**IPv4(Internet Protocol version 4)**

Topic is being covered broadly under the following heads

Part 1

* Networks – just a brief overview
* Components in a computer NW – various terms that we come across
* Communication means between hosts – why the need for addressing
* Characteristics of IPv4 broadly - in brief
* IPv4 Packet structure – and its components
* IPv4 Addressing – the 3 addressing modes
* Hierarchical addressing scheme of IP address – the NW part and subnet mask part
* The IPv4 Address classes – A, B, C, D, E
* IPv4 – Subnetting for each class and its variations
* IPv4 – VLSM vs FLSM with an example

Part 2

* IPv4 – Reserved addresses
* IPv4 Packet flow in the NW – describe how actual communication happens on the Network using Internet Protocol version 4 - from acquiring an IP address to delivery of message till the other end.
* Summarize, leading to the need for IPv6.

Part 1

Network –

* A collection of interconnected hosts, via some shared media which can be wired or wireless.
* Enables its hosts to share and exchange data and information over the media
  + - media 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 states

Components involved in a Network

* **Hosts** − situated at ultimate end of the network,
  + - One host is a source of information and another host will be the destination. Information flows end to end between hosts.
    - a host can be - user’s PC, an internet Server, a database server etc.
* **Media** – wired - copper cable, fiber optic cable, coaxial cable.

- wireless,

* **Hub** − A hub is a multiport repeater
  + - used to connect hosts in a LAN segment.
    - 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.
  + - much faster than Hubs and operate on wire speed.
    - Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches(switch – L3) are also available.
* **Router** − A router is Layer-3 (Network Layer) device
  + - makes routing decisions for the data/information sent for some remote destination.
* **Gateways** − A software or combination of software and hardware put together,
  + - **required** 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.

Host Addressing need?

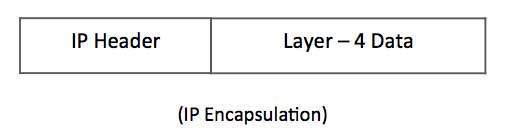
* Communication between hosts happen only if they can identify each other on the network.
* In a single collision domain (where every packet sent on the segment by one host is heard by every other host) hosts can communicate directly via MAC address.
* MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host.
* But for 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**.

## Characteristics of IPv4 Address

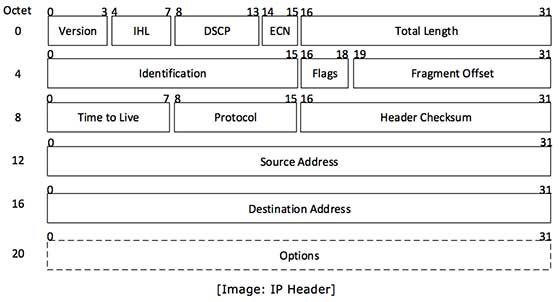
* This protocol works at the **network layer of the OSI mode**l and at the **Internet layer of the TCP/IP model**
* IPv4 addresses - 32-bit long.
* Represented in binary, dotted-decimal, or hexadecimal notation. The most common form to represent IPv4 addresses is the dotted decimal notation.
* Classified into classful addressing where the address space is divided into five classes- Class A, Class B, Class C, Class D, and Class E.
* Addresses are unique, so no two devices on a network can have the same IP address.
* Consists of two parts - the network part and the host part.
* The IPv4 packet header(handled at the NW layer) consists of 20 bytes of data.
* Connectionless protocol - can be unreliable while transmitting packets-best effort delivery
* 3 modes of addressing- unicast, broadcast, and multicast.
* Can be assigned manually or by a protocol known as DHCP(Dynamic Host Configuration Protocol).

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 the **data Segments** received from above layer(Transport) and its own header information.



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



* **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.

IPv4 – Addressing Modes

Addressing mode refers to the mechanism of hosting an address on a given network.

Different Types of Addressing Modes supported by IPv4.

* Unicast addressing mode –
  + - most common mode of addressing
    - Data sent to only a single host
    - One source and one receiver.
    - The relationship between the source and the destination network is one-to-one.
* Broadcast addressing mode
  + - data is sent to all the devices in the network, i.e., multiple hosts.
    - Special Broadcast address which is represented by 255.255.255.255255.255.255.255.
* Multicast addressing mode
  + - there is one source and a group of destinations or hosts
    - Relationship between the source and the destination is one too many.
    - The destination address consists of a special address starting with 224.x.x.x.

Hierarchical Addressing Scheme of IP address

* IPv4 uses hierarchical addressing scheme.
* 32-bits in length - divided into two or three parts

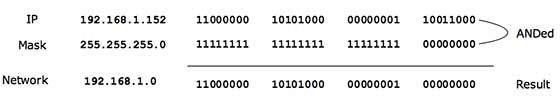


* A single IP address contains information about
  + the network
  + its sub-network
  + ultimately the host.
  + IP Address is hierarchical – i.e. a network can have many sub-networks which in turn can have many hosts.

Subnet Mask

* IP address contains info about NW Id and Host Id
* Routers need to distinguish both.
* Routers use Subnet Mask, which is also 32 bit
* If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address.

Example - say IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then −

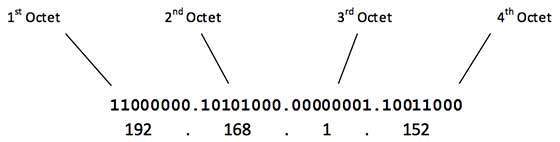


* Can be identified that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.
* Subnet Mask helps extract the Network ID and the Host from an IP Address.

IPv4 - Address Classes

* The IPv4 Addressing system - divided into five classes of IP Addresses – namely A, B, C, D, E classes
* All the five classes are **identified by the first octet of IP Address**. The first octet is the left most of all.
* Internet Corporation for Assigned Names and Numbers(ICANN) is responsible for assigning IP addresses.

The octets numbered as follows depicting dotted decimal notation of IP Address −



* The number of networks & number of hosts in each class is derived as



* No of hosts IP addresses -2 IP addresses are decreased - 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).
* 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
  + => Class A addressing can have 126 networks (27-2) and 16777214 hosts (224-2).
* Class A IP address format is  **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 – data not destined for a particular host =>no need to extract host address from the IP address

=>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 does not have any subnet mask.

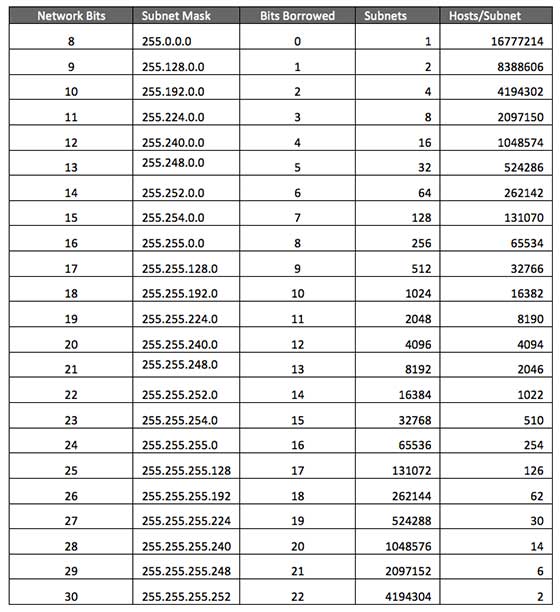
IPv4 - Subnetting

* **Classful IP** addressing –
  + Each class has its own default subnet mask
  + => Prefixed number of Networks and Hosts per network.
  + => No flexibility to have less number of Hosts per Network or more Networks per IP Class.
* CIDR or **Classless Inter Domain Routing** provides flexibility to borrow bits of Host part and use them to have more Networks in that Network, called Subnets.
  + 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

* The **default subnet mask** for Class A IP address is 255.0.0.0 =>126(27-2) networks and 16777214 (224-2) hosts.
* 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.
* Sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two 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 −



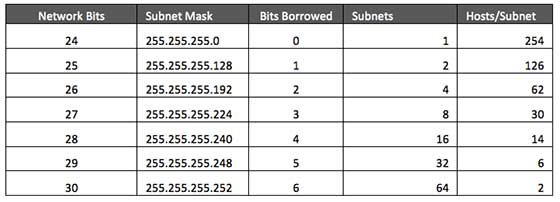
Class B Subnets

* The **default subnet mask** for Class B IP address is 255.255.0.0 =>14 bits are used as Network bits providing 16384(214) Networks and 65534(216-2) Hosts.
* Class B can be sub netted by borrowing bits from Host bits.
* Given below all possible combination of Class B subnetting −



Class C Subnets

* The **default subnet mask** for Class C IP address is 255.255.255.0 => 21 bits are used as Network bits providing 2097152 (221) Networks and 254 (28-2) Hosts.
* Class C IP addresses are normally assigned to a very small size network as it can only have 254 hosts in a network.
* Given below all possible combination of Class C subnetting −



IPv4 – Variable Length Subnet Mask(VLSM)

* Customers requiring IP addresses approach the ISP(Internet Service Providers)
* For an ISP - not feasible to divide the IP addresses into fixed size subnets
* ISPs will want to **subnet the subnets** in such a way which results in minimum wastage of IP addresses.
* Ex PSG Tech and PSGR Krishnammal college may approach the same ISP provider in the region with different no of host requirements. May have same Class C address(subnet mask 255.255.255.x), but the 4th octet of the Subnet Mask will have different masking bits to differentiate the 2 NW IP address allotment.

Note: In **CIDR** or **Classless Inter Domain Routing** the subnets are of fixed size.

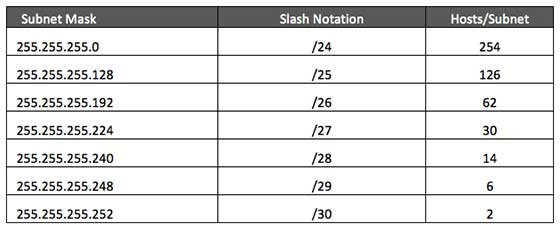
An example of VLSM within an organisation

* Administrator of 192.168.1.0/24 network – 24 bits used for NW address, 255.255.255.x is the sub net mask.
* Has 3 different departments with different number of hosts –
  + Sales - 100 computers
  + Purchase - 50 computers
  + Accounts - 25 computers
  + Management - 5 computers.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses for the above 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
  + Sales – assign 192.168.1.0 /25 (255.255.255.128)- 126 valid hosts, against the requirement of 100 hosts.
  + The subnet mask used for this subnet has 10000000(128) as the last octet.

Step - 4

* Allocate the next highest range to next highest requirement
  + Purchase – assign 192.168.1.128 /26 (255.255.255.192) - 62 valid hosts against the requirement of 50 hosts.
  + The subnet mask used for this subnet has 11000000(192) as the last octet.

Step – 5

* Allocate the next highest range to next highest requirement
  + Accounts – assign 192.168.1.192 /27 (255.255.255.224)) - 30 valid hosts against the requirement of 25 hosts.
  + The subnet mask used for this subnet has 11100000(224) as the last octet.

Step – 6

* Allocate the next highest range to next highest requirement
  + Management – assign 192.168.1.224 /29 (255.255.255.248)) - 6 valid hosts against the requirement of 5 hosts.
  + The subnet mask used for this subnet has 11111000(248) as the last octet.

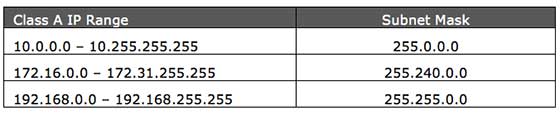
Part 2

IPv4 - Reserved Addresses

* 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
  + Loopback IP Addresses
  + Link-local Addresses

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.



* For private NW to communicate with the outside world, their private NW IP addresses must be translated to some public IP addresses using NAT(Network address translation) process, or Web Proxy server can be used.
* Purpose 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.
* 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(Ex- PSG Tech), smaller organizations may opt for class C.
* These private IP addresses within the organization 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(NW interface card).
* 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.
* 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

* Link local address ranges from 169.254.0.0 -- 169.254.255.255.
* 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.
* How it works -
  + 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.
  + 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.
  + Windows (98 or later), and Mac OS (8.0 or later) supports this functionality of self-configuration of Link-local IP address
* These IP addresses cannot help systems 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.