



Implementing IPv6 in the Enterprise A Planning Guide

1. Deciding where to use IPv6

You could use IPv6 in one or more of the following ways:

- IPv6 outward connectivity

To enable your staff or extranet partners to access IPv6 services in the outside world.

- IPv6 for customers to access to your services

Running IPv6 on your web services or other online systems, to enable IPv6 customers to talk to you. This is particularly important if you are targetting developing economies, where IPv6 takeup is more prevalent.

- IPv6 for internal network management

This is an excellent way to gain experience in using IPv6 and solve the initial technical and operational difficulties. It can also free up valuable IPv4 addresses for reuse elsewhere in the enterprise.

- IPv6 for a private network

If you are considering building a new private network, either within your organisation or across partners or on behalf of a customer, then IPv6 is the logical choice. It will be future-proofed, not limited by IPv4 scarcity and valuable experience for using it in the rest of your enterprise.

2. Writing the IPv6 Implementation Plan

Your IPv6 implementation plan should contain the following stages:

- Applying for addresses

IPv6 addresses are not available to enterprises to 'own' in the same way some 'own' IPv4 addresses independently of any ISP. They are only provided to enterprises that intend to supply them to other organisations.

If you are an enterprise that has your own “provider independent” allocation of IPV4 addresses for your internal network then you may not be able to establish the same IPv6 infrastructure. You may need to consider having a subsidiary operating entity apply for the addresses to then supply to the rest of the enterprise.

- Check connectivity from ISP(s)

Not all ISPs provide IPv6 and those that do, do so in a variety of ways. It may be that moving ISPs to get dual support, aggregated bandwidth or integrated billing, may be beneficial.

- Assess impact on technical staff

IPv6 is not one of those technologies that can be picked up from reading a Wikipedia article, there is a lot more to it.

- Design an addressing scheme and address management system

IPv6 addresses are very different from IPv4, other than just being longer, and there are several important things to consider (more details below).

- Check off-the-shelf equipment and applications for IPv6 compatibility, upgrade as necessary

When you investigate it is surprising just how many off-the-shelf applications or systems use IP address information. Do not assume that a whole class of applications can be excluded from your checks.

- Check internally developed applications, upgrade as necessary

Hopefully this is something you will have better control over.

3. Applying for addresses

Many enterprises have an ISP, who provides them both connectivity and IPv4 addresses as a package. In this case, very little changes as it should be the ISP that supplies IPv6 addresses and connectivity. If they don't then you will need to consider changing ISP, with the downside of probably having to change your IPv4 addressing, or using a secondary ISP solely for IPv6.

Some enterprises, particularly the larger ones, have their own ISP-like infrastructure operating as a Local Internet Registry (LIR). This infrastructure comprises an Autonomous System number, a portable IP address allocation, Internet transit connectivity and a peering arrangement with ISPs and other enterprises. These enterprises have the most difficulty in implementing IPv6 as they cannot get IPv6 addresses on the same terms. The rules for IPv6 are that you must either¹:

¹ <http://www.apnic.net/policy/ipv6-address-policy>

- *Have a plan for making at least 200 assignments to other organizations within two years OR*
- *Be an existing LIR with IPv4 allocations from an APNIC or an NIR, which will make IPv6 assignments or sub-allocations to other organizations and announce the allocation in the inter-domain routing system within two years*

Some might have an operating unit that operates with some form of cross-charging, which could apply for the addresses.

4. Checking connectivity

The following checklist should aid in checking connectivity:

- Does your current ISP support IPv6?
- Does it come at additional cost?
- Does it use the same infrastructure as the IPv4 service (especially international transit routes)?
- Is billing integrated with IPv4 service?
- Are bandwidth calculations aggregated with IPv4 service?
- Are volume calculations aggregate with IPv4 service?
- Does it have the same support SLA as the IPv4 service?

5. Assessing the impact on technical staff

IPv6 is very different from IPv4 and technical staff will need proper training on IPv6 to even begin to understand it. Beyond that it is likely they will continue to learn new things all the time and they should be helped in that learning and encouraged to help colleagues by recording their knowledge.

Here are just a couple of examples of how it differs from IPv4:

- Whilst the new IPv6 address is 128 bits long (up from 32 bits in IPv4) only the first 64 bits are equivalent to the old IPv4 addressing scheme. In IPv6 addresses the last 64 bits are a new concept of host identifiers, with no equivalent in IPv4.
- IPv6 addresses are written with colons (:) in between groups of four characters of the address. However Microsoft Windows does not allow colons in path names and so Microsoft has provided a clever workaround, but not one that could be guessed at.

If you enter an IPv6 address as a special domain name: for example

2001:0db8:85a3:08d3:1319:8a2e:0370:7348

as

2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net

then Windows will automatically translate it to the IPv6 address.

With IPv4 certain working habits have built up amongst technical staff. For example many of them can remember important IPv4 addresses or do some calculations in their heads. With IPv6 they might need specialist tools to manage the addresses and a carefully chosen address scheme to help them remember it.

6. Designing an addressing scheme

This is an area where spending time now could save huge problems in the future. Here is a checklist to get you started:

- Relationship between IPv4 addresses and IPv6 addresses on the same network.

Without some relationship it will not be easy for technical staff to spot any correlation between problems on the same network as being on the same network, just in different address spaces.

Some technical solutions are possible (IPv4 mapped addresses) but these are not available for all systems.

- Filling the reverse address space

With IPv4 many enterprises just fill the whole reverse address space to prevent enumeration of active hosts. With IPv6 this is impractical as the space of address is too large, so a decision on how to manage reverse address space must be made. One good suggestion is to randomly fill the IPv6 reverse space to mask active nodes.

- Use of NAT and private addresses

Lots of enterprises use NAT for very good reasons to hide internal address space. They generally use RFC1918 private addresses internally and then NAT through to a small number of 'real' IPv4 addresses.

IPv6 does not have RFC1918 private addresses to use in the same way. It did have once but they were removed. It now has "unique local addresses" but those still have global scope even if they should not normally be routed.

NAT has been the subject of strong debate within the Internet community for many years, with strong arguments on both sides. With IPv6 an attempt has been made to eliminate it² but support for it does exist in some networking equipment, though if you intend to use it is likely to be in a different way from its use in IPv4.

- Address allocation

² <http://tools.ietf.org/rfc/rfc4864.txt>

IPv6 has DHCP (called DHCPv6) as IPv4 does but it also introduces “stateless address autoconfiguration”, which should be used in preference to DHCP as it is simpler and easier to support.

- Minimum site allocations, point to point links etc

IPv6 has special provisions for site-to-site addressing and recommends a general allocation of /48 per end site. This is a good starting point for your own internal standards.

- DNS support

In order to run IPv6 your DNS will need to support AAAA records. If you have a DNS/IP address management system then that will need to support IPv6.

- Privacy considerations

You should pay special attention to last 64 bits of IPv6 addresses, the host identifiers. In early implementations of IPv6 these were automatically set to the MAC address, which meant that an individual computer could be tracked across multiple IPv6 networks because a MAC address is globally unique.

A standard solution does exist in RFC3401 but this is not very well supported. Other obfuscation solutions are in place but some of them appear trivial to decode.

A final warning about online resources. A lot has changed in IPv6 since it was first introduced and there is a lot of out of date information around (like the obsolete A6 record in DNS).

7. Checking off-the-shelf equipment compatibility

Much equipment includes IPv6 support and has done for many years. There are however still a number of issues to watch for, particularly with the cheaper ‘consumer’ oriented equipment. A good checklist is:

- Is IPv6 supported out of the box or is an upgrade required and if so then is the upgrade free now and will it remain free?
- Are all the same features supported with IPv6 as IPv4?
- Can the equipment run IPv4 and IPv6 at the same time?
- Does the equipment maintain the same performance with IPv6 as IPv4?

8. Checking application compatibility

Every application you use, whether off-the-shelf or internally developed needs to be checked to see it uses IP address information. There are several ways in which an application might use this information:

- some record IP addresses of client connections such as web server logs or access logs on security appliances
- some access control systems, such as dongles or 'phone home' technology use IP addresses

You should also be aware that it is not just the addresses that are different but some of the algorithms for manipulating them are different. In IPv4 if two addresses are the same then they are the same machine but with IPv6 only first 64 bits matter for this.

9. Conclusion

A proper implementation of IPv6 will future-proof your enterprise for years, but it is a complex process and should be planned thoroughly. Hopefully this planning guide will make that easier.

Written by .nz Registry Services, a wholly owned subsidiary of InternetNZ that operates .nz.