IP PROTOCOL – IPV4

Packets in the IPv4 format are called datagram. An IP datagram consists of a header part and a text part (payload). The header has a 20-byte fixed part and a variable length optional part. It is transmitted in big-endian order: from left to right, with the high-order bit of the Version field going first. IPv4 can be explained with the help of following points:

1. IP addresses
2. Address Space
3. Notations used to express IP address
4. Classfull Addressing
5. Subnetting
6. CIDR
7. NAT
8. IPv4 Header Format

5.4.1 IP addresses

Every host and router on the Internet has an IP address, which encodes its network number and host number.

The combination is unique: in principle, no two machines on the Internet have the same IP address.

An IPv4 address is 32 bits long

They are used in the Source address and Destination address fields of IP packets.

An IP address does not refer to a host but it refers to a network interface.

5.4.2 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 $\boldsymbol{2^N}$ because each bit can have two different values (0 or 1) and *N* bits can have $\mathbf{2^N}$ values.

IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion).

5.4.3 Notations

There are two notations to show an IPv4 address:

1. Binary notation

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

2. 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. Ex. 129.11.11.239 **5.4.4 Classful addressing** In classful addressing, the address space is divided into five classes: A, B, C, D, and E. **Figure: Classful addressing : IPv4 Netid and Hostid**

In classful addressing, an IP address in class A, B, or C is divided into netid and hostid.

These parts are of varying lengths, depending on the class of the address as shown above.

55

Information on the Number of networks and host in each class is given below:

The IP address 0.0.0.0 is used by hosts when they are being booted.

All addresses of the form 127.xx.yy.zz are reserved for loopback testing, they are processed locally and treated as incoming packets.

5.4.5 Subnetting

It allows a network to be split into several parts for internal use but still act like a single network to the outside world.

To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.

Consider a class B address with 14 bits for the network number and 16 bits for the host number where some bits are taken away from the host number to create a subnet number.

4Fig: A Class B network subnetted into 64 subnets.

56

If 6 bits from the host Id are taken for subnet then available bits are :

14 bits for network + 6 bits for subnet + 10 bits for host

With 6 bits for subnet the number of possible subnets is 2_6 which is 64.

With 10 bits for host the number of possible host are 2_{10} which is 1022 (0 & 1 are not available)

5.4.6 CIDR A class B address is far too large for most organizations and a class C network, with 256 addresses is too small. This leads to granting Class B address to organizations who do not require all the address in the address space wasting most of it. This is resulting in depletion of Address space. A solution is CIDR (Classless InterDomain Routing) The basic idea behind CIDR, is to allocate the remaining IP addresses in variable-sized blocks, without regard to the classes. **5.4.7 NAT (Network Address Translation)**

The scarcity of network addresses in IPv4 led to the development of IPv6.

IPv6 uses a 128 bit address, hence it has 2_{128} addresses in its address space which is larger than 2_{32} addresses provided by IPv4.

Transition from IPv4 to IPv6 is slowly occurring, but will take years to complete, because of legacy hardware and its incompatibility to process IPv6 address.

NAT (Network Address Translation) was used to speed up the transition process

The only rule is that no packets containing these addresses may appear on the Internet itself. The three reserved ranges are:

10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts) 172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts) 192.168.0.0 – 192.168.255.255/16 (65,536 hosts)

Operation:

Within the Organization, every computer has a unique address of the form 10.x.y.z. However, when a packet leaves the organization, it passes through a NAT box that converts the internal IP source address, 10.x.y.z, to the organizations true IP address, 198.60.42.12 for example.

57

5.4.8 IP Header Figure: The IPv4 (Internet Protocol) header The description of the fields shown in the diagram is as follows:

No	Field Name	Description
1	Version	Keeps track of the version of the protocol the datagram belongs to (IPV4 or IPv6)
2	IHL	Used to indicate the length of the Header. Minimum value is 5 Maximum value 15
3	Type of service	Used to distinguish between different classes of service
4	Total length	It includes everything in the datagram—both header and data. The maximum length is 65,535 bytes
5	Identification	Used to allow the destination host to identify which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same Identification value

6	DF	1 bit field. It stands for Don't Fragment. Signals the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again
7	MF	MF stands for More Fragments. All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.
8	Fragment offset	Used to determine the position of the fragment in the current datagram.
9	Time to live	It is a counter used to limit packet lifetimes. It must be decremented on each hop. When it hits zero, the packet is discarded and a warning packet is sent back to the source host.
10	Header checksum	It verifies Header for errors.
11	Source address	IP address of the source
12	Destination address	IP address of the destination
13	Options	The options are variable length. Originally, five options were defined: 1. Security : specifies how secret the datagram is 2. Strict source routing : Gives complete path to be followed 3. Loose source routing : Gives a list of routers not to be missed 4. Record route: Makes each router append its IP address 5. Timestamp: Makes each router append its IP address and timestamp

5.5 SUMMARY 1. TCP/IP has 4 layers: host to network, IP, Transport & Application
2. It uses 4 levels of address: physical, logical, port & specific