

crumpet

6IX  
Euro6IX  
Plus the new Internet  
www.6ix.eu

IR6 WINIT

6Q  
6Q  
6Q

May 2005

Edition of the 6LINK European IPv6 Research and Development Series

DRIVE

ANDRISIP

Euro v6

FUTURE HOME

GAP

GEANT

HARMONICS

INTERMON

IPv6 TASK FORCE

LONG



NGN lab

MIND

MOBY DICK

NGN  
Next Generation Networks

XROTION



European Commission



Information Society  
Technologies

# IPv6 Cluster

## Moving to IPv6 in Europe



# Moving to IPv6 in Europe



# Moving to IPv6 in Europe

---



## **IPv6 Cluster Moving to IPv6 in Europe**

ISBN 3-00-011727-X

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/ISTClusterbooklet2003.pdf>).

Copyright 2003 EC IST 6LINK.


Reproduction in whole or in part is only authorized with explicit reference to this source.



## Index of contents

Preface .....	7
1. Introduction .....	9
2. IPv6 Research & Development in Europe.....	11
2.1. What is IPv6?.....	11
2.2. IPv6 in FP5.....	12
2.2.1. IPv6 Task Force .....	12
2.2.2. The Council of the European Union.....	12
2.2.3. The IPv6 Cluster .....	13
3. Development Issues for IPv6.....	15
3.1. IPv6 Plug and Play.....	15
3.1.1. State-of-the-Art.....	15
3.1.2. Service Discovery in IPv6 .....	17
3.1.3. IPv6 Plug and Play Networking in EU IPv6 Projects.....	18
3.1.4. Conclusions.....	18
3.2. Multicast .....	18
3.2.1. Why IP Multicast? - Some Application Scenarios .....	19
3.2.2. Role of Multicast in IPv6 .....	19
3.2.3. Short Introduction to IP Multicast.....	19
– Basic (simplified) Multicast Architecture.....	19
– Short Overview of Available IPv6 Multicast Implementations.....	22
– Open issues.....	23

# Moving to IPv6 in Europe



3.2.4. IPv6 Multicast Investigations in European Research Activities .....	24
– 6NET .....	24
– 6WINIT .....	24
– Android.....	25
– Euro6IX.....	25
– M6bone .....	26
– OverDRiVE .....	27
3.2.5. Conclusions.....	27
3.3. Mobility .....	27
3.3.1. State-of-the-Art.....	28
– Mobile IP.....	28
– Micro-mobility, or Local Mobility.....	29
– Mobile Networks.....	30
– Mobility based on Routing for Ad-Hoc Networks.....	31
3.3.2. EU Projects .....	32
– MIND (Mobile IP based Network Developments) .....	32
– Moby Dick (Mobility and Differentiated Services in a Future IP Network) .....	33
– OverDRiVE (Spectrum Efficient Uni- and Multicast Over Dynamic Radio Networks in Vehicular Environments) .....	34
3.4. Performance, Conformance and Interoperability Testing .....	34
3.4.1. Introduction.....	34
3.4.2. IPv6 Conformance and Interoperability .....	35
– Basic Principles of Conformance Testing.....	35
– IPv6 Conformance Requirements .....	35
– Worldwide IPv6 Conformance Test Facilities .....	35
– ETSI IPv6 Plugtests™ Events .....	36
3.4.3. IPv6 Performance Monitoring.....	37
– Requirements for Performance Monitoring in IPv6 Networks.....	37
– Performance Metrics.....	37
– Measurement Methods.....	37
– Intra- and Inter-domain Network Monitoring.....	38
– Performance Testing.....	39
– Performance Considerations for IPv6.....	40
– 5 <sup>th</sup> FP IST Projects Working on IPv6 Performance .....	40
3.4.4. Future Work Items.....	42
3.5. Security and IPv6 .....	43
3.5.1. State-of-the-Art.....	43
– IPsec.....	43
– Secure Neighbour Discovery .....	43
– Mobile IPv6.....	44
– CGA.....	44
– Transition mechanisms and security .....	45
– Firewalling .....	48
– Transient Addresses for Related Processes .....	49
3.5.2. Road Warrior .....	49
– Road Warrior Architecture .....	49

4. Impact of IPv6 on Applications and Services.....	51
4.1. Transition and Porting of Applications to IPv6 .....	52
4.1.1. Application Porting Problems.....	53
– Parsing IP addresses .....	53
– Use of special addresses .....	54
– Local IP address selection .....	54
– ADU fragmentation.....	55
– Use of IP addresses to identify elements.....	55
4.2. IPv6 Wireless Internet Initiative: Medical Application Scenarios .....	56
4.2.1. 6WINIT Project .....	56
4.2.2. The Whittington Hospital Scenario .....	56
4.2.3. The John Paul II Hospital Scenario.....	57
4.2.4. The Tübingen Guardian Angel System - GANS .....	58
4.3. eMobile Test-bed for Interoperability of Test-beds in eLogistics.....	59
4.4. IPv6 UMU-PKI Security Service .....	60
4.4.1. Porting the UMU-PKI to IPv6.....	60
4.4.2. Conclusions.....	61
4.5. IPv6-Enabled Real-Time Adaptive Applications .....	61
4.5.1. Architecture for Application Adaptation .....	61
4.5.2. Empirical Results .....	62
4.5.3. Conclusions.....	64
5. Research Networks Deployments.....	65
5.1. Rise and Fall of the 6Bone .....	65
5.1.1. Network Growth.....	65
5.1.2. 6Bone Phase-out Plan .....	66
5.1.3. Conclusion.....	67
5.2. 6NET: Large-Scale International IPv6 Pilot Network.....	68
5.2.1. Introduction.....	68
5.2.2. Network Design .....	68
– IGP .....	68
– Routing policy .....	69
– Addressing plan .....	69
5.2.3. Network Monitoring and Management .....	69
5.3. Euro6IX: Pan-European IPv6 Internet Exchanges Backbone.....	69
5.3.1. Introduction.....	69
5.3.2. Network Design .....	69
– Study of IX Models .....	70
5.3.3. Euro6IX Backbone Routing Policy .....	78
5.3.4. Other Research Activities .....	79
5.4. GÉANT - Providing Native IPv6 in Dual-Stack Mode .....	79
5.4.1. IGP Transition .....	79
5.4.2. IPv6 Design .....	80
– Routing policy .....	80
– Addressing plan .....	80
5.4.3. IPv6 Service Offering on GÉANT .....	80

# Moving to IPv6 in Europe



6. Future Development Paths .....	81
6.1. Brian E. Carpenter .....	81
6.2. Hiroshi Esaki .....	82
6.3. Patrick Grossetete .....	83
6.4. Christian Huitema .....	85
6.5. Wolfgang Noszek .....	87
6.6. Charles E. Perkins .....	87
6.7. Dale Robertson .....	88
Table of Figures .....	90
Links to IPv6 .....	91



## Preface

This publication provides an overview of European R&D activities in the IPv6 area, focussing on projects, networks, 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.

Editorial team:

- Olaf Bonneß (T-Systems Nova Berkom);
- Tim Chown (University of Southampton);
- Peter Christ (T-Systems Nova Berkom);
- Mat Ford (British Telecommunications plc);
- Hong-Yon Lach (Motorola Labs, France);
- Jordi Palet (Consulintel);
- Dale Robertson (DANTE).

The editors are particularly grateful to Vladimir Ksinant (6WIND), Pedro Ruiz (Agora Systems), Sven Ubik (CESNET), Nicolas Simar (DANTE), Pascal Drabik (European Commission), Elisa Boschi, Peter Deussen, Andreas Hoffmann, Axel Rennoch, Rudolf Roth, Florian Schreiner, Tanja Zseby (Fraunhofer FOKUS), Emile Stephan (FTR&D), Victor Reijs (HEANET), César Viho (IRISA), Paul Christ (RUS), Simon Leinen (SWITCH), Thomas Scheffler (T-Systems), Stig Venaas (Uninett), Antonio Gómez Skarmeta (Universidad de Murcia), Andreas Timm-Giel (University of Bremen), Tomás de Miguel, Juan Quemada (Universidad Politécnica de Madrid) and Eva Castro (Universidad Rey Juan Carlos I) for their valuable contributions to this publication.

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



# Moving to IPv6 in Europe

---





## 1. Introduction

The objective of this publication is to provide an overview of European R&D activities in the IPv6 technology area. The focus is on projects, networks, trials, and applications developed and demonstrated in the Information Society Technologies (IST) Programme.

The following topics are specifically addressed:

- Overview of the IST work programme and its relation to IPv6;
- Deployment issues related to IPv6 technology: IPv6 Plug and Play, Multicast, Mobility, Security, Performance and Conformance;
- Description of projects that have developed IPv6 applications and services, and;
- Research networks.

To complete the picture of the status of IPv6 technology in Europe, some interviews with key actors in the research domain are provided, offering insight into the potential impact 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.

For non technical information, like deployment roadmaps, please refer to the work of the IPv6 Task Force Steering Committee (IPv6 Overall Status documents at <http://www.ipv6tf-sc.org/html/deliverables.php>).

## Moving to IPv6 in Europe





## 2. IPv6 Research & Development in Europe

### 2.1. What is IPv6?

IPv6 is an upgrade to the data networking protocols that power the Internet. The Internet Engineering Task Force (IETF) developed the basic specifications during the 1990s after a competitive design phase used to select the best overall solution. The primary motivation for the design and deployment of IPv6 is to expand the available “address space” of the Internet, thereby enabling billions of new devices (PDAs, cellular phones, appliances, etc.), new users (countries like China, India, etc.), and new, “always-on” technologies (xDSL, cable, Ethernet-to-the-home, fibre-to-the-home, PLC, etc.).

While the existing protocol, IPv4, has a 32-bit address space that provides for a theoretical  $2^{32}$  (approximately 4 billion) unique globally addressable hosts, IPv6 has a 128-bit address space that can uniquely address  $2^{128}$  (about 340 undecillion!) hosts. In practice, the number of global IPv4 addresses that can be used is far less, due to inefficiencies in their allocation and use. IPv4 simply cannot support an Internet scaling to many billions of globally connected hosts. Network Address Translation (NAT) has extended IPv4's life<sup>2</sup> in conjunction with private IPv4 addresses<sup>3</sup>. However, NAT complicates application deployment and, more importantly, cannot support new Internet growth areas including those always-on and peer-to-peer services that require connections be established into devices in home networks and those networks obfuscated by NAT routers.

During the design of IPv6, the IETF took the opportunity to make further improvements above and beyond providing extra address space, making IPv6 extensible and highly adaptable to future requirements.

In short, technically speaking, the main advantages of IPv6 are:

- Expanded addressing capabilities;
- Server-less auto-configuration (“plug-n-play”) and reconfiguration;

<sup>1</sup> Actually 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses.

<sup>2</sup> Network Address Translator, IETF RFC1631, <http://www.ietf.org/rfc/rfc1631.txt>

<sup>3</sup> Address Allocation for Private Internets, IETF RFC1918, <http://www.ietf.org/rfc/rfc1918.txt>

# Moving to IPv6 in Europe

- More efficient and robust mobility mechanisms;
- Built-in, strong IP-layer encryption and authentication;
- Streamlined header format and flow identification, and;
- Improved support for options/extensions.

Some interesting features to mention are the removal of the checksum field from the IPv6 header (checksumming is now performed by upper layers), and the removal of fragmentation-related fields, (fragmentation is performed only by the communicating end systems). In fact, most IPv6 “options” (now called “extension headers”, with no limit to their size or number), are also processed end-to-end, obviating the need for routers to perform tasks other than simple packet forwarding.

Taken together, these features provide the means for restoring the end-to-end Internet paradigm<sup>4</sup>, facilitating peer-to-peer applications, end-to-end security, and avoiding network address translators.

## 2.2 IPv6 in FP5

### 2.2.1. IPv6 Task Force

The European Commission initiated a European-wide IPv6 Task Force driven by key European and worldwide players, to develop a comprehensive action plan by the end of 2001 aiming at ensuring the timely availability of IPv6.

The conclusions and recommendations of the Task Force were successfully submitted to the European Council Spring Meeting of 2002, under the Spanish presidency. In the context of this document, the Commission proposed a series of recommendations pertaining to the implementation of IPv6 by all relevant ICT sectors.

As a result, the Heads of State resolution was to prioritise the widespread availability and use of broadband networks throughout the Union by 2005 and the deployment of the new Internet protocol, IPv6, as part of the eEurope 2005 initiative.

One of the main achievements was a Communication from the Commission to the Council and the European Parliament called, “Next Generation Internet: Priorities for action in migrating to the new Internet protocol IPv6”.

As a complementary action, the European Commission called for the renewal of the mandate of the IPv6 Task Force as a platform for debate on critical issues concerning the deployment of IPv6.

As a consequence, a second phase of the European IPv6 Task Force was launched in September 2002. It provides a regularly updated review and plan of action, the “European IPv6 Roadmap”, on the development and future prospects of IPv6, including guidelines for transition from IPv4 to IPv6. It ensures a working liaison with international standardisation organisations, industry associations and Internet governance bodies. It also establishes collaboration arrangements and working relationships with similar initiatives being launched in other world regions.

The European IPv6 Task Force<sup>5</sup> is one of the main strategic instruments fostering the deployment of IPv6 technology in Europe.

### 2.2.2. The Council of the European Union

The Council of the European Union<sup>6</sup> in its meeting in June 2002<sup>7</sup> adopted several conclusions that address the Member States, the European Commission and the Private Sector. One of the conclusions regarding the European Commission concerns the renewal of the European IPv6 Task Force. This has been described in the previous section.

<sup>4</sup> Internet Transparency, IETF RFC2775, <http://www.ietf.org/rfc/rfc2775.txt>

<sup>5</sup> EU IPv6 Task Force, <http://www.ec.ipv6tf.org/>

<sup>6</sup> “Transport, Telecommunications and Energy” configuration.

<sup>7</sup> The outcome of the proceedings is available at the URL: <http://register.consilium.eu.int/pdf/en/02/st10/10381en2.pdf>

In its conclusions, the Council of the European Union:

- Stresses the need to remove obstacles to facilitate the transition to IPv6;
- Encourages the Member States:
  - To facilitate the efforts of stakeholders regarding the adoption and the deployment of IPv6, for instance through awareness-raising campaigns,
  - To facilitate, among other things by enabling IPv6, the integration of research networks with European-wide networks (e.g. GÉANT),
  - To monitor and assess the current development and take-up of IPv6, including the definition of guidelines and dissemination of best practice related to the transition towards IPv6, in cooperation with the private sector and standardisation bodies;
- Welcomes the Commission's intention to support research and development in the context of the 6<sup>th</sup> Framework Programme related to the deployment of IPv6 in fixed and wireless network infrastructures and in advanced infrastructures for research (e.g. GÉANT and GRID);
- Supports the Commission's intention to renew the mandate of the IPv6 Task Force;
- Invites the Commission to:
  - Evaluate the social impact on society, citizens and businesses of the implementation of IPv6,
  - Investigate security issues related to IPv6;
- Invites the Private Sector:
  - To consider initiatives aimed at the integration of IPv6 infrastructures, including the interoperability aspects of IPv6 services and applications,
  - To participate actively in the establishment of a European wide, vendor independent, training and education programme on IPv6,
  - To provide regularly updated information on the increased demand for IP addresses and the current status of IPv4 address space,
  - To actively contribute towards on-going IPv6 work within standards and specification bodies,
  - To fully participate in R&D activities in the context of the 6<sup>th</sup> Framework Programme, notably in the large-scale tests of IPv6 based services and applications.

## 2.2.3. The IPv6 Cluster

The European Commission Information Society Technologies Programme (IST) is funding 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 EC (about 90 M€). The project partners have collectively made a similar level of investment.

These projects can be divided into two categories. The projects of the first category, that can be called IPv6 Projects, have a particular emphasis on IPv6, with the main goal being research and development related to the protocol itself, its deployment and its promotion. Projects of the second category, that can be called IPv6 Related Projects, are employing IPv6 as part of their broader goals.

The projects are addressing different areas. Two complementary very large-scale experimentation platforms—6NET and Euro6IX—are investigating the real deployment of IPv6. Some other projects are devoted to the promotion of IPv6, including a political dimension. A large set of projects is addressing several technical aspects related to IPv6 (e.g. IPv4 to IPv6 transition, Quality of Service, etc).

The IPv6 Projects as well as the IPv6 Related Projects have been collaborating in the context of the IPv6 Cluster since June 2001. A specific project, 6LINK, is supporting the activity of the IPv6 Cluster.

A brief description of all the IPv6 projects launched in the context of the 5<sup>th</sup> Framework Programme can be found in the IPv6 Booklet "IPv6 Research and Development in Europe" produced by the IPv6 Cluster in October 2002<sup>8</sup>.

<sup>8</sup> Available for free download from the IST IPv6 Cluster website, <http://www.ist-ipv6.org>





## 3. Development Issues for IPv6

### 3.1. IPv6 Plug and Play

In this section we discuss the technical aspects of plug and play networking and how they may be affected and improved by the introduction of IPv6.

Plug and play networking refers to the ability for network devices to be deployed and configured, as much as possible, without significant human intervention. Ideally, devices could be deployed without any prior configuration. This is an important requirement in many network scenarios, particularly where user expertise is minimal, e.g. in home-networking environments. The average commodity user of IPv6 devices will not want to, or be able to, handle IP-based network configuration.

In emerging deployment scenarios, plug and play will become even more important. With sensor-based networks, pervasive and embedded devices, we expect to see the number of IP-based devices growing into the billions in the years to come. Many sensor and embedded devices will be difficult to pre-configure, thus plug and play networking is highly desirable.

IPv6 offers the globally unique address space to make such devices addressable from anywhere on the IPv6 Internet. It also gives mechanisms for such devices to autoconfigure their network connectivity.

#### 3.1.1. State-of-the-Art

IPv6, like IPv4, offers the option for devices to be configured through stateful autoconfiguration, via the Dynamic Host Configuration Protocol (DHCP). The IETF Dynamic Host Configuration Working Group has defined DHCPv6 for IPv6 hosts and devices. DHCPv6 has been through a lengthy definition process within the IETF, having just at the time of writing reached Proposed Standard status after 28 revisions.

Where existing site policy requires the use of managed configurations, DHCPv6 offers the network manager similar functionality to DHCP for IPv4. Many DHCPv6 options are also being defined for IPv6, including the ability to configure optional settings such as DNS resolvers, NIS, time settings and preferred network prefixes.

Where managed configurations are not required, IPv6 offers the alternative of stateless address auto-configuration through RFC2462. Through this standard, an IPv6 device can learn 128-bit IPv6 link-local and global network addresses, and the default router through which to send traffic to off-link destinations.



# Moving to IPv6 in Europe

The basic operation of RFC2462 runs as follows. An IPv6 router on-link will send periodic multicast Router Advertisements (RAs) that indicate the global scope 64-bit IPv6 network prefix to be used on the link, and, by the source address of the RA, the default router address for devices on the link. A host may listen for RAs on link, or send a Router Solicitation multicast message to request the on-link router(s) to send an RA. The RA includes a bit indicating whether devices on link should use managed (DHCPv6) or stateless auto-configuration.

The stateless autoconfiguration process requires two components, the RA and a unique EUI-64 identifier for the IPv6 host. The EUI-64 identifier is formed by taking the 48-bit IEEE MAC (usually Ethernet) address of the interface receiving the RA, and inserting "fffe" as 16 bits of "filling" in the middle of the identifier. A single bit in the identifier is used to indicate global uniqueness of the identifier (although this can never be verified). The apparently excessive size of the EUI-64 identifier allows expansion to 64-bit MAC addresses at a later date.

On receiving an RA, if stateless autoconfiguration is indicated, an IPv6 host can form a global IPv6 address by concatenating the IPv6 network prefix with the 64-bit EUI-64 identifier. It can also independently form a link-local address by taking the link-local prefix `fe80::/10` and concatenating the EUI-64 identifier with that. In disconnected networks, link local addresses provide a means for local communication in the absence of a router on-link.

As an example, if the RA indicates a global scope network prefix of `2001:630:ffd0:131::/64`, and the MAC address of the device is `00:30:48:51:56:4e`, then the EUI-64 identifier (with global bit set) is `230:48ff:fe51:564e`, and the statelessly autoconfigured global IPv6 address will be `2001:630:ffd0:131:230:48ff:fe51:564e`.

On a Linux system, the `ifconfig` command indicates network configuration:

```
/sbin/ifconfig
eth0  Link encap:Ethernet  HWaddr 00:30:48:51:56:4E
      inet addr:152.78.123.123  Bcast:152.78.123.255  Mask:255.255.255.0
      inet6 addr: 2001:630:ffd0:131:230:48ff:fe51:564e/64  Scope:Global
      inet6 addr: fe80::230:48ff:fe51:564e/10  Scope:Link
```

IPv6 includes a very useful feature not included in IPv4, namely Duplicate Address Detection. When a host forms an IPv6 address, it can use Neighbour Discovery to check whether another host on link has the same (link local or global) address.

In addition to link-local and global scope addresses, the IPv6 architecture also currently includes site-local addresses, which carry a prefix of `fec0::/10`. However, site-local addresses are seen as a potential cause of address ambiguity (e.g. when sites merge, or a device has two interfaces in different site-local addressed networks) and address leakage. At the time of writing, the IETF IPv6 working group is considering deprecating site-local addressing.

Where a site or a link has two ISPs providing connectivity, a host may see RAs from one or more routers with different global 64-bit prefixes. A host may thus statelessly autoconfigure with multiple IPv6 addresses, of various scopes. An RA may indicate router preference (priority) to indicate to a host which router should be used where two or more exist on-link. In addition, the host may use RFC3484 to select which source and destination addresses to use when communicating with other (possibly multi-addressed) IPv6 devices.

There are some important issues arising from stateless address autoconfiguration.

First, it is by default not secure. Any host may autoconfigure on a link, whether the network administrator wishes it or not. Similarly, any host can send out RAs, by design or misconfiguration, and cause other IPv6 hosts to add a new prefix and default router. The IETF Secure Neighbour Discovery Working Group is working on securing Neighbour Discovery to provide a more secure autoconfiguration environment.

Second, the use of the MAC address in autoconfiguration means that a host using RFC2462 on different network links will have a different (global) IPv6 address prefix on each link, but a common 64-bit EUI-64 host part of the address. As a result, a device may be tracked (correlated) when its source address is obser-

ved in IP packets on the network. To reduce this potential privacy threat, RFC3041 defines IPv6 Privacy Extensions, by which a host in essence uses a random 64-bit number for the host part of its IPv6 address. A host may generate new privacy addresses on a periodic basis (e.g. daily), meaning that host activity is more anonymous even when the host is static on a single link. While a host may have several privacy addresses over time, it may keep a single regular global IPv6 address to receive communications (avoiding the need to register each privacy address in the DNS, for example).

The introduction of RFC3041 (at the time of writing it is implemented by Windows XP) means that application developers need to consider, for example, that communications directed to a certain IPv6 address resolved in the DNS may result in data being returned from a different (privacy) address.

Also, IP address-based authentication for hosts (not a particularly great method, but one in widespread use) becomes problematic if the application cannot choose to use the host's regular IPv6 address for the connection requiring that authentication.

It is also perfectly possible to manually configure IPv6 addresses on hosts, and not use DHCPv6 or stateless autoconfiguration. As a general rule, it may not be wise to use stateless autoconfiguration on servers, since a change in network interface card will lead to a new EUI-64 based address being used (and a DNS update being required). However, in the IPv6 Internet, many more hosts will be servers (with the restrictive shackles of IPv4 NAT being removed).

A consideration for address selection in manually configured networks is network port scanning. In IPv4, port scans are a real threat to reveal potentially vulnerable ports or services. In IPv6, a typical subnet (link) will have  $2^{64}$  addresses (billions of billions) rather than  $2^8$  (256). Thus IPv6 provides some security through obscurity, simply by the address space being much more difficult to probe in a timely fashion, unless administrators are kind enough to run services on prefix : : 1, prefix : : 2, etc.

Note that IPv6 stateless autoconfiguration does not define how a host gets a unique name automatically, nor how a host can securely register its IPv6 address in an appropriate DNS server.

Autoconfiguration techniques also exist at the level of IPv6 routers. For example, there is a DHCPv6-based method for IPv6 prefix delegation to routers. This is an important tool for ISPs who are beginning to offer IPv6 services to customers. Also, RFC2894 defines the Router Renumbering protocol, which can be used to either add or deprecate IPv6 network prefixes on IPv6 routers. However, while the renumbering effort may be less than it is in IPv4, the problems of hard-coded IPv6 addresses in hosts, routers, firewalls and other devices remains a problem, unless developers of IPv6 devices and applications seek to rectify this problem by design, where possible.

The wider issues of zero-configuration ad-hoc networks are being considered in the IETF in Working Groups such as Zero Configuration Networking and Mobile Ad-Hoc Networks.

### 3.1.2. Service Discovery in IPv6

There are many service discovery mechanisms cited in a variety of IPv6 standards. At present, the variety of methods for service discovery is quite broad, with network administrators potentially needing to support multiple mechanisms to enable service discovery in their networks.

These mechanisms include:

- *Well-known site-local unicast addresses.* These are currently a proposed method (a last resort method) to find DNS resolvers on a network. However, the likely deprecation of site-local IPv6 addresses means this mechanism may be short-lived;
- *Multicast link local addresses.* A range of services and device types can be addressed on link by a well-known multicast address, e.g. `ff02::1` is "all hosts";
- *Multicast site or organisation scope addresses.* While unicast site local addressing may be deprecated, multicast site and organisational addressing may prove to be valuable service discovery tools;
- *Service Location Protocol (SLP).* SLP (RFC2165) and its extensions employ user, service and directory agents to allow multicast or unicast service discovery in a network;

# Moving to IPv6 in Europe

- *Well-known name.* In the presence of DNS (or some name resolution method) then well-known names can be used to refer to specific services, potentially in combination with a dedicated local scope domain name, e.g. local;
- *DHCPv6.* There are many proposed extensions to DHCPv6 to enable discovery of DNS, time, NIS and other network-related settings and services;
- *IPv6 Anycast.* IPv6 includes anycast addressing as a method for a device to address a set of devices and get a response from the “nearest” host in that set of devices. Anycast can be used to provide “farms” of servers for resilience purposes; nevertheless, the actual specifications indicate that anycast is only for routers, so this work needs to be further researched in future work;
- *Router Advertisement piggyback.* Given a host may use an RA as a method to configure its global IPv6 address and default router, the RA could also carry extensions for other network settings. DNS discovery has been proposed via this method, for example;
- *Link-local multicast name resolution (LLMNR).* LLMNR (formerly mDNS or multicast DNS) is a method to allow networks without DNS servers to offer a name resolution service.

There is some discussion in the IETF as to which set of services is the “basic set” that should be discoverable without stateful configuration. In particular, DNS resolver discovery is currently under discussion. It seems likely that DHCPv6 will be the recommended method, but this is currently under discussion in the DNS Operations Working Group.

## 3.1.3. IPv6 Plug and Play Networking in EU IPv6 Projects

Interestingly there does not appear to be significant research underway in plug and play networking in European IST projects. There are many interesting areas open for research, including secure autoconfiguration, secure DNS updates, zeroconf networking and user-friendly plug and play mechanisms.

The 6NET project has carried out a review (Deliverable D3.2.3.) of DHCPv6 implementations, which can be found in the Publications section of the 6NET web site<sup>9</sup>.

We suspect that many projects use stateless autoconfiguration for IPv6 devices, in particular client-oriented hosts. Stateless autoconfiguration may be used in Mobile IPv6 test-beds, where devices can autoconfigure on a foreign network without the requirement for an explicit foreign agent. The 6WINIT project (<http://www.6winit.org>) demonstrated Mobile IPv6 in clinical application environments.

## 3.1.4. Conclusions

It will become increasingly important for network devices to be able to be deployed as simply as possible, with minimal requirements of the users of the devices. This will be most evident in home networking scenarios, but also where new classes of sensor and embedded devices are deployed. However, we may also anticipate security requirements for such devices (e.g. secure access to a device in the home from a remote mobile PDA) in which case security mechanisms also need to be simple to configure and deploy. Research in this area would seem appropriate in the IPv6 context.

## 3.2. Multicast

This section gives a short overview of the application scenarios for IP multicast in general and discusses the technical background to realising IPv6 multicast in today's networks. A short overview of available multicast-capable implementations is also presented.

Furthermore, some multicast-related investigations of several 5<sup>th</sup> Framework IST projects are presented in order to underline the actual approach of using and deploying IPv6 multicast services.

This multicast chapter concludes with a short discussion about open issues of IPv6 multicast, which have to be solved with respect to a European wide deployment of IPv6 multicast services in the context of e-Europe 2005.

<sup>9</sup> 6NET web site, <http://www.6net.org/>

## 3.2.1. Why IP Multicast? - Some Applications Scenarios

In recent decades, the Internet developed from a simple transport network for unstructured, bulk information data (e-mail, news, World Wide Web) to a network that is used today for the distribution of multimedia content (audio and video). Big content providers recognised the possibilities of Internet technologies for building up a distribution channel of TV sessions, live events and concerts to billions of customers around the world.

In addition, many large enterprises implement streaming media services and business TV in order to broadcast news from their executives to all their employees in a timely manner and without a waste of resources within their enterprise intranets. Car vendors as well as railway agencies and airlines are investigating IP multicast technology together with wireless network access in order to use these technologies for entertaining passengers during long journeys.

Today, universities are offering tele-teaching seminars to their students in order to give them the opportunity to join their lectures every time —from every location— everywhere. IP multicast can also be used for other application areas, e.g. software updates to remote sensor devices, for distribution of data in multiplayer online games, or for service discovery. By enabling a multicast infrastructure, further innovation in these areas is made possible.

All the scenarios mentioned above, have one common approach —they rely on IP multicast, a network layer mechanism, which allows the sender to distribute identical content to a large group of receivers in a very efficient manner. With IP multicast, the sender injects the whole content only once into the network and the network itself handles duplication and transport to the receivers, which have explicitly joined a so-called “multicast group” in order to receive this special content. This approach is very efficient in terms of server load, network usage and bandwidth requirements.

## 3.2.2. Role of Multicast in IPv6

With the standardisation of IPv6, multicast technology became a much more important mechanism than it was for IPv4. In IPv6, many protocol internal functionalities are realised on the basis of IP multicast, which is used as a substitution for the well-known IPv4 broadcast mechanisms.

Some of these new IPv6 multicast-based mechanisms within the general IPv6 specification are, for instance:

- Stateless auto-configuration;
- Home Agent discovery in Mobile IPv6;
- Transition scenarios (for instance 6over4, although this method appears little used);
- Service-, Router- and Neighbour Discovery, and;
- Router Renumbering procedure.

Besides these, IPv6 multicast is also used in the application scenarios mentioned above, just like IPv4. Hence it could be stated that IPv6 multicast is one of the most important basic IPv6 mechanisms of which implementation and deployment is very necessary to realise an IPv6-based Internet and to allow future applications to work and behave in the same way as they are working for IPv4 today.

## 3.2.3. Short Introduction to IP Multicast

IP multicast was developed for IPv4 in the early years of the Internet (RFC966-1985) and multicast technology gained a more and more important role in the Internet over time. Nevertheless, the basic mechanisms have not changed very much and are pretty similar for IPv4 and IPv6. However, IPv6 does offer advantages, e.g. in the way scoping is handled.

### Basic (simplified) Multicast Architecture

IPv6 multicast is based on the concept of a group, like IPv4 multicast. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries: the hosts can be located anywhere on the Internet. Hosts that are interested in receiving

# Moving to IPv6 in Europe

data flowing to a particular IPv6 multicast group must join the group using MLD (Multicast Listener Discovery). Hosts must be a member of the group to receive the data stream. The Multicast Listener Discovery (MLD) protocol manages the membership of hosts and routers in multicast groups. IPv6 multicast routers use MLD to learn, for each of their attached physical networks, which groups have interested listeners. Each router maintains a list of host multicast addresses that have listeners for each subnet, as well as a timer for each address. However, the router does not need to know the address of the listeners —just the address of the hosts. The router provides addresses to the multicast routing protocol it uses; this ensures that multicast packets are delivered to all subnets where there are interested listeners. This way, MLD is used as transport for Protocol Independent Multicast (PIM).

In multicast routing, the source is sending traffic to an arbitrary group of hosts represented by a multicast group address.

8 Bit		4 Bit	4 Bit	112 Bit	
1111	1111	Flags	Scope	Group Identifier	

Figure 2: IPv6 Multicast Address Format

IPv6 multicast addresses are reserved and assigned from the Format Prefix  $0xFF::/16$  and contain a “Scope” field in order to restrict the range where the IPv6 multicast packet will be distributed and a “Flags” field, which signals if this IPv6 multicast address was allocated by IANA. More information about IPv6 multicast addresses can be found in RFC3306 and 3307.

The Group Identifier within the IPv6 multicast address can be used to identify and address theoretically up to  $2^{112}$  different IPv6 multicast groups, which is an enormous amount of available address space in comparison to IPv4.

In order to forward the IPv6 multicast traffic, a multicast router must determine which direction is upstream (toward the source) and which direction (or directions) is downstream. If there are multiple downstream paths, the router replicates the packet and forwards the traffic down the appropriate downstream paths —which are not necessarily all paths. This concept of forwarding multicast traffic away from the source, rather than to the receiver, is called reverse path forwarding.

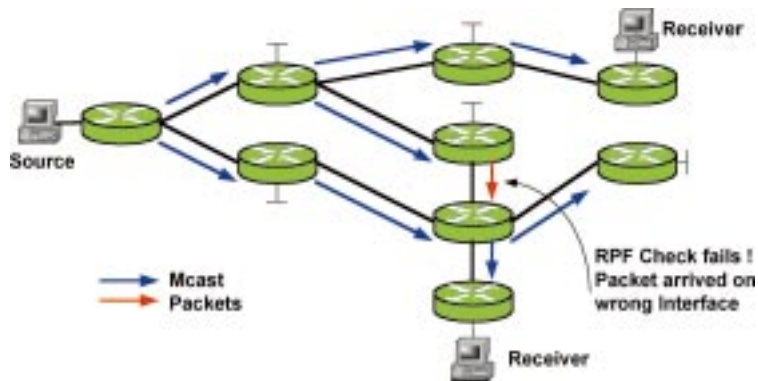


Figure 3: Reverse Path Forwarding

PIM gets its name from the fact that it is IP routing protocol-independent. PIM can leverage whichever unicast routing protocols are used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static routes. PIM uses this unicast routing information to perform the multicast forwarding function, so it is IP protocol-independent. Although PIM is called a multicast routing protocol, it actually uses the unicast rou-

ting table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols do. There are three different orientations of the flooding process.

**PIM Dense Mode (PIM-DM)** uses a push model to flood multicast traffic to every corner of the network. This is a brute-force method for delivering data to the receivers, but in certain applications, this might be an efficient mechanism if there are active receivers on every subnet in the network.

PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbours prune back the unwanted traffic. This process repeats every 3 minutes.

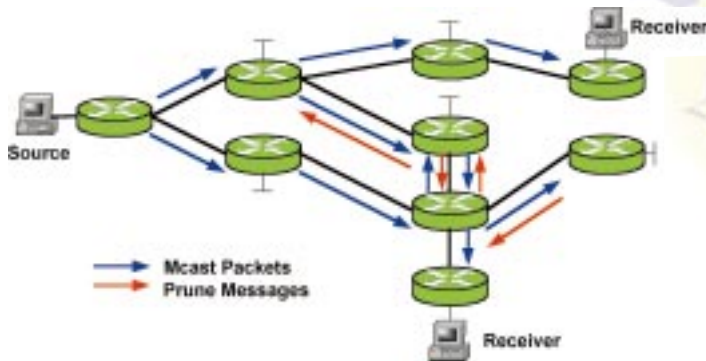


Figure 4: PIM Dense Mode

**PIM Sparse Mode (PIM-SM)** uses a pull model to deliver multicast traffic. Only networks that have active receivers that have explicitly requested the data will be forwarded the traffic.

PIM-SM uses a shared tree to distribute the information about active sources. Depending on the configuration options, the traffic can remain on the shared tree or switch over to an optimized source distribution tree. The traffic starts to flow down the shared tree and then routers along the path determine whether there is a better path to the source. If a better, more direct path exists, the designated router (the router closest to the receiver) will send a join message toward the source and then re-route the traffic along this path.

PIM-SM has the concept of a Rendezvous Point (RP), since it uses shared trees—at least initially. The RP must be administratively configured in the network. Sources register with the RP, and then data is forwarded down the shared tree to the receivers. If the shared tree is not an optimal path between the source and the receiver, the routers dynamically create a source tree and stop traffic from flowing down the shared tree.

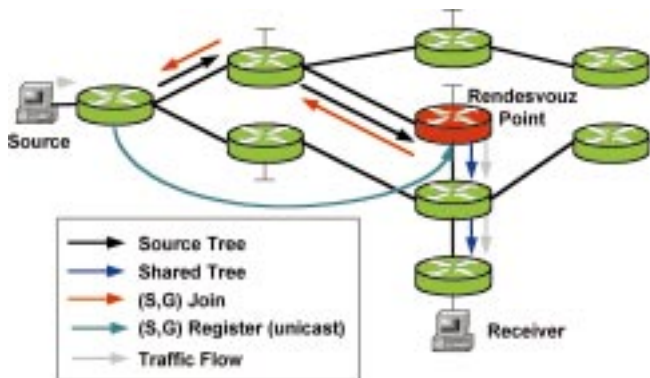


Figure 5: PIM Sparse Mode

# Moving to IPv6 in Europe

In PIM-SSM (Source Specific Multicast), delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the (S, G) channel. No signalling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels that they are subscribed to, so a RP is not necessary.

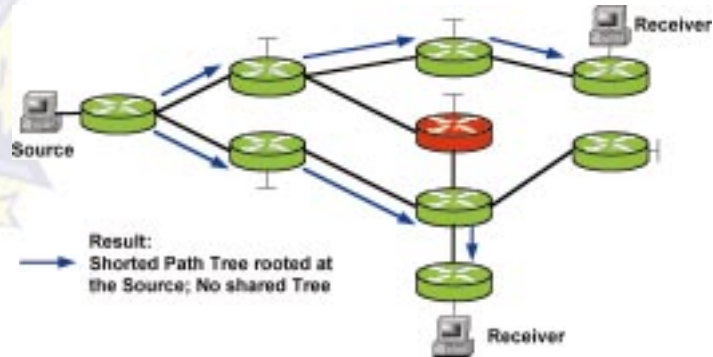


Figure 6: PIM Source Specific Multicast

Hence, from a more abstract perspective the general IP multicast architecture can be decomposed into the following three fundamental building blocks:

- *Group Management.* The Group Management mechanisms allow the receivers, which want to receive the multicast transmission, to become part of a dedicated IP multicast receiver group. In IPv4 the IGMP protocol (Version 1 to 3) is used in order to signal that the receiver wants to join/leave a dedicated multicast group, whereas IGMPv3 gives it the possibility to join the multicast sender as well. For IPv6, the Multicast Listener Discovery protocol is used where the functionality of MLDv2 is equivalent to IGMPv3.
- *Multicast Routing.* In order to realise the data transport between multicast sender and all its receivers, a multicast routing protocol has to be used, in order to establish a so-called "Multicast Distribution Tree". In today's IPv4 networks mostly PIM-DM (Protocol Independent Multicast-Dense Mode), PIM-SM (Sparse Mode) and PIM-SSM (Source-specific Multicast) are implemented. PIM-SM is most widely deployed. For IPv6, the main focus of the standardisation work is PIM-SM and PIM-SSM, where many router vendors and ISPs prefer PIM-SSM because of its much simpler approach with respect to inter-domain multicast distribution.
- *Data Transport.* The Multicast Data Transport deals with delivering the multicast content from the multicast sender to all the receivers, allowing the multicast packets to travel along the Multicast Distribution Tree, which was established using the Multicast Routing Protocols.

## Short Overview of Available IPv6 Multicast Implementations

Here we give a short overview of currently available IPv6 multicast implementations. This is not intended to be a complete list of all implementations, but includes implementations used within various European research activities.

- *Software/Operating systems.* Most of the research projects are dealing with open source IPv6 multicast solutions, especially the implementations for BSD and Linux. Microsoft also offers some IPv6 multicast functionality within their operating systems.
  - KAME Project (BSD): The KAME project was started to realise IPv6 on BSD platforms. With respect to IPv6 multicast, implementations of PIM-DM and PIM-SM are available. Therefore investigations and tests will be possible using the multicast routing functionality of a BSD platform based router.

Furthermore, KAME has already implemented the multicast tools VIC, RAT, and ICECAST that were ported from the well-known IPv4 multicast streaming tools and plans to implement PIM-SSMv6, MLDv2 based on IGMPv3 for PIM-SSM and the routing socket API in the near future.

- USAGI Project (Linux): The USAGI (UniverSAI playGround for IPv6) Project is an IPv6 development project, mainly for Linux systems. The USAGI implementer group is on the way to implement the IPv6 multicast routing protocol PIM-SM for Linux.
- MRT: The MRT (Multi-Threaded Routing Toolkit) is a partnership between the University of Michigan and Merit Network. The target of the group is the research of new routing software architecture. MRT realised routing software with support for IPv4/IPv6 BGP4+, DVMRP, RIP/RIPng, PIM-DM, and OSPF. Therefore IPv6 multicast routing is available with DVMRP and PIM-DM. The software is running under BSD, Linux, SunOS/Solaris and Windows NT/2000.
- *Hardware*. Nearly all major and a lot of the minor router vendors (6WIND, Cisco, Hitachi, Juniper, NEC, etc.) deliver their products with IPv6 multicast code included. Mostly the router vendors implemented the “mainstream” IPv6 features, like
  - PIM-SM for IPv6;
  - PIM-SSM for IPv6, and;
  - MLDv2.
- *Some Applications supporting IPv6 Multicast*. A short and non-exhaustive overview of IPv6 multicast-enabled applications is given below.
  - ICECAST: The icecast open source audio streaming tool is IPv6 enabled, including multicast support. It can be downloaded from <http://www.icecast.org/>. It is used for example for streaming of live radio stations.
  - ISABEL: Besides these relatively simple applications, some more complex applications can be used as for instance the ISABEL video conferencing tool, which was developed and ported to IPv6 by the Universidad Politécnica de Madrid (<http://isabel.dit.upm.es>).
  - MGEN: MGEN is a toolset, which was initially designed to perform measurements over IPv4 networks, gathering results about packet loss rate, delay, jitter, etc. Besides that, MGEN provides support for RSVPD and subscription to multicast groups. MGEN was developed by the Naval Research Laboratory (<http://manimac.itd.nrl.navy.mil/MGEN>) and has been ported to IPv6 by Universidad Carlos III de Madrid in the scope of the LONG project (<http://www.ist-long.com>).
  - RAT-Robust Audio Tool: The RAT Tool is one of the tools that were initially developed for use and testing within the Mbone (an IPv4 multicast overlay network). RAT is able to transmit audio on an IPv6 multicast basis and can be downloaded from the UCL Mbone conferencing tool Web pages<sup>10</sup>.
  - VIC-Videoconferencing Tool: Another multicast capable and easy to use tool out of the set of Mbone tools is the VIC video conferencing application, which was also ported to support IPv6. Both basic test applications (RAT and VIC) can be downloaded from the UCL web pages and are available in different releases for many operating systems (BSD, Linux, Microsoft, Solaris, etc.). The packages can be downloaded in source code as well as in binary format.

## Open Issues

Many problems occurred with the implementation and deployment of IPv4 multicast especially within the areas of multicast address delegation, inter-domain IPv4 multicast support and security issues for multicast communication. Lots of these problems are already solved (for instance with new protocols —MADCAP, MSDP, etc.) and some remain open.

<sup>10</sup> UCL Mbone conferencing tools, <http://www.mice.cs.ucl.ac.uk/multimedia/software/>



# Moving to IPv6 in Europe

However, these problems are not related only to IPv4 multicast, so that IPv6 multicast has to struggle with more or less the same questions. But in contrast to IPv4, IPv6 has the chance to solve these problems during the standardisation phase, keeping in mind the lessons the Internet community learned with IPv4. Thus, the European research projects can generate very important input and can support the standardisation bodies as well as the vendors and network operators with their knowledge and their investigations in order to smooth the way for a successful IPv6 multicast roll-out in Europe.

## 3.2.4. IPv6 Multicast Investigations in European Research Activities

The following section illustrates the research activities within the 5<sup>th</sup> Framework Programme of the European Commission. It describes projects dealing with IPv6 multicast and research areas needed to gather knowledge and to provide guidelines on how IPv6 multicast can be implemented and deployed.

### 6NET

- *Project.* 6NET is a three-year European project to demonstrate that continued growth of the Internet can be met using new IPv6 technology. It also aims to help European research and industry play a leading role in defining and developing the next generation of networking technologies.

6NET involves thirty-five partners from the commercial, research, and academic sectors and represents a total investment of EUR 26.5 million; 65% of which will come from the project partners themselves, and 35% from the Information Society Technologies Programme of the European Commission.

- *Multicast Activity.* Within the 6NET project, several IPv6 multicast-related issues are being investigated including IPv6 multicast reflectors, transition aids and gateways.

In the IPv4 multicast world, reflectors have been around for a long time. The idea is generally to receive multicast and send it out again as multiple unicast streams (or vice versa), so that people without multicast connectivity can receive the data and can participate within the multicast communication.

Besides that, IPv4 and IPv6 will co-exist for many years, possibly decades. There are several solutions for how IPv4 and IPv6 hosts and networks can inter-operate. This is usually easy if a host is dual stack. If, however, an IPv6-only host needs to communicate with an IPv4-only host, then somewhere along the data path there must be some form of translation.

There are several ways of doing this for unicast, while for multicast the only mechanism known to the author is an IPv6/IPv4 multicast Translator based on IGMP/MLD Proxying (MTP).

A multicast gateway solution is being tested in 6NET. This gateway can provide multicast connectivity between IPv6-only and IPv4-only networks. It gives an IPv6 host full access to send to and receive from any IPv4 multicast group by using the usual IPv6 multicast protocols and applications which will then operate on the respective IPv6 groups.

The gateway uses a one-to-one mapping of IPv4 addresses onto a subset of the IPv6 multicast addresses. An IPv6 host is then able to receive data from any IPv4 multicast group by joining the corresponding IPv6 group. An IPv6 host can also send, without necessarily joining, to any IPv4 multicast group by sending to the corresponding IPv6 group. A detailed description of the gateway solution was provided to the IETF as Internet Draft *draft-venaas-mboned-v4v6mcastgw-00.txt* in February 2003.

### 6WINIT

- *Project.* The IPv6 Wireless Internet Initiative project (6WINIT-<http://www.6winit.org>) was launched in 2001 and finished its work very successfully in January 2003. 6WINIT validated the introduction of the new mobile wireless Internet in Europe and set up a demonstrator of IPv6 running over 3G mobile networks. It included wireless services over 802.11b Wireless LAN, which were then later migrated to and tested on a 3G test-bed. It included a focus on problems raised from the mobile dimension. It built on the existence of an experimental fixed IPv6 environment from other initiatives, and linked into such existing infrastructures. The project provided a number of test-beds, including applications for the healthcare environments.
- *Multicast Activity.* The 6WINIT project researched multicast scenarios in Mobile IPv6 networks. Such scenarios include multimedia conferencing and media distribution. For mobile devices the provision of multicast varies depending on the transport layer and whether protocols such as Mobile IP are employed. Wireless LAN

Hot-Spots can benefit greatly from the use of multicast, since people are sharing the available bandwidth of the access-point. Conversely, if the multicast application is high bandwidth, the shared Wireless LAN medium may cause degradation in service for all hosts associated to the receiving access point.

For implementation purposes only local multicast scenarios were deployed and studied by the individual partners which themselves were partly connected to global IPv6 multicast networks such as the M6bone.

### Android

- *Project.* Future networks must support a wide and rapidly evolving range of service types. Besides that, future networks may need to be programmable to provide the required flexibility. The Android project proved the feasibility of constructing a managed, scalable, programmable network infrastructure that uses application layer active networking to provide dynamic customisation of services. It developed innovative solutions to support security, mobility and multicast. An improved active network architecture was implemented. Flexible and scalable management solutions based on policy driven autonomous agents were investigated and wide-area tests of an integrated prototype proved that the project results offer a coherent deployment option.
- *Multicast Activity.* The term secure multicast is a general one that can be addressed in several ways. With respect to the Android project, the term “secure multicast” is constrained to terms of confidentiality of multicast flows. Issues such as denial-of-service or non-repudiation were outside the scope of the project and are topics for future research in policy based management of active services.

The Android project has developed two forms of secure multicast. The first was realized at the network layer and is in the form of multicast reflection through Virtual Private Networks (VPN). Historically, multicast reflection has been accomplished by one node converting multicast data packets into unicast packets and forwarding them to another node —typically in a client/server format. If confidentiality was required, the user could attempt to establish an IPsec tunnel between the two end-points. Two constraining characteristics of this approach is the man-in-the-middle establishment of confidentiality, as well as the one-to-one relationship in reflection.

In the Android project, a more aggregated approach was taken and developed as an active service in the form of a proxylet (Java-based software) that reflects local multicast within a network to other network(s). This inter-network path is part of a meshed VPN that connects other sites participating in the same multicast session. The implementations that have been developed support both IPv4 and IPv6 reflection and are underlying VPN support.

Another key aspect in the Android project was the development of VPNs on a data-driven and on-demand manner.

### Euro6IX

- *Project.* The goal of the Euro6IX project is to support the rapid introduction of IPv6 in Europe. The project researches, designs, and operates a native pan-European IPv6 network, which interconnects seven IPv6 Internet Exchange points. This network is called the Euro6IX test-bed and within this network the Euro6IX project includes the most advanced services obtainable from present technology following the architecture of the current Internet (based on IPv4). For this reason also IPv6 multicast services are investigated from an IPv6 Internet Exchange point of view.
- *Multicast Activity.* The Euro6IX project investigates the technical realisation of IPv6 Internet Exchange points and looks for new possibilities for offering new services to Internet Exchange customers. To this end, the project made some initial tests and evaluations of how IPv6 multicast could be offered to potential IPv6 IX customers within one IX, as well as between different customers of different IPv6 Internet exchanges. For this reason, in a first step some of the actual available IPv6 router implementations were investigated within different IPv6 multicast network scenarios (ranging from a simple link-local IPv6 multicast distribution to IPv6 multicast streaming using a centralized Rendezvous Point within the service area of an IPv6 IX.) It proved that it is possible to establish a single IX-wide RP for PIM-SMv6 which can be used as a “condensation point” for future IPv6 multicast services.

Future investigations are targeted on realising IPv6 multicast traffic between different IX points and between different European networks. These investigations will be synchronized with equivalent activities of



The M6bone also gathered major experience in operation and maintenance of an international IPv6 multicast network.

In 2003, the M6bone project, 6NET, and Euro6IX will coordinate and synchronize their IPv6 multicast network activities in order to maximise the impact of their results and to minimise possible overlap in their research activities.

## OverDRIVE

- *Project.* The European research project OverDRIVE (Spectrum Efficient Uni- and Multicast Over Dynamic Radio Networks in Vehicular Environments) aimed at UMTS enhancements and coordination of existing radio networks into a hybrid network to ensure spectrum efficient provision of mobile multimedia services. An IPv6-based architecture enables interworking of cellular and broadcast networks in a common frequency range with dynamic spectrum allocation (DSA). The project built on the findings of the successful DRIVE project.
- *Multicast Activity.* Within the "Mobile Multicast" section of deliverable D03, OverDRIVE described several scenarios (including WLAN, UMTS) and derived requirements relevant to the continuous distribution of multicast sessions. These requirements include for instance:
  - Support for node and network mobility while maintaining multicast sessions;
  - Separated multicast and unicast sessions and separate handover;
  - Per-flow handover for IP multicast;
  - Seamless multicast handover between different access systems, and;
  - Scalability and fault tolerance.

The realisation of these requirements within the networks of the ISPs and network operators is one of the challenges the future IPv6 Internet has to deal with.

## 3.2.5. Conclusions

This IPv6 multicast chapter has underlined state-of-the-art of the IPv6 multicast deployment and research which was done within the framework of the European research initiatives or is still ongoing research in EU projects.

As in IPv4, the deployment of IPv6 multicast plays an important role for future Internet applications and is one of the key requirements for a global and seamless IPv6 Internet, which offers lots of new opportunities to all Internet users and companies.

Nevertheless, there are still lots of open issues with IPv6 multicast. Some of them are given here:

- Standardisation of (inter-domain) IPv6 multicast architecture;
- Secure multicast with IPv6;
- Interoperation of IPv4 and IPv6 multicast during the transition phase of the Internet;
- Lack of deployment know-how with respect to IPv6 multicast;
- New business perspectives with IPv6 multicast for end-users, ISPs and network operators;
- Role of IPv6 multicast within future wireless/mobile networks, and;
- Denial of service within secure IPv6 multicast networks.

Hence, one of the main objectives of all IPv6-related multicast projects within the 6<sup>th</sup> framework of the European Commission is directed to solve these open issues and to lead the way for an IPv6-based Internet, which plays an important role within the eEurope initiative of the EC.

## 3.3. Mobility

This section describes the current framework of IPv6 protocols for mobility in the Internet. The section takes a double approach: at first, a longer-term retrospective of IPv6 Mobility research and results is presented, covering a period starting with the mobility requirements in the earliest Internet up to now; this is continued

# Moving to IPv6 in Europe

subsequently by a shorter term retrospective analysis of IPv6 Mobility research, as performed within a representative sample of ongoing or recently concluded IST 5<sup>th</sup> Framework projects: OverDRIVE, MobyDick and MIND.

In the first section, the important aspects of mobility as reflected by Mobile IPv6, micro-mobility and ad-hoc routing are presented; a few references to other forms of mobility are made, but no detailed analysis is given.

In the second section, the three EU projects are introduced by their initial goals and a selection of their important results with respect to IPv6 Mobility.

The references section contains pointers to the three IST projects closely related to the IPv6 Mobility area.

## 3.3.1. State-of-the-Art

Even if the earliest Internet protocol requirements were addressing mobility (among other more stringent requirements), host mobility protocols have constituted a rich research area only during the last decade, sparked mainly by the ubiquitous deployment of the Internet and of portable computers, personal digital assistants, wireless cellular phones, and other portable devices.

Existing proposals that accommodate moving hosts with a TCP/IP stack provide solutions at various layers of the stack and make different assumptions on the availability of certain types of services in the Internet. For example, solutions exist to offer mobility with DHCP-style allocated addresses, mobility with directory services such as DNS or SIP, mobility with the assistance of routing protocols, and mobility with overlaying tunnels and/or source routing.

### Mobile IP

The Mobile IP class of protocols is positioned within this latter category and, when compared with most other protocols, it exposes the following salient characteristics:

- *Strong delimitation within the TCP/IP stack.* Mobile IP introduces modifications to a TCP/IP stack but only at the network conceptual layer (layer 3). As a matter of fact it uses existing mechanisms of IP protocols (e.g. tunnels, Neighbour Discovery, source routing) while keeping actual additions to the lowest possible level (the various types of caches can be blended with existing IP structures). As a consequence of this, transport layer protocols are not modified and, even more important, applications are not modified when a computer uses Mobile IP instead of vanilla IP;
- *Easy deployment.* In order to deploy Mobile IP, it is required to install new protocol entities: Home Agents within the domains that accept moving hosts and in the domains that can offer IP mobility services. Both these types of domains are leaf networks with respect to the larger Internet. Mobile IP does not require any modifications to existing routing infrastructure nor to the name-to-address services (DNS);
- *Continuous connection.* Mobile IP provides for transparency to applications by keeping socket connections up even when the assigned address changes as a result of physical mobility.

In the simplest Mobile IP mechanism, a host is assigned a Home Address that is supposed to be more permanent than any other addresses which that host might be assigned while changing IP attachment points. The temporary addresses are referred to as Care-of Addresses and represent each distinctive current location of the mobile node. Traffic from and towards the mobile node is re-directed from the home domain towards the visited domain by the Home Agents. The Home Agents maintain Binding Caches that list the current associations of Home Addresses to Care-of Addresses of the Mobile Nodes.

Various related schemes exist in the Mobile IP class of protocols. With Route Optimisation, the Correspondent Nodes (typically a web server browsed by a client MN) also maintain Binding Caches such that traffic between MNs and CNs will not necessarily flow through the home domain (or the HA) but take the direct route between MN and CN. Hierarchical Mobile IP and Regional Registrations address the potentially long delays induced by updating Home Agents at each change between visited domains and introduce new protocol entities closer to the points of attachment: local mobility agents.

## Micro-mobility, or Local Mobility

From this main requirement of avoiding the long delays involved in updating remote home agents, several other requirements have been proposed, such as:

- Low powered devices that must be in dormant mode most of their working time and that should be awakened only when actual communication is needed, led to the paging requirement and solutions;
- Identification, change and preference issues between several attachment points led to the candidate access router requirements;
- Handover enhancements and real-time application constraints led to various forms of performance enhancing handovers (Fast Handovers, Context Transfer, etc.).

These types of requirements are often grouped into a common mobility domain identified as the “micro-mobility domain”, as opposed to the “macro-mobility” that is mainly addressed by the simple generic Mobile IP protocol. There are obvious interrelations between micro-/macro-mobility and intra-/inter-domain mobility (here domain stands for a routing domain, like OSPF domain). The micro-mobility field is also sometimes referred to as “local mobility management” to illustrate the fact that mobility updates are confined to a small domain and not across the entire Internet (this is similar to the “local access” concept in memory access that gave birth to the “memory cache” and “memory hierarchy” concepts). In the following, we will use these two terms (micro-mobility and local mobility) interchangeably to stand for the same unique concept.

There is an important distinction to be made with respect to the techniques used for managing paths in a local domain. The key issue is whether the mobile host is assigned a new address each time it changes its attachment point, or whether the mobile host keeps the same unique address while being attached to any point in that domain. Even if the address changes, the mobility updates happen only within the micro-mobility domain. When the host is assigned a new address each time it moves, the mobility management schemes will only update binding caches in central entities (like MAP in HMIP, ANP in BCMP) and basic IP routing tables will not be affected. On the other hand, when the address does not change, the IP routes will automatically be updated (e.g. Path Updates in Cellular IP). With respect to this scenario, mobile host outgoing communication triggers the path updates and establishes new proper routes, but incoming communication towards the mobile might not find the right path if the mobile host was not emitting recently. This behaviour opens an additional necessity to the use of paging schemes, where the dormant mobile host is periodically “awakened” or “paged” by another central entity, thus paths get updated and thus incoming communication will find the right paths.

Again in relation to the path updates within the local mobility domain, the host-based routes might constitute a scalability risk. Consider a domain of  $x$  fixed routers, where  $y$  mobiles move around. Depending on the movement pattern, on  $x$  and  $y$ , assume  $z$  as the number of new routes added or deleted to the set of routing tables of fixed routers in that domain (let's say there are  $t$  routing tables). It is important to note that a local mobility management scheme will scale well (or simply will scale) when  $t$  and  $z$  are growing directly proportional with  $x$  and  $y$ . The fuzziness factor in this analysis is, of course, the mobility pattern, which should be properly formalized in order to attain a correct scalability analysis.

The handover enhancements are mainly targeting a faster and loss-less, or fewer packets lost, handover than that offered by Mobile IP. In the “fast” schemes, the starting point is a mobile host that has a CoA configured. Then, one tries to measure the time it takes to move under another attachment point, acquire a new CoA and re-establish routing towards that CoA. For example, the Fast Mobile IPv6 protocol aims at re-directing packets from an old AR towards the new AR (Access Router, or attachment point). Bi-casting techniques are sometimes used, where a CN will simultaneously send duplicated packets towards the two attachment points around which the mobile might be at a certain moment, thus ensuring the reception of at least one of the pairs of sent packets by the mobile host. In this scenario, Context Transfer techniques can be employed. An entire set of data pertinent to a mobile host communication is moved from the present AR towards the next. For example, if MH currently has a Security Association established with the current AR, then the physical movement of MH will trigger the correspondent “wire” move of the respective SA entry in the old AR's SA database towards the new AR's SA database. In this way, the mobile host is freed from the necessity to exchange new SA-establishment control messages with the new AR, thus saving in the use of wireless environment resources.

# Moving to IPv6 in Europe

## Mobile Networks

Mobile IPv6 defines host mobility support in the Internet. It enables a mobile node moving from one IPv6 subnet to another to preserve the ability to be reached at its permanent (or home) address and maintain continuity of its ongoing sessions. While Mobile IPv6 is well suited to handle host mobility, some extensions are required when it comes to support a mobile network, i.e. an IPv6 subnet that can change its point of attachment to the Internet. The NEMO working group in IETF, which started in October 2002, is chartered to specify a base network mobility protocol, as an extension of the Mobile IPv6 bi-directional tunnel, adapted to complex mobility scenarios including nested mobility and multi-homed mobile networks. At the same time the working group will study the possible approaches and issues with providing more optimal routing than can be had with (potentially nested) tunnelling. However, the WG is not chartered to actually standardize a solution to such route optimisation for mobile networks at this point in time.

The formation of a mobile network can exist at various levels of complexity. In the simplest case, a mobile network contains just a mobile router and a host. In the most complicated case, a mobile network is itself a multi-level aggregation of mobile networks with collectively thousands of mobile routers and hosts. The idea of the mobile router is taken for granted to refer to the router in a mobile network that attaches the mobile network dynamically to various parts of an IP infrastructure. Each mobile node and router can have one or more IP interfaces.

Here are the scenarios of various instances of mobile networks:

- A cell phone with one cellular interface and one Bluetooth interface together with a Bluetooth-enabled PDA constitute a very simple instance of a mobile network. The cell phone is the mobile router while the PDA is used for web browsing or runs a personal web server;
- Train passengers use their laptops with Wireless LAN cards to connect to Wireless LAN Access Points deployed in the train. The mobile router is used to link together the Access Points and to provide connectivity to the Internet. A similar scenario can occur as well on a plane, on a ship, and any moving vehicles;
- A car network links its electronic devices (such as brake or injection electronics but also the onboard computer offering maps on LCD's or the audio player) to the mobile router that is connected to the Internet via a cellular network;
- Multi-level aggregation of mobile networks can be desirable. For example, a person carrying a personal area network of a cell phone and a PDA getting into a car, might wish to offer Internet access to the car's electronic devices, or it might want to use the car's own mobile router to connect his/her PDA to the Internet (instead of the cell phone).

More complex cases, but still real, arise when a larger number of larger sets of equipment interact. One specific case is a typical Fire Department deployment in action. A fire-fighter would carry a personal area network (with a mobile router and numerous IP-enabled devices). The fire-fighter's mobile router has a wireless connection to a vehicle whose mobile router is attached to a private public-safety backbone via a wireless link (maybe satellite link). Being part of the public-safety network, the fire-fighter can receive data such as building plans, and send data such as photographs, thermal images, life sign information, etc.

The basic approach for network mobility support is to leverage Mobile IPv6 technology introducing minimal extensions. Similarly to Mobile IPv6 for hosts, a Mobile Router (MR) will have a home agent, and use bi-directional MR-HA tunnelling between the MR and HA to preserve session continuity of the nodes within its mobile network while the mobile router (and its mobile network) moves. While the mechanism to maintain the MR-HA bi-directional tunnel is essentially the same as for mobile hosts, some enhancements of binding cache and routing table management on the MR and HA are needed. To recognize the nodes inside a mobile network, it is sufficient to know the prefix of the IP address owned by the MR. This information must then be configured in the HA. By reusing exactly Mobile IP unchanged, the mobile network prefix must be configured in the HA in a pre-arranged manner. However, one could also envisage the modification of binding update messages to convey also the mobile network prefix to the HA [5]. It is worth mentioning that the MR-HA bi-directional tunnelling mechanism is general enough to support nested mobile networks, in which a mobile network could move inside another mobile network. Besides, it also supports the situation in

which a Mobile IP mobile node moves within a mobile network, continuing its sessions with its corresponding nodes.

However, extensions to this approach, forming an advanced network mobility support, should be provided in order to address advanced issues for performance and scalability. Note that such extensions may require changes in other elements such as correspondent nodes, although such modification should be minimised. Advanced network mobility support should encompass at least these additional requirements:

- *Route optimisation for nested mobility.* The solution must allow packets between a correspondent node and a node within a mobile network to be routed along the optimal path irrespective of the number of nested mobile networks above that node. While basic network mobility support with the MR-HA tunnel supports nested mobility, it introduces very sub-optimal (multi-leg) routing in the topology and severe header overhead as the packets from CN are consecutively encapsulated by all the home agents of the mobile routers above the Mobile Network Node (MNN).
- *Optimisation for disconnected operation.* Ideally, the solution should allow visiting mobile nodes to be reachable by other nodes within this mobile network even in situations where the mobile router is disconnected from the fixed infrastructure.
- *Seamless mobility.* The solution should provide or support (optionally) seamless mobility that is, mobility of MRs or MNNs with ideally no loss of packets nor delay.

## Mobility based on Routing for Ad-Hoc Networks

In this class of protocols, it is considered that the mobility of hosts (or routers) is principally managed by protocols that are very similar to the classic routing protocols. Two important instances in this class are the AODV (Ad-hoc On Demand Distance Vector) protocol which was designed and implemented as an evolution of RIP (Router Information Protocol) which is itself a distance-vector routing protocol (routing protocols used in the Internet are generally classified as distance-vector and link-state) and OLSR (Optimized Link-state Routing) protocol which was designed as an evolution of OSPF which is itself classified as link-state.

The main kernel of routing protocols for ad-hoc networks has another relatively simple classification associated with it. These protocols group into “on-demand” and “flooding” types of protocols. The relation between these two types are as follows: the on-demand type of protocols generates route updates and propagates routing information between two communication ends only when these nodes exchange application data, thus satisfying an associated requirement to minimise the number of overhead control packets circulated on wireless links; the “flooding”, or “continuous” types of protocols will trigger new updates periodically, or at any time that an entity moves out or into the range of a neighbour, this having the advantage of always benefiting from a complete and correct routing information available within the network. The on-demand aspect was itself a result of a practical observation with the RIP protocol, where disconnection events (or “bad news”) are badly propagated due to, among other things, the periodic nature of RIP: every exchange is done at periodic time events, in no relation to the actual physical movement events.

When comparing routing-based protocols to the Mobile IP protocol for supporting mobility, it is important to notice that Mobile IP offers the important “home address” concept, where a mobile entity is reachable at a permanent home address, while it can physically attach to virtually any part of the Internet. This concept is not available with ad-hoc routing protocols, they can only cover small regions or mobility domains due to scalability reasons: the number of routing table entries added to the large number of routers in the Internet due to the movement of a large number of mobile entities can become too large.

The initial requirements behind ad-hoc routing protocols were driven by scenarios where random groups of small computers need to communicate to each other in an infrastructure-less manner, i.e. there is no fixed entity (Access Point or other) that might help in this communication. These types of very high-level requirements were tightly related to the auto-configuration aspects, where hosts need to be dynamically configured with various initial parameters, such as addresses, default routes or DNS locations.

From these initial requirements, the field of ad-hoc routing and networks has expanded to an extremely rich and continuously flourishing area of research and engineering that has a large number of inter-relations and direct connections to Mobile IP-based mobility and to local mobility management. Due to space constraints, we will only mention here some of these aspects.



# Moving to IPv6 in Europe

In location-based ad-hoc routing, it is considered that entities participating in the network are aware of their physical positioning. When this information is used in combination with detailed knowledge of L2 coverage ranges, it is possible to attain more accurate IP (or L3) routing information and effectively reduce the number of messages exchanged on wireless links.

Clustering for ad-hoc networks considers very large groups of nodes. It is considered that in such environments, a natural organization approach is that sub-groups (or “clusters”) of nodes exchange routing information more often and more detailed than information exchanges between clusters.

Multicast for ad-hoc networks is another very rich area of research, as indicated by a strong publication activity in the recent years. The very nature of wireless links has broadcast features built in, meaning that messages sent by one entity are potentially received by all interested parties within a certain vicinity. This can be seen as an important advantage or disadvantage. It is an advantage when it allows for many receivers to receive a route update, but it is a disadvantage when a route update is targeting only towards one or a small group of other entities (in that case many other non-interested parties will receive non-needed messages, or the bandwidth is used in a non-efficient manner). The exact notion of broadcast-capable or multicast-capable wireless links is not yet clearly defined and is subject to future research.

Other important aspects are: security in ad-hoc networks, guaranteed quality-of-service in ad-hoc networks and QoS routing in ad-hoc networks.

Ad-hoc networks are typically composed of small devices, ranging from laptop PCs in conference rooms to extremely small devices (on the scale of cubic millimetres) that compose “smart dust”. Energy consumption is a fundamental issue that needs to be dealt with, and as such routing in an ad-hoc network is heavily influenced by the availability, or non-availability thereof, of energy supply.

One last aspect of ad-hoc routing that deserves particular attention is the field of ad-hoc networks connected to the Internet with the help of MANET Gateways. This is particularly important when considering the mobile networks mentioned previously. MANET Gateways are fixed entities that connect an ad-hoc network to the Internet infrastructure at large. Research in this area has dealt with the means of configuring publicly routable addresses on the mobile nodes and with a clean separation between local (within ad-hoc network) routing and the global routing of the Internet.

## 3.3.2. EU Projects

### MIND (Mobile IP based Network Developments)

MIND is a 24-month project that ended in November 2002. In the following, we first give a brief description of the project’s initial generic goals and key IPv6 Mobility issues, followed by a partial presentation of some of the main results related to IPv6 Mobility.

The project takes as a starting point the concept of an IP core, accessed by a variety of technologies. It develops this vision with business models and user considerations (including scenarios—which look at the user side of ad-hoc networks). From this, the project derives the requirements on the network and air interface parts of the vision. In addition the project conducts a trial—practical research—into the use of HIPERLAN/2 and an IP-based access network, using IP QoS and IP mobility management techniques, as a complement to UMTS and as a part of this vision. The project is not concerned with the core IP network and focuses only on those aspects of the problem that specifically relate to mobility. Thus the concept of an access network is important—where different IP QoS protocols could run, for example, and where IP micro-mobility management is being introduced. The key objectives related to IPv6 Mobility are the following:

- Extend the concepts of IP mobile networks. This includes: new network topologies—ad hoc, self-organising and meshed networks; enhanced support for QoS, ad-hoc networks and self-organisation at all layers of HIPERLAN/2; QoS support in IP-based mobile networks; investigation of the spectrum requirements for systems beyond 3G;
- The project researches into the use of WLAN and an IP-based access network as complement to UMTS for high bandwidth provision in hot spot areas.

One deliverable of this project that is highly relevant to the IPv6 Mobility area is D2.2 Core Report “MIND Protocols and Mechanisms Specifications, Simulation and Validation”. BCMP (BRAIN Candidate Management Protocol) is a protocol described in high-level terms in this deliverable, and in detail in the D2.2 Annex. Overall, BCMP is a set of protocols constituted in a network that uses IPv6 concepts to manage address assignment, handover (normal handover, lossless handover and network-controlled handover), access control (the protocol MURP, or MIND User Registration Protocol), candidate access router discovery and paging. Most of these important features are considered as micro-mobility aspects, and in relation to the main thread linking the deliverable which is ad-hoc, self-organizing and mesh access networks.

### **Moby Dick (Mobility and Differentiated Services in a Future IP Network)**

This 36-month project ends in December 2003. In the following, we first give a brief description of the project's initial generic goals and key IPv6 Mobility issues, followed by a short presentation of some current results in IPv6 mobility as described in two of the current deliverables.

The project Moby Dick defines, implements, and evaluates an IPv6-based mobility-enabled end-to-end QoS architecture starting from the current IETF QoS models, Mobile IPv6, and AAA framework. A representative set of interactive and distributed multimedia applications serve to derive system requirements for the verification, validation, and demonstration of the Moby Dick architecture in a test-bed comprising UMTS, 802.11 Wireless LANs and Ethernet. In case the existing applications or the underlying architectures do not provide what is required, the necessary modification will be undertaken. Among the major key issues in the project, the following are worth mentioning in the IPv6 mobility context:

- Definition of a common architecture integrating QoS, IPv6 mobility, and AAA (out of the separate architectural approaches for each component currently provided by the IETF) with respect to wireless issues;
- Implementation and evaluation of an IPv6-based end-to-end technological approach to fulfil the requirements of present and future mobile communication services;
- Implementation and evaluation of QoS models (e.g. Differentiated Services) in highly dynamic and heterogeneous network topologies (understanding of QoS models is normally restricted to relatively static environments);
- Definition of a suitable charging concept, which would enable permanent Mobile IP based services on a large scale (a strong requirement related to AAA, but currently not a topic within the IETF).

The current deliverable D0301 entitled “Initial Design and Specification of a Moby Dick Mobility Architecture” Milestone 2, specifies components and protocols for IPv6-based mobility management. The baseline of mobility management is the Mobile IPv6 protocol in its 13<sup>th</sup> draft version. The project is using fast handover to improve latency and cut data loss (latency drawbacks and data loss are exposed with simulation results); the deliverable also extends the supported mobility functions to include paging. Though this work has indicated further improvements in the performance of mobility management via hierarchical mobility schemes, such as Hierarchical MIPv6 and Regional Registration, these have not been included in this deliverable. Fast handover, which takes place between Access Routers the mobile devices attach to, is also used in this project to transfer security information (keys) and QoS parameters to allow QoS and AAA functions to proceed in parallel, to not lose the benefit gained via fast handover by the need to wait for time-consuming AAA and QoS signalling to complete. Overall, the deliverable covers the mobility architecture, fast handover, care-of-address acquisition and paging. It further outlines software including software architecture, hardware and operating systems used for the various physical elements, such as mobile nodes, Access Routers, Home Agents, etc.

Another current deliverable D0302 entitled “Mobility Architecture Implementation Report” Milestone 3 contains a detailed specification and design of the mobility part of the overall system, and is intended to be a reference for the implementation work, which has started in parallel. It specifies all mobility related signalling flows, referring where necessary to the remaining flows. The deliverable shows the details of the software architecture of all relevant physical elements, i.e. the Mobile Terminal, the Access Router, the Radio Gateway, the Home Agent and the Paging Agent. The functions of each of the mobility-related software modules are described, and an indication on whether the module is implemented in user space or kernel space. Finally, the interfaces between the modules are specified. The architecture of the physical elements

# Moving to IPv6 in Europe

also includes some non-mobility modules that are referenced only, and not completely specified. The document contains an Appendix explaining why the ad hoc mode for wireless LAN is being considered (this is link layer ad-hoc “networking”, not actual IP-layer networking).

## OverDRiVE (Spectrum Efficient Uni- and Multicast Over Dynamic Radio Networks in Vehicular Environments)

This 24-month project ends in March 2004. In the following section, we first give a brief description of the project’s initial generic goals and key IPv6 Mobility issues, followed by a short presentation of some current results in IPv6 network mobility as described in one current deliverable.

Overall, the project aims at UMTS enhancements and coordination of existing radio networks into a hybrid network to ensure spectrum efficient provision of mobile multimedia services. An IPv6 based architecture enables interworking of cellular and broadcast networks in a common frequency range with dynamic spectrum allocation (DSA). The project’s main stated objective is to enable and demonstrate the delivery of spectrum efficient multi- and unicast services to vehicles. The key issues related to IPv6 Mobility in OverDRiVE are the following:

- Develop a vehicular router, providing multi-radio access to a moving intra-vehicular area network (IVAN);
- Develop and demonstrate efficient mobile multicast techniques (MMC).

Currently, the document deliverable D03 entitled “Scenarios Services and Requirements” contains two sections related to IPv6 Mobility. The section “Mobile Router and IVAN” considers the scenarios and requirements for a protocol that supports IPv6 mobility of entire networks, moving homogeneously towards any part of the IPv6 Internet at-large. In OverDRiVE, mobility management is a framework of functionalities dealing with IP mobility management within the architecture of the Internet. This framework is described in terms of concepts of IP mobility for hosts and the deliverable presents the necessity of enhancing this picture with network mobility elements. In high-level terms, the functionality of a mobile router of an IVAN is far beyond the normal forwarding of IP packets and even beyond what IP mobility provides for hosts. These characteristics of the IP mobility protocols expose important difficulties in adapting their functionality for mobile routers. In OverDRiVE it is considered that the mobile router will handle mobility management on behalf of the nodes that are part of the IVAN. In this way, new extensions are needed to Mobile IP. An extension of the Mobile IP protocol should consider from its inception all the implications induced by replacing the movement of a Home Address with the movement of a Home Prefix.

The section “Mobile Multicast” of D03 considers the scenarios and requirements relevant to the continuous distribution of multicast sessions towards independent mobile nodes as well as nodes that are parts of entire mobile networks.

## 3.4. Performance, Conformance and Interoperability Testing

### 3.4.1. Introduction

The move to IPv6 will enhance the convergence of mobile and wireless systems, Internet, telecommunication and broadband into an integrated networking infrastructure. The resulting communication and information systems are characterized by higher complexity, ubiquity of computing and communications, mobility, and increased service dynamism. This technologically heterogeneous environment employing diverse equipment and offering services in open multi-provider markets poses great challenges to guarantee general interworking and a high level of reliability for applications based on IPv6.

Components developed by different manufacturers should interoperate effectively when deployed. For this purpose, it is necessary to have both conformance and interoperability relevant test suites to test the IPv6 protocol stacks being developed by manufacturers. Conformance testing deals with verifying that an implementation of a protocol behaves as foreseen in its specification according to the standards on which it is based. Interoperability testing consists in verifying if several implementations put together will effectively behave as expected. It is also essential to provide places where these tests can be executed against implementations.

Besides pure functional correctness also performance issues need to be addressed. For a correct interworking of different components it is necessary to ensure that a certain level of service is maintained. Therefore the verification of performance forms an integral part of testing, but it extends also towards the deployment and operational phase. Network operators will need up-to-date performance data for a variety of tasks such as network health surveillance, SLA auditing, traffic engineering and trend analysis.

## 3.4.2. IPv6 Conformance and Interoperability

### Basic Principles of Conformance Testing

The objective of conformance testing is to establish whether the Implementation Under Test (IUT) conforms to the relevant specification(s). Practical limitations make it impossible to test exhaustively, and economic considerations may restrict testing still further. Conformance comprises static and dynamic requirements:

- Static conformance requirements pose limitations on the permissible selections of implemented features in order to conform to a respective base or profile specification. They define minimum required capabilities for interworking, they prescribe mandatory support for functional units or protocol classes, and required ranges of values for specific parameters or timers;
- Dynamic conformance requirements specify what observable behaviour is permitted by the relevant base or profile specification(s) in instances of communication using a particular protocol. They form the bulk of each protocol specification and may also be a major aspect of other base specifications. They define the set of allowable behaviours of an implementation or real system.

A conforming system is one that satisfies both static and dynamic conformance requirements. Nevertheless we have to note that while conformance is a necessary condition, it is not sufficient on its own to guarantee interworking. It does ensure, with a reasonable degree of confidence, that the implementation is consistent with its specification, and hence does increase the probability that implementations will interwork. Even if two implementations conform to the same protocol specification, they may fail to interwork fully. Trial interworking is therefore recommended.

### IPv6 Conformance Requirements

The IPv6 Internet Protocol provides numerous important enhancements over its predecessor IPv4. Its addressing scheme provides a 128-bit address space, hierarchical addressing and routing infrastructure, and built-in security features for authentication, encryption and data integrity. In order to assure the new protocol implementations to be conforming to the standard and in turn to assure the interoperability between different IPv6 implementations, IPv6 protocol conformance tests are required.

A large number of Standard Track RFCs are associated with the IPv6 protocol. They specify mandatory requirements that each conforming implementation must support. Comprehensive IPv6 Conformance and IPv6 Routing Conformance Test Suites will need to encompass standards defined in more than 30 RFC documents originating from nine working groups. IPv6 conformance test suites need to comprise tests that address the new IPv6 core protocol features. This includes functionality for neighbour discovery, stateless address configuration, path MTU discovery, and basic transition mechanisms. Special emphasis has to be given to the Header Format.

### Worldwide IPv6 Conformance Test Facilities

In the USA (see the University of New Hampshire/IOL project) and in Asia (see the TAHI/WIDE project), there already exist infrastructures that offer test services for American and Asian manufacturers, respectively. For a long time, European industries involved in IPv6 stack development were obliged to call upon IOL or TAHI structures to test their stacks. Thus, it became essential to create a European infrastructure allowing to identify the testing needs of manufacturers and to gather expertise in the field for the benefit of the European community. Consequently a lot of work has been over the past couple of years by main actors in IPv6 deployment and test laboratories to provide a suitable environment for conformance and interoperability testing to the European Community.

# Moving to IPv6 in Europe

Among the means needed to move to IPv6 in Europe, there is an important activity concerning the generation of conformance and interoperability test suites. G6Test is a recent sub-group of the G6 (Groupe Francophone des utilisateurs d'IPv6) dedicated to IPv6 Conformance and Interoperability Testing. In the context of the NGN-I (Next Generation Networks Initiative) project, G6Test contributed via the Armor team of IRISA at Rennes in France together with the RSM/ENST-Bretagne —in the following ways:

- Sensitising of the organizations to the need of developing test benchmarks in Europe;
- Analysing the needs of the main actors involved in the development of next generation IPv6 networks in Europe;
- Facilitating the creation of infrastructure for testing IPv6 protocol stacks developed by European partners.

## ETSI IPv6 Plugtests™ Events

The main result of this work is the growth of number of participants to the so-called IPv6 interoperability events (called previously bake-off) organized by the Plugtests service of ETSI (European Telecommunication Standardisation Institute).

Interoperability events refer to a session of about one week where engineers get together to test their implementations against each other. All are winners in the end as bugs in both the standards and the implementations are discovered. Such events are part of the process of improving standards and a means of enhancing the quality of conforming products.

In collaboration with the G6Test, ETSI at Sophia-Antipolis, France has been organizing an IPv6 interoperability event each year since 2000. One can observe that the number of participants is increasing.

In October 2000, ETSI held its first IPv6 interoperability event (then called bake-off) at Sophia-Antipolis. The second, a bit larger with new features and more expertise, was held in November 2001, at Cannes. Almost 40 people coming from 16 different companies and 6 different countries (mainly in Europe) participated. The last ETSI/IPv6 interoperability event was held in September 2002 and had a large participation and broad range of topics addressed (including interaction with the 3GPP community). This demonstrates the rapidly growing importance of this activity in Europe and the need for continued development.

Record numbers of engineers (55 participants) from 24 competing organisations from all over the world (44% from Europe, 28% from Asia and 28% from North America) gathered to test their IPv6 and IPv6-related protocol implementations at the third IPv6 interoperability testing event. More services were offered than ever before, including testing of the IPv6 core protocol, mobile IPv6, routing, transition and IP security.

Major results of the ETSI IPv6 Plugtests Event include:

- Most of the implementations already passed the tests on Basic Protocols during the previous interoperability events showing that IPv6 Core protocol (Neighbour Discovery, Stateless Address Auto-configuration, Redirect, PMTU discovery, etc.) is stable. Even though some minor bugs have been detected, implementations are now quite mature Re-testing will be required to evaluate non-regression of modifications;
- Concerning transition mechanisms (6to4, NAT-PT, ISATAP), interoperability tests have highlighted misinterpretations of the RFCs that were reported to the IETF and have been clarified since;
- As the number of companies that integrate IPsec in their development environment is still small, tests have showed the need to furnish more tests. We can expect that requests for security testing will become more and more important in each protocol that could have to negotiate to provide authenticated keying material for security associations in a protected manner;
- Test results showed that routing protocols (RIPng, OSPFv3, IS-IS, BGP4+) seem to have reached an acceptable level of stability;
- Concerning MIPv6, the difficulty came from the coexistence of several versions (v13 to v19) of the draft. Main tests have been done based on draft v19. A stable draft and even an RFC is required quickly.

## 3.4.3. IPv6 Performance Monitoring

### Requirements for Performance Monitoring in IPv6 Networks

Performance monitoring functions are a fundamental component in a variety of scenarios. Network performance must be monitored by operators for ensuring network health and correct operation. The measurement results may be used for traffic engineering, performing load balancing to optimize network resource usage. SLA validation depends on the availability of efficient monitoring facilities, and metered performance may be recorded for accounting purposes. Performance monitoring is essential in application areas where there is strong dependability on the network availability e.g. in emergency communication, and monitoring provides a means to alert for unexpected traffic patterns to help in detecting security threats such as unauthorized intrusion or DoS attacks.

### Performance Metrics

Performance of networked applications and communication services is based on parameters characterizing network behaviour such as delay, jitter and loss. In order to come to an accurate common understanding of the performance and reliability and to generate efficient and consistent measurements, it is important to refer to standardised metrics for performance evaluation. ITU-T and IETF are actively working on performance metrics for IP-based networks. Of particular relevance are the RFCs of the IETF IPPM (IP Performance Metrics) Working Group.

IPPM specified a general framework for performance metrics, and a set of standardised metrics, conforming to his framework including OWD (one way delay), IPDV (IP Packet Delay Variation), and OWL (one way loss). The framework is open for further emerging metrics such as packet re-ordering, which is currently under preparation. Derived from the single value measurement are further statistical values for means, quantiles, distributions, etc. that characterize the overall performance. Indications on measurement accuracy help to improve comparability of different measurement results.

Depending on the usage context, performance needs to be measured at various granularities. Measurements may be performed to a single application flow in order to evaluate the performance of a specific application, or to a certain traffic class, up to the full traffic aggregate that is traversing a network between a specific ingress and egress point. In order to contain the amount of measurement data, it is in practice necessary to resort to sampling methods, which drastically reduce the costs and additional network traffic caused by measurement processes.

A further step in performance measurement is measuring on the basis of connections. Connection and Session Based Metrics of interest include Connection Setup/Tear-down Rate, Session Capacity, Session Rate, Call Capacity, Peak Call Rate. Application Based Metrics take into account the specific behaviour of the application. Through proactive analysis of the network or device abilities factors have to be considered such as multicast traffic, the performance of firewalls/VPNs, the effect of router and DiffServ management processes, and queue depth and processor loading which may have an impact on performance.

In order to obtain a meaningful performance characterization, it is important to measure both network data delivery performance (data plane) as well as session control performance (control plane). These measurements include assessments of routing protocol performance (i.e., RIP and OSPF) and the network's ability to perform convergence in the event of an outage. It is also important to measure the effect that queuing management and additional policy requirements have on the processing power of the individual devices and ultimately on network performance.

*Edge Device and Cross Technology Metrics.* On a typical network, traffic may travel over LANs, WAN links, the Internet, and a high-speed backbone, and satellite links. Integration of different technologies presents a complex and formidable network analysis challenge. Since overall performance is determined end-to-end, every technology along the path must work together on a sufficient performance level.

### Measurement Methods

Active measurement methods inject test traffic into the network in order to measure network characteristics, while, passive measurements rely on the observation of traffic that already exists in the network. Each method

# Moving to IPv6 in Europe

has its specific advantages and disadvantages, and depending on the usage context both approaches are needed.

Active measurement experiments offer full control over the traffic profile that is measured. The generated traffic stream uses a pre-defined distribution of sending rate and packet size. The test packet can carry specific load data that helps in the computation of the metrics, e.g. time-stamps and sequence numbers. Active measurements are reproducible and can be performed at any time and with any kind of traffic that is of interest for the specific measurement objective. However active measurements are generating additional traffic load for the network under test, which may have an impact on measured results. Test traffic may cause annoyance for intermediate providers, especially if test traffic is not recognizable as such, and providers could even suspect an attack.

In contrast to this, passive measurements are based on passive observation of traffic in the network. They provide a statement about performance at the moment in the monitored network section. It is particularly useful for scenarios where a statement about the actual situation in the network is required (like SLA validation, traffic engineering).

Formerly, passive monitoring mainly performed simple operations like packet and bytes counting for associated metrics, like volume or throughput. It operated on the link/interface level, hence collecting information on the aggregated traffic only; correlation of observational data from different observation points is hard at this granularity level. With fast packet filtering and classification, however, more significant metrics can be quantified by passive methods.

For most metrics, observations from at least two measurement points have to be correlated. The usual approach to realize passive OWD measurements e.g. is to generate a timestamp and a unique packet ID for each packet at the two points and send this information to a control instance that calculates the delay. Particular difficulties in packet event correlation arise when packets are lost or duplicated.

Different algorithms exist for the generation of a unique packet ID. Packet-IDs can be generated by using "compression" functions (hash functions, CRCs, etc.) over the invariant header fields and parts of the payload. It is important that:

- The probability of collisions (the generation of the same packet ID for non-identical packets) is low;
- The packet ID generation consists of operations that allow a fast and inexpensive realisation, and;
- The size of the ID is as small as possible in order to reduce the amount of data captured. In addition, passive methods need to address privacy issues when capturing traffic from customers.

Under certain circumstances it is not possible to measure performance directly end-to-end but only piece-wise on a domain-to-domain basis and one needs to concatenate measurements. Research on so-called spatial metrics measurement examines the derivation of end-to-end performance characterizations from the sequence of measurements of segments in an IP path trajectory.

Another issue that needs to be addressed is *time synchronization*. If the test system is geographically distributed, precise synchronization of local clocks is necessary. Since oscillators tend to drift, synchronization has to take place reasonably frequently. A good solution is to use an external reference clock to synchronize the decentralized components. For global synchronization, the following solutions are available:

- For public NTP, several servers exist. Depending on the distance of these servers to the test system, network conditions, etc. public NTP can achieve a precision of up to 10 ms;
- Satellite based Global Positioning System (GPS) is precise up to 10  $\mu$ s.

## Intra- and Inter-domain Network Monitoring

IPv6 performance analysis requires the integrated combination of intra-domain and inter-domain approaches. A comprehensive infrastructure must include components for a diverse range of functions. For network-wide inter-domain interoperability it is necessary to base the monitoring and measurement system on standardised interfaces, data formats and protocols for the exchange of data between components and across administrative domains.

Basic components in the monitoring infrastructure comprise the probes and meters that perform the active and passive monitoring functions. They need to perform functions such as test traffic generation, exact time stamping, packet capturing and ID generation. In order to keep the amount of measurement data manageable intelligent algorithms have to be deployed for sampling and aggregation of results.

The control plane must handle probe configuration, flexible setting of filters and establishment of an efficient data collection process, which should be adaptable to network conditions, e.g. reduce network load generated by test traffic and result transmission under network congestion or start certain monitoring functions triggered by particular events. Policy-based configuration approaches are promising means to cope with the complexities of the heterogeneous multi-domain environment.

In addition to the plain monitoring operations, supporting functions are required such as topology and path detection, localization of suitable monitoring points. End-to-end performance issues require the cooperation of multiple parties. Federated inter-domain databases with automated information processing are needed to derive full path performance metrics. For the exchange of measurement data across domain boundaries privacy issues have to be taken into account. Rules and policies have to be agreed between providers that regulate the access and availability of performance data; anonymity of measurement data has to be supported to protect user privacy.

Visual data mining creates graphical presentations for vast data volumes and supports the network operator in a variety of tasks. The measurement infrastructure is utilized for verification of SLAs and QoS of application classes. Measurement data constitutes a basis for modelling and supporting simulation suitable for short-term traffic predictions in traffic engineering and trend analysis for the mid-term network planning. The performance traffic matrix helps in troubleshooting tasks that rely on timely response. The study of event patterns allows for automated identification and localisation of specific network problems and detecting anomalies e.g. DoS attacks, bottlenecks or unused excess capacity. Collected trace and performance data form valuable input for further networking research allowing analysis of the effects and interplay of various application and traffic mixes.

## Performance Testing

The primary goal of performance testing is to evaluate the behaviour of an implementation under test under conditions that emulate various environment conditions such as different traffic mixes of background load and overload situations. System performance is usually tested against a background scenario, i.e. a load that realistically model those conditions expected for the target production environment of a system.

In performance testing, active and passive methods can be applied. Active test methods are used to determine end-to-end related system properties. However, even if a network provides sufficient performance, this does not mean that component interoperability is optimal or that there are no bottlenecks. Thus, additional link or device based monitoring is a key factor in performance evaluation. Another reason to introduce passive measurement components into active network test setups is to validate the appropriateness of the chosen test scenario which usually is defined on a per link level but implemented on the basis of ingress/egress nodes of a network.

An intricate task is the modelling of meaningful test scenarios, and to achieve a realistic distribution of appropriately shaped test traffic. Network load modelling can be done either “trace-based” or “analytic”. The “trace-based” approach uses pre-recorded data. It has the advantages that it is easy to implement and moreover, mimics activities of known systems of the “real work”. However, it treats workload as a “black box”, i.e. it provides no insight into the cause of the recorded behaviour. There is no way to adjust the workload model for future conditions or varying demands. This problem puts limits on the usefulness of a pure trace based approach for scenarios that validate new technologies and novel network setups.

The analytical approach tries to explain network load profiles by means of mathematical models. Clearly, finding those models is a challenging task. Which characteristics are important to which extent? Are identified factors independent or do they influence each other? Can a developed model be verified empirically? Can the model be updated to reflect changing user behaviour caused by the availability of new technologies, more bandwidth, new services, etc.



# Moving to IPv6 in Europe

## Performance Considerations for IPv6

It is expected that the introduction of new and evolving IPv6 services may lead to additional performance metrics, or that existing metrics may need to be modified. Items that have to be considered in this context include:

- Performance of translation mechanisms for IPv6: NAT-PT (Network Address Translation-Protocol Translation, IETF RFC for IPv4 to IPv6 protocol translation), Tunnelling, and Dual stack;
- Mobile IP related performance: e.g. time for re-authentication in the new domain, neighbour discovery in IPv6 (which doesn't exist in IPv4 architectures);
- Use of IPv6 security mechanisms such as IPsec through the new IPv6 extension headers.

The notion of a “micro-flow” in IPv4 is based upon the 5-tuple: Source address, destination address, source port, destination port, and protocol (TCP, UDP). With the introduction of the flow label in IPv6, and with the possibility of application specific information being added to the flow label, the “micro-flow” in IPv6 can be regarded as a 3-tuple: Source address, Destination address, and Flow Label.

All of the above criteria have implications not only on metrics for IPv6, but also on the SLA associated with IPv6 services. In particular, the flow description, as defined in the SLA changes, and also the associated methodologies for capturing flow data and the corresponding metrics.

## 5<sup>th</sup> FP IST Projects Working on IPv6 Performance

- *IST 6QM*: 6QM (<http://www.6qm.org>) is specifically devoted to measurement technologies for Quality of Service in IPv6 networks. 6QM develops a comprehensive system integrating functions for QoS measurement, such as packet capturing, precise time-stamping, data collection, QoS metrics derivation (delay, loss, jitter, etc.) and result presentation.
- *IST Intermon*: Intermon (<http://www.ist-intermon.org/>) looks at IPv4/IPv6 multi-domain Internet infrastructures. It develops an inter-domain QoS monitoring and analysis architecture for validation, planning, forecasting and optimisation of inter-domain QoS (with “QoS feedback”) integrating different components for automated Internet inter-domain structure analysis, QoS and traffic monitoring, measurement-based modelling, simulation and visual data mining using policy controlled data bases.
- *TF-NGN Performance Monitoring Infrastructure*: The Task Force on Next Generation Networks TF-NGN is a collaborative effort of European national research and education networks (NRENs) and associated research organizations, coordinated by TERENA and DANTE, performing early trials and studying performance and deployment issues. As the development part of the IST project GN1, it complements the infrastructure building effort of the GÉANT network. GÉANT forms the pan-European research networking backbone with core network capacity of up to 10 Gbit/s. It interconnects more than 30 NRENs in Europe and provides connectivity to other research networks worldwide.

TF-NGN explores technologies viewed as strategically important for the NRENs and GÉANT. One of the activities newly included in the GÉANT technology roadmap for 2003 explores a monitoring and measurement infrastructure for the research networks. Performance Monitoring has the goal of devising an international inter-domain monitoring infrastructure that can serve for Service Level Agreement (SLA) verification as well as for other research and operational purposes.

Intra- and inter-domain monitoring infrastructure aims to monitor “performance” metrics (such as one-way delay, jitter, packet loss, available bandwidth, etc) inside a domain and across several domains. The aim is to provide to different groups of users (NOCs, GRIDs, etc) a cross-domain view.

In its first phase, focus lies on identifying the subset of metrics that should be monitored, the interactions between the domains and to provide recommendations on how the metrics should be monitored. Measurements need to be performed for IPv4, IPv6 and different types of service. An embryonic system of the inter-domain monitoring infrastructure is planned to be setup by Q3 2003.

For each domain the measurements are collected and stored in a domain central storage from which domain measurements can be retrieved and exchanged with other domains on request. The architecture will be tested during a trial phase. During this phase, measurement boxes and the domain central storage

will be installed on at least three adjacent domains. The metrics monitored during the early trials are the One-Way Delay (OWD), the Instantaneous Packet Delay Variation (IPDV), the One-Way Packet Loss (OWPL) and packet re-ordering. But the architecture has to be generic such that emerging metrics can be added. In later studies, the group will focus on the integration of further metrics and the development of tools to support in detection, localisation and diagnosis of performance problems. Those tools should be tailored for use by network managers of all involved networks (transit backbone, NREN, access, campus) and if possible for end-users.

- *Pilot PERT Initiative:* The focus of attention is currently shifting from purely network-centred QoS mechanisms to a more holistic view of what is termed the “end-to-end performance problem”. The performance experienced by network users is the result of a complex interaction of many components: application software, operating systems, network adapters, and networks belonging to separately administered domains (campus, regional and national backbone, international backbones). In the past, the “wide-area” parts of the network would form the bottleneck. But over the last few years, abundant network capacity has been rolled out globally, and is now available at competitive prices. Hence performance limitations may become apparent also at other segments along the end-to-end path.

The networking and computing community includes many specialists with expertise for certain aspects of performance: system administrators for hardware resource dimensioning and operating system effects, campus network specialists for cabling and LAN topology problems, wide-area network operators for routing, queuing, and peering issues. Such experts often show a tendency to delegate direct communication with end users. And in the case of performance issues involving several domains of responsibility, end users may end up being referred between different support centres, of which none is willing to accept “ownership” of the problem.

What is missing, are cross-disciplinary experts that help locate the problematic area(s) before relevant area-specific experts can take over. Such generalists need to understand the totality of factors contributing to the end-to-end performance equation, as well as their interplay. The term PERT refers to such a cross-disciplinary group with the task of looking at performance issues in an integrated way, where PERT stands for “Performance Enhancement and Response Team”.

The PERT focuses vertical expertise. They will need to communicate with application developers, users, and network operators of involved domains. For their task, they depend on access to measurements or monitoring data from various points in the network, including participating host systems and applications in order to identify domains that need to react. They propose possible remedies, and provide the “logistics” function to bring multi-disciplinary experts together to jointly solve the problem.

The PERT’s task includes accepting reports about performance problems, or “cases”, from users or developers or networked applications, when preliminary diagnosis of the issue with the help of local staff (system and network administrators) had failed in clearly identifying a single cause of the problem. The PERT may reject a case if it decides that the reporter hasn’t sufficiently tried to resolve the issue using ordinary support channels.

The PERT should collect required information from sources including the reporting user, other users of the distributed application, system administrators and network operators along the end-to-end path and data collected from the monitoring and diagnostic infrastructure. These activities will generate vast and diverse sets of data. Data storage and access functions must support several different tasks, including: ongoing diagnosis and resolution of a PERT “case”; research of “historic” data in relation with a new case; evaluation of data for the purposes of scientific research or trend analysis. Data privacy issues must be given particular care. Collected information may need to be post-processed to hide privacy-sensitive or otherwise confidential content, and users (the PERT clients) will have to give consent that the information will be stored for analysis and future reference.

An important function of the PERT is to document known performance issues, together with possible ways to address them. This will hopefully allow application developers, network operators, and users to solve these issues themselves in the future. The PERT will also document successful diagnostic strategies in an “End-to-End Performance Cookbook”, so that users/developers and their local support staff can analyse

# Moving to IPv6 in Europe

end-to-end performance problems by themselves. Another important contribution is to make available tools for the diagnosis of difficult end-to-end performance problems, along with guidance on when and how to use them.

Where such tools may require measurement and monitoring infrastructures, these infrastructures should be made as openly available as possible, so that it can be deployed on additional networks, and used by more people at the “edges” of those networks.

The PERT should maintain productive relations with software developers, manufacturers, standardisation bodies and the networking research community or involve them in participation in PERT. If successful, it should strive to reproduce by spinning off regional or mission-specific PERTs, just like the initial CERT at Carnegie Mellon spun off hundreds of CERTs that operate in an autonomous, but federated manner.

In the context of GÉANT research activities it is planned to establish a pilot PERT organization for the academic and research networking community. This network will include experts from as wide a range of development, systems, and networking domains as possible. The major challenge for the PERT will be to integrate the various types of expertise of its members, so that an integrated view of network performance issues can emerge.

For the pilot PERT it is necessary to install an efficient organization and communication infrastructure that supports the internal information exchange and provides a clear and convenient user interface externally. This includes a public web site with contact information, a base of problem-solving documentation and pointers to diagnostic tools. Case submission should be based on e-mail and form-based Web interfaces to streamline the process. Internally, mailing list exploder and a ticketing/case management system will find usage, besides telephone, ad-hoc phone conferences and instant messaging.

The pilot PERT will cooperate with the Internet2 e2ePI (End-to-End Performance Initiative) as well as with the Performance Monitoring activity of TF-NGN.

## 3.4.4. Future Work Items

IPv6 will be a central enabler for realising strategic goals towards the information and knowledge-based society and economy in Europe. The common IPv6-based networking layer will create the basis for mobile and wireless systems beyond 3G, where different terrestrial access technologies are combined to realise the vision of being “optimally connected anywhere, anytime”, and IPv6 will be the underlying technology in moving to affordable and wide-spread broadband access for European users including those in less developed regions.

The development of conformance and performance technologies for the All IPv6 network will create a powerful leverage for realising a fast transition scenario. The supporting environment for IPv6 conformance and performance helps to establish confidence in the IPv6 technology among the players and creates assurance for the adoption of the next generation IP protocol by manufacturers, service providers and end users.

There is currently a set of 5<sup>th</sup> FP IST projects focusing on the topics of IPv6 Conformance and Performance, of whom several partners contributed to the contents of this section. However it is obvious, that more work will remain to be done, and the All-IPv6-World working group identified in its work item list Conformance and Performance for IPv6 among its topics for which they recommend further research to be performed in the upcoming 6<sup>th</sup> Framework Programme.

It becomes apparent that the formerly separate fields of testing and network monitoring are coming closer together. Performance monitoring and measurement devices are indispensable components for realising complex test scenarios. On the other hand, testing approaches are seen to move beyond the deployment phase also into network operation. Testing capabilities are expected to become readily available functionality used in network management for diagnosis and exception handling. Detection of network state is needed for fast reaction to unforeseen events and conditions in order to maintain network health. Useful synergies and innovative approaches can be derived by further integrating and harmonising methodologies and approaches from these two areas.



## 3.5. Security and IPv6

This section provides an overview of some of the most interesting areas of research and development currently evolving with regard to IPv6 and security. Firstly we examine the state-of-the-art with regard to IPv6 technology and security, briefly exploring the subjects of IPsec, Secure Neighbour Discovery, Mobile IPv6, Cryptographically-Generated Addresses, securing transition mechanisms, and firewalling. Secondly, a specific example of innovative research undertaken as part of the IST project 6WINIT (IPv6 Wireless Internet Initiative) is explored.

### 3.5.1. State-of-the-Art

Research into IPv6 security technologies covers a range of complex subjects that are developing at a considerable rate. This section is intended to highlight some of the most interesting areas and to provide the reader with an overview of the subject and some pointers to further reading.

#### IPsec

IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. RFC2460, "Internet Protocol, Version 6 (IPv6) Specification", states that, "a full implementation of IPv6 includes implementation of the... Authentication Header and the Encapsulating Security Payload", as specified in RFC2402 and RFC2406 respectively. RFC2401, "Security Architecture for the Internet Protocol", states that, "All IPv4 systems that claim to implement IPsec MUST comply with all requirements of the Security Architecture document. All IPv6 systems MUST comply with all requirements of the Security Architecture document". This latter statement is one of the important differences to bear in mind when discussing IPv4 and IPv6 security, and is one reason why it is sometimes claimed that IPv6 is "more secure" than IPv4. IPv4 systems *may* support IPsec —IPv6 systems *must* support IPsec.

Furthermore, work is ongoing within the IETF to define a set of minimal requirements for IPv6 nodes allowing IPv6 to function well and interoperate in a large number of situations and deployments<sup>11</sup>. This work emphasises once more that, "An IPv6 node MUST be able to process [ESP & AH] headers", and, "Security Architecture for the Internet Protocol [RFC2401] MUST be supported. ESP [RFC2406] MUST be supported. AH [RFC2402] MUST be supported". This document also places requirements on IPv6 nodes with regard to key management methods and states that manual keying must be supported, IKE<sup>12</sup> may be supported for unicast traffic, and that automated keying (e.g. IKE) must be supported whenever the key refresh or anti-replay features of AH and ESP are required, or whenever dynamic creation of IPsec Security Associations (SAs) is required. It should be noted that IKE has come in for considerable criticism<sup>13</sup> and the IPsec working group of the IETF is developing a simplified successor to IKE<sup>14</sup>.

#### Secure Neighbour Discovery

IPv6 nodes use the Neighbour Discovery (ND) protocol to discover other nodes on the link, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbours. If not secured, the ND protocol is vulnerable to various attacks. The existing IETF standards specify that IPv6 Neighbour Discovery and Address Autoconfiguration mechanisms may be protected with

<sup>11</sup> IPv6 Node Requirements, *draft-ietf-ipv6-node-requirements-04.txt*, John Loughney et al.

<sup>12</sup> Internet Key Exchange, see RFCs 2407, 2408, 2409.

<sup>13</sup> See, for example, "A Cryptographic Evaluation of IPsec", N Ferguson & B. Schneier (<http://www.counterpane.com/ipsec.html>).

<sup>14</sup> Internet Key Exchange (IKEv2) Protocol, *draft-ietf-ipsec-ikev2-05.txt*, Charlie Kaufman (ed.).

# Moving to IPv6 in Europe

IPsec AH. However, the current specifications limit the security solutions to manual keying due to practical problems faced with automatic key management. In order to address this shortcoming, a new effort has begun in the IETF to develop solutions for secure neighbour discovery and a recent draft has been published which provides details of a potential solution based on IPsec and cryptographically generated addresses<sup>15</sup>.

## Mobile IPv6

Mobile IPv6<sup>16</sup> uses IPsec to protect signalling between the home agent and the mobile node. The base document defines the main requirements these nodes must follow whilst an additional document discusses these requirements in more depth, illustrates the used packet formats, describes suitable configuration procedures, and shows how implementations can process the packets in the right order<sup>17</sup>. In order to protect signalling between correspondent nodes and the mobile node, a new approach has been specified known as "Return Routability".

The Return Routability procedure enables the correspondent node to obtain some reasonable assurance that the mobile node is in fact addressable at its claimed care-of address as well as at its home address. Only with this assurance is the correspondent node able to accept Binding Updates from the mobile node that would then instruct the correspondent node to direct that mobile node's data traffic to its claimed care-of address.

This is done by testing whether packets addressed to the two claimed addresses are routed to the mobile node. The mobile node can pass the test only if it is able to supply proof that it received certain data (the "keygen tokens"), which the correspondent node sends to those addresses. These data are combined by the mobile node into a binding management key, denoted Kbm.

The figure below shows the message flow for the Return Routability procedure.

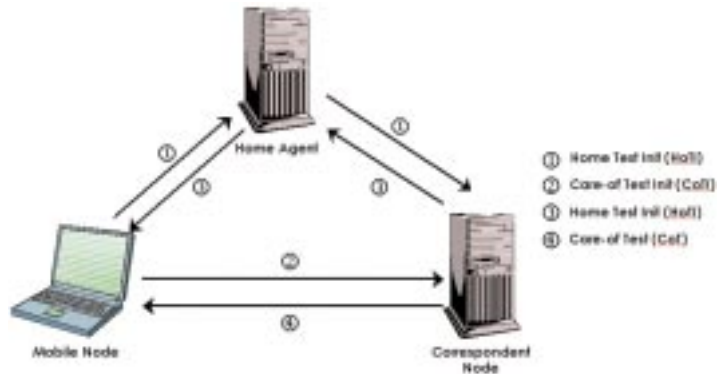


Figure 9: Mobile IPv6 Return Routability Procedure

The Home and Care-of Test Init messages are sent at the same time. The procedure requires very little processing at the correspondent node, and the Home and Care-of Test messages can be returned quickly, perhaps nearly simultaneously. These four messages form the Return Routability procedure.

## CGA

Cryptographically generated addresses (CGA) are IPv6 addresses where the interface identifier is generated by hashing the address owner's public key. The address owner can then use the corresponding private key to assert

<sup>15</sup> SEcure Neighbor Discovery (SEND), *draft-ietf-send-ipsec-00.txt*, J. Arkko et al.

<sup>16</sup> Mobility Support in IPv6, *draft-ietf-mobileip-ipv6-21.txt*, D. Johnson et al.

<sup>17</sup> "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", *draft-ietf-mobileip-mip6-ha-ipsec-03.txt*, J. Arkko et al.

address ownership and to sign messages sent from the address without any additional security infrastructure. The main advantage of the CGA-based authentication is that additional security infrastructure, such as a PKI or TTP, is not needed. Potential applications include Mobile IPv6 binding update authentication, proof of address ownership in secure neighbour discovery and duplicate address detection, and key exchange for opportunistic IPsec encryption and authentication.

The figure below illustrates a simplified model for CGA-based authentication. The recipient of a Neighbour Advertisement with a CGA Address, a public key, and a digital signature in the header can have confidence that:

- The packet was not modified in transit (due to the signature), and;
- The sender of the packet has a right to claim possession of the address (due to the authenticated CGA address).

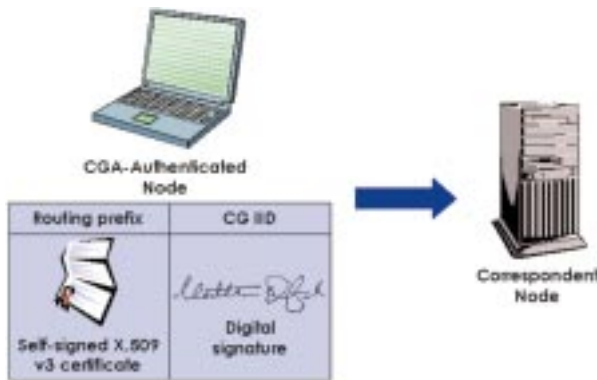


Figure 10: A Simplified Model of CGA-based Authentication

When the correspondent node receives such a packet, it can verify that the hash of the public key contained in the X.509 v3 certificate matches the interface ID portion of the source address, and it can use the public key to verify the digital signature and thereby ensure that the packet was not modified in transit.

## Transition mechanisms and security<sup>18</sup>

- *Tunnelling*: A site may filter some traffic at its border routers or may be using a firewall. If they do not support IPv6 one may want to get IPv6 connectivity by setting up a tunnel from an internal router at the site, to some router outside the site. The internal router then becomes a border router with respect to IPv6. If filtering is done at the border for IPv4 one will probably also want to do the same for IPv6. This filtering should be done at the tunnel end-point. One could consider employing filtering at the border routers or other routers the tunnel passes through, but this is not recommended. First of all, the filtering can be done much more efficiently at the endpoint. Secondly it is unlikely that the routers can do this if they do not support IPv6. A firewall could perhaps be configured to look for specific bit patterns in the payload though. This might make it possible to filter on at least IPv6 source and destination addresses; but again, this approach is not recommended. One might also want traffic statistics showing the amount of IPv6 traffic per prefix, port etc. Once more, since peeking inside tunnels is hard, one should inspect the packets when they are outside the tunnel, perhaps at the end-points.

When deploying IPv6 inside a site, using a different border router than the one used for IPv4, it is necessary to be sure that IP protocol 41 is not filtered along the path between the two IPv6 tunnel end-points if

<sup>18</sup> This section is an extract from 6NET deliverable D6.2.2 "Operational procedures for secured management with transition mechanisms" which is available online at <http://www.6net.org>

# Moving to IPv6 in Europe

direct IPv6 encapsulation is used. In the case that GRE encapsulation is used, it must be checked that IP protocol 47 is not filtered between the tunnel end-points. As filtering is usually done at the site level, then this check can be done directly at the network operation centre (or network administrator) of the site that wants to connect or at both end-point sites if the tunnel is aimed at connecting the sites directly (without third intermediate sites). Note that this situation tends to disappear as more and more backbones offer IPv6 connectivity.

There might be IPv6 implementations that do not allow the same management operations for tunnel interfaces as for physical interfaces. We have seen at least one host implementation that did not allow `tcpdump` on tunnel interfaces. There are probably other examples.

- *Tunnel Brokers*

- Authentication: In general one would like to have some idea of who is using the different tunnels, and also make sure that only the owner of the tunnel can change the configuration. If a broker is run by an organisation with directory type structures installed (e.g. a university for their students) one may be able to use usernames and passwords or other means of authentication that the organisation already utilises for other services. If there is no prior relationship with the user, one typical approach is to have people register with name, e-mail address, etc. and then receive through e-mail an auto-generated password. This way there is uncertainty about the real identity of the final users, but one knows that the e-mail address is confirmed as operating and the person receiving the password is one of the receivers of e-mails to this address.

An alternative approach could be to employ RFC3129 “Requirements for Kerberized Internet Negotiation of Keys”. Clients authenticate to a centralized server —the Key Distribution Centre—, which in turn issues tickets that servers can decrypt thus proving that the client is who it claims to be. One of the elements of a Kerberos ticket is a session key, which is generated by the KDC that may be used by the client and server to share a secret. Kerberos also allows for both symmetric key authentication, as well as certificate based public key authentication (PKinit).

- Enabling/disabling tunnels: A user might be able to enable and disable the tunnel by using a web interface or perhaps a script using HTTP or other protocol to communicate with the broker. If the user is always connected with a fixed IP address, all should be well. As long as the user leaves the tunnel enabled, it should forward packets. However if a user uses a connection method that does not guarantee a static IPv4 address (e.g. dial-up) and somehow gets disconnected, it would be prudent to take the tunnel down automatically to prevent unnecessary use of resources. More seriously, this would assure that the session is not (intentionally or unintentionally) “hijacked” by someone else who connects with the same address, thus receiving traffic intended for the original user. One possibility would be to automatically take down the tunnel if no packets are received from the user for some time, especially if packets are flowing in the other direction. This could be combined with some utility at the user end that sends some sort of keep-alive messages. The type of packets does not really matter as long as something is sent. One could also have some TCP session between user and broker for controlling the tunnel, and have keep-alive messages sent over the TCP session. If no data arrives or the session is reset the tunnel can be taken down. The downside to all this is that a solution is harder to deploy if it would require some specialised software for the user operating systems.

- Guarding against misuse and statistics: When running a tunnel broker, one should also apply filtering to some IPv6 packets. The broker (or more correctly, the router that is the end-point for the tunnels the broker manages) should drop any packets received on a tunnel interface, that have a source address not belonging to the remote side (no route for that address in that interface). And it should also not send packets into a tunnel that has source address belonging to the remote side. The first kind of filtering may be problematic if the remote end is multihomed, but for typical broker users, this would be the exception. There should also be filters for packets with IPv4-mapped addresses and some consideration for monitoring of the tunnels usage.

At least some statistics on bandwidth usage per tunnel might be useful. If somebody offers a broker to random Internet users, people should not be very surprised if they encounter DoS attacks. It is good if similar attacks and other problems can be detected, and such traffic blocked if necessary.

- *Dual-stack*: The network administrators should remain cautious not to deploy IPv6 on IPv4 equipment when the IPv6 filtering is not equivalent to the current IPv4 filtering.

It is possible for malicious users to access a private network by using IPv6 as an entry point, since basic filtering that should normally prevent this (as it should be for IPv4) is not often deployed. For an outsider to discover the IPv6 address of an important server may not be difficult, given that the system administrators tend to prefer allocating IPv6 addresses at the beginning of their prefix class (usually lower than  $:\text{f}\text{f}\text{f}$ ), which makes the range of IPv6 addresses to scan for such a purpose a lot smaller. As a result, when connecting to a device running in dual-stack mode inside a network that was considered inaccessible by the outside world, it is likely without much effort to compromise further equipment inside this network (using either IPv4 or IPv6 from the entry machine).

In an incident, hackers, after they have compromised an IPv4 device, have enabled IPv6 in IPv4 tunnelling, with the aim to successfully bypass filtering and Intrusion Detection Systems (IDS) capabilities on the system for exchanging sensitive data.

- *6to4*: Tunnelling mechanisms, especially automatic ones, are always questionable from the security point of view; if IPv4 addresses can be spoofed, anyone can inject any kind of traffic to the tunnel one wants —and even if the source address spoofing is not possible, one may be able to launch several kinds of attacks. Secure management of 6to4 is only an issue if using 6to4. As 6to4 is a transition mechanism, its use should be avoided if other alternatives, such as manually configured tunnelling or native IPv6 are available.

If 6to4 routers or relays are present, there are a lot of ways to attack or abuse them. However, it should be noted that in most cases, this is not any more attractive than abusing or attacking any other IPv4 (or IPv6) services.

The threats can be classified into several categories. Those that can be easily protected against include:

- Attacks against the 6to4 pseudo-interface; these can be defended against by adding an access-list to the pseudo-interface to filter out bad tunnelled packets;
- Local directed broadcast attacks (on relays only); as above, an access list will handle this case;
- Theft of service, if providing restricted 6to4 relay service; generally, this is not considered a big issue, but can be handled with careful routing policy and if necessary, access lists;
- Relay spoofing attack; a 6to4 pseudo-interface is an interface like any other, and one must install the usual access lists on it. For example, the site should configure the inbound access list to reject any source addresses that have been spoofed to belong to the site itself.

In addition, there are several methods whereby 6to4 can be used to reflect a denial-of-service attack, to make it more difficult to trace. However, these problems remain unresolved. Therefore, it is recommended to monitor the traffic levels of the 6to4 pseudo-interfaces regularly to see whether there are any anomalies and react if necessary.

- *ISATAP*: Since ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) uses tunnelling, the general tunnelling issues are valid. Another issue worth considering is that all the site's ISATAP hosts will be on the same IPv6 link. It's very hard to protect someone on the link from someone else on the same link. Also there are several protocols that have some additional security by using link local addresses or hop limit (setting it to 255).

With no filtering in site border routers, the entire IPv4 Internet would be part of the link. It's important that the site does IPv4 and IPv6 ingress filtering. At the site border one should also drop IPv4 protocol 41 packets (IPv6 over IPv4 tunnels) unless they belong to known tunnels. There is still some spoofing possible inside the site, but that is comparable to the threat on a physical link. The problem might be somewhat bigger due to the potentially large number of hosts on the same link though. Except for the security aspects, there is no technical reason preventing the use of ISATAP between sites, but it is strongly recommended that this is not done.

Monitoring traffic between the ISATAP hosts at a site is difficult. The hosts are on the same virtual link, so the packets do not pass through any routers (of course the packets might pass through IPv4 routers on the layer below). At the ISATAP router one can monitor traffic as usual though, but packets between hosts on the ISATAP link do not pass through the router.



# Moving to IPv6 in Europe

- *DSTM (Dual Stack Transition Mechanism)*
  - Filtering on the DSTM server: It is important for the network administrator to be sure that the hosts using the DSTM server are allowed to do so and therefore appropriate filters should be deployed on the DSTM server;
  - Authentication: Future implementations of DSTM that plan to use the Tunnel Setup Protocol (see below) and DHCPv6 should support authentication;
  - Monitoring: For monitoring a DSTM enabled network, the system administrator should monitor the tunnels created on the TEP (Tunnel End Point) and the allocations made by the DSTM server. The system should be able to check that the tunnels correspond to the allocations performed by the DSTM server and send alert messages in case an error occurs.
- *Tunnel Setup Protocol (TSP):* The protocol makes it possible to authenticate the message sender (using MD5 as an example). This leads to many deployment possibilities:
  - DSTM servers can check that tunnel requests come from allowed hosts;
  - DSTM servers can communicate the IPv4 in IPv6 tunnel characteristics to the DSTM client and the TEP. The TEP and the client can check the data comes from a well-known server before configuring access;
  - Tunnel brokers can check whether tunnel requests come from the correct host or router;
  - A tunnel broker's TEP and the client can check whether the tunnel data come from a well-known broker.

## Firewalling

There are quite a few potential problems regarding firewalling or packet filtering in IPv6 environment. These include problems parsing packets beyond unknown Extension Headers, and introduction of end-to-end encrypted traffic and peer-to-peer applications. There may also be need to extend packet matching to include some Extension Header or Destination Option fields.

IPv4 silently ignores options it does not recognize; options have a specific, pre-defined format. IPv6 Extension Headers are structured differently: the header format can change, and generally it is not possible to parse the header, or proceed to the following Extension Headers unless the processing of the previous header has been implemented.

The above is problematic as it is often the case that a packet filter will want to examine terminal headers, e.g. TCP or UDP. That is not possible if there is a problem processing any one of the preceding headers.

With the promise of the restoration of end-to-end transparency, and if at least some of the challenges for implementing Public Key Infrastructures are worked around, it may be possible that the amount of end-to-end encrypted traffic will increase enormously. The traffic is likely to be encrypted using IPsec. In this case, on-the-path observers (such as a firewall) do not have the possibility to examine usually critical headers (such as TCP/UDP). This may result in an administrative decision to disable IPsec-encrypted traffic by filtering it out completely. A possible approach would be to try to shift the focus, at least partially, to end-node firewalls; if end-nodes are not particularly trusted, an end-node, admin-controlled firewall might be provide a reasonable trade-off between security policy and cryptography.

There appears to be no network-based solution for this, which is indeed a feature of end-to-end cryptography.

As above, the restoration of end-to-end transparency provides a possibility for a more widespread use of peer-to-peer applications. Such applications are often a bit problematic from the firewall perspective: it is often the practise to allow outbound (from the protected site) traffic while allowing in only the related traffic (and naturally some other administratively permitted traffic). Being able to run (some) peer-to-peer applications easily in a controlled environment would be valuable.

A possible approach, as above, would be to try to shift, at least partially, the focus to end-node firewalls; if end-nodes are not particularly trusted, an end-node, admin-controlled firewall might be provide a reasonable trade-off between security policy and cryptography.

## Transient Addresses for Related Processes

In a paper entitled “Transient Addressing for Related Processes: Improved Firewalling by Using IPv6 and Multiple Addresses per Host”, Peter Gleitz and Steve Bellovin have presented an interesting adaptation to current firewall models<sup>19</sup>. Encouraged by the new abundance of addressing possibilities provided by IPv6, they propose a method whereby hosts temporarily employ and subsequently discard IPv6 addresses in servicing a client host’s network requests. The method provides certain security advantages and neatly finessees some well-known firewall problems caused by dynamic port negotiation used in a variety of application protocols, although it is not without limitations. This technique is mentioned here to provide a reference point for interested readers to research further.

There now follows a description of an advanced IPsec implementation for IPv6 that formed part of the 6WINIT project<sup>20</sup>.

### 3.5.2. Road Warrior

While the usual IPsec implementations provide security between two IPsec gateways (tunnel mode) or two IPsec clients (transport or tunnel mode), the Road Warrior is an extension for the provision of security between a client and a gateway, using the IPsec tunnel mode. The term Road Warrior more specifically identifies the IPsec client itself.

Furthermore the Road Warrior supports scenarios in which the client is mobile and dynamically changes its access point to the global Internet. While in usual scenarios the IPsec devices involved (gateways or clients) are constrained to keep their fixed access point to the global Internet, and therefore their fixed configured IP addresses, the Road Warrior scenario only forces the IPsec gateway to keep a fixed IP address; the address of the client can be changed dynamically. This property makes the Road Warrior especially valuable for mobile users. Of course, to be able to route properly over the Internet, these dynamically changing IP addresses of the Road Warrior have to be global IP addresses. IPv6 provides a sufficient address space for a large-scale deployment of devices such as Road Warriors.

Even if the Road Warrior is suitable for mobile users, it does not provide transparent mobility, as is the case with Mobile IP. As the Road Warrior establishes a secure connection to an IPsec gateway, this connection will be terminated every time the Road Warrior changes its IP address. That is, after changing the access point to the global Internet, the establishment of a secure connection to an IPsec gateway has to be re-initiated before any other applications can be restarted using the security functionality provided by the Road Warrior.

#### Road Warrior Architecture

The following figure shows an example scenario to illustrate the Road Warrior functionality. In this example scenario, a mobile user (Road Warrior) has a laptop with an IPsec stack running on it, and attaches to the global Internet via different WLAN access point. This mobile user wants to exchange information over the Internet with its company network, which is protected by an IPsec gateway. While the IPsec gateway is configured with a fixed IP address, the Road Warrior’s IP addresses change from access point to access point.

Having accessed the network, the Road Warrior is first configured with an IP address. In IPv6, this can be done using stateless address autoconfiguration or DHCP. Once this address is configured, the Road Warrior initiates the establishment of a security association to the IPsec gateway. Once this security association has been successfully established, all applications running on the Road Warrior can communicate with the company network in a secure fashion.

<sup>19</sup> For the full text, see <http://www.research.att.com/~smb/papers/tarp.pdf>

<sup>20</sup> <http://www.6winit.org>

# Moving to IPv6 in Europe

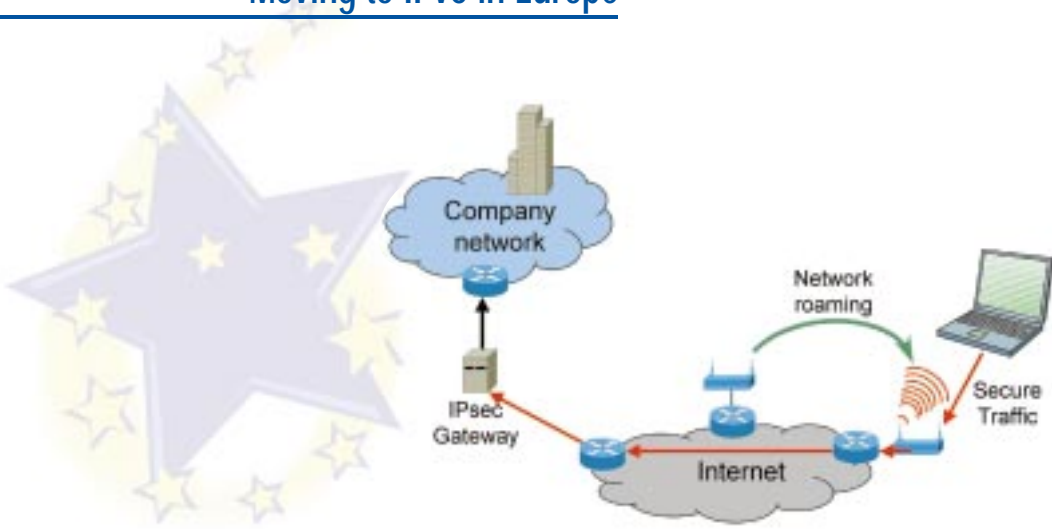


Figure 11: An example of Road Warrior functionality



## 4. Impact of IPv6 on Applications and Services

Users perceive the Internet through the applications they use in their daily work and do not care about the underlying protocols. It is therefore difficult to explain the impact of the IPv6-based Next Generation Internet to the users, because they will see only more new applications. As many new applications have appeared during the last years without IPv6 being there, it is very important to define clearly what applications IPv6 will make possible that would never have existed (or would have been significantly more costly to deploy) if the Internet were to remain IPv4 only.

Let's briefly review what will be the main benefits that IPv6 will bring to the applications and that therefore will be visible to the users.

The main benefit brought by IPv6 is a huge address space that will allow a public IPv6 address for any system or device connected to the Internet. The impact of this huge address space on the applications is expected to be big, because it will allow the recovery of the end-to-end connectivity of applications lost after the introduction of NAT devices. It will enable:

- An enhanced security based on end-to-end IPsec usage complemented by a proper security framework providing digital identities;
- The deployment of applications and services which require public IP addresses with end-to-end connectivity and which are disabled by today's NAT devices, such as
  - Deployment of Voice over IP;
  - Deployment of Mobile IP;
  - Deployment of the previously mentioned IPsec, which is mandatory in IPv6;
  - Deployment of UMTS Multimedia Services based in Release 5 of 3GPP;
  - All kinds of devices needing end-to-end access, for example: remote sensors, PDAs, transport, mobile phones, home devices, etc.;
  - Development of proper P2P or GRID applications needs also public IP addresses.

This chapter provides an overview of the impact that the IPv6 protocol will have on applications and services. The section starts first with a contribution from the LONG project, which focuses on one of the challenge that the transition to IPv6 is facing, the porting of applications to IPv6.

# Moving to IPv6 in Europe

The following sections provide examples of IPv6-based applications and services that illustrate the potential of IPv6. The first example is a contribution from the 6WINIT project and describes several scenarios of wireless medical applications over IPv6 deployed in various hospitals. The second one is a contribution from the xMOTION project and describes a mobile application in eLogistics. The third one is a contribution from the Euro6IX project and describes a Public Key Infrastructure (PKI) implementation of the security framework of the project. Finally, the fourth contribution comes from the MIND and 6POWER projects and describes the use made by adaptive real-time applications of new facilities of IPv6 such as QoS or Flow Labels.

## 4.1. Transition and Porting of Applications to IPv6

The Internet is a huge network with a large number of applications available and in use. Those applications will need to continue to function during the transition from IPv4 to IPv6. Both protocols will coexist for a considerable time to come. IPv6 was designed<sup>21</sup> to fulfil several criteria that should help assure a smooth coexistence during the transition. Those criteria were that:

- Internet hosts and routers may use IPv4 only, IPv6 only or both IPv4 and IPv6 in a dual stack configuration;
- Existing IPv4-only hosts can upgrade to IPv6 at any time, without dependencies on the IP stack used by the rest of hosts or routers in the network;
- New hosts, using only IPv6, can be added at any time, without dependencies on the IP stack used by the rest of hosts or routers in the network;
- Existing IPv4-only hosts can be reconfigured to use also IPv6 in dual stack configuration, without any modification in the IPv4 addresses and configuration used.

These requirements have an impact in at least three areas:

- Application capability: IPv4-only, IPv6-only or IPv4/IPv6 capable;
- IP support in host: IPv4-only, IPv6-only or dual (or hybrid) IPv4/IPv6 stack;
- Network support: IPv4-only, IPv6-only or IPv4/IPv6 enabled.

The most common transition scenario, sees IPv4/IPv6 capable applications running in dual stack hosts connected to an IPv4/IPv6 enabled network. But there will be other scenarios that will need different solutions. For example:

- A legacy IPv4 application which cannot be modified and which needs to be accessible from IPv6 only hosts/applications;
- An IPv6 only host/application that should connect over an IPv4 only network to another IPv6 only host/application.

To support the previous criteria several transition mechanisms have been proposed by the IETF. Some transition mechanisms make use of mappings of IPv4 addresses into the IPv6 address space, which allow automatic address translation.

In the general case, existing IPv4 applications need modifications when ported to IPv6, because the TCP/IP network architecture was not properly layered. Applications can use either symbolic domain addresses or IP addressing to identify hosts and routers. Many applications perform a proper decoupling and use only symbolic domain names above the socket interface. But other applications use IP addresses as parameters needing a big redesign when ported to IPv6.

IPv6 forces the use of a slightly modified version of the transport interface (the IPv6 socket interface<sup>22</sup>). Hence, from the applications point of view, the IPv6 deployment requires changes in the existing code and maybe a redesign of the parts that are IPv4 dependent.

<sup>21</sup> S. Bradner, A. Mankin, "The Recommendation for the IP Next Generation Protocol", RFC1752. January 1995.

<sup>22</sup> R. Gilligan et al., "Basic socket interface extensions for IPv6", RFC2553. March 1999.

# Impact of IPv6 on Applications and Services

The present document provides a summary of guidelines which apply to the design of new IPv6 applications, as well as, to the porting of existing ones to make them IPv4/IPv6 capable. More extensive guidelines produced in the LONG project<sup>23</sup> can be found in “Programming Guidelines on Transition to IPv6”<sup>24/25</sup>, where guidelines for porting applications in the most relevant scenarios are given. This guidelines collect the experience gained from the porting of the Isabel CSCW application<sup>26/27</sup> to IPv6.

## 4.1.1. Application porting Problems

When porting IPv4 applications to IPv6, there may be different levels of difficulty in carrying out the task. If applications use only basic communications facilities, developers only have to identify the application communication module and change some functions and data structures to be ready for the new IPv6 API. However, if applications make more exhaustive use of IP addresses or advanced network facilities, such as multicasting, raw sockets, quality of service or mobility, the porting requires a complete application analysis and much more porting effort.

The standard transport API based on the sockets interface makes the protocol version visible to the application and therefore if the protocol changes address data structures should be adapted to the new environment. Moreover, other facilities such as conversion functions between hostnames and IP addresses are different in the new IPv6 environment too.

Differences between IPv4 and IPv6 sockets APIs are related to a new socket address structure to carry IPv6 addresses, new address conversion functions and several new socket options<sup>22</sup>. These extensions are designed to provide access to the basic IPv6 features required by TCP and UDP applications, including multicasting, while introducing a minimum of change into the system and providing complete compatibility for existing IPv4 applications.

There are additional recommendations to access more advanced features like raw sockets or header configuration<sup>28</sup>.

However, in other applications not only communication blocks also but other modules or application parts, include dependencies on IP addresses and must be reviewed deeply. All these dependencies can be grouped in one of the following subjects:

- Parsing IP addresses;
- Use of special IP addresses;
- Local IP address selection;
- Application Data Unit (ADU) fragmentation;
- Use of IP addresses to identify application elements.

### Parsing IP addresses

Many applications require an IP address as an argument to establish a new connection to this address, for example using the peer-to-peer model one peer needs to know the IP address or the hostname where the remote peer is running.

The use of a Fully Qualified Domain Name (FQDN) instead of an IP address is preferable since nodes can change their addresses and this process should be transparent to applications. Applications can store and use a FQDN, delegating the resolution of the IP addresses to the name resolution system, which will return the associated IP address at the moment of the query (subject to DNS caching timeouts).

<sup>23</sup> LONG Lab, “Over Next Generation Networks”, IST-1999-20393, <http://www.ist-long.com/>

<sup>24</sup> T.P. de Miguel, E. Castro, “Programming Guidelines on Transition to IPv6. North American IPv6 Task Force (NAV6TF)”, January 2003, [http://www.nav6tf.org/slides/trans\\_ipv6\\_v013.pdf](http://www.nav6tf.org/slides/trans_ipv6_v013.pdf)

<sup>25</sup> E. Castro, T.P. de Miguel, “Guid. for migration of collab. appl.”, LONG D3.2\_v2, July 15 2002.

<sup>26</sup> “Isabel CSCW Application”, <http://isabel.dit.upm.es>

<sup>27</sup> T.P. de Miguel et al., “Isabel—Experimental Distributed Cooperative Work Application over broadband Networks”, Springer-Verlag, vol. LNCS 868, pp. 353-362, September 1994.

<sup>28</sup> W. Stevens, M. Thomas, “Advanced sockets API for IPv6”, RFC2292, February 1998.

# Moving to IPv6 in Europe

From the application's point of view, name resolution is a system-independent process. Applications call functions in a system library to access it. Developers should change the use of the IPv4 resolution functions to the new IPv6 —the protocol-independent— ones wherever possible.

Typically, applications do not need to know the version of IP they are using, hence applications should only try to establish communications using each address returned by the name resolver until one of them works. However, applications could have a different behaviour when using IPv4, IPv6, IPv4-compatible-IPv6 or IPv4-mapped addresses. Rapid failover is also desirable, e.g. so that an IPv4 connection is promptly fallen back to if the IPv6 connection fails.

Sometimes applications accept IP addresses and include parsers to translate from textual to binary form and validate inputs. IP address parsers must be modified in order to include the new IPv6 string address format.

IPv4 addresses are represented using dotted quad format, each decimal integer represents one octet of the 4-octet address, a value between 0 and 255; for instance 138.4.2.10. The written length of the IPv4 address string varies between 7 and 15 bytes. IPv6 addresses are represented using hexadecimal notation which can be abbreviated, requiring between 3 and 39 bytes; for instance 2001:720:1500:1::a100. So, IPv4 uses dot (".") to separate octets and IPv6 uses colon (":") to separate each pair of octets. Application address parser code should be reviewed to be in conformance with the IPv6 address representation.

There could be an ambiguity with the colon character. The colon character is used in the IPv6 addresses as a separator between each pair of address octets. However, it is used as a separator between the address and the service port number in IPv4 networks. Applications can use the same format as the literal IPv6 addresses in URLs, enclosing the IPv6 address within square brackets, to solve the ambiguity<sup>29</sup>, for instance: *http://[2001:720:1500:1::a100]:80/index.html*.

## Use of special addresses

There are some special addresses, which some applications use in certain circumstances. The most frequent is the localhost interface. Although it is possible to use the symbolic name, most IPv4 applications use the IP address.

Symbolic name	IPv4 address	IPv6 address
INADDR_ANY	0.0.0.0	::
IN6ADDR_ANY_INIT	0.0.0.0	::
INADDR_LOOPBACK	127.0.0.1	:::1
IN6ADDR_LOOPBACK_INIT	127.0.0.1	:::1
INADDR_BROADCAST	255.255.255.255	Does not exist

## Local IP address selection

IPv6 allows many IP addresses per network interface. These may have different scope (link-local, site-local or global). Hence, there should be mechanisms to select which source and destination addresses applications should use in order to know the behaviour of the systems.

Normally, the name resolution functions return a list of valid addresses for a specific FQDN. Applications should iterate this list to select the address to be used in the communication channel. Source address selection is a critical operation that gives information to the receiver about the address to send the reply to. If the selection is not appropriate, the backward path could be different from forward path, even if the addresses are administratively scoped, the reply may be lost and communication between applications will fail.

When choosing source address, some applications use unspecific addresses to let the OS kernel make this selection, named default address selection. When choosing destination address, some criteria could be used to

<sup>29</sup> R. Hinden, S. Deering, "IPv6 addressing architecture", RFC2373, 1998.

# Impact of IPv6 on Applications and Services

prefer one address based on the pair of source/destination values. The default address selection algorithm returns a preferred address from a set of candidates, based on a policy to make the best choice<sup>30</sup>.

There is currently quite a strong movement within the IETF to consider deprecation of IPv6 site-local addresses, to reduce application complexity, and the problems of site-local address ambiguity and address leakage. However, site locals also provide a useful function for disconnected and intermittently connected networks. It is expected that some resolution will be reached soon. There is currently very little use of site-local addressing in IST IPv6 projects (site-local addresses require additional configuration to exist alongside link-local and other scope addresses).

## ADU fragmentation

An application Data Unit (ADU) is the block of data sent or received in a single communication operation at the application level. Sometimes the ADU is different from the amount of data that can be handled on the network interface; the Transfer Unit (TU) and therefore the ADU is fragmented.

The problem is how to select the most adequate TU size. Bigger packets are transmitted more efficiently, as the application overhead of the end systems is reduced. On the other hand, longer packets tend to increase transit delays because of the intermediate relaying process, which is not good in real time applications. The size of the TUs is directly related to the maximum size of the IP packet used over a network (PMTU, Path Maximum Transmission Unit) and the IP fragmentation process. Then, longer packets are likely to be fragmented to adapt the packet size to the link layer.

Since IPv6 fragmentation is an end-system specific algorithm, IPv6 recommends<sup>31</sup> that all IPv6 nodes should implement PMTU Discovery (PMTU-D) to optimize the throughput of fragmented ADUs. PMTU-D is a mechanism to use the longest IPv6 packet size that fits the IPv6 minimum MTU through all the networks traversed, increasing the efficiency of transmission and guaranteeing that the IPv6 packets can travel through all networks unfragmented to reach the destination. If a packet is too large for a router to forward on to a particular link, the router must send an ICMP message to the source address; the source host then adjusts the packet size based on the ICMP message.

Unfortunately, PMTU-D is only a recommendation not a mandatory network module. There are applications, which include their own packetisation process. If PMTU discovery is not working properly, data will not reach its destination. In this situation, applications must implement their own mechanisms to detect black hole problems and send smaller packets, or use the minimum supported MTU for IPv6; 1280 octet packets.

## Use of IP addresses to identify elements

One of the most popular ways to register remote nodes in a collaborative system is based on using the IP addresses as keys for searching in a registry system. Group communication is often related to a group membership concept based on a participant registry system.

The registry system provides an identification method to allow connections from different remote participants to a session. The problem is that an IP address cannot be used to identify a peer node since IP addresses can change over time, for instance after a renumbering process, or due to use of RFC3041 (IPv6 privacy extensions). Renumbering should be an infrequent event, but sometimes it will happen and it should as far as possible be a transparent process for applications.

The best solution to this problem is the use of identifiers independent of the network layer or maybe the FQDN. The FQDN remains invariable over the time although its associated IP address(es) can change.

<sup>30</sup> R. Draves, "Default address selection for IPv6", <http://www.ietf.org/internet-drafts/draft-ietf-ipv6-default-addr-select-09.txt>, August 2002.

<sup>31</sup> J. McCann *et al*, "Path MTU discovery for IPv6", RFC1981, August 1996.



# Moving to IPv6 in Europe

## 4.2. IPv6 Wireless Internet Initiative: Medical Application Scenarios

### 4.2.1. 6WINIT Project

Targeting the promotion of IPv6-related mobility and wireless—including 2.5 and 3G— infrastructures in and for the European and international Internet, 6WINIT has chosen three medical application scenarios as one of its major demonstration vehicles. These scenarios have been supported by a whole range of test-beds, network technology elements and generic applications provided within the project. This latter set did comprise dual stack routers supporting Mobile IPv6 and related transition mechanisms, Road Warrior functionality via IPsec/IKE, active network components and relays for media and protocol conversion, the provisioning of protocol stacks and Java support for e.g. handhelds, multi-access enhanced MIPv6, location support, video streaming, etc. 6WINIT's achievements have been demonstrated at the INET and IST conferences 2001 and 2002 and, using GPRS and UMTS in on-site audits in BTexact's and Ericsson's test-bed in 2002 and 2003 respectively. 6WINIT deliverables are publicly available at <http://www.cs.ucl.ac.uk/research/6winit/>

In the following we are going to describe the three medical application scenarios with special emphasis on IPv6 aspects.

Supported by “technology providers”, the 6WINIT medical scenarios are developed in co-operation with and by 6WINIT partners from Whittington Hospital, London, UK, the John Paul II Hospital, Krakow, Poland and the Universitätsklinikum of the Eberhard-Karls University, Tübingen, Germany. In addition to their obvious value as medical ones these application scenarios are equally highly generic and could serve as template for a large class of other application—to be made possible in an IPv6 context.

### 4.2.2. The Whittington Hospital Scenario

The Whittington Hospital Scenario addresses the routine and emergency access from paradigmatic “locations” to the patient's medical standard records maintained in the hospital database. Such access “locations” or “situations” do include:

- The roadside emergency access to patient's medical summary;
- The Hospital outpatient access to patient's medical summary;
- The patient access to their medical summary and personal health diary;
- The hospital outpatient access to cardiovascular applications;
- The ward (bedside) access to cardiovascular applications;
- The access to cardiovascular applications from a patient's home, and;
- The hospital outpatient access to cardiovascular investigation results.

In 6WINIT, this amazingly large scenario set was demonstrated in a test-bed as shown in the following figure—the Road Warrior-secured emergency access even from Washington to London on the occasion of INET 2002.

The Figure 12 also shows many of the IPv6-related technology elements mentioned in the introduction as present in the Whittington Hospital Scenario: IPv6-enabled Application—and Web-Server in a Java environment, a dual-stack Router providing firewalling and the Road Warrior VPN securing the remote access e.g. from remote in an emergency together with an IPv6-enabled PKI, protocol translation to the legacy database of the hospital, and access via GPRS from BT's lab.

Why IPv6? The Whittington Hospital Scenario supports at least the following pro-IPv6 arguments: Using mainly handhelds deployed at large scale as end-systems and possibly extended from its present nomadic orientation to full mobility—this scenario supports the “large address space”— and “fully routable Internet address” argument. Additionally it can be argued, that for “Mobility and Security” IPv6 is the way to go.

# Impact of IPv6 on Applications and Services

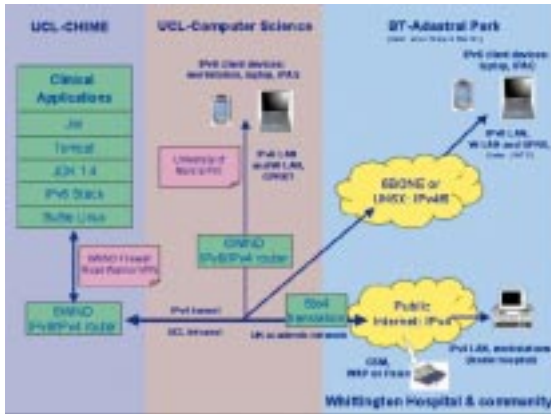


Figure 12: The Whittington Hospital Scenario



## 4.2.3. The John Paul II Hospital Scenario

The John Paul II Hospital addresses the following applications:

- Mobile multi-access to Clinical Appointment System (CAS);
- Hospital Appointment Clerks' access to CAS;
- Inter-wards hospital intranet access to CAS;
- Hospital intranet access to the NetRAAD medical radiology database system;
- Mobile emergency multi-access to the NetRAAD medical radiology database system;
- Konsul: operating theatre access to results of advanced medical examinations (angiography films).

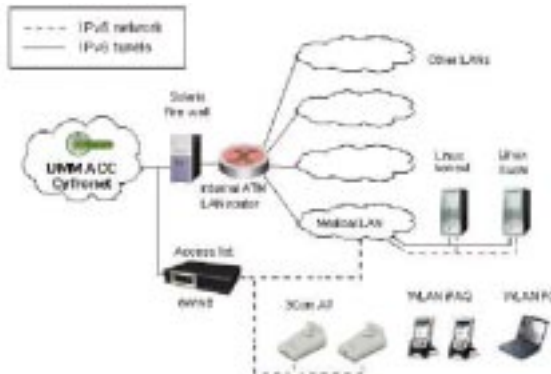


Figure 13: The John Paul II Hospital Scenario

The scenario proposes the idea of multi-access to networks of different capabilities —e.g. coverage versus capacity— mainly in the context of advanced medical picture transmission e.g. in radiology. The figure above and the following figure are showing the related network infrastructure and an iPAQ-based DICOM viewer.

# Moving to IPv6 in Europe



Figure 14: Animation of multi-frame DICOM images (movies) in the UMM's Java DICOM viewer

Why IPv6? The Krakow scenario supports the same pro-IPv6 arguments as the initial scenario.

## 4.2.4. The Tübingen Guardian Angel System - GANS

Conceived in the context of the Tübingen high-fidelity patient simulator centre, the Guardian Angel System provides support (by the "angel") in real-life emergency situations to stressed and possibly error-prone professionals or paramedics. In 6WINIT, the Guardian Angel concept was mapped to an Ambulance-to-Hospital situation: Vital data and video transmission to the hospital plus bi-directional audio between ambulance and hospital would allow for optimal advice to the ambulance and preparation of treatment in the hospital. Different from the two scenarios above, GANS requires more upstream than down-stream transmission capacity.

In 6WINIT, it was also assumed that the ambulance would encounter typical multi-access situations: While maintaining "guaranteed" connectivity via GPRS or UMTS for audio and vital data, the ambulance would simultaneously exploit every WLAN hotspot which might become available to improve video quality.

The following figure is showing the Final Audit demonstration, Stockholm January 2003, using Ericsson's UMTS test-bed and Ericsson's Multi-Access enhancement to Mobile IPv6. SIP controlled audio was transmitted using the IPv6/v4 and transcoding gateway from TZI Bremen.

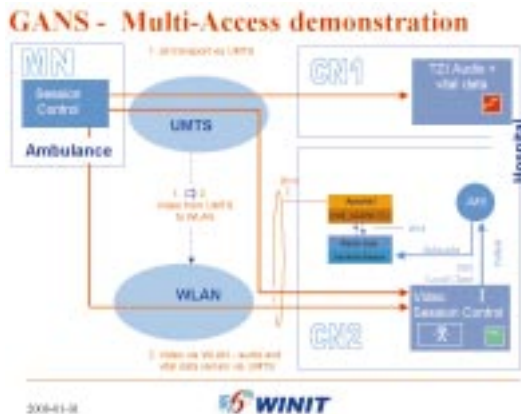


Figure 15: GANS demonstration using Ericsson's UMTS test-bed and Multi-access enhancement to Mobile IPv6

# Impact of IPv6 on Applications and Services

A typical screen as seen by the Guardian Angel is shown in the last picture from the INET 2002 Washington —to— Tübingen demonstration.



Figure 16: A “Guardian Angel Centre” at INET 2002 supporting an “ambulance” in Tübingen



Why Mobile IPv6? The demonstrated GANS scenario is one of the typical “car on the move” applications. While the single one could be possibly realized in IPv4, it is now accepted by important car manufacturers that the totality of car relevant applications definitely requires IPv6.

## 4.3. eMobile Test-bed for Interoperability of Test-beds in eLogistics

In the framework of the IST Project xMOTION (eMobile test-bed for interoperability of networks in eLogistics) different applications for 2.5 and 3G mobile communication networks and services are developed, demonstrated and evaluated in three different application areas. In each area a demonstrator is set up.

The application areas are Emergency Management, Transport Surveillance and Teleambulance. With the Emergency Management demonstrator improved communications for fire engines and fire attack teams are trialled and evaluated. The second trial, transport surveillance, is addressing the surveillance of armoured cars. The third trial, Teleambulance, establishes a communication link between the hospital, e.g. the intensive care unit, and the paramedics either at the emergency location or in the ambulance itself. Therefore two different scenarios are trialled. The first is the “emergency case” and the second is the “patient transport” scenario.

The communication networks used in all three trials range from GPRS to WLAN and UMTS. xMOTION is one of the first users of the T-Mobile UMTS test-bed in Bremen, Germany. UMTS trials are planned to start within the second quarter of this year.

For all three trials a common system architecture has been developed, which consists of:

- A stationary system in the headquarters, e.g. hospital;
- A vehicle mounted system, e.g. in the ambulance, and;
- Optionally a portable system, which is e.g. taken to the emergency location.

This generic architecture is implemented in total or partially for all three demonstrators. Synergies in developing and integrating the three different demonstrators are used wherever possible, e.g. video coding technology, security, Mobile IP and inter-system (vertical) handovers.

Unfortunately the critical communication networks utilised in the xMOTION project, UMTS and GPRS, are in their most recent implementations based on IPv4. As the throughput is already at the minimum, which is acceptable for the application and the access to the networks, IPv4 is used in the first and second implementation and trial phase. However the usage of IPv4 has a considerable impact on the usage of Mobile IP.

# Moving to IPv6 in Europe

As NAT is commonly used in IPv4 and GPRS as well as first generation UMTS networks combined with firewalls, workarounds for applying Mobile IP have to be implemented.

This is one of the major reasons, why in addition to the application device, which is PC hosting the applications and interface e.g. to medical devices, a Communication Gateway is implemented providing and managing access seamlessly to different communication networks.

Applying IPv6 in the future will decrease complexity for Mobile IP implementation. Therefore the feasibility of using IPv6 is investigated for phase 3 of the xMOTION trials.

## 4.4. IPv6 UMU-PKI Security Service

Generally speaking, a public key infrastructure (PKI) is a set of hardware, software, people, and procedures needed to create, manage, store, distribute, and revoke public key certificates. With these in place, a PKI can provide trusted and efficient private-key and public-key certificate management, thus enabling the use of authentication, nonrepudiation, and confidential security services. To provide such services, a PKI uses its base components, which include a certification authority, at least one registration authority, and a directory server. Some PKIs use extra components, depending on what services their particular implementations offer.

The Euro6IX project's primary objective is to support the fast introduction of IPv6 in Europe by advancing research on the issues of network design and deployment, advanced services, and development and porting of user-validated services and applications.

Within these services, security, especially a security infrastructure based on the PKI concept, represents a major interest. The objective of having a PKI supporting IPv6 is to provide a trust point (or basic security framework) for the deployment of new security services over IPv6, as it is the case of IPsec-based VPNs, Security Policy Management or AAAv6.

The UMU-PKI is based on the design and later implementation of a robust group of certification services, has been ported within Euro6IX project to support IPv6. It lets end users perform a whole set of operations from a Web browser: requesting, renewing, or revoking a certificate, looking for another user's certificate, and so on. It also allows the use of smartcards to store cryptographic information, which gives users greater mobility and increases the whole system's level of security. The UMU-PKI's most innovative characteristics are that it:

- Supports the definition of a certification policy to establish restrictions needed inside an organization regarding security; this policy is defined by the administrator and is applicable to every PKI component—registration authority, certification authority, request server, and so on;
- Is completely developed in Java, allowing implementations of the PKI to run on any operating system;
- Is based on the drafts and standards specified by the IETF's PKIX working group;
- Supports the simple certificate enrolment protocol (SCEP), enabling router-certificate requests;
- Supports the online certificate status protocol (OCSP), and;
- Implements time stamping in the system.

### 4.4.1. Porting the UMU-PKI to IPv6

Why port an application-level service such as a PKI to a network-level protocol such as IPv6? The first reason is to provide direct and native access through an IPv6-only or dual-stack Internet to all the PKI's services. Final entities—both users and processes—use these services to generate and manage their cryptographic information. IPv6 seems to be one of the scientific community's best answers to the challenges presented by the Internet's continuous growth, which requires architectures to evolve to accommodate new technologies that support an increasing numbers of users, applications, and services.

The second reason is to enable and promote security-related services and applications in an IPv6-only or dual-stack network. Virtual private networks, secure Web servers, and AAA (authentication, authorization, and accounting) services, which are common in communication architectures and distributed application environments, use public key information to protect communications. Therefore, they benefit in efficiency and scalability with the use of IPv6 as the network-layer protocol.

# Impact of IPv6 on Applications and Services

The third reason concerns the services or devices, such as IPv6 virtual private network (VPN) end points, that need their IPv6 addresses to be included in their public X.509 certificates to establish secure communications. Only an IPv6-enabled PKI can generate and manage such certificates.

Finally, we come to the IP security protocol (IPSec), which is mandatory in IPv6 for communication between PKI components, such as the CA and the directory server.

## 4.4.2. Conclusions

A public key infrastructure is a key component for most of the current and future secure communications architectures and distributed application environments. Thus, the process of porting the UMU-PKI to IPv6 is important for the successful deployment of IPv6 as a base component of the future Internet.

Lot of services and applications depend on this basic security framework to be properly deployed. This is the case of secure VPNs or AAAv6, for example, which the Euro6IX consortium is currently working on.

Regarding the UMU-PKI, new services are under design and testing in the Euro6IX network. This is the case of supporting cross certification between different certification authorities, the use of DNSsec as a distributed certificate store, or the management of attribute certificates defining the different role of user or processes inside an organization.

## 4.5. IPv6-Enabled Real-Time Adaptive Applications

IPv6 is going to be one of the key players in future mobile and wireless networks (often known as “beyond 3G” or 4G wireless networks). These networks will be formed by a core IPv6 packet-based network to which a plethora of different access networks based on different technologies (including self-organising ad-hoc networks) will attach. IPv6 is a key enabler technology in this scenario in which mostly every device needs a globally routable IP address, and end-to-end (including peer-to-peer) services will be common.

In addition, adaptive applications, another key player for such networks, are characterised by constantly changing network conditions causing packet losses, abrupt bandwidth changes and substantial delay variations. These applications, which are able to adapt their internal settings to the network conditions, can strongly benefit from the use of IPv6 at the network layer because they require tight cooperation with the network layer QoS support that is much better in IPv6. The same problems apply to wired technologies like power line, as demonstrated in the 6POWER<sup>32</sup> IST project. In these concrete network scenarios, we propose the use of adaptive applications, being able to adapt the specific network conditions to guarantee a similar QoS perception, while reducing data-rates. In addition, we think that adaptive applications become much more effective when using new IPv6 features such as the better QoS support, identification of flows using the Flow Label field, etc.

In the remainder of this section we describe the architecture for adaptive applications, we will justify why IPv6 can help very much on improving adaptive applications behaviour and we will show some empirical experiments which have been carried out to test our adaptive approach in a vertical handover between WLAN and UMTS. These trials were performed in the framework of the MIND IST-project<sup>33</sup>.

### 4.5.1. Architecture for Application Adaptation

Quality of Service (QoS) is defined in ITU-T recommendation E.800<sup>34</sup> as the collective effect of service performance, which determines the degree of satisfaction of a user of a service. It is characterized by a combination of service performance factors such as operability, accessibility, retainability and integrity. Placing some additional features in the application layer would allow presenting a better QoS to the user in environments in which traditional solutions would perform badly. The main items in this architecture are in the Figure 17.

<sup>32</sup> “IPv6, QoS & Power Line integration”, 6POWER, <http://www.6power.org>

<sup>33</sup> “Mobile IP-based Network Developments”, IST-MIND project, <http://www.ist-mind.org>

<sup>34</sup> ITU-T Recommendation E.800 (08/94), “Terms and definitions related to quality of service and network performance including dependability”.

# Moving to IPv6 in Europe

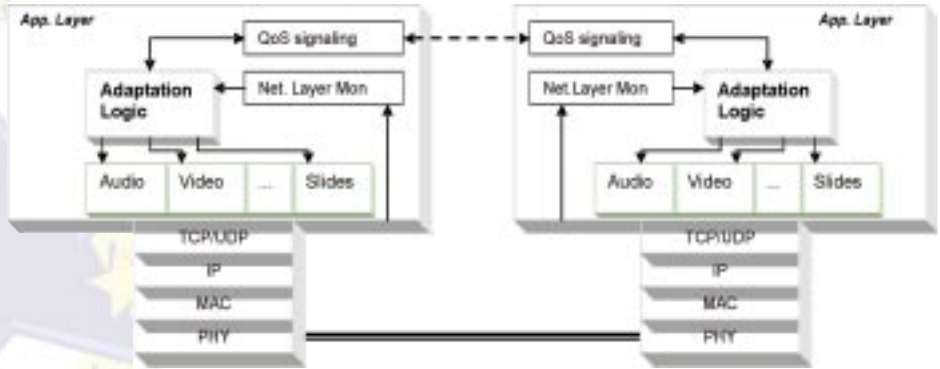


Figure 17: Framework for adaptive applications

The QoS signaling mechanism is the protocol in charge of sending and receiving reports describing the network conditions from the other end. When such a report is received it is passed to the Adaptation Logic as an additional input. Additionally, the Adaptation Logic is in charge of deciding which set of parameters is best suited to the current network conditions, taking into account user's preferences as well.

The QoS signalling is another key point of the adaptation architecture as it is the only feedback that the source has from the other end. It is basically an end-to-end transport mechanism for signalling data; no special protocol is needed. In fact, it may be enough with a TCP/UDP socket in both sides, and even a standard protocol like Session Initiation Protocol (SIP). However, this part of the adaptation can benefit very much from the flow identification functions provided by IPv6.

The problem is that the feedback packets themselves have to traverse the network back to the server, and the probability of it actually making it there on time is inversely proportional to its importance. That is, a feedback packet is most important when it carries information about a congested network and it is not important when it is just saying that all is going well. In our case, the use of the flow\_id to identify these signalling packets and to offer them a better QoS treatment, allow us to keep the applications always informed on the latest network information, preventing such signalling packets from getting lost. In addition, the new advanced QoS features which IPv6 implements, allow adaptive applications to trigger their adaptation only when the network-layer QoS reservations are violated, which clearly optimises the adaptive performance.

All these extensions are being implemented within the ISABELv6<sup>35</sup> application. The most important adaptation capabilities introduced in ISABEL are changes in codecs, sampling rates, component sizes, selection of the components to use, and adaptive buffering.

## 4.5.2. Empirical Results

The scenario shown in Figure 18, combines macromobility, micromobility, vertical handovers and adaptive applications, in a European-wide IPv6 trial. In this integrated scenario (which was used in the final trial in the MIND project<sup>36</sup>), we demonstrated that adaptive applications maintain the user perceived QoS measuring and adapting to the link quality thanks to the IPv6 improved QoS functionalities. The network scenario interconnecting Agora Systems S.A, T-Systems and King's College London is shown in the next page.

<sup>35</sup> "ISABEL CSCW application", <http://www.agora-2000.com/productos/isabel>

<sup>36</sup> MIND Trials final Report, IST-MIND Consortium, Deliverable 6.4, available from <http://www.ist-mind.org>

# Impact of IPv6 on Applications and Services

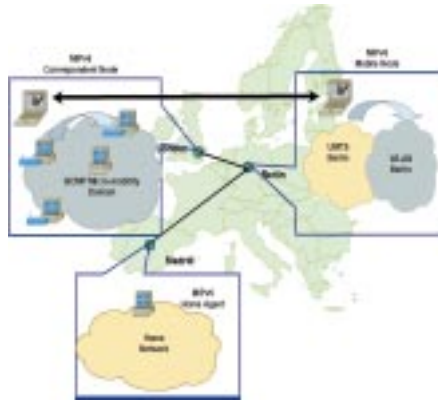


Figure 18: Global Mobility Scenario

The figure below represents the inter-arrival jitter of the packets measured from the London side (packets generated at Berlin). This jitter represents the variation between the expected times of reception of packets, and the actual ones, due to changing delay in the transmission and other factors.

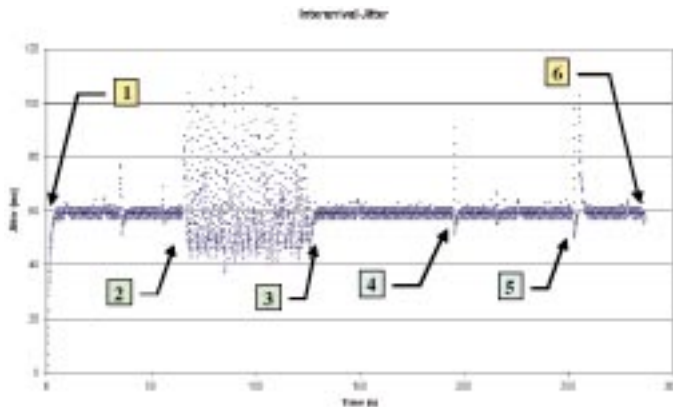


Figure 19: Jitter Experienced at KCL (London)

Figure 20 represents the packet losses measured at the Berlin side, i.e. packets sent from London that did not reach Berlin. As the bandwidth can be considered symmetrical, the graph obtained from data at London site is quite close to that one (as seen in the various experiments). Packet loss is cumulative, so that "flat" portions represent zero-loss zones.

The results are quite straightforward to analyse, because they correspond to each event on the experiment as expected. Some glitches appear from time to time (marked with red circles in Figure 20), but they can be safely disregarded as being caused by the non-guaranteed quality of the link between Berlin and London (it can be seen that they only imply the lost of one or two packets). The first glitch, a major one, (30s) can be associated with the selection of the parameters in each videoconferencing end terminal, and can thus also be disregarded.



# Moving to IPv6 in Europe

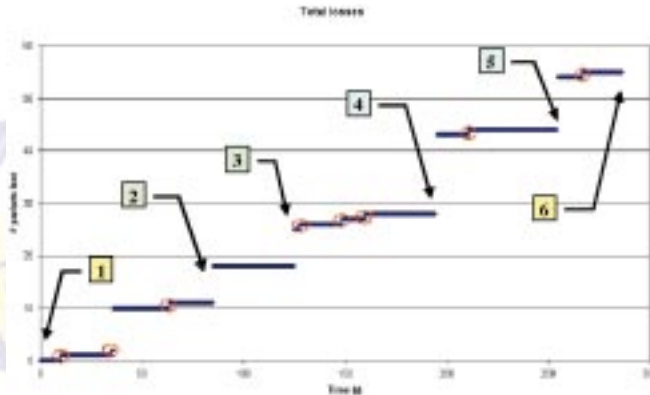


Figure 20: Loss at T-Systems (Berlin)

The figure above demonstrates how in the different phases of the session (1) Connection, (2) Handover WLAN-UMTS, (3) Handover UMTS-WLAN, (4,5) Handovers in micro-mobility BCMP scenario and (6) disconnection, the packet losses are minimal and only during handovers. After handovers, the adaptive applications approach eliminates any packet losses due to the network congestion.

## 4.5.3. Conclusions

Adaptive applications are clearly a hot topic in the wireless and mobile research community, which is so in favour of IPv6 deployment. We have demonstrated that adaptive real-time applications are one of the key applications that might clearly benefit from IPv6 deployment. Such benefit is inherently tied to the great QoS management functions offered by IPv6 as a means to meet the strong QoS requirements that are usually needed by the signalling mechanisms of adaptive applications. IPv6 can make adaptive applications obtain a much higher performance than when utilised in today's networks. It is clear that IPv6-enabled adaptive applications will play a preponderant role in the provision of future QoS-enabled real-time multimedia services in the next generation Internet, and the future Mobile Information Society.



## 5. Research Networks Deployments

### 5.1. Rise and Fall of the 6Bone

#### 5.1.1. Network Growth

Since its creation in 1996 the 6Bone has been steadily growing in the number of connected sites (See Figure 21 and Figure 22). In July 1997 the network encompassed about 150 sites; in October 2002 more than 1200 sites distributed in 59 countries all over the world were officially registered in the 6Bone registry database. Over the same period of time the number of 6Bone backbone sites (i.e. assigned pTLAs) has increased from 36 to 133.

Date	Backbone Sites	All sites
7/2/1997	36	150
12/9/1997	43	203
3/31/1998	45	240
8/25/1998	47	302
12/12/1998	51	332
3/17/1999	55	361
7/17/1999	62	412
1/18/2000	67	505
3/21/2000	67	536
7/5/2000	68	590
12/6/2000	75	688
2/27/2001	82	759
12/10/2001	101	952
7/11/2002	126	1133
10/21/2002	133	1225

Figure 21: Growth of the 6Bone in the Period from 1997 to 2002

# Moving to IPv6 in Europe

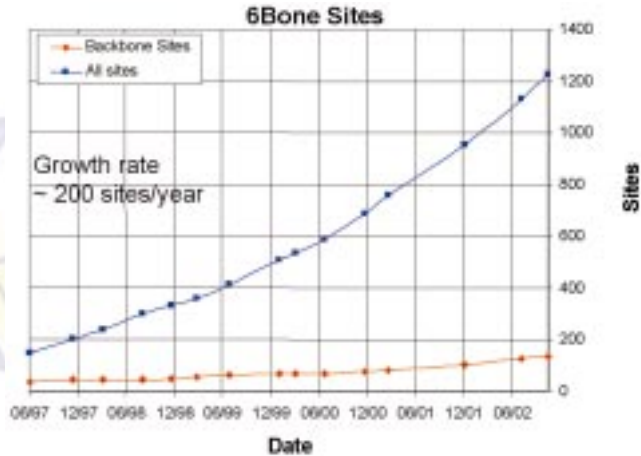


Figure 22: Graphical Representation of 6Bone Growth (Source: 6Bone Registry)

## 5.1.2. 6Bone Phase-out Plan

6Bone routing performance and stability is not always the best (e.g., see the Savola 6Bone-mess I-D), and there is a clear need of a more robust core that can support test-beds.

In early 2002 discussions were started with the RIRs driven by two issues: Clarifying the role the 6Bone address registry has with respect to the RIRs IPv6 address registry and gaining access to the ip6.arpa reverse registry.

During the course of early discussions, the RIRs' management made it clear that they could not speak to the issue of how long the 6Bone allocation authority would last. Rather, it was an issue that the IETF and/or the IANA would have to deal with. To this end, a discussion was opened within the IETF on 6Bone phase-out planning.

Also there was the issue of the 6Bone operation. Even though the 6Bone came under the IETF ngtrans wg, it really had almost nothing to do with its operational policies. The 6bone community itself controls its policies and everyone expects that it will continue to do so.

Many comments came from the 6Bone community, but most relevant ones focus on having to pay for test-bed addressing when they haven't had to pay in the past. Note that many 6Bone participants (at all levels) do so to get experience and in the process convince their organizations that there is something worth paying for, i.e., the price is an issue, no matter how small it is.

There was concern about having to go through more complexity. It isn't clear if this is a real issue as we don't know what a pTLA-level request process might be with the RIRs. This may be a holdover of dislike of necessary procedures for scarce IPv4 address space.

Another concern is what is pay for service when the 6Bone is a volunteer effort... RIR services aren't needed. There is unwillingness to pay for service and then be expected to hand our free address services to downstream users.

Many comments have come from the RIR community as well: "...why should the 6Bone community get cheaper services than the dues paying members?".

Also, the RIRs are supposed to recover costs for providing their services. Giving away any service would seem to go against this. A corollary to the above is, if the RIRs are just covering costs for a special service to the 6Bone, what are the RIRs doing for their regular customers. The feeling seemed to be, why should RIR members care about the 6Bone? Let 6Bone do their thing, and the RIRs theirs.

It isn't clear this proposal should proceed, given the opinions expressed on both sides, a soon to be in place 6Bone phase-out plan, a decline in the request rate for 6Bone prefixes, and a steady increase in allocated production prefixes.

Also, there is now the ability for the RIRs to temporarily allocate IPv6 addresses for Internet experiments.

As for `e.f.f.3.ip6.arpa` support, Bob Fink has proposed that the 6Bone operate the servers for this themselves, which would mean that the 6Bone community would sustain the cost of entering and maintaining the pTLA data in the `e.f.f.3.ip6.arpa` server, and that when phase-out is complete, the RIRs simply pull the `eff3.ip6.arpa` delegation and they have reclaimed it.

The RIRs have agreed that in light of the foregoing that there is no need to continue planning for a 6Bone RIR integration, and that the 6Bone would continue to manage its own allocations throughout the life of the phase-out plan.

The RIRs will delegate `e.f.f.3.ip6.arpa` to name servers that the 6Bone community provides.

Bob Hinden then presented the 6bone phase-out plan I-D, under the subtitle "be careful what you start". RFC2471 says 6Bone addresses would be temporary addresses that would be reclaimed in the future (with implied renumbering for sites using 6Bone addresses). The RIRs have been allocating production SubTLAs since 1999.

In 2002 more production allocations were made than 6Bone ones. The v6ops WG replaced ngrtrans, which used to oversee the 6Bone, but the 6Bone is not in the v6ops WG Charter.

The current plan outlined in the *draft-fink-6bone-phaseout-04.txt* is to allocate 6Bone addresses until January 1, 2004, and for these to remain valid until June 6th 2006, after which no 6Bone prefixes should be carried on the Internet. The plan obsoletes RFC2471 that will become historic. It is up to IPv6 address holders to gain new address space, of whatever prefix length is appropriate (some pTLA holders may only require a site prefix, for example). In addition, IANA must not reallocate `3ffe::/16` for at least two years to avoid confusion with new allocations.

All these decisions were taken, finally, in the IETF-56, 6Bone BOF, chaired by Jordi Palet, from Euro6IX. Minutes available at <http://www.ietf.org/proceedings/03mar/minutes/6bone.htm>.

## 5.1.3. Conclusion

After years of work within the IETF, the standardization of IPv6 and the related components is coming to an end. Although at the same time the existing IPv4-based technology has been enhanced to partially cope with the problem of IP addressing space depletion as well as with the growing demand for new services like security, mobility and QoS, this has not removed but just delayed the need for a new network protocol as a long-term solution. In fact, it is quite clear that no low cost IPv4 patches will ever be able to guarantee the end-to-end network transparency and the huge amount of globally unique IP addresses required by the Internet evolution (e.g. the future xDSL or wireless data services based on the always-on paradigm). This is the real strong reason for deploying IPv6 within the Internet.

This is why most of major Internet ISPs are already looking with great attention at IPv6 and have been involved in the experimentation of the new protocol within the 6Bone for years now. Their contribution, together with the increasing effort coming from manufactures, universities and research centers from all over the world, is making the experimental IPv6 Internet growing fast. Nowadays, more than an environment to test IPv6 implementations, debug vendor equipment and make practice with it, the 6Bone and the ISP trials look like the down of the transition process.

Nevertheless, it is important to note that some other issues still need to be solved before a large-scale deployment of IPv6 within the Internet can take place. The 6Bone experience shows that multi-homing is still a problem, given that many of the un-aggregated IPv6 prefixes advertised within the BGP4+ cloud are due to lack of an alternative to the current inefficient IPv4 practice. Moreover, also the renumbering issue is worth further investigation and standardization effort.

Finally, to make IPv6 attractive for the users, and particularly for the new users who may foster the world-wide adoption of IPv6 by choosing the IPv6 only transition scenario, a suitable range of IPv6 applications must

# Moving to IPv6 in Europe

be available, starting from the basic services typical of the present Internet and Intranet environments. The present lack of such application services clearly indicates that the application developers and manufacturers will have a key role in breeding the transition process and making the new IPv6 Internet really happen.

## 5.2. 6NET: Large-Scale International IPv6 Pilot Network

### 5.2.1. Introduction

6NET is a three-year European project to demonstrate that continued growth of the Internet can be met using new IPv6 technology. It also aims to help European research and industry play a leading role in defining and developing the next generation of networking technologies.

The project has built a native IPv6-based network with both static and mobile components in order to gain experience of IPv6 deployment and transition from existing IPv4-based networks. This has been used to extensively test a variety of new IPv6 services and applications, as well as interoperability with legacy applications.

### 5.2.2. Network Design

The network architecture is based on Packet over Sonet technology, with a meshed international network in a single management domain that interconnects national IPv6 test-bed networks via a single access router. This meshed topology provides resilience against failure of individual links and allows the 6NET partners to have access to the 6NET core network in a native IPv6 technology.

A diagram below shows the current 6NET core network topology in May 2003. All trunk circuits inside the core are POS STM1/OC3 - 155 Mbps speed. Most of the access circuits are also STM1/OC3 - 155 Mbps speed except to SURFnet - double Gigabit Ethernet, NORDUnet - POS STM16/OC48 - 2.5 Gbps and NTT - E1 link. Only two tunnelled access links have been established for connecting the Greek and Polish networks.

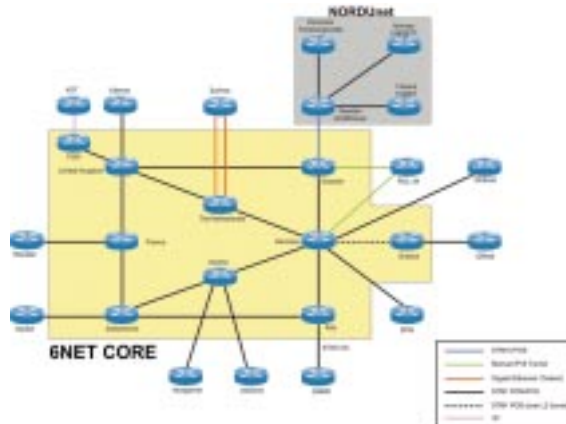


Figure 23: 6NET Core Network

### IGP

The ISIS routing protocol is used as IGP inside the core network because it was the only IGP with IPv6 support available at design time. Since the bandwidth in trunk circuits is the same, ISIS metrics are based on delay times between physically connected routers allowing a faster transmission on one hand and on the other hand to avoid equal cost routing paths for easier troubleshooting.

## Routing policy

6NET policy accepts all routes coming from NRENs (National Research and Education Networks) and exports them to the rest of the 6NET partners. 6NET BGP routes are tagged based on an NREN prefix-list giving the tag 6NET-nren (6680:10) to routes belonging to NRENs and 6NET-others (6680:99) to other routes. This tagging policy permits NRENs to build their routing policies in their IPv6 networks based on this tagging.

## Addressing plan

The 6NET network design explicitly supports native IPv6 allowing all partners to connect to the core natively. DANTE has divided an IPv6 subTLA from GÉANT address space for 6NET and GÉANT IPv6 use. The sTLA assigned to DANTE is 2001:798::/32 of which 2001:798::/40 has been allocated for 6NET. The 6NET address space has been divided into logical portions to summarize the addressing in a simple way. Each national research IPv6 network uses their own sTLA allocated by RIPE.

For management and monitoring purposes the 6NET core routers are reachable in IPv4 via GÉANT. All 6NET routers have got an IPv4 address on their management port allocated from GÉANT IPv4 address space.

### 5.2.3. Network Monitoring and Management

The management of the 6NET network is done over IPv4 via the management port in order to be reachable by the 6NET NOC and also to use the GÉANT workstations for IPv6 monitoring. It is also possible to manage the network over IPv6 but most of the MIBs are currently defined only for IPv4.

There are several monitoring tools available for the 6NET network. Tools such as a looking glass facility —to have configuration snapshots or a network “weather map”— a geographical map of the network that presents the current IPv6 traffic usage —have been developed by 6NET partners to manage and monitor the 6NET network at every moment.

Intermapper network monitoring and alerting tool is used to monitor the network state. It provides a real-time view of traffic flows through and between critical networks, routers and links. It also provides a viewing of the state of the 6NET network. It also has utilisation statistics that show traffic, errors and outage information that help in troubleshooting the problems that may occur.

## 5.3. Euro6IX: Pan-European IPv6 Internet Exchanges Backbone<sup>37</sup>

### 5.3.1. Introduction

Euro6IX is the largest research project currently funded by the European IST Programme, with a duration of 3 years. The goal of the Euro6IX project is to support the rapid introduction of IPv6 in Europe. Towards this target, the project has defined a work plan. This describes the Pan-European network design (native IPv6), network deployment, research on advanced network services, development of applications (that will be validated through the involvement of user groups and international trials), and active dissemination activities, including events and conferences, contributions to standards (IETF and RIPE among others), publication of papers and active promotion of all the publicly available project results through the project web site.

### 5.3.2. Network Design

The project is researching, designing and deploying a native Pan-European IPv6 network, called the Euro6IX testbed. It includes the most advanced services obtainable from present technology and follows the architecture of the current Internet (based on IPv4). It considers all the levels needed for the worldwide deployment of the next generation Internet. The infrastructure of Euro6IX consist of the following different network levels:

- IX-level: Regional native IPv6 exchanges;
- Backbone-level: Pan-European core network that interconnects the regional exchanges and creates the highest level in the network hierarchy;

<sup>37</sup> Text extracted from several Euro6IX deliverables. See <http://www.euro6ix.org> for the complete documents.

# Moving to IPv6 in Europe

- Node-level: Service providers, ISPs and other providers accessing the core network to provide IPv6 services and end user access. The users are connected by means of a variety of access technologies, including legacy IPv4 networks and services whenever no IPv6 native links are available or feasible. This level includes a set of academic, research and non-commercial trial users who will use native IPv6 services and generate IPv6 native traffic.

The backbone is constructed from 34 Mbps links, while the users are connected mainly by 8 Mbps links. Most of the links, including the backbone, have been sponsored by the telecommunications operators related to some of the project partners.



Figure 24: Euro6IX Network

## Study of IX Models

One of the goals of the Euro6IX project is to analyse the different Internet Exchange models that can be adopted inside the Euro6IX network to better understand their main features and the reciprocal advantages.

In order to make a more detailed analysis, three different models (from now on called Model A, Model B and Model C) have been considered and analysed. We started just from the classical model of the IX, described in detail in the following section, consisting of a simple switched architecture where the ISP's routers are connected. Then we considered newer models, where the IX itself can assign the addresses and the IX user can change ISP without any change in the addressing plan, described in the Model B and Model C sections below.

However, inside the Euro6IX network, model A won't be implemented because it does not introduce any new features. It has been taken into account in this document because it could be interesting to compare it with the other models that will be implemented. In particular, it could be interesting to compare the different routing frameworks and the adopted addressing policies to better understand the improvements and the advantages of the new models with reference to this well-known model.

- *Model A*: The IX Model A, here described, can be considered as the traditional model of an Internet Exchange and by now it is the model most widely adopted in the Internet IPv4 community. The Figure 25 shows its internal architecture.

In this case, the IX is an "interconnection point" where the ISPs come together in order to exchange traffic between each other according to some defined routing policies.

Normally, inside the IX building, there is a layer 2 section (the dotted area that represents the neutral part of this IX model) consisting of a set of switches where the routers (belonging to the ISPs) are connected. The routing policy is normally quite simple: Each ISP inside the IX belongs to a particular Autonomous System. The routers exchange routing information using the eBGP protocol and also decide which kind of routing information to filter by implementing routing rules that enable (or disable) the reachability of connected networks. With this model, the IX does not have the capability to assign addresses and normally each ISP accessing the IX has its own internal addressing plan.

# Research Network Deployments

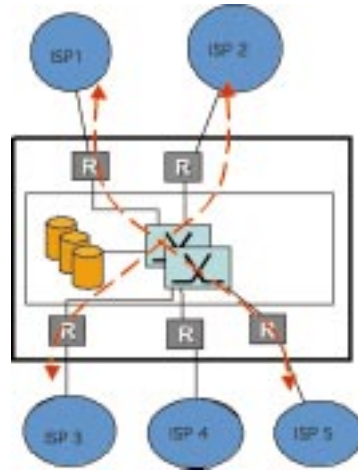


Figure 25: Architecture of IX Model A



- *Model B*

– IX Internal Network Architecture: The Internal Architecture for the IX Model B is shown in Figure 26. This shows the infrastructure necessary to develop full redundancy inside the IX.

The different elements composing the IX Model B are the following:

- Layer 2 Infrastructure (L2) composed of SW1 and SW2, which provides fully redundant physical connectivity inside the IX. There are also several routers (Ra, Rb, Rc and Rd), necessary to establish peerings among the different Telcos and/or ISPs. In this model, this is the neutral area of the Exchange, so it's operated by a neutral organisation.
- Layer 3 Infrastructure (L3), which provides new functionalities to the IX compared with the traditional IX (Model A) and is composed of R1, R2, R3, R4 and optionally the IPv6 Route Server. L3 provides IPv6 connectivity among the equipment. This is the non-neutral area of the IX.
- Application Services: Available because of the Layer 3 capabilities of the IX. These services are, for example:
  - Basic Internet Services: NTP, DNS;
  - Content Delivery Services: HTTP, FTP;
  - Network Access Services: RADIUS;
  - Other services: POP3, SMTP, IRC.
- Monitoring Applications and Statistics Systems. The following one is a list of possible applications:
  - Routing Monitoring: (AS-Path tree);
  - Reachability Monitoring (Ping view);
  - Management Systems (Magalia);
  - Traffic Monitoring (Cricket, MRTG).
- Customers of the IX that can be divided in three main groups:
  - Other national Telcos connected to the Layer 2 IX Infrastructure;
  - Large Customers of the incumbent Telco connected to the Layer 3 IX Infrastructure;
  - Standard Customers connected to the Layer 3 IX Infrastructure through the national backbone of the incumbent Telco.
- Transit Providers, such as connections to the other Euro6IX IXs and connections to external IPv6 Networks (6Bone, 6NET, etc.).



# Moving to IPv6 in Europe

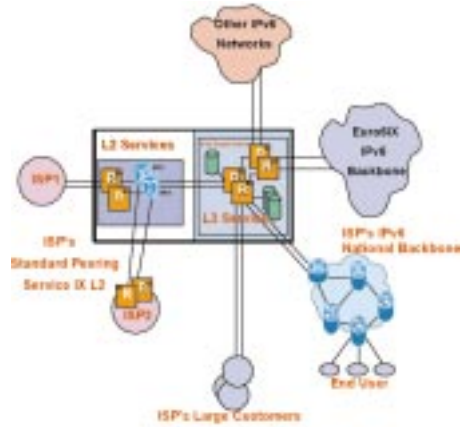


Figure 26: Architecture of IX Model B

– IX Functionality: There are two differentiated areas according to the functionality in the IX Model B.

- a) Layer 2 Infrastructure: The layer 2 infrastructure is based on the concept of the traditional IXs (Model A), where several ISPs present in the same geographical area, and interested in peering agreements, will be connected. This infrastructure is the core of the IX and must be high performance, switched and fully redundant infrastructure, connecting all the equipment in the IX. To provide redundancy, each IX node should consist of two switches supporting local connectivity inside the IX. Routers are used to establish peering between these ISPs.

The interest of a Telco in peering with another one is based on the amount of traffic exchanged between them. If they do not peer in the national IX, all the traffic exchanged between them will flow through their own international links. On the other hand, if they peer in the national IX, traffic will be exchanged there and thus transmission costs could be reduced.

This Layer 2 side must offer neutral services for those customers connected, and must be managed by a neutral organization with clear Statements and Operation Rules. All ISPs interested in being connected to the Layer 2 side must agree and follow these rules that preserve the correct operation of the neutral L2 node.

Finally, the development of the architecture of the IX consists of several stages with regard to the complexity of the infrastructure used:

- The first of these stages is developing the IX with one switch for the layer 2 infrastructure and one link among the equipment.
  - The second stage will consist of improving the equipment of the IX by implementing redundancy, so that two switches should provide connectivity to the various blocks inside the IX.
- b) Layer 3 Infrastructure: Layer 3 infrastructure (L3) provides new added functionalities to the traditional IX. With this topology, the IX works like an IPv6 Network Access Point (NAP) or like an IPv6 Point of Presence (PoP) of the owner. Layer 3 infrastructure consists, basically, of Router Equipment and optional elements, such as an IPv6 Route Server.

The Router Equipment of the IX owner provides IPv6 connectivity within the network inside the IX, as well as establishing peerings with other IXs and other IPv6 networks. Besides, it can provide IPv6 services to new L3 customers.

IPv6 Route Server is the equipment that centralizes the interchange of eBGP routes between the different elements in the IX. All the peers communicate only with the Route Server, instead of creating a dense peering mesh between themselves, thereby saving router resources.

# Research Network Deployments

– Addressing plan: The Addressing plan for the Exchanges and for the whole Euro6IX network is in full conformance with the RFC2374 “An IPv6 Aggregatable Global Unicast Address Format”.

In the commercial phase, is expected that every IX Model B will have a commercial prefix delegated from  $2001::/16$ . The aggregatable address format is designed to support long-haul providers, Exchanges, multiple levels of providers and subscribers, as shown in the following figure.

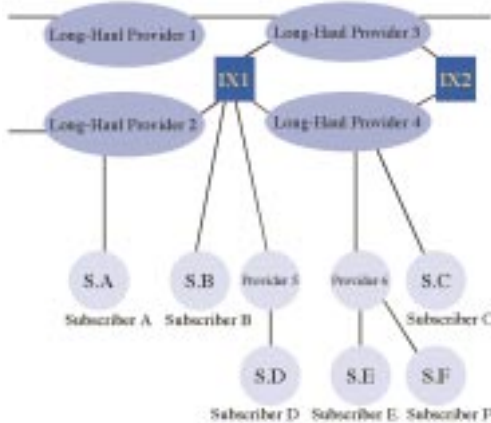


Figure 27: Public Topology Hierarchy

Exchanges will allocate IPv6 addresses. In IX Model B, this condition is fulfilled since the L3 IX is owned by one of the providers. This ISP assigns addresses to its customers delegated from its own  $2001:xxxx::/32$  prefix(es).

Based on RFC2374, a new concept for study and research is that, considering that the delegated addresses belong to the ISP in charge of the IX, organizations that connect to these IXs will achieve addressing independence from long-haul providers. Then, they will be able to change long-haul providers without renumbering their organization. They can also be multihomed via the IX to more than one long-haul provider.

a) Example of Addressing plan (MAD6IX): The Addressing plan for MAD6IX has been made following the above guidelines. The addresses used have been delegated by Telefónica Data, who owns a  $2001:800::/32$  prefix. The whole prefix for all Euro6IX networks connecting to MAD6IX is  $2001:800:40:2000::/52$ , also including point-to-point links and MAD6IX networks.

- Point-to-Point Links: The prefix  $2001:800:2fxy::z/126$  has been used for the point-to-point links. The format for these addresses has been selected to correctly identify them, with the criteria explained below.

MAD6IX and every organization connecting to MAD6IX has been identified with an integer number. Every point-to-point link has the following structure:  $2001:800:40:2fxy::z/126$ .

The fields XY are designed according to the number assigned to the organizations, and in numerical order.

For example, MAD6IX has been assigned the number 0 and TID has been assigned the number 1. So the point-to-point link between MAD6IX and TID will be  $2001:800:40:2f01::/126$ .

The criteria selected for the addressing of each side of the link (field Z) is to use  $::1$  for MAD6IX side and  $::2$  for the other side.

For the point-to-point connections to other IXs, the prefix used has been  $2001:800:40:2exy::z/126$ . Every IX connecting to MAD6IX and MAD6IX has been identified with an integer number. The fields XY are designed according to the number assigned to the IXs, and in numerical order.

# Moving to IPv6 in Europe

MAD6IX has been assigned number 0, LON6IX has been assigned number 2 and LIS6IX has been assigned number 3. The criteria selected for the addressing of each side of the link (field Z) has been to use ::1 for MAD6IX side and ::2 for the other side.

- MAD6IX Attached Networks: For those networks connected to MAD6IX a ::/56 prefix has been delegated from the ::/52 available. So, the prefix delegation is as follows:
  - MAD6IX Services Network: 2001:800:40:2000::/56
  - MAD6IX Management Network: 2001:800:40:2100::/56
  - TID Services Network: 2001:800:40:2200::/56
  - TID Management Network: 2001:800:40:2300::/56
  - TID Customers Network: 2001:800:40:2400::/56
  - Consulintel Network: 2001:800:40:2a00::/56
  - UPM Network: 2001:800:40:2b00::/56
  - UMU Network: 2001:800:40:2c00::/56
  - Vodafone Network: 2001:800:40:2d00::/56

All the above considerations are only suggestions and every IX administrator should choose their own address delegation architecture.

- b) Services and Monitoring: The IX Model B provides a large variety of services to offer to the customers of the Exchanges, due to the added layer 3 functionality. Those application services are:
- Basic Internet Services: Synchronised Time Services (NTP) and Domain Name Service (DNS). These services were traditionally offered by the carrier's national backbones and ISPs, and now they can be delivered directly from the IX.
  - Content Delivery Services: Web Servers (HTTP), File Transfer Protocol Servers (FTP) and Video Streaming Servers. These services were traditionally offered by ISPs. The high demand from customers for these services gives the Exchanges more presence, and demand for these services leads to a requirement for increased performance of the IX carrier's network.
  - Network Access Services: Remote Authentication Dial In User Service (RADIUS). This service, currently offered by carriers and ISPs, can be provided directly by the IX, providing more reliability for ISPs as they connect directly to the Exchange instead of connecting through a national carrier. Moreover, providing RADIUS service at the IX increases the range of potential customers accessing the IX.
  - Other services: Mail Servers (POP3, SMTP) and Internet Relay Chat Servers (IRC). These are value added services that complete the variety of new possibilities of the Layer 3 Exchanges.

Layer 3 capabilities of the IX includes the use of monitoring applications inside the Exchanges such as:

- Routing Monitoring Systems:
    - AS-Path tree (developed by Telecom Italia) that permits controlling the AS-path of BGP4+ routes.
    - Looking Glass that permits executing predefined commands, such as ping or traceroute, over network elements.
  - Reachability Monitoring Systems (Ping view) that provides information about alive and dead machines in the network.
  - Management Systems (Magalia developed by TID) that is a distributed environment for managing and monitoring links and machines of the whole network.
  - Traffic Monitoring Systems (Cricket, MRTG ported to IPv6 by nGn) that provides information and statistics about the traffic flow of the network.
- c) Customers: One of the differences between traditional L2 IXs (Model A) and new L3 IXs (ModelB) is the possibility of offering a wide range of new services to new customers. In traditional IXs, only hosted L2 equipment is offered and the ISP must bring their own router equipment for peering with other ISPs. So, the only customers connecting to L2 IXs were ISPs.

With L3 IXs (Model B) a new set of potential customers appears, adding to the traditional customers of L2 IXs (ISPs). These new customers can be:

# Research Network Deployments

- Large Customers (Corporate Networks of large/world-wide companies). These customers have the suitable infrastructure to connect themselves directly to the Exchanges (avoiding the usage of a national carrier). Layer 3 IX (Model B) brings them the possibility of connecting directly to the IX node.
  - Standard Customers and ISPs connected to the L3 IX through the carrier's IPv6 national backbone. This is the traditional service offered by L2 IX (Model A), and it is also offered with the new L3 IX (Model B).
  - ISPs offer L3 dependent services. They need L3 infrastructure to connect to. With L2 IX (Model A) they need the carrier's national backbone to connect to the Exchanges. With L3 IX (Model B), L3 capabilities are fulfilled inside the IX, so ISPs can connect directly without carrier's backbone dependence.
- *Model C:* The third model that will be investigated inside the Euro6IX network is related to an advanced concept of Internet Exchange (IX) that, assuming an IX as a neutral point of traffic exchange among IP networks (in general Internet Service Providers), takes into consideration the importance of prefix aggregation inside the backbone of the next generation IPv6 Internet. The proposal starts from a suggestion inside RFC2374 "IPv6 Global Unicast Address Format", where, "... the IPv6 aggregatable address format is designed to support long-haul providers (shown as P1, P2, P3, and P4), exchanges (shown as IX), multiple levels of providers (shown at P5 and P6), and Exchanges (unlike current NAPs, FIXes, etc.) will allocate IPv6 addresses. Organizations who connect to these exchanges will also subscribe (directly, indirectly via the exchange, etc.) for long-haul service from one or more long-haul providers. Doing so, they will achieve addressing independence from long-haul transit providers. They will be able to change long-haul providers without having to renumber their organization. They can also be multihomed via the exchange to more than one long-haul provider without having to have address prefixes from each long-haul provider."

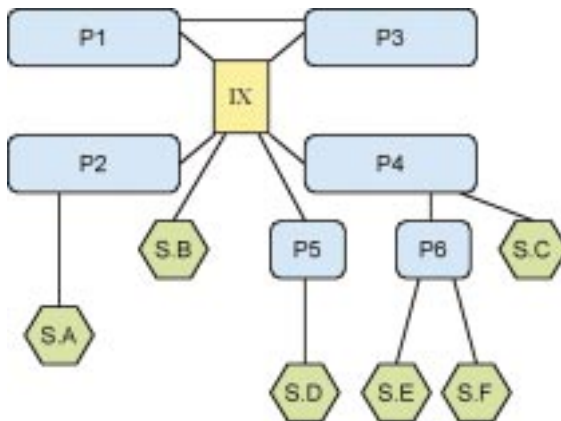


Figure 28: Network Architecture as Shown in RFC2374

It is easy to understand that the current models of Layer 2 based Internet Exchange cannot be considered an optimal solution to reproduce this architecture. In fact, even if it was possible to:

- Configure routing between Exchange Subscribers and Long Haul providers announcing disaggregated prefixes;
- The Long Haul Providers take care to announce to the IPv6 Internet the aggregated IX prefix.

This results in the Internet Exchanges losing the ability to control the routing of its own prefixes.

For this reason, the Euro6IX project is going to study a new functionality inside the architecture of an Internet Exchange: This functionality is called "Layer 3 mediation function".

# Moving to IPv6 in Europe

- Internet Exchanges Architecture: The following figure depicts the proposed model of the IX interconnecting Long Haul Providers and Exchange Subscribers (indicated in the figure as “Next Generation Customers”).

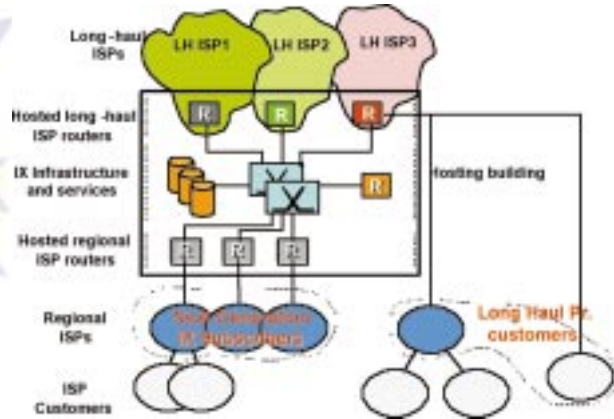


Figure 29: Internet Exchanges Structure

The Layer 3 device on the right side of the Figure performs the “Layer 3 Mediation Function”. It can be just a router (but in this case the IX forwarding performances are influenced by the performance of this router) or can perform only a control function leaving the forwarding to the high speed Layer 2 infrastructure of the Internet Exchange (the exact definition of the “Layer 3 Mediation Function element” will be investigated during the research activities of the Euro6IX project).

As shown in Figure 29 the Internet Exchange is installed inside a building that in general contains:

- The IX equipment (Switches, Layer 3 device performing “L3 Mediation Function”, and management devices such as Route Server, Monitoring Workstation, etc.) shown inside the central dotted area;
  - Routers belonging to the Long Haul Providers (linked to the switched infrastructure);
  - Routers belonging to the Internet Exchanges Customers (linked to the layer 2 switch infrastructure).
- Goals of the Model: As already indicated, this model has been proposed in order to experiment with the new IPv6 IX model defined in RFC2374. This model considers a new concept of IX, which is no longer simply a point where ISPs meet each other and exchange their traffic but can be considered like an entity that assigns IPv6 prefixes that are not dependent on the Long Haul Provider used by the user for the long haul connection. A Long Haul Provider places its own router inside the IX building (outside the dotted area) and uses the high-speed layer 2 connections to connect with its users. This scenario makes easier the renumbering process since if a user wants to change their provider they have only to modify their routing policies while the addresses are always the same because they are assigned by the IX and not by the Long Haul Provider.
  - Routing and Addressing: The model described here basically relies on the idea of considering the Euro6IX backbone, or part of it (at least the router of the Euro6IX network collocated with an IX), like an autonomous entity that can be seen, by the IXs, as one of the providers that they connect to.

In this way, the part of Euro6IX backbone emulating the long haul provider will have an AS number whereas each IX will use its own AS number.

Even if the Euro6IX project doesn't define a common policy for the routing inside the Internet Exchange it is useful to define some guidelines about the routing suggested for the model of IXs with the new Layer 3 Mediation Function. In this model the routing guidelines are shown in Figure 30 and are:

- a) eBGP4+ between layer three mediation function router and backbone routers;
- b) eBGP4+ between layer three mediation function router and Next Generation IX Customers routers;
- c) eBGP4+ between routers belonging to the backbone and Standard IX Customers (accessing IX without using layer 3 mediation service);
- d) eBGP4+ between routers belonging to the backbone and Standard IX Customers (Standard Long Haul Provider Customers);
- e) IGP and iBGP4+ inside the part of Euro6IX backbone emulating the Long Haul provider. IGP needs to be used to guarantee the loop-back interfaces reachability inside the backbone.

The routing inside the overall network depends on which part of the Euro6IX backbone will be used to emulate the long haul provider. In order to guarantee the maximum independence of which model each partner reproduces inside the Euro6IX network and in order to guarantee the stability of the routing, the majority of partners hosting the Internet Exchanges agreed that the Long Haul provider will be emulated only by the router collocated inside the Internet Exchanges. This Long Haul provider will have one or more direct peerings with other providers or other Internet Exchanges.

The routing framework to be adopted is shown in the following diagram:

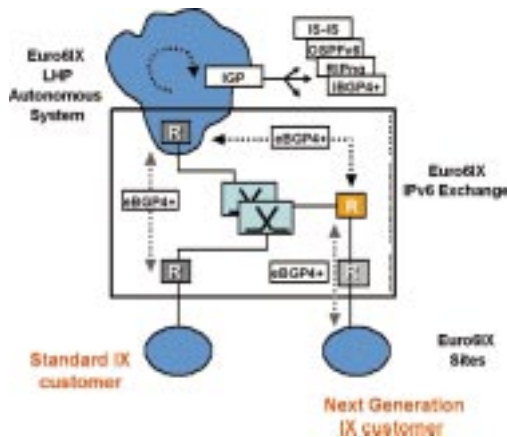


Figure 30: Routing Architecture Inside an IX

From the addressing point of view, every long haul provider and every Internet Exchange will have its own prefix. For example, a prefix assigned to one of the Long Haul Providers could be the Euro6IX 6Bone prefix (3ffe:4011::/32) and prefixes already owned by the partners hosting Internet Exchanges could be used as IX owned prefixes.

Every Long Haul Provider will use its own prefix to number all the links and the routers belonging to its backbone and to assign prefixes to their directly connected customers.

In particular the part of Euro6IX emulating a Long Haul provider will number with the same prefixes:

- a) The routers belonging to the Long Haul Provider collocated in the IX building outside the dotted area;
- b) The links inter-connecting the Long Haul Provider routers;
- c) Providing the IPv6 addresses to the Standard Long Haul Provider Customers.

The s/pTLA belonging to each IX will be used for:

- a) Assigning the addresses to the Next Generation Customers;
- b) Numbering the layer 3 part of the Internet Exchange (including the Layer 3 mediation Function Router).

# Moving to IPv6 in Europe

The addressing framework to be adopted is shown in the following diagram:

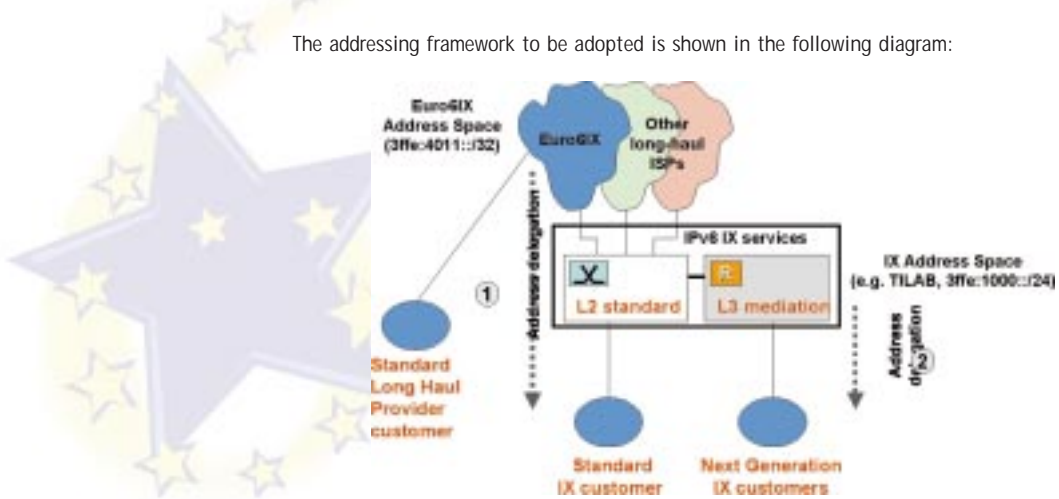


Figure 31: Addressing Framework

## 5.3.3. Euro6IX Backbone Routing Policy

The accepted proposal for the implementation of Euro6IX Routing Policy, uses the BGP4+ routing control mechanisms to control the traffic flow inside the Euro6IX network.

Given the necessity of controlling the traffic flows, they will be grouped by using the “community tagging” mechanism. The “tag” will be chosen taking into account the kind of traffic, its source and the required handling.

The community tagging will be done when network announcements enter the Euro6IX network and the same pattern will work throughout the whole network.

All routes exchanged among IXs must use a community and this community must remain constant throughout the Euro6IX Backbone. Peers will discard all the routes announced by IXs with no community tag.

Every AS has to be known and described within the Internal Euro6IX Backbone Routing Policy. When any community inherits from another network, the IX that is injecting those routes with that community must convert the remote community to a known community defined in this document.

The “extended communities” format will be used to tag routes. They will be used as an identifier of the network, so that customised information for that route can be generated.

Extended communities will be composed by two numerical parts separated by two points (<ASNumber>:<Value>), representing:

- *ASNumber*: Autonomous System Number of the announcer of the network. This field will be used to identify the AS Number of the IX that is injecting a concrete route into the Euro6IX backbone;
- *Value*: Numerical value *XYZ*.

Value field can be divided into:

- *XX*: Numerical value between 00 and 99, which defines the nature of a route;
- *Y*: Numerical value between 0 and 9, reserved for future use. It can be used for defining the kind of traffic associated to a route (experimental, commercial, testing, etc.);
- *Z*: Numerical value between 0 and 9, which represents the action to be taken for that route.

As stated before, these communities will remain the same throughout the Euro6IX IXs.

## 5.3.4. Other Research Activities

The deployed IPv6 IX infrastructure is being used to research, test and validate IPv6-based applications and services, such as:

- Investigations on the maturity of advanced IPv6 network services, as well as the feasibility of their inclusion in the Euro6IX test-bed, for example CoS/QoS, Mobility, Anycast and multicast, security, multihoming, renumbering, and policy languages;
- The development, porting, adaptation, or enhancement of IPv6 enabled applications, which will be made available for project trials and to third parties;
- The research of the legal implications of the project related to users, networks, and service providers addressing, personal data protection, and privacy concerns about IPv6 addressing.

The network built within the Euro6IX project is open to specific user groups (existing or to be created), who will be connecting to the Euro6IX network by means of a variety of access technologies —mobile, xDSL, cable— and internetworking with legacy IPv4 networks and services, to test the performance of future IPv6 networks, and non-commercial native IPv6 advanced services and applications. The network's Acceptable Use Policy (AUP) excludes the possibility of carrying commercial traffic.

## 5.4. GÉANT - Providing Native IPv6 in Dual-Stack Mode

GÉANT is the pan-European multi-gigabit research network, connecting more than thirty countries at backbone speeds of up to 10 Gbit/s. GÉANT operates at the leading edge of networking and employs state-of-the-art technology and techniques to provide its services to Europe's research and education community. As research becomes increasingly international, GÉANT forms a core resource for an ever-expanding number of researchers whose demands on the network are constantly increasing, not only in terms of bandwidth requirements, but also for network services.

Work is continually taking place within DANTE, the company that operates GÉANT on behalf of Europe's NRENs, to upgrade and refine the range and quality of the services provided by GÉANT in recognition of the need for the network to continue to satisfy the requirements of its users. An important objective of the GÉANT project is the development and implementation of IPv6 services within an ambitious timeframe.

A major milestone was achieved in April 2003 when the first set of NRENs were connected to GÉANT on native IPv6 accesses. As a result, GÉANT offers a dual stack core IPv6 backbone based on Juniper M160 and M40 and Cisco 7500 routers. The engineering work to reach this point was begun in September 2002 and involved a number of important steps that are described in more detail below.

### 5.4.1. IGP Transition

Firstly, although the routers could provide dual stack forwarding, in order for the actual network to be capable of operating in dual stack fashion, dynamic routing protocols had to be implemented across the backbone. To achieve this, the network's Internal Gateway Protocol first had to be migrated from its original OSPFv2 to IS-IS, to ensure GÉANT will remain at the forefront of future networking developments.

This transition took 6 weeks in total, from planning and preparation through to completion. DANTE's engineers drew on the previous experience of engineers from Abilene in migrating IGP, and an IS-IS training programme was provided by Juniper to ensure necessary levels of knowledge were achieved in advance of the transition.

The transition was tested and validated in a laboratory environment for 1 week, before performing the transition for real on GÉANT's 22 core routers across Europe.

IS-IS was configured on GÉANT 24 hours before the transition, but at this point was tuned to be the non-preferred IGP. The actual transition took place overnight, over a period of 3 hours. In practice, OSPFv2 and IS-IS were cohabiting on GÉANT during this time, before OSPF was deactivated on each router in turn to complete the move to IS-IS.

No interruption of services was experienced during the transition. Further technical details of this transition are available at <http://www.dante.net/nep/ipv6/index.html>.



# Moving to IPv6 in Europe

## 5.4.2. IPv6 Design

Once the IGP transition was complete, work could begin on implementing native IPv6 on the GÉANT backbone in dual stack fashion. For each router to perform native forwarding of IPv4 and IPv6 packets, IPv4 and IPv6 addresses had to be configured on the core backbone.

Once again this plan was validated in a laboratory environment to establish the most appropriate design prior to implementation on the network itself. The lab testing showed good performance results from the Juniper routers being used in dual stack fashion.

Use of BGP (Border Gateway Protocol) with IPv6 was also tested in the laboratory environment, and the GÉANT core backbone was then re-configured internally with a full mesh I-BGP for each of v4 and v6, in place of its current single I-BGP mesh. With the separate meshes in place, IS-IS continues to be used to route IPv4 traffic as well as that for IPv6.

### Routing policy

The IPv6 routing policy between GÉANT and the NRENs is very similar to the one in place for IPv4, but a cautious approach has been adopted to the type and length of prefixes GÉANT receives: to avoid instability, only prefix lengths in the range /35 to /32 will be accepted. GÉANT originates and announces the address space 2001:0798/32 allocated to it by RIPE.

The routing policy continues to be developed in discussion with other research networks such as Abilene, in the context of the GÉANT v6 task force.

### Addressing plan

The core backbone has been addressed in the range 2001:0798:20/40.

The range 2001:0798:4/35 is specifically reserved for allocating /48 blocks to small projects or small networks and /40 blocks to middle range projects.

Further information and full details of the addressing of the core backbone and the allocation of address space provided by RIPE can be found at <http://www.dante.net/nep/ipv6/design/index.html>.

## 5.4.3. IPv6 Service Offering on GÉANT

The introduction of IPv6 services on GÉANT is being achieved via a 6-month pilot phase, which started in April 2003, during which GÉANT itself is capable of delivering IPv6 service. NRENs and projects are connected to the IPv6 service during this period, as and when they are ready to do so. It is expected that the majority of the IPv6 enabled European NRENs, and also Abilene, will be connected by the end of the pilot phase in September 2003.

The configuration of the network in preparation for the pilot started in February 2003 and was completed in less than two weeks. This involved assigning IPv6 addresses not only to the core GÉANT routers but also to trunks and access links. In addition, the configuration of the I-BGP mesh for IPv6, mentioned earlier, was performed in this phase.

Connecting NRENs to IPv6 services on GÉANT requires an E-BGP v6 to be implemented on the primary access to GÉANT, to run in addition to the existing E-BGP v4 connection. This BGP peering can be done on the native access or via a tunnel if the NREN access router is not dual stack.

The first NRENs to be connected to GÉANT IPv6, in early April, were RedIRIS (Spain) and RENATER (France).

The network's stability and reliability is being carefully monitored during the pilot phase using dedicated IPv6 monitoring tools and any necessary debugging performed. This phase also serves to define the operating procedures required for production service.

Work to implement and evaluate the operation of IPv6 on GÉANT continues. GÉANT will enter into operational IPv6 service by October 2003. The GÉANT IPv6 service will benefit from the same level of support as the IPv4 service, and similar levels of reliability may be expected.

Further details of the rollout of IPv6 services on GÉANT can be viewed in Deliverable D30.1, "Implementation and Rollout Plan for IPv6", available at <http://www.dante.net/geant/geant-publicity.html#pd>



## 6. Future Development Paths



### 6.1. BRIAN E. CARPENTER

Brian E. Carpenter works as Distinguished Engineer, Internet Standards & Technology, with the IBM Systems Group, IBM Zurich Laboratory, Switzerland.

#### 1. What is the major driving force behind IPv6 deployment?

Up to now, this has largely been a technology push, from people in the Internet technical community who are aware of the serious scaling and operational problems that we face. But we now seem to be close to the tipping point, where we begin to feel market pull from user communities who see these problems as a real cost and see IPv6 as the solution. The best-known community is the 3G telephone industry, but there are

others, especially in regions of the world where IPv4 addresses are particularly lacking.

It's difficult to be more precise without giving confidential customer details.

#### 2. What are your business interests in this context? What products are available from IBM?

IBM believes that the Internet must continue to scale up, to allow us to move forward into the era of e-business on demand. IPv6 is a key part of that scaling process. All IBM server platforms now support IPv6 at operating system level, and we have stated our intention to enable all our software, as we see customer demand evolving.

#### 3. What are the constraints from your point of view?

IPv6 competes for priority with other customer requirements. There are no particular technical constraints, especially now that Java (TM) supports IPv6.

#### 4. What are the alternatives to avoid IPv6?

None.

# Moving to IPv6 in Europe

## 5. What applications do you support this year using IPv6?

In the 6NET project, IBM and its partners will be deploying and testing a large set of IPv6-enabled applications. See <http://6net.laeres.info/apps.phtml> for details.

## 6. What are the main steps for deploying IPv6?

Now that operating systems and routers support IPv6, enabling middleware and applications is the next step, which will in turn generate demand for ISP support. For enterprise and business use, we can go a long way using just the basic dual stack model and tunnels.

## 7. Which role does the US play in this context?

The address space shortage is better hidden in the US, for historical reasons. So we can expect the US to be a little behind the rest of the world in commercial adoption of IPv6—maybe they will be a couple of years late. However, that doesn't exclude major IPv6 investments for non-traditional applications in the pervasive computing environment, where the US will probably lead.

## 8. Which role does the rest of the world (or Europe, Japan) play in this context?

Logically, therefore, Europe and the stronger Asian economies will deploy sooner. And there is enormous potential in India and China, which are particularly starved of IPv4 address space.

## 9. How long will it take?

Serious deployments outside the research community will start quite soon now, so this year is the right time to make evaluation plans. IPv4 and IPv6 will probably co-exist indefinitely. However, we can expect IPv6 to be in truly widespread use by about 2010, i.e. 15 years after its design was sketched out.



## 6.2. HIROSHI ESAKI

Hiroshi Esaki is a prominent member of the WIDE Project and the IPv6 Promotion Council of Japan. Hiroshi is Associate Professor at the Graduate School of Information Science and Technology at the University of Tokyo, Japan.

### 1. What is the major driving force behind IPv6 deployment?

There are several: peer-to-peer communications, the application of IP technology to make business operations more efficient for all industrial segments, and the closer integration of cyberspace with real-space.

### 2. Does Peer-to-Peer communication include GRID technology in your understanding as well?

Grid covers a wide variety of applications. These reach from high-end science and technology to consumer communications. From this point of view, I include the Grid into the peer-to-peer communications. However, Grid has various communication architectures, that are both client-server and peer-to-peer. They, basically, do not mind about IP version number. What they need is a stable and common infrastructure (network and operating system) to explore the Grid technology.

### 3. What do you mean by closer integration of cyberspace and real-space?

For example:

- Applications aware of the geographical location of the user;
- Mobile digital equipment connected to the Internet;
- Non-PC digital equipment is going to be connected too.

### 4. What kind of applications do you have this year using IPv6?

VoIP is the first wave for residential users. Then, the cross-media communication will emerge. For corporate use, a lot of applications will come out, so as to improve every business activity.

## 5. What are the constraints from your point of view?

The bad economic situation slows down the introduction of new equipment and software. There is a certain conservativeness of network and system operators and of corporate executives.

## 6. What is the situation in Japan?

Well, a lot of corporate executives are always conservative to continue the profitable business structure. A small percentage of corporate executives take a good action, which improves and explores the new business structure for their companies, I think. In fact, Japan can show to the rest of the world that the IPv6 technology works fine and some examples of killer applications.

## 7. What are the main steps for deploying IPv6?

Managing the co-existence with IPv4 technology and the development of applications.

## 8. Which role does the US play in this context?

The development of IPv6-ready products.

## 9. How long will it take?

The deployment and integration is not a sudden step, but will take place gradually. IPv6 and IPv4 will be coexisting for many years. Already, some network and services are based on dual stack.



## 6.3. PATRICK GROSSETETE

Patrick Grossetete is Cisco IOS IPv6 Product Manager and works in the Internet Technology Division (ITD) at Cisco Systems in Issy les Moulineaux, France.

### 1. What is the major driving force behind IPv6 deployment?

Scaling the Internet for our Next Generations. We can argue—and a lot of people do—on the technical advantages of IPv6 but the key driver is the medium/long term need for addressing. I always find it strange that nobody complains to the telephone companies about renumbering from 5 to 8 to 10 digits—although anybody already having a telephone number in one of the major cities may have seen no reason to use large numbers, even if it is useful for the rest of the people living in a country—but some don't see the same need for IP. IP is the real convergence layer for applications (audio, video, voice and data) but only 10% of the current global population gets access to the Internet. If we want to grow this percentage + sustain the earth's population growth for the next 50 years + add IP to any kind of devices/applications + get mobile. What are the alternatives?

### 2. What are your business interests in this context? What products are available from Cisco?

I am the Cisco IOS IPv6 Product Manager, responsible to set the development direction for the integration and support of IPv6 on Cisco IOS software run by our router series. I am also in charge of the marketing activities related to Cisco IOS IPv6. As the worldwide leader in networking for the Internet, Cisco Systems integrates the support of IPv6 in its product portfolio to enable our customer's installed base to deploy IPv6 where and when required by their business. As announced in June 2000, in our IPv6 Statement of Direction—see <http://www.cisco.com/warp/public/732/Tech/ipv6/docs/sod.pdf>, Cisco added the IPv6 feature set as part of the Cisco IOS software, meaning that any Cisco customer can IPv6-enable their networking infrastructure through a software upgrade. Cisco routers running one of the following Cisco IOS releases can be configured for IPv6:

- Cisco IOS 12.2T;
- Cisco IOS 12.2S;
- Cisco IOS 12.0S for Cisco 12000 series.

# Moving to IPv6 in Europe

## 3. What are the constraints from your point of view?

As with any new technology, IPv6 requires a learning curve to get people educated as well as a business case to justify the deployment. This cannot happen overnight but is a step-by-step process. Today, networking equipment is available for IPv6 and can be installed and configured. Operating systems integrate IPv6 stacks allowing applications to be ported to IPv6.

The next step is to develop some business models that justify the investments to deploy IPv6 on a large scale. As we observed during Y2K, a large-scale upgrade of software/hardware means human resources, training and cost justification/control. The benefits for all parties must be demonstrated.

From a technology and product standpoint, some areas still need to be developed to attract customers. For example, network management—including provisioning and billing applications—as well as security products must become available before we can expect a wide adoption.

Back to the business model, just let me take an example. Today, you can get an ADSL connection with a temporary IPv4 address for around 30 Euros. That's what most of the people get (permanent IPv4 address is more expensive) but what do they do with that? Just browse the web and send e-mails. If an ISP adds an IPv6 service with a permanent /48 prefix, there is little chance many end-users will pay 50-60 Euros for it if they only run the same applications.

Now, assume IPv6 devices and applications are marketed, e.g. Gaming stations running IPv6 for distributed gaming and contests, consumer electronic devices integrating IPv6, e.g. a fridge, the business model being that the retailer will do 3 years tele-maintenance for the 100 Euros you generally agree to pay for 3 years warranty extension + pre-configuration of the fridge's screen to be connected to an on-line ordering company (Walmart, Carrefour, etc.). We now have a win-win situation as the retailer and on-line ordering companies propose better services to their customers but also grab their loyalty... forget about telnet/ftp... from a fridge, just focus on 2-3 applications. —Fax over IPv6— (could become phone as well but is far more complex technically, politically and economically). Once again, it's a win-win situation, you pay more for your broadband access connection but don't have to pay for each fax you send—tele-metering— all utility companies will agree to serve customers that can be reachable—computer applications such as web server, video-conferencing. Pick 1 or 2 of the above cases, and you develop a business model that can be correctly marketed as a win-win for the ISP as they get more revenue for the service, more people paying 50-60 Euros versus 30 the end-users as he gets more from the service and can compensate what he is paying retailers and service companies who can create additional offering and revenues from the always-on environment.

## 4. What are the alternatives to avoid IPv6?

Don't really see one... but is dependent on what we want to achieve with the Internet. If the goal is a ubiquitous Internet, IPv6 is the only solution to scale IP. Other alternatives are multiple NAT layers but it will certainly fragment the Internet and constrain the innovation or a new protocol but that will delay for years the evolution on a large scale since I don't know about any proposal.

## 5. What applications do you support this year using IPv6?

As a networking company, we mostly enable applications to run over an IPv6 infrastructure. This can be done today using Cisco equipment. For an overview of IPv6 supported features, please refer to [http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6\\_sol/ipv6dswp.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/ipv6dswp.htm).

## 6. What are the main steps for deploying IPv6?

First, you have to identify your business case(s). IPv6 deployment represents a cost (training, human resources, software/hardware upgrade, etc.). In the current economic situation, every euro has to be justified. If you are an ISP, you must evaluate the services and expected revenues from your IPv6 services. If you are an enterprise, you look at IPv6 applications and their benefits for your business environment. If you are an end-user, you consider new products/devices you may have a need for—or that a nice marketing campaign may let you think you need.

From there, you build your deployment scenario and move forward. If I focus on the ISP and enterprise markets, I have to say that the scenario can be split between edge and core infrastructures. The edge is the

most important as this is how you connect people/devices/applications so your native IPv6 connectivity looks like the best approach. Core can have various scenarios as long as you transport IPv6 as you feel confident with.

From a technical standpoint, Cisco described the scenario in [http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6\\_sol/ipv6dswp.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/ipv6dswp.htm).

## 7. Which role does the US play in this context?

Today, most of the networking and operating systems come from the U.S. and most of them already integrate IPv6 protocols to satisfy the worldwide market requirements. As the focus is now on applications and non-computing devices (e.g. gaming, consumer electronics, etc.) as well as ISP deployment, I will say the U.S. has an important role to play on its regional market for the U.S. users as well as economically for the industries that are selling worldwide as no region can stay away from market evolution.

It is important to consider that the U.S. is the major transit region for the Internet, so IPv6 infrastructures such as IPv6 Peering Point (i.e.: 6TAP) are crucial for the worldwide success of IPv6.

As market globalisation is now a fact, I can't see any enterprise deciding to be unreachable from half of the world that could run IPv6 by not at least IPv6 enabling some of its IT services (web, e-mail), note this is true for any worldwide region.

## 8. Which role does the rest of the world (or Europe, Japan) play in this context?

Industrial sectors such as mobile phones, consumer electronics, transportation (airplane, cars, trains), broadcasting are all moving to IP technology now. The scale of the targeted end-user's market justifies the need for IPv6. It is important for Europe and Japan to play a similar role as U.S. in the economic area they master today.

Infrastructure and globalisation aspects are exactly the same as for the U.S.

And by the way, who knows how a market sector can evolve over time we have seen car manufacturers, electronics, computer companies growing and disappearing across the world for years. IPv6 represents opportunities and nemesis for all market sector players!!!

## 9. How long will it take?

5-10 years as for any new technology to be adopted. Does it mean IPv4 will disappear? Certainly not before years, people still use Telex, X.25 and other old technologies today as long as it fits their business needs. Let's move forward with IPv6 innovations and applications, those represent the best chance of success for IPv6.

Then we may see if there is a need to deprecate the old technology.



## 6.4. CHRISTIAN HUITEMA

Christian Huitema works for Windows Networking and Communications Group, United States.

### 1. What is the major driving force behind IPv6 deployment?

IPv6 will be deployed because it enables the development of new experiences. For example, we see Real-Time Communications (RTC) that combine instant messaging, voice, video, real-time game play and sharing; collaboration where project members can collaborate on documents in shared workspaces; and shared experiences such as concerts, company meetings, virtual class rooms, or distribution of product updates. We call that Pervasive Collaborative Computing, and it will be the major driving force behind IPv6.

## 2. What are your business interests in this context?

We are interested in enabling next generation network-based applications without additional expense or expertise, and without major investment in new network infrastructure.

# Moving to IPv6 in Europe

## 3. What are the constraints from your point of view?

One often hears that deploying IPv6 will require many years and vast investments. In fact, we believe that the opposite is true. Transition technologies such as 6to4, ISATAP and Teredo allow an initial deployment over the existing infrastructure. The deployment will be driven by the first IPv6-enabled applications. However, upgrading all existing applications to support IPv6 takes time. We must thus assume that there will be coexistence between IPv4 and IPv6 applications, and that for the next years the networks will support both protocols.

## 4. What are the alternatives to avoid IPv6?

I don't think that IPv6 is avoidable.

## 5. What products can you offer this year using IPv6?

IPv6 is supported in several Microsoft operating system products: Windows(r) XP SP1 and Windows Server 2003, Windows CE .NET, Pocket PC (2003), and Windows Embedded SP1. We are releasing an Advanced Networking pack for Windows XP (currently in Beta) that provides support for IPv6 traversal of IPv4 NAT (Teredo), as well as a personal IPv6 Firewall.

We have also released several developer solutions: Winsock, HTTP, RPC, DirectPlay, Peer to Peer SDK (Beta), Visual Studio(r) & .Net Framework, DCOM.

IIS 6.0, IE 6.0, Windows Media Server & Client (4/24), File Sharing, and the Windows 2003 DNS Server and Client are IPv6 enabled. We also released the beta version of "Three Degrees" (<http://www.threedegrees.com>), which is an add-on to MSN Messenger enabling collaborative online music and picture sharing for the "NetGen" market (12-24 year-old). Three degrees is built on our P2P SDK and requires IPv6 connectivity.

## 6. What are the main steps for deploying IPv6?

While it may vary from place to place, we think that the typical transition will start with transition technologies before enabling native connectivity. First, client-based applications will be enabled using Teredo or 6to4; this will enable new applications within networks with NAT or via 6to4 with no NAT. ISATAP routers will be deployed within existing corporate networks to improve connectivity, and allows test deployments of native IPv6 networks. As internal routers get replaced over time, native connectivity will replace the ISATAP service; 6to4 may enable access to the public IPv6 Internet. Finally, as new routers get deployed, the transition technologies will be replaced by IPv6 services provided by IPv6 ISPs.

## 7. Which role does the US play in this context?

In the US, the market forces decide which technologies get used and when. IPv6 will be deployed on its merits, which we believe are substantial. In fact, significant IPv6 deployments are under way in government agencies, in research networks such as Internet2, and in corporate networks such as those of Microsoft. In many cases, deployment will be quasi-transparent: the users of "Three Degrees" all enabled IPv6 on their computers, without requiring any particular set up.

## 8. Which role does the rest of the world (or Europe, Japan) play in this context?

There are clearly many experimental IPv6 networks in Europe, and Japan has made a lot of interesting developments of IPv6 connected appliances. But we believe that eventual deployment in Europe and Japan will be parallel to the US. Here as there, the market forces will determine the outcome.

## 9. How long will it take?

For the next couple of years, there are lots of opportunities in home networking with Windows fully supporting IPv6; we will see significant deployment in 2003. Deployment in enterprise will follow, probably one or two years later, as new applications get deployed.

Dual-stack support will remain important in the foreseeable future.



## 6.5. WOLFGANG NOSZEK

Wolfgang Noszek works for Innovation Management, Deutsche Telekom, Germany.

### 1. What is the major driving force behind IPv6 deployment?

For us at Deutsche Telekom the most important aspect of IPv6 is the increase in address space—all the other features of IPv6 are nice to have but do not in themselves justify the update to a new network protocol.

### 2. What are the business interests in this context?

We are currently envisioning a lot of new services which will be using these addresses. On the other hand, we must match customer needs and demand

with our actual service offering. Something that is not done overnight for a big provider such as Deutsche Telekom AG.

### 3. What are the alternatives to avoid IPv6?

We currently see no other alternative but a showstopper would be a different technology than IP getting used by people to overcome the limitations of IPv4.

### 4. What are the main steps for deploying IPv6?

An integration plan exists for DTAG. Again, the first and most important issue is the infrastructure, then we deploy applications.

### 5. Which role does the US play in this context?

If address is the real problem—then the USA has no real problem at the moment. However, hardware vendors and software companies are very active.

### 6. Which role does the rest of the world play in this context?

Japan will pay a lot of “tuition fees” in IPv6—Europe is the follower— (best way for IPv6) and can avoid many mistakes in deployment.

### 7. How long will it take?

The actual timeline might be 2005 to 2007—but this means we must start to act now.



## 6.6. CHARLES E. PERKINS

Charles E. Perkins is a Research Fellow at Nokia Corporation in the Silicon Valley Division of Nokia Research Centre.

### 1. What is the major driving force behind IPv6 deployment?

The major force is the need for additional address space. With new address space, we can see the more rapid deployment of interactive applications.

### 2. What are your business interests in this context?

My interest is the development and deployment of wireless Internet technology worldwide, as economically as possible. My employer shares these interests, naturally, and specifically would like to enable markets for consumer applications using 3G voice and data communications.

### 3. What are the constraints from your point of view?

The constraints are mainly co-existence and smooth evolution from the existing IPv4 Internet. Furthermore, from the practical point of view, there are not enough ISPs offering IPv6 service yet.



# Moving to IPv6 in Europe

## 4. What are the alternatives to avoid IPv6?

We can try to build out further repairs to IPv4. There may be some way to retrofit various IPv6 mobility technologies into IPv4, but doing so will be considerably more complex than just moving to IPv6 in the first place. There are also other technical alternatives that are less attractive (e.g., new IPv4 options, new ways of using DNS, new layers in the protocol stack). Each of them is imaginable, but there are a lot of details where devils can hide, perhaps invisibly for a long time.

IPv6 represents a more mature technology than any of these others, and a generally cleaner approach.

## 5. What applications do you have this year using IPv6?

We are researching various techniques to support smooth handovers for interactive wireless applications. We are also investigating various techniques related to ad-hoc networks and mobile networks.

## 6. What are the main steps for deploying IPv6?

Buy the equipment. Install the IPv6-ready platforms. Find an ISP that offers IPv6. It's a lot easier than it was to deploy IPv4 when we were starting from disconnected PCs or mainframe terminals. IPv6 supports the same applications as IPv4, naturally, and most of the popular applications have already been ported from IPv4 to IPv6.

## 7. Which role does the US play in this context?

The U.S. has a lot of strong technology firms that offer IPv6 products, including Microsoft, Cisco, Sun, and most of the major technology firms.

## 8. Which role does the rest of the world (or Europe, Japan) play in this context?

The whole rest of the world seems to have a stronger need for address space than the U.S. does. I think that IPv6 has created a very cosmopolitan and trans-national constituency, and I hope that the technical underpinnings being created by this new community will enable rapid development and deployment of many new wireless technologies and applications. Interest in those technologies also seems stronger in countries outside the U.S., perhaps because it is often easier to install new wireless facilities than to install new wired networks.



## 6.7. DALE ROBERTSON

Dale Robertson works as Public Relations Manager for the DANTE company in Cambridge, United Kingdom.

### 1. What is the major driving force behind IPv6 deployment?

IPv6 will remedy the current restrictions on address space experienced with IPv4 due to the longer address lengths supported by the IPv6 protocol. This will help to remove one of the limitations on the rate of deployment of networked technology applications, and in particular will help to clear the way towards the uptake of wireless applications.

### 2. What are your business interests in this context?

The partners in the GÉANT project have recognised the importance of remaining at the forefront of network technology developments, and of ensuring that GÉANT provides a state-of-the-art network to Europe's researchers, providing an environment capable of supporting new applications and services. Deploying IPv6 on GÉANT is clearly in keeping with this strategy, hence the priority given to this activity.

### 3. What are the constraints from your point of view?

DANTE, in cooperation with several NREs, is implementing native IPv6 in dual-stack mode on GÉANT. The constraint we have encountered is that older network routing equipment is not capable of supporting dual-stack operation and has to be replaced by more up-to-date equipment. In addition, IPv6 service on GÉANT

has had to be implemented on a production network already offering a number of different services (premium IP, best efforts, less than best efforts, multicast) without impacting adversely on these services.

#### 4. What are the alternatives to avoid IPv6?

For a network such as GÉANT, with the purpose of providing a state-of-the-art network to support the requirements of the European research and education community, there is no alternative to IPv6: offering an IPv6-capable network at the present time is core to achieving our mission.

#### 5. What are the main steps for deploying IPv6?

These are described in detail in Section 5.4. of this publication.

#### 6. Which role does the US play in this context?

Please see next question.

#### 7. Which role does the rest of the world play in this context?

The development of new markets based on applications that rely on IPv6 will be accelerated by widespread deployment of IPv6-capable networks. The achievement of a globally accepted protocol and its uniform interpretation avoids market fragmentation due to technical incompatibilities. The deployment of IPv6 on networks globally, not just in Europe, is thus of importance commercially. The increasingly international nature of research collaboration makes it important for IPv6-ready networks to be available around the world and not just across Europe. This would provide a uniform global basis for research communications.

#### 8. How long will it take?

Pilot IPv6 service has already begun on GÉANT. Native IPv6 production service in dual-stack mode will be available by October 2003.



## Table of Figures

Figure 1: The IPv6 Cluster

Figure 2: IPv6 Multicast Address Format

Figure 3: Reverse Path Forwarding

Figure 4: PIM Dense Mode

Figure 5: PIM Sparse Mode

Figure 6: PIM Source Specific Multicast

Figure 7: Multicast Between Customer Sites of IPv6

Figure 8: M6bone Network Map

Figure 9: Mobile IPv6 Return Routability Procedure

Figure 10: A Simplified Model of CGA-based Authentication

Figure 11: An example of Road Warrior functionality

Figure 12: The Whittington Hospital Scenario

Figure 13: The John Paul II Hospital Scenario

Figure 14: Animation of Multi-frame DICOM Images (movies) in the UMM's Java DICOM Viewer

Figure 15: GANS Demonstration Using Ericsson's UMTS Test-bed and Multi-access Enhancement to Mobile IPv6

Figure 16: A "Guardian Angel Centre" at INET 2002 supporting an "ambulance" in Tübingen

Figure 17: Framework for Adaptive Applications

Figure 18: Global Mobility Scenario

Figure 19: Jitter Experienced at KCL (London)

Figure 20: Loss at T-Systems (Berlin)

Figure 21: Growth of the 6Bone in the Period from 1997 to 2002

Figure 22: Graphical Representation of 6Bone Growth (Source: 6Bone Registry)

Figure 23: 6NET Core Network

Figure 24: Euro6IX Network

Figure 25: Architecture of IX Model A

Figure 26: Architecture of IX Model B

Figure 27: Public Topology Hierarchy

Figure 28: Network Architecture as Shown in RFC2374

Figure 29: Internet Exchanges Structure

Figure 30: Routing Architecture Inside an IX

Figure 31: Addressing Framework



## Links to IPv6

@HOM	<a href="http://www.at-hom.org">http://www.at-hom.org</a>
6INIT	<a href="http://www.6init.org">http://www.6init.org</a>
6LINK	<a href="http://www.6link.org">http://www.6link.org</a>
6NET	<a href="http://www.6net.org">http://www.6net.org</a>
6POWER	<a href="http://www.6power.org">http://www.6power.org</a>
6QM	<a href="http://www.6qm.org">http://www.6qm.org</a>
6WINIT	<a href="http://6winit.org">http://6winit.org</a>
6HOP	<a href="http://www.cwc.oulu.fi/projects/6hop">http://www.cwc.oulu.fi/projects/6hop</a>
ANDROID	<a href="http://www.cs.ucl.ac.uk/research/android">http://www.cs.ucl.ac.uk/research/android</a>
CRUMPET	<a href="http://ist-crumpet.org">http://ist-crumpet.org</a>
DRIVE	<a href="http://ist-drive.org">http://ist-drive.org</a>
EC IPv6 Task Force	<a href="http://www.ec.ipv6tf.org">http://www.ec.ipv6tf.org</a>
Euro6IX	<a href="http://www.euro6ix.org">http://www.euro6ix.org</a>
Eurov6	<a href="http://www.eurov6.org">http://www.eurov6.org</a>
Future Home	<a href="http://www.future-home.org">http://www.future-home.org</a>
GCAP	<a href="http://www.laas.fr/GCAP">http://www.laas.fr/GCAP</a>
GEANT	<a href="http://www.geant.net">http://www.geant.net</a>
HARMONICS	<a href="http://www.ist-harmonics.net">http://www.ist-harmonics.net</a>
IETF	<a href="http://www.ietf.org">http://www.ietf.org</a>
INTERMON	<a href="http://www.ist-intermon.org">http://www.ist-intermon.org</a>
IPv6 Forum	<a href="http://www.ipv6forum.org">http://www.ipv6forum.org</a>
IPv6 Task Force	<a href="http://www.ipv6tf.org">http://www.ipv6tf.org</a>
IPv6 Task Force SC	<a href="http://www.ipv6tf-sc.org">http://www.ipv6tf-sc.org</a>
IST IPv6 Cluster	<a href="http://www.ist-ipv6.org">http://www.ist-ipv6.org</a>
IST Projects	<a href="http://www.cordis.lu/ist/overview.htm">http://www.cordis.lu/ist/overview.htm</a>
IST Research Networking	<a href="http://www.cordis.lu/ist/rn/ipv6.htm">http://www.cordis.lu/ist/rn/ipv6.htm</a>
LONG	<a href="http://www.ist-long.com">http://www.ist-long.com</a>
MESCAL	<a href="http://www.ist-mescal.org">http://www.ist-mescal.org</a>
MIND	<a href="http://www.ist-mind.org">http://www.ist-mind.org</a>
Moby Dick	<a href="http://www.ist-mobydick.org">http://www.ist-mobydick.org</a>
NGNI	<a href="http://www.ngni.org">http://www.ngni.org</a>
NGNLab	<a href="http://www.ngnlab.org">http://www.ngnlab.org</a>
OverDRIVE	<a href="http://www.ist-overdrive.org">http://www.ist-overdrive.org</a>
SATIP6	<a href="http://satip6.tilab.com">http://satip6.tilab.com</a>
SERREEN	<a href="http://www.sereen.org">http://www.sereen.org</a>
TORRENT	<a href="http://www.torrent-innovations.org">http://www.torrent-innovations.org</a>
Tsunami	<a href="http://www.eurescom.de/public/projects/P1100-series/P1113">http://www.eurescom.de/public/projects/P1100-series/P1113</a>
Wireless Cabin	<a href="http://www.wirelesscabin.com">http://www.wirelesscabin.com</a>
xMotion	<a href="http://www.ist-xmotion.org">http://www.ist-xmotion.org</a>



European Commission



# IPv6 Cluster



Information Society  
Technologies