Advanced Computer Networks

DD sir.

Saathi

Date Date:- 27/1/2022 CLASS-1

Before we move into Computer networks, 3 terms come in the picture:-

i) Data Communication.
ii) Computer Networks.
iii) Advance Computer Networks.

In data communication, we have gone through the roles of sender, receiver, communication medium. Along with these three, we also need to understand the importance of protocols (these protocols are different for different types of devices). Data communication refers to all of these things at a whole.

Networking is a topic which needs the participation of hardware as well as software.

Layered Architecture (OSI , TCP/IP)

OSI → OSI Protocol Suite

TCP/IP → TCP/IP protocol Suite

We have seven layers in OSI and in TCP/IP we have five layers.

There's a famous sentence to remember the seven layers of OSI:-

- Application.
  Presentation.
  Session.
  Transport.
  Network.
  Data link.
  Physical.

(Please Do not Touch Steve's Pet Alligator)

The purpose of the application layer is to help the communication environment in accessing the network's resources. The main protocols used in application layer are HTTP, SMTP, etc. We actually access the network resources that we intend to use. Different applications demand different parameters or different characteristics. Those characteristics should be incorporated before going further.

The purpose of the presentation layer is basically encryption and compression, i.e., how the actual data (message will be presented before sending the message. Presentation means a particular format, by compression we are converting a particular message into a pre-defined format. We can include Encoding & Decoding part here as well. How the message will be represented is the purpose of the presentation layer.

The session layer is used for managing different sessions. Sessions mean a range of time within which 2 communicating parties are communicating b/w themselves (this is one particular session). When we log into a system a particular session starts & when we log out from the system, that particular session ends. This is the responsibility of the session layer.

Transport layer & network layer work hand in hand.

The main thing that the transport layer does is to provide reliable communication. Network

layer ensures that the packet which contains a particular message will reach the correct destination. But it doesn't ensure that the packets will arrive in a particular order.

This reliable communication or message delivery is the purpose of the transport layer.

Till network layer, we have mainly focussed on the software part of networking. Once we reach the data link layer, we are now concerned with the hardware part. The basic purpose of the data link layer is to generate frames, i.e., before physical layer comes into the picture data link layer arranges frames. So each frame consists of a certain no. of bits. ~~The b~~ This layer organizes bits into frames.

The purpose of the physical layer is to ~~transmit~~ ~~transfer~~ the bits. At the end of everything, the message from one source to destination through communication medium. This is the responsibility of the physical layer.

When we move to TCP/IP, the application layer, presentation layer and session layer are merged together to form the actual presentation layer.

The purpose of the application layer here is to hold diff. application protocols.

Q. In which of these layers, we have the LAN or WAN technology installed?

→ Data link and Physical layers.

Saathi

Date __/__/____

LAN Technologies - Wifi, Ethernet, etc.

Q) In which of these layers we have FSK, ASK?
- Before transmitting the bits

Q) " " " " " " " the concept of Hamming code?

- Data Link layer.

Unit of Communication in the data link layer is frame. Unit of Communication in the Physical layer - Bit. Unit of Communication in the Network layer - Datagram. Unit of Communication in Transport layer - Segment or packet or user datagram Unit of Communication in the Application layer - message

Internet Protocol (IP) :-

Name of the layers	Protocols Used
Application Layer	SMTP, FTP, TFTP, DNS, SNMP, DHCP etc
Transport Layer	SCTP, TCP, UDP etc.
Network Layer	IGMP, ICMP, IP, ARP etc
Data link layer and Physical Layer.	Underlying LAN or WAN technologies.

Diff. protocols in diff. layers in the TCP/IP Protocol suite

Saath

Date ___/___/_____

- ~~IP is an unreliable and connectionless datagram protoc~~

Internet Protocol - One of the mostly used protocols in data communication. There are diff. aspects of Internet Protocol.

- IP is an unreliable & connectionless datagram protocol.

Unreliability means we don't have any acknowledgement mechanism. If we use IP to send a message to one receiver, we won't receive any acknowledgement ~~that yes we have~~ from the receiver that yes I have received the ~~msg~~ message from you.

- IP packets can be lost, delivered out of order, may create congestion for the network.

If we have multiple packets, the receiver may receive them in an undesirable order.

- For ensuring reliability, IP should be paired with a reliable protocol like TCP.

This justifies the use of IP along with TCP. IP can be clubbed / paired together with TCP. So TCP and IP can work together because TCP is a reliable protocol. So to ensure reliability, IP can be paired with TCP.

Datagram:-
Unit of Communication at the network

Date __/__/____

layer is a datagram.

- Datagrams are packets in the network layer

- Any packet is a variable length packet with 2 parts - header & data.

Any packet may be of diff. size. We have 2 parts - header part & data part. Any packet/datagram has 2 diff. components - header component & data component.

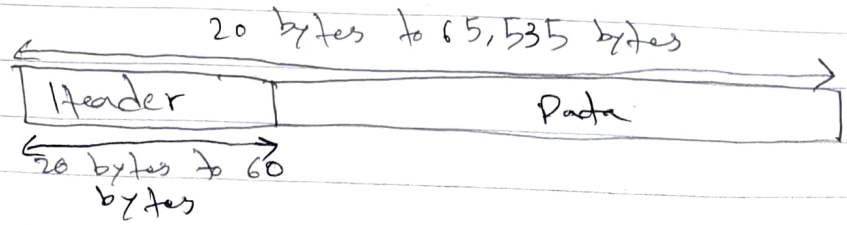
Data components store the actual message in the form of bits & the header component stores different techniques, protocols, mechanisms which will be used to send the message from the sender to the receiver. So the networking details are included in the header component & the actual message is included inside the data component.

The address of sender & receiver, the management part - all these are included and responsibility of the header component.

Date - 28/01/2022

CLASS-2

IP Datagram format :-



This diagram depicts the generic format of IP Datagram.

Saathi

Date

As we can see, the header component can be of any length between 20 bytes to 60 bytes. The minimum length of a header field can be 20 bytes & the maximum length of the header component can be 60 bytes and together the header & data can be maximum of 65,535 bytes.

That means in a single datagram, maximum 65,535 bytes can be transmitted. So if we want to send a large message, the message needs to be divided into certain datagrams & this diagram talks about the maximum capacity of a IP datagram

The header is responsible for containing the information that is required for routing and delivery.

Routing means how the datagram will be transmitted, through which path it will be transmitted and delivery means it should be transmitted to the correct destination. These 2 things are the responsibilities of the header component & the message is storing the data component.

Q) Why the length of the header component is variable?

→ This happens because if we expand the header component, there are diff. fields involved in this header component.

One of the fields in the header component is known as optional field or options.

Options field = 0 byte (may be) to 40 bytes (max. length) — large

Date __/__/____

Saathi

Since it is options field, its not that it is always required but if required, the max. length of the options field can be 40 bytes. These 40 bytes, if required, will be added to the original 20 bytes of the other component of the header field.

So,

20 bytes + 40 bytes = 60 bytes

So, the max. value of the header component is 60 bytes and the min. value is 20 bytes. Min. value happens when the options field doesn't contain any byte. The max. value happens when the options field contains the max. no. of bytes.

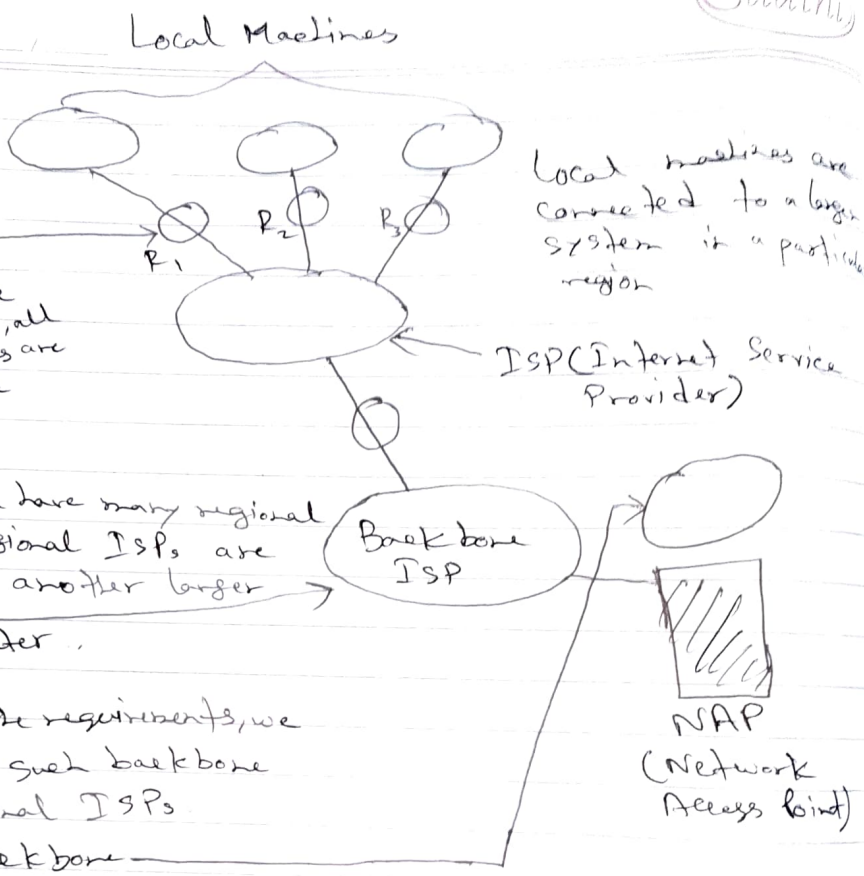
This header component, acc. to TCP/IP protocol suite should be demonstrated/shown in 4-byte section. That means when we will be expanding this header component, we will be " each field or a collection of fields in 4-byte format.

Q) Why header component is such an important field?

- The internet essentially consists of 2 types of networks:-
  i.) LAN
  ii.) WAN

And individually we know the purpose & characteristics of both of them.

Date ___/___/___



← LAN is used

So individually all the local machines are connected to their respective routers using local area networks.

The respective routers may or may not be connected to the regional ISPs through LAN. If the region is a larger one, there can be involvement of wide area network. And obviously the regional ISPs are connected to the backbone ISP through wide area network. So one portion is LAN, another portion is WAN

we have many such instances.

All these backbone ISPs are required to maintain a database known as NAP (Network Access Point). We can have different NAPs. If we have 5 diff. backbone ISPs, we will have 5 diff. NAPs. So all the switching and routing information are stored in these NAPs.

So there are involvement of diff. types of connecting devices.

When we are talking about a particular datagram or a particular protocol, we have to keep all these routing details in mind. The header part, which is responsible for routing & delivery, should contain all these necessary details.

Importance of Regional & Backbone ISPs:-

Regional ISPs store all the necessary details of a particular region. Necessary information means the details of connecting devices, i.e., the routing information. If required switching information

Multiple regional ISPs are connected to a single backbone ISP. How a single ISP will be able to communicate with diff. regional ISPs, ~~Those~~ these complex information are maintained in a NAP.

In the networking world, NAPs are also known as switching stations. Because with the help of NAPs, the router will be able to understand the destination device.

All the necessary complex switching information are stored inside a NAP. These are basically known as switching stations.

Saathi

Date ___/___/___

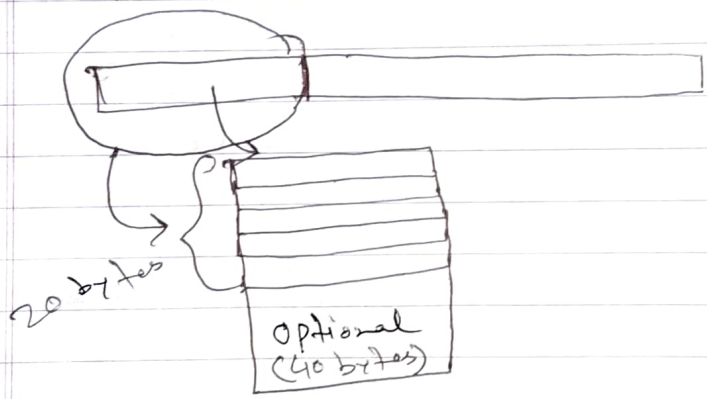
All these things are maintained by the header component.

Header format :- may be thought of having 6 rows.

VER (4 bits)	HLEN (4 bits)	Service Type (8 bits)	Total length (16 bits)

Fields in the 1st row.

Total 32 bits, so 4 bytes.



Each row has 32 bits of length. This is how the IP protocol has been developed.

- Version (VER) :- It defines the version of the IP protocol. The current widely used version is IPv4. IPv6 is also used. If the processing machine is using some other version, the datagram is totally discarded.

When we are talking about IPv4, this version field will contain 0100 because 0100 is the binary equivalent of 4. So we will just put 0100 in the version field. Similarly, when we will be using IPv6, we will just put 0110 in the version field because it is the binary equivalent of 6.

Saathi

Date __/__/____

- Header Length (HLEN):- It defines the total length of the datagram header in 4-byte words. It is required because of the variable length header. The minimum value is $5(0101_2)$, so the length specified is $5 \times 4 = 20$ (in bytes) and the maximum value is $15(1111)_2$, so the length specified is $15 \times 4 = 60$ (in bytes).

The way HLEN stores the required information is a bit different. The purpose of HLEN field is to store the total length of the datagram header (only the header length). But it doesn't store either 20 or 60.

Explanation:-

20 would ~~require~~ require 5 bits. But the length of HLEN is 4 bits. So obviously 20 is not directly stored. We are storing 20 in a diff. way known as 4-byte word format. That means the value which is stored in HLEN is multiplied by 4 to get the actual header length.

So if we want to represent, HLEN will store the binary equivalent of 5. Because 5 is multiplied by 4 to get 20. So, for e.g., if we want to store (0111_2) in HLEN, the header length that we are talking about is 28 bytes.

Service type - will be explained later.

- Total length :- It has 16 bits. So the max. value that we can represent is 65535 bytes. This total length field stores the total length of the IP datagram. It contains the header length + data length in bytes.

Page No.

The max. length of an IP datagram is 65,535 bytes because the total length is of 16 bits.

Header Format :- Maybe thought of having 6 rows.

Identification (16 bits)	Flags (3 bits)	Fragmentation offset (13 bits)

Fields in the 2nd row

All these fields are used for fragmentation. (will be explained later).

Header Format : Maybe thought of having 6 rows.

Time to Live (8 bits)	Protocol (8 bits)	Header Checksum (16 bits)

Fields in the 3rd row

- Time to live :- It is used for calculating the max. no. of hops since a datagram has a limited lifetime. The sender initiates this field with an integer that is 2 times the max. no. of hops to the intended receiver. Each router decrements this value by 1. If this field contains 0, the datagram is discarded.

Q.) Why this TTL field is required?

- TTL field is required because every datagram has a limited lifetime, when it is travelling through diff. networks. It cannot travel for infinite no. of times.

When we talk about hop, we mean transmission of message to the adjacent machine.

In case of IP datagram transmission, if we don't have this TTL field, this (hop) will continue forever if the destination address is erroneous. So there has to be some restriction on that and that restriction is imposed using a field called TTL or Time to Live.

There can be many ways to represent this TTL value.

Suppose we are storing 6 in TTL value. It stores the max. no. of hops allowed multiplied by 2. So that means that particular IP datagram can have 3 hops maximum.

For one hop, we also get a response message. Similarly if we store 10, the max. no. of hops allowed will be 5. This is one way of storing the TTL field value.

Another way is by giving direct value, i.e., if we write 10 we are allowing 10 hops. After 10 hops, that particular datagram will be simply discarded.

Another way of storing TTL value is by maintaining timestamp value. This timestamp information will be decremented by each visited router. So if the original timestamp value, is, say 7 and if there are intermediate 5 routers, so after the visit of the last router the TTL value will be 2. So when the TTL value becomes 0, that particular IP datagram will be rejected.

Why does a datagram has a limited lifetime

It will unnecessarily make the network busy. Suppose the destination address is wrong and it doesn't have a limited lifetime, it will keep on hopping from one router to another router taking the network bandwidth. So unnecessarily the network bandwidth gets lost. And in a busy network, it will create a condition.

Data communication never comes free of cost. We have to pay for the network bandwidth, we cannot simply allow anything unnecessary to roam about freely.

Protocol :- It defines the final destination protocol to which the IP datagram should be delivered.

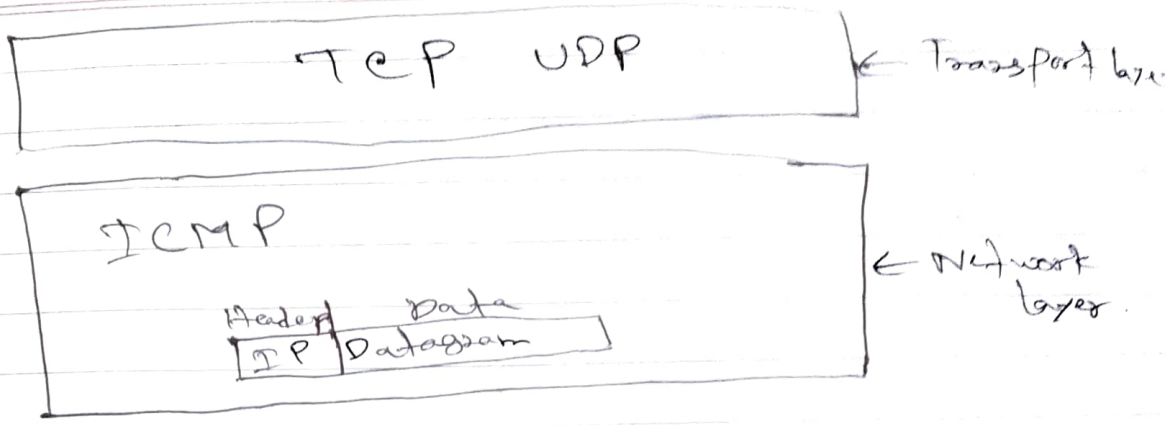
In IP datagram header, the protocol field is used for a specific purpose which stores a value related to a higher level protocol.

How can we store the protocol value?

Each protocol is uniquely identified by a pre-defined entry.

Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP

Protocols with their values.



When the data of an IP Datagram needs to be transported to another device, it needs the services of both the network & the transport layers. (needs the help of other protocols basically).

So if for transmitting the data present in IP Datagram, it needs the help of TCP, then the protocol field will be updated to 6. So with the value 6, it is understood that the higher level protocol that will be required for the transmission is TCP.

Whatever be the situation, that value gets updated in the protocol field.

IP Protocol does the data multiplexing information. So it needs the help of other protocols for the communication. These other protocols may be present in either of the network or transport layers.

- Header Checksum:- It is used for error checking. It is a 16 bit checksum field. Checksum is one of the techniques for error checking. Here also it does the error checking option & every protocol should have an error checking option.

Saathi

Date / /

[Source IP Address (32 bits)]
field in the 4th row

- The fourth row entirely contains the source IP Address (since we are dealing with IP version 4).

[Destination IP Address (32 bits)]
Field in the 5th row

- The fifth row is entirely occupied by the destination IP Address.

These were about the five logical sections of the header.

• Service Type:- It defines how the IP datagram should be handled. According to the current interpretation, the first 6 bits (from MSB) are used as codepoint subfield and the last 2 bits are unused. The codepoint subfield is used in one of the 2 following ways:-

• If the 3 right-most bits are 0s, other 3bits are used for precedence bits.

• Otherwise, the format given in the following table is considered.

- Originally this field was known as type of service. Its purpose was to define how the datagram should be handled, how the datagram should be monitored. This is the purpose of service type field.

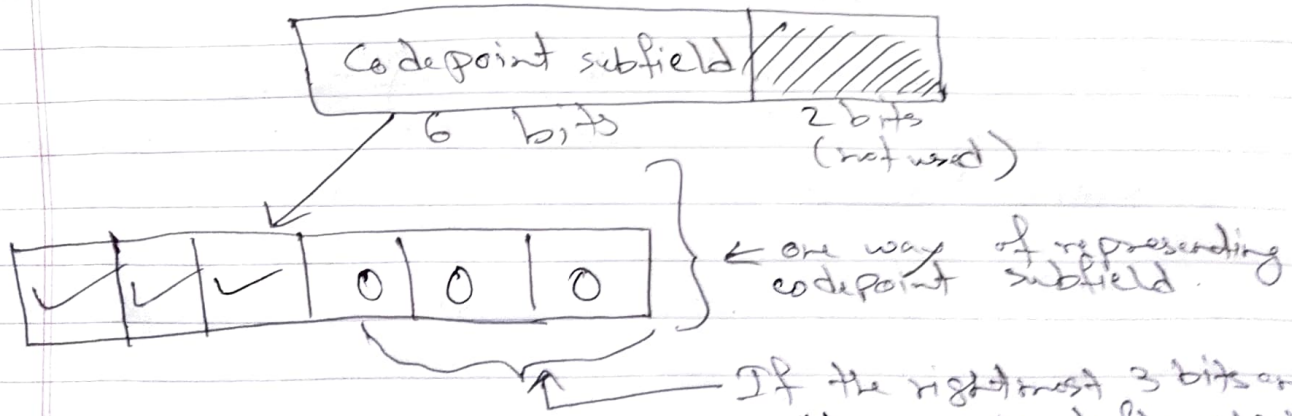
In todays IPv4 datagram format, the service type

field which contains 8 bits has different things to be performed. A part of this field is used to identify the precedence of a datagram.

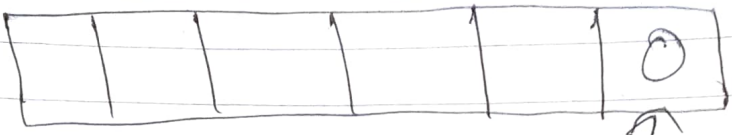
Q) What do you mean by the precedence of a datagram?

- Precedence plays a major factor when there is a congestion in the router. If the router gets conjested with multiple IP datagrams, it will not be able to forward all the datagrams together. It may have to discard some of the datagrams also (in the worst case). W.r.t such situations, the precedence factor plays an important part. So the datagram having the highest precedence cannot be discarded, another datagram with the lowest precedence may be discarded if required

So the service type field contains some bits which play an important part in precedence interpretation.



Another way of representing codepoint subfield:-



If this bit is 0, the other 5 bits are used for internet related operations

If the last 2 bits are 1 and 1, the services are used for local area network.

If the last 2 bits are 0 and 1, it is used for experimental purposes.

Category	Codepoint	Assigning Authority
1	xxxxx0	Internet
2	xxxx11	Local
3	xxxx01	Experimental

Values for Codepoint

Q) How many total types of services are provided by the service codepoint subfield other than Precedence Interpretation?

— With 6 bits, we can have 2^6, i.e., 64 services apparantly.

Out of these 64 services, if the last 3 bits are 0 (which are used for Precedence Interpretation), the remaining no. of services are $64 - 2^3 = 64 - 8 = 56$. These 56 services are divided among Internet, local & Experimental.

For local and experimental services, 16+16=32 bits are required. So for Internet purpose, 56-32=24 services are provided

Q) Will the precedence of a datagram packet remain constant throughout?

→ Not necessarily. When we are interested in internet operation, diff. IDPs, LANs, WANs come into the picture and we never know what is the priority level of a particular LAN. If an IP datagram carries information regarding network management, the priority level of that datagram shouldn't change But for other normal services, the precedence value of an IP datagram may have to be changed, but for a local area network communication, it doesn't change.

Identification (16 bits)	flags (3 bits)	fragmentation offset (13 bits

fields in the 2nd row

All these fields are used for fragmentation.

Fragmentation:-

- It is a process to make an IP datagram acceptable to any physical network.
- Only data portion in a datagram is fragmented.
- Required parts of the header must be copied to all the fragments.

- A datagram may have to travel through diff. types of networks. When it is travelling from one network to another network, the connecting device

Saathi

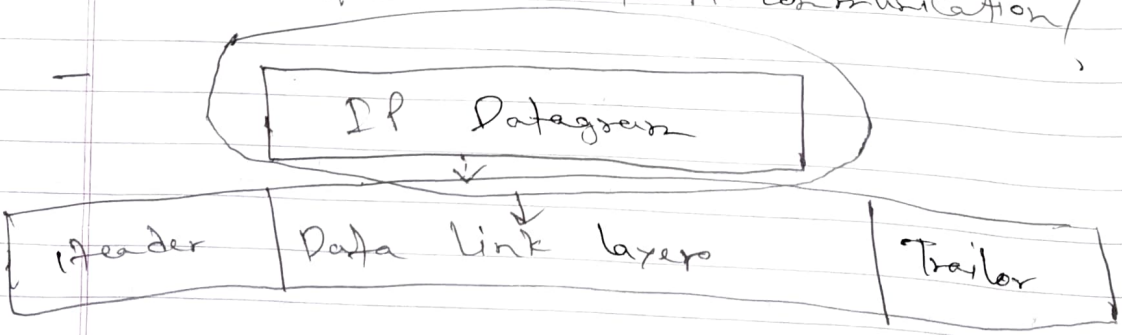
Date ___/___/_____

is a router, so when the router receives an IP datagram, it decapsulates that. After decapsuleting, the router does the processing and again it encapsulates into a different frame. These frame sides are different for different types of protocols present in the physical network. So as the datagram passes through different characteristics while travelling " " networks, it is quite obvious that each characteristic needs to be handled separately. Specifically, it is important when there is transition from local area network to wide area network.

When it is travelling from a local area network to a wide area network, it needs to be encapsulated in a different way so that the new network can recognise the IP datagram.

Q.7 What happens in network communication?

—



If the data link layer protocol is diff. from one router to another router, the no. of bits to be added with the header and trailor will be different. (as it depends on ~~MTU~~ MTU (Maximum Transfer Unit)).

MTU - talks about the maximum amount of bytes a frame can contain at a time.

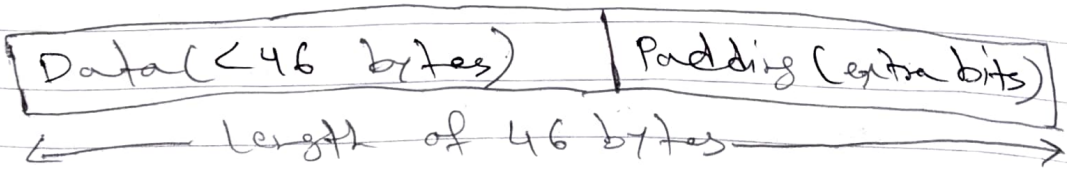
Suppose for a particular data link layer protocol or physical network, the MTU value is 1000 bytes and IP datagram size is 2000 bytes. If this happens, this IP datagram which is coming to the data link layer needs to be fragmented. This is the responsibility of the fragmentation layer.

Only the data portion in a datagram needs to be fragmented if possible

So if we want to pass an IP datagram through heterogeneous physical networks, we may have to fragment the datagram into different segments/components depending on the value of MTU.

The final row is not used for defining any field as such. It is mainly used for padding purpose. Some underlying technologies in the data link layer restrict the no. of bytes in a single frame.

For example, the minimum frame size for the Ethernet protocol is 46 bytes so, if the IP datagram frame size is less than that, extra padding bits are added. The following diagram depicts the situation:-



-Padding means to add some extra bits to be accomodated into the physical network.

Date - 3/2/2022 CLASS-4

Q) An IP packet with the first byte of 01000100 arrives. Will the receiver accept the packet?

— No. The first 4 bits are correct because it correctly identifies the IP version ($0100_2 = 4$). But the next 4 bits are wrong since (4×4) bytes or 16 bytes is less than the minimum header length of 20 bytes.

Note:- For a wrong IP version (the first 4 bits), if there is any correction mechanism involved in the routing process then that would have been corrected but we cannot correct the header length because it depends on other factors.

Q) An IP packet with the first few digits are $(4900\,0033\,0001\,0800\,0506\ldots)_H$. Which higher level protocol is used by this datagram & how many hops can be allowed before dropping it? What is the length of data carried by this datagram?

— The 9th byte is 05, so the datagram can travel 5 hops. The 10th byte is 06 which is the number corresponding to TCP. The 3rd & 4th byte, taken together is 0033_H which is 51_{10}. The HLEN value is 9 giving the header length to be 36 bytes. So, the data length is (51-36) bytes or 15 bytes.

$(4900\,0033\,00\ldots\ldots)_H$ = Hexadecimal digits.

TTL (9th byte)
Protocol (10th byte).

1 hex digit = 4 bits.
2 hex digits = 8 bits (1 byte).

4 and 9 together take up the first byte.
Next 2 zeroes " " " 2nd "
" 2 zeroes " " " 3rd "

In this way, we see that the 9th byte is 05, that means the no of hops allowed is 5 and the 10th byte is 06 which means the higher level protocol which is to be used is TCP

Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP

This is how we can perform different types of ~~routing~~ masking in the router.

IPv4 Addresses:-

- An IPv4 address is 32 bits long.
- All the IPv4 addresses are unique and universal
- The address space of IPv4 is 2^{32}.
- An IPv4 address is normally written in dotted-decimal notation.
- IPv4 addresses are classified into 2 types: Classful Addresses and Classless Addresses

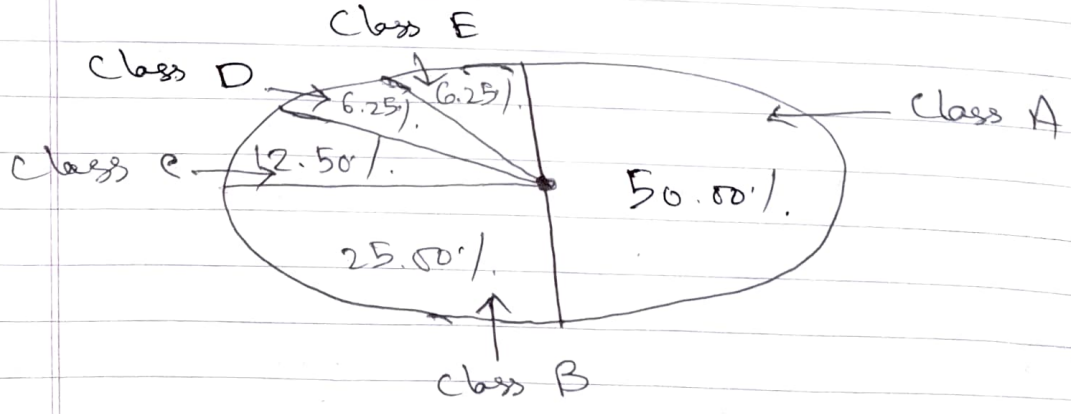
- The version 4 address takes 32 bits whereas the version 6 address takes 128 bits. So obviously more no. of addresses can be accomodated in version 6. In version 4 since we have 32 bits

allotted, the address space is 2^{32}. This doesn't mean we can use all these 2^{32} addresses, some addresses are reserved and some addresses are not made for the client machines.

Some addresses are private addresses, some are public ". Private addresses can be used for private networks, those addresses shouldn't be used for public networks and most of the other addresses are reserved for public network.

Dotted decimal notation means 192.168.10.7. There are 4 parts and each part is separated from the other by a dot. If we don't want to follow dotted decimal notation, the alternative would have been binary notation. Each of these segments would then have been represented by 8 bit binary format. But that would be clumsy.

Classful IPv4 Addresses:-



Distribution of IPv4 address space

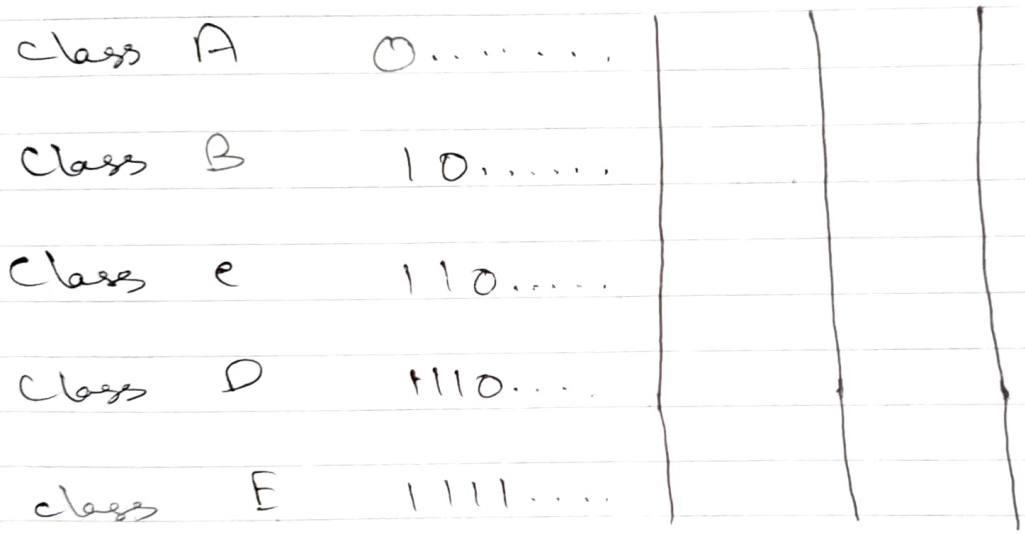
The 2^{32} addresses are distributed among 5 diff. classes in classful Addressing Scheme. In classless Addressing Scheme, we don't have any

Class Concept

What is the logic behind such address space distribution?

Classful IPv4 Addresses:-

An IPv4 address is divided into 4 octets. In binary notation, the following happens:-



- Any IPv4 address (classful or classless) is divided into 4 octets. The first octet is very important for identifying the classes of the addresses.

Lets begin with class A address. Here the first bit (MSB) will always be zero. Since the " " is reserved, we can make a combination of 2^{31} out of 2^{32}.

$$\text{Ratio} = \frac{2^{31}}{2^{32}} = \frac{1}{2} = 50\%.$$

So this is why class A addresses will take up 50% of address space.

For class B, the first 2 bits are reserved & they are 1 and 0. So we can make a combination of 2^{30}.

$$\text{Ratio} = \frac{2^{30}}{2^{32}} = \frac{1}{4} = 25\%.$$

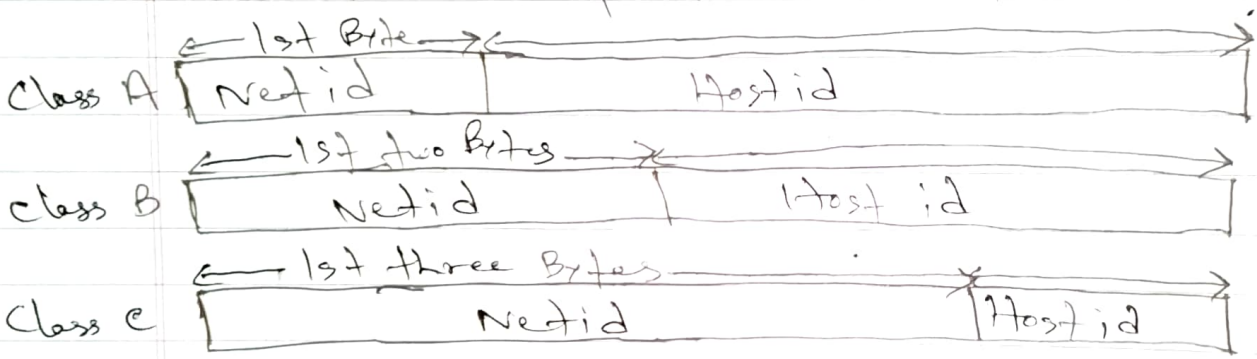
Page No.

So that's why class B addresses take 25% of the address space.

Similarly we can calculate the address space of classes C, D & E respectively.

Classful IPv4 Addresses:-

An IPv4 address has 2 parts. The first part of this addresses identifies the network on which the host resides and the second part identifies a particular host in a network.



In class A, the first byte is reserved for network id and the 2nd to 4th byte (24 bits) are reserved for hostid. In case of class B, the first 16 bits are reserved for network id and the last 16 bits are reserved for the hostid. For Class C, the first 24 bits are reserved for network id and the last 8 bit are reserved for the host id.

Netid is used for identifying the network address. When we are moving from one network to another network, to identify a particular network in the routing process, we use the network id.

Hostid is used for identifying a particular device/machine in that network.

Date __/__/____

So after identifying the network, we have to identify a machine where we will be sending the data. So for that we need host id.

If the network id takes 8 bits and the host id takes 24 bits with the help of class A in a single network, how many hosts can we expect?

- 2^{24}. (theoretically).

There is no network where 2^{24} no. of hosts will be present.

In class B, total no. of hosts is still quite large. So 2^{16} no of hosts per network are to class B address.

In class C, total no. of hosts will be 2^8, i.e., 256 is quite reasonable for a large network.

If we choose class A address, for addressing, (say for 70 machines), we are wasting $2^{24} - 70$ addresses.

If we ever want to address 500 diff. machines through class A address, we are still wasting $2^{24} - 500$. This is a huge wastage.

As a result, class A addresses are not at all recommended for private networks.

Class C is a good option. Class B is basically a compromise between Class A and C.

Class D is used for multicast addressing and class E is reserved for future use. (not used actually in practical purpose).

Saathi

Date __/__/____

Another important note:-

For identifying the class of an IPv4 address specified in dotted decimal notation, the decimal value of the 1st octet is used in the following way:-

Class	Decimal value Range of the 1st Octet
A	0-127
B	128-191
C	192-223
D	224-239.
E	240-255.

We have to consider both v4 and v6 addresses together.

For class A, the first bit (0) is reserved, that means we are left with 0000000.

So, the min. value = 0 0000000 = 0
the max. " = 0 1111111 = 127.

So that's why the decimal value range is from 0-127 and for class B it is from 128-191 if we make the first 2 bits constant as 1 and 0.

Usefulness of classful IPv4 Addresses:-

Each class is divided into a fixed no. of blocks with fixed size. The following table describes the situation.

Saathi

Date __/__/____

Class	No. of blocks (no. of organizations)	No. of addresses in each block
A	$2^7 = 128$ (The MSB is fixed)	$2^{24} = 16,777,216$
B	$2^{14} = 16,384$ (Two MSBs are fixed)	$2^{16} = 65,536$
C	$2^{21} = 2,097,152$ (3 MSBs are fixed).	$2^8 = 256$

An address in a block assigned to an organization is given as 80.21.29.110. Find out the no. of addresses in this block, the first address and the last address of this block.

- We will first check under which class this address belongs to. Since the first octet is 80, the address belongs to class A.

So the total no. of addresses theoretically will be $2^{24} = 16,777,216$.

The first address is known as the network address.

Given address = 80.21.29.110

So the first address = 80.0.0.0.

" last " = 80.255.255.255