INTERCONNECT COMMUNICATIONS

Ofcom

MC/111
Internet Protocol Version 6 Deployment Study

Final Report

Merlin House
Chepstow
NP16 5PB
United Kingdom

Telephone: +44 1291 638400
Facsimile: +44 1291 638401
Email: info@icc-uk.com
Internet: www.icc-uk.com

INTERCONNECT COMMUNICATIONS
A Telcordia Technologies Company

Notice

This document is provided in good faith and is based on InterConnect's understanding of the recipient's requirements. InterConnect would be pleased to discuss the contents of this document particularly if the recipient's requirements have in any way changed.

InterConnect is a wholly owned subsidiary of Telcordia Technologies Inc.

InterConnect Communications Ltd
Merlin House
Station Road
Chepstow
NP16 5PB
United Kingdom

Telephone: +44 1291 638400
Facsimile: +44 1291 638401
www.icc-uk.com

Persons to contact in relation to this document:

Brian Aitken
Business Development Executive
DDI: +44 (0) 1291 638426
Fax: +44 (0) 1291 638401
Email: brianaitken@icc-uk.com

Contents

1. Executive Summary

The Internet has become one of the most important infrastructures of modern society. Today it is essential for organizations, companies and individuals to work, play, learn and conduct business. As with any important piece of infrastructure, the Internet must evolve to survive.

There are well-documented socio-economic benefits to ensuring that as many people as possible have access to high-speed broadband. For example the European Commission's 2009 Digital Competitiveness Report suggests that the deployment of widespread broadband access will help generate up to two million new jobs in Europe by 2015. Yet, universal broadband access will put heavy strain on the Internet, as all computers connected to the global network need a unique address.

Today's Internet is based on the IPv4 protocol (Internet Protocol version 4). It is the foundation for the addressing and routing that largely goes unseen, but is essential to the function of the Internet. In February of 2011, the Internet Assigned Numbers Authority announced that the pool of available IPv4 addresses had been exhausted. In September 2012, Europe's registry for Internet addresses announced that its pool was exhausted and that extremely restrictive rules for IPv4 address allocation were now in effect. As a result there are no longer enough IPv4 addresses to support future growth, development and economic competitiveness in the global market. This is compounded by trends in Internet use such as mobility, smart devices, smart transport, and remote monitoring. Even without these important trends, the shortage of addresses will be a significant problem.

The successor to the IPv4 protocol has been available for almost 15 years. It is called IPv6 (Internet Protocol version 6). The transition from IPv4 to IPv6 is an essential evolution in the Internet. However, despite being essential to future growth, this evolution has been delayed and has encountered serious difficulties. This report examines those difficulties, which stem from the incompatibility of IPv4 and IPv6. The report provides an overview of IPv6, highlighting the potential impact of slow uptake of IPv6, both to the UK economy and the Internet. The report also looks at how the transition from IPv4 to IPv6 is likely to take place. The report finds that by any measure, the UK lags behind its peers in IPv6 deployment. Whether in comparison with; economies of a similar size, G20 and EU member states, or with Asian economies, the UK is behind in IPv6 adoption. IPv4 address exhaustion and a failure to transition to IPv6 has a significant impact on innovation as it is the essential building block for any technology that connects to the Internet. Failure to keep up with competitor economies will have an impact on the UK's consumer access to broadband, on eGovernment, intelligent highway systems, sensor technologies, mobile Internet applications, distributed generation of renewable energy, remote and automated monitoring of natural resources, and support for advanced employment, immigration and welfare applications.

Just as important to the United Kingdom's competitiveness are those applications and services that have not yet emerged in the marketplace. The potential is enormous and offers the UK an opportunity to become a centre of innovation, research and development in the United Kingdom as billions of devices connect to this common standard infrastructure using the IPv6 protocol.

To safeguard the future growth of the digital economy, timely adoption of IPv6 is essential.

2. Implications of the Exhaustion of the IPv4 Address Space

While few users understand the nature of Internet addresses, they are fundamental to the operation of the Internet. Without them, the Internet as we know it, would not work.

During the emergence of popular, public Internet in the 1990's and 2000's, a single, standard format for Internet addresses was in use. This format, and the organization of the packets that contained information to be sent from place to place in the Internet, was called the Internet Protocol version 4 (IPv4).

The format for the IPv4 address was simple: a string of 32 consecutive ones or zeroes (each digit called a bit). The 32-bit address space provided addresses for more than four billion devices to be connected to the Internet. That seems a vast address space for connected devices. But it isn't. And, at the time of the commissioning of this paper, that address space is exhausted. No new IPv4 address space is available for attaching new devices to the public Internet.

The implications of this are significant because of our economic, social, political and personal dependence on the public Internet. It is not an exaggeration to say that the United Kingdom's economic competitiveness, security and capacity for growth are dependent on the continuing innovation of the Internet. And without the ability to acquire Internet address space, that continuing innovation will be seriously impeded and in some areas will become impossible.

2.1 Has the IPv4 Address Space Really Run Out?

At the time this report was written, the five Regional Internet Registries (RIRs) reported the following statistics for available IPv4 address space:

- APNIC, the Regional registry that serves the Asian/Pacific region, is effectively already out of IPv4 addresses. APNIC is only now allocating very small blocks of IPv4 addresses under its final /8 allocation policy.
- RIPE, the Regional registry for Europe and parts of the Middle East reports that it has 2.3 /8 blocks remaining. Those will be exhausted by the summer of 2012[1].
- ARIN, the registry for North America has about 4 /8 blocks available; enough to last until the summer of 2013.
- LACNIC, the Latin American, Caribbean and South American registry, and AfriNIC, the African regional registry both have about 2 /8 blocks in their regions. Because they use addresses at a slower rate, they will probably last until the summer of 2014.

Crucially for the United Kingdom, there are no IPv4 address space resources available from the traditional source, RIPE, starting in the summer of 2012.

There is an apparent correlation between the timing of the recent economic slowdown and a slower rate of consumption of IPv4 addresses. In the last 24 months this correlation is most evident. There has been research that clearly links the rate of consumption of IP address

[1] Our research suggests that this may be as early as June 2012.

resources to the state of the economy[2]. For instance, if we examine which economic regions allocated IPv4 addresses in recent years, we can see that there appear to be clear connections between the state of the regional economy and IPv4 address allocations.

At a regional level it's possible to compare the allocations made by each RIR.[3]

IPv4 Allocations	2005	2006	2007	2008	2009	2010	2011	2012
Asian/Pacific	31%	31%	34%	44%	46%	48%	53%	55%
Europe/Middle East	35%	33%	31%	22%	23%	22%	22%	19%
North America	27%	28%	26%	28%	22%	18%	11%	10%
Latin and South America	6%	7%	7%	6%	6%	6%	10%	11%
Africa	1%	2%	3%	1%	3%	3%	5%	5%

In 2011 there was an evident land-rush for IPv4 addresses in the Asian/Pacific region. In fact, the typical annual distribution of IPv4 resources took place in the first four months of the calendar year. Policy-based brakes were put into place to prevent further large-scale exhaustion for the remainder of the year in that region[4].

The decrease in relative allocation rates in Europe and North America can be traced to economic factors that slowed some expansion of network investment. For instance, in Europe, RIPE allocated more than 55 million IPv4 addresses in 2010, but this number fell by 23% in 2011. The fall was even more precipitous in North America. Beyond simple economics, a policy decision in both regions[5] to limit the number of IPv4 address an organization can request (now, a three-month supply) when it requests an allocation.

Even with the brakes being put on through administrative means in the three largest utilization regions of the world, there simply are not enough remaining resources to support continued growth. Even in the areas of least consumption, the rate of consumption is forecast to exhaust the existing supply of IPv4 addresses by the summer of 2014.[6]

2.2 The Exhaustion of the IPv4 Address Space

The exhaustion of the IPv4 address space in the RIPE NCC region (which includes the UK) is predicted to take place in June 2012. Once the IPv4 address space is exhausted the Regional Internet Registrars such as RIPE NCC will then revert to their last slash-eight (/8) allocation policy. This policy greatly restricts the address space that can be allocated to RIPE members.

---

[2] Internet Address Space: Economic Considerations in the Management of IPv4 and in the Deployment of IPv6; http://www.oecd.org/dataoecd/7/1/40605942.pdf

[3] http://www.isoc.org for 2005 to 2011. Our own research for 2012.

[4] The policy based brakes were made in revisions to APnic's IPv4 address allocation and assignment rules. The rule changes are outlined at: http://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details

[5] http://www.ripe.net/ripe/policies/proposals/2009-03 in Europe and https://www.apnic.net/services/services-apnic-provides/helpdesk/faqs/ipv4-stage3-faq in the Asia/Pacific region

[6] See http://www.potaroo.net/tools/ipv4/index.html

Members will only ever receive one more allocation of IPv4 addresses, this allocation will be a /22 or only 1024 addresses.

The impact upon organisations will vary enormously depending on their requirements for global IPv4 addresses. At one extreme an organisation that has a stock of IPv4 addresses and a low allocation rate will not initially be affected. At the other extreme a new business that requires IPv4 addresses for its services (e.g. mobile operators), it Internet connectivity (to use NAT) or for providing Internet services will not be able to do so using the traditional end-to-end model of Internet connectivity.

Consequently there will be a long period of time in which some organisations have a significant advantage over others in the market-place just because they are fortunate in having some remaining IPv4 address space. Consumers of services from Internet Service Providers (ISPs), hosting companies and others will begin to specify as a requirement that the service provider has enough IPv4 addresses for their current and future requirements. This will become a differentiator in the market-place. Note too that this will not only have an impact with the UK or Europe but also globally.

The scenarios in the examples above are nearly certain to happen if IPv4 addresses are unavailable. Such businesses would have very limited options to avoid this scenario and are likely to not be feasible in most circumstances.

2.3 Market Forces and IPv4 Exhaustion

The traditional view of IPv4 address availability was one where there were no limits: if you could justify the need for the space, you were assigned the block without question. In the absence of available space, one could envision those who had spare IPv4 addresses making it available to those who needed it in exchange for something else of value. In the last decade it has been suggested that the creation of markets could be a mechanism to link those who had spare IPv4 address space to those who were in need.

It is worth considering whether such a strategy could be a solution to IPv6 scarcity and if a market would be an effective mechanism of redistributing a scarce resource.

2.3.1 Is There a Market?

There is evidence of buyers and sellers meeting to exchange IPv4 address space for money. In possibly the most famous case, Microsoft outbid three other interested parties in an auction of 666,624 IPv4 addresses during the bankruptcy sale of Nortel for a fee of 7.5 million dollars (USD) in 2011[7].. Outright purchase of IPv4 address space as an asset is only one approach to linking buyers and sellers. Another approach is through mergers: CenturyLink, the third-largest telecommunications company in North America acquired Savvis, Inc. Savvis has vast IPv4 addressing resources, much of which is space (sometimes called “legacy” space) that was allocated in the early part of the Internet’s history.

[7] Microsoft Spends $7.5M on 666K Nortel IPv4 Addresses, PCMAG.COM; http://www.pcmag.com/article2/0,2817,2382616,00.asp

In February of 2012, Addrex, a company that purports to broker exchanges of IP address space for money, announced that it had an IPv4 /8 block for sale (more than 16 million addresses)[8]. Unlike the Microsoft and Savvis cases, this was a case where the address space was transferred without the involvement or approval of the Regional Registry (in this case, ARIN in North America). What is interesting about this development is that the transfer of address space may, in some special circumstances, be separated from the needs-based test that governs transfers of address space inside the RIR system.

2.3.2 Legal Background

Historically, IPv4 addresses have not been transferrable. In the past, if a network operator found that they no longer needed IP addresses, they were supposed to return those addresses to the Regional Internet Registry. Each RIR had policies in place that allowed addresses to transfer in the case of mergers and acquisitions; however, direct sale of address space was prohibited.

In response to scarcity, the RIRs have gradually changed their policies. Perhaps the most complex is ARIN's Specified Transfer Listing Service which allows those needing address space to meet up with those that have IPv4 address space available. Organizations who want to act as brokers can also participate in the listing service. The main advantage, from the point of view of the Regional Registries, is that control is kept of the address space, and the need-based test continues to be applied to the applicant for new space. Specifically, in the ARIN case, the buyer of the address space must sign the ARIN Registry Services Agreement which stipulates that addresses are not property and provides a fee schedule for ARIN's future services. For those who need address space, the listing service provides some certainty of the identity of those who are selling space in the marketplace.

One interesting exception to the Regional Internet Registries desire to keep control of the IP addressing assets is the address space allocated to consultants and contractors in the period before the emergence of the RIR system. This address space, often called "legacy" address space, is not under any contractual arrangement with any RIR. That makes for interesting consequences when it is available for brokering.

In a sworn affidavit in the United States Federal Court by Mr. Ray Plzak, formerly the President and CEO of ARIN, Mr. Plzak states that: "Like other 'legacy' address holder's issued resources before ARIN began, ARIN has never had an agreement with (. . .the Legacy IPv4 owner. . .) that would give it authority over those specific resources." ARIN describes these "resources" (i.e. Legacy IPv4 number blocks) as "IP Resources Not Issued Or Controlled By ARIN."

While the transfer policies for traditional RIR IPv4 address space have evolved to allow transfer under RIR control, transfer of legacy IPv4 space may be able to happen outside the RIR system. This is precisely what happened in the Addrex case mentioned above.

2.3.3 Transparency in the Marketplace

Recently there has been a move to bring transfers between sellers and buyers out into the open. All of the RIRs have adopted some form of IPv4 address transfer policy that attempts

[8] A Whole /8 for Sale; http://www.internetgovernance.org/2012/02/14/a-whole-8-for-sale/

to allow for the movement of address space between willing participants in the market. The important difference between a free marketplace and the RIR system is that the RIR policies enforce the needs-based test for address allocation and, in many cases, provide transparency regarding who is a participant in the market.

In the European region, RIPE does have mature IPv4 address transfer policies but is the only RIR that fails to make the transactions transparent to the Internet community. However, a proposal is in place to change that and make Europe consistent with the rest of the globe regarding market transparency[9].

2.3.4 Economic Studies

Several studies have been published in the last five years that attempt to analyze and comment upon the intersection of economics and IPv4 address space scarcity. Milton Mueller, Professor at Syracuse University in the United States, published an article arguing that a free and transparent market would provide the foundation for more effective distribution of a scarce resource[10]. Ben Edelman of the Harvard Business School and Michael Schwarz proposed a market rule that would avoid fragmentation of the address space while allowing for an efficient market in addresses[11]. Edelman also published a working paper where he proposed policies for establishing a market in address space[12].

Each of the economic studies of the potential marketplace comes up against two important barriers:

- If a marketplace for IP addresses is established, it is difficult to ensure that the results are not detrimental to the technical operation of the Internet (especially the Internet's underlying routing system); and,
- The existing policy mechanisms for IP address management are not well suited to an evolution to market-based dynamics.

2.3.5 Can Markets Be Successful?

While it may be tempting to think that a market, linking those in need with those who have IPv4 addresses to spare, would result in an efficient redistribution of scarce resources. In practice this has not proved to be so. A review of transfers in the Asian Pacific region in 2012 shows two key things: 1) the size of the blocks being transferred are very small, sometimes as small as 256 addresses at a time; and 2) many of the transfers are simply transfers between two operating units of the same organization or from an acquired company to its new owner[13].

---

[9] Transparency in Address Block Transfers; https://www.ripe.net/ripe/policies/proposals/2012-05

[10] Critical resource: An institutional economics of the Internet addressing-routing space." Telecommunications Policy Vol. 34 (2010) 405–416.

[11] Pricing and Efficiency in the Market for IP Addresses; http://www.benedelman.org/publications/ipmarkets-092711.pdf

[12] Running Out of Numbers: Scarcity of IP Addresses and What to do About It; http://www.hbs.edu/research/pdf/09-091.pdf

[13] APNIC Transfer Log 2012; http://ftp.apnic.net/transfers/apnic/2012/transfer-apnic-20120604

How well has ARIN's Specified Transfer Listing Service worked? The current, full listing service is given here[14]:

```
Public STLS Summary Report

CIDR Blocks Listed for Transfer

Quantity           Block Size
1                                  /24
1                                  /16

CIDR Blocks Listed As Needed

Quantity           Block Size
0                                  None at this time

Current number of facilitators: 5

Updated: 28 February 2012
```

In fact, in none of the Regional Internet Registries has a meaningful market for IPv4 addresses emerged. The transfer policies created by the RIRs do not expand the available pool of addresses – and we have seen that large blocks needed by large ISPs for growth are simply not available. Even if a market were able to identify and place into market unused IPv4 addresses, the scale of the need would soon swamp the available market resource.[15] A market would only delay the practical exhaustion of the IPv4 address space by a very tiny amount of time.

Could the emergence of greater demand, or trading outside the RIR system lead to a more efficient market that would solve the problem of IPv4 scarcity? No. Even if the scale of new addresses in the market were two or three orders of magnitude greater than what is transferred today, the amount of available addresses could not support the current rate of growth in the public Internet. In fact, while brokers have emerged to facilitate trade in IPv4 address space[16], there is no public evidence that those brokers have been successful in transferring anything but minimal quantities of IPv4 addresses.

Markets will continue to be a niche resource for meeting very small needs, but markets currently do not represent a reliable solution to the exhaustion of the IPv4 address space.

2.4 Fundamental and Inconvenient Truths about IPv4 Exhaustion

It is important to understand that the public Internet will continue to work at the point of IPv4 address exhaustion. The fundamental problem is that there are no further addresses to be used to add new devices and services onto the Internet.

It is not possible to "create" new IPv4 addresses. The Internet Protocol only supports a fixed number of bits (32) for the IP address and these bits can only be one or zero. The number of IPv4 addresses is limited to the unique set of combinations of digits that can be created using only 32 ones and zeros.

[14] ARIN Transfer Listing Service, 4 June 2012; https://www.arin.net/resources/transfer_listing/listings.txt

[15] Economics of IPv4 Transfer Market on IPv6 Deployment, Andrew Dul, September 2011; http://www.quark.net/docs/Economics_of_IPv4_on_IPv6.pdf

[16] For instance, Addrex (http://addrex.net) or Accuro (http://www.ipaddressbroker.net/iana-ip-broker.html).

Internet users will not see an immediate or catastrophic change to the Internet in the immediate future. Instead, the growth of the Internet, and the applications that run on it, will begin to be constrained (we examine this more closely in Sections 5 and 7 of the report). Later, when parts of the Internet are connected via IPv4 replacement protocol, IPv6, there may be sites and services that are unreachable by computers or programs that have only legacy IPv4 addresses. While it may be too early to say with certainty how significant this issue will be, it has the potential to disrupt the expected end-to-end connectivity that we take for granted in the current Internet.

In some economies this has led to a market push toward transition. But not in the United Kingdom. In other parts of the world, IPv6 is seen as an enabler for new services that only work over IPv6. In the UK the priority seems to be avoiding the cost of deploying IPv6 regardless of the circumstances. It is important to understand that, from the perspective of certain parts of the Internet ecosystem, IPv6 is a disruptive technology that will undermine the value of the IPv4 services they provide today.

2.5 Implications

The most important implication of IPv4 exhaustion is its effect on growth.

Without new IPv4 addresses available, new computers, mobile devices, sensors, and other consumer and commercial devices cannot connect directly to the Internet.

Many new, innovative applications use multiple IP addresses to perform their services. In the absence of an alternative to IPv4/IPv6 transition, these new, innovative applications will be unavailable to new entrants. Indeed, many new peer-to-peer Internet applications require far more Internet address space than the, “one computer, one address” model of the first thirty years of the public Internet.

In fact, the IPv4 Internet has been short of addresses for nearly twenty years. Billions of computers currently share addresses, inhibiting the deployment of innovative applications and new services. We will look at a classic example of an application – Google Maps - that, when sharing becomes part of the underlying architecture of the Internet, is becomes unusable. The exhaustion of IPv4 addresses will eventually make it extremely difficult, if not impossible, to get by on shared addresses. As the pool of available addresses disappears, there are no longer addresses to share.

While growth in traditional use of the Internet is affected by IPv4 address depletion, perhaps a more insidious implication is the effect on new applications. The contemporary Internet is seeing a vast and varied group of objects connected to the Internet that have nothing to do with human-to-human communication. Intelligent infrastructure for electrical utilities, health care networks, disaster management systems, highway systems, and industrial automation are just examples of places where the demand for IP addresses is non-traditional, growing and voracious.

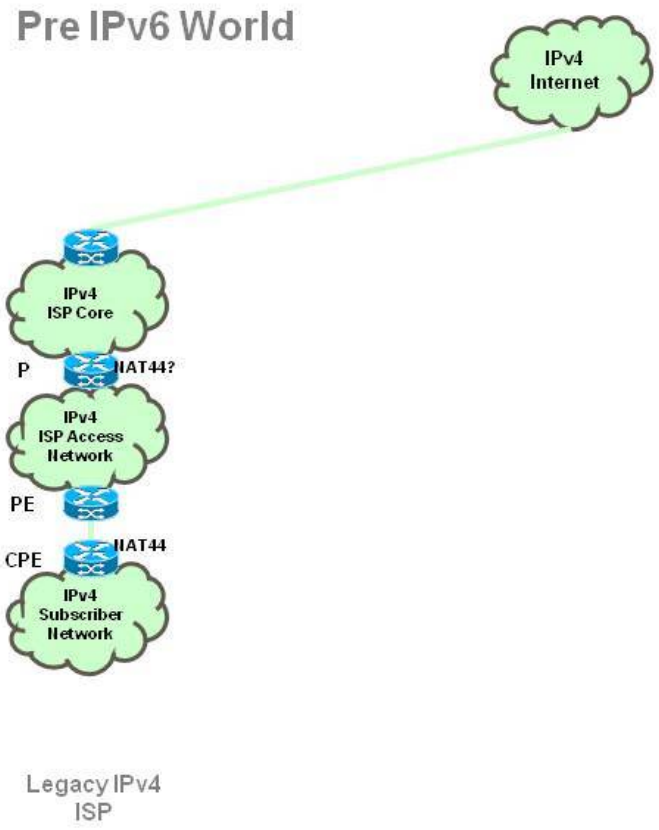
And beyond the new Internet of things, new, mobile and always-on applications require additional address space as well.

The implications of exhaustion have particular challenges for providers of Internet services. For ISPs, a serious problem will be finding ways to continue offering access to the IPv4 Internet for existing and new customers when the number of customers becomes greater

than the number of available IPv4 addresses in the ISP's pool. Beyond this, managing, securing and extending network infrastructure is going to be more costly and more complex when parallel networks need to be implemented. It is clear that more work needs to be done to quantify the scale of the problem in the UK (in fact, many ISPs are unwilling to discuss the size of the problem in a public conversation). However, in interviews conducted amongst large ISPs for this study, many admitted that the scale of the problem is so vast that, in many cases, these companies are reduced to inaction or limited trials by the scale of the problem.

Without IPv4 address space, the ability to grow the Internet's technologies and services – both the legacy and traditional ones and the new and innovative ones – will be severely hampered.

In fact, as we have seen even in the Executive Summary, the most important implication of IPv4 exhaustion is that the limitations on growth will probably pose risks to competitiveness and innovation in the United Kingdom.



The following diagram illustrates the historic pre-IPv6 Internet. It shows how Network Address Translation (NAT) has been deployed, for almost two decades, to preserve IPv4 addresses. In contrast, today's Internet is largely dual-stack with the capability to use both IPv4 and IPv6. As a result of NAT, the current IPv4 Internet is very different from the Internet that was originally envisioned by its designers. The traditional capability of end-to-end connectivity between any node on the global Internet has been effectively broken. The implications of this are that, greater complexity has had to be added to the network to enable many applications to work, the development and deployment of some applications has been hindered and some applications simply cannot work behind NAT. Overall this has been a significant limiting factor on how the IPv4 Internet can be used.

3. IPv6 – A Short Overview

The version of the Internet Protocol that is presently ubiquitous is called the Internet Protocol version 4 (IPv4) and dates from 1981. The commercial popularity of the Internet in the 1990's led engineers to consider whether or not IPv4 would withstand the onslaught of popularity that global deployment would bring. Even 4.2 billion addresses would not be enough for the growing range of devices being attached to the Internet. In 1994 one of the Internet's key standards groups, the Internet Engineering Task Force (IETF), decided to commission a study on how long IPv4, and its address space, would last.

The small working group charged with the responsibility with coming up with an answer projected the IPv4 address exhaustion to occur sometime between 2005 and 2011. The exhaustion of the IPv4 address space has been long understood. Between 1994 and today many things happened that influenced the consumption of IP address space, but the prediction was remarkably accurate given the statistics and knowledge available at the time. The IETF next moved to design a successor to IPv4.

3.1 IPv6 – Design by Committee and Compromise

Perhaps the most important feature of IPv6 is its enormous (by IPv4 standards) address space. With 128 ones and zeroes (bits), the address field was exponentially larger than its predecessor. However, the compromises and committee work led to multiple, competing visions for a successor to IPv4. After much discussion, IPv6 was standardized in November of 1994.

3.2 IPv6 – The Improvements

IPv6 was intended to be the successor to IPv4 with deployment taking place long before the public Internet ran out of IPv4 addresses. In fact, the most obvious positive feature of IPv6 is its greatly expanded address space. For many, the exhaustion of the IPv4 address space is the single most important reason to transition to IPv6. For others, the size of the IPv6 address space will remove the need for Network Address Translation – a potential benefit on many technical fronts[17]. Where IPv4 provides address space for more than 4 billion devices, IPv6 has:

340,282,366,920,938,463,463,374,607,431,768,211,456

available addresses.

However, IPv6 brings with it some other improvements as well. The address itself is not just larger, but capable of meaningful hierarchical organization. Nodes on networks are able to create their own addresses without having to rely on a network server for that function. Besides providing for very large addresses, IPv6 also supports very large packet sizes for very large payloads[18]. IPv6 also changed the approach used to support mobility, Quality of Service and anycast in networks.

IPv6 also provides the potential for processing improvements by making the header of the packet (comparative to the front of a postal envelope) simpler and easier to process. The

[17] The implications of NATs and especially Carrier Grade NATs are discussed in Section 5 of this report.

[18] Where the underlying physical transport supports this.

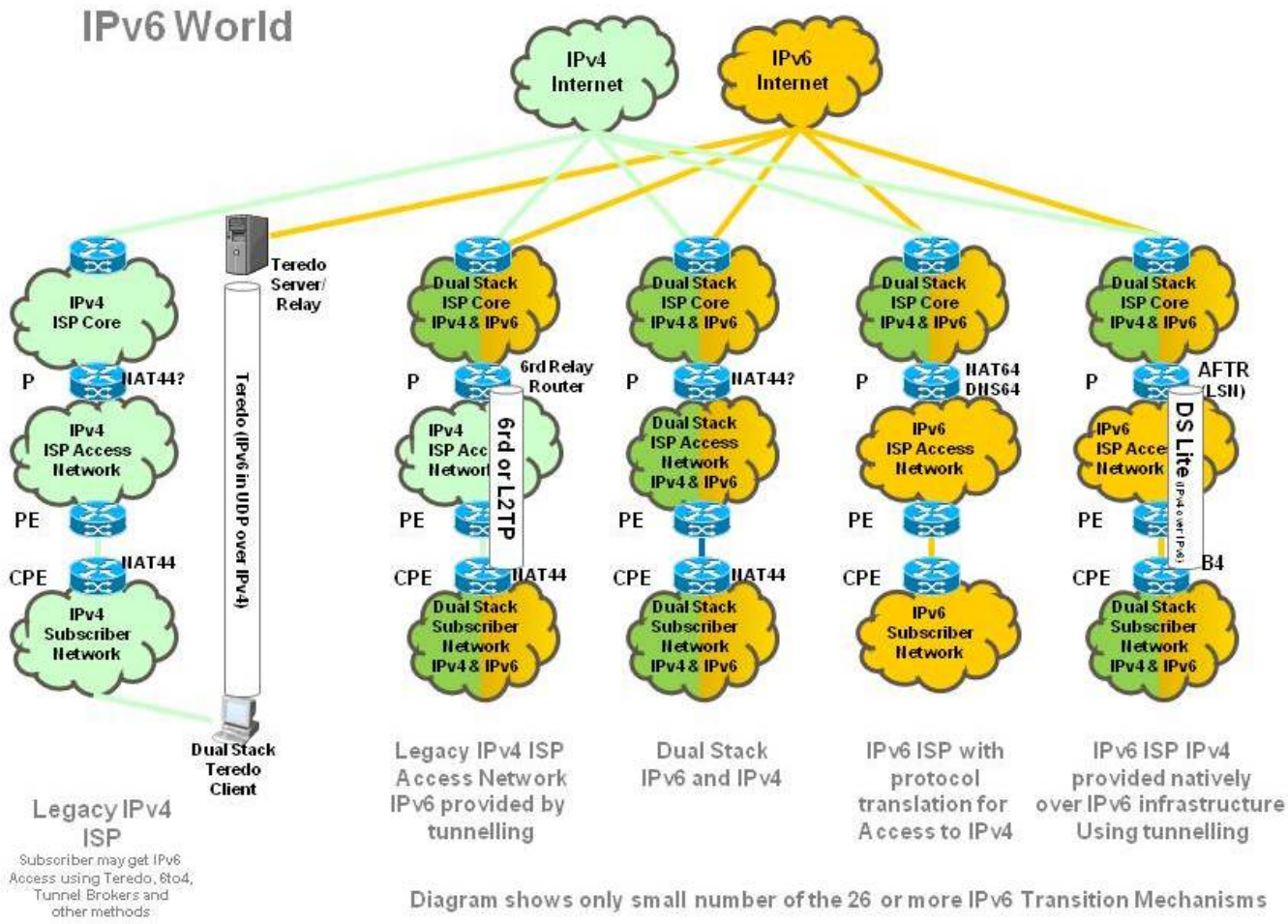
reduction in overhead makes it possible for the Internet's routers to more efficiently process the packets that contain the payloads that are crucial to the Internet's applications. In practice no improvement is realized in header efficiencies because the IPv4 limitations have been overcome by clever engineering. In fact, IPv6 extension headers, which were designed to make processing much simpler, have in fact become much more complex than IPv4 and harder to process in routers and firewalls.

Despite these potential improvements over IPv4, the primary interest in IPv6 today is in its larger address space. Growth in the public Internet drives this and the exhaustion of IPv4 address space makes IPv6 deployment an important issue for everyone interested in the infrastructure, growth and use of the public Internet.

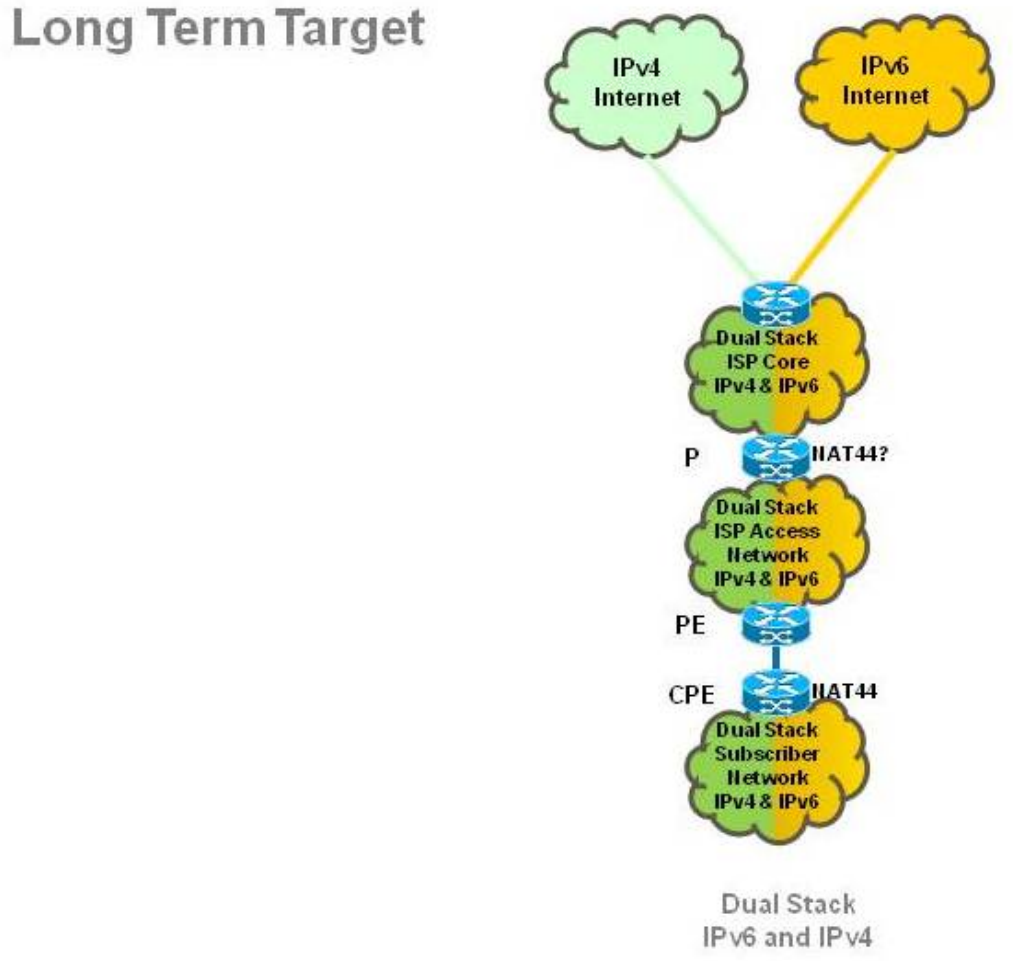
Fundamentally:

- ***We are nearly out of legacy IPv4 address space;***
- ***IPv6 appears to be the only long-term, practical approach to supporting continued growth of the public Internet;***
- ***IPv6 is not backwards compatible with IPv4;***
- ***IPv4 and IPv6 will co-exist in the public Internet for the foreseeable future; and,***
- ***IPv6 deployment has already begun in many regions around the world.***

3.3 What will the Transitional IPv6 World Look Like?



Eventually: A Stabilized IPv4 legacy/IPv6 Future Network



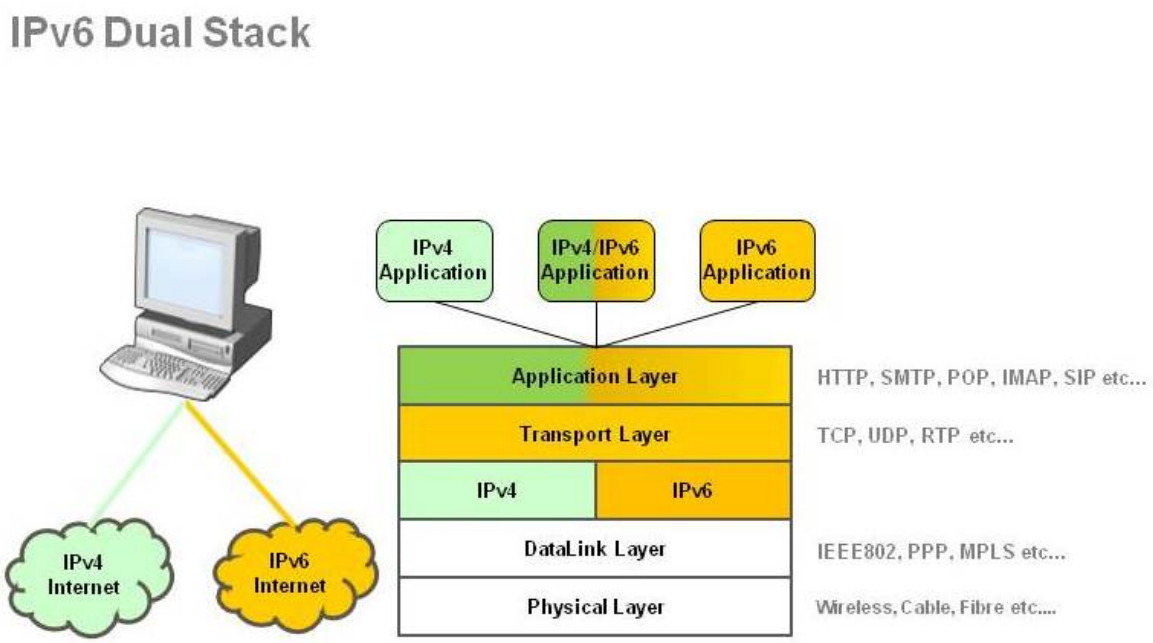
4. IPv6 - Summary of Deployment Options

4.1 Introduction to Technologies and Strategies

4.1.1 Dual Stack Approaches

A common approach to managing the transition from IPv4 to IPv6 is to recognize that both are going to be part of the Internet landscape for the foreseeable future. Reflecting this, a single computer can use the same network interface to use more than one network protocol. We call a computer whose network interface supports both IPv4 and IPv6 a dual-stack node.

Multiple stack approaches have been around for almost as long as there have been networks. In the 1980s it was not unusual to run network implementations of Novell's NetWare on the same machine as IPv4 on the same interface. Because of the incompatibility of IPv4 and IPv6 on the network – they appear to computers as different networking protocols. Despite their names being similar, IPv4 and IPv6 are incompatible protocols that must be processed differently by nodes on the network



Dual stack approaches are fundamental to the transition because that allow networks to support both IPv4 and IPv6 services during the period in which IPv6 applications and services are beginning to emerge. The dual-stack approach allows transport providers and applications designers to introduce IPv6 gradually into IPv4 networks.

Dual stack implementations are easy to understand: when communicating with another IPv6 network device, it behaves just like an IPv6-only node. When communicating with an IPv4 network device, it behaves just like an IPv4-only node. Usually both stacks are in operation together, but many implementations have a setting that allows turning off or on one of the stacks.

An ironic and counter-intuitive downside to dual stack approaches is that every machine that is going to support dual stack solutions requires an IPv4 address. Obviously, the downside is that implementation of IPv6 is motivated by the scarcity of IPv4 addresses. A solution that depends upon IPv4 addresses simply extends the period in which IPv4 scarcity is a problem. It also means more overhead in the local network: for instance, the IPv4 node will use mechanisms to obtain and use IPv4 addresses (e.g. DHCP or static configuration) and the IPv6 node will use its separate set of mechanisms to set up IP addresses (e.g. static configuration or autoconfiguration).

Dual stack networks are infrastructures that support both IPv4 and IPv6 packets. In these networks, each router must keep separate routing tables for the two addressing schemes. In addition, network management tools are often duplicated across the two addressing schemes.

In practice, dual stack is often not implemented throughout an entire network. Instead, in dual stack environments some parts of the network are dual-stacked, while others are IPv4 only or IPv6 only. Clients and end-nodes in the network are often dual-stacked so that they can connect to IPv4-only legacy services while also being able to take advantage of newer IPv6 services.

Those legacy services are the key motivation to dual-stack approaches: there are applications that are so old or have their network code so deeply embedded that they may never be adapted or re-written for IPv6. In practical terms this means that there will be legacy applications and services that are IPv4-only and will never be migrated to IPv6. The implication is that there will always be a need for IPv4 access for these older, legacy applications. Even though there will be a steady shift to IPv6 compliant services and applications, the evolution will take many years – and in some cases where the applications are deeply embedded, perhaps decades.

The complexity obviously includes supporting multiple network stacks on the devices that are dual-stacks. But routers might also require support for multiple routing protocols and capacity to do routing calculations for multiple stacks. We shall also see that there is a clear implication in dual-stack implementations for security. Security requirements and administration is different for IPv4 compared to IPv6 and security devices, such as firewalls and border gateways, need separate capacity for managing access control for each protocol.

The complexity also includes some implications for the DNS and network access. For example, when a dual-stacked client connects to a server (for instance http://www.google.com) it issues two separate DNS requests – one for IPv4 and the other for IPv6. After receiving the responses, the client usually prefers the IPv6 connection over the IPv4. If, for whatever reason, the usage of that address was non-successful, an alternate address will be used, potentially a valid IPv4 address to connect to the remote location. The additional overhead associated with the DNS has obvious implications for bandwidth and DNS server capacity. Perhaps an even greater problem is when a DNS query results in a failed attempt to use an unreachable address. For instance, when the DNS returns both IPv6 and IPv4 addresses, but the node's IPv6 connectivity is broken. It tries IPv6, times out and then falls back to IPv4. This can take many tens of seconds.

4.1.2 Supporting Dual Stacks

IPv4 is likely to be with us for the foreseeable future. Other widely used network protocols, such as IPX/SPX and Token Ring have largely disappeared over a short number of years. IPv4 is very different, unlikeprevious legacy protocols IPv4 is deployed much more extensively and is integrated more tightly into the modern world's infrastructure. At best it is likely to take many decades before IPv4 is largely replaced by IPv6.

As a consequence, networks will have to support both legacy IPv4 and IPv6 well into the future. This has an impact on infrastructure and management requirements. Although it might be easy to make the assumption that having two protocols doubles the infrastructure and management requirements. This is an over-simplistic view. In some cases, the management overhead is reduced but more commonly it is significantly increased. In some cases, there is a need for a substantial investment in infrastructure to support both protocols; in other cases no infrastructure investment is required. For the majority of organisations the truth will be between these extremes[19].

Overall, IPv6 brings greater complexity to the network. Much more than double that of IPv4. This is not due to the IPv6 protocol alone but to the additional new features and transition mechanisms included in or with IPv6. Some of these bring with them extra complexity due to the interaction between the protocols. Transition mechanisms such as Teredo and 6to4 bury IPv4 address information into the IPv6 addresses and therefore create a complex interaction between IPv4 and IPv6.

It is important to note nearly all networks today already need to support dual-stacks even if they have not formally deployed IPv6. Almost all modern operating systems, network equipment and applications now support IPv6 by default and in many cases will automatically use IPv6 in preference to IPv4. Therefore, most networks will already be seeing IPv6 traffic of some form. This is an urgent issue for all organisations as at the very least they should be considering the security implications of dual-stack networks[20].

4.1.3 Tunnelling

Tunnelling strategies are simple in concept: to connect remote islands of IPv6 networks, you use IPv4 as a “tunnel.” Each IPv6 packets gets put into an IPv4 packet, goes through the IPv4 network, and emerges in the IPv6 network. Tunnelling is sometimes referred to as “encapsulation.” The core idea is to be able to use IPv6 across networks that do not have IPv6 transit.

The key techniques are:

- Putting the IPv6 packet inside a IPv4 packet; called “encapsulation”;
- Retrieving the IPv6 packet from the payload of the IPv4 packet; called “decapsulation”;
- Managing the end-to-end connectivity of the IPv4 network between the IPv6 islands; called tunnel management.

[19] An examination of the costs and deployment options for Dual Stack IPv6/IPv4 support is covered in Section 7.

[20] These security implications are discussed at length in Section 7.5.

The "tunnel" is the IPv4 network used as the unwitting transport for connectivity between IPv6 networks.

For example, if an ISP does not provide native IPv6 transport, tunnelling allows an enterprise network to run IPv6 across diverse and geographically separated areas. The corporate network would use IPv6 and to reach each island in the network, the IPv6 packets would be encapsulated inside IPv4 packets.

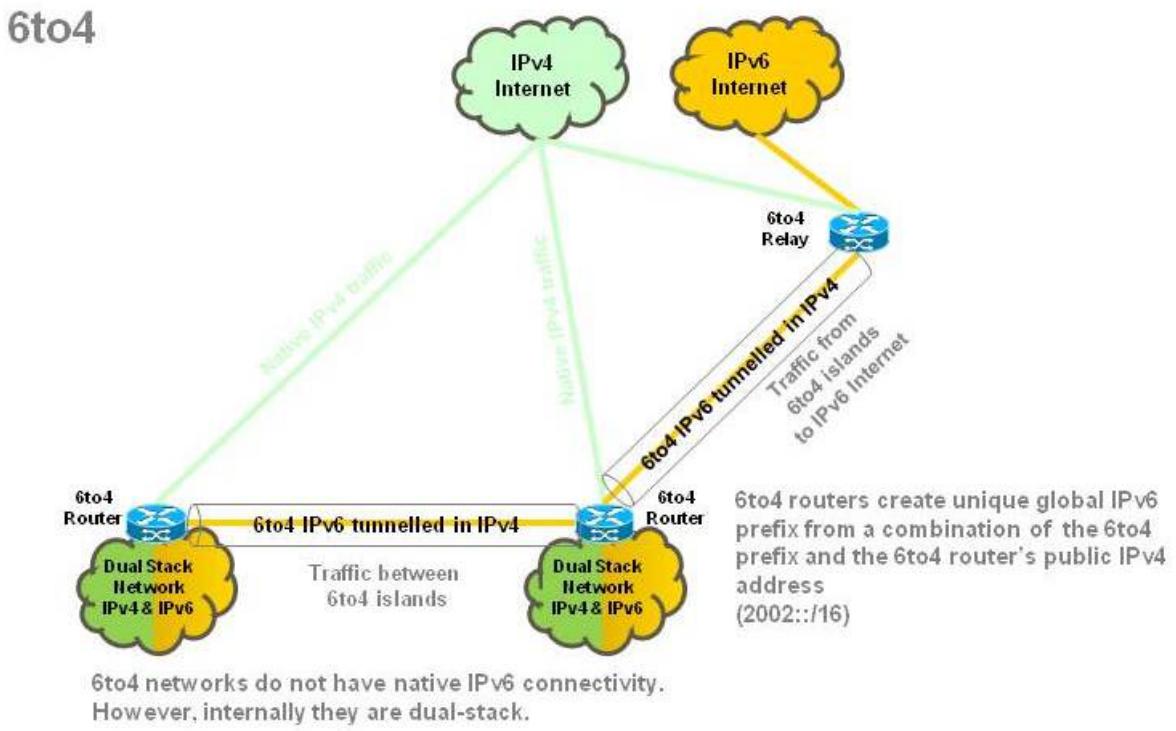
There are two kinds of tunnelling supported in the modern IPv6 Internet:

1. Automatic tunnels, where IPv6 packets use a gateway that is located on a special router that does the encapsulation. The advantage is that the links between the IPv6 aware routers do not need to be set up in advance.
2. Manually configured tunnels, where the tunnel endpoints are manually configured at the routers which do the encapsulation and decapsulation.

Tunnelling is a phenomenally complex topic because, over time, several different strategies for tunnelling have emerged, each with benefits and weaknesses.

6to4

6to4 is a tunnelling strategy that allows separate IPv6 networks to exchange packets without setting up an explicit, manually configured tunnel. In 6to4, specially prepared routers, called 6to4 routers, provide gateways between the IPv6 networks. The IPv6 packets are encapsulated inside an IPv4 packet at the gateway.



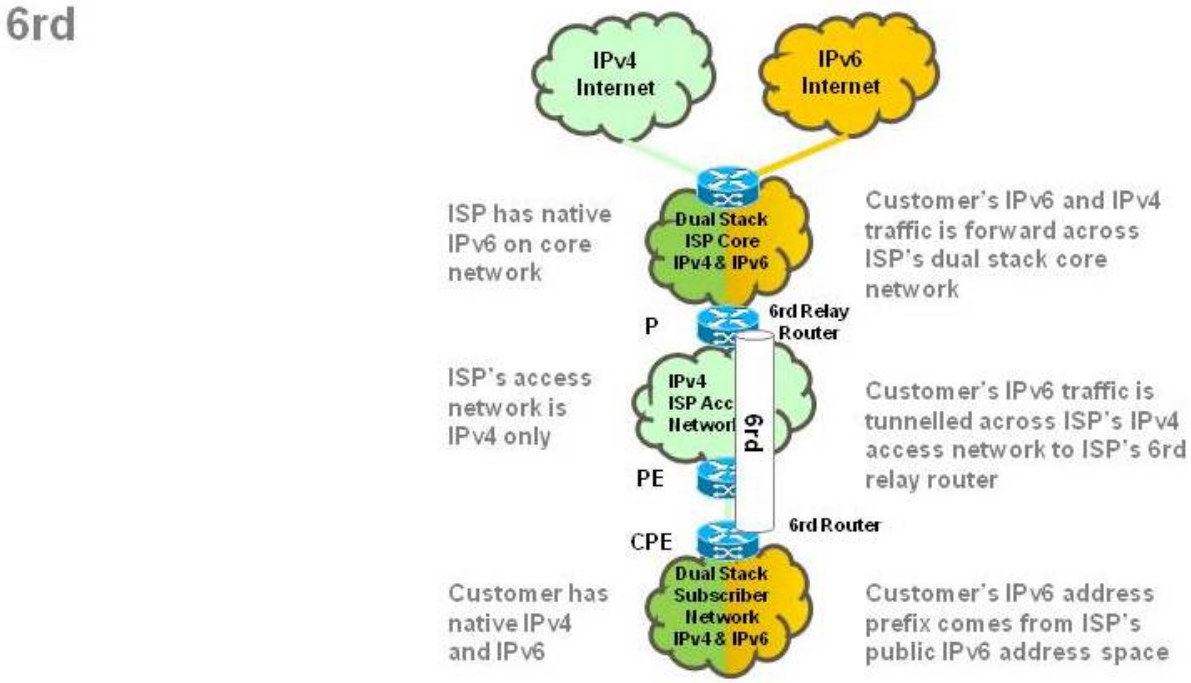
Any global IPv4 address that is assigned to a host or router can have a special IPv6 address assigned to it (by adding a special IPv6 prefix to the IPv4 address). The resulting address is special: it is called a 6to4 address to distinguish it from native IPv6 addresses. An important limitation of 6to4 addresses is that private addresses are not allowed to be used to create a

in 6to4 address. Also, the IPv4 packets are specially marked with a protocol number of 41 so that they can be easily identified[21], and routed, as 6to4 packets.

6to4 relays provide connectivity to the global IPv6 Internet. 6to4 routers connect independent islands of 6to4 together. In theory, as the number of commercial networks that support 6to4 grows, the number of public 6to4 relay routers will increase[22].

6rd

6to4 has some significant problems in practice. First, it relies on the 6to4 prefix to find 6to4 routers. However, the 6to4 prefix is not globally routable on the IPv6 Internet, which means that nodes on some parts of the IPv6 Internet cannot reach 6to4 networks or nodes. 6to4 also has a number of security issues that are difficult to mitigate leaving some network operators to block 6to4 traffic (resulting in the previous problem).



"IPv6 Rapid Deployment" (6rd) is an attempt to improve on 6to4 by restricting its use within an ISP's networks. An ISP that supports 6rd has its own relay router that can only be used by people and networks under the ISP's administrative control. The other benefit of this change is that, since the ISP must supply its own IPv6 prefix (instead of using the special 6to4 prefix), 6rd networks are reachable by anyone who has a native IPv6 network.

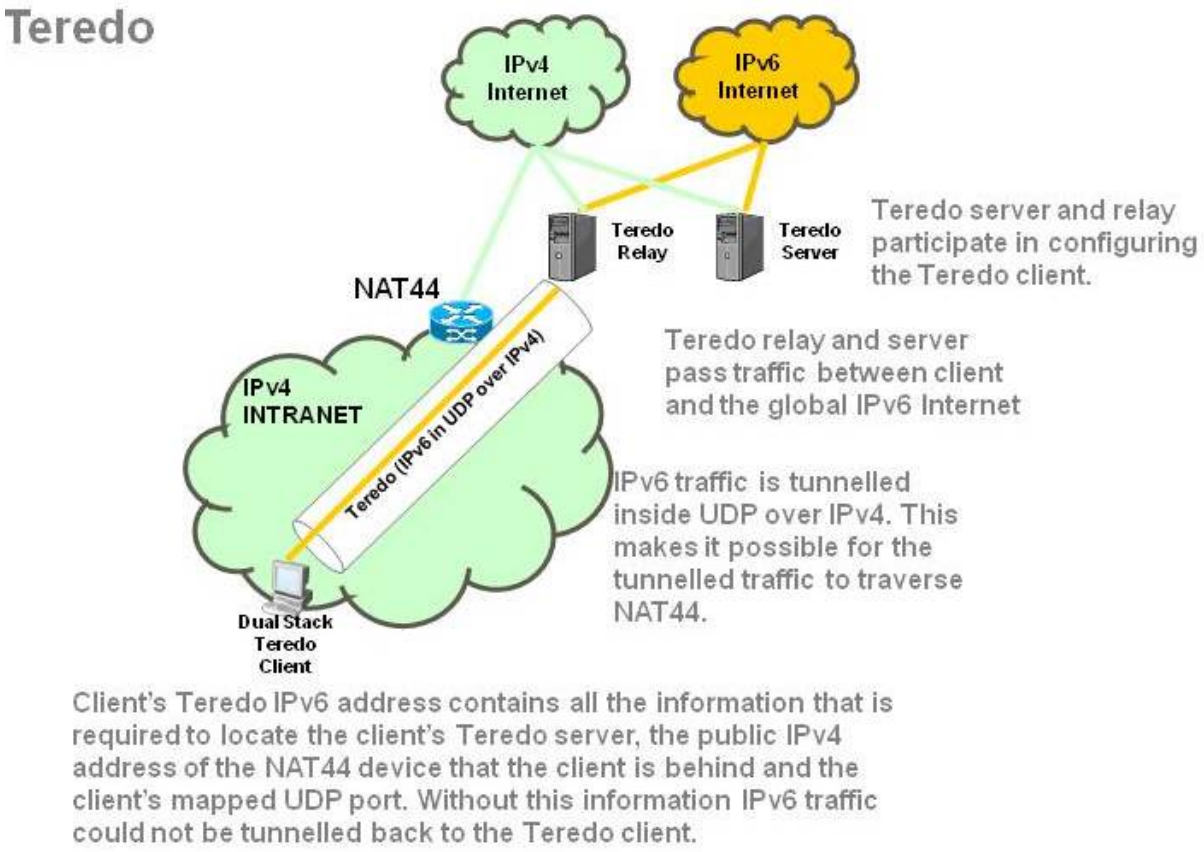
ISATAP

Another approach to automatic tunnelling is the Intra-Site Automatic Tunnel Addressing Protocol, (ISATAP). ISATAP is a special approach that allow for IPv6 connectivity for dual-stack nodes over an IPv4-based intranet. Instead of forcing the effort onto routers in the network, the end nodes use the dual-stack implementations to build tunnels for themselves. ISATAP is designed specifically for private intranets and not for the public IPv4 Internet.

[21] A number of tunnelling techniques use protocol 41 encapsulation. ISATAP, 6rd etc.
[22] However, in the public network, the support for 6to4 as measured by the percentage of 6to4 traffic is declining.

1.1.2.3 Teredo

Tunnelling is complex: 6to4 is designed to make IPv6 available over the global IPv4 Internet using public IPv4 addresses, while ISATAP is designed for Intranets and is not intended to be used on the public Internet. But the most complex type of tunnelling occurs when a tunnel is built to cross a Network Address Translation (NAT) boundary. NAT boundaries are at the edges of almost every residential and commercial network in the world.



It would seem intuitive that there is a need for a tunnel technology that can send IPv6 packets through a network regardless of whether there was a NAT implementation between the endpoints of the IPv6 connection.

Teredo is the protocol that was designed to allow for IPv6 hosts to communicate with each other regardless of whether layers of NATs were in between the two endpoints. Crucially, it is designed to provide clients that are on an IPv4 Intranet behind one or more layer of NAT with IPv6 connectivity.

Many networks in the UK are built using NATs. Residential users, for instance, have a home access box that functions partly as a NAT. There are two significant issues when trying to tunnel IPv6 in IPv4 over NATs:

1. NATs provide the interior network with private address space. Thus, home computers or gaming equipment get assigned private address space when turned on.
2. Most NATs filter out certain kinds of packets based on particular implementation choices.

6to4 and NAT do not work well together because 6to4 does not work with private address space.[23] In addition, most NATs do not support protocol 41 tunnels. ISATAP works in intranets, however ISATAP tunnels require termination on an ISATAP router that provides connectivity to the global IPv6 Internet.

Teredo is a very complex protocol and beyond the scope of this paper to cover in detail. However, because it transports IPv6 packets in a User Datagram Protocol (UDP) payload, the design allows users sitting behind a traditional NAT to access the global IPv6 network. As long as there are NATs in residential and customer networks, some way will have to be found to connect devices inside the NAT's network to IPv6 networks in the public Internet. Teredo is one such technique.

Teredo's essential feature is to encapsulate the IPv6 packet in a IPv4/UDP datagram which will not be intercepted or interfered with by the NAT. As a result, the IPv6 computer behind the traditional NAT is able to work as a tunnel endpoint even when they are using private, RFC 1918 address space.

4.1.4 Translation

A completely different transition strategy is to provide translation: a device that will translate an IPv4 packet into and IPv6 packet; and vice versa. This strategy seems to be a simple enough proposition: where needed Internet –connected devices translate, or have access to a device that can translate, between IPv4 and IPv6 networks.

For instance, as new networks are given IPv6 addresses, the legacy networks will need access to the new services. That way, an older device can still communicate with new services on the IPv6 Internet as long as a protocol translator is available.

Like tunnelling, translation would be a transitional approach to deploying IPv6. As more and more of the network was IPv6-enabled, the need for translation would gradually disappear.

Clearly, there would be a need to provide translation in the other direction as well. A new node in an IPv6-only network should still be able to connect tof IPv4 legacy applications or services (instance.g., a search engine available on an IPv4 only web site). In this instance, the host computer's IPv6 network packet would need a service to translate into IPv4 packets.

Translation and its Perils

Address translation has been in use for a long time. The Network Address Translation (NAT) devices that act as the boundary in most residential and small business offices use private IPv4 address space on the interior network and then use the NAT box to translate the private address to a single or limited number of public addresses.

Adding protocol translation seems like it should be a natural extension of NAT. The result was a standardized protocol translation tool called NAT-PT (Network Address Translation - Protocol Translator). Unfortunately, in practice, NAT-PT has been found to have some

[23] Again, IPv4's RFC 1918 private address space.

serious problems[24] – and in a fairly dramatic event, the IETF moved to deprecate its use in 2007.

Key problems with translation as defined by NAT-PT include:

- Problems with any protocols that embed IP addresses or port numbers directly in packet payloads;
- Problems with protocols[25] that base integrity mechanisms on source or destination IP addresses;
- Problems with state management and timeouts at the box doing the NAT-PT translation;
- Problems with packet reconstruction in the case of fragmentation;
- Inability to handle multicast traffic; and,
- The requirement to use the DNS as a tool for address mapping.

The problems with NAT-PT caused the IETF to abandon this style of translation.

Is Translation Possible?

Despite the failings of NAT-PT, protocol translation will be necessary during the transition to IPv6. There are a number of scenarios where an IPv6-only and IPv4-only nodes will need to interact. Some of the problems with NAT-PT, identified above can never be solved and all protocol translators will suffer from these issues. As a result, there is no such thing as a perfect protocol translator and it is important to consider its limitations in implementation. It may prove best to avoid translation if at all possible.

However, for the cases where translation cannot be avoided, new standards have emerged for translators that reduce the translation problems by limiting their scope.

NAT64[26] and DNS64[27] allow IPv6-only nodes to reach IPv4 nodes. This avoids many of the problems of NAT-PT by removing the NAT46 translation functionality which was at the root of many of the problems. NAT64 and DNS64 still suffer from some of the failure modes found in any protocol translator but they are substantially more robust than NAT-PT.

It is likely that NAT64 and DNS64 will become widely used. In particular, some mobile operators are using these in their 4G deployments to provide connectivity to IPv4 nodes from IPv6-only mobile nodes.

[24] Although it is still widely deployed. NAT-PT has well-documented, significant problems and failure modes. Many of these problems have been reported upon in RFC 4966: http://www.ietf.org/rfc/rfc4966.txt

[25] See RFC 4966 for examples of these

[26] RFC 6146, Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, http://tools.ietf.org/html/rfc6146.

[27] RFC 6147, DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers, http://tools.ietf.org/html/rfc6147.

4.2 Carrier Grade NATs

Carrier Grade NAT (CGN), also known as Large Scale NAT (LSN) or NAT444, is a technique that makes it possible to continue to provide an IPv4 service with fewer public IPv4 addresses than were previously required.

The Internet was designed with each host or node being assigned at least one IP address. As we have seen, in the mid-1990s it became apparent that the IPv4 address space was not sufficient for the growing Internet and that it would be exhausted if action was not taken. As a result, addresses began to be shared. Address sharing was implemented using a technique called Network Address Translation (NAT). This form of NAT is referred to as NAT44. NAT44 has delayed the exhaustion of the IPv4 address space for over a decade, effectively saving the Internet. However, there are disadvantages to NAT44. NAT makes the network more complex and harder to manage, it limits performance, restricts scalability and stops or hinders the deployment of many types of applications.[28] Despite these problems, NAT44 is very widely deployed and significant efforts have been put into mitigating its limitations.

4.2.1 NATs Inside NATs

CGN is based on multiple layers of NAT44. This compounds all of the problems found with NAT44 and introduces new problems. NAT44 and CGN work by sharing addresses amongst groups of users. This is possible by using, transport layer port numbers, to uniquely identify the different users who are sharing the same address.

The problems of NAT and CGN have been widely discussed and documented[29,30]. The main points that are common to NAT and CGN are summarised below:

- Breaks end to end connectivity and makes peer to peer applications difficult to implement
- Breaks many application layer protocols[31]
- Breaks network layer security (e.g. IPSec)
- Introduces a single point of failure into the network
- Makes load balancing difficult
- Has security issues due to maintaining state
- Requires public IPv4 addresses to reach the global IPv4 Internet

CGN introduces some new problems and compounds others[32]:

- Peer-to-Peer applications become even harder to implement. Specifically, many of the solutions that work in NAT fail with CGN

[28] See, for example, Experience from NAT44 Translation Testing, http://tools.ietf.org/pdf/draft-li-behave-nat444-test-01.pdf

[29] An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition, RFC6264.

[30] Issues with IP Address Sharing, RFC6269.

[31] For examples, see RFC 6269; http://tools.ietf.org/pdf/rfc6269.pdf

[32] Assessing the Impact of Carrier-Grade NAT on Network Applications, at http://tools.ietf.org/html/draft-donley-nat444-impacts-04

- Devices and software that need to determine if an IPv4 address is a public address will have to be updated
- Keeping records for law-enforcement operations is significantly more difficult
- It is impossible or very difficult for end-users to host services on well-known ports
- Common IPv6 transition mechanisms such as 6to4 and Teredo will not work. This will make the transition to IPv6 harder for subscribers
- Some applications fail
- Performance degradation is experienced with some applications[33]
- Geo-location information is lost
- Deployment of CGN delays the transition to IPv6 and will result in double costs (once to implement CGN and again to implement IPv6)
- May trigger Distributed Denial of Service (DDoS) protection measures
- Some web applications will degrade or fail[34]. Graphic example is Google Maps. As the number of port numbers available to a subscriber is reduced less and less of the map will be displayed until eventually no map appears at all[35].

Despite all these problems with CGN, it will be widely deployed to maintain connectivity to the legacy IPv4 Internet. One question remains: is CGN a solution to the IPv4 address exhaustion problem? There are two parts to the answer; first it is a poor solution and second, it is not a long term solution.

The list of CGN problems illustrates that CGN does not provide an equivalent level of service or functionality to a non-NATed network.

CGN is also not a long term solution – however, it does provide a short term solution for ISPs that do not have enough IPv4 addresses to be able to give one public address to each of their subscribers. It allows them to share public IPv4 addresses across many subscribers.

4.2.2 NATs and Ports

Any form of NAT requires public IPv4 addresses to function. Each IPv4 address can only be shared amongst users when there are enough free transport layer ports available to multiplex the addresses. Depending on the NAT implementation, over 60,000 ports may be available for multiplexing user connections through each public IPv4 address. This sounds a lot, until you consider that one device might consume large number of ports.

Take for example the popular application Google Maps. Google Maps typically requires thirty to fifty ports to function correctly. Less than this and it will not be able to fully display a map.

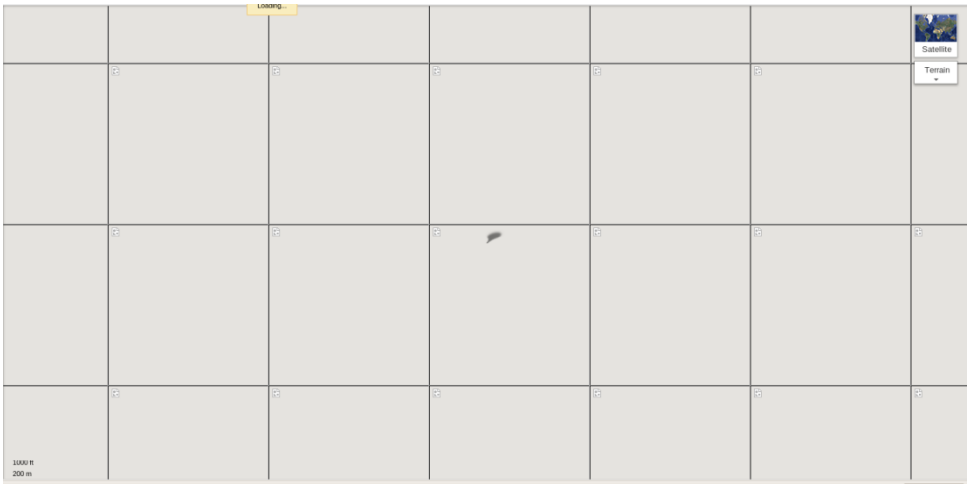
[33] Examples of performance degradation is also examined in RFC 6269; http://tools.ietf.org/pdf/rfc6269.pdf

[34] Further examples are at: http://tools.ietf.org/html/draft-donley-nat444-impacts-04

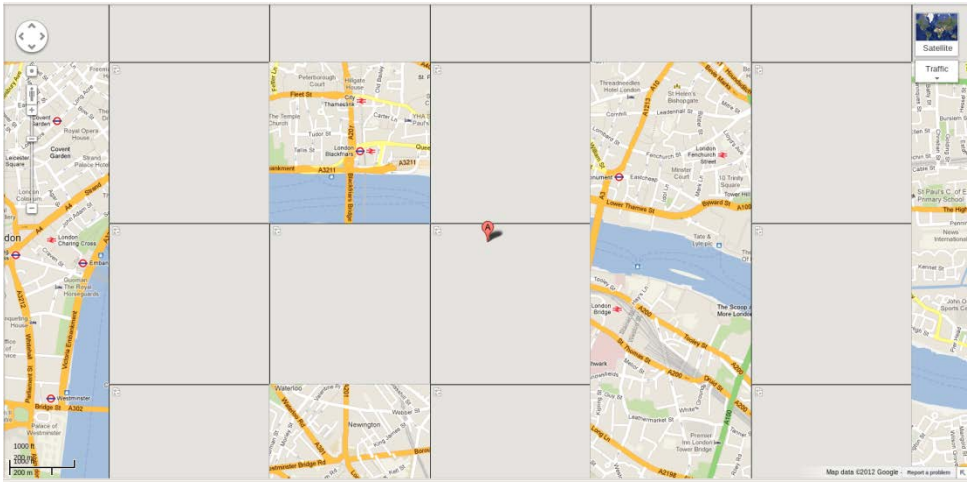
[35] From IPv4 to IPv4/6 Dual Stack Internet, Dr Shin Miyakawa, NTT, August 2011, at http://meetings.apnic.net/__data/assets/file/0011/38297/Miyakawa-APNIC-KEYNOTE-IPv6-2011-8.pptx.pdf

This is illustrated in the screenshots[36] below for a range of connections.

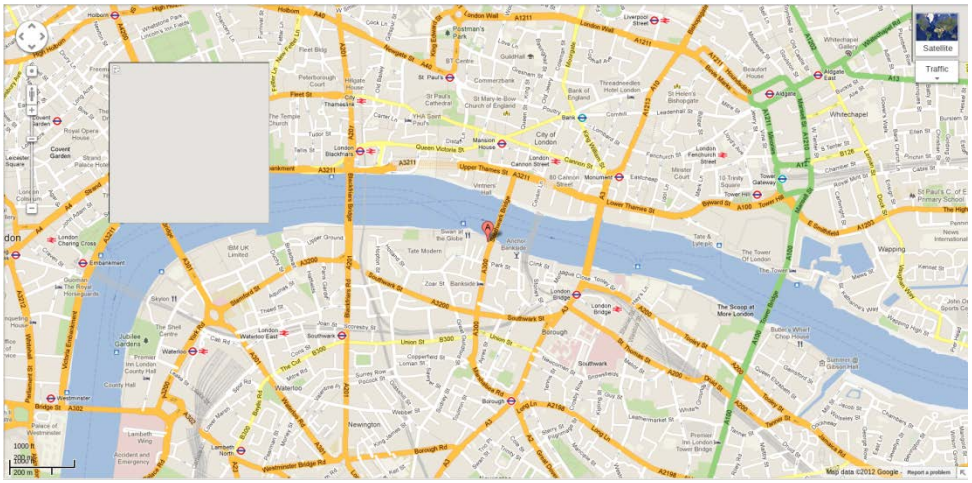
5 connections



10 connections

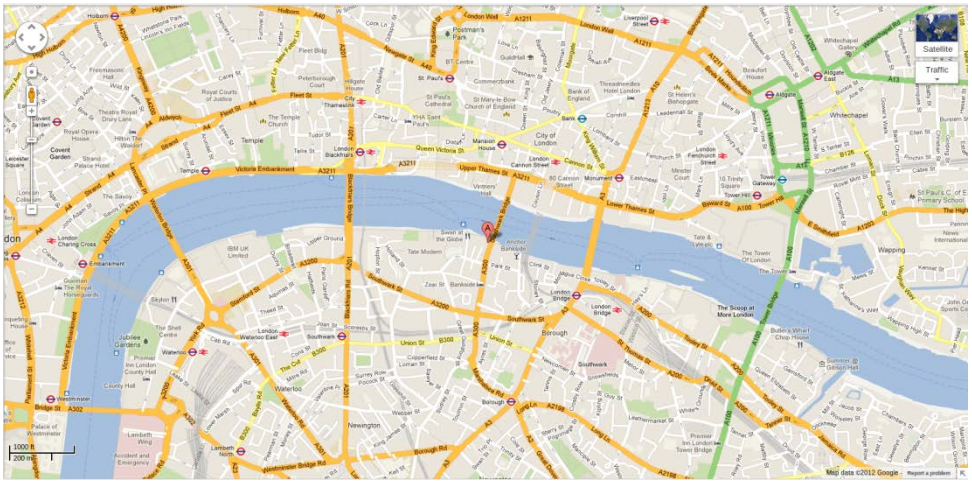


20 connections



[36] Screenshots provided by Erion Ltd.

30 connections



A home, a small business or a medium sized business will all have many people using many devices each of which could be using applications that consume a large numbers of ports. The requirement for ports is likely to increase over time. This greatly reduces the number of subscribers that can be multiplexed through a single IPv4 address.

Furthermore, ISPs are likely to be forced to limit the number of ports per subscriber to a set maximum to mitigate certain types of DDoS (Distributed Denial of Service) attacks. The choice of this limit will be a balance between providing a service to customers and protecting their infrastructure from attacks. A limit that is too low could stop customers using Google Maps or similar applications. The number of ports per subscriber is also an important metric when considering the potential for Denial of Service attacks where a perpetrator effectively exhausted the available ports – thus making services unavailable for subscribers.

4.2.3 The Future for CGN Approaches

It is difficult to estimate how long CGN will enable ISPs to continue to provide an IPv4 service. The answer will vary depending on the ISP's number of customers, stock of IPv4 addresses and the profile of the customers (that is, how many connections they use). From all indications, it appears that CGN cannot provide the necessary long term solution that IPv6 offers. CGN will present new and difficult operational challenges for operators and subscribers.

CGN will be necessary in some networks to provide a legacy IPv4 service. However, this does not mean that IPv6 connectivity will not be required as well. As the rest of the world migrates to IPv6, customers will increasingly require IPv6 connectivity. Not only does CGN not provide IPv6 connectivity it actually hinders its deployment.

It is important to remember that CGN is not applicable to many end-users. Any end-user that requires one or more public IPv4 addresses cannot be placed behind CGN. These include many businesses that require public IPv4 addresses to operate Internet services (e.g. businesses that provide public access to services within their own network).

4.2.4 CGN and IPv4 Exhaustion

Why then do some argue that CGN is a solution to the IPv4 address shortage?
For some organizations there are significant business benefits to be had from delaying the deployment of IPv6 which may include:

- Extending the life of their investment in IPv4
- Delaying the cost of deploying IPv6
- Maximizing any advantage over competitors who are unable to obtain IPv4 addresses (an existing stock of IPv4 addresses coupled with CGN will allow the ISP to continue to provide an IPv4 service without having to obtain large numbers of additional addresses)
- Making it more difficult for new competitors to enter the market (note that if IPv6 was globally deployed an organization's stock of IPv4 addresses would no longer be a market advantage)

The result is a complex technical and economic balance. Incumbent and legacy service providers may be able to trade the disadvantages of CGN (which mainly affect their customers and not themselves) against the economic and competitive benefits that come from extending the lifetime of their IPv4 networks. In some cases, the economic and competitive advantage may be enough to significantly delay IPv6 investment and deployment – while passing along the disadvantages of CGN to the end customer.

4.3 Comparing the Approaches

The three main categories of approaches to deploying IPv6. These are:

- Native Dual-stack
- Tunnel
- Protocol translation

Each category has many different permutations of implementation. However, this section seeks to compare them at a high level to see their overall pros and cons and which approach or approaches are the most desirable.

Approach	Pros	Cons
Dual stack	- Cleanest approach. - Allows all features of IPv4 and IPv6 to be utilised - Provides for best performance and minimum overheads - Fewer failure mechanisms compared with other approaches	- Requires upgrade to dual-stack of all network infrastructure, network services, applications and end nodes
Tunnel	- Does not require infrastructure to be upgraded to support IPv6 - Can be used where non-native IPv6 services are not available - Some approaches are largely automatic and are reasonably easy to deploy	- Overheads of tunnel can affect performance - Some features of IPv6 will not work - Failure mechanisms exist with some techniques (e.g. 6to4) - Many security issues - In some cases not scalable

	- Can appear to be a native service to end-users	
Protocol Translation	- Translation is the only solution where IPv6-only nodes wish to reach IPv4-only nodes or vice versa[37] - Can be used to pseudo IPv6 enable many IPv4 nodes in one translator[38]	- Failure mechanisms always exist with protocol translation - Performance, scalability and availability are limited by involvement of a translation device - Some features cannot be translated - Some higher layer protocols cannot be translated without an Application Layer Gateway (ALG) - Security issues

Overall the best, but usually the hardest implementation approach, is the native Dual-stack approach. Protocol translation is best avoided if at all possible as it has by far the most serious disadvantages. Providing a Dual-stack service using tunnelling is better than utilising protocol translation. This is why, for example, Dual-Stack Lite (DS Lite) is a better solution than IPv6-only and protocol translation, because DS Lite allows for the use of native IPv6 and native IPv4 even though the IPv4 goes through NAT44.

4.3.1 One Size Fits None

We will see a variety of scenarios when organizations move to IPv6. Because the scenarios are so different, it is simply not possible to pick a single strategy for transition to IPv6. There can be no single strategy that covers all requirements or be a “best practice” for all scenarios.

Almost always, IPv6 is not a greenfield implementation. As a result, the current infrastructure and the goals and needs of the transition determine which of the strategies in this section will work best. In many cases, a variety of strategies are combined – and we will see many examples of this as we look at IPv6 implementations in practice.

The fact that one size does not fit all makes implementation more complex and has, in some cases, led to delay in the integration/transition for IPv6.

[37] Note that NAT-PT, NAPT-PT, NAT64 and NAT46 are not the only kinds of protocol translation transition mechanisms. However, they are the most common. For example, translation can take place at higher layers such as the Transport layer using the Transport Relay Translator (TRT) mechanism.

[38] There are many products that make it possible to give the impression that whole data centres full of servers are IPv6-enabled when in fact they are actually IPv4-only nodes sitting behind a translator. There are many disadvantages to this approach but there are scenarios where it maybe necessary.

5. IPv6 – The Deployment Experience

IPv6 has been under development since before 1995 when the first IPv6 RFC[39] was issued. In the years since then, IPv6 has been deployed in many countries and organisations. Today there is a wealth of experience of deploying IPv6. This section looks at this experience and breaks it down into a number of categories; by region and by type of organisation.

When reviewing IPv6 deployment experience, it is useful to consider the current status of deployment using selected measures. As will be seen later in this report, there are a large number of different measures attempting to measure the status of IPv6 deployment. There is no one measure that indicates the current status of IPv6 deployment accurately. So alongside descriptions of IPv6 deployment experience some measures have been included.

Population [40]	6,930,055,154
Internet Users	2,267,233,742
IPv4 Addresses Allocated	3,706,650,000
IPv6 Prefixes Allocated/Live	42,451 / 8,171

These measures require some background explanation which is given in the following table and associated references. These statistics are useful for a rough comparison of IPv6 deployment by region.

Population	The estimated population as of 2011
Internet Users	The estimated number of Internet users as of June 2011
IPv4 Addresses Allocated [41]	This information is collated from the RIRs as of March 2012
IPv6 Prefixes Allocated /Live [42]	The left hand figure is the number of prefixes allocated and the right hand figure the number that are routable
Google IPv6 Adoption [43] [44]	This figure is an estimate of how many users of Google's websites are IPv6-enabled. This figure may be affected by local filters (e.g. China) and Google' presence in a country (e.g. China).
Web (top 50 Alexa list)[45]	This is the percentage of the top 50 Alexa websites that have IPv6 addresses that work. There can be a wide variation in results depending on sample size.
Email (top 50 Alexa list)[46]	This is the percentage of the top 50 Alexa domain names that have IPv6 addresses for their Email servers (MX records) that work. There can be a wide variation in results depending on

[39] Internet Protocol Version 6 (IPv6) Specification, (Obsoleted by RFC 2460), http://www.ietf.org/rfc/rfc1883.txt.

[40] Internet World Stats, http://www.internetworldstats.com/ as of June 2011.

[41] IPv4 addresses in use by country, http://www.bgpexpert.com/addressespercountry.php, as of March 2012.

[42] "IPv6 Deployment Aggregated Status (IPv6 Networks), http://www.vyncke.org/ipv6status/prefixes.php as of 14th March 2012.

[43] Google IPv6 Statistics, http://www.google.com/intl/en/ipv6/statistics/ as of 14th March 2012.

[44] The Google IPv6 statistics for China may possibly be affected by Google's exit from China.

[45] IPv6 Deployment Aggregated Status, http://www.vyncke.org/ipv6status/index.php, as of 14th March 2012.

[46] IPv6 Deployment Aggregated Status, http://www.vyncke.org/ipv6status/index.php, as of 14th March 2012.

	sample size.
DNS (top 50 Alexa list)[47]	This is the percentage of the top 50 Alexa domain names that have IPv6 addresses for their name servers and that can be queried over IPv6. There can be a wide variation in results depending on sample size.
National Mandates	Does this country have any mandates for the adoption of IPv6?
Government IPv6 Agencies	Does this country have any government agencies or government funded organisations promoting IPv6?
GDP[48]	Gross Domestic Product

One difficultly with many of the above measurements is the sample size and where the sample was obtained. For example, a number of the sites collecting IPv6 statistics make measurements of deployments based on popular sites on the Alexa list. This considers deployment from the viewpoint of popular websites. However, not all important or large websites are popular and not all appear on the Alexa list. Another approach is to look at domain names held by leading businesses that may or may not be high on the Alexa list. We[49] have used the Fortune500 top 100 and the FTSE 100 list of companies to create a list of major companies whose IPv6 deployment status can be measured. The results from March 2012 are shown below:

List	Web Sites Enabled	Name Servers IPv6-enabled	Mail Servers IPv6-enabled
Top 100 Fortune500 Companies	0%	13%	0%
FTSE100	1%	16%	0%

In 2009, the same measurements had only 4% of name servers enabled, 0% of mail servers and 0% of webservers[50].

World-wide, the majority of client nodes are IPv6 capable. However, very few of them use IPv6 as their local access networks are not IPv6-enabled[51].

[47] IPv6 Deployment Aggregated Status, http://www.vyncke.org/ipv6status/index.php, as of 14th March 2012.

[48] The World FactBook, CIA, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html.

[49] A list built by Erion – http://www.erion.co.uk/

[50] http://www.ipv6consultancy.com/ipv6blog/wp-content/uploads/case-study-ipv6-enabling-malaysias-my-domain-web.pdf

[51] Most nodes are dual-stack nodes, that is they support IPv4 and IPv6. However, the order in which either protocol is used depends on a number of factors. See RFC 3484 for details.

5.1 In Europe (EU)

Population	816,426,346
Internet Users	500,723,686
IPv4 Addresses Allocated	152,000,000
IPv6 Prefixes Allocated /Live	173 / 162
Google IPv6 Adoption	N/A
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP (USD)	N/A

In Europe, the EU has long supported and encouraged the adoption of IPv6[52]. A number of EU projects have invested in IPv6 technology, supporting IPv6 deployment and in providing basic IPv6 education. Further the EU mandated that all EU funded research projects should be IPv6 ready[53].

The EU has run a number of IPv6 events and projects to encourage awareness of and the adoption of IPv6. These include the 6DISS[54], 6NET[55], Go4IT[56] and other projects[57].

The status of deployment of IPv6 in European countries varies widely. The maturity of IPv6 in a country is not related to the number of IPv6 prefixes allocated. For example, the UK has a large number of IPv6 prefixes allocated but very few large-scale deployments of IPv6. This is illustrated by a comparison between Slovenia where 23% of LIRs have no IPv6 and the UK where 53% of LIRs have no IPv6.

5.2 In North America (USA)

Population	313,232,044
Internet Users	245,000,000
IPv4 Addresses Allocated	1,538,160,000
IPv6 Prefixes Allocated /Live	2649 / 2420
Google IPv6 Adoption	0.55%
Web (top 50 Alexa list)	0%
Email (top 50 Alexa list)	2%
DNS (top 50 Alexa list)	24%
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP (USD)	$15,040,000,000,000

[52] For instance, see http://europe.eu/rapid/pressReleasesAction.do?reference=IP/01/591&format=HTML&aged=0&language=EN&guiLanguage=en

[53] Also at: http://europe.eu/rapid/pressReleasesAction.do?reference=IP/01/591&format=HTML&aged=0&language=EN&guiLanguage=en

[54] See: http://www.6diss.org

[55] At: http://www.6net.org

[56] http://www.go4-it.eu/

[57] http://www.ec.ipv6tf.org/in/i-index.php and http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=7871093

Prior to 2003, interest in deploying IPv6 in the USA was almost nonexistent. This was despite significant efforts by voluntary organisations such as the North American IPv6 Task Force[58] and the IPv6 Forum[59].

Then in 2003, John Stenbit, the assistant secretary of defence, signed a memo mandating the adoption of IPv6 by the Department of Defence (DoD)[60]. The memo set a deadline of 2008. The DoDs interest in IPv6 stemmed from their need for vast numbers of IP addresses to support their vision of a networked battlefield.

John Stenbit's memo sparked a substantial rise in interest in IPv6. Organisations that were suppliers to the DoD rushed to IPv6 enable their products and other organisations, saw this as an opportunity to enter the market with new IPv6-enabled products and services. Whilst financial backing for this mandate was lacking, it still resulted in many suppliers and aspiring suppliers, IPv6 enabling products and creating IPv6 services. This resulted in an increase in IPv6-enabled products and an increase in IPv6 skills in the industry.

In January 2004, the US Department of Commerce (DoC) released a Request For Comments[61] (RFC) stating that the President's National Strategy to Secure Cyberspace had directed the Secretary of Commerce to form a task force to examine the issues implicated by the deployment of Internet Protocol version 6 (IPv6) in the United States. As a result of this process, the Office of Management and Budget (OMB) mandated the deployment of IPv6 in agency networks by June 2008. This again had the effect of simulating the development of IPv6 products and services in the US. In particular, the fact that IPv6 is a requirement for network enabled products and services purchased by the US government, has had a significant impact on the IPv6 market in the US.

There are a number of consequences of the government support for IPv6 in the US. The US defined profiles for IPv6 conformance that have global significance. The country gained many skilled IPv6 professionals as a result of the educational efforts initiated in response to the mandates. The mandates raised the priority of IPv6 deployment in the Service Provider market which made it easier for these services to be provided to the general market.

Another feature of the IPv6 mandates in the US has been the production of a number of world leading guidelines, profiles and testing methods for IPv6[62].

---

[58] The North American IPv6 Task Force, http://www.nav6tf.org.

[59] The IPv6 Forum, http://www.ipv6forum.com.

[60] DoD memorandum, 9th June 2003, http://www.defense.gov/news/Jun2003/d20030609nii.pdf.

[61] *Request for Comments on Deployment of Internet Protocol, Version 6,* Docket No. 040107006-4006-01, 69 Fed Reg. 2890 (National Institute of Standards and Technology [NIST] and National Telecommunications and Information Administration [NTIA], Jan. 21, 2004

[62] These include; Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), National Telecommunications and Information Administration (NTIA) USA, 2006, http://www.ntia.doc.gov/report/2006/technical-and-economic-assessment-internet-protocol-version-6-ipv6, Guidelines for the Secure Deployment of IPv6, National Institute of Standards and Technology (NIST) US Department of Commerce, 2010, http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf, A Profile for IPv6 in the U.S. Government – Version 1.0, National Institute of Standards and Technology (NIST) US Department of Commerce, 2008, http://www.antd.nist.gov/usgv6/usgv6-v1.pdf, USGv6 Test Methods: General Description and Validation, National Institute of Standards and Technology (NIST) US Department of Commerce, 2009, http://www.antd.nist.gov/usgv6/docs/NIST-SP-500-273.v2.0.pdf and USGv6 testing Program User's Guide, National Institute of Standards and

Government and enterprises in the US have now begun to take IPv6 seriously. This is illustrated by some very large IPv6 deployments in the US.

Comcast is one of the world's leading communication companies and is the largest provider of cable services in the US. The Comcast IPv6 programme began prior to 2005. Comcast's initial focus for IPv6 was network management as its network had outgrown the address space of RFC1918 addresses or similar. Comcast saw IPv6 as a solution to this, providing enough addresses to easily manage all of their networks.

Since 2010, Comcast's entire network has been IPv6-enabled. This includes back office systems and the majority of their access network. Comcast has provided an IPv6 trial service to customers since 2012. A pilot live IPv6 service started in 2011[63]. This process has taken Comcast over six years.[64]

Verizon has had support for IPv6 in some parts of their networks for many years. More recently, Verizon has built a 4G LTE network. This network mandates the use of IPv6 and is fully IPv6-enabled[65]. IPv6 is a mandatory protocol for 4G networks.

5.3 In Asia

In Asia, the adoption of IPv6 began earlier and is more developed that elsewhere in the world. Countries such as Japan, South Korea, Taiwan, Malaysia and China accepted the need to support the deployment of IPv6 at an early stage. In these and other counties in the region, IPv6 development and deployment was encouraged through a range of government initiatives.

The primary reason why IPv6 was seen as so important was the rate of depletion of IPv4 address space in the region. In addition to this, IPv6 is also seen as an opportunity to develop IPv6 services and products and also to provide an IPv6 based infrastructure capable of supporting new technologies.

On the 3rd February 2011, the Regional Internet Registrar for the Asia Pacific region, APNIC, was allocated the final IPv4 address blocks from IANA[66]. This initiated the last /8 allocation policy[67]. Under this policy, APNIC can allocate one further small block of IPv4 addresses to its members. Each block is a /22 which translates to 1024 addresses. These small allocations of addresses are necessary to allow APNIC's members to continue to function during the deployment of IPv6.

Technology (NIST) US Department of Commerce, 2009, http://www.antd.nist.gov/usgv6/docs/NIST-SP-500-281-v1.0.pdf.

[63] Deployment of IPv6 Begins, Comcast, 2011, http://blog.comcast.com/2011/11/ipv6-deployment.html.

[64] Metrics on Comcast's deployment experience can be found at: http://www.comcast6.net/

[65] Verizon and IPv6, 2012, http://policyblog.verizon.com/BlogPost/780/VerizonandIPv6.aspx.

[66] IPv4 Exhaustion Details, APNIC, http://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details.

[67] Policies for IPv4 address space management in the Asia Pacific region, APNIC, http://www.apnic.net/policy/add-manage-policy#9.10.

The exhaustion of APNIC's IPv4 address pool justified the aggressive support for IPv6 in the region. Prior to the exhaustion, APNIC had been allocating many millions of IPv4 addresses per month.

The Asia-Pacific region serves as an example of what will happen in all other regions in the next few years. The region contains some of the world's best prepared countries for IPv4 address exhaustion.

5.3.1 China

Population	1,336,718,015
Internet Users	485,000,000
IPv4 Addresses Allocated	330,440,000
IPv6 Prefixes Allocated /Live	168 / 70
Google IPv6 Adoption	0.57%
Web (top 50 Alexa list)	4%
Email (top 50 Alexa list)	N/A
DNS (top 50 Alexa list)	2%
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP (USD)	$6,989,000,000,000

As China's economy has grown, it has seen a rapid growth in the Internet. In 2000, China had just over 22 million Internet users. Today, China has over 485 million Internet users[68]. This massive growth is reflected in its consumption of IPv4 addresses. In 2000, China had 13 million IPv4 addresses in use. Today, China has 330 million in use[69]. A Forbes article in 2006 reported that "China Surpasses U.S. in Internet Use" estimating that China has between 150 and 200 million Internet users whilst the US has 154 million users[70].

The Chinese government has long supported the adoption of IPv6. This is only partially because of the IPv4 address depletion. The primary driver is seen as an opportunity for China to take a leading role, in the governance and technology of the new Internet. This is seen as an opportunity to develop the country's national IT industry.

A major step in the deployment of IPv6 was taken in November 2003 when the China Next Generation Internet (CNGI) was launched[71]. CNGI was showcased at the Beijing Olympics in 2008, where everything was IPv6-enabled from taxis to street lights[72].

Today, China has the world's largest IPv6 Internet. This has been built using domestic routers, Chinese-developed technologies and local skills. Chinese companies are well

[68] Internet World Stats, http://www.internetworldstats.com/ as of June 2011.

[69] IPv4 addresses by country, from BGP Expert, at http://www.bgpexpert.com/addressespercountry.php, as of 14th March 2012.

[70] "China Surpasses U.S. In Internet Use", Forbes 3rd March 2006, http://www.forbes.com/2006/03/31/china-internet-usage-cx_nwp_0403china.html.

[71] "China Leads Next Generation Internet Development", Xinhuanet, 24th September 2006, at http://news.xinhuanet.com/english/2006-09/24/content_5130188.htm.

[72] "IPv6 and the 2008 Beijing Olympics" at http://ipv6.com/articles/general/IPv6-Olympics-2008.htm.

placed to profit from their IPv6 experience and technologies. Indeed, Chinese companies have been able to win IPv6 business throughout Asia and World-wide.

5.3.2 India

Population	1,189,172,906
Internet Users	100,000,000
IPv4 Addresses Allocated	34,670,000
IPv6 Prefixes Allocated /Live	151 / 129
Google IPv6 Adoption	0.04%
Web (top 50 Alexa list)	2%
Email (top 50 Alexa list)	N/A
DNS (top 50 Alexa list)	6%
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP	$4,463,000,000,000

India is another large Asian country where a significant portion of GDP comes from the IT industry. The IT industry in India is heavily dependent on Internet connectivity. Indian companies must be able to connect to their clients whatever Internet protocol they use. Internally, India is seeing a widespread growth in Internet access through Internet Cafes and mobile phone networks. To support all of these needs, India will need the address resources of IPv6.

The "Migration from IPv4 to IPv6 in India" was listed as one of the items in the Ten Point Agenda given by the Honourable Minister of Communications & Information Technology of India in 2004. The government in India further recognised the importance of IPv6 in a consultation paper by the Telecom Regulatory Authority of India (TRAI) released in 2005[73].

Following this, the task of leading India to deploy IPv6 was given to the Telecommunications Engineering Centre (TEC) whichcarried out a number of activities to raise awareness in IPv6 and encourage the adoption of IPv6. In 2009, the TEC prepared the "National IPv6 Deployment Roadmap"[74].

In the "National IPv6 Deployment Roadmap", it was noted that whilst many large ISPs are in various stages of IPv6 deployment, medium and small ISPs generally are not prepared for IPv6. One of the largest backbone networks in India, operated by Tata Communications,is already fully dual-stack.

5.3.3 Japan

• Population	• 126,475,664
Internet Users	99,182,000
IPv4 Addresses Allocated	202,060,000
IPv6 Prefixes Allocated /Live	399 / 360
Google IPv6 Adoption	1.54%
Web (top 50 Alexa list)	4%

[73] "Issues Relating to Transition from IPv4 to IPv6 in India", http://www.cu.ipv6tf.org/pdf/recom20dec05.pdf

[74] India IPv6 National Deployment Roadmap, India, http://www.tec.gov.in/National-IPv6-Deployment-Roadmap.pdf.

Email (top 50 Alexa list)	4%
DNS (top 50 Alexa list)	12%
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP	$4,389,000,000,000

Japan has a long history of promoting the deployment of IPv6. Under the e-Japan Priority Policy Program introduced in March 2001, the Japanese government set the goal of deploying IPv6 within Japan. There are two main organisations promoting IPv6 within Japan: the IPv6 Promotion Council established in 2000, and The Task Force on IPv4 Address Exhaustion established in 2008.

Whilst there has been an IPv6 service provided by ISPs in Japan for many years, full deployment to all consumers is only now in progress. The first IPv6 service was a tunnelled service provided by NTT in 2001. The widespread deployment of native dual-stack IPv6 services is more recent with a large number of ISPs beginning to provide service in 2011[75]. Due to the government support, Japan has one of the world's leading IPv6 deployments, it has become a leading innovator in IPv6 services and applications and it has become a leader in IPv6 knowledge and expertise.

5.3.4 South Korea

Population	48,754,657
Internet Users	39,440,000
IPv4 Addresses Allocated	112,230,000
IPv6 Prefixes Allocated /Live	117 / 117
Google IPv6 Adoption	0.01%
Web (top 50 Alexa list)	N/A
Email (top 50 Alexa list)	N/A
DNS (top 50 Alexa list)	N/A
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP	$1,549,000,000,000

South Korea initiated its IPv6 programmes in 2001 under the "Next Internet Infrastructure Constructing Plan by Diffusing IPv6" established by the Korean Ministry of Information and Communication (MIC). In 2001, the MIC drew up the IT839 ICT strategy. IT839 identified a number of areas for national development including IPv6. By 2006, Korea was the number four OECD country in the world in terms of Internet access and broadband access penetration. Regarding IPv6, by 2004 Korea had created a national trial IPv6 service and undertaken a wide range of initiatives. However, the Korean government did not support IPv6 through financial initiatives.

In 2006, a study reviewed the effects of the Korean government's IPv6 strategy. Of the 34 companies surveyed, 17% had implemented IPv6, 11% had no plans to implement IPv6 and the remainder were in the planning stage. Respondents stated that the government's initiatives had positively affected their decisions to adopt IPv6. However, respondents also indicated that the government initiatives alone were not sufficient and that the business benefits of IPv6 had not been clearly demonstrated.

[75] "Current Stats and the Future Direction of IPv6 in Japan", 2011, http://www.kokatsu.jp/blog/ipv4/en/news/Current_status_on_IPv6_deployment_in_Japan_Nov15r.pdf.

A presentation at APNIC in 2011[76] estimated that the subscriber network is 27.7% IPv6-enabled whilst backbone networks are 70.7% IPv6-enabled. In the public sector, the transition rate to IPv6 is around 47%.

5.3.5 Malaysia

Population	28,728,607
Internet Users	16,902,600
IPv4 Addresses Allocated	6,330,000
IPv6 Prefixes Allocated /Live	74 / 62
Google IPv6 Adoption	0.07%
Web (top 50 Alexa list)	N/A
Email (top 50 Alexa list)	N/A
DNS (top 50 Alexa list)	20%
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP	$447,000,000,000

The Malaysian government recognised the need for IPv6 prior to 2004 and created a long-term plan with the aim of having the Malaysian government and industry ready for IPv6 by 2010.

As a result Malaysia is well on the way to having IPv6 extensively deployed. Furthermore, Malaysia has developed a significant skill base in IPv6 which has allowed them to sell their IPv6 services to other countries in the region.

Malaysia has two main government initiatives for IPv6: the National IPv6 Council (established in 2004) and the National Advanced IPv6 Centre of Excellence (NAv6) (established in 2005). Key achievements include:

- 2007 Tier-1 ISPS IPv6 compliance audit and certification.
- 2008 .my domain registry IPv6-enabled.
- 2009 ISPs completed IPv6 compliance audit phase 2.
- 2010 ISPs completed IPv6 compliance audit phase 3.

Erion Ltd, a UK company, provided Malaysia's domain name registry with training and consultancy to migrate the .my domain to IPv6 and secure it for IPv6.

Government support for NAv6 has led to it becoming a major player in IPv6 training and certification in the region and beyond.

5.3.6 Singapore

Population	4,740,737
Internet Users	3,658,400
IPv4 Addresses Allocated	5,730,000
IPv6 Prefixes Allocated /Live	114 / 93

[76] Next Generation Internet Address (IPv6) Transition Plan, APNIC 21, 2011, http://meetings.apnic.net/__data/assets/pdf_file/0013/31333/IPv6-Transition-Plan-of-Korea.pdf.

Google IPv6 Adoption	N/A
Web (top 50 Alexa list)	2%
Email (top 50 Alexa list)	N/A
DNS (top 50 Alexa list)	16%
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP	315,000,000,000

In 2010, the Singapore government, in the form of the Infocomm Development Agency (IDA), began a series of projects to support the deployment of IPv6[77]. As a result the IDA has carried out an IPv6 readiness survey[78], created an IPv6 website[79], written an IPv6 Adoption Guide[80] and written an IPv6 profile for Singapore[81].

The country has now begun an aggressive programme of IPv6 deployment.

What is particularly interesting about the survey and subsequent plans is that many organisations in Singapore, including ISPs, were not IPv6 ready at the time of the survey and the time required for them to deploy IPv6 is measured in years.

As a part of the IPv6 deployment programme, the IDA and other organisations within Singapore have been undertaken a significant awareness and educational effort. This is to raise awareness amongst key stakeholders and to provide the skills required to carry out the IPv6 deployment.

Since Singapore's IPv6 effort is relatively recent, it is interesting to look at the percentage of Autonomous Systems (ASes) within Singapore that support IPv6 and to see how quickly it has ramped up as the government IPv6 effort has taken place.

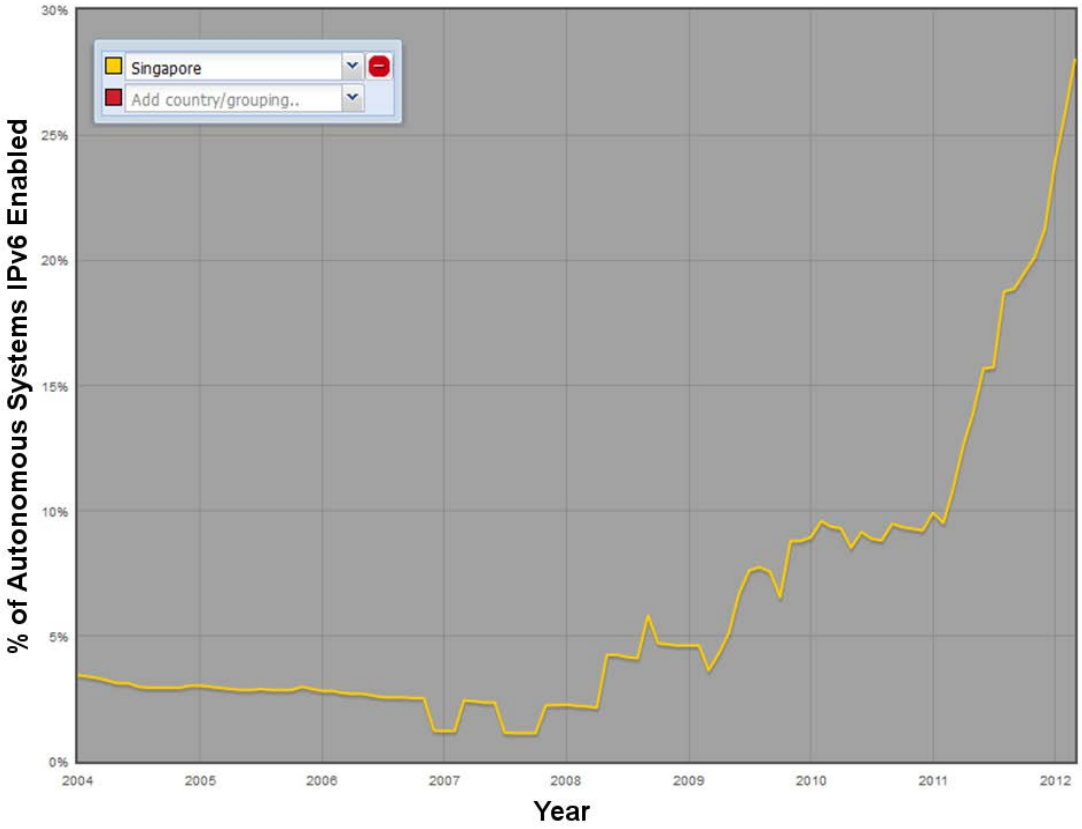
[77] IPv6 Transition Programme for Singapore, 2011, http://www.ipv6.com.sg/presentation/D103_IPv6%20Transition%20Programme%20for%20Singapore_Liang%20Seng%20Quee.pdf.

[78] IPv6 Readiness Survey for Singapore, IDA, 2011, http://www.ida.gov.sg/images/content/Technology/Technology_Level1/ipv6/download/IPv6ReadinessSurveyforSingapore.pdf.

[79] IDA Singapore IPv6 Transition Web Site, IDA, 2012, http://www.ida.gov.sg/Technology/20060419151629.aspx.

[80] IPv6 Adoption Guide for Singapore, IDA, 2011, http://www.ida.gov.sg/images/content/Technology/Technology_Level1/ipv6/download/IPv6AdoptionGuideforSingapore.pdf.

[81] IDA Singapore IPv6 Profile, IDA, 2011, http://www.ida.gov.sg/Technology/20110414110942.aspx.



5.3.7 Taiwan

Population	23,071,779
Internet Users	16,147,000
IPv4 Addresses Allocated	35,380,000
IPv6 Prefixes Allocated /Live	57 / 51
Google IPv6 Adoption	0.3%
Web (top 50 Alexa list)	N/A
Email (top 50 Alexa list)	N/A
DNS (top 50 Alexa list)	10%
National Mandates	Yes
Government IPv6 Agencies	Yes
GDP	$885,000,000,000

Taiwan's IPv6 activities began in the late 1990s when the government in cooperation with industry created an IPv6 programme. The first phase of the programme lasted from 2002-2008 and focused on development and preparation for IPv6. The second phase is the transition phase which is scheduled to be completed in 2012[82].

Taiwan has carried out a range of IPv6 initiatives including setting IPv6 policy, carrying out transition to IPv6 on national networks, creating IPv6 test labs, developing new IPv6 based services and promotion and education.

[82] Taiwan IPv6 Status Short Report, 2010, http://icons.apnic.net/download/attachments/983220/TW-Taiwan+IPv6+Short+Report+Yeh0608.pdf?version=1&modificationDate=1276169886591.

Government networks in Taiwan were IPv6 ready by 2008 and there are millions of IPv6-enabled broadband users in Taiwan. Furthermore, Taiwanese companies have produced many IPv6-enabled products, including Customer Premises Equipment (CPEs), wireless routers, firewall software, security devices and video phones.

5.4 In the Rest of the World

5.4.1 In the UK

Population	62,698,362
Internet Users	52,731,209
IPv4 Addresses Allocated	84,530,000
IPv6 Prefixes Allocated / Live	3283 / 2996
Google IPv6 Adoption	0.12%
Web (top 50 Alexa list)	0%
Email (top 50 Alexa list)	N/A
DNS (top 50 Alexa list)	14%
National Mandates	No
Government IPv6 Agencies	No
GDP	$2,250,000,000,000

The UK has a large allocation of IPv6 address prefixes, many of which appear in the global routing tables. Despite this, the deployment of IPv6 in the UK is comparatively immature. IPv6 services are limited to a few early adopters and visionary companies. There are few large-scale deployments of IPv6. As a result IPv6 skills in the UK are limited as demonstrated by user experience.

The UK IPv6 Task Force website's latest material is dated 2006. Most of the materials and activities are much older.

A not for profit organisation, 6::UK was created in 2010. After an initial spurt of activities, including a launch event, there has been little activity on their website, apart from a small number of blog posts.

BT closed down the UK6x IPv6 Internet Exchange and the BTExact IPv6 tunnel broker services in 2007. These were world-leading services.

Out of the 51 UK broadband access service providers listed on ThinkBroadband website, only six provide some form of IPv6 service[83]. These six[84] do not include the UK's largest broadband providers such as BT, Sky and Virgin Media. One of those six, Andrews and Arnold (AAISP) has been providing IPv6-enabled services for many years. Their broadband service is delivered over the BT network. BT's network should pass any network protocol (IPv4 or IPv6), however they have experienced a number of problems[85].

In sharp contrast to the Beijing 2008 Olympics, the London 2012 Olympics will not be IPv6-enabled.

[83] Broadband Internet Service Providers, Thinkbroadband, as of 15th March 2012.

[84] The six broadband providers with an IPv6 service on Thinkbroadband, as of 15th March 2012 are; AAISP, Claranet, Entanet, Exa Networks, Goscomb Technologies, IDNet and Web Tapestry.

[85] BT & IPv6, Andrews and Arnold, http://aaisp.net.uk/news-ipv6.html.

The IPv6 Deployment Aggregated Status website run by Eric Vyncke of Cisco shows the UK ranked 73rd in the world for IPv6 support on websites and 67th in the world for IPv6 support on DNS servers. Statistics provided by Dan Wing of Cisco show that the UK has two working IPv6-enabled websites out of a sample of the top 292 sites from the Alexa list. This gives the UK a figure of 0.7% compared with a global average figure of 1.85%.

On the UK Stock Exchange, out of the FTSE 100 companies, one has an IPv6-enabled website, 16 have IPv6-enabled DNS servers and none have IPv6-enabled email servers.

5.5 Deployment Experience in Transit Providers

Some transit providers have had IPv6 service for over a decade, while others have only just begun to provide IPv6 services. There is a wide variation in the type of IPv6 service provided by those that offer an IPv6 service.

The best IPv6 transit service is one which provides a fully dual-stack native IPv6 service. A native IPv6 service is likely to have better performance, be more reliable and easier for the provider to manage and operate. Non-native IPv6 offerings are provided by the use of a range of tunnelling mechanisms. Some of these provide a service that is almost indistinguishable from a native IPv6 service, whilst others do not. For example, one quick way to provide an IPv6 service over an IPv4 infrastructure is to use manually configured IPv6 in IPv4 tunnels (or IPv6 over MPLS circuits). Whilst this provides an IPv6 connection with minimal infrastructure changes, it does require significant effort to manage and is not scalable.

When choosing an IPv6 transit service provider it is important to go beyond the simple question of whether they have IPv6. The detail of how they provide IPv6 is crucially important to performance reliability and other factors.

Some IPv6 transit suppliers provide IPv6 connectivity using their current infrastructure upgraded to dual stack, others provide IPv6 connectivity by building a new IPv6 infrastructure and some provide IPv6 connectivity over their current IPv4 infrastructure using IPv6 in IPv4 tunnels. The level of service, including performance, can vary significantly depending on the approach taken by the transit provider.

Customers will have a range of experiences depending on the approach taken by the transit provider. For example, there are examples of customers who have experienced substantial improvements in throughput and latency after migrating to IPv6. This is because the supplier's network was a new network built to support IPv6 and was not over-congested with legacy IPv4 traffic.

5.6 Deployment Experience in ISPs

Broadband access providers include suppliers of DSL services and cable network operators. Regardless of the underlying technology, the service provides a connection to the Internet allowing the customer to connect one of more computers.

The majority of broadband services in the UK are provided over either the telephone local loop (DSL) or over cable networks (DOCSIS). Broadband services may also be provided using other technologies such as wireless or satellite. In the UK, the open marketplace for broadband access services means that ISPs can use services from different Network

Access Providers (NAP). To carry traffic over the NAP's network between the ISP and its customers, protocols such as the Layer 2 Tunnelling Protocol (L2TP) can be used.

In theory, at least much of the access network is network layer protocol independent and should support IPv4 and IPv6. In practice it can be more complex than that. There are a number of areas where changes may be required to support IPv6. These include, the customer premises equipment (CPE), the last mile technology (e.g. ADSL or cable), intermediate devices (e.g. Broadband Remote Access Server - BRAS), provisioning servers, authentication authorisation and accounting (AAA) servers, backhaul networks, security systems, network management systems, back office systems.

For an ISP to support native IPv6, it must:

- Upgrade or replace IPv4 CPEs with IPv6 ready CPEs
- Upgrade access technology to support IPv6 (for example DOCSIS V3 in cable networks)
- Provide backbone IPv6 connectivity
- Migrate internal networks and infrastructure to dual-stack
- Upgrade network management and security systems to support IPv6
- Upgrade provisioning systems to support IPv6
- IPv6 enable all customer facing systems (billing, management etc)
- Train staff in IPv6

CPE support (or the lack of it) is one issue which ISPs have had to tackle. Until very recently, few CPE devices (Cable or xDSL) had IPv6 support. Today that has changed significantly and many new CPEs do support IPv6. Furthermore some legacy CPEs can be upgraded to support IPv6[86]. This means that ISPs may face replacing or upgrading large numbers of CPE devices. If ISPs had planned for IPv6 some years ago they could have ensured that they only deployed IPv6 ready CPEs.

In Asia, many ISPs are already providing native IPv6 service. For example, in Korea over 30% of the subscriber network was already IPv6-enabled in 2011. In the US, as has been previously noted, a number of ISPs provide IPv6, the biggest of which is Comcast. The same is true in Europe[87] where an increasing number of ISPs provide IPv6-enabled services, including Deutsche Telekom[88] and France Telecom[89].

In France, all of the major providers have support for IPv6. For example, Free has been providing a native IPv6 service since 2007. All of its over 4 million subscribers have IPv6 provision.

[86] A useful list of IPv6 compatible CPEs can be found on ARIN's IPv6 wiki at, http://getipv6.info/index.php/Broadband_CPE.

[87] IPv6 Provider list of IPv6-enabled ISPs in Europe at http://ipv6-provider.eu/. This list is far from complete but the feedback is interesting.

[88] "The Internet is full up", 2011, http://www.telekom.com/company/64714.

[89] "IPv6: What Else?", 2012, http://meetings.apnic.net/__data/assets/pdf_file/0004/45094/apricot-2012-ft-orange-presentation_1330276102.pdf.

In the UK, only a small number of ISPs provide IPv6 service. Only one of these is in the top ten by subscriber numbers with under 100,000 subscribers[90]. Because the major players do not support IPv6, the maximum number of broadband subscribers with access to IPv6 in the UK is less than 100,000 out of 18,000,000[91] subscribers: only0.56%.

On the IPv6 Provider's website, Virgin Media are quoted as saying there are, "No plans for IPv6 in the near future, but the cable network is ready for DOCSIS 3"[92].

On BT's community website, a response on 7/6/2011 to the question; " When might we see BT Retail broadband supporting IPv6 fully?" states:

> "*The BT Total Broadband network & Home Hubs currently work using IPV4 only. BT has plans and is investing to upgrade the network over the next couple of years so that it will also work with IPV6 (known as 'dual stack'). We expect future models of Home Hub to support IPV6 and we're exploring updating existing Home Hubs also, alongside our network upgrade plans.*
>
> *Only when our network and Home Hub both support IPV6 will our customers be able to use IPV6 on the internet. Until then we'll continue to fully support all our customers on the internet using IPV4 connections*."[93]

ISPs deploying IPv6 over BT's network have faced some technical difficulties. Andrews and Arnold found that on BT's IPStream service where Cisco ESR RASes (Remote Access Servers) are used, IPv6 packets were truncated. As a result, IPv6 datagrams were not able to traverse the BT network.

One lesson that has been learnt from many migrations around the world is that migrating a large ISP to support IPv6 can take many years. Smaller ISPs are likely to find it easier to deploy IPv6.

5.7 Deployment Experience in Mobile Networks

In the early days of 3G, the 3G standards mandated the use of IPv6 in the All-IP system (now called IP Multimedia Subsystem or IMS). The relatively immature status of IPv6 at that time meant that mobile operators found it difficult to deploy 3G based on IPv6. As a consequence the standards were relaxed to allow for deployment using IPv4. As a result, 3G networks were mainly deployed based on IPv4 and not IPv6. Only in recent years have 3G networks begun to deploy IPv6 connectivity.

4G is different, unlike 3G, 4G has no circuit switched component. Instead, all provided services – including voice, video, and data -- are carried over an IP network. For 4G to support the large number of devices that it must support, the only network-wide protocol that is practical is IPv6 making IPv6 effectively mandatory for 4G.

---

[90] Top ten ISPs by subscriber number at http://www.ispreview.co.uk/review/top10.php.

[91] Ofcom Facts and Figures at http://media.ofcom.org.uk/facts/.

[92] IPv6 Providers, Europe, http://ipv6-provider.eu/. Note that like other similar sites this one is not comprehensive.

[93] IPv6 Support, BT At home help, http://community.bt.com/t5/Other-BB-Queries/IPv6-support/td-p/203913.

True 4G networks that are being deployed today use IPv6. IPv4 connectivity is provided over the IPv6 network using translated technologies such as NAT64/DNS64 and/or tunnelling techniques such as Dual-Stack Lite (DS Lite).

As 4G networks are deployed, an increasing number of carriers are deploying production or test IPv6 mobile networks and they are upgrading their current networks to support IPv6. In countries that are seeing the deployment of 4G services, this is resulting in a significant increase in interest in IPv6.

In the US, Verizon has deployed a LTE 4G network that is IPv6 based[94]. All LTE devices are required to be IPv6 capable. T-Mobile (USA) is also deploying IPv6 on its mobile networks and is running a beta trial for interested users[95]. The motivations behind the T-Mobile approach are described in a recent presentation[96].

5.8 Deployment Experience in Internet Infrastructure Operators

The following sections describe the IPv6 deployment experience in Internet Infrastructure Operators including DNS registrars and registries, hosting and co-location providers, content providers and service providers.

5.8.1 DNS Registries and Registrars

The domain name system (DNS) is crucial to the operation of the global Internet. Users rarely refer to websites or email addresses using IP addresses. Almost every service or host is referred to using its domain name.

IPv6's longer addresses make the use of domain names even more important than in the IPv4 world. This is because in the IPv4 world it is relatively easy for system and network administrators to remember and use IPv4 addresses whilst in the IPv6 world the longer addresses are much harder to remember. It is therefore going to become normal to use domain names in situations where in the past addresses might have been used.

The DNS system has an hierarchical naming structure. At its top are the root name servers. Below these are the generic Top Level Domains (gTLDs) and the Country Code Top Level Domains (ccTLDs) such as uk. The DNS name space is coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN).

IPv6 domain name lookups do not have to take place over IPv6 transport. That is, you can look up the IPv4 or IPv6 address of a name using IPv6. However, for IPv6-enabled hosts, the ideal is that the DNS query will take place over IPv6 transport and the result will return both IPv4 and IPv6 addresses for the domain name.

A domain name registry is an organisation responsible for maintaining a database of all domain names registered in a TLD. A domain name registrar is an organisation that is accredited by one or more domain name registry to manage the reservation of domain names. A domain name registrar offers registration services.

[94] Verizon and IPv6 at http://policyblog.verizon.com/BlogPost/780/VerizonandIPv6.aspx.

[95] T-Mobile IPv6 Beta Google Group at http://groups.google.com/group/tmoipv6beta.

[96] T-Mobile USA IPv6 Deployment at http://4g-portal.com/t-mobile-usa-ipv6-deployment.

For a domain name registry to fully support IPv6, it must[97]:

- Have IPv6 addresses for its name servers
- Have IPv6 glue records[98] for its domain in the root domain
- Answer DNS queries over IPv6 transport
- Support the registration of domain names with IPv6 addresses
- Provide registrar systems and tools that support IPv6 addresses
- Provide registrar systems and tools that work over IPv6 transport
- The domain name registry should also have implemented IPv6 in their infrastructure, including for example, back-end systems, servers and security systems.

The DNS root name servers coordinated by ICANN were IPv6-enabled for the first time in February 2008. Of the 312 TLDs, 268 have IPv6 name servers[99]. Of these 256 (82.1%) have name servers with IPv6 glue records in the root zone.

The UK's domain name registry, Nominet, first enabled IPv6 on a .uk name server in 2004[100]. Nominet made changes to their EPP system in November 2009 to support IPv6 addresses[101]. Today Nominet supports the registration of IPv6 addresses over IPv6 transport. Nominet's servers also answer DNS queries over IPv6 transport.

However, the fact that a registry such as Nominet supports IPv6 does not mean that the registrars selling domain names to end-users support IPv6. Registrars also need to provide the ability to register IPv6 addresses for domain servers and they need to provide this server over IPv6 transport. So just as Nominet has deployed IPv6, so too registrars need to deploy IPv6 as well.

In the UK, few registrars support the automatic registration of name servers with IPv6 addresses. Even fewer support this service over IPv6 transport. Not only that but poor understanding of and support for IPv6 can lead to catastrophic failures. For example, in 2011 a leading UK IPv6 consultancy firm found that maintenance at their registrar had removed the glue records to an important domain name due to the registrar's domain name management tools not properly supporting IPv6. This effectively removed connectivity to servers in that domain because the domain names could not be resolved into an IPv6 address. As a result, that registrar lost the consultancy's business.

From an end user's perspective, it is not only important that Nominet and Nominet's registrars support IPv6. It is also important for connectivity that other registrars around the

[97] Case Study: IPv6 Enabling Malaysia's .my Domain, Erion, Google IPv6 Implementer's Conference 2009, http://www.ipv6consultancy.com/ipv6blog/wp-content/uploads/case-study-ipv6-enabling-malaysias-my-domain-web.pdf.

[98] Glue records are information in the DNS that provide a way for a DNS client to determine the IP address for an authoritative nameserver mentioned in the zone delegation. Glue records are used to avoid certain problems that can occur with lookups at a delegating nameserver.

[99] Global Ipv6 Deployment Progress Report, Hurricane Electric, retrieved 28/2/2012, http://bgpmon.net/weathermap.php?inet=6.

[100] IPv6 Nameserver for .uk, Nominet, 2004, http://lists.nominet.org.uk/pipermail/nom-announce/2004-November/000136.html.

[101] Changes to Nominet EPP, Nominet, 2009, http://www.nominet.org.uk/registrars/systems/nominetepp/changestoepp/.

globe also support IPv6 becauseUK end users do not only consume UK domain names, they also consume global and regional domain names from around the world.

From a registrar's perspective, it is important that they migrate to support IPv6 soon as they risk losing business to registrars that can support IPv6. It is also important that their support for IPv6 is reliable.

5.8.2 Hosting and Co-Location Providers

Hosting and co-location providers have many similar experiences to other organisations seeking to deploy IPv6. However, they have a number of unique characteristics.

Hosting providers are different in that they are hosting customer's websites and applications on their servers (including virtual servers). Therefore hosting providers need to upgrade the platforms upon which their customer's websites and applications are hosted.

As is noted in section 6.2.1, most modern operating systems have had IPv6 support for many years. This means that it is likely that the hosting provider's operating systems are IPv6 ready. Further, basic services such as web and email services have also had IPv6 support for many years.

However, most hosting providers use a mix of their own, commercially available and open-source tools to manage their hosting services. These may or may not be IPv6 ready. Compounding this problem, hosting providers do not know if their customer's websites or applications are IPv6 ready. In rare cases, it is possible that some may fail if hosted on IPv6-enabled platforms.

In the main, it is relatively straightforward for a co-location provider to migrate their networks to IPv6 and provide IPv6 service to their customers. It is sometimes harder for hosting providers to migrate to IPv6 as they also need to migrate their host's and virtual host's operating systems to IPv6.

5.8.3 Content Providers and Service Providers

Content providers and service providers include organisations that develop and provide Internet applications. These can range from static websites to complex Internet based applications such as business applications and multi-player games.

These organisations often have similar infrastructure issues to content with when deploying IPv6 as hosting and co-location providers. In addition to these, content and service providers have a greater focus on software development and application layer issues.

Applications that have network functionality of any kind will be impacted in some way by the deployment of IPv6. The level of impact will depend on a mix of the complexity of the application itself and the extent to which the application uses network features.

Over the years, best practice for IPv6 application development has evolved. It is no longer the same as it was envisaged to be in the earliest standards. Standards, reference books, training courses and web-pages often provide inadequate or inaccurate guidance on migrating applications to support IPv6. The cost and success of migrating applications to support both IPv4 and IPv6 is heavily dependent on fully understanding the options and choosing the correct approach from a wide range of options. This is very different from the

IPv4 world of software development where using software developers had only one approach to take.

As a result, depending on the nature of the applications involved, the impact of deploying IPv6 in content and service providers can vary enormously. In some cases it will require substantial effort to IPv6 enable applications.

5.9 Deployment Experience in End Networks

5.9.1 Impacts on Consumer and Enterprise Security Models

Security is an on-going and growing concern in consumer and enterprise networks. It is well known that there are many security weaknesses in IPv4 networks. Each year, new security vulnerabilities are discovered and exploited. As a result, end users utilise a range of security measures, including firewalls and intrusion detection systems (IDS) to mitigate network vulnerabilities.

The sophistication of the security model varies depending on the nature and size of the end-user. Consumers commonly rely on a firewall built into their broadband CPE and software firewalls and security applications on their hosts. Enterprises are likely to have their own security policy and network security administrators who implement a broad range of mitigation technologies.

IPv6 significantly increases the "attack surface" of networks and network devices. The attack surface refers to the number of possible ways a network can be attacked. So at an over simplistic level, duplicating the Internet Protocol by adding a new version at least doubles the attack surface.

In reality, the attack surface of IPv6 is much larger than IPv4. This is because adding IPv6 is not just the addition of another IPv4 but the addition of a new and different network layer protocol with a significant number of new features and a set of often complex transition technologies that are commonly implemented and activated by default. This problem is worse in IPv6 dual-stacks asthe two protocols have a complex interaction allowing IPv4 to be attacked from IPv6 and vice versa.

Since the majority of end-nodes implement IPv6 dual-stacks today and they are turned on by default, many of the security risks arising from IPv6 deployment exist *now, before* IPv6 is deployed.

For example, it is trivial to undertake a Denial-of-Service (DoS) attack against networks containing Windows, Linux, Mac or Unix nodes using IPv6's StateLess Address Auto-Configuration (SLAAC) feature. Worse, in the case of Windows, this attack vector can be used to consume resources on a node and cause it to hang[102]. This zero-day vulnerability can be mitigated through the implementation of appropriate IPv6 security.

Furthermore, the reach of some of these vulnerabilities is significant. Some IPv6 transition mechanisms make it possible to attack any IPv6 node from the IPv4 Internet and to attack any IPv4 node from the IPv6 Internet. This makes the laundering of attacks easier and prevention and tracing much harder.

[102] Vulnerability Summary for CVE-2010-4669, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4669.

As an illustration of this problem, in some countries where access to certain Internet services is restricted, it is still possible to access those services using IPv6 transition techniques such as Teredo and 6to4. This also has implications for the monitoring and auditing of network traffic to meet regional legislation.

At the present time, support for IPv6 in security products is changing rapidly. This is a problem for any end user that is using older security products they may not have sufficient support for IPv6. It is also a problem for those with newer products as there is a need for network security administrators to keep their knowledge of these products up to date in the light of recent experience with IPv6.

In conclusion, consumer and enterprises are at risk from new attacks arising from IPv6 functionality even if their networks are not yet IPv6-enabled. Mitigating IPv6 vulnerabilities may require upgrading or replacing security products, and staff will require training in IPv6, its vulnerabilities and current mitigation techniques.

5.9.2 IPv6 Implications for the Internet of Things and LowPAN

The Internet of Things refers to networks that use the Internet Protocols to communicate with almost everything in daily life. The "things" are uniquely identifiable objects in the network which can in theory be almost any object you can think of from livestock, to products to household devices.

The potential benefits of networking everything are huge.

One key technology in the Internet of Things is LowPAN (Low Power Wireless Personal Area Networks). This is an important technology if everything, even very small objects, are to be connected.

IPv6 can and is playing a key role in the development of the Internet of Things. IPv6 provides the necessary address space that is essential to uniquely identify vast numbers of things. Furthermore, IPv6 networks restore end-to-end connectivity that was broken in IPv4 through the widespread deployment of NAT. This is important because it makes it possible to communicate with things wherever they are without the need for complex mechanisms to get behind NAT. The Internet of Things involves so many devices that neither IPv4 nor private addressing can cope with the huge number of addresses required.

IPv6 and the Internet of Things have been found to bring unexpected benefits once previously unconnected things are networked. For example, a project in Japan to IPv6 enable taxis[103] resulted in an unexpected transport application. Once the taxis were IPv6-enabled, the speed of their windscreen wipers became available. It was found that the speed of the wipers was directly proportional to how heavy the rain was. As a result it became possible to provide a road map showing the rain density. No one had anticipated this application prior to information becoming available.

[103] A look into Japan's Internet Appliances, http://ipv6.com/articles/applications/Japan-Internet-Appliances.htm.

5.10 Survey of the Current Deployment of IPv6 – A Quantitative View

To gain an indication of the current state of IPv6 deployment, you need measurements. There is no single measurement that shows directly what the state of IPv6 deployment is. Instead, a number of measurements should be made. These include;

- IPv6 address allocations
- IPv6 address space that is visible in the global routing tables
- DNS servers that are IPv6-enabled
- Domain names that have IPv6 addresses associated with them
- Domains that have an IPv6-enabled mail server
- Volume of IPv6 traffic

Some things cannot be measured directly. For example, there is no simple measure that shows how many organisations have deployed IPv6 in their networks. This information could only be realistically obtained through a survey. Furthermore, these measurements do not tell you how fully or how well IPv6 has been deployed. This can only be determined through audits and certifications.

Another factor to consider is that these measurements do not test if the IPv6 service or address is valid or if it actually works. This may seem obvious, but it is rarely verified[104]. So for example, if a domain name has an IPv6 address, is it a valid address and is it possible to connect to it[105]?

This section provides information from the wealth of publicly available IPv6 measurements. The aim is to provide an indication of that state of IPv6 deployment in the UK and how it compares to other regions. In doing so, we need to keep in mind factors that can skew the results and comparisons such as the size of a region and the penetration of Internet (IPv4 or IPv6) use within that nation.

A number of organisations and governments have already produced measures based on some or all of those listed above.

RIPE has produced a service called IPv6 RIPEness that measures a number of factors by Local Internet Registry (LIR) including; IPv6 allocation, visibility in the IPv6 Routing Information Service (RIS), route6 object in the RIPE database and configured reverse DNS delegation[106]. Each LIR is given a star rating where 4 stars indicates that LIR meets all the criteria.

[104] Interestingly, the fact that domains with IPv6 address continue to contain up to 2% that are bogus, is an indication of the lack of understanding of IPv6 deployment amongst administrators.

[105] See for example, Dan Wing's analysis of top websites (from Alexa) which not only checks for IPv6 addresses but verifies that they are sane and that they work. His most recent figures show that of the domains that have IPv6 addresses nearly 2% are bogus.

[106] RIPE's IPv6 RIPEness web page, http://ipv6ripeness.ripe.net/.

A comparison of the UK with other European countries using the RIPE data is shown below[107]:

Country	LIRs with no IPv6	4 Star LIRs
Netherlands	33%	34%
Germany	40%	27%
France	45%	20%
EU Average	46%	16%
UK	54%	13%

The UK is less IPv6 ready that the EU average and comparable neighbours. There are some interesting results in the RIPEness figures. For example, Slovenia, which is a relatively small country with just over two million people, has had significant support for IPv6 from its government. As a result, Slovenia's RIPEness figures are some of the best; with LIRs with no IPv6 at 21% and LIRs with 4 stars at 30%. It should be noted that it is probably easier to deploy IPv6 in a relatively small environment.

Absolute figures can be misleading.. In absolute terms, the UK has one of the highest numbers of LIRs with 4 star RIPEness (127). However, this only represents 13% of the total number of LIRs in the UK (918). This is because the UK has a much higher number of LIRs than other countries in the region.

An alternative way to look at IPv6 deployment is to consider the percentage of autonomous systems (ASes) that are IPv6-enabled. Using RIPE data, it is possible to list the top twenty countries. It is notable that neither the UK nor the US appear in the top twenty countries[108].

Country	% of IPv6-enabled ASes	Number of ASes
Norway	48.9%	135
Netherlands	42%	445
Malaysia	38.5%	95
Japan	31.8%	550
Sweden	31.3%	383
Germany	30.3%	1125
Belgium	29.9%	137
Ireland	28.7%	101
Finland	28.2%	142
Singapore	28%	164
New Zealand	27.9%	219
Denmark	27.7%	173
Switzerland	26.8%	418
Austria	25.8%	330
Portugal	24.5%	53
France	22.2%	580
Taiwan	22%	118
South Africa	21.6%	227
Hong Kong	20.1%	278

[107] Taken from http://ipv6ripeness.ripe.net/pies.html on 1st March 2012.

[108] IPv6 by Numbers, 2012, at http://www.daniweb.com/hardware-and-software/networking/news/417061.

In contrast, the UK has 17.4% of ASes that are IPv6-enabled[109]. However, these figures can also be misleading. There is a very wide variation in the number of ASes in a region and in their size so this is only a very rough guide to the status of IPv6 deployment.

Another useful measure of IPv6 deployment is the number of websites, email servers and DNS servers that are IPv6-enabled.

Country	Web with IPv6	Email with IPv6	DNS with IPv6
UK	0%	N/A	14%
China	4%	N/A	2%
France	6%	2%	12%
Germany	6%	2%	28%
India	2%	N/A	6%
Japan	4%	4%	12%
Malaysia	N/A	N/A	20%
Netherlands	10%	18%	30%
Singapore	2%	N/A	16%
Slovenia	24%	6%	46%
South Korea	2%	N/A	N/A
Taiwan	N/A	N/A	10%
USA	0%	2%	24%

The sample size for these figures is small at 50 of the top Alexa sites. In some cases, figures were not available (N/A). Previous measurements by Erion[110], which are consistent with these figures, have shown that Email is the service least likely to be IPv6-enabled. Experience has shown that the service which is most likely to be IPv6-enabled is the DNS service.

This table shows that UK and the USA have no websites in the top 50 that are IPv6-enabled. Further, in this list of countries, the UK comes 7th out of 12 that have a DNS measurement.

The Google IPv6 adoption statistics for the same set of countries, show the UK coming 10th out of 13 countries. This figure attempts to measure the percentage of Google users that are IPv6 capable. This is an indication of how many clients and their access networks are IPv6-enabled.

Country	Google IPv6 Adoption
France	4.48%
Singapore	2.00%
Japan	1.54%
China	0.57%
USA	0.55%
Taiwan	0.30%
Germany	0.15%
Netherlands	0.20%
Slovenia	1.26%
UK	0.12%
Malaysia	0.07%
India	0.04%
South Korea	0.01%

[109] IPv6-enabled Networks, RIPE, March 2012, http://v6asns.ripe.net/v/6?s=GB.

[110] Erion Ltd, http://www.erion.co.uk.

Notice that France comes top of this list because of the widespread availability of IPv6 in France's broadband service providers. Given our earlier estimate that the UK was that less than 0.56% of the UK's broadband subscribers are IPv6-enabled, the figure of 0.12% indicates that our estimate may be much larger than the actual figure.

5.10.1 A View of IPv6 Transit in the UK

The UK has had IPv6 transit connectivity for many years. The Japanese carrier NTT was one of the earliest providers in the UK and world-wide. Level 3 Communications has also been an early provider in the UK with several ISPs reselling Level 3 services as their own.

5.10.2 A Comparison of IPv6 Allocations to UK ISPs

Any comparison of IPv6 prefix allocations amongst UK ISPs is meaningless. For many ISPs one IPv6 /32 prefix allocation (the default) will be sufficient for their needs forever. A /32 IPv6 prefix represents 4 billion /64 networks all with a practically unlimited number of node addresses. Even if the ISP decides to allocate /56 IPv6 prefixes to its customers, a single /32 still represents 16 million customer prefixes.

In the majority of cases, a small number of /32 IPv6 prefix allocations will be all that is required by any ISP for the foreseeable future.

This is very different from IPv4 where allocations of addresses are critical to the ISP's operation.

5.10.3 A Comparison of IPv6 Allocations to Similar ISPs in Europe and Elsewhere

The UK has 3283 assigned IPv6 prefixes which is second only to Germany with 7016. However, the number of assigned prefixes does not tell you how many are routable. In the case of Germany, 6742 (96%) are routable whereas in the UK 2996 (91%) are routable. Many of the UK's prefixes are aggregated and are not seen in the BGP table. Only 258 (7.9%) prefixes are announced in the BGP table unaggregated.

The number of allocations to a country is to some extent meaningless. It has more to do with the number of LIRs and organisations that ask for prefixes than it has to do with the extent of IPv6 deployment. For example Japan’s 400 assigned prefixes. This is just over a tenth of the prefixes assigned to the UK. However, we know that Japan has one of the most developed IPv6 networks in the world. China has the world's largest IPv6 network, but it only has 168 IPv6 prefixes assigned 70 of which are routable.

One of the reasons that countries with large IPv6 deployments do not require large numbers of prefix assignments is that each IPv6 prefix represents a huge address space. Fewer prefixes are required. A single IPv6 /32 prefix allocation (the default allocation to an LIR) is sufficient for four billion /64 prefix assignments. The reason the UK has a large number of prefixes allocated is not a sign of a large deployment of IPv6, instead it is a feature of the open market place where many prefixes are required to supply the large number of LIRs.

This is very different from IPv4 where prefix allocation is tightly coupled to address usage and is a good indicator of the size of the IPv4 Internet in a region or country.

IPv6 prefix allocations are widely monitored and measured yet they represent a very poor indicator of IPv6 deployment.

5.10.4 Allocation Comparisons between IPv4 and IPv6

Comparisons of address allocations between IPv4 and IPv6 are largely meaningless. As mentioned in the previous section, even a single allocation to an LIR is sufficient for 4 billion networks each with an unimaginable number of node addresses. There are more networks in a single IPv6 LIR /32 prefix allocation than there are total unicast IPv4 addresses.

Ignorance of IPv6 addressing is leading to some bizarre allocations in the UK. For example, one hosting company assigns an IPv6 /48 prefix to each customer's server. This means that a server which with IPv4 probably had one or two IPv4 addresses, with IPv6 has 1,208,925,819,614,629,174,706,176 addresses which can be split across 65,535 subnets.

Industry inertia that has resulted in the UK lagging behind other countries with IPv6 implementation should not be viewed as a market failure to date e.g. where the quantity of a product demanded by consumers does not equate to the quantity supplied by suppliers. IPv6 address space is readily available but the demand has not been there to drive its rapid take-up. Neither can it be argued that the market has produced socially unacceptable outcomes because IPv4 has met most requirements. However with the exhaustion of IPv4 addresses market failure will now occur if action isn't taken.

5.10.5 Traffic Data for IPv6 - A View

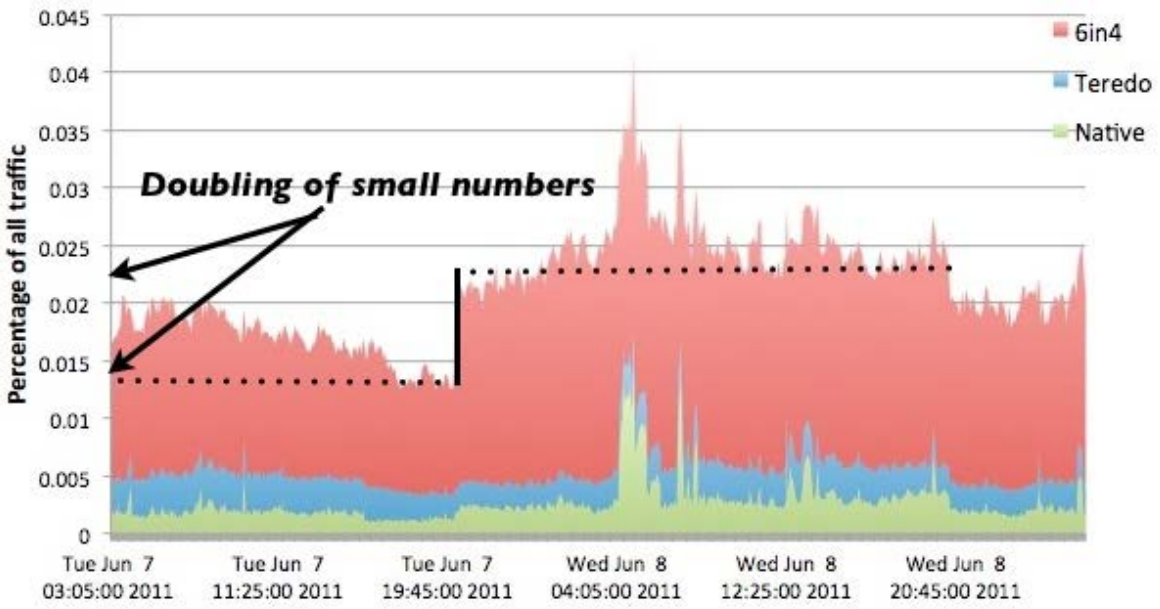
An important indicator for the status of IPv6 deployment is the volume of IPv6 traffic on the Internet compared with the volume of IPv4 traffic. A figure for the global IPv6 traffic is difficult to obtain as it requires measurements from many different providers.

IPv6 traffic measurements have not historically been made by country or region which makes it almost impossible to comment on the relative volumes of traffic by region or country.

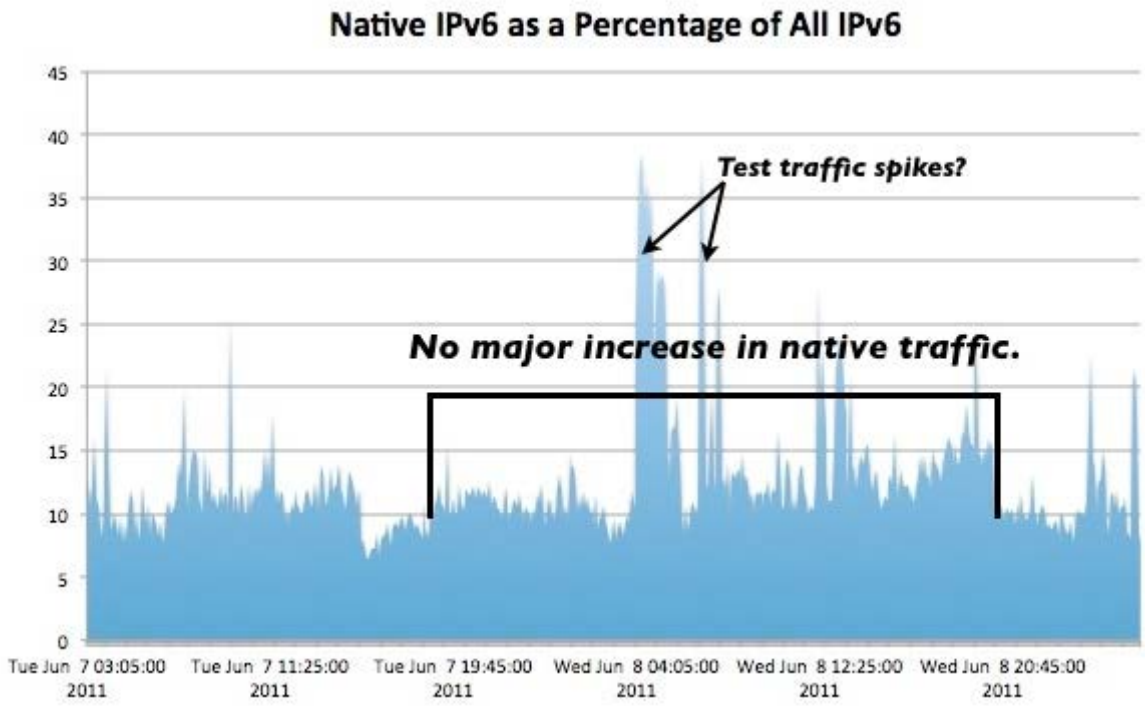
However, overall IPv6 traffic measurements have been carried out by organisations that have global reach and access to network traffic measurements from a large number of the biggest carriers.

One such organisation is Arbor Networks. In 2011, over the period of the World IPv6 day, Arbot measured the IPv6 traffic over six carriers[111]. These measurements showed that the IPv6 traffic over the World IPv6 day was tiny compared with the IPv4 traffic. At its peak, IPv6 traffic was below 0.5% of all traffic.

[111] World IPv6 Day: Final Look and "Wagon's Ho!", at http://ddos.arbornetworks.com/2011/06/world-ipv6-day-final-look-and-wagons-ho/.

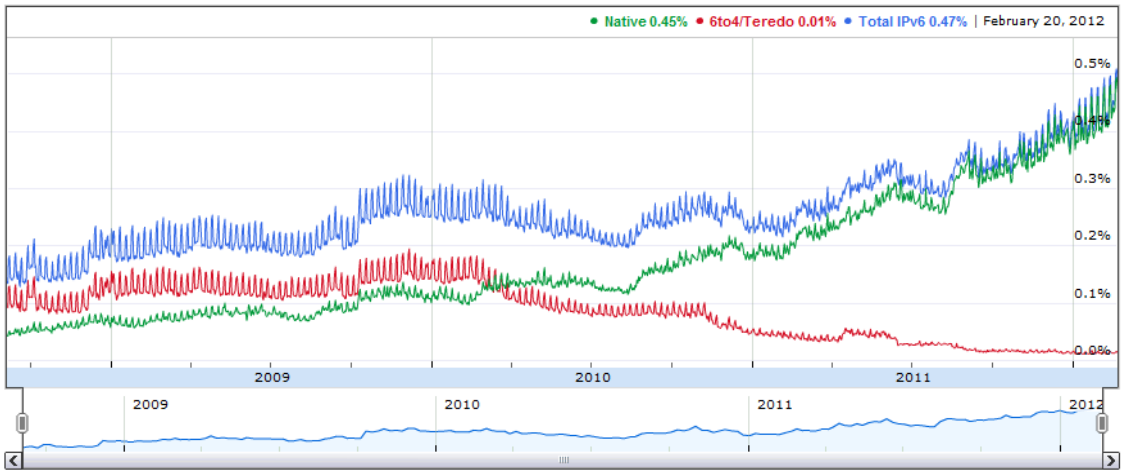


Furthermore, when it is broken down into native and non-native IPv6 traffic, it is clear that the majority of IPv6 traffic is non-native. This is because the clients are connecting using transition mechanisms such as 6to4 and Teredo. The lack of native IPv6 is an indication of the limited deployment of native IPv6 in access networks. So whilst a server may have native IPv6, clients still have to connect using tunnels because their access networks only support IPv4.



It is also important to look not only at the absolute volumes of IPv6 traffic but also the growth trend. The measurements made by Google are useful when looking at traffic trends. These

show an on-going growth in IPv6 traffic. The rate of growth of IPv6 traffic has increased since the beginning of 2011. What is also interesting about the Google statistics is the split of IPv6 traffic between native and non-native traffic. Since mid-2009 it can be seen that the percentage of traffic that is non-native has been gradually falling indicating that there is an increasing deployment of native IPv6 connectivity.



The volume of IPv6 traffic is just less than 0.5% of all traffic. This is consistent with the figures measured by Arbor Networks.

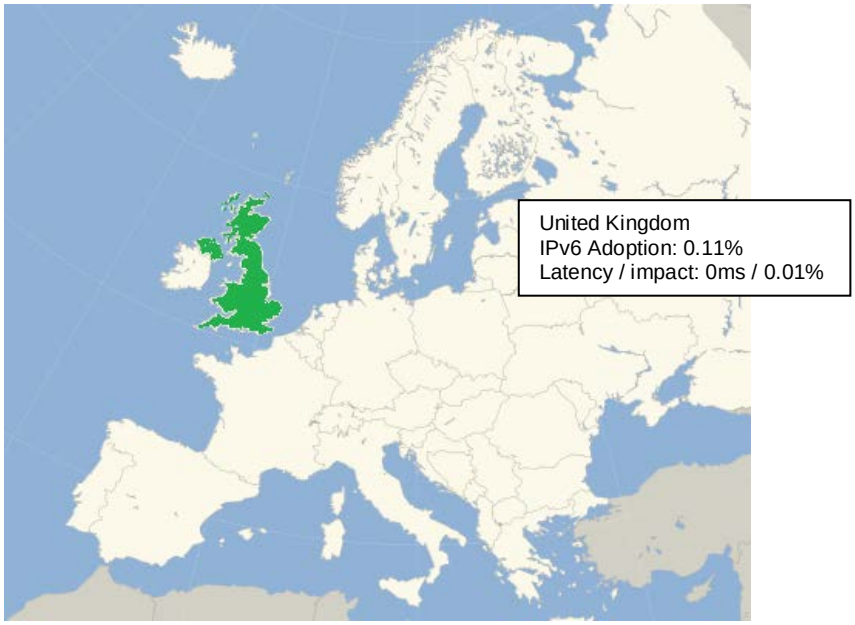
Traffic alone does not provide a complete picture of IPv6 deployment. For example, even if all clients were IPv6-enabled they would still continue to use IPv4 to connect to IPv4 only services. This means that if the majority of the services that they use are still using legacy IPv4, then most of the traffic will be IPv4 despite the client having IPv6 capability. Worse, some IPv4 only services account for large volumes of traffic and can swamp traffic measurements.

An example is Skype, which is currently IPv4 only. A Skype session typically uses many orders of magnitude more bandwidth than browsing a website. So IPv4 traffic generated by Skype sessions will easily generate much more traffic than large numbers of IPv6-enabled low volume connections. This type of scenario limits the conclusions that can be safely drawn from IPv6 traffic volumes.

Google also provides a breakdown of their measurements by country. The measurements are an aggregate of information and so are not an indication of traffic volumes alone. They are useful in terms of comparing the comparative usage of IPv6 by country.

IPv6 adoption as measured by Google[112] is shown below:

[112] See http://www.google.com/intl/en/ipv6/statistics/ for details of Google IPv6 statistics. The figures in this report were obtained on 12th March 2012. How these figures are calculated is described in the paper "*Evaluating IPv6 Adoption in the Internet*", Lorenzo Colitti, Steinar H. Gunderson, Erik Kline, Tiziana Refice at, http://research.google.com/pubs/pub36240.html.

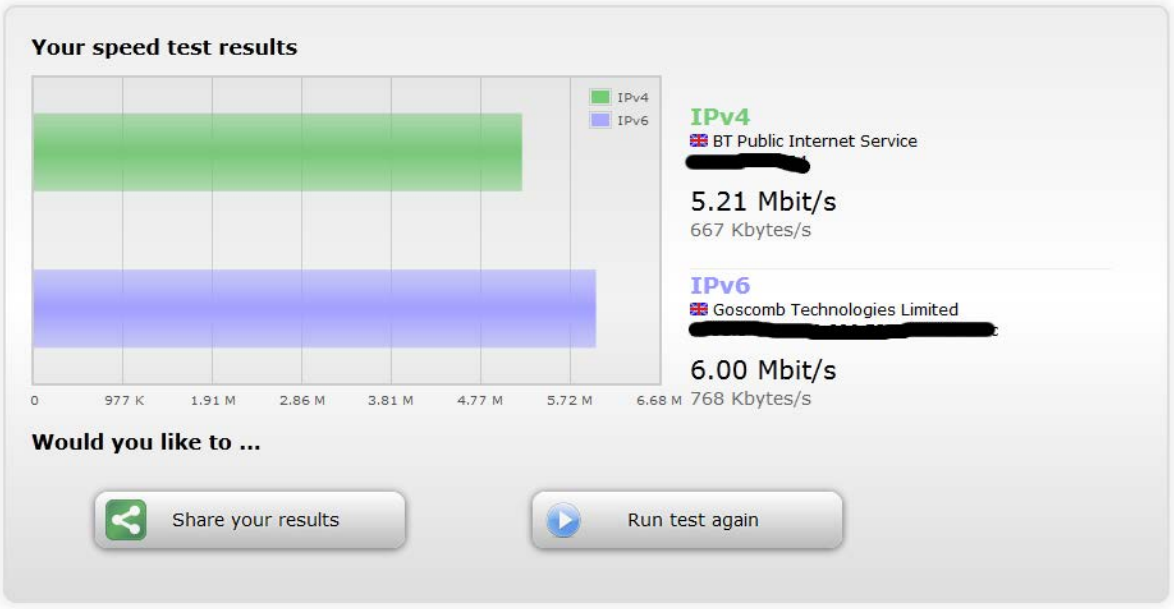


• Country	• IPv6 Adoption
France	4.53%
Japan	1.54%
China	0.55%
USA	0.51%
Netherlands	0.22%
Germany	0.15%
UK	0.12%

This measures IPv6 adoption by testing a subset of clients connecting to Google's website in each country. Therefore, this is not a measure of all Internet users but of Google users only.

Although it is often stated that tunnelled IPv6 has worse performance than native IPv4, in fact this is often not the case. Furthermore, it is even possible to get higher throughput using tunnelled IPv6 than with native IPv4. This is illustrated with the figure below[113].

[113] IPv6 speed test, http://ipv6-test.com/speedtest/.



Example ADSL Speed Test Comparing Native IPv4 with Tunnelled IPv6

The reason for this is that if the IPv6 tunnel end-point is topologically near to the client, once the traffic reaches the native IPv6 Internet it often has fewer hops to the destination over less congested routes. This can result in lower latencies and higher effective throughput for 6to4, Teredo and other tunnelled IPv6 traffic.

6. IPv6 Deployment Scenarios, Implications and Costs

Experience in many different types of organisations around the world has shown that there are many different deployment scenarios for IPv6. This section enumerates these scenarios and describes how they are most likely to be utilised by three main categories of organisations. There is no single deployment scenario that fits every organisation.

IPv6 includes a range of transition mechanisms that were designed to ease its deployment. These transition mechanisms were deliberately designed to allow the deployment of IPv6 in an organisation in a wide range of different ways. It is possible to deploy IPv6, on nodes first or on network infrastructure first. You can begin at the network edge (at the nodes in the network) or at the network core (in the heart of the network's infrastructure).

It is important to appreciate that many of the deployment scenario options apply equally across different categories of organisations. The first section below provides an overview of IPv6 deployment scenarios and the following sections consider how they apply to specific categories of organisations.

The organisations we are considering in this section have been broken down into three categories:

- Internet Infrastructure Suppliers
- Communication Service Providers
- End Users (Business and Consumers)

At a very high-level, there are three different types of scenarios for deploying IPv6:

1. Native Dual-stack deployment, in which IPv6 and IPv4 are deployed natively.
2. Use of tunnel based transition mechanisms, in which IPv6 is deployed over the current IPv4 infrastructure, typically using IPv6 in IPv4 tunnels. There are a large number of different transition mechanisms and scenarios that are based on tunnelling techniques.
3. Use of protocol translators to translate between IPv4 and IPv6.

It is common for a mixture of approaches to be used in a single organisation.

Experience has shown that the best deployment scenarios are those that are based on the native dual-stack approach. The dual-stack approach typically results in the most reliable, scalable, efficient and manageable deployments of IPv6. However, while dual-stack is the best practice deployment scenario, it may not be the cheapest and it is not always possible in all organisations.

There are currently over twenty six transition mechanisms that can be used to aid the deployment of IPv6 in either tunnelled or translated scenarios. Not all approaches are equal. Over time a number of deployment scenarios have become favoured, due to their reliability, cost, ease of deployment and manageability.

Understanding which approach is appropriate can be a complex task requiring a detailed knowledge of the options and the organisation in which they are to be deployed. In many cases it will be necessary to deploy IPv6 using mixed approaches combining the high-level scenarios listed above.

It is not only the features of the deployment scenario that must be considered, it is also necessary to consider the organisation. Each organisation's budget, current infrastructure and future requirements will have an impact upon which deployment scenario should be followed.

6.1 Native Dual-Stack Strategies and Costs Including Security Implications

A native dual-stack strategy is one where hosts, network infrastructure, services and applications all work seamlessly over both the IPv4 and IPv6 protocols. Deployment using this approach consists of IPv6 enabling everything whilst continuing to support IPv4 in parallel.

Before proceeding to consider the strategies in more detail, it is important to understand the term "dual-stack" more clearly. A "dual-stack" node is a node which supports both protocols natively. That is, a dual-stack node can use IPv4 and IPv6 directly on the network without tunnelling. An IPv6 node is *by definition* a dual-stack node. That is an IPv6 node can also communicate using IPv4. An IPv6 node is not a node which only communicates using IPv6, although it can be configured to do so.

In a native dual-stack scenario, both protocols can be used natively without tunnelling or translation. Using IPv4 and IPv6 natively avoids the performance, management, security and potential failure mechanisms that can result from tunnelling or translation techniques.
To deploy a native dual-stack solution, every aspect of the network infrastructure, hosts, services and applications need to be IPv6-enabled. Specifically, at a high-level:

- Desktop and server operating systems should be IPv6-enabled
- Network services should be IPv6-enabled
- Network and business applications should be IPv6-enabled
- Bespoke internal applications should be IPv6-enabled
- Network subnets should be IPv6-enabled
- Routing and switching infrastructure should be IPv6-enabled
- External Internet links should be IPv6-enabled
- Network management tools should be IPv6-enabled
- Network and host security services and systems should be IPv6-enabled and secured
- Network and Systems administrators should be trained in IPv6
- Support staff should be trained in IPv6.

Any organisation that wishes to deploy native dual-stack IPv6 must determine whether each piece of their ecosystem -- hardware, software and human -- has the ability to support IPv6 and has sufficient resources to support IPv6. For example, in routers, an organisation must determine first if the router can support IPv6 and secondly if, when IPv6 is enabled, it has the resources to support both IPv4 and IPv6 concurrently.

Sometimes determining whether a device supports IPv6 is not sufficient. In IPv6 deployments, technical details can be critical. For example, if a router supports IPv6 and has the resources to be IPv6-enabled, is the service it provides equivalent to that provided for IPv4? In some routers it is not. There are routers where IPv6 is supported in software when

IPv4 is supported in hardware. This leads to a significant performance differential between IPv4 and IPv6 that may compromise the success of an IPv6 deployment.

The following sections consider the implications and impact of a dual-stack strategy.

6.2 Impacts and Implications of Dual-Stack Strategies on End Systems

IPv6 support in end systems varies enormously depending on the type of end system.

6.2.1 Server and Desktop Operating Systems

All major modern operating systems have excellent support for IPv6. They are all based on IPv6 dual-stack implementations and have native support for both IPv6 and IPv4.

Microsoft Windows operating systems since Windows Vista and Windows Server 2008 have all been built upon an IPv6 dual-stack. That is, the stack is an IPv6 stack that also supports IPv4. All aspects of the operating system that are capable of working of IPv6 do so by default. This includes, for example, Microsoft Active Directory and CIFS file sharing.

Pre-Windows Vista operating systems do not have the same level of support for IPv6 and have a number of key differences that limit their use in IPv6 dual-stack deployments.

Unix, in its many different versions, has long had support for IPv6. Indeed, the reference implementation of IPv6 is the KAME[114] implementation used in a number of variants of BSD (including FreeBSD). Nearly all commercial versions of Unix have had support for IPv6 for over a decade. This includes, HP-UX, AIX and Solaris.

Linux has also has support for IPv6 for over a decade with some features being based on the KAME implementation.

Mac OS has had support for IPv6 since Mac OS X v10.1 and it has been enabled by default since Mac OS X v10.3.

This means, in principle, that support for IPv6 is widespread in operating systems. In many cases, currently deployed versions of the most common operating systems have included IPv6 as standard for many years. As such, operating system support for IPv6 is often not a limitation to a dual-stack deployment.

For the operating systems listed above, deploying a dual-stack solution may require no configuration changes on the end-host. Once IPv6 is implemented in the network and the local router on a subnet is IPv6-enabled, end-hosts will automatically use SLAAC and optionally DHCPv6 to configure IPv6.

However, there are some issues with operating systems that do need to be considered when deploying IPv6. These include:

- Limited functionality implementations (for example Windows XP which has limited support for IPv6 in the operating systems and the IPv6 stack is not a true dual-stack)
- Differences in address selection can cause routing and connectivity issues (implementation of RFC3484)

[114] The KAME project 1998 to 2006, http://www.kame.net/.

- Support for IPV6_V6ONLY and its default setting may affect behaviour of applications (some platforms have this flag, some have it on by default and some don't have it at all. Also, applications may change it from the default)
- Use of privacy addresses in Windows is on by default (extremely difficult to turn off, but introduces management and security challenges)
- Use of temporary addresses in Windows is on by default (extremely difficult to turn off, but introduces management and security challenges)
- Differences in support for host IPv6 firewalls and differences in default settings (some even break basic functionality, e.g. RHEL 6.x blocked DHCPv6 responses)
- Rogue 6to4 relays sending router advertisements (for example Windows systems with ICS enabled)
- Linux kernel 2.6.20 or earlier drops IPv6 fragments

In the main, the capital cost of deploying IPv6 on current operating systems is likely to be zero, as they include IPv6 support as standard.

However, the costs associated with the deployment can vary significantly. The deployment costs will include:

- Training of Systems Administrators and support staff
- Deployment planning
- Implementing a pilot and carrying out testing
- Fixing any esoteric issues that might arise (such as those listed above)

One crucial point to remember when deploying IPv6 on end-systems is that it is essential that backhaul IPv6 connectivity is operational first. Otherwise when hosts are attempting to connect to IPv6-enabled destinations, they will fail before falling back to using IPv4. The fallback delay can be many tens of seconds (typically an average of 30 seconds).

6.2.2 Hardware and Network Devices

Hardware IPv6 support in end systems is a rapidly changing area. There are two types of hardware to consider; that in end systems such as servers and desktops and that in stand-alone network devices such as network cameras and environmental monitoring devices.

In servers, desktops and other devices the only hardware that is usually involved in the processing of IPv6 and associated network protocols is the network interface card (NIC). Some NICs include hardware support for the processing of network stack protocol information, for example checksums, to relieve the system processor from the burden of such tasks. Network operating systems include functionality in their network drives that allow them to make use of such "off-loading" to the NIC.

In some servers and desktops, off-loading processor intensive operations to the NIC can be important for system and network performance. If this functionality is utilised in IPv4 then it is important to ensure that it is also supported in IPv6. Many modern NICs and operating systems support IPv6 off-loading. However, older equipment may not support IPv6 off-loading. In scenarios where the performance benefits are critical, it may be necessary to replace NICs.

Stand-alone network devices vary significantly in their functionality and capabilities. Some have native IPv6 dual-stacks and others do not. Some may be upgraded to support IPv6 and others cannot be upgraded. This means that there are likely to be some network devices in an IPv6 dual-stack deployment scenario that cannot be upgraded.

It is important that an organisation carry out an audit of network devices to determine if they can support IPv6. If a device cannot support IPv6, a decision needs to made as to how to deal with this. There are a number of options:

1. Replace the device
2. Continue to use the device over IPv4
3. Introduce a translation mechanism, such as NAT64, into the network to provide IPv6 connectivity to the IPv4 only network device. Introducing translators, such as NAT64, will not always be possible if the network device uses protocols or application layer data that contains IPv4 addresses.

In some cases, the only option may be option (2). Specifically, if a device does not and cannot support IPv6 and it uses protocols that cannot be translated even with an Application Layer Gateway (ALG) then if you cannot find a replacement device you can only use it over IPv4.

The impact of deploying IPv6 in end systems such as NICs and network devices will be very different for each organisation. The only way to determine the impact and cost to a specific organisation is to carry out an audit and gap analysis of their NICs and network devices.

6.3 Impacts and Implications of Dual-Stack Strategies on Transit Providers

Transit providers carry and route IP traffic between their peers. To provide a transit service, they not only need to be able to connect to peers, they also need to be able to share routes with them. Routes are usually configured either statically or more commonly using the Border Gateway Protocol (BGP).

In an IPv6 native dual-stack deployment, a transit provider's infrastructure must be upgraded to carry IPv6 datagrams and they must also be able to share routes using IPv6-enabled BGP. It is common for transit providers to deploy IPv6 natively as dual-stack, but it is not the only way that they can deploy IPv6. Indeed, some have utilised tunnelling to provide IPv6 service. From a customer's perspective, a native service is likely to provide better performance without the overheads of tunnelling. Furthermore, tunnelling at the ISP is an indication that their IPv6 deployment is not mature.

It is wrong to assume that because a transit provider is well connected for IPv4 that they are also well connected for IPv6. For example, one of the best connected service providers for IPv6 is Hurricane Electric. Whilst Hurricane Electric is not a Tier-1 ISP for IPv4, it is very well connected for IPv6 and is considered by some[115] to be a Tier-1 ISP for IPv6[116].

[115] Tier 1 for IPv4 != Tier 1 for IPv6, Scott Hogg, Network World, 2010, http://www.networkworld.com/community/blog/tier-1-ipv4-tier-1-ipv6.

[116] See section "Top 25 Transit/Upstream AS numbers in the routing table" at BGPmon's IPv6 BGP weather map, http://bgpmon.net/weathermap.php?inet=6. Hurricane Electric comes top of this ranking.

The implication is that transit provider customers might well choose different providers for IPv6 than they do for IPv4. Or they may move to different transit providers for both IPv4 and IPv6 depending on the level of IPv6 support that a transit provider has.

6.4 Impacts and Implications of Dual-stack Strategies on ISPs

As with any organisation, ISPs have a number of options when they are deciding how to deploy IPv6. First they need to obtain IPv6 transit connectivity which is becoming relatively easy. Then they need to deliver that to their down-stream customers. How they do this will depend on many factors.

In an ideal world, an ISP would deliver an IPv6 service to their customers that is equivalent to their IPv4 service. A desirable solution is the native dual-stack approach. In this scenario, the ISP enables IPv6 on their infrastructure in addition to IPv4. Both protocols are carried natively using the same infrastructure without the overheads of tunnelling or the unreliability of translation. From the customer's perspective, whether they are a consumer or an enterprise, they would have native IPv4 and IPv6 connectivity to the global Internet.

To deploy a native dual-stack solution, the ISP must be able to dual-stack enable all parts of their infrastructure. This includes the ISP's:

- Internal network infrastructure
- Backhaul connectivity
- Customer access network/s
- Customer CPEs
- Network services (DNS, DHCP etc)
- Authentication, Authorisation and Accounting (AAA) systems
- Network management and support systems
- Customer management systems.

For many ISPs, this is a significant undertaking that may take a number of months or years to complete.

6.5 Tunnelling Strategies and Costs - Including Security Implications

Tunnelling strategies leverage the existing IPv4 infrastructure to carry IPv6 traffic by encapsulating the IPv6 datagrams inside IPv4 datagrams. This is called tunnelling. Tunnels can be created manually or automatically. IPv6 includes a large range of transition mechanisms (currently over 26) many of which utilise automatic tunnelling.

Tunnelling mechanisms exist to help end-users to connect to the global IPv6 Internet, to help ISPs provide a dual-stack service to customers over a native IPv4 infrastructure and to help organisations use IPv6 over IPv4 MPLS.

There are a number of benefits of tunnelling IPv6 over IPv4 infrastructure:

- The IPv4 infrastructure does not need to be upgraded
- IPv6 infrastructure does not need to be deployed
- IPv6 connectivity is possible where it would otherwise not be available
- Utilises current IPv4 infrastructure

- It is usually cheaper to deploy IPv6 via tunnelling than natively
- It is usually quicker to deploy IPv6 via tunnelling than natively

Tunnelling strategies are particularly useful where the end user cannot obtain IPv6 connectivity from an upstream supplier. In these cases, the end user has little option but to tunnel to obtain IPv6 connectivity.

An example of a successful use of tunnelling is in the French ISP Free[117]. Free had a broadband network that for technical reasons could not be easily migrated to native IPv6. To provide an IPv6 service, Free turned to a transition technology called 6rd that allowed them to use their IPv4 infrastructure to provide what appears to their customers as a native IPv6 service. This solution was relatively cheap to implement and was implemented in weeks rather than the months or years of a native deployment.

Tunnelling strategies can be used in a number of different scenarios:

- Individual end users connecting to the IPv6 Internet from an IPv4 Intranet behind IPv4 NAT (Teredo)
- Islands of IPv6 networks without native IPv6 connectivity connecting to the global IPv6 Internet (6to4, Tunnel Brokers, Configured Tunnels)
- ISPs providing IPv6 service to broadband customers over an IPv4 access network (6rd)
- Carriers and enterprises deploying IPv6 over an IPv4 MPLS infrastructure (6PE and 6VPE)

Tunnelling can also be used to carry IPv4 traffic over an IPv6 network. This is a common scenario where an organisation has migrated their infrastructure to IPv6 and still wishes to provide an IPv4 service at the edge of their network. This is used in large ISPs and 4G mobile operators who are deploying IPv6 only infrastructures but still need to provide IPv4 connectivity to subscribers. The mechanism most commonly used in this scenario is Dual-Stack Lite (DS-Lite). Examples of such deployments include Comcast and Verizon in the USA.

All tunnelling techniques have disadvantages in comparison with a native IPv6 deployment. The most obvious disadvantage of tunnelling is the overhead of the tunnel itself. Carrying IPv6 inside other protocols adds processing and bandwidth overheads that can reduce performance[118]. Not only is there a traffic overhead, there can be an administrative overhead in setting up and managing the tunnels. This varies significantly depending on the tunnel type.

Certain types of tunnelling solutions are not guaranteed to work. There are two main reasons for this. Firstly, there exist failure mechanisms in some techniques. Secondly, the address prefixes used by some mechanisms are not guaranteed to be globally routable on the IPv6 Internet. For example, 6to4 traffic is not routable on some networks. As a consequence, end users using 6to4 may find that there are unexpected connectivity failures.

[117] IPv6 @ Free, Free, 2012, http://ripe58.ripe.net/content/presentations/ipv6-free.pdf.

[118] This does not always reduce performance. Interestingly it is possible to get better performance from tunnelled IPv6 than from native IPv4. This unexpected result arises because between some end points the IPv6 routing is more efficient that taking the native IPv4 path.

There are many situations where organisations will find it difficult to deploy IPv6 natively and will therefore opt for a tunnelling solution. The table below summarises some of these tunnel based solutions.

Tunnelling Technology	Comments
Configured Tunnel	Manual configuration has an administrative overhead that is not scalable to large deployments.
6to4	Requires a global public IPv4 address. Provides a unique /64 prefix. Failure mechanisms exist and is not guaranteed to be globally routable. Standard in many operating systems. Can be used by end user hosts or networks.
ISATAP	Used in IPv4 Intranets to provide IPv6 connectivity. Has security and operational issues.
6over4	Deprecated but still available on many platforms.
DSTM	Replaced by DS-Lite and never used today.
6rd	Provides globally routable dual-stack service to end users over IPv4 access network. Useful for ISPs that wish to deploy native IPv6 to customers but have reasons why they cannot migrate their access network to dual-stack operation.
Dual-Stack Lite (DS-Lite)	Provides globally routable dual-stack service to end users over IPv6 access network. Useful where infrastructure has been migrated to IPv6 only for operational reasons. Uses Large Scale NAT (LSN) at the end. Avoids the use of translation mechanisms so reduces number of failure mechanisms. Likely to be widely deployed in mobile and large ISP networks.
Teredo	Provides IPv6 connectivity to individual nodes in Intranets behind IPv4 NAT and firewalls. Available in many platforms including Windows. On by default in Windows Home editions. Has security implications. Useful for end-users connecting to IPv6 only services such as DirectAccess and Remote Assistant services.
Tunnel Brokers	Provides IPv6 connectivity where IPv6 is not available from service provider. Can provide unique global IPv6 prefixes and can be made secure. Can be a secure and quick way of getting IPv6 connectivity when service provider does not have native IPv6 service.
6PE	Uses IPv4 MPLS core to provide dual-stack service at the edge. Avoids changing MLPS core. Popular solution in large service providers and enterprises.
6VPE	Uses IPv4 MPLS core to provide dual-stack VPN service at the edge. Avoids changing MLPS core. Popular solution in large service providers and enterprises.

Tunnelling mechanisms introduce a large number of security vulnerabilities. Furthermore, the complexity of these mechanisms and their interaction between both IPv4 and IPv6 makes them challenging to secure.

Many of the mechanisms provide attackers with opportunities to launder attacks from IPv4 to IPv6 networks or vice versa. They increase the difficulty of determining where an attack originates. This has implications for security, for auditing and for the ease of tracing the source of traffic to meet the requirements of national regulations in some regions.

Laundering is where the origin of a datagram is disguised so that it is hard or impossible to determine which node sent the datagram. Typically, the source IP address is faked to hide the true source of the datagram. Attackers use laundering to make it hard for them to be caught and brought to justice. Laundering can and does take place within both native IPv4 and IPv6 networks. However, many networks (especially ISPs) implement techniques to

limit, detect or prevent IP address spoofing. This means that within the IPv4 Internet or the IPv6 Internet, it is often possible to determine the source of datagrams, if not to the specific node at least to the network that they originated from.

On today's networks, most nodes have transition mechanisms such as 6to4 and Teredo built in as standard. These mechanisms encapsulate IPv6 datagrams inside an IPv4 datagram (and in the case of Teredo an extra UDPv4 header as well) and then deliver these datagrams to the global IPv6 Internet.

The nature of these mechanisms means that any node on the IPv4 Internet can send faked IPv6 datagrams to any node on the IPv6 Internet. Since the IPv4 headers are removed when the datagram is delivered to the IPv6 Internet, some of the information that is essential to determine the source of the traffic is lost. The extra headers and intermediate devices (such as 6to4 relays and 6to4 routers) make it significantly more difficult to trace the datagram back to its source. In the case of 6to4, an attacker could fake the IPv4 header, fake the source IPv6 address and then send an attacking IPv6 datagram via a 6to4 relay. The relay would put that datagram onto the IPv6 Internet where it would eventually reach the victim node. Tracing back to the attacker would require determining the 6to4 relay used (in itself a non-trivial task) and then hoping that it has kept records that would allow a trace back to the source network (this is very unlikely).

The actually problem is more complex than this simplified description. Further, this is not the only way that transition mechanisms impact network security. However, the above example serves to illustrate the difficulties facing law enforcement agencies and Internet Service Providers when tracing the source of traffic laundered using the transition mechanisms.

A big concern with a number of mechanisms is the potential that they can be used to circumvent existing security measures. For example, Teredo is designed to punch a hole through NAT and firewalls to provide connectivity to the IPv6 Internet. One of the authors of this report has used this in countries where national firewalls limit access to certain Internet services to gain connectivity over to those services over IPv6. Tunnelling, particularly with IPv6, makes deep packet inspection much harder than it is with native IPv4 or native IPv6.

Furthermore, the complexity of each of these transition mechanisms increases the vulnerability of hosts and intermediate devices to attack both from the IPv4 and IPv6 Internets.

Tunnelling techniques are not the only transition mechanisms. A further set of mechanisms provides ways of translating between the IPv4 and IPv6. These techniques have many issues including security vulnerabilities. Still they are likely to be widely deployed. The most commonly used translation techniques are NAT64/DNS64. These are designed to be used in an IPv6 only network to provide connectivity to IPv4 nodes using IPv6. Networks that have IPv6 only nodes or subnets are likely to deploy NAT64/DNS64.

A recent study[119] has reported on the operation of IPv6-only networks from which IPv4 only nodes were reachable through translators. The study reported success with most network services. A small number of common services could not be reached using translators due to

[119] Experiences from an IPv6-Only Network, http://tools.ietf.org/html/draft-arkko-ipv6-only-experience-05.

their dependence on the network layer protocol. These included the widely used Skype[120] service.

6.6 Implications of Transition Scenarios on Address Management

All transition scenarios require both IPv6 and IPv4 addresses. This may seem counter-intuitive as the end-game is a transition to IPv6. However, even a native IPv6-only deployment will require IPv4 addresses for protocol translation in the short term.

Public IPv4 addresses are required in each scenario for the following reasons:

1. There has to be a way that IPv6-only nodes can communicate with legacy IPv4-only nodes.
    a. When using protocol translation (such as NAT64/DNS64), a public IPv4 address must be used for the IPv4 traffic before it reaches the IPv4 Internet
    b. When using native IPv4 in an Intranet, NAT44 or Large Scale NAT (LSN) will be still be required to connect to the IPv4 Internet. NAT44 and LSN require public IPv4 addresses to pass traffic to and from the IPv4 Internet
2. For those scenarios where IPv6 peering is involved the BGP speakers must have a public IPv4 address.

In the longer term, IPv6-only nodes without any IPv4 connectivity will become increasingly common.

This means that even during IPv6 deployment, there will be a need for more IPv4 addresses to support BGP for new Autonomous Systems (ASes) and to support the increasing use of NAT44 and LSN.

6.6.1 At RIPE and other RIRs

The exhaustion of IPv4 addresses in the RIPE region is predicted to take place in June 2012[121]. APNIC has already exhausted its pool of IPv4 addresses.

Once the IPv4 address space is exhausted, the Regional Internet Registrars such as RIPE NCC will then revert to their last slash-eight (/8) allocation policy. This policy greatly restricts the address space that can be allocated to RIPE members. Members will only ever receive one more allocation of IPv4 addresses, this allocation will be a /22 or only 1024 addresses. The impact upon organisations will vary enormously depending on their requirements for global IPv4 addresses. At one extreme, an organisation that has a stock of IPv4 addresses and a low allocation rate will not be affected. At the other extreme, a new business that requires IPv4 addresses for its services (for example mobile operators), its Internet connectivity (to use NAT) or for providing Internet services will not be able to do so.

Consequently, there will be a long period of time whereby some organisations have a significant advantage over others in the market-place just because they are fortunate in

[120] Interestingly, one of the main reasons for Skype's success is lack of IPv4 addresses and the consequent widespread use of NAT44. NAT44 breaks many other VoIP applications. Skype gets round this by tunnelling the VoIP and instant messaging traffic over HTTP. IPv6 makes this unnecessary. It remains to be seen if this will have any impact on Skype's popularity.

[121] Conversation with Tony Hain 29th February 2012.

having some remaining IPv4 address space. Purchasers of services from Internet Service Providers (ISPs), Hosting Companies and others will begin to specify as a requirement that the service provider has enough IPv4 addresses for their current and future requirements. This will become a differentiator in the market-place. Note too that this will not only have an impact with the UK or Europe but also globally.

There is another interesting side-effect of deploying IPv6. It affects the importance of address allocations. For the majority of organisations, one IPv6 address allocation will be sufficient for *all* their future needs. For example, the default allocation of a /48 prefix to end users provides them with 65,536 subnets, each with 18,446,744,073,709,551,616 node addresses (more than the grains of sand on the face of the planet).

This means that end users will not ever need to return to registrars for further address allocations.

The large address space also reduces the need for LIR and ISPs to obtain multiple address blocks. For example, a consumer ISP that provides customers with /64 (a single subnet) allocations can with one /32 block of Provider Assigned (PA) space, service 4,294,967,296 customers. Even if the ISP was to provide customers with multiple subnets by allocating /56 prefixes, the ISP would still be able to provide prefixes for 16,777,216 customers.

This means that even ISPs will not need to request blocks of IPv6 addresses from their registrar frequently, if at all after the first allocation.

There has been some discussion of the impact that the changes in the address space will have on registries. In the short term, registries will play an important role in managing the small amount of remaining IPv4 address space. In the long term their role in administering IPv6 address space will be just as important as administering IPv4 address space has been in the past, but it will take much less administrative effort to do so.

It should be noted that one activity that the RIRs will pursue is that of retrieving IPv4 address blocks. This is an important activity as has been noted earlier IPv4 addresses will be necessary for a long time to come.

6.6.2 At ISPs

In the previous section, we noted that IPv6 allocations to ISPs are much larger than IPv4 allocations. The default allocation of PA space to ISPs is a /32. This represents 4,294,967,296 subnets. Depending on how an ISP breaks down its IPv6 address space, it is unlikely to require large numbers of address allocations in the future.

ISPs will provide their customers with prefix lengths between /32 and /64. The most common allocation is likely to /64 closely followed by /48[122] (the default allocation).

6.6.3 At DNS registrars

IPv6 address management is unlikely to have a significant impact on DNS registrars.

[122] Best practice in the length of prefix allocations is likely to change with time as ISPs gain more experience with IPv6. Currently there are many sub-optimal allocations being made. For example, one hosting company in the UK provides each customer's server with a /48 prefix. This is totally unnecessary. However, because of the huge IPv6 address space this is not a major problem.

6.6.4 At Hosting Companies

Hosting companies are unlikely to require more than one IPv6 address block allocation per region that they operate in. One /32 allocation is likely to be more than they require for the foreseeable future.

One change that may occur in web-hosting, is with virtual hosting. There are two types of web virtual hosting, address based and name based. Address based virtual hosts require a different IP address for each virtual web server. Name based virtual hosts use the domain name presented in the HTTP header rather than the address to redirect the HTTP to the correct virtual web-server. Name based virtual hosts are common in IPv4 due to the shortage of IPv4 addresses.

However, name based virtual hosts have some limitations. They require special configuration to support SSL virtual hosts[123] and they may break certain types of load-balancing. IPv6 presents a solution to both these problems, as with IPv6 there is no need to use name based virtual hosts. There are enough addresses to assign an address for each virtual host.

6.6.5 At Enterprises that Manage their Own Address Space

Enterprises that manage their own address space have their own Autonomous System Number (ASN) or ASNs and they peer with one or more carrier advertising routes using BGP.

Any enterprise that wishes to manage their own address space must obtain an ASN, obtain an IPv6 address prefix, peer with one or more carriers and run BGP. As with IPv4, it is possible for enterprises to obtain their own provider-independent (PI) address space. Enterprises that already have an ASN for IPv4 can use the same ASN for their IPv6 network too.

Any enterprise deploying IPv6 should create an IPv6 address design as part of their overall IPv6 strategy. IPv6 addressing is very different from IPv4 addressing. Therefore there are new opportunities and challenges when designing an IPv6 address plan. It is important to avoid applying IPv4 thinking to IPv6 addressing.

For example, the massive address space in an IPv6 subnet[124] means that an IPv6 address scheme does *not ever* have to make provision for adding more addresses to a subnet.

6.6.6 IP Address Management Issues in a Combined IPv4/IPv6 Environment

The introduction of an additional address family, IPv6, into a network has a significant impact on address management. This is not only because there are now two address families to manage rather than one, but it is also because the two address families are significantly different.

[123] This is called "Server Name Indication", see RFC 4366. It is not supported in all browsers or applications.

[124] The address space in an IPv6 subnet is 2^64 = 18,446,744,073,709,551,616. This is an unimaginably large number.

IP address management (IPAM), covers the planning, deployment, tracking and management of IP addresses. It is usually closely integrated into system and network management tools, SNMP, DHCP, DNS, AAA, network security devices and auditing tools.

On a very small scale, IPAM may be a manual system, for networks of even moderate sizes IPAM systems are used instead.

The deployment of IPv6 has an impact on all aspects of IPAM. IPv6 presents new challenges to IPAM resulting from differences in IPv6 addresses, the IPv6 protocol and associated protocols. These differences also have an impact on security and network governance.

For example, in IPv6-enabled networks some nodes (most notably Windows hosts) use IPv6 privacy addresses and IPv6 temporary addresses by default. These addresses, when deployed using SLAAC, make it difficult to associate a particular address with a specific node. IPv6 temporary addresses, as the name suggests are temporary. These addresses are changed *every day*[125]. IPv6 temporary addresses are used by hosts for outgoing client connections. They reduce the chance that their permanent address will become known on the wider Internet. This feature makes it very difficult to trace network traffic to a specific client. As a consequence network forensics and accounting can be much harder in IPv6 networks. This is an issue for security in general but also in scenarios where records must be kept to meet regional legislation or organisational governance policies.

Other difficulties arise from: managing two address families, managing two types of addresses per interface, managing many IPv6 addresses per interface and managing IPv6 addresses with different scopes. This makes dual-stack IPAM potentially much more complex than IPv4 only IPAM.

6.7 Implications and Experience of Incentive Based Transitions

The previous sections in this report have shown that many countries have adopted some kind of incentives to encourage the adoption of IPv6. These vary from mandates to guidance. In some cases the incentives have been backed by financial support and in others they have not. Here are some general observations:

1. Countries with incentives are further ahead in IPv6 deployment than those without
2. Countries without incentives have less awareness of IPv6 and have a smaller IPv6 skills base
3. Countries without incentives tend to have built up little experience of IPv6 deployments. It has found that experience is very important in IPv6 deployments
4. Even countries with incentives are only just going to be ready for IPv6 exhaustion. Those without are behind
5. Experience has shown that there are many organisations that will require longish projects (months to years) to deploy IPv6. This includes ISPs and other types of service operators. The consequence for countries that have left deployment of IPv6 to market forces is that many of these organisations have not begun deploying IPv6 and will fail to do so before it becomes an issue for them and their customers.

[125] This is the default on Windows operating systems. This is configurable.

Countries that have had incentive based transitions now have sellable services, products and skills. They are competing in the global market. For example, Malaysia's NAv6 wins a lot of IPv6 training and consultancy business in the APAC region, for two reasons (a) they are competitively priced due to government support and (b) they have built up a lot of experience due to government support.

The readiness of countries for the exhaustion of IPv4 addresses has a clear link to government support. In countries with little support you can find two things (a) little or immature deployment of IPv6 and (b) a higher percentage of decision makers who still believe that there is no need to deploy IPv6.

There are many reasons why IPv6 deployments have progressed better where there is government support. These include:

1. IPv6 is a strategic service. Governments are better able to support long-term strategic projects whereas most organisations are looking to short-term tactical gains.
2. IPv6 is not a killer-application. Governments can see that the killer application is the Internet and that IPv6 is required to ensure the long-term growth of the Internet and Internet based services. Businesses are more likely to take the view that the Internet is working and nothing needs to be done.
3. IPv6 does not have a clear return on investment (ROI) in most organisations. Governments can take a broader view and see the necessity of IPv6 to underpin growth of the Internet and the businesses that are dependent upon the Internet. Furthermore, Governments can consider what is in the national interests on a global scale. Businesses look for a clear ROI and instead see a deployment cost and on-going support costs.
4. There is a lack of pressure to deploy IPv6. IPv6 often suffers from a "chicken and egg" situation. Customers do not use IPv6 because it is not available, suppliers do not supply it because there is no demand. Governments can break this cycle and kick-start the deployment of IPv6 creating demand.

The perception is that there is no business case for IPv6. It terms of ROI this is often true. Deploying IPv6 costs money. As a result, particularly in the current financial climate, deploying IPv6 becomes a low priority. IPv6 is more about reducing business risk than it is about ROI.

In a sense, IPv6 is like buying insurance, you don't get anything for that spend until something goes wrong. In the case of IPv6, it is insurance for when the Internet runs out of addresses and your business loses out to those who have IPv6. Unlike general insurance, the exhaustion of IPv4 addresses *will* happen and many implications of this event are yet to be determined.

A related problem is as assumption by organisations that when they need to deploy IPv6 it will be a simple matter to obtain new addresses. Naivety regarding the complexity of deploying IPv6 is a big risk that needs to recognised and addressed.

7. Implications of IPv6 Deployment on Privacy, Security and Policy

The objective of this task is:

- Evaluate and document security and privacy implications for business and consumers of IPv6 adoption
- Evaluate and document implications for Communications Providers regarding their duties under "The Data Retention (EC Directive) Regulations 2009" including subscriber identification, take-down and management of Digital Rights
- Evaluate and document the implications of IPv6 adoption regarding site blocking measures relating to Copyright Infringement and the blocking of material relating to child abuse
- Document the implications of IPv6 adoption regarding site blocking measures for law enforcement agencies.

7.1 Inputs

In approaching this task, we took into account the following inputs:

- Desk based research including legal precedents and publicly available materials on IPv6 deployment with regard to privacy, site blocking, law enforcement and security.
- Interviews with subject experts including representatives of the Serious Organised Crime Agency, Coalition of Children's Charities in the UK, and international experts on IPv6 one of whom has first hand experience of IPv6 advocacy within the European institutions and Swedish domestic policy.

7.2 Key results and conclusions

An analysis of the materials, and policy debate relating to IPv6 reveals a primary focus on the need for more effective, rapid deployment of IPv6. EU policy makers cite failure to adopt IPv6 as potentially inhibiting innovation, that reliance on the market only to implement IPv6 had "failed miserably"[126], and that EU competitiveness may be adversely affected compared with other regions, such as Asia, where IPv6 deployment has been more rapid[127].

The policy debate relating to the impact of IPv6 on data retention, content blocking, copyright infringement / takedown of infringing materials, privacy and child protection has been more limited. One reason for this is the Internet's fundamental design.

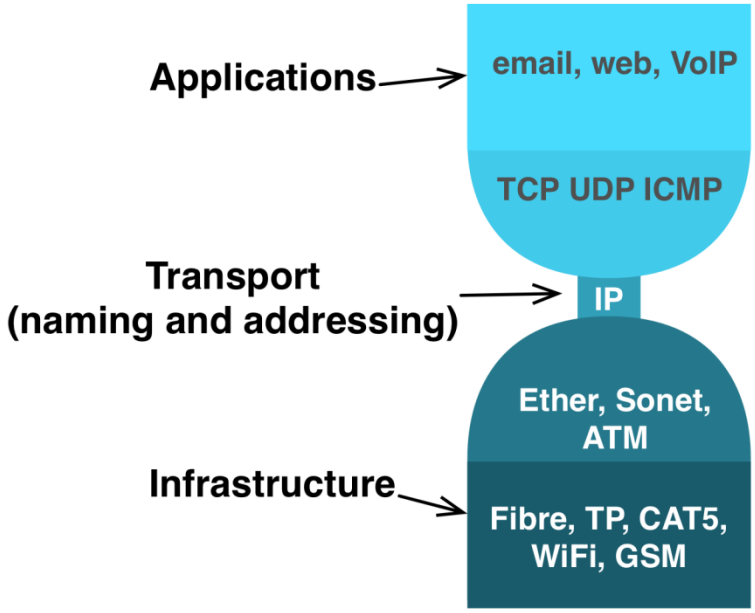
[126] Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the European and Social Committee and the Committee of the Regions on Advancing the Internet Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe (COM (2008) 313 final) http://eescopinions.eesc.europa.eu/EESCopinionDocument.aspx?identifier=ces\ten\ten351\ces1914-2008_ac.doc&language=EN

[127] For example, see Report from the Digital Agenda Assembly, 16-17 June 2011, 3 "If Europe is not to be left behind in the digital age, more needs to be done to encourage IPv6 deployment now." http://ec.europa.eu/information_society/events/cf/daa11/document.cfm?doc_id=18306

That said, the move from IPv4 (a scarce resource) to IPv6 (almost unlimited) originally was perceived to have altered the existing balance between law enforcement and individual privacy, and the Article 29 Working Party amongst others noted concerns in 2003. There followed the development and widespread implementation of IPv6 privacy extensions. At the time of writing, these privacy extensions are extensively deployed by default in new software and devices. Our evaluation is that, while the detail may vary within IPv4 and IPv6 environments, at a high level, the ability to identify individual users through IP addresses remains broadly unchanged. Both IPv4 and IPv6 provide opportunities to obscure individuals' identity – whether by accident or design.

7.2.1 The Internet Hourglass

A feature of the Internet's basic design is the separation of infrastructure, transit and application layers. Referred to as the "internet hourglass" model, while the infrastructure and application layers continue to expand, the transport layer, IP, remains thin.



Source: Rosenberg, 2008, IETF Tools

This model is adaptable to innovation both in the types of infrastructure that support Internet connectivity, and the burgeoning number and types of Internet applications now available. The connecting layer in the middle, IP, remains separable and distinct. Whether the means of transport is IPv4 with IPv6, it usually will not affect the behaviour of the content above it, or infrastructure below it.

7.3 Content Blocking, Privacy, Security and Child Protection – Recent Precedents

2010-2011 saw plenty of litigation in relation to content blocking (including the Newzbin cases[128] and the decision of the European Court of Justice in *Scarlett Extended SA v*

[128] Twentieth Century Fox Film Corporation and others v Newzbin Ltd [2010] EWHC 608 (Ch), 29 March 2010; [2011] EWHC 1981 (Ch), 28 July 2011; and [2011 EWHC 2714 (Ch), 26 October 2011.

Société belge des auteurs, compositeurs et éditeurs SCRL[129]). The cases explore the controversial issue of using technical measures to block content which allegedly infringes copyright. Most recently the ECJ held that an order requiring an ISP to block access to such material was incompatible with EU law, as eroding the fair balance between protecting intellectual property on the one hand and the fundamental rights of individuals to protect their personal data and their freedom to receive or impart information, and an ISP's freedom to conduct its business, on the other.

While European member states have introduced laws such as the Digital Economy Act in the UK, or the introduction of the state agency HADOPI in France in an effort to combat online copyright piracy, the measures themselves have proved unpopular[130], difficult to implement, and in at least one case (e.g. HADOPI) elements were found to be unconstitutional[131].

For the purposes of this study, however, the focus is narrow. It is to evaluate the impact of the transport layer on such activities, and measures to try and combat them.

7.4 IPv6, No Longer a Scarce Resource

It is unclear whether substituting an IPv6 address for an IPv4 address changes anything. Does it make life easier or more difficult for law enforcement agencies, or those committing online crimes?

IPv4 addresses have been treated as a scarce resource for many years. In practical terms, this scarcity has been one of the reasons why IPv4 addresses are allocated on connection, and rotate amongst an ISP's user base. Therefore, there is no firm 1:1 mapping between a device, or connection, and an individual. This supports user anonymity on the network, and inhibits reliable identification by law enforcement of individual perpetrators by means of IP address mapping. This is the current situation.

In contrast, IPv6 jumps from 32 bit (IPv4) to 128 bit addresses, an almost unlimited supply. The impact of this change from scarcity to plenty should be a more reliable 1:1 mapping between individual and device.

7.5 IPv6 and Tracking Devices

IPv6 has a feature which is not present in IPv4. IPv6 addresses on a local link are auto-configured using a combination of network information and an "interface identifier". The "interface identifier" is a number often generated using an IEEE identifier or MAC address. Every device on the network[132] has an IEEE identifier, which is unique to the device. On the assumption that a device's movements and activities correlate to those of its individual owner, IPv6 therefore created a potential to track and trace individual behaviour on the

[129] Case C-70/10, 24 November 2011

[130] For example, recent popular demonstrations in the US, and websites going "dark" in protest against the proposed SOPA law.

[131] Decision of French Constitutional Council, 10 June 2009.

[132] On Ethernet's family of IEEE 802-based networks

network through their IPv6 address, even across jurisdictions as Internet use increasingly becomes mobile[133].

Therefore, in broad terms, IPv6 as originally designed created new opportunities for law enforcement and detection of crime as it also posed threats to individual consumers' fundamental rights to protect their personal data. The ability of predators to track vulnerable individuals through their mobile devices or things (e.g. children's toys) was also cited as a child protection concern relating to IPv6.[134]

7.6 Article 29 Working Party and IPv6

In 2002, the Article 29 Data Protection Working Party, an independent advisory body on data protection and privacy set up under Article 29 of Directive 95/46/EC, published an Opinion[135] expressing concern that IPv6 addresses posed risks to individuals' privacy, of manipulation, and fraudulent use. It called for protective measures to be introduced.

By 2003, the European Commission IPv6 Task Force in a discussion document addressed to the Article 29 Working Party noted that privacy extensions to IPv6 (introduced by RFC 3041 in 2001[136]) "provide a set of necessary and unique tools to empower a user's privacy in ways that are not possible in IPv4." The paper describes the privacy extensions as "a potentially powerful tool to improve the possibilities for user privacy." The Task Force recommended that privacy extensions be enabled by default.

7.7 How Far are the Privacy Extensions Enabled?

According to our research, implementation of IPv6 privacy extensions is already significant, with many manufacturers increasingly enabling them by default:

[133] Active mobile-broadband subscriptions per 100 inhabitants 2007-2011 in the developed world has grown from 19 in 2007 to 55 in 2011 (Source ITU, http://www.itu.int/ITU-D/ict/statistics/ accessed 22 March 2012)

[134] Source: Interview with John Carr, CCHIS, 2012.

[135] "Opinion 2/2002: on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6"

[136] http://tools.ietf.org/html/rfc3041

MacOS X 10.5, 10.6		✔	
Mac OS X 7	✔		
Windows XP	✔		IPv6 support is not pre-installed. However, once installed, privacy extensions are enabled by default
Windows 7	✔		Windows 7 generates automatically random interface IDs for every attached IPv6 interface and uses them for privacy addresses
Linux		✔	Many variants of Linux exist, most disable privacy extensions by default
UNIX		✔	Many versions of UNIX exist. Most have privacy extensions in the kernel, but disabled by default.
iPhone/iPad		✔	Privacy extensions are part of the kernel, but there is nothing in the user interface which allows users to turn on privacy extensions. While there are some reports that since iOS 4.3 extensions are turned on by default, there are conflicting reports on this.
Android			Many versions. Privacy extensions appear to be disabled by default in versions below 2.2

However, this is not the full story. Privacy extensions have two aspects. The first replaces the MAC address or IEEE identifier with a pseudo-random identifier. However, while this disjoints the individual user from his or her Internet enabled device, such numbers can (albeit with greater difficulty) still be used to identify an individual through an IPv6 address. The other aspect of privacy extensions is that a portion of the address is programmed to change at intervals, sometimes as often as every day.

While this presents a more robust level of privacy protection, it has knock-on effects on network management, with the result that in practice many organisations turn off the privacy features.

7.8 Conclusions

Without security extensions, IPv6 could assist tracking both for network aspects and for relevant security organisations. Privacy extensions have been developed and are enabled

by default (or by user opt in) in many versions of software, browsers, and hardware currently on the market. However, in practice, privacy extensions are disabled, because of the additional management and cost overheads that they create. In any event, the transport layer does not impact many other tools (e.g. cookies) which exist to track user behaviour online.

Our view is that, while it is correct to say that IPv4 does not offer the same privacy extensions as IPv6, the way that IPv4 was treated as a scarce resource provided inbuilt privacy protection because it was unlikely that a single IPv4 address would always identify the same user, and IPv4 addresses do not have the ability to identify uniquely a device connected to the network.

In other words, even with privacy extensions in place, IPv6 does not significantly change the previous position for privacy under IPv4.

Policy makers and advocates are only beginning to understand the implications of IPv6, however, and the policy dialogue has not yet matured. A result of the slow implementation of IPv6 is that many agencies, such as law enforcement, have not yet developed a coordinated response, or even ownership of the issue internally. The implication of this is that the policy issues that will accompany large scale implementation of IPv6 are currently poorly understood.