# EDU ENGINEERING

PIONEER OF ENGINEERING NOTES

## TAMIL NADU'S BEST EDTECH PLATFORM FOR ENGINEERING

**CONNECT WITH US**

**WEBSITE:** www.eduengineering.net

**TELEGRAM:** @eduengineering

**INSTAGRAM:** @eduengineering

- **Regular Updates for all Semesters**
- **All Department** Notes AVAILABLE
- **Handwritten** Notes AVAILABLE
- **Past Year** Question Papers AVAILABLE
- **Subject wise** Question Banks AVAILABLE
- **Important Questions** for Semesters AVAILABLE
- Various **Author Books** AVAILABLE

# Unit III Network Layer

Switching: Packet Switching - Internet Protocol - $IPV_4$ - IP Addressing - Subnetting - $IPV_6$, ARP, RARP, ICMP, DHCP.

## 3.1 Network Layer:

Network Layer is the third layer of the OSI model. It handles the service requests from the transport layer and further forwards the service request to the data link layer. The network layer translates the logical addresses into physical addresses.

It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.

The main role of the network layer is to move the packets from sending host to the receiving host.

### 3.1.1 Network Layer services

Main task of the network layer is to move packets from the source host to the destination host. Network layer services are packetizing, routing & forwarding and other services.

- Packetizing: Encapsulating the payload in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination called packetizing.

- Routing: Network layer is responsible for finding the best one route from the source to the destination is called routing.
- Forwarding: For warding refers to the way a packet is delivered to the next node.
- Other services expected from the network layer is error control
  flow control
  congestion control
  Quality of service
  Security

## 3.2 Switching

A router infact is a switch that creates a connection between an input port and an output port, just as an electric switch connects the input to the output to let electricity flow.

Switching techniques are divided into two broad categories: circuit switching and packet switching, but only packet switching is used at the network layer because the unit of data at this layer is a packet.

Packet switched network use two different approaches to route the packets:

- The datagram approach
- The virtual circuit approach

## • Datagram Approach: Connectionless Service

When the network layer provides a connectionless service, each packet traveling in the internet is an independent entity; there is no relationship between packets belonging to the same message. The switches in this type of network are called routers.

A packet may be followed by a packet coming from the same or from a different source.

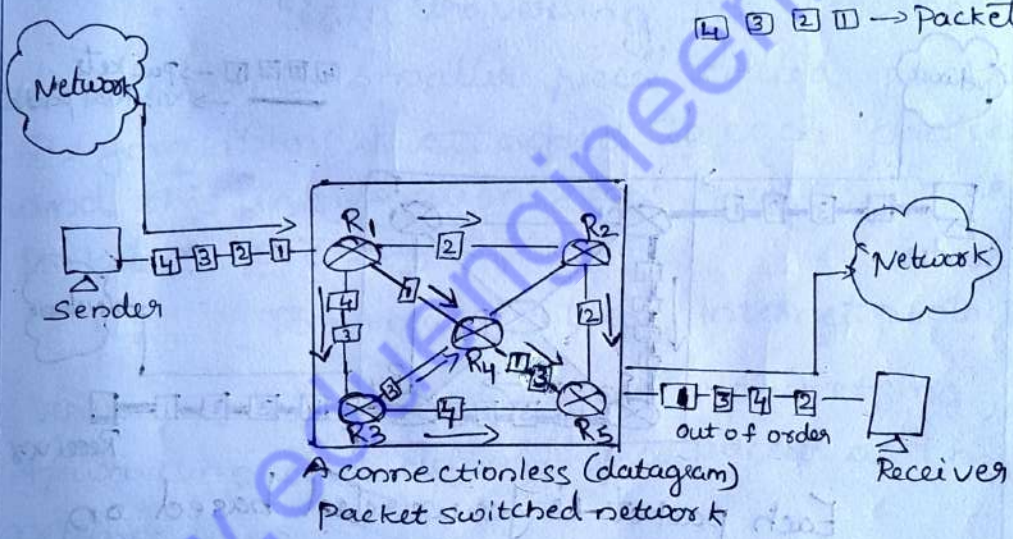



Fig: A connectionless packet switched Network

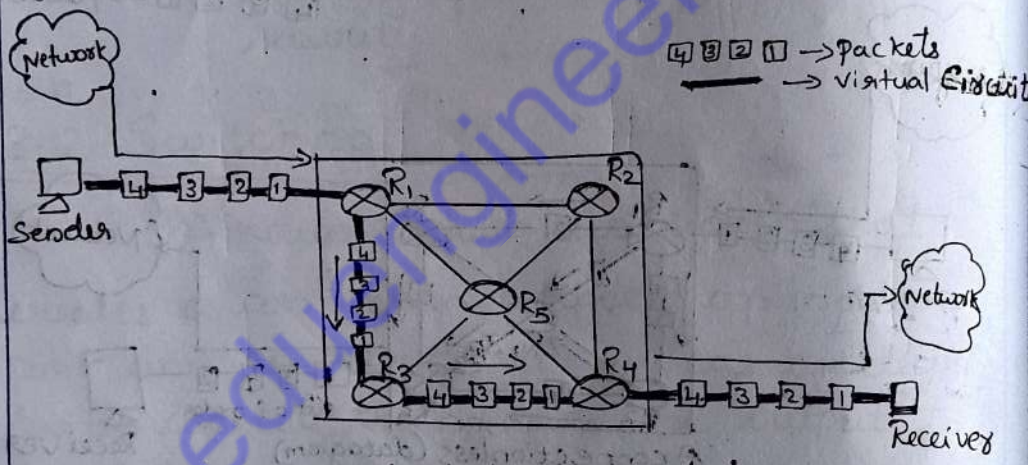
Each packet is routed based on the information contained in its header: source and destination addresses.

The router in this case routes the packet based only on the destination address. The router in this case routes the packet based only on the destination address. The source address may be used to send an error message to the source if the packet is discarded

- Virtual-Circuit approach: connection oriented service:

In connection-oriented service, there is a relationship between all packets belonging to a message. Before all datagrams in a message can be sent, a virtual connection should be setup to define the path for the datagrams. After connection setup, the datagrams can all follow the same path.

In this type, not only must the packet contain the source and destination addresses, it must also contain a flow label.




Each packet is forwarded based on the label in the packet. In this case, the forwarding decision is based on the value of the label.

To create a connection oriented service, a three phase process is used

- Setup
- data transfer
- Teardown phase

In setup phase, the source and destination addresses of the sender and receiver are used to make table entries for the connection oriented service.

In teardown phase, the source and destination inform the router to delete the corresponding entiries.

Data transfer occurs between these two phases.

## 3.3 Internet Protocol

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.

The main protocol, Internet protocol version 4 (IPV4) is responsible for packetizing, forwarding and delivery of a packet at the network layer.

### 3.3.1 IPV4

This protocol has the responsibility of identifying host based upon their logical addresses and to route data among them over the underlying network. Internet protocol version 4 uses 32 bit logical address

- IPV4 - Packet structure:

Internet protocol being a layer 3 protocol takes data segments from transport layer and divides it into packets.

(b)

IP Packet encapsulates data unit received from above layer and add to its own header information.

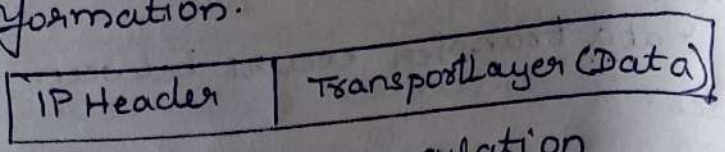
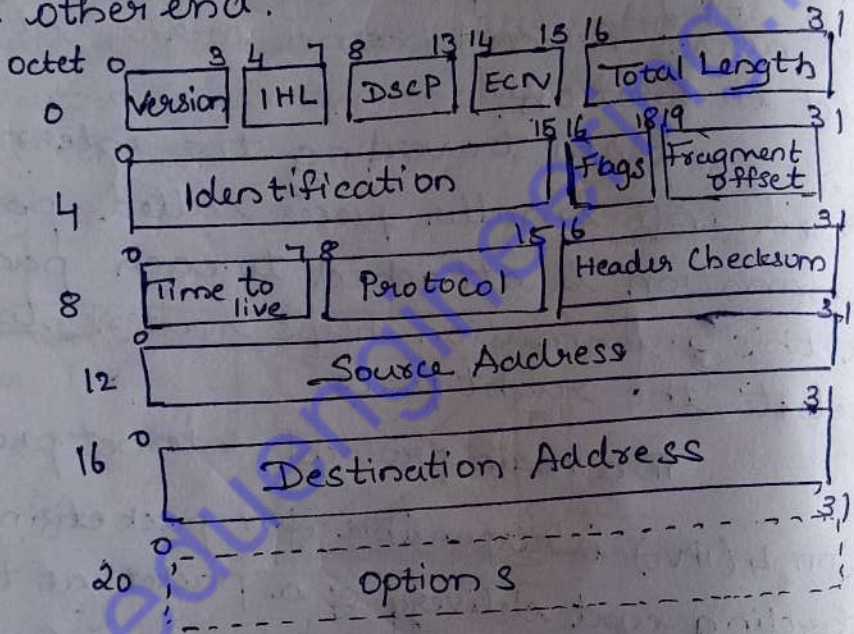



Fig: IP Encapsulation

The encapsulated data is referred to as payload. IP header contains all the necessary information to deliver the packet at the other end.




- ✓ Version — Version no. of internet protocol used.
- ✓ IHL — Internet Header Length; Length of entire IP header.
- ✓ DSCP — Differentiated Services Code Point; this is type of service.
- ✓ ECN — Explicit Congestion Notification: It carries information about the congestion seen in the route.
- ✓ Total Length — Length of entire IP packet (including IP header and IP payload)

✓ Identification – If IP Packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to

✓ Flags – As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not.

✓ Fragment offset – This offset tells the exact position of the fragment in the original IP Packet

✓ Time to Live – To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

✓ Protocol – Tells the network layer at the destination host, to which protocol this packet belongs to, ie the next level protocol. Eg: Protocol number of TCP is 6 and UDP is 17

✓ Header checksum – This field is used to keep checksum value of entire header which is then used to check if the packet is received error free.

✓ Source Address – 32 bit address of the sender of the Packet.

✓ Destination Address – 32 bit address of the receiver of the packet.

✓ Options – This is optional field, which is used if the value of IHL is greater than 5.

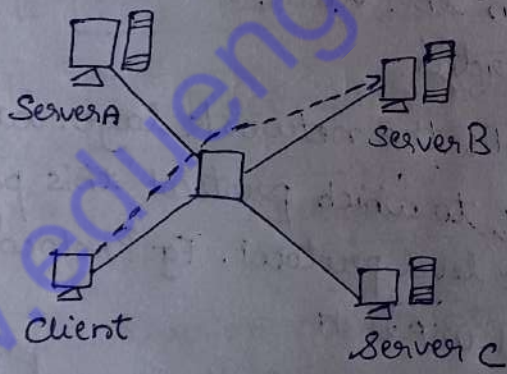
- IPV4 – Addressing:

IPV4 supports three different types of addressing modes.

- Unicast Addressing mode
- Broadcast Addressing mode
- Multicast Addressing mode

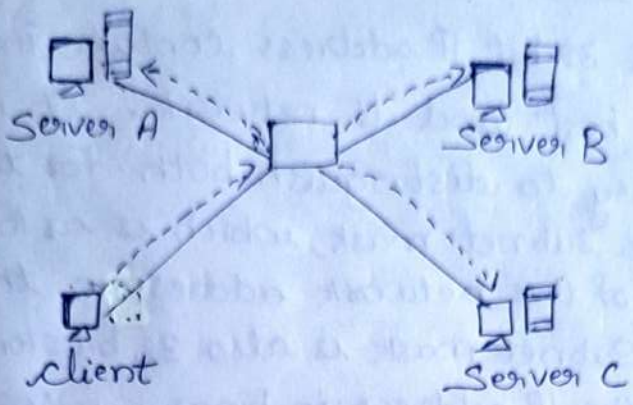
Unicast Addressing mode:

In this mode, data is sent only to one destined host. The distination address field contains 32 bit IP address of the destination host. Here the client sends data to the targeted server.



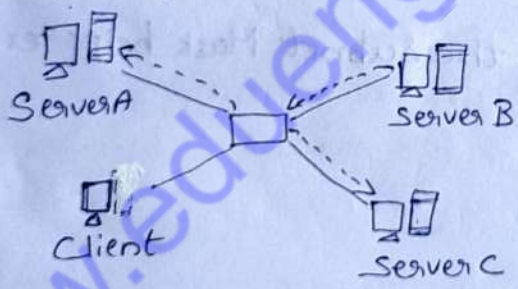

Broadcast Addressing mode:

In this mode, the packet is addressed to all the hosts in a network segment. The destination address field contains a special broadcast address ie, 255.255.255.255. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the servers.




## Multicast Addressing Mode:

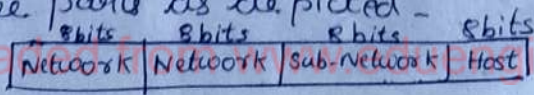
This mode is a mix of the previous two modes ie the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the destination address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.




Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the network number which represents the network and one IP address reserved for the broadcast address, which represents all the hosts in that network.

## Hierarchical Addressing scheme:

IPv4 uses hierarchial addressing scheme. An IP address, which is 32 bits in length is divided into two or three parts as depicted -



## ■ Subnet Mask :

The 32 bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address.

Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its subnet mask, the result yields the network address. For example, say the IP address is 192.168.1.152 and the subnet mask is 255.255.255.0 then.

| | | | | | | |
|---|---|---|---|---|---|---|
| IP | 192.168.1.152 | 11000000 | 10101000 | 00000001 | 10011000 | ANDed |
| Mask | 255.255.255.0 | 11111111 | 11111111 | 11111111 | 00000000 | |
| Network | 192.168.1.0 | 11000000 | 10101000 | 00000001 | 00000000 | Result |

This way the subnet mask helps extract the network ID and the host from an IP address. It can be identified now that 192.168.1.0 is the network number and 192.168.1.152 is the host on that network.

## ■ Binary Representation :

The positional value method is the simplest form of converting binary from decimal value. IP address is 32 bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of each bit can be determined by the position of bit value 1 in the octet.

| MSB | 8th | 7th | 6th | 5th | 4th | 3rd | 2nd | 1st | LSB |
|---|---|---|---|---|---|---|---|---|---|
| | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |
| Positional Value | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | |

Positional value of bits is determined by 2 raised to power (position - 1), that is the value of a bit 1 at position 6 is $2^{(6-1)}$ that is $2^5$ that is 32 The total value of the octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below -

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Value |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 2 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 3 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 4 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 5 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 6 |
| | | | ⋮ | | | | | |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 255 |

- **$IPV_4$ - Address Classes:**

Internet protocol hierarchy contains several classes of IP addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the $IPV_4$ addressing system is divided into five classes of IP addresses. All the five classes are identified by the first octet of IP Address.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP address.

1st octet, 2nd octet, 3rd octet, 4th octet

11000000 . 10101000 . 00000001 . 10011000

192 . 168 . 1 . 152

The number of networks and the number of hosts per class can be derived by this formula

Number of networks = 2^network_bits

Number of host/network = 2^host_bits - 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, ie. the first IP of a network is network number and the last IP is reserved for broadcast IP.

→ Class A Address:

The first bit of the first octet is always set to 0. Thus the first octet ranges from 1-127 ie 00000001 - 01111111

1 - 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for class A IP address is 255.0.0.0 which implies that class A addressing can have 126 networks ($2^7 - 2$) and 16777214 hosts ($2^{24} - 2$).

Class A IP address format is thus:

ONNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

## Class B Address:

An IP address which belongs to class B has the first two bits in the first octet set to 10 ie

10000000 - 10111111
128 - 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for class B is 255.255.x.x.

Class B has 16384 ($2^{14}$) Network addresses and 65534 ($2^{16}-2$) Host addresses

Class B IP address format is

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

## ⇒ Class C Address:

The first octet of class C IP address has its first 3 bits set to 110 that is:

11000000 - 11011111
192 - 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for class C is 255.255.255.x

Class C gives 2097152 ($2^{21}$) Network addresses and 254 ($2^8-2$) Host addresses.

Class C IP address format is:

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

→ Class D Address:

Very first four bits of the first octet in class D IP addresses are set to 1110, giving a range of -

11100000 - 11101111
224 - 239

Class D has IP address range from 224.0.0.0 to 239.255.255.255. class D is reserved for multicasting. In multicasting data is not destined for a particular host that is why there is no need to extract host address from the IP address and class D does not have any subnet mask.

→ Class E Address:

This IP class is reserved for experimental purposes only for study. IP addresses in this class ranges for 240.0.0.0 to 255.255.255.254 Like class D, this class too is not equipped with any subnet mask.

## 3.4 Subnetting:

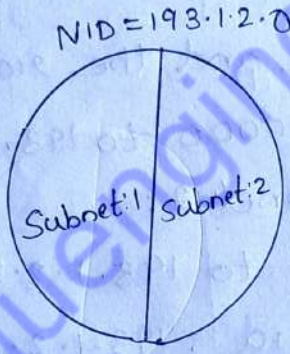
Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of networks and prefixed number of hosts per network.

Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more networks per IP class.

CIDR or classless inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as network in network called subnet. By using subnetting, one single class A IP address can be used to have smaller subnetworks which provide better network management capabilities.

"When a bigger network is divided into smaller networks, to maintain security then that is known as subnetting".

To divide a network into two parts, you need to choose one bit for each subnet from the host ID part.




NID=193.1.2.00000000
Range=193.1.2.00000000
to
193.1.2.01111111

NID=193.1.2.1000000
Range=193.1.2.10000000
to
193.1.2.11111111

In the above diagram, there are two subnets.

"Note: It is a class C IP address, there are 24 bits in the network id part and 8 bits in the host id part"

Subnetting for a network should be done in such a way that it does not affect the network bits. In class C the first 3 octets are network bits so it remains as it is.

→ For subnet 1:

The first bit which is chosen from the host id part is zero and the range will be from

193.1.2.00000000 to 193.1.2.01111111 except for the first bit which is chosen zero for subnet id part. Thus the range of subnet 1:

193.1.2.0 to 193.1.2.127

∴ Subnet id of subnet 1 is : 193.1.2.0

Direct Broadcast id is : 193.1.2.127

Total number of host : 126 (out of 128 2 id's are used for subnet id & Direct broadcast id)

Subnet mask : 255.255.255.128

→ For Subnet 2: The first bit chosen from the host id part is one and the range will be from 193.1.2.10000000 to 193.1.2.11111111. Thus the range of subnet 2:

193.1.2.128 to 193.1.2.255

Subnet id : 193.1.2.128

Direct broadcast ID : 193.1.2.255

Total number of host : 126

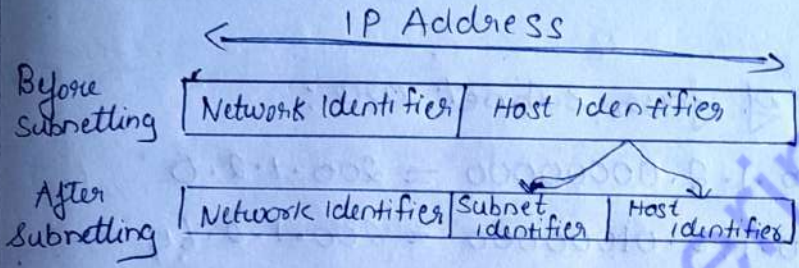
Subnet mask : 255.255.255.192

Finally after using the subnetting the total number of usable hosts are reduced from 254 to 252.

To divide a network into four ($2^2$) parts you need to choose two bits from the host id part for each subnet ie 00, 01, 10, 11

To divide a network into eight ($2^3$) parts you need to choose three bits from the host id part for each subnet ie 000, 001, 010, 011, 100, 101, 110, 111.

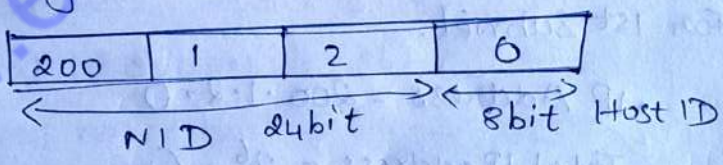
If the total number of subnet in a network increases the total number of usable hosts decreases.




Example 1:

Consider we have a big single network having IP address 200.1.2.0 we want to do subnetting and divide this network into 4 subnets.

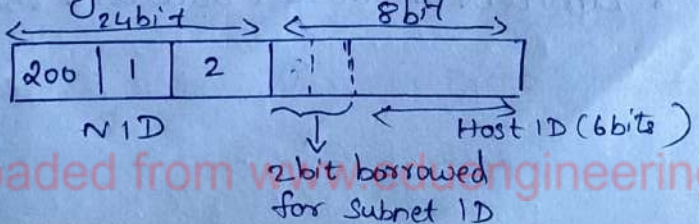
Clearly the given network belongs to class C.




For creating four subnets and to represent their subnets ID, we require 2 bits.

So,

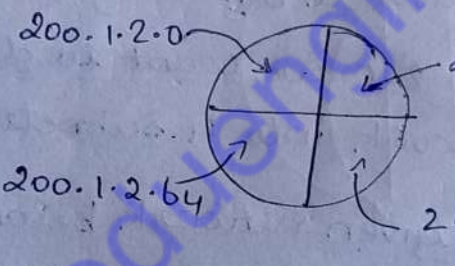
- We borrow two bits from the Host ID part
- After borrowing two bits, Host ID part remains with only 6 bits



- If borrowed bits = 00, then it represents 1st subnet
- If borrowed bits = 01, then it represents 2nd subnet
- If borrowed bits = 10, then it represents 3rd subnet
- If borrowed bits = 11, then it represents 4th subnet

IP address of four subnet are:

- 200.1.2.00000000 = 200.1.2.0
- 200.1.2.01000000 = 200.1.2.64
- 200.1.2.10000000 = 200.1.2.128
- 200.1.2.11000000 = 200.1.2.192




→ For 1st subnet:

- IP Address = 200.1.2.0
- Total IP address = $2^6 = 64$
- Total number of host = 64 − 2 = 62
- Range of IP address = 200.1.2.00000000 to 200.1.2.00111111
  ie 200.1.2.0 to 200.1.2.63
- Direct broadcast address = 200.1.2.63
- Limited broadcast address = 255.255.255.255

→ for 2nd Subnet

- IP address = 200.1.2.64
- Total IP address = $2^6 = 64$
- Total no: of host = 64-2 = 62
- Range = 200.1.2.01000000 to 200.1.2.01111111
  ie; 200.1.2.64 to 200.1.2.127
- Direct broadcast address = 200.1.2.127
- Limited broadcast address = 255.255.255.255

→ for 3rd Subnet

- IP address = 200.1.2.128
- Total IP address = $2^6 = 64$
- Total no: of host = 64-2 = 62
- Range = 200.1.2.10000000 to 200.1.2.10111111
  ie 200.1.2.128 to 200.1.2.191
- Direct broadcast address = 200.1.2.191
- Limited broadcast address = 255.255.255.255

→ for 4th Subnet

- IP address = 200.1.2.192
- Total IP address = $2^6 = 64$
- Total no: of host = 64-2 = 62
- Range = 200.1.2.11000000 to 200.1.2.11111111
  ie 200.1.2.192 to 200.1.2.255
- Direct broadcast address = 200.1.2.255
- Limited broadcast address = 255.255.255.255

Disadvantages of Subnetting.

1. Subnetting leads to loss of IP addresses
2. Subnetting leads to complicated communication process.

## 3.5 IPV6

IPV6 is a network layer protocol that allows communication to take place over the network.

IPV6 is designed to overcome the shortfalls of the IPV4

Some advantages of IPV6 over IPV4 are mentioned below:

1. Addressspace : IPV6 has a 128 bit long address which is larger than IPV4
2. Header format: IPV6 has a new header format in which options are separated from the base header and inserted between the base header and upper layer data.
3. Extension: IPV6 is designed to allow the extension of the protocol, if required for new applications.
4. Security: Encryption and authentication mechanism provides confidentiality and integrity to the packets in IPV6

- IPV6 Addresses

A new notation has been devised for writing 16 byte addresses. They are written as eight groups of four hexadecimal digits with colons between the group like this

8000:0000:0000:0000:0123:4567:89AB:CDEF

Leading zeros within a group can be omitted so 0123 can be written as 123.

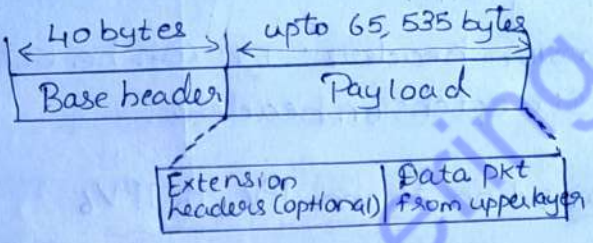
One or more groups of 16 zero bits can be replaced by a pair of colons. The address now becomes 8000::123:4567:89AB:CDEF

## IPV6 Packet format:

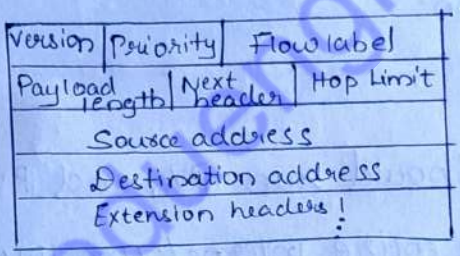
Each packet is composed of a mandatory base header followed by the payload.

The payload consists of two parts optional extension headers and data from an upper layer.

The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information




### -> Base header




Version: This 4bit field defines the version number of the IP

Priority: This 4bit priority field defines the priority of the packet.

Flow label: The flow label is a 3byte (24bit) field used for control the flow of data

Payload length: The 2byte payload length field defines the length of the IP datagram excluding the base header

Next header: The next header is an 8bit field defining the header that follows the base header in the datagram.

Hop limit: This 8bit hop limit field used to indicati life time of the packet

Source address: The source address field is a 16byte (128bit) internet address that identifies the original source of the datagram

Destination address: The destination address field is a 16byte (128bit) internet address that usually identifies the final destination of the datagram.

Extension headers: It can be extended upto six extension headers.

- Transition from $IPV_4$ to $IPV_6$

Three strategies have been invented by IETF (Internet Engineering Task force) to help the transition:

1. Dual Stack

The host should run $IPV_4$ and $IPV_6$ simultaneously until the entire internet uses $IPV_6$. The source host queries the DNS to determine which version can be used at the time of sending a packet to destination. If DNS returns an IPV6 address, the source host sends an IPV6 Packet

2. Tunneling

When two computers uses IPV6 and want to communicate with each other and the packet passes through a region that uses $IPV_4$, it is called Tunneling. The $IPV_6$ packet is encapsulated in an $IPV_4$ packet, when it enters the region. It leaves the capsule when it exits the region

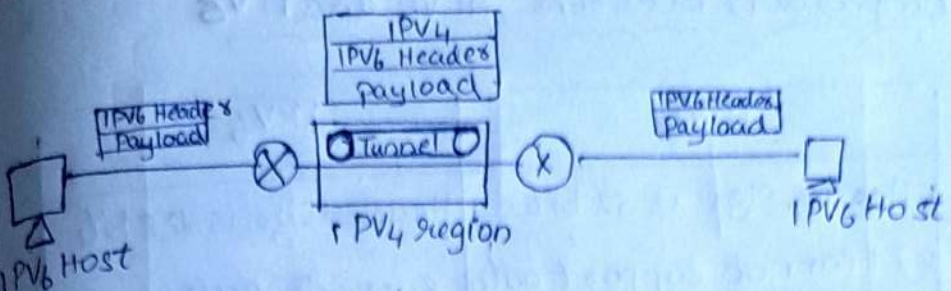
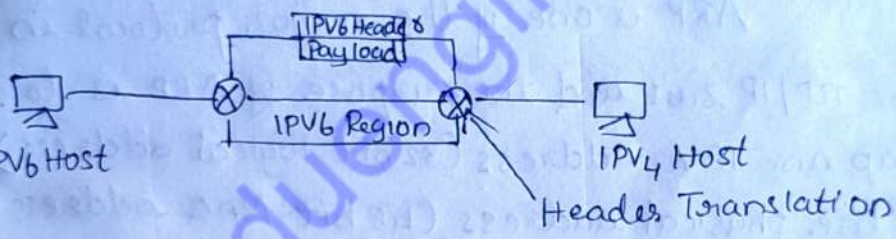



Fig: Tunneling

3. Header Translation:

It is used when some of the systems use the IPV4 and the sender wants to use IPV6 but the receiver does not understand IPV6.

The header format should be totally changed through header translation. The header of the IPV6 packet is converted to an IPV4 header




Header Translation procedure

1. Change the IPV6 mapped address to an IPV4 address by extracting the rightmost 32 bits
2. Discard the value of IPV6 Priority field
3. Set the type of service field in IPV4 to be zero
4. Calculate the checksum for IPV4 and insert in the corresponding field.
5. Ignore the IPV6 flow label
6. Convert the compatible extension headers to options and insert them in the IPV4 header
7. Calculate the length of IPV4 header and insert it into the corresponding field
8. Eventually compute the total length of the IPV4 packet and insert it into the corresponding field.

## Comparison between IPV4 and IPV6

| IPV4 | IPV6 |
|---|---|
| 1. Header Size is 32 bits | Header size is 128 bits |
| 2. It cannot support auto configuration | Supports auto configuration |
| 3. Cannot support real time application | Supports real time application |
| 4. No security at network layer | Provides security at network layer |
| 5. Throughput and delay is more | Throughput and delay is less |

## 3.6 ARP (Address Resolution Protocol)

ARP is one of the major protocol in the TCP/IP suit and the purpose of ARP is to map an IPV4 address (32 bit logical address) to the physical address (48 bit MAC address)

Networks applications at the application layer use IPV4 address to communicate with another device. But at the data link layer, the addressing is MAC address and this address is burned into network card permanently.

The purpose of ARP is to find out the MAC address of a device in your LAN for the corresponding IPV4 address, which network application is trying to communicate

Types of mapping

- static mapping
- Dynamic mapping

• Static mapping

Static mapping means creating a table that associates a logical address with a physical address. This table is stored in each machine on the network. Each machine that knows (for example, the IP address of another machine but not its physical address) can look it up in the table.

This has some limitations because physical addresses may change in the following ways:

1. A machine could change its NIC, resulting in a new physical address
2. In some LANs the physical address changes every time the computer is turned on.
3. A mobile computer can move from one physical network to another, resulting in a change in its physical address.

To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance.

• Dynamic Mapping

Here, each time a machine knows the logical address of another machine, it can use a protocol to find the physical address. Two protocols have been designed to perform dynamic mapping

→ ARP (Address resolution Protocol)
→ RARP (Reverse Address Resolution Protocol)

ARP maps a logical address to a physical address
RARP maps a physical address to a logical address.

## ARP Packet format

| Hardware Type | | Protocol type |
|---|---|---|
| Hardware Length | Protocol length | Operation Request 1, Reply 2 |
| Sender hardware address (for example, 6 bytes for Ethernet) | | |
| Sender protocol address (for example, 4 bytes for IP) | | |
| Target Hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request | | |
| Target protocol address For example, 4 bytes for IP | | |

The fields in the Address resolution Protocol (ARP) message format are:

Hardware Type: Specifies the type of hardware used for the local network transmitting the ARP message. Ethernet is the common hardware Type and the value for ethernet is 1. The size of this field in 2 bytes.

Protocol type: Each protocol is assigned a number used in this field. IPV4 is 2048 (0x0800 in Hexa)

Hardware Address Length: is length in bytes a hardware (MAC) address. Ethernet MAC addresses are 6 bytes long.

Protocol Address Length: Length in bytes of a logical address (IPV4 address). IPV4 addresses are 4 bytes long.

Operation: Specifies the nature of the ARP message for 1. ARP request and 2. ARP reply.

Sender Hardware Address: address of the device sending the message.

Sender protocol address: The protocol address (IPV4 address) of the device sending the message.

Target Hardware Address: MAC address of the intended receiver. This field is ignored in requests.

Target Protocol Address: The protocol address (IPV4 address) of the intended receiver.

## Encapsulation

An ARP packet is encapsulated directly into a data link frame. For example, in figure an ARP packet is encapsulated in an ethernet frame. The type field indicates that the data carried by the frame is an ARP Packet

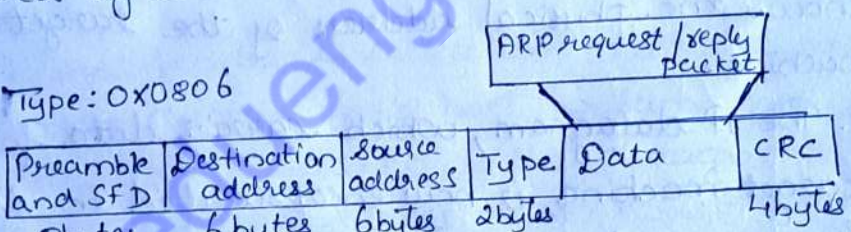



Fig: Encapsulation of ARP Packet

## Operation:

There are seven steps involved in an ARP process:

1. The Sender knows the IP address of the target.
2. IP Asks ARP to create as ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0's.

3. The message is passed to the data link layer where it is encapsulated in a frame using the physical address of the sender as the source address and the physical broadcast address as the destination address.

4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes the IP address.

5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.

6. The sender receives the reply message. It now knows the physical address of the target machine.

7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

■ Four Different cases:

The following are four different cases in which the services of ARP can be used.

Case 1: The sender is a host and wants to send a packet to another host on the same network. In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.

Case 2: The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination. If it does not have a routing table, it looks for the IP address of the default router. The IP address of the router becomes the logical address that must be mapped to a physical address.

Case 3: The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of next router. The IP address of the next router becomes the logical address that must be mapped to a physical address.

Case 4: The sender is a router that has received a datagram destined for a host in same network. The destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

## 8.7 RARP (Reverse Address Resolution Protocol)

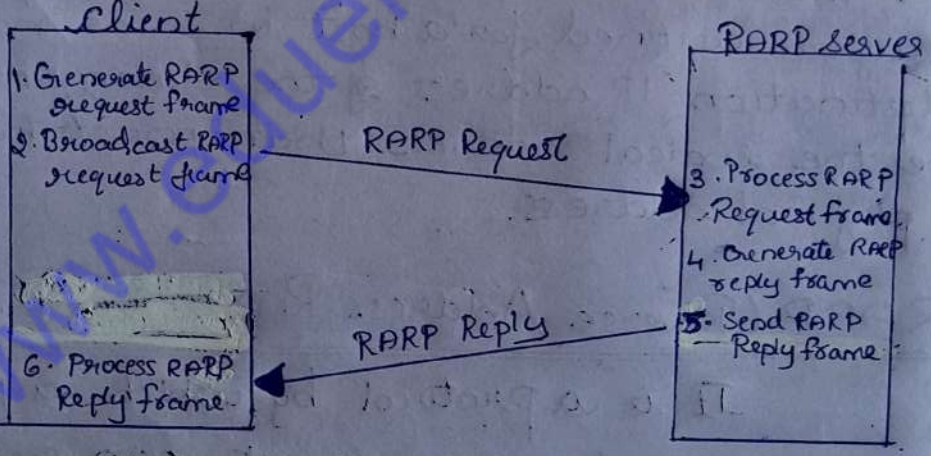
It is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache.

A network administrator creates a table in a local area networks gateway router that maps the physical machine (MAC address) to corresponding Internet protocol addresses.

When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router's table, the RARP server will return the IP address to the machine which can store it for future use.

There are four types of arp messages that may be sent by the arp protocol. These are identified by four values in the operation field of an arp message. The type of message are:

1. ARP request
2. ARP reply
3. RARP request
4. RARP reply




1. Source device generates RARP request message:

The source device generates an RARP request message. Thus it uses the value 3 for the opcode in the message. It puts its own data link layer address as both the sender hardware address and also

Target hardware address. It leaves both the sender protocol address and the target protocol address blank, since it doesn't know either.

2. Source device broadcast RARP request message:

The source broadcasts the ARP request message on the local network.

3. Local Devices process RARP request message

The message is received by each device on the local network and processed. Devices that are not configured to act as RARP servers ignore the message.

4. RARP Server generates RARP reply message

Any device on the network that is setup to act as an RARP server responds to the broadcast from the source device. It generates an RARP reply using an opcode value of 4

5. RARP server sends RARP reply message:

The RARP server sends the RARP reply message unicast to the device looking to be configured.

6. Source Device processes RARP reply message:

The source device processes the reply from the RARP server. It then configures itself using the IP address in the target protocol address supplied by the RARP server. It is possible that more than one RARP server may respond to any request, if two or more are configured on any local network. The source device will typically use the first reply and discards the others.

## 3.7 ICMP (Internet Control Message Protocol)

The ICMP is the protocol that handles error and other control message. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. ICMP messages are encapsulated by IP Packets.

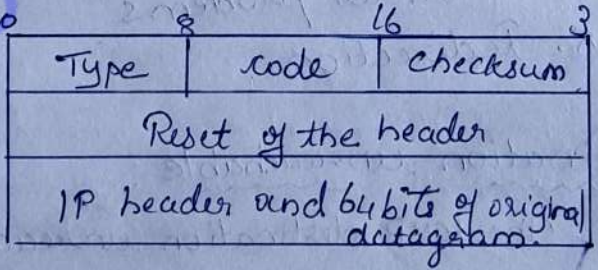
### 3.7.1 Message Types:

All ICMP messages fall in the following classes: 1. Error reporting
2. Query

Error reporting messages report problems that a router or a host may encounter when it processes an IP Packet.

The query messages, which occurs in pairs, help a host or a network manager specific information from a router or another host.

### 3.7.2 Message Format:




The above figure shows the basic error message format. An ICMP message is encapsulated into the data field of an IP Packet. An ICMP header is 8 bytes long and a variable size data section

1. Type: It is a 8 bit field identifies the type of the message.

2. Code: Size of the code field is 8 bits. It provides the information of the message type

3. Checksum: This 16 bit field is used to detect errors in the ICMP messages.

4. IP header and original datagram: This field can be used for diagnostic purposes by matching the information in the ICMP message with the original data in the IP Packet

### 3.7.3 Error reporting

ICMP does not correct errors it simply reports them. ICMP handles five types of errors

1. Destination unreachable
2. Source quench
3. Time exceeded
4. Parameter problems
5. Redirection

#### 1. Destination unreachable:

The ICMP destination unreachable message is sent by a router in response to a packet which it cannot forward because the destination is unreachable or a service is unavailable.

| Type: 3 | Code: 0 to 5 | Checksum |
|---|---|---|
| unused (All 0s) | | |
| Part of the received IP datagram including IP header plus first 8 bytes of datagram data | | |

Fig: Destination unreachable format

Code field: The code field is used by the different message formats to indicate specific error conditions.

For destination unreachable, the code field is:

0 = Net unreachable
1 = Host unreachable
2 = Protocol unreachable
3 = Port unreachable
4 = Fragmentation needed and DF set
5 = Source route failed.

2. Source Quench:

ICMP source quench messages to report congestion to the original source. A source quench message is a request for the source to reduce its current rate of datagram transmission

| Type: 4 | code: 0 | Checksum |
|---|---|---|
| unused (All 0s) | | |
| Part of the received IP datagram including IP header Plus the first 8 bytes of datagram data | | |

Fig: Source Quench format

3. Time exceeded message:

| Type: 11 | code 0 or 1 | Checksum |
|---|---|---|
| unused (All 0s) | | |
| Part of the received IP datagram including IP header plus the first 8 bytes of datagram data. | | |

Fig: Time exceeded message format

Code field:

0 = Time to live exceeded in transit
1 = Fragment reassembly time exceeded.

4. Parameter Problem:

The parameter problem message identifies the octet of the original datagram's header where the error was detected.

| Type: 11 | code: 0 or 1 | checksum |
|---|---|---|
| Pointer | unused (All 0s) | |
| Part of the received IP datagram including IP header plus the first 8 bytes of datagram data | | |

Fig: Parameter Problem message format

Code field: The code field is 0 when the pointer field indicates the error

5. Redirection:

| Type: 5 | code: 0 or 3 | checksum |
|---|---|---|
| IP address of the target router | | |
| Part of the received IP datagram including IP header plus the first 8 bytes of datagram data | | |

Fig: Redirection message format

Code field:

0 = Redirect datagrams for the network
1 = Redirect datagrams for the host
2 = Redirect datagrams for the type of service and network
3 = Redirect datagrams for the type of service and host

## 3.7.4 Query

ICMP query messages are of four types

1. Echo request and reply
2. Timestamp request and reply
3. Address-mask request and reply
4. Router solicitation and advertisement

## 1. Echo request and reply

The echo request and echo reply messages can be used to determine if there is communication at the IP level.

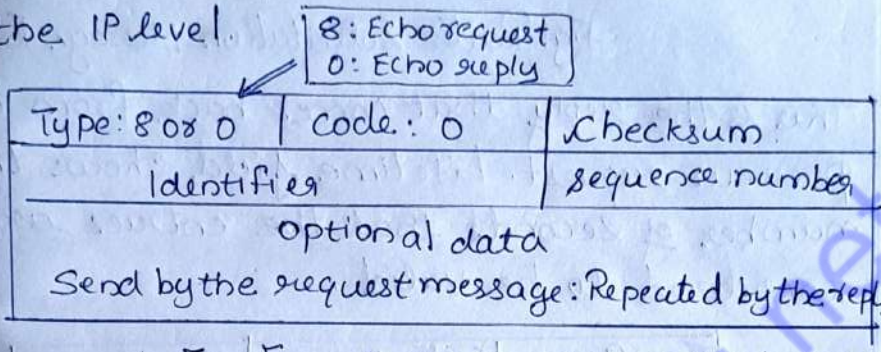
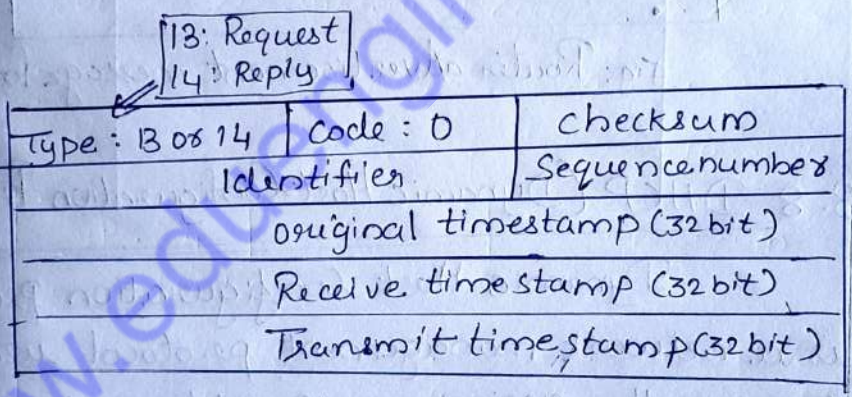



Fig: Format of echo request & reply messages

## 2. Timestamp Request and Reply

used to calculate the round trip time between a source and destination machine




## 3. Address Mask request and reply message

The address mask request is used by a host to determine what its address mask is on a network. The address mask reply message is the reply from a router or a host to the source host with the correct address mask for the network

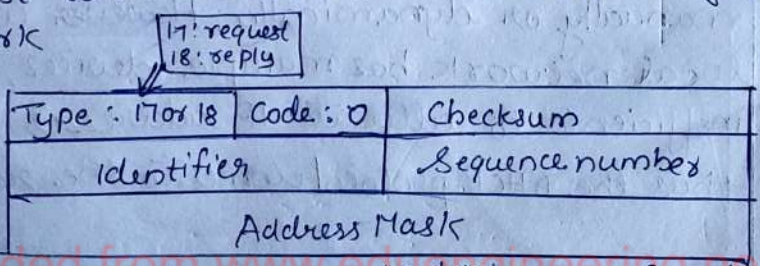



Fig: Mask request and reply message format

4. Router Solicitation and Advertisement

| Type: 10 | Code: 0 | Checksum |
|---|---|---|
| Identifier | | Sequence number |

Fig: Router Solicitation Message format

This is the reply that comes back from the previous request. Lifetime field shows the number of seconds that the entries are considered to be valid.

| Type: 9 | Code: 0 | Checksum |
|---|---|---|
| Number of addresses | Address entry size | Lifetime |
| Router address 1 | | |
| Address Preference 1 | | |
| Router address 2 | | |
| Address Preference 2 | | |
| ⋮ | | |

Fig: Router advertisement message format

## 3.8 DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol is a network management protocol used to dynamically assign an IP address to devices connected to the network using a client / server architecture.

When new devices appear on the network, they receive unique IP addresses. The addresses can be assigned by the network administrator manually or dynamically. However when the local network has multiple devices, it becomes inefficient to allocate IP addresses by hand. Thus the DHCP protocol comes to the rescue

On residential network, router is a DHCP server that uses DHCP to assign IPs and send important information.

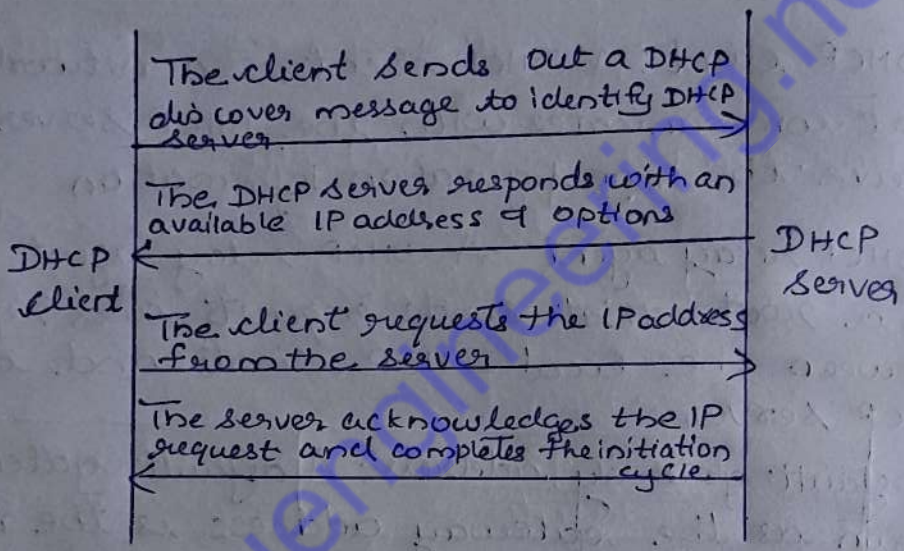
### 3.8.1 Components of DHCP Server:

- DHCP Server: A DHCP server can be either a server, dedicated computer or router that manages network configuration information including IP addresses
- DHCP client: A DHCP client is a network device that communicates with the DHCP server to receive the configuration information
- DHCP relay agent: A DHCP relay agent is a host or a router that sends requests and replies between the local DHCP clients and a remote DHCP server.
- Default gateway address: A default gateway, also known as the gateway address, is the node that forwards information between local networks or subnets and the internet
- IP address pool: An IP address pool is a list of all IPs that are available for allocation.
- Subnet mask: Subnet masks are the segments of an IP address. IP addresses are divided into subnet masks to differentiate between network and host bits. Thus, a subnet mask allows a host to determine the exact network it currently exists in
- DHCP options: DHCP has numerous configuration which are called options. Some of the more common DHCP options include:
  - option 3 (router option)
  - option 6 (DNS server option)

- option 33 (Static route option)
- option 51 (IP address lease option)

- Lease Time: The lease time defines the period, during which the client can use the IP address that was assigned to it

## 3.8.2 DHCP Handshake:




## 3.8.3 Static Vs Dynamic DHCP leases:

With Dynamic DHCP, a client does not own the IP address assigned to it but instead leases it for a period of time. Each time a device with a dynamic IP address is powered up, it must communicate with the DHCP server to lease another IP address.

Wireless devices are examples of clients that are assigned dynamic IP addresses when they connect to a network.

On the other hand, static devices such as web servers and switches are assigned permanent IP addresses.

### 3.8.4 DHCP uses and functions :

1. Used to distribute IP addresses within a network.
2. Prevent IP conflict.
3. Updates IP address automatically.
4. Supports IP address Reuse

## Problems

1. Change the following IPV4 addresses from binary notation to dotted-decimal notation
   a) 10000001 00001011 00001011 11101111
   b) 11000001 10000011 00011011 11111111

2. Change the following IPV4 addresses from dotted-decimal notation to binary notation.
   a) 111.56.45.78
   b) 221.34.7.82

3. Find the class of each address
   a) 00000001 00001011 00001011 11101111
   b) 11000001 10000011 00011011 11111111
   c) 14.23.120.8
   d) 252.5.15.111

For example 11100000, the number of 1s gives us $2^3$ subnets. In this example there are 8 subnets.

2. **How many host per subnet ?**

Number of host per subnet = $2^y - 2$

Where y is the number of unmasked bits or the 0s (zeros)

For example 11100000, the number of 0s gives us $2^5 - 2$ hosts. In this example there are 30 hosts per subnet. Your need to subtract 2 for subnet address and the broadcast address.

3. **What are the valid subnets?**

For valid subnet = 256 – Subnet mask = Block size. An example would be 256 – 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96, 128, 160, 192, 224.

4. **What is the broadcast address for each subnet ?**

Our subnets are 0, 32, 64, 96, 128, 160, 192, 224, the broadcast address is always the number right before the next subnet. For example, the subnet 0 ha a broadcast address of 31 because next subnet is 32. The subnet 32 has a broadcast address of 63 because next subnet is 64.

5. **What are the valid hosts ?**

Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 32 is the subnet number and 63 is the broadcast address, then 32 to 63 is the valid host range. It is always between the subnet address and the broadcast address.

**Example 3.3.2** What is the sub-network address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0 ?

**Solution**: Using AND operation, we can find sub-network address,

1. Convert the given destination address into binary format:

   200.45.34.56 =>11001000 0010110100100010 00111000

2. Convert the given subnet mask address into binary format:

   255.255.240.0 =>11111111 1111111111110000 00000000

3. Do the AND operation using destination address and subnet mask address.

   200.45.34.56 =>11001000 0010110100100010 00111000

   255,255.240.0 => 11111111 1111111111110000 00000000

   ---

   11001000 0010110100100000 00000000

**Subnet work address is 200.45.32.0**

**Example 3.3.2** For a network address 192.168.10.0 and subnet mask 255.255.255.224 then calculate:

i) Number of subnet and number of host

ii) Valid subnet

**Solution:** Given network address 192.168.10.0 is class C address. Subnet mask address is 255.255.255.224. Here three bits is browse for subnet.

i) **Number of subnet and number of host**

255.255.255.224 convert into binary =>11111111 11111111 11111111 11100000

Number or subnet = $2^x = 2^3 = 8$

So there are 8 subnet.

Number of host per subnet = $2^y - 2 = 2^5 - 2 = 30$

ii) **Valid subnets**

For valid subnet = 256 - Subnet mask = Block size. An example would be 256 - 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96,128,160,192, 224.

**Example 3.3.3**Find the sub-network address for the fallowing;

| Sr. No. | IP address | Mask |
|---|---|---|
| a) | 140.11.36.22 | 255.255.255.0 |
| b) | 120.14.22.16 | 255.255.128.0 |

**Solution**

a) IP address Mask

140.11.36.22 255.255.255.0

The values of mask (i.e. 255.255.255.0) is boundary level. So

IP address 140.11.36.22

Mask 255.255.255.0

140.11.36.0

b) IP address 140.11.36.22

Mask 255.255.128.0

**Example 3.3.4**Find the sub-network address for the fallowing;

| Sr. No. | IP address | Mask |
|---|---|---|
| a) | 141.181.14.16 | 255.255.224.0 |
| b) | 200.34.22.156 | 255.255.255.240 |
| c) | 125.35.12.57 | 255.255.0.0 |

**Solution**

a)

141.181.14.16 IP address

255.255.224.0 Mask

141.181.0.0 Sub-network address

b)

| | |
|---|---|
| 200.34.22.156 | IP address |
| 255.255.255.240 | Mask |
| 200.34.22.144 | Sub-network address |

c)

| | |
|---|---|
| 125.35.12.57 | IP address |
| 255.255.0.0 | Mask |
| 125.35.0.0 | Sub-network address |

(i.e. 128) So for byte-3 value use bite-wise AND operators. It is shown below.

| | |
|---|---|
| 120.14.22.16 | IP address |
| 255.255.128.0 | Mask |
| 125.14.0.0 | Sub-network address |

In the above example, the bite wise ANDing is done in between 22 and 128. It is as follows.

| | | |
|---|---|---|
| 22 | Binary representation | 0 0 0 1 0 1 1 0 |
| 128 | Binary representation | 1 0 0 0 0 0 0 0 |
| 0 | | 0 0 0 0 0 0 0 0 |

Thus the sub-network address for this is 120.14.0.0.

**Example 3.3.5** Finde the class of the following address.

a) 1.22.200.10 b) 241.240.200.2 c) 227.3.6.8 d) 180.170.0.2

**Solution:**

a) 1.22.200.10 Class A IP address

b) 241.240.200.2 Class E IP address

c) 227.3.6.8 Class D IP address

d) 180.170.0.2 Class B IP address

**Example 3.3.6**Find the retid and Hositd for the following.

a) 19.34.21.5 b) 190.13.70.10 c) 246.3.4.10 d) 201.2.4.2

**Solution**

a) netid => 19 Hostid => 13.70.10

b) netid => 190.13 Hostid => 70.10

c) No netid and No Hostid because 246.3.4.10 is the class E address.

d) netid =>201.2.4 Hostid =>2

**Example 3.3.7:** Consider sending a 3500 - byte datagram that has arrived at a router $R_1$that needs to be sent over a link that has an MTU size of 1000 bytes to $R_2$. Then it has to traverse a link with an MTU of 600 bytes. Let the identification number of the original datagram be 465.

How many fragments are delivered at the destination ? Show the parameters associated with each of these fragments.

**Solution:** The maximum size of data field in each fragment = 680 (because there are 20 bytes IP header). Thusthe number of required fragments) = [3500 - 20/680] - 5.11 ≃ 6.

Each fragment will have Identification number 465. Each fragment except the last one will be of size 700 bytes (including IP header). The last datagram will be of size 360 bytes (including IP header). The offsets of the4 fragments will be 0, 85, 70, 255. Each or the first 3 fragments will have flag=l; the last fragment will have flag=0.

**Example 3.10**

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a) The first group has 64 customers; each needs 256 addresses.

b) The second group has 128 customers; each needs 128 addresses.

c) The third group has 128 customers; each needs 64 addresses.

Design the sub blocks and find out how many addresses are still available after these allocations.

**Solution**

Figure 3.11 shows the situation.

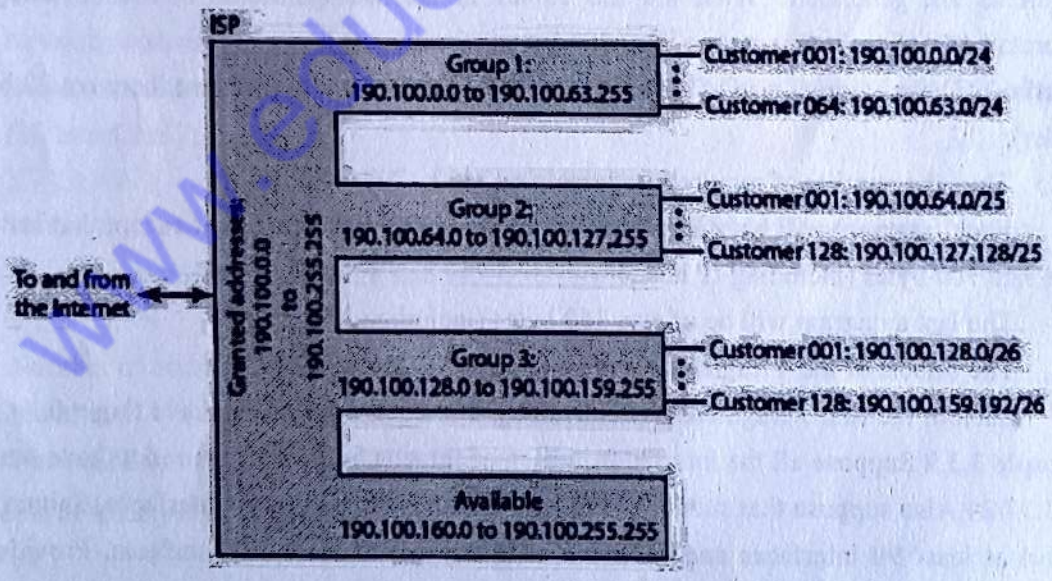



Fig 3.11 An example of address allocation and distribution by an ISP

1. Group 1

For this group, each customer needs 256 addresses. This means that 8 (log2256) bits are needed to define each host. The prefix length is then 32 - 8 =24. The addresses are

1st Customer: 190.100.0.0/24 100.0.255/24

2nd Customer: 190.100.1.0/24190 190.100.1.255/24

64th Customer: 190.100.63.0/24 190.100.63.255/24

Total =64 X 256 =16,384

2. Group2

For this group, each customer needs 128 addresses. This means that 7 (10g2 128) bits are needed to define each host. The prefix length is then 32 - 7 =25. The addresses are

3. Group3

For this group, each customer needs 64 addresses. This means that 6 (log2 64) bits are needed to each host. The prefix length is then 32 - 6 =26. The addresses are

1st Customer: 190.100.128.0/26 190.100.128.63/26

2nd Customer: 190.100.128.64/26 190.100.128.127/26

128th Customer: 190.100.159.192/26 190.100.159.255/26

Total =128 X 64 =8192

Number of granted addresses to the ISP: 65,536

Number of allocated addresses by the ISP: 40,960

Number of available addresses: 24,576

**Example 3.3.8**Consider sending a 2400-byte datagram into link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 422. How many fragments are generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation.

**Solution:** The maximum size of data field in each fragment = 680 (because there are 20 bytes IP header).

Thus the number of required fragments = (2400 - 20) / 680 =4

Each fragment will have Identification number 422. Each fragment except that last one to be of size 700 bytes (including IP header.

The last datagram will be of size 360 bytes (including IP header).

The offsets of the 4 fragments will be 0, 85, 170, 255.

Each of the first 3 fragments will have flag = 1; last fragment will have flag = 0.

**Example 3.3.9** Suppose all the interfaces in each of three subnets are required to have the prefix 223.1.17/24.Also suppose that subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces and subnet 3 is to support at least 22 interfaces. Provide three network addresses that satisfy these constraints.

**Solution:** The network address cannot be used for an interface (Network prefix + all zeros).

- The broadcast address cannot be used for an interface (Network prefix + all ones)

**Subnet 2 (90 interfaces)**

$2^n - 2 \geq 90$

Notice that we subtract 2 from the total number of available IP addresses because 2 IP addresses are reserved for the network and broadcast addresses.

$2^n \geq 92^n = 7$

Number of bits allocated to host part =n = 7

Number of bits allocated to network part = Pre filength = 32 - n = 32 - 7 = 25

The network address of the first subnet is always the address of the given address space.

Network address of first subnet = 223.1.17.0/25 = 223.1.17/25

To obtain the broadcast address of a subnet, we keep to network part of the subnet's network address as it is, and convert all bits in its host part to 1s.

Broadcast address of first subnet = 223.1.17.01111111 / 25 = 223.1.1.7.127/25

**Subnet 1 (60 interfaces)**

2n - 2 ≥ 60

Notice that we subtract 2 from the total number of available IP addresses because 2 IP addresses are reserved for the network and broadcast addresses.

$2^n \geq 60$ n =6

Number of bits allocated to host part = n = 6

Number of bits allocated to network part = Prefix length = 32 - n = 32 - 6 = 26 The network address of any subnet (that is NOT the first subnet) is obtained by adding one to the broadcast address of its preceding subnet.

Network address of second subnet = 223.1.17.128/26

Broadcast address of second subnet = 223.1.17.10111111/26 =223.1.17.191/26 Subnet 3 (12 interfaces) :

$2^n - 2 \geq 12$

Notice that we subtract 2 from the total number of available IP addresses because 2 IP addresses are reserved for the network and broadcast addresses.

$2^n \geq 14$ n = 4

Number of bits allocated to host part = n = 4

Number of bits allocated *to* network part = Prefix length = 32 - n = 32 - 4 = 28

Network address of third subnet = 223.1.17.192/28

c) 212.208.63.23 - Class C

d) 255.255.255.255 - Broadcast address.

**2 What is the purpose of the Address Resolution Protocol ?(May 11)**

**Ans:** ARP is a dynamic mapping method that finds a physical address for given a logical address, i.e. mapping IP address to physical address.

**3 Define an internetwork.**

**Ans:** A collection of interconnected networks is called an internetwork.

**4 Define geographic routing.**( May 10)

**Ans:** To decrease the size of the routing table even further, it necessary to extend hierarchical routing to include geographical routing. It divides the entire address space into a few large blocks.

**5 What is multicasting routing ?( May 18)**

**Ans:** Deliveryof information to a group of destinations simultaneously using themost efficient strategy to deliver the messages over each link of the network only once.

**6 What are the different kinds of multicast routing ?(May 11)**

**Ans:** Different kinds of multicast routing are reverse path multicasting and reverse path broadcasting.

**7 Define subnetting.( Dec 15)**

**Ans:** Subnetting is a technique that allows a network administrator to divide one physical network into smaller logical networks and thus, control the flow of traffic for security or efficiency reasons.

**8 What is multicast ? What is the motivation for developing multicast ?( May 11)**

**Ans:** Multicasting means delivering the same packet simultaneously to a group of clients. Motivation for developing multicast is that there are applications that want to send a packet to more than one destination hosts.

**9 What is the use of CIDR value in IP addressing ?**

**Ans:** Class C address's concept becomes meaningless on these routes between domains; the technique is call Classless Inter-domain Routing or CIDR. A key concept is to allocate multiple IP address in the way that allows summarization into a smaller number of routing table.

**10 Expand and define MTU.( May 12)**

**Ans:** MTU :. Maximum Transmission Unit. MTU is a networking term defines the biggest packet size that can be sent over a network connection.

**11. Compare the Ethernet address with IP address**

| Sr. No. | Ethernet Address | IP Addresses |
|---|---|---|
| 1. | Flat, i.e. switches look all the bits always. | Hierarchical, i.e., backbone routers may just look higher order bits. |
| 2. | Assigned by ethernet hardware vendor | Statically or dynamically assigned by |

| | | |
|---|---|---|
| | (Ethenet addresses are supposed to be unique) | ISP or IT managers. |
| 3. | No geographical nor organizational association (Convenient for small Networks) | Geographical or organizational association. |
| 4. | For example: 8-0-20-b-de-3e | For example: 172.16.16.1 |

**12. Define Routing? ( Dec 15)**

**Ans:** Routing is the process of selecting paths in a network through which network trafrfic is sent.

**13. Find the class of each address**

a) 00000001 00001011 00001011 11101111

b) 14.23.120.8

**Ans.** a) The first bit is 0. This is a class A address.

b) The first byte is 14 (between 0 and 127). This is a class A address

**14. What do you mean by unicast routing ?**

**Ans:** Unicast routing is a process of forwarding unicasted traffic from a source to destination on an Internet.

**15. What are the salient features of IPv6 ?( Dec 12)**

**Ans:** Salient features are :

a. Efficient and hierarchical addressing and routing infrastructure

b. IPv6 networks provide auto-configuration capabilities.

c. Improved security features.

d. Better support for QoS.

e. Large address space.

f. Stateless and stateful address configuration.

**16. Define source routing( Dec 13)**

**Ans:** All the information about the network topology is required to switch a packet across the network is provided by the source host. For switching that uses neithervirtual circuits nor conventional datagrams is known as source routing.

**17. What is the need of subnetting?(Dec 13)**

**Ans:** Subnetting divides one large networkinto several smaller ones. Subnetting adds an intermediate level of hierarchy in IP addressing.

**18. Define BGP. (Dec 14,17)**

**Ans:** Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed routing and reachability information between autonomous systems on the Internet.

**19. What are the metrics used by routing protocols ?(May 15)**

**Ans:** 1. Traffic matrices

2. Distance matrices

3. Adjacency matrices

4. Service matrices
5. Performance matrices

**20.Define VCI( Dec 16)**

**Ans:** VCI is an acronym for virtual channel identifier. VCI is a 16-bit field in ATMcell header that identities the cell's next destination as it travels through ATM network. VCI is used in conjunction with Virtual Path Identifier (VPI).

**21. What is fragmentation and reassembly (Dec 16)**

**Ans:** IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. Large datagram are fragmented (divided) i.e. one datagram becomes several datagram of small sizes. This process is called fragmentation. At final destination the datagrams are reassembled with the help of IP header bits.

**22. Give the comparison of unicast, multicast and broadcast routing.(Dec 16)**

**Ans:**

| Sr. No. | Unicast | Multicast | Broadcast |
|---|---|---|---|
| 1. | Unicast is a type of communication where a piece of information is sent from one point to another. | The information is sent from one or more points to set of other points. | The information is sent from one point to other points. |
| 2. | Only one sender and one receiver | One or more sender and set of receiver | One sender and several receivers. |

**23 How routers do differentiates the incoming unicast, multicast or broadcast IPpackets ?(May 17)**

**Ans:** The Ethernet network uses two hardware addresses which identify the source and destination of each frame sent by the Ethernet. The MAC destination address (all 1 s) is used to identify a broadcast packet (sent to all connected computers in a broadcastdomain) or a multicast packet (lsb of 1st byte=1) (received by a selected group of computers).

Routers are operating at layer 3. Router use IP addresses to make forwarding decisions. Each port on a router is a member of a different network. When a router receives traffic from one network, it uses the destination IP address to determine which port to forward.

**24. Differentiate between forwarding table and routing table. (Dec 17)**

**Ans:** Routing means finding a suitable path for a packet from sender to destination and Forwarding is the process of sending the packet toward the destination based on routing information.

**25 What are the benefits of Open Shortest Path First (OSPF) protocol ? (May 18)**

**Ans: Benefits**

1. Low traffic overhead
2. Support for complex address structures
3. Fast convergence

4. Good security. OSPF supports interface-based plain text and MD5 authentication.
5. Area based topology. Large OSPF networks are organized as a set of areas linked by a backbone.

**26. What is the network address in a class A subnet with the IP address of one of the hosts as 25.34.12.56 and mask 255.255.0.0 ? (May 14)**

**Ans:** 25.34.12.56
255.255.0.0
25.34.0.0
Network address is 25.34.0.0

**27. Expand ICMP and write the function.( May 16)**

**Ans:** ICMP stands for internet control message control.

**Functions of ICMP**

1) Error reporting 2) Rechability testing 3) Congestion control 4) Route change notification 5) Performance measuring 6) Subnet addressing

**28. When is ICMP redirect message used ?**( May 17)

**Ans**: The ICMP Redirect message is used to notify a remote host to send data packets on an alternative route. A host SHOULD NOT send an ICMP Redirect message, Redirects SHOULD only be sent by gateways.

The ICMP "redirect" message indicates that the gateway to which the host sent the datagram is no longer the best gateway to reach the net in question. The gateway willhave forwarded the datagram, but the host should revise its routing table to have a different immediate address for this net.

**29. Why is IPv4 to IPv6 transition is required ? (May 17)**

**Ans:** As publicly available IPv4 addresses have been exhausted. IPv4, the current internet protocol version has crossed 30 years of time period. The expanding user base and increased number of IP-enabled devices created a need for an upgraded version.

From mobile apps to non-traditional computing devices populating the Internet of Things, businesses rely on ITs ability to deliver new services to both end users and customers. But these services and the infrastructure used to support them require IP addresses and that means an IPv6 migration.

**30. Highlight the characteristics of datagram networks. (Dec 17)**

**Ans:** Characteristics of datagram networks are as follows :

a. Host can send a packet anywhere at any time.
b. Each packet is forwarded independently.
c. Link failure would not have any serious effect on communication if it is possibleto find an alternate route around the failure and update the forwarding tableaccordingly.

**31 Check whether the following IPv6 address notations are correct ? (Dec 18)**

a) **: : OF53:6382:AB00:67DB:BB27:7332.**

b) **7803:42F2:::88EC-D4BA:B75D:11CD**

**Ans:** a) : : OF53:6382:AB00:67DB:BB27:7332 : Correct

b) 7803:42F2:::88EC-D4BA:B75D:11CD : Incorrect because of two many (:)

**Prepared by** **Verified by** **Approved by**

# EDU ENGINEERING

PIONEER OF ENGINEERING NOTES

## TAMIL NADU'S BEST EDTECH PLATFORM FOR ENGINEERING

**CONNECT WITH US**

**WEBSITE:** www.eduengineering.net

**TELEGRAM:** @eduengineering

**INSTAGRAM:** @eduengineering

- **Regular Updates for all Semesters**
- **All Department** Notes AVAILABLE
- **Handwritten** Notes AVAILABLE
- **Past Year** Question Papers AVAILABLE
- **Subject wise** Question Banks AVAILABLE
- **Important Questions** for Semesters AVAILABLE
- Various **Author Books** AVAILABLE