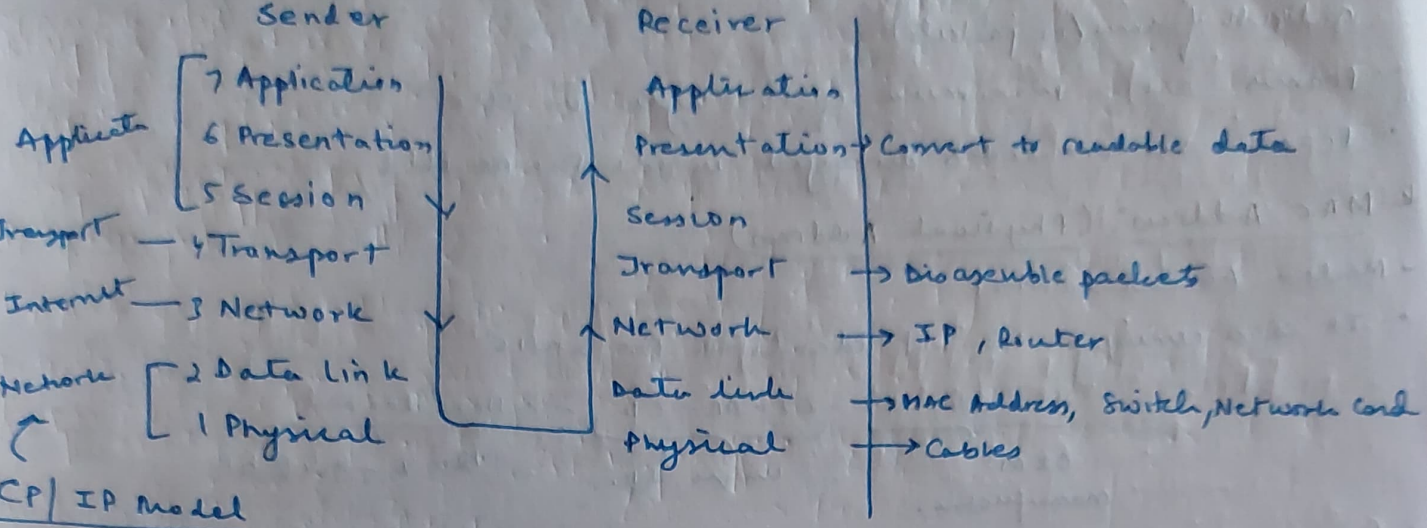
Computer Networks

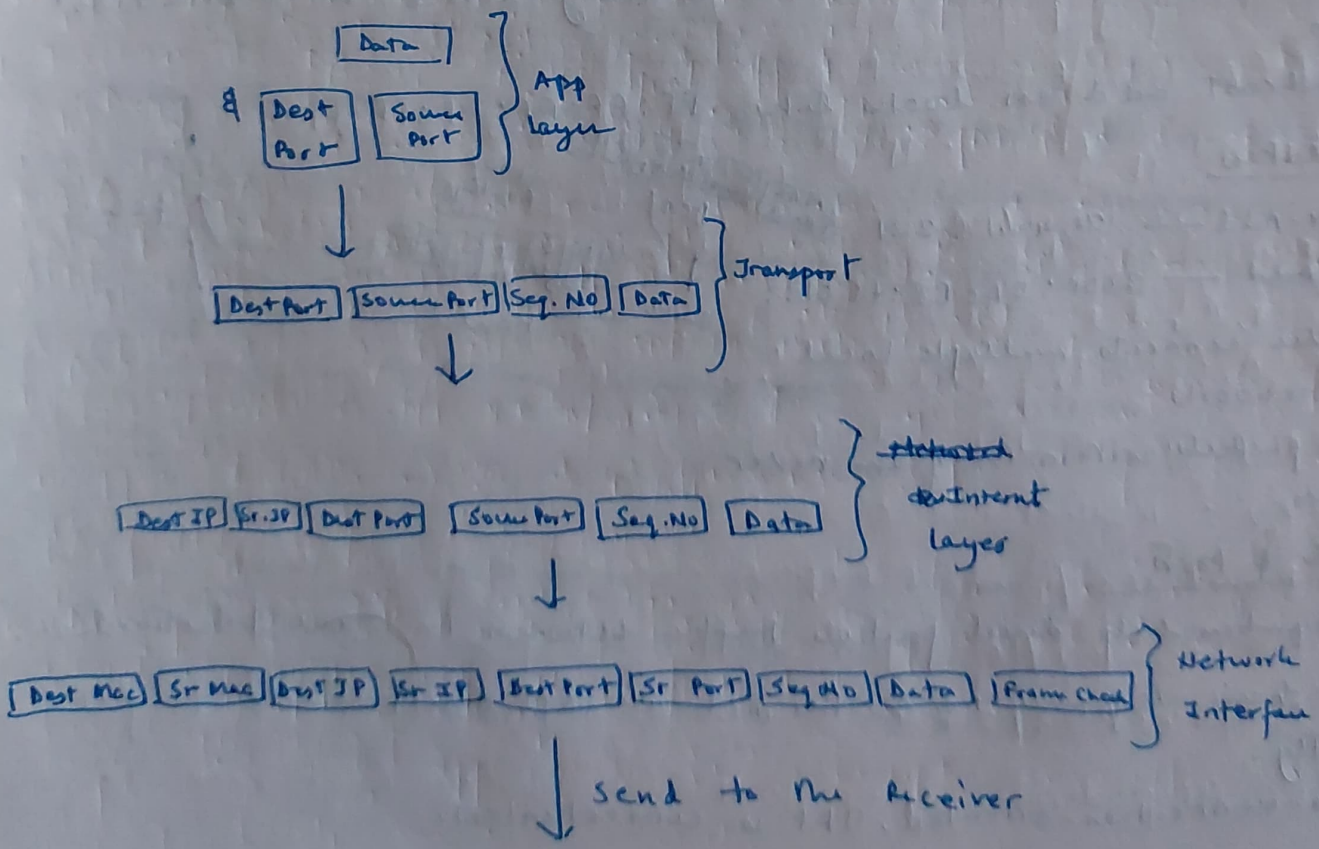
Layers are used to organise protocols like HTTP, TCP, UDP, IP...

OSI Model (Open Systems Interconnection)



TCP/IP Model

4 Application
3 Transport
2 Internet
1 Network Interface



NIC → Network Interface Card.

Frames:

- Devices on a network send & receive data in discreet chunks called frames (or packets)
- Frames are a maximum of 1500 bytes in size
- Frames are created & destroyed inside the NIC

MAC Address: (Physical Address)

- Media Access Control
- It is a unique 48-bit identifier for a NIC

12-34-54-67-AB-CD → Hexadecimal

12-34-54 → OEM manufactu.

67-AB-CD → unique ID.

12 × 4 → 48 bit

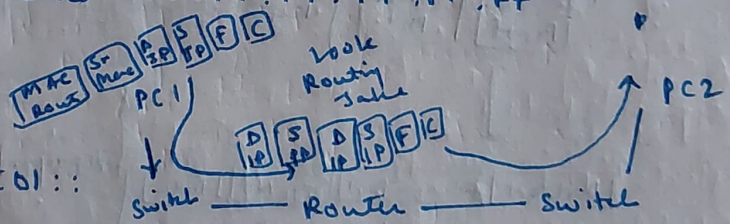
- frames have destination & source MAC Addresses
- NIC use MAC addresses to decide whether or not to process a frame.

Unicast / Broadcast:

- Unicast transmission is addressed to a single device on a network.
- A broadcast transmission is sent to every device in a broadcast domain
- A broadcast address looks like FF:FF:FF:FF:FF:FF

IP Address

- IPv4 Add — 31.44.17.231
- IPv6 Add — 2001:0DB8:fE01::
- A router connects multiple local area networks
- The IP packets within the frame never changes.



Packets & Ports

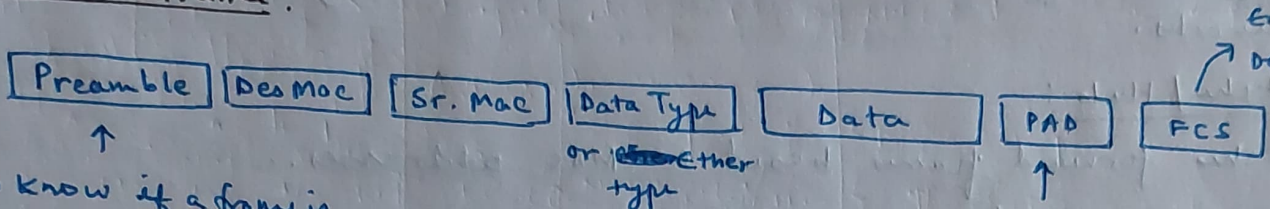
- Port numbers help direct packets traffic between the source & destination.
- Packets have sequence no. so the network soft can resemble the file correctly.
- TCP is connection-oriented, UDP is connectionless.

Ethernet:

Ethernet is defined by the IEEE 802.3 standard.

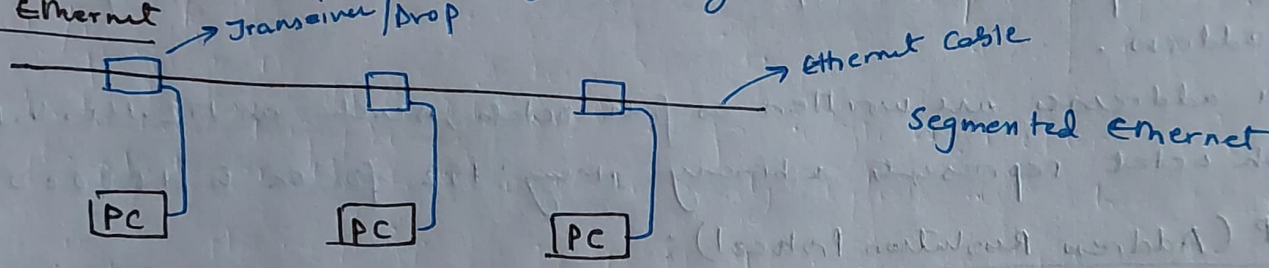
- The IEEE has defined many versions of ethernet.
- Syntax: 10 Base 5
  - 10 ↑ speed in megabit/sec

Ethernet frame:



- Minimum data size – 64 bytes
- Max data size – 1522 bytes
- A jumbo frame can carry 9000 bytes

Old Ethernet



Segmented Ethernet

- In order for them to talk at the same time, CSMA/CD.
- CSMA/CD – Carrier sense Multiple Access / Collision Detection
- 10 Base 5 and 10 Base 2 require terminating resistors at both ends of a segment (cable)
- When connecting to 10 Base 2, always use a 'T' connector.

10 Base T:

- MSAU – Multistation Access Unit
- 10 Base T runs at 10 Mbps over Cat 3 or better UTP.
- 10 Base T can have up to 1024 nodes per switch
- 10 Base T cable runs are a maximum of 100 meters b/w the switch & node.

* Terminating Twisted Pair:

- An RJ-45 (aka 8P8C) connector is used to connect to most network cards.
- Watch the position of the wires when crimping to follow 568A or 568B standards.
- Straight-Through cables are the most commonly used cable in networks.

* Switches / Hubs:

- Switches forward frames based on MAC addresses.
- Hubs use CSMA/CD to avoid collisions.
- Switches create & use MAC address tables to map ports & host devices.

* TCP/IP Basics:

- Each computer on a TCP/IP network must have a unique IP address.
- IPv4 addresses are written as four octets, such as 192.168.4.12
- Each octet represents a binary string; 192 for ex is 11000000

* ARP (Address Resolution Protocol):

- ARP resolves MAC addresses from IP addresses.
- arp -a //stores MAC. (shows ARP cache)
- ARP requests a broadcast over the network.

* IANA (Internet Assigned Numbers Authority)

- RIR (Regional Internet Registry)

* Class

- A - 0-126 /8
- B - 128-191 /16
- C - 192-223 /24
- Subnetting divides Network IDs into two or more networks

Subnet Masks:

Cannot use 0 & 255 for host ID.

- The default gateway will figure out where to forward the message.
- Each host needs a subnet mask.
- The host uses the subnet mask to know if the destination is on the local network or a remote network.

* Subnetting with CIDR:

- CIDR – Classless Inter-Domain Routing
- Subnet masks have all 1's on the left & all 0's on the right
- The more subnets you have the less hosts are available.

/24	→ 254 hosts	/28	→ 14 hosts
/25	→ 126 hosts	/29	→ 6 hosts
/26	→ 62 hosts	/30	→ 2 hosts
/27	→ 30 hosts	/31	→ 0 hosts

To remember

$\frac{254}{2} - 1 = 126$

$\frac{126}{2} - 1 = 62$

⋮

* Dynamic & Static IP Addressing:

- DHCP – Dynamic Host Configuration Protocol

for Linux its. BOOTP – Bootstrap Protocol

- Each broadcast domain must have only one DHCP server.
- DHCP server has to be run within broadcast domain.
- APIPA – Automatic Private IP Addressing

A APIPA addresses always start with 169.254

- If you get an IP address other than your current network ID, you may have a rogue DHCP server.

* Special IP Addresses:

1. 10.x.x.x → private IP address
2. 172.16.x.x – 172.31.xx → private IP addresses
3. 192.168.x.x → private ip address

* Loopback Address

IPv4 – 127.0.0.1

IPv6 – :: 1

* Routing :-

- Router - A box that connects network IDs.
- Routers only care about destinations
- Routers can use any network medium.
- All routers have a routing table.

Switch - MAC
Router - IP

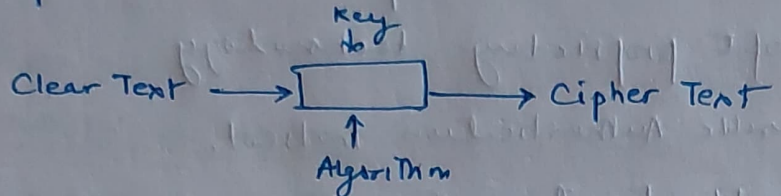
Securing TCP/IP:

CIA – Confidentiality Integrity Availability

- Authentication – login + password (who you are)
- Authorization – permissions (what you are allowed to do)

* Symmetric encryption:

- Caesar cipher – Rotations



- Symmetric Enc. Algo uses same key for enc & decryption

* Asymmetric Encryption:

- Two keys, public key & private key.
  - public key → encrypt
  - private key → decrypt

* Cryptographic Hashes:

- Hash Algo – A hash algo creates a fixed-size hash value.
- Hashes are used to verify data integrity, not for encryption
- Ex: MD5, SHA-1

* Identification:

- **Authentication factors**
  1. Something you know – passwords, captcha, pin, security ques.
  2. Something you have – cards
  3. Something you are – biometrics

* Access control:

- MAC – Mandatory Access control – (Top secret) – uses labels
- DAC – Discretionary Access control – (Owner) – gives creator control over permissions
- RBAC – Role-based Access control – uses groups

Kerberos / EAP:

- KDC - Key Distribution Center
  - AS: Authentication Service
  - TGS: Ticket-Granting service
- TGT - Ticket-Granting Ticket
- TGT issues token based on timestamp
- Kerberos is a Microsoft proprietary technology
- PEAP - Protected Extensible Authentication Protocol.
- Kerberos handles authentication & authorization for wired networks.
- Kerberos relies heavily on time stamps

Single sign-on:

- For local area networks, use Windows Active Directory for single sign-on
- SAML is used to manage multiple apps using a single account.

Certificates & Trust:

- Certificates include a public key and at least one digital signature.
- Public key infrastructure uses a hierarchical structure with root servers.

Advanced Networking Devices:

Telnet:- Telnet enables you to access a remote computer

Telnet runs on TCP port 23.

PUTTY is a free, robust telnet/SSH client

Telnet (unsecure) & SSH [Secure Shell] (Secure) (port=22) are both terminal emulators.

SSH uses an authentication.

- **VPN (Virtual Private Networks)**:

Tunnel connection for remote computer to get to a designated endpoint.

- **IDS vs IPS**

→ IDS – Intrusion Detection System
- Inside of network & monitors
- IDS out-of-band does monitoring & alert

→ IPS – Intrusion Prevention System
- IPS in-band actively stops or rejects

A firewall can block connections while IDS cannot

* **Protecting your Network**:

* **Denial of service**:

- Volume Attack: Ping flood, UDP flood
- Protocol Attack: SYN flood / TCP SYN Attack
- Application Attack
- Amplification Attack: Smurf Attack
- DDOS – Distributed Denial of Service
  - Multiple comp attacks / Botnet

Malware

- **Virus** –
  - → Attach to other files
  - → Propagate
  - → Spread to other devices
  - → Activate
- **Adware** –
  - → Adv pop ups on the browser
- **Spyware** –
  - → Hidden & collecting data
- **Trojan Horse & Rats**
  - → Remote Access Trojans (RATs)
- **Polymorphic Malware, Keyloggers & Armored Viruses**
  - ↳ Changes itself
  - → **Armored Virus** – Hard for Anti-malware to detect
  - → **Keylogger** – Captures keystrokes.
- **Ransomware / Crypto-malware** –
  - → Locks system
- **Logic Bomb** –
  - → Triggered by an event
- **Rootkit & Backdoor**
  - → Rootkit is soft that escalates privileges to execute other things on a computer.

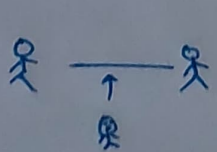
Social Engineering :-

- Dumpster diving
- Phishing
- Shoulder surfing

Access control :-

- **Stateless Firewall** – Use pattern analysis & heuristics to decide which packets should be blocked.
- **Stateful Firewall** – Examine each packet to decide which packets should be blocked.

MITM - Man In The Middle :-

- Third-party interception between a two-party conversation
- Uses the information to the third party's advantage.
- Ettercap Tool
- Session Hijacking – 

Firewalls:

Firewalls filter traffic based on specific criteria.

- Typical firewall placement at edge of network.
- All routers may have firewall, but its not mandatory; firewall can be separate as well.
- Network firewall protect the network.
- A physical firewall device is called a hardware firewall.
- Host-based software firewall on individual stations.
- UTM - Unified Threat Management
- Stateless - Filter based on IP & port numbers
- ACL - Access Control list
- Stateful - Track the state of the conversations
- Context - & - Application - aware firewalls filter based on the content of packets.

DMZ:

- A DMZ is an area of a network that hosts public-facing servers.
- Servers in the DMZ are still protected by a firewall.
- A bastion host is any machine directly exposed to the public Internet.
- Honeypot - Invite attacks to capture information. (Ex: HoneyBot)
- Honeynets - Busy network sites used to attract attackers.

- Driver Update
- Firmware Update
- Switch Update
- OS Update
- Port Management
- Vulnerability Assessment
- Role separation, access control list, and privileged account security are all examples of user account management.

* Virtualization & Cloud computing:

- Hypervisor – Virtual Machine Monitor (VMM)
- Type 2 hypervisor – runs on top of host OS
- Type 1 hypervisor – runs directly on top of hardware, independent of host OS.

* Cloud ownership

- Private • Public • Hybrid • community
- Private clouds allow access to members only.
- Public clouds are available to anyone.
- A private cloud with contracted management is considered a hybrid cloud.

* Cloud implementations

- VPC – Virtual Private Cloud
- VPC depends on the services requested, including IAAS, PAAS
- VPC services are very flexible, expandable & can provide many types of services.
- Building Web servers on cloud applications is very easy, but there can be costs associated with the service

* NAS & SAN:

- NAS - Network Attached storage (file level)
- SAN - Storage Area Network (Block level)

* PAAS (Platform As A Service)

Ex: Heroku.

- PAAS enables access to a software development platform without the need to personally host it.
- A PaaS allows very quick access to software running live on the Internet.

* Saas (Software as a Service):

- Enables access to applications via subscription. Ex. Office 365

* Iaas (Infrastructure as a Service)

- Iaas enables quick configuration of network resources hosted by someone else
- Ex: AWS