iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** X **Month of publication:** October 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Concept of Subnets in Computer Networking

Ramanpreet Kaur[1], Ramandeep Kaur[2]
[1,2]Faculty of Computer Science, Baba Farid group of Institutions, Bathinda, Punjab, India

Abstract: An organization can subdivide its host address space into groups called subnets. The subnet ID is generally used to group hosts based on the physical network topology. Subnets can simplify routing. IP subnet broadcasts have a hostID of all 1s. Subnetting is a process of dividing large network into the smaller networks based on layer 3 IP address. Every computer on network has an IP address that represents its location on network. Two version of IP addresses are available IPv4 and IPv6. In this article we will perform subnetting on IPv4.

I. INTRODUCTION TO SUBNETS

A subnetwork, or subnet, is a logically visible subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. All computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. This results in the logical division of an IP address into two fields, a network or routing prefix and the rest field or host identifier.A subnet mask is what tells your computer (or other network device) what portion of the IP address is used to represent your network and what part is used to represent hosts (other computers) on your network. For example, if you have an IP address of 1.1.1.1 and a subnet mask of 255.255.255.0, the 255s mask off the first three 1s

A. Need of Subnets

Users need to talk to printers, email programs need to talk to servers, and each of these "things" needs to have some sort of address. This is no different from a house address, but with one minor exception: the addresses need to be in numerical form. It is not possible to have a device on a network that has alphabetical characters in its address like "23rd Street." Its name can be alphanumeric - and we could translate that name to a numeric address - but the address itself must be numbers alone.There are two ways to denote these masks. First, since you are using three bits more than the "natural" Class C mask, you can denote these addresses as having a 3-bit subnet mask. Or, secondly, the mask of 255.255.255.224 can also be denoted as /27 as there are 27 bits that are set in the mask. This second method is used with CIDR. With this method, one of these networks can be described with the notation prefix/length. For example, 204.17.5.32/27 denotes the network 204.17.5.32 255.255.255.224. When appropriate the prefix/length notation is used to denote the mask throughout the rest of this document.

If you are asked for valid hosts in the 192.168.30.7/28 range, you begin by counting off the chart to see the numerical value for the 28th bit, which is 16. Then, take a look at the last octet -- since 28 puts us in the last octet range -- and divide it by 16. In this case, we don't have to, because we can see it is less than 16, but if you are given .189 rather than .7, you would divide 189 by 16 and see it was over 11. Then, multiply 11 times 16 to see the first address in that subnet, 176. Then, add 16 to 176, and you'll get the first address of the next subnet, 192. That means .189 falls in the subnet 176 – 188. We know the first number is the network address, 192.168.30.176, and the last number is the broadcast address, 255.255.255.188. Remember, we are breaking down that 256 block, so we can't use the full 256 subnet -- only the portion blocking our network. That means the hosts must fall in the range of 177 – 187 -- one after 176 and one before 188.

B. IPv4

IP addresses are displayed in dotted decimal notation, and appear as four numbers separated by dots. Each number of an IP address is made from eight individual bits known as octet. Each octet can create number value from 0 to 255. An IP address would be 32 bits long in binary divided into the two components, network component and host component. Network component is used to identify the network that the packet is intend for, and host component is used to identify the individual host on network.

IP addresses are broken into the two components:

Network component: Defines network segment of device.

Host component: Defines the specific device on a particular network segment

IP Classes in decimal notation

Class A addresses range from 1-126

Class B addresses range from 128-191
Class C addresses range from 192-223
Class D addresses range from 224-239
Class E addresses range from 240-254

0 [Zero] is reserved and represents all IP addresses.
127 is a reserved address and is used for testing, like a loop back on an interface.
255 is a reserved address and is used for broadcasting purposes.

C. Subnet mask

Subnet mask is a 32 bits long address used to distinguish between network address and host address in IP address. Subnet mask is always used with IP address. Subnet mask has only one purpose, to identify which part of an IP address is network address and which part is host address.

For example how will we figure out network partition and host partition from IP address 192.168.1.10 ? Here we need subnet mask to get details about network address and host address.

In decimal notation subnet mask value 1 to 255 represent network address and value 0 [Zero] represent host address.

In binary notation subnet mask **ON** bit [1] represent network address while **OFF** bit[0] represent host address.

1) In decimal notation

IP address 192.168.1.10
Subnet mask 255.255.255.0

Network address is **192.168.1** and host address is **10**.

2) In binary notation

IP address 11000000.10101000.00000001.00001010
Subnet mask 11111111.11111111.11111111.00000000

Network address is 11000000.10101000.00000001 and host address is 00001010

D. 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.

E. Block Size

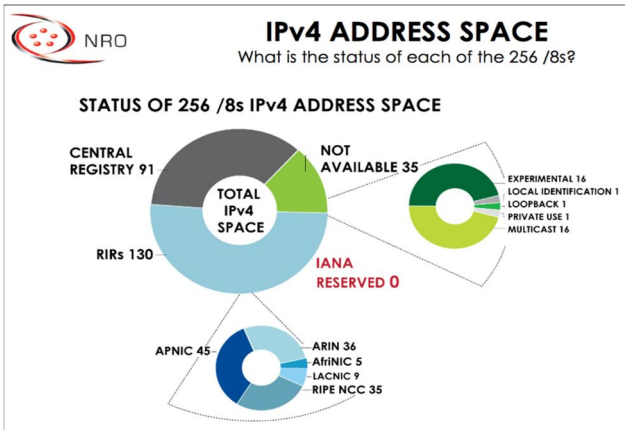
Block size is the size of subnet including network address, hosts addresses and broadcast address.

F. 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



The main difference between direct broadcast and full broadcast is that routers will not propagate local broadcasts between segments, but they will propagate directed broadcasts.

G. 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.

1) 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. In above example address 0,64,128,192 are the network address.

a) Network address is always the first IP address of subnet.

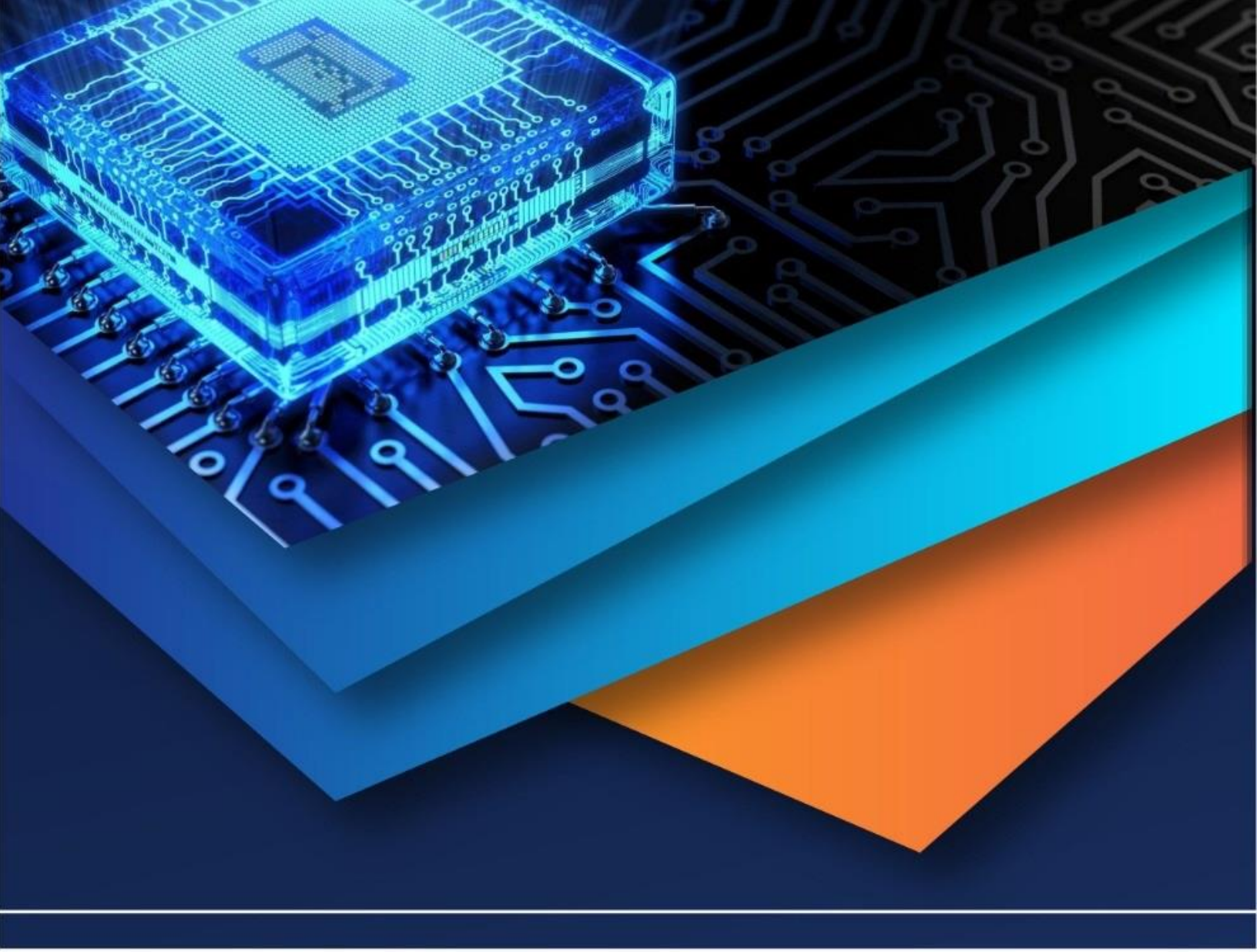
b) Broadcast address is always the last IP address of subnet (IP address before the next subnet).

II. CONCLUSION

A subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. Without subnets, an organization could get multiple connections to the Internet, one for each of its physically separate subnetworks, but this would require an unnecessary use of the limited number of network numbers the Internet has to assign. It would also require that Internet routing tables on gateways outside the organization would need to know about and have to manage routing that could and should be handled within an organization.

REFERENCES

[1] TCP/IP and Internetworking by Douglas E Comer, 2009
[2] Xianhui Che, Lee J. Cobley, “VoIP Performance over Different Interior Gateway Protocols”, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 1, April 2009.
[3] Radia Perlman, “A Comparison between Two Routing Protocols: OSPF and IS-IS,”IEEE Network Magazine, September, 1991.
[4] Bernard Fortz,Jennifer Rexford and Mikkel Thorup., Traffic Engineering With Traditional IP Routing Protocols." IEEE Communications Magazine. October 2002,
[5] Computer Networks byAndrew s Tenenbaum, 4th edition
[6] M. Gunes and K. Sarac. Resolving IP aliases in building traceroute-based Internet maps. Technical report, University of Texas at Dallas, December 2006
[7] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman. PlanetLab: An overlay testbed for broad-coverage services. ACM/SIGCOMM Computer Communication Review, 33(3):3–12, 2003
[8] S. Bilir, K. Sarac, and T. Korkmaz. Intersection characteristics of end-to-end Internet paths and trees. In IEEE ICNP, Boston, MA, November 2005
[9] Sandra Sendra, Sandra, Pablo, A., Miguel, A. and Lloret, Jaime 2010. Study and Performance of Interior Gateway IP Routing Protocols, Network Protocols and Algorithms
[10] Cisco Visual Networking Index: Forecast and Methodology, 2012–2017 White Paper Proceedings , Cisco system Inc., 2013
[11] Uyless D. Black, Computernetworks: protocols, standards, and interfaces, 2nd ed, PTR Prentice Hall, 1993.
[12] Cisco Visual Networking Index: Forecast and Methodology, 2012–2017 White Paper Proceedings , Cisco system Inc., 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY