IPv6 Node Requirements
draft-ietf-ipv6-node-requirements-01.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 a minimal 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 requirements listed in this document.

   The document is written to minimize protocol discussion in this
   document but instead make pointers to RFCs. 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, if any issue is raised
   regarding the normative RFCs, the consensus is, whenever possible, to
   fix the RFCs 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](#) 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 & Conformance Groups

   This document defines three classes of conformance for an IPv6 node:
   Unconditionally Mandatory, Conditionally Mandatory and
   Unconditionally Optional. The three classes of conformance are
   defined in [section 1.2](#).

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.

Usage of IPv6 nodes

   TBD

Conformance Group

   A conformance group is a collection of related behavioral
   specifications that appear in standards. A single RFC may contain
   multiple independent pieces of functionality that belong to
   separate conformance groups. If a node claims compliance to a
   given conformance group, that means it implements all of the
   mandatory behavior therein, including implementing all MUSTs, and
   none of the MUST NOTs.

Unconditionally Mandatory

   If a node claims compliance to this document, then it must support
   the behavior specified within each conformance group listed of
   type unconditionally mandatory.

Conditionally Mandatory

   Conditionally mandatory groups include those which are mandatory
   only if a particular condition is true, such as whether a specific
   type of hardware is present, or whether another given group is
   implemented. When a conditionally mandatory specification or
   group is described, the condition will also be described. A given
   RFC or portion thereof can sometimes appear in multiple
   conformance groups, with different conditions.

Unconditionally Optional

Behavior that is neither unconditionally mandatory nor
conditionally mandatory is unconditionally optional for compliance
to this document.

[2](#). Abbreviations Used in This Document

AH   Authentication Header

DAD   Duplicate Address Detection

ESP   Encapsulating Security Payload

ICMP   Internet Control Message Protocol

MIB   Management Information Base

MTU   Maximum Transfer Unit

NA   Neighbor Advertisement

ND   Neighbor Discovery

NS   Neighbor Solicitation

NUD   Neighbor Unreachability Detection

[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
conditionally mandatory, based upon what layer-2 is used. In
general, it is reasonable to be a conformant IPv6 node and NOT
support some legacy interfaces.

[3.1](#) A.K.A - IPv6 over Foo

[3.1.1](#) [RFC2464](#) - Transmission of IPv6 Packets over Ethernet Networks

Transmission of IPv6 Packets over Ethernet Networks [[RFC-2464](#)] is
conditionally mandatory if the node supports Ethernet interfaces.

[3.1.2](#) [RFC2467](#) - A Method for the Transmission of IPv6 Packets over FDDI Networks

A Method for the Transmission of IPv6 Packets over FDDI Networks
[[RFC-2467](#)] is conditionally mandatory if the node supports FDDI
interfaces.

3.1.3 RFC2470 - A Method for the Transmission of IPv6 Packets over Token Ring Networks

A Method for the Transmission of IPv6 Packets over Token Ring Networks [RFC-2470] is conditionally mandatory if the node supports token ring interfaces.

3.1.4 RFC2472 - IP version 6 over PPP

IPv6 over PPP [RFC-2472] is conditionally mandatory if the node supports PPP.

3.1.5 RFC2491 - IPv6 over Non-Broadcast Multiple Access (NBMA) Networks

IPv6 over Non-Broadcast Multiple Access (NBMA) Networks [RFC2491] is conditionally mandatory if the node supports NBMA network interfaces.

3.1.6 RFC2492 - IPv6 over ATM Networks

IPv6 over ATM Networks [RFC2492] is conditionally mandatory if the node supports 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.

3.1.7 RFC2497 - A Method for the Transmission of IPv6 Packets over ARCnet Networks

A Method for the Transmission of IPv6 Packets over ARCnet Networks [RFC2497] is conditionally mandatory if the node supports ARCnet network interfaces.

3.1.8 RFC2529 - Transmission of IPv6 Packets over IPv4 Domains without Explicit Tunnels

Transmission of IPv6 Packets over IPv4 Domains without Explicit Tunnels [2529] is unconditionally optional.

3.1.9 RFC2590 - Transmission of IPv6 Packets over Frame Relay Networks Specification

Transmission of IPv6 Packets over Frame Relay Networks Specification [RFC2590] is conditionally mandatory if the node supports Frame Relay interfaces.

4. IP Layer

4.1 General

4.1.1 RFC2460 - Internet Protocol Version 6

   The Internet Protocol Version 6 is specified in [RFC-2460]. This
   specification is unconditionally mandatory.

   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 is unconditionally
   mandatory, whereas the capability of being an intermediate
   destination is unconditionally optional (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]

   It is unconditionally mandatory for an IPv6 node 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

4.2.1 RFC2461 - Neighbor Discovery for IPv6

   Neighbor Discovery is conditionally mandatory. 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 is unconditionally mandatory for
implementations. However, the implementation MAY support disabling
this feature.

Prefix Discovery is how hosts discover the set of address prefixes
that define which destinations are on-link for an attached link.
Prefix discovery is unconditionally mandatory for implementation with
option to disable this function.

Address resolution is how nodes determine the link-layer address of
an on-link destination (e.g., a neighbor) given only the
destination's IP address. It is conditionally mandatory
implementation depending on the link type support. Address Resolution
for point-to-point links may not be mandatory; working group
clarification is needed on this.

Neighbor Unreachability Detection (NUD) is conditionally mandatory.
It is unconditionally mandatory for all paths between hosts and
neighboring nodes. It is unconditionally optional for paths between
routers. It is unconditionally optional 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 is unconditionally mandatory (RFC2462
section 5.4 specifies DAD MUST take place on all unicast addresses).

Sending Router Solicitation is unconditionally mandatory for host
implementation, with a configuration option to disable this
functionality.

Receiving and processing Router Advertisements is unconditionally
mandatory for host implementation, with a configuration option to
disable this functionality. 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) are unconditionally mandatory. NS and NA messages
are required for Duplicate Address Detection (DAD).

Redirect Function is conditionally mandatory. If the node is a
router, Redirect Function is unconditionally mandatory.

4.3 Path MTU Discovery & Packet Size

4.3.1 RFC1981 - Path MTU Discovery

Path MTU Discovery [RFC-1981] is unconditionally optional. The IPv6
specification [RFC-2460] states in section 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]).

4.3.2 RFC2675 - IPv6 Jumbograms

IPv6 Jumbograms [RFC2675] is unconditionally optional.

4.4 ICMPv6

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

ICMPv6 [RFC-2463] is unconditionally mandatory.

4.5 Addressing

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

4.5.1 RFC2373 - IP Version 6 Addressing Architecture

The IPv6 Addressing Architecture [RFC-2373] is a mandatory part of
IPv6. Currently, this specification is being updated by [ADDRARCHv3].

4.5.2 RFC2462 - IPv6 Stateless Address Autoconfiguration

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

It is unconditionally mandatory for nodes that are routers 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) is unconditionally mandatory for
all interface addresses assigned to the node.

4.5.3 RFC3041 - Privacy Extensions for Address Configuration in IPv6

Privacy Extensions for Stateless Address Autoconfiguration [RFC-3041]
is unconditionally optional. Currently, there is discussion of the
applicability of temporary addresses.

4.5.4 Default Address Selection for IPv6

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

The rules specified in the document are the only MUST to implement
portion of the architecture. There is no requirement that a node be
able to be part of more than one zone.

4.5.5 Stateful Address Autoconfiguration

IPv6 Stateless Address Autoconfiguration [RFC2462] defines stateless
address autoconfiguation. However, it does state that in the absence
of routers, hosts MUST attempt to use stateful autoconfiguration.
There is also reference to stateful address autoconfiguration being
defined elsewhere. Additionally, DHCP [DHCP] states that it is on
option for stateful address autoconfiguation.

From the current set of specification, it is not clear the level of
support that is needed for statefull Address Autoconfiguration.

4.6 Other

4.6.1 RFC2473 - Generic Packet Tunneling in IPv6 Specification

Generic Packet Tunneling [RFC-2473] conditionally mandatory, with the
condition being implementing the mobile node functionality or Home
Agent functionality of Mobile IP [MIPv6].

4.6.2 RFC2710 - Multicast Listener Discovery (MLD) for IPv6

Multicast Listener Discovery [RFC-2710] is Conditionally Mandatory,
where the condition is if the node joins any multicast groups other
than the all-nodes-on-link group (which will always be the case if it
runs ND or DAD on the link).

There has been some discussion that hosts may not be able to depend
on MLD if there is no connection to a router, therefore this may not
be Mandatory. Further discussion is needed on this.

5. Transport Layer and DNS

5.1 Transport Layer

5.1.1 RFC2147 - TCP and UDP over IPv6 Jumbograms

This specification is conditionally mandatory, 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

Support for DNS, as described in [RFC-1034], [RFC-1035] and [RFC-
1886], is unconditionally optional. Not all nodes will need to
resolve addresses.

**5.2.1 RFC2874 - DNS Extensions to Support IPv6 Address Aggregation and
       Renumbering**

DNS Extensions to Support IPv6 Address Aggregation and Renumbering is
unconditionally optional

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

RFC 2732 is conditionally mandatory if the node uses URL's.

5.3 Other

5.3.1 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

The Dynamic Host Configuration Protocol for IPv6 [DHCPv6] is
unconditionally optional.

6. Transition

6.1 Transition Mechanisms

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

6.1.1 RFC2893 - Transition Mechanisms for IPv6 Hosts and Routers

   If an IPv6 node implement dual stack and/or tunneling, then RFC2893
   is unconditionally mandatory.

   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.

   The Mobile IP specification [MIPv6] specifies the following classes
   of functionality: Correspondent Node, Mobile Node, Route Optimization
   functionality and Home Agent Functionality.

   Correspondent Node functionality is Unconditionally Mandatory.

   Mobile Node functionality is Conditionally Mandatory for nodes that
   need to maintain sessions while changing their point of attachment to
   the Internet.

   Route Optimization functionality is conditionally mandatory for
   hosts. Route Optimization is unconditionally optional for routers.
   There is ongoing discussion about the role of Route Optimization.
   This document should list some of the benefits of Route Optimization.

   Home Agent functionality is Unconditionally Optional.

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] is
   unconditionally mandatory except of the following description.

Requirements that this section describes explicitly MUST refer to
RFC-2401.

IPsec transport mode is unconditionally mandatory.

IPsec tunnel mode is unconditionally mandatory.

[DISCUSSION: Network administrators want to make separated
networks to be a single network by using a site-local address
space. The routers should be implemented both IPsec transport
mode and a generic tunnel in this case, but if there is no
statement what it should be, the administrators must use IPsec
tunnel mode because it is used now in IPv4 network.]

Applying single security association of ESP [RFC-2406] to a packet is
unconditionally mandatory, although RFC-2401 defines four types of
combination of security associations that must be supported by
compliant IPsec hosts.

Applying single security association of AH is conditionally mandatory
if AH [RFC-2402] is implemented.

The following packet type is conditionally mandatory if AH is
combined with ESP: IP|AH|ESP|ULP.

The summary of Basic Combinations of Security Associations in section
4.5 of RFC-2401 is:

case 1-2 is unconditionally mandatory.
case 1-1 and 1-3 is conditionally mandatory if AH is implemented.
case 1-4, 1-5, 2-5 and 4 is conditionally optional if IPsec tunnel
      mode is implemented.
case 2-4 is conditionally optional if IPsec tunnel mode and AH is
      implemented.
case 3 is not applicable to this document.

8.2 Security Protocols

ESP [RFC-2406] is unconditionally mandatory even when ESP is not
used. AH [RFC-2402] is unconditionally mandatory also.

AH is need if there is data in IP header to be protected, for
example, an extension header.

In practice, ESP can provide the same security services as AH and as
well as confidentiality, thus there is no real need for AH.

8.3 Transforms and Algorithms

The ESP DES-CBC Cipher Algorithm With Explicit IV [RFC-2405] is
conditionally mandatory if you need to have interoperability with old
implementation by using DES-CBC. Note the IPsec WG recommends not
using this algorithm. 3DES-CBC is conditionally mandatory so that the
part of ESP CBC-Mode Cipher Algorithms [RFC-2451] is unconditionally
mandatory. Note that the IPsec WG also recommends not using this
algorithm. AES-128-CBC [ipsec-ciph-aes-cbc] is unconditionally
mandatory but there is on-going work in the IPsec WG. NULL Encryption
algorithm [RFC-2410] is conditionally mandatory. It is only for
providing integrity service, and also for debugging use.

The use of HMAC-SHA-1-96 within ESP, described in [RFC-2404], is
unconditionally mandatory. This MUST be used if AH is implemented.
The Use of HMAC-MD5-96 within ESP, described in [RFC-2403], is
unconditionally mandatory. This MUST be used if AH is implemented.
The "HMAC-SHA-256-96 Algorithm and Its Use With IPsec" [ipsec-ciph-
sha-256] is unconditionally mandatory, but it is being discussed in
the IPsec WG. An implementer MUST refer to Keyed-Hashing for Message
Authentication [RFC-2104].

8.4 Key Management Method

Manual keying is unconditionally mandatory.

Automated SA and Key Management is conditionally mandatory for the
use of the anti-replay features of AH and ESP, and to accommodate
on-demand creation of SAs, session-oriented keying.

IKE [RFC-2407, RFC-2408, RFC-2409] is unconditionally optional for
unicast traffic. Note that the IPsec WG is working on the successor
to IKE [SOI].

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 RFC2711 - IPv6 Router Alert Option

The Router Alert Option [RFC-2711] is conditionally mandatory if the
node performs packet forwarding at the IP layer (i.e. - the node is a
router).

9.1.2 RFC2461 - Neighbor Discovery for IPv6

   Sending Router Advertisements and processing Router Solicitation is
   unconditionally mandatory.

10. Network Management

   Network Management, is generally not a requirement for 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 can be considered conditionally mandatory
   when the node supports an SNMP agent. This section is for further
   study. It should be also noted that these specifications are being
   updated updated.

**10.1.1 RFC2452 - IPv6 Management Information Base for the Transmission
        Control Protocol**

   TBA

**10.1.2 RFC2454 - IPv6 Management Information Base for the User Datagram
        Protocol**

   TBA

**10.1.3 RFC2465 - Management Information Base for IP Version 6: Textual
        Conventions and General Group**

   TBA

**10.1.4 RFC2466 - Management Information Base for IP Version 6: ICMPv6
        Group**

   TBA

10.1.5 RFC2851 - Textual Conventions for Internet Network Addresses

   TBA

**10.1.6 RFC3019 - IP Version 6 Management Information Base for the
        Multicast Listener Discovery Protocol**

TBA

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 RFC2401 describes,

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

IPsec cannot cover all of security requirement for IPv6 node. For
example, IPsec cannot protect the node from kind of DoS attack. The
node may need a mechanism of IPv6 packet filtering functionality, and
also may need a mechanism of rate limitation.

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 chick en-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.

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.

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

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

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

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

12.2 Non-Normative

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

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

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

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

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

    [RFC-2452]   M. Daniele, "IPv6 Management Information Base for the
                    Transmission Control Protocol", RFC2452, December
                    1998.

    [RFC-2454]   M. Daniele, "IPv6 Management Information Base for the
                    User Datagram Protocol, RFC2454", December 1998.

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

    [RFC-2465]   D. Haskin, S. Onishi, "Management Information Base for
                    IP Version 6: Textual Conventions and General Group",
                    RFC2465, December 1998.

    [RFC-2466]   D. Haskin, S. Onishi, "Management Information Base for

                    IP Version 6: ICMPv6 Group", RFC2466, December 1998.

    [RFC-2467]   M. Crawford, "A Method for the Tranmission of IPv6
                    Packets over FDDI Networks", RFC2467, December 1998.

    [RFC-2470]   M. Crawford, T. Narten, S. Thomas, "A Method for the
                    Tranmission of IPv6 Packets over Token Ring Networks",
                    RFC2470, December 1998.

    [RFC-2491]   G. Armitage, P. Schulter, M. Jork, G. Harter, "IPv6
                    over Non-Broadcast Multiple Access (NBMA) networks",
                    RFC2491, January 1999.

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

    [RFC-2497]   I. Souvatzis, "A Method for the Transmission of IPv6
                    Packets over ARCnet Networks", RFC2497, January 1999.

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

    [RFC-2590]   A. Conta, A. Malis, M. Mueller, "Transmission of IPv6
                    Packets over Frame Relay Networks Specification", RFC
                    2590, May 1999.

    [RFC-2675]   Borman, D., Deering, S. and Hinden, B., "IPv6 Jumbo-
                    grams", 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 Net-
                    work Addresses", RFC2851, June 2000.

   [RFC-2874]   Crawford, M. and Huitema, C., "DNS Extensions to Sup-
                   port IPv6 Address Aggregation and Renumbering", RFC
                   2874, July 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.

   [RFC-3041]   Narten, T. and Draves, R., "Privacy Extensions for
                   Stateless Address Autoconfiguration in IPv6", RFC
                   3041, 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 Adam Machalek, 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.
         - Refomated chapters.
         - Added Appendix B - List of RFCs.

      TBD

Appendix B: List of RFCs

   This is a list of RFC to look at during the editing process. They are
classified by generic categories and by level of potential conformance. The *
denotes some sections of the specification have lesser level of conformance
required.

       RFC   Section   Conformance
       ==
       RFC-1034   5.2.1   unconditionally optional
       RFC-1035   5.2.1   unconditionally optional
       RFC-1886   5.2.1   unconditionally optional
       RFC-1981   4.3.1   unconditionally optional
       RFC-2104   8.3   conditionally mandatory
       RFC-2147   5.1.1   conditionally mandatory
       RFC-2373   4.5.1   unconditionally mandatory
       RFC-2401   8.1   unconditionally mandatory *
       RFC-2402   8.1   conditionally mandatory
       RFC-2403   8.3   unconditionally mandatory
       RFC-2404   8.3   unconditionally mandatory
       RFC-2405   8.3   conditionally mandatory
       RFC-2406   8.1   unconditionally mandatory
       RFC-2407   8.4   unconditionally mandatory
       RFC-2408   8.4   unconditionally mandatory
       RFC-2409   8.4   unconditionally mandatory
       RFC-2410   8.3   unconditionally mandatory
       RFC-2451   8.3   unconditionally mandatory
       RFC-2452   10.1.1   conditionally mandatory
       RFC-2454   10.1.2   conditionally mandatory
       RFC-2460   4.1.1   unconditionally mandatory *
       RFC-2461   4.2.1   unconditionally mandatory *
       RFC-2462   4.5.2   unconditionally mandatory *
       RFC-2463   4.5.1   unconditionally mandatory
       RFC-2464   3.1.1   conditionally mandatory
       RFC-2465   10.1.3   conditionally mandatory
       RFC-2466   10.1.4   conditionally mandatory
       RFC-2467   3.1.2   conditionally mandatory
       RFC-2470   3.1.3   conditionally mandatory
       RFC-2472   3.1.4   conditionally mandatory
       RFC-2473   4.6.1   conditionally mandatory
       RFC-2491   3.1.5   conditionally mandatory
       RFC-2492   3.1.6   conditionally mandatory
       RFC-2497   3.1.7   conditionally mandatory
       RFC-2529   3.1.8   unconditionally optional
       RFC-2590   3.1.9   conditionally mandatory
       RFC-2675   4.3.2   unconditionally optional
       RFC-2710   4.6.2   conditionally mandatory
       RFC-2711   9.1.1   conditionally mandatory
       RFC-2732   5.2.2   conditionally mandatory
       RFC-2851   10.1.5   conditionally mandatory

RFC-2874	5.3.1	unconditionally optional
RFC-2893	6.1.1	conditionally mandatory
RFC-3019	10.1.6	conditionally mandatory

   RFC-3041   4.5.3   unconditionally optional

Appendix C: 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