IP Address Classes

IP Address classes were the original organizational structure for IP addresses. The specific address class would determine the maximum potential size for a computer network. The address class would define which of the specific bits of the address would be used to identify the network and network identification, the bits to identify the host computer and host ID, and total number of host subnets permitted per network. Five total classes of IP addresses were defined, class A through E. Although the IP class term will commonly be used to describe the difference between one network and another, the practical use of addressing is not commonly used any more. It has been replaced with classless addressing where a netmask can be assigned to any IP address range.

What is an IP Address?

An Internet Protocol (IP) address is a numeric label consisting of a 32 bit number assigned to a network capable device that uses IP for communication. The address fundamentally serves two purposes: location addressing and computer host or network interface identification. The address indicates where the connected device resides with the majority of hosts/devices still using the IPv4 (Internet Protocol Version 4) form of addressing. A significant limitation of the legacy IPv4 addressing is that it supports less than 4.3 billion total addresses. Based on the rapid growth of the Internet and related technologies, the use of IPv4 is not sustainable for the long term. In the mid-1990's, the new IPv6 technique was developed which makes use of 128 bits for the IP address. IPv6 technology continues to be deployed, albeit slowly. The Internet Assigned Numbers Authority (IANA) is responsible under the IETF for management of the IP address space allocation globally. Beneath the IANA, there are five regional Internet registries (RIRs) that are responsible for allocating IP address blocks to Internet service providers (ISPs) and other trusted organizations.

Where Are IP Addresses Defined?

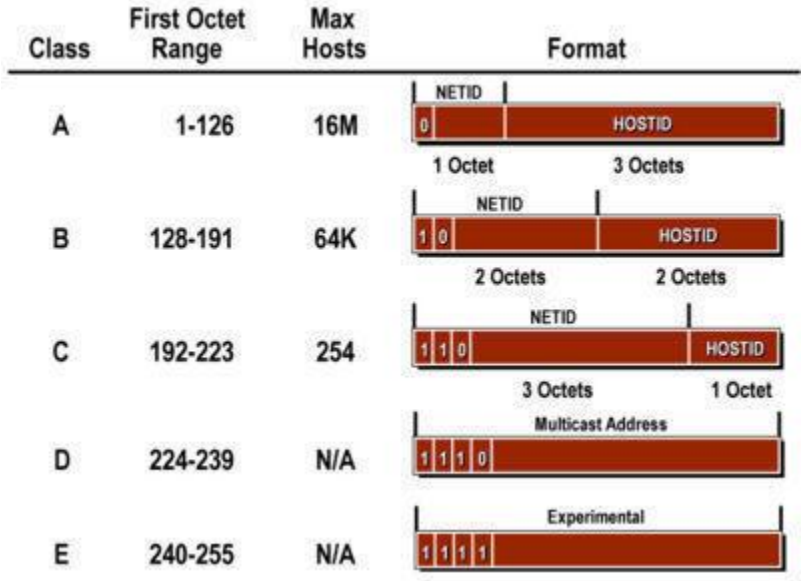
The Internet Protocol is defined in, RFC 791: Internet Protocol, published in 1981. The protocol is designed to be used in a packet-switched computer network and

provides for the transmission of data packets (defined as datagrams) from source devices to destinations. The source and destination devices are identified by a fixed length address defined by the protocol. The specification also takes into account fragmentation of data and the reassembly of longer blocks of data when required. The IP specification does not address data reliability, flow control, sequencing, quality of service, etc. These aspects are handled by supporting technologies such as the TCP (transmission control protocol). The four key mechanism used in the IP definition are: type of service, time to live, options, and the header checksum. Type of service is used to indicate the quality of service desired intended to be used by routers (or gateways) to select the transmission parameters applicable for the network or forwarding of the information. Time to live indicates the upper bound on how long the datagram or data packet should be forwarded until dropped. Options allow for control functions implemented for specific networks such as special routing, security, or timestamps but are not otherwise required for standard communication. The header checksum is used to ensure that the data packet has been transmitted correctly. If the checksum fails, the datagram should be dropped.

What Are the IP Address Classes?

There were five IP address classes in use before the majority of industry switched to classless routing. There were A, B, C, D, and E. Class A addresses were used for networks with a very large number of total hosts. Class B was designed for use on medium to large networks, and C for small local area networks (LANs). Class D and E were set aside for multicast and experimental purposes. In the following table, the four octets that make up an IP address (a, b, c, and d respectfully) are displayed in how they were distributed in classes A, B, and C.
classes A, B, and C.

Class	**IP Address**	Network ID	Host ID
A	a.b.c.d	a	b.c.d
B	a.b.c.d	a.b	c.d
C	a.b.c.d	a.b.c	d



Class A IP Address

Class A IP addresses were used for networks that had a large number of hosts on the network. The class permitted up to 126 networks by using the first octet of the address for the network identification. The first bit in this octet was always fixed or set to be zero. The following seven bits in the octet were then set to one which would complete the network identification. The remaining octets (24 bits) represented the hosts ID and would allow up to 126 networks with 17 million hosts per network. In a Class A address, the network number values start at the number 1 and end at 127.

Class B IP Address

Class B IP address were assigned to medium to large networks. They allow 16,384 networks by using the first two octets in the address for the network identification. The first two bits of the first octet are fixed to 1 0. The next 6 bits along with the following octet then complete the network identification. The third and fourth octet (16 bits) then represents the host ID. This allows approximately 65,000 hosts per network. Class B network number values start at 128 and finish at 191.

Class C IP Address

Class C IP addresses were used in small LAN configurations. They allow for approximately 2 million networks by using the first three octets of the address for the network identification. In a Class C address, the first three bits are fixed to 1 1

0. In the following three octets, 21 bits make up the network identification. The last octet then represents the host identification. This allows for 254 hosts per network. A Class C network number value starts at 192 and ends at 223.

Class D IP Address

Class D IP addresses were reserved for multicasting purposes. These addresses begin with an octet in the 224-239 range. They would have leading bits of 1 1 1 0 and includes addresses from 224.0.0.0 to 239.255.255.255.

Class E IP Address

Class E IP addresses are reserved for experimental use. The first octet of these addresses ranges between 240 and 255. This range is reserved by the IETF and similar to Class D networks, should not be assigned to a host device.

What is IPv6?

The IETF identified the problem with the rapid exhaustion of the IPv4 address space several decades ago. Despite the invention of classless IP addressing, it was assessed that a new addressing protocol was required to address long term needs. IPv6 was then designed as the succeeding standard to IPv4 and released in 1995. The resulting address space was then increased from 32 to 128 bits (16 octets) and deemed to be adequate for at least the mid-term requirements for Internet growth. The design of IPv6 incorporates the idea of allowing efficient aggregation of subnet routing prefix at the router level. This results in the reduction of routing table sizes and actual address utilization rates being small on any IPv6 network segment. The design also allows for the separation of the addressing infrastructure of a local segment's space from the addressing used to route to or from external network traffic. The large number of network addresses also allows large blocks to be assigned for a specific purpose and when required aggregated for more efficient routing. The need for more complicated addressing conservation methods such as now used in Classless Inter-Domain Routing (CIDR) is also eliminated with the implementation of IPv6.

Similar to IPv4, IPv6 reserves blocks of IP address for private use. In IPv6; however, these are referred to as unique local addresses (ULA). This block of addresses uses the routing prefix fc00::/7 that is then divided into two /8 blocks that have different implied policies. The addresses include a 40-bit pseudorandom

number which minimizes the risk of address collisions if packets are routed inappropriately or sites merge. None of the current or legacy IPv6 private address prefixes are supposed to be routed on the public Internet just like the behavior expected from IPv5. Finally, despite the majority of modern operating systems now providing support for IPv6, it has not yet seen widespread deployment in the home networking, VoIP, and networking peripheral fields.

What is Classless IP Addressing?

After the invention of the Domain Name System (DNS), industry realized that the use of IP address classes would limit the scalability of the Internet. As a result, the IETF published RC 1518 and 1519 in 1993 to define the classless method of routing IPv4 data packets. The most recent definition of the standard occurred in 2006 under RFC 4632. Classless IP addressing was introduced as a more efficient means to make use of the IP address space when compared to Classful addressing. In classless addressing, the IP address is treated as a 32 bit stream where the boundary between the network identification and host can be at any of the bit positions. The network portion of the address is determined by the number of 1's that are in the subnet mask being applied to the address. A subnet mask is used locally on the hosts connected to the network and are never transmitted in an IPv4 data packet or datagram. All of the hosts on the same network are configured to use the same subnet mask with the host section of the IP address being unique to the host. The classless version of address is referred to as Classless Inter-Domain Routing (CIDR) and allows networks to be divided into different-sized subnets. The system avoids wasting IP addresses through the use of the subnet mask.

How Does a Subnet Mask Work?

In classless IP address, a subnet mask is used on a network to define how many bits are used for the network address and how many are used for the host address. The subnet mask is the same for all users on a specific network. When overlay on a host address, it tells the host or device what part of the IP address is the network address and which is used for the host. Subnet masks will typically start with 255.*.*.* with the remaining digits specific to the network. Every subnet address on a large network will have its own subnet mask which in essence means the

specific subnet has a subnet mask. This allows for the current form of classless IP addressing that has been in use for IPv4 networks since the 1990s.

How Long Until IPv6 Is Fully Implemented?

Unfortunately, at the time of this writing the answer remains "It depends." The discussion of running out of IP addresses has been ongoing for more than a decade, and it will likely continue to do so for at least another. The advent of Network Address Translation (NAT) and Dynamic Host Control Protocol (DHCP) has been implemented and very successful. As a result, consumers have essentially been sharing IP addresses through their ISP without really noticing for the past decade. As the popularity for "Always On," high demand services such as video or television streaming increases; however, the quality of service realized at the user level may start to suffer. Just think if you could not watch your favorite sitcom because all of the users in your assigned addressing block with the ISP were actually 1 – Online, and 2 – Actively using their Internet connection at the same time. This rarely occurs now, but as more and more of the devices in the home become "connected" it may in the future. When / if this occurs, then a more significant shift of major service providers to IPv6 will occur. In the meantime; however, the Internet 2 research group is operating on and conducting research on what is considered to be the Internet of the future running on IPv6, providing significant quality of service improvements, and a higher data rate capacity than currently realized on networks running on the IPv4 standard. Most modern computing devices; however, are being sold with native IPv6 support so if the change does occur sooner than later consumers won't necessarily be forced into buying a new computer.

Source: http://www.tech-faq.com/ip-address-classes.html