Internet Engineering Task Force J. Loughney
Internet-Draft Nokia
Intended status: Informational T. Narten
Expires: January 14, 2010 IBM Corporation
July 13, 2009

IPv6 Node Requirements RFC 4294-bis
draft-ietf-6man-node-req-bis-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. Requirements 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 [RFC2119].

2. 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 this document summarizes requirements from other published Standards Track documents in one place.

This document tries to avoid discussion of protocol details, and references RFCs for this purpose. This document is informational in nature and does not update Standards Track RFCs.

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 Jon Postel's Robustness Principle:

Be conservative in what you do, be liberal in what you accept from others [RFC0793].

2.1. 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 to ensure interoperability.

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

2.2. Description of IPv6 Nodes

From the Internet Protocol, Version 6 (IPv6) Specification [RFC2460], 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.

3. 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

4. Sub-IP Layer

An IPv6 node must include support for one or more IPv6 link-layer specifications. Which link-layer specifications are included will depend upon what link-layers are supported by the hardware available on the system. It is possible for a conformant IPv6 node to support IPv6 on some of its interfaces and not on others.

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.

4.1. Transmission of IPv6 Packets over Ethernet Networks - RFC 2464

Nodes supporting IPv6 over Ethernet interfaces MUST implement Transmission of IPv6 Packets over Ethernet Networks [RFC2464].

4.2. IP version 6 over PPP - RFC 5072

Nodes supporting IPv6 over PPP MUST implement IPv6 over PPP [RFC5072].

4.3. IPv6 over ATM Networks - RFC 2492

Nodes supporting IPv6 over ATM Networks MUST implement IPv6 over ATM Networks [RFC2492]. 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.

5. IP Layer

5.1. Internet Protocol Version 6 - RFC 2460

The Internet Protocol Version 6 is specified in [RFC2460]. 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 send, receive, and process fragment headers. All conformant IPv6 implementations MUST be capable of sending and receiving IPv6 packets; the forwarding functionality MAY be supported.

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. An exception is Routing Header type 0 (RH0) which was deprecated by [RFC5095] due to security concerns, and which MUST be treated as an unrecognized

routing type.

5.2. Neighbor Discovery for IPv6 - RFC 4861

Neighbor Discovery SHOULD be supported. [RFC4861] 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.

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. 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 (RFC 4862, Section 5.4, specifies DAD MUST take place on all unicast addresses).

A host implementation MUST support sending Router Solicitations.

Receiving and processing Router Advertisements MUST be supported for host implementations. 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 functionality MUST be supported.

5.3. IPv6 Router Advertisement Flags Option - RFC 5175

Router Advertisements include an 8-bit field of single-bit Router Advertisement flags. The Router Advertisement Flags Option extends the number of available flag bits by 48 bits. At the time of this writing, 6 of the original 8 bit flags have been assigned, while 2 are available for future assignment. No flags have been defined that make use of the new option, and thus strictly speaking, there is no requirement to implement the option today. However, implementations that are able to pass unrecognized options to a higher level entity that may be able to understand them (e.g., a user-level process using a "raw socket" facility), MAY take steps to handle the option in anticipation of a future usage.

5.4. Path MTU Discovery and Packet Size

5.4.1. Path MTU Discovery - RFC 1981

From [RFC2460]:

> It is strongly recommended that IPv6 nodes implement Path MTU Discovery [RFC1981], in order to discover and take advantage of path MTUs greater than 1280 octets. However, 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.

The rules in RFC 2460 MUST be followed for packet fragmentation and reassembly.

5.5. IPv6 Jumbograms - RFC 2675

IPv6 Jumbograms [RFC2675] MAY be supported.

5.6. ICMP for the Internet Protocol Version 6 (IPv6) - RFC 4443

ICMPv6 [RFC4443] MUST be supported.

5.7. Addressing

5.7.1. IP Version 6 Addressing Architecture - RFC 4291

The IPv6 Addressing Architecture [RFC4291] MUST be supported.

5.7.2. IPv6 Stateless Address Autoconfiguration - RFC 4862

IPv6 Stateless Address Autoconfiguration is defined in [RFC4862]. This specification MUST be supported for nodes that are hosts. Static address can be supported as well.

Nodes that are routers MUST be able to generate link local addresses as described in RFC 4862 [RFC4862].

From 4862:

> 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.

5.7.3. Privacy Extensions for Address Configuration in IPv6 - RFC 4941

Privacy Extensions for Stateless Address Autoconfiguration [RFC4941] 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.

5.7.4. Default Address Selection for IPv6 - RFC 3484

The rules specified in the Default Address Selection for IPv6 [RFC3484] document MUST be implemented. It is expected that IPv6 nodes will need to deal with multiple addresses.

5.7.5. Stateful Address Autoconfiguration

Stateful Address Autoconfiguration MAY be supported. DHCPv6 [RFC3315] is the standard stateful address configuration protocol; see Section 6.2 for DHCPv6 support.

Nodes which do not support Stateful Address Autoconfiguration 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 that contains no prefixes advertised

for Stateless Address Autoconfiguration (see Section 4.5.2). Additionally, such nodes 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.

5.8. Multicast Listener Discovery (MLD) for IPv6 - RFC 2710

Nodes that need to join multicast groups MUST support MLDv1 [RFC3590]. MLDv1 is needed by any node that is expected to receive and process multicast traffic. Note that Neighbor Discovery (as used on most link types -- see Section 5.2) depends on multicast and requires that nodes join Solicited Node multicast addresses.

Nodes that need to join multicast groups SHOULD implement MLDv2 [RFC3810]. However, if the node has applications that only need support for Any-Source Multicast [RFC3569], the node MAY implement MLDv1 [RFC2710] instead. If the node has applications that need support for Source-Specific Multicast [RFC3569], [RFC4607], the node MUST support MLDv2 [RFC3810]. In all cases, nodes are strongly encouraged to implement MLDv2 rather than MLDv1, as the presence of a single MLDv1 participant on a link requires that all other nodes on the link operate in version 1 compatability mode.

When MLDv1 is used, the rules in the Source Address Selection for the Multicast Listener Discovery (MLD) Protocol [RFC3590] MUST be followed.

6. DNS and DHCP

6.1. DNS

DNS is described in [RFC1034], [RFC1035], [RFC3363], and [RFC3596]. Not all nodes will need to resolve names; those that will never need to resolve DNS names do not need to implement resolver functionality. However, the ability to resolve names is a basic infrastructure capability that applications rely on and generally needs to be supported. All nodes that need to resolve names SHOULD implement stub-resolver [RFC1034] functionality, as in RFC 1034, Section 5.3.1, with support for:

- AAAA type Resource Records [RFC3596];

- reverse addressing in ip6.arpa using PTR records [RFC3596];
- EDNS0 [RFC2671] to allow for DNS packet sizes larger than 512 octets.

Those nodes are RECOMMENDED to support DNS security extensions [RFC4033], [RFC4034], and [RFC4035].

Those nodes are NOT RECOMMENDED to support the experimental A6 Resource Records [RFC3363].

6.2. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) - RFC 3315

6.2.1. **5.2.1.** Managed Address Configuration

The method by which IPv6 nodes that use DHCP for address assignment can obtain IPv6 addresses and other configuration information upon receipt of a Router Advertisement with the \'M' flag set is described in Section 5.5.3 of RFC 4862.

In addition, in the absence of a router, those IPv6 nodes that use DHCP for address assignment MAY initiate DHCP to obtain IPv6 addresses and other configuration information, as described in Section 5.5.2 of RFC 4862. Those IPv6 nodes that do not use DHCP for address assignment can ignore the 'M' flag in Router Advertisements.

6.2.2. Other Configuration Information

The method by which IPv6 nodes that use DHCP to obtain other configuration information can obtain other configuration information upon receipt of a Router Advertisement with the \'O' flag set is described in Section 5.5.3 of RFC 4862.

Those IPv6 nodes that use DHCP to obtain other configuration information initiate DHCP for other configuration information upon receipt of a Router Advertisement with the 'O' flag set, as described in Section 5.5.3 of RFC 4862. Those IPv6 nodes that do not use DHCP for other configuration information can ignore the 'O' flag in Router Advertisements.

An IPv6 node can use the subset of DHCP (described in [RFC3736]) to obtain other configuration information.

6.2.3. Use of Router Advertisements in Managed Environments

Nodes using the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) are expected to determine their default router information and on-link prefix information from received Router Advertisements.

7. IPv4 Support and Transition

IPv6 nodes MAY support IPv4.

7.1. Transition Mechanisms

7.1.1. Basic Transition Mechanisms for IPv6 Hosts and Routers - RFC 4213

If an IPv6 node implements dual stack and tunneling, then [RFC4213] MUST be supported.

8. Mobile IP

The Mobile IPv6 [RFC3775] 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 [RFC3775], including support of generic packet tunneling [RFC2473] and secure home agent communications [RFC4877].

Hosts SHOULD support route optimization requirements for correspondent nodes described in Section 8.2 of [RFC3775].

Routers SHOULD support the generic mobility-related requirements for all IPv6 routers described in Section 8.3 of [RFC3775]. Routers MAY support the home agent functionality described in Section 8.4 of [RFC3775], including support of [RFC2473] and [RFC4877].

9. Security

This section describes the specification of IPsec for the IPv6 node.

9.1. Basic Architecture

Security Architecture for the Internet Protocol [RFC4301] MUST be supported.

9.2. Security Protocols

ESP [RFC4303] MUST be supported. AH [RFC4302] MAY be supported.

9.3. Transforms and Algorithms

Current IPsec RFCs specify the support of transforms and algorithms for use with AH and ESP: NULL encryption, DES-CBC, HMAC-SHA-1-96, and HMAC-MD5-96. However, 'Cryptographic Algorithm Implementation Requirements For ESP and AH' [RFC4835] contains the current set of mandatory to implement algorithms for ESP and AH. It also specifies algorithms that should be implemented because they are likely to be promoted to mandatory at some future time. IPv6 nodes SHOULD conform to the requirements in [RFC4835], as well as the requirements specified below.

Since ESP encryption and authentication are both optional, support for the NULL encryption algorithm [RFC2410] and the NULL authentication algorithm [RFC4303] MUST be provided to maintain consistency with the way these services are negotiated. However, while authentication and encryption can each be NULL, they MUST NOT both be NULL. The NULL encryption algorithm is also useful for debugging.

The DES-CBC encryption algorithm [RFC2405] SHOULD NOT be supported within ESP. Security issues related to the use of DES are discussed in 'DESDIFF', 'DESINT', and 'DESCRACK'. DES-CBC is still listed as required by the existing IPsec RFCs, but updates to these RFCs will be published in the near future. DES provides 56 bits of protection, which is no longer considered sufficient.

The use of the HMAC-SHA-1-96 algorithm [RFC2404] within AH and ESP MUST be supported. The use of the HMAC-MD5-96 algorithm [RFC2403] within AH and ESP MAY also be supported.

The 3DES-CBC encryption algorithm [RFC2451] does not suffer from the same security issues as DES-CBC, and the 3DES-CBC algorithm within ESP MUST be supported to ensure interoperability.

The AES-128-CBC algorithm [RFC3602] MUST also be supported within ESP. AES-128 is expected to be a widely available, secure, and efficient algorithm. While AES-128-CBC is not required by the current IPsec RFCs, it is expected to become required in the future.

9.4. Key Management Methods

An implementation MUST support the manual configuration of the security key and SPI. The SPI configuration is needed in order to

delineate between multiple keys.

Key management SHOULD be supported. Examples of key management systems include IKEv2 [RFC4306] and Kerberos; S/MIME and TLS include key management functions.

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.

Key management methods for multicast traffic are also being worked on by the MSEC WG.

10. 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.

10.1. General

10.1.1. IPv6 Router Alert Option - RFC 2711

The IPv6 Router Alert Option [RFC2711] is an optional IPv6 Hop-by-Hop Header that is used in conjunction with some protocols (e.g., RSVP [RFC2205] or MLD [RFC2710]). The Router Alert option will need to be implemented whenever protocols that mandate its usage are implemented. See Section 4.6.

10.1.2. Neighbor Discovery for IPv6 - RFC 4861

Sending Router Advertisements and processing Router Solicitation MUST be supported.

11. Network Management

Network Management MAY be supported by IPv6 nodes. However, for IPv6 nodes that are embedded devices, network management may be the only possible way of controlling these nodes.

11.1. Management Information Base Modules (MIBs)

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

11.1.1. IP Forwarding Table MIB

IP Forwarding Table MIB [RFC4292] SHOULD be supported by nodes that support an SNMP agent.

11.1.2. Management Information Base for the Internet Protocol (IP)

IP MIB [RFC4293] SHOULD be supported by nodes that support an SNMP agent.

12. Open Issues

1. General: should this document be more of an applicability statement providing context for when a technology may be useful, but without just saying SHOULD or MUST?
2. Need to address contradiction that this document is Informational, yet tries to make recommendations that go beyond what is stated in current RFCs in some cases. (see previous point)
3. Should we try and tackle the confusion related to the M&O bits in Router Advertisements? (probably not in this document -- see previous point.)
4. Need to provide more context for MIPv6 recommendations. Blanket SHOULD for RO in nodes does not reflect current state of MIPv6 deployment.
5. Security Considerations Section needs updating.
6. For things like link-layer types, may be better to just list all the IPv6-over-Foo documents as a summary table, making no recommendations at all.
7. Privacy Extensions recommendation needs more context. It makes no sense for a server to implement this. It is only applicable to mobile devices.
8. Security Recommendations may need updating. Are they still correct? And what is value of mandating IPsec if there is no key management? Also, what is the sense of mandating IPsec for limited-functionality devices that have a limited number of applications, each using their own security? Relax current requirement or leave as is?

13. Security Considerations

This document 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' [RFC2411] is important for everyone to read.

The security considerations in RFC 2460 state the following:

The security features of IPv6 are described in the Security Architecture for the Internet Protocol [RFC2401].

RFC 2401 has been obsoleted by RFC 4301, therefore refer RFC 4301 for the security features of IPv6.

14. Authors and Acknowledgments

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. Thanks to Mark Andrews for comments and corrections on DNS text. Thanks to Alfred Hoenes for tracking the updates to various RFCs.

15. Appendix: Changes from RFC 4294

This appendix keeps track of the chances from RFC 4294

1. Section 5.1, removed "and DNAME" from the discussion about RFC-3363.

2. RFC 2463 references updated to RFC 4443.

3. RFC 3513 references updated to RFC 4291.

4. RFC 3152 references updated to RFC 3596.

5. RFC 2893 references updated to RFC 4213.

6. AH [RFC-4302] support chanced from MUST to MAY.

7. The reference for RFC 3152 has been deleted, as the RFC has been obsoleted, and has been incorporated into RFC 3596.

8. The reference for RFC 3879 has been removed as the material from RFC 3879 has been incorporated into RFC 4291.

16. References

16.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[RFC2411] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, October 1999.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3363] Bush, R., Durand, A., Fink, B., Gudmundsson, O., and T. Hain, "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", RFC 3363, August 2002.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3590] Haberman, B., "Source Address Selection for the Multicast Listener Discovery (MLD) Protocol", RFC 3590, September 2003.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4292] Haberman, B., "IP Forwarding Table MIB", RFC 4292, April 2006.

[RFC4293] Routhier, S., "Management Information Base for the Internet Protocol (IP)", RFC 4293, April 2006.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in

IPv6", RFC 4941, September 2007.

[RFC5072] S.Varada, Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.

16.2. Informative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

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

[RFC2675] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, August 1999.

[RFC3569] Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

Authors' Addresses

John Loughney
Nokia
955 Page Mill Road
Palo Alto 94303
USA

Phone: +1 650 283 8068
Email: john.loughney@nokia.com

Thomas Narten
IBM Corporation
3039 Cornwallis Ave.
PO Box 12195
Research Triangle Park, NC 27709-2195
USA

Phone: +1 919 254 7798
Email: narten@us.ibm.com