Electronic Communications Committee (ECC)
within the European Conference of Postal and Telecommunications Administrations (CEPT)

PREPARING FOR IPv6

Lisbon, February, 2010

EXECUTIVE SUMMARY

There are two forms of the Internet Protocol that are used on the Internet today. One is IP version 4 (IPv4), which has been in use for over 25 years, and the overwhelming use of the Internet today is based around IPv4. The other is IP version 6 (IPv6) which was invented in the early 1990s and has had limited uptake to date but is considered to be essential to the longer-term future of the Internet. Very few devices and services use IPv6. The two versions are fundamentally incompatible.

One of the main reasons for the change from IPv4 to IPv6 is that the addresses available for IPv4 are running out and the transition to IPv6 needs to be accelerated to avoid a serious problem of address shortages. IPv6 has a much longer address than IPv4 and hence there are many more IPv6 addresses available - almost an infinite number.

The pool of available new IPv4 addresses is expected to be exhausted by 2011. Once this happens, it will be difficult to introduce new users and services because IPv4 addresses will be hard to obtain. Future growth of the Internet will almost certainly involve much greater uptake and deployment of IPv6 than there has been to date.

The exhaustion of the available IPv4 address space will not be abrupt or cataclysmic from an operational perspective. The Internet will continue to work. Traffic will still flow and existing users will continue to send email, visit web sites and use the other services they enjoy on the Internet. However it will become increasingly difficult to introduce new services or expand networks based on IPv4 because IPv4 addresses will become harder to obtain. There will of course be an abundance of readily available IPv6 addresses. IPv4 will not disappear for the foreseeable future - there will be a long co-existence.

This report:

- Describes how the process of migration from IPv4 to IPv6 may work
- Evaluates the likely timescale
- Identifies actions that governments and regulators should take to ensure that:
    - there is adequate information and that
    - the motivations of individual all parties are aligned so that there can be a market led migration that
will minimise the problems for service providers and users.

This report recommends that:

1) Governments and regulators should encourage that the essential parts of the Internet in their countries are adapted to support IPv6 in time for the rest of the migration to proceed under normal commercial arrangements and market forces. This is even more important than including IPv6 in Government procurements although this is itself worthwhile and important.

2) Governments and regulators should set specific but realistic targets for achieving IPv6 support in the main parts of the Internet infrastructure.

3) Publish progress on IPv6 migration through the ECO Internet website

Table of contents

Preparing for IPv6

1   INTRODUCTION

The Internet Protocol is the central architectural element in providing the worldwide connectivity of the Internet. This is the "common language" that all the machines connected to the Internet use.

The Internet Protocol uses standardised unique addresses to identify interfaces at the edge of the Internet and these addresses are used to identify where a message is being sent to and where it is being sent from. The address is broadly similar in function to a telephone number.

There are two forms of the Internet Protocol that are used on the Internet today. One is IP version 4 (IPv4), which has been in use for over 25 years, and the overwhelming use of the Internet today is based around IPv4. The other is IP version 6 (IPv6) which was invented in the early 1990s and has had limited uptake to date but is considered to be essential to the longer-term future of the Internet. Very few devices and services use IPv6. The two versions are fundamentally incompatible.

One of the main reasons for the change from IPv4 to IPv6 is that the addresses available for IPv4 are running out and the transition to IPv6 needs to be accelerated to avoid a serious problem of address shortages. IPv6 has a much longer address than IPv4 and hence there are many more IPv6 addresses available - almost an infinite number.

The pool of available new IPv4 addresses is expected to be exhausted by 2011. Once this happens, it will be difficult to introduce new users and services because IPv4 addresses will be hard to obtain. Future growth of the Internet will almost certainly involve much greater uptake and deployment of IPv6 than there has been to date.

The exhaustion of the available IPv4 address space will not be abrupt or cataclysmic from an operational perspective. The Internet will continue to work. Traffic will still flow and existing users will continue to send email, visit web sites and use the other services they enjoy on the Internet. However it will become increasingly difficult to introduce new services or expand networks based on IPv4 because IPv4 addresses will become harder to obtain. There will of course be an abundance of readily available IPv6 addresses.

Many organisations worldwide are discussing this problem and best way to manage the transition from IPv4 to IPv6; they include the European Commission, OECD and the IPv6 Forum. These discussions to date focussed more on promoting general awareness of the IPv4 exhaustion problem and the features of IPv6, than on clarifying and explaining how the migration process should or will work in practice, ie the sequence of events and the decisions at each point, and the motivations of the individual players.

The objectives of this paper are to:

- Explain the issues

- Describe how the process of migration from IPv4 to IPv6 may work

- Evaluate the likely timescale

- Identify actions that governments and regulators should take to ensure that:
  o   there is adequate information and that
  o   the motivations of individual layers are aligned

so that there can be a market led migration that will minimise the problems for service providers and users.

Action is needed because if we do nothing we risk:

- a later and more haphazard migration to IPv6 that will affect the scope and quality of Internet services;

- reduced effectiveness of programmes to promote the Information Society.

2   ABBREVIATIONS

ARIN	American Registry for Internet Numbers,
DNS	Domain name System
IANA	Internet Assigned Numbers Authority,
ICANN	Internet Corporation for Assigned Names and Numbers,
IP	Internet Protocol
ISP	Internet Service Provider
ITP	Internet Transport Provider
NAT	Network Address Translator
RIPE NCC	Reseaux IP Europeens - Network Coordination Centre
RIR	Regional Internet Registries

3   THE IPV4 ALLOCATION PROBLEM

3.1   Introduction

The master registry for IP addresses is the Internet Assigned Numbers Authority, IANA (www.iana.org). It is responsible for the global coordination of the root of the DNS system, IP addressing, and other Internet protocol resources. IANA has existed since the early days of the network that has become today's Internet. Today it is a part of the Internet Corporation for Assigned Names and Numbers, ICANN (www.icann.org), a not-for-profit public-benefit corporation with participants from all over the world. ICANN co-ordinates the development of policy on the use of the Internet's unique identifiers.

IANA does not allocate IP addresses directly to the general public. It allocates blocks of 16M addresses (called /8s) to the 5 Regional Internet Registries (RIRs) who then distribute those addresses amongst their members, which are mostly ISPs and Telecommunication Companies. The RIRs are non-profit organisations. RIPE NCC, based in Amsterdam (www.ripe.net) is the RIR for Europe, Central Asia and the Middle East. Each RIR develops its own policies on how address resources are managed and allocated.

Address allocation policies at each RIR are broadly similar. Addresses are allocated on the basis of need. When an organisation needs address space, it submits an address plan to the RIR if it obtains addresses directly from the RIR. If is obtains addresses from an ISP, then it would normally submit an address plan to the ISP and ISP submits aggregated plan to the RIR The address plan is checked by the RIR to ensure its correctness and that it conforms to the prevailing allocation policies. If all is in order, the address space is assigned to the organisation, which then uses it as it sees fit: for instance by assigning some of that space to its customers. When a RIR runs low on unallocated addresses, it submits a request to IANA, which then assigns it another block of address space.

None of these address assignments involves payment. IANA's services to the RIRs are free. RIRs charge fees to their members for registration services, but not for the allocation of addresses themselves. Some ISPs however charge customers for blocks of address space. These charges vary depending on the ISP, how much address space they have available for assignment and how much space the end customer requests.

The concept of ownership of IP addresses is not established in property law. A recent paper jointly authored by Raymond Plzak, outgoing President and CEO of the American Registry for Internet Numbers, ARIN, states:

> "There is broad agreement that IP addresses are not "property.". They are part of a service, and the IP address is "loaned" as part of the service, to permit a routable address. "

3.2   Current situation

The total size of the IPv4 address space is 256 /8s, in total some 4 billion addresses. 34 of the 256 /8s were still available in early 2009. Figure 1 shows the current allocation situation. There are four general categories:

- Allocations still available

- Allocations used or reserved for experimental purposes

- Historical allocations made before the RIR system was created, some of which may have been substantially greater than were really needed

- Allocations made through the current system of RIRs.

There are currently 34 from the total of 256/8s still available.
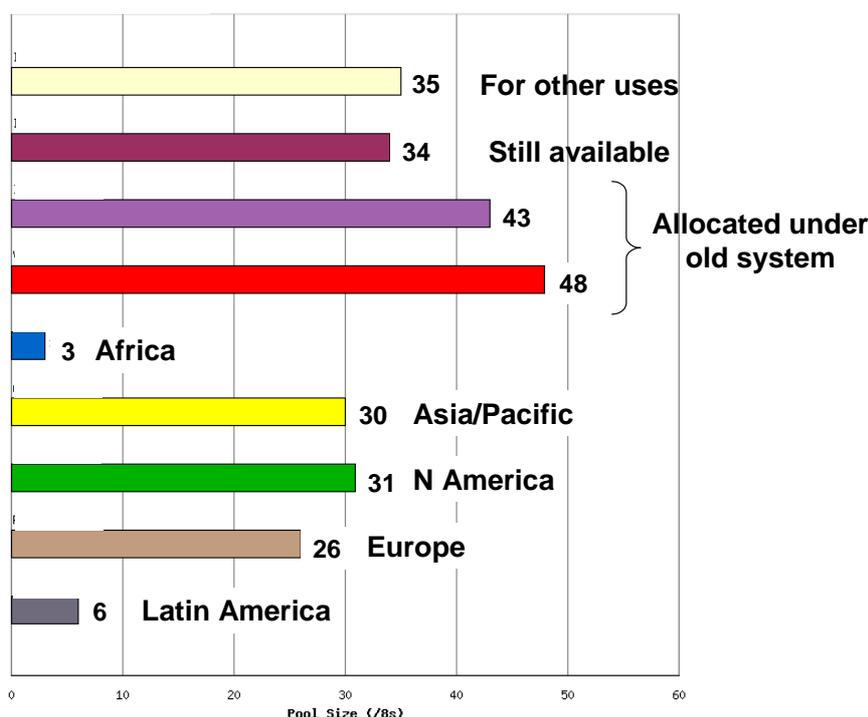
Figure 1: Current IPv4 allocations (March 2009)
(From: http://www.potaroo.net/tools/ipv4/index.html)

The allocations to the RIRs consist of the following types:

- Unallocated (pool)

- Allocated but unadvertised, ie not visible to the rest of the Internet

- Allocated and advertised, ie actively used and seen by the rest of the Internet.

Some organisations are using public IPv4 addresses internally without advertising them to the rest of the Internet (second type). The reason why they are using public and not private addresses is that they wish to be prepared to connect their networks in the future to the public Internet and advertise the addresses. If alternatively they used private addresses then they would need to change their addresses in the future. Consequently no one knows how much of this allocated but unadvertised space is not used at all.

The quantity of allocated but unused addresses in quite large and dates back to allocations of more space than is necessary that were made in the earlier days of the Internet before the RIR system was started. Many of these allocations are held by organisations based in North America.

Figure 2 shows the growth in allocations by IANA to the RIRs.
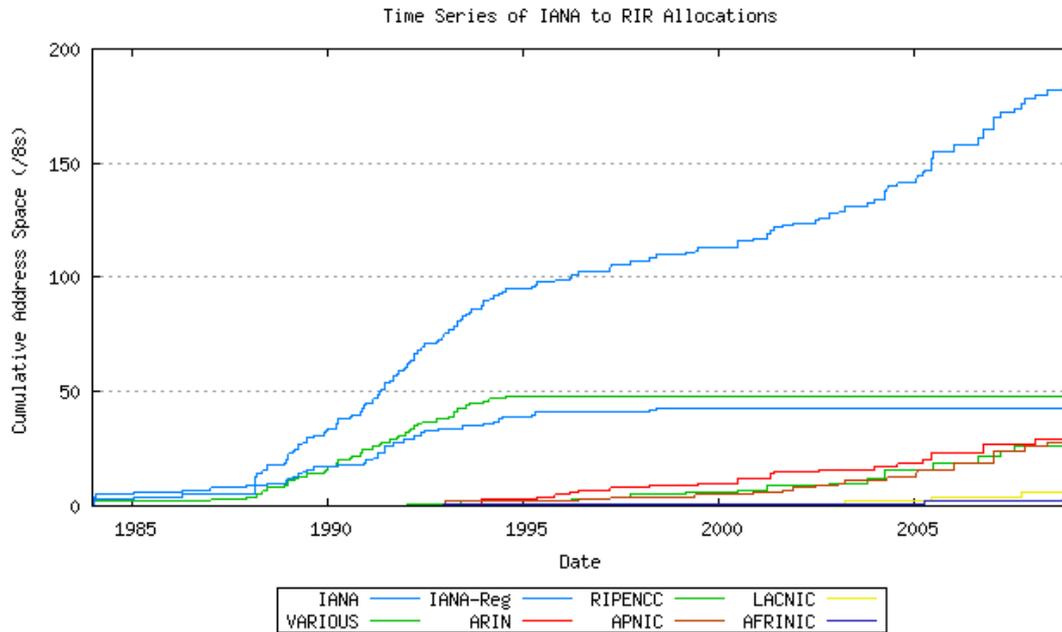
Figure 2: Growth in allocations to RIRs
(From: http://www.potaroo.net/tools/ipv4/index.html)

The following table lists the RIRs.

RIR	Region
AFRINIC	Africa
APNIC	Asia Pacific
ARIN	America
LACNIC	Latin America and Caribbean
RIPE	Europe

Extrapolating at the current growth rate of 8% pa, the available capacity held by IANA will run out in March 2011 and the capacity held by the RIRs in May 2012.

3.3 Methods of extending the lifetime of IPv4

The predictions of running out of addresses in 2011/12 are not the whole of the story. There are various methods for extending the life of IPv4 such as:

- organisations releasing back unused allocations to the RIRs for re-allocation.

- organisations exchanging unused allocations on commercial terms - a secondary market in IPv4 addresses.

- organisations using the existing allocations more efficiently, possibly with the incentive of the RIRs introducing charges.

The method for more efficient use involves a Network Address Translator (NAT), which works at the boundary between a private address area and the public address area. This allows a larger quantity of private addresses to be represented on the public Internet by a smaller quantity of public addresses. The relationship between specific private and public addresses changes continually depending on user demand. This can make it difficult to determine which device behind the NAT was using a particular public IP address at a given time.

Many home and small office networks use NAT. All the devices on the local network use private IP addresses that are translated typically to just one public IP address assigned to the customer by the ISP. Some ISPs are introducing "carrier grade" NAT where the ISP uses private addresses for all its customers and map those addresses into a large block of public address space.

Based on our assessment of the current situation, 4 years would be our best estimate of the additional life for IPv4 from these measures.

3.4   Future growth in demand for addresses and eventual exhaustion date

It is difficult to predict how demand for addresses will grow and the growth rates will be different in different countries depending on the wealth of the country and on the penetration of broadband.

Some European countries have a reasonably mature broadband market where increased broadband penetration will generate new low volume users and some new demand. Higher access speeds will not necessarily increase numbers of transactions and demand for addresses. In other countries with lower levels of broadband penetration there will be greater scope for increased demand.

Management changes within organisations tend to increase demand as growing organisations and new systems require additional addresses for these changes, whereas when organisations contract or replace old systems they may fail to release the addresses that they no longer really need.

The biggest factor in the growth in demand for addresses is the increasing growth of the Internet penetration in the developing world.

There is a possibility that usage of IPv4 addresses in some countries will reach a plateau within the existing capacity, and so they will not run out of IPv4 addresses. However, it is unlikely that global demand will saturate within existing capacity as some large countries still have large growth potential, and so even if they does not run out of addresses the world will. Therefore migration to IPv6 will definitely be needed at some stage.

3.5   What happens when IPv4 runs out?

In the absence of IPv6, the existing Internet will continue to run but new users and new content providers will be either unable to gain access to the Internet or, assuming that some price mechanisms have developed, will have to pay more for access, or accept lower quality access as a result of increased sharing or public addresses by NATs.

Users and content providers that can only obtain IPv6 addresses then will only be able to communicate with other parties that have IPv6 addresses.

4   THE STRUCTURE OF THE INTERNET

The Internet consists of:

- A "backbone" connectivity platform provided by a number of relatively large interconnected operators (hereinafter Internet Transport Providers, ITP) who normally exchange traffic without payments, called peering. These ITPs may be Telecommunication Companies with their own transmission infrastructure (ducts, fibre) or companies that rent leased lines or other forms of transmission capacity from Telecommunication Companies.

- Many Internet Service Providers (ISPs) who provide access services to large and small customers. These ISPs may exchange traffic using peering between each other locally but they also pay the ITPs for the global connectivity.

- The broadband (wireline (i.e. xDSL, cable) and wireless (i.e. 3G/4G)) access systems between the end customers and the ISPs, which mostly are provided by the Telecommunication Companies.

- The Domain Name System (DNS), which is a distributed hierarchical database consisting of many servers whose primary role is to translate domain names into IP addresses.

- Many other servers such as:
    - email servers that support the email service
    - web servers that store content that is accessed on the web
    - SIP servers that support voice and other media communications
  These servers may be either run by users or by ISPs on behalf of their users.

- The networks on customers' premises.

The physical arrangements are highly varied, but there is extensive use of third party hosting facilities where a third party runs the physical equipment that is used to provide a wide variety of services and content that is sold by others to provide economies of scale and scope. Some of the physical arrangements are concentrated at Internet Exchanges such as LINX in UK or AMS-IX in Amsterdam where ITPs, ISPs and hosting organisations all run their equipment in specially designed secure buildings and are able to make easy interconnection to each other.

5 MIGRATION TECHNIQUES

There are a number of techniques to facilitate migration:

5.1 Dual stack

The Internet uses a multi-layer reference model shown in Figure 3. Each layer is designed to be independent of the others. Therefore a change of technology in one layer should be completely transparent to the layers above and below it.

The lowest layer is the physical level. This is concerned with transmission speeds, radio and optical frequencies, voltages and the characteristics of network cabling.

The link or MAC layer deals with the transmission of data over a physical link such as an Ethernet or a wireless network.

The network or inter-network layer determines how data is organised into packets and routed between end-points on the network. These may not necessarily be connected to the same physical network. The network layer also assigns a globally unique address to identify a device on that network. For the Internet these are either IPv4 or IPv6 addresses. The transport layer is responsible for re-assembling the data received from the network layer, performing flow control and handling lost packets. Most services on the Internet use Transmission Control Protocol (TCP) to provide reliable connections between devices.

The application layer deals with high-level services such as email or web access. Most of these services are connection-oriented and therefore depend on TCP connections between the client and server. Some Internet applications use lightweight connectionless transport protocols such as Universal Datagram Protocol (UDP) because these are better suited to Voice over IP (VoIP) and streaming audio or video services.

This layering principle is one of the reasons why the Internet is so successful and ubiquitous. The network layer does not care or need to know which physical networks are used. Similarly the transport layer does not need to know or care about how packets get routed across the network. So if the network topology changes or a new data transmission protocol is invented (say Bluetooth or WiFi), the higher level layers can use them without knowing they are there. For example, someone using a web browser on a mobile phone will probably use 3G or GPRS to send data to the Telecommunication Companies network which then transmits it over fibre to an Internet Exchange where it passes through several Ethernets to reach a web server in some ISP's network.

In the context of Internet addressing, this means that in principle traffic that is currently using the IPv4 network layer could move to IPv6 without troubling the transport and network layers above or the physical or link layers beneath. Broadly speaking, these should be unchanged. There will be no need to deploy IPv6-only cabling. And apart from minor changes or upgrades to accommodate IPv6 addresses, application software will not need to be replaced neither for clients nor servers. In fact, most operating systems in use today already support both IPv4 and IPv6. Many applications do too.

Dual stack enables equipment to handle both IPv4 and IPv6 addresses. Since the equipment is designed in a layered structure the existence of alternative protocols at the addressing layer should not affect the upper TCP and application software or lower link layer software. This is illustrated in figure 3.
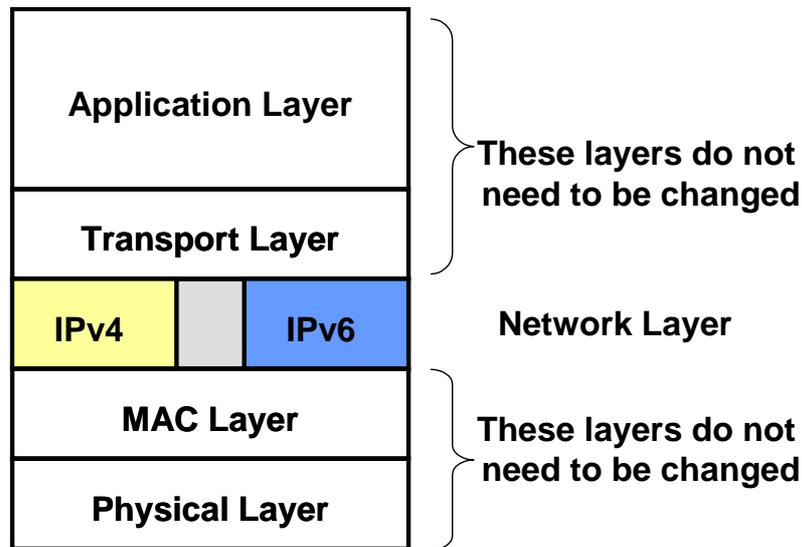

Figure 3: Dual stack operation

In dual stack operation, both IPv4 and IPv6 packets can be sent intermingled on the same transmission path. This means that in principle IPv6 can be introduced on an existing network without disrupting the existing IPv4 installed base. The routers within the Internet will have different routing tables for IPv4 and IPv6 and so packets will take different paths. The routing tables will have to ensure that IPv6 packets are sent only to other routers that can handle them and not to routers that can handle only IPv4. This is illustrated in figure 4.
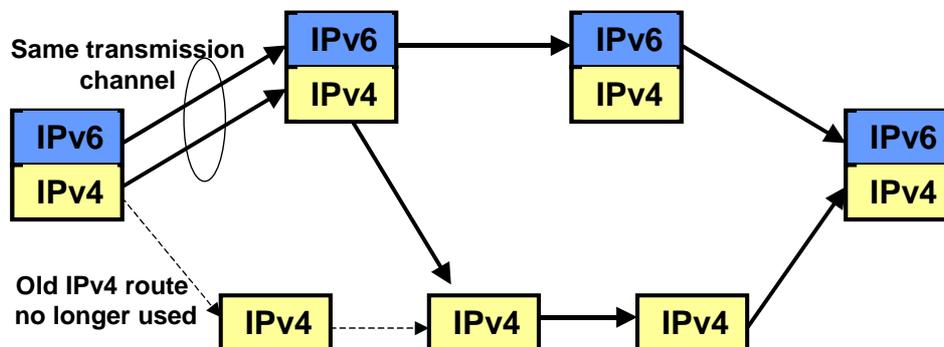
Figure 4: Dual stack router network

The genius of the Internet is the Border Gateway Protocol, which automatically updates routing tables as new addresses are advertised, thus the continual process of updating routing tables during the migration will be automated.

5.2   Network Address Translation (NAT)

Just as NAT can be used between private IPv4 addresses within a customer network and public IPv4 addresses in the public Internet, NAT can be used between IPv6 addresses in a customer network and IPv4 addresses in the public Internet or vice versa. Thus NAT could be used to enable a customer network to start using IPv6 addresses, possibly with some tunnels, before their main ISP implements IPv6 with dual stack. This arrangement might for example be used by a university or academic institution that wishes to experiment with IPv6.

5.3   Tunnelling

Tunnelling allows isolated areas of the Internet with one type of address to establish links across areas with the other type of address, so for example areas that use IPv6 can be linked across areas that use IPv4 only. The tunnel needs to be pre-established between the routers at each end of the tunnel. When the router at one end of the tunnel handles an packet with an IPv6 address within a given range relating to the tunnel it will wrap the packet with an IPv4 header containing the IPv4 address of the other end of the tunnel, and route the packet across the IPv4 network to the other end where the IPv4 header will be removed. The packet is then routed further using the IPv6 address. This is illustrated in figure 5.
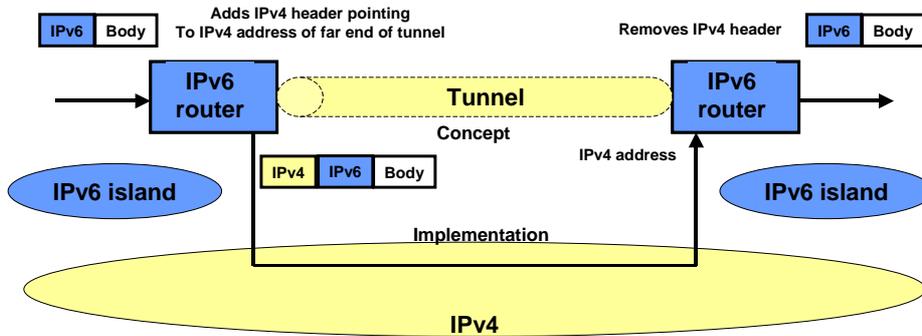
Figure 5: Tunnelling

Tunnelling is satisfactory as a small scale short term expedient but not as a larger scale solution. Tunnels require hands-on management and this is costly and complex.

6   ADDRESS EMBEDDING

IPv4 addresses can be embedded within an IPv6 address. Part of the IPv6 address space is reserved for this purpose. This would enable an IPv6 only network to route traffic to an IPv4 address. In practice, the routers would probably send the packets as soon as possible to a router on an IPv4 network where the IPv6 header would be replaced with an IPv4 header. This technique may be used late in the migration when only a small amount of IPv4-only equipment is left.

6.1   Application-Level Gateways (ALGs)

Application-Level Gateways are typically proxy systems at the border between two networks, specific to a network service. The gateway is connected to both networks and relays traffic between them. For example, a proxy for web browsing could accept traffic from clients on an IPv4 network, forward them to an IPv6 server and pass the results back to those IPv4 browsers who otherwise would have been unable to contact that web server because it only had an IPv6 address. These solutions do not scale well and can have substantial operating costs. They are also inflexible because discrete gateways are needed for each distinct network service: email, web, VoIP and so on.

6.2   Conclusion

While there are various techniques for accommodating the hybrid world of IPv4 and IPv6, the main approach to the migration to IPv6 should be based on the introduction of dual stack operation, until such time as the availablity of IPv6 is so widespread that the support of IPv4 can be discontinued. There will be a long period of co-existence and it is unclear whether IPv4 will cease to be used or will continue indefinitely alongside IPv6.

7   MIGRATION IN DIFFERENT PARTS OF THE INTERNET

7.1   Migration in the backbone

The backbone of the Internet is the main international transit structure that ISPs connect to. This core infrastructure needs to support IPv6 before migration to IPv6 can start seriously and this means that the backbone routers will need to start to operate in dual stack mode.

Without these developments ISPs will not be able to start to use IPv6 other than between "closed user groups" where they provide all their own resolution facilities and use tunnels across the backbone. Thus adding IPv6 to the backbone is the starting step.

As far as we are aware, most of the major ITPs are IPv6 ready but may need to configure or upgrade some management equipment. The core routers are transparent to IPv4 and IPv6. However there is very little IPv6 traffic up to now.

7.2   Migration at the ISPs

ISPs need to start to support IPv6 before their customers, the end users, can start to use IPv6. A small number of ISPs (eg Claranet) are already making this step.

There are two options for the ISPs:

- To use the dual stack approach so that each customer access becomes capable of supporting both IPv4 and IPv6 with the customer choosing when they wish to IPv6 (or possibly in the future their own dual stack equipment managing this choice automatically for them).

- To use just IPv6 on the customer side of the ISP but to use a NAT technique to present both IPv4 and IPv6 addresses to the public Internet.

ISPs run both customer access services and email/web hosting services and some may also support DNS servers. It is important that the ISPs start to provide connectivity for those servers that they run themselves and for customers who run their own such servers at a relatively early stage of the migration to IPv6. The support of IPv6 for the majority of customers who are users rather than hosts can follow later.

Few of the servers used for the provision of information and email services currently offer access using IPv6.

7.3   Migration in the Telecommunication Company access systems

Many ISPs do not have their own physical access to the customer. Hence they use either local loop unbundling or bitstream services from the incumbent:

- With local loop unbundling, the ISP controls the DSLAM equipment used on the line but with bitstream the incumbent owns the equipment and determines what will be used.

- With bitstream services, the incumbent may also provide some authentication or access control, and may provide some IP-level backhaul and this would need to support IPv6 unless IPv6 could be carried in IPv4 tunnels.

Although in theory the access systems should be transparent to whether IPv4 or IPv6 are used by the ISP, in practice they may not be transparent, and even if they are believed to be transparent, it may be necessary to do some testing to confirm this in practice since there may be features or settings that affect the transparency.

Of the major Telecommunication Companies that provide access to the Internet, ie BT, Virgin Media and Cable and Wireless, none is yet offering an IPv6 based access service and they are probably 1-2 years away from doing so, but BT is running some trials and pilots and most of its equipment is capable of being upgraded without needing to be totally replaced.

The net result is that there is very little traffic using IPv6 at present. An assessment of the proportion of IPv6 traffic ratio in major European IXPs shows that in practice there is typically less than 0.5% of the total traffic (e.g. statistics from AMS-IX show and annual average of: 99,8 % of IPv4 traffic compared to 0,2% of IPv6, Source: http://www.ams-ix.net/technical/stats/sflow/?type=ether).

7.4   Migration in DNS

DNS is the hierarchical distributed database that translates domain names (eg "ero.dk") into an IP addresses and is an essential component of the operation of the Internet since most applications such as email and web-browsing work with domain names. DNS servers will need to receive and respond to queries over IPv6. This could be done incrementally as IPv6 becomes available at each location where DNS servers are installed. There will also be a need for DNS servers to publish IPv6 contact data: the IPv6 address of a web server for example. This can and should be done irrespective of whether the DNS server has an IPv6 address or not. DNS servers will also need to receive and respond to queries over IPv6. This could be done incrementally as IPv6 becomes available at each location where DNS servers are installed. At present very few DNS servers have IPv6 connectivity.

The hierarchy of DNS is:

- **Root servers**: There are 13 logical root servers but over 150 physical servers since some are replicated at different locations. The current situation is that 8 of the 13 servers have IPv6 addresses that are published in the root. Although most of the others have IPv6 addresses, these cannot be easily added to the root zone because of technical constraints on the size of conventional DNS responses. In effect well over 75% of the physical root servers can handle queries and responses over IPv6.

- **Top Level Domains** (TLDs): There are many TLDs including both the generic TLDs such as .com .org .biz and the country TLDs such as .dk. These servers, together with any second level servers under country TLDs (eg .co.dk) are in practice the most important and heavily used part of DNS. **It is highly desirable that up to date information should be collected and published on the IPv6 readiness of all these servers.**

Although the core infrastructure DNS servers probably have reasonably good IPv6 connectivity, this does not present a true or complete picture. Very few of the second level domain name servers have IPv6 connectivity. There are many million name servers handling delegations for European domain names. Only a small number have IPv6 addresses.

7.5   Migration in other servers, email, web

Internet "services" such as email and the world wide web are run using servers. These servers may be run by ISPs or by larger customers, eg many larger companies may run their own email servers whereas smaller ones use hosting services from ISPs.

Where ISPs start to offer IPv6, they would be likely to incorporate IPv6 into their hosting services so that any content uploaded to their services by customers becomes accessible with both IPv4 and IPv6. The domain names that they register for customers would also have both IPv4 and IPv6 addresses added to the DNS. Thus the migration to IPv6 should be invisible in terms of content hosting for users of ISP hosting services.

Larger organisations (including public institutions) that use their own email/web hosting facilities will have to introduce their own dual stack arrangements.

Migration of these servers to IPv6 is an important early part of the migration but not as important as DNS.

7.6   Migration at the customer networks

Customer networks (subnets) are normally connected to the Internet via an xDSL or cable router, which includes a NAT so that the customer equipment behind the router uses private addresses.

The current situation is that almost all these routers support IPv4 only but there are a few, mostly from Japan, that support IPv6. (e.g. Amazon sells only one router that supports IPv6)

Microsoft has an article encouraging the support of IPv6 in home routers:

- http://www.microsoft.com/whdc/device/network/IPv6_IGD.mspx

and Microsoft's IPv6 support information is available on:

- http://technet.microsoft.com/en-gb/network/bb530961.aspx.

The IETF has also developed Teredo, which is an IPv6 transition technology that allows IPv6 connectivity across the IPv4 Internet between hosts that are located behind network address translators (NATs).

When ISPs start to support IPv6, vendors of home routers are likely to start including IPv6 functionality.

How home routers will support IPv6 is not yet clear. There are essentially two options:

- Use dual stack with similar functionality to IPv4 so that the management software does not need to be altered significantly. This would mean that IPv6 would operate with a NAT and this in turn means that some of the advantages claimed for IPv6 will not be realised.

- Operate IPv6 differently without a NAT so that users have more potential to benefit from permanently assigned public IPv6 addresses and can take greater advantage of the new features in IPv6. This approach, however, means that new management software will be needed and the setup of the router may be more complicated. In addition, if NAT is not used then the home becomes more vulnerable and separate firewalls may be needed.

7.7 Migration of applications and software

For most application and server-side software, the introduction of IPv6 will be invisible. It will perform DNS lookups to get the address of some resource, say a web server or a client. This could return IPv4 and IPv6 addresses. Most application software can already accommodate that. Sometimes there may be a configuration setting to choose IPv6 over IPv4 or vice versa.

Badly written or very old software that assumes IP addresses are only 32 bits long will need to be upgraded or replaced. Such software will fail if presented with a 128-bit IPv6 address. One challenge for an organisation introducing IPv6 will be to conduct an audit to identify legacy software that cannot handle IPv6 and then decide what to do about it. In principle, there will be a small administrative and management overhead to ensure most software on servers and desktop or laptop systems are able to use IPv6. This is comparable to the effort that was needed for the Y2K problem, but on a smaller scale because most current applications and systems software already supports IPv6.

Perhaps the biggest challenge for an IPv6 migration will be security considerations. There is widespread use of access control lists (ACLs) to determine how data is routed and which devices get access to resources. These ACLs tend to contain IPv4 addresses. They will need to be reviewed so that "trusted" IPv6 addresses get added and to ensure there are no false positives or negatives on the ACL: ie the resource is only available to trusted users with acceptable IPv4 or IPv6 addresses. Certificates and SSL are widely used to secure connections. These often depend on hostname to address mappings. New certificates should take account of any IPv6 specific names and addresses.

7.8 Timeline

The timeline for the migration path would then appear as shown in figure 6.
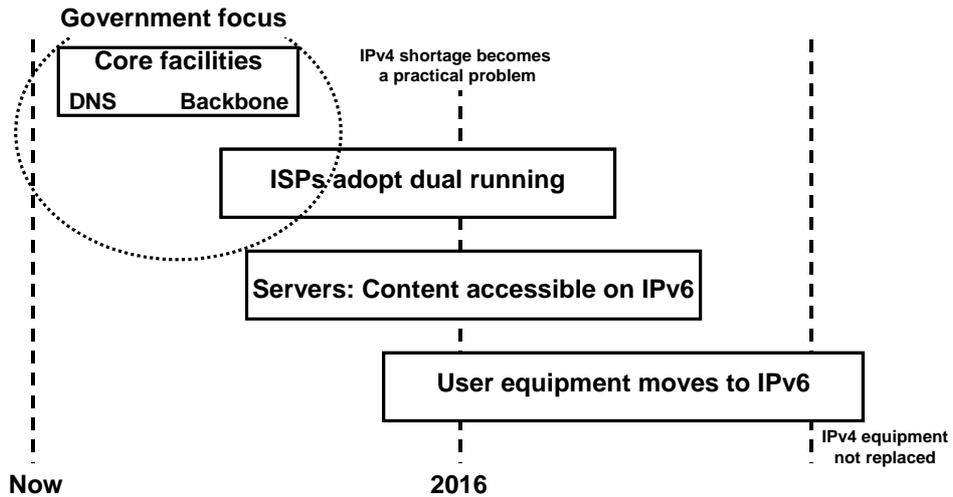
Figure 6: Timeline for the migration path

It is important however to understand that the migration process will not be a simple sequential number of coordinated steps. Many different parties will each be taking their own steps in an uncoordinated manner, but overall the sequence will be:

- backbone and DNS
- ISPs for email and web servers
- Retail customer access
- Customer equipment.

7.9   The migration path

The following diagrams attempt to give a picture of how migration may occur. IPv6 is shown in blue and IPv4 in yellow. The existence of a colour indicates that the protocol is supported and the strength of the colour indicates the volume of traffic using that protocol.

Figure 7 shows the all IPv4 Internet.
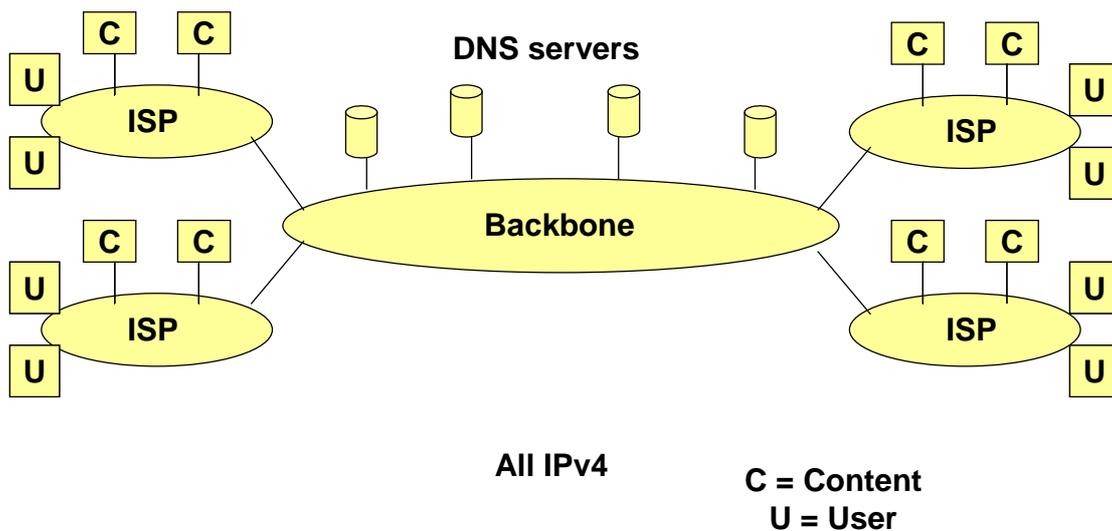
Figure 7: All IPv4 Internet

Figure 8 shows IPv6 readiness in the backbone and DNS servers.
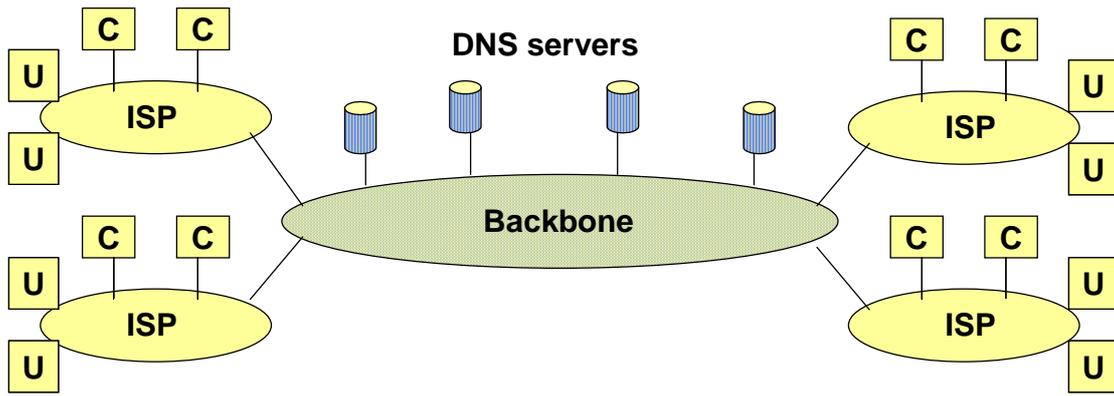
Core readiness - DNS and backbone

Figure 8: IPv6 readiness in the backbone and DNS servers

Figure 9 shows early ISPs supporting IPv6 especially for hosting email and content.
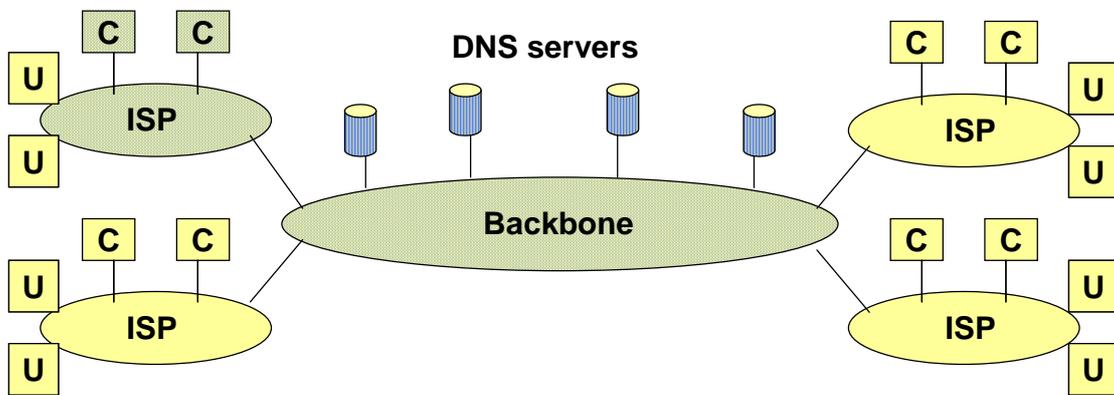
Early ISPs go dual mode and add IPv6 access to hosted content

Figure 9: Early ISPs supporting IPv6

Figure 10 shows most other ISPs following although traffic levels are still low.
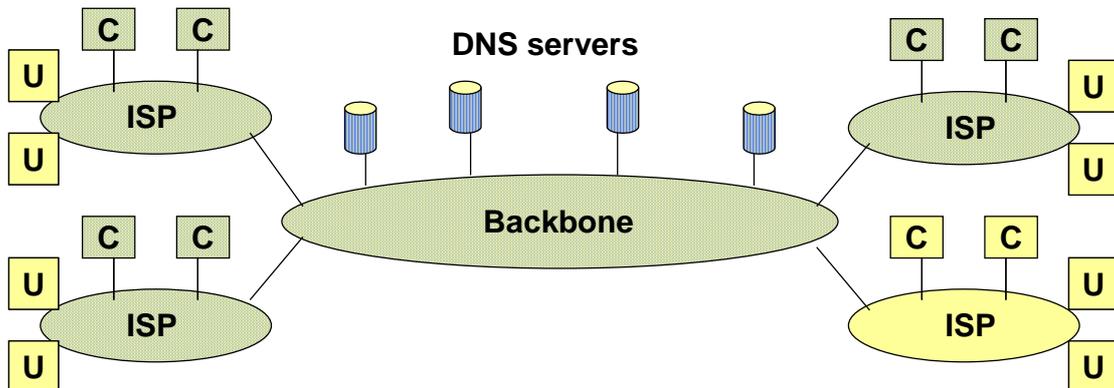
Most other ISPs follow, IPv6 traffic still low

Figure 10: Most other ISPs follow

Figure 11 shows users starting to use IPv6 wherever possible.
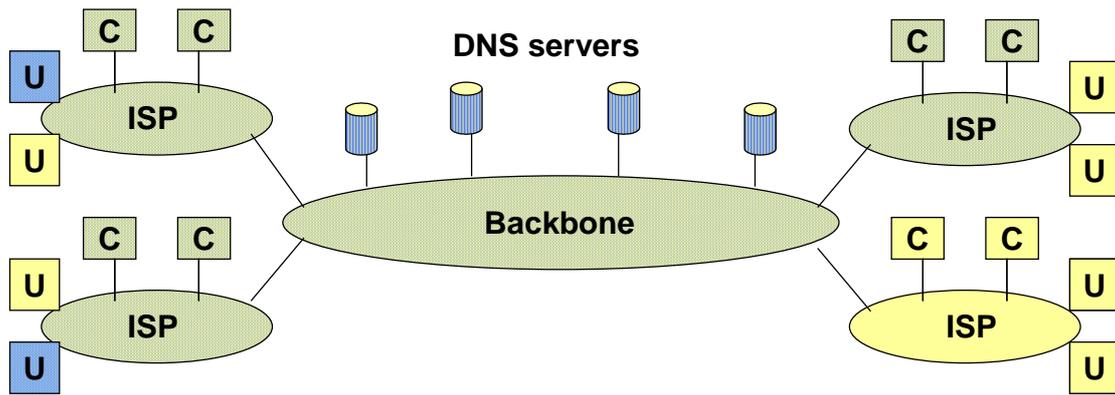
User migration starts, users use IPv6 where possible

Figure 11: Users start to use IPv6 wherever possible

Figure 12 shows IPv6 traffic growing.
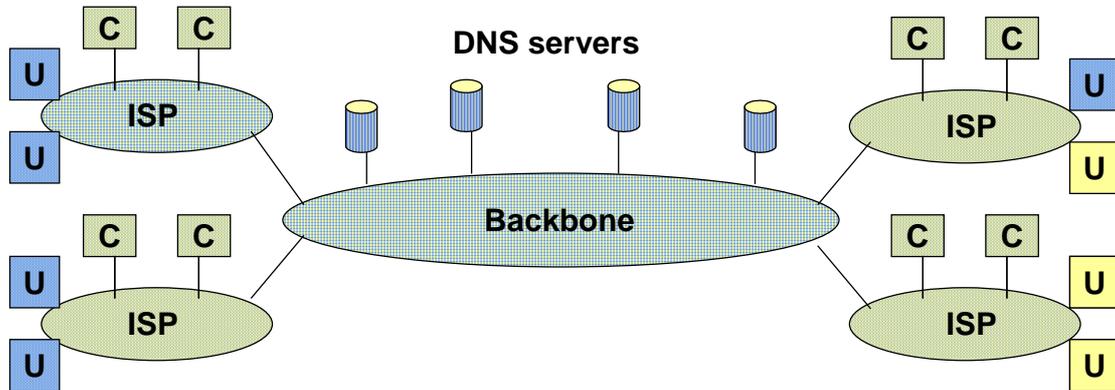
User migration progresses, IPv6 traffic grows

Figure 12: IPv6 traffic grows

Figure 13 shows most users using IPv6.
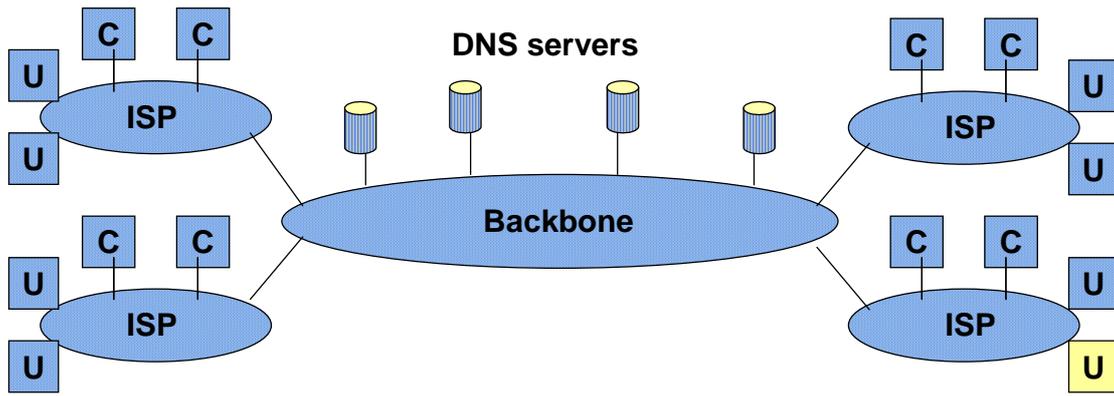
Most users and traffic are now IPv6

Figure 13: Most users use IPv6

Figure 14 shows some ISPs ceasing to support IPv4.
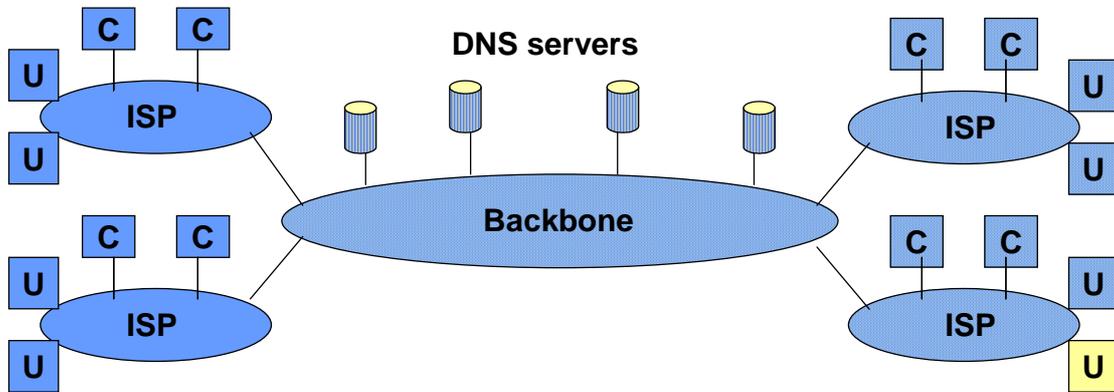
Some ISPs cease to support IPv4

Figure 14: Some ISPs cease to support IPv4

Figure 15 shows the IPv6 based Internet after support of IPv4 is withdrawn.
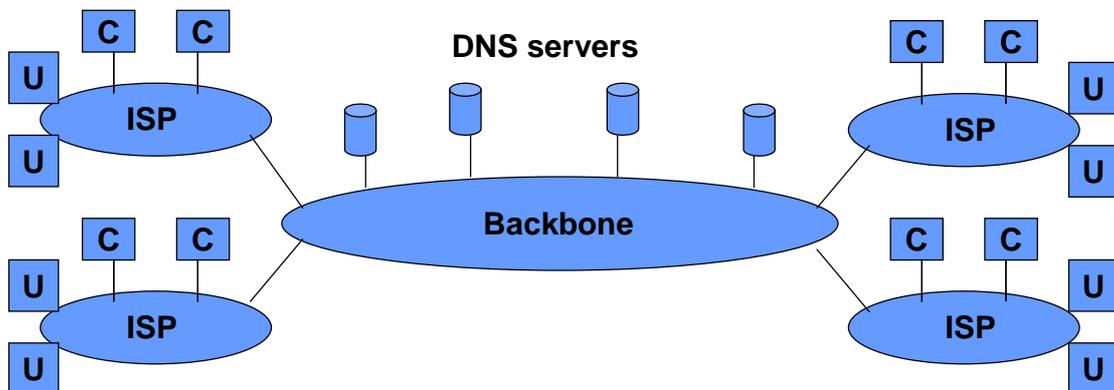
Support for IPv4 is withdrawn

Figure 15: Support of IPv4 is withdrawn

8   THE COSTS OF MIGRATION TO IPV6

8.1   Equipment

The costs of adding dual stack capability to the Internet backbone routers and to the main servers, eg DNS, email and web servers, is likely to be relatively low. Software to support the IPv6 stack is usually bundled in the core operating system alongside the IPv4 stack. Most UNIX and Linux systems have had this dual stack capability for over a decade. Sometimes an additional charge and/or software upgrade is necessary to add IPv6 capabilities to routers and switches. The additional costs in terms of network equipment may be less than 5%. The working life of this sort of equipment is relatively short (3-5 years) and so dual stack equipment can be bought at the next upgrade if it has not already been procured and deployed.

The fact that IPv4 and IPv6 packets can share the same transmission path means that the backbone will not need additional transmission capacity and that the shift in the proportion of traffic types will not require a continual re-dimensioning of the backbone.

Home router equipment may have a longer life than network equipment. Churn is promoted by offers for higher speed broadband that include new routers but there is a wide range of lifetimes of equipment depending on whether or not the users require higher speed services. The need for speeds in excess of 2 Mbit/s is largely driven by interest in video content and given the high penetration of satellite, digital TV broadcasting and cable in many countries this demand is somewhat uncertain. The cost of equipment that supports IPv6 may initially be higher but as volumes grow the cost differences are likely to be minimal and IPv6 will eventually be included in all new routers sold. At present, a DSL router for home or small office use that supports IPv6 is typically £300-500 compared to £25-50 for one that does not. This is not because IPv6 support is expensive. Since there's no mass-market demand, IPv6 does not yet benefit from the economies of scale that commodity hardware enjoys.

PC operating systems such as Windows have frequently issued upgrades and so capabilities can be added or updated automatically. Windows XP and Vista upwards include the basic IPv6 stack as do Macintosh and Linux.

Existing software applications should not be affected since they are normally built on top of another protocol such as TCP or UDP that functions above the IP layer.

8.2   Compatibility and Interworking

Although there are standards for IPv6 this does not ensure that all IPv6 equipment will immediately be compatible. There may be differences in options and other issues where there will be a process of learning before a high level of compatibility and interworking is achieved without further effort.

Compatibility and interworking can be promoted through testing.

These activities are an additional cost to the industry.

With assistance from the European Commission's eEurope programme, ETSI has developed a comprehensive test specification for the IPv6. This specification includes Test Purposes and Test Cases for both conformance and interoperability tests.

Each of the IETF specifications associated with core IPv6 have been analysed to derive over 1000 requirements which characterize IPv6 systems. These requirements have been classified and catalogued.

A valuable role for the Commission would be to promote a Europe-wide marking to indicate that equipment and software supports IPv6. The use of the mark should be based on sufficient practical testing for the mark to be meaningful.

The IPv6 Forum has introduced a mark but it is little used to date. One option is to promote the use of this mark, and this may be better than introducing a different mark.

8.3   Operation

The additional costs of IPv6 operation are likely to be a higher proportion than the additional costs of equipment. The operational costs include:

- training of technicians
- training of customer support staff
- establishment of new procedures for IPv6

In the earlier phases there will be a skill shortage that will increase the rates for staff with the necessary skills and in turn increase the additional costs further. The EC 6Deploy project to provide training for technicians will help to address this shortage.

The operating cost element of ISPs could increase by say 15% for a few years during the main migration phase.

9   ASSESSING THE INCENTIVES FOR THE PLAYERS

9.1   Advantages of IPv6

To assess the incentives for the players it is necessary to understand the claimed advantages of IPv6.

Advocates of IPv6 such as the IPv6 Forum have attempted to draw attention to the advantages of IPv6 over IPv4. They claim that as well as providing in effect unlimited quantities of addresses so that NAT is no longer needed and every device can have its own permanently assigned address, IPv6 offers better security and better support of "plug and play" setup. These claims typically present examples of highly automated houses with remote mobile control systems. They also claim that NAT is contrary to the fundamental Internet end-to-end principle and that IPv6 will allow this paradigm to be recovered.

IPv6 will solve the address shortage problem but the other features and examples can be provided on IPv4 and IPv4 could be used equally well to support the digital home and digital automation. Good security can also be achieved on IPv4-based systems. Therefore the advantages of IPv6 are not unique to IPv6 and do not provide a strong incentive to migrate.

A further potentially important factor is that views differ on the issue of NAT. Advocates of IPv6 argue that IPv6 will make NAT redundant but some users see NAT as device that increases security and would not cease to use NAT when they migrate to IPv6. Thus some of the claimed advantages of IPv6 may not be realised for other reasons. This issue is especially uncertain at this stage because there is to date little experience of the best way to manage IPv6 operation in the home.

The conclusion is that the advantages of IPv6 are unlikely to be sufficient in themselves to motivate users, other than specialist users, to migrate in order to obtain greater functionality. Consequently migration is likely to be driven mainly by the motivation to avoid the difficulties of IPv4 shortages.

Migration to IPv6 may be driven by a wish to avoid problems in the future, rather than a wish to achieve enhanced functionality

9.2   Backbone connectivity and DNS

This area includes:

- Backbone connectivity
- TLD registries and servers
- Internet exchanges.

Although the operators of the backbone and the upper level DNS servers do not have a direct short term commercial incentive to introduce dual stack operation, they are likely to introduce it when it is needed as part of their long term commitment to the Internet. Some have already done this.

This appears therefore to be a relatively low risk area, however we recommend that one of the top international bodies could set a deadline for supporting IPv6 in these parts of the Internet and publish a list of all the main players and the dates when they migrate. At a regional level, each RIR could undertake this task and if necessary the Commission could propose this to RIPE. The publication of information is generally an effective tool to increase peer pressure.

9.3   ISPs and email and web servers

ISPs will have two different commercial incentives to migrate to IPv6 and they do not necessarily have to change all their systems at the same time.

- Where ISPs run servers (email, web) for their own and their customers' services, there will start to be commercial pressure from their users to migrate to dual stack operation so that the servers can be used with IPv6.

- Where ISPs provide access to customers, some customers will start to ask for IPv6 access and they will also be affected by the increasing shortage of IPv4 addresses because they will no longer be able to obtain additional allocations.

Thus there should be sufficient natural commercial pressure for ISPs to migrate under commercial forces. However we think that it would be useful to increase the commercial pressure by the publication of national tables of which ISPs support IPv6 and to provide this information separately for:

- Support of IPv6 on servers (email and web)
- Support of IPv6 on access systems.

ISPs are not the only organisations that run servers. Many larger organisations run their own servers and it is important that these servers and the access systems that they use are made compatible with IPv6. Governments themselves run many such servers for information, tax, etc. and they also need to implement IPv6.

**Few of the servers used for the provision of information and email services
currently offer access using IPv6.**

9.4   Telecommunication Companies – access

Telecommunication companies' access is a potentially important bottleneck that needs further research. This is especially the case where there is a drive to upgrade and extend broadband access and so there is likely to be significant further investment. The forms of access used need testing to ensure that they support IPv6 and need adapting if they do not, otherwise they will form a serious bottleneck to the migration to IPv6.

Of the major telecommunication companies that provide access to the Internet, ie BT, Virgin Media, and Cable and Wireless, none is yet offering an IPv6 based access service and it is unlikely that such a service will be available widely before mid 2010.

The net result is that there is very little traffic (<1%) using IPv6 at present.

**A high priority is to involve the main Telecommunication Companies
that provide access in discussions with the rest of
the Internet industry over the implementation of IPv6 and including systematic testing
to identify and eliminate practical bottlenecks**

---

10   ACTIONS BEING TAKEN

10.1   IPv6 Forum

The IPv6 Forum, which is a world-wide consortium of Internet vendors aiming to promote IPv6, has been raising awareness of the need to migrate to IPv6 for several years.

See http://www.ipv6forum.com/.

10.2   OECD

The OECD published a report in 2007 on "Economic Considerations in the Management of IPv4 and in the Deployment of IPv6" where it recommended that Governments should:

- Work with the private sector and other stakeholders to increase education and awareness and reduce bottlenecks
- Demonstrate government commitment to adoption of IPv6
- Pursue international co-operation and monitoring IPv6 deployment

Our proposals are in line with these recommendations.

The OECD has recently started work on a methodology to track implementation of IPv6.

10.3   Actions by the European Commission

In 2008, the European Commission issued a communication to the European Parliament, the Council and others on "Advancing the Internet: Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe".

The Action Plan set the objective that IPv6 should be widely implemented by 2010, with at least "25% of users able to connect to the IPv6 Internet and to access their most important content and service providers without noticing a major difference compared to IPv4".

10.4   Actions by other governments

A number of governments are taking action on IPv6.

In August 2005, the Office of Management and Budget in the USA Government established the goal of enabling all Federal government agency network backbones to support the next generation of the Internet Protocol Version 6 (IPv6) by 30 June 2008.

In 2007 the Dutch Government financed a study on the Practical Implications of IPv6 and identified the problems of there being no hard deadline for implementation and a lack of skills and sample implementations. It suggested that the Government could create greater expertise and awareness by including IPv6 in its own procurements.

The Japanese government has established a Task Force on IPv6 to synchronise and coordinate activities, solve problems and promote awareness.

11   PROPOSED ACTIONS

11.1   Proposed actions

What do Governments and regulators in Europe need to do to ensure that the migration to IPv6 is smooth and that it does not disadvantage the Internet community and users?

The migration path is complex with some steps such as the method of supporting IPv6 in home networks not yet clear. In these circumstances it would be inappropriate to consider any regulatory intervention. There is also some uncertainly about the timing for the migration.

We consider that the primary objective for Governments and regulators should be to ensure that the ISPs are able to introduce IPv6 and use it when they need to under market forces. This means working from the centre outwards.

The market forces will be demand for the features of the new protocol (whether essential or not and to whatever degree promoted to the public) and increasing shortages of IPv4 addresses. It is the ISPs that will be the main controllers of the speed of the migration.

In order to provide this freedom for a market led solution, the Governments and regulators need to ensure that:

- The main backbone and DNS servers support IPv6 and that any initial teething troubles are resolved

- The access systems run predominantly by BT and Virgin do not inhibit the adoption of IPv6 by ISPs or subscribers

- All parties have adequate up-to-date information and a forum where issues can be raised, discussed and resolved

- There are adequate training facilities for the operational and support staff

- Vendors are able easily to undertake conformance and interworking testing

- Target dates and deadlines are established and lists organisations and their IPv6 readiness are compiled and published.

In terms of enabling a market led migration, Governments and regulators should set a timeline for the backbone and their part of DNS to be ready for IPv6. The suggested date is March 2012.

11.2   Role of the academic community

The Internet world has benefited greatly from the contributions made by the academic community. Some UK universities have a high profile in IPv6 developments and research, though this activity is considered experimental and therefore somewhat removed from the responsibilities of operating a production network. However it is not clear how much traffic these servers receive over IPv6.

Possible actions by the academic community are:

- To migrate to IPv6 at the earliest practical opportunity as an operational system to gain operational experience as opposed to conducting experimental research;

- To migrate the networks in schools to IPv6.

Both these actions could be valuable at some stage. They focus on a special segment of the market and operate from a different perspective to our main recommendation of working from the centre outwards to enable market forces to lead to IPv6 implementation. They will add value but not necessarily stimulate a market-led migration.

11.3   Role of Government procurement

The Government could require all its new IT procurements to include IPv6 and use certain procurements as pilot programmes. This is an approach used in the past to promote other technologies such as OSI, but the results were disappointing. The difficulty is that it diverts attention from the main objective of the procurement, which can often be difficult enough to achieve on its own.

We recommend that future procurements should include dual stack software capability wherever possible as a preparation for future migration but that the timing of the actual migration should remain for the programme managers to decide. This is a "low interference" approach.

The rationale is the same as for the use of IPv6 in the academic community because adoption by one market sector does not necessarily help the objectives of enabling market led migration.

The one area where the Government should take action is to ensure that where it runs web servers for public access to its own information these web servers are adapted to support dual stack and access via IPv6 within the next year.

12   CONCLUSIONS

The main conclusions of this study are as follows:

a)   IPv4 allocations will run out around mid 2012. Measures to make better use of existing allocations will help and may add the equivalent of another 4 years of growth.

b)   Where IPv6 is not introduced and IPv4 shortages occur, the existing Internet will continue to run but new users and new content providers will either be unable to gain access to the Internet or will have to pay more for access or accept lower quality access as a result of increased sharing of IPv4 addresses. Thus the Internet is not heading for a brick wall but for steadily increasing difficulties unless the implementation of IPv6 makes adequate progress.

c)   IPv6 offers more than a huge increase in address capacity and its other features are generally beneficial, however they can all be implemented in other ways based on IPv4. Therefore the migration to IPv6 will be driven much more by the need to avoid problems than by the attraction of these other features.

d)   Although there has been awareness of the problem for around a decade, and manufacturers and developers of operating systems have created the capability to support IPv6, there is very little effective implementation so far and negligible IPv6 traffic.

e)   The operators that provide the main connectivity backbone of the Internet are in the process of introducing IPv6.

f)   Part of the top level of the DNS already supports IPv6 but much of the rest of the DNS needs to have IPv6 added.

g)   Few of the servers used for the provision of information and email services currently offer access using IPv6.

h)   Few if any the major telecommunication companies that provide access to the Internet is yet offering an IPv6 based access service and they are probably 1-2 years away from doing so, but some are running trials and pilots and much of the equipment is capable of being upgraded without needing to be totally replaced.

i)   Various international bodies such as the OECD and the European Commission and national governments are starting to address the migration issue.

We recommend that:

1) Governments and regulators should encourage that the essential parts of the Internet in their countries are adapted to support IPv6 in time for the rest of the migration to proceed under normal commercial arrangements and market forces. We are not advocating major changes to Government procurement because we doubt if this would have sufficient impact although it would be of some benefit.

2) Governments and Regulators should make public content and services available on dual stack IPv4/IPv6 servers.

3) Governments and regulators should set specific but realistic targets for achieving IPv6 support in the main parts of the Internet infrastructure in their countries.

4) The ECO Internet website should publish progress on IPv6 migration.

ANNEX: INFORMATION ON INDIVIDUAL COUNTRIES

This is based on the PT2/TRIS IPv6 survey and covers the following countries:

• Bulgaria	• Malta
• Denmark	• Norway
• Finland	• Portugal
• France	• Spain
• Greece	• Sweden
• Ireland	• Switzerland
• Latvia	• UK
• Lithuania	

The following questions were asked:

1. Could you please describe public incentives related to IPv6 deployment in your country?
2. How active your market is in relation to IPv6 deployment (e.c. forums, projects)?
3. What are regulator's role and incentives encouraging IPv6 deployment in your country?

BULGARIA

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

As a result of an inquiry sent to all 23 operators, providers of voice telephony and carriers, we
have received the following information:

1. actual usage of IPv6 - 1 operator;
2. available IPv6 addresses - 2 operators;

There are technological possibilities of IPv6 usage. IPv6 addresses are available upon client's request.

3. no plans of usage – 2 operators

One of them buys only equipment that allows easy migration to IPv6.

Unfortunately the received data do not allow to make any conclusions about public incentives in Bulgaria. The question about IPv6 usage will be added to the annual questionnaires, which CRC sends to operators and internet providers. By this we hope to acquire more information.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

In March 2008, Southeast Europe's first lab for training and research in IPv6 was opened by Bulgarian State Agency for ICT - DAITS in collaboration with Cisco. The lab's networking and communication equipment was donated by Cisco.

Located in Sofia, this is Europe's second IPv6 lab, after the one operated by RENATER, the French national research network in Paris. The laboratories are interconnected to enable sharing of resources and access.

The objective of the lab is to provide an open environment for validating solutions, network setups and applications built on IPv6. Internet experts, including academics, government administrators and telecom specialists can be trained, both on-site and through virtual access, on innovative ICT solutions relating to the adoption of IPv6.

The laboratory is managed by the Bulgarian Research and Education Network (BREN) in cooperation with DAITS. BREN's specialist team is already participating in the 6DEPLOY project funded by European Union's Seventh Framework Program, which involves 13 institutions from all over the world and aims at disseminating knowledge about IPv6 and supporting its deployment.

Through this laboratory more than 100 technical experts from English-speaking countries in Africa were trained. The virtual training was carried out in Nairobi, Kenya. The training was aimed toward improving the capacity of IT

managers in Africa in deployment of IPv6 networks and was offered by Africa Network Information Center (AfriNIC) with support from the European Union through the 6DEPLOY initiative, which promotes IPv6 awareness and training in developing countries.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

Bulgarian State Agency for ICT – DAITS is responsible for all initiatives and projects in the area of ICT.

DENMARK

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

Complying with the international recommendations the Danish government is taking the lead in the promotion of IPv6 in Denmark.

This includes drawing up a national strategy and action plan. There has been a public hearing, which will result in a final strategy and action plan, ready to be rolled out.

The draft strategy plan aims to establish a public private partnership that will ensure the transition from IPv4 to IPv6, and it includes a number of strategic themes that will ensure the continued development and utilisation of the Internet which is essential to the potential growth and innovation of society.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

 As mentioned above the Danish National IT- and Telecom Agency plans to establish a public private partnership with the participation of all relevant actors within the area in order to ensure seamless transition from IPv4 to IPv6.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

DK-Hostmaster (the Danish RIR) supports IPv6 in their systems. TDC (PSTN incumbent and one of the major Danish ISPs) has introduced IPv6 based solutions both within TDC and to business customers. IPv6 is supported in all TDC routers, native IPv6 connectivity is offered, full IPv6 service is expected to be available in 2010 and onwards as all tunnel customers will be migrated to native IPv6.

In Denmark the public procurement strategy as a general rule calls for IPv6 enabled solutions, except where this is absolutely impossible, and in the agreement with DK-Hostmaster (the Danish RIR) it is stated that they must (continue to) support IPv6.

FRANCE

The G6, an association providing technical expertise and training on IPv6 has been formally established in 2001 but finds its roots in 1995 and was the first-ever IPv6 test network set up. In 2007, the G6 took over and integrated the IPv6 Task Force France (TFF), an IPv6 dissemination group, which has been established in France as early as 2002 following an European Commission directive (establishment of the European Task Force and call for establishment of national TFs across Europe). The G6/TFF is run by voluntary experts coming from a large range of entities: academia, research, private sector… The French IPV6 Task Force has organised regular meetings and has participated to numerous international conferences over the last years and again recently. The G6 has also issued an IPV6 contest: winners will be designated in July 2009.

In October 2008, Eric Besson, the French "Secrétaire d'Etat chargé de la prospective, de l'évaluation des politiques publiques et du développement de l'économie numérique », in his Plan for the Développement of the Digital Economy (« Pan de développement de l'Economie Numérique / France Numérique 2012 »), decided a wide range of actions. One of these actions is dedicated to the IPV6 topic ("Introduire progressivement, à partir de 2009, la compatibilté avec IPV6 dans les marches publics") : to introduce, starting in 2009, IPV6 compatibility provisions in all public calls for tender.

More over, several large companies, SME's, and public and/or private research labs in France have contributed and are still contributing to the development of IPv6 itself, but also to operational, industrial or consumer applications based upon IPv6 in cooperative research an development projects. Those projects are coordinated at various levels, national and pan-European, like Eureka, "ITEA-2" and "Celtic", as well as at the European Commission level, with IST-FP6 and

now IST-FP77 (a non exhaustive list of projects and organizations which have contributed can be provided upon request after some effort).

Other examples include Renater, the French academic network, which is providing native IPv6 to all willing public institutions in France, and the ".fr" ccTLD (country code Top Level Domain Name) that has been offering IPV6 since 2003, which should also facilitate national deployment of IPV6.

FINLAND

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

There has been an active national IPv6 Task Force from the year 2002. There has been a lot of activities planned in the Task Force and implemented by FICORA, e.g. two IPv6 seminars and two IPv6 questionnaires. There is a small number of operators which already offer IPv6 services and in universities there is training for IPv6 and IPv6 is available in university networks. The national .fi-root is made IPv6 capable.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

At this moment some operators have IPv6 mainly in trial use; the Finnish operators seem to have still plenty of IPv4 addresses so that for that reason there seems to be no hurry in IPv4-IPv6 transition; however, in the longer run there will inevitably be new internet applications which are available only via IPv6 and for that reason it is important at least to start the transition now

There is national IPv6 task force which is chaired by Ficora; the group has more than 30 persons on the mailing list and has meetings four times per year; after discussions in the group Ficora has e.g. arranged two IPv6 seminars and two IPv6 questionnaires; the group has its own www-page in Ficora www-pages which contains documents handled in the group
http://www.ficora.fi/index/palvelut/palvelutaiheittain/standardointi/standardointiryhmat/ipv6.html
(the group has also www-page in European IPv6TF-pages which is available via IPv6)

in Finland (as also in European Commission) the idea so far has been that from the governmental side IPv6 is actively promoted but there are no regulatory requirements or financial support for the transition

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

Ficora is responsible for the .fi ccTLD. The IPv6 support for the .fi can be divided in three steps.

The first step is to provide IPv6 connectivity for the .fi root name servers. This step was taken in 2006 when we implemented the first name server "D.fi" with IPv6-addresses. Currently we are having three name servers supporting IPv6 - including one name server based on the anycast technology with more than 20 name servers worldwide.

The second step is to allow .fi domain names to use name servers with IPv6 address. This possibility was given to domain holders in May this year through an on-line management service.

The third step is to have a registration/on-line management system available via IPv6. This requires the IPv6 connnectivity for the system and also system upgrade in order to support IPv6. The upgrade is estimated to be ready Q1/2011.

GREECE

We have only one backbone network working on IPv6 protocol . it is the "Greek Research and Technology Network (GR-Net)" and you can look below what this is :

http://www.grnet.gr/default.asp?pid=32&la=2

The Greek Research and Technology Network (GR-Net) is the Greek National Academic and Research Network (NRN). It is an initiative of the General Secretariat for Research and Technology (GSRT) of the Ministry of Development, initially as part of the EPET II subprogramme of the 2nd Framework Programme of the European Union (EU). The goal of GR-Net is to provide advanced and high quality inter-networking and Internet connectivity services to both Greek Universities and Technological Educational Institutes

(TEI) in cooperation with GUnet (http://www.gunet.gr/), as well as research organizations. GR-Net is a non-commercial national backbone and includes Points of Presence (pops) in major Greek cities, where the above mentioned educational and research institutions are located. "Non-commercial" means that GR-Net provides its services with education and research, rather than commercial profit and the greater "market" in mind. From a financial point of view, profit per se is not a goal. The coverage of expenses and the future availability of the necessary capital for upgrades of the provided services are expected instead. The services provided by GR-Net include:

> a.. IP v4 connectivity
>
> b.. IP v6 connectivity
>
> c.. Multiprotocol connectivity
>
> d.. Managed and guarantied bandwidth services
>
> e.. Voice transmission
>
> f.. Still and moving image transmission
>
> g.. Tele-education and Tele-conferencing

> GR-Net is also aiming at the support of research

Also, a new task force group for IPv6 ("Hellenic Task Force for IPv6") has been created in Greece just a few monts ago. It is not a governmental organisation. its members are from the market, big companies, Universities and also from some Governmental bodies. This task force group is only at its first meetings.

IRELAND

Current IPv6 usage according to the Internet Neutral Exchange Association (INEX):
- 13 IPv6 enabled members out of 37
- Limited access from most providers
- Some test beds deployed but these are not monitored or officially supported
- If you want IPv6, you need a tunnel
- Not 'proper' IPv6

Incentives – Irish IPv6 Summit

- IPv6 summit held in January 2009
- The aim was to raise awareness in the public and private sectors about the need for IPv6 deployment and issues surrounding deployments

Portal containing information, slides and video streams from the summit to act as an ongoing resource for those promoting IPv6

Forum participation

- ▪ The Irish IPv6 Task Force was established under the auspices of the Department of Communications as a group of both public and private sector representatives seeking to promote IPv6 deployment and awareness in Ireland
- ▪ In addition, the chair of the Irish IPv6 Task Force participates in the EU IPv6 Task Force

Members also attend the RIPE IPv6 WGs

Role of the regulator and incentives for encouraging IPv6 deployments

- ▪ The Department of Communications has taken the lead in exploring incentives for deployments

Currently, ComReg maintains a watching brief, contributing to the Irish IPv6 Task Force as necessary.

LATVIA

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

The Institute of Mathematics and Computer Science, University of Latvia (IMCS UL) develops academic network in Latvia IMCS UL is the first academic organization who has realized application of IPv6 addresses in cooperation with GEANT (in 2008). IPv6 addresses are distributed to IMCS UL and from 2009 these addresses can get every academic client. Also there are some discussions about IPv6 deployment among regulator, Government and merchants.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

There are no official data, however some large electronic communications merchants (like Lattelecom) are testing IPv6 and making some projects in relation to IPv6.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

As technological neutrality is used and regulators role in relation to IPv6 is not still defined regulator is not leading any working groups or drafting IPv6 strategy. Regulator is following IPv6 development and is participating in some discussions or working groups in EU at the moment.

LITHUANIA

Only 3 Lithuanian organizations (Local Internet Registries) have IPv6 address allocations.
IPv6 is a production service in Lithuanian research and education network LITNET. Transmission currently is limited to unicast only. Public 6to4 relay is operational.

There are few areas that will require different level of upgrade for transition from IPv4 to IPv6:

- Transmission systems. Most of current transmission (SDH/DWDM) systems do not support IPv6 for management. Forklift upgrades may be required since this functionality might be highly integrated.
- IP backbones. Most ISP networks in Lithuania rely on Cisco Cat6500/7600 platform. There are few installations of GSR or Juniper M (M320/M120) series routers. No CRS or Juniper T series are present. Mere software or configuration upgrade should make these networks capable of running IPv6 in native mode.
- Aggregation/distribution level, including CPE's. The wide variety of equipment is used on this level, and it is difficult to assess actual requirements for transition to v6. It seems that forklift upgrade will be necessary in cases where equipment does not support IPv6.

Services: Strong business case will be required to facilitate services to start transition to IPv6, and lack of such business case on the other hand hinders wider deployment of the new version of IP.

MALTA

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

To date, no public incentives related to the deployment of IPv6 in Malta exist. However, the Malta Communications Authority (MCA) and Government are currently discussing a number of public incentives which could help to promote IPv6 uptake in Malta.

The MCA is a member of the IPv6 Forum. It has also participated in a number of IPv6-related summits, conferences and meetings.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

A national IPv6 Task Force was set up in 2005 so as to help stakeholders prepare for the transition to IPv6. Furthermore, an IPv6 test-bed (connected to GEANT) has been deployed, allowing interested Maltese stakeholders to connect to it and experiment with IPv6.

To date, no IPv6 services are publicly available. However, some large stakeholders are testing IPv6. Indeed, certain service providers might offer trial IPv6 services to their customers in the near future. To date, the major obstacle for Maltese stakeholders has been the availability of IPv6 applications and content.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

The MCA chairs the Maltese IPv6 Task Force in Malta. It is in constant communication with Maltese stakeholders, discussing their concerns and foreseeable issues with regards to the deployment of IPv6 in Malta. The MCA is currently drafting an IPv6 strategy for Malta - setting out a number of IPv6-related objectives that need to be achieved within a stipulated timeframe. The MCA has, and continues, to deliver lectures on IPv6 thus helping to raise IPv6 awareness and disseminate IPv6 information. The MCA will, in the near future, be evaluating incentives (either offered by itself or by other stakeholders) which could serve to encourage the deployment of IPv6 in Malta.

NORWAY

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

It has not been established any formal public incentives related to IPv6 in Norway

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

In Norway, it is mainly UNINETT (network operator for universities and research organizations) who has been active through participation in EU research programs and also had national field trials with IPv6.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

NPT participates in international fora such as RIPE and ICANN in order to coordinate and facilitate resource allocation for IPv6 deployment. In addition, NPT provides relevant information to market players about IPv6 related matters. This topic is also regularly discussed in our permanent Internet working group with interested partners.

PORTUGAL

The Portuguese IPv6 Task-Force Mailing List includes staff from many of the most relevant organizations (e.g. ISPs, .pt TLP registry – FCCN). The TF has been created in 2004 and since then has been actively collecting and distributing information related to IPv6 technologies and activities.

FCCN, the Portuguese Research and Education Network has been an active promoter of IPv6 since the late 90s. The main activities are related to the promotion of the adoption of IPv6 in a timely manner inside all higher education and R&D institutions. The backbone of the network has been operated in dual-stack mode (IPv4 and IPv6) since 2003. During 2008 significant investments have been done to enable dual-stack operation of the following services in these institutions: DNS servers, mail servers and Web servers. Training and Workshops have been organized in the past.

In compliance with RFC1886, the portuguese ccTLD .pt registry service has been adapted to allow the definition of DNS domains supported by IPv6 servers.

The Portuguese Internet Exchange (GigaPix), also managed by FCCN, is ready to leverage interest from its members about IPv6 technology and usage. There is also a test infrastructure that enables anyone to test if their e-mail service over IPv6 is working. auto@apenasipv6.fccn.pt returns an automatic e-mail to any sender on the IPv6 Internet.

A webserver which is only accessible over IPv6 is also available under www.apenasipv6.fccn.pt.

For more information please consult the following site:
http://www.fccn.pt/index.php?module=pagemaster&PAGE_user_op=view_page&PAGE_id=465&MMN_position=166:159.

SPAIN

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

The Spanish IPv6 Task Force was established in 2002 to study the future of IPv6 technology and the actions to take in relation to the market requirements and to promote migration to IPv6. The Ministry of Industry, Tourism and Trade (MITYC, in Spanish) is a member of this IPv6 TF.

Since 2003, RedIRIS (the Spanish academic and research network that provides advanced communication services to the scientific community and national universities) offers a backbone able to support IPv4 and IPv6 in a dual-stack configuration. RedIRIS has over 350 affiliated institutions, mainly universities and public research centres.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

See point 1. Many meetings and summits have been celebrated in Spain, including several Global IPv6 Summits.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

The Ministry of Industry, Tourism and Trade has launched many R&D Programmes that include IPv6 as part of several topics related to security, communication systems and information society services.

SWEDEN

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

We i.e the Swedish Post and Telecom Agency work in different ways to foster early IPv6 deployment and use. Inter alia we plan to make our web site accessible via IPv4 as well as IPv6 through dual stack technology.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

The Swedish University Network, SUNET; has full IPv6 compliant network connecting all universities and student's lodgings.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

The ccTLD for Sweden has made several investigations in Sweden regarding the preparedness for IPv6, the current use of IPv6, impediments for IPv6 deployment etc.

The Governmental E-delegation has recently compiled a policy document that also expresses a wish that public content should be available also via IPv6 connection. The delegation is obliged to report the progress of the policy development to the Ministry of Finance.

SWITZERLAND

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

The Swiss IPv6 Task Force has been established to group all the different persons active in the IPv6 field in Switzerland and to leverage the work done in the EC IPv6 Task Force. The common goal is to identify the opportunities for the IPv6 technology and to encourage its deployment in Switzerland.

Since June 2004, SWITCH (the Swiss company who manage the internet addresses and create, promote and offer the necessary basis for the effective use of modern methods of telecomputing in teaching and research in Switzerland), offers a SWITCHlambda <http://www.switch.ch/network/projects/switchlambda/> backbone fully "dual-stacked", supporting IPv4 and IPv6 in parallel over the same links and using the same routers. Existing SWITCH network customers (mainly universities, schools of higher education, and some research laboratories) can get IPv6 connectivity at no extra cost.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

See point 1 above. Only a few ISP offers IPv6 services today, even if many IPv6 forums and events are organized by Engineer Schools and the Schools of Computer & Communication Sciences of the Swiss Federal Institute of Technology of Lausanne and Zurich.

The Swiss telecom incumbent (Swisscom) has launched its first "all IP" services in May, based on an IMS core network. This IMS CN, which is supposed to replaced the traditional TDM network in the future, supports IPv6 but run actually on IPv4. The migration on IPv6 is planned for 2010 or 2011.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

BAKOM/OFCOM follows the IPv6 developments in Switzerland but is not actually leading any working group or forum. As the impact of IPv6 on the regulation is not now defined the regulator is actually in technology foresight.

UK

Question 1: Could you please describe public incentives related to IPv6 deployment in your country?

There are no financial incentives or tax advantages specifically to promote support for IPv6.

Question 2: How active your market is in relation to IPv6 deployment (e.c. forums, projects)?

The Department for Business Innovation and Skills (formerly BERR/DTI) has prepared a draft report on IPv6 with recommendations:
- a) To bring the various interested parties in UK together to discuss progress and issues at regular workshops that would be hosted at BERR;
- b) To set specific but realistic targets for achieving IPv6 support in the main parts of the Internet infrastructure in UK. Where possible we will coordinate these targets with other European countries and the USA;
- c) To publish progress on IPv6 migration in UK through an Internet website.

What will happen to this report is not certain at present as BIS may not have funding to support what it was planning. The recommendations have not been formally adopted or accepted.

Few of the servers used for the provision of information and email services in UK currently offer access using IPv6. Only 30 of 25 million UK based name servers have IPv6 addresses.

Of the major Telecommunication Companies that provide access to the Internet, ie BT, Virgin Media and Cable and Wireless, none is yet offering an IPv6 based access service and they are probably 1-2 years away from doing so, but BT is running some trials and pilots.

The net result is that there is very little traffic (<1%) using IPv6 at present.

LINX (London Internet Exchange) ran a well-attended workshop on IPv6 in March 2009, primarily for ISPs. LINX is the main UK forum for discussion about IPv6 at present.

Question 3: What are regulator's role and incentives encouraging IPv6 deployment in your country?

There are no Ofcom publications specifically on IPv6.