Module 4 – Network layer protocols.

Vipin Das
SAINTGITS College of Engineering

Internet Protocol [IP]

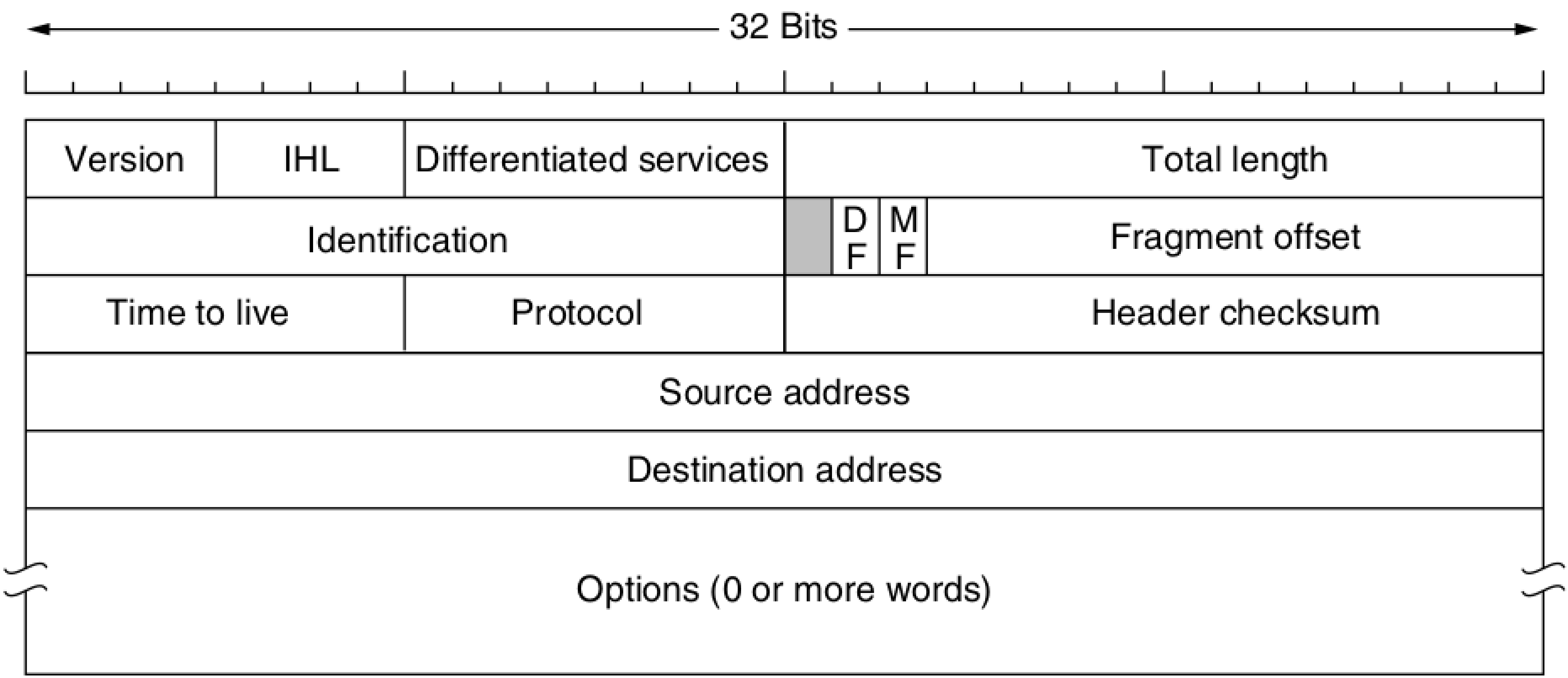
The main reason for the wide spread usage of Internet.

IP Packets are used in the Internet.

The primary thought that went into the creation of IP is internetworking.

IP provides best effort packet delivery.

IP Version 4 packet structure -Header



IP v4

Ipv4 packet contains a header part and a data part.

Header part is minimum 20 bytes and max of 60 bytes.

The standard includes optional bytes in the header.

The bits are transmitted left to right and follows top to bottom order.

IP v4 Header components

Version – Identifies the version of the protocol.

IHL- Internet Header Length --> Indicates the length of the header in 32 bit words.Varies based on the presence of options.

Differentiated service- This field was added to specify the quality of service required.Also referred as type of service.In new standard top 6 bits marks the service class and two bits represent the Explicit congestion.

Total Length- Total length of the packet.Max of 65535 bytes.

Identification – The identifier given to packets.

DF- Dont fragment-single bit.

MF-More fragments-Single bit.

Fragment offset – Specifies the position of this fragment packet in the larger packet. All packets except the last one should be in multiples of 8 bytes.

TTL – Time to live – The packet lifetime. Max of 255 seconds.Decremented on each hop and the packet is discarded when the value becomes zero.

Protocol- Specifies the upperlayer protocol [transport layer] in use.

Header checksum-Checksum of the header to detect errors.

Source and destination addresses – 32 bit address commonly known as IP address.

Optional values supported

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Fragmentation of IP packets

Every router enforces a maximum size for the packet that is passing through it.

This is known as Maximum Transmission Unit [MTU]

The fragmentation and reassembly is managed by using the id,DF,MF and offset fields.

If a packet of 800 bytes is split into two-

Fragment 1

- DF will be 0
- MF will be 1
- Offset will be 0

Fragment 2

- DF will be 0
- MF will be 0
- Offset will be 50 --> indicating 50 words of size 8bytes (50 *8)=400

Example

A packet of size 1440 bytes needs to be transmitted through a network of MTU 576 bytes

The packet total size is 1440 bytes which includes the 20 byte header also.[Assuming no options]

So we have a data of size 1420 bytes.

The data part in a fragment has to be multiples of 8.

So since MTU is 576 bytes , a fragment can have a maximum of 556 bytes.(576-20)

But 556 is not divisible by 8 and the nearest possible value is 552.

So data in a fragment is 552 bytes.

No.of fragments required= 1440/552=2.9... =>3 fragments

Add 20 byte header,the packet size is 572 bytes which is less than 576.

ID field is same for all the fragments.

Fragment 1

DF=0

MF=1

Fragment offset =0

Now we have sent 552 bytes from original data.

Fragment 2

DF=0

MF=1

Fragment offset =552/8 =69 [Offset is added as a factor of 8 byte word]

Now we have send 1104 bytes leaving 316 bytes of data

Fragment 3

MF=0

DF=0

Fragment offset=1104/8=138

Now we have transmitted all the data.

Some GATE Questions

An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are

(A) MF bit: 0, Datagram Length: 1444; Offset: 370

(B) MF bit: 1, Datagram Length: 1424; Offset: 185

(C) MF bit: 1, Datagram Length: 1500; Offset: 37

(D) MF bit: 0, Datagram Length: 1424; Offset: 2960

MTU is 1500 .So data inside one packet is 1480.

1480 is divisible by 8. fragment 1 offset is 0

Transmitted 1480 bytes.So fragment2 offset is 1480/8=185

Transmitted 2960 bytes.So fragment offset is 2960/8=370

And the last fragment contains 1444 bytes [4404 -2960]

Ans A

Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header ans 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0.

The fragmentation offset value stored in the third fragment is ______ .

(A) 0

(B) 72

(C) 144

(D) 216

MTU = 600 bytes and IP Header = 20 bytes

So, Payload will be 600 – 20 = 580 bytes

580 is not multiple of 8, but fragment size should be multiple of 8. So fragment size = 576 bytes

Kth fragmentation offset value = Fragment Size * (Kth fragment – 1) / Scaling Factor

Offset value of 3rd fragment = 576 * (3 – 1) / 8 = 144

Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How may total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

(A) 6 and 925

(B) 6 and 7400

(C) 7 and 1110

(D) 7 and 8880

UDP data = 8880 bytes

UDP header = 8 bytes

IP Header = 20 bytes

Total Size excluding IP Header = 8888 bytes.

[UDP Header is a part of upper layer data.So data part in network layer becomes UDP data+UDP Header]

Number of fragments = $\lceil 8888 / 1480 \rceil$

= 7

Offset of last segment = (1480 * 6) / 8 = 1110

IP Version 6

IP V4 used 32 bit addresses.

The total available address space was not at all sufficient.

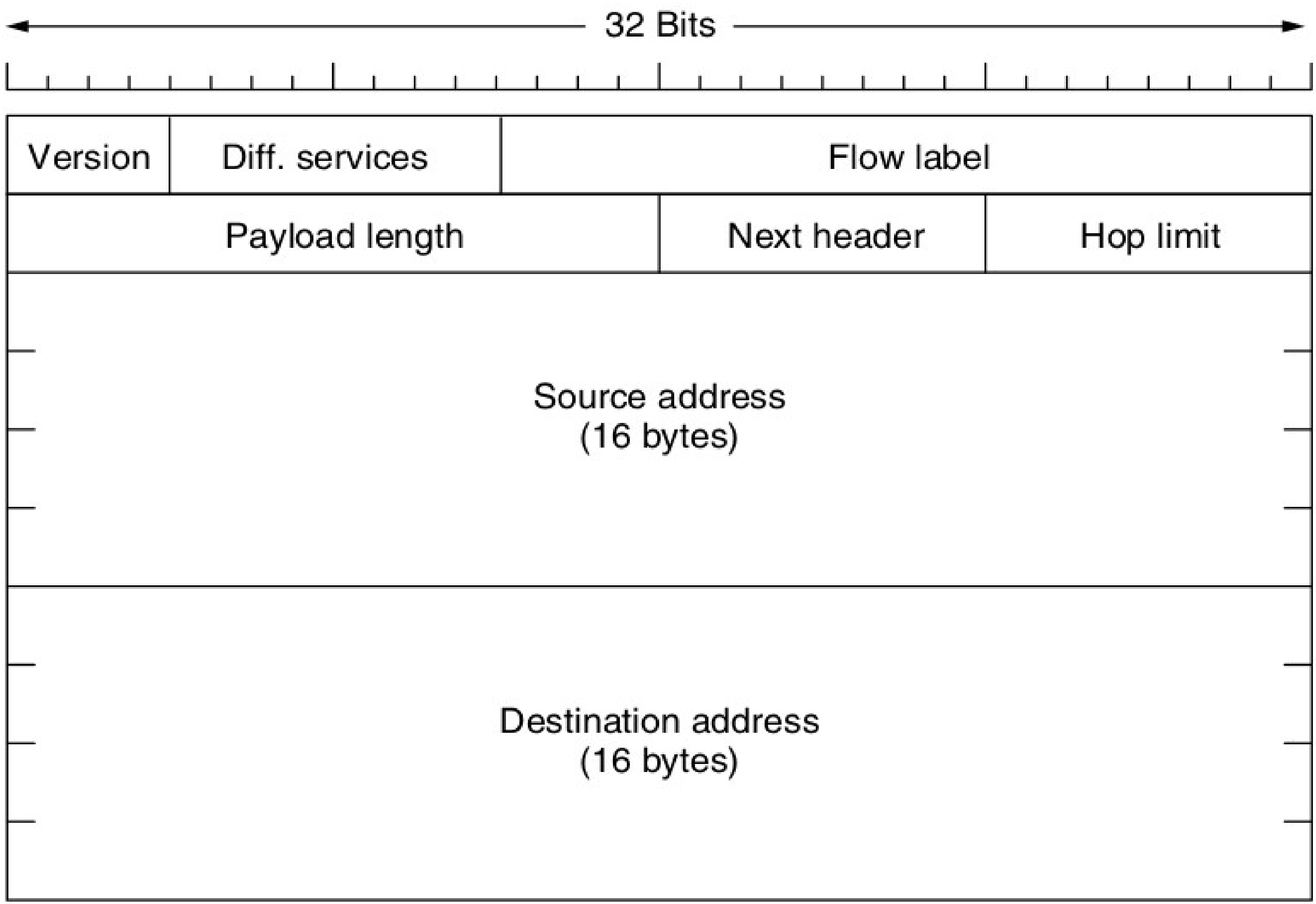
So inorder to accomodate a larger address space Ipv6 was proposed and eventuallu used.

IPV6 addresses are 128 bit.

Follows different header structure than Ipv4.

Earlier implementations caused difficulities in seamless interoperation.

But header has less number of fields,making things easier for routers.


32 Bits
Version
Diff. services
Flow label
Payload length
Next header
Hop limit
Source address
(16 bytes)
Destination address
(16 bytes)

Header fields

Version – To indicate the version

Differntiated service – To specify the QoS parameters.The last two bits are reserved for Explicit Congestion Notification.

Flow label – Packets with similiar requirements will be assigned same flow label.

Payload length- The length of the actual data.

Next header- If there are options specified ,this field points to those else to the upper layer protocols.

Hop Limit- Similiar to time to live in IP V4.The routers decrement this on each hop and when the value becomes zero the packet is discarded.

Source and destination address- 128 bit ip address.

The checksum field is avoided.The datalink layer protocol has checksum fields.Some upperlayer protocols also has checksum.

IP V6 optional headers.

The standard defines a set of optional headers.

If more than one option header is present,their order is also specified by the standard.

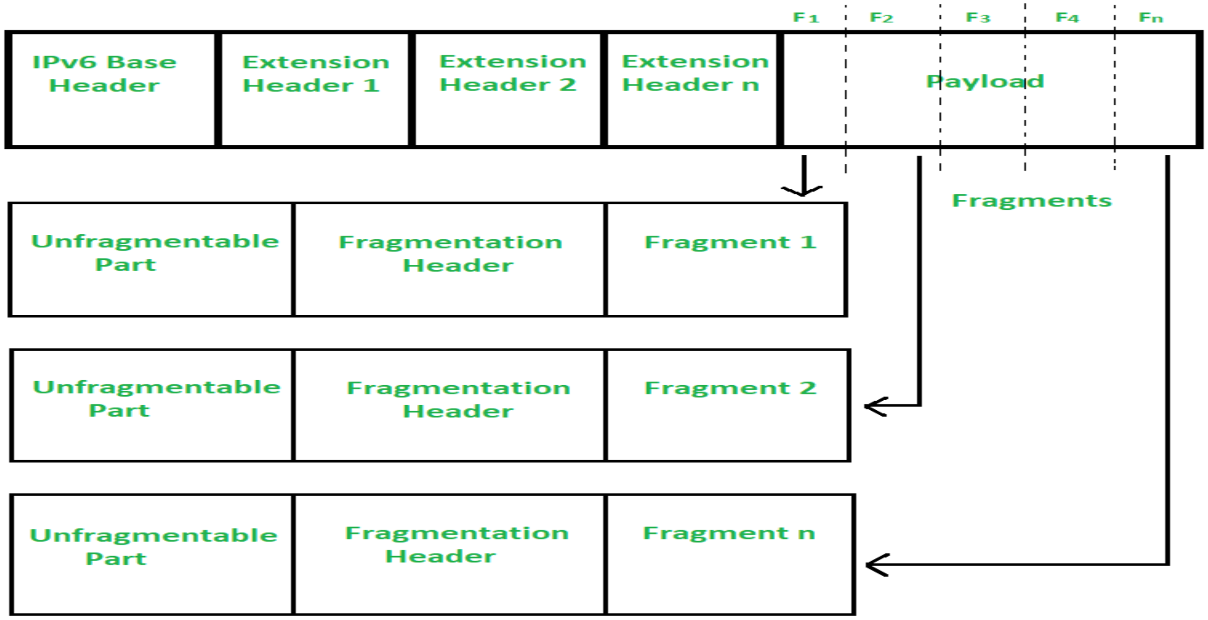
Some have fixed format,others follow <type,length,value> tuple.

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

IP V6 fragmentation

No intermediate node will do fragmentation or defragmentation.

The fragmentation is done at the source and the the defragmentation is done by the recepient.

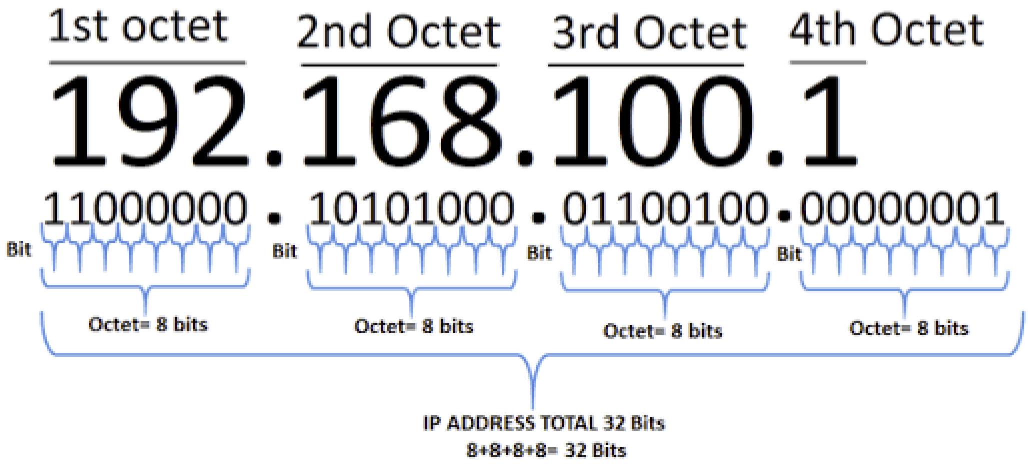


https://datatracker.ietf.org/doc/html/rfc2460#section-4.5

IP v4 and IP v6 address

IP v4 follows a 32 bit addressing scheme.

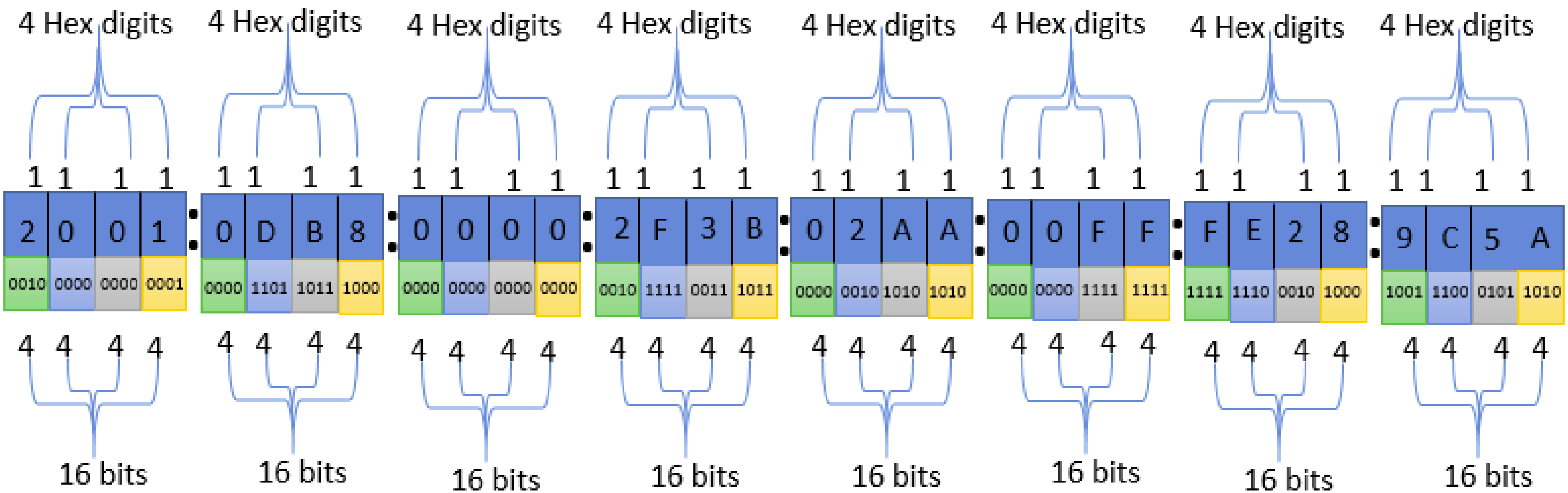
IP V6 Address follows a 128 bit addressing scheme.



<--IP v4 address

IPv6 address in Hexadecimal notation

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A



00100000000000010000110110111000000000000000000000101111001110110000001010101010000000001111111111111110001010001001110001011010

IPv6 address in binary notation

Assignment 2

1. IPSec – Uses in IP network.

Write a one page note and upload scan to linways.

Submission dead line **03rd Feb -2022.**