CHAPTER 2

2. Internet Protocol Overview **6 Hrs.**

2.1 TCP/IP and the IP Layer overview

[Resource: *.PPT Files.]

2.2 IPv4 and IPv6 Address Types and Formats

What Is an IP Address?

An IP address is a series of binary numbers that provide information about the network and the host (the computer or other device). These numbers are typically written as four numbers separated by dots in the older, IP Version 4 (IPv4) address numbering that is most common. Because the number of available addresses in the IPv4 format is limited and running out, a new numbering scheme called IPv6 was devised in the 1990s. In this format, IP addresses are written as eight groups of four letters and numbers separated by colons, although groups with zero value may be omitted. Private addresses are known as "local-use" in IPv6.

Public Addresses

Public IP addresses are those that allow any two computers to identify each other. When a person connects to the Internet, his/her computer is usually assigned an address from a pool that has been set aside for her Internet Service Provider (ISP) to use for its customers. When s/he types in a website address — that domain name is converted into the IP address for the server that hosts the website. The server uses the computer's public IP address to know where to send the requested site page.

Most of the addresses in the IPv4 host range are public addresses. These addresses are designed for used by hosts that are publicly accessible from the Internet. Even within these address blocks, there are many addresses that are designated for other special purposes.

Private Addresses

When several computers or devices are connected to each other, either with cables or wirelessly, they can make up a private network. Each device within this network is assigned a different IP address in order to exchange files and share resources within the network. Although addresses must be unique within the private network, different private networks could all use the same addresses; since the computers in different networks don't directly communicate, it doesn't matter if they have the same

address. A device called a network router passes data back and forth among the connected computers using the private IP addresses as identifiers.

The private network, or one of the computers in the network, usually connects to the Internet through a modem. The router or firewall within the network is assigned a public IP address by the Internet Service Provider (ISP); this single public IP address identifies the entire network on the Internet. Using a built-in device called a Network Address Translator (NAT), the router acts as a gatekeeper and passes requests from individual computer users to the Internet. Returning data is delivered back to the public IP address, with the router determining which private IP address requested the information.

Private IP addresses that are designated for networks that have limited or no access to the Internet. Hosts or packets using these addresses as a source and destination are not to appear on the public Internet.

These private address blocks are:

10.0.0.0 – 10.255.255.255 (10.0.0.0 /8)

10.0.1.0 – 172.16.0.0 to 172.16.255.255 (172.16.0.0 /12)

10.0.2.0 – 192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

What is IPv6?

IPv6 is short for "Internet Protocol Version 6". IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4.

In order to communicate over the Internet, computers and other devices must have sender and receiver addresses. These numeric addresses are known as Internet Protocol addresses. As the Internet and the number of people using it grows exponentially, so does the need for IP addresses.

IPv6 is a standard developed by the Internet Engineering Task Force, an organization that develops Internet technologies. The IETF, anticipating the need for more IP addresses, created IPv6 to accommodate the growing number of users and devices accessing the Internet.

IPv6 allows more users and devices to communicate on the Internet by using bigger numbers to create IP addresses. Under IPv4, every IP address is 32 bits long, which allows 4.3 billion unique addresses. An example IPv4 address is:

172.16.254.1

In comparison, IPv6 addresses are 128 bits, which allow for approximately three hundred and forty trillion, trillion unique IP addresses. An example IPv6 address is:

2001:db8:ffff:1:201:02ff:fe03:0405

IPv6 offers other networking advantages. In most cases, computers and applications will detect and take advantage of IPv6-enabled networks and services without requiring any action from the user. IPv6 also relieves other networking issues that can arise due to the limited number of addresses available on IPv4. For example, IPv6 reduces the need for Network Address Translation, a service that allows multiple clients to share a single IP address, but is not always reliable.

- To test your IPv6 connectivity, you can visit **Test your IPv6**.

http://[3ffe:1900:4545:3:200:f8ff:fe21:67cf]:80/index.html

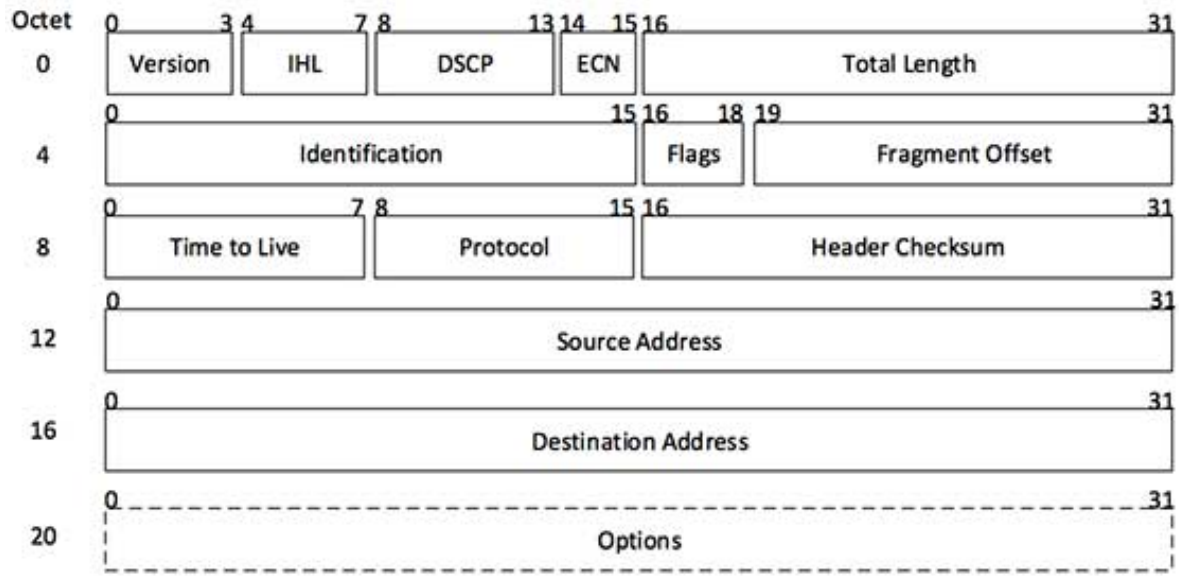
2.3 IPv4 and IPv6 Header Structure

Packet Header

Packet Headers are affixed to the beginning of all IP packets. You can think of them as being like "shipping labels" pasted on a package. A Packet Header contains a "from" address (where the packet is being sent from) called the ***source address***; and a "to" address (where the packet is going) called the ***destination address***. In the case of packets, these addresses are not "street" addresses, but IP addresses. On IPv4 packets, there is an IPv4 Packet Header. On IPv6 packets, there is an IPv6 Packet Header. These have the same purpose, but are fairly different due to improvements in the IPv6 protocol.

IPv4

The IPv4 Packet Header is 20 bytes long (plus the length of the options field, if any). All but one bit of the first 20 bytes has long since been accounted for. There is no official Header Extension mechanism. Some fields are used only in fragmented packets, but take up room on all packets.



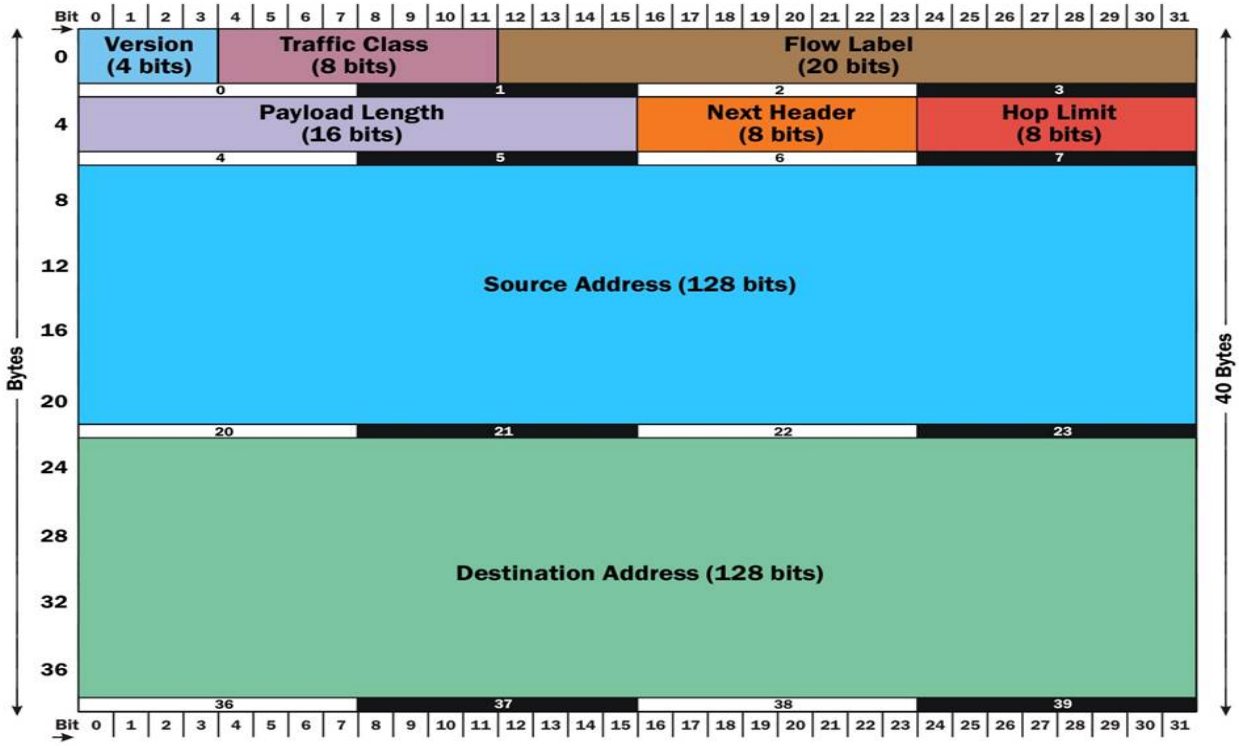
[Image: IP Header]

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, 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 no. 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' tell that 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, and Time Stamp etc.

IPv6

The IPv6 Packet Header is actually simpler than the IPv4 Packet Header, because some fields were eliminated, and others moved to Extension Headers. It is twice as large (40 bytes) due to the gigantic (128-bit) source and destination IPv6 addresses (four times the size of IPv4 addresses). Every bit of the basic IPv6 Packet Header has been accounted for, but it is possible to add any number of new ***Extension Headers***, which didn't exist in IPv4, so this is not a problem.

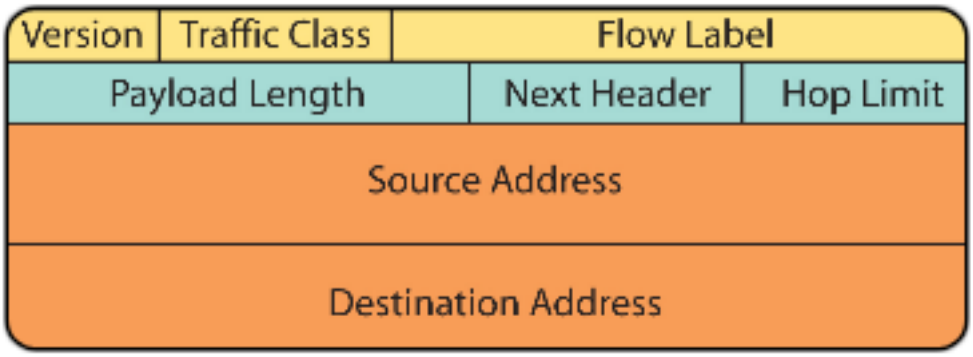


The changes from IPv4 Packet Header to IPv6 Packet Header are as follows:

- IPv4 **Version** field - same size (4 bits), same name, same function, in IPv6 Packet Header.
- IPv4 **IHL** (Internet Header Length) field - ***discarded*** since IPv6 Packet Header is fixed length (40 bytes).
- IPv4 **Type of Service** field - same size (8 bits), ***new name*** (**Traffic Class**), same function in IPv6 Packet Header.
- IPv4 **Total Length** field - same size (16 bits), ***new name*** (**Payload Length**), now does not include length of the Packet Header, so new Payload Length = old Total Length - 40.
- IPv4 **Identification (Fragment ID)** field - twice as big (32 bits), same name, same function, ***moved to Fragmentation Extension Header.***
- IPv4 **DF** flag - ***discarded***, effectively always 1 (set) in IPv6.
- IPv4 **MF** flag -same size (1 bit), same name, same function, ***moved to Fragmentation Extension Header***.
- IPv4 **Fragment Offset** field - same size (13 bits), same name, same function, ***moved to Fragmentation Extension Header***.

- IPv4 **Time-To-Live (TTL)** field - same size (8 bits), ***new name*** (**Hop Limit**), same function in IPv6 Packet Header.
- IPv4 **Protocol** field - same size (8 bits), ***new name*** (**Next Header**), same function, in IPv6 Packet Header. There is a new set of possible values (some are the same as in the Protocol field in the IPv4 Packet Header, such as values for TCP, UDP and SCTP).
- IPv4 **Header Checksum** field - ***discarded***, considered to be superfluous.
- IPv4 **Source Address** field - ***new size*** (128 bits instead of 32), same name, same function, in IPv6 Packet Header.
- IPv4 **Destination Address** field - ***new size*** (128 bits instead of 32), same name, same function, in IPv6 Packet Header.
- IPv4 **Options** field - ***discarded*** (virtually never used in IPv4 Packet Header) - now Packet Header is fixed length (40 bytes) instead of 20 bytes + length of options field.

An Internet Protocol version 6 (IPv6) data packet comprises of two main parts: the header and the payload. The first 40 bytes/octets (40x8 = 320 bits) of an IPv6 packet comprise of the header that contains the following fields:



Source address (128 bits) The 128-bit source address field contains the IPv6 address of the originating node of the packet. It is the address of the originator of the IPv6 packet.

Destination address (128 bits) The 128-bit contains the destination address of the recipient node of the IPv6 packet. It is the address of the intended recipient of the IPv6 packet.

Version/IP version (4-bits) The 4-bit version field contains the number 6. It indicates the version of the IPv6 protocol. This field is the same size as the IPv4 version field that contains the number 4. However, this field has a limited use because IPv4 and IPv6 packets are not distinguished based on the value in the

version field but by the protocol type present in the layer 2 envelope.

Packet priority/Traffic class (8 bits) The 8-bit Priority field in the IPv6 header can assume different values to enable the source node to differentiate between the packets generated by it by associating different delivery priorities to them. This field is subsequently used by the originating node and the routers to identify the data packets that belong to the same traffic class and distinguish between packets with different priorities.

Flow Label/QoS management (20 bits) The 20-bit flow label field in the IPv6 header can be used by a source to label a set of packets belonging to the same flow. A flow is uniquely identified by the combination of the source address and of a non-zero Flow label. Multiple active flows may exist from a source to a destination as well as traffic that are not associated with any flow (Flow label = 0). The IPv6 routers must handle the packets belonging to the same flow in a similar fashion. The information on handling of IPv6 data packets belonging to a given flow may be specified within the data packets themselves or it may be conveyed by a control protocol such as the RSVP (Resource reSerVation Protocol).

When routers receive the first packet of a new flow, they can process the information carried by the IPv6 header, Routing header, and Hop-by-Hop extension headers, and store the result (e.g. determining the retransmission of specific IPv6 data packets) in a cache memory and use the result to route all other packets belonging to the same flow (having the same source address and the same Flow Label), by using the data stored in the cache memory.

Payload length in bytes (16 bits) The 16-bit payload length field contains the length of the data field in octets/bits following the IPv6 packet header. The 16-bit Payload length field puts an upper limit on the maximum packet payload to 64 kilobytes. In case a higher packet payload is required, a Jumbo payload extension header is provided in the IPv6 protocol. A Jumbo payload is indicated by the value zero in the Payload Length field and are frequently used in supercomputer communication using the IPv6 protocol to transmit heavy data payload.

Next Header (8 bits) The 8-bit Next Header field identifies the type of header immediately following the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet. This field usually specifies the transport layer protocol used by a packet's payload. The two most common kinds of Next Headers are TCP (6) and UDP (17), but many other headers are also possible. The format adopted for this field is the one proposed for IPv4 by RFC 1700. In case of IPv6 protocol, the Next Header field is similar to

the IPv4 Protocol field.

Time To Live (TTL)/Hop Limit (8 bits) The 8-bit Hop Limit field is decremented by one, by each node (typically a router) that forwards a packet. If the Hop Limit field is decremented to zero, the packet is discarded. The main function of this field is to identify and to discard packets that are stuck in an indefinite loop due to any routing information errors. The 8-bit field also puts an upper limit on the maximum number of links between two IPv6 nodes. In this way, an IPv6 data packet is allowed a maximum of 255 hops before it is eventually discarded. An IPv6 data packet can pas through a maximum of 254 routers before being discarded.

RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification.

2.4 Internet RFCs

A **Request for Comments** (**RFC**) is a publication of the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet.

An RFC is authored by engineers and computer scientists in the form of a memorandum describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. It is submitted either for peer review or simply to convey new concepts, information, or (occasionally) engineering humor. The IETF adopts some of the proposals published as RFCs as Internet standards.

RFC Index - http://www.rfc-editor.org/rfc-index.html

e.g.

RFC 792 — *Internet Control Message Protocol*

RFC 768 — *User Datagram Protocol*

RFC 793 — *Transmission Control Protocol*

RFC 854 — *Telnet Protocol specification*

RFC 855 — *Telnet option specifications*

RFC 959 — *File Transfer U*pdated by RFC 2228, RFC 2640

RFC 821 — *Simple Mail Transfer Protocol*

RFC 1034 — *Domain names - concepts and facilities*, Updated by RFC 2535, RFC 2308, RFC 2181, RFC 1982,RFC 1876, RFC 1348, RFC 1183, RFC 1101

RFC 1035 — *Domain names - implementation and specification* Updated by RFC 2535, RFC 2308, RFC 2181,RFC 2137, RFC 2136, RFC 1996, RFC 1995, RFC 1982, RFC 1876, RFC 1348, RFC 1183, RFC 1101

RFC 974 — *Mail routing and the domain system*

RFC 1157 — *A Simple Network Management Protocol*, Updated by RFC 1098.

RFC 903 — *Reverse Address Resolution Protocol*

RFC 1661 — *The Point-to-Point Protocol*

RFC 1939 — *Post Office Protocol*

[Resource: *.PPT Files.]

~