Title:	Document Version:
Deliverable D4.1A **Report on the first year Network and Application Research Activities**	0.7

Project Number:	Project Acronym:	Project Title:
IST-2001-32161	Euro6IX	European IPv6 Internet Exchanges Backbone

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/12/2002	09/03/2003	R – PU

* Type:	P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class:	PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
David Fernández Antonio F. Gómez-Skarmeta	UPM UMU	WP4

Authors (organizations):

Miguel Á. Díaz (Consulintel), Miguel A. Morales (Consulintel), César Olvera (Consulintel), Jordi Palet (Consulintel), Alvaro Vives (Consulintel), Cesar Martín (novaGnet), Jesús Muñoz (novaGnet), Francisco Fontes (PTIN), Victor Marques (PTIN), Carlos Parada (PTIN), Carlos Rodrigues (PTIN), Jacinto Vieira (PTIN), Sathya Rao (Telscom), Eduardo Azañón (TID), Aurora Ferrándiz (TID), Ignacio Grande (TID), Cristina Peña (TID), Carlos Ralli (TID), Francisco Romero (TID), Mario Morelli (TILAB), Olaf Bonnes (T-Nova), Lothar Grimm (T-Nova), Roland Schott (T-Nova), Stefan Spiewok (T-Nova), Guido Steinkamp (T-Nova), Félix J. García (UMU), Gabriel López (UMU), Rafael Marín (UMU), Gregorio Martínez (UMU), Tim Chown (UoS), Xiang Fei (UoS), Diego Acosta (UPM), Juan L. Fernández (UPM), Fermín Galán (UPM), Tomas P. de Miguel (UPM), Maria J. Perea (UPM), Juan Quemada (UPM), Tomás Robles (UPM), Javier Sedano (UPM)

Abstract:

This document summarizes the results of the research and innovative tasks planned for the first year of Euro6IX project in the context of WP4 activities A4.1 (Advanced Network Services Design and Evaluation) and A4.2 (IPv6 Application Development). WP4 main aim is the design, consolidation and validation of an IPv6 based integrated end user service scenario, which integrates advanced network services and applications into a common framework. For that purpose, work has been organized around sub-activities covering: Mobility, multicast, QoS, AAA, and a broad range of security aspects like IPsec based VPNs, PKIv6 or DNSSEC, in the case of A4.1 activity; and basic and advanced IPv6 applications, network management and operation tools, IX support tools and code porting in the case of A4.2. As the number of sub-activities and the effort invested is high, the document just outlines the main objectives and results of each sub-activity. More detailed information can be found in the associated Technical Reports referenced at the end of the document.

Keywords:

AAA, Agent-based computing, AGWS, Audio-Conferencing, Certificate, Code Porting, DIAMETER, DiffServ, DNSSEC, Dynamic VPN, Euro6IX, Handover, IKE, Instant Messaging, IPsec, IPv6 Repository, IPv6, IX, M6Bone, Macromobility, Magalia, Micromobility, Mobile IPv6, MRTG, Multicast, NIDS, Peer-to-Peer, PHP, PKIv6, QoS, Roaming, Route Server, RPSL, RPSLng, SIP, Static VPN, Traffic Class, Unified IM, VNC.

Revision History

Revision	Date	Description	Author (Organization)
v0.1	20/12/2002	Document creation.	David Fernandez (UPM) Antonio G. Skarmeta (UMU)
v0.2	28/12/2002	Integration of sub-activity summaries.	David Fernández (UPM) Antonio G. Skarmeta (UMU)
v0.3	30/01/03	Introduction added.	Juan Quemada (UPM)
v0.4	3/02/03	Integration of missing sub-activities summaries	David Fernández (UPM)
v0.5	13/02/2003	Conclusions added.	Juan Quemada (UPM) David Fernández (UPM)
v0.6	17/02/2003	Final revision.	David Fernández (UPM)
v0.7	09/03/2003	Final changes and PSC Review	Jordi Palet (Consulintel)

Executive Summary

This document summarizes the results of the research and innovative tasks carried out along the first year of Euro6IX project in the context of WP4 activities A4.1 (Advanced Network Services Design and Evaluation) and A4.2 (IPv6 Application Development).

WP4 main aim is the design, consolidation and validation of an IPv6 based integrated end user service scenario, which integrates advanced network services and applications into a common framework, which will be called the "Euro6IX Integrated Service Framework". Therefore WP4 considers the integration of several advanced network services together with applications, which exploit the new features as one important goal.

For that purpose, work under A4.1 and A4.2 has been organized around sub-activities covering a wide variety of IPv6 network services and features: Mobility, multicast, QoS, AAA, and a broad range of security aspects like IPsec based VPNs, PKIv6 or DNSSEC, in the case of A4.1 activity; and basic and advanced IPv6 applications like SIP based audio-conferencing, ISABEL, Instant and Unified Messaging or Groupware applications, as well as network management and operation tools, IX support tools and code porting, in the case of A4.2.

The document is organized as follows. Section 1 introduces WP4 general context, objectives and organization, as well as summarizes the specific objectives and results A4.1 and A4.2 activities. Section 2 and 3 outline the objectives and results of the different sub-activities under A4.1 and A4.2 respectively. As the number of sub-activities and the effort invested in them is high, only a brief summary about each sub-activity objectives and results has been included. More detailed information can be found in the associated Technical Reports referenced at the end of the document. Finally, Section 4 comes to conclusions about the work done during the first year and ideas about future activities.

Table of Contents

Table of Figures

1. INTRODUCTION

This Deliverable describes the results obtained after the first project year in the network and application research activities of Work Package 4 "Associated Research Activities, Trials and Evaluation".

The Euro6IX test-bed has been conceived as a small-scale model of the Internet. It includes the main components of the actual global Internet such as a backbone of IX nodes (traffic exchange nodes) interconnecting AS's (Autonomous Systems) which represent regional networks containing a variety of providers and access technologies.

WP4 has as its main aim, the design, consolidation and validation of an integrated end user service scenario, which integrates advanced network services and applications into a common framework, which will be called the "Euro6IX Integrated Service Framework". Therefore WP4 considers the integration of several advanced network services together with applications, which exploit the new features as one important goal.

During the first year WP4 has concentrated in consolidating activities and teams covering the most important network and application components needed for the deployment of the Euro6IX test-bed, as well as for the "Euro6IX Integrated Service Framework". Therefore the results presented in this deliverable include the components which will be integrated in a common service framework and deployed and validated in the Euro6IX test-bed during the next project years, when the focus of the project will be much more on integration, than on individual feature development and consolidation.

The deployment on the Euro6IX test-bed of new architectures and features made possible by IPv6 is also another important priority for WP4. Therefore tools for management and operation of the test-bed, as well as experimentation with new features such as autoconfiguration, provider independent addressing, multihoming, route servers, etc, have been addressed during the first year.

The introduction of security into the future Internet is considered one of the main challenges and, therefore, the first year has included activities dealing with security from several perspectives and with different approaches. All this activities must provide the foundations for assembling and validating in the forthcoming years of Euro6IX an integral security approach based on IPv6. The introduction of security implies advanced network security feature deployment, as well as adaptation and tuning of applications. Therefore many sub-activities such as IPsec-VPNs, PKIv6, DNSSEC or AAA have consolidated during the first year the new network security features. Several applications are being adapted in parallel to make use of those security features, such as SIP based audio-conferencing, the Isabel CSCW application, unified instant messaging, as well as some groupware applications.

The support to the various types of mobility components, as well as the adaptation and validation of previously mentioned applications in a mobile scenario, is another important goal. Therefore the consolidation of IPv6 based mobility has been included in the first year activities. QoS, anycast and multicast are considered also potential components of the integrated service framework and have been therefore included in the first year activities.

All this activities are complemented with the porting of generic software libraries and packages, as well as applications, which are considered important for the transition to IPv6.

1.1 Structure of WP4

To achieve the goals assigned to WP4 in Euro6IX, the work package has been divided in four activities which have to work in close cooperation and which are:

- **A4.1 - Advanced network services design and evaluation:** Groups all the research, development, integration and validation of advanced IPv6 network services which are candidates for integration in the Euro6IX test-bed, such as mobility, multicast and anycast, security, multihoming, renumbering, QoS/CoS, etc.

  Rather than considering the services in isolation, this activity will focus on the integration of all those services into the common operational framework of the Euro6IX test-bed, which will be called the "Euro6IX Integrated Service Framework". The integration will be performed considering:

  - Incompatibilities and interaction problems of the integration of services.
  - Scalability of services across the IX core and impact of the service in the IX architecture.
  - Relevance for the deployment of IPv6.

- **A4.2 - IPv6 application development:** Groups all the research, development, adaptation, enhancement, maintenance and validation of applications, which are considered most relevant for the successful deployment of the Euro6IX test-bed and for facilitating the transition to IPv6.

  This activity identifies the following important areas of work:

  - Application porting, adaptation, development or tuning as needed for the deployment, operation and management of the Euro6IX test-bed.
  - Application porting, adaptation, development or tuning as needed for the validation and assessment of the "Euro6IX Integrated Service Framework" development done in Activity A4.1.
  - Application development when considered important to facilitate the transition to IPv6 or to extract the potential of IPv6 advanced network services.

  This activity will mainly perform the porting and adaptation of existing applications to meet the above-mentioned goals. For example, the adaptation of existing VoIP or videoconferencing applications to make use of security, mobility, QoS, etc.

  Additionally, new applications will be developed when no existing one is considered able to exploit the features offered by IPv6.

  Finally the activity will also consolidate all the experience gained in making the transition from IPv4 to IPv6 in the form of a Guide for the porting and transition of applications to IPv6.

- **A4.3 - Trials and evaluation:** Groups all the definition, planning, realization and evaluation of trials to be performed over the Euro6IX test-bed. Trials will include internal trials to evaluate and assess user services in an end-to-end user scenario, as well as public trials, which will demonstrate the new capabilities of IPv6.
- **A4.4 - Legal aspects:** Deals with the impact of IPv6 in Privacy/Civil Liberty, data protection, and IPR issues.

It is important to remark that activities A4.1 and A4.2 will provide the network service, application development and integration as needed for the realization of the trials in A4.3. Therefore all three activities will work in close cooperation.

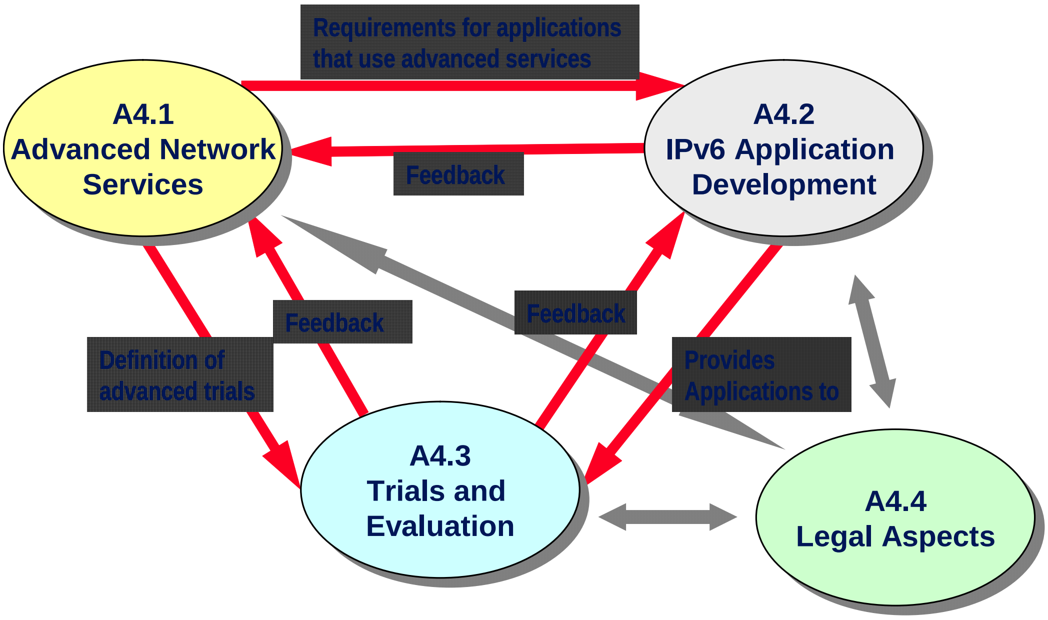

Requirements for applications that use advanced services
A4.1
Advanced Network Services
A4.2
IPv6 Application Development
Feedback
Feedback
Feedback
Definition of advanced trials
Provides Applications to
A4.3
Trials and Evaluation
A4.4
Legal Aspects

Figure 1-1: Relations between WP4 Activities

Figure 1-1 shows graphically the relations between WP4 activities.

1.2 Structure of this Document

This document summarizes the results obtained during the first Euro6IX year in activities A4.1 Advanced network services design and evaluation and A4.2 IPv6 application development.

The document has been structured therefore following the work and management structure of those activities. The results of each activity are described in each of the two next chapters and each chapter contains one section for each of the sub-activities.

This deliverable contains only an overview of the work done and is complemented when needed with additional "Technical Reports", which are referenced in section 5 and held in electronic format in the Euro6IX Web server at http://www.euro6ix.org.

1.3 Summary of A4.1: Advanced Network Services Design and Evaluation

A4.1 groups all the research, development, integration and validation of advanced IPv6 network services and features, which are candidates for inclusion into the Euro6IX Integrated Service Framework. Those services include mobility, various security components, multicast, anycast, multihoming, renumbering, QoS/CoS, etc. The summary of results produced in A4.1 during the first year of the project is as follows:

- **Mobility:** Sub-activity A4.1-1 Mobility over IPv6 has deployed and tested a mobility scenario including micro and macro mobility over IPv6. Several implementations of MIPv6 are considered mature and stable enough to perform deployment over Euro6IX test-bed.

- **Security components:** The sub-activities described below have deployed and tested security components in order to assess the maturity and suitability for integration in an integral IPv6 security framework.
    - A4.1-3 Deployment of Static VPNs and Security: The sub-activity has deployed and tested static IPsec/IKE VPN deployment and IPv6 firewalls. Some IPv6/IKE implementations are starting to be mature (KAME, 6WIND, FreeS/WAN), but not enough yet. Definition of architecture for VPN broker at IX based on policy based dynamic VPN management has started. IPv6 Firewalls and filtering policies needs further development and maturity.
    - A4.1-4 PKIv6: A Java based PKIv6/v4 service has been deployed which provides issuance, renewal, revocation and cross-certification of certificates for end users and software processes. PKIv6 is a fundamental component for the deployment of other security components, such as IPsec-VPNS, DNSSEC, AAA, etc.
    - A4.1-5 DNSSEC: DNSSEC is being investigated as a means to facilitate the deployment of an integral security infrastructure. A pilot of DNSSEC based on BIND has been setup to gain a better understanding, with the goal of starting the definition of an architecture, which assigns to an IX a certification authority.
    - A4.1-7 AAA for IPv6: AAA functions are necessary components for the deployment of mobility and are being investigated and validated in A4.1, with the goal of starting the definition of an architecture which assigns to an IX AAA functions.
- **Multicast and Anycast:** Sub-activity A4.1-2 has deployed and tested multicast scenarios over IPv6 with successful results. Additional research does not seem necessary and multicast is transferred to WP3 for experimental deployment over Euro6IX test-bed.
- **QoS over IPv6:** During the first year sub-activity A4.1-2 has deployed and tested QoS implementations for DiffServ, which seem stable and mature. The main issue is at the SLA negotiations between providers at IXs. The sub-activity has also investigated the use of flow labels without concluding results.

1.4 Summary of A4.2: IPv6 Application Development

A4.2 groups all the research, development, adaptation, enhancement, maintenance and validation of applications which are considered of relevance for the successful deployment and validation of the Euro6IX test-bed and Integrated Service Framework, as well as for facilitating the transition to IPv6. The summary of results produced in A4.2 during the first year of the project is as follows:

- **Basic Applications:** Sub-activity A4.2-1 has gathered a set of IPv6 enabled basic applications, which will be installed by all Euro6IX partners. The work has focused mainly in validating existing applications to select the ones which best support IPv6. The basic application set is available to third parties by means of the IPv6 repository. The basic application set includes: Web severs, clients and proxies; E-mail servers and proxies; FTP servers and clients; News servers and clients; IRC servers and clients; Secure shell; Network file systems such as NFS and Samba; LDAP directory.
- **Advanced Applications:** The sub-activities described below have been carried out in order to support the creation of a realistic set of end user services, which is used to validate the Euro6IX Integrated Service Framework, and for the realization of the trials.

  - A4.2-3 IPv6 capable audio-conferencing: The sub-activity has studied and experimented with SIP based IPv6 audio-conferencing. Several tools and libraries have been tested or ported to IPv6 if necessary, such as 6VOICE, VOCAL or jSIP. The activity will focus on the feasibility of deploying a SIP based VoIP over the Euro6IX test-bed.
  - A4.2-4 IPv6 capable ISABEL: The sub-activity focuses on the evolution of ISABEL to support and make use of all IPv6 features, such as security, QoS, Mobility, etc. The IPv4 dependencies still existing in ISABEL should be also removed. During the first year experiments for using and deploying ISABEL over IPsec-VPNs and with MIPv6 have been made. Isabel is used also as a Euro6IX working tool, to perform, distributed project meetings, workshops and public trials.
  - A4.2-5 IPv6 Unified Instant Messaging Systems: This sub-activity investigates the benefits of using IPv6 in unified and instant messaging. During the first year the following two activities have started. 1) Jabber IM has been ported to IPv6, because it conforms to existing standards (IETF CPIM and XML). 2) A P2P IM system has been built which should interwork with the first tool.
  - A4.2-7 Groupware applications: This sub-activity is performing the porting of a couple of representative tools, including: a shared collaborative space including doc repository, calendar, forums, groups, etc, which is called AGWS; the VNC remote application sharing tool; other packages and tools used by AGWS, such as the Postgress database. The goal of this sub-activity is to assess the state of porting of a representative set of open software developments and getting feedback about groupware application adaptation to the "Euro6IX Integrated Service Framework". During the first year the AGWS and VNC have been partially ported to IPv6 and integrated with PKIv6 and made accessible over the Euro6IX test-bed.

- **IPv6 Network Management and Operation Tools:** Sub-activity A4.2-8 has integrated two network management and operation tools to support the deployment of the Euro6IX test-bed. The first one is an SNMP network management tool called Magalia, which implements a distributed management model adapted to Euro6IX IX architecture. The second one is a network intrusion detection system that will implement IPv6 specific detection patterns.
- **IX Support Tools:** Sub-activity A4.2-9 has focused on the analysis and development of route server functions. Route servers are considered necessary for managing complex BGP mesh topologies at IXs and will be developed for inclusion in the Euro6IX test-bed. The sub-activity has investigated the functions of a route server, experimented with RPSLng, defined testing scenarios, developed an emulation environment and started the study for introduction of security in routing protocols.
- **Code Porting:** Sub-activity A4.2-10 has contributed to the porting or ported some libraries or software packages such as MRTG, DTD, PHP, Webalizer or Graphic trace router. Those portings are made available to third parties by means of the IPv6 repository, which has been set up in activity A4.2-11.

2. RESULTS ON ADVANCED NETWORK SERVICES

This section summarizes the main results obtained in WP4 in the context of activity A4.1, Advanced Network Services, during the first year of Euro6IX project. The subsections below outline the results of the different sub-activities under A4.1. More detailed information can be found in the associated Technical Reports referenced at the end of this document and available on the Euro6IX project web server.

2.1 Mobility over IPv6 Networks (A4.1-1)

Partners:

CONSULINTEL, PTIN, TILAB, UMU, UPM

Objectives:

This activity groups the work done around mobility services. The objectives have been:

- Review the status of macro and micro-mobility standards.
- Study and test new implementations mainly related with micro-mobility services.
- Study the feasibility of deploying a mobility service over the whole Euro6IX network.
- Test other Euro6IX services on top of mobility framework.

Description:

The aim of this sub-activity is to test both basic micro and macro mobility protocols operation. Both kinds of protocols complement each other, but macro mobility implementations are much more matured than micro mobility ones.

There is a strong demand to provide a mobility service in general and over Euro6IX network in particular to increase collaboration during the meetings without complex configurations requirements. So, it seems very interesting to make any kind of trials on this field in order to check the “state of the art” nowadays and get a lot of experience before the complete deployment over Euro6IX network.

The sub-activity has been divided in two tasks: local partner tests and multi-partner tests. The first was devoted to evaluate some implementation alternatives with different operating systems not only in macro but also in micro mobility field. The second task has been devoted to demonstrate the availability of Euro6IX network to support such type of services.

Therefore, basic MIPv6 operation has been tested in local test-beds of several partners, testing Home Agent (HA), Mobile Node (MN) and Correspondent Node (CN) functionality, using different implementations and testing interoperability and performance. In addition, multi-partner mobility tests have involved visiting mobile nodes from a home to a foreign network geographically distant in order to test the basic ‘roaming’ service. Additional test have covered mobility within foreign networks, so handovers and performance of re-registration to far HA have been tested. Another important issue that has been focused is the interoperability of different MIPv6 implementations: Linux, Windows, CISCO, 6WIND, etc.

Results:

MIPv6 tests have shown that analyzed implementations have a different stability and maturity level. In particular, the Microsoft implementation is still at a basic stage and far from providing a mobility support transparent to the applications. Many bugs have been individuated and it is still unstable. On the other hand, tests carried out over MIPL showed that this implementation has a good maturity level, since it is in accordance to the MIPv6 drafts and provides a mobility support transparent to the high layer protocols.

Therefore, MIPv6 is not a closed issue but a “work in progress” field as it was said in previous lines and this field was traditionally bound to developing environments like Linux. HUT is an excellent and well-known implementation example of MIPv6 on Linux. However, there is no compatibility between ICR IPv6 Stack for Windows 2000 and HUT implementation for Linux because first one is based on Mobility Internet draft 13 whereas last one is based on draft 15.

Future Work:

The main activity during the second year of the project will be the deployment a permanent MIPv6 test-bed between most of Euro6IX partners. The idea is to configure a Home Agent in each sub-network to allow participants mobility.

In parallel the objective will be to obtain throughput measurements from the known and future implementations, analyzing in particular micro mobility proposals over Linux and Windows XP. This activity will include the integration of micro mobility with macro Mobile IPv6 to increase service performance.

Finally, the sub-activity will analyze AAA framework and will study and how could it improve MIPv6 security.

More detailed information about “Mobility over IPv6 Networks” sub-activity can be found in [1].

2.2 Multicast over IPv6 Networks (A4.1-2)

Partners:

TID, T-NOVA, CONSULINTEL, UoS, PTIN

Objectives:

The main objective of this sub-activity is the integration of Multicast services in the Euro6IX network. Hence, intermediate aims are to investigate Multicast, verify the functionality of the IPv6 implementations, and allow the transport of IPv6 Multicast Traffic through the Euro6IX Backbone between the IPv6 Internet Exchanges.

Description:

Like IPv4, IPv6 uses also Multicast to distribute data to a group of receivers. However, the Multicast has in IPv6 a special significance, because IPv6 does not provide any broadcast mechanisms. Hence dedicated Multicast groups are used to implement broadcast-like mechanisms. Therefore the Multicast under IPv6 is not a special feature like in IPv4; it is a necessary component of the system. Jobs about Multicast have followed two main guidelines.

First of all, in order to verify the proper functionality of the IPv6 Multicast implementations and features of the networking infrastructure several test scenarios have been defined. These first scenarios were defined using a straightforward approach keeping in mind that more sophisticated investigations will be carried out in the later semesters of the project.

Besides, it must be noticed that the delivering of multimedia contents to multiple users has in multicast networks the natural way of work. That is why a video service streaming has been implemented, in order to test a multicast multimedia streaming service.

Results:

As regards to the investigation of the proposed scenarios, it has been only possible to implement and study the first, second and third proposed scenarios. From these experiences, the following statements can be done:

- There are a lot of easy to use IPv6 Multicast applications, which are well suited to verify the IPv6 Multicast functionality of a given scenario.
- The actual/used IPv6 Multicast applications were easy to compile and to install.
- The basic IPv6 Multicast functionality of Linux end systems works without any problems.
- The performance seems to be much more stable on Linux than for Windows. .
- Some scenarios need a very complex network infrastructure and can only be investigated if the whole Euro6IX network is up and running.
- There is more input needed from the other project partners in order to light up a broader scope of IPv6 multicast related issues.

About the multimedia streaming service, the video streaming server application developed and ported to IPv6 by TID, was adapted to multicast traffic. Besides, in order to be able of testing the service, the mplayer client for Linux boxes was ported to IPv6. In a few words, the result of the experiment was that the service worked perfectly over LAN networks separated by a multicast router as well as over VLANs. In the later case, it was necessary to develop a mechanism that permits multicast connectivity in unicast networks, because of the lack of multicast support for the majority of commercial routers today. Two new tools were developed: a Unicast/Multicast relay and the 802.1Q VLAN splitter.

First connections to the M6Bone have been established.

Future Work:

Depending on the network implementation and development, scenarios 4 and 5 will be performed during the next few semesters of the project. Furthermore the theoretical part of this deliverable will be completed in order to include more some statements to still open issues with respect to Multicast address allocation as well as IPv6 Multicast routing.

More router vendors will be asked for IPv6 Multicast capable implementations and the list of IPv6 Multicast applications will be completed.

The connectivity to the M6bone will be one of the main topics of the future IPv6 Multicast investigations because from the today’s point of view IPv6 Multicast is considered as one of the new Network Services, which could be implemented and offered to the customers, which are connected to an IPv6 Internet Exchange. In this sense, an approach for establishing IPv6 Multicast connectivity to the M6bone will be designed and implemented.

Inter-operational IPv6 Multicast trials together with the 6NET project have also to be defined and scheduled during the next 2 semesters of the Euro6IX project.

Regarding the video service, the implementation of a MPEG-2 Transport Stream video server, the addition of MPEG-2 Transport Stream de-multiplexing support to mplayer, as the development or porting a multicast video client to Microsoft Windows are planned. It will be also tested the use of “Traffic Class” and “Flow Label” fields.

More detailed information about “Multicast over IPv6 Networks” sub-activity can be found in [2].

2.3 Deployment of Static VPNs and Security (A4.1-3)

Partners:

UMU, UPM, CONSULINTEL, TID

Objectives:

This sub-activity has been divided in two different parts. The first part is related to **Static VPNs with IPv6**, and its main objectives are:

- To select the main IPsec/IKE solutions with IPv6 support and resume their features according to their web pages and public documentation.
- To define the IPsec/IKE scenarios, a plan of evaluation and a test suite.
- To realize the plan of evaluation for all IPsec/IKE solutions. We will generate test reports of interoperability and conformance. PKIv6 will be our public key infrastructure to test the IKE solutions using certificates.
- The reports will be grouped by scenario type, so if we need create an IPsec connection between two entities (hosts or secure gateways), we will have a complete report of multi-implementation environment that is possible.
- To approach to dynamic VPNs based on policies.
- To study how IPv6 VPNs could be deployed in an IX.

The second part is related to **Network Security**. The main objective of this part is to set the network security requirements in the Euro6IX network. This includes a description and analysis of network security elements (filters and firewalls) and the presentation of a network security model applicable in the Euro6IX context.

Description:

Related to Static VPNs with IPv6. IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

The IPsec protocols are designed so that different implementations should be able to work together, so IPsec was designed for interoperability. The evaluation of the interoperability between IPsec/IKE implementations is necessary to establish the scenarios that can be really developed.

We have analyzed the main IPsec/IKE implementations for IPv6 of the world and defined the basic scenarios where a host and/or a secure-gateway apply IPsec. We have evaluated the IPsec/IKE interoperability and the conformance of all proposal solutions. We have considered the below steps to evaluate the solutions:

- Step-1. Interoperability with uni-implementation environment.
- Step-2. Interoperability with multi-implementation environment.

Using a test suite we have checked the features and limitations of the implementations using different scenarios.

IPsec is the right way to protect the services and data communications of an IPv6 Internet Exchange but the IPsec configuration and administration are difficult and complex. The use of policy based VPN management provides a dynamic and automated mechanism to manage IPsec VPNs (dynamic VPNs).

Related to Security Network. This has been divided in two different parts.

The first part describes the existing IPv6 network security elements. Differences between filter and firewall features are discussed. Next, a complete list of IPv6 filters and firewalls are presented, where the main features are detailed. Finally, an IPv6 filter and an IPv6 firewall are selected to be tested, and the results obtained during the tests carried out in order to check these firewalls features are presented.

The second part presents a generalized network model applicable in the Euro6IX context. It defines interfaces between functional blocks and recommends network security measures both at these interfaces and at network elements to protect the network from attacks.

Results:

Related to Static VPNs with IPv6. The main result of this sub-activity is that now we really know the scenarios supported by the most representative IPsec/IKE implementations.

The main results of the evaluation are:

- There are several scenarios where the interoperability between different solutions does not exist and when it exists, the network throughput is worse. In that sense seems to be clear that it is better to use the same implementation.
- KAME and 6WIND provide the most complete IPsec/IKE support, but FreeS/WAN in the scenarios supported has better network throughput.
- The RTT (round trip time) charts show that the use of IPsec compared with the case of not using it, increase this measure in the band of 15%-20%. This value is not considered to be high. Furthermore, using authentication compared to the case of not using it increases the RTT lowly.
- Normally, implementations are manually configured. This is clearly creates a real disadvantage of IPsec compared to other solutions, as SSL/TSL or SSH.

The IPsec/IKE implementations are mature for IPv4 but currently they are not for IPv6, though there are a lot of efforts to get a full support of IPsec/IKE compliant RFCs in the IPv6 stacks.

An architecture of dynamic VPNs based on policies, seems to be the right way to build a VPN service in an IX. We have proposed a preliminary architecture that is the first step to develop a complete policy system, called VPN Broker, as an IX service.

Related to Security Network. The analyzed IPv6 filters and firewalls are still very far from their IPv4 equivalents and in some cases they are not enough tested. Porting IPv4 firewall features to IPv6 is not trivial as the protocol stacks IPv4-IPv6 are separated. IPv6 security is still considered as experimental and there is not enough staff working on it. Efforts should concentrate to provide full connection tracking. Another drawback is the lack of documentation. There are very few references related to IPv6 filtering or firewall.

Future Work:

Related to Static VPNs with IPv6. Our intention is to continue developing the architecture of Dynamic VPNs and to create the VPN Broker service in the IXs; we will do it in a new sub-activity for the next year called “Dynamic VPNs”.

Another important issue will be to link the work on VPN with the provision of services for IXs, and the integration of the VPN and, in general the security services, with another network services such as mobility and end-to-end applications. Also the relation and functionalities of services like Tunnel Brokers and its integration with the VPN services will be investigated.

Related to Security Network. The tested firewalls should be installed in a more realistic scenario in order to carry out more sophisticated tests. Other firewalls described above which have not been tested (i.e. Packet Filter for OpenBSD) should be tested.

More detailed information about “Deployment of Static VPNs and Security” sub-activity can be found in [3].

2.4 PKIv6 (A4.2-4)

Partners:

UMU, UPM, CONSULINTEL

Objectives:

The main objective is to design and deploy a complete Java-based PKI service with IPv6 support (PKIv6), allowing users and processes to carry out a complete group of cryptographic operations. The main services to offer will be: issuance, renewal and revocation of certificates for both end users and software processes, LDAPv6 directory support, and use of smart cards for end users. Besides, advanced services should be included, like OCSP, TSP, cross-certification and Attribute Certificates support.

Description:

The target of a PKI is to provide Public Key Certificate (PKC) management to the group of security protocols designed to protect Internet. These protocols, as IPsec, SSL, TLS or S/MIME use public key cryptography to provide services such as confidentiality, data integrity, data origin authentication and non-repudiation. Users of public key based systems must trust in a PKC, which is a data structure binding a public key to the user's subject. This binding is achieved by having a trusted CA that verify the subject identity and sign each digital certificate. A PKI infrastructure includes software, people, policies, hardware, etc, allowing the creation, management, store, distribution and revocation of public key certificates.

An important extension to a PKI, is the cross-certification. This is a way to extend trust between Certification Authorities. It is used to allow client systems or end entities in one administrative domain to communicate securely with client systems or end users in another administrative domain. There are two methods to extend this trust: peer-to-peer cross-certification and hierarchical cross-certification.

Other important extension to a PKI is the support of attribute certificates (AC). An AC is a data structure containing a set of attributes for an end-entity and some other information, which is digitally signed by the Attribute Authority, which issued it. This powerful architecture allows users to access information in relation to their certificate's attributes.

PKI over IPv6 communications is necessary to offer security services to final users/entities using IPv6-only communications. One of the most important advantages is the access to digital certificates to entities wanting to create VPN using IPsec/IPv6. Besides, now it will allow communications between PKIv6 components are in the network level using IPsec and not using application level protocols like SSL or SSH.

Results:

UMU has released the first IPv6-only fully supported implementation of a Public Key Infrastructure, PKIv6. This PKIv6 is being currently tested as a basic security service for static and dynamic IPv6 VPNs, Mobile IPv6 implementations and AAAv6 frameworks. It is also being used with high-level applications such as collaborative environments and videoconference applications.

The main characteristics are:

- Users can issue, renew and revoke certificates.
- LDAPv6 repository support.
- Smart Cards support to end-users.
- Policy definition to establish the opportune restrictions inside an organization.
- PKIv6 has been developed completely in Java language.
- SCEP protocol and 6WIND VPN routers supported.
- Cross-certification allowed (peer-to-peer and hierarchical cross-certification).
- Communications between components are over either IPv6 or IPv4.

PKIv6 is an important service inside the Euro6IX project for two reasons. The first one is PKIv6 will allow the establishment of trust relationship between involved partners (IXs and ISPs), offering an easy way to exchange secure information. The second one is PKIv6 will be an advanced service that ISPs could offer to their end users which will be able to make use of public key certificates.

Future Work:

The first action should be the establishment of real scenarios inside de Euro6IX project, where involved entities will be able to establish trust relationship between them and they will be able to offer certification services to end users. Another basic service should be included, like DNSSec support. In this service a PKI should be able to publish certificates in a DNS environment and users could be able to retrieve them. This is particularly useful in ISP environments.

More detailed information about “PKIv6” sub-activity can be found in [4].

2.5 DNSSEC (A4.1-5)

Partners:

UPM, UMU, CONSULINTEL

Objectives:

This sub-activity is centered around secure DNS services based on DNSSEC extensions. Its main objectives are to:

- Study the status of initiatives, standards and implementations related with secure DNS services.
- Set-up a limited secure DNS pilot experiment over Euro6IX network to study the behavior of available implementations and gain experience in the configuration and management of a secure DNS service.
- Study the feasibility of deploying a secure DNS service to the whole Euro6IX network and how to integrate it as a service inside IXs.
- Develop a tool to allow the emulation of complex DNS scenarios inside one computer and create a set of examples to help in the understanding and deployment of IPv6 DNS services.
- Study the use of a secure DNS service to publish digital certificates in cooperation with a PKI.

Description:

Domain Name System (DNS) is a critical service for the Internet to work properly. During past years several security weaknesses related to DNS protocols and their implementations have been discovered. Possible attacks include: faked answers that redirect clients to different servers from the ones they try to connect to; the poisoning of DNS caches, with a similar result; or just denial of services (DoS) attacks.

There is at present a strong demand to secure the Domain Name System (DNS), in order to provide them with data integrity and data origin authentication. In recent years, several extensions have been proposed to secure DNS by means of the use of cryptographic digital signatures, like Transaction Signatures (TSIG) that add security to DNS transactions by means of hash functions, or DNSSEC extensions, that propose the use of public key cryptography to provide data integrity and authentication to secure aware resolvers and applications.

In view of the importance of the deployment of secure DNS services based on these extensions, it was decided to start a new sub-activity inside WP4 during the second semester of the first year to study the initiatives, standards and implementations available and set-up a preliminary test-bed, with the long-term objective of deploying a secure DNS service over the Euro6IX network.

The most widespread DNS implementation in use nowadays is *Berkely Internet Name Domain (BIND)*. It has been selected for being tested in this sub-activity because, apart from being the DNS “reference implementation”, includes support for security extensions (TSIG, DNSSEC, etc) and IPv6. However, as concluded from the preliminary results and described in detail in this sub-activity Annex, it lacks some important functionalities related to security and to IPv6.

Results:

Work invested in DNSSEC sub-activity during the second semester has been basically devoted to get experience on the configuration and management of DNSSEC using BIND and to set-up the necessary infrastructure to run a limited pilot service over Euro6IX test-bed. Specifically, the activities carried out have focused on:

- Development of a **DNS emulation environment**, to allow the creation inside one computer of complex DNS scenarios made of complete name server hierarchies. Apart from its specific use as a tool for testing DNSSEC scenarios and configuration alternatives, the preliminary version of the tool has shown to be very useful:
    - As a general **DNS testing tool** to test complex DNS scenarios over a single machine, without involving several different computers or interfering with production services.
    - As a **DNS training tool** to easily test DNS example configurations in isolated environments, speeding up the DNS learning process.
    - As a tool to help the **operation of DNS servers**. DNS managers could use such a tool to maintain an “emulated copy” of their DNS servers, allowing them to test changes before deploying them to real servers.
- **Local tests** made by each participating partner inside its test-bed network, in order to acquire the basic know-how and to create the basic infrastructure needed for a DNSSEC service. These tests, together with the ones made over the emulated environment, have allowed the creation of basic “cookbooks” about how to configure and manage DNSSEC.
- **Inter-partner tests** over the Euro6IX network. Based on the know-how acquired in the local and emulated tests, a limited pilot service between the three partners involved in this sub-activity was created. Although only basic tests have been carried out over it, this pilot service will be used during the second year to do deeper tests, concentrating on service management procedures (key synchronization and distribution, foreseen and unforeseen key changes, etc).

The dual approach we have followed –doing tests over an emulated environment and over real networks– has shown to be powerful and versatile. It has allowed us to test and debug the configurations locally before deploying them to the different sites, with the resulting saving in time. Besides, when a problem is detected over the real network test-bed, the real configurations can be reproduced over the emulated environment in order to diagnose and experiment the solutions that later be implemented over the test-bed. The approach has been very useful in the activities carried out till now; but we think it will be even more useful for next year activities, when the pilot experiments will involve a higher number of domains, servers and organizations.

Future Work:

The main activity during the second year of the project will be the deployment of a secure DNS service over the Euro6IX network. For that purpose, a limited service restricted to partners participating in this sub-activity will be deployed, in order to mature the management procedures and generate the documentation and recommendations necessary for extending the service to the whole network under the scope of WP3.

Moreover, effort will be invested also in the improvement of DNS emulation environment, in the study about how to integrate DNSSEC as an IX service and the study of approaches to publish certificates using DNSSEC.

More detailed information about “DNSSEC” sub-activity can be found in [5].

2.6 QoS over IPv6 (A4.1-6)

Partners:

CONSULINTEL, PTIN, T-NOVA, UPM

Objectives:

The main objectives of this sub-activity are:

- Evaluate the current status of the actual standards and implementations (end systems, routers) with respect to IPv6 QoS functionality.
- Evaluate actual IPv6 applications, which use Flow Labels or DiffServ.
- Investigate the current possibilities for an IPv6 QoS deployment using Flow Labels and Traffic Classes.
- Investigate the possibilities of IXs to support IPv6 QoS.
- Deploy IPv6 QoS services in the Euro6IX test-bed.
- Test and evaluate the interconnection of different DiffServ administrative domains.
- Deploy bi-directional services (as far as possible) and investigate the influence of routing and signaling protocols/routes regarding quality levels.
- Evaluate the conformance of SLAs (Service Level Agreements) for real-time applications.

Within the proposed objectives, we are special interested in to accomplish:

- Extend know-how in using and implementing IPv6 QoS services.
- Deeper knowledge about the impacts in networks of IPv6 Flow Labels and Traffic Classes.
- Achieve the QoS expected for each class of service, accomplishing the previously established SLAs.
- Proper behavior of real-time application such as VoIP, video, etc., using premium classes.

Description:

With the rapid growth of the IP based networks there has been a large focus on providing necessary network resources to certain applications. Real-time applications often do not work well across the Internet because of variable queuing delays and congestion losses. The Internet, as originally conceived, offers only a very simple Quality of Service (QoS), point-to-point Best Effort (BE) data delivery. This basic IP best-effort mechanism, assumed by default either for IPv4 or IPv6, doesn't provide natively the capability to differentiate the traffic. Before real-time applications such as Voice over IP, remote video, multimedia conferencing, visualization, and virtual reality can be broadly used, the networks infrastructure must be modified to support real-time QoS, which provides some control over end-to-end packet delays.

One of the most highlighted IPv6 advantage is the build-in QoS functionality, which manage better the traffic compared to IPv4 Best Effort feature. This enables IP-based real-time and multimedia applications. In IPv6 header [RFC2460] are two QoS-related fields: Flow Label and Traffic Class.

Currently, DiffServ is probably the most viable solution to implement QoS in a scalable way. In IPv4 environments, DiffServ platforms are more or less well tested. So the goal is to test in the same way some IPv6 implementations. Conformance and interoperability tests should comprehend at least the standard CoS (Classes of Service): EF (Expedited Forwarding), AF (Assured Forwarding) and BE (Best Effort).

In a first phase, the tests can be achieved using traffic generation tools, obtaining detailed information about the behavior of the different flows. In a second phase, the evaluation can be performed using “real traffic”, through the use of voice, video or other applications provided by the A4.2 activity.

For completing the task objectives, IPv6 QoS will be enabled within Consulintel, PTIN, T-Nova and UPM site networks and the within Euro6IX backbone. In this scenario several tests and investigation will be performed in order to gather knowledge about the actual status quo of IPv6 Flow Label and Traffic Classes support. Heterogeneous end systems will be used and also routers from different vendors.

Results:

The main result of this sub-activity can be summarized as follows:

- Currently we have studied several QoS related terms, in special about DiffServ, and the current status of standardization of IPv6 Traffic Class and Flow Label fields.
- We have analyzed public information about some available IPv6 QoS tools for both open-source and commercial solutions.
- We have defined two general tests scenarios based on DiffServ, one focused in DS Edge tasks and other focused in DS Core tasks. The tested open-source solutions for IPv6 DiffServ are the implementations of FreeBSD, KAME and ALTQ. And the commercial ones are the implementations of Cisco, Hitachi and NEC.
- The tests performed during this first year, are just conformance tests to assess the DiffServ model working and to test the capabilities in order to provide differentiated services to the final customers. The same tests will be performed using other designs and platforms to evaluate and compare the correctness of all functionalities. This way, will be easy to know what the best deployment for a particular functionality are and what the best to do another one.

Future Work:

The IPv6 QoS sub-activity will be continued along the next semesters in order to keep on the overall development of our tasks. We will focus on:

- Evaluate actual IPv6 applications, which use Flow Labels or DiffServ.
- Investigate the possibilities of IXs that support IPv6 QoS.
- Deploy IPv6 QoS services in the Euro6IX network.
- Deploy bi-directional services (as far as possible) and investigate the influence of routing and signaling protocols/routes regarding quality levels.
- Participate in internal and external trial that validate our QoS test scenarios and implementation on Euro6IX.

Furthermore, there are two important areas of study that Euro6IX is interested:

- Other uses of the Flow Label field, which may be useful for aggregated flows.
- Possible additional header types, using the “Next Header” construction of IPv6.

We will enable a more complete test-bed involving in a first step the site networks of T-Nova, PTIN, Consulintel so as to measure the real impact and performance of a QoS-enabled router in the usage of a network. Using a traffic generator and then a real videoconferencing application (Isabel) we will to estimate the impact of such technology on the numeric performance of the application. In a second step, several site networks, in addition of Euro6IX backbone, will participate in a test-bed with one DS domain. Lastly, in a third step, we will test a multi DS domain architecture within Euro6IX.

More detailed information about “QoS over IPv6” sub-activity can be found in [6].

2.7 AAA for IPv6 protocol (A4.1-7)

Partners:

UMU, UPM

Objectives:

In this semester, objectives defined for this sub-activity and stated in this deliverable document are:

- To gather information related with AAA architecture in order to get a clearer vision about it.
- To analyze several AAA protocols and possible infrastructure models, obtaining conclusions about which solution could be more suitable in order to support roaming networks and taking into account Mobile IPv6 as protocol supporting mobility.
- To analyze more deeply user authentication and IPv6 network access control through AAA by considering mainly Mobile IPv6.
- To define a basic AAA infrastructure based on the conclusions from the previous analysis and having in mind the design of the Euro6IX network.

Description:

AAA stands for Authentication, Authorization and Accounting. It defines a general architecture regarding to these three topics:

- Authentication: The act of verifying the identity of an entity
- Authorization: The act of determining whether a requesting entity will be allowed to access to a resource (for example a network)
- Accounting: The act of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation

These topics are especially important when we talk about mobility and roaming scenarios, because it is needed to be aware about which user/users can connect to a foreign network (**Authentication**) and what things they can do inside these networks (**Authorization**). Moreover, it could be also interesting to have a register about those movements for charging reasons (**Accounting**). Therefore, although there are several AAA-aware services/applications, we mainly focus on Mobile IPv6 and what it is needed for supporting AAA for Mobile IPv6. In this sense, several approaches has been already released so they are analyzed in order to compile information to obtain ideas, and conclusions which allow us to build a suitable AAA architecture for Euro6IX network and to contribute new ideas or proposals.

Results:

Our initial interest is mainly focused on trying to solve user authentication and access control problematic based on an underlying AAA infrastructure in order to support roaming mobile users. Initially, the deliverable document shows s a basic overview about the AAA architecture and related protocols in order to clarify concepts. After this initial analysis DIAMETER protocol has been envisaged as a candidate AAA protocol to support AAA infrastructures. Furthermore, some information has been compiled about integration about Mobile IPv6 and AAA (see chapter 5), particularly:

- Analysis has been obtained about some protocols, which allow carrying user/device authentication, and network access control information from a node (i.e. Mobile IPv6 node) to a back-end deployed AAA infrastructure. PANA has been explained as the standard option and we envisage it as the best option to carry authentication information.
- Analysis about typical AAA infrastructures used for integrate both concepts. Two models have been selected in order to support Mobile IPv6: Roaming Case-Pull Sequence and/or Distributed Service Case (see chapter 3).

On the other hand, we have exposed several basic ideas about how an AAA infrastructure could be deployed in Euro6IX network (see chapter 6). Our intention is that these ideas serve as beginning of discussion in order to define a suitable AAA infrastructure between different partners. The main idea is that each IX defines a macro-domain and it could have several customers or ISPs under its control. In his turn, an ISP could be divided into different sub-domains owning end users. User-related authentication, authorization and accounting information would be managed by AAA servers in each sub-domain. IX provides AAA servers in order to manage its own end users, AAA routers (relay/proxy agents) in order to carry AAA information between ISPs' AAA infrastructures, and finally it provides information about how to reach a particular domain through redirect agents. DIAMETER would be the protocol chosen in the whole AAA infrastructure. Finally, we have included a little example on how an available implementation of DIAMETER can be used.

Future Work:

Future lines of work inside this sub-activity follow:

- Obtain a more precise design of an AAA infrastructure for each IX in Euro6IX network.
- Design our own solution that allows users using Mobile IPv6 to be authenticated by an AAA infrastructure besides providing network access control. This initial design must be based on several gathered ideas extracted of this deliverable and future research about these topics. Trying to solve this problem may need to solve other problems as key distribution process between different AAA entities and Mobile IPv6 nodes in order to establish security associations. In fact, we will also deal with this issue. Due to the fact that one of the problems in Mobile IPv6 security is key distribution in order to authenticate Binding Updates and Binding Acknowledgements, designs should also aim to offer an alternative solution.
- To work on authorization and accounting, aspects that have not been considered in this analysis and early design.

More detailed information about “AAA for IPv6 protocol” sub-activity can be found in [7].

3. RESULTS ON APPLICATION DEVELOPMENT

This section summarizes the main results obtained in WP4 in the context of activity A4.2, Applications Development, during the first year of Euro6IX project. The subsections below outline the results of the different sub-activities under A4.2. More detailed information can be found in the associated Technical Reports referenced at the end of this document and available on the Euro6IX project web server.

3.1 Basic Applications and Services (A4.2-1 and A4.2-2)

Partners:

UPM, nGn

Objectives:

The objectives of this sub-activity were:

- The definition of a basic set of application and services each partner test-bed network should support.
- The selection of specific applications and operating systems to be used.
- The testing of applications in local and Euro6IX wide experiments.
- The maintenance of the set of applications during the life of the project, incorporating new versions, applications or services once they are available.

Description:

As stated in the Technical Annex, each partner has to set-up its own IPv6 test-bed network, including basic services and applications used in today’s Internet. In order to easy the deployment of these services, this sub-activity has coordinated the efforts invested in selecting, testing and maintaining a common basic set of applications.

Basic services covered by this sub-activity include: Web servers, clients and proxies; E-mail servers and clients, including e-mail access from web; FTP servers and clients; News servers and clients; IRC servers and clients; Secure shell applications, Network File systems like NFS or samba, etc.

Apart from basic applications oriented to the end user, this sub-activity has also selected and partly developed some tools oriented to help in the diagnostic of network problems. Basically, the effort has been invested in the development of a Looking Glass facility adapted to Euro6iX environment, which allows the remote execution of network trace tools like ping, traceroute or mtr, as well as the consultation of DNS and BGP related information from the point of view of any partner’s network.

Results:

The main tasks carried out in this activity have consisted in:

- The definition of the basic set of applications and services to be deployed in IPv6 test-beds and the selection of specific applications and operating systems to be used.

- The testing of some of these applications over local and Euro6IX wide scenarios and the documentation or just the annotation of the applications installation process in case it was needed.
- The development of a Looking Glass network facility, in order to help in the diagnostic of network problems.
- The development of a Web Mail Tool, in order to access IPv6 capable mail servers from the web.

The delays accumulated in the set-up of the Euro6IX network have delayed the complete deployment of the applications collected here. However, it is expected to have most of them running on every partner network during the first weeks of 2003.

Future Work:

The effort related to basic applications and services will be carried out in the future inside WP3. Besides, the maintenance and new developments of the Looking Glass and related applications will be moved to the "IX Support Tools" sub-activity. Therefore this sub-activity will not continue in the future.

3.2 Advanced Applications

3.2.1 IPv6 capable Audio-conferencing (A4.2-7)

Partners:

UPM, UoS, TELS

Objectives:

Audio-conference services are one of the key services any IPv6 network is going to offer to end-user. In the framework of Euro6IX, we have explored different videoconference applications in order to deploy videoconference services over IPv6 networks.

During the first year, this activity focuses on the creation of basic audio-conferencing applications that may be used for global experiments during the second year. Not only specific multimedia and communications code has been identified for porting and experimentation in the Euro6IX network, but key complementary elements are required for the successful deployment of VoIP services: SIP, SDP, and ENUM have been also investigated.

During the first year of this activity it is intended to study and evaluate VoIP services over IPv6, providing a complete set of component for the deployment of audio-conferencing services of the Euro6IX network.

The main objectives of this trial are:

- To port to IPv6 of a VoIP audio-conferencing system already developed for IPv4
- To provide a SIP support for the deployment of Audio-conferencing services over the Euro6IX network
- To enable IPv4 based services to interact with IPv6 services running at Euro6IX network
- Evaluate and demonstrate the correct operation of the application and its installation in several platforms.

Description:

Two audio-conferencing applications have been ported to IPv6: VOCAL and 6VOICE in order to investigate specific problems of porting audio-conference applications.

Telscom has developed 6VOICE, the IPv6 voice over IP application and has been tested across wide area networks end-to-end. The tests were also conducted using Diffserv and proprietary QoS flow label implementation system to test the impact of QoS models and it is important that voice like applications need the QoS inbuilt into the IP network for the good performance. This work comprises also the porting of some element for providing VoIP support such as SIP, SDP and RTP required for the deployment of the application.

The initial IPv6 porting for Vovida Open Communication Application Library (VOCAL) has been added by University of Southamton. The Vovida Open Communication Application Library (VOCAL) is an open source project targeted at facilitating wider adoption of Voice over IP technology (see http://www.vovida.org). UoS has made the VOCAL code IPv6-enabled, and fed that code back into the main VOCAL development tree, such that v1.5.0 will support IPv6 "out of the box".

The code has been run and tested by many groups, including BT Exact and TZI, and the code has shown to interwork successfully with the TZI SIP proxy and with BonePhone via the SIP proxy.

There are still some parts of the code left to port, but the bulk of the work is done. UoS aims to promote the use of VOCAL between 6NET and Euro6IX partners over the coming months, as a joint activity between the projects. UoS has also joined the UK ENUM pilot, and will seek to use IPv6 DNS and IPv6-enabled VOCAL in that pilot service. Lessons learnt from porting will be fed into the project "porting guide" document.

Finally we investigated the provision of general SIP services over Ipv6 networks. This work, performed by University of Madrid, was based on the Open source code library jSIP (http://jsip.sourceforge.net). This work intends to provide generate a SIP library IPv6 enabled, which allows the creation of mayor SIP elements (User Agents and Proxies); and to develop a mechanism for allowing interworking between IPv4 and IPv6 SIP.

We selected an OpenSource library (jSIP) which was originally developed for SIP over IPv4 networks and is implemented using Java. This provides some additional benefits such gaining experience in porting general purpose libraries, and not only final applications, and the development of general patterns for porting software which is much more general applicable when porting general software than when porting ad-hoc applications.

Finally the final library has been evaluated by the creation of key SIP elements such as UAs and Proxies, enabling the creation of a Sip service provision environment, which will be further investigated for interworking between IPv4 and IPv6 audio-conferencing applications, using the feature of the new library.

Results:

This activity explored the porting of Audio-conferencing applications to IPv6. Due to the importance of session negotiation in this framework, SIP porting has been also deeply investigated.

Two applications and one general purpose SIP library have been ported to IPv6. The combination of these experiments provides the basic for building more complex scenarios during the second year of the projects, and basic pieces developed during this first year are ready for being used in the global experiment of Euro6IX.

Porting Audiconference applications involved not only working with basic communications and multimedia code, but also some key standards such as SDP, SIP and ENUM are involved. Those services may be used, and in deed they will be mandatory, for many other services that will be deployed in future IPv6 networks.

Nevertheless the porting activities have not being completed several lessons have been learned, which will be fed into the project “porting” guide document. Those experiences include: porting of multimedia and communication code, porting of VoIP required elements such as SIDP and SDP, porting of general purpose libraries and experience in de creation of transition scenarios for SIP based services, where IPv4 and IPv6 elements will coexist for a long time.

Future Work:

Results of this first year work will be completed during second year, and will be included and evaluated in the Euro6IX network during second year. More detailed information about “IPv6 capable Audio-conferencing” sub-activity can be found in [8].

3.2.2 IPv6 capable ISABEL (A4.2-9)

Partners:

UPM, UMU

Objectives:

This sub-activity focuses on the evolution of ISABEL application to support and make use of the IPv6 features, such as security, QoS, mobility, etc, that will be offered by the Integrated Service Framework created over the Euro6IX network.

During the first year, work has concentrated on adding security capabilities to ISABEL, although some preliminary studies about ISABEL over mobile scenarios have also been made.

Related to security, this year objectives were:

- To initiate a general study about how to adapt ISABEL collaboration tool to allow secure communications over the IPv6 security framework being developed on the context of A4.1 activity.
- To test and demonstrate ISABEL over IPsec scenarios based on IKE network services using pre-shared keys, as well as to evaluate its behavior and performance.
- To integrate the set-up of IPsec tunnels inside the ISABEL general set-up procedure.

Related to mobility, this year objectives were:

- To study and test ISABEL application behavior in a simple mobile scenario where a mobile node participates in an ISABEL session. In particular, the study will concentrate on application behavior and performance during handovers.
- To define the requirements for Correspondent Nodes and central nodes like Flow Servers and MASTER node.

Description:

Security is a key service to be offered by the Integrated Services Framework of Euro6IX network. As described before, several experiences related to security have been initiated in the context of A4.1. For example, IPsec based VPNs have been experimented, ensuring confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPsec, which is mandatory for IPv6, is the framework of open standards for ensuring secure private communications over IP networks.

However, there is a lack of security aware applications, especially when speaking about multimedia applications, that makes difficult to experiment and evaluate security services in real scenarios.

The ISABEL CSCW application is a group communication tool for the Internet, based on advanced videoconferencing features. ISABEL allows efficient organization of working procedures over the Internet in large enterprises or groups. ISABEL has been ported to IPv6 on the context of IST LONG project.

However, ISABEL, as many other multimedia applications, lacks security support in its data or control communications. That is to say, communications are not protected in any way and therefore no confidentiality, integrity, or authenticity is offered as an application service.

Being ISABEL a complex application, involving multiple multimedia and data control flows in a great variety of possible topologies, it is a very good candidate to be used to test security services in Euro6IX project, apart from the added value of developing a secure ISABEL application.

For all the above reasons, the main objective of this sub-activity is the adaptation of ISABEL to take advantage of network security services, in order to offer secure communications to the user. For the first year, simple configurations and scenarios have been used, mainly based on IPsec and IKE using pre-shared keys using a star interconnection topology.

For that purpose, new security parameters have been added to ISABEL sessions, being the main one the pre-shared key that is known by all participants. The MCU and master terminal, located at the central point in the star configuration, create each one an IPsec tunnel for each participant, therefore, each terminal maintains two secure tunnels. Other security parameters can be configured with default values, for example 3DES for data encryption, HMAC-SHA1 for data integrity, and other values for IKE parameters.

Besides, work has been invested in studying the behavior of an IPv6 Mobile Node connected to an ISABEL Session, focusing on how to maintain the communication during handovers. As in the case of security, only simple star based scenarios have been studied. Due to the network architecture of ISABEL, an ISABEL Node does not require connectivity with all the other participant nodes, only with a central control node called the “Master” and a “FlowServer”, which acts as data distribution center. So, a mobile node participating in an ISABEL Session would keep TCP and UDP communications with the Master and Flowserver (MCU) systems. Consequently, at least these two systems, apart from the mobile node itself, will need basic Mobile IPv6 support when simple star interconnection topology is used. For more complex scenarios more systems will need to support mobility.

ISABEL does not require special modifications for supporting IPv6 Mobility, since it is an IPv6 enabled application. In principle, the mobility is transparent for ISABEL.

However, the main problem is the loss of connectivity the mobile node experiments during handovers. The loss has typically a variable duration around few seconds, but it can take minutes sometimes. Apart from the effect on multimedia data (audio and video), if the handover takes a long time, the effect is very problematic on the TCP control connections between the Mobile Node and the ISABEL master, as the mobile node can be even disconnected from the session. So it is critical to have a bounded handover time and adjust application timers according to it.

A more detailed description of the experiments made to evaluate ISABEL behavior in mobile scenarios can be found in the Technical Report [1] that describes the detailed results of Mobility sub-activity of A4.1.

Results:

Secure ISABEL sessions using IPsec have been successfully demonstrated in a trial (documented in deliverable D4.3 [12]) using FreeS/WAN implementation. A specific tool, named *isabelvpncfg*, has been developed to take care of the IPsec configuration, determining the IKE parameters and inserting the pre-shared key in the system.

This tool has to be used manually from the session terminals to configure the tunnels before the session is up. Once the tunnels are established, all ISABEL sessions started use IPsec secure data channels to communicate with the master and flowserver nodes. This tool is being integrated at present inside ISABEL application to automate the process.

As mentioned before, in the scheme designed the responsibility of initiating the secure communications resides on the terminals, which are in charge of establishing the secure communications to the flowserver and to the session master. The designed scheme has been tested locally in local network test-beds and also between two Euro6IX partners (UMU and UPM). The application behavior using secure communications was very similar as it is over traditional insecure scenarios. Therefore, no performance problems have been observed when powerful workstation is used.

The main problems experimented were related to the simultaneous configuration of IPsec services and drivers for audio and video boards. FreeS/Wan IPsec services require a specific Linux kernel version together with specific modules loaded that conflict with driver's requirements. That made the workstation installation very difficult or almost impossible when using some Linux distributions. However, this problem it is expected to disappear when IPsec is included as standard module in Linux distributions (late tests made with distributions available at the end of 2002 showed some simplifications in this aspect).

Related to mobility, the preliminary experiments made have allowed assessing the correct behavior of ISABEL application over simple mobile scenarios based on start topology configurations. As experimented, after each handover, the mobile node stops receiving traffic for few seconds, but it keeps connected to the session, and goes on receiving traffic once the handover has succeeded. Handover times measured over WLAN networks were not long enough to break the TCP control between the mobile node and the Isabel master.

In summary, the behavior of the application was basically as expected: the UDP data traffic was lost during handover, therefore video and audio signals experimented interruptions, but TCP control connections kept alive.

Future Work:

ISABEL has been successfully secured when working over star interconnection topologies. However, ISABEL is able to work over much more complex scenarios based on trees and multicast topologies. Tree topologies allow the interconnection of any number of ISABEL nodes using Flow Servers as intermediate nodes. Besides, ISABEL can interconnect all or part of participant nodes using multicast network services. Therefore, there are two pending tasks.

The first task is the adaptation to a general tree interconnection topology, defining how to distribute shared keys or designing a new authentication procedure. There are two possible solutions. The first solution is to try to integrate the tunnel creation and set up within the ISABEL EDL language -used to define the sessions, participants and other general characteristics-. The extension of this description language will be necessary in order to include the specification of the security parameters. The second solution is to progress in the use of digital certificates X.509 within the VPN security services as an alternative to the use of pre-shared keys. The second task is the study definition of secure communication environment over multicast networks.

Related to mobility, future tests will concentrate on more complex ISABEL scenarios, where, for example, the main nodes, a FlowServer or even a Master, are also mobile nodes. In this case, all participants will need IP mobile support, as all of them communicate directly with the central nodes. Besides, deeper investigations could be made in order to reduce handover effect, for example, giving priority to audio flows over video.

More detailed information about “IPv6 capable ISABEL” sub-activity can be found on [8].

3.2.3 IPv6 Unified Instant Messaging Systems (A4.2-4 and A4.2-8)

Partners:

UoS, nGn

Objectives:

Here we define "Unified Instant Messaging" as a general messaging service among peers over the Internet. The peer represents the person using or the application running on various kinds of devices. And the goals of the Euro6IX work being done by UoS and nGn in P2P and IM systems are described as follows:

The Unified Instant Messaging system. For UoS, the Unified Instant Messaging system proposed would contain the following features:

- Messages are precisely formatted using XML.
- Messages between peers are asynchronous, concurrent, reliable and real-time.
- Peers can exchange messages with peers on the Internet at any time, anywhere or even while they are on the move.
- Properties such as presence and message communication should follow interoperable IETF standards.
- Security and privacy should be guaranteed.
- For different P2P application requirements, different messaging models (C/S. pure decentralized, hybrid) should be provided.

The objective of the Unified Instant Messaging System, is to develop a network platform for messaging over IPv6, and then, use that platform to develop an Agent-based Unified Instant Messaging service for P2P applications. We will start with Instant Messaging (C/S messaging model) for users, then extend it to other messaging models and more general messaging services.

A complete Peer-to-Peer system. For nGn, the objectives of this sub-activity are:

- To study how to apply mobility and messaging in IPv6 to P2P tools, and demonstrate the advantages and benefits of the use of IPv6 in this type of applications.
- To coordinate with the obtained results by IPv6 Mobility sub-activity in A4.1 and with Unified Messaging System (6UMS) sub-activity of UoS (see above) in A4.2.
- To develop a complete P2P Instant Messaging application using the libraries developed.
- To study the possibilities to use P2P Instant Messaging between devices of different types, mobile telephones, PDA, Digital TV, etc. We will try to use XML to develop a complete structure of libraries in this sense.

Description:

Instant Messaging (IM) has become one of the most popular tools for people to communicate with peers over the Internet. Instant messaging differs from ordinary messaging such as e-mail in that it enables the immediacy of the message exchange and also enables a continued exchange.

Some most popular Instant Messaging systems include AOL Instant Messenger, ICQ, Windows Messenger and Yahoo Messenger, etc. Up to now, there have been several working groups and bodies which focus on Instant Messaging, such as the IETF IMPP working group, the Jabber software foundation, the IETF SIMPLE working group, and Wireless Village.

In addition to the Instant Messaging system which provides the typical P2P (Peer-to-Peer) services for users, nowadays the Peer-to-Peer (P2P) applications are becoming more and more pervasive, such as Napster and Gnutella for file sharing, GRID and distributed computing, JXTA which is to provide a collaboration platform, and Web Services, etc. In all these P2P systems, messaging is the main mechanism for the information delivery between peers. Different P2P applications need different kinds of messaging model, such as client/server model, pure decentralized model, and the hybrid model.

With more and more users and devices, especially 3G mobile handsets and pervasive devices, being connected to the Internet, a much larger amount of globally routable IP addresses is needed. However, the existing messaging systems are built over IPv4. The limited IPv4 address space will be the bottleneck of future P2P messaging systems. Network Address Translation (NAT) is not a good solution for P2P systems because of its poor scalability and lack of end-to-end transport mode IPsec security; devices trying to communicate into NAT networks face many problems. IPv6, the next generation Internet, provides a huge address space that allows each individual device to have its own globally routable IP address. In addition, it provides several advanced services, such as mobility, security, multicast, stateless autoconfiguration, etc. Thus the research and development of Messaging systems over IPv6 is of great importance.

Results:

Both UoS and nGn are now developing Instant Messaging systems over IPv6. nGn has a very early prototype developed.

Unified Instant Messaging. For UoS, the Unified Instant Messaging system is based on the Jabber IM system at this stage. The main reason of choosing Jabber IM is simply because Jabber provides open source code and it conforms to the IETF CPIM standard. However, Jabber IM is IPv4-based. It has no mobility support and security guarantee, and there is a lot to do to improve its performance. Up to now UoS has:

- Built up an IPv6 based networking environment, including IPv6 connectivity, mobile connectivity, etc over which IM system will be running.
- Deployed the basic Instant Messaging protocol using Java and XML.
- Deployed the basic Instant Messaging Server based on Jabber IM.
- Ported some of the Jabber based IM services to IPv6 platform, such as message delivery, presence state delivery, etc.
- Implement the basic Group Messaging over IPv6.

UoS has two Java development servers (Solaris and Linux) running JDK1.4.1 with IPv6 functionality; UoS is on the Sun CAP program to gain early access to new Java developments.

Towards a peer-to-peer system. For the application of Instant Messaging nGn has developed a prototype including IPv6 functionality, to demonstrate the appropriate working of IPv6-based connections, as the first step towards a complete peer-to-peer application. The current state of the sub-activity is as follows:

- Adapting GUI.
- Developing multi-session capability.
- Including presence service in the system.
- Including ‘white papers’ information.
- Preparing documentation to allow us to coordinate our work with 6UMS sub-activity.

Apart from that, nGn has also made a study about how to integrate P2P applications features into standard e-mail, in order to create a P2P Mail Tool. IPv6 protocol favors these features due to: Huge address space, MIPv6, autoconfiguration and security of IPv6 networks.

Instant Messaging specific developments for P2P applications, like the presence protocol, will be used too for P2P Mail Tool, defining and creating a common service to both. Current e-mail applications are based on client/server model using the scheme:

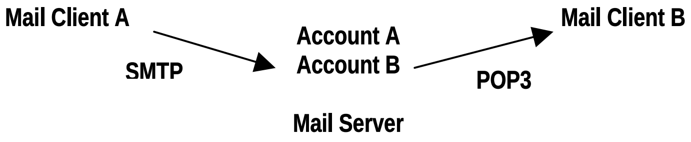
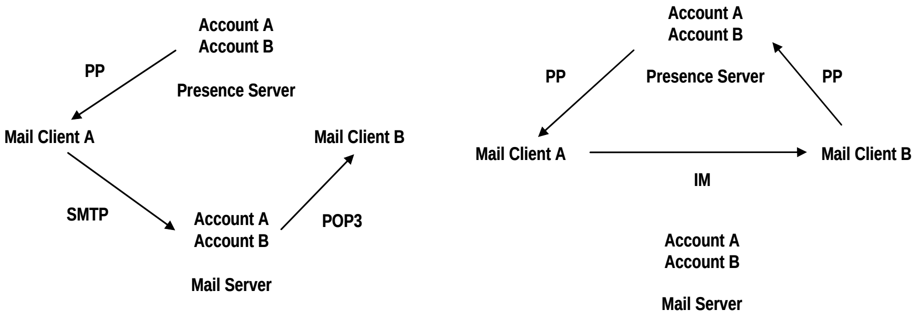


Figure 3-1: Client-Server Model

P2P Mail Tool will follow this other scheme:



a) User B off-line b) User B on-line

Figure 3-2: P2P Model

This is a way to integrate Mail Services and Instant Messaging Services. Currently, Mail Services are the most used services by final users and Instant Messaging systems are seen as most rising kind of applications, within IPv6 networks, thinking on final users too. So, the P2P Mail Tool deployment can become in a main way to increase network traffic and to get final users.

Future Work:

IPv6 applications play an important role of getting IPv6 accepted by end users. The IPv6 Unified Instant Messaging system aims at the vision of providing advanced messaging services for peers to exchange information, share resources and cooperate. We leverage the advantages of IPv6 in the context of IM, namely its suitability for Peer-to-Peer communications through expanded address space, improved Mobile IP, autoconfiguration, and support for IPsec and Multicast.

We propose to build an agent-based unified IM system on top of this IPv6 networking platform, using IETF standards for presence and per - communication session initialization, for maximum interoperability. We expect to re-use some existing components where possible, and to build prototype components towards trials of a working system in the scope of the Euro6IX project. Up to now some of the IM services have been developed over IPv6 networks, based on which the completed IPv6 Unified IM system will be implemented in the near future.

The P2P system being developed also under this activity will also follow IETF and related standards where possible. By using such open standards, and agreeing common message exchange formats, we expect the two messaging applications being developed to be interoperable.

In the near future, UoS plans to continue the research and development of an IPv6 Unified IM system in the following areas:

- Deploy and implement a prototype of IM system over IPv6 based on the Jabber IM system (in the future, a SIP-based IM will be deployed), which includes Presence service, Info/Query service, Client Registration and Authentication, etc.
- Improve the Group chat service by making use of the multicast services provided by IPv6.
- Research and develop Mobile IM services including mobile messaging, mobile presence management, mobile IM over ad hoc networks, etc. Mobile IPv6 itself is being studied under A4.1, and UoS has its own MIPv6 test-bed.
- Research and deploy the end-to-end security mechanism for IM based on IPsec; this should be provided by other project partners, from work done elsewhere in the project.
- Research and compare different messaging models (C/S, pure decentralized and hybrid) in terms of performance and their effects on different P2P applications.

For nGn, they will continue working to finish current open issues and complete their P2P application:

- We plan to coordinate this activity with the activity Unified Messaging System (6UMS) studied in A4.2 Application Development Sub-activities with the objective of getting an Instant Messaging application completely integrated in 6UMS, exchanging different data types, sharing files and publishing connection status. Mainly focused on defining common protocols, Unified Messaging System and Instant Messaging would be much more related tasks.
- In a further stage we will study to include security considerations in data exchanges.

More detailed information about “IPv6 Unified Instant Messaging Systems” sub-activity can be found in [8].

3.2.4 IPv6 Groupware Applications (A4.2-5 and A4.2-6)

Partners:

UPM, UMU

Objectives:

This sub-activity is performing the porting of a couple of groupware representative tools, including a shared project space called Agora Groupware Web Server (AGWS), which includes doc repository, calendar, forums, groups, etc, and the Virtual Network Computing (VNC) remote application sharing tool. The general goal of this sub-activity is to assess the state of porting of a representative set of open software developments and getting feedback about groupware application porting.

The particular objectives of the sub-activity during the first year were:

- To port AGWS to IPv6 and to integrate it into the Euro6IX security framework, including confidentiality, data integrity, data origin authentication and non-repudiation services.
- To analyze the issues and problems arising from the porting to IPv6 of a collaborative web based tool.
- To analyze the issues and problems arising from the integration of AGWS into the Euro6IX security framework.
- To port VNC application to IPv6, supporting Windows, Linux and Java versions.

Description:

AGWS (Agora Groupware Web Server) is a web based collaboration suite, which provides a rich set of collaboration functions accessible from a standard Web browser and is therefore a good example of a Web collaboration tool. It has been chosen to validate the integration of collaborative tools into the Euro6IX service integration framework.

AGWS supports the creation of “collaboration spaces” which provide a virtual meeting place for teams in projects, distributed classrooms, groups or disperse enterprises. The AGWS server is accessed by standard Web access or email. Each collaboration space includes:

- A shared file repository with version control, notification, etc.
- A calendar of events and shared activities.
- A virtual room for sharing Windows™ applications in synchronous collaborations.
- Group management functions, including mailing list, group repository, calendar, etc.
- A membership management function.
- Other support functions such as group and mailing list management, forums or voting.

The architecture of AGWS is based on an Apache Web Server, which provides access to the AGWS collaboration application. AGWS makes use of the following servers: a database (Postgres SQL or Oracle) accessed via SQL, a mail SMTP server and a ROOMS server, which uses VNC and chat servers. The database and the SMTP server are accessed via TCP sockets and can be hosted in the same machine as AGWS or in a different one. The ROOMS server is very CPU intensive and is usually installed in another machine, although it can run in the same machine as AGWS.

In order to port AGWS to IPv6 as well as to adapt it to use Euro6IX services framework, the following plan was designed:

- **Step 1: Enabling external IPv6 Access.** Porting of the external interface to IPv6 and support for email addresses mapped to IPv6 only domains. After Step 1 AGWS will support external access from IPv6 Web clients and will be able to send and receive emails from email addresses mapped to IPv6-only domains. Step 1 implies the porting of AGWS to an IPv6 capable version of Apache web server, and the connection to a properly installed and configured IPv6 capable SMTP mail server.
- **Step 2: Fully IPv6 compliant AGWS.** Make AGWS fully IPv6 compliant, avoiding any need of IPv4 addresses or connections in any part of it. This includes the porting of: The IP address check in AGWS license, the database interface, and the interface between the AGWS software and the ROOMS server.
- **Step 3: Integrating AGWS in the Euro6IX security framework.** Integrate AGWS with the IPv6 based Euro6IX security framework, such that it makes use of the standard facilities for confidentiality, data integrity, data origin authentication and non-repudiation services.

The integration of security into AGWS is based on the PKI developed by UMU, which allows certificate based user authentication, avoiding the need of user identifiers and passwords. The certificate of the CA can be included in the Apache web server as a trusted CA, without any specific developments in the AGWS. Therefore the adaptation of AGWS can be performed just reconfiguring the installation procedure. This step can be performed in parallel with steps 1 and 2.

VNC is a client/server remote display software package allowing remote network access to graphical desktops. Using VNC a user can gain access to his computer 'desktop' environment from anywhere on the Internet using a wide variety of machine architectures. VNC has lots of applications, either used isolated or combined with other applications. In our case, VNC is used as an integral part of the AGWS collaboration suite.

VNC application has client and server support for Windows and UNIX operating systems, as well as a platform independent java client named vncviewer.

VNC was originally distributed by AT&T Laboratories Cambridge. However, this sub-activity will concentrate on porting TightVNC, which is an enhanced version of VNC -grown from the VNC Tight Encoder project- optimized to work over slow network connections such as low-speed modem links. Besides bandwidth optimizations, TightVNC also includes many other improvements, optimizations and bugfixes over VNC. TightVNC is free, cross-platform and compatible with the standard VNC.

Although some work was already done to porting VNC to IPv6 (inside KAME project), it was neither available for Linux nor based on TightVNC version.

Results:

Steps 1 and 3 of the AGWS porting plan have been successfully performed, enabling external IPv6 access, as well as the integration of AGWS into the Euro6IX security framework. The HTTPS server provided with the application is now IPv6 compliant, so it can accept IPv6 browsers. The SMTP server has been integrated with the AGWS installation and can accept email addresses mapped into IPv6 only domains.

Besides, TightVNC has been completely ported, adding IPv6 support to VNC clients and servers running over Linux and Windows operating systems, as well as to the VNC java client (vncviewer).

Both applications were demonstrated in trial experiments described in [12].

Future Work:

This sub-activity will continue along the second year. In the case of AGWS, work will focus on completing the porting, dealing with step 2 of the porting plan. This step requires additional work and will begin exploring in detail the changes needed to fully support IPv6. Key points on the porting follow:

- An IPv6 enable DB server is needed, so available solutions must be explored. And the application needs to be changed to use such IPv6 DB server.
- The core application license mechanism needs to be reviewed, in order to allow the use of IPv6 addresses.
- The ROOMS working team must be contacted, to coordinate with them a joint porting to IPv6.

The main impediment for the realization of step 2 is the lack of support to IPv6 in Java applets for Windows. Therefore we will monitor the status of porting of Java 1.4 and the support for IPv6 on Windows browsers before performing the complete porting. The realization of step 2 will only start when this condition is fulfilled.

More detailed information about “Groupware Applications” sub-activity can be found in [8].

3.3 IPv6 Network Management and Operation Tools (A4.2-11 & A4.2-14)

Partners:

TID

Objectives:

The main objective is to develop applications for the management and security control of the Euro6IX backbone.

Description:

Magalia

Magalia is designed to have an SNMP monitor and management system of IPv6 networks. This application has been developed starting from zero (not adapting a free source one) to allow the implementation of an innovative modular design with new features to test within Euro6IX.

More exactly, Magalia will implement a distributed model, i.e. each IX runs a Magalia instance that sends authorized information to others. This feature is required in Euro6IX since the backbone is made of networks owned and managed by different Telcos but the experience will work also in other networks where “shared management” is required.

All of this control/monitoring over the network is made using IPv6 connections and SNMP queries. Thanks to Magalia modular design, the modules that perform SNMP queries may use SNMP IPv4 until concrete equipment supports native v6 queries. The modules transmit the results to the application kernel using IPv6, so it is possible to manage IPv4 equipments remotely through an IPv6 network.

Topaz

Topaz is a Network Intrusion Detection System (NIDS from here on). This application involves analysis, test and diagnostic activities of an IPv6 network, like is specified in WP4.2 from Euro6IX project.

An adaptation of an existing IDS has been evaluated but it has been decided to develop the system starting from zero due to the following reasons:

- A modular specific design is preferred to match Euro6IX requirements.
- The sniffer and basic functionalities software is not a great development since the largest effort in an IDS is spent when “learning” and configure detection patterns (the IDS Logic) and this has to be re-write anyway because IPv6 and IPv4 attack patterns are different).

Results:

Magalia

Features developed during 2Y1:

- Context Maps in Graphical Interface. Exploration of the net through different IXs network maps.

- Communication between Graphical Interface-Magalia Kernel. Connection of the graphical interface (Xges) and Magalia Kernel using IPv6.
- Communication between External Modules-Magalia Kernel. Connection of the external modules and Magalia Kernel using IPv6.
- External Modules implemented:
  - Hostlive. Detection of the state of a host by means of the use of “fping”.
  - Module_SNMP. Implements SNMP queries about the load of a link.

Topaz

Work done during 1Y2:

- Network Monitor: Capture and analysis of IPv6 packets
- Implementation of ICMP attacks and connections limit to a port.
- Client Interface development as a Windows-styled application.
- Integration of Network monitor and Client interface.

Future Work:

Magalia

New features planned for 1Y2:

- “Shared Network Management”.
- Authentication and/or Encrypted Transactions.

Topaz

Next features planned for 2Y1:

- Server failed mechanism.
- Detection of new attacks (TID accepts suggestions from the partners).
- Reactions against detected attacks.

More detailed information about “Network Management and Operation Tools” sub-activity can be found in [9].

3.4 IX Support Tools (A4.2-12)

Partners:

UPM

Objectives:

This sub-activity has to do with the development and testing of applications and tools related with Internet eXchange points (IX) architecture and associated services in the context of Euro6IX network. IXs will include, apart from the basic layer 2 switching infrastructure, a set of associated services like routing support tools (route servers, looking glasses, etc), transition facilities, router hosting facilities, server farms infrastructure, basic services like DNS, etc. This sub-activity will cover the development, integration or adaptation of applications or tools that support the services.

During the first year of the project, work under this sub-activity has focused on the Route Server functionality. The general objective was to gain experience on the design, set-up and management of a route server based IPv6 IXs. The work carried out here complements and provides experimental feedback to WP2 and WP3 activities in this area, with the final object of experimenting with and deploying route server based IXs over Euro6IX network.

In particular, the specific objectives for the first year have been the following:

- Collect and study information about available Route Server implementations for IPv6 (mainly based on open source code), as well as related functionalities like routing policy databases and associated tools. Focus has been on knowing the degree of IPv6 support on the implementations investigated.
- Select one or more implementations for further testing over laboratory test-beds. Pilot scenarios will include, if available, the set-up of a routing policy registry and the use of RS tools to automate the configuration of routers.
- Design and implement an IX emulation environment that allows the experimentation of complex IPv6 BGP routing scenarios without involving the cost of maintaining a laboratory test-bed made of an important number of machines. Basically, we will focus on how to emulate an IX scenario where an important number of ISPs (around fifty) are peering through a route server using a small number of computers (ideally only one).

Description:

Maintaining a complete mesh topology of BGP peering sessions in an IX could be difficult to manage if the number of participants is high or if some of the participants do not have enough technical expertise. Each router has to maintain a high number of peering sessions and configure a different set of filters for each one. Besides, when a new participant comes, almost all routers would have to modify its configuration to peer with the new participant. For all of these reasons, the scalability of IXs based on full mesh peering sessions is seriously compromised.

The main proposal to solve these scalability problems is based on the use of ***Route Server (RS)***: a system, which centralizes the interchange of routes between participants in an IX. Instead of peering among each other, providers peer only with the RS. Route Servers facilitate and make safer peering at an IX, improving its scalability. Besides, they facilitate the centralization of routing policy management.

Having into account the importance of the route server functionality and being Euro6IX a project centered on IPv6 IXs, it is important to study, test and deploy route servers, at least on some of the IXs, in order to gain experience in the management of global routing IPv6 scenarios.

Results:

Most of the sub-activity objectives planned for this year have been fulfilled: implementations of the basic components of a route server based IX have been tested successfully and a first prototype of the IX emulation environment has been developed and used to test medium size IX scenarios (around twenty peering routers).

Related to basic route server functionality, tests have mainly focused on Zebra's BGP implementation, as it has demonstrated to be the most stable and up-to-date among the implementations evaluated. Using zebra as route server and BGP clients from three different BGP implementations, basic scenarios have been successfully tested, showing the advantages of a route server based IX architecture.

However, the lack of maturity of the IPv6 extensions to RPSL language (generally named RPSLng) and, as a consequence of that, the unavailability of routing policy database implementations that support them, has prevented us from testing a complete scenario, where routing policy information stored in the database is used to automatically derive router configurations. Hopefully, this support will be available during the next year.

The IX emulation environment developed has shown to be very useful in order to emulate BGP complex scenarios without needing costly laboratory environments. This tool, based on User Mode Linux virtualization techniques, is able to emulate a complete IX made of a route server and tenths of peering clients inside only one machine. Its use in future activities will greatly simplify the process of testing new functionalities or scenarios, not necessarily tied to route server functionality, as the tool is flexible enough to emulate other general networking scenarios.

Future Work:

Future work around the activities presented in this document will be proposed in the following areas (although not necessarily to be carried out inside A4.2):

- **Experimentation with RPSLng.** Study and experimentation with the RPSL IPv6 extensions being proposed in RPSLng drafts should be initiated as soon as possible, probably in the context of WP2, in order to gain experience in its use and contribute to its standardization process and implementation.
- **Study about Route Server functions.** Further investigations are needed to define what functions can be incorporated to the route server of an IX. Being the route server a central point in the routing information flow, it seems very reasonable to incorporate to it functions that nowadays are being done in ISP routers or simply not done.
- **Definition of Testing Scenarios**. Although complex scenarios have already been tested using the emulation environment, they have been used as a proof-of-the-concept test. Additional work has to be invested in defining the precise scenarios to study route server based IXs architectures and implementations.
- **Improvement of the IX Emulation Environment.** Now we have a basic IX emulation environment made of a basic set of scripts. Work will be invested in the future in order to improve the flexibility and easy the use of the environment.

- **Routing Policy Databases.** Availability of RPSLng compliant policy routing databases is a key point for the activities described here. A deeper study should be done to know when RPSLng support they will be available.
- **Security in IXs.** Due to its importance for the correct operation of IP networks, a significant effort is being invested at present in securing routing protocols. It would be interesting to analyze how the current proposals to secure the BGP protocol match the route server based IX architecture.

More detailed information about “IX Support Tools” activities can be found in [10].

3.5 Code Porting

3.5.1 Code Porting (A4.2-15)

Partners:

nGn

Objectives:

This activity consists of porting existing application to enhance and use it in IPv6 networks.

Description:

As a broad view of what we are going to do in the code porting section, we will port a variety of languages and applications that are under GPL license, staying in the open-source movement. In that way we hope that we can make easier the implication of new users and programmers on the development of applications over the IPv6 protocol.

This three-year task is now focused in the following:

- **MRTG**. It is a program written in PERL that is used to register and to measure the traffic that is generated in the routers. The porting would consist on adapting the already mentioned application to routers that work under IPv6.
- **DTD**. We will define a DTD that will enable the communication of data structures between IPv6 applications.
- **PHP**. Porting PHP interpreter for web server introducing IPv6 structures to it network utilities and adapting several functions to this new data definitions. There are some functions yet ported so we want identify the rest and porting them.
- **Webalizer**. It is a very used tool for obtaining analysis of web sites visits. The porting of this tool will allow the analysis of the records generated by the web servers in IPv6, promoting some new analysis of the application like the identification of the country or region of the user. Actually this tool only analyzes the IPv4 addresses and the purpose is to include the 128 bits addresses. The idea is to use all the possible introduced improvements by IPv6. The IPv6 special multicast and anycast addresses have a special treatment too.
- **Graphic trace router**. The idea is to develop an application in order to follow the path of the IPv6 packages geographically in a map. This application, similar to standard traceroute, will help network administrators and users to make an idea of the route IP packets follow. With the possibility of sending IPv6 packets through a known route this application can be used to check this.

Results:

- **MRTG**. We have started to work in this tool studying the way in which SNMP protocol gets and stores network information later MRTG tool uses to show traffic measures through routers. We are also treating how Perl deal with IPv6 addresses.
- **DTD**. The is a set of XML DTDs already finished describing data structures of IPv6 protocol and some more protocols related with IPv6.

- **PHP**. Some ported PHP functions to IPv6 already exist. We have found not yet ported several important functions and we have ported them. Also we have included them in a real application using IPv6 connection between different PHP pages server from an Apache server. We have also developed a basic Java server to register PHP pages served from other web server. The idea is to include porting PHP functions into a possible real application such a centralized registry of served pages that could be a useful tool to get statistic information inside an IPv6 server farm system. It can demonstrate the properly porting of PHP functions.

Future Work:

Our objective for year 2003 is to have at our own disposal a Mail Tool working on the Euro6IX net and using all the previous described advantages.

From the analysis done, we have started with the developing tool tasks, with the idea of having a very advanced prototype in the next Euro6IX revision.

More detailed information about “Code Porting” activities can be found in [11].

3.5.2 IPv6 Repository (A4.2-17)

Partners:

nGn

Objectives:

The objective of this activity is the creation and development of a big software and IPv6 documentation library and to be a reference in this subject for Europe and the whole world.

Description:

At the beginning, the developed tool is used to manage the documentation and Betas that are generated in Euro6IX.

The repository is equipped with a document classification by groups and subgroups where you can store the information.

You can associate key words with each object (software or documentation) that is in the repository, in such a way that you are able to do quickly and accurate searches that are based on the key words.

Also applications can be associated to documents and vice versa. In this way we will be easily able to know if an application has installing guide, etc.

Two areas exist, a public and a private one. In the public area we will include all we see prepared to offer to the outward of the project.

The latest objective is to get the tool being a great library where we could find any kind of Euro6IX documentation or any other project based on IPv6. We hope this being one of the most important references about IPv6 in Europe and above all, we hope it being a place where other projects could make good use of the gotten Euro6IX experiences and use them in their projects.

Tool has been developed in PHP and it has been integrated in the Web Site. It has been working under an IPv6 server since June 2002.

Results:

The activity has been ended with the setting in motion of the tool. It is had at one’s disposal a guide of use.

Future Work:

It is needed to do maintenance and supervision jobs of all the contents. Some bettering or modifying tasks can be developed in a future if the consortium says so.

More detailed information about “IPv6 Repository” activities can be found in [11].

4. SUMMARY AND CONCLUSIONS

This document has presented all the research and innovative tasks carried out during the first year of Euro6IX project in the context of WP4 A4.1 and A4.2 activities. As mentioned before, the main goal of these activities has been:

- To support the deployment of the Euro6IX test-bed with new components or functionalities needed.
- To consolidate the teams, activities and components needed to built and validate the "Euro6IX Integrated Service Framework".

The two goals have been achieved. In the first case, the Network and IX support tools sub-activities have provided some missing items necessary for the consolidation of the Euro6IX test-bed during year 2 of the project. Tools for network management and analysis have been assembled, as well as important elements for the validation of the future new IX functionalities to de deployed in the next year. In the second case, the most important components for the creation of the Euro6IX Integrated Service Framework have been consolidated, including security (VPNs, PKIv6, DNSSEC, AAA), mobility, multicast and QoS.

The effort invested in A4.1 and A4.2 has covered a wide range of network services and applications, leading most of the sub-activities initially planned for this year to interesting and useful results.

A4.1 activity results mainly come in the form of a good understanding of the maturity of standards, solutions and implementations, which will allow us to rightly design and deploy advanced services over the Euro6IX test-bed in the near future, as well as to contribute to the standardization processes with a good knowledge.

In a few cases, sub-activities initially planned for this year have not led to practical results, due to the unavailability of mature solutions or implementations. That is the case, for example, of multihoming or anycast.

Anycast is still an open research issue and has been postponed until it reaches a higher degree of maturity. Work on multihoming, renumbering, provider independent addressing and other IX related issues has been only outlined during the first year in cooperation with WP2 and WP3, with the intention of starting well focused activities in the next year. In summary, these sub-activities, far from being abandoned, have been followed in the forums where they are being discussed, in order to contribute to their maturity and to incorporate them as a service in our test-bed as soon as solutions are available.

The IPv6 application development activities performed during the first year have consolidated a rich set of basic and advanced applications, which will provide the basic elements for the validation of the Euro6IX Integrated Service Framework. Not all the application activities have reached the expected results and therefore some will be discontinued in the second year.

Although presented separately, reflecting the internal organization of WP4, the results of A4.1 and A4.2 sub-activities are all oriented towards the creation of an integrated end user service scenario, which integrates advanced network services and applications into a common framework. The results of this first year constitute the building blocks that will allow us the creation of what we have named the "Euro6IX Integrated Services Framework".

Apart from the specific technical results of each sub-activity, the first year has been very productive in allowing us the consolidation of the WP4 organization and the teams covering the most important network and application components needed for the deployment of the advanced test-bed. This is an important point for the future, especially inside a big project as Euro6IX is.

During the second year, work will be much more focused on integration than on individual developments. We expect to increase notably the interrelations between the different sub-activities. In this sense, having the network services being tested using a wide variety of real applications will allow us to get useful feedback to network experts about how to design and configure new network services. On the other hand, testing applications over a network offering novel and advanced services will allow us to get valuable feedback to application developers about how applications should be adapted to efficiently use the new services.

Besides, the second project year will bring a new sub-activity inside A4.2 for the maintenance of an IPv6 Transition and Porting Guide, which shall describe all the experience gained within Euro6IX, as well as develop transition recommendations and guidelines.

Finally, the experimentation over a scenario of integrated network services and applications will put us in a good position to study what should be the role of IXs in this context. In general, the potentiality of IXs is not exploited enough at present, as they are typically used as L2 infrastructures not offering any L3 services. As an example, being the present IXs places where security is a must in terms of accessibility and equipment protection, this fact could be exploited to locate there some of the components needed to offer network and application security services. Or some of the routing and addressing functions being made nowadays by ISP equipment on IXs could be done more efficiently by route servers managed from the IX.

5. REFERENCES

[1] *"Mobility over IPv6 Networks"*. Euro6IX Technical Report TR4.1A.1. February, 2003.

[2] *"Multicast over IPv6 Networks"*. Euro6IX Technical Report TR4.1A.2. February, 2003.

[3] *"Deployment of Static VPNs and Security"*. Euro6IX Technical Report TR4.1A.3. February, 2003.

[4] *"PKIv6".* Euro6IX Technical Report TR4.1A.4. February, 2003.

[5] *"DNSSEC"*. Euro6IX Technical Report TR4.1A.5. February, 2003.

[6] *"QoS over IPv6. Tests and Results"*. Euro6IX Technical Report TR4.1A.6. February, 2003.

[7] *"AAA for IPv6 protocol"*. Euro6IX Technical Report TR4.1A.7. February, 2003.

[8] *"Advanced Applications"*. Euro6IX Technical Report TR4.1A.8. February, 2003.

[9] *"IPv6 Network Management and Operation Tools".* Euro6IX Technical Report TR4.1A.9. February, 2003.

[10] *"IX Support Tools".* Euro6IX Technical Report TR4.1A.10. February, 2003.

[11] *"Code Porting"*. Euro6IX Technical Report TR4.1A.11. February, 2003.

[12] *"First Internal Trial Report"*. Euro6IX D4.3 Deliverable. February 2003.

All Euro6IX Technical Reports and Deliverables referenced above are publicly available on Euro6IX web server: http://www.euro6ix.org.