CLASS OF IP ADDRESS (COMPUTER NETWORK)

Pavan Kumar[1], Himanshu Raj[2], Neeraj Kumar[3], Indu Khatri[4]
[1,2,3]Student Of Computer science, BMCEM, Sonipat Computer,
[4]Asistant Professor Department of Computer Science, BMCEM, Sonipat

ABSTRACT: In order for systems to locate each other in a distributed environment, nodes are given explicit addresses that uniquely identify the particular network the system is on and uniquely identify the system to that particular network. When these two identifiers are combined, the result is a globally-unique address. This address, known as IP addresses, as IP number, or merely as IP is a code made up of numbers separated by three dots that identifies a particular computer on the Internet. These addresses are actually 32-bit binary numbers. In this paper we will explain the IP address and their classification, subnetting and super netting and also explain the method of subnetting and super netting with the help of suitable examples. We can secure our network and enhance the performance of the network with the help of Subnetting and Super netting.

I. IP ADDRESSES

The original Internet Protocol, IPv4, was developed in the early 1980s and served the global Internet community for more than three decades. IPv4 had a capacity of just over four billion IP addresses, which was enough for the experiment that the Internet started as in the 1980s. But IPv4 is a finite space, and after years of rapid Internet expansion, the pool of available unallocated addresses for IPv4 has been fully allocated to Internet services providers (ISPs) and users. Only 3.7 billion IPv4 addresses are usable by ordinary Internet access devices. The others are used for special protocols, like IP Multicasting. Today, none of those 3.7 billion IPv4 addresses remain unallocated.

[2] Every machine on a network has a unique identifier. Just as you would address a letter to send in the mail, computers use the unique identifier to send data to specific computers on a network. Most networks today, including all computers on the Internet, use the TCP/IP protocol as the standard for how to communicate on the network. In the TCP/IP protocol, the unique identifier for a computer is called its IP address. IPv4 uses 32 binary bits to create a single unique address on the network. An IPv4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10). For example: 192.168.1.100. It is actually 32- bit binary (base-2) numbers. Binary representation of 192.168.1.100 = 11000000.10101000.00000001.01100100

The binary number is important because that will determine which class of network the IP address belongs to. The Class of the address determines which part belongs to the network address and which part belongs to the node.

II. ASSIGNING IP ADDRESS

We can assign the IP address to computer with the help of two methods

1. Static IP (Manually)

2. Dynamic IP (Automatically with the help of DHCP Server)

2.1 IP ADDRESS CLASSIFICATION

IP addresses are divided into 5 classes

1. Class A
2. Class B

These Classes (A & B)are used in LAN & WAN

3.Class C (most used)
4.Class D (Reserved for Multicasting)
5. Class E (Reserved for Research & Development)

2.2 FIND THE RANGE OF CLASS

To find the range of each Class a bit called priority bit is used. Priority bit is the left most bit of the first octet.

Table- 1: IP Class and their respective Priority bit

Class	Priority bit
A	0
B	10
C	110
D	1110
E	1111

Table-2 Range of IP address

Class	Binary Number	Range of IP Address
A	00000000	0 -126
B	10000000	128 -191
C	11000000	192 -223
D	11100000	224 -239
E	11110000	240 -255

Note: 127.0.0.1 is the loopback Internet protocol (IP) address also referred to as the “localhost.” The address is used to establish an IP connection to the same machine or computer being used by the end-user.[3]

A. 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. 000000001-01111111
range: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.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (27 -2) and 16777214 hosts (224 -2).

Class A IPaddress format is thus:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

B.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. 100000001-10111111

range: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 B has 16384 (214) Network addresses and 65534 (216 -2) Host addresses.

Class B IP address format is:

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

C.Class C

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

that is: 1100000001-110111111

range:192-223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.Class C gives 2097152 (221) Network addresses and 254 (28 -2) Host addresses.

Class C IP address format is: 110NNNNN.NNNNNNNN.NNN

D. Class D

Address Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of that is: 11100000001-1110111111

range: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 is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

E.Class E

Address This IP Class is reserved for experimental purposes only 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.

3.IP4

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts 3. THE TCP/IP MODEL Ipv4 6 based upon their logical addresses and to route data among them over the underlying network. IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address. Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.

III. CONCLUSION AND FUTURE WORK

A major issue that has been ignored in this paper is security. We assumes that each node trusts every other node, but if this is Not the case then the following situations can arise:

**A node requests IP addresses for nodes that do not exist. In this way a node can acquire all the IP addresses denying others to participate in the network.

** A node assigns IP addresses to other nodes without following the given protocol. This can lead to IP address con_icts which might be dif_cult to resolve.

**A node selectively gives wrong information to other nodes. The synchronization process in our protocol depends on reliable broadcast. Since no such broadcast exists in a mobile distributed environment, one can question the robustness of the protocol.

Migration Process from IPv4 to IPv6 is been often compared to the Y2K problem, demanding time and investment of resources. Companies are yet to recognize IPv4 number exhaustion as an alarming problem, and are not ready to put off the investment required into the future. In the future there may be risk of insufficient time and cost [10]. The cost of migration to IPv6 could be a problem. Costs involved include renumbering networks and running two protocol stacks (IPv4 and IPv6) at the same time, upgrade to relevant software and hardware, training the manpower, and testing network implementations. However IPv6 does provide considerable benefits and features required by the modern secure internet. Given the number of problems in the current internetwork, migration process may be the only solution viable in the long run.

REFERENCES

[1] Paessler-A short introduction to IP Addresses: https://www.paessler.com/support/kb/ questions /50

[2] ICANN - IPv6 Fact Sheet: https://www.icann.org/en/system/files/files/factsheetipv6-03feb11-en.pdf

[3] Tech-Faq 127.0.0.1 – What Are its Uses and Why is it Important? http://www.tech-faq.com/127-0-0-1.html

[4] Calculation of Max Networks and Max Hosts: http://www.infocellar.com/networks/ip/maxnetworks-hosts.htm

[5] Vicomsoft - What are private and public IP addresses? http://www.vicomsoft.com/glossary/ipaddresses/

[6] Techopedia- Subnetting: https://www.techopedia.com/definition/28328/subnett

[7] http://ipv6security.wikia.com/wiki/Ipv6_header

[8] IETF IPv6 Transition Working Group, http://www.6bone.net/ngtrans.

[9] http://en.wikipedia.org.
[10] http://www.cybertelecom.org/dns/ipv6_transition.htm