JCSE Journal of Computing Science and Engineering

Regular Paper

Journal of Computing Science and Engineering,
Vol. 11, No. 2, June 2017, pp. 49-57

IPv6 Networking with Subnet ID Deprecated

Young Hee Kim
Dept. of Global ICT Cooperation, National Information Society Agency, Daegu, Korea
runa.kim@nia.or.kr

Dae Young Kim*
Independent, Gangwon, Korea
dykim6@gmail.com

Jong Won Park
Dept. of InfoCom Engineering, Chungnam National University, Daejeon, Korea
jwpark@cnu.kr

Abstract

This paper proposes a new IPv6 networking paradigm as a counter answer to the rationale for locator/identifier separation. Instead of involving separate number spaces each for node identifiers and locators, the context of the IP address as a node identifier alone is utilized and no additional locators are incorporated. That is, there are only node addresses and no locators, and location information is indirectly derived from neighbor relations between nodes. In order to accomplish this, no subnet IDs are utilized; the ID value is set to zero for all subnets. The paper details how to construct this paradigm through novel choice of operational policies in various IPv6 protocols and some trivial modifications. Especially, inherent provision of intra-domain node- as well as subnet-mobility by use of standard link-state intra-domain routing protocols is discussed. A number of important advantages of this paradigm over the canonical IPv6 networking and various known solutions of locator/identifier separation are discussed. Tailoring for multi-area domains and IPv4 is left for further study.

Category: Ubiquitous computing

Keywords: Future Internet; No subnet IDs; No locator/identifier separation

I. INTRODUCTION

In the past 15 years, the idea of locator/identifier separation (LIS) has been a hype in networking research and a number of proposals have been introduced with varying success. The motivation for this idea was through attention that a number of networking anomalies arise because the IP address which is primarily assigned to the node's interface (interface address) is also used as the node address for end-to-end transport connections. Since the interface address is coupled with the subnet identifier (ID) and so changes as a node moves across subnets, the transport connection would break at every such move of a node. Mobile nodes would suffer significantly from this frequent connection breakage unless an additional functionality like Mobile IP is incorporated. This semantic

Open Access http://dx.doi.org/10.5626/JCSE.2017.11.2.49 http://jcse.kiise.org

Received 19 February 2017; **Accepted** 14 March 2017
*Corresponding Author

 pISSN: 1976-4677 eISSN: 2093-8020

overloading (the interface address as 'where' and the node address as 'what') of the IP address was also recognized as the main reason for the Internet's incompetence in multihoming and so for the explosion of the default-free zone (DFZ) routing tables [1].

LIS solutions are based on the view that separate networking objects representing each semantics (what and where) are indispensable necessities in networking architecture, and hence all offered solutions deal with two number spaces to accommodate the overloaded semantics. HIP [2] maintains the IP address intact loaded with its locator semantics and introduces separate host-identity for use in transport connections. ILNP [3] builds on global node IDs as identifiers and subnet (or equivalently link) prefixes as locators. LISP [4] relies on usual use (as both the node address and the interface address) of the semantically-overloaded global IP address (oddly called Endpoint ID or EID) within a site, while each site is again mapped to a global IP address called Routing Locator (RLOC). In effect, LISP constructs a two-tier nested addressing by naming nodes plus associated interfaces with global IP addresses and naming a collection of nodes (called LISP sites) with another global IP address.

This paper proposes an approach drastically different from known LIS solutions in responding to the concern about the semantic overloading of the IP address. Instead of introducing a new number space to unload the equivocal semantics of the IP address, the proposed approach, called SID6 (Subnet ID Deprecated for IPv6), removes the interface semantics of the Global Unicast IPv6 address which is then to exclusively identify a node and so is to be used solely as the node address. The approach is based on the view that not both semantics are necessary in networking. That is, all that is needed is the node address, and the location information can be obtained indirectly through nodes' neighbor relations assisted by link-state routing protocols [5].

One major measure taken in SID6 for the purpose is to deprecate the subnet ID in the IP address. That is, the value of the ID is set to zero for all subnets within a routing domain. This ensures that the node address be kept invariant and thus transport connections don't break when nodes move across links (or subnets) within a domain.

A number of advantages arise with SID6. Most importantly, node- (either host- or router-) mobility is provided inherently within a routing domain. An additional functionality like Mobile IP would not be needed for intra-domain mobility and be needed only for inter-domain mobility. Multihoming of nodes, subnets, and sites are also provided more smoothly with SID6 than with the canonical IP networking or usual LIS solutions.

Following sections discuss the architectural rationale for SID6 and the construction details thereof. Consequential advantages of this new paradigm are discussed before concluding the paper.

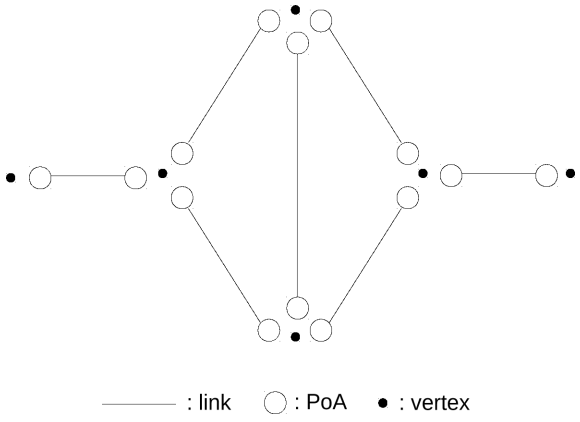

Fig. 1. Named links before nodes in place.

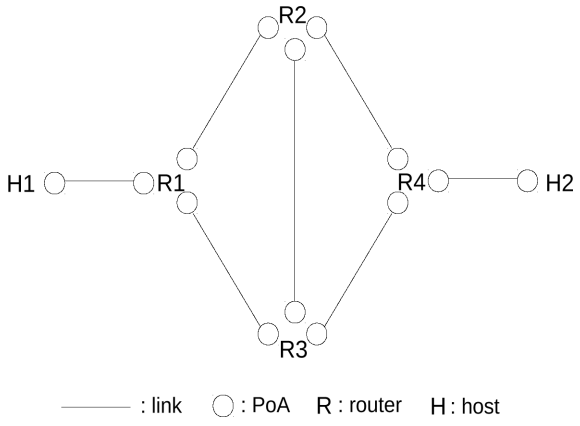

Fig. 2. Network graph with nodes in place.

II. ARCHITECTURAL RATIONALE

A. Links-First Model

Saltzer [6] states that there are four primary object types to be named in networking; services (users), nodes, attachment points (or points of attachment: PoAs), and paths (routes). Especially, an important message of his to our primary interest is that both nodes and PoAs should be named separately.

The way of thinking behind this notion might be the following:

1. Links are first-class citizens and so available before nodes come into play. Links provide PoAs (locators) as receptacles for nodes later to attach to.
2. Each node, already with an ID, attaches to one or more of these PoAs, thus further associating itself with one or more locators.

A transitional network graph in Step 1 where nodes are not yet at play may look like Fig. 1. Edges (lines) represent links and vertices (dots) the places reserved for

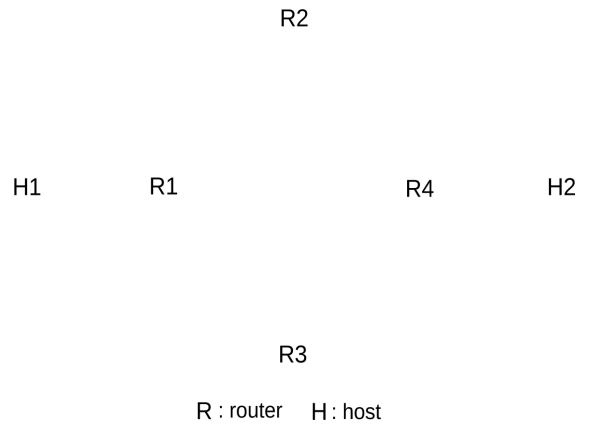

Fig. 3. Named nodes waiting to be connected.

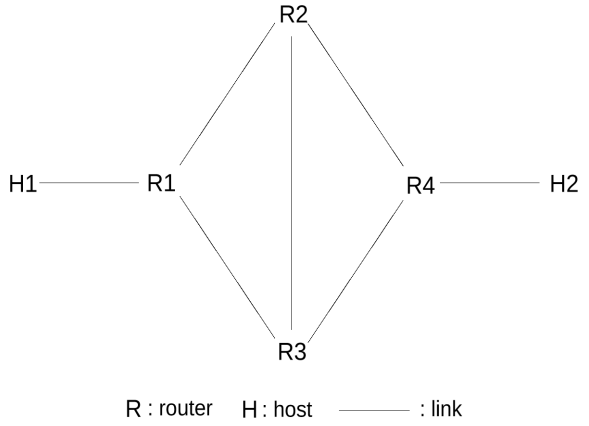

Fig. 4. Network graph with named nodes connected by unnamed links.

nodes. Each PoA, i.e., each end of a link, is then named by a locator, ready for accepting a node.

Complete it may seem, this graph is incomplete for networking. With no routers in place, to be specific, no packets can traverse the vertices. Unless vertices are filled with nodes, this is only a set of disconnected links, bearing no meaning from the perspective of networking. The links as yet are as good as nonexistent in strict view of networking.

Links will assume networking significance only when each vertex is filled (Step 2 above), like in Fig. 2, with either a relay node (router, R) or a leaf node (host, H). Note in the figure that each node, already given an ID, will additionally be associated with one or more locators. Thus, nodes are involved with two different types of names.

B. Nodes-First Model

One might ask oneself whether involving the two independent sets of names as in the previous subsection is absolutely necessary to accomplish seamless networking.

Let us take another way of thinking in building a network:

1. There are nodes first, waiting to be connected. Nodes are named with node IDs.
2. As links are secured, nodes are connected by links. Links are not named.
3. With links connecting them, neighbor nodes establish connectivity relations.
4. Collection of all neighbor relations between nodes within a region of interest completes a network graph.

The steps in this way of thinking can be illustrated by Figs. 3 and 4. Fig. 3 shows named nodes in place waiting to be connected. As links are secured, the nodes are connected to form a network graph as in Fig. 4.

Note that reaching a complete network graph of Fig. 4 involves only one type of names, i.e., node IDs. Neighbor relations of the nodes are sufficient to build a network, and names of the links or PoAs are neither involved nor necessary. This is in stark contrast to the way a network is built through a different way of thinking associated with Figs. 1 and 2 in the previous subsection.

C. Fallacy of Duplicate Naming of Attachment Points

One might wonder why the second way of building a network above is possible. An explanation might be that naming PoAs (thus effectively naming links) is not a job of the network layer and so is not necessary; the very job belongs to the underlying link layer. That is, each PoA is already named in the underlying layer by a link-layer address; for example, by a MAC address. Naming PoAs again in the network layer is simply duplicate and redundant. By doing so, the same PoAs would be named twice, once by the link layer and again by the network layer [7].

It is to be reemphasized that this duplicate naming of PoAs in the network layer is unnecessary. Involving only one name type in the network layer is enough to build a network in the layer of interest. Not an additional separate name set but a set of neighbor relations between nodes completes a network.

III. CONSTRUCTION

Construction of SID6 is based on the existing legacy IPv6 network with minimal changes. In fact, the only significant change is to deprecate the subnet ID. The rest of the changes are minimal to null, and extensive discussions would highlight how the current system works intact with these changes.

For the sake of our discussion, it is to be noted that site, (routing) domain, and Autonomous System (AS) are used interchangeably in this paper. Also, although care should be taken to differentiate subtle semantic difference between the two, subnet and link will be used interchangeably.

A. IPv6 Address

The IPv6 address type of interest is the Global Unicast address which contains the subnet ID [8]:

```
IPv6 Global Unicast address
    = (interface address)
    = (subnet prefix, interface ID)
    = (global routing prefix, subnet ID,
       interface ID)
```

The interface ID is 64 bits long [8] while, according to IAB/IESG recommendations, the subnet ID is 16 bits long [9, 10].

Now, we reset the subnet ID, and the IPv6 Global Unicast address will no longer depend on the subnet ID; it doesn't change as a node moves across subnets within a domain:

```
IPv6 Global Unicast address
    = (global routing prefix, 0x0000,
       interface ID)
```

In order to keep the global uniqueness of the address, the interface ID should be unique within a domain. That is, the scope of the interface ID is the domain of interest in contrast to its usual scope of a subnet [8]. Duplicate Address Detection (DAD) would be affected through this new constraint. See Section III-C for more discussion.

For the sake of SID6 description, we take the interface ID as the node ID. When a node has multiple interfaces, there would be multiple interface IDs associated. In that case, we pick the interface ID of the smallest value and take it as the node ID. The result is:

```
IPv6 Global Unicast address
    = (node address)
    = (subnet prefix, node ID)
    = (global routing prefix, 0x0000,
       node ID)
```

The node ID is unique for the node and invariant within a site or routing domain. The address is now a node address, not an interface address.

When a site is multi-homed on multiple Internet Service Providers (ISPs), it would be associated with multiple global routing prefixes and hence every intra-site node would be associated with multiple addresses. For seamless site-multihoming of such an instance, nodes should be able to receive inbound packets destined to any of such multiple addresses, and also be able to source outbound packets with one of such multiple addresses as appropriate.

Remember all we did here is to reset the subnet ID. And that, this is not any change in the definition of the IPv6 address format, but is just an operational choice. All others are natural corollary consequences with no enforcement of any significant artificial policies; the mechanism remains the same. We will subsequently see how other parts of the IPv6 networking continue to work correctly as usual with either some changes or no further substantial manipulation.

B. Neighbor Discovery

Addresses involved in ICMPv6-derived [11] messages of Neighbor Discovery (ND) for IPv6 [12] 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), and both are agnostic to subnet ID. Otherwise, the involved addresses are unicast or anycast addresses not anymore dependent on subnet ID as prescribed in SID6.

As defined above, the subnet prefixes (global routing prefix + 0x0000) advertised by all routers within a domain are the same. Although substantially simplifying router configuration in regard to prefix loading, this necessitates the change in on-link determination. The original ND [12] specifies that a node considers an address to be on-link (reachable on the same 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 [13].

Criterion 2 should continue to be valid in SID6. However, Criterion 1 is of no more use since all prefixes are the same and hence the on-link flag loses its semantics. To be exact, the subnet prefix is not just link-local but rather site-local. Since on-link information cannot be obtained through prefixes provided by a pair procedure of Router Solicitation (RS) and Router Advertisement (RA), some other means has to be secured for on-link determination. For this purpose, we propose to add the following procedure to the ND protocol:

- When a node is first injected into a domain and attaches to a link, it might acquire prefix information through a pair of RS and RA, and auto-configure itself with a node address sanitary-checked through Duplicate Address Detection (DAD) described in the following subsection. 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 the link-layer

address shall also be included in 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 [12] times. The first NA should be issued after a random delay between 0 and MAX_RTR_SOLICITATION_DELAY [12] 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 determines the forward reachability from the new node's perspective; the responding address is on-link. The new node creates an entry for the responding address in Neighbor Cache. 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 determines reachability from the responding node's perspective; the address of the new node is on-link. The responding node then creates an entry for the new node's address in its own Neighbor Cache.
- All addresses in Neighbor Cache of a node are considered to be on-link.

This new procedure differs from the existing ND procedure in that on-link determination is made not through Prefix List (for addresses with on-link flag set) but through Neighbor Cache. The role of Prefix List reduces simply to providing the global routing 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 the 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.

C. 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 [14]. 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 [8]:

```
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 address (unicast or anycast) 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 [14], 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 Section 5.4 of SLAAC indicate the presence of a duplicate address within RetransTimer milliseconds after having sent DupAddrDetectTransmits DSs [14]. A side effect of this site-wide DAD is that uniqueness of the node ID(s) is confirmed site-wide.

D. Interior Gateway Protocols

A link-state Interior Gateway Protocols (IGP) is to be used in SID6; OSPFv3 [15] or IS-IS for IPv6 [16, 17]. 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 (full IPv6 node addresses) 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 128 (host PrefixLength); see Section 4.4.3.9 of [15]. 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 manner as other IPv6 Reachability entries [16, 17].

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.

E. Other Address-Related Protocols

DHCPv6 [18] 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 [19] is not affected, either. One thing to note is in regard to scope comparison in selecting a source address for a multicast destination address; see Section 3.1 of [19]. 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 authors.

IV. CONSEQUENCES AND BENEFITS

A. No Locator/ID Separation

SID6 does not introduce a separate number space extra to that already existing IPv6 address space; no locator/ID separation is pursued. Within a site, the node ID identifies a node whose location is done through an intra-domain link-state routing protocol. Between sites, the global routing prefix both identifies and locates a site. In fact, SID6 is an instance of recursive addressing as explored in NARA [5].

B. Inherent Intra-Domain 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 (reachability) is done through a normal link-state routing protocol like OSPFv3 or IS-IS for IPv6. No extra locators are necessary in SID6.

When a given node is a router, node mobility essentially means (sub-)network mobility. A whole subnet, along with the router 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 nodes.

A following consequence is that no Mobile IP protocol like MIPv6 [20] is necessary for intra-site mobile nodes. A MIPv6 client would be enabled only when a node visits a foreign site, and MIPv6 Home Agent (HA) needs to be installed only on AS border routers, not on every intra-site router. This simplification may stand for substantial resource saving in providing intra-domain mobility.

C. Faster Intra-Domain Mobility

Now a valid question might be whether intra-domain 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, Default Router (DR) not reachable, or a new prefix heard from RA, etc.; see Section 11.5.1 of MIPv6 [20]. 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 to acquire prefix
3. Select DR
4. Create addresses including care-of-address
5. DAD for all unicast addresses
6. Register care-of-address with HA

Since the prefix acquired in Step 2 should be the same as the one already installed on the SID6 mobile node, Step 4 is to be skipped in SID6. Step 5 is not necessary, either, since uniqueness of the node ID(s) has already been guaranteed by previous site-wide DAD in accordance with the new DAD procedure introduced in Section III-C. Saving DAD could be substantial since it would involve a number of message exchanges appended by possible retransmissions.

As for the last step, registering with HA may consume several Binding message exchanges. In the case of SID6, the mobile node would multicast an unsolicited NA to inform all nodes (including routers) on the newly visited link of its emergence. This would then be immediately followed by DR flooding an event-driven area-scoped link-state updates to inform all other intra-domain routers of the arrival of the visiting mobile node. Time lapses caused by the two schemes could be considered approximately equal.

As a result, time saving in SID6 should be what address creation and DAD would consume. Thus, intra-domain mobility provided by SID6 should be faster than MIPv6 by as much. This faster mobility would be a notable advantage in those Internet-of-Things applications where nodes would experience frequent changes in subnet attachment.

D. Seamless Multihoming

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 different links. With the usual IPv6 or some LIS protocols, 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 could be 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 global routing prefixes assigned by different upstream ISPs. Each of such node addresses is used to reach the node via the corresponding upstream ISP 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 assigned by different upstream ISPs. Nodes in other subnets would not be affected.

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

E. Legacy Renumbering

Renumbering can be done seamlessly as usual. The site would first be multihomed on the old as well as the new ISP. 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 ISP.

F. Legacy Inter-Domain Mobility

Inter-domain mobility would be done through MIPv6 as usual. HAs need be installed only on AS border routers.

G. Prefix Aggregation and Scalability

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

H. Incremental Deployability

SID6 can be deployed incrementally. A site can adopt SID6, yet the external behavior of the site remains the same as a legacy IPv6 site.

I. Incentive for Deployment

The obvious incentive to deploy SID6 should be that transport connection resilience can be provided with no extra infrastructure like mapping servers found in most LIS protocols [2-4], resulting in significant resource saving. In addition, intra-domain mobility, and that faster, can be provided inherently by any intra-domain link-state protocols, with no hassle of installing MIPv6 functionality on every router in a site. Considering that a site can be arbitrarily large, this can be considerable additional resource saving in terms of network operation.

J. Security Considerations

SID6 should be as secure or insecure as the legacy IPv6 networking. As for privacy, there are proposals to hide node locality within a site [21-23]. Randomizing interface IDs works fine with SID6 since randomizing takes place only at node (re-)initialization once or not frequently enough [21].

Interface ID hashing is a function of not only routing prefix but also subnet ID [22, 23]; when a node moves to a foreign link, a new interface ID would be generated to hide the locality of the node from other hosts. In SID6, the hashed interface ID (thus node ID) would not change at such an intra-site move, and hence its locality would be exposed. However, this exposure is only to routers which keep locality information of nodes in their routing tables opaque to hosts. Hosts have no clue on which link other nodes reside 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 [22, 23] would be scarcely affected.

V. CONCLUSIONS

A new IPv6 networking paradigm called SID6 is introduced, wherein the IPv6 subnet ID is deprecated, that is, set to zero. With such deprecation, interface IDs are site-local in SID6 in contrast to the legacy IPv6 networking wherein they are link-local. While the interface ID is used as the SID6 node ID for a node with a single interface, the interface ID of the minimum value is used as the node ID for a node with multiple interfaces.

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 in two tiers; intra-site and inter-site:

- Within a site (intra-domain), node identification is provided through node IDs (or equivalently node addresses) while location is through an intra-domain link-state routing protocol.
- Across sites (inter-domain), identification is provided through (global) node addresses while location is by the global routing prefix.

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

An additional advantage of SID6 is that intra-domain mobility is provided inherently by a link-state protocol,

and that faster and more efficiently than with MIPv6. Moreover, HA need be installed only on site border routers, not on every intra-site router, thus resulting in another notable resource saving.

SID6 is presented only for the case of a single-area routing domain in this paper. 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.

ACKNOWLEDGEMENTS

This work was supported by research fund of Chungnam National University.

REFERENCES

1. D. Meyer, L. Zhang, and K. Fall, "Report from the IAB Workshop on routing and addressing," The Internet Engineering Task Force, RFC 4984, 2007.
2. R. Moskowitz and P. Nikander, "Host identity protocol (HIP) architecture," The Internet Engineering Task Force, RFC 4423, 2006.
3. R. J. Atkinson, S. N. Bhatti, and U. St. Andrews, "Identifier-locator network protocol (ILNP) architectural description," The Internet Engineering Task Force, RFC 6740, 2012.
4. D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "The locator/ID separation protocol (LISP)," The Internet Engineering Task Force, RFC 6830, 2013.
5. Y. H. Kim and D. Y. Kim, "NARA: Network Architecture with Recursive Addressing," *Telecommunications Review*, vol. 25, no. 2, pp. 261-273, 2015.
6. J. H. Saltzer, "On the naming and binding of network destinations," The Internet Engineering Task Force, RFC 1498, 1993.
7. J. D. Day, *Patterns in Network Architecture: A Return to Fundamentals*, Boston, MA: Prentice Hall, 2008.
8. R. Hinden and S. Deering, "IP version 6 addressing architecture," The Internet Engineering Task Force, RFC 4291, 2006.
9. R. Hinden, S. Deering, and E. Nordmark, "IPv6 global unicast address format," The Internet Engineering Task Force, RFC 3587, 2003.
10. IAB/IESG, "IAB/IESG Recommendations on IPv6 address allocations to sites," The Internet Engineering Task Force, RFC 3177, 2001.
11. A. Conta, S. Deering, and M. Gupta, "Internet control message protocol (ICMPv6) for the internet protocol version 6 (ipv6) specification," The Internet Engineering Task Force, RFC 4443, 2006.
12. T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor discovery for IP version 6 (IPv6)," The Internet Engineering Task Force, RFC 4861, 2007.
13. H. Singh, W. Beebee, and E. Nordmark, "IPv6 subnet model: the relationship between links and subnet prefixes," The Internet Engineering Task Force, RFC 5942, 2010.
14. S. Thomson, T. Narten, and T. Jinmei, "IPv6 stateless address autoconfiguration," The Internet Engineering Task Force, RFC 4862, 2007.
15. R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," The Internet Engineering Task Force, RFC 5340, 2008.
16. C. Hopps, "Routing IPv6 with IS-IS," The Internet Engineering Task Force, RFC 5308, 2008.
17. R. Callon, "Use of OSI IS-IS for routing in TCP/IP and dual environments," The Internet Engineering Task Force, RFC 1195, 1990.
18. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic host configuration protocol for IPv6 (DHCPv6)," The Internet Engineering Task Force, RFC 3315, 2003.
19. D. Thaler, R. Draves, A. Matsumoto, and T. Chown, "Default address selection for internet protocol version 6 (IPv6)," The Internet Engineering Task Force, RFC 6724, 2012.
20. D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," The Internet Engineering Task Force, RFC 6275, 2011.
21. T. Narten, R. Draves, and S. Krishnan, "Privacy extensions for stateless address autoconfiguration in IPv6," The Internet Engineering Task Force, RFC 4941, 2007.
22. F. Gont, A. Cooper, D. Thaler, and W. Liu, "Recommendation on stable IPv6 interface identifiers," The Internet Engineering Task Force, RFC 8064, 2017.
23. F. Gont, "A method for generating semantically opaque interface identifiers with IPv6 stateless address autoconfiguration (SLAAC)," The Internet Engineering Task Force, RFC 7217, 2014.

Young Hee Kim

Young Hee Kim received the B.S. and M.S. degrees in information communications engineering from Chungnam National University (CNU), Korea, in 1997 and 1999, respectively. She was a senior member of research staff in Electronics and Telecommunications Research Institute (ETRI) from 1999 to 2003. Since 2003, she has worked for National Information Society (NIA), Korea, and is now director of the E-Government Global Cooperation Team. Her works at NIA have been management of high-speed national testbed networks, pilot projects for national ICT policy, and e-Government. Her research interests are in Future Internet and quality of service for communication networks.

Dae Young Kim

Dae Young Kim received the B.S. degree from Seoul National University, Korea, in 1975, and the M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Korea, in 1977, and 1983, respectively. He joined CNU in 1983, and retired as professor in the Dept. of Information Communications Engineering in 2015. In addition to academic achievements including more than 250 technical papers, he has been active in research network communities and international standardization; he was chair of Asia-Pacific Advanced Network (APAN) and chair of ISO/IEC JTC 1/SC 6. His research interest is in Future Internet.

Jong Won Park

Jong Won Park received the B.E. degree in electronics engineering from CNU, Korea, in 1979. He received the M.S. and Ph.D. degrees in computer science from KAIST, in 1981 and 1991, respectively. From 1981 to 1993, he was with the Dept. of Computer Science at CNU. In 1992, he was a visiting associate professor at the Dept. of Electrical Engineering, University of Texas at Dallas. Since 1994, he has been with the Dept. of Information Communications Engineering at CNU. His main research interests include parallel memory system and SIMD computer architecture for image processing, and medical image processing. He is a senior member of the IEEE Computer Society. He is also an essayist and a literary critic of Korea.