.

Multiple jobs are executed by the CPU by switching between them, but the switches occur so frequently. Thus, the user can receive an immediate response. For example, in a transaction processing, the processor executes each user program in a short burst or quantum of computation. That is, if n users are present, then each user can get a time quantum. When the user submits the command, the response time is in few seconds at most.

The operating system uses CPU scheduling and multiprogramming to provide each user with a small portion of a time. Computer systems that were designed primarily as batch systems have been modified to time-sharing systems.

Advantages of Timesharing operating systems are as follows −

- Provides the advantage of quick response.
- Avoids duplication of software.
- Reduces CPU idle time.

Disadvantages of Time-sharing operating systems are as follows −

- Problem of reliability.
- Question of security and integrity of user programs and data.
- Problem of data communication.

Distributed operating System

Distributed systems use multiple central processors to serve multiple real-time applications and multiple users. Data processing jobs are distributed among the processors accordingly.

The processors communicate with one another through various communication lines (such as high-speed buses or telephone lines). These are referred as loosely coupled systems or distributed systems. Processors in a distributed system may vary in size and function. These processors are referred as sites, nodes, computers, and so on.

The advantages of distributed systems are as follows −

- With resource sharing facility, a user at one site may be able to use the resources available at another.
- Speedup the exchange of data with one another via electronic mail.
- If one site fails in a distributed system, the remaining sites can potentially continue operating.
- Better service to the customers.
- Reduction of the load on the host computer.
- Reduction of delays in data processing.

Network operating System

A Network Operating System runs on a server and provides the server the capability to manage data, users, groups, security, applications, and other networking functions. The primary purpose of the network operating system is to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks.

Examples of network operating systems include Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX, Linux, Mac OS X, Novell NetWare, and BSD.

The advantages of network operating systems are as follows −

- Centralized servers are highly stable.
- Security is server managed.
- Upgrades to new technologies and hardware can be easily integrated into the system.
- Remote access to servers is possible from different locations and types of systems.

The disadvantages of network operating systems are as follows −

- High cost of buying and running a server.
- Dependency on a central location for most operations.
- Regular maintenance and updates are required.

Real Time operating System

A real-time system is defined as a data processing system in which the time interval required to process and respond to inputs is so small that it controls the environment. The time taken by the system to respond to an input and display of required updated information is termed as the response time. So in this method, the response time is very less as compared to online processing.

Real-time systems are used when there are rigid time requirements on the operation of a processor or the flow of data and real-time systems can be used as a control device in a dedicated application. A real-time operating system must have well-defined, fixed time constraints, otherwise the system will fail. For example, Scientific experiments, medical imaging systems, industrial control systems, weapon systems, robots, air traffic control systems, etc.

There are two types of real-time operating systems.

Hard real-time systems

Hard real-time systems guarantee that critical tasks complete on time. In hard real-time systems, secondary storage is limited or missing and the data is stored in ROM. In these systems, virtual memory is almost never found.

Soft real-time systems

Soft real-time systems are less restrictive. A critical real-time task gets priority over other tasks and retains the priority until it completes. Soft real-time systems have limited utility than hard real-time systems. For example, multimedia, virtual reality, Advanced Scientific Projects like undersea exploration and planetary rovers, etc.

TOPIC 3 : Networking

What is a network?

A network is a collection of network-enabled devices, typically made up of computers, switches, routers, printers, and servers. Networks are a fundamental part of day-to-day life and exist in homes, workplaces, and public areas. Networks allow all types of network-enabled devices to communicate.

Network types

Networks vary in size, shape, and usage. To make it easier to identify different network types, they're categorized into one of the following network categories:

- Personal area networks

- Local area networks
- Metropolitan area networks
- Wide area networks

What is a personal area network?

A personal area network (PAN) provides networking needs around an individual. An example of a PAN is where a smartphone, smartwatch, tablet, and laptop all connect and share data without the need to connect to an access point or other third-party network services. PAN networks typically use Bluetooth to communicate because it provides a low-power, short-range data-sharing capability. The network standards associated with a PAN are Bluetooth and IEEE 802.15.

What is a local area network?

A local area network (LAN) provides networking needs around a single location. This location might be an organization's office, a school, a university, a hospital, an airport, and many others. A LAN is usually privately owned and needs authentication and authorization to access. Of the different classifications of a network, a LAN is by far the most commonly used.

What is a metropolitan area network?

A metropolitan area network (MAN) provides networking capabilities between two different locations within a city or metropolitan area to provide a single extensive network. Typically, a MAN requires a dedicated and secure connection between each LAN joined to the MAN.

What is a wide area network?

A wide area network (WAN) provides networking capabilities between two different geographical locations locally or worldwide. For example, a WAN is used to connect an organization's head office with branch offices all over the country. A WAN links multiple LANs together to create one super network. As a WAN, you use a virtual private network (VPN) to manage the connection between different LANs.

Differences between LAN and WAN networks

Several aspects set a LAN apart from a WAN. Knowing what these items are makes it easier to plan the services to deploy across these networks.

DIFFERENCES BETWEEN LAN AND WAN NETWORKS	
LAN	**WAN**
A LAN is a privately operated network typically contained in a single building.	A WAN is used to connect geographically separate offices to each other. Multiple organizations might operate WANs.
A LAN operates at speeds of 10 Gbps or higher.	A WAN typically operates at speeds of less than 1 Gbps.
A LAN is less congested compared to other network types.	A WAN is more congested compared to other network types.
A LAN can be managed and administrated in-house.	A WAN typically requires the use of a third party to configure and set up, which increases cost.

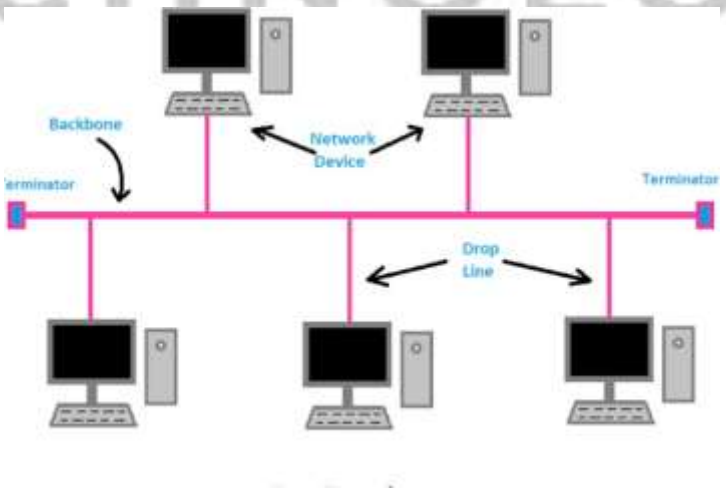
Network topologies

A network topology describes the physical composition of a network. Let's look at four topologies you can choose from when you design a LAN. They are:

- Bus
- Ring
- Mesh
- Star

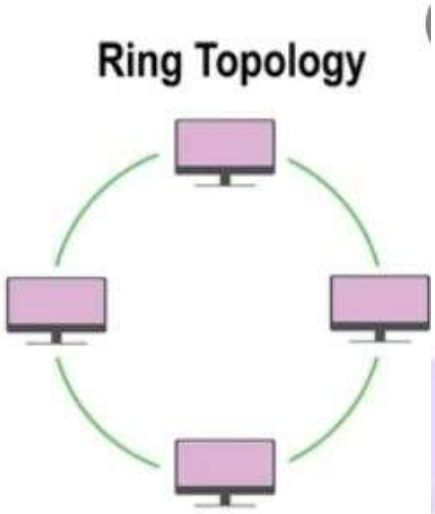
Bus topology

In a bus topology, each network device is connected to a single network cable. Even though it's the simplest type of network to implement, there are limitations to it. The first limitation is the length of the main cable or bus. The longer it gets, the higher the chance of signal dropout. This limitation constrains the physical layout of the network. All devices have to be physically located near each other, for example, in the same room. Finally, if there's a break in the bus cable, the whole network fails.



Ring topology

In a ring topology, each network device is connected to its neighbor to form a ring. This form of network is more resilient than the bus topology. A break in the cable ring also affects the performance of the network.

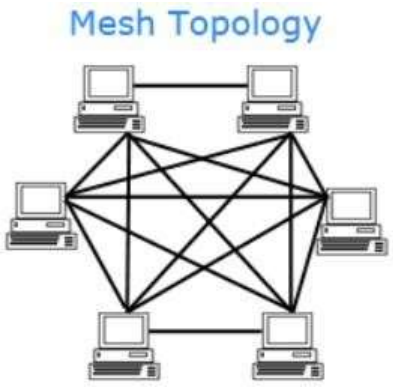


Mesh topology

The mesh topology is described as either a physical mesh or a logical mesh.

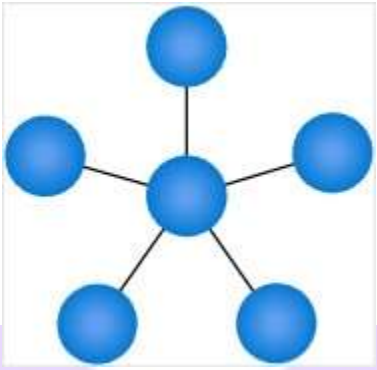
In a physical mesh, each network device connects to every other network device in the network. It dramatically increases the resilience of a network but has the physical overhead of connecting all devices. Few networks today are built as a full mesh. Most networks use a partial mesh, where some machines interconnect, but others connect through one device.

There's a subtle difference between a physical mesh network and a logical one. The perception is that most modern networks are mesh based, since each device can see and communicate with any other device on the network. This description is of a logical mesh network and is primarily made possible through the use of network protocols.



Star topology

The star topology is the most used network topology. Each network device connects to a centralized hub or switch. Switches and hubs can be linked together to extend and build more extensive networks. This type of typology is, by far, the most robust and scalable.



Ethernet

Ethernet is a networking standard that's synonymous with wire-based LAN networks and also used in MAN and WAN networks. Ethernet has replaced other wired LAN technologies like ARCNET and Token Ring and is an industry standard.

While Ethernet is associated with wired networks, keep in mind that it's not limited to wire, since it's used over fiber-optic links as well.

The Ethernet standard defines a framework for data transmission, error handling, and performance thresholds. It describes the rules for configuring an Ethernet network and how each element in the network interacts with each other.

Ethernet is used in the OSI model at the data link and physical layers. It formed the basis for the IEEE 802.3 Standard. This standard helped to unify network and hardware development.

Ethernet is a continually evolving standard, and the original version supported a data transmission rate of only 2.94 Mbps. In recent years, several iterations were released to keep up with the demands for increased speed. Today, rates extend up to 400 Gbps.

Fast Ethernet

Fast Ethernet (IEEE 802.3u) was developed to support data transmission speeds of up to 100 Mbps. Faster Ethernet is also referred to as the 100BASE-TX standard.

Gigabit Ethernet

Gigabit Ethernet (IEEE 802.3ab) was developed to support faster communication networks that can support services like streaming multimedia and Voice over IP (VoIP). The 1000BASE-T standard runs 10 times faster than the 100BASE-TX standard. Gigabit Ethernet is now included in the 802.3 standards and recommended for enterprise networks. The new standard is backward compatible with the 100BASE-T and the older 10BASE-T standards.

10 Gigabit Ethernet

The 10 Gigabit Ethernet (IEEE 802.3ae) standard has a nominal data transfer speed of 10 Gbps, which is 10 times faster than its predecessor. This speed improvement is made possible only by using fiber optics. The standard now requires that 10 Gigabit Ethernet networks use area-based routing rather than broadcasting data to all nodes. In that way, network noise and traffic are reduced.

Terabit Ethernet

Terabit Ethernet offers data transfer speeds of 200 Gbps and 400 Gbps. It's expected that Terabit Ethernet will offer speeds of 800 Gbps and 1.6 Tbps in the future.

The 802 family of standards

The 802 specification covers all the physical networking standards for both Ethernet and wireless. The following table shows some of the more widely used standards.

THE802FAMILYOFSTANDARDS		
802	**Overview**	**Basics of physical and logical networking concepts**
802.1	Bridging	LAN/MAN bridging and management of the lower sublayers of OSI Layer 2
802.2	Logical Link	Commonly referred to as the logical link control (LLC) specification
802.3	**Ethernet**	Provides asynchronous networking by using carrier sense, multiple accesses with collision detect (CSMA/CD) over coaxial cable, twisted- pair copper cable, and fiber media
802.5	Token ring	The token-passing standard for shielded copper cables and twisted-pair cable
802.11	Wi-Fi	Wireless local area network (WLAN) media access control (MAC) and physical layer (PHY) specification
802.11a	Wi-Fi	Specifies a PHY that operates in 5 GHz
802.11b	Wi-Fi	Enhances 802.11, adds higher data rate modes
802.11d	Wi-Fi	Enhances 802.11a/b, allows for global roaming
802.11e	Wi-Fi	Enhances 802.11, adds Quality of Service (QoS) features
802.11g	Wi-Fi	Extends WLAN maximum data rate
802.11 h	Wi-Fi	Enhances 802.11a, now resolves interference issues
802.11i	Wi-Fi	Enhances 802.11, adds security for WLAN applications
802.11j	Wi-Fi	Enhances 802.11a for Japanese regulatory extensions
802.11n	Wi-Fi	Higher-speed standards
802.12	Demand Priority	Ethernet data rate increased to 100 Mbps
802.15	Wireless personal area networks	Support for wireless personal area networks (WPANs)
802.15.1	Bluetooth	Short-range (10 m) wireless technology

802.15.3a	UWB	Short-range, high-bandwidth ultra-wideband (UWB) link
802.15.4	ZigBee	Short-range wireless sensor networks
802.16	Wireless metropolitan area networks	Covers mobile and wireless broadband access in wireless metropolitan area networks (WMANs)

Network infrastructure

There are several network standard-compliant devices that make up the structure of your networks. Depending on the network's size, you might use several of these devices to build the backbone of your network. These devices are:

- Repeaters
- Hubs
- Bridges
- Switches
- Routers

Nearly all these devices depend on a media access control or an Internet Protocol (IP) address to deliver data on the network.

Networking terms and concepts

Some of the most used terms in day-to-day networking life are as discussed below:

1. IP address

An IP address or Internet Protocol is a unique number that represents the address where you live on the Internet. Every device that is connected to the network has a string of numbers or IP addresses unlike house addresses.

You won't find two devices connected to a network with an identical IP address. When your computer sends data to another different, the sent data contains a 'header' that further contains the devices' IP address, i.e., the source computer and the destination device.

2. Nodes

A node refers to a networking connection point where a connection occurs inside a network that further helps in receiving, transmitting, creating, or storing files or data.

Multiple devices could be connected to the Internet or network using wired or wireless nodes. To form a network connection, one requires two or more nodes where each node carries its unique identification to obtain access, such as an IP address. Some examples of nodes are computers, printers, modems, switches, etc.

3. Routers

A router is a physical networking device, which forwards data packets between networks. Routers do the data analysis, perform the traffic directing functions on the network, and define the top route for the data packets to reach their destination node. A data packet may have to surpass multiple routers present within the network until it reaches its destination.

4. Switches

In a computer network, a switch is a device that connects other devices and helps in node-to-node communication by deciding the best way of transmitting data within a network (usually if there are multiple routes in a more extensive network).

Though a router also transmits information, it forwards the information only between networks, whereas a switches forwards data between nodes present in a single network.

Switching is further classified into three types, which are as follows:

- Circuit Switching
- Packet Switching
- Message Switching

Circuit Switching: In this switching type, a secure communication path is established between nodes (or the sender and receiver) in a network. It establishes a dedicated connection path before transferring the data, and this path assures a good transmission bandwidth and prevents any other traffic from traveling on that path. For example, the Telephone network.

Packet Switching: With this technique, a message is broken into independent components known as packets. Because of their small size, each packet is sent individually. The packets traveling through the network will have their source and destination IP address.

Message Switching: This switching technique uses the store and forward mechanism. It sends the complete unit of the message from the source node, passing from multiple switches until it reaches its intermediary node. It is not suitable for real-time applications.

5. Ports

A port allows the user to access multiple applications by identifying a connection between network devices. Each port is allocated a set of string numbers. If you relate the IP address to a hotel's address, you can refer to ports as the hotel room number. Network devices use port numbers to decide which application, service, or method is used to forward the detailed information or the data.

6. Network cable types

Network cables are used as a connection medium between different computers and other network devices. Typical examples of network cable types are Ethernet cables, coaxial, and fiber optic. Though the selection of cable type usually depends on the size of the network, the organization of network components, and the distance between the network devices.

TOPIC 4 : Internet

INTERNET – THE HISTORY

In 1969, the U.S. Defence Department funded a project to develop a network, which can withstand the bombing. Basically the idea was to develop a very secure network which can work even after a nuclear attack. This project was known as ARPANET.

The proposed network was not supposed to have a central control – which would be an obvious

target. Ten years of research brought Local Area Ethernet Networks (LANs) and workstations were developed to get connected to LAN. These workstations and LANs were then connected to the ARPANET.

For next decade the ARPANET grew and its decentralized features helped its rapid expansion. Computers connected to ARPANET used to standard or rule to communicate with each other.

This standard used by ARPANET is known as NCP (National Control Protocol). Protocol is a network term used to indicate the standard used by a network for communication. But the passing time and rapid change in information technology suppressed NCP and brought TCP/IP (Transmission Control Protocol/Internet Protocol) in to the world of networking. TCP converts messages into streams of packets at the source, and they are reassembled back into messages at the destination. IP handles the dispatch of these packets. It handles the addressing, and makes sure that a packet reaches its destination through multiple nodes and even across multiple networks with multiple standards.

This flexibility of TCP/IP to handle multiple networks with multiple protocols encourages other networks to get connected to ARPANET. Slowly the ARPANET became a massive network of networks and now it is known as 'Internet'.

SERVICES OF INTERNET –E-mail, FTP, Telnet, WWW

Internet mail is (e-mail or electronic mail), much faster as compared to normal postal mail. One can also send software and certain forms of compressed digital image as an attachment. News groups or discussion groups facilitate Internet user to join for various kinds of debate, discussion and news sharing. Long-distance computing was an original inspiration for development of ARPANET and does still provide a very useful service on Internet. Programmers can maintain accounts on distant, powerful computers, execute programs. File transfer service allows Internet users to access remote machines and retrieve programs, data or text.

- **E-Mail (Electronic Mail) E-mail or Electronic mail** is a paperless method of sending messages, notes or letters from one person to another or even many people at the same time via Internet. E-mail is very fast compared to the normal post. E-mail messages usually take only few seconds to arrive at their destination. One can send messages anytime of the day or night and it will get delivered immediately. You need not to wait for the post office to open and you don't have to get worried about holidays. It works 24 hours a day and seven days a week. What's more, the copy of the message you have sent will be available whenever you want to look at it even in the middle of the night. You have the privilege of sending something extra such as a file, graphics, images etc. along with your e-mail. The biggest advantage of using e-mail is that it is cheap, especially when sending messages to other states or countries and at the same time it can be delivered to a number of people around the world.

  Components of an E-mail Address As in the case of normal mail system, e-mail is also based upon the concept of a recipient address. The email address provides all of the information required to get a message to the recipient from anywhere in the world. Consider the e-mail ID john@hotmail.com In the example above, "john" is the local part, which is the name of a mailbox on the destination computer, where finally the mail will

be delivered. Hotmail is the mail server where the mailbox "john" exist, .com is the type of organization on net, which is hosting the mail server.

There are six main categories:

1. **com** Commercial institutions or organization
2. **edu** Educational institutions
3. **gov** Government site
4. **mil** Military site
5. **net** Gateways and administrative hosts
6. **org** Private organizations

- **FTP (File Transfer Protocol) File Transfer Protocol**, is an Internet utility software used to upload and download files. It gives access to directories or folders on remote computers and allows software, data and text files to be transferred between different kinds of computers. FTP works on the basis of same principle as that of Client/Server. FTP "Client" is a program running on the your computer that enables you to talk to, and get stuff from, remote computers. The FTP client takes FTP commands and send them as requests for information from the remote computer or known as FTP servers. To access remote FTP server it is required but not necessary to have an account in the FTP server. When the FTP client gets connected, FTP server asks for the identification in- terms of User Login name and password of the FTP client. If one does not have an account in the remote FTP server, still he can connect to the server using anonymous login.
  The basic objectives of FTP are to give flexibility and promote sharing of computer programs, files and data to transfer data reliably and more efficiently over network to encourage implicit or indirect use of remote computers using Internet to shield a user from variations in file storage systems among hosts.

- **Telnet (Remote Computing) Telnet or remote computing** is telecommunication utility software, which uses available telecommunication facility and allows you to become a user on a remote computer. Once you gain access to the remote computer, you can use it for the intended purpose. The TELNET works in a very step by step procedure. The commands typed on the client computer are sent to the local Internet Service Provider (ISP), and then from the ISP to the remote computer that you have gained access. Most of the ISP provides facility to TELENET into your own account from another city and check your e-mail while you are traveling or away on business.

- **WORLD WIDE WEB (WWW)** WWW is the acronym for the World Wide Web. It is also commonly known as 'The Web'. The WWW is hypertext based information retrieval tool. One can easily surf the Web by jumping from one document to another using the links in those documents. These documents can be in many formats, such as text, graphics, animation, sound and latest is video. They may also be a combination of all these. All the information on Internet are presented to the user as a document or more popularly known as Web Page. All these Web Pages are link to each other or even to section within a Web Page. And these links are known as Hyper Links.

Internet Address

Just like every house, every office, every location has an address, every page on the Internet has a unique address. This address is used to get the web page for user from Internet. Just as the address of a house or office is known as its postal address, the address on the Internet is known as URL (Uniform Resource Locator). A typical Internet address or URL would look like; https://dxc.com

SEARCHING ON THE WEB One of the most common problems all Internet users face is the fact that it can be quite difficult to find what you want on the Internet. There is no central "main menu" that users can access to navigate through the Internet. Although there might not be an official menu, there are several resources available – both on-line and off-line that can make "surfing the net" easier. The Internet is a terrific resource. It contains hundreds of web sites dedicated to thousands of topics. There are some web sites, which are used to search information on the web. There are more than 2,500 search services presently on the Web.

Search services on the Internet come in two main flavors:

1) 'search engine' that index words or terms in Internet documents

2) 'directories' that classify Web documents or locations into an arbitrary subject classification scheme or taxonomy.

Topic 5 : Computers & Cyber Security

What is cybersecurity?

Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

The term cybersecurity refers to techniques and practices designed to protect digital data. The data that is stored, transmitted or used on an information system. After all, that is what criminal wants, data. The network, servers, computers are just mechanisms to get to the data. Effective cybersecurity reduces the risk of cyber-attacks and protects organizations and individuals from the unauthorized exploitation of systems, networks, and technologies.

Robust cybersecurity implementation is roughly based around three key terms: people, processes, and technology. This three-pronged approach helps organizations defend themselves from both highly organized attacks and common internal threats, such as accidental breaches and human error.

The attacks evolve every day as attackers become more inventive, it is critical to properly define cybersecurity and understand cybersecurity fundamentals.

The history of Cybersecurity

About forty years ago words like worms, viruses, trojan-horse, spyware, malware weren't even a part of conventional information technology (IT) vocabulary. Cybersecurity only came into existence because of the development of viruses. But how did we get here?

The history of cybersecurity began as a research project. In the 1970's, Robert Thomas, a researcher for BBN Technologies in Cambridge, Massachusetts, created the first computer "worm". It was called The Creeper. The Creeper, infected computers by hopping from system to system with the message "I'M THE CREEPER: CATCH ME IF YOU CAN." Ray Tomlinson, the inventor of email, created a replicating program called The Reaper, the first antivirus software, which would chase Creeper and delete it.

Late in 1988, a man named Robert Morris had an idea: he wanted to test the size of the internet. To do this, he wrote a program that went through networks, invaded Unix terminals, and copied itself. The Morris worm was so aggressive that it slowed down computers to the point of being unusable. He subsequently became the first person to be convicted under Computer Fraud and Abuse Act.

From that point forward, viruses became deadlier, more invasive, and harder to control. With it came the advent of cybersecurity.

Why is cybersecurity important?

Listed below are the reasons why cybersecurity is so important in what's become a predominant digital world:

- With each passing year, the sheer volume of threats is increasing rapidly. According to the report by McAfee, cybercrime now stands at over $400 billion, while it was $250 billion two years ago.
- Cyber attacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

The eight most basic elements of a strong cybersecurity posture are:

- Asset Management & Identification.
- Risk Management.
- Access Management.
- Threat Management.
- Security Controls.
- Disaster Recovery & Business Continuity.
- Incident Management.
- Security Education, Training, and Awareness.

What Are the Different Types of Cyber Security?

- Cloud Security. Cloud-based data storage has become a popular option over the last decade due to its enhanced privacy. ...
- Network Security. Guard your internal network against outside threats with increased network security. ...

- Application Security.

Identifying Types of Threats

Various sources have divided threats into different categories based on specific criteria. In this section we will examine threats that have been divided into categories based on the nature of the attack. Most attacks can be categorized as one of seven broad classes:

■ Malware: This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system. One reason the relatively generic term malware is now widely used is that many times a piece of malware does not fit neatly into one of these categories.

■ Security breaches: This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server…all the things you probably associate with the term hacking.

■ DoS attacks: These are designed to prevent legitimate access to your system. And, as you will see in later chapters, this includes distributed denial of service (DDoS).

■ Web attacks: This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.

■ Session hijacking: These attacks are rather advanced and involve an attacker attempting to take over a session.

How to improve cyber security?

Keeping software and systems updated with the latest patches limits their vulnerability to cyber-attacks. Using the security features that come with your apps supplements other security measures you have in place.

1. Enforce password rules

Strong passwords are one of the first lines of defense against breaches and changing them occasionally may help keep hackers out. But most staff will not voluntarily update their passwords, even when prompted. Make regular password updates mandatory and teach users how to create and remember strong passwords.

2. Update regularly

Any connection to the Internet is vulnerable, and it's a key feature hackers try to exploit. Keep every connection, operating system, and application up to date with patches and enhancements. Implementing software and system security updates quickly limits possible exposure to vulnerabilities.

3. Implement VPNs for all connections

Networks that are protected only by generic security measures are more vulnerable to attack. Implement virtual private network (VPN) connections between office locations and make their use easy—and mandatory—for mobile employees who may connect through public Wi-

Fi services.

4. Retire all unused services

When limited-duration products expire, decommission the applications, logins, and user credentials associated with them. In cases when you don't use every available feature of a UC deployment, such as a video chat function, turn it off to further limit unauthorized access to the enterprise.

5. Leverage existing security options

Some applications come bundled with their own security features. While it's still important to implement additional safeguards, vendors know their own products and typically devote significant resources to deliver a safe environment for customers. Find out what security measures are included with your software and use them to the fullest extent in conjunction with other security you have in place.