Network Working Group
Internet-Draft
Intended status: Experimental
Expires: March 7, 2019

DY Kim
Independent

September 3, 2018

Subnet ID Deprecation for IPv6
draft-dykim-6man-sid6-00

Abstract

Deprecation of the subnet ID in IPv6 networking is proposed; the subnet ID is set to zero so that all nodes in a site carry the same prefix. While the procedures for neighbor discovery and duplicate address detection have to be changed, possible simplification gains in IPv6 networking including that of intra-site host- and subnet-mobility might be worth the modification. Site-external behaviors don't change through this modification, enabling incremental deployment of the proposal. Sites of manageable sizes for which scalability is not much a critical issue might consider the mode of operation proposed in this document.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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

This Internet-Draft will expire on March 7, 2019.

Table of Contents

1. Introduction

The idea of IPv4 subnet has been imported intact into IPv6 networking so that each subnet (link) in an IPv6 site is assigned a separate subnet ID (SID). As a result, the IPv6 host has to change the link prefix every time it moves from one link to another even within the same site or routing domain; you have to install MIPv6 agents [MIPv6] on every intra-site router and a MIP6 client on every mobile node in order to provide intra-site node mobility. It might be challenged whether this legacy way of IPv6 operation should continue to be the best way in networking environments ever evolving to a form vastly different from that of the past.

For one thing, scalability, one of the main reasons for subnetting, might bear different implications from the past. Moor's Law has continued to be relevant for decades since the time IPv6 was first conceived, and cost or performance concerns for memories and processors have been dramatically relaxed. There might be many potential network administrators who would consider to weigh the burden of managing SIDs and the associated MIPv6 infrastructure against that of inherent mobility support by link-state routing.

This document proposes to change the operation of IPv6 networking by deprecating the SID. That is, the value of SID shall be set to zero. This results in all intra-site nodes carrying the same prefix and the mobile nodes keeping the same address as long as the mobility is confined within a given site.

A number of operational efficiency might result from this change. The price to pay might be some changes in the procedures for neighbor discovery (ND) and duplicate address detection (DAD). This document presents how this new operational paradigm, to be abbreviated as SID6, could be constructed and discusses possible impacts from this change.

It is to be noted that this document limits its SID6 discussions to the case of a site consisting of a single routing area; there are no Level 2 routers in the site under discussion. The multi-area case is left for further study.

2. Terminology

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 [KEYWORDS].

This document introduces the following terminology.

DA: Duplicate Advertisement. A unicast message, back to the source address of the previous DS message received, to report the duplicity of the target address in the DS message.

DS: Duplicate Solicitation. A site-wide multicast message to solicit the response from a node in possession of the same address as the target address in this message.

3. SID6 Construction

3.1. IPv6 Address

The IPv6 address type of interest is the Global Unicast address (GUA) which contains the SID and interface ID (IID) [v6ADDR]:

IPv6 GUA

= (interface address)

= (subnet prefix, IID)

= (global routing prefix, SID, IID)

Now, we reset the SID, and the IPv6 GUA will no longer depend on the SID; it doesn't change as a node moves across subnets (links) within a site:

IPv6 GUA

= (interface address)

= (subnet prefix, IID)

= (global routing prefix, null, IID)

Furthermore, we change the use of the IID as the node ID (NID). That is, each node is associated with an NID unique within a site. When a node has multiple interfaces, there would be multiple IIDs associated. In that case, we enforce all IIDs to be the same, thus ensuring a unique NID per node. The result is:

IPv6 GUA

= (node address)

= (subnet prefix, NID)

= (global routing prefix, null, NID)

This unique NID is invariant within a site or routing domain. The address is now a node address, not an interface address.

When a site is multihomed on multiple upstream networks, it would be associated with multiple site prefixes and hence every intra-site node would be associated with multiple addresses. For seamless site-multihoming in such an instance, a node should be able to receive inbound packets destined to any of its multiple addresses, and also

be able to source outbound packets with one of such multiple addresses as appropriate [DASv6].

Remember all we do here is to reset the SID. And that, it is not any change in the definition of the IPv6 address format, but is just an operational choice. All other effects are natural corollaries thereof; the basic IPv6 mechanisms remain the same. We will subsequently see how other parts of the IPv6 networking continue to work correctly as usual, with minimal modifications where necessary.

3.2. Neighbor Discovery

Addresses involved in ICMPv6-derived [ICMPv6] ND messages [NDv6] are either All-Nodes multicast addresses (FF02:0:0:0:0:0:0:1) or All-Routers multicast addresses (FF02:0:0:0:0:0:0:2), both of which being agnostic to SID. Otherwise, the involved addresses are unicast or anycast addresses which are not anymore dependent on SID as prescribed by SID6. The resulting link prefixes (global routing prefix + null) advertised by all routers within a site are the same, except for the inter-router point-to-point links [p2p127]. Although substantially simplifying router configuration in regard to prefix loading, this SID deprecation necessitates a change in on-link determination. The original ND [NDv6] specifies that an address is considered to be on-link if:

1. it is covered by one of the link's prefixes (e.g., as indicated by the on-link flag in the Prefix Information option), or

2. a neighboring router specifies the address as the target of a Redirect message.

3. a (solicited) Neighbor Advertisement message is received for the (target) address, or

4. any ND message is received from the address.

The latter two, however, have been deprecated by [v6SUBNET].

Criterion 2 should continue to be valid in SID6. However, Criterion 1 is of no more use since all links share the same prefix(es) throughout the site, except for the inter-router point-to-point links [p2p127]. Hence, a prefix with the on-link flag set is not a guarantee that a neighbor address with the very prefix is on-link.

Since on-link determination cannot be done through prefixes provided by a pair procedure of Router Solicitation (RS) and Router Advertisement (RA), some other means has to be secured. We propose

to use the Reachability test for the purpose and thus to accommodate the following procedure to the ND protocol for on-link determination:

- When a node is first injected into a site and attaches to a link, it might acquire the prefix information through a pair of RS and RA, and auto-configure itself with a node address sanitary-checked through DAD described in Section 3.3. If the node comes from a different link in the same site, these steps should be skipped.

- It then multicasts an unsolicited Neighbor Advertisement (NA) to the link-local All-Nodes address, FF02:0:0:0:0:0:0:1, to explicitly notify all other nodes on the same link of its emergence. The source address of this NA SHALL be the node address of the new node, and its link-layer address SHALL also be included as an option. In addition, a new option SHALL be incorporated to indicate that every recipient of this unsolicited NA SHOULD return a unicast NS back to the sender. Since NA transmission is unreliable, it can be repeated MAX_NEIGHBOR_ADVERTISEMENT times [NDv6] . The first NA SHOULD be issued after a random delay between 0 and MAX_RTR_SOLICITATION_DELAY [NDv6] to avoid race condition among multiple newly emerging nodes.

- On receipt of this unsolicited NA, other nodes on the link SHOULD return Neighbor Solicitation (NS) back to the new node. In this action, issuing of each NS SHOULD be random delayed to avoid race condition. Also, the link-layer address of the responding node SHALL be included in each NS. Duplicate NAs received through retransmission SHALL be silently ignored.

- Successful receipt of such a returning NS confirms the forward reachability from the new node's perspective; the responding address is declared to be on-link. The new node creates an entry for the responding address in Neighbor Cache, with the on-link flag set. This is done for each responding address.

- For each of such returning NSs, the new node unicasts an NA to the responding address. Successful receipt of this NA by each responding node confirms reachability from the responding node's perspective; the address of the new node is on-link. The responding node then creates an on-link entry for the new node's address in its own Neighbor Cache.

- Addresses in Neighbor Cache of a node acquired only through this procedure SHOULD be considered and flagged as on-link.

This new procedure differs from the existing ND procedure in that on-link determination is made not through Prefix List (for prefixes with

on-link flag set) but through Reachability tests between neighbors. The role of Prefix List reduces simply to providing the common prefix(es) for the given site. Another difference is in regard to the semantics of the source address for NA and NS; whereas it is the sender's interface address in the original ND, it is its node address in SID6.

With the introduction of this revised procedure for on-link determination, it follows that Criterion 3 of the original on-link determination SHOULD be revived:

> When a solicited NA message is received for the target address, the address is confirmed to be on-link.

Criterion 4 remains deprecated.

3.3. Duplicate Address Detection

DAD per IPv6 Stateless Address Autoconfiguration (SLAAC) is done for all unicast addresses by use of a pair of link-local ND messages, namely, NS and NA [SLAAC]. NSs are musticast to link-local Solicited-Node address [v6ADDR]:

> link-local Solicited-Node address: FF02:0:0:0:0:1:FFXX:XXXX

In SID6, however, DAD should be done site-wide, and hence new site-local messages should be introduced to do the job.

We name the new pair of ICMPv6 messages as Duplicate Solicitation (DS) and Duplicate Advertisement (DA). Also, we introduce a new type of multicast address named site-local Solicited-Node address defined in a way similar to the (link-local) Solicited-Node multicast address [v6ADDR]:

> site-local Solicited-Node address: FF05:0:0:0:0:1:FFXX:XXXX

A site-local Solicited-Node address is formed by taking the low-order 24 bits of an (unicast or anycast) address and appending those bits to the prefix FF05:0:0:0:0:1:FF00::/104 resulting in a multicast address in the range

> FF05:0:0:0:0:1:FF00:0000 ~ FF05:0:0:0:0:1:FFFF:FFFF

A DS is multicast to a site-local Solicited-Node address formed with the unicast or anycast address of the target node. If the target address of the returning DA is tentative, it is an indication that the address is a duplicate. Both nodes SHOULD then refresh their addresses and repeat DAD until no duplicates are observed. An

address is considered site-unique if none of the tests equivalent to the ones in Sec. 5.4 of [SLAAC] indicate the presence of a duplicate address within RetransTimer milliseconds after having sent DupAddrDetectTransmits DSs. A natural corollary of this site-wide DAD is that uniqueness of the NID(s) is confirmed site-wide.

3.4. Interior Gateway Protocols

A link-state Interior Gateway Protocols (IGP) is to be used in SID6; OSPFv3 [OSPFv3] or IS-IS for IPv6 [ISISv6][ISISv4]. The most important impact of SID6 on these link-state routing protocols is the way routers locate the hosts; they are not anymore locatable by link prefixes.

In SID6 operation of OSPFv3, host routes are to be included in intra-area-prefix-LSAs. For each of these host routes, the PrefixOptions LA-bit SHOULD be set and the PrefixLength SHOULD be set to a host PrefixLength; see Sec. 4.4.3.9 of [OSPFv3]. In SID6 operation of IS-IS for IPv6, host routes are to be included in the IPv6 Reachability entries, and will be handled in the same way as other IPv6 Reachability entries [ISISv6][ISISv4].

It is to be noted that SID6 of this document focuses on a single-area operation in a site. The multi-area case is left for further study.

3.5. Other Address-Related Protocols

DHCPv6 [DHCPv6] is not affected since most addresses involved there are link-local. The site-local All_DHCP_Servers multicast address in the case of Relay Agent is also intact for correct operation.

Default Address Selection [DASv6] is not affected, either. One thing to note is in regard to the scope comparison in selecting a source address for a multicast destination address; see Sec. 3.1 of [DASv6]. The scope of the node address as defined in SID6 is global as well as site. Hence, the same source node address would be selected for a multicast destination address of site scope as well as of global scope as appropriate.

No other IPv6-address related protocols are affected, to the best knowledge of the author.

3.6. Generalization

The description of SID6 so far has been based on nullifying the SID. Alternatively, the same field can be used in a way similar to Unique IPv6 Prefix Per Host [Uv6pH]. The field originally occupied by SID can be populated by random numbers to render intra-site local

prefixes. Each node in the site is then assigned a unique (global || local) prefix:

IPv6 GUA

= (node address)

= (prefix, NID)

= (global prefix, local prefix, NID)

How to use this local prefix is up to the discretion of each node. If a node is a host, it can generate a 128-bit address by use of the combined (global || local) prefix and SLAAC as described in [Uv6pH]. If a node is a router, it is in fact the border router of a child site wherein all internal nodes share the same specific unique (global || local) prefix given to the router.

If the original SID field is wide enough, it can be replaced with a tuple of multiple local sub_prefixes so that a recursive routing hierarchy could be installed within the original site:

IPv6 GUA

= (node address)

= (prefix, NID)

= (global prefix, local prefix, NID)

= (global prefix, (local prefix 1, local prefix 2, ..., local prefix N), NID)

For example, local prefix 1 could be appended to the global prefix to assign a unique (global || local 1) prefix to every node in the sub_routing_tier 1. Then within each such (virtual) node, the next local prefix could be appended to assign a unique prefix to every internal nodes in the sub_routing_tier 2, etc. This incremental building of the local routing hierarchy can recur until all local sub_prefix components are concatenated.

By now, it is apparent that the concept of 'node' in SID6 is a recursive abstraction of a network entity within a tier of the local routing hierarchy. A 'node' can really be a physical node, or it can represent a 'virtual' node which in fact forms a intra-node child site for itself. If any 'virtual' node would terminate the recursion by shifting to a physical node, it can generate a 128-bit address by use of its given unique prefix. Routes managed by routers in any

specific local routing tier n, 1 <= n <= N, are the host routes of PrefixLength which equals the length of the combined prefix up to the very tier n, (global prefix || local prefix 1 || ... || local prefix n).

Also, it is to be noted that, although SID is not there anymore, there do exist subnets. The only difference is that, with SID6, a subnet is not identified by its SID but by the NID of the Default Router (DR). DR keeps, in its Neighbor Cache, the list of intra-subnet (on-link) hosts for relaying packets in and out across the subnet boundary. There may, of course, be multiple routers associated with the same subnet, and one of them would act as DR as usual.

As a result of the described generalization, the architecture of SID6 could be summarized as follows:

- SID6 is a recursive IPv6 networking architecture wherein sites are recursively repeated inwards (and possibly also outwards).

- A site is a collection of (virtual) nodes wherein all nodes share the same prefix.

- A subset of directly connected intra-site nodes bordered by one or more router(s) is called a subnet. Thus, a site can also be defined as a collection of subnets. Each subnet is identified by the NID of DR.

- Intra-site mobility is provided by a link-state routing protocol, whereas inter-site mobility is by MIPv6 agents installed on one or more site border router(s).

4. Consequencies

4.1. Recursive Networking

As described in Section 3.6, SID6 presents a recursive IPv6 networking paradigm. By recursion, it follows that SID6 is scalable. That is, SID6 is a scalable recursive IPv6 networking paradigm.

4.2. No Locator/ID Separation

SID6 does not introduce a separate number space extra to that already existing IPv6 address space; no locator/ID separation (LIS) is pursued. Within a site, the NID identifies a node whose locality is determined through an interior link-state routing protocol. Between sites, the site prefix both identifies and locates a site.

4.3. Inherent Interior Mobility

The most important consequence of SID6 is that the node address is invariant across links as long as the node resides within a given site. Since the node address is used for transport connections, the latter do not break while nodes move around within a site. That is, intra-site node mobility is inherently provided. Locating a given node is done through a normal link-state routing protocol like OSPFv3 or IS-IS for IPv6. No extra locators are incorporated in SID6.

When a given node is a router, node mobility essentially means subnet mobility. A whole subnet, along with the router(s) and attached hosts, can move around within a site without losing reachability and transport connections. Instantaneous event-driven link-state updates will keep tight track of the moving subnet and its associated nodes.

A following consequence is that no Mobile IP protocol like MIPv6 [MIPv6] is necessary for intra-site mobile nodes. A MIPv6 client would be enabled only when a node visits a foreign site, and MIPv6 agents need be installed only on site border routers, not on every intra-site routers. This simplification may stand for a substantial resource saving in providing intra-site mobility.

4.4. Faster Interior Mobility

Now a valid question might be whether the intra-site mobility provided by link-state routing protocols should be faster or slower than that provided by MIPv6-installed intra-site routers. First of all, movement detection by a mobile node should be the same for both cases; any of link-layer indication, DR not reachable, or a new prefix heard from RA, etc.; see Sec. 11.5.1 of [MIPv6]. Differences, if any, should be with the actions taken thereafter. Typical actions by a mobile node after movement detection, in accordance with MIPv6, should be:

1. Send RS (if no RA heard)

2. Receive RA

3. Create addresses including care-of-address

4. DAD for all unicast addresses

5. Register care-of-address with Home Agent (HA)

Since the prefix acquired in Step 2 should be the same as the one already installed on the SID6 mobile node, Step 3 is to be skipped in SID6. Step 4 is not necessary, either, since uniqueness of the

NID(s) has already been guaranteed by a previous site-wide DAD before the move, in accordance with the new DAD procedure introduced in Section 3.3. Saving a DAD could be substantial since it would involve a number of message exchanges appended by possible retransmissions.

As for the last step, registering with a MIPv6 HA may consume several Binding message exchanges. In the case of SID6, the modified ND procedure described in Section 3.2 would be executed, which would then be immediately followed by DR flooding an event-driven link-state update to inform all other intra-site routers of the successful arrival of the visiting mobile node. Time lapses caused by the two schemes could be considered approximately equal.

As a result, the time saving in SID6 should be what the address creation and a DAD would consume. Thus, the intra-site mobility provided by SID6 should be faster by as much than that by MIPv6. This faster mobility would be an advantage in many disruptive applications wherein nodes might experience frequent changes in link attachment.

4.5. Legacy Exterior Mobility

Exterior mobility would be done through MIPv6 as usual. MIPv6 agents need be installed only on site border routers.

4.6. Legacy Migration and Multihoming

Renumbering at migration can be done seamlessly as usual. The site would first be multihomed on the old as well as the new upstream networks. Once all nodes are successfully renumbered and corresponding DNS records are updated, the old addresses would be removed and the site would be single-homed on the new upstream network.

If a host is multihomed on different links within a single-homed site, the node would be associated with only one node address since the prefixes would be the same for all different links. The node can be reached through any of these links. With the usual IPv6 or some LIS protocols [HIP][ILNP], each interface of the node would be given a distinct locator so that the peer node should choose between multiple locators to reach the same node, which task being either arbitrary or complicated. With SID6, however, the node is associated with a single node address so that there'd be no confusion or extra work burden on the part of the peer node.

If a host is multihomed on different sites, the node would possess multiple node addresses each derived from different site prefixes.

Each of such node addresses is used to reach the node via the corresponding site network.

If a subnet is multihomed on different sites, only the nodes within the very subnet would be given multiple node addresses each derived from prefixes of the different sites. Nodes in other subnets would not be affected.

If a site is multihomed on different upstream networks, all internal nodes, either hosts or routers, would be given multiple node addresses derived from different site prefixes assigned by different upstream networks.

4.7. Usual Use of NPTv6 and ULA

As an alternative to the approaches of migration and multihoming described in the previous subsection, use of IPv6-to-IPv6 Network Prefix Translation [NPTv6] and Unique Local Address [ULA] can also be considered as appropriate.

4.8. Incremental Deployability

SID6 can be deployed incrementally. A site can adopt SID6, yet the external behaviors exposed to DFZ remain the same as with a legacy IPv6 site and so cause no disturbance to DFZ.

4.9. Prefix Aggregation and Scalability

Prefix aggregation in DFZ is done as usual. That is, DFZ routing scalability of SID6 is as good as the legacy IPv6 networking.

4.10. Incentives for Deployment

An apparent incentive to deploy SID6 should be that transport connection resilience for intra-site mobile nodes can be provided with no extra infrastructure like mapping servers found in most LIS protocols [HIP][ILNP][LISP], resulting in a significant resource saving. An equivalent incentive in comparison with the legacy IPv6 networking would be that intra-site mobility, and that faster, can be provided inherently by any interior link-state protocols, with no hassle of installing MIPv6 functionalities on every router in a site. Considering that a site can be arbitrarily large, this can be a considerable additional resource saving in terms of network operation.

5. Conclusions

A new IPv6 networking paradigm called SID6 is introduced, wherein the IPv6 SID is deprecated, that is, set to zero or replaced by a local prefix tuple. As a result, a node is associated with a site-local NID, instead of one or more link-local IIDs as with the legacy IPv6 networking.

With SID6, the task of simultaneous identification and location of a node, wrestled with by other LIS solutions through separate (ID and locator) number spaces, is accomplished without introducing a number space extra to that already available for node addresses. Furthermore, the job is done stepwise across two adjacent tiers; intra-site and inter-site:

- Within a site (intra-site), identification is provided through the NID or the local prefix while location is through an intra-domain link-state routing protocol.

- Across sites (inter-site), identification is provided through (global) node addresses while location is by the site prefix.

With SID6, there's no need for deployment and management of the mapping servers (IDs versus locators), which should be a substantial resource saving over usual LIS solutions.

An additional advantage of SID6 is that intra-site mobility is provided inherently by a link-state protocol, and that faster and more efficiently than with MIPv6. Moreover, MIPv6 agents need be installed only on site border routers, not on every intra-site router, thus resulting in another notable resource saving.

Behaviors of a SID6 site externally exposed to DFZ remain the same as with usual legacy IPv6 sites, enabling incremental deployment.

This document has presented SID6 only for the case of a single-area routing domain. The case of a multi-area domain is for further study. Application of the equivalent idea to IPv4 networking is also left for further study.

6. Security Considerations

SID6 should be as secure or insecure as the legacy IPv6 networking. As for privacy, there are documents for hiding node locality within a site [SLAACPRIV][IIDSv6][IIDOPAQUE]. Randomizing IIDs works fine with SID6 since randomizing takes place only at node (re-)initialization once or not frequently enough [SLAACPRIV].

IID hashing is a function of not only the global routing prefix but also SID [IIDSv6][IIDOPAQUE]; when a node moves to a foreign link, a new IID would be generated to hide the locality of the node from other hosts. In SID6, the hashed NID would not change at such an intra-site move, and hence its locality would be exposed. However, this exposure is only to the routers which keep locality information of nodes in their routing tables which are opaque to hosts. Hosts have no clues which link other nodes reside in or have moved to, except for on-link nodes in Neighbor Cache. Hosts would simply rely on DRs for packet deliveries to off-link nodes. Therefore, the privacy offered by [IIDSv6][IIDOPAQUE] would be scarcely affected.

7. IANA Considerations

There are no requests to IANA at the current stage of the document.

8. References

8.1. Normative References

[DASv6] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/rfc6724, Sep. 2012, <http://www.rfc-editor.org/info/rfc6724>.

[DHCPv6] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/rfc3315, Jul. 2003, <http://www.rfc-editor.org/info/rfc3315>.

[ICMPv6] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, DOI 10.17487/rfc4443, Mar. 2006, <http://www.rfc-editor.org/info/rfc4443>.

[IIDOPAQUE] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/rfc7217, Apr. 2014, <http://www.rfc-editor.org/info/rfc7217>.

[IIDSv6] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/rfc8064, Feb. 2017, <http://www.rfc-editor.org/info/rfc8064>.

[ISISv4] Callon, R., "Use of OSI IS-IS for Routing in TCP/IP and Dual Environments", RFC 1195, DOI 10.17487/rfc1195, Dec. 1990, <http://www.rfc-editor.org/info/rfc1195>.

[ISISv6] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, DOI 10.17487/rfc5308, Oct. 2008, <http://www.rfc-editor.org/info/rfc5308>.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/rfc2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[MIPv6] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/rfc6275, Jul. 2011, <http://www.rfc-editor.org/info/rfc6275>.

[NDv6] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/rfc4861, Sep. 2007, <http://www.rfc-editor.org/info/rfc4861>.

[NPTv6] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, DOI 10.17487/rfc6296, June 2011, <http://www.rfc-editor.org/info/rfc6296>.

[OSPFv3] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, Ed., "OSPF for IPv6", RFC 5340, DOI 10.17487/rfc5340, Jul. 2008, <http://www.rfc-editor.org/info/rfc5340>.

[p2p127] Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", RFC 6164, DOI 10.17487/rfc6164, Apr. 2011, <https://tools.ietf.org/html/rfc6164>.

[SLAAC] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/rfc4862, Sep. 2007, <http://www.rfc-editor.org/info/rfc4862>.

[SLAACPRIV] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/rfc4941, Sep. 2007, <http://www.rfc-editor.org/info/rfc4941>.

[ULA] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/rfc4193, Oct. 2005, <http://www.rfc-editor.org/info/rfc4193>.

[Uv6pH] Brzozowski, J. and G. Van De Velde, "Unique IPv6 Prefix per Host", RFC 8273, DOI 10.17487/rfc8273, December 2017, <http://www.rfc-editor.org/info/rfc8273>.

[v6ADDR] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/rfc1149, Feb. 2006, <http://www.rfc-editor.org/info/rfc4291>.

[v6SUBNET] Singh, H. and W. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, DOI 10.17487/rfc5942, Jul. 2010, <http://www.rfc-editor.org/info/rfc5942>.

8.2. Informartive References

[HIP] Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, DOI 10.17487/rfc4423, May 2006, <http://www.rfc-editor.org/info/rfc4423>.

[ILNP] Atkinson , R., Bhatti, S., and U. Andrews, "ILNP Architectural Description", RFC 6740, DOI 10.17487/rfc6740, Nov. 2012, <http://www.rfc-editor.org/info/rfc6740>.

[LISP] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/rfc6830, Jan. 2013, <http://www.rfc-editor.org/info/rfc6830>.

[SID6P] Kim, YH., Kim, DY., and JW. Park, "IPv6 Networking with Subnet ID Deprecated", Journal of Computing Science and Engineering , vol. 11, no. 2, pp. 49-57, June 2017, <http://dx.doi.org/10.5626/JCSE.2017.11.2.49>.

Author's Address

DY Kim
Independent
Gangwon
South KOREA

Email: dykim6@gmail.com