IPv6 and ICMP

IPv6

Back in the 1990s it started to become apparent that we would eventually run out of IPv4 addresses. Those addresses are 32 bits, meaning there are around 4 billion addresses theoretically possible, though because of the way the address space was divided up, there are considerably fewer possible addresses. In the late 1990s, IP version 6 was developed to deal with the lack of addresses. Version 5 was the designation given to an experimental protocol that never went anywhere.

IPv6 simplified some facets of IP and replaced 32-bit addresses with 128 bit addresses. That means that whereas there are 2^{32} possible IPv4 addresses, there are 2^{128} possible IPv6 addresses. To give a sense for how large this number is, below we show what these values equal.

$2^{32} = 4294967296$
$2^{128} = 340282366920938463463374607431768211456$

Also, just for effect, here is what an IPv6 address would look like if written in the same notation as IPv4 addresses:

10.47.112.90
10.47.112.90.254.11.67.6.103.14.97.212.144.192.87.206

Dotted decimal notation is too unwieldy to use for IPv6 addresses, so a different scheme is used. They are broken into 8 groups of 4 hex digits. Here is an IPv6 address of Google, shown in two different ways:

2607:f8b0:4004:0802:0000:0000:0000:200e
2607:f8b0:4004:802::200e

The first way shows all 32 hex digits written out. IPv6 addresses tend to have long runs of zeros, and the address can be displayed in a shortened form called *zero-compressed form*, where a run of all zeros is replaced with a double colon (::). This can only be done once in the address, as otherwise it would be ambiguous. To convert a zero-compressed address into its full form, add enough zeros until you get 8 full blocks. The address abcd::1234 would require 6 blocks of zeros to get to 8 blocks, becoming abcd:0000:0000:0000:0000:0000:0000:1234.

IPv6 address structure CIDR notation is used for IPv6 similarly to how it is used for IPv4 but with one important difference. In IPv4, a /24 network has 24 bits for the network and $32-24=8$ bits for the host, meaning $2^8 = 256$ addresses on that network. In IPv6, a /24 would mean 24 for the network and $128-24=104$ bits for the host, meaning 2^{104} addresses on that network, a mindbogglingly huge number.

IPv6 addresses are generally broken up into 3 parts: 48 bits for the network ID, 16 bits for the subnet ID, and 64 bits for the host ID. Unlike in IPv6, this is not variable. The network portion of the address is never allowed past the 64th bit.

So if you ask for a block of addresses and get a /48, you will get a network large enough to accommodate 2^{16}=65,536 subnets of 2^{64} =18,446,744,073,709,551,616 hosts each. This is of course more than almost anyone would reasonably need, and it's led to some people complaining about the IPv6 address space being wasted in a similar way to how the IPv4 address space was initially wasted. IANA hands out networks to organizations that ask in sizes of /48 or possibly larger (like /32). You can't get something small, like a /104. The address space is really huge, so this doesn't seem to be a problem right now to be handing out such large networks.

The reason that such big networks are handed out is that it makes life a lot easier for routers. Routers use the network part of an address along with a routing table to know where to forward packets. The more complicated the routing scheme is, the larger and slower the routing table will be. The growth of routing tables is already a problem for IPv4, and people want to keep it from being a problem in IPv6.

Using IPv6 All major operating systems support IPv6. If your home router is fairly new, then it supports IPv6. Your ISP may support it or it may not.

Dual Stack is where a system can use IPv4 or IPv6 and can use whichever one it needs in a given situation. *Tunnelling* is used if you are on an IPv4 network and need to contact someone using IPv6. Since you're on an IPv4 network, you can't send an IPv6 packet directly, so instead you put your IPv6 packet into an IPv4 packet as its data. That IPv4 packet can then travel through your network, and when it gets to the transition point between IPv4 and IPv6, the packet is "unwrapped" and the IPv6 packet is pulled out of the IPv4 packet. Tunnelling is a broader concept than just this. It applies to any situation in which one type of protocol is hidden inside another. The concept is important in networking and security.

Though it's been around for over 20 years, IPv6 has still not taken over for IPv4. Currently (as of 2020), Google reports that around 1/3 of users accessing their sites are using IPv6, with the rest using IPv4. Part of the reason for this is that it takes some effort for network administrators to convert their systems from IPv4 to IPv6. As long as IPv4 still works, unless IPv6 provides them with some significant benefits, there's not much point in taking something that works and replacing it with a new system and all the glitches that come with doing something new. At least for now, though it's not perfect, Network Address Translation (NAT) seems to be solving the problem of the lack of IP addresses. NAT allows multiple users to share the same IP address. We will have more on it later. Another part of it is psychological. People are comfortable with IPv4 and IPv6, with its huge addresses, looks really strange.

The IPv6 header Below is what the IPv6 header looks like.

Ver.	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		
Optional additional headers...		

The version is set to 6. The Traffic Class and Flow Label fields are used to prioritize certain types of traffic over others. The Payload Length field is the length of the packet's data along with the length of any optional headers. It is 16 bits, which limits IPv6 packets to 65535 bytes. However, there is a jumbogram optional header that allows for larger packets. The Next Header field is used to help software process the headers and know where the packet data starts. The Hop Limit field is the TTL, renamed to more accurately describe its function.

The IPv6 header is considerably simpler than the IPv4 header. One of the goals of IPv6 was to simplify things for routers. Gone is fragmentation, which is moved to an optional additional header. In IPv4, fragmentation could be done by either the original sender or any of the intermediate routers, but in IPv6, it's only done by the original sender. The receiver is the one that puts the fragments back together.

Also missing from the IPv6 header is the checksum. The problem with the checksum in IPv4 is that the checksum is done on the header content, and the TTL changes at each router, so the checksum has to be recomputed by each router. This adds additional work for the router, which adds up when it's processing millions of packets. Both TCP and UDP, as well as layer 2, have checksums, which makes the IPv4 checksum is somewhat redundant.

Types of traffic IPv6 support unicast, multicast, and *anycast*. Anycast is similar to multicast in that the packet can go to multiple different destinations; however, instead of going to all of them, it goes to just one, whichever is the most convenient. It's a little like how a phone call to a help center could theoretically go to any of the lines in the help center, but it will end up going to the first available line. Note also that IPv6 does not specifically have broadcast addresses. Broadcast is achieved via multicast.

Internet Control Message Protocol

The Internet Control Message Protocol (ICMP) is a system by which hosts and routers can send status and error messages to each other. There are many different ICMP message types. Here we will cover the most important types.

Type	Name	Use
0	Echo Reply	This is the reply sent to a ping.
3	Destination Unreachable	This can happen in many different ways. A router may send this if you try to access a nonexistent host on its network or if you try to access a port on a host that is not listening for traffic. Another way is if a packet needs to be fragmented but the DF flag is set.
5	Redirect Message	This allows someone to inform a router of a more direct route to a destination.
8	Echo Request	This is a ping, used to send a quick message to another machine to see if it is listening.
11	Time Exceeded	This is sent if the TTL of a packet reaches 0.

Attackers often use the ping and traceroute tools to map out a network. Those tools use ICMP to do what they do, so network administrators will often configure their routers to not send ICMP messages. ICMP has also sometimes been used in denial of service attacks. The drawback of blocking ICMP is that it makes it harder to do legitimate networking things, such as path MTU discovery or diagnosing network connectivity problems.

Note: There is also ICMPv6, which is the version of ICMP that goes along with IPv6.