Internet Protocol Version 4 *IPv4*

Internet Protocol is one of the major protocol in TCP/IP protocols suite.

This protocol works at Network layer of OSI model and at Internet layer of TCP/IP model.

Thus this protocol has the responsibility of identification of hosts based upon their logical addresses and to route data between/among them over the underlying network.

IP provides a mechanism to uniquely identify host by IP addressing scheme.

IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to destined host but it will do its best to reach the destination.

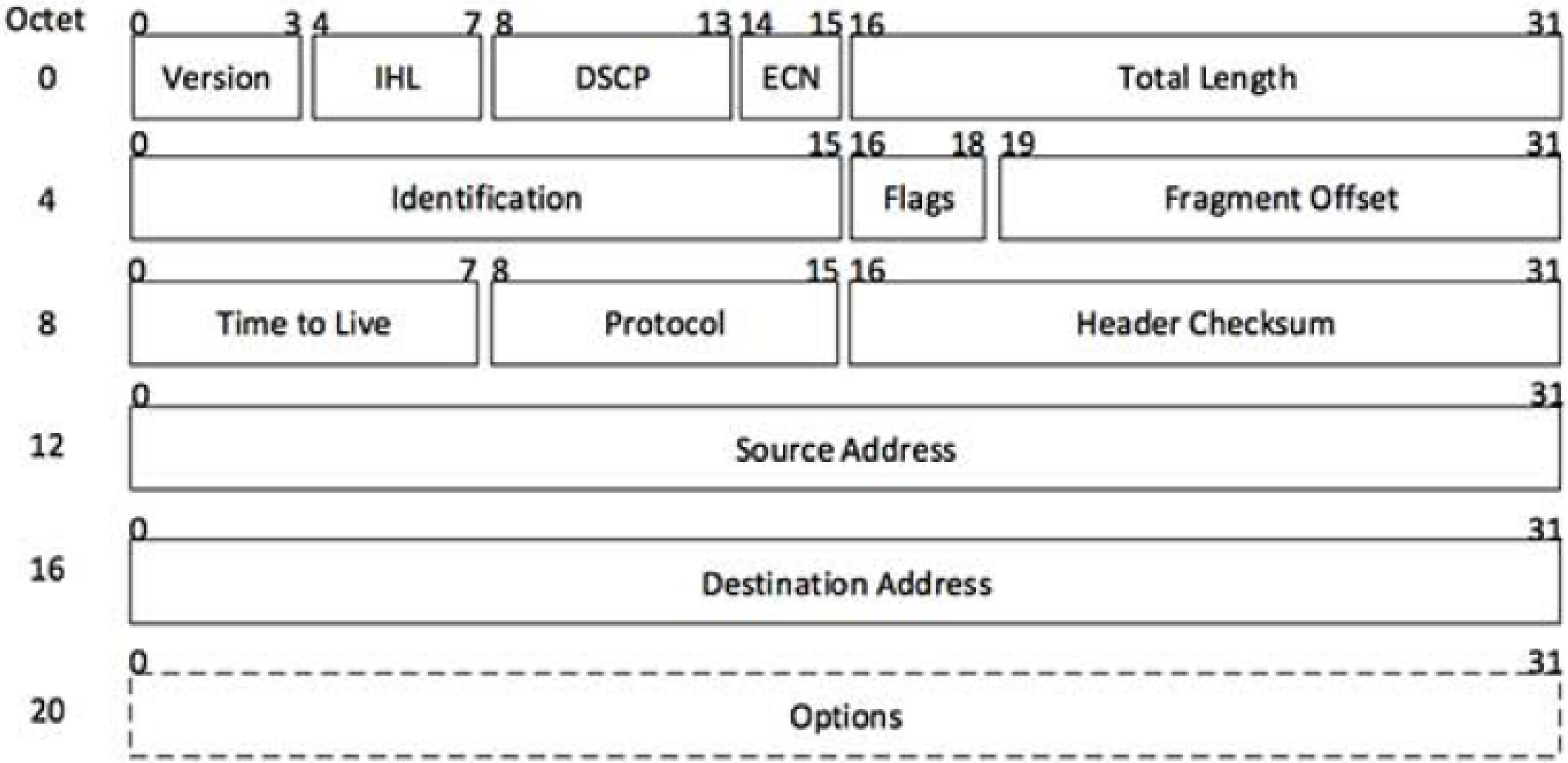
Internet Protocol version 4 uses 32-bit logical address.

IPV4 - PACKET STRUCTURE

Internet Protocol being a layer-3 protocol *OSI* takes data Segments from layer-4 *Transport* and divides it into what's called packet. IP packet encapsulates data unit received from above layer and adds its own header information.

(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

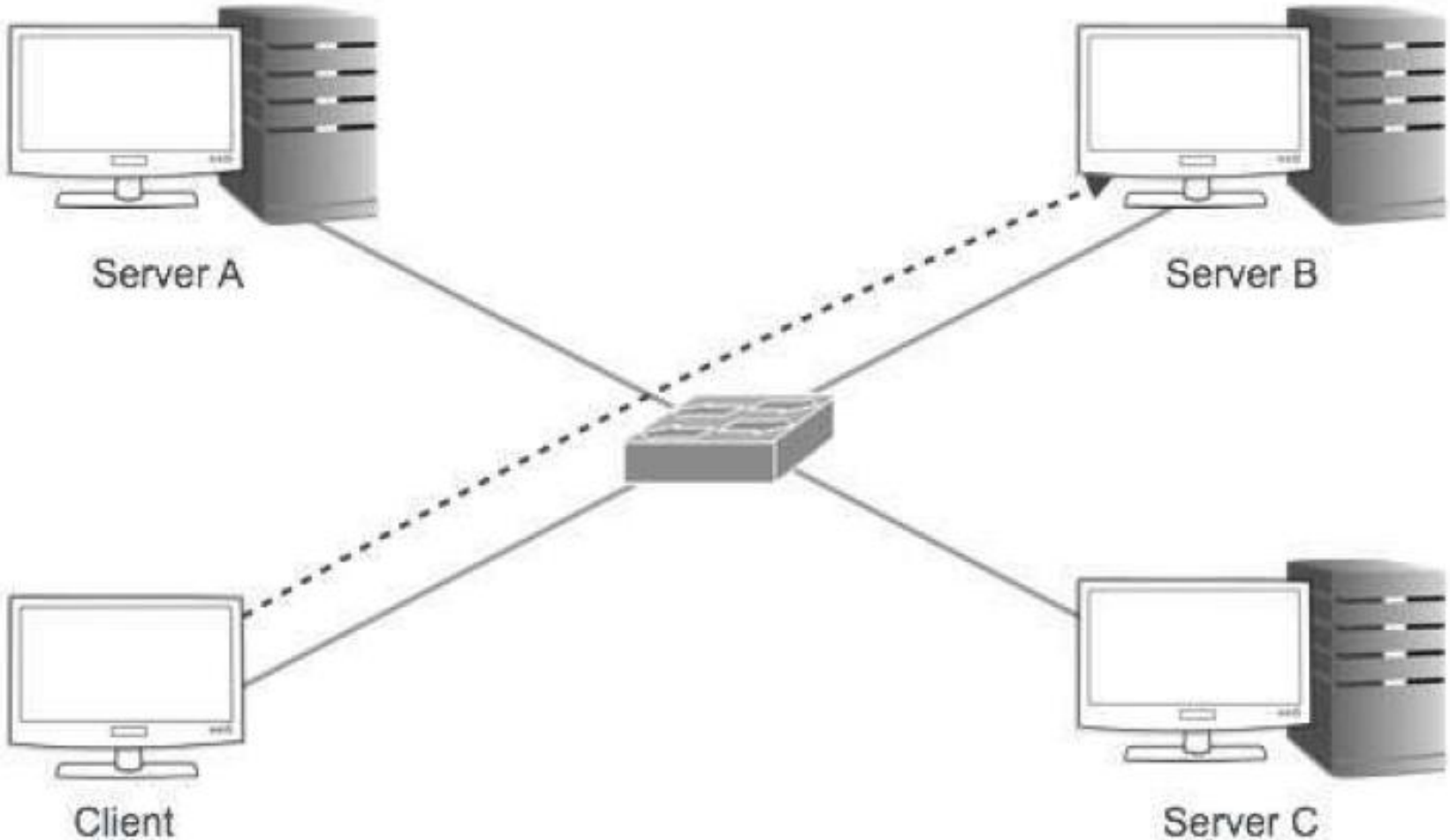
- **Version:** Version no. of Internet Protocol used *e. g. IPv4*
- **IHL:** Internet Header Length, Length of entire IP header
- **DSCP:** Differentiated Services Code Point, This is Type of Service.
- **ECN:** Explicit Congestion Notification, carries information about the congestion seen in the route.
- **Total Length:** Length of entire IP Packet *includingIPheaderandIPPayload*
- **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 *orsource* of the packet.
- **Destination Address:** 32-bit address of the Receiver *ordestination* of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These option may contain values for options such as Security, Record Route, Time Stamp etc.

IPV4 - ADDRESSING

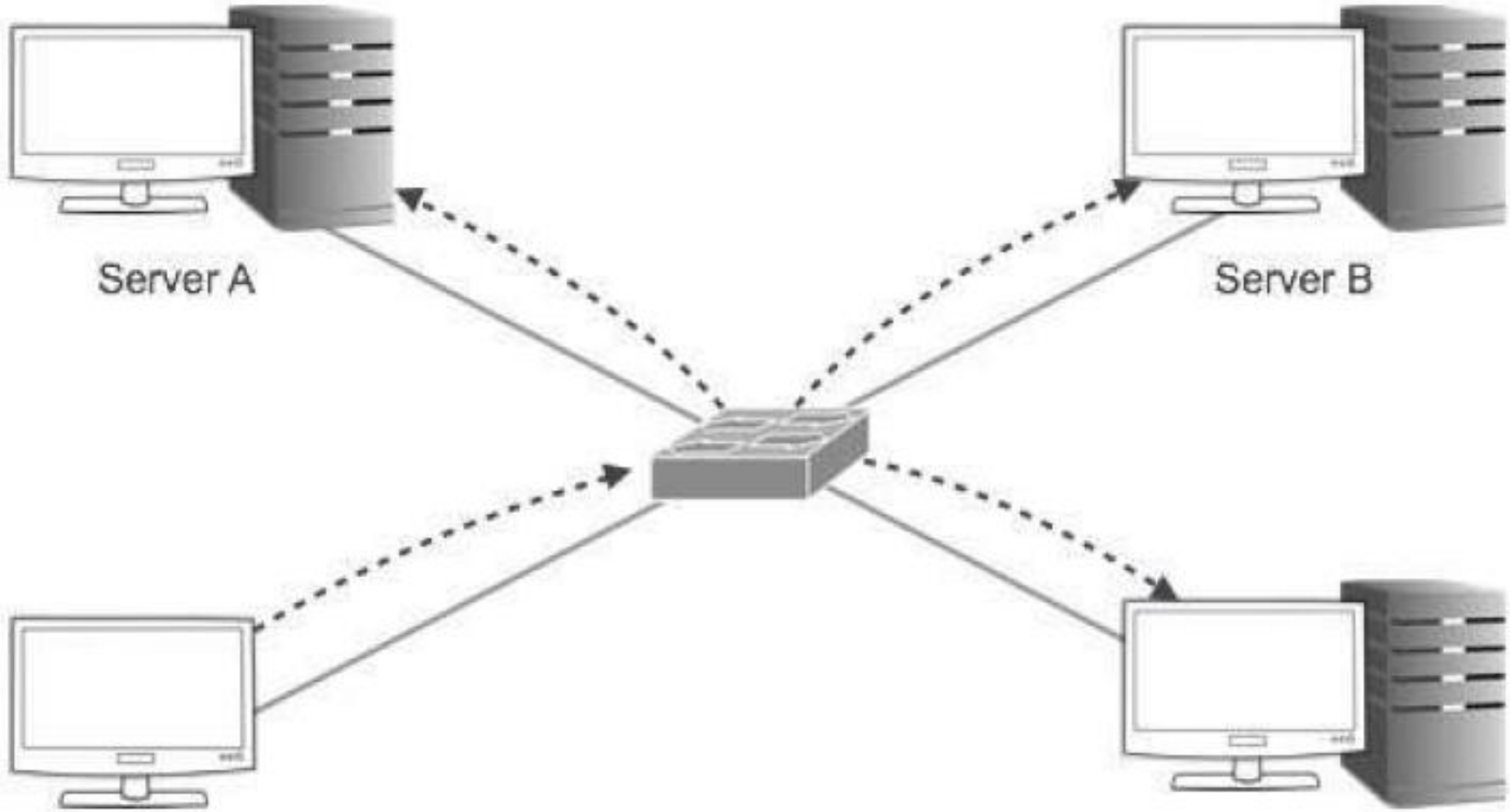
Unicast Addressing Mode:

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here client sends data to the targeted server:



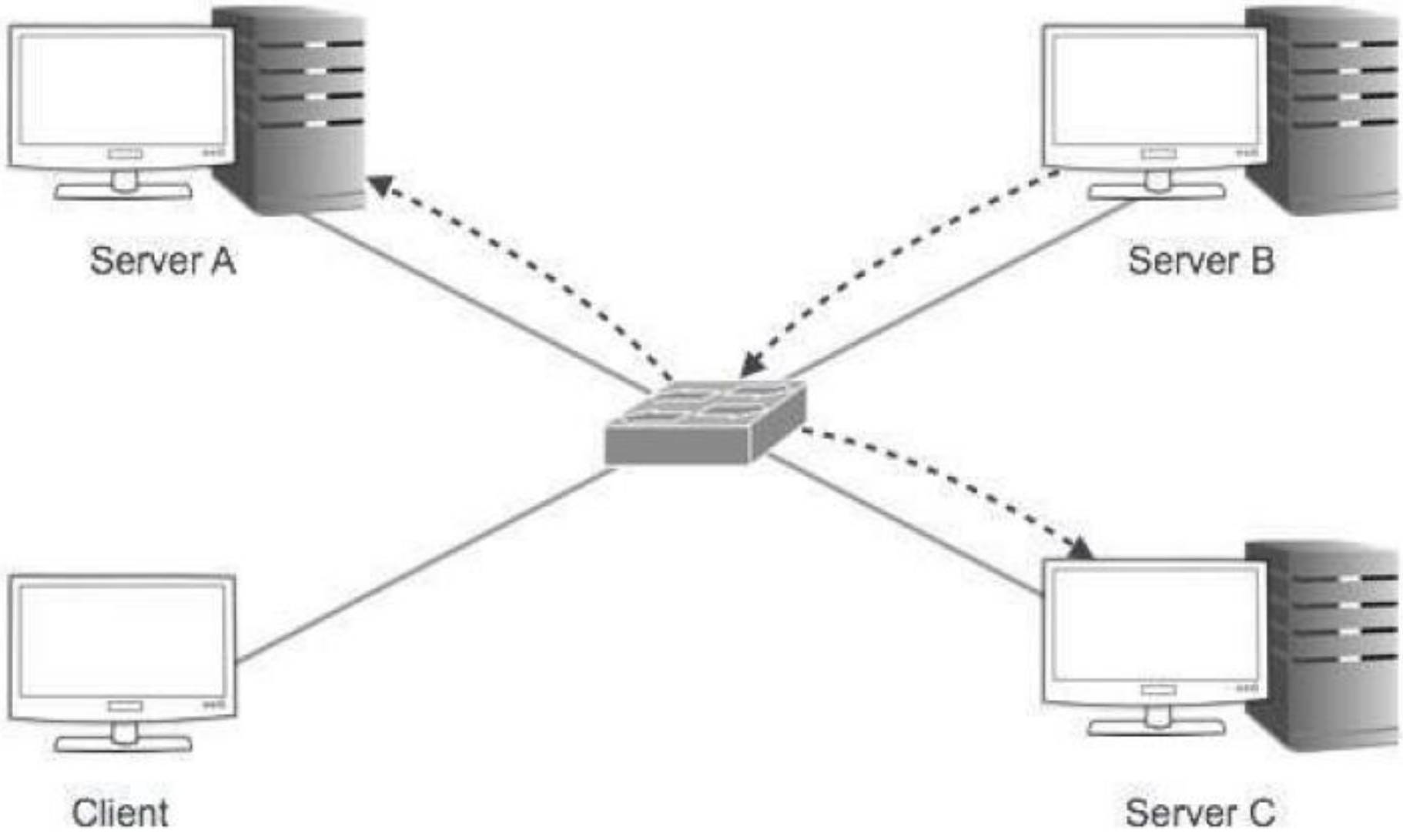
Broadcast Addressing Mode:

In this mode the packet is addressed to all hosts in a network segment. The Destination Address field contains special broadcast address i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here client sends packet, which is entertained by all the Servers:



Multicast Addressing Mode:

This mode is a mix of previous two modes, i.e. the packet sent is neither destined to a single host nor all the host on the segment. In this packet, the Destination Address contains special address which starts with 224.x.x.x and can be entertained by more than one host.



Hierarchical Addressing Scheme

IPv4 uses hierarchical addressing scheme. An IP address which is 32-bits in length, is divided into two or three parts as depicted:

A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

Subnet Mask

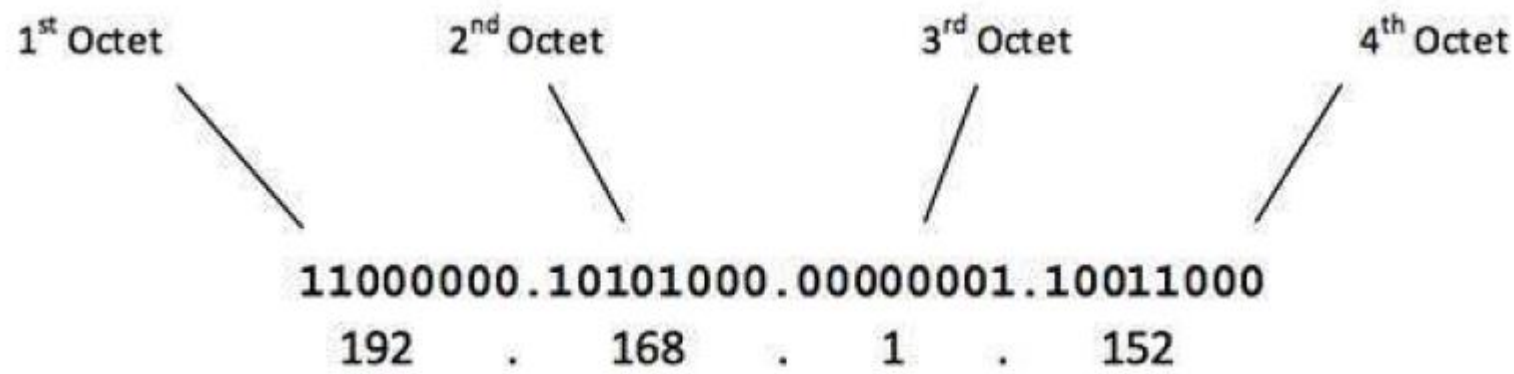
The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish the both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address 192.168.1.152 and the Subnet Mask is 255.255.255.0 then

IP	192.168.1.152	11000000	10101000	00000001	10011000	
Mask	255.255.255.0	11111111	11111111	11111111	00000000	ANDed
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

This way Subnet Mast helps extract Network ID and Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

IPV4 - ADDRESS CLASSES

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situation as per the requirement of hosts per network. Broadly, IPv4 Addressing system is divided into 5 classes of IP Addresses. All the 5 classes are identified by the first octet of IP Address.



Class A Address

The first bit of the first octet is always set to 0 *zero*. Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is

11000000 – **110**11111

192 – 223

Class C IP addresses range from 192.0.0.x to 192.255.255.x. The default subnet mask for Class B is 255.255.255.x.

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of

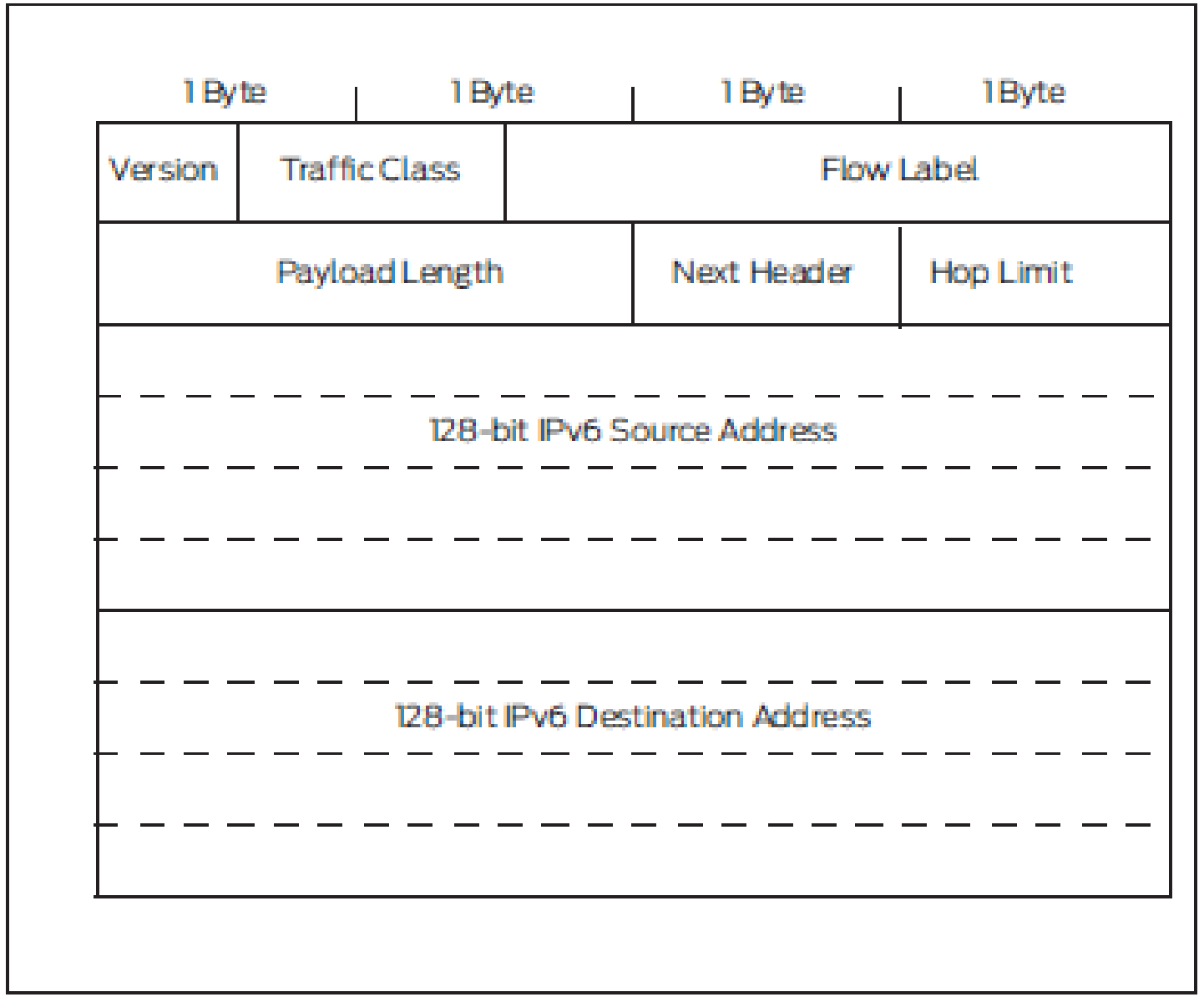
11100000 – **1110**1111
224 – 239

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that's why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only like for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

IPv4	IPv6
32-bit (4 byte) address supporting 4,294,967,296 address (although many were lost to special purposes, like 10.0.0.0 and 127.0.0.0)	128-bit (16 byte) address supporting 2^{28} (about 3.4 x 1038) addresses
NAT can be used to extend address limitations	No NAT support (by design)
IP addresses assigned to hosts by DHCP or static configuration	IP addresses self-assigned to hosts with stateless address auto-configuration or DHCPv6
IPSec support optional	IPSec support required
Options integrated in header fields	Options supported with extensions headers (simpler header format)


1 Byte
1 Byte
1 Byte
1 Byte
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
128-bit IPv6 Source Address
128-bit IPv6 Destination Address

IPv6 Header

- **Version:** A four-bit field for the IP version number (0x06).
- **Traffic Class:** An 8-bit field that identifies the major class of the packet content (for example, voice or video packets). The default value is 0, meaning it is ordinary bulk data (such as FTP) and requires no special handling.
- **Flow Label:** A 20-bit field used to label packets belonging to the same flow (those with the same values in several TCP/IP header parameters). The flow label is normally 0 (flows are detected in other ways).
- **Payload Length:** A 16-bit field giving the length of the packet in bytes, excluding the IPv6 header.
- **Next Header:** An 8-bit field giving the type of header immediately following the IPv6 header (this serves the same function as the Protocol field in IPv4).
- **Hop Limit:** An 8-bit field set by the source host and decremented by 1 at each router. Packets are discarded if Hop Limit is decremented to zero (this replaces the IPv4 Time To Live field). Generally, implementers choose the default to use, but values such as 64 or 128 are common.