

Expires: April 31, 2003

IPv6 Node Requirements  
draft-ietf-ipv6-node-requirements-02.txt

### Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 31, 2003

### Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

### 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.

---

Internet-Draft

October 31, 2002

## Table of Contents

1. Introduction
    - 1.1 Scope of this Document
    - 1.2 Description of IPv6 Nodes
  2. Abbreviations Used in This Document
  3. Sub-IP Layer
    - 3.1 [RFC2464](#) - Transmission of IPv6 Packets over Ethernet Networks
    - 3.2 [RFC2472](#) - IP version 6 over PPP
    - 3.3 [RFC2492](#) - IPv6 over ATM Networks
  4. IP Layer
    - 4.1 General
    - 4.2 Neighbor Discovery
    - 4.3 Path MTU Discovery & Packet Size
    - 4.4 [RFC2463](#) - ICMP for the Internet Protocol Version 6 (IPv6)
    - 4.5 Addressing
    - 4.6 Other
  5. Transport and DNS
    - 5.1 Transport Layer
    - 5.2 DNS
    - 5.3 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
  6. IPv4 Support and Transition
    - 6.1 Transition Mechanisms
  7. Mobility
  8. Security
    - 8.1 Basic Architecture
    - 8.2 Security Protocols
    - 8.3 Transforms and Algorithms
    - 8.4 Key Management Method
  9. Router Functionality
    - 9.1 General
  10. Network Management
    - 10.1 MIBs
  11. Security Considerations
  12. References
    - 12.1 Normative
    - 12.2 Non-Normative
  13. Authors and Acknowledgements
  14. Editor's Address
- [Appendix A](#): Change history  
[Appendix B](#): List of Specifications Included  
[Appendix C](#): Specifications Not Included

---

Internet-Draft

October 31, 2002

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

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

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

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

### 1.1 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

Loughney (editor)

[Page 3]

---

Internet-Draft

October 31, 2002

- 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
MIB	Management Information Base
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  
ULP Upper Layer Protocol

### [3.](#) Sub-IP Layer

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

Loughney (editor)

[Page 4]

---

Internet-Draft

October 31, 2002

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

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

#### [3.2 RFC2472](#) - IP version 6 over PPP

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

#### [3.3 RFC2492](#) - IPv6 over ATM Networks

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

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

## [4. IP Layer](#)

### [4.1 General](#)

#### [4.1.1 RFC2460](#) - Internet Protocol Version 6

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

Unrecognized options in Hop-by-Hop Options or Destination Options extensions MUST be processed as described in [RFC 2460](#).

The node MUST follow the packet transmission rules in [RFC 2460](#).

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

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

[RFC 2460](#) specifies extension headers and the processing for these headers.

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

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

### [4.2 Neighbor Discovery](#)

#### [4.2.1 RFC2461](#) - Neighbor Discovery for IPv6

Neighbor Discovery is 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 is 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 is MUST be supported for implementations. However, the implementation MAY support the option of disabling this function.

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

Duplicate Address Detection is MUST be supported ([RFC2462 section 5.4](#)

specifies DAD MUST take place on all unicast addresses).

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

Receiving and processing Router Advertisements MUST be supported for host implementation s. However, the implementation MAY support the

option of disabling this function. The ability to understand specific Router Advertisements is dependent on supporting the specification where the RA is specified.

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

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

### [4.3](#) Path MTU Discovery & Packet Size

#### [4.3.1](#) [RFC1981](#) - Path MTU Discovery

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

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

If Path MTU Discovery is not implemented then the sending packet size is limited to 1280 octets (standard limit in [[RFC-2460](#)]). However, if this is done, the host MUST be able to receive packets with size up to the link MTU before reassembly. This is because the node at the other side of the link has no way of knowing less than the MTU is accepted.

#### [4.3.2](#) [RFC2675](#) - IPv6 Jumbograms

IPv6 Jumbograms [[RFC2675](#)] MAY be supported.

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

ICMPv6 [[RFC-2463](#)] MUST be supported.



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](#)] MUST be supported. 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 MUST be supported for nodes that are hosts.

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

From 2462:

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

Duplicate Address Detection (DAD) MUST be supported.

#### [4.5.3 RFC3041](#) - Privacy Extensions for Address Configuration in IPv6

Privacy Extensions for Stateless Address Autoconfiguration [[RFC-3041](#)] MAY be supported. Currently, there is discussion of the applicability of temporary addresses.

#### [4.5.4](#) Default Address Selection for IPv6

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

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

This draft has been approved as a proposed standard.

#### [4.5.5](#) Stateful Address Autoconfiguration

Stateful Address Autoconfiguration MAY be supported. For those IPv6 Nodes that implement a stateful configuration mechanism such as [[DHCPv6](#)], those nodes MUST initiate stateful address autoconfiguration upon the receipt of a Router Advertisement with the Managed address flag set. In addition, as defined in [[RFC2462](#)], in the absence of a router, hosts that implement a stateful configuration mechanism such as [[DHCPv6](#)] MUST attempt to use stateful address autoconfiguration.

For IPv6 Nodes that do not implement the optional stateful configuration mechanisms such as [[DHCPv6](#)], the Managed Address flag of a Router Advertisement can be ignored. Furthermore, in the absence of a router, this type of node is not required to initiate stateful address autoconfiguration as specified in [[RFC2462](#)].

### [4.6](#) Other

#### [4.6.1](#) [RFC2473](#) - Generic Packet Tunneling in IPv6 Specification

Generic Packet Tunneling [[RFC-2473](#)] MUST be supported for nodes implementing 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](#)] MUST be supported by nodes supporting multicast applications. A primary IPv6 multicast application is Neighbor Discovery (all those solicited-node mcast addresses must be joined).

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

## [5](#). Transport Layer and DNS

### [5.1](#) Transport Layer

#### [5.1.1](#) [RFC2147](#) - TCP and UDP over IPv6 Jumbograms

This specification is 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.

Internet-Draft

October 31, 2002

DNS, as described in [[RFC-1034](#)], [[RFC-1035](#)] and [[RFC-1886](#)] MAY be supported. 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 MAY be supported.

### 5.2.2 [RFC2732](#) - Format for Literal IPv6 Addresses in URL's

[RFC 2732](#) is MUST be supported if applications on the node use URL's.

## 5.3 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

The Dynamic Host Configuration Protocol for IPv6 [[DHCPv6](#)] is MAY be supported.

## 6. IPv4 Support and Transition

IPv6 nodes MAY support IPv4. However, this document should consider the following cases: native IPv6 only; native IPv6 with IPv4 supported only via tunneling over IPv6; and native IPv6 and native IPv4 both fully supported.

### 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](#) MUST be supported.

This document is currently being updated.

## 7. Mobility

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

Mobile Node functionality MAY be supported.

Route Optimization functionality SHOULD be supported for hosts.  
Route Optimization is not required for routers.

Home Agent functionality is MAY be supported.

## [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. IPsec transport mode MUST be supported. IPsec tunnel mode MUST be supported.

Applying single security association of ESP [[RFC-2406](#)] to a packet is MUST, 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 MUST be supported, if AH [[RFC-2402](#)] is implemented.

The following packet type MUST be supported 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 MUST be supported.

case 1-1 and 1-3 MUST be supported if AH is implemented.

case 1-4, 1-5, 2-5 and 4 MUST be supported if IPsec tunnel mode is implemented.

case 2-4 is MUST be supported if IPsec tunnel mode and AH is

implemented.  
case 3 is not applicable to this document.

## [8.2](#) Security Protocols

ESP [[RFC-2406](#)] MUST be supported.

AH [[RFC-2402](#)] MUST be supported. AH is needed if there is data in IP header to be protected, for example, an extension header.

However, in practice, ESP can provide the same security services as AH 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 MUST

be supported if interoperability is required with old implementations supported DES-CBC. Note, however, the IPsec WG recommends not using this algorithm. 3DES-CBC is SHOULD be supported, so that ESP CBC-Mode Cipher Algorithms [[RFC-2451](#)] MUST be supported. Note that the IPsec WG also recommends not using this algorithm.

AES-128-CBC [ipsec-ciph-aes-cbc] is MUST be supported. NULL Encryption algorithm [[RFC-2410](#)] MUST be supported for providing integrity service and also for debugging use.

The use of HMAC-SHA-1-96 within ESP, described in [[RFC-2404](#)] MUST be supported. This MUST be used if AH is implemented. The Use of HMAC-MD5-96 within ESP, described in [[RFC-2403](#)] MUST be supported. This MUST be used if AH is implemented. The "HMAC-SHA-256-96 Algorithm and Its Use With IPsec" [ipsec-ciph-sha-256] MUST be supported, 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 Methods

Manual keying MUST be supported

Automated SA and Key Management SHOULD be supported 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](#)] MAY be supported 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 MUST be supported by nodes that perform 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 MUST

be supported.

## [10](#). Network Management

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

### [10.1](#) MIBs

In a general sense, MIBs are required by the nodes that support a SNMP agent. It should be also noted that these specifications are being 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

Loughney (editor)

[Page 13]

---

Internet-Draft

October 31, 2002

## [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 some kinds 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 chicken-and-egg problems on running automated key management protocols on top of IP. However, manually keyed IPsec may require a large number of SAs in order to run on a large network due to the use of many addresses during ICMPv6 Neighbor Discovery.

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.



- [MLDv2] Vida, R. et al., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", Work in Progress.
- [RFC-1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [RFC-1886] Thomson, S. and Huitema, C., "DNS Extensions to support 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, 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.

---

Internet-Draft

October 31, 2002

- [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 Anycast" Work in Progress.
- [SOI] C. Madson, "Son-of-IKE Requirements", Work in Progress.
- [RFC-793] Postel, J., "Transmission Control Protocol", [RFC 793](#), August 1980.
- [RFC-1034] Mockapetris, P., "Domain names - concepts and facilities", [RFC 1034](#), November 1987.
- [RFC-2147] Borman, D., "TCP and UDP over IPv6 Jumbograms", [RFC 2147](#), May 1997.
- [RFC-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 Ethernet 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.

Loughney (editor)

[Page 17]

---

Internet-Draft

October 31, 2002

[RFC-2470] M. Crawford, T. Narten, S. Thomas, "A Method for the Transmission 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 Network Addresses", [RFC2851](#), June 2000.
- [RFC-2874] Crawford, M. and Huitema, C., "DNS Extensions to Support 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.

Loughney (editor)

[Page 18]

---

Internet-Draft

October 31, 2002

- [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

Loughney (editor)

[Page 19]

---

Internet-Draft

October 31, 2002

[raraghun@cisco.com]

Shoichi Sakane  
[shoichi.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

#### 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](mailto:ipng@sunroof.eng.sun.com)) or to:

John Loughney

Nokia Research Center  
Itämerenkatu 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.
- Reformatted chapters.
- Added [Appendix B](#) - List of RFCs.

TBD

## Appendix B: Specifications Not Included

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

### Upper Protocols

2428 FTP Extensions For IPv6 And NATs

### Compression

2507 IP Header Compression

2508 Compressing IP/UDP/RTP Headers For Low-Speed Serial Links

2509 IP Header Compression Over PPP

### Informational

1752 The Recommendation For The IP Next Generation Protocol API RFCs

Loughney (editor)

[Page 20]

---

Internet-Draft

October 31, 2002

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