University of Technology

Computer Science

Computer Networks

2023-2024

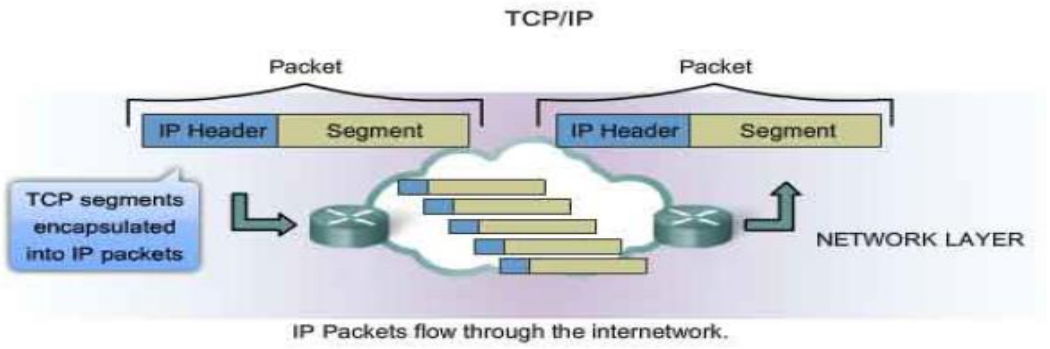
Dr. Asia Ali

Network Layer Addressing

the Network layer services implemented by the TCP/IP protocol suite are the Internet Protocol (IP). Version 4 of IP (IPv4) is currently the most widely-used version of IP. IP version 6 (IPv6) is developed and being implemented in some areas. IPv6 will operate alongside IPv4 and may replace it in the future. **The services provided by IP, as well as the packet header structure and contents, are specified by either IPv4protocol or IPv6 protocol**.
These services and packet structure are used to encapsulate UDP datagrams or TCP segments for their trip across an internetwork. The characteristics of each protocol are different. The Internet Protocol was designed as a protocol with low overhead. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks. The protocol was not designed to track and manage the flow of packets. These functions are performed by other protocols in other layers.
IPv4 basic characteristics:

- ✓ ***Connectionless - No connection is established before sending data packets.***
- ✓ ***Best Effort (unreliable) - No overhead is used to guarantee packet delivery.***

Media Independent - Operates independently of the medium carrying the data.



IP Packets flow through the internetwork.

- Connectionless - No connection is established before sending data packets.
- Best Effort (unreliable) - No overhead is used to guarantee packet delivery.
- Media Independent - Operates independently of the medium carrying the data.

The IP datagrams (IPv4)

•The Header (H) has 20-byte Fixed Part (FP) and a variable Options (Op) part (40 bytes). Total 20 to 60 bytes.

•The Header includes a number of fields: The Version field which defines the version of IP used to create the datagram (needed to ensure that all systems processing the datagram during its transfer from S to D across the Internet interpret all fields correctly). The current version is 4 and the IP is referred to as IP version 4 or IPv4.

•The Intermediate Header Length (IHL) specifies the actual length of the header in multiples of 32–bit (4- byte) words. The minimum length (without Options) is 5.

• IP Header Payload (IP Data) 1

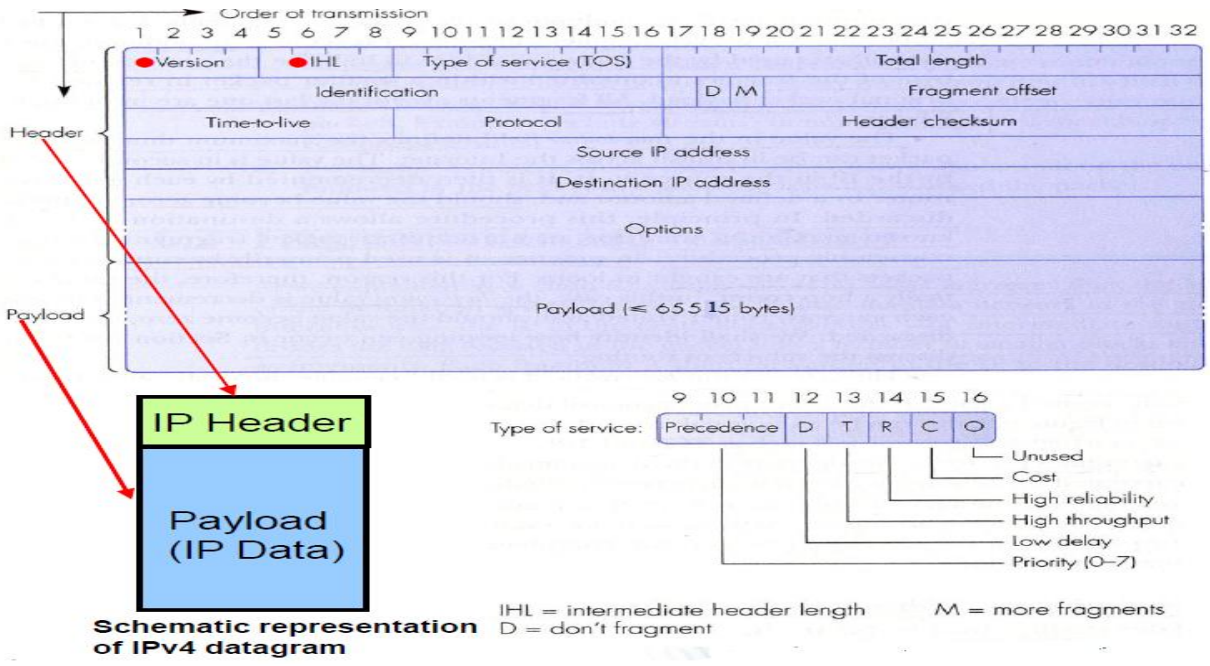
•We start study of the Network Layer protocol with the IP datagram. The discussed fields are marked by .

•The IP is a connectionless protocol and all data are transferred in the payload part of a datagram (or packet). The IP datagram consists of a Header part and a Payload part each of which contains a number of fields.

•The Header (H) has 20-byte Fixed Part (FP) and a variable Options (Op) part (40 bytes). Total 20 to 60 bytes.

•The Header includes a number of fields: The Version field which defines the version of IP used to create the datagram (needed to ensure that all systems processing the datagram during its transfer from S to D across the Internet interpret all fields correctly). The current version is 4 and the IP is referred to as IP version 4 or IPv4.

•The Intermediate Header Length (IHL) specifies the actual length of the header in multiples of 32–bit (4- byte) words.



Schematic representation of IPv4 datagram

IP addressing (IPv4)

•Each host, gateway and router has a unique Internet-wide IP address (IP = netid + hostid). In case of a host/computer, the netid identifies the network to which the host is attached, the hostid identifies the host on this network. In case of an access gateway or router, each network interface

of the gateway or router has different netid assigned to it, i.e. the gateway or router may have a few IP addresses for each interface. In IPv4 all IP ad-dresses are 32 bits long, which means that there are 232=4,294,967,296 different addresses. Network addres-sing affects efficiency and implementation of Internet routing and transmission of datagrams within routers.

•There are 5 different schemes used for assigning IP addresses:

(i) Class-based addresses also known as Classful addressing: A 32-bit address space is divided into 5 address classes: A, B, C, D, E. Each of the classes A, B, C has a defined boundary between the netid part and hosid part of the address space; Class D is used for multicasting; class E is reserved.

(ii) Subnetting: It is designed to overcome the problem of need of large number of IP addresses for a site which has many LANs attached to one IP router. With subnetting only a single IP address is required at each site.

(iii) Classless addresses (CIDR): The network part of an IP address is not constrained to the fixed class boundary. It can be any number of bits. This leads to a more efficient use of the total address space.

(iv) Network address translation (NAT): For each access network only a single IP address is allocated, and this is used by all hosts when communicating outside of their local access network. For communicating within the access network every host is assigned its private IP address.

(v) IPv6: This is a completely new version of IP (version 6). It was developed to overcome the limited address space of IPv4 by increasing of the address space to 128 bit.

The 32-bit address space is divided into 5 different address formats (address classes). A, B, C are used for unicast (between a pair of hosts); D for multicast. The IP address formats are shown in figure. Each class is intended for use with a different size of network. The class to which an address belongs is determined by by the position of first 0 bit in the first 4 bits. The remaining bits specify the netid and hostid parts with fixed boundaries.

IPv4 addressing – Class-based addresses

•Class A is marked by 0 as a first bit; the next 7 bits are used for the netid and 24 bits for hostid.

•Class B is marked by 10 as first two bits.

•Class C is marked by 110 as first three bits.

•Class D is marked by 1110 as first 4 bits.

•Class E is marked by 1111 as first 4 bits.

•The first bits indicating class in each ad-dress, are fixed and cannot be changed.

•Class A addresses are suitable for net-works with large number of hosts (up to 224).

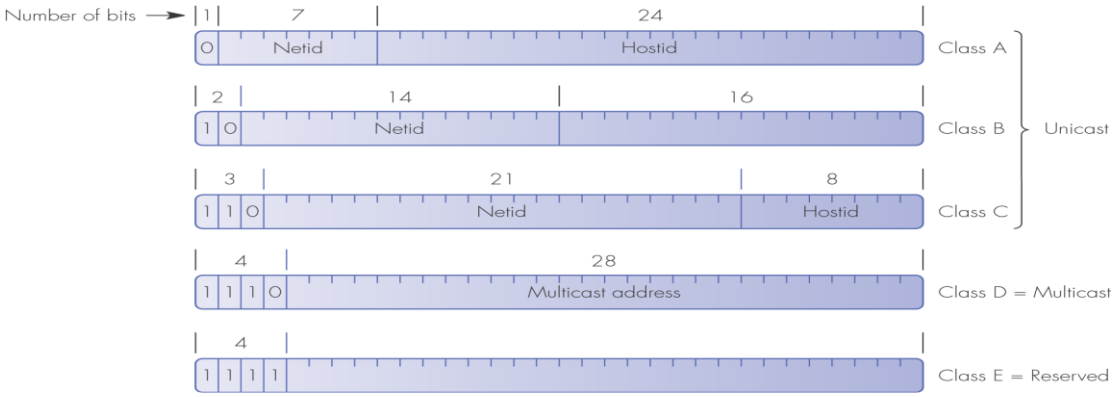
•Class C is suitable for large number of networks each attached to a small num-ber of hosts (up to 28=256).

•Class B is just right balance of A and C.

•Class D is for multicast use. In case of LANs the group address is a MAC add-ress and the class D IP address extends this mode of operation to the complete Internet.

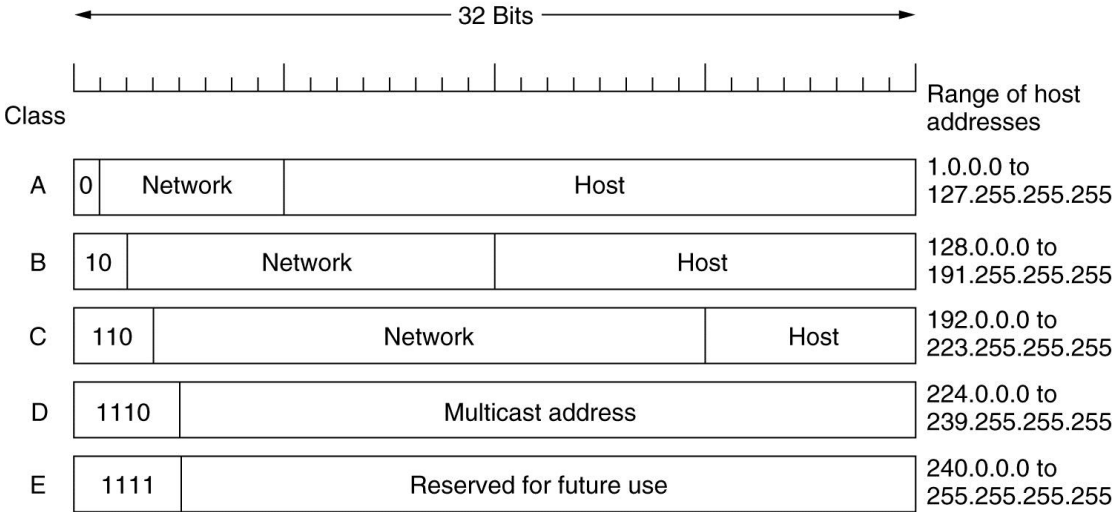
Examples of classful addresses: 00001010 00000000 00000000 00000000 = 10.0.0.0 – class A, netid 10 10000000 00000011 00000010 00000011 = 128.3.2.3 – class B, netid 128.3. hostid 2.3

The presentation of all classful addresses is simplified by dividing 32 bits into 4 bytes; each byte then is converted into its equivalent decimal form; the total IP address is represented as 4 decimal numbers with a dot between them – dotted decimal notation.



IPv4 addressing – Class-based addresses

•The range of possible host addresses for each class (in dotted decimal notations) are shown below:



Important: Observe that each class has a fixed number of the most significant bits (msbs). These bits are called a prefix. This is necessary in order to fix the position of the first 0 bit on the left which determines the corresponding class. This in turn means that, for example, all Class C

addresses will have the prefix 110 which must be kept unchanged for all Class C addresses. Therefore, in Class C there are in total (24-3)=21 bits to be used for netids, i.e. Class C address can handle in total 221 = 2,097,152 networks (not 224 = 16, 777,216 networks!). One also should exclude all 0s and all 1s as they are for the special netid addresses which are discussed next.

Public and Private Addresses

Although most IPv4 host addresses are public addresses designated for use in networks that are accessible on the Internet, there are blocks of addresses that are used in networks that require limited or no Internet access. These addresses are called private addresses.

Private Addresses

The private address blocks are:
10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)
192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)
Private space address blocks, as shown in the figure, are set aside for use in private networks. The use of these addresses need not be unique among outside networks. Hosts that do not require access to the Internet at large may make unrestricted use of private addresses. However, the internal networks still must design network address schemes to ensure that the hosts in the private networks use IP addresses that are unique within their networking environment. Many hosts in different networks may use the same private space addresses. Packets using these addresses as the source or destination should not appear on the public Internet. The router or firewall device at the perimeter of these private networks must block or translate these addresses. Even if these packets were to make their way to the Internet, the routers would not have routes to forward them to the appropriate private network.

Continue with class-based addresses also known as classful addressing (IPv4)

Class A: 00000000.00000000.00000000.00000000 to
01111111.11111111.11111111.11111111

Network Hosts

In decimal notation:

Class A: 0.0.0.0 to
:127.255.255.255

Network Hosts

Class B: 10000000.00000000.00000000.00000000 to
10111111.11111111.11111111.11111111

Network Hosts

In decimal: 128.0.0.0 to
191.255.255.255

Network Hosts

1 byte=8 bits

Example: 192.1.1.1

1st Octet 2nd Octet 3rd Octet 4th Octet

Class C: 11000000.00000000.00000000.00000000 to
11011111.11111111.11111111.11111111

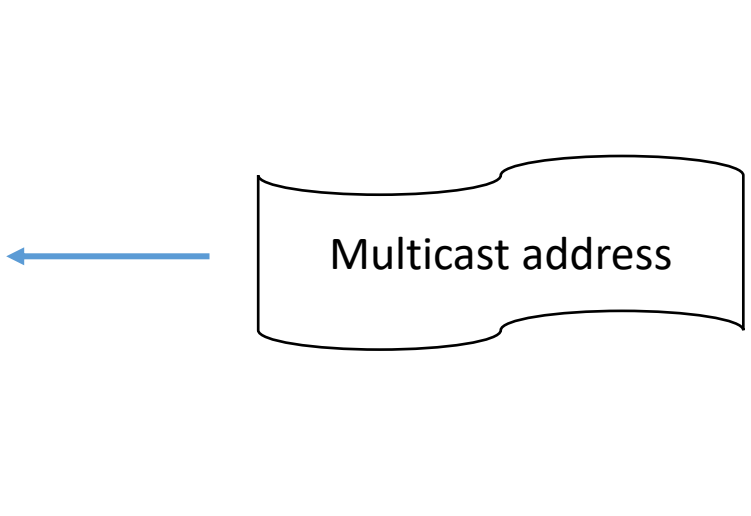
Network Hosts

In decimal: 192.0.0.0 to
223.255.255.255

Network Hosts

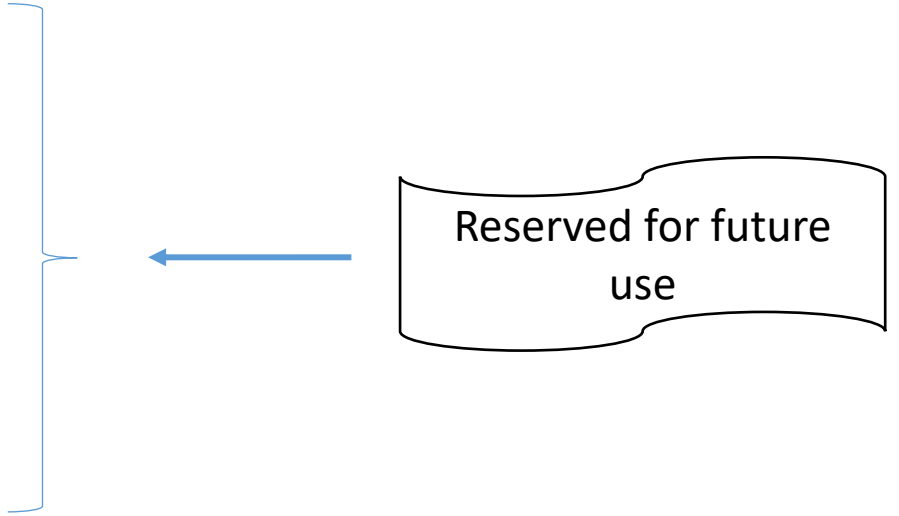
Class D: 11100000.00000000.00000000.00000000 to
11101111.11111111.11111111.11111111

In decimal: 224.0.0.0 to
239.255.255.255



Class E: 11110000.00000000.00000000.00000000 to
11111111.11111111.11111111.11111111

In decimal: *240.0.0.0* *to*
240.255.255.255



As you know the 8 bit =1 byte, the most significant bit is 2^7 and least significant bit is 2^0 as shown
Each bit in the 8 bit format: 0 0 0 0 0 0 0 0

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Note that when we say the address starts from 0 to 255 it means=256, the highest number you can see is 255.

HW:

Q\ In which class are the following IP addresses?

1- 10.10.10.1

2- 20.90.1.5

3-162.90.220.20

4- 127.1.1.200

5- 129.1.1.1

6- 200.1.1.200

7- 190.10.40.50

8- 226.30.60.10

9- 245.1.0.1

10- 216.255.255.0

IP Mask

Example: Which portion of the following IP address is network and which is the host ID:

IP:192.168.1.15

MASK:255.255.255.0

Solution: The first step is to write down the binary representation for the IP address and the MASK, put first the binary representation of the IP address then the binary representation of the MASK value.

IP:192.168.1.15

11000000.10101000.00000001.00001111

AND

MASK: 11111111.11111111.11111111.00000000

11000000.10101000.00000001.00000000

AND OPERATION: 1AND 1=1,
0 AND 0=0
1 AND 0=0
0 AND 1=0

192.168.1.0/24 bit ← The result is always first host IP address

Note that the 24 bit is represent the network and the left IP 192.168.1.0 address is the host.
The mask “on” or (1) bits= network portion of the IP. Hence, counting the number of 1’s in the mask you will know directly that the 24 bit is received for the net work and the remaining 8 bit is for hosts.

Example: if we have the mask 255.255.0.0 , IP: 192.168.1.35 what is the network and host

Solution: The first step is to write down the binary representation for the IP address and the MASK, put first the binary representation of the IP address then the binary representation of the MASK value.

IP:192.168.1.35
11000000.10101000.00000001.00100011 ***AND***
MASK: 11111111.11111111.00000000.00000000

The result:11000000.10101000.00000000.00000000 ← The result is always first host IP address

As we have explained before the number of 1's in mask address represent the network so counting the 1's will show, the 16 bits are for the network and the remaining values o's are for the hosts addresses.

MASK: 11111111.11111111 00000000.00000000

network Host id(s)

As the result above shows 11000000.10101000.00000000.00000000 which is equivalent to 192.168.0.0/16 bit network and 16 bit host address

Example: IP:192.168.1.15 if the mask is 255.255.255.0 then the class is C. as shown below:

IP:192.168.1.15
11000000.10101000.00000001.00001111

Class c

The mask 255.255.255.0 is : 11111111.11111111.11111111.00000000

Now if we change the mask from 255.255.255.0 to 255.0.0.0 how many network and hosts are available?

The mask value 255.0.0.0 which means the

IP:192.168.1.15
11000000.10101000.00000001.00001111 ***AND***
MASK: 11111111.00000000.00000000.00000000

The result:11000000.00000000.00000000.00000000 ← The result is always first host IP address

The result: 192.0.0.0/8bit, this means the 8 bit only for the network and the remaining bits are to define hosts

More about the mechanism of the MASK

Example: IP:10.25.3.99

Mask: 255.255.0.0

What is the network, host, number of bits for the network?

Solution: **first we focus on the Mask, the first octet is 255, the second octet is 255 which means 16 bit is for the Network and the other 16 bit is for the host .**

Hence, the IP:10.25.3.99

16 bit for network 16 bit for host

Do you think the first host address is :10.25.0.0/16 bit is right or not?