Networking

Networking means an interconnection of multiple devices known as hosts, that are connected using multiple paths. The devices that can connect to a network are known as **nodes**. For example, Clients, Servers, Hubs, Switches, etc.

A **Network** is a collection of computing devices that are connected in various ways to communicate and share resources. Usually, the connections between computers in a network are made using physical wires or cables.

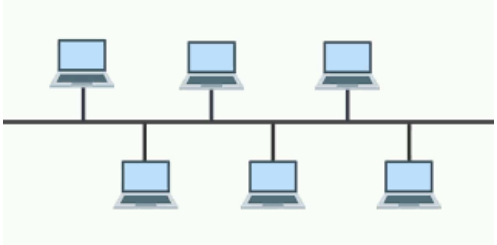
Client: An end-user like you, me, phone, laptops, etc.
Server: It is a piece of computer hardware or software (computer program) that provides functionality for other programs or devices, called **clients**.

Types Of Networks

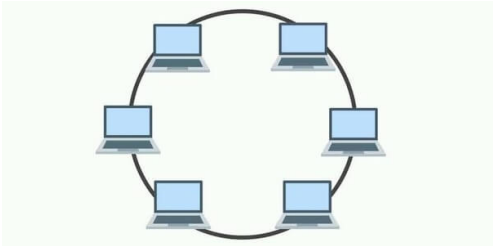
1. **Personal Area Network (PAN)**: A personal area network, or PAN, is a computer network that enables the communication between computer devices near a person. For example, Bluetooth cellphone to Car.
2. **Local Area Network (LAN)**: A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus, or office building.
3. **Campus Area Network (CAN)**: It is a LAN that spans across many buildings. It can cover up to square miles. For example, College Campus, Military Bases, etc.
4. **Metropolitan Area Network (MAN)**: A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities, and towns, or any given large area with multiple buildings.
5. **Wide Area Network (WAN)**: A wide area network (WAN) is a large computer network that connects groups of computers over large distances. For example, you can connect with Google's data centers from your home (local area) network.

Network Topologies

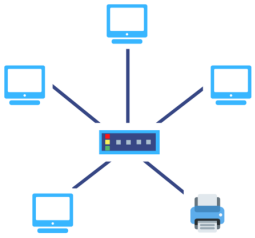
1. **Bus Topology**: It is a network type in which every device is connected to a single cable. Devices on that cable form a single **collision domain**.



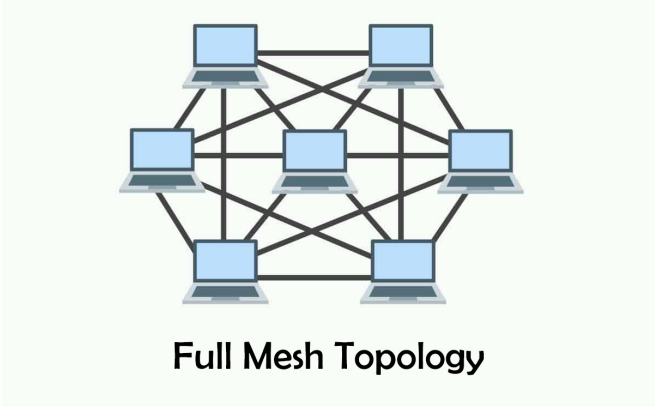
2. **Ring Topology**: It uses a cable running in a circular loop that connects to each device in the network.



3. **Star Topology**: In this network, all the devices are connected to a single hub through a cable.



4. **Mesh Topology**: A mesh topology is a network setup where each computer and network device is interconnected with one another. This topology setup allows for most transmissions to be distributed even if one of the connections goes down.

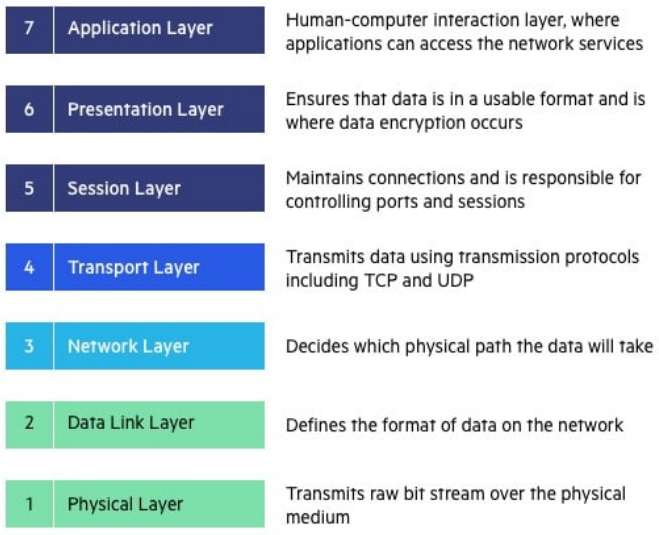


Internet Of Things

1. **802.11**: It is the communication standard for wireless devices. It operates on **Infrastructure Mode** or **Ad-hoc Mode**.
2. **Bluetooth**: It is a short-range wireless communication technology that uses radio waves to transmit information. It is a high-speed and low-power communication technology.
3. **Radio Frequency Identification (RFID)**: It uses **Electromagnetic Fields** to read data stored in embedded tags.
4. **Near Field Communication (NFC):** It enables Electronic Devices to communicate within a range of 4 Cm. For example, when you put your card on a machine.
5. **Infrared (IR)**: It is a wave that is used to transmit data over very short distances like, 4 to 5 m. For example, TV remote.
6. **Z-Wave**: This wave is based on low-powered **Radio Frequency** technology. It is mainly used for home automation.

OSI (Open Systems Interconnection) Model

The OSI Model is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements to support interoperability between different products and software.



💡 **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

1. **Physical Layer**: It is the bottom-most layer of the OSI model. It sends data in the form of bits (1s and 0s) from one device to another. It defines the relationship between a device and a transmission medium, such as a copper or optical cable.
2. **Data Link Layer**: Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. It packages data into **Frames** and transmits those frames on the network, performing error correction.
3. **Network Layer**: This layer is used for the transmission of data from one host to another located in different networks. In this layer, the data is divided into packets and then forwarded.

💡 It also prevents the sender from sending data faster than the receiver can receive.

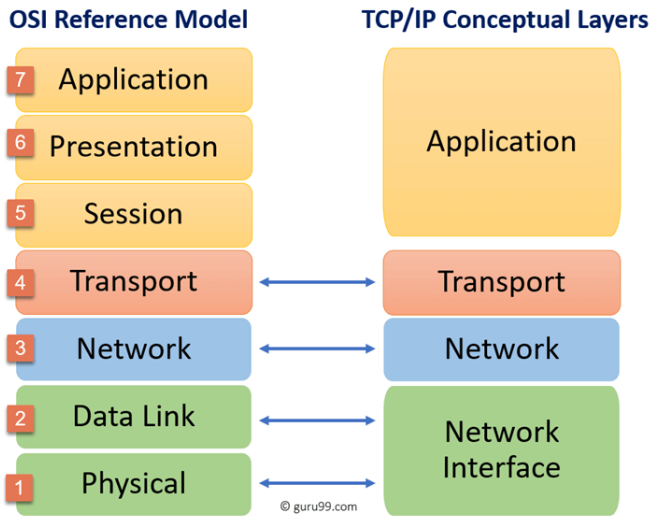
4. **Transport Layer**: Transport Layer provides transparent transfer of data between end-users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through **flow control**, **segmentation** and **desegmentation**, and **error control**.
5. **Session Layer**: This layer is responsible for the establishment of connection, maintenance, and authentication of a network connection between two devices.

💡 **H.323** standard is used to set up, maintain, and tear down a voice/video connection in the Session Layer.

6. **Presentation Layer**: It is the 6th layer in the OSI model. This layer is also known as the Translation layer, as this layer serves as a data translator for the network. The data which this layer receives from the Application Layer is extracted and manipulated here as per the required format to transmit over the network. The main responsibility of this layer is to provide or define the data format and encryption. For example, **ASCII** to **EBCDIC**.
7. **Application Layer**: The application layer interface directly interacts with the application and provides common web application services. Manipulation of data (information) in various ways is done in this layer which enables users or software to get access to the network. For example, protocols like, IMAP, SMTP, HTTPS, etc.

TCP/IP Model

This protocol stands for **Transmission Control Protocol/Internet Protocol**. The TCP/IP model is a concise version of the OSI model. It contains four layers, The Application layer, Transport Layer, Internet Layer, and Network interface Layer.



1. **Network Interface Layer**: This layer corresponds to the combination of the Data Link Layer and the Physical Layer of the OSI model.
   It does the hardware addressing and protocols. This layer allows for the physical transmission of data.
2. **Internet Layer**: The Internet layer is responsible for the logical transmission of data packets over the internet. It transmits data packets to the link layer. It routes each of the data packets independently from the source to the destination, using the optimal route.
3. **Transport Layer**: The transport layer is responsible for the error-free, end-to-end delivery of data from the source host to the destination host. It also provides an interface for the users to the underlying network.
4. **Application Layer**: This layer performs the functions of the top three layers of the OSI model: Application, Presentation, and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, etc.

Network Devices

Medium Access Control (MAC) Address

It is a 48-bit hardware number that is embedded into a **Network Interface Controller** at the time of manufacturing. It is written in hexadecimal numbers. For example, **3A:34:65:D2:51:F1**.

The first 24-bits (or 6 numbers) represent the vendor code and the last 24-bits represent the device code.

1. **Hub**: Hubs connect computers in a star topology network. Due to their design, they increase the chances of collisions. Hubs operate in the physical layer of the OSI model and have no intelligence. They flood incoming packets to all the ports.

   Types Of Hubs

   i. **Active Hubs**: These Hubs can clean, boost, and relay the signal along with the network. These are used to extend the maximum distance between nodes.

   ii. **Passive Hubs**: These Hubs relay signals into the network without cleaning and boosting them. They cannot be used to extend the distance between nodes.

   iii. **Smart Hubs**: It works as an active Hub but enables the administrator to monitor the traffic passing through the hub.

2. **Bridge**: Bridges can be identified by the fact that they operate at the data link layer of the OSI model. Bridges have intelligence and can "bridge" two of their ports together at very high speed. They use a database of MAC addresses to determine where computers are located and very efficiently send frames only where they need to go. The database is created dynamically as computers communicate on the network.

3. **Switch**: Switches provide a central connection between two or more computers on a network, but with some intelligence. They provide traffic control for packets; rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected. They also use a database of MAC addresses to determine where computers are located and very efficiently send packets only where they need to go.

4. **Router**: Routers operate at the network layer of the OSI model and efficiently route information between Local Area Networks. They are like a switch, but routes data packets based on the IP addresses.
   Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets.

5. **Repeater**: A repeater is an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of obstruction so that the signal can cover longer distances without degradation.

6. **Modem**: Modem (**modulator-demodulator**) is a device that turns the digital 1s and 0s of a personal computer into sounds that can be transmitted over the telephone lines and once received on the other side, converts those sounds back into a form used by a USB, Ethernet, serial, or network connection. Modems are generally classified by the amount of data they can send in a given time, normally measured in **bits per second**, or "**bps**".

7. **Network Interface Controller (NIC)**: A network interface controller is a computer hardware component that connects a computer to a computer network. It provides physical access to a

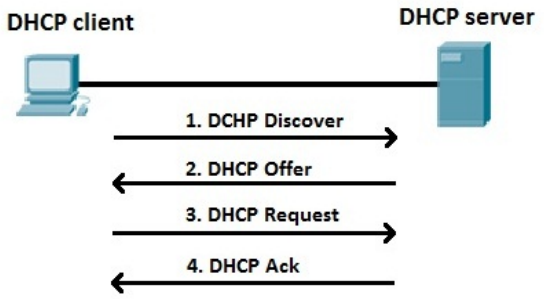
networking medium and provides a low-level addressing system through the use of MAC addresses.

8. **Gateway**: A gateway is a piece of networking hardware or software used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
9. **Wireless Access Point (WAP)**: A wireless access point, or more generally just an access point, is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.

Special Network Devices

1. **VPN Concentrators**: VPN stands for **Virtual Private Network**. It creates a virtual network tunnel that is connected to some other network.
   A VPN concentrator is a type of networking device that provides the secure creation of VPN connections and the delivery of messages between VPN nodes.
2. **Firewall**: It is a network security device that monitors the incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
3. **Next-generation firewall (NGFW)**: It is the new version of the standard Firewall that can conduct packet inspection up to the **Application layer**. It continuously connects to cloud resources for the latest information on threats.
4. **Intrusion Detection or Prevention System (IDS/IPS)**: An IDS is a system that monitors network traffic for suspicious activity and issues alert when such activity is discovered, It is a software application that scans a network or a system for harmful or policy breaching activities. Any malicious data is normally reported either to an administrator or collected centrally.
5. **Proxy Server**: A proxy server is a computer system or router that functions as a relay between client and server. Likewise, responses come back to the proxy server and then to the user. Proxy Servers Provide Anonymity. Like a virtual private network (VPN), a proxy server hides the user's IP address when accessing the Internet. It does several kinds of filters such as:
   a. Content Filtering
   b. Examine Packet Headers
   c. Logging

   It fastens the service by the process of retrieving content from the cache which was saved when a previous request was made by the client.
6. **DHCP Server**: A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices.



1. **Load Balancer**: Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a **server farm** or **server pool**. Load Balancers are used to do load balancing.

Transmission Media

Copper Media

UTP Categories - Copper Cable				
UTP Category	**Data Rate**	**Max. Length**	**Cable Type**	**Application**
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

It is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It is primarily used by cable TV companies to connect their satellites antenna facilities to customer homes and businesses.

1. **Coaxial Cable (Coax)**: This wire has an insulated conductor or wire at the center which passes the data. It has a **braided metal shield** used to help shield and protect data transmission and EMI resistance.
   RG-6 - is commonly used by cable components to connect individual homes.
   RG-56 is used to carry composite video between two nearby devices. For example, TV to the cable box.

2. **Twisted Pair Cable**: It is the most popular physical LAN media type. It consists of eight individual insulated strands of copper wire inside a cable that are twisted in a pair of two strands.
    a. **Unshielded Twisted Pair Cable (UTP)**: In this wire, the twisted pairs are covered inside a plastic tube. It is cheaper and the media of choice in most LANs.
    b. **Shielded Twisted Pair Cable (STP)**: In this wire, the twisted pairs are covered by metallic shielding. Also, there is outer shielding which minimizes EMI. It is expensive as compared to UTP.

    Types of Connectors

    i. **RJ-45**: It is only used in Ethernet networks. It has 8 pins but uses only 4 pins
    ii. **RJ-11**: It is a 6 pin connector but uses only 2 or 4 pins. It is commonly found in telephone systems.
    iii. **DB-9 or DB-25**: It is a 9 pin or 25 pins D-subminiature for connecting to an external modem.
3. **Crossover Cables**: These cables are used to connect two devices of the same type. For example, Server to Server or Switch to Switch.

> 💡 There is no need to use crossover cables if the switch supports **Medium Dependent Interface Crossover** (MDIX).

4. **Plenum Cables**: It is a special UTP/STP cable that has a fire retardant outer insulator. Minimize dangerous fumes if the cable is on fire. Safe to use in ceilings, walls, and raised floors.

Fiber Optic Cables

These cables use light from an LED or laser to transmit information through glass fiber. It can cover up to thousands of miles.

1. **Multimode Fiber (MMF)**: It is a type of optical fiber designed to carry multiple light rays or modes simultaneously, each at a marginally different reflection angle inside the optical fiber core. It is used to cover shorter distances.
2. **Single-mode Fiber (SMF)**: Single-mode fiber is a common type of optical fiber that is used to transmit over longer distances. Single-mode fiber is a single glass fiber strand used to transmit a single-mode or ray of light.

Types of Connectors

a. **SC**: Subscriber Connector
b. **ST**: Straight Tip Connector
c. **LC**: Lucent Connector
d. **MTRJ**: Mechanical Transfer Registered Jack

e. **Media Converters**: These devices convert media from one form to another. For example, Coaxial to Fiber or Fiber to Ethernet.

f. **Transceivers**: It is a device that is capable of both transmit and receive information through transmission media. It is a combination of Transmitter or Receiver. For example, Phone.

Ethernet Fundamentals

Ethernet is the traditional technology for connecting devices in a wired local area network (LAN) or wide area network (WAN), enabling them to communicate with each other via a protocol.

Collision Domain

It is a group of devices that are connected in a single domain. For example, 4 devices connected with the same hub form a single collision domain.
Whenever a device sends out a message to the network, all other devices are included in the domain have to listen to the transmission, no matter if it was destined for them or not.

Carrier Sense Multiple Access/Collision Domain (CSMA/CD)

It is a network protocol for carrier transmission that operates in the MAC layer. It listens whether the shared channel for transmission is busy or not.
The Collision Detection technology detects collision by sensing transmission from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

Link Aggregation (802.3ad)

It is a way of bundling a bunch of individual ports together so they can act as a single logical link. If you have a switch with a whole lot of Gigabit Ethernet ports, you can connect a fraction of ports to another device that has also a bunch of ports and balance the traffic among these links to improve speed performance.

Power Over Ethernet (POE 802.3af/POE+ 802.3at)

Power over Ethernet (PoE) is a technique for delivering DC power to devices over copper Ethernet cabling, eliminating the need for separate power supplies and outlets. It requires a CAT5 or higher cable.
A POE can support up to 15.4 watts of power, while POE+ can support up to 25.5 watts of power. It uses an RJ-45 cable.

Port Mirroring

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port to a network monitoring connection on another switch port.

First Hop Redundancy

The main function of the First Hop Redundancy mechanism is to select a key device as active and send the traffic through it. Besides, provides one more available backup device and turns the traffic flow through it during a failure. A virtual IP address is used and shared in these mechanisms.

Spanning Tree Protocol (802.1D)

The STP prevents the looping of frames around LANs by placing ports of switch in either forwarding state or blocking state. Interfaces that are in forwarding state act as normal but interfaces that are in blocking state don't process any frame received except STP messages.

Broadcast Storm: A broadcast storm is an abnormally high number of broadcast packets within a short period. A broadcast storm can overwhelm switches and endpoints as they struggle to keep up with processing the flood of packets.

Prevention of Broadcast Storm: A switch is elected as a root switch to act as a reference point for a Spanning Tree Protocol.

All switches in the network declare themselves as root bridges and start exchanging each other's **BPDU**s (Bridge Protocol Data Units). The BPDU with the lowest bridge I'd is declared as the root bridge.

Root Port: It is the closes port to the root bridge.

Designated Port: It is the port that has been determined as having the lowest cost. A designated port will be a forwarding port.

Non-designated Port: It is a port that blocks traffic to create a loop-free topology.

Virtual Local Area Network (VLAN)

A VLAN is a custom network that is created from one or more LANs. It enables a group of devices in multiple networks to be connected into one logical network. It can group client devices that communicate frequently with each other.

VLAN Trunking Protocol (802.1q): It is a CISCO Proprietary Protocol that is used to exchange VLAN information.

Important Protocols

Network Protocols

IP Addressing

The Internet Protocol is the method or protocol by which data is sent from one computer to another on the internet. Each computer on the Internet has at least one IP address that uniquely identifies it from

all other computers on the Internet. Two versions of IP are currently in use: IPv4 and IPv6.

Subnet Mask

A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs. It is created by setting host bits to all 0s and setting network bits to all 1s.

Classes of IP Address

Name	First Octet	Mask	Prefix Notion
A	1 - 126	255.0.0.0	8
B	128 - 191	255.255.0.0	16
C	192 - 223	255.255.255.0	24

> 💡 127 is skipped between class A and class B. It is a reserved block for the **Loopback Address** (127.0.0.0 to 127.255.255.255).

Routable IP Address

it is the IP address that can be routed, i.e., available to the public or also known as a **Public IP Address**.

The non-routable IP addresses are known as **Private IPs**. These are not routable outside of a local area network.

> 💡 **Network Address Translation (NAT)** allows the routing of private IPs through a public IP.

Private IP Classes

Name	Address Range	Default Subnet Mask
A	10.0.0.0 - 10.255.255.255	255.0.0.0
B	172.16.0.0 - 172.31.255.255	255.255.0.0
C	192.168.0.0 - 192.168.255.255	255.255.255.0

Loopback Address

IP addresses range from 127.0.0.0 to 127.255.255.255 are reserved for loopback IP addresses. It is entirely managed within the **OS (Operating System)**. These addresses enable a server and a client on a single system to communicate with each other.

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask, default gateway, router address, and DNS server address.

> 💡 Each IP is leased for a given amount of time and given back to the pool when the lease expires.

Automatic Private IP Address (APIPA)

APIPA is used when a device does not have a static IP address or cannot reach a DHCP server. In this case, it allows a network device to self-assign an IP address from the pool of **169.254.0.0** network.

Network Address Translation (NAT)

NAT is the process in which one or more local IP addresses are translated into a single global IP address. It allows a single device, such as a router to act as an agent between the internet and a local is a network. A single IP address is required to represent an entire group of computers to the outside network.

Multicast Routing

It is used to distribute data (for example, audio/video) to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

Internet Protocol Version 4 (IPv4)

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks.

It is a 32-bit number that uniquely identifies a network interface on a machine. Each IPv4 address is divided into four separate numbers and divided by dots. For example, 10.1.2.3 or 192.168.1.4.

Types of IPv4 Addresses

1. **Unicast Address**: A unicast address is an address that identifies a unique node on a network. it typically refers to a single sender or a single receiver.
2. **Multicast Address**: A multicast address is a logical identifier for a group of hosts in a computer network that are available to process datagrams or frames intended to be multicast for a designated network service.
3. **Broadcast Address**: A broadcast address is an IP address that is used to target all systems on a specific subnet network instead of single hosts. The broadcast address allows information to be

sent to all machines on a given subnet rather than to a specific machine.

Internet Protocol Version 6 (IPv6)

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

It is a 128-bit number written in hexadecimal. Each hexadecimal number is of 4 bits. For example, ABCD:EF01:2345:6789:ABCD:B201:5482:D023.

Types of IPv6 Addresses

1. **Unicast Address**: It is the same as the Unicast address in the IPv4 address. A packet sent to a unicast address is received by the interface that is assigned to that address.
2. **Multicast Address**: An IPv6 multicast address defines a group of devices known as a multicast group. IPv6 multicast addresses use the prefix **ff00::/8**. It is also used to send data to multiple hosts.
3. **Anycast Address**: This IPv6 address is allocated to a set of interfaces that typically belong to different routers. When a packet is destined to an anycast address, it is delivered to the closest interface that has this anycast address.

Routing

Routing means forwarding the data packets to a specific route. A router is a networking device that forwards data packets between computer networks.

Routing Table: A routing table, or routing information base, is a data table stored in a router or a network host that lists the routes to particular network destinations.

Split Horizon: It is the method of preventing a routing loop in a network. Information about the routing for a particular packet is never sent back in the direction where it can come from.

Distance Vector Routing

This protocol requires that a router inform its neighbors of the topology changes periodically. Each router maintains a Distance Vector table containing the distance between itself and all possible destination nodes.
Each router transmits its distance vector to each of its neighbors. Each router receives and saves the most recently received distance vector from each of its neighbors. Routers recalculate their distance and update their routing tables.

Link State Routing

It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network. A router sends the information about its neighbors only to all the routers through **flooding**.

Routing Protocols

1. **Routing Information Protocol (RIP)**: It is a dynamic routing protocol that uses **hop count** as a routing metric to find the best path between the source and the destination network.
2. **Open Shortest Path First (OSPF)**: It is a link-state routing protocol that is used to find the best path between the source and the destination router.

Wireless Networks (802.11)

Computer networks that are not connected by cables are called **wireless networks**. They generally use radio waves for communication between the network nodes.

Wireless Networks operates on two network modes

1. **Infrastructure Mode**: It uses a **wireless access point (WAP)** as a centralized point like a star topology. It is the most common type of wireless network.
2. **Ad-Hoc Mode**: It is a decentralized wireless network. Forwarding decisions for data on the network are made dynamically by the clients.

Gateway: A gateway is a device that provides communication to a remote network that is out of bounds for the host network nodes.

Basic Service Set (BSS) and Extended Service Set (ESS)

BSS is a network topology that allows all wireless devices to communicate with each other through a common medium, i.e., **WAP**.
ESS allows using the same wireless configuration across several WAPs which are connected to a central Hub or Router.

Wireless Range Extender

It takes an existing wireless signal from a router or wireless access point and rebroadcasts it to extend the network coverage.

Wireless Antennas

It is a transducer, which converts electrical power into electromagnetic waves.

1. **Omnidirectional Antenna**: This Antenna radiates an equal amount of frequency in every direction. Modern WAPs use this antenna.
2. **Unidirectional Antenna**: This Antenna focuses all the power in one direction for covering greater distances. The most common unidirectional antenna is the "**Yagi**" antenna.

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

CSMA/CA is a network protocol for carrier transmission that operates in the MAC layer. In contrast to CSMA/CD that deals with collisions after their occurrence, CSMA/CA prevents collisions before their occurrence.

Virtualization and Cloud Computing

Virtualization is the creation of a virtual service or operating system on top of physical hardware or a host system.

Virtualization

Virtual Server: It mimics the functionality of a physical dedicated server. Multiple virtual servers may be implemented on a single bare metal server, each with its OS.

Hypervisor

It is a hardware virtualization technique that allows multiple guest operating systems to run on a single operating system at the same time.

Types of Hypervisors

1. **Type-1 Hypervisor**: It runs directly on the underlying host system. It is also known as "**Bare Metal Hypervisor**". It does not require any base server Operating system. It has direct access to hardware resources.
2. **Type-2 Hypervisor**: A guest operating system runs on the underlying host operating system. It is also known as a "**Hosted Hypervisor**".

Network Attached Storage (NAS)

NAS is a storage device connected to a network that allows for the storage and retrieval of data from a central location.

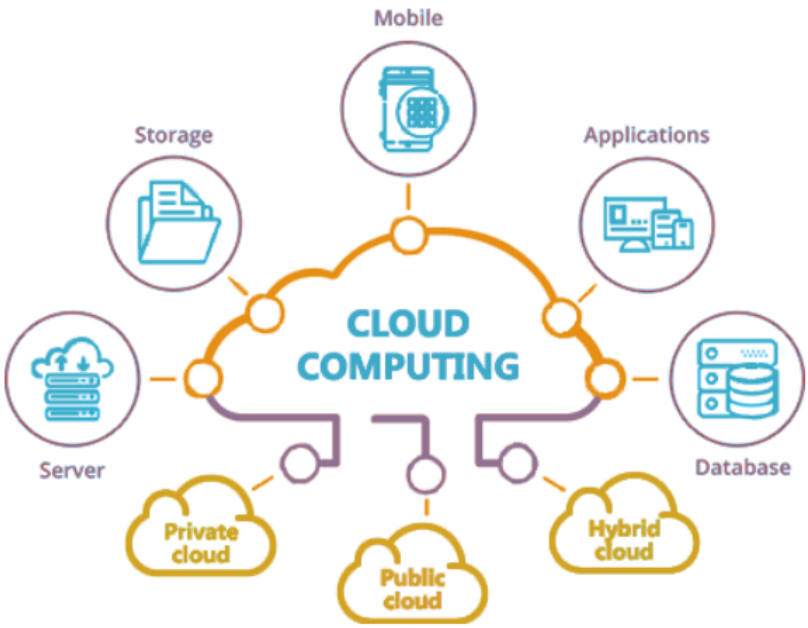
Storage Area Network (SAN)

A SAN is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, and other storage elements that are interconnected using a variety of technologies and protocols.

Voice Over IP (VOIP)

VOIP is a technology that allows you to make voice calls over an internet connection instead of an analog phone line.

Cloud Computing



It is the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

1. **Private Cloud**: In this service, all the software and hardware resources are dedicated exclusively to, and accessible only by a single customer.
2. **Public Cloud**: It is a type of cloud computing in which a service provider makes resources available to the public via the internet. Resources may vary by the provider but may include storage capabilities, applications, or virtual machines.
3. **Hybrid Cloud**: Hybrid cloud refers to a mixture of storage, and services environments made up of on-premises infrastructure.

Cloud Computing Models

1. **Network as a Service (NaaS)**: In this model, customers rent networking servers from cloud providers. It allows customers to operate their networks with maintaining the infrastructure.
2. **Infrastructure as a Service (IaaS)**: It delivers fundamental compute, network, and storage resources to customers over the internet on a pay-as-you-go basis.
3. **Platform as a Service (PaaS)**: It provides customers complete platform hardware, software, and infrastructure for developing, running, and managing applications without the cost, complexity, and flexibility of building and maintaining that platform on-premises.
4. **Software as a Service (SaaS)**: In this model, access to a particular software is provided on a subscription basis, with the software being located on external servers.

Network Security

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

Encryption

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called **cryptography.** In computing, unencrypted data is also known as **plaintext**, and encrypted data is called **ciphertext**.

Encryption Algorithms

1. **Data Encryption Standard (DES)**: The **DES** is a symmetric-key algorithm for the encryption of digital data. Its length is 56-bits that makes a less secure for algorithms to encrypt data.
2. **Triple DES (3 DES)**: It is the upgraded version of DES. It uses three 56-bit keys which make up a key of a 168-bit key.
3. **Advanced Encryption Standard (AES)**: The AES algorithm is a symmetric block cipher that can encrypt (**encipher**) and decrypt (**decipher**) information. It s capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data.

Hashing

Hashing is an algorithm that takes an arbitrary amount of data and produces a fixed-size output of enciphered text called a "**Hash**".

Hashing Algorithms

1. **Message-Digest Algorithm 5 (MD5)**: MD5 is a cryptographic hash algorithm that can be used to create a 128-bit string value from an arbitrary length string. It is most commonly used to verify the integrity of files.
2. **Secure Hash Algorithm 1 (SHA-1)**: SHA-1 is a cryptographic hash function that takes an input and produces a 160-bit hash value known as a **message digest** – typically rendered as a hexadecimal number, 40 digits long.
3. **Secure Hash Algorithm 256 (SHA-256)**: SHA-256 is the upgraded version of SHA-2 (**Secure Hash Algorithm 2**). It creates a 256-bit hash digest.

Network Attacks

1. **Man in the Middle**: This attack causes the data from the client to flow through the attacker's computer where the attacker can intercept or manipulate the data.
2. **Session Hijacking**: This attack is also known as **TCP Session Hijacking** in which the attacker guesses the session ID for a web browser session, enabling them to take over the already authorized session of the client.
3. **Botnets**: A Botnet is a network of computers infected by malware that is under the control of a single attacking party. Each machine under the control of the **bot-herder** is known as a **bot**.
4. **Denial of Service or Distributed DoS (DoS or DDoS)**: A DDoS attack is the subclass of the DoS attack. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic. When the server could not handle traffic anymore, it crashes the website.
5. **TCP SYN Flood**: When a client and server establish a normal TCP "**three-way handshake**", the exchange looks like this:
    a. The client requests a connection by sending an SYN (synchronize) message to the server.
    b. The server acknowledges by sending an SYN-ACK (synchronize-acknowledge) message back to the client.
    c. The client responds with an ACK (acknowledge) message, and the connection is established.

    In an SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. The malicious client either does not send the expected ACK packet. The server under attack will wait for acknowledgment of its SYN-ACK packet for some time.

During this time, the server cannot close down the connection by sending an RST packet, and the connection stays open. Before the connection can time out, another SYN packet will arrive. This leaves an increasingly large number of connections half-open. Eventually, as the server's connection overflow tables fill, service to legitimate clients will be denied, and the server may even malfunction or crash.

Other Attacks

1. **Logic Bombs**: It is a piece of malicious code that is intentionally inserted into the software. Logic Bombs execute their functions or launch their payload once a certain condition is met, such as upon the termination of an Employee.
2. **Phishing**: Phishing is a type of **social engineering** attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of **malware**, the freezing of the system as part of a **ransomware attack,** or the revealing of sensitive information.
3. **Ransomware**: Ransomware is a type of malicious software (**malware**) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.

Securing Networks

1. **Vulnerability Scanners**: A vulnerability scanner is a computer program designed to assess computers, networks, or applications for known weaknesses. These scanners are used to discover the weaknesses of a given system. For example, Nessus, Zenmap, Nmap, etc.
2. **Patching**: A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called **bug fixes**. The process of applying a patch is known as **patching**.
3. **Honey Pots**: A honeypot is a network-attached system set up as a decoy to lure cyberattackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers and report the administrators about the unauthorized attempt.