Whitepaper
on
IPv6 Adoption by New Zealand Enterprise

Prepared by

The New Zealand IPv6 Task Force

In conjunction with

InternetNZ

Version 1.0 April 2013

1. Introduction

This whitepaper has been prepared by the New Zealand IPv6 Task Force (see Appendix A) in conjunction with InternetNZ to be used as a primer for enterprises in New Zealand, to encourage them to adopt IPv6 in a cost effective and low risk manner. It is expected to provide a roadmap for the adoption of IPv6. The target audience for this message is any organisation which uses Internet Protocol technology within New Zealand.

2. The Problem

The Internet is now a pervasive tool for the support of all types of business, government and consumer activity throughout New Zealand and around the world. It would be hard to imagine our daily routine without the use of the Internet.

The Internet is based on a specific set of protocols, which are standardised globally and enable the Internet to transparently interchange all types of information seamlessly between users, who may be located anywhere in the world. One of the primary standards supporting the Internet today is defined as Internet Protocol version 4 (or IPv4). This protocol defines how users of the Internet are uniquely addressed. It supports about 4 billion unique IP addresses.

The amazing growth in the use of the Internet over the last couple of decades has meant that these 4 billion unique addresses are now used up. On 4 February 2011, the global allocation body for Internet addresses (called the Internet Assigned Numbers Authority - IANA), exhausted its allocations of these IPv4 addresses. Hence there are no longer any IPv4 addresses remaining in the global pool.

Internet addresses are allocated on a regional basis by Regional Internet Registries. New Zealand lies within the allocation coverage area of the Asia Pacific region administered by the Asia Pacific Network Information Centre (APNIC). This region encompasses some of the largest developing economies, such as India, China and Indonesia, so is an enormous and growing user of Internet addresses. It is not surprising that it was the first regional registry to reach exhaustion of the original, IPv4, addresses. Today, APNIC has implemented austerity measures which mean that new and existing members are only entitled to an additional 1024 IPv4 addresses.

In practical terms, the supply of new IPv4 address allocations has essentially been exhausted. However, it must be emphasised that this does not mean that there are no longer IPv4 addresses available for use by many entities around the world, including within New Zealand. Many Internet Service Providers (ISPs), telecommunication service providers and other organisations within New Zealand will continue to have some stock of IPv4 addresses for local use, for some time to come, possibly several years.

However, this remaining address stock does not exist uniformly across organisations within New Zealand and certainly not across the globe. This is especially true for those countries where economic growth and the use of the Internet is expanding rapidly, such as in China and India. Many organisations in these countries will need to find IP addressing alternatives soon, and the number of such organisations is expected to expand rapidly over the next few years around the globe.

The same situation will emerge in New Zealand over the next few years, with the growth of more devices, mobile and machine to machine (m2m) interaction, consuming the remaining IPv4 addresses.

3. The Solution

Fortunately, there is a solution to the exhaustion of IPv4 addresses. Over a decade ago, this situation was predicted and the Internet Standards Organisation developed a new protocol to extend the life of the Internet for many more decades into the future. This new protocol is called Internet Protocol version 6 (or IPv6) and is being adopted slowly, but surely, around the globe today.

The IPv6 protocol increases the address range from 4 billion to around 340 trillion, trillion, trillion addresses. This is an enormous number and should enable the Internet to deliver current and new services well into the future.

Unfortunately, the adoption of this new protocol is not seamless, in that it is not backward compatible with IPv4. It essentially creates a new Internet, which sits alongside the existing Internet. Most functions and features of this new Internet look and feel to end users much the same as those of the old Internet. However, the users on the existing IPv4-based Internet cannot communicate directly with users on the new IPv6-based Internet. It is critically important therefore, that all New Zealand organisations and network providers adopt IPv6 for use in conjunction with IPv4. This will ensure end users will continue to be able to connect with any other user on the Internet. Otherwise the most important feature of the Internet, its ubiquity, will be compromised.

Even if IPv4 exhaustion is not an immediate problem for your organisation, every organisation and user of the Internet needs to consider the potential impact of the loss of ubiquity which staying with IPv4-only will cause.

Commencing in 2011, there are organisations around the globe that only have access to IPv6 address allocations. Hence they are developing services and applications based on this address space only. Those organisations that remain without IPv6 visibility will not be able to see and take advantage of these new services and applications.

Over time, it is expected that these new IPv6-based services and applications will rapidly grow, while those developed specifically for the IPv4-based Internet will slowly diminish. The greatest innovation will occur on the IPv6-based Internet, while innovation on the IPv4-based Internet will stagnate and slowly die.

This trend is already starting to occur, with many of the most recent innovative applications being delivered using IPv6 only. This includes applications such as Microsoft's "Direct Access" which comes bundled with all the latest versions of the Microsoft operating system, through to the next generation of mobile telephony and data technology. Many of the next generation of Internet applications will require IPv6 in order to function properly. This makes it essential for all organisations to understand the issue and risks, and plan their adoption of the IPv6-based Internet – it is not a matter of if, but only when.

In a survey of enterprises in the United States back in July 2011, 92% of the 210 respondents agreed with the following statement: "IPv6 is fundamentally important to the future of the Internet"

(Network World survey, July 2011). Today we have the launch of LTE based mobile services by the two leading mobile operators in New Zealand and in line with strong international trends they will launch with IPv6 capable networks. Hence the reality of IPv6 adoption is emerging. The sheer scale of the emerging "Internet of Things" makes IPv6 adoption mandatory in the longer term.

4. When to Adopt IPv6

The adoption of IPv6 within any organisation is inevitable – it is only a matter of when to undertake this implementation. For any given organisation, the adoption of IPv6 can vary from being very simple to very complex, depending on:

- How IPv4 addresses are embedded within your organisation's ICT infrastructure and applications.
- The extent of this infrastructure and its associated applications suite within your organisation.
- The extent to which your organisation manages its own network and or relies on outsourcing (impacts knowledge / skill-set requirements).

Experience from around the world has shown that whatever the situation within your organisation, it is best to commence an adoption strategy earlier rather than later. **Delaying adoption will almost certainly increase the risk that the business will be constrained in some way in the future and the cost for implementation will increase over time**.

Another factor that supports moving early is the lag relating to knowledge uptake and institutionalisation of that knowledge, particularly as it relates to building the technical skill-sets required for planning and implementing a transition. It takes time for new skills to become pervasive across any organisation. So this is another good reason to start early on the adoption journey.

The worst outcome in terms of cost impact and potential for business disruption is to leave the adoption until some external event forces the timing. Such an event is inevitable, but the timing and severity will be different for every organisation. Hence prudent business risk management always suggests planning for adoption as soon as possible. This will always be the lowest risk and lowest cost approach. How to minimise the cost of adoption is developed further in the following sections.

5. Pre-requisites to IPv6 Adoption

5.1. Overview

The adoption of the IPv6 protocol within any business is best undertaken using the following well-proven approach. Every organisation will be different in terms of detail, but a single high-level approach can be adopted universally. The first step in the journey is to undertake a number of pre-requisite steps as follows:

- Gain senior management commitment to the need for IPv6 adoption across the business. (Refer to Appendix B - Successful strategies - T. Limoncelli & V. Cerf).
- Based on the senior management commitment, allocate specific resource to achieve the required outcome (this may include both internal and external resource).
- Ensure that the allocated resource is adequately trained in IPv6 technology to ensure a successful outcome.

- Undertake an audit of the use of IPv4 addresses across the business in order to identify where IPv6 addresses will need to be adopted within the business.
- Establish an internal business policy that ensures that IPv6 adoption is included as part of any procurement, refresh, upgrade or rehabilitation of any ICT infrastructure or application.
- Establish a commitment to develop a planned approach to the adoption of IPv6 in association with any ICT procurement and refresh cycles.

It should be noted that this process may not be a linear one, nor occur in any particular order. There may be feedback loops and iterations at any point (particularly if the knowledge base of stakeholders is relatively low to begin with). For example, impacts / risks to critical business applications may not be fully understood until the internal knowledge base has grown sufficiently, or has been augmented with external expert advice.

5.2. Senior Management Commitment

The senior management commitment to the adoption of IPv6 within the organisation is essential to ensure that adequate resource is committed to the program and success occurs within an agreed timeframe. It is also essential that senior management understand the risks to the business associated with not adopting IPv6 and with the process of adopting IPv6. In both cases, there are significant risks, ***but it needs to be emphasised that the risks associated with not implementing or delaying the implementation of the adoption of IPv6 increase exponentially over time.***

Getting senior management commitment to the adoption of IPv6 may require some form of education program, so that the basics of this change are understood. This includes both the scope and impact of the change at a business and technology level. In particular, it is essential that the risks of not undertaking the required change or delaying it are fully understood in business terms.

5.3. IPv6 Training

Training for people at all levels of an organisation needs to be an essential ingredient of any IPv6 adoption plan. It is difficult to understand business impacts and assess real risks and opportunities without this knowledge. It is important, for instance, that senior management have a broad understanding of the key issues, while more technical members of staff have a detailed understanding of the technical requirements and implications for ICT infrastructure and applications.

Even when much of the actual work to be undertaken as part of an adoption plan is to be outsourced, it is still essential that some selected internal resource are familiar with the detailed issues involved, so that they can intelligently manage the risks to the business associated with the change. Failure to have an expert either in-house or contracted may lead to confusion in requirements and adoption approaches throughout the adoption strategy and planning. There needs to be a ‘Go To’ expert that controls the strategy, plan and its execution.

5.4. The Audit

There are a number of well-defined procedures available for undertaking a thorough audit of all infrastructure and applications to identify the precise impact of IPv6 adoption within a particular organisation. The critical issue is to identify where and how IP addresses are used within the ICT capability used by the business and which business functions / operations will be affected. This, in turn, provides visibility of risk exposure. A thorough review of the following business infrastructure is recommended:

- External facing websites,
- Internal (intranet) websites,
- Local Area Network (LAN) facilities,
- Wide Area Network (WAN) facilities,
- Internet gateway facilities, including firewalls and related cyber security facilities,
- Application server and storage facilities,
- Telecommunication facilities.

The most critical issues to identify are where IP addresses are "hard" coded into applications and infrastructure. These situations will be the hardest to address in an adoption programme.

Support for the audit process is available from a number of service providers and system integrators, including some of those listed on the www.IPv6.org.nz website.

5.5. Procurement Guidelines

The best way to facilitate change is to ensure that the required change is integrated into technology procurement processes. This is absolutely true for the adoption of IPv6. Most new equipment today (but not all – see below) can be purchased to be fully compatible with the IPv6 protocol. Typically this will involve functionality that delivers a "dual stack" approach which provides both IPv4 and IPv6 capability in parallel within the same facility. This dual stack approach is the preferred approach for the adoption of IPv6, as it ensures seamless compatibility with both the old and the new Internet (providing you have sufficient IPv4 addresses for any new services). Furthermore, when technology is purchased that has IPv6 as an inherent capability, the cost of this capability is either a very small increment on the cost for IPv4 only equivalent technology, or in many cases has no cost impact at all. Hence purchasing new technology with IPv6 incorporated is the lowest cost approach to the adoption of IPv6. If the purchase of this technology is done as part of normal technology refresh cycles within the business, then this will make the adoption of IPv6 minimum cost overall. In a recent survey of enterprises in the United States, 60% of the 210 respondents **disagreed** with the following statement: "I expect the upgrade to IPv6 will involve a big investment in new hardware and software" (Network World survey, July 2011).

As an example, a case study from Tauranga City Council indicates that a network of 40 switches, 30 Layer 3 VLANs and approximately 110 servers servicing 650 staff can be migrated to a dual stack deployment by one trained person over the course of a year, without needing to work full time on the migration. This, of course, assumes that suitably compliant equipment had been purchased prior to commencement of the full adoption project.

It is essential to ensure that procurement procedures within any organisation includes an approach to purchasing that ensures that all technology purchased is IPv6 compatible. The sooner that this procedure is put into place, the sooner all technology across the business will be replaced with IPv6 compatible technology. Refresh cycles take some years to complete within most organisations, so the sooner the right procurement procedures are put into place, the better the outcome.

There are several guidelines available to assist making procurement procedures IPv6 compatible. It is strongly recommended that these be reviewed and adapted to a given organisation's procurement procedures at the earliest possible opportunity.

The most cost effective way to adopt IPv6 is to ensure that any change to the ICT infrastructure and application suite is done with IPv6 adoption as a specific requirement. In this way the adoption will occur continuously, but at a pace which is appropriate to the particular business. The end goal may take some time (possibly several years) to complete, but every dollar spent over this period will be spent with the right outcome in mind.

The IPv6 Task Force website (www.IPv6.org.nz) offers a couple of approaches which have been taken to procurement from different parts of the world. A simple approach has been adopted by the Tasmanian State Government (www.egovernment.tas.gov.au/__data/assets/pdf_file/0017/113237/IPv6_procurement_and_audit_standards.pdf) while the Europeans are promoting a more comprehensive approach (http://ripe.net/docs/ripe-501.html).

5.6. Key Insights

During the pre-requisite phase, it is useful to always keep in mind, the following key insights related to IPv6 adoption:

1. Keep reminding your organisation about IPv6:
    - Without a dedicated champion we know you will find this to be very difficult.
2. Remember to include IPv6 in the 5 P's:
    - Policies,
    - Procedures,
    - Procurement,
    - Planning,
    - Projects.
3. Think big, but **START SMALL**
    - External facing web sites are the best place to start,
    - Do not overwhelm your investment manager with the need for a BIG $ investment, you may never get started.

6. Planning for adoption

6.1. Overview

Once the pre-requisites have been established, it should be possible to develop a plan for the adoption of IPv6 across the business. If there is no specific timing constraint for IPv6 adoption, then the timing for the key steps in the plan should be integrated with the normal technology and workforce skill-set refresh and upgrade requirements as defined by the business. This is by far the lowest cost and lowest risk approach to the adoption of IPv6. Alternatively, there may be some specific business initiatives overlaid on the normal technology refresh cycles, which relate to IPv6. For example, it may be desirable to undertake some specific work on making external websites IPv6 enabled, as a specific business priority.

Given the key principle above, the components of any plan will include the following:

- External website upgrade,
- Service provider provision of dual IPv4 and IPv6 backhaul,
- Internal website upgrade,
- Wide Area Network dual stack upgrade,

- Local Area Network dual stack upgrade,
- Internet Gateway dual stack upgrade,
- Business application suite upgrade.

Each of these components is described briefly below. A typical approach to IPv6 adoption is also outlined in Appendix C attached, as derived from the IPv6 website.

6.2. External Website Upgrade

The enabling of external websites to support IPv6 is considered by many businesses to be the most important first step in IPv6 adoption. This step ensures that the business remains visible to the entire Internet population worldwide. Furthermore, enabling external websites to be IPv6 compatible is not normally a large exercise for most organisations. Modern websites are usually readily made IPv6 compatible at a very small incremental cost.

The biggest challenge can be when websites are hosted by a third party who is not ready to adopt IPv6. In the past, this could be a challenging situation to resolve. However, clients should apply pressure to have this situation resolved in an agreed timeframe, as there is no excuse for intransigent behaviour by hosting service providers today.

One of the most common excuses for not moving to enable IPv6 websites was the lack of native IPv6 backhaul. This applied to both internal and external hosted services. However, as discussed below, this is no longer a valid reason for not progressing this aspect of the adoption plan in a timely manner.

6.3. Service Provider IPv6 Backhaul

In order to successfully adopt IPv6 within a business, it is essential to have a telecommunication and / or Internet service provider that supports native IPv6 backhaul. In the past, such service providers have been hard to locate in New Zealand. However, more recently, service providers have begun stepping up to the mark, so that now a wide variety of service providers offer suitable services into the market. A list of some of these can be found at http://www.ipv6.org.nz/service-providers/ website.

6.4. Internal Website Upgrade

For many companies, it is convenient to upgrade internal website capabilities at the same time as the external website capabilities are upgraded. Often they are supported by the same service provider and may be hosted together.

6.5. Wide Area Network Upgrade

The upgrade of Wide Area Networking (WAN) capability will require close cooperation with one or more telecommunication service providers and ISPs. Appendix C provides an outline of the step by step process required to achieve this outcome, including:

- Developing an IPv6 address plan,
- Getting IPv6 address allocations from either an ISP or direct from APNIC,
- Implementing the plan,
- Testing to ensure the required outcome is achieved.

The most important issue to consider as part of this activity is the capability of your upstream service provider(s). It will be very difficult to progress this step unless the upstream service providers support IPv6 natively in a dual stack configuration. Even then it is likely that in the near term the routing for IPv6 traffic may not be as efficient as that for equivalent IPv4 traffic. This arises due to the need to tunnel IPv6 over IPv4 to reach some destinations and end users.

6.6. Local Area Network Upgrade

Once the Local Area Network (LAN) equipment has been upgraded to support both IPv4 and IPv6 in a dual stack configuration, it will then be a matter of establishing the IPv6 address tables in alignment to those for IPv4 (hopefully largely using IPv6 DHCP) and then turning the IPv6 functionality on and testing its end-to-end integrity.

This may be a later step in the IPv6 adoption programme, as it will usually be best to ensure the outward facing aspects of the ICT infrastructure are made operational with IPv6 first before looking back into the internals of the ICT infrastructure.

6.7. Internet Gateway Upgrade

The Internet Gateway into any organisation is a critical part of the ICT infrastructure today and usually also incorporates the security perimeter for the organisation. Thus it is important to plan this part of the infrastructure upgrade very carefully. It will also be essential to ensure that your upstream ISP is fully engaged in the process and is able to support both the IPv4 and IPv6 protocols simultaneously.

An important consideration is the upgrading of the security features of the network to support IPv6 and IPv4. Up until recently, some security devices (e.g. Firewalls, IDS, IPS, etc) have been lagging in IPv6 functionality and if your security infrastructure is aging then this may be a problem. It will be essential to ensure that there is full support for IPv6 within the security infrastructure before commencing any change in this space. Even where support is claimed, this still may be one of the more challenging areas to upgrade, so due care is essential.

6.8. Business Application Suite Upgrade

Many applications within any business will be readily upgraded to support IPv6 through appropriate reconfiguration of DNS and DHCP servers. However, there will be other applications where the addressing is more integral to the application and the support for IPv6 is lagging. This can apply in a variety of situations, including:

- Certain types of web servers,
- Legacy applications and associated host platforms.

It is recommended that the audit process be used very diligently to identify these potential bottlenecks at the earliest possible opportunity so that remedies can be developed in a timely and cost effective manner. It may well be that for some applications, the only cost effective approach is the quarantine the applications within an IPv4 only domain and to provide IPv6 to IPv4 Network Address Translation (NAT) for these applications through to end of life. Given that these applications are likely to be in the older category, the use of NAT is unlikely to provide noticeable performance degradation, as might be the case for some modern applications.

Where applications are upgraded to be IPv4 and IPv6 capable, it will be necessary to test the applications thoroughly with both protocols before committing to full production within the business.

7. Executing the Plan

As identified above, it is almost always most cost effective to implement the adoption of IPv6 alongside other technology refresh and upgrade cycles. Hence it is likely in many businesses that the adoption of IPv6 commences well in advance of any actual use of IPv6 within the business. Given typical technology refresh cycles of between 3-7 years, it may take several years before sufficient technology is IPv6 compliant so that these features can be turned on and used to deliver end-to-end IPv6 compliant services.

The typical refresh and upgrade activities which provide an opportunity for the adoption of IPv6 compliant technology include:

- Periodic refresh of websites, both internal and external, ensuring that the refresh is IPv6 compatible,
- Any purchase of network technology, ensuring that it is IPv6 compatible,
- Any upgrade of business applications, to ensure that they are IPv6 compatible.

Fundamentally, no opportunity should be missed whenever technology change is involved to ensure that the resulting outcome is IPv6 compatible. The incremental cost of executing the IPv6 compatibility over that required to undertake the normal refresh or upgrade will be minimal, providing it is properly planned into the refresh or upgrade process.

Using this incremental approach, the IPv6 adoption plan will be very much integrated into every other activity that is undertaken to ensure the successful and sustainable operation of technology within the business. This process does emphasise the need to commence the IPv6 adoption process at the earliest possible point in time. The longer it is left, the longer it will take to execute the change and this will leave the business with increasing risk over time. The risk increases over time as the rest of the world adopts IPv6 and the innovative applications that use IPv6 begin to emerge.

At some point in time, which will be different for every organisation, the adoption of IPv6 compatible technology across the business by this incremental means will be sufficient to commence actual adoption of IPv6 in anger. This “tipping point” should be carefully planned or it will never happen. At this time, the sequence of execution steps should be undertaken, which will involve turning on the capability installed previously and working through a test program to ensure that it is all working satisfactorily, both in modules and end-to-end across the business. Any gaps in functionality found during this test phase will need to be filled and retested to ensure successful end-to-end operation. This incremental approach is highlighted in the case study presented in Appendix E.

8. Challenges to IPv6 Adoption

The IPv4 protocol has been in use worldwide within millions of organisations for over 30 years now. Hence it is a very mature and stable protocol, with very few “bugs” that haven’t already been found. In comparison, the IPv6 protocol is at the start of its maturity journey. In recent years, it has been deployed much more widely in equipment across a wide variety of organisations. However, this does not mean that all the bugs have been eliminated to date. The protocol is stable, but some of the implementations within different types of equipment are less than perfect. Problems are still being identified, even when working with equipment from highly reputable suppliers. It is fully recognised that this aspect of uncertainty does present a challenge for most organisations in terms of adoption, so care must be taken during implementation.

Some of the areas that are still providing the greatest challenge include the following:

- Uncertainty around the delivery of native IPv6 connectivity and in particular the complexity of routing for IPv6 connectivity globally, which can introduce high latency relative to equivalent IPv4 connectivity:
    - This high or variable latency can affect the performance of certain applications.

- Difficulties with implementation of IPv6 capability on some devices, even where the capability is claimed to be present:
    - This difficulty appears to be most prevalent in security devices and with certain types of web hosting software.

- Protocol analysis and testing tools are at an early stage of evolution in their support of IPv6, as compared to what is available for use with IPv4:
    - This can be very frustrating and misleading for technical and administration staff involved in keeping applications and connectivity operating at specified performance levels.

It is essential that organisations planning to adopt the IPv6 protocol recognise the potential for these challenges and take the necessary steps to mitigate any potential downside from these risks.

The most important mitigations for these risks is to:

- Take an incremental approach to the adoption,
- Execute a dual protocol strategy in the adoption of the IPv6 protocol.

The first of these mitigation approaches is largely self-explanatory and follows the approach outlined in this paper. A “big bang” approach to the adoption of IPv6 within any organisation is not a recommended course of action.

The second has also been mentioned previously, but it is worthy of emphasis. Both the IPv4 and IPv6 protocols are certain to operate alongside each other for many years to come. Hence it is best to implement an adoption strategy for IPv6 that supports this outcome. This suggests that progressing adoption while IPv4 address space is still available has merit and to execute the adoption with this approach as a deliberate strategy. This means that when a problem occurs with IPv6 adoption, the IPv4 capability should still continue to operate, ensuring that business continuity is assured. There are many other benefits to be derived from taking this “dual stack” approach and so it is widely considered to be best practice globally.

9. A Typical Case Study

The New Zealand IPv6 Task Force was approached by representatives from the Tauranga City Council (TCC) and the Bay of Plenty Local Authority Shared Services (BOPLASS) organisations in 2010, concerning the possibility of them being a lead organisation for the adoption of IPv6 in local government within New Zealand. The Task Force was very keen to promote “pathfinder” organisations, so this offer was gratefully accepted. The Task Force has continued to provide some support and mentoring, but most of the hard work has been implemented within TCC. Over the next 12 months or so, TCC worked towards adoption of IPv6 in a dual stack configuration, and by the end of 2011 had achieved a high degree of compliance. A summary of the Case Study resulting from this project is included in Appendix E.

The project was implemented using most of the practices highlighted in this paper. It has largely been achieved through the efforts of a single technical champion, explicitly supported by the executive team. It required both individual enthusiasm and dedication combined with a supportive team effort. The end result has been excellent, with the following objectives having been largely achieved:

1. Put into place some degree of IPv6 firewalling,
2. Get a web presence for most of our websites,
3. Enable IPv6 connectivity from internal machines to the internet where needed,
4. Put into place DHCP for IPv6,
5. Setup RA (router advertisements) to enable gateways to be automatically located,
6. Enable IPv6 on all the internal network infrastructure devices – licensing, configuration changes, RIPng and RA needed to be sorted,
7. Down the track enable IPv6 across all L3 VLANs in addition to IPv4,
8. Put into place 6in4 tunnels where needed – infrastructure that could not cope with IPv6 traffic at this stage,
9. Put into place a teredo relay for 2001:0:: addresses,
10. Put into place a 6to4 relay router for 2002:: addresses,
11. Carry out internal training on IPv6,
12. Put an IPv6 multicast infrastructure into place,
13. Determine the issues presented with IPv6 on different Windows platforms.

10. Conclusion

The adoption of IPv6 is an essential business risk management issue for all organisations in New Zealand that use the Internet as an essential business tool. No enterprise in New Zealand is an exception to this emerging risk. All enterprises need to play a role in the adoption of this inevitable change and the associated prudent management of the risks of not adapting to this global change. It is essential that all New Zealand enterprises remain connected with their customers and suppliers, where-ever they may be and promote their products and services to potential customers and partners across the globe.

This paper provides an outline of the approach required to address this change and the associated risks of both undertaking the adoption of IPv6 and of not taking this path of action. The adoption of IPv6 is certainly not without its risks, but the potential business risks associated with not adopting will be even more substantial in the longer term. If a properly planned and managed approach is taken to the adoption, the risks associated with change can be successfully managed as has been demonstrated within this paper.

The critical issue is to commence the planning early, before any specific pressure for change hits the business and then an incremental transition is possible with minimum risk and cost to the business. The worst situation is to delay until the change is forced on an organisation, wherein the costs and risks for the business can be substantial. The paper highlights many of the issues which need to be managed in undertaking the adoption of IPv6 and presents some best practices which have been proven to provide a low risk approach through actual use within the industry. Detail is included within the appendices to further support the best practice approach.

Appendix A: The New Zealand IPv6 Task Force (www.IPv6.org.nz)

Purpose

"The New Zealand IPv6 Task Force is tasked with promoting the adoption of IPv6, assisting with training and education options and implementation planning. The Task Force is aligned with the Global IPv6 Forum, and its work is driven by the impending exhaustion of IPv4 addressing and the associated risk and additional cost that this is expected to impose on New Zealand organisations." http://www.IPv6.org.nz/about/

Structure

The IPv6 Task Force is an industry group working to promote the adoption of IPv6 in NZ. It is constituted as a Charitable Trust: with Murray Milner, Dean Pemberton and Vikram Kumar as Trustees.

The IPv6 Task Force has Murray Milner and Dean Pemberton (technical) as Convenors: and InternetNZ as a secretariat. The prime funders are:

- InternetNZ,
- FX Networks,
- Microsoft,
- InspireNet,
- Prophecy Networks.

Members include a wide cross-section of the New Zealand ICT industry.

Principles

The IPv6 Task force operates under a set of principles, including:

- We remain aware of what is happening globally and locally,
- We share our information and help others find the information they need,
- We are supportive of progress across all stakeholders, large and small,
- We refrain from vilifying real or perceived lack of progress.

Key Activities

Under these principles, the Task Force undertakes a variety of activities, including:

- Conducting various surveys to gain insight into trends,
- Encourage early adopters,
- Provide support through our technical special interest group,
- Industry sector liaison,
- Government sector liaison,
- Facilitate training capability,
- Facilitate evolution of IPv6 products and services,
- Leverage our web & social media presence,
- Work with pathfinders to discover learning's that can be shared,
- Stay connected to progress and news from around the world,
- Media and publicity.

Appendix B: Successful Strategies – T. Limoncelli & V. Cerf

Summary

The IPv4 address space is depleted. People who have been ignoring IPv6 for years need to start paying attention. It is real - and really important. IPv6 deployment projects seem to be revealing two successful patterns and one unsuccessful pattern. The unsuccessful pattern is to scream that the sky is falling and ask for permission to upgrade "everything."

The lessons we have learned:

1. Proposals to convert everything sound crazy and get rejected. There is no obvious business value in making such a conversion at this time.
2. Work from the outside in. A load balancer that does IPv6-to-IPv4 translation will let you offer IPv6 to external customers now, gives you a "fast win" that will bolster future projects, and provides a throttle to control the pace of change.
3. Proposing a high-value reason (i.e. your "one thing") to use IPv6 is most likely to get management approval. There are no simple solutions, but there are simple explanations. Convert that "one thing" and keep repeating the value statement that got the project approved, so everyone understands why you are doing this. Your success here will lead the way to other projects.

For a long time IPv6 was safe to ignore as a "future requirement". Now that the IPv4 address space is depleted, it is time to take this issue seriously. Yes, really.

Appendix C: Steps in IPv6 Deployment

Adapted from the IPv6-TechSIG Website

The key steps involved in IPv6 deployment include the following:

1. Check the status of IPv6 support on your networking equipment. This can be done through vendors, or by posting a question to the IPv6 TechSIG list.
2. Gain some low level IPv6 knowledge. This can be supported by asking questions on the TechSIG website.
3. Develop an addressing plan. This might seem to be putting the cart before the horse because you don't even have any addresses yet. But you need a plan in order to get an address allocation either direct from APNIC or via your service provider. This process is also a good way to get your head around IPv6. Look at your IPv4 addressing plan and mirror it in IPv6.

   This is the easiest way to start off. Current guidelines for completing this task would include:

   - Allocate a /64 for loopbacks and another for linknets,
   - Loopbacks can be /128s which can have the IPv4 prefix inserted in the last 64 bits, eg 192.168.4.2 becomes :0192:0168:0004:0002,
   - Linknets can be /112s with the two ends of the link on different ranges, eg one end on :1 and :2 and the other end on :101 :102, :fffff, :fffe etc,
   - General purpose subnets which will have client machines on them look to be /64s /48s and /56s can be allocated to customers if you are an ISP.
4. Decide where you are going to get an upstream connection from. This will depend on what you will be doing for addresses and depend on your existing service provider relationships. There are many options. You can get native IPv6 from some NZ providers now (it will almost certainly be tunnelled internationally though), or you can choose to tunnel to international locations yourself. Remember, native connectivity is almost always better than tunnelled connectivity from a performance, troubleshooting and TE point of view. However, this market is only in its infancy today, so there will be some constraints.
5. Get some IPv6 addresses. If you're going to be using an upstream ISP within NZ and you are not an APNIC member, then you can go to them and get a block of addresses. This is when your addressing plan from step 3 comes in handy. You just pass this to your ISP and they will give you a block which can accommodate your specific needs. They should not have any difficulty in fulfilling this request, as they can use addressing plans such as this to hand to APNIC for their next allocation. They should hand you out some from their allocation and you'll be able to get started. Remember though that the chance of getting some other upstream to route this block (unless it's a /32) is unlikely. If you intend to heavily multi-home, then approaching APNIC might be a better idea (this could potentially be arranged on a group basis through ALGIM).

   If you are an APNIC member, then you need to approach APNIC for your initial allocation. The current policies for IPv6 address allocation are summarised in Appendix D below (see also http://www.apnic.net/policy/ipv6-address-policy). Under the APNIC allocation regime you have to either be making 200 assignments within 2 years, or have some existing APNIC allocated IPv4 space. If you do meet this criterion, then you will be allocated a /32. Any questions on the forms see your APNIC host master or post a question to the TechSIG website.
6. Populate your addressing document with your new prefix and start looking at your network and routing design. Hopefully by this stage, you have some pretty clued up people in your organisation when it comes to IPv4. Well these people will need to also be as clued up on IPv6. The best way to start this is to devise a plan to roll out addresses onto your network.

   Here is an example of such a plan:

   a) Put IPv6 loopbacks on all routers which have IPv4 loopbacks.

b) Put IPv6 linknet addresses on all network links which are numbered out of your current IPv4 netblock (i.e. don't worry about your upstream peering links).

c) Design and deploy an IPv6 IGP routing protocol. If you use OSPF then you're probably going to be looking to deploy OSPFv3. If you use ISIS then you don't need to do anything (I'm an ISIS fan, so it serves all you OSPF user's right). If you use EIGRP then you're on your own (post to TechSIG and we'll work it out). At this stage you should have a network where all of your routers should be able to talk to each others loopbacks using native IPv6 transport.

d) Turn up iBGP peering sessions.

e) STOP. At this stage you are about to turn up external connectivity. You should be aware that any firewall rules or host based firewalls you have will need to be reconfigured to accommodate your new IPv6 addresses. This is a bit of a large step to go through here. But you should sit down with your current IPv4 security policy and generate / implement an IPv6 one BEFORE you connect yourself to the outside world.

f) Turn ip eBGP peering sessions and advertising your aggregate route. Easy ones are WIX and APE. Speak to Citylink if you are already a customer, they have a form you will need to fill out to get IPv6 peering.

g) STOP. At this stage it's a good point to stop. Your core network infrastructure is pretty much done (with the edge still to go) and it's not a bad time to sit back and look at the next stage of the plan.

7. Build a list of products and applications, and check the IPv6 support plan for each of them. Identify any problem cases (i.e. supplier has no plan) and beat up on them.
8. Enable AAAA records (internally) and dual stack access to DNS (think carefully before exporting AAAA records).
9. Set up initial management and measurement for IPv6.
10. Enable gateway for Teredo / 6to4 access (Tui boxes) (because of Vista).
11. Create test IPv6 web server (www.IPv6.example.co.nz) - progressively duplicate the real site there. Test everything, especially interactive stuff and authentication. Catalogue any applications that need updating. Consider reducing MTU to 1280.
12. Dual stack the real website (again, think carefully before exporting AAAA records).

Appendix D: APNIC Address Allocation Process

If you are an APNIC member, then you can approach APNIC for your initial allocation of IPv6 addresses. A copy of their current guidelines can be found at http://www.apnic.net/policy/IPv6-address-policy.html.

Initial Allocation Criteria

To qualify for an initial allocation of IPv6 address space, an organisation must:

1. *Be an LIR,*
2. *Not be an end site,*
3. *Plan to provide IPv6 connectivity to organisations to which it will make assignments, by advertising that connectivity through its single aggregated address allocation,*
4. *Meet one of the following two criteria:*
   - *Have a plan for making at least 200 assignments to other organisations 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 organisations and announce the allocation in the inter-domain routing system within two years.*

Private networks (those not connected to the public Internet) may also be eligible for an IPv6 address space allocation provided they meet equivalent criteria to those listed above.

Minimum Initial Allocation Size

Organisations that meet the initial allocation criteria are eligible to receive a minimum allocation of /32.

Appendix E: Tauranga City Council Case Study

Introduction

During 2010 the IPv6 Task Force commenced discussions with the Tauranga City Council (TCC) and the Bay of Plenty Local Authority Shared Services (BOPLASS) organisation concerning the potential for TCC to become an early adopter of IPv6 within the government sector. In this regard, TCC would become a "pathfinder" organisation in terms of the Task Force's strategic direction.

Late in 2010, it was agreed that TCC would take up this challenge and during 2011 has implemented its programme of IPv6 adoption across most of its ICT infrastructure. The Task Force has continued to work with TCC in this activity and has encouraged TCC to prepare a summary of the work undertaken, including challenges on the way, to share with others. This case study is summarised below.

My thanks go out to the following people for their efforts in making this initiative happen and in the preparation of the material which follows:

- Geoffrey Brown,
- Miles McConway,
- Anne O'Malley.

Background

The TCC ICT infrastructure consists of the following:

- Websites – there are about 25 different domains that have their web services hosted at TCC.
- Major Network Elements – around 40 internal switches with 24 to 96 ports each; about 650 users across approximately 10 sites; an extensive virtual desktop infrastructure (around 300) and around 110 servers (mostly virtualised also).
- Internet Service Provider – FX Networks provide the internet feed to TCC and some other councils that are part of the BOPLASS group. They supply native IPv6 connectivity.
- Council Fibre Network – TCC has put a reasonable amount of single mode fibre around the city along with roadside cabinets. This fibre infrastructure is used by both TCC and parties external to council.

The goal of the initiative was to achieve the following:

1. Put into place some degree of IPv6 firewalling.
2. Get a web presence for most of our websites.
3. Enable IPv6 connectivity from internal machines to the internet where needed.
4. Put into place DHCP for IPv6.
5. Setup RA (router advertisements) to enable gateways to be automatically located.
6. Enable IPv6 on all the internal network infrastructure devices – licensing, configuration changes, RIPng and RA needed to be sorted.
7. Down the track enable IPv6 across all L3 VLANs in addition to IPv4.
8. Put into place 6in4 tunnels where needed – infrastructure that could not cope with IPv6 traffic at this stage.

9. Put into place a Teredo relay for 2001:0:: addresses.
10. Put into place a 6to4 relay router for 2002:: addresses.
11. Carry out internal training on IPv6.
12. Put an IPv6 multicast infrastructure into place.
13. Determine the issues presented with IPv6 on different Windows platforms.

Progress to Date

The progress that has been achieved through to September 2011 can be summarised as follows:

Objective Item	Status
Put into place some degree of IPv6 firewalling	Complete
Get a web presence for most of our websites	Complete
Enable IPv6 connectivity from internal machines to the internet where needed	Complete
Put into place DHCP for IPv6	Complete
Setup RA (router advertisements) to enable gateways to be automatically located.	Complete
Enable IPv6 on all the internal network infrastructure devices – licensing, configuration changes, RIPng and RA needed to be sorted	Partially complete
Down the track enable IPv6 across all L3 VLANs in addition to IPv4	Partially complete
Put into place 6in4 tunnels where needed – infrastructure that could not cope with IPv6 traffic at this stage	Complete
Put into place a Teredo relay for 2001:0:: addresses	Complete
Put into place a 6to4 relay router for 2002:: addresses	Complete
Carry out internal training on IPv6	Pending
Put an IPv6 multicast infrastructure into place	Pending
Determine the issues presented with IPv6 on different Windows platforms	Complete

This is a tremendous outcome in less than 1 year for a very small team of people.

Knowledge Development and Training

The initiative was supported by knowledge development and training, both from external sources and on the job, as follows:

1. Number of staff required to implement = 1 (with supportive executive).
2. Training was initially undertaken at Auldhouse and a lot of additional in house experimentation was done to fully complete understanding in several areas. This was particularly the case for improved understanding of the IPv6 limitations in the Windows Operating System (XP and Server 2003).
3. Using spare network switches went through setting up some test networks, separate from main council network, to verify understanding of IPv6 operation on several devices including any differences between different switch firmware. Tested much of the IPv6 functions including ACLs, RAs etc.

4. There was a considerable amount of reading and testing of the various IPv6 tunnel types available and going through the configuration of these using the Extreme switches we were going with (X460 model). There was also a lot of work done to get the Teredo relay setup on a Linux platform. The 6to4 site-specific relay was relatively easy to implement as functionality for this was built into the Extreme X460 switches.

Lessons Learnt

The key lessons learnt through this initiative from a business perspective were as follows:

- The background work to get IPv6 implemented is made easiest when done at the time of network infrastructure equipment refresh.
    - This also provides an opportunity, before network equipment is deployed, to test various configurations using a test lab / network.

- There needs to be the commitment to move to IPv6.
    - Doing the change at network equipment refresh time is still quite involved - especially when operating system, continued service provision and other network issues are factored in.

- The amount of planning required to implement will really depend on how much of a handle your network team has on the complete topology and operation of the network.
    - Where little knowledge is present a full audit of the network and paper based documentation and attendant checklists will be needed.
    - For teams with lots of knowledge some discussions and emails are probably sufficient covering what will be the problem areas, costs and time frames needed to complete the changes.

The key lessons learnt from a more technical perspective were as follows:

- Carefully analyse the real costs of providing IPv6 functionality particularly with regard to network switch infrastructure - where any cost may be multiplied many times for switching the entire infrastructure in place.
    - Carefully compare the IPv6 base features from different vendors as there is a large variation in real costs incurred to get the same functionality.
    - Some vendors have a lot of functionality built-in which requires licensing from other network switch vendors.

- By using a dual stack solution you should not cause any impact to existing network operation in most cases.
    - Some software, when IPv6 is enabled, either does not work or generates errors of some sort. In our case we have a very large list of software covering 2 A4 pages and the number of issues caused by IPv6 was limited to about 3 pieces of software.
    - Testing software would be the best method of determining where IPv6 is an issue.
    - To my knowledge all Microsoft products, with the exception of ISA or the later iteration ForeFront, don't have any issues with IPv6.

- By getting onto sorting out an IPv6 deployment plan early I believe it is quite possible that you can take 1 year to get all aspects sorted.
    - We are currently running some networks as IPv4 only and others as IPv4 and IPv6.
    - Transition of IPv4 only networks to IPv4+IPv6 happens as time permits for me which makes for very low stress and fitting around other work.

  - Much of the IPv6 configuration changes, when using dual stack on the operating system, can be done during business hours with no impact to users.
  - Use this to your advantage.

- IPv6 is really only a must have for web facing services at this stage, but you should be getting prepared for implementing IPv4+IPv6 internally as well.
  - Doing so will enable some nice features that come with IPv6 and because IPv6 removes the need for NATing life in certain areas can become a lot easier.
  - This particularly applies to SIP, H323 and encryption of traffic.
  - Users moving between WiFi access points can have a more seamless transition from one WiFi IP subnet to another one using some of the extra features in IPv6.

Final Network Topology

The final high level network topology implemented for TCC is illustrated in Figure 1 below. The 6to4 site-specific relay handles delivery of 2002::/16 traffic back to IPv6 users on the internet.

The Teredo relay (also site specific) handles delivery of 2001:0::/32 traffic back to IPv6 users on the internet.

These two services have been implemented to ensure good IPv6 communication where transition technologies (as opposed to native IPv6) are in use at the client end.

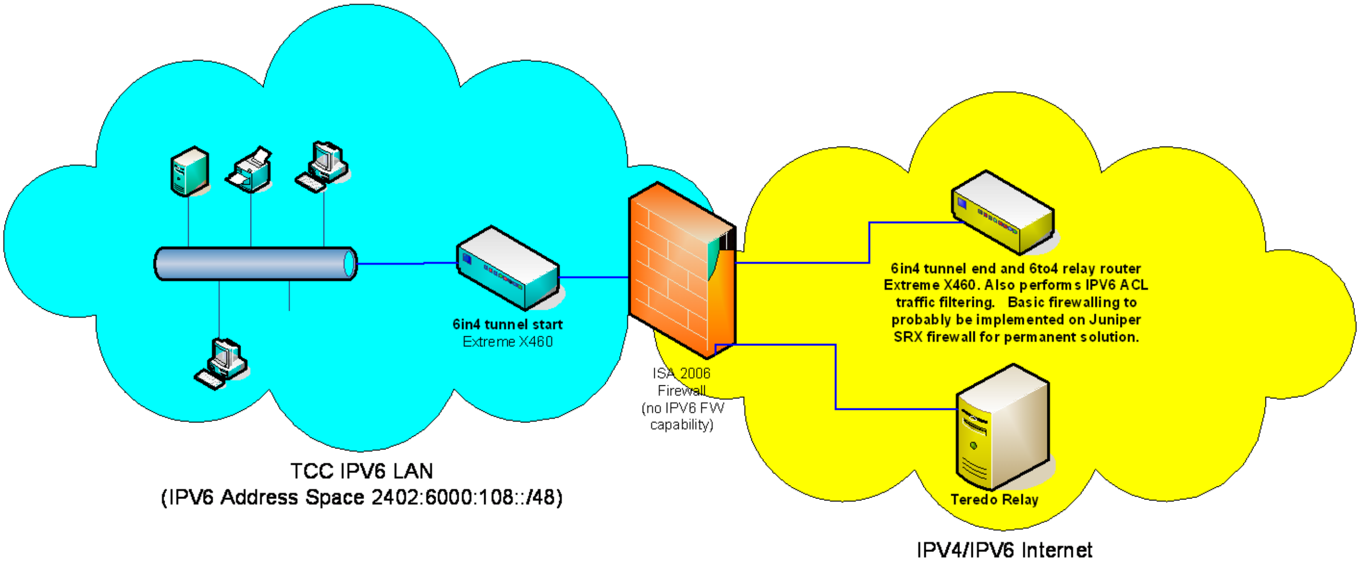
6in4 tunnel start
Extreme X460
ISA 2006
Firewall
(no IPV6 FW
capability)
6in4 tunnel end and 6to4 relay router
Extreme X460. Also performs IPV6 ACL
traffic filtering. Basic firewalling to
probably be implemented on Juniper
SRX firewall for permanent solution.
Teredo Relay
TCC IPV6 LAN
(IPV6 Address Space 2402:6000:108::/48)
IPV4/IPV6 Internet

Figure 1: Final High Level Network Topology for Tauranga City Council after the adoption of IPv6.

Conclusions

The move to IPv6 has not been painful and is eased by doing the move at network infrastructure equipment refresh time. The use of Windows 7 for the desktop is advisable to get the best experience and make life easy at the desktop in terms of IT support. Windows Server 2008 is advisable at the server end. Windows Server 2003 requires a level of manual configuration as does Windows XP.

There is a need for some training of all IT staff in general principles of IPv6 operation. It would probably be best to send staff who will be managing the L3 routing and network infrastructure setup on advanced training. Other staff doing more desktop support will need to be aware of some of the options on ping, trace route and other diagnostic tools to enable selection of IPv4 or IPv6 and correctly interpret the results.

The setup of a site-specific Teredo relay and 6to4 site-specific relay router is not necessary and will depend on what level of service is provided by your ISP and the reliability of the service.

For an organisation of our size (650 staff, 40 network switches, 30 L3 VLANs and approx 110 servers) I would allow approximately 1 year to complete the transition. It is important to understand that this timeframe is stated on the basis that 1 person is making all the necessary changes, for the most part to servers and network infrastructure and that this is still just a part of my daily workload. Depending on IT staffing this can occur more quickly.

Dual stack used on the client operating system will mean much of the changes, once familiar, can be performed during business hours thereby minimising out of hours work required.

Contact Details:

Geoffrey Brown, IT Department
Tauranga City Council
91 Willow Street, TAURANGA
New Zealand
Email: geoffrey.brown@tauranga.govt.nz