UNIT III

WIRELESS LAN

by Prajith Prakash Nair

IEEE 802.11: MAC Sub layer

MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation. The basic services provided by MAC are the mandatory asynchronous data service and an optional time-bounded service.There are two main MAC sub layers available in IEEE 802.11

i) **Distributed Coordination Function (DCF)**

ii) **Point Coordination Function (PCF)**

DCF uses CSMA/CD as access method .It only offers asynchronous service. PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

MAC Frame:

The MAC layer frame consists of 9 fields as shown in the figure below.

FRAME CONTROL	Duration ID	Address 1	Address 2	Address 3	SC	Address 4	Data	CRC

1) Frame Control

It is 2 bytes long field which defines type of frame and some control information. There are various fields present in FC as shown in the diagram.

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mnmnt	More date	WEP	ORDER

1. **Protocol Version:**
   It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.

2. **Type:**
   It is a 2 bit long field which determines the function of frame i.e management(00), control(01) or data(10). The value 11 is reserved.

3. **Subtype:**
   It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.

4. **To DS:**
   It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).

5. **From DS:**
   It is a 1 bit long field which when set indicates frame coming from DS.

6. **More frag (More fragments):**
   It is 1 bit long field which when set to 1 means frame is followed by other fragments.

7. **Retry:**
   It is 1 bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.

8. **Power Mgmt (Power management):**
   It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.

9. **More data:**
   It is 1 bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode

that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.

10. **WEP:**
    It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.

11. **Order:**
    It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

2) Duration / ID

It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in µs).

3) Address 1 to 4

These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.

4) SC

It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.

5) Data

It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s)

6) CRC

It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

IEEE 802.11 Addressing Mechanism

There are 4 main cases by which the addressing mechanism operates with the help of To DS and From DS fields in the Frame Control. Each flag can either be a 0 or 1, resulting in the 4 cases which is interpreted in the 4 address fields as shown in the diagram.

TO DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

IEEE 802.11 Physical Layer

Since the IEEE 802.11 standard deals with wireless connection the OSI model mainly deals with the 2 lowest levels of the model (Physical and DLL).The main difference in the standard is in its physical layer which defines the electrical and physical specification for the devices.The Physical layer is divided into three sublayers :

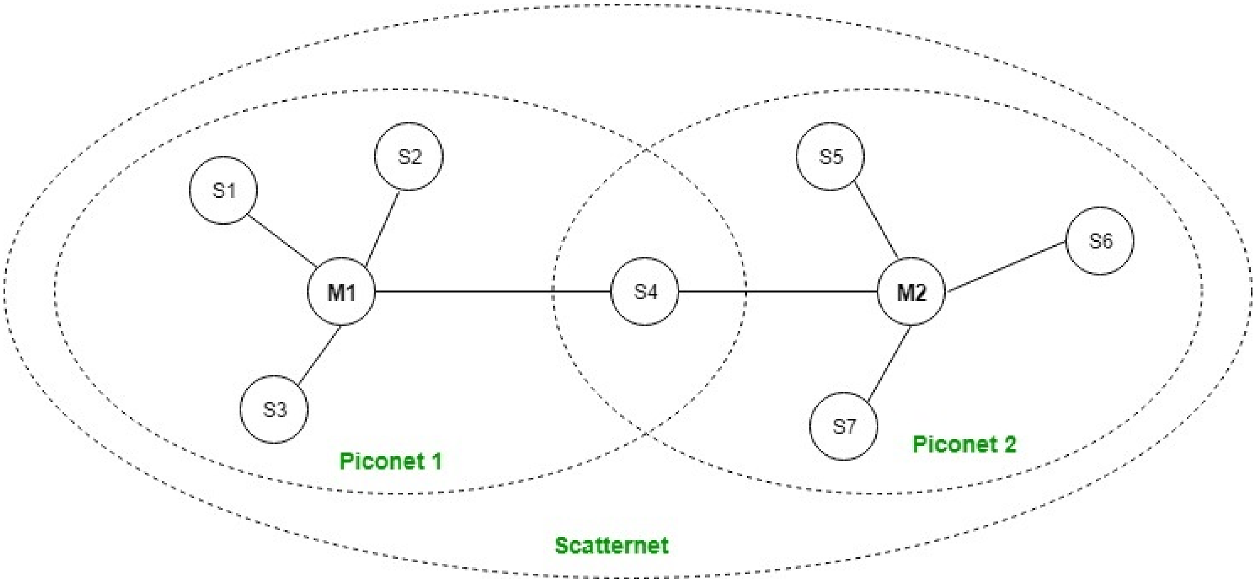
1) Physical Layer Convergence Protocol (PLCP)
2) Clear Channel Assessment (CCA)
3) Physical Medium Dependent (PMD)

PLCP	PHY Management
PMD	

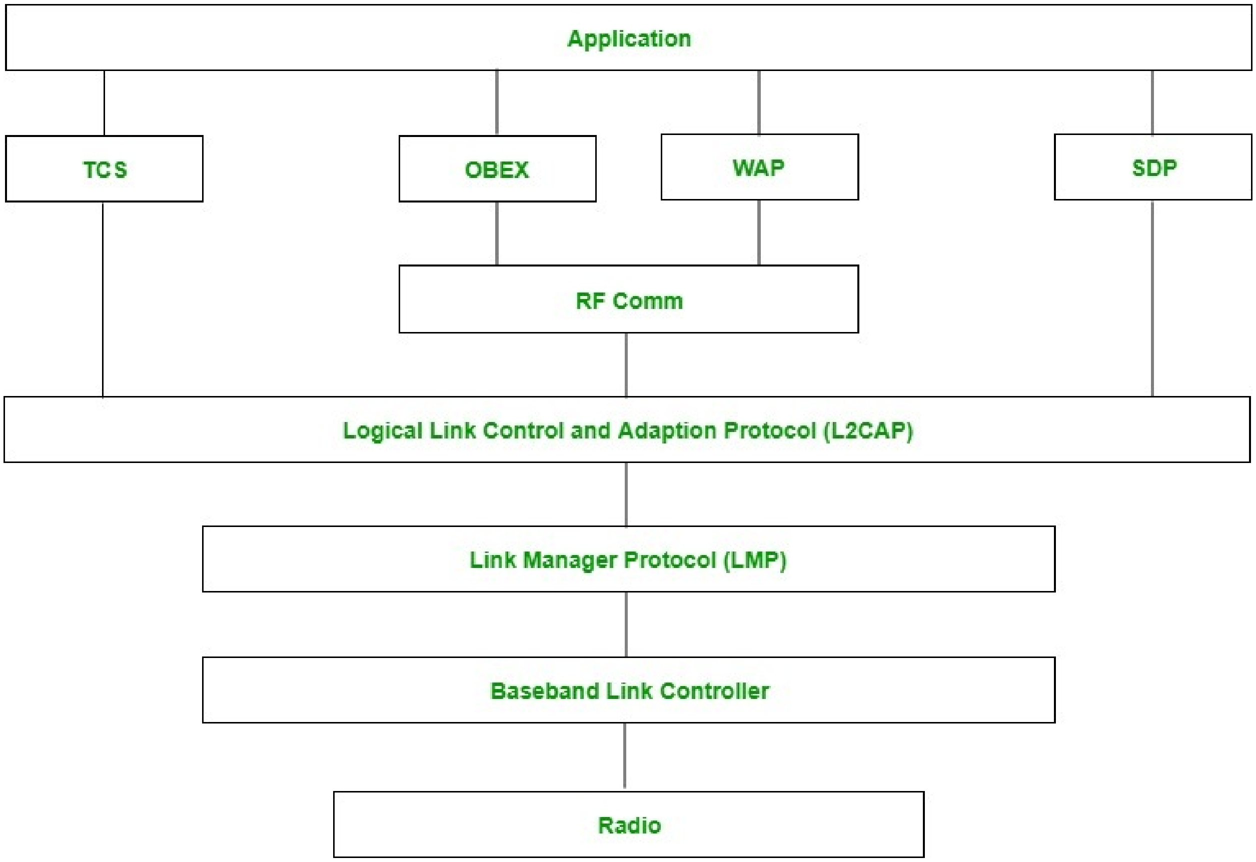
Bluetooth

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version and uses FHSS (Frequency hopping spread spectrum) for transmission. A bluetooth network is called piconet and a collection of interconnected piconets is call scatternet.

Bluetooth Architecture :



Bluetooth Protocol stack :


Application
TCS
OBEX
WAP
SDP
RF Comm
Logical Link Control and Adaption Protocol (L2CAP)
Link Manager Protocol (LMP)
Baseband Link Controller
Radio

1. **Radio (RF) layer:**

   It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of bluetooth transceiver. It defines two types of physical link: connection-less and connection-oriented.

2. **Baseband Link layer:**

   It performs the connection establishment within a piconet.

3. **Link Manager protocol layer:**

   It performs the management of the already established links. It also includes authentication and encryption processes.

4. **Logical Link Control and Adaption protocol layer:**

   It is also known as the heart of the bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation and multiplexing.

5. **SDP layer:**

   It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device.

6. **RF comm layer:**

   It is short for Radio Frontend Component. It provides serial interface with WAP and OBEX.

7. **OBEX:**

   It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

8. **WAP:**

   It is short for Wireless Access Protocol. It is used for internet access.

9. **TCS:**

   It is short for Telephony Control Protocol. It provides telephony service.

10. **Application layer :**

    It enables the user to interact with the application.

Advantages of Bluetooth:

- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an adhoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages of Bluetooth:

- It can be hacked and hence, less secure.
- It has slow data transfer rate: 3 Mbps.
- It has small range: 10 meters.

Connecting Devices

Hub:

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

[1] **Active Hub:-**

These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

[2] **Passive Hub :-**

These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.

Switch –

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

Virtual LAN (VLAN)

Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divides broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.

A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive the entire broadcast packet but it is limited to switches only as routers don't forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domain, inter Vlan routing is needed. Through VLAN, different small size sub networks are created which are comparatively easy to handle.

The types of VLAN are:

1) VLAN 0, 4095: These are reserved VLAN which cannot be seen or used.
2) VLAN 1: It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
3) VLAN 2-1001: This is a normal VLAN range. We can create, edit and delete these VLAN.
4) VLAN 1002-1005: These are CISCO defaults for FDDI and token rings. These VLAN can't be deleted.
5) VLAN 1006-4094: This is the extended range of VLAN.

Advantages –

Performance

The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destination.e.g-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain therefore all will receive the traffic i.e wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.

Formation of virtual groups

As there are different departments in every organisation namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.

Security

In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.

Flexibility

VLAN provide flexibility to add, remove the number of host we want.

Cost reduction

VLANs can be used to create broadcast domains which eliminate the need for expensive routers.By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

NETWORK LAYER

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 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).

There are two types of network transmission techniques, circuit switched network and packet switched 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.

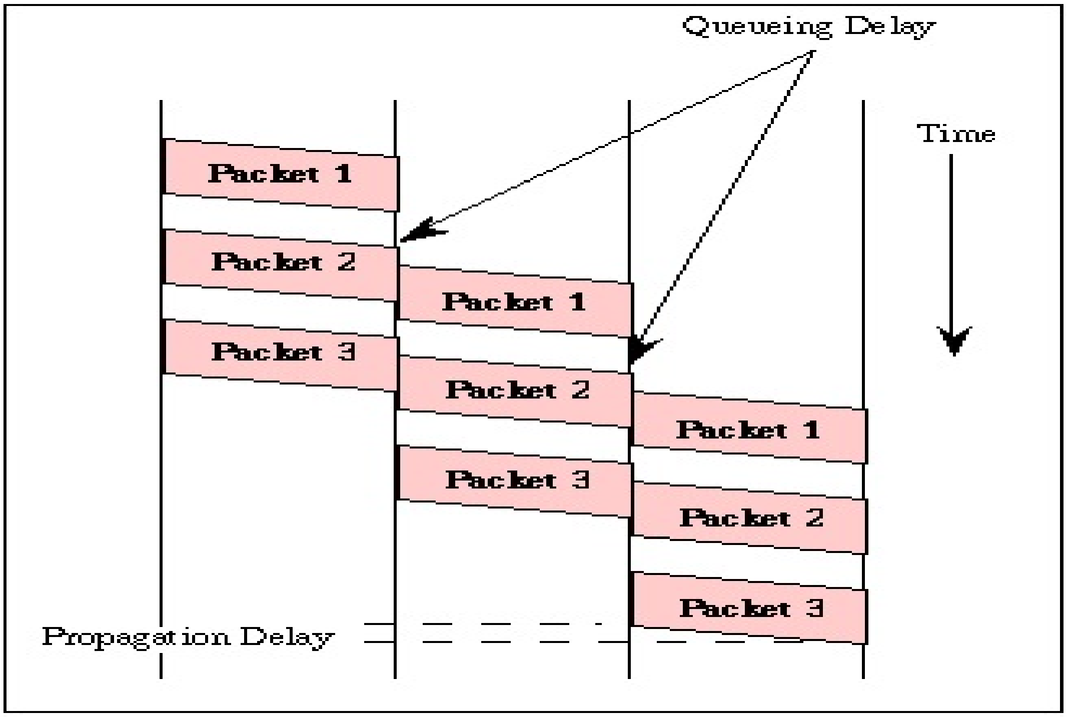
In a circuit switched network, the data packets are received in order whereas in a packet switched network, the data packets may be received out of order.

The packet switching is further subdivided into Virtual circuits and Datagram. Packet switching is similar to message switching using short messages. Any message exceeding a network-defined maximum length is broken up into shorter units, known as packets, for transmission; the packets, each with an associated header, are then transmitted individually through the network. Packet network equipment discards the "idle" patterns between packets and processes the entire packet as one piece of data. The equipment examines the packet header information (PCI) and then either removes the header (in an end system) or forwards the packet to another system. If the out-going link is not available, then the packet is placed in a queue until the link becomes free. A packet network is formed by links which connect packet network equipment.

There are two important benefits from packet switching.

1. The first and most important benefit is that since packets are short, the communication links between the nodes are only allocated to transferring a single message for a short period of time while transmitting each packet. Longer messages require a series of packets to be sent, but do not require the link to be dedicated between the transmission of each packet. The implication is that packets belonging to other messages may be sent between the packets of the message being sent from A to D. This provides a much fairer sharing of the resources of each of the links.

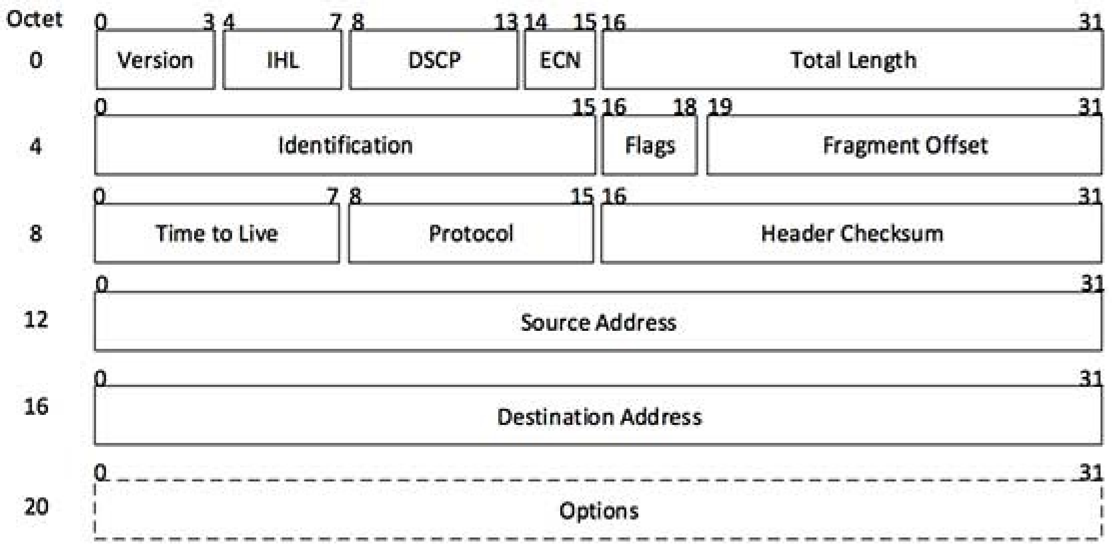
2. Another benefit of packet switching is known as "pipelining". Pipelining is visible in the figure above. At the time packet 1 is sent from B to C, packet 2 is sent from A to B; packet 1 is sent from C to D while packet 2 is sent from B to C, and packet 3 is sent from A to B, and so forth. This simultaneous use of communications links represents a gain in efficiency, the total delay for transmission across a packet network may be considerably less than for message switching, despite the inclusion of a header in each packet rather than in each message.



Internet Protocol Version 4 (IPv4)

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address. Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows −

- **Version** − Version no. of Internet Protocol used (e.g. IPv4).
- **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. In this 3-bit flag, the MSB is always set to ‘0’.
- **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, i.e. the next level Protocol. For example protocol number of ICMP is 1, 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 (or source) of the packet.
- **Destination Address** − 32-bit address of the Receiver (or destination) of the packet.
- **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPv4 supports three different types of addressing modes. – (Discussed in unit 2)

1) Unicast Addressing Mode
2) Broadcast Addressing Mode
3) Multicast Addressing Mode

It also has 5 main classes of IP address (Discussed in unit 2)

1) Class A
2) Class B
3) Class C
4) Class D
5) Class E

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 sub-networks which provides better network management capabilty

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

Classless Addressing

To overcome address depletion and give more access points to the internet classless addressing was designed and implemented.There are no classes,but the address are still granted in blocks.

Address Blocks (Classless Allocation)

In classless addressing when an entity small or large need to be connected to the net it is granted with a block of address. The sum of the block varies based on the nature. Block allocation is given by the global authority called as Internet Corporation for Assigned Names and Number (ICANN).

Steps for Assigning:

1) The address in a block must be continuous one after another
2) The number of addresses in a block must be a power of 2
3) The first address must be venly divisible by no. of Addresses.

Prefix Length :Slash Notation

Since classless Addressing is of variable length the prefix length n is added to the address, seperated by a slash .This is refered to as CIDR .eg. 12.24.76.7/8

Extracting Information from Adddress

In IPv4 Addressing ; any Address in the block gives the information about

1) The number of Address: $N=2^{32-n}$
2) The first Address:

The n leftmost bit is kept and all the right most bit is set to 0

3) The Last Address

The n leftmost bit is kept and all the rightmost bit is set to 1

Network Address

An Internet is made of m network and a router with m interfaces. When a packet arrives at the router from any source host, the router consults its forwarding table to find the corresponding port through which the packet should be forwarded to reach the destination.each network is identified by its network address.

For Network Address and subneting please view

https://www.youtube.com/watch?v=rs39FWDhzDs

Dynamic Host Configuration Protocol (DHCP)

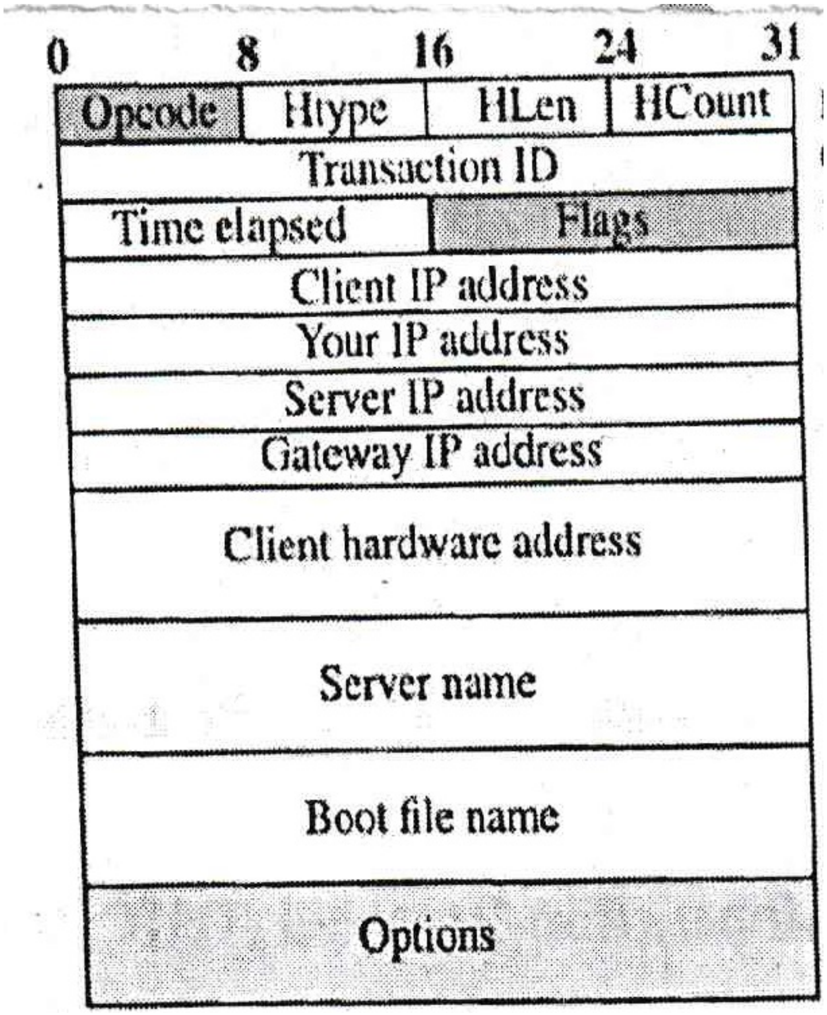
Assigning address in an organization can be done automatically using DHCP.It is an application layer program which help TCP/IP at the Network Layer.It consist of 4 pieces of Address

1) Computer Address
2) The Prefix
3) The address of the router
4) The IP address of a name server

DHCP Message Format

DHCP is a client server protocol in which the client sends a request message to the server .

The frame format is as below



0 8 16 24 31

Opcode	Htype	HLen	HCount
Transaction ID			
Time elapsed		Flags	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address			
Server name			
Boot file name			
Options			

Please see : https://www.youtube.com/watch?v=e6-TaH5bkjo

NPTEL

https://www.youtube.com/watch?v=O--rkQNKqls&list=PLbRMhDVUMngf-peFloB7kyiA40EptH1up