Project Number:	**IST-2001-32603**
Project Title:	**6NET**
CEC Deliverable Number:	**32603/TERENA/DS/7.5/A1**
Contractual Date of Delivery to the CEC:	31 July 2004
Actual Date of Delivery to the CEC:	31 August 2004
Title of Deliverable:	Report on 2nd 6NET Open Workshop
Work package contributing to Deliverable:	WP7
Type of Deliverable*:	R
Deliverable Security Class**:	PU
Editors:	Kevin Meynell
Contributors:	Jane Butler, Tim Chown, Jeróme Durand, Chris Edwards, Patrick Grossetete, Xing Li, Michael Mackay, Kevin Meynell, János Mohácsi, Jordi Palet Martinez, Thomas Schmidt & Vasilios Siris

* 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)

Abstract:

This document provides a report of the 2nd 6NET Open Workshop held on 9 June 2004 in Rhodes, Greece.

Table of Contents

Introduction 3
6NET Update 4
Euro6IX Update 4
IPv6 Multicast 5
IPv6 Transition: moving into the campus 6
Mobile IPv6 in 6NET: An Overview 7
IPv6 Prospects 8
6POWER, IPv6 and PLC for home automation 8
IPv6 Development in China 9
Managed IPv6 Transitioning Architectures 10
Performance Analysis of Multicast Mobility in a H-MIP Proxy Environment 10
IP Security from point of view of firewalls 11
A test-bed investigation of QoS mechanisms for supporting SLAs in IPv6 12

Introduction

The 2nd 6NET Open Workshop was held on 9 June 2004 in conjunction with the TERENA Networking Conference (TNC 2004) in Rhodes, Greece. The objective was to publicise the 6NET and Euro6IX project activities, and other related IPv6 developments. It also provided an opportunity for feedback from the European research networking community.

The workshop discussed the current status of the 6NET project, focusing on innovative aspects such as multicasting, mobility and new applications. It also considered deployment and transitioning issues, drawing on the experiences of 6NET and other IPv6 projects.

There were other interesting presentations on the future prospects for IPv6, its use in home automation, and rollout in China. The final session of the workshop featured submitted papers on performance and security issues.

The workshop ran from 09.00 to 15.30 and was divided into three sessions. Presentations and attendance figures were as follows:

09.00-10.30 Chair: Kevin Meynell Attendance: 81

- 6NET Update – *Jane Butler, Cisco*
- Euro6IX Update – *Jordi Palet Martinez, Consulintel*
- IPv6 Multicast – *Jeróme Durand, RENATER*
- IPv6 transition: moving into the campus – *Tim Chown, University of Southampton*

11.00-12.30 Chair: Kevin Meynell Attendance: 73

- Mobile IPv6 in 6NET: An Overview – *Chris Edwards, Lancaster University*
- IPv6 Prospects – *Patrick Grossetete, Cisco*
- 6POWER, IPv6 and PLC for home automation – *Jordi Palet Martinez, Consulintel*
- IPv6 Development in China, *Xing Li, CERNET*
- Managed IPv6 Transitioning Architectures – *Michael Mackay, Lancaster University*

14.00-15.30 Chair: Kevin Meynell Attendance: 63

- Performance Analysis of Multicast Mobility in a H-MIP Proxy Environment – *Thomas Schmidt, HAW Hamburg & FHTW Berlin*
- IPv6 Security from point of view of firewalls – *János Mohácsi, Hungarnet*
- A test-bed investigation of QoS mechanisms for supporting SLAs in IPv6 – *Vasilios Siris, University of Crete & FORTH*

The full proceedings of the workshop can be found on the 6NET website at:

http://www.6net.org/events/workshop-2004/

6NET Update
Jane Butler, Cisco

6NET is a three-year IST project that started in January 2002, and aims to prepare the next generation of the Internet. It is one of the largest projects in the European Union's IST Programme, and represents a total investment of EUR 18 million.

The establishment of a pan-European native IPv6 network was extremely important to test and validate IPv6 functionality, and enabled IPv6 to be offered earlier than expected on the production GÉANT network. With IPv6 shown to be stable and usable, much of the remaining activity will focus on the development of applications and demonstrators.

A number of IPv6 demonstrators have been developed such as SIP-based VoIP, multicast file transfer, a Grid-based weather station, mobile video streaming, and H.323 conferencing. An IPv6-enabled car was also developed in conjunction with Renault, and this technology will be extended to vehicles used by the emergency services.

6NET has ported the OpenH323 toolkit to IPv6 which has allowed the GnomeMeeting videoconferencing application to be IPv6-enabled. In addition, the porting of Globus toolkit is close to completion, and a couple of demonstrators (weather station and eProtein) are already available.
The project has been actively involved in the IPv6 standardisation process and has authored or contributed to 43 Internet Drafts. It has also contributed to the GGF with respect to IP independence and a survey of the IPv4 dependencies in the Grid specifications.

6NET co-organised the Global IPv6 Service Launch at the beginning of the year in Brussels. This was an opportunity to promote IPv6 to an audience that included politicians, government officials and commercial organisations.

There are still a few outstanding technological issues to work on such as renumbering, multihoming, and mobility, but the project will also focus on providing deployment assistance for those wishing to adopt IPv6. This includes making documentation available, and the establishment of support teams at national and international level. This will be allied with a promotional programme in conjunction with other projects and forums to make users and organisations aware of the benefits of IPv6.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/butler.pdf

Euro6IX Update
Jordi Palet Martinez, Consulintel

Euro6IX is a three-year IST project to build a native IPv6 backbone of traffic exchanges across Europe. It aims to gain experience of designing and deploying IPv6 networks, and to introduce IPv6 to specific user groups. The project consortium consists of seventeen partners from the telecommunications, industrial, academic and NGO sectors.

The core network currently links Internet Exchanges (IXs) in London, Paris, Madrid. Lisbon, Turin, Berlin and Zürich, with a number of additional nodes. The infrastructure provides both a Layer 2 and 3 interconnection service, and several IXs are able to offer direct peering. Each IX uses a p- or sTLA prefix to assign NLA prefixes to ISPs or customers, with project partners using their xTLA prefix to assign NAL to regional ISPs and customers. This model is based on RFC 2374 to verify that customers can change their service providers without changing their addressing space, and that renumbering and multihoming functionality can be more easily realised.

The project is also working on mobility issues based on different access technologies, the deployment of a static VPN service using IPsec and IKE, and the establishment of a public key infrastructure based on PKIv6 and LDAPv6. A number of applications are also being trialled such as peer-to-peer messaging services, audio- and videoconferencing, web-based mail tools, VNC over IPv6 and various network management tools. In addition, the use of DNSSEC to publish certificates is being investigated in conjunction with the work on PKI.

The activities in the final year of the project will focus on secure roaming services, policy management, multihoming, end-to-end QoS, and unmanaged IPv6 connectivity for IPv4 users. There will also be work on SIP 3GPP, as well as to develop authentication and network management tools. The general focus will be to move away from testing individual aspects of IPv6, and towards provision of an integrated testbed.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/palet-euro6ix.pdf

IPv6 Multicast
Jeróme Durand, RENATER

The M6Bone is an IPv6-based multicast network that was established in 2001 by the Aristote Association, G6 and RENATER. As of June 2004, it connected around forty sites in five continents, and aims to provide an environment to test multicast-related hardware and software, learn about deployment issues, and provide a conferencing infrastructure.

There were originally no IPv6 multicast implementations from hardware vendors, so multicast tunnels were established in order to trial the technology. MBGP was not available, so a hacked version of RIPng was used for routing. The next phase starting in March 2003, aimed to deploy multicast in the core of the 6NET network, and this was completed by September the same year. This provided most NRENs with a fairly stable native multicast service, along with a common routing policy. Additional functionality such as Embedded-RP, MLDv2, Scoped BSR and Bidirectional PIM was then subsequently added in response to requests.

A number of applications are being successfully run over the M6Bone such as VideoLAN, ISABEL, Windows Media Player, Freeamp, and the traditional Mbone tools. In addition, IPv6-to-IPv4 multicast and IPv6 unicast reflectors are available.

Unfortunately, the dedicated 6NET network is likely to disappear at the end of 2004 as the GÉANT production network is now able to support dual-stack. However, it is unlikely to initially support IPv6 multicasting, which leaves an issue of how to continue to interconnect NRENs. There is also

the problem that many NRENs only have IPv6 multicast in testbeds which currently get their connectivity through 6NET.

Much of the IPv6 multicast experience has been documented in a cookbook and in several Internet Drafts. A collaborative website (http://www.M6Bone.net) and mailing list (m6bone@ml.renater.fr) are also available for exchanging information.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/durand.pdf

IPv6 Transition: moving into the campus
Tim Chown, University of Southampton

The two key aspects to deploying IPv6 are enabling it in both the NREN and university campus networks. There is also interest in providing IPv6 access to researchers and students in commercial networks, such as those available via ADSL or WiFi hotspots. The user should be unaware which IP version they are running, which requires networks to provide both IPv4 and IPv6, and for applications to be version independent.

There are a number of approaches to this such as using automatic or manually configured tunnels to connect IPv6 clouds. Another approach is the use of translation services where packets are actually translated from one protocol to another. It is also possible to have servers and devices that speak both protocols, and choose whatever is available.

At the present time, IPv6 has been deployed in GÉANT and a number of European NRENs, on Abilene and CA*net4 (North America), on WIDE (Japan), and in Korea and China. It is also being run on a number of pre-commercial networks such as Euro6IX and Moonv6, although full commercial deployment is still lacking.

Nearly all networks have taken the dual-stack approach, which provides an environment for future IPv6-only devices, but has performance and possible service interaction issues. However, two NRENs have deployed a parallel infrastructure, whilst another two have implemented MPLS (6PE). Campuses are also mainly interested in the dual-stack approach, although there is a much higher complexity in the type of systems being used.

The steps towards providing IPv6 have been to analyse current IPv4 systems and identify anything that IPv6 cannot provide, consider workarounds, and then deploy IPv6 using VLANs or ISATAP. IPv6 services and management tools can also be deployed, of course ensuring that policy and security issues are covered.

Most major operating systems (desktop and server) now support IPv6, and it is even supported by some PDAs. The main network services such DNS, NTP, SMTP, HTTP, NNTP, IRC, multicast, SSH, NFS, Samba, and LDAP can be run over IPv6, even though some popular applications (e.g. Outlook, Active Directory) still do not always support this properly. Perhaps the biggest gap though is a lack of IPv6 support for all X11 implementations.

The 6NET project has documented much of this in two cookbooks aimed at NRENs/ISPs (see http://www.6net.org/publications/deliverables/D2.2.3.pdf) and campus networks (see http://www.6net.org/publications/deliverables/D2.3.3bis1.pdf). These outline the scenarios, analyse NREN solutions, and provide specific case studies. A more generalised white paper aimed at campus management is also being produced in conjunction with the Euro6IX project.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/chown.pdf

Mobile IPv6 in 6NET: An Overview
Chris Edwards, Lancaster University

MIPv6 is a routing protocol for mobile IPv6 hosts that is transparent to upper-layer protocols and applications. It tries to avoid actively involving routers as its protocol state is held by end-stations. Each mobile node holds a home address, and acquires a care-of address (at its current location) which is registered with a home agent. This provides the information necessary to allow the correct routing of packets to the mobile node, wherever it may be.

In order to prevent an attacker sending bogus update messages, IPsec protects signalling between the mobile node and its home agent. A 'return routability' test then allows nodes to determine whether the binding updates are authentic.

The protocol specification is currently at the status of an Internet Draft, although it has been accepted by the IESG for RFC status. The MIPv6 Working Group is continuing to work on issues that are necessary for wide-scale deployments, whilst the MIPSHOP Working Group is working on signalling optimisation. There are currently implementations (v24 compliant) available for Linux various BSD flavours and Cisco IOS, whilst Microsoft expects a beta release in the fourth quarter of 2004.

The 6NET project is trialling several MIPv6 implementations in order to investigate deployment issues in both large and small-scale setups. This includes consideration of interoperability, autoconfiguration, handover performance, security, and multicast issues. These trials utilise the TAHI test suite and the IETF Remote Interop Testing guidelines.

Some of the problems being encountered are slow handovers, high latency and loss, and poor route optimisation. It is hoped that many of these problems will be resolved when the MIPv6++ implementations become available.

The 6NET project is collating its experience into a MIPv6 Support Guide, aimed at those wishing to deploy MIPv6. An interim version of this is currently available (see http://www.6net.org/publications/deliverables/D4.1.2.pdf)

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/edwards.pdf

IPv6 Prospects
Patrick Grossetete, Cisco

Although IPv6 brings many advantages, the end user is interested in the services and applications they receive, not how they are provided. The network manager though, is interested in the cost of deployment and operation, and the stability of the technology.

The core IPv6 specifications are already draft standards, are well tested and stable, and it is possible to run full production services. This combined with the increasing ubiquity of broadband, means that it is feasible to start utilising IPv6 in home networks. In particular, IPv6 is necessary to provide many of the features that users will expect in an increasingly mobile and multimedia world.

In reality though, most of the challenges that need to be overcome are financial or political, rather than technological. For example, there needs to be a different charging model for address allocation if the end-to-end advantages of IPv6 are to be realised. ISPs need to shift their focus to associated services to raise revenue, rather than simply charge for basic network provision. In addition, users need to be made aware of the possibilities of IPv6, and this is an area where the next generation of graduates will be key.

Of course, some of the enhanced features of IPv6 such as multihoming, security and network management do require more work. There also needs to be much more work to integrate home applicances such as televisions, hi-fis, telephones so that they can communicate with each other and the rest of the Internet. Another big area for growth is the use of Internet technologies in vehicles, for navigation, entertainment and safety purposes. It has been estimated that the telematics industry will be worth USD 8 million in 2005, and will continue to increase thereafter.

Schools in particular could benefit from IPv6 as communication within and between schools could be improved. This would open the possibility of having remote specialist teachers (e.g. for foreign languages), the sharing of resources (e.g. teaching aids and datasets), tele-surveillance for security purposes, and out-of-hours support.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/grossetete.pdf

6POWER, IPv6 and PLC for home automation
Jordi Palet Martinez, Consulintel

IPv6 is useful for home automation because it allows IP addresses to be assigned to all manner of devices in the home, plus it has ‘plug-and-play’ features, efficient mobility mechanisms, and improved support for options/extensions. The 6POWER project is working to provide IPv6 connectivity over existing electrical power lines, which have the advantage of already being installed in most locations. This would allow service providers, through the use of power line modems, to offer always-on connectivity at speeds of up to 200 Mbps. In addition, it could facilitate the creation of more WLAN access points in public and private spaces.

In the future, every electronic-based device could have a unique IP address which would enable it to communicate with other devices such as a control point. Universal Plug-and-Play (UPnP) is a

protocol that enables discovery and control of network devices and services. Each device has an XML file that describes its services (amongst other things), and may be interrogated with SOAP to determine its status or to invoke actions.

6Plug is a control point application that has been developed to provide secure access to home and industrial devices. This runs on Windows XP/CE, Linux and BSD platforms, and can be accessed via port 80 (or 433 when using SSL), thus avoiding problems with proxies. Clients are authenticated through the use of digital certificates or standard logins, and UPnP security is maintained through the use of public/private keys.

X.10 is currently used to communicate with the end devices. This is a long-established control technology that allows the transmission of digital information over power line wiring. There are many X.10 devices available (e.g. lights, door controllers), and these are interfaced to the control point via an X.10 to UPnP bridge. Bridges are also being developed for other control technologies such as EIB (European Installation Bus) and LonWorks, giving the potential to remotely control every electrical and electronic device in a building.

A live demonstration was given to show how lights and curtains could be remotely controlled in a house in Spain.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/palet-6power.pdf

IPv6 Development in China
Xing Li, CERNET

China has a population of approximately 1.2 billion people, with nearly sixty million currently using the Internet. This figure is increasing, and assuming one IP address per person, that would require the equivalent of 72 Class A addresses. Furthermore, assuming every person went online for one hour per day, that would require 1.68 Terabits per second of bandwidth. The use of IPv6 is therefore extremely important in China.

In 1998, the first IPv6 testbed was established by CERNET (Chinese Education and Research Network), and this evolved into the CNGI (China Next Generation Internet) project by 2003. CNGI is a government-led collaboration between CERNET and a number of commercial organisations such as China Telecom and China Mobile. It provides a core network covering more than twenty provinces, which allows various IPv6 services and applications to be trialled. It also aims to promote hardware and software developed in China.

CERNET2 has also been established in parallel to the existing CERNET network, in order to rollout IPv6. This currently connects twenty cities at speeds of 2.5 to 10 Gbps, with onward connections to other global IPv6 networks. This enables the scalability and functionality of the technology to be tested, and is also working on video delivery, the integration of smart devices, and charging models.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/li.pdf

Managed IPv6 Transitioning Architectures
Michael Mackay, Lancaster University

The deployment of IPv6 will bring a lengthy period of co-existence with IPv6 that will require improved management. Not only will there be two protocols to manage within the same environment, but also the transitioning process introduces significant disruption to the operation of the network.

There are various transitional mechanisms that may be employed at different stages and removed when redundant, while others may be necessary for the entire deployment process. It would be useful to organise these into a standard framework and manage them using a common protocol such as SNMP. To this end, a transitioning MIB has been specified and will be developed further by 6NET.

A site transitioning architecture (STA) for IPv6 would be able to integrate network management, simplify the provision of services, and provide standard fault reporting. An STA operates on two planes: operational and management. The operational plane is composed of the actual transitioning mechanisms such as hosts, servers and border devices, whilst the management plane dictates how they are controlled and operated.

The use of IPv6 is initially likely to be limited and so a lot management support will be required. A mixture of transitioning and tunnelling is likely to be necessary in the early stages, gradually moving to dual-stack solutions, and finally protocol translation where IPv4-only nodes need to communicate with IPv6-only nodes. Although much of this management infrastructure is already available or under development, a great deal more work is required.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/mackay.pdf

Performance Analysis of Multicast Mobility in a H-MIP Proxy Environment
Thomas Schmidt, HAW Hamburg & FHTW Berlin

Mobile IP permits devices to roam between local subnets whilst retaining a home address at which they can always be contacted. This is of particular use in 3G applications where handsets or PDAs make use of voice- and video-conferencing.

Mobile group conferencing requires bi-directional multicast capabilities, with multicast applications being dependent on the source address. The problem is that connections are asymmetric and convergence is often slow at up to thirty seconds at the listeners end, and three minutes at the senders end. This is clearly unacceptable which is why improved multicast protocols are being developed for MIPv6 to improve handover and reduce loss and delay.

The Fast Multicast Protocol relies on remote subscription with agent support, and improves reception only. It extends the signaling of Fast Handovers for MIPv6 (FMIPv6) which predicts handovers based on Layer 2/3 mappings.

Seamless Multicast Handover is agent-based and works at both reception and source. It is built on Hierarchical MIPv6 (HMIPv6) and uses reactive handovers based on Mobility Anchor Points (MAPs) and forwarding over unicast tunnels. When a node moves between MAPs, traffic is bicast through both the old and new MAP.

The handover performance of the different protocols was analysed based on packet loss, jitter and delay; the number of performed and processed handovers; the robustness of the connections, and signalling overhead. This showed that M-FMIPv6 had faster handovers at intermediate distances from routers, but was more liable to fail when there were a number of rapid handovers. On the other hand, M-HMIPv6 would function for any handover frequency, although delays were liable to increase.However, more analysis of mobile scenarios needed to be undertaken in order to optimise these protocols.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/schmidt.pdf

IP Security from point of view of firewalls
János Mohácsi, Hungarnet

The IPv6 specification mandates the use of IPSec, but few IPv6 implementations actually support this at present. The use of firewalls is well understood by network managers, and would be one method of improving security in IPv6.

A firewall is a system that implements and enforces a security policy between two networks; usually a private intranet and the external Internet. However, IPv6 firewalls have particular requirements in that they should support header chaining, they should not break existing IPv4-based protocols, and they must be aware of the tunnels that are often used by transition mechanisms. They also need to support ICMP completely differently. Support for neighbour and path MTU discovery is mandatory, and in most cases, letting router advertisements and solicitation pass through the firewall is unavoidable. In other cases, MLD messages and IPv6 packets with router alert options need to be allowed.

There are currently only a few IPv6 firewalls generally available such as Kame ip6fw, IPFilter, OpenBSDPF, NetFilter, Cisco IOS and JunOS. An evaluation of each of these has been undertaken, and the results published in a paper (see http://www.terena.nl/conferences/tnc2004/core_getfile.php?file_id=323). They are all generally usable and can be used on a production IPv6 network with little or no impact on performance. Unfortunately though, they still lack support for some of the new and advanced features of IPv6 such as mobility. Some work is therefore being undertaken by the 6NET project to identify and resolve these issues.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/mohasci.pdf

A test-bed investigation of QoS mechanisms for supporting SLAs in IPv6
Vasilios Siris, University of Crete & FORTH

It is important to understand the operation and interaction of QoS mechanisms in IPv6 networks, and whether they perform differently compared to IPv4. An IPv6 testbed comprised of both Linux-based and Cisco 7x00 routers connected via Fast Ethernet was established, which was used to perform a variety of tests on traffic policing, traffic shaping and class-based queuing (see http://www.terena.nl/conferences/tnc2004/core_getfile.php?file_id=197).

The results demonstrated that the interaction of QoS mechanisms is important if service level agreements are to be supported effectively. They also showed that traffic shaping can increase aggregate throughput where policing is present, and that the tuning of parameters should consider both throughput and delay. However, further research needs to be undertaken on bigger networks with a longer round trip time, as well as wireless networks.

This presentation can be found on the web at:

http://www.6net.org/events/workshop-2004/siris.pdf