Basic Support for IPv6 over IEEE Std 802.11 Networks Operating Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)
draft-ietf-ipwave-ipv6-over-80211ocb-49

Abstract

This document provides methods and settings, and describes limitations, for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link. This support does only require minimal changes to existing stacks. Optimizations and usage of IPv6 over more complex scenarios is not covered in this specification and is subject of future work.

Status of This Memo

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

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

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

This Internet-Draft will expire on January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
Table of Contents

1. Introduction ................................................. 3
2. Terminology .................................................. 3
3. Communication Scenarios where IEEE 802.11-OCB Links are Used 4
4. IPv6 over 802.11-OCB ......................................... 4
   4.1. Maximum Transmission Unit (MTU) .......................... 4
   4.2. Frame Format ........................................... 5
   4.3. Link-Local Addresses .................................... 5
   4.4. Stateless Autoconfiguration ............................... 5
   4.5. Address Mapping ........................................ 6
      4.5.1. Address Mapping -- Unicast .......................... 6
      4.5.2. Address Mapping -- Multicast ........................ 6
   4.6. Subnet Structure ....................................... 7
5. Security Considerations ..................................... 8
   5.1. Privacy Considerations .................................. 8
      5.1.1. Privacy Risks of Meaningful info in Interface IDs .. 9
   5.2. MAC Address and Interface ID Generation ................ 9
5.3. Pseudonym Handling ....................................... 10
6. IANA Considerations ........................................ 10
7. Contributors ............................................... 10
8. Acknowledgements .......................................... 11
9. References .................................................. 11
   9.1. Normative References ................................... 12
   9.2. Informative References ................................ 14
Appendix A. 802.11p ........................................... 16
Appendix B. Aspects introduced by the OCB mode to 802.11 ........ 16
Appendix C. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver ... 21
Appendix D. Protocol Layering .................................. 22
Appendix E. Design Considerations ............................. 23
Appendix F. IEEE 802.11 Messages Transmitted in OCB mode ...... 23
Appendix G. Examples of Packet Formats ........................ 23
   G.1. Capture in Monitor Mode ................................. 24
   G.2. Capture in Normal Mode ................................ 27
Appendix H. Extra Terminology .................................. 29
Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links ................................. 30
Authors’ Addresses ........................................... 32
1. Introduction

This document provides a baseline with limitations for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link [IEEE-802.11-2016] (a.k.a., "802.11p" see Appendix A, Appendix B and Appendix C) with minimal changes to existing stacks. Moreover, the document identifies limitations of such usage. Concretely, the document describes the layering of IPv6 networking on top of the IEEE Std 802.11 MAC layer or an IEEE Std 802.3 MAC layer with a frame translation underneath. The resulting stack inherits from IPv6 over Ethernet [RFC 2464], but operates over 802.11-OCB to provide at least P2P (Point to Point) connectivity using IPv6 ND and link-local addresses.

The IPv6 network layer operates on 802.11-OCB in the same manner as operating on Ethernet with the following exceptions:

- Exceptions due to different operation of IPv6 network layer on 802.11 than on Ethernet. The operation of IP on Ethernet is described in [RFC1042], [RFC2464].

- Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure and movement detection. Security and privacy recommendations are discussed in Section 5 and Section 4.4. The subnet structure is described in Section 4.6. The movement detection on OCB links is not described in this document. Likewise, ND Extensions and IPWAVE optimizations for vehicular communications are not in scope. The expectation is that further specifications will be edited to cover more complex vehicular networking scenarios.

The reader may refer to [I-D.ietf-ipwave-vehicular-networking] for an overview of problems related to running IPv6 over 802.11-OCB. It is out of scope of this document to reiterate those.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The document makes uses of the following terms: IP-OBU (Internet Protocol On-Board Unit): an IP-OBU denotes a computer situated in a vehicle such as a car, bicycle, or similar. It has at least one IP interface that runs in mode OCB of 802.11, and that has an "OBU"
transceiver. See the definition of the term "OBU" in section Appendix H.

IP-RSU (IP Road-Side Unit): an IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. An IP-RSU communicates with the IP-OBU in the vehicle over 802.11 wireless link operating in OCB mode. An IP-RSU is similar to an Access Network Router (ANR) defined in [RFC3753], and a Wireless Termination Point (WTP) defined in [RFC5415].

OCB (outside the context of a basic service set - BSS): is a mode of operation in which a STA is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality.

802.11-OCB: refers to the mode specified in IEEE Std 802.11-2016 when the MIB attribute dot11OCBActivited is 'true'. Note: compliance with standards and regulations set in different countries when using the 5.9GHz frequency band is required.

3. Communication Scenarios where IEEE 802.11-OCB Links are Used

The IEEE 802.11-OCB networks are used for vehicular communications, as 'Wireless Access in Vehicular Environments'. In particular, we refer the reader to [I-D.ietf-ipwave-vehicular-networking], that lists some scenarios and requirements for IP in Intelligent Transportation Systems (ITS).

The link model is the following: STA --- 802.11-OCB --- STA. In vehicular networks, STAs can be IP-RSUs and/or IP-OBUs. All links are assumed to be P2P and multiple links can be on one radio interface. While 802.11-OCB is clearly specified, and a legacy IPv6 stack can operate on such links, the use of the operating environment (vehicular networks) brings in new perspectives.

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

The default MTU for IP packets on 802.11-OCB is inherited from RFC2464 and is, as such, 1500 octets. This value of the MTU respects the recommendation that every link on the Internet must have a minimum MTU of 1280 octets (stated in [RFC8200], and the recommendations therein, especially with respect to fragmentation).
4.2. Frame Format

IP packets MUST be transmitted over 802.11-OCB media as QoS Data frames whose format is specified in IEEE 802.11 spec [IEEE-802.11-2016].

The IPv6 packet transmitted on 802.11-OCB are immediately preceded by a Logical Link Control (LLC) header and an 802.11 header. In the LLC header, and in accordance with the EtherType Protocol Discrimination (EPD, see Appendix D), the value of the Type field MUST be set to 0x86DD (IPv6). The mapping to the 802.11 data service MUST use a ‘priority’ value of 1, which specifies the use of QoS with a ‘Background’ user priority.

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers MAY implement IPv6-over-Ethernet as per RFC 2464 and then a frame translation from 802.3 to 802.11 in order to minimize the code changes.

4.3. Link-Local Addresses

There are several types of IPv6 addresses [RFC4291], [RFC4193], that may be assigned to an 802.11-OCB interface. Among these types of addresses only the IPv6 link-local addresses can be formed using an EUI-64 identifier, in particular during transition time.

If the IPv6 link-local address is formed using an EUI-64 identifier, then the mechanism of forming that address is the same mechanism as used to form an IPv6 link-local address on Ethernet links. Moreover, whether or not the interface identifier is derived from the EUI-64 A identifier, its length is 64 bits as is the case for Ethernet [RFC2464].

4.4. Stateless Autoconfiguration

The steps a host takes in deciding how to autoconfigure its interfaces in IPv6 are described in [RFC4862]. This section describes the formation of Interface Identifiers for IPv6 addresses of type ‘Global’ or ‘Unique Local’. For Interface Identifiers for IPv6 address of type ‘Link-Local’ are discussed in Section 4.3.

The RECOMMENDED method for forming stable Interface Identifiers (IIDs) is described in [RFC8064]. The method of forming IIDs described in Section 4 of [RFC2464] MAY be used during transition time, in particular for IPv6 link-local addresses. Regardless of how to form the IID, its length is 64 bits, as is the case of the IPv6 over Ethernet [RFC2464].

The bits in the IID have no specific meaning and the identifier should be treated as an opaque value. The bits ‘Universal’ and ‘Group’ in the identifier of an 802.11-OCB interface are significant, as this is an IEEE link-layer address. The details of this significance are described in [RFC7136].

Semantically opaque IIDs, instead of meaningful IIDs derived from a valid and meaningful MAC address ([RFC2464], Section 4), help avoid certain privacy risks (see the risks mentioned in Section 5.1.1). If semantically opaque IIDs are needed, they MAY be generated using the method for generating semantically opaque IIDs with IPv6 Stateless Address Autoconfiguration given in [RFC7217]. Typically, an opaque IID is formed starting from identifiers different than the MAC addresses, and from cryptographically strong material. Thus, privacy sensitive information is absent from Interface IDs, because it is impossible to calculate back the initial value from which the Interface ID was first generated.

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose IIDs don’t change too often. It is RECOMMENDED to use the mechanisms described in RFC 7217 to permit the use of Stable IIDs that do not change within one subnet prefix. A possible source for the Net-Iface Parameter is a virtual interface name, or logical interface name, that is decided by a local administrator.

4.5. Address Mapping

Unicast and multicast address mapping MUST follow the procedures specified for Ethernet interfaces specified in Sections 6 and 7 of [RFC2464].

4.5.1. Address Mapping -- Unicast

This document is scoped for Address Resolution (AR) and Duplicate Address Detection (DAD) per [RFC4862].

4.5.2. Address Mapping -- Multicast

The multicast address mapping is performed according to the method specified in section 7 of [RFC2464]. The meaning of the value "3333" mentioned in that section 7 of [RFC2464] is defined in section 2.3.1 of [RFC7042].

Transmitting IPv6 packets to multicast destinations over 802.11 links proved to have some performance issues [I-D.ietf-mboned-ieee802-mcast-problems]. These issues may be
exacerbated in OCB mode. A future improvement to this specification should consider solutions for these problems.

4.6. Subnet Structure

A subnet may be formed over 802.11-OCB interfaces of vehicles that are in close range (not by their in-vehicle interfaces). A Prefix List conceptual data structure ([RFC4861] Section 5.1) is maintained for each 802.11-OCB interface.

An IPv6 subnet on which Neighbor Discovery protocol (ND) can be mapped on an OCB network if all nodes share a single broadcast Domain, which is generally the case for P2P OCB links; The extension to IPv6 ND operating on a subnet that covers multiple OCB links and not fully overlapping (NBMA) is not in scope.

The structure of this subnet is ephemeral, in that it is strongly influenced by the mobility of vehicles: the hidden terminal effects appear; the 802.11 networks in OCB mode may be considered as ‘ad-hoc’ networks with an addressing model as described in [RFC5889]. On another hand, the structure of the internal subnets in each vehicle is relatively stable.

As recommended in [RFC5889], when the timing requirements are very strict (e.g. fast drive through IP-RSU coverage), no on-link subnet prefix should be configured on an 802.11-OCB interface. In such cases, the exclusive use of IPv6 link-local addresses is RECOMMENDED.

Additionally, even if the timing requirements are not very strict (e.g., the moving subnet formed by two following vehicles is stable, a fixed IP-RSU is absent), the subnet is disconnected from the Internet (i.e., a default route is absent), and the addressing peers are equally qualified (that is, it is impossible to determine that some vehicle owns and distributes addresses to others) the use of link-local addresses is RECOMMENDED.

The baseline ND protocol [RFC4861] MUST be supported over 802.11-OCB links. Transmitting ND packets may prove to have some performance issues as mentioned in Section 4.5.2, and Appendix I. These issues may be exacerbated in OCB mode. Solutions for these problems should consider the OCB mode of operation. Future solutions to OCB should consider solutions for avoiding broadcast. The best of current knowledge indicates the kinds of issues that may arise with ND in OCB mode; they are described in Appendix I.

Protocols like Mobile IPv6 [RFC6275], [RFC3963] and DNAv6 [RFC6059], which depend on a timely movement detection, might need additional
5. Security Considerations

Any security mechanism at the IP layer or above that may be carried out for the general case of IPv6 may also be carried out for IPv6 operating over 802.11-OCB.

The OCB operation is stripped off of all existing 802.11 link-layer security mechanisms. There is no encryption applied below the network layer running on 802.11-OCB. At the application layer, the IEEE 1609.2 document [IEEE-1609.2] provides security services for certain applications to use; application-layer mechanisms are out-of-scope of this document. On another hand, a security mechanism provided at networking layer, such as IPsec [RFC4301], may provide data security protection to a wider range of applications.

802.11-OCB does not provide any cryptographic protection, because it operates outside the context of a BSS (no Association Request/Response, no Challenge messages). Any attacker can therefore just sit in the near range of vehicles, sniff the network (just set the interface card’s frequency to the proper range) and performs attacks without needing to physically break any wall. Such a link is less protected than commonly used links (wired link or protected 802.11).

The potential attack vectors are: MAC address spoofing, IP address and session hijacking, and privacy violation Section 5.1. A previous work at SAVI WG identifies some threats [RFC6959], while SeND presented in [RFC3971] and [RFC3972] is a solution against address theft but it is complex and not deployed.

More IETF protocols are available in the toolbox of the IP security protocol designer. Some ETSI protocols related to security protocols in ITS are described in [ETSI-sec-archi].

5.1. Privacy Considerations

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11-OCB interface may involve privacy, MAC address spoofing and IP hijacking risks. A vehicle embarking an IP-OBU whose egress interface is 802.11-OCB may expose itself to eavesdropping and subsequent correlation of data; this may reveal data considered private by the vehicle owner; there is a risk of being tracked. In outdoors public environments, where vehicles typically circulate, the privacy risks are more important than in indoors settings. It is highly likely that attacker sniffers are deployed along routes which listen for IEEE frames, including IP
packets, of vehicles passing by. For this reason, in the 802.11-OCB deployments, there is a strong necessity to use protection tools such as dynamically changing MAC addresses Section 5.2, semantically opaque Interface Identifiers and stable Interface Identifiers Section 4.4. An example of change policy is to change the MAC address of the OCB interface each time the system boots up. This may help mitigate privacy risks to a certain level. Furthermore, for privacy concerns ([RFC8065]) recommends using an address generation scheme rather than addresses generated from a fixed link-layer address.

5.1.1. Privacy Risks of Meaningful info in Interface IDs

The privacy risks of using MAC addresses displayed in Interface Identifiers are important. The IPv6 packets can be captured easily in the Internet and on-link in public roads. For this reason, an attacker may realize many attacks on privacy. One such attack on 802.11-OCB is to capture, store and correlate Company ID information present in MAC addresses of many cars (e.g. listen for Router Advertisements, or other IPv6 application data packets, and record the value of the source address in these packets). Further correlation of this information with other data captured by other means, or other visual information (car color, others) MAY constitute privacy risks.

5.2. MAC Address and Interface ID Generation

In 802.11-OCB networks, the MAC addresses MAY change during well defined renumbering events. In the moment the MAC address is changed on an 802.11-OCB interface all the Interface Identifiers of IPv6 addresses assigned to that interface MUST change.

The policy dictating when the MAC address is changed on the 802.11-OCB interface is to-be-determined. For more information on the motivation of this policy please refer to the privacy discussion in Appendix B.

A ‘randomized’ MAC address has the following characteristics:

- Bit "Local/Global" set to "locally administered".
- Bit "Unicast/Multicast" set to "Unicast".
- The 46 remaining bits are set to a random value, using a random number generator that meets the requirements of [RFC4086].

To meet the randomization requirements for the 46 remaining bits, a hash function may be used. For example, the SHA256 hash function may
be used with input a 256 bit local secret, the ‘nominal’ MAC Address of the interface, and a representation of the date and time of the renumbering event.

A randomized Interface ID has the same characteristics of a randomized MAC address, except the length in bits. An Interface ID SHOULD be of length specified in other documents.

5.3. Pseudonym Handling

The demand for privacy protection of vehicles’ and drivers’ identities, which could be granted by using a pseudonym or alias identity at the same time, may hamper the required confidentiality of messages and trust between participants — especially in safety critical vehicular communication.

- Particular challenges arise when the pseudonymization mechanism used relies on (randomized) re-addressing.

- A proper pseudonymization tool operated by a trusted third party may be needed to ensure both aspects simultaneously (privacy protection on one hand and trust between participants on another hand).

- This is discussed in Section 4.4 and Section 5 of this document.

- Pseudonymity is also discussed in [I-D.ietf-ipwave-vehicular-networking] in its sections 4.2.4 and 5.1.2.

6. IANA Considerations

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

Romain Kuntz contributed extensively about IPv6 handovers between links running outside the context of a BSS (802.11-OCB links).

Tim Leinmueller contributed the idea of the use of IPv6 over 802.11-OCB for distribution of certificates.

Marios Makassikis, Jose Santa Lozano, Albin Severinson and Alexey Voronov provided significant feedback on the experience of using IP messages over 802.11-OCB in initial trials.
Michelle Wetterwald contributed extensively the MTU discussion, offered the ETSI ITS perspective, and reviewed other parts of the document.

8. Acknowledgements

The authors would like to thank Alexandre Petrescu for initiating this work and for being the lead author until the version 43 of this draft.

The authors would like to thank Pascal Thubert for reviewing, proofreading and suggesting modifications of this document.

The authors would like to thank Witold Klaudel, Ryuji Wakikawa, Emmanuel Baccelli, John Kenney, John Moring, Francois Simon, Dan Romascou, Konstantin Khait, Ralph Droms, Richard ‘Dick’ Roy, Ray Hunter, Tom Kurihara, Michal Sojka, Jan de Jongh, Suresh Krishnan, Dino Farinacci, Vincent Park, Jaehoon Paul Jeong, Gloria Gwynne, Hans-Joachim Fischer, Russ Housley, Rex Buddenberg, Erik Nordmark, Bob Moskowitz, Andrew Dryden, Georg Mayer, Dorothy Stanley, Sandra Cespedes, Mariano Falcitelli, Sri Gundavelli, Abdussalam Baryun, Margaret Cullen, Erik Kline, Carlos Jesus Bernardos Cano, Ronald in ‘t Velt, Katrin Sjoberg, Roland Bless, Tijink Jasja, Kevin Smith, Brian Carpenter, Julian Reschke, Mikael Abrahamsson, Dirk von Hugo, Lorenzo Colitti, Pascal Thubert, Ole Troan, Jinmei Tatuya, Joel Halpern, Eric Gray and William Whyte. Their valuable comments clarified particular issues and generally helped to improve the document.

Pierre Pfister, Rostislav Lisovy, and others, wrote 802.11-OCB drivers for linux and described how.

For the multicast discussion, the authors would like to thank Owen DeLong, Joe Touch, Jen Linkova, Erik Kline, Brian Haberman and participants to discussions in network working groups.

The authors would like to thank participants to the Birds-of-a-Feather "Intelligent Transportation Systems" meetings held at IETF in 2016.

Human Rights Protocol Considerations review by Amelia Andersdotter.

9. References
9.1. Normative References


9.2. Informative References


[I-D.ietf-mboned-ieee802-mcast-problems]

[IEEE-1609.2]

[IEEE-1609.3]

[IEEE-1609.4]

[IEEE-802.11-2016]
"IEEE Standard 802.11-2016 - IEEE Standard for Information Technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Status - Active Standard. Description retrieved freely; the document itself is also freely available, but with some difficulty (requires registration); description and document retrieved on April 8th, 2019, starting from URL https://standards.ieee.org/findstds/standard/802.11-2016.html".

Appendix A.  802.11p

The term "802.11p" is an earlier definition. The behaviour of "802.11p" networks is rolled in the document IEEE Std 802.11-2016. In that document the term 802.11p disappears. Instead, each 802.11p feature is conditioned by the IEEE Management Information Base (MIB) attribute "OCBActivated" [IEEE-802.11-2016]. Whenever OCBActivated is set to true the IEEE Std 802.11-OCB state is activated. For example, an 802.11 STA station operating outside the context of a basic service set has the OCBActivated flag set. Such a station, when it has the flag set, uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

Appendix B. Aspects introduced by the OCB mode to 802.11

In the IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. In OCB mode, the manner in which channels are selected and used is simplified compared to when in BSS mode.
Contrary to BSS mode, at link layer, it is necessary to set statically the same channel number (or frequency) on two stations that need to communicate with each other (in BSS mode this channel set operation is performed automatically during ‘scanning’). The manner in which stations set their channel number in OCB mode is not specified in this document. Stations STA1 and STA2 can exchange IP packets only if they are set on the same channel. At IP layer, they then discover each other by using the IPv6 Neighbor Discovery protocol. The allocation of a particular channel for a particular use is defined statically in standards authored by ETSI (in Europe), FCC in America, and similar organisations in South Korea, Japan and other parts of the world.

Briefly, the IEEE 802.11-OCB mode has the following properties:

- The use by each node of a ‘wildcard’ BSSID (i.e., each bit of the BSSID is set to 1)
- No IEEE 802.11 Beacon frames are transmitted
- No authentication is required in order to be able to communicate
- No association is needed in order to be able to communicate
- No encryption is provided in order to be able to communicate
- Flag dot11OCBActivated is set to true

All the nodes in the radio communication range (IP-OBU and IP-RSU) receive all the messages transmitted (IP-OBU and IP-RSU) within the radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

The message exchange diagram in Figure 1 illustrates a comparison between traditional 802.11 and 802.11 in OCB mode. The ‘Data’ messages can be IP packets such as HTTP or others. Other 802.11 management and control frames (non IP) may be transmitted, as specified in the 802.11 standard. For information, the names of these messages as currently specified by the 802.11 standard are listed in Appendix F.
STA                    AP              STA1                   STA2

|<------ Beacon ------->|               |<------ Data -------->|\
|---- Probe Req. ------->|               |<------ Data -------->|
|---- Probe Res. ------->|               |<------ Data -------->|
|---- Auth Req. ------->|               |<------ Data -------->|
|---- Auth Res. ------->|               |<------ Data -------->|
|---- Asso Req. ------->|               |<------ Data -------->|
|---- Asso Res. ------->|               |<------ Data -------->|
|<------ Data --------> |               |<------ Data -------->|
|<------ Data --------> |               |<------ Data -------->|

(i) 802.11 Infrastructure mode         (ii) 802.11-OCB mode

Figure 1: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

The interface 802.11-OCB was specified in IEEE Std 802.11p (TM) -2010 [IEEE-802.11p-2010] as an amendment to IEEE Std 802.11 (TM) -2007, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, this amendment has been integrated in IEEE 802.11(TM) -2012 and -2016 [IEEE-802.11-2016].

In document 802.11-2016, anything qualified specifically as "OCBActivated", or "outside the context of a basic service" set to be true, then it is actually referring to OCB aspects introduced to 802.11.

In order to delineate the aspects introduced by 802.11-OCB to 802.11, we refer to the earlier [IEEE-802.11p-2010]. The amendment is concerned with vehicular communications, where the wireless link is similar to that of Wireless LAN (using a PHY layer specified by 802.11a/b/g/n), but which needs to cope with the high mobility factor inherent in scenarios of communications between moving vehicles, and between vehicles and fixed infrastructure deployed along roads. While 'p' is a letter identifying the Amendment, just like 'a, b, g' and 'n' are, 'p' is concerned more with MAC modifications, and a little with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a 'p' MAC with an 'a' PHY by operating outside the context of a BSS with OFDM at 5.4GHz and 5.9GHz.

The 802.11-OCB links are specified to be compatible as much as possible with the behaviour of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11-OCB MAC layer offers practically the same interface to IP as the 802.11a/b/g/n and 802.3. A packet sent by an IP-OBU may be received by one or multiple IP-RSUs. The link-layer resolution is performed by using the IPv6 Neighbor Discovery protocol.

To support this similarity statement (IPv6 is layered on top of LLC on top of 802.11-OCB, in the same way that IPv6 is layered on top of LLC on top of 802.11a/b/g/n (for WLAN) or layered on top of LLC on top of 802.3 (for Ethernet)) it is useful to analyze the differences between 802.11-OCB and 802.11 specifications. During this analysis, we note that whereas 802.11-OCB lists relatively complex and numerous changes to the MAC layer (and very little to the PHY layer), there are only a few characteristics which may be important for an implementation transmitting IPv6 packets on 802.11-OCB links.

The most important 802.11-OCB point which influences the IPv6 functioning is the OCB characteristic; an additional, less direct influence, is the maximum bandwidth afforded by the PHY modulation/demodulation methods and channel access specified by 802.11-OCB. The maximum bandwidth theoretically possible in 802.11-OCB is 54 Mbit/s (when using, for example, the following parameters: 20 MHz channel; modulation 64-QAM; coding rate R is 3/4); in practice of IP-over-802.11-OCB a commonly observed figure is 12Mbit/s; this bandwidth allows the operation of a wide range of protocols relying on IPv6.

- **Operation Outside the Context of a BSS (OCB):** the (earlier 802.11p) 802.11-OCB links are operated without a Basic Service Set (BSS). This means that the frames IEEE 802.11 Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always 0xffffffffffff (48 '1' bits, represented as MAC address ff:ff:ff:ff:ff:ff, or otherwise the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by administrator (e.g. 'My-Home-AccessPoint'). The OCB operation - namely the lack of beacon-based scanning and lack of authentication - should be taken into account when the Mobile IPv6 protocol [RFC6275] and the protocols for IP layer security [RFC4301] are used. The way these protocols adapt to OCB is not described in this document.

- **Timing Advertisement:** is a new message defined in 802.11-OCB, which does not exist in 802.11a/b/g/n. This message is used by stations to inform other stations about the value of time. It is similar to the time as delivered by a GNSS system (Galileo, GPS,
(... or by a cellular system. This message is optional for implementation.

- Frequency range: this is a characteristic of the PHY layer, with almost no impact on the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, ECC/CEPT based on ENs from ETSI, FCC, etc.); as part of the regulation process, specific applications are associated with specific frequency ranges. In the case of 802.11-OCB, the regulator associates a set of frequency ranges, or slots within a band, to the use of applications of vehicular communications, in a band known as "5.9GHz". The 5.9GHz band is different from the 2.4GHz and 5GHz bands used by Wireless LAN. However, as with Wireless LAN, the operation of 802.11-OCB in "5.9GHz" bands is exempt from owning a license in EU (in US the 5.9GHz is a licensed band of spectrum; for the fixed infrastructure an explicit FCC authorization is required; for an on-board device a 'licensed-by-rule' concept applies: rule certification conformity is required.) Technical conditions are different than those of the bands "2.4GHz" or "5GHz". The allowed power levels, and implicitly the maximum allowed distance between vehicles, is of 33dBm for 802.11-OCB (in Europe), compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to a maximum distance of approximately 1km, compared to approximately 50m. Additionally, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in US) and on the use of frequencies for Intelligent Transportation Systems (in EU), compared to Wireless LAN (802.11a/b/g/n).

- 'Half-rate' encoding: as the frequency range, this parameter is related to PHY, and thus has not much impact on the interface between the IP layer and the MAC layer.

- In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in Section 5. A relevant function is described in documents IEEE 1609.3-2016 [IEEE-1609.3] and IEEE 1609.4-2016 [IEEE-1609.4].
Appendix C. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver

The 802.11p amendment modifies both the 802.11 stack’s physical and MAC layers but all the induced modifications can be quite easily obtained by modifying an existing 802.11a ad-hoc stack.

Conditions for a 802.11a hardware to be 802.11-OCB compliant:

- The PHY entity shall be an orthogonal frequency division multiplexing (OFDM) system. It must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11-OCB layer, in France: 5875MHz to 5925MHz.

- The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.

- The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).

- The chip should be able to transmit up to 44.8 dBm when used by the US government in the United States, and up to 33 dBm in Europe; other regional conditions apply.

Changes needed on the network stack in OCB mode:

- Physical layer:
  - The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.
  - The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).
  - The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules, if used by the kernel to enforce local specific restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

- MAC layer:
  - All management frames (beacons, join, leave, and others) emission and reception must be disabled except for frames of subtype Action and Timing Advertisement (defined below).
* No encryption key or method must be used.

* Packet emission and reception must be performed as in ad-hoc mode, using the wildcard BSSID (ff:ff:ff:ff:ff:ff).

* The functions related to joining a BSS (Association Request/Response) and for authentication (Authentication Request/Reply, Challenge) are not called.

* The beacon interval is always set to 0 (zero).

* Timing Advertisement frames, defined in the amendment, should be supported. The upper layer should be able to trigger such frames emission and to retrieve information contained in received Timing Advertisements.

Appendix D. Protocol Layering

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated in Figure 2. The IP layer operates on top of the EtherType Protocol Discrimination (EPD); this Discrimination layer is described in IEEE Std 802.3-2012; the interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).

```
+---------------------------------------------+
| IPv6                                        |
+---------------------------------------------+
+---------(       )--------------------------+
| LLC_SAP    802.11-OCB                       |
+---------(       )--------------------------+
| EPD     Boundary                            |
+---------(       )--------------------------+
| MAC_SAP  MLME_SAP                          |
+---------(       )--------------------------+
| MAC Sublayer and ch. coord.                |
| 802.11-OCB SME Services                   |
+---------(       )--------------------------+
| PHY_SAP  PLME_SAP                          |
+---------(       )--------------------------+
| PHY Layer                                   |
+---------------------------------------------+
```

Figure 2: EtherType Protocol Discrimination
Appendix E. Design Considerations

The networks defined by 802.11-OCB are in many ways similar to other networks of the 802.11 family. In theory, the transportation of IPv6 over 802.11-OCB could be very similar to the operation of IPv6 over other networks of the 802.11 family. However, the high mobility, strong link asymmetry and very short connection makes the 802.11-OCB link significantly different from other 802.11 networks. Also, the automotive applications have specific requirements for reliability, security and privacy, which further add to the particularity of the 802.11-OCB link.

Appendix F. IEEE 802.11 Messages Transmitted in OCB mode

For information, at the time of writing, this is the list of IEEE 802.11 messages that may be transmitted in OCB mode, i.e. when dot11OCBActivated is true in a STA:

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;
- The STA MUST send data frames of subtype QoS Data.

Appendix G. Examples of Packet Formats

This section describes an example of an IPv6 Packet captured over a IEEE 802.11-OCB link.

By way of example we show that there is no modification in the headers when transmitted over 802.11-OCB networks - they are transmitted like any other 802.11 and Ethernet packets.

We describe an experiment of capturing an IPv6 packet on an 802.11-OCB link. In topology depicted in Figure 3, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11-OCB interface. The packet is captured on the Host, using a network protocol analyzer (e.g. Wireshark); the capture is performed in two different modes: direct mode and 'monitor' mode. The topology used during the capture is depicted below.

The packet is captured on the Host. The Host is an IP-OBU containing an 802.11 interface in format PCI express (an ITRI product). The kernel runs the ath5k software driver with modifications for OCB mode. The capture tool is Wireshark. The file format for save and
analyze is ‘pcap’. The packet is generated by the Router. The Router is an IP-RSU (ITRI product).

```
+--------+                                +-------+
|        |        802.11-OCB Link         |       |
|        |                                |       |
+--------+                                +-------+
```

Figure 3: Topology for capturing IP packets on 802.11-OCB

During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

G.1. Capture in Monitor Mode

The IPv6 RA packet captured in monitor mode is illustrated below. The radio tap header provides more flexibility for reporting the characteristics of frames. The Radiotap Header is prepended by this particular stack and operating system on the Host machine to the RA packet received from the network (the Radiotap Header is not present on the air). The implementation-dependent Radiotap Header is useful for piggybacking PHY information from the chip’s registers as data in a packet understandable by userland applications using Socket interfaces (the PHY interface can be, for example: power levels, data rate, ratio of signal to noise).

The packet present on the air is formed by IEEE 802.11 Data Header, Logical Link Control Header, IPv6 Base Header and ICMPv6 Header.

```
Radiotap Header v0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Header Revision | Header Pad | Header length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Present flags |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data Rate | Pad |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
IEEE 802.11 Data Header

Logical-Link Control Header

IPv6 Base Header

Router Advertisement
The value of the Data Rate field in the Radiotap header is set to 6 Mb/s. This indicates the rate at which this RA was received.

The value of the Transmitter address in the IEEE 802.11 Data Header is set to a 48bit value. The value of the destination address is 33:33:00:00:00:1 (all-nodes multicast address). The value of the BSS Id field is ff:ff:ff:ff:ff:ff, which is recognized by the network protocol analyzer as being "broadcast". The Fragment number and sequence number fields are together set to 0x90C6.

The value of the Organization Code field in the Logical-Link Control Header is set to 0x0, recognized as "Encapsulated Ethernet". The value of the Type field is 0x86DD (hexadecimal 86DD, or otherwise #86DD), recognized as "IPv6".

A Router Advertisement is periodically sent by the router to multicast group address ff02::1. It is an icmp packet type 134. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags, as described in [RFC4861].

The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1.

The Ethernet Type field in the logical-link control header is set to 0x86dd which indicates that the frame transports an IPv6 packet. In the IEEE 802.11 data, the destination address is 33:33:00:00:00:01 which is the corresponding multicast MAC address. The BSS id is a broadcast address of ff:ff:ff:ff:ff:ff. Due to the short link duration between vehicles and the roadside infrastructure, there is no need in IEEE 802.11-OCB to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11-OCB enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.
G.2. Capture in Normal Mode

The same IPv6 Router Advertisement packet described above (monitor mode) is captured on the Host, in the Normal mode, and depicted below.
Ethernet II Header

IPv6 Base Header

Router Advertisement

One notices that the Radiotap Header, the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On the other hand, a new header named Ethernet II Header is present.

The Destination and Source addresses in the Ethernet II header contain the same values as the fields Receiver Address and Transmitter Address present in the IEEE 802.11 Data Header in the "monitor" mode capture.

The value of the Type field in the Ethernet II header is 0x86DD (recognized as "IPv6"); this value is the same value as the value of the field Type in the Logical-Link Control Header in the "monitor" mode capture.

The knowledgeable experimenter will no doubt notice the similarity of this Ethernet II Header with a capture in normal mode on a pure Ethernet cable interface.

A frame translation is inserted on top of a pure IEEE 802.11 MAC layer, in order to adapt packets, before delivering the payload data to the applications. It adapts 802.11 LLC/MAC headers to Ethernet II headers. In further detail, this adaptation consists in the elimination of the Radiotap, 802.11 and LLC headers, and in the insertion of the Ethernet II header. In this way, IPv6 runs straight over LLC over the 802.11-OCB MAC layer; this is further confirmed by the use of the unique Type 0x86DD.

Appendix H. Extra Terminology

The following terms are defined outside the IETF. They are used to define the main terms in the main terminology section Section 2.

DSRC (Dedicated Short Range Communication): a term defined outside the IETF. The US Federal Communications Commission (FCC) Dedicated Short Range Communication (DSRC) is defined in the Code of Federal Regulations (CFR) 47, Parts 90 and 95. This Code is referred in the definitions below. At the time of the writing of this Internet Draft, the last update of this Code was dated October 1st, 2010.

DSRCS (Dedicated Short-Range Communications Services): a term defined outside the IETF. The use of radio techniques to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments. DSRCS systems may also transmit status and instructional messages related to the units involve. [Ref. 47 CFR 90.7 - Definitions]
OBU (On-Board Unit): a term defined outside the IETF. An On-Board Unit is a DSRC transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of the respective chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of the respective chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands. - [CFR 90.7 - Definitions].

RSU (Road-Side Unit): a term defined outside of IETF. A Roadside Unit is a DSRC transceiver that is mounted along a road or pedestrian passageway. An RSU may also be mounted on a vehicle or is hand carried, but it may only operate when the vehicle or hand- carried unit is stationary. Furthermore, an RSU operating under the respective part is restricted to the location where it is licensed to operate. However, portable or hand-held RSUs are permitted to operate where they do not interfere with a site-licensed operation. A RSU broadcasts data to OBUs or exchanges data with OBUs in its communications zone. An RSU also provides channel assignments and operating instructions to OBUs in its communications zone, when required. - [CFR 90.7 - Definitions].

Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861][RFC4862] was designed for point-to-point and transit links such as Ethernet, with the expectation of a cheap and reliable support for multicast from the lower layer. Section 3.2 of RFC 4861 indicates that the operation on Shared Media and on non-broadcast multi-access (NBMA) networks require additional support, e.g., for Address Resolution (AR) and duplicate address detection (DAD), which depend on multicast. An infrastructureless radio network such as OCB shares properties with both Shared Media and NBMA networks, and then adds its own complexity, e.g., from movement and interference that allow only transient and non-transitive reachability between any set of peers.

The uniqueness of an address within a scoped domain is a key pillar of IPv6 and the base for unicast IP communication. RFC 4861 details the DAD method to avoid that an address is duplicated. For a link local address, the scope is the link, whereas for a Globally Reachable address the scope is much larger. The underlying assumption for DAD to operate correctly is that the node that owns an
IPv6 address can reach any other node within the scope at the time it claims its address, which is done by sending a NS multicast message, and can hear any future claim for that address by another party within the scope for the duration of the address ownership.

In the case of OCB, there is a potentially a need to define a scope that is compatible with DAD, and that cannot be the set of nodes that a transmitter can reach at a particular time, because that set varies all the time and does not meet the DAD requirements for a link local address that could possibly be used anytime, anywhere. The generic expectation of a reliable multicast is not ensured, and the operation of DAD and AR (Address Resolution) as specified by RFC 4861 cannot be guaranteed. Moreover, multicast transmissions that rely on broadcast are not only unreliable but are also often detrimental to unicast traffic (see [draft-ietf-mboned-ieee802-mcast-problems]).

Early experience indicates that it should be possible to exchange IPv6 packets over OCB while relying on IPv6 ND alone for DAD and AR (Address Resolution) in good conditions. In the absence of a correct DAD operation, a node that relies only on IPv6 ND for AR and DAD over OCB should ensure that the addresses that it uses are unique by means others than DAD. It must be noted that deriving an IPv6 address from a globally unique MAC address has this property but may yield privacy issues.

RFC 8505 provides a more recent approach to IPv6 ND and in particular DAD. RFC 8505 is designed to fit wireless and otherwise constrained networks whereby multicast and/or continuous access to the medium may not be guaranteed. RFC 8505 Section 5.6 "Link-Local Addresses and Registration" indicates that the scope of uniqueness for a link local address is restricted to a pair of nodes that use it to communicate, and provides a method to assert the uniqueness and resolve the link-Layer address using a unicast exchange.

RFC 8505 also enables a router (acting as a 6LR) to own a prefix and act as a registrar (acting as a 6LBR) for addresses within the associated subnet. A peer host (acting as a 6LN) registers an address derived from that prefix and can use it for the lifetime of the registration. The prefix is advertised as not onlink, which means that the 6LN uses the 6LR to relay its packets within the subnet, and participation to the subnet is constrained to the time of reachability to the 6LR. Note that RSU that provides internet connectivity MAY announce a default router preference [RFC 4191], whereas a car that does not provide that connectivity MUST NOT do so. This operation presents similarities with that of an access point, but at Layer-3. This is why RFC 8505 well-suited for wireless in general.
Support of RFC 8505 may be implemented on OCB. OCB nodes that support RFC 8505 SHOULD support the 6LN operation in order to act as a host, and may support the 6LR and 6LBR operations in order to act as a router and in particular own a prefix that can be used by RFC 8505-compliant hosts for address autoconfiguration and registration.

Authors’ Addresses

Nabil Benamar
Moulay Ismail University of Meknes
Morocco

Phone: +212670832236
Email: n.benamar@est.umi.ac.ma

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

Phone: +33493008134
Email: Jerome.Haerri@eurecom.fr

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan 31066
Republic of Korea

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr
Basic Support for IPv6 over IEEE Std 802.11 Networks Operating Outside the Context of a Basic Service Set
draft-ietf-ipwave-ipv6-over-80211ocb-52

Abstract

This document provides methods and settings, for using IPv6 to communicate among nodes within range of one another over a single IEEE 802.11-OCB link. Support for these methods and settings require minimal changes to existing stacks. This document also describes limitations associated with using these methods. Optimizations and usage of IPv6 over more complex scenarios is not covered in this specification and is subject of future work.

Status of This Memo

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

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

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

This Internet-Draft will expire on February 10, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ............................................. 3
2. Terminology ............................................. 3
3. Communication Scenarios where IEEE 802.11-OCB Links are Used  4
4. IPv6 over 802.11-OCB .................................... 4
   4.1. Maximum Transmission Unit (MTU) ...................... 4
   4.2. Frame Format ....................................... 5
   4.3. Link-Local Addresses ............................... 5
   4.4. Stateless Autoconfiguration .......................... 5
   4.5. Address Mapping .................................... 6
      4.5.1. Address Mapping -- Unicast ..................... 6
      4.5.2. Address Mapping -- Multicast ................... 6
   4.6. Subnet Structure .................................... 7
5. Security Considerations .................................. 8
   5.1. Privacy Considerations ............................. 8
      5.1.1. Privacy Risks of Meaningful info in Interface IDs  9
   5.2. MAC Address and Interface ID Generation ............. 9
   5.3. Pseudonymization impact on confidentiality and trust . 10
6. IANA Considerations ..................................... 10
7. Contributors ............................................. 10
8. Acknowledgements ....................................... 11
9. References .............................................. 12
   9.1. Normative References ............................... 12
   9.2. Informative References ............................. 14
Appendix A. 802.11p ....................................... 16
Appendix B. Aspects introduced by the OCB mode to 802.11 .... 16
Appendix C. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver ............................ 20
Appendix D. Protocol Layering ................................ 21
Appendix E. Design Considerations ........................... 22
Appendix F. IEEE 802.11 Messages Transmitted in OCB mode .... 22
Appendix G. Examples of Packet Formats ...................... 23
   G.1. Capture in Monitor Mode ............................ 24
   G.2. Capture in Normal Mode ............................. 26
Appendix H. Extra Terminology ................................ 28
Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links ............................................ 29
1. Introduction

This document provides a baseline for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link [IEEE-802.11-2016] (a.k.a., "802.11p" see Appendix A, Appendix B and Appendix C) with minimal changes to existing stacks. Moreover, the document identifies limitations of such usage. Concretely, the document describes the layering of IPv6 networking on top of the IEEE Std 802.11 MAC layer or an IEEE Std 802.3 MAC layer with a frame translation underneath. The resulting stack is derived from IPv6 over Ethernet [RFC2464], but operates over 802.11-OCB to provide at least P2P (Point to Point) connectivity using IPv6 ND and link-local addresses.

The IPv6 network layer operates on 802.11-OCB in the same manner as operating on Ethernet with the following exceptions:

- Exceptions due to different operation of IPv6 network layer on 802.11 than on Ethernet. The operation of IP on Ethernet is described in [RFC1042] and [RFC2464].

- Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure and movement detection. Security and privacy recommendations are discussed in Section 5 and Section 4.4. The subnet structure is described in Section 4.6. The movement detection on OCB links is not described in this document. Likewise, ND Extensions and IPWAVE optimizations for vehicular communications are not in scope. The expectation is that further specifications will be edited to cover more complex vehicular networking scenarios.

The reader may refer to [I-D.ietf-ipwave-vehicular-networking] for an overview of problems related to running IPv6 over 802.11-OCB. It is out of scope of this document to reiterate those.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The document makes uses of the following terms: IP-OBU (Internet Protocol On-Board Unit): an IP-OBU denotes a computer situated in a vehicle such as a car, bicycle, or similar. It has at least one IP
interface that runs in mode OCB of 802.11, and that has an "OBU" transceiver. See the definition of the term "OBU" in section Appendix H.

IP-RSU (IP Road-Side Unit): an IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. An IP-RSU communicates with the IP-OBU in the vehicle over 802.11 wireless link operating in OCB mode. An IP-RSU is similar to an Access Network Router (ANR) defined in [RFC3753], and a Wireless Termination Point (WTP) defined in [RFC5415].

OCB (outside the context of a basic service set - BSS): is a mode of operation in which a STA is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality.

802.11-OCB: refers to the mode specified in IEEE Std 802.11-2016 when the MIB attribute dot11OCBActivited is 'true'.

3. Communication Scenarios where IEEE 802.11-OCB Links are Used

The IEEE 802.11-OCB networks are used for vehicular communications, as 'Wireless Access in Vehicular Environments'. In particular, we refer the reader to [I-D.ietf-ipwave-vehicular-networking], that lists some scenarios and requirements for IP in Intelligent Transportation Systems (ITS).

The link model is the following: STA --- 802.11-OCB --- STA. In vehicular networks, STAs can be IP-RSUs and/or IP-OBUs. All links are assumed to be P2P and multiple links can be on one radio interface. While 802.11-OCB is clearly specified, and a legacy IPv6 stack can operate on such links, the use of the operating environment (vehicular networks) brings in new perspectives.

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

The default MTU for IP packets on 802.11-OCB is inherited from [RFC2464] and is, as such, 1500 octets. As noted in [RFC8200], every link on the Internet must have a minimum MTU of 1280 octets, as well as follow the other recommendations, especially with regard to fragmentation.
4.2. Frame Format

IP packets MUST be transmitted over 802.11-OCB media as QoS Data frames whose format is specified in IEEE 802.11 spec [IEEE-802.11-2016].

The IPv6 packet transmitted on 802.11-OCB are immediately preceded by a Logical Link Control (LLC) header and an 802.11 header. In the LLC header, and in accordance with the EtherType Protocol Discrimination (EPD, see Appendix D), the value of the Type field MUST be set to 0x86DD (IPv6). The mapping to the 802.11 data service SHOULD use a ‘priority’ value of 1 (QoS with a ‘Background’ user priority), reserving higher priority values for safety-critical and time-sensitive traffic, including the ones listed in [ETSI-sec-archi].

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers MAY implement IPv6-over-Ethernet as per [RFC2464] and then a frame translation from 802.3 to 802.11 in order to minimize the code changes.

4.3. Link-Local Addresses

There are several types of IPv6 addresses [RFC4291], [RFC4193], that may be assigned to an 802.11-OCB interface. Among these types of addresses only the IPv6 link-local addresses can be formed using an EUI-64 identifier, in particular during transition time, (the time spent before an interface starts using a different address than the LL one).

If the IPv6 link-local address is formed using an EUI-64 identifier, then the mechanism of forming that address is the same mechanism as used to form an IPv6 link-local address on Ethernet links. Moreover, whether or not the interface identifier is derived from the EUI-64 identifier, its length is 64 bits as is the case for Ethernet [RFC2464].

4.4. Stateless Autoconfiguration

The steps a host takes in deciding how to autoconfigure its interfaces in IPv6 are described in [RFC4862]. This section describes the formation of Interface Identifiers for IPv6 addresses of type ‘Global’ or ‘Unique Local’. Interface Identifiers for IPv6 address of type ‘Link-Local’ are discussed in Section 4.3.

The RECOMMENDED method for forming stable Interface Identifiers (IIDs) is described in [RFC8064]. The method of forming IIDs described in Section 4 of [RFC2464] MAY be used during transition
time, in particular for IPv6 link-local addresses. Regardless of how to form the IID, its length is 64 bits, similarly to IPv6 over Ethernet [RFC2464].

The bits in the IID have no specific meaning and the identifier should be treated as an opaque value. The bits ‘Universal’ and ‘Group’ in the identifier of an 802.11-OCB interface are significant, as this is an IEEE link-layer address. The details of this significance are described in [RFC7136].

Semantically opaque IIDs, instead of meaningful IIDs derived from a valid and meaningful MAC address ([RFC2464], Section 4), help avoid certain privacy risks (see the risks mentioned in Section 5.1.1). If semantically opaque IIDs are needed, they may be generated using the method for generating semantically opaque IIDs with IPv6 Stateless Address Autoconfiguration given in [RFC7217]. Typically, an opaque IID is formed starting from identifiers different than the MAC addresses, and from cryptographically strong material. Thus, privacy sensitive information is absent from Interface IDs, because it is impossible to calculate back the initial value from which the Interface ID was first generated.

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose IIDs don’t change too often. It is RECOMMENDED to use the mechanisms described in RFC 7217 to permit the use of Stable IIDs that do not change within one subnet prefix. A possible source for the Net-Iface Parameter is a virtual interface name, or logical interface name, that is decided by a local administrator.

4.5. Address Mapping

Unicast and multicast address mapping MUST follow the procedures specified for Ethernet interfaces specified in Sections 6 and 7 of [RFC2464].

4.5.1. Address Mapping -- Unicast

This document is scoped for Address Resolution (AR) and Duplicate Address Detection (DAD) per [RFC4862].

4.5.2. Address Mapping -- Multicast

The multicast address mapping is performed according to the method specified in section 7 of [RFC2464]. The meaning of the value "3333" mentioned there is defined in section 2.3.1 of [RFC7042].
Transmitting IPv6 packets to multicast destinations over 802.11 links proved to have some performance issues [I-D.ietf-mboned-ieee802-mcast-problems]. These issues may be exacerbated in OCB mode. A future improvement to this specification should consider solutions for these problems.

4.6. Subnet Structure

When vehicles are in close range, a subnet may be formed over 802.11-OCB interfaces (not by their in-vehicle interfaces). A Prefix List conceptual data structure ([RFC4861] Section 5.1) is maintained for each 802.11-OCB interface.

IPv6 Neighbor Discovery protocol (ND) requires reflexive properties (bidirectional connectivity) which is generally, though not always, the case for P2P OCB links. IPv6 ND also requires transitive properties for DAD and AR, so an IPv6 subnet can be mapped on an OCB network only if all nodes in the network share a single physical broadcast domain. The extension to IPv6 ND operating on a subnet that covers multiple OCB links and not fully overlapping (NBMA) is not in scope. Finally, IPv6 ND requires a permanent connectivity of all nodes in the subnet to defend their addresses, in other words very stable network conditions.

The structure of this subnet is ephemeral, in that it is strongly influenced by the mobility of vehicles: the hidden terminal effects appear; the 802.11 networks in OCB mode may be considered as ‘ad-hoc’ networks with an addressing model as described in [RFC5889]. On another hand, the structure of the internal subnets in each vehicle is relatively stable.

As recommended in [RFC5889], when the timing requirements are very strict (e.g., fast-drive-through IP-RSU coverage), no on-link subnet prefix should be configured on an 802.11-OCB interface. In such cases, the exclusive use of IPv6 link-local addresses is RECOMMENDED.

Additionally, even if the timing requirements are not very strict (e.g., the moving subnet formed by two following vehicles is stable, a fixed IP-RSU is absent), the subnet is disconnected from the Internet (i.e., a default route is absent), and the addressing peers are equally qualified (that is, it is impossible to determine that some vehicle owns and distributes addresses to others) the use of link-local addresses is RECOMMENDED.

The baseline ND protocol [RFC4861] MUST be supported over 802.11-OCB links. Transmitting ND packets may prove to have some performance issues as mentioned in Section 4.5.2, and Appendix I. These issues may be exacerbated in OCB mode. Solutions for these problems should
consider the OCB mode of operation. Future solutions to OCB should consider solutions for avoiding broadcast. The best of current knowledge indicates the kinds of issues that may arise with ND in OCB mode; they are described in Appendix I.

Protocols like Mobile IPv6 [RFC6275], [RFC3963] and DNAv6 [RFC6059], which depend on a timely movement detection, might need additional tuning work to handle the lack of link-layer notifications during handover. This is for further study.

5. Security Considerations

Any security mechanism at the IP layer or above that may be carried out for the general case of IPv6 may also be carried out for IPv6 operating over 802.11-OCB.

The OCB operation does not use existing 802.11 link-layer security mechanisms. There is no encryption applied below the network layer running on 802.11-OCB. At the application layer, the IEEE 1609.2 document [IEEE-1609.2] provides security services for certain applications to use; application-layer mechanisms are out of scope of this document. On another hand, a security mechanism provided at networking layer, such as IPsec [RFC4301], may provide data security protection to a wider range of applications.

802.11-OCB does not provide any cryptographic protection, because it operates outside the context of a BSS (no Association Request/Response, no Challenge messages). Therefore, an attacker can sniff or inject traffic while within range of a vehicle or IP-RSU (by setting an interface card’s frequency to the proper range). Also, an attacker may not heed to legal limits for radio power and can use a very sensitive directional antenna; if attackers wish to attack a given exchange they do not necessarily need to be in close physical proximity. Hence, such a link is less protected than commonly used links (wired link or aforementioned 802.11 links with link-layer security).

Therefore, any node can join a subnet, directly communicate with any nodes on the subnet to include potentially impersonating another node. This design allows for a number of threats outlined in Section 3 of [RFC6959]. While not widely deployed, SeND [RFC3971], [RFC3972] is a solution that can address Spoof-Based Attack Vectors.

5.1. Privacy Considerations

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11-OCB interface may involve privacy, MAC address spoofing and IP hijacking risks. A vehicle embarking an IP-
OBU whose egress interface is 802.11-OCB may expose itself to eavesdropping and subsequent correlation of data. This may reveal data considered private by the vehicle owner; there is a risk of being tracked. In outdoors public environments, where vehicles typically circulate, the privacy risks are more important than in indoors settings. It is highly likely that attacker sniffers are deployed along routes which listen for IEEE frames, including IP packets, of vehicles passing by. For this reason, in the 802.11-OCB deployments, there is a strong necessity to use protection tools such as dynamically changing MAC addresses Section 5.2, semantically opaque Interface Identifiers and stable Interface Identifiers Section 4.4. An example of change policy is to change the MAC address of the OCB interface each time the system boots up. This may help mitigate privacy risks to a certain level. Furthermore, for privacy concerns, ([RFC8065]) recommends using an address generation scheme rather than addresses generated from a fixed link-layer address. However, there are some specificities related to vehicles. Since roaming is an important characteristic of moving vehicles, the use of the same Link-Local Address over time can indicate the presence of the same vehicle in different places and thus leads to location tracking. Hence, a vehicle should get hints about a change of environment (e.g., engine running, GPS, etc.) and renew the IID in its LLAs.

5.1.1. Privacy Risks of Meaningful info in Interface IDs

The privacy risks of using MAC addresses displayed in Interface Identifiers are important. The IPv6 packets can be captured easily in the Internet and on-link in public roads. For this reason, an attacker may realize many attacks on privacy. One such attack on 802.11-OCB is to capture, store and correlate Company ID information present in MAC addresses of many cars (e.g. listen for Router Advertisements, or other IPv6 application data packets, and record the value of the source address in these packets). Further correlation of this information with other data captured by other means, or other visual information (car color, others) may constitute privacy risks.

5.2. MAC Address and Interface ID Generation

In 802.11-OCB networks, the MAC addresses may change during well defined renumbering events. In the moment the MAC address is changed on an 802.11-OCB interface all the Interface Identifiers of IPv6 addresses assigned to that interface MUST change.

Implementations should use a policy dictating when the MAC address is changed on the 802.11-OCB interface. For more information on the
motivation of this policy please refer to the privacy discussion in
Appendix B.

A ‘randomized’ MAC address has the following characteristics:

- Bit "Local/Global" set to "locally administered".
- Bit "Unicast/Multicast" set to "Unicast".
- The 46 remaining bits are set to a random value, using a random
  number generator that meets the requirements of [RFC4086].

To meet the randomization requirements for the 46 remaining bits, a
hash function may be used. For example, the [SHA256] hash function
may be used with input a 256 bit local secret, the ‘nominal’ MAC
Address of the interface, and a representation of the date and time
of the renumbering event.

A randomized Interface ID has the same characteristics of a
randomized MAC address, except the length in bits.

5.3. Pseudonymization impact on confidentiality and trust

Vehicles ‘and drivers’ privacy relies on pseudonymization mechanisms
such as the ones described in Section 5.2. This pseudonymization
means that upper-layer protocols and applications SHOULD NOT rely on
layer-2 or layer-3 addresses to assume that the other participant can
be trusted.

6. IANA Considerations

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

Romain Kuntz contributed extensively about IPv6 handovers between
links running outside the context of a BSS (802.11-OCB links).

Tim Leinmueller contributed the idea of the use of IPv6 over
802.11-OCB for distribution of certificates.

Marios Makassikis, Jose Santa Lozano, Albin Severinson and Alexey
Voronov provided significant feedback on the experience of using IP
messages over 802.11-OCB in initial trials.
Michelle Wetterwald contributed extensively the MTU discussion, offered the ETSI ITS perspective, and reviewed other parts of the document.

8. Acknowledgements

The authors would like to thank Alexandre Petrescu for initiating this work and for being the lead author until the version 43 of this draft.

The authors would like to thank Pascal Thubert for reviewing, proofreading and suggesting modifications of this document.

The authors would like to thank Mohamed Boucadair for proofreading and suggesting modifications of this document.

The authors would like to thank Eric Vyncke for reviewing suggesting modifications of this document.

The authors would like to thank Witold Klaudel, Ryuji Wakikawa, Emmanuel Baccelli, John Kenney, John Moring, Francois Simon, Dan Romascanu, Konstantin Khait, Ralph Droms, Richard ‘Dick’ Roy, Ray Hunter, Tom Kurihara, Michal Sojka, Jan de Jongh, Suresh Krishnan, Dino Farinacci, Vincent Park, Jaehoon Paul Jeong, Gloria Gwynne, Hans-Joachim Fischer, Russ Housley, Rex Buddenberg, Erik Nordmark, Bob Moskowitz, Andrew Dryden, Georg Mayer, Dorothy Stanley, Sandra Cespedes, Mariano Falcitelli, Sri Gundavelli, Abdussalam Baryun, Margaret Cullen, Eric Kline, Carlos Jesus Bernardos Cano, Ronald in ’t Velt, Katrin Sjoberg, Roland Bless, Tijink Jasja, Kevin Smith, Brian Carpenter, Julian Reschke, Mikael Abrahamsson, Dirk von Hugo, Lorenzo Colitti, Pascal Thubert, Ole Troan, Jinmei Tatuya, Joel Halpern, Eric Gray and William Whyte. Their valuable comments clarified particular issues and generally helped to improve the document.

Pierre Pfister, Rostislav Lisovy, and others, wrote 802.11-OCB drivers for linux and described how.

For the multicast discussion, the authors would like to thank Owen DeLong, Joe Touch, Jen Linkova, Erik Kline, Brian Haberman and participants to discussions in network working groups.

The authors would like to thank participants to the Birds-of-a-Feather "Intelligent Transportation Systems" meetings held at IETF in 2016.

Human Rights Protocol Considerations review by Amelia Andersdotter.
9. References

9.1. Normative References

[IEEE-802.11-2016]
"IEEE Standard 802.11-2016 - IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Status - Active Standard. Description retrieved freely; the document itself is also freely available, but with some difficulty (requires registration); description and document retrieved on April 8th, 2019, starting from URL https://standards.ieee.org/findstds/standard/802.11-2016.html".


9.2. Informative References

[ETSI-sec-archi]

[I-D.ietf-ipwave-vehicular-networking]

[I-D.ietf-mboned-ieee802-mcast-problems]

[IEEE-1609.2]

[IEEE-1609.3]


Appendix A. 802.11p

The term "802.11p" is an earlier definition. The behaviour of "802.11p" networks is rolled in the document IEEE Std 802.11-2016. In that document the term 802.11p disappears. Instead, each 802.11p feature is conditioned by the IEEE Management Information Base (MIB) attribute "OCBActivated" [IEEE-802.11-2016]. Whenever OCBActivated is set to true the IEEE Std 802.11-OCB state is activated. For example, an 802.11 STAion operating outside the context of a basic service set has the OCBActivated flag set. Such a station, when it has the flag set, uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

Appendix B. Aspects introduced by the OCB mode to 802.11

In the IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. In OCB mode, the manner in which channels are selected and used is simplified compared to when in BSS mode. Contrary to BSS mode, at link layer, it is necessary to set statically the same channel number (or frequency) on two stations that need to communicate with each other (in BSS mode this channel set operation is performed automatically during 'scanning'). The manner in which stations set their channel number in OCB mode is not specified in this document. Stations STA1 and STA2 can exchange IP packets only if they are set on the same channel. At IP layer, they then discover each other by using the IPv6 Neighbor Discovery protocol. The allocation of a particular channel for a particular use is defined statically in standards authored by ETSI (in Europe), FCC in America, and similar organisations in South Korea, Japan and other parts of the world.

Briefly, the IEEE 802.11-OCB mode has the following properties:
The use by each node of a ‘wildcard’ BSSID (i.e., each bit of the BSSID is set to 1)

- No IEEE 802.11 Beacon frames are transmitted
- No authentication is required in order to be able to communicate
- No association is needed in order to be able to communicate
- No encryption is provided in order to be able to communicate
- Flag dot11OCBActivated is set to true

All the nodes in the radio communication range (IP-OBU and IP-RSU) receive all the messages transmitted (IP-OBU and IP-RSU) within the radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

The message exchange diagram in Figure 1 illustrates a comparison between traditional 802.11 and 802.11 in OCB mode. The ‘Data’ messages can be IP packets such as HTTP or others. Other 802.11 management and control frames (non IP) may be transmitted, as specified in the 802.11 standard. For information, the names of these messages as currently specified by the 802.11 standard are listed in Appendix F.

```
STA                      AP                      STA1                   STA2
<------ Beacon ------    <------ Data ------->
---- Probe Req. ------>
<---- Probe Res. ------>
---- Auth Req. ------>
<---- Auth Res. ------>
---- Asso Req. ------>
<---- Asso Res. ------>
<------ Data ------>
<------ Data ------>

(i) 802.11 Infrastructure mode          (ii) 802.11-OCB mode
```

Figure 1: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)
The interface 802.11-OCB was specified in IEEE Std 802.11p (TM) -2010 [IEEE-802.11p-2010] as an amendment to IEEE Std 802.11 (TM) -2007, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, this amendment has been integrated in IEEE 802.11(TM) -2012 and -2016 [IEEE-802.11-2016].

In document 802.11-2016, anything qualified specifically as "OCBAvivated", or "outside the context of a basic service" set to be true, then it is actually referring to OCB aspects introduced to 802.11.

In order to delineate the aspects introduced by 802.11-OCB to 802.11, we refer to the earlier [IEEE-802.11p-2010]. The amendment is concerned with vehicular communications, where the wireless link is similar to that of Wireless LAN (using a PHY layer specified by 802.11a/b/g/n), but which needs to cope with the high mobility factor inherent in scenarios of communications between moving vehicles, and between vehicles and fixed infrastructure deployed along roads. While ‘p’ is a letter identifying the Amendment, just like ‘a, b, g’ and ‘n’ are, ‘p’ is concerned more with MAC modifications, and a little with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a ‘p’ MAC with an ‘a’ PHY by operating outside the context of a BSS with OFDM at 5.4GHz and 5.9GHz.

The 802.11-OCB links are specified to be compatible as much as possible with the behaviour of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11-OCB MAC layer offers practically the same interface to IP as the 802.11a/b/g/n and 802.3. A packet sent by an IP-OBU may be received by one or multiple IP-RSUs. The link-layer resolution is performed by using the IPv6 Neighbor Discovery protocol.

To support this similarity statement (IPv6 is layered on top of LLC on top of 802.11-OCB, in the same way that IPv6 is layered on top of LLC on top of 802.11a/b/g/n (for WLAN) or layered on top of LLC on top of 802.3 (for Ethernet)) it is useful to analyze the differences between 802.11-OCB and 802.11 specifications. During this analysis, we note that whereas 802.11-OCB lists relatively complex and numerous changes to the MAC layer (and very little to the PHY layer), there are only a few characteristics which may be important for an implementation transmitting IPv6 packets on 802.11-OCB links.

The most important 802.11-OCB point which influences the IPv6 functioning is the OCB characteristic; an additional, less direct influence, is the maximum bandwidth afforded by the PHY modulation/demodulation methods and channel access specified by 802.11-OCB. The maximum bandwidth theoretically possible in 802.11-OCB is 54 Mbit/s
(when using, for example, the following parameters: 20 MHz channel; modulation 64-QAM; coding rate R is 3/4); in practice of IP-over-802.11-OCB a commonly observed figure is 12Mbit/s; this bandwidth allows the operation of a wide range of protocols relying on IPv6.

- **Operation Outside the Context of a BSS (OCB):** the (earlier 802.11p) 802.11-OCB links are operated without a Basic Service Set (BSS). This means that the frames IEEE 802.11 Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always 0xffffffffffff (48 '1' bits, represented as MAC address ff:ff:ff:ff:ff:ff, or otherwise the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by administrator (e.g. 'My-Home-AccessPoint'). The OCB operation - namely the lack of beacon-based scanning and lack of authentication - should be taken into account when the Mobile IPv6 protocol [RFC6275] and the protocols for IP layer security [RFC4301] are used. The way these protocols adapt to OCB is not described in this document.

- **Timing Advertisement:** is a new message defined in 802.11-OCB, which does not exist in 802.11a/b/g/n. This message is used by stations to inform other stations about the value of time. It is similar to the time as delivered by a GNSS system (Galileo, GPS, ...) or by a cellular system. This message is optional for implementation.

- **Frequency range:** this is a characteristic of the PHY layer, with almost no impact on the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, ECC/CEPT based on ENs from ETSI, FCC, etc.); as part of the regulation process, specific applications are associated with specific frequency ranges. In the case of 802.11-OCB, the regulator associates a set of frequency ranges, or slots within a band, to the use of applications of vehicular communications, in a band known as "5.9GHz". The 5.9GHz band is different from the 2.4GHz and 5GHz bands used by Wireless LAN. However, as with Wireless LAN, the operation of 802.11-OCB in "5.9GHz" bands is exempt from owning a license in EU (in US the 5.9GHz is a licensed band of spectrum; for the fixed infrastructure an explicit FCC authorization is required; for an on-board device a 'licensed-by-rule' concept applies: rule certification conformity is required.) Technical conditions are different than those of the bands "2.4GHz" or "5GHz". The allowed power levels, and implicitly the maximum allowed distance between vehicles, is of 33dBm for 802.11-OCB (in Europe), compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to a maximum distance of approximately 1km, compared to approximately 50m.
Additionally, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in US) and on the use of frequencies for Intelligent Transportation Systems (in EU), compared to Wireless LAN (802.11a/b/g/n).

- 'Half-rate' encoding: as the frequency range, this parameter is related to PHY, and thus has not much impact on the interface between the IP layer and the MAC layer.
- In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in Section 5. A relevant function is described in documents IEEE 1609.3-2016 [IEEE-1609.3] and IEEE 1609.4-2016 [IEEE-1609.4].

Appendix C. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver

The 802.11p amendment modifies both the 802.11 stack’s physical and MAC layers but all the induced modifications can be quite easily obtained by modifying an existing 802.11a ad-hoc stack.

Conditions for a 802.11a hardware to be 802.11-OCB compliant:

- The PHY entity shall be an orthogonal frequency division multiplexing (OFDM) system. It must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11-OCB layer, in France: 5875MHz to 5925MHz.
- The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.
- The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).
- The chip should be able to transmit up to 44.8 dBm when used by the US government in the United States, and up to 33 dBm in Europe; other regional conditions apply.

Changes needed on the network stack in OCB mode:
Physical layer:

* The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.
* The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).
* The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules, if used by the kernel to enforce local specific restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

MAC layer:

* All management frames (beacons, join, leave, and others) emission and reception must be disabled except for frames of subtype Action and Timing Advertisement (defined below).
* No encryption key or method must be used.
* Packet emission and reception must be performed as in ad-hoc mode, using the wildcard BSSID (ff:ff:ff:ff:ff:ff).
* The functions related to joining a BSS (Association Request/Response) and for authentication (Authentication Request/Reply, Challenge) are not called.
* The beacon interval is always set to 0 (zero).
* Timing Advertisement frames, defined in the amendment, should be supported. The upper layer should be able to trigger such frames emission and to retrieve information contained in received Timing Advertisements.

Appendix D. Protocol Layering

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated in Figure 2. The IP layer operates on top of the EtherType Protocol Discrimination (EPD); this Discrimination layer is described in IEEE Std 802.3-2012; the interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).
Appendix E. Design Considerations

The networks defined by 802.11-OCB are in many ways similar to other networks of the 802.11 family. In theory, the transportation of IPv6 over 802.11-OCB could be very similar to the operation of IPv6 over other networks of the 802.11 family. However, the high mobility, strong link asymmetry and very short connection makes the 802.11-OCB link significantly different from other 802.11 networks. Also, the automotive applications have specific requirements for reliability, security and privacy, which further add to the particularity of the 802.11-OCB link.

Appendix F. IEEE 802.11 Messages Transmitted in OCB mode

For information, at the time of writing, this is the list of IEEE 802.11 messages that may be transmitted in OCB mode, i.e. when dot11OCBActivated is true in a STA:

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;
- The STA MUST send data frames of subtype QoS Data.
Appendix G. Examples of Packet Formats

This section describes an example of an IPv6 Packet captured over a IEEE 802.11-OCB link.

By way of example we show that there is no modification in the headers when transmitted over 802.11-OCB networks - they are transmitted like any other 802.11 and Ethernet packets.

We describe an experiment of capturing an IPv6 packet on an 802.11-OCB link. In topology depicted in Figure 3, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11-OCB interface. The packet is captured on the Host, using a network protocol analyzer (e.g. Wireshark); the capture is performed in two different modes: direct mode and 'monitor' mode. The topology used during the capture is depicted below.

The packet is captured on the Host. The Host is an IP-OBU containing an 802.11 interface in format PCI express (an ITRI product). The kernel runs the ath5k software driver with modifications for OCB mode. The capture tool is Wireshark. The file format for save and analyze is 'pcap'. The packet is generated by the Router. The Router is an IP-RSU (ITRI product).

![Figure 3: Topology for capturing IP packets on 802.11-OCB](image)

During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.
G.1. Capture in Monitor Mode

The IPv6 RA packet captured in monitor mode is illustrated below. The radio tap header provides more flexibility for reporting the characteristics of frames. The Radiotap Header is prepended by this particular stack and operating system on the Host machine to the RA packet received from the network (the Radiotap Header is not present on the air). The implementation-dependent Radiotap Header is useful for piggybacking PHY information from the chip’s registers as data in a packet understandable by userland applications using Socket interfaces (the PHY interface can be, for example: power levels, data rate, ratio of signal to noise).

The packet present on the air is formed by IEEE 802.11 Data Header, Logical Link Control Header, IPv6 Base Header and ICMPv6 Header.

Radiotap Header v0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Header Revision| Header Pad | Header length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Present flags |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data Rate | Pad |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

IEEE 802.11 Data Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type/Subtype and Frame Ctrl |  Duration |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Receiver Address...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... Receiver Address | Transmitter Address...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... Transmitter Address |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| BSS Id...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... BSS Id | Frag Number and Seq Number |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Logical-Link Control Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| DSAP |I| SSAP |C | Control field | Org. code... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| ... Organizational Code | Type |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
The value of the Data Rate field in the Radiotap header is set to 6 Mb/s. This indicates the rate at which this RA was received.

The value of the Transmitter address in the IEEE 802.11 Data Header is set to a 48bit value. The value of the destination address is 33:33:00:00:00:1 (all-nodes multicast address). The value of the BSS Id field is ff:ff:ff:ff:ff:ff, which is recognized by the network protocol analyzer as being "broadcast". The Fragment number and sequence number fields are together set to 0x90C6.
The value of the Organization Code field in the Logical-Link Control Header is set to 0x0, recognized as "Encapsulated Ethernet". The value of the Type field is 0x86DD (hexadecimal 86DD, or otherwise #86DD), recognized as "IPv6".

A Router Advertisement is periodically sent by the router to multicast group address ff02::1. It is an icmp packet type 134. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags, as described in [RFC4861].

The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1.

The Ethernet Type field in the logical-link control header is set to 0x86dd which indicates that the frame transports an IPv6 packet. In the IEEE 802.11 data, the destination address is 33:33:00:00:00:01 which is the corresponding multicast MAC address. The BSS id is a broadcast address of ff:ff:ff:ff:ff:ff. Due to the short link duration between vehicles and the roadside infrastructure, there is no need in IEEE 802.11-OCB to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11-OCB enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.

G.2. Capture in Normal Mode

The same IPv6 Router Advertisement packet described above (monitor mode) is captured on the Host, in the Normal mode, and depicted below.
Ethernet II Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Destination...                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Source...                                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Type                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

IPv6 Base Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Router Advertisement
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Reachable Time                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Retrans Timer                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
One notices that the Radiotap Header, the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On the other hand, a new header named Ethernet II Header is present.

The Destination and Source addresses in the Ethernet II header contain the same values as the fields Receiver Address and Transmitter Address present in the IEEE 802.11 Data Header in the "monitor" mode capture.

The value of the Type field in the Ethernet II header is 0x86DD (recognized as "IPv6"); this value is the same value as the value of the field Type in the Logical-Link Control Header in the "monitor" mode capture.

The knowledgeable experimenter will no doubt notice the similarity of this Ethernet II Header with a capture in normal mode on a pure Ethernet cable interface.

A frame translation is inserted on top of a pure IEEE 802.11 MAC layer, in order to adapt packets, before delivering the payload data to the applications. It adapts 802.11 LLC/MAC headers to Ethernet II headers. In further detail, this adaptation consists in the elimination of the Radiotap, 802.11 and LLC headers, and in the insertion of the Ethernet II header. In this way, IPv6 runs straight over LLC over the 802.11-OCB MAC layer; this is further confirmed by the use of the unique Type 0x86DD.

Appendix H. Extra Terminology

The following terms are defined outside the IETF. They are used to define the main terms in the main terminology Section 2.

DSRC (Dedicated Short Range Communication): a term defined outside the IETF. The US Federal Communications Commission (FCC) Dedicated Short Range Communication (DSRC) is defined in the Code of Federal Regulations (CFR) 47, Parts 90 and 95. This Code is referred in the definitions below. At the time of the writing of this Internet Draft, the last update of this Code was dated October 1st, 2010.

DSRCS (Dedicated Short-Range Communications Services): a term defined outside the IETF. The use of radio techniques to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments. DSRCS systems may also transmit status and instructional messages related to the units involve. [Ref. 47 CFR 90.7 - Definitions]
OBU (On-Board Unit): a term defined outside the IETF. An On-Board Unit is a DSRCS transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of the respective chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of the respective chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands. - [CFR 90.7 - Definitions].

RSU (Road-Side Unit): a term defined outside of IETF. A Roadside Unit is a DSRCS transceiver that is mounted along a road or pedestrian passageway. An RSU may also be mounted on a vehicle or is hand carried, but it may only operate when the vehicle or hand-carried unit is stationary. Furthermore, an RSU operating under the respective part is restricted to the location where it is licensed to operate. However, portable or hand-held RSUs are permitted to operate where they do not interfere with a site-licensed operation. A RSU broadcasts data to OBUs or exchanges data with OBUs in its communications zone. An RSU also provides channel assignments and operating instructions to OBUs in its communications zone, when required. - [CFR 90.7 - Definitions].

Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861][RFC4862] was designed for point-to-point and transit links such as Ethernet, with the expectation of a cheap and reliable support for multicast from the lower layer. Section 3.2 of RFC 4861 indicates that the operation on Shared Media and on non-broadcast multi-access (NBMA) networks require additional support, e.g., for Address Resolution (AR) and duplicate address detection (DAD), which depend on multicast. An infrastructureless radio network such as OCB shares properties with both Shared Media and NBMA networks, and then adds its own complexity, e.g., from movement and interference that allow only transient and non-transitive reachability between any set of peers.

The uniqueness of an address within a scoped domain is a key pillar of IPv6 and the base for unicast IP communication. RFC 4861 details the DAD method to avoid that an address is duplicated. For a link local address, the scope is the link, whereas for a Globally Reachable address the scope is much larger. The underlying assumption for DAD to operate correctly is that the node that owns an
IPv6 address can reach any other node within the scope at the time it claims its address, which is done by sending a NS multicast message, and can hear any future claim for that address by another party within the scope for the duration of the address ownership.

In the case of OCB, there is a potentially a need to define a scope that is compatible with DAD, and that cannot be the set of nodes that a transmitter can reach at a particular time, because that set varies all the time and does not meet the DAD requirements for a link local address that could possibly be used anytime, anywhere. The generic expectation of a reliable multicast is not ensured, and the operation of DAD and AR (Address Resolution) as specified by RFC 4861 cannot be guaranteed. Moreover, multicast transmissions that rely on broadcast are not only unreliable but are also often detrimental to unicast traffic (see [draft-ietf-mboned-ieee802-mcast-problems]).

Early experience indicates that it should be possible to exchange IPv6 packets over OCB while relying on IPv6 ND alone for DAD and AR (Address Resolution) in good conditions. In the absence of a correct DAD operation, a node that relies only on IPv6 ND for AR and DAD over OCB should ensure that the addresses that it uses are unique by means others than DAD. It must be noted that deriving an IPv6 address from a globally unique MAC address has this property but may yield privacy issues.

RFC 8505 provides a more recent approach to IPv6 ND and in particular DAD. RFC 8505 is designed to fit wireless and otherwise constrained networks whereby multicast and/or continuous access to the medium may not be guaranteed. RFC 8505 Section 5.6 "Link-Local Addresses and Registration" indicates that the scope of uniqueness for a link local address is restricted to a pair of nodes that use it to communicate, and provides a method to assert the uniqueness and resolve the link-Layer address using a unicast exchange.

RFC 8505 also enables a router (acting as a 6LR) to own a prefix and act as a registrar (acting as a 6LBR) for addresses within the associated subnet. A peer host (acting as a 6LN) registers an address derived from that prefix and can use it for the lifetime of the registration. The prefix is advertised as not onlink, which means that the 6LN uses the 6LR to relay its packets within the subnet, and participation to the subnet is constrained to the time of reachability to the 6LR. Note that RSU that provides internet connectivity MAY announce a default router preference [RFC4191], whereas a car that does not provide that connectivity MUST NOT do so. This operation presents similarities with that of an access point, but at Layer-3. This is why RFC 8505 well-suited for wireless in general.
Support of RFC 8505 may be implemented on OCB. OCB nodes that support RFC 8505 SHOULD support the 6LN operation in order to act as a host, and may support the 6LR and 6LBR operations in order to act as a router and in particular own a prefix that can be used by RFC 8505-compliant hosts for address autoconfiguration and registration.

Authors’ Addresses

Nabil Benamar
Moulay Ismail University of Meknes
Morocco

Phone: +212670832236
Email: n.benamar@est.umi.ac.ma

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

Phone: +33493008134
Email: Jerome.Haerri@eurecom.fr

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan 31066
Republic of Korea

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr
IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-09

Abstract

This document discusses the problem statement and use cases of IP-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document explains use cases using V2V, V2I, and V2X networking. Next, it makes a problem statement about key aspects in IP-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document specifies requirements in IP-based vehicular networking, and suggests the direction of solutions satisfying those requirements.

Status of This Memo

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

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

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

This Internet-Draft will expire on November 25, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1. Introduction

Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC] in the Intelligent Transportation Systems (ITS) with the frequency band of 5.850 - 5.925 GHz (i.e., 5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. Also, the European Union (EU) passed a decision to allocate a radio spectrum for safety-related and non-safety-related
applications of ITS with the frequency band of 5.875 - 5.905 GHz, which is called Commission Decision 2008/671/EC [EU-2008-671-EC].

For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety services based on the DSRC in terms of standards for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC of the DSRC, while IEEE 1609.2 [WAVE-1609.2] covers security aspects, IEEE 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE 1609.4 [WAVE-1609.4] specifies the multi-channel operation. Note that IEEE 802.11p was a separate standard, but was later enrolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set in 2012 [IEEE-802.11-OCB].

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC5944], MIPv6 [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213][RFC5844]) can be applied (or easily modified) to vehicular networks. In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. Note that a GN protocol is useful to route an event or notification message to vehicles around a geographic position, such as an accident area in a roadway. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].

This document explains use cases and a problem statement about IP-based vehicular networking for ITS, which is named IP Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in the ITS. Next, it makes a problem statement about key aspects in IPWAVE, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect of the problem statement, this document specifies requirements in IP-based vehicular networking, and proposes the direction of solutions fulfilling those requirements. Therefore, with the problem statement, this document will open a door to develop key protocols for IPWAVE that will be essential to IP-based vehicular networks in near future.

2. Terminology

This document uses the following definitions:

- DMM: Acronym for "Distributed Mobility Management" [RFC7333][RFC7429].
o LiDAR: Acronym for "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.

o Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support their address autoconfiguration and mobility management with a binding table. It has end-to-end connections with RSUs under its control.

o On-Board Unit (OBU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and Cellular V2X (C-V2X) [TS-23.285-3GPP]) 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.

o OCB: Acronym for "Outside the Context of a Basic Service Set" [IEEE-802.11-OCB].

o Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) 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.

o 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.

o Vehicle: A node that has an OBU for wireless communication with other vehicles and RSUs. It has a radio navigation receiver of Global Positioning System (GPS) for efficient navigation.

o Vehicular Ad Hoc Network (VANET): A network that consists of vehicles interconnected by wireless communication. Since VANET is a connected network component, two vehicles in a VANET can communicate with each other through ad hoc routing via other vehicles as relays even where they are out of one-hop wireless communication range.

o Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network nodes.
Vehicle Detection Loop (i.e., Loop Detector): An inductive device used for detecting vehicles passing or arriving at a certain point, for instance, at an intersection with traffic lights or at a ramp toward a highway. The relatively crude nature of the loop’s structure means that only metal masses above a certain size are capable of triggering the detection.

V2I2P: Acronym for "Vehicle to Infrastructure to Pedestrian".

V2I2V: Acronym for "Vehicle to Infrastructure to Vehicle".

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

3. Use Cases

This section explains use cases of V2V, V2I, and V2X networking. The use cases of the V2X networking exclude the ones of the V2V and V2I networking, but include Vehicle-to-Pedestrian (V2P) and Vehicle-to-Device (V2D).

3.1. V2V

The use cases of V2V networking discussed in this section include

- Context-aware navigation for driving safety and collision avoidance;
- Cooperative adaptive cruise control in an urban roadway;
- Platooning in a highway;
- Cooperative environment sensing.

These four techniques will be important elements for self-driving vehicles.

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely by letting the drivers recognize dangerous obstacles and situations. That is, CASD navigator displays obstacles or neighboring vehicles relevant to possible collisions in real-time through V2V networking. CASD provides vehicles with a class-based automatic safety action plan, which considers three situations, such as the Line-of-Sight unsafe, Non-Line-of-Sight unsafe, and safe situations. This action plan can be performed among vehicles through V2V networking.
Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles in an urban roadway or a highway. Thus, CACC can help adjacent vehicles to efficiently adjust their speed in an interactive way through V2V networking in order to avoid collision.

Platooning [Truck-Platooning] allows a series of vehicles (e.g., trucks) to move together with a very short inter-distance. Trucks can use V2V communication in addition to forward sensors in order to maintain constant clearance between two consecutive vehicles at very short gaps (from 3 meters to 10 meters). This platooning can maximize the throughput of vehicular traffic in a highway and reduce the gas consumption because the leading vehicle can help the following vehicles to experience less air resistance.

Cooperative-environment-sensing use cases suggest that vehicles can share environmental information from various vehicle-mounted sensors, such as radars, LiDARs, and cameras with other vehicles and pedestrians. [Automotive-Sensing] introduces a millimeter-wave vehicular communication for massive automotive sensing. Data generated by those sensors can be substantially large, and these data shall be routed to different destinations. In addition, from the perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver-operated vehicles. Through the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the context.

3.2. V2I

The use cases of V2I networking discussed in this section include

- Navigation service;
- Energy-efficient speed recommendation service;
- Accident notification service.

A navigation service, such as the Self-Adaptive Interactive Navigation Tool (called SAINT) [SAINT], using V2I networking interacts with TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles for appropriate navigation paths in real time. The enhanced version of SAINT [SAINTplus] can give the fast moving paths to emergency vehicles (e.g., ambulance and fire engine) to let them reach an accident spot while providing other vehicles near the accident spot with efficient detour paths.
A TCC can recommend an energy-efficient speed to a vehicle driving in different traffic environments. [Fuel-Efficient] studies fuel-efficient route and speed plans for platooned trucks.

The emergency communication between accident vehicles (or emergency vehicles) and TCC can be performed via either RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, such as emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to the FirstNet’s network core. The current RAN is mainly constructed by 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Report], but it is expected that DSRC-based vehicular networks [DSRC] will be available for V2I and V2V in near future.

3.3. V2X

The use case of V2X networking discussed in this section is pedestrian protection service.

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., WiFi) with an RSU. Vehicles and pedestrians can also communicate with each other via an RSU that delivers scheduling information for wireless communication in order to save the smartphones’ battery through sleeping mode.

For Vehicle-to-Pedestrian (V2P), a vehicle and a pedestrian’s smartphone can directly communicate with each other via V2X without the relaying of an RSU as in the V2V scenario that the pedestrian’s smartphone is regarded as a vehicle with a wireless media interface to be able to communicate with another vehicle. In Vehicle-to-Device (V2D), a device can be a mobile node such as bicycle and motorcycle, and can communicate directly with a vehicle for collision avoidance.

4. Vehicular Networks

This section describes a vehicular network architecture supporting V2V, V2I, and V2X communications in vehicular networks. Also, it describes an internal network within a vehicle or RSU, and the internetworking between the internal networks via DSRC links.
4.1. Vehicular Network Architecture

Figure 1 shows an architecture for V2I and V2V networking in a road network. As shown in this figure, RSUs as routers and vehicles with OBU have wireless media interfaces for VANET. Also, it is assumed that such the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking.

Especially, for IPv6 packets transporting over IEEE 802.11-OCB, [IPv6-over-802.11-OCB] specifies several details, such as Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. Especially, an Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC...
layer and IPv6 network layer, which is located between IEEE 802.11-OCB’s logical link control layer and IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IP-based vehicular networks.

In Figure 1, three RSUs (RSU1, RSU2, and RSU3) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of RSUs and vehicles in the road network. A Mobility Anchor (MA) is located in the TCC as its key component for the mobility management of vehicles. Two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and one vehicle (Vehicle3) is wirelessly connected to RSU2. The wireless networks of RSU1 and RSU2 belong to two different subnets (denoted as Subnet1 and Subnet2), respectively. Also, another vehicle (Vehicle4) is wireless connected to RSU3, belonging to another subnet (denoted as Subnet3).

In wireless subnets in vehicular networks (e.g., Subnet1 and Subnet2 in Figure 1), vehicles can construct a connected VANET (with an arbitrary graph topology) and can communicate with each other via V2V communication. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the wireless communication range for each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., RSU2 and RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range for each other.

In vehicular networks, unidirectional links exist and must be considered for wireless communications. Also, in the vehicular networks, control plane can be separated from data plane for efficient mobility management and data forwarding using Software-Defined Networking (SDN) [SDN-DMM]. The mobility information of a GPS receiver mounted in its vehicle (e.g., trajectory, position, speed, and direction) can be used for the accommodation of mobility-aware proactive protocols. Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275] and PMIPv6 [RFC5213], so the TCC maintains the mobility information of vehicles for location management. Also, IP tunneling over the wireless link should be avoided for performance efficiency.

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle’s internal network (i.e., moving network) and an RSU’s internal network (i.e., fixed network) via V2I communication.
Nowadays, a vehicle’s internal network tends to be Ethernet to interconnect electronic control units in a vehicle. It can also support WiFi and Bluetooth to accommodate a driver’s and passenger’s mobile devices (e.g., smartphone and tablet). In this trend, it is reasonable to consider a vehicle’s internal network (i.e., moving network) and also the interaction between the internal network and an external network within another vehicle or RSU.

As shown in Figure 2, the vehicle’s moving network and the RSU’s fixed network are self-contained networks having multiple subnets and having an edge router for the communication with another vehicle or RSU. Internetworking between two internal networks via V2I communication requires an exchange of network prefix and other parameters through a prefix discovery mechanism, such as ND-based prefix discovery [ID-Vehicular-ND]. For the ND-based prefix discovery, network prefixes and parameters should be registered into a vehicle’s router and an RSU router with an external network interface in advance.

Figure 2: Internetworking between Vehicle Network and RSU Network
The network parameter discovery collects networking information for an IP communication between a vehicle and an RSU or between two neighboring vehicles, such as link layer, MAC layer, and IP layer information. The link layer information includes wireless link layer parameters, such as wireless media (e.g., IEEE 802.11-OCB and LTE-V2X) and a transmission power level. The MAC layer information includes the MAC address of an external network interface for the internetworking with another vehicle or RSU. The IP layer information includes the IP address and prefix of an external network interface for the internetworking with another vehicle or RSU.

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle’s moving network and the RSU’s fixed network. DNS services should be supported to enable name resolution for hosts or servers residing either in the vehicle’s moving network or the RSU’s fixed network. It is assumed that the DNS names of in-vehicle devices and their service names are registered into a DNS server in a vehicle or an RSU, as shown in Figure 2.

Figure 2 shows internetworking between the vehicle’s moving network and the RSU’s fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Fixed Network1) inside RSU1. RSU1 has the DNS Server (DNS2), one host (Host3), the two routers (Router3 and Router4), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1’s Router1 (called mobile router) and RSU1’s Router3 (called fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for I2V networking. Thus, one host (Host1) in Vehicle1 can communicate with one server (Server1) in RSU1 for a vehicular service through Vehicle1’s moving network, a wireless link between Vehicle1 and RSU1, and RSU1’s fixed network.

4.3. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles via V2V communication.
Figure 3 shows internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (DNS3), the two hosts (Host4 and Host5), and the two routers (Router5 and Router6).

Vehicle1’s Router1 (called mobile router) and Vehicle2’s Router5 (called mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. Thus, one host (Host1) in Vehicle1 can communicate with one host (Host4) in Vehicle1 for a vehicular service through Vehicle1’s moving network, a wireless link between Vehicle1 and Vehicle2, and Vehicle2’s moving network.
Figure 4 shows multihop internetworking between the moving networks of two vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host6 in Vehicle3 via Router 5 in Vehicle2 that is an intermediate vehicle being connected to Vehicle1 and Vehicle3 in a linear topology as shown in the figure.

5. Problem Statement

This section makes a problem statement about key topics for IPWAVE WG, such as neighbor discovery, mobility management, and security & privacy.

5.1. Neighbor Discovery

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for point-to-point links and transit links (e.g., Ethernet). It assumes an efficient and reliable support of multicast from the link layer for various network operations such as MAC Address Resolution (AR) and Duplicate Address Detection (DAD).

IPv6 ND needs to be extended to vehicular networking (e.g., V2V, V2I, and V2X) in terms of DAD and ND-related parameters (e.g., Router Lifetime). The vehicles are moving fast within the communication coverage of a vehicular node (e.g., vehicle and RSU). Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and recognize each other in the aspect of IPv6 ND.
The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks.

The vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD, and two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and RSUs, as shown in Figure 1. By using the vehicular-network-wide DAD, vehicles can assure that their IPv6 addresses are unique in the vehicular network whenever they are connected to the vehicular infrastructure or become disconnected from it in the form of VANET. Even though a unique IPv6 address can be derived from a globally unique MAC address, this derivation yields a privacy issue of a vehicle as an IPv6 node. The vehicular infrastructure having RSUs and an MA can participate in the vehicular-network-wide DAD for the sake of vehicles [RFC6775][RFC8505].

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval should be adjusted for high-speed vehicles and vehicle density. As vehicles move faster, the NA interval should decrease (e.g., from 1 sec to 0.5 sec) for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase (e.g., from 0.5 sec to 1 sec) for the NA messages to reduce collision probability with other NA messages.

When ND is used in vehicular networks, the communication delay (i.e., latency) between two vehicles should be bounded to a certain threshold (e.g., 500 ms) for collision-avoidance message exchange [CASD]. For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. The real implementations for such applications are not available yet. Thus, ND needs to appropriately operate to support IP-based safety applications.

5.1.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in a vehicular wireless link [VIP-WAVE] [RFC5889]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces. However, interference and different levels of transmission power may cause unidirectional links to appear in vehicular wireless links. As a result, a new vehicular
link model is required for a dynamically changing vehicular wireless link.

There is a relationship between a link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IP link.

A VANET can have multiple links between pairs of vehicles within wireless communication range, as shown in Figure 4. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Assume that a global-scope IPv6 prefix is assigned to VANETs in vehicular networks. Even though two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, they may not communicate with each other not in a one hop in the same VANET because of the multihop network connectivity. Thus, in this case, the concept of a on-link IPv6 prefix does not hold because two vehicles with the same on-link IPv6 prefix cannot communicate directly with each other. Also, when two vehicles are located in two different VANETs with the same IPv6 prefix, they cannot communicate with each other. When these two VANETs are converged into one VANET, the two vehicles can communicate with each other in a multihop fashion. Therefore, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility.

An IPv6 prefix can be used in a multi-link subnet as an extended subnet. IPv6 Stateless Address Autoconfiguration (SLAAC) needs to be performed even in the multiple links where all of the links are configured with the same subnet prefix [RFC4861][RFC4862]. Thus, a vehicular link model can consider a multi-hop V2V (or V2I) over a multi-link subnet in a vehicular network having multiple VANETs and RSUs, as shown in Figure 1. For example, in this figure, vehicles (i.e., Vehicle1, Vehicle2, and Vehicle3) in Subnet1 and Subnet2 having RSU1 and RSU2, respectively, construct a multi-link subnet with VANETs and RSUs. Vehicle1 and Vehicle3 can also communicate with each other via either multi-hop V2V or multi-hop V2I2V. When two vehicles (e.g., Vehicle1 and Vehicle3 in Figure 1) are connected in a VANET, it will be more efficient for them to communicate with each other via VANET rather than RSUs. On the other hand, when two vehicles (e.g., Vehicle1 and Vehicle3) are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V.

Therefore, IPv6 ND needs to be extended for an efficient Vehicular Neighbor Discovery (VND) to support the concept of an IPv6 link.
corresponding to an IPv6 prefix even in a multi-link subnet consisting of multiple vehicles and RSUs [ID-Vehicular-ND].

5.1.2. MAC Address Pseudonym

For the protection of drivers’ privacy, the pseudonym of a MAC address of a vehicle’s network interface should be used, with the help of which the MAC address can be changed periodically. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP) session with an IPv6 address pair. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

In the ETSI standards, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities (e.g., MAC address) and the corresponding IPv6 addresses [Identity-Management]. Whenever the network interface identifier changes, the IPv6 address based on the network interface identifier should be updated, and the uniqueness of the address should be performed through the DAD procedure. For vehicular networks with high-mobility, this DAD should be performed efficiently with minimum overhead.

For the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, with a mobility management scheme (e.g., MIPv6 and PMIPv6), the new IP address for the transport-layer session can be notified to an appropriate end point, and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address. This mobility management overhead for pseudonyms should be minimized for efficient operations in vehicular networks having lots of vehicles.

5.1.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes in within the internal networks of two vehicular nodes (e.g., vehicle and RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is required. It is assumed that a vehicular node has an external network interface and its internal network, as shown in Figure 2 and Figure 3. The vehicular ND (VND) [ID-Vehicular-ND] can support the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) of vehicular nodes with a vehicular prefix information option. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without a vehicular ad hoc routing protocol (e.g., AODV [RFC3561] and OLSRv2 [RFC7181]).
5.1.4. Routing

For multihop V2V communications in a VANET (or a multi-link subnet), a vehicular ad hoc routing protocol (e.g., AODV and OLSRv2) may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead. As a feasible approach, Vehicular ND can be extended to accommodate routing functionality with a prefix discovery option. In this case, there is no need to run a separate vehicular ad hoc routing protocol in VANETs. The ND extension can allow vehicles to exchange their prefixes in a multihop fashion [ID-Vehicular-ND]. With the exchanged prefixes, they can compute their routing table (or IPv6 ND’s neighbor cache) for the multi-link subnet with a distance-vector algorithm [Intro-to-Algorithms].

Also, an efficient, rapid DAD needs to be supported in a vehicular network having multiple VANETs (or a multi-link subnet) to prevent or reduce IPv6 address conflicts in such a subnet. A feasible approach is to use a multi-hop DAD optimization for the efficient vehicular-network-wide DAD [RFC6775][RFC8505].

5.2. Mobility Management

The seamless connectivity and timely data exchange between two end points requires an efficient mobility management including location management and handover. Most of vehicles are equipped with a GPS receiver as part of a dedicated navigation system or a corresponding smartphone App. The GPS receiver may not provide vehicles with accurate location information in adverse, local environments such as building area and tunnel. The location precision can be improved by the assistance from the RSUs or a cellular system with a GPS receiver for location information.

With a GPS navigator, an efficient mobility management will be possible by vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having RSUs and an MA in TCC) [ID-Vehicular-MM]. This vehicular infrastructure can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the efficient mobility management (e.g., proactive handover). For a better proactive handover, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]), can be used to determine the moment of a handover between RSUs along with mobility information.
With the prediction of the vehicle mobility, the vehicular infrastructure needs to support RSUs to perform efficient DAD, data packet routing, horizontal handover (i.e., handover in wireless links using a homogeneous radio technology), and vertical handover (i.e., handover in wireless links using heterogeneous radio technologies) in a proactive manner [ID-Vehicular-MM]. For example, when a vehicle is moving into the wireless link under another RSU belonging to a different subnet, the RSU can proactively perform the DAD for the sake of the vehicle, reducing IPv6 control traffic overhead in the wireless link. To prevent a hacker from impersonating RSUs as bogus RSUs, RSUs and MA in the vehicular infrastructure need to have secure channels via IPsec.

Therefore, with a proactive handover and a multihop DAD in vehicular networks, RSUs needs to efficiently forward data packets from the wired network (or the wireless network) to a moving destination vehicle along its trajectory. As a result, a moving vehicle can communicate with its corresponding vehicle in the vehicular network or a host/server in the Internet along its trajectory.

5.3. Security and Privacy

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe. Sybil attack, which tries to illude a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. This sybil attack should be prevented through the cooperation between good vehicles and RSUs. Applications on IP-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device’s identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., RSU) connected to an authentication server in TCC. Also, Transport Layer Security (TLS) certificates can be used for secure E2E vehicle communications.
For secure V2I communication, a secure channel between a mobile router in a vehicle and a fixed router in an RSU should be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym should be provided to the vehicle; that is, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicular nodes (e.g., vehicle and RSU) in terms of transport layer for a long-living higher-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IP addresses, because an adversary can see the change of the MAC and IP addresses and track the vehicle with those addresses.

6. Security Considerations

This document discussed security and privacy for IP-based vehicular networking.

The security and privacy for key components in IP-based vehicular networking, such as neighbor discovery and mobility management, need to be analyzed in depth.

7. Informative References

[Automotive-Sensing]

[CA-Cruise-Control]


[ISO-ITS-IPv6]  

[RFC3561]  

[RFC4086]  

[RFC4861]  

[RFC4862]  

[RFC4941]  

[RFC5213]  

[RFC5844]  

[RFC5889]  

[RFC5944]  

[RFC6275]  

[RFC6775]  

[RFC7181]  


[VIP-WAVE]

[WAVE-1609.0]

[WAVE-1609.2]

[WAVE-1609.3]

[WAVE-1609.4]
Appendix A. Changes from draft-ietf-ipwave-vehicular-networking-08

The following changes are made from draft-ietf-ipwave-vehicular-networking-08:

- This version is revised based on the comments from Charlie Perkins and Sri Gundavelli.
- This version focuses on the problem statement about IP-based vehicular networking, such as IPv6 neighbor discovery, mobility management, and security & privacy.

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 the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2017-0-01633) supervised by the IITP (Institute for Information & communications Technology Promotion).

This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

Appendix C. Contributors

This document is a group work of IPWAVE working group, greatly benefiting from inputs and texts by Rex Buddenberg (Naval Postgraduate School), Thierry Ernst (YoGoKo), Bokor Laszlo (Budapest University of Technology and Economics), Jose Santa Lozanoi (Universidad of Murcia), Richard Roy (MIT), Francois Simon (Pilot), Sri Gundavelli (Cisco), Erik Nordmark, Dirk von Hugo (Deutsche Telekom), and Pascal Thubert (Cisco). The authors sincerely appreciate their contributions.

The following are co-authors of this document:

Nabil Benamar
Department of Computer Sciences
High School of Technology of Meknes
Moulay Ismail University
Morocco

Phone: +212 6 70 83 22 36
EMail: benamar73@gmail.com
IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases

draft-ietf-ipwave-vehicular-networking-11

Abstract

This document discusses the problem statement and use cases of IP-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document explains use cases using V2V, V2I, and V2X networking. Next, it makes a problem statement about key aspects in IP-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document specifies requirements in IP-based vehicular networking, and suggests the direction of solutions satisfying those requirements.

Status of This Memo

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

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

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

This Internet-Draft will expire on January 21, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
Table of Contents

1. Introduction .................................................. 2
2. Terminology ..................................................... 3
3. Use Cases ....................................................... 5
   3.1. V2V ....................................................... 5
   3.2. V2I ....................................................... 6
   3.3. V2X ....................................................... 7
4. Vehicular Networks .............................................. 7
   4.1. Vehicular Network Architecture ................................ 8
   4.2. V2I-based Internetworking ................................... 9
   4.3. V2V-based Internetworking .................................. 11
5. Problem Statement ............................................... 13
   5.1. Neighbor Discovery ......................................... 13
       5.1.1. Link Model ........................................... 14
       5.1.2. MAC Address Pseudonym ................................ 16
       5.1.3. Prefix Dissemination/Exchange .......................... 16
       5.1.4. Routing ............................................... 17
   5.2. Mobility Management ....................................... 17
   5.3. Security and Privacy ...................................... 18
6. Security Considerations ......................................... 19
7. Informative References ......................................... 19
Appendix A. Changes from draft-ietf-ipwave-vehicular-networking-10 ........................................... 25
Appendix B. Acknowledgments ...................................... 25
Appendix C. Contributors .......................................... 25
Author’s Address .................................................. 27

1. Introduction

Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC] in the Intelligent Transportation Systems (ITS) with the frequency band of 5.850 - 5.925 GHz (i.e., 5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. The European Union (EU) allocated radio spectrum for safety-related and non-safety-related applications of ITS with the
frequency band of 5.875 - 5.905 GHz, as part of the Commission Decision 2008/671/EC [EU-2008-671-EC].

For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety services based on DSRC for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC of the DSRC, while IEEE 1609.2 [WAVE-1609.2] covers security aspects, IEEE 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE 1609.4 [WAVE-1609.4] specifies the multi-channel operation. IEEE 802.11p was first a separate amendment, but was later rolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) in 2012 [IEEE-802.11-OCB].

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC5004], MIPv6 [RFC6275], and Proxy MIPv6 [RFC5213][RFC5844]) can be applied to vehicular networks. In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. GN protocols are useful to route an event or notification message to vehicles around a geographic position, such as an accident area in a roadway. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].

This document describes use cases and a problem statement about IP-based vehicular networking for ITS, which is named IP Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, it makes a problem statement about key aspects in IPWAVE, namely, IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect of the problem statement, this document specifies requirements in IP-based vehicular networking, and proposes the direction of solutions fulfilling those requirements. This document is intended to motivate development of key protocols for IPWAVE.

2. Terminology

This document uses the following definitions:

- LiDAR: "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.
o Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support their address autoconfiguration and mobility management with a binding table. An MA has end-to-end connections with RSUs under its control.

o On-Board Unit (OBU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and Cellular V2X (C-V2X) [TS-23.285-3GPP]) 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.

o OCB: "Outside the Context of a Basic Service Set" [IEEE-802.11-OCB].

o Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) 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 a car parking area.

o 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.

o Vehicle: A Vehicle in this document is a node that has an OBU for wireless communication with other vehicles and RSUs. It has a radio navigation receiver of Global Positioning System (GPS) for efficient navigation.

o Vehicular Ad Hoc Network (VANET): A network that consists of vehicles interconnected by wireless communication. Two vehicles in a VANET can communicate with each other using other vehicles as relays even where they are out of one-hop wireless communication range.

o Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network forwarding elements (e.g., switch and router).

o Vehicle Detection Loop (i.e., Loop Detector): An inductive device used for detecting vehicles passing or arriving at a certain point, for instance, at an intersection with traffic lights or at

Jeong, Ed. Expires January 21, 2020
a ramp toward a highway. The relatively crude nature of the
loop’s structure means that only metal masses above a certain size
are capable of triggering the detection.

- V2I2P: "Vehicle to Infrastructure to Pedestrian".
- V2I2V: "Vehicle to Infrastructure to Vehicle".
- WAVE: "Wireless Access in Vehicular Environments" [WAVE-1609.0].

3. Use Cases

This section explains use cases of V2V, V2I, and V2X networking. The
use cases of the V2X networking exclude the ones of the V2V and V2I
networking, but include Vehicle-to-Pedestrian (V2P) and Vehicle-to-
Device (V2D).

3.1. V2V

The use cases of V2V networking discussed in this section include

- Context-aware navigation for driving safety and collision
  avoidance;
- Cooperative adaptive cruise control in an urban roadway;
- Platooning in a highway;
- Cooperative environment sensing.

These four techniques will be important elements for self-driving
vehicles.

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers
to drive safely by alerting the drivers about dangerous obstacles and
situations. That is, CASD navigator displays obstacles or
neighboring vehicles relevant to possible collisions in real-time
through V2V networking. CASD provides vehicles with a class-based
automatic safety action plan, which considers three situations,
namely, the Line-of-Sight unsafe, Non-Line-of-Sight unsafe, and safe
situations. This action plan can be put into action among multiple
vehicles using V2V networking.

Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps
vehicles to adapt their speed autonomously through V2V communication
among vehicles according to the mobility of their predecessor and
successor vehicles in an urban roadway or a highway. Thus, CACC can
help adjacent vehicles to efficiently adjust their speed in an interactive way through V2V networking in order to avoid collision.

Platooning [Truck-Platooning] allows a series of vehicles (e.g., trucks) to follow each other very closely. Trucks can use V2V communication in addition to forward sensors in order to maintain constant clearance between two consecutive vehicles at very short gaps (from 3 meters to 10 meters). Platooning can maximize the throughput of vehicular traffic in a highway and reduce the gas consumption because the leading vehicle can help the following vehicles to experience less air resistance.

Cooperative-environment-sensing use cases suggest that vehicles can share environmental information from various vehicle-mounted sensors, such as radars, LiDARs, and cameras with other vehicles and pedestrians. [Automotive-Sensing] introduces a millimeter-wave vehicular communication for massive automotive sensing. A lot of data can be generated by those sensors, and these data typically need to be routed to different destinations. In addition, from the perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver-operated vehicles. Through the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment.

3.2. V2I

The use cases of V2I networking discussed in this section include

- Navigation service;
- Energy-efficient speed recommendation service;
- Accident notification service.

A navigation service, for example, the Self-Adaptive Interactive Navigation Tool (SAINT) [SAINT], using V2I networking interacts with TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles for appropriate navigation paths in real time. The enhanced version of SAINT [SAINTplus] can give fast moving paths to emergency vehicles (e.g., ambulance and fire engine) to let them reach an accident spot while redirecting other vehicles near the accident spot into efficient detour paths.

A TCC can recommend an energy-efficient speed to a vehicle that depends on its traffic environment. [Fuel-Efficient] studies fuel-efficient route and speed plans for platooned trucks.
The emergency communication between accident vehicles (or emergency vehicles) and TCC can be performed via either RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, e.g., emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to the FirstNet’s network core. The current RAN is mainly constructed by 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Report], but it is expected that DSRC-based vehicular networks [DSRC] will be available for V2I and V2V in near future.

3.3. V2X

The use case of V2X networking discussed in this section is pedestrian protection service.

A pedestrian protection service, such as Safety-Aware Navigation Application (SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., WiFi) with an RSU. Vehicles and pedestrians can also communicate with each other via an RSU that delivers scheduling information for wireless communication in order to save the smartphones’ battery through sleeping mode.

For Vehicle-to-Pedestrian (V2P), a vehicle and a pedestrian’s smartphone can directly communicate with each other via V2X without the relaying of an RSU as in the V2V scenario that the pedestrian’s smartphone is regarded as a vehicle with a wireless media interface to be able to communicate with another vehicle. There are lightweight mobile nodes such as bicycle and motorcycle, and they can communicate directly with a vehicle for collision avoidance using V2V.

4. Vehicular Networks

This section describes a vehicular network architecture supporting V2V, V2I, and V2X communications in vehicular networks. Also, it describes an internal network within a vehicle or RSU, and the internetworking between the internal networks via DSRC links.
Traffic Control Center in Vehicular Cloud

*-----------------------------------------*
*                                           *
*             +-----------------+             *
*              | Mobility Anchor |              *
*             +-----------------+              *
*                      ^                      *
*                     |                     *
*--------------------v--------------------*
|                         ^                    ^
|                        |                    |
|------------------------v---------------------v|
|                         |                    |
|  +--------+ Ethernet +--------+            +--------+|
|     |  RSU1  |<-------->|  RSU2  |<---------->|  RSU3  ||
|     +--------+          +--------+            +--------+|
|                        |                    |
|   ^                   ^                        ^   |
|   |       |       |       |       |       |   |
|   | V2I    | V2I    | V2I    | V2I    |     |
|   +--------+ +--------+ +--------+ +--------+|
|                         |                    |
|                        |                    |
|                      :                     :
|                      |                     |
|  +-----------------+ +-----------------+   +-----------------+
|                  : V2I                  | | V2I :       |
|                  v                   v |
| Vehicle1 ====> | Vehicle2 ===> | Vehicle3 ===> | Vehicle4 ===> |
| +--------+     +--------+            +--------+    V2V    +--------+|
| V2V              +--------+            +--------+    V2V    +--------+|
|                  +-----------------+   +-----------------+   +-----------------+
|                                           Subnet1              Subnet2              Subnet3 |
|                                           ^                        v                  |
|                                           |                    |
|                                           Wired Link       Wireless Link Moving Direction |

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

4.1. Vehicular Network Architecture

Figure 1 shows an architecture for V2I and V2V networking in a road network. As shown in this figure, RSUs as routers and vehicles with OBU have wireless media interfaces for VANET. Furthermore, the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking. Note that 2001:DB8::/32 is a documentation prefix [RFC3849] for example prefixes in this document, and also that any routable IPv6 address needs to be routable in a VANET and a vehicular network including RSUs.

For IPv6 packets transported over IEEE 802.11-OCB, [IPv6-over-802.11-OCB] specifies several details, including Maximum Transmission Unit (MTU), frame format, link-local address, address
mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. An Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC layer and IPv6 network layer, which is located between IEEE 802.11-OCB’s logical link control layer and IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IP-based vehicular networks.

In Figure 1, three RSUs (RSU1, RSU2, and RSU3) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of RSUs and vehicles in the road network. A Mobility Anchor (MA) is located in the TCC as its key component for the mobility management of vehicles. Two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and one vehicle (Vehicle3) is wirelessly connected to RSU2. The wireless networks of RSU1 and RSU2 belong to two different subnets (Subnet1 and Subnet2), respectively. Another vehicle (Vehicle4) belonging to another subnet (Subnet3) is wirelessly connected to RSU3.

In wireless subnets in vehicular networks (e.g., Subnet1 and Subnet2 in Figure 1), vehicles can construct a connected VANET (with an arbitrary graph topology) and can communicate with each other via V2V communication. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the wireless communication range for each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., RSU2 and RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range for each other.

In vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications. In vehicular networks, the control plane can be separated from the data plane for efficient mobility management and data forwarding. The mobility information of a GPS receiver mounted in its vehicle (e.g., position, speed, and direction) can be used to accommodate mobility-aware proactive protocols. Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275] and PMIPv6 [RFC5213], so the TCC maintains the mobility information of vehicles for location management. IP tunneling over the wireless link should be avoided for performance efficiency.

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle’s internal network (i.e., moving network) and an RSU’s internal network (i.e., fixed network) via V2I communication.
Nowadays, a vehicle’s internal network tends to be Ethernet to interconnect electronic control units in a vehicle. It can also support WiFi and Bluetooth to accommodate a driver’s and passenger’s mobile devices (e.g., smartphone and tablet). In this trend, it is reasonable to consider a vehicle’s internal network (i.e., moving network) and also the interaction between the internal network and an external network within another vehicle or RSU. A vehicle’s internal network often uses Ethernet to interconnect control units in the vehicle. The internal network also supports WiFi and Bluetooth to accommodate a driver’s and passenger’s mobile devices (e.g., smartphone or tablet). It is reasonable to consider the interaction between the internal network and an external network within another vehicle or RSU.

As shown in Figure 2, the vehicle’s moving network and the RSU’s fixed network are self-contained networks having multiple subnets and having an edge router for the communication with another vehicle or RSU. Internetworking between two internal networks via V2I.
communication requires an exchange of network prefix and other parameters through a prefix discovery mechanism, such as ND-based prefix discovery [ID-Vehicular-ND]. For ND-based prefix discovery, network prefixes and parameters should be registered with a vehicle’s router and an RSU router with an external network interface in advance.

For an IP communication between a vehicle and an RSU or between two neighboring vehicles, the network parameter discovery collects information relevant to the link layer, MAC layer, and IP layer. The link layer information includes wireless link layer parameters and transmission power level. The MAC layer information includes the MAC address of an external network interface for the internetworking with another vehicle or RSU. The IP layer information includes the IP address and prefix of an external network interface for the internetworking with another vehicle or RSU.

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle’s moving network and the RSU’s fixed network. A DNS service should be supported for the DNS name resolution of in-vehicle devices within a vehicle’s internal network as well as for the DNS name resolution of those devices from a remote host in the Internet for on-line diagnosis (e.g., an automotive service center server). The DNS names of in-vehicle devices and their service names can be registered with a DNS server in a vehicle or an RSU, as shown in Figure 2.

Figure 2 also shows internetworking between the vehicle’s moving network and the RSU’s fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Fixed Network1) inside RSU1. RSU1 has the DNS Server (DNS2), one host (Host3), the two routers (Router3 and Router4), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1’s Router1 (a mobile router) and RSU1’s Router3 (a fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2I networking. Thus, one host (Host1) in Vehicle1 can communicate with one server (Server1) in RSU1 for a vehicular service through Vehicle1’s moving network, a wireless link between Vehicle1 and RSU1, and RSU1’s fixed network.

4.3. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles via V2V communication.
Figure 3 shows internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (DNS3), the two hosts (Host4 and Host5), and the two routers (Router5 and Router6).

Vehicle1’s Router1 (a mobile router) and Vehicle2’s Router5 (a mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. Thus, one host (Host1) in Vehicle1 can communicate with one host (Host4) in Vehicle2 for a vehicular service through Vehicle1’s moving network, a wireless link between Vehicle1 and Vehicle2, and Vehicle2’s moving network.
Figure 4: Multihop Internetworking between Two Vehicle Networks

Figure 4 shows multihop internetworking between the moving networks of two vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host6 in Vehicle3 via Router 5 in Vehicle2 that is an intermediate vehicle being connected to Vehicle1 and Vehicle3 in a linear topology as shown in the figure.

5. Problem Statement

This section presents key topics such as neighbor discovery, mobility management, and security & privacy.

5.1. Neighbor Discovery

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for point-to-point links and transit links (e.g., Ethernet). It assumes an efficient and reliable support of multicast from the link layer for various network operations such as MAC Address Resolution (AR) and Duplicate Address Detection (DAD).

DAD and ND-related parameters (e.g., Router Lifetime) need to be extended to vehicular networking (e.g., V2V, V2I, and V2X). Vehicles move quickly within the communication coverage of any particular vehicle or RSU. Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and run IPv6 ND.

The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its
address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks.

The vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD, and two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and RSUs, as shown in Figure 1. By using the vehicular-network-wide DAD, vehicles can assure that their IPv6 addresses are unique in the vehicular network whenever they are connected to the vehicular infrastructure or become disconnected from it in the form of VANET. A vehicular infrastructure having RSUs and an MA can participate in the vehicular-network-wide DAD for the sake of vehicles [RFC6775]. For the vehicle as an IPv6 node, deriving a unique IPv6 address from a globally unique MAC address creates a privacy issue. Refer to Section 5.3 for the discussion about such a privacy issue.

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval should be adjusted for high-speed vehicles and vehicle density. As vehicles move faster, the NA interval should decrease (e.g., from 1 sec to 0.5 sec) for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase (e.g., from 0.5 sec to 1 sec) for the NA messages to reduce collision probability with other NA messages.

According to a report from the National Highway Traffic Safety Administration (NHTSA) [NHTSA-ACAS-Report], an extra 0.5 second of warning time can prevent about 60% of the collisions of vehicles moving closely in a roadway. A warning message should be exchanged every 0.5 second. Thus, if the ND messages (e.g., NS and NA) are used as warning messages, they should be exchanged every 0.5 second.

For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. Implementations for such applications are not available yet. ND needs work to support IP-based safety applications.

5.1.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in a vehicular wireless link [VIP-WAVE] [RFC5889]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces [RFC6250]. However, interference and different levels of transmission power may cause
asymmetric links to appear in vehicular wireless links. As a result, a new vehicular link model is required for a dynamically changing vehicular wireless link.

There is a relationship between a link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IP link.

A VANET can have multiple links between pairs of vehicles within wireless communication range, as shown in Figure 4. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Suppose that a global-scope IPv6 prefix is assigned to VANETs in vehicular networks. Even though two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, they may not communicate with each other not in a one hop in the same VANET because of the multihop network connectivity. Thus, in this case, the concept of an on-link IPv6 prefix does not hold because two vehicles with the same on-link IPv6 prefix cannot communicate directly with each other. Also, when two vehicles are located in two different VANETs with the same IPv6 prefix, they cannot communicate with each other. When these two VANETs are converged into one VANET, the two vehicles can communicate with each other in a multihop fashion. Therefore, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility.

The vehicular link model needs to support the multihop routing in a connected VANET where the vehicles with the same global-scope IPv6 prefix are connected in one hop or multiple hops. It also needs to support the multihop routing in multiple connected VANETs via an RSU that has the wireless connectivity with each VANET. For example, in Figure 1, suppose that Vehicle1, Vehicle2, and Vehicle3 are configured with their IPv6 addresses based on the same global-scope IPv6 prefix. Vehicle1 and Vehicle3 can also communicate with each other via either multi-hop V2V or multi-hop V2I2V. When two vehicles of Vehicle1 and Vehicle3 are connected in a VANET, it will be more efficient for them to communicate with each other via VANET rather than RSUs. On the other hand, when the two vehicles of Vehicle1 and Vehicle3 are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V. Thus, two separate VANETs can merge into one network via RSU(s). Also, newly arriving vehicles can merge two separate VANETs into one VANET if they can play a role of a relay node for those VANETs.
5.1.2. MAC Address Pseudonym

For the protection of drivers’ privacy, a pseudonym of a MAC address of a vehicle’s network interface should be used, so that the MAC address can be changed periodically. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP) session with an IPv6 address pair. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

In the ETSI standards, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities (e.g., MAC address) and the corresponding IPv6 addresses [Identity-Management]. Whenever the network interface identifier changes, the IPv6 address based on the network interface identifier should be updated, and the uniqueness of the address should be performed through the DAD procedure. For vehicular networks with high mobility and density, this DAD should be performed efficiently with minimum overhead so that the vehicles can exchange warning messages with each other every 0.5 second [NHTSA-ACAS-Report].

For the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, with a mobility management scheme (e.g., MIPv6 and PMIPv6), the new IP address for the transport-layer session can be notified to an appropriate end point, and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address. This mobility management overhead for pseudonyms should be minimized for efficient operations in vehicular networks having lots of vehicles.

5.1.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes within the internal networks of two vehicles (or within the internal networks of a vehicle and an RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is required. Either a vehicle or an RSU needs an external network interface for its internal network, as shown in Figure 2 and Figure 3. The vehicular ND (VND) [ID-Vehicular-ND] can support the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) with a vehicular prefix information option. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without a vehicular ad hoc routing protocol (e.g., AODV [RFC3561] or OLSRv2 [RFC7181]).
5.1.4. Routing

For multihop V2V communications in either a VANET or VANETs via RSUs, a vehicular ad hoc routing protocol (e.g., AODV and OLSRv2) may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead [ID-Multicast-Problems].

Vehicular ND can be extended to accommodate routing functionality with a prefix discovery option. The ND extension can allow vehicles to exchange their prefixes in a multihop fashion [ID-Vehicular-ND]. With the exchanged prefixes, they can compute their routing table (or IPv6 ND’s neighbor cache) for the VANETs with a distance-vector algorithm [Intro-to-Algorithms].

5.2. Mobility Management

The seamless connectivity and timely data exchange between two end points requires an efficient mobility management including location management and handover. Most of vehicles are equipped with a GPS receiver as part of a dedicated navigation system or a corresponding smartphone App. The GPS receiver may not provide vehicles with accurate location information in adverse, local environments such as building area and tunnel. The location precision can be improved by the assistance from the RSUs or a cellular system with a GPS receiver for location information.

With a GPS navigator, an efficient mobility management will be possible by vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having RSUs and an MA in TCC) [ID-Vehicular-MM]. This vehicular infrastructure can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the efficient mobility management (e.g., proactive handover). For a better proactive handover, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]), can be used to determine the moment of a handover between RSUs along with mobility information.

By predicting a vehicle’s mobility, the vehicular infrastructure can better support RSUs to perform efficient DAD, data packet routing, horizontal handover (i.e., handover in wireless links using a homogeneous radio technology), and vertical handover (i.e., handover in wireless links using heterogeneous radio technologies) in advance along with the movement of the vehicle [ID-Vehicular-MM]. For example, when a vehicle is moving into the wireless link under
another RSU belonging to a different subnet, the RSU can proactively perform the DAD for the sake of the vehicle, reducing IPv6 control traffic overhead in the wireless link. To prevent a hacker from impersonating RSUs as bogus RSUs, RSUs and MA in the vehicular infrastructure need to have secure channels via IPsec.

Therefore, with a proactive handover and a multihop DAD in vehicular networks, RSUs needs to efficiently forward data packets from the wired network (or the wireless network) to a moving destination vehicle along its trajectory.

5.3. Security and Privacy

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe. Sybil attack, which tries to confuse a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. This sybil attack should be prevented through the cooperation between good vehicles and RSUs. Note that good vehicles are ones with valid certificates that are determined by the authentication process with an authentication server in the vehicular network. Applications on IP-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device’s identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., RSU) connected to an authentication server in TCC. Also, Transport Layer Security (TLS) certificates can be used for secure E2E vehicle communications.

For secure V2I communication, a secure channel between a mobile router in a vehicle and a fixed router in an RSU should be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.
To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym should be provided to the vehicle; that is, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an RSU) in terms of transport layer for a long-living higher-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IP addresses, because an adversary can see the change of the MAC and IP addresses and track the vehicle with those addresses.

For the IPv6 ND, the vehicular-network-wide DAD is required for the uniqueness of the IPv6 address of a vehicle’s wireless interface. This DAD can be used as a flooding attack that makes the DAD-related ND packets are disseminated over the VANET and vehicular network including the RSUs and the MA. The vehicles and RSUs need to filter out suspicious ND traffic in advance.

For the mobility management, a malicious vehicle can construct multiple virtual bogus vehicles, and register them with the RSU and the MA. This registration makes the RSU and MA waste their resources. The RSU and MA need to determine whether a vehicle is genuine or bogus in the mobility management.

6. Security Considerations

This document discussed security and privacy for IP-based vehicular networking.

The security and privacy for key components in IP-based vehicular networking, such as neighbor discovery and mobility management, need to be analyzed in depth.

7. Informative References

[Automotive-Sensing]


ETSI Technical Committee Intelligent Transport Systems, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality", ETSI EN 302 636-4-1, May 2014.


[FirstNet-Report]

[Fuel-Efficient]

[ID-Multicast-Problems]

[ID-Vehicular-MM]

[ID-Vehicular-ND]

[Identity-Management]

[IEEE-802.11-OCB]

[IEEE-802.11p]
[Intro-to-Algorithms]

[IPv6-over-802.11-OCB]

[ISO-ITS-IPv6]

[NHTSA-ACAS-Report]


[Truck-Platooning]
California Partners for Advanced Transportation Technology
(PATH), "Automated Truck Platooning", [Online] Available:
http://www.path.berkeley.edu/research/automated-and-

[TS-23.285-3GPP]
3GPP, "Architecture Enhancements for V2X Services", 3GPP

[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

[WAVE-1609.0]
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-ietf-ipwave-vehicular-networking-10

The following changes are made from draft-ietf-ipwave-vehicular-networking-10:

- This version is revised based on the comments from Charlie Perkins and Sri Gundavelli.
- Many editorial comments and questions from Charlie Perkins are addressed in this document.
- According to Sri Gundavelli’s comments, the solution text and RFC 8505 reference for the vehicular ND are deleted from Section 5.1 in this document.

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 the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2017-0-01633) supervised by the IITP (Institute for Information & communications Technology Promotion).

This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

Appendix C. Contributors

This document is a group work of IPWAVE working group, greatly benefiting from inputs and texts by Rex Buddenberg (Naval Postgraduate School), Thierry Ernst (YoGoKo), Bokor Laszlo (Budapest University of Technology and Economics), Jose Santa Lozanoi (Universidad of Murcia), Richard Roy (MIT), Francois Simon (Pilot), Sri Gundavelli (Cisco), Erik Nordmark, Dirk von Hugo (Deutsche Telekom), and Pascal Thubert (Cisco). The authors sincerely appreciate their contributions.

The following are co-authors of this document:

Nabil Benamar
Department of Computer Sciences
High School of Technology of Meknes
Moulay Ismail University
Morocco
IPv6 Neighbor Discovery on Wireless Networks
draft-thubert-6man-ipv6-over-wireless-03

Abstract

This document describes how the original IPv6 Neighbor Discovery and Wireless ND (WiND) can be applied on various abstractions of wireless media.

Status of This Memo

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

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

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

This Internet-Draft will expire on November 3, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

IEEE Std. 802.1 [IEEEstd8021] Ethernet Bridging provides an efficient and reliable broadcast service for wired networks; applications and protocols have been built that heavily depend on that feature for their core operation. Unfortunately, Low-Power Lossy Networks (LLNs) and local wireless networks generally do not provide the broadcast capabilities of Ethernet Bridging in an economical fashion.

As a result, protocols designed for bridged networks that rely on multicast and broadcast often exhibit disappointing behaviours when employed unmodified on a local wireless medium (see [I-D.ietf-mboned-ieee802-mcast-problems]).

Wi-Fi [IEEEstd80211] Access Points (APs) deployed in an Extended Service Set (ESS) act as Ethernet Bridges [IEEEstd8021], with the property that the bridging state is established at the time of association. This ensures connectivity to the node (STA) and protects the wireless medium against broadcast-intensive Transparent Bridging reactive Lookups.
In other words, the association process is used to register the MAC Address of the STA to the AP. The AP subsequently proxies the bridging operation and does not need to forward the broadcast Lookups over the radio.

Like Transparent Bridging, IPv6 [RFC8200] Neighbor Discovery [RFC4861] [RFC4862] Protocol (IPv6 ND) is a reactive protocol, based on multicast transmissions to locate an on-link correspondent and ensure the uniqueness of an IPv6 address. The mechanism for Duplicate Address Detection (DAD) [RFC4862] was designed for the efficient broadcast operation of Ethernet Bridging. Since broadcast can be unreliable over wireless media, DAD often fails to discover duplications [I-D.yourtchenko-6man-dad-issues]. In practice, IPv6 addresses very rarely conflict because of the entropy of the 64-bit Interface IDs, not because address duplications are detected and resolved.

The IPv6 ND Neighbor Solicitation (NS) [RFC4861] message is used for DAD and address Lookup when a node moves, or wakes up and reconnects to the wireless network. The NS message is targeted to a Solicited-Node Multicast Address (SNMA) [RFC4291] and should in theory only reach a very small group of nodes. But in reality, IPv6 multicast messages are typically broadcast on the wireless medium, and so they are processed by most of the wireless nodes over the subnet (e.g., the ESS fabric) regardless of how few of the nodes are subscribed to the SNMA. As a result, IPv6 ND address Lookups and DADs over a large wireless and/or a LowPower Lossy Network (LLN) can consume enough bandwidth to cause a substantial degradation to the unicast traffic service [I-D.vyncke-6man-mcast-not-efficient].

Because IPv6 ND messages sent to the SNMA group are broadcasted at the radio MAC Layer, wireless nodes that do not belong to the SNMA group still have to keep their radio turned on to listen to multicast NS messages, which is a total waste of energy for them. In order to reduce their power consumption, certain battery-operated devices such as IoT sensors and smartphones ignore some of the broadcasts, making IPv6 ND operations even less reliable.

These problems can be alleviated by reducing the IPv6 ND broadcasts over wireless access links. This has been done by splitting the broadcast domains and by routing between subnets, at the extreme by assigning a /64 prefix to each wireless node (see [RFC8273]).

Another way is to proxy at the boundary of the wired and wireless domains the Layer-3 protocols that rely on MAC Layer broadcast operations. For instance, IEEE 802.11 [IEEEstd80211] situates proxy-ARP (IPv4) and proxy-ND (IPv6) functions at the Access Points (APs).
But proxying ND requires a perfect knowledge of the peer IPv6 addresses for which proxying is provided. In a generic fashion, radio connectivity changes with movements and variations in the environment, which makes forming and maintaining that knowledge a hard problem in the general case.

Discovering peer addresses by snooping the IPv6 ND protocol as proposed for SAVI [I-D.bi-savi-wlan] was found to be unreliable. An IPv6 address may not be discovered immediately due to a packet loss, or if a "silent" node is not currently using one of its addresses, e.g., a node that waits in wake-on-lan state. A change of state, e.g. due to a movement, may be missed or misordered, leading to unreliable connectivity and an incomplete knowledge of the set of peers.

Wireless ND (WiND) introduces a new approach to IPv6 ND that is designed to apply to the WLANs and WPANs types of networks. On the one hand, WiND avoids the use of broadcast operation for Address Resolution and Duplicate Address Detection, and on the other hand, WiND supports use cases where Subnet and MAC-level domains are not congruent, which is common in those types of networks unless a specific MAC-Level emulation is provided.

To achieve this, WiND applies routing inside the Subnets, which enables MultiLink Subnets. Hosts register their addresses to their serving routers with [RFC8505]. With the registration, routers have a complete knowledge of the hosts they serve and in return, hosts obtain routing services for their registered addresses. The registration is abstract to the routing protocol, and it can be protected to prevent impersonation attacks with [I-D.ietf-6lo-ap-nd].

The routing service can be a simple reflexion in a Hub-and-Spoke Subnet that emulates an IEEE Std 802.11 Infrastructure BSS at Layer 3. It can also be a full-fledge routing protocol, in particular RPL [RFC6550] that was designed to adapt to various LLNs such as WLAN and WPAN radio meshes with the concept of Objective Function. Finally, the routing service can also be ND proxy that emulates an IEEE Std 802.11 Infrastructure ESS at Layer 3. WiND specifies the IPv6 Backbone Router for that purpose in [I-D.ietf-6lo-backbone-router].

More details on WiND can be found in Section 4.1.

2. Acronyms

This document uses the following abbreviations:

6BBR: 6LoWPAN Backbone Router
6LBR: 6LoWPAN Border Router
6LN: 6LoWPAN Node
6LR: 6LoWPAN Router
ARO: Address Registration Option
DAC: Duplicate Address Confirmation
DAD: Duplicate Address Detection
DAR: Duplicate Address Request
EDAC: Extended Duplicate Address Confirmation
EDAR: Extended Duplicate Address Request
MLSN: Multi-Link Subnet
LLN: Low-Power and Lossy Network
NA: Neighbor Advertisement
NBMA: Non-Broadcast Multi-Access
NCE: Neighbor Cache Entry
ND: Neighbor Discovery
NDP: Neighbor Discovery Protocol
NS: Neighbor Solicitation
RPL: IPv6 Routing Protocol for LLNs
RA: Router Advertisement
RS: Router Solicitation
WiND: Wireless Neighbor Discovery
WLAN: Wireless Local Area Network
WPAN: Wireless Personal Area Network
3. IP Models

3.1. Physical Broadcast Domain

At the physical (PHY) Layer, a broadcast domain is the set of nodes that may receive a datagram that one sends over an interface, in other words the set of nodes in range of radio transmission. This set can comprise a single peer on a serial cable used as point-to-point (P2P) link. It may also comprise multiple peer nodes on a broadcast radio or a shared physical resource such as the legacy Ethernet shared wire.

On WLAN and WPAN radios, the physical broadcast domain is defined by a particular transmitter, as the set of nodes that can receive what this transmitter is sending. Literally every datagram defines its own broadcast domain since the chances of reception of a given datagram are statistical. In average and in stable conditions, the broadcast domain of a particular node can be still be seen as mostly constant and can be used to define a closure of nodes on which an upper-layer abstraction can be built.

A PHY-layer communication can be established between 2 nodes if their physical broadcast domains overlap.

On WLAN and WPAN radios, this property is usually reflexive, meaning that if B can receive a datagram from A, then A can receive a datagram from B. But there can be asymmetries due to power levels, interferers near one of the receivers, or differences in the quality of the hardware (e.g., crystals, PAs and antennas) that may affect the balance to the point that the connectivity becomes mostly unidirectional, e.g., A to B but practically not B to A. It takes a particular effort to place a set of devices in a fashion that all their physical broadcast domains fully overlap, and it can not be assumed in the general case. In other words, the property of radio connectivity is generally not transitive, meaning that A may be in range with B and B may be in range with C does not necessarily imply that A is in range with C.

We define MAC-Layer Direct Broadcast (DMC) a transmission mode where the broadcast domain that is usable at the MAC layer is directly the physical broadcast domain. IEEE 802.15.4 [IEEE802154] and IEEE 802.11 [IEEEstd80211] OCB (for Out of the Context of a BSS) are examples of DMC radios. This constrasts with a number of MAC-layer Broadcast Emulation schemes that are described in the next section.
3.2. MAC-Layer Broadcast Emulations

While a physical broadcast domain is constrained to a single shared wire, Ethernet Bridging emulates the broadcast properties of that wire over a whole physical mesh of Ethernet links. For the upper layer, the qualities of the shared wire are essentially conserved, with a reliable and cheap broadcast operation over a closure of nodes defined by their connectivity to the emulated wire.

In large switched fabrics, overlay techniques enable a limited connectivity between nodes that are known to a mapping server. The emulated broadcast domain is configured to the system, e.g., with a VXLAN network identifier (VNID). Broadcast operations on the overlay can be emulated but can become very expensive, and it makes sense to proactively install the relevant state in the mapping server as opposed to rely on reactive broadcast lookups.

An IEEE Std 802.11 Infrastructure Basic Service Set (BSS) also provides a closure of nodes as defined by the broadcast domain of a central Access Point (AP). The AP relays both unicast and broadcast packets and ensures a reflexive and transitive emulation of the shared wire between the associated nodes, with the capability to signal link-up/link-down to the upper layer. Within an Infrastructure BSS, the physical broadcast domain of the AP serves as emulated broadcast domain for all the nodes that are associated to the AP. Broadcast packets are relayed by the AP and are not acknowledged. To ensure that all nodes in the BSS receive the broadcast transmission, AP transmits at the slowest PHY speed. This translates into maximum co-channel interferences for others and longest occupancy of the medium, for a duration that can be 100 times that of a unicast. For that reason, upper layer protocols should tend to avoid the use of broadcast when operating over Wi-Fi.

In an IEEE Std 802.11 Infrastructure Extended Service Set (ESS), infrastructure BSSes are interconnected by a bridged network, typically running Transparent Bridging and Spanning tree Protocol. In the original model, the state in the Transparent Bridge is set by observing the source MAC address of the frames. When a state is missing for a destination MAC address, the frame is broadcasted with the expectation that the response will populate the state. This is a reactive operation, meaning that the state is populated reactively to a need for forwarding. It is also possible to send a gratuitous frame to advertise self throughout the bridged network, and that is also a broadcast. The process of the association prepares a bridging state proactively at the AP, so as to avoid the reactive broadcast lookup. It may also generates a gratuitous broadcast sourced at the MAC address of the STA to prepare or update the state in the Transparent Bridges. This model avoids the need of multicast over
the wireless access, and it is only logical that IPv6 ND evolved towards proposes similar methods at Layer-3 for its operation.

In some cases of WLAN and WPAN radios, a mesh-under technology (e.g., a IEEE 802.11s or IEEE 802.15.10) provides meshing services that are similar to bridging, and the broadcast domain is well defined by the membership of the mesh. Mesh-Under emulates a broadcast domain by flooding the broadcast packets at Layer-2. When operating on a single frequency, this operation is known to interfere with itself, forcing deployment to introduce delays that dampen the collisions. All in all, the mechanism is slow, inefficient and expensive.

Going down the list of cases above, the cost of a broadcast transmissions becomes increasingly expensive, and there is a push to rethink the upper-layer protocols so as to reduce the dependency on broadcast operations.

There again, a MAC-layer communication can be established between 2 nodes if their MAC-layer broadcast domains overlap. In the absence of a MAC-layer emulation such as a mesh-under or an Infrastructure BSS, the MAC-layer broadcast domain is congruent with that of the PHY-layer and inherits its properties for reflexivity and transitivity. IEEE 802.11p, which operates Out of the Context of a BSS (DMC radios) is an example of a network that does not have a MAC-Layer broadcast domain emulation, which means that it will exhibit mostly reflexive and mostly non-transitive transmission properties.

3.3. Mapping the IPv6 Link Abstraction

IPv6 defines a concept of Link, Link Scope and Link-Local Addresses (LLA), an LLA being unique and usable only within the Scope of a Link. The IPv6 Neighbor Discovery (ND) [RFC4861][RFC4862] Duplicate Address Detection (DAD) process leverages a multicast transmission to ensure that an IPv6 address is unique as long as the owner of the address is connected to the broadcast domain. It must be noted that in all the cases in this specification, the Layer-3 multicast operation is always a MAC_Layer broadcast for the lack of a Layer-2 multicast operation that could handle a possibly very large number of groups in order to make the unicast efficient. This means that for every multicast packet regardless of the destination group, all nodes will receive the packet and process it all the way to Layer-3.

On wired media, the Link is often confused with the physical broadcast domain because both are determined by the serial cable or the Ethernet shared wire. Ethernet Bridging reinforces that illusion by providing a MAC-Layer broadcast domain that emulates a physical broadcast domain over the mesh of wires. But the difference shows on legacy Non-Broadcast Multi-Access (NBMA) such as ATM and Frame-Relay,
on shared links and on newer types of NBMA networks such as radio and composite radio-wires networks. It also shows when private VLANs or Layer-2 cryptography restrict the capability to read a frame to a subset of the connected nodes.

In mesh-under and Infrastructure BSS, the IP Link extends beyond the physical broadcast domain to the emulated MAC-Layer broadcast domain. Relying on Multicast for the ND operation remains feasible but becomes detrimental to unicast traffic, energy-inefficient and unreliable, and its use is discouraged.

On DMC radios, IP Links between peers come and go as the individual physical broadcast domains of the transmitters meet and overlap. The DAD operation cannot provide once and for all guarantees on the broadcast domain defined by one radio transmitter if that transmitter keeps meeting new peers on the go. The nodes may need to form new LLAs to talk to one another and the scope where LLA uniqueness can be dynamically checked is that pair of nodes. As long as there’s no conflict a node may use the same LLA with multiple peers but it has to revalidate DAD with every new peer node. In practice, each pair of nodes defines a temporary P2P link, which can be modeled as a sub-interface of the radio interface.

3.4. Mapping the IPv6 Subnet Abstraction

IPv6 also defines a concept of Subnet for Glocal and Unique Local Addresses. Addresses in a same Subnet share a same prefix and by extension, a node belongs to a Subnet if it has an interface with an address on that Subnet. A Subnet prefix is Globally Unique so it is sufficient to validate that an address that is formed from a Subnet prefix is unique within that Subnet to guarantee that it is globally unique. IPv6 aggregation relies on the property that a packet from the outside of a Subnet can be routed to any router that belongs to the Subnet, and that this router will be able to either resolve the destination MAC address and deliver the packet, or route the packet to the destination within the Subnet. If the Subnet is known as onlink, then any node may also resolve the destination MAC address and deliver the packet, but if the Subnet is not onlink, then a host that does not have an NCE for the destination will need to pass the packet to a router.

On IEEE Std. 802.3, a Subnet is often congruent with an IP Link because both are determined by the physical attachment to an Ethernet shared wire or an IEEE Std. 802.1 bridged broadcast domain. In that case, the connectivity over the Link is transitive, the Subnet can appear as onlink, and any node can resolve a destination MAC address of any other node directly using IPv6 Neighbor Discovery.
But an IP Link and an IP Subnet are not always congruent. In a shared Link situation, a Subnet may encompass only a subset of the nodes connected to the Link. In Route-Over Multi-Link Subnets (MLSN) [RFC4903], routers federate the Links between nodes that belong to the Subnet, the Subnet is not onlink and it extends beyond any of the federated Links.

The DAD and lookup procedures in IPv6 ND expects that a node in a Subnet is reachable within the broadcast domain of any other node in the Subnet when that other node attempts to form an address that would be a duplicate or attempts to resolve the MAC address of this node. This is why ND is only applicable for P2P and transit links, and requires extensions for other topologies.

4. Wireless ND

4.1. Introduction to WiND

Wireless Neighbor Discovery (WiND) [RFC6775][RFC8505][I-D.ietf-6lo-backbone-router][I-D.ietf-6lo-ap-nd] defines a new ND operation that is based on 2 major paradigm changes, proactive address registration by hosts to their attachment routers and routing to host routes (/128) within the subnet. This allows WiND to avoid the classical ND expectations of transit links and Subnet-wide broadcast domains.

The proactive address registration is performed with a new option in NS/NA messages, the Extended Address Registration Option (EARO) defined in [RFC8505]. This method allows to prepare and maintain the host routes in the routers and avoids the reactive NS(Lookup) found in IPv6 ND. This is a direct benefit for wireless Links since it avoids the MAC level broadcasts that are associated to NS(Lookup).

The EARO provides information to the router that is independent to the routing protocol and routing can take multiple forms, from a traditional IGP to a collapsed ub-and-Spoke model where only one router owns and advertises the prefix. [RFC8505] is already referenced for RIFT [I-D.ietf-rift-rift], RPL [RFC6550] with [I-D.thubert-roll-unaware-leaves] and IPv6 ND proxy [I-D.ietf-6lo-backbone-router].

WiND does not change IPv6 addressing [RFC4291] or the current practices of assigning prefixes to subnets. It is still typical to assign a /64 to a subnet and to use interface IDs of 64 bits. Duplicate Address detection within the Subnet is performed with a central registrar, using new ND Extended Duplicate Address messages (EDAR and EDAC) [RFC8505]. This operation modernizes ND for application in overlays with Map Resolvers and enables unicast.
lookups [I-D.thubert-6lo-unicast-lookup] for addresses registered to the resolver.

WiND also enables to extend a legacy /64 on Ethernet with ND proxy over the wireless. This way nodes can form any address they want and move freely from an L3-AP (that is really a backbone router in bridging mode, more in [I-D.ietf-6lo-backbone-router]) to another, without renumbering. Backbone Routers federate multiple LLNs over a Backbone Link to form a MultiLink Subnet (MLSN). Backbone Routers placed along the LLN edge of the Backbone handle IPv6 Neighbor Discovery, and forward packets on behalf of registered nodes.

An LLN node (6LN) registers all its IPv6 Addresses using an NS(EARO) as specified in [RFC8505] to the 6BBR. The 6BBR is also a Border Router that performs IPv6 Neighbor Discovery (IPv6 ND) operations on its Backbone interface on behalf of the 6LNs that have registered addresses on its LLN interfaces without the need of a broadcast over the wireless medium.

WiND is also compatible with DHCPv6 and other forms of address assignment in which case it can still be used for DAD.

4.2. Links and Link-Local Addresses

For Link-Local Addresses, DAD is performed between communicating pairs of nodes. It is carried out as part of a registration process that is based on a NS/NA exchange that transports an EARO. During that process, the DAD is validated and a Neighbor Cache Entry (NCE) is populated with a single unicast exchange.

For instance, in the case of a Bluetooth Low Energy (BLE) [RFC7668][IEEEstd802151] Hub-and Spoke configuration, Uniqueness of Link local Addresses need only to be verified between the pairs of communicating nodes, a central router and a peripheral host. In that example, 2 peripheral hosts connected to the same central router can not have the same Link Local Address because the Binding Cache Entries (BCEs) would collide at the central router which could not talk to both over the same interface. The WiND operation is appropriate for that DAD operation, but the one from ND is not, because peripheral hosts are not on the same broadcast domain. On the other hand, Global and ULA DAD is validated at the Subnet Level, using a registrar hosted by the central router.

4.3. Subnets and Global Addresses

WiND extends IPv6 ND for Hub-and-Spoke (e.g., BLE) and Route-Over (e.g., RPL) Multi-Link Subnets (MLSNs).
In the Hub-and-Spoke case, each Hub-Spoke pair is a distinct IP Link, and a Subnet can be mapped on a collection of Links that are connected to the Hub. The Subnet prefix is associated to the Hub. Acting as 6LR, the Hub advertises the prefix as not-onlink to the spokes in RA messages Prefix Information Options (PIO). Acting as 6LNs, the Spokes autoconfigure addresses from that prefix and register them to the Hub with a corresponding lifetime. Acting as a 6LBR, the Hub maintains a binding table of all the registered IP addresses and rejects duplicate registrations, thus ensuring a DAD protection for a registered address even if the registering node is sleeping. Acting as 6LR, the Hub also maintains an NCE for the registered addresses and can deliver a packet to any of them for their respective lifetimes. It can be observed that this design builds a form of Layer-3 Infrastructure BSS.

A Route-Over MLSN is considered as a collection of Hub-and-Spoke where the Hubs form a connected dominating set of the member nodes of the Subnet, and IPv6 routing takes place between the Hubs within the Subnet. A single logical 6LBR is deployed to serve the whole mesh. The registration in [RFC8505] is abstract to the routing protocol and provides enough information to feed a routing protocol such as RPL as specified in [I-D.thubert-roll-unaware-leaves]. In a degraded mode, all the Hubs are connected to a same high speed backbone such as an Ethernet bridging domain where IPv6 ND is operated. In that case, it is possible to federate the Hub, Spoke and Backbone nodes as a single Subnet, operating IPv6 ND proxy operations [I-D.ietf-6lo-backbone-router] at the Hubs, acting as 6BBRs. It can be observed that this latter design builds a form of Layer-3 Infrastructure ESS.

5. WiND Applicability

WiND allows P2P, P2MP hub-and spoke, MAC-level broadcast domain emulation such as mesh-under and Wi-Fi BSS, and Route-Over meshes.

There is an intersection where Link and Subnet are congruent and where both ND and WiND could apply. These includes P2P, the MAC emulation of a PHY broadcast domain, and the particular case of always on, fully overlapping physical radio broadcast domain. But even in those cases where both are possible, WiND is preferable vs. ND because it reduces the need of broadcast (this is discussed in the introduction of [I-D.ietf-6lo-backbone-router]).

There are also numerous practical use cases in the wireless world where Links and Subnets are not P2P and not congruent:

- IEEE std 802.11 infrastructure BSS enables one subnet per AP, and emulates a broadcast domain at L2. Infra ESS extends that and
recommends to use an IPv6 ND proxy [IEEEstd80211] to coexist with Ethernet connected nodes. WiND incorporates an ND proxy to serve that need and that was missing so far.

- BlueTooth is Hub-and-Spoke at the MAC layer. It would make little sense to configure a different subnet between the central and each individual peripheral node (e.g., sensor). Rather, [RFC7668] allocates a prefix to the central node acting as router (6LR), and each peripheral host (acting as a host (6LR) forms one or more address(es) from that same prefix and registers it.

- A typical Smartgrid networks puts together Route-Over MLSNs that comprise thousands of IPv6 nodes. The 6TiSCH architecture [I-D.ietf-6tisch-architecture] presents the Route-Over model over a [IEEEstd802154] Time-Slotted Channel-Hopping mesh, and generalizes it for multiple other applications. Each node in a Smartgrid network may have tens to a hundred others nodes in range. A key problem for the routing protocol is which other node(s) should this node peer with, because most of the possible peers do not provide added routing value. When both energy and bandwidth are constrained, talking to them is a bad idea and most of the possible P2P links are not even used. Peerings that are actually used come and go with the dynamics of radio signal propagation. It results that allocating prefixes to all the possible P2P Links and maintain as many addresses in all nodes is not even considered.

5.1. Case of LPWANs

LPWANs are by nature so constrained that the addresses and Subnets are fully pre-configured and operate as P2P or Hub-and-Spoke. This saves the steps of neighbor Discovery and enables a very efficient stateful compression of the IPv6 header.

5.2. Case of Infrastructure BSS and ESS

In contrast to IPv4, IPv6 enables a node to form multiple addresses, some of them temporary to elusive, and with a particular attention paid to privacy. Addresses may be formed and deprecated asynchronously to the association. Even if the knowledge of IPv6 addresses used by a STA can be obtained by snooping protocols such as IPv6 ND and DHCPv6, or by observing data traffic sourced at the STA, such methods provide only an imperfect knowledge of the state of the STA at the AP. This may result in a loss of connectivity for some IPv6 addresses, in particular for addresses rarely used and in a situation of mobility. This may also result in undesirable remanent state in the AP when a STA ceases to use an IPv6 address. It results
that snooping protocols is not a recommended technique and that it should only be used as last resort.

The recommended alternate is to use the IPv6 Registration method specified in p. By that method, the AP exposes its capability to proxy ND to the STA in Router Advertisement messages. In turn, the STA may request proxy ND services from the AP for one or more IPv6 addresses, using an Address Registration Option. The Registration state has a lifetime that limits unwanted state remanence in the network. The registration is optionally secured using [I-D.ietf-6lo-ap-nd] to prevent address theft and impersonation. The registration carries a sequence number, which enables a fast mobility without a loss of connectivity.

The ESS mode requires a proxy ND operation at the AP. The proxy ND operation must cover Duplicate Address Detection, Neighbor Unreachability Detection, Address Resolution and Address Mobility to transfer a role of ND proxy to the AP where a STA is associated following the mobility of the STA. The proxy ND specification associated to the address registration is [I-D.ietf-6lo-backbone-router]. With that specification, the AP participates to the protocol as a Backbone Router, typically operating as a bridging proxy though the routing proxy operation is also possible. As a bridging proxy, the proxy replies to NS lookups with the MAC address of the STA, and then bridges packets to the STA normally; as a routing proxy, it replies with its own MAC address and then routes to the STA at the IP layer. The routing proxy reduces the need to expose the MAC address of the STA on the wired side, for a better stability and scalability of the bridged fabric.

5.3. Case of Mesh Under Technologies

The Mesh-Under provides a broadcast domain emulation with reflexive and Transitive properties and defines a transit Link for IPv6 operations. It results that the model for IPv6 operation is similar to that of a BSS, with the root of the mesh operating an Access Point does in a BSS/ESS. While it is still possible to operate IPv6 ND, the inefficiencies of the flooding operation make the IPv6 ND operations even less desirable than in a BSS, and the use of WiND is highly recommended.

5.4. Case of DMC radios

IPv6 over DMC radios uses P2P Links that can be formed and maintained when a pair of DMC radios transmitters are in range from one another.
5.4.1. Using IPv6 ND only

DMC radios do not provide MAC level broadcast emulation. An example of that is OCB (outside the context of a BSS), which uses IEEE Std. 802.11 transmissions but does not provide the BSS functions.

It is possible to form P2P IP Links between each individual pairs of nodes and operate IPv6 ND over those Links with Link Local addresses. DAD must be performed for all addresses on all P2P IP Links.

If special deployment care is taken so that the physical broadcast domains of a collection of the nodes fully overlap, then it is also possible to build an IP Subnet within that collection of nodes and operate IPv6 ND.

The model can be stretched beyond the scope of IPv6 ND if an external mechanism avoids duplicate addresses and if the deployment ensures the connectivity between peers. This can be achieved for instance in a Hub-and-Spoke deployment if the Hub is the only router in the Subnet and the Prefix is advertised as not onlink.

5.4.2. Using Wireless ND

Though this can be achieved with IPv6 ND, WiND is the recommended approach since it uses more unicast communications which are more reliable and less impacting for other users of the medium.

Router and Hosts respectively send a compressed RA/NA with a SLLAO at a regular period. The period can be indicated in a RA as in an RA-Interval Option [RFC6275]. If available, the message can be transported in a compressed form in a beacon, e.g., in OCB Basic Safety Messages (BSM) that are nominally sent every 100ms. An active beaconing mode is possible whereby the Host sends broadcast RS messages to which a router can answer with a unicast RA.

A router that has Internet connectivity and is willing to serve as an Internet Access may advertise itself as a default router [RFC4191] in its RA. The NA/RA is sent over an Unspecified Link where it does not conflict to anyone, so DAD is not necessary at that stage.

The receiver instantiates a Link where the sender’s address is not a duplicate. To achieve this, it forms an LLA that does not conflict with that of the sender and registers to the sender using [RFC8505]. If the sender sent an RA(PIO) the receiver can also autoconfigure an address from the advertised prefix and register it.
The lifetime in the registration should start with a small value (X=RMin, TBD), and exponentially grow with each reregistration to a larger value (X=Rmax, TBD). The IP Link is considered down when (X=NbBeacons, TDB) expected messages are not received in a row. It must be noted that the Link flapping does not affect the state of the registration and when a Link comes back up, the active -lifetime not elapsed- registrations are still usable. Packets should be held or destroyed when the Link is down.

P2P Links may be federated in Hub-and-Spoke and then in Route-Over MLSNs as described above. More details on the operation of WiND and RPL over the MLSN can be found in section 3.1, 3.2, 4.1 and 4.2.2 of [I-D.ietf-6tisch-architecture].

Figure 1: Initial Registration Flow
<table>
<thead>
<tr>
<th>6LoWPAN Node (RPL leaf)</th>
<th>6LR (router)</th>
<th>6LBR (root)</th>
<th>6BBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>6LoWPAN ND LLN link</td>
<td>6LoWPAN ND+RPL Route-Over mesh</td>
<td>6LoWPAN ND Ethernet/serial</td>
<td>IPv6 ND Backbone</td>
</tr>
<tr>
<td>IPv6 ND RS</td>
<td>&lt;------------&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;------------&gt;</td>
<td>IPv6 ND RA</td>
<td>&lt;once&gt;</td>
</tr>
<tr>
<td>NS(EARO)</td>
<td>&lt;------------&gt;</td>
<td>6LoWPAN ND Extended DAR NS(EARO)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;------------&gt;</td>
<td></td>
<td>NS-DAD &lt;----------&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(EARO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NA(EARO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>------&lt;timeout&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NA(EARO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>------&lt;timeout&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NA(EARO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>------&lt;timeout&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6LoWPAN ND Extended DAC</td>
</tr>
</tbody>
</table>

Figure 2: Initial Registration Flow over Multi-Link Subnet

An example Hub-and-Spoke is an OCB Road-Side Unit (RSU) that owns a prefix, provides Internet connectivity using that prefix to On-Board Units (OBUs) within its physical broadcast domain. An example of Route-Over MLSN is a collection of cars in a parking lot operating RPL to extend the connectivity provided by the RSU beyond its physical broadcast domain. Cars may then operate NEMO [RFC3963] for their own prefix using their address derived from the prefix of the RSU as CareOf Address.

6. IANA Considerations

This specification does not require IANA action.
7. Security Considerations

This specification refers to the security sections of IPv6 ND and WiND, respectively.

8. Acknowledgments

Many thanks to the participants of the 6lo WG where a lot of the work discussed here happened. Also ROLL, 6TiSCH, and 6LoWPAN.

9. References

9.1. Normative References

[I-D.ietf-6lo-ap-nd]

[I-D.ietf-6lo-backbone-router]


9.2. Informative References


[I-D.yourtchenko-6man-dad-issues]

[IEEE802154]
IEEE standard for Information Technology, "IEEE Std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks".

[IEEEstd8021]
IEEE standard for Information Technology, "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks Part 1: Bridging and Architecture".

[IEEEstd80211]
IEEE standard for Information Technology, "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks-- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[IEEEstd802151]
IEEE standard for Information Technology, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)".

[IEEEstd802154]
IEEE standard for Information Technology, "IEEE Standard for Local and metropolitan area networks -- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)".


Applying Wireless ND


Author’s Address

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis 06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com