IST-2000-25153

Deliverable D4

"Review of status of early relevant standards"

Contractual Date of Delivery to the European Commission:	**31 December 2001**
Actual Date of Delivery to the European Commission:	**January 2002**
Editor(s):	**Sathya Rao (Telscom)**
Participant(s):	**WP2 members**
Workpackage :	**2**
Title of Deliverable:	**Review of status of early relevant standards**
Security:	**R/Pub**
Nature:	**O**
Version:	**Final**
Number of pages:	**26**

Abstract: This deliverable identifies the Wireless internet and related IPv6 standards. The status of such standards is reviewed and ongoing work is identified which may impact the work progress in the 6WINIT project.

Keywords: Mobile IP, IPv6, Wireless internet, Standards

Table of Contents

1 INTRODUCTION

In the context of the 6WINIT project, the main standards organisations that are being tracked are IETF, 3GPP, UMTS Forum, ETSI, and ITU.

IETF is the main specifications development group for IP technology, including both IPv6 and the related protocols. ETSI provides a platform for testing during the interoperability events organised regularly. 3GPP is the main working group working for early specifications development of 3rd generation mobile networks with IPv6 as a chosen protocol. UMTS is a forum for discussing and dissemination of 3rd generation mobile networks, but the detailed technical work is being done in the 3GPP and 3GPP2 projects; because the latter has very frequent meetings in the US, it was not possible to track it very intensely. While the ITU includes members of all the other bodies, it is less appropriate for most of the 6WINIT work.

We do not attempt to tie the standards described here with specific activities in the technical work-packages. However the interest in this work by the project partners is just because they require many of them in their work.

2 STATUS OF STANDARDS

The IETF working group for Next Generation Internet Protocol (IPng) is responsible for developing the IPv6 standards within IETF. The issues range from header format and functionalities association, addressing and routing issues, Quality of service and security, transition mechanisms, and design issues for interworking across inter-networks.

IPv6 specifications development has become a central issue in recent meetings of IETF. There are already a number of RFCs available which have been approved and others are being produced.

Similarly the GPRS Forum, UMTS forum and 3GPP bodies are driving the mobile IP standards incorporating IPv6 into future networks. Within 6WINIT the project is following both these two areas, with the ongoing discussions.

2.1 IPv6 standards

Many issues related to IPv6 have been finalised and the standards for minimum implementation of IPv6 production networks is possible today with the approved standards. However, there are further specifications addressing the address allocation (as a policy issue), renumbering, DHCP, DNS, anycast, multihoming, autoconfiguration, security and quality of services issues are yet to be resolved. These issues are presently discussed in the IPv6 working groups in the framework of IETF.

ETSI is supporting early testing of implementation of these standards by organising interoperability testing among multivendor equipment available from different sources.

2.1.1 RIPE: IPv6 address allocation issues

RIPE-196 is the European version of the policy document which attempts to govern the allocation of IPv6 address space for the RIRs. In the IPv6 classful addressing model, subTLAs are "divisions" of a TLA used during the initial period of IPv6 takeup. They have three important properties:

- They appear in the global routing table.
- They are very large: A /35 starting allocation is (potentially) 8192 networks with up to 64kK IP nodes of a subnet on a site; each of these contains as many hosts as the current Internet.
- One can plan the network with them, without the need for renumbering.

Another of the ambitions of IPv6 is to make network renumbering easier. Some aspects of that behaviour are still undefined, however, and the quality of IPv6 stack in (for example) 3G terminals is still up for debate.

SubTLAs are initally a /35 allocation. There is also another boundary at /48, for "sites", which effectively reduces it by another 16 bits to 13 bits. 13 bits allows you to make 2^{13} (=8192) assignments.

Issues with size of IPv6 allocation

There are three problems with the subTLA allocation guidelines as they stand.

1. /48s are now almost the default allocation for an end-node.

   Some of the assumptions in the document do not bear up under the change in community consensus about the numbering of end-nodes. For example, there is strong momentum within the RIPE/APNIC community to allocate nodes with the capability of supporting routing a /48 block - i.e., consider them a "site" in IPv6 terminology. This kind of thinking extended to (for example) 3G mobile phones means that providers wishing to account for a few million phones in their addressing plan have much less space than they thought they did to create a routing hierarchy.

2. The space is not large enough to create a world-wide routing hierarchy

   For very large entities looking to create a hierarchy across multiple countries, the subTLA bit width is not actually sufficient. Particularly for 3G mobile operators, who may have to assign a /48 to end-node phones with Bluetooth, ethernet, or other routing capability.

3. The 80% usage rule does not combine well with aggregation

   The rules state that a LIR or an ISP can ask for more address space once they reach 80% utilisation of their /35, in which case the additional address space will come from the reserved /29. However, when you hit 80% usage of your /29 your next assignment will not be from the same aggregation block.

Suggestions made for improving RIPE-196

Recommendation 1

- Accept the /48 numbering recommendation for hosts that may need subnetting. Other hosts get /64s, or /128s depending on what they will be doing.

Recommendation 2

- If the registries still want hierarchical address assignments and support giving a /48 to customers, then change the subtla initial allocation to /29 rather than /35.

Recommendation 3

- Change 6 month 6bone membership to 3 months OR For the post-bootstrap period, change the "experience with IPv6/6bone" criterion to be "experience with IPv4".

Recommendation 4

- Set up a task force to look into the matter of subTLA allocation sizes. Ask the registries what they are looking for from subTLA holders. Ask the subTLA holders what they would like from the RIRs. Build consensus in community and produce further document. This effort should go ahead whether or not these short-term fixes are successful.

2.2 Mobile IP standards

The Mobile IP Working Group (MIP WG) has developed routing support to permit IP nodes (hosts and routers) using either IPv4 or IPv6 to seamlessly "roam" among IP subnetworks and media types. The Mobile IP method supports transparency above the IP layer, including the maintenance of active TCP connections and UDP port bindings. Where this level of transparency is not required, solutions such as DHCP and dynamic DNS updates may be adequate and techniques such as Mobile IP not needed.

The WG moving forward will focus on deployment issues in Mobile IP (MIP) and provide appropriate protocol solutions to address known deficiencies and shortcomings. For example, the wireless/cellular industry is considering using MIP as one technique for IP mobility for wireless data. The working group will work to gain an understanding of data service in cellular systems such as GPRS, UMTS, CDMA2000, and interact with other standards bodies that are trying to adopt and deploy MIP WG protocols in these contexts. In order to provide a complete solution and a set of protocols that can be used as a roadmap for widespread deployment, the following work needs to be accomplished by this WG:

- Use of NAIs to identify mobile users/nodes.
- Specifying how Mobile IP should use Authentication, Authorisation and Accounting (AAA) functionality to support inter-domain and intra-domain mobility.
- Develop solutions for IPv4 private address spaces for the scenarios needed for deployment.
- Documenting any requirements specific to cellular/wireless networks.
- QoS in the mobile IP environment using diff-serv and/or int-serv/RSVP.
- Location Privacy.

The Working Group will ensure that solutions proposed for these problem domains are suitable for IPv4 and IPv6 respectively.

2.2.1 MIPv6

Mainly due to scalability issues based on the use of IPSec for securing MIPv6 control information the IESG refused the MIPv6 draft progressing to standard.

In response to this, the IETF MIP WG removed the IPSec part in the new MIPv6 draft version 14 and introduced a new destination option containing authentication data. While this draft exactly specifies over which part of the MIPv6 control messages this authentication data has to be calculated, it still leaves the important question open about how this authentication data should be calculated, that is draft version 14 defines the packet fields for the authentication data, but doesn’t specify how to fill them.

A discussion in the WG also underlined, that people still want to be allowed to make use of the previous IPSec solution. This would work for example in scenarios, where scalability is not a major issue, e.g. if a company network supports MIPv6 but allows its Mobile Nodes only roaming inside the company network. In such a scenario a trust relationship among all Nodes inside the company network can be achieved in advance. Furthermore people also want to keep the IPSec approach as one alternative to be able to use it when the Internet will have a Public Key Infrastructure (PKI).

Having both solutions, the generic authentication data in a destination option as well as the IPSec approach, would require the specification of a mechanism to decide case by case, which one of the both possibilities for authentication should be used.

These issues, which are currently being discussed in the MIP WG, should be addressed in the new draft version 15, which is expected to be distributed soon officially.

2.2.2 Access Networks

6WINIT addresses end-to-end services across a mobile internet. Different types of access networks can be used including the fixed networks. The project addresses more of wireless access networks. In this context wireless LAN based on 802.11b and Bluetooth access will be studied experimentally.

Wireless LAN

802.11 is a family of wireless networking protocols from the IEEE.

The most popular of these is the 802.11b standard which has been in commercial use since 1999. It has a maximum theoretical throughput of 11 Mbps, which is much faster than broadband solutions like DSL or cable modems. 802.11 Wavelan technology supports native IPv6 connectivity without any special adaptation. A higher speed technology, 802.11a, is under study; this is not expected to lead to many products in the time-scale of 6WINIT. At present the family based on 802.11 is the most popular wireless LAN being deployed.

Bluetooth

Bluetooth is a wireless communication technology using a frequency hopping scheme in the unlicensed 2.4 GHz ISM (Industrial-Scientific-Medical) band. Two or more Bluetooth (BT) units sharing the same channel form a piconet. Within a piconet a BT unit can have either of two roles: master or slave. Within each piconet there may be only one master (and there must always be one) and up to seven active slaves. Any BT unit can become a master in a piconet.

The Bluetooth specification consists of different profiles for different applications. So far, only one profile exists which explicitly supports IP (v4 or v6). This is the LAN access profile, used between a laptop/PDA etc. and a LAN access point.

The dial-up profile can also be used to transport IP. This profile is used between a laptop/PDA etc and e.g. a cellular phone or a modem. It also uses RFCOMM, and AT commands for dialling and control. It does not specify what protocols are used on top or RFCOMM, but clearly, PPP can be used as over any serial link/modem connection.

In addition to this, a new profile will be published soon which is designed specifically for IP networking, the Personal Area Networking (PAN) profile. This profile does not use RFCOMM, but instead defines a new protocol, Bluetooth Network Encapsulation Protocol (BNEP), which is an Ethernet emulation layer. This means that any protocol that can run over Ethernet will be supported, such as IPv6. One important function in the PAN profile is that the master in a piconet will forward packets between its slaves, both unicast packets from one slave to another, and broadcast packets from one slave (or itself) to all the others, thus hiding the point-to-point nature of Bluetooth and making one piconet look like an Ethernet link.

2.2.3 Wide Area Networks

The mobile internet addressed by the 6WINIT project can use all kinds of wide area networks: fixed, wireless or satellite. However, the project addresses mainly GPRS (which is available in many EU countries) and UMTS (when available) for trials.

GPRS

GPRS is a new service designed for the Global System for Mobile Communications (GSM) networks. GSM is a digital cellular technology that is used worldwide, predominantly in Europe and Asia, with current estimates of 400 million subscribers and growing. GSM is the world's leading standard in digital wireless communications.

GPRS is standardised by the European Telecommunications Standards Institute (ETSI). The most common application of GPRS is expected to be Internet/intranet access. GPRS solution enables mobile wireless service providers to supply their mobile subscribers with packet-based data services in GSM networks with permanent connection to the network.

GPRS introduces the following two new major network elements:

- SGSN—Sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates between the MS and the GGSN
- GGSN—A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks

UMTS/3GPP

UMTS is one of the major new third generation (3G) mobile systems being developed within the framework which has been defined by the International Telecommunications Union (ITU) and known as IMT-2000 (International Mobile Telecommunications).

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement among a number of telecommunications standards bodies such as ARIB, CWTS, ETSI, T1, TTA, and TTC.

The scope of 3GPP is to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support (i.e. Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes).

3GPP has produced all necessary specifications adopted by ETSI and regional standards groups. The full list of 3GPP specifications can be seen at http://www.3gpp.org/

3GPP specifications are continually being enhanced with new features. In order to provide developers with a stable platform for implementation while at the same time allowing the addition of new features, the 3GPP uses a system of parallel "releases". At present the Rel-4 has been frozen; Rel-5 is expected to be released during March 2002, with enhanced features.

UMTS is being standardised by the European Telecommunications Standards Institute (ETSI) in the IMT-2000 framework, in co-operation with other regional and national standardisation bodies around the world to produce the detailed standards to satisfy growing market needs for global roaming and service availability. IMT-2000 has been defined by the ITU as an open international standard for a high capacity, high data rate mobile telecommunications system incorporating both terrestrial radio and satellite components.

2.3 Health Informatics standards

The 6WINIT London Demonstrator focuses on the distributed access to EHR information.

The major health informatics standards applicable to EHR representation and secure communication originate from CEN (Comité Européen de Normalisation). Technical Committee 251.

2.3.1 ENV 13606: EHCR Communication (1999)

This four-part pre-standard[i] (ENV) governs the representation of EHR information as it might be communicated between two repositories or between a client and a server. In its four parts it defines:

- the object model that must be used to represent the EHR;
- a set of term lists that must be used to populate key attributes defining the classes of information being communicated;
- a set of rules and an information model governing how access control requirements should be specified;
- a set of message specifications to support message-based exchange (EDI) e.g. using EDIFACT or XML.

CHIME (UCL) has been at the forefront internationally in the specification of information models needed to underpin the capture and communication of electronic health records (EHRs). The R&D results of research projects involving CHIME have largely underpinned this standard, and the UCL EHR middleware components closely match the standard. CHIME has been invited to lead a new CEN Task Force to revise ENV 13606 based on its experience in this field, to develop a definitive standard (EN). As this new standard and the UCL components evolve forward, the London Demonstrator is likely to provide a unique reference implementation of the new standard.

2.3.2 Health Level 7

This US based international organisation, generally known as HL7, is responsible for the most widely adopted standard for message-based communication in healthcare. HL7, whose message specifications were first published in 1988 as an industry standard, was awarded Standards Development Organisation (SDO) status in 1993 so that newer versions of the specification are official ANSI standards. The messages primarily support the interoperability of components of a hospital information system and purchaser-provider contractual communications. The most recent version, HL7 version 3 Reference Information Model (RIM), now in final draft form, has been extended to meet some of the requirements of clinical shared care. Although sometimes regarded as an alternative EHR information model, it is primarily a process model of health care activity and is not a record model.

The CEN Task Force referred to above will include harmonisation with HL7 within its terms of reference.

2.3.3 Data Protection Legislation

The processing of personal health data must comply with the 1995 EU Directive[ii] and the 1997 Council of Europe Recommendations[iii] regarding its acquisition, storage, communication and analysis. Each member state has passed national legislation to reinforce these instruments, such as the 1998 Data Protection Act in the UK. In the UK it is also necessary to comply with the Caldicott Report[iv] recommendations governing the use of patient identifiable data inside the NHS, between organisations.

Although conformance with the act is in practice still variable, the UCL R&D agenda includes the prototyping and evaluation of components that will permit the rigorous adoption of these principles. Many of these will be incorporated within the London Demonstrator during year 2 of 6WINIT, even though the pseudonymous nature of the demonstration data would not legally require it.

2.3.4 Security Standards

There are several CEN standards relating to the secure handling of EHR information. The key ones are listed below; in practice many of the general security requirements are similar to those adopted by other industry sectors. They are therefore not discussed further in this report.

- Algorithm for Digital Signature Services in Health Care, ENV 12388:1996
- Security Categorisation and Protection for Healthcare Information Systems, ENV 12924:1997
- Secure User Authentication for Health Care: Management and Security of Authentication by Passwords, ENV12251:2000
- Security for Healthcare Communication ENV13608:1999
- Secure User Identification for Healthcare - Strong Authentication using microprocessor cards ENV 13729:1999

2.3.5 UK Security Policy

Health care organisations within the UK NHS have been encouraged to produce a security policy and to ensure it is regularly audited. In the early 1990s the NHS published its own security policy, but has recently advocated the use of ISO 17799[v] as the blueprint for organisational security policy.

CHIME is working with colleagues in UCL Computer Science to develop a security policy governing its demonstrator EHR deployments. In practice, however, real EHR implementations will be governed by the security policy at each installation site.

2.3.6 Networks

The UK NHS net has been described in 6WINIT Deliverable 3 Section 3.8.2, together with the technical problems with utilising it with IPv6. The 6WINIT project has agreed not to mount a demonstrator inside the NHSnet firewall, although client access from inside a hospital is proposed.

The NHSnet is therefore not discussed further here.

3 ONGOING WORK

3.1 Interaction of Transition Mechanisms

The ngtrans working group of the IETF has made the INTERACTION draft (draft-krampell-v6transition-interaction-01.txt) a current work item.

This document discusses interaction of transition mechanisms that can be involved during the transition phase where both IPv4 and IPv6 will be concurrently used. On one hand, several transition mechanisms have been defined to solve different transition issues. On the other hand, one can face multiple transition issues and may have to use several transition mechanisms at the same time.

Since an applicability scope is attached to each transition mechanism, specifying where the mechanism applies, i.e. host, domain or global, this memo aims at identifying cases where multiple transition mechanisms may be involved within the same scope, and what can be the interaction effects between them.

As more and more transition mechanisms are deployed in the different local networks, the likelihood increases that a packet undergoes more than one transition on its way from source to destination. This may lead to unexpected effects and in the worst case make it unable for the network connection to become established.

This work will guide the administrator of a network domain to choose the appropriate transition mechanism and pinpoint the possible side effects.

3.2 3GPP-IPv6 Design Team

The joint 3GPP/IETF design team was founded during a joint IPng working group and 3GPP session at the IPng interim meeting in Redmond May 30th – June 1st 2001.

Goals:

- Review 3GPP's current usage of IPv6 and make recommendation for improvements
- Write ID to be submitted to IPv6 w.g.

Non-Goals:

- Redesign of 3GPP architecture / protocols

Topics

The following topics were announced during a status presentation of the design team at the 51th IETF in London, August 2001:

- Allow the use of standard IPv6 implementations in 3GPP usage scenarios
- Addressing
  - ➢ Single address per PDP context (current)
  - ➢ Prefix per PDP context
    - Per device
    - same prefix for all PDP contexts for same device
    - shared among PDP context's for many devices
  - ➢ Node able to create multiple addresses
  - ➢ Static or temporary IPv6 addresses

- Model for support of devices behind handset
  - Router, bridge, proxy
- DNS
  - Locating a DNS server
  - Handset address in DNS
- Security
- MTU
- Issues left to implementers in 3GPP specifications
- Transition
  - IPv6 only, dual stack, etc
  - Communication with IPv4 internet
- Remote Management
  - MIB support

The design group has issued a first draft *"Recommendations for Ipv6 in 3GPP Standards"* (draft-wassermann-3gpp-advice-00.txt, November 2001).

This draft deals primarily with the IPv6 address assignments as specified in 3GPP and by the IETF.

3GPP has defined a very narrow approach to IPv6 address configuration. Address auto-configuration is based on PPPv6 and therefore works similarly to dialup networks. Each primary PDP context gets a single 64-bit identifier and /64 prefix assigned by the GGSN. Handsets and attached equipment may request multiple PDP contexts. The design group now gives the recommendation to 3GPP to make the address configuration process more compatible with the current defined praxis for IPv6. This would make it easier to base implementations in handsets and equipment on standard IPv6 stacks. The recommendation takes into account the specific requirements of mobile equipment (many devices, scarce bandwidth on air interface).

Recommendations:

1. Multiple prefixes should be allowed for each primary PDP context

2. A given prefix must not be assigned to more than one primary PDP context to allow 3GPP nodes to use multiple identifiers under those prefixes including randomly generated ones. This would effectively treat every single 3GPP node as a single /64 subnet and would allow standards-compliant IPv6 nodes to connect to the Internet through 3GPP handsets without modification.

4 6WINIT Contributions to Standards

6WINIT project is very active in both technical standards (IETF) and Health sector standardisation. Several of its workers participate regularly in IETF and EHR standards meetings and have made several contributions. The list below shows the details of the contributions reported officially; it includes several contributions to IETF from 6WINIT members:

Topic	Journal/Conference	Status
A Message Bus for Local Coordination	draft-ietf-mmusic-mbus-transport-04.txt	

The local Message Bus (Mbus) is a simple message-oriented coordination infrastructure for group communication within groups of co-located application entities. The Message Bus comprises three logically distinct parts: a message transport infrastructure, a structured message hierarchy, and a general purpose addressing scheme. This document specifies message addressing, transport, and security procedures and defines the message syntax for the Mbus. It *does not define application oriented semantics and procedures for using the message bus.*

A Message Bus for Local Coordination	IETF (Internet Draft draft-ietf-mmusic-mbus-transport-06.txt)	A

The local Message Bus (Mbus) is a simple message-oriented coordination infrastructure for group communication within groups of co-located communication peers. The Mbus provides automatic location of communication peers, subject based addressing, reliable message transfer and group communication. The protocol uses an IP multicast group as a common communication channel between peers. The scope of this group is strictly limited to link-local communication. This document specifies the Mbus protocol, i.e., message syntax, addressing and transport mechanisms.

Advice for Internet Subnetwork Designers	Internet Draft draft-ietf-pilc-link-design-06.txt	A

This document provides advice to the designers of digital communication equipment, link layer protocols and packet switched subnetworks (collectively referred to as subnetworks) who wish to support the Internet protocols but who may be unfamiliar with Internet architecture and the implications of their design choices on the performance and efficiency of the Internet.

An Mbus Profile for Call Control	draft-ietf-mmusic-mbus-call-control-00.txt	

This document defines an Mbus application profile for call control services. This application profiles is designed to provide the most common basic services of call signaling protocols like SIP, H.323/Q.931 related to call setup and tear downbut also defines a set of optional Mbus commands for supplementary services. The targeted applications include gateway and endpoint decomposition and remote controlling of call signalling engines.

An Mbus Profile for Internet Appliance Control	draft-kutscher-mbus-ipac-00.txt	

This document discusses scenarios for the control of Internet Appliances -- Internet hosts with with specific user functionalities - using the Mbus protocol. A first sketch of an Mbus application profile for controlling Internet appliances ispresented, describing mechanisms for controlling a group of co-located appliances without the need for central controlling entities.

Extended RTP Profile for RTCP-based Feedback (RTP/AVPF)	IETF - draft-ietf-avt-rtcp-feedback-01.txt	A
Extended RTP Profile for RTCP-based Feedback (RTP/AVPF)	IETF - draft-ietf-avt-rtcp-feedback-01.txt	A

Real-time media streams are not resilient against packet losses. RTP [1] provides all the necessary mechanisms to restore ordering and timing to properly reproduce a media stream at the recipient. RTP also provides continuous feedback about the overall reception quality from all receivers - thereby allowing the sender(s) in the mid-term (in the order of several seconds to minutes) to adapt their coding scheme and transmission behaviour to the observed network QoS. However, except for a few payload specific mechanisms [10], RTP makes no provision for timely feedback that would allow a sender to repair the media stream immediately: through retransmissions, retro-active FEC, or media-specific mechanisms such as reference picture selection. Generally, real-time transport of media streams across IP networks follows RTP[1] in conjunction with the RTP Profile for Audio and Video Conferences with Minimal Control [2]. This document modifies the profile defined in [2] in two ways: by providing additional RTCP messages that enable a receiver to convey more precise feedback to a sender and* by adapting the timing algorithm for scheduling RTCP packets in order to allow for occasional timely feedback about events observed by a receiver (such as lost packets).The result is an RTP Profile for Audio and Video Conferences with Minimal Control that allows for more explicit and more immediate receiver feedback but shares all other properties (including all other message types and formats, all code points for coecs, payload formats, scaling capabilities, etc. of [2]). Therefore, this document only specifies the additions and modifications to [2] rather than the repeating the entire specification.*

NACK-Oriented Reliable Multicast (NORM) Protocol Building Blocks	IETF - Internet Draft draft-ietf-rmt-norm-bb-03.txt	A

This memo describes issues related to the creation of negative acknowledgment (NACK) oriented reliable multicast (NORM) protocols. The general goals and assumptions for NORM are defined. The technical challenges related to NACK-oriented (and in some cases general) reliable multicast protocol design are identified. These challenges are resolved into a set of applicable 'building blocks' which are described in further detail. It is anticipated that these building blocks (as they are further refined and defined in future revisions of this document) will be useful in generating different instantiations of reliable multicast protocols.

NACK-Oriented Reliable Multicast Protocol (NORM)	Internet Draft draft-ietf-rmt-pi-norm-02.txt	A

This document describes the messages and procedures of the Negative-acknowledgement (NACK) oriented reliable multicast (NORM). This revision of the document represents an initial outline of the protocol description. The document requires refinement in a number of areas to be considered complete. At this time, the document describes the high level details of the reliable multicast bulk transfer service model this protocol hopes to fulfill and the general message types and mechanisms which will be used to accomplish those goals.

ROHC over PPP	draft-ietf-rohc-over-ppp-01.txt	

This document describes an option for negotiating the use of robust header compression (ROHC) on IP datagrams transmitted over the Point-to-Point Protocol [RFC1661]. It defines extensions to the PPP Control Protocols for IPv4 and IPv6 [RFC1332,RFC 2023]

ROHC over PPP	IETF - Internet Draft draft-ietf-rohc-over-ppp-04.txt	A

This document describes an option for negotiating the use of robust header compression (ROHC, RFC3095) on IP datagrams transmitted over the Point-to-Point Protocol (RFC1661). It defines extensions to the PPP Control Protocols for IPv4 and IPv6 (RFC1332, RFC2472).

RObust Header Compression (ROHC)	draft-ietf-rohc-rtp-09.txt	
RObust Header Compression (ROHC)	draft-ietf-rohc-rtp-09.txt	

Existing header compression schemes do not work well when used over links with significant error rates and long round-trip times. For many bandwidth limited links where header compression is essential, such characteristics are common.

Existing header compression schemes do not work well when used over links with significant error rates and long round-trip times. For many bandwidth limited links where header compression is essential, such characteristics are common.

RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed	IETF - RFC 3095	A
RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed	IETF - RFC 3095	A

This document specifies a highly robust and efficient header compression scheme for RTP/UDP/IP (Real-Time Transport Protocol, User Datagram Protocol, Internet Protocol), UDP/IP, and ESP/IP (Encapsulating Security Payload) headers. Existing header compression schemes do not work well when used over links with significant error rates and long round-trip times. For many bandwidth limited links where header compression is essential, such characteristics are common. This is done in a framework designed to be extensible. For example, a scheme for compressing TCP/IP headers will be simple to add, and is in development. Headers specific to Mobile IPv4 are not subject to special treatment, but are expected to be compressed sufficiently well by the provided methods for compression of sequences of extension headers and tunnelling headers. For the most part, the same will apply to work in progress on Mobile IPv6, but future work might be required to handle some extension headers, when a *standards track Mobile IPv6 has been completed.*

RTCP Extension for Source Specific Multicast Sessions with Unicast RTCP feedback	IETF - Internet-Draft draft-chesterfield-avt-rtcpssm-02.txt	A

This document specifies a modification to the Real-time Transport Control Protocol to enable the operation of RTP/RTCP with unicast RTCP feedback in Single Source multicast sessions such as Source Specific Multicast (SSM) Communication where the traditional model of Any Source Multicast (ASM) group communication of many to many is not possible and for any group communication which might benefit from a sender controlled summarised reporting mechanism. This specification extends [1], section 6 which defines the RTP session group control channel.

RTCP-based Feedback: Concepts and Message Timing Rules	draft-wenger-avt-rtcp-feedback-02.txt	

Real-time media streams are not resilient against packet losses. RTP [1] provides all the necessary mechanisms to restore ordering and timing to properly reproduce a media stream at the recipient. RTP also provides continuous feedback about the overall reception quality from all receivers -- thereby allowing the sender(s) in the mid-term (in the order of several seconds to minutes) to adapt their coding scheme and transmission behaviour to the observed network QoS. However, except for a few payload specific mechanisms [2], RTP makes no provision for timely feedback that would allow a sender to repair the media stream immediately: through retransmissions, retro-active FEC, or media-specific mechanisms such as reference picture selection.

RTP Payload Format for 12-bit DAT, 20- and 24-bit Linear Sampled Audio	Internet Draft draft-ietf-avt-dv-audio-04.txt	A

This document specifies the packetisation scheme for encapsulating the 12-bit nonlinear, 20-bit linear and 24-bit linear audio data streams into a payload of the Real-time Transport Protocol (RTP). This draft also specifies the way of SDP announcement, when the audio data is pre-emphasised before sampling. The treatment of preemphasised audio data specified this document could be used in other audio formats such as L16.

RTP Payload Format for DV Format Video	Internet Draft draft-ietf-avt-dv-video-04.txt	A

RTP Payload Format for DV Format Video	Internet Draft draft-ietf-avt-dv-video-04.txt	A

This document specifies the packetisation scheme for encapsulating the compressed digital video data streams commonly known as 'DV' into a payload format for the Real-Time Transport Protocol (RTP). There are two kinds of DV, one for consumer use and the other for professional. The original 'DV' specification designed for consumer-use digital VCRs is approved as the IEC 61834 standard set. The specifications for professional DV are published as SMPTE 306M(D-7) and 314M(D-9). Both are based on consumer DV. The RTP payload format specified in this document supports IEC 61834 consumer DV and professional SMPTE 306M and 314M(DV-Based) formats.
This document specifies the packetisation scheme for encapsulating the compressed digital video data streams commonly known as 'DV' into a payload format for the Real-Time Transport Protocol (RTP). There are two kinds of DV, one for consumer use and the other for professional. The original 'DV' specification designed for consumer-use digital VCRs is approved as the IEC 61834 standard set. The specifications for professional DV are published as SMPTE 306M(D-7) and 314M(D-9). Both are based on consumer DV. The RTP payload format specified in this document supports IEC 61834 consumer DV and professional SMPTE 306M and 314M(DV-Based) formats.

Requirements for Session Description and Capability Negotiation	IETF (Internet Draft draft-ietf-mmusic-sdpng-req-01.txt)	A

Requirements for Session Description and Capability Negotiation	IETF (Internet Draft draft-ietf-mmusic-sdpng-req-01.txt)	A

This document defines some terminology and lists a set of requirements that are relevant for a framework for session description and endpoint capability negotiation in multiparty multimedia conferencing scenarios.

Robust Header Compression (ROHC) - The last mile in all-IP wireless	IP in Cellular Networks 2001, Paris	A

Making All-IP networks a reality requires a spectrum-efficient way to run IP over the wireless link. For many applications, the size of the headers in Internet protocols poses a significant problem. Earlier standards for header compression do not work well on links that both exhibit non-trivial round-trip times and significant loss. This talk reports on recent work in the IETF on robust header compression for RTP traffic that resulted in a standard that can compress RTP headers to an average of just over one byte, even in the presence of severe channel impairments. Discussing future work in the area of TCP and signalling protocol compression as well as further optimisation opportunities for RTP (coding improvements as well as "zero-byte header compression").

SIP/VoIP	ComVerse User Forum	A

A brief overview of the use of the Session Initiation Protocol (SIP) by the 3GPP community for next generation signalling in 3G networks. The talk addresses the architectural principles of SIP as well as of the 3G IMS subsystem and presents how 3GPP intends to use SIP. It is particularly pointed out that service creation in 3G networks as currently foreseen seems to be largely derived from traditional telephony service models and is thus centralized.This approach obviously differs significantly from the distributed end-to-end model enabled (and encouraged) by the SIP community. The result of the more traditional model pursued so far in the 3G community is that many of SIP's strengths may not be exploitable in future 3G networks.

SIP/VoIP	IIR IP-PSTN Service Integration	A

An update on recent development of the major standards for VoIP technologies is given including SIP, H.323, and MEGACO/H.248. Latest common developments are reviewed and the current areas of primary interest for successful deployment of VoIP technologies are given. With respect to future development of the entire technological area of "VoIP" it is pointed out that many current (commercial) efforts strive for replicating the existing phone system (manifested in softswitches and IP PBXes) - rather than aiming at providing an innovative platform for future services. Future services must not be restricted to voice-only communications but should include other media as well as other applications (personal presence and instant messaging is one of these which is already being embraced by the industry). Additionally, the many devices of personal communications (including palm tops, organisers, phone, computers, laptops, etc.) should no longer be viewed as isolated pieces but rather combined to create an integrated desk area environment for interpersonal communication and co-operation. Overall, in the long-term, we will most likely not be witnessing a convergence of networks as is frequently pointed out in today's softswitch architectures - instead, we will be seeing a conversion of non-IP networks to an all-IP environment.

Session Description and Capability Negotiation	IETF (Internet Draft draft-ietf-mmusic-sdpng-00.txt)	A
Session Description and Capability Negotiation	IETF (Internet Draft draft-ietf-mmusic-sdpng-00.txt)	A

This document defines a language for describing multimedia sessions with respect to configuration parameters and capabilities of end systems. capability negotiation in multiparty multimedia conferencing scenarios.
This document defines a language for describing multimedia sessions with respect to configuration parameters and capabilities of end systems. capability negotiation in multiparty multimedia conferencing scenarios.

Session Description and Capability Negotiation	IETF - Internet Draft draft-ietf-mmusic-sdpng-03.txt	A
Session Description and Capability Negotiation	IETF - Internet Draft draft-ietf-mmusic-sdpng-03.txt	A

This document defines a language for describing multimedia sessions with respect to configuration parameters and capabilities of end systems.

Simple Conference Control Protocol draft-ietf-mmusic-sccp-01.txt

This document defines the services for a simple conference control protocol (SCCP) to be used for tightly coupled conferences. It is part of the Internet Multimedia Conferencing Architecture

The Message Bus: Guidelines for Application Profile Writers draft-ietf-mmusic-mbus-guidelines-00.txt

This memo defines a list of conventions for terminology, algorithms and procedures for interaction models that are useful for applications using the Message Bus (Mbus) [1]. These conventions are intended as guidelines for designers of Mbus application profiles and Mbus implementations/applications.

5 SUMMARY

This deliverable provides an overview of technologies and standards involved with mobile internet evolution. It is a continuous process and the project members follow all these developments very closely with active participation in different concerned organisations. Since the 6WINIT project specifically addresses the clinical applications for their trials, the groups concerned with these standards also follow the standards related to the health issues very closely.

6 LIST OF KNOWN STANDARDS

IPv6 Specification

RFC 2460: Internet Protocol, Version 6 (IPv6) Specification

Addressing

RFC 2373: IP Version 6 Addressing Architecture

RFC 1881: IPv6 Address Allocation Management

RFC 1887: An Architecture for IPv6 Unicast Address Allocation

RFC 2374: An IPv6 Aggregatable Global Unicast Address Format

RFC 2450: Proposed TLA and NLA Assignment Rules

RFC 2928: Initial IPv6 Sub-TLA ID Assignments

RFC 2471: IPv6 Testing Address Allocation

RFC 2375: IPv6 Multicast Address Assignments

RFC 2526: Reserved IPv6 Subnet Anycast Addresses

RFC 2732 : Format for Literal IPv6 Addresses in URLs

Drafts in discussion:

R. Hinden, S. Deering, IP Version 6 Addressing Architecture , Internet Draft, draft-ietf-ipngwg-addr-arch-v3-06.txt , July 2001.

D. Harrington, Link Local Addressing and Name Resolution in IPv6 , Internet Draft, draft-ietf-ipngwg-linkname-01.txt , January 1997

M. Blanchet, A flexible method for managing the assignments of bits of an IPv6 address block , Internet Draft, draft-ietf-ipngwg-ipaddressassign-02.txt , March 2001.

R. Draves, Default Address Selection for IPv6 , Internet Draft, draft-ietf-ipngwg-default-addr-select-05.txt , June 2001.

J. Yu, IPv6 Multihoming with Route Aggregation, Internet Draft, draft-ietf-ipngwg-ipv6multihome-with-aggr-01.txt , August 2000.

F. Dupont, Multihomed routing domain issues for IPv6 aggregatable scheme, Internet Draft, draft-ietf-ipngwg-multi-isp-00.txt , September 1999.

S. Deering, B. Haberman, B. Zill, IP Version 6 Scoped Address Architecture, Internet Draft, draft-ietf-ipngwg-scoping-arch-02.txt , March 2001.

B. Haberman, D. Thaler, Unicast-Prefix-based IPv6 Multicast Addresses, Internet Draft, draft-ietf-ipngwg-uni-based-mcast-02.txt , June 2001.

Multihoming

Drafts in discussion:

R. Draves, Default Address Selection for IPv6, Internet Draft, draft-ietf-ipngwg-default-addr-select-05.txt , June 2001.

J. Yu, IPv6 Multihoming with Route Aggregation, Internet Draft, draft-ietf-ipngwg-ipv6multihome-with-aggr-01.txt , August 2000.

F. Dupont, Multihomed routing domain issues for IPv6 aggregatable scheme, Internet Draft, draft-ietf-ipngwg-multi-isp-00.txt , September 1999.

Internet Control Message Protocol

RFC 2463: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)

Drafts in discussion:

A. Conta, S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) , Internet Draft , draft-ietf-ipngwg-icmp-v3-00.txt"> Internet Control , June 1999.

Hop by Hop Options

RFC 2711: IPv6 Router Alert Option

RFC 2675: IPv6 Jumbograms

Multicast

RFC 2710: Multicast Listener Discovery (MLD) for IPv6 . Path MTU Discovery

RFC 1981: Path MTU Discovery for IP version 6 Header Compression

RFC 2507: IP Header Compression

RFC 2509: IP Header Compression over PPP

RFC 2508: Compressing IP/UDP/RTP Headers for Low-Speed Serial Links Packet Tunneling

RFC 2473: Generic Packet Tunneling in IPv6 Specification

Domain Name System

RFC 1886: DNS Extensions to support IP version 6

RFC 2874: DNS Extensions to Support IPv6 Address Aggregation and Renumbering

Draft in discussion:

M. Crawford, IPv6 Node Information Queries, Internet Draft, draft-ietf-ipngwg-icmp-name-lookups-07.txt , August 2000.

M. Crawford, Discovery of Resource Records Designating IPv6 Address prefixes, Internet Draft, draft-ietf-ipngwg-prefix-rr-disc-00.txt , November 2000.

Transition Mechanisms

RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers

RFC 2185: Routing Aspects Of IPv6 Transition

RFC 3056: Connection of IPv6 Domains via IPv4 Clouds without Explicit Tunnels

Routing

RFC 2080: RIPng for IPv6

RFC 2740: OSPF for IPv6

RFC 2283: Multiprotocol Extensions for BGP-4

Drafts in discussion:

R. Minnear, R. Hinden, IGRPng for IPv6 , Internet Draft, draft-minnear-igrpng-00.txt , November 1996.

Renumbering

RFC 2894: Router Renumbering for IPv6

Security

RFC 2401: Security Architecture for the Internet Protocol

RFC 2402: IP Authentication Header

RFC 2406: IP Encapsulating Security Payload (ESP)

RFC 1828: IP Authentication using Keyed MD5

RFC 1829: The ESP DES-CBC Transform

Neighbour Discovery

RFC 2461: Neighbor Discovery for IP Version 6 (IPv6)

RFC 3122: Extensions to IPv6 Neighbor Discovery for Inverse Discovery

Auto Configuration

RFC 2462: IPv6 Stateless Address Autoconfiguration

RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6

Drafts in discussion:

J. Bound, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) , Internet Draft, draft-ietf-dhc-dhcpv6-19.txt , June 2001.

C. Perkins, Extensions for DHCPv6, Internet Draft, draft-ietf-dhc-dhcpv6exts-13.txt , May 2000.

D. Thaler, Analysis of DNS Server Discovery Mechanisms for IPv6, Internet Draft, draft-ietf-ipngwg-dns-discovery-02.txt , July 2001.

R. Draves, Default Router Preferences and More-Specific Routes, Internet Draft, draft-ietf-ipngwg-router-selection-00.txt , May 2001.

Program Interfaces

RFC 2553: Basic Socket Interface Extensions for IPv6

RFC 2292: Advanced Sockets API for IPv6

Drafts in discusssion:

R. Gilligan, S. Thomson, J. Bound, W. Stevens, Basic Socket Interface Extensions for IPv6 , Internet Draft, draft-ietf-ipngwg-rfc2553bis-04.txt, January 2001.

W. Stevens, M. Thomas, Advanced Sockets API for IPv6 Internet Draft, draft-ietf-ipngwg-rfc2292bis-02.txt , November 2000.

OSI NSAP Mapping

RFC 1888: OSI NSAPs and IPv6

Mobility

Drafts in discussion:

D. Johnson, C. Perkins, Mobility Support in IPv6 , Internet Draft, draft-ietf-mobileip-ipv6-13.txt , November 2000.

IPv6 over Different Media

RFC 2464: A Method for the Transmission of IPv6 Packets over Ethernet Networks

RFC2 467: A Method for the Transmission of IPv6 Packets over FDDI Networks

RFC 2470: A Method for the Transmission of IPv6 Packets over Token Ring Networks

RFC 2529: Transmission of IPv6 Packets over IPv4 Domains without Explicit Tunnels

RFC 2497: A Method for the Transmission of IPv6 Packets over ARCnet Networks

RFC 2472: IP Version 6 over PPP

RFC 2491: IPv6 over Non-Broadcast Multiple Access (NBMA) networks

RFC 2492: IPv6 over ATM Networks

RFC 2590 : Transmission of IPv6 Packets over Frame Relay Networks Specification

Drafts in discussion:

D. Thaler, Transmission of IPv6 Packets over IEEE 1394 Networks , Internet Draft, draft-ietf-ipngwg-ipngwg-1394-02.txt , July 2001.

Network Management

RFC 3019: IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol

RFC 2851: Textual Conventions for Internet Network Addresses

RFC 2465: Management Information Base for IP Version 6: Textual Conventions and General Group

RFC 2466: Management Information Base for IP Version 6: ICMPv6 Group

RFC 2452: IPv6 Management Information Base for the Transmission Control Protocol

RFC 2454: IPv6 Management Information Base for the User Datagram Protocol

3GPP/ETSI standards

The specifications produced by 3GPP and adopted by ETSI are available on their respective web sites.

http://www.3gpp.org and http://www.etsi.org

7 LIST OF 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
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
CBR	Committed Bandwidth Rate
CCU	Clinical Care Unit
CEN	Comité Européen de Normalisation
CHIME	Centre for Health Informatics and Multi-professional Education
CHTML	Compact HTML
CLI	(1) Calling Line Identification (2) Command Line Interface
CN	Correspondent Node
COPS	Common Open Policy Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CRL	Certificate Revocation Lists
CRTP	Compressed RTP
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
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
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
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
JDBC	Java Database Connectivity
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
MAN	Metropolitan Area Network
MDML	Market Data Mark-up Language
MGW	Media Gateway
MIP	Mobile Internet Protocol
MIP WG	Mobile IP Working Group
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
NHS	National Health Service (United Kingdom)
NRN	National Research Network
O&M	Operations and Management
OCSP	Online Certificate Status Protocol
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
RUS	Rechenzentrum Universität Stuttgart
SA	Security Association(s)
SADB	Security Association Database
SCEP	Simple Certificate Enrolment Protocol
SCO	Synchronous Connection Oriented
SCS	(1) Secure Conference Store (2) Service Capability Server
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
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
TDD	Time Division Duplex
TE	Terminal Equipment
TEID	Tunnel Endpoint IDentifier
TEIN	TransEurasia Information Network
TLA	Top Level Aggregator
TS	Tunnel Server
ToS	Type of Service
UAC	User Agent Client
UAS	User Agent Server
UCL	University College London
UDP	User Datagram Protocol
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
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
XHTML	Extensible Hypertext Mark-up Language
XML	Extensible Markup Language

[i] Available from: http://www.centc251.org

[ii] European Community Directive 95/46/EC *"On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data"*. OJ L281/31 - 50, 24 October 1995

[iii] Council of Europe Recommendation, R(97)5 *"On the Protection of Medical Data"*. Council of Europe, Strasbourg, 12 February 1997

[iv] The Caldicott Committee. *"Report on the review of patient-identifiable information"*. Department of Health, London, December 1997

[v] Available from http://www.iso-17799.com