wightfibre
because we care

A Technical Guide to IPv6 in the WightFibre Network

IPv6 in the WightFibre Network

This White Paper serves as a primer on IPv6 for readers already familiar with IPv4

IPv6 is the most recent version of the Internet Protocol and supersedes IPv4. The main reason that IPv6 was developed was because of the explosion of Internet usage following the invention of the World Wide Web in the 1990's, which meant that it was forecast that the IPv4 Internet addresses would soon run out.

The Basics of IPv4

You are probably familiar with the 32-bit addresses that IPv4 uses that are normally expressed as four decimal numbers separated by dots to make them more humanly readable, for example 169.254.1.29.

The 32 bits means that there are theoretically 2^32 or a little over 4 billion addresses. In the early days the address space was carved up into sections or 'classes' with half the space carved up into 128 possible Class A networks which could have up to 16,777,216 devices attached, over sixteen thousand Class B networks which could theoretically each have up to 65,536 devices attached and over 2 million Class C networks which theoretically could each have up to 256 devices attached. The remainder of the address space was allocated to Class D (Multicast) and Class E (reserved).

So, you can see that as the Internet exploded the demand for IPv4 addresses would have quickly outstripped supply as in total there would have been only two million or so organisations in the world that would have been able to have networks, and they in turn would have been limited as to how many devices they could connect.

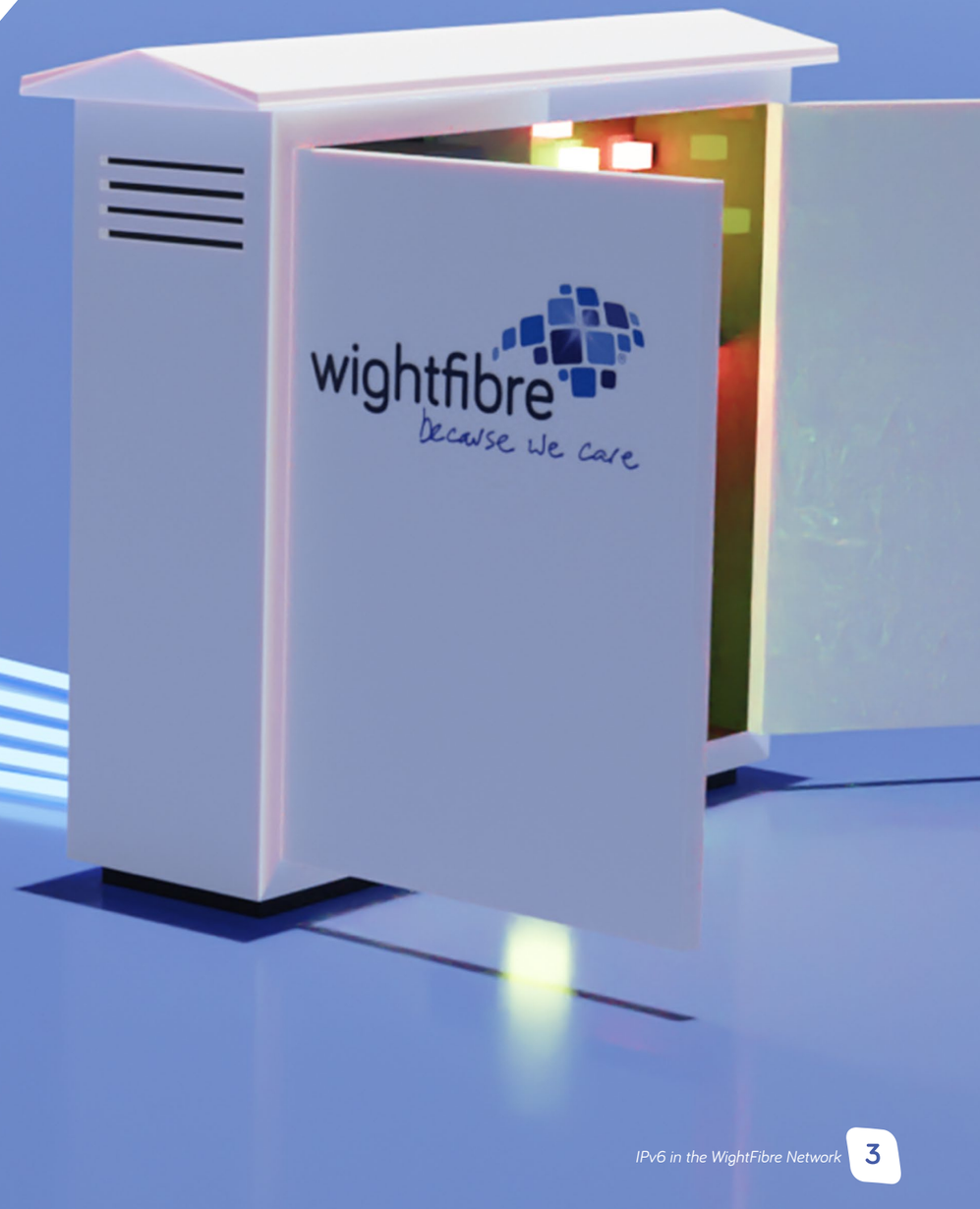
Luckily there were a few innovations introduced to get around this problem and some address ranges were assigned to special use; for example, the address above 169.254.1.29 is actually a Class B address and addresses in this range are typically ones that a device like a PC will give itself if it hasn't been allocated one by a network administrator or automatically via something called DHCP.

The Class A range starting 10.x.x.x and Class B range starting 192.168.x.x were allocated as 'private' addresses. If you ever look at the IP address given to your device in an office or connecting to Wi-Fi, you will most probably find it is one of these ranges. This means that an Internet Services Provider only needs to use one of its valuable 'public' IP addresses up regardless of how many devices its customer has. The customer's gateway will normally provide a Network Address Translation (NAT) function to map and route traffic between the public IPv4 address and one of the private IPv4 addresses.

A further issue that means IPv6 adoption is important is in the days of dial-up and early ADSL where the line was dropped when there was no activity, the ISPs could share IP addresses around multiple customers. Now, most customers are almost 'always on' and so almost every customer always needs a public IP address.

In a typical residential address or small business the 'router' that is provided by the ISP typically does 5 things.

1. It connects you to the Internet.
2. It provides Wi-Fi and possibly a handful of wired connections.
3. It provides Dynamic Host Configuration Protocol (DHCP). Basically, devices on the private network 'ask' the router for an IP address and the router uses this protocol to inform the devices the information it needs. As above it will normally be configured to allocate an address in the range starting 10.x.x.x or 192.168.x.x
4. It provides Network Address Translation (NAT). This is needed because you can't use the private address outside of the private network, so when your PC opens a connection, for example to get a web page, the router actually sends the request substituting its public IP address and keeps a record of which internal device sent the original request so when the reply comes back, it knows where to send it.
5. It acts as a DNS proxy. The Domain Name System (DNS) is the system that translates the easy to remember Internet domain names into the much more difficult to remember 32 bit addresses. For example, if you type google.co.uk the router will send the request to the domain name system and give your device the result translating it into the server address of one of Google's servers, e.g. 142.250.187.195



The Basics of IPv6

IPv6 doesn't just have 32-bit addresses, it has 128-bit addresses. This means that the number of theoretical addresses is more than three hundred and forty undecillion, two hundred and eighty-two decillion, three hundred and sixty-six nonillion, nine hundred and twenty octillion, nine hundred and thirty-eight septillion. Those are big numbers!

As a result, IPv6 addresses look a little bit more complicated than IPv4 addresses as they are written in eight groups with four hexadecimal digits in each group, separated by colons. For example:

2001:0db8:0000:0000:0000:8a2e:0370:7334.

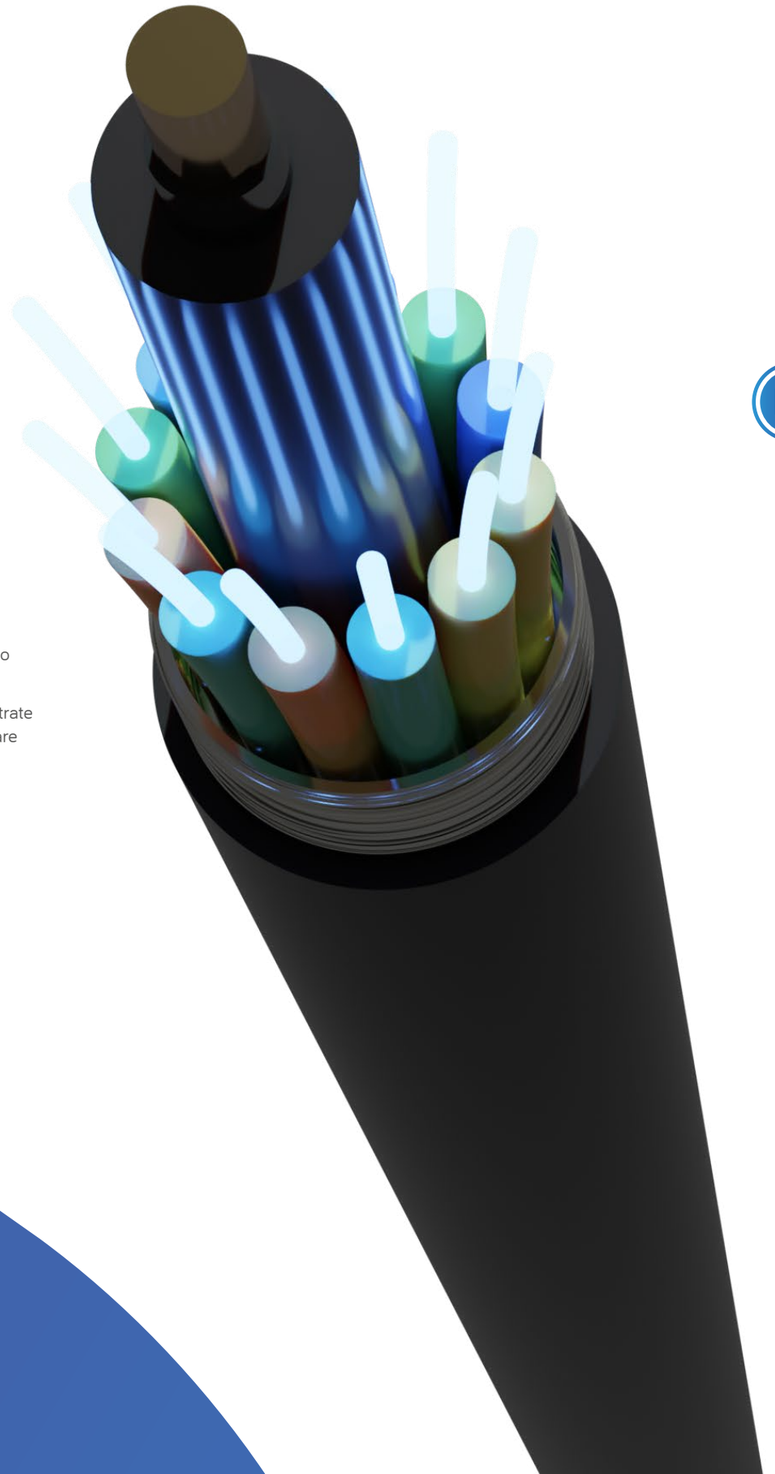
To make things simpler any leading zeros are normally omitted so this address would become

2001:db8::8a2e:370:7334.

The other thing that changes is how the number of addresses in any individual network or 'subnet' are specified. This can get a bit complicated! You may have seen in an IPv4 network configuration something called the subnet mask, for example 255.255.255.0. What this means is that in a network that starts 192.168.1.x you can't change the first three group numbers (where the subnet bits are all 1) but you can change the last group (where the subnet bits are all 0), in this case to form addresses from 192.168.1.0 to 192.168.1.255.

There is another way of writing this which is to count the bits that are set to one and write them after a forward slash symbol so a network with a subnet mask of 255.255.255.0 can also be written to say you have a /24 subnet. What this means is that 24 bits are fixed, but you can have an IP address made up by varying the remain bits (in this case 8), so again in a network specified as 192.168.1.x/24 the network addresses are from 192.168.1.0 to 192.168.1.255.

In the IPv6 world the mask method isn't generally used to illustrate the subnet as this would yield very big masks, so the subnets are defined using the forward-slash method.



Old IPv4 address example 169.254.1.29.

New IPv6 address example 2001:0db8:0000:0000:0000:ff00:0042:8329. Simpler form 2001:db8::ff00:42:8329.

The Advantages of IPv6

The most obvious advantage from all of his is it means that there are now more than enough addresses to go around and every device can have its own address.

At WightFibre we give you a /48 subnet which is a staggering 1,208,925,819,614,629,174,706,176 addresses!

Devices in IPv6 networks are able to configure themselves. This is called Stateless Address Auto-Configuration (SLAAC). This effectively allows devices on a network to select their own IP address automatically. The ability to statically assign addresses or use a version of DHCP for IPv6 still exists.

DHCPv6 is used to provide the subnet to both residential customers and businesses using something called DHCPv6 Prefix Delegation. In simple terms what that means is that the Customer Premises Equipment (CPE) in your network is given an address pool it can use (the /48 subnet) and the CPE in turn makes sure that the devices configure themselves so that their full 128-bit address is unique and within the subnet.

The upshot of this is that every device has a unique 'public' address, and this means you don't have to have Network Address Translation and can remove this bottleneck in your Internet connectivity. The CPE acts as a firewall and can block access to specific ports making your network safe. Instead of port forwarding, you simply have to allow access to the client device via the firewall making configuration simpler and routing quicker. It also deals with the issue in instances where you might want to forward the same port to more than one address.

Another benefit of IPv6 is that regardless of NAT, packets can be routed more quickly. This may seem counterintuitive as IPv6 has a 128-bit address rather than the 32-bit address of IPv4, but the address is just part of the header and actually IPv4 weas developed with quite a complex header structure with other data blocks that are relatively rarely used but which need to be examined by routers because the header size is actually variable. The simpler approach of IPv6 with a fixed header size (and other factors such as Quality of Service) means that the address can be read, often by dedicated hardware, and the packet forwarded on more quickly.

IPv6 also has something called a 'flow label' in its header. This means that true quality of service can be implemented at the network layer as touched on above.

Finally, Security. IPv6 has Internet Protocol Security (IPSEC) 'baked in'. In fact IPSEC was originally designed for IPv6 and only later adapted for IPv4. This means that you can configure direct peer to peer secure connections over IPv6, obsoleting the need for VPNs for example if you have satellite premises or are working from home.

wightfibre
because we care

01983 300 000

www.wightfibre.com