IP Subnetting

Article *in* International Journal of Knowledge Engineering and Soft Data Paradigms · March 2013

1 author:

Shailesh N Sisat
Newtek Electrical
2 PUBLICATIONS **1** CITATION

International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 2, Issue 5

IP Subnetting

Shailesh N. Sisat Prajkta S. Bhopale Vishwajit K. Barbudhe

Abstract - **Network management becomes more and more important as computer-networks grow steadily. A critical skill for any network administrator or security admin that supports a network environment is IP Subnetting. This knowledge can be gained by different methods and it is needed in different point of views. These individual views arise from distinct needs of persons, who are involved in network management. The following use cases represent selected groups of managers or engineers. They are not complete, but should increase comprehension of the complexity of network discovery. This paper discusses why subnetting is important, IP addressing basics, decimal to binary conversion and early subnetting.**

Keywords: **TCP/IP, IP Subnetting, Class of network**

I. INTRODUCTION

This article is focusing on the basics of Subnetting. While using IP address it is very easy to break it in to subnets so that the one network address can be used for more than one networks, The theory called as Subnetting. Subnetting allows us to break a large network into a bunch of smaller networks. If an organization is large or if its computers are geographically dispersed, it makes good sense to divide network into smaller ones connected together by routers. Subnetting is important for several reasons.

- Reduced Network Traffic: By subnetting

the network we can partition it to as many smaller networks as we need and this also helps reduce traffic and hides the complexity of the network.

- Optimized network performance:

Reduced network traffic results in optimized network performance.

- Simplified management: quickly identify

and resolve network problem in a bunch of smaller networks than within a single big network.

- Security: Subnetting can help ensure

network security by facilitating communication between computers on the same subnet while preventing access from computers on other subnets.

- Facilitates spanning of large

Geographical distance: Because WAN links are comparatively slower and more expensive than LAN links, a single large network that spans long distances can create problems in every area. Connecting multiple smaller networks makes the system more efficient.

Introduction to IP: Before we start dive into subnetting, we need to study some basics. The first item for discussion is the IP address. An IP address is a numeric identifier assigned to each machine on an IP network. It designates the specific location of a device on the network. An IP address is a 32-bit number typically represented in four sections called *octets*. These sections are segregated by a dot called as dotted decimal representation. A sample IP address is 172.16.10.15. This IP address is what identifies a system or resource on a particular IP network. The IP address itself is actually made up of two parts. One part identifies the network that the host belongs to, and the other part identifies the host. To figure out where
the network portion stops and the host part begins you need a subnet mask. A subnet mask is also represented in dotted decimal notation. When you see an IP address, you will always see another number associated with the IP address that looks something like one of the following:

- 255.0.0.0
- 255.255.0.0
- 255.255.255.0

This number is called as subnet mask. Following figure shows an IP header

<table>
<tr><td>Version (4)</td><td>Header Length (4)</td><td>Type of service (8)</td><td colspan="2">Total length (16)</td></tr>
<tr><td colspan="3">Identification (16)</td><td>Flags (3)</td><td>Fragment offset (13)</td></tr>
<tr><td>Time to live (8)</td><td colspan="2">Protocol (8)</td><td colspan="2">Header checksum (16)</td></tr>
<tr><td colspan="5">Source IP address (32)</td></tr>
<tr><td colspan="5">Destination IP address (32)</td></tr>
<tr><td colspan="5">Options + Padding (0 or 32 if any)</td></tr>
</table>

The fields are as follows.

- Version: IP version number.
- Header length: Header length in 32-bit words.
- Type of service: Type of service tells how the datagram should be handled. The first three bits are the priority bits which are now called the differentiated services bits.
- Total length: Length of the packet including header and data.
- Identification: Unique IP- packet value used to differentiate fragmented packets from different datagram.
- Flags: Specifies whether fragmentation should occur.
- Fragment offset: Provides fragmentation and reassembly if the packet is too large to put in a frame. It also allows different maximum transmission units on the internet.
- Time to live: This field indicates the maximum time the

datagram is allowed to remain in the internet system. If this field contains the value zero, then the datagram must be destroyed. This field is modified in internet header processing. The time is measured in units of seconds, but since every module that processes a datagram must decrease the TTL by at least one even if it process the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram may exist. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime.

- Protocol: In the Internet Protocol version 4 (IPv4) [RFC791] there is a field called "Protocol" to identify the next level protocol. This is an 8 bit field. In Internet Protocol version 6 (IPv6) [RFC2460], this field is called the "Next Header" field.
- Header checksum: Cyclic redundancy check (CRC) on header only.
- Source IP address: 32-bit IP address of sending station.
- Destination IP address: 32-bit IP address of the station this packet is destined for.
- Options: Used for network testing, debugging, security. Encodes the options requested by the sending user.

II. DECIMAL AND BINARY

In IP subnetting, it is important that we know how to convert IP addresses and subnet masks from their decimal form to the binary form because the locations of the 1s and 0s is extremely important.

If we use the sample IP address from before, 172.16.10.15, and represent it in binary format, it would look like this: 10101100.00010000.000001010.00001111. So, how do we get from the decimal form to the binary form, and vice versa?

First, let's convert from binary to decimal. If we take the first octet of our sample IP address and map it to the binary numbering system, it looks like this:

Binary	2^7 =128	2^6 =64	2^5 =32	2^4 =16	2^3 =8	2^2 =4	2^1 =2	2^0 =1
IP address	1	0	1	0	1	1	0	0

Now all we have to do is add the decimal numbers together where a 1 appears and we will get the decimal equivalent of the binary number. In this case it looks like this:

128 + 32 + 8 + 4 = 172.

Now let's convert from binary to decimal. let's take our 172 example from previously. The formula for conversion is as follows.

1. First divide the number by 2. The remainder will be either 0 or 1.
2. Write down the remainder.
3. Divide the remaining number without the remainder by 2. Again, the remainder will be either 1 or 0.
4. Write down the remainder to the left of the previous remainder.
5. Repeat this until you end up with 0.

For 172, the formula would look like this:

172 ÷ 2 = 86 remainder 0
86 ÷ 2 = 43 remainder 0
43 ÷ 2 = 21 remainder 1
21 ÷ 2 = 10 remainder 1
10 ÷ 2 = 5 remainder 0
5 ÷ 2 = 2 remainder 1
2 ÷ 2 = 1 remainder 0
1 ÷ 2 = 0 remainder 1

So binary number for 172 = 10101100.

Each section of an IP address is 8 bits long. In the previous example, the conversion worked out to 8 bits exactly, so that was easy. If we used a smaller number such as 12, we would have reached 0 before we had 8 bits. If this occurs, fill in the remaining bits with 0s. For example:

12 ÷ 2 = 6 remainder 0
6 ÷ 2 = 3 remainder 0
3 ÷ 2 = 1 remainder 1
1 ÷ 2 = 0 remainder 1

Because we got to 0 in only four steps, the remaining bits are 0---so the binary of 12 is 00001100.

III. IP TERMINOLOGY

- Network address: This is the designation used in routing to send packets to a remote network. for example, 10.0.0.0,172.16.0.0 and 192.168.0.0
- Broadcast address: The address used by applications and hosts to send information to all nodes on a network is called the *broadcast address*. Example include 255.255.255.255, which is any network, all nodes; 172.16.255.255, which is all subnets and hosts on network 172.16.0.0; and 10.255.255.255, which broadcasts to all subnets and hosts on network10.0.0.0
- Class of network: The designer of the Internet decided to create classes of network based on network size, for the small number of networks possessing a very large number of nodes, they created the rank *Class A network.* At the other extreme is the *Class C network*, which is reserved for the numerous networks with a small number of nodes. The class distinction for networks between very large and very small is predictably called the *Class B network.*

Subdividing an IP address into a network and node address is determined by the class designation of one's network. Following fig summarizes the three classes of networks.

	8bits	8bits	8bits	8bits
Class A:	Network	Host	Host	Host
Class B:	Network	Network	Host	Host
Class C:	Network	Network	Network	Host

Class D: Multicast
Class E: Research

The determination of which class a particular network fell in was determined by the first octet of the IP address, specifically by the first few bits of the first octet. This is represented in the following table.

	First Bits	1st Octet	Number of networks	Hosts per network
Class A	0	1-126	126	16,777,214
Class B	10	128-191	16,384	65,534
Class C	110	192-223	2,097,152	254
Class D	1110	224-239	n/a	n/a
Class E	11110	240-254	n/a	n/a

The network ID cannot be 127. The 127.0.0.0 network is reserved for loop-back and was originally designed for testing purposes. *Class D* and *E* are special classes; in this article discussion is focus on Classes A, B, and C. Each of these classes has a default subnet mask and a private address range.

***Private Addresses*:** The address can be public (i.e., unique) or private. In today's enterprise networks, private addressing is commonly used because of the address shortage in IPv4. In enterprise networks private addressing is preferred because it provides secure access rather than open and public access to the enterprise network. The private address ranges are utilized on internal networks, and addresses in these ranges cannot be routed in the public network of the Internet. These defaults and private ranges are shown here:

Class	Default Subnet Mask	Private Address Range
Class A	255.0.0.0	10.0.0.0 - 10.255.255.255
Class B	255.255.0.0	172.16.0.0 - 172.31.255.255
Class C	255.255.255.0	192.168.0.0 - 192.168.255.255

***Subnetting the network*:** A large network is divided into a smaller network the process is known as Subnetting and the smaller network is known as subnetwork or subnet.
To create subnetworks, take bits from the host portion of the IP address and reserve them to define the subnet address. This means fewer bits for hosts, so the more subnets, the fewer bits available for defining hosts.

***Subnet Mask*:** In order to reduce the conjunction, network is logically break into pieces. Netmask is mechanisum, we have to use it to identify the range of IP to create a network.A subnet mask is a 32 bit value that allows the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID portion of the IP address. Following table shows the default subnet masks for class A, B and C.

Class	Format	Default Subnet Mask
A	network.node.node.node	255.0.0.0
B	network.networ.node.node	255.255.0.0
C	network.networ.network.node	255.255.255.0

Classless Inter Domain Routing (CIDR):
CIDR is the method that ISP (Internet service providers) use to allocate a number of addresses to a company or a customer. ISP provide addresses in a certain block size. for example 192.168.10.32/28. We may identify the subnet mask from this block size. The slash notation (/) means how many bits out of 32 bits are turned on (1s).
for example , a Class C default mask would be 255.255.255.0, which is /24 because 24 bits are ones (1s),
11111111.11111111.11111111.0
Following table shows every available subnet mask and its equivalent CIDR slash notation.

Subnet Mask	CIDR Value	Subnet Mask	CIDR Value
255.0.0.0	/8	255.255.240.0	/20
255.128.0.0	/9	255.255.248.0	/21
255.192.0.0	/10	255.255.252.0	/22
255.224.0.0	/11	255.255.254.0	/23
255.240.0.0	/12	255.255.255.0	/24
255.248.0.0	/13	255.255.255.128	/25
255.252.0.0	/14	255.255.255.192	/26
255.254.0.0	/15	255.255.255.224	/27
255.255.0.0	/16	255.255.255.240	/28
255.255.128.0	/17	255.255.255.248	/29
255.255.192.0	/18	255.255.255.252	/30
255.255.224.0	/19		

The largest mask available (regardless of the class of address) can only be a /30 because at least 2 bits for host bits are required.
The /8 through /15 can only be used with Class A network addresses. /16 through /23 can be used by Class A and B network addresses. /24 through /30 can be used by Class A, B, and C network addresses.
Hosts and routers use Boolean math to determine the netid and the hostid and the hosted by the use of ANDing.

Bit1	Bit2	Result
0	0	0
0	1	0
1	0	0
1	1	1

Simple steps in Subnetting:

- Identify Class of network
- Default Net mask
- Number of networks = $2^{(\text{number of stolen bits})}$
- Number of hosts per network= $2^{(\text{available bit} - \text{stolen bit})} - 2$

Subnetting a *Class C* address:

Example: Network address = 192.168.10.**0**
Subnet mask = 255.255.255.**192**

- 1st step: identify class of network
  It's a *Class C* network
- 2nd step: Default subnet mask
  255.255.255.0

192=128+64

	128	64	32	16	8	4	2	1
0 →	0	0	0	0	0	0	0	0
192 →	1	1	0	0	0	0	0	0
	0	0	0	0	0	0	0	0

Result of above AND operation is zero (0) hence the first IP address is 192.168.10.0

- 3rd step: Number of subnetworks = $2^{(\text{number of stolen bits})}$

  $2^2 = 4$ subnets
- 4th step:
  Number of hosts per subnetwork= $2^{(\text{available bit} - \text{stolen bit})} - 2$

  $= 2^{(8-2)}-2$
  $= 62$ hosts

a) 192.168.10.0 1st subnet IP
b) 192.168.10.1 1st valid host IP
c) 192.168.10.62 last valid host
d) 192.168.10.63 broadcast IP

Similarly the following table shows the all possible subnets, the valid host ranges of each, and the broadcast address of each subnet.

subnet IP	x.x.x.0	x.x.x.64	x.x.x.128	x.x.x.192
1st valid host IP	x.x.x.1	x.x.x.65	x.x.x.129	x.x.x.193
last valid host	x.x.x.62	x.x.x.126	x.x.x.190	x.x.x.254
Broadcast IP	x.x.x.63	x.x.x.127	x.x.x.191	x.x.x.255

Example: Network address = 192.168.10.**49**
Subnet mask = 255.255.255.**240**

what is the subnet and broadcast address of the network of which the above address is a member?

- 1st step: identify class of network
  It's a *Class C* network
- 2nd step: Default subnet mask
  255.255.255.0

49=32+16+1
240=128+64+32+16

	128	64	32	16	8	4	2	1
49 →	0	0	1	1	0	0	0	1
240 →	1	1	1	1	0	0	0	0
	0	0	1	1	0	0	0	0

32+16=48

Result of above AND operation is zero 48 hence the first IP address is 192.168.10.48

- 3rd step: Number of subnetworks = $2^{(\text{number of stolen bits})}$

  $2^4 = 16$ subnets
- 4th step:
  Number of hosts per network= $2^{(\text{available bit} - \text{stolen bit})} - 2$

  $= 2^{(8-4)}-2$
  $= 14$ hosts

Now we know the possible subnets are 16. Now keep adding 16 until we pass the host address 49, starting from zero.0, 16,32,48,64, and so on. The host address of 49 is between 48 and 64 so the subnet is 48.

a) 192.168.10.48 1st subnet IP
b) 192.168.10.49 1st valid host IP
c) 192.168.10.62 last valid host
d) 192.168.10.63 broadcast IP

Subnetting a *Class B* address:

Example: Network address = 172.16.**0.0**
Subnet mask = 255.255.**128.0**

1st step: identify class of network
It's a Class B network
2nd step: Default subnet mask
255.255.0.0

128

	128	64	32	16	8	4	2	1
0 →	0	0	0	0	0	0	0	0
128 →	1	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0

Result of above AND operation is zero (0) hence the first IP address is 172.16.0.0

- 3rd step: Number of subnetworks = $2^{(\text{number of stolen bits})}$

  $2^1 = 2$ subnets

- 4th step:
  Number of hosts per network= $2^{(\text{available bit} - \text{stolen bit})} - 2$

  In this case, available bits are addition of third and fourth octet.

  $= 2^{(16-1)}-2$
  $= 32{,}766$ hosts

subnet IP	172.16.0.0	172.16.128.0
1st valid host IP	172.16.0.1	172.16.128.1
last valid host	172.16.127.254	172.16.255.254
Broadcast IP	172.16.127.255	172.16.255.255

CONCLUSION

This article has discussed IP Subnetting as it is an important skill to acquire because it offers many benefits in any networked environment. Using the information in this paper, you should be able to subnet any network to take full advantage of the IP address space you utilize.

REFERENCES

[1]Y. Rekhter *et al.*, "Address Allocation for Private Intranets," IETF RFC 1918, Feb. 1996.
[2] BEHCET SARIKAYA, "Home agent placement and IP address management for integrating WLANS with cellular networks" 1536-1284/06/$20.00 © 2006 IEEE
[3] G. Montenegro, "Reverse Tunneling for Mobile IP," IETF RFC 3024, Jan. 2001.
[4] S. Vaarala *et al.*, "Mobile IPv4 Traversal Across IPSec based VPN Gateways," Internet draft, Nov. 2005; http://ietfreport.isoc.org/all-ids/draft-ietf-mip4-vpn-prob
lem-solution-02.txt
[5] Bolt Beranek and Newman, "Specification for the Interconnection of a Host and an IMP," BBN Technical Report 1822, Revised May 1978.
[6] Shoch, J., "Inter-Network Naming, Addressing, and Routing," COMPCON, IEEE Computer Society, Fall 1978.
[7] Postel, J., "Address Mappings," RFC 796, USC/Information Sciences Institute, September 1981.
[8] Shoch, J., "Packet Fragmentation in Inter-Network Protocols," Computer Networks, v. 3, n. 1, February 1979.

AUTHOR'S PROFILE

Shailesh N. Sisat is a master degree candidate in Electronics & Telecommunication Engineering of SGB Amravati University, Maharashtra, India. He received his B.E. degree in Electronics & Telecommunication Engineering from SGB Amravati University. He is Red Hat Certified Engineer having industrial experience in networking industry

Prajkta S. Bhopale is a master degree candidate in Electronics & Telecommunication Engineering of SGB Amravati University Maharashtra, India. She received her B.E. degree in Electronics & Telecommunication Engineering from SGB Amravati University.

Vishwajit K. Barbudhe is a professor in the Department of Electronics & Telecommunication Engineering, Agnihotri C.O.E. Wardha, Nagpur University, Maharashtra, India. He received his M.Tech degree in Electronics & communication Engineering from PIT C.O.E. RGPV University, MP, India. He received his B.E. degree in Electronics & Telecommunication Engineering from SGB Amravati University.