Lecture-2

Network Layer

Services and protocols:

- transport segment from sending to receiving host.

  sender: encapsulates segments into datagrams, passes to link layer.

  receiver: delivers segment to transport layer protocol.

- Network layer procols are in every Internet device such as hosts, routers.

- Routers: It examines header ~~file~~ fields in all IP datagrams passing through it. It moves datagrams from input ports to output ports to transfer datagram along end-end path.

Two-key network-layer functions:

- Network-layer functions:
  - forwarding: It move packets from a router's input link to appropriate router output link.
  - routing: It determine route taken by packets from source to destination using routing algorithm

Network layer:

• Data Plane (Per-route function)

- It operates locally with each router. It also determines how a datagram (packet) arriving at an ~~output~~ input port is forwarded to router output port based on packet header.

• Control plane (Network-Wide Logic)

- It network-wide logic
- It determines how datagram is routed among routers along end-end path from source host to destination host.

Per-route control plane:

আগে control plane এ routing algorithm use করে then data plane এ result অনুযায়ী data পাঠায়

Each router independently makes routing decisions based on its own routing algorithm. It exchanges routing ~~algorithm~~ ~~wit~~ information with other routers in the control plane, and then forwards packets based on the local forwarding table in the data plane.

Connection and Connection-less service:

① Unlike the transport layer (TCP/UDP), network layer provides datagram and virtual circuit.

datagram → Connectionless Service
virtual-circuit → Connection Service

② However, network-layer service operate host-to-host, whereas transport " " " end-to-end.

Service:

③ no choice: The network decides whether it provides a connection-oriented or connectionless service.

④ Implementation: The decision is made within the network core; not by end-user.

Virtual Circuits: A VC behaves like a telephone circuit where path is established before data can flow.

- sender request
- network best path determine করে
- VCI assign করে
- Update forward table
- Ack, by destination

- Call setup, teardown for each call before data can flow
- Each packet carry [unique number] VC identifier (not destination host address)

Link to link যখন data পাঠায় তখন router আগে থেকে resource and link reserve করে

- Link, router resources (bandwidth, buffers) may be allocated to VC (dedicated resource = predictable service)

A VC consists of:

① path from source to destination

② VC number, one for each link along path

③ Entries in forwarding tables in routers along path

Packet belonging to VC carries VC number. VC number can be changed on each link.

VC Signaling Protocol: Signaling protocols are used to maintain and tear down VCs in connection-oriented ~~sen~~ networks. VC signaling is used in ATM, frame-relay, X.25. It is not used in modern Internet.

Datagram networks:

- no call setup at network layer
- routers: no state (information) about end-to-end connections.
- packet forwarded using destination host address. (No dedicated path)
  - destination host address → IP address

Datagram forwarding table: Instead of listing individual destination addresses, forwarding tables use address ranges. IP addressess in packet headers determine the output link.

Q: But what happens if ranges don't divide up so nicely?

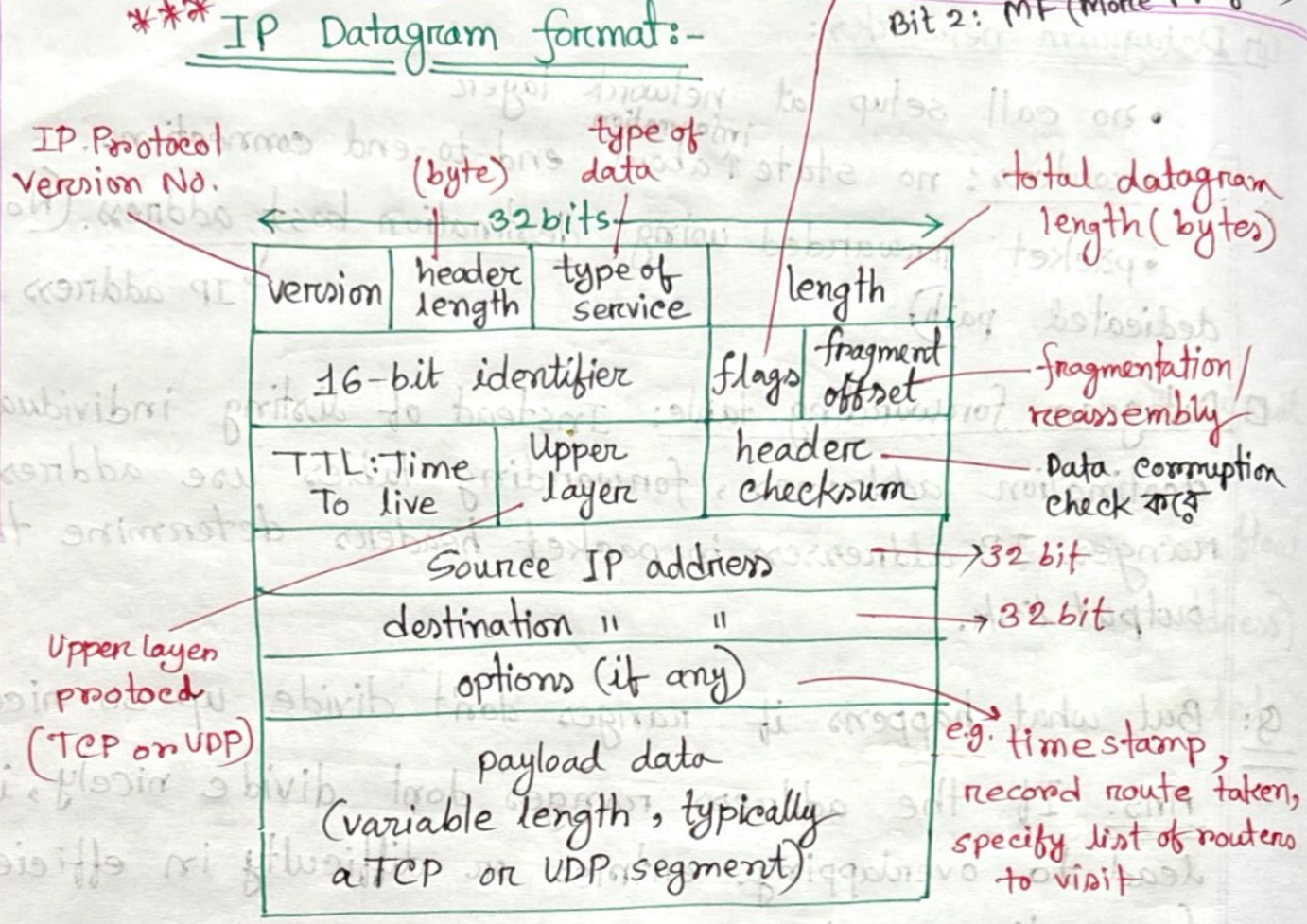
Ans: If the address ranges dont divide nicely, it can lead to overlapping entries or difficulty in efficiently forwarding packets.

Solution:

① Destination based-forwarding: The table still works by assigning destination ranges to specific link interfaces.

② Longest-Prefix matching: When multiple ranges overlap, the router selects the most specific match (longest matching prefix) ~~to determine that matches~~ to determine correct forwarding interface/route.

*** IP Datagram format:-



IP fragmentation/reassambly

Network link have MTU (maximum transfer size) - largest possible link-level frame.

Different link types has different MTUs. A large IP datagram may be fragmented, ~~as it travels throw~~ into multiple smaller datagrams. These fragments then transmitted seperately and only reassemble at destination. IP header contains specific bits that helps to identify and order fragments.

Example: slide 21

IP addressing: An IP address is a 32-bit identifier assigned to each host or router interface in a network.

Interface: It is a connection between host/router and physical link. Routers typically have multiple interfaces, while hosts usually have one or two. Each interface is assigned a unique IP address, which is written in dotted decimal notation (e.g. 192.168.1.1)

Notation:

- **Binary notation:**

  IP address is displayed as 32 bits

  Example: 01110101 10010101 11101010 11101010

- **Dotted - Decimal notation:**

  Example: 128.11.3.31

- **Hexadecimal notation:**

  Example: 0x7595 1DEA

Error:

111.56.045.78 → must be no leading zero

221.34.7.8.20 → can't be more than four number

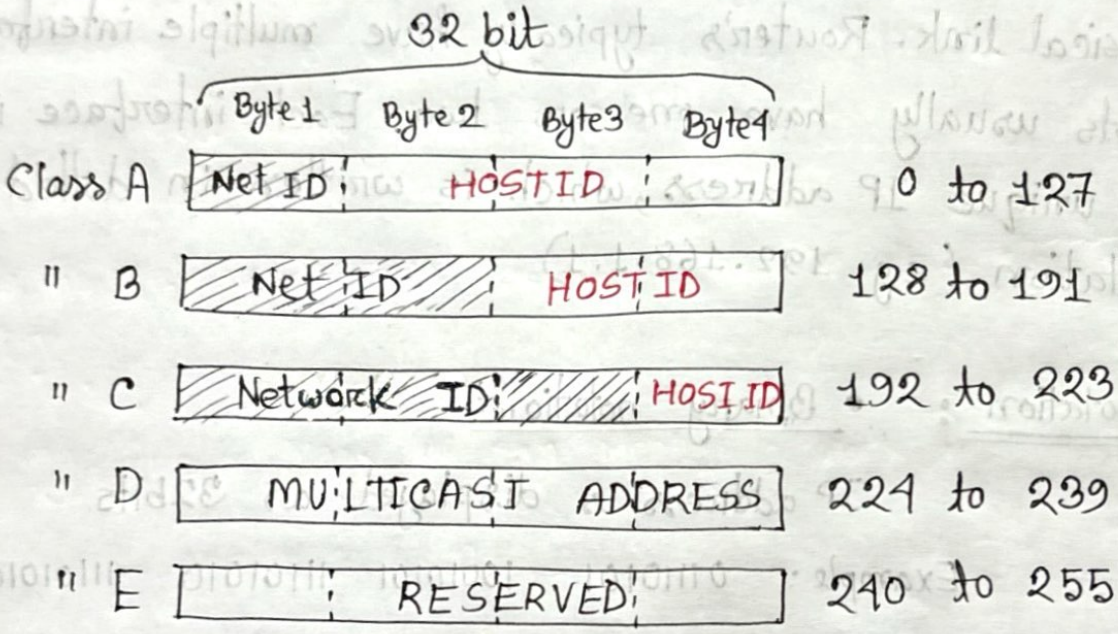
75.45.301.14 → each number need to be less than 255

11100010.23.14.67

mix of binary notation and dotted notation is not allowed.

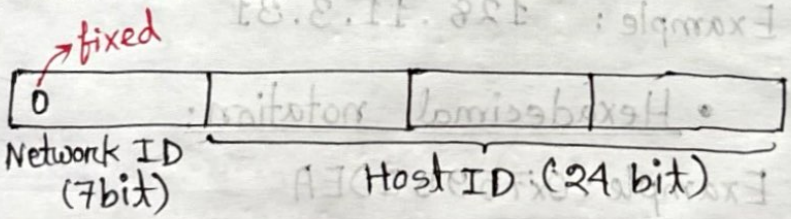
IP Addressing (Classful Addressing):

Classful method categorizes IP addresses into five classes (A, B, C, D and E)



Net ID = Network ID

Class A:

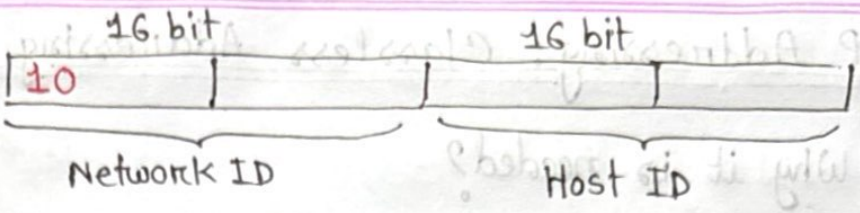


0-127

- Total IP Address: $2^{32-1} = 2^{31}$
- Total Number of network: 2^7 ⇒ No. of block
- Total " " host: 2^{24}
- Range = 0.0.0.0 – 127.255.255.255

128-191

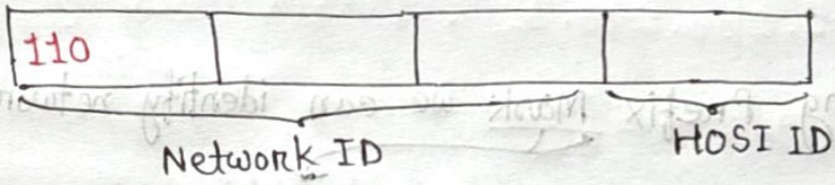
□ **Class B:**



- Total Number of IP address : 2^{30}
- " " " network : 2^{14} ⇒ No. of block
- " " " host : 2^{16}
- Range = 128.0.0.0 – 191.255.255.255

□ **Class C:**

192-223



- Total Number of IP address : 2^{29}
- " " " Network ID : 2^{21} ⇒ No. of Block
- " " " Host ID : 2^{8}

□ **Class D:** Addresses are multicast, where one sender, multiple recipients.

□ **Class E:** These addresses are reserved for special purposes.

Practice :

① 17.0.0.0
② 132.21.0.0
③ 220.34.76.0

IP Addressing: Classless Addressing

- Why it is needed?

In classful addressing, a large part of the available addresses were wasted. Whereas classless addressing is replaced with classful address.

- How do we or devices identify the network part and host part?

⇒ Using Prefix Mask we can identify network and host part

192.168.10.2 /24

first 24 bits are network portion
last 8 " " host "

For device:

Subnet mask: default 32 bits থাকে
Network portion কে 1, Host portion কে 0

192.16.8.0 /8 ⟶ 255.0.0.0

192.168.0.0/20 ⟶ 255.255.1111.0000
⇒ 255.255.240.0

Practise: slide 45

① IP Address : 10.24.36.2/8 , Subnet Mask = ?

⇒ 255.0.0.0

② IP Address : 10.24.36.2/12 , Subnet Mask = ?

11111111.11110000.00000000.00000000.

⇒ 255.240.0.0

③ IP Address 10.24.36.2/16 , Subnet Mask = ?

11111111.11111111.00000000.00000000

⇒ 255.255.0.0

④ 10.24.36.2/23 , Subnet mask = ?

11111111.11111111.11111110.00000000

⇒ 255.255.254.0.

⑤ IP Address 10.24.36.2

- Subnet Mask 255.255.224.0 , Prefix Mask = ?

⇒ 11111111.11111111.11100000.00000000

prefix length = 19

∴ Prefix Mask = 10.24.36.2/19

- Subnet Mask 255.255.255.192 , Prefix Mask = ?

⇒ 11111111.11111111.11111111.11000000

prefix length is = 26

∴ Prefix Mask = 10.24.36.2/26

- 255.255.255.252 , Prefix Mask = ?

⇒ 10.24.36.2/30

- 255.254.0.0 , Prefix ~~leng~~ Mask = ?

11111111.11111110.00000000.00000000

⇒ Prefix length = 15

⇒ 10.24.36.2/15

- 255.255.240.0 , Prefix Mask = ?

10.24.36.2/20

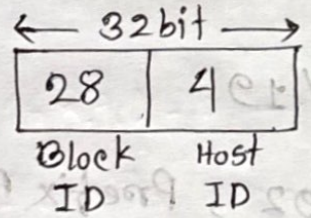
IP addressing : CIDR

CIDR = Classless InterDomain Routing

address format: a.b.c.d /(x)

prefix mask

Example: 200.10.20.40/28



No. of host 2^4.

- 200.10.20.40/28

200.10.20.00101000

28 bit

00100000

32

∴ Network ID is

⇒ 200.10.20.32/28

Network ID ber করতে AND operation ও use করে ও বলা যায়,

IP Address : 200.10.20.40
Subnet Mask : 255.255.255.240
200.10.20.32/28

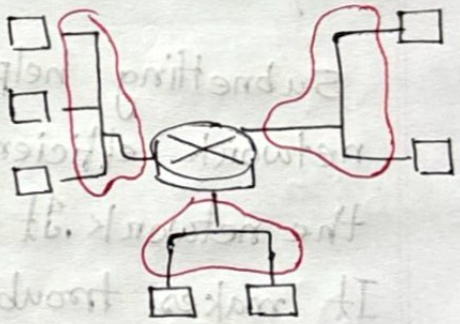
11001000
11111111
11001000 = 200

00101000
11110000
00100000 = 32

Subnets: Device interfaces that can physically reach each other without passing through routers.

IP addresses have structure:

- Subnet part (Network ID)
  223.1.1.0/24
- Host part (Host ID)



each "island" or isolated network is called subnet.

Page-52 Example

167.199.170.82/27

What is the network address?

167.199.10101010.01010010

27 bit

00000

01000000

64

∴ Network Address is 167.199.170.64/27

Calculating Subnets and hosts

Subnets create এর জন্য host part কে বড় করতে হবে।

So, Subnets are created using one or more of the host bits as network bits. It is done by extending the mask to borrow some of the bits from the host portion to create additional network bits.

Subnet: $2^{\text{No. of subnet bits}} = 2^n$

Usable/Valid Hosts: $2^{\text{No of host bits}} - 2 = 2^h - 2$ (network address, broadcast ॥)

Subnetting help to prevent waste of IP addresses, improve network efficiency by isolating different parts of the network. It also improve security by isolating network. It makes troubleshooting and network control easier.

Example of subnetting:

if ~~yove~~ you have class C network 192.168.1.0/24 you can subnet it into smaller networks:

192.168.1.0/25 → 2 subnets

⇒ 25 bits represent network, 7 bits represent the host.

11111111.11111111.11111111.10000000

Since we're using /25, so we are borrowing 1 extra bit from host portion.

∴ Subnet = $2^1 = 2$ subnets.

So we divide the network into 2 subnets

Where, usable host per subnet is $2^7 = 126$

The two subnet will be,

Subnet 1: 192.168.1.0/25 ⟶ Host range : 192.168.1.1 - 192.168.1.126

Network Address — Usable host ID

Broadcast address : 192.168.1.127

Subnet 2: 192.168.1.128/25 ⟶ 192.168.1.129 - 192...254

network address

Broadcast address : 192.168.1.255

Page-57

130.34.12.64/26

32-26 = 6 bit are available as hostid.

~~usable host per subnet~~ $= 2^6 = 64$ = no of hosts

↳ total number of addresses in block

Network address: 255.255.255.01000000

To have ~~for~~ 4 subnets, we need to borrow 2 more bits from host portion. ∴ New subnet = /28

each subnet will have 16 addresses $= 2^4$

Subnet 1: 130.34.12.64/28 – 130.34.12.79/28

Subnet 2: 130.34.12.80/28 – 130.34.12.95/28

Subnet 3: 130.34.12.96/28 – 130.34.12.111/28

Subnet 4: 130.34.12.112/28 – 130.34.12.127/28

190.100.0.0/16

(a) for each ↑ 256 addresses, we need 8 bits to define each host, 32 - 8 = 24 is prefix length.

New subnet prefix is 24.

1st customer : 190.100.0.0/24 - 190.100.0.255/24
2nd " : 190.100.1.0/24 - 190.100.1.255/24
3rd " : 190.100.2.0/24 - 190.100.2.255/24
⋮ ⋮ ⋮ ⋮
64th " : 190.100.63.0/24 - 190.100.63.255/24

(b) 128 customers

for each 128 .

DHCP: Dynamic Host Configuration Protocol

dynamically get address from as server.

DHCP allows a host to obtain IP address automatically.

⇒ DHCP is a service that automatically gives devices an IP address when they join network. It connects devices without manual set up.

goal: host dynamically obtains IP address from network servers when it joins network.

- can renew it lease on address in use
- allows reuse of addresses (only hold address while connected / on)
- support mobile users who join / leave network.

DHCP overview:

- host broadcasts: DHCP discover message
- DHCP server responds with: DHCP offer message
- host requests IP address: DHCP request "
- DHCP server sends address: DHCP ack "

NAT: Network Address Translation

Private IP কে Public IP তে Translate করে

Public " " Private " " " "

all devices in local network share just one IPv4 address as far as outside world is concerned.

⇒ NAT is a technique used in routers to allow multiple devices on a private network to share a single public IP address to access the internet

Advantages:

- Just one IP address needed from provider ISP for all devices.
- Can change addresses of host in local network without notifying outside world.
- Can change ISP without changing addresses of devices in local network.
- Security: devices inside local network not directly addressable, visible by outside world.

• How NAT works?

A NAT router operates transparently, which means devices in the local network don't even notice the translation process.

• Outgoing datagrams (From Local Devices to the Internet)

→ NAT Router replaces source IP address (private IP) and port number with public NAT IP address and a new port number.

→ Remote clients / servers respond to NAT Router using (NAT IP address, new port) as destination address.

→ It saves every (source IP address, Port #) to NAT IP address, new port #) translation pair in NAT Translation Table.

Incoming datagrams: When response come back, it reaches NAT router as it public IP and new port #.
~~When~~ The router checks NAT Table and finding match, it replaces destination IP (pubic IP) with corresponding private IP and port #.

IPv6:-

IPv4 ⟶ 32 bit
IPv6 ⟶ 128 bit

- fixed length 40 byte header
- no fragmentation allowed
- ভার Block সাপোর্ট
- Better traffic handling
  ⇒ IpV6 enable different network layer treatment for flows of traffic

128 bit = 16 bytes = 32 hexa decimal digits

Addreviated Address (Address কে short করে লিখা)

Rule 1: Drop leading zeroes

0074 ⟶ 74
000F ⟶ F

Rule-2: Collapse Consecutive Zeroes

0:0:0:0 ⟶ ::

only use once in an address

Exercise :-

- FDEC : BA98 : 0074 : 3210 : 000F : 0000 : FFFF

⇒ FDEC : BA98 : 74 : 3210 : F : 0 : FFFF

- FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF , addreviate :—

⇒ FDEC : : BBFF : 0 : FFFF

ore, ⇒ FDEC : 0 : 0 : 0 : 0 : BBFF : : FFFF

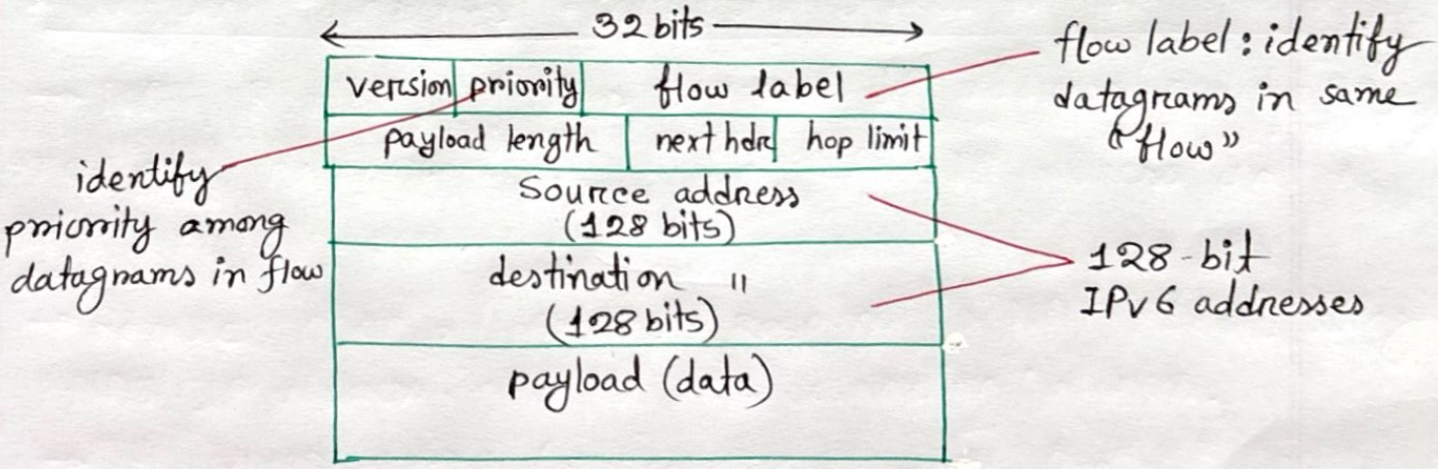
- ABBA : CAB : 1234 : : FEED : 3 : BEEF , complete this :—

⇒ ABBA : 0CAB : 1234 : 0000 : 0000 : FEED : 0003 : BEEF

- ABBA : : 7 : : FEED ; complete this —

⇒ invalid. Only one group of zeroes can be suppressed.

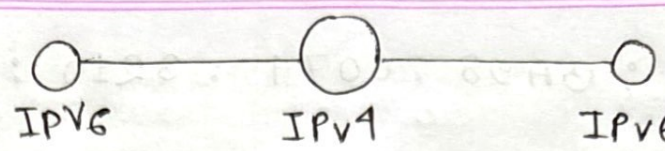
IPv6 datagram format:



Compared to IPv4 :

- no checksum (to speed processing at routers)
- no fragmentation / reassembly
- no option (available as upper layer, next header protocol at router)

Tunneling:



IPv6 এর packet কে IPv4 এর packet এ compress করে, আবার IPv6 যখন দরকার হয় তখন ওই packet কে IPv6 এ নেয়।

~~Prob~~ Why Tunneling is used?

- Helps Ipv6 traffic cross IPv4 networks without modifying existing routers.
- Provides a transition method