

Network Layer

Unit - 9

Network Layer: Logical Addressing

- In order to provide computer to computer communication via Internet, we need a global addressing scheme. We call this as logical addressing. Such an addressing is provided by Internet Protocol (IP) at the network layer. The address is called **IP address or logical address**.
- The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. .
- IP has two primary responsibilities:
 1. Providing connectionless, best effort delivery of datagrams through a internetwork. The term best effort delivery means that IP does not provides any error control or flow control. The term connectionless means that each datagram is handled independently, and each datagram can follow different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order.
 2. Providing fragmentation and reassembly of datagrams to support data links with different maximum transmission unit (MTU) sizes.

IPv4 : Internet Protocol Version 4

- It is a 32-bit long address. They are unique and universal.
- Every Host and router on the internet has an IP Address. This IP address is **unique** and no two devices on the Internet can have the same address at the same time.
- It is **universal** in the sense that the addressing scheme must be accepted by any host that wants to be connected to the internet.

Address Space

- An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2^N .
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion).

Notations

There are two ways to represent IPv4.

1. Binary notation
2. Dotted-decimal notation

Binary Notation

- The IPv4 address is displayed as 32 bits.
- ex. 11000001 10000011 00011011 11111111

Dotted –Decimal Notation

- To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes.
- Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value ranging from 0 to 255.
- Example: 129.11.11.239

IP Addressing

- IP Addressing uses the concept of class. So this architecture is called **Classful addressing**.
- In Classful addressing, the address space is divided into five classes: A, B, C, D and E.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0-127			
Class B	128-191			
Class C	192-223			
Class D	224-239			
Class E	240-255			

b. Dotted-decimal notation

<u>Rule</u>	<u>Minimums and maximums</u>	<u>Decimal range</u>
Class A: First bit is always 0.	00000000 = 0 01111111 = 127	1 - 126* * 0 and 127 are reserved.
Class B: First two bits are always 10.	10000000 = 128 10111111 = 191	128 - 191
Class C: First three bits are always 110.	11000000 = 192 11011111 = 223	192 - 223
Class D: First four bits are always 1110.	11100000 = 224 11101111 = 239	224 - 239

Exercise:

Find the class of each address.

- a. 00000001 00001011 00001011 11101111
- b. 11000001 10000011 00011011 11111111
- c. 14.23.120.8
- d. 252.5.15.111

Solution

- a. The first bit is 0. This is a class A address.
- b. The first 2 bits are 1; the third bit is 0. This is a class C address.
- c. The first byte is 14 (between 0 and 127); the class is A.
- d. The first byte is 252 (between 240 and 255); the class is E.

Netid and Hostid

- In classful addressing, an IP address of class A, B and C is divided into two parts: netid and hostid.
- The netid and hostid are of varying lengths, depending on the class of the address.
- Netid: The part of an IP address that identifies the network.
- Hostid: The part of an IP address that identifies a host in a network.

- Class A: One byte netid Three bytes host ID.
- Class B: Two bytes netid Two bytes host ID.
- Class C: Three bytes netid One byte host ID

Example:

1. IP address: 84.42.58.11

Binary Notation: 01010100 00101010 00111010 00001011

It is a class A IP address.

The network address /netid is 84.0.0.0

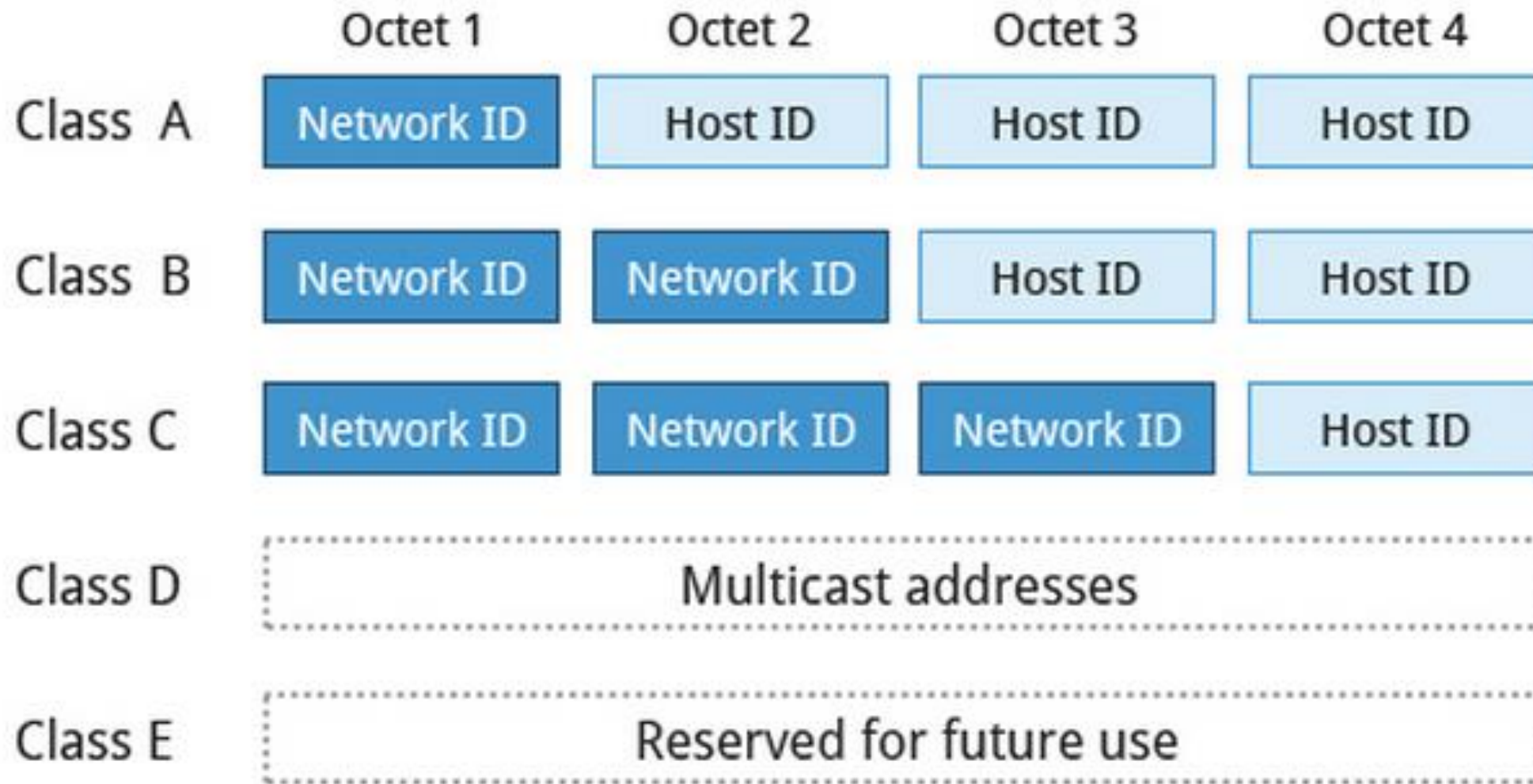
The host addresses /hostid is 0.42.58.11

2. IP address: 144.62.12.9

It is a class B IP address.

The network address /netid is 144.62.0.0

The host addresses /hostid is 0.0.12.9



Number of Networks and Hosts in Different Class of IP Address

Class	Number of Networks	Number of Hosts	Application
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Subnetting

- Subnetting is the process of dividing a large network up into smaller networks, called subnets or sub networks.
- Each of these subnets has its own specific address.
- To create these additional networks we use a subnet mask. The subnet mask simply determines which portion of the IP address belongs to the host.
- The subnet address is created by dividing the host address into network address and host address.
- For example, 172.16.1.0, 172.16.2.0, 172.16.3.0 and 172.16.4.0 are all subnets within network 171.16.0.0.

How to create subnets?

- To create subnetworks, you take (borrow) bits from the host portion of the IP address and reserve them to define the subnet address.
- That means fewer bits for hosts, so the more subnets.

Subnet Masks

- For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning a ***subnet mask*** to each machine.
- A subnet is 32 bit value that allows the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID portion of the IP address.
- Subnet mask has binary 1s in all bits specifying the network field, and binary 0s in all bits specifying the host field.
- A subnet address is created by borrowing the bits from host field of IP address.
- Subnet mask bits should come from the high-order (left most) bits of the host field.

Default subnet mask

Address Class	Bits Used for Subnet Mask	Dotted Decimal Notation
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

Class A
Subnet Mask

Network	Host	Host	Host
255	0	0	0

Class B
Subnet Mask

Network	Network	Host	Host
255	255	0	0

Class C
Subnet Mask

Network	Network	Network	Host
255	255	255	0

- Each class has a predefined default subnet mask that tell us the octets, which are already part of the network portion, as well as how many bits we have available to work with.
- Whatever network class is it, we cannot change those bits that are already assigned.
- We cannot assign the network ID and the broadcast address to a host.
- Regardless how many bits are left in the host field, network ID and the broadcast address must be reserved.
- Subnet bits start at the left and go to the right, without skipping bits.

IP Class	Default Subnet	Network bits	Host bits	Total hosts	Valid hosts
A	255.0.0.0	First 8 bits	Last 24 bits	16, 777, 216	16, 777, 214
B	255.255.0.0	First 16 bits	Last 16 bits	65,536	65,534
C	255.255.255.0	First 24 bits	Last 8 bits	256	254

Network ID

- First address of subnet is called network ID. This address is used to identify one segment or broadcast domain from all the other segments in the network.

Block Size

- Block size is the size of subnet including network address, hosts addresses and broadcast address.

Broadcast ID

- There are two types of broadcast, direct broadcast and full broadcast.
- **Direct broadcast or local broadcast** is the last address of subnet and can be hear by all hosts in subnet.
- **Full broadcast** is the last address of IP classes and can be hear by all IP hosts in network. Full broadcast address is 255.255.255.255

Host Addresses

- All address between the network address and the directed broadcast address is called host address for the subnet. You can assign host addresses to any IP devices such as PCs, servers, routers, and switches.

CIDR (Classless Inter Domain Routing)

- CIDR is a slash notation of subnet mask. CIDR tells us number of on bits(i.e. number of 1s) in a network address.
- It is the basically the methods that ISPs (Internet Service Provider) use to allocate a number of addresses to a company, a home-a customer.
- CIDR provide addresses in a certain block size.

Example:

- Class A has default subnet mask 255.0.0.0. that means first octet of the subnet mask has all on bits. In slash notation it would be written as /8, means address has 8 bits on.
- Class B has default subnet mask 255.255.0.0. that means first two octets of the subnet mask have all on bits. In slash notation it would be written as /16, means address has 16 bits on.
- Class C has default subnet mask 255.255.255.0. that means first three octets of the subnet mask have all on bits. In slash notation it would be written as /24, means address has 24 bits on.

Binary Mask				Prefix Length	Subnet Mask
11111111	00000000	00000000	00000000	/8	255.0.0.0
11111111	10000000	00000000	00000000	/9	255.128.0.0
11111111	11000000	00000000	00000000	/10	255.192.0.0
11111111	11100000	00000000	00000000	/11	255.224.0.0
11111111	11110000	00000000	00000000	/12	255.240.0.0
11111111	11111000	00000000	00000000	/13	255.248.0.0
11111111	11111100	00000000	00000000	/14	255.252.0.0
11111111	11111110	00000000	00000000	/15	255.254.0.0
11111111	11111111	00000000	00000000	/16	255.255.0.0
11111111	11111111	10000000	00000000	/17	255.255.128.0
11111111	11111111	11000000	00000000	/18	255.255.192.0
11111111	11111111	11100000	00000000	/19	255.255.224.0
11111111	11111111	11110000	00000000	/20	255.255.240.0
11111111	11111111	11111000	00000000	/21	255.255.248.0
11111111	11111111	11111100	00000000	/22	255.255.252.0
11111111	11111111	11111110	00000000	/23	255.255.254.0
11111111	11111111	11111111	00000000	/24	255.255.255.0
11111111	11111111	11111111	10000000	/25	255.255.255.128
11111111	11111111	11111111	11000000	/26	255.255.255.192
11111111	11111111	11111111	11100000	/27	255.255.255.224
11111111	11111111	11111111	11110000	/28	255.255.255.240
11111111	11111111	11111111	11111000	/29	255.255.255.248
11111111	11111111	11111111	11111100	/30	255.255.255.252

NOTE:

Example: 192.168.10.32/28.

- It tells what your subnet mask is.
- The slash notation (/) means how many bits are turned on (1s).
- Obviously, the maximum could only be /32 because a byte is 8 bits and there are 4 bytes in an IP address. (4*8=32).
- But, regardless of the class of address, the largest subnet mask can be only /30 because you've got to keep at least 2 bits for host bits.

In subnetting we find the answer of following questions:

- What is subnet mask for given address?
- How many subnets does given subnet mask provide ?
- What is block size for given subnet mask?
- What are the valid subnets?
- What are the total hosts?
- How many valid hosts are available per subnet?
- What is broadcast address of each subnet?
- What is network address of each subnet?

To answer above questions we use following method of subnetting.

What is subnet mask for given address?

Steps:

1. Find the class of given IP address.
2. Write down the default subnet mask.
3. Now find the host bits borrowed to create subnets and convert them in decimal.

For example: find the subnet mask of address 188.25.45.48/20 ?

- This address belong to class B and class B has default subnet mask 255.255.0.0[/16 in CIDR].
- We borrowed 4 bits from hosts portion. As you know subnetting move from left to right and it cannot skip any network bit.
- So this subnet mask in binary would be 11111111. 11111111.11110000.00000000..
- Our answer subnet mask would be 255.255.240.0

How many subnets does given subnet mask provide ?

- Number of subnets provided by given subnet mask $= 2^N$,
where N = number of bits borrowed from host bits to create subnets.

For example in 188.25.45.48/20, N is 4.

- Now $2^4 = 16$, so our answer is 16.

What is block size for given subnet mask?

- Block size = $256 - \text{Subnet mask}$
- For example block size for subnet mask 255.255.240.0 is $256 - 240 = 16$.

What are the valid subnets?

Calculating valid subnet is two steps process:

1. First calculate total subnet by using formula 2^N .
2. In second step find the block size and count from zero in block until you reach the subnet mask value.

For example: calculate the valid subnets for 188.25.45.48/20.

subnet mask : 255.255.240.0

Borrowed bits = 4

Subnets : $2^N = 2^4 = 16$.

Block size = $256 - 240 = 16$

Valid subnets = 0,16,32,48, etc..... up to 240.

What are the total hosts?

- Total hosts are the hosts available per subnet.
- Total hosts = 2^H .
- Where H is number host bits.

For example: in address 188.25.45.48/20.

Subnet mask : 255.255.240.0

Borrowed bits = 4

$H = 16 - 4 = 12$

Total Hosts = $2^H = 2^{12} = 4096$

How many valid hosts are available per subnet?

- Valid hosts are the number of hosts those can be assigned to devices.
- As we know, we need to reduce two address per subnet, one for network ID and another for broadcast ID.
- So, Valid hosts = Total hosts - 2

For example: In network address 88.25.45.48/20

Total host = $2^H = 2^{12} = 4096$

Valid hosts per subnet = $2^H - 2 = 4096 - 2 = 4094$

What is broadcast address of each subnet?

- Broadcast address is the last address of subnet.
- This address is reserve for network broadcast, and cannot be assigned to any host

What is the network address of each subnet?

- Network address is the first address of subnet.
- This address is used to locate the network, and cannot be assigned to any host.

Note:

- Network address(gateway address) is always the first IP address of subnet.
- Broadcast address is always the last IP address of subnet (IP address before the next subnet).
- Valid hosts are the IP addresses between network address and broadcast address.

Supernetting

- Supernetting is an addressing scheme in which several class C blocks can be combined to create a larger range of addresses.
- In other words, several networks are combined to create a supernetwork or a supernet.
- For example, an organization that needs 1,000 addresses can be granted four contiguous class C blocks. The organization can then use these addresses to create one supernetwork.
- Supernetting decreases the number of 1's in the mask. For example, if an organization is given four class C addresses, the mask changes from /24 to /22.

Variable Length Subnet Masks (VLSM)

- VLSM is a process of dividing an IP space into the subnets of different sizes without wasting IP addresses.
- VLSM is a process of breaking down subnets into the smaller subnets, according to the need of individual networks. It is subnetting a subnet.
- It can also be called a classless IP addressing
- When we perform subnetting, all subnets have the same number of hosts, this is known as FLSM (Fixed length subnet mask).
- In FLSM all subnets use same subnet mask, this lead to inefficiencies because of wastage of IP address. In real life scenario, some subnets may require large number of host addresses while other may require only few addresses.
- In VLSM Subnetting, we do subnetting of subnets according the network requirement.

VLSM Subnetting

- In VLSM Subnetting, we do subnetting of subnets according the network requirement.

Steps for VLSM Subnetting (not mandatory to do with largest one!!!)

1. Find the largest segment. Segment which need largest number of hosts address.
2. Do subnetting to fulfill the requirement of largest segment.
3. Assign the appropriate subnet mask for the largest segment.
4. For second largest segments, take one of these newly created subnets and apply a different, more appropriate, subnet mask to it.
5. Assign the appropriate subnet mask for the second largest segment.
6. Repeat this process until the last network.

Implementing VLSM Networks

- To create VLSM quickly and efficiently, you need to understand how block sizes and charts work together to create the VLSM.
- Table below show the block sizes used when creating VLSMs with Class C networks.

Prefix	Mask	Subnets	Valid Hosts	Block Size
/25	128	2	126	128
/26	192	4	62	64
/27	224	8	30	32
/28	240	16	14	16
/29	248	32	6	8
/30	252	64	2	4

Example

- Suppose following given networks a number of hosts. You are given network address 192.168.10.0. Create a VLSM table and VLSM chart.
- Network A = 14 Hosts
- Network B = 30 Hosts
- Network C = 20 Hosts
- Network D = 6 Hosts
- Network E = 2 Hosts
- Network F = 2 Hosts
- Network G = 2 Hosts
- Network H = 2 Hosts

VLSM Table: 192.16.10.0

Network	Hosts	Block	Subnet	Mask
A	14	16	/28	240
B	30	32	/27	224
C	20	32	/27	224
D	6	8	/29	248
E	2	4	/30	252
F	2	4	/30	252
G	2	4	/30	252
H	2	4	/30	252

VLSM chart

Network	IP
D	192.168.10.8/29 – 192.168.10.15/29
A	192.168.10.16/28 – 192.168.10.31/28
B	192.168.10.32/27-192.168.10.63/27
C	192.168.10.64/27-192.168.10.95/27
E	192.168.10.96/30-192.168.10.99/30
F	192.168.10.100/30-192.168.10.103/30
G	192.168.10.104/30-192.168.10.107/30
h	192.168.10.108/30-192.68.10.111/30

Private Address

- An IP address is considered private if the IP number falls within one of the IP address below.

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

- These addresses are commonly used for home, office, and enterprise local area networks (LANs). Any organization can use it.
- They are unique inside the organization, but they are not unique outside globally.
- No router will forward a packet that has one of these addresses if need to connect to internet. Likewise, computer outside local network cannot directly connect with device with private IP. It must do so via Network Address Translator.

•

Network Address Translator

- Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network.
- The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

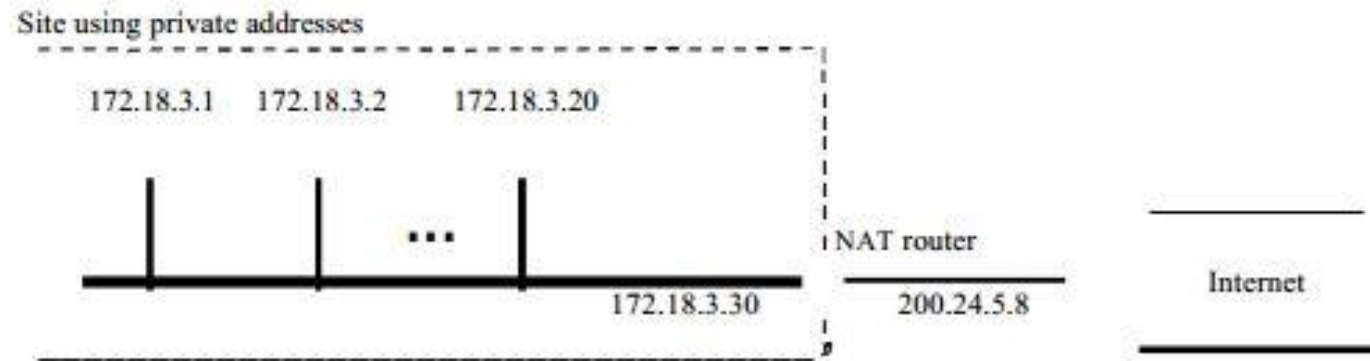
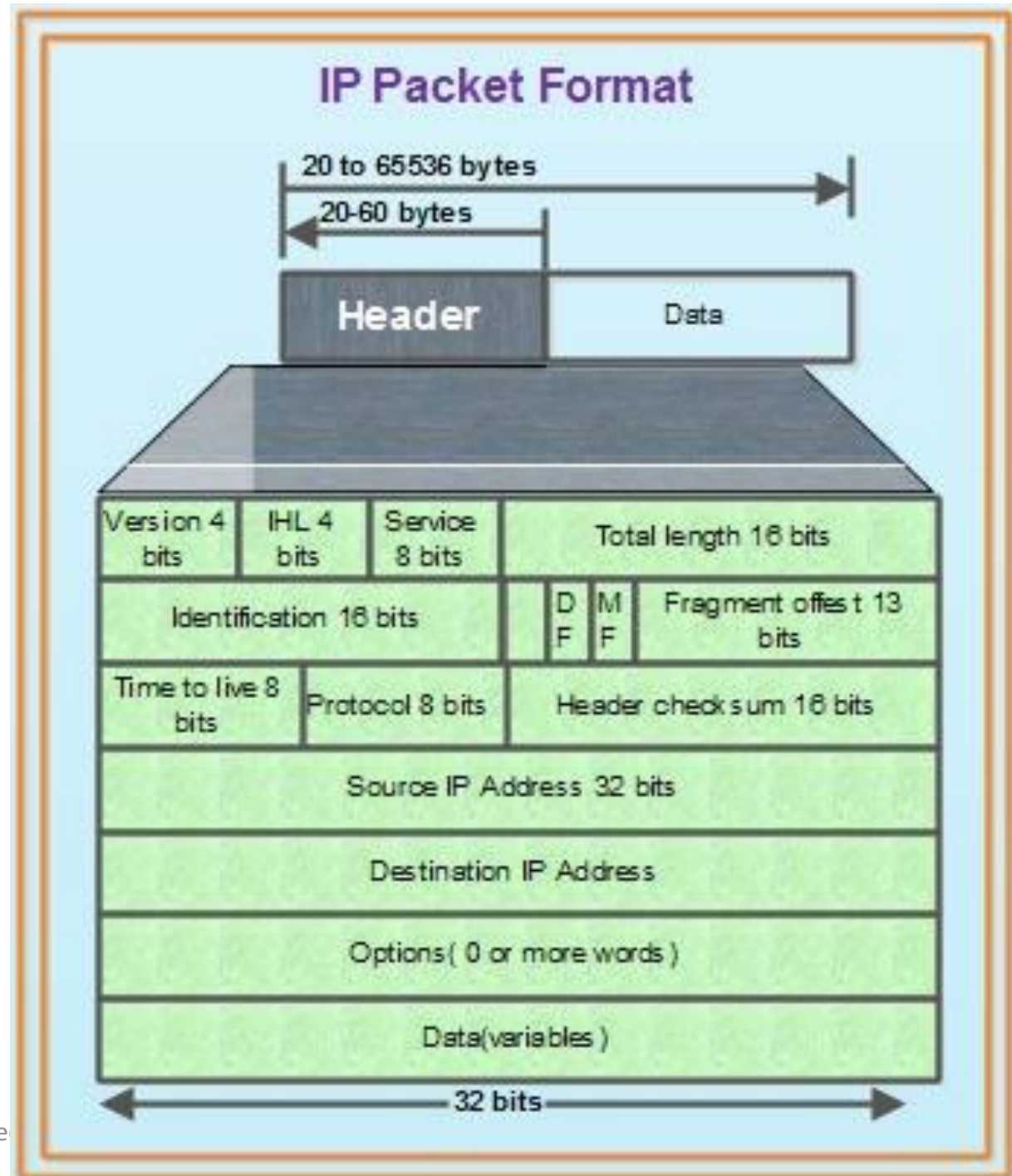


Figure: A NAT Implementation

Ipv4 Datagram

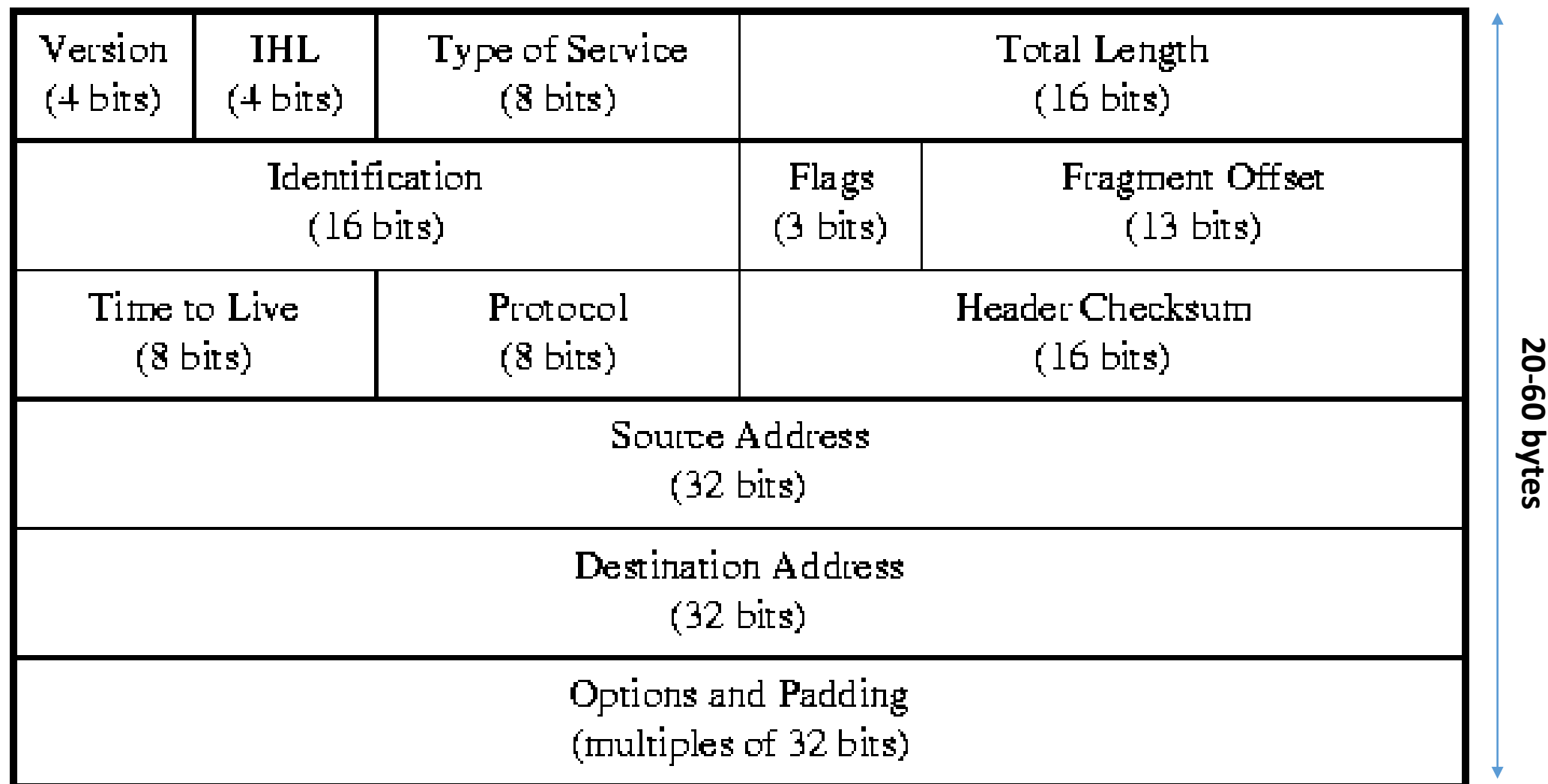
- Packets in IPV4 layer is called datagrams.
- A datagram is a variable length packet consisting of two parts: header and data.
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.
- Figure shows the format of IPV4 datagram.

IP Header



0

31



1. **Version:**

- It is a 4-bit field that specifies the version of IP currently being used. It has value 4 for IPV4.
- Two different versions of protocols are IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

2. **IP Header Length (IHL):**

- This 4-bit field indicates the datagram header length in 32 bit word (4 byte). The header length is not constant in IP. It may vary from 20 to 60 bytes. When there are no options, the header length is 20 bytes, and the value of this field is 5. When the option field is at its maximum size, the value of this field is 15. the total length is divided by 4 and the value is inserted in the field. The receiver needs to multiply the value of this field by 4 to find the total length.

3. **Types of Services:**

- This is 8 bit field was previously called services type but is now called differentiated services.
- It tells how datagram should be handled.

4. **Total length:**

- 16 bit field specifies the total length of entire IP datagram including data and header in bytes.
- As there are 16 bits, the total length of IP datagram is limited to 65,535 ($2^{16} - 1$) bytes.
- Length of data = total length – (HLEN) x 4.

5. Identification:

- This 16 bit field is used in fragmentation. A datagram when passing through different networks may be divided into fragments to match the network frame size. Therefore, this field contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.

6. Flags:

- Consists of a 3 bit field of which the two low order bit DF and MF control fragmentation. DF stands for Don't Fragment. DF specifies whether the packet can be fragmented. MF stands for more fragments. MF specifies whether the packet is the last fragment in a series of fragmented packets. The third or high order bit is not used.

7. Fragment Offset:

- This 13 bit field indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

8. Time to Live:

- It is 8 bit field that maintain a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps the packet from looping endlessly.

9. Protocol:

- This 8 bit field indicates which upper layer protocol (ICMP is port 1, IGMP is port 2, TCP is port 6, UDP port is 17, OSPF port is 89).
- Also supports network layer protocols like ARP, ICMP.

10. Header Checksum:

- This 16 bit field contains a checksum that covers only the header and not the data.

11. Source IP address:

- These 32-bit field contains the IP address of source machine.

12. Destination IP address:

- This 32-bit field contains the IP address of destination machine.

13. Options:

- This field allows IP to support various options such as security, routing, timing management and alignment.

14. Data:

- It contains upper layer information.

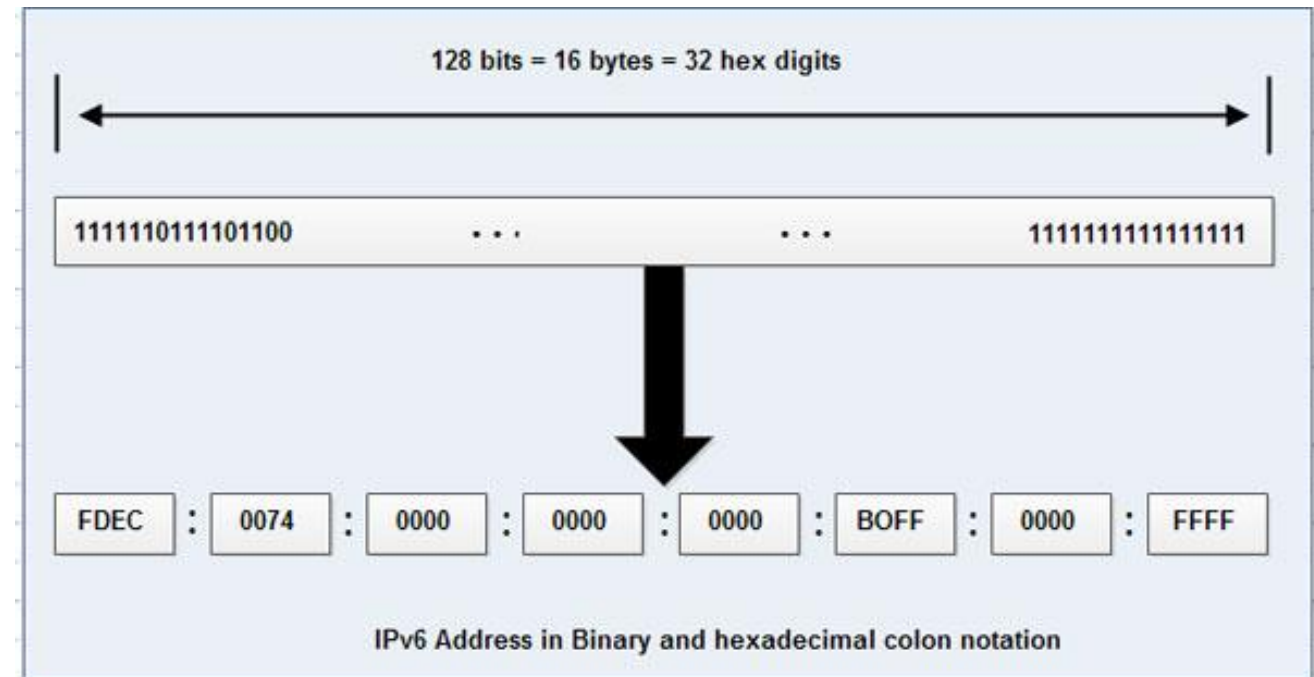
IPv6

- IPV6 is also known as IPng (Internetworking Protocol, next generation).
- Internet working protocol version 6 (IPv6) was developed to overcome the shortcomings of IPv4 and meet the future needs for internet.
- Problem of address depletion, lack of accommodation for real-time audio and video transmission , and encryption and authentication of data for some applications.
- Features:
 - i. IPv6 address is 128 bits long. This is far more than 32 bit long addresses used by Ipv4. This provides 2^{96} more unique addresses
 - ii. Ipv6 header has got separate options field. This speeds up the routing as most of the times, options are not needed.
 - iii. Several new options have been added to set of options.
 - iv. To accommodate the real time traffic, the Ipv6 uses Flow Label field instead of Type of Service field of Ipv4. With this field, a user can request for the type of service to be given to the datagram.
 - v. The Ipv6 contains options for encryption and decryption of data. This provides additional security to the information.

Structure of IPv6

Hexadecimal colon notation

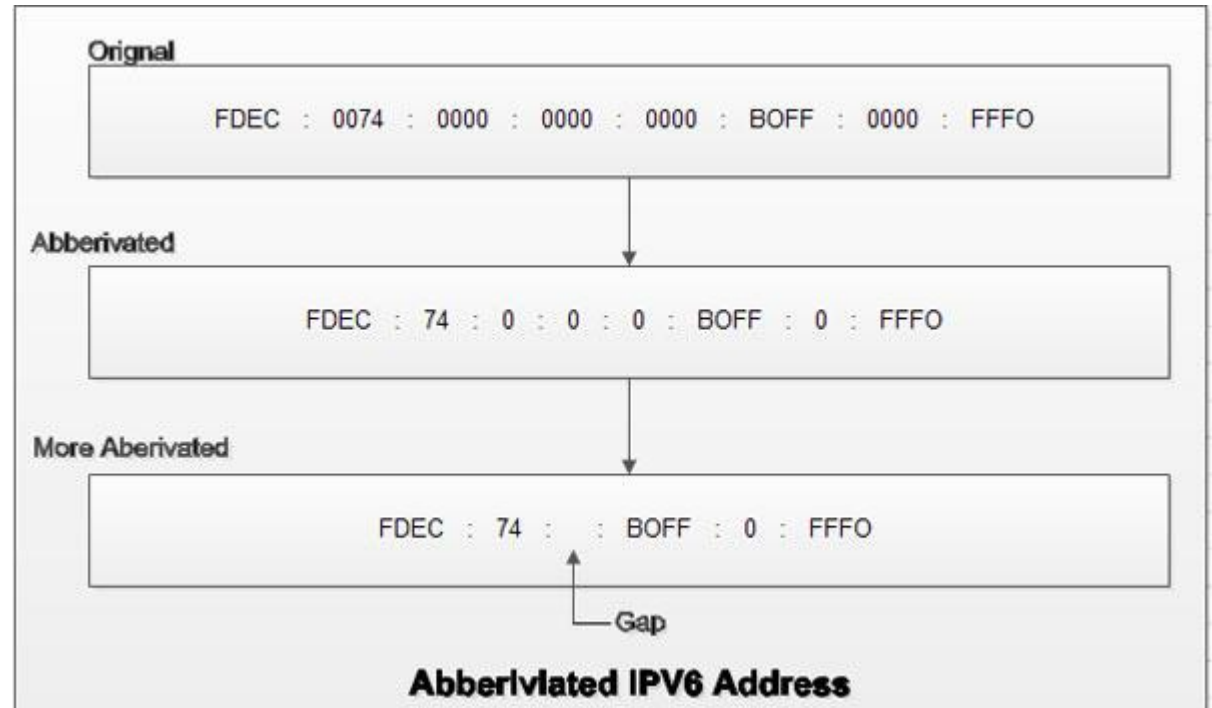
- An IPv6 address consists of 16 bytes (octets)
- Thus an IPv6 address is 128 bits long
- It uses hexadecimal colon notation.
- In this notation 128 bits is divided into eight sections. Each section is 2 bytes long.
- Two bytes in hexadecimal notation require four hexadecimal digits. Thus, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.

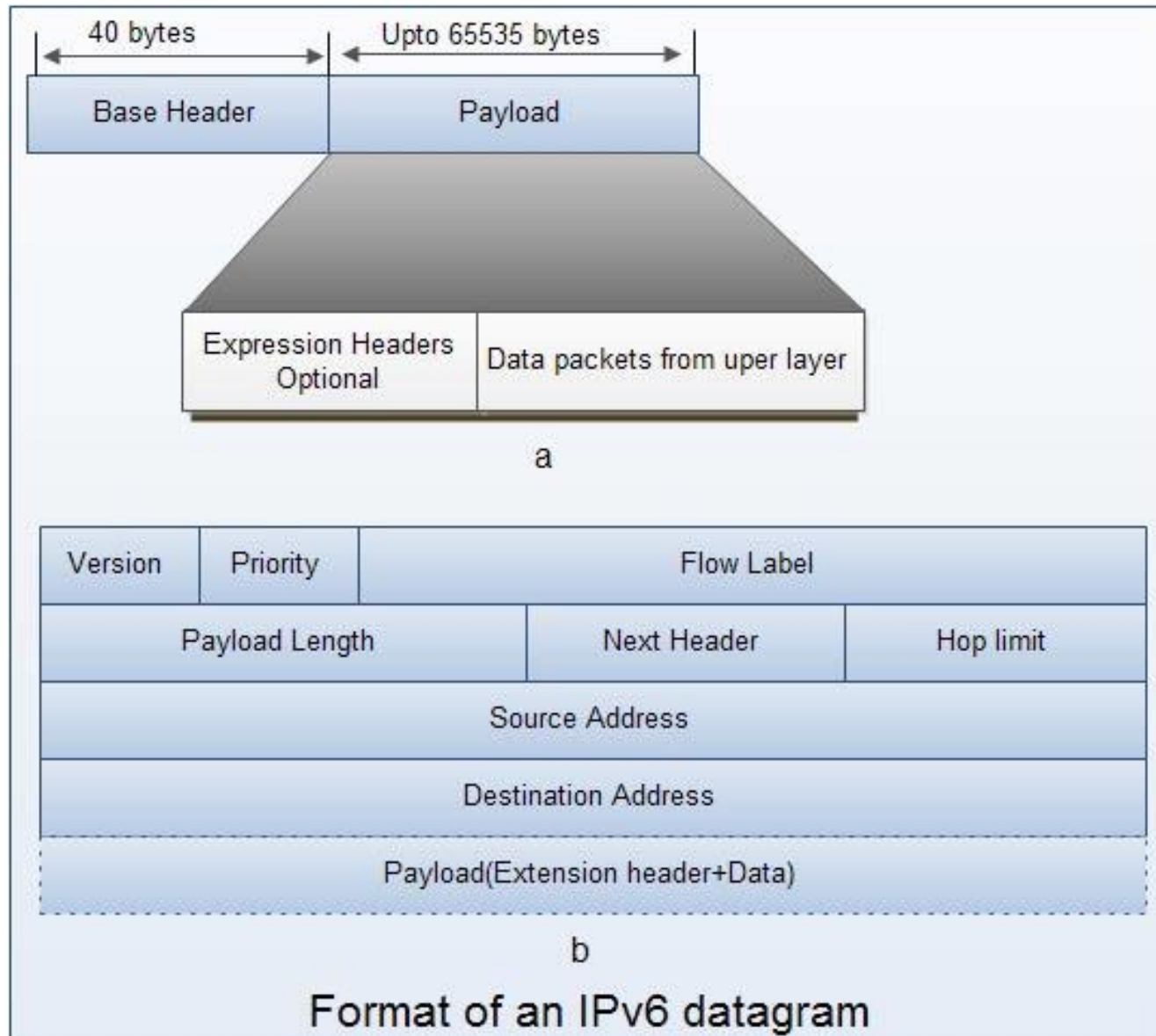


Abbreviation

We can write IPv6 in abbreviated form:

- This can be done by omitting the leading zeros of a section (four digits between two colons)
- In such a form, only leading zero can be omitted and not the trailing zeros.
- Using this form of abbreviation, 0074 can be written as 74, 000F as F, and 0000 as 0. Note 3210 cannot be abbreviated.
- Further abbreviations are also possible if there are consecutive sections consisting of zeros only. Using this scheme, zeros can be removed altogether and can be replaced with a double colon.





1. **Version:** This four bit field indicates the version of internet protocol which is 6 for IPv6.
2. **Priority:** This four bit field specifies the priority of level of the packet with respect to traffic congestion. It specifies the class of traffic to which the IP packet belongs.
3. **Flow Label:** This is a 3 byte (24 bit) field. It is used to identify all the packet in an individual flow. A flow is uniquely identified by a combination of source address, destination address and a non-zero flow label. Thus, all the packets that are part of the same flow are assigned the same label by the source.
4. **Payload length:** This 2 byte field indicates the number of octets present in the payload.
5. **Next header:** The next header is an 8 bit field and identifies the protocol to which the contents(data field) of this datagram will be delivered(for example, to TCP or UDP).
6. **HOP limit:** This 8-bit field has the same function as TTL in IPv4. In IPv6, it is decremented by one on each hop.
7. **Source address:** This field is of 16 byte (128 bit) and identifies the original source of datagram.
8. **Destination address:** This 16 byte (128-bit) field determines the final destination of the datagram.


Advantages of IPv6

1. **Larger address space:** An IPv6 address is 128 bit long as compared to 32- bit address of IPv4. It has huge 2^{96} increases in the address space.
2. **Allowance for extension:** IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
3. **Better header format:** IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and upper-layer data.
4. **New options:** IPv6 has new options to allow for additional functionalities.
5. **Support for more security:** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.
6. **Support for resource allocation:** In IPv6, the source can request the special handling of the packet with the help of flow label field. This mechanism can be used to support traffic such as real-time audio and video.

Comparison between IPv4 and IPv6


- The major difference in IPv4 and IPv6 packet formats are as follows:
 1. IPv6 packet format does not contain header length field as IPv6 base header has fixed length of 40 bytes. IPv4 head is variable in length so header length field is required.
 2. The header checksum field is not present in IPv6. As a result error detection is not done on the header, checksum is provided by upper layer protocols. It reduces the processing time of an IP packet.
 3. In IPv6, *maximum hop* field is used whereas in IPv4 *Time to live (TTL)* field is used.
 4. In IPv6, the size of payload (excluding header) is specified whereas in IPv4 *total length* field is used that specifies the total size of IP packet including header.
 5. There is no fragmentation field in the base header in IPv6. It has been moved to the extension header.
 6. The identification, flag, and offset field are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
 7. The options field is moved under extension headers in IPv6.
 8. The source and destination address sizes in IPv6 are 128 bits as against 32 bits in IPv4.
 9. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.

Header comparison



vers	hlen	TOS	total length	
identification		flags	flag-offset	
TTL	protocol	header checksum		
source address				
destination address				
options and padding				

IPv4



vers	traffic class	flow-label		
payload length		next header	hop limit	
source address				
destination address				

IPv6

Removed (6)

- ID, flags, flag offset
- TOS, hlen
- header checksum

Changed (3)

Added (2)

- traffic class
- flow label

Expanded

- address 32 to 128 bits

No longer present in IPv6

➤ Fragmentation/Reassembly

- Results in fast IP

forwarding

➤ Header checksum

- Result in fast processing

➤ Option field

- Replaced by extension

header; result in a fixed

length, 40-byte IP header

Internet Control Protocols

- Heart of internet → IP → responsible for routing data to destination.
- In addition to IP, the Internet has various control protocols operating at the network layer (layer three of the OSI model), including:
 - **ICMP:** Internet Control Message Protocol
 - **IGMP:** Internet Group Message Protocol
 - **ARP:** Address Resolution Protocol
 - **RARP:** Reverse Address Resolution Protocol
 - **BOOTP:** Bootstrap Protocol
 - **DHCP:** Dynamic Host Configuration Protocol

ICMP: Internet Control Message Protocol

- The **Internet Control Message Protocol (ICMP)** is an error reporting message and query message protocol.
- Due to the unreliability and the connectionless behavior of IP, some error may occur during the data transmission. In such case, ICMP informs the source.
- ICMP are encapsulated within IP datagram.

Some messages and events that relates to ICMP are as follows:

1. Destination Unreachable

- If a router can't send an IP datagram any further, it uses ICMP to send message back to the sender, advising of a situation.

2. Buffer Full/Source Quench

- If a router's memory buffer for receiving incoming datagrams is full, it will use ICMP to send out this message until the congestion is removed.

3. Hops/Time Exceeded

- This message is sent when packet is dropped because its counter(Time to live) has reached zero.

4. Ping

- Packet Internet Groper(Ping) used ICMP echo request and reply message to check the physical and logical connectivity of machines on an internetwork.
 - Echo request → ask if machine is alive
 - Echo reply → Yes, I am alive
 - **Echo Request** and **Echo Reply** (the response to an Echo Request) messages are concurrently used to find whether a host is alive and reachable.

IGMP: Internet Group Management Protocol

- IGMP is group management protocol that mainly manages the group membership in a multicast network.
- It helps multicast router create and update a list of loyal members related to each router interface.
- This protocol uses three different messages: query message, membership report and leave report.

Background

- In a multicast network, multicast routers are used to route packets to all the computers that are having membership of a particular group.
- The multicast routers use the information from IGMP to determine which hosts are having membership of which group.
- A multicast router generally receives thousands of multicast packets that have to be transmitted to various groups. If a router has no knowledge about the group membership, it will broadcast packet to every host and this will increase the load on the network.
- In order to save the network from such a problem, a list of groups is maintained when members of the group are present in the network.

Operation of IGMP

- The multicast router of the network has a list of multicast addresses of the groups with at least one loyal member in that network. (figure below).
- There is one multicast router for each group that distributes multicast packet to members of that group. It means the network will have two multicast routers, if there are two multicast groups.
- A host or a multicast router can be a member of the group.
- When a host is having membership, it means that any process running on that host is a member of the group and when a router is having membership of group, it means one of the networks connected to the router is having membership of the group.

