Classification categories of the computer networks

1) **Size of the physical area:**
    a. BAN: Body Area Net., BCI – Brain Computer Interface
    b. PAN: Personal Area Network
    c. SOHO: Small Office/Home Office
    d. LAN: Local Area Network
        - System of a communication computers.
        - Area: n * km^2, one site/institute/company/organization
        - Continuous access to the network services
        - Management done by the owner
        - Transmission rate: 100 Mbps … 10 Gbps …
        - High Level of reliability (short distances, robust technology)
        - Lan Types: **Connected media** (galvanic: twisted pair, coaxial cable, optical cable), **Connectionless** (wireless, radio waves).
        - Basic elements of the LAN: Computers, Network Interface Cards (NIC), Network Media (twisted pair, coaxial cable, optical fiber, radio wave), Network Devices (Repeater/Hub, Bridge, Switch, Router)
    e. MAN: Metropolitan Area Network
        - System of LANs
        - Area: n * 100 km^2, one city/region
        - Connects two to more LANs
        - E.g.: Bank or travel agency or university with several sites
        - Leased lines of a service provider are used (usually)
        - Technology: Similar to LANs
        - Connection between the sites can be wired or wireless.
    f. WAN: Wide Area Network
        - System of LANs and MANs
        - Area: country, continent, World
        - All users can communicate among
        - Remote access of the resources
        - Services: E-mail, WWW, file transfer, e-commerce, etc.
    g. GAN/Internet: Global Area Network
2) **Transmission Rate:**
    a. Classical Networks: kbps …. Mbps
    b. High Speed Networks: 100 Mbps … Tbps
3) **Ownership:**
    a. Private Network
    b. Public Network
4) **Mobility:**
    a. Fixed Network
    b. Mobile Network

Layered network models

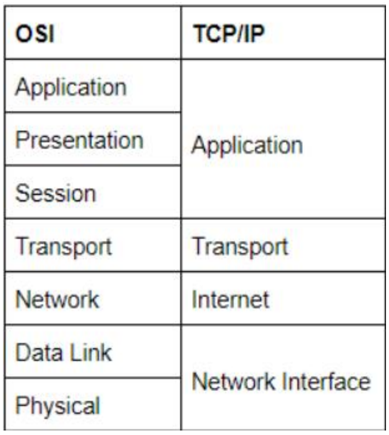
There are two models that are widely referenced today: OSI and TCP/IP. The concepts are similar, but the layers themselves differ between the two models.

While TCP/IP is the newer model, the Open Systems Interconnection (OSI) model is still referenced a lot to describe network layers. The OSI model was developed by the International Organization for Standardization. There are 7 layers:

1. Physical (e.g., cable, RJ45)
2. Data Link (e.g., MAC, switches)
3. Network (e.g., IP, routers)
4. Transport (e.g., TCP, UDP, port numbers)
5. Session (e.g., Syn/Ack)
6. Presentation (e.g., encryption, ASCII, PNG, MIDI)
7. Application (e.g., SNMP, HTTP, FTP)

The TCP/IP model is a more concise framework, with only 4 layers:

1. Network Access (or Link)
2. Internet
3. Transport (or Host-to-Host)
4. Application (or Process)

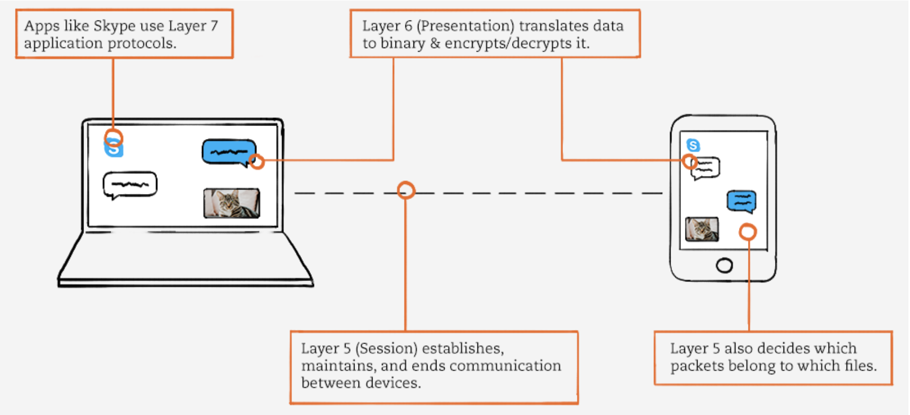


OSI	TCP/IP
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link	Network Interface
Physical	

Skype, as a network-connected application, uses **Layer 7 (Application) protocols** like Telnet. If you send your friend a picture of your cat, Skype would be using the File Transfer Protocol (FTP).

Layer 6 (Presentation) receives application data from Layer 7, translates it into binary, and compresses it. When you send a message, Layer 6 encrypts that data as it leaves your network. Then it decrypts the data when your friend receives it.

Applications like Skype consist of text files and image files. When you download these files, **Layer 5 (Session)** determines which data packets belong to which files, as well as where these packets go. Layer 5 also establishes, maintains, and ends communication between devices.



Apps like Skype use Layer 7 application protocols.

Layer 6 (Presentation) translates data to binary & encrypts/decrypts it.

Layer 5 (Session) establishes, maintains, and ends communication between devices.

Layer 5 also decides which packets belong to which files.

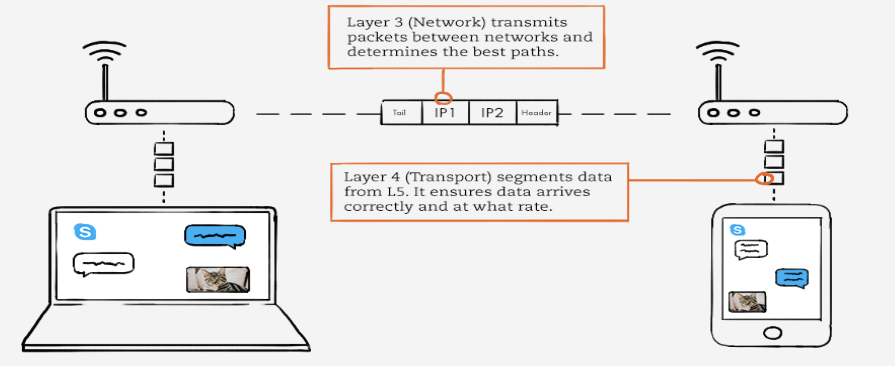
Layer 4 (Transport) receives data from Layer 5 and segments it. Each segment, or data unit, has a source and destination port number, as well as a sequence number. The port number ensures that the segment reaches the correct application. The sequence number ensures that the segments arrive in the correct order.

This layer also controls the amount of data transmitted. For example, your laptop may be able to handle 100 Mbps, whereas your friend's phone can only process 10 Mbps. Layer 4 can dictate that the server slows down the data transmission, so nothing is lost by the time your friend receives it. But when your friend sends a message back, the server can increase the transmission rate to improve performance.

Lastly, Layer 4 performs error-checking. If a segment of data is missing, Layer 4 will re-transmit that segment.

TCP and UDP are both very well-known protocols, and they exist at Layer 4. TCP favors data quality over speed, whereas UDP favors speed over data quality.

Layer 3 (Network) transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination. Layer 3 also determines the best paths for data delivery.



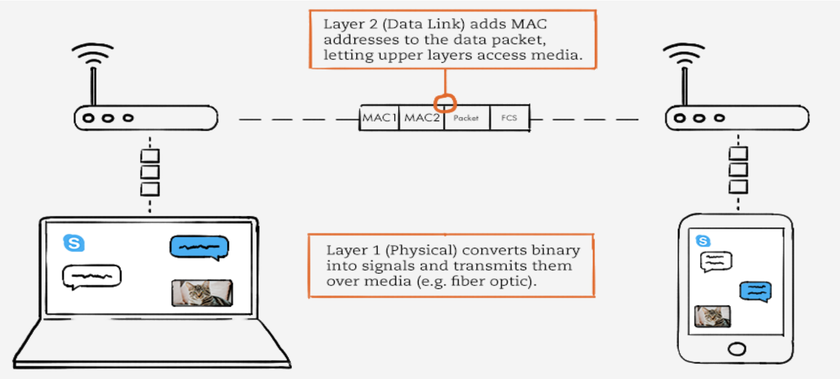
Layer 3 (Network) transmits packets between networks and determines the best paths.

Layer 4 (Transport) segments data from L5. It ensures data arrives correctly and at what rate.

Layer 2 (Data Link) focuses on the physical addressing of the transmission. It receives a packet from the network layer (that includes the IP address for the remote computer) and adds in the physical (MAC) address of the receiving endpoint. Inside every network enabled computer is a Network Interface Card (NIC) which comes with a unique MAC (Media Access Control) address to identify it. When information is sent across a network, it's actually the physical address that is used to identify where exactly to send the information. Additionally, it's also the job of the data link layer to present the data in a format suitable for transmission.

In short, Layer 2 allows the upper network layers to access media, and controls how data is placed and received from media.

Layer 1 (Physical) is right down to the hardware of the computer. This is where the electrical pulses that make up data transfer over a network are sent and received. It's the job of the physical layer to convert the binary data of the transmission into signals and transmit them across the network, as well as receiving incoming signals and converting them back into binary data.


Layer 2 (Data Link) adds MAC addresses to the data packet, letting upper layers access media.

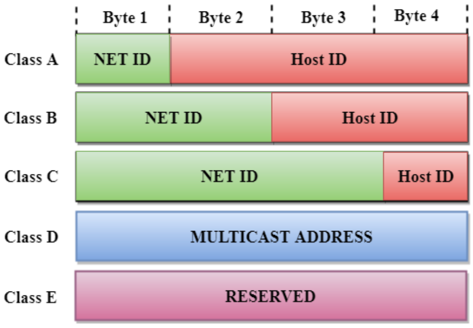
Layer 1 (Physical) converts binary into signals and transmits them over media (e.g. fiber optic).

Addressing System of IP technology

- Every node in the computer network can be identified by IP address, it’s a logical address.
- Can be changed based on the location of the device.
- An IPv4 address is 32-bit long and are unique.
- The address space in a protocol that uses N-bit to define an address is 2^N.
- The address space of IPv4 is 2^{32}.
- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.
- An ip address is divided into two parts:
    - **Network ID**: It represents the number of networks.
    - **Host ID**: It represents the number of hosts.
- Two types of addressing – Classful and Classless.

Classful Addressing

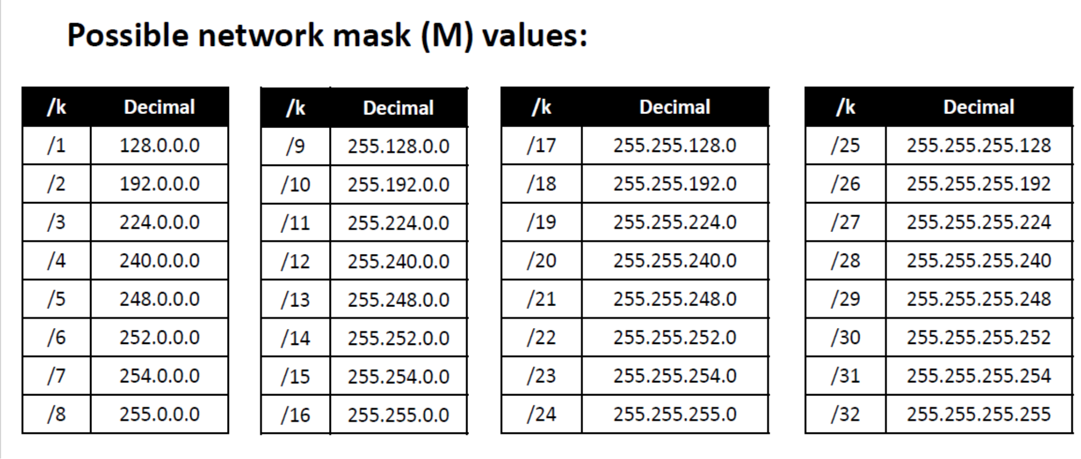
- An IP address is divided into sub-classes:



	NETWORK ID (in bits)	HOST ID (in bits) [N]	Total no. of host ($2^N – 2$)	Range
CLASS A	8	24	2^{24} - 2	0.0.0.0 to 127.255.255.255
CLASS B	16	16	2^{16} – 2	128.0.0.0 to 191.255.255.255
CLASS C	24	8	2^8 – 2	192.0.0.0 to 223.255.255.255
CLASS D	Not Defined			224.0.0.0 to 239.255.255.255
CLASS E	Not Defined			240.0.0.0 to 255.255.255.255

Classless Addressing

- Classless Addressing is an improved IP Addressing system.
- It makes the allocation of IP Addresses more efficient.
- It replaces the older classful addressing system based on classes.
- It is also known as Classless Inter Domain Routing (CIDR).
- CIDR IP Addresses look like – **a.b.c.d / n**
  - They end with a slash followed by a number called as IP network prefix or netmask.
  - IP network prefix tells the number of bits used for the identification of network.
  - Remaining bits are used for the identification of hosts in the network.
  - An example of CIDR IP Address is – **182.0.1.2 / 28**
    - 28 bits are used for the identification of network.
    - Remaining 4 bits are used for the identification of hosts in the network.



Possible network mask (M) values:

/k	Decimal	/k	Decimal	/k	Decimal	/k	Decimal
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

ICMP of IP Technology

What is ICMP (Internet Control Message Protocol)?

ICMP is a transport level protocol within TCP/IP which communicates information about network connectivity issues back to the source of the compromised transmission. It sends control messages such as destination network unreachable, source route failed, and source quench. It uses a data packet structure with an 8-byte header and variable-size data section.

ICMP and Ping

Ping is a utility which uses ICMP messages to report back information on network connectivity and the speed of data relay between a host and a destination computer. It's one of the few instances where a user can interact directly with ICMP, which typically only functions to allow networked computers to communicate with one another automatically.

Basic aspects of the routing and characterization of the routing categories

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

There are 3 types of routing:

Default Routing

Static routing – Static routing is a process in which we have to manually add routes in routing table. i.e., the IP is FIXED.

- Advantages:
  - No routing overhead for router CPU which means a cheaper router can be used to do routing.
  - It adds security because only administrator can allow routing to particular networks only.
  - No bandwidth usage between routers.
- Disadvantage:
  - For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
  - The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Dynamic Routing – Most routers use dynamic routing. The routers should have the same dynamic protocol running in order to exchange routes. When a router finds a change in the topology then router advertises it to all other routers.

- Advantages:
  - Easy to configure.
  - More effective at selecting the best route to a destination remote network and also for discovering remote network.
- Disadvantage:
  - Consumes more bandwidth for communicating with other neighbors.
  - Less secure than static routing.

See video - https://www.coursera.org/lecture/computer-networking/basic-routing-concepts-eCwJA (from time 1:40)

TCP and UDP mechanisms

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

UDP stands for User Datagram Protocol (A datagram is a transfer unit associated with a packet-switched network). The UDP protocol works almost similar to TCP, but it throws all the error-checking stuff out, all the back-and-forth communication and deliverability.

How TCP work?

A TCP connection is established with the help of three-way handshake. It is a process of initiating and acknowledging a connection. Once the connection is established, data transfer begins, and when the transmission process is finished, the connection is terminated by the closing of an established virtual circuit.

How UDP work?

UDP uses a simple transmission method without implied hand-shaking dialogues for ordering, reliability, or data integrity. UDP also assumes that error checking and correction is not important or performed in the application, to avoid the overhead of such processing at the network interface level. It is also compatible with packet broadcasts and multicasting.

KEY DIFFERENCES:

- TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol.
- The speed for TCP is slower while the speed of UDP is faster
- TCP uses handshake protocol like SYN, SYN-ACK, ACK while UDP uses no handshake protocols
- TCP does error checking and also makes error recovery, on the other hand, UDP performs error checking, but it discards erroneous packets.
- TCP has acknowledgment segments, but UDP does not have any acknowledgment segment.
- TCP is heavy-weight, and UDP is lightweight.

When to use UDP and TCP?

TCP

- File transfer
- HTTP
- Real life analogy - TCP is mailing a letter with a return receipt at the post office, except that the post master will organize the letters in-order-of mailing and only deliver them in-order.

UDP

- Call (Voice) over the Internet (VoIP)
- Media streaming (lost frames are ok)
- Real life analogy – UDP is mailing a letter at the post office. No guarantee if the receiver will receive it or not.