Network Layer of the internet

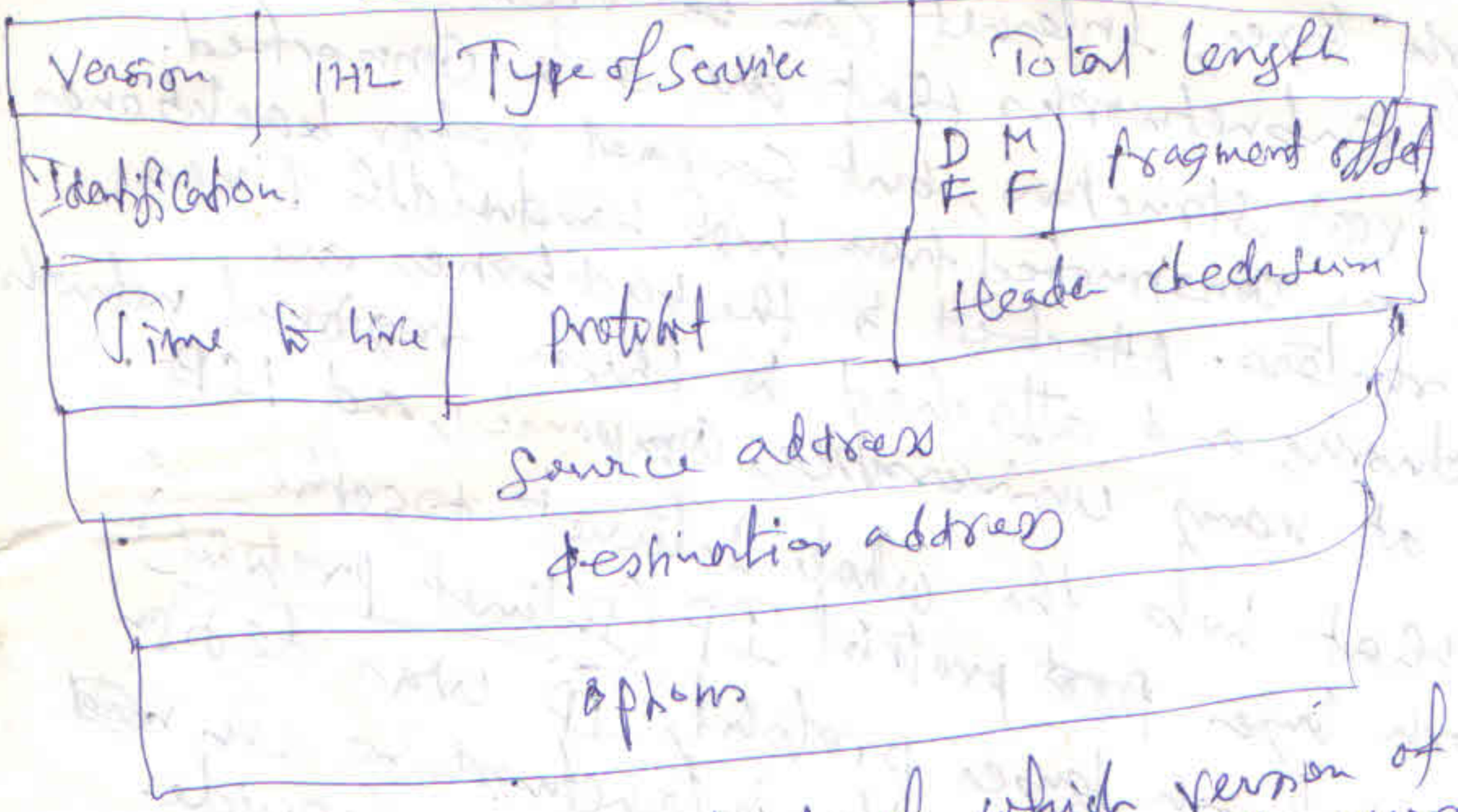
At the network layer, Internet can be viewed as a collection of subnetworks that are inter-connected. there is no real structure, but several major backbones exist. there are constructed from high-bandwidth lines and fast routers. Attached to the backbones are regional networks, and attached to them are LANs at many universities, companies, and ISPs. the glue that hob the whol Internet together is the network layer protocol IP (Internet protocol). Unlike older network layer protocol, IP was designed from the very beginning with internetworking in mind. The job of network layer is to provide a best-efforts way to transport datagrams from source to destination, without regard to whether these machines are on the same network or whether there are other networks in between.

How Communication takes place in the Internet

The Communication in the Internet works as follows - The transport layer takes data streams and breaks them up into datagrams. Each datagram is transmitted through the Internet possibly being fragmented into smaller units as it goes. when all the pices finally get to the destination machine, they are reassembled by the network layer into the original datagram. The datagram is then handed to the transport layer, which enters it into the receiving process' input stream.

Format of the IP datagram. An IP datagram consists of a header part and a data part. The header has a 20-byte fixed part and a variable length part.

The IPv4 header



The version field keeps track of which version of the protocol the datagram belongs to. By including the version in each datagram, it becomes possible to have the transition between versions (For example IPv4 & IPv6) with some ~~m~~ running the old version and other running new one

IHL provides the length of the header in 32-bit words as the header length is not constant. Minimum value of it is 5 (i.e. 20-byte) and maximum value is (60-byte). For the later one, option field is 40-bytes as the fixed part is 20-byte

Type of service field is used to distinguish between different classes of service such as voice, file transfer etc. For voice, fast delivery is more important than accurate delivery, whereas for file transfer error-free transmission is more important than fast delivery. This 6-bit field contains 3-bit precedence field and three flags D, T and R. The precedence field is the priority from 0 to 7 and the three flags allowed the host to specify what it cared most from the set {Delay, throughput, Reliability}. These fields allow the routers to make appropriate routing decisions.

The Total length includes everything in the datagram — both header and data. The maximum is 65535 bytes. At present this upper limit is tolerable but with future gigabit networks, larger datagram may be needed.

The Identification field is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragment of datagram contain the same Identification value.

Next comes two 1-bit fields DF and MF. DF stands for Don't fragment and MF stands for More fragment. DF is required as some destination is incapable of putting the pieces back together again. For example, when a computer boots ROM might ask a memory image to be sent to it in a single datagram.

fragment offset tells where in the datagram this fragment belongs. Since 13-bits are provided, there is a maximum of 8192 fragments per datagram, giving a maximum datagram length of 65,536 bytes.

The Time to Live field is a counter used to limit packet lifetime. Normally measured in number of hops. It must be decremented on each hop and dropped to be decremented multiple times when queued for a long time in a router. ⊕

The protocol field tells which transport process to give the datagram. TCP is one possibility, but so are UDP and some others. Numbering of protocol is global across the entire Internet

The header checksum verifies the header only. Such checksum is useful for detecting error generated by bad memory words inside a router. Normally this checksum is recomputed at each hop because at least one field always changes (Time to live).

the source address and destination address indicate the network number and host number. This will be discuss in details later on.

the options field was designed to provide information not present in the original design, to permit experimenters to try out new ideas. The following five options are defined currently.

option	description
Security	specified how secret the datagram is
Strict source routing	give the complete path to be followed (a sequence of IP addresses)
Loose " "	Give a list of routers not to be missed
Record route	make each router append its IP address (for debugging purpose)
Time stamp	make each router append its address and time stamp (for debugging purpose)

IPv6

* due to Deering and Francis:
* SIPP – Simple Internet protocol plus (original name).

~~the reason~~ Ultimate Goal:
1. Support billions of host. 2. Reduce routing table size
3. Simplify the protocol to work faster. 4. Provide better security
5. More attention to type of service, particularly real-time data
6. Aid multicasting by allowing scopes to be specified.
7. Make it possible for host to roam without changing it address.
8. permit old and new protocol to co-exist for years.
9. Allow the protocol to evolve in future.

major features → ① IPv6 has longer address than IPv4 (128-bit vs 32-bit).
② Simplification of header. It contains only seven field. this change allows router to process packets faster.
③ Better support for options. this way options are represented, is it is now simple for routers to skip options not intended for them. this speed up the processing time.
④ Better Security.

The main IPv6 header —

Version	Traffic class	Flow label	
Payload byte	Next header	Hop limit	
Source address (16 bytes)			
Destination address (16 bytes)			

① Version field specifies the version of protocol. It is 4 for IPv4 and 6 for IPv6.
② Traffic class – to distinguish between packets with different real-time requirements.
③ ~~to~~ Flow label – to allow a source and destination to set up a pseudo-connection with particular requirement. for example, a stream of packet might have stringent delay requirements and then need reserved bandwidth. When a packet with non-zero flow label comes, the router can look it up what kind of special requirement it has. Here the flexibility of datagram Subnet and guarantees of virtual-Circuit comes up again.

(4) Payload length – tells how many bytes follow the 40-byte header. The name Total length used in IPv4 is changed as the meaning is different. The payload length does not include 40-byte header.

(5) Next header – In IPv6 there are optional extension header. this next header field tells which of the six extension headers, if any, follow this one. If this header is last, next header say which of TCP, UDP to pass the packet.

[Extension header – six kind of extension headers are defined at present. If more than one is present, they must appear in short order. ~~Some are fixed~~

Hop-by-hop options – all routers along the path must be visited

Destination options – more information for the destination so that routing algo can be made more efficient.

Routing – ~~list of one or more~~ (more strict routes) lose list of routers to visit. other not listed can be visited too.

fragmentation – deals with fragmentation and holds the datagram identifier, fragment number and a bit telling whether more fragments will follow. Unlike in IPv4, IPv6 allows only the source host to fragment a packet. Routers along the way may not do this. It simplies the routers works and makes routing faster.

Authentication – receiver of a packet can be sure who send it.

Encrypted security payload – allows encrypt the content of a packet so that only the intended recipient can read it through cryptographic techniques.]

(6) Hop limit – same as Time to live in IPv4. As we router use time in second and prefer hop count to be use, the name has been changed.

Source and destination address - fixed length 16-byte addresses. the notation of writing 16-byte addresses are — 8000 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF i,e., eight group of four hexadecimal digits with colons between the groups. The leading zeros within a group can be omitted, so 0123 can be written as 123. One or more group of 16 zeros can be replaced by a pair of colon. thus, 8000 : : 123 : 4567 : 89AD : CDEF ~~is deleted~~. The dotted decimal can be written in combination with colon such as : : 192.31.20.46.

What left out from IPv4 in IPv6: IHL field gone as IPv6 header has fixed length. protocol field not there as next header tells what follows the last IP header (e.g. TCP, UDP). fragmentation fields are removed as there are taken care here differently. checksum also removed as DLL and Transport layer normally have there own checksum so not required.

The Internet transport protocol : UDP