IPWAVE Working Group J. Jeong
Internet-Draft Y. Shen
Intended status: Standards Track Z. Xiang
Expires: September 12, 2019 Sungkyunkwan University
March 11, 2019

IPv6 Neighbor Discovery for IP-Based Vehicular Networks
draft-jeong-ipwave-vehicular-neighbor-discovery-06

Abstract

This document specifies a Vehicular Neighbor Discovery (VND) as an extension of IPv6 Neighbor Discovery (ND) for IP-based vehicular networks. An optimized Address Registration and a multihop Duplicate Address Detection (DAD) mechanism are performed for having operation efficiency and also saving both wireless bandwidth and vehicle energy. Also, three new ND options for prefix discovery, service discovery, and mobility information report are defined to announce the network prefixes and services inside a vehicle (i.e., a vehicle's internal network). Finally, a mobility management scheme is proposed for moving vehicles in vehicular environments to support seamless communication for the continuity of transport-layer sessions (e.g., TCP connections).

Table of Contents

1. Introduction

Vehicular Ad Hoc Networks (VANET) have been researched for Intelligent Transportation System (ITS) such as driving safety, efficient driving and entertainment. Considering the high-speed mobility of vehicular network based on Dedicated Short-Range Communications (DSRC), IEEE 802.11p [IEEE-802.11p] has been specialized and was renamed IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012. IEEE has standardized Wireless Access in Vehicular Environments (WAVE) [DSRC-WAVE] standard which is considered as a key component in ITS. The IEEE 1609 standards such as IEEE 1609.0 [WAVE-1609.0], 1609.2 [WAVE-1609.2], 1609.3 [WAVE-1609.3], 1609.4 [WAVE-1609.4] provide a low-latency and alternative network for vehicular communications. What is more, IP-based vehicular networks specialized as IP Wireless Access in Vehicular Environments (IPWAVE) [IPWAVE-PS] can enable many use cases over vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications.

VANET features high mobility dynamics, asymmetric and lossy connections, and moderate power constraint (e.g., electric cars and unmanned aerial vehicles). Links among hosts and routers in VANET can be considered as undetermined connectivities with constantly changing neighbors described in [RFC5889]. IPv6 [RFC8200] is selected as the network-layer protocol for Internet applications by IEEE 1609.0 and 1609.3. However, the relatively long-time Neighbor Discovery (ND) process in IPv6 [RFC4861] is not suitable in VANET scenarios.

To support the interaction between vehicles or between vehicles and Rode-Side Units (RSUs), this document specifies a Vehicular Neighbor Discovery (VND) as an extension of IPv6 ND for IP-based vehicular networks. VND provides vehicles with an optimized Address Registration, a multihop Duplicate Address Detection (DAD), and an efficient mobility management scheme to support efficient V2V, V2I, and V2X communications.

2. Requirements Language

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 RFC 2119 [RFC2119].

3. Terminology

This document uses the terminology described in [RFC4861], [RFC4862], and [RFC6775]. In addition, the following new terms are defined as below:

- WAVE: Acronym for "Wireless Access in Vehicular Environments" [WAVE-1609.0].

- Road-Side Unit (RSU): A node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, LTE-V2X, etc.) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in car parking area.

- On-Board Unit (OBU): A node that has a DSRC device for wireless communications with other OBUs and RSUs, and may be connected to in-vehicle devices or networks. An OBU is mounted on a vehicle. It is assumed that a radio navigation receiver (e.g., Global Positioning System (GPS)) is included in a vehicle with an OBU for efficient navigation.

- Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support the address autoconfiguration and mobility management of them. It has end-to-end connections with RSUs under its control. It maintains a DAD table having the IP addresses of the vehicles moving within the communication coverage of its RSUs.

- Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network nodes.

- Traffic Control Center (TCC): A node that maintains road infrastructure information (e.g., RSUs, traffic signals, and loop detectors), vehicular traffic statistics (e.g., average vehicle speed and vehicle inter-arrival time per road segment), and vehicle information (e.g., a vehicle's identifier, position, direction, speed, and trajectory as a navigation path). TCC is included in a vehicular cloud for vehicular networks and has MAs under its management.

4. Overview

This document proposes an optimized ND with a more adaptive structure for vehicular networks considering fast vehicle mobility and wireless control traffic overhead related to the legacy ND. Further more, prefix and service discovery can be implemented as part of the ND's process along with an efficient Address Registration procedure and DAD mechanism for moving vehicles. This document specifies a set of behaviors between vehicles and RSUs to accomplish these goals.

4.1. Link Model

There is a relationship between a link and a network prefix along with reachability scopes, such as link-local and global scopes. The legacy IPv6 ND protocol [RFC4861] has the following link model. All IPv6 nodes in the same on-link subnet, which use the same subnet prefix with on-link bit set, are reachable with each other by one-hop link. The symmetry of the connectivity among the nodes is preserved, that is, bidirectional connectivity among two on-link nodes. However, a link model in vehicular networks (called vehicular link model) should consider the asymmetry of the connectivity that unidirectional links can exist due to interference in wireless channels and the different levels of transmission power in wireless network interfaces.

The on-link subnet can be constructed by one link (as a basic service set) or multiple links (as an extended service set) called a multi-link subnet [RFC6775]. In the legacy multi-link subnet, an all-node-multicasted packet is copied and related to other links by an ND proxy. On the other hand, in vehicular networks having fast moving vehicles, multiple links can share the same subnet prefix for operation efficiency. For example, if two wireless links under two adjacent RSUs are in the same subnet, a vehicle as an IPv6 host does not need to reconfigure its IPv6 address during handover between those RSUs. However, the packet relay by an RSU as an ND proxy is not required because such a relay can cause a broadcast storm in the extended subnet. Thus, in the multi-link subnet, all-node-multicasting needs to be well-calibrated to either being confined to multicasting in the current link or being disseminated to other links in the same subnet.

In a connected multihop VANET, for the efficient communication, vehicles in the same link of an RSU can communicate directly with each other, not through the serving RSU. This direct wireless communication is similar to the direct wired communication in an on-link subnet using Ethernet as a wired network. The vehicular link model needs to accommodate both the ad-hoc communication between vehicles and infrastructure communication between a vehicle and an RSU in an efficient and flexible way. Therefore, the IPv6 ND should be extended to accommodate the concept of a new IPv6 link model in vehicular networks.

To support multi-link subnet, this specification employs the Shared-Prefix model for prefix assignments. Shared-Prefix model refer to an addressing model where the prefix(es) are shared by more than one node. In this document, we assume that in a specified subnet, all interfaces of RSUs responding for prefix assignments to vehicles hold

same prefix, which ensure vehicles obtain and maintain same prefix in this subnet scope.

4.2. ND Optimization

This document takes advantage of the optimized ND for Low-Power Wireless Personal Area Network (6LoWPAN) [RFC6775] because vehicular environments have common parts with 6LoWPAN, such as the reduction of unnecessary wireless traffic by multicasting and the energy saving in battery. Note that vehicles tend to be electric vehicles whose energy source is from their battery.

In the optimized IPv6 ND for 6LoWPAN, the connections among nodes are assumed to be asymmetric and unidirectional because of changing radio environment and loss signal. The authors proposed an improved IPv6 ND which greatly eliminates link-scope multicast to save energy by constructing new options and a new scheme for address configurations. Similarly, this document proposes an improved IPv6 ND by eliminating many link-scope-multicast-based ND operations, such as DAD for IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. Thus, this document suggests an extension of IPv6 ND as vehicular ND tailored for vehicular networks along with new ND options (e.g., prefix discovery, service discovery, and mobility information options).

4.3. Design Goals

The vehicular ND in this document has the following design goals:

o To perform prefix and service discovery through ND procedure;

o To implement host-initiated refresh of Router Advertisement (RA) and remove the necessity for routers to use periodic or unsolicited multicast RA to find hosts;

o To replace Neighbor Unreachable Detection(NUD), create Neighbor Cache Entries (NCE) for all registered vehicles in RSUs and MA by appending Address Registration Option (ARO) in Neighbor Solicitation (NS), Neighbor Advertisement (NA) messages;

o To support a multihop DAD with two new ICMPv6 messages called Duplicate Address Request(DAR) and Duplicate Address Confirmation(DAC) to eliminate multicast storm and save energy;

o To support multi-hop communication for vehicles outside the coverage of RSUs to communicate with the serving RSU via a relay neighbor; and

- o To provide a mobility management mechanism for seamless communication during a vehicle's travel in subnets via RSUs.

5. Vehicular Network Architecture

This section describes a vehicular network architecture for V2V and V2I communication. A vehicle and an RSU have their internal networks including in-vehicle devices or servers, respectively.

5.1. Vehicular Network

A vehicular network architecture for V2I and V2V is illustrated in Figure 1. Three RSUs are deployed along roadside and are connected to an MA through wired links. There are two subnets such as Subnet1 and Subnet2. The wireless links of RSU1 and RSU2 belong to the same subnet named Subnet1, but the wireless link of RSU3 belongs to another subnet named Subnet2. Vehicle2 is wirelessly connected to RSU1 while Vehicle3 and Vehicle4 are connected to RSU2 and RSU3, respectively. Vehicles can directly communicate with each other through V2V connection (e.g., Vehicle1 and Vehicle2) to share driving information. In addition, vehicles not in range of any RSU may connect with RSU in multi-hop connection via relay vehicle (e.g., Vehicle1 can contact RSU1 via Vehicle2). Vehicles are assumed to start the connection to an RSU when they entered the coverage of the RSU.

The document recommends a multi-link subnet involving multiple RSUs as shown in Figure 1. This recommendation aims at the reduction of the frequency with which vehicles have to change their IP address during handover between two adjacent RSUs. To construct this multi-link subnet, shared-prefix model is proposed. That is, for RSUs in the same subnet, the interfaces responsible for prefix assignment for vehicles should hold the same prefix in their global address. This also promises vehicles achieve same prefix in this scope. When they pass through RSUs in the same subnet, vehicles do not need to perform the Address Registration and DAD again because they can use their current IP address in the wireless coverage of the next RSU. Moreover, this proposal accord with the assumption that noes belonging to the same IP prefix are able to communicate with each other directly. On the other hand, if vehicles enter the wireless coverage of an RSU belonging to another subnet with a different prefix, they repeat the Address Registration and DAD procedure to update their IP address with the new prefix.

```
                        Traffic Control Center in Vehicular Cloud
                       *-----------------------------------------*
                      *                                           *
                     *             +----------------+              *
                    *              | Mobility Anchor|               *
                    *              +----------------+               *
                     *                      ^                      *
                      *                     |                     *
                       *--------------------v--------------------*
                       ^               ^                        ^
                       |               |                        |
                       |               |                        |
                       v               v                        v
                  +--------+ ethernet +--------+            +--------+
                  |  RSU1  |<-------->|  RSU2  |<---------->|  RSU3  |
                  +--------+          +--------+            +--------+
                     ^                     ^                    ^
                     :                     :                    :
              +--------------------------------------+ +------------------+
              |      : V2I             V2I :         | |    V2I :         |
              |      v                     v         | |        v         |
+--------+    |   +--------+          +--------+     | |    +--------+    |
|Vehicle1|=======>|Vehicle2|=========>|Vehicle3|====>| |    |Vehicle4|===>|
|        |<......>|        |<........>|        |     | |    |        |    |
+--------+   V2V  +--------+    V2V   +--------+     | |    +--------+    |
              |                                      | |                  |
              +--------------------------------------+ +------------------+
                      Subnet1                              Subnet2

            <----> Wired Link   <....> Wireless Link   ===> Moving Direction
```

Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

In Figure 1, RSU1 and RSU2 are deployed in a multi-link subnet with the same prefix address in their interfaces responding for connection with vehicles. When vehicle2 leaves the coverage of RSU1 and enters RSU2, it maintains its address configuration and ignores Address Registration and DAD steps. If vehicle2 moves into the coverage of RSU3, since RSU3 belongs to another subnet and holds a different prefix from RSU1 and RSU2, so vehicle2 must do Address Registration and DAD just as connecting to a new RSU. Note that vehicles and RSUs have their internal networks including in-vehicle devices and servers, respectively. The structures of the internal networks are described in [IPWAVE-PS].

5.2. V2I Internetworking

This subsection explains V2I internteworking between vehicle network and RSU network where vehicle network is an internal network in a vehicle, and RSU network is an internal network in an RSU, as shown in Figure 2.

```
                                                   +-----------------+
                          (*)<........>(*)  +----->| Vehicular Cloud |
       2001:DB8:1:1::/64 |             |   |       +-----------------+
+-------------------------------+  +----------------------------------+
|                        v      |  |   v   v                          |
| +-------+ +------+ +-------+ |  | +-------+ +------+ +-------+     |
| | Host1 | |RDNSS1| |Router1| |  | |Router3| |RDNSS2| | Host3 |     |
| +-------+ +------+ +-------+ |  | +-------+ +------+ +-------+     |
|     ^        ^         ^      |  |     ^         ^        ^         |
|     |        |         |      |  |     |         |        |         |
|     v        v         v      |  |     v         v        v         |
| ---------------------------- |  | ------------------------------  |
| 2001:DB8:10:1::/64 ^         |  |     ^ 2001:DB8:20:1::/64         |
|                    |          |  |     |                            |
|                    v          |  |     v                            |
| +-------+      +-------+      |  | +-------+ +-------+   +-------+ |
| | Host2 |      |Router2|      |  | |Router4| |Server1|...|ServerN| |
| +-------+      +-------+      |  | +-------+ +-------+   +-------+ |
|     ^              ^          |  |     ^         ^           ^      |
|     |              |          |  |     |         |           |      |
|     v              v          |  |     v         v           v      |
| ---------------------------- |  | ------------------------------  |
|      2001:DB8:10:2::/64      |  |       2001:DB8:20:2::/64         |
+-------------------------------+  +----------------------------------+
   Vehicle1 (Moving Network1)            RSU1 (Fixed Network1)

   <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 2: Internetworking between Vehicle Network and RSU Network

Figure 2 shows the V2I networking of a vehicle and an RSU whose internal networks are Moving Network1 and Fixed Network1, respectively. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). RSU1 has the DNS Server (RDNSS3), one host (Host5), the two routers (Router5 and Router6).

It is assumed that RSU1 has a collection of servers (Server1 to ServerN) for various services in the road networks, such as road emergency notification and navigation services. Vehicle1's Router1 and RSU1's Router3 use 2001:DB8:1:1::/64 for an external link (e.g.,

DSRC) for I2V networking for various vehicular services. The vehicular applications, such as road emergency notification and navigation services, can be registered into the DNS Server (i.e., RDNSS) through DNSNA protocol in [ID-DNSNA] along with IPv6 ND DNS options in [RFC8106].

Vehicle1's Router1 and RSU1's Router5 can know what vehicular applications exist in their internal network by referring to their own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know what network prefixes exist in their internal network through an intra-domain routing protocoli, such as OSFP. Each vehicle and each RSU announce their network prefixes and services through ND options defined in Section 6.

5.3. V2V Internetworking

This subsection explains V2V internteworking between vehicle networks, which are internal networks in vehicles, as shown in Figure 3.

```
                           (*)<..........>(*)
          2001:DB8:1:1::/64 |              |
   +------------------------------+  +------------------------------+
   |                        v     |  |     v                        |
   | +-------+ +------+ +-------+ |  | +-------+ +------+ +-------+ |
   | | Host1 | |RDNSS1| |Router1| |  | |Router5| |RDNSS3| | Host4 | |
   | +-------+ +------+ +-------+ |  | +-------+ +------+ +-------+ |
   |     ^        ^         ^     |  |     ^         ^        ^     |
   |     |        |         |     |  |     |         |        |     |
   |     v        v         v     |  |     v         v        v     |
   | ---------------------------- |  | ---------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |         ^ 2001:DB8:30:1::/64 |
   |                    |         |  |         |                    |
   |                    v         |  |         v                    |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   | | Host2 |      |Router2|     |  |     |Router6|      | Host5 | |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   |     ^              ^         |  |         ^              ^     |
   |     |              |         |  |         |              |     |
   |     v              v         |  |         v              v     |
   | ---------------------------- |  | ---------------------------- |
   |      2001:DB8:10:2::/64      |  |       2001:DB8:30:2::/64     |
   +------------------------------+  +------------------------------+
      Vehicle1 (Moving Network1)        Vehicle2 (Moving Network2)

      <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 3: Internetworking between Vehicle Networks

Figure 3 shows the V2V networking of two vehicles whose internal networks are Moving Network1 and Moving Network2, respectively. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). Vehicle2 has the DNS Server (RDNSS2), the two hosts (Host3 and Host4), and the two routers (Router3 and Router4).

It is assumed that Host1 and Host3 are running a Cooperative Adaptive Cruise Control (C-ACC) program for physical collision avoidance. Also, it is assumed that Host2 and Host4 are running a Cooperative On-board Camera Sharing (C-OCS) program for sharing road hazards or obstacles to avoid road accidents. Vehicle1's Router1 and Vehicle2's Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking for various vehicular services. The vehicular applications, such as C-ACC and C-BCS, can be registered into the DNS Server (i.e., RDNSS) through DNSNA protocol in [ID-DNSNA] along with IPv6 ND DNS options in [RFC8106].

Vehicle1's Router1 and Vehicle2's Router3 can know what vehicular applications exist in their internal network by referring to their own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know what network prefixes exist in their internal network through an intra-domain routing protocoli, such as OSFP. Each vehicle announces its network prefixes and services through ND options defined in Section 6.

6. ND Extension for Prefix and Service Discovery

This section specifies an IPv6 ND extension for vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) networking. This section also defines three new ND options for prefix discovery, service discovery, and mobility information report: (i) Vehicular Prefix Information (VPI) option, (ii) Vehicular Service Information (VSI) option, and (iii) Vehicular Mobility Information (VMI) option. It also describes the procedure of the ND protocol with those options.

6.1. Vehicular Prefix Information Option

The VPI option contains IPv6 prefix information in the internal network. Figure 4 shows the format of the VPI option.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     | Prefix Length |   Distance    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                            Reserved                           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    :                             Prefix                            :
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: Vehicular Prefix Information (VPI) Option Format

Fields:

Type — 8-bit identifier of the VPI option type as assigned by the IANA: TBD

Length — 8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The value is 3.

Prefix Length — 8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Distance — 8-bit unsigned integer. The distance between the subnet announcing this prefix and the subnet corresponding to this prefix in terms of the number of hops.

Reserved — This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Prefix — An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

6.2. Vehicular Service Information Option

The VSI option contains vehicular service information in the internal network. Figure 5 shows the format of the VSI option.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |     Length    |           Reserved1           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Protocol    |   Reserved2   |          Port Number          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    :                          Node Address                         :
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: Vehicular Service Information (VSI) Option Format

Fields:

Type — 8-bit identifier of the VSI option type as assigned by the IANA: TBD

Length — 8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The value is 3.

Reserved1 — This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Protocol — 8-bit unsigned integer to indicate the upper-layer protocol, such as transport-layer protocol (e.g., TCP, UDP, and SCTP).

Reserved2 — This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Port Number — 16-bit unsigned integer to indicate the port number for the protocol.

Service Address — 128-bit IPv6 address of a node proving this vehicular service.

6.3. Vehicular Mobility Information Option

The VMI option contains one vehicular mobility information of a vehicle or an RSU. Figure 6 shows the format of the VMI option.

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |     Type      |     Length    |           Reserved1           |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                           Reserved2                           |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     :                      Mobility Information                     :
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: Vehicular Mobility Information (VMI) Option Format

Fields:

Type — 8-bit identifier of the VMI option type as assigned by the IANA: TBD

Length — 8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The value is 3.

Reserved1 — This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Reserved2 — This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Mobility Information — 128-bit mobility information, such as position, speed, and direction.

6.4. Vehicular Neighbor Discovery

Prefix discovery enables hosts (e.g., vehicles and in-vehicle devices) to distinguish destinations on the same link from those only reachable via RSUs. A vehicle (or its in-vehicle devices) can directly communicate with on-link vehicles (or their in-vehicle devices) without the relay of an RSU, but through V2V communications along with VPI ND option. This VPI option contains IPv6 prefixes in a vehicle's internal network.

Vehicles announce services in their internal networks to other vehicles through an VSI ND option. The VSI option contains a list of vehicular services in a vehicle's or an RSU's internal network.

A vehicle periodically announces an NS message containing VPI and VSI options with its prefixes and services in all-nodes multicast address to reach all neighboring nodes. When it receives this NS message, another neighboring node responds to this NS message by sending an NA message containing the VPI and VSI options with its prefixes and services via unicast towards the NS-originating node.

Therefore, prefix and service discovery can be achieved via ND messages (e.g., NS and NA) by vehicular ND with VPI and VSI options. This VND-based discovery eliminates an additional prefix and service discovery scheme, such as DNS-based Service Discovery [RFC6763] (e.g., Multicast DNS (mDNS) [RFC6762] and DNSNA [ID-DNSNA]), other than ND. That is, vehicles and RSUs can rapidly discover the network prefixes and services of the other party without any additional service discovery protocol.

6.5. Message Exchange Procedure for V2I Networking

This subsection explains a message exchange procedure for vehicular neighbor discovery in V2I networking, where a vehicle communicates with its correponding node in the Internet via an RSU.

Figure 7 shows an example of message exchange procedure in V2I networking. Detailed steps of the procedure are explained in Section 7 and Section 8.

Note that a vehicle could also perform the prefix and service discovery simultaneously along with Address Registration procedure, as shown in Figure 9.

This document specified that RSUs as routers do not transmit periodical and unsolicited multicast RA messages including a prefix for energy saving in vehicular networks. Vehicles as hosts periodically initiate an RS message according to a time interval (considering its position and an RSU's coverage). Since they have a digital road map with the information of RSUs (e.g., position and communication coverage), vehicles can know when they will go out of the communication range of an RSU along with the signal strength (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]) from the RSU. RSUs replies with a solicited RA in unicast only when they receive an RS message.

```
          Vehicle                    RSU          Mobility Anchor
             |                        |                  |
             |-RS with Mobility Info->|                  |
             |         [VMI]          |                  |
             |                        |                  |
             |                        |--------PBU------>|
             |                        |                  |
             |                        |                  |
             |                        |<-------PBA-------|
             |                        |                  |
             |                        |                  |
             |                        |===Bi-Dir Tunnel==|
             |                        |                  |
             |                        |                  |
             |<----RA with prefix-----|                  |
             |                        |                  |
             |                        |                  |
             |                        |                  |
             |--NS with Address Reg-->|                  |
             |     [ARO+VPI+VSI]      |                  |
             |                        |                  |
             |                        |--------DAR------>|
             |                        |                  |
             |                        |                  |
             |                        |<-------DAC-------|
             |                        |                  |
             |                        |                  |
             |<--NA with Address Reg--|                  |
             |     [ARO+VPI+VSI]      |                  |
```

Figure 7: Message Interaction for Vehicular Neighbor Discovery

7. Address Registration and Duplicate Address Detection

This section explains address configuration, consisting of IP Address Autoconfiguration, Address Registration, and multihop DAD via V2I or V2V.

This document recommends a new Address Registration and DAD scheme in order to avoid multicast flooding and decrease link-scope multicast for energy and wireless channel conservation on a large-scale vehicular network. Host-initiated refresh of RA removes the necessity for routers to use frequent and unsolicited multicast RAs to accommodate hosts. This also enables the same IPv6 address prefix(es) to be used across a subnet.

There are three scenarios feasible in Address Registration scheme:

1. Vehicle enters the subnet for the first time or the current RSU belongs to another subnet: Vehicles need to perform the Address Registration and multihop DAD in the following subsections.

2. Vehicle has already configured its IP addresses with prefix obtained from the previous RSU, and the current RSU located in the same subnet: This means RSUs have the same prefix and the vehicle has no need to repeat the Address Registration and multihop DAD.

3. Vehicle is not in the coverage of RSU but has a neighbor registered in RSU: This document proposes a new V2V scenario for vehicles which are currently not in the range of the RSU. If a user vehicle failed to find an on-link RSU, it starts to look for adjacent vehicle neighbors which can work as relay neighbor to share the prefix obtained from RSU and undertake the DAD of the user vehicle by forwarding DAD messages to RSU.

7.1. Address Autoconfiguration

A vehicle as an IPv6 host creates its link-local IPv6 address and global IPv6 address as follows [RFC4862]. When they receive RS messages from vehicles, RSUs send back RA messages containing prefix information. The vehicle makes its global IPv6 addresses by combining the prefix for its current link and its link-layer address.

The address autoconfiguration does not perform the legacy DAD as defined in [RFC4862]. Instead, a new multihop DAD is performed in Section 7.3.

7.2. Address Registration

After its IP tentative address autoconfiguration with the known prefix from an RSU and its link-layer address, a vehicle starts to register its IP address to the serving RSU along with multihop DAD. Address Register Option (ARO) is used in this step and its format is defined in [RFC6775].

ARO is always host-initiated by vehicles. Information such as registration time and registration status contained in ARO is also included in multihop Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages used between RSU and MA, but ARO is not directly used in these two messages.

An example message exchange procedure of Address Registration is presented in Figure 8. Since Address Registration is performed simultaneously with the multihop DAD, the specific procedure is together described with the DAD mechanism in Section 7.3.

```
                   Vehicle                      RSU
                      |                           |
                      |                           |
               1.     |----NS with Address Reg--->|
                      |            [ARO]          |
                      |                           |
                      |                           |
                      |                           |
               2.     |<---NA with Address Reg----|
                      |            [ARO]          |
```

Figure 8: Neighbor Discovery Address Registration

7.3. Multihop Duplicate Address Detection

Before it can exchange data, a node should determine whether its IP address is already used by another node or not. In the legacy IPv6 ND, hosts multicast NS messages to all nodes in the same on-link subnet for DAD. Instead of this, an optimized multihop DAD is designed to eliminate multicast messages for energy-saving purpose. For this multihop DAD, Neighbor Cache and DAD Table are maintained by each RSU and an MA, respectively, for the duplicate address inspection during the multihop DAD process. That is, each RSU makes Neighbor Cache Entries (NCE) of all the on-link hosts in its Neighbor Cache. Similarly, the MA stores all the NCEs reported by the RSUs in its DAD Table.

With the multihop DAD, a vehicle can skip the multicast-based DAD in its current wireless link whenever it enters the coverage of another RSU in the same subset, leading to the reduction of traffic overhead in vehicular wireless links.

For the multihop DAD, two new ICMPv6 message types are defined in [RFC6775], such as Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC). Information carried by ARO options are copied into these two messages for the multihop DAD in the MA.

```
          Vehicle                    RSU         Mobility Anchor
             |                        |                  |
             |                        |                  |
        1.   |--NS with Address Reg-->|                  |
             |     [ARO+VPI+VSI]      |                  |
             |                        |                  |
             |                        |                  |
        2.   |                        | -------DAR------>|
             |                        |                  |
             |                        |                  |
        3.   |                        |<-------DAC-------|
             |                        |                  |
             |                        |                  |
             |                        |                  |
        4.   |<--NA with Address Reg--|                  |
             |     [ARO+VPI+VSI]      |                  |
```

Figure 9: Neighbor Discovery Address Registration with Multihop DAD

Figure 9 presents the procedure of Address Registration and multihop DAD. The detailed steps are explained as follows.

1. A vehicle sends an NS message to the current RSU in unicast, containing the ARO to RSU to register its address.

2. The RSU receives the NS message, and then inspects its Neighbor Cache to check whether it is duplicate or not. If there is no duplicate NCE, a tentative NCE is created for this address, and then the RSU sends a DAR to the MA for the multicast DAD.

3. When the MA receives a DAR from an RSU, it checks whether the register-requested address exists in its DAD Table or not. If an entry with the same address exists in the DAD Table, which means that the address is considered "Duplicate Address", then MA returns a DAC message to notify the RSU of the address duplication. If no entry with the same address exists in the DAD Table, which means that an entry for the address is created, then MA replies a DAC message to the RSU to confirm the uniqueness of the register-requested address to the RSU.

4. If the address duplication is notified by the MA, the RSU deletes the tentative NCE, and sends back an NS to the address-registration vehicle to notify the registration failure. Otherwise, the RSU changes the tentative NCE into a registered NCE in its Neighbor Cache, and then send back an NS to the vehicle to notify the registration success.

Thus, the multihop DAD is processed simultaneously with the Address Registration. Note that the tentative address is not considered assigned to the vehicle until the MA confirms the uniqueness of the register-requested address in the multihop DAD.

```
User Vehicle          Relay Vehicle                RSU       Mobility Anchor
   |                        |                        |                 |
   |------------------------|                        |                 |
   |        RD failed       |                        |                 |
   |------------------------|                        |                 |
   |                        |                        |                 |
   |                        |                        |                 |
   |-----------NS---------->|                        |                 |
   |                        |                        |                 |
   |<--NA with Prefix Info--|                        |                 |
   |                        |                        |                 |
   |                        |                        |                 |
   |--NS with Address Reg-->|                        |                 |
   |    [ARO+VPI+VSI]       |                        |                 |
   |                        |----- Forward NS ----->|                 |
   |                        |                        |                 |
   |                        |                        |-----------------|
   |                        |                        | Same as Figure 9|
   |                        |                        |-----------------|
   |                        |                        |                 |
   |                        |<--NA with Address Reg-|                 |
   |                        |     [ARO+VPI+VSI]      |                 |
   |<------ Forward NA -----|                        |                 |
   |                        |                        |                 |
```

Figure 10: Address Registration and Multihop DAD via V2V Relay

If a vehicle failed to register a default router, it triggers neighbor discovery to look for vehicle neighbors which can provide relay service using multi-hop communication. In this specification, we assumed vehicles would not emulate V2V communication and trigger relay scenario only if Router Discovery(RD) failed. On the other hand, at most one intermediate vehicle acts as a relay for another vehicle to communicate with the RSU.

Since vehicles have a digital road map with the information of RSUs (e.g., position and communication coverage), they can determine if they are available to serve as relay vehicle. Only vehicles with ability to serve as temporary relays will take action when they receive relay service requests. The user vehicle can process global address configuration, Address Registration and DAD through relay vehicle before it enters the coverage of RSUs. See Figure 10.

When a user vehicle failed to directly register with a RSU, it initiates neighbor discovery to detect vehicle neighbors through V2V communication. Vehicle sends NS messages to connect with neighbors in range. If neighbor can provide relay service, it creates a NCE for user vehicle, setting its own address as relay address, and sends back NA with prefix information received from RSU.

With receipt of NA, user vehicle configures its global address with prefix information as mentioned in Section 7.1. After this, user vehicle takes up to initiate the Address Registration along with DAD process via relay vehicle. NS message is configured as specified in Section 7.2 but indicate the relay vehicle's address as next-hop for reaching the RSU. In such a case, when relay vehicle receives relay request message, it will forward NS message to RSU. The procedure set up on the rails except MA will include the relay vehicle's address as relay address in NCE to indicate that at this moment it is not a directly attached vehicle, and set the relay address as next-hop address. Relay vehicle forwards DAD result information message to user vehicle as soon as it received.

7.4. Pseudonym Handling

Considering the privacy protection of a vehicle, a pseudonym mechanism for its link-layer address is requested. This mechanism periodically modifies the link-layer address, leading to the update of the corresponding IP address. A random MAC Address Generation mechanism is proposed in Appendix F.4 of [IEEE-802.11-OCB] by generating the 46 remaining bits of MAC address using a random number generator. When it changes its MAC address, a vehicle should ask the serving RSU to update its own NCE, and to register its IP address into the MA again.

8. Mobility Management

A mobility management is required for the seamless communication of vehicles moving between the RSUs. When a vehicle moves into the coverage of another RSU, a different IP address is assigned to the vehicle, resulting in the reconfiguration of transport-layer session information (i.e., end-point IP address) to avoid service disruption. Considering this issue, this document proposes a handover mechanism for seamless communication.

```
          Vehicle                    RSU          Mobility Anchor
             |                        |                  |
             |-RS with Mobility Info->|                  |
             |          [VMI]         |                  |
             |                        |                  |
             |                        |--------PBU------>|
             |                        |                  |
             |                        |                  |
             |                        |<-------PBA-------|
             |                        |                  |
             |                        |                  |
             |                        |===Bi-Dir Tunnel==|
             |                        |                  |
             |                        |                  |
             |<----RA with prefix-----|                  |
             |                        |                  |
```

Figure 11: Message Interaction for Vehicle Attachment

In [VIP-WAVE], the authors constructed a network-based mobility management scheme using Proxy Mobile IPv6 (PMIPv6) [RFC5213], which is highly suitable to vehicular networks. This document uses a mobility management procedure similar to PMIPv6 along with prefix discovery.

Figure 11 shows the binding update flow when a vehicle entered the subnet of an RSU. RSUs act as Mobility Anchor Gateway (MAG) defined in [VIP-WAVE]. When it receives RS messages from a vehicle containing its mobility information (e.g., position, speed, and direction), an RSU sends its MA a Proxy Binding Update (PBU) message [RFC5213][RFC3775], which contains a Mobility Option for the vehicle's mobility information. The MA receives the PBU and sets up a Binding Cache Entry (BCE) as well as a bi-directional tunnel (denoted as Bi-Dir Tunnel in Figure 11) between the serving RSU and itself. Through this tunnel, all traffic packets to the vehicle are encapsulated toward the RSU. Simultaneously, the MA sends back a Proxy Binding Acknowledgment (PBA) message to the serving RSU. This serving RSU receives the PBA and sets up a bi-directional tunnel with the MA. After this binding update, the RSU sends back an RA message to the vehicle including its own prefix for the address autoconfiguration.

```
      Vehicle            c-RSU          Mobility Anchor        n-RSU
         |                  |                  |                  |
         |                  |===Bi-Dir Tunnel==|                  |
         |                  |                  |                  |
         |                  |                  |                  |
         |                  |----DeReg PBU---->|                  |
         |                  |                  |                  |
         |                  |                  |                  |
         |                  |<-------PBA-------|                  |
         |                  |                  |                  |
         |                  |                  |                  |
         |                  |                  |                  |
         |                  |                  |                  |
         |                  |                  |                  |
         |---------------------------RS-------------------------->|
         |                                                        |
         |         Registration step as shown in Figure 5         |
         |                                                        |
         |                  |                  |===Bi-Dir Tunnel==|
         |                                                        |
         |<--------------------------RA---------------------------|
         |                                                        |
```

Figure 12: Message Interaction for Vehicle Handoff

When the vehicle changes its location, the MA has to change the end-point of the tunnel for the vehicle into the new RSU's IP address. As shown in Figure 12, when the MA receives a new PBU from the new RSU, it changes the tunnel's end-point from the current RSU (c-RSU) to the new RSU (n-RSU). If there is ongoing IP packets toward the vehicle, the MA encapsulates the packets and then forwards them towards n-RSU. Through this network-based mobility management, the vehicle is not aware of any changes at its network layer and can maintain its transport-layer sessions without any disruption.

If c-RSU and n-RSU are adjacent, that is, vehicles are moving in specified routes with fixed RSU allocation, the procedure can be simplified by constructing bidirectional tunnel directly between them (cancel the intervention of MA) to alleviate the traffic flow in MA as well as reduce handover delay. See Figure 13.

```
          Vehicle              c-RSU             n-RSU
             |                     |                  |
             |---------------------|                  |
             |c-RSU detects leaving|                  |
             |---------------------|                  |
             |                     |--------PBU------>|
             |                     |                  |
             |                     |===Bi-Dir Tunnel==|
             |                     |                  |
             |                     |<-------PBA-------|
             |                     |                  |
             |                     |                  |
             |(-------------------RS---------------->)|
             |                                        |
             |                                        |
             |<-------------------RA------------------|
             |                                        |
```

Figure 13: Vehicle Handoff between Adjacent RSUs

Since RSUs are in charge of detecting when a node joins or moves through its domain, if c-RSU detects the vehicle is going to leave its coverage and enter the area of adjacent RSU, it sends a PBU message to inform n-RSU about the handover of vehicle and update its mobility information. n-RSU receives the request and construct a bidirectional tunnel between c-RSU and itself, then send back PBA message for acknowledgment. If there are ongoing IP packets, c-RSU encapsulates the packets and then forwards them to n-RSU. When n-RSU detects the entrance of the vehicle, it directly sends RA mesage to vehicle for connection establishment (or replies solicited RA if vehicle sends request RS message first).

9. Security Considerations

This document shares all the security issues of the neighbor discovery protocol and 6LoWPAN protocol. This document can get benefits from secure neighbor discovery (SEND) [RFC3971] in order to protect ND from possible security attacks.

10. References

10.1. Normative References

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

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3971] Arkko, J., "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.

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

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., and K. Chowdhury, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

[RFC6775] Shelby, Z., Ed., "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, March 2017.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 8200, July 2017.

10.2. Informative References

[DSRC-WAVE] Morgan, Y., "Notes on DSRC & WAVE Standards Suite: Its Architecture, Design, and Characteristics", IEEE Communications Surveys & Tutorials, 12(4), 2012.

[ID-DNSNA] Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-05 (work in progress), March 2019.

[IEEE-802.11-OCB] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, December 2016.

[IEEE-802.11p]
"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments", June 2010.

[IPWAVE-PS]
Jeong, J., Ed., "IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", draft-ietf-ipwave-vehicular-networking-08 (work in progress), March 2019.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

[VIP-WAVE]
Cespedes, S., Lu, N., and X. Shen, "VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks", IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, March 2013.

[WAVE-1609.0]
IEEE 1609 Working Group, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture", IEEE Std 1609.0-2013, March 2014.

[WAVE-1609.2]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", IEEE Std 1609.2-2016, March 2016.

[WAVE-1609.3]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services", IEEE Std 1609.3-2016, April 2016.

[WAVE-1609.4]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation", IEEE Std 1609.4-2016, March 2016.

Appendix A. Changes from draft-jeong-ipwave-vehicular-neighbor-discovery-05

The following changes are made from draft-jeong-ipwave-vehicular-neighbor-discovery-05:

- In Section 4.1, a Shared-Prefix model is introduced for prefix assignment specified in this document.

- In Section 4.3, design goals are refined including the cancellation of Neighbor Unreachable Detection, and also the support of multi-hop communication for vehicles not in the coverage of RSUs.

- In Section 5.1, the Vehicular Network Architecture is updated on subnet division and V2V communication.

- In Section 7, a new scenario is added to facilitate vehicles outside the coverage of RSU to do Address Registration and DAD via relay vehicle.

- In Section 8, a simplified mobility management in vehicle handoff for adjacent RSUs is supplemented based on the original proposal.

Appendix B. Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

This work was supported in part by Global Research Laboratory Program through the NRF funded by the Ministry of Science and ICT (MSIT) (NRF-2013K1A1A2A02078326) and by the DGIST R&D Program of the MSIT (18-EE-01).

Authors' Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4957
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Yiwen Chris Shen
Department of Electrical and Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu

Zhong Xiang
Department of Electrical and Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 10 9895 1211
Fax: +82 31 290 7996
EMail: xz618@skku.edu