IPv6 & Broadband

IPv6 Cluster

European Commission

Information Society Technologies

IPv6 Cluster

IPv6 and Broadband

IPv6 Cluster
IPv6 and Broadband

ISBN 3-00-013801-3

Edited by 6LINK with the support of the European Commission and the EC IPv6 Cluster.

This booklet was made possible thanks to the cooperation and contributions of the IPv6 Cluster projects.

If you have any questions or comments or you would like to receive another copy of this book, please visit *http://www.ist-ipv6.org.*

On-line PDF version also available *(http://www.ist-ipv6.org/pdf/ISTClusterbooklet2005.pdf).*

Table of Contents

Preface

'IPv6 and Broadband' provides an overview of the European R&D activities in the IPv6 area, focussing on projects, network aspects, trials and applications developed and demonstrated in the Information Society Technologies (IST) Programme.

This overview has been edited by the IST project 6LINK based on inputs from 6LINK partners and from many external contributors, including representatives of the European Commission, other IST projects, and other companies and research institutions.

The editorial team was as follows:

- Peter Christ, T-Systems Nova Berkom, Germany
- Mat Ford, BT, UK
- Jordi Palet, Consulintel, Spain

The editors are particularly grateful to Arturo Azcorra, Marcelo Bagnulo, Tim Chown, Peter Christ, Paulo De Sousa, Pascal Drabik, Mat Ford, Wolfgang Fritsche, Alberto García-Martínez, Gopi Garge, Christophe Janneteau, Sheng Jiang, Jayachandra K., Mounir Kellil, Peter Kirstein, Hong-Yon Lach, Latif Ladid, Izumi Miki, David Mills, Piers O'Hanlon, Jordi Palet, Juan Quemada, Tomas Robles, Pierrick Seite, Soren-Aksel Sørensen and H.-J. Vögel, for their valuable contributions to this publication.

Special thanks are given to those individuals who kindly agreed to spend their time and effort in contributing to the interviews. Their insight into this area provides a significant added value to this publication.

This book is also available on the web, via the homepage of the IST IPv6 Cluster:

http://www.ist-ipv6.org/

Introduction

The objective of this publication, **'IPv6 and Broadband'**, is to provide an overview of European R&D activities in the IPv6 area. The publication focuses on projects, network aspects, trials, and applications developed and demonstrated in the Information Society Technologies (IST) Programme.

The following issues are specifically addressed:

- Overview of IPv6 deployment in Europe;
- Discussion of issues related to IPv6 in broadband, for example multi-homing, GRID, Broadcast, Privacy and Security and other aspects, and;
- A vision of ambient intelligence which focuses on scenarios and applications for e-government, e-health, education and training.

Finally, the status of **'IPv6 and Broadband'** in other regions in the world is discussed.

To complete the picture of IPv6 technology status and perspectives in Europe, this publication provides interviews with some key actors in the domain, providing their insight into the potential impact of the deployment of IPv6 technology and applications.

This publication is targeted mainly at professionals working in, or in areas related to, telecommunications and information technologies for the information society. This includes not only researchers, consultants and decision makers, but also users interested in the current status of IPv6 and its evolution in the near future. Readers are expected to have a good knowledge of telecommunication technologies, but need not be specialised in IPv6.

In summary, this publication is expected to increase general knowledge about the state of the art of IPv6 in Europe. It will contribute to the visibility of the IST work among the R&D and business community, as well as to the circulation of information between IST projects.

2 *e*Europe and IPv6

2.1 Introduction

The original Internet that was designed in the early 1970s has been gradually showing its weaknesses and today is no longer capable of responding to the requirements of a modern and dynamic society. It can not efficiently meet the challenges of a new networking landscape. Efforts to develop a new communications protocol, IPv6, that would give the Internet new functionality while responding to the need to significantly expand its addressing capability, started in the early 1990s and are still on-going, notably through a determined investment in R&D by European players.

2.2 *e*Europe

By setting for itself the goal to become the most competitive and dynamic knowledge-based economy in the world, the European Union at the Lisbon Summit, in March 2000, has given industry a much needed political signal that highlighted the importance of stimulating the use of the Internet.

*e*Europe is part of the Lisbon strategy. The initial action plan, *e*Europe 2002 [1], was endorsed by the Feira European Council in June 2000 and had three main objectives:

1. A cheaper, faster, more secure Internet
    - Cheaper and faster Internet access
    - Faster Internet for researchers and students
    - Secure networks and smart cards
2. Investigating in people and skills
    - European youth into the digital age
    - Working in the knowledge-based economy
    - Participation for all in the knowledge-based economy
3. Stimulate the use of the Internet
    - Accelerating *e*Commerce
    - Government online: electronic access to public services
    - Health online
    - European digital content for global networks
    - Intelligent transport systems

*e*Europe 2002, with the joint effort of all stakeholders, has already delivered major changes and has increased the number of citizens and businesses connected to the Internet. It has reshaped the regulatory environment for communications networks and services and for *e*Commerce, and has opened the door to new generations of mobile and multimedia services. It is providing opportunities for people to participate in society and helping the workforce to acquire the skills needed in a knowledge-driven economy. It is bringing computers and the Internet into schools across the Union, bringing governments on-line and focusing attention on the need to ensure a safer online world.

Following the success of the *e*Europe 2002 action plan, the Barcelona European Council in March 2002 called on the Commission to draw up an *e*Europe 2005 [2] action plan focussing on "widespread availability and use of broadband networks throughout the Union by 2005 and the development of Internet protocol IPv6... the security of networks and information, *e*Government, *e*Learning, *e*Health and *e*Business".

The objective of the *e*Europe 2005 action plan is to provide a favourable environment for private investment and for the creation of new jobs, to boost productivity, to modernise public services, and to give everyone the opportunity to participate in the global information society. *e*Europe 2005 therefore aims to stimulate secure services, applications and content based on a widely available broadband infrastructure. As a consequence, Europe should have by 2005 modern online public services (*e*Government, *e*Learning, *e*Health), and a dynamic *e*Business environment. These applications and services should be based on the widespread availability of broadband access at competitive prices and on a secure information infrastructure.

2.3 IPv6 and *e*Europe

Today it is recognised worldwide that the new version of the Internet Protocol, IPv6, can play a fundamental role in shaping the future communications landscape, in providing tools for ubiquitous access to the Internet, in liberatinge the innovation potential of Internet users, and in strengthening European industry, notably in the domain of mobile communications.

IPv6 is one of the corner stone technologies enabling *e*Europe.

It has the potential to boost the deployment of applications and services relying on security and to provide new Quality of Service (QoS) possibilities. Security and (QoS) are fundamental features for applications and services related to *e*Commerce, *e*Health, *e*Government, *e*Learning, etc.

The availability of so many possible addresses [3] makes IPv6 the only realistic technology at the dawn of the 21st century that can be used for the real deployment of innovative peer-to-peer applications, with the potential of inviting every citizen in the world to access services, to share knowledge and enhance skills.

The expanded address space, together with more efficient and robust mobility mechanisms, is especially important in the context of the proliferation of more and more sophisticated mobile communication devices.

The main features of IPv6 presented above, as well as others like auto-configuration, will enable the creation of new applications and services, only limited by our imagination. IPv6 is essential to ensuring the growth and development of tomorrow's Internet, and will allow Europe to translate its leadership in mobile communications into stronger positions in fields as diverse as network equipment, consumer electronics, and communication services.

Besides the potential for the economic aspects of *e*Europe, IPv6, by facilitating communications in general, also has the power to improve social cohesion, which is another part of *e*Europe.

2.4 Achievements

The European Commission acted as a pioneer regarding the deployment and promotion of IPv6 as early as 1999. The work performed in the context of the IST R&D Programme combined aspects of technology deployment with policy, promotion and dissemination. The European Commission Information Society Technologies Programme funded (between 1999 and 2003, in the context of the 5th Framework Programme) a number of projects with a very important focus on IPv6 research and development activities. These projects represent a huge investment on behalf of the European Commission (estimated 90 MioEuro) and the project partners.

This has been made in close co-ordination with the views expressed by the European Parliament and the Council of the European Union, notably as a result of the Commission Communication on IPv6 of 2001. The European Parliament underlined several times the importance of the next-generation Internet while the European Council explicitly underlined the priority attached to both broadband networks and to IPv6.

At the beginning of the 6th Framework programme, we are getting the benefit of our efforts. The European high speed research network, GÉANT, together with most of the National Research and Education Networks of the Member States and Acceding countries, offers IPv6 connectivity and services to the whole European research community. The IPv6 interconnection of GÉANT and other similar networks around the globe makes IPv6 available to the research communities worldwide for the first time.

To further strengthen our message on IPv6 and give a wide visibility to our actions, and to celebrate formally the availability of IPv6 to the research communities, a 'Global IPv6 Service Launch Event' took place in Brussels on 15th and 16th January 2004. More than 200 participants attended the event where about 50 high-level speakers, including ministers, senior government officials, directors from research networks and relevant industries worldwide, expressed their views.

The event has succeeded in reinforcing the awareness of IPv6 to industry, Internet service providers, and telecom operators, and has provided further encouragement towards the early deployment of IPv6.

The success of this event, for which the press coverage was very significant, may be regarded as a highly important milestone along the way towards the ubiquitous availability of IPv6.

2.5 Conclusion

New steps can now be taken, such as considering the inclusion of compliance with IPv6 in the Information Technology equipment procurement exercises of public administrations. The National IPv6 Task Forces that have already been created can play a significant role in this regard, and the European IPv6 Task Force is ready to play a catalysing role.

Three years after the launch of a set of co-ordinated actions we are harvesting the fruits of our efforts. IPv6 is here now and Europe now has a challenge to transform the results achieved so far into commercial competitive advantages for European industry.

IPv6 is a key enabler technology, one of the corner-stones for *e*Europe. A second corner-stone is the wide availability of broadband infrastructures. Their deployment has to progress in parallel with IPv6 deployment, such that the creation and the offer of innovative communication services at the core of *e*Europe is not jeopardised.

2.6 Acknowledgements

This section has been contributed by Pascal Drabik (European Commission).

2.6 References

[1] http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/actionplan_en.pdf

[2] http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf

[3] About 340 undecillions; Actually: 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses in theory

3 IPv6 Deployment in Europe

3.1 Introduction

The European IPv6 Task Force was launched in April 23rd, 2001, as the result of an open call to the industry by the European Enterprise Commissioner, Erkki Liikanen.

Four Working Groups were established, which in January 2002 generated their final reports:

- Internet Infrastructure [1]
- Mobile Wireless [2]
- Next Generation Applications [3]
- Trials Framework [4]

A summary and conclusions document, the "Main IPv6 Task Force Report" [5], was drafted by the editorial team, and then submitted for the consideration of the European Commission.

The Communication from the European Commission to the Council and the European Parliament, "Next Generation Internet – Priorities for action in migration to the new Internet protocol IPv6" [6] was generated as a direct consequence of the IPv6 Task Force Main Report, and delivered in February 2002.

Furthermore, the Barcelona European Council, under the Spanish Presidency, in March 2002, in the Presidency Conclusions [7] considered IPv6 as one of the foundations for European competivity, which was further stressed, together with broadband and 3G, in the e-Europe 2005 plan approved in the Seville meeting, in June 2002.

One of the actions called upon was the continuation of the work of the European IPv6 Task Force, in its 2nd phase, and the setup of equivalent initiatives at national levels. The conclusion of the current IPv6 Task Force Steering Committee project (in May 2004) marks the end of the 2nd phase, with the 3rd phase beginning at the time of writing with a renewed Steering Committee project.

The IPv6 Task Force Steering Committee project undertook this mission to continue the initial work, succeeding in Phase 2 in the creation of the European National IPv6 Task Forces, from September 2002 up to May 2004.

The volunteer work of the members of the National IPv6 Task Forces in Europe, together with the IPv6 Task Force Steering Committee project partners, and the broad and extensive international cooperation from all around the world, have been very important to help kick-off the broad IPv6 deployment, which is starting to happen now at all the industrial levels.

IPv6 is no longer a utopia, it is here, and is slowly waking up in all the business fields, with a slow but firm progress, and the national, international and regional initiatives have been key for this progress.

3.1.1 The European IPv6 National Task Forces

The following National IPv6 Task Forces have been created:

- Spain (May 2002)
- Finland (August 2002)
- France (September 2002)
- Luxembourg (November 2002)
- United Kingdom (January 2003)
- Portugal (February 2003)
- Switzerland (April 2003)
- Germany (April 2003)
- Denmark (May 2003)
- Sweden (May 2003)
- Belgium (June 2003)
- Italy (October 2003)
- Austria (March 2004)
- Ireland (April 2004)

Several other countries including Netherlands, Norway, Poland, Greece, Slovakia and Russia, at least, will follow in the next few months.

3.1.2 Key Results of the IPv6 National Task Forces

3.1.2.1 Approach and Mission of the National Task Forces

The various national task forces have used similar approaches. So far, most of the National Task Forces have a good mix of industry and academic support. They have mission statements that aim to address the introduction of IPv6 in the country or region. Most of the Task Force members have contact to governmental agencies, although there are few examples where there is an active support (not financial) from a ministry (positive examples are Spain and France). Other governmental agencies have been supportive in words or are not fully aware of the IPv6 Task Force activities. A main problem is that the current economic situation reduces the possibilities to get funding support for awareness-initiatives like that of the IPv6 Task Force. In such cases the Task Forces may seek to piggyback other funding, e.g. broadband initiatives.

Due to the voluntary character of the National IPv6 Task Force, the power of the task forces is dependant on the available workload of the members. But all national IPv6 TF aim at the awareness for and deployment of IPv6 and therefore the cohesion between the national Task Forces is quite good. One of the aims of the European IPv6 TF-SC has been to aggregate the plans of the national IPv6 Task Forces and to avoid duplication of work among the Task Forces.

3.1.2.2 Reaching a Critical Mass

The question about what is being done to attract more organizations/industries and especially the key movers into these national IPv6 Task Forces is a tough one. The possibilities to attract players depend heavily of the activities on the national Task Forces and their connections. Where there is a strong network and experts are available, the situation of the Task Force is usually better than where there are only technical people with few outreach possibilities. Some Task Forces have managed to get a fair level of press attention.

There are usually limitations in the outreach capabilities of the Task Forces, since they usually have no budget for dissemination activities and therefore the means to achieve and address a larger community are somewhat limited. None of the Task Forces with their limited means could claim to target all industries and this does not seem to be an important goal (given the limitation). Some Task Forces have instead looked for high-quality members who are willing to contribute, rather than having a large number of silent members.

3.1.2.3 Targeting the EU Enlargement Countries

So far now, the main focus has been to reach out for larger economic countries and countries where there were good opportunities for activities to be successful. This means there is still a need to address countries where there is no recognizable IPv6 activity. Resources to achieve this are very limited for the IPv6 TF-SC at this stage. Further resource support would be required to engage these nations.

Initial activities have been started, though it is a slow process.

3.2 Key Findings from the IPv6 National Task Forces

After this initial "kick-off" period and after achieving a reasonable critical mass and representation, the European IPv6 Task Force started to reap the benefits of its initiatives by collecting the key findings from the field, combining country-specific results to identify common successes and common areas that need concerted action to resolve.

3.2.1 Achievements

Most of the National IPv6 Task Forces have achieved a certain level of:

- Awareness and working meetings.
- Different focused working groups.
- Local web site, ftp, mail exploders, and archives.
- Press releases and articles.
- Participation from key industry, education, research and government groups.
- National Research and Education Networks connected to GÉANT with IPv6 (frequently using native connections), and offering IPv6 services to their communities.
- Trials in different business sectors.

In some cases, Internet Exchanges (IX) have incorporated IPv6, or started to consider doing so. So far, only a couple of countries have deployed IPv6 services at the national NIC (e.g. in France with AFNIC), though many plan to do so.

Only a few ISPs, in some countries, have started to offer IPv6 services, but several have concrete plans to start deploying. We expect these to reach a broader base of customers during 2005.

3.2.2 Challenges

There is a consensus about the following challenges for the success of this mission:

- Lack of official commitment from governments.
- Lack of strategic recognition of the importance of IPv6.
- Lack of new IPv6-ready applications.
- Lack of concrete business models.
- Lack of customer demand (customers/consumers want services not protocols).
- Lack of European Industrial leaders.
- Lack of simpler and clearer technical answers.
- Lack of funding for the local National Task Forces activities.
- Lack of funding for IPv6 take-off in the ISPs and industry in general.
- Lack of benchmarking of the real IPv6 deployment status and the bigger picture.

It is also interesting to note that in several countries most of the achievements have not been well disseminated and recognized by the media. For example, at least in one country several public and private entities have confirmed that they are mandating IPv6 in their new procurements policies, but this has gone unnoticed and not been advertised publicly. In many cases, organizations do not wish to make their future technology plans public; the outlook and policy of such companies will vary. One major router vendor only announced IPv6 in its roadmap three months ahead of releasing it in production code, while in contrast another had made open beta code available for many months. Of course now, all major router vendors have IPv6 support in production code, but this example shows how product announcements may hide true progress in application and service support in the coming months.

Though government support has been provided in most of the countries to kick-off the National IPv6 Task Forces, there is in general a lack of real commitment (or funding) from the government to set the pace. There are relatively simple technical solutions available to enable IPv6 in common web server platforms (e.g. current versions of Apache and IIS on Windows Server 2003), but none of the EC or European governmental web sites have been enabled up to now. Anyway, some work in this direction is already ongoing in several European entities and results are expected in a few months. One problem here is that such sites are often outsourced, and thus changes in technology can take significant time. The outsourcing issue is a wider one, affecting many government and public sector organizations (including schools and health services).

3.2.3 Next Steps

In general, there is a unanimous agreement to push forward with the following activities:

- Continue and strengthen the work and cooperation of the National and EU IPv6 Task Forces, defining National and European recommendations.
- Focus on IPv6 deployment and application opportunities.
- Continue the awareness and dissemination activities, communicating on best practices.
- Update the national Task Force web sites and create an EU IPv6 web portal.
- Promote the creation of a centre of excellence, which can be an independent reference point for those wishing to design, build, develop, or deploy IPv6 products.

- Convince the public and private organizations to demonstrate their commitment, demanding IPv6 in any procurement.
- Arrange for key public web sites to be accessible with IPv6.
- Gather more potential industrial actors (SMEs, integrators, ISPs, WISPs, etc.).
- Work on "business case" examples.
- Study a detailed deployment roadmap.

3.2.4 IPv6 Deployment Status in Europe and Required Actions

As a result of the October 2003 meeting in Milan and the work and initiatives undertaken by the European and National IPv6 Task Forces in Europe during the first half of the 2nd phase, a deployment status and updated call for action have been released, including a press release .

This report makes comprehensive recommendations for EU Member State governments, for the European Commission and for industry.

The collective initial findings of the 2nd phase of the European Union IPv6 Task Force are detailed in this report and in the minutes of the Milan meeting including the following key messages:

- The critical mass needed for IPv6 adoption in Europe and the member states has been garnered, though in a slow process, which needs further strengthening through increased active participation of key industry players and involvement of the new European countries to design a comprehensive European IPv6 roadmap.
- Global cooperation, including Research & Development, policy-making and real life deployment, should be strengthened to pave the way to a global scale deployment of IPv6 and equitable access to knowledge, avoiding the creation of isolated Internets and allowing a rhythmic adoption at a global scale.
- The National IPv6 Task Forces are still in the formation phase (many of them with less than one year of activity) with a relative degree of success engaging their governments in the dialogue and recruiting volunteer experts to formulate objectives and action plans. The "volunteer model" delivers on a best effort basis. A dedicated or funded model would be more suitable for such an important, large-scale undertaking.
- The actual level of IPv6 deployment is still imperceptible, especially when compared with Asia Pacific and the expected growth in other areas (including North America).
- A number of barriers and hurdles towards IPv6 deployment have been detected, namely deployment business models, return on investment models, CEO/CTO unawareness and some political showstoppers. The creation of a new panel of experts, led by the IPv6 Task Forces, winning stakeholders from the public and private sector, including SMEs, will allow in depth investigation of these barriers and the generation of new recommendations and case studies.
- Similarly, a number of technical barriers had been identified, and it is necessary to address these, while driving forward technology in a networked world that will increasingly rely on IPv6 as an enabler. The creation of a research-led center of IPv6 expertise or excellence would address this requirement. Such a center should combine a technology-driven focus with the needs determined by the IPv6 panel of experts, and both should liaise in this mission.

- The adoption of IPv6 by governments, universities, schools and the European Commission, where it make sense (e.g. deployment on web sites), will generate confidence in the minds of end-users (as is happening with the DoD announcement in the US), and a possible trigger for business cases.
- Public and private sector procurements should require IPv6 capabilities for future-proof investment.
- Top-level national NICs should accelerate their support of IPv6.
- IPv6 deployment progress should be benchmarked in order to monitor its success.
- The achievements and progress of the Task Forces must be widely disseminated by means of an extended IPv6 Task Force portal.
- It is of paramount importance to take all required actions aiming at the continuation of the work performed by the "European IPv6 Task Force" and renew its mandate for the third phase with an enlarged team including the national IPv6 Task Forces and selected key industry players (ISPs, ASPs, vendors) with a "funded model". The third phase, beginning Summer 2004, should focus on tangible success in the short-term deployment in wired and wireless broadband access and strategic innovative revenue-generating applications (consumer electronics, end-two-end security, e-vehicle, etc.) and in the longer term strategic objectives (e-Infrastructure, GRID, 4G, Ambient technology,…).

While IPv6 deployment should be market led, the European IPv6 Task Force encourages the consideration of the recommendations contained in this report because of their critical importance towards the achievements of the eEurope 2005 goals (including "broadband for all", security and Ambient Intelligence) and the future development of Internet technology in Europe.

The European Commission is called upon to submit the results of the work of the 2nd phase of the IPv6 Task Force, contained in this document, to the European Council.

See the complete "IPv6 Deployment Status in Europe and Required Actions" [9] document for more information.

The press has widely spread this message, including articles and interviews to some of the key actors [10].

3.2.5 Global IPv6 Service Launch Event

One of the key events that have been organized in cooperation with the IPv6 Task Force, was the Global IPv6 Service Launch Event, in Brussels on 15-16th of January 2004 [11].

The event was funded and hosted by the European Commission together with the 6NET and Euro6IX projects, with some contributions from other projects, including GÉANT.

It was targeted to policy-makers, leading experts and managers from Research, Industry and Business active in the area of IPv6 and research networking from around the world.

The event included several end-user oriented demonstrations, a press conference, appearances in EuroNews and a virtual inauguration ceremony to celebrate the availability of Global IPv6 connectivity.

A picture gallery is available, together with streaming of the complete event (which was streamed live over both IPv4 and IPv6).

Figure 3.1: **Global IPv6 Service Launch Event Logo**

The Global IPv6 Service Launch Event had the following objectives:

- Highlight the importance and impact of IPv6.
- Publicize the advanced capabilities of the large IPv6 test-beds, GÉANT and the national research and education networks with regard to their IPv6 deployment.
- Promote international coordination and collaboration.
- Emphasize the international dimension of research expanding from regional into global cooperation.
- Further develop a global perspective on research networking.
- Inform leading edge and influential users about the achievements of the large European IPv6 tests-beds and GÉANT and how they can benefit from them.
- Promote the new possibilities available with IPv6.

Representatives of the Informatics Directorate (Telecommunications and Network) of the European Commission were present, in order to prepare for the internal adoption of IPv6, with the support of the IPv6 TF-SC.

Several members of the IPv6 TF-SC participated in the event committee and in several related activities, including the preparation of the final report, which included the following summary:

On January 15-16, 2004, the European Commission hosted the Global IPv6 Service Launch event in Brussels. The event formally heralded the availability of worldwide native IPv6 connectivity spanning IPv6-enabled research networks around the globe, including networks such as GÈANT in Europe, Abilene in the United States, CA*net4 in Canada and WIDE in Japan.

The two-day event saw presentations from key players from the worldwide research networks, from industry and from the political arena. This document summarises the talks given by the speakers, and documents the launch ceremony and parallel IPv6 technology demonstrations.

The focal point of the event was the launch ceremony held on the evening of the 15th January. Eight representatives of the worldwide research networks were each invited to speak briefly on the importance of IPv6 from their perspective. European Commissioner Erkki Liikanen added his view:

"Today we are here to celebrate the arrival of IPv6 and its integration into Europe's key research infrastructure. IPv6 is part of the next generation of Internet technology. It will improve the performance of the Internet and it will enable the Internet to be integrated into a wide range of devices and services in our homes, businesses and while on the move. Some of these are demonstrated at this event - from household appliances to the IPv6 enabled vehicles.

The introduction of IPv6, alongside unrestricted access to broadband, is of great importance. Together they will help to offer citizen's wider access to an advanced Information Society. They will deliver improvements in economic growth, competitiveness, and productivity through the provision of a whole new generation of services and applications, including 3G.

Possible applications and services that this new technology promises to usher in are limited only by the imagination and many applications are currently under development now. If you consider that every device in the world is individually addressable, then this opens up limitless possibilities."

Figure 3.2: **Commissioner Erkki Liikanen at the Global IPv6 Service Launch Ceremony**

In parallel to the presentations, a demonstration area was set up which showcased the results of a number of IST and other research projects where IPv6 has been the base technology for deployment. The demonstrations included examples of collaborative work undertaken with international partners around the world, illustrating the potential for a global perspective on research networking.

In terms of its goals, the Launch Event was considered a success. It managed to demonstrate future potential for IPv6 services and applications, highlighting the results achieved in research to date and the capabilities of the international research networks to offer a production quality IPv6 service to universities and research institutions.

See the complete "Report on the Global IPv6 Service Launch Event" for more information [12].

During the press conference, European Commissioner Erkki Liikanen, stated:

- Today we are here to celebrate the arrival of IPv6 and its integration into Europe's key research infrastructure.
- IPv6 is part of the next generation of Internet technology. It will improve the performance of the Internet and it will enable the Internet to be integrated into a wide range of devices and services in our homes, businesses and while on the move. Some of these are demonstrated at this event - from household appliances to the IPv6 enabled vehicles.

- The introduction of IPv6, alongside unrestricted access to broadband, is of great importance. Together they will help to offer citizens wider access to an advanced Information Society. They will deliver improvements in economic growth, competitiveness, and productivity through the provision of a whole new generation of services and applications, including 3G.
- Possible applications and services that this new technology promises to usher in are limited only by the imagination and many applications are currently under development now. If you consider that every device in the world is individually addressable, then this opens up limitless possibilities.

Take as one example road and traffic systems. Your in-built navigation system would do more than direct you to your destination based solely on global positioning and a set of passive digital maps, it would interact far more intelligently with the environment and could find routes dynamically based on information it receives back from other IPv6-enabled devices - for example enabling you to find the quickest or most efficient route taking into account heavily congested/blocked roads. Traffic signalling would become more intelligent and be able to respond instantaneously to the different patterns of traffic flow throughout the day. Road safety would benefit too. Drivers could be forewarned of accidents on the motorway or of slow-moving traffic and sensors of vehicles involved in collisions could automatically notify the emergency services.

Home appliances are another area which springs immediately to mind. Appliances enabled with IPv6 could be controlled remotely via a PC or even a hand-held 3G device giving home-owners total control of their homes from anywhere in the world. DVD players could be developed which would download or stream films from the Internet and alarm sensors could be manufactured cheaply which would automatically detect problems and forewarn the relevant services preventing unnecessary loss of life or damage to homes.

IPv6 also opens up enormous potential too for the end-user. With fast data connections and IPv6 at their fingertips, end-users will find they have the wherewithal to become tomorrow's data providers, opening up untold possibilities for end-user industries.

- The Union's commitment to IPv6 started with the creation of a European IPv6 Task Force in 2001. Since then the European Commission has provided policy orientations which have been taken up at the highest political level.
- These efforts have been well rewarded. GÉANT, the European Research Networks backbone, is now IPv6-enabled and is today the world's largest IPv6 research network.
- GÉANT offers the greatest geographical coverage of any network of its kind in the world (from Iceland to the Caucasus). GÉANT has a dual role of providing an infrastructure to support the advanced communication needs of the scientific community (such as IPv6), as well as providing an infrastructure for research on state-of-the-art communication technologies itself.
- The GÉANT network is being continually upgraded, and currently has a total trunk capacity of 185 Gigabits per second (more than twice as powerful than any other research network in the world). In addition, the network provides 14.5 Gigabits per second of international connectivity to North America and Japan. Further links, to the Latin American and Mediterranean regions, are being implemented by the EU-projects ALICE and EUMEDconnect respectively and will become operational within the next few months. These regional backbone networks will be IPv6-enabled as well.
- During these two days we are celebrating the world's first global native IPv6 research network which is an important first step towards an IPv6-based commercial Internet. This event therefore underlines the fact that IPv6 is here and beginning to make its presence felt.

3.3 Roadmap for Deployment of IPv6 in Selected Industry Sectors

3.3.1 Overview

The following picture gives an overview on the expected deployment of IPv6 in various industry sectors. It starts with an overview on the expected private and industry sectors that we expect to be affected first.

Members of the IPv6TF-SC are involved in scenario description and analysis in the IETF for enterprise, unmanaged, ISP and 3G network deployment of IPv6. IST IPv6 projects are being proactive in such standards contributions, as a better understanding is gained on potential priorities and timeframes for deployment from a technical perspective. Political and commercial uptake of the IETF technology is still required. The IST IPv6 projects are also heavily involved in IPv6 application development and porting, again giving insight for the IPv6 TF-SC on potential adoption. The task in hand is to turn potential into reality. The first signs of that reality are now emerging, initially in the Asia-Pacific region (e.g. IPv6-capable printer hardware).

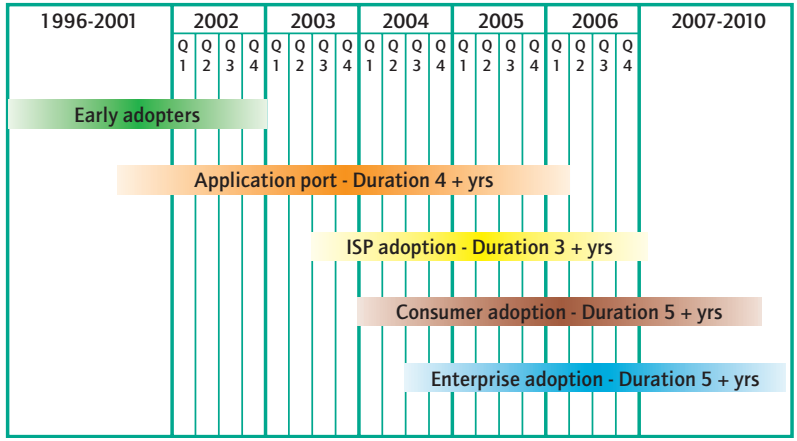

Figure 3.3: **IPv6 Rollout**

The following table provides a list (for reference only, not exhaustive) of manufacturers (Hardware and Software) and Service Providers, with an active involvement in IPv6.

Hardware
6WIND, Agilent, Alcatel, Allied Telesyn, ARtem, Bay Micro, Cisco, Conexant, dpi, Enterasys Networks, Ericsson, Extreme Networks, EZchip, Fortinet, Foundry Networks, Fujitsu, Hexago, Ixia, Juniper, Matsushita, Nec, NetLogic Microsystems, NetScreen, Newport Networks, Motorola, Nokia, Nortel Networks, Paion, Polypix, Procket Networks, Renault, Samsung, Sony, Spirent, Sumitomo, Telco Systems, Teldat, Teradiant, Xcelerated, Xiran, Yamaha

Applications, Software, OSs

Accelerated Technology/Nucleus, Apple, Ariel Networks, BSD, Check Point, Consulintel, Elmic Systems, Enea/OSE, FreeBit, Firebird, Green Hills/Integrity, Hexago, HIfn, HP/UX/Tru64, IBM/AIX, Interpeak,InterWorking Labs, IP Infusion, Java, Linux, Matsushita, Mentat, Microsoft, MontaVista, Mozilla, NextHop Technologies, NFR Security, Novell, Opera, Panasonic, QNX, Radvision, SCO, SGI, Sun/Solaris, Symbian, TeamF1, Teja, Trolltech, Ubo System, WindRiver/VxWorks

Native IPv6 Service Providers

arsys, AsiaNetcom, Biglobe, Bersafe, British Telecom, Cegetel, Chita Medias Network, Colt, Deutsche Telekom, Dream Train Internet, France Telecom OpenTransit, Flag Telecom, FreeBit, Gitoyen, Global Crossing, HKNET, HiNet, HTnet, Hurricane Electric, IIJ, Japan Telecom, Japan Sustainable Community Center, Jens, KDDI/KDDI Lab, Level3, Matsushita Graphic Communication Systems, MCI, Media Exchange, Nerim, Nifty, NTT Australia, NTT Communications, NTT East, NTT Europe, NTT MCL, NTT MSC, NTTPC, Poweredcom, SpaceNet, Stealth Communications, STnet, Telecom Italia, Telefonica, Teleglobe, Telia, Tiscali, TIWS, Verio, vBNS+, XS4ALL

Internet Exchangers

6TAP, 6IIX, 6NGIX, AMS-IX, ASNet, Equinix, FICIX, Florida-MIX, FNIX6, INXS, JPIX, mad-iX, MCI MAE, NaMeX, NL-SIX, NSPIXP-6, NTT MCL IPv6 IX, NY6IX, PAIX, S-IX, Sphinx, TIX, TOP-IX, TREX, TWIX, UK6X, Wellington Internet Exchange, XchangePoint Europe

Figure 3.4: **Known Commercial IPv6 Products/Services (partial selection only)**

3.3.2 IT-Rollout for IPv6

The following picture provides an overview on expected steps in organizations and companies that are starting to integrate IPv6 into their IT planning. The initial plans would generally assume a transition to dual-stack deployment (addition of IPv6 capability) rather than an immediate transition to IPv6 only operation (which is the long-term goal). IPv6 only networking may emerge earlier in places where IPv4 global address space is not so readily available, e.g. in many areas of the Asia Pacific, or African or Latin American regions.

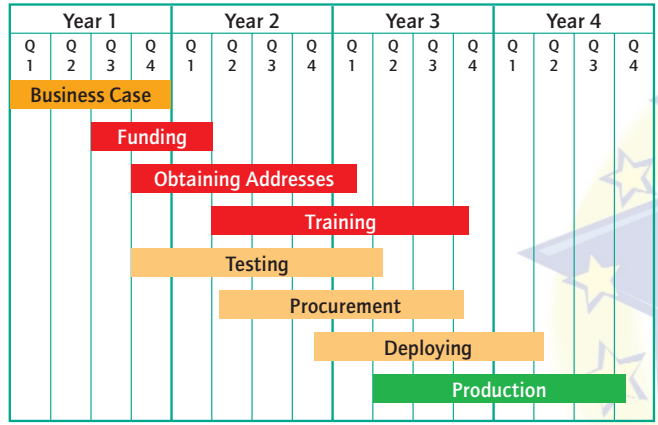

Figure 3.5: **IPv6 Deployment**

3.3.3 Internet Service Providers (ISP)

One of the main problems currently is that many of the ISPs currently are hesitating to invest in major new activities due to the current economic situation in general. New business is welcome, of course, but IPv6 currently does not automatically imply a new big business. Indeed, deploying a dual-stack IPv4-IPv6 infrastructure may imply a short-term increase in costs (managing both protocols) until operations become streamlined and new IPv6 functionality can be leveraged.

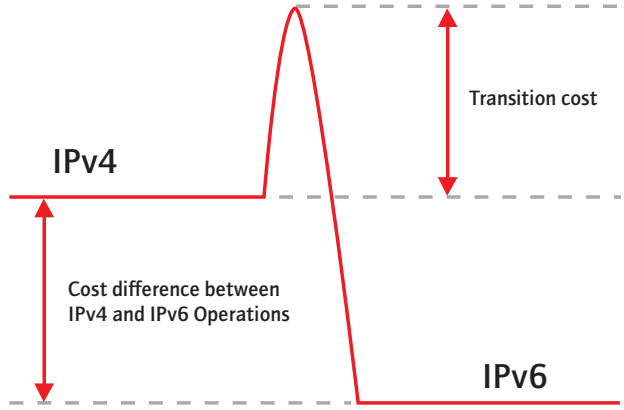

Figure 3.6: IPv6 Transition Cost (depiction following Chown, Doyle, Ladid, et. al. [13])

The best way to overcome this dilemma is through creating customer awareness so that they are motivated enough to request their ISP for IPv6 service. Particularly (large) business customers requesting IPv6, asking to move some parts or all of their networks or VPNs to support IPv6 would be a big incentive for ISPs to start providing services and products beyond customer projects. This would lead to more investments in IPv6 on the provider side. This would also be of benefit for private customers. Not many private customers, though a growing number, are currently asking for IPv6. In comparison their impact seems to be less than a large network contract with a big customer.

Many major ISPs are prepared internally to do a rollout of IPv6, once a business decision is made. A business decision currently largely depends on customer requests. First customer requests are apparently handled as a project business. Massive customer requests would lead to an acceleration of internal decisions and a quicker IPv6 rollout. It is expected that over the coming 24 months IPv6 demand from customers will grow to a level, where few ISPs will be able not to offer IPv6 services in Europe. This situation seems to hold true for Backbone networks as well as for access and broadband access networks.

IPv6 capability is now present in all major router vendor implementations. A natural procurement cycle will lead to the deployment of IPv6 capability at very low additional cost in terms of acquisition, though additional costs exist in terms of management of the network, and areas including training.

Thus another point that could bring the ISPs to the decision of implementing IPv6 service is simply the rising number of supported IPv6 features within the actual router implementations that meet the special ISPs requirements. Especially the support of IPv6 for broadband access as well as the IPv6 transport possibilities over an IPv4 (MPLS) based provider backbones (without service degradation for IPv4) are a big step towards an IPv6 enabled carrier scale provider infrastructure.

The encouraging exception in IPv6 deployment can be observed within the academic networks, where no business case is required for deployment of IPv6. Here, IPv6 is seen as the "right thing to do" for the benefit of researchers and students alike. As a result, at the time of writing GÉANT (the pan-European IPv6 research network interconnecting all the NRENs) is dual-stack IPv6 and 18 of the NRENs have connected natively to this service, most of them having their own dual-stack service. The 6NET project accelerated significantly the deployment of IPv6 in these networks (from a planned end-of-2004 to reality in the early part of 2003). The academic deployment has been important for validating the production deployment of IPv6 for commercial ISPs. In some cases, academic deployment leads to IPv6 technology awareness and adoption in commercial ISPs, e.g. where regional networks are outsourced to commercial ISPs, who then deploy IPv6 for the academic network using technologies like 6PE.

In a similar way, the US DoD did not require a business case for IPv6, rather it knew that IPv6 was the tool to do the job for their personnel, including the military forces. As a side effect, the scale of the US DoD market for procurement of IP-enabled products creates a business case for vendors and developers in itself.

Besides that the necessity of supporting IPv6 within the global military communication radiates to the other Defense Departments of NATO, so that the requests from these big customers can trigger their ISPs to offer IPv6 services faster than expected.

A few ISPs in Spain and France have already started to provide some initial commercial services, most probably as a result of the Spanish and French IPv6 Task Forces activities and the major push done in these countries, including a strong government involvement. Other European ISPs are also involved in their national Task Forces and investigate in internal as well as EU triggered research programs their own IPv6 implementation strategies.

Regarding the lack of a business case in terms of short-term revenue, it is necessary to consider that the "business cases" are here already here in terms of an obligation to fulfill missions.

For academic research, the mission is to educate, to train, to produce engineers, PhDs as well as operators, technical, marketing, commercial people. Their "business case" is to provide efficient tools for Research Education, for the benefit of the economy. This is a key driver for universities to deploy IPv6, perhaps initially in their Computer Science departments, and then to the wider campus. Such a deployment scenario is being built within the IETF through the work of 6NET and Euro6IX project partners, some of whom are also IPv6 TF-SC members.

Today we have mostly succeeded in demonstrating the validity and robustness of deployment of IPv6 on backbones, but so far very few large universities or research organizations are running an IPv6 operational network. Consequently, one of the priorities should be not only to have connected labs working on the technology, but deploying IPv6 pervasively in European universities, where new IPv6 applications and services can then be built.

The same is true for military businesses. They need to deploy more efficient networks to fulfill their missions and to be cost effective with technologies. The DoD moved from ISO to IP because of the availability of products. The business model was clear: Low cost and product availability.

Where early adopter ISPs are moving to IPv6, it is often because they have people who know the technology and because they see IPv6 as a necessity and an opportunity. Early deployment experience can lead to potential market advantage in the long term.

Encouraging to the ISPs is the statement from NTT/Verio, one of the earlier large-scale adopters, regarding the cost of IPv6 in their network. Cody Christman, Verio's Director of Product Engineering indicated that the deployment costs are extremely low. IPv6 has been on their roadmap for years, and therefore the transition to IPv6 has been a consideration in all normal hardware and software upgrade cycles since that time. Some resources have been enlisted to perform testing related to IPv6, but testing is always performed on new hardware and OS releases. NTT/VERIO's transition to a dual-stack backbone will normally require some software and hardware upgrades, but the costs for those are already factored in as part of an overall maintenance strategy to maintain the highest-possible network performance. As a result, it is difficult to quantify the specific costs for the deployment independently of an ongoing maintenance strategy.

Is interesting to note that the same stance is being facilitated by several other telcos and ISPs, even in Europe, which are deploying IPv6. Basically, they indicate that the upgrade is (relatively) almost zero cost, except for the education and training of the maintenance personnel, and the requirements for network management of IPv6 services. Also it is observed that the maintenance of IPv6 networks is usually 30-35% cheaper than equivalent IPv4 networks, according to what is being indicated by early adopters in big telco-networks.

3.3.4 3GPP/UMTS

While 3GPP networks were initially perceived as one of the prime motivators of IPv6, and indeed was part of the standard (3GPP release 5), there was a pushback from some of the operators and vendors to allow the usage of IPv4.

The release 5 of the 3GPP standard mandates the usage of IPv6 (and only IPv6) for the IMS (IP Multimedia Subsystem). However, at the end of 2003, a few operators stated that they would much prefer to be able to use also IPv4 for IMS. It seems that the main motivation for that request was the lack of a complete set of all the equipment pieces required for this deployment (supporting IMS with IPv6, which was not available from most of the manufacturers).

Today we can state, after several talks with different mobile operators, that this pushback is not longer going to be a hurdle, because during 2004 the equipment started to be ready and they have also indicated that they don't want to pass by the pain of deploying IMS with IPv4 and private addresses, which will definitively generate some interoperability problems, not only within their own networks, but also when roaming from one network to another, or even just when calls need to work across different operator's networks.

The other problem was also that the deployment of UMTS itself was delayed and somehow being endangered because the extremely high cost of the licenses. But this situation seems to be now clearer and the deployment started already during 2004.

The conclusion is that UMTS will be deployed with IPv6, with a small delay from the initial planning, and is only a question of which applications will take advantage of IMS, in order to predict the utilization rate and the market grow. This will for sure have an impact in the deployment of IPv6 across the rest of the non-mobile networks, considering the need to interoperate and make sure that those services and applications become transparent regardless the type of network and terminals being used.

3.3.5 VoIP

One frequently asked question is about actual or future "killer IPv6 applications" and whether VoIP is a good example.

Many countries around the world are aggressively rolling out various always-on broadband access mechanisms aimed at the domestic and SME market. Many of these always-on access mechanisms are based on cable modem or xDSL type technologies. With the current IPv4 address allocation rules adopted by the Internet Registries around the world the number and type of IPv4 addresses allocated to these always on connections range from (best to worst):

- A few static IPv4 globally routable IPv4 addresses.
- One static globally routable IPv4 address.
- One dynamic globally routable IPv4 address.
- One private IPv4 address – access to the global Internet is only via NAT.

The vast majority being of the middle two types i.e. one static or dynamic globally routable address, with multiple addresses often being available only at an additional, premium price. The result is that end users are installing NAT devices on their premises to enable multiple devices to be connected to the broadband always on access (which of course then hampers the ability to run services end-to-end between two such NATed networks). In fact there is a complete range of small cheap xDSL modems/ /routers that have NAT and a variety of interfaces (Wi-Fi, USB hub, etc.) built in.

Many of the xDSL providers are also the old incumbent telcos that still have a large proportion of their revenue streams from the existing PSTN. The telcos are however facing a problem that the existing PSTN exchanges are in need of replacement/upgrades but with lifetimes of 20+ years are reluctant to invest money in the PSTN when there is a generally accepted view that voice traffic will migrate from the PSTN to IP technology. Deutsche Telekom, for instance, announced in January 2004 that by 2020 all telephone traffic will run over IP.

Telcos around Europe that also have an increasing always-on xDSL network are therefore facing a problem. On the one hand they do not want to invest in the PSTN. But on the other hand they cannot easily migrate voice to the emerging xDSL networks. This is because of the way IP addresses have been allocated, resulting in many users deploying their own NAT devices, which would cause significant problems for a VoIP service. This is because while it is quite possible to connect *out* from a NAT network, it is considerably harder, if in some cases not impossible in a realistically manageable way, to connect *in* to a NAT network, especially with multiple services running within it.

The answer, of course, is IPv6. IPv6 over xDSL allows multiple globally routable addresses per access network and hence all the problems of NAT are overcome. It is also logical to use SIP as the controlling protocol and then considerable synergies with the 3GPP Release 5 specification are achieved. In practice this would allow true seamless services between the fixed and mobile environments. The use of IPv6 also allows Mobile IPv6 to be used and hence inter-domain roaming to be possible i.e. fixed to Wi-Fi, etc.

The type of voice service offered over IP would not be a direct replacement of the PSTN service but could be a much richer offering as presence, multimedia, multi party etc services could also be offered.

The "price" for the removal of NAT is that the "security by obscurity" principle of NATs is also removed, and thus with all devices globally addressable security has to be introduced in gateway devices (firewalls in xDSL routers) or in devices (e.g. personal firewalls). However, the advantage in end-to-end service should be seen to significantly outweigh the perceived advantage that NAT offers. Indeed, IPv6 has the property of being resilient to network port scanning, because an IPv6 subnet has 2^{64} potential IPv6 addresses (not just the one or at most 256 addresses a typical IPv4 host or subnet would contain in a SOHO environment).

In summary it would seem that technically VoIPv6 has much to offer; gets around the NAT problem, has synergy with the 3G (or the 802.11 Wireless LAN) environment, enables mobility and additionally allows adjunct services to be offered. It also has a business model of saving investment in the PSTN and providing additional revenue streams on the current predominately flat rate xDSL access offerings.

Whether SIP-based VoIP is an "IPv6 killer application" remains to be seen. It may certainly prove to be a strong candidate, especially where available in IPv6-enabled WiFi hotspots.

The potential advantage for Mobile IPv6 as a key feature in 3G and Beyond Networks also has yet to be fully explored; with it, IPv6could find a dominating position in the future telecoms environment (e.g by enabling direct peer-to-peer communication between two roaming hosts in a WLAN hotspot by removal of the triangular routing of IPv4 MIP).

Nevertheless, there exist still some open issues with VoIPv6 (e.g. interworking between IPv4 and IPv6 VoIP systems in a carrier scale environment), but those should be solved within the near future (a number of IST IPv6 projects are working in this area) so that VoIP will develop to a communication scenario that motivates ISPs for implementing and offering IPv6.

3.3.6 Broadband PLC

Power Line Communications (PLC) allows transmission of data over power lines. PLC is the network with the most enabling infrastructure already in place in the world: Power line is ubiquitous.

IPv6 provides a package of enhancements to the Internet compared to the capabilities of the existing IPv4 protocol sustained by the Network Address Translation (NAT). NAT has unfortunately created new barriers during the massive and unexpected growth of the Internet with the consequence of breaking the initial end-to-end communications concept.

But nevertheless, this massive IPv4 deployment happened mainly in rich countries, creating a digitally divided society. IPv6, together with other technologies, like PLC, are key in order to restore the situation and alleviate the digital divide pain, enabling more people, entire countries to access information, knowledge which in turn will allow them to take part in the global economy, benefit and possibly create new knowledge.

New access technologies, like PLC, that have already been evaluated for a number of years, have failed to support the initial Internet paradigm. These new technologies have now a new opportunity with IPv6, because IPv6 will facilitate their deployment.

That seems the case for Power Line Communications (PLC). PLC has been around since the 30's but was never seriously thought of as a medium for communication due to its low speed, low functionality and high deployment cost. However, new modulation techniques have enabled this medium to become a realistic and practical means of communication.

Over the last years, new technology designs have led to integrated chips and modems that have been introduced into the market, providing high speeds over the power lines infrastructure at reasonable if not low cost.

Although several broadband PLC technologies have been successfully developed, a standard in this area does not exist yet. Some vendors provide "low-speed" (up to 2 Mbps) data rates using single-carrier technologies (GMSK, CDMA). Some technologies are based on multicarrier modulations (OFDM) and offer higher data rate, starting with a 45 Mbps OFDM PLC chipset, which is the highest data rate available at this time.

On December 2002, at least one PLC technology vendor announced that during the second half of 2003, a new generation of broadband PLC technology providing 200 Mbps of physical layer data rate would be available as a commercial product. That technology is now reality, and is being exploited in the IST project 6POWER [14].

A complete document describing this technology, and how IPv6 can improve the deployment status for both technologies and simultaneously facilitate the addressing of the digital divide, has been published by ISOC, as part of the ISOC members' briefing series [15].

Several ongoing activities are being addressed to allow the take-off and further cooperation between these technologies, with the cooperation of the IPv6 Task Force.

3.3.7 Digital Video Broadcasting (DVB)

The Digital Video Broadcasting Project (DVB) is an industry-led consortium of over 300 broadcasters, manufacturers, network operators, software developers, regulatory bodies and other organizations in over 35 countries committed to designing global standards for the global delivery of digital television and data services. DVB technology has become an integral part of global broadcasting, setting the global standard for satellite, cable and terrestrial transmissions and equipment. DVB standards are available from ETSI.

The move towards interactive services and the convergence at application and service level as well as convergence in networks as increased even further the future importance of the Internet Protocol (IPv4 now, and IPv6 in the future)

The steps taken include awareness creation, presenting the benefits with respect to home networking, coexistence and interoperability with IPv4 and guidelines for dual-stack networking. The first steps have already been taken, and this is actually a key activity of some of the Task Force members.

An example of this was the release in January 2004, by data planet international AG [16], of the world's first IPv6/DVB encapsulator including support for Ultra light encapsulation (ULE) - especially designed to fulfill the needs of existing and upcoming IPv6 based DVB platforms. This has been possible as a direct consequence of several European projects working on this topic, with the participation of IPv6 Task Force members. Current activities include further standardization work in IETF (IPDVB WG).

3.3.8 Home Networking

Looking at the current situation one can conclude that most computers using generic operating systems (e.g. Linux or Windows XP) have IPv6 available as a production protocol. For consumer devices based on embedded operating systems (even for broadband modems and home routers) IPv6 is not yet common in the commercially available devices. However, new embedded systems developers are releasing IPv6 capable code, e.g. Symbian, WindRiver, Elmic Systems and the Microsoft CE .NET. Elmic Systems also have an implementation of the final version of Mobile IPv6 (which was given RFC status early in 2004).

We are still in the stage that only knowledgeable early adopters can set-up an IPv6 home network. An important step will be when broadband modems and routers (wired as well as wireless) can be configured to use IPv6 in the home and support tunneling on IPv4 to IPv6 services. While some ISPs offer IPv6 services the access networks are still on IPv4. For the consumer world these solutions should be easy to install and to manage, e.g. through adaptive appliances and auto-configuration. The ideal goal is to have native IPv6 services to end customers. In the meantime methods for (tunneled) access over existing IPv4 infrastructure are desirable. IPv6TF-SC members are involved in standardizing these methods in the IETF through IST research project work.

Current consumer applications are based on sessions where the connection is initiated from within the home. However, many applications (such as VoIP, remote monitoring, web cam access or video calls) would benefit from connections being initiated from the outside *into* the home. This would be impossible or at least difficult in situations where NAT is used. IPv6 creates an opportunity for new classes of application, it is possible not only to reach external services but also applications and services can be reached from outside (e.g. from mobile handsets), or - under proper control (easy-to-use security mechanisms are required) - by others.

The usage of Wi-Fi, Bluetooth, together with new technologies like PLC, will facilitate home automation, possibly via OSGi gateways, already being developed by a few IST projects. Consequently this will increase the deployment of home networks and home appliances with embedded IPv6 features, even small GRIDs, Personal Area Networks, and at the end facilitate the enabling of the Ambient Intelligence concept, described in the next section.

Besides that the v6ops working group of the IETF is working to speed up the introduction and support of IPv6 in home networking, offering recommendations about how IPv6 could best be implemented in unmanaged and home network scenarios.

Some early announcements about IPv6-based commercial services and products related to this have already been made by several entities, including European companies.

3.3.9 Ambient Intelligence

Ambient Intelligence (AmI) has been described as a vision of the Information Society where the emphasis is on greater user-friendliness, more efficient services support, user-empowerment, and support for human interactions, where people are surrounded by intelligent intuitive interfaces embedded in the environment. Since we are talking here about the Information Society as a whole we should realize that this has an impact on telecom, home appliances, business and industrial applications, healthcare and vehicles.

To make this possible Ambient Intelligence depends on seamless networking. There will be a need to be a large number and variety of devices, within spaces and as part of the electronic outfit, communicating with each other and with services. For this communication a variety of networks (wired as well as wireless) will be used, which will need to operate seamlessly as one logical network for the applications and the users. Different devices would roam across multiple networks. Interleaving such networks is a challenging task, but can be made easier by avoiding use of private IP addressing (common in IPv4 with NAT) by adopting IPv6.

The needs expressed above stress again the requirement for the address space, autoconfiguration (plug and play), ad-hoc networking, security, and mobility aspects offered by IPv6. Steps have to be taken in several domains such as infra-structures covering wide area, local area and personal networks, devices and services (e.g. location and situational awareness, identity management, etc).

3.3.10 Smart Tags

RF-ID is one of the new application areas that are being investigated in terms of opportunities for adoption with IPv6.

There are several ongoing activities on this field and Nokia Japan have already exhibited a technical demonstration model of a name-card sized PDA that supports Wireless LAN and includes an RF-ID reader. It realizes an easy-to-use security system by configuring the network setting of the PDA using information obtained from the RF-ID tag the user is wearing.

A bracelet with a built-in RF-ID tag identifies the user. Each RF-ID tag contains a unique IPv6 address and a pre-shared key for IPsec. The PDA reads the information and automatically reconfigures its own address to prepare for the new IPsec session.

It is important to note here that RFID is simply a technology to identify something, by attachment of an RFID tag. IPv6 becomes important where either the device tagged has IP connectivity, or the reader for the tag needs to have global IP connectivity.

3.3.11 Security

There are many aspects to IPv6 and security.

Some early commercial IPv6 firewall products are now available, e.g. from 6WIND, Cisco (basic ACLs), Nokia, Checkpoint and NetScreen among others, but their functionality is currently limited (e.g. in not allowing scanning of certain IPv6 headers, or not having stateful operation modes). Microsoft already offers a personal firewall in XP SP1.

A new challenge lies in enabling IPv6 access for peer-to-peer applications where firewalls would otherwise be blocking the traffic. Such end-to-end usage may currently be prevented by a site's security policy (or may involve the use of NAT as a "security" measure). Current policies tend to be site-to-site or device-to-site, rather than device-to-device.

The new SEINIT IST FP6 project has a broad brief to study IPv6 and security and to publish new frameworks appropriate for an IPv6 environment. This project should be a reference point for IPv6 security issues.

The Euro6IX IST project is working on deployment of an IPv6 PKI and IPv6 VPNs.

Euro6IX has also started a new interesting activity regarding new distributed security models for IPv6, considering the end-to-end paradigm with the enterprises and individuals interest, with a requirements draft already submitted to the IETF.

One open topic is the availability of commercial IPv6-enabled IDS (Intrusion Detection Systems) tools. Euro6IX and 6NET are among the projects working in this area.

3.4 Development of IPv6 in the World

While IPv6 in Europe is only slowly gaining momentum, IPv6 is continuing to gain rapid interest in the Asia Pacific region. Due to restraints in the growth of IPv4 address space, the limitations of IPv4 put a growing limitation of the growth of the Internet in the important Asia Pacific economies, in particular in China, Taiwan, Korea and Japan.

In the Americas, the interest in IPv6 is growing slowly but steadily. Recent reports suggest that IPv6 will start to take up so rapidly, that there is the danger of a divide in the of Internet users: Those with IPv4 and those with IPv6. It is therefore essential to assure that the growth in IPv6 is happening all over the Internet with comparable speeds.

The following picture gives an overview on the development of major IPv6 initiatives worldwide.

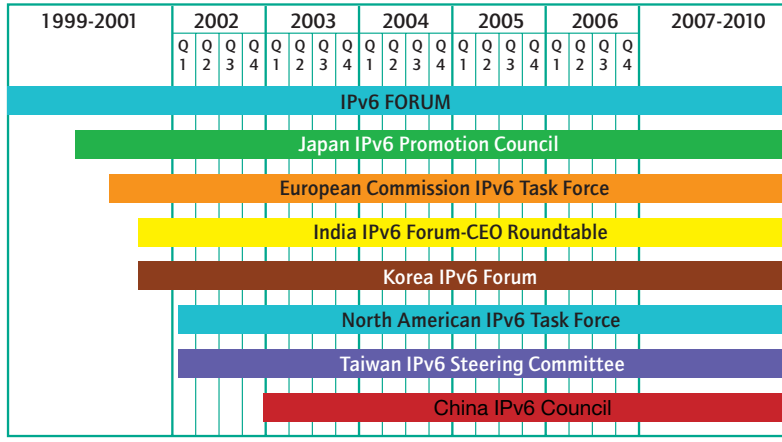

Figure 3.7: Major IPv6 Activities Worldwide

The following picture gives an overview on the current status of IPv6 deployment in major economies worldwide.

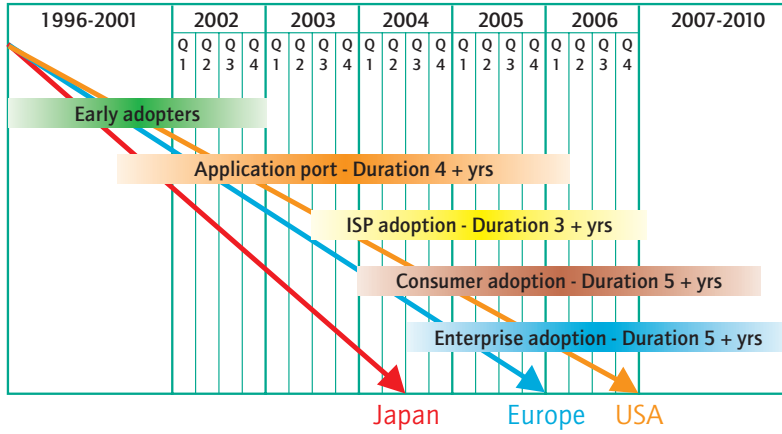

Figure 3.8: Major IPv6 Activities Worldwide

The Japanese lead in IPv6 technology is marked. Indeed, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) of Japan, working towards "New, Japan-Inspired IT Society" (FY2004 IT Policy Principles), indicates that their IPv6 expertise is one of their competitive advantages, key for realization of a ubiquitous network society. Consequently MPHPT will address advancement of the Internet, including promotion of IPv6.

Furthermore, on September 8, 2003, the second China-Japan-Korea IT Ministerial Meeting was held at Shilla Hotel, Cheju, Republic of Korea. Attendees from Japan included Mr. Katayam Toranosuke, Minister for Public Management, Home Affairs, Posts and Telecommunications; Vice-Minister Nabekura Shin'ichi; Mr. Oku, Director of International Cooperation Division, and others; from China, Mr. Wang Xudong, Minister of Information Industry; Mr. Qu, Deputy Director-General of Foreign Affairs Department, and others; and from Korea, Dr. Chin Dae-Je, Minister of Information and Communication; Dr. Yang, Director-General of International Cooperation Bureau and others.

During the Ministerial Meeting part, acknowledging that ICT is an indispensable infrastructure in order to develop Asia and enhance mutual ties, and that the cooperation among the three countries accelerates the deployment of broadband platforms through Asia, the three ministers exchanged opinions on wide-ranging topics including development and cooperation through establishment of new cooperation models for the ICT field. Upon conclusion of the meeting, toward further development of the ICT field, the three ministers agreed that the three countries should promote cooperation in the seven information and communications areas, such as 3G and the next-generation (4G) mobile communications systems, the next-generation Internet (IPv6) and information security; the three ministers then signed the Arrangement.

This meeting continued with the Japan-China ICT Ministers Bilateral Meeting among Minister Katayama and Minister Wang of MII, China, which exchanged opinions on bilateral cooperation in the ICT field. It included the strengthening of cooperation under the scheme of Japan-China ICT partnership, cooperation on IPv6 and introduction of 3G into China. Regarding Next-generation Internet (IPv6), the goals include: Exchange of information and joint hosting of seminars for the promotion of IPv6, cooperation in R&D and standardization of IPv6, development and promotion of IPv6 application services, exchange of policies and experts on IPv6, establishment of a Working Group in order to promote the abovementioned cooperation.

As a consequence, several companies from those countries increased their cooperation on these fields.

One more immediate result of this cooperation is the cooperation among Japan and China in order to jointly test 4G networks.

In addition, in November 2003, the South Korean Ministry of Information and Communication (MIC) unveiled the plan to foster Broadband convergence Network (BcN) infrastructure, indicating that for BcN to be successful, it must provide a high quality of service, security, and sufficient Internet protocol (IP) addresses using IPv6 [17].

In the same direction, coincidently with the Global IPv6 Service Launch Event, in one of the first cross-continent agreements, the EU agreed to work with South Korea to develop applications for IPv6.

3.4.1 Non-European IPv6 Task Force Initiatives

Here we summarize the statuses and initiatives of IPv6 TFs around the world. All these regions were represented at the IPv6 Global Service Launch Event in Brussels in January 2004.

3.4.1.1 Asia Pacific

The Asia Pacific IPv6 Task Force [18] was launched as a consequence of the IPv6 Summer Retreat meeting in Seoul (23rd August 2003), with the participation and cooperation of IPv6 TF-SC members.

In the region the most active countries are Japan, Korea, India, Taiwan, China and Malaysia. All of them have different related activities and initiatives.

In Japan the e-Japan Priority Policy Program that was established in March 2001 is very relevant. The Program states that it will realize an Internet environment equipped with IPv6 by 2005 where everyone can receive, share and transmit diverse information securely, promptly and easily, regardless of location. With current ongoing cooperation with non-governmental organizations, the Japanese IPv6 Promotion Council is determined to contribute in the most effective manner.

The Japanese IPv6 Promotion Council was the first entity in the world that achieved the corresponding government embracement of IPv6. In fact, the history of this group is a continuous history of achievements.

They organized the 1st IPv6 Application Contest in 2003, and the IPv6 Task Force was invited to participate. The 2nd Appli-Contest was launched in May 2004.

The award delivery ceremony was organized in a joint ceremony simultaneously in Madrid and Tokyo, during the Madrid 2003 Global IPv6 Summit.

Members of the EC IPv6 TF attended and presented at the EuroIndia 2004 event in New Delhi. A number of new contacts and potential collaborations have been seeded as a result of this activity, including a new proposal for dissemination of the work of IST IPv6 projects to Indian academic and commercial organizations.

3.4.1.2 North America

The NAv6TF [19] is an open group, accepting members from all geographies (not just North America), and all members of the NAv6TF represent themselves as individuals, not their companies.

The EC IPv6 Task Force helped in the creation of the North American IPv6 Task Force to focus on the adoption of IPv6 to the US government and the Department of Defense.

The following actions were undertaken:

- Meeting with Richard Clarke, Chair of the US Cybersecurity initiative Oct 17, 2002 in Boston. Latif Ladid (EC IPv6 TF chairman) presented the impact of IPv6 on security and privacy [20].
- Meeting with Howard Schmidt, co-chair of the US Cybersecurity initiative Nov 8th, 2002 in Washington. Latif Ladid presented the draft of the NAv6TF's Response to U.S. National Security.

This action has led to the inclusion of IPv6 in the final recommendations document: The National Strategy to Secure Cyberspace, which led to the decision of the DoD to announce adoption of IPv6-capable products. "The National Strategy to Secure Cyberspace is part of our overall effort to protect the Nation. It is an implementing component of the National Strategy for Homeland Security and is complemented by a National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society, the federal government, state and local governments, the private sector, and the American people" [21].

In June 13th, 2003, the DoD announced their strategy towards gradually implementing IPv6, requesting that all the acquisitions after September 30th 2003 should be IPv6-Ready. The complete deployment will be done by 2007. The EC IPv6 TF was represented in discussions with the DoD at the US IPv6 Summit event in June 2003.

A North American IPv6 Backbone Network Pilot, Moonv6 [22], has been deployed. The Moonv6 project is a collaborative effort between the North American IPv6 Task Force (NAv6TF), the University of New Hampshire - InterOperability Laboratory (UNH-IOL), the Joint Interoperability Testing Command (JITC) and various other DoD agencies, and Internet2. Taking place across the US at multiple locations, the Moonv6 project represents the most aggressive collaborative IPv6 interoperability and application demonstration event in the North American market to date.

In October 2003, the Commerce Department announced the launch of a federal government task force to study how deployment of a new industry-developed version of the Internet Protocol, known as IPv6, will affect competitiveness, security and the needs of Internet users [23].

In January 2004, the Task Force released a Request for Comments on the costs and benefits of a transition from IPv4 to IPv6.

In cooperation with the NAv6TF and the IPv6 TF-SC, a workshop on Consumer Electronics was organized in Las Vegas, at CES (Consumer Electronics show), in January 2004.

3.4.1.3 Latin America and Caribbean

Coincidently with the 6th LACNIC meeting, in Montevideo (Uruguay), 29th of March to 1st April 2004 the FLIP-6 (First Latin American IPv6 Forum) was organized, with the support and participation of the IPv6 TF-SC.

Several relevant organizations supported this meeting, as a precursor to the implementation of the IPv6 Task Force in Latin America and the Caribbean [25].

The aim of this Forum was to encourage and promote the adoption of the IPv6 protocol within the region covered by LACNIC through the exchange of experiences relating to this subject.

The Forum targeted a wide group of participants, including professionals working within the academic and commercial areas, university networks, ISPs, NAP operators, ccTLDs, etc.

Subsequent meetings are being organized already. In addition, a few countries started already related activities, with Cuba, Mexico and Brazil being the most advanced, but also strong R&D activities are being organized in most of the countries.

3.5 Conclusions

The setup of the European IPv6 Task Force has been a key driver for the fostering of localized similar activities across Europe and the rest of the world, which have been very relevant in terms of achieving worldwide press coverage about IPv6 and the high number of new products and services supporting it everywhere.

Is also a remarkable achievement that worldwide there is a growing take-up of IPv6 in industry and governments, including its consideration in private and public tenders. First business "because is IPv6-Ready", can be already accounted.

While IPv6 was generally not considered as something "going to happen soon" just four years ago, the picture has radically changed since just a couple of years, when the IPv6 Task Forces increased its presence worldwide and achieved a high impact in the penetration in several key industry sectors, not just in the field of the Internet Service Providers.

3.6 Acknowledgements

This section has been contributed by Jordi Palet (Consulintel), and the rest of the co-authors of the IPv6 Task Force Steering Committee Final Report [26].

3.7 References

[1] http://www.eu.ipv6tf.org/PublicDocuments/IPv6TF-Infra.pdf
[2] http://www.eu.ipv6tf.org/PublicDocuments/IPv6TF-Mobilewireless.pdf
[3] http://www.eu.ipv6tf.org/PublicDocuments/IPv6TF-Apps.pdf
[4] http://www.eu.ipv6tf.org/PublicDocuments/IPv6TF-Trials.pdf
[5] http://www.eu.ipv6tf.org/PublicDocuments/IPv6TF-Report.pdf
[6] http://www.eu.ipv6tf.org/PublicDocuments/com2002_0096en01.pdf
[7] http://www.eu.ipv6tf.org/PublicDocuments/consejo_europeo-barcelona.pdf
[8] http://www.eu.ipv6tf.org/PublicDocuments/ipv6tf_phase2_v5.pdf
[9] http://www.eu.ipv6tf.org/PublicDocuments/status_and_required_v1.8.pdf
[10] http://www.ist-ipv6.org/modules.php?op=modload&name=News&file=article&sid=187
[11] http://www.global-ipv6.net
[12] http://www.eu.ipv6tf.org/PublicDocuments/ipv6-global-service-launch-03.pdf
[13] http://www.ipv6forum.com/navbar/papers/IPv6-an-Internet-Evolution.pdf
[14] http://www.6power.org
[15] http://www.isoc.org/briefings/013
[16] http://www.ist-ipv6.org/modules.php?op=modload&name=News&file=article&sid=344
[17] http://www.ist-ipv6.org/modules.php?op=modload&name=News&file=article&sid=190
[18] http://www.ap.ipv6tf.org
[19] http://www.na.ipv6tf.org
[20] http://www.nav6tf.org/slides/repository.html
[21] http://www.whitehouse.gov/pcipb
[22] http://www.moonv6.org
[23] http://www.ntia.doc.gov/ntiahome/press/2003/IPv6_101403.html
[24] http://lacnic.net/en/flip6.html
[25] http://www.lac.ipv6tf.org
[26] http://www.ipv6tf-sc.org/html/public/ipv6tf-sc_pu_d4v1_9.pdf

4 IPv6 and Broadband

4.1 IPv6 Site Multi-Homing

4.1.1 Introduction

A site is multi-homed when it obtains Internet connectivity through two or more service providers. Through multi-homing an end-site improves the fault tolerance of its connection to the global network and it can also optimise the path used to reach the different networks connected to the Internet.

4.1.1.1 Multi-Homing in IPv4

In IPv4, the most widely deployed multi-homing solution is based in the announcement of the site prefix through all its providers, as it is described in Figure 4.1.

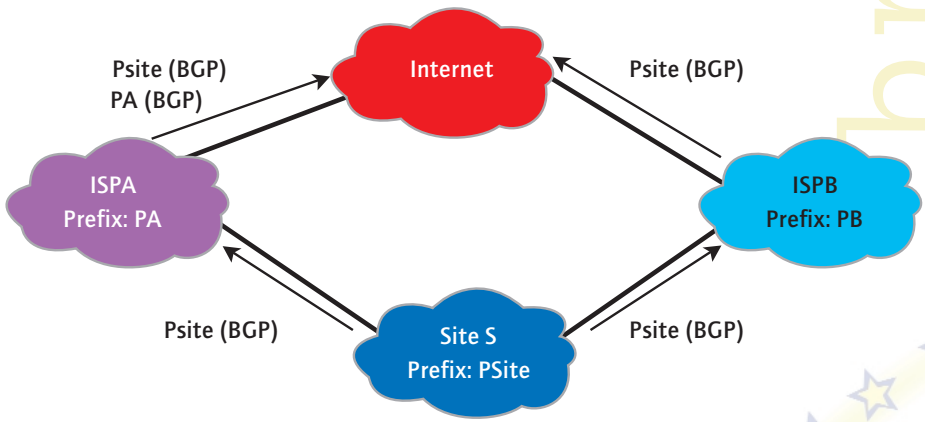

Figure 4.1: **IPv4 Multi-Homing Solution**

In this solution, the site S obtains a prefix allocation directly from the RIR (Regional Internet Registry) or from one of its providers (ISPA or ISPB). Then, the site announces this prefix (PSite) to its providers using BGP. ISPA and ISPB announce the prefix to their upstream providers and so on, so that the route is announced in the default free zone. It must be noted that even when PSite is part of one provider's aggregate, PSite has to be announced separately in order to avoid that longest prefix match rule diverts all the traffic to the provider announcing the more specific route.

This mechanism presents many advantages, such as good fault tolerance capabilities, including preserving established connections throughout an outage, since alternative routes are used without end node perception. However, each multi-homed site using this solution contributes with routes to the default free zone routing table, imposing additional stress to already oversized routing tables. For this reason, more scalable multi-homing solutions are being explored for IPv6.

4.1.1.2 Provider Aggregation and Multi-Homing

In order to reduce routing table size, the usage of some form of provider aggregateable addressing is considered. This means that sites obtain prefixes which are part of their provider allocation, so that its provider only announces the aggregate to their non-client peers, as it is illustrated in figure 4.2. Most aggressive aggregation is achieved by aggregating end-sites into their provider prefixes, so provider aggregation of end-sites is deemed necessary. Further aggregation i.e. direct provider prefixes aggregated into transit provider prefix, provides much more moderate aggregation benefits while it does present some deployment challenges such as multi-homed provider issues, so its adoption remains uncertain.

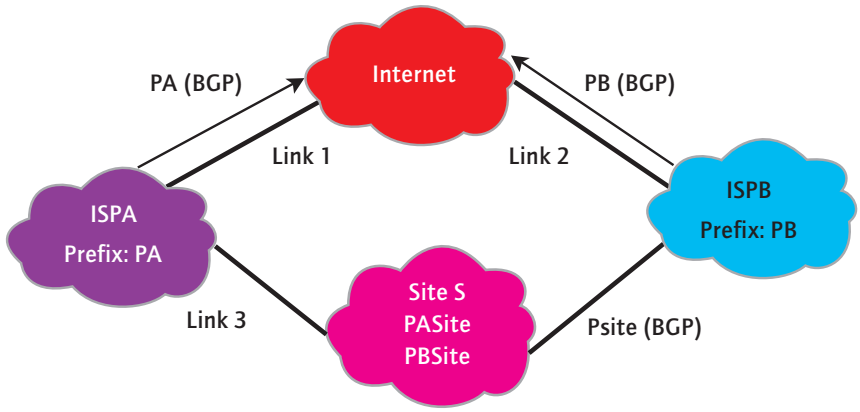

Figure 4.2: **Provider Aggregation of End-Site Prefixes**

When provider aggregation of end-site prefixes is used, end-site host interfaces obtain one IP address from each allocation, in order to benefit from multi-homing capabilities, since ISPs will only forward traffic addressed to their own aggregates. Note that ISPs only announce their aggregates to their providers, and they do not announce prefixes belonging to other ISP aggregates. This configuration presents several concerns and these will be presented next.

Increased connection establishment time in case of failure: When Link 1 or Link 3 becomes unavailable, addresses containing the PASite prefix are unreachable from the Internet. New incoming (from the site perspective) connections addressed to PASite addresses will suffer from an increased establishment time, since the connection request will timeout until the alternative address, containing PBSite prefix can be used.

Established connections will not be preserved in case of outage: If Link 1 or Link 3 fails, already established connections that use addresses containing PASite prefix will fail, since packets addressed to the PASite aggregate will be dropped because there is no route available for this destination. Note that an alternative path exists, but the routing system is not aware of it.

Ingress filtering incompatibility: Ingress filtering [1] is a widely used technique for preventing the usage of spoofed addresses. However, in the described configuration, its usage presents additional difficulties for the source address selection mechanism and intra-site routing systems, since the exit path and source address of the packet must be coherent with the path, in order to bypass ingress filtering mechanisms.

These difficulties make it clear that additional mechanisms are needed in order to allow the usage of provider aggregateable addresses while still providing multi-homing benefits.

4.1.2 Developing an IPv6 Multi-Homing Solution: IETF Multi6 Working Group

The multi6 working group has been chartered [2] within the IETF to design IPv6 multi-homing solutions that provide the required scalability and that are capable of overcoming the described difficulties.

Initially, multi6 has generated a document describing the goals for multi-homing [3]. Basically, an IPv6 multi-homing solution has to provide the features provided by the current IPv4 solution, that is, fault tolerance against multiple failure modes including the preservation of established connection through an outage, load sharing capabilities, possibility to perform some form of policing, simplicity and compatibility with currently deployed ingress filtering mechanisms.

Additionally, an IPv6 multi-homing solution has to provide the required scalability and has to be deployable, meaning that the impact of the solution on the current installed base of routers and hosts has to be limited.

Since the goals have been stated, the working group has been analysing possible approaches.

4.1.2.1 Session Survivability

The preservation of the established communication through an outage has been identified as the most challenging problem.

Several approaches have been proposed to provide transport layer session survivability, among which we can find the following:

Transport layer solutions: A possible approach is to modify the transport layer, essentially TCP, in order to support multiple IP addresses per connection. Current TCP specification identifies a connection by the combination of source and destination addresses and source and destination port numbers and protocol. The idea is to modify TCP in order to recognize packets with alternative addresses as belonging to the established connection as presented in [4]. Note that there already exist transport protocols such as SCTP or DCCP that support this type of functionality, so their usage in multi-homed environments should be straightforward.

Locator identifier split approaches: Another approach is based on the conception that the difficulty of this problem is caused by the multiple roles that IP addresses play in the Internet architecture. Essentially, IP addresses play two roles in the current architecture: the locator role and the identifier role. IP addresses are locators since they contain information about where in the topology a node is located. IP addresses are identifiers, since they are used by transport and upper layers to identify the nodes involved in a communication. When using provider aggregateable addresses, each node within the multi-homed site is simultaneously mapped to multiple locations of the topology, since it has multiple IP addresses assigned to it. In order to preserve an established communication when an outage occurs, the communication has to be moved to an alternative path that is represented by the IP address assigned by the alternative provider.

However, packets addressed to the alternative IP address will not be recognized as belonging to the established communication because the identifier of the communicating node presented to the transport and upper layers (i.e. the IP address) has changed.

So, solutions to this problem seem to require a decoupling of those two roles, that is, the usage of an identifier by transport and upper layers that can be mapped to multiple locators in the IP layer to actually reach a given node.

Among the different proposals that attempt to split the locator and the identifier role in the IP architecture, we can find proposals that create a new namespace for the identifiers, proposals that just use a regular IP address as the identifier and proposals that reserve some part of the IP address space for the identifiers.

Examples of the first case are HIP [5] and SIM [6]. Examples of the second case are LIN6 [7] and CB64 [8]. Examples of the third case are NOID [9] and ODT [10].

The main difficulty that appears when attempting to split the locator and the identifier roles is security. As long as the identifier is the locator the Internet routing architecture provides a minimum level of security that packets are routed to the desired end node. This is because we identify the desired end node by its locator (the IP address) and the routing system makes sure the packet is routed to the correct location i.e. end node. When we separate the location from the identity, the routing system only guarantees that the packet is routed to the correct location, but it does not provide any guarantees about the identity of the node located in that place. So splitting location and identity enables redirection attacks, where the attacker hijacks the victim's identity and redirects its traffic towards the attacker (or someone else's location). A multi-homing threat analysis can be found in [11].

4.1.2.2 Ingress Filtering Compatibility

Another issue that has to be addressed when designing a multi-homing solution is the compatibility with ingress filtering. Ingress filtering is performed by ISPs for security reasons and it essentially consists of verifying that the source address of the packets received from a customer contains the prefix delegated by the ISP to that customer. This technique prevents source address spoofing. In our multi-homing scenario, where every host will have one address from each ISP, ingress filtering may cause some problems because the source address selected by the host may not be compatible with the exit ISP selected by the intra-site routing system. In the case that the source address does not contain the prefix of the selected ISP the packet is discarded. In order to guarantee ingress filtering compatibility, additional tools are required. Different approaches can be used to overcome this issue as presented in [12]. Some of them are briefly described next.

Relaxation of the source address checks: An obvious way to overcome address filtering is to allow the end-site to inform the ISP about its multiple prefixes so that the ISP configure its filters to allow such prefixes in packets coming from this particular customer. Such a procedure is suitable when a certain amount of trust between the ISP and its customers exists. For those cases where this level of trust is not possible, alternative approaches are required.

Source-address-based routing: Another possible approach is to let the host select the source address and then route the packet towards the correspondent ISP. This implies the adoption of source address based routing in the multi-homed site. A simpler possibility is to establish a mesh of tunnels between the exit routers, so that when a packet reaches the site border router, the router will forward the packet through its directly connected ISP if the address contains the appropriate source prefix or it will send it over a tunnel to the correct exit router.

Host-based exit selection: Another option is that the host sends the packet through the ISP that matches the selected source address. A way to achieve this is that the host sends the packets through a tunnel directly to the appropriate exit router, overruling the site exit router selection performed by the intra-site routing system.

Source-address rewriting at site exit router: Finally, another approach is to let the site exit router rewrite the source address of the packets in order to make them compatible with ingress filters. This implies some sort of cooperation from the host, since the packet will be altered.

4.1.2.3 Address Selection

Hosts in multi-homed sites will have multiple addresses. Not all of them may be reachable at the same time from any location. Moreover, it is expected that the performance obtained may vary depending on the address used to reach the multi-homed site (note that each address prefix is associated with a different ISP which may provide a different service). So, address selection is a critical issue in multi-homed environments. At least a multi-homing solution has to provide a mechanism to identify which one of the addresses of a host in the multi-homed site is reachable and use it to establish a communication. More advanced features may allow a performance based address (ISP) selection.

4.1.3 Summary

In this section we have presented the issues concerning the design of an IPv6 multi-homing solution. We have described the currently deployed IPv4 multi-homing solution and we have made the case why this solution cannot be directly adopted in IPv6. We have explained why the adoption of Provider Aggregateable addresses is required to guarantee the scalability of the IPv6 Internet. We have then described the difficulties to be considered when designing a multi-homing solution that is compatible with the usage of Provider Aggregateable addressing. We have identified the preservation of established connection, the provision of ingress filtering compatibility and the address selection. We have presented proposed solutions to these problems. There is still much work to be done in order to finish the design of a multi-homing solution for IPv6, but progress is being made and a solution will be available in the mid term.

4.1.4 Acknowledgements

This section was contributed by Marcelo Bagnulo (Universidad Carlos III de Madrid), Alberto García-Martínez (Universidad Carlos III de Madrid) and Arturo Azcorra (Universidad Carlos III de Madrid).

4.2 IPv6 over Broadcast

4.2.1 Introduction

Many broadcast systems are available today, allowing mass information delivery to large regions. They split into two main categories, satellite and terrestrial systems, differing in terms of coverage and required terminal capabilities, but often complementing each other for an optimal service deployment. Traditionally, broadcast systems have been used for TV-like services based on analogue and then digital transmissions of audio and video information.

With the ongoing convergence of the Internet and cellular systems, enabling new data and multimedia services to mobile users, the Internet Protocol (IP) is becoming the convergence layer for future communication systems. At the same time, exploiting the natural synergies of cellular and broadcast systems is now foreseen as an opportunity for enabling advanced interactive services to mobile users, while maximizing network efficiency. Naturally, efficient transport of IP-based services over broadcast is important to achieve this convergence.

In parallel, the transition of the Internet network protocol from IPv4 to IPv6 is on the way. This new version of the Internet Protocol is mainly aimed at overcoming issues due to the IPv4 address space depletion, and should facilitate the large scale deployment of new "peer-to-peer" or "always-on" applications both in fixed and mobile environments.

This chapter aims at investigating issues surrounding the effective transport of IPv6 over broadcast systems. Section 4.2.2 starts with a brief overview of the broadcast systems landscape, and discusses the existing support for transport of IP-based services in these systems. Section 4.2.3 revisits the broadcast cellular convergence, highlighting the foreseen advantages, the possible architectures, as well as some of the new functions required in the network. Finally, section 4.2.4 presents some of the issues with IPv6 over broadcast, as well as possible solutions currently investigated by the research and standards communities. Both IPv6 unicast and multicast transports are addressed.

4.2.2 Overview of Broadcast Systems

4.2.2.1 Existing Standards

Similar to cellular systems, broadcast systems, initially analogue, have evolved towards the digital paradigm during the last ten years. New standards have emerged; one of the most predominant being the set of Digital Video Broadcasting (DVB) standards developed by the DVB Project [13] and published by the European Telecommunications Standards Institute (ETSI).

The family of DVB standards covers satellite, cable and terrestrial broadcast systems. The DVB-S satellite transmission standard is based on a Quadrature Phase Shift Keying (QPSK) modulation technique. It was the first approved DVB standard in 1994, and is now the de-facto world satellite transmission standard for digital TV applications. DVB-C, for cable delivery, is based around a Quadrature Amplitude Modulation (64-QAM) and is closely related to DVB-S. Finally, DVB-T, for terrestrial broadcast systems, is based on Coded Orthogonal Frequency Divisional Multiplexing (COFDM) and QPSK, 16-QAM and 64-QAM modulation schemes. The MPEG-2 standard, from the Moving Pictures Experts Group (MPEG), is the basis for video, audio and data transmission in DVB. That is, any transport of information over DVB relies on MPEG-2 Transport Stream (MPEG-2 TS).

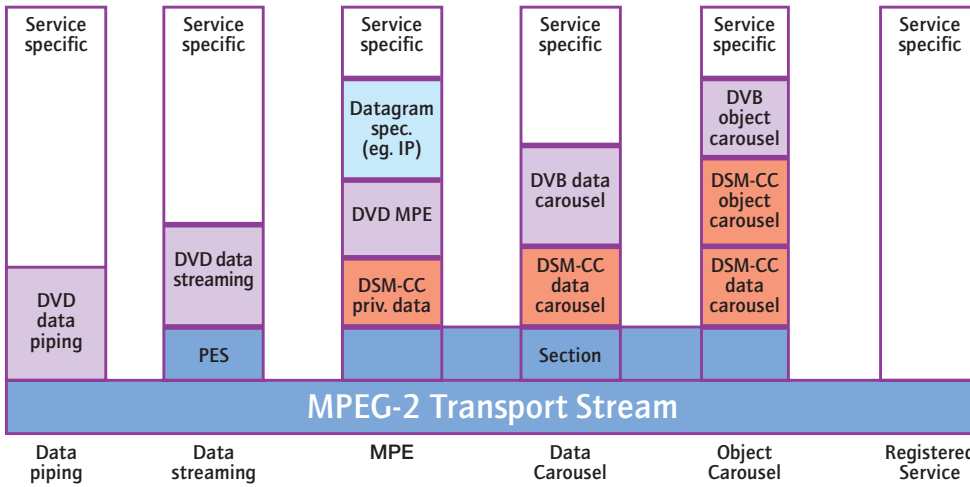

Figure 4.3: Data Encapsulation Modes in MPEG-2 Transport Stream

Figure 4.3 shows the various data encapsulation methods specified by the DVB standards [14]. They offer various levels of sophistication, selected according to the service requirements:

- **Data Piping:** This profile is a minimum overhead, simple and flexible profile that makes no assumptions concerning the format of the data being sent. Only a minimum set of functions including MPEG-2 TS Packet Identifier (PID) filtering, packet reassembly, error detection and link encryption are provided at the receiver side. The encapsulated user data stream can be either unstructured or organized into packets. It may by any type of protocol, such as IP or Ethernet. This profile supplies limited support, and may require specific hardware or software to be developed depending on the service to be supported.

- **Data Streaming:** This profile maps an IP packet into a single Packetized Elementary Stream (PES) packet payload. PES is a format of MPEG-2 TS packet payload usually used for video or audio information. PES supports unicast and multicast data services that require a stream-oriented delivery of data packets.

- **Multi-Protocol Encapsulation (MPE):** This profile uses the DSM-CC MPEG-2 format, carried in so-called private sections of MPEG-2 TS packet. Specific sections processing hardware can be exploited at the receiver to perform a first-level filter of the packets received. MPE is suitable for transmitting non-cyclical datagrams in an asynchronous way. MPE sections cover unicast, multicast and broadcast transmission and have been optimised to carry IP datagrams. Nevertheless, MPE sections can also be used to transport any other protocol (e.g. IPv6, Address Resolution Protocol – ARP, and all protocols over IP) by LLC/SNAP encapsulation. For example, for some target architectures, it will be better to encapsulate IP datagrams directly into MPE sections. For other ones, it will be preferable to encapsulate Ethernet Frames using IEEE 802.1 LLC/SNAP encapsulation or IEEE 802.2 LLC/SNAP encapsulation. As using IP datagrams in MPE sections any kind of IP applications can be implemented on a DVB support. Moreover the MPE section header contains MAC addresses (IEEE format) in order to address receivers and to perform hardware filtering at the receiver level. In conclusion, MPE gives a fully specified way to broadcast IP over DVB. MPE is currently a widely used scheme, supported by most of DVB-IP Gateway equipment vendors. Support for IPv4 is available in DVB products for several years already, while equipment offering commercial-grade support for IPv6 has only appeared recently.

- For cyclical data contents, data carousels or object carousels could be used.

Other types of broadcast systems include for instance the Advanced Television Systems Committee (ATSC) [15] standards that are also exploiting MPEG-2 TS transport. Similarly to DVB, ATSC standards have been defined for satellite, cable and terrestrial transmissions.

4.2.2.2 Evolution Trends

4.2.2.2.1 IP-Based Services

While broadcast systems are traditionally designed for video and audio transmission, the support of IP-based services has gained an increasing importance recently. In addition to IP multicast based audio or video streaming applications, new services have to be supported such as mass data push (e.g. web content) to broadcast receivers. This is known as IP Datacast (IPDC). As opposed to streaming, datacasting requires reliable transmission of the content.

4.2.2.2.2 Mobility

In addition to the IP-based services trend, the need for broadcast systems to be able to accommodate receivers' mobility is foreseen as critical for the near future. Indeed, some mobile phone manufacturers are already developing today some combined cellular-broadcast devices (e.g. GPRS-DVB) for mobile users to access broadcast services. Receiver mobility introduces new issues both at the radio and system level.

For instance in DVB-T, issues at the radio level coming from mobility include additional fading, versatile echoes varying in amplitude, delay and Doppler effect. The last one being the most predominant issue due to the relative speed of the receiver. Indeed, frequency shift from Doppler effect introduces Inter-Carrier Interference (ICI) and Inter-Symbol Interference (ISI), resulting in a degradation of the Carrier over Interference ratio (C/I), that is strong signal degradation. Various studies [16] have been conducted and have identified optimum DVB-T configuration providing the maximum data-rate for the given Bit Error Rate (BER) estimated to offer a satisfying quality to mobile receivers.

At the system level, mobility issues relate to the need for a DVB-T receiver moving from one DVB-T cell to another to maintain service continuity. More precisely, in a multi frequency network, the receiver has to tune a new frequency and, eventually, to get the new transport stream providing the same service, when it performs a handover. Various mechanisms have been defined in DVB-T to facilitate receiver handover. They rely on additional signalisation information (DVB-SI [17]) containing some network and service descriptors, broadcast by the DVB-T cells. [18]

Nevertheless, in order to make DVB-T more suitable for mobile receivers, an extension called DVB-H has been specified by the DVB project in January 2004. DVB-H stands for Digital Video Broadcasting Handhelds. It includes four extensions to the DVB-T standard.

- **Time Slicing** for reducing the average power consumption of the terminal and enabling smooth handover (up to 95% power reduction).
- **MPE-FEC** for improving C/N-performance and Doppler performance in mobile channels and improving tolerance to impulse interference.
- **4k-mode** for improving single antenna reception in medium to large SFNs and adding flexibility to the network design.
- **Extended TPS**-bit signalling to allow enough information of the service carried in a robust way to enhance and speed up service discovery and to conserve the free TPS-bits.

4.2.2.2.3 Interactive Applications

Another trend is the foreseen potential of interactive applications over broadcast, requiring a return path to complement the broadcast system. This return path can be provided for instance by a separate cellular system (e.g. GPRS/UMTS) or even by a reverse satellite link such as DVB-RCS [19]. DVB Return Channel via Satellite (DVB-RCS) forms the specification for the provision of the interaction channel for geostationary (GEO) satellite interactive networks. In particular, some efforts [20] are ongoing to integrate DVB-S and DVB-RCS into a unified satellite system.

4.2.3 Broadcast Cellular Convergence

The flexible integration of broadcast and cellular systems into a hybrid system has been actively researched for several years already, especially as part of the European Information Society Technologies (IST) 5th and 6th Framework Programme projects [21]. The objective is to exploit the natural synergies of cellular and broadcast systems in order to enable new type of services, as well as to maximize network efficiency.

More precisely, broadcast operators can take advantage of a cellular system to serve as a return path for mobile broadcast receivers. With such a return path, offering interactive broadcast services enriching the broadcaster bouquet is now possible. An example of such a service is for instance the broadcast of a high quality real-time football match through DVB-T, where some parts of the image on the receiver's screen is "clickable" and automatically connect the user (through the cellular system) to additional information related to the content being displayed, such as the biography of the players etc.

Implementing this vision, IP Data-Cast (IPDC) is a platform for convergence of services from mobile/cellular and broadcast/media domains. IPDC is an end-to-end broadcast system for delivery of any types of digital content and services using IP-based mechanisms. An inherent part of the IPDC system is that it comprises a unidirectional DVB broadcast path and a bi-directional mobile/cellular interactivity path. The DVB TM ad hoc group CBMS (Convergence of Broadcast and Mobile Services) has been set up to convert the "Commercial Requirements, IP Data-Cast in DVB-H" to IPDC technical requirements and specifications during 2004. The CBMS technical specifications will focus on network functions enabling service convergence and service roaming between broadcast and mobile domains. The service delivery system should be network independent to a great extent. All content is delivered in the form of IP-packets using IP-based mechanisms. The broadcast interface shall use only IPv6 packet format. In the unidirectional broadcast path DVB-H is the preferred broadcast bearer but the parallel use of "IPDC over DVB-H" with other systems should not be excluded. The interactivity path shall be a mobile/cellular solution (e.g. GSM / GPRS / UMTS). The specifications shall have a focus on (audio-visual content) services for mobile handheld terminal use. Mobile handheld terminal use assumes several resource limitations: terminals with low power consumption, small displays, limited processing power and memory size. Existing open standards and relevant ongoing work to become open international standards (e.g. Multimedia Broadcast / Multicast Service of UMTS - MBMS) shall be adopted if the development fits with the IPDC specification schedule.

From the cellular operator perspective, completing the point-to-point service of a cellular system - sometime also offering multicast and broadcast support such as MBMS - with a broadcast service (e.g. DVB-T) allows more flexible and efficient delivery of group services to mobile users, by optimising network and radio resource usage. The way by which network and radio efficiency can be achieved in a hybrid system is threefold:

1) The use of a broadcast delivery scheme to deliver the same service to a large group of receivers in a given area is obviously more efficient than multiple point-to-point connections.

2) The relatively small size of cellular cells, compared to a broadcast system cell, allows adapting more precisely the shape of the broadcast area (i.e. set of cellular cells) to the geographical region where receivers are located, thus optimising overall radio resources. Of course, intelligence is required in the network to dynamically control the spreading of the broadcast area. Parameters such as the density of receivers in a given region should be considered in this decision process.

3) Leverage on the hierarchical structure of a hybrid system to select the most suitable cell for broadcasting in a given area. For instance, an operator would optimize its network and radio resources by broadcasting a popular session in a given area through a single DVB-T cell rather than for instance ten UMTS cells covering the same region. Again, intelligence is required in the network to determine when a session should be redirected to another hierarchical level.

Several architectural approaches can be envisaged for hybrid networks: loosely coupled architecture, tightly coupled architecture, and an intermediate approach known as balanced coupled architecture [22]. Hybrid networks based on a loosely coupled approach consider co-operation between heterogeneous access networks, viewed as independent peers at the same level by a convergence network. In this scenario, independent operators, and even competitors, own the access networks and a convergence network chooses the best radio access system with respect to some predefined rules (cheapest access, less load, most appropriate support according data to deliver, etc…). In loosely coupled architecture, the convergence network acts as a mediation platform between the access networks. On the other hand, the tightly coupled approach provides integration of all radio systems without the need of having a third network. This is feasible in cases where only one operator is running all the different radio systems, or there is more than one partner but they have a trusted cooperation. An example of a tightly couple architecture of an UMTS/DVB-T hybrid system is the use of the UMTS Core Network to handle both the UMTS Terrestrial Radio Access Network (UTRAN) and DVB radio accesses. Another example could be the Satellite Digital Multimedia Broadcast System (S-DMB) [23], designed to complement the UMTS terrestrial cellular network with a satellite broadcast link.

Irrespective of the type of hybrid network architecture selected, new functions are required in the network in order to coordinate the distribution of traffic among the cellular and broadcast accesses, and thus take full advantage of their combination. These functions include:

- Transmission mode selection and switching: Ideally, for real-time group communications, the network should be able to switch the transmission mode between point-to-point (unicast) and point-to-multipoint (multicast/broadcast) depending on the popularity of the session; in order to optimize the network and radio resources.

- Hierarchical cell selection and switching: As explained before, a multicast communications may be more optimally delivered through a cell upper in the hierarchy – with a larger coverage – than through a set of smaller cells, when the number of receivers in the region exceeds a certain threshold.

Such functions require the network to collect the needed information in order to take the right decision and execute the switching. This includes for instance the type of users' active sessions, the users' location, the capabilities and current loads of the various accesses, terminal capabilities, etc.
Investigations of concepts and implementation approaches for these functions have started, for instance as part of the specification of the OverDRiVE project "group partitioning" function [22].

It is worth noting that the above-mentioned cell selection and switching function requires a form of interaction between the network and the terminal so that the latter is informed of the new cell to receive traffic from. New protocols such as the Network Access Co-ordination Protocol (NACP) [24], initially proposed for network-assisted Mobile IP handover, can be used to support this form of network-assisted handover for IP multicast sessions.

4.2.4 Issues of IPv6 over Broadcast

This section focuses on technical issues of IPv6 over broadcast. It also presents some of the possible solutions currently investigated by the research and standard communities. Both IPv6 unicast and multicast transports are addressed.

4.2.4.1 Issues of IPv6 Encapsulation over Broadcast

The first type of issue is related to the feasibility or overhead of transporting IPv6 packets over a broadcast link.

IPv6 [25] requires that all links in the network have a Maximum Transmission Unit (MTU) of 1280 bytes or greater. On any link that cannot convey a 1280-byte packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6. This minimum link MTU value imposed by IPv6 is not an issue for some broadcast systems, such as DVB-T MPE for instance where transport schemes standardized for Europe limit maximum section size to 4096 bytes. On the other hand, transmission of IPv6 packets is an issue with some other systems, such as some of the ATSC standards whose specifications limit the MTU to 1008 bytes.

In addition, even when transmission of IPv6 packets is allowed by the MTU size of the broadcast link, the encapsulation scheme used for IPv6 is sometime sub-optimal. A typical example is the use of the MPE profile in DVB, which results in significant overhead when encapsulating IP [26], mainly due to the fact that MPE has been designed with the requirement to support any type of data packet and not only IPv4 or IPv6. As broadcast of IPv4/v6 based services becomes more popular, link efficiency (i.e. small overhead) becomes critical. And thus the need for a specific encapsulation scheme optimized for IPv4/v6 packets. This has been acknowledged by the Internet and MPEG-2 networks community, and resulted in the creation of the ipdvb working group in the Internet Engineering Task Force (IETF) [27], whose one responsibility is to standardize lightweight encapsulation methods for transmission of IPv4/v6 datagrams over MPEG-2 networks (such as DVB). A first solution, called Ultra Lightweight Encapsulation (ULE) [28], has already been proposed. ULE defines an encapsulation mechanism for the transport of IPv4 and IPv6 datagrams (and other network protocol packets) directly over MPEG-2 Transport Streams (TS) as TS Private Data. It uses the Data Piping profile (see figure 4.3). It is worth mentioning that, as opposed to MPE, the method permits a single TS Packet to carry more than one IP packet.

4.2.4.2 Issues of IPv6 Unicast over Broadcast

Because of its unidirectional nature, a broadcast system is usually not well-suited for transport of unicast traffic. This is because point-to-point communications most of the time are duplex, and thus require IP packets to be exchanged in both directions (e.g. TCP-based application such a file transfer, web browsing). Anyway, support of unicast communication is sometime desired in order to extend the service offering. In such a situation, the following issues must be addressed.

First, the unidirectional broadcast link must be complemented with a return path, as a way to emulate a bi-directional link between the broadcast base station and the receiver. As explained before, this return path can be provided for instance by a separate cellular system (e.g. GPRS/UMTS). In order to emulate the bi-directional link, a dedicated IP tunnel implementing the uplink can be setup from the receiver, through the return system (e.g. cellular), to the IP subnet where the broadcast base station

is located. The Uni-Directional Link Routing (UDLR) [29] protocol has been standardized by the IETF to provide this support. UDLR enables the receiver to dynamically discover the IP address of the tunnel end point, located in the same IP subnet as the broadcast base station, and provides a virtual network interface emulating a bi-directional link (UDLR tunnel uplink, broadcast downlink) for the transparent operation of IP and other protocols like addresss resolution protocols. Such a return path will also allow for more flexible IP address assignment mechanism to be used, as opposed to static address configuration that may lack flexibility especially in mobile environment. Stateful address auto-configuration (e.g. DHCP) for IPv4 and IPv6 needs a return path to get the IP address from the server in the network. On the other hand, stateless address auto-configuration allows the receiver to auto-configure an IPv6 address without the need of the return path, by appending a unique identifier to the network prefix received in the Router Advertisements. If uniqueness of the identifier cannot be guaranteed a priori, the return path is then still needed to test the IPv6 address with the Duplicate Address Detection procedure [30, 31]. It is worth mentioning that the setup of the UDRL tunnel through the return system may not always be possible, for instance when the return system is an IPv4-only network with a Network Address Translator (NAT) deployed at its edge. This is a typical configuration of today's cellular system. The choice of the UDLR encapsulation method (GRE [32] or others) is thus critical, and may require the broadcast system to discover capabilities of the return system. Such functionality is currently not supported by UDLR.

Efficient ways to achieve IP address resolution on top of a broadcast system are being investigated. For instance, the ipdvb working group in IETF is chartered to define appropriate standards to support transmission of IPv4 and IPv6 datagrams on MPEG-2 transport sub-networks such as DVB and ATSC. One of the objectives is to design flexible mechanisms allowing the mapping of an IP address to a broadcast Layer-2 identifier, such as a Packet ID (PID) and specific transmission multiplex in the case of MPEG-2 transmission networks. Various solutions have already been proposed in [33].

In the context of multi-technology mobile devices (e.g. UMTS/DVB-H), Mobile IPv6 must be able to operate with unidirectional broadcast system in order to allow those devices to receive unicast traffic, addressed to their home address, at the care-of address obtained from the broadcast network. Again, UDLR allows running Mobile IPv6 over a unidirectional link, at the cost of additional header overhead and a longer routing path due to the nesting of the Mobile IPv6 tunnel into the UDLR tunnel.

Coming to transport protocols, TCP was originally specified when links had small bandwidth-delay product, packet losses were occasional and links were quite symmetric. On the other hand, a unidirectional broadcast link coupled with a return path (typically DVB-T with cellular system) introduces high asymmetry between the forward and return directions in term of bandwidth and delay; thus acting as a Long Fast Network (LFN), where both bandwidth and delay are high. In such environment, the acknowledgement driven TCP sending rate can dramatically decrease, and does not allow taking full advantage of the high date rate of the downlink. TCP performance over LFN has mainly been researched in the context of satellite links, but some studies also addressed the specific case of terrestrial broadcast [34].

4.2.4.3 Issues of IPv6 Multicast over Broadcast

Issues of IPv6 multicast over broadcast naturally include general issues of IPv6 multicast, which are under investigation today, such as multicast address delegation, inter-domain multicast routing, multicast security, or mobile multicast. Most of these issues are addressed in various IETF working groups, such as v6ops, mboned, bgmp, msec, rmt, or mip6.

4.2.4.3.1 Multicast Address Allocation

Protocols, such as the Multicast Address Dynamic Client Allocation Protocol (MADCAP) [35], have been defined to allow hosts to request multicast addresses from multicast address allocation servers. However, dynamic inter-domain multicast address assignment may be complex in a global network encompassing a large number of multicast domains. This has been addressed, in the context of IPv6, by allowing for unicast-prefix-based allocation of multicast addresses [36] (RFC3306). In IPv6, by delegating multicast addresses at the same time as unicast prefixes, network operators will be able to identify their multicast addresses without needing to run an inter-domain allocation protocol.

4.2.4.3.2 Inter-Domain Routing

Some basic solutions for IPv4 multicast inter-domain routing, such as the Multicast Source Discovery Protocol (MSDP) [37] and the Multi-protocol extensions for BGP-4 (MBGP) [38], are available today. They complement existing intra-domain multicast routing protocols, such as the Protocol Independent Multicast - Sparse Mode (PIM-SM) protocol [39]. Similarly, current best practices for deployment of inter-domain routing are also available [40]. However, these mechanism lack of flexibility and are unlikely to scale for the long term. The Border Gateway Multicast Protocol (BGMP) [41] is a scalable inter-domain multicast routing protocol under definition, which addresses these problems. At the same time, there are some issues concerning the deployment of IPv6 multicast. As explained in [42], currently, global IPv6 inter-domain multicast is impossible except using Source Specific Multicast (SSM), because there is no way to convey information about multicast sources between PIM-SM Rendezvous Points (RP). A solution [43] to this problem has been proposed. It suggests that the address of the Rendezvous Point is encoded in the IPv6 multicast group address.

4.2.4.3.3 Security

The IP Multicast security problem can be broadly divided into two areas: End-to-end Data Security area, and Multicast Infrastructure Security area.

The End-to-end Data Security area covers the following problems:

- **Source authentication & data integrity (optionally, non-repudiation):** Neither the symmetric key-based authentication nor the asymmetric key based authentication can be used to authenticate multicast sources traffic. While the symmetric scheme does not provide source authentication (as all the members can impersonate the source), the asymmetric scheme introduces a high authentication cost. The existing approaches propose a hybrid scheme by coupling the symmetric and asymmetric scheme [44]. However, the common problem among the existing approaches is how to achieve a trade-off between packet buffering and authentication cost.
- **Data confidentiality in dynamic groups:** As the group membership is typically dynamic, ensuring data confidentiality (encryption) in dynamic groups requires updating the current encryption keys each time a member joins or leaves the multicast group (to ensure backward and forward secrecies). These operations are ensured by the group key management service [45]. Two problems remain unsolved with respect to this problem: (a) How to reduce the re-keying cost for the whole multicast group when a member leaves the group (1 affects N problem) [46]; (b) How to reliably deliver the re-keying messages [47].

The Multicast Infrastructure Security area is concerned with the following problems:

- **Multicast routing protocol security:** This part aims at securing control message exchanges of the multicast routing protocols (unicast and multicast messages) such as in PIM-SM [48].
- **Sender and receiver access control:** The sender access control problem is related to the risk of sending bogus multicast traffic through the multicast tree in order to generate traffic overhead and Denial of Service (DoS) attacks against multicast groups. The receiver access control problem relates to the exploitation of group membership protocols to launch bogus subscriptions (processing and memory overhead in the multicast routers). Whereas the sender access control problem has not been sufficiently addressed, a number of solutions have been proposed to the receiver access control problem using credentials (e.g. tokens, passwords, etc) [49]. Some proposed approaches however introduce a high authentication cost (due to public key schemes) at the multicast router side, while other may not scale to large groups due to storage requirements in the multicast router.

4.2.4.3.4 Mobility

Mobility issues of multicast include support of mobile sources and mobile receivers of an IP multicast group. Two main approaches can be envisaged to enable delivery of IP multicast to a mobile node. They are known as bi-directional tunnelling and remote subscription [50].

In the bi-directional tunnelling approach a mobile terminal subscribes to a multicast group through its home network, via a Mobile IPv6 bi-directional tunnel to its Home Agent (HA). The mobile terminal tunnels its multicast group membership control packets to its Home Agent, and the Home Agent forwards multicast packets down the tunnel to the mobile terminal. This approach does not require any re-construction of the multicast tree while the mobile terminal – either multicast source or receiver - changes its location; however, it introduces a non-optimal routing of the multicast traffic, due to the forwarding of the packets through the Home Agent.

If remote subscription is used, the mobile terminal joins the multicast group via a local multicast router, on the foreign link being visited. For this purpose, the mobile terminal behaves like any other fixed multicast receiver in the visited network, e.g., it sends multicast signalling (Multicast Listener Discovery - MLD) report messages to the local multicast router using an IPv6 link-local source address. This approach optimizes network and radio resources by allowing optimal routing of the multicast traffic in the network, and avoiding header overhead and packet duplication at the Home Agent. It is independent of Mobile IPv6 and allows per-flow handover. On the other hand, the remote subscription does not support mobile sources and may introduce high handover delay due to the reconstruction of the multicast tree at each move. Some extensions of the remote subscription approach have been researched into to address the abovementioned issues, including hierarchical approaches (called Multicast Agent) or fast mobile multicast scheme based on bi-casting techniques [22, 51]. The source mobility problem has also been researched into [18].

Similarly, the need to support multicast delivery to receivers located inside moving networks has been identified recently. Various solutions, inherited from the mobile multicast host scenario, have already been proposed and evaluated [22, 51].

4.2.4.3.5 Reliable Transport

There are two major applications of IP multicast over a broadcast system: streaming and datacasting, both with different requirements. IP multicast based streaming deals with real time transmission of video or audio content, sensitive to delay and jitter but relatively tolerant to packet loss. On the other hand, datacasting deals with transmission of data content (e.g. web content, files, etc.), where reliability is critical while delay or jitter are not.

The User Datagram Protocol (UDP) and the Real-time Transport Protocol (RTP) [52] are well-known transport protocols commonly used for multicast streaming. IPv6 multicast video streaming over a broadcast link, like DVB-T, has already been demonstrated [53].

On the other hand, reliable multicast transport has been researched into for several years already, with many different proposals, but real progresses in standardization have only been achieved recently through the IETF rmt working group. The working group is standardizing a set of building blocks with abstract APIs, which can be combined in several protocol instantiations. This includes building block for congestion control, negative acknowledgments, and forward error correction. Two reliable multicast protocol instantiations are now under definition:

- The Asynchronous Layered Coding (ALC) [54] protocol, that provides reliability through Forward Error Correction (FEC). ALC combines the Layered Coding Transport (LCT) building block, a multiple rate congestion control building block and the Forward Error Correction (FEC) building block to provide congestion controlled reliable asynchronous delivery of content to an unlimited number of concurrent receivers from a single sender. Thanks to a FEC-based reliability, ALC does not require any back channel from the receiver to the sender, which makes it very attractive for datacasting over a unidirectional link like a broadcast system. Especially, the File Delivery over Unidirectional Transport (FLUTE) [55] protocol has been proposed recently, as an application protocol on top of ALC, for reliable unidirectional delivery of files.
- The NACK-Oriented Reliable Multicast Protocol (NORM) [56] uses a selective, negative acknowledgement mechanism for transport reliability. A congestion control scheme is specified to allow the NORM protocol to fairly coexist with other transport protocols such as TCP. It is worth mentioning, NORM is capable of operating with asymmetric connectivity (e.g. broadcast system with return path) between the sender and receivers.

Other alternative protocols, like the Broadcast Trivial File Transfer Protocol (BTFTP), [57], have been proposed to achieve reliable multicast transmission of data over unidirectional link. They rely on the simple concept of cyclical retransmissions, where the source will periodically retransmit the data over the link. From the consecutive retransmissions, the receiver will be able to overcome packet losses and reconstruct the whole content (e.g. a web page). This is the same principle as the carrousel mechanism in DVB. IPv6 datacasting with BTFTP over DVB-T has already been demonstrated [53].

4.2.4.3.6 Multicast Branch Setup over Broadcast

A typical issue of IP multicast over broadcast is the construction of the multicast branch over such unidirectional link. Classical group membership model of IP multicast requires that receivers join the multicast group using group membership protocols (i.e. MLD), to request delivery of multicast data and thus trigger creation of the multicast branch towards the IP subnet they are located in. Such user-initiated branch construction typically requires a return path ala UDLR. Another approach, proposed in [51], defines an architecture where the network itself will establish this multicast branch towards the broadcast link when there are receivers, without the need for the receivers to send MLD reports. Such a centralized approach avoids the burden of maintaining a UDLR tunnel, and allows the network operator to fully control traffic distribution within his hybrid system.

4.2.5 Conclusion

This chapter has investigated issues surrounding the effective transport of IPv6 over broadcast systems, in the context of cellular broadcast convergence. As of today, the potential of IPv6 for delivery of unicast and multicast (streaming or datacast) services in hybrid networks, encompassing unidirectional

broadcast links, has been demonstrated, as part of European research activities. At the same time, standardization of IPv6 protocols has now reached a suitable maturity level to enable its deployment in real systems. Next steps are the continuation of the definition of appropriate protocol extensions for more efficient transport of IPv6 over broadcast links, and the specification of new network functions allowing optimised operation of hybrid networks, such as resource-efficient traffic distribution.

4.2.6 Acknowledgements

This section was contributed by Hong-Yon Lach and Christophe Janneteau (Motorola Labs).

The authors would like to thank Pierrick Seite for his indirect contribution to the description of the DVB systems; Mounir Kellil for his contribution on IP multicast security issues; and Peter Christ for his valuable inputs on IP Datacast.

4.3 The combination of IPv6 and Grid Systems

This article focuses on what is required to integrate IPv6 functionality into Grid systems. The status of global Grid IPv6 standardisation is introduced. We discuss the necessary transition consideration that should be given in heterogeneous IPv4/IPv6 networks. We then introduce the methodology and efforts we have used to provide IPv6 support on Grid systems, using the Globus Toolkit Version 3 as our concrete working example.

4.3.1 Grid Systems over IP Networks

During the last few years, Grid systems [58, 59, 60, 61, 62, 63] have emerged to perform large-scale computation and data storage over IP-enabled data communication networks. They use distributed, potentially remote, resources to optimise computation and storage resources.

Grid systems are normally considered as network middleware [64], since they lie between applications and network resources. The data of Grid systems is currently transported using Internet Protocol version 4 (IPv4), [65]. The next generation Internet Protocol - IPv6 [66, 67, 68] is replacing IPv4 with improvements.

Since IPv6 is expected to become the core protocol for next generation networks, Grid computing systems must track the transition of the lower-layer network protocols to IPv6. However, the period of transition from IPv4 to IPv6 will not be short. Hence, it is important to make Grid systems work on both IPv4 and IPv6, and to be able to communicate in heterogeneous IPv4/IPv6 networks.

While it is clear to those concerned with networks that IPv6 is an important development, most of those concerned with Grid computing are not interested in the network level at all. This has resulted in some problems in the way that the relevant software has been structured, which causes some problems in the transition to IPv6.

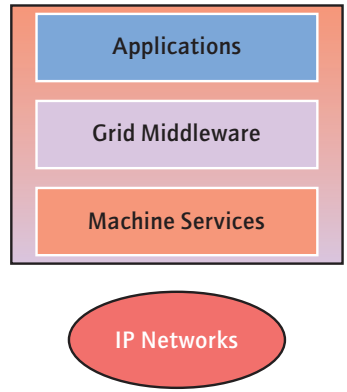

Figure 4.4: **Schematic of grid computing software**

There is a very substantial body of activity in the development of Grid computing. It deals with the provision of networks, the provision of special middleware between Grid applications and the network software, and the applications themselves. Each is considered in this article.

While it is intended that Grid computing be carried out over the general Internet or Enterprise Intranet, the requirements made by the networks on either the applications or the middleware are largely ignored. The activities described here are designed to address this current gap.

The generic software normally used in Grid computing is illustrated in Figure 4.4.

The vital differentiator of Grid computing from other types of computation is the middleware that is used. This is designed so that the applications of Figure 4.4 can be run on clusters of computers and on distributed computing platforms. The aim of the middleware is to provide all the support functions that the applications need. The interest in Grid computing is so large, that there is now an international body to standardise interfaces and services for the middleware systems. This body is the Global Grid Forum (GGF, [69]). The GGF produces a wide range of standards. It has now started an IPv6 Working Group. The deliberations of this Working Group are discussed in section 4.3.2. While there are many implementations of Grid middleware, that of the Globus Consortium [70] is the one used most heavily. The Globus software is discussed in section 4.3.3, and the endeavours to move it to work over IPv6 networks are discussed in section 4.3.4.

Even when researchers claim to have ported a middleware package to IPv6, the product will not be trusted in reality, until it has been used in real applications. Some activity in this regard is given in section 4.3.4. Finally some conclusions are presented in section 4.3.5.

4.3.2 The GGF IPv6 Working Group

While many working groups of the Internet Engineering Task Force (IETF) devote much of their efforts to the impact of IPv6, most do not consider the requirements of specific applications. The Global Grid Forum's IPv6 Working Group (GGF-IPv6-WG [71]) is specifically tasked with considering the impact that IPv6 may have on Grid computing, as regards development and implementation of standards and protocols.

So far the GGF-IPv6-WG has been addressing three tasks: Firstly a survey of the current GGF standards with respect to their IPv4 dependencies, secondly a guide on how to develop and implement IP independent specifications, and finally some recommendations on what additional IPv6 specific features should be added to Java.

We will use the term IP-neutral to express the concept that something can be used in both IPv4 and IPv6 environments. Each of the tasks is considered in the IPv6 WG below.

4.3.2.1 Survey of IPv4 Dependencies in GGF Protocols

The report written by the IPv6 WG [72] surveyed some 88 protocols for IPv4 dependencies. It concluded that about one third had such dependencies.

Of the documents that were found to contain IPv4 dependencies, about 60% of them failed to reference RFC2732 [73] when mentioning URIs. A quarter contained some form of IPv4 biased textual explanations, while the remainder contained other minor dependencies. Thus the protocol specifications themselves caused relatively few problems. However more problems may be expected in their implementations.

This document was published, in January 2005, by the Global Grid Forum as and Informational Grid Forum Document (GFD. 41) [72].

4.3.2.2 Guidelines for IP Version Independence in GGF Specifications

In this report [74] the authors used a methodology similar to that used in the IETF. Indeed, the reports already issued by the IETF [75] and documents from projects such as those from LONG project [76] apply equally well to Grid computing.

The document serves two functions. Its motivation is to aid in the creation of IP-version independent specifications and consequently, in the transition of IPv4 applications to support IPv6 operation.

First, it describes how to avoid IPv4 dependencies in GGF specifications. Secondly, it outlines new, IPv6-specific issues for application designers and implementers. The idea is that it should be used by all GGF WGs and as a checklist for document approval.

This report begins by discussing the operational relationships between IPv6 and IPv4, such as the benefits of the larger address space. It then highlights the differences between IPv6 and IPv4 including information on specifics on address storage and representation. It is recommended that hosts exchange Fully Qualified Domain Names (FQDNs) rather than addresses wherever possible. There is discussion on the extension needed in the APIs – but a warning that the two systems may behave differently in different implementations due to the way that they bind to IPv4 and IPv6 simultaneously. IPv6 support is now available in C, Java, Python and Perl.

There is detailed discussion on how addresses should be parsed and used, name resolution functions, and mapped IPv4 addresses. There are some vital differences in the perceived need for Network Address Translation (NATs, [77]) in the two systems, though this is hotly disputed. IPv6 has some special features: scope specifiers, anycast, flow labels, privacy extensions; these have particular impact when one tries to write implementations which are IP-neutral.

There is an important section on recommendations. For specifications, there are several suggestions, e.g.:

- If addresses must be included, add an address type code
- For literal IPv6 addresses use RFC2732
- Use FQDNs

For implementations ensure that:

- Code is written as IP-independent, including its use of APIs
- Code should be modular
- Care should be taken over which of IPv4 or IPv6 is preferred, if both are available
- One may need to address several sources in parallel, because of the existence of multiple interfaces
- Graphical user interfaces must take into account the different lengths and display formats
- It may be impossible to make implementations IP-independent if some of the unique features of IPv6 are used.

This document was published, in December 2004, by the Global Grid Forum as and Informational Grid Forum Document (GFD. 40) [74].

4.3.2.3 The Changes Desirable in Java

It was originally expected that this would be a major task. In the end, since JDK 1.5.0, Java supports IPv6 well, the recommendations were pretty slight – mainly towards the API. In particular, it was considered desirable to support the setting of the Flow Label in the API.

4.3.3 The Globus System

As an example of Grid middleware, we will consider the Globus Toolkit [78, 70], developed mainly in the Argonne National Laboratory (ANL). This provides one of the most popular systems for furnishing the libraries and services for Grid computing. The current edition of Globus Toolkit – Version 3 (GT3) is based on the recent Grid standards – the Open Grid Services Infrastructure (OGSI) [59, 79].

In this paper we provide details on work done on GT3 systems running over mixed IPv4/IPv6 networks carried out jointly by University College London and the University of Southampton. GT3 was designed to work with IPv4, though many aspects are compatible with IPv6. The developers have tried hard to make their system IP-neutral. We discuss our attempts to provide dual-stack, IPv4 and IPv6 facilities in Grid systems in this paper. We have worked with the Globus implementation group in ANL to include the IPv6 modifications into the official release. Since the Grid systems became IPv6-enabled, we have been able to experiment with several features that are possible with IPv6 support including mobility, security and auto-configuration [80].

Moreover there is a new version of Globus – GT4 – expected to be released in March 2005. The authors of this article have not yet been able to view the code, to understand the ease of porting this version of Globus.

4.3.3.1 Architecture of Globus

The Globus system described in Figure 4.5 below describes the Grid middleware in the overall architecture shown in Figure 4.4.

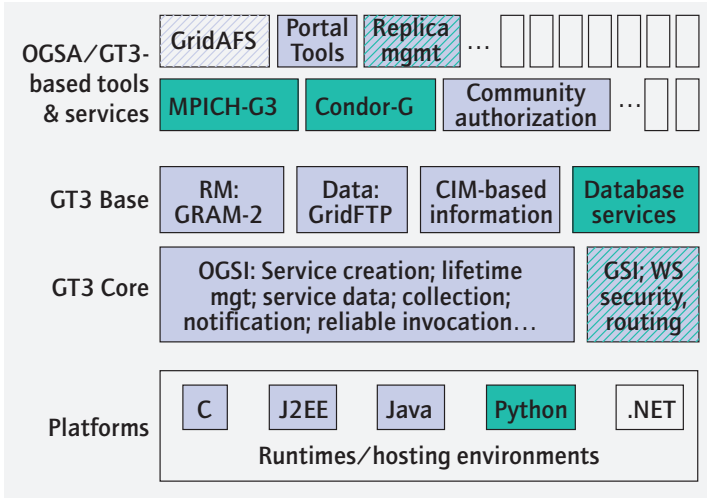

Figure 4.5: Schematic of Globus System

The High Level Services are independent of the network layer, and need not be considered in the porting exercise. The local services are independent of Globus. Here it is vital that they support dual-stack working, and that the dual-stack configurations are chosen. Thus the porting is mainly concerned with the Grid Core Services (GCS).

In GT2, the previous version of Globus, many of the core services were written in C which required extensive porting work. Whilst the authors undertook some initial work on porting GT2, when GT3 was released the work on GT2 was discontinued. Nonetheless the Japanese 6Grid project has now ported a version of GT2 to IPv6. In GT3, however, almost all of GCS is written in Java. If one ensures that JDK 1.5 or later is used, then the Java components are largely IP-neutral. Two further steps need to be taken. Firstly one must investigate which GCS components are dependent on C code; GridFTP turns out to be the main such component. Secondly one must ensure that the guidelines of section 4.2.3 are followed. This work was done by UCL and the University of Southampton under the 6NET project, and the results were fed back to ANL – who incorporated the results into the main code of subsequent GT3 releases.

4.3.3.2 Built-in Security

While scalability, performance and heterogeneity are desirable goals for any distributed systems, including Grid systems, the characteristics of computational Grids lead to security issues. Though the potential security improvements from IPv6 do not solve all the security problems, Grid systems can benefit from IPv6's security features. The IPv6 security and Grid Security Infrastructures are running at different levels. They can be employed together to provide better security control.

The Grid security modules are in some cases linked to the IP address. This does not cause any particular problem in single IPv4 or IPv6 environments. They can, however, cause problems in mixed environments as discussed in section 4.3.3.

Whilst IP security (IPsec) [81] is mandated for IPv6, it is not currently provided by all stacks, though it is increasingly being made available. IPsec provides for integrity, authentication and encryption of IP traffic. With IPsec, all IP traffic between two nodes can be handled without adjusting any applications. Using IPsec, all applications on a machine can benefit from encryption and authentication, and policies can be set on a per-host (or even per-network) basis instead of per application/service. Full IPsec security operates over IPv4 today – when there is a full end-to-end connectivity. If NATs are used, as often occurs in IPv4 networks, it may not be possible to fully deploy IPsec on the end-to-end communications path. These considerations are not too significant in GT3, but would be serious if the security mechanisms intended for IPv6 were adopted.

In GT3, Web Services are leveraged to provide security functions. GT3 implements a session based security service similar to what is described in the WS-Trust and WS-SecureConversation documents. The GT3 implementation (GSI-SecureConversation) allows for GSI's SSL-based authentication to take place over standard Web Services SOAP messages, which in turn allows for the use of Web Services security specifications for message protection (WS-Security, XML-Encryption and XML-Signature). In addition to the session based security mechanism GT3 also provides WS-Security and XML-Signature based per-message security using standard public key cryptography (GSI-SecureMessage).

4.3.3.3 Communication in Heterogeneous IPv4/IPv6 Networks

While it is important to take advantage of IPv6 features, we have stated already that we expect IPv4 environments to persist for a long time [82]. This makes it vital to consider the heterogeneous IPv4/IPv6 networks. The simplest such case is illustrated in Figure 4.6 below.

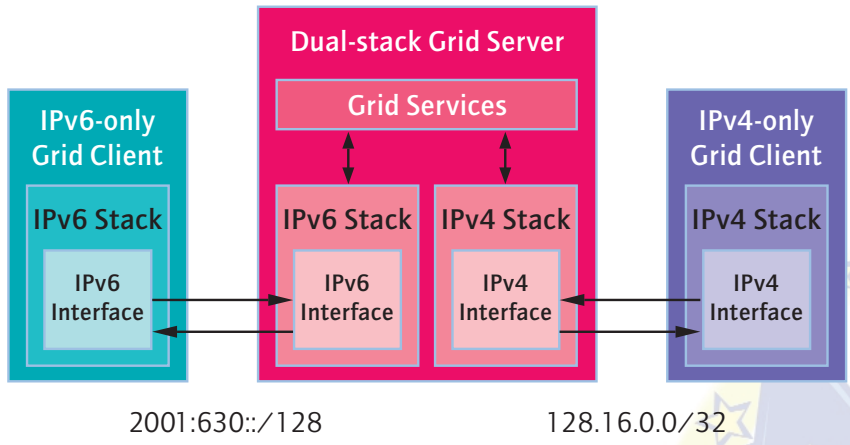

Figure 4.6: **IP Communication of Client/Server in Simple Heterogeneous IPv4/IPv6 Networks**

During the IP transition period, there will be situations like that of Figure 4.6. One effort to integrate IPv6 into Grid systems takes an IP-protocol independent [75] approach, i.e. it supports both IPv4 and IPv6. The IP-independent server, shown in Figure 4.6, has to be able to respond to client calls according to the IP family that the client uses. In other words, the client decides which version of IP is to be used. For instance, an IP-independent Grid server on a dual-stack machine starts and listens on both its IPv4 and IPv6 interfaces. When an IPv4 client connects over IPv4, the Grid server uses its IPv4

interface to call back; only IPv4 communication takes place – similarly with IPv6. With dual-stack servers, the client can choose which IP family is the default or preferred. In order to run Grid services on the dual-stack server, the following fundamental network services need to be dual-stack as well: HTTP, FTP, DNS, SSL, routing etc.

For communication in heterogeneous IPv4/IPv6 networks, there are a number of network transition aids [83, 84], which essentially translate the packet headers between IPv4 and IPv6, leaving the payload untouched. Network-level gateways can work only under the circumstance that no IP addresses are passed in the content of the payload. A higher-level approach, which is employed by other services for transition, is application-level gatewaying. This operates in a dual-stack node and actually does an application-level translation of the payload of the packets between the two communicating nodes. Here the environment is significantly more complex, as illustrated in Figure 4.7.

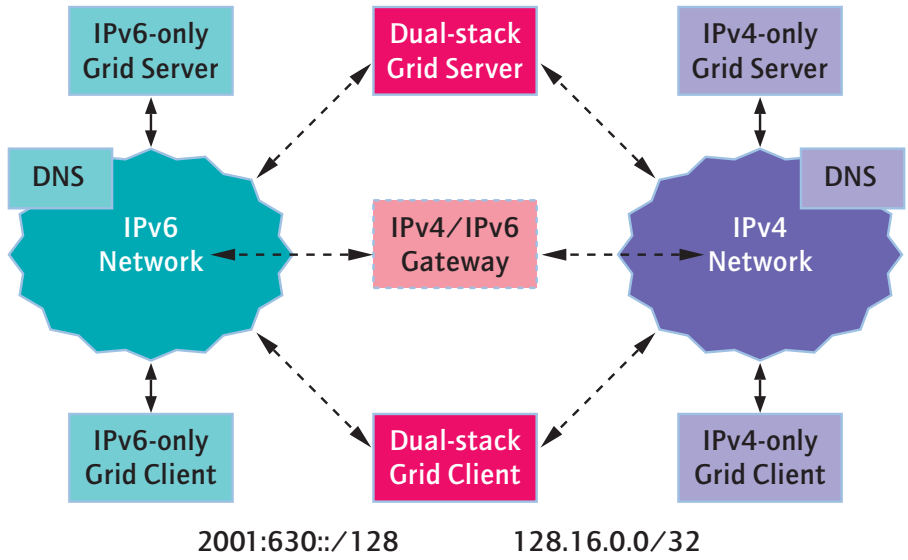

Figure 4.7: IP Transition in Heterogeneous Grid Networks

This shows a heterogeneous IP environment with IP-transition network services. With the IP-independent Grid services running on the dual-stack Grid server, IPv4-only Grid clients, IPv6-only Grid clients and dual-stack Grid clients can access it. Of course, the IPv4-only server is accessible by an IPv4-only client, and the IPv6-only server is accessible by an IPv6-only client.

The situation becomes complicated when an IPv6-only client requires access to an IPv4-only server. In the UCL/UoS activity under the 6NET project, a standard NAT-PT gateway [85] was used to provide network level transition of Grid traffic.

To succeed in the above scenarios, the Grid systems should only use hostnames in the content of the payload rather than any IP addresses. If any IP addresses are passed in the packets' content, it would lead to later failure if that IP address was used. In practice, UCL experienced difficulties when an IPv4-only Grid client submitted jobs to an IPv6-only Grid server, because the specific NAT-PT implementation [86] failed to provide DNS reverse lookups for the temporary IPv4 addresses. This problem is not serious conceptually, but illustrates the problems that must be resolved in this sort of activity.

4.3.3.4 Mobility Support

Until recently, most Grid research focused only on fixed systems. However, the mobility support within Grid systems will be needed as mobility takes an ever more important role in modern life. More Grid scenarios will involve mobile users or mobile resources. Since Mobile IP is mandated for IPv6, a project at UCL is proposing a Mobile-Grid-specific management, based on the deployment of Mobile IPv6 [87, 88]. Its functionalities include mobile connection reconfiguration, Grid resource discovery, security and Grid task scheduling. This work is still in the research phase.

4.3.4 The Porting of Globus to IPv6

While the general principles have been discussed in section 4.3.3, it is illuminating to consider a case history of the UCL efforts to port Globus to IPv6. Firstly, of course, the host must be IPv6-enabled, preferably dual stack. The IPv6-capable application API libraries are required in order to run the IPv6-enabled or IP-independent applications over IPv6. All network-associated applications, such as database applications and web containers, need to be IPv6-enabled. In order to run tests over a network rather than only on local hosts, IPv6 support on the network is essential. We discuss how to build up an IPv6 environment step-by-step, using the UCL IPv6-enabled Grid test bed as an example.

4.3.4.1 Operating System Support on Hosts

The IPv6 support on hosts depends on the operating system and its kernel. UCL concentrated on the LINUX/PC platform since GT3 was only fully working on Linux systems. An IPv6-enabled Grid test-bed was setup, which included 7 nodes running Linux Red Hat 8 and 2 nodes running Linux Fedora Core 1.

Since Linux Red Hat 7.3 (kernel 2.4.18) IPv6 support has been included in all Redhat distributions. Linux IPv6 functionality is provided by a kernel-loadable module. In the earlier distributions of Linux, users had to re-compile the kernel to get the IPv6 support [89]. On Windows 2000, an IPv6 preview package (free download [90]) is available with limited functionality. The IPv6 package in Windows XP/2003, which provides better IPv6 support, is distributed with the edition, but requests individual installation [91] and requires installation of Service Pack 1 for correct operation of multicast.

4.3.4.2 IPv6-Capable Application API Libraries

IPv6-capable application API libraries need to provide support for upper-layer applications. GT3 is mainly written in Java. For the IPv6 support, they used Sun Java SDK 1.5.0, in the IPv6-enabled Grid test bed.

The Linux glibc libraries provide a few IPv6 data structures, such as sockaddr_in6, in6_addr and in6addr_loopback. However, both the data structures and IPv6 system functions, such as inet_ntop() and inet_pton(), are available, but are IP-version-dependent. To be IP-independent, data structures, such as addrinfo and sockaddr_storage, and functions, such as getaddrinfo() and getnameinfo() should be used on dual-stack servers and server applications.

As a platform-independent runtime environment, JDK 1.5.0 provides the IPv6 support under Solaris, Linux, and WinXP/2003. Within any Java SDK that is later than 1.4.0, the class java.net.InetAddress has two direct subclasses: java.net.Inet4Address and java.net.Inet6Address. They provide the support for IPv4 and IPv6 addresses. The InetAddress class uses the Host Name Resolution mechanisms to resolve host names to their appropriate host address type. Additionally there are various system preferences that can influence protocol preferences, such as preferIPv6Addresses and preferIPv4Stack.

4.3.4.3 Associated Applications

The Globus system also utilised external applications. All network-associated applications need to be IPv6-enabled as well. In GT3, the Java run-time environment needs to be IPv6-enabled as mentioned earlier. Java DataBase Connectivity, which is used for Reliable File Transfer, needs an IPv6 patch. As recommended by the Globus Implementation Group, Jakarta Tomcat is used as the web container for the Grid services on a Grid server. The container environment needs to provide IPv6 Web services for Grid services. Tomcat v5 has been tested with IPv6 capabilities.

4.3.4.4 Networking Support for IPv6

In order to run IPv6 tests over a network rather than only on local hosts, IPv6 support for networking is essential. It requires IPv6-enabled routers, which provide forwarding and dynamic routing, and support from IPv6-enabled network services, such as IPv6 DNS, and routing etc. For the communication in the heterogeneous IPv4/IPv6 networks, there are many approaches to the provision of transition aids, but a NAT-PT gateway was used in practice.

4.3.4.5 Integration of IPv6 into Globus Toolkit

The integration of IPv6 into Grid systems starts with finding IP-version-dependencies in the network protocols. The implementation of network APIs within applications may involve a few IP-dependent functions. We introduce our methodologies in later sections using Globus IPv6 porting as an example. A number of modifications need to be made for IP-dependent operation. In order to operate in heterogeneous IPv4/IPv6 networks, a few configuration options are needed.

4.3.4.5.1 Methods of Finding IP Dependencies

To find out exactly which lower-layer protocols and APIs are being used, two approaches are taken – firstly the 'top-down' approach, where we execute some upper layer applications. Secondly the 'bottom-up' approach, where we monitor all the data traffic between nodes and on the Loopback interface. The following have been identified as relevant; they have been modified to be IP-independent:

1. Which network protocols are involved and whether they are IP-dependent
2. Where to get or generate IP addresses
3. How to generate and manipulate URLs [92] and URIs [93] with IP addresses
4. How to create sockets and network connections
5. Hard-coded IPv4 addresses
6. Shipped IPv4-only libraries

4.3.4.5.2 GT3 Protocols Modification for IPv6

The specifications of a few protocols have needed to be modified to suit IPv6. In the Globus Toolkit, Grid FTP is being modified in a way similar to FTP [94]. Correspondingly, the specific implementations of these protocols need modification as well. Within the Globus project, GridFTP is currently implemented in standard C. A new IP-independent network module known as Globus XIO is being developed for use by GridFTP.

4.3.4.5.3 IPv6 Modification in GT3 Implementation

While modifying the IP-independent protocols and their implementation, the implementation of the Globus Toolkit has required modification as well. Corresponding to the IP network functions found, the following modifications have been made to various modules to realise IPv6 functionality in GT3, while Java SDK has provided the IP-independent data structures and functions:

1. Where to get or generate IP addresses

"Localhost" or particular hostname are used in both the Globus configuration file and Globus initial functions. Then IP-independent functions (InetAddress.getByName in Java, getaddrinfo in standard C) are used everywhere that needs to translate hostname into IP address.

2. How to generate/manipulate URLs and URIs with IP addresses

All URLs and URIs generating and manipulating functions have been modified in order to handle the particular format of the literal IPv6 addresses in URLs [73]. It ensures the literal IPv6 addresses in URLs are surrounded by square brackets.

3. Hard-coded IPv4 addresses

All hard-coded IPv4 addresses have been replaced by "localhost" or particular hostnames. IP-independent functions are employed to look up the IP addresses when requiring translation of a hostname into an IP address.

4. Shipped IPv4-only libraries

Some Globus libraries are shipped as IPv4-only. For instance, the Axis library from the Apache project is used to produce URIs. It was not IPv6-compatible. It was modified to support IPv6-enabled Globus.

UCL worked with the Globus implementation group at ANL to include the IPv6 modifications into the official release.

4.3.4.5.4 Configuration for IP Operations

In GT3, a few configuration options are available to allow the user to choose the start-up IP bindings. To use the hostname instead of an IP address, the user needs to set the configuration option "publishHostName" to be "true" in the globalConfiguration section of server-config.wsdd and client-server-config.wsdd. If there are multiple IP addresses that are associated with a host, i.e. a dual stack host, the user needs to set which address will bind to the hostname by using the configuration option "logicalHost". In Java by default, the IPv6 address has higher priority on dual-stack machines. To operate in an IPv4-only network or to set IPv4 to a higher priority, the user needs to set the Java system properties "preferIPv6Addresses" to "false" and "preferIPv4Stack" to "true".

4.3.4.5.5 IPv6-enabled Globus Toolkit Tests

Having realised the IPv6-enabled Globus system, a few experiments and tests have been run successfully in different scenarios. These include scenarios where some of the system is IPv4-only, where some are IPv6-only, and where most are dual stack. These tests helped to allow the necessary transition to IPv6 since most current Grid systems are mainly in IPv4. A few upper-layer services have run successfully over IPv6-enabled Grid systems in order to validate the adaptation between IPv6 and Grid applications. Finally, the whole system was tested using some application programs, which had previously worked successfully with the IPv4-enabled GT3. These tests used the environment given in Figure 4.7.

After some initial problems, all the tests were carried out successfully; it is now possible to run the GT3 application in a heterogeneous environment. The implementation was also tested with externally developed GT3 services as well. The eProtein project [95], which is a large protein analysis project in UCL, had developed a remote execution service based on GT3 GRAM, using GT3 GridFTP to transfer data between clusters in different domains. It was successfully transplanted to the IPv6-enabled Globus infrastructure.

In early 2005, ANL released a pre-production version of GT4, the next major milestone in Globus. Early tests with GT4 indicate that almost all the problems in GT3 have been resolved, and that most of it was almost IPv6-enabled "from the box". Several of the parts of GT3 which were written in C had been re-written for GT4 – in particular the I./O routines. The main part still giving difficulties were the security portions. These are in the process of being rewritten, so that we can expect even this portion to be remedied shortly.

4.3.5 Conclusion and Future Work

This article shows that mechanisms for porting Grid middleware to IPv6 can be carried out successfully. The example of providing GT3 with IPv6 support was used to demonstrate these mechanisms. The mechanisms and approach for integrating IPv6 into Globus introduced in this article would allow the integration of IPv6 into other Grid systems. UCL worked with the Globus implementation group at ANL to include the IPv6 modifications in the official release. The latest official version of the Globus toolkit – GT 3.2.1 has been tested to work with IPv6 on a dual-stack system. UCL also provided an online porting guide titled "How-to IPv6 in GT3" [96], which has become part of the official Globus technology reference documentation.

While keeping modifications in GT3 to a minimum during the tests and experiments, UCL have identified a few further modifications still required that could make IPv6 configuration and operation easier and smoother.

4.3.6 Acknowledgements

This section was contributed by Sheng Jiang, Piers O'Hanlon and Peter Kirstein (University College London).

The authors wish to thank Soren-Aksel Sørensen, (University College London) and Tim Chown and David Mills (University of Southampton), who made substantial contributions to the work of this article. This work was done under the aegis of the IST 6NET project. The support of the European Commission is gratefully acknowledged.

4.4 Security and Privacy with IPv6

4.4.1 Introduction

The Internet today provides a generic communication infrastructure for packet-based communications. Several edge networks that carry both business and non-business oriented traffic communicate with each other via this public infrastructure. This public infrastructure uses IPv4 for its network functions. There have been a variety of exploits on both end and intermediate systems due to the protocol design, as well as implementation problems resulting in substantial loss of revenues. IPv4 has therefore been supplemented by IPsec [RFC 2401] for the provision of security at the network layer. IPv6, the new version of IP, has IPsec mandated for support as part of its basic design.

IPsec provides data privacy and integrity for data in transit across the Internet in addition to providing authenticity of the data. Traditionally, the term 'security' concerns availability (both host availability and service availability), privacy, authentication, integrity and secrecy. IPsec provides for all these facilities, except availability. Consequently, IPv6 provides these facilities too. Such factors are a critical requirement for enterprises that use the Internet or Internet-like infrastructure for their day-to-day business.

In the present Internet, the conservative address allocation policies of the Internet Registries (ARIN, RIPE-NCC, APNIC etc.), the service providers as well as the asymmetric user traffic characteristics (users are data sinks; most of the traffic is from the Internet to the user rather than the other way around) have resulted in the feasible use of address translation devices (NATs). These devices effectively conserve the IPv4 Internet address space by 'sharing' one or a few globally routable address/es amongst a large number of hosts using private IPv4 addresses [RFC1918] that are interconnected to a network infrastructure 'behind' such a translation device. The context is very similar to using EPABXs to interconnect an internal telephone network to the PSTN. All users can place outgoing calls to users both within the internal network as well as the global network, but the capability to call an internal user 'directly' from the global network is not possible (unless there is Direct-Inward-Dialling – DID). NATs have thus broken the peer-to-peer model of the Internet. With its huge address space, IPv6 is expected to re-enable peer-to-peer applications over the Internet. Security will therefore play a very vital role in sustaining this attribute.

4.4.2 Technical Issues

Hosts and devices on the Internet are subjected to various attacks such as identity impersonation (referred to as spoofing), loss of privacy, loss of data integrity, communications monitoring, and Denial-of-Service. Such attacks are the result of discovering exploits that emerge from flaws in the basic protocol design or from flaws in the implementation of protocols and applications. Exploiting such discoveries will continue for as long as the flawed implementations remain deployed.

While the objective of introducing security mechanisms like IPsec is to ensure data privacy and authenticity, the mere usage of these security mechanisms may not render the security mechanisms at other layers (application, transport etc.) redundant and ensure end-to-end communications fully secure, forever. However, the framework provided by IPsec is generic enough to allow additional security mechanisms without a major change in the framework complementing the other security mechanisms (such as PGP, S/MIME etc). For instance, IPsec cannot provide application level authentication (user level) but can only ensure packet source authentication (host level).

IPsec implementation in IP is achieved by means of two optional extension headers (ESP & AH) and cryptographic key management. Using these extension headers in different combinations can provide some or all of the security services such as data integrity, authenticity, confidentiality, protection against spoofing and session replays. These security services are provided using symmetric / /asymmetric key mechanisms.

4.4.3 Security with IPv4

IPv4 doesn't mandate IPsec and hence does not have security mechanism inbuilt at the network layer. However, most major vendors today support IPsec in their products. IPsec is realised (implemented) in various forms, the common forms being Bump-in-the-Stack (BIS), Bump-in-the-Code (BIC) and Bum-in-the-Wire (BIW).

The use of IPsec has resulted in tunnelled traffic for Virtual Private Network (VPN) implementations.

VPNs have become popular due to the technical and economical benefits that accrue when the edge networks use a public Internet infrastructure, instead of setting up a captive network infrastructure, to interconnect and communicate privately.

One desirable attribute on an Internet like infrastructure is to have an authenticated source. Such authentication relies on the global addressability of hosts and devices. Hosts and devices connected behind NATs have private addresses that are mapped onto globally routable addresses, behind the translation device. Hence only the translating host can be authenticated at the destination and not the real source that sits behind the translating device. The source will have to be authenticated separately at the translating device. A similar scheme has to be adopted at the destination host, should such a host be behind a translating device. Thus it is evident that a direct end-to-end authentication is not possible with translating devices in between. There are current efforts at the IETF to find a solution for this problem.

For true end-to-end authentication, the basic need therefore is a distinct un-translated IP address. On the global Internet, the lack of IPv4 address space will prevent the use of end-to-end authentication.

4.4.4 Security with IPv6

IPsec is mandated in the IPv6 protocol. Every implementation of IPv6 is expected to support IPsec as part of the protocol.

To effectively use IPsec, there is a need for a key management framework [ISAKMP and IKE] to make an end-to-end secure communication truly happen. Public Key Infrastructures (PKIs) are required for wide scale deployment of security infrastructure across the Internet. The PKIs will function as authoritative sources for certified keys of hosts and services on the Internet and somewhat similar operationally to the DNS service. There is no accepted standard for PKI, yet. It is also very unlikely that there will be a single PKI for the entire Internet. It is neither acceptable operationally nor does it go with the Internet philosophy. Current day implementations use static key allocations and often do a manual exchange of keys.

An alternative for the provision of public-key authentication for IP addresses without relying on any trusted third parties, PKI, or other global infrastructure, is the use of Cryptographically Generated Addresses (CGAs). CGAs are currently being investigated in the IETF, and provide an intermediate level of security below strong public-key authentication and above routing-based methods. The idea is to form the last 64 bits of an IPv6 address, the interface identifier, by computing a 64-bit one-way hash of the node's public signature key. The node signs its data with the corresponding private key and sends the public key along with the signed data. The recipient hashes the public key and compares the hash to the interface identifier of the source IP address before verifying the signature on the transmitted data. This prevents anyone except the node itself from sending data for its address. As only IPv6 addresses have a 64-bit interface identifier, CGAs consequently can only be used with IPv6.

4.4.5 Privacy

While privacy of the data in transit is assured, the privacy of a network layer session (defined as a set of IP datagrams for the duration of communication between two end hosts) depends on the choice of the mode of transfer – tunnel mode/transport mode. Using tunnel mode, a local IPv6 peer's packet destined to a remote peer is encapsulated in an IPv6 packet generated at the local network's tunnel end point. With the payload of the tunnel's packet encrypted, the traffic between the local and the remote peer is completely hidden. Given the fact that the session between the peers occurred is completely hidden from an intruder on the tunnel, the session can be deemed as private. In contrast, using transport mode will ensure that the data transferred is private and not the fact that the session between two endpoints occurred.

In many instances, a constant 64-bit interface identifier is used to form a global IPv6 address (stateless address auto-configuration). In the event secure transfers are not using tunnel mode, the IPv6 source and destination addresses are visible rendering the fact that the occurrence of the session itself can be noticed by an intermediate snooper. In cases where the devices move between networks, it then becomes possible to track the movement of the device and hence the sessions it participates in. This is considered a serious threat to privacy, especially for mobile/wireless users. RFC 3041 is proposed as a solution to this. The solution involves the use of a pseudo-random number as an interface identifier that changes over time, to generate an IPv6 address. This would make it difficult for the intruders to detect or track a given device.

4.4.6 Principal Security Benefits of IPv6

The availability of globally routable addresses brings about the possibility of end-to-end authentication for hosts on the Internet. However, the success of this depends entirely on the needs of the application, the supporting infrastructure available for the authentication of individual hosts and applications as well as the provision of a choice for selectively using the authentication support in IPv6.

IPv6 brings the virtually unlimited, global address space needed for a large scale IPsec deployment as IP address space depletion means security depletion. Only IPv6 can provide such a critical resource. The IPv4 address space is melting, so is IP security.

With the availability of global address space in IPv6, NAT devices may no longer be needed. However, the large proliferation of such devices does not enable end-to-end authentication. The IETF is currently addressing this. Such a solution is required to enable a smooth transition from existing IPv4 infrastructure to an IPv6 only infrastructure.

IPsec does not really work with NATs. In an IPv6 world, NATs are no longer needed. The ability to get rid of NATs will remove a major current difficulty in deploying secure (encrypted) VPNs. We see many customer scenarios in which NAT traversal by IPsec is a big issue today. NAT modifies addresses, which causes at the IPsec peer the problem of how to transparently communicate with the peer and authenticate / decrypt its packets. Both could only work together if the IPsec peer knew in advance about the existence of the NAT and its mapping scheme, which is an unreasonable assumption. Several other security mechanisms are impeded by NAT. The ones that NAT makes life tough with right now are GSS-based or pure Kerberos.

IPv6 mandates support for IPsec. This implies that OSs, hosts and routers that support IPv6 will provide better interoperability. IPsec mandated in IPv6 means 'my peer supports IPsec'. IPv6-based OS, routers and hosts are mandated to support IPsec. So, IPv6 guarantees a much better interoperability of IPsec implementations.

The large globally routable address space enables new security models for peer-to-peer communication. Some examples are:

- Using separate globally routable addresses per service (email service, directory services etc.) for services provided on the Internet. Server-to-server access in such cases (mail-relays, directory servers for synchronisation etc.) can be authenticated at the IP layer, in addition to the application layer authentication.
- Using differently scoped (link-local and global) addresses for different services based on their scope of access within a network; each such access could be authenticated at the IP layer too. This, however, does not eliminate the fact that the hosts on the LAN are implicitly trusted (wireless LANs are a concern here). Therefore, a user on the LAN can still be malicious and exploit weaknesses in an application or kernel. The bright side is that she/he will not be able to deny the source of the attack, since the source address is authenticated.
- A Mobile IPv6 host (like an IPv4 host using IPsec) can communicate securely with its home location LAN from a foreign LAN, providing both security and privacy to the mobile user as well as the home location network.

Enabling multiple functions such as end-2-end communications, security and mobility will be a lot simpler and widely deployed in view of the end-user benefits offered by the built-in mobility in IPv6.

IPsec in IPv4 has been deployed mainly in host-to-server and gateway–to-gateway. IPsec in IPv6 will enable host-to-server, gateway-to-gateway and host–to-host, due to the abundant supply of address space.

4.4.7 Implications

4.4.7.1 Security

End-to-end security models that imply security above the transport layer, e.g. PGP, S/MIME, secure application layer objects and hand them down to the lower layers, whereas SSL secures the data in transit at the transport layer.

Additionally, link layer security mechanisms ensure privacy on the physical communications link, hop-by-hop. IPsec implies security at the network layer. It complements the security mechanisms at the other layers and does not eliminate the need for them.

With IPsec in IPv6, applications can choose to use the network layer security. This implies that applications that do not want to use the security features of IPv6 can still work on IPv6 infrastructure.

4.4.7.2 Applications

Business applications such as e-commerce applications, m-commerce applications, e-business applications etc., will benefit the most by taking advantage of the IPv6 security infrastructure. Typically, e-business has two specific characteristics – transactions between members of a business community and such transactions manifesting as an exchange of business data, client-server oriented. There is an implicit need here for confidentiality as well as authentication. While security mechanisms today provide for confidentiality of objects, data in transit (transport payload) as well as complete frame encryption on the link, there is no specific security mechanism at the network layer. This gap is addressed by IPsec.

The most important benefits for such a specific community are twofold:

1. All sources of data can be authenticated and data confidentiality can be provided with the use of IPsec
2. The feasibility of the use of IPsec for confidentiality and authentication stems from the fact that such a community may have a specific PKI for its own use.

Such a framework becomes feasible to deploy since the interoperability between IPv6 implementations (that already contain IPsec) will be much better than similar IPv4 infrastructure where the inclusion of IPsec is not mandatory (note that the use of IPsec is not mandatory in IPv6).

Peer-to-peer applications are based on many-to-many model as against the one-to- many model of the client-server applications. End-to-end security is a key requirement for peer-to-peer applications such as VoIP, video conferencing etc. Deployment of IPv6 will enable such end-to-end security mechanisms over the public Internet. If however, a malicious user gains access to the keys that authenticate a source IP address she/he can still cause damage despite that fact that she/he will be authenticated and have a confidential session as well.

Home networking is gaining momentum. Typically, the home needs to be connected to the public Internet to enable access away from home. It is very critical to secure data to and from these home networks. IPv6 (due to its mandated use of IPsec) will be the favoured network protocol for such home networks. Accessing home networks from foreign locations may include the office.

The home host can be accessed from the office and the access model will be a VPN with the end points on the office host and the home gateway.

An ideal host will be configured with two globally routable IPv6 addresses, one from the office block and one from the home block. When in the office, the home network considers the host as a mobile host and when at home, the office network considers the host as a mobile host.

4.4.8 Network Management & Billing

Network management data is collected to analyse and monitor the traffic across the network. This information is strategic to decision makers in the corporation and hence the need to secure such data. On the other hand, from the service provider perspective billing data collected to bill subscribers for the services provided is very critical. This data needs to be absolutely secure and authentic, else it would result in inappropriate billing and revenue losses. IPv6 security fits the need here.

4.4.9 End-to-end Security Infrastructure

To ensure that every end-to-end session is private in the real sense of the word, a large support infrastructure to support security is required. A Public Key Infrastructure (PKI), much like the existing DNS service, with the objective of providing certified public keys for every potential IPv6 host is required. An IPv6 host that intends to communicate securely with a remote host will require to have the latter's public key to begin a secure communication. Such a service requires to be made available. However, in some scenario alternatives, such as the use of CGAs, IPv6 can provide the required security even without these support infrastructures.

4.4.10 Conclusion

Business applications will benefit the most from the IPv6 security infrastructure as they can secure the data and authenticate the clients as well as the client applications. Clearly, the integration of security and privacy mechanisms into the basic protocol will prove advantageous and provide a hitherto inexperienced advantage – an authenticated originator.

4.4.11 Acknowledgements

This section was contributed by Jayachandra K. and Gopi Garge (IPv6 Forum India), and received comments and revisions from Wolfgang Fritsche (IABG), Mat Ford (BT) and Latif Ladid (IPv6 Forum).

4.5 References

[1] P. Ferguson, D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2267, January 1998.

[2] multi6 working group charter: http://www.ietf.org/html.charters/multi6-charter.html

[3] J. Abley, B. Black, V. Gill, Goals for IPv6 Site-Multi-homing Architectures, RFC 3582, August 2003.

[4] A. Matsumoto, M. Kozuka, K. Fujikawa, Y. Okabe,Y., "TCP Multi-Home Options", Internet draft (work in progress), September 2003.

[5] P. Nikander, J. Arkko, End-Host Mobility and Multi-Homing with Host Identity Protocol, Internet draft (work in progress), December 2003.

[6] E. Nordmark, Strong Identity Multi-homing using 128 bit Identifiers (SIM/CBID128), Internet draft (work in progress), October 2003.

[7] F. Teraoka, M. Ishiyama, M. Kunishi, LIN6: A Solution to Multi-homing and Mobility in IPv6 Internet draft (work in progress), December 2003.

[8] E. Nordmark, Multi-homing using 64-bit Crypto-based Ids, Internet draft (work in progress), October 2003.

[9] E. Nordmark, Multi-homing without IP Identifiers, Internet draft (work in progress), October 2003.

[10] I. van Beijnum, On Demand Tunneling For Multi-homing, Internet draft (work in progress), January 2004.

[11] E. Nordmark, T. Li, Threats relating to IPv6 multi-homing solutions, Internet draft (work in progress), October 2003.

[12] C. Huitema, R. Draves, Host-Centric IPv6 Multi-homing, Internet draft (work in progress), June 2002.

[13] DVB Project, http://www.dvb.org/

[14] EN 301 192, "Digital Video Broadcasting (DVB): DVB specification for data broadcasting", ETSI.

[15] Advanced Television Systems Committee (ATSC), http://www.atsc.org/

[16] AC318-MOTIVATE – Deliverable 05 – "Report on Measurements of State-of-the-Art DVB-T receivers", Dec. 1998.

[17] EN 300 468, "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems", ETSI.

[18] IST-OverDRiVE Deliverable D04, "Current approaches to IP Multicast in a Mobile Environment", November 2002, http://www.ist-overdrive.org

[19] EN 301 790, "Digital Video Broadcasting (DVB); Interaction Channel for Satellite Distribution Systems", ETSI.

[20] Interactive Broadband DVB-RCS/S OBP Communication System (AMERHIS), http://telecom.esa.int/telecom/www/object/index.cfm?fobjectid=7923

[21] European's Information Society Technologies research programmes, http://www.cordis.lu/ist/

[22] IST-OverDRiVE Deliverable D09, "Concepts for Mobile Multicast in Hybrid Networks", May 2003, http://www.ist-overdrive.org

[23] B. Martin, MG. Françon, C. Nussli, JD. Gayrard, N. Chuberre, "Satellite Digital Multimedia Broadcast system for Public Protection Disaster Recovery mission"

[24] H.Y. Lach, M. Catalina, "Network Access Co-ordination to Complement IP Mobility Protocols", draft-lach-nac-01.txt, work in progress, October 2003.

[25] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 2460, December 1998.

[26] G. Fairhurst, H. D. Clausen, B. Collini-Nocker, H. Linder, "Requirements for transmission of IP datagrams over MPEG-2 networks",draft-fair-ipdvb-req-04.txt, IETF Internet draft, work in progress, December 2003

[27] IETF ipdvb WG, http://www.ietf.org/html.charters/ipdvb-charter.html

[28] G. Fairhurst, B. Collini-Nocker, "Ultra Lightweight Encapsulation (ULE) for transmission of IP datagrams over MPEG-2/DVB networks", draft-fair-ipdvb-ule-02.txt, IETF Internet draft, work in progress, November 2003.

[29] E. Duros, W. Dabbous, H. Izumiyama, Y. Zhang, "A Link Layer Tunnelling Mechanism for Unidirectional Links", IETF RFC3077.

[30] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, December 1998.

[31] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", IETF RFC 2462, December 1998.

[32] D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, "Generic Routing Encapsulation (GRE)", IETF RFC 2784, March 2000.

[33] G. Fairhurst, M.-J. Montpetit, "Address Resolution for IP datagrams over MPEG-2 networks", IETF internet draft, work in progress, June 2003.

[34] J. Ljungquist, "Transport Protocols for IP-traffic over DVB-T", March 1999.

[35] S. Hanna, B. Patel, M. Shah, "Multicast Address Dynamic Client Allocation Protocol (MADCAP)", IETF RFC2730, December 1999.

[36] B. Haberman, D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", IETF RFC3306, August 2002.

[37] D. Meyer, W. Fenner, "The Multicast Source Discovery Protocol (MSDP)", IETF RFC 3618, October, 2003.

[38] T. Bates, Y. Rekhter, R. Chandra, D. Katz, "Multi-protocol Extensions for BGP-4", IETF RFC 2858, June 2000.

[39] D. Estrin, et. al., "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification", IETF RFC 2362, June, 1998.

[40] M. McBride, J. Meylor, D. Meyer, "Multicast Source Discovery Protocol (MSDP) Deployment Scenarios", draft-ietf-mboned-msdp-deploy-05.txt>, January 2004.

[41] D. Thaler, "Border Gateway Multicast Protocol (BGMP): Protocol Specification", IETF Internet draft, draft-ietf-bgmp-spec-06.txt, work in progress, January 2004.

[42] P. Savola, "IPv6 Multicast Deployment Issues", IETF Internet draft, draft-savola-v6ops-multicast-issues-03.txt, work in progress, February 2004.

[43] P. Savola, B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", IETF Internet draft, draft-ietf-mboned-embeddedrp-01.txt, work in progress, February 2004.

[44] Perrig and R. Canetti, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels", in Proc. of IEEE Security and Privacy Symposium S&P2000, May 2000, pp. 56 – 73.

[45] M. Baugher, R. Canetti, L. Doneti, and F. Lindholm, "Group Key Management Architecture", IETF Internet draft, draft-ietf-msec-gkmarch-07.txt, work in progress, January 2004.

[46] S. Mittra, "IOLUS: A Framework for Scalable Secure Multicasting", Proceedings of the ACM SIGCOMM'97, Cannes, 1997, pp.277-288

[47] Y. R. Yang, X. S. Li, X. B. Zhang, S. S. Lam, "Reliable Group Rekeying: A Performance Analysis", Proceedings of the ACM SIGCOMM '01, San Diego, CA, August 27-31, 2001, pp. 27-38.

[48] Van Moffaert and O. Paridaens, "Security issues in Protocol Independent Multicast - Sparse Mode (PIM-SM)", IETF Internet draft, draft-irtf-gsec-pim-sm-security-issues-01.txt, work in progress, February, 2002.

[49] P. Judge and M. Ammar, "Gothic: A Group Access Control Architecture for Secure Multicast and Anycast", IEEE INFOCOM, New York, June 2002, pp. 1547 – 1556

[50] C. Janneteau et al., "Comparison of Three Approaches Towards Mobile Multicast", IST Mobile Summit, Aveiro, Portugal, 2003 June.

[51] IST-OverDRiVE Deliverable D16, "Functional Description and Validation of the Mobile Multicast Architecture and the Group Management", March 2004, http://www.ist-overdrive.org

[52] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", IETF RFC 1889, January 1996

[53] IST-OverDRiVE Deliverable D14, "Description of Demonstrator for Mobile Multicast and the Vehicular Router", February 2004, http://www.ist-overdrive.org

[54] M. Luby, J. Gemmell, L. Vicisano, L. Rizzo, J. Crowcroft, "Asynchronous Layered Coding (ALC) Protocol Instantiation", IETF RFC 3450, December 2002.

[55] T. Paila, M. Luby, R. Lehtonen, V. Roca, R. Walsh, "FLUTE - File Delivery over Unidirectional Transport", IETF Internet draft, draft-ietf-rmt-flute-07.txt, work in progress, December 2003.

[56] B. Adamson, C. Bormann, M. Handley, J. Macker, "NACK-Oriented Reliable Multicast Protocol (NORM)", IETF Internet draft, draft-ietf-rmt-pi-norm-09.txt, work in progress, January 2004.

[57] P.Casagranda, L.Vignaroli, "Broadcast Trivial File Transfer Protocol", IETF Internet draft, draft-casagranda-vignaroli-btftp-01.txt, work in progress, December 2000.

[58] Chervenak, A. 2001. "The Data Grid: Towards an Architecture for the Distributed Management and Analysis of Large Scientific Datasets," Journal of Network and Computer Applications 23: 187-200.

[59] Foster I. 2002. "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration", Global Grid Forum.

[60] Foster, I. 2002. "The Grid: A New Infrastructure of 21st Century Science," Physics Today Volume 55: 42-52.

[61] Foster, I. 2001. "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International J. Supercomputer Applications Volume 15(3).

[62] Foster, I. 1998. "The Grid: Blueprint for a New Computing Infrastructure," Published by: Morgan Kaufmann.

[63] Laszewski, von G. 1999. "Grid Infrastructure to Support Science Portals for Large Scale Instruments," Proc. of the Workshop Distributed Computing on the Web (DCW).

[64] Aiken, B. 2000. "Network Policy and Services: A Report of a Workshop on Middleware," RFC 2768.

[65] ISI. 1981 "Internet Protocol DARPA Internet Program Protocol Specification", RFC 791.

[66] Deering, S. 1998. "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460.

[67] Thomson S. 2003. "Basic Socket Interface Extensions for IPv6", RFC 3493.

[68] Stevens, W. 2003. "Advanced Sockets Application Program Interface (API) for IPv6", RFC 3542.

[69] Global Grid Forum: http://www.ggf.org

[70] Globus Toolkit: http://www.globus.org

[71] GGF IPv6 Working Group: http://forge.gridforum.org/projects/ipv6-wg/

[72] Sofia, R. et al, "Survey of the IPv4 Dependencies in Global Grid Forum Specifications", GFD 41, December 2004.

[73] Hinden R. 1999. "Format for Literal IPv6 Addresses in URL's", RFC 2732.

[74] Chown, T. et al, "Guidelines for IP version independence in GGF Specifications", GFD 40, January 2005.

[75] Shin, M. 2003. "Application Aspects of IPv6 Transition", IEFT Internet Draft, (work in Progress).

[76] de Miguel, T et al: Programming guidelines on transition to IPv6, LONG Project, http://www.ist-long.com/, January 2003.

[77] Srisuresh P. 2001. "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022.

[78] Foster, I. 1997. "Globus: A Metacomputing Infrastructure Toolkit," Intl J. Supercomputer Applications Volume 11(2): 115-128

[79] Tuecke, S. 2003. "Open Grid Service Infrastructure (OGSI) – Version 1.0 (draft)", Global Grid Forum.

[80] Thomson, S. 1998. "IPv6 Stateless Address Autoconfiguration," Request For Comments 2462.

[81] Kent, S. 1998. "Security Architecture for the Internet Protocol", RFC 2401.

[82] Davies, J. 2002. "IPv6/IPv4 Coexistence and Migration," White paper of Microsoft Corporation.

[83] Chown, T. 2003. "Advanced Aids to Deployment", Deliverable 17, the 6WINIT Project.

[84] R, Gilligan. 2000 "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893.

[85] Tsirtsis G. 2000. "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766.

[86] NAT-PT: http://www.ipv6.or.kr/english/natpt-overview.htm

[87] Fritsche, W. 2000. "Mobile IPv6 - the Mobility Support for Next Generation Internet," IPv6 forum.

[88] Johnson, D. 2003. "Mobility Support in IPv6", IETF Internet Draft.

[89] IPv6 How-to pages: http://www.bieringer.de/linux/IPv6/

[90] Win2k IPv6 http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp.

[91] WinXP IPv6: http://microsoft.com/technet/prodtechnol/winxppro/plan/faqipv6.mspx

[92] Berners-Lee T. 1994. "Uniform Resource Locators (URL)", RFC 1738.

[93] Berners-Lee T. 1998. "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396.

[94] Allman M. 1998. "FTP Extensions for IPv6 and NATs", RFC 2428.

[95] eProtein project: http://www.e-protein.org

[96] How-to IPv6 in GT3: http://www.cs.ucl.ac.uk/staff/sjiang/webpage/how-to-IPv6-Globus.htm

5 IPv6 and *e*Society Services

5.1 Introduction

This section provides an overview of the new possibilities and opportunities that IPv6 technology offers in combination with broadband networks, as well as business opportunities, threats, current technical difficulties and strategies to overcome these limitations.

Users expectations concerning services provided by next-generation networks create requirements for service delivery anywhere, anytime and with sufficient quality of the specific service in question. This is especially relevant in knowledge-related activities, where the transparency of the technology is the key for allowing the required immersion of the user into the ongoing activity.

IPv6 will be a key piece of this vision thanks to some key features: security support, QoS support, large number of IP addresses, multicast and anycast support, and Plug&Play facilities based on auto-configuration characteristics.

The next generation of broadband networks will enable the creation of new service models providing ubiquitous seamless access to a large variety of services. They will make extensive use of the characteristics of the IPv6 protocol for building simpler, more powerful and more easily manageable networks. These facilities will be combined with enough bandwidth available at affordable price for any kind of services.

The creation of new hardware and software components will also be an unavoidable requirement for the provision of advanced services. These new components with more intelligence, context awareness and re-configurability facilities, and user-centric orientation will be basic for the ubiquitous and transparent access to the services by the users. They will be simpler than the current ones because they will delegate several of the complex tasks (QoS, security, service configuration, etc.) to the underlying IPv6 Broadband network. So the overall system will be simpler than the current one, which will enable the design, deployment and operation of much more powerful services with a wider coverage and enhanced user-friendly characteristics.

In this section the following areas are specifically addressed:

- Ambient Intelligence (AmI)
- Defence
- Transport
- Education

This section is targeted mainly at professionals working in, or in areas related to, telecommunications and information technologies for the information society. This includes not only researchers, consultants and decision makers, but also users interested in the capabilities of IPv6 applied to specific areas.

Analysing technical, business and social elements, this section intends to contribute to the creation of a common perspective about those challenges and opportunities that IPv6 focuses on in order to become a worldwide reality in the near future impacting many areas of the information society.

5.2 IPv6 and AmI: I Had a Dream

My alarm clock woke me earlier than expected: it's snowing and the motorway is dangerous, and most probably will be congested. My electronic assistant already turned on the coffee maker and the toaster. It has also called a taxi.

I just received my weekly health report. I'm under medical surveillance all the time, because I suffer from a heart problem. During the night I passed a special weekly check, and it seems that I only need some minor adjustments in my diet and my medicine. All this information is automatically stored in a database, so I can collect the new medicine at my preferred pharmacy. Also my next meals are programmed to match my diet, regardless of the restaurant, plane, train or whatever place I choose to get the food. The information is also stored in my smart card, so in case of any emergency, the medical services can know about my condition.

We are on the way to the airport. There is an enormous traffic jam and it will take close to an hour. Fortunately, in the taxi, I can use my wireless Internet access to finish an important project that I need to deliver to the customer this afternoon. I'm subscribed to a service that allows me to be 'always-on', using any of the media that the technology provides: radio, power line, infrared, etc. It is very comfortable and flexible; gives me the security, privacy and quality of service as never before any provider offered.

There is an obstruction in the road ahead. The conditions are very treacherous, but the taxi has a safety system that ensures the communication with other cars, and among them, shares the information about this. The system provides a lot of very useful information about the traffic conditions, weather, dangers, accidents, and so on, and the intelligence in the car takes care of some of them directly and warns the driver and passengers about the others.

Well, at last we arrive; no need to wait in the long queue at the check-in. I bring only hand baggage, and I have already confirmed my reservation from the laptop. Then, this has been automatically transmitted to my watch, PDA or cellular phone. Now, I just need to show up at the boarding pass area to be authenticated and the boarding pass certificate is generated. Biometrics will complete the security check. When I do not carry electronic devices (not often today), it is stored into any of my credit cards, or in the new smart frequent traveller card. Soon it will be stored in the new digital identity card. With this, I will be automatically identified in the boarding gate, even in the plane. For security reasons, the system can check my location in the airport, if I lose the plane, or even to know what seat I am using.

Unfortunately, my baggage is too big for such a small plane, so I can't carry it by hand. No problem: the baggage has a small device with my personal certificate, and has received my flight information. Just leave it in any of the baggage check-in points anywhere in the airport and the system will move it to the correct plane, without errors, never lost again!

The security control is also much easier and faster, because my electronic devices will verify my personal certificate and double-check with a biometric device.

With this check-in automation, the waiting time in the airport is really short, but I also have good connectivity there. In this case, I still need to charge my laptop battery, so I use the same power cord to get connected thru the power line. The speed is amazing, up to 200 Mbps. I can attach to my office and work in the same way as if I really was there. It's wonderful, because for several months, I do not need to reconfigure my laptop or the applications; it is the new mobility service, and all these complicated tasks are past history.

Indeed, with this speed, I can download the latest Spielberg movie which I was not able to see last weekend; with my laptop I was able to check the in-flight program and the selection of films that they will offer don't appeal to me.

Also I need to check if I left everything right in my home, if I had activated the security system, and if there is enough food and water for my pets; as usual, I left too quick, and still prefer to see everything with my eyes with all the wonderful technology that I have in my hands. No problem; I connect to my home system, just need a mouse "click", and guide the cameras in order to review everything. As always, everything is OK. I do not know if I left any light on, but my assistant has solved it. My pets are playing and they react to my voice, recognize me and calm down. It is snowing again, and the cover was closed by the system, because although they are Nordic dogs, I feel better if they are more protected. I am waiting for an important telephone call, which will probably be during the flight. I don't mind, as by default, the call will be redirected from my cellular to the laptop, so I can attend it in the plane. Fortunately, my hands-free kit works the same with my mobile, laptop or PDA. Now I carry fewer devices, more universal and featuring auto-configuration.

Surprisingly, there is no delay waiting for a slot time for take-off. With the new air traffic control that was deployed in Europe, I have almost forgotten this tedious waiting. A drawback: I liked the Champagne the crew usually served to keep passengers quiet during the delay.

In the plane there is connectivity, now with a Bluetooth link. Also, I can use a Gigabit connection; in the case I need a higher bandwidth. I ask the cabin purser for my favourite newspaper. I get it after a minute from business class spares from the upper deck, brought by another stewardess, which can be contacted by the Bluetooth wireless intercom of the crew.

The screen shows me a bell; it is my call. The customer has to provide me with the last minute instructions to finish the project. He does not know that I am travelling, but he called to the office and the system transferred the call to my mobile; as this one was disconnected, the call was forwarded to my computer. The system locates me automatically and I decide whether to take the call or not. Also, if I wish, I could automatically send to the customer the information about where I am, or activate the videoconference call. In this occasion, I will not do that, the customer is too formal and I'm not wearing a suit; also, I have not accepted to tell him where I am, because he is not very confident with the idea of the job being done outside the office, and will get nervous.

The quality of the call was impressive; I'm sure the customer won't know it was from a flight. Simultaneously he sent me several megabytes of new data, graphics and statistics. It's becoming a trouble to finish everything on time for this afternoon, but with this customer, everything is always at the last minute. It will be impossible without the versatility of these communications technologies!

We have just landed. I must get my baggage, and I need to take a train for downtown. Indeed, I confirmed everything on my laptop, and the assistant instructed to forward my baggage to the correct lane, already in the train station, located next to the airport. No need to carry it through the airport. When I reach the delivery point, in a few seconds, my certificate is authenticated and my case appears.

In the train station, and also in the train itself, was able retrieve some additional documents and finish the report. Also, from the train I printed some notes, which are delivered to me in the hotel front desk; I need them for tomorrow's conference!

It is true that I might arrange to participate remotely in the conference, as I used to, but there will be a lot of people to whom I want to say hello in person, and also, I will have the opportunity to go skiing during the weekend. I do not like 'virtual' sports.

Finally, the day is over. I will stay only this night, as tomorrow I will fly back home. But fortunately this is one of these new hotels where the room is configured automatically to match my personal preferences, like the light intensity, volume of the music, temperature and anything like that, so I can feel myself like in home. I can see the same TV or radio channels, as they will be served from my origin country using broadband access. I can even enjoy the same music and DVDs that I have at home, again using broadband access over IP networks, and of course I can play karaoke. Moreover I can provide my preferred recipes directly from my kitchen to the hotel one, so they can cook it for me. All this and much more is done without any special knowledge, I can speak with my room, ask for the lights to dim, control the TV, or play a shared game, which is projected at any wall in the room.

It's not a dream, it is becoming real with IPv6 and the new Ambient Intelligence systems. Our environment is becoming safer, more friendly, self-adaptative, and intelligent to fit our best comfort.

We should not mind the technology, but the freedom and services that it provides. These services offer an increased level of safety, freedom, mobility, quality of life and security.

5.3 Defence Related Activities and IPv6

5.3.1 Introduction

Defence has long played lip service to the importance of IPv6, but until recently its penetration has been limited. While the US went into this area early under the Defence Advanced Projects Agency (DARPA) [1] auspices, this work was not carried through very far. DARPA set up the CAIRN activity [2] back in 1996, as a test network for its high-speed activities. All the early work in IPv6, secure DNS and multicast were under the aegis of that DARPA programme. They were done with FreeBSD, and eventually found their way into the Japanese Kame Project [3] work. Small later exercises, like the work at University College London (UCL) and the Information Science Institute (ISI) at Marina del Rey on VPNs and active networks [4] though funded by DARPA, could hardly be called defence work. SPAWAR [5] the Naval Research Centre, carried out most of the work for DoD in this area up to the beginning of 2003. This led to their holding a meeting in Charleston, US, in October 2002, entitled: "Deploying IPv6 in the military" [6]. In fact the impact of IPv6 was being studied seriously by DoD towards the end of this period.

Prior to 2001, most of the international IPv6-related, defence activities were devoted to implementations and interoperability testing. An early such project was, involving Denmark, France and Italy, developed a stack, a router and various protocols (RSVP, Multi-Link PPP, Header Compression, Weighted Fair Queuing (WFQ)). The security infrastructure consisted of IPsec, secure DNS and ISAKMP/Oakley. This work was based mainly on FreeBSD. A more serious international activity from the Defence sector has been the Interoperable Networks for Secure Communications (INSC) project, in which 8 NATO countries participate (Canada, France, Germany Italy, Netherlands, Norway, UK and the US) plus the NATO Agency [7]. The special characteristic of the €15M INSC project has been the integration of many advanced features into a common test bed, such as OSPF for IPv6, PIM, MIPv6, OLSR for IPv6 and IPsec. This project started in early 2001, and its first phase has now finished; the programme for the next phase is under discussion. The initial goal was to evaluate IPv6 technologies for future coalition internetworking. More than 15 centres have been connected using more than 100 routers and setting up more than 160 IPsec VPNs. Information about the project is lightly restricted. There was a meeting to describe the results at NATO-C3A in November 2003 [8].

Various defence interests are still represented in R&D projects. Thus DARPA is still supporting the Xbone hierarchical VPN work at ISI, which has just transitioned to IPv6, and Defence Research and Development Canada has transitioned its DVC VPN system to IPv6. Further information here is given as a result of a workshop held in November 2003 at UCL [9], in the context of the International Collaboration Board (ICB) [10]

5.3.2 The DoD Announcement

The whole defence situation changed on June 9, 2003, when John P. Stenbit, assistant secretary of defence for networks and information integration and DoD chief information officer, announced [11] that:

> **"Beginning in October, all Defence Department assets acquired for the Global Information Grid must be compatible with the next-generation Internet Protocol Version 6 (IPv6). The GIG is a massive DoD network designed to connect war-fighters anywhere in the world. Moving to IPv6 will help the department achieve its goal of network-centric warfare and operations by the end of the decade."**

Stenbit signed a policy memorandum June 9, 2003, that outlines DoD's transition to the new protocol by 2008. That year was chosen because most experts estimated widespread commercial adoption will take place from 2005 to 2007. he stated:

> **"We want to make it clear to our programs' major development activities that come on line in the 2008-2010 timeframe that the IPv6 standard, as it evolves, will be the department's standard,"**

He added that, "IPv6 was designed to meet future commercial and DoD requirements, including:

> *** Improved end-to-end security, which is critical for DoD intranets that contain large amounts of classified information and traffic.**
>
> *** Improved quality of service through work-arounds that will eliminate packet drops and instability on video teleconferences and voice-over-IP systems.**
>
> *** Facilitation of mobile communications.**
>
> *** Better system management.**
>
> *** Expanded IP address space, which is a major problem in Europe."**

He added that:

> **"DoD is in the process of selecting three large programs to serve as early adopters of the new protocol, and the results of those three experiments will [determine] if we pull the switch in 2008."**
>
> **"One pilot program per year will be launched between 2005 and 2007 and they will be large enough, but also controlled enough, so that DoD can properly analyze results for possible enterprise use."**
>
> **"Either the Secret Internet Protocol Router Network (SIPRNET) or the Non-Classified Internet Protocol Router Network (NIPRNET) might be one of the programs switched over to IPv6, and the Navy Marine Corps Intranet also is also being considered. Definitive choices will be made within 30 days."**
>
> **"NMCI has a large population of users. . .and when they get to [a suite] of standard applications, there's a technology refresh in the contract in a couple of years," he said, noting that could be the time to make a switch to IPv6."**
>
> **"Vendors, including Cisco Systems Inc., already are producing equipment that is compatible with both IPv4 and IPv6, and as competition heats up in the next few years, costs should level out."**

5.3.3 The Aftermath

The initial announcement has been followed up by several others. Thus at the US IPv6 Summit in December, Marilyn Kraus (Architecture & Interoperability DoD Chief Information Officer) stated that DoD intends a complete transition to IPv6 by 2008. They will address transition issues and demonstrate transition readiness by pilot implementations, test beds and demonstrations in 2004-2007. Their rough timetable of events is outlined in [12].

An initial activity to prove their intentions is the strong participation of DoD in Moonv6 [13]. The Moonv6 test bed is a collaboration by the DoD's Joint Interoperability Test Command at Fort Huachuca (JITC), the University of New Hampshire lab and the North American IPv6 Task Force. Military Moonv6 sites included JITC at Fort Huachuca; the Space and Naval Warfare Centers (SPAWAR) East and West in Charleston, S.C., and San Diego; the Air Force Communications Agency at Scott Air Force Base, Ill.; the Army Communications-Electronics Command at Fort Monmouth, N.J.; and the Marine Corps Network Security Operations Center at Quantico, VA. The Moonv6 project's initial interoperability and test period ran Oct. 7 - Oct. 17. The DoD's Joint Interoperability Test Command at Fort Huachuca, Arizona, is assessing the results. Moonv6 will continue to operate past this initial phase as a U.S.-wide proving ground for use by industry, universities, research labs, Internet providers, application providers, the DoD and other government agencies, and as a tool to assist in the evolution of IPv6 for early adoption and deployment within the North American geography. The next phase will dig deeper into security, mobility and routing protocol testing, as well as network stability and management according to Major Dixon, of the DoD's Joint Interoperability Test Command at Fort Huachuca. The NAv6TF mission is to keep Moonv6 up and running permanently as the North American IPv6 backbone.

The US announcement led to several others. Thus the German Bundeswehramt stated [14] on October 1, 2003 (our translation):

> **In the long term, the communications platform requirements for networked operations, will force the stepwise replacement of IPv4 by IPv6. Hence the use of IPv6 will be introduced in steps. The first step is that all new projects which use IP will use IPv6. Moreover, from now on, all equipment purchases must bear in mind that for an interim period both IPv4 and IPv6 must be able to be installed.**

Similar representations have been made to other countries such as Australia and France for implementations, test beds and demonstrations in 2004-2007. The British are rather more cautious in their approach [15, 16]. In response to a parliamentary question, Lord Bach responded, on April 21:

> **The Ministry of Defence is developing a strategy for the adoption of IPv6. The adoption of IPv6 is planned to be gradual, since the department has adequate IPv4 address space to meet its current needs. Since IPv6 and v4 can coexist, no specific date has been set for cessation of the IPv4 service. New projects have been directed by DEC CCII (Director Equipment Capability Command, Control and Information Infrastructure) to procure a dual v4/v6 capability and work is in hand to identify non IPv6 compliant legacy equipment and the implications of converting to IPv6. The MoD is in the process of applying for the UK MoD IPv6 address space to the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA).**

The MoD recently hosted a conference to explore problems of transition. They are not short of IPv4 address space for their immediate needs, and so far the main decision on introducing IPv6 into their projects is that of requiring equipment to be capable of dual-stack operation. Nevertheless, they are conscious of the needs for interoperability, and are encouraging their suppliers to participate in large scale demonstrators, like the annual Coalition Warrior Interoperability Demonstrators (CWID). While the CWID-2005 demonstrators will not yet feature any UK IPv6 activity, they expect that CWID-2006 may feature IPv6 ones.

The European Defence Agency is currently exploring whether it should make a decision to adopt mainly IPv6 in view of its interoperability needs. It is expected that a firm decision on this matter will be announced shortly.

5.3.4 The Future

It seems clear that the US DoD will try to carry through the plans they have outlined in sections 5.3.2 and 5.3.3 above. We can, of course, expect substantial delays. The main reasons they originally gave for the move were security, QoS, mobility and management. While these areas are very important, they are all ones where substantial work is still needed. We would expect that the facilities for multi-homing will also figure highly in the future.

The pilot test beds, such as Moonv6 and INSC, will assume an additional importance as one starts to put IPv6 into real operational procurements. They are likely to drive the vendors into providing advanced capabilities which truly meet the above needs. Our own experience in 6NET is, however, that the advanced capabilities will still require significant further experimentation and refinement before they deliver the advantages currently anticipated. The US DoD has given all the indications that they are prepared to put adequate resources in to resolve the remaining problems; though their magnitude in real military environments with tactical mobile systems should not be underestimated. While the work done under INSC is quite impressive, they have not had a real large-scale IPv6 network; certainly nothing approaching the scale of the research networks in 6NET, Internet-2 or the larger Japanese deployments. A European version of Moonv6 for the defence community is required – or access to the research networks, which are starting to become available on a serious scale.

Few European Defence Departments allow themselves the luxury of putting substantial resources into test beds; such investments will be mandatory to make the hopes of emulating the US DoD announcements a reality in Europe. This is particularly because it is in some of the more difficult areas like security, mobility, management and QoS that the environment in the military arena is substantially different from most civil ones.

5.4 eTransport

Telematics markets in Europe are in their infancy. While there certainly are a number of very interesting applications and services being conceived, they generally lack the connectivity, common technology platforms and standardized interfaces to become widely adopted. Among those applications, multi-modal travelling, hybrid navigation, hazardous goods tracking, inter-vehicle safety communication, extended vehicle management, real-time traffic information, extended floating car data and high-end infotainment are just a few examples of upcoming services that have a cross-European mass market potential. Many SME service developers are creatively designing innovative services finding clever ways to implement them, but they generally lack the access both to the markets and the vehicles to truly be able to participate in the e-transport value chain. Public authorities are debating new safety initiatives and join forces with the industry to develop service concepts leveraging new communication and information technologies to solve many of today's road network and transport headaches [17]. For all those concepts to materialize in real-world applications some significant challenges have to be overcome. Vehicles need to become truly connected systems that adhere to open platform standards at all levels.

Networking will be a crucial enabling technology for *e*transport. People and vehicles on the move will require sustainable, scalable, reliable, ubiquitous, and affordable means of one- and two-way communication. Transparently providing connectivity to mobile end points will be a prime goal as much as fielding innovative mobility supporting services. The success of *e*transport systems will depend on them being able to deliver services and timely information to vehicles, devices and people regardless of their location, network operator and access technology available at that location. A number of key *e*transport communication scenarios can be identified:

- People accessing personal services that they have subscribed to;
- Service agents connecting to vehicles for advanced diagnostics, maintenance, updating, and fleet management;
- Public safety information broadcast at a regional or urban level;
- Safety-related, local, peer-to-peer communication among vehicles and infrastructure;
- Authorities and associated providers communicating to vehicles or devices therein, and;
- Last, but by no means least, multi-media communication among persons.

Evidently, these scenarios require end-to-end connectivity to be established transparently for a broad variety of application categories. This includes both, mobile-initiated and mobile-terminated sessions. The capability to connect to a peer application entity on any target from any device will be truly established by IPv6. Its mechanisms for routing and mobility support enable e-transport applications to communicate in the first place. Next generation mobile platforms like 3GPP UMTS have chosen IPv6 as their networking protocol. Hence, clearly e-transport systems need to be based on IPv6 to fully benefit from their coverage and capacity. Moreover, additional access network technologies are being deployed and will be developed further. With IPv6 as a unifying networking platform, *e*transport services will become pervasively accessible across heterogeneous networks, maintaining security, quality of service, and mobility across different underlying air interface technologies and operators. In this way, IPv6 will greatly improve the range of e-transport services and their availability. Initiatives such as the EC FP6 project DAIDALOS are aiming at such a universal service provisioning platform based on IPv6 and extending it to vehicles [18].

An important additional asset of IPv6 is the extended addressing space. It will allow *e*transport services to be enabled across a growing number of personal terminals, vehicles, and in-vehicle devices. Communication addressing entities directly and uniquely without gateways, port filters, or address translators maintaining end-to-end security is a mandatory feature for many *e*transport services. Spontaneously establishing connectivity without infrastructure forming dynamic networks of networks is facilitated by the ability to assign each device its unique, fixed network address.

The enabling factors of IPv6 are not only going to boost commercial e-transport services, but will also help to improve road network safety. Wide availability of telematic services delivered through homogeneous IPv6 infrastructure will enable on-line safety applications contributing significantly to the reduction of fatal accidents and reducing critical time gaps in rescue operations. Telematics can even enhance autonomous safety by updating on-board information and improving the accuracy and reliability of on-board applications. Such telematic architectures are currently being investigated by the EC FP6 project GST [19].

An important building block of an esafety initiative for European roads is the availability of high quality Real-time Traffic and Traveller Information RTTI. Currently based on RDS-TMC, it will require significant extensions of the encoding and location referencing approach when extending coverage to urban areas [17]. This in turn will lead to increased bandwidth demand, which is not readily available on the current broadcast distribution channels. Hence new approaches will contain bearer independent safety channel service definition and multi-bearer distribution concepts [19]. This has to be supported by a networking platform capable of distributing the service to as many vehicles as possible in order for the intended safety impact to take effect.

An area of active standardization is vehicle-to-vehicle, vehicle-to-infrastructure, and infrastructure-to-infrastructure communication in the short and medium range. It has been addressed at ISO through its effort on Continuous Air-interface for Long and Medium distance, CALM. Integrating multiple air interface technologies, it is centred on a Mobile IPv6 networking kernel [20]. It is targeting traffic information, tolling, safety and other intelligent transport systems applications. Recently, the inter-vehicle communication aspects are being targeted in related initiatives such as the EC FP6 project PReVENT [21]. Industry forums focusing on inter-vehicle safety communication have been formed in Europe with the Car-to-Car Communications Consortium C2CCC [22] and the US with the Vehicle Safety Communication Consortium VSCC [23].

Overall, unfortunately IPv6 is not yet being actively promoted as such by the etransport community. However, it is clear that the Intelligent Transport Systems targeted will require a viable communication platform that is both scalable for a massive amount of uniquely identifiable devices and ubiquitously available to sustain pan-European mobility. Evidently, the implications are significant challenges in numbering space, end-to-end security and quality of service control, and most of all mobility support that all but IPv6-based networking approaches cannot adequately address. Large fleets, different categories of devices and infrastructure, and a great number of networks of frequently ad-hoc, temporary nature that need to be spontaneously set-up and dissolved also pose systems management challenges that IPv6 is best positioned to meet.

Significant harmonization and standardization efforts will be necessary to bring the fragmented, often proprietary developments in the etransport sector behind a unified communication platform based on IPv6. This however is the conditio sine qua non in future etransport, avoiding conflicting approaches, unifying technology platforms, simplifying design and reducing system complexity.

5.5 Education Related Activities and IPv6

5.5.1 Introduction

The development of applications and systems for creating tele-education systems requires the integration of different elements belonging to different levels of the telecommunication systems where IP protocols are involved. Meanwhile this kind of application seems to be quite independent of the underlying network; practical experience shows that complex applications are based on underlying and common components, which may take advantages of using underlying network protocol services.

In this section we will analyse the impact of IPv6 usage on the different levels, so a complete picture of how IPv6 will influence education related activities will result as the composition of those influences. In parallel the use of broadband networks will also be analysed.

5.5.2 Components of Tele-education Systems

Figure 5.1 [24] shows a scheme of current solutions offered by different technologies for the education field and how they may be applied to different education scenarios. Over this scheme we will analyse how IPv6 and broadband are contributing to each element of the scheme and how it may contribute in the future.

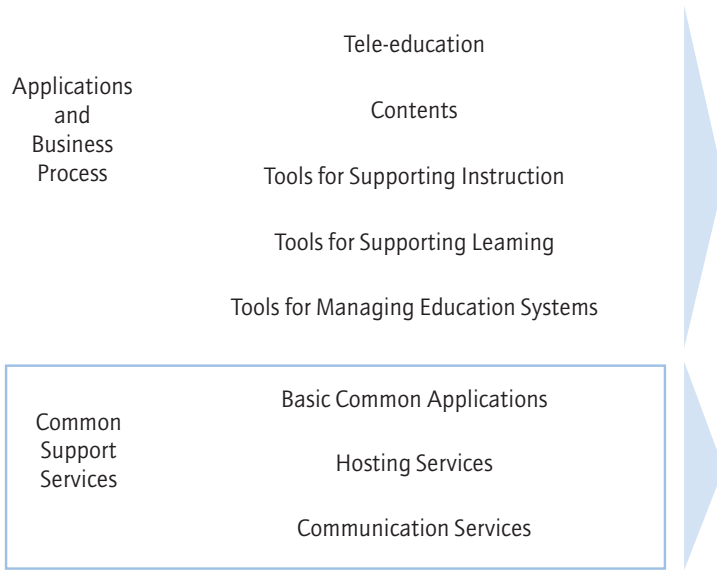

Figure 5.1: **Elements involved in a Tele-education System**

Common support services may be classified in three categories:

- **Communication Services.** They include the basic communication networks supporting IP protocols, including low and high bandwidth technologies. Such supporting networks include ADSL, Wireless LAN, GPRS, VPN IP, Internet, Intranet, Extranet, etc. [25].
- **Hosting Services.** They include hosting and housing services with high availability characteristics. The hosting systems require high availability and robustness with complex management systems in order to reduce the cost of operation and maintenance.
- **Basic Common Applications.** There is a common set of services that are not specific to education related activities, but are basic services used for building the education applications and services. These basic applications provide: identity management, content management, payment systems, and public Internet access systems, among others [26].

Using the Common Supporting Services, the tele-education services are based on portals, contents and tools:

- **Portals.** They are a vertical component related with all the elements of the applications and business process. They facilitate the access to the tools and content from a web interface from both Intranet and Internet [27].

- **Tools for managing education systems.** They include tools for supporting the management of education resources such as: systems for automated management of equipment, students database, classrooms, laboratories, etc.
- **Tools for supporting learning.** Learning tools provides complementary and core services to persons directly related with the content delivery and teaching and learning activities. They include e-mail, chat, instant messaging, collaboration tools, tools for self-learning, etc.[28]
- **Tools for supporting teaching.** This group includes applications that make possible the creation of new learning models or that support already existing ones. They include specific tools and components used during the education activities, which including tools for portals and contents accessible via the web, tools for the creation of virtual education communities, user interfaces for childrens education, digital blackboards, virtual classrooms, etc.
- **Contents.** The development of digital education contents is a key element for the integration of telecommunications in the education process. In this process, it is not simply enough simply to digitise standard teaching material, but the material should be adapted for the specific support being used. In this area the role of the teachers is remarkable, often they will do this adaptation task. Therefore, it is very important to provide suitable tools for the creation of these materials. In any case the success of education activities via telecommunications systems will depend very much of the quality of the education content [29].

5.5.3 IPv6 and Broadband Contributions to Tele-education Systems

From the previous scheme, we identified the elements required for building any tele-education system. In this section, we analyse how IPv6 and broadband influences each element involved in the realisation of a tele-education system.

Regarding **communication services,** IPv6 based networks are simpler than IPv4 networks, specifically because they do not require the use of NAT in order to deal with the scarce number of addresses. IPv6 offers other advantages at this level, because it incorporates mobility and QoS support, which are basic capabilities required by most of the tele-education systems [30]. Broadband networks will offer not only larger bandwidth but also reduce latency and jitter, which will improve quality perceived by the end user.

Hosting services are not directly influenced by the use of IPv6. As an indirect effect, the abundance of addresses will facilitate the provision of hosting services. Complex service design and deployment is simplified when the usage of NAT is reduced or eliminated. Then **tools for managing education systems** will become simpler and easily manageable, taking advantage of the IPv6 capabilities regarding security, QoS and especially self-configuration.

Tools to supporting learning will benefit from self-configuration capabilities, anycast support and the availability of addresses for facilitating the creation, deployment, scalability and operation of such basic supporting services.

With respect to the **tools for supporting instruction,** the availability of IPv6 addresses combined with self-configuration capabilities of IPv6 will facilitate the creation and deployment of new tools. In this respect, the developers of tools will be able to concentrate on the service to the user and delegating into basic IPv6 capabilities such communication aspects, which are not critical for the teachers and learners experience.

Anycast services will facilitate the location of servers, load balancing and service discovery transparently for the application access through the portals. The access to the web servers will be easier because of the elimination of NATs and the availability of IPv6 addresses for each person or company that want to maintain a permanent web server.

Regarding the production of **content** there is not any relevant influence of IPv6 that could improve their production and/or distribution.

The use of broadband networks will simplify the design of tools and enrich the content information tele-education services will be able to distribute. More information (video, audio, slides, etc.) distributed at the same time, and with better quality will have a direct impact on the learning process. It will increase the immersion effect of the tele-education sessions, decrease the fatigue of students and teachers and improve the effectiveness of the media used during the sessions.

5.5.4 Future Trends

According to the scheme described in section 5.5.1, and the impact of IPv6 and broadband facilities described in section 5.5.2, we may foresee some characteristics of education services and applications based on IPv6 using broadband networks:

- More complex but easier to build systems relying on the basic IPv6 facilities: IPsec, QoS, self-configuration, and IPv6 address availability. Overlay networks required for such services will be simpler.
- Distributed systems based on small collaborating agents and hardware components, focused on the functionality delegating on IPv6 such communications functionalities, which are more complex: self-configuration, QoS and security.
- The acceptance of IPv6, larger network bandwidth, and uniform software facilities such as Java or C# will combine to provide a powerful platform for creating new and much more effective education platforms.
- An indirect effect of IPv6 deployment will be the wide availability of devices with wireless. One of the current problems related to IPv4 is the shortage of IP addresses for wireless devices. This problem will be solved by the usage of IPv6, enabling the integration into education systems many tools for supporting learning with wireless and self-configuration support.
- Broadband networks will enable the use of richer media, with higher quality that is less tiring for the people involved. The expected ubiquity of the broadband all-IP networks will allow students to use tele-education services anywhere, anytime according to the demand of the highly mobile users of the future.

Summarising, the deployment of IPv6 and broadband networks will allow the deployment of ubiquitous and high quality tele-education services affordable for most users, surpassing the limitations imposed by current narrowband and IPv4 networks.

6.5.6 Acknowledgements

Sections 5.1 and 5.5 were contributed by Juan Quemada and Tomas Robles (Universidad Politécnica de Madrid). Section 5.2 was contributed by Jordi Palet (Consulintel). Section 5.3 was contributed by Peter Kirstein (University College London). Section 5.4 was contributed by H.-J. Vögel (BMW).

5.6 References

[1] http://www.darpa.mil/

[2] http://www.cairn.net/

[3] http://www.kame.net/

[4] 14. P. Kirstein, P. O'Hanlon, K. Carlberg, P. Gevros and K. Hasler: "The Radioactive Networking Architecture", DARPA Active Networks Conference and Exposition, 29 – 30 May, 2002, San Francisco, USA, pp 394-408, IEEE Computer Society

[5] http://www.netinformations.com/Detailed/113602.html

[6] http://www.ipv6.or.kr/archive/ipv6forum/html/0570.html

[7] http://insc.nodeca.mil.no/ifs/files/startframe.html

[8] http://www-jta.itsi.disa.mil/ipv6/docs/insc-symposium.pdf

[9] http://www-mice.cs.ucl.ac.uk/multimedia/projects/vpn/

[10] http://www.cs.ucl.ac.uk/research/icb/

[11] http://lists.jammed.com/ISN/2003/06/0061.html

[12] http://www.landfield.com/isn/mail-archive/2003/Jun/0064.html

[13] http://moonv6.sr.unh.edu/Moonv6FAQv1.7.pdf

[14] http://www.heise.de/newsticker/data/anw-21.10.03-000/

[15] http://www.ist-ipv6.org/modules.php?op=modload&name=News&file=article&sid=509

[16] http://www.parliament.the-stationery-office.co.uk/pa/ld199900/ldhansrd/pdvn/lds04/text/40421w03.htm

[17] *e*Safety Forum: "Intelligent Vehicle Safety Systems - *e*Safety Forum 2003 Summary Report", Information Society DG, Commission of the European Communities, March 2004.

[18] http://www.ist-daidalos.org

[19] http://www.ertico.com/activiti/projects/gst/gst.htm

[20] ISO TC204 ITS (Intelligent Transport Systems) - Working Group 16 - Wide Area Communication

[21] http://www.ertico.com/activiti/projects/prevent/prevent.htm

[22] Car-to-Car Communications Consortium C2CCC

[23] Vehicle Safety Communication Consortium VSCC

[24] "La sociedad de la Información en España 2003". Telefónica S.A. 2003.

[25] T. de Miguel, J. Quemada, S. Pavón, J. Salvachua, T. Robles, G. Huecas, H. Velayos, E. Castro. "Advanced Collaboration Service over Broadband Networks: The ISABEL Experience". Internet Next Generation in Europe, ISBN 84-923942-1-8, pp. 143-160, 2000.

[26] "Definition of Statistics, Management and Security Control Systes". Euro6IX Project. December 2002.

[27] "Learning Management Network Specification." D1.2. Elena Project. April 2003.

[28] J. Quemada, J. Salvachúa, G. Huecas, Blanca Rodríguez. "Sharing live educational resources in UNIVERSAL with ISABEL". Computers and Education Towards a Lifelong Learning Society, Kluwer Academic Publishers. Dordrecht The Netherlands. ISBN 1-4020-1599-2, pags: 115-126, 2002.

[29] Tomás P. de Miguel, Juan Quemada, Eva Castro, Santiago Pavón, Gabriel Huecas, Tomás Robles, Joaquín Salvachua, Javier Sedano, María José Perea. "Porting applications to New Generation Internet, the ISABEL case study" CONFTELE 2003 18, 20 June Aveiro, Portugal.

[30] Yann Adam. Bruno Fillinger, Isabelle Astic, Addelkader Lahmadi and Patric Brigant. "Deployment and Test of IPv6 Services in the VTHD Network". IEEE Communications Magfazine, January 2004.

6 Broadband in Europe and Rest of the World

6.1 Introduction

The following sections introduce the development of broadband in Europe, with some brief introduction to details about the overall progress, and more specific data for U.S.A. and Japan.

The information from Japan is key when related to IPv6, as this country is, at the present time, the one that is having the biggest penetration in terms of IPv6 development, considering both industrial products and service providers. That doesn't mean that all the broadband deployment is actually being done with IPv6, but announcements oner recent years show the potential for the bigger providers, such as NTT, IIJ and SoftBank BB, amongst others, to make their broadband infrastructure and access networks IPv6 capable in a short time.

Is also clear that the deployment of broadband without the provision of IPv6, in the long term, is a potential stumbling block for the deployment of new and better services and applications. IPv6 is a key driver for innovation, enabling secure end-to-end connectivity for all broadband subscribers, and allowing an unlimited number of devices, services and applications to work seamlessly.

Excellent examples have already been introduced in the previous section, such as GRIDs, Ambient Intelligence, *e*Learning, etc. But we can also consider new green fields like *e*Safety, *e*Health, among others, which remain to be exploited to take full advantage of broadband. This will not happen if not done together with the deployment of IPv6.

There is not an easy technical way, today, to fully exploit the broadband capabilities of new services and applications, other than using IPv6.

IPv6 is turning quickly into a "new business enabler", adding value to existing and future broadband technologies. An interesting case has been introduced already with the deployment of Power Line Communications (PLC), also called Broadband Power Line (BPL) in North America. IST funded projects such as 6POWER [1] worked on exploiting the advantages of PLC and IPv6, and even developed business plans that show the key relevance of IPv6 to those deployments [2].

Other IST funded projects, such Euro6IX [3], are still working on the provision of IPv6 in broadband core and access infrastructures, in order to fully take advantage of the potential exploitation of IPv6 in European networks.

Finally, when extending the concept of 'Broadband' into 'Broadband for All', is key to ensure that the deployment of broadband does not mean a widening of the digital divide. IPv6, once more, together with technologies like PLC and Wireless, is a facilitator for this goal, as depicted in 'Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communications' [4].

6.2 Broadband in Europe

6.2.1 Introduction

Broadband plays a major role in modernising economies. As an enabling technology, it is at the core of the diffusion of the information society and of the development of information and communication technologies (ICTs). These technologies in turn are key drivers of productivity and growth. Broadband also enables the delivery of new advanced content. It promotes the development of new services and improved delivery of those that already exist. It allows the re-organisation of working and production processes. All of these developments bring significant benefits to businesses, administrations and consumers.

The benefits of broadband are widely recognised. All Member States of the Union are already exploiting these benefits as they experience significant increases in deployment and take-up. This development, which is largely market driven, is highly encouraging. There are nevertheless obstacles to more rapid progress. It is clear that public policies to encourage investment in broadband infrastructure, applications and services can have an impact. Indeed all Member States have now drawn up National Broadband Strategies, which propose a series of initiatives to deal with these obstacles and to accelerate the deployment and take-up of broadband.

These strategies contain a wide array of initiatives both on the supply-side (infrastructure deployment) and on the demand-side (increased usage) of the market. Two key areas of focus include increasing deployment in underserved areas, with public support foreseen in areas where market forces fail to work, and on aggregating demand from public administrations.

6.2.2 What is "Broadband"

The term "broadband" is defined as follows in the "Broadband Manifesto" (March 2002) by EICTA: "a basic utility that allows people to access and exchange rich media content, video, music, community services, business applications, and much more, at high speed over a variety of wireline and wireless access networks".

When commonly talking about broadband we usually to refer to a high-speed digital connection. The Federal Communications Commission (FCC) considers high-speed connection to be 0.2 Megabits per second (Mbps) or faster.

That speed permits a new Web page of mixed text and graphics to appear on a computer monitor in about the same length of time that it takes to turn the page of a book. Critics of the FCC's definition say 0.2 Mbps is not fast enough to deliver compelling applications and new services to the consumer. For example, transmission of DVD-quality video in real time requires a speed of about 5 Mbps, HDTV requires about 10 Mbps and the proposed digital cinema standard up to 200 Mbps.

Anyway, for all that, broadband may enable in terms of applications and services, the availability of broadband depends primarily on infrastructure or broadband access. "Broadband access" refers to the physical connection between terminal equipment at end user premises and the communication network.

There does not appear to be a universally optimal broadband technology. Rather, different broadband technologies seem suited to different environments, with relative benefits depending largely on what

they are used for. This is emphasised by the fact that a technology that proves successful in some countries may not work well in others, due to economicl, cultural, political, geographical, or other factors. Indeed, the medium of choice may depend upon the legacy medium, the regulatory framework and the supporting institutional arrangements.

The infrastructure or broadband access can be said to fall into two basic categories: wired (fixed - line) and wireless.

6.2.3 Fixed-Line Infrastructure

Digital Subscriber Lines and cable modems are the most popular fixed-line technologies for the last mile. While a single strand of fibre optic cable carries tens of billions of bits of data per second, residential Internet connections over copper phone and cable wires rarely exceed one million bits per second down-stream.

Recently, fibre optic networks have become a solution for residential Internet connections, and in several European cities power lines may also be used through the Power Line Communications technologies (PLC).

In the figure below we summarise some fixed-line solutions for broadband access.

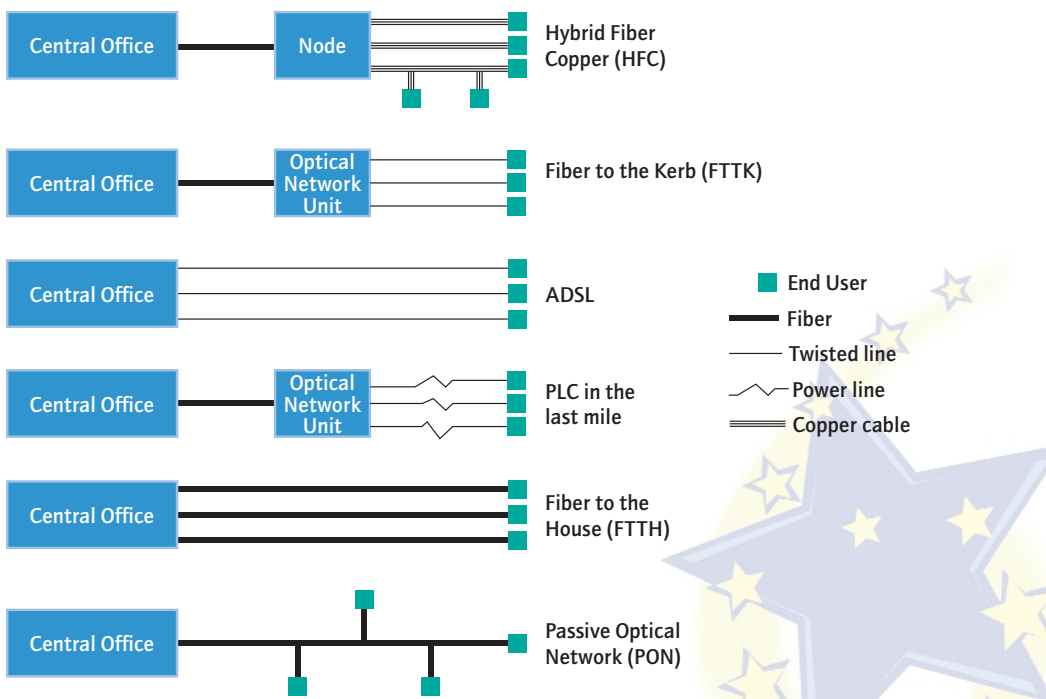

Figure 6.1: Fixed-Line Solutions for Broadband Access

6.2.4 The Role of Content, Services and Applications

The value-add of broadband depends on the applications it enables, the content it makes accessible, and the way it is effectively used. Like all networks, however, broadband is characterised by the 'chicken-and-egg' problem: demand for broadband will lag as long as innovative applications, services and content are not developed, and there will be no real push for new applications, services and content as long as the supporting infrastructure is not sufficiently deployed. The need to promote a virtuous circle by promoting a secure broadband infrastructure, while at the same time promoting more attractive content, services and applications is at the heart of the strategy of the *e*Europe 2005 Action Plan. It is also reflected in the mix of demand- and supply- side initiatives currently underway in the Member States. Several important issues, however, have to be addressed in this context.

The first relates to the fact that, while the increased availability of online music, films, and other kind of multimedia content improves the attractiveness of broadband, it also raises concerns related to the violation of copyright laws. In this context, there is a broad consensus that DRM technologies will help to establish the right incentives for all stakeholders, including a secure environment for ensuring remuneration of right-holders, payment for online content, and prevention of illegal copying. DRM technologies are key to the development of new business models that minimise risks and costs faced by content providers when bringing content online.

Two other issues are security and interoperability, and the effect they have on take-up by consumers. The 'always-on' feature of broadband increases the vulnerability of networks and of the information transmitted on them. Fully interactive applications, including for public services, require an adequate level of confidence in areas such as identity management or e-payment. Interoperability is also an area of concern in particular in view of the convergence of technologies and the increasing availability of content on different platforms. These issues are addressed in the framework of *e*Europe 2005 and its current update following the mid-term review of the Action Plan.

6.2.5 Main Elements of National Broadband Strategies

Competition has a central role in driving broadband penetration and take-up, which stresses the importance of effective implementation of the new regulatory framework for electronic communications. At the same time, developments across the EU are far from uniform, and in particular cases, for example rural and remote areas, SMEs, there are obstacles to deployment and take-up of broadband.

It is against this background that Member States have drawn up their strategies for broadband. While all Member States highlight the importance of competition and convergence across alternative platforms, and the role of the new regulatory framework for electronic communications to enhance competition, there is recognition that competition is most effective in densely populated areas. Other policy instruments are needed to address market failures such as insufficient commercial incentives to provide infrastructure to rural and remote areas. Public policy may also improve the functioning of the market by addressing simultaneously problems on the demand and the supply side, thus breaking out of the vicious circle where development of better content and services depends on infrastructure deployment, and vice versa.

The main initiatives presented in the national strategies address both the need to increase broadband deployment in under-served areas and to stimulate demand through financial incentives, aggregation of public demand, and increased usage by administrations, schools, health centres and SMEs.

6.2.6 Growth of Broadband

Deployment and take up of broadband are increasing at a fast pace in the European Union. At the end of 2003 there were 22.8 million connections, an increase of about 150% in eighteen months. All Member States are experiencing this rapid expansion, but disparities are still significant. The average EU-15 penetration rate (defined as number of subscribers as a percentage of total population) increased from less than 4% at the end of 2002 to 7.6% at the middle of 2004. Data on broadband connections from household surveys indicate that more than 20% of Internet connections were broadband connections in the first quarter of 2003. This is a substantial achievement though it falls short of the target of 50% for broadband Internet connections in the EU by 2005 proposed by the Commission in 2003.

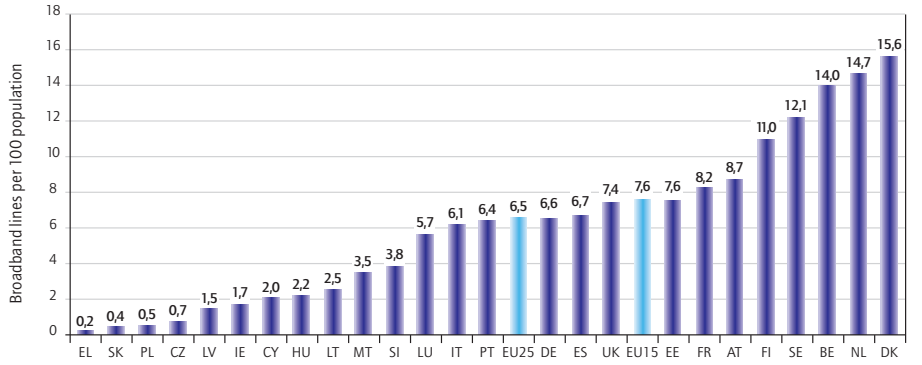

Figure 6.2: **Fixed Broadband Penetration Rates (EU-25, July 2004)**

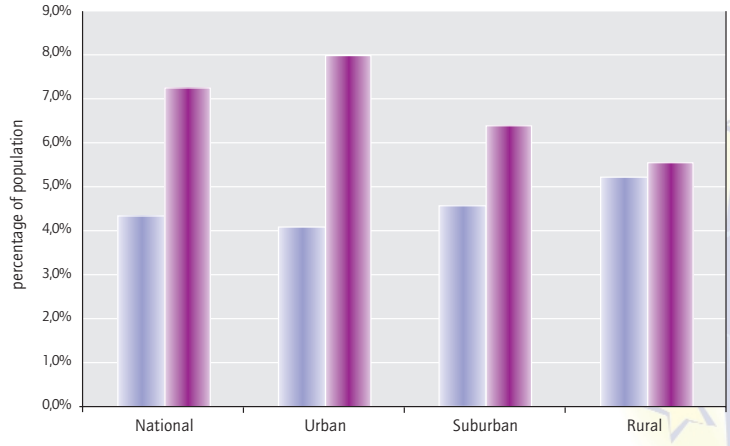

Figure 6.3: **Growth in Penetration/Coverage Rates (June 2003 - 2004)**

Recent broadband developments are mainly driven by DSL technologies. This is mainly because of the wide reach of Public Switched Telephone Networks. Where available, however, cable networks started being upgraded to broadband. Other technology platforms are still in the early stages with few subscribers.

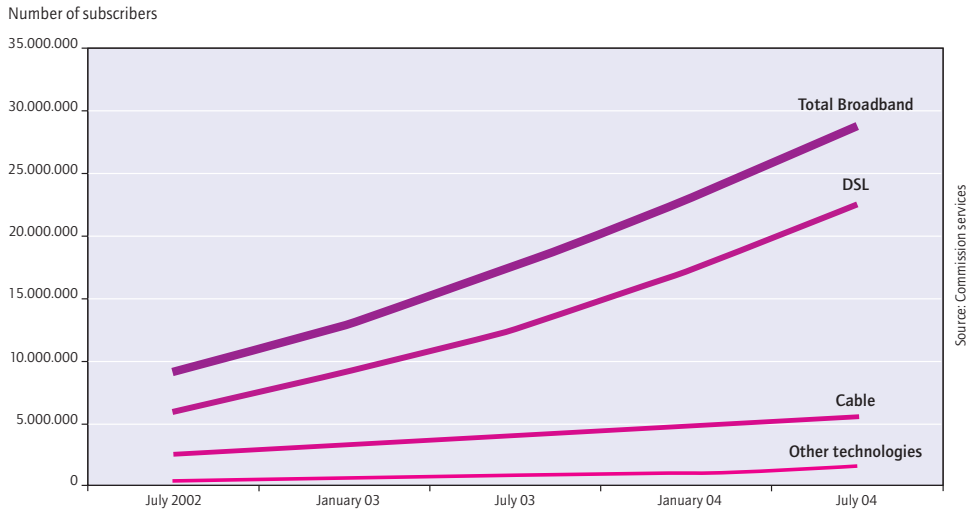

Figure 6.4: **Broadband Take-up by Technology (EU-15, July 2004)**

6.2.7 An International Comparison

Some Member States had an early start in broadband deployment and have reached levels of penetration of above 10% of the population. Five countries have penetration rates above the United States, but they still lag behind South Korea and Canada.

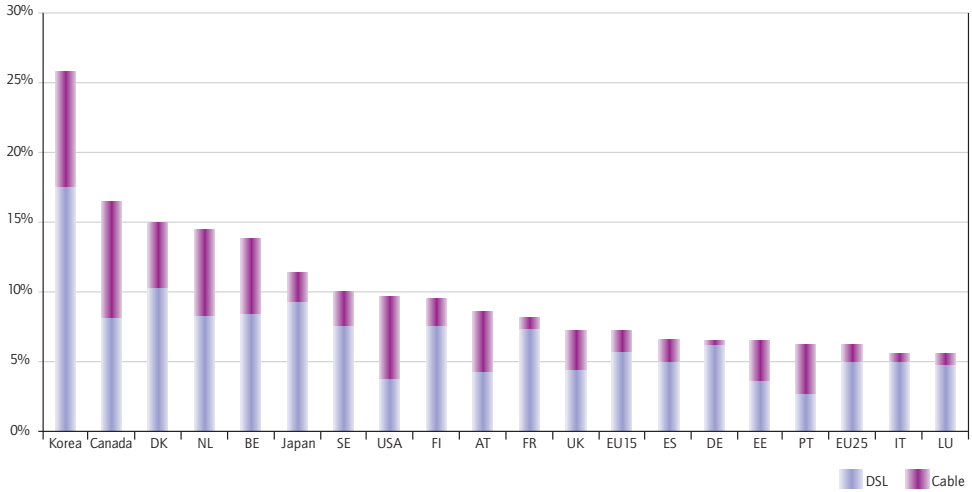

Figure 6.5: **Broadband Penetration (per 100 population, July 2004)**

South Korea, with a penetration rate of 26%, has maintained its leader position. Markets in other Asian countries such as China are beginning to take off. During the second half of 2003, the fastest growing markets in the European Union have been those of Denmark, the Netherlands, France and Italy. France and Italy are witnessing strong growth in DSL connections, with France achieving a penetration rate above EU average. Data from Greece and Ireland also show significant growth rates, witnessing a true take-off of the market.

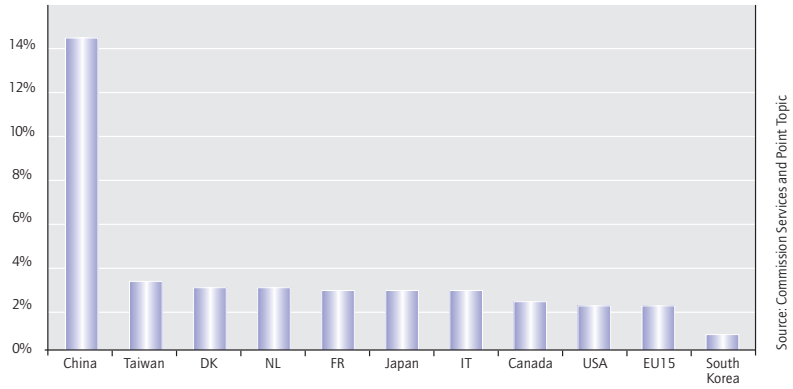

Figure 6.6: **Growth in Broadband Penetration Rates (July 2003 – January 2004)**

6.2.8 The Role of Competition

Competitive broadband markets are prone to grow faster. Facility-based competition or open access provisions on incumbent's networks delivers benefits in terms of the price/performance ratio and increased diversity of choice for consumers. These principles have been embedded in the new regulatory framework for electronic communications. Recent developments corroborate these views. Competition on the broadband market is still weak but generally improving.

The best performing countries in the Union and abroad are characterised by a significant degree of facility-based competition between DSL and cable. Competition between alternative platforms improves customers' choice and allows providers to control all aspects of their network, including costs and maintenance. In general, there is a positive correlation between facility-based competition and growth in penetration rates:

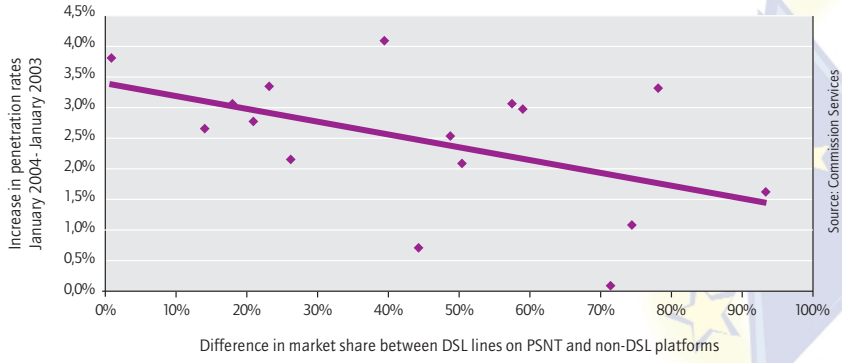

Figure 6.7: **Broadband: Facility-based Competition and Growth in Penetration rate**

Facility-based competition is not widespread in the Union. Cable coverage is relatively limited, especially in the large countries (with the exception of the UK). New platforms bringing fibre-to-the-home have been built in Sweden and Italy, although mainly in urban areas. Wireless technologies are expected to change the market in the medium term, but currently provide a viable alternative only through local trials.

6.2.9 Price Considerations

Stronger competition is ultimately reflected in the behaviour of retail prices. It is therefore useful to investigate the relationship between broadband take up and prevailing retail prices. Prices vary across countries, and the comparison is complicated by the different speeds offered and by variations in pricing structures. The Figure below shows prices charged by incumbents in the Member States for different speeds as of February 2004. Prices relate to monthly residential unmetered offers, and do not take into account the initial fixed cost of the modem. Prices are comparable across countries at low speeds, while variations are more pronounced at higher performances. Tests on the correlation between broadband penetration and prices confirm that prices are significant determinants of broadband take up at all performance levels, except for speeds above 2Mb/s. In this category, the availability of high-speed offers seems to be attractive in itself, independently of the price.

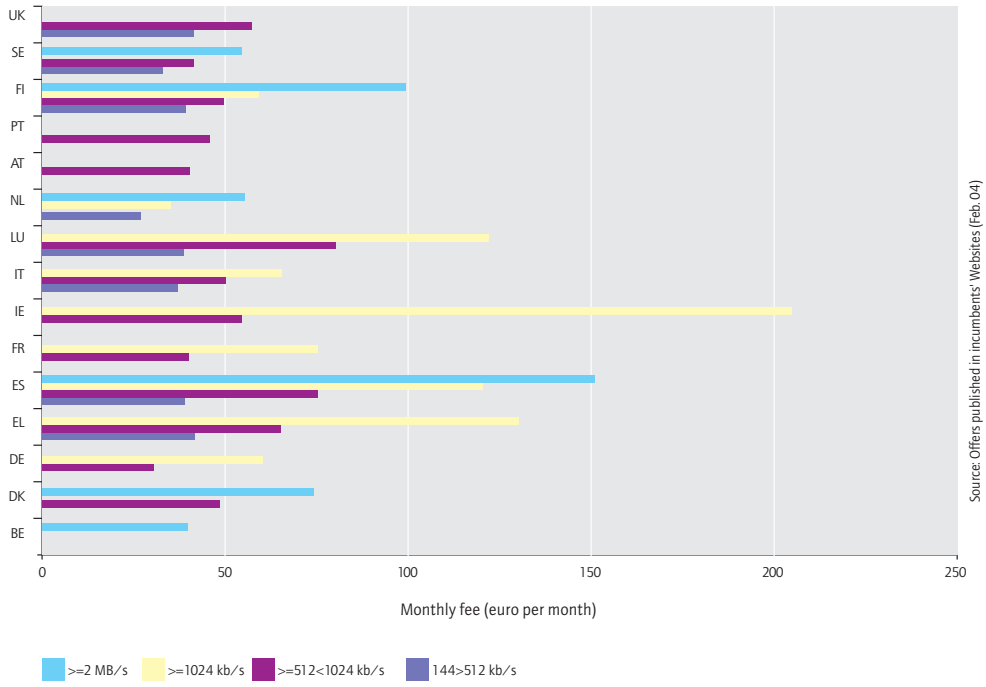

Figure 6.8: **Incumbents' Prices for Unmetered Residential DSL (february 2004)**

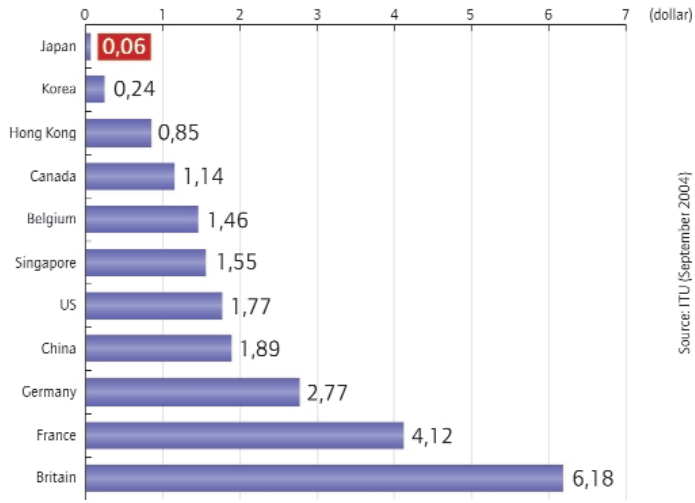

Figure 6.9: **Comparison of DSL Service Charge per Speed (in dollar per 100kbps) among Different Countries**

6.2.10 Latest Developments

Broadband has soared in 2004, according to the BBC, and such enthusiasm is unlikely to dampen any time soon. The two key factors in whetting people's appetite were falling prices and a huge marketing push.

For those who became 'broadbanders' in 2004 there was no turning back and the days of waiting for the modem to kick in began to seem as outdated an idea as a jungle without celebrities.

The entire world was falling in love with the benefits of fast Internet access, to the tune of 100 million connections worldwide by April, prompting research firm Point Topic to declare it one of the fastest growing technologies ever.

In countries such as France and the Netherlands, homes are routinely enjoying speeds of up to 15Mb (megabits per second). World leaders are Japan and South Korea, where around 70% of households have a broadband connection of more than 20mb.

Another big piece of news for broadband users in 2004 was the extension of DSL's reach. For example, BT assumes now that more than 95% of the UK population could get broadband, regardless of how far away from the exchange they live.

Broadband can seem confusing for consumers, with the huge amount of operators offering so many different products, some with capped bandwidth and different length contracts and set-up fees.

It is unlikely to get any easier to understand in 2005 but remains a plane worth catching.

As it gets faster and offers extras such as cheap telephone calls online, the only real thing to remember for the coming year is to enjoy the ride.

6.2.11 Powering Up Broadband

Providers flipped the switch on a new form of broadband access this year, with the first deployment of broadband-over-power-line being rolled out in China and the U.S. With the FCC giving the thumbs up to BPL, many are expecting it to give other high-speed access options like DSL and cable a run for their money.

Big power companies see BPL as a way to expand their business and note that the infrastructure is already in place, but there are still several serious technological hurdles that must be overcome before BPL becomes a major player in broadband access.

6.2.12 The Future

In the future Broadband is set to get even faster, with video-quality bandwidth expected by 2010.

Services will increasingly come bundled with telephony and TV. High-definition television over broadband networks is likely.

Future services will include video-on-demand and time-shifted TV.

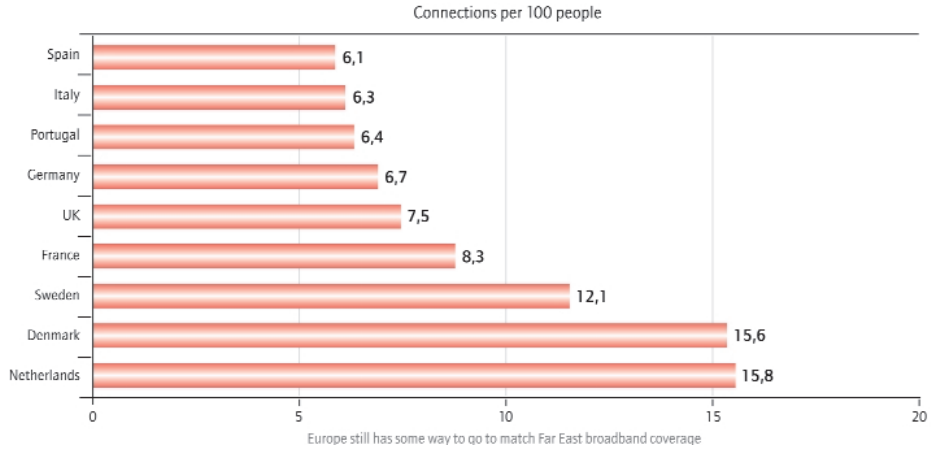

Figure 6.10: **Broadband around Europe**

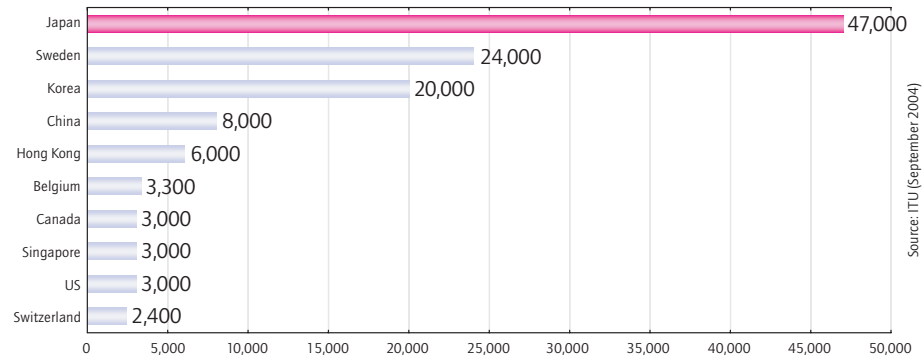

Figure 6.11: **Comparison of DSL Downstream Speed (in 100kbps) among Different Countries**

6.2.13 New Member States

Eastern Europe is emerging as a hotbed of growth for broadband connectivity, with connections in new European Union countries rising more rapidly than in the rest of Europe, according to the latest stats from the European Competitive Telecommunications Association (ECTA) [5].

The 10 newest E.U. states racked up 1 million connections by the end of last year's third quarter, a 29 percent increase on the previous quarter, and double the 14% growth for the E.U. as a whole, which had 33.7 million lines.

As the map below shows, while broadband growth is in double digits in countries across the E.U., the most rapid growth is in these newer members [6]. Slovakia and the Czech Republic, for example, both saw the number of connections jump by more than 40 percent between the second and third quarters last year.

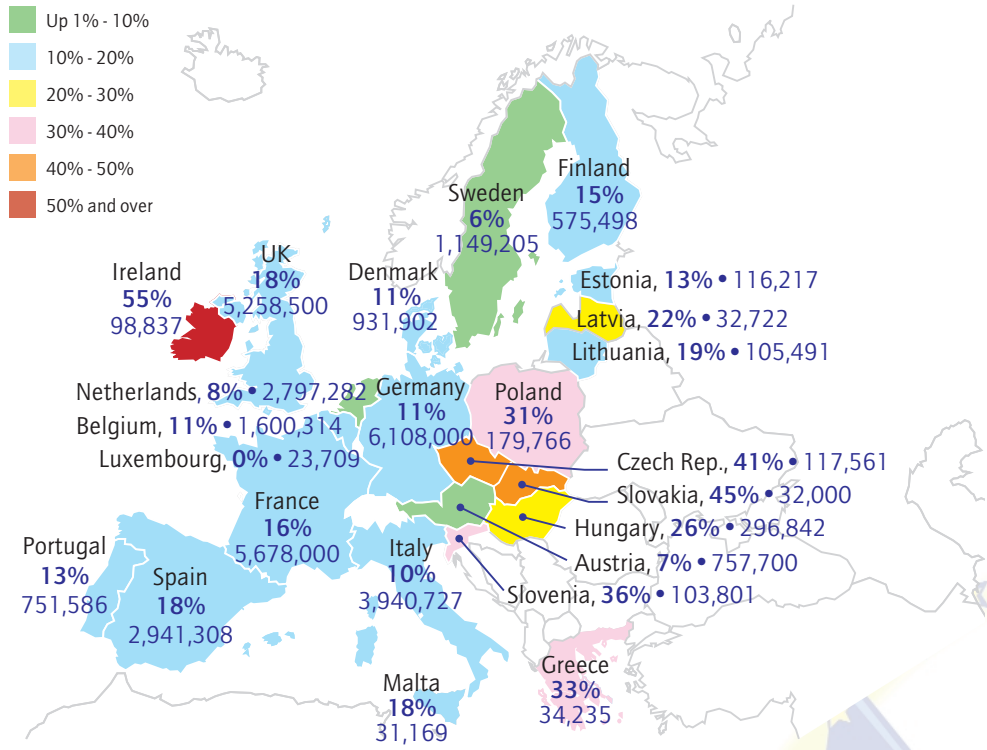

Figure 6.12: **Broadband growth in Europe**

6.2.14 Conclusion

Overall, competition is limited but there are signs of improvement. The rapid growth in broadband take-up witnessed over the past two years is clearly linked both to facility-based competition and the increase in competition in DSL. High penetration rates are related to more attractive offers in terms of prices and speeds. This strengthens the importance of the quick transposition and consistent implementation of the new regulatory framework for electronic communications, which facilitates market entry and is based on a technology-neutral approach that takes convergence into account.

6.3 Broadband in U.S.A.

The number of American consumers and businesses that subscribe to high-speed Internet service, or broadband, jumped 38 percent in the year ended June 30, 2004.

About 32.5 million broadband lines connected homes and businesses to the Internet, up from 23.5 million at the end of June 2003, the U.S. Federal Communications Commission said in its semi-annual report of the latest statistics.

Even with the penetration rate increasing, the United States continues to fall behind other countries in the rankings for broadband subscribers, falling to 13th in the most recent rankings by the International Telecommunications Union.

The FCC has argued that many Americans have broadband at work and thus are less likely to subscribe at home. Further, agency officials have said that some countries higher in the rankings have subsidized deployment and are more densely populated.

6.4 Broadband in Japan

Japanese broadband Internet services connected 17.6 million subscribers at the end of September 2004, according to the Ministry of Information and Communications. The growth of subscribers has been steady for the past several years, although it has somewhat slowed in 2004. With the number of households in Japan amounting to 49.8 million, the broadband penetration rate is 35.3%. According to an Impress survey [6], the Internet penetration rate (including narrowband connections) in July 2004 is 78.8%.

ADSL connections reached 12.8 million, or 72.7% of total broadband connections in Japan. CATV Internet subscribers and FTTH subscribers reached 2.8 million and 2.0 million, respectively. One of the most notable trends in recent months is the growth of FTTH services. Comparison of the growth rates between ADSL and FTTH from June 2004 to September 2004 illustrates this. In this three-month period, FTTH grew 15.3%, exceeding the ADSL growth rate of 5.6%. NTT group is increasingly aggressive in its attempt to move their users to fibre-based services, while power utility companies are prepared to battle it out.

Flet's ADSL NTT East, an average Japanese ADSL service, charges 3,000 yen (29 dollars) per month for maximum 47Mbps downstream and 5Mbps upstream connection. B Flet's, an FTTH service bythe same company, is offered at exactly the same monthly charge for collective housings, and 5700 yen (55 dollars) for individual houses for 100Mbps maximum upstream and downstream connections.

Service providers are also coming up with richer application services for FTTH. Many FTTH service providers offer video-on-demand or IPTV services for viewing TV through dedicated set-top boxes, while ADSL users can enjoy limited video contents only on their PC in general.

It is also noted that mobile phones have become a very popular terminal with which to access e-mail, Web browsing, music and other contents in Japan. According to the Ministry of Information and Communications, 73.6 million out of 85.5 million total mobile phone subscriptions used "browser phone" services. "au" by KDDI, one of three mobile phone service providers along with NTT Docomo

and Vodafone, introduced a fixed monthly charge for its multimedia content services, followed by a more limited but similar scheme from NTT Docomo. Such new pricing schemes will only accelerate the use of content services with mobile phones.

In general, Japanese ISPs are enthusiastically seeking to offer so called "Triple Play" or combined broadband data communication, IP phone and video services. The first generation of triple play services has used PCs as user terminals, but in the second generation, they have begun to try to bring these services to the living room.

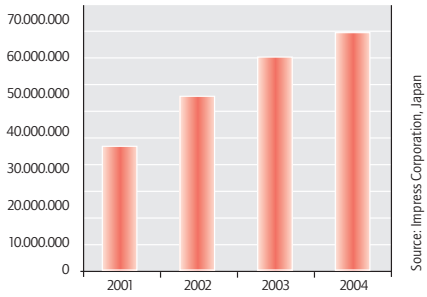

Figure 6.13: **Number of Internet Users in Japan (Broadband and Narrowband)**

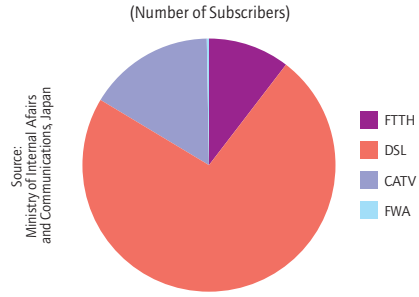

Figure 6.14: **Broadband Internet Access in Japan (June 2004)**

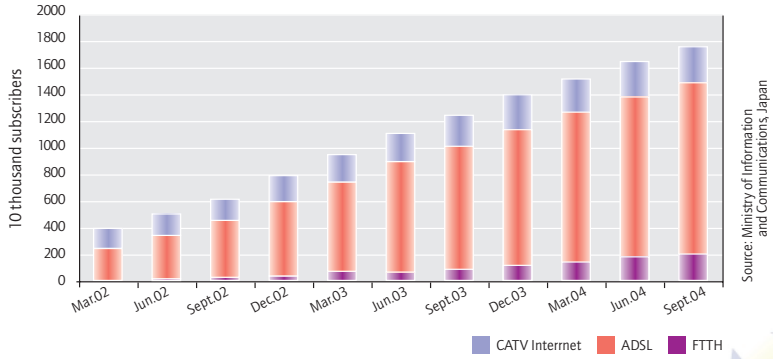

Figure 6.15: **Internet services in Japan (September 2004)**

Japan has achieved the best broadband Internet environment in the world in price and speed.

6.5 Acknowledgements

This section was contributed by Paulo De Sousa (European Commission), Izumi Miki (Impress Corporation) and Jordi Palet (Consulintel).

6.6 References

[1] http://www.6power.org

[2] http://www.6power.org/open/6power_pu_d1_2b_v1_3.pdf

[3] http://www.euro6ix.org

[4] http://www.isoc.org/briefings/013/index.html

[5] http://www.ectaportal.com/html/index.php

[6] The new member states, which joined the E.U. on May 1 last year, are Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, and Slovenia.

[7] http://en.impressholdings.com/

7 eServices, Broadband and IPv6

Athanassios Liakopoulos

Greek Research & Technology Network S.A. (GRNET)

1. Is there a need for IPv6 ? If yes, why ?

People in modern communities demand

a) easy and diverse ways of communication

b) to exchange gradually larger volumes of data

IPv6 protocol allows a huge number of new devices to be connected to the worldwide data network infrastructure. As the number of connected devices is increased, requirements (a) and (b) are more easily fulfilled. Obviously, these devices are not possible to get connected today due to the lack of IPv4 addresses. Therefore, IPv6 is a necessity for modern societies.

2. What are the major driving forces for IPv6?

The deployment of broadband services extends the network infrastructure almost everywhere. For example, "always on" connectivity for xDSL home Users extends the network inside the residences and gives the opportunity to connect devices that wouldn't be otherwise connected with any other technology. Furthermore, wireless hotspots will extend the network infrastructure to public areas, e.g. airports, allowing Users to connect their personal devices to the network in order to get access to services. Consequently, broadband services will increase the demand for IP addresses and, thus, for IPv6 technology.

The 3G mobile phones will further extend the network infrastructure. The number of mobile devices (and thus the need for extra IP address) is analogous to the number of mobile subscribers. Once again, the IPv6 technology will be only reasonable alternative to be used.

GRID technology and middleware aims to connect and control a huge number of devices, which are currently not connected to the network. Once again, IPv6 technology will be used to satisfy such needs.

a. What uniqueness/advantages one will gain with IPv6 to provide e-Services over Broadband?

The large number of available IPv6 addresses will minimize the need for NAT technology, which imposes significant limitations to services provided to devices behind firewalls, e.g. VoIP.

b. Will new p2p services be a driving force for IPv6?

Each "IPv6 device" connected to the network is a potential "p2p device", i.e. a device that communicates and exchange information with other devices. It is reasonable to believe that p2p services will be probably increased when IPv6 services are available in the network infrastructure as the number of connected devices will be sharply increased. However, p2p services may not be a driving force for IPv6 if the number of p2p devices is analogous to the number of Users. In such case, demand may be satisfied with currently available technologies.

3. What are the major driving forces concerning Broadband?

People demand efficient ways of communication and ask to be able to transfer more and more data volumes. This demand for "communication" can only be satisfied with broadband technology.

4. Which functions of IPv6 will facilitate the development of e-Services: Integrated IPsec support, Plug&play, QoS, etc.?

IPv6 stateless auto-configuration will definitely facilitate the development of new e-Services as devices will automatically get connected to the network without the need of human intervention. This will ease access to e-Services for Users that are less (or not) familiar with communication technologies. Also, MIPv6 technology will allow continuous access to e-Services by allowing Users to smoothly change networks without loosing access to offered service.

IPv6 "IPSec" and "QoS" features are needed for the deployment of advance services. However, these features alone are not "adequate" for the provisioning of secure communications with performance guarantees.

5. Will new IPv6-based mobile devices and UMTS broadband access impact the access to e-Services?

Definitely, it will have impact. Access to e-Services will be considered granted form everywhere, as they are voice services to GSM subscribers.

6. Are there any Business implications of IPv6 in Broadband?

IPv6 technology is not widely understood by the network administrators and by the potential Users. This may cause unexpected security problems or service degradation and, thus, the deployment of IPv6 services has to be well planned.

What are the alternatives to avoid IPv6 in your business?

IPv6 is the only future-proof solution that can satisfy the expected user needs. Therefore, there are no plans to avoid or delay the deployment of IPv6.

7. What is the current situation of Broadband applications and services concerning IPv6?

Broadband access in Greece is not widely available due to luck of competition in the local telecommunication market. The cost for broadband access, e.g. for DSL services to home users, is significant higher that the average cost of western European countries. Consequently, there is a limited portfolio for broadband applications and services while the IPv6 services are not provided at all.

What is the role of your Organization in this area?

GRNET, the Greek Research and Technology Network, currently provide native IPv6 services to the local Universities and research Institutes in Greece. Furthermore, IPv6 services are gradually deployed to all primary and secondary schools in Greece.

GRNET regularly organizes technical workshops, where technical administrators from universities, research institutes and commercial companies are invited to participate. Also, technical know and support is given to Universities that deploy IPv6 services in their campus networks.

GRNET set as a compulsory requirement the support of IPv6 for the in-house developed software. Also, it actively supports the campaign for IPv6 support for all the software developed with governmental funding.

GRNET provide also IPv6 service in the Athens IX.

8. Does your Organization have plans concerning the deployment of broadband networks, applications or services with IPv6 support for the next year?

GRNET will further support IPv6 deployment in local academic and research institutes. As GRNET is a research organization, it will continue to test IPv6 services or applications and provide feedback to research groups, network vendors, commercial companies and standardization bodies.

9. How long will take to deploy IPv6 services and applications for broadband networks?

Commercial IPv6 connectivity services will be supported by the end of 2005. Few applications will not be available by that time.

José Fernandes

Fundação para a Computação Científica Nacional (FCCN)

1. Is there a need for IPv6 ? If yes, why ?

Yes. Restoring end-to-end Internet and ending/reducing NAT usage and its false sense of security and give the chance to everyone to have an always-on connection at anytime.

2. What are the major driving forces for IPv6?

The political issues (unbalanced distribution of IPv4 address space), restoring end-to-end Internet and improving security and increase of address space to a virtually unlimited number. To launch new and innovative services and applications.

a. What uniqueness/advantages one will gain with IPv6 to provide e-Services over Broadband?

Network management gains. Possibility to offer public addresses to customers, and ending complex mechanisms usage like NAT and PAT. To give the chance to everyone to have an always-on connection at anytime.

b. Will new p2p services be a driving force for IPv6?

Yes. But probably after current p2p services start using IPv6.

3. What are the major driving forces concerning Broadband?

Improving the e-Society concept. More people will use e-services because with broadband it is more fun and a wider range of services is possible, more internet penetration leading to a mass usage of Internet.

Will new e-Services be a driving force for Broadband?

They can help in terms of growth.

4. Which functions of IPv6 will facilitate the development of e-Services: Integrated IPsec support, Plug&play, QoS, etc.?

Mostly the Integrated IPsec support. Some e-Services have serious gaps in terms of security. Changing the paradigm (making IPsec usage mandatory) will probably have a positive impact.

5. Will new IPv6-based mobile devices and UMTS broadband access impact the access to e-Services?

It should, as this means there are new ways of accessing it, potentially increasing the users accessing e-Services, and perhaps by bringing new users that will now start using some e-Services through these new platforms.

6. Are there any Business implications of IPv6 in Broadband?

Again, it should. Broadband also means an always-on access. The current practice in many countries is charging each customer for public IPv4 addresses (even against recommendations). By selling IPv6 local area network prefixes (/64s) or a set of them as recommended (/48s), instead of single or limited range IPv4 addresses, ISPs will provide better services to their customers, increasing their satisfaction and probably also their revenue. (If one sells a better product, why not charging a higher price?)

a. What are your business interests in this context?

Providing a true broadband connection to schools, Universities, etc.

b. What are the constraints from your point of view?

Limited amount of e-Services, and other end-users/endpoints using IPv6. If the user base increases, the value of having IPv6 connectivity also increases.

c. What are the alternatives to avoid IPv6 in your business?

None. As an NREN, we should be on the frontline, in terms of Internet evolution.

7. What is the current situation of Broadband applications and services concerning IPv6?

Very limited. Very early stage.

a. What is the role of your Organization in this area?

Our organization role has been to promote IPv6 usage. Unfortunately we are not seeing a wide set of broadband applications and services go live.

b. If you address specific sectors (e-defense, e-health, e-transport, e-learning, e-administration, etc.) please specify the main players in that area, their business interest and available products?

We are mainly on e-learning and e-administration. We've already had some talks with Microsoft Portugal (MSFT).

8. Does your Organization have plans concerning the deployment of broadband networks, applications or services with IPv6 support for the next year?

Yes. The school network will upgrade from ISDN to ADSL on Q42004, and IPv6 is on the roadmap starting Q12005. This network should have around 8000 schools. In terms of Services, we've deployed several services in 2004, namely the webcast system (live feeds), and there is a considerable set of services scheduled for Q42004 and 2005 (Web-based services, and network services mainly).

9. How long will take to deploy IPv6 services and applications for broadband networks?

Our view is that this is a long and an evolving process. Generally speaking, it will take years to see every ISP to do that. From our point of view, enabling IPv6 on a given service is always a process that will take some months. Ensuring the IPv4 service is not affected is our main concern. Then in some cases, platform upgrades are needed, and that takes also some time.

Jeff Doyle

Juniper Networks

1. Is there a need for IPv6 ? If yes, why ?

IPv6 is essential for the continued growth of existing network services and the development of new services and applications. The growing economies of countries with enormous populations such as China and India is creating vast numbers of new consumers demanding mobile and Internet-based information, communication, and entertainment. IPv4 cannot long sustain the growth these new users represent.

2. What are the major driving forces for IPv6?

In addition to the increasing demand for new IP addresses as mentioned in answer to the previous question, the other major force driving IPv6 is the roadblock that existing Network Address Translation (NAT) devices pose to the development of new network applications. Security and QoS is distinctly limited when passing through NAT, as is the global network transparency necessary for large-scale peer-to-peer applications.

I am often asked what the "killer application" is for IPv6; such a question puts the cart before the horse. New "killer apps" will appear as the result of widespread IPv6 deployment, which by eliminating NAT creates a fertile environment for the creation of innovative new network applications.

a. What uniqueness/advantages one will gain with IPv6 to provide e-Services over Broadband?

By removing NAT from the equation, new security models using true end-to-end encryption and authentication, and end-to-end QoS models can be developed. These in turn are essential to new services.

b. Will new p2p services be a driving force for IPv6?

Absolutely. Mobile IP is often cited as an early IPv6 driver, but P2P is likely to be an even stronger driver. High-performance online gaming, content sharing, distributed data processing (grid computing), and groupware applications will all grow on P2P or hybrid client-server/P2P models. And as stated in answer to the previous question, vastly improved security and QoS, which can happen only over an IPv6 infrastructure, are essential to P2P.

3. What are the major driving forces concerning Broadband?

The popular buzzword in Asia is "Triple-Play Services": Internet, VoIP, and video services such as video on demand (VoD). The highly concentrated population centers in countries such as Japan, South Korea, Taiwan, and Singapore make broadband relatively cheap to deploy, which is why you currently see such strong leadership in triple-play broadband services in these countries.

Will new e-Services be a driving force for Broadband?

e-Services are essential to making broadband profitable. High-speed Internet and VoIP are a start, but entertainment and business services are where the profits lay.

4. Which functions of IPv6 will facilitate the development of e-Services: Integrated IPsec support, Plug&play, QoS, etc.?

All of the above—end-to-end security and QoS, plug-andplay capabilities, and mobile IP—are essential for new e-Services. IPv6 is not inherently any more secure than IPv4, nor does it offer better QoS (although there is the potential for developing better QoS qualities with IPv6). Rather, it is the elimination of NAT that will allow the application of new security and QoS models, and NAT cannot be eliminated without the enormous global address space provided by IPv6.

5. Will new IPv6-based mobile devices and UMTS broadband access impact the access to e-Services?

Only if they offer services that are observably better than services available with IPv4. Users do not care about the underlying technology, only the services.

6. Are there any Business implications of IPv6 in Broadband?

Not yet, but there will be as (again) better security and QoS models are introduced over IPv6.

What are your business interests in this context?

Core and edge IPv6 routers and access devices, and IPv6-enabled firewalls (Netscreen).

7. What is the current situation of Broadband applications and services concerning IPv6?

Services based on IPv6 broadband access to the home is currently being in trial deployment in Japan. Juniper Networks has been a leader in developing the IPv6 BRAS equipment necessary for these deployments, and is working closely with Japanese service providers to support the technologies and standards behind IPv6 Broadband access.

8. How long will take to deploy IPv6 services and applications for broadband networks?

IPv6 roadmaps provided by various countries and governmental organizations (Japan's e-Japan and e-Japan II, China's China Next Generation Internet (CNGI), the government-backed initiatives in South Korea and Taiwan, and the US Department of Defense's initiative) all set deployment goals between 2005 and 2011, at the latest. Academic IPv6 networks such as the US Abilene/Internet2, China's CERnet, and Europe's Dante/GEANT are well established. Commercial deployment is in the very early stages, and is focused on services to the home where technological challenges are minimal. Deployment of IPv6 services in enterprise networks is likely to take longer, due to a few technical hurdles yet to be crossed (such as IPv6 multihoming) and the need for a compelling economic incentive to switch to IPv6. Nonetheless, IPv6 broadband access will become ubiquitous over this decade, likely completely replacing IPv4 in the 2010 – 2015 timeframe.

Table of Figures

Links to IPv6

@HOM	http://www.at-hom.org
6INIT	http://www.6init.org
6LINK	http://www.6link.org
6NET	http://www.6net.org
6POWER	http://www.6power.org
6QM	http://www.6qm.org
6WINIT	http://6winit.org
6HOP	http://www.cwc.oulu.fi/projects/6hop
ANDROID	http://www.cs.ucl.ac.uk/research/android
CRUMPET	http://ist-crumpet.org
Daidalos	http://www.ist-daidalos.org
DRiVE	http://ist-drive.org
EU IPv6 Task Force	http://www.eu.ipv6tf.org
Euro6IX	http://www.euro6ix.org
Eurov6	http://www.eurov6.org
Future Home	http://www.future-home.org
GCAP	http://www.laas.fr/GCAP
GEANT	http://www.geant.net
HARMONICS	http://www.ist-harmonics.net
IETF	http://www.ietf.org
INTERMON	http://www.ist-intermon.org
IPv6 Forum	http://www.ipv6forum.org
IPv6 Task Force	http://www.ipv6tf.org
IPv6 Task Force SC	http://www.ipv6tf-sc.org
IST IPv6 Cluster	http://www.ist-ipv6.org
IST Projects	http://www.cordis.lu/ist/overview.htm
IST Research Networking	http://www.cordis.lu/ist/rn/ipv6.htm
LONG	http://www.ist-long.com
MESCAL	http://www.ist-mescal.org
MIND	http://www.ist-mind.org
Moby Dick	http://www.ist-mobydick.org
NGNI	http://www.ngni.org
NGNLab	http://www.ngnlab.org
OverDRiVE	http://www.ist-overdrive.org
SATIP6	http://satip6.tilab.com
SEINIT	http://www.seinit.org
SEREEN	http://www.sereen.org
TORRENT	http://www.torrent-innovations.org
Tsunami	http://www.eurescom.de/public/projects/P1100-series/P1113
Wireless Cabin	http://www.wirelesscabin.com
xMotion	http://www.ist-xmotion.org

For a complete and updated list, look at the IPv6 Cluster web site (http://www.ist-ipv6.org)

Design

sus@**susum**.org

IPv6 Cluster