Internet Engineering Task Force (IETF)
Request for Comments: 6059
Category: Standards Track
ISSN: 2070-1721

S. Krishnan
Ericsson
G. Daley
Netstar Logicalis

November 2010

Simple Procedures for Detecting Network Attachment in IPv6

Abstract

Detecting Network Attachment allows hosts to assess if its existing addressing or routing configuration is valid for a newly connected network. This document provides simple procedures for Detecting Network Attachment in IPv6 hosts, and procedures for routers to support such services.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6059.

Table of Contents

1. Introduction

Hosts require procedures to simply and reliably identify if they have moved to a network to which they had been recently connected. In order to detect reconnection to a previously visited network, router and neighbor discovery messages are used to collect reachability and configuration information. This information is used to detect if the host has attached to a link for which it may still have valid address and other configuration information, and which it can use until it receives confirmation through either the Neighbor Discovery protocol or DHCPv6.

This document incorporates feedback from host and router operating systems implementors, which seeks to make implementation and adoption of IPv6 change detection procedures simple for general use.

1.1. Goals

The goal of this document is to specify a simple procedure for Detecting Network Attachment (Simple DNA) that has the following characteristics.

- Routers do not have to be modified to support this scheme.
- The most common use cases are optimized.
- In the worst case, detection latency is equal to that of standard neighbor discovery so that performance is never degraded.
- False positives are not acceptable. A host must not wrongly conclude that it has reattached to a previously visited network.
- False negatives are acceptable. A host may fail to identify a previously visited link correctly and attempt to acquire fresh addressing and configuration information.

1.2. Applicability

The Simple DNA protocol provides substantial benefits over standard neighbor discovery procedures [RFC4861] in some scenarios and does not provide any benefit at all in certain other scenarios. This is intentional as Simple DNA was designed for simplicity rather than completeness. In particular, the Simple DNA protocol provides maximum benefits when a host moves between a small set of known links. When a host moves to a completely new link that is previously unknown, the performance of the Simple DNA protocol will be identical to that using standard neighbor discovery procedures [RFC4861]. In this case, the main benefit of the Simple DNA protocol is to

immediately flush out the inoperable addresses and configuration instead of timing them out. The Simple DNA procedure provides support for addresses configured using either IPv6 Stateless Address Autoconfiguration [RFC4862] or DHCPv6 [RFC3315]. It does not support manually configured addresses since they are not widely used and can cause unpredictable results and/or aggressive probing behavior (see Appendix A).

1.3. Link Identification Model

Earlier methods of Detecting Network Attachment, e.g., the procedure defined in [DNA-PROTOCOL], relied on detecting whether the host was still connected to the same link. If the host was attached to the same link, all information related to the link such as the routers, prefixes, and configuration parameters was considered to be valid. The Simple DNA protocol follows an alternate approach where it relies on probing each previously known router to determine whether to use information learnt from THAT router. This allows Simple DNA to probe routers learnt from multiple earlier attachments to optimize movement between a known set of links.

1.4. DNA Overview

Detecting Network Attachment is performed by hosts after detecting a link-layer "up" indication. The host uses a combination of unicast Neighbor Solicitations (NSs) and multicast Router Solicitations (RSs) in order to determine whether previously encountered routers are present on the link, in which case an existing configuration can be reused. If previously encountered routers are not present, then either IPv6 Stateless Address Autoconfiguration and/or DHCPv6 is used for configuration.

Hosts implementing Simple DNA may also send DHCPv6 packets, as described in Section 5.5.4. Since Simple DNA does not modify the DHCPv6 protocol or state machine, the operation of DHCPv6 is unchanged.

Routers that follow the standard neighbor discovery procedure described in [RFC4861] will delay the router advertisement (RA) by a random period between 0 and MAX_RA_DELAY_TIME (defined to be 500 ms) as described in Section 6.2.6 of [RFC4861]. In addition, consecutive RAs sent to the all-nodes multicast address are rate limited to no more than one advertisement every MIN_DELAY_BETWEEN_RAS (defined to be 3 seconds). This will result in a worst-case delay of 3.5 seconds in the absence of any packet loss.

Hosts implementing Simple DNA can detect the presence of a previously encountered router using unicast Neighbor Solicitations. As a result, where the host with a valid configuration is returning to a previously encountered link, delays in the sending of a Router Advertisement (RA) will not delay configuration as long as NS probing is successful. However, in situations where the host is attaching to a link for the first time, or where it does not have a valid IP address on the link, it will be dependent on the receipt of an RA for stateless autoconfiguration. In these situations, delays in the receipt of an RA can be significant and may result in service disruption.

1.5. Working Assumptions

There are a series of assumptions about the network environment that underpin these procedures.

- The combination of the link-layer address and the link-local IPv6 address of a router is unique across links.

- Hosts receive indications when a link layer comes up. Without this, they would not know when to commence the DNA procedure.

If these assumptions do not hold, host change detection systems will not function optimally. In that case, they may occasionally detect change spuriously or experience some delay in Detecting Network Attachment. The delays so experienced will be no longer than those caused by following the standard neighbor discovery procedure described in [RFC4861].

2. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Terminology

Term	Definition
Valid IPv6 address	An IPv6 address configured on the node that has a valid lifetime greater than zero.
Operable IPv6 address	An IPv6 address configured on the node that can be used safely on the current link.
Router identifier	Identifier formed using the link-local address of a router along with its link-layer address.
D-Flag	Flag indicating whether the address was obtained using Stateless Address Autoconfiguration (SLAAC) or DHCPv6. If it is set to 0, then SLAAC was used to configure the address. If it is set to 1, then DHCPv6 was used to configure the address.
O-Flag	Flag indicating whether the address is operable. If it is set to 0, the address is inoperable. If it is set to 1, the address is operable.
S-Flag	Flag indicating whether SEND [RFC3971] was used in the Router Advertisement that resulted in the creation/modification of this SDAT entry. If it is set to 0, then SEND was not used. If it is set to 1, then SEND was used.
Candidate Router Address	A router address in the SDAT that is associated with at least one valid address.
Candidate Router Set	A set of router addresses that has been identified for NS-based probing.

Table 1: Simple DNA Terminology

4. The Simple DNA Address Table (SDAT)

In order to correctly perform the procedure described in this document, the host needs to maintain a data structure called the Simple DNA address table (SDAT). The host needs to maintain this data structure for each interface on which it performs Simple DNA. Each entry in the SDAT table will be indexed by the router identifier (link-local + link-layer address of the router) and consists of at least the following parameters. Fields tagged as [S] are used for addresses configured using SLAAC. Fields tagged as [D] are used for addresses obtained using DHCPv6. Fields tagged as [S+D] are used in both cases.

- [S+D] Link-local IPv6 address of the router(s)
- [S+D] Link-layer (MAC) address of the router(s)
- [S+D] Flag indicating whether the address was obtained using SLAAC or DHCPv6. (The D-Flag)
- [S+D] IPv6 address and its related parameters like valid lifetime, preferred lifetime, etc.
- [S] Prefix from which the address was formed.
- [S] Flag indicating whether SEND was used. (The S-Flag)
- [D] DHCP-specific information in case DHCPv6 [RFC3315] was used to acquire the address. This information includes the DUID, the IAID, a flag indicating IA_NA/IA_TA, and configuration information such as DNS server address, NTP server address, etc.
- [S+D] Flag indicating whether the address is operable. (The O-Flag)

5. Host Operations

On connecting to a new point of attachment, the host performs the Detecting Network Attachment procedure in order to determine whether the existing addressing and configuration information are still valid.

5.1. On Receipt of a Router Advertisement

When the host receives a Router Advertisement and the router identifier of the sending router is not present in the SDAT, the host processes the Router Advertisement as specified in Section 6.3.4 of [RFC4861]. Additionally, the host performs the following operations.

If the Router Advertisement is protected by SEND, the S-Flag MUST be set to 1 in the SDAT entries created/modified by this RA.

- The host configures addresses out of the autoconfigurable prefixes advertised in the RA, as specified in [RFC4862]. The host MUST add an SDAT entry (indexed by this router identifier) for each such address the host configures.

- The host might have already configured addresses out of the autoconfigurable prefixes advertised in the RA. This could be a result of receiving the prefix in an RA from another router on the same link. The host MUST add an SDAT entry (indexed by this router identifier) for each such address the host had already configured.

- The host might have DHCPv6-assigned addresses that are known to be operable on the link. The host MUST add an SDAT entry (indexed by this router identifier) for each such DHCPv6 address.

5.2. After Assignment of a DHCPv6 Address

After the host is assigned an address by a DHCPv6 server, it needs to associate the address with the routers on link. The host MUST create one SDAT entry for each of the on-link routers associated with the DHCPv6-assigned address.

5.3. Steps Involved in Detecting Link Change

The steps involved in basic detection of network attachment are:

- Link-layer indication

- Sending of neighbor discovery probes

- Response gathering and assessment

These steps are described below.

5.4. Link-Layer Indication

In order to start detection of network attachment procedures, a host typically requires a link-layer indication that the medium has become available [RFC4957].

After the indication is received, the host MUST mark all currently configured (non-tentative) IP addresses as inoperable until the change detection process completes. It MUST also set all Neighbor

Cache (NC) entries for the routers on its Default Router List to STALE. This is done to speed up the acquisition of a new default router in case the host attaches to a previously unvisited link.

5.5. Sending Neighbor Discovery probes

5.5.1. Sending Router Solicitations

When a host receives a link-layer "up" indication, it SHOULD immediately send a Router Solicitation (as specified in Section 6.3.7 of [RFC4861]). The Router Solicitation is sent to the all-routers multicast address using a link-local address as the source address [RFC4861]. Even if the host is in possession of more than one valid IPv6 address, it MUST send only one router solicitation using a valid link-local address as the source address.

5.5.2. Sending Neighbor Solicitations

The host iterates through the SDAT to identify a set of candidate routers for NS-based probing. Each router in the SDAT that is associated with at least one valid address is added to the candidate router set exactly once. For each router in the candidate router set, the host MUST send a unicast Neighbor Solicitation to the router's link-local address it obtained from the lookup on the SDAT. The host MUST set the link-layer destination address in each of these neighbor solicitations to the link-layer address of the router stored in the SDAT. The host MUST NOT send unicast Neighbor Solicitations to a router that is not associated to a valid address in the SDAT. If at least one entry in the SDAT for a given router had the S-Flag set, the host SHOULD use SEND to secure the NS probe being sent to the router.

5.5.3. Concurrent Sending of RS and NS Probes

The host SHOULD send the Neighbor-Solicitation-based unicast probes in parallel with the multicast Router Solicitation. Since sending NSs is just an optimization, doing the NSs and the RS in parallel ensures that the procedure does not run slower than it would if it only used a Router Solicitation.

NOTE: A Simple DNA implementation SHOULD limit its NS-based probing to at most six previously seen routers.

5.5.4. Initiating DHCPv6 Exchange

On receiving a link-layer "up" indication, the host will initiate a DHCPv6 exchange (with the timing and protocol as specified in [RFC3315]) in order to verify whether the addresses and configuration

obtained using DHCPv6 are still usable on the link. Note that DHCPv6, as specified today, only attempts to confirm addresses obtained on the most recently attached link.

5.6. Contents of the Neighbor Discovery Messages

5.6.1. Neighbor Solicitation Messages

This section describes the contents of the neighbor solicitation probe messages sent during the probing procedure.

Source Address:	A link-local address assigned to the probing host.
Destination Address:	The link-local address of the router being probed as learned from the SDAT.
Hop Limit:	255
ND Options:	
Target Address:	The link-local address of the router being probed as learnt from the SDAT.
Link-Layer Header:	
Destination Address:	The link-layer (MAC) address of the router being probed as learnt from the SDAT.

The probing node SHOULD include the source link-layer address option in the probe messages.

5.6.2. Router Solicitation Messages

This section describes the contents of the router solicitation probe message sent during the probing procedure.

Source Address:	A link-local address assigned to the probing host.
Destination Address:	The all-routers multicast address.
Hop Limit:	255

The probing node SHOULD NOT include the source link-layer address option in the probe messages.

5.7. Response Gathering

5.7.1. Receiving Neighbor Advertisements

When a Neighbor Advertisement is received from a router in response to an NS probe, the host MUST verify that both the IPv6 and link-layer (MAC) addresses of the router match the expected values before utilizing the configuration associated with the detected network (prefixes, MTU, etc.). The host MUST then go through the SDAT and mark the addresses (both SLAAC and DHCPv6 acquired) associated with the router as operable.

5.7.2. Receiving Router Advertisements

On reception of a Router Advertisement, the host MUST go through the SDAT and mark all the addresses associated with the router (both SLAAC and DHCPv6 acquired) as inoperable. The host MUST then process the Router Advertisement as specified in Section 6.3.4 of [RFC4861].

5.7.3. Conflicting Results

5.7.3.1. Conflicting Results between RS and NS Probes

Where the conclusions obtained from the Neighbor Solicitation/Advertisement from a given router and the RS/RA exchange with the same router differ, the results obtained from the RS/RA will be considered definitive. In case the Neighbor Advertisement was secured using SEND and the Router Advertisement was not, the host MUST wait for SEND_NA_GRACE_TIME to see if a SEND-secured RA is received. If a SEND-secured RA is not received, the conclusions obtained from the NS/NA exchange will be considered definitive.

5.7.3.2. Conflicting Results between DHCPv6 and NS Probes

Where the conclusions obtained from the Neighbor Solicitation/Advertisement for a given DHCPv6-assigned address and the conclusions obtained from the DHCPv6 exchange differ, the results obtained from the DHCPv6 exchange will be considered definitive.

5.8. Further Host Operations

Operations subsequent to Detecting Network Attachment depend upon whether or not the host has reconnected to a previously visited network.

After confirming the reachability of the associated router using an NS/NA pair, the host performs the following steps.

- The host SHOULD rejoin any solicited nodes' multicast groups for addresses it continues to use.

- The host SHOULD select a default router as described in Section 6.3.6 of [RFC4861].

If the host has determined that it has reattached to a previously visited link, it SHOULD NOT perform duplicate address detection on the addresses that have been confirmed to be operable.

If the NS-based probe with a router did not complete or if the RS-based probe on the same router completed with different prefixes than the ones in the SDAT, the host MUST begin address configuration techniques, as indicated in a received Router Advertisement [RFC4861] [RFC4862].

5.9. On Connecting to a New Point of Attachment

A host usually maintains SDAT entries from some number of previously visited networks. When the host attaches to a previously unknown network, it MAY need to discard some older SDAT entries.

5.10. Periodic Maintenance of the SDAT

The host SHOULD maintain the SDAT table by removing entries when the valid lifetime for the prefix and address expires, that is, at the same time that the prefix is removed from the Prefix List in [RFC4861]. The host SHOULD also remove a router from an SDAT entry when that router stops advertising a particular prefix. When three consecutive RAs from a particular router have not included a prefix, then the router should be removed from the corresponding SDAT entry. Likewise, if a router starts advertising a prefix for which there already exists an SDAT entry,then that router should be added to the SDAT entry.

5.11. Recommended Retransmission Behavior

Where the NS probe does not complete successfully, it usually implies that the host is not attached to the network whose configuration is being tested. In such circumstances, there is typically little value in aggressively retransmitting unicast neighbor solicitations that do not elicit a response.

Where unicast Neighbor Solicitations and Router Solicitations are sent in parallel, one strategy is to forsake retransmission of Neighbor Solicitations and to allow retransmission only of Router Solicitations or DHCPv6. In order to reduce competition between unicast Neighbor Solicitations and Router Solicitations and DHCPv6

retransmissions, a DNAv6 implementation that retransmits may utilize the retransmission strategy described in the DHCPv6 specification [RFC3315], scheduling DNAv6 retransmissions between Router Solicitations or DHCPv6 retransmissions.

If a response is received to any unicast Neighbor Solicitation, pending retransmissions of the same MUST be canceled. A Simple DNA implementation SHOULD NOT retransmit a Neighbor Solicitation more than twice. To provide damping in the case of spurious link-up indications, the host SHOULD NOT perform the Simple DNA procedure more than once a second.

6. Pseudocode for Simple DNA

```
/* Link-up indication received on INTERFACE */
/* Start Simple DNA process */

/* Mark all addresses as inoperable */
Configured_Address_List=Get_Address_List(INTERFACE);
for each Configured_Address in Configured_Address_List
{
  if (Get_Address_State(Configured_Address)!=AS_TENTATIVE)
  {
    Set_Address_State(Configured_Address,AS_INOPERABLE);
  }
}

/* Mark all routers' NC entries as STALE to speed up */
/* acquisition of new router if link change has occurred */
for each Router_Address in DEFAULT_ROUTER_LIST
{
  NCEntry=Get_Neighbor_Cache_Entry(Router_Address);
  Set_Neighbor_Cache_Entry_State(NCEntry,NCS_STALE);
}

/* Thread A : Send Router Solicitation */
RS_Target_Address=FF02::2;
RS_Source_Address=Get_Any_Link_Local_Address(INTERFACE);
Send_Router_Solicitation(RS_Source_Address,RS_Target_Address);

/* Thread B : Send Neighbor Solicitation(s) */
Previously_Known_Router_List=Get_Router_List_from_SDAT();
NS_Source_Address=Get_Any_Link_Local_Address(INTERFACE);
```

```
   for each Router_Address in Previously_Known_Router_List
   {
     if (Get_Any_Valid_Address_from_SDAT(Router_Address))
     {
       Send_Neighbor_Solicitation(NS_Source_Address,
                                  Router_Address.L3_Address,
                                  Router_Address.L2_Address);
     }
   }

   /* Thread C : Response collection of RAs */

   /* Received Router Advertisement processing */
   /* Only for RAs received from routers in the SDAT */

   L3_Source=Get_L3_Source(RECEIVED_MESSAGE);
   L2_Source=Get_L2_Source(RECEIVED_MESSAGE);
   SDAT_Entry_List=Get_Entries_from_SDAT_L2L3(L3_Source,L2_Source));

   /* Mark all the addresses associated with the router as inoperable */
   for each SDAT_Entry in SDAT_Entry_List
   {
       Set_Address_State(SDAT_Entry,AS_INOPERABLE);
   }

   /* Ignore further NAs from this router */
   /* after delaying for x milliseconds */
   Add_Router_to_NA_Ignore_List(L3_Source,SEND_NA_GRACE_PERIOD);

   /* Perform Standard RA processing as per RFC 4861 / RFC 4862 */


   /* Thread D : Response collection of NAs */

   /* Received Neighbor Advertisement processing */
   /* Only for NAs received as response to DNA NSs */

   L3_Source=Get_L3_Source(RECEIVED_MESSAGE);
   L2_Source=Get_L2_Source(RECEIVED_MESSAGE);

   if (Is_Router_on_NA_Ignore_List(L3_Source)) {
     /* Ignore message and wait for next message */
     continue;
   }

   SDAT_Entry_List=Get_Entries_from_SDAT_L2L3(L3_Source,L2_Source));
```

```
for each SDAT_Entry in SDAT_Entry_List
{
    /* Address is operable. */
    Set_Address_State(SDAT_Entry,AS_OPERABLE);
    /* Configure on Interface */
}
```

Figure 1: Pseudocode for Simple DNA

NOTE: This section does not include any pseudocode for sending of the DHCPv6 packets since the DHCPv6 exchange is orthogonal to the Simple DNA process.

7. Constants

SEND_NA_GRACE_TIME

Definition: An optional period to wait after Neighbor Solicitation before adopting a non-SEND RA's link change information.

Value: 40 milliseconds

8. Relationship to DNAv4

DNAv4 [RFC4436] specifies a set of steps that optimize the (common) case of reattachment to an IPv4 network that a host has been connected to previously by attempting to reuse a previous (but still valid) configuration. This document shares the same goal as DNAv4 (that of minimizing the handover latency in moving between points of attachment) but differs in the steps it performs to achieve this goal. Another difference is that this document supports stateless autoconfiguration of addresses in addition to addresses configured using DHCPv6.

9. Security Considerations

A host may receive Router Advertisements from non-SEND devices, after receiving a link-layer indication. While it is necessary to assess quickly whether a host has moved to another network, it is important that the host's current secured SEND [RFC3971] router information is not replaced by an attacker that spoofs an RA and purports to change the link.

As such, the host SHOULD send a Neighbor Solicitation to the existing SEND router upon link-up indication as described above in Section 5.4. The host SHOULD then ensure that unsecured router

information does not cause deletion of existing SEND state, within MIN_DELAY_BETWEEN_RAS, in order to allow for a present SEND router to respond.

If the current default router is a SEND-secured router, the host SHOULD wait SEND_NA_GRACE_TIME after transmission before adopting a new default router.

Even if SEND signatures on RAs are used, it may not be immediately clear if the router is authorized to make such advertisements. As such, a host SHOULD NOT treat such devices as secure until and unless authorization delegation discovery is successful.

Unless SEND or another form of secure address configuration is used, the DNA procedure does not in itself provide positive, secure authentication of the router(s) on the network, or authentication of the network itself, as would be provided, e.g., by mutual authentication at the link layer. Therefore, when such assurance is not available, the host MUST NOT make any security-sensitive decisions based on the DNA procedure alone. In particular, it MUST NOT decide that it has moved from an untrusted to a trusted network, and MUST NOT make any security decisions that depend on the determination that such a transition has occurred.

10. Acknowledgments

This document is the product of a discussion the authors had with Bernard Aboba, Thomas Narten, Erik Nordmark, and Dave Thaler at IETF 69. The authors would like to thank them for clearly detailing the requirements of the solution and the goals it needed to meet and for helping to explore the solution space. The authors would like to thank the authors and editors of the complete DNA specification for detailing the overall problem space and solutions. The authors would like to thank Jari Arkko for driving the evolution of a simple and probabilistic DNA solution. The authors would like to thank Bernard Aboba, Thomas Narten, Jari Arkko, Sathya Narayan, Julien Laganier, Domagoj Premec, Jin Hyeock-Choi, Alfred Hoenes, Frederic Rossi, Ralph Droms, Ted Lemon, Erik Nordmark, Lars Eggert, Brian Carpenter, and Yaron Sheffer for performing reviews on the document and providing valuable comments to drive the document forward.

11. References

11.1. Normative References

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

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

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

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

11.2. Informative References

[DNA-PROTOCOL] Narayanan, S., Ed., "Design Alternative for Detecting Network Attachment in IPv6 Networks (DNAv6 Design Alternative)", Work in Progress, November 2009.

[RFC4436] Aboba, B., Carlson, J., and S. Cheshire, "Detecting Network Attachment in IPv4 (DNAv4)", RFC 4436, March 2006.

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

[RFC4957] Krishnan, S., Montavont, N., Njedjou, E., Veerepalli, S., and A. Yegin, "Link-Layer Event Notifications for Detecting Network Attachments", RFC 4957, August 2007.

Appendix A. Issues with Confirming Manually Assigned Addresses

Even though DNAv4 [RFC4436] supports verification of manually assigned addresses, this feature of DNAv4 has not been widely implemented or used. There are two major issues that come up with confirming manually assigned addresses using Simple DNA.

- When DHCPv6 or SLAAC addresses are used for probing, there is no need to aggressively retransmit lost probes. This is because the address configuration falls back to vanilla DHCPv6 or SLAAC, and the host will eventually obtain an address. This is not the case with manually assigned addresses. If the probes are lost, the host runs the risk of ending up with no addresses at all. Hence, aggressive retransmissions are necessary.

- Another issue comes up when the host moves between two networks, one where manual addressing is being used (say, NET1) and the other where dynamic addressing (stateless autoconfiguration or DHCPv6) is being used (say, NET2). Since the host can obtain a dynamic address in some situations, it will need to send Simple DNA probes and may also engage in a DHCPv6 exchange. In a situation where the host moves to NET1 and the NS probes are lost and in addition an RA is not received, the host will not be able to confirm that it attached to NET1, and therefore that it should use the manual configuration for that network. As a result, if DHCPv6 is enabled on NET1, then the host could mistakenly obtain a dynamic address and configuration instead of using the manual configuration. To prevent this problem, Simple DNA probing needs to continue even after the DHCPv6 exchange has completed, and DNA probes need to take precedence over DHCPv6, contrary to the advice provided in Section 5.7.3.

Given these issues, it is NOT RECOMMENDED to use manual addressing with Simple DNA.

Authors' Addresses

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
EMail: suresh.krishnan@ericsson.com

Greg Daley
Netstar Logicalis
Level 6/616 St Kilda Road
Melbourne, Victoria 3004
Australia

Phone: +61 401 772 770
EMail: hoskuld@hotmail.com