IPv4 - Overview

This era is said to be the era of computers. Computers have significantly changed the way we live. A computing device when connected to other computing device(s) enables us to share data and information at lightning fast speed.

What is Network?

A Network in the world of computers is said to be a collection of interconnected hosts, via some shared media which can be wired or wireless. A computer network enables its hosts to share and exchange data and information over the media. Network can be a Local Area Network spanned across an office or Metro Area Network spanned across a city or Wide Area Network which can be spanned across cities and provinces.

A computer network can be as simple as two PCs connected together via a single copper cable or it can be grown up to the complexity where every computer in this world is connected to every other, called the Internet. A network then includes more and more components to reach its ultimate goal of data exchange. Below is a brief description of the components involved in computer network −

* **Hosts** − Hosts are said to be situated at ultimate end of the network, i.e. a host is a source of information and another host will be the destination. Information flows end to end between hosts. A host can be a user’s PC, an internet Server, a database server etc.
* **Media** − If wired, then it can be copper cable, fiber optic cable, and coaxial cable. If wireless, it can be free-to-air radio frequency or some special wireless band. Wireless frequencies can be used to interconnect remote sites too.
* **Hub** − A hub is a multiport repeater and it is used to connect hosts in a LAN segment. Because of low throughputs hubs are now rarely used. Hub works on Layer-1 (Physical Layer) of OSI Model.
* **Switch** − A Switch is a multiport bridge and is used to connect hosts in a LAN segment. Switches are much faster than Hubs and operate on wire speed. Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches are also available.
* **Router** − A router is Layer-3 (Network Layer) device which makes routing decisions for the data/information sent for some remote destination. Routers make the core of any interconnected network and the Internet.
* **Gateways** − A software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data.
* **Firewall** − Software or combination of software and hardware, used to protect users data from unintended recipients on the network/internet.

All components in a network ultimately serve the hosts.

Host Addressing

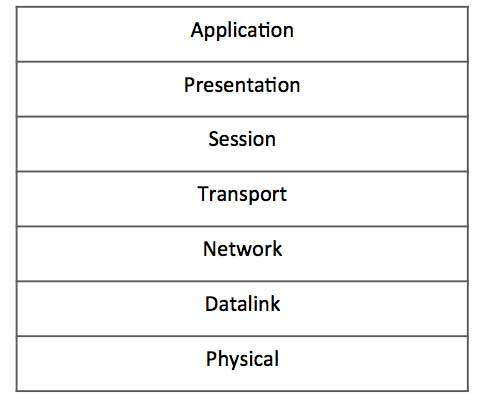
Communication between hosts can happen only if they can identify each other on the network. In a single collision domain (where every packet sent on the segment by one host is heard by every other host) hosts can communicate directly via MAC address.

MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host. But if a host wants to communicate with a remote host, i.e. not in the same segment or logically not connected, then some means of addressing is required to identify the remote host uniquely. A logical address is given to all hosts connected to Internet and this logical address is called **Internet Protocol Address**.

IPv4 - OSI Model

The International Standard Organization has a well-defined model for Communication Systems known as Open System Interconnection, or the OSI Model. This layered model is a conceptualized view of how one system should communicate with the other, using various protocols defined in each layer. Further, each layer is designated to a well-defined part of communication system. For example, the Physical layer defines all the components of physical nature, i.e. wires, frequencies, pulse codes, voltage transmission etc. of a communication system.

The OSI Model has the following seven layers −



* **Application Layer (Layer-7)** − This is where the user application sits that needs to transfer data between or among hosts. For example − HTTP, file transfer application (FTP) and electronic mail etc.
* **Presentation Layer (Layer-6)** − This layer helps to understand data representation in one form on a host to other host in their native representation. Data from the sender is converted to on-the-wire data (general standard format) and at the receiver’s end it is converted to the native representation of the receiver.
* **Session Layer (Layer-5)** − This layer provides session management capabilities between hosts. For example, if some host needs a password verification for access and if credentials are provided then for that session password verification does not happen again. This layer can assist in synchronization, dialog control and critical operation management (e.g., an online bank transaction).
* **Transport Layer (Layer-4)** − This layer provides end to end data delivery among hosts. This layer takes data from the above layer and breaks it into smaller units called Segments and then gives it to the Network layer for transmission.
* **Network Layer (Layer-3)** − This layer helps to uniquely identify hosts beyond the subnets and defines the path which the packets will follow or be routed to reach the destination.
* **Data Link Layer (Layer-2)** − This layer takes the raw transmission data (signal, pulses etc.) from the Physical Layer and makes Data Frames, and sends that to the upper layer and vice versa. This layer also checks any transmission errors and sorts it out accordingly.
* **Physical Layer (Layer-1)** − This layer deals with hardware technology and actual communication mechanism such as signaling, voltage, cable type and length, etc.

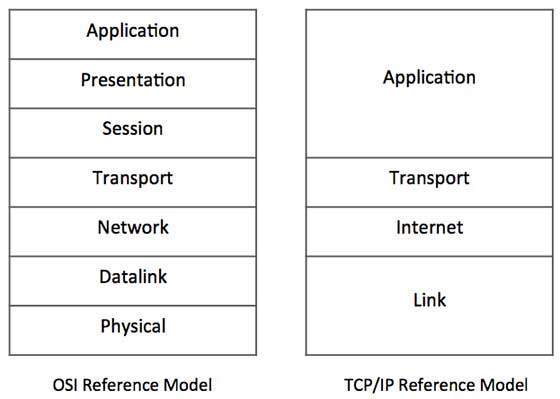
Network Layer

The network layer is responsible for carrying data from one host to another. It provides means to allocate logical addresses to hosts, and identify them uniquely using the same. Network layer takes data units from Transport Layer and cuts them in to smaller unit called Data Packet.

Network layer defines the data path, the packets should follow to reach the destination. Routers work on this layer and provides mechanism to route data to its destination.

IPv4 - TCP/IP Model

A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite. This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because the two major protocols in this suites are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite. This protocol suite has its own reference model which it follows over the internet. In contrast with the OSI model, this model of protocols contains less layers.



**Figure** − Comparative depiction of OSI and TCP/IP Reference Models

This model is indifferent to the actual hardware implementation, i.e. the physical layer of OSI Model. This is why this model can be implemented on almost all underlying technologies. Transport and Internet layers correspond to the same peer layers. All three top layers of OSI Model are compressed together in single Application layer of TCP/IP Model.

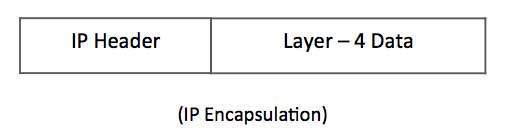
Internet Protocol Version 4 (IPv4)

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 based upon their logical addresses and to route data among them over the underlying network.

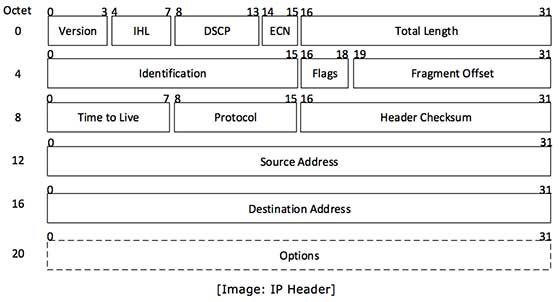
IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.

IPv4 - Packet Structure

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.



The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows −

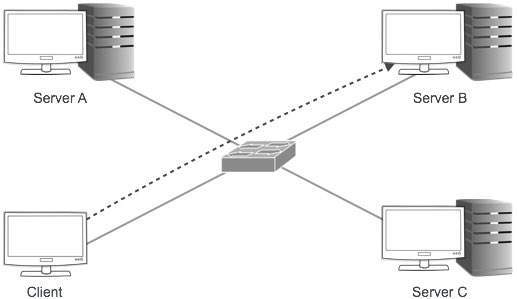
* **Version** − Version no. of Internet Protocol used (e.g. IPv4).
* **IHL** − Internet Header Length; Length of entire IP header.
* **DSCP** − Differentiated Services Code Point; this is Type of Service.
* **ECN** − Explicit Congestion Notification; It carries information about the congestion seen in the route.
* **Total Length** − Length of entire IP Packet (including IP header and IP Payload).
* **Identification** − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
* **Flags** − As required by the network resources, if IP Packet is too large to handle, these ‘flags’ tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to ‘0’.
* **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet.
* **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
* **Protocol** − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
* **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
* **Source Address** − 32-bit address of the Sender (or source) of the packet.
* **Destination Address** − 32-bit address of the Receiver (or destination) of the packet.
* **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPv4 - Addressing

IPv4 supports three different types of addressing modes. −

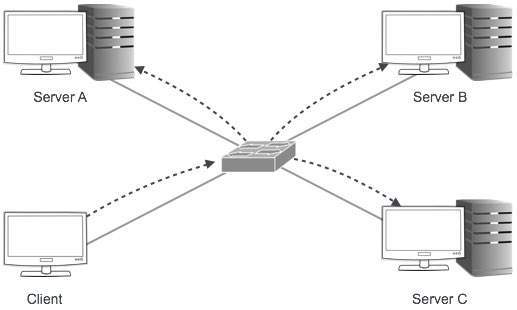
Unicast Addressing Mode

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server −



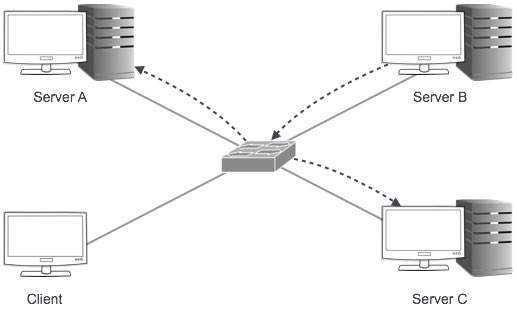
Broadcast Addressing Mode

In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers −



Multicast Addressing Mode

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

Hierarchical Addressing Scheme

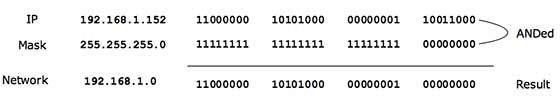
IPv4 uses hierarchical addressing scheme. An IP address, which is 32-bits in length, is divided into two or three parts as depicted −



A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables the IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

Subnet Mask

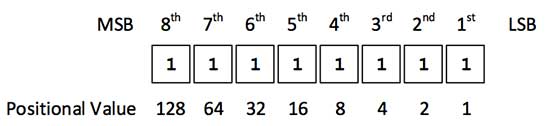
The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then −



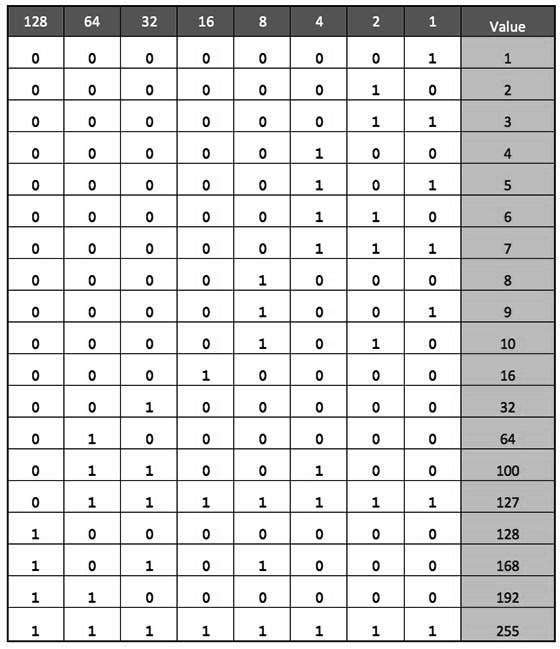
This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

Binary Representation

The positional value method is the simplest form of converting binary from decimal value. IP address is 32 bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of each bit can be determined by the position of bit value '1' in the octet.



Positional value of bits is determined by 2 raised to power (position – 1), that is the value of a bit 1 at position 6 is 2^(6-1) that is 2^5 that is 32. The total value of the octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below −

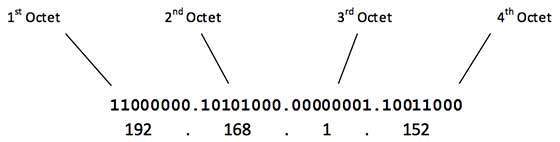


IPv4 - Address Classes

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address −



The number of networks and the number of hosts per class can be derived by this formula −



When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

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.

Class A Addresses

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 IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

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.

Class B Addresses

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

Class C Address

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

Class C Addresses

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.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of −

Class D Addresses

Class D has IP address range 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.

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.

IPv4 - Subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

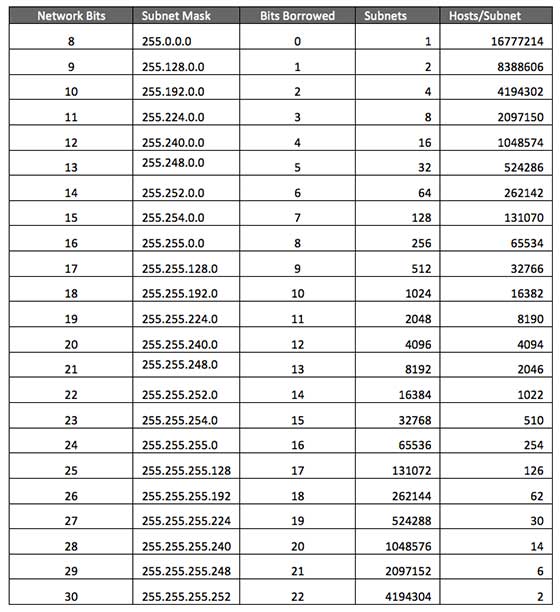
CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (21=2) with (223-2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets −



In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

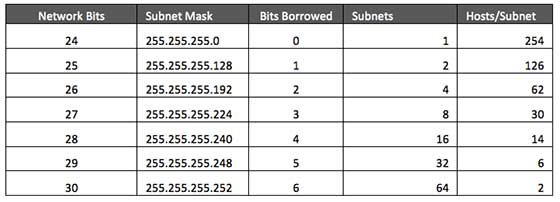
Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (214) 16384 Networks and (216-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting −



Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address −



IPv4 - VLSM

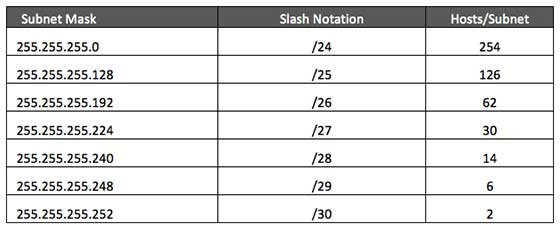
Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step - 1

Make a list of Subnets possible.



Step - 2

Sort the requirements of IPs in descending order (Highest to Lowest).

* Sales 100
* Purchase 50
* Accounts 25
* Management 5

Step - 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step - 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step - 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step - 6

Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

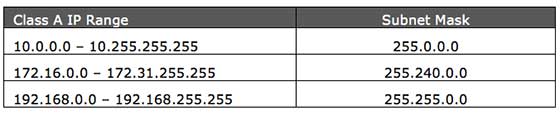
By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used CIDR.

IPv4 - Reserved Addresses

There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.

Private IP Addresses

Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.



In order to communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.

The sole purpose to create a separate range of private addresses is to control assignment of already-limited IPv4 address pool. By using a private address range within LAN, the requirement of IPv4 addresses has globally decreased significantly. It has also helped delaying the IPv4 address exhaustion.

IP class, while using private address range, can be chosen as per the size and requirement of the organization. Larger organizations may choose class A private IP address range where smaller organizations may opt for class C. These IP addresses can be further sub-netted and assigned to departments within an organization.

Loopback IP Addresses

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host’s self-address, also known as localhost address. This loopback IP address is managed entirely by and within the operating system. Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine. Other than that, if a host machine can successfully ping 127.0.0.1 or any IP from loopback range, implies that the TCP/IP software stack on the machine is successfully loaded and working.

Link-local Addresses

In case a host is not able to acquire an IP address from the DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses. Link local address ranges from 169.254.0.0 -- 169.254.255.255.

Assume a network segment where all systems are configured to acquire IP addresses from a DHCP server connected to the same network segment. If the DHCP server is not available, no host on the segment will be able to communicate to any other. Windows (98 or later), and Mac OS (8.0 or later) supports this functionality of self-configuration of Link-local IP address. In absence of DHCP server, every host machine randomly chooses an IP address from the above mentioned range and then checks to ascertain by means of ARP, if some other host also has not configured itself with the same IP address. Once all hosts are using link local addresses of same range, they can communicate with each other.

These IP addresses cannot help system to communicate when they do not belong to the same physical or logical segment. These IPs are also not routable.

IPv4 - Example

This chapter describes how actual communication happens on the Network using Internet Protocol version 4.

Packet Flow in Network

All the hosts in IPv4 environment are assigned unique logical IP addresses. When a host wants to send some data to another host on the network, it needs the physical (MAC) address of the destination host. To get the MAC address, the host an broadcasts ARP message and asks to give the MAC address whoever is the owner of destination IP address. All the hosts on that segment receive the ARP packet, but only the host having its IP matching with the one in the ARP message, replies with its MAC address. Once the sender receives the MAC address of the receiving station, data is sent on the physical media.

In case the IP does not belong to the local subnet, the data is sent to the destination by means of Gateway of the subnet. To understand the packet flow, we must first understand the following components −

* **MAC Address** − Media Access Control Address is 48-bit factory hard coded physical address of network device which can uniquely be identified. This address is assigned by device manufacturers.
* **Address Resolution Protocol** − Address Resolution Protocol is used to acquire the MAC address of a host whose IP address is known. ARP is a Broadcast packet which is received by all the host in the network segment. But only the host whose IP is mentioned in ARP responds to it providing its MAC address.
* **Proxy Server** − To access the Internet, networks use a Proxy Server which has a public IP assigned. All the PCs request the Proxy Server for a Server on the Internet. The Proxy Server on behalf of the PCS sends the request to the server and when it receives a response from the Server, the Proxy Server forwards it to the client PC. This is a way to control Internet access in computer networks and it helps to implement web based policies.
* **Dynamic Host Control Protocol** − DHCP is a service by which a host is assigned IP address from a pre-defined address pool. DHCP server also provides necessary information such as Gateway IP, DNS Server Address, lease assigned with the IP, etc. By using DHCP services, a network administrator can manage assignment of IP addresses at ease.
* **Domain Name System** − It is very likely that a user does not know the IP address of a remote Server he wants to connect to. But he knows the name assigned to it, for example, tutorialpoints.com. When the user types the name of a remote server he wants to connect to, the localhost behind the screens sends a DNS query. Domain Name System is a method to acquire the IP address of the host whose Domain Name is known.
* **Network Address Translation** − Almost all PCs in a computer network are assigned private IP addresses which are not routable on the Internet. As soon as a router receives an IP packet with a private IP address, it drops it. In order to access servers on public private address, computer networks use an address translation service, which translates between public and private addresses, called Network Address Translation. When a PC sends an IP packet out of a private network, NAT changes the private IP address with public IP address and vice versa.

We can now describe the packet flow. Assume that a user wants to access www.TutorialsPoint.com from her personal computer. She has internet connection from her ISP. The following steps will be taken by the system to help her reach the destination website.

Step 1 – Acquiring an IP Address (DHCP)

When the user’s PC boots up, it searches for a DHCP server to acquire an IP address. For the same, the PC sends a DHCPDISCOVER broadcast which is received by one or more DHCP servers on the subnet and they all respond with DHCPOFFER which includes all the necessary details such as IP, subnet, Gateway, DNS, etc. The PC sends DHCPREQUEST packet in order to request the offered IP address. Finally, the DHCP sends DHCPACK packet to tell the PC that it can keep the IP for some given amount of time that is known as IP lease.

Alternatively, a PC can be assigned an IP address manually without taking any help from DHCP server. When a PC is well configured with IP address details, it can communicate other computers all over the IP enabled network.

Step 2 – DNS Query

When a user opens a web browser and types www.tutorialpoints.com which is a domain name and a PC does not understand how to communicate with the server using domain names, then the PC sends a DNS query out on the network in order to obtain the IP address pertaining to the domain name. The pre-configured DNS server responds to the query with IP address of the domain name specified.

Step 3 – ARP Request

The PC finds that the destination IP address does not belong to his own IP address range and it has to forward the request to the Gateway. The Gateway in this scenario can be a router or a Proxy Server. Though the Gateway’s IP address is known to the client machine but computers do not exchange data on IP addresses, rather they need the machine’s hardware address which is Layer-2 factory coded MAC address. To obtain the MAC address of the Gateway, the client PC broadcasts an ARP request saying "Who owns this IP address?" The Gateway in response to the ARP query sends its MAC address. Upon receiving the MAC address, the PC sends the packets to the Gateway.

An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data. It is important that source and destination MAC addresses change as they travel across the Internet (segment by segment) but source and destination IP addresses never change.

IPv4 - Summary

The Internet Protocol version 4 was designed to be allocated to approx. imately 4.3 billion addresses. At the beginning of Internet this was considered a much wider address space for which there was nothing to worry about.

The sudden growth in internet users and its wide spread use has exponentially increased the number of devices which needs real and unique IP to be able to communicate. Gradually, an IPS is required by almost every digital equipment which were made to ease human life, such as Mobile Phones, Cars and other electronic devices. The number of devices (other than computers/routers) expanded the demand for extra IP addresses, which were not considered earlier.

Allocation of IPv4 is globally managed by Internet Assigned Numbers Authority (IANA) under coordination with the Internet Corporation for Assigned Names and Numbers (ICANN). IANA works closely with Regional Internet Registries, which in turns are responsible for efficiently distributing IP addresses in their territories. There are five such RIRS. According to IANA reports, all the IPv4 address blocks have been allocated. To cope up with the situation, the following practices were being done −

* **Private IPs −** Few blocks of IPs were declared for private use within a LAN so that the requirement for public IP addresses can be reduced.
* **NAT −** Network address translation is a mechanism by which multiple PCs/hosts with private IP addresses are enabled to access using one or few public IP addresses.
* Unused Public IPs were reclaimed by RIRs.

Internet Protocol v6 (IPv6)

IETF (Internet Engineering Task Force) has redesigned IP addresses to mitigate the drawbacks of IPv4. The new IP address is version 6 which is 128-bit address, by which every single inch of the earth can be given millions of IP addresses.

Today majority of devices running on Internet are using IPv4 and it is not possible to shift them to IPv6 in the coming days. There are mechanisms provided by IPv6, by which IPv4 and IPv6 can co-exist unless the Internet entirely shifts to IPv6 −

* Dual IP Stack
* Tunneling (6to4 and 4to6)
* NAT Protocol Translation

# Variable Length Subnet Mask (VLSM) Tutorial

**To fully understand VLSM, we need to know the fundamentals. This tutorial explains what a subnet mask, subnetting, and supernetting is and how to implement.**

[**AMAKIRI WELEKWE**](https://www.comparitech.com/author/amakiri-welekwe/)**TECHNOLOGY ADVISOR | CYBERSECURITY EVANGELIST**

**UPDATED:** August 9, 2023

The exponential growth of the Internet in the last 30 years exposed shortcomings in the original IP protocol design. As the internet began to rapidly expand from its initial military network research status into commercial prominence, the demand for IP addresses (particularly in the class B space) skyrocketed.

Experts started to worry about the long-term scaling properties of classes A, B, and C IP address scheme, and began considering ways to modify IP assignment policy and routing protocols to accommodate the growth.

This led to the establishment of the Routing and Addressing (ROAD) group by the Internet Engineering Task Force (IETF) in the early 1990s to work out ways of restructuring the IP address space to increase its lifespan.

**The group according to**[**IETF RFC 4632**](https://tools.ietf.org/html/rfc4632)**identified three major problems:**

1. Exhaustion of the Class B network address space
2. Growth in internet routers’ routing tables beyond the capacity of current hardware and software.
3. Eventual exhaustion of the 32-bit IPv4 network address space

As a short to mid-term measure, the ROAD group proposed a solution to allow the use of “classless” IP assignment systems to slow the growth of global routing tables and to reduce the rate of consumption of IPv4 address space. This eventually gave birth to what we now know as Classless Inter-Domain Routing (CIDR), and Variable Length Subnet Mask (VLSM), which allows greater flexibility in the creation of sub-networks, overcoming the strict rules of the A, B, and C classes. In this guide, we’re going to help you understand the concept of VLSM, and show you how to implement VLSM Subnetting.

## VLSM Fundamentals

In order to fully grasp the concept of VLSM, we first need to understand the term **subnet mask**, [**subnetting**](https://www.comparitech.com/net-admin/subnetting-guide/)**,** and **Supernetting**.

### Subnet Mask

**Subnet masks** are used by a computer to determine if any computer is on the same network or on a different network. An IPv4 subnet mask is a 32-bit sequence of ones (1) followed by a block of zeros (0). The ones designate the network prefix, while the trailing block of zeros designates the host identifier. In shorthand, we use /24, which simply means that a subnet mask has 24 ones, and the rest are zeros.

| **Binary Notation** | **Decimal Notation** |  |
| --- | --- | --- |
| IP address | 11000000.00000000.00000010.10000010 | 192.0.2.130 |
| Subnet mask | 11111111.11111111.11111111.00000000 | 255.255.255.0 |

***Table 1.0*** IP address and subnet mask in binary and decimal format

### Subnetting

As the name implies, **subnetting** is the process of dividing a single large network into multiple small networks known as subnets. The primary purpose of subnetting is to help relieve network congestion and improve efficiency in the utilization of the relatively small network address space available especially in IPv4.

### Supernetting

#### **What is Supernetting?**

**Supernetting** is the direct opposite of subnetting, in which multiple networks are combined into a single large network known as supernets. Supernetting provides route updates in the most efficient way possible by advertising many routes in one advertisement instead of individually.

#### **Benefits of Supernetting**

The main objective of supernetting is to simplify or summarize network routing decisions to minimize processing overhead when matching routes, and storage space of route information on routing tables. A routing table is a summary of all known networks. Routers share routing tables to find the new path and locate the best path for the destination. Without Supernetting, the router will share all routes from routing tables as they are. With Supernetting, it will summarize them before sharing, which significantly reduces the size of routing updates.

Figure 1.0 Diagram depicting supernetting Vs. subnetting

#### **Approaches to Subnetting: FLSM vs. VLSM**

There are two approaches to subnetting an IP address for a network: Fixed length subnet mask (FLSM) and variable-length subnet mask (VLSM). In FLSM subnetting, all subnets are of equal size with an equal number of host identifiers. You use the same subnet mask for each subnet, and all the subnets have the same number of addresses in them. It tends to be the most wasteful because it uses more IP addresses than are necessary.

#### **Advantages of VLSM**

VLSM is a subnet design strategy that allows all subnet masks to have variable sizes. In VLSM subnetting, network administrators can divide an IP address space into subnets of different sizes, and allocate it according to the individual need on a network. This type of subnetting makes more efficient use of a given IP address range. VLSM is the defacto standard for how every network is designed today. Table 2.0 below is a summary of the differences between FLSM and VLSM Subnetting. VLSM is supported by the following protocols: Open Shortest Path First (OSPF), Enhanced Interior Gateway Router Protocol (EIGRP), Border Gateway Protocol (BGP), Routing Information Protocol (RIP) version 2 and 3, and Intermediate System-to-Intermediate System (IS-IS). You need to configure your router for VLSM with one of those protocols.

| **FLSM (Fixed Length Subnet Masks) Subnetting** | **VLSM (Variable Length Subnet Masks) Subnetting** |
| --- | --- |
| Old-fashioned | Modern |
| Subnets are equal in size | Subnets are variable in size. |
| Subnets have an equal number of hosts | Subnets have a variable number of hosts |
| Supports both classful and classless routing protocols | Supports only classless routing protocols |
| Wastes more IP addresses | Wastes fewer IP addresses |
| Subnets use the same subnet mask | Subnets use different subnet masks |
| Simple configuration and administration | Complex configuration and administration |

***Table 2.0*** Differences between FLSM and VLSM Subnetting

#### **Practical Scenarios and Decision Making**

Now imagine this scenario: John has just been hired as a network administrator for a new company with six departments. He’s expected to create six separate subnets, one for each department.  He was given a class A 10.0.0.0 private network address for this purpose; and so from all indications, he obviously has a lot of IP address space and can’t even come close to imagining that he’d ever run out of IP addresses. For this reason, John has been wondering why he should bother with the VLSM design process. Should he use a VLSM or an FLSM network design?  Well, the answer is simple. By creating contiguous blocks of valid addresses to specific areas of the network, he can then easily summarize the network and keep route updates with a routing protocol to a minimum. Why would anyone want to advertise several networks between buildings when you can just send one summary route between buildings and achieve the same result?

#### **Implications of Wastage in Addressing**

Besides, wasting of public network IP addressing space has both technical and economic implications. On the technical side, it accelerates its exhaustion; and on the economic side, it costs a lot of money because public network IP addresses are expensive. Therefore, the introduction of VLSM allowed the IP address allocation of a smaller block.

## Implementing VLSM Subnetting

We will begin this section by attempting to solve a practical VLSM problem.  Now, imagine you were recently hired as a Network Engineer for Braxton Investment Limited. Using the VLSM technique, design an IP plan for the company with an IP range of 192.168.4.0/24.  The company’s network consists of three local area networks: LAN A, LAN B, and LAN C as shown in Figure 2.0 below. These three LANs are connected with three serial links: Link AB, Link BC, and Link AC.

Figure 2.0 Network diagram Braxton Investment Limited

One of the easiest ways to solve VLSM problems is by using a subnetting chart like the one shown in Table 3.0 below. We will use this chart to tackle the above problem

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
| **Host** | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| **Subnet Mask** | /24 | /25 | /26 | /27 | /28 | /29 | /30 | /31 | /32 |

***Table 3.0*** VLSM subnetting chart

As you can see from the diagram, we have six networks LAN A, LAN B, LAN C, and link A, link B and a link C.  Links A, B, and C are also three separate networks and each requires two host identifiers.  Thus our task is to design an IP plan for each of the six networks according to their stipulated sizes using VLSM subnetting method. We need five steps to solve the problem:

### Step 1: Arrange the networks from the largest to the smallest as shown in Table 4.0 below:

| **LAN Name** | **No of Host** |
| --- | --- |
| LAN A | 60 |
| LAN B | 29 |
| LAN C | 14 |
| Link AB | 2 |
| Link AC | 2 |
| Link BC | 2 |

***Table 4.0*** LAN arranged according to the number of hosts

### Step 2: Implement VLSM subnetting for the largest network (LAN A)

The largest network LAN A requires 60 hosts. From the Host section (row) of our subnetting chart below, the closest to the required 60 hosts is 64, which corresponds to 4 subnets and a new CIDR value of /26 (the column is in bold). From this relevant information, we will build a new table containing Network ID, Subnet Mask in CIDR notation, Usable, and Name of Local Area Network affected. Keep in mind the first host identifier is reserved for the network ID and the last host ID is reserved for the broadcast ID, so the total number of usable host IDs for each subnet in this particular case is 62 (64-2).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | 1 | 2 | **4** | 8 | 16 | 32 | 64 | 128 | 256 |
| **Host** | 256 | 128 | **64** | 32 | 16 | 8 | 4 | 2 | 1 |
| **Subnet Mask** | /24 | /25 | **/26** | /27 | /28 | /29 | /30 | /31 | /32 |

Given the IP range: 192.168.4.0/24

| **Network ID** | **Subnet Mask** | **Total Host** | **Usable Host Range** | **Name of LAN** |
| --- | --- | --- | --- | --- |
| 192.168.4.0 | /26 | 64 | 192.168.4.1–192.168.4.62 | LAN A |
| 192.168.4.64 | /26 | 64 |  | Unassigned |
| 192.168.4.128 | /26 | 64 |  | Unassigned |
| 192.168.4.192 | /26 | 64 |  | Unassigned |

***Table 5.0*** IP plan for LAN A (60 hosts)

Now let’s list a network ID for each subnet. Keep in mind that only the fourth octet changes; the first three octets remain the same:

* The first network ID is always the original given ID which is 192.168.4.0
* The second network ID is 192.168.4.64
* The third network ID is 192.168.4.128
* The fourth network ID is 192.168.4.192

Here is the pattern:  The first network ID is always the original one. The next network ID is obtained by adding 64 to the previous one.  We can assign any of these for subnets to LAN A since they are all equal in size, but for the sake of simplicity, we assign the first subnet (192.168.4.0) to LAN A. The other three available subnets can be marked as unassigned and reserved for future use. We have completed the task of designing the IP plan for the largest LAN – LAN B.

### Step 3: Implement VLSM subnetting for the second-largest network (LAN B)

The second-largest network, LAN B, requires 29 hosts. The minimum number of hosts which can satisfy LAN B with the 29 hosts on our subnetting chart is 32. This corresponds to eight subnets and a new CIDR value of /27 (the column is in bold).

Now select the first unassigned large subnet in Table 5.0 above and subdivide into two smaller subnets. This gives us 192.168.4.64 and 192.168.4.96 marked in green in Table 6.0 below. Again the pattern is simple: The first network ID is always the original one. The next network ID is obtained by adding 32 to the previous one. We can then assign 192.168.4.64 to LAN B, and mark the second one (192.168.4.96) as unassigned and reserved for future use. We have completed designing the IP plan for LAN A.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | 1 | 2 | | 4 | | **8** | 16 | 32 | 64 | | 128 | 256 |
| **Host** | 256 | 128 | | 64 | | **32** | 16 | 8 | 4 | | 2 | 1 |
| **Subnet Mask** | /24 | /25 | | /26 | | **/27** | /28 | /29 | /30 | | /31 | /32 |
| **Network ID** | **Subnet Mask** | | **Total Host** | | **Usable Host Range** | | | | | **Name of LAN** | | |
| 192.168.4.64 | /27 | | 32 | | 192.168.4.65 – 192.168.4.94 | | | | | LAN B | | |
| 192.168.4.96 | /27 | | 32 | |  | | | | | Unassigned | | |

***Table 6.0*** IP plan for LAN B (29 hosts)

### Step 4: Implement VLSM subnetting for LAN C

This step repeats the process above. The minimum number of hosts which can satisfy LAN C with the 14 hosts on our subnetting chart is 16. This corresponds to 16 subnets and a new CIDR value of /28 (the column is in bold).

Now select the first unassigned subnet in Table 6.0 above and subdivide into two smaller subnets. This gives us 192.168.4.96 and 192.168.4.112 in Table 7.0 below. Again the pattern is simple: The first network ID is always the original one. The next network ID is obtained by adding 16 to the previous one. We can then assign 192.168.4.96 to LAN C, and mark the second one (192.168.4.112) as unassigned and reserved for future use. We have completed designing the IP plan for LAN C.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | 1 | 2 | | 4 | | 8 | **16** | 32 | 64 | 128 | 256 |
| **Host** | 256 | 128 | | 64 | | 32 | **16** | 8 | 4 | 2 | 1 |
| **Subnet Mask** | /24 | /25 | | /26 | | /27 | **/28** | /29 | /30 | /31 | /32 |
| **Network ID** | **Subnet Mask** | | **Total Host** | | **Usable Host Range** | | | | | **Name of LAN** | |
| 192.168.4.96 | /28 | | 16 | | 192.168.4.97– 192.168.4.110 | | | | | LAN C | |
| 192.168.4.112 | /28 | | 16 | |  | | | | | Unassigned | |

***Table 7.0*** IP plan for LAN C (14 hosts)

### Step 5: Implement VLSM subnetting for Link A, B, and C

The last step is to assign three smaller subnets for serial links A, B, and C.  Each link requires two host IDs.  Therefore, the minimum number of hosts which can each link with two hosts on our subnetting chart is four. This corresponds to 64 subnets and a new CIDR value of /30 in our subnetting chart (the column is in bold).

Now select the unassigned subnet in Table 7.0 above and subdivide into four smaller subnets to accommodate the subnets for the three serial links. This gives us four unique IPs as shown in Table 8.0 below.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Subnet** | 1 | 2 | | 4 | | 8 | 16 | 32 | **64** | 128 | 256 |
| **Host** | 256 | 128 | | 64 | | 32 | 16 | 8 | **4** | 2 | 1 |
| **Subnet Mask** | /24 | /25 | | /26 | | /27 | /28 | /29 | **/30** | /31 | /32 |
| **Network ID** | **Subnet Mask** | | **Total Host** | | **Usable Host Range** | | | | | **Name of LAN** | |
| 192.168.4.112 | /30 | | 4 | | 192.168.4.113–192.168.4.114 | | | | | LINK AB | |
| 192.168.4.116 | /30 | | 4 | | 192.168.4.117–192.168.4.118 | | | | | LINK AC | |
| 192.168.4.120 | /30 | | 4 | | 192.168.4.121–192.168.4.122 | | | | | LINK BC | |
| 192.168.4.124 | /30 | | 4 | |  | | | | | Unassigned | |

***Table 8.0****IP plan for Link A, B, and C (2 hosts each)*

Again here’s the pattern: The first network ID is always the original one. The next network ID is obtained by adding four to the previous one. We can then assign the first three IPs to Link A, B, and C respectively, and mark the last one (192.168.4.124) as unassigned and reserved for future use. We have completed designing the IP plan for Link A, B, and C, and indeed the entire network. The table below is the complete IP plan for Braxton Investment Limited.

| **Network ID** | **Subnet Mask** | **Total Host** | **Usable Host Range** | **Name of LAN** |
| --- | --- | --- | --- | --- |
| 192.168.4.0 | /26 | 64 | 192.168.4.1–192.168.4.62 | LAN A |
| 192.168.4.64 | /27 | 32 | 192.168.4.65 – 192.168.4.94 | LAN B |
| 192.168.4.96 | /28 | 16 | 192.168.4.97– 192.168.4.110 | LAN C |
| 192.168.4.112 | /30 | 4 | 192.168.4.113–192.168.4.114 | LINK AB |
| 192.168.4.116 | /30 | 4 | 192.168.4.117–192.168.4.118 | LINK AC |
| 192.168.4.120 | /30 | 4 | 192.168.4.121–192.168.4.122 | LINK BC |

***Table 9.0****IP plan for Braxton Investment limited*

VLSM is a crucial technique in modern network design. If you want to design and implement scalable and efficient networks, you should definitely master the art of VLSM subnetting. One of the key objectives of VLSM subnetting in IPv4 is to improve efficiency in the utilization of the space available. This has managed to keep it going in the last 30 years. But on the 25th of November 2019, [RIPE Network Coordination Centre](https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses) announced that it made the final /22 IPv4 address allocation, and has officially run out of IPv4 addresses. A longer-term solution to the eventual exhaustion of the 32-bit IPv4 network address space is the 64-bit IPv6 protocol.

## VLSM Subnetting FAQs

## What is VLSM with example?

VLSM (Variable Length Subnet Mask) is a technique that allows network administrators to divide an IP address space into subnets of different sizes, rather than dividing it into subnets of the same size. This allows for more efficient use of IP addresses, as smaller subnets can be used for smaller networks, and larger subnets can be used for larger networks.

For example, if a network administrator is given a Class C IP address space of 192.168.1.0/24, they can use VLSM to divide it into two subnets: one with a /25 mask for a smaller network, and one with a /26 mask for a larger network. The smaller network would have 128 host addresses, and the larger network would have 64 host addresses.

This allows the administrator to assign IP addresses more efficiently, as they can use the larger subnet for a network that needs more IP addresses and the smaller subnet for a network that needs fewer IP addresses.

## What does it mean when it says "IP not in subnet range"?

“IP not in subnet range” simply means that you are attempting to use  an IP address that doesn’t belong to the block of IP’s defined by the subnet mask in question. Based on our VLSM example above, if the network address and subnet mask for LAN B is 192.168.4.0 and 255.255.255.192 (/26) respectively, and you are trying to use an ip address of 192.168.2.2 then you will get an “ip not in subnet range” error. The only usable host IP addresses in range are 192.168.4.1–192.168.4.62 as shown on Table 9.0.

## How do you calculate VSLM?

The simplest way to calculate VLSM is by using a subnetting chart like the one shown in Table 3.0 above, and then following the steps below:

1. Arrange the requirements of IP addresses in descending order like the one shown on Table 4.0 above
2. Using the subnetting chart, assign the appropriate subnet masks to each subnet based on the required number of hosts.
3. Allocate one the resulting subnets to the designated LAN  and reserve the rest for future use
4. Pick the next available subnet from step 3 above, and repeat the subnetting process using the chart till you get to last network on your list
5. Review and document your subnetting summary

Please see the “Implementing VLSM Subnetting” section above for detailed explanation.

## How would the use of VLSM impact your choice of routing protocols?

Well, the bad news is that not all routing protocols support VLSM. Classful routing protocols such as RIPv1 and IGRP, do not support VLSM. Therefore, it’s important to ensure that you configure your router for VLSM with one of the supported protocols. But the good news is that all current generation of routing protocols such as RIPv2/v3, OSPF, IS-IS, EIGRP,  BGP, and even Static routes, are classless and therefore support VLSM.

## What are the 5 classes in subnetting?

In IP addressing, there are five classes of IP addresses: A, B, C, D, and E.

1. Class A addresses have a default mask of 255.0.0.0 and a range of 1.0.0.0 to 127.255.255.255. The first octet is used for the network address and the remaining three octets are used for the host address.
2. Class B addresses have a default mask of 255.255.0.0 and a range of 128.0.0.0 to 191.255.255.255. The first two octets are used for the network address and the remaining two octets are used for the host address.
3. Class C addresses have a default mask of 255.255.255.0 and a range of 192.0.0.0 to 223.255.255.255. The first three octets are used for the network address and the last octet is used for the host address.
4. Class D addresses are reserved for multicast groups and have a range of 224.0.0.0 to 239.255.255.255
5. Class E addresses are reserved for experimental or future use and have a range of 240.0.0.0 to 254.255.255.255

Note that, nowadays Class A,B,C are mostly used for subnetting, class D and E are not used for subnetting