

IP address

An IP address (Internet Protocol address) is a unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any participating network device — including routers, computers, time-servers, printers, Internet fax machines, and some telephones — must have its own unique address. An IP address can also be thought of as the equivalent of a street address or a phone number (compare: VoIP) for a computer or other network device on the internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network.

An IP address can appear to be shared by multiple client devices either because they are part of a shared hosting web server environment or because a proxy server (e.g. an ISP or anonymizer service) acts as an intermediary agent on behalf of its customers, in which case the real originating IP addresses might be hidden from the server receiving a request. The analogy to telephone systems would be the use of predial numbers (proxy) and extensions (shared).

Domain names Main article: Domain Name System

A network lookup service, the Domain Name System (DNS), provides the ability to map hostnames to an IP address. This allows humans to easily remember a name and not a series of numbers. DNS allows multiple addresses and names to point to one Internet resource.

Another reason for DNS is to allow, for example, a web site to be hosted on multiple servers (each with its own IP address) to provide rudimentary load balancing.

For example, www.wikipedia.org resolves to 207.142.131.248.

Note: 207.142.131.248 is both Wikipedia and Wikimedia. The web browser sends the desired hostname as a part of the request, allowing the web server to present the appropriate page.

Dynamic and static IP addresses This section does not cite its references or sources.
You can help Wikipedia by introducing appropriate citations.

IP addresses may either be assigned permanently (for example, to a server which is always found at the same address) or temporarily from a pool of available addresses.

Dynamic

Dynamic IP addresses are issued to identify non-permanent devices such as personal computers or clients. Internet Service Providers (ISPs) use dynamic allocation to assign addresses from a small pool to a larger number of customers. This is used for dial-up access, WiFi and other temporary connections, allowing a portable computer user to automatically connect to a variety of services without needing to know the addressing details of each network.

Users with a dynamic IP may have trouble running their own email server as in recent years services such as mail-abuse.org [1] have collected lists of dynamic IP ranges and blocked them.

The most common protocol used to dynamically assign addresses is Dynamic Host Configuration Protocol (DHCP). DHCP includes a lease time which determines how long the requester can use an address before requesting its renewal, allowing addresses to be reclaimed if the requester goes offline. The DHCP server listens for requests and then assigns an address. System administrators may set the DHCP server so that it assigns addresses at random, or based on a predetermined policy.

Once a machine receives its new IP address, it may tell that address to a Dynamic DNS server.

It is common to use dynamic allocation for private networks. Since private networks rarely have an address shortage, it is possible to assign the same address to the same computer on each request or to define an extended lease time. These two methods simulate static IP address assignment.

Static

Static IP addresses are used to identify semi-permanent devices with constant IP addresses. Servers typically use static IP addresses. The static address can be configured directly on the device or as part of a central DHCP configuration which associates the device's MAC address with a static address.

IP versions

The Internet Protocol has two primary versions in use. Each version has its own definition of an IP address. Because of its prevalence, "IP address" typically refers to those defined by IPv4.

IP version 4 Main article: [IPv4#Addressing](#)

IPv4 uses 32-bit (4 byte) addresses, which limits the address space to 4,294,967,296 (2³²) possible unique addresses. However, many are reserved for special purposes, such as private networks (~18 million addresses) or multicast addresses (~1 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 contender to replace IPv4.

IP version 5

What would be considered IPv5 existed only as an experimental non-IP real time streaming protocol called ST2, described in RFC 1819. In keeping with standard UNIX release conventions, all odd-numbered versions are considered experimental, and this version was never intended to be implemented; the protocol was not abandoned. RSVP has replaced it to some degree.

IP version 6 Main article: [IPv6#Addressing](#) In IPv6, the new (but not yet widely deployed) standard protocol for the Internet, addresses are 128 bits wide, which, even with generous assignment of netblocks, should suffice for the foreseeable future. In theory, there would be exactly 2¹²⁸, or about 3.403 × 10³⁸ unique host interface addresses. The exact number is 340,282,366,920,938,463,463,374,607,431,768,211,456. This large address space will be sparsely populated, which makes it possible to again encode more routing information into the addresses themselves.