



IST-2000-25153

Deliverable D20

Evaluation of Components, Networks and Services developed in the 6WINIT Project

Contractual Date of Delivery to the EC:	31 December 2002
Actual Date of Delivery to the European Commission:	20 January 2003
Editor(s):	Peter Kirstein (UCL)
Participant(s):	All Partners
Workpackage:	10
Title of Deliverable:	Evaluation of the Components, Networks and Services developed in the 6WINIT Project
Security:	Public
Nature:	Report
Version:	Final
Number of pages:	73

Abstract: This is the final Deliverable for the 6WINIT project, which has been investigating a range of IPv6-enabled applications over an IPv6-enabled wireless Internet. It summarises and evaluates all the work done in the project, which covers the areas of end-stations, routers, gateways, generic technologies and applications – with specific emphasis on following the IPv6-related standards emerging in the IETF. Thus clearly Mobile IP, Road Warrior technology, Quality of Service, agent technology and security are of particular concern. Generic applications investigated included conferencing, voice/IP, video streaming and home environments. There was specific emphasis on clinical applications, where secure mobile access to clinical data and radiographic images, and emergency treatment from ambulances for A & E. Most of the work was in the context of Wireless LANs, since the access to and functionality of GPRS were very limited and the access to UMTS test facilities was provided only at the project end

Keywords: IPv6, wireless Internet, clinical applications, conferencing, VoIP, agents, active networks, routers, gateways, A&E, radiographic images, Road Warrior, Mobile IP, security, IPv6-IPv4 transition, WLAN, GPRS, UMTS

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

Executive Summary

This project was set up to investigate the problems arising in running IPv6-based applications over the emerging wireless Internet. The wireless Internet was considered as the backbone network we all know, with access networks consisting of Wireless LANs (WLANs), third Generation Cellular Wireless (UMTS), and the intermediate extension to GSM called GPRS. When the project was proposed, in early 2000, GPRS was considered only as a stepping-stone to UMTS, but was expected to be exploitable immediately, while UMTS was not expected to be deployed before mid- 2001. The financial climate of the industrial partners, and the expectations of the Communications Industry were quite different from the climate a year later, when the project started. This impacted many parts of the project. The most important of these were: the availability of 3G network facilities (even for testbeds), the speed at which UMTS or GPRS moved to IPv6, and the readiness of industry to develop IPv6-based components and applications for UMTS. While this led to a dearth of GPRS and UMTS equipment, the WLAN use grew rapidly; its equipment became widely available on both laptops and PDAs. At the same time, the IPv6-based products from the main hardware providers matured, and the availability of a complete range of such equipment became a reality.

The project has required the utilisation, and often the development, of a number of different types of component: end stations, routers and relays, generic technologies, different network technologies, applications. They require a variety of standards – many of which have been evolving during the project. Almost all the components have been used as part of applications and/or demonstrations. Many of the applications are generic, and can be used in their own right. However a major emphasis in the project has been on clinical applications; these have been found to be a fertile, but demanding, user of the developments from outside the clinical area. The clinical partners have found it turn that it has been very instructive and useful to work with their technical partners. Because of the intentions to investigate major real-life applications, it has been very important also to consider the transition from the IPv4 wired world to the IPv6-enabled, all-IP, wireless world.

The work done in the project was largely practical, and there was little interest in defining or using proprietary solutions. For this reason, there was a major activity in following, influencing, and implementing the rapidly changing IPv6 standards. There was little similar activity in the GPRS and UMTS standards, because the project was not setting up such networks. It was essential that we had access to real networks for our work; this was the case for IPv6-enabled wired and WLAN networks. There was limited access to the IPv4-enabled GPRS, which could be used for IPv6 by encapsulation; there was no access to even UMTS testbed equipment until the last two weeks of the project. Thus most of the practical work involved WLANs and some GPRS. UMTS was used only in the final demonstration.

The main activity on workstations was to ensure that the applications could run on both PDAs and laptops, using WLANs and where possible GPRS with reduced functionality. These had to be able to support the relevant protocols for secure, mobile working – resulting in activity on mobile IP, Public Key infrastructures and Road Warrior technology. There was corresponding activity in developing routers. Moreover, since the wired world operates at much higher speeds than the wireless world, there was also significant activity in gateways for speed adaptation, transition and between technologies. This work included the use of agent technology and active networks. Generic applications pursued included conferencing, Voice/IP, video streaming, home environments, a weather station and location-awareness. The corresponding clinical applications

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

included mobile, secure access to clinical data, accident and emergency work with ambulances and access to radiographic images.

It was a fundamental tenet of the project that we would demonstrate our results publicly. The report describes the public demonstrations made of our results during the project.

Table of Contents

1	INTRODUCTION	7
1.1	Background.....	7
1.2	Overview	7
1.3	Method of Evaluation.....	7
1.4	Structure of this Report	7
2	THE NETWORK STANDARDS (D15)	9
2.1	The Assumptions	9
2.2	Implementations.....	9
2.3	Utility	10
2.4	Evaluation.....	10
3	THE CLINICAL STANDARDS (D15).....	11
3.1	The Assumptions	11
3.2	Implementations.....	11
3.3	Discussion.....	11
3.4	Evaluation.....	12
4	THE ARCHITECTURE (D6, D11, D15, D18)	13
4.1	The Assumptions	13
4.2	Implementations.....	14
4.3	Utility and Evaluation	15
5	THE NETWORKS (D11, D18).....	16
5.1	Fixed IPv6 Networks.....	16
5.2	Wireless LANs.....	16
5.3	GPRS.....	16
	5.3.1 <i>Functionality</i>	16
	5.3.2 <i>Availability and Cost</i>	17
	5.3.3 <i>Performance</i>	17
	5.3.4 <i>Cards and Drivers</i>	17
5.4	UMTS.....	18
5.5	The Partners' Local Infrastructures.....	18
5.6	Summary	18
6	THE TERMINALS AND SERVERS (D10, D13)	19
6.1	Laptops.....	19
	6.1.1 <i>Operating Systems</i>	19
	6.1.2 <i>Applications</i>	19
	6.1.3 <i>Utility</i>	19
6.2	PDA's	19
6.3	Telephones.....	20
6.4	Summary	20
7	THE ROUTERS AND GATEWAYS (D8, D11, D17).....	21
7.1	Edge Routers.....	21
	7.1.1 <i>The Ericsson Router</i>	21

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

7.1.2	<i>The 6WIND Router</i>	21
7.1.3	<i>Other Routers</i>	22
7.2	Gateways	22
7.2.1	<i>The TZI Gateway</i>	22
7.2.2	<i>The UCL TAG</i>	22
7.3	Summary	23
8	GENERIC TECHNOLOGIES (D12, D16)	24
8.1	The Road Warrior	24
8.2	Mobile IP.....	24
8.3	Multiaccess	25
8.3.1	<i>Simultaneous Multiaccess</i>	25
8.3.2	<i>Current Implementation</i>	26
8.3.3	<i>Connection Management</i>	26
8.3.4	<i>Details</i>	26
8.4	Multicast.....	27
8.5	Agents	28
8.6	Location Awareness	28
8.7	Public Key Infrastructures for Security	29
8.8	Quality of Service	29
8.9	Active Networks	30
8.10	Dynamic Service Discovery	30
8.10.1	<i>Motivation</i>	30
8.10.2	<i>Architecture</i>	31
8.10.3	<i>Implementation</i>	32
8.10.4	<i>Evaluation</i>	32
8.11	Summary	32
9	TRANSITION TECHNIQUES (D9, D17).....	34
9.1	Introduction	34
9.2	IETF Activities	34
9.3	The IPv6 Operations Working Group and 6WINIT Mechanisms	34
9.4	Tunnelling Mechanisms	35
9.5	Translation Mechanisms.....	36
9.6	Application Level Gateways.....	36
9.6.1	<i>Real-time Media Applications</i>	36
9.6.2	<i>The TZI Gateway</i>	37
9.6.3	<i>The Mbone Conferencing Application</i>	37
9.6.4	<i>The Slite Agent Framework</i>	37
9.6.5	<i>The ULTIMA Gateway</i>	37
9.6.6	<i>Summary</i>	38
9.7	Conclusions	38
10	GENERIC APPLICATIONS (D16)	39
10.1	Weather Station.....	39
10.2	Agent Frameworks	39
10.3	Location Aware Applications	40
10.4	Home Environment Applications.....	40
10.5	Streaming Applications	42
10.6	Conferencing Applications	42
10.6.1	<i>Architecture</i>	42
10.6.2	<i>The Internet Multimedia Conferencing Architecture</i>	42
10.6.3	<i>Implementations</i>	43
10.6.4	<i>Evaluation</i>	44

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

10.7	Voice over IP	45
10.8	Other Applications	45
10.9	Conclusions	45
11	THE CLINICAL APPLICATIONS (D3, D14, D19).....	46
11.1	Access to Clinical Records	46
11.1.1	<i>Overview</i>	46
11.1.2	<i>Access Networks</i>	47
11.1.3	<i>Security Infrastructure</i>	47
11.1.4	<i>Transition Strategies</i>	47
11.1.5	<i>General Conclusions</i>	47
11.2	The Applications in Krakow.....	49
11.2.1	<i>The Applications</i>	49
11.2.2	<i>Network and Equipment</i>	49
11.2.3	<i>Adaptation of Application Packages to IPv6</i>	50
11.2.4	<i>Security</i>	50
11.2.5	<i>Generic Technologies</i>	50
11.2.6	<i>Radio Interference Tests</i>	51
11.2.7	<i>Conclusions</i>	51
11.3	The Guardian Angel System (GANS) and the Ambulance Scenarios	52
11.3.1	<i>Introduction and Overview</i>	52
11.3.2	<i>Technical Abstraction</i>	53
11.3.3	<i>GANS as a Middleware System</i>	53
11.3.4	<i>Security and Transition Mechanisms</i>	53
11.3.5	<i>The Clinical Applications</i>	54
11.3.6	<i>Communication requirements from the clinical viewpoint</i>	54
11.3.7	<i>Evaluation of the GANS - The “Proof of concept” study</i>	55
11.3.8	<i>Clinical problems to be solved</i>	56
11.3.9	<i>Potential of GANS for the Healthcare sector</i>	56
11.3.10	<i>Conclusions</i>	57
11.4	Conclusions and Comparisons.....	58
12	THE DEMONSTRATIONS (D16, D17, D18, D19).....	59
12.1	IST 2001 (QR4)	59
12.2	INET 2002 (D18).....	60
12.3	IST 2002.....	60
12.4	Final Review	62
13	OVERALL EVALUATION	63
14	ACRONYMS AND ABBREVIATIONS	65

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

1 INTRODUCTION

1.1 Background

This project was conceived in the beginning of 2000. The financial climate of the industrial partners, and the expectations of the Communications Industry were quite different from the climate a year later, when the project started. This impacted many parts of the project. The most important of these were in the availability of 3G network facilities, the probability that there would be a rapid financial return from its introduction, and hence the availability of both the network itself and the readiness to develop new components for it.

While the mobile community retains a strong interest in IPv6, its move to introduce it in commercial networks has moved several years beyond the horizon of the 6WINIT project; this has strongly impacted the range of networks available for the project. It has also impacted severely the rate of development of IPv6-enabled telephones and PDAs.

The progress by the main hardware providers has remained strong in IPv6 – but more in an R & D aspect than large-scale commercial deployment. There has been steady progress in the availability of IPv6 stacks in all components – even though this has been a little slower than expected in 2000. An important aspect has been that there have been such frequent updates in software, that it has been hard to track the upgrades.

1.2 Overview

The project has embraced a number of different types of component: end stations, routers and relays, generic technologies, different network technologies and applications. They require a variety of standards – many of which have been evolving during the project. Almost all the components have been used as part of applications and/or demonstrations. Many of the applications are generic, and can be used in their own right. However a major emphasis in the project has been on clinical applications; these have been found to be a fertile, but demanding, user of the developments from outside the clinical area. The clinical partners have found, in turn, that it has been very instructive and useful to work with their technical partners.

1.3 Method of Evaluation

For each type of component, we have first summarised the component, including its characteristics, and then tried to analyse its strengths and weaknesses. In the process we have extracted material from the individual Deliverables in sufficient detail that the analysis makes sense. We have then tried to state which aspects of the components need further work - and why. Because we have had no experience of UMTS and IPv6 together at the time of writing, and will have little by the end of the project, we have had to base much of our UMTS evaluation on extrapolation from our experience with GPRS and 802.11b WLANs.

1.4 Structure of this Report

Of course this report in no way gives the level of detail of the other Deliverables. For this reason we have indicated with each section which Deliverables will give most supplementary material on the contents of that section. In Section 2, we consider the network standards, which most impact

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

the work in 6WINIT, and in Section 3, the corresponding Health Informatics ones. In Section 4, we say a little about the underlying architecture that is assumed. This section also indicates clearly what areas are not considered appropriate to address in the project.

In the following sections, we concentrate on the different aspects of the work done in the 6WINIT project. In Sections 5-7, we evaluate the work on networks, terminals and servers, and routers and relays. In most cases we restrict ourselves to the work done in the project; we do not try to provide a general survey of the field. In Section 8, we consider generic technologies, which are needed to make applications work in the 6WINIT environment. Although we are concerned principally with IPv6 environments, we realise that IPv4 networks will remain for some time. For this reason we analyse, in Section 9, our work on transition technologies.

6WINIT was always intended to be a systems project. The scene has now been set for complete applications and their evaluation. In Section 10 we consider the generic applications that are being brought in to stress the IPv6 wireless Internet. Some of these are merely because they existed at the start of the project; others were introduced because they were considered important in their own right. In Section 11, we consider the corresponding clinical applications. Here it was less a conscious choice of possible clinical applications, than a choice by our clinical partners of what applications they thought might have particular leverage in their environments. These made extensive use, of course, of the components of the earlier Sections – but always in the context of specific clinical situations.

It was a fundamental tenet of the project that we would try to demonstrate almost everything on which we worked. There were a number of particular international events; what we demonstrated there is discussed in Section 12. Finally some general conclusions are presented in Section 13.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

2 THE NETWORK STANDARDS (D15)

2.1 The Assumptions

We are assuming that the stated intentions of the principal Standards bodies will indeed be followed. From the Internet Engineering Task Force (IETF), this means that they will indeed modify their standards to meet the more urgent needs of the wireless community. From the UMTS operators, this means that they really are intending to move to an all-IP, IPv6 architecture. So far everything done in 6WINIT has been within an all-IPv6 framework – except where we have looked at transition problems. Facilities such as IPv6 DNS are provided by partners, but not all facets of a full IPv6 site deployment would be present in the constrained 6WINIT environments (e.g. no IPv6 email).

We are not envisaging that the move to IPv6 will be sudden and immediate. That is why there is considerable work in transition technologies in the project. However everything demonstrated has been within an IPv6 framework. We also assume that any of the problems in current implementations – of software, hardware, standards and services will eventually be solved. We are justified, therefore, in pursuing applications with very demanding requirements, which will not be met with the present offerings.

We are making another big architectural assumption, for which the evidence is still shaky. We are assuming that eventually there will be an all-IPv6 solution, where the difference between doing something over WLANs and UMTS (or post-UMTS), is seamless. We say that this is shaky, since it is not yet obvious that this will occur within the next decade. The UMTS operators are much more concerned with being backwards compatible with GSM than with WLAN!

2.2 Implementations

The project has been making considerable input to the IETF standards. We attended every IETF meeting, and provided reports back. Moreover, we participated also in the activities of 6LINK, the IPv6 Cluster project, so that we benefited from, and contributed to, the wider knowledge of IPv6 standards in the European IST community. The parts of IETF standards of most relevance to 6WINIT were those on mobile IP, extension of Mobile IP to mobile routers, anycast, multi-homing, DHCP, ENUM, SIMPLE, *ad hoc* networks, mobile VPNs, mobility management, secure bindings in MIP, reverse routing, mobile IP AAA, robust header compression and access networks.

The 6WINIT partners have also been active in the UMTS committees, albeit to a lesser extent. We have identified the different places where there are still major discrepancies between the two bodies. These include whether to use Mobile IP, to what extent the continuous media streams will use an all IP package, whether IPsec will be used at all for media streams, mechanisms for QoS and transition strategies.

We have participated in the IETF Working Party on 3GPP – IETF reconciliation. At present this is mainly concerned with analysing the scenarios. The decision on whether to start off with IPv4 and then migrate to IPv6 or start off with IPv6 has not yet been made. It is clear that some areas are more urgent than others – for instance with the IP Multimedia Subsystem (IMS), some decisions are very urgent.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

2.3 Utility

The project has assisted in providing input between the two communities. It has helped speed up certain of the IETF standards, but has had less impact on the changes in the UMTS standards. The fact that many of the 6WINIT participants have been sensitised to the considerations of mobile working, will have a strong influence on how informed these same attendees will be in future activities in these standards bodies.

2.4 Evaluation

This aspect of the work has been essential, and the project has had an almost unique position in being across the two communities. This melded well with the technical work also being across the two communities. If there had been a realistic chance of having a deep experimental involvement with UMTS, the input to that activity would have been greater. However the 6WINIT partners were concerned with activities that they felt could be validated experimentally during the project; it was clear by the end of the 1st quarter of the second year that this could not be the case – though no fault of the original planning, but due to the major slowdown in the UMTS deployment. Many of the 6WINIT participants in the Standards Bodies will continue there activities in the future under other auspices; the fact that they have done so with 6WINIT interests will have a long-lasting impact.

We have considered various forms of security in the project; we have not, however, implemented the simplest form of 802.11 WLAN security – namely the use of the Wireless Encryption Protocol (WEP) since we did not feel it to be sufficiently secure - and various forms of WLAN authentication. These subjects do need to be considered for production use; without them the use of WLANs will probably be considered hopelessly insecure. It is already not permitted to use unencrypted WLANs in most commercial or defence establishments just because of this insecurity; using WEP on a consistent basis would head off some of these concerns.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

3 THE CLINICAL STANDARDS (D15)

3.1 The Assumptions

Wide use of the sort of applications piloted in 6WINIT for the health sector require that there be relevant and agreed standards. We assume that the current practice of carrying out all standards inside a specific health application will be agreed to be too expensive and impractical, as broader communications mechanisms are introduced to deliver the services.

3.2 Implementations

The 6WINIT partners have been very active in the implementation of the CEN standards for Electronic Health Records. They have also been very concerned with the development of open standards for delivery of services and products from different vendors. They are active in the standards for message-based communications in health records, in standards for images, and security.

3.3 Discussion

The principal standards applicable to the 6WINIT technical partners relate to networking, wireless and security protocols, mainly developed through the IETF. The focus of health informatics standards, usually addressed by CEN/TC 251 and ISO/TC 215, has been to achieve data and service level interoperability at the application layer. This might be expressed, for example, as messages or middleware services. A range of security standards has also been developed, for example for healthcare enterprise security policy, password management, and encryption. In security the tendency has been to adapt generic standards for health service use rather than to develop independent or *ad hoc* healthcare-specific standards. We do consider the impact of 802.11b WLAN operations on some classes of hospital equipment in Section 11.2; we have not considered the more general question of whether this equipment could be harmful for any hospital equipment. This last is a subject which will have to be investigated before the production use of WLANs in hospitals is permitted.

The majority of current standards focusing on the interoperability of health data have envisaged communications taking place asynchronously through messages between healthcare enterprises, rather than as real-time communications to support distributed or mobile healthcare personnel. This trend is changing, and this section of the deliverable report has summarised the progress of the CEN EHRcom and HISA Task Forces, and of the HL7 CDA, all of which are specifically targeting clinical shared care.

The healthcare sector has historically been slow to adopt new technical solutions and to adapt its business processes to take advantage of them. There are many reasons for this, including the low overall spending on Information and Communications Technology (ICT) compared with other sectors, which is now being rectified by many EU member states through extensive modernisation programmes. Ethical and legal concerns over distributed (and especially mobile) systems are gradually being tackled, with several recent demonstrators across Europe showing, for example, that simple WAP applications (via WAP phones) can provide acceptably secure access to patient data and alert messages.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

Another major obstacle to the growth of mobile technologies in healthcare has been the lack of interoperability between clinical applications, requiring the prohibitively expensive bespoke development of interfaces to support every shared information interaction.

The set of standards now in the pipeline has every possibility to enable next-generation clinical applications to be fully interoperable. The demonstration within 6WINIT of successful mobile applications, including their security via IPSec (although so far only over wireless LANs), should help to stimulate the adoption of these technologies. From a standards perspective, the rigorous security provided by IPSec must be extended to GPRS and UMTS wireless communications, and further demonstration is probably required of how this can interwork in practical healthcare settings with PKI services and strong authentication including biometrics.

Health informatics standards, for example the intended EN 13606 through EHRcom, need to include the features by which access control and disclosure policies for electronic health records can be represented for a large and distributed set of healthcare professionals.

Standards for specific data types, such as images and waveforms, have largely been driven by industry and co-ordinated through professional or not-for-profit organisations (such as DICOM and openECG). DICOM is already a widely adopted standard internationally and is used to enable the communication of images and other multi-media health data between heterogeneous applications.

Migrating the present use of the Internet towards IPv6 is more an issue of national policy than of legislative standards. National health service and e-Government strategies refer to the eventual migration to IPv6, but the samples reviewed (e.g. UK, France) do not yet specify a schedule for this to become a formal part of the infrastructure framework

3.4 Evaluation

The standardisation processes needed to advance the wide-scale adoption of IPv6 within the health sector are very much 'work in progress', with further standardisation and standards uptake needed to enable clinical data interoperability and thereby to expand this market. National policy within EU member states on the migration to IPv6 probably needs to be more directive. The combination of multi-country partners, real demonstrations and close contact with the technical standards partners, has contributed to making this aspect of the work unexpectedly useful.

The participation of healthcare professionals in 6WINIT has brought the realisation of the need for a number of changes required in the national healthcare policies, legal background, clinical personnel acceptance, patient attitudes (e.g. to their records being shared across sites, including consent for disclosure). This will clearly be reflected in future changes in Standards.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

4 THE ARCHITECTURE (D6, D11, D15, D18)

4.1 The Assumptions

While this project requires both wireless networks and wired ones, the main focus is on the wireless portion – and its interface to the wired system. Since the 6WINIT project is focusing on building IPv6-based networks we address also the problems and solutions connected to the co-existence and interoperability with the IPv4-based networks and applications. The security and QoS (Quality of Service) problems and solutions of the IPv6 based networks are outlined. Thus the architectural considerations underpin the whole project.

The integration of voice and data brings many changes to the wireless network. New types of network elements and new protocols are being added, including ATM and Frame Relay and IP routers, and the number of network elements is increasing. Furthermore as demand for data services grows, it also means that the network usage and the number of services offered will increase.

The business model for wireless services is also changing. The cellular network operators expect to do more than simply provide wireless access to communication systems. They will also carry data and provide part of the content sent across their networks. So the network operators assume that subscribers will also pay for the value of that content or for an agreed service (level), rather than for usage time. Price, coverage, availability of services, and quality of service will all affect a subscriber's choice of service provider and access type. In addition to factors that affect traditional voice networks, such as voice quality, dropped calls, congestion in network, roaming and customer service, there will be new factors as data speed, bandwidth, jitter and delay that will have an influence on customer loyalty.

In this environment, the network operators have to offer different wireless access technologies supporting vertical handover between varied access networks in order to meet the desired quality of service aspects. Nevertheless, the incumbent wireless operators are very concerned with maintaining the customer base, and backwards compatibility with their GSM customers. This causes severe problems, since their audio, video and messaging standards are quite different from the Internet ones. If they are backwards compatible with GSM, then they will not be compatible with the Wireless LAN standards – since these in turn are compatible with the wired ones and an all-IP world.

The continuous growth of mobile users requires that its overall architecture evolve to accommodate the new technologies that support the growing numbers of users, applications, appliances, and services. IPv6 is designed to meet these requirements and allow a return to a global environment where the addressing rules of the network are again transparent to the applications. Standards bodies for the wireless data services are preparing for the future, and IPv6 provides the end-to-end addressing required by these new environments for mobile phones and residential Voice over IP (VoIP) gateways. IPv6 provides the services, such as integrated auto-configuration, QoS, security, and direct-path mobile IP, also required by these environments.

In the 6WINIT architecture, we largely ignore the obvious inconsistencies still existing between the Internet and UMTS standards. We assume that these will eventually disappear. We assume, therefore, that the wired Internet is the normally implemented, IPv6-enabled one, and that we can work with GPRS, UMTS and WLAN as if all the payloads will be IPv6 eventually; if we have to worry about transition, it is only between IPv4 and IPv6 – not between the partial IP solutions of even UMTS v5 and the IETF. We assume that mobile IP will be used partly to support mobility,

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

and partly to disguise differences between the cellular and wireless LAN operations. We consider on the whole only the Internet versions of security – largely ignoring the SIM-based ideas that are so popular in the UMTS community. One reason is that the UMTS ideas are still not fully explored, and we have had no lengthy access to UMTS. Moreover, the UMTS used at Kista does not even support Release 5 yet, so that none of the standards that are designed to assist conversion are yet supported.

We assume also that the wireless operators intend to provide any services for which there is a market but that they do not really know what these services are yet. For this reason, there is a considerable future for a number of forward-looking offerings, even if the operators do not yet know which they might offer. A lot of the architecture here assumes sophisticated processing at the boundary between the wired and wireless boundaries.

It is not the intention of the 6WINIT project to address the air interface for wireless systems. Nevertheless there has been some work on micro-mobility, as well as the normal Mobile IP activity.

4.2 Implementations

It is not quite clear that the format adopted for technologies and applications is equally relevant to architecture. Nevertheless, we will mention some of the activities implemented. There are different versions of location awareness inside buildings and over UMTS. Inside buildings, these will often be derived from triangulation from routers in the building; outside one can use either the facilities provided with UMTS, or those provided with the Global Positioning System (GPS). An activity has been shown in this area, and integrated in with applications.

Multimedia conferencing remains an interesting application for many reasons. There are two different approaches - the ITU-T/H.323 series of recommendations and the Internet Multimedia Conferencing Architecture of Section 10.6. Different aspects have been pursued in the project for the two. Both approaches media/UDP; thus the implementations of many of the conferencing audio and video codecs can be used with either mechanism - in fact, portions of the Mbone tools of Section 10.6 can be used both for multimedia conferencing, and for Interworking with tools for VoIP.

For real-time media transport, both approaches rely on RTP -- but they provide different models and protocols for conference control and signalling. While H.323 has gained quite a lot commercial importance in the past, SIP is agreed to be adopted for the UMTS IMS. To date, both technologies are usually deployed with IPv4 only, as most endpoints and intermediate systems that are currently available are still limited to IPv4. However, some first IPv6 endpoints have recently been developed and made available. For this reason, one approach adopted in 6WINIT is to provide IPv4 and IPv6 interworking services for both H.323 and SIP (the TZI gateway of Section 7.2.1). In order to provide conferencing services for heterogeneous networks, media adaptation can be employed in order to achieve bandwidth-efficiency, interoperability for otherwise incompatible endpoints and other services such as multicast-to-unicast relaying. These functions can be accomplished by media gateways which can reprocess the media streams. The processing may be simple, like blocking complete media, reasonably straight forward, like blocking most of the packets for certain destinations for certain media (e.g. packet video, leading only to a reduction in frame rate); some may be even more complex like requiring media transcoding. The implementation of this device is the UCL Transcoding Active Gateway (TAG) of Section 7.2.2, and the TZI Gateway also provides media processing capabilities. A variant of the TAG, appealing to the uncertainty of the operators in what they want to provide, involves using Active Network techniques to load the TAG dynamically, when there is a demand from a wireless user. A third variant of edge processing is the 6WIND support in their routers for edge

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

services; this includes the Mobile IP of Section 8.2, dynamic VPNs and the Road Warrior of Section 8.1.

The more such varieties of edge services exist, the more it is necessary to support some form of neighbouring service discovery of Section 8.10. Such a mechanism has been integrated with the TAG work, but should be used much more widely.

4.3 Utility and Evaluation

All the implementations mentioned above have been tested at several sites. They have either been shown already at INET 2002 or IST 2002, or will be part of the Final Review. They have all been shown to work, though the services they support are still rudimentary. Often the implementations were actually introduced from other projects in which the partners were engaged.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

5 THE NETWORKS (D11, D18)

5.1 Fixed IPv6 Networks

The 6WINIT partners have been connected by the 6Bone network throughout the project. This gave them the basic connectivity needed in the early stages. Unfortunately the latency and bandwidth of this connection was very variable, and was often inadequate for real-time services like audio and video.

In early 2002, both the 6NET and the Euro6IX projects started. By mid-2002, 6NET was connecting, via native IPv6 mainly, all the NRENs of the European partners in 6WINIT. There were National Pilot NRENs in most of the partner countries able to provide IPv6 connectivity in Denmark, Finland, France, Germany, Korea, Poland, Sweden, Switzerland and the United Kingdom – i.e. all the countries from which 6WINIT partners came. The commercial partners in Denmark, France, Germany, Switzerland and the United Kingdom were not connected to these IPv6 NRENs. However several of these commercial partners were part of Euro6IX (6WIND, Ericsson, T-Nova, BT); these were able to come in via the Euro6IX IPv6 exchanges, which were connected to DFN (Germany), Renater (France), UCL (United Kingdom) and Nordunet (Denmark, Finland and Sweden). Thus all partners needing the connectivity could get it through these newer networks – with performance quite adequate for the multimedia communications required. Here the throughput was typically tens of Mbit/s, and the end-to-end transit times tens (or even hundreds) of milliseconds.

5.2 Wireless LANs

Most of the partners put in Wireless LANs supporting 802-11b; i.e. 11 Mbit/s. These could provide a net data flow of around 5 Mbit/s with very low delays. Moreover because WLANs are at layer 2, it was no problem to have these IPv6-enabled. A full range of interface cards and their relevant software were available at low cost; these were used heavily in the project. Nevertheless, at present a WLAN access point can only be managed over IPv4, so unless its just run completely "out of the box" it needs dual-stack on the wired link, even if the air link is v6 only. This is still one of the missing pieces mentioned in D18.

5.3 GPRS

5.3.1 Functionality

GPRS is a wireless system with a number of time slots in a cell; each time slot is capable of achieving about 13.4 Kbit/s on the tested networks, which utilise the CS2 coding scheme. The different operators configure their capability in different ways; typically up to four time slots are available to a subscriber. The number of times slots utilised is largely dependent on the capabilities of GPRS handset devices, for example, some provide one time slot upstream and three downstream (13.4/40.2 Kbit/s); in others it is a symmetric 2/2 (26.4/26.4 Kbit/s). There is a large range of device classes, though currently available devices do not provide for access to more than a maximum of four timeslots.

All operators support only IPv4; so if IPv6 is to be used, it can only be as IPv6/IPv4 – further reducing the bandwidth available. The operators have varied policies on addressing; some allow only dynamic addresses, some only private addresses, and some restrict the addresses that can be

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

used with certain servers. Roaming agreements between the mobile operators used in 6WINIT came into existence only in the second half of 2002. GPRS roaming has not developed in the most obvious direction. Mobile Operators want to keep close control over their customers therefore the current approach is to tunnel the GPRS connection back to the home network of the subscriber. This makes it easy to keep the same configuration for the terminal equipment while abroad, but adds further to the delay experienced. The other approach would have been to terminate Internet connections right in the visited country.

5.3.2 Availability and Cost

By mid-2002, GPRS was available for most of the uses needed. It was required only in Denmark (for IST 2002), Germany (for IST 2001), Poland (for use in their demonstrations), Sweden (for the final Review), and the United Kingdom (for applications testing) and the US (for INET 2002).

In the US (for INET 2002) it was just not available to the partners. In Germany (for IST 2001), it was available; however it did not reach inside UKT, which is where it was actually needed; the restriction to dynamic addresses, and the blocking of ping, made its use difficult for 6WINIT purposes. In Sweden it was available in Stockholm, where the Final Review is being held.

The cost was so high that it would make GPRS unsuitable for many applications; it is clearly targeted at specific WAP applications by most operators. While we have used it for VoIP, its cost is unaffordable for many real multimedia applications – though in any case only voice can be carried because of the limited throughput.

5.3.3 Performance

In the UK, as in other countries, the channels were configured automatically, with up to two channels on the uplink and three on the downlink. We found that we could transmit UDP packets at a maximum of around 21 Kbit/s on the uplink and around 31 Kbit/s on the downlink. Occasionally the throughputs would drop to substantially lower values for tens of seconds. The networks only supported IPv4, so that the applications had to use IPv6/IPv4 tunnels; this was very inefficient. In the UK case we needed to have a 256 Kbps direct channel back to BT, where they ran an IPv6 Server; the costs of the server and its direct channel were borne by BT. T-Nova bore any GPRS costs in Germany, but did not have to make such special arrangements; one only accessed GPRS services on a switched basis. In the BT case, it took nearly six months to be able to access the BT server from UCL. This is because it was not a completely open server, and UCL was not part of BT; the difficulties are related to the fact that GPRS for retail customers is regarded as an IPv4 WAP service by many carriers, and there can be difficulties in connecting in others to the Corporate GPRS services, because of differences in billing systems.

At its best, the latency was around 0.4s; however at start-up or when the links are congested, this latency can rise to many seconds. Some of the results in D18 show delays of 5-8 seconds in the two directions.

5.3.4 Cards and Drivers

The situation with cards and drivers were not too good either. In the end, five different GPRS cards were acquired – some of them even supporting WLANs and GPRS. However the availability of drivers was poor – particularly for Linux, which was our preferred choice for some applications. Most of the cards we found did not allow the user control of the number of channels used; this could be very serious in some conferencing applications. None of the cards supported *simultaneous use* of GPRS and WLANs – even when both were supported. This was unfortunate

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

for the applications where one wished to switch between WLAN and GPRS terminations, when the workstation came in range of a WLAN.

Overall, the utility of GPRS for the 6WINIT applications was very limited.

5.4 UMTS

Initially we were promised UMTS access in many partner countries. In the end neither of the carrier partners were able to provide such access during the period of the project. This was a direct consequence of the slow-down in deployment plans of the carriers, and the decision to hive off the wireless carriers into very separate entities. With both T-Nova and BT, it was the R & D components involved – not the wireless operators; incidentally, the same occurred with NTT, where the partner was not NTT-DoCommo. As a result, there was no access to UMTS prior to the last two weeks of the project (when it had been extended a month).

Luckily, Ericsson offered to provide access to their test facility in Stockholm. This has very limited facilities – supporting only PPP, and one terminal at a time. However we have been promised that the service will be connected to the 6NET location in Kista, Sweden – allowing UMTS access to remote services via IPv6 end-to-end. We cannot at this point provide performance or functionality results based on experience with the 6WINIT applications; we hope to provide these, however, during the Final Review.

5.5 The Partners' Local Infrastructures

Most of the partners put in WLANs, Fast Ethernet, and connection to WANs – all IPv6-enabled. Various makes of WLAN were used – with no interoperability problems. For IPv6 routers, there were a number of Ericsson-Telebit routers – used in the IST 2001 and INET 2002 demonstrations. These had been intended as an interim for the new Ericsson product; when this was delayed, partners outside Ericsson were not interested in acquiring the older product. Nevertheless, it continued to be made available by Ericsson to those partners desiring it; indeed it was the only product optimised for UMTS use; it was used regularly for the GANS application of Section 11.3, and the only one implementing the simultaneous multi-access of Section 8.3. Cisco routers were used by some partners to provide ordinary access for IPv6 services; indeed these were the main access routers used for 6NET access and Euro6IX access by the 6WINIT partners. However, the IPv6 versions of the Cisco products did not support some of the advanced features that the applications wanted (multicast, anycast, Mobile IP, and active services). Hence most of the partners planning demonstrations were provided with 6WIND routers. Any of the partners requiring such access, connected themselves either directly to a 6NET or a Euro6IX node – using IPv6/IPv4 encapsulation through an NREN or ISP in some cases. Here the partners used FreeBSD routers a lot, but also Telebit TBC2000, 6WINDGate 6200 and Hitachi GR2000.

5.6 Summary

All the partners put in a reasonable IPv6 infrastructure to allow experience with their applications. Most also put in WLANs – and these were used extensively also in the demonstrations. About six partners put in GPRS access facilities – though they made very limited use of them. Nobody was able to put in UMTS access facilities except Ericsson Research. The others plan to test their GPRS-enabled applications over UMTS in the Final Review. In general, GPRS facilities were found to be too limited and expensive for extensive 6WINIT use. There would have been no access to UMTS, if Ericsson had not made it available for the last two weeks of the project on their site.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

6 THE TERMINALS AND SERVERS (D10, D13)

6.1 Laptops

6.1.1 Operating Systems

Four operating systems (OSs) were used in the project: Linux, Microsoft Windows, Solaris and FreeBSD. Obviously various dialects of each were used. There was no project-wide agreement on what was to be used; it depended partly on the application needs, partly on the facilities available under each operating system, and partly on timing. Since this was a comparatively short project – two years, OS decisions had to be made fairly early by each partner. Thus, for example, the IPv6 versions of Java were not available for Microsoft Windows; this made it unusable for many of the applications.

The majority of the applications used Linux, since this was the best balance between availability of drivers for the cards and availability of IPv6-enabled facilities such as IPSec, Mobile IP and Multicast, and Java language support. Unfortunately several of the newer GPRS cards, or GPRS/WLAN cards, did not come with Linux support. As a result, many of the partners landed up buying cards that they have not been able to use. In at least one case, the GISMO card, there is an on-going development agreement between the supplier and a 6WINIT partner, so that the card may still be usable eventually.

There was a most unfortunate conflict between the OS needs for middleware and drivers; this resulted in a very considerable waste of effort. It also led to above average OS-support needs by the 6WINIT partners.

6.1.2 Applications

The majority of applications were put onto laptops, because they were the best combination of portability availability of network interfaces and ease of programming. In most applications, only laptops were used. Only in very particular cases were PDAs employed.

6.1.3 Utility

While clearly not as portable as PDAs, the smaller laptops were considered the best development and utilisation platform. With laptops, it was usually possible to completely configure the device at the home base, before taking it to a remote site for integration and/or demonstration. Moreover, the power of laptops was quite adequate for all the applications (and routers) being used in 6WINIT. Finally, laptops had a good range of network interfaces, cameras and audio devices. The only problem was when too many simultaneous interfaces were required.

6.2 PDAs

For PDAs, we used entirely iPAQs in the project. These were not the only PDAs that could have been used, but the iPAQ had a good Linux implementation, with Mobile IPv6 support from the Helsinki University of Technology (the HUT Linux). This now comes with the Familiar Linux (<http://familiar.handhelds.org/>). There is no Java for iPAQs that supports IPv6 out of the box (blackdown.org is only offering Java 2 version 1.3 that has no IPv6 support) – it is necessary to

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

add some additional patches to use JAVA for applications on the PDAs. While we were developing the applications, several improvements in the hardware were made. This meant that each new model was significantly more powerful than the previous one; there is no sign that this cycle has ended.

Towards the end of the project, we did receive Microsoft WINDOWS-CE versions of IPv6 code for PDAs, including Mobile IPv6. Presumably we could have tried to use these in the project. However these arrived so late, that none of the partners still had time to port their applications to these platforms.

Interesting support cards were produced for the iPAQ, which meant it would have been possible to use the devices for GPRS and WLANs without the need for a telephone; unfortunately, however, these devices did not have Linux drivers. They could not, therefore, be used.

6.3 Telephones

It was originally intended that there would be a significant usage of GPRS and UMTS from Ericsson telephones. There was indeed a suggestion that there would be complete IPv6 stacks available to the project on such phones. In practice, the coupling between that part of Ericsson and the project was not very strong – since early in the project it was decided that all telephone manufacture would be transferred to a new Ericsson-Sony company. Moreover, the lateness of the deployment was matched by the lateness of UMTS. To date only Ericsson Research, amongst the 6WINIT partners, has managed to obtain a UMTS phone.

The GPRS phones were state of the art, and were purchased by several partners; Ericsson and Nokia were the main phones used. Unfortunately, while these had very limited capability for inputting Java programs, this capability was not used in practice. Phones with built-in WAP browsers were used in some of the clinical demonstrations – but this was not even with IPv6. For the more sophisticated GPRS applications, one used PPP connections between a laptop and a GPRS telephone.

Several IP telephones have been used for developing and testing the 6WINIT-VoIP-components - - the set of telephone includes products from Cisco, Pingtel and Siemens.

It will be necessary to improve the development tools and interfaces for telephones significantly, before it is justified to program them directly for this type of project.

6.4 Summary

While a variety of operating systems were used, Linux turned out to be the system of choice – with the most advanced set of facilities and a reasonable range of equipment; some applications used Windows, however. For portable appliances, laptops remained the equipment of choice – though iPAQs running Linux became quite popular near the end of the project as their power increased, and Java support became available. Virtually no use was made of telephones by themselves; none had IPv6 support, and programming them was in any case very tedious.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

7 THE ROUTERS AND GATEWAYS (D8, D11, D17)

7.1 Edge Routers

7.1.1 The Ericsson Router

The Ericsson Telebit AXI 462 router was very suitable for 6WINIT purposes; its basic IPv4/IPv6 functionality had most of the functionality needed. It was, in fact, the principal router used in the earlier demonstrations. Unfortunately, however, the effort planned (from outside the 6WINIT project, became unavailable; therefore the development of the Mobile IPv6 stopped with V13 of the specifications. As a result support for authenticated MIPv6 along the lines of the latest versions of the MIPv6 specification was never provided to the 6WINIT applications. This, in turn, implied that the implementation was going to become increasingly at variance with the latest versions of the specifications, and that there was no scope for further developments to meet the needs of specific applications. As a result, it has been used in the later application work only by the GANS system of Section 11.3 – for which it was very suitable.

The new Ericsson Router product, the RXI 820 Realtime Router, was delayed and is being provided for the Stockholm UMTS demonstration at the Final Review only. Apart from supporting the basic IPv6/IPv4 functions of the AXI 462 Router, the RXI 820 is optimised with QoS mechanisms for real time wireless internet traffic (numerous small/UMTS size packets) and QoS (DiffServ). and supports more advanced transition mechanisms such as 6to4, configured tunnels and ISATAP. This router will support the UMTS access at the Final Review.

7.1.2 The 6WIND Router

The 6WIND Edge Router is the main component that has been used in the later applications. Some ten routers have been made available to the project partners. In some cases these were supplied originally for other purposes, such as the ANDROID and Euro6IX projects; however it has been agreed that they could be used for 6WINIT purposes. The basic IPv4/IPv6 functionality is exactly what is required. In addition, it continued to be developed to meet the needs of the applications. Thus its Road Warrior capability was enhanced to deal with certificates and be compatible with the Linux IPsec. Implementation of Mobile IP is continuing and following up the latest IETF drafts (currently up to release 19). Anycast implementations have been provided, which are needed for some of the Service Discovery work of Section 8. Specific VPN functionality, partly derived from the ANDROID project has been added.

The one problem with the router is that, being a commercial development, it has been necessary to freeze some aspects of its language support. While it supports code in Java running on the machine, this uses a version of Java 1.3, with some additions for IPv6 support. In fact the official Java releases have progressed significantly beyond the version used by 6WIND; this makes it difficult to include current Java application code in this router at the moment.

The result of the continued development of this router has made it a very suitable research vehicle for ongoing research. Several of the partners expect to continue using it in this role in future projects – and 6WIND has agreed to such usage.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

7.1.3 Other Routers

Two other routers have been used extensively in 6WINIT. Several of the partners use Cisco routers for their IPv6 and other infrastructures. These can be IPv6-enabled, and are able to provide much higher throughputs than the other routers mentioned. However, there is less scope for experimental software to be incorporated – other than the experimental versions being put in by Cisco itself. Hence for the purposes of 6WINIT, where Mobile IP, Anycast and multicast were important, it was more convenient to use the 6WIND or Ericsson routers. In other projects, where Cisco is also a partner, use of Cisco routers is very appropriate; if there are specific needs of the project, Cisco can then provide them.

Another router, which has been used extensively for different purposes, is a PC router using the Open Source Kame software. This has much advanced functionality – often even newer than the 6WIND – this applies to Mobile IP, multicast and IPSec support. For those experimental functions, which have not yet been put in by 6WIND, this router has proved very useful.

7.2 Gateways

Two gateways have been developed and employed with quite different functionality to the routers of Section 7.1. One is the H.323 – SIP gateway of TZI, and one is the Transcoding Active Gateway of UCL. Both were developed originally in other projects, and then further improved for 6WINIT purposes.

7.2.1 The TZI Gateway

The TZI-Gateway provides both signalling and media gateway functions because for many applications it is required to provide gatewaying functionality for the signalling communication as well as for the media transport, e.g. in order to gateway between SIP and ISDN. However, the orthogonality of the functions suggests a clear separation of functional components. For implementing a conference bridge, a different feature set is needed than for implementing a SIP-H.323 gateway. The TZI-Gateway is therefore realised as a modular application - using the Mbus co-ordination protocol - that can be adapted to different needs.

The functionality has been discussed in some detail in D8 and D17. In the context of 6WINIT, it has already been used for enabling a number of IPv6 VoIP functions. Here the independence of the signalling and media transport functions is very important. SIP is agreed to be the signalling system of choice for many UMTS release 5 payloads; it is also the main signalling mechanism used in VoIP. However, SIP is not very common in many existing conferencing applications; this is one reason why this TZI gateway has proved very useful. Secondly its modular approach allows specific media processing and telephone functionality to be incorporated; for this reason it has been shown to be very useful for 6WINIT,

One large Open-source system incorporating SIP and VoIP is the VOCAL system from Cisco. Their source distribution was IPv4 only, and the bulk of the VOCAL porting was done in the Euro6IX project. Nevertheless, 6WINIT and IST 2002 allowed useful testing and bug-hunting of the system, and allowed interoperation with the TZI gateway to be achieved.

7.2.2 The UCL TAG

The UCL Transcoding Active Gateway (TAG) has some similarity with and some important differences from the TZI gateway. The similarity is because both were initially conceived in the MECCANO project and the differences are because the application concerns are quite different.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

Where the TZI gateway has concentrated on transformation of signalling, the TAG has adopted a client/server approach for this, with no special wider signalling components. The client can ensure that the TAG joins a conference or other service; the TAG can even be requested to join conferences by SIP. Knowledge of what to join, and how, most commonly comes from the Conference Store or the Session Announcement Protocol.

There are two considerable advances in the TAG over other gateways. It can be loaded dynamically, when needed, and has a powerful policy-based architecture for media adaptation. The first is important in the UMTS environment, since we doubt if we can persuade the operators to run specific operations unless there is a clearly expressed user need, and potential revenue. Media adaptation is clearly required in gatewaying to GPRS and UMTS from wider bandwidth conferences. A flexible architecture, which allows code to be loaded dynamically, only when requested by a user, is clearly valuable here. It should allow the operator to load this functionality only when users are willing to pay for it. The media adaptation is also a policy-controlled functionality; this allows the type of adaptation to be a function of the performance of the edge networks.

The basic functionality of the TAG was developed principally under the ANDROID project; there it was used, however, mainly to provide VPNs. Its extension to the needs of the wireless environment has been developed in 6WINIT.

There has been too little practical experience with either the TZI or the TAG gateways to ascertain how useful either is in practice. Both will be deployed more widely in later projects, and their functionality improved further in the light of experience.

7.3 Summary

The project did not have to consider backbone routers, since it was concerned mainly with access networks. Both the Ericsson router and the 6WIND router were used equally in year 1. By the middle of year 2, Ericsson had to reduce considerably their involvement in the project, and therefore no further work was done on Ericsson routers in the context of 6WINIT. This decision prevented the Ericsson team from spending resources from outside the project on developing prototype features for the RXI 820 – which would also probably not be available during the lifetime of the project. The AXI 462 continued to be provided free of charge to RUS/UKT, who continued to use it for the GANS work. While there were no particular such features, this deterred the other partners who might want further prototype features, and they did not request these routers. 6WIND, on the other hand, were both willing to deploy their routers, and were putting in the latest facilities in collaboration with the 6WINIT partners. As a consequence their routers became the one of choice, and versions of all the facilities needed became available on that router – at speeds quite adequate for the wireless environment.

Two gateways were developed which plugged the gap in the infrastructure available. The TZI gateway provides a transition service between IPv4 and IPv6 and media adaptation services for supporting conferencing in heterogeneous networks - both for SIP and H.323. Its SIP capability was also very useful in the VoIP space. The UCL TAG filled another role of multicast-unicast conversion and bandwidth management for media streams; both are clearly essential for 6WINIT purposes

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

8 GENERIC TECHNOLOGIES (D12, D16)

It is often difficult to distinguish between a *router and gateway*, a *generic technology* and an *application*. We make the distinction that the *generic technologies* can be used more widely. Thus the *Road Warrior* of Section 8.1, and the *location awareness* of Section 8.4 are generic activities, which could be used in many situations.

8.1 The Road Warrior

The Road Warrior software allows a mobile user to initiate a secure connection based on IPSec from itself to an IPSec gateway. Thereby it is possible for the mobile user to access securely, for example, a database located and protected behind an IPSec gateway via a network which is not secured, such as the public Internet. Furthermore the Road Warrior supports a kind of mobility in a way, that the mobile user can use an arbitrary IP address at its present point of attachment to the Internet, and set up the security association to the IPSec gateway based on this dynamically changing IP address. When a Road Warrior moves to another point of attachment and gets assigned a new IP address, it has to set up a new security association to the IPSec gateway based on the newly assigned IP address.

This mobility support is therefore opposite to Mobile IP in that it is not transparent to the application layer; that is after moving to a new point of attachment the mobile user has to use a new IP address and therefore all applications have to be restarted with this new IP address. Therefore a Road Warrior supports a type of applications, which have to access an insecure network on different points of attachment, but which have neither a requirement for a seamless roaming between these points of attachment nor for using always the same IP address in their applications. Some clinical applications belong to this type.

The Road Warrior implementation used in 6WINIT was one based on a client under Linux in the remote node, and on the 6WIND router. It used the correct X.509 v3 certificates required in the latest versions of the IPSec standard.

8.2 Mobile IP

With mobile IP, the functionality is the opposite of the Road Warrior. Now the mobile node keeps its permanent address, and notifies a *Home Agent* of this address. When it moves to a foreign network, it obtains a second *Care-of-Address* by an IPv6 auto-configuration process between the local router and the mobile node. This new address is notified to the Home Agent, which updates a local Binding Cache with the information. The Home Agent is able to redirect the traffic coming from the correspondent, which is not aware of the new location of the mobile node.

For the correct implementation, one requires a Home Agent, Mobile IP support in the router, and Mobile IP support in remote terminal. The Home Agent and remote terminal support used in most of 6WINIT are provided by the implementations from Helsinki University of Technology (HUT) and those in the routers are provided by the various routers of Section 7. For several reasons, mostly concerned with security, Mobile IP has gone through many iterations in the last few years (cf. Section 2). Both the HUT implementation and some of the router ones have tracked these changes.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

Ericsson Telebit attempted to provide a full MIPv6 implementation including support for both authenticated MIPv6 and IPSec and MIPv6 interworking in general. With this purpose Ericsson Telebit was quite heavily involved in the MIPv6 HA draft specification of these issues in the spring of 2002. However both the standardisation and continued implementation work stopped when they had to withdraw from the area in April 2002. At this stage only full support for draft v13 was available.

6WIND did continue the tracking, and their current implementation is almost compliant with the latest IETF Draft Standards; there is a commitment to provide the version of the definitive standard when it has been defined. Its implementation is quite usable, though its security capability (because of deficiencies in binding updates in the earlier releases of Mobile IP) still needs updating. Mobile IP is considered an excellent way of going between different network technologies – e.g. GPRS, WLAN and UMTS – since at the IP layer there is no dependency on the technology. It will not, however, address *simultaneous* access to different technologies, until one has also solved problems of multi-homing – where a single node has two simultaneous attachment points. The current interfaces, which support GPRS and WLAN, could work, because they normally support both interfaces – but only one or the other at any one time. It is this aspect of the work that Ericsson has pursued further (cf. Section 8.3).

Several of the clinical demonstrations showed that they could work with great advantage with Mobile IP, using the property of moving to different networks.

Some of the partners are also tracking developments from outside the 6WINIT project. For example, the newest KAME code seems to have MIPv6 Draft 18 support, but there was no longer time or effort in the 6WINIT project to integrate this into any demonstrations.

8.3 Multiaccess

Always-best-connected mobile Internet nodes in the future heterogeneous networking environment require an ability to seamlessly make use of and move between different types of access networks. These might be attached to personal-, local-, or wide-area networks, and use different link layer technologies.

Ericsson Research in Finland has implemented this functionality at the IP/network layer within a Multiaccess Mobile IPv6 stack. The implementation fully conforms to the Mobility Support in the IPv6 Internet-Draft. and therefore is compatible with any existing Mobile IPv6 nodes.

The implementation is based on standard Mobile IPv6 and is integrated into the Linux Mobile IPv6 stack (MIPL) provided by the GO research project at the Helsinki University of Technology.

8.3.1 Simultaneous Multiaccess

In Multiaccess Mobile IPv6, in addition to Mobile IPv6 handovers, IP traffic can be transferred between different network interfaces connected in a Mobile Node (MN). These may be called *vertical handovers*. Available interfaces are found by using the standard IPv6 address autoconfiguration. In addition, several interfaces may be in use simultaneously in one MN. This may be called as *simultaneous multiaccess*.

Many possible reasons exist for doing vertical handovers. For example, higher bandwidth, better signal level or different services may become available. Simultaneous multiaccess is needed, for example, when a user wants to stay connected in a corporate network through a GPRS access network while accessing a local WLAN-based commercial network.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

In Multiaccess Mobile IPv6, vertical handovers will also be *smooth handovers* (zero packet loss) if the old interface stays connected until all packets sent with the old Care-of-Address (CoA) have arrived at the MN. This implementation therefore supports session continuity and real-time performance while users are moving between access networks.

Multiaccess Mobile IPv6 solution does not require any modification to applications using IPv6 access networks or any additional nodes to the access network. The solution is also independent of access technology.

8.3.2 Current Implementation

Our design goal was that the implementation would change only the MN and that the Mobile IPv6 signalling and other IPv6 nodes would not require any changes. The implementation was also to be transparent to applications. Our intention was also to provide controllability of interface selection for the user.

The platform for the implementation was chosen to be Linux and the Mobile IPv6. The GO-project at Helsinki University of Technology provided us their Mobile IPv6 implementation, called MIPL.

The MIPL code has been modified to support multiple interfaces and multiple Care-of Addresses. The actual separation of traffic flows is done with special routing table entries for correspondent nodes or destination networks. These routing table entries correspond to the policy entries in the connection management and whenever the user changes policies, or the status of the network interfaces changes, these routes are updated accordingly. This way the packets are built correctly from the beginning of their traversal through the networking layers and no changes to them are necessary except for the standard Mobile IPv6 functionality replacing the home address with the Care-of Address and adding necessary destination options. These changes enable simultaneous multiaccess.

8.3.3 Connection Management

When using any multiaccess, it must be possible to configure and control the operation of this functionality according to the - dynamically changing - needs of applications and users. Multiaccess Mobile IPv6 currently implements a connection management capable of this.

Using the developed technology mobile users can dynamically define local policies where the preferred interfaces are listed on account of a connection association and possibly QoS-related information. Several possible interfaces can be listed in a priority order – the system automatically selects the best possible based on availability. The connection association information (destination IP address, destination port, and protocol) is received from the local IP stack. However, in future, the QoS-related information (e.g. bandwidth, price) could be retrieved from the end-user or applications via an API, or from the network. The connection association and QoS-related information could be used to select the correct policy that finally defines the interface for the outgoing IP packet. The current implementation includes interface selection mechanisms on account of the remote IP addresses (or domains) and port numbers of the connections.

8.3.4 Details

Both the Linux IPv6 and the MIPL were originally designed so that only one network interface could be used at a time. We first had to fix the IPv6 stack so that it would operate with several simultaneous network interfaces and routers. Then we modified certain parts of MIPL to make it

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

also support multiple interfaces. During the operation the IPv6 routing table and the Mobile IPv6 Binding Update List are updated, based on the user-defined policies and the status of the network interfaces. The policies are defined so that a destination address (host or network) has a list of interfaces in the preferred order. The system then uses always the best available interface for traffic destined to this address. Policies can be seen as instructions on how to select a network interface for a traffic flow under different circumstances. For example, the user may have defined a policy that has a destination address of his e-mail server, and the list of interfaces has the LAN interface as the first option, and WLAN as the second. This maps to the following actions: first, we create a routing table entry for the e-mail server and put the LAN interface as the outgoing interface for this route. We also put the next-hop address to be the IPv6 link-local address of the router found on the LAN interface. Then we update the MIPv6 Binding Update List to have the entry for the destination address, and the used interface. After that we send a Binding Update to the e-mail server, where the Care-of Address of the LAN interface is used and the message is sent through the LAN interface. That causes the return packets to come through the same interface.

The idea of policies was found to be an interesting research topic, which was further continued to inspect the usefulness of even more complex rules for changing and controlling the behaviour of the interface selection mechanism. This work resulted in a research paper, which documented our ideas and findings on a policy-based interface selection system.

The described functionality can also be used to change from one interface to another on a demand-basis. Further in our example scenario, the user updates the policy so that he changes the order of LAN and WLAN. In that case, the handover will be smoother, as the packets keep coming through LAN until the CN has processed the BU and start sending packets towards the CoA of the WLAN interface.

When none of the user's policies do match a so-called default policy specifies which of the interface should be used. In our solution there always has to be a default policy, which gives a list of interfaces that can be used, in preference order.

It is also possible that an interface is not listed in the policy, which means that it will not be used for any traffic that the policy defines. In the examples above, if the user adds a GPRS interface to his laptop, but does not update the policy, then his e-mail will never go through the GPRS interface, even if both LAN and WLAN interfaces lose their connectivity.

8.4 Multicast

Multicast in IPv6 has a special significance, because IPv6 does not provide any Broadcast mechanisms. Hence dedicated Multicast groups are used to implement Broadcast-like mechanisms. Nevertheless, IPv6 is still very much in the experimental stage for inter-domain usage. In 6WINIT, we were able to define a single domain, and hence were able to deploy multicast in a limited way – using the m6bone experimental facilities put in under the 6NET project.

With UMTS and GPRS, multicast is not available; thus services such as the TAG of Section 7.2.2 have incorporated a multicast-unicast converter.

Multicast is useful where a group of participants require to exchange data efficiently, or a single source wishes to distribute material to a large number of receivers. Such scenarios include the multimedia conferencing of Section 10.6 and the streaming application of Section 10.7. Local multicast is available over the LAN on individual subnets, and multicast plays a fundamental role in the operation of IPv6 (e.g. for link-local Neighbour Discovery and Router Advertisements)

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

where IP broadcast was used in IPv4. All the routers that are used heavily in 6WINIT and are listed in Section 7 support multicast. Similarly all the main Host operating systems support it.

The applications of the Agent Framework (Section 10.2), Streaming (10.5) and Conferencing (10.6) all can use it on their wired and WLAN portions; hence the need in 6WINIT of something like the TAG when wired and wireless users collaborate, and when GPRS or UMTS are used.

In 6WINIT the lack of an operational wide-area multicast infrastructure was only not very serious because the use of GPRS was so limited. In the 6NET project the provision of such an infrastructure is now of high urgency. UCL and UoS are participating in their m6bone work. It is important to note that in a WLAN a large multicast stream can saturate a flat WLAN network, which has no or little subnetting. Hence there is immediately a need of the sort of facility provided in the TAG in an operational setting.

8.5 Agents

There are many versions of Agent Frameworks. The one used in 6WINIT is Slite - a lightweight agent distributed agent architecture adaptation of the Southampton Framework for Agent Research (SoFAR). The framework uses a set of performance-based communication primitives to support auction based and argumentative agent negotiation strategies for Distributed Information Management tasks. It is implemented in Java 1.4, with IPv6 support running under Linux.

The use of IPv6 within the Slite Agent Framework, with its vastly increased address space, makes it feasible for pervasive devices within home environments to have global Internet addresses. Pervasive devices, which implement their own end-to-end security model (e.g. IPSec), are become feasible in this setting. The scoped multicast offered by IPv6 allows some control over how far agent capabilities are advertised on the Internet. Agent advertisements can be restricted in the network in terms of organisational boundaries rather than just via the TTL mechanism.

8.6 Location Awareness

The purpose of the positioning system is to help services function more intelligently; they should give applications and users the information needed of present location. There has been work on integrating various indoor and outdoor positioning methods (WLAN, Bluetooth or GPS). An instant messaging based software architecture for this purpose has been developed in the Gigamobile project. They originally used Bluetooth positioning, which was then combined with WLAN positioning that was developed in 6WINIT. In 6WINIT this architecture is being extended to outdoor use using GPS satellite positioning. The actual usage made of the technology during the 6WINIT project was limited – mainly because the development focused on positioning infrastructure – not the applications yet. However, its promise was shown by using location awareness in some applications.

The implementation of the WLAN positioning is a combination of pre-knowledge of a signal map that is used for the distance calculations and an extended Kalman-filter configuration for making the positioning results more accurate. The WLAN implementation of the system forms a static architecture, meaning that the base stations have to have fixed locations in the area and the signal map has to be based on these positions. This was combined with one based on use of Bluetooth.

They were able to locate objects with an average accuracy of 2 m within a region of 1000 m³. The reason that the base stations have to be fixed, is that the signal strengths must be calibrated to take account of walls and other obstacles that attenuate signals. This mechanism clearly has great promise inside a campus; Carnegie Mellon has deployed it within their whole campus with great effect – locating persons to this accuracy throughout the whole campus.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

The use of GPS is clearly complementary to the WLAN techniques. GPS operates well on a global scale. While the current consumer units operate only to an accuracy of about 30m, the WIDE project has shown that this accuracy can be improved to about 1m with differential GPS using terrestrial adjuncts. The forthcoming E112 emergency standard for 'Enhanced 112' emergency services requires location information to be made available (see the LOCUS/CGALIES IST projects <http://www.telematica.de/locus>). While this will be incorporated into the next generation of cellular technology, no such telephones were available during the 6WINIT project.

8.7 Public Key Infrastructures for Security

The Public Key Infrastructure (PKI) from the University of Murcia is one of the few PKIs, which is IPv6-enabled. It uses an LDAP directly to store certificates. . An attacker would not be able to modify the certificates or Certificate Revocation Lists (CRLs) held within the directory because these are digitally signed by the PKI. One of the features that have been added recently is the use of the Simple Authentication and Security Layer (SASL) between the directory and other PKI components. This strengthens the system, and makes it much more difficult to perform a denial of service attack by removing certificates/CRLs from the repository and preventing applications from authenticating their users. The authentication phase uses a negotiated SASL mechanism - this provides 'pluggable' support for different authentication systems. LDAPv3 servers providing password-based security must support the Digest-MD5 SASL mechanism and this was chosen as the default for interactions between the PKI and the directory. This provides protection against passive attacks but does not prevent active intermediary attacks, e.g. dictionary attacks. This was chosen in preference to more secure mechanisms in order to maintain the compatibility of the PKI with the majority of LDAPv3 servers.

This mechanism is used in some of the Health Informatics applications; in the future it will be integrated also with the Road Warrior application, to automate the certificate distribution further.

8.8 Quality of Service

Quality of Service (QoS) is recognised as being of vital concern in wireless access to the Internet. How it is implemented is less widely agreed. In the core routers of the Internet, various techniques such as Intserv, Diffserv and MPLS have been proposed and partially deployed. We do not regard the core Internet as being a subject of concern in 6WINIT. The performance of the access networks is important, but again is something with which we have had only limited concern in 6WINIT. There have been performance measurements of WLANs, GPRS and to some extent UMTS – but these have been mainly to understand the limitations of the access networks, not to perform much work on the provision of QoS in them. There has been some theoretical work on fast hand-off on moving nodes; this has been written up as publications, and entered into some of the IETF working groups.

However, we have considered it a vital part of the project to provide the optimum QoS we could through application or edge router activity. Thus both the 6WIND and Kame routers provide DiffServ on various classes of traffic. This allows applications to provide better classes of service to specific application classes.

Some of the applications themselves provide QoS support for classes of traffic. Thus RAT sends a normal talk spurt in one packet, and appends a lower quality encoding of that talk spurt appended to the data of the subsequent packet. This allows considerable improvement of voice comprehensibility in the presence of frequent losses of single packets.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

Use of RTP and RTCP reception packets give to source information on the loss of data of recipients. This can be used by the source to slow down the rate of transmission if the RTCP packets indicate an unacceptable error rate of media streams.

The TAG of Section 7.2.2 uses Active Network techniques to change the media adaptation in the gateways based on RTCP reports. At present, the mechanisms are limited; video is sharply curtailed if audio packets are lost; however the basic feedback could be used to provide a more sharply compressed coding if this was desired.

8.9 Active Networks

While in this project only one application, the TAG of Section 7.2.2, has been built using active networks, the mechanism is much more general – and has wide application to the components and services being considered in 6WINIT. Active Networks is a broad category of components; in 6WINIT we used only ones based on Application Level Active Networking (ALAN), and used the FunnelWeb implementation obtained from the ANDROID Project.

FunnelWeb provides an execution environment (EE) for Java-based active applications, known as proxylets. The FunnelWeb EE is termed the Execution Environment for Proxylets (EEP), which provides a Java environment with a Remote Method Invocation (RMI) control interface for loading, running, modifying operations and stopping proxylets. The proxylets are Java applications implementing the *Proxylet* base class, which exposes methods for initialising, starting, modifying operations, and stopping of the proxylet.

The FunnelWeb EEP component runs many types of networks; in 6WINIT examples are Routing, Service Discovery and media adaptation proxylets. A client can use the Routing and Discovery proxylets to identify its location in relation to other parts of the Active Network. A client communicates with the remote EEP via the RMI interface and queries the local Routing proxylet for information regarding the current EEPs available and the closest EEP in relation to the client. Once a connection has been established to an EEP, the client can start, stop and configure application proxylets. An EEP downloads the proxylets from a central web server, allowing them to be upgraded easily. Proxylets contain additional information for execution on a FunnelWeb EEP. The added metadata policy file limits control of the proxylet to a range of hosts. In the implementation developed under ANDROID, the proxylets are policy controlled using XML policies. In the 6WINIT use of FunnelWeb for the TAG, the proxylets run in an active server. It is also possible to have an active router; in this case the amount of code that one can afford to execute is very limited without incurring unacceptable overheads. It is normal just to have active packets use a different routing table. It is then possible to combine these techniques, and have the active packets route automatically to an active server.

The *active network* technology is potentially very useful in any environment involving edge activities; wireless networks are clearly targets for this. It is then possible to have active packets directed at an end device; because it is active, it can be re-directed to an *active server*, and the Edge processing done there.

8.10 Dynamic Service Discovery

8.10.1 Motivation

Dynamic service or (more generally) execution task deployment over an expanding network infrastructure can be very important for on-demand services. This is especially true in the mobile environment, where the executable task/service cannot provide service or quality guarantees from

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

statically configured onto fixed serving hosts. One reason is that topological mobility of IP hosts may induce a highly variable quality of service as a result of the change of IP link connectivity. Both the Agent Technology of Section 8.5 and the Active Network technology of Section 8.9 are examples of this capability.

The question of Service Discovery is recognised as of considerable importance, and a number of generalised algorithms for it are being standardised in the IETF. The IPv6 service discovery methods cited in 6NET D2.5.1 include ones based on: Use of IPv4 or IPv6 Anycast addresses, Link or site scope IPv6 Multicast (e.g. in Neighbour Discovery), well-known site local addresses, the Service Location Protocol [rfc2165], a well-known DNS name (e.g. isatap. as used in the current ISATAP Internet Draft), advertising services in Router Advertisement .piggyback. messages and use of DHCP(v6) and Linklocal Multicast Name Resolution (LLMNR), aka. MDNS. While there are many candidates, there is no clear favourite yet.

While we were waiting for a clear direction in the standards arena, we needed a suitable implementation in the project. We consider here a specific embodiment which is concise enough to be embedded in other services, and can complement the specific needs of the Active Service and Agent technologies – while capitalising on facilities provided in IPv6. We do not claim that it is optimal; it is merely the one that was developed in the project, and illustrates the requirements in such a service.

8.10.2 Architecture

These technologies follow a pull service model where a mobile host, having identified its service requirements, requests that the relevant software be downloaded from a code server; In some cases, it is necessary to discover which nodes are already running a specific service; in others it is important to be able to discover which nodes could run the relevant service (e.g. with the technology of Section 8, the location of a code server, or that of nodes which have the FunnelWeb loaded there. An important adjunct for these and related services is a module for service discovery.

In 6WINIT we defined, and partially implemented, a novel service discovery mechanism that relies on a synergistic approach between routers as well as server hosts to signal the location of specific resources. In the project we employed this service only to the identification of where FunnelWeb is running – but it could have much wider applicability. In view of the IPv6 availability in 6WINIT, we were able to take advantage of the IPv6 *anycast* feature for identification and distribution of discovered services among serving hosts and mobile nodes. The model described is more general than there was been time to implement in the 6WINIT project.

The service discovery model comprises of two tiers; **Tier I**, employs *anycast* to determine islands of network host entities supporting an identifiable set of capabilities that define a respective set of discoverable resources. In **Tier II**, the discovery mechanism is concerned with bridging these islands, through some efficient form of partial or fully meshed algorithm employing either explicit registration or alternatively, multicast if available.

The discovery mechanism assumes that only routers may configure an anycast address on their interface. In the Tier I phase of discovery, a mobile node inquires about one or more available network nodes supporting specific capabilities that are located (currently) within the visited domain; the mobile node performs the inquiry by means of sending a Service Discovery Solicitation (SD-Solicitation) to a well known anycast destination address. The closest topologically router, supporting service discovery at this anycast address responds to this message by means of a unicast Service Discovery Advertisement (SD-Advert). The SD-Advert message contains one or more discovered nodes that can handle a forthcoming service discovery request.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

On receipt of this message, the mobile node sends a Service Discovery Request to the discovered node provided by the SD-Advert message.

Network hosts that support service functions such as Active Services (AS) build a topology map of all AS hosts within the domain by indicating *discoverability* through a *discoverable node advertisement (DN-Advert)*, to a well known anycast address serving as a *discoverability registration point (DRP)*. Routers that are configured with the CRP anycast address and thus receive DN-Adverts, forming parts of AS topology. Routers supporting the DRP anycast address exchange random elements of their AS host addresses to obtain a connected view of the entire AS topology forwarded to advertising hosts.

In the Tier II, a topology map is first made of locations in the different islands, which serve as Tier I servers. A hierarchical topology map of the regions supporting the services is then compiled. Since we have implemented only Tier I, and there are many design choices, and potential pitfalls, in Tier II, we will consider only Tier I here.

8.10.3 Implementation

The mechanism of Tier I node discoverability is has been completed. The capability discovery mechanism has been implemented for a minimal set of capabilities. This implementation provides a proof of concept about how submission of capability requirements and selection of specific AS hosts can be provided.

8.10.4 Evaluation

The technique does provide a useful Service Discovery, without incurring unacceptable overheads. By prohibiting individual hosts from registering as *anycast servers*, we avoid introducing new host routes to routing tables. It achieves ease of deployment of service discovery without a need of explicit registration on directory servers or registry servers. This improves resilience in the event of a failure, and avoids hot spots in registration points – both inherent problems in Application-level anycast. It has the penalty that there is a requirement to support Anycast on routers attached to the Servers - but this is expected to be supported eventually in all IPv6 routers.

By means of anycast signalling between routers and subsequently push messaging to the discoverable nodes, the discovery model allows formation of an island of discovered node entities that subsequently overlay capability discovery at intra-domain level. Anycast messages may be digitally signed to ensure authenticity of the originating node while its availability for discovery may be time-bound by means of lifetime information. This allows for a node to effect availability for discovery and use of its capabilities for specific time periods.

Node discovery incurs lighter weight signalling than capability discovery; this is because node discovery messages are used only to proclaim or convey discoverability about a node, taking no account of capabilities of that node. On the contrary, capability discovery requires exchange of one or more attributes, which are inherently described by multiple data components; as such this incurs longer messages.

8.11 Summary

Summarising this section is particularly difficult. There were a variety of generic services, all of which are relevant to 6WINIT purposes. Security is an important area; the PKI deployed and the use of the Road Warrior are important technologies. Mobile IP is important both to ease the

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

addressing of mobile users, and to assist in simultaneous multi-access; in fact for the latter multi-homing is also desirable – but that has not yet been standardised or implemented. Multicast is an essential technology for wide deployment of many applications; it has only not taken off sooner in the IPv4 world because there was no large-scale stable deployment, and the ISPs have not really understood how to charge for it. Location Awareness is considered one of the key facilities, which will lead to value-added services in UMTS; it was not used heavily in 6WINIT only because the UMTS was not available, and the need for it on LANs is less universal. Both Agent technologies and Active Networks will have an important role in future Value Added Services; the implementations described here show how they can be used in earnest. For a widely distributed deployment of either technology, the Dynamic Service Discovery is clearly important; here again, only very limited use of it has been made in 6WINIT, but this is sure to change in future projects.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

9 TRANSITION TECHNIQUES (D9, D17)

9.1 Introduction

Deliverable D9 (“Early Aids to Deployment”) presented an overview of general IPv6 transition mechanisms, and those that were planned for use within the 6WINIT project at the end of the first year. While this was a useful snapshot, by no means all of these were developed further inside the project. In D17 (Advanced Aids to Deployment) we concentrated on the tools and techniques actually developed by project partners and how they were deployed as part of the project, and at public technology demonstrators of the project.

The ones we actually used, and the section in which they are considered, is listed below:

- IETF Activities (9.2)
- The IPv6 Operations Working Group and 6WINIT Mechanisms (9.3)
- Tunnelling mechanisms (9.4)
- Translation mechanisms (9.5)
- Application Level Gateways (9.6)

9.2 IETF Activities

The ngtrans working group of the IETF has made the INTERACTION draft (draft-krampell-v6transition-interaction-01.txt) a current work item. This document discusses interaction of transition mechanisms that can be involved during the transition phase where both IPv4 and IPv6 will be concurrently used. On one hand, several transition mechanisms have been defined to solve different transition issues. On the other hand, one can face multiple transition issues and may have to use several transition mechanisms at the same time.

Since an applicability scope is attached to each transition mechanism, specifying where the mechanism applies, i.e. host, domain or global, this memo aims at identifying cases where multiple transition mechanisms may be involved within the same scope, and what can be the interaction effects between them. As more and more transition mechanisms are deployed in the different local networks, the likelihood increases that a packet undergoes more than one transition on its way from source to destination. This may lead to unexpected effects and in the worst-case make it unable for the network connection to become established. This work will guide the administrator of a network domain to choose the appropriate transition mechanism and pinpoint the possible side effects.

While 6WINIT partners have contributed to several of the IETF drafts in this area, It seems unnecessary to say more about the IETF activities than to stress both that this item is receiving attention, and that the INTERACTION draft is aiming to provide just the sort of overview which would otherwise be appropriate here. We mention only one other activity, the IPv6 Operations Group.

9.3 The IPv6 Operations Working Group and 6WINIT Mechanisms

This new group was launched in the summer of 2002. The rationale for the new group was that IPv6 is now ready for deployment; it is thus imperative that deployment scenarios are clearly defined in the light of experience to date, and all existing mechanisms be tested for applicability against those scenarios. At present, only a small subset of methods has been accepted into the

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

v6ops charter, but this set will expand as the analysis continues. The goal is to focus deployment on a small well-understood set of tools.

The methods adopted by v6ops to date are: Transition Mechanisms (RFC 2893), SIIT (RFC 2765), NAT-PT (RFC 2766) and 6to4 (RFC 3056 & 3068). In addition to these, the 6WINIT partners have been using: ISATAP (Internet Draft) and the Tunnel Broker (RFC 3053). ETRI developed also a "Bump-in-the-Application" (BIA, RFC 3338) but this has not been used in the project.

We expect that the tunnel broker tool will continue to be used, and be quite popular for connecting either dual-stack hosts (most commonly) or isolated IPv6 networks over IPv4 networks. In Deliverable 9, a tunnel broker built by UoS was described (using Apache, ssh and OpenLDAP all running over IPv6), and is still in use. Another Tunnel broker solution from Ericsson Research ("Pulkkinen") would have been used in IST 2001 had we got GPRS access for that demonstration; this implementation does allow for dynamic address allocation, as does ISATAP, but this functionality was available late in the project, only. The importance of the dynamic address allocation, is this is the functionality often used in current GPRS provisions.

ISATAP is likely to continue to be used, despite its current Internet Draft status in the IETF, and its (to date) lack of adoption by v6ops – where it is only being proposed as an Experimental Standard. Implementations of ISATAP include those in Windows XP, Linux and FreeBSD (client), and Cisco IOS, FreeBSD, Ericsson's RXI 820 Realtime Router (router side support) and 6WIND's router. ETRI has provided much the same tool in their IPv6 Transition Toolbox.

6WIND has implemented DSTM (currently at Internet-Draft status), but this has not been used extensively in the project: its scenario is an IPv6-only network running dual-stack hosts wishing to access external IPv4 and IPv6 services; the IPv4 services are accessed by tunnelling through the local IPv6 network to an edge device that decapsulates the tunnel and forwards data to the target host. DSTM could be useful when IPv6-only network infrastructure is deployed, which may be in the near future in some cases (e.g. in Wireless LANs).

Application Layer Gateways (ALGs) are a non-IETF item, but worthy of mention. The TZI SIP proxy of Section 7.2.1 can handle IPv4 and IPv6 connectivity, as does UCL's TAG of Section 7.2.2 and UoS' Slite agent framework of Section 9.6 (through dual-stack support in Java). Other common ALGs include web proxies, FTP proxies, and dual-stack SMTP servers.

9.4 Tunnelling Mechanisms

Tunnels are the simpler way to make two networks communicate over a network that uses a different protocol. There are three standard tunnelling mechanisms: Configured IPv6 in IPv4 tunnels, Configured IPv4 in IPv6 tunnels, and 6to4. In this context, the 6WINDGate supports all three; the 6WINDGates are gateways that act as tunnel endpoints. The Ericsson AXI 462 supports configured IPv6 in IPv4 and the Ericsson RXI 820 supports configured IPv6 in IPv4 and 6to4.

The configured tunnels require that the endpoint addresses be explicitly configured; though a tunnel broker can help in this task; one such tunnel broker was developed by UoS in 6WINIT, and has been deployed. In order to avoid the manual set-up, the "6to4" method (RFC3056) allows the endpoint gateway to automatically build an IPv6 address based on the 2002:: prefix and the IPv4 address of the external router of the IPv6 site. The result is 2002:IPv4:ADDR::/48. A router knows that it needs to tunnel to a known IPv4 endpoint when it sees a prefix of 2002::/16 for a destination. 6to4 is typically used when two IPv6 network islands are separated by an IPv4 network. The advantage is the simple configuration. The drawback is that the routing possibility

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

of the 2002:: prefix is limited, because it is specific to other hosts running 6to4, unless a 6to4 relay is made available to reach the “normal” IPv6 address space.

Another way of tunnelling is to tunnel natively by using the Dual Stack Transition Mechanism (DSTM); while this has been implemented by the 6WINDGate, it is not yet a standard. It works well, but at this stage probably suffers from interoperability problems between different suppliers.

9.5 Translation Mechanisms

NAT-PT provides a migration system based upon protocol translation of packets. NAT-PT is specified in RFC 2766. With NAT-PT, outgoing IPv6 packets are translated into IPv4 packets. The 6WIND implementation of NAT-PT allows use of either static or dynamic mode and provides a bi-directional NAT-PT functionality including DNS and FTP Application Layer Gateways (ALGs) as described in RFC 2766. In static mode, translation rules can be set up on address and/or port. In this case, the translation is bi-directional. In dynamic mode, only the connections coming from the IPv6 host can be established. As NAT-PT uses the same public address for translating the source address, it may be necessary to translate also the source port in order to distinguish different sessions.

ETRI has provided much the same tool in their IPv6 Transition Toolbox, but the Ericsson activity was discontinued.

9.6 Application Level Gateways

9.6.1 Real-time Media Applications

In the Internet multimedia conferencing architecture, multimedia conferences consist of different data streams that are required to successfully establish communication channels between endpoints. Real-time multimedia communication, consisting of one or multiple media streams (audio, video or other media types) that are used to carry the real-time media data, is only one element in a multimedia conference. Another element is conference control communication. Conference control is used to co-ordinate a common state at all endpoints that is suitable for conducting the conference. For example, before a conference can start, all endpoints need to be configured appropriately with respect to media codecs and transport parameters.

Multimedia conference sessions are usually described using Session Description Protocol (SDP). A number of ways of distributing SDP are used in 6WINIT: SIP (Session Initiation Protocol, RFC 3261), SAP (the Session Announcement Protocol) and the Secure Conference Store. The call signalling components of the ITU-T/H.323 series of recommendations use their own methods for session description and set-up. However, all these are roughly equivalent in their call control features.

For multimedia real-time applications (audio/video conferencing), all the above are used in conjunction with the Real-time Transport Protocol (RTP, RFC 1889). RTP is usually used with UDP/IP and provides the service of transmitting real-time data efficiently, maintaining the time relationships between individual packets. For establishing a conference between two participants, e.g. a voice call, the two endpoints must negotiate proper media types, codecs and transport addresses for the RTP sessions, i.e. IP addresses and UDP port numbers.

Adapting conferencing applications from IPv4 to IPv6 is more or less straightforward: Applications must be extended to deal with IPv6 addresses, to use the corresponding system services for DNS lookups, and to represent IPv6 in conference set-up messages, e.g., in SDP

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

content for SIP and SAP requests (and responses). However, for using these applications in mixed IPv4/IPv6 environments, e.g., for calling an IPv6-SIP-phone from an IPv4-SIP-phone, it is not sufficient to deploy the translation mechanisms described in Section 9.5.

Translation mechanisms like NAT-PT that work on the network layer are insufficient because they can only translate the IP-header information and cannot provide the necessary adaptations for the application layer communication. Therefore, NAT-PT systems are often combined with application layer gateways for supporting IPv4/IPv6 interworking for multimedia conferencing applications. For the RTP streams themselves, the basic NAT-PT functionality is sufficient for providing IPv4/IPv6 interworking. For the call and configuration signalling, more is required.

9.6.2 The TZI Gateway

The TZI-Gateway can be set it up as a SIP gateway or as an H.323 gateway in IPv4 and IPv6 networks. In both variants it relies on a media processing engine that performs RTP translating, transcoding and forwarding. It contains all the features needed both to initiate calls in both IPv4 and IPv6, and to maintain sessions in both features. It contains other features also, but these are considered elsewhere in this report. It has been tested also with other audio tools the Vocal and BonePhone agents.

The system has been shown to work well in the interworking environment.

9.6.3 The Mbone Conferencing Application

The Mbone conferencing components have been set up to work in either the IPv4 or IPv6 environments. Thus the conferencing components (VIC, RAT and NTE) and the call signalling (SIP, SAP and SPAR) work in both environments. In a mixed environment it would be straightforward to set up the conferences by announcing them with any of the mechanisms in both forms, and arranging for the two forms to communicate via a NAT-PT gateway. This has not been implemented in the 6WINIT project, because none of the application scenarios required it.

In a mixed environment, it would be particularly easy to organise this with the TZI gateway, initiating the calls with SIP in only one form. If it were initiated with both IPv4 and IPv6, a much less functional gateway would be adequate.

9.6.4 The Slite Agent Framework

The Slite framework consists of a number of agent platforms. A platform is an instance of the Java Virtual Machine (JVM), and hosts a number of agents. Each platform has a special agent, an *agent launcher*, which oversees the launching of agents and registration into their capabilities to the platform. The Slite framework has been implemented in Java 1.4 and works in both the IPv4 and IPv6 environments utilising the Sun IPv6-enabled *java.net* package. This system has been tested to run on the Red Hat Linux 7.1-7.3 operating systems. Slite can bridge between the two network protocols, by virtue of the *java.net* package being able to talk both protocols.

9.6.5 The ULTIMA Gateway

Ultima is a BText Technologies IP product that provides interworking between IPv4 and IPv6. Ultima utilises [NAT-PT](#)¹ technology to enable IPv4 to IPv6 interworking to be achieved, without

¹ <http://www.ietf.org/rfc/rfc2766.txt>

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

any modifications to either the IPv4 or the IPv6 host protocol stacks. Ultima allows bi-directional IPv4 to IPv6 translation and exceeds the functionality specified in IETF RFC 2766. DNS Application Level Gateway (ALG) handles translation between A and AAAA records for both UDP and TCP. The DNS ALG supports DNS message relaying, File Transfer Protocol (FTP) ALG, Session Initiation Protocol (SIP) ALG, Automatic IPv6 address advertisement via RIPng and Router Advertisement, Efficient IPv4 address management. It supports NAPT-PT, allowing further IPv4 address conservation, it has a simple installation process, Web-based remote monitoring and configuration process.

This product was not developed under the 6WINIT project, but has been made available to it. While BT is not developing it further as a commercial product, it is typical of the better type of gateways, which are designed specifically as an aid to deployment. It can be used, therefore, by all the applications, which need such gateways – for example the conferencing application mentioned already in Section 9.6.1.

9.6.6 Summary

While several Application Level gateways (ALGs) were developed in the 6WINIT project, they were not used heavily. Generally this is because 6WINIT ran IPv6 applications that did not need to talk to v4 services. The main two methods actually used were v6 in v4 tunnels and ALGs, with a little dash of translation (NAT-PT). The Ericsson UMTS testbed uses ISATAP, for example. In the future deployment work, we do expect to also require ALGs with their special functionality.

9.7 Conclusions

With the huge deployment of IPv4 technology, it is clear that facilities for IPv6/IPv4 transition are of fundamental importance. This has been recognised in the IETF, and a new urgency has resulted in a new working party being formed to look at this issue. The fundamental services of tunnelling and translation mechanisms are the basic mechanisms that must be used; both the Ericsson and the 6WIND routers have implemented these technologies to some extent. While Application Level Gateways are possible points of failure, they are very important tools in the transition armoury. The TZI Gateway, The Slite Framework and the ULTIMA gateway have specific functionality – which are actually quite separate. The first two transition between different application spaces as well as the IPv4/IPv6 transition. Mbone conferencing has transition aids in that it can be accessed from both worlds; for simultaneous collaboration, one of the other gateways must be used as well.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

10 GENERIC APPLICATIONS (D16)

10.1 Weather Station

The weather station is a device containing a variety of sensors (i.e. temperature, wind speed and direction, humidity, air pressure and precipitation) and needed computing and communication capabilities. It has no strict mobility requirements, but it must be possible to install the station without a need for massive wiring and also to move the station from one place to another easily. Communication security (authenticity of the weather data) needs to be ensured at least when the data is used for professional purposes like weather forecasts.

Wireless access and manufacturing costs set requirements for the hardware that can be installed on the weather station – normal PCs are overkill in this environment due to their large size and power consumption. There are lots of embedded devices available, which provide enough computing power at lower cost, but the IPv6 support in these devices is often non-existent.

VTT utilised a micro-controller running under a micro-UNIX. This was IPv6 enabled by upgrading the operating system and adding IPv6 support to system libraries and web server software. A statistics server was developed in Java and deployed on a separate high-end machine, which ran happily with IPv6 under JDK 1.4.

Many of the required components already had IPv6 support, though there are still missing pieces on Linux and uClinux: The problems identified do not prevent IPv6 deployment, but make it more difficult. Also dual-stack functionality on all devices is still required. Providing solutions to all these problems is not possible in the scope of 6WINIT, but luckily there are open-source activities in some of the areas (e.g. IPv6 support in databases).

The data transfer requirements are low; this is an ideal application for using GPRS.

10.2 Agent Frameworks

The Southampton SoFAR group developed the generic agent framework described in Section 8.5, and then applied it to several specific applications. Three applications were developed: MIDI data routing, RTP-based video stream routing and intrusion management.

All the demonstrators employ a subscription model of brokering their respective streams. The MIDI demonstrator has been successfully installed into their meeting room space, where MIDI is used for industry-standard automation of devices in the meeting room. The MIDI demonstrator allows for subscription to various MIDI events, e.g. fader settings and configuration of audio routes through a digital mixing deck (Yamaha O1V). The RTP relay demonstrator provides routing capability for RTP data streams, such as those used by the VIC tool, as a result of agent negotiation. The intrusion management demonstrator provides an argumentation scenario where agents, on behalf of external entities, can negotiate access to devices within a home environment rich with networked pervasive devices. Currently these applications have been used only with WLAN.

The use of IPv6 within the Slite Agent Framework offers us a number of advantages. The vastly increased address space makes it feasible for pervasive devices within home environments to have global Internet addresses. Pervasive devices that implement their own end-to-end security model (e.g. IPsec) are becoming feasible in this setting. The scoped multicast offered by IPv6 allows us

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

some control over how far agent capabilities are advertised on the Internet. Agent advertisements can be restricted in the network in terms of organisational boundaries rather than just via the TTL mechanism.

10.3 Location Aware Applications

Many applications can be envisaged which use the location-aware technology of Section 8.6. VTT has chosen to develop one in which a web-based client tracking system shows the client's position within the area. The Mobile Location Protocol (MLP), an XML based presentation language, is used to present the location information. The client acquires the X/Y co-ordinate pair in the WLAN case, and the room number in the Bluetooth case. In both positioning technology cases (more generically in all positioning technology cases) the location information is stored in a PLIM (Presence and Location Instant Messaging) server. In both cases the client parses the information from an MLP presentation and an avatar representing the user's location is drawn accordingly over the floor plan of the building.

The WLAN positioning has some limitations, which need to be taken into account when the network is built. The access points are supposed to use full power for transmission. This means that power management may not be used. The reason for that is that when the signal map is once created with certain level of signal strength the use of the system requires that the access points still use the same power – thus the collected signal map is up to date and does not change in the use. Also the access points are recommended to use external antenna for giving more stable signal strength values during the calibration and further use of the system.

The coverage of three WLAN base stations, as in the basic configuration, reaches up to 1000 m³ of office area with an average accuracy of ~2 metres. The parameters of the algorithm have to be fixed for the specific environment because the attenuation of signal depends on different obstacles and materials located in the area. In the office surroundings the walls have to be taken into account but in the open space like in exhibition halls etc. the parameters have to be changed to be less restrictive

While this application is apparently simple, it has important ramifications. When the two technologies chosen are an indoor one like WLAN, and a WAN one like UMTS or GPS, then a truly seamless map of in-door and out-of-door location of object can be presented.

10.4 Home Environment Applications

This application is based on an existing home-environment demonstration, which has been developed in VTT's Interactive Intelligent Electronics (IIE) programme. The application allows wireless access to controllable devices such as TV, heating and lighting via a variety of control methods, which include speech recognition, normal browsers and gestures. The system is based on OSGi (Open Services Gateway initiative) architecture and it uses UIML (User Interface Markup Language) to provide an appliance independent description of the user interface.

In 6WINIT, the home environment has been extended with secure remote access. Remote user can see real-time video from home and control the appliances remotely. This is also useful for safety purposes, for example if a burglar alarm triggers, user can check the reason for the alarm remotely.

The home environment system can be divided into three parts: home server, control devices and controllable devices. The system was IPv6-enabled in the 6WINIT project. The biggest change was migration to Linux machines from previously used Windows, which did not support Java with IPv6.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

Controllable devices include TV and Video through an infrared link, lighting through an X10 system and heating through a LON network. Control devices include a PDA with WLAN connection and a laptop with WLAN or LAN connection, speech control and remote access. Currently TV, video and lighting are controlled from the Linux-server. LON control interface (heating) is not supported on Linux, as the drivers are not available there.

The home server is based on an Open Services Gateway initiative (OSGi) architecture, which delivers an open, common architecture to develop, deploy and manage services in a co-ordinated fashion. In the OSGi environment applications are delivered as bundles, which comprise Java classes and other resources, which together can provide functions to end-users and provide components to other bundles, called *services*.

From the user interface point of view, the system is based on UIML-technology, which supports Java, HTML and Voice XML clients. In the system, every device has its own device driver that provides a description of its user interface using UIML. The UI broker then adapts this description to the desired client format (i.e. to HTML, VoiceXML or Java client).

The home environment itself has been implemented entirely in Java, using a Linux PC as server. The OSGi implementation used the freely available IBM Service Management Framework (SMF). In principal, running the system in Java 2 version 1.4 was enough to make the system IPv6 enabled. However, older SMF versions treated IPv6 addresses wrongly, which caused problems with browsers other than Mozilla.

For the remote demonstrations, a real-time video service was implemented in the OSGi environment. It uses Java Media Framework (JMF 2.1.1) for video capture and transmission over RTP. On the client side, both JMF based client and VIC can be used for video display. JMF proved to be quite immature especially in relation to IPv6, but finally the many problems were worked out and the instructions were posted to the jmf-interest mailing list in order to help others with similar problems.

Currently, the home server is running following services:

- "Home theatre" for controlling TV and VCR using infrared access
- "X10" for controlling electrical devices (e.g. lighting)
- "Video service" which delivers video from the web camera

Both Home theatre and X10 devices require an external device connected to the home server using serial connection. On Linux, this requires a RXTX-library together with Sun's CommAPI interface. The RXTX -library can be downloaded from <http://www.rxtx.org/>.

Remote access to the home environment is secured with IABG's Road Warrior IPsec-implementation of Section 8.1. However, there were some problems either with Redhat 7.1 or the hardware we were using that caused some data corruption.

The current state of the implementation is working well and is easy to use. The LON communication is currently made through a Windows-server and it would be interesting to have it working also via a Linux-server but this was not possible during the 6WINIT project.

In the future it would be interesting to combine the home environment with other applications and technologies. For example, the home environment application combined with location awareness of Section 8.6 enables a lot of new services.

Home environment has been demonstrated in INET 2002, IST 2002 and MUM 2002 - conferences. The demonstrations were based on fixed networks providing native IPv6 connections in IST 2002 and MUM 2002 conferences and a tunnelled connection in INET 2002.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

Home environment has also been demonstrated over wireless HSCSD connection, but the bandwidth was not quite sufficient for the video transmission there. HSCSD was used, since the GPRS networks in Finland do not allow setting up IPv6 connections due to the NATs and firewalls.

10.5 Streaming Applications

Video streaming applications have been provided by ETRI and BT; these have been introduced into the project, but were developed mainly outside. The ETRI and BT (VideoLan) systems use both RTP/UDP and HTTP/TCP based streaming - while the BT one supports also UDP multicast. Both support IPv4 and IPv6, MPEG 1 and MPEG 2; ETRI also supports MPEG-4. The ETRI system is server based; the BT one supports also satellite and DVD input. Both support Windows and Linux clients.

The ETRI IPv6 streaming system consists of the streaming server, the monitor & contents manager and contents server. The web-based contents server provides information about the clips. Based on this information, the clients can request the clips from the streaming server. They can also do network monitoring and content management. BT has provided a video channel functionality, which allows a user to switch between different movie or multicast streams by pushing a button.

The IPv6-based streaming applications both work well though the buffering should be improved for worst network conditions. The MPEG-2 version requires between 5.6 and 10.4 Mbit/s; this is too much bandwidth for the 6Bone and for a 10 Mbit/s Ethernet, but is fine on the 6NET network and a 100 Mbit/s fast Ethernet. It is just on the borderline for WLANs using 802.11b – providing there is no other traffic on the network. The MPEG-1 variant uses about 2 Mbit/s, and works well over WLAN.

10.6 Conferencing Applications

10.6.1 Architecture

There are primarily two forms of Internet-based multimedia conferencing: those based on the Internet Multimedia Conferencing Architecture, and those based on the ITU-T/H.323 series of recommendations. In fact the H.323-based conferencing is more widespread in commercial systems. However little work has been done with this in 6WINIT, except for the gateway work of TZI of Section 7.2.1. One reason for the lack of interest in H.323 inside the 6WINIT project is the increasing importance and availability of SIP-based solutions. Since H.323 was not seriously used in the 6WINIT project, it will not be discussed further here.

10.6.2 The Internet Multimedia Conferencing Architecture

The Internet Multimedia Conferencing architecture distinguishes between continuous media transport, shared workspace transport and Conference/Call initiation transport. Continuous media transport is done via the Real Time Protocol (RTP), with optional acknowledgement Real Time Control (RTCP) acknowledgements; this does not provide reliable transport, but signals packet loss and so can be used for QoS management. Shared workspace uses a reliable transport mechanism. The underlying network level protocol can be either Unicast or Multicast; multi-way communication often uses multicast. As an aid to transition, where it is not available, a Multicast-Unicast reflector can be used at strategic places. Reliable multicast is still a research issue, but several shared workspace tools have developed their own versions. Security on the data streams

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

is provided either by application-level encryption, or by a special form of RTP called Secure RTP (SRTP).

Conference/call initiation can be done in several ways. Fundamentally there is a Session Description Protocol (SDP), which defines the parameters of a session; for encrypted sessions, this includes the parameters for the encryption.

There is usually a User Agent, which configures the local end-station automatically on receiving an SDP unit. This SDP entity for a specific session can be sent over the Internet in many ways: stored in a Server, sent by the Session Announcement Protocol (SAP) as a multicast announcement on a specific address, or sent as an invitation to join a conference to a specific IP address or even person using SIP. The choice of transmission mechanism for the SDP unit impacts the security mechanisms that must be used; all have been used in 6WINIT – though SRTP has not yet been implemented.

There are media engines for voice and audio; the audio and video coding used have a choice of specific pre-defined identifiers. The media engines for each media usually recognise a range of codings.

In the 6WINIT context, there is often a requirement to be able to change the bandwidth used by specific media streams. In a two-person conversation, it may be possible to negotiate bandwidth down to a value that ensures no loss. In a multi-way conversation, where only some of the participants are on a wireless link, it may be necessary to adapt the bandwidth of specific streams. This is usually done at a gateway near the wireless portion; it may be by transcoding, or by reducing the bandwidth given to a less urgent medium (e.g. discarding some or all video frames).

10.6.3 Implementations

In 6WINIT, the most commonly used audio engine is RAT, developed by UCL. This includes facilities for many coding schemes, and also for redundancy in the case of loss of single packets. It operates over both IPv4 and IPv6, and over both Unicast and Multicast. ETRI has developed a higher quality variant of RAT that includes an MPEG audio codec. RAT allows application-level encryption.

The most common video engine is VIC; this was originally developed at the University of California, but has been extensively modified by UCL. Again, it operates over both IPv4 and IPv6, and over both Unicast and Multicast. It allows for layered coding, which can be utilised in the bandwidth reduction mentioned in Section 10.6.2. VIC allows application-level encryption.

ETRI has developed a High Quality Video Conferencing Tool (HVCT), which uses HAT, MPEG-4 Video. The system can show the traffic monitoring data per participant basis and has an Adaptive Bandwidth Control (Frame Rate control) based on the network status.

UCL has developed also a Network Text Editor (NTE), which is a shared text editor for use with multicast. It has also developed another tool (WBD), based on the Berkeley tool, WB.

From the RTCP reports, it is possible to derive a picture of the quality of a conference. UCL has developed a further tool, the RTP Quality Matrix (RQM).

Finally, to provide the information on the session parameters, UCL has developed three mechanisms. SDR allows the regular announcement of the sessions using SAP; they can be stored in a Secure Conference Store (SCS); or they can be used as an invitation to join the session via SIP. Secure SAP has not been standardised due to concerns over wasting public bandwidth for private sessions. SIP provides mechanisms to secure session invitations, though these

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

methods have not been implemented in the tool tested. The SCS uses an Apache web store with the normal HTTP-S access constraints, to limit who may view the session descriptions.

To allow for the media adaptation, UCL has developed the Transcoding Active Gateway of Section 7.2.2. This has several important properties for the wireless environment. It can provide Unicast-Multicast conversion – which is a transition aid. It allows selective bandwidth limiting, policy controlled – though only crude discard of specific types of frame are implemented so far. It also allows dynamic loading by active network techniques – using the FunnelWeb infrastructure of Section 8.9 and the service discovery mechanisms of Section 8.10.

All the tools mentioned here are able to run over both IPv4 and IPv6 stacks for all the platforms on which they run.

10.6.4 Evaluation

The tools have been tested in variety of environments, on WLAN networks and over GPRS links. The systems operate in a straightforward manner over 802.11b networks – i.e. low latency and good throughput observed. However with GPRS links the bandwidth is significantly limited (20 Kbit/s upstream, 30 Kbit/s downstream, with a 3+2 device); additionally the latency is of the order of a second. Thus only very low frame rate video and low bit rate audio are possible.

The VIC, RAT and WBD tools work on a variety of platforms: FreeBSD, Linux, Windows and Solaris. HVCT runs only with Windows. They also have been shown to operate also on iPAQ PDAs. However they are not implemented in pure Java, hence some maintenance will still be required as operating systems change.

The application security used in the tools is quite satisfactory; nevertheless, it would be desirable to integrate SRTP in favour of the basic application-level security. It would not be good to use IPSec, since this would prevent use of edge devices like the TAG. With the current mechanisms, selective dropping of secured media packets is possible, though transcoding is not, without the gateway knowing the decryption key.

The secure announcements can currently be done only via SCS. Neither the SIP nor the SAP portions of SDR can announce sessions securely; the code for this was not completed, since the relevant proposed standard was not ratified by the IETF. There are now standards for secure SIP, but these have not been implemented in SDR.

In fact the version of SIP in SDR is an early version; we have not checked whether it is compatible with the SIP used in the VoIP of Section 10.7. It would be desirable to ensure such compatibility; it would be quite feasible for any of the VoIP implementations to join Mbone conferences, implementing only the audio part of the conference.

While all the tools are capable of dual-stack operation, there is no transitioning tool in the set described in this section. It is quite possible to use the TAG for application level dual-stack interoperation. However it would be possible to use the TZI gateway for this purpose; it is fully compatible with the Mbone tools.

The dynamic loading and service discovery components of the TAG have been tested and work; extensive more experience with this tool is needed to really evaluate these portions of its capability. The bandwidth limiting capability of the TAG is based on RTCP reports, and thus can adjust to network conditions. However it has also had little field usage; more experience is required to ascertain the most useful way to limit bandwidth. The service discovery currently works only over a limited space; inter-domain service discovery has not been implemented.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

Some development possibilities:

- RAT: Further work is required on transcoding and support for interleaved formats.
- HAT: Further work is required on improving the user interfaces and error correction features for more stable operation.
- VIC: Further work is required on use of direct video display and integration of more codecs
- TAG needs more sophisticated facilities for bandwidth limitation, dynamic loading and security.

10.7 Voice over IP

6Voice from Telscom is the only Voice over IP application developed under 6WINIT, though several others were used. Bonephone and VOCAL are two other packages, which have been upgraded to IPv6 capability. All of them use voice/RTP/UDP as a transport medium for the voice data. All the calls are initiated by SIP. Telscom has provided an IPv6-enabled version of SIP; again another version is available from Vocal, where UoS has ported the code to IPv6, and TZI (see Section 7.2.1). All three have been shown to interwork.

Telscom has tested 6Voice also over MIPv6 with satisfactory results.

This application has proved very useful in demonstrating some of the other components of 6WINIT – and is likely to be a very important one in the future. Operation of VoIP over WLANs and the Internet has been very successful. Experiments over GPRS have been poor for three reasons: the latency can be very variable – up to several seconds, the bandwidth requirements can be too high – some voice coders use up to 64 Kbit/s, whereas some of the GPRS uplinks are limited to 9.6 Kbit/s. With suitable codecs, GPRS is adequate under some conditions – though using it would incur a prohibitive cost in most countries.

10.8 Other Applications

Many other IPv6-enabled applications are used in 6WINIT. These include the following: Internet Explorer, Netscape, Konqueror, Network games, Quake, the XMMS audio and video player, and the MMCR multimedia recorder. Since these are either normal service utilities, or have been used only in isolated instances, no further evaluation will be done here.

10.9 Conclusions

A quite extensive set of applications has been introduced into the 6WINIT project; most of these were developed outside the project, but were modified for integration into the project. Moreover, in many cases they make use of generic tools; these in turn have been separated out from the applications, so that a much richer set of applications can be derived in the future based on the current set. Examples are the powerful extensions that can be envisaged for VoIP, multimedia conferencing and media streaming applications thanks to the availability of active gateways, agent technology and location awareness. Clearly we have only scratched the surface of what can be achieved in the home environment.

It is unfortunate that we have not been able to test many of these applications with a real UMTS. However the partners do plan to carry them over into future projects – like 6NET and Euro6IX and others to be proposed under Framework 6. Thus it is certain that the groundwork laid here will be continued.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

11 THE CLINICAL APPLICATIONS (D3, D14, D19)

This section considers the work of three collaborating, complementary, but quite different instantiations of clinical applications using IPv6 wireless techniques over the Internet. In each case, a real clinical organisation controlled the work, but needed assistance from academic departments with the requisite technical expertise. The first considered access to clinical records in the UK, the second a number of different scenarios including complex equipment in Poland, the third remote emergency treatment in Germany. We consider each of the three in the following sections, and then draw some conclusions.

Much of the material here is extracted directly from D19 in much greater details than in the other sections of this report. We do not apologise for this; D19 was supposed to be a description and discussion of the achievements of the clinical testbeds; hence much of the material is directly relevant.

11.1 Access to Clinical Records

11.1.1 Overview

The London 6WINIT Clinical Demonstrator comprises a set of primary and secondary care sites in north London working in partnership with University College London (CHIME). The long term vision for this demonstrator site involves the following healthcare settings: the Department of Cardiovascular Medicine at the Whittington hospital, 2-4 community-based cardiology clinics, several GP practices in north London, several community pharmacies in north London, patients managing aspects of their own healthcare at home

Because of the complexity of providing external access to information services and applications from inside the Whittington Intranet (or indeed any other *NHSnet* site) CHIME effectively “cloned” the Whittington EHR server within the University network at CHIME. This 6WINIT Electronic Health Record (EHR) server contains an identical suite of clinical applications and services to the live clinical server, but uses anonymised or pseudonymised patient data. This demonstration server is sited on a localised IPv6 network within CHIME and tunnelled over IPv4 to the IPv6 network at the Computer Science Department of UCL, and from there to other IPv6 network nodes including wireless services. This has enabled IPv6 solutions to be tested more easily by the 6WINIT partners, and provided project participants with demonstrator access to the web server applications. However, NHS legal constraints would prevent such an approach scaling up to a live or large-scale demonstrator, and alternatives including an *NHSnet* hosted solution should be investigated for the longer term. The NHS does not now normally permit mainstream NHS data to reside outside the *NHSnet*.

The clinical application and middleware components have also been deployed in the live setting, and the demonstrator site parties still intend to establish a full live 6WINIT IPv6 deployment (including wireless access) in the future.

Because of their interest in deploying the full 6WINIT infrastructure in earnest, they have been very concerned with different access networks, security and transition strategies. Each is considered below.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

11.1.2 Access Networks

Access to the UCL-CHIME databases has been effected via UCL-CS. This has allowed access to be obtained via WLAN, GPRS (at BT Adastral Park), UMTS (at Stockholm during Final Review), and all the other IPv6-enabled networks to which UCL-CS has access. The GPRS access has been both with PDAs and Laptops.

11.1.3 Security Infrastructure

Because of their desire to make real use of the technology, they have been very concerned to experiment with as much security technology as possible. Initially their servers could be accessed by name and password; the different names have different privileges. For added security, they have adopted the PKI of Section 8.7 and the Road Warrior of Section 8.1. They were one of the few groups who even wished to use the attribute certificates in the PKI, since the different classes of health workers have different access rights.

All access to UCL-CHIME has been via a 6WIND router there; in addition to its other functions, it has provided an IPv6-enabled firewall.

11.1.4 Transition Strategies

IPv6 transition mechanisms have been an important component of this demonstrator, since each scenario of usage needs at a minimum to utilise one IPv6/IPv4 tunnel for the UCL Intranet. The hospital staff working in the Whittington will require translation to enable IPv4 “legacy” access from existing their devices and networks.

The infrastructure deployed at CHIME mirrors that which would be required at a healthcare site that has no direct connection to a native IPv6 network. This will be the situation in many healthcare sites for some time to come. Hence there has been need to install IPv6-IPv4 translation, IPv4/IPv6 dual stack routers, and IPv6/IPv4 tunnelling.

Numerous successful *ad hoc* test connections have been made over the whole second year of the project, for which it has been continuously live. The Linux server running Tomcat and the clinical application Java servlets, connecting to other application services within CHIME via Jini, has also served as a development workstation and the target of several concurrent IPv4 demonstrations without problem. Our conclusion is that the 6WIND device has been able to support IPv6 access without adversely affecting legacy access to the same web applications running on the same server (in fact, sometimes simultaneously viewing the same web pages).

Clearly the 6WIND device could also be deployed in situations where an enterprise does have a direct IPv6 Internet connection, as demonstrated in UCL Computer Science itself.

11.1.5 General Conclusions

The management of chronic illnesses and conditions such as stroke, diabetes, asthma and coronary artery disease represent a major and growing challenge to healthcare services throughout the world. Mobile devices are needed to measure, communicate, inform and support individual patient decisions and choices based on clinical guidance. This will permit chronically ill patients to benefit from healthcare support by multi-professional teams at unpredictable times and places and will enable them to lead as full a life as possible.

There is evidence that the greater the patient’s involvement in the management of their illness, the better their compliance with treatment and the clinical outcomes achieved. Patients requiring

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

careful management of symptoms, physiology or function will need to communicate changes in monitored readings to their clinical team and obtain and obtain management advice, possibly via a decision support system. The latest generation of PDAs with a secure mobile link to the patient's (web-based) electronic health record would allow the delivery of this kind of patient care.

The main change in the healthcare delivery pattern through the wide adoption of IPv6 and wireless services will be to support and integrate distributed clinical care across sites within and outside a hospital, GP surgeries, community clinics and patients' homes. The challenge is to convince healthcare providers that distributed access to health information is feasible, scalable, and is of an acceptable quality to support clinical practice. It is also important to end users, managers and to the NHS that user authentication and system security is demonstrably robust and conforms to national policies.

The 6WINIT project has provided a valuable opportunity for the UCL-CHIME team to understand the limitations of the existing IPv4 Internet, and of the components that are required and now available to utilise an IPv6 network. CHIME has provided a realistic test bed for the combined deployment of the 6WIND edge device, the Road Warrior application and the University of Murcia PKI server, utilising the UK6X and other IPv6 networks via an IPv4 tunnel. It has also provided a demonstrable scenario for IPv6 configured iPAQs and other access devices. We hope that this test-bed has helped to validate these various components, and provided a useful way in which they could be demonstrated to the wider community.

The CHIME deployment also illustrates an example migration strategy that could be adopted in a healthcare enterprise with a significant legacy of IPv4 servers and networks.

However the wide-scale adoption of wireless (IPv6) communications within healthcare requires several areas of cultural change as well as sound technical solutions:

- The demonstrable security and reliability of access to a patient record information;
- Conformance to NHS security policies;
- Interoperability with the present version of NHSnet;
- Impact on the procurement strategy for the replacement of NHSnet;
- The practical usability of PDAs in place of workstations and laptops, at least for emergency access;
- Clinical acceptance of the idea of shared (multi-site and multi-agency) records;
- Patient attitudes to their records being shared across sites, including consent for disclosure;
- Patient attitudes to accessing and requirements for interpreting their own health record.

The research and development work at CHIME into federated electronic health record services is ongoing, and the research team hopes to build on the infrastructure developments achieved through 6WINIT in future projects. The existing demonstrator will remain functioning after the end of 6WINIT, providing the technology partners with continued access to the clinical applications and sample patient data for further testing and for marketing purposes. It is hoped that future opportunities will allow some of these clinical and organisational challenges to be explored through live clinical demonstrations.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

11.2 The Applications in Krakow

11.2.1 The Applications

Like in the applications of Section 11.1, the Polish clinical demonstrator required collaboration between the John Paul II Hospital (JPiI) as the clinical site, the Department of Computer Science of the University of Mining and Metallurgy (UMM CS) as providing technical expertise and equipment, and the Academic Computer Centre CYFRONET as providing both Intranet and external communications.

Again the result has been to adapt, develop, set-up, deploy and test real clinical applications in a real clinical establishment in wireless networks with usage of the IPv6 protocol. These clinical applications are real in the meaning that:

- They are substantially based on Hospital Information Systems and applications now in “production” use at the John Paul II Hospital in Krakow, Poland, and in other hospitals in Poland and Germany, and/or
- They are adapted instances (clones) of these applications, working for test with non- production databases (anonymised data), or
- They are new clinical applications in trial use with a plan to be introduced to operational work in the coming years.

The following applications were trialled:

- Mobile multi-access to the Clinical Appointment System (CAS),
- Hospital Appointment Clerks’ access to the Clinical Appointment System (CAS)
- Hospital intranet access to the NetRAAD medical radiology database system.
- Mobile access to the NetRAAD medical radiology database system from outside the hospital
- Konsul: operating theatre access to results of advanced medical examinations (angiography films)

11.2.2 Network and Equipment

The hospital is well equipped with medical instrumentation. Many of these devices provide external output, also in a digital form, with an important share of the DICOM *de facto* imaging standard. On the other side, the hospital’s buildings are cross-connected with broadband networks over fibre infrastructure (622 Mbit/s ATM and 100 Mbit/s Fast Ethernet), and are all located in a tight and compact campus, providing excellent conditions for deploying a wireless intranet all over the hospital area. The Hospital is also well populated in different computer equipment (desktop PCs, laptops, PDAs), and has recently implemented a “hospital without films” policy basing on a prevalent usage of a database of electronic patient care records (including JPEG referential and DICOM diagnostic-quality images from different radiological examinations). This database management system and its web clients are called NetRAAD and are now in use in all wards of the Hospital, eliminating the need for a traditional “paper and film” clinical documentation.

The hospital runs only IPv4 for its own activities, and all its production use is over an Intranet which covers only the hospital. Indeed as in the activities of Section 11.1, external access to clinical data is not permitted off-site. Even access to real appointment systems would probably not be permitted. Thus there was a need for the other Krakow partners to help with the external connectivity. IPv6 access was provided, however, via the Polish NREN initially (with IPv6/IPv4 tunnelling), and 6NET from October 2002. Attempts to use the 6Bone suffered from severe

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

performance problems; use of the direct tunnels helped. The availability of the 6NET route removed any performance problems.

In addition to its extensive 100 Mbit/s Ethernet, ATM and 622 Mbit/s cable infrastructure, the JPII Hospital installed a small pilot WLAN installation for wireless tests with usage of laptops and iPAQs. The Hospital also temporarily installed a Pico Bluetooth Access Point to perform Bluetooth radio interference tests with medical equipment.

However, the basic extensive tests of Krakow clinical applications after their development were carried over the Krakow MAN, where the client machines and software were located in a Cisco Aironet WLAN in the UMM Computer Science Department, while the servers were located in the JPII Hospital's intranet. A dedicated connection was set up in October 2002 between UMM CS, ACC Cyfronet and JPII Hospital, to carry native IPv6 traffic.

Both WLAN and GPRS were available in Krakow for the project. Discussions have started about access to UMTS, but this will not occur during the period of 6WINIT.

They have used mainly laptops and iPAQs with IPv6 Linux as user terminals.

11.2.3 Adaptation of Application Packages to IPv6

This was straightforward in most cases because most of the packages were written in Java. The lack of IPv6 support in Java in the early stages of the project was overcome by using an external C library. In some cases this was invoked via JNI from the Java viewer application. The adaptation/transition of web-based applications has been also simplified by the appropriate IPv6-compatible web servers already available around, and the fact that they can be relatively easily used in more complex multi-tier system architectures, e.g. J2EE, instead of the proprietary IPv4 servers currently used by application server vendors."

11.2.4 Security

In principle, all the Krakow clinical applications developed for demonstration are web-based applications, and therefore the standard application-level security approach used for web applications has been chosen. The DICOM viewer, as well as CAS and Konsul applications, all use SSL and http-s on all tested types of client machines (iPAQ, laptop) for encryption. The DICOM viewer additionally uses a mutual authorisation of the NetRAAD server (GateRAAD) and the viewer application, respectively, on an iPAQ/laptop with usage of HTTPS, certificates for both sides and a dedicated CA. However, the University of Murcia PKI infrastructure has not been used in Krakow for its limited availability and Spanish-only documentation

A secure virtual private network (VPN) has been used and tested between the servers' network in JPII Hospital and the clients' WLAN network in UMM CS over the insecure MAN link. This VPN was implemented with two 6WIND IP Gates, deployed in these two locations, respectively.

11.2.5 Generic Technologies

Several of the generic technologies of Section 8 were used, in particular mobile IP (based on the 6WIND router Home Agent, and the Linux release for the iPAQ and Laptop). It was used mainly with the VIC and RAT of Section 10.6.

For the CAS application, a WAP server was also used – with an IPSec tunnel between the UMM WAP gateway and the operators GPRS infrastructure.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

11.2.6 Radio Interference Tests

The Krakow clinical 6WINIT site performed most of the tests and demonstrations in a real clinical environment in the John Paul II Hospital. Thus, the management of the Hospital and the Hospital's IT Department were concerned about the potential mutual influence of wireless networks and the medical equipment and the consequences of using wireless technologies in the Hospital's premises. Therefore, a series of tests have been performed to measure the effects of radio interference of 802.11b WLAN and Bluetooth devices (access points and client PCMCIA cards), respectively, with three basic equipment types normally daily operating in the Hospital, and also emitting strong electromagnetic fields. These equipment types were:

- A microwave coagulator, operating at impulses (maximum a couple of seconds each usage) several times during a cardiovascular surgery in an operating theatre, thus potentially affecting the wireless Konsul application using a WLAN;
- A computer tomograph (CT) emitting a strong X-ray field, however, in a well isolated room in a separate building of the Diagnostics Department;
- A Nuclear Magnetic Resonance (NMR) device, emitting a strong, but constant, magnetic field (1.5 T), also in a well isolated room (actually, a Faraday Cage) in a separate building of the Diagnostics Department.

With the microwave coagulator, it had a serious negative impact on the WLAN performance, since it works in neighbouring or even partially overlapping frequency bands. However, the proper functioning of the Konsul application should not be threatened thanks to its web nature, if the actual download of the medical films is done before using the coagulator and only a local playback is done afterwards. A similar effect, for the same reason, was obtained with the Bluetooth access point and the Socket Bluetooth PCMCIA notebook card,

With nuclear magnetic resonance, the access points and the measuring notebook were located just outside the isolated examination room (Faraday cage), behind the leaden observation window, a couple of meters near the NMR device. Nobody except the patient stays in examination room during the actual NMR examination. Generally, no anomalies were been noticed with regards to the operation of the NMR device – except a slight problem in Bluetooth performance during the switch-on of the NMR.

From the tests with Bluetooth, in the vicinity of a working Computer Tomography device, the strong X-ray field seems to have no effect on the Bluetooth devices outside the examination room.

11.2.7 Conclusions

A number of tests and demonstrations with various medical applications developed in the Krakow 6WINIT site have been successfully performed, both in local settings in the city of Krakow, in particular in the real clinical testbed in the John Paul II Hospital, and at remote sites in Europe, on many occasions, including public events.

The state-of-the-art clinical applications developed and adapted for wireless IPv6 usage have attracted a substantial interest from healthcare staff, media, local authorities, SMEs, larger IT companies, and research institutions. Throughout demonstrations, these applications have proved their usefulness in the wireless access scenarios for both healthcare professionals and patients – citizens of the European Information Society. They can clearly bring an improvement of the quality of healthcare services and better utilisation of limited medical resources, as well as more comfort and quality of life for the patients.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

The Krakow clinical applications have been developed to the state of advanced prototypes, which can be, from the technical point of view, relatively easy transformed into market products.

The Krakow 6WINIT clinical demonstrator has also performed several radio interference tests of WLAN and Bluetooth wireless technologies with three types of advanced medical equipment emitting electromagnetic fields. These preliminary experiments have shown the feasibility of usage of these wireless technologies in hospital premises, provided that the normal security measures and appropriate patterns of applications' operation are in place.

An important impact of the project will be the deployment of the Clinical Appointment System and the Konsul system and possibly also the NetRAAD-based DICOM applications in a network of cardiology-focused hospitals in Warsaw and Mazowsze Region in 2003. Equally importantly, a dissemination of the 6WINIT project results, including the clinical applications themselves is planned within the activities of the Krakow Centre of Telemedicine (KCTM) and further within the PRO-ACCESS (IST-2001-38626) accompanying measures project targeted on take-up and transfer of advanced e-health and telemedicine solutions to so called Newly Associated States (NAS).

11.3 The Guardian Angel System (GANS) and the Ambulance Scenarios

11.3.1 Introduction and Overview

UKT runs one of the few dozen high-fidelity patient simulator centres worldwide. The Tübinger Patienten Simulator System (TUPASS) has the following relevant characteristics. In a standard operation theatre a simulated "patient" is connected via (standard) interfaces to the corresponding environment. The "patient" is a simulator-driven realistic doll capable of receiving and reacting to all relevant treatment such as injections, intubation etc. Possible reactions are then observable on a standard patient monitor. Separated from the operation theatre by a semi-transparent mirror wall is a control room. The control room personnel can overview the operation theatre through the mirror wall and several controllable video cameras. Additionally, it has a bi-directional audio connection to the theatre. From the theatre also the patient monitor data are transmitted to the control room. Finally, the control room team can directly influence the simulator operation, possibly putting stress on the operation theatre team. Recorded simulation sessions are eventually used for debriefing. TUPASS and comparable centres have a proven record in training students, anaesthesia specialists, intensive care personnel and other paramedics.

The proven and very positive experiences from TUPASS led to the concept of the Guardian Angel System (GANS). This is a real-time, mobile and wireless telemedicine system, designed to provide acute medical help to healthcare professionals outside the hospital. Here the Operation theatre and control room are virtually remote from each other. Assuming the role of a "Guardian Angel", the control room personnel can provide acute telemedical help to a local physician team, which has to cope with a life-threatening emergency – no matter if the emergency is taking place in a "fixed" hospital setting or in a mobile ambulance car rushing towards the hospital. Medical experts not located at the scene of the emergency can participate in the first aid, giving advice. This will enable the team on scene to solve the crisis situation in time preventing severe damage to the patient.

To be able to consult the remote physician, it is necessary to transmit all vital data streams such as blood pressure, oxygen saturation, ECG, live audio and video from a possibly moving ambulance to the supporting hospital centre. In order to realistically simulate the use of the system without risk to real patients, we use our full-scale patient simulator system is used at the Tübingen technologies clinical site - simulating the ambulance car in the existing first prototype tested.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

In 6WINIT, the GANS concept was applied to an “ambulance car to hospital/GANS centre” scenario. The network technology assumed is initially “Mobile IPv6-over-IPv4-based GPRS over GSM and WLAN”. In the final review a demo using UMTS is envisaged. Although not addressed in 6WINIT, other systems such as ETSI TETRA may become technology candidates for GANS.

11.3.2 Technical Abstraction

A meaningful abstraction for a “6WINIT Guardian Angel System” comprises “only” a mobile terminal in the ambulance car, a sufficiently powerful public network providing or allowing for (IPv6) edge mobility and IPv6 transport to the hospital and within the hospital a “consultation terminal”, the latter for security reasons initially even isolated from the patient record system of the hospital.

In this abstraction, the mobile station had to provide audio, video, patient administration data and patient vital functions data. The Hospital side had the multimedia services and an Apache store, with a data retrieval system based on MySQL.

The system must allow various IPv6-enabled communications systems between the mobile and hospital terminal, allowing the transmission of video, audio and real-time data. It was considered particularly important to allow simultaneous Mobile IP access to several mechanisms of communication; the concept being that one uses whichever of the ones available is best at the time. In practice, one used MIPv6/Ethernet and MIPv6/WLAN most of the time. GPRS was available, and some of the modules were shown to work over it. However with at most 9.6 Kbit/s on the link, a need to use MIPv6/IPv4/GPRS, and only dynamic addresses, it proved impractical to use GPRS seriously as an access network. In the final review, it is planned to use MIPv6/UMTS and MIPv6/WLAN. It was also necessary to achieve QoS of the media; one requirement here was to limit the bandwidth for the different media.

In this activity, Ericsson provided the routers and hosts with their multi-access and MIPv6 capability, UKT the clinical knowledge and real-time data, and RUS the network and software development skills. Thus a good IPv6 infrastructure between these three partners was needed. It was provided by 6WIN between RUS and UKT, where it was principally needed. Between Ericsson and the other partners, it was provided by IPv6/GEANT when needed.

11.3.3 GANS as a Middleware System

To allow for future seamless integration of the GANS into existing hospital infrastructures, the GANS adopts a standard software approach based on J2EE. While the present JDK 1.4 perfectly supports IPv6, the version used for the Server is still lacking IPv6 support. Hence IPv6 had to be introduced at the hospital, i.e. the server side by means of a combination of an Apache2 web server and the Resin servlet engine. At the remote client side, i.e. the ambulance, an application representing a JMS client and the different media applications as used IPv6 directly.

11.3.4 Security and Transition Mechanisms

Considerable effort was devoted to ensuring that all the components of GANS could work in native IPv6; as a result, the only transition problems were that it was necessary to tunnel to demonstration sites.

No effort was undertaken in network level security. Targeting not only a nomadic but also a real mobile application the present Road Warrior approach is not directly applicable to the GANS. At application level, using the Java Security Framework, a certificate-based key management

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

solution for GANS was prepared; corresponding exchanges with the certificate server at UCL-CS (developed by University of Murcia) have been carried out. However security was not really targeted in this activity.

At the demonstrations, MIPv6 Home Agent was always provided by the Ericsson's AXI 462 router. At RUS such a router was included in the IPv6 testbed since the preparation of IST 2001.

Multi-access was improved during the project; it will be only in the Final Review demonstration that the GANS application system will exploit these capabilities in order to show the 'always best connected' paradigm.

11.3.5 The Clinical Applications

In order to get as much feedback as possible to improve and refine the clinical GANS application, the GANS idea and system was presented by UKT/RUS not only at many international communication technology events, but also at some interdisciplinary, international expert. Wherever it was presented the feedback was very positive and many could not understand why such solutions have not been in place since many years. An anonymous questionnaire at a meeting of anaesthesiologists (RiMa2002) in private practice revealed that the need for such a system is so high that some recommended to start it even with lower fidelity and reduced bandwidth (in the sense of "something is better than nothing"). Also GANS was continuously evaluated medically at the Patient Simulation Centre at UKT. Many different experiments and training sessions simulating different aspects of care (field emergencies, ward emergencies, OR complications, ICU care) revealed many feedback suggestions.

11.3.6 Communication requirements from the clinical viewpoint

The requirements can be split into the different locations of the GANS parts: the emergency location and the GANS Centre. At the **emergency location** (remote), where the patient needs to be treated urgently and the local team needs help. This could be an ambulance, an OR, an ICU, or any other place where patients are treated. As there is a lot of personnel turnover, the training requirements to use the GANS as a "user" must be minimal. This side of the system must be as "fool-proof" as possible.

The system to store and send the vital signs must be "on stand-by" all the time since it is not foreseeable when an emergency happens. In case help is needed the time available locally is very limited, because that is where the emergency happens and every hand is needed to treat the patient. Therefore a "one-button-activation" of the GANS is required. All connections and settings must be made and checked automatically. This includes the logon, identification, the connection, the choice of the best available network (LAN, WLAN, UMTS, GPRS), the audio/video settings and related decisions. The local team must use a wireless headset to communicate with the GANS centre in order to have the hands free. The local trends of the vital signs stored in a run-through buffer should be transmitted as soon as bandwidth allows it to provide as much information and reduce personal communication requirements ("how was the blood pressure 10 minutes ago") as much as possible.

At The **GANS centre**, trained professional GANS instructors (tele-mentors) work. Here two main applications can be distinguished.

- The communication with the remote location. This includes all the vital signs, video and audio developed in 6WINIT, including the transmission and display of acute trends
- The information support system for the GANS experts.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

The GANS centre has the whole session control except the initiation and termination of the connection. In order to give critical advice the GANS centre personnel needs to have a real-time video image of the treatment scene and the online vital signs of the patient including the waveforms. The waveforms need to be scalable concerning amplitude and horizontal speed in order to make diagnostic decisions. Also the corresponding waveforms of every heartbeat need to be synchronised in the display. The display of the stored vital signs before the GANS was involved, need to be shown as a trend plot, also with scalable zoom functionality. In addition to that control of the audio and video settings is important. The centre needs control of the camera picture including pan, tilt and zoom. The audio mix from the ambient room microphone and the wireless headset must be adjustable. An option to decide between a direct communication to the headset or to a room loudspeaker may be advisable. The problem of session storage, data annotation and retrieval has not yet been investigated. We found that WLAN gave quite adequate performance for these functions. The 9.6 Kbit/s available with GPRS, in an IPv6/IPv4 mode, was completely inadequate – though it could provide just about enough bandwidth for the vital data. With the two up-channels offered by the UK MMO₂, both the vital data and the audio could probably be provided. We believe that the UMTS bandwidths would be completely adequate for this application.

We found that even the experts need systems to get information e.g. on rare diseases or seldom-used drugs. Also they need support in tracking the recommendations given to the local team and automated checklists in order not to forget important items. This part is outside the focus of 6WINIT, but will be an important area in future projects implementing GANS centres in the real world.

11.3.7 Evaluation of the GANS - The “Proof of concept” study

At UKT, there is an ongoing study for the proof of the GANS concept. They are investigating physicians from different medical departments who are supposed to treat simulated emergencies at the patient simulator with or without the telemedical assistance of a “Guardian Angel”. This Guardian Angel is a very experienced emergency physician, who can remotely be consulted by the physician on the emergency scene.

They have set up a clinical testbed for this study in the fixed environment of their simulation centre. This is used to avoid endangering patients before both the real benefit for patient safety and proof of technical security has been clarified scientifically. The construction of the standardised emergency scenarios for the participants was a big effort. All scenarios (e.g. Myocardial Infarction) are scripted and brought close to reality for a high validity of the data. They developed a so-called “Technical Emergency Advanced Rating Score” (TEARS) to measure the quality of the medical treatment. The Live-Rating of this score leads to objective data to compare the treatment of the physician alone with the treatment assisted by the Guardian Angel.

The study is not finished yet, but preliminary results are showing a remarkable increase of emergency patient treatment. Measured by the TEARS, the average improvement of patient treatment with GANS is 50%. Also the participating doctors reported that the GANS was very helpful for them in caring for these “patients”. They said it reduced their stress very much and contributed to a feeling of more control over the scenario. These results are demonstrating in an impressive way the importance of acute telemedical help, such as provided by the GANS.

After the end of study and analysis of results, the approval of ethic committees, medical associations and health insurers, they plan to start the equipment of several patient beds at UKT with the technical architecture necessary for the implementation of the GANS under real conditions.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

11.3.8 Clinical problems to be solved

The Proof-of-Concept study (POC) was performed in the realistic patient simulation centre of UKT. This made the study possible without endangering real patients while at the same time getting information about the system in an almost real atmosphere. Regarding the communication requirements and the transmission of the vital signs everything was in fact real and would not change in the setting of actual patient care, as the used vital sign monitors are the routinely used in the hospital.

Of course the baptism of fire will be the deployment of a GANS in the real clinical environment in different fields of emergency patient care (ambulance, OR, ICU). The problems to be solved before a GANS can be initiated in real patient care can be summarised under different headings:

Legal concerns:

A legal basis is needed for the adoption of GANS centres by member states regarding telemedical remote counselling. This concerns the doctor-patient relationship as well as security aspects of data. We see the GANS as a “human reference book” and no contract with the patient directly. We also think that the application of telemedicine in acute emergencies is less problematic than under normal conditions. But the decisions of European courts will be important for the spread and future of GANS centres.

Process of distributed decision making:

The emergency help from the GANS team involves distributed decision making between the local and the GANS team itself. Also the diagnostics are only made remotely. This involves several psychological factors that will have to be considered further.

Costs and financing:

Because the budgets in healthcare are calculated differently in each member state, it is difficult to get exact numbers, to decide who will have to pay for a GANS service and to define who will save money by the reduced rate of complications and disability. From a more general budget viewpoint, we think that the GANS will be worth more for a state than it costs. Savings due to reduced expenses for claims and lawsuits may even lead to a good business model for individual hospitals and private practice offices.

Partners:

To establish GANS centres in the European health sector and market we need strong partners from industry, government, health insurers and healthcare.

11.3.9 Potential of GANS for the Healthcare sector

The telemedical system called “Guardian Angel System (GANS)” developed in 6WINIT has a huge potential for the whole healthcare system. It could improve the treatment of patients in medical emergencies in all fields of medicine and in every medical location where patients are to be observed or treated (Intensive Care Units, Operating Rooms, Intermediate Care Units, Monitored bed wards, Interventional procedure locations, out-patient invasive institutions, dentists, ambulance cars, helicopters). Due to the communication possibilities demonstrated in 6WINIT, this acute help seems to be deliverable to all treatment scenes, even to ambulance crews caring for patients out in the field alone. Through the common use of the experts in future GANS

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

Centres it could be economically possible to provide the GANS service 24 hours and 7 days a week.

From a medical point of view GANS proved to be very useful and applicable in the real clinical scenarios performed by the UKT/RUS team in Tübingen (see 11.3.2). When clinical studies in the future with real patients and larger samples confirm this magnitude of benefit shown in the POC-study, the success and widespread application and use of GANS centres throughout Europe will be inevitable. One must be aware of the fact that an improvement of the treatment score in emergencies by 50% through the use of the GANS (shown in the POC-study) is not marginal but close to a revolution in the emergency medical treatment.

The social and ethical value of this unsurpassed improvement in acute medical treatment will be demonstrated in the avoidance of complications and disabling sequels of treatment errors and delays, as well as in many lives saved. The economic benefit of a widespread GANS application is similarly attractive and promising: The political economy costs saved by the earlier initiation of effective and correct treatment regimens and the avoidance of treatment errors and the implicated costs for prolonged stays in the intensive care unit and rehabilitation are tremendous.

Another aspect of a widely used GANS is that it could offer an important contribution to quality improvement and documentation in medical incidents. One must be aware of the fact that problems and errors during emergencies are not systematically analysed. GANS could become a very innovative case archive of critical incidents (online-recording of video, audio and vital data) unparalleled by any existing critical incident reporting-system. This could offer new insights in the evolution of errors in medicine and the proposal of effective countermeasures.

The EC promotes the development of e-Health applications, the networking of healthcare professionals and the introduction of a personal electronic health card. It also required the member states to implement these steps until 2005. With the solution of the (minor) problems mentioned in 1.6.1 this is a very positive climate for the further development and deployment of GANS applications Europe-wide.

In 6WINIT many problems could be identified and solved. Now is the time to transfer the research results into ready-to-use real-world applications, successful business cases and to let the European citizens profit from the widespread use of GANS centres.

11.3.10 Conclusions

The Guardian Angel System concept was successfully implemented in a sophisticated and realistic research test-bed in the patient simulation centre of UKT. The technical tasks to support the medical team during acute emergencies and the advanced communication requirements (IPv6, multi-access, seamless handover) were solved and demonstrated in prototype versions, which should be usable directly with UMTS when it becomes available. The immense medical value of a GANS could be demonstrated impressively in the proof-of-concept study at UKT. Thus the 6WINIT project developed a functional prototype of a revolutionary medical emergency help system.

This system should be made market ready and introduced to the modern medicine as soon as possible to make it available in the real world of European citizens, wherever emergencies happen: Emergency rooms, operation theatres, intensive or intermediate care units and – in the future – in an mobile environment for ambulance cars as well. The impact of such systems will not only be enormous regarding the reduction of healthcare costs but also in enhancing patient safety and the quality of life.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

11.4 Conclusions and Comparisons

These three case studies have attacked three complementary aspects of the healthcare problem. In each case, it was not possible to use real patients or even their live data; legal and ethical constraints made this quite impractical. They all tackled their chosen problem successfully, and pursued it far enough that introduction of their solutions into live healthcare situations could be envisaged – and the problems in the way were identified. These problems were seldom technical; they were more the resolution of ethical, legal, organisational and cultural problems. Moreover, the different pilots went to different depths in some key areas; the solutions adopted in one will solve some unresolved problems in others. We will give some examples.

The London activity of Section 11.1 addressed problems of security in the access to clinical data very thoroughly; they also addressed problems of transitioning between large legacy IPv4 systems and IPv6 ones. These problems were largely side-stepped in the other two activities. The Krakow activity of Section 11.2 investigated a much wider set of clinical applications. They also investigated the interference between the wireless technology and the clinical instruments. The resolution of interference concerns will be vital to the introduction of any wireless technology in the hospital environment. The Tübingen work of Section 11.3 concentrated on the simultaneous access to several different network technologies and the combination of audio, video and vital data modes of communication. Again these are vital to the introduction of the technology in the accident and emergency environment – while the security aspects of the London work and the radiographic aspects of the Polish should eventually augment its capabilities.

All the activities felt that they would be ready for live use as soon as identified concerns had been overcome. All were optimistic that their approach would make a real impact on healthcare.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

12 THE DEMONSTRATIONS (D16, D17, D18, D19)

It is always difficult to decide how much effort to put into public demonstrations, as distinct from those at Project Reviews. Because of the newness of the subject area – both wireless and IPv6, we decided to put considerable effort into three public demonstrations: IST 2001 in Düsseldorf in November 2001, INET 2002 in Washington in June 2002 and IST 2002 in Copenhagen in November 2002. There was a fourth demonstration at the Project Review in Adastral Park in January 2002, and there will be another demonstration at the Final Project Review in Stockholm in January 2003. In addition there have been many smaller demonstrations, usually involving one or two Partners. These are described in the project's Periodic Progress Reports and other Deliverables. A few examples of such smaller demonstrations are as follows:

- ICC 2001, Helsinki (Ericsson Research – demonstration of simultaneous multi-access)
- MUM 2002, Oulu (VTT - home environment)
- 19th Congress of the European Association of Hospital Managers, Krakow (UMM - implementation of CAS and DICOM viewer applications)

Well-planned demonstrations have the huge advantage that they force the partners to make their components work together. In addition, they cause a maximum exposure of the technologies involved – this is good if it a successful demonstration; disastrous if the demonstration fails. We put a large effort into the three public demonstrations to ensure that they were successful. We discuss here the way the three public demonstrations and the Final Review have contributed both to public awareness of the technologies and the success of the project itself. We feel that the effort we put in was worthwhile – even though much of the effort in the last nine months of the project was concentrated on activities, which would be demonstrated.

12.1 IST 2001 (QR4)

Two applications were demonstrated at IST 2001: the navigation system from VTT of Section 10.3, and the ambulance demonstration of Section 11.3, VTT configured their indoor navigation system, which is based on WLANs and IPv6. It attracted some attention – mainly because WLANs are so widespread. From this viewpoint it was interesting, but it did not lead to any additional collaboration between partners, because it was just a VTT demonstration.

The Guardian Angel ambulance (GANS) demonstration was much more complex, and many partners were involved in making it very successful – particularly Ericsson, RUS and UKT. The Tübingen hospital (UKT) and RUS were responsible for the applications scenario development and implementation. Ericsson Telebit provided the MIPv6 Home Agent and the router and configured them for this special event. Ericsson Research provided the multi-access MIPv6 solution as well as a tunnel broker to be used in connection with GPRS (dynamic address allocation). T-Nova provided the GPRS infrastructure – though in the end this was not used. There were two reasons for this; the unavailability of fixed addresses made its use very difficult (though the Ericsson tunnel broker had got round this problem), and it was not possible to access GPRS from inside UKT where the GANS patient simulator was sited. The press release was co-ordinated by Telscom, who prepared and distributed it to the visitors and to the press. The 6WINIT booth was a main attraction of the IST 2001 exhibition centre and even the dignitaries visited the booth and expressed their satisfaction. In this demonstration, the Ericsson Telebit AXI 462 Router was used as IPv6 access router at the conference site. The audio and video were IPv6, encapsulated to go over the IPv4 GEANT infrastructure using the AXI 462 as decapsulation

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

endpoint. Mobile IPv6 was used together with the Multi-access solution from Ericsson Research, with a home agent in the Ericsson Telebit AXI 462 router.

The ambulance demonstration forced many partners (T-Nova, Ericsson, UKT and RUS) to work together. It ensured that we had a really viable basis for future development of more advanced concepts. It also gave us our first example of the potential, and pitfalls for working with GPRS. These last have already been discussed in Section 5.3, and so will not be repeated. Finally, it did create an excellent public awareness of the project in the most important venue for IST projects.

12.2 INET 2002 (D18)

The demonstration at the joint "IPv6 Forum's IPv6 Technology Deployment Summit" and INET 2002, in June 2002 in Washington DC was much more ambitious than that at IST 2001. This time we demonstrated: GANS (UKT, RUS, Ericsson), the Road Warrior System (IABG, UCL/CHIME) and the Home environment (VTT). In these demonstrations, there was a much more complete IPv6 infrastructure, with the main router provided by Ericsson Telebit. While IPv6/IPv4 was used over Internet2 and GEANT to each of the remote sites, and GPRS was not available in Washington, the remote sites all had full IPv6 infrastructures. Moreover, there was full Mobile IPv6 and IPsec/IPv6 over the WANs to the sites requiring it. .

In this version of the GANS demonstration, we showed Ericsson's multi-access – "always best connected" – solution for MIPv6, choosing whichever was best of WLAN and a slower network access. At the demo, GANS embedded control and secure the real-time data (vital data, video, bi-directional voice) in a J2EE environment. At INET 2002 the then current version of JBoss' J2EE implementation - not fully IPv6 capable - was 'simulated' by 'private' IPv6 based code (this situation has been fixed since then).

In the Road Warrior System (IABG, UCL-CHIME), we showed how users could establish secure communication channel in a MIPv6 context using its fixed Fully Qualified Domain Name (FQDN) instead of its IP address. The demonstration showed both an unsecured and a secured access from Washington to CHIME/London.

In the Home environment demonstration we showed VTT's Home environment system, which controls and integrates appliances such as saunas, TV sets etc. It showed the use of UIML (user interface mark-up language) tools to handle control data from different home control devices via its innovative User Interface Broker architecture, The standardised OSGi concept, IPv6 and IABG's Road Warrior system. In the demonstration, "the traveller" in Washington was able to switch on and off home appliances in Oulu, Finland, such as lamps and a TV set – the audience was able to observe the effect of the traveller's action in Oulu via a live JMF video over IPv6.

In these demonstrations, there was a much more complete IPv6 infrastructure, with the main router provided by Ericsson. While IPv6/IPv4 was used over Internet2 and GEANT to each of the remote sites, and GPRS was not available in Washington, the remote sites all had full IPv6 infrastructures. Moreover, there was full Mobile IPv6 and IPsec/IPv6 over the WANs to the sites requiring it. .

12.3 IST 2002

The demonstration at IST 2002 was different in several respects. The demonstrations were part of the IPv6 cluster, and shared both infrastructure and exhibition area with other IPv6 projects. All wide-area connectivity was now provided by IPv6/IPv4 to the 6NET Point-of-Presence in Copenhagen; from there it was provided by 6NET to all the project partners. In all cases there was native IPv6 from there via 6NET and the IPv6-enabled NREN: VTT (Finland), UCL (UK),

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

UMM (Poland) and ETRI (Korea). While there was extensive use of WLANs, it was impossible to show UMTS; this was not available. Almost all the demonstrations used WLANs to the end terminals; since there were many demonstrations in parallel in the IPv6 cluster, it was impressive that there were no noticeable performance problems.

Deliberately few of the demonstrations already made in INET 2002 or planned for the Final Review were shown here. Thus the main demonstrations were: access to radiographic data from PDAs in UMM (Krakow, Poland), access to patient data at UCL (London, UK), access to streaming media in ETRI (Daejeon, Korea) and SIP IPv4-IPv6 interworking and media transcoding via TZI (Bremen, Germany). Now the aim was more to show IPv6-enabled applications working successfully over WLANs, in a way that would also work over UMTS if the networks had been available.

The two clinical demonstrations provided a valuable end-to-end validation of the reliability of connection, the network performance and security. The main demonstrations this time came from Krakow, which showed:

- NetRAAD DICOM images viewer on iPAQ in an emergency conditions scenario; this demo was joint with CHIME showing access to the basic textual electronic patient record of the demo “patient”.
- Clinical Appointment System - a full functionality demo including the patient making and checking his appointments from an iPAQ in the conference WLAN and the JPII Hospital’s appointment clerk revising and scheduling the appointments on a WLAN-equipped laptop. The patient notification on accepted appointments via SMS has also been demonstrated.
- VIC/RAT-based audio/video teleconference employing Mobile IPv6; this demo was prepared jointly with 6WIND.

Given that the IPv6 wireless access point in the exhibition hall was serving several simultaneous IPv6 Cluster demonstrations, it was pleasing to find that web screens were downloading from London within about half a second (albeit with only textual data). There were no timeout problems or periods of inaccessibility during or in between demonstrations. The scaling, resolution and performance of the Compaq iPAQ, as adapted for IPv6, was excellent. The UMM radiology application showed a good response times for this application, including the downloads of DICOM image series from Krakow within several seconds, which is perfectly acceptable for that kind of clinical data. The quality of the angiographic data downloaded from Krakow was of very reasonable quality enabling actual clinical use, as referential images for x-ray, CT, NMR images and angiography; it was not considered adequate for diagnostic use. The download time of several seconds was sufficiently rapid to be acceptable to health professionals. The battery life of the iPAQ was only sufficient for around an hour of continual use, which is far from ideal for mobile clinicians, and we would hope for this to improve in future versions of this hand-held device. There was genuine interest in the clinical use of wireless IPv6 as an exploitation of this technology; we feel that a secure demonstration of access to these applications over GPRS and UMTS could be very attractive to the healthcare sector.

The conferencing application from the 6WINIT viewpoint was only to show how H.323-based conferences could interwork with Mbone ones – with emphasis on the audio. We showed also that IPv6-based VoIP clients from Telscom and VOCAL could interwork also, and that it was possible for GSM telephones to come into the same conferences.

VTT’s Home environment demonstration shown at INET 2002 was repeated – but this was more advanced as it also combined the intrusion control mechanism developed by UoS.

Additionally the anticoagulant application from UCL CHIME demonstrated a remote access to a Federal Health Record Server. In order to secure the sensitive data transmitted over insecure

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

networks the Road Warrior has been used. While the Road Warrior client was running on a Linux system, the Road Warrior gateway functionality run on a 6WIND Edge Device. Between both of them X.509 v3 based certificates were used for authentication purposes.

The ETRI demonstration of streaming showed impressive football matches with video on demand over full IPv6 connections to Korea; unfortunately this required at least 2 Mbit/s bandwidth – and we do not yet know when that will be available over UMTS.

12.4 Final Review

The Final Review will be held in Stockholm at the premises of Ericsson. This is the only venue at which we can have access to UMTS. We now expect to show demonstrations that have not been shown previously, or ones that can be shown to work over UMTS. The access to the UMTS will be limited; at most we will have a few days to prepare the demonstrations. There are few UMTS phones available; we will have access to them only when we are physically in Stockholm. The only access to these phones is via IPv4/PPP – with only one channel; as a result, all demonstrations will need to be carefully planned; only tunnelled IPv6/IPv4/PPP will be available. Clearly it is not possible to evaluate now the results of these demonstrations; it is possible only to describe what we expect to show, and what might be learnt from it.

We currently plan four demonstrations: VoIP of Section 10.7, using a SIP user agent, the GANS demonstration of Section 11.3, active bandwidth adaptation of Section 10.6 and media streaming of Section 10.5. The first is the standard sort of demonstration that is a pre-requisite for media conferencing over UMTS. Since SIP is required by UMTS, it is an essential first step.

In the GANS application, we expect to emulate all the separate components that have worked previously over WLANs, but also show simultaneous movement with Mobile nodes from UMTS to WLANs. There will be simultaneous use of Audio, video and vital data over the different modes of access. This should help us evaluate the performance and applicability of the system for these purposes.

In the active bandwidth adaptation demonstration, we expect first to show video conferencing over WLANs. We then expect to use the UMTS, with its lower bandwidth. At first there will be significant errors; then as the active bandwidth management kicks in, the quality of the video should recover. Again, this would be an example of a value added service that operators may want to provide when UMTS is more mature.

Finally, in the media streaming application, we will get a realistic idea of the quality of the video that can be achieved in these UMTS environments.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

13 OVERALL EVALUATION

The more we participate in two-year projects, the more we realise that they are too short-lived. This is partly because of the time it takes for partners to work well together. It is also because only after they have worked together for some time, is one able to profit from the total activity being greater than its parts. In this project great progress was made in the provision of the basic components: routers, network provision, middleware, end-stations and applications. Few were ready for use by other partners by the end of the first year, most only by the middle of the second. Thus the last nine months were a hectic and rewarding activity in integration. The necessary concentration on the last three major demonstrations were immensely useful as forcing functions – but left us all sad that we did not have time to really profit from the individual achievements.

By the end of the project, we had excellent connectivity with each other. Certain of the non-clinical applications – like conferencing, agent technology and streaming were ready for large-scale deployment. The gateways and routers which would allow such deployment in a mixed world were also finally ready – but there was no time for the operational use, which would uncover those extra adjustments which would be needed for excellent services. The clinical applications had reached a surprising maturity, but again each had had to gloss over certain necessary components – security in one case, proper only an *ad hoc* transition mechanism in another, applying the lessons learnt from interference measurements in Poland to the British scene in a third.

There was clearly one vital place where we had failed. The use of UMTS was only a last-minute activity - far too little to draw real conclusions or to understand the impact of that technology on the wealth of components that have been developed. This was not due to any failure by the project partners; it was due to the delay in the availability of any UMTS facilities, because of the financial and technical problems with the whole industry.

We were able to make limited use of GPRS. That technology clearly has its place, but at the present juncture, its place has little to do with 6WINIT. The speed that it offers is too low, and the round-trip times too long, for the applications we wished to address in any case; the constraints in the way that it has been implemented made it almost useless to the project. Delays of months to get at servers, the need to tunnel IPv6/IPv4 and the lack of fixed IP addresses, reduced its usefulness yet further. Finally, deployment and usage costs, while bearable in a research project, may prevent some of the applications in 6WINIT from being commercially deployable..

The project has made a considerable impact on what can be done over the IPv6-enabled wireless Internet. We expect that many of the partners will develop further the activities they have brought to such an interesting stage in existing projects like Moby Dick, 6NET and Euro6IX. Beyond that, it is clear that Framework-6 offers immense potential to finish the job, which we were unable to complete in 6WINIT. Provided only that UMTS really does take off, and that its integration with WLANs is not blocked by deliberate sabotage, 6WINIT has laid an excellent basis for the future.

There is one area where the lack of UMTS has not been a vital factor, and that is the clinical domain. Here it is extremely gratifying how much progress has been made. Some of the components do need UMTS, for instance audio/video in GANS and radiographic images at a distance. In fact institutional and organisational constraints will probably need more time for real clinical deployment than it will take to deploy UMTS widely. However, the collaboration

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

between the clinical and the technical sides has been immensely fruitful; it has galvanised the 6WINIT clinical partners to allow the technology developed to be deployed for real in healthcare.

All in all, a huge amount has been achieved. All of us are looking forward to using and commercialising our results over the next few years.

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

14 ACRONYMS AND ABBREVIATIONS

2G	Second Generation Mobile Telecommunications (including GSM and GPRS technologies)
3DES	Triple Data Encryption Standard
3G	Third Generation Mobile Telecommunications (including WCDMA/UMTS technology)
3GPP	3rd Generation Partnership Project
6WINIT	IPv6 Wireless INternet IniTiative
6to4	Automatic IPv6 in IPv4 tunnelling method, used router-to-router (RFC 3056)
AAA	Authentication, Authorisation and Accounting
ACC	Academic Computer Centre "Cyfronet", a part of the UMM
ACL	Asynchronous Connectionless Links
ACR	American College of Radiologists
ADPCM	Adaptive Differential Pulse Code Modulation
AF	Assured Forwarding
AH	Authentication Header (IPsec)
AIIH	Assignment of IPv4 Addresses to IPv6 Hosts
ALAN	Application Level Active Networking
ALG	Application Layer Gateway
AM_ADDR	Active Member Address
AN	Active Networking
ANP	Anchor Points
AP	Access Point
API	Application Level Interface
AR	Access Routers
AS	Application Server
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
B2BUA	Back-to-Back User Agent
BACK	Binding Acknowledgement
BAKE	Binding Authentication Key Establishment
BD_ADDR	Bluetooth Device Address
BGP	Border Gateway Protocol
BGW	Border Gateway
BNEP	Bluetooth Network Encapsulation Protocol

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

BSR	Bootstrap Router
BSS	Base Station System
BU	Binding Update
CA	Certificate Authority
CAS	Clinical Appointment System
CBR	Committed Bandwidth Rate
CCU	Clinical Care Unit
CEN	Comité Européen de Normalisation
CHIME	Centre for Health Informatics and Multi-professional Education
CHTML	Compact HTML
CLI	(1) Calling Line Identification (2) Command Line Interface
CN	Correspondent Node
COPS	Common Open Policy Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CRL	Certificate Revocation Lists
CRTP	Compressed RTP
CS2	Coding Scheme 2
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSP	Cryptographic Service Provider
CoA	Care-of Address
DAO	Data Access Objects
DCF	Distributed Co-ordination Function
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DIAC	Dedicated Inquiry Access Code
DICOM	Digital Imaging and Communications in Medicine
DMZ	Demilitarised Zone
DNS	Domain Name Server/System
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DSTM	Dual Stack Transition Mechanism
DTI	Dynamic Tunnelling Interface

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

DTMF	Dual-Tone Multi-Frequency
DiffServ	Differentiated Services
DoS	Denial of Service
Dx	6WINIT Deliverable x
ECG	Electrocardiogram/graphy
EEP	Execution Environment for Proxylets
EF	Expedited Forwarding
EHR	Electronic Healthcare Record
EJB	Enterprise JavaBeans Components
EPR	Electronic Patient Record
ESP	Encapsulation Security Payload
ETCP	Extended Transport Control Protocol
ETRI	Electronics and Telecommunications Research Institute
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FHR	Federated Health Record
FHSS	Frequency Hopped Spread Spectrum
FQDN	Fully-Qualified Domain Name
GANS	Guardian ANgel System (UKT-RUS)
GB	Gigabyte (10^9 bytes)
GEK	Group Encryption Key
GGSN	Gateway GPRS Support Node
GIAC	General Inquiry Access Code
GPRS	General Packet Radio Service
GRX	GPRS Roaming Exchange
GSM	Global System for Mobile communications
GSN	GPRS Support Node
GTP	GPRS Tunnelling Protocol
GW	Gateway Routers
HA	Home Agent
HAT	High-quality Audio Tool
HCSS	Health Care Service System
HI	Host Identity
HIP	Host Identity Payload Protocol
HIT	Host Identity Tag
HLP	Host Layer Protocol

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

HLR	Home Location Register
HMIP	Hierarchical Mobile IP
HSCSD	High Speed Circuit Switched Data
HTML	HyperText Mark-up Language
HTTP	HyperText Transfer Protocol
HVCT	High-quality Video Conferencing Tool
ICMP(v6)	Internet Control Message Protocol
ICP	Internet Content Provider
ICU	Intensive Care Unit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Multicast Protocol
IGP	Internet Gateway Protocol
IKE	Internet Key Exchange
IMS	Interactive Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	IP Security Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR	Infra-Red
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Information Society Technologies
ITU	International Telecommunications Union
IntServ	Integrated Services
J2EE	Java 2 Enterprise Edition
J2SE	Java 2 Standard Edition
JDBC	Java Database Connectivity
JNDI	Java Naming and Directory Interface
JPEG	Joint Photographic Experts' Group
JSP	Java Server Pages
Kbit/s	Kilobits per second

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

KLIPS	Kernel IPSec Support
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LI	Lawful Interception
LON	Local Operating Network
MAN	Metropolitan Area Network
MD5	Message Digest 5
MDML	Market Data Mark-up Language
MGW	Media Gateway
MIDI	Musical Instrument Digital Interface
MIP	Mobile Internet Protocol
MIP WG	Mobile IP Working Group
MIPL	Mobile IPv6 for Linux
MLD	Multicast Listener Discovery
MLP	Mobile Location Protocol
MMUSIC	Multiparty Multimedia Session Control
MN	Mobile Node
MSC	Mobile Service Centre
MT	Mobile Terminal
Mbit/s	Megabits per second
NAI	Network Access Identifier
NAPT-PT	Network Address Port Translation - Protocol Translation
NAS	Network Access Server
NAT-PT	Network Address Translation - Protocol Translation
NEMA	National Electrical Manufacturers' Association
NFS	Network File System
NHS	National Health Service (United Kingdom)
NREN	National Research and Education Network
NRN	National Research Network
NTE	Network Text Editor
NetRAAD	Network Radiology Acquisition, Access and Distribution
O&M	Operations and Management
OCSP	Online Certificate Status Protocol
OSGi	Open Services Gateway initiative
PACS	Picture Archiving and Communication System
PAN	Personal Area Networking

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

PCBI	Protocol Control Block Identifier
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDP	Packet Data Protocol
PDR	Per Domain Reservation
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PHB	Per-Hop Behaviour
PHR	Per-Hop Reservation
PIM	Protocol Independent Multicast
PIM-SM	PIM Sparse Mode
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLIM	Presence and Location Instant Messaging
PLMN	Public Land Mobile Network
POP	Point of Presence
PPP	Point-to-Point Protocol
PS	Paging Servers
PSK	Phase Shift Keying
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Access Dial-in User Server
RAN	Radio Access Network
RAS	Remote Access Server
RAT	Robust Audio Tool
RFC	(Internet) Request for Comments
RM	Reflection Manager
RMD	Resource Management in DiffServ
RMI	Remote Method Invocation
RODA	Resource Management in DiffServ On DemAnd
ROHC	Robust Header compression
RP	Rendezvous Point
RQM	RTP Quality Matrix

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSVP	Resource ReSerVation Protocol
RTCP	RTP control protocol
RTP	Real Time Transport Protocol
RTSP	Real Time Streaming Protocol
RTT	Round-Trip Time
RUS	Rechenzentrum Universität Stuttgart
SA	Security Association(s)
SADB	Security Association Database
SAP	Session Announcement Protocol
SASL	Simple Authentication and Security Layer
SCEP	Simple Certificate Enrolment Protocol
SCO	Synchronous Connection Oriented
SCS	(1) Secure Conference Store (2) Service Capability Server
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SDR	Session Directory Tool
SGSN	Serving GSN
SGW	(1) Signalling Gateway (2) Security Gateway
SIIT	Stateless IP/ICMP Translation Algorithm
SIMA	Simultaneous Multi-Access
SIP	Session Initiation Protocol
SMF	Service Management Framework (IBM)
SN	Service Network
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETWORK
SPAR	SDP Parser Applet
SPD	Security Policy Database
SRM	Scalable Reliable Multicast protocol
SRTP	Secure Real Time Transport Protocol
SSH	Secure SHell
SSL	Secure Socket Layer
SecGW	Security Gateway

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	-----	-------------

SoFAR	Southampton Framework for Agent Research
TAG	Transcoding Active Gateway
TB	Tunnel Broker
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TE	Terminal Equipment
TEID	Tunnel Endpoint IDentifier
TEIN	TransEurasia Information Network
TETRA	Trans-European Trunked Radio
TLA	Top Level Aggregator
TLS	Transport Layer Security
TS	Tunnel Server
TTP	Trusted Third Party
ToS	Type of Service
UAC	User Agent Client
UAS	User Agent Server
UCL	University College London
UDP	User Datagram Protocol
UIML	User Interface Markup Language
UKT	Universitätsklinikum Tübingen
UMM	University of Mining and Metallurgy (Krakow, Poland)
UMTS	Univeral Mobile Telecommunications System
UR	User Registries
UTRA	Universal Terrestrial Radio Access
VIC	Video Conference Tool
VJ	Van Jacobsen
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTT	Technical Research Centre of Finland
VoIP	Voice over IP
W3C	World-Wide Web Consortium
WAE	Wireless Application Environment
WAN	Wide Area Network
WAP	Wireless Application Protocol
WBD	Whiteboard (application)
WCDMA	Wideband Code Division Multiple Access

Deliverable 20	Evaluation of the Components, Networks and Services developed in the 6WINIT Project	V.1	6WINIT/0050
----------------	--	------------	--------------------

WDP	Wireless Datagram Protocol
WEP	Wire Equivalent Privacy
WLAN	Wireless Local Area Network
WML	Wireless Mark-up Language
WTA	Wireless Telephony Application
WTLS	Wireless Transport Layer Security
WWW	World-Wide Web
X10	Powerline carrier protocol
XHTML	Extensible Hypertext Mark-up Language
XML	Extensible Markup Language