RESEARCH ARTICLE OPEN ACCESS

Very Simple Way of Sub Netting for Internetworking Protocol Version 4

Er. Shaikh Wasim Shaikh Ayyub[1], Prof. V. J. Kadam[2]

[1]*(Tata Communication Transformation Services, Limited, Dighi, Pune, Maharashtra, India).*
[2]*(Department of Information Technology, Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra).*

ABSTRACT
When a student performs sub netting he has ample amount of time in exam to do it using various ways. But when same thing a network admin or security admin does, he has time frame limit. Consider in real corporate world a person who is security admin is using very traditional and time consuming methods instead of simple and easy approach, in the situation where site is down and business is hampering. Thus I think there should be very simple way of doing it for both student as well as corporate person.

Keywords: Security, Admin, Corporate, Business, Network.

I. INTRODUCTION

This article is focusing on simplest and easiest way of subnetting. Most of the people have only this perception that IP subnetting is used to break large network into small network only for the purpose of security, creating VLAN and breaking organizational network domain. Yes it is, but simultaneously it is very useful for saving hundreds of IP addresses. Also router routes between two network, thus in order to perform routing, two ports of router must be in different Subnets. Hence subnetting is needed. If the network administrator is versed in subnetting, he won't waste bunch of IP addresses. If it is Ethernet network then it may possible that network admin will avoid wastage of IP address if he has broken that subnet in wrong way into small, small subnets. But if it is WAN, where it works on serial technology and where we need only 4 IP addresses, and admin has broken subnet in the wrong way then it may cause wastage of many addresses. Thus this article is focusing on different scenarios of subnetting, network admin should use to avoid wastage of IP addresses. We represent subnet mask using dotted decimal numbers from 0-255 etc. But when someone performs subnetting, he needs reference of bits and bytes to convert /8, /16, /24, /27 etc. to subnet mask. Counting binary 1's and 0's and then converting it in the decimal is really time consuming and requires a lot attention which network admin feels hectic job. This article is focussing on how to perform subnetting by merely using bits and bytes in the account.

Shaikh Wasim Shaikh Ayyub is currently working at Tata Communication Transformation Service Limited, Dighi, Pune, Maharashtra, India (e-mail: wasimahemadshaikh@gmail.com).

Vinod J.Kadam, is currently working as Assistant Professor in department of Information Technology Dr. Babasaheb Ambedkar Technological University, Lonere, Tal-Mangaon. Dist-Raigad, Maharashtra, India Pin- 402103 (e-mail: vjkadam@dbatu.ac.in).

II. TERMINOLOGY

Classes of IP address: IP addresses are having range 0.0.0.0 to 255.255.255.255 and they are 2^32= 4 billion plus. IP addresses are divided into 5 classes name as A, B, C, D and E.

Prefix mask: Some classes have default prefix mask like class A has /8, class B has /16 and class C has /24 etc. It is also known as CIDR value i.e. Classless Inter Domain Routing.

Subnet mask: While performing configuration, we cannot give prefix mask, we assign subnet mask to the IP address. We can represent default mask as,
/8=255.0.0.0
/16=255.255.0.0
/24=255.255.255.0
/32=255.255.255.255

III. SUBNETTING

Rules of Subnetting:
Two directly connected devices should be in same network or subnet, two ports of router should not be in same subnet.

Methods of Subnetting:
We generally follow two corporate methods for subnetting.
1. Subnetting by network point of view.
2. Subnetting by host point of view.

DOI: 10.9790/9622-0701051315

1. Subnetting by network point of view Steps to be followed:

- Get the required number of networks.
- Subtract given CIDR value of network from 32.
- Find number of host you will get using binary 2.
- Divide that value by number of network and you will get number of host in each subnet.
- Represents that number in power of 2 and you will have decimal value.
- Subtract that decimal value from 32 and you will have CIDR value for each small subnets.

Example: In your organization you have established 4 new offices and you as network admin will give them IP addresses. Given subnet for you is 16.20.20.0/24
Step 1: Get number of required networks or subnets you want.
Thus for 4 offices you may need 8 networks as shown below in fig.
Step 2: Subtract given CIDR value from 32.
Thus subtract 24 from 32, you will get 8.
Step 3: Number of host you have is,
2^8=256
Step 4: Divide this value by number of network.
So 256/8=32….. Host in each subnets.
Step 5: Represents this value in power of 2 to get decimal number.
So 2^x=32………… Hence decimal value is 5.
Step 6: Subtract this decimal value from 32 and you will have new CIDR value for your small subnet.
So new CIDR is 32-5=27

Thus we have following subnets:
16.20.20.0/27-16.20.20.31/27
16.20.20.32/27-16.20.20.63/27
16.20.20.64/27-16.20.20.95/27
16.20.20.96/27-16.20.20.127/27
16.20.20.128/27-16.20.20.159/27
16.20.20.160/27-16.20.20.191/27
16.20.20.192/27-16.20.20.223/27
16.20.20.224/27-16.20.20.255/27
Where first subnet is known as subnet zero.

2. Subnetting by host point of view
Steps to be followed:

- Get number of host you want in total.
- Divide it by number of subnets you need.
- Find decimal number for it in power of 2.
- Subtract that number from 32.
- You will get CIDR value or subnet mask for small subnets.
- Now, use the same method to form subnets and IP addresses in it.

Example: In your organization you have established 4 new offices and you as network admin will give them IP addresses. Given subnet for you is 16.20.20.0/24
Step 1: Get number of host you want.
Here suppose according to business team they need 256 host.
Step 2: Divide it by number of subnets.
So suppose for 4 offices you may need 8 networks.
So 256/8=32
Step 3: Make it decimal in power of 2
So 2^x=32
So x=5
Step 4: Subtract this from 32 to get subnet mask (CIDR) you are forming.
So 32-5=27.
So you have now all the things to form subnets. Just make the list of it.
Thus we have following subnets:
16.20.20.0/27-16.20.20.31/27
16.20.20.32/27-16.20.20.63/27
16.20.20.64/27-16.20.20.95/27
16.20.20.96/27-16.20.20.127/27
16.20.20.128/27-16.20.20.159/27
16.20.20.160/27-16.20.20.191/27
16.20.20.192/27-16.20.20.223/27
16.20.20.224/27-16.20.20.255/27

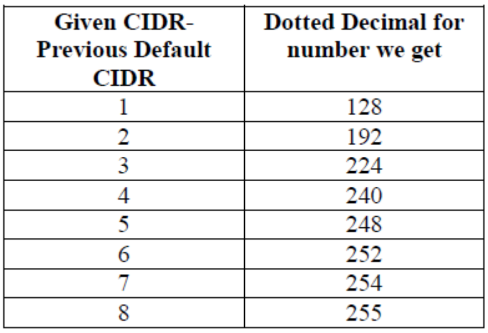
IV. CONVERTING CIDR VALUE INTO SUBNET MASK

CISCO has given specific format for all the CIDR values from /1- /32. But keeping them all in mind while configuration is hectic, as well as finding them manually using bits and bytes calculation is also boring. Thus we can do it in simple way.

We have octet which represents 256 possibilities. Thus when we will convert any CIDR value we will keep it in mind. Also we will keep default CIDR’s in mind like,
/8=255.0.0.0
/16=255.255.0.0
/24=255.255.255.0
/32=255.255.255.255

But when we will get any CIDR value other than default, we will use its previous default value to find its subnet mask
Subtract default value from given CIDR.
Example: /27
Default CIDR value=24
So 27-24=3

Now use following chart for converting CIDR value into dotted decimal value instead of traditional approach:



Given CIDR-Previous Default CIDR	Dotted Decimal for number we get
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

How we can avoid mugging up all the dotted decimal mask for CIDR values, using this chart.
First find previous default CIDR value and make it dotted decimal like,
/8= 255.0.0.0
/16= 255.255.0.0
/24= 255.255.255.0
Now for next octet use above chart.
If after subtraction you get 1 use 128, for 2 use 192 and so on.
First write default dotted decimal for default CIDR and then use chart to write value in next octet.
Example: 1
Write 192.168.2.1/18
So default is 16 i.e. 255.255.0.0 and next octet will have 18-16=2
So for 2 we have 192 in the chart,
Thus it will be 192.168.2.1 255.255.192.0
Example: 2
Write 172.16.0.18/30
So default is 24 i.e. 255.255.255.0 and next octet will have 30-24=6
So for 6 we have 252 in the chart,
Thus it will be 192.168.2.1 255.255.255.252
Example: 3
Write 72.16.8.8/13
So default is 8 i.e. 255.0.0.0 and next octet will have 13-8=5
So for 5 we have 248 in the chart,
Thus it will be 192.168.2.1 255.248.0.0

This is how for any CIDR value admin can easily find dotted decimal value while configuration, without going into the details of bits and bytes and octets and class of IP address etc.

V. CONCLUSION

Subnetting is very crucial part when it comes to IPV4. Even though now we are moving toward use of next version of IP that is V6, we cannot drop the importance of V4 as most of the organization have model and network built in IPV4. Nowadays use of tunnelling like IPV4 to IPV6 and vice versa has increased to maintain compatibility between new and old infrastructure. Thus we still need study on various aspects which will kill time consuming and traditional way of doing work. Here I have suggested different approach by which we can make hectic task of subnetting for network and security admin very easy. Even though there are some websites which have application interface to provide help to complete this task of subnetting, using it in daily practice will definitely improve quality of concepts and help students as well as person working in industry.

REFERENCES

[1] Jiff Doyle, "CCIE Professional Development - Routing TCP-IP, Volume I". Edition 1, 2002.
[2] Jiff Doyle, "CCIE Professional Development - Routing TCP-IP, Volume I". Edition 2, 2005.
[3] Rene Molenaar, "How to Master Subnetting". Edition published in 2002-2013
[4] John J Kowalski, "IP Subnetting Made Easy". Edition released in 2007.
[5] Adam Vardy, "Subnetting for Beginners". Published in 2016.
[6] Todd Lammle, "CCNA Routing and Switching complete study guide: Exam 100-105". Published in 2013.
[7] Wendell Odom, "Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide". Published in 2013
[8] Paul William, "Cisco CCNA in 60 Days". Published in 2012.
[9] Gary A. Donahue, "Network Warrior". Published in 2007.
[10] Tim Boyles, "CCNA Security'. Published in 2010.