DNA Working Group
Internet-Draft
Intended status: Experimental
Expires: June 2, 2010

S. Narayanan, Ed.
iTCD/CSUMB

November 30, 2009

Design Alternative for Detecting Network Attachment in IPv6 Networks (DNAv6 Design Alternative) draft-ietf-dna-protocol-09.txt

Status of this Memo

Copyright Notice

Abstract

In this memo, a mechanism that was developed for detection of network attachement is documented for future reference. This memo is an informational document and thus does not define a new standard. The mechanism proposed in this experimental RFC requires the hosts to monitor all the prefixes advertised on the link and use it for link identification in the presence of non-DNAv6 routers is presented. A more efficient link-identification mechanism requiring the DNAv6 routers to monitor the link for advertised prefixes to assist the hosts in link identification combined with a fast router advertisement mechanism that selects the order of response for the router deterministically is also presented.

Table of Contents

1. Introduction

An efficient but complex mechanism to achieve the goals for detecting network attachment (DNA) [1] is documented in this memo. As the community decided to simplify the goals of DNA, this document was modified to be an informational RFC for archival purpose only. Hence, this document MUST NOT be considered to be making recommendation for the behavior of IPv6 hosts or routers. A simplied solution to achieve detection of network attachment can be found at [8].

This memo documents the mechanism for an IPv6 host to detect link-change in the presence of unmodified (non-DNAv6) routers and proposes new extensions to "IPv6 Neighbor Discovery" [2] to increase the efficiency of link-change detection in the presence of DNAv6 enabled routers. The proposed mechanism defines the construct that identifies a link, proposes an algorithm for the routers on the link to send a quick RA response without randomly waiting for upto MAX_RA_DELAY_TIME seconds as specified in RFC4861 [2].

The rest of the document refers to the proposed mechanisms by the term "DNAv6".

2. Terms and Abbreviations

The term "link" is used as defined in RFC 2460 [7]. NOTE: this is completely different from the term "link" as used by IEEE 802, etc.

Attachment: The process of establishing a layer-2 connection. Attachment (and detachment) may cause a link-change.

DNA Hint: An indication from other subsystems or protocol layers that link-change may have occurred.

Link-Change: Link-Change occurs when a host moves from a point-of-attachment on a link, to another point-of-attachment where it is unable to reach devices belonging to the previous link, without being forwarded through a router.

Point-of-Attachment: A link-layer base-station, VLAN or port through which a device attempts to reach the network. Changes to a host's point-of-attachment may cause link-change.

Reachability Detection: Determination that a device (such as a router) is currently reachable. This is typically achieved using Neighbor Unreachability Detection procedure [2].

3. Overview

The DNA protocol presented in this document tries to achieve the following objectives:

- Eliminate the delays introduced by RFC 4861 in discovering the configuration.
- Make it possible for the hosts to accurately detect the identity of their current link from a single RS-RA pair in the presence of either DNAv6 enabled routers and/or non-DNAv6 routers.

DNAv6 assumes that the host's link interface software and hardware is capable of delivering a 'link up' event notification when layer 2 on the host is configured and sufficiently stable for IP traffic. This event notification acts as a DNA Hint to the layer 3 DNA procedures to check whether or not the host is attached to the same link as before. DNAv6 also assumes that an interface on the host is never connected to two links at the same time. In the case that the layer 2 technology is capable of having multiple attachments (for instance, multiple layer 2 associations or connections) at the same time, DNAv6 requires the individual layer-2 associations to be represented as separate (virtual interfaces) to layer 3 and DNAv6 in particular.

3.1 Link Identification

DNAv6 uses the set of prefixes that are assigned to the link to uniquely identify the link, which is quite natural and doesn't require introducing any new form of identifier. However, this choice implies that the protocol needs to be robust against changes in the set of prefixes assigned to a link, including the case when a link is renumbered and the prefix is later reassigned to a different link. The protocol handles this during graceful renumbering (when the valid lifetime of the prefix is allowed to decrease to zero before it is removed and perhaps reassigned to a different link), it describes how to remove and reassign prefixes earlier than this without any incorrect behaviour, and will also recover in case where a prefix is reassigned without following the draft recommendations.

DNAv6 is based on using a Router Solicitation/Router Advertisement exchange to both verify whether the host has changed link, and if it has, provide the host with the configuration information for the new link. The base method for detecting link change involves getting routers to listen to all of the prefixes that are being advertised by other routers on the link. They can then respond to solicitations with complete prefix information. This information consists of the prefixes a router would advertise itself as per RFC 4861, and also, the prefixes learned from other routers on the link that are not

being advertised by itself. These learned prefixes are included in a new Learned Prefix Option in the Router Advertisement.

A host receiving one of these "Complete RAs" - so marked by a flag - then knows all of the prefixes in use on a link, and by inference all those that are not. By comparing this with previously received prefixes the host can correctly decide whether it is connected to the same link as previously, or whether this Router Advertisement is from a router on a new link.

If the link contains all non-DNAv6 routers, then the host relies on the completeness (which the host always keeps track) of its own prefix list to make a decision; i.e. if its own prefix list is known to be 'complete', the host can make a decision by comparing the received prefixes with its prefix list, if its own prefix is not yet 'complete', the host will wait for the completeness criteria to be met before making the comparison.

Though frequently all routers on a link will advertise the same set of prefixes and thus experience no cost in making the RAs complete, there is potential for the RAs to be large when there are many prefixes advertised. Two mechanisms are defined that allow certain RAs to be reduced in size. Both these mechanisms use one prefix as a representative for the set of prefixes on a particular link.

One uses a technique called a "landmark", where the host chooses one of the prefixes as a landmark prefix, and then includes this in the Router Solicitation message in the form of a question "Am I on the link which has this prefix?". The landmark is carried in a new option, called the Landmark Option.

In the case when the host is still attached to the same link, which might occur when the host has changed from using one layer 2 access point to another, but the access points are on the same link, the Router Advertisement(s) it receives will contain a "yes, that prefix is on this link" answer by the inclusion of the landmark prefix in the RA, and no other information. Thus, such RA messages are quite small.

In the case when the landmark prefix is unknown to the responding router, the host will receive a "No" answer by non-inclusion of the landmark prefix in the RA, and also the information it needs to configure itself for the new link. The routers try to include as much information as possible in such messages, so that the host can be informed of all the prefixes assigned to the new link as soon as possible.

A second mechanism for reducing packet sizes applies to unsolicited

Router Advertisements. By selecting a common prefix on the link to be the representative for the entire set of prefixes on the link, and making sure that it is included in every advertisement, it is possible to omit some prefixes. The smallest prefix on the link is selected as the common prefix. Such advertisements will not inform a host of all of the prefixes at once, but in general these unsolicited advertisements will not be the first advertisement received on a link. Inclusion of the smallest prefix simply ensures that there is overlap in the information advertised by each router on a link and that hosts will thus not incorrectly interpret one of these incomplete RAs as an indication of movement.

The Router Advertisement messages are, in general, larger than the solicitations, and with multiple routers on the link there will be multiple advertisements sent for each solicitation. This amplification can be used by an attacker to cause a Denial of Service attack. Such attacks are limited by applying a rate limit on the unicast Router Advertisements sent directly in response to each solicitation, and using multicast RAs when the rate limit is exceeded.

In order for the routers be able to both respond to the landmark questions and send the complete RAs, the routers need to track the prefixes that other routers advertise on the link. This process is initialized when a router is enabled, by sending a Router Solicitation and collecting the resulting RAs, and then multicasting a few RAs more rapidly as already suggested in RFC 4861. This process ensures with high probability that all the routers have the same notion of the set of prefixes assigned to the link.

3.2 Fast Router Advertisement

According to RFC 4861 a solicited Router Advertisement should have a random delay between 0 and MAX_RA_DELAY_TIME, to avoid the advertisements from all the routers colliding on the link causing congestion and higher probability of packet loss. In addition, RFC 4861 suggests that the RAs be multicast, and multicast RAs are rate limited to one message every 3 seconds. This implies that the response to a RS might be delayed up to 3.5 seconds.

DNAv6 avoids this delay by using a different mechanism to ensure that two routers will not respond at exactly the same time while allowing one of the routers on the link to respond immediately. Since the hosts might be likely to use the first responding router as the first choice from their default router list, the mechanism also ensures that the same router doesn't respond first to the RSs from different hosts. This modified mechanism replaces the rate limit on responses to RS required by [2]

The mechanism is based on the routers on the link determining (from the same RAs that are used in Section 3.1 to determine all the prefixes assigned to the link), the link-local addresses of all the other routers on the link. With this loosely consistent list, each router can independently compute some function of the (link-local) source address of the RS and each of the routers' link-local addresses. The results of that function are then compared to create a ranking, and the ranking determines the delay each router will use when responding to the RS. The router which is ranked as #0 will respond with a zero delay.

If the routers become out-of-sync with respect to their learned router lists, two or more routers may respond with the same delay, but over time the routers will converge on their lists of learned routers on the link.

4. Data Structures

This memo defines two new flags and three new options. The flags and the options MUST be implemented using Router Advertisement Flags option specified in RFC 5075 [21].

4.1 New Flags

This document defines two new flags to be exchanged between the router and hosts. One to indicate that the router sending the message is participating in the proposed protocol as well as a flag to indicate the completeness of the set of prefixes included in its messages.

DNAAware (D)

The DNAAware (D) bit indicates that the router sending the message is participating in the protocol documented in this memo. Other routers should include this router in calculating response delay tokens.

Complete (C)

The Complete (C) bit indicates that the Router Advertisement contains PIOs for all prefixes explicitly configured on the sending router, and, if other routers on the link are advertising additional prefixes, a Learned Prefix Option containing all additional prefixes that the router has heard from other routers on the link.

4.2 Landmark Option

The Landmark Option is used by hosts in a Router Solicitation message to ask the routers on a link if the specified prefix is being advertised by some router on the link.

4.3 Learned Prefix Option

The Learned Prefix Option (LPO) is used by a router to indicate prefixes that are being advertised by other routers on the link, but not by itself.

5. DNA Operation

5.1 DNA Router Operation

Routers MUST collect information about the other routers that are advertising on the link.

5.1.1 Data Structures

The routers maintain a set of conceptual data structures for each interface to track the prefixes advertised by other routers on the link, and also the set of DNA routers (the routers that will quickly respond to RSs) on the link.

For each interface, routers maintain a list of all prefixes learned from other routers on the link but not explicitly configured on the router's own interface. The list will be referred to in this document as "DNARouterLearnedPrefixList". Prefixes are learned by their reception within Prefix Information Options [2] in Router Advertisements. Prefixes in Learned Prefix Options (see Section 4.3) MUST NOT update the contents of DNARouterLearnedPrefixList. For each prefix the router MUST store sufficient information to identify the prefix and to know when to remove the prefix entry from the list. This may be achieved by storing the following information:

1. Prefix

2. Prefix length

3. Prefix valid lifetime

4. Expiry time

The expiry time for entries in DNARouterLearnedPrefixList is LEAST_VALID_LIFETIME after the last received Router Advertisement affecting the entry, or the scheduled expiry of the prefix valid

lifetime, whichever is earlier.

For each interface, routers also maintain a list of the other routers advertising on the link. The list will be referred to in this memo as "DNARouterList". For each router from which a Router Advertisement is received with the DNAAware flag set, the following information MUST be stored:

1. Link-local source address of advertising router

2. Expiry time

Each router MUST include itself in the DNARouterList based on the link-local address used in its RA messages.

The expiry time for entries in DNARouterList is LEAST_VALID_LIFETIME after the last received Router Advertisement affecting the entry.

5.1.2 Bootstrapping DNA Data Structures

As per RFC 4861 [2], when an interface on a host first starts up, it SHOULD transmit up to MAX_RTR_SOLICITATIONS Router Solicitations separated by RTR_SOLICITATION_INTERVAL in order to quickly learn of the routers and prefixes active on the link. DNAv6 requires the router to follow the same steps when its interface first starts up.

Upon startup, a router interface SHOULD also send a few unsolicited Router Advertisements as recommended in Section 6.2.4 of RFC 4861 [2], in order to inform others routers on the link of its presence.

During the bootstrap period ((MAX_RTR_SOLICITATIONS - 1) * RTR_SOLICITATION_INTERVAL + RetransTimer [2]), a router interface both sends unsolicited Router Advertisements and responds to Router Solicitations, but the Router Advertisements MUST NOT include any DNA specific options except for setting the DNAAware flag. The DNAAware flag is set so that other routers will know to include this router in their timing calculations for fast RA transmission. Other DNA options are omitted because the router may have incomplete information during bootstrap.

During the bootstrap period, the Complete flag in Router Advertisements MUST NOT be set.

During the bootstrap period, the timing of Router Advertisement transmission is as specified in RFC 4861.

5.1.3 Processing Router Advertisements

When a router receives a Router Advertisement, it first validates the RA as per the rules in RFC 4861, and then performs the actions specified in RFC 4861. In addition, each valid Router Advertisement is processed as follows:

If the DNAAware flag is set in the RA, the router checks if there is an entry in its DNARouterList by looking up the source address of the RA in that list. If not found, a new entry is added to DNARouterList, including the source address. The entry's expiry time is updated.

Regardless of the state of the DNAAware flag, each PIO in the RA is examined. If the prefix is not in the router's DNARouterLearnedPrefixList and not in the router's AdvPrefixList [2], the prefix is added to the DNARouterLearnedPrefixList, and its expiry time is set.

5.1.4 Processing Router Solicitations

The usual response to a Router Solicitation SHOULD be a unicast RA. However, to keep control of the rate of unicast RAs sent, a token bucket is used. The token bucket is filled at one token every UNICAST_RA_INTERVAL. A maximum of MAX_UNICAST_RA_BURST tokens are stored.

When a Router Solicitation is received, the router checks if it is possible to send a unicast response. A unicast response requires that the following conditions to be met:

- A unicast send token is available.
- The source address of the Router Solicitation is NOT the unspecified address (::).

If a unicast response is possible and the Router Solicitation contains a Landmark Option whose prefix is present in DNARouterLearnedPrefixList or AdvPrefixList, the router SHOULD send an abbreviated Router Advertisement. This abbreviated advertisement includes the Landmark prefix in a PIO if the prefix is in the AdvPrefixList or in a LPO if the prefix is found in the DNAROuterLearnedPrefixList, plus the base RA header and any SEND options as appropriate. The DNAAware flag MUST be set. The Complete flag MUST NOT be set. This is the one exception where the common prefix (i.e. the smallest prefix) MAY be omitted.

If there is NO Landmark Option in the received Router Solicitation or

it contains a Landmark Option whose prefix is NOT present in DNARouterLearnedPrefixList or AdvPrefixList or a unicast response is not possible, then the router SHOULD generate a Complete RA as specified in Section 5.1.5. The Router Advertisement MUST include the common prefix(es), as described in Section 5.1.6.

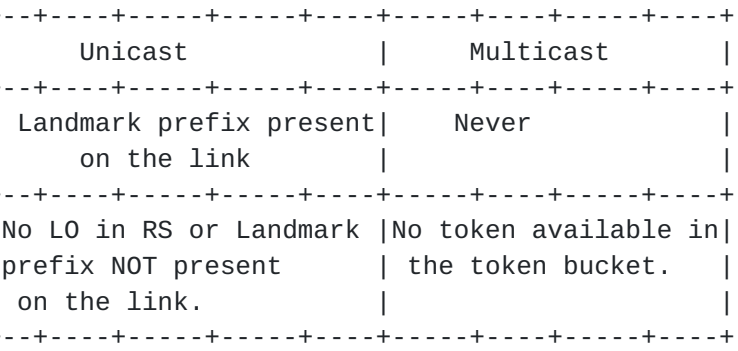
If a unicast response is possible, then a token is removed and the Router Advertisement is scheduled for transmission as specified in Section 5.1.7.

If a unicast response is not possible and there is no multicast RA already scheduled for transmission in the next MULTICAST_RA_DELAY the RA MUST be sent to the link-scoped all-nodes multicast address at the current time plus MULTICAST_RA_DELAY.

If a unicast response is not possible but there is a multicast RA already scheduled for transmission in the next MULTICAST_RA_DELAY, then the Router Solicitation MUST be silently discarded.

All Router Advertisements sent by a DNA router MUST have the "D" flag set so that hosts processing them know that they can interpret the messages according to this specification.

In order to understand the conditions leading to the different type of Router Advertisement messages, please refer to the figure below,



5.1.5 Complete Router Advertisements

A Complete RA is formed as follows:

Starting with a Router Advertisement with all fixed options (MTU, Advertisement Interval, flags, etc.), the DNAAware flag is set. As many Prefix Information Options for explicitly configured prefixes as will fit are added to the Router Advertisement. If there is sufficient room, a Learned Prefix Option as defined in Section 4.3

containing as many of the learned prefixes as will fit is added.

It may not be possible to include all of the prefixes in use on the link due to MTU or administrative limitations. If all Prefix Information Options and a Learned Prefix Option containing all of the learned prefixes were included in the RA, then the Complete flag in the Router Advertisement header is set.

If there are known to be prefixes that are not included in the Router Advertisement, then the Complete flag MUST NOT be set.

Note that although it may not be possible to fit all of the prefixes into an RA, the smallest prefix(es) MUST be included as discussed in Section 5.1.6.

5.1.6 Inclusion of a common prefixes

Among the prefixes advertised on a link, all routers selects one prefix and include that as a common prefix whenever they send an RA, both solicited and unsolicited.The inclusion of the common prefix ensures that there always is an overlap in the information advertised by each router on the link and that hosts will have a common prefix to correlate all RA messages received from routers on the same link.

This section presents how the routers select the common prefix without pre-arrangement,advertise it and change the common prefix gracefully without causing hosts to mistakenly assume a link change.

Even when stateful address configuration (DHCPv6) is used, at least one router on a link MUST be configured with one prefix, so that the common prefix can be included in the RA messages.

5.1.6.1 Selecting the common prefix

The router MUST pick the smallest prefix of all the prefixes configured on the routers on the link as the common prefix. The selection is made from among the prefixes whose valid lifetime is greater than LEAST_VALID_LIFETIME, and learned prefixes which were received within LEAST_VALID_LIFETIME.

For comparing prefixes, they are padded to the right with zeros to make them 128 bit unsigned integers. Note that this smallest prefix is the smallest of all the prefixes configured on the routers on the link and may not be the smallest prefix used in the link through stateful address configuration. Although, at the time of the writing of this memo, prefixes used even for stateful address autoconfiguration come from RAs.

When a router receives a new prefix in PIO or new prefix is configured on the router, if the prefix is smaller than the current common prefix and has valid lifetime greater than LEAST_VALID_LIFETIME, the router selects that new prefix as a new common prefix. In case a new prefix smaller than the current common prefix is advertised in LPIO, the router doesn't change the common prefix.

5.1.6.2 Advertising the common prefix

Whenever a router sends an RA, whether solicited or unsolicited, it MUST include the common prefix in it. Hence, all RAs MUST carry the common prefix except the abbreviated RA message sent in response to a RS with LO.

When a router advertises the common prefix, if the common prefix is explicitly configured on the router, it sends it in PIO. If the prefix was learned from advertisement of another router on the link, the router sends the common prefix in LPIO.

5.1.6.3 Changing the common prefix gracefully

Basic idea is, when a router changes a common prefix, it MUST send both the new common prefix and the old common prefix to ensure an overlapping prefix among RAs for LEAST_VALID_LIFETIME period and then it can retire the old common prefix.

When either a new prefix is added to a link that is numerically smaller than the current common prefix or the lifetime of the current common prefix falls below LEAST_VALID_LIFETIME, a new common prefix MUST be determined. In order to ensure that there is overlap between consecutive RAs on the link, the old common prefix must continue to be advertised for some time alongside the new common prefix. After the change, the old common prefix MUST be included in RAs for the following LEAST_VALID_LIFETIME. If the common prefix changes multiple times within LEAST_VALID_LIFETIME time window, the RA SHOULD include all of the previous common prefixes that were advertised during that time window.

For the purposes of propagating information, it is reasonable to assume that after three advertisements of the change, all routers have been made aware of it.

5.1.7 Scheduling Fast Router Advertisements

RAs may need to be delayed to avoid collisions in the case that there is more than one router on a link. The delay is calculated by determining a ranking for the router for the received RS, and

multiplying that by RA_SEPARATION.

A Host identifier is needed from the RS to calculate the router's ranking. The first 64 bits of an SHA-1 hash of the source address of the RS MUST be used as the RS host identifier.

A router's ranking is determined by taking the XOR of the RS Host identifier and first 64 bits of an SHA-1 hash of the link local source address of the router to be used in the RA. The results of these XOR operations are sorted lowest to highest. The router corresponding to the first entry in the sorted list is ranked zero, the second, one, and so on.

> Note: it is not necessary for a router to actually sort the whole list. Each router just needs to determine its own position in the sorted list.

If Rank < FAST_RA_THRESHOLD, then the RA MUST be scheduled for transmission in Rank * RA_SEPARATION milliseconds. When the router is ranked as zero, the resulting delay is zero, thus the RA SHOULD be sent immediately.

If Rank >= FAST_RA_THRESHOLD, then the RA MUST be replaced with a Complete RA, if there is not one already, and scheduled for multicast transmission as in RFC 4861.

5.1.8 Scheduling Unsolicited Router Advertisements

Unsolicited router advertisements MUST be scheduled as per RFC 4861.

The "D" flag in the RA header MUST be set.

They MAY be Complete RAs or MAY include only a subset of the configured prefixes, but MUST include the common prefix as discussed in Section 5.1.6.

This ensures that there will be overlap in the sets of prefixes contained in consecutive RAs on a link from DNA routers, and thus an absence of that overlap can be used to infer link change.

5.1.9 Removing a Prefix from an Interface

When a prefix is to stop being advertised in a PIO in RAs by an interface before the expiry of the prefix's valid lifetime, then the router MUST add the prefix to the DNARouterLearnedPrefixList and set it to expire in LEAST_VALID_LIFETIME or at the expiry of the last advertised valid lifetime, whichever is earlier. This ensures that to hosts there will be overlap in the prefixes in the RAs they see

and prevent them from incorrectly interpreting changed prefixes as movement.

5.1.9.1 Early Removal of the common Prefix

If the common (the smallest) prefix is to be withdrawn early from a link, that is before the expiry of its previously advertised valid lifetime, it MUST be advertised for at least LEAST_VALID_LIFETIME with a valid lifetime of less than LEAST_VALID_LIFETIME. This ensures that all of the other routers are notified to begin the process of changing the common prefix as well, and hosts will always see overlap between the prefixes in consecutive RAs and thus not mistake an RA for an indication of link change.

5.1.10 Prefix Reassignment

A prefix whose lifetime has expired after counting down in real time for at least LEAST_VALID_LIFETIME may be reassigned to another link immediately after expiry. If a prefix is withdrawn from a link without counting down to the expiry of its valid lifetime, it SHOULD NOT be reassigned to another link for at least LEAST_VALID_LIFETIME or until the original expiry time, whichever is earlier. This gives sufficient time for other routers that have learned the prefix to expire it, and for hosts that have seen advertisements from those routers to expire the prefix as well.

Earlier reassignment may result in hosts that move from between the old and new links failing to detect the movement.

When the host is sure that the prefix list is complete, a false movement assumption may happen due to renumbering when a new prefix is introduced in RAs at about the same time as the host handles the 'link UP' event. We may solve the renumbering problem with minor modification as specified below.

When a router starts advertising a new prefix, it includes at least one old prefix in the same RA. The old prefix assures that the host doesn't falsely assume a link change because of a new prefix. After a while, hosts will recognize the new prefix as the one assigned to the current link and update its prefix list.

In this way, we may provide a fast and robust solution. If a host can make the Complete Prefix List with certainty, it can check for link change fast. Otherwise, it can fall back on a slow but robust scheme. It is up to the host to decide which scheme to use.

5.2 DNA Host Operation

Hosts collect information about the prefixes advertised on the link to facilitate change detection.

5.2.1 Data Structures

Hosts MUST maintain a list of prefixes advertised on the link. This is separate from the RFC 4861 "Prefix List" and will be referred to here as the "DNAHostPrefixList". All prefixes SHOULD be stored, however an upper bound MUST be placed on the number stored to prevent overflow. For each prefix stored the host MUST store the following information:

1. Prefix

2. Prefix length

3. Expiry time

If a host is not able to store this information for every prefix, there is a risk that the host will incorrectly decide that it has moved to a new link, when it receives advertisements from a non-DNA router.

Prefix entries in the DNAHostPrefixList expire and MUST be removed LEAST_VALID_LIFETIME after they are last seen in a received Router Advertisement (in either a PIO or LPIO) or at the expiry of the valid lifetime of the prefix, whichever is earlier.

Hosts SHOULD also maintain a "Landmark Prefix" as described in Section 5.2.4.

5.2.2 Host Configuration Variables

Hosts MUST make use of the following conceptual variables and they SHOULD be configurable:

DNASameLinkDADFlag

Boolean value indicating whether or not a host should re-run DAD when DNA indicates that link change has not occurred.

Default: False

5.2.3 Detecting Network Attachment Steps

An IPv6 host SHOULD follow the following steps when they receive a DNA Hint indicating the possibility of link change.

1. Mark all the preferred IPv6 addresses in use as optimistic. See Section 5.2.7.2.

2. Set all Neighbor Cache entries for routers on its Default Router List to STALE.

3. Send router solicitation. (See Section 5.2.5).

4. Receive router advertisement(s).

5. Mark the router Neighbor Cache Entry [3] as REACHABLE for the router from which RA(s) arrived, or add a new Neighbor Cache Entry for the router in the REACHABLE state if one does not currently exist.

6. Process received router advertisement. (See Section 5.2.6).

7. If the link has changed

   Change the IP configuration parameters of the host (see Section 5.2.7).

8. If the link has NOT changed

   Restore the address configuration state of all the IPv6 addresses known to be on the link. See Section 5.2.7.2.

9. Update default routers list and their reachability information (see Section 5.2.6.3).

5.2.4 Selection of a Landmark Prefix

For each interface, hosts SHOULD choose a prefix to use as a Landmark Prefix in Router Solicitations. The following rules are used in selecting the landmark prefix:

The prefix MUST have a non-zero valid lifetime. If the valid lifetime of a previously selected Landmark Prefix expires, a new Landmark Prefix MUST be selected.

The prefix MUST be one of those that the hosts has used to assign a non-link-local address to itself.

The prefix SHOULD be chosen as the one with the longest preferred lifetime, but it is not necessary to switch to different prefix if the preferred lifetime of the current landmark prefix changes.

5.2.5 Sending Router Solicitations

Upon the occurrence of a Layer 2 link-up event notification, hosts SHOULD send a Router Solicitation. Hosts SHOULD apply rate limiting and/or hysteresis to this behaviour as appropriate to the link technology subject to the reliability of the DNA Hints.

Editor's note: The following two paragraph are talking about behavior specified by 4861. Do we want to keep these?

The host also uses this to trigger sending an RS, subject to the rate limitations in [2]. Since there is no natural limit on how frequently the link UP notifications might be generated, we take the conservative approach that even if the host establishes new link layer connectivity very often, under no circumstances should it send Router Solicitations more frequently than RTR_SOLICITATION_INTERVAL as specified by RFC 4861 [2].

If the RS does not result in the host receiving at least one RA with at least one valid prefix, then the host can retransmit the RS. It is allowed to multicast up to MAX_RTR_SOLICITATIONS RS messages spaced RTR_SOLICITATION_INTERVAL apart as per RFC 4861 [2].

Note that if link-layer notifications are reliable, a host can reset the number of sent Router Solicitations to 0, while still maintaining RTR_SOLICITATION_INTERVAL between RSs. Resetting the count is necessary so that after each link up notification, the host is allowed to send MAX_RTR_SOLICITATIONS to reliably discover the, possibly new, prefix list.

Hosts SHOULD include a Landmark Option (LO) in the RS message with the landmark prefix chosen based on the rules in Section 5.2.4.

Hosts SHOULD include a tentative source link layer address option (TO) in the RS message. The router solicitation message is sent to the All_Routers_Multicast address and the source address MUST be the link local address of the host.

The host MUST consider its link local address to be in the "Optimistic" state for duplicate address detection [5] until either the returned RA confirms that the host has not switched to a new link or, if an link change has occurred, until the host has performed optimistic duplicate address detection for the address.

5.2.6 Processing Router Advertisements

When the host receives a Router Advertisement, the host checks for the following conditions in the given order and derives the associated conclusions given below:

If the RA includes a prefix that matches an entry in its DNAHostPrefixList, then the host SHOULD conclude that no link change has occurred and the current configuration can be assumed to still be current.

If the RA is a Complete RA, as indicated by the "Complete" flag in the RA header, and there are no prefixes included in it in either a PIO or LPIO that are also in the host's DNAHostPrefixList, then the host MUST conclude that it has changed link and MUST initiate re-configuration using the information in the received Router Advertisement.

If the host has the complete prefix list (CPL) and the RA does NOT include any prefixes in either a PIO or LPIO that matches a prefix in CPL then the host MUST conclude that link change has occurred and use the information in the received RA to configure itself.

If the host doesn't have the complete prefix list (CPL), the received RA is not complete, contains no prefixes that are stored in DNAHostPrefixList, then the host SHOULD execute RS/RA exchange until num_RS_RA is equal to NUM_RS_RA_COMPLETE to create a new CPL and compare it with the already known prefixes. If after NUM_RS_RA_COMPLETE exchanges still no prefix received in either a PIO or LPO of the RAs match known prefixes, the host MUST conclude link change. If a matching prefix is received in the RAs, then the host SHOULD conclude that no link change has occured.

5.2.6.1 Pseudocode

```
IF (Receive RA contains a prefix matching a prefix in
DNAHostPrefixList) THEN

{

   /* This case covers the landmark prefix being included in the RA,
   smallest prefix included in RA or CompleteRA message containg all
   prefixes*/
```

```
      No link change has occured.

      RETURN; // Don't have to do the following checks.

   }

   IF (Receive RA is a CompleteRA) THEN

   {

      /* We already checked if there are any matching prefix before.
      Since this is a CompleteRA, implies link-change.*/

      Link change has occured.

      RETURN; // Don't have to do the following checks.

   }

   IF (DNAHostPrefixList is marked as complete (i.e. the completeness
   criteria is already met)) THEN

   {

      /* We already checked if there are any matching prefix before.
      Since the DNAHostPrefixList is complete, implies link-change.*/

      Link change has occured.

      RETURN; // Don't have to do the following checks.

   }

   Increment variable 'numberOfReceivedRAsSinceLastLinkUPEvent.

   IF (numberOfReceivedRAsSinceLastLinkUPEvent IS EQUAL TO
   NUM_RS_RA_COMPLETE), THEN

   {

      /* numberOfReceivedRAsSinceLastLinkUPEvent is a variable that
      tracks the number of RA received since last link up event.
      Previous link UP event here refers to the link UP received before
      the current link UP event that lead to this processing */

      Set numberOfReceivedRAsSinceLastLinkUPEvent to zero.
```

```
      IF (One of the received RA contains a prefix matching a prefix in
      DNAHostPrefixList from before the current link UP event), THEN

      {

         No link change has occured

      }

      ELSE

      {

         link change has occured.

      }

   }

   ELSE

   {

      No Decision.  Wait for more RAs to collect NUM_RS_RA_COMPLETE
      number of RS/RA exchanges.

   }
```

5.2.6.2 Maintaining the DNAHostPrefixList

The host should maintain a current DNAHostPrefixList with the prefixes learned after the current link UP event and a previous DNAHostPrefixList with prefixes learned prior to the link UP event. These data structures are maintained per interface.

If the Router Advertisement has the C flag set, then the host SHOULD make the current DNAHostPrefixList match the contents of the advertisement and mark it as complete (i.e. it becomes CPL). Any new prefixes are added and any prefixes in the list that are absent in the advertisement are removed. Expiry times on prefixes are updated if the prefix was contained in a PIO, but not if it was contained in an LPO.

If the Router Advertisement does not have the C flag set, then the host SHOULD add any new prefixes and update expiry times as above, but SHOULD NOT remove any entries from DNAHostPrefixList.

If the host decides that a link change has occurred after processing

the received RA message, it uses the information available in the current DNAHostPrefixList to configure itself as specified in Section 5.2.7. If the host decides that it is on the same link, then the current DNAHostPrefixList and the previous DNAHostPrefixList are merged as specified in the next sub-section and the merged list becomes the current DNAHostPrefixList.

For each interface, the host also maintains a counter (called num_RS_RA) which counts how many successful RS/RA exchanges have been accomplished since the last time the host moved to a different link. Note that this is not necessarily since the last link UP event as a link UP event may not correspond to an actual link change. The host declares "one successful RS/RA exchange" is accomplished after it sends an RS, waits for MIN_RA_WAIT seconds and receives a positive number of resulting RAs. At least one RA (with at least one prefix) should be received. After the RS, if a link UP event occurs before MIN_RA_WAIT seconds expire, the host should not assume that a successful RS/RA exchange is accomplished. This counter is used to determine when DNAHostPrefixList is considered to be complete. The host SHOULD conclude that the prefix list is complete when NUM_RS_RA_COMPLETE number of RS/RA exchanges have been completed or a RA message with the complete bit set is received. The complete DNAHostPrefixList is also refered to as CPL (Complete Prefix List).

After NUM_RS_RA_COMPLETE RS/ RA exchange, the host will generate the Complete Prefix List if there is no packet loss.

5.2.6.2.1 Merging DNAHostPrefixList

When a host has been collecting information about a potentially different link in its Current DNAHostPrefixList, and it discovers that it is in fact the same link as another DNAHostPrefixList, then it needs to merge the information in the two objects to produce a single new object. Since the DNAHostPrefixList contains the most recent information, any information contained in it will override the information in the old DNAHostPrefixList, for example the remaining lifetimes for the prefixes. When the two objects contain different pieces of information, for instance different prefixes or default routers, the union of these are used in the resulting merged object.

5.2.6.3 Router Reachability Detection and Default Router Selection

The receipt of a unicast RA from a router in response to a multicast RS indicates that the host has bi-directional reachability with the routers that responded. Such reachability is necessary for the host to use a router as a default router, in order to have packets routed off the host's current link. It is notable that the choice of whether the messages are addressed to multicast or unicast address

will have different reachability implications. The reachability implications from the hosts' perspective for the four different message exchanges defined by RFC 4861 [2] are presented in the table below. The host can confirm bi-directional reachability from the neighbor discovery or router discovery message exchanges except when a multicast RA is received at the host for its RS message. In this case, using IPv6 Neighbour Discovery procedures, the host cannot know whether the multicast RA is in response to its solicitation message or whether it is a periodic un-solicited transmission from the router [2].

Exchanges:	Upstream	Downstream
multicast NS/NA	Y	Y
unicast NS/NA	Y	Y
RS/multicast RA	N	Y
RS/unicast RA	Y	Y

If the destination address of the received RA is a unicast address, the host knows the router heard its RS, and therefore that the host has reachability with the router.

Prior to sending a DNA RS in response to an indication of link change, the host SHOULD set all Neighbor Cache entries for routers on its Default Router List to STALE. When the host receives an RA in reply to the RS, the host SHOULD mark that router's Neighbor Cache Entry [2] as REACHABLE, or add a Neighbor Cache Entry in the REACHABLE state if one does not currently exist.

The host SHOULD also update its Default Router List in the following fashion. If any of the routers returning RAs are already on the default router list, the host SHOULD use the information in the RA to update the Default Route List entry with the new information. The host SHOULD add entries to the Default Router List for any routers returning RAs that are not on the list. The host SHOULD confine selection of a router from the Default Router List to those routers whose Neighbor Cache entries are in the REACHABLE state. Note that the Default Router List SHOULD be updated as described here regardless of whether the RA indicates that the host has changed to a new IP link, since changes in router reachability are possible on some link types even if the host remains on the same IP link.

Note that this procedure does not prevent a host from sending packets

to its current default router while the RA solicitation is in progress and if reachability with the current default router is unchanged, there should be no change in default router after the RA solicitation completes. If the current default router is still reachable, it will forward the packets.

5.2.7 DNA and Address Configuration

When a host moves to a new point of attachment, a potential exists for a change in the validity of its unicast and multicast addresses on that network interface. In this section, host processing for address configuration is specified. The section considers both statelessly and statefully configured addresses.

5.2.7.1 Duplicate Address Detection

A DNA host MUST support optimistic Duplicate Address Detection [5] for autoconfiguring unicast link local addresses. If a DNA host uses address autoconfiguration [3] for global unicast addresses, the DNA host MUST support optimistic Duplicate Address Detection for autoconfiguring global unicast addresses.

5.2.7.2 DNA and the Address Autoconfiguration State Machine

When a link level event occurs on a network interface indicating that the host has moved from one point of attachment to another, it is possible that a change in the reachability of the addresses associated with that interface may occur. Upon detection of such a link event and prior to sending the RS initiating a DNA exchange, a DNA host MUST change the state of addresses associated with the interface in the following way (address state designations follow RFC 4861):

- Addresses in the "Preferred" state are moved to the "Optimistic" state, but the host defers sending out an NS to initiate Duplicate Address Detection.

- Addresses in the "Optimistic" state remain in the "Optimistic" state, but the host defers sending out an NS to initiate Duplicate Address Detection.

- Addresses in the "Deprecated" state remain in the "Deprecated" state.

- No addresses should be in the "Tentative" state, since this state is unnecessary for nodes that support optimistic Duplicate Address Detection.

A host MUST keep track of which "Preferred" addresses are moved to the "Optimistic" state, so it is possible to know which addresses were in the "Preferred" state and which were in the "Optimistic" state prior to the change in point of attachment.

In order to perform the DNA transaction, the DNA host SHOULD select one of the unicast link local addresses that was in the "Preferred" state prior to switching to "Optimistic" and utilize that as the source address on the DNA RS. If the host had no "Preferred" unicast link local address but did have an address in the "Optimistic" state, it MUST utilize such an address as the source address. If the host currently has no unicast link local addresses, it MUST construct one and put it into the "Optimistic" state and note this address as having been in the "Optimistic" state previously, but defer sending the NS to confirm. Note that the presence of a duplicate unicast link local address on the link will not interfere with the ability of the link to route a unicast DNA RA from the router back to the host nor will it result in corruption of the router's neighbor cache, because the TO is included in the RS and is utilized by the router on the RA frame without changing the neighbor cache.

When the host receives unicast or multicast RAs from the router, if the host determines from the received RAs that it has moved to a new link, the host MUST immediately move all unicast global addresses to the "Deprecated" state and configure new addresses using the subnet prefixes obtained from the RA. For all unicast link local addresses, the host MUST initiate NS signaling for optimistic Duplicate Address Detection to confirm the uniqueness of the unicast link local addresses on the new link.

If the host determines from the received RAs that it has not moved to a new link (i.e. the link has not changed) and the previous state of an address was "Optimistic", then the host MUST send an NS to confirm that the address is unique on the link. This is required because optimistic Duplicate Address Detection may not have completed on the previous point of attachment, so the host may not have confirmed address uniqueness. If the previous state of an address was "Preferred", whether or not the host initiates optimistic Duplicate Address Detection depends on the configurable DNASameLinkDADFlag flag. A host MUST forgo sending an NS to confirm uniqueness if the value of the DNASameLinkDAD flag is False. If, however, the DNASameLinkDAD flag is True, the host MUST perform optimistic duplicate address detection on its unicast link local and unicast global addresses to determine address uniqueness.

5.2.7.3 DNA and Statefully Configured Addresses

The DHCPv6 specification [18] requires hosts to send a DHCPv6 CONFIRM

message when a change in point of attachment is detected. Since the DNA protocol provides the same level of movement detection as the DHCPv6 CONFIRM, it is RECOMMENDED that DNA hosts not utilize the DHCPv6 CONFIRM message when a DNA RA is received, to avoid excessive signaling. If, however, a non-DNA RA is received, the host SHOULD use the DHCPv6 CONFIRM message as described in RFC 3315 [18] rather than wait for additional RAs to perform CPL, since this will reduce the amount of time required for the host to confirm whether or not it has moved to a new link. If the CONFIRM message validates the addresses, the host can continue to use them.

When a DNA RA is received and the received RA indicates that the host has not moved to a new link, the host SHOULD apply the same rules to interpreting the 'M' flag in the received RA and any subsequently received RAs as in RFC 4861 [2]. That is, if an RA is received with the 'M' flag set, then the 'M' flag value is copied into the ManagedFlag, and if the ManagedFlag changes from False to True the host should run DHCPv6, but if the ManagedFlag changes from True to False, the host should continue to run DHCPv6. If, however, the value of the ManagedFlag remains the same both before and after the change in point of attachment on the same link has been confirmed, it is NOT RECOMMENDED that the host run DHCPv6 to obtain new addresses, since the old addresses will continue to be valid.

If the DNA RA indicates that the host has moved to a new link or the DHCPv6 CONFIRM indicates that the addresses are invalid, the host MUST move its old addresses to the "Deprecated" state and MUST run DHCPv6 to obtain new addresses. Normally, the DHCPv6 operation is 4-message exchange, however, this exchange allows for redundancy (multiple DHCPv6 servers) without wasting addresses, as addresses are only provisionally assigned to a host until the host chooses and requests one of the provisionally assigned addresses. If the DNA host supports the Rapid Commit Option [18], the host SHOULD use the Rapid Commit Option in order to shorten the exchange from 4 messages to 2 messages.

5.2.7.4 Packet Delivery During DNA

The specification of packet delivery before, during, and immediately after DNA when a change in point of attachment occurs is out of scope for this document. The details of how packets are delivered depends on the mobility management protocols (if any) available to the host's stack.

5.2.7.5 Multicast Address Configuration

Multicast routers on a link are aware of which groups are in use within a link. This information is used to undertake initiation of

multicast routing for off-link multicast sources to the link [11][19].

If the returning RAs indicate that the host has not moved to a new link, no further action is required for multicast addresses to which the host has subscribed using MLD Report [19]. In particular, the host MUST NOT perform MLD signaling for any multicast addresses unless such signaling was not performed prior to movement to the new point of attachment. For example, if an address is put into the "Optimistic" state prior to movement but the MLD Report for the Solicited_Node_Multicast_Address is not sent prior to movement to a new point of attachment, the host MUST send the MLD Report on the new point of attachment prior to performing optimistic Duplicate Address Detection. The host SHOULD use the procedure described below for sending an MLD Report.

If, on the other hand, the DNA RA indicates that the host has moved to a new link, the host MUST issue a new MLD Report to the router for subscribed multicast addresses. MLD signaling for the Solicited_Node_Multicast_Addresses [3] MUST be sent prior to performing signaling for optimistic DAD.

To avoid lengthy delays in address reconfiguration, it is RECOMMENDED that the host send the MLD Report for newly configured addresses immediately, as soon as the addresses have been constructed, rather than waiting for a random backoff.

Hosts MUST defer MLD signaling until after the results of DNA have confirmed whether or not a link change has occurred.

6. Security Considerations

6.1 Attacks on the Token Bucket

A host on the link could easily drain the token bucket(s) of the router(s) on the link by continuously sending RS messages on the link. For example, if a host sends one RS message every UNICAST_RA_INTERVAL, and send a additional RS every third UNICAST_RA_INTERVAL, the token bucket in the router(s) on the link will drain within MAX_UNICAST_RA_BURST * UNICAST_RA_INTERVAL * 3 time-units. For the recommended values of UNICAST_RA_INTERVAL and MAX_UNICAST_RA_BURST, this value is 3000 milliseconds. It is not clear whether arrival of such RS messages can be recognized by the router as a DoS attack. This attack can also be mitigated by aggregating responses. Since only one aggregation is possible in this interval due to MIN_DELAY_BETWEEN_RAS restriction, the routers may not be able protect the tokens in the bucket.

6.2 Attacks on DNA Hosts

RFC 3756 outlines a collection of threats involving rouge routers. Since DNAv6 requires a host to obtain trustworthy responses from routers, such threats are relevant to DNAv6. In order to counter such threats, DNAv6 hosts SHOULD support RFC 3971 [4](SEND) secure router discovery.

6.3 Tentative options

The use of the Tentative Option in Neighbour and Router Solicitation messages acts in a similar manner to SLLAO, updating neighbour cache entries, in a way which causes packet transmission.

An attacker may cause messages be sent to another node by an advertising node (a reflector), without creating any ongoing state on the reflector.

This attack requires one solicitation for each advertisement and the advertisement has to go to a unicast MAC destination. That said, the size of the advertisement may be significantly larger than the solicitation, or the attacker and reflector may be on a medium with greater available bandwidth than the victim.

For link-layers where it isn't possible to spoof the link-layer source address this allows a slightly increased risk of reflection attacks from nodes which are on-link.

Additionally, since a SEND host must always advertise using SEND options and signatures, a non-SEND attacker may cause excess computation on both a victim node and a router by causing SEND advertisement messages to be transmitted to a particular MAC address and the all-nodes multicast. SEND specifies guidelines to hosts receiving unsolicited advertisements in order to mitigate such attacks [4].

While this is the same effect as experienced when accepting SLLAO from non-SEND nodes, the lack of created neighbour cache entries on the advertiser may make such attacks more difficult to trace.

Modification of Neighbour Discovery messages on the network is possible, unless SEND is used. [4] provides a protocol specification in which soliciting nodes sign ND messages with a private key and use addresses generated from this key.

Even if SEND is used, the lifetime of a neighbour cache entry may be extended by continually replaying a solicitation message to a particular router or hosts. Since this may be achieved for any

Neighbour or Router Solicitation message, corresponding advertisements to the original transmitters of these solicitation messages may occur.

SEND defines use of Timestamp values to protect a device from attack through replay of previously sent messages. Although this applies to Neighbour and Router Solicitation messages, granularity of the timestamp allows the messages to be used for up to five minutes [4].

All Router and Neighbour Solicitations using SEND contain a Nonce option, containing a random identifier octet string. Since SEND messages are digitally signed, and may not be easily modified, replay attacks will contain the same Nonce option, as was used in the original solicitation.

6.4 Authorization and Detecting Network Attachment

When a host is determining if link change has occurred, it may receive messages from devices with no advertised security mechanisms purporting to be routers, nodes sending signed router advertisements but with unknown delegation, or routers whose credentials need to be checked [14]. Where a host wishes to configure an unsecured router, it SHOULD confirm bidirectional reachability with the device, and it MUST mark the device as unsecured as described in [4].

In any case, a secured router SHOULD be preferred over an unsecured one, except where other factors (unreachability) make the router unsuitable. Since secured routers' advertisement services may be subject to attack, alternative (secured) reachability mechanisms from upper layers, or secured reachability of other devices known to be on the same link may be used to check reachability in the first instance.

6.5 Addressing

While a DNA host is checking for link-change, and observing DAD, it may receive a DAD defense NA from an unsecured source.

According to the SEND specification (RFC 3971 [4]) DAD defenses MAY be accepted even from non SEND nodes for the first configured address [4].

While deconfiguring the address is a valid action in the case where a host collides with another address owner after arrival on a new link, In the case that the host returns immediately to the same link, such a DAD defense NA message may be a denial-of-service attempt.

7. Constants

NUM_RS_RA_COMPLETE

Definition: Number of RS/RA exchange messages necessary to declare the prefix list to be complete.

Value: 2

MIN_RA_WAIT

Definition: Minimum time the host will have to wait before assuming receipt of all possible RAs.

Default: 4 seconds

UNICAST_RA_INTERVAL

Definition: The interval corresponding to the maximum average rate of Router Solicitations that the router is prepared to service with unicast responses. This is the interval at which the token bucket controlling the unicast responses is replenished.

Value: 50 milliseconds

MAX_UNICAST_RA_BURST

Definition: The maximum size burst of Router Solicitations that the router is prepared to service with unicast responses. This is the maximum number of tokens allowed in the token bucket controlling the unicast responses.

Value: 20

RA_SEPARATION

Definition: The separation between responses from different routers on the same link to a single Router Solicitation.

Value: 20 milliseconds

MULTICAST_RA_DELAY

Definition: The delay to be introduced when scheduling a multicast RA in response to a RS message when the token bucket is empty.

Value: 3000 milliseconds

FAST_RA_THRESHOLD

Definition: The maximum number of fast responses that a host should receive when soliciting for Router Advertisements.

Value: 3

LEAST_VALID_LIFETIME

Definition: The time for which received prefix can be considered valid for use in link indentification.

Value: LEAST_VALID_LIFETIME

8. Contributors

This document is the result of merging four different working group documents. The draft-ietf-dna-protocol-01.txt authored by James Kempf, Sathya Narayanan, Erik Nordmark, Brett Pentland and JinHyeock Choi was used as the base for the merger. The draft-ietf-dna-cpl-02 authored by JinHyeock Choi and Erik Normark provided the idea/text for the complete prefix list mechanism described in this document. The best current practice for hosts draft (draft-ietf-dna-hosts-03) authored by Sathya Narayanan, Greg Daley and Nicolas Montavont, and the tentative options (draft-ietf-dna-tentative-00) authored by Greg Daley, Erik Normark and Nick Moore were also adopted into this document.

9. Acknowledgments

The design presented in this document grew out of discussions among the members of the DNA design team (JinHyeock Choi, Tero Kauppinen, James Kempf, Sathya Narayanan, Erik Nordmark and Brett Pentland). The spirited debates on the design, and the advantages and dis-advantages of various DNA solutions helped the creation of this document.

Thanks to Syam Madanapalli who co-authored draft-jinchoi-dna-protocol2 from which this draft draws ideas, as well as providing feedback on draft-pentland-dna-protocol from which most of the text for this draft comes.

Thanks to Greg Daley for much feedback on draft-pentland-dna-protocol and for helping to work out how to merge the two drafts into this one.

Thanks to Jari Arkko, Jim Bound, Tero Kauppinen, Syam Madanapalli, Mohan Parthasarathy, Subba Reddy, and Christian Vogt for their review of draft-ietf-dna-protocol-01.

Thanks to Gabriel Montenegro for his review of draft-pentland-dna-protocol.

Thanks also to other members of the DNA working group for their comments that helped shape this work.

10. References

10.1 Normative References

[1] Choi, JH. and G. Daley, "Goals of Detecting Network Attachment in IPv6", RFC 4135, August 2005.

[2] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861, December 1998.

[3] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC2462 2462, December 1998.

[4] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[5] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, April 2006.

10.2 Informative References

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

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

[8] Krishnan, S. and SG. Daley, "Simple procedures for Detecting Network Attachment in IPv6", draft-ietf-dna-simple-01 (work in progress), July 2008.

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

[10] Haskin, D. and E. Allen, "IP Version 6 over PPP", RFC 2472, December 1998.

[11] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener

Discovery (MLD) for IPv6", RFC 2710, October 1999.

[12] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC2463 2463, December 1998.

[13] Christensen, M., Kimball, K., and F. Solensky, "Considerations for IGMP and MLD Snooping Switches", draft-ietf-magma-snoop-12 (work in progress), February 2005.

[14] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[15] Liebsch, M., Singh, A., Chaskar, H., Funato, D., and E. Shim, "Candidate Access Router Discovery (CARD)", RFC 4066, July 2005.

[16] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[17] O'Hara, B. and G. Ennis, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999.

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

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

[20] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[21] Haberman, B. and R. Hinden, "IPv6 Router Advertisement Flags Option", RFC 5175, March 2008.

[22] Yegin, A., "Link-layer Event Notifications for Detecting Network Attachments", draft-ietf-dna-link-information-00 (work in progress), September 2004.

[23] Manner, J. and M. Kojo, "Mobility Related Terminology", draft-ietf-seamoby-mobility-terminology-06 (work in progress), February 2004.

[24] Choi, J. and E. Nordmark, "DNA with unmodified routers: Prefix list based approach", draft-ietf-dna-cpl-00 (work in progress), April 2005.

Authors' Addresses

Sathya Narayanan (editor)
School of Information Technology and Communications Design
California State University, Monterey Bay
3110, Inter-Garrison Road, Building 18, Room 150
Seaside, CA 93955
USA

Phone: +1 (831) 582-33411
Email: snarayanan@csumb.edu

James Kempf
DoCoMo Communications Labs USA
USA

Phone:
Email: kempf@docomolabs-usa.com

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Mountain View, CA
USA

Phone: +1 650 786 2921
Email: erik.nordmark@sun.com

Brett Pentland
Centre for Telecommunications and Information Engineering
Department of Electrical and Computer Systems Engineering
Monash University
Clayton, Victoria 3800
Australia

Phone: +61 3 9905 5245
Email: brett.pentland@eng.monash.edu.au

JinHyeock Choi
Samsung Advanced Institute of Technology
PO Box 111
Suwon 440-600
Korea

Phone: +82-31-280-8194
Email: jinchoe@samsung.com

Greg Daley
Centre for Telecommunications and Information Engineering
Department of Electrical adn Computer Systems Engineering
Monash University
Clayton, Victoria 3800
Australia

Phone: +61 3 9905 4655
Email: greg.daley@eng.monash.edu.au

Nicolas Montavont
LSIIT - Univerity Louis Pasteur
Pole API, bureau C444
Boulevard Sebastien Brant
Illkirch 67400
FRANCE

Phone: (33) 3 90 24 45 87
Email: montavont@dpt-info.u-strasbg.fr
URI: http://www-r2.u-strasbg.fr/~montavont/

Nick 'Sharkey' Moore

Email: sharkey@zoic.org