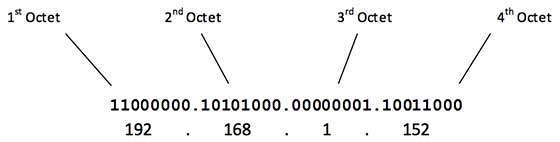
Week four lecture seven and eight

# 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 rage 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 SUBNETING

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.

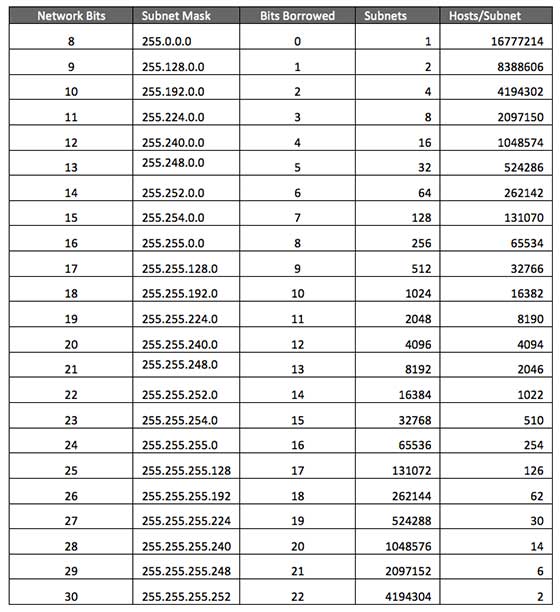
CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management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

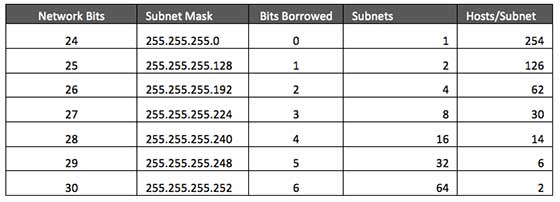
**Class B Subnets**

By default, using Classful Networking, 14 bits are used as Network bits providing (214) 16384 Networks and (216-1) 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:



**VLSM(VARIABLE LENGTH SUBNET MASKING )**

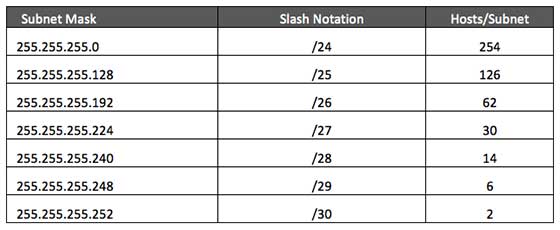
Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size 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 EXAMPLE:**

## 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, mixbazar24.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.MIXBAZAR24.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.MIXBAZAR24.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.

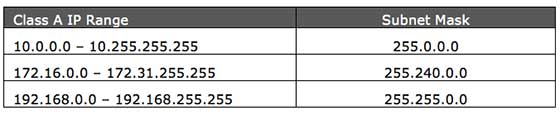
An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data. It is important that source and destination MAC addresses change as they travel across the Internet (segment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

**IPv4 - 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. This IPs is also not routable.

IPv4 – Summary

The Internet Protocol version 4 was designed to be allocated to approximately 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.