IST-2000-25153

Deliverable 14

Description and Experience of the Clinical Testbeds

Contractual Date of Delivery to the EC:	30 June 2002
Actual Date of Delivery to the European Commission:	July 2002
Editor(s):	Dr Dipak Kalra (UCL), Dr Aleksander Laurentowski (UMM)
Participant(s):	UCL: Tony Austin, Vivienne Griffith, David Patterson, David Lloyd, David Ingram, Peter Kirstein, Nalini Mahadeo, Richard Priestly, John Andrews, Stephen Hailes UKT: M. Rall, J. Zieger, B. Schaedle, A. Wengert RUS: P. Christ, Y. Liang, J. Scheerer UMM: Krzysztof Zielinski, Jacek Cala, Lukasz Czekierda, Jacek Kosinski, Bartosz Kwolek, Dominik Radziszowski, Pawel Rzepa, Slawomir Zielinski JPII Hospital: Adam Koprowski, Pawel Banys, Roman Rogoz, Marcin Swat
Workpackage:	5 & 9
Title of Deliverable:	Description and Experience of the Clinical Testbeds
Security:	IST
Nature:	R
Version:	Final
Number of pages:	97

Abstract: This deliverable describes the up-to-date technical environment at three clinical testbed demonstrator sites of the 6WINIT Project, including the adapted clinical applications, project components and network transition technologies in use at these sites after 18 months of the Project. It also provides an interim description of early experiences with deployment and usage of these applications, components and technologies, and their clinical service impact.

Keywords: Health informatics, e-health applications, computerised medical records, distributed systems, IPv6, IPv6/IPv4 transition, IP security, Mobile IPv6, wireless networks

Executive Summary

The 6WINIT project aims to validate the introduction of the new mobile wireless internet in Europe. Three clinical sites have been chosen to represent the early marketing targets within the healthcare domain as demonstrator sites:

- John Paul II Hospital, Krakow, Poland
- Eberhard-Karls University, Tübingen, Germany
- Whittington Hospital, London, UK

These sites were chosen partly because they have a longstanding relationship with three of the technical partners in the project (UMM, RUS and UCL respectively), and partly because the applications they proposed were useful tests of the type of services which could be provided well in the mobile environment.

This deliverable builds on the previous two clinical site deliverables:

- Deliverable 3: Specification and needs of the Clinical Testbeds
- Deliverable 7: Description of Implementations of the Clinical Testbeds

It provides an update to Deliverable 7 by incorporating a summary of work accomplished to date at each of the sites, and a more concrete statement of the expected target to be reached by the project conclusion in December 2002. It is therefore a description of work in progress, and not a complete presentation of each of the sites. Much of their initial clinical and organisational background was presented in Deliverable 3 and has not been repeated here.

The deliverable consists of three similarly-structured sections, one describing each site. Each site description in turn comprises:

1. the clinical scenarios to be demonstrated, including the locations, user, devices and kinds of information services to be accessed;

2. a structured analysis of the functional requirements and proposed technical solutions for each site, presented as a set of small tables, one per functional requirement; as an update to Deliverable 7; each requirement now includes a statement of work accomplished, of outstanding issues and of the expected endpoint to be reached;

3. a definitive description and technical status of the clinical applications that have been developed, the extent to which these have been deployed;

4. an early indication of the experiences from the deployment and demonstrations;

5. conclusions and/or an outline of the further plans at each site for the remaining six months of the project, and of the 6WINIT components and technologies that are needed to realise this further demonstration and exploitation.

These final sections are each a first candidate proposal for evolving each site, and the ideas in them will be extended in discussion with the technical partners over the next few weeks.

Table of Contents

1 DESCRIPTION AND EARLY EXPERIENCES OF THE LONDON CLINICAL DEMONSTRATOR

1.1 User Scenarios

The following access scenarios describe the various technical settings in which healthcare staff or patients may need to access electronic health record information via 6WINIT networks. (A fuller description of the London clinical scenario was published in 6WINIT Deliverable 3.)

1.1.1 Roadside emergency access to patient's medical summary

Clinical information requirement The doctor, nurse or ambulance worker needs to review (but not change) the basic medical summary of an accident victim or other emergency care patient, held on the CHIME record server, from any public location including the street. A web-based (WAP) application has now been developed to display this information.

Device and location They will need to view the data on a hand-held device, and may be some kilometres from their own place of work but will not need to roam while connected.

Security The user will need to be authenticated and verified (e.g. via token and PKI), and their connection needs to be secured (i.e. encrypted).

Telecommunications pathway The hand-held device will need connection to a GPRS service, and onward routing to the server at CHIME via UCL Computer Science.

QoS The need here is primarily for reliability of connection. The data are character based and neither performance nor bandwidth is of concern.

Intended demonstration GPRS access has now been demonstrated from test-bed locations in Adastral Park (provided by BT) using 6WINIT CHIME clinical staff in lieu of real users. It is intended later to demonstrate this from Berlin (provided by DTAG). A more forward-looking demonstration is also intended using UMTS facilities at the Ericsson "Kista Ring": CHIME and Ericsson staff (mimicking real emergency clinicians) will access medical summary information using a PDA or mobile phone from within the Kista shopping centre.

1.1.2 Hospital outpatient access to patient's medical summary

Clinical information requirement The cardiologist or nurse specialist needs to add, review or update the basic medical summary of a patient attending a cardiac outpatient clinic, accessing the record server based at CHIME. A web-based (html) application is being developed for this.

Device and location They will need to use the existing networked PC workstations situated in the Whittington hospital. There is no mobility requirement.

Security The user will already be authenticated (by the hospital), and a trustworthy mechanism needs to be established for their user profile to be forwarded with their data request. The connection needs to be secured (i.e. encrypted).

Telecommunications pathway The workstations, connected to a legacy IPv4 network inside the wider ***NHSnet***, will need to access the CHIME IPv6 server via an ***NHSnet*** managed gateway to the public Internet.

QoS The need here is primarily for reliability of connection. The data are character based and neither performance nor bandwidth is of concern.

Intended demonstration It is intended to demonstrate this legacy access actually from the Whittington Hospital, by clinical staff users of equivalent real applications.

1.1.3 Patient access to their medical summary and personal health diary

Clinical information requirement Patients may wish to review their basic medical summary as it is held by their GP or hospital. They may wish to add information about their present symptoms or to record the results of period home monitoring tests. The records will need to be accessed from the CHIME record server, potentially from any public location including the home or place of work. A web-based (WAP) application has now been developed for this.

Device and location For simplicity and in view of the likely availability of such devices, it is proposed that they should view or edit their record using a hand-held device. For the present, it has been agreed that they will not be able to roam while connected but in the longer term such roaming access may be desirable to some classes of citizen.

Security The user will need to be authenticated and verified (e.g. via token and PKI), and their connection needs to be secured (i.e. encrypted).

Telecommunications pathway The hand-held device will need connection to a GPRS service, and onward routing to the server at CHIME via UCL Computer Science.

QoS The need here is primarily for reliability of connection. The data are character based and neither performance nor bandwidth is of concern.

Intended demonstration GPRS access has now been demonstrated from test-bed locations in Adastral Park (provided by BT) using 6WINIT CHIME clinical staff in lieu of real users. It is intended later to demonstrate this from and Berlin (provided by DTAG),

1.1.4 Hospital outpatient access to cardiovascular applications

Clinical information requirement The cardiologist or nurse specialist needs to add, review or update the medical record of a patient attending a cardiac outpatient clinic, accessing the record server based at CHIME. A web-based (html) application has been developed for this.

Device and location They will need to use the existing networked PC workstations situated in the Whittington hospital. There is no mobility requirement.

Security The user will already be authenticated (by the hospital), and a trustworthy mechanism needs to be established for their user profile to be forwarded with their data request. The connection needs to be secured (i.e. encrypted).

Telecommunications pathway The workstations, connected to a legacy IPv4 network inside the wider ***NHSnet***, will need to access the CHIME IPv6 server via an ***NHSnet*** managed gateway to the public Internet.

QoS The need here is primarily for reliability of connection. The data are character based and neither performance nor bandwidth is of concern.

Intended demonstration It is intended to demonstrate this legacy access actually from the Whittington Hospital, by clinical users of equivalent real applications.

1.1.5 Ward (bedside) access to cardiovascular applications

This scenario is identical to 1.1.4 above, except that the clinical staff need to use a tablet-style device to access the same cardiovascular applications at the patient's bedside, connected via WLAN.

Intended demonstration As there is no WLAN provision in the hospital as yet, this access has been simulated using a conventional laptop connected to the WLAN at the UCL Computer Science Department. This is an IPv6 connection, thereby demonstrating a future, rather than legacy technical, scenario for this kind of access.

1.1.6 Access to cardiovascular applications from a patient's home

This scenario is identical to 1.1.4 above, except that the clinical staff need to use a tablet-style device to access the same cardiovascular applications at the patient's bedside, connected via WLAN.

Intended demonstration A secure dial-up connection to the Whittington Hospital communications server will permit the laptop to be logically part of the Hospital Intranet

1.1.7 Hospital outpatient access to cardiovascular investigation results

This scenario is still being considered, and would involve extending the scope of the cardiovascular applications to include multimedia investigation results such as ECG and Doppler ultrasound studies. This scenario is more complex, because the original data will reside inside the hospital, and is not presently available in the form of anonymised records that could be used in a demonstration. The main benefit of this scenario would be to challenge the technical architecture from the bandwidth perspective. This challenge is at the heart of another 6WINIT demonstrator site in Tübingen.

1.2 Description of Deployed Technologies and Components

This section draws mainly on the Technical Component Descriptions section of D7, enhancing them with up-to-date descriptions of work accomplished and the status anticipated at the end of the project. However, the section also refers to previously published material in 6WINIT Deliverables 1, 2, 8, 9 and 10. References given to technical descriptions in these deliverables use the notation style [D1 Section x.y.z].

1.2.1 IPv6 Transition Mechanisms

1.2.1.1 **Tunnelling**
Functional Requirement Native IPv6 services from the main application server need to be tunnelled via IPv4 from CHIME (north London) to Computer Science (central London) using UCL's main University Intranet. Additional tunnel(s) may be required for remote connectivity to other IPv6 islands via UK6X and 6BONE.
Proposed Technical Solution: 6WIND IP Edge Device The 6WIND IP Edge Device implements the v4-v6 migration mechanisms over a dual stack entirely developed by 6WIND. Several types of tunnels are available, especially 6in4, 4in6 and 6to4. This dual stack also integrates IPv6 features such as DiffServ and IPSec. [D1 Section 6.5.2.3, D2 Section 2.2.1, D9 Section 2.2.2]
Work Accomplished One Edge device has been configured and installed at CHIME, and another at UCL Computer Science. Satisfactory external IPv6 connection has been verified from Adastral Park during the 2002 Technical Review, and from Washington DC during INET 2002.
Anticipated Endpoint Reached
Outstanding Issues - none
Industrial Benefit This installation provides proof of concept validation of the IPv6/4 tunnelling mechanisms within the Edge Device.

1.2.1.2 **Translation**
Functional Requirement a) IPv6 to 4 translation may be required to permit hand-held (PDA) access to the native IPv6 services via GPRS. b) Some scenarios involve users having access to the native IPv6 services using IPv4 clients from within IPv4 networks (e.g. from inside a hospital Intranet, accessed via an NHSnet managed gateway to the public Internet).
Proposed Technical Solution: a) BT Ultima b) 6WIND IP Edge Device a) Ultima is a BTexact Technologies IP product that provides interworking between IPv4 and IPv6. NAT-PT (Network Address Translator - Protocol Translator) provides a translation facility between IPv4 and IPv6. Translation is bi-directional (i.e. can be initiated at either IPv6 or IPv4 host) without any modifications to either the IPv4 or the IPv6 host protocol stacks, and the operation of the translator is totally transparent to the end user. Translation is initiated via the initial DNS exchange; this requires the addition of a special DNS translator (DNS ALG) to the standard NAT-PT packet translation process. [D2 Section 2.5, D9 Section 2.6] b) The dual stack in the Edge Device should soon include a translation mechanism that allocates a temporary IPv4 address to a dual stack host in the IPv6 network, when it is required for IPv4 communication. IPv4 user devices will access clinical applications via this temporary IPv4 address, rather than the IPv6 address of the main clinical server. [D2 Section 2.1.1]
Work Accomplished None
Anticipated Endpoint Still to be confirmed; a possible demonstration at IST2002 is under discussion
Outstanding Issues None
Industrial Benefit This installation provides proof of concept validation of the translation mechanisms within the 6WIND Edge Device and BT Ultima.

1.2.2 Security Mechanisms

1.2.2.1 **VPNs using IP Routers**
Functional Requirement To provide an encrypted channel of communication between the clinical applications server and the end-user (possibly including the use of wireless devices). Certificate-based key management also needs to be implemented e.g. via PKI. [D10 Section 4.1]
Proposed Technical Solution: 6WIND IP Edge Device 6WIND routers are able to create IPsec tunnels over IPv6 connections, including also the possibility of being certified by a PKI. [D8 Section 3.1.1, D10 Section 4.2] The 6WIND IP Edge Device supports IPSec and IKE functionality compliant with the corresponding RFCs. Different configurations can be accommodated: IPSec with static keys; IPSec with IKE pre-shared keys; IPSec with IKE certificates. All the security features proposed in the IP Edge Device are available for the both IPv4 and IPv6 versions with similar management interfaces. [D2 Section 3.2.1] Because IPSec VPNs are complex to configure, 6WIND provides a management tool called Network Management System (NMS). [D1 Section 6.1.1, D2 Section 3.2.1.2] 6WIND provides a tool to produce and manage certificates. This tool could be sufficient for small or medium configurations. [D2 Section 3.2.1.3] UCL-CS also has experience of using the Public Key Infrastructure of the University of Murcia, based on the design and implementation of a complete and robust group of IPv6-enabled certification services. The interoperation of this PKI with the 6WIND Edge Device will also be explored. [D10 Section 4.1.3] The key management methodology for the demonstrator will be decided later, balancing the practical needs to provide a small and stable number of certificates with the wish to demonstrate a realistic and scalable scenario. A VPN will be established between CHIME and UCL Computer Science, to users connected via fixed LAN and WLAN. Ideally the VPN will extend to remote users connected via the Internet both using a fixed address and using GPRS.
Work Accomplished The CHIME clinical applications have been adapted to communicate with a certificate server at UCL-CS (developed by University of Murcia), subject to final testing. This is part of - but not a complete - VPN solution and further work to extend the configuration is in progress.
Anticipated Endpoint Working VPN configuration
Outstanding Issues How to establish a VPN through to fixed and mobile users using native IPv4 devices connected via the public Internet (and possibly GPRS).
Industrial Benefit Proof of concept verification of the Edge Device IPSec functionality and demonstration of a secure infrastructure for future adoption by regional health care networks.

1.2.2.2 Road Warrior
Functional Requirement To provide an authenticated and encrypted channel of communication between the clinical applications server and the end-user specifically supporting the use of mobile devices connected via GPRS or UMTS. Although PKI certificate-based security will be needed in real deployment situations, authentication using a pre-exchanged (public) RSA key would be the preferred method for a demonstration.
Proposed Technical Solution: IABG in partnership with 6WIND IABG and 6WIND will collaborate to validate a mechanism to support the authentication and certificate/key management approach for mobile users whose IP address is allocated only at the time of connection. [D8 Section 3.2]
Work Accomplished The Road Warrior has been installed and configured to provide a VPN using IPsec, using a Linux server and the 6WIND Edge Device.
Anticipated Endpoint Reached
Outstanding Issues - none
Industrial Benefit The collaboration will verify a technical approach that could inform IETF on potential modifications to IPSec to support Mobile IP. Component interoperability between IABG and 6WIND might lead to other future collaborations.

1.2.2.3 Firewall

Functional Requirement

The CHIME-hosted clinical applications server (running SuSe Linux 7.2) needs to be protected from hostile attack including unauthorised access and denial of service attack.

Proposed Technical Solution: 6WIND IP Edge Device

The 6WIND IPSec VPN will limit access to authorised users and from known IP addresses (the Mobile IP scenario is a specific exception, to be protected separately). This will provide firewall protection by way of packet filtering.

The 6WIND Edge Device provides IPv4 and IPv6 Packet Filtering mechanisms that have been recently implemented and that are available in version 4.1. This Firewall functionality is used to protect local networks when they are interconnected with non-secure networks, like Internet. [D10 Section 4.3.1]

Work Accomplished

This has yet to be configured

Anticipated Endpoint

Configured and verified firewall

Outstanding Issues

Mobile IP security measures will need to be managed separately

Industrial Benefit

This feature is an important “by-product” of the VPN, as a demonstrated security solution for regional health networks.

1.2.3 Mobile IPv6

1.2.3.1 **MIPv6 Home Agent**
Functional Requirement Users need to be able to reliably connect to the clinical applications server from a mobile (non-roaming) device whose Care of (IP) Address is dynamically provided by an ISP or other foreign network. [D8 Section 2, D10 Section 2.2.1]
Proposed Technical Solution: 6WIND IP Edge Device A native IPv6 mobility is included in a prototype of the IP Edge Device, though this function is not currently included in commercial version of the IP Edge Device. The “Home Agent” functionality is implemented according to the IETF draft [Joh01]. Like the implementation of other providers, all the aspects have not yet been taken into account mainly because they are not well defined at the moment. [D2 Section 4.1.1, D2 Section 4.2.1, D1 Section 7.3, D8 Section 2.2.3, D10 Section 2.3.4]. The practical demonstration of this will be considered later in the project. UCL-CS is also prototyping Helsinki University’s mobile IPv6 stack implementation (http://ww.mipl.mediapoli.com) on the mobile hosts, since this is widely believed to be amongst the most progressive work on mobile IPv6 stacks. [D8 Section 2.2.1]
Work Accomplished Initial tests have been conducted at UCL-CS, but the use of the iPAQ for MIP testing requires further device drivers for Linux or an IPv6 stack for WindowsCE.
Anticipated Endpoint To be confirmed
Outstanding Issues This function is work in progress; see note about drivers above
Industrial Benefit 6WIND will study how to add security over the mobility and will see if the privileged location at the boundary of the network can be exploited by the Edge Device to solve the problem of security and mobility. [D2 Section 4.2.2.1]

1.2.3.2 **802.11b Access**
Functional Requirement Users need to be able to reliably connect to the clinical applications server from a wireless LAN, using a laptop, hand-held or tablet device.
Proposed Technical Solution: 6WIND IP Edge Device The 6WIND IP Edge Device can be used at the border between wired and wireless networks. WLAN technology like 802.11b has been tested and proved to be compatible with IPV6 networks…. The Aironet kit from Cisco has been used in the preliminary experiments. [D2 Section 4.2.1.2] The deployment of the Edge Device to enable WLAN users to access the CHIME clinical applications will build on early work carried out at UCL in the ANDROID project.
Work Accomplished This has been configured, and tested at UCL Computer Science and from Adastral Park at the 2002 Technical Review, and demonstrated at INET2002 in Washington
Anticipated Endpoint Reached
Outstanding Issues None
Industrial Benefit To verify that the 6WIND IP Edge Device is suitable to act as a wireless gateway (D2 Section 4.2.2.2]. 6WIND also wish to verify their 802.11b solution with Lucent WLAN.

1.2.3.3 **GPRS**
Functional Requirement Users need to be able to connect to the clinical applications server reliably from a mobile (non-roaming) hand-held device. This will include the need for wireless access via GPRS.
Proposed Technical Solution: 6WIND IP Edge Device This is very new (emerging) functionality within the 6WIND Device, and its demonstration will be confirmed later in the project. [D1 Section 4.1.2.2, D2 Section 4.2.1.2] It will ideally be verified eventually at the 6WINIT partner GPRS test-beds in Ipswich and London and Berlin.
Work Accomplished This has been configured, and tested at Adastral Park at the 2002 Technical Review
Anticipated Endpoint Reached
Outstanding Issues
Industrial Benefit One of the main objectives for 6WIND in the scope of the 6WINIT project is to integrate in the IP Edge Device new wireless interfaces like GPRS and UMTS for the WAN side… [D2 Section 4.2.2.2]

1.2.4 QoS

1.2.4.1 TAG

Not required at this site

1.2.4.2 JMF

Not required at this site

1.2.4.3 DiffServ

Functional Requirement

The proposed London user scenarios place only a limited demand for QoS functionality, primarily for reliability. However, future planned clinical applications will include the use of multimedia data requiring high bandwidth and high performance capability, so an opportunity to test this could be engineered.

Proposed Technical Solution: 6WIND IP Edge Device

The 6WIND IP Edge Device implements the standard mechanisms and is compliant with RFC 2475 *"Architecture for Differentiated Services"*. It implements flow classification, queues management and scheduling mechanisms. All the QoS mechanisms of the Edge Device can be applied on the two versions of IP, IPv6 and IPv4. [D1 Section 2.2.1, D2 Section 5.2, D10 Section 5.1, D10 Section 5.1.2]

The 6WIND Edge Device implementation of DiffServ allows interoperability with IPSEC/IKE functions and Migration mechanisms (tunnels) also provided by this equipment. [D10 Section 5.1.2.3]

Plans for exploiting this in the demonstrator will be considered later.

Work Accomplished

Not tackled

Anticipated Endpoint

Probably not to be demonstrated at the London site

Outstanding Issues – none

Industrial Benefit

To be confirmed

1.2.5 Signalling Gateways – SIP

1.2.5.1 SIP

Not required at this site

1.2.6 Multimedia Conferencing Gateways

1.2.6.1 Multimedia Conferencing Gateways

Not required at this site

1.2.7 WAP Gateways

1.2.7.1 **WAP Gateways**

Functional Requirement

There is considerable attraction to making a patient's medical summary available to the patient using a WAP phone or a PDA using a WAP connection, since this is present-day and widely-available technology. However, there may be secondary benefit in showing the advantage of Mobile IP as a successor to WAP if both options are capable of demonstration.

Proposed Technical Solution – to be confirmed

During clinical application development at CHIME a commercial ISP will be used as the WAP provider to enable rapid testing of the basic screen design and to establish performance.

An independent WAP gateway has been recommended by the 6WINIT partners [in D2 Section 8.5] as a means of enhancing security (many commercial WAP providers cache customer WML pages for some days before deletion, which may not be secure). The Krakow (Poland) site has indicated an intention to pursue a secure WAP solution, and their experience will be sought before confirming the approach of the London site.

Work Accomplished

None

Anticipated Endpoint

This might not be in scope for 6WINIT as WAP is not an IPv6 technology

Outstanding Issues

Unknown as yet

Industrial Benefit

None identified

1.2.8 Access Network Provision

1.2.8.1 **GPRS**
<u>Functional Requirement</u> Wireless GPRS network access is required to demonstrate the "roadside" access to clinical applications. In practice this will be simulated from GPRS test-bed locations.
<u>Proposed Technical Solution</u> 1) The BT GPRS test-bed located at Ipswich and London (UK) 2) The DTAG GPRS test-bed located at Berlin (Germany) Additional test locations might become available towards the end of the project. However, the above sites will be sufficient to provide proof-of-concept verification.
<u>Work Accomplished</u> This has still to be tested
<u>Anticipated Endpoint</u> Demonstration of GPRS connection from London and from IST 2002 (Copenhagen)
<u>Outstanding Issues</u> The availability of GPRS cards ("mobile modems") for each client and drivers for each operating system. NOTE: iPAQ drivers are now available for WindowsCE which does not have an IPv6 stack in the standard release; however they are available in an experimental release. Drivers are not yet available for Linux.
<u>Industrial Benefit</u> Demonstration of the value of GPRS for the rapid and reliable retrieval of health information via wireless, to help stimulate a health care market for such solutions.

1.2.8.2 **WLAN**
Functional Requirement Wireless (WLAN) network access is required to demonstrate the "bedside" access to clinical applications. Although IPv4 WLAN is becoming prevalent now, in the future this is likely to be IPv6. In 6WINIT this kind of access will be simulated from the IPv6 WLAN network at UCL Computer Science.
Proposed Technical Solution The Lucent Orinoco Wireless LAN and Cisco's Aironet WLAN architectures are described in D1 Section 5.1. The Wireless 802.11b LAN operational at UCL Computer Science will be the primary test location for the London demonstrator. Secondary connection to other islands of wireless access at other partner sites may be attempted later, possibly utilising 6BONE (see below) or 6NET.
Work Accomplished Demonstrated from UCL Computer Science and at the 2002 Technical Review at Adastral Park
Anticipated Endpoint Reached
Outstanding Issues – none
Industrial Benefit Demonstration of an IPv6 wireless methodology suitable for use inside hospitals in the vicinity of medical devices.

1.2.8.3 **IPv4 WANs**
<u>Functional Requirement</u> IPv4 WAN is required to demonstrate hospital-based access to the IPv6 clinical applications using legacy networks. In practice this will be routed from UCL Computer Science to the Public Internet, and accessed from inside ***NHSnet*** via a managed firewall.
<u>Proposed Technical Solution</u> Clinical application web services routed from CHIME via UCL Computer Science and the JANET national academic network to the Internet and the ***NHSnet***. 6WIND translation mechanisms have been described above. Security provisions described above might not be fully implementable when using IPv6to4 translation.
<u>Work Accomplished</u> Demonstrated from UCL Computer Science
<u>Anticipated Endpoint</u> Reached
<u>Outstanding Issues</u> - none
<u>Industrial Benefit</u> Demonstration of a viable migration approach, and of rigorous IP translation mechanisms.

1.2.8.4 **IPv6 WANs**
<u>Functional Requirement</u> Native IPv6 distributed access is required to validate the future scenario of widely available IPv6 networks within hospitals. In practice this will be demonstrated within UCL Computer Science using local IPv6 networks, and from fixed connections at other clinical sites such as RUS (Stuttgart), via 6BONE.
<u>Proposed Technical Solution</u> The UCL IPv6 LAN is well-established, and is connected to the UCL Intranet. With the use of 6WIND IP Edge Devices (described in earlier sections of this report) the CHIME and Computer Science IPv6 islands will be connected through an IPv4 tunnel. This will be in turn connected to the IPv6 LAN at RUS in Germany, via 6BONE. This tunnelled interconnection of IPv6 islands will simulate a homogenous IPv6 WAN.
<u>Work Accomplished</u> Demonstrated from UCL Computer Science and at the 2002 Technical Review at Adastral Park
<u>Anticipated Endpoint</u> Reached
<u>Outstanding Issues</u> – none
<u>Industrial Benefit</u> Demonstration of a migration solution that would permit distributed organisations to upgrade their sites to IPv6 without loss of organisation-wide connectivity.

1.2.8.5 **UMTS**
Functional Requirement Wireless UMTS network access is required to demonstrate the next-generation "roadside" access to clinical applications. In practice this will be simulated from a UMTS test-bed location.
Proposed Technical Solution: Ericsson "Kista Ring" The routing of network traffic via 6BONE described above can be extended to include the UMTS test-bed near Stockholm (Sweden).
Work Accomplished Still to be tested
Anticipated Endpoint Demonstration at the 2003 Technical Review
Outstanding Issues To be identified later
Industrial Benefit Provide proof-of-concept verification of UMTS access to web-based application services, as market stimulation. Ideally the demonstration will highlight the benefits of UMTS over GPRS.

1.2.9 Access Devices

1.2.9.1 **Terminals**
Functional Requirement The various London user scenarios require four different user access devices. 1) an IPv4 desktop workstation, running a web browser 2) an IPv6 desktop workstation, running a web browser 3) a laptop simulating a tablet client, running a web browser 3) a hand-held device, such as a PDA, running a web browser (both IPv4 and IPv6 versions)
Proposed Technical Solutions Compaq iPAQ: running Linux, IPv4/IPv6 and a web/WAP browser, with a wireless GPRS connection (or UMTS, in Stockholm) or a Wireless LAN connection. Laptops: running Linux or other operating systems, IPv6, with fixed Ethernet or Wireless LAN connection. PC: various platforms, running IPv4 or IPv6 or dual stack, a browser, with connection either to IPv6 LAN or IPv4 LAN within a legacy environment. All the mobile devices (iPAQ and laptop) will require a mobile IPv6 stack. Currently development is being done by the 6WINIT partners with the University of Helsinki's Mobile IPv6 stack (HUT) which is explored in Deliverable 10. The basic functions have been used with both laptops and iPAQs.
Work Accomplished Demonstrated from UCL Computer Science and at the 2002 Technical Review at Adastral Park without IPSec Demonstrated from INET 2002 (Washington DC) using laptops with IPSec
Anticipated Endpoint Reached
Outstanding Issues IPv6 operating systems and browsers supporting IPSec are not yet available for all devices.
Industrial Benefit A spectrum of devices is important to show the compatibility of 6WINIT solutions with a wide range of user needs.

1.2.9.2 **Security Devices**
Functional Requirement The ideal requirements are for strong authentication and user certification (including access control role-based profiles). A comprehensive security solution would add credibility to the overall 6WINIT technical architecture.
Proposed Technical Solution: PKIs and Smart Cards Certificate handling has been described above. Coupling the proposed architecture with strong authentication tools (e.g. using tokens or biometric devices) would be ideal.
Work Accomplished Not yet tackled
Anticipated Endpoint Still to be confirmed
Outstanding Issues This may add an unnecessary complexity to the demonstrator
Industrial Benefit This needs to be confirmed, since the demonstration of these security tools themselves is not the focus of 6WINIT.

1.2.10 Location Awareness

1.2.10.1 **Location Awareness**
Not required at this site

1.3 Clinical Applications

The primary CHIME clinical application services are a set of middleware components providing controlled access to patient electronic healthcare records (EHRs). Access to these EHRs is provided through a set of web-based applications, each written as Java Servlet scripts executing on the same server as the middleware components. The persistent repositories are themselves distributed within a local area network and accessed by the middleware components using Jini. This overall component architecture has been described in 6WINIT Deliverable 3. The technical configuration of the main server running these components, and serving them via IPv6, is summarised below in Section 1.3.2.

Three sets of clinical web applications have been developed:

1. medical summary for hospital care (web browser version)

2a. medical summary for emergency care (PDA version)

2b. medical summary and personal diary for patient use (PDA version similar to 2a above)

3. outpatient clinic application for chest pain and heart failure management (web browser version).

Each of these applications is summarised below in Section 1.3.1, and illustrated using screen captures from the near-final version of these applications. However, these screen captures have been taken from a developmental version of the application and depict experimental data values that are not intended to reflect realistic clinical examples. The application set has been collectively known as the Chest Pain application, as its intended initial use within the demonstrator is for a new Rapid Access Chest Pain Clinic (RACPC) at the Whittington Hospital. These applications focus on the collection and presentation of health record information, and are not intended to act as an internal departmental system to manage clinic sessions, human or other material resources. The focus of these applications is the support of clinical interactions with the patient’s record in an electronic form, for which secure distributed access is of clinical value.

Some elements of the cardiovascular record are being designed in parallel with General Electric / Marquette, relating to the capture of multi-media investigations and will be developed during 2002/03.

1.3.1 Definitive technical status of clinical applications

1.3.1.1 Login screen

Because the system is a web application, it is ‘invoked’ simply by pointing a web browser at an appropriate server. Although the screens here are using Internet Explorer, there is no dependency on this browser and Netscape is in active use within the department. Little use is made of JavaScript or stylesheets to ensure that the maximum number of browser types may function.

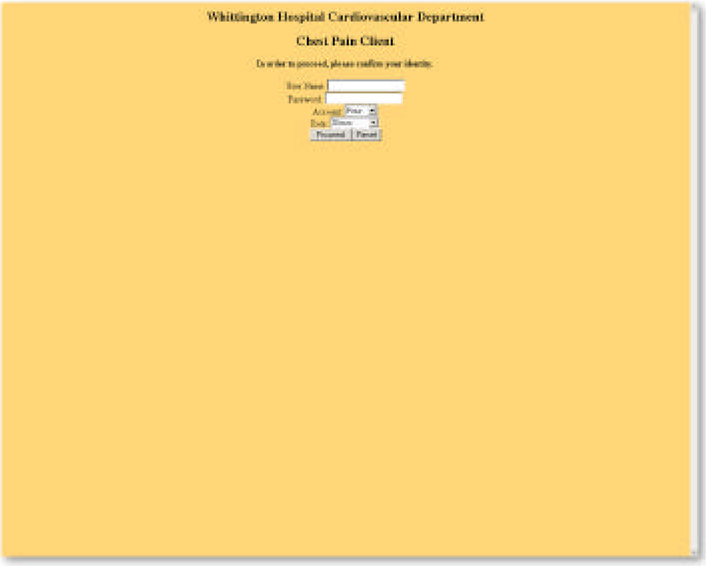

Figure 1: The Chest Pain login screen

A password is required to protect the access to the patient records (

Figure 1). The accounts are the organisational contexts contained within the global patient context specified therein. These are represented within Novell Directory Service (NDS) and contain the patient details specific to that account.

This login process has recently been updated to refer to a PKI server at UCL-CS (developed in partnership with University of Murcia) to establish a valid user session.

1.3.1.2 Welcome screen

Figure 2: The Chest Pain welcome screen

Once successfully authenticated, the user will be given the opportunity to search for patients. Patient searches can be conducted on the basis of surname, date of birth, postcode or on the patient’s NHS number. In the case of a surname search, a wildcard may be used (‘*’) to match multiple entries. Just entering ‘*’ will return the whole patient database as in Figure 2. There is a button on this screen enabling a record for a new patient to be created.

1.3.1.3 Patient Search

The result of a complete patient search is shown in Figure 3. This is the set of patients associated with the same account as the logged in user. In this way, patient confidentiality is preserved since users who do not have clinical interactions with a given patient are unable to see their details. If in fact a patient is seen legitimately by users in two accounts, it is possible to provide an alias in the directory service so that the patient appears to be in both accounts, but does not have duplicated data (which would have to be separately managed).

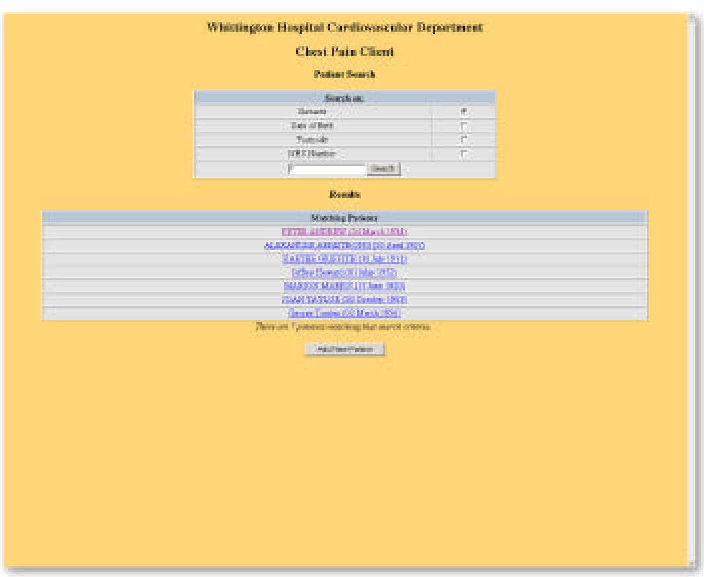

Figure 3: The Chest Pain patient search result screen

From the patient search screen, a new search can be launched, or a record for a new patient can be added. If the patient is already in the database, a simple click on the hyperlink associated with their name will go straight to that patient's record.

The patients included here are not real individuals, but pseudonymous patients for demonstration purposes. A considerable amount of legacy data from a previous system at the hospital has accumulated over a decade, and this has been mapped into the data structure used by this new application. It will shortly be migrated across and made available to support the ongoing care of those patients.

1.3.1.4 Demographic screen

Figure 4 shows the demographics screen for the chest pain application. If we were creating the record for a new patient, the details here would be blank text fields so that data could be added anew. Since we have in fact selected an existing patient, the fields are simply filled in from the NDS details presently held for the patient.

Should the user choose to, there is a button at the bottom of the screen enabling him to edit the patient demographics. Clicking this will refresh the screen with editable fields enabling him to make the appropriate changes.

Figure 4: The Chest Pain demographics screen

Because some of these fields are complex, and require significant attention to detail, it is too great an inconvenience to lose the entire set of entered data if a button is mispressed. For this reason all actions must be confirmed twice, *including cancel*. From a completed screen, OK may be pressed. The OK may itself be OK'd (resulting in a commit) or cancelled (resulting in a return to the editing state). Cancel may be pressed, which itself can either be cancelled (returning to the editing state), or OK'd (resulting in a return to the original state before editing was invoked). Reset at all times clears the fields in the form so that they don't each have to be highlighted and removed individually.

1.3.1.5 The Medical Summary screen

Referring once again to Figure 4, we notice that across the top of the demographics screen are the links taking us to the various elements of the chest pain application. The first of these, and the most complex, is the medical summary screen (Figure 5).

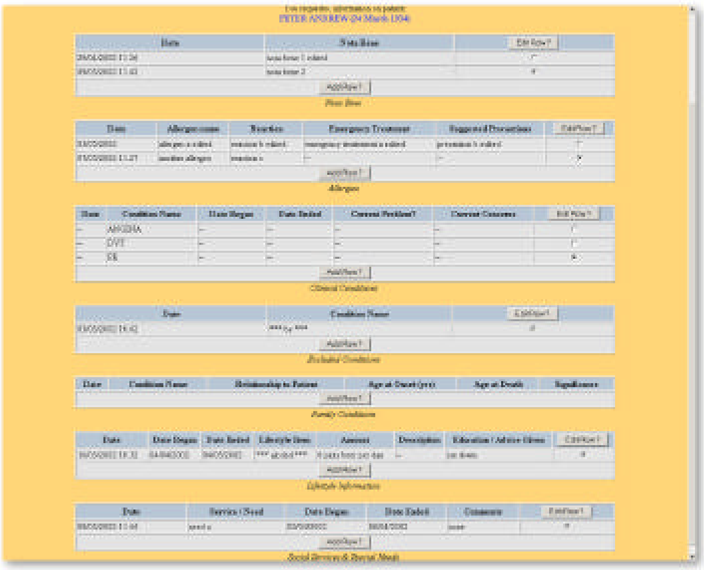

Figure 5: The Chest Pain medical summary screen

This informative screen contains several tables describing key aspects of the patient's medical state. All the tables offer the ability to edit an individual row (with a formal revision process) or to add a new entry (which becomes a new row in the table). The tables are sorted on the date added in descending order (most recent at the top) unless described otherwise below. Many of these summary tables have a fairly comprehensive set of columns, which may not be filled in on every occasion.

In each individual table, {Add Row} will add a new entry in the table. The screen will be refreshed with a new set of blank fields at the base of the table. These can be filled in as desired, then OK'd twice as described above.

To edit a row, select the row to be edited using the radio buttons in the table, and press {Edit Row}. The table will then be refreshed with the fields editable and ready to change. Cancel followed by OK will indicate to the application that no change should be enacted after all.

Please note that at this point no other tables can be edited - only one table can be changed at one time, to ensure that committed data is kept consistent with the requirements of any dependent programs.

Nota Bene

This is a set of dated text boxes for critical information that any clinician should know when they see the patient. This section could include patient wishes for things like resuscitation policy.

Clinical Conditions

Although a drop-down box will initially limit this table to cardiac conditions, the wider use of the record server may in the long-term mean that other disciplines share this part of the record. A whole person perspective has therefore been retained, but with a focus on cardiology for this clinic. If the diagnosis changes over time as more information about patient emerges, the user will have two options:

- to revise the original entry if it now appears to be inappropriate (the original entry will be hidden, but retained in the audit trail); or
- to edit the entry and give it an end date with a comment stating that the condition has evolved, and to create a new entry with the new diagnosis.

Excluded Conditions

There is little point in offering a rich data set for excluded conditions. Clearly though, it must be possible to delete entries (noting this still forms part of the revision process) if the condition subsequently occurs!

Lifestyle information

The benefit of this table is the consolidated and flexible approach to capturing any kind of lifestyle information. However this flexibility within one table means that the amounts are completed as free text rather than as computable quantities.

1.3.1.6 The Review screens

The next three links across the top of the window (Figure 6-Figure 8) provide further components of the patient's medical summary that might in the future be shared by several departments within the hospital.

The first application specific screen is the medication and prescriptions screen, which shows the current drugs that the patient is taking. All three review screens work in exactly the same way as the tables on the medical summary screen.

There is an additional facility to generate mail merge text from this screen. This will include basic patient demographic information and current medication in a structured file that can form the data source for a mail merge application such as a word processor. This is intended to permit locally defined prescribing stationery to be automatically completed ready for printing and signature, if local policies permit this.

Figure 6: The Chest Pain medications and prescriptions screen

Figure 7: The Chest Pain investigation results screen

Figure 8: The Chest Pain education and self management screen

1.3.1.7 Cardiovascular service referral

The next screen works in a slightly different way to the previous vertical tables we have seen. There are two elements to this screen, one for referrals into the clinic, and one for DNAs (occasions when the patient Did Not Attend). The former is required to capture the management of the referral process itself, and is required for statutory reports on performance of the new National Service Framework and for the hospital's own service audit. The latter provides the staff with a means to record their actions following the non-attendance of a patient, for medico-legal purposes.

Figure 9: The cardiovascular service referral screen

It can clearly be seen now, that the lower table for the DNA cases is as we have seen before where the data set is presented and the user simply clicks {Add Row} to provide a new case.

However the top table has rather too large a data set to fit comfortably in a horizontal table. In addition, only a few referrals might be expected for a patient. So in order to avoid the need to scroll right and left, especially on a screen of low resolution, we have provided an alternative where the data is available in a column rather than a row. In Figure 6 we can see an entry that has already been added. In the normal way, if we click {Edit this one} we will get a set of editable fields with the current values pre-filled so that they can be changed. {Add New Referral} will give us simply a set of blank fields.

However what differs is the presence of the “Previous / Next” and number links at the base of the table. We now have the facility to move back and forth through the referrals using these links, either sequentially or directly to a particular referral (such as the first).

1.3.1.8 Cardiovascular Presentation

This screen captures the main features of a patient’s symptoms and cardiovascular history that are specific to the management of their chest pain or heart failure. The columnar layout has also been used here (Figure 10), with the facility to move back and forth through the entered items using the links at the bottom of the table. In this case the table contains so much potential information that it is itself grouped into logical areas.

Figure 10: The Chest Pain Cardiovascular presentation screen

The large text entry boxes are intended to provide the user with an open environment to record positive or important features of the symptoms. We have presently avoided introducing a specific set of boxes separately to capture chest pain location, radiation, duration, severity, precipitating or aggravating factors such as exertion or eating, relieving factors such as the use of glyceryl trinitrate etc. In general, templates take longer to complete and make the screens look busy, and should be used when most items will have an important value (e.g. the examination screen below). It has also been found that highly structured presentation formats take longer to review than short narrative remarks. The users were specifically involved in these decisions and confirmed their preference for a small number of medium-sized text boxes. They also understood that such narrative is less suitable for subsequent fine-grained analysis for audit purposes.

1.3.1.9 Cardiovascular Examination

One further innovation is introduced in this screen, where the top Cardiovascular Examination table is both too large to use a row based structure, and yet previous readings are convenient to be able to see. In this case, although the mechanics of addition and editing remain the same, four readings are shown. They are, from left to right, the most recent reading, the previous two readings, and the very first reading recorded (ever). Since multiple readings are included in this table, there are no “Previous / Next” navigation links.

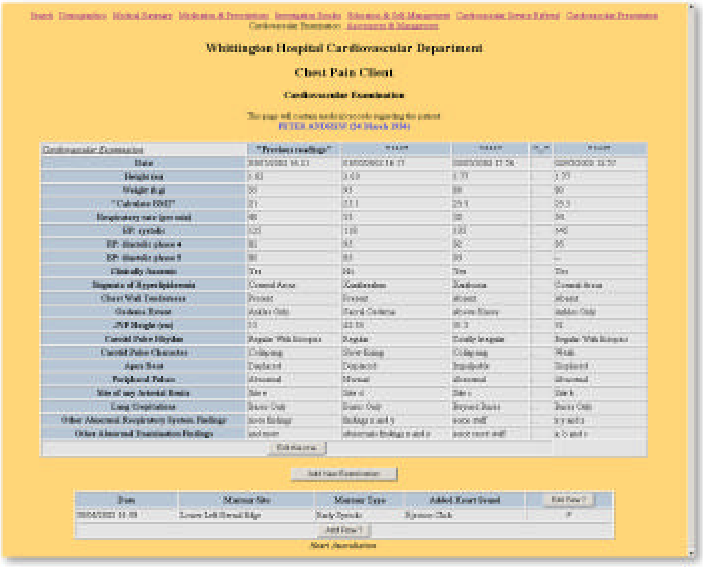

Figure 11: The Chest Pain cardiovascular examination screen

The Heart Auscultation table permits the recording of more than one murmur or added heart sound, to show the global history of these recordings. This ensures changes or new sounds are recognised as such.

1.3.1.10 Assessment and Management

The final screen (Figure 12) concludes a clinical encounter by recording what assessments have been performed, what the patient has been told and how the author proposes that future care should be managed. This screen is also expected to serve as the primary resource for communication to the referring GP and to support future shared care. Any planned tests are recorded here in the lower part of the screen: once these have been performed and reported they will be deleted from this table and added to the Completed Tests table described earlier.

Figure 12: The Chest Pain assessment and management screen

Figure 13 shows this screen with new data. The large text boxes serve as an indicator to the clinical staff that it was envisaged that they might wish to enter a narrative sentence or paragraph.

Figure 13: Editing in the Chest Pain assessment and management screen

1.3.1.11 Medical summary for emergency care (PDA version)

In addition to the web browser application described above, we have developed a cut down, largely read-only, pair of applications that can be run from a handheld device. These are a clinician-focussed emergency summary application and a patient-focussed summary with a home-monitoring diary application.

Although nominally these applications are both WAP applications and can therefore be run from a suitably equipped Personal Digital Assistant or from a mobile telephone we have made no assumptions about the memory requirement of the downloaded data, since this might be considerable for a long-term patient. It is likely therefore that a PDA will be the optimum display device for the foreseeable future since it is likely to have an appropriate amount of memory. As telephones become more sophisticated, this may change especially as the new 3G mobile networks place greater demands on the technology. In any case, as will be seen, by and large there are no excessively telephone-unfriendly aspects to the display.

1.3.1.12 Login screen

The PDA equivalent login screen is given in Figure 14. We are displaying these screens using the Klondike WAP browser, as this seems to be presently the one that is able to show the greatest number of features that we have implemented. However, there are many WAP browsers in existence, WAP being a relatively low cost-of-entry environment to join. Each browser has strengths and weaknesses.

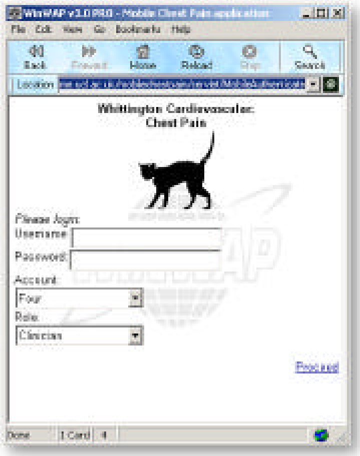

Figure 14: The Mobile Chest Pain PDA login screen

As for the web application, a username and password are required. The accounts are generated from the organisational contexts in the NDS tree as before, however here there are only two roles provided, clinician and patient. It is presumed that if a clinician has rights to login to this read only environment then they have rights to see all the data contained therein.

1.3.1.13 Patient Search

The result of a patient search takes the user to a differently structured patient home page (the root of their “PDA summary record”) depending on their role (patient or clinician). However, in the case of the patient role this will not first require an explicit patient search to be carried out (since the search will be done silently for the patient that has logged in). Figure 15 shows the PDA equivalent patient search screen, and Figure 16 shows the results set. At this point the applications are very similar to their web-based equivalents.

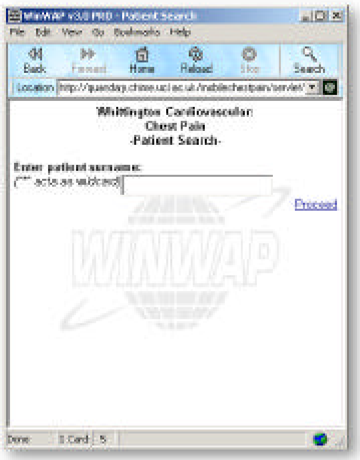

Figure 15: The Mobile Chest Pain patient search screen

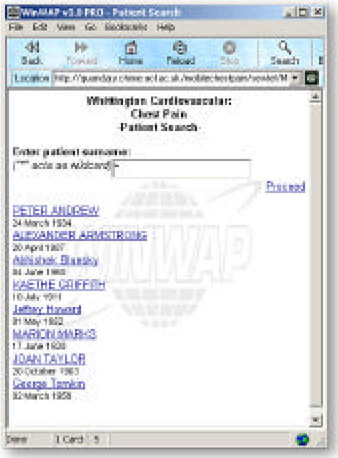

Figure 16: The results of a Mobile Chest Pain patient search

1.3.1.14 The EHR Summary

The EHR Summary screen (Figure 17) provides links to the key data provided in the read only application. In other screens obtained from here, the [Patient Home] hyperlink returns at all times to this location.

The key item of information presented on this screen is the Note Bene; items added in the web application that any emergency care provider will want to be aware of. These may include the patient's religious or personal preferences for care, as well as key drug contraindications or disease susceptibilities.

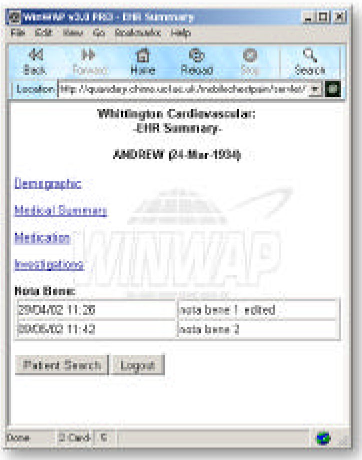

Figure 17: The Mobile Chest Pain EHR Summary screen

1.3.1.15 Demographic screen

The demographic detail screen (Figure 18) is similar to the desktop equivalent, but with the GP and other details below the patient details to enable them to fit.

Figure 18: The Mobile Chest Pain demographics screen

1.3.1.16 The Mobile Medical Summary

In general, the PDA views all follow a set pattern. Unlike the web application where the screen real estate is sufficient to allow the complete data set to be presented at once, the PDA view must be split into two types of screen. The first screen offers a summary view of the key data pertaining to the patient, and then an appropriate hyperlink can be followed to give the complete data set available for that entry.

Figure 19: The Mobile Chest Pain medical summary screen

The complete list of medical summary sections is quite large as will be recalled from section 1.3.1.5, and in Figure 19 we have given some entries in the majority of the tables. To save space, blank headings are not shown: for example the heading Family Conditions only appear if entries exist in that table (it is therefore missing in this example screen). This is the summary view of the situations known for the patient, the hyperlinks having been generated from the primary fields in the web application tables. The rest of the data set is always available, and as an example, clicking the first allergen link gives the richer detail set in Figure 20.

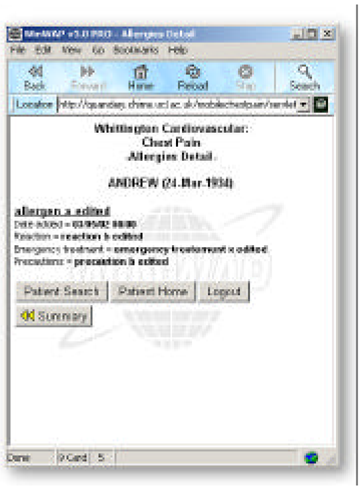

Figure 20: Allergen condition detail

1.3.1.17 The PDA Review screens

The Medications and Investigations screens for the patient both operate in a similar fashion, the summaries presented in Figure 21 and Figure 22.

In the latter case, one additional item of information is included in the summary where a result is available it is also given along with the hyperlink. This is particularly useful when emergency teams are trying to discover the value of a test result. They can quickly establish which results need to be reviewed in greater detail without being forced to examine the detail screens for each test that has been undertaken.

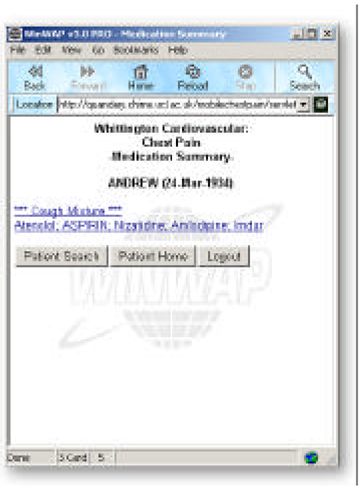

Figure 21: The Mobile Chest Pain medication summary screen

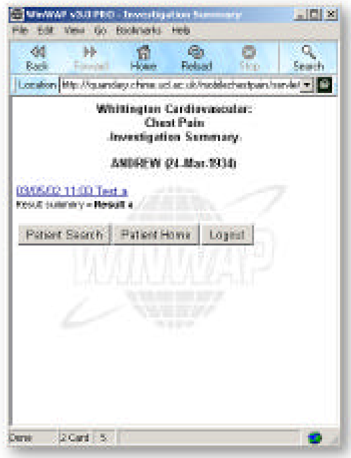

Figure 22: The Mobile Chest Pain investigations summary screen

The detail screen for a test may still reveal further information about it as in Figure 23.

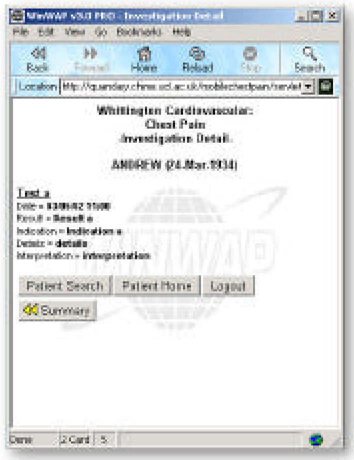

Figure 23: The investigation detail screen

1.3.1.18 Medical summary and diary for patient use (PDA version)

The application for patient use is very similar to the application described above for emergency care. The patient logs into the system in the normal way, selecting “Patient” as the chosen role. They provide their ID (which will be given to them) as their “user name”.

The differences between the patient and clinical versions of the application are:

- no nota bene is included;
- the patient search screen is omitted, clearly since the patient is only entitled to see his or her own data;
- the main menu screen layout is adjusted slightly to reflect differing patient options;
- a Patient Diary section is added to provide patients with the opportunity to record their own medical information.

1.3.1.19 The Patient Diary screen

The patient diary comprises two elements: a summary screen from which all of the patient diary entries can be seen (Figure 24) and an entry screen enabling new data to be provided (Figure 25).

This is the first time that we have seen data being edited in the mobile applications and the process is complicated only by the editing mechanism provided by the PDA. Simply enter the required data into the given text box and press {Proceed}. The data will be entered into the database and should be included on the newly refreshed summary screen.

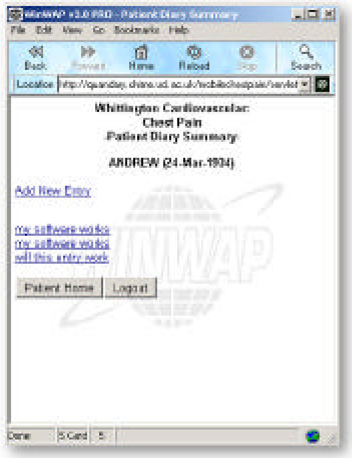

Figure 24: The Mobile Chest Pain patient diary summary screen

The structure of the patient diary has deliberately been kept simple, as further evaluation is required to verify the optimal approach to this screen. The diary is sorted on the Topic, and provided that Topic names are agreed with the patient in advance the diary could be used, for example, to capture both diabetes home monitoring readings and the periodic occurrence of asymptomatic arrhythmia.

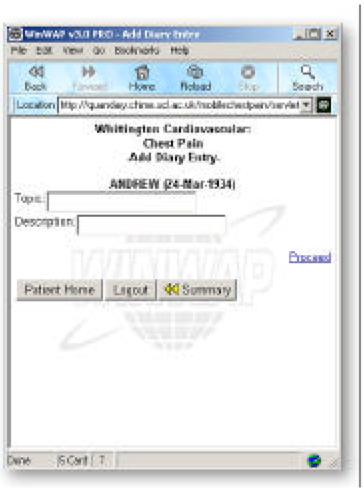

Figure 25: The patient diary entry screen

1.3.2 Early experiences from deployment, use and evaluation

The UCL FHR (Federated Health Record) demonstrator has been extended to exploit the opportunities presented by wireless Internet services and IPv6. The cardiovascular applications described in Section 1.3.1 above are being demonstrated within a set of clinical scenarios illustrating requirements for distributed and mobile access to the patients FHR, for example at the roadside scene of an accident.

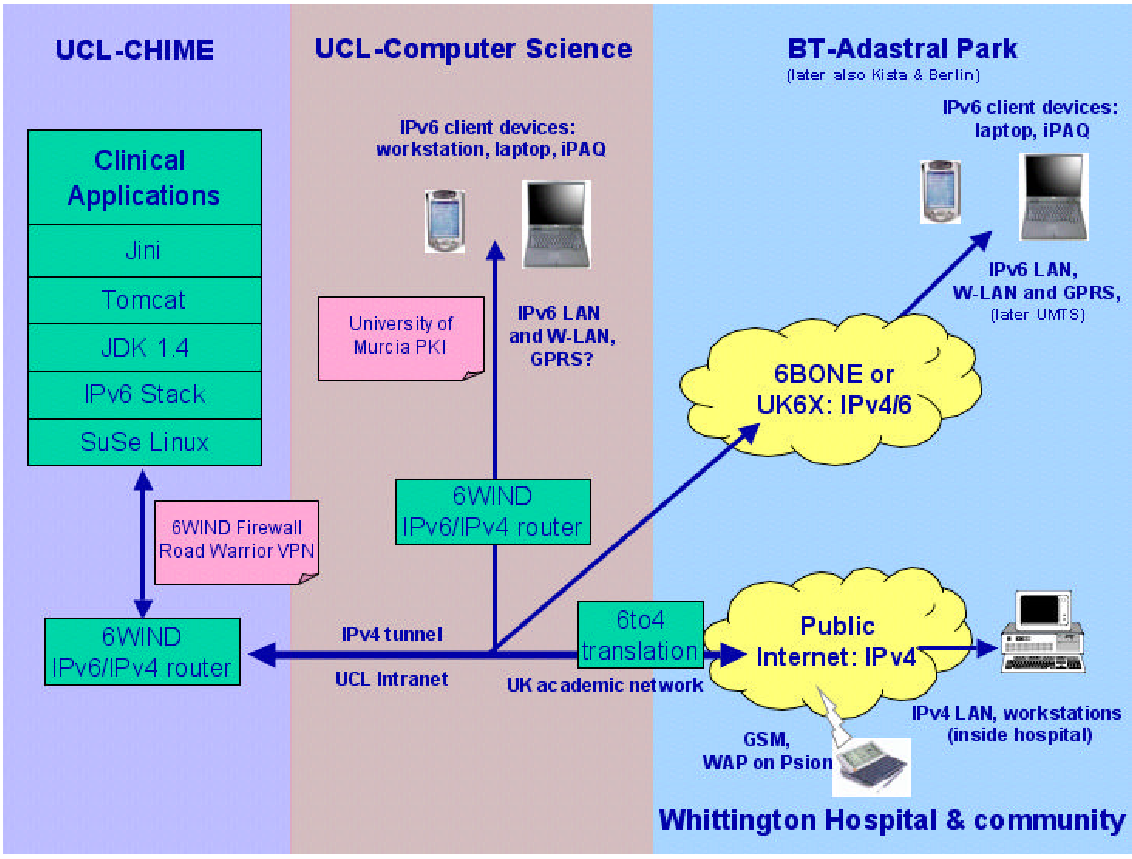

Figure 26: Network architecture of the London demonstrator site

Figure 26 above shows the principal clinical application (health record) services, located at CHIME, being delivered via an IPv6 stack infrastructure, communicated to UCL Computer Science and routed forward to the public Internet and to new IPv6 networks (6BONE and UK6X). The communications pathway involves the use of some IPv4 networks, such as the UCL Intranet connecting CHIME in north London to Computer Science in central London, and the public Internet. IPv6 networks exist within UCL Computer Science, including WLAN, and at nominated wireless demonstrator locations in London (GPRS, provided by BT), Adastral Park (Ipswich), Berlin (GPRS, provided by DTAG) and Kista (UMTS, provided by Ericsson). The technology description of the live demonstration given at the first 6WINIT technical review in Adastral Park, Ipswich, is shown diagrammatically in Figure 27.

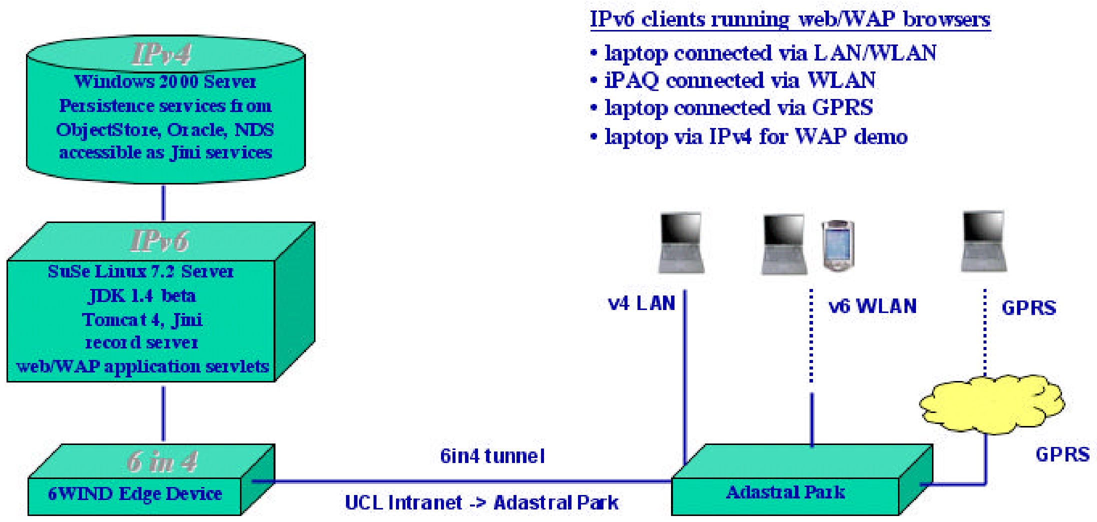

Figure 27: Network configuration of the demonstration, given at the 6WINIT Technical Review

IPv6 transition mechanisms are an important component of this demonstrator, since each scenario described above will need at minimum to use one IPv6/IPv4 tunnel for the UCL Intranet. The hospital staff working in the Whittington (scenarios 1.1.2, 1.1.4 and 1.1.5) will require translation to enable IPv4 "legacy" access from existing their devices and networks.

The web applications described above are intended both as demonstrators for 6WINIT and as real operational applications at the Whittington Hospital. The data model, screen layout and functionality of the applications have all been designed in partnership with the anticipated real clinical users at the hospital, and confirmed and documented by the development team.

Java servlet development is almost complete, subject to final review by the clinical teams. Some performance and concurrency improvements in the record server middleware components are still being investigated to improve the practical utility of the implementation.

Security requirements include the use of end-user authentication, certificate handling (using PKI) and encrypted data flows. The final phase of development, which is currently in progress, is the implementation of access control services closely tied to the record server itself, and the inter-working with PKI certification services at UCL-CS (developed at the University of Murcia). In practice, it has been agreed that the demonstration will only use pseudonymised data to permit the gradual introduction of security measures independently of other aspects of the 6WINIT network architecture during 2002. For encryption and firewall protection IPSec tunnels have been proposed to create a VPN; this will ideally be demonstrated both for fixed IP and Mobile IP scenarios. The integration of the Road Warrior application to provide VPN of the clinical applications has been installed, tested, and demonstrated at the INET2002 conference in Washington.

1.4 Checklist of 6WINIT Components and Technologies Needed for Further Demonstration and Exploitation

The principal outstanding challenges for the London site are:

- to finalise and test the installation of security features: PKI and VPN, optionally consider using MIPv6;
- to deploy the clinical applications in a live setting at the Whittington Hospital, albeit initially in a legacy IPv4 environment for NHS policy reasons;
- to establish the details of a joint demonstration across the three sites, showing portability and interoperation, targeted at the IST2002 conference and at the final 6WINIT Technical Review.

The first of these is actively in progress, with adaptations to the clinical applications and CHIME record server largely complete to permit a user to be validated by the University of Murcia PKI certificate server installed at UCL-CS. The recent demonstration of the Road Warrior integration at INET2002 is the first important step towards full IPsec VPN protection and of inter-working of the Road Warrior with the 6WIND Edge Device. Further collaboration between UCL-CS, 6WIND and IABG will be needed to complete the security infrastructure at the London site.

The deployment of the applications in a live clinical environment is expected to be completed during the summer of 2002. Much of the core infrastructure is already in place and has been used by a different clinical team using previously developed applications. The major outstanding steps are:

- the development of certain reports and standard letters needed by the team to manage communication (particularly to GPs) via paper and to maintain the existing principal hospital paper record for each patient - this task is being funded as part of a local project;
- the migration of the underlying record server to the infrastructure successfully prototyped in 6WINIT, so that the deployment is IPv6-ready for a time when IPv6 routers and networks can be accommodated.

Inter-site demonstration is still being discussed within the consortium, and three candidate scenarios are under consideration:

- portability of the GANS monitoring station so that a clinician in London could act as the expert reviewer of data transmitted from an ambulance simulator in Tübingen;
- distributed access to medical images stored in Krakow, so that a patient's record in London could logically include an x-ray held in Krakow;
- a logically integrated and fully distributed multimedia record bringing together a basic medical record from London, images from Krakow and monitoring data from Tübingen as a single record, accessed from the IST2002 conference in Copenhagen.

The technical issues associated with each of these, and the dependence upon interoperability of clinical and technical components, have still to be explored.

2 DESCRIPTION AND EARLY EXPERIENCES OF KRAKÓW CLINICAL DEMONSTRATOR

2.1 User Scenarios

The following scenarios were eventually chosen for deployment, demonstrations and evaluation in the Kraków clinical demonstrator.

2.1.1 Mobile multi-access to Clinical Appointment System (CAS)

Device and location The Clinical Appointment System (CAS) in the John Paul II Hospital in Kraków, basically for the needs of outpatient clinics. At the moment, the CAS servers are physically located in the CS Dept. of UMM, but they will ultimately be installed either in the hospital or in the ACC Cyfronet UMM (in an Application Service Provider model). As CAS is a web-based system with a J2EE back-end and a separate database, protected on the application level of security (SSL, HTTPS), its location is transparent to the users and does not influence or change any technology settings. From the user point of view, the CAS system will be available from any public location including a patient home or a street. The users (patients) will use IPv6-enabled web browsers as client applications. These will be running on desktop PCs, laptops or iPAQ PocketPC computers connected to wired and wireless networks, the later including WLANs and possibly also GPRS networks. Another access protocol in this scenario is WAP, supported by the WML-producing CAS server and UMM WAP gateway on the server side and Ericsson mobile phones as WAP terminals. The WAP interface offers only a subset of the web interface functionality.

Target users of the system in this scenario will be the patients of the JP II Hospital's outpatient clinics, wishing to book appointments with their doctors via WWW or WAP.

Current status of scenario demonstration The CAS system working in this scenario has been demonstrated to the Director of the JPII Hospital and to the Hospital's IT staff at a special demonstration session. It has been initially evaluated positively. The system has been handed over for evaluation in the Hospital and is now being tested and evaluated within the Hospital's intranet. First access tests over Wireless LAN have been performed. CAS is envisaged to be accessible from the main web page of the JPII Hospital.

2.1.2 Hospital Appointment Clerks' access to Clinical Appointment System (CAS)

Device and location The Clinical Appointment System (CAS) has been handed over for evaluation in the John Paul II Hospital in Kraków, basically for the needs of outpatient clinics. The system will be available inside the hospital's intranet over the Hospital's LAN and WLAN. In this scenario the client application will be an IPv6-enabled web browser running on a desktop PC or a laptop.

Target users of the system in this scenario will be the appointment clerks of hospital outpatient clinics whose job is preparing the schedule of patients' appointments in these clinics. They will verify and approve the requests of patients coming from locations outside the hospital (see scenario 1.1.2

Current status of scenario demonstration After a successful initial demonstration session, the system in this usage scenario has been handed over for tests on the Hospital's intranet. Specialised hospital staff (appointment clerks) are now performing an initial evaluation of this scenario. Also, it is envisaged that the same staff may play in the name of patients calling the hospital's "appointments call-centre" to make appointments for them.

2.1.3 Inter-wards hospital intranet access to Clinical Appointment System (CAS)

Device and location An experimental intra-hospital deployment of the Clinical Appointment System is considered by the JPII Hospital IT staff, to enable electronic communication and information exchange between Hospital wards. Different wards would thus use CAS to order and book consultation visits of clinicians from other wards. A modified version of the CAS system would be installed in the John Paul II Hospital in Kraków for that purpose. The client applications would be IPv6-enabled web browsers running on desktop PCs, laptops or iPAQ PocketPC computers connected to wired and wireless networks of the hospital intranet (WLAN).

Target users of the system in this scenario would be doctors ordering expert clinical consultation visits and hospital personnel dealing with appointments at wards.

Current status of scenario demonstration Demonstration and deployment of this scenario is still being considered by the JPII Hospital staff, but it is rather controversial, as this functionality is implemented by the Medical Orders Module of the Computerland's Hospital Information System (HIS) that is currently being deployed in the Hospital in clinical practice.

2.1.4 Hospital intranet access to the NetRAAD medical radiology database system.

Device and location The NetRAAD medical radiology examinations database system installed and operating in the John Paul II Hospital has been adapted to work under IPv6 throughout WP5. The usage scenario desired by the hospital's clinical staff is a mobile wireless access to patient data and DICOM and JPEG images stored in the NetRAAD from any place in the hospital, mostly at patients' beds. This will be implemented by using a laptop with a WLAN card, carried on a trolley during the daily visits at patients' beds and in other places in the hospital where access to these data is vital. The client application used in this scenario will be an IPv6-enabled web browser with a DICOM plug-in running on this laptop. Emergency access scenario with usage of PDAs and a different client application (a lightweight DICOM viewer) within the hospital intranet is also desired. It is described below, under Sec. 2.1.5.

Target users of the system in this scenario will be the doctors and other hospital staff (including nurses) of the JP II Hospital in Kraków.

Current status of scenario demonstration NetRAAD is a JPII Hospital "production" system working over IPv4 in the wired network now. Wireless access will be enabled immediately after finalisation of WLAN deployment in the Hospital. Wireless IPv6 usage will be demonstrated in parallel, as all the components needed are available (except the WLAN access points).

2.1.5 Mobile emergency multiaccess to the NetRAAD medical radiology database system.

Device and location The NetRAAD medical radiology examinations database system has been adapted to work under IPv6 throughout WP5. Its servers reside in the John Paul II Hospital. However, access to the DICOM-encoded radiology data and basic medical summary of patients stored there may be required from any location outside the hospital area, including a street, patient's or doctor's home or away clinic/hospital. WLAN and GPRS/UMTS communication technologies are considered for this scenario. A lightweight DICOM viewer, integrated with the hospital database, has been implemented for this purpose under WP5. This Java-based viewer application is especially dedicated to PDA devices and has been tested on iPAQs; however it is fully portable and works also on laptops, PCs and workstations. In many cases this client application can be also used within the hospital area over the intranet WLAN, mostly for emergency consultations by the hospital's clinical radiology experts, e.g. when one doctor is monitoring two examinations held in parallel in two different hospital buildings and a decision on terminating or continuing a "remote" examination (be it a NMR or CT) is urgently needed.

Target users of the system in this scenario could be external radiology experts or hospital experts temporarily located outside the hospital area who may wish to access and review (but not change) the DICOM encoded radiology data and basic medical summary of hospital patients from any location. In the hospital intranet WLAN variant of usage, clinical experts may access the NetRAAD data while they wander between wards and buildings and are temporarily located outside the scene of emergency action or examination.

Current status of scenario demonstration First two demonstrations of this scenario on an iPAQ and laptop have been made in the JPII Hospital, so far using the wired network first and then a WLAN access point brought from UMM. The system has been warmly welcomed by radiology doctors and the Director of the Hospital, and its basic functionality has been accepted. Several comments on updating the DICOM viewer application on iPAQ have been gathered. This scenario is scheduled for implementation as a pilot installation.

2.1.6 Konsul: operating theatre access to results of advanced medical examinations (angiography films)

Device and location The John Paul II Hospital IT staff is currently developing a system called Konsul supporting surgeons in accessing selected results of advanced medical examinations (films from angiography in most cases) directly from the operating theatres. Aseptic conditions required for the operating theatres preclude usage of desktop workstations with fixed wired connections and thus wireless access is highly demanded. The usage scenario will be implemented by using a special laptop with a WLAN card, carried on a trolley inside the operating theatres. The client application used in this scenario will be an IPv6-enabled web browser running on this laptop. The server side of the system is a Web server and FP Image: a software package performing conversion from DICOM to compressed digital video format (with lossy compression) and composing the resulting video files into appropriate web pages.

Target users of the system in this scenario are cardiac surgeons operating in an operating theatre.

Current status of scenario demonstration: the server side of the system has been implemented. The WLAN infrastructure in the JPII Hospital is not ready yet, but it will be operational in the coming weeks. The system will be demonstrated immediately after the wireless connectivity is assured.

2.2 Description of Deployed Technologies and Components

This section draws mainly on the Technical Component Descriptions section of D7, enhancing them with up-to-date descriptions of work accomplished and the status anticipated at the end of the project. However, the section also refers to previously published material in 6WINIT Deliverables 1, 2, 8, 9 and 10. References given to technical descriptions in these deliverables use the notation style [Dn Section x.y.z].

2.2.1 Changes to Network Architecture at Krakow Site

Several changes to the Krakow site's IPv6 network configuration have been made since Deliverable 7, i.e. December 2001; therefore they are described as follows.

2.2.1.1 IPv6in4 tunnel to UK

For the needs of demonstration of clinical applications developed by UMM at the Technical Review in February 2002, an SIT tunnel between the IPv6 network in Adastral Park UK and the local IPv6 network at the UMM Institute of Computer Science (ICS) was set up. The ultimate goal of this tunnel was to ensure a direct end-to-end IPv6 connection to IPv6 services in John Paul II Hospital network that is via the ICS IPv6 network. The two actual ends of this Poland-UK tunnel were: a Linux host on the ICS UMM site (http://azalea.ics.agh.edu.pl) and a CISCO router located in the UCL Computer Science Department London. Communication between Adastral Park and UCL was also accomplished with an appropriate tunnel. The tunnelling technique was chosen after prior tests of communication via the 6BONE, which showed serious disadvantages, especially the slow and unstable connections through the main Polish 6BONE node at ICM in Warsaw, so this option was dropped.

The Krakow-London tunnel is still in use for the needs of cross-Europe experiments developed jointly with the UCL Computer Science Department, e.g. for the vic/rat teleconferences on IPv6-enabled iPAQ handhelds.

2.2.1.2 Changes in local IPv6 network configuration in Krakow

The previous configuration of local Krakow IPv6 network comprising ICS UMM and John Paul II Hospital was based on two separate tunnel connections passing through a Solaris dual stack host. In the face of frequent reconfigurations during the February Review, this caused many problems, among others a problem with routing for the 2001::/8 network. Thus, the Solaris IPv6 router was omitted and a direct tunnel between ICS UMM and John Paul II Hospital IPv6 networks has been set up (see Figure 28).

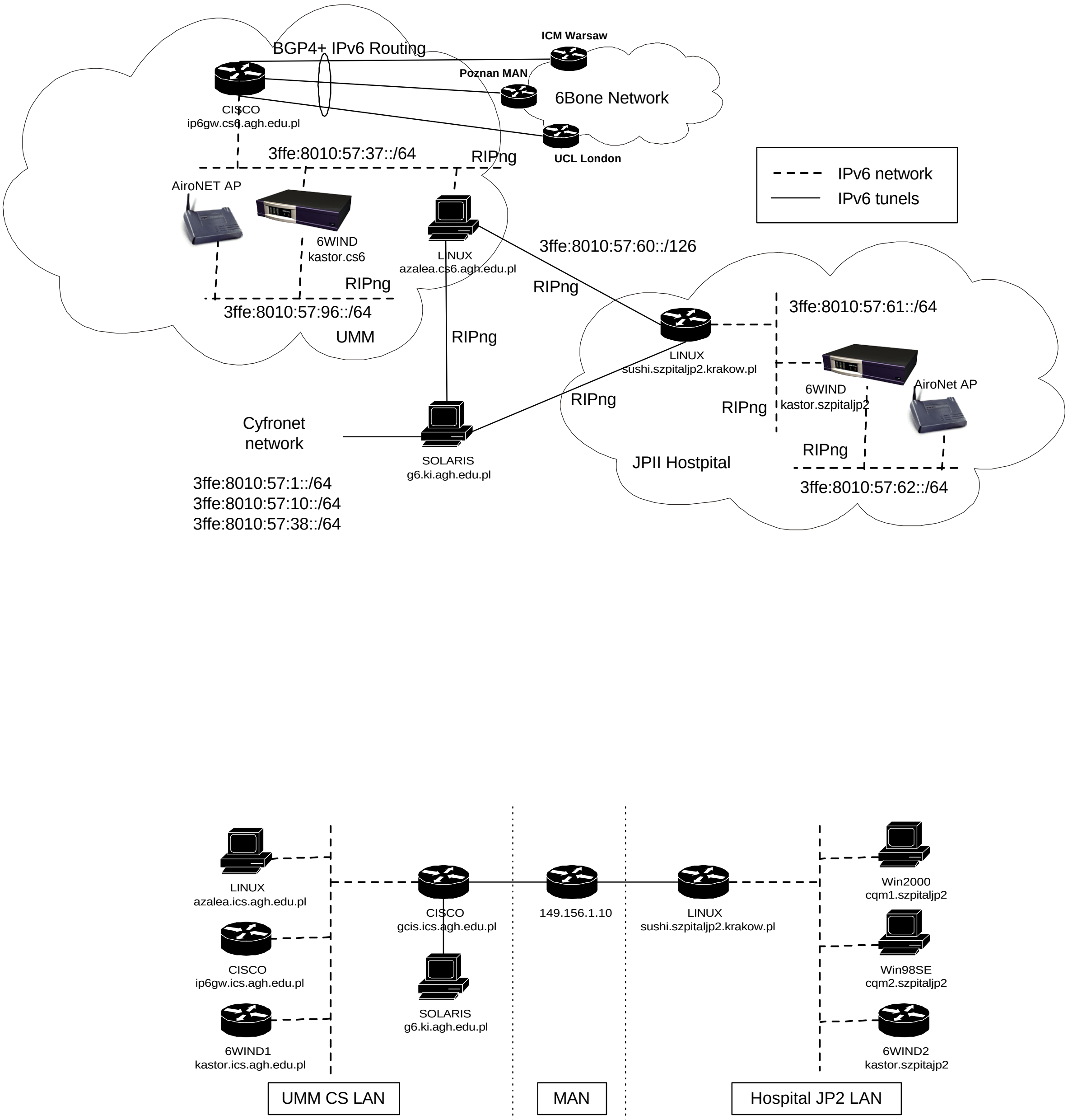

Figure 28: Network Diagram of the Krakow Site

2.2.1.3 6WIND Gates in Krakow

Two 6WIND 6200 Gates were lent to UMM by 6WIND S.A. in March 2002 for a period of one year. One of these devices was installed in the John Paul II Hospital in Krakow, while the other one in the Computer Science Department of UMM. These devices will be used primarily for setting up VPN connections between the secure intranets of UMM and the JPII Hospital over the insecure IPv4 Internet (Krakow campus and Metropolitan Area Network). Their other uses will be: IPv6 dynamic routing (+BGP4), alternative tunnel endpoints and experiments with Mobile IPv6.

2.2.1.4 Set up of a DNSv6 service

A DNSv6 service was set up at the Krakow site. This is based on the BIND 9.1.0 that supports IPv6 query/response. This server is working as a slave for the cs6.agh.edu.pl domain.

2.2.2 IPv6 Transition Mechanisms (Revised)

2.2.2.1 **Tunnelling**
Functional Requirement Native IPv6 services provided by various servers of the systems/applications chosen for demonstration have to be tunnelled via IPv4 Internet/MAN/campus networks from JP II Hospital to the IPv6 networks/devices where their IPv6 clients run. IPv6 networks at UMM Computer Science serve as a testbed of such client side. Additional tunnels are set for the needs of remote connectivity to other IPv6 islands via 6BONE (see Sec.2.2.1.1).
Chosen Technical Solution: a) iproute tool run on Linux platform or/and b) 6WIND IP Gate
Work Accomplished The tunnels set up between JPII Hospital and UMM Computer Science and further to remote IPv6 islands (London, Poznan and Warsaw) are shown in Figure 28. These were obtained with the Linux tunnelling tool.
Anticipated Endpoint To set up and test the tunnelling functionality of 6WIND Gates between JPII Hospital and UMM Computer Science. However, this probably will not be the ultimate solution as the Krakow site has to return the 6WIND routers in March 2003.
Outstanding Issues - none
Industrial Benefit This installation provides proof of concept validation of the IPv6/4 tunnelling mechanisms within the Linux platform and 6WINIT Gate.

2.2.2.2 **Translation**
Functional Requirement As the Kraków site uses IPv6-enabled terminals (laptops and PDAs with Linux), IPv6-enabled dual-stack servers and tunnelling, generally there is no need to provide translation for the demonstrated clinical services and applications at the Krakow site. An exception to this is WAP access, which needs translation. Translation may be also important when 6NET is available in Krakow (probably September-October 2002) and native IPv6 services from foreign locations are to be accessed (pure IPv4 access to dual-stack servers in Krakow is already possible).
Chosen Technical Solution: a) Socks64 Translator or b) 6WIND IP Gate – to be compared and a choice made
Work Accomplished None
Anticipated Endpoint To test access from a WAP device to IPv6 services via an IPv4-only WAP gateway and a translator. To test access from IPv4-only terminals to native IPv6 services over 6NET.
Outstanding Issues To install and test both translation devices and choose one for tests and demonstrations with the clinical servers
Industrial Benefit This installation will provide proof of concept validation of the translation mechanisms within the 6WIND Gate and Socks64 Translator.

2.2.2.3 **Reverse-proxy support for IPv4-only J2EE application servers**
Functional Requirement Most J2EE application servers (like e.g. BEA WebLogic or Orion) are bundled with IPv4-only HTTP servers. This normally precludes IPv6 clients to access the Clinical Appointment System (CAS) server implemented under such J2EE platforms. The first version of CAS was developed with the BEA WebLogic application server, which required an appropriate remedial mechanism.
Chosen Technical Solution: Application proxy: an IPv6-enabled HTTP server working in the reverse-proxy mode, running on a different machine in a common intranet. This server responds to IPv6 requests in the name of the IPv4 web server of the J2EE (EJB) application server.
Work Accomplished An Apache HTTP server working in the reverse-proxy mode was tested as one doing well with the Orion J2EE application server running the Clinical Appointment System. The same proxy with BEA WebLogic had problems with proper resolution of URLs.
Anticipated Endpoint The anticipated endpoint will be to separate the J2EE HTTP server from the J2EE application server and use an IPv6-enabled HTTP server, thus allowing native IPv6 communication from client applications without the need of an extra proxy.
Outstanding Issues To choose an ultimate J2EE platform, to separate its modules and use an IPv6-enabled HTTP server (Apache) instead of the bundled IPv4 one. To test the final setting with the CAS application.
Industrial Benefit To show easy adaptability of the powerful J2EE platform (gaining more and more significance for building scalable e-business systems) to IPv6.

2.2.3 Security Mechanisms (Revised)

2.2.3.1 **VPNs using IP Routers**
Functional Requirement To provide an encrypted channel of communication between the two kinds of networks in the Kraków site: the JPII Hospital intranet providing the clinical application servers and the end-user networks (simulated by the UMM Computer Science Department) over an insecure Internet (Krakow MAN/campus network).
Chosen Technical Solution: 6WIND IP Gate (the CISCO option was dropped as there is no support for VPNs yet in IOS IP Plus)
Work Accomplished One 6WIND IP Gate was installed in the JPII Hospital and the other one in CS Dept. UMM. First VPN tests with encryption failed due to the lack of licence for encryption software and the obsolete version of software for the 6WIND devices. 6WIND acquired an export licence for UMM and provided an upgrade in the software at the end of May 2002. Further tests at Krakow site are continuing.
Anticipated Endpoint To provide and test VPNs set up between the JPII Hospital and UMM with two 6WIND Gates
Outstanding Issues To test the current setting and the up-to-date software from 6WIND S.A.
Industrial Benefit Proof of concept verification of the 6WIND Gate IPSec functionality and demonstration of a secure infrastructure for future adoption by regional health care networks.

2.2.3.2 Application-level Security Mechanisms

Functional Requirement

All the Krakow site clinical applications chosen for demonstration need to be secured and all of them are either web applications or at least they use HTTP as the communication protocol between clients and front-end servers. This encouraged introduction of application-level security as a "must" for them, regardless of the availability of network-level security like VPNs between IP routers or Road Warrior.

Chosen Technical Solution:

SSL and HTTPS

Work Accomplished

- The Konqueror web browser has been tested to work with IPv6 and HTTPS over IPv6 both on a PC/laptop and iPAQ.
- The clinical applications' web servers (of CAS and NetRAAD) in the JPII Hospital have been upgraded to provide HTTPS over IPv6
- The DICOM viewer (Java application) must be adapted to use HTTPS over IPv6. It has been seamlessly achieved on a PC/laptop with JDK 1.4, but it is a serious problem on iPAQ, where this IPv6-enabled JDK is not available yet and probably will not be before the IST2002 Conference, where the main external demonstration of the project is scheduled. Thus, the emergency-variant approach taken in Krakow was to use a C+ programming language HTTP/HTTPS library (cURL http://curl.haxx.se/) and invoke it via the Java Native Interface (JNI) from a Java application. Successful tests with HTTPS over IPv6 connectivity have been made with a Java test application on iPAQ under Linux.

Anticipated Endpoint

To demonstrate secure IPv6 access to clinical application servers from end-devices including iPAQ PDAs.

Outstanding Issues

To finally update/patch the DICOM viewer Java application with the IPv6-enabling solution described above. To introduce authentication based on certificates for clients and servers.

Industrial Benefit

To verify usability of application-level security solutions in wireless IPv6 applications and estimate the efforts needed to achieve them, possibly by using and adapting existing tools.

2.2.3.3 **Firewall**
Functional Requirement The JPII Hospital-hosted clinical applications dual-stack server (running RedHat Linux) needs to be protected from hostile attacks including unauthorised access and denial of service attacks. Moreover, filtering can be used to protect the medical “production” intranet at JPII Hospital and wireless access LANs at both ends of the tunnel across Krakow site (JPII Hospital WLAN and UMM WLAN), e.g. only traffic from known MAC or IP addresses might be forwarded. This security mechanism may supplement the encryption protocols used in various WLAN technologies.
Chosen Technical Solution: a) Linux with the iptables package and b) 6WIND Gate
Work Accomplished A Linux-based filtering firewall was installed on the 6WINIT clinical applications server in the JPII hospital and is constantly working.
Anticipated Endpoint To test also the filtering capabilities of 6WIND Gates for the needs of protection of WLANs and medical “production” intranet at JPII Hospital.
Outstanding Issues The 6WIND Gate’s filtering capabilities must be deployed in the JPII Hospital (see Figure 31). The JPII Hospital’s “legacy” main edge firewall that filters IPv4 traffic was not able to pass IPv6 tunnelled traffic. Therefore the 6WINIT clinical applications server is connected “before” the firewall. This problem enforced implementation of filtering on the end-node, because it was not secured by the main firewall.
Industrial Benefit Verification of the filtering security mechanisms for securing clinical servers and clients in a mixed wired/wireless IPv6 network infrastructure.

2.2.4 Mobile IPv6

UMM has carried successful experiments with the HUT Mobile IPv6 stack and 6WIND Gate Home agent (IETF Draft 13). Continuity of service have been shown with a mobile node running the VIC and RAT videoconferencing applications moving between different IPv6 networks. This scenario will be demonstrated (in co-operation with 6WIND) at the IST2002 Event in Kopenhagen in November 2002. However, clinical demonstrations of Mobile IPv6 in the Krakow site and JPII Hospital are not envisaged, mainly for the reasons of lack of security mechanisms in the current implementations.

2.2.5 QoS

There are no real-time multimedia applications to be deployed and demonstrated in the Krakow site. Therefore, there is no need for usage of QoS mechanisms.

2.2.6 WAP Gateway

2.2.6.1 UMM WAP Gateway
Functional Requirement WAP access to the Clinical Appointment System is desired. Enabling booking of clinical services by patients with WAP devices is attractive since this is present-day and widely available technology.
Chosen Technical Solution: Nokia WAP Server customised at UMM CS Department
Work Accomplished The Nokia WAP Server has been customised and tested at UMM CS Department for co-operation with the CAS clinical application via the infrastructure of the Plus GSM (Polkomtel SA) GSM/GPRS operator. For security reasons, an IPsec connection is established between the UMM's WAP Server and the Polkomtel's infrastructure. The UMM WAP Gateway solution is described in D2 Section 8 and D8 Section 5. The Nokia WAP Server and Ericsson WAP Gateway/Proxy are described in D2 Section 8.2.
Anticipated Endpoint To provide access to CAS from an WAP device to an IPv6 service via an IPv4-only WAP gateway and a translator.
Outstanding Issues The Ericsson WAP Gateway is not IPv6-enabled and has not been provided by Ericsson PL. The Nokia WAP Server is also IPv4-only, so translation is required (see Sec. 2.2.2.2).
Industrial Benefit Business application of the UMM's medical WAP solutions (using the WAP Gateway) will be considered by the JP II Hospital and GSM/GPRS providers in Poland. To the 6WINIT partners, the benefit may be in showing the limitations of what can be achieved with WAP.

2.2.7 Access Network Provision (Revised)

2.2.7.1 GPRS

Functional Requirement

Wireless GPRS network access is required to demonstrate the “roadside” access to clinical applications.

Chosen Technical Solution:

GPRS infrastructure: Polkomtel SA (Plus GSM network)

Devices and software:

- Laptop running Linux or Windows 2000, with a Bluetooth PCMCIA card (Socket or Digianswer MK2 DemoCard, respectively) and BlueZ Bluetooth stack (on Linux) + mobile phone with GPRS and Bluetooth (Ericsson T68, T39m, R520m),
- iPAQ 3630 and iPAQ H3860 running Linux, with Bluetooth (Socket PCMCIA or embedded, respectively) and BlueZ Bluetooth stack + GPRS/Bluetooth mobile phone (Ericsson T68, T39m, R520m)

Protocols: 6in4 tunnelling → Bluetooth → GPRS

Work Accomplished

The GPRS infrastructure provided by Polkomtel SA was evaluated and actual available throughput at different times of day was measured. An appropriate report was prepared. Successful tests on a laptop with Linux and Windows 2000 have been made under IPv4. Tests with tunnelled IPv6 connections on Linux and Windows 2000 are underway. Tests with both types of iPAQs with Linux are underway. The BrandNewWorld’s Gismo device (an expansion pack for iPAQ providing GPRS, GSM and 802.11b) was tested with IPv4 but it still does not provide drivers for Linux, which excludes IPv6 on the client side. However, UMM is talking to BrandNewWorld about a possibility of providing the relevant API to enable porting to Linux to be done at UMM.

Anticipated Endpoint

To provide a wide range of solutions enabling access to IPv6 services from various IPv6-enabled terminals via GPRS by integrating the existing components/technologies.

Outstanding Issues

To finalise tunnelled IPv6 connectivity from laptops (both Windows and Linux) over GPRS (with Bluetooth in the middle). To provide and test tunnelled IPv6 connectivity from iPAQs over GPRS (also via with Bluetooth). To verify the prospects of using the Gismo multi-access device.

Industrial Benefit

Demonstration of the value of GPRS for retrieval of health information via wireless, to help stimulate a health care market for such solutions.

2.2.7.2 **WLAN**
Functional Requirement Wireless (WLAN) network access is required to demonstrate hospital intranet access to clinical applications, including bedside and surgery theatre, but access from other public places providing WLAN cannot be precluded. In Krakow site these will be IPv6 WLAN networks in the JPII Hospital and UMM Computer Science Department.
Chosen Technical Solution: Cisco's Aironet 802.11b (CS Dept UMM) and 3COM's 802.11b (JPII Hospital)
Work Accomplished CS Dept UMM: WLAN hosting IPv6 networks has been set up and is in a day-to-day use. JPII Hospital: deployment of 3COM WLAN access points is in progress.
Anticipated Endpoint To achieve a stable wireless network environment for IPv6 access networks in Krakow site.
Outstanding Issues To finalise WLAN installation at JPII Hospital.
Industrial Benefit Demonstration of an IPv6 wireless methodology suitable for use inside hospitals in the vicinity of medical devices. Demonstration of IPv6 working seamlessly over wireless networks in a demanding real-world environment.

2.2.7.3 **IPv6 WANs**
<u>Functional Requirement</u> Native IPv6 distributed access is required to validate the future scenario of widely available IPv6 networks within and between hospitals. It will be demonstrated in the Krakow site using local networks at JPII Hospital and UMM Computer Science, connected via Krakow MAN, tunnelling to Polish and foreign 6BONE sites and by native IPv6 access to services over 6NET.
<u>Chosen Technical Solution:</u> 6in4 direct tunnelling between IPv6 islands, native IPv6 connectivity via 6NET
<u>Work Accomplished</u> The tunnels between JPII Hospital and UMM IPv6 networks have been set up and are in use. Tunnels from UMM to Polish 6BONE sites (Poznan, ICM Warsaw) have been set up. The tunnel to UK (UCL-CHIME UK) has been set up in February 2002 and can be of use any time.
<u>Anticipated Endpoint</u> To establish 6NET nodes (native IPv6 routers) in Krakow: one in ACC Cyfronet UMM, one in CS Dept UMM and one in JPII Hospital. To use native IPv6 and permanent IPv6 addressing for Krakow intra-site communication and for accessing external services provided by 6WINIT partners and other institutions.
<u>Outstanding Issues</u> To set up, test and demonstrate the 6NET infrastructure in Krakow site. This is (optimistically) scheduled for October 2002.
<u>Industrial Benefit</u> To demonstrate clinical services available in a metropolitan and cross-Europe IPv6 WAN in order to show the marketing potential of IPv6.

2.2.7.4 **UMTS**
<u>Functional Requirement</u> Wireless UMTS network access may be required to demonstrate the next-generation “roadside” access to clinical applications. In practice this can be simulated from a UMTS test-bed location.
<u>Chosen Technical Solution:</u> Ericsson “Kista Ring”, Polkomtel’s UMTS test infrastructure
<u>Work Accomplished</u> Polkomtel SA, the operator of Plus GSM network in Poland, have proposed usage of their UMTS test infrastructure to UMM. Details of this offer are under negotiation now.
<u>Anticipated Endpoint</u> To use and test the UMTS access network for Krakow clinical applications before and during the 6WINIT Final Review in January 2003. Possibly, to incorporate the JPII Hospital infrastructure and staff to provide real usage scenario of some bandwidth-sensitive applications (particularly those related with DICOM files).
<u>Outstanding Issues</u> To test the UMTS terminals and access infrastructure, once they are provided by Ericsson or Polkomtel, for the purpose of clinical applications.
<u>Industrial Benefit</u> Provide proof-of-concept verification of UMTS access to medical applications and services, as a market stimulation. Ideally the demonstration will highlight the benefits of UMTS over GPRS.

2.2.7.5 Multi-access

Functional Requirement

Portable devices like PDAs will need multi-access technology to switch seamlessly between access networks, as their users (e.g. clinical doctors) move between different places covered by different network access technology on a daily basis.

Chosen Technical Solution:

- WLAN interfaces for iPAQs
- Ericsson mobile phones as GPRS "modems" available via Bluetooth
- BrandNewWorld's Gismo device

Work Accomplished

The CISCO Aironet WLAN PCMCIA cards have been tested for all the WLAN scenarios with iPAQs to work perfectly. Alternatively, the iPAQ user may manually switch on to GPRS (operated by a mobile phone) via the iPAQs's Bluetooth interface. The BrandNewWorld's Gismo device (an expansion pack for iPAQ providing GPRS, GSM and 802.11b) is a real multi-access "all-in-one" devices and it was tested to work perfectly with IPv4 but it still does not provide drivers for Linux, which excludes IPv6 on the PDA.

Anticipated Endpoint

To add and test UMTS as a faster and more IPv6-focused technology, thus replacing GPRS and to show WLAN/UMTS multi-access.

Outstanding Issues

To finally confirm all GPRS scenarios not verified yet. To clarify the Gismo/Linux availability or to develop appropriate drivers. To clarify UMTS availability.

Industrial Benefit

To validate the WLAN/GPRS/UMTS multi-access scenarios in a set of clinical applications.

2.2.8 Access Devices

2.2.8.1 **Terminals**

Functional Requirement

The various Krakow user scenarios require three different user access devices.

1. a laptop computer to run the web applications (CAS, NetRAAD, movie library browsing) and play the coronarography movies
2. a PDA (iPAQ), to run the web applications (CAS, NetRAAD) and the Java DICOM viewer (in the “Home/street multi-access to NetRAAD radiology imaging database” scenario)
3. a mobile phone for two roles: a WAP terminal for WAP access to CAS or a GPRS modem for other scenarios

Chosen Technical Solution:

Laptops: running dual-stack Linux or Windows 2000 with IPv6 stack, with Wireless LAN (Aironet PCMCIA card) or GPRS connection through a mobile phone, a web browser with IPv6 support (Konqueror or IE), Java 1.4, Windows Media Player as a plug-in for the web browser

Compaq iPAQ: running dual-stack Linux, with a Wireless LAN (Aironet PCMCIA card) or GPRS connection through a mobile phone, an IPv6-enabled web browser (Konqueror), Java 1.4

Ericsson T68, T39m, R520m GSM/GPRS phones with WAP browser and GPRS service

Work Accomplished

The terminals enumerated above have been adapted and tested.

Anticipated Endpoint

To have terminals suitable for respective applications and acceptable by end-users.

Outstanding Issues

To test the new iPAQs 3900 series (400 MHz CPU) and high-capacity flash memory cards (SD) for the needs of DICOM files storage and display. Availability of drivers for iPAQ’s SD expansion slot under Linux must be researched.

Industrial Benefit

A spectrum of devices is important to show the compatibility of 6WINIT solutions with a wide range of user needs.

2.3 Clinical Applications

2.3.1 Definitive technical status of clinical applications

2.3.1.1 Clinical Appointment System (CAS)

The Clinical Appointment System has been updated and the following changes to CAS have been and will ultimately be made, as compared to the status described in [D7 Sec. 3.4.3].

- CAS has been supplemented to produce code suitable for iPAQ (see Figure 29). New JSP code has been developed and new graphics has been designed and implemented.
- CAS has been ported to open-source application servers (EJB containers): Orion and JBoss (http://www.JBoss.org). The initial version of CAS was developed under an evaluation license of BEA WebLogic for technical reasons (full support for EJB 2.0, ease of development, comprehensive documentation), but a real deployment in Polish hospital has to be done under a non-expensive license, for economical reasons. The final decision is that JBoss will be used, for its supreme performance, maturity and compliance with EJB 2.0 specification. JBoss is distributed under GNU LGPL licence.
- The CAS web server (HTTP server) will ultimately be separated (unbundled) from the application server and replaced by an IPv6-aware one (see Sec. 2.2.2.3) to enable access over IPv6.
- The CAS web server will ultimately be patched with a HTTPS module and the Konqueror web browser will be configured and tested with HTTPS. Eventually, tests with application-level security in CAS will be made to demonstrate secure IPv6 access to clinical application servers from end-devices including laptops and iPAQ PDAs.
- GPRS connectivity via Bluetooth-enabled Ericsson mobile phones has been achieved for laptops and will eventually be set up and made available for iPAQ.

CAS is being tested with the Konqueror web browser on the client side and is being evaluated by the hospital staff.

Figure 29: Access to Clinical Appointment System (CAS) from iPAQ 3630 (left) and H3860 (right)

2.3.1.2 NetRAAD

The NetRAAD system has been adapted to work with IPv6. Its servers have been ported to IPv6 and have been installed on a special dual-stack machine in the JPII Hospital, named sushi. Security based on HTTPS has been provided - the NetRAAD's web server on this machine has been upgraded with an HTTPS module. Access from a web browser on a laptop is possible both on the Windows 2000 platform with IPv6 stack and on the Linux platform. The latest version of Konqueror web browser on Linux (KDE 3.0) works properly with NetRAAD and enables its full functionality (earlier versions used to have problems with execution of Java Script scripts which disabled some essential NetRAAD menus).

2.3.1.3 DICOM viewer using the NetRAAD's medical images database

The UMM's DICOM viewer Java application targeted for Pocket PC PDAs (e.g. iPAQs), using the NetRAAD's medical images database, has been refined, debugged and updated as compared to the status described in [D7 Sec. 3.4.6]. Now it is more stable and provide additional functionality, including:

- Animation of multi-frame DICOM images – "DICOM movies" (see Figure 30);
- image properties (Hounsfield window);
- zoom option;
- magnifying glass tool;
- more DICOM tags displayed.

These options were added after an analysis and validation performed by radiology doctors. Thus, this application has reached the final stage of envisaged functionality. It is now being optimised to display the DICOM movies (sequences of DICOM frames) faster. The viewer has been also Jini-enabled, allowing dynamic downloading of code to the end-device on request.

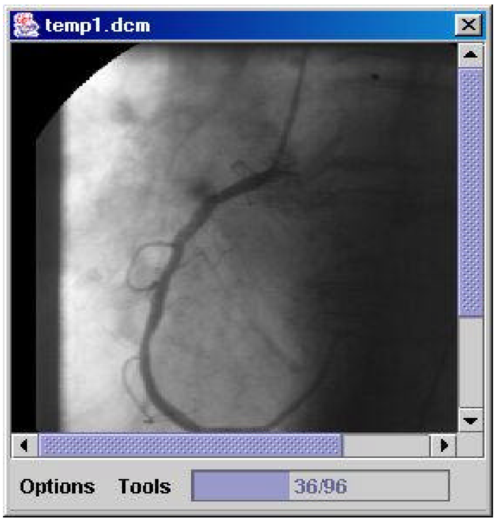

Figure 30: Animation of multi-frame DICOM images (movies) in the UMM's Java DICOM viewer

A separate issue is adding security mechanisms while preserving the IPv6 communication capabilities. It is not a problem on a PC/laptop with the IPv6-enabled JDK 1.4, but it is a serious problem on iPAQ, where this JDK is not available yet and probably will not be before the main 6WINIT presentation at IST2002. Work is underway to use a C++ programming language HTTP/HTTPS library (cURL http://curl.haxx.se/) and use it form the Java application via the Java Native Interface (JNI). First tests of this solution on iPAQ under Linux have been successful and therefore a full application-level security for the DICOM viewer on PDAs is envisaged eventually.

2.3.1.4 Konsul: Mobile viewer for medical examination films (angiography)

The Krakow site will also demonstrate access to results of advanced medical examinations (angiography films) over wireless IPv6 connections from an operating (surgery) room. The need for this kind of application has emerged in May 2002, when 6WINIT was well advanced. The Konsul system, implemented by the JPII Hospital IT staff, is based on the FP Image conversion system, providing output in form of a set of web pages containing compressed video sequences from angiography examinations (the inputs are original DICOM documents, the compression is lossy). These films will be browsed in an IPv6-enabled browser (Internet Explorer) and then displayed in an appropriate plug-in (Windows Media Player) on the Windows 2000/IPv6 stack platform running on a laptop with a WLAN card in an operation theatre within the JPII Hospital intranet. The system has been implemented and initially deployed in the JPII Hospital. A different machine, called Konsul, is envisaged to host the server of the Konsul system.

2.3.2 Early experiences from deployment, use and evaluation

2.3.2.1 Experiences with Clinical Appointment System

The Clinical Appointment System is in its initial stage of demonstration and deployment in the JPII Hospital in Krakow. The dictionary databases were filled in with an initial set of proper and consulted data and a table of trustee rights for medical staff is being prepared at the moment. After the first tests, the part of the system responsible for assigning medical examinations to diagnostic devices was modified for better and more comfortable use. The Hospital IT staff are collecting comments from first medical end-users. All observations and irregularities of the system are noted and delivered to the technical partner (UMM). The CAS graphical user interface was adapted to integrate fully with the hospital intranet system.

A real concern on the way of broader deployment, tests and evaluation of CAS is user acceptance. At present, only about 19% of the Polish population uses Internet on a more or less regular basis. However, the main target user group for CAS is ill people requiring follow-up in an outpatient clinic. The JPII Hospital statistics show that a majority of their outpatient clinics' patients are elderly people with generally low level of computer skills. The second target group are people wishing to purchase medical services (mostly specialised examinations like NMR, CT, digital X-ray) who play as customers in a free market competition between hospitals. In this group the probability of using the Internet channel of access to the offered services is much higher, but this group is much smaller.

For these reasons, in a realistic deployment scenario, it is envisaged that mostly specialised personnel will use the system. Primarily, these will be GP doctors who would make electronic Internet booking of hospital services in the name of the patient, from the GPs' points of work, including their surgeries and patients' homes. The second group of users would be the hospital "call-centre" staff , once such division is established.

The key technical requirement is assuring security of the hospital's network, as CAS is indeed a publicly accessible server possibly residing inside the hospital.

With regards to the inter-ward intra-hospital usage scenario (see Sec. 2.1.3), the possible added value of CAS working in this scenario (versus the standard HIS module) must still be identified. It might be the possibility of ordering an expert consultation immediately, during a doctor's visits at the patient's bed.

2.3.2.2 Experiences with NetRaad

At this stage, the wired IPv4 version of NetRaad is used as a "production" system. Results and descriptions of all examinations made in the Centre of Diagnostic and Rehabilitation of Heart and Lung Diseases of the John Paul II Hospital are entered into the NetRaad system (computer tomography (CT), nuclear magnetic resonance (NMR), nuclear medicine, ultrasound, radiology, consultations). The system delivers medical images with diagnostic quality (DICOM), reference quality (JPG) and descriptions of examinations for doctors and radiology staff. Access to all data stored in the system is fully authorised through SSL. The JPII Hospital staff plan to implement smart card authorisation in the future.

The IPv6 version of NetRAAD server for 6WINIT demonstrations purposes has been installed in the JPII Hospital on a special dual stack Linux host named sushi.szpitaljp2.krakow.pl (IPv4) and sushi.cs6.agh.edu.pl (IPv6 - temporarily registered in UMM's DNS for convenience). This machine physically resides in the JPII Hospital and is connected to this testbed's internal test & demonstration IPv6 network, but is accessible also from outside the hospital (see Figure 28). Such setting enabled both local in-site tests and a cross-Europe access scenario involving a client roaming in a IPv6 WLAN in Adastral Park in the UK, and the server running in the JPII Hospital Krakow, Poland, which was demonstrated at the Project Technical Review in February 2002. However, some changes to this configuration may be needed as Wireless LAN access to this NetRAAD is envisaged from inside clinical “production” networks - see Figure 31 in Sec. 2.3.2.4. This machine has been set up to host:

1. demonstration version of the NetRAAD system adapted to Linux and IPv6 under WP5
2. IPv6-enabled Apache HTTP server
3. Tomcat servlet engine
4. Postgres DBMS - the NetRAAD's database with DICOM and JPEG images and alphanumeric patient data

The NetRAAD's database has been fed with a small number real results of radiological examinations held in the John Paul II Hospital, but with dummy personal data associated with these images, for security reasons. Therefore, the 6WINIT NetRAAD is an IPv6 clone of its “production” ancestor, but it still suffers so far from the lack of sufficient amount of representative medical data. However, the latest agreements between UMM and JPII Hospital envisage feeding its database with results of research and educational examinations, routinely held once a week (in the past, these results used to be deleted after a short time).

The first demonstrations of DICOM images and patient data transferred from NetRAAD on iPAQ PDAs were successful and generally positively evaluated. Three radiology experts, hospital IT staff and UMM Computer Science representatives had a long evaluation session of the DICOM viewer on iPAQ and produced the following opinions, criticism and conclusions:

1. Mobile and wireless access to DICOM images on PAQs can be useful in several application scenarios (see Sec. 2.1.5).
2. The quality of image on iPAQ series H3800 is acceptable for referential (non-diagnostics) usage, e.g. for making a decision on terminating or continuing a set of examinations of a patient laying down under the examination equipment (e.g. CT or NMR machines) in an away building.
3. The parameters of iPAQ’s display predestine it for lower resolution images (e.g. CT, NMR, ultrasound), rather than the higher-resolution ones (e.g. X-ray).
4. Wireless bandwidth is crucial: e.g. DICOM files from a single NMR examination may have a total size of 12MB (5 files with 20 images each, 128KB each picture), while for CT this may be up to 150MB (300 images of 512 KB each). Ideally, all this should be available at the terminal within minutes, thus setting the effective data transfer rate around 4 Mbps! Thus, the only wireless technologies to consider for transferring DICOM files are WLAN and UMTS. GPRS is insufficient. Methods for transferring data while browsing and displaying the image should be employed.
5. For the reasons mentioned above under point 4, memory of the PDA is also crucial. Current Pocket PC PDAs like iPAQ or Jornada offer 64 MB RAM and 32MB (soon 48MB) of Flash

ROM. Expansion slots enable supplementing the Flash ROM by additional 64-256MB (CF and SD standards). However the following problems are envisaged:

a. Flash memory has a slow write speed, which may impact the time needed to save the large DICOM files in ROM before displaying them and thus make the user wait.

b. Availability of drivers for iPAQ’s SD expansion slot under Linux must be researched.

6. The DICOM viewer needs to be updated before it is put for larger-scale testing. The need for the following corrections was raised:

   a. Pre-set Hounsfield window values should be available in relevant buttons/menus, as well as an “original window” button.

   b. The pencil movement procedure for manual setting of the Hounsfield window should be adapted to the standards and habits of radiology doctors (the directions of movement, the sensitivity).

   c. Arrow menu for browsing slices/images in a single file should be provided.

   d. Enlargement of referential images (JPEGs) available in NetRAAD should be enabled.

   e. On-screen measurements should be considered.

2.3.2.3 Experiences with wireless access to angiography films

Direct wireless access to previously taken angiography films (video sequences) inside cardiosurgery theatres is foreseen to be beneficial in the work of cardiac surgeons. In particular, it can be helpful in considering indistinct situations. Before initiation of the Konsul system, surgeons had to leave the operating room to access a standalone “wired” workstation were they could see the angiography film. Because of septic limitations, such a conventional PC workstation cannot be installed and used near the operating table. Thus the need for a portable wireless solution.

The Konsul system has been initially tested in an IPv4 wired network. Work on its adaptation and deployment of this application to Wireless LAN and IPv6 is underway.

After the first tests, the surgeons suggested the use of a better quality LCD panel with a bigger angle of view. Additionally, the possibility of controlling the speed of playing the scene, playing it frame by frame and zooming into small parts of stopped frame will be needed.

2.3.2.4 Changes in local IPv6 network configuration in John Paul II Hospital network

CAS is a service open to the public from one side and it must be attached to/accessible from the hospital administration network from the other side. There is no need to attach it to the “clinical production” network where patients’ personal data and examination results are stored. Thus its location would best be outsourced (at UMM CS as the current status is or at ACC Cyfronet UMM) or an appropriate security setting should be worked out in the coming weeks.

A different setting concerns the two other systems (NetRAAD and Konsul): their servers must be connected to the “clinical production” networks and they may have a restricted set of authorised users. Thus, the NetRAAD and Konsul must be placed behind a filtering firewall with an access lists of known addresses of authorised terminals, to minimize the risk of unauthorized access to the clinical networks. We have chosen the 6WING Gate to act in this role and the resulting internal testbed network in the JPII Hospital in Krakow is sketched in Figure 31 below.

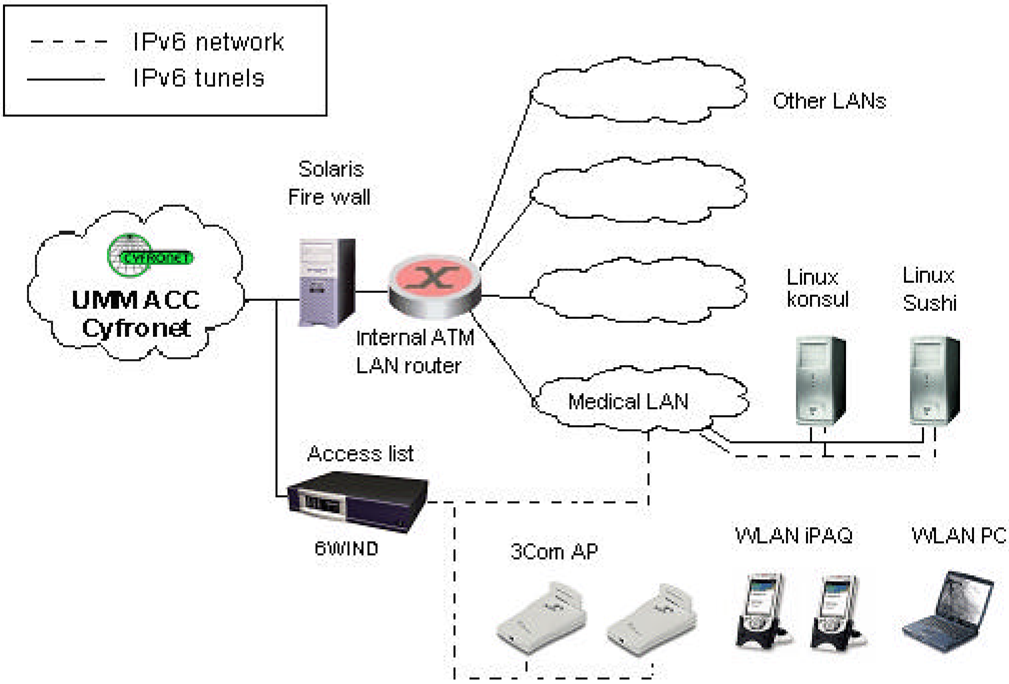

Figure 31: Simplified diagram of the internal IPv6 network in the John Paul II Hospital

2.3.2.5 Conclusions from early deployment and use

The following main conclusions may be drawn out of the early deployment and use of clinical application at the Krakow site.

1. The medical radiology applications requiring delivery of DICOM documents/images require fast transfer of large files. In fact, this kind of applications has higher bandwidth requirements than real-time MPEG-1 video, as its effective data rate may easily exceed 2 Mbps.

2. For the reasons mentioned above, a scarcely populated WLAN is highly desired in a hospital intranet to serve digital wireless radiology applications.

3. Outside, a full-speed UMTS (2 Mbps) is a minimum, while GPRS is insufficient for DICOM images, but it may be useful for transmission of compressed images (JPEGs) and textual data.

3 DESCRIPTION AND EARLY EXPERIENCES OF TÜBINGEN CLINICAL DEMONSTRATOR

3.1 The Guardian Angel System GANS

3.1.1 The Tübingen Simulator Centre TÜPASS

The Universitätsklinikum Tübingen, UKT, of Tübingen University runs one of the few dozen of high-fidelity patient simulator centres world-wide. In the given context, the key features of this centre, called TÜPASS – Tübinger Patienten Simulator System – are the following: In an 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.

TÜPASS and comparable centres have a proven record in training both students, anaesthesia specialists, intensive care personnel and other paramedics.

3.1.2 From TÜPASS to GANS – the Guardian Angel System

The proven and very positive experiences from TÜPASS led to the concept of the Guardian Angel System: 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 an "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.

3.1.3 GANS in 6WINIT

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". Towards the end of the project, a trial using UMTS is envisaged. Although not addressed in 6WINIT, other systems such as ETSI TETRA may become technology candidates for GANS.

3.2 GANS Technical Architecture

Not being a formal element of 6WINIT, the development of the GANS application is carried out in close co-operation with and exploitation of 6WINIT results evolving over the project's duration. At present, the GANS target architecture is based on J2EE and JMF standard software according to the following figure:

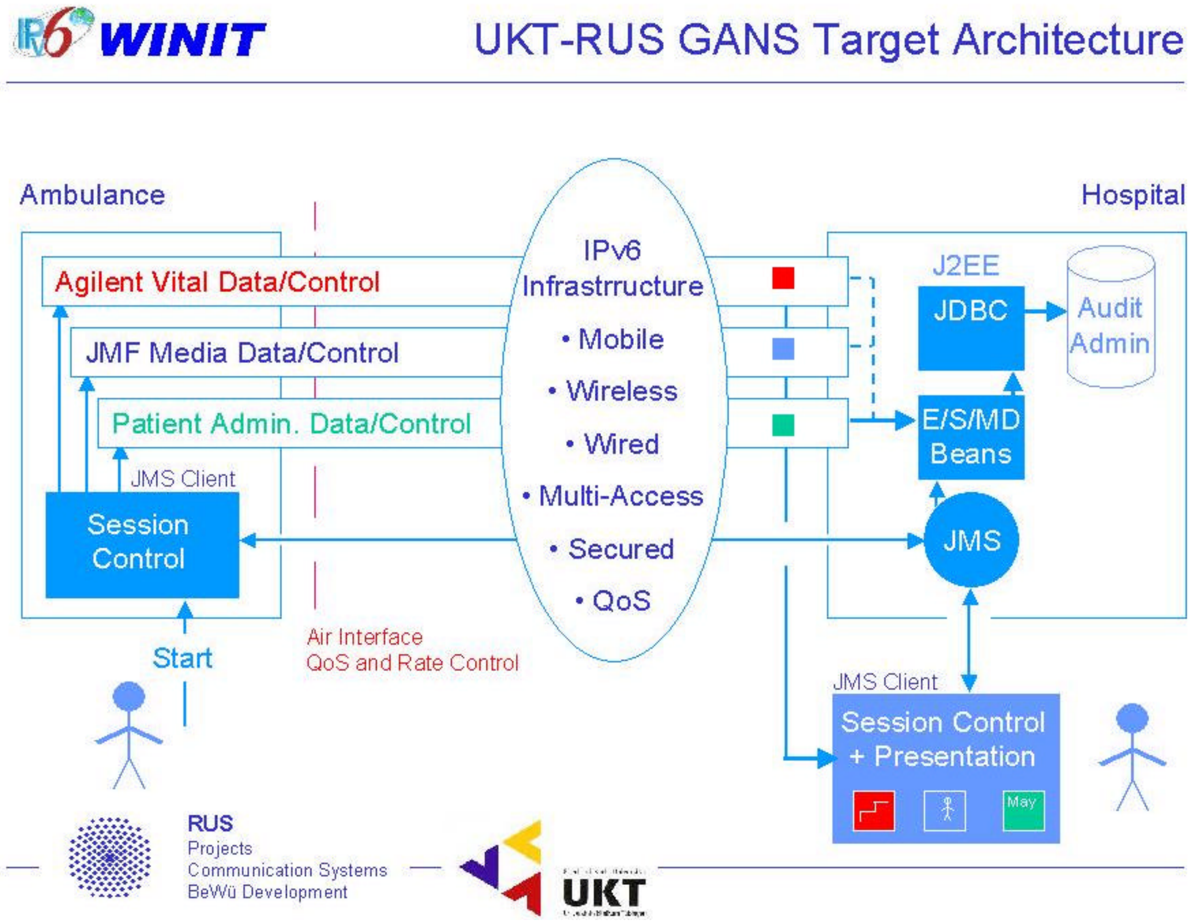

Figure 32: Guardian Angel GANS Target Architecture

Following this exploitation and adaptation strategy, after a demonstration of a GANS initial version at the IST 2001 conference in Düsseldorf, December 3rd – 5th , an advanced GANS version was demonstrated between Washington and Tübingen at the INET 2002, June 18th – 21st , 2002.

At present, the main technical improvements of the GANS development and adaptation to 6WINIT goals over the IST 2001 state are the following:

- The whole GANS system is now integrated via J2EE/JMS, i.e. vital data, audio and video are controlled via JMS messages
- The whole system is “close to all Mobile IPv6” – see section 3.4 below; for the INET demonstration the JMS component was still replaced by an IPv6 capable-module.
- Although still in need of improvement, in addition to video full-duplex audio was realised over JMF on Linux and MIPv6.

The following figures show GANS at INET 2002:

Figure 33: INET 2002, Washington June 18 – 21: GANS presentation and live demonstration

The following figure shows the (integrated) GANS screen at INET 2002:

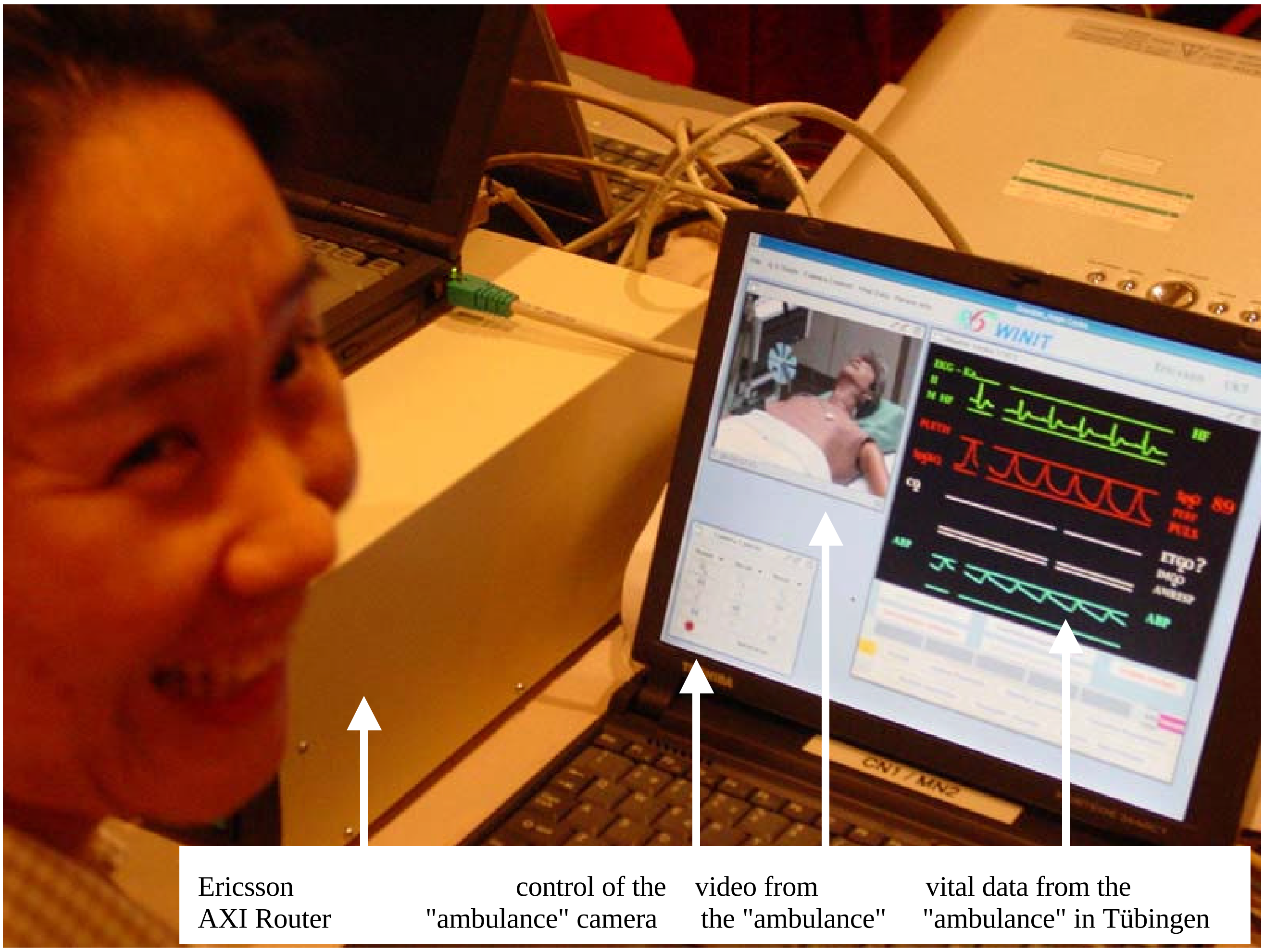

Figure 34: INET 2002, Washington June 18 – 21: GANS live demonstration screen

In addition to GANS, the 6WINIT network at INET also supported the VTT Home Environment and the IABG-UCL/CHIME Road Warrior demonstration; the following picture shows the corresponding configuration:

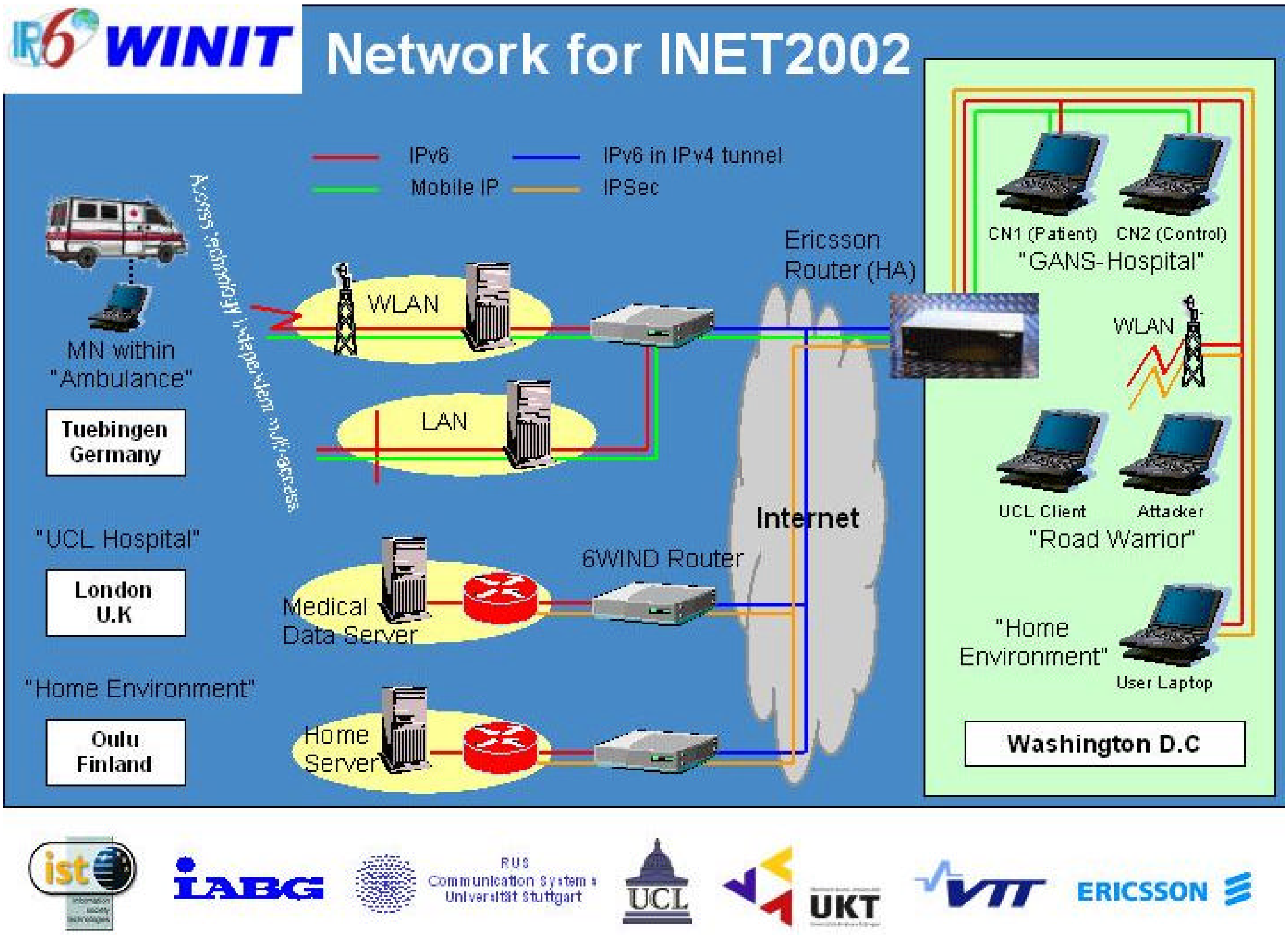

Figure 35: INET 2002, Washington June 18 – 21: 6WINIT MIPv6 network

3.3 Description of Deployed Technologies and Component

The following section draws mainly on the Technical Component Descriptions section of Deliverable 7, enhancing or revising them with the corresponding up-to-date descriptions of work accomplished and - if possible - the status anticipated at the end of the project.

3.3.1 IPv6 Transition Mechanisms

3.3.1.1 **Tunnelling**
<u>Functional Requirement:</u> Mobile/wireless and/or wired IPv6 services from the Ambulance will need to be tunnelled via IPv4-GPRS and 6BONE or to the UKT Hospital. Additional tunnel(s) may be required for remote connectivity to other IPv6 sites.
<u>Chosen Technical Solution:</u> Tunnels between fixed IPv6 sites: configured IPv6 in IPv4 tunnels. Tunnels over IPv4 based wireless access network (GPRS, WLAN): dynamic IPv6 in IPv4 tunnel setup. Ericsson Tunnel Broker solution, part of Ericsson Multiaccess technology.
<u>Work Accomplished :</u> Tunnels have been set up for GANS testing between Stuttgart and Helsinki, and for the INET 2002 demonstration between Washington and Tübingen. The Stuttgart RUS IPv6 testbed was reorganised, and updated following a change of the German 6Bone configuration at Münster University.
<u>Anticipated Endpoint:</u> For an GPRS-adapted GANS, e.g. vital data transmission only, the present Ericsson solution would be sufficient.
<u>Industrial Benefit:</u> The IST 2001 and INET 2002 demonstration provided a convincing proof of concept validation of Ericsson's solutions for the IPv6/4 tunnelling mechanisms both in the mobile and/or wired/wireless case.

3.3.1.2 **Translation**
Functional Requirement: -

3.3.2 Security Mechanisms

3.3.2.1 **VPNs using IP Routers**
Functional Requirement: Eventually, the GANS application does require 'all' state-of-the-art security mechanisms
Proposed Technical Solution: GANS security will be provided by a combination of 6WINIT developed network layer mechanisms and such which are inherent in the J2EE framework the latter possibly supported by the work of UCL concerning the usage of the University of Murcia IPv6 enabled PKI infrastructure.
Work Accomplished: None in the present period
Anticipated Endpoint To be determined (tbd)
Industrial Benefit: As application server usage is definitely a must in many commercial environments. The integration mentioned above would be of real importance for the acceptance of IPv6 in such environments.

3.3.2.2 **Road Warrior**
Functional Requirement: -

3.3.2.3 **Firewall**
Functional Requirement: The GANS J2EE application server needs to be firewall protected also at IPv6 level.
Proposed Technical Solution: No special solution envisaged so far.
Work Accomplished: None in this period
Anticipated Endpoint: tbd
Industrial Benefit: -

3.3.3 Mobile IPv6

3.3.3.1 **MIPv6 Home Agent**
Functional Requirement: The GANS application as such does require Mobile IPv6.
Chosen Technical Solution: UKT-RUS will pursue the successful co-operation with 6WINIT partner Ericsson
Work Accomplished: RUS/UKT have successfully experimented with the HUT-based Ericsson Mobile IPv6 solution for mobile nodes as well as the Ericsson Mobile IPv6 Home Agent (implemented on two AXI routers for the INET 2002).
Anticipated Endpoint: Assuming the availability of a “GPRS sufficient for GANS”, the present Ericsson MultiAccess solution would be a good starting point for a prototypical deployment. The possibly open issue of securing of the MIPv6 BU etc. is not considered to be a major obstacle.
Industrial Benefit: -

3.3.3.2 **802.11 Access**
Functional Requirement: It is assumed that, in hot-spot locations, MIPv6 WLAN access is beneficial .
Chosen Technical Solution: Ericsson’s Multi-Access; see above.
Work Accomplished The Ericsson solution was used for preparation of and conducting the INET 2002 demonstration between Stuttgart–Helsinki and Washington-Tübingen respectively. RUS has studied an Ericsson implementation proposal for a simple 802.1x-based AAA-solution needed in the case of public 802.11 deployment.
Anticipated Endpoint: As far as the ambulance-oriented of the GANS scenario is concerned, the role of 802.11 is dependent on its corresponding (public) deployment; technically, the present Ericsson MultiAccess solution would be sufficient. The related inter-ISP AAA issues are not considered here. It can be assumed, that at least initially a pioneering spirit would allow to initiate an appropriate initiative.
Industrial Benefit: Public handover scenarios between GPRS/GSM/UMTS and 802.11 hotspots

3.3.3.3 GPRS

Functional Requirement:

Wide-area coverage of Mobile IPv6/IPv4 wireless GPRS access is essential for the ambulance-based GANS application. In order to reach the GANS centre addresses provided must be globally routable. An initial GANS system would need only 8.5 Kbit/s upstream net capacity if the stream is reduced to the vital data only and the sampling rate is cut down so that it fits into one GPRS slot capacity (as only one is currently available in Germany).

Chosen Technical Solution:

Ericsson's MultiAccess - i.e. MIPv6 over GPRS; see above. In addition to GPRS, UKT-RUS will also explore forthcoming UMTS test beds both within and outside of 6WINIT (RUS as partner of IST project MobyDick will establish an UMTS TDD cell at Stuttgart University).

Work Accomplished:

Only indirect contributions: Work has pursued to further reduce the bandwidth requirements of the vital data transmission.

Anticipated Endpoint

In the constraints of the present 4:1 (downstream – upstream) offering of GPRS by Deutsche Telekom in addition to the MIPv6/IPv4 component lossless data compression is required.

Industrial Benefit:

GANS is basically an 'up-stream-oriented' application (the Mobile Node is sending more data up-stream ...). Help to make 'up-stream-oriented' professional applications more visible and accepted.

3.3.4 QoS

3.3.4.1 **TAG**
Functional Requirement: -

3.3.4.2 **JMF**
Functional Requirement (revised): In the GANS target architecture a QoS framework both for the Best-Effort, BE, case and possible other architectures will be foreseen. For the better-then-E case, to possibly avoid complexity DiffServ was and will be the starting point.
Chosen Technical Solution: (revised): The present effort is concentrated on an initial “low-profile” solution for GANS – making GANS fit the low bit rate environment of GPRS.
Work Accomplished RUS has studied the present activities in the IETF concerning “access technology agnostic applications that use IP level QoS primitives to specify their QoS requirements” (ID “NSIS QoS Signaling Requirements from a Multi-access Wireless perspective”) and is participating as IST MobyDick partner in corresponding QoS work which, starting from DiffServ, is following the same “L2 agnostic” philosophy.
Anticipated Endpoint While in the time scale of 6WINIT no “L2 agnostic” “MultiAccess QoS framework” will become available, RUS/UKT will in the future leverage the results of MobyDick and similar projects.
Industrial Benefit: -

3.3.4.3 **DiffServ**
Functional Requirement: ‘DiffServ for GPRS’.
Proposed Technical Solution: see above
Work Accomplished: A Linux based DiffServ testbed was set up; Linux traffic control, tc for IPv6 was tested.
Anticipated Endpoint see above
Industrial Benefit: see above

3.3.5 Signalling Gateways – SIP

3.3.5.1 **SIP**
Functional Requirement: -

3.3.6 Multimedia Conferencing Gateways

3.3.6.1 **Multimedia Conferencing Gateways**
Functional Requirement: -

3.3.7 WAP Gateways

3.3.7.1 **WAP Gateways**
Functional Requirement: At present, the usage of handheld devices in the ambulance such the iPAQ are under consideration.
Proposed Technical Solution: Assuming an iPAQ-type of device in the ambulance, a Bluetooth connection and Web-to-WAP conversion as developed by the 6WINIT partner UMM will be studied.
Work Accomplished iPAQs were tested with IPv6/Linux.
Anticipated Endpoint no confirmed plans yet
Industrial Benefit: tbd

3.3.8 Access Network Provision

3.3.8.1 **GPRS**
Functional Requirement: At present, GPRS is provided by German T-Mobile. The IPv4 addresses provided are globally routable, the downstream – upstream slot relation is 4:1, i.e. the upstream capacity is less than 15Kbit/s.
Proposed Technical Solution: Ericsson's Multi-Access technology; see above.
Work Accomplished The usability of the present GPRS for GANS is still to be demonstrated.
Anticipated Endpoint tbd
Industrial Benefit: - see above

3.3.8.2 **WLAN**
Functional Requirement: see above 802.11
Proposed Technical Solution: see above
Work Accomplished see above
Anticipated Endpoint see above
Industrial Benefit: see above

3.3.8.3 **IPv4 WANs**
Functional Requirement: (At present) required for the GANS application.
Proposed Technical Solution: UKT - RUS are sufficiently well connected to the existing German and International Research infrastructure; the German T-Mobile GPRS service uses standard IPv4 addresses;
Outstanding Issues: -
Industrial Benefit: -

3.3.8.4 IPv6 WANs

Functional Requirement:

International connectivity to reach 6WINIT co-operation and demonstration partners.

Proposed Technical Solution:

RUS/UKT is using direct tunnels for demonstrations and has connectivity to 6Bone; 6Net connectivity is under consideration.

Work Accomplished

International tunnels for demonstrations (IST 2001, INET 2002) have been established, 6Bone connectivity was updated, no activities so far towards 6Net

Anticipated Endpoint

6Net connectivity

Industrial Benefit: -

3.3.8.5 UMTS

Functional Requirement:

Assuming “sufficient” upstream capacity, routable endpoint addresses for a “GPRS/UMTS” will be required.

Proposed Technical Solution:

Ericsson’s present MultiAccess solution readied for UMTS

Work Accomplished

RUS/UKT has started initial exchanges with Ericsson for a GANS demonstration using the forthcoming Kista testbed.

RUS as MobyDick partner has ordered the UMTS HW from MobyDick partner EURECOM for the planned Stuttgart UMTS testbed (TDD mode).

Anticipated Endpoint

tbd

Industrial Benefit: tbd

GANS would be an valuable demonstration for the capabilities of UMTS surpassing GSM.

3.3.9 Access Devices

3.3.9.1 **Terminals**
Functional Requirement: The GANS application requires the following terminals • Portable (Agilent) patient monitor connected via a serial link to the Mobile Node MN (notebook) in the ambulance; Ericsson's Multi-Access MIPv6 software. In the final scenario, the MN will also capture and deliver Audio and Video (so far handled by an additional machine) • In the Hospital-Home-network a workstation (notebook, PC) delivering the Vital Data from the ambulance and running the bi-directional audio and the unidirectional video from the ambulance (Linux) • An iPAQ-type of control terminal in the ambulance is under consideration (Linux; the existing serial connection must be replaced then by Bluetooth or WLAN) • In the target scenario, at the hospital a J2EE server (Linux) including JMS
Chosen Technical Solution: As a result of the co-operation with the 6WINIT partner Ericsson Research, their Multiaccess software (and follow-on development based on the University of Helsinki's Mobile IPv6 stack (HUT)) is used on Linux notebooks.
Work Accomplished "GANS terminals" have been successfully implemented on notebooks with the HUT-based Ericsson Research Multiaccess technology.
Anticipated Endpoint -
Industrial Benefit: A spectrum of devices is important to show the compatibility of 6WINIT solutions with a wide range of user needs.

3.3.9.2 **Security Devices**
Functional Requirement: The ideal requirements are for strong authentication and user certification (including access control role-based profiles).
Proposed Technical Solution: PKI's and possibly Smart Cards. Coupling the proposed architecture with strong authentication tools (e.g. using tokens or biometric devices) would be ideal.
Work Accomplished Study of the University of Murcia PKI system with respect to GANS requirements
Anticipated Endpoint tbd.
Industrial Benefit: tbd

3.3.10 Location Awareness

3.3.10.1 **Location Awareness**
Functional Requirement: At present still under consideration
Proposed Technical Solution: Initial discussions with 6WINIT partner VTT.
Work Accomplished no further work undertaken
Anticipated Endpoint tbd
Industrial Benefit: tbd

3.3.10.2 **IPv6-enabled J2EE application servers**
Functional Requirements: GANS assumes an IPv6 capable JEE-based application server including JMS
ChosenTechnical Solution: JBoss in an IPv6 capable version
Work Accomplished: Pursuing the target architecture, remote controls for Video, Camera and Vital Data, an integrated scenario for GANS over JMS on a JBoss and a SUN J2EE application server are running. The first version of GANS J2EE system was developed with a JBoss application server and SUN's J2EE 1.3.1 application server. It runs well in an IPv4-only or a dual-stack network. In an IPv6-only network a client can't find the server. An analysis with an Ethereal monitor shows JNDI starting with an IPv6-based GIOP request-reply exchange. But then all the following IIOP traffic exchanges are using IPv4; i.e., the current version of an application server doesn't support IPv6 completely. Using JDK 1.4, at present we have successfully compiled a JBoss 3.0 Qalpha version; the results concerning IPv6 are still to be seen.
Anticipated Endpoint: JDK 1.4 supports IPv6 completely. The current application servers are based on JDK1.3.1. The anticipated endpoint is to get an JDK1.4 based application server.
Outstanding Issues: Waiting for SUN's announcement for a new version of an IPv6 capable application server and at the same time testing the JDK 1.4-compiled JBoss system.
Industrial Benefit: J2EE-based application servers as a core element of many industrial applications in an IPv6 environment would be a strong argument for the new protocol.

3.3.10.3 **JMF**
Functional Requirement: In GANS, a video and a full duplex audio communication between an ambulance and the clinic are conceived.
Proposed Technical Solution: The current JMF version does not support any QoS mechanisms, we can only try to transmit data with e.g. desired bit rate, frame rate, etc. At the operating system level Support for Diffserv is already integrated into Linux 2.4 kernels. We are using SuSE Linux 2.4.18, may have to reconfigure and rebuild our kernel in order to enable it
Work Accomplished: Updated Linux to SuSE 8.0. SuSE 8.0 is the first Linux edition to present the new sound drivers ALSA version 0.9. A full-duplex audio is running over IPv6 is running.
Anticipated Endpoint: Audio/Video full duplex on Linux over MIPv6 using a layer 2 agnostic QoS philosophy.
Outstanding Issues: Improvements of audio quality (mainly delay); lower bandwidth requirements; develop QoS framework
Industrial Benefit: Enable the development of media streaming applications in Java in mobile environments

3.4 The Vital Data Transmission System

3.4.1 Overview

The vital data transmission is one component of GANS developed by RUS. It consists of an object - oriented software which is written in Java SDK 1.4 and is able to run on a Linux platform.

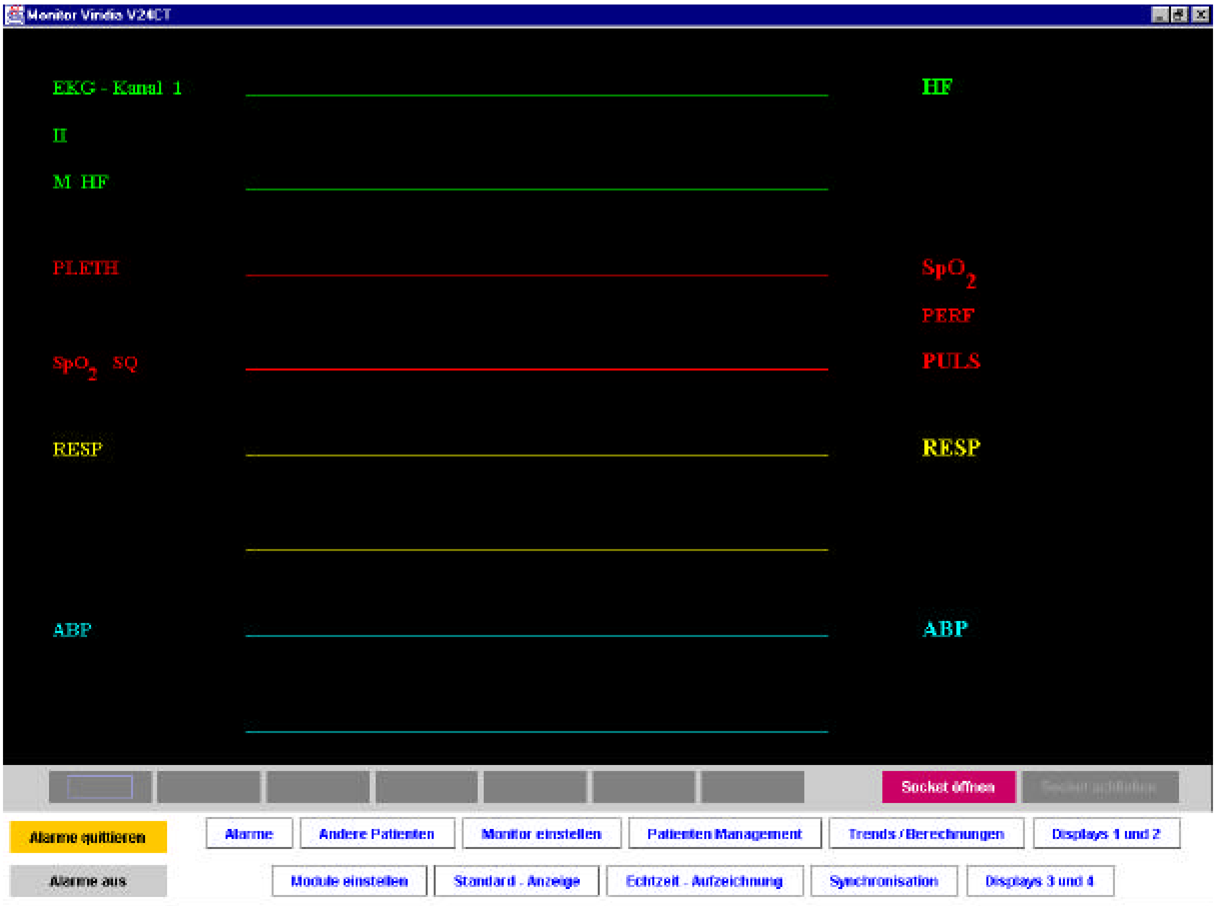

Figure 36 : The GUI of the application in the remote hospital

Figure 36 shows the graphical user interface (GUI) of the application in the GANS centre . The GUI is able to show 4 wave messages and the corresponding numerical messages simultaneously in real time. The coloured horizontal lines are the displays within the wave messages are painted. Each vital parameter has its own colour and is described by the labels on the left side. The numerical values of each vital parameter are painted on the right side of the screen. These numerical values are derived from the wave message. In this figure one can see the displays for the electrocardiogram (ECG) of channel 1 (green), the oxygen saturation (red), the respiration (yellow) and the invasive blood pressure (light blue). Some of the wave messages can maximally show three different types of numerical values.

3.4.1.1 The presentation of the vital data

Figure 37 : The transmitted wave messages and numerical messages

Figure 37 gives an impression of the vital data transmission. The wave messages and the numerical messages are drawn on the GUI. The doctors of the Guardian Angel System have now the same information concerning the vital data as the medical staff who takes care for the patient in the emergency situation. In this figure the parameter module for the invasive blood pressure (ABP) is not activated.

3.4.1.2 The usage of the GUI

The usage of the GUI is simple and comfortable. The components of the GUI can be activated by mouse clicks. Apart of the presentation of the vital data the GUI contains further graphical components with the functionality to configure the transmission of the vital parameters. In regard to the implementation of this functionality the GUI consists of several layers containing these components. This means for example that a further menu will be opened after clicking a button with the mouse and that a previous opened menu will disappear. The GUI of this application has been implemented according the GUI of an original patient monitor. The following figures give an impression of the mentioned functionality :

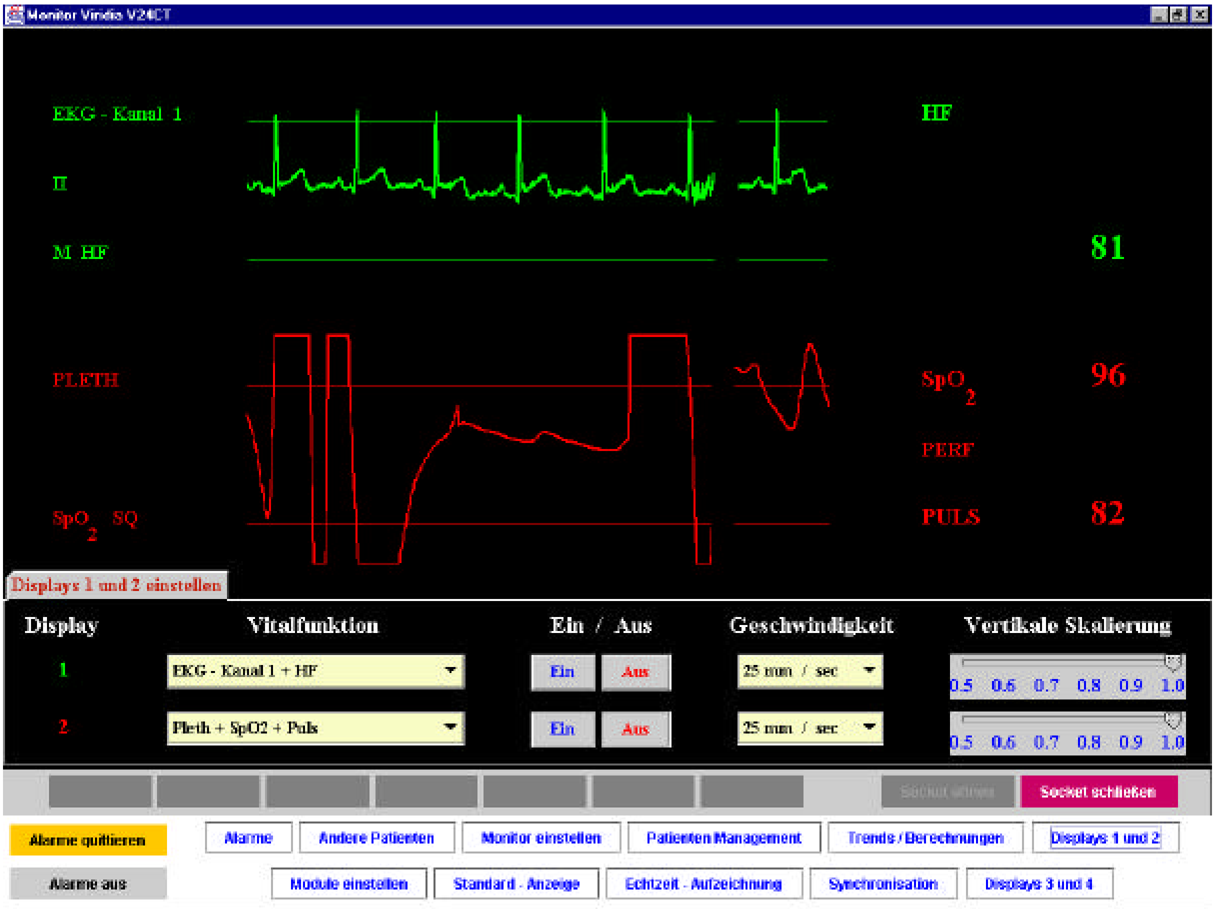

Figure 38 : The configuration for the vital parameters of the two upper displays

Figure 38 shows a graphical component in order to influence the presentation of the corresponding vital parameters which are drawn in the upper two displays. This component includes buttons, list fields and sliders to realise several features. Each display is identified by a number which has the same colour like the painted wave message. In addition, each display has its own graphical components. The list fields are implemented as combination fields and allow always a single selection of an item. The combination fields on the left are responsible for the selection of a vital parameter which has to be painted in the display. Each vital parameter consists of a wave message and one or several numerical messages. Some wave message can have maximally 3 numerical messages. It is also possible to vary the number of the numerical wave messages of a vital parameter by the selection of the corresponding item in the combination field. A mouse click on the right button with the red label will detune the current vital parameter and stop its data transmission. In contrast to this fact a mouse click on the left button with the blue label will tune the selected vital parameter and start its data transmission. The combination field on the right is responsible for the selection of the velocity of the painted wave message. There are four different values for the velocity of such a wave message :

- 5 cm / sec
- 2.5 cm / sec
- 1.25 cm / sec
- 0.625 cm / sec

The slider on the right side enables the vertical scalability of the wave message. This means, that the vertical extension respectively the height of the painted wave message can be adjusted in dependency of the position of the slide control. This is particularly important for the presentation of the electrocardiogram (3 - Channel - ECG). All these kinds of selections and regulations can be done during the vital data transmission. As a result a user is able to influence the presentation of the vital parameters during runtime.

Figure 39 : The configuration for the vital parameters of the two lower displays

Figure 39 shows a graphical component in order to influence the presentation of the corresponding vital parameters which are painted in the lower two displays. The functionality of the components is identical according to the previous mentioned facts.

3.4.1.3 The tunable vital data

Currently, the vital data transmission of the following wave messages is implemented :

- electrocardiogram - channel 1 (ECG - 1)
- electrocardiogram - channel 2 (ECG - 2)
- electrocardiogram - channel 3 (ECG - 3)
- pleth
- respiration (Resp)
- carbon dioxide of the respiration (CO2)
- invasive blood pressure (ABP)
- central venuous pressure (CVP)

In addition the vital data transmission of the following numerical messages belonging to the previous mentioned wave messages is implemented, too :

- heart rate (ECG - 1, ECG - 2, ECG - 3)
- oxygen saturation of the blood (Pleth)
- pulse rate (Pleth)

- relative perfusion (Pleth)
- respiration (Resp)
- endexspiratory partial pressure of carbon dioxide (CO2)
- inspiratory partial pressure of carbon dioxide
- respiration rate as numbers of breaths in a minute
- invasive blood pressure (ABP)
- central venuous pressure (CVP)
- non invasive blood pressure (NBP)

The abbreviations in the brackets refer to the allocation of the numerical message to the wave message.

3.4.1.4 Some more features of the application

Synchronisation of the wave messages :

The graphical presentation of the four painted wave messages is synchronised. This means that there is no translational displacement between the wave messages that are running with the same velocity. There is an automatic synchronisation which is implemented by a specific algorithm. When the wave messages are running through from the left to the right on their displays the automatic synchronisation is produced after every fourth pass. This is always at the beginning of a new pass when the cursor is on the left end of the display. A user does not notice this automatic synchronisation. After the close of an opened menu the wave messages might have a translational displacement. Now the wave messages can be synchronised manually by clicking the button with the label “Synchronisation”. The click on this button calls the same synchronisation method and the user doesn’t need to wait for the next automatic method invocation.

Presentation and storage of the trend values :

The values of the numerical messages can be stored as functions of the time. These values are also called the trend values of the vital parameters. This application is able to represent the trends both as trend table and as well as trend diagram. The trend table shows the numerical values of the vital parameters and their current time as list represented by rows and columns. The trend diagram shows the same values by a graphical representation as functions in a coordinate system. The user can switch from the trend table to the trend diagram and vice versa by clicking some buttons. The graphical representation in the trend diagram is supported by six different zoom steps. The user has also the possibility to move forward and backward on the horizontal time axis. In addition to this features the trend values of the vital parameters are stored in an external relational database which is connected to the application via the JDBC - interface. The trend table of the vital parameters is shown in Figure 40 and the trend diagram in Figure 41.

Implementation of further vital parameters :

The implementation of further vital parameters is very easy. The corresponding implementation is based on a serial interface protocol called MECIF - Medical Computer Interface Protocol. In the scope of this protocol every vital parameter respectively every kind of tunable message has got its own specific key numbers like the sourceID, the channelID, the channelNo, the messageType, the message layer and so on. The first step is the determination of the request message and the response message for a certain vital parameter. This is realised by the correct composition of this key numbers in suitable data structures. In several methods these requests and responses have to be analysed.

The design of this application allows a very simple and comfortable upgrading with regard to the implementation of additional vital parameters and graphical components. As a result of the strict object - oriented design the application is expandable.

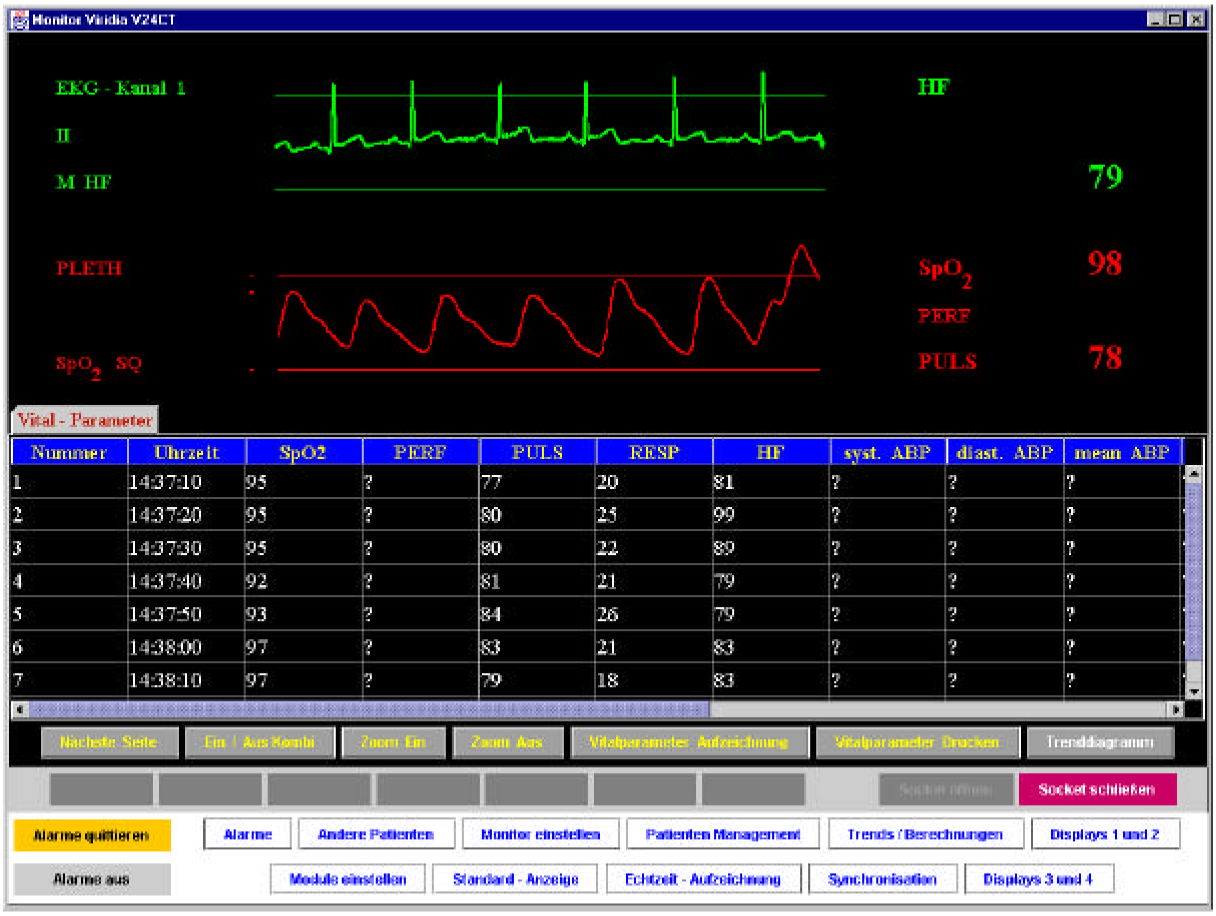

Figure 40: The trend table of the vital parameters

Figure 41: The trend diagram of the vital parameters

3.5 Early experiences from deployment, use and evaluation

3.5.1 Exploitation and dissemination

As a part of the 6WINIT project, several efforts were undertaken to introduce the idea of the Guardian-Angel-System to a world wide audience. These actions were also performed in order to find partners for both scientific projects and commercial exploitation of the project idea.

We introduced the GANS Project in the European Conference Teleinsula "Information Society and Sustainable Regional Development" in Puerto de la Cruz, Tenerife, Spain, on April 10th – 11th with the specific goal to develop concepts for the integration of insular and outermost regions in the terms of technological and telecommunication connectivity.

The GANS was presented at medical conferences for "Risk management" in Heilbronn, Germany, on April 27th 2002 for office-based anaesthetists and delegates of several German health insurance companies who showed interest in the commercial use of the system. On the German Congress of Anaesthesiology ("Deutscher Anästhesie Kongress") in Nuremberg, Germany, June 22nd, 2002, the issue has been presented to the international audience of anaesthetists all over the world.

Concerning further dissemination and exploitation matters, the GANS was introduced to the Slovene regional development agencies in Rogaska Slatina, Slovenia, on June 20th, 2002, where clinical co-operation was discussed to set up the GANS in a fixed environment between different hospitals connected to a centre in a University Hospital.

Several efforts were undertaken to continue the publication of the idea of our project. German TV was invited to join the INET 2002 demo in the Centre for Patient Safety and Simulation at UKT, several newspapers and press agencies (“Deutsche Presse Agentur” (dpa)) were interested in the subject as well as the most read medical newspaper in Germany, the “Deutsches Ärzteblatt” which is preparing an article about the Guardian Angel System.

As a result of the dissemination plans, a cost calculation was made for the establishment of a GANS in a fixed environment between several hospitals and a Guardian Angel Centre. The equipment of 100 beds for connection to a GANS-Centre will mean an effort of approximately €90.000 per year. Due to income of GANS rent by the hospitals connected and the money saved by the reduced number of medical complications which are usually followed by longer stay in hospital, insurance pay outs and expenses for possible court claims after fatal incidents, there would be a positive balance of around € 400.000 per year.

3.5.2 The proof of concept study

At UKT, a study for the proof of the GANS concept has been prepared in order to set up a clinical testbed for telemedical help in the fixed environment of our simulation centre. This will be used to avoid endangering patients before both the real benefit for patient safety and proof of technical security has been clarified scientifically. After the end of study and analysis of results, the approval of ethics committees, medical associations and health insurance providers, we 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.

Our work in co-operation with RUS in the last part of the 6WINIT project will include clinical tests of the GANS in UMTS testing areas in Stuttgart or Kista with a mobile patient simulator “SimMan” in an ambulance car moving on the testbed campus.

3.5.3 Conclusion

The Guardian Angel System concept as such is ready for use in the real world of all fields of modern medicine where medical emergencies are likely to happen: Emergency rooms, operation theatres, intensive or intermediate care units and – in the future – in an mobile environment for ambulance cars as well. An enormous impact can be reached for patient safety and quality of life. Finally, it also seems promising to reduce health care costs significantly.

4 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
AAA	Authentication, Authorisation and Accounting
ACC	Academic Computer Centre "Cyfronet", a part of the UMM
ACL	Asynchronous Connectionless Links
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
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
BSS	Base Station System
BU	Binding Update
CA	Certificate Authority
CAS	Clinical Appointment System
CBR	Committed Bandwidth Rate

CCU	Clinical Care Unit
CEN	Comit, Europ,en 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
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSP	Cryptographic Service Provider
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
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
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
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
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
HLR	Home Location Register
HMIP	Hierarchical Mobile IP
HTML	HyperText Mark-up Language
HTTP	HyperText Transfer Protocol
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
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
MMUSIC	Multiparty Multimedia Session Control
MN	Mobile Node
MSC	Mobile Service Centre
MT	Mobile Terminal
Mb/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
NFS	Network File System
NHS	National Health Service (United Kingdom)
NRN	National Research Network
O&M	Operations and Management
OCSP	Online Certificate Status Protocol
OSGi	Open Services Gateway initiative
PAN	Personal Area Networking
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
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PS	Paging Servers
PSK	Phase Shift Keying
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
RMD	Resource Management in DiffServ
RMI	Remote Method Invocation
RODA	Resource Management in DiffServ On DemAnd
ROHC	Robust Header compression
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSVP	Resource ReSerVation Protocol

RTCP	RTP control protocol
RTP	Real Time Transport Protocol
RTSP	Real Time Streaming Protocol
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
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SGSN	Serving GSN
SGW	(1) Signalling Gateway
	(2) Security Gateway
SIIT	Stateless IP/ICMP Translation Algorithm
SIP	Session Initiation Protocol
SN	Service Network
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
SPD	Security Policy Database
SRTP	Secure Real Time Transport Protocol
SSL	Secure Socket Layer
SecGW	Security Gateway
TB	Tunnel Broker
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TE	Terminal Equipment
TEID	Tunnel Endpoint IDentifier
TEIN	TransEurasia Information Network
TLA	Top Level Aggregator
TLS	Transport Layer Security
TS	Tunnel Server
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 Tuebingen
UMM	University of Mining and Metallurgy (Krak¢w, 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
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
WCDMA	Wideband Code Division Multiple Access
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