Network Programming

On Linux

Prayas Mohanty (Red Hat Certified Instructor)

Red Hat Certification ID: 100-005-594

Objective

- What IP address & why we need it?
- What is Class in IP address?
- What is classless routing & the role of subnet
- How to debug network using tools.
- What is OSI model
- What is the role of Network Layer?
- Why multiple fields in IP header?
- What is Fragmentation & Reassembling
- What is Routing & Forwarding
- Why transport layer?
- Why multiple fields in TCP header?
- What is flow control
- What is multiplexing
- What is 3-way handshake data exchange
- What is Internet Protocol Suite.

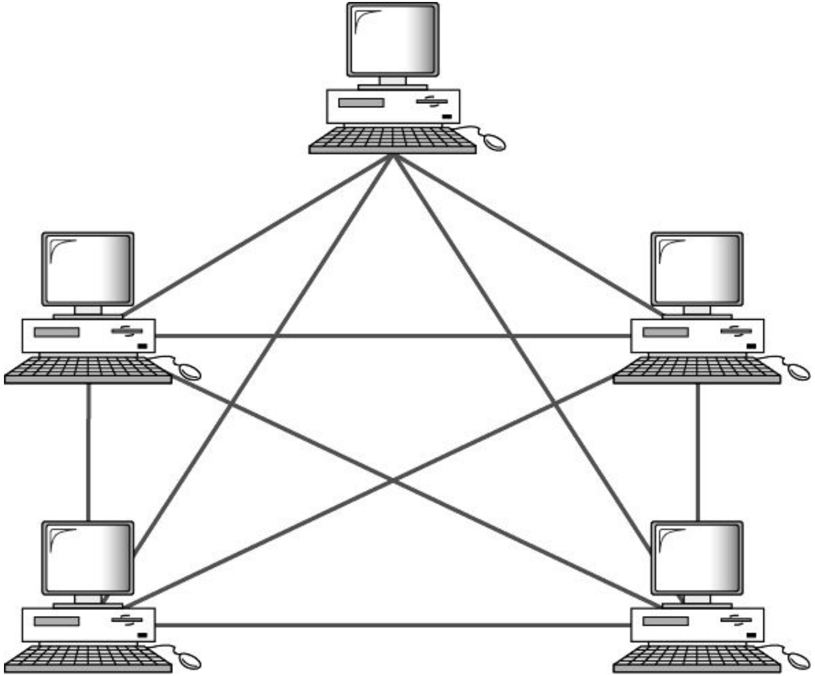
Prerequisite of Participants

- Having Knowledge on Linux Platform
- Having familiarity with Linux Command line
- Basic Knowledge on vi Editor
- Proper Knowledge on C programming
- Basic Knowledge on File Handling in C

What is network Programming

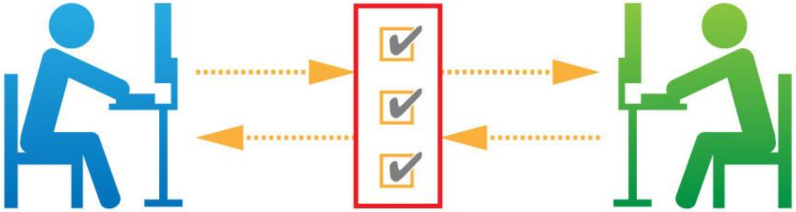
- Computer network programming involves writing computer programs that enable processes to communicate with each other across a computer network.
- With networks, a single program can retrieve information stored in millions of computers located anywhere in the world.
- A single program can communicate with tens of millions of people.
- A single program can harness the power of many computers to work on one problem.

What is Network



- Net + Work
- A system of computers interconnected by means of wires or even wireless medium in order to share information or other computing resources is called Network.
- Through Network
  - Create files and store them in one computer, access those files from the other computer(s) connected over the network.
  - Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over network.

What is Network protocols



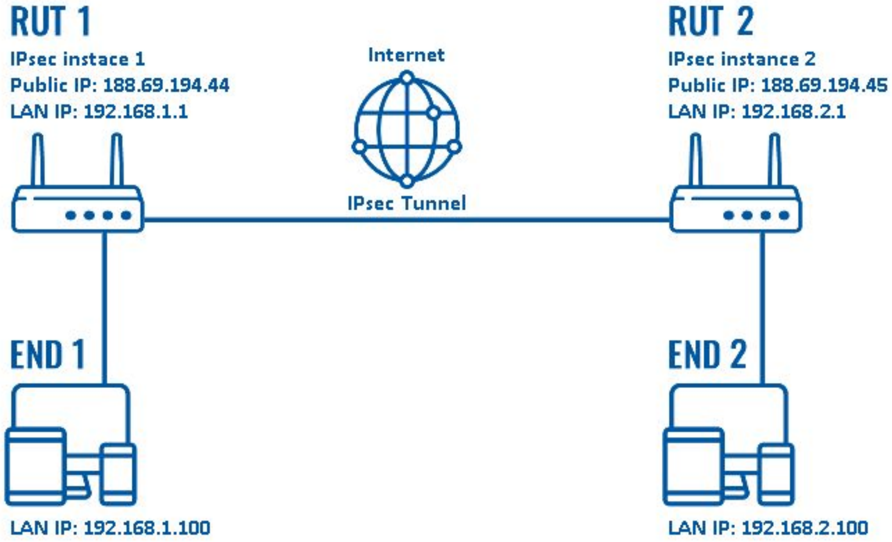
- A network protocol is a set of established rules that dictate how to format, transmit and receive data so that computer network devices, like servers, routers, switches etc can communicate, regardless of the differences in their underlying infrastructures, designs or standards.
- The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods.

Network Vs Internet

Network	Internet
Network is defined as the group of two or more computer systems.	Internet is the interrelationship of a few networks.
The coverage of network is limited in comparison of internet.	While it covers the entire world.
It provides the link between many computers and network-enabled devices.	While it provide connection among many networks.
The types of network are: LAN, MAN, WAN.	Whereas the types of internet is Intranet, Extranet & Internet.
It requires less number of hardware devices.	While it requires various hardware devices.

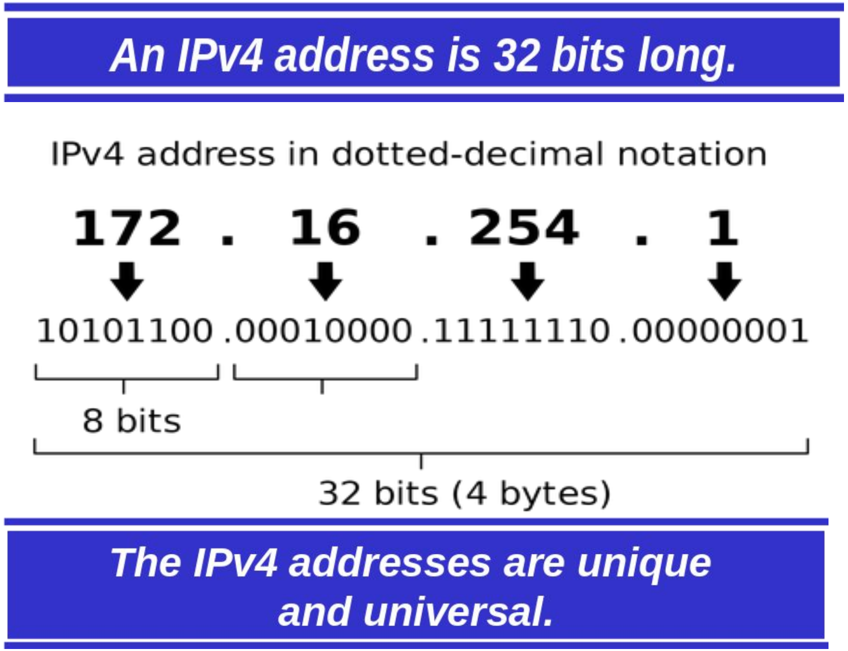
- The basic distinction between network and internet is that the Network consists of pcs that area unit physically connected and may be used as a private computer yet on share data with one another.
- Conversely, the Internet could be a technology that links these little and huge networks with one another and builds a additional in depth network.

Internet Protocols



- The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place.
- Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

What is IP address

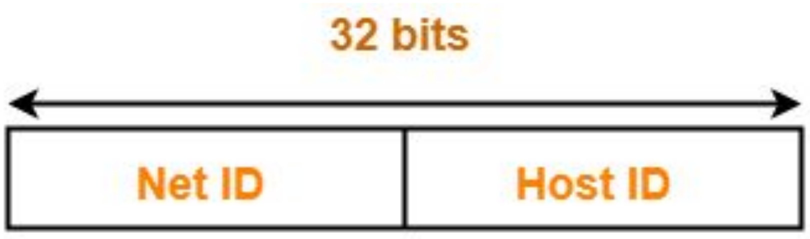


An IPv4 address is 32 bits long.

The IPv4 addresses are unique and universal.

- An Internet Protocol address is a binary label attached to each computers / network devices that is connected to a computer network that uses the Internet Protocol for communication.
    - Addresses in IPv4 are 32-bits long.
    - Addresses in IPv6 are 128-bits long.
- An IPv4 address is typically expressed in dotted-decimal notation, with every eight bits (octet) represented by a number from zero to 255, each separated by a dot.

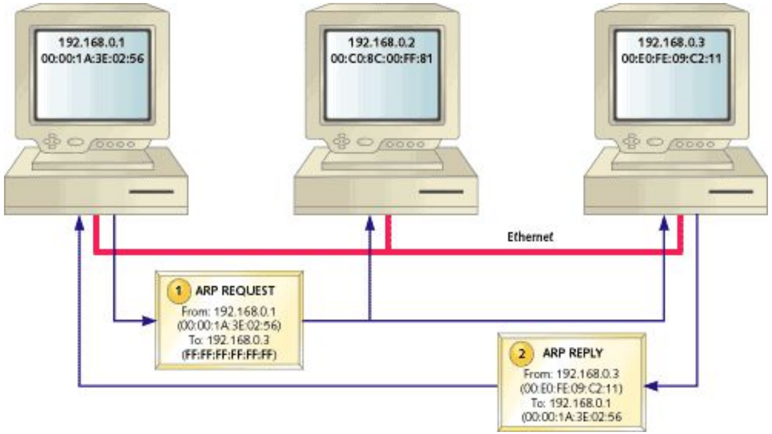
Why IP address



Format of an IP Address

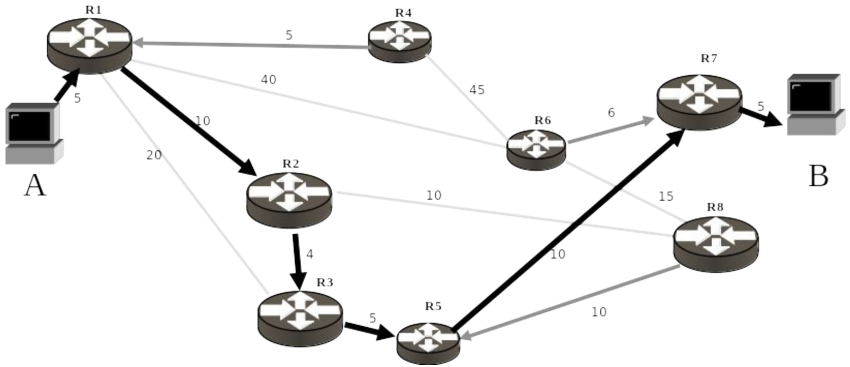
- The purpose of an IP address is to handle the connection between devices that send and receive information across internet.
- Why do you need to know the telephone number of the person you want to call, before you can place a phone call to that person ?
    - That same logic can be applied to the need for IP addresses.
- An IP address serves two primary functions.
    - It is used as an identification for network.
    - It also used to serve identification for node.

Node(host) to Node(host) Delivery



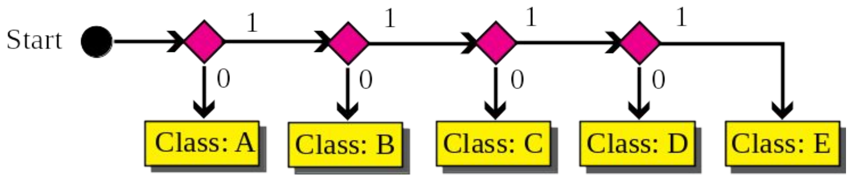
- Ethernet communication depend on a unique 48 bit hardware dependent address call MAC address.
    - MAC address are not used by any users.
    - They uses IP address instated
    - Before sending an IPv4 packet, the sender sends a broadcast message onto the LAN using ARP in order to discover the Ethernet MAC address of an interface that is listening for that desired target IPv4 address.
    - If operational, an appropriate unit will reply that it has a network interface with a certain MAC address that is associated with the IPv4 address in question.
    - The original sender now has the information needed and can send its IPv4 packet to the destination, inserting it into an Ethernet frame with the correct destination MAC address for the appropriate recipient.

Network to Network Delivery



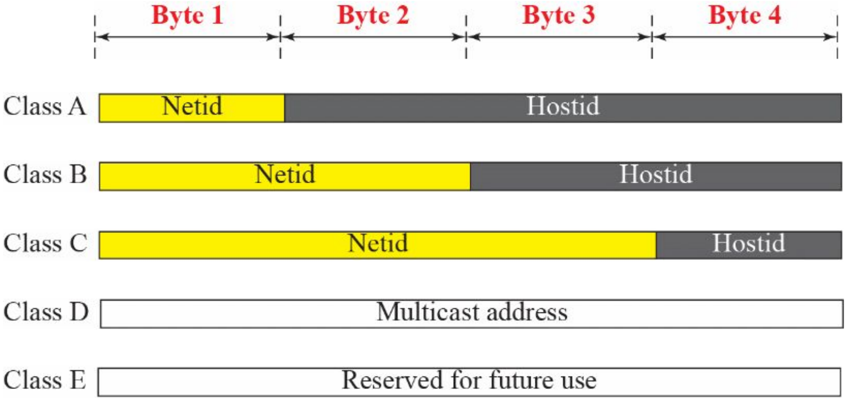
- All network have a single entry & exit point called gateway controlled by a router.
- Routers examine a packet’s destination and determine the best path by enlisting the aid of a routing table
- Each router makes a LOCAL decision call routing to forward the packet towards B.
- They uses 2 type routing methods using netid part of IP address which are:
  - Classfull routing
  - Classless routing

Classfull Routing



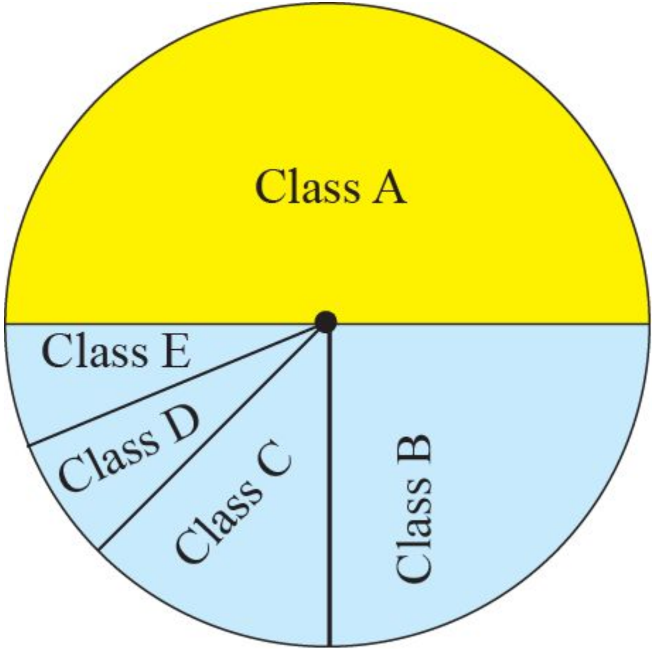
- A classful network is a network addressing architecture used in the Internet from 1981.
- The method divides the IP address space for Internet Protocol version 4 into five address classes based on the leading four address bits.
- In 1993, a new architecture, called classless addressing, was introduced that supersedes the original architecture.
    - In this section, we introduce classful addressing because it paves the way for understanding classless addressing and justifies the rationale for moving to the new architecture.

What is An IP Class

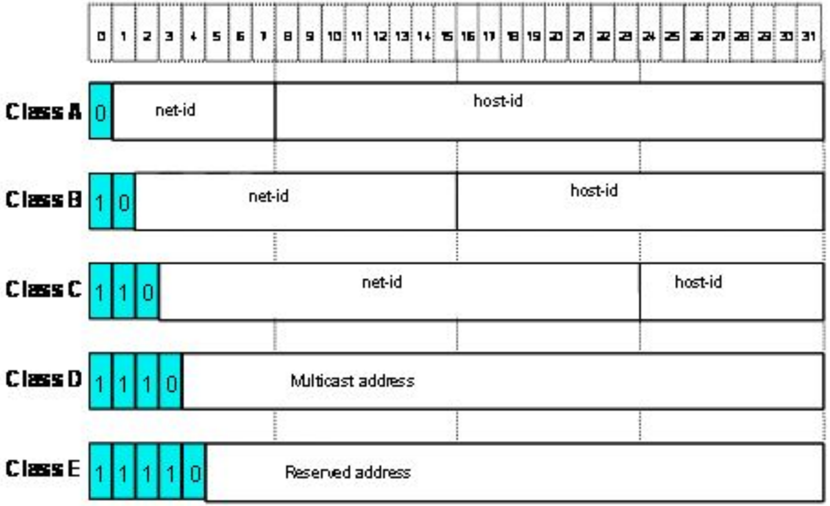


- This addressing method divides the IP address into five separate classes based on four address bits.
- Classes A, B, C offers addresses for networks of three distinct network sizes.
  - Class A for Big Networks (3 byte for hostid)
  - Class B for Moderate Networks (2 byte for hostid)
  - Class C for Small Networks (1 byte for hostid)
- Class D is only used for multicast.
- Class E reserved exclusively for experimental purposes.

Class Wise IP Allocation

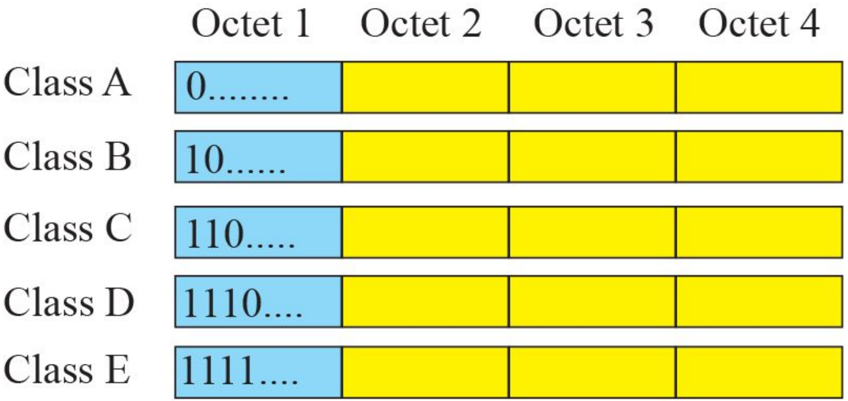


0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Class A 0 net-id host-id
Class B 1 0 net-id host-id
Class C 1 1 0 net-id host-id
Class D 1 1 1 0 Multicast address
Class E 1 1 1 1 0 Reserved address

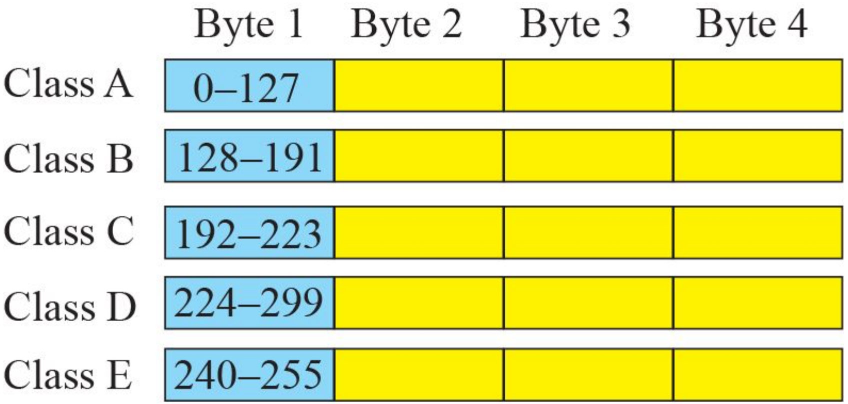
net-id: Network ID; host-id: Host ID

Determining Class from IP Address



	Octet 1	Octet 2	Octet 3	Octet 4
Class A	0........			
Class B	10......			
Class C	110.....			
Class D	1110....			
Class E	1111....			

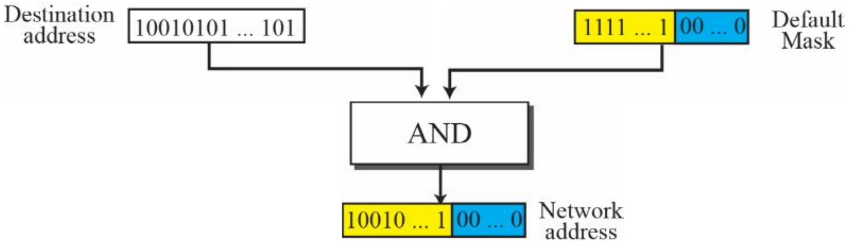
Binary notation



	Byte 1	Byte 2	Byte 3	Byte 4
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–299			
Class E	240–255			

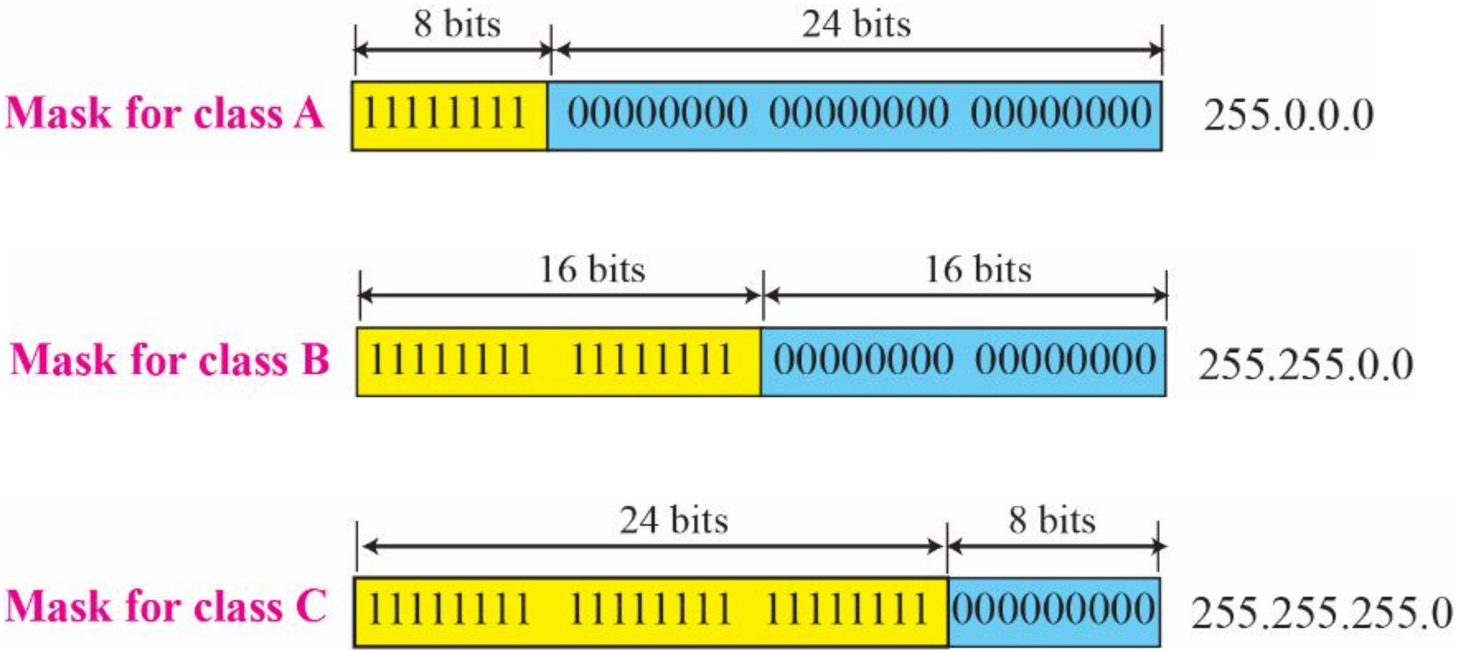
Dotted-decimal notation

Classless Inter-Domain Routing



- This type of routing does not depend upon it's class to determine network id.
- In order to find network id of the destination ip address it uses a mask also known as subnet mask.
  - It is also a 32 bit number, containing 0's and 1's. Here network id part is represented by all 1's and host ID part is represented by all 0's.
  - This mask is bitwise processed with an AND operation to produce a network ID.
  - This mask is also called subnet mask as it has the capacity to divide a network to many subnetwork.

Default Subnet Mask



8 bits | 24 bits

Mask for class A 11111111 00000000 00000000 00000000 255.0.0.0

16 bits | 16 bits

Mask for class B 11111111 11111111 00000000 00000000 255.255.0.0

24 bits | 8 bits

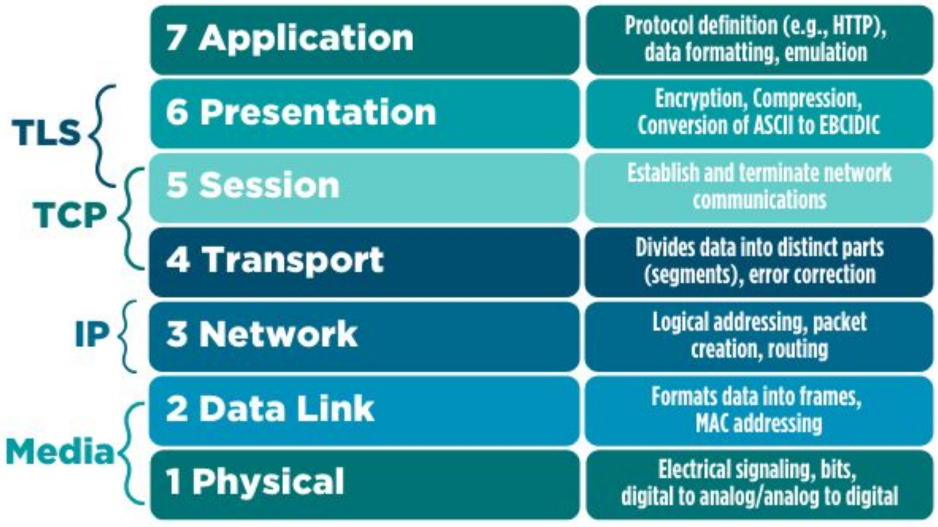
Mask for class C 11111111 11111111 11111111 000000000 255.255.255.0

Network tools to debug and monitor networks

- Ifconfig
  - Monitor & configure a network interface.
- ping
  - To debug connection problems by monitoring Round-trip times and packet loss statistics.
- traceroute
  - It tracks the route packets taken from an IP network on their way to a given host.
- netstat
  - Netstat prints information about the Linux networking subsystem which may includes network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
- tshark/wireshark
  - Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Overview of OSI model

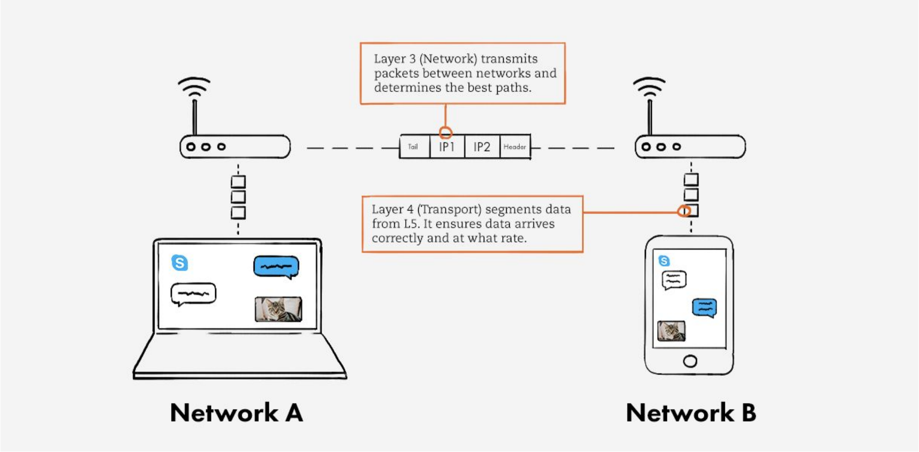
- In the year 1983 ISO formulated a standard for multivendor network, the result is OSI (Open System Interconnect) Model.
- According to this model all the Networking Operating Systems consist of Seven Layers.
  - Application Layer
  - Presentation Layer
  - Session Layer
  - Transport Layer
  - Network Layer
  - Data link Layer
  - Physical Layer



	7 Application	Protocol definition (e.g., HTTP), data formatting, emulation
TLS	6 Presentation	Encryption, Compression, Conversion of ASCII to EBCIDIC
TCP	5 Session	Establish and terminate network communications
	4 Transport	Divides data into distinct parts (segments), error correction
IP	3 Network	Logical addressing, packet creation, routing
Media	2 Data Link	Formats data into frames, MAC addressing
	1 Physical	Electrical signaling, bits, digital to analog/analog to digital

Role of network layer

- The primary function of the network layer is to enable different networks to be interconnected. It does this by forwarding packets to network routers, which rely on algorithms to determine the best paths for the data to travel.
- The network layer has two main functions.
  - One is breaking up segments into network packets, and reassembling the packets on the receiving end.
  - The other is routing packets by discovering the best path across a physical network.
  - This layer also assigns source and destination IP addresses to the data segments.

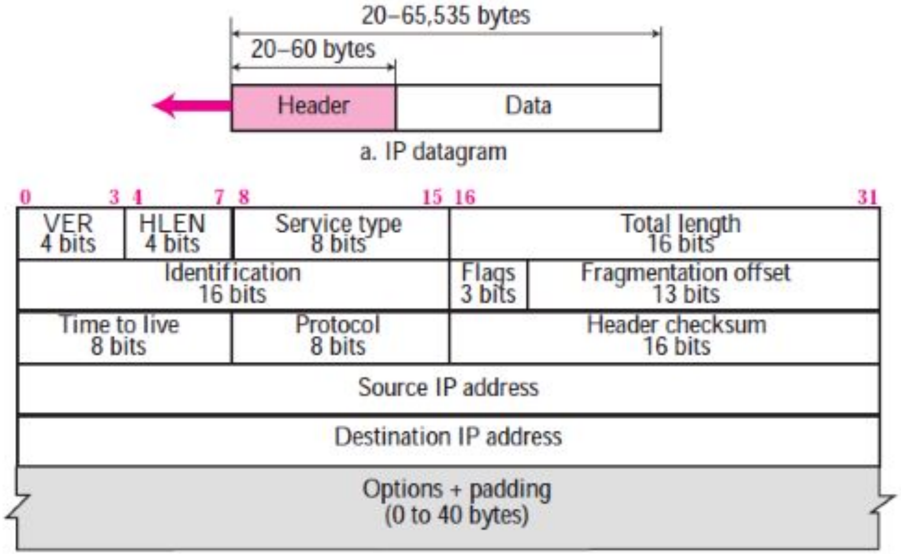


Layer 3 (Network) transmits packets between networks and determines the best paths.

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

Why multiple fields in IP header?

- The header contains information about IP version, source IP address, destination IP address, time-to-live, etc.
- IPV4 header format is of 20 to 60 bytes in length, contains information essential to routing and delivery, consist of 13 fields.
- Source and Destination IPv4 Address fields are the most important fields of IPv4 header.
- The Protocol field is used to identify the upper-layer protocol that is to receive the IPv4 packet payload that may be TCP or UDP.



a. IP datagram

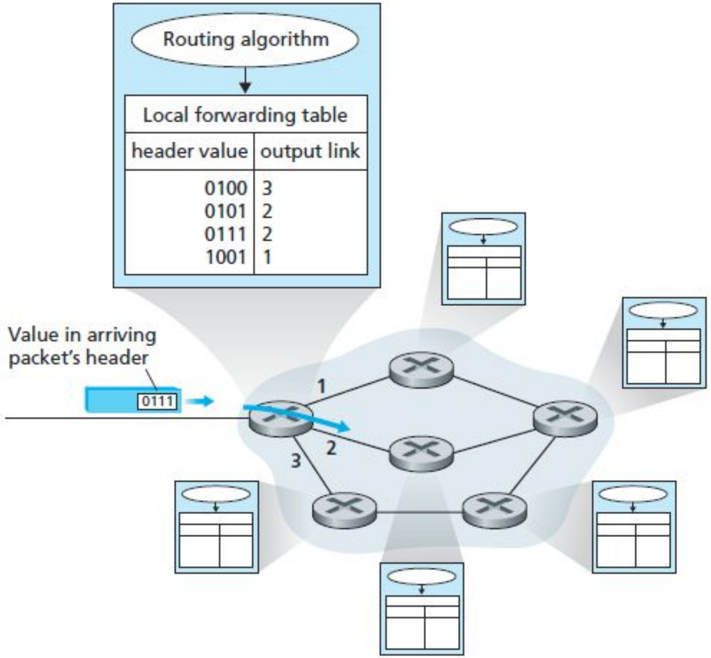
b. Header format

Fragmentation and reassembly

- Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held in a frame (MTU).
- The network layer divides the datagram received from the transport layer into fragments so that data flow is not disrupted.
- Fields in IP header for fragmentation –
    - Identification (16 bits) – use to identify fragments of the same frame.
    - Fragment offset (13 bits) – use to identify the sequence of fragments in the frame. It generally indicates a number of data bytes preceding or ahead of the fragment.
    - More fragments (MF Flag = 1 bit): if MF = 1, more fragments are ahead of this fragment and if MF = 0, it is the last fragment.
    - Don't fragment (DF Flag = 1 bit): If we don't want the packet to be fragmented then DF = 1.
- Reassembly of Fragments takes place only at the destination and not at routers since packets take an independent path(datagram packet switching), so all may not meet at a router and hence a need of fragmentation may arise again. The fragments may arrive out of order also.
- Algorithm used for Reassemble:
    - Destination should identify that datagram is fragmented from MF, Fragment offset field.
    - Destination should identify all fragments belonging to same datagram from Identification field.
    - Identify the 1st fragment(offset = 0).
    - Identify subsequent fragments using header length, fragment offset.
    - Repeat until MF = 0.

Routing and Forwarding

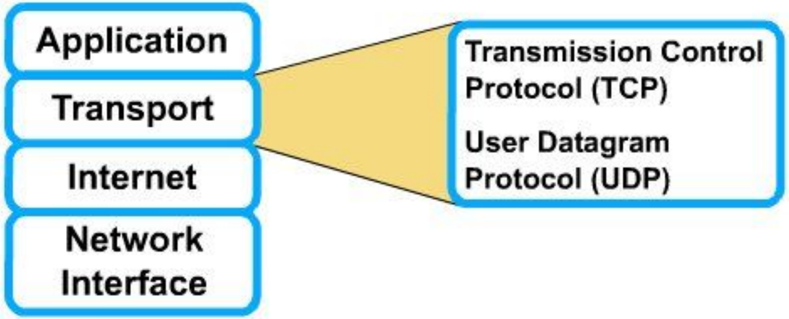
- Routing gains all the information that data needs to reach its endpoint whereas forwarding is the active movement of the data to its best possible path.
    - Forwarding refers to the router-local action of transferring packet from an input link interface to the appropriate output link interface.
    - Routing refers to the network-wide process that determines the end-to-end paths that packets take from source to destination.
- Both are activities that take place at a router in the Network Layer.



Local forwarding table	
header value	output link
0100	3
0101	2
0111	2
1001	1

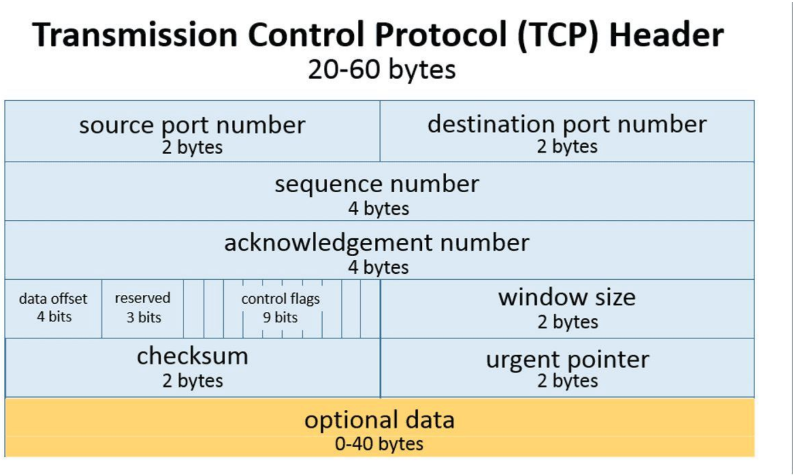
Why transport layer?

- The basic function of the Transport layer is to accept data from the session layer, split it up into smaller units if need be, pass these to the Network layer, and ensure that all the pieces arrive correctly at the other end.
- Transport layer provides the communication services directly to the application processes running on different hosts.
- Responsibilities of the transport layer includes:
  - Segmenting data at the source and reassembling the data at the destination
  - Identifying the proper application for each communication stream through the use of port numbers.
  - Multiplexing the communications


Application
Transport
Internet
Network Interface
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)

Why multiple fields in TCP header?

- TCP (Transmission Control Protocol) is a reliable transport protocol as it establishes a connection before sending any data and everything that it sends is acknowledged by the receiver.
- TCP wraps each data packet with a header containing 10 mandatory fields totaling 20 to 60 bytes, followed by data from the application program.
- Each header holds information about the connection and the current data being sent.



Transmission Control Protocol (TCP) Header
20-60 bytes

source port number
2 bytes

destination port number
2 bytes

sequence number
4 bytes

acknowledgement number
4 bytes

data offset
4 bits

reserved
3 bits

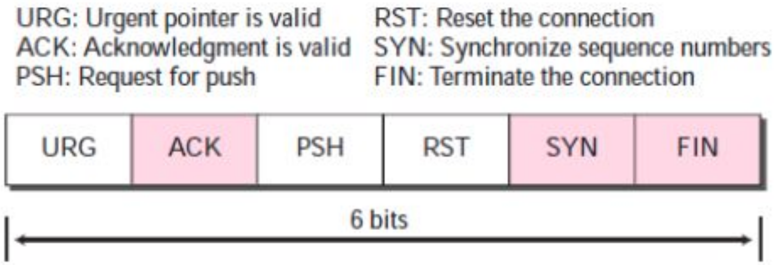
control flags
9 bits

window size
2 bytes

checksum
2 bytes

urgent pointer
2 bytes

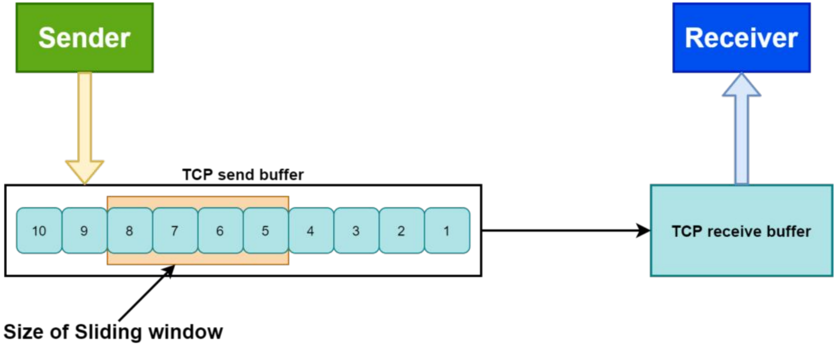
optional data
0-40 bytes



URG: Urgent pointer is valid
ACK: Acknowledgment is valid
PSH: Request for push
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection

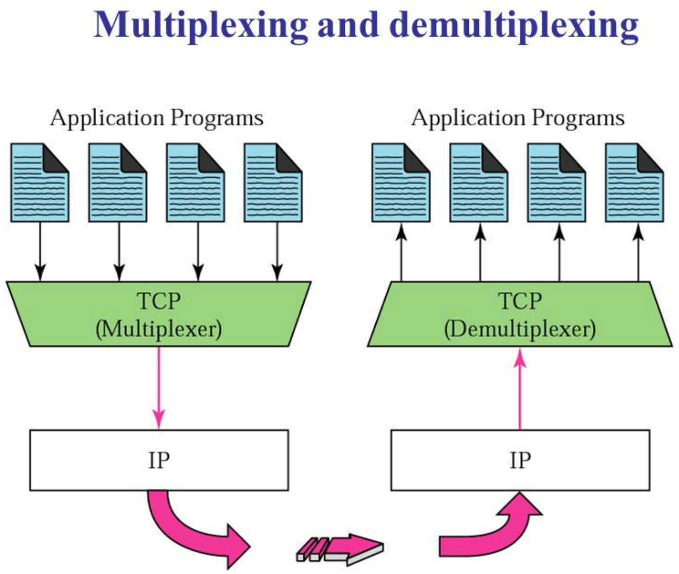
Flow Control

- Flow control deals with the amount of data sent to the receiver side without receiving any acknowledgment.
- It makes sure that the receiver will not be overwhelmed with data.
- It's a kind of speed synchronization process between the sender and the receiver.
- Transmission Control Protocol (TCP) uses a sliding window for flow control.
    - The TCP sliding window determines the number of unacknowledged bytes, x, that one system can send to another. Two factors determine the value of x:
        - The size of the send buffer on the sending system.
        - The size and available space in the receive buffer on the receiving system.



Multiplexing & Demultiplexing

- Multiplexing is the process of collecting the data from multiple application processes of the sender, enveloping that data with headers and sending them as a whole to the intended receiver.
- Delivering the received segments at the receiver side to the correct app layer processes is called demultiplexing.
- The main objective of multiplexing and demultiplexing is to allow us to use a multitude of applications simultaneously.

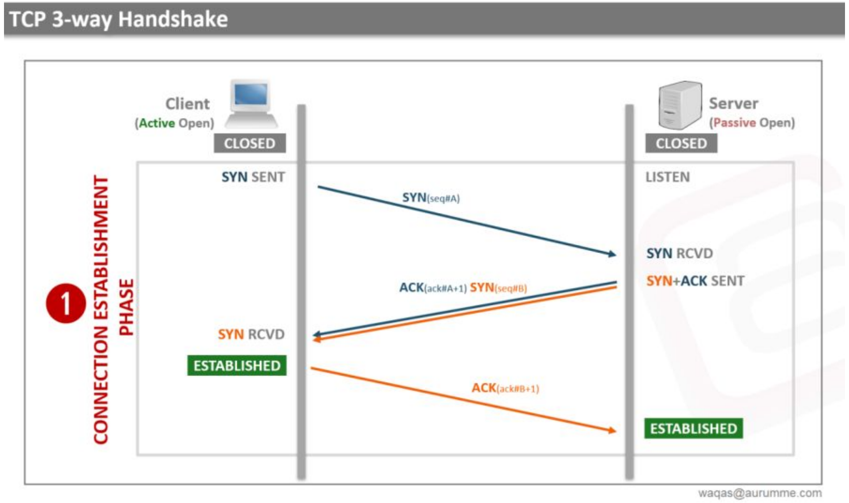


3 way Handshaking

- The 3-Way Handshake process is the defined set of steps that takes place in the TCP for creating a secure and reliable communication link and also closing it.

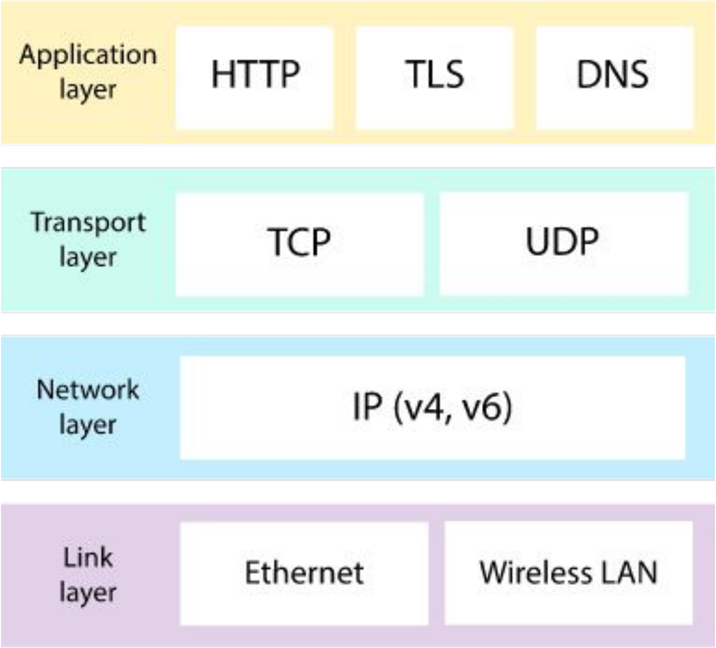
- A three-way handshake is also known as a SYN-SYN-ACK, and requires both the client and server to exchange (synchronization) SYN and ACK (acknowledgment) packets before actual data communication begins.

- Transmission Control Protocol (TCP) provides a secure and reliable connection between two devices using the 3-way handshake process.

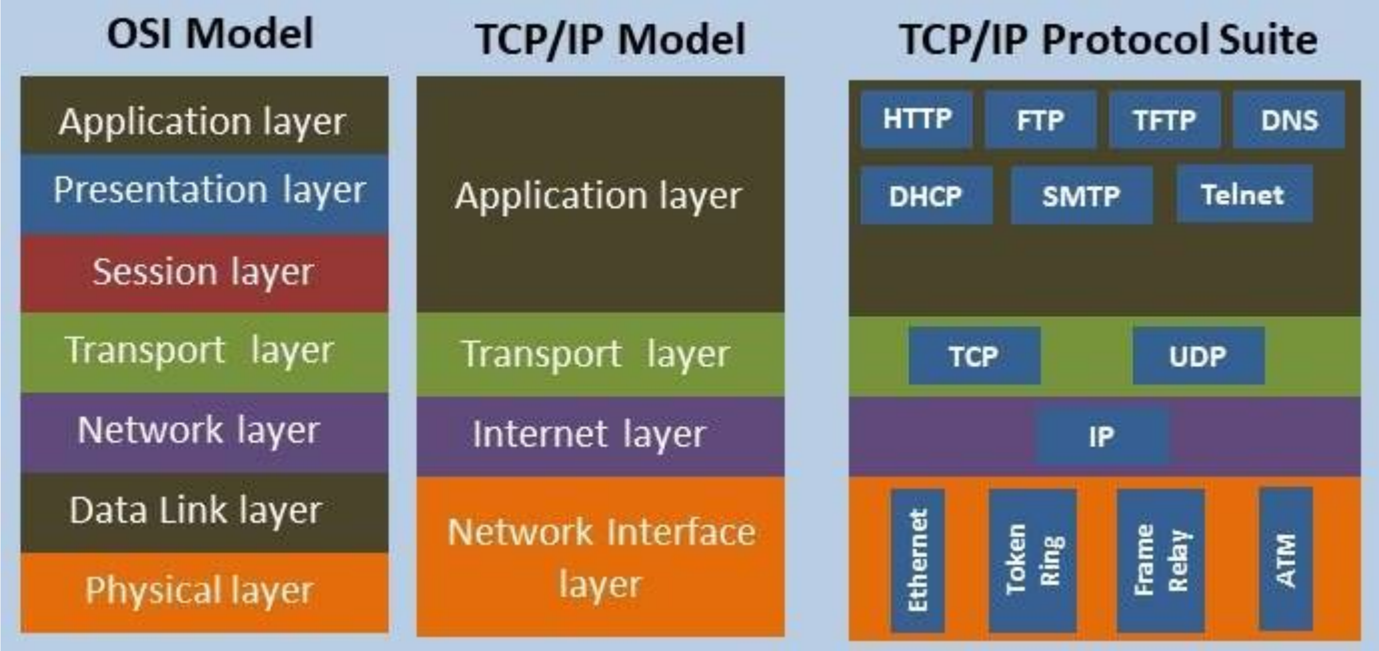


Internet protocol suite

- The Internet protocol suite, commonly known as TCP/IP, is the set of communications protocols used in the Internet and similar computer networks.
- Internet Protocol suite (IP suite) is the standard network model and communication protocol stack used on the Internet and on most other computer networks.
- The current foundational protocols in the suite are the Transmission Control Protocol and the Internet Protocol, as well as the User Datagram Protocol.



Internet protocol suite Vs OSI



OSI Model

Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data Link layer
Physical layer

TCP/IP Model

Application layer
Transport layer
Internet layer
Network Interface layer

TCP/IP Protocol Suite

HTTP FTP TFTP DNS
DHCP SMTP Telnet
TCP UDP
IP
Ethernet Token Ring Frame Relay ATM

Summary

- What IP address & why we need it?
- What is Class in IP address?
- What is classless routing & the role of subnet
- How to debug network using tools.
- What is OSI model
- What is the role of Network Layer?
- Why multiple fields in IP header?
- What is Fragmentation & Reassembling
- What is Routing & Forwarding
- Why transport layer?
- Why multiple fields in TCP header?
- What is flow control
- What is multiplexing
- What is 3-way handshake data exchange
- What is Internet Protocol Suite.

Any Questions ?

Thank you!