IP address

An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.[1][2] An IP address serves two main functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number.[2] However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was standardized in 1998.[3][4][5] IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are written and displayed in human-readable notations, such as *172.16.254.1* in IPv4, and *2001:db8:0:1234:0:567:8:1* in IPv6. The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits, e.g., *192.168.1.15/24*, which is equivalent to the historically used subnet mask *255.255.255.0*.

The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for assignment to local Internet registries, such as Internet service providers (ISPs), and other end users. IPv4 addresses were distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each, but have been exhausted at the IANA level since 2011. Only one of the RIRs still has a supply for local assignments in Africa.[6] Some IPv4 addresses are reserved for private networks and are not globally unique.

Network administrators assign an IP address to each device connected to a network. Such assignments may be on a *static* (fixed or permanent) or *dynamic* basis, depending on network practices and software features.

Contents

Function

IP versions

Subnetworks

IPv4 addresses
- Subnetting history
- Private addresses

IPv6 addresses
- Private addresses

IP address assignment
- Sticky dynamic IP address
- Address autoconfiguration
- Addressing conflicts

Routing
- Unicast addressing
- Broadcast addressing
- Multicast addressing

Anycast addressing
Geolocation
Public address
Firewalling
Address translation
Diagnostic tools
See also
References

Function

An IP address serves two principal functions: it identifies the host, or more specifically its network interface, and it provides the location of the host in the network, and thus the capability of establishing a path to that host. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."[2] The header of each IP packet contains the IP address of the sending host, and that of the destination host.

IP versions

Two versions of the Internet Protocol are in common use on the Internet today. The original version of the Internet Protocol that was first deployed in 1983 in the ARPANET, the predecessor of the Internet, is Internet Protocol version 4 (IPv4).

The rapid exhaustion of IPv4 address space available for assignment to Internet service providers and end-user organizations by the early 1990s, prompted the Internet Engineering Task Force (IETF) to explore new technologies to expand the addressing capability on the Internet. The result was a redesign of the Internet Protocol which became eventually known as Internet Protocol Version 6 (IPv6) in 1995.[3][4][5] IPv6 technology was in various testing stages until the mid-2000s when commercial production deployment commenced.

Today, these two versions of the Internet Protocol are in simultaneous use. Among other technical changes, each version defines the format of addresses differently. Because of the historical prevalence of IPv4, the generic term *IP address* typically still refers to the addresses defined by IPv4. The gap in version sequence between IPv4 and IPv6 resulted from the assignment of version 5 to the experimental Internet Stream Protocol in 1979, which however was never referred to as IPv5.

Other versions v1 to v9 were defined, but only v4 and v6 ever gained widespread use. v1 and v2 were names for TCP protocols in 1974 and 1977, as there was to separate IP specification at the time. v3 was defined in 1978, and v3.1 is the first version where TCP is separated from IP. v6 is a synthesis of several suggested versions, v6 *Simple Internet Protocol*, v7 *TP/IX: The Next Internet*, v8 *PIP — The P Internet Protocol*, and v9 *TUBA — Tcp & Udp with Big Addresses*.[7]

Subnetworks

IP networks may be divided into subnetworks in both IPv4 and IPv6. For this purpose, an IP address is recognized as consisting of two parts: the *network prefix* in the high-order bits and the remaining bits called the *rest field*, *host identifier*, or *interface identifier* (IPv6), used for host numbering within a network.[1] The subnet

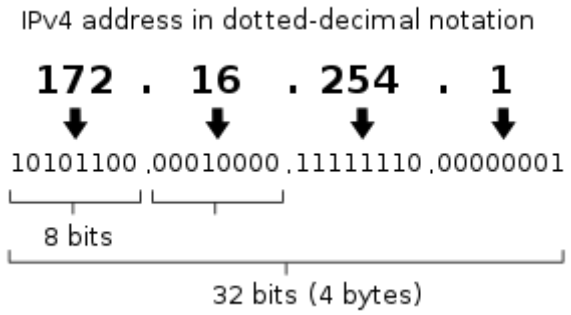
mask or CIDR notation determines how the IP address is divided into network and host parts.

The term *subnet mask* is only used within IPv4. Both IP versions however use the 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.

IPv4 addresses

An IPv4 address has a size of 32 bits, which limits the address space to 4 294 967 296 (2^{32}) addresses. Of this number, some addresses are reserved for special purposes such as private networks (~18 million addresses) and multicast addressing (~270 million addresses).

IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., *172.16.254.1*. Each part represents a group of 8 bits (an octet) of the address. In some cases of technical writing, IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.



Decomposition of an IPv4 address from dot-decimal notation to its binary value

Subnetting history

In the early stages of development of the Internet Protocol, the network number was always the highest order octet (most significant eight bits). Because this method allowed for only 256 networks, it soon proved inadequate as additional networks developed that were independent of the existing networks already designated by a network number. In 1981, the addressing specification was revised with the introduction of classful network architecture.[2]

Classful network design allowed for a larger number of individual network assignments and fine-grained subnetwork design. The first three bits of the most significant octet of an IP address were defined as the *class* of the address. Three classes (*A*, *B*, and *C*) were defined for universal unicast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (*B* and *C*). The following table gives an overview of this now-obsolete system.

Historical classful network architecture

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Number of addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16 777 216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16 384 (2^{14})	65 536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2 097 152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255

Classful network design served its purpose in the startup stage of the Internet, but it lacked scalability in the face of the rapid expansion of networking in the 1990s. The class system of the address space was replaced with Classless Inter-Domain Routing (CIDR) in 1993. CIDR is based on variable-length subnet masking (VLSM) to allow allocation and routing based 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.

Private addresses

Early network design, when global end-to-end connectivity was envisioned for communications with all Internet hosts, intended that IP addresses be globally unique. However, it was found that this was not always necessary as private networks developed and public address space needed to be conserved.

Computers not connected to the Internet, such as factory machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses. Today, such private networks are widely used and typically connect to the Internet with network address translation (NAT), when needed.

Three non-overlapping ranges of IPv4 addresses for private networks are reserved.[8] These addresses are not routed on the Internet and thus their use need not be coordinated with an IP address registry. Any user may use any of the reserved blocks. Typically, a network administrator will divide a block into subnets; for example, many home routers automatically use a default address range of *192.168.0.0* through *192.168.0.255* (*192.168.0.0/24*).

Reserved private IPv4 network ranges[8]

Name	CIDR block	Address range	Number of addresses	*Classful* description
24-bit block	10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 216	Single Class A.
20-bit block	172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 576	Contiguous range of 16 Class B blocks.
16-bit block	192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 536	Contiguous range of 256 Class C blocks.

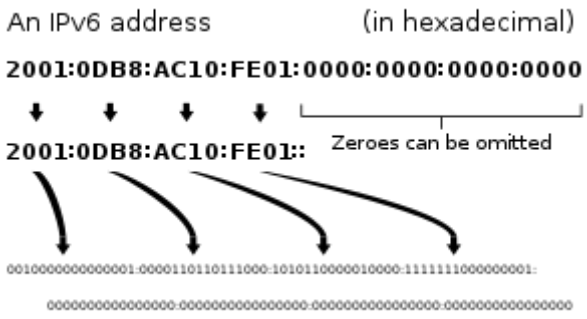
IPv6 addresses

In IPv6, the address size was increased from 32 bits in IPv4 to 128 bits, thus providing up to 2^{128} (approximately 3.403×10^{38}) addresses. This is deemed sufficient for the foreseeable future.

The intent of the new design was not to provide just a sufficient quantity of addresses, but also redesign routing in the Internet by allowing more efficient aggregation of subnetwork routing prefixes. This resulted in slower growth of routing tables in routers. The smallest possible individual allocation is a subnet for 2^{64} hosts, which is the square of the size of the entire IPv4 Internet. At these levels, actual address utilization ratios will be small on any IPv6 network segment. The new design also provides the opportunity to separate the addressing infrastructure of a network segment, i.e. the local administration of the segment's available space, from the addressing prefix used to route traffic to and from external networks. 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 manual 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 no need to have complex address conservation methods as used in CIDR.

All modern desktop and enterprise server operating systems include native support for IPv6, but it is not yet widely deployed in other devices, such as residential networking routers, voice over IP (VoIP) and multimedia equipment, and some networking hardware.



Decomposition of an IPv6 address from hexadecimal representation to its binary value

Private addresses

Just as IPv4 reserves addresses for private networks, blocks of addresses are set aside in IPv6. In IPv6, these are referred to as unique local addresses (ULAs). The routing prefix *fc00::/7* is reserved for this block,[9] which is divided into two */8* blocks with different implied policies. The addresses include a 40-bit pseudorandom number that minimizes the risk of address collisions if sites merge or packets are misrouted.

Early practices used a different block for this purpose (*fec0::*), dubbed site-local addresses.[10] However, the definition of what constituted a *site* remained unclear and the poorly defined addressing policy created ambiguities for routing. This address type was abandoned and must not be used in new systems.[11]

Addresses starting with *fe80::*, called link-local addresses, are assigned to interfaces for communication on the attached link. The addresses are automatically generated by the operating system for each network interface. This provides instant and automatic communication between all IPv6 hosts on a link. This feature is used in the lower layers of IPv6 network administration, such as for the Neighbor Discovery Protocol.

Private and link-local address prefixes may not be routed on the public Internet.

IP address assignment

IP addresses are assigned to a host either dynamically as they join the network, or persistently by configuration of the host hardware or software. Persistent configuration is also known as using a **static IP address**. In contrast, when a computer's IP address is assigned each time it restarts, this is known as using a **dynamic IP address**.

Dynamic IP addresses are assigned by network using Dynamic Host Configuration Protocol (DHCP). DHCP is the most frequently used technology for assigning addresses. It avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows devices to share the limited address space on a network if only some of them are online at a particular time. Typically, dynamic IP configuration is enabled by default in modern desktop operating systems.

The address assigned with DHCP is associated with a *lease* and usually has an expiration period. If the lease is not renewed by the host before expiry, the address may be assigned to another device. Some DHCP implementations attempt to reassign the same IP address to a host, based on its MAC address, each time it joins the network. A network administrator may configure DHCP by allocating specific IP addresses based on MAC address.

DHCP is not the only technology used to assign IP addresses dynamically. Bootstrap Protocol is a similar protocol and predecessor to DHCP. Dialup and some broadband networks use dynamic address features of the Point-to-Point Protocol.

Computers and equipment used for the network infrastructure, such as routers and mail servers, are typically configured with static addressing.

In the absence or failure of static or dynamic address configurations, an operating system may assign a link-local address to a host using stateless address autoconfiguration.

Sticky dynamic IP address

Sticky is an informal term used to describe a dynamically assigned IP address that seldom changes. IPv4 addresses, for example, are usually assigned with DHCP, and a DHCP service *can* use rules that maximize the chance of assigning the same address each time a client asks for an assignment. In IPv6, a prefix delegation can be handled similarly, to make changes as rare as feasible. In a typical home or small-office setup, a single router is the only device visible to an Internet service provider (ISP), and the ISP may try to provide a configuration that is as stable as feasible, i.e. *sticky*. On the local network of the home or business, a local DHCP server may be designed to provide sticky IPv4 configurations, and the ISP may provide a sticky IPv6 prefix delegation, giving clients the option to use sticky IPv6 addresses. *Sticky* should not be confused with *static*; sticky configurations have no guarantee of stability, while static configurations are used indefinitely and only changed deliberately.

Address autoconfiguration

Address block *169.254.0.0/16* is defined for the special use of link-local addressing for IPv4 networks.[12] In IPv6, every interface, whether using static or dynamic addresses, also receives a link-local address automatically in the block *fe80::/10*.[12] These addresses are only valid on the link, such as a local network segment or point-to-point connection, to which a host is connected. These addresses are not routable and, like private addresses, cannot be the source or destination of packets traversing the Internet.

When the link-local IPv4 address block was reserved, no standards existed for mechanisms of address autoconfiguration. Filling the void, Microsoft developed a protocol called Automatic Private IP Addressing (APIPA), whose first public implementation appeared in Windows 98.[13] APIPA has been deployed on millions of machines and became a de facto standard in the industry. In May 2005, the IETF defined a formal standard for it.[14]

Addressing conflicts

An IP address conflict occurs when two devices on the same local physical or wireless network claim to have the same IP address. A second assignment of an address generally stops the IP functionality of one or both of the devices. Many modern operating systems notify the administrator of IP address conflicts.[15][16] When IP addresses are assigned by multiple people and systems with differing methods, any of them may be at fault.[17][18][19][20][21] If one of the devices involved in the conflict is the default gateway access beyond the LAN for all devices on the LAN, all devices may be impaired.

Routing

IP addresses are classified into several classes of operational characteristics: unicast, multicast, anycast and broadcast addressing.

Unicast addressing

The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but a device or host may have more than one unicast address. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient.

Broadcast addressing

Broadcasting is an addressing technique available in IPv4 to address data to all possible destinations on a network in one transmission operation as an *all-hosts broadcast*. All receivers capture the network packet. The address *255.255.255.255* is used for network broadcast. In addition, a more limited directed broadcast uses the all-ones host address with the network prefix. For example, the destination address used for directed broadcast to devices on the network *192.0.2.0/24* is *192.0.2.255*.

IPv6 does not implement broadcast addressing and replaces it with multicast to the specially defined all-nodes multicast address.

Multicast addressing

A multicast address is associated with a group of interested receivers. In IPv4, addresses *224.0.0.0* through *239.255.255.255* (the former Class D addresses) are designated as multicast addresses.[22] IPv6 uses the address block with the prefix *ff00::/8* for multicast. In either case, the sender sends a single datagram from its unicast address to the multicast group address and the intermediary routers take care of making copies and sending them to all interested receivers (those that have joined the corresponding multicast group).

Anycast addressing

Like broadcast and multicast, anycast is a one-to-many routing topology. However, the data stream is not transmitted to all receivers, just the one which the router decides is closest in the network. Anycast addressing is a built-in feature of IPv6.[23][24] In IPv4, anycast addressing is implemented with Border Gateway Protocol using the shortest-path metric to choose destinations. Anycast methods are useful for global load balancing and are commonly used in distributed DNS systems.

Geolocation

A host may use geolocation software to deduce the geographic position of its communicating peer.[25]

Public address

A public IP address is a globally routable unicast IP address, meaning that the address is not an address reserved for use in private networks, such as those reserved by RFC 1918 (https://tools.ietf.org/html/rfc1918), or the various IPv6 address formats of local scope or site-local scope, for example for link-local addressing. Public IP addresses may be used for communication between hosts on the global Internet. In a home situation, a public IP address is the IP address assigned to the home's network by the ISP. In this case, it is also locally visible by logging into the router configuration. [26]

Most public IP addresses change, and relatively often. Any type of IP address that changes is called a dynamic IP address. In home networks, the ISP usually assigns a dynamic IP. If an ISP gave a home network an unchanging address, it's more likely to be abused by customers who host websites from home, or by hackers

who can try the same IP address over and over until they breach a network.[27]

Firewalling

For security and privacy considerations, network administrators often desire to restrict public Internet traffic within their private networks. The source and destination IP addresses contained in the headers of each IP packet are a convenient means to discriminate traffic by IP address blocking or by selectively tailoring responses to external requests to internal servers. This is achieved with firewall software running on the network's gateway router. A database of IP addresses of restricted and permissible traffic may be maintained in blacklists and whitelists, respectively.

Address translation

Multiple client devices can appear to share an IP address, either because they are part of a shared web hosting service environment or because an IPv4 network address translator (NAT) or proxy server acts as an intermediary agent on behalf of the client, in which case the real originating IP address is masked from the server receiving a request. A common practice is to have a NAT mask many devices in a private network. Only the public interface(s) of the NAT needs to have an Internet-routable address.[28]

The NAT device maps different IP addresses on the private network to different TCP or UDP port numbers on the public network. In residential networks, NAT functions are usually implemented in a residential gateway. In this scenario, the computers connected to the router have private IP addresses and the router has a public address on its external interface to communicate on the Internet. The internal computers appear to share one public IP address.

Diagnostic tools

Computer operating systems provide various diagnostic tools to examine network interfaces and address configuration. Microsoft Windows provides the command-line interface tools ipconfig and netsh and users of Unix-like systems may use ifconfig, netstat, route, lanstat, fstat, and iproute2 utilities to accomplish the task.

See also

- Hostname
- IP address spoofing
- IP aliasing
- IP multicast
- List of assigned /8 IPv4 address blocks
- Reverse DNS lookup
- Virtual IP address
- WHOIS

References

1. RFC 760, *DOD Standard Internet Protocol*, DARPA, Information Sciences Institute (January 1980).
2. J. Postel, ed. (September 1981). *Internet Protocol, DARPA Internet Program Protocol Specification* (https://tools.ietf.org/html/rfc791). IETF. doi:10.17487/RFC0791 (https://doi.org/10.17487%2FRFC0791). RFC 791 (https://tools.ietf.org/html/rfc791). Updated by RFC 1349 (https://tools.ietf.org/html/rfc1349), 2474 (https://tools.ietf.org/html/rfc2474), 6864 (https://tools.ietf.org/html/rfc6864).

3. S. Deering; R. Hinden (December 1995). *Internet Protocol, Version 6 (IPv6) Specification* (https://tools.ietf.org/html/rfc1883). Network Working Group. doi:10.17487/RFC1883 (https://doi.org/10.17487%2FRFC1883). RFC 1883 (https://tools.ietf.org/html/rfc1883).
4. S. Deering; R. Hinden (December 1998). *Internet Protocol, Version 6 (IPv6) Specification* (https://tools.ietf.org/html/rfc2460). Network Working Group. doi:10.17487/RFC2460 (https://doi.org/10.17487%2FRFC2460). RFC 2460 (https://tools.ietf.org/html/rfc2460).
5. S. Deering; R. Hinden (July 2017). *Internet Protocol, Version 6 (IPv6) Specification* (https://tools.ietf.org/html/rfc8200). IETF. doi:10.17487/RFC8200 (https://doi.org/10.17487%2FRFC8200). RFC 8200 (https://tools.ietf.org/html/rfc8200).
6. "IPv4 Address Report" (https://ipv4.potaroo.net/).
7. DeLong, Owen. "Why does IP have versions? Why do I care?" (https://www.socallinuxexpo.org/sites/default/files/presentations/Why%20IP%20Versions%20and%20Why%20do%20I%20care.pdf) (PDF). *Scale15x*. Retrieved 24 January 2020.
8. Y. Rekhter; B. Moskowitz; D. Karrenberg; G. J. de Groot; E. Lear (February 1996). *Address Allocation for Private Internets* (https://tools.ietf.org/html/rfc1918). Network Working Group. doi:10.17487/RFC1918 (https://doi.org/10.17487%2FRFC1918). BCP 5. RFC 1918 (https://tools.ietf.org/html/rfc1918). Updated by RFC 6761 (https://tools.ietf.org/html/rfc6761).
9. R. Hinden; B. Haberman (October 2005). *Unique Local IPv6 Unicast Addresses* (https://tools.ietf.org/html/rfc4193). Network Working Group. doi:10.17487/RFC4193 (https://doi.org/10.17487%2FRFC4193). RFC 4193 (https://tools.ietf.org/html/rfc4193).
10. R. Hinden; S. Deering (April 2003). *Internet Protocol Version 6 (IPv6) Addressing Architecture* (https://tools.ietf.org/html/rfc3513). Network Working Group. doi:10.17487/RFC3513 (https://doi.org/10.17487%2FRFC3513). RFC 3513 (https://tools.ietf.org/html/rfc3513). Obsoleted by RFC 4291 (https://tools.ietf.org/html/rfc4291).
11. C. Huitema; B. Carpenter (September 2004). *Deprecating Site Local Addresses* (https://tools.ietf.org/html/rfc3879). Network Working Group. doi:10.17487/RFC3879 (https://doi.org/10.17487%2FRFC3879). RFC 3879 (https://tools.ietf.org/html/rfc3879).
12. M. Cotton; L. Vegoda; R. Bonica; B. Haberman (April 2013). *Special-Purpose IP Address Registries* (https://tools.ietf.org/html/rfc6890). Internet Engineering Task Force. doi:10.17487/RFC6890 (https://doi.org/10.17487%2FRFC6890). BCP 153. RFC 6890 (https://tools.ietf.org/html/rfc6890). Updated by RFC 8190 (https://tools.ietf.org/html/rfc8190).
13. "DHCP and Automatic Private IP Addressing" (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc958957(v%3dtechnet.10)). *docs.microsoft.com*. Retrieved 20 May 2019.
14. S. Cheshire; B. Aboba; E. Guttman (May 2005). *Dynamic Configuration of IPv4 Link-Local Addresses* (https://tools.ietf.org/html/rfc3927). Network Working Group. doi:10.17487/RFC3927 (https://doi.org/10.17487%2FRFC3927). RFC 3927 (https://tools.ietf.org/html/rfc3927).
15. "Event ID 4198 — TCP/IP Network Interface Configuration" (https://technet.microsoft.com/en-us/library/dd379838(v=ws.10).aspx). Microsoft. 7 January 2009. Archived (https://web.archive.org/web/20131224215139/http://technet.microsoft.com/en-us/library/dd379838(v=ws.10).aspx) from the original on 24 December 2013. Retrieved 2 June 2013. "Updated: January 7, 2009"
16. "Event ID 4199 — TCP/IP Network Interface Configuration" (https://technet.microsoft.com/en-us/library/dd379922(v=ws.10).aspx). Microsoft. 7 January 2009. Archived (https://web.archive.org/web/20131222151743/http://technet.microsoft.com/en-us/library/dd379922(v=ws.10).aspx) from the original on 22 December 2013. Retrieved 2 June 2013. "Updated: 7 January 2009"
17. Mitchell, Bradley. "IP Address Conflicts – What Is an IP Address Conflict?" (http://compnetworking.about.com/od/workingwithipaddresses/f/ip_conflict.htm). About.com. Archived (https://web.archive.org/web/20140413194343/http://compnetworking.about.com/od/workingwithipaddresses/f/ip_conflict.htm) from the original on 13 April 2014. Retrieved 23 November 2013.

18. Kishore, Aseem (4 August 2009). "How to Fix an IP Address Conflict" (http://www.online-tech-tips.com/computer-tips/ip-address-already-in-use/). Online Tech Tips Online-tech-tips.com. Archived (https://web.archive.org/web/20130825040120/http://www.online-tech-tips.com/computer-tips/ip-address-already-in-use/) from the original on 25 August 2013. Retrieved 23 November 2013.
19. "Get help with "There is an IP address conflict" message" (https://web.archive.org/web/20130926071157/http://windows.microsoft.com/en-us/windows7/get-help-with-there-is-an-ip-address-conflict-message). Microsoft. 22 November 2013. Archived from the original (http://windows.microsoft.com/en-us/windows7/get-help-with-there-is-an-ip-address-conflict-message) on 26 September 2013. Retrieved 23 November 2013.
20. "Fix duplicate IP address conflicts on a DHCP network" (http://support.microsoft.com/kb/q133490). Microsoft. Archived (https://web.archive.org/web/20141228223206/http://support.microsoft.com/kb/q133490) from the original on 28 December 2014. Retrieved 23 November 2013. Article ID: 133490 – Last Review: 15 October 2013 – Revision: 5.0
21. Moran, Joseph (1 September 2010). "Understanding And Resolving IP Address Conflicts - Webopedia.com" (http://www.webopedia.com/DidYouKnow/Internet/2007/IP_Address_Conflicts.asp). Webopedia.com. Archived (https://web.archive.org/web/20131002155215/http://www.webopedia.com/DidYouKnow/Internet/2007/IP_Address_Conflicts.asp) from the original on 2 October 2013. Retrieved 23 November 2013.
22. M. Cotton; L. Vegoda; D. Meyer (March 2010). *IANA Guidelines for IPv4 Multicast Address Assignments* (https://tools.ietf.org/html/rfc5771). IETF. doi:10.17487/RFC5771 (https://doi.org/10.17487%2FRFC5771). ISSN 2070-1721 (https://www.worldcat.org/issn/2070-1721). BCP 51. RFC 5771 (https://tools.ietf.org/html/rfc5771).
23. RFC 2526 (https://tools.ietf.org/html/rfc2526)
24. RFC 4291 (https://tools.ietf.org/html/rfc4291)
25. Holdener, Anthony T. (2011). *HTML5 Geolocation* (https://archive.org/details/htmlgeolocation00iiia_202). O'Reilly Media. p. 11 (https://archive.org/details/htmlgeolocation00iiia_202/page/n19). ISBN 9781449304720.
26. "How to Find Your Public IP Address" (https://www.lifewire.com/what-is-a-public-ip-address-2625974#mntl-sc-block_1-0-38).
27. "Why Public IP Addresses Change" (https://www.lifewire.com/what-is-a-public-ip-address-2625974#mntl-sc-block_1-0-51).
28. Comer, Douglas (2000). *Internetworking with TCP/IP:Principles, Protocols, and Architectures – 4th ed* (http://www.cs.purdue.edu/homes/dec/netbooks.html). Upper Saddle River, NJ: Prentice Hall. p. 394. ISBN 978-0-13-018380-4. Archived (https://web.archive.org/web/20100413232359/http://www.cs.purdue.edu/homes/dec/netbooks.html) from the original on 13 April 2010.
