IPv6 Working Group John Loughney (ed)
Internet-Draft Nokia
October 25, 2003

Expires: April 24, 2004

IPv6 Node Requirements
draft-ietf-ipv6-node-requirements-06.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 common functionality required from both IPv6 hosts and routers. 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.

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. [RFC-793].

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

3. Sub-IP Layer

An IPv6 node must follow the RFC related to the link-layer that is sending packets. 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

Nodes supporting IPv6 over Ethernet interfaces MUST implement Transmission of IPv6 Packets over Ethernet Networks [RFC-2464].

3.2 IP version 6 over PPP - RFC2472

Nodes supporting IPv6 over PPP MUST implement IPv6 over PPP [RFC-2472].

3.3 IPv6 over ATM Networks - RFC2492

Nodes supporting IPv6 over ATM Networks MUST implement IPv6 over ATM

Networks [RFC-2492]. Additionally, RFC 2492 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 a limitation to the 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. [RFC-2460]

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, an 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. 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 on all links supporting link-layer multicast (RFC2462 section 5.4 specifies DAD MUST take place on all unicast addresses).

A host implementation MUST support sending Router Solicitations, but it MAY support a configuration option to disable this functionality.

Receiving and processing Router Advertisements MUST be supported for host implementations. However, an implementation MAY support the option of disabling this function. The ability to understand specific Router Advertisement options 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 functionality SHOULD be supported. If the node is a router, Redirect functionionality 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. It is expected that most implementations will indeed support this, although the possible exception cases are sufficient that the used of "SHOULD" is not justified. The rules in RFC 2460 MUST be followed for packet fragmentation and reassembly.

4.3.2 IPv6 Jumbograms - RFC2675

IPv6 Jumbograms [RFC-2675] 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 support for site-local addressing.

4.5.1 IP Version 6 Addressing Architecture - RFC3513

The IPv6 Addressing Architecture [RFC-3513] MUST be supported.

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 RFC 2460 [RFC-2460].

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 - RFC3484

The the rules specified in the Default Address Selection for IPv6 [RFC-3484] document MUST be implemented. It is expected that IPv6 nodes will need to deal with multiple addresses. 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.

4.5.5 Stateful Address Autoconfiguration

Stateful Address Autoconfiguration MAY be supported. DHCP [RFC-3315] is the standard stateful address configuration protocol, see section 5.3 for DHCPv6 support.

For nodes which do not support Stateful Address Autoconfiguration, the node may be unable to obtain any IPv6 addresses aside from link-local addresses when 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).

4.6 Multicast Listener Discovery (MLD) for IPv6 - RFC2710

If an application is going to join any-source multicast group addresses, it SHOULD implement MLDv1. When MLD is used, the rules in "Source Address Selection for the Multicast Listener Discovery (MLD) Protocol" [RFC-3590] MUST be followed.

If an application is going to support Source-Specific Multicast, it MUST support MLDv2 [MLDv2] and conform to the Source-Specific Multicast overview document [RFC3569]; refer to Source-Specific Multicast architecture document for details [SSMARCH].

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 names. Note that RFC 1886 is currently being updated [RFC-1886BIS].

All nodes, that need to resolve names, SHOULD implement stub-resolver [RFC-1034] functionality, in RFC 1034 section 5.3.1 with support for:

- AAAA type Resource Records [RFC-1886BIS];
- reverse addressing in ip6.arpa [RFC-3152];
- EDNS0 [RFC-2671] to allow for DNS packet sizes larger than 512 octets.

Those nodes are RECOMMENDED to support DNS security extentions [DNSSEC-INTRO], [DNSSEC-REC] and [DNSSEC-PROT].

Those nodes are NOT RECOMMENDED to support the experimental A6 and DNAME Resource Records [RFC-3363].

Format for Literal IPv6 Addresses in URL's" [RFC-2732] MUST be supported if applications on the node use URL's.

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) - RFC3315

5.3.1 Managed Address Configuration

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). 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.

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.

5.3.2 Other Stateful Configuration

DHCP provides the ability to provide other configuration information to the node. An IPv6 node that does not include an implementation of DHCP will be unable to obtain other configuration information such as the addresses of DNS servers when it is connected to a link over which the node receives a router advertisement in which the 'O' flag ("Other stateful configuration") is set.

For those IPv6 Nodes (acting as hosts) that implement DHCP, those nodes MUST use DHCP upon the receipt of a Router Advertisement with the 'O' flag set (see section 5.5.3 of RFC2462). In addition, in the absence of a router, hosts that implement DHCP MUST attempt to use DHCP. For IPv6 Nodes that do not implement DHCP, the 'O' flag of a

Router Advertisement can be ignored. Furthermore, in the absence of a router, these types of node are not required to initiate DHCP.

Stateless DHCPv6 [DHCPv6-SL], a subset of DHCPv6, can be used to obtain configuration information. A node that uses stateless DHCP must have obtained its IPv6 addresses through some other mechanism, typically stateless address autoconfiguration.

6. IPv4 Support and Transition

IPv6 nodes MAY support IPv4.

6.1 Transition Mechanisms

IPv6 nodes SHOULD use native addressing instead of transition-based addressing (according to the algorithms defined in RFC 3484).

6.1.1 Transition Mechanisms for IPv6 Hosts and Routers - RFC2893

If an IPv6 node implements dual stack and/or tunneling, then RFC2893 MUST be supported.

RFC 2893 is currently being updated.

7. Mobile IP

The 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 described in Section 8.5 of [MIPv6], including support of generic packet tunneling [RFC-2473] and secure home agent communications [MIPv6-HASEC].

Hosts SHOULD support route optimization requirements for correspondent nodes described in Section 8.2 of [MIPv6].

Routers SHOULD support the generic mobility-related requirements for all IPv6 routers described in Section 8.3 of [MIPv6]. Routers MAY support the home agent functionality described in Section 8.4 of [MIPv6], including support of [RFC-2473] and [MIPv6-HASEC].

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] SHOULD NOT be supported. Security issues related to the use of DES are discussed in [DESDIFF], [DESINT], [DESCRACK]. It is still listed as required by the existing IPsec RFCs, but as it is currently viewed as an inherently weak algorithm, and no longer fulfills its intended role.

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 [RFC-2451] 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, but is expected to become required in the future.

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 Security Associations (SAs) is required, automated keying MUST be supported. Note that the IPsec WG is working on the successor to IKE [IKE2]. Key management methods for multicast traffic are also being worked on by the MSEC WG.

9. Router-Specific Functionality

This section defines general host considerations for IPv6 nodes that act as routers. Currently, this section does not discuss routing-specific requirements.

9.1 General

9.1.1 IPv6 Router Alert Option - RFC2711

The IPv6 Router Alert Option [RFC-2711] is an optional IPv6 Hop-by-Hop Header that is used in conjunction with some protocols (e.g., RSVP [RFC-2205], or MLD [RFC-2710]). The Router Alert option will need to be implemented whenever protocols that mandate its usage are implemented. See Section 4.6.

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 Management Information Base Modules (MIBs)

The following two MIBs SHOULD be supported MIBs by nodes that support an SNMP agent.

10.1.1 IP Forwarding Table MIB

Support for this MIB [RFC-2096BIS] 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 [RFC-2011BIS] 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 describe the following:

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

12. References

12.1 Normative

[DHCPv6-SL] R. Droms, "A Guide to Implementing Stateless DHCPv6

Service", draft-ietf-dhc-dhcpv6-stateless-00.txt, Work in Progress.

[MIPv6] J. Arkko, D. Johnson and C. Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24.txt, Work in progress.

[MIPv6-HASEC] J. Arkko, V. Devarapalli and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", draft-ietf-mobileip-mipv6-ha-ipsec-06.txt, Work in Progress.

[MLDv2] Vida, R. et al., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", draft-vida-mld-v2-07.txt, 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-1886BIS] Thomson, S., et al., "DNS Extensions to support IP version 6", draft-ietf-dnsext-rfc1886bis-03.txt, Work In Progress.

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

[RFC-2096BIS] Haberman, B. and Wasserman, M., "IP Forwarding Table MIB", draft-ietf-ipv6-rfc2096-update-05.txt, Work in Progress.

[RFC-2011BIS] Routhier, S (ed), "Management Information Base for the Internet Protocol (IP)", draft-ietf-ipv6-rfc2011-update-03.txt, 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-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. Xxx add

[RFC-2671]

[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-3315] Bound, J. et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

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

[RFC-3484] Draves, R., "Default Address Selection for IPv6", RFC 3484, February 2003.

[RFC-3513] Hinden, R. and Deering, S. "IP Version 6 Addressing Architecture", RFC 3513, April 2003.

[RFC-3590] Haberman, B., "Source Address Selection for the Multicast Listener Discovery (MLD) Protocol", RFC 3590, September 2003.

12.2 Non-Normative

[ANYCAST]   Hagino, J and Ettikan K., "An Analysis of IPv6 Anycast", draft-ietf-ipngwg-ipv6-anycast-analysis-02.txt, 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.

[DNSSEC-INTRO] Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S., "DNS Security Introduction and Requirements" draft-ietf-dnsext-dnssec-intro-06.txt, Work in Progress.

[DNSSEC-REC]   Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S., "Resource Records for the DNS Security Extensions", draft-ietf-dnsext-dnssec-records-04.txt, Work in Progress.

[DNSSEC-PROT]   Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S., "Protocol Modifications for the DNS Security Extensions", draft-ietf-dnsext-dnssec-protocol-02.txt, Work in Progress.

[IKE2]   Kaufman, C. (ed), "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-10.txt, Work in Progress.

[IPv6-RH]   P. Savola, "Security of IPv6 Routing Header and Home Address Options", draft-savola-ipv6-rh-ha-security-03.txt, Work in Progress, March 2002.

[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.

[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-2205] Braden, B. (ed.), Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP)", RFC 2205, September 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", RFC 2492, 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-3569] S. Bhattacharyya, Ed., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

[SSM-ARCH] H. Holbrook, B. Cain, "Source-Specific Multicast for IP", draft-ietf-ssm-arch-03.txt, Work in Progress.

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]

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
Itamerenkatu 11-13
00180 Helsinki
Finland

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

Notices