CHAPTER FOUR

Communication Network Protocols

Network Protocol Overview

Networking protocols define a common format and set of rules for exchanging messages between devices. There are two Internet protocols used to assign addresses to links on a host, Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6). The majority of current internets use IPv4.

Every device connected to the internet is assigned an IP address. This enables the identification and location of networked computers on the internet. There are two versions of internet protocol, i.e., internet protocol version 4 and internet protocol version 6. IP V6 is the newest version of the internet protocol suite as of now developed to replace the fourth version, the IPv4.

Differences between IPv4 and IPv6

- IPv6 has packet flow identification in the header while IPv4 offers no packet flow information.
- IPv6 uses 128-bit hexadecimal, i.e., base 16 IP addresses, while IPv4 uses 32-bit IP addresses written in a decimal number system which is a base 10.
- IPv4 supports dynamic host configuration protocol setup, while IPv6 supports renumbering address setup.
- IPv4 has no connection integrity, whereas IPv6 has end-to-end connection integrity.
- IPv4 uses the decimal representation of addresses, while IPv6 uses hexadecimal representation.

Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP). Communication between a web server and web client is an example of an interaction between several protocols:

- HTTP - an application protocol that governs the way a web server and a web client interact.
- TCP - transport protocol that manages the individual conversations.
- IP – encapsulates the TCP segments into packets, assigns addresses, and delivers to the destination host.
- Ethernet - allows communication over a data link and the physical transmission of data.

A protocol suite is a set of protocols that work together to provide comprehensive network communication services.

The TCP/IP protocol suite is an open standard, the protocols are freely available, and any vendor is able to implement these protocols on their hardware or in their software's the network media.

Computer Network Addressing

In the internet employing TCP/IP protocol, we have four levels of addresses being in use for different layers.

- Physical address
- Logical address (IP)
- Port address and
- Specific address

1. MAC Addresses (Physical Address):

It is further included inside the frame which is utilized by the DLL (data link layer) of OSI model. It is the bottom-most layer (bottom-most address in OSI model) address. The Ethernet (LAN) uses a 48-bit (6-byte) physical address which is normally produced in the network interfacing card (NIC). A MAC address is most often represented in hexadecimal, using one of two accepted formats: 00:43: AB: F2:32:13 or 0043.ABF2.3213

2. Logical Address (IP Addresses):

Logical addressing is a function of the Network layer of the OSI Model (Layer-3), and provides a hierarchical structure to separate networks. A logical address contains two components:

- Network ID – identifies which network a host belongs to.
- Host ID – uniquely identifies the host on that network.

The logical address is also called the IP (Internet Protocol) address. The logical address used on the internet is currently a 32-bit address.

3. Port Address:

The IP and Physical address are essential for any level of data traveling from the certain specific source to the destination host that is required. But in today's modern computers, we may require to run multiple processes on it simultaneously. Let us suppose a computer says 'A' first initiate communication with another computer named 'C' by using TELNET. Further, consider now, the same computer 'A' communicates with any computer 'B' simultaneously by means of the File Transfer Protocol (FTP).

The main objective of the internet is the process to process communications. For this purpose, it is necessary to label or name a specific process. Thus the process needs addresses. The label that is allocated to a process is known as the port address. It is a 16 bit address field. The physical addresses change for each and every trip a packet takes, but the logical and port addresses basically will remain as it is.

4. Specific Addresses:

A few of the applications generally have simple (easy to use) address. Examples of specific addresses are the e-mail addresses of the University Resource Locators (URL). Examples mainly consist of the email address (cs@gmail.com) and the Universal Resource Locator (URL), example (**www.gmail.com**).

IP Addressing and Subnetting

Internet Protocol (IP)

IP provides two fundamental Network layer services:

- Logical addressing – provides a unique address that identifies both the host, and the network that host exists on.
- Routing – determines the best path to a particular destination network, and then routes data accordingly.

IPv4 employs a 32-bit address, which limits the number of possible addresses to 4,294,967,296. IPv4 will eventually be replaced by IP Version 6 (IPv6), due to a shortage of available IPv4 addresses.

IPv4 Addressing

A core function of IP is to provide logical addressing for hosts. An IP address provides a hierarchical structure to both uniquely identify a host, and what network that host exists on. An IP address is most often represented in decimal (ex.:- 158.80.164.3). An IP address is comprised of four octets, separated by periods:

First Octet	Second Octet	Third Octet	Fourth Octet
158	80	164	3

Each octet is an 8-bit number, resulting in a 32-bit IP address. The smallest possible value of an octet is 0, or 00000000 in binary. The largest possible value of an octet is 255, or 11111111 in binary.

The above IP address represented in binary would look as follows:

First Octet	Second Octet	Third Octet	Fourth Octet
10011110	01010000	10100100	00000011

The Subnet Mask

Part of an IP address identifies the network. The other part of the address identifies the host.

A subnet mask is required to provide this distinction: 158.80.164.3 255.255.0.0

The above IP address has a subnet mask of 255.255.0.0. The subnet mask follows two rules:

- If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies the network.
- If a binary bit is set to a 0 (or off) in a subnet mask, the corresponding bit in the address identifies the host.

Looking at the above address and subnet mask in binary:

IP Address: 10011110.01010000.10100100.00000011

Subnet Mask: 11111111.11111111.00000000.00000000

The first 16 bits of the subnet mask are set to 1. Thus, the first 16 bits of the address (158.80) identify the network. The last 16 bits of the subnet mask are set to 0. Thus, the last 16 bits of the address (164.3) identify the unique host on that network.

The network portion of the subnet mask must be contiguous. For example, a subnet mask of 255.0.0.255 is not valid.

IP Address Classes

The IPv4 address space has been structured into several classes. The value of the first octet of an address determines the class of the network:

Class	*First Octet Range*	*Default Subnet Mask*
Class A	1 - 127	255.0.0.0
Class B	128 - 191	255.255.0.0
Class C	192 - 223	255.255.255.0
Class D	224 - 239	-
Class E	240-255	-

Class A networks range from 1 to 127. The *default* subnet mask is 255.0.0.0. Thus, by *default,* the first octet defines the network, and the last three octets define the host. This results in a maximum of 127 Class A networks, with 16,777,214 hosts per network!

Example of a Class A address:

Address:	64.32.254.100
Subnet Mask:	255.0.0.0

Class B networks range from 128 to 191. The *default* subnet mask is 255.255.0.0. Thus, by *default*, the first two octets define the network, and the last two octets define the host. This results in a maximum of 16,384 Class B networks, with 65,534 hosts per network.

Example of a Class B address:

Address:	152.41.12.195
Subnet Mask:	255.255.0.0

Class C networks range from 192 to 223. The default subnet mask is 255.255.255.0. Thus, by *default*, the first three octets define the network, and the last octet defines the host. This results in a maximum of 2,097,152 Class C networks, with 254 hosts per network.

Example of a Class C address:

Address:	207.79.233.6
Subnet Mask:	255.255.255.0

Class D networks are reserved for multicast traffic. Class D addresses do not use a subnet mask.

Class E networks are reserved for research and experimental use.

CIDR (Classless Inter-Domain Routing).

Classless Inter Domain Routing (CIDR) is a method for assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C. It is a newer addressing scheme for IP Networks which allows for a more efficient allocation of IP addresses than the older method which was by assigning organizations a class of IPs.

For example, rather than assigning a Class C block, you can use a network prefix of 27 bits and assign the block of 32 IP Addresses. This allows for address assignments that can better fit an organization's specific needs with very little waste of IP addresses. CIDR and subnetting is virtually the same thing. The term **Subnetting** is generally used when you use it at the organizational level. CIDR is generally used when you it at the **ISP** level or higher.

- Classless Inter-Domain Routing (CIDR) is a simplified method of representing a subnet mask.
- It identifies the number of binary bits set to a 1 (or on) in a subnet mask, preceded by a slash.
- For example, a subnet mask of 255.255.255.240 would be represented as follows in binary:
- 11111111.11111111.11111111.11110000

- The first 28 bits of the above subnet mask are set to 1.
- The CIDR notation for this subnet mask would thus be /28.

The CIDR mask is often appended to the IP address.

For example, an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0 would be represented as follows using CIDR notation:

192.168.1.1 /24

CIDR is also superneting in contrast to subnetting.

- **Subnetting** is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network and reduces the size of the broadcast domain. In subnetting, a single big network is divided into multiple smaller subnetworks.
- **Supernetting** is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

Difference between Subnetting and Supernetting

S.NO	Subnetting		Supernetting
1.	Subnetting is the procedure to divide the network into sub-networks.		While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network addresses's bits are increased.		While in supernetting, Host addresses's bits are increased.
3.	In subnetting, The mask bits are moved towards right.		While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.		While supernetting is implemented via Classless interdomain routing.
SS5.	In subnetting, Address depletion is reduced or removed.		While It is used for simplify routing process.

Address Classes vs. Subnet Mask

Remember the following three rules:

- The first octet on an address dictates the class of that address.
- The subnet mask determines what part of an address identifies the network, and what part identifies the host.
- Each class has a default subnet mask. A network using its default subnet mask is referred to as a classful network.

For example, 10.1.1.1 is a Class A address, and its default subnet mask is 255.0.0.0 (/8 in CIDR).

It is entirely possible to use subnet masks other than the default. For example, a Class B subnet mask can be applied to a Class A address: 10.1.1.1 /16

However, this does not change the class of the above address. It remains a Class A address, which has been subnetted using a Class B mask. Remember, the only thing that determines the class of an IP address is the first octet of that address. Likewise, the subnet mask is the only thing that determines what part of an address identifies the network, and what part identifies the host.

Subnet and Broadcast Addresses

On each IP network, two host addresses are reserved for special use:

- The subnet (or network) address
- The broadcast address

Neither of these addresses can be assigned to an actual host. The subnet address is used to identify the network itself. A routing table contains a list of known networks, and each network is identified by its subnet address. Subnet addresses contain all 0 bits in the host portion of the address.

For example, 192.168.1.0/24 is a subnet address. This can be determined by looking at the address and subnet mask in binary:

- IP Address: 11000000.10101000.00000001.00000000
- Subnet Mask: 11111111.11111111.1 1111111.00000000

Note that all host bits in the address are set to 0.

The broadcast address identifies all hosts on a particular network. A packet sent to the broadcast address will be received and processed by every host on that network. Broadcast addresses contain all 1 bits in the host portion of the address.

For example, 192.168.1.255/24 is a broadcast address. Note that all host bits are set to 1:

- IP Address: 11000000.10101000.00000001.11111111
- Subnet Mask: 11111111.11111111.11111111.00000000

Broadcasts are one of three types of IP packets:

• Unicasts are packets sent from one host to one other host

• Multicasts are packets sent from one host to a group of hosts

• Broadcasts are packets sent from one host to all other hosts on the local network

A router, by default, will never forward a multicast or broadcast packet from one interface to another.

A switch, by default, will forward a multicast or broadcast packet out every port, except for the port that originated the multicast or broadcast.

Subnetting

Subnetting is the process of creating new networks (or subnets) by borrowing bits from the host portion of a subnet mask. There is one caveat: borrowing bits from hosts creates more networks but fewer hosts per network.

Consider the following Class C network:

192.168.254.0

The default subnet mask for this network is 255.255.255.0. This single network can be segmented, or subnetted, into multiple networks. For example, assume a minimum of 10 new networks are required. Resolving this is possible using the following magical formula:

2^{n} the exponent 'n' identifies the number of bits to borrow from the host portion of the subnet mask.

The default Class C mask (255.255.255.0) looks as follows in binary:

11111111.1111111.1111111.00000000

There are a total of 24 bits set to 1, which are used to identify the network.

There are a total of 8 bits set to 0, which are used to identify the host, and these host bits can be borrowed.

Borrowed bits essentially involves changing host bits (set to 0 or off) in the subnet mask to network bits (set to 1 or on). Remember, network bits in a subnet mask must always be contiguous - skipping bits is not allowed.

Consider the result if three bits are borrowed. Using the above formula:

- $2^{n}= 2^{3}= 8 = 8$ new networks created
- However, a total of 8 new networks do not meet the original requirement of at least 10 networks. Consider the result if four bits are borrowed:
  - $2^{n}= 2^{4}= 16 = 16$ new networks created
- A total of 16 new networks does meet the original requirement. Borrowing four host bits results in the following new subnet mask:
  - 11111111.11111111.11111111.11110000 = 255.255.255.240

In the previous example, a Class C network was subnetted to create 16 new networks, using a subnet mask of 255.255.255.240 (or /28 in CIDR). Four bits were borrowed in the subnet mask, leaving only four bits for hosts.

To determine the number of hosts this results in, for each of the new 16 networks, a slightly modified formula is required:

- $2^n - 2$ where n is remaining host bit.

Consider the result if four bits are available for hosts:

- $2^n - 2 = 2^4 - 2 = 16 - 2 = 14$ usable hosts per network. Thus, subnetting a Class C network with a /28 mask creates 16 new networks, with 14 usable hosts per network.

Why is the formula for calculating usable hosts $2^n - 2$? Because it is never possible to assign a host an address with all 0 or all 1 bits in the host portion of the address. These are reserved for the subnet and broadcast addresses, respectively. Thus, every time a network is subnetted, useable host addresses are lost.

- The 2^n-2 Rule and Subnetted Networks

To avoid confusion, it was historically unacceptable to use the first and last new networks created when subnetting, as it is possible for a classful network to have the same subnet and broadcast address as its subnetted networks. This required the $2^n - 2$ formula to also be used when calculating the number of new networks created while subnetting. Remember though, the formula for calculating usable hosts is always $2^n - 2$.

Determining the Range of Subnetted Networks

Determining the range of the newly created networks can be accomplished using several methods.

- The long method involves some binary magic.
- How to Calculate Subnets
- Subnets and Hosts

Borrow 2 bits

S	S	H	H	H	H	H	H

# of subnets = $2^2 = 4$

Subnet mask = 2 bits = 128 + 64 = 192

Range of hosts =$2^{rhb} = 2^6 = 64$, where **rhb** is remaining host bit.

IP Address	Range	Useable Range	Network address	Broadcast Address
192.168.254.0	0 – 63	1- 62	192.168.254..0	192.168.254..63 .63
	64 – 127	65 – 126	192.168.254..64	192.168.254..127
	128 – 191	129 – 190	192.168.254..128	192.168.254..191
	192 – 255	193- 254	192.168.254..192	192.168.254..255

Consider the example 192.168.254.0 network again, which was subnetted using a 255.255.255.240 mask:

- 192.168.254.0: 11000000.10101000.11111110.00000000
- 255.255.255.240: 11111111.11111111.11111111.11110000

Subnetting borrowed four bits in the fourth octet, creating a total of 16 new networks. Looking at only the fourth octet, the first newly created network is 0000. The second new network is 0001. Calculating all possible permutations of the four borrow bits:

Calculating the ranges of subnetted networks can quickly become tedious when using the long binary method.

- The shortcut method involves taking the subnet mask (255.255.255.240 from the previous example), and subtracting the subnetted octet (240) from 256.
- 256 – 240 = 16

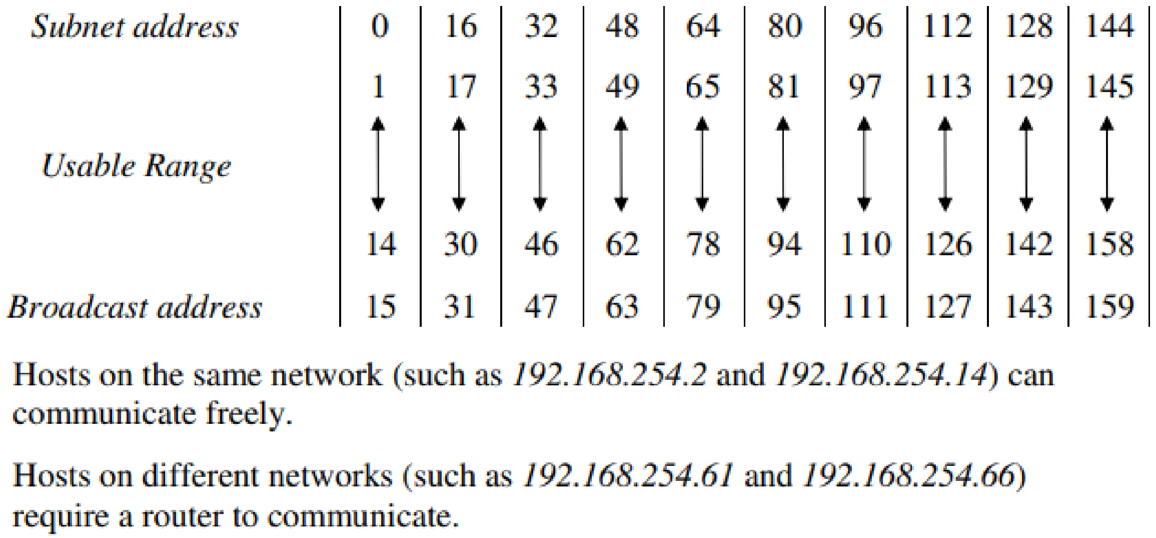
Assuming ip subnet-zero is enabled; the first network will begin at 0. Then, simply continue adding 16 to identify the first address of each new network:

- 0 16 32 48 64 80 96 112 128 144 160 176 192 208 224 240

Knowing the first address of each new network makes it simple to determine the last address of each network:

- First address of network 0 16 32 48 64 80 96 112 128 144
- Last address of network 15 31 47 63 79 95 111 127 143 159
  - Only the first 10 networks were calculated, for brevity. The first address of each network becomes the subnet address for that network.

- The last address of each network becomes the broadcast address for that network.
- Once the first and last address of each network is known, determining the usable range for hosts is straightforward:



Subnet address	0	16	32	48	64	80	96	112	128	144
	1	17	33	49	65	81	97	113	129	145
Usable Range	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	14	30	46	62	78	94	110	126	142	158
Broadcast address	15	31	47	63	79	95	111	127	143	159

Hosts on the same network (such as *192.168.254.2* and *192.168.254.14*) can communicate freely.

Hosts on different networks (such as *192.168.254.61* and *192.168.254.66*) require a router to communicate.

variable-length subnet mask (VLSM)

Variable-Length Subnet Masking (VLSM) amounts to subnetting subnets, which means that VLSM allows network engineers to divide an IP address space into a hierarchy of subnets of different sizes, making it possible to create subnets with very different host counts without wasting large numbers of addresses.

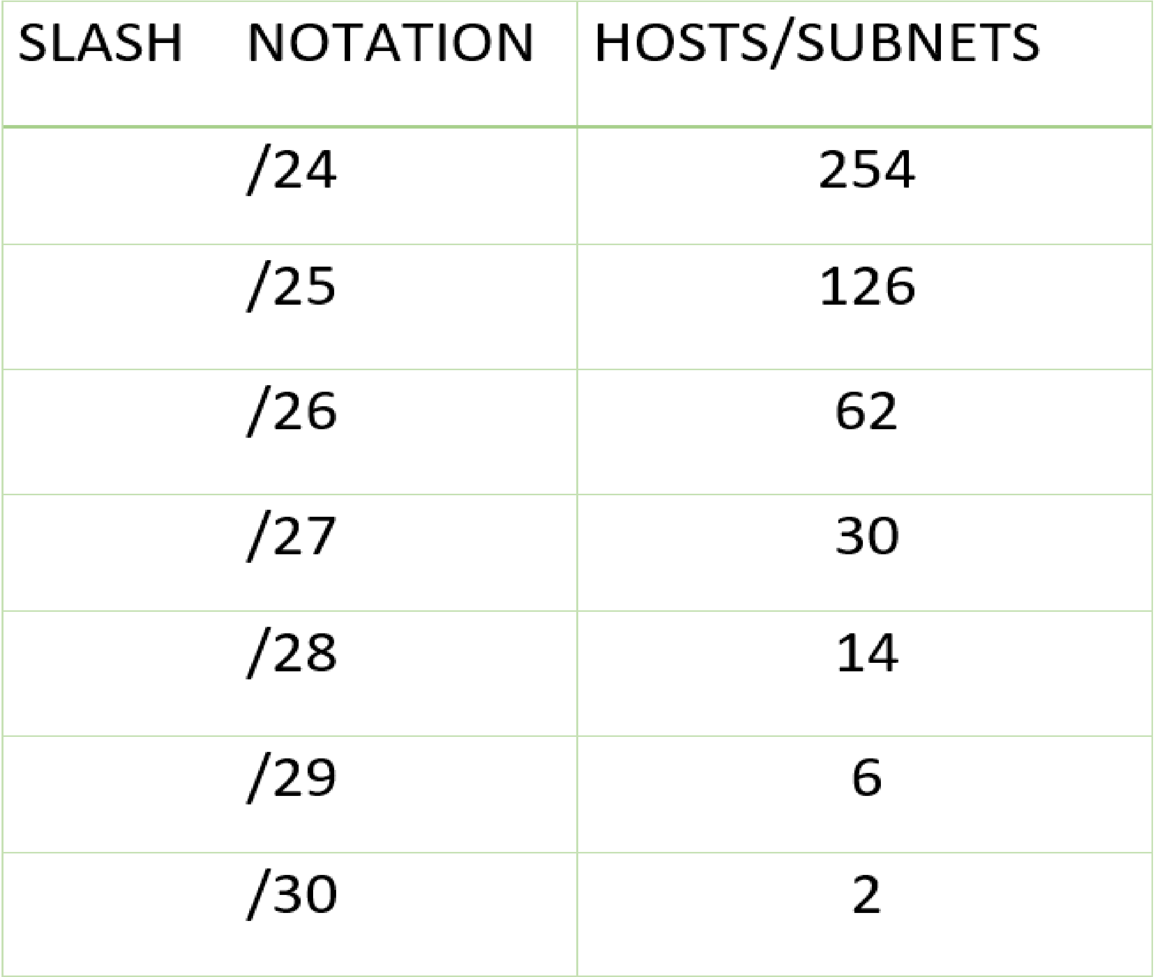
The subnet design uses more than one mask in the same network which means more than one mask is used for different subnets of a single class A, B, C or a network. It is used to increase the usability of subnets as they can be of variable size.

Fixed-Length Subnet Masking (FLSM) creates subnets all the same size. But where some subnets will have many hosts and some have few, FLSM results in some subnets having many orphaned addresses, or some sets of hosts being too big to fit into a subnet. Where VLSM is enabled, a large subnet can be divided into a set of smaller sub-subnets, which can be used to handle smaller sets of hosts.

Procedure of implementing VLSM

- In VLSM, subnets use block size based on requirement so subnetting is required multiple times.
  - Suppose there is an administrator that has four departments to manage. These are CS with 120 computers, IT with 50 computers, SW with 26 computers and IS department with 5 computers.
  - If the administrator has IP 192.168.1.0/24, department wise IPs can be allocated by following these steps:

1. For each segment select the block size that is greater than or equal to the actual requirement which is the sum of host addresses, broadcast addresses and network addresses. Make a list of subnets possible:



SLASH NOTATION	HOSTS/SUBNETS
/24	254
/25	126
/26	62
/27	30
/28	14
/29	6
/30	2

Table: - possible subnets list

2. Arrange all the segments in descending order based on the block size that is from highest to lowest requirement.
   - ✓ CS: 120
   - ✓ IT: 50
   - ✓ SW: 26
   - ✓ IS: 5
3. The highest IP available has to be allocated to highest requirement so the CS department gets 192.168.1.0/25 which has 126 valid addresses that can easily be available for 120 hosts. The subnet mask used is 255.255.255.128

4. The next segment requires an IP to handle 50 hosts. The IP subnet with network number 192.168.1.128/26 is the next highest which can be assigned to 62 hosts thus fulfilling the requirement of IT. The subnet mask used is 255.255.255.192.
5. Similarly the next IP subnet 192.168.1.192/27 can fulfill the requirements of SW department as it has 30 valid hosts IP which can be assigned to 26 computers. The mask used is 255.255.255.224
6. The last segment requires 5 valid hosts IP which can be fulfilled by the subnet 192.168.1.224/29 which has the mask as 255.255.255.248 is chosen as per the requirement. The IP with the mask 255.255.255.240 could be chosen but it has 14 valid hosts IPs and the requirement is less in comparison so the one that is comparable with the requirement is chosen. Thus there is less IP wastage in VLSM as compared to FLSM.

Advantages of VLSM over FLSM

- In Fixed length subnet mask subnetting (FLSM), all subnets are of equal size and have equal number of hosts but in VLSM the size is variable and it can have variable number of hosts thus making the IP addressing more efficient by allowing a routed system of different mask length to suit requirements.
- In FLSM there is wastage of IP addresses but in VLSM there is a minimum wastage of IP addresses.
- FLSM is preferred for private IP addresses while for public IP addresses VLSM is the best option.

Private vs. Public IPv4 Addresses

The rapid growth of the Internet resulted in a shortage of available IPv4 addresses. In response, a specific subset of the IPv4 address space was designated as private, to temporarily alleviate this problem.

A public address can be routed on the Internet. Thus, hosts that must be Internet-accessible must be configured with (or reachable by) public addresses. Allocation of public addresses is governed by the Internet Assigned Numbers Authority (IANA).

A private address is intended for internal use within a home or organization, and can be freely used by anyone. However, private addresses can never be routed on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses. Three private address ranges were defined in RFC 1918, one for each IPv4 class:

- ✓ Class A 10.0.0.0 – 10.255.255.255 (10.0.0.0/8),
- ✓ Class B 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)

- ✓ Class C 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)

By universally recognizing these ranges as private and non-routable in the Internet, multiple organizations can use these ranges internally without causing a conflict with public Internet addresses

It is possible to translate between private and public addresses, using Network Address Translation (NAT). It allows a host configured with a private address to be stamped with a public address, thus allowing that host to communicate across the Internet.

It is also possible to translate multiple privately-addressed hosts to a single public address, which conserves the public address space.

NAT provides an additional benefit – hiding the specific addresses and addressing structure of the internal (or private) network.

> Note: NAT is not restricted to private-to-public address translation, though that is the most common application.

NAT is only a temporarily solution to the address shortage problem. IPv4 will eventually be replaced with IPv6, which supports a vast address space.

Reserved IPv4 Addresses

In addition to the three private IPv4 ranges, several other addresses and ranges are reserved for specific purposes:

- ✓ The 0.0.0.0 /0 network is used to identify all networks, and is referred to as the default route.
- ✓ The 0.0.0.0 /8 ranges are used to identify hosts on the local network.
- ✓ The entire 127.x.x.x /8 range is reserved for diagnostic purposes. The most commonly used address in this range is 127.0.0.1, which identifies the local host, and is referred to as the loopback or localhost address.
- ✓ The 169.254.x.x /16 range is reserved for Automatic Private IP Addressing (APIPA). A host assigns itself an address in this range, if it cannot dynamically obtain an address from a DHCP server.
- ✓ The 224.x.x.x – 239.x.x.x ranges are reserved for multicast, and are referred to as Class D addresses.
- ✓ The 240.x.x.x – 255.x.x.x ranges are reserved for future and experimental use, and were formerly referred to as Class E addresses.
- ✓ The 255.255.255.255 address can be used as a broadcast address for the local network.