IPv6 Working Group
Internet-Draft

John Loughney (ed)
Nokia
March 3, 2003

Expires: September 3, 2003

IPv6 Node Requirements
draft-ietf-ipv6-node-requirements-03.txt

Status of this Memo

Copyright Notice

Abstract

This document defines requirements for IPv6 nodes. It is expected that IPv6 will be deployed in a wide range of devices and situations. Specifying the requirements for IPv6 nodes allows IPv6 to function well and interoperate in a large number of situations and deployments.

Table of Contents

1. Introduction

The goal of this document is to define the set of functionality required for an IPv6 node. Many IPv6 nodes will implement optional or additional features, but all IPv6 nodes can be expected to implement the mandatory requirements listed in this document.

This document tries to avoid discussion of protocol details, and references RFCs for this purpose. In case of any conflicting text, this document takes less precedence than the normative RFCs, unless additional clarifying text is included in this document.

During the process of writing this document, any issue raised regarding the normative RFCs, the consensus is, whenever possible, to fix the RFCs and not to add text in this document. However, it may be useful to include this information in an appendix for informative purposes.

Although the document points to different specifications, it should be noted that in most cases, the granularity of requirements are smaller than a single specification, as many specifications define multiple, independent pieces, some of which may not be mandatory.

As it is not always possible for an implementer to know the exact usage of IPv6 in a node, an overriding requirement for IPv6 nodes is that they should adhere to John Postel's Robustness Principle:

> Be conservative in what you do, be liberal in what you accept from others. [RFC793].

1.1 Requirement Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC-2119].

1.2 Scope of this Document

IPv6 covers many specifications. It is intended that IPv6 will be deployed in many different situations and environments. Therefore, it is important to develop the requirements for IPv6 nodes, in order to ensure interoperability.

This document assumes that all IPv6 nodes meet the minimum requirements specified here.

1.2 Description of IPv6 Nodes

From Internet Protocol, Version 6 (IPv6) Specification [RFC-2460] we have the following definitions:

Description of an IPv6 Node

- a device that implements IPv6

Description of an IPv6 router

- a node that forwards IPv6 packets not explicitly addressed to itself.

Description of an IPv6 Host

- any node that is not a router.

2. Abbreviations Used in This Document

ATM	Asynchronous Transfer Mode
AH	Authentication Header
DAD	Duplicate Address Detection
ESP	Encapsulating Security Payload
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
MIB	Management Information Base
MLD	Multicast Listener Discovery
MTU	Maximum Transfer Unit
NA	Neighbor Advertisement
NBMA	Non-Broadcast Multiple Access
ND	Neighbor Discovery
NS	Neighbor Solicitation
NUD	Neighbor Unreachability Detection
PPP	Point-to-Point Protocol

PVC Permanent Virtual Circuit

SVC Switched Virtual Circuit

ULP Upper Layer Protocol

3. Sub-IP Layer

An IPv6 node must follow the RFC related to the link-layer that is sending packet. By definition, these specifications are required based upon what layer-2 is used. In general, it is reasonable to be a conformant IPv6 node and NOT support some legacy interfaces.

As IPv6 is run over new layer 2 technologies, it is expected that new specifications will be issued. This section highlights some major layer 2 technologies and is not intended to be complete.

3.1 Transmission of IPv6 Packets over Ethernet Networks - RFC2464

Transmission of IPv6 Packets over Ethernet Networks [RFC-2464] MUST be supported for nodes supporting Ethernet interfaces.

3.2 IP version 6 over PPP - RFC2472

IPv6 over PPP [RFC-2472] MUST be supported for nodes that use PPP.

3.3 IPv6 over ATM Networks - RFC2492

IPv6 over ATM Networks [RFC2492] MUST be supported for nodes supporting ATM interfaces. Additionally, the specification states:

> A minimally conforming IPv6/ATM driver SHALL support the PVC mode of operation. An IPv6/ATM driver that supports the full SVC mode SHALL also support PVC mode of operation.

4. IP Layer

4.1 Internet Protocol Version 6 - RFC2460

The Internet Protocol Version 6 is specified in [RFC-2460]. This specification MUST be supported.

Unrecognized options in Hop-by-Hop Options or Destination Options extensions MUST be processed as described in RFC 2460.

The node MUST follow the packet transmission rules in RFC 2460.

Nodes MUST always be able to receive fragment headers. However, if it

does not implement path MTU discovery it may not need to send fragment headers. However, nodes that do not implement transmission of fragment headers need to impose limitation to payload size of layer 4 protocols.

The capability of being a final destination MUST be supported, whereas the capability of being an intermediate destination MAY be supported (i.e. - host functionality vs. router functionality).

RFC 2460 specifies extension headers and the processing for these headers.

> A full implementation of IPv6 includes implementation of the following extension headers: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication and Encapsulating Security Payload. [RFC2460]

An IPv6 node MUST be able to process these headers. It should be noted that there is some discussion about the use of Routing Headers and possible security threats [IPv6-RH] caused by them.

4.2 Neighbor Discovery for IPv6 - RFC2461

Neighbor Discovery SHOULD be supported. RFC 2461 states:

> "Unless specified otherwise (in a document that covers operating IP over a particular link type) this document applies to all link types. However, because ND uses link-layer multicast for some of its services, it is possible that on some link types (e.g., NBMA links) alternative protocols or mechanisms to implement those services will be specified (in the appropriate document covering the operation of IP over a particular link type). The services described in this document that are not directly dependent on multicast, such as Redirects, Next-hop determination, Neighbor Unreachability Detection, etc., are expected to be provided as specified in this document. The details of how one uses ND on NBMA links is an area for further study."

Some detailed analysis of Neighbor discovery follows:

Router Discovery is how hosts locate routers that reside on an attached link. Router Discovery MUST be supported for implementations. However, an implementation MAY support disabling this function.

Prefix Discovery is how hosts discover the set of address prefixes that define which destinations are on-link for an attached link. Prefix discovery MUST be supported for implementations. However, the

implementation MAY support the option of disabling this function.

Neighbor Unreachability Detection (NUD) MUST be supported for all paths between hosts and neighboring nodes. It is not required for paths between routers. It is required for multicast. However, when a node receives a unicast Neighbor Solicitation (NS) message (that may be a NUD's NS), the node MUST respond to it (i.e. send a unicast Neighbor Advertisement).

Duplicate Address Detection MUST be supported (RFC2462 section 5.4 specifies DAD MUST take place on all unicast addresses).

Sending Router Solicitation MUST be supported for host implementation, but MAY support a configuration option to disable this functionality.

Receiving and processing Router Advertisements MUST be supported for host implementation s. However, the implementation MAY support the option of disabling this function. The ability to understand specific Router Advertisements is dependent on supporting the specification where the RA is specified.

Sending and Receiving Neighbor Solicitation (NS) and Neighbor Advertisement (NA) MUST be supported. NS and NA messages are required for Duplicate Address Detection (DAD).

Redirect Function SHOULD be supported. If the node is a router, Redirect Function MUST be supported.

4.3 Path MTU Discovery & Packet Size

4.3.1 Path MTU Discovery - RFC1981

Path MTU Discovery [RFC-1981] MAY be supported. Nodes with a link MTU larger than the minimum IPv6 link MTU (1280 octets) can use Path MTU Discovery in order to discover the real path MTU. The relative overhead of IPv6 headers is minimized through the use of longer packets, thus making better use of the available bandwidth.

The IPv6 specification [RFC-2460] states in chapter 5 that "a minimal IPv6 implementation (e.g., in a boot ROM) may simply restrict itself to sending packets no larger than 1280 octets, and omit implementation of Path MTU Discovery."

If Path MTU Discovery is not implemented then the sending packet size is limited to 1280 octets (standard limit in [RFC-2460]). However, if this is done, the host MUST be able to receive packets with size up to the link MTU before reassembly. This is because the node at the

other side of the link has no way of knowing less than the MTU is accepted.

4.3.2 IPv6 Jumbograms - RFC2675

IPv6 Jumbograms [RFC2675] MAY be supported.

4.4 ICMP for the Internet Protocol Version 6 (IPv6) - RFC2463

ICMPv6 [RFC-2463] MUST be supported.

4.5 Addressing

Currently, there is discussion on-going on support for site-local addressing.

4.5.1 IP Version 6 Addressing Architecture - RFC2373

The IPv6 Addressing Architecture [RFC-2373] MUST be supported. Currently, this specification is being updated by [ADDRARCHv3].

4.5.2 IPv6 Stateless Address Autoconfiguration - RFC2462

IPv6 Stateless Address Autoconfiguration is defined in [RFC-2462]. This specification MUST be supported for nodes that are hosts.

Nodes that are routers MUST be able to generate link local addresses as described in this specification.

From 2462:

> The autoconfiguration process specified in this document applies only to hosts and not routers. Since host autoconfiguration uses information advertised by routers, routers will need to be configured by some other means. However, it is expected that routers will generate link-local addresses using the mechanism described in this document. In addition, routers are expected to successfully pass the Duplicate Address Detection procedure described in this document on all addresses prior to assigning them to an interface.

Duplicate Address Detection (DAD) MUST be supported.

4.5.3 Privacy Extensions for Address Configuration in IPv6 - RFC3041

Privacy Extensions for Stateless Address Autoconfiguration [RFC-3041] SHOULD be supported. It is recommended that this behavior be configurable on a connection basis within each application when

available. It is noted that a number of applications do not work with addresses generated with this method, while other applications work quite well with them.

4.5.4 Default Address Selection for IPv6

Default Address Selection for IPv6 [DEFADDR] SHOULD be supported, if a node has more than one IPv6 address per interface or a node has more that one IPv6 interface (physical or logical) configured.

If supported, the rules specified in the document MUST be implemented. A node needs to belong to one site, however there is no requirement that a node be able to belong to more than one site.

This draft has been approved as a proposed standard.

4.5.5 Stateful Address Autoconfiguration

Stateful Address Autoconfiguration MAY be supported. DHCP [DHCPv6] is the standard stateful address configuration protocol. See section 5.3 for details on DHCP.

4.6 Multicast Listener Discovery (MLD) for IPv6 - RFC2710

Multicast Listener Discovery [RFC-2710] MUST be supported by nodes supporting multicast applications. A primary IPv6 multicast application is Neighbor Discovery (all those solicited-node mcast addresses must be joined).

When MLDv2 [MLDv2] has been completed, it SHOULD take precedence over MLD.

5. Transport Layer and DNS

5.1 Transport Layer

5.1.1 TCP and UDP over IPv6 Jumbograms - RFC2147

This specification MUST be supported if jumbograms are implemented [RFC-2675]. One open issue is if this document needs to be updated, as it refers to an obsoleted document.

5.2 DNS

DNS, as described in [RFC-1034], [RFC-1035], [RFC-1886], [RFC-3152] and [RFC-3363] MAY be supported. Not all nodes will need to resolve addresses. Note that RFC 1886 is currently being updated [RFC-1886-BIS].

5.2.2 Format for Literal IPv6 Addresses in URL's - RFC2732

RFC 2732 MUST be supported if applications on the node use URL's.

5.3 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

An IPv6 node that does not include an implementation of DHCP will be unable to obtain any IPv6 addresses aside from link-local addresses when it is connected to a link over which it receives a router advertisement with the 'M' flag (Managed address configuration) set and which contains no prefixes advertised for Stateless Address Autoconfiguration (see section 4.5.2). An IPv6 node that receives a router advertisement with the 'M' flag set and that contains advertised prefixes will configure interfaces with both stateless autoconfiguration addresses and addresses obtained through DHCP.

For those IPv6 Nodes that implement DHCP, those nodes MUST use DHCP upon the receipt of a Router Advertisement with the 'M' flag set (see section 5.5.3 of RFC2462). In addition, in the absence of a router, IPv6 Nodes that implement DHCP MUST attempt to use DHCP.

For IPv6 Nodes that do not implement DHCP, the 'M' flag of a Router Advertisement can be ignored. Furthermore, in the absence of a router, this type of node is not required to initiate DHCP.

An IPv6 node that does not include an implementation of DHCP will be unable to dynamically obtain any IPv6 addresses aside from link-local addresses when it is connected to a link over which it receives a router advertisement with the 'M' flag (Managed address configuration) set and which contains no prefixes advertised for Stateless Address Autoconfiguration (see section 4.5.2). In this situation, the IPv6 Node will be unable to communicate with other off-link nodes unless a global or site-local IPv6 address is manually configured.

6. IPv4 Support and Transition

IPv6 nodes MAY support IPv4.

6.1 Transition Mechanisms

IPv6 nodes SHOULD use native address instead of transition-based addressing.

6.1.1 Transition Mechanisms for IPv6 Hosts and Routers - RFC2893

If an IPv6 node implement dual stack and/or tunneling, then RFC2893

MUST be supported.

This document is currently being updated.

7. Mobility

Currently, the MIPv6 specification [MIPv6] is nearing completion. Mobile IPv6 places some requirements on IPv6 nodes. This document is not meant to prescribe behaviors, but to capture the consensus of what should be done for IPv6 nodes with respect to Mobile IPv6.

7.1 Mobile IP

Mobile IPv6 [MIPv6] specification defines requirements for the following types of nodes:

- mobile nodes
- correspondent nodes with support for route optimization
- home agents
- all IPv6 routers

Hosts MAY support mobile node functionality.

Hosts SHOULD support route optimization requirements for correspondent nodes. Routers do not need to support route optimization.

Routers MAY support home agent functionality.

Routers SHOULD support the requirements set for all IPv6 routers.

7.2 Securing Signaling between Mobile Nodes and Home Agents

The security mechanisms described in [MIPv6-HASEC] MUST be supported by nodes implementing mobile node or home agent functionality specified in Mobile IP [MIPv6].

7.3 Generic Packet Tunneling in IPv6 Specification - RFC2473

Generic Packet Tunneling [RFC-2473] MUST be suppored for nodes implementing mobile node functionality or Home Agent functionality of Mobile IP [MIPv6].

8. Security

This section describes the specification of IPsec for the IPv6 node. Other issues that IPsec cannot resolve are described in the security

considerations.

8.1 Basic Architecture

Security Architecture for the Internet Protocol [RFC-2401] MUST be supported.

8.2 Security Protocols

ESP [RFC-2406] MUST be supported. AH [RFC-2402] MUST be supported.

8.3 Transforms and Algorithms

Current IPsec RFCs specify the support of certain transforms and algorithms, NULL encryption, DES-CBC, HMAC-SHA-1-96, and HMAC-MD5-96. The requirements for these are discussed first, and then additional algorithms 3DES-CBC, AES-128-CBC, and HMAC-SHA-256-96 are discussed.

NULL encryption algorithm [RFC-2410] MUST be supported for providing integrity service and also for debugging use. The "ESP DES-CBC Cipher Algorithm With Explicit IV" [RFC-2405] MUST be supported. Security issues related to the use of DES are discussed in [DESDIFF], [DESINT], [DESCRACK]. It is currently viewed as an inherently weak algorithm, and no longer fulfills its intended role. It is still required by the existing IPsec RFCs, however. This document recommends the use of ESP DES-CBC only where interoperability is required with old implementations supporting DES-CBC.

The NULL authentication algorithm [RFC-2406] MUST be supported within ESP. The use of HMAC-SHA-1-96 within AH and ESP, described in [RFC-2404] MUST be supported. The Use of HMAC-MD5-96 within AH and ESP, described in [RFC-2403] MUST be supported. An implementer MUST refer to Keyed-Hashing for Message Authentication [RFC-2104].

3DES-CBC does not suffer from the issues related to DES-CBC. 3DES-CBC and ESP CBC-Mode Cipher Algorithms [RFC2451] MAY be supported. AES-128-CBC [ipsec-ciph-aes-cbc] MUST be supported, as it is expected to be a widely available, secure algorithm that is required for interoperability. It is not required by the current IPsec RFCs, however.

The "HMAC-SHA-256-96 Algorithm and Its Use With IPsec" [ipsec-ciph-sha-256] MAY be supported.

8.4 Key Management Methods

Manual keying MUST be supported

IKE [RFC-2407] [RFC-2408] [RFC-2409] MAY be supported for unicast traffic. Where key refresh, anti-replay features of AH and ESP, or on-demand creation of SAs is required, automated keying MUST be supported. Note that the IPsec WG is working on the successor to IKE [SOI]. Key management methods for multicast traffic are also being worked on by the MSEC WG.

9. Router Functionality

This section defines general considerations for IPv6 nodes that act as routers. It is for future study if this document, or a separate document is needed to fully define IPv6 router requirements. Currently, this section does not discuss routing protocols.

9.1 General

9.1.1 IPv6 Router Alert Option - RFC2711

The Router Alert Option [RFC-2711] MUST be supported by nodes that perform packet forwarding at the IP layer (i.e. - the node is a router).

9.1.2 Neighbor Discovery for IPv6 - RFC2461

Sending Router Advertisements and processing Router Solicitation MUST be supported.

10. Network Management

Network Management, MAY be supported by IPv6 nodes. However, for IPv6 nodes that are embedded devices, network management may be the only possibility to control these hosts.

10.1 MIBs

In a general sense, MIBs SHOULD be supported by nodes that support a SNMP agent.

10.1.1 IP Forwarding Table MIB

Support for this MIB does not imply that IPv4 or IPv4 specific portions of this MIB be supported.

10.1.2 Management Information Base for the Internet Protocol (IP)

Support for this MIB does not imply that IPv4 or IPv4 specific portions of this MIB be supported.

11. Security Considerations

This draft does not affect the security of the Internet, but implementations of IPv6 are expected to support a minimum set of security features to ensure security on the Internet. "IP Security Document Roadmap" [RFC-2411] is important for everyone to read.

The security considerations in RFC2460 describes the following:

> The security features of IPv6 are described in the Security Architecture for the Internet Protocol [RFC-2401].

For example, specific protocol documents and applications may require the use of additional security mechanisms.

The use of ICMPv6 without IPsec can expose the nodes in question to various kind of attacks including Denial-of-Service, Impersonation, Man-in-the-Middle, and others. Note that only manually keyed IPsec can protect some of the ICMPv6 messages that are related to establishing communications. This is due to chicken-and-egg problems on running automated key management protocols on top of IP. However, manually keyed IPsec may require a large number of SAs in order to run on a large network due to the use of many addresses during ICMPv6 Neighbor Discovery.

The use of wide-area multicast communications has an increased risk from specific security threats, compared with the same threats in unicast [MC-THREAT].

An implementer should also consider the analysis of anycast [ANYCAST].

12. References

12.1 Normative

[ADDRARCHv3] Hinden, R. and Deering, S. "IP Version 6 Addressing Architecture", Work in progress.

[DEFADDR] Draves, R., "Default Address Selection for IPv6", Work in progress.

[DHCPv6] Bound, J. et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Work in progress.

[MIPv6] Johnson D. and Perkins, C., "Mobility Support in

IPv6", Work in progress.

[MIPv6-HASEC] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling betweenMobile Nodes and Home Agents", draft-ietf-mobileip-mipv6-ha-ipsec-03 (work in progress), February 2003.

[MLDv2] Vida, R. et al., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", Work in Progress.

[RFC-1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC-1886] Thomson, S. et al.and Huitema, C., "DNS Extensions to support IP version 6", RFC 1886, December 1995.

[RFC-1886-BIS] Thomson, S., et al., "DNS Extensions to support IP version 6" Work In Progress.

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

[RFC-2096-BIS] Wasserman, M. (ed), "IP Forwarding Table MIB", Work in Progress.

[RFC-2011-BIS] Routhier, S (ed), "Management Information Base for the Internet Protocol (IP)", Work in progress.

[RFC-2104] Krawczyk, K., Bellare, M., and Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC-2373] Hinden, R. and Deering, S., "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

[RFC-2401] Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC-2402] Kent, S. and Atkinson, R., "IP Authentication Header", RFC 2402, November 1998.

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

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

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

[RFC-2406] Kent, S. and Atkinson, R., "IP Encapsulating Security Protocol (ESP)", RFC 2406, November 1998.

[RFC-2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC-2408] Maughan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[RFC-2409] Harkins, D., and Carrel, D., "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC-2410] Glenn, R. and Kent, S., "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998

[RFC-2451] Pereira, R. and Adams, R., "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998

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

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

[RFC-2462] Thomson, S. and Narten, T., "IPv6 Stateless Address Autoconfiguration", RFC 2462.

[RFC-2463] Conta, A. and Deering, S., "ICMP for the Internet Protocol Version 6 (IPv6)", RFC 2463, December 1998.

[RFC-2472] Haskin, D. and Allen, E., "IP version 6 over PPP", RFC 2472, December 1998.

[RFC-2473] Conta, A. and Deering, S., "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

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

[RFC-2711] Partridge, C. and Jackson, A., "IPv6 Router Alert Option", RFC 2711, October 1999.

[RFC-3041] Narten, T. and Draves, R., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[RFC-3152] Bush, R., "Delegation of IP6.ARPA", RFC 3152, August 2001.

[RFC-3363] Bush, R., et al., "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", RFC 3363, August 2002.

12.2 Non-Normative

[ANYCAST] Hagino, J and Ettikan K., "An Analysis of IPv6 Anycast" Work in Progress.

[DESDIFF] Biham, E., Shamir, A., "Differential Cryptanalysis of DES-like cryptosystems", Journal of Cryptology Vol 4, Jan 1991

[DESCRACK] Cracking DES, O'Reilly & Associates, Sebastapol, CA 2000.

[DESINT] Bellovin, S., "An Issue With DES-CBC When Used Without Strong Integrity", Proceedings of the 32nd IETF, Danvers, MA, April 1995.

[MC-THREAT] Ballardie A. and Crowcroft, J.; Multicast-Specific Security Threats and Counter-Measures; In Proceedings "Symposium on Network and Distributed System Security", February 1995, pp.2-16.

[SOI] C. Madson, "Son-of-IKE Requirements", Work in Progress.

[RFC-793] Postel, J., "Transmission Control Protocol", RFC 793, August 1980.

[RFC-1034] Mockapetris, P., "Domain names - concepts and facilities", RFC 1034, November 1987.

[RFC-2147] Borman, D., "TCP and UDP over IPv6 Jumbograms", RFC 2147, May 1997.

[RFC-2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2462, December 1998.

[RFC-2492] G. Armitage, M. Jork, P. Schulter, G. Harter, IPv6 over ATM Networks", RFC2492, January 1999.

[RFC-2675] Borman, D., Deering, S. and Hinden, B., "IPv6 Jumbograms", RFC 2675, August 1999.

[RFC-2732] R. Hinden, B. Carpenter, L. Masinter, "Format for Literal IPv6 Addresses in URL's", RFC 2732, December 1999.

[RFC-2851] M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC2851, June 2000.

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

[RFC-3019] B. Haberman, R. Worzella, "IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol", RFC3019, January 2001.

[IPv6-RH] P. Savola, "Security of IPv6 Routing Header and Home Address Options", Work in Progress, March 2002.

13. Authors and Acknowledgements

This document was written by the IPv6 Node Requirements design team:

Jari Arkko
[jari.arkko@ericsson.com]

Marc Blanchet
[marc.blanchet@viagenie.qc.ca]

Samita Chakrabarti
[samita.chakrabarti@eng.sun.com]

Alain Durand
[alain.durand@sun.com]

Gerard Gastaud
[gerard.gastaud@alcatel.fr]

Jun-ichiro itojun Hagino
[itojun@iijlab.net]

Atsushi Inoue
[inoue@isl.rdc.toshiba.co.jp]

Masahiro Ishiyama
[masahiro@isl.rdc.toshiba.co.jp]

John Loughney
[john.loughney@nokia.com]

Okabe Nobuo
[nov@tahi.org]

Rajiv Raghunarayan
[raraghun@cisco.com]

Shoichi Sakane
[shouichi.sakane@jp.yokogawa.com]

Dave Thaler
[dthaler@windows.microsoft.com]

Juha Wiljakka
[juha.wiljakka@Nokia.com]

The authors would like to thank Ran Atkinson, Jim Bound, Brian Carpenter, Ralph Droms, Christian Huitema, Adam Machalek, Thomas Narten, Juha Ollila and Pekka Savola for their comments.

14. Editor's Contact Information

Comments or questions regarding this document should be sent to the IPv6 Working Group mailing list (ipng@sunroof.eng.sun.com) or to:

John Loughney
Nokia Research Center
It merenkatu 11-13
00180 Helsinki
Finland

Phone: +358 50 483 6242
Email: John.Loughney@Nokia.com

Appendix A: Change history

The following is a list of changes since the previous version.

- Small updates based upon feedback from the IPv6 mailing list.
- Updated information on Stateful Address Autoconfiguration & DHCP.
- Updated MIBs section.
- Updated Mobile IP section.

- Rewrote Security section.

Appendix B: Specifications Not Included

Here is a list of documents considered, but not included in this document. In general, Information documents are not considered to place requirements on implementations. Experimental documents are just that, experimental, and cannot place requirements on the general behavior of IPv6 nodes.

Upper Protocols
- 2428 FTP Extensions For IPv6 And NATs

Compression
- 2507 IP Header Compression
- 2508 Compressing IP/UDP/RTP Headers For Low-Speed Serial Links
- 2509 IP Header Compression Over PPP

Informational
- 1752 The Recommendation For The IP Next Generation Protocol API RFCs
- 1881 IPv6 Address Allocation Management.
- 1887 An Architecture For Ipv6 Unicast Address Allocation
- 2104 HMAC: Keyed-Hashing For Message Authentication
- 2374 An IPv6 Aggregatable Global Unicast Address Format.
- 2450 Proposed TLA And NLA Assignment Rules.

Experimental
- 2874 DNS Extensions To Support Ipv6 Address Aggregation
- 2471 IPv6 Testing Address Allocation.

Other
- 2526 Reserved IPv6 Subnet Anycast
- 2732 Format For Literal IPv6 Addr In URLs
- 2894 Router Renumbering
- 3122 Extensions To IPv6 ND For Inverse Discovery

Appendix C: Notices

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary

rights, which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.