The Future of the Internet: IPv6

Keziah Knopp

August 2021

The internet was invented by the Advanced Research Project Agency (ARPA), funded by the US Department of Defense in 1969, as a means to communicate between multiple computers via packet switching. First established in 1990, the world wide web, commonly referred to as "the internet," has evolved significantly over time. Internet protocol (IP) sets a standard for communication across the internet. With the expansive growth of connectivity, the first publicly used protocol, IP version 4, has reached its limitations, and there is a need for a more encompassing internet protocol. The introduction of IP version 6 extends the capabilities of version 4 and adds new features which make communication easier and safer.

A set of protocols, known as TCP/IP were developed as standards for communication in 1983. TCP/IP is updated and maintained by the Internet Engineering Task Force (IETF) with Requests for Comments (RFCs). IP is a connectionless packet delivery protocol based on destination addresses. This protocol acts on best effort, meaning it does not guarantee the accuracy or delivery of information. Because of this unreliability, IP assumes that higher-layer protocols will account for any discrepancies. Transmission Control Protocol (TCP) is a higher-layer protocol that ensures a connection has been made before attempting to send any information. TCP includes congestion and flow control for data traffic, and in the process, avoids duplicating sent information. In the TCP/IP Five-Layer Networking Model (or the Open Systems Interconnection Model), internet protocol resides in the network layer, and TCP fits into the transport layer.

Due to tremendous growth of internet usage in the later 1990s, the protocol for communication needed to be broadly standardized. The first public, widely-used protocol was IPv4. Versions 1 through 3 of IP were experimental. IPv4 addresses consist of 32 binary bits, which translates to approximately four billion (4,294,967,296) possible internet addresses. Evolved from IPv4 in 1998, IPv6 is the next generation of internet protocol. Instead of the 32-bits of version 4, version 6 has an addressing scheme of 128 bits, which provides approximately 340 undecillion (340 x 10^{36}) possible addresses, 85 octillion (85 * 10^{27}) more addresses than IPv4.

These addresses are determined by one of three Regional Internet Registries (RIRs) that are geographically based. For example, the internet addresses used in the United States are assigned by the American Registry for Internet Numbers (ARIN). The other RIRs are Reseaux IP Europeans (RIPE) and Asian Pacific Network Information Centre (APNIC).

Information is sent according to the specifications of the protocol, using a system of addressing, similar to the US postal system. An IP address for version 4 is the set of thirty-two bits of binary digits. Those thirty-two bits consist of a network number and a host number. For an address to be more human-readable, it is written in dotted decimal notion. For example, an IPv4 address of 128.2.7.9 is equivalent to the binary of 10000000 00000010 00000111 00001001. The addressing system is written in colon hexadecimal notion. One IPv6 address looks like 3FFE:0000:0000:0001:0200:F8FF:FE75:50DF. To make these addresses more digestible, leading zeros can be trimmed, and consecutive zeros can be reduced to a double colon once per address. The same example can be expressed as 3FFE::1:200:F8FF:FE75:50DF.

Each device, router, or hub connected to the internet is assigned an address. With the postal system analogy, a person who mails a letter addresses the envelope with the destination address and their own address; much like a packet of information is addressed with a destination address and source address. Routers and hubs incorporated into the world wide web make the connections for the packet of information to get to its destination, like mailmen and post offices will do for mailing a letter. The Domain Name System (DNS) maps the numerical IP address to the human-readable address that is typed into a browser, such as www.ibm.com.

The host portion of the IP address is associated with the "local" device that is connected to the internet. Whereas, the network portion of the IP address is a region of the broader internet. To determine the host portion and the network portion of the IP address, IPv4 has a set of address classes, each with a set range for the network and host portions, as shown in Figure 1. The first few bits indicate the class of the IP address.

Class	**Address Range**	**Bit 0**	**1**	**2**	**3**	**4**	**…**	**8**	**…**	**16**	**…**	**24**	**…**	**31**
Class A	1.0.0.1 – 126.255.255.254	0	net ID					host ID						
Class B	128.1.0.1 – 191.255.255.254	1	0	net ID						host ID				
Class C	192.0.1.1 – 223.255.254.254	1	1	0	net ID							host ID		
Class D	224.0.0.0 – 239.255.255.255	1	1	1	0	multicast								
Class E	240.0.0.0 – 254.255.255.254	1	1	1	1	0	experimental							

Figure 1: IPv4 Address Classes

Classes A through C are used to connect to devices to the internet. Class D is reserved for multicasting, sending information to multiple receipts using one address for the group[1]. Class E is reserved for experimental use.

[1] (Price-Evans 2021)

IPv6 is divided in allocation spaces, similar to address classes, as shown in the figure below.

Allocation	Fraction of the Space	Bit 0	1	2	3	4	5	6	7	8	9	…
Reserved	1/256	0	0	0	0	0	0	0	0			
Reserved for NSAP Collection	1/128	0	0	0	0	0	0	1				
Aggregatable Global Unicast	1/8	0	0	1								
Link-local Unicast	1/1024	1	1	1	1	1	1	1	0	1	0	
Multicast	1/256	1	1	1	1	1	1	1	1			

Figure 2: IPv6 Address Allocations

All other IPv6 addresses are available to be assigned. The set allocations in Figure 2 make up less than 15% of the possible IPv6 addresses. In version 6, the host portion of the IP address is always 64 bits, and the subnet is the last 16 bits of the network portion. These numbers are defined in the packet header, which includes more specifications than IPv4, such as authorizations and encryption options. Each device, router, or host that is connected with IPv6 is called a node. Version 6 has stateless address autoconfiguration, where a node can configure its own address with an IPv6 router, as opposed to using a configuration server.[2] Duplicate address detection, available with version 6, ensuring the chosen address is unique on the local area network (LAN).[2] IPv6 messages can be encapsulated and sent over IPv4 routers; this process is known as tunneling.[3]

With the limited number of IPv4 addresses and the ever-expanding internet, subnets were developed in 1984 to allow for more flexibility within the IPv4 address classes[4]. The host number portion of the IP address is subdivided into a second network number and the host

[2] (IBM Corporation 2013)
[3] (Parziale 2006, 335)
[4] (Parziale 2006, 95-97)

number of the device. An IPv4 address with subnetting would follow the format: <network number><subnet number><host number>. Because the assignment of a subnet is done locally, there is no need to keep requesting more IP addresses from the network. The subnet and host section of the IP address appear as one location to the network, although the subnet may connect multiple hosts to the internet. The method of determining the host number separate from the subnet number is by using a subnet mask. A subnet mask is a binary number that can be used to identify which group of the IP addresses is the subnet, apart from the host. The number is listed after the IP address, following a forward slash: <IPv4 address>/<subnet mask>. In the example, 128.2.7.9/24, the "/24" represents twenty-four 1's out of the 32-bit number. This format is known as Class-less Inter-Domain Routing (CIDR). IPv6 also makes use of the similar variable length subnetting. An IPv6 subnet is limited to 16 bits or less and will be defined in the header. The IPv6 address will be written with CIDR notation, as well.[5]

There are different types of IP addresses that serve different functions. An IP address that is assigned to a particular interface on the internet is called a unicast address. A unicast address can be assigned to one device or an interface that the global network relates to as one particular host. A loopback address can test for communication between a server and client on a single machine; the addresses between Class A and Class B (127.0.0.0 to 127.255.255.255) are reserved for this purpose. Multicast addresses, indicated by Class D and one of the version 6 allocations, are used to send messages to all of the hosts on the same subnet or groups in which a host belongs. These types of addresses are helpful, but the reserved address space on IPv4 limits the space for other devices to connect to the network.

[5] (IPv6 - Subnetting 2021)

Network address translation (NAT) extends the breadth of IPv4 addresses by mapping of internal IP addresses to an assigned external IP address allowing for multiple hosts to access the internet with one public address. A device within the private network can request information that needs to be gathered from the public internet. A firewall, a device which monitors the flow of information to the private network, will request the information from the greater network and send it back to the device that requested it. This exchange happens without the public internet realizing the firewall is connected to several devices on the private network and without the private network realizing the information came from the broader, public network. This translation of IP addresses and transmission of information happens in an instant, and the end user is unaffected. With the large amount of space associated with version 6, NAT is not necessary, making it easier to connect nodes to the internet.[6]

Subnetting and NAT have increased the usability of IPv4 addresses; however the growth of the internet increases the complexity of these functions. IP address exhaustion is the phenomenon that all of the possible IPv4 addresses have been used up. The addresses are exhausted by regions, and for example, ARIN had completely exhausted IPv4 addresses by September 2015[7]. The number of internet users is only continuing to increase, an estimated 4.7 billion in 2021 and 5 billion in 2022. Following the trend, the number of devices connected to the internet is also dramatically increasing. With the internet of things (IoT) and machine-to-machine connections, an efficient and spacious form of communication is needed. It's estimated that more than 25 billion devices will be connected to the internet in 2022, paving the way for a new internet protocol.[8]

[6] (Parziale 2006, 89-95)

[7] (Huston 2021)

[8] (Cisco Annual Internet Report 2020)

There are similar categories of IPv6 addresses, such as unicast and multicast. The unicast addresses include global, link-local, and loopback ones. The multicast addresses consist of addresses for all-nodes, all-routers, and solicited node groups. Since multicasting can encompass all necessary addresses, there are no broadcast addresses in version 6, like there are in version 4. There is an anycast category, where an address can be assigned to multiple interfaces, and the sent message will be received by the nearest interface with that address.[9] Some IPv4 addresses have been mapped to version 6.

The IPv6 packet header is more strictly defined than IPv4 and allows for a number of extensions that enhance the capabilities of this protocol. The main portion of the header specifies necessary information: protocol version, traffic class, flow label, payload length, next header, hop limit, source address, destination address. The extension headers include the following: routing, fragmentation, authentication, encapsulating security payload, hop-by-hop options, and destination options. With a fixed size, the simplified packet header format makes it easier to process the information in the header and the payload. The extension adds a variety of features that IPv4 cannot address. The routing extension can be used to ensure routing specifics are included, such as loose source routing, where routers can be listed to hit across the network. The fragmentation extension indicates a payload will be sent through multiple packets. The payload is carefully fragmented. Routing and fragmentation are also available with IPv4.

Authentication and encapsulating security payload are special to version 6. The authentication header (AH) can be enabled for data origin checking and connectionless integrity[10]. It can be paired with the encapsulating security payload (ESP) header for further security measures. ESP can provide confidentiality or integrity for the data and for traffic flow or

[9] (Bahita 2013, 42)

[10] (Kent 2005)

a combination of both. The hop-by-hop extension headers specify parameters for the data payload at each router, or “hop,” along the path from source to destination[11]. Destination option header specifies parameters for either the final destination or intermediate stops, with certain processing or delivery function[12]. All of these extension headers improve the capabilities of internet protocol.

Although IPv6 was developed in 1998, it was not widely adopted until the late 2010s. The delay in adoption can be attributed to subnetting, NAT, and the process to adopt the technology.[13] Now, the number of IPv6 users is growing. By the end of 2020, approximately 35% of Google users are able to connect with IPv6. Most mobile carriers have adopted IPv6. The more IPv6 users there are, the more common it will become. According to Bahita[14], internet addresses with 128 bits are expected to last until the year 16285, so even with sets of reserved addresses, there are considerably more addresses available with version 6 than there were with version 4.[15] With the additional packet headers, IPv6 includes further security and efficiency benefits[16]. Ultimately, IPv6 allows for the continued, significant growth of the internet.

[11] (Davies 2012)
[12] (Kent 2005)
[13] (IPv6 Basics: What is IPv6 2020)
[14] (Bahita 2013)
[15] (Cisco Annual Internet Report 2020)

Bibliography

Bahita, Khaldoun. 2013. "Improving IPv6 Addressing Types and Size." *International Journal of Computer Networks and Communications.*

2020. "Cisco Annual Internet Report." *Cisco.* Accessed 2021. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

Davies, Joseph. 2012. "Understanding the IPv6 Header." Vers. 3. *Microsoft Press Store.* Pearson Education. June 15. https://www.microsoftpressstore.com/articles/article.aspx?p=2225063.

Google. 2021. "Google IPv6 Statistics." *Google.* March. Accessed March 2021. http://www.redbooks.ibm.com/abstracts/gg243376.html?Open&PDFBookmark.

Huston, Geoff. 2021. "IPv4 Address Report." May 27. Accessed May 27, 2021. https://ipv4.potaroo.net/.

IBM Corporation. 2013. "z/OS Communications Server: IPv6 Network and Application Design Guide." Vers. 2. *IBM Documentation.* September. Accessed 2021. https://www.ibm.com/docs/en/zos/2.1.0?topic=zcs-zos-communications-server-ipv6-network-application-design-guide.

2021. "IPv6 - Subnetting." *Tutorialspoint.* https://www.tutorialspoint.com/ipv6/ipv6_subnetting.htm.

2020. "IPv6 Basics: What is IPv6." *WhatIsMyIPAddress.* December 15. https://whatismyipaddress.com/ip-v6.

Kent, S. 2005. "IP Authentication Header." *Internet Engineering Task Force.* Network Working Group. December. https://www.ietf.org/rfc/rfc4302.txt.

Microsoft. 2015. "IPv6 Addressing." *Microsoft Docs.* November 18. https://docs.microsoft.com/en-us/previous-versions/aa917150(v=msdn.10)?redirectedfrom=MSDN.

Parziale, Lydia. 2006. "TCP/IP Tutorial and Technical Overview." Vers. 8. *IBM Redbooks.* Accessed 2021. http://www.redbooks.ibm.com/abstracts/gg243376.html?Open&PDFBookmark.

Price-Evans, Iwan. 2021. "What Is Multicast IP Routing?" *Metaswitch.* https://www.metaswitch.com/knowledge-center/reference/what-is-multicast-ip-routing.