CMR INSTITUTE OF TECHNOLOGY

* UGC AUTONOMOUS *

* Approved by AICTE * Accredited by NAAC with 'A' Grade * All B.Tech programs Accredited by NBA*

(Kandlakoya (v),Medchal Road,Hyderabad - 501 401)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

II – B.Tech – II – Sem (CSE ‘C’ & CSE – DS ‘A’)

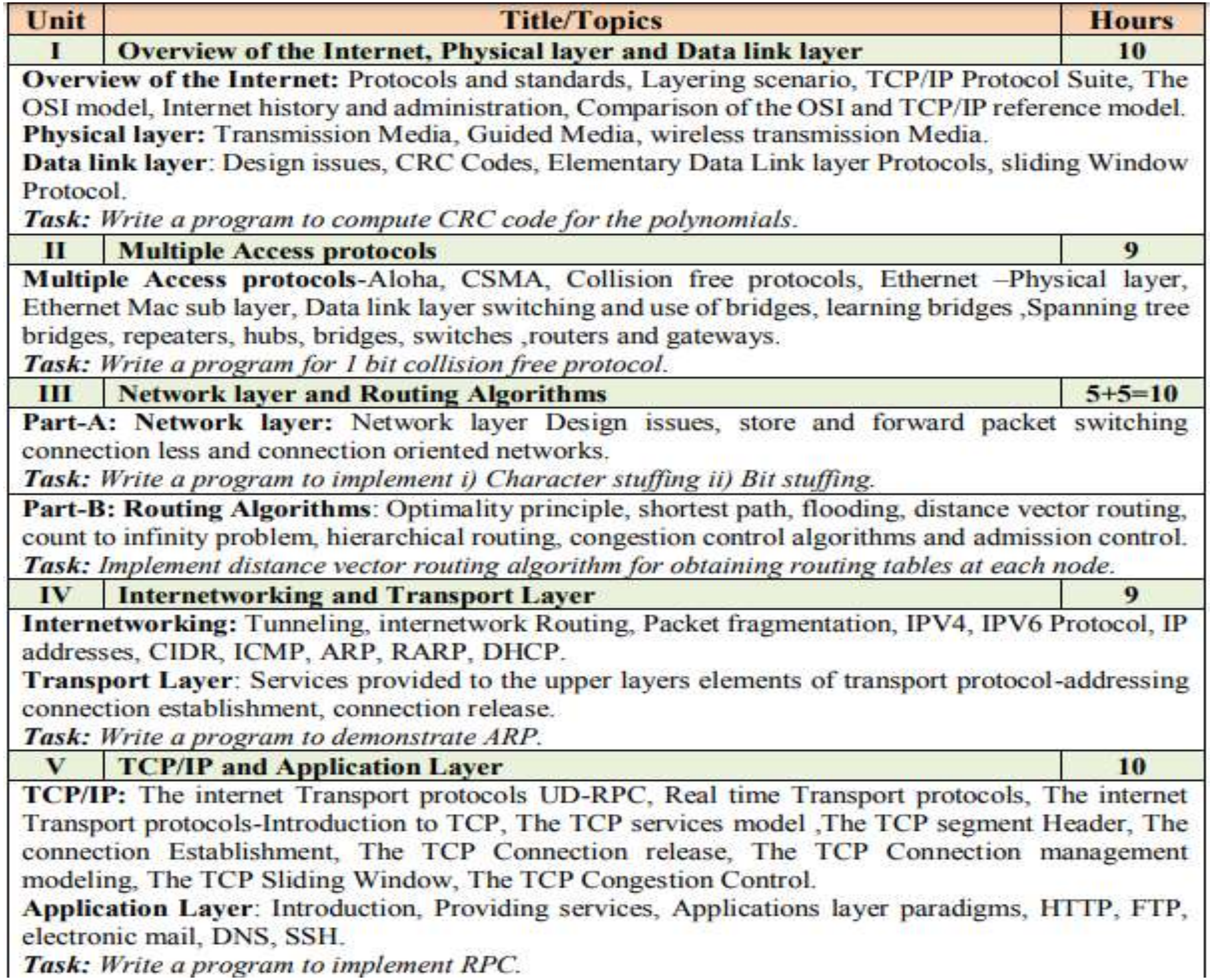
COMPUTER NETWORKS (20-CS-PC-224)
(R20 Regulations)

By

Dr.A.Nirmal Kumar

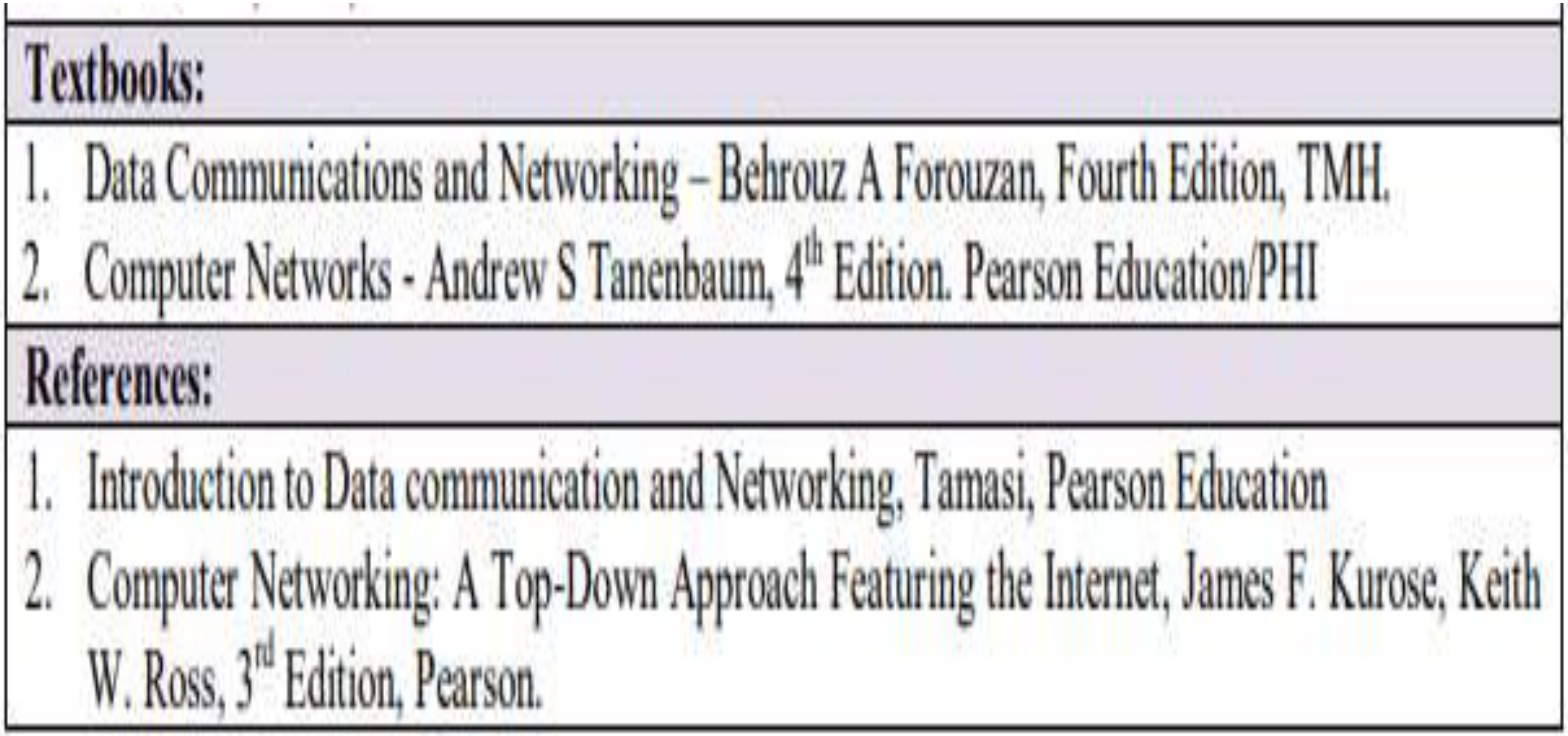
COMPUTER NETWORKS

SYLLABUS



Unit	Title/Topics	Hours
I	**Overview of the Internet, Physical layer and Data link layer**	10
	Overview of the Internet: Protocols and standards, Layering scenario, TCP/IP Protocol Suite, The OSI model, Internet history and administration, Comparison of the OSI and TCP/IP reference model. **Physical layer:** Transmission Media, Guided Media, wireless transmission Media. **Data link layer**: Design issues, CRC Codes, Elementary Data Link layer Protocols, sliding Window Protocol. ***Task:*** *Write a program to compute CRC code for the polynomials.*	
II	**Multiple Access protocols**	9
	Multiple Access protocols-Aloha, CSMA, Collision free protocols, Ethernet –Physical layer, Ethernet Mac sub layer, Data link layer switching and use of bridges, learning bridges ,Spanning tree bridges, repeaters, hubs, bridges, switches ,routers and gateways. ***Task:*** *Write a program for 1 bit collision free protocol.*	
III	**Network layer and Routing Algorithms**	5+5=10
	Part-A: Network layer: Network layer Design issues, store and forward packet switching connection less and connection oriented networks. ***Task:*** *Write a program to implement i) Character stuffing ii) Bit stuffing.*	
	Part-B: Routing Algorithms: Optimality principle, shortest path, flooding, distance vector routing, count to infinity problem, hierarchical routing, congestion control algorithms and admission control. ***Task:*** *Implement distance vector routing algorithm for obtaining routing tables at each node.*	
IV	**Internetworking and Transport Layer**	9
	Internetworking: Tunneling, internetwork Routing, Packet fragmentation, IPV4, IPV6 Protocol, IP addresses, CIDR, ICMP, ARP, RARP, DHCP. **Transport Layer**: Services provided to the upper layers elements of transport protocol-addressing connection establishment, connection release. ***Task:*** *Write a program to demonstrate ARP.*	
V	**TCP/IP and Application Layer**	10
	TCP/IP: The internet Transport protocols UD-RPC, Real time Transport protocols, The internet Transport protocols-Introduction to TCP, The TCP services model ,The TCP segment Header, The connection Establishment, The TCP Connection release, The TCP Connection management modeling, The TCP Sliding Window, The TCP Congestion Control. **Application Layer**: Introduction, Providing services, Applications layer paradigms, HTTP, FTP, electronic mail, DNS, SSH. ***Task:*** *Write a program to implement RPC.*	

TEXT BOOKS & REFERENCES



Textbooks:

1. Data Communications and Networking – Behrouz A Forouzan, Fourth Edition, TMH.
2. Computer Networks - Andrew S Tanenbaum, 4th Edition. Pearson Education/PHI

References:

1. Introduction to Data communication and Networking, Tamasi, Pearson Education
2. Computer Networking: A Top-Down Approach Featuring the Internet, James F. Kurose, Keith W. Ross, 3rd Edition, Pearson.

COURSE OUTCOMES

Upon completion of the course, the student will be able

CO 1: To outline the basics of computer networks and various layers **(Unit – I)**

CO 2: To demonstrate multiple access protocols **(Unit – II)**

CO 3: To interpret network layer and routing algorithms (Unit – III)

CO 4: To illustrate internetworking and various transport protocols (Unit – IV)

CO 5: To make use of various protocols of application layer **(Unit – V)**

UNIT – IV

Internetworking: Tunneling, internetwork Routing, Packet fragmentation, IPV4, IPV6 Protocol, IP addresses, CIDR, ICMP, ARP, RARP, DHCP.

Transport Layer: Services provided to the upper layers elements of transport protocol-addressing connection establishment, connection release.

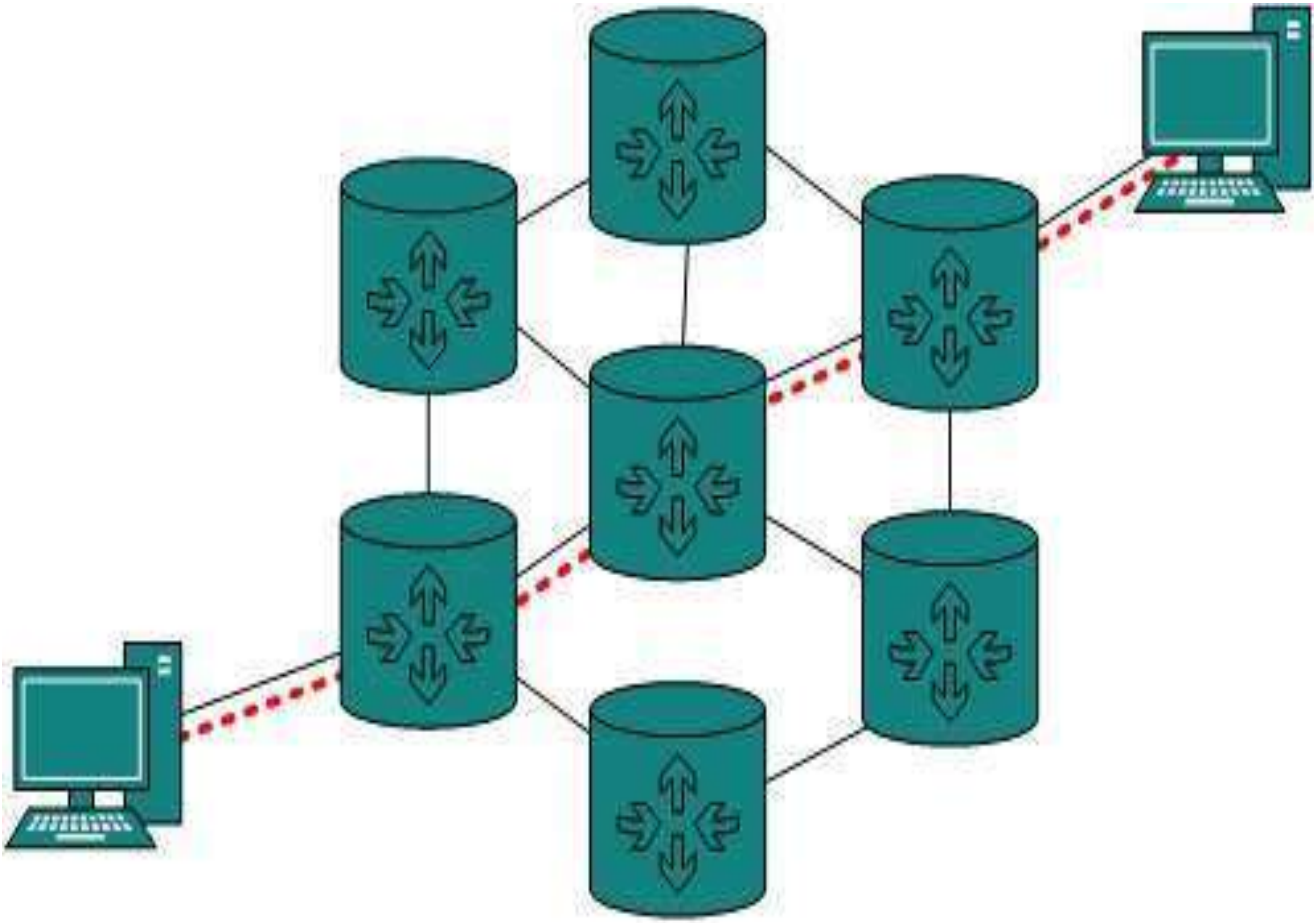
Task: Write a program to demonstrate ARP.

Internetworking

- In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking.
- Networks can be considered different based on various parameters such as, Protocol, topology, Layer-2 network and addressing scheme.

In internetworking, routers have knowledge of each other’s address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

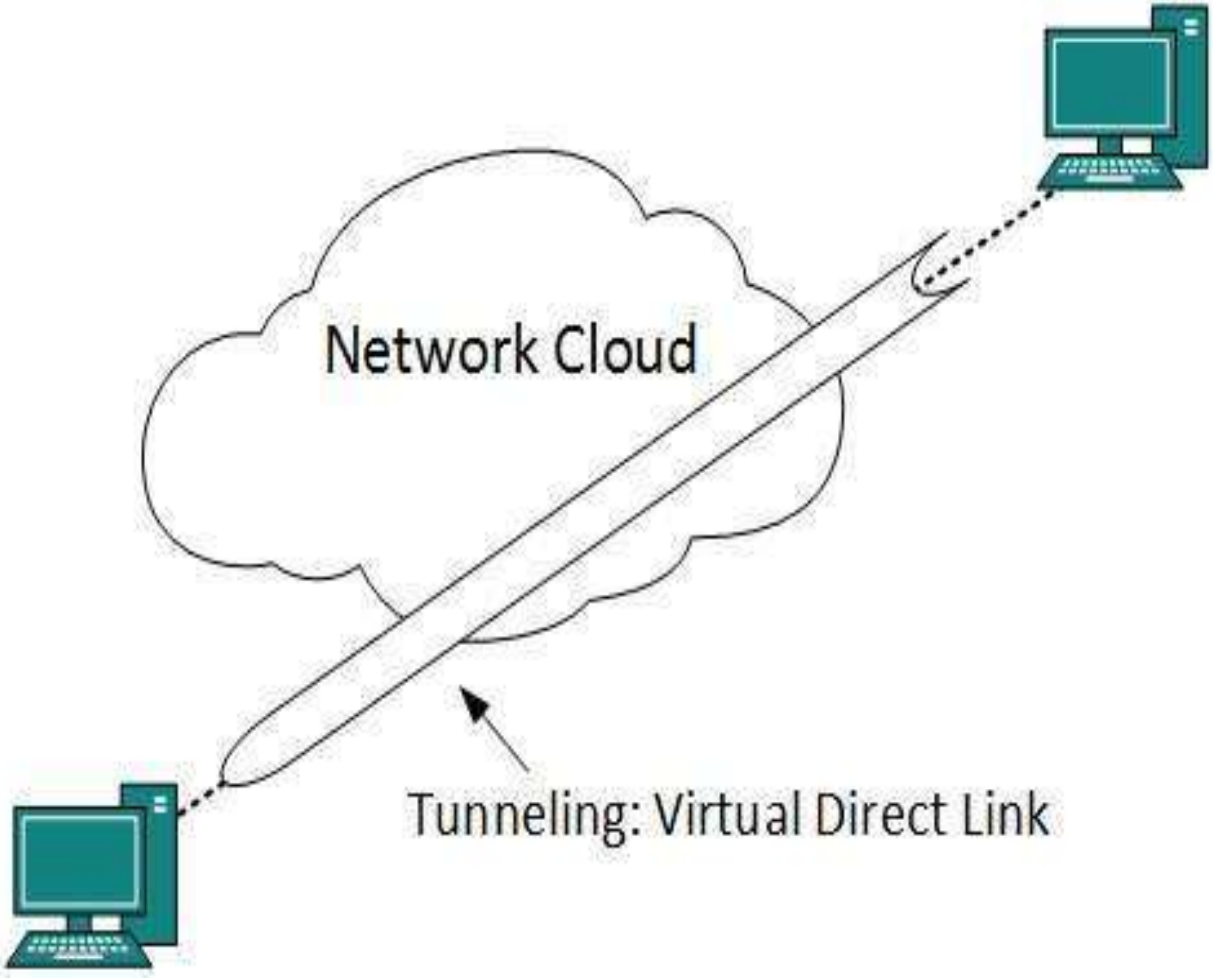
Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP. RIP, OSPF are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.



Tunneling

- If they are two geographically separate networks, which want to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.
- Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.

- When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.
- Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.



Network Cloud
Tunneling: Virtual Direct Link

Packet Fragmentation

- Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.
- If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.

- If a packet with DF (don’t fragment) bit set to 1 comes to a router which can not handle the packet because of its length, the packet is dropped.
- When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way.
- If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

Introduction and IPv4 Datagram Header

The network layer is the third layer (from bottom) in the OSI Model. The network layer is concerned with the delivery of a packet across multiple networks. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. This layer contains hardware devices such as routers, bridges, firewalls, and switches, but it actually creates a logical image of the most efficient communication route and implements it with a physical medium.

Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it. Internet Protocol and Netware IPX/SPX are the most common protocols associated with the network layer.

In the OSI model, the network layer responds to requests from the layer above it (transport layer) and issues requests to the layer below it (data link layer).

Responsibilities of Network Layer:

- ***Packet forwarding/Routing of packets:*** *Relaying of data packets from one network segment to another by nodes in a computer network*
- ***Connectionless communication(IP):*** *A data transmission method used in packet-switched networks in which each data unit is separately addressed and routed based on information carried by it*
- ***Fragmentation of data packets:*** *Splitting of data packets that are too large to be transmitted on the network*

Circuit Switch vs Packet Switch

In circuit switched network, a single path is designated for transmission of all the data packets. Whereas in case of a packet-switched network, each packet may be sent through a different path to reach the destination.

- In a circuit switched network, the data packets are received in order whereas in a packet switched network, the data packets may be received out of order.
- The packet switching is further subdivided into Virtual circuits and Datagram.

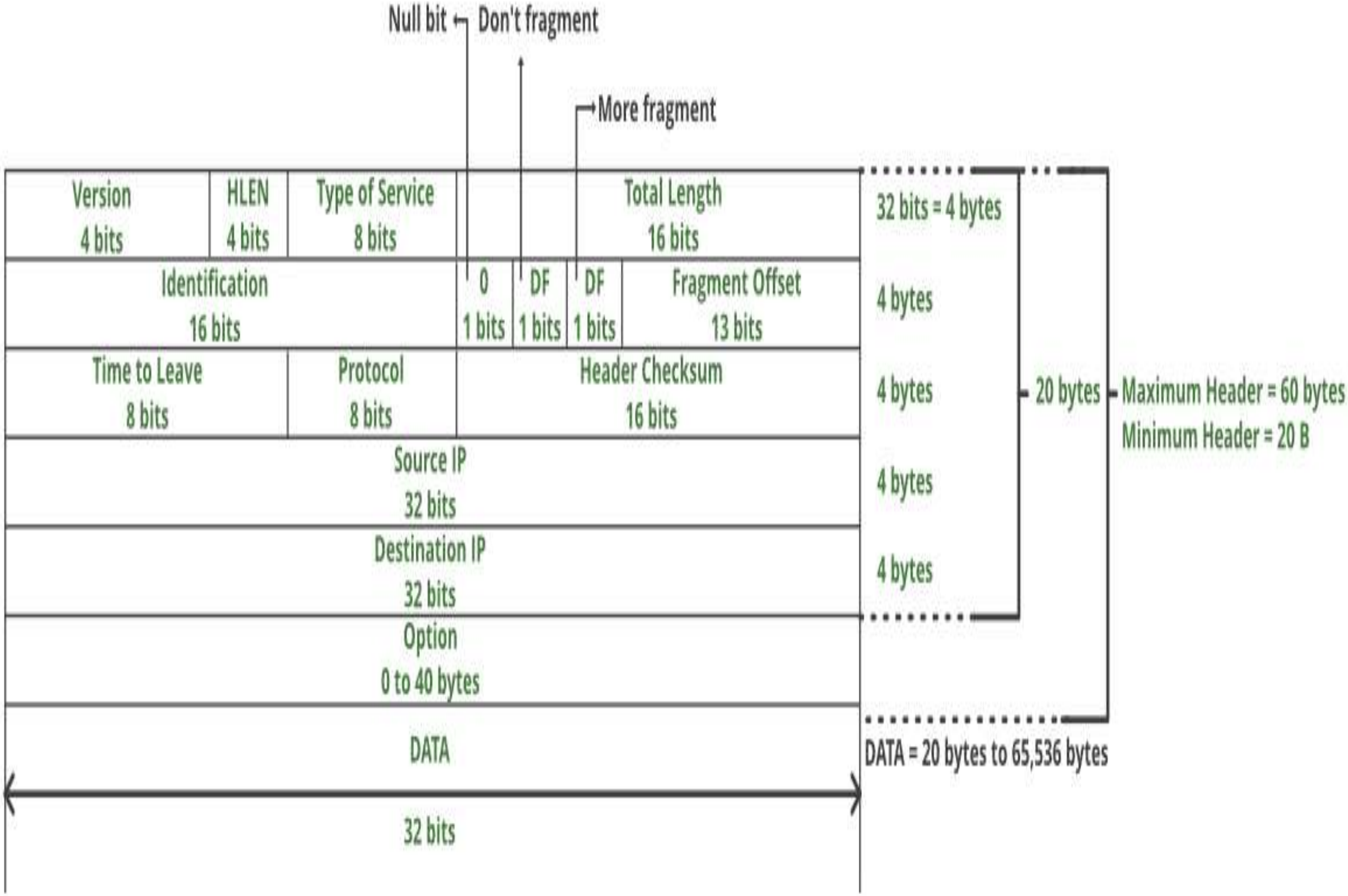
IPv4

IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet.

- It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.
- IPv4 is defined and specified in IETF publication RFC 791.
  IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use.

- IPv4 uses 32-bit (4 byte) addressing, which gives 2^{32} addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.
- **IPv4 Datagram Header**

  Size of the header is 20 to 60 bytes.



Null bit

Don't fragment

More fragment

Version 4 bits

HLEN 4 bits

Type of Service 8 bits

Total Length 16 bits

32 bits = 4 bytes

Identification 16 bits

0 1 bits

DF 1 bits

DF 1 bits

Fragment Offset 13 bits

4 bytes

Time to Leave 8 bits

Protocol 8 bits

Header Checksum 16 bits

4 bytes

20 bytes

Maximum Header = 60 bytes

Minimum Header = 20 B

Source IP 32 bits

4 bytes

Destination IP 32 bits

4 bytes

Option 0 to 40 bytes

DATA

DATA = 20 bytes to 65,536 bytes

32 bits

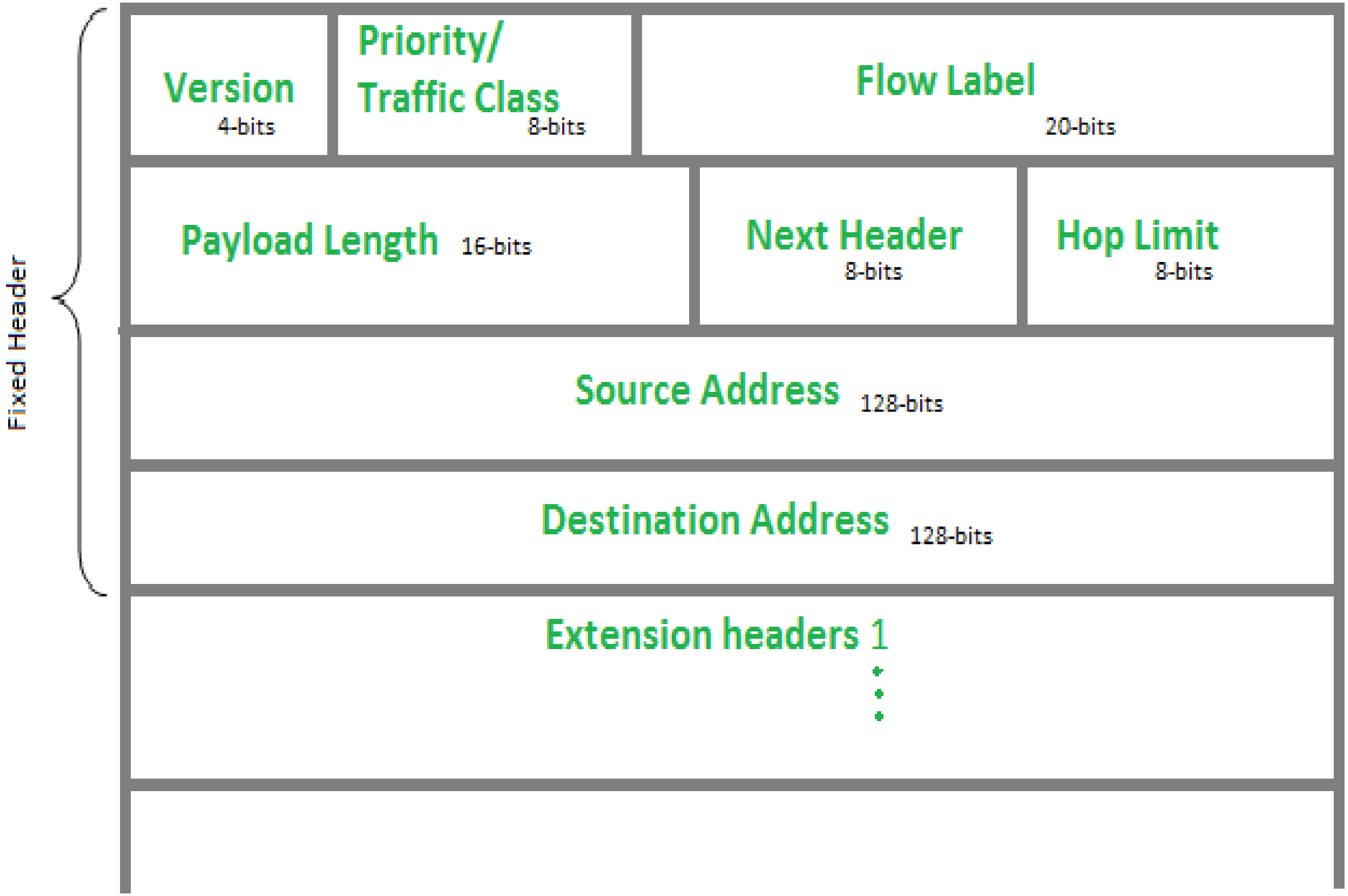
- ***VERSION:*** *Version of the IP protocol (4 bits), which is 4 for IPv4*
- ***HLEN:*** *IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*
- ***Type of service:*** *Low Delay, High Throughput, Reliability (8 bits)*
- ***Total Length:*** *Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.*
- ***Identification:*** *Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)*

- ***Flags:*** *3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)*
- ***Fragment Offset:*** *Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.*
- ***Time to live:*** *Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*

- ***Protocol:*** *Name of the protocol to which the data is to be passed (8 bits)*
- ***Header Checksum:*** *16 bits header checksum for checking errors in the datagram header*
- ***Source IP address:*** *32 bits IP address of the sender*
- ***Destination IP address:*** *32 bits IP address of the receiver*
- ***Option:*** *Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*
- Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).
-

Internet Protocol version 6 (IPv6) Header

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let’s look at the header of IP version 6 and understand how it is different from the IPv4 header.



Fixed Header

Version 4-bits

Priority/ Traffic Class 8-bits

Flow Label 20-bits

Payload Length 16-bits

Next Header 8-bits

Hop Limit 8-bits

Source Address 128-bits

Destination Address 128-bits

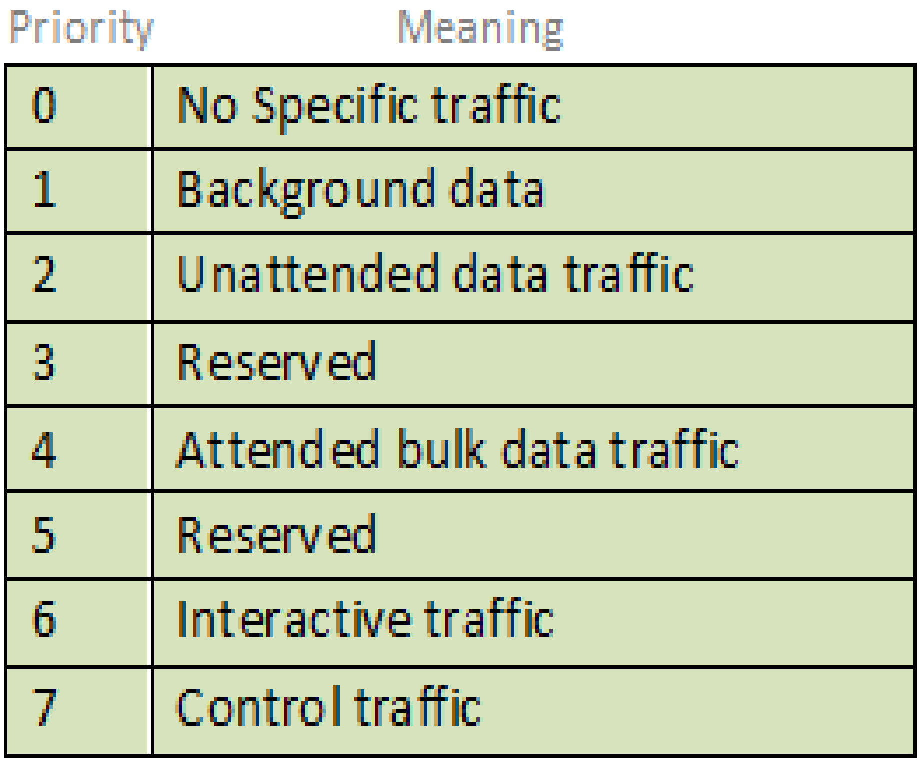
Extension headers 1

⋮

- **Version (4-bits):** Indicates version of Internet Protocol which contains bit sequence 0110.
- **Traffic Class (8-bits):** The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.

  As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.

- Priority assignment of Congestion controlled traffic :



Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

- Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic. The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

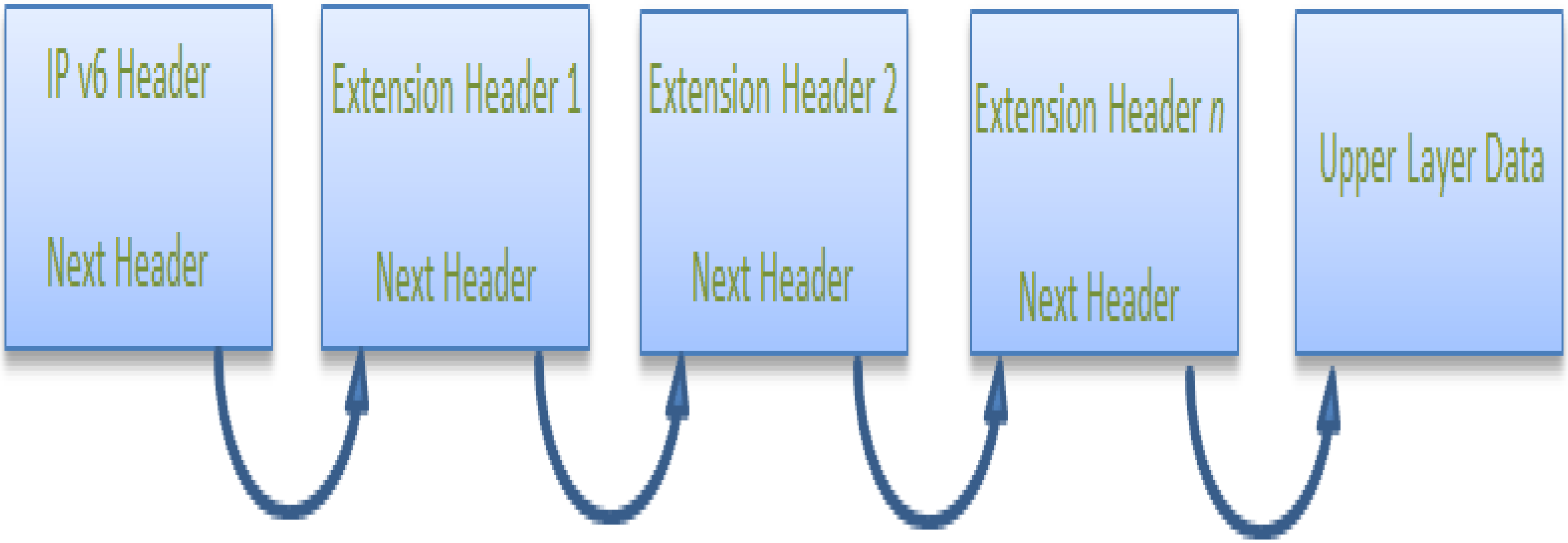
- **Flow Label (20-bits):** Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.

- **Payload Length (16-bits):** It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

- **Next Header (8-bits):** Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.
- **Hop Limit (8-bits):** Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

- **Source Address (128-bits):** Source Address is the 128-bit IPv6 address of the original source of the packet.
- **Destination Address (128-bits):** The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

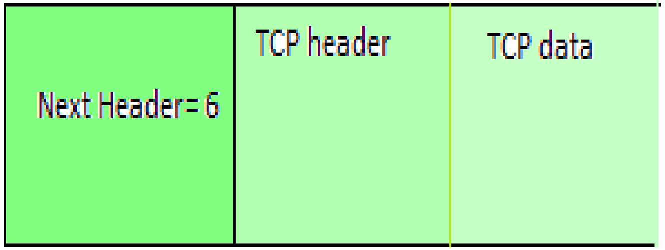
- **Extension Headers:** In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.



IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Example: *TCP is used in IPv6 packet*

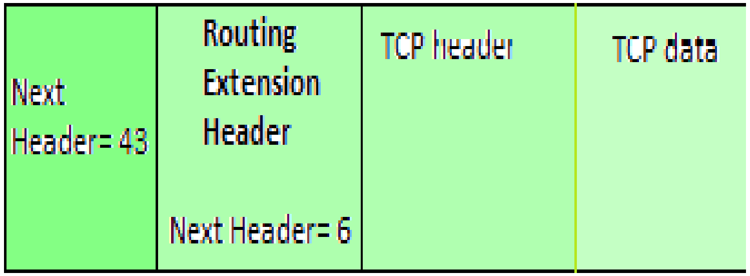


Next Header= 6

TCP header

TCP data

Example2:



Next Header= 43

Routing Extension Header

Next Header= 6

TCP header

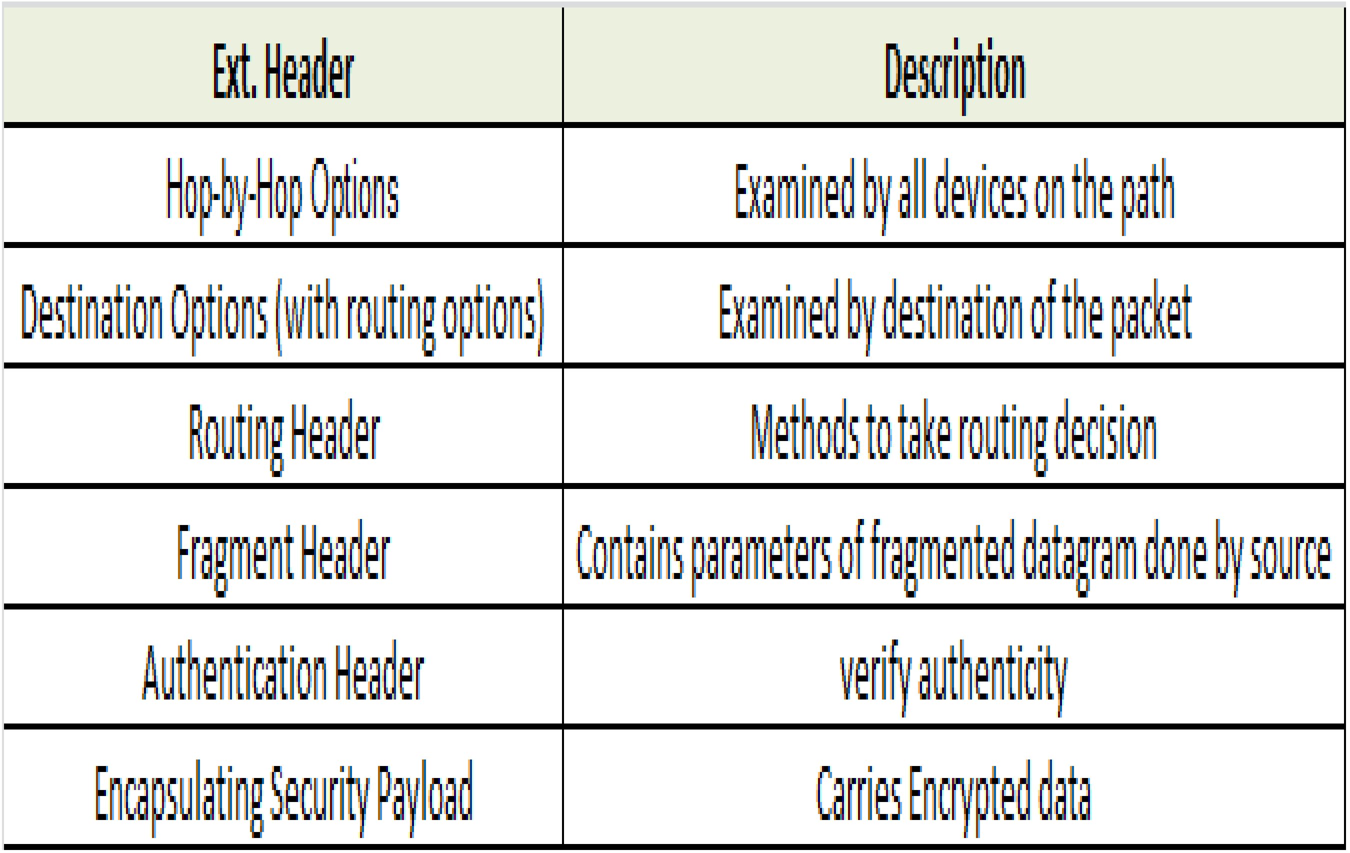
TCP data

- **Rule:** Hop-by-Hop options header(if present) should always be placed after the IPv6 base header.

Conventions :

- Any extension header can appear at most once except Destination Header because Destination Header is present two times in the above list itself.
- If Destination Header is present before Routing Header then it will be examined by all intermediate nodes specified in the routing header.
- If Destination Header is present just above the Upper layer then it will be examined only by the Destination node.

- Given order in which all extension header should be chained in IPv6 packet and working of each extension header :



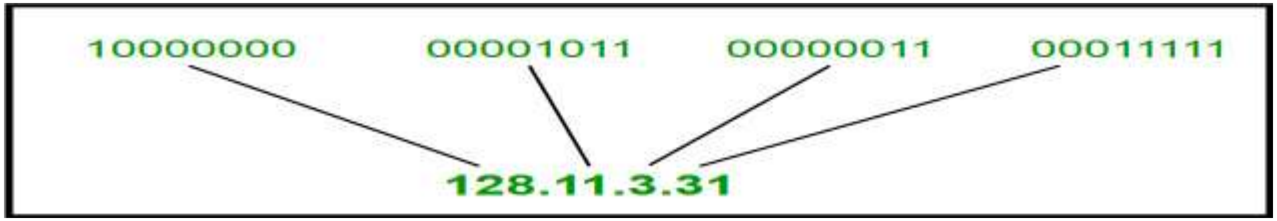
Ext. Header	Description
Hop-by-Hop Options	Examined by all devices on the path
Destination Options (with routing options)	Examined by destination of the packet
Routing Header	Methods to take routing decision
Fragment Header	Contains parameters of fragmented datagram done by source
Authentication Header	verify authenticity
Encapsulating Security Payload	Carries Encrypted data

Introduction of Classful IP Addressing

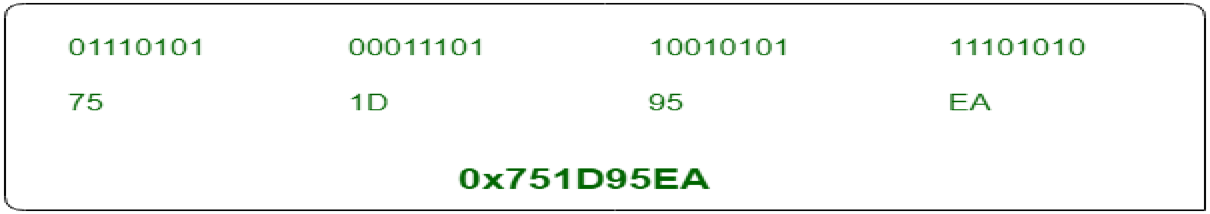
IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32} (**4,294,967,296)**

Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation:



Hexadecimal Notation:



01110101	00011101	10010101	11101010
75	1D	95	EA

0x751D95EA

Some points to be noted about dotted decimal notation:

- The value of any segment (byte) is between 0 and 255 (both included).
- There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

Classful Addressing

The 32 bit IP address is divided into five sub-classes. These are:

Class A

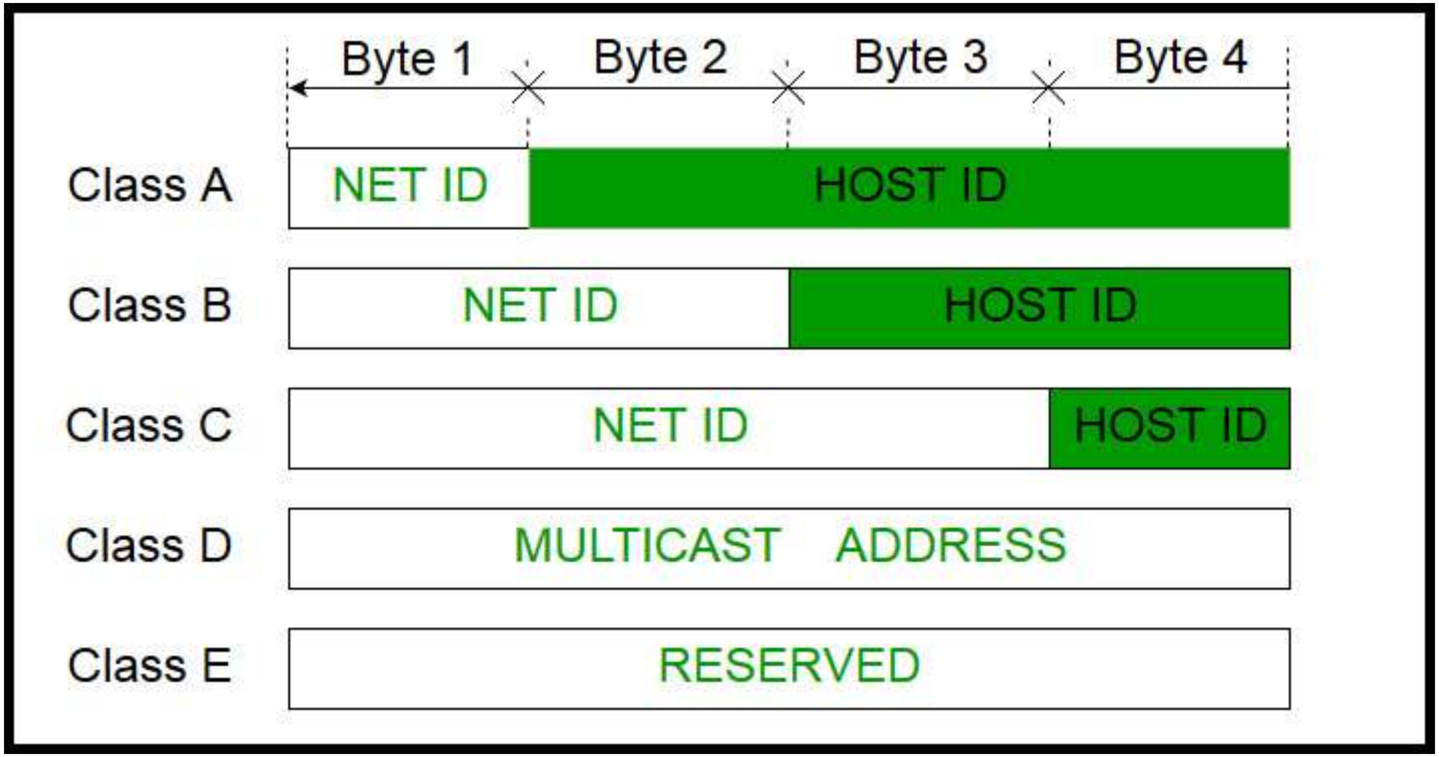
Class B

Class C

Class D

Class E

- Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.
  IPv4 address is divided into two parts:
- **Network ID**
- **Host ID**
- The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



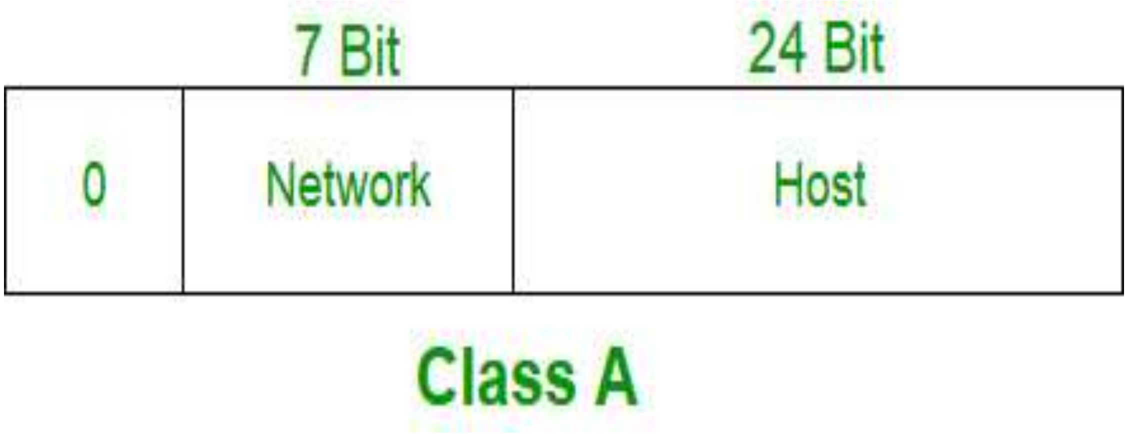
Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

- IP address belonging to class A are assigned to the networks that contain a large number of hosts.
- The network ID is 8 bits long.
- The host ID is 24 bits long.
- The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

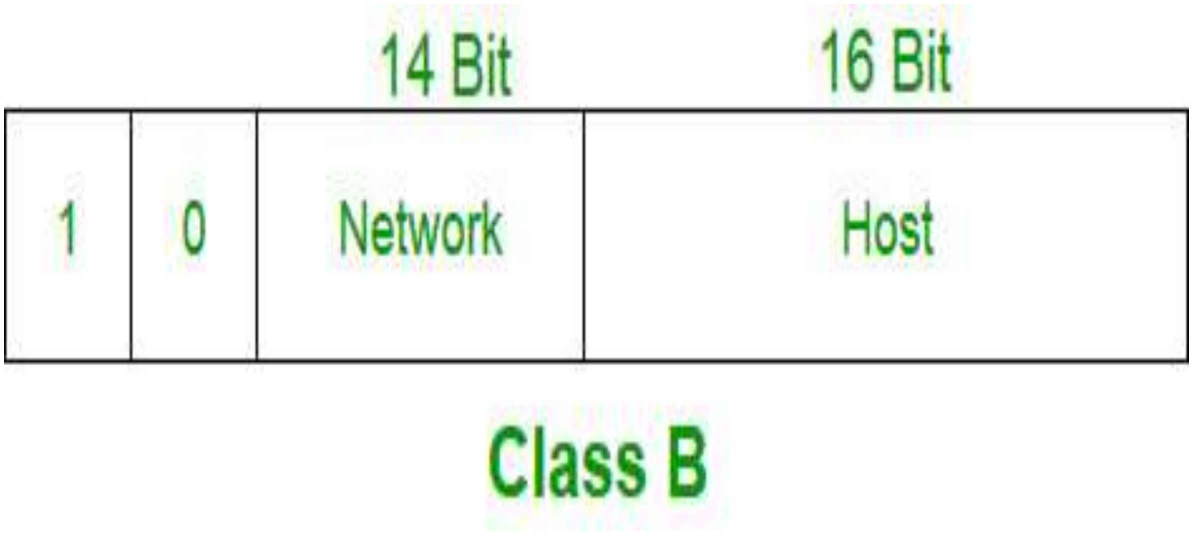
- 2^7-2= 126 network ID(Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID
- IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x



Class B:

- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.
- The network ID is 16 bits long.
- The host ID is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address
- IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

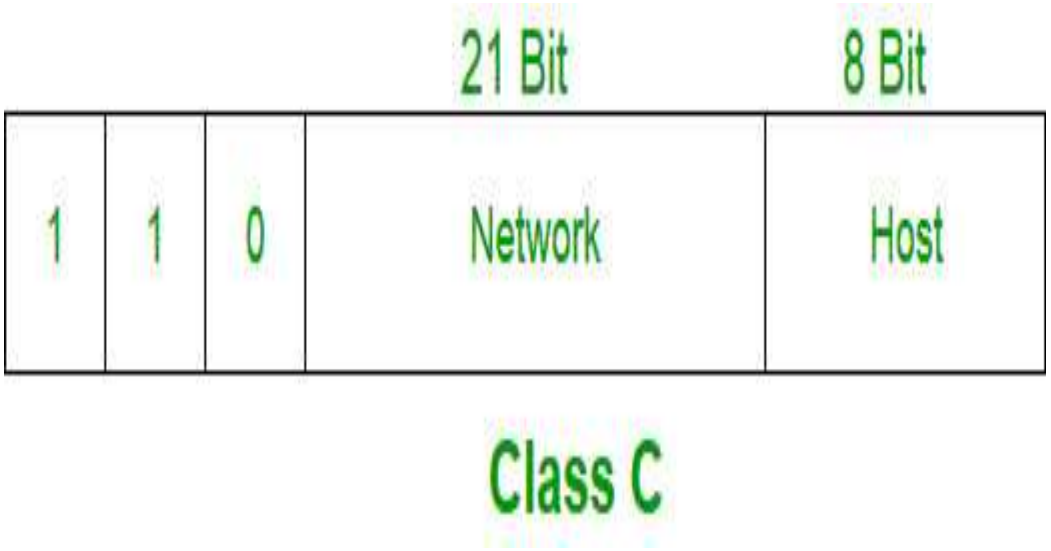


Class C:

- IP address belonging to class C are assigned to small-sized networks.
  - The network ID is 24 bits long.
  - The host ID is 8 bits long.
- The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

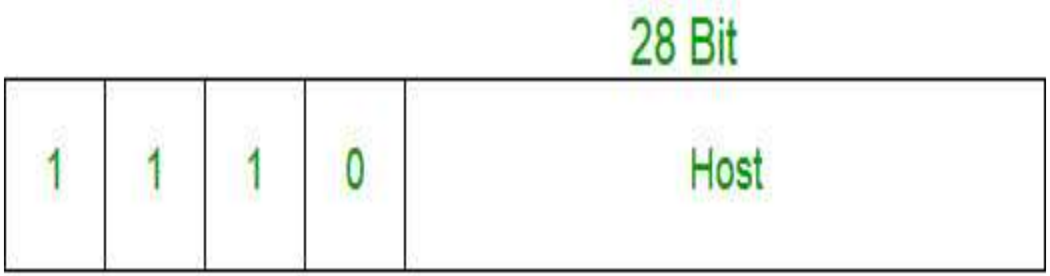
- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.



Class D:

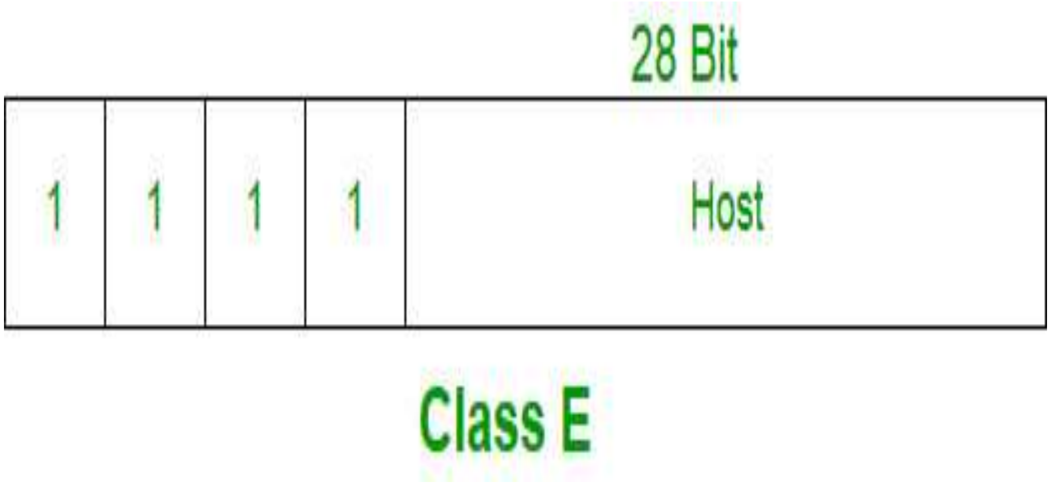
- IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class D

Class E:

- IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Range of special IP addresses:

- **169.254.0.0 – 169.254.0.16** : Link local addresses
  127.0.0.0 – 127.0.0.8 : Loop-back addresses
  0.0.0.0 – 0.0.0.8 : used to communicate within the current network.

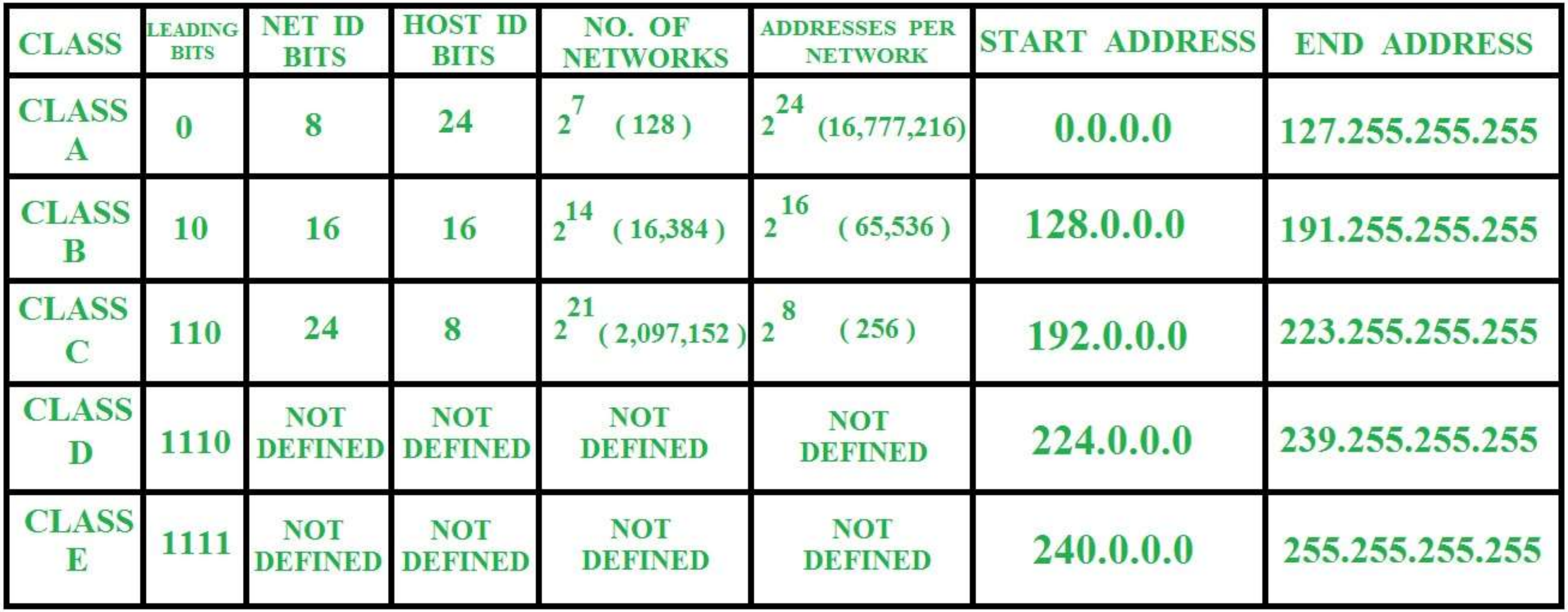
Rules for assigning Host ID:

- Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:
  - Within any network, the host ID must be unique to that network.
  - Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
  - Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

- Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:
  - The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
  - All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
  - All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren’t used.

Summary of Classful addressing :



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Problems with Classful Addressing:

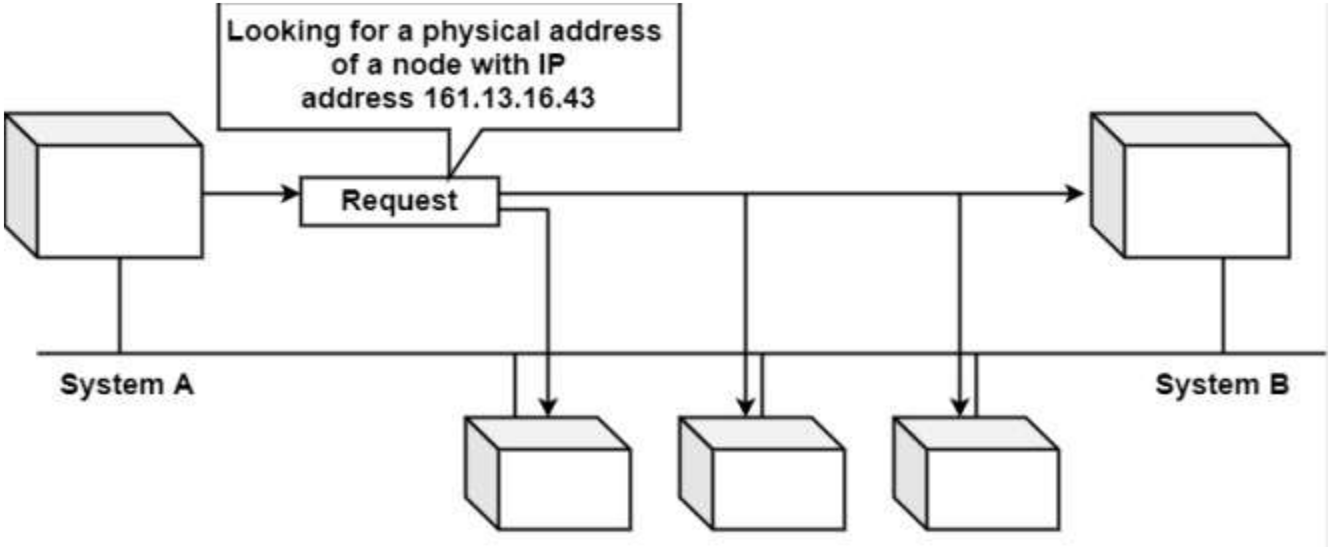
- The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.
- Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993.

Address Resolution Protocol (ARP)

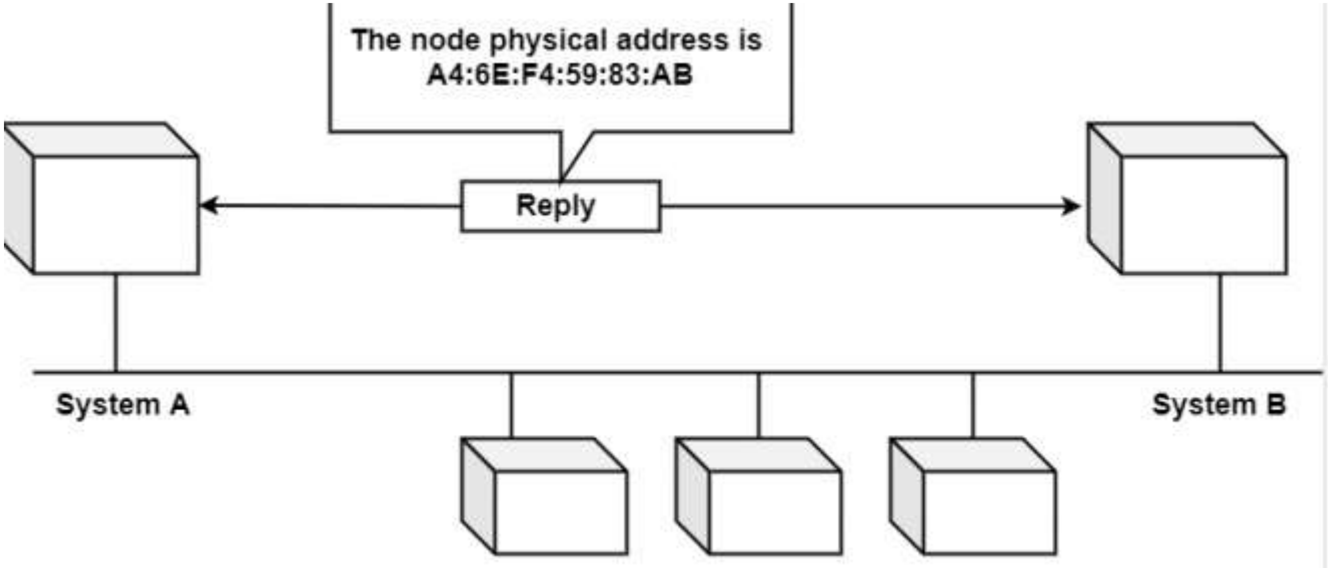
Address Resolution Protocol (ARP) is a network-specific standard protocol. The Address Resolution Protocol is important for changing the higher-level protocol address (IP addresses) to physical network addresses. It is described in RFC 826.

ARP relates an IP address with the physical address. On a typical physical network such as LAN, each device on a link is identified by a physical address, usually printed on the network interface card (NIC). A physical address can be changed easily when NIC on a particular machine fails.

- The IP Address cannot be changed. ARP can find the physical address of the node when its internet address is known. ARP provides a dynamic mapping from an IP address to the corresponding hardware address.
- When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address.


Looking for a physical address of a node with IP address 161.13.16.43
Request
System A
System B

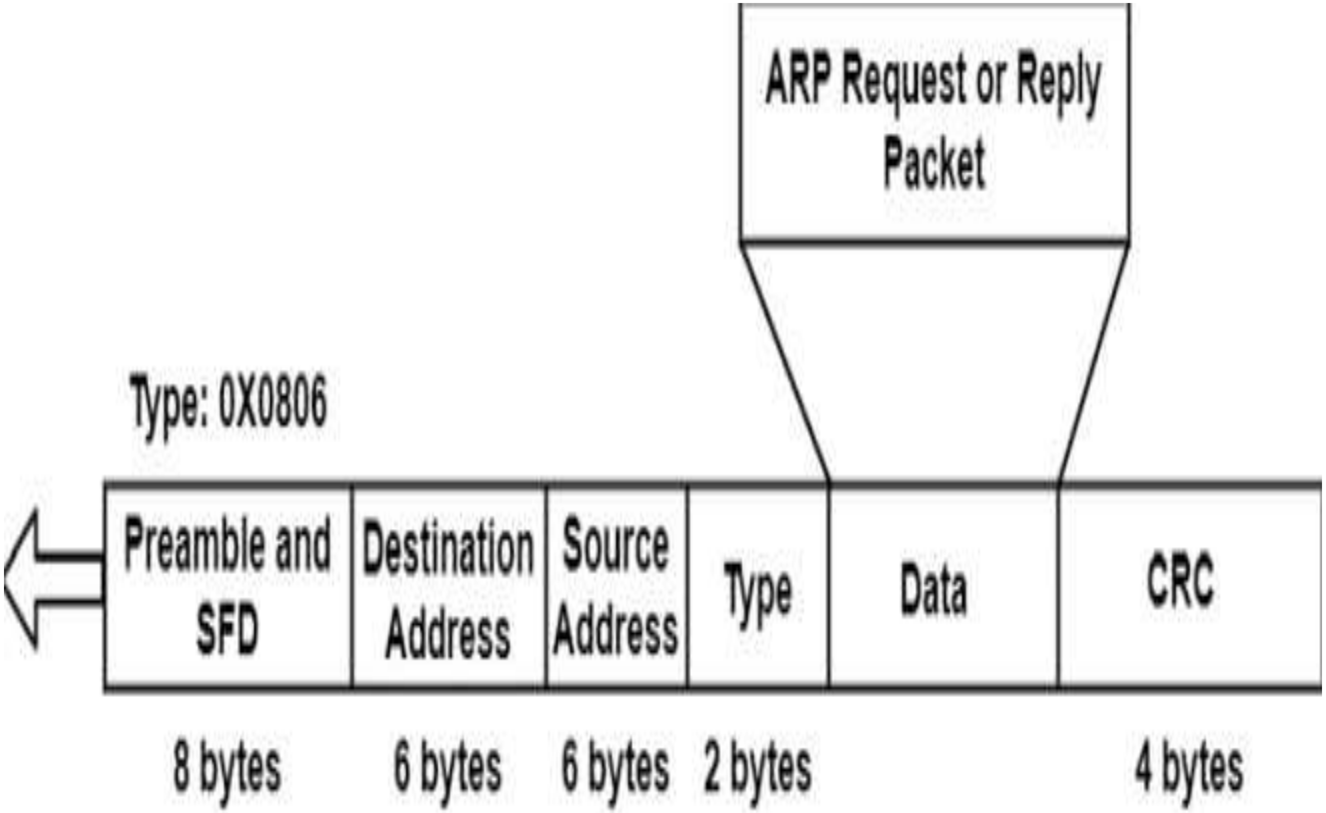
(a) ARP request is broadcast



(b) ARP reply is unicast

ARP Packet Generation

- **Hardware address space:** It specifies the type of hardware such as Ethernet or Packet Radio net.
- **Protocol address space:** It specifies the type of protocol, same as the Ether type field in the IEEE 802 header (IP or ARP).
- **Hardware Address Length:** It determines the length (in bytes) of the hardware addresses in this packet. For IEEE 802.3 and IEEE 802.5, this is 6.
- **Protocol Address Length:** It specifies the length (in bytes) of the protocol addresses in this packet. For IP, this is 4 byte.
- **Operation Code:** It specifies whether this is an ARP request (1) or reply (2).
- **Source/target hardware address:** It contains the physical network hardware addresses. For IEEE 802.3, these are 48-bit addresses.



Encapsulation of ARP Packet

Reverse Address Resolution Protocol (RARP)

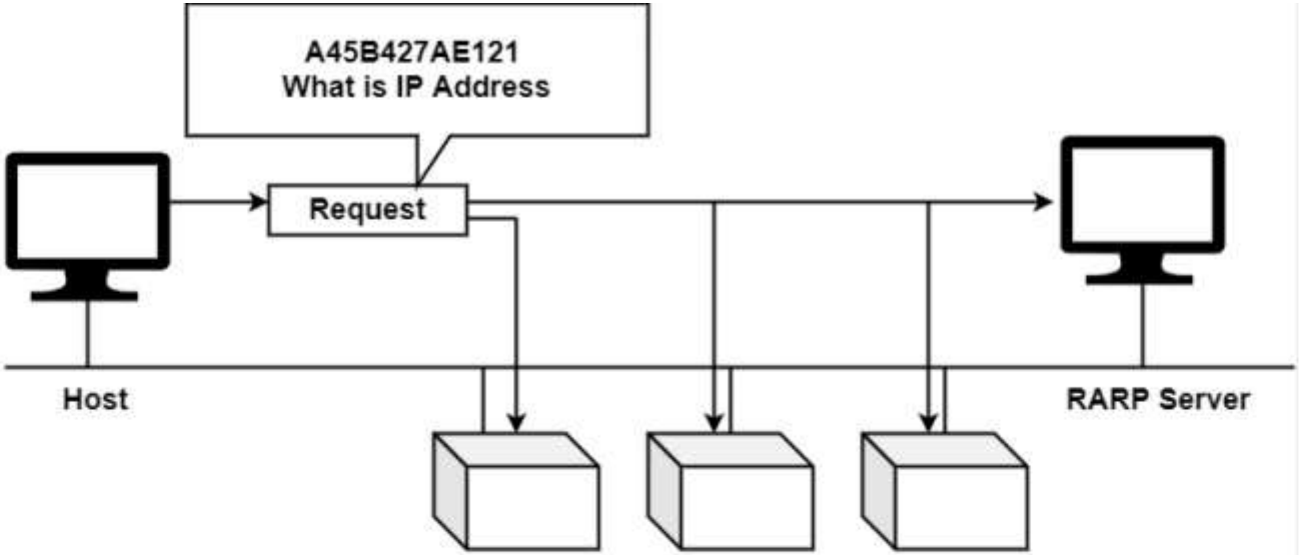
- Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol. It is described in RFC 903. Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted. To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.
- The reverse address resolution is performed the same way as the ARP address resolution. The same packet format is used for the ARP.

- An exception is the operation code field that now takes the following values–

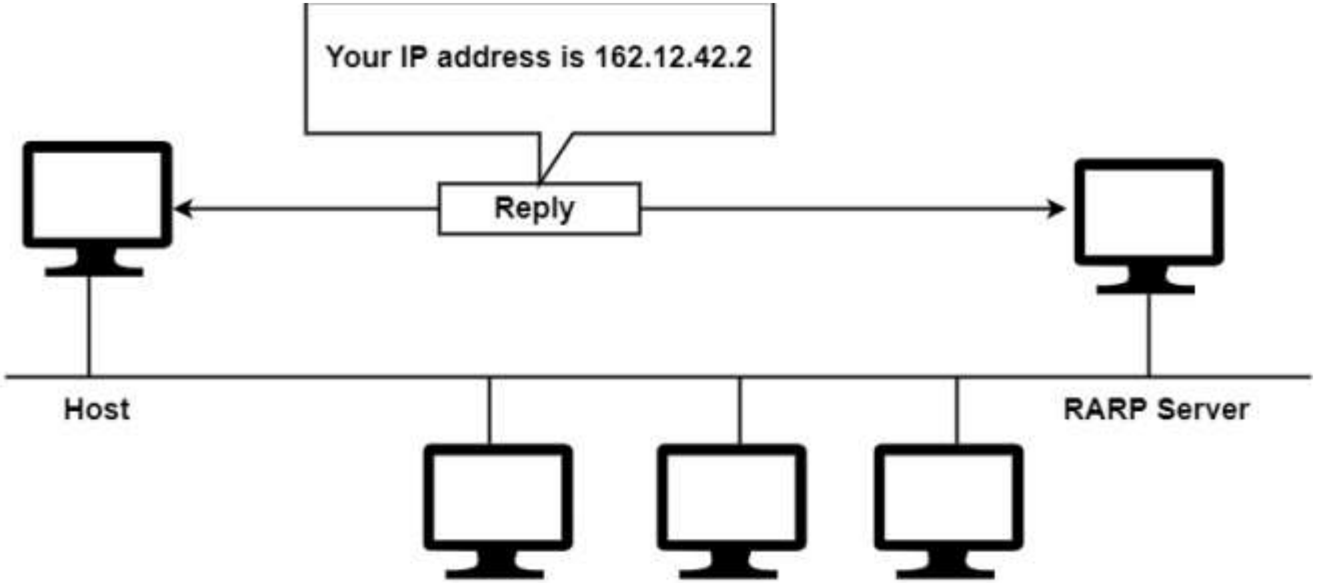
  3 for RARP request

  4 for RARP reply

- The physical header of the frame will now indicate RARP as the higher-level protocol (8035 hex) instead of ARP (0806 hex) or IP-(0800 hex) in the Ether type field.



(a) RARP request is broadcast



(b) RARP reply is unicast

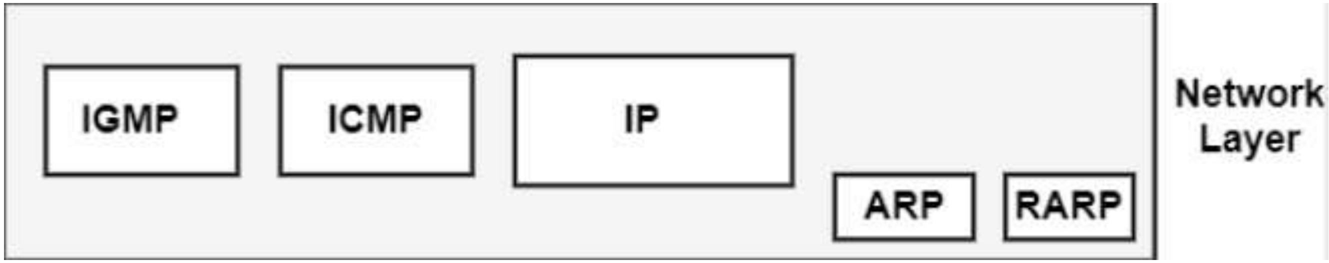
- When a framework with a local disk is bootstrapped, it generally accepts its IP address from a configuration document that's read from a disk file. But a system without a disk, including an X terminal or a diskless workstation, needs some other way to accept its IP address.
- The feature of RARP is for the diskless framework to read its specific hardware address from the interface card and send a RARP request asking for someone to reply with the diskless systems IP address.
- The format of a RARP packet is almost identical to an ARP packet. The only difference is that the frame type is 0X8035 for a RARP request or reply, and the op-field has a value of 3 for a RARP request and 4 for a RARP reply.

Internet Control Message Protocol (ICMP)

- The ICMP represents Internet Control Message Protocol. It is a network layer protocol. It can be used for error handling in the network layer, and it is generally used on network devices, including routers. IP Protocol is a best-effect delivery service that delivers a datagram from its original source to its final destination. It has two deficiencies−

  Lack of Error Control, Lack of assistance mechanisms

- IP protocol also lacks a structure for host and management queries. A host needs to resolve if a router or another host is alive, and sometimes a network manager needs information from another host or router. ICMP has been created to compensate for these deficiencies.



ICMP is a network layer protocol. But, its messages are not passed directly to the data link layer. Instead, the messages are first encapsulated inside the IP datagrams before going to the lower layer.

The cost of the protocol field in the IP datagram is I, to indicate that IP data is an ICMP message.

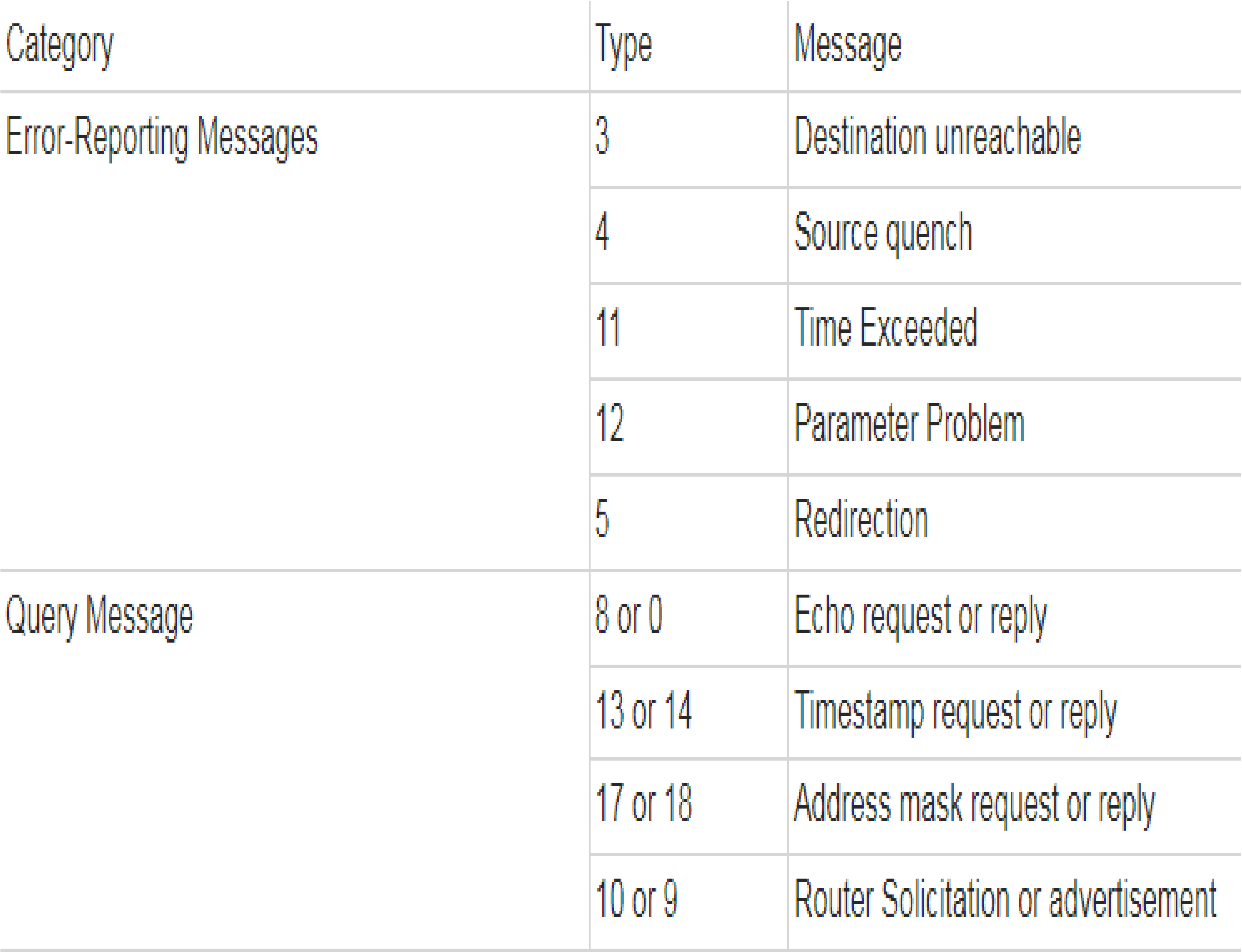
The error reporting messages report issues that a router or a host (destination) may encounter when it phases an IP packet.

The query messages, which appear in pairs, help a host or a network manager to get specific data from a router or another host.

- Internet Control Message Protocol (ICMP) works in the network layer of the OSI model and the internet layer of the TCP/IP model. It is used to send control messages to network devices and hosts. Routers and other network devices monitor the operation of the network. When an error occurs, these devices send a message using ICMP. Messages that can be sent include "destination unreachable", "time exceeded", and "echo requests".
- ICMP is a network layer protocol.
- ICMP messages are not passed directly to the data link layer. The message is first encapsulated inside the IP datagram before going to the lower layer.

Types of ICMP messages

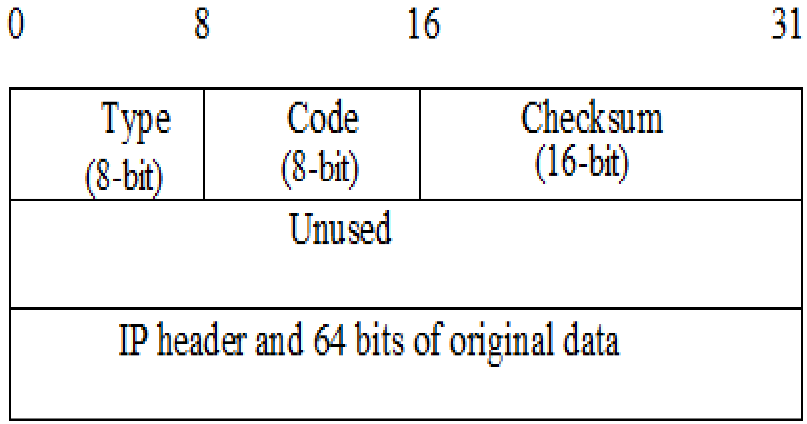
- **Information Messages** − In this message, the sender sends a query to the host or router and expects an answer. For example, A host wants to know if a router is alive or not.
- **Error-reporting message** − This message report problems that a router or a host (destination) may encounter when it processes an IP packet.
- **Query Message** − It helps a router or a network manager to get specific information from a router or another host.



Category	Type	Message
Error-Reporting Messages	3	Destination unreachable
	4	Source quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Message	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router Solicitation or advertisement

- **Source Quench** − It requests to decrease the traffic rate of message sending from source to destination.
- **Time Exceeded** − When fragments are lost in a network the fragments hold by the router will be dropped and then ICMP will take the source IP from the discarded packet and inform the source, that datagram is discarded due to the time to live field reaches zero, by sending time exceeded message.
- **Fragmentation Required** − When a router is unable to forward a datagram because it exceeds the MTU of the next-hop network and the DF (Don't Fragment) bit is set, the router is required to return an ICMP Destination Unreachable message to the source of the datagram, with the Code indicating fragmentation is needed and DF (Don’t Fragment) set.

- **Destination Unreachable** − This error message indicates that the destination host, network, or port number that is specified in the IP packet is unreachable. This may happen due to the destination host device is down, an intermediate router is unable to find a path to forward the packet, and a firewall is configured to block connections from the source of the packet.
- **Redirect Message** − A redirect error message is used when a router needs to tell a sender that it should use a different path for a specific destination. It occurs when the router knows a shorter path to the destination.



0 8 16 31

Type (8-bit)	Code (8-bit)	Checksum (16-bit)
Unused		
IP header and 64 bits of original data		

Type – The type field identifies the type of the message.

Code – The code field in ICMP describes the purpose of the message.

Checksum – The checksum field is used to validate ICMP messages.

Dynamic Host Configuration Protocol (DHCP)

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.
- DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC 2131.

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

- DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.
- There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

How DHCP works

- DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

- DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

The DHCP lease process works as follows:

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.

- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

- When working with DHCP, it is important to understand all of the components. Following are the list of components:
- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.

- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.

- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.

Benefits of DHCP

- **Centralized administration of IP configuration:** DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.
- **Dynamic host configuration:** DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

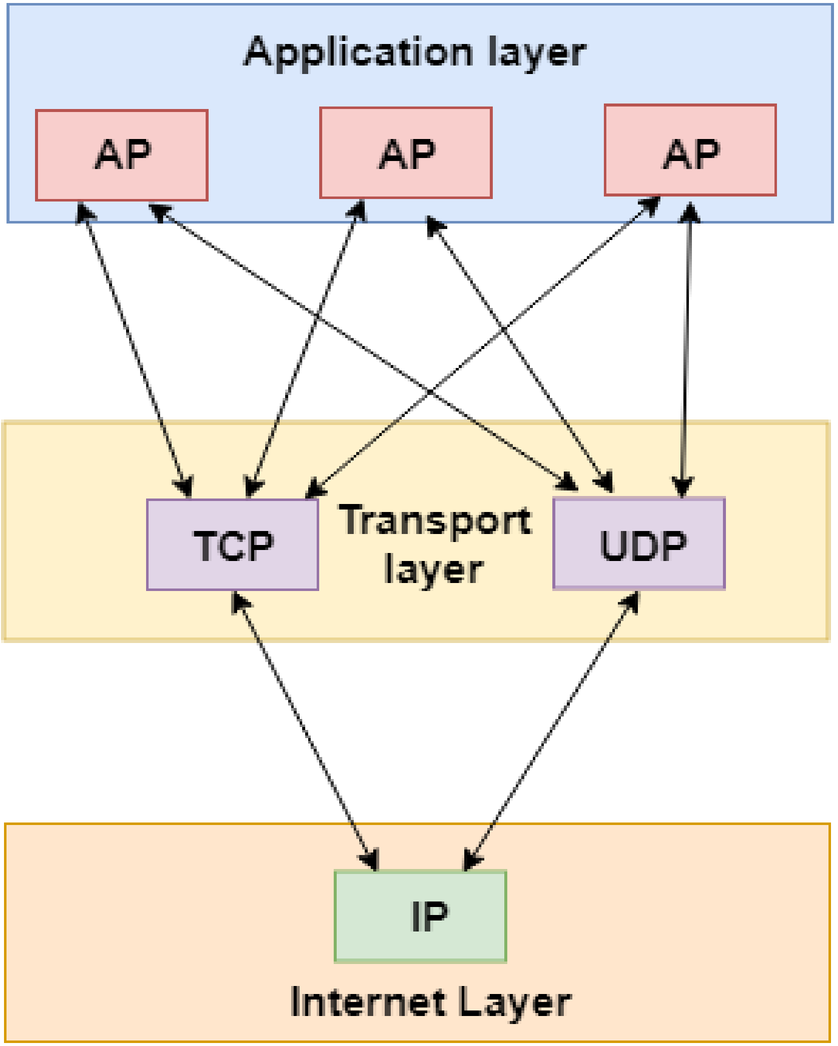
- **Seamless IP host configuration:** The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.
- **Flexibility and scalability:** Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

Transport Layer

- The transport layer is a 4th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.

- The transport layer protocols are implemented in the end systems but not in the network routers.
- A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.
- All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.

- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.


Application layer
AP
AP
AP
TCP
Transport layer
UDP
IP
Internet Layer

Services provided by the Transport Layer

- The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing

End-to-end delivery:

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Reliable delivery:

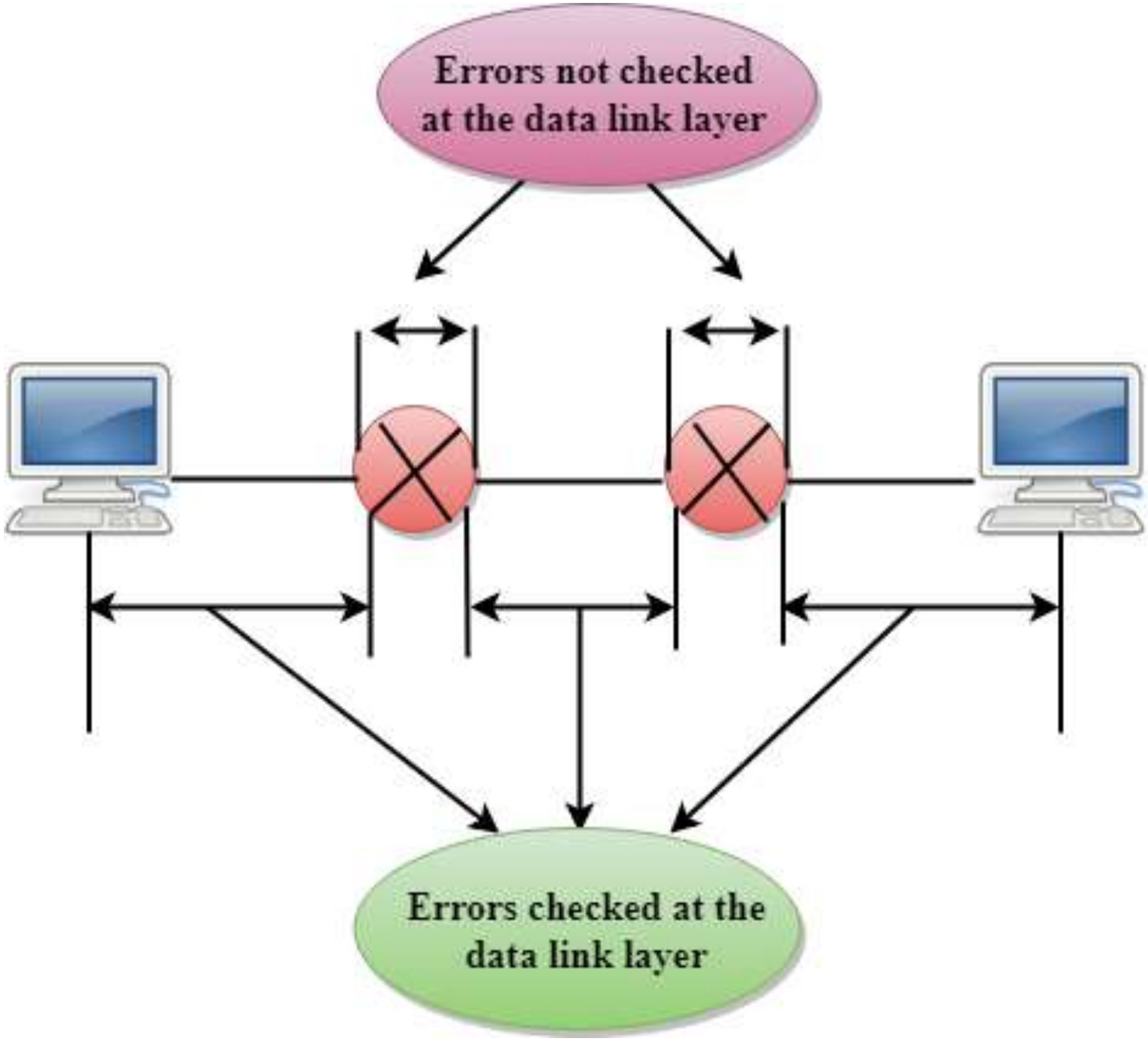
- The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:

- Error control
- Sequence control
- Loss control
- Duplication control

Error Control

- The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.


Errors not checked at the data link layer
Errors checked at the data link layer

Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control

- Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver’s transport layer to identify the missing segment.

Duplication Control

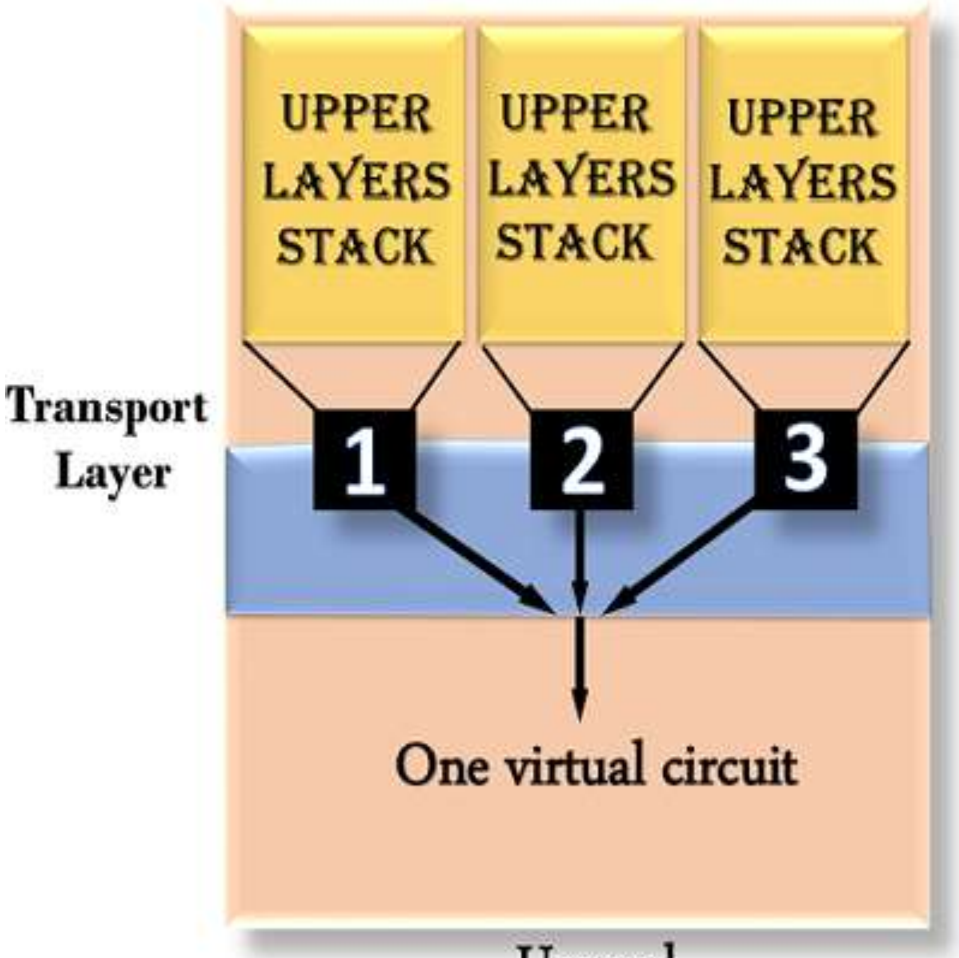
- Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control

- Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing

- The transport layer uses the multiplexing to improve transmission efficiency.
- **Multiplexing can occur in two ways:**
- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.



Transport Layer

UPPER LAYERS STACK

UPPER LAYERS STACK

UPPER LAYERS STACK

1

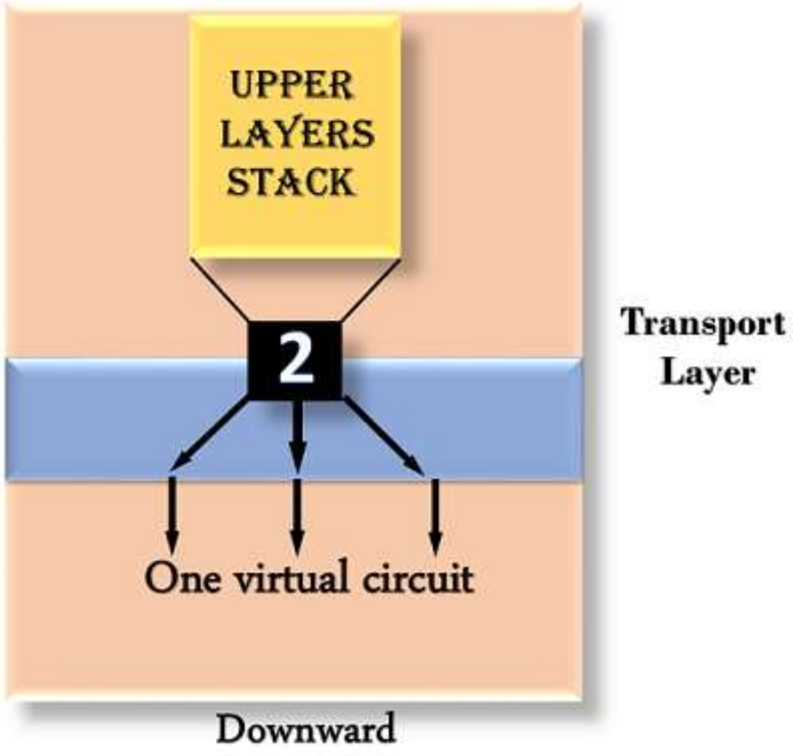
2

3

One virtual circuit

Upward

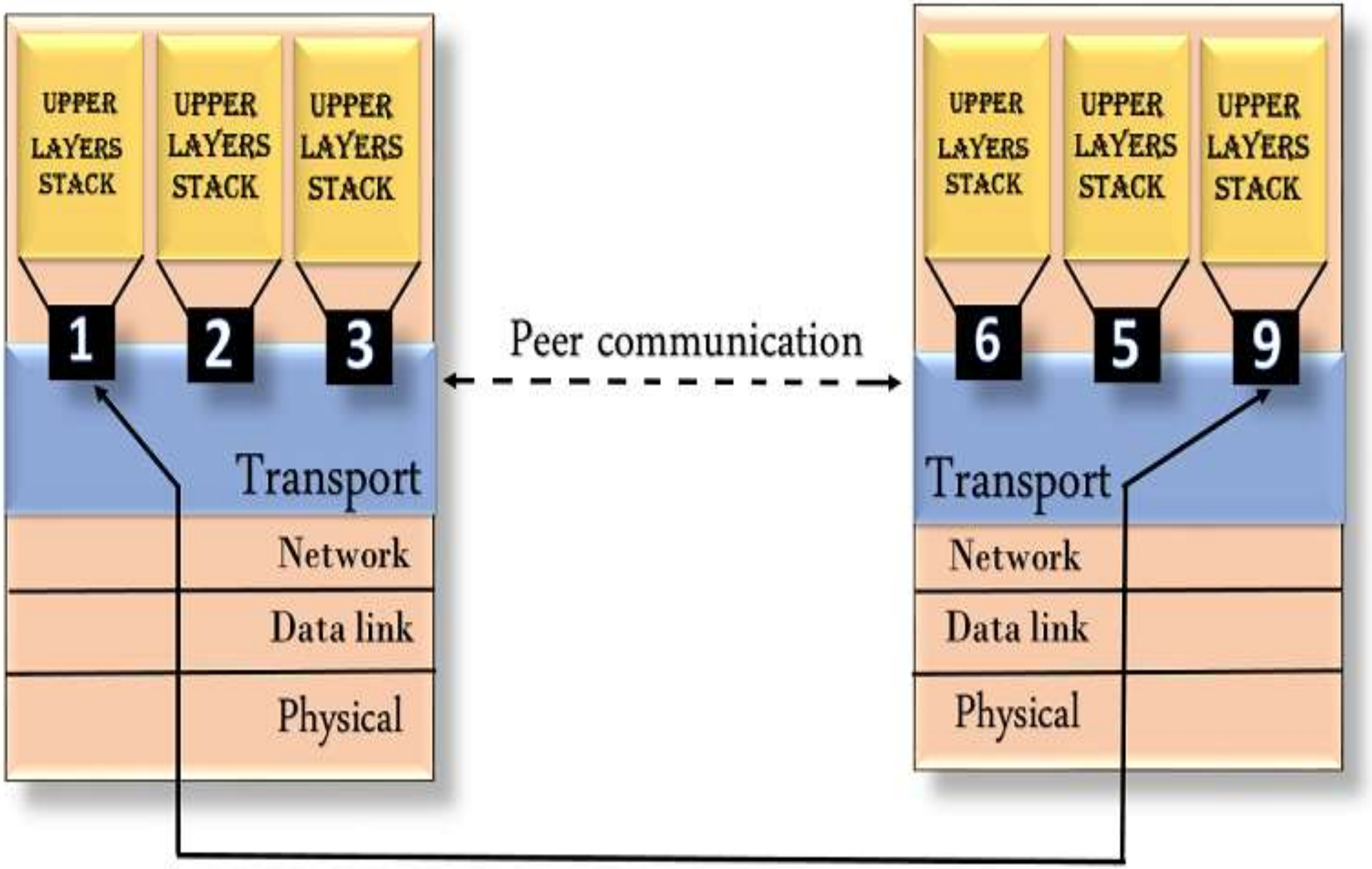
- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.



Addressing

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.

- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.


UPPER LAYERS STACK
UPPER LAYERS STACK
UPPER LAYERS STACK
1
2
3
Peer communication
UPPER LAYERS STACK
UPPER LAYERS STACK
UPPER LAYERS STACK
6
5
9
Transport
Network
Data link
Physical
Transport
Network
Data link
Physical

Classless Inter Domain Routing (CIDR)

As we have already learned about Classful Addressing, so in this article, we are going to learn about Classless Inter-Domain Routing. which is also known as Classless addressing. In the Classful addressing the no of Hosts within a network always remains the same depending upon the class of the Network.

Class A network contains 2^{24} Hosts, Class B network contains 2^{16} Hosts, Class C network contains 2^{8} Hosts.

- Now, let’s suppose an Organization requires 2^{14} hosts, then it must have to purchase a Class B network. In this case, 49152 Hosts will be wasted. This is the major drawback of Classful Addressing.
- In order to reduce the wastage of IP addresses a new concept of **Classless Inter-Domain Routing** is introduced. Now a days *IANA* is using this technique to provide the IP addresses. Whenever any user asks for IP addresses, IANA is going to assign that many IP addresses to the User.
-

- **Representation:** It is as also a 32-bit address, which includes a special number which represents the number of bits that are present in the Block Id.
-

  a . b . c . d / n
  Where, n is number of bits that are present in Block Id / Network Id.

Example:

- 20.10.50.100/20