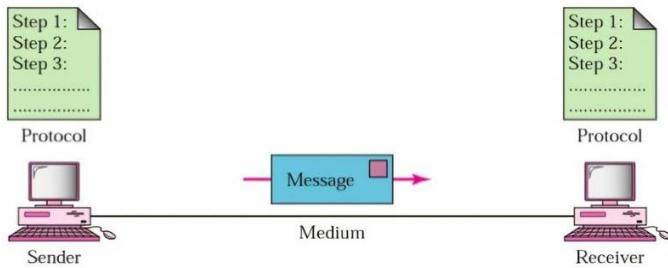


NETWORKING SHORTNOTE

Data Communication - the process of transmitting data between two or more communicating devices over some transmission media. Establishing such connections between computing devices is called **computer networking**.

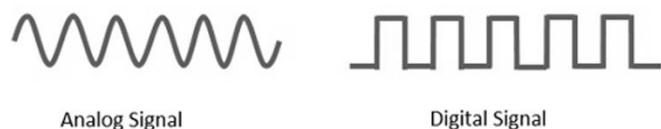
Components of a Data Communication



1. **Message** - The information to be communicated.
2. **Sender (Transmitter, Source)** - Any device of sending the Message
3. **Receiver (Destination)** - A device that the sender wants to communicate the message
4. **Communication Medium** - The path by which the message travels from sender to receiver.
5. **Protocol** - Defines the order and the format of data when the data is exchanged between two networking devices.

Signals - An electronic voltage or current, which varies with time. It is used to transfer data from one end to another.

- **Analog signal** - Are in continuous wave form in nature and represented by continuous electromagnetic waves.
Eg - sound, light and temperature
- **Digital signal** - Digital means discrete values & only two values are used to represent something, 1 and 0 (binary values).

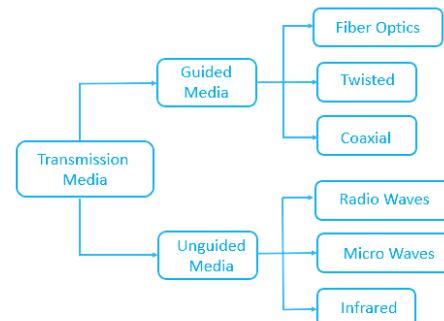


Properties of signals

1. **Amplitude** : The height of the wave measured in meters.
2. **Frequency** : The number of Complete waves that pass a point in one Second, Measured in Hertz (Hz)
3. **Wavelength** : The distance between adjacent crests, measured in meters.
4. **Phase**: A position of a point in time (instant) on a waveform cycle.

Propagation speed in a media : The speed at which a wave propagates through a given medium. The propagation speed also varies from medium to medium depending on the properties of the medium.

Transmission media - A communication channel that carries the information from the sender to the receiver.



Guided / Wired : If the medium used for data transmission is a physical medium, it is called guided or wired because they guide the data from one point to another without altering the frequencies. therefore, data impairments are reduced.

1. **Twisted Pair Cable** - Pairs of twisted copper wire are used for data transmission.

i. **Unshielded Twisted Pair (UTP)** : Used for telephone connections. These are very flexible and low-priced. However, it is difficult to transmit data for a long distance through UTP wires. suitable for <100M.

ii. **Shielded Twisted Pair (STP)** : STP is a better quality and secure data transmission medium. However, it is expensive.

Characteristics - Both digital and analog signals can be transmitted, Less cost, Easy to handle, Made of copper cable, Used in telephone lines and computer networks, Twisting reduces cross talk.

2. **Coaxial Cable** -consists of an electronic cable pair. The outer cable which is like a braided copper net produces electromagnetic field around the central cable. These two cables are separated by a plastic shield. These cables are expensive and used for TV antenna and CCTV.

3. **Fiber Optics cable** - consists of a pair of cables. There's a plastic jacket to separate the two cables. Core is a glass tube and there is glass cladding around it. The data transmission is carried out by reflecting light. These are used in modern telephone networks. The cable is relatively more expensive.

Unguided/Wireless Media : Data is transmitted as signal through the air without using physical medium.

Radio waves - Data transmission is performed using radio waves. Eg- Mobile phone signals, AM/FM radio signals, Wifi and Bluetooth

Infrared – Used for short distance communications, Slow;less than 10mbps (Eg- Tv remotes, Wireless keyboards and mouse)

Micro Waves – Microwaves travel in a straight line between transmission centers. These are positioned based on the area's geography. They're used in satellite communication, where satellites 36,000 km above capture and resend data. This method helps transmit data over long distances and is also used for internet communication.

Properties of signal transmission media

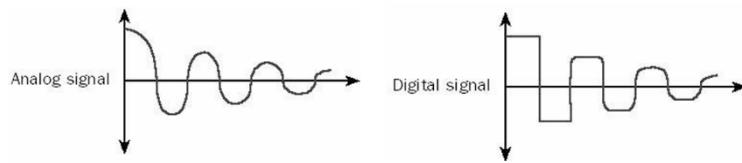
- **Latency**: An expression of how much time it takes for a unit of data to travel from one point to another. usually measured in milliseconds.
- **Bandwidth**: A range of frequencies and measured in Hertz.

Transmission Impairments in Data Communication

When analog signals travel through transmission media, their quality can deteriorate. This means the signal at the start isn't the same as at the end. This imperfection is known as signal impairment.

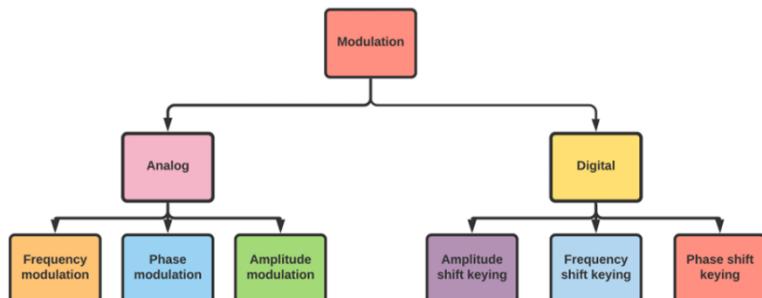
Causes of impairments:

- **Attenuation**: Reduction in signal strength due to increased distance. Amplifiers used to amplify the attenuated signal which gives the original signal back and compensate for this loss.

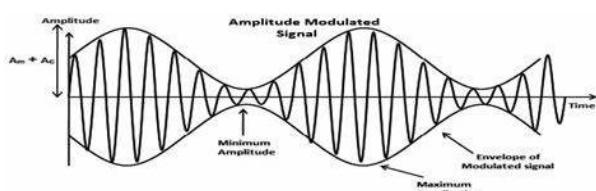


- **Distortion**: Changes in signal shape due to the medium's properties.
- **Noise**: Unwanted signals that interfere with the original signal.
 - **Induced noise**: Caused by motors and appliances acting as antennas.
 - **Thermal noise**: Created by electron movement in wires.
 - **Crosstalk noise**: One wire interfering with another.
 - **Impulse noise**: High-energy signals from lightning or power lines.

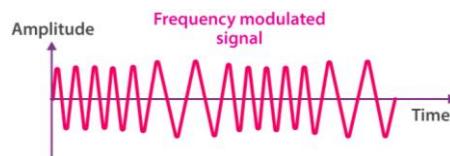
Modulation - Modulation is the technique used to send information by modifying the basic characteristics such as frequency, amplitude and phase, of an electromagnetic signal (modulating signal) by attaching it to a higher frequency signal (carrier signal), producing a modulated signal.



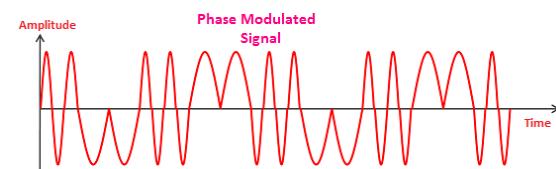
1. **Amplitude Modulation (AM)** : Amplitude of carrier signal varies according to the amplitude of modulating signal. The frequency or phase of the carrier signal remains unchanged.



2. Frequency Modulation (FM) : The carrier signal frequency changes according to the frequency of the Modulating signal.

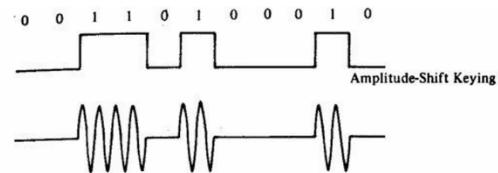


3. Phase Modulation (PM) : The phase of a carrier signal is modulated in order to reflect the changes in voltage (amplitude) of an analog data signal.

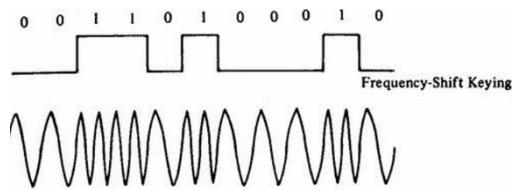


Digital-to-Analog Conversion

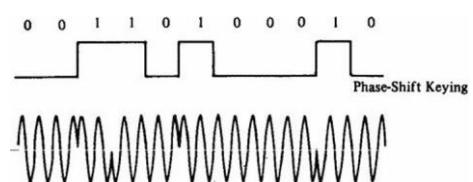
1. **Amplitude Shift Keying (ASK)** : The amplitude of an analog carrier signal is modified to reflect binary data. When binary data represents digit 1, the amplitude is held at 1, otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal .



2. **Frequency Shift Keying (FSK)** : The frequency of the analog carrier signal is modified to reflect binary data.



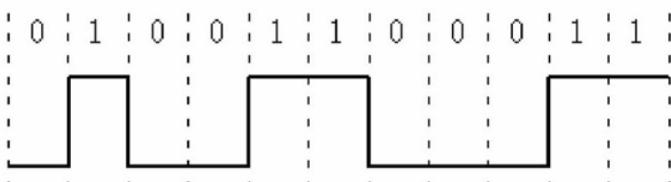
3. **Phase Shift Keying (PSK)** : In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



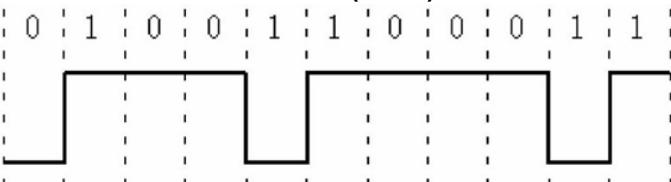
Synchronization ensures that data streams are correctly received and transmitted between devices by using a clock signal to maintain proper timing.

Signal Encoding - The conversion of data into digital signals.

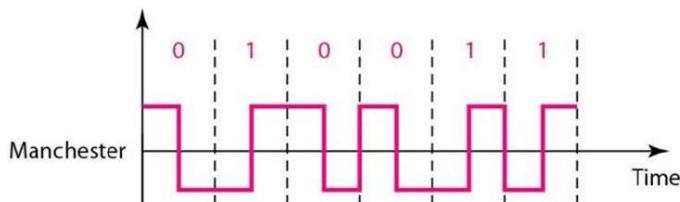
- **Non-return to Zero Level (NRZ-L):**



- **Non-return to Zero Inverted (NRZ-I):**



- **Manchester encoding:** 0 is 1 is



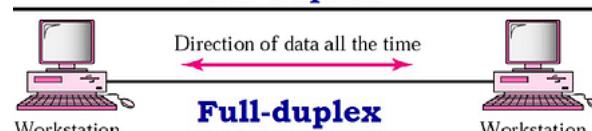
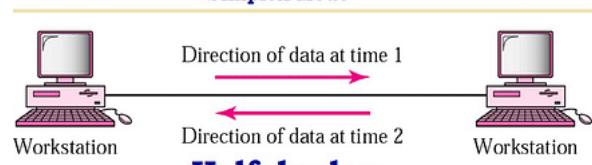
Error Control: Error detection identifies altered data bits during transmission. Error correction and recovery mechanisms fix these errors and restore the actual data bits.

- **Parity Check-** An extra bit of data is added and sent along with the original data bits

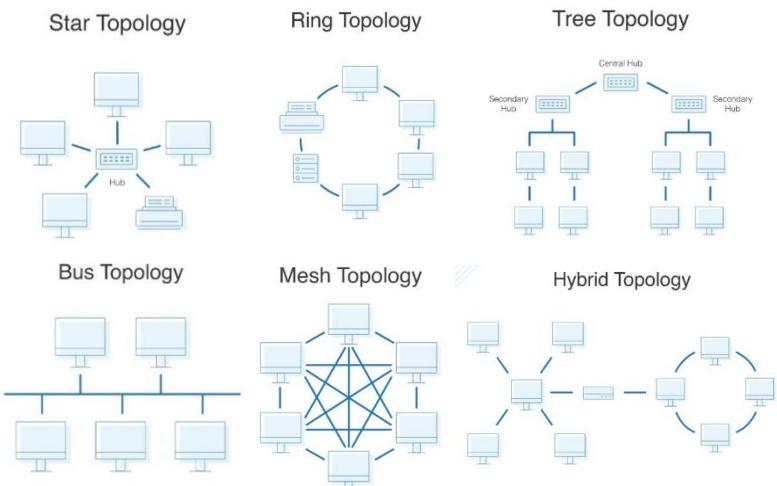
- **Odd Parity** – number of 1s in the data is odd
- **Even Parity** – Number of 1s in the data is even

Public Switched Telephone network (PSTN) is the global network of circuit-switched telephone systems, operated by various telephony providers. It includes telephone lines, fiber optics, microwaves, cellular networks, satellites, and undersea cables, all linked by switching centers, enabling most telephones to connect.

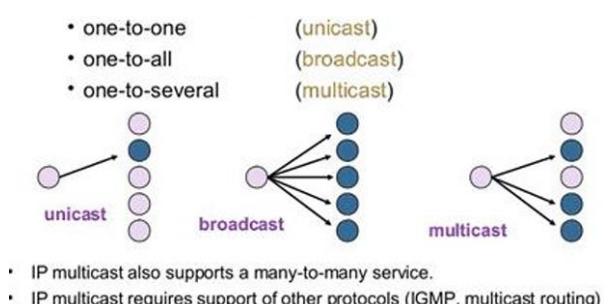
Data Transmission modes



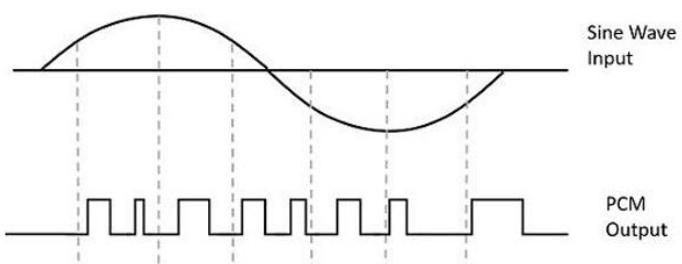
Network Topology - the pattern of connection in designing computer network



Topology	Advantages	Disadvantages
Bus	The easiest network topology for connecting peripherals or computers in a linear fashion. It is easy to connect or remove devices in this network without affecting any other device.	Bus topology is not great for large networks. If a main cable is damaged, whole network fails or splits into two. This network topology is very slow as compared to other topologies.
Ring	In this data flows in one direction which reduces the chance of packet collisions. Equal access to the resources. Speed to transfer the data is very high. Minimum collision. It is cheap to install and expand.	Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes. If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
Star	It is very reliable – if one cable or device fails then all the others will still work. It is high-performing as no data collisions can occur. Easy fault detection because the link are often easily identified.	Requires more cable than a linear bus. If hub goes down everything goes down, none of the devices can work without hub. Extra hardware is required (hubs or switches) which adds to cost.
Mesh	Failure during a single device won't break the network. Adding new devices won't disrupt data transmissions. This topology provides multiple paths to succeed in the destination and tons of redundancy.	It's costly as compared to the opposite network topologies i.e. star, bus, point to point topology. Installation is extremely difficult in the mesh. Maintenance needs are challenging with a mesh.



PCM (pulse code modulation) - It converts an analog signal into digital form.



Network Devices

- **Modem** - A modem connects computers to the internet by Converting digital signals to analog and vice versa (Modulation and Demodulation). Types include internal, external, and wireless modems, with routers often having built-in modems.
 - **Repeater** – Receives weak signals & retransmits signals at a higher level or power.
 - **Network Interface Card(NIC)** – Hardware component that connects a computer to a network.
 - A **hub** receives data in one of its incoming connections and then shall forward the data to all of its outgoing connection
 - A **switch** receives data in one of its incoming connections and forwards the data only on the outgoing connection which connects to the destination device.
 - **Bridge** – Has 2 ports each attached to different segments of the network.
 - **Router** – Connect multiple LANs with WANs , Makes Intelligent decisions on routing a data packet based on IP network address
 - A **gateway** is a device that connects different networks and manages traffic flow. It uses multiple protocols, making it more complex than a switch or router. In workplaces, it routes traffic from the main workstation to external networks. At home, it provides internet access.

In **FDMA**, the bandwidth is divided into frequency bands, each assigned to a specific station permanently.

In **TDMA**, stations share the channel's bandwidth over time. Each station gets a specific time slot to send data, ensuring organized transmission.

CDMA uses different codes for communication, allowing multiple stations to share the entire bandwidth simultaneously, unlike FDMA (which uses separate frequency bands) and TDMA (which assigns time slots).

ALOHA is designed for wireless LAN and shared mediums, allowing multiple stations to transmit data simultaneously. This can lead to collisions and garbled data.

- **Pure Aloha:** Sends data, waits for acknowledgment. If none, waits random time and resends. Reduces collisions.
 - **Slotted Aloha:** Sends data at start of time slots. Missed slot? Wait for next slot. Efficiency?

CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data.

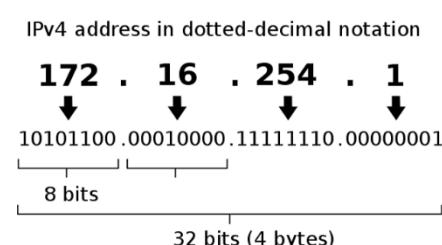
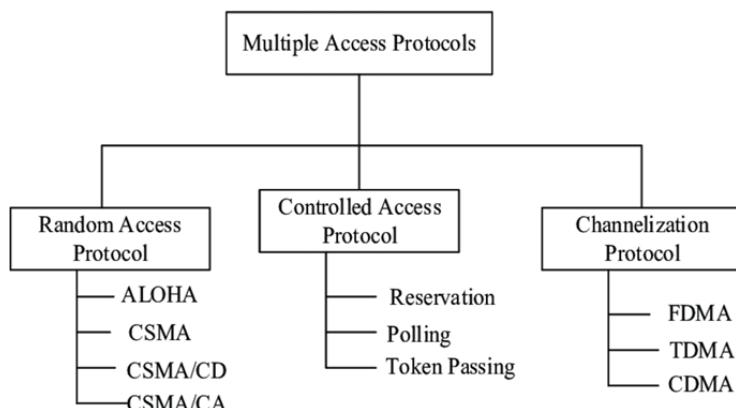
- **CSMA/CD**: Stations detect collisions and stop transmission if one occurs.
 - **CSMA/CA**: Stations avoid collisions by waiting for the channel to be idle before starting transmission.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Used to interconnect devices in internet or in ethernet. In TCP/IP, a unique identifier is called an IP address; every machine in a network has a unique IP address.

Protocol – defines how data is formatted and exchanged between devices.

Multiple Access Control Protocols - required to decrease
Collision and avoid crosstalk.

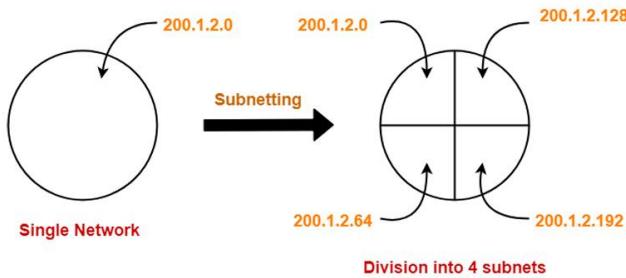


	First byte	Second byte	Third byte	Fourth byte
Class A	0 to 127			
Class B	128 to 191			
Class C	192 to 223			
Class D	224 to 239			
Class E	240 to 255			

First IP Address – Network Address

Last IP Address – Broadcast Address

127.0.0.1 – for loopback testing



Classless Inter Domain Routing (CIDR): instead of full class A, B or C networks, organizations can be allocated any number of addresses using this scheme.

Private IPs: Three sets of address ranges are used for private use.

- 10.0.0.0 – 10.255.255.255 (10.0.0.0/8) – 16M addresses
- 172.16.0.0 – 172.31.255.255 (172.16.0.0/12) - 1M addresses
- 192.168.0.0 – 192.168.255.255 (192.168.0.0/16) – 64k addresses

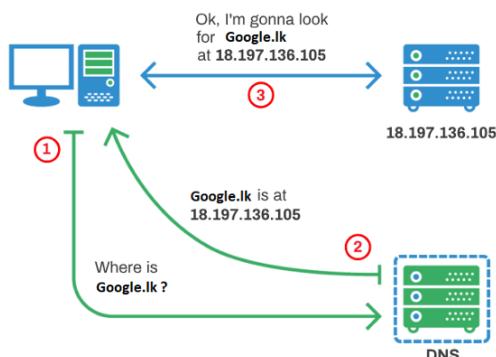
IPv6 - Uses 128-bit addresses (compared to 32-bit addresses of IPv4), offering more IP addresses. Written as eight groups of four hexadecimal digits, separated by colons.

- Eg: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Media Access Control Address (MAC address)

MAC addresses uniquely identify each network interface of a device. They are 48-bit long, divided into 6 blocks, shown as hex numbers separated by colons (e.g., 4A:8F:3C:4F:9E:3D).

Domain Name System (DNS): DNS provides directory lookup service for given URLs and the web addresses. (translate domain names into IP addresses)



Dynamic Host Configuration Protocol (DHCP) - Assigning IP addresses dynamically on a network. Provides a central database for keeping track of computers that have connected to the network. DHCP simplifies network administration it keeps track of IP address than requiring an administrator to manage the task.

Multiplexing: Combining multiple signals into one signal for transmission over a single medium.

Demultiplexing: Separating the combined signal back into individual signals at the receiving end.

Servers - A server runs specific programs to offer services that other machines (clients) request to perform tasks. This forms a client/server network, providing centralized access to information, resources, and data.

i. FILE SERVER - File Transfer Protocol (FTP) is a common server type. It is responsible for transferring files from server to a computer and vice versa. The default port of FTP is 20/21.

ii. Proxy servers improve network speeds and save bandwidth by compressing traffic and caching files. They also hide your real IP address from websites, logging the proxy server's IP instead.

iii. web server: hosts website files and serves them to web browsers. It loads each file of a web page and displays it as a complete page in the browser.

- **HTTP (Hypertext Transfer Protocol):** The main protocol for data on the web, linking text with hyperlinks. Default port is 80, and secured version (HTTPS) uses port 443.

- **SSH (Secure Shell):** The main method for securely managing network devices at the command level, replacing Telnet. Default port is 22.

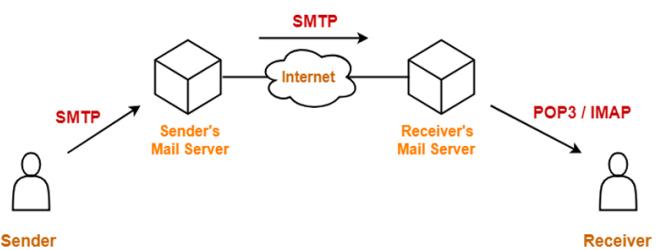
- **Telnet:** A protocol used to remotely access and manage network devices over the internet, but it's not secure.

iv. MAIL SERVER - crucial for sending, receiving, and storing emails on networks and the internet, using standard email protocols.

- **SMTP(Simple Mail Transfer Protocol)** is a protocol used to send emails between servers and from users to mail systems. Default port is 25

- **pop3 (Post Office Protocol version 3)** A protocol to retrieve emails from the internet. It lets you download emails from the server and then deletes them from the server. Default port is 110

- **IMAP:** A protocol to retrieve emails from a server, but unlike POP3, it keeps the emails on the server. Default port is 143.



v. Printer server: Accepts print jobs connected in a network and send to printers(print spooling)

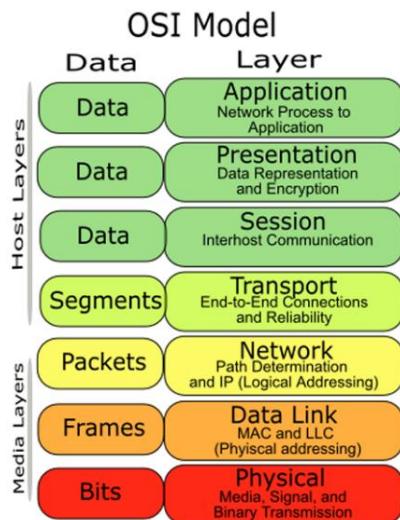
Network Models		
TCP/IP Model	OSI Model	Protocols
Application layer	Application layer	FTP, HTTP, Telnet
	Presentation layer	JPEG, MPEG
	Session layer	NFS, SQL, PAP
Transport layer	Transport layer	TCP, UDP
Internet layer	Network layer	IPv4, IPv6
Network Access Layer	Data Link Layer	ARP, CDP, STP
	Physical layer	Ethernet, Wi-Fi

TCP/IP Model (Transmission Control Protocol/Internet Protocol)

- **Network Access Layer:** The lowest layer; delivers data to devices, transmits IP datagrams, encapsulates into frames, and maps IP to physical addresses.
- **Internet Layer:** Manages network connections, addresses, and data delivery. Handled by Internet Protocol (IP).
- **Transport Layer:** Deals with data transmission using TCP and UDP.
- **Application Layer:** Provides network services to applications, using protocols like HTTP, SMTP, and FTP.

OSI model (Open Systems Interconnection Model)

The OSI model is a framework that defines the functions of a networking system into universal rules, ensuring different products and software can work together seamlessly. It helps achieve interoperability.



7. **Application Layer:** Interfaces with end-user and applications, using protocols like HTTP, SMTP, FTP, DNS, DHCP, Telnet, POP3

6. **Presentation Layer:** Handles data presentation, encoding, and encryption, with formats like JPEG, MP3.

5. **Session Layer:** Manages communication sessions, establishing, maintaining, and terminating connections.

4. **Transport Layer:** Controls data flow, error detection, and correction. Key protocols are TCP, UDP.

3. **Network Layer:** Routes data packets between devices in Different networks, using IP addresses. Manages packet forwarding.

2. **Data Link Layer:** Connects devices within the same physical network, breaking data into frames. Handles flow control and error detection.

2 sub layers:

- i. **MAC – Media Access Layer** → MAC addresses
- ii. **LLC – Logical Link layer** → frame synchronization, frame control & error checking

1. **Physical Layer:** Deals with physical components like cables and radios, delivering raw data between devices.

ICMP -Internet Control Message Protocol – Used by devices such as routers to send error messages (For reliable & ordered delivery of data)

TCP vs UDP	
TCP is a connection-oriented protocol	UDP is a connectionless protocol
TCP is comparatively slower than UDP	UDP is much faster
Can guarantee delivery of data	Cannot guarantee delivery of data
Does not support Broadcasting	Does support Broadcasting
Packets arrive in order at the receiver.	There is no sequencing of data in UDP.
Used by HTTPS, HTTP, SMTP, POP, FTP, etc	Video conferencing, streaming, DNS, VoIP, etc

Network Commands

- **ipconfig:** Contains IP address, network mask, default gateway for all physical & virtual network adapters
- **ipconfig /all:** Contains IP address, Ethernet MAC address, DNS settings, DHCP server info, host name, default gateway for all physical & virtual network adapters
- **nslookup:** Finds the IP address associated with a domain name.
- **tracert:** (Trace route) Display all the routers between source to destination
- **netstat:** (Network Statistics) Lists active network connections and ports.
- **ping:** Used to test reachability of a host on an IP network, measure round trip time from sending messages to destination and back again

Threats

- **Malware:** Software designed with harmful intentions.(virus, trojans, worms etc..)
- **Viruses:** Programs that enter your system and perform harmful activities without your knowledge.(Boot sector viruses, macro viruses, logic bomb, time bomb)
- **Trojans:** Appears as a useful code, but does something harmful when executed
- **Phishing:** Attempts to steal sensitive information by pretending to be a trustworthy entity.
- **Spyware:** spying and stealing personal information
- **Adware:** Ads displayed without user permission
- **Spoofing:** A technique where an attacker impersonates another device or user by falsifying data to gain unauthorized access to a system.

- **Information Disclosure:** The unauthorized release of confidential information, often due to poor security controls or vulnerabilities.
- **Denial of Service (DoS):** An attack that overwhelms a system, network, or service, rendering it unavailable to legitimate users.
- **Port Scan:** A method of probing networked devices to identify open ports, which can reveal potential vulnerabilities to exploit.
- **Espionage:** The act of spying or gathering confidential information, typically by governments or organizations, often for political or competitive advantage.
- **Eavesdropping:** Intercepting private communications or data transfers, often covertly, to gain sensitive information.
- **Man-in-the-Middle (MitM):** An attack where an adversary secretly intercepts and possibly alters the communication between two parties to exploit or manipulate the data being exchanged.

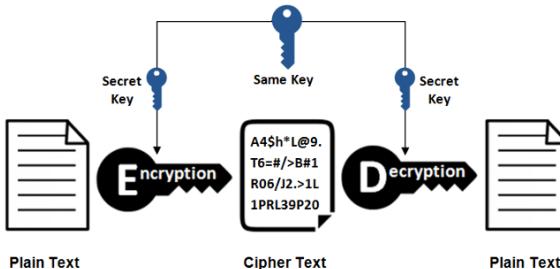
Protection against unauthorized malicious accesses

- **Firewalls:** Devices that monitor and filter network traffic, acting as barriers between private networks and the internet.
- **Antivirus Software:** Programs that detect and isolate malicious software trying to harm a computer.
- **User Education:** Essential for protecting devices from attacks. Choose strong passwords and regularly update antivirus software to safeguard systems.

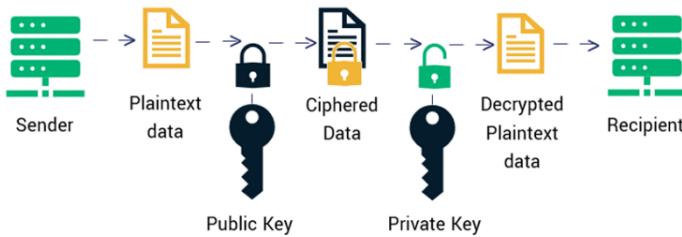
Network Security

Encryption: A method in cryptography ensuring data confidentiality during transmission.

• Symmetric Key Encryption:



• Asymmetric Key Encryption



A **digital signature** is like a signature on a paper document — it shows the receiver that the content is trustworthy. For digital documents, a digital signature verifies the source, author, date, and time, confirming that the message content is authentic and hasn't been changed.

ISPs: An Internet service provider (ISP) is an organization that provides services to accessing and using the Internet services.

Dialup connection – Uses traditional telephone lines, and an analog modem. Can't make calls when connected to internet and vice versa.

Advantages of DSL

- **Independent Services:** Losing internet doesn't mean losing phone service. With cable, a failure can knock out all services.
- **Security:** DSL keeps each user separate, unlike some cable networks where users share the network, risking security.
- **Compatibility:** DSL connects easily with other network tech, making remote work setups easier.

Advantages of ADSL

- **Lower Cost:** ISPs often offer high-speed ADSL at affordable rates, usually with a static IP.
- **Flexible Setup:** Engineers can adjust VPN connections quickly to solve network issues.
- **Fast Internet:** ADSL provides high-speed browsing, streaming, and large file downloads, much faster than dial-up.

Network Address Translation

typically found in routers and firewalls. These devices use NAT to convert private IP addresses to a public IP address