INTERNET DRAFT
IPng Working Group
<draft-wasserman-ipv6-nd-division-00.txt>

Margaret Wasserman
Epilogue Technology

January 1998
Expires July 1998

Division of IPv6 Neighbor Discovery Into Separable Mechanisms

Status of this Memo

This document is an Internet-Draft. 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.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet- Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind, but proposes changes to existing Internet Drafts. Distribution of this memo is unlimited.

Abstract

This memo proposes a formal division of the existing IPv6 Neighbor Discovery protocol into eight separable, related mechanisms: Address Resolution, Duplicate Address Detection (DAD), Router Discovery, Prefix/Parameter Discovery, Address Autoconfiguration, Router Unreachability Detection (RUD), Neighbor Unreachability Detection (NUD) and ICMPv6 Redirects. These mechanisms all depend upon a common set of ICMPv6 Neighbor Discovery messages, but can be enabled and disabled independently, subject to the restrictions and recommendations outlined in this draft.

It is not the intention of this memo to propose substantive changes to the existing IPv6 Neighbor Discovery protocol, but to allow the separate portions of IPv6 Neighbor Discovery to be unambiguously identified, making it possible to specify or configure different portions of IPv6 Neighbor Discovery for use on specific link-types, links or interfaces.

1. Introduction

In discussions within the IETF IPng Working Group and on the mailing list, it has become clear that different portions of the IPv6 Neighbor Discovery (ND) protocol[1] may or may not be applicable to specific situations (e.g. tunnels). For example, it might be desireable to perform DAD on a link for which Router Discovery is unnecessary. Or, RD could be valuable in a situation where Address Resolution is not needed.

It has also become clear that the use of some portions of ND, such as Address Resolution, could be specified in the link-type specifications ("IPv6 over XXXX"), whereas it might be useful to configure some portions of ND on a per-link or per-interface basis (e.g. DAD).

In order to advance these discussions, it is necessary to view ND as a group of separable, related mechanisms -- mechanisms which share a common set of conceptual datastructures and ICMPv6 ND messages but which can be used (or not used) independently. Although this view is already discussed in the IPv6 ND specification, the current specification does not separately describe the behaviour of these mechanisms or divide them with sufficiently fine granularity. It is the purpose of this draft to specify eight separable ND mechanisms, identify their dependencies, determine restrictions on their configuration and use, make recommendations regarding their default state and propose their requirement levels within compliant IPv6 implementations. This draft is highly derivative of the IPv6 Neighbor Discovery specification[1] and does not describe the ND mechanisms in their entirety. This draft attempts to clarify, not substantially modify, the mechanisms defined in the ND specification.

2. Terminology

This draft relies on the terminology included in the current IPv6 Neighbor Discovery Internet Draft [1].

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY and OPTIONAL, when they appear in this document are to be interpreted as described in [2].

3. ND Messages and Conceptual Datastructures

Although the basic mechanisms of IPv6 Neighbor Discovery remain unchanged, the ability to selectively enable specific mechanisms will result in some nodes which only require a subset of the messages or datastructures required for a full IPv6 ND implementation. The messages, options, datastructures and states used by each portion of IPv6 ND are described in the mechanism-specific and summary sections below.

The five ICMPv6 messages described in the Neighbor Discovery specification and their options remain unchanged. Depending upon

which ND mechanisms are in use, however, a node could support sending or receiving only a subset of the ND messages or none at all. Unsupported messages MUST be silently discarded in most cases.

The conceptual datastructures described in the ND specification are also unmodified. However, a full set of conceptual datastructures may not be needed on a node which only implements a subset of IPv6 ND.

3.1 Levels of Neighbor Cache Support

The full set of Neighbor Cache states and the corresponding semantics may not be necessary on all nodes (e.g. those which do not have both Address Resolution and Neighbor Unreachability Detection enabled). In order to specify which portions of the full Neighbor Cache are necessary on different systems, it is useful to define three different levels of Neighbor Cache implementation:

Level 0: No Neighbor Cache.

This level would be applicable to a host which does not implement either Address Resolution or Neighbor Unreachability Detection. In this case, no Neighbor Cache lookup is necessary to send an IPv6 packet, so no Neighbor Cache need be maintained.

Level 1: 2-State Neighbor Cache.

This level would be applicable to a host which implements Address Resolution but does not implement Neighbor Unreachability Detection. This datastructure would be roughly equivalent to the ARP cache on IPv4 hosts.

This cache would have only two states: INCOMPLETE and COMPLETE.

Entries in the INCOMPLETE state do not have any valid link-layer address information associated with them. They may have one or more queued packets awaiting address resolution.

Entries in the COMPLETE state do have link-layer address information suitable for use in sending packets. They can be updated by subsequent Neighbor Advertisements with new link-layer address information.

COMPLETE entries periodically timeout. An implementation MAY choose whether to detect such a timeout immediately, on a periodic sweep, or when the next packet is sent to the corresponding

destination. When a timeout is detected, the timed-out entry MAY be returned to the INCOMPLETE state or removed from the cache.

These two states can be viewed as a degenerate version of the states in the full Neighbor Cache described in the current ND specification as follows:

INCOMPLETE PROBE	INCOMPLETE
STALE REACHABLE DELAY	COMPLETE

Viewing the Neighbor Cache as a two-state cache when Neighbor Unreachability Detection is not in use can greatly simplify the implementation of Address Resolution for minimal systems which do not provide any support for Neighbor Unreachability Detection.

If there is significant resistance to having different cache semantics for different combinations of ND features, the same functionality can be achieved by adjusting the default timer values based upon the specific ND options currently enabled.

Level 2: 5-State Neighbor Cache.

This level would be applicable to a host which implements both Address Resolution and Neighbor Unreachability Detection. This is the full Neighbor Cache currently described in the ND specification.

4. Address Resolution

Address Resolution is one of the core mechanisms of IPv6 Neighbor Discovery. It allows IPv6 addresses to be mapped to link-layer addresses via the exchange of Neighbor Solicitation and Neighbor Advertisement ICMPv6 messages containing Source Link-Layer Address and Target Link-Layer Address options. Information regarding the address mapping is stored in a Neighbor Cache conceptual datastructure (Level **1 or higher).** IPv6 ND Address Resolution is not dependent upon the use of other IPv6 ND mechanisms.

IPv6 ND Address Resolution is only useful on multicast-capable link-types which require a network-layer mechanism for mapping IPv6 addresses to link-layer addresses.

For multicast-capable links that require an address

resolution mechanism, the link-type specification SHOULD mandate the use of IPv6 ND Address Resolution.

For multicast-capable links that do not require an address resolution mechanism (e.g. some point-to-point links) the link-type specification SHOULD specifically state that IPv6 ND Address Resolution will not be used.

For non-multicast-capable links, the link-type specification MAY specify modifications to the IPv6 ND Address Resolution mechanism or MAY specify a different address resolution mechanism.

>From a node's perspective, use of IPv6 ND Address Resolution is enabled or disabled on a per-interface basis based solely upon the link-type of the interface's link. Interfaces to links which support IPv6 ND Address Resolution MUST have Address Resolution support enabled while others MUST have support for IPv6 ND Address Resolution disabled. ICMPv6 Neighbor Solicitation or Advertisement messages received on links which have IPv6 ND Address Resolution disabled MUST be silently discarded, unless they are of interest to other enabled ND mechanisms.

The basic mechanism for IPv6 ND Address Resolution is unchanged from the ND specification, except for the possible changes in the Neighbor Cache states described in the previous section.

All compliant IPv6 implementations MUST support IPv6 ND Address Resolution for any link-types which require it.

5. Duplicate Address Detection

Duplicate Address Detection (DAD) involves sending an ICMPv6 Neighbor Solicitation message (with or without link-layer address options) when a new address token is added to an interface in order to detect duplicate address tokens in use on the link. DAD can be very valuable when it is possible for two or more nodes to accidentally (or through human error) choose the same interface token for use on a shared link. DAD's usefulness is sharply curtailed on a given link if it is not implemented for all nodes on the link. DAD requires support for both the ICMPv6 Neighbor Solicitation and Advertisement messages, but does not require support for either of the link-layer address options. If DAD is enabled and IPv6 ND Address Resolution is not enabled, any received link-layer address options MAY be ignored.

DAD does, however, introduce some traffic overhead and a delay in interface initialization. For links that do not implement IPv6 ND Address Resolution, DAD also introduces additional ICMPv6 messages. So the benefits may not justify the costs in some cases. Therefore, a link-type specification SHOULD specify whether DAD is or is not REQUIRED for a specific link-type. If the link-type specification

indicates that use of DAD is optional for a given link-type, it SHOULD specify what mechanism will be used to determine whether or not DAD is in use on a given link at a given time (e.g. automatic mechanism, manual configuration, etc.).

Because DAD may introduce too much overhead in specific situations, implementations MAY allow DAD to be disabled on a per-node or per-interface basis via stateful or manual configuration (within the restrictions imposed by the link-type specifications). Implementations which support DAD SHOULD default to using DAD for all new interface tokens on all interfaces for which it has not be explicitly disabled.

DAD does not depend upon any other ND mechanisms and can be implemented without support for any of the ND conceptual datastructures. Compliant IPv6 implementations MUST support the use of DAD on all link-types for which it is not explicitly disabled by the link-type specification.

6. Router Discovery

Router Discovery allows IPv6 hosts to dynamically discover routers which can be used to forward packets off-link. This is accomplished through the use of ICMPv6 Router Solicitations and Router Advertisements. In general hosts send Router Solicitations and process received Advertisements while routers send Router Advertisements periodically or in response to Solicitations. Hosts which support Router Discovery store the information received in Router Advertisements in a Default Router List. Routers which support Router Discovery MAY or MAY NOT store information based upon received Router Advertisements, but the use of that information lies outside the scope of the Neighbor Discovery protocol.

Router Discovery is a complex process which can be extremely valuable when hosts are configured on complex or changing networks, but it may be unnecessary for some link-types (e.g. Point-to-point links where all traffic is sent through the remote end-point). There are also security issues with Router Discovery that may make it undesireable in some environments. Therefore, Router Discovery MAY be explicitly enabled or disabled for a particular link-type in the link-type specification. Implementations SHOULD also allow Router Discovery to be disabled on a per-interface basis (via stateful or manual configuration).

Nodes MUST silently discard Router Solicitations and Advertisements received on interfaces which do not have Router Discovery enabled, unless those messages are of interest to other enabled ND mechanisms.

The term Router Disocovery refers only to the process of receiving Router Advertisements and adding and deleting advertised routers to/from the Default Router List. Processing the additional configuration information obtained in Router Advertisments, configuring addresses based upon that information and maintaining

reachability information for routers are covered by Prefix/Parameter Discovery, Address Autoconfiguration and Router Unreachability Detection, respectively. It is possible to enable Router Discovery to dynamically create and maintain a Default Router List without enabling any of these separate, related mechanisms.

When a router is placed in the Default Router List, its lifetime is also included. This lifetime may be updated by subsequent Router Advertisements, pursuant to the restrictions in the ND specification. When the lifetime of a Router Advertisement expires, the corresponding router will be removed from the Default Router List. It is also RECOMMENDED that nodes which implement Router Discovery include support for Router Unreachability Detection to allow ongoing communications using the "unreachable" router to choose a new next-hop address.

It is REQUIRED that all compliant IPv6 routers support Router Discovery. It is also RECOMMENDED that a compliant IPv6 host support Router Discovery, and hosts which do implement Router Discovery SHOULD default to using it for all interfaces for which it has not been explicitly disabled.

7. Prefix/Parameter Discovery

Prefix/Parameter Discovery is the mechanism by which hosts obtain information about an attached link to use in configuration of the interface. This information might include MTU information and the site local and/or global prefixes in use on the link and their associated lifetimes. Although this information is contained in Router Advertisement messages, it is possible to use this information for interface configuration without choosing to place the supplied router address(es) in the Default Router List.

Prefix/Parameter Discovery is the mechanism used to obtain this link-specific configuration information and store it in the Prefix List and other interface-specific configuration structures. The mechanism used for creating IPv6 addresses from this information is handled by a separate mechanism called Address Autoconfiguration.

Since Prefix/Parameter Discovery is required for Address Autoconfiguration, it is automatically enabled whenever Address Autoconfiguration is in use. It is also possible to configure Prefix/Parameter Discovery separately to allow configuration of link-specific information (e.g. MTU) when the IPv6 addresses will be obtained elsewhere (e.g. through either stateful or manual configuration).

It is possible for a link-type specification to explicitly disable the use of Prefix/Parameter Discovery for a specific link-type. The use of Prefix/Parameter Discovery MAY also be configurable on a per-interface basis.

A compliant IPv6 host SHOULD implement Prefix/Parameter Discovery on any applicable link-type. Routers MUST implement the ability to send Prefix and Parameter information in Router Advertisements on any applicable link-types, although they MAY allow use of this mechanism to be disabled on a per-interface basis.

8. Address Autoconfiguration

Address Autoconfiguration is an extremely powerful and desireable Neighbor Discovery mechanism for use in many situations. It is described in a separate ND-related document [3], but relies upon information contained in ND Router Advertisement messages and upon the Prefix/Parameter Discovery mechanism. After discovering prefix information via Prefix/Parameter Discovery, a host can automatically generate site-local and global IPv6 addresses to allow for global communication without any explicit configuration (manual or stateful).

This mechanism SHOULD be supported for all link-types which do not inherently allow discovery of address information through other means. When Address Autoconfiguration is in use for a particular link-type, the link-type specification SHOULD also specify use of DAD, unless another mechanism is provided for preventing or discovering duplicate IPv6 addresses.

A compliant IPv6 host SHOULD implement Address Autoconfiguration for applicable link-types. However, a host which supports Address Autoconfiguration SHOULD allow it to be disabled on a per-host or per-interface basis. Address Autoconfiguration is a host-only mechanism; routers obtain their address information through other means outside the scope of the Neighbor Discovery protocol.

9. Router Unreachability Detection

Router Unreachability Detection is dependent upon the use of Router Discovery. When a "discovered" router times-out and is removed from the Default Router List, the same router may also be currently in-use as a next-hop for communication with any number of destinations, either because it was originally chosen as the default router for that communication or due to subsequent ICMPv6 Redirects. Router Unreachability Detection is the process of looking through the destination cache, and causing all communications through the "unreachable" router to perform a new next-hop determination.

Although Router Discovery can be somewhat useful without the implementation of Router Unreachability Detection, it is highly RECOMMENDED that this mechanism be enabled when Router Discovery is enabled, as it introduces very little additional overhead and allows existing communications to recover smoothly when a router becomes unreachable.

10. Neighbor Unreachability Detection

Neighbor Unreachability Detection (NUD) uses Neighbor Solicitations, Neighbor Advertisements and on-going advice from upper-layer protocols to determine the two-way reachability of a particular neighbor. When a neighbor becomes unreachable, a node can perform Address Resolution again to determine if the neighbor is now reachable at a new link-layer address.

Neighbor Unreachability Detection is an interesting concept, the uses for which have not been completely established. When Address Resolution is in use, NUD allows for fairly quick recovery when a node changes to a new link-layer address. Also, when upper layer advice is available, this mechanism can help to eliminate unnecessary Address Resolution traffic.

However, on a link which does not use ND Address Resolution (e.g. point-to-point links), in situations where upper-layer advice may not be available (e.g. an SNMP agent or a transaction processing system), this mechanism may actually result in more traffic than otherwise necessary, determining two-way reachability on an ongoing basis when the information is not of interest.

Ultimately, Neighbor Unreachability Detection may prove very useful to allow for dynamically switching between treating a particular node as on-link or off-link for particular link-types with assymetric reachability (e.g. for RF links), but insufficient experience is available to be certain at this time.

For certain link-types, reachability may already be established by a link-layer mechanism before any packets are sent. In this case, Neighbor Unreachability Detection is redundant and should be disabled by the link-type specification.

For other situations, there are two factors that most influence whether Neighbor Unreachability Detection is useful for a given link:

- Whether ND Address Resolution is in-use.
- Whether upper-layer advice is available for
  a significant portion of the communications.

If ND Address Resolution is in use, and upper-layer advice is likely to be available, it is RECOMMENDED that Neighbor Unreachability Detection be used to cut down on superfluous Address Resolution traffic. Although use of Address Resolution is specified on a per-link-type basis, it may only be possible to determine if upper-layer advice will be available on a per-node basis. Therefore, implementations should allow Neighbor Discovery to be configured on a per-node or per-interface basis.

On links which do not use ND Address Resolution, it is RECOMMENDED that Neighbor Unreachability Detection be disabled unless specifically

overridden by the link-layer specification.

Given the uncertainty of the trade-offs between the complexity of Neighbor Unreachability Detection and its benefits, it is OPTIONAL for an implementation to support Neighbor Unreachability Detection unless the implementation supports a link-type for which Neighbor Unreachability Detection is REQUIRED by the link-type specification.

11. ICMPv6 Redirects

It is expected that the use of ICMPv6 Redirects will be supported on most, if not all, IPv6 interfaces. This mechanism allows a router to inform a host that IP datagrams destined for a particular node or subnet should be sent to a different next-hop address than the one currently in-use. This is accomplished via sending an ICMPv6 Redirect message.

The use of ICMPv6 Redirects on a particular link-type MAY be disabled by a link-type specification. A host implementation MAY allow ICMPv6 Redirects to be disabled on a per-interface basis. When ICMPv6 Redirects are not in use on a particular link, routers SHOULD NOT send Redirect messages. Any Redirect messages received by a host on an interface which has ICMPv6 Redirects disabled MUST be silently discarded.

For all applicable link-types, ICMPv6 Redirects MUST be supported by compliant IPv6 implementations.

12. Levels of Compliance

After separating the IPv6 Neighbor Discovery protocol into separate mechanisms, it becomes possible to discuss a minimal compliant IPv6 implementation which does not implement the full set of IPv6 Neighbor Discovery Mechanisms. This section attempts to summarize the requirement levels for the individual mechanisms discussed in this document.

12.1 Host Compliance

It is possible, on a link-type that does not require Address Resolution, DAD or support for ICMPv6 Redirects (e.g. a point-to-point link with a fixed end-point address), to have a compliant IPv6 host implementation that does not implement any ND mechanisms at all. This is not likely to be the case for a majority of IPv6 implementations, however.

To allow for minimal IPv6 host implementations, only those ND mechanisms which rely upon cooperation from all hosts on a given link have been strictly REQUIRED. It is anticipated that most IPv6 implementations will also include some or all of the RECOMMENDED mechanisms, but their usefulness to the nodes that implement them will not diminished if some nodes do not participate.

Each of the requirement levels discussed in this document may be overridden, in either direction, for a particular link-type by the link-type specification.

Compliant IPv6 hosts are REQUIRED to implement the host portions of the following mechanisms if they support any applicable link-types:

- Address Resolution
- Duplicate Address Detection
- ICMPv6 Redirects

It is strongly RECOMMENDED that IPv6 hosts implement the host portions of the following mechanisms, as applicable to their supported link-types:

- Router Discovery
- Prefix/Parameter Discovery
- Router Unreachability Detection
- Address Autoconfiguration

The following IPv6 ND mechanism is OPTIONAL for a compliant IPv6 host implementations, unless explicitly required by a supported link-type:

- Neighbor Unreachability Detection

12.2 Router Compliance

Compliant IPv6 routers are REQUIRED to implement the router portions of the following IPv6 ND mechanisms if applicable to any of their supported link-types:

- Address Resolution
- Duplicate Address Detection
- ICMPv6 Redirects
- Router Discovery
- Prefix/Parameter Discovery

The following ND mechanisms are not applicable to routers:

- Address Autoconfiguration
- Router Unreachability Detection
- Neighbor Unreachability Detection

Routers MAY choose to use information contained in ND messages normally processed only by hosts (e.g. Router Advertisements), but use of that information is outside the scope of the Neighbor Discovery protocol.

13. Summary of Separable ND Mechanisms

Each of the eight separable ND mechanisms has been summarized

below. These summaries include the methods by which the mechanisms are configurable, the default state of each mechanism, the requirement level for implementation of each mechanism in a compliant IPv6 node and the messages and datastructures used by each mechanism.

12.1 ADDRESS RESOLUTION

```
Enabled Scope:          By Link-Type (in link-type specification)
Default:                Enabled on all interfaces
Requirement Level:      REQUIRED (for applicable link-types)
Dependencies:           None
Messages Required:      Neighbor Solicitation
                               with Source Link-Layer Address Option
                        Neighbor Advertisement
                               with Target Link-Layer Address Option
Datastructures:         Neighbor Cache, Level 1 or higher
```

12.2 DUPLICATE ADDRESS DETECTION (DAD)

```
Enabled Scope:          By Link-Type (in link-type spec)
                          with OPTIONAL Per-Node or Per-Interface override
Default:                Enabled on all interfaces
Requirement Level:      REQUIRED (for applicable link-types)
Dependencies:           None
Messages Required:      Neighbor Solicitation
                        Neighbor Advertisement
Datastructures:         None
```

12.3 ROUTER DISCOVERY

```
Enabled Scope:          By Link-Type (in link-type spec)
                          with RECOMMENDED Per-Interface override
Default:                Enabled on all interfaces, if supported
Requirement Level:      Router:  REQUIRED (for applicable link-types)
                        Host:    RECOMMENDED (for applicable link-types)
Dependencies:           None
Messages Required:      Router Solicitation
                        Router Advertisement
Datastructures:         Default Router List
```

12.4 PREFIX/PARAMETER DISCOVERY

```
Enabled Scope:          By Link-Type (in link-type spec)
                          with RECOMMENDED Per-Interface override
Default:                Enabled on all interfaces, if supported
Requirement Level:      Router:  REQUIRED (for applicable link-types)
                        Host:    RECOMMENDED (for applicable link-types)
Dependencies:           None
Messages Required:      Router Solicitation
                        Router Advertisement
Datastructures:         Prefix List
```

12.5 ADDRESS AUTOCONFIGURATION

```
Enabled Scope:          By Link-Type (in link-type spec)
                          with RECOMMENDED Per-Interface override
Default:                Router:  N/A
                        Host:    Enabled on all interfaces, if supported
Requirement Level:      Host:    RECOMMMENDED
                        (N/A for routers)
Dependencies:           Requires Prefix/Parameter Discovery
Messages Required:      Router Solicitation
                        Router Advertisement
Datastructures:         Prefix List
```

12.6 ROUTER UNREACHABILITY DETECTION

```
Enabled Scope:          By Link-Type (in link-type spec)
                          with RECOMMENDED Per-Interface override
Default:                Router:  N/A
                        Host:    Enabled on all interfaces, if supported
Requirement Level:      Host:    RECOMMENDED
                        (N/A for routers)
Dependencies:           Requires Router Discovery
Messages Required:      Router Solicitation
                        Router Advertisement
Datastructures:         Default Router List
```

12.7 NEIGHBOR UNREACHABILITY DETECTION

```
Enabled Scope:          By Link-Type (in link-type spec)
                          with RECOMMENDED Per-Interface override
Default:                Router:  N/A
                        Host:    Disabled on all interfaces
Requirement Level:      Host:    OPTIONAL
                        (N/A for routers)
Dependencies:           None
Messages Required:      Neighbor Advertisement
                        Neighbor Solicitation
Datastructures:         Neighbor Cache, Level 2
```

12.8 ICMPv6 REDIRECTS

```
Enabled Scope:          By Link-Type (in link-type spec) or
                          with OPTIONAL Per-Node or Per-Interface override
Default:                Enabled on all interfaces
Requirement Level:      REQUIRED (for applicable link-types)
Dependencies:           None
Required Messages:      ICMPv6 Redirect Message
Datastructures:         Destination Cache
```

14. Impact on other documents

If the working group agrees with the text of this document, or a

modified version thereof, it would be desireable to incorporate this information into the main IPv6 Neighbor Discovery specification. It is also possible that the current ND specification could be broken up into multiple documents to allow some mechanisms (which have remained constant for some time, are widely implemented and have no known problems) to advance in the standards process while we continue to gather experience with other mechanisms.

Link-type specifications SHOULD be modified, if necessary, to explicitly state whether IPv6 ND Address Resolution, DAD or ICMPv6 Redirects are in use for their link-type. In addition, link-type specifications SHOULD specify requirement levels and/or defaults for the other ND mechanisms individually if different from those discussed in this document. If a link-type specification does not explicitly state otherwise, it is assumed that all unmentioned ND mechanisms are applicable to the interface type and are subject to the requirements and defaults outlined above.

15. Security considerations

This draft introduces no new protocols or mechanisms and, therefore, does not introduce new security concerns. There are some existing security issues with the IPv6 Neighbor Discovery protocol, as discussed in [1], which are unaffected by the organizational change proposed in this draft.

16. Acknowledgments

The author would like to acknowledge the input of the IPng Working Group. This draft reflects ideas put forth at the IETF meeting in Washington, D.C., December 1997 by several working group members.

16. References

[1] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", draft-ietf-ipngwg-discovery-v2-01.txt.

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

[3] S. Thompson, T. Narten, "IPv6 Address Autoconfiguration", draft-ietf-ipngwg-addrconf-v2-00.txt.

17. Author's contact information

Please address all comments or questions regarding this draft to:

Margaret Wasserman mrf@epilogue.com
Director of IP Development (617)245-1805
Epilogue Technology Corporation FAX: (617) 245-0804