ETSI TR 102 235 V1.1.1 (2003-07)

Technical Report

Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); Pre-normative Study for IPv6 Testing

Reference

DTR/MTS-00083

Keywords

IP, methodology, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

Introduction

The main objective of the present document is to investigate the need for and the scope of *conformance* and *interoperability* test specifications to support the European Commission's IPv6 deployment goals, the IPv6 Forum's "IPv6 Ready" certification programme and ETSI's own needs for IPv6 testing (including 3GPP).

Effective testing of IPv6 products will be one of the key factors in ensuring the *deployment*, *interoperability*, *security* and *reliability* of the IPv6 infrastructure on which the success of e-Government, e-Business, e-Health, e-Learning and e-Procurement will eventually depend.

The complexity of implementing IPv6 technology means that rigorous testing is absolutely necessary, especially in the context of NGN, convergence and wireless communications. This fact is already recognized by the IPv6 Forum who have set up an ambitious testing and certification scheme known as "IPv6 Ready" as part of their strategy for fast deployment of IPv6.

North American and Japanese testing activities are well represented in the IPv6 Forum and there is a good case for promoting a strong European representation in the "IPv6 Ready" programme. ETSI participation by providing formal test specifications would be welcomed and encouraged by the Forum.

The present document has two main technical goals:

1) to contribute to making the IPv6 testing process more flexible, efficient and cost-effective by the development of an IPv6 test suite development kit based on TTCN-3;

2) to identify the priorities and Areas of Interest for testing;

3) to propose work packages that can be used as a basis for making proposals for STFs to perform the work identified in the present document.

The present document is structured as follows:

- needs and aims of the European Commission for IPv6, with a focus on eEurope 2005 and testing (see clause 5);
- identification and discussion on the potential users of the test specifications recommended by the present document (see clause 6);
- identification of the major Areas of Interest for IPv6 test specifications (see clause 7);
- discussion of the IETF approach to testing (see clause 8);

- description of the test specification components with an emphasis on minimum requirements and the toolkit approach recommended by the present document (see clause 9);
- details of Work Packages for each Area of Interest (see clauses 10 to 18);
- informational tables summarizing the necessary IETF RFCs, 3GPP IPv6-related documents and existing IPv6 test specifications (see annex A).

1 Scope

The present document defines the scope of an IPv6 test specification programme that supports the "IPv6 Ready" certification programme, the European Commission's IPv6 deployment goals and priorities, and ETSI's own needs for IPv6 testing. Analyses, justifications, and supporting documentation are included.

The testing programme is closely associated with the eEurope 2005 action plan. This plan asks the European standardization organizations to propose a 3-year work plan (for 2003, 2004, and 2005) to support new priorities, some of which concern IPv6 testing. Thus, the testing programme is composed of short and medium-term plans (from 2003 through 2005) using resources from eEurope 2005 and ETSI members' voluntary and funded contributions.

The present document also contains proposals to request 2003 funding via the eEurope 2005 action plan.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] COM(2002)96: "Next Generation Internet - priorities for action in migrating to the new Internet protocol IPv6".

[2] COM(2002)263: "eEurope 2005: An information society for all".

[3] IETF RFC 791: "Internet Protocol".

[4] IETF RFC 1006: "iso transport services on top of the tcp: version 3".

[5] IETF RFC 1058: "Routing Information Protocol", C.L. Hedrick, June1988.

[6] IETF RFC 1771: "A Border Gateway Protocol 4 (BGP-4)".

[7] IETF RFC 1809: "Using the Flow Label Field in IPv6", C. Partridge, June 1995.

[8] IETF RFC 1886: "DNS Extensions to support IP version 6", S. Thomson, C. Huitema, December 1995, PROPOSED STANDARD.

[9] IETF RFC 1981: "Path MTU Discovery for IP version 6", J. McCann, S. Deering, J. Mogul, August 1996.

[10] IETF RFC 1990: "The PPP Multilink Protocol (MP)".

[11] IETF RFC 2026: "The Internet Standards Process - Revision 3", S. Bradner, October 1996.

[12] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997.

[13] IETF RFC 2080: "RIPng for IPv6", G. Malkin, R. Minnear, January 1997.

[14] IETF RFC 2126: "ISO Transport Service on top of TCP (ITOT)".

[15] IETF RFC 2328: "OSPF Version 2", J. Moy, April 1998, STANDARD.

[16] IETF RFC 2373: "IP Version 6 Addressing Architecture", R. Hinden, S. Deering, July 1998.

[17] IETF RFC 2401: "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, November 1998.

[18] IETF RFC 2402: "IP Authentication Header", S. Kent, R. Atkinson, November 1998.

[19] IETF RFC 2403: "The Use of HMAC-MD5-96 within ESP and AH", C. Madson, R. Glenn, November 1998.

[20] IETF RFC 2404: "The Use of HMAC-SHA-1-96 within ESP and AH", C. Madson, R. Glenn, November 1998.

[21] IETF RFC 2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV", C. Madson, N. Doraswamy, November 1998.

[22] IETF RFC 2406: "IP Encapsulating Security Payload (ESP)", S. Kent, R. Atkinson, November 1998.

[23] IETF RFC 2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

[24] IETF RFC 2409: "The Internet Key Exchange (IKE)".

[25] IETF RFC 2410: "The NULL Encryption Algorithm and Its Use With IPSec", R. Glenn, S. Kent, November 1998.

[26] IETF RFC 2412: "The OAKLEY Key Determination Protocol".

[27] IETF RFC 2453: "RIP Version 2", November 1998.

[28] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification", S. Deering, R. Hinden, December 1998.

[29] IETF RFC 2461: "Neighbor Discovery for IP Version 6 (IPv6)", T. Narten, E. Nordmark, W. Simpson, December 1998.

[30] IETF RFC 2462: "IPv6 Stateless Address Autoconfiguration", S. Thomson, T. Narten, December 1998.

[31] IETF RFC 2463: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", A. Conta, S. Deering, December 1998.

[32] IETF RFC 2472: "IP Version 6 over PPP".

[33] IETF RFC 2473: "Generic Packet Tunneling in IPv6 Specification", A. Conta, S. Deering, December 1998.

[34] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", K. Nichols, S. Blake, F. Baker, D. Black, December 1998.

[35] IETF RFC 2475: "An Architecture for Differentiated Services", S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, December 1998.

[36] IETF RFC 2507: "IP Header Compression".

[37] IETF RFC 2508: "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links".

[38] IETF RFC 2509: "IP Header Compression over PPP".

[39] IETF RFC 2529: "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", B. Carpenter, C Jung, March 1999.

[40] IETF RFC 2545: "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", P. Marques, F. Dupont, March 1999.

[41] IETF RFC 2597: "Assured Forwarding PHB Group", J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, June 1999.

[42] IETF RFC 2598: "An Expedited Forwarding PHB", V. Jacobson, K. Nichols, K. Poduri, June 1999.

[43] IETF RFC 2641: "Cabletron's VlanHello Protocol Specification Version 4".

[44] IETF RFC 2642: "Cabletron's VLS Protocol Specification".

[45] IETF RFC 2675: "IPv6 Jumbograms", D. Borman, S. Deering, R. Hinden, August 1999.

[46] IETF RFC 2686: "The Multi-Class Extension to Multi-Link PPP".

[47] IETF RFC 2710: "Multicast Listener Discovery (MLD) for IPv6", S. Deering, W. Fenner, B. Haberman, October 1999.

[48] IETF RFC 2711: "IPv6 Router Alert Option", C. Partridge, A. Jackson, October 1999.

[49] IETF RFC 2740: "OSPF for IPv6", R. Coltun, D. Ferguson, J. Moy, December1999.

[50] IETF RFC 2765: "Stateless IP/ICMP Translation Algorithm (SIIT)", E. Nordmark, February 2000.

[51] IETF RFC 2766: "Network Address Translation - Protocol Translation (NAT-PT)", G. Tsirtsis, P. Srisuresh, February 2000.

[52] IETF RFC 2767: "Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)", K. Tsuchiya, H. Higuchi, Y. Atarashi, February 2000.

[53] IETF RFC 2858: "Multiprotocol Extensions for BGP-4", T. Bates, Y. Rekhter, R. Chandra, D. Katz, June 2000.

[54] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[55] IETF RFC 2874: "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", M. Crawford, C. Huitema, July 2000.

[56] IETF RFC 2893: "Transition Mechanisms for IPv6 Hosts and Routers", R. Gilligan, E. Nordmark, August 2000.

[57] IETF RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[58] IETF RFC 3053: "IPv6 Tunnel Broker", A. Durand, P. Fasano, I. Guardini, D. Lento, January 2001.

[59] IETF RFC 3056: "Connection of IPv6 Domains via IPv4 Clouds", B. Carpenter, K. Moore, February 2001.

[60] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles".

[61] IETF RFC 3152: "Delegation of IP6.ARPA", R. Bush, August 2001.

[62] IETF RFC 3162: "RADIUS and IPv6".

[63] IETF RFC 3260: "New Terminology and Clarifications for Diffserv".

[64] IETF RFC 3338: "Dual Stack Hosts Using Bump-in-the-API (BIA)", S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, A. Durand, October 2002.

[65] draft-ietf-bgmp-spec-05.txt: "Border Gateway Multicast Protocol (BGMP): Protocol Specification", D. Thaler, June 2003.

[66] draft-ietf-mobileip-fast-mipv6-06.txt: "Fast Handovers for Mobile IPv6", Rajeev Koodli, 1 March 2003, Internet-Draft.

[67] draft-ietf-ipv6-flow-label-07.txt: "IPv6 Flow Label Specification", J. Rajahalme et al, April 2003, Internet-Draft.

[68] draft-ietf-mobileip-hmipv6-08.txt: "Hierarchical Mobile IPv6 mobility management (HMIPv6)", Hesham Soliman, Claude Castelluccia, Karim El-Malki, Ludovic Bellier, June 2003, Internet-Draft.

[69] ISO/IEC 9646 (Parts 1, 2, 6 and 7) (1994): "Information technology, Open Systems Interconnection, Conformance testing methodology and framework":.

[70] draft-ietf-mobileip-ipv6-24.txt: "Mobility Support in IPv6", D. Johnson, C. Perkins, J. Arkko, June 30, 2003, Internet-Draft.

[71] draft-vida-mld-v2-07.txt: "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", R. Vida, L. Costa, November 2002.

[72] draft-ietf-mobileip-mipv6-ha-IPSec-06.txt: "Using IPSec to Protect Mobile IPv6 Signalling between Mobile Nodes and Home Agents", J. Arkko, V. Devarapalli, F. Dupont, June 30, 2003, Internet-Draft.

[73] draft-ietf-ipv6-node-requirements-04.txt: "IPv6 Node Requirements", John Loughney (ed), Internet-Draft, IPv6 Working Group, 27 June 2003.

[74] draft-ietf-dhc-dhcpv6-26: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[75] ETSI OCG#17, Temporary Document 27: "eEurope 2003 to 2005 and EC support", ETSI Director-General.

[76] ETSI ES 201 873: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 3: TTCN-3 Graphical presentation Format (GFT)".

[77] ITU-T Recommendation Z.140: "The testing and test control notation version 3: TTCN-3 core language".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3G	3rd Generation mobile telephony
3GPP	3rd Generation Partnership Project
AH	Authentication Header
ALG	Application Level Gateway
ATS	Abstract Test Suite
BGP-4+	Border Gateway Protocol adapted to IPv6
DiffServ	Differentiated Services
DSTM	Dual Stack Transition Mechanism
ESP	Encapsulating Security Payload
ETS	Executable Test Suite
ICS	Implementation Conformance Statement
IntServ	Integrated Services
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
IUT	Implementation Under Test
MLD	Multicast Listener Discovery
MoT	Means of Testing
NAT-PT	Network Address Translation - Protocol Translation
NGN	Next Generation Network
OCG	(ETSI) Operational Co-ordination Group
OSPFv3	Open Shortest Path First v3 adapted to IPv6
PCO	Point of Control and Observation
PDP	Packet Data Protocol
PHB	Per-Hop Forwarding Behaviours
PICS	Protocol Implementation Conformance Statement
PTCC	ETSI Protocol and Testing Competence Centre
QoS	Quality of Service
RFC	Request for Comments
RIPng	Routing Internet Protocol v2 adapted to IPv6
SIIT	Stateless IP/ICMP Translation Algorithm
SIP	Session Initiation Protocol
STF	Specialist Task Force
SUT	System Under Test
TC-MTS	Methods for Testing & Specification-Internet Protocol Testing (Group)
TP	Test Purposes
TSS	Test Suite Structure
TTCN	Tree Tabular Combined Notation, Testing and Test Control Notation
UMTS	Universal Mobile Telecommunications System
UNH	The University of New Hampshire
v6LC	IPv6 Logo Committee

v6LC/TC	Technical Committee of v6LC

4 Void

5 Needs and aims of the EC for IPv6

5.1 Introduction

This clause reviews the European Commission policy documents COM(2002)96 [1] and COM(2002)263 [2]. It also considers information acquired from websites concerning the EC and its IPv6-related activities.

5.2 EC policy

COM(2002)96 [1] presents the following Commission policies and views:

- Policies:
  - accelerate the development of a high capacity, reliable and secure communications infrastructure with always-on connectivity and high wireless mobility;
  - maintain and build upon Europe's technological leadership in wireless and mobile communications;
  - provide for an efficient transition to the next generation Internet based on IPv6;
  - promote the standards and specifications work in order to deploy IPv6 deployment in a timely manner;
  - "Make the necessary investments in research and technological development, in particular in the 6th Framework Program, to ensure **interoperability** and **dependability** in the next generations of infrastructures and open systems." (29 Nov 2001 Ministers declaration)
  - 6th Framework Program intends to continue the R&D effort on IPv6 with a view to provide further opportunities to the research community and ensure notably the development of innovative tools, services, and applications.
  - member states are called upon to "provide the required incentives towards the development and testing of IPv6 products, tools, services, and application in the new economy sectors. In particular, IPv6 enabled broadband access to the home, to small and medium size enterprises and in public areas is of key importance."
  - industry is called upon to:
    - "Develop key guidelines permitting the efficient integration of IPv6 infrastructures and interoperability of IPv6 services and applications, notably in the context of 3G mobile communications";
    - "Address the multi-vendor interoperability issues impeding the wide-scale deployment of IP security and conduct extensive IP security trials".
- Views:
  - the wireless and Internet sectors are converging;
  - embedded Internet access, including cars and consumers electronics, will be a new market;
  - IPv6 reintroduces end-to-end security;

  - any delay in the transition to all-IPv6 networks may hinder the deployment of advanced 3G service features at a later stage;
  - service interoperability will both strengthen competition and enhance social cohesion within the European Union;
  - application developers and organizations tendering for new IP-based services should also consider the IPv6-ready status and future proofing of the services they intend to deploy.

Other actions by the European Commission to increase and refocus EU support to RTD in the context of 6th FP are as follows:

- promotion of IPv6 broadband fixed and wireless network infrastructure deployment and interoperability;
- development of IPv6 tools, devices, and network elements;
- large scale testing of IPv6 based services and applications across heterogeneous, fixed and wireless, access platforms;
- production of a European Code Base for IPv6 including the development of IPv6 open source code.

5.3 EC IPv6 priorities

The following are understood to be the EC's IPv6 priorities.

- promote IPv6 Security:
  - secure services, applications, and content are necessary;
  - IPv6 security is a key enabler for e-business and a pre-requisite for privacy;
  - end-to-end security is a "must" that IPv6 can support and that IPv4 cannot support;
  - there are multi-vendor interoperability issues impeding the wide-scale deployment of IP security. One solution is to conduct extensive IP security trials.
- promote converging technologies
  - applications must run easily across multiple different platforms belonging to the same user. These platforms may be either Ipv4 or Ipv6 or dual stack machines. Large scale testing of IPv6 based services and applications across heterogeneous, fixed and wireless, access platforms is required. Embedded Internet access will become important;
  - the user sees fixed and mobile networks as converging into one network;
  - the wireless and internet sectors are converging.
- promote efficient transition from IPv4 to IPv6 to avoid hindering the deployment of advanced 3G services;
- promote IPv6 interoperability:
  - key guidelines are needed to permit the efficient integration of IPv6 with existing infrastructures and the interoperability of IPv6 services and applications with those that are already deployed. This is particularly important in the context of 3G mobile communications;
  - the interoperability of broadband fixed and wireless network infrastructures to support IPv6 is essential;
  - interoperability and dependability in the next generations of infrastructures and open systems must be ensured;
  - application developers and organizations tendering for new IP-based services should consider the IPv6-ready status (as described in clause 6.1) and future proofing of the services they intend to deploy;
- promote IPv6's ability to support mobility;

- maintain and build upon Europe's technological leadership in mobile and wireless communications;
- promote the timely deployment of IPv6. Accelerate the roll-out of leading edge applications and infrastructure;
- promote IPv6 products, tools, services, and application in the new economy sectors. In particular, IPv6 enabled broadband access to the home, to small and medium size enterprises and in public areas is of key importance;
- promote open IPv6 source code.

In the context of this study, standardized TTCN-3 test suites and modules are open source code in the sense that they will be available without cost for all interested parties.

5.4 eEurope 2005 guidance

European standardization organizations are invited to prepare a "Rolling action plan for standardization in support of eEurope 2005" OCG17(02)27 [75]. The action plan should provide a 3-year work plan in support of the new priorities of on-line public services, widespread availability of broadband access with a secure information infrastructure. The Commission proposes a 3 year overall budget with contracts to be negotiated yearly on the same basis as for eEurope 2002.

There are several changes in philosophy from the eEurope 2002 action plan. Proposals must now directly address social policy goals as well as technical policy. The EC also expects cost-sharing by the ETSI members by either voluntary or funded contributions. The eEurope 2002 action plan provided 100% funding. Such is not the case for eEurope 2005.

ETSI Technical Bodies are invited to prepare proposals for consideration by the EC and EFTA to fund activities that are well defined and have a clear relation to COM(2002)263 [2].

The following policies and views (additional to those expressed in COM(2002)96 [1]) are identified in COM(2002)263 [2]:

- Policies:
    - users are now at the centre with emphasis on e-Accessibility and e-inclusion. Ensure the multi-platform provision of services;
    - stimulate secure services, applications, and content based on a widely available broadband infrastructure;
    - accelerate the roll-out of leading edge applications and infrastructure.
- Views:
    - security is a key enabler for e-businesses and a pre-requisite for privacy;
    - multi-platform access/convergence is a priority.

5.5 How testing supports these needs and aims

Testing is directly in line with the eEurope 2005 objectives, as stated in COMM(2002) 263 [2]. The reasons are listed as follows:

- **IPv6** (COM(2002) 263 [2] pages 6, 17):

    The objective of this STF is to facilitate the development and deployment of the Internet Protocol version 6 (IPv6), a cornerstone of eEurope 2005. The importance of IPv6 testing is highlighted in COM(2002)96 [1].

- **Deployment** (COM(2002) 263 [2] pages 6, 8, 11, 17):

    One of the key factors for the successful deployment of IPv6 in Europe will be the smooth migration from IPv4 to IPv6. This is often called *infrastructure upgrading* or *transitioning*. Testing is essential to ensure the *rapid rollout* of IPv6 with minimal disruption and cost. This is especially relevant to *trans-European networks* and to 3G networks where there may be varying levels of IPv6 penetration and where IPv4 and IPv6 will need to co-exist for many years to come.

- **Interoperability** (COM(2002) 263 [2] pages 10, 11, 15):

  While the concepts behind the core IPv6 protocol are relatively simple it does not necessarily follow that IPv6 systems will not be complex. IPv6 is defined in hundreds of related IETF documents which are in varying degrees of maturity and impinge on all aspects of implementing IPv6. This richness means that implementers are forced to make interpretations and choices which is already leading to real interoperability problems.

  Lack of interoperability impacts on every level. A *combination* of focussed conformance tests together with controlled interoperability testing is one of the best methods of removing interoperability problems at an early stage.

  It will be necessary to analyse the minimum set of requirements for each area of interest and design the test specifications accordingly. The present document proposes the implementation of test selection mechanisms that can be applied (or not applied as the case may be) in different contexts. This approach will be especially beneficial to the IPv6 Logo programme and 3GPP.

- **Security** (COM(2002) 263 [2] pages 3, 7, 9, 10, 13, 15, 16):

  Security is one of the key issues for eEurope 2005. IPv6 provides security mechanisms not available in IPv4. If a secure information infrastructure is to be guaranteed, these mechanisms *must* be tested, both for conformance and interoperability.

  It will be necessary to develop the new methods that will be needed for testing IPSec.

- **3G mobile systems** (COM(2002) 263 [2] pages 7, 17):

  Both GSM and 3GPP have a long and successful history of testing. Even in financially restricted times, the 3GPP test program has not suffered. It is considered essential to achieving the interoperability and reliability required of 3G systems. The inclusion of IPv6 in 3G will put even more demands on the development of standardized 3GPP test specifications. While TC MTS will not provide a final set of test cases for 3GPP it can deliver the toolkit, methodology and generic tests that can be adapted by 3GPP.

- **Good practices** (COM(2002) 263 [2] page 18):

  The present document recommends the development and implementation of an IPv6 test specification toolkit which will be applicable to Interoperability events as well as to conformance testing processes as performed, for example, by 3GPP.

  The toolkit will be based on well-proven software engineering techniques and which will be integrated into the test specification development process. The toolkit will be built using the standardized test specification language TTCN-3 (published jointly as ES 201 873 [76] and ITU-T Recommendation Z.140 [77]).

  Use of the toolkit will lead to consistency of style, efficient re-use of code, easier extensibility and adaptation and cheaper maintenance.

- **Research aspects** (COM(2002) 263 [2] page 11):

  Some areas of the toolkit will require advanced engineering solutions. ETSI should maintain a close liaison with similar work in universities and other European projects to ensure feedback in both directions.

- **Reduction of costs** (COM(2002) 263 [2] page 6):

  The generic nature of the test specifications developed within the project will mean that the tests can, with some adaptation, be applied in many contexts. The open availability of the toolkit at the end of the project will make it possible for large industries (e.g., telecom, aerospace, automotive) as well as SMEs to reduce their costs with respect to IPv6 testing.

  The pragmatic nature of this work will result in solutions that are highly likely to be adopted by European industry and 3GPP as well as by sector certification groups such as the IPv6 Forum.

- **Global standardization:**

  This project will build on existing testing methodologies such as ISO/IEC 9646 [69] and TS 102 237-1 (see bibliography). Results from this work will provide feedback to relevant working groups in ETSI, ITU-T and possibly ISO. It will also provide technical feedback to the protocol standards developers in the IETF.

- **Not commercial:**

  The testing of infrastructure has traditionally been regarded as a commercial activity. On some levels that is still true. However, the development of standardized test specifications for use in a European and a global context is beyond commercialization. Formal, validated test specifications coupled with the type of certification programme proposed by the IPv6 Forum, will be essential to rapid deployment of a pan-European IPv6 infrastructure.

6 Potential users of TC-MTS IPv6 test specifications

6.1 IPv6 Task Force Label Committee

6.1.1 Introduction

The IPv6 Forum (http://www.ipv6forum.org) brings together industrial organizations in order to develop and deploy the new generation of IP protocols. Unlike IPv4 which started with a small closed group of implementers, IPv6 is attracting a wide range of suppliers. This is leading to a large number of possible implementations with a correspondingly large uncertainty of interoperability. Interoperability has always been considered crucial by the Internet community as a means of giving the market a strong indication of the compatibility of various products.

To avoid customer confusion, a single world-wide certification programme is required. Thus, the IPv6 Forum is launching a certification programme called the "IPv6 Logo Programme". The IPv6 logo is intended to increase user confidence by showing that IPv6 is available now and ready to be used. The Committee intends the Logo Programme to clearly indicate that the technology is here to stay.

The IPv6 Forum has created a small committee, the IPv6 Logo Committee (v6LC), to manage the logo programme. It comprises representatives from equipment vendors, service providers, academic institutions, IPv6 organizations and test laboratories.

The v6LC has proposed a two phase logo programme to allow its smooth and gradual implementation:

- Phase I (in the short term):

  The Phase I Logo will indicate that the product includes IPv6 mandatory core protocols and has interoperated with other similar IPv6 equipment. For pragmatic reasons and speedy implementation, the Logo Committee will use existing relevant interoperability events and conformance and interoperability test suites as a basis for awarding the logo.

- Phase II (in the long term):

  The "IPv6 ready" step requires test engineering, technical consensus, and clear technical references. The IPv6 ready logo indicates that a product has successfully satisfied the stringent requirements of the v6LC. The v6LC will specify requirements for each product category.

Phase I commenced in March 2003 and the requirements for Phase II are due to be published at the end of 2003. The first awards of the Phase II logo are scheduled to start at the beginning of 2004. The v6LC has established a Technical Committee (v6LC/TC) to supervise the programme's technical aspects.

6.1.2 Proposed ETSI Support of the Logo Programme

The second phase of the world wide IPv6 Logo Programme will include formal testing. Both conformance and interoperability test suites are required. The v6LC/TC has decided to use technical input from the USA, Asia and Europe for Phase 2. Each region will provide test specifications needed for the logo programme. The v6LC/TC looks to ETSI as the principal European source of these specifications. The IPv6 Forum are very interested in using ETSI's testing specification expertise and interoperability event support for Phase 2.

v6LC/TC will define categories of products. For each of these it will identify IPv6-related protocols and mechanisms that are to be implemented in a product. It will then determine the general Phase II conformance and interoperability test requirements. Subsequently, v6LC/TC will request ETSI to provide reference Test Suites for these product categories and test requirements. The Asian and American sources will be asked to do the same. Any applicant for the IPv6 Ready logo will be informed of the logo requirements, the specific testing program, and the available test suites for implementing the test program. The applicant can then choose the Test Suite from those offered, one of which will be, of course, the ETSI specification.

v6LC/TC has already identified some high priority Areas of Interest which are:

- Routing;
- Mobility;
- Transition mechanisms;
- Quality of Service.

v6LC/TC plans to publish the first list of tests suite requirements in September 2003. Using this date as its start, the following events comprise the current Phase II implementation schedule.

September 2003:	Publication of the Phase II requirements for high priority categories.
During 2004:	Publication of the Phase II requirements for the remaining categories.
End of 2004:	Test suites for first priority categories (Procedures to request the Phase II Logo can start for these categories)
During 2005:	Test suites for the other priority categories (Procedures to request the Phase II Logo can start for these categories)
End 2005:	Test suites for all categories (defined by the v6LC) are available.
From 2006:	Test suites are updated per v6LC requests.

6.2 3GPP

IPv6 is mandatory for Release 5 of UMTS, published at the end of 2002, and onwards. UMTS uses IPv6 for two different purposes:

- as the transport layer in the access network especially at the Iu, Iur and Iub interfaces;
- as a transport medium for services which are on top of the 3G architecture. IPv6 packets are transmitted from the mobile station via the Internet interfaces of the 3G network and in the reverse direction.

Four IPv6 Areas of Interest for testing apply to 3GPP:

- Core:

  Aspects of the minimum node requirements apply to 3G for both the network transport layer and the service transport medium. Autoconfiguration is of special interest because mobiles obtain their IPv6 address using it. Thus, the IPv6 autoconfiguration tests must be embedded within 3G PDP context activation tests. Topics of interest within the core area of interest are stateless and stateful autoconfiguration RFC 2641 [43], RFC 2642 [44], privacy extensions for stateless autoconfiguration RFC 3041 [57], address architecture RFC 2373 [16], core base functions and core header processing RFC 2460 [28].

- Transition:

  Release 99 and Release 4 do not require the use of Ipv6. Some UMTS-networks currently use IPv4 as both a transport layer and the service medium transport means. Transition from IPv4 to IPv6 is necessary to migrate from release 99 or release 4 to release 5 of UMTS. Topics of interest within the Transition area of interest are IPv6 tunnelling over IPv4 (RFC 2893 [56]), Network Address Translation, and Protocol Translation (RFC 2766 [51])

- QoS:

  QoS is an important issue in UMTS. To guarantee a specific QoS at the UMTS level it is necessary that the IPv6 layer provide the same quality of service or better. As for the core area of interest, IPv6 QoS tests must be embedded in 3G specific QoS tests. The topic of interest within the QoS area of interest is Differentiated Services (RFC 2474 [35]).

- Security:

  In release 5, security functions are mainly required for IMS to protect SIP Messages sent via IPv6. Topics of interest within the security area of interest are the security architecture (RFC 2401 [17]), ESP (RFC 2402 [18]), and the Authentication Header (RFC 2406 [22]).

For more details about the use of IPv6 functionality in 3G, see table 8 and 9.

It is not clear at this time what aspects of IPv6 will be used in UMTS. To date, only the addressing scheme has been adopted. IPv6 routing is not currently seen as a requirement for UMTS.

3GPP test suites are presently written in TTCN-2 and are intricate. IPv6 test cases will be written in TTCN-3. The most efficient manner to embed these TTCN-3 test cases within a TTCN-2 test suite and test cases must be determined. Possible solutions include automatically converting the TTCN-2 test suites to TTCN-3, writing Release 5 and succeeding test suites in TTCN-3, or finding a way to import a TTCN-3 module into a TTCN-2 test suite or vice versa.

6.3 ETSI Technical Bodies and members

Apart from within 3GPP, there is no requirement by ETSI Technical Bodies for IPv6 test specifications in 2003. However, it is anticipated that technical bodies such as the merged SPAN and TIPHON will require methodologies and test specifications from mid-2004.

6.4 ETSI Plugtests^{TM} service

The ETSI Plugtests^{TM} Service organizes interoperability events when there is a perceived need and a critical mass of participants. One of the event organization services includes interoperability tests. Presently, IPv6 interoperability tests are provided either by a volunteers from the participants, the other testing organizations such as TAHI or UNH, or from ETSI experts under contract to the Service. The Plugtests^{TM} Service strongly supports ETSI's involvement in the eEurope 2005 program in order to obtain interoperability tests for use in the ETSI IPv6 interoperability events.

6.5 The IETF

The IETF does not produce test specifications (see clause 8). However, it is important to distinguish between the IETF as a standards making organization and the Internet community (i.e. implementers, users, developers etc.). There are strong indications that the latter require rigorous testing of both conformance and interoperability. This requirement is manifest in the creation of the v6LC by the IPv6 Forum.

6.6 SMEs and other European interests

The testing programme presented in the present document, especially the core toolkit approach described in clause 9.7, is aimed at a very wide audience and not just the telecoms market. It is hoped that its general approach will provide a cost-effective, flexible and adaptable set of IPv6 test specifications that can be used by many sectors of European industry. This includes the major players in the automotive and aerospace industry as well SMEs looking for general test solutions with wide acceptance in the IPv6 community.

There may also be interest from e-Government and e-Health entities looking for operational guarantees prior to making product and service acquisition decisions.

7 IPv6 Areas of Interest for testing

The following IPv6 Areas of Interest have been compiled based on the needs of the EC (see clause 5) and potential users (see clause 6). The testing programme described in the remainder of the present document is aligned with these Areas of Interest and are as follows:

- Core IPv6 protocol
- Transitioning (IPv4 -> IPv6)
- Mobility
- IPSec (Security)
- Quality of Service (QoS)
- Routing
- Multicasting

8 The IETF and testing

8.1 Introduction

Unlike ETSI, the IETF does not consider the production of test specifications to be part of their standardization process. In their own words, "an Internet Standard is a specification that is stable and well understood, is technically competent, has multiple, independent and interoperable implementations with substantial operational experience, …". Indeed, in the Internet community, the testing that takes places at interoperability events is considered part of the base standardization development process. An interoperability event (also called a bake-off, a plugfest, connecthaton, etc.) is a session of about one week during which companies involved in a technology come together to test their products against each other. Both conformance and interoperability testing is undertaken at these events but the approach taken is less formal than that of ETSI, ISO and ITU-T. The IETF does not have formally defined concepts such as test purposes, ICS/PICS, ATS and ETS based on ISO 9646 [69].

The test suites used at the interoperability events are developed by third parties such as testing labs, equipment producers and non-profit organizations.

8.2 Optional requirements

There are differences in the use of terms specifying requirements types within IETF and ETSI. IETF uses the terms MAY, SHOULD and RECOMMENDED which are defined in RFC 2119 [12] and RFC 2026 [11]. These terms affect test configuration and, consequently, test writing. In its base standards, ETSI uses similar, though not identical, terms such as MAY, SHALL and SHOULD to specify different types of requirement. In developing test specification it will be necessary to resolve the semantics of both terminologies into conditions and rules that test specification writers can implement.

ETSI specifications include a full set of both mandatory and optional requirements. There is no such rule for Internet test suites. A suite may or may not specify tests for all the required items and optional items. There is no generally accepted practice on the test specification's extent of coverage of the base specification.

Within the IETF, there is a new initiative to consolidate the minimum requirements for IPv6 nodes into a single, authoritative RFC which adds explanation and clarification where necessary.

8.3 The Internet draft-test suite cycle

Because the Internet standard development process can be long, test specifications are usually developed for each draft of a base specification. A draft is valid for a six month period during which time an interoperability event usually occurs. New test suites are written for each of these events with the results being input into the next draft version. In effect, the testing occurring during a cycle is used to validate or improve the current draft version. This cycle of draft-interoperability event-draft occurs until a final draft is accepted and converted into a Proposed Standard. Drafts going through more than 20 versions are not uncommon.

The IETF view is that the best time to provide test suites is before implementation deployment. Early and cyclic test writing is useful to testers, implementers, standardization organizations and certification bodies (e.g. IPv6LC) in several ways:

- Testers can provide test suites that will be ready to use and validated as soon as the standard is published as an RFC. Development and maintenance costs for a test suite after approval of the standard is minimal. In addition, the testing specifications are available when needed either during product development or afterwards.

- Developers can use the test suites during the development of their implementations. Conformance tests are used in order to validate implementations for interoperability purposes. This is important because the interoperability of at least two implementations from different vendors is the usual requisite for IETF to raise an RFC to Draft Standard and Standard status.

- Associating testing with the standardization process benefits the whole community. Reports on problems and inconsistencies in the draft seen by implementers and testers result in better base standards.

- The IETF believes that updating a test suite can be done effectively and quickly by incorporating the differences between the two drafts. These are reported in an annex of each new release. Expertise gained from the definition of previous test suite versions allows accelerated test suite production. In general, an entire test suite is not rewritten each time a new draft is published. Writing the original test suite requires the most resources.

ETSI does not expect to have any influence upon the Internet community's draft-interoperability event cycle. It will, however, be necessary to determine the best way to support the cyclic process. This may involve some adaptation of current practices for writing test suites in the event that the base standards are unstable.

9 Elements of IPv6 test specifications

9.1 Types of test specifications

Interoperability testing is the act of determining if end-to-end functionality between (at least) two communicating systems is as required by the base standard(s) for those systems. Conformance testing is the act of determining to what extent a single implementation conforms to the individual requirements of its base standard. ETSI can support IPv6 interoperability and conformance testing by developing the specifications for these activities.

Both types of testing are needed. Conformance and interoperability testing are already used extensively in the various IPv6 interoperability events. The IPv6 label program also includes both types in its second phase. Finally, only the combination of interoperability and conformance testing yields the greatest assurance of a product's interoperability.

These specifications can include the following elements: test purposes, test methods and architecture, test suite structure, abstract test cases, abstract test suites, and Implementation Conformance Statement proformas. The elements of a specific specification can vary according to the test type, the Terms of Reference of the specification, and the resources available.

As a rule, the IETF develops only base specifications whereas ETSI integrates test specification development with base specification development. Third parties independently without IETF control or supervision develop the test specifications from the current drafts or standards. These tests are then used in the IETF's interoperability events.

IPv6 standardization is now in its tenth year without ETSI involvement. Thus, the usual ways in which ETSI combines base protocol and test specification development do not apply. ETSI test specification support will need to adapt to the IETF iterative base specification/interoperability event cycle. For 3GPP, TIPHON and BRAN test specifications have been developed based upon periodic revisions to the base specifications. In addition, some of these test specifications have been developed concurrently with the development of the base standards. The methods and experience developed in the 3GPP, TIPHON, and BRAN work should be used for IPv6 test specification development.

RFCs that are now standards will most likely require only one round of test specification writing. On the other hand, test specifications for RFCs in the draft stage present a fundamental problem. Are test specifications written and maintained for each new draft? If not, what is the process for deciding which draft be the basis for a test specification? Each package proposed to the EC shall present recommendations concerning one-time and/or iterative test specification development

9.2 Minimum sets of requirements

IPv6's mandatory and optional requirements must be known for writing test specifications. Determining these mandatory and optional requirements may be problematical. There are many IPv6 base specification documents and the requirements for a single protocol or other testable item are usually spread across several RFCs. The use of the terms SHOULD and MAY in IETF base specifications can also lead to confusion when the IETF's guidance is not followed. These are not new problems and, in the case of ETSI standards, have been addressed by effective working practices.

"IPv6 Node Requirements" [73] consolidates IPv6 requirements into a single document. It provides a list of "mandatory" RFCs for IPv6. In some instances, it also lists mandatory functions from within these RFCs. "IPv6 Node Requirements" [73] is used as a basis for the "minimum base specification requirements".

An additional step is then needed to identify the minimum set of requirements. The set of RFCs in "IPv6 Node Requirements" [73] contains items qualified by the terms MUST, SHOULD, MAY, etc. The next step is to include only those requirements qualified by the terms MUST, SHOULD, MUST NOT, and SHOULD NOT. This step concludes the identification of the minimum set.

Test specifications should be written for at least the minimum set of requirements determined using the above procedure. Additional specifications may be written for the optional requirements depending upon executive decisions and resources.

9.3 Test methods and architecture

The abstract test method is the description of how an Implementation Under Test (IUT) is to be tested at a level of abstraction that makes the description independent of any Means of Testing (MoT), but with enough detail to allow specification of abstract test cases. It is also known as the test architecture.

Its three major components are the IUT, the Points of Control and Observation (PCO) used during the testing, and the category of testing chosen from the four possibilities: Remote, Local, Distributed, and Coordinated. For an overview of these testing categories, see the ISO/IEC 9646-1 [69], Open Systems Interconnection - Conformance Testing Methodology and Framework.

The abstract test method shows graphically and explains textually the relationship between the Implementation Under Test (IUT) and the testing environment. If one cannot directly access the IUT, the System Under Test (SUT) must be included as well. In this, the abstract test method shows the interface(s) where test equipment is attached, the relationship between the IUT and SUT, the type of test equipment, cabling requirements, and test and IUT operator locations. Much thought is required to determine the points where tests are controlled and observed.

Abstract test methods and test architectures are well defined for ETSI's conformance test specifications. Such is not the case for IPv6 interoperability test specifications. However, work is underway in EP TIPHON to define generic interoperability testing concepts and methodology for NGN. This work should be used as a basis and then adapted to fit IPv6 interoperability testing needs (if necessary). The ETSI IPv6 interoperability test methodology must also be compatible with v6 Labelling Committee's test methods so that ETSI's products can be used in the v6LC labelling program.

9.4 Test Purposes (TPs)

A Test Purpose is a prose description of a well-defined testing objective focusing on a single requirement or a set of requirements as specified in the base requirements or another appropriate specification. For IPv6 test specifications, test purposes should be written for each member of the set of minimum requirements for a protocol or testable object.

Formats of test purposes vary according to whether they are written for conformance or interoperability testing.

The Internet community conducts much testing with public domain test suites. Some of these contain test purposes similar to ETSI's, others contain short textual descriptions of the tests and do not separate test purposes from the tests. ETSI has found that this separation (as recommended by ISO 9646 [69]) useful in the design and development process of test specifications as well as providing a concise and understandable overview of what is being tested. The majority of the existing tests are in the Core Area of Interest where several test suites cover the same requirements.

Analysis of the coverage and consistency of the existing IPv6 test suites will be the basis upon which decisions are made regarding the range of tests to be developed by ETSI. Test Purpose comparison and synthesis is the most appropriate method to use in this analysis. By specifying a complete set of test purposes for the base specifications and then comparing this with the existing test purposes, it is possible to determine whether there are requirements that a test suite has not covered.

9.4.1 Feasibility of test purpose compilation and synthesis

Test purpose comparison and synthesis is also appropriate to determine the range of possible interpretations of a specification. Experts working in ETSI on the TIPHON SIP profile test suite made a different interpretation of the SIP RFCs from that made by some major vendors. Regardless of which interpretation was strictly correct, this highlights the fact that requirements in the SIP RFCs are expressed ambiguously and without clarity such that a wide range of interpretations are possible.

But, is compiling, comparing, and synthesizing test purposes feasible? The general concept of test purposes is not widely understood in the Internet community. And, there is certainly no IETF standard for writing test purposes that would ease comparison and identification. Thus, test purposes from different testing organizations for the same IPv6 RFC would have to be converted to a common format to allow their comparison. Where test purposes do not exist, they would have to be derived from each test case or from its specific RFC reference, if one exists.

Once in a common format, the test purposes would have to be compared one by one with each other to determine if they were identical or similar. If identical, then it is clear that the two test suites concerned cover the same requirement. If similar, closer inspection would determine to see if there is any specific difference between the two test purposes or if the only differences were in syntax and/or word choice. If the latter, the test purposes are in essence identical and cover the same requirement. They should then be synthesized into the same text in order to convey the equivalence and same understanding to the test suite users. Also the specific RFC references in the source documents could be used to give a first indication of compatibility. For example, if the same section and sub-section of the RFC is cited for two test purposes of origin, it could indicate they are identical. If, on the other hand, the references are different, then the test purposes are certainly different.

In any event, this is a burdensome process. For example, if three organizations have each prepared a test suite covering Core functions with each having 200 test purposes, it would require the writing of 600 test purposes in a common format. In excess of 10^5 comparisons would then be required. Added to this is the rewriting of similar test purposes.

Thus, it appears to be feasible but very onerous to compile, compare, and synthesize test purposes. Compilation should be done if there is a reason worth this effort. If the purpose of the work is simply to be the first step in writing a test suite from scratch, then it is probably more efficient to develop the test purposes from reading the requirements documents rather than using existing test purposes.

If the purpose of the work is to determine the extent of test suite coverage, it likely to be more efficient to write the test purposes from scratch, organize them into the same structure as the test suite, and then compare the test purposes with the corresponding test cases.

If the purpose of the work is to develop a single set of requirements from the existing test purposes, one-by-one comparison would be a reasonable solution. However, it is unlikely that the v6LC or any other organization will ask ETSI to compile and synthesize existing and future test purposes or test suites.

9.5 Test Suites (TSs)

The Abstract Test Suite (ATS) is a collection of test cases organized according to the Test Suite Structure (TSS). Test suites and test cases will be written in the TTCN-3 language which is particularly well suited for satisfying IPv6 test language requirements. It is a standardized and non-proprietary test language that includes advanced test language concepts. It has been designed so that the meaning of tests can be clearly understood and implemented on any platform. A test case written in TTCN-3 should compile on any hypothetical test platform and give identical results for the same IUT regardless of the platform. TTCN-3 is also C-like in its appearance, thereby increasing the likelihood of the test suite's readability by members of the IETF community.

The TSS is simply the logical grouping of test cases usually by functional areas.

9.6 Implementation Conformance Statements (ICS)

An ICS is a questionnaire and part of a telecommunications specification (e.g. protocol, interface, or telecommunications service). The supplier of an implementation fills in the questionnaire. The objective of the ICS is to provide a statement of which capabilities and options of the telecommunications specification have been implemented. It is used in two contexts:

- For conformance testing purposes: it is mainly used to check the static conformance of the implementation and to select and parameterize the tests to be run for dynamic conformance determinations. For example, if some base specification optional features are not implemented, the ICS will show this. The tester will then know that the tests for the unimplemented features will not have to be executed.

- Outside the conformance testing context: it is used to provide information on the capabilities supported by the implementation. It then can be used in determining the chances of interoperability between two implementations. If one implementation has an optional function and the other does not, the two implementations risk interoperability problems.

The Protocol Implementation Conformance Statement is a type of ICS and is protocol-specific.

9.7 IPv6 test specification toolkit

The development of test specifications will require some preparatory work. In addition, there will also be elements common to at least two or more work packages. This preparatory work and common elements will be components of the IPv6 test specification toolkit. The toolkit will be built at the start of work and will be maintained and added to throughout the lifetime of the IPv6 work. The toolkit's purpose is to provide the widest array of tools for quickly writing precise and correct test cases. It will be both a repository for essential information and a selection of work-to-date that will avoid "reinventing the wheel" in writing test cases. It will also improve the style consistency between the various test suites.

The toolkit will consist of textual material, TTCN-3 modules and a User's Manual. A basic set of toolkit components is presented below. The set is certainly not inclusive. The toolkit will be available to both test writers and testers.

Textual toolkit components will include the following:

- The minimum set of requirements per work package (see clause 9.2).

- The Test Methods and architectures available for both IPv6 interoperability and conformance testing.

TTCN-3 software toolkit components/modules should include:

- Parameterized IPv6 general header.

- Parameterized IPv6 extension headers.

- Option selection switches for each work package.

- Common data structures; e.g. URLs, address notations, and other kinds of regular expressions.

- Preambles and postambles.

- IPv6 datagram data to be used as content: text, voice, multimedia, files, etc.

The use of "patterns" in the software engineering sense applied to testing has proved very valuable for an ETSI member during the development of their testing specifications. This member strongly recommends using patterns in the proposed IPv6 work in order to save development time and to write more succinct and precise test cases. The concept is discussed in annex B. A feasibility study using voluntary effort should be conducted before inclusion of the patterns concept into the work packages.

If adopted, patterns would certainly not increase the total required effort for a work package but should, hopefully, reduce it. Additional effort would be required at the start of each work package to identify the patterns, especially in the Core package (WP1). Correspondingly less effort would be required in the actual test case and suite writing.

9.8 Option selection switches

The IETF does not use ICS/PICS and profiles or anything similar and it is unlikely that this will change in the foreseeable future.

The lack of selection schemas in IETF specifications raises many potential areas of non-interoperability. The present document proposes the use of "selection switches" as a flexible solution which might be attractive to the members of both ETSI and IETF. For each element in an implementation, a selection switch represents the status of one possible option.

Selection switches are written in TTCN-3 and return or assign Boolean results. All switches are contained in a separate module that contains no code other than switches. They could be grouped into this module in a graphically structured way so that the configuration under test could easily be viewed. This module could also be viewed as a kind of PICS proforma in TTCN-3.

Mandatory requirements such as those in "IPv6 Node Requirements" [73] are not switchable and, thus, are permanently set to "on". The complete set of switches set to "on" in the switch module defines the configuration under test. The TTCN-3 test suite uses the switch settings to determine the tests to be executed for the specific configuration. Thus, what was a proforma becomes a module incorporated into the test suite.

Option selection switches for SHOULD requirements are set to "on" by default. If they are switched off in the switch module, then a comment to justify the switching is required. Switches for MAY requirements are set to "off" by default. Switching them on requires no justification comments. Similar logic would exist for the other types of IETF requirements (e.g. SHOULD NOT).

The switch modules could be used for another purpose. It is possible that two implementations that are supposed to be compatible, but not identical, cannot interoperate because of configuration differences.

10 Proposed work packages for each Area of Interest

10.1 Introduction

The programme is composed of packages that correspond to the Areas of Interest presented in clause 7.

- WP0: Ipv6 test specification toolkit
- WP1: Test specifications for Core IPv6
- WP2: Test specifications for Transition Mechanisms
- WP3: Test specifications for Mobility
- WP4: Test specifications for IPsec
- WP5: Test specifications for QoS
- WP6: Test specifications for Routing

- WP7: Test specifications for Multicast

WP0 and WP1 are essential to all the other work packages and must be completed first. Otherwise, WP2 - WP7 are independent of each other.

10.2 The minimum set of documents

Test specifications should cover at least the minimum functions necessary for each Area of Interest. This is the approach taken by v6LC for their certification program which is to be based on a minimal set of functions. Test specifications are not restricted to just the minimal set, but it does make this set the first priority.

The IETF started to develop a successor to IPv4 in the early 1990s. Roughly ten years of effort have resulted in many Internet standards track documents and drafts. The Areas of Interest, the number and type of requirements, and their relationships lead to a complex system difficult to conceptualize and test as a whole. Thus, a simplifying and unifying principle is needed. The present document adopts the method of John Loughney, editor of the Internet Draft "IPv6 Node Requirements" "IPv6 Node Requirements" [73] in identifying the minimal set of requirements for an IPv6 node. These functionalities include all the Areas of Interests except for QoS which is considered to be significant enough to add as an element in the minimal set.

Lougney's work is summarized in figures 1, 2 and 3 which show the functional requirements as MUSTs, SHOULDs, and MAYs pertaining to documents. Each block shows the function in its upper part and the IETF document reference and document type in its lower part. The hierarchy of functions in "IPv6 Node Requirements" [73] is shown in a standard tree diagram. The type of line connecting blocks in the hierarchy indicates the relationship of the inferior to its superior. If the line is solid, then the inferior block is necessary (MUST): if dashed, then recommended (SHOULD); and if broken, then optional (MAY).

A node can be either a host or a router. Rather than show separate figures for each type of node, the requirements to a specific type are indicated by a note next to the connecting line that designates a host or router-specific requirement and in the function part of the block. For example, in figure 1 local link addressing is shown as a router specific requirement.

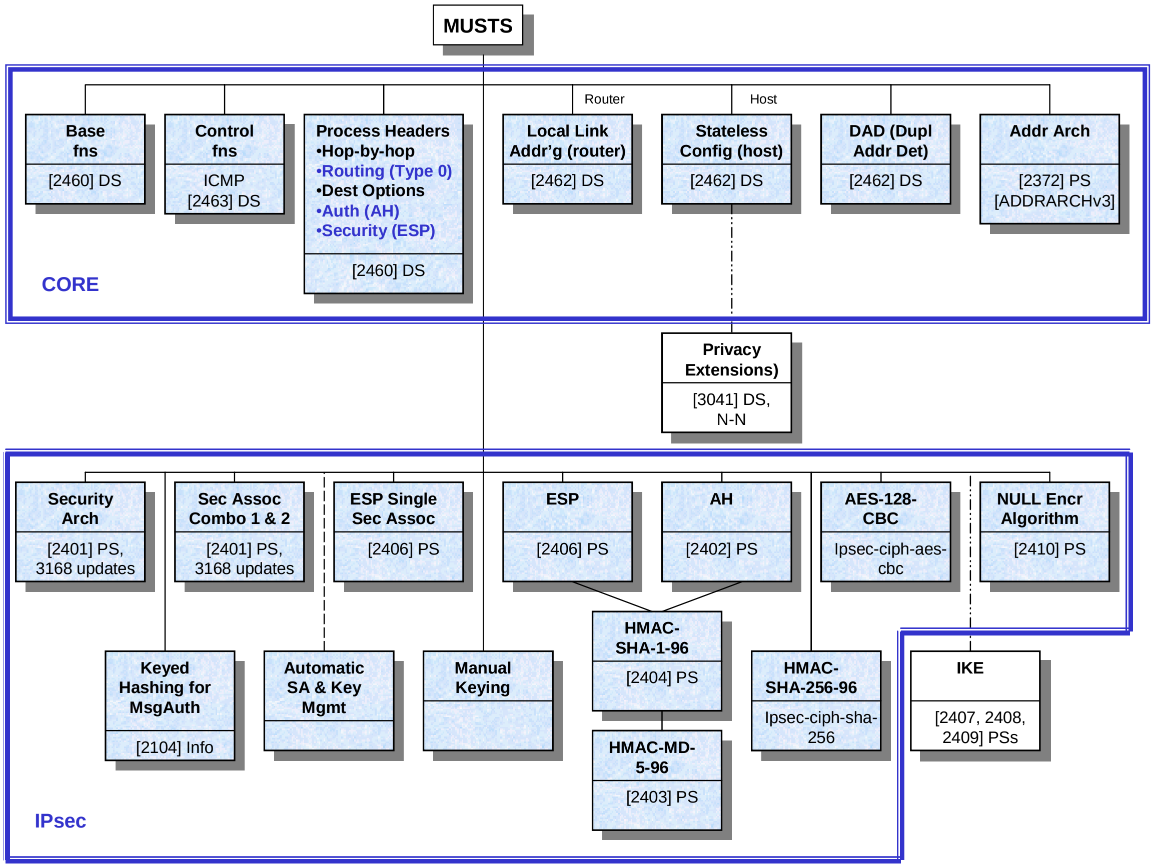

Figure 1: "IPv6 Node Requirements" [73] MUST Functions

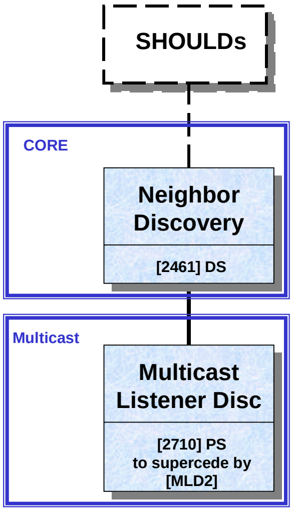

Figure 2: "IPv6 Node Requirements" [73] SHOULD Functions

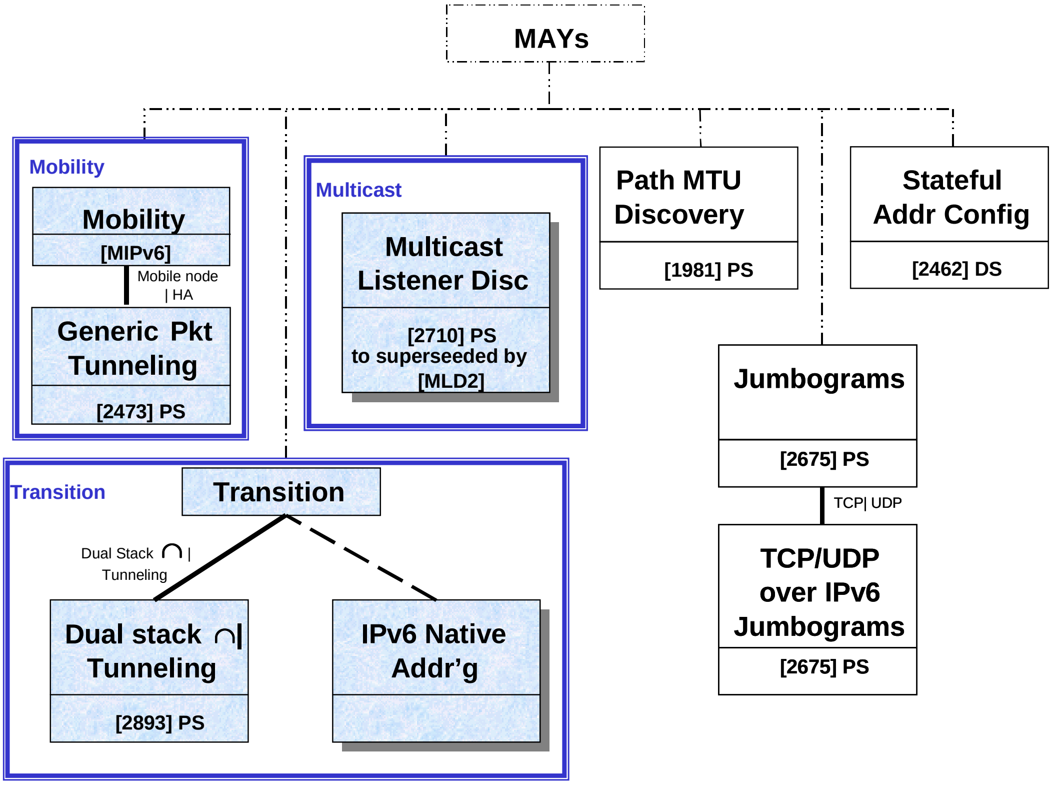

Figure 3: "IPv6 Node Requirements" [73] MAY Functions

The blocks associated with the project Areas of Interests are have a blue background and are enclosed by double lines. The Areas of Interest shown are the Core, Transition, Mobility, IPSec, and Multicast.

Not all blocks are true functions. For example, the AH (Authentication Header) block refers to structure of message data. nevertheless, all the blocks are associated with an IPv6 function - Authentication in the case of AH. These non-functional blocks do contain functional requirements in the document referenced and, thus, are shown. Other blocks are true function blocks but have an empty document reference part (Manual Keying for example) as no source of requirements is identified in "IPv6 Node Requirements" [73] for these items.

NOTE: Since Loughney's work is still in the draft stage and has missing items, it was necessary to determine the missing elements and add their source to the requirements documents list.

10.3 Task development and analysis

Tasks for each work package have been selected from the following possibilities:

- General aspects (applicable to both conformance and interoperability testing):
  - analysis of the minimum requirements based on the minimum set of documents;
  - test architecture and methods. This includes the identification of test interfaces, test components, use of toolkit. A key component will also be the development of testing methodology for specific areas of interest (e.g. IPSec, QoS);
  - Toolkit development;
  - definition of upper test interface API (common to both conformance and interoperability);
- 3G specific issues:
  - descriptions of how to incorporate TTCN-3 suites into 3G Release 5 and beyond and the integration of existing TTCN-2 test specifications with the new TTCN-3 specifications;
- testing specifications for either interoperability or conformance testing or both:
  - Test Purposes, which can be either new or compiled and synthesized from existing testing purposes and suites;
  - (Abstract) Test Suites in TTCN-3.

NOTE 1: The Toolkit (WP0) and Core package (WP1) are essential to all the other packages and should be completed first. The other work packages (WP2 - WP7) can then be developed independently.

In each package, the "General" aspects contain elements related to both conformance testing and interoperability testing.

These task possibilities have been compared with existing test specifications (IRISA, TAHI, UNH, etc) and other documents to determine if they overlapped. Those tasks that were not covered by existing documents have been analysed further. For those items that are already covered, the existing specifications' utility, such as timeliness, coverage and content were evaluated.

Resource estimates for each of the project Work Packages are included in clauses 11 to 18. These are based upon a number of aspects:

- the existence and stability of the base protocol specifications;
- the availability and extent of existing test suites;
- the complexity of integrating existing test suites into a TTCN-3 environment;
- common resource indicators such as the number of pages in the base specification and the number of individual requirements included.

NOTE 2: To obtain an indicator for the amount of effort required for the Core package, the number of pages and the requirements in the document set was determined. The seven requirements documents have a total of 192 pages of content excluding annexes and notes. There are a total of 841 composed of 354 MUSTs, 233 SHOULDs, and 254 MAYs. The MUSTs and SHOULDs may be considered as the equivalent of mandatory in the ETSI sense and the MAYs as optional. This indicates that there is may be at least 587 test cases.

11 WP0: The IPv6 test specification toolkit package

The IPv6 Test Specification Toolkit is one of two essential packages of the programme, the other being the Core Package.

The IPv6 Test Specification Toolkit includes methodologies, tools, requirements, and other items that are applicable across all packages. As such, it is the programme's horizontal component.

Components of the toolkit are presented in the following clauses.

11.1 Test methodologies

11.1.1 Methodologies for conformance and interoperability testing

It is expected that the development of conformance test suites and interoperability test suites will each follow a clearly defined methodology. ISO/IEC 9646 [69] is generally accepted within the standardization world as the base methodology for conformance testing. The IPv6 conformance test suites will be produced according to those parts of ISO/IEC 9646 [69] which are appropriate to this type of protocol.

There is no equivalent to ISO/IEC 9646 [69] in widespread use for interoperability testing. However, EP TIPHON is defining a methodology and framework for interoperability testing for NGN. Any adopted methodology must also be acceptable to the IPv6 Label Committee since they plan to use both the interoperability and conformance testing specifications in their certification program. The present document recommends using the TIPHON methodology as a basis for deriving the IPv6 interoperability testing methodology in accordance with the IPv6 community's and the IPv6 Label Committee's approaches. Ideally this should result in a single, general methodology. TC-MTS will continue to liaise with EP TIPHON on this issue.

11.1.2 Integration with current 3GPP test suites

IPv6 will be embedded in UMTS systems and it will, therefore, be necessary for individual test cases to include extensive preambles that are not directly connected to IPv6 in order to bring an SUT into the context of IPv6 testing. Considering the huge investment in 3GPP test specifications it would be beneficial to investigate the possibility of reusing parts of these existing tests.

The current 3GPP test suites are in TTCN-2. The 3GPP testing group does not wish to write additional code in existing test suites to trap Ipv6 control messages in 3GPP data PDUs. Their future test suites may be in either TTCN-2 or 3. The IPv6 work will be in TTCN-3. Thus, a method of using the new eEurope 2005 TTCN-3 test suites with existing 3GPP TTCN-2 test suites without changing the latter must be found in order that the IPv6 work supports 3GPP's efforts.

11.1.3 Scheduling the production of test specifications

It is clear to the IETF community and ETSI that the best time for providing the test suites is during development before deployment. Early and cyclic test writing is useful in several ways to testers, implementers, standardization organizations and certification bodies (e.g. IPv6LC) (see clause 8).

11.2 Toolkit components

The generic testing toolkit has three major components:

- the textual components (see clause 9.7)
- the software components in TTCN-3 code (see clause 9.7);
- user's manual.

After development, each component of the testing toolkit should be validated during development and execution of the subsequent test suites - especially for the Core package. The three components will be used in the development of the test suites in each of the other packages.

11.3 Identification of tasks and resource estimate

The following tasks have been identified for WP0:

- Determine the elements of ISO/IEC 9646 [69] to incorporate into IPv6 conformance testing. Areas of interest include, but are not limited to, the appropriate test methods, possible POC locations, appropriate use of primitives or APIs, multi-layer protocol testing, and the requirements of testing different types of SUTs.
- Derive IPv6 interoperability testing methodology from the TIPHON's work on this subject.
- Develop an approach to incorporating TTCN-3 IPv6 specifications into the existing or future 3GPP TTCN-2 and TTCN-3 test suites.
- Determine the selection combinations and model them with switches. Check configuration compatibility across the possible combinations.
- Write common data structures; e.g. URLs, address notations, and other kinds of regular expressions.
- Collect preambles and postambles.
- Determine and write IPv6 datagram data to be used as content: text, voice, multimedia, files, etc.
- Write a User's Manual.

Table 1: Resource requirements for WP0

Task	Resource (MM)	Totals
General		**2**
Minimum requirements and selections	2	
Methodologies		**4**
IPv6 Interoperability Testing	3	
Conformance Testing based on ISO 9646 series [69]	1	
3GPP Specific		**4**
Incorporating IPv6 TTCN-3 suites into 3GPP R5 and beyond	2	
3GPP TTCN-2/3 Adaptations	2	
Generic Toolkit Development		**33**
Toolkit Development	6	
TTCN-3 tools	12	
Selection Switches	1	
User's Guide	2	
Validation of toolkit	12	
GRAND TOTAL		**43**

12 WP1: The Core package

12.1 Introduction

The Core Package is one of two essential packages of the programme, the other being the IPv6 Test Specification Toolkit.

This package contains the test specifications necessary for testing all functions that any node must perform in any situation regardless of any other additional features. For example, one node may implement mobility functions while another might implement QoS functions. However, each node must implement certain basic functions regardless of the node's specific function. These required basic functions compose the core requirements.

Figures 1 and 2 show the Core functional areas.

12.2 The minimum set of documents

The minimum set of requirements documents for the Core Package is as follows:

- RFC 2460 [28], IPv6 Specification;
- RFC 2461 [29], Neighbour Discovery for IPv6;
- RFC 2462 [30], IPv6 Stateless Address Autoconfiguration;
- RFC 2463 [31], Internet Control Message Protocol (ICMPv6) for IPv6;
- RFC 1981 [9], Path MTU Discovery for IPv6;
- RFC 2675 [45], IPv6 Jumbograms;
- RFC 2373 [16], IPv6 Addressing Architecture.

See table A.1 for an analysis of these documents in the context of the IPv6 test suite development project.

12.3 Identification of tasks and resource estimate

- Determine the functional and option selection requirements for the IPv6 node type.
- Write conformance and interoperability Test Suite Structure and Test Purposes for these requirements.
- Write the Core Test Suite using the TTCN-3 software tools from the Generic toolkit for both conformance and interoperability testing. Incorporate the option selection switches into the Test Suite.
- Code the adaptations required for incorporating the TTCN-3 test suites into the 3GPP TTCN-2 and 3 test suites.

Table 2: Resource requirements for WP1

Task	Resource (MM)	Totals
Conformance Test Specifications		**17**
Test Purposes	3	
Test Suite Development	5	
Validation	9	
Interoperability Test Specifications		**10**
Test Purposes	2	
Test Suite Development	6	
Validation	2	
GRAND TOTAL		**27**

13 WP2: The Transition package

13.1 Introduction

The transition mechanisms ensure the integration of IPv6 networks into existing IPv4 infrastructures and guarantee communications between the IPv4 and IPv6 worlds.

The transition between today's IPv4 Internet and a future IPv6-based one will be a long process during which both protocol versions will coexist. The IETF created the NGTrans Working Group, now dissolved, to assist in and proposed technical solutions for IPv6 transition. Currently, the global deployment of IPv6 is underway creating an Internet composed of IPv4-only, IPv6-only and IPv4/IPv6 networks and nodes. This deployment must be properly handled to avoid the separation of the Internet into distinct IPv4 and IPv6 networks while ensuring global addressing and connectivity for all IPv4 and IPv6 nodes.

A new IETF working group, the IPv6 Operations Working Group (v6ops), develops guidelines for the operation of a shared IPv4/IPv6 Internet and provides guidance for network operators on deploying IPv6 into existing IPv4-only networks as well as into new network installations. V6ops also defines scenarios for the Third Generation Partnership Project (3GPP) to assure transition towards IPv6. It shows clearly that transition mechanisms are one of the major issues both the IETF and 3GPP communities.

The transition mechanisms can be classified into four groups:

- *Mechanisms permitting the construction of an IPv6 network over an IPv4 infrastructure*. These mechanisms allows isolated IPv6 hosts, located on a physical link which is not directly connected to an IPv6 router, to become fully functional IPv6 hosts by using an IPv4 multicast domain as their virtual local link. The set of these mechanisms essentially uses v6 over v4 tunnels. The main mechanisms developed are 6over4 (Transmission of IPv6 over IPv4 Domains without Explicit Tunnels) and ISATAP (Intra-Site Automatic Tunnel Addressing Protocol).

- *Mechanisms permitting the accessibility to an already existing IPv6 network.* This method allows isolated IPv6 domains or hosts, attached to an IPv4 network which has no native IPv6 support, to communicate with other such IPv6 domains or hosts with minimal manual configuration before they can obtain native IPv6 connectivity. Transition mechanisms are 6to4 (Connection of IPv6 Domains via IPv4 Clouds) and Tunnel Broker.

- *Cohabitation mechanisms* permit communication between IPv4 and IPv6 applications. These mechanisms are used to allow communication between IPv4 and IPv6 applications. The translation can be done at different layers of the protocol stack:

    - At layer 2: by the creation of IPv4 over IPv6 tunnels. This is the operation mode of DSTM (Dual Stack Transition Mechanism) that uses IPv4 over IPv6 tunnels. This permits IPv4 applications to communicate over IPv6 infrastructure even if they have not been v6fied (not adapted to be used with IPv6).

    - At the transport layer: by the use of UDP or TCP Gateways.

    - At the application layer: by the use of ALG (Application Level Gateways) which integrate the dual stack. This can be the case for printer spoolers and web proxies.

    - At the edge of the site: by the use of header translation. SIIT and NAT-PT implement header translation.

- *Mechanisms to generate IPv6 packets from IPv4 applications*. The main mechanisms are "Bump in the Stack" RFC 2767 [52] and "Bump in the API" [64].

13.2 The minimum set of documents

For a full list and analysis of the reference documents for transitioning see table A.2.

Mechanisms for construction of an IPv6 network over an IPv4 infrastructure

6over4, defined in RFC 2529 [39], allows isolated IPv6 hosts, located on a physical link which has no directly connected IPv6 router, to become fully functional IPv6 hosts by using an IPv4 domain that supports IPv4 multicast as their virtual local link. In fact, IPv4 multicast can be considered as a virtual Ethernet.

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is described by an Internet draft. This mechanism is quite similar to 6over4. ISATAP treats the site's IPv4 infrastructure as a link layer for IPv6 but without requirement for IPv4 multicast. ISATAP enables intra-site automatic IPv6-in-IPv4 tunnelling whether globally assigned or private IPv4 addresses are used. To do this, ISATAP uses a particular interface identifier format that embeds an IPv4 address. This format supports IPv6 address configuration and simple link-layer address mapping. Because ISATAP is not yet stable, it is not included in this work package.

Mechanisms for accessing an existing IPv6 network

6to4 (Connection of IPv6 Domains via IPv4 Clouds) is described in RFC 3056 [59], a Proposed Standard. This mechanism permits to IPv6 sites to communicate with each other over an IPv4 network without explicit tunnel set-up, and for them to communicate with native IPv6 domains via relay routers. In fact it treats the wide area IPv4 network as a unicast point-to-point link layer.

Tunnel Broker is described by RFC 3053 [58]. Its standard type is Informational. The Tunnel Broker mechanism is based on the provision of dedicated web servers, called Tunnel Brokers, that automatically manage tunnel requests coming from the users. The web server provides information to create tunnels and automatically configures a router in the foreign site.

Because RFC 3053 [58] is in informational status only the 6to4 mechanisms described above should be considered, i.e. testing of Tunnel Broker is not included in this work package.

Cohabitation Mechanisms

SIIT RFC 2765 [50] is a protocol translation mechanism at the edge of the network that allows communication between IPv6-only and IPv4-only nodes via protocol independent translation of IPv4 and IPv6 datagrams. Thus, no state information is required for the session. The SIIT proposal assumes that V6 nodes are assigned a V4 address for communicating with V4 nodes.

NAT-PT RFC 2766 [51] is quite similar to SIIT. It provides transparent routing to end-nodes in the v6 realm communicating with end-nodes in the v4 realm and vice versa. This is achieved using a combination of Network Address Translation and Protocol Translation. Nevertheless, NAT-PT uses a pool of v4 addresses for assignment to v6 nodes on a dynamic basis as sessions are initiated across v4-v6 boundaries.

DSTM, not yet standardized, is intended for IPv6-only networks in which hosts still need to exchange information with other IPv4 hosts or applications. The main benefit of DSTM is that IPv4 applications can be run over an IPv6-only network.

Because DSTM is not yet standardized it is not included in this work package.

Mechanisms to generate IPv6 packets from IPv4 applications

The "Bump-in-the-Stack" mechanism described in RFC 2767 [52] translates IPv4 into IPv6, and vice versa using the IP conversion mechanism defined in SIIT [50]. Thus, the "Bump-in-the-Stack" mechanism permits hosts to communicate with other IPv6 hosts using existing IPv4 applications. This mechanism use an API translator inserted between the TCP/IP module and network card driver. When they communicate with the other IPv6 hosts, pooled IPv4 addresses are assigned to the IPv6 hosts internally, but the IPv4 addresses never leave them. Moreover, since the assignment is automatically carried out using DNS, users do not need to know if the target hosts are IPv6.

The "Bump-in-the-API" mechanism defined in RFC 3338 [64] inserts an API translator between the socket API module and the TCP/IP module in the dual stack hosts. It translates the IPv4 socket API function into the IPv6 socket API function and vice versa. With this mechanism, the translation can be simplified without IP header translation.

The status of the [RFC 2767] describing the "Bump-in-the-Stack" mechanism is Informational and the [64] for the "Bump-in-the-API" mechanism is currently Experimental. For that reason, these mechanisms are not included in this work package.

The minimum set of documents for transitioning is RFC 2529 [39], RFC 2765 [50], RFC 2766 [51] and RFC 3056 [59] and RFC 2893 [56] (e.g. Dual Stack, Configured tunnelling of IPv6 over IPv4, IPv4-compatible IPv6 addresses, and Automatic tunnelling of IPv6 over IPv4). The test specifications should also take into account that DNS mechanisms. These are defined in NAT-PT [51] (which is already a member of the set) and the DNS standards adapted to IPv6 described in RFC 1886 [8] and RFC 3152 [61] as Best Current Practices.

13.3 Identification of tasks and resource estimate

A few conformance and interoperability test suites have already been written. Conformance test suites exist only for the 6over4 protocol. Interoperability scenarios exist for 6to4 and SIIT/NAT. These interoperability scenarios are quite basic and need to be improved. Although there are a lot of different transition mechanisms (6to4, 6over4, SIIT and NAT-PT) their specification is based only on a few small RFCs which are quite easy to understand.

Table 3: Resource requirements for WP2

Task	Resource (MM)	Totals
General		**5**
Analysis of Minimum Requirements	2	
Test Methodology and Architecture	2	
Toolkit (Transitioning specific)	1	
3GPP specific		**4**
Incorporating IPv6 (Transitioning) TTCN-3 suites into 3GPP R5 and beyond	2	
(3GPP) TTCN-2/3 Adaptations	2	
Conformance Test Specifications		**11**
Test Purposes	2	
Test Suite Development	6	
Validation	3	
Interoperability Test Specifications		**7**
Test Purposes	1	
Test Suite Development	5	
Validation	1	
GRAND TOTAL		**27**

14 WP3: The Mobility package

14.1 Introduction

The Mobile IPv6 protocol allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. The mobile node may also continue to communicate with other stationary or mobile nodes after moving to a new link. The movement of a mobile node away from its home link is transparent to transport and higher-layer protocols and applications thanks to a particular router: the Home Agent. A Home Agent is a router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address. Thus, the Mobile IPv6 protocol adds more possibilities and benefits to the new IP protocol.

The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another just as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell. The mobile node's IP address remains unchanged during such movement.

Some newer IETF working groups (e.g. the NEMO Working Group working on network mobility support) need a complete and stable specification of Mobile IP. Network mobility support manages the mobility of an entire network that changes its single point of attachment and, thus, its reachability in the topology. These kinds of networks mobile networks and include one or more mobile routers connecting the network to the global Internet. Nodes behind the mobile routers are either fixed (keeping the same address on the mobile network at all times) or mobile (entering and leaving the mobile network as they roam with respect to it). Possible uses of network mobility support are in public transportation networks (buses, trains, taxis, aircrafts) or networks of sensors and computers deployed in vehicles.

14.2 The minimum set of documents

For a full list and analysis of the reference documents for mobility see table A.3.

Mobile IPv6 is mainly described in two drafts. The main draft called "*draft-ietf-mobileip-ipv6-XX*" where "XX" is the version number describing the complete MIPv6 architecture. At the time of writing, the last draft (Version 24) was released in July 2003. Implementation of the different draft versions cannot interoperate. The second important draft is "*draft-ietf-mobileip-mipv6-ha-IPSec-XX*" (06 is the current version) that describes the use of IPSec to protect Mobile IPv6 Signalling between Mobile Nodes and Home Agents.

Two other drafts are also important for the Mobile IPv6 community.

- *draft-ietf-mobileip-fast-mipv6-XX* (current version is 06): Fast Handovers for Mobile IPv6. When a mobile Node changes its Access Router to another, a process referred to as handover takes place. During this process, there is a time period when the Mobile Node is unable to send or receive IPv6 packets both due to link switching delay and IP protocol operations. This time period is referred to as handover latency. In many instances, the handover latency resulting from standard Mobile IPv6 handover procedures could be greater than what is acceptable to support real-time or delay sensitive traffic. Furthermore, reducing the handover latency could be beneficial to non real-time, throughput-sensitive applications as well. This document describes protocol enhancements to reduce as much as possible handover latency due to IP protocol operations. Link switching latency is unavoidable at the IPv6 protocol layer level.

- *draft-ietf-mobileip-hmipv6-XX (*current version is 08): Hierarchical Mobile IPv6 mobility management (HMIPv6). This draft introduces extensions to Mobile IPv6 and IPv6 Neighbour Discovery to allow for local mobility handling. Hierarchical mobility management for Mobile IPv6 reduces the amount of signalling between the different entities of MIPv6 (Mobile Node, Correspondent Nodes and Home Agent). The mechanisms described in the present document can also improve the Mobile IPv6 handoff performance.

Nevertheless, these two drafts were not implemented at the time of writing the present document. In fact, the minimum set of documents to use now is essentially the base draft "*draft-ietf-mobileip-ipv6-XX. draft-ietf-mobileip-mipv6-ha-IPSec-XX* has additional elements. This draft will become quickly mandatory. Indeed, it is not worthwhile to have a macro-mobility mechanism such as MIPv6 if the link between home-Agent and mobile node is unsecured.

In addition, nodes implementing mobile node functionality or Home Agent functionality must support Generic Packet Tunnelling (RFC 2473 [33])

The minimum set of reference documents for mobile IPv6 is RFC 2473 [33], MIPv6 [70], MobIPSec [72], HMIPv6 [68], and FastMIPv6 [66].

14.3 Identification of tasks and resource estimate

- MIPv6 is considered key for IPv6. Although IPv6 mobility support protocol continues to be "work-in-progress," the demand for tests is very strong. Whether at IPv6 interoperability events like Connectathon in the USA, TAHI events in Japan, and Plugtests in Europe, the largest demand is for Mobile IPv6 conformance and interoperability tests. Many are involved in MIPv6 test development, the principal players being the TAHI Project in Japan and the IRISA in France.

The MIPv6 protocol is quite difficult to understand. The associated draft is one of the biggest in the IETF community. Nevertheless, updating a test suite can be done effectively and quickly by incorporating the differences between the two drafts. These are reported in an annex of each new release. Expertise gained from the definition of previous test suite versions allow accelerated test suite production. In general, an entire test suite is not rewritten each time a new draft is published. Most of the resources are required to generate the first test suite.

Note that mobility in this sense is not the same as mobility as understood by 3GPP. IPv6 mobility is not considered to be relevant to 3GPP (see clause 6.2) in the context of this work package.

Table 4: Resource requirements for WP3

Task	Resource (MM)	Totals
General		**8**
Analysis of Minimum Requirements	2	
Test Methodology and Architecture	3	
Toolkit (Mobility specific)	3	
Conformance Test Specifications		**14**
Test Purposes	3	
Test Suite Development	8	
Validation	3	
Interoperability Test Specifications		**8**
Test Purposes	1	
Test Suite Development	6	
Validation	1	
GRAND TOTAL		**30**

15 WP4: The IPSec package

15.1 Introduction

IPSec RFC 2401 [17] provides security services at the IP layer for both IPv4 and IPv6 and is mandatory for IPv6 implementations. IPSec is designed to provide interoperable, high quality, and cryptographically-based security functions so that a system can select security protocols, determine the encryption algorithms to use for the services, and put in place the required cryptographic keys.

15.2 The minimum set of documents

For a full list and analysis of the reference documents for IPSec see table A.4.

The IPSec objectives are met by each of the two traffic security means: the Authentication Header (AH) RFC 2402 [18] and Encapsulating the Security Payload (ESP) RFC 2406 [22]. Cryptographic key management procedures and protocols allow either manual or automatic distribution of keys. Automatic key management is covered in IKE RFC 2409 [24], RFC 2408 [23], RFC 2412 [26].

Both AH and ESP protocols may be applied individually or jointly to provide a desired set of security services. Each protocol supports two modes of use: transport mode and tunnel mode. In the first mode, the protocols provide protection primarily for upper layer protocols; in the second mode, the protocols are applied to tunnelled IP packets.

The minimum set of requirements documents for IPSec is composed of RFC 2401 [17], RFC 2402 [18], RFC 2403 [19], RFC 2404 [20], RFC 2405 [21], RFC 2406 [22], and RFC 2410 [25].

15.3 Identification of tasks and resource estimate

There are some interoperability test suites for IPSec protocols. There are very few conformance test suites. These test suites were developed for the principal IPSec elements AH, ESP and IKE. There are no test suites for the other elements.

Imperative security needs coupled with the lack of IPSec test suites creates an excellent opportunity for ETSI to create IPv6 IPSec test suites and to host interoperability events that will satisfy the objectives of the EU, 3GPP, the IPv6 Forum, and the v6LC.

Testing IPSec is a new area and it is still uncertain how best to achieve it. For that reason a significant amount of resource needs to be spent on methodology, architectural and toolkit tasks.

Table 5: Resource requirements for WP4

Task	Resource (MM)	Totals
General		**18**
Analysis of Minimum Requirements	2	
Test Methodology and Architecture	8	
Toolkit (IPSec specific)	8	
3GPP specific		**2**
Incorporating IPv6 (IPSec) TTCN-3 suites into 3GPP R5 and beyond	1	
3GPP TTCN-2/3 Adaptations	1	
Conformance Test Specifications		**28**
Test Purposes	8	
Test Suite Development	10	
Validation	10	
Interoperability Test Specifications		**18**
Test Purposes	4	
Test Suite Development	11	
Validation	3	
GRAND TOTAL		**66**

16 WP5: The QoS package

16.1 Introduction

IPv6 has two QoS-related fields in its header:

- The Traffic Class Field - This 8-bit field can be used by originating nodes and/or routers to identify and distinguish between different classes or priorities of IPv6 packets. This element indicates to each node of the network the forwarding handling of each packet. This Traffic Class field is used in the Differentiated Service (DiffServ) QoS approach.

- The Flow Label Field - This 20-bit field can be used by a source to label sequences of packets for which it requests special handling by IPv6 routers. "Real-time" services are an example. This mechanism is still experimental and subject to change. It is in the early draft stages. The Flow label is used in the Integrated Services (IntServ) approach but may have other uses as well.

Flow Label usage standardization is still in its early stages. This, coupled with the fact that DiffServ appears as the most scalable solution to implement QoS, indicates that the first for QoS conformance and interoperability test development should cover the Traffic Class field for DiffServ.

When mature, Flow Label field for IntServ or other QoS solutions should be considered for test specifications but for the time being should not be considered for testing.

16.2 The minimum set of documents

For a full list and analysis of the reference documents for QoS see table A.5.

The IETF Differentiated Services (DiffServ) Working Group has standardized a common scheme for the 6-bit DS field RFC 2474 [34] and has defined the architecture and general use of DS field within the IPv6 Traffic Class byte RFC 2475 [35].

The minimum set of conformance and interoperability tests should include, as a minimum, the Per-Hop forwarding Behaviours (PHB): Assured Forwarding (AF) RFC 2597 [41], Expedited Forwarding (EF) RFC 2598 [42], and Best Effort (BE). Bandwidth assurance, delay assurance, and packet drop should be included in the test specifications

The informational RFC 1809 [7] contains opinions and suggestions about IPv6 Flow Label usage made during the concept's early development. The current intended semantics and usage of the Flow Label is in RFC 2460 [28], Appendix A. Finally, there are several proposals on Flow Label use in some IETF Internet Drafts. In conclusion, the test specifications must wait for a stable definition of Flow Label handling.

The minimum set of reference documents for Differentiated Services is RFC 2474 [34], RFC 2475 [35], RFC 2597 [41], and RFC 2598 [42].

For information, Flow Label references include RFC 1809 [7] and FlowLblSpec [67].

16.3 Identification of tasks and resource estimate

Until now there is no methodology for either conformance or interoperability QoS testing despite the express interest of network operators. The usual test suites developers do not include QoS in their products. It is also important to note that there are few performance test solutions in the IETF community.

QoS DiffServ conformance and interoperability testing requires a methodology that will include:

- Determination of the minimum functional and option selection requirements from the few documents available.
- Determination of appropriate QoS test methodologies for both conformance and interoperability testing.
- Development of appropriate methods for incorporating the TTCN-3 IPv6 specifications into the existing or future 3GPP TTCN-2 and -3 test suites.

QoS test specifications for conformance and interoperability tests will include the following items:

- Test Purposes for the minimum and remaining requirements.
- Toolkit components
- QoS conformance and interoperability Test Suites by using the TTCN-3 software tools from the Generic toolkit. Incorporate the option selection switch module into the Test Suite
- Finally, include the adaptations required for incorporating the TTCN-3 test suites into the 3GPP TTCN-2 and 3 test suites

Table 6: Resource requirements for WP5

Task	Resource (MM)	Totals
General		**11**
Analysis of Minimum Requirements	2	
Test Methodology and Architecture	7	
Toolkit (QoS specific)	2	
3GPP specific		**2**
Incorporating IPv6 (QoS) TTCN-3 suites into 3GPP R5 and beyond	1	
(3GPP) TTCN-2/3 Adaptations	1	
Conformance Test Specifications		**10**
Test Purposes	2	
Test Suite Development	4	
Validation	4	
Interoperability Test Specifications		**6**
Test Purposes	1	
Test Suite Development	4	
Validation	1	
GRAND TOTAL		**29**

17 WP6: The Routing package

17.1 Introduction

Routing protocols are divided into two groups. The interior gateway protocols (IGP) are in charge of routing packets within an autonomous IPv6 domains, whereas the exterior gateway protocols (EGP) are used between two or more domains.

Interior Gateway Protocols:

RIPng is the Routing Internet Protocol version 2 adapted to IPv6. This protocol uses distance vectors. It was the first routing protocol to be implemented because of its simplicity and stability in IPv4.

OSPFv3 (Open Shortest Path First for IPv6) is, as for IPv4, destined to become the required routing protocol. This protocol is based on the maintenance of link states. However, the IPv6 version is younger than RIPng.

IS-IS is a routing protocol developed by the OSI based on the maintenance of link states.

Exterior Gateway Protocols:

BGP-4 is the principal inter-domain routing protocol for IPv4. There are IPv6 extensions for routing of traffic between domains. In the IPv6 case, the protocol is called BGP-4+.

17.2 The minimum set of documents

For a full list and analysis of the reference documents for routing see table A.6.

According to "IPv6 Node Requirements" [73], routers must support the IPv6 Router Alert Option described in RFC 2711 [48].

Concerning the routing protocols, RIPng, OSPFv3 and BGP-4+ are required. IS-IS is in draft process and unstable.

- RIPng is described by RFC 2080 [13]. This RFC presents the changes required to the Routing Information Protocol (RIP) as specified in RFC 1058 [5] and RFC 2453 [27]. Thus, these two RFCs are required documents as well.

- OSPFv3 is discussed in RFC 2740 [49]. Similarly to RFC 2080 [13], it presents the modifications of OSPFv2 RFC 2328 [15] required to support IPv6. Thus, RFC 2080 [13] is a required document.

- RFC 2858 [53] adds extensions to BGP-4 RFC 1771 [6] to enable it to carry routing information for multiple Network Layer protocols (e.g., IPv6, IPX, etc.). In addition, RFC 2545 [40] provides IPv6 extensions. Thus, the minimum set of documents for BGP-4+ is RFC 1771 [6], RFC 2545 [40], and RFC 2858 [53].

17.3 Identification of tasks and resource estimate

To be a router, a host must perform the required router functions and run a routing protocol which is either an IGP, or an EGP, or both. Routers are the most important part in a network. Consequently a test development is mandatory. Routers developed by different companies must interoperate. If they implement the routing specification differently, they cannot forward messages. Conformity with standards is a must.

A lot of interoperability scenarios have been developed for routing. However, they are, in general, at a basic level. No methodology has been clearly defined. Thus, it is not rare to find two routers in the Internet with some interoperability problems even if they have made assurances to the contrary. Complete conformance test suites have not been developed for routing protocols, although this should have been the first step to assure a quality service. First of all, a methodology has to be defined for interoperability and conformance test activity. Moreover this work could be reused for some others protocols not directly related to IPv6.

The second step concerns the test development of routing protocols. The easiest protocol to understand and to implement is certainly the longstanding RIPng. The more complicated OSPFv3 is to become the routing protocol of reference and will replace RIPng in a near future. OSPFv3 is without doubts the most difficult routing protocol. Its specification is very bulky; its concepts are not easy to understand. Concerning EGP, test specifications are required for BGP-4+. This protocol is less complicated than OSPFv3 but more so for RIPng.

As a result, a large amount of resources are needed to write test specifications for these three protocols.

Table 7: Resource requirements for WP6

Task	Resource (MM)	Totals
General		**19**
Analysis of Minimum Requirements		5
Base Spec	1	
Ripng	1	
OSPFv3	2	
BGP-4+	1	
Test Methodology and Architecture		10
Base Spec	2	
Ripng	2	
OSPFv3	4	
BGP-4+	2	
Toolkit (Routing specific)		4
Base Spec	1	
Ripng	1	
OSPFv3	1	
BGP-4+	1	
Conformance Test Specifications		**26**
Test Purposes		9
Base Spec	1	
Ripng	2	
OSPFv3	3	
BGP-4+	3	
Test Suite Development		10
Base Spec	1	
Ripng	2	
OSPFv3	4	
BGP-4+	3	
Validation		
Base Spec	1	7
Ripng	2	
OSPFv3	2	
BGP-4+	2	
Interoperability Test Specifications		**16**
Test Purposes		4
Base Spec	1	
Ripng	1	
OSPFv3	1	
BGP-4+	1	
Test Suite Development		8
Base Spec	1	
Ripng	1	
OSPFv3	3	
BGP-4+	3	
Validation		4
Base Spec	1	
Ripng	1	
OSPFv3	1	
BGP-4+	1	
GRAND TOTAL		**61**

18 WP7: The Multicast package

18.1 Introduction

In order to have a Multicast service, two components are mandatory: a multicast routing protocol and a protocol to handle multicast groups.

An IETF working group is working on several protocols to provide multicast service. For the moment, the protocol of preference to handle multicast groups is Multicast Listener Discovery (MLD). For multicast routing, a few IGP (Interior Gateway Protocols) like PIM-SM, PIM-DM and some EGP (Exterior Gateway Protocols) such as BGMP are in development.

18.2 The minimum set of documents

For a full list and analysis of the reference documents for multicast see table A.7.

Because multicast routing protocols are still in early development, they should not be considered at this point in time.

Only MLD is of concern. This protocol enables each IPv6 router to discover the presence of multicast listeners on its directly attached links and to determine which multicast addresses are of interest to those nodes. There are two versions: MLDv1 and MLDv2. MLDv1 is derived from version 2 of IPv4's Internet Group Management Protocol IGMPv2. MLDv2 is derived from IGMPv3. MLDv2 adds support for "source filtering", that is, the ability of a node to report interest in listening to packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address. The status of MLDv1 is Proposed Standard (RFC 2710 [47]) whereas MLDv2 is the draft "draft-vida-mld-v2-XX.txt" [71] (current version is 07). When MLDv2 has been completed, it should take precedence over MLDv1.

As a consequence, the minimum document set is simply RFC 2710 [47]. Consideration should be given to test development for MLDv2 once its standard becomes stable.

18.3 Identification of tasks and resource estimate

In the next years, multicast will be of strong interest for both the Internet Community and the Telecommunication operators. Although the multicast protocols are not yet stable, a few experimentations have already been done on the M6Bone. The M6Bone network offers an IPv6 multicast service to interested sites. It enables use of multicast videoconference tools broadcasting events. The routing multicast protocol used on the whole network is PIM Sparse Mode and the protocol to handle groups is MLDv1.

Some very basic interoperability scenarios for MLDv1 have been developed by the UNH (University of New Hampshire InterOperability Lab). It is unknown if any conformance test suites exist.

The protocol specification of MLDv1 is quite easy to understand and has few requirements. It should be very easy to accomplish this work item. It should be kept in mind that, once adopted, MLDv2 will rapidly supersede MLDv1. MLDv2 should be downward compatible and, if required, it should not be difficult to upgrade an MLDv1 test suite.

Table 8: Resource requirements for WP7

Task	Resource (MM)	Totals
General		***2***
Analysis of Minimum Requirements	1	
Test Methodology and Architecture	1	
Conformance Test Specifications		**3**
Test Purposes	1	
Test Suite Development	1	
Validation	1	
Interoperability Test Specifications		**3**
Test Purposes	1	
Test Suite Development	1	
Validation	1	
GRAND TOTAL		**8**

19 Resources and funding

19.1 Roll-up of resources

The following chart rolls-up the resource requirements.

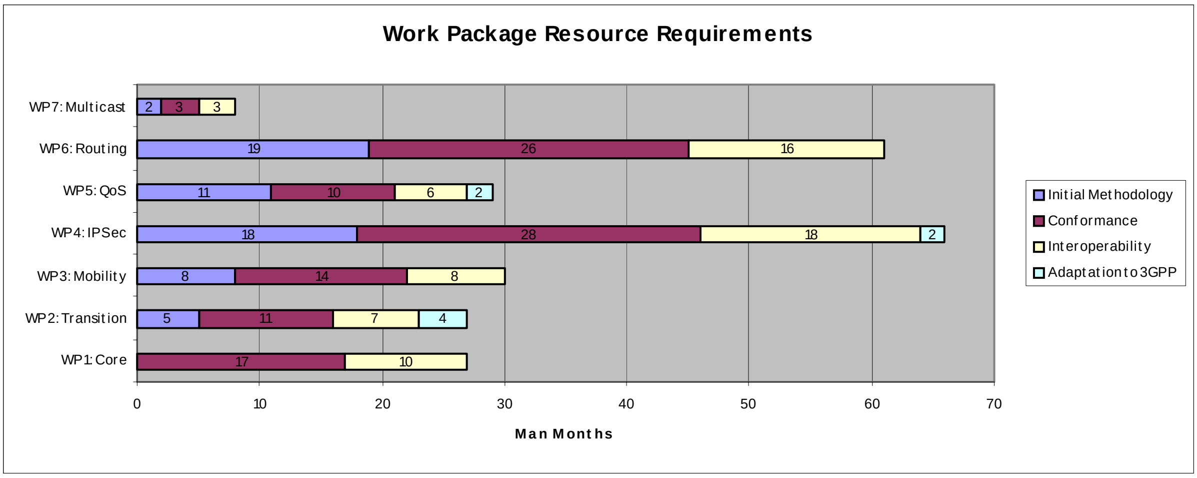

Figure 4: Roll-up of resources in man-months

19.2 Dependencies

The Toolkit (WP0) and Core package (WP1) are essential to all the other packages and should be completed first. The other work packages (WP2 - WP7) can be developed independently.

In each package, the 'General' aspects contain elements related to both conformance testing and interoperability testing.

The estimates for the resources needed to produce interoperability test specifications are based on the assumption that there is a certain amount of reuse of knowledge gained when writing the conformance test specifications. If conformance test specifications are not produced then the resource for interoperability testing should be increased by 20 %.

19.3 Funding

The programme presented in this proposal is extensive and will probably require a multiplicity of funding options. This can be

- voluntary contributions in terms of funding and/or manpower;
- STFs funded from the ETSI FWP and PTCC budgets;
- eEurope 2005;
- other European projects.

Note that the eEurope 2002 action plan provided 100 % funding. Such is not the case for eEurope 2005, where the EC expects 50 % cost-sharing. TC-MTS need to take these factors into account when planning the implementation of this programme.

Annex A:
Informational tables

Table A.1: Core Reference Documents

Area	Number	Testable Objects, Protocols	3GPP Utility (10-high) (0-low)	EU Utility (10-high) (0-low)	IPv6 Forum Priority (10-high) (0-low)	User Priority (10-high) (0-low)	Test Suites Coverage (10-low) (0-high)	Specification Stability (10-stable) (0-1st draft)	Conformance Test Suites (0-none) (10-many)	InterOp Test Suites (0-none) (10-many)
Core	RFC 1981	Path MTU Discovery	0	10	10	7	3	7	4	
Core	RFC 2675	IPv6 Jumbograms	0	10	10	7	3	7	0	
Core	RFC 2461	Neighbour Discovery & Redirect	4	10	10	7	4	8	5	
Core	RFC 2462	Stateless Address Autoconfiguration	10	10	10	10	3	8	4	
Core	RFC 2463	ICMPv6	0	10	10	7	3	8	5	4
Core	RFC 2460	IPv6 Basic Specification	2	10	10	7	3	9	5	6
Core	RFC 2373	IPv6 Addressing Architecture	10	2	10	8	3	9	1	

Table A.2: Transition Reference Documents

Area	Number	Testable Objects, Protocols	3GPP Utility (10-high) (0-low)	EU Utility (10-high) (0-low)	IPv6 Forum Priority (10-high) (0-low)	User Priority (10-high) (0-low)	Test Suites Coverage (10-low) (0-high)	Specification Stability (10-stable) (0-1st draft)	Conformance Test Suites (0-none) (10-many)	InterOp Test Suites (0-none) (10-many)
Transition	RFC 2766	NAT-PT	9	9	4	7	6	6	0	1
Transition	RFC 2893	Dual Stack, Configured tunnelling of IPv6 over IPv4, IPv4-compatible IPv6 addresses, Automatic tunnelling of IPv6 over IPv4	9	9	4	7	9	7		
Transition	RFC 2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels (v6overv4)	0	9	5	5	6	7	3	
Transition	RFC 2765	SIIT	0	9	4	4	6	7	0	1
Transition	RFC 3056	6to4	0	9	5	5	6	7		4
Transition	RFC 2473	IPv6 Tunnelling	0	9	4	4	4	8		

Table A.3: Mobility Reference Documents

Area	Number	Testable Objects, Protocols	3GPP Utility (10-high) (0-low)	EU Utility (10-high) (0-low)	IPv6 Forum Priority (10-high) (0-low)	User Priority (10-high) (0-low)	Test Suites Coverage (10-low) (0-high)	Specification Stability (10-stable) (0-1st draft)	Conformance Test Suites (0-none) (10-many)	InterOp Test Suites (0-none) (10-many)
Mobility	draft-ietf-mobileip-ipv6-21	MIPv6	0	8	10	8	5	1 (DRAFT)	2 (Draft-19)	2 (Draft-19)

Table A.4: IPSec Reference Documents

Area	Number	Testable Objects, Protocols	3GPP Utility (10-high) (0-low)	EU Utility (10-high) (0-low)	IPv6 Forum Priority (10-high) (0-low)	User Priority (10-high) (0-low)	Test Suites Coverage (10-low) (0-high)	Specification Stability (10-stable) (0-1st draft)	Conformance Test Suites (0-none) (10-many)	InterOp Test Suites (0-none) (10-many)
Security	RFC 3162	RADIUS	4	9	5	6	10	7		
Security	RFC 2402	IPSec AH	7	9	7	9	7	8	1	3
Security	RFC 2406	IPSec ESP	7	9	7	9	3	8	1	3

Table A.5: QoS Reference Documents

Area	Number	Testable Objects, Protocols	3GPP Utility (10-high) (0-low)	EU Utility (10-high) (0-low)	IPv6 Forum Priority (10-high) (0-low)	User Priority (10-high) (0-low)	Test Suites Coverage (10-low) (0-high)	Specification Stability (10-stable) (0-1st draft)	Conformance Test Suites (0-none) (10-many)	InterOp Test Suites (0-none) (10-many)
QoS	RFC 3175	RSVP, RSVP aggregation	0	5	7	5	10	5		
QoS	RFC 2507	Compression of IPv6 base and extension headers, IPv4 headers, TCP and UDP headers, and encapsulated IPv6 and IPv4 headers	8	5	4	6	10	7		
QoS	RFC 3095	Compression of RTP/UDP/IP, UDP/IP, and ESP/IP Header	8	5	6	6	10	7		1
QoS	RFC 2508	Compression of IP/UDP/RTP Header	0	5	4	3	10	7		
QoS	RFC 2474	IPv6 Traffic Class Field for Diffserv	8	5	7	7	8	8	1	0

Table A.6: Routing Reference Documents

Area	Number	Testable Objects, Protocols	3GPP Utility (10-high) (0-low)	EU Utility (10-high) (0-low)	IPv6 Forum Priority (10-high) (0-low)	User Priority (10-high) (0-low)	Test Suites Coverage (10-low) (0-high)	Specification Stability (10-stable) (0-1st draft)	Conformance Test Suites (0-none) (10-many)	InterOp Test Suites (0-none) (10-many)
Routing	RFC 2740	OSPFv3	0	0	6	3	7	7		
Routing	RFC 2080	RIPng	0	0	6	3	5	8	2	
Routing	RFC 2545	BGP4+	0	0	6	3	7	8	1	
Routing	draft-ietf-pim-sm-v2-new-06	PIM-SM	0	0	4	1	10	1 (DRAFT)		
Routing	RFC 2711	IPv6 Router Alert Option in Hop-by-Hop Option	0	0	3	0	10	5		
Routing	RFC 2894	Router renumbering	0	0	3	0	10	5		

Table A.7: Multicast Reference Documents

Area	Number	Testable Objects, Protocols	3GPP Utility (10-high) (0-low)	EU Utility (10-high) (0-low)	IPv6 Forum Priority (10-high) (0-low)	User Priority (10-high) (0-low)	Test Suites Coverage (10-low) (0-high)	Specification Stability (10-stable) (0-1st draft)	Conformance Test Suites (0-none) (10-many)	InterOp Test Suites (0-none) (10-many)
Mobility	draft-ietf-mobileip-ipv6-21	MIPv6	0	8	10	8	5	1 (DRAFT)	2 (Draft-19)	2 (Draft-19)
Multicast	RFC 2710	MLDv1	3	0	7	4	10	7		3
Multicast	RFC 3019	MIB for MLD	0	0	6	2	10	7		

Table A.8: 3GPP Reference Documents - by 3G TS

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 21.111	TS Group Terminals; USIM and IC card req.	R5 Pub.		
3G TS 23.002	TS Group Services and System Aspects; Network Aspects	R5 Pub.		IPv6 network services
3G TS 23.003	TS Group Core Network; Numbering, addressing and identification	R5 Pub.	2373, 2462, 3041	IPv6 addresses for MS: One or more IP address domains could be allocated to each PLMN. The IP v6 address structure is defined in RFC 2373 [16]. An IP v6 address may be allocated to an MS either permanently or temporarily during a connection with the network If the dynamic IPv6 stateless address autoconfiguration procedure is used, then each PDP context, or group of PDP contexts sharing the same IP address, is assigned a unique prefix as defined in 3GPP TS 23.060. As described in RFC 2462 [30] and IETF RFC 3041 [57], the MS can change its interface identifier without the GPRS network being aware of the change;
3G TS 23.060	TS Group Services and System Aspects; GPRS; Service description stage 2	R5 Pub.	2460, 2461, 2462, 2373	IPv6 (+ support for IPv4) for backbone network; PDCP supports IPv6 (+ IPv4); stateless or stateful address autoconfiguration for MS; GSN Address mand. IPv4 opt IPv6; RNC/BSC ATM option IPv6 opt IP option IPv6+IPv4 mand; Traffic Flow Template packet filters for IPv6 ; stateful: DHCP; stateless: RFC 2462 [30] without duplicate address detection
3G TS 23.107	TS Group Services and System Aspects; QoS concept and Architecture	R5 Pub.		Integrated Services (IntServ) signalled by RSVP and Differentiated Services (6-bit QoS attribute on each IP packet, DiffServ) controlled by applications residing in the TE different application specific QoS levels for the same PDP context
3G TS 23.207	TS Group Service and System Aspects; End-to_end QoS concept and architecture	R5 Pub.	2475, 2474	For each bi-directional media flow, the UE shall ensure that the 64 bit IPv6 address prefix of the source address of outgoing packets is the same as the prefix of the destination address supplied for incoming packets; - For bi-directional media flows, the P-CSCF(PDF), according to operator policy, may assume that the 64-bit IPv6 address prefix of the source address for downstream packets is the same as the prefix of the destination address for upstream packets of the same media flow; Service Based Local Policy may restrict the destination of packets to the addresses/ports included in the SIP signalling (SDP). Mechanisms such as MIPv6 Route Optimization which send packets to other addresses/ports may therefore not operate correctly; Diffserv required for GGSN; IP policy enforcement required for GGSN
3G TS 23.218	TS Group Core Network; IP Multimedia Session Handling; IP Multimedia call model; Stage 2	R5 Pub.		
3G TS 23.221	TS Group Services and System Aspects; Architectural requirements	R5 Pub.	2766, 2893, 3041	Interoperability between IPv4 and IPv6 for IPv4 and Ipv6 services: Mobile has IPv4 and Ipv6 Stack, Mobile has IPv6 and access IPv4 services (NAT-PT), Mobile has IPv6 and access IPv6 services via IPv4 network (RFC 2893 [56]); UE comply with RFC 3316 for Basic IP and IP Security. UE is assigned an IPv6 prefix, it can change the global IPv6 address according RFC 3041 [57] or similar means without updating the PS domain;

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 23.228	TS Group services and System Aspects; IP Multimedia Subsystem(IMS); Stage 2	R5 Pub.	3041	Mb: Reference Point to IPv6 networks; UE is assigned an IPv6 prefix, it can change the global IPv6 address according RFC 3041 [57] or similar means without updating the PS domain; As a result of the registration procedure, the P-CSCF determines the next hop toward the Serving-CSSEE These next-hop addresses could be IPv6 addresses, or could be names that are translated via DNS to an IPv6 address;
3G TS 23.228	TS Group services and System Aspects; IP Multimedia Subsystem(IMS); Stage 2	R6 Pub.	3041	no changes to R5
(3G TS 23.923)				
3G TR 23.974	TS Group Services and System Aspects; Support of Push service	R5 latest Draft	2460	With IPv6 carriers shall be able to assign static IP address to UE and so might be able to offer push services without needing a PDNS; The address of UE may be a private IPv4 or an IPv6 address;
3G TS 24.228	TS Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3	R5 Pub.		The PDP context will provide the UE with an IPv6 address, which will serve as the host address for the duration of the PDP context; Proxy-CSCF discovery with DHCPv6 or PDP Context Activation signalling; As a result of the registration procedure, the P-CSCF determines the next hop toward the Serving-CSSEE These next-hop addresses could be IPv6 addresses, or could be names that are translated via DNS to an IPv6 address;
3G TS 24.229	TS Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3	R5 Pub.	2401	All IM CN subsystem entities are allocated IPv6 addresses in accordance with the constraints specified in 3GPP TS 23.221 clause 5.1; For the purpose of access to the IM CN subsystem, UEs are assigned IPv6 prefixes in accordance with the constraints specified in 3GPP TS 23.221 clause 5.1; As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv6 address; for P-CSCF discovery employ Dynamic Host Configuration Protocol for IPv6, the DHCPv6 options for SIP servers and if needed DNS after PDP context activation or Transfer P-CSCF IPv6 address(es) within the PDP context activation procedure; The UE may request a DNS Server IPv6 address(es) via draft-ietf-dhc-dhcpv6-26 [74] or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060; For the purposes of the present document, the following terms and definitions given in RFC 2401 [17] Appendix A apply: Security association NOTE: A number of different security associations exist within the IM CN subsystem. Within the present document the term specifically applies to the security association that exists between the UE and the P-CSCF, as this is the only security association that has direct impact on SIP.

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 25.323	TS Group Radio Access Network; PDCP Specification	R5 Pub.	2507, 3095	header compression and decompression of IP data streams (e.g., TCP/IP and RTP/UDP/IP headers for IPv4 and IPv6) at the transmitting and receiving entity, respectively; Every PDCP entity uses zero, one or several different header compression protocol types. Several PDCP entities may be defined for a UE with each using the same or different protocol type. In this version of the specification, only two header compression protocol types, RFC 2507 [36] and RFC 3095 [60], are supported; The detailed operation of the RFC 2507 [36] header compression protocol is specified in RFC 2507 [36]. The mechanisms related to error recovery and packet reordering are also described in RFC 2507 [36]. These mechanisms shall be included in the functionality of the header compression supported by PDCP;
3G TS 25.412	TS Group Radio Access Network; UTRAN Iu interface signalling transport	R5 Pub.	2507, 2509, 2460, 2474,	CS and PS Domain IP Transport Option : IPv6 shall be supported. IPv4 support is optional; Due to the possible transition from IPv4 to IPv6 the IP dual stack support is recommended; An RNC using IP transport option shall support Diffserv code point marking. The Diffserv code point may be determined from the application parameters; An RNC using IP transport option having interfaces connected via slow bandwidth PPP links like E1/T1/J1 shall also support IP Header Compression and the PPP extensions ML/MC-PPP. In this case, the negotiation of header compression over PPP shall be performed via RFC 2474 [34]. An RNC using IP transport option shall support Diffserv code point marking. The Diffserv code point may be determined from the application parameters.
3G TS 25.413	TS Group Radio Access Network; UTRAN Iu interface RANAP signalling	R5 Pub.		Transport Layer Address contains IPv6 Address
3G TS 25.414	TS Group Radio Access Network; UTRAN Iu interface data transport and transport signalling	R5 Pub.	2460, 2474, 2507	CS-Domain User Plane IP Transport Option: An IP RNC/CN-node shall support IPv6. The support of IPv4 is optional. NOTE 1: This does not preclude single implementation and use of IPv4. IP dual stack support is recommended for the potential transition period from IPv4 to IPv6 in the transport network. RTCP over UDP over IPv6 shall be used (IPv4 may be used optionally); PS-Domain User Plane ATM Transport Option: IPv4 (RFC 791 [3]) shall be supported; IPv6 (RFC 2460 [28]) support is optional; PS-Domain User Plane IP Transport Option: An IP RNC/CN-node shall support IPv6. The support of IPv4 is optional. NOTE 2: This does not preclude single implementation and use of IPv4.IP dual stack support is recommended for the potential transition period from IPv4 to IPv6 in the transport network. RNC shall support fragmentation and assembly of GTP packets at the IP layer; Broadcast-Domain User Plane ATM Transport Option: IPv4 (RFC 791 [3]) shall be supported, IPv6 (RFC 2460 [28]) support is optional; Broadcast-Domain User Plane IP Transport Option: An IP RNC/CN-node shall support IPv6. The support of IPv4 is optional. NOTE 3: This does not preclude single implementation and use of IPv4.IP dual stack support is recommended for the potential transition period from IPv4 to IPv6 in the transport network. IP Differentiated Services code point marking shall be supported. The Diffserv code point may be determined from the application parameters.

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 25.424	TS Group Radio Access Network; UTRAN Iur Data Transport & Transport Signalling for Common Transport Channel Data Streams	R5 Pub.	2507, 2460, 2474,	Iur Data Transport IP Option: An IP UTRAN Node shall support IPv6 [28]. The support of IPv4 [3] is optional. Note: This does not preclude single implementation of IPv4.IP dual stack support is recommended for the potential transition period from IPv4 to IPv6 in the transport; An RNC using IP transport option having interfaces connected via slow bandwidth PPP links like E1/T1/J1 shall also support IP Header Compression RFC 2507 [36] and the PPP extensions ML/MC-PPP RFC 1990 [10], RFC 2686 [46]. In this case, negotiation of header compression RFC 2507 [36] over PPP shall be performed via RFC 2509 [38]; IP Differentiated Services code point marking RFC 2474 [34] shall be supported. The Diffserv code point may be determined from the application parameters.
3G TS 25.434	TS Group Radio Access Network; UTRAN Iub Interface Data Transport and Transport Signalling for Common Transport Channel Data Streams	R5 Pub.	2460, 2474, 2507,	Iub Data Transport IP Option: An IP UTRAN node shall support IPv6. The support of IPv4 is optional. NOTE: This does not preclude single implementation and use of IPv4.IP dual stack is recommended for the potential transition period from IPv4 to IPv6 in the transport network; IP Differentiated Services code point marking RFC 2474 [34] shall be supported. The Diffserv code point may be determined from the application parameters; Data Link Layer for IP Transport Option: An RNC or Node B supporting IP transport option and having interfaces connected via slow bandwidth PPP links like E1/T1/J1 shall also support IP Header Compression RFC 2507 [36] and the PPP extensions ML/MC-PPP RFC 1990 [10], RFC 2686[46]. In this case, negotiation of header compression RFC 2507 [36] over PPP shall be performed via RFC 2509 [38].

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 25.933	TS Group Radio Access Network; IP transport in UTRAN	R5 Pub.	2508, 2460, 2462, 2893, 2401, 2507, 2874	The use of Ipv6 shall not be precluded; Discussion of use of IPv6 in UTRAN, Transition IPv4 Ipv6. The dual stack mechanism is defined in RFC 2893 [56] as "a technique for providing complete support for both Internet protocols - IPv4 and IPv6 - in hosts and routers". Also in RFC 2893 [56], it is stated that the dual stack mechanism is "the most straightforward way for IPv6 nodes to remain compatible with IPv4-only nodes". A dual stack mechanism consists basically of the support for both IPv6 and IPv4 in the UTRAN IP nodes. However, as stated in [64], it is possible that a dual stack node (i.e. IPv6/IPv4 node) may operate, in IPv6-only or IPv4-only mode; a configuration switch may implement the selection of protocol version. This is very useful in the case of introducing UTRAN IPv6/IPv4 nodes in IPv4-only networks and in the IPv6-only network scenarios. Although the Dual Stack technique, as described in RFC 2893 [56], is enough to handle the migration from IPv4 to IPv6 networks, it is still possible to use the dual stack approach in conjunction with tunnelling mechanisms, as an option. This provides extra-flexibility in the configuration of the networks by the operators.; Since the dual stack nodes support both protocols, IPv6/IPv4 nodes may be configured with both IPv4 and IPv6 addresses, depending on the operation mode, i.e. if the node is in IPv4-only operation it requires only an IPv4 address, if the node is in IPv6-only operation it requires only an IPv6 address, and if the node is in IPv6/IPv4 operation, it requires both IPv4 and IPv6 addresses. The IPv6/IPv4 nodes use IPv4 mechanisms (e.g. DHCP, manual configuration, etc) to acquire their IPv4 address and the IPv6 mechanisms (e.g. stateless address autoconfiguration, manual configuration, etc) to obtain their IPv6 address. There are other mechanisms described in RFC 2893 [56] to acquire IPv4-compatible IPv6 addresses for the case where automatic tunnelling is used by the IPv6/IPv4 nodes. It is also necessary to keep track of which UTRAN hosts use IPv4 and which use IPv6 in order to know which type of address information to provide in the bearer control signalling. The only possible limitation that RFC 2893 [56] envisages for the dual stack mechanism is that in the near future scenario all of the nodes connected to both IPv6/IPv4 network would require IPv4 public addresses. This can be a problem if the operator is running out of IPv4 public addresses. However, note that the UTRAN does not require many IP addresses, so that should not be the case. Dynamic IPv4 address assignment may also be implemented by the use of a DHCPv6 server; Discussion of Security Architectures based on RFC 2401 [17]; UMTS decided to support RFC 2507 [36] for PDCP (3GPP TS 25.323). TS 25.323 specifies RFC 2507 [36] as the protocol being operated according to clause 3 of the IETF specification RFC 2507 [36] and to use the mechanisms related to error recovery and packet reordering as described in clauses 10 and 11 of RFC 2507 [36]. The clause 5.1.2.2 clearly includes the compressed_non_TCP as part of the Protocol IDentifiers. So, for the benefice of reusability, since it is the one selected for PDCP, RFC 2507 [36] should be preferred (compared with RFC 2508 [37]); RFC 2462 [30] and RFC 2874 [55] are not mentioned in the text.

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 27.007	TS Group Terminals; AT command set for User Equipment (UE)	Rel. 5 Pub.	2460, 2507, 3095	Change of the AT Command set according to the requirements on UE in other TS/TR.
3G TS 27.007	TS Group Terminals; AT command set for User Equipment (UE)	Rel. 6 Pub.	2460, 2507, 3095	Change of the AT Command set according to the requirements on UE in other TS/TR.
3G TS 27.060	TS Group Core Network; Packet Domain; MS supporting Packet Switched Services	Rel. 5 Pub.	2472, 2373, 1886	R: optionally IPv6 over PPP; An MS supporting IPv6 shall comply with the guidelines specified in 3GPP TS 23.221, clause "UE support of IPv6"; In the IMS the MS can request a P-CSCF IPv6 address(es) for SIP signalling via normal IETF DHCPv6 request/response signalling in combination with normal IETF DNS request/response signalling or by using the Protocol Configuration Option information element when requesting PDP context activation. The P-CSCF discovery procedure is specified in 3GPP TS 24.229; When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the uniqueness of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix itself is unique. Interface-Identifiers shall in any case be 64-bit long and follow standard interface-identifier guidelines as per RFC 2373 [16] and RFC 2472 [32]; The network responds with an Activate PDP Context Accept or an Activate PDP Context Reject, to the MS. The Protocol Configuration Options IE may contain configuration data such as a list of DNS server IPv6 addresses as described in 3GPP TS 29.061 [17]. In cases where the MS receives more than one server address, the MS shall adhere to the explicit prioritization order of the list. The PDP Address shall contain an IPv6 address composed of a Prefix and an Interface-Identifier. The size of the Prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [16] . The Interface-Identifier shall be used to create a link-local IPv6 address, to be used in continued MS - GGSN user-plane signalling. The Prefix in the PDP Address shall be ignored by the MS; RFC 1886 [8] not mentioned in the text.
3G TS 29.060	TS Group Core Network; GPRS; GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface	Rel. 5 Pub.	2460	Handling of IPv4/IPv6 Addresses in Create PDP Context Response, Update PDP Context Request, Update PDP Context Response, Forward Relocation Response; On the Gn and Gp interfaces the IPv4 (RFC 791 [3]) protocol shall be supported, IPv6 (RFC 2460 [28]) support is optional. This also applies to the Iu interface, when the ATM transport option is applied. When the IP transport option is applied on the Iu interface, both the IPv6 (RFC 2460 [28]) protocol and the IPv4 (RFC 791 [3]) protocol shall be supported;

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 29.061	TS Group Core Network; Packet Domain; Interworking between the PLMN supporting Packet Based Services and PDN	Rel. 5 Pub.	2373, 2462, 2472, 2461, 2710, 2460, 3162, 1886	When interworking with the IP networks, the Packet Domain can operate IPv4 or Ipv6; Transparent Access: The MS is given an address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address or IPv6 Prefix is used for packet forwarding between the Internet and the GGSN and within the packet domain. With IPv6, either Stateless or Stateful Address Autoconfiguration shall be used to assign an IPv6 address to the MS. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per APN; Non Transparent Access: When using IPv6 Address Autoconfiguration (either Stateless or Stateful), the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the PDP context activation, followed by a second signalling phase done in the user plane. The user plane signalling phase shall be either stateless or stateful. The stateless procedure involves only the MS and the GGSN. The stateful procedure involves the MS, GGSN (as DHCP relay agent) and one or several DHCP servers on the Intranet or ISP; When using IPv6, in some situations the MS may need additional configuration information from the Intranet or ISP besides the IP address. It may for example be IMS related configuration options (see 3GPP TS 24.229 [47]). If the MS is DHCP capable and the IPv6 address has been allocated using Stateless Address Autoconfiguration, the MS may use a procedure as in the example below to configure additional external network protocol parameters, or other parameters that apply to the Intranet or ISP. The GGSN shall in this case indicate to the MS that there is additional configuration information to retrieve by setting the O-flag in the Router Advertisements. This shall be configured per APN in the GGSN; The GGSN shall support IPv6 addresses and protocol for IMS signalling and IMS bearers; RADIUS: The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IP address or IPv6 prefix for the user; The Packet Domain could allow access to IP Multicast traffic coming from an external network. The support of IP-Multicast in the Packet Domain is optional. In order for the Packet Core Network to support Multicast traffic that will allow the MS to subscribe to multicast groups from outside the PLMN, the GGSN shall support IGMP (IPv4) and/or MLD (IPv6) and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM. IGMP/MLD is an integral part of IP. All hosts wishing to receive IP multicasts are required to implement IGMP (or equivalent) and class-D IPv4 addresses or MLD and IPv6 multicast according to RFC 2710 [47]. IGMP/MLD messages are encapsulated in IP datagrams. To be able to deliver IP-Multicast packets to the appropriate TEs, the GGSN may have an IP-Multicast proxy functionality; Gi-Interface: RADIUS Authentication and RADIUS Accounting shall be used according to RFC 2865 [54] and RFC 3162 [62]; RFC 1886 [8] is not mentioned in the text.

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
3G TS 29.162	TS Group Core Network; Interworking between the IM CN subsystem and IP networks	Rel. 5 latest Draft		
3G TS 29.163	TS Group Core Network; Interworking between the IM CN subsystem and CS networks	Rel. 6 latest Draft	2474, 2475	The IM CN subsystem shall use SIP to manage IP multimedia sessions in a 3GPP environment, it shall also use IPv6 as the transport mechanism for both SIP session signalling and media transport; The IM-MGW shall perform DiffServ Code Point (DSCP) markings (see RFC 2474 [34]) on the IP packets sent towards the UE across the Gi interface, and allows DiffServ compliant routers and GGSNs to schedule the traffic accordingly. The IETF Differentiated Services architecture (see RFC 2475 [35]) shall be used to provide QoS for the external bearer service. The DSCP shall be operator configurable
3G TS 32.015 (12.05??)				
3G TS 33.108	TS Group Services and System Aspects; 3G Security; Handover interface for Lawful Interception	Rel. 5 Pub., Rel. 6 Pub.	2126	Use of IPv6 addresses; Since the upper-layer protocols are not self-describing, ISO Transport Service on top of TCP (ITOT), also referred to as TPKT, as defined in RFC 1006 [4] and later updated by RFC 2126 [62] is used to encapsulate the "LI application" messages before handing them off to TCP. Therefore, TPKT shall be required and used in the transport stack of the IRI delivery interface (i.e., "LI application" messages/TPKT/TCP/IP). Protocol class 0 defined in RFC 2126 [62] shall be supported (Annex G:infomative).
3G TS 33.203	TS Group Services and System Aspects; 3G Security; Access security for IP-based services	Rel. 5 Pub.	2406, 2401, 2402	IPSec ESP as specified in reference RFC 2406 [22] shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. IPSec ESP general concepts on Security Policy management, Security Associations and IP traffic processing as described in reference RFC 2401 [17] shall also be considered. ESP integrity shall be applied in transport mode between UE and P-CSCF; For protecting IMS signalling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode set-up (see clause 7.2) is used to negotiate the SA parameters required for IPSec ESP with authentication, but without confidentiality.
(3G TS 42.017) only Rel. 4				
3G TS 48.018	TS Group GSM/EDGE Radio Access Network; GPRS; BSS - SGSN; BSSGP	Rel. 5 Pub.		
TIPHON				
TS 101 314 V4.1.1	TIPHON; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points	Rel. 4 Draft		
TS 101 882-1	TIPHON; Protocol Framework Definition - part1; Meta-protocol design rules, development method, and mapping guideline	Rel. 4 Draft		

Reference	Title	Release/ Status	Referenced RFC and internet drafts relating to IPv6	Use of IPv6 (citations)
TS 101 882-2	TIPHON; Protocol Framework Definition - part 2; Registration and Service Attachment service Meta Protocol definition	Rel. 4 Draft		
TS 101 882-3	TIPHON; Protocol Framework Definition - part 3; Simple Call service Stage 1 and 2 definition (meta-protocol)	Rel. 4 Draft		IPv6 Addresses may be used in the Protocol
TS 101 882-4	TIPHON; Protocol Framework Definition - part 4; Media Control Service; meta-protocol definition	Rel. 4 Draft		IPv6 Addresses may be used in the Protocol
TS 101 883	TIPHON; Technology Mapping; Implementation of TIPHON architecture using H.323	Rel. 4 Draft		IPv6 Addresses may be used in the Protocol
TS 101 884	TIPHON; Technology Mapping; Implementation of TIPHON architecture using SIP	Rel. 4 Draft		
TS 101 885	TIPHON; Technology Mapping; Technology Mapping of TIPHON reference point N to H.248/MEGACO protocol	Rel. 3		
TS 102 108	TIPHON; H248/MEGACO Profile for TIPHON reference point I3; ICF control over reference point I3	Rel. 4 Pub.		IPv6 Addresses may be used in the Protocol, QoS: DiffServ and RSVP
TR 101 308	TIPHON; Requirements Definition Study; SIP and H.323 Interworking		2401	
TR 101 326 V.2.0.0	TIPHON; The procedure for determining IP addresses for routing packets on interconnected IP networks that support public telephony			The TIPHON standards do not specify the choice of version of IP protocol and are compatible with either version because the TIPHON standards generally apply above the network layer. Thus the choice of Internet Protocol version and any interworking between versions is outside the scope of TIPHON. Using IPv6 Addresses
TS 101 329-3	TIPHON; End-to-end QoS in TIPHON systems; Par t3: Signalling and control of end-to-end QoS	Rel. 3	2475	
DEG/TIPHON -08006		work started		Security, Authentication of IPv6 in TIPHON

Table A.9: 3GPP Reference Documents - by IETF RFC

IETF Reference	Title	Domain	3G Reference
RFC 1886 [8]	DNS Extensions to support IP version 6	DNS	3G TS 27.060, 3G TS 29.061
RFC 2126 [62]	ISO Transport Service on top of TCP (ITOT)		3G TS 33.108
RFC 2373 [16]	IP Version 6 Addressing Architecture	Core	3G TS 23.003, 3G TS 23.060, 3G TS 27.060, 3G TS 29.061
RFC 2401 [17]	Security Architecture for the Internet Protocol	Security	3G TS 24.229, 3G TS 25.933, 3G TS 33.203, TR 101 308
RFC 2402 [18]	IP Authentication Header	Security	3G TS 33.203
RFC 2406 [22]	IP Encapsulating Security Payload (ESP)	Security	3G TS 33.203
RFC 2460 [28]	Internet Protocol, Version 6 (IPv6) Specification	Core	3G TS 23.060, 3G TR 23.974, 3G TS 25.412, 3G TS 25.414, 3G TS 25.424, 3G TS 25.434, 3G TS 25.933, 3G TS 27.007, 3G TS 29.060, 3G TS 29.061
RFC 2461 [29]	Neighbour Discovery for IP Version 6 (IPv6)	Autoconfiguration	3G TS 23.060, 3G TS 29.061
RFC 2462 [30]	IPv6 Stateless Address Autoconfiguration	Autoconfiguration	3G TS 23.003, 3G TS 23.060, 3G TS 25.933, 3G TS 29.061
RFC 2472 [32]	IP Version 6 over PPP	IPv6 over L L	3G TS 27.060, 3G TS 29.061
RFC 2474 [34]	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	QoS	3G TS 23.207, 3G TS 25.412, 3G TS 25.414, 3G TS 25.424, 3G TS 25.434, 3G TS 29.163
RFC 2475 [35]	An Architecture for Differentiated Services	QoS	3G TS 23.207, 3G TS 29.163, TS 101 329-3

IETF Reference	Title	Domain	3G Reference
RFC 2507 [36]	IP Header Compression	Compression	3G TS 25.323, 3G TS 25.412, 3G TS 25.414, 3G TS 25.424, 3G TS 25.434, 3G TS 25.933, 3G TS 27.007
RFC 2508 [37]	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links	Compression	3G TS 25.933
RFC 2710 [47]	Multicast Listener Discovery (MLD) for IPv6	Multicast	3G TS 29.061
RFC 2766 [51]	Network Address Translation - Protocol Translation (NAT-PT)	Transition	3G TS 23.221
RFC 2874 [55]	DNS Extensions to Support IPv6 Address Aggregation and Renumbering	DNS	3G TS 25.933
RFC 2893 [56]	Transition Mechanisms for IPv6 Hosts and Routers	Transition	3G TS 23.221, 3G TS 25.933
RFC 3041 [57]	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	Autoconfiguration	3G TS 23.003, 3G TS 23.221, 3G TS 23.228
RFC 3095 [60]	RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed	Compression	3G TS 25.323, 3G TS 27.007
RFC 3162 [62]	RADIUS and IPv6	AAA	3G TS 29.061

Table A.10: Existing Conformance Test Suites

Conformance test suites	Standard Status	IRISA/ENST-Bretagne	TAHI	UNH	Agilent	Spirent	NETTEST	IXIA	Row Total
Test suites availability		**All Free**	**All Free**	**ATS**	**Nothing**	**Nothing**	**Nothing**	**Nothing**	
IPv6 Core Protocol:									
a) IPv6 Specification RFC 2460 [28]	PROPOSED STANDARD		X	X	X		X	X	5
b) IPv6 Jumbo Payload Option RFC 2675 [45]	PROPOSED STANDARD								0
c) ICMPv6 RFC 2463 [31]	PROPOSED STANDARD		X	X		X	X	X	5
d) Neighbour Discovery RFC 2461 [29]	PROPOSED STANDARD		X	X		X	X	X	5
e) Path MTU Discovery RFC 1981 [9]	PROPOSED STANDARD		X	X			X	X	4
f) Stateless Address Autoconfiguration RFC 2462 [30]	PROPOSED STANDARD		X	X			X	X	4
g) Redirect RFC 2461 [29]	PROPOSED STANDARD			X			X		2
Mobile IPv6 (v19): [the last is v20]	DRAFT								2
a) Correspondent Node Part		X							
b) Home Agent Part		X							
c) Mobile Node Part		X	X						
Transition:									
a) IPv6 over IPv4 Tunnel RFC 2529 [39]	PROPOSED STANDARD		X			X		X	3
b) SIIT/NAT-PT RFC 2765 [50], 2766 [51]	PROPOSED STANDARD								
Routing:									
a) RIPng Operations RFC 2080 [13]	PROPOSED STANDARD			X		X			2
b) BGP4+ RFC 2858 [53], 2545 [40]	PROPOSED STANDARD				X				1
c) IS-IS	DRAFT				X				1
Security:									
a) IPSec AH RFC 2401 [17], 2402 [18]	PROPOSED STANDARD		X						1
b) IPSec ESP RFC 2401 [17], 2406 [22]	PROPOSED STANDARD		X						1
QOS:									
a) IPv6 Traffic Class Field for Diffserv RFC 2474 [34], 2475 [35], 3260 [63]	PROPOSED STANDARD					X			1

Table A.11: Existing Interoperability Test Suites

Interoperability test scenarios		IRISA/ ENST-Bretagne	TAHI	UNH	Agilent	HSC	ULB	Spirent	NETTEST	IXIA	Row Total
Test scenarios availability		**All Free**	**All Free**	**All Free**	**Nothing**	**Nothing**	**All Free**	**Nothing**	**Nothing**	**Nothing**	
IPv6 Basic Interoperability:											
a) IPv6 Basic Specifications			X	X	X			X	X	X	6
b) IPv6 over PPP RFC 2472 [32]	PROPOSED STANDARD	X			X			X		X	4
c) ICMP echo interoperability				X				X	X	X	4
d) TCP interoperability				X				X		X	3
e) UDP interoperability				X				X	X	X	4
Transition Mechanisms:											
a) 6over4 RFC 2529 [39]	PROPOSED STANDARD										
b) 6to4 encapsulation RFC 3056 [59]	PROPOSED STANDARD	X			X			X	X		4
c) SIIT/NAT-PT RFC 2765 [50], 2766 [51]	PROPOSED STANDARD	X									1
Routing:											
a) RIPng RFC 2080 [13]	PROPOSED STANDARD	X	X					X	X	X	5
b) OSPFv3 RFC 2740 [49]	PROPOSED STANDARD		X	X			X	X	X		5
c) BGP4+ RFC 2545 [40],2858 [53]	PROPOSED STANDARD		X		X					X	3
d) IS-IS	DRAFT				X						1
Security:											
a) IPSec RFC 2401 [17], 2402 [18], 2406 [22]	PROPOSED STANDARD		X			X			X		3
b) IKE RFC 2409 [24]	PROPOSED STANDARD		X			X					2
Header Compression:	PROPOSED STANDARD										
a) ROHC RFC 3095 [60]		X									1
Multicast											
a) Multicast Listener Discovery(MLD) RFC 2710 [47]	PROPOSED STANDARD			X					X	X	3
QOS											
a) IPv6 Traffic Class Field for Diffserv RFC 2474 [34], 2475 [35], 3260 [63]	PROPOSED STANDARD										
Mobile IPv6	DRAFT	X		X							2

Annex B: Patterns

Some test specification users are likely to want to embed the IPv6 test specifications into their own specific test specifications. Other users may want to extend the existing test specifications with their own test cases. In both cases, the test architecture may be changed even if the types of the test components are the same. To fulfil these needs in an efficient way, it is proposed to use a pattern approach. This allows extensive reuse of code which will speed up test development.

The pattern approach uses principles already established in software engineering. The general concepts are decomposition, abstraction, encapsulation and parameterization.

In decomposition, a test purpose is broken down into parts. Abstraction is then done on these parts leading to a parameterized abstract part with its set of actual parameters. The parameterized abstract local part as well as the different parameters values are the test patterns. These are simple patterns which describe only local views of the test purpose. Abstraction can be done on a general level as well but it is recommended to remain at the local level.

Test patterns should be independent from concrete architectures and represent the local view of one entity implementing a function or a part of a service together with other entities.

Test patterns must be applicable to a number of different test purposes to justify the effort in deriving them. A local part of a test purpose which is usable in only one test purpose is not a test pattern.

When putting together different patterns to describe a test purpose it is necessary to describe the coordination to be done. This description is documented in the "coordination policy".

From these test patterns, the pattern is implemented in TTCN-3. For each test pattern and each protocol, an altstep, function or template is written. The coordination policy defined for the patterns is then implemented within the TTCN-3 entities.

The steps for developing and using patterns are shown below:

- Decomposition of the Test Purposes into local parts.
- Abstraction of the local parts into parameterized local parts.
- Decision if a test pattern exists.
- Decision if the toolkit already contains the test pattern.
- Incorporate the co-ordination policy.
- The test case for the test purpose is written using the test patterns and the co-ordination policy. The PTCs are created for the different local entities executing the functions and/or altsteps according to the test patterns with their appropriate parameters.

The test patterns may be derived in the following ways:

- Top-down-approach: Look at different test purposes and finding out by decomposition and abstraction what the test patterns are. Then, implement all test patterns for the different protocols.
- Bottom-up approach: Look at the functions and services a protocol implements and find out the local parts of these functions and services. Abstract the protocol local parts and determine the concrete values of the parameters. Define the test patterns. Afterwards implement the test patterns for the different protocols.
- Mixed approach: combination of the top-down and bottom-up approach.

Like test purposes, test patterns are written in prose. A pattern contains specific information separated into different paragraphs:

- name and intent,
- problem and context including the parameters,
- abstract description of the pattern structure with requirements for the coordination policy and assignment of verdicts,
- known uses and related patterns.

The patterns are written in TTCN-3 in one or possibly more modules.

The result is a set of test patterns and their implementation in TTCN-3. It does not contain test coordination measures and test architecture.

It is possible to embed the IPv6 specific parts into specific test cases of the users in the same way IPv6 Protocols are embedded into user-specific protocols.

It is also possible to add user-specific IPv6 test cases for a new test architecture. The test cases for the new test architecture are composed from parts already implemented with the appropriate coordination measures.

When using a patterns approach for testing, the costs for generating test specifications can be reduced depending on the ratio between the new and the reusable parts. For testing protocols in general, the implementation of the protocol specific parts of the tests is the most costly and have a high reuse factor. Our member's experience has shown that the reduction of costs will be approximately 60 % to 80% when using an existing toolkit. The specification of test patterns and the implementation of a toolkit has a high up-front cost. The member estimates that this up-front work brings down the cost savings of using the toolkit approach in this project to between 10 % and 20 %.

Annex C: Bibliography

IETF RFC 3068: "An Anycast Prefix for 6to4 Relay Routers", C. Huitema, June 2001.

IETF RFC 3089: "A SOCKS-based IPv6/IPv4 Gateway Mechanism", H. Kitamura, April 2001.

IETF RFC 3142: "An IPv6-to-IPv4 Transport Relay Translator", J. Hagino, K. Yamamoto, June 2001.

draft-ietf-isis-ipv6-05.txt: "Routing IPv6 with IS-IS", Christian E. Hopps, January 2003, Internet-Draft.

draft-ietf-ngtrans-isatap-12.txt: "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", F. Templin, T. Gleeson, M. Talwar, D. Thaler, January 24, 2003.

draft-ietf-pim-dm-new-v2-03.txt: "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification" (Revised), Andrew Adams, Jonathan Nicholas, William Siadak, February 2003.

draft-ietf-pim-sm-v2-new-07.txt: "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification" (Revised), Bill Fenner, Mark Handley, Hugh Holbrook, Isidor Kouvelas, 2 March 2003.

ETSI TS 102 237-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Interoperability test methods & approaches; Part 1: Generic approach to interoperability testing".

History

Document history		
V1.1.1	July 2003	Publication