IP ADDRESSING

An Internet Protocol (**IP**) **address** is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as **208.77.188.166 (for IPv4)**, and **2001:db8:0:1234:0:567:1:1 (for IPv6)**. The role of the IP address has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there.”

The original designers of TCP/IP defined an IP address as a 32-bit number and this system, now named Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the resulting depletion of the address space, a new addressing system (IPv6), using 128 bits for the address, was developed.

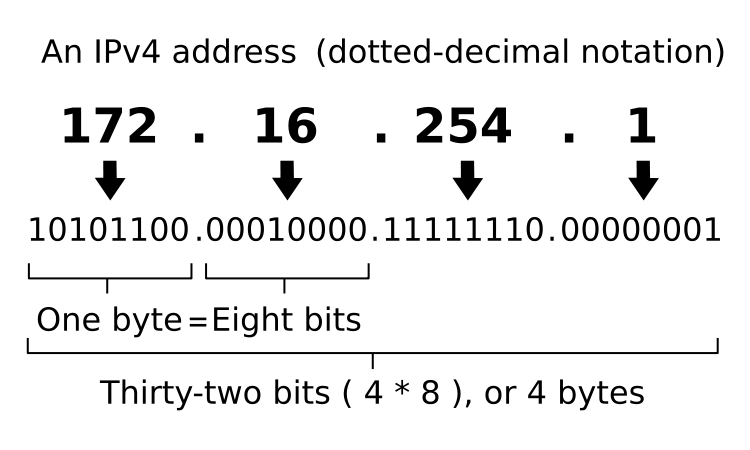
The Internet Protocol also has the task of routing data packets between networks, and IP addresses specify the locations of the source and destination nodes in the topology of the routing system. For this purpose, some of the bits in an IP address are used to designate a subnetwork. The number of these bits is indicated in CIDR notation, appended to the IP address, e.g., *208.77.188.166/24*.

With the development of private networks and the threat of IPv4 address exhaustion, a group of private address spaces was set aside by RFC 1918. These *private addresses* may be used by anyone on private networks. They are often used with network address translators to connect to the global *public* Internet.

The **Internet Assigned Numbers Authority (IANA)** manages the IP address space allocations globally. IANA works in cooperation with five Regional Internet Registries (RIRs) to allocate IP address blocks to Local Internet Registries (Internet service providers) and other entities.

**IPv4 Addresses**

IPv4 uses 32-bit (4-byte) addresses, which limits the address space to 4,294,967,296 (232) possible unique addresses. However, IPv4 reserves some addresses for special purposes such as private networks (~18 million addresses) or multicast addresses (~270 million addresses). This reduces the number of addresses that can be allocated as public Internet addresses, and as the number of addresses available is consumed, an IPv4 address shortage appears to be inevitable in the long run. This limitation has helped stimulate the push towards IPv6, which is currently in the early stages of deployment and is currently the only offering to replace IPv4.



IPv4 addresses are usually represented in dot-decimal notation (four numbers, each ranging from 0 to 255, separated by dots, e.g. 208.77.188.166). Each part represents 8 bits of the address, and is therefore called an *octet*. In less common cases of technical writing, IPv4 addresses may be presented in hexadecimal, octal, or binary representations. When converting, each octet is usually treated as a separate number.

IPv4 Networks

In the early stages of development of the Internet protocol, network administrators interpreted an IP address as a structure of network number and host number. The highest order octet (most significant eight bits) were designated the *network number*, and the rest of the bits were called the *rest field* or host identifier and used for host numbering within a network. This method soon proved inadequate as local area networks developed that were not part of the larger networks already designated by a network number. In 1981, the Internet addressing specification was revised with the introduction of classful network architecture.

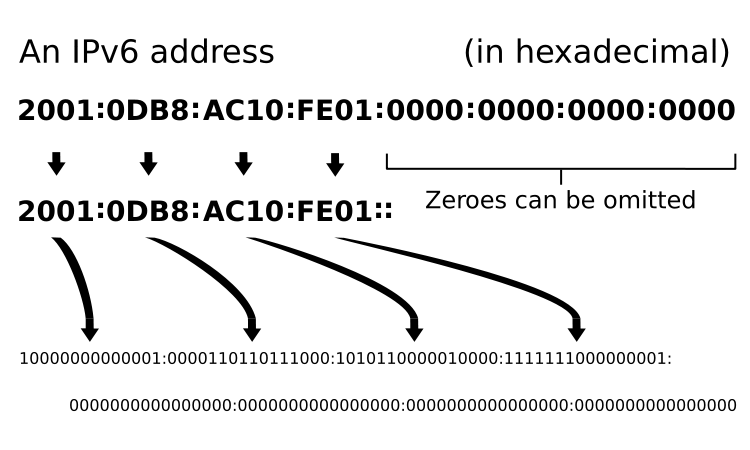
Classful network design allowed for a larger number of individual assignments. The first three bits of the most significant octet of an IP address was defined as the "class" of the address, instead of just the network number and, depending on the class derived, the network designation was based on octet boundary segments of the entire address. The following table gives an overview of this system.

Although classful network design was a successful developmental stage, it proved unscalable in the rapid expansion of the Internet and was abandoned when **Classless Inter-Domain Routing (CIDR)** created for the allocation of IP address blocks and new rules of routing protocol packets using IPv4 addresses. CIDR is based on **variable-length subnet masking (VLSM)** to allow allocation and routing on arbitrary-length prefixes.

Today, remnants of classful network concepts function only in a limited scope as the default configuration parameters of some network software and hardware components (e.g. netmask), and in the technical jargon used in network administrators' discussions.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Class | First Octet in Binary | Range of First Octet | Network ID | Host ID | Possible number of Networks | Possible number of Hosts |
| A | 0XXXXXXX | 0 – 127 | a | b.c.d | 128 = (2)7 | 16,777,214 = (224 - 2) |
| B | 10XXXXXX | 128 – 191 | a.b | c.d | 16,384 = (2)14 | 65,534 = (216 - 2) |
| C | 110XXXXX | 191 - 223 | a.b.c | d | 2,097,152 = (2)21 | 254 = (28 - 2) |

**IPv6 Addresses**

The rapid exhaustion of IPv4 address space, despite conservation techniques, prompted the **Internet Engineering Task Force (IETF)** to explore new technologies to expand the Internet's addressing capability. The permanent solution was deemed to be a redesign of the Internet Protocol itself. This next generation of the Internet Protocol, aimed to replace IPv4 on the Internet, was eventually named Internet Protocol Version 6 (IPv6). The address size was increased from 32 to 128 bits (16 bytes), which, even with a generous assignment of network blocks, is deemed sufficient for the foreseeable future. Mathematically, the new address space provides the potential for a maximum of 2128, or about 3.403 × 1038 unique addresses.

The new design is not based on the goal to provide a sufficient quantity of addresses alone, but rather to allow efficient aggregation of subnet routing prefixes to occur at routing nodes. As a result, routing table sizes are smaller, and the smallest possible individual allocation is a subnet for 264 hosts, which is the size of the square of the size of the entire IPv4 Internet. At these levels, actual address utilization rates will be small on any IPv6 network segment. The new design also provides the opportunity to separate the addressing infrastructure of a network segment--that is the local administration of the segment's available space--from the addressing prefix used to route external traffic for a network. IPv6 has facilities that automatically change the routing prefix of entire networks should the global connectivity or the routing policy change without requiring internal redesign or renumbering.

The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. With a large address space, there is not the need to have complex address conservation methods as used in classless inter-domain routing (CIDR).

Windows Vista, Apple Computer's Mac OS X, all modern[[update]](http://en.wikipedia.org/w/index.php?title=IP_address&action=edit) Linux Distributions, and an increasing range of other operating systems include native support for the protocol, but it is not yet widely deployed in other devices.

Example of an IPv6 address:

**2001:0db8:85a3:08d3:1319:8a2e:0370:7334**

**IP Subnetworks**

The technique of subnetting can operate in both IPv4 and IPv6 networks. The IP address is divided into two parts: the *network address* and the *host identifier*. The subnet mask (in IPv4 only) or the CIDR prefix determines how the IP address is divided into network and host parts.

The term *subnet mask* is only used within IPv4. Both IP versions however use the Classless Inter-Domain Routing (CIDR) concept and notation. In this, the IP address is followed by a slash and the number (in decimal) of bits used for the network part, also called the *routing prefix*. For example, an IPv4 address and its subnet mask may be 192.0.2.1 and 255.255.255.0, respectively. The CIDR notation for the same IP address and subnet is 192.0.2.1/24, because the first 24 bits of the IP address indicate the network and subnet.

**Static and Dynamic IP Addresses**

When a computer is configured to use the same IP address each time it powers up, this is known as a *Static IP address*. In contrast, in situations when the computer's IP address is assigned automatically, it is known as a *Dynamic IP address.*

Uses of Dynamic Addressing

Dynamic IP addresses are most frequently assigned on LANs and broadband networks by **Dynamic Host Configuration Protocol (DHCP)** servers. They are used because it avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows many devices to share limited address space on a network if only some of them will be online at a particular time. In most current desktop operating systems, dynamic IP configuration is enabled by default so that a user does not need to manually enter any settings to connect to a network with a DHCP server. DHCP is not the only technology used to assigning dynamic IP addresses. Dialup and some broadband networks use dynamic address features of the **Point-to-Point Protocol**.

Uses of Static Addressing

Some infrastructure situations have to use static addressing, such as when finding the Domain Name System host that will translate domain names to IP addresses. Static addresses are also convenient, but not absolutely necessary, to locate servers inside an enterprise. An address obtained from a DNS server comes with a time to live, or caching time, after which it should be looked up to confirm that it has not changed. Even static IP addresses do change as a result of network administration.

**IP Address Spoofing**

In computer networking, the term **IP (Internet Protocol) address spoofing** refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.

How Spoofing Works

The basic protocol for sending data over the Internet and many other computer networks is the Internet Protocol ("IP"). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send response back to the forged source address, which means that this technique is mainly used when the attacker does not care about response or the attacker has some way of guessing the response.

In certain cases, it might be possible for the attacker to see or redirect the response to his own machine. The most usual case is when the attacker is spoofing an address on the same LAN or WAN.

Uses of Spoofing

IP spoofing is most frequently used in denial-of-service attacks. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to his attack packets. Packets with spoofed addresses are thus suitable for such attacks. They have additional advantages for this purpose - they are more difficult to filter since each spoofed packet appears to come from a different address, and they hide the true source of the attack. Denial of service attacks that use spoofing typically randomly choose addresses from the entire IP address space, though more sophisticated spoofing mechanisms might avoid unroutable addresses or unused portions of the IP address space. The proliferation of large botnets makes spoofing less important in denial of service attacks, but attackers typically have spoofing available as a tool, if they want to use it, so defenses against denial-of-service attacks that rely on the validity of the source IP address in attack packets might have trouble with spoofed packets. Backscatter, a technique used to observe denial-of-service attack activity in the Internet, relies on attackers' use of IP spoofing for its effectiveness.

IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines. For example, it is common on some corporate networks to have internal systems trust each other, so that a user can log in without a username or password provided he is connecting from another machine on the internal network (and so must already be logged in). By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authenticating.

Services vulnerable to IP Spoofing

Configuration and services that are vulnerable to IP spoofing :

* RPC (Remote Procedure Call services)
* Any service that uses IP address authentication
* The X Window system
* The R services suite (rlogin, rsh, etc.)

Defense against Spoofing

Packet filtering is one defense against IP spoofing attacks. The gateway to a network usually performs ingress filtering, which is blocking of packets from outside the network with a source address inside the network. This prevents an outside attacker spoofing the address of an internal machine. Ideally the gateway would also perform egress filtering on outgoing packets, which is blocking of packets from inside the network with a source address that is not inside. This prevents an attacker within the network performing filtering from launching IP spoofing attacks against external machines.

It is also recommended to design network protocols and services so that they do not rely on the IP source address for authentication.

**Submitted By :**

**Name : Rohit Aggarwal**

**Roll No. : 7CS-097**