

IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2020

N. Benamar
Moulay Ismail University of Meknes
J. Haerri
Eurecom
J. Lee
Sangmyung University
T. Ernst
YoGoKo
July 8, 2019

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

(<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. 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:

- o 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] .
- o 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 "OBUS"

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 dot11OCBActivated 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

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 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-OBUE 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:

- o Bit "Local/Global" set to "locally administered".
- o Bit "Unicast/Multicast" set to "Unicast".
- o 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.

- o Particular challenges arise when the pseudonymization mechanism used relies on (randomized) re-addressing.
- o 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).
- o This is discussed in Section 4.4 and Section 5 of this document.
- o 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 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, 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

- [RFC1042] Postel, J. and J. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", STD 43, RFC 1042, DOI 10.17487/RFC1042, February 1988, <<https://www.rfc-editor.org/info/rfc1042>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <<https://www.rfc-editor.org/info/rfc2464>>.
- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <<https://www.rfc-editor.org/info/rfc4086>>.
- [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <<https://www.rfc-editor.org/info/rfc4193>>.
- [RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, DOI 10.17487/RFC4210, September 2005, <<https://www.rfc-editor.org/info/rfc4210>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <<https://www.rfc-editor.org/info/rfc4301>>.
- [RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <<https://www.rfc-editor.org/info/rfc4302>>.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <<https://www.rfc-editor.org/info/rfc4303>>.

- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, DOI 10.17487/RFC5374, November 2008, <<https://www.rfc-editor.org/info/rfc5374>>.
- [RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <<https://www.rfc-editor.org/info/rfc5415>>.
- [RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <<https://www.rfc-editor.org/info/rfc5889>>.
- [RFC6059] Krishnan, S. and G. Daley, "Simple Procedures for Detecting Network Attachment in IPv6", RFC 6059, DOI 10.17487/RFC6059, November 2010, <<https://www.rfc-editor.org/info/rfc6059>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <<https://www.rfc-editor.org/info/rfc6275>>.
- [RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <<https://www.rfc-editor.org/info/rfc6959>>.
- [RFC7042] Eastlake 3rd, D. and J. Abley, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 7042, DOI 10.17487/RFC7042, October 2013, <<https://www.rfc-editor.org/info/rfc7042>>.
- [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <<https://www.rfc-editor.org/info/rfc7136>>.

- [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <<https://www.rfc-editor.org/info/rfc7217>>.
- [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <<https://www.rfc-editor.org/info/rfc7721>>.
- [RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <<https://www.rfc-editor.org/info/rfc8064>>.
- [RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <<https://www.rfc-editor.org/info/rfc8065>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.

9.2. Informative References

- [ETSI-sec-archi]
"ETSI TS 102 940 V1.2.1 (2016-11), ETSI Technical Specification, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, November 2016. Downloaded on September 9th, 2017, freely available from ETSI website at URL http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf".
- [I-D.ietf-ipwave-vehicular-networking]
Jeong, J., "IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", draft-ietf-ipwave-vehicular-networking-09 (work in progress), May 2019.

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

Perkins, C., McBride, M., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-ietf-mboned-ieee802-mcast-problems-05 (work in progress), April 2019.

[IEEE-1609.2]

"IEEE SA - 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Security Services for Applications and Management Messages. Example URL <http://ieeexplore.ieee.org/document/7426684/> accessed on August 17th, 2017."

[IEEE-1609.3]

"IEEE SA - 1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services. Example URL <http://ieeexplore.ieee.org/document/7458115/> accessed on August 17th, 2017."

[IEEE-1609.4]

"IEEE SA - 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation. Example URL <http://ieeexplore.ieee.org/document/7435228/> accessed on August 17th, 2017."

[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>".

[IEEE-802.11p-2010]

"IEEE Std 802.11p (TM)-2010, 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, Amendment 6: Wireless Access in Vehicular Environments; document freely available at URL <http://standards.ieee.org/getieee802/download/802.11p-2010.pdf> retrieved on September 20th, 2013."

[RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <<https://www.rfc-editor.org/info/rfc3753>>.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <<https://www.rfc-editor.org/info/rfc3963>>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <<https://www.rfc-editor.org/info/rfc3971>>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <<https://www.rfc-editor.org/info/rfc3972>>.

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 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:

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

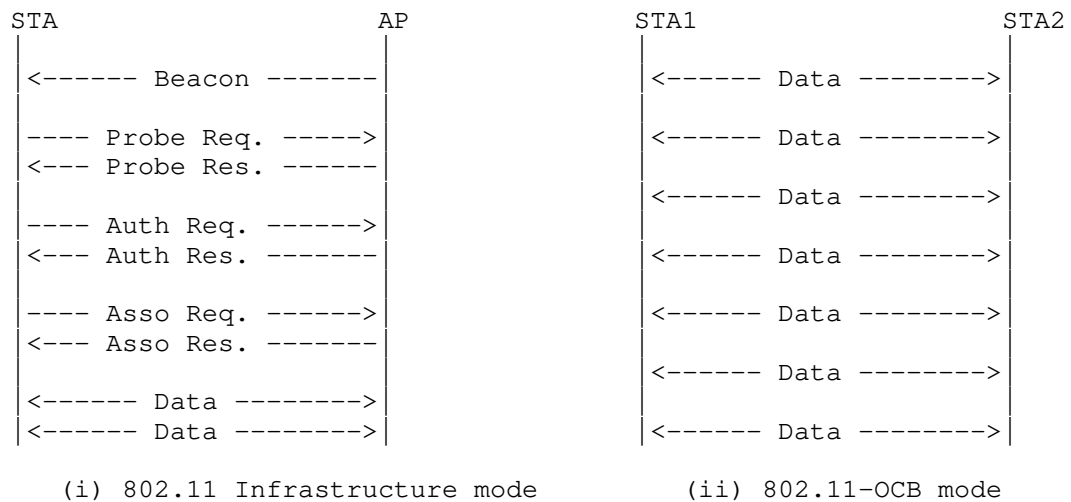


Figure 1: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

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-OBUS 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.

- o 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.
- o 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.

- o 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).
- o '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.
- o 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:

- o 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.
- o The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.
- o The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).
- o 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:

- o 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).

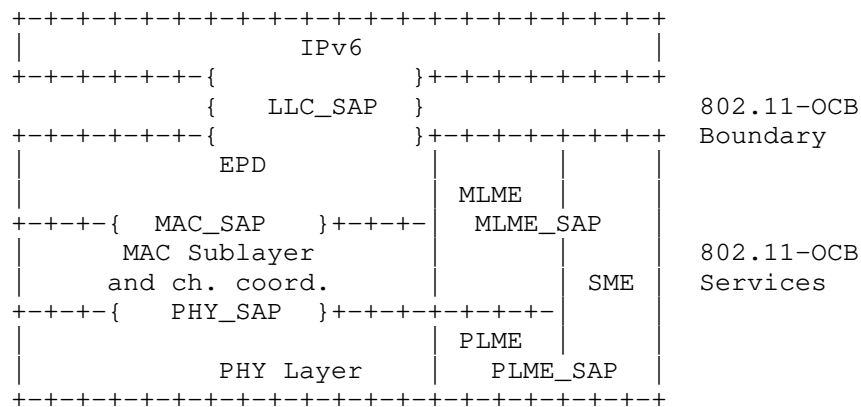


Figure 2: EtherType Protocol Discrimination

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:

- o The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- o The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CF-Ack;
- o 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).

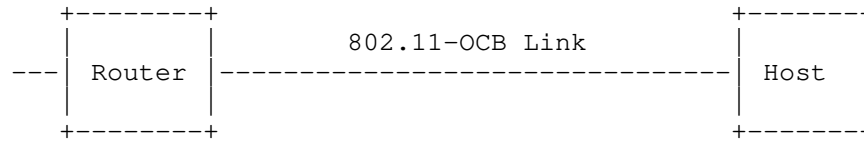


Figure 3: Topology for capturing IP packets on 802.11-OCB

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 |
+-----+

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

Router Advertisement

```

```

+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Code      |      Checksum      |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Cur Hop Limit |M|O|  Reserved  |      Router Lifetime      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Reachable Time                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Retrans Timer                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Options ...      |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

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...
+++++
...Destination | Source...
+++++
...Source |
+++++
| Type |
+++++

```

IPv6 Base Header

```

+++++
|Version| Traffic Class | Flow Label |
+++++
| Payload Length | Next Header | Hop Limit |
+++++
|
+
|
+
Source Address
+
|
+++++
|
+
|
+
Destination Address
+
|
+++++

```

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 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

IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 10, 2020

N. Benamar
Moulay Ismail University of Meknes
J. Haerri
Eurecom
J. Lee
Sangmyung University
T. Ernst
YoGoKo
August 9, 2019

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

Authors' Addresses	31
--------------------	----

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:

- o 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].
- o 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 dot11OCBActivated 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:

- o Bit "Local/Global" set to "locally administered".
- o Bit "Unicast/Multicast" set to "Unicast".
- o 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, 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

[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>".

[RFC1042] Postel, J. and J. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", STD 43, RFC 1042, DOI 10.17487/RFC1042, February 1988, <<https://www.rfc-editor.org/info/rfc1042>>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <<https://www.rfc-editor.org/info/rfc2464>>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <<https://www.rfc-editor.org/info/rfc4086>>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <<https://www.rfc-editor.org/info/rfc4191>>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <<https://www.rfc-editor.org/info/rfc4193>>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.

- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <<https://www.rfc-editor.org/info/rfc4301>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <<https://www.rfc-editor.org/info/rfc5415>>.
- [RFC6059] Krishnan, S. and G. Daley, "Simple Procedures for Detecting Network Attachment in IPv6", RFC 6059, DOI 10.17487/RFC6059, November 2010, <<https://www.rfc-editor.org/info/rfc6059>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <<https://www.rfc-editor.org/info/rfc6275>>.
- [RFC7042] Eastlake 3rd, D. and J. Abley, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 7042, DOI 10.17487/RFC7042, October 2013, <<https://www.rfc-editor.org/info/rfc7042>>.
- [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <<https://www.rfc-editor.org/info/rfc7136>>.
- [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <<https://www.rfc-editor.org/info/rfc7217>>.
- [RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <<https://www.rfc-editor.org/info/rfc8064>>.

- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.

9.2. Informative References

- [ETSI-sec-archi]
"ETSI TS 102 940 V1.2.1 (2016-11), ETSI Technical Specification, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, November 2016. Downloaded on September 9th, 2017, freely available from ETSI website at URL http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf".
- [I-D.ietf-ipwave-vehicular-networking]
Jeong, J., "IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", draft-ietf-ipwave-vehicular-networking-11 (work in progress), July 2019.
- [I-D.ietf-mboned-ieee802-mcast-problems]
Perkins, C., McBride, M., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-ietf-mboned-ieee802-mcast-problems-07 (work in progress), July 2019.
- [IEEE-1609.2]
"IEEE SA - 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Security Services for Applications and Management Messages. Example URL <http://ieeexplore.ieee.org/document/7426684/> accessed on August 17th, 2017."
- [IEEE-1609.3]
"IEEE SA - 1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services. Example URL <http://ieeexplore.ieee.org/document/7458115/> accessed on August 17th, 2017."

- [IEEE-1609.4]
"IEEE SA - 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation. Example URL
<http://ieeexplore.ieee.org/document/7435228/> accessed on August 17th, 2017."
- [IEEE-802.11p-2010]
"IEEE Std 802.11p (TM)-2010, 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, Amendment 6: Wireless Access in Vehicular Environments; document freely available at URL
<http://standards.ieee.org/getieee802/download/802.11p-2010.pdf> retrieved on September 20th, 2013."
- [RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <<https://www.rfc-editor.org/info/rfc3753>>.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <<https://www.rfc-editor.org/info/rfc3963>>.
- [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <<https://www.rfc-editor.org/info/rfc3971>>.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <<https://www.rfc-editor.org/info/rfc3972>>.
- [RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <<https://www.rfc-editor.org/info/rfc5889>>.
- [RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <<https://www.rfc-editor.org/info/rfc6959>>.

- [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <<https://www.rfc-editor.org/info/rfc7721>>.
- [RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <<https://www.rfc-editor.org/info/rfc8065>>.
- [SHA256] "Secure Hash Standard (SHS), National Institute of Standards and Technology. <https://csrc.nist.gov/CSRC/media/Publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf>".

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 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:

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

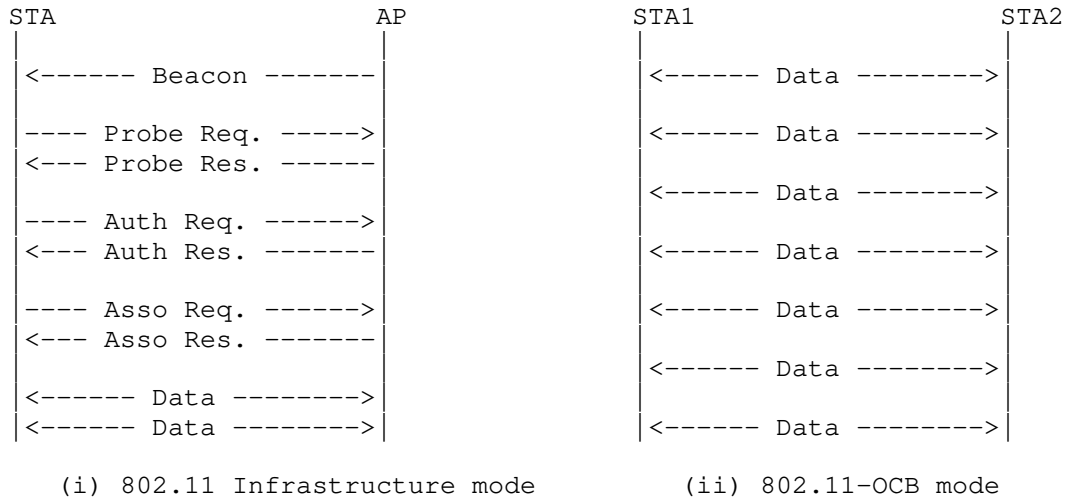


Figure 1: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

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-OBUS 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.

- o 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 0xfffffffffff (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.
- o 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.
- o 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).

- o '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.
- o 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:

- o 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.
- o The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.
- o The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).
- o 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:

- o 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).

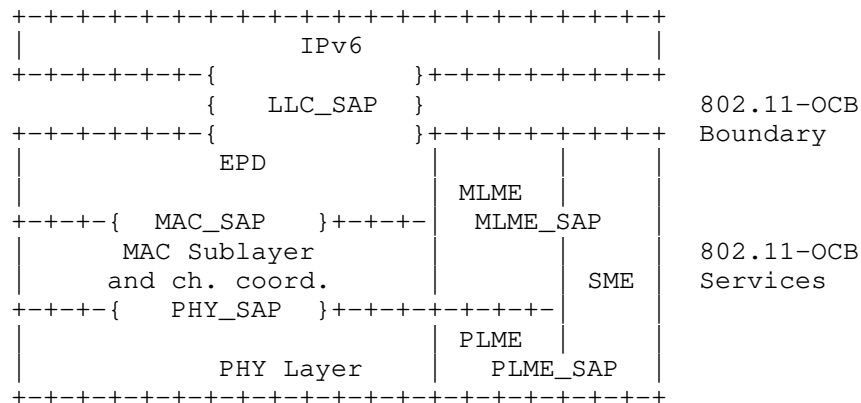


Figure 2: EtherType Protocol Discrimination

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:

- o The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- o The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFack;
- o 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).

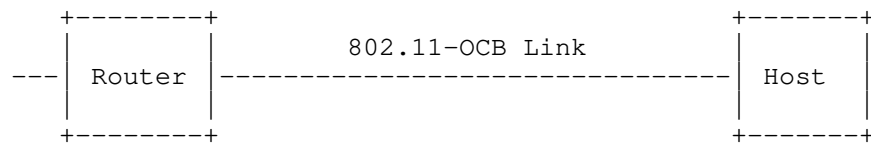


Figure 3: Topology for capturing IP packets on 802.11-OCB

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 |
+-----+-----+-----+-----+-----+-----+-----+-----+

```


IPv6 Base Header

[illegible]

Router Advertisement

Type	Code	Checksum
Cur Hop Limit	M O Reserved	Router Lifetime
Reachable Time		
Retrans Timer		
Options ...		

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...
+-----+
...Destination | Source...
+-----+
...Source
+-----+
|               Type               |
+-----+

```

IPv6 Base Header

```

+-----+
| Version | Traffic Class | Flow Label |
+-----+
| Payload Length | Next Header | Hop Limit |
+-----+
|
+
|
+
| Source Address
+
|
+
|
+
|
+
| Destination Address
+
|
+
+-----+

```

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 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 [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

IPWAVE Working Group
Internet-Draft
Intended status: Informational
Expires: November 25, 2019

J. Jeong, Ed.
Sungkyunkwan University
May 24, 2019

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

(<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	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-08	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. 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:

- o 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.

- 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 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.
- o V2I2P: Acronym for "Vehicle to Infrastructure to Pedestrian".
- o V2I2V: Acronym for "Vehicle to Infrastructure to Vehicle".
- o 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

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

- o Navigation service;
- o Energy-efficient speed recommendation service;
- o 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.

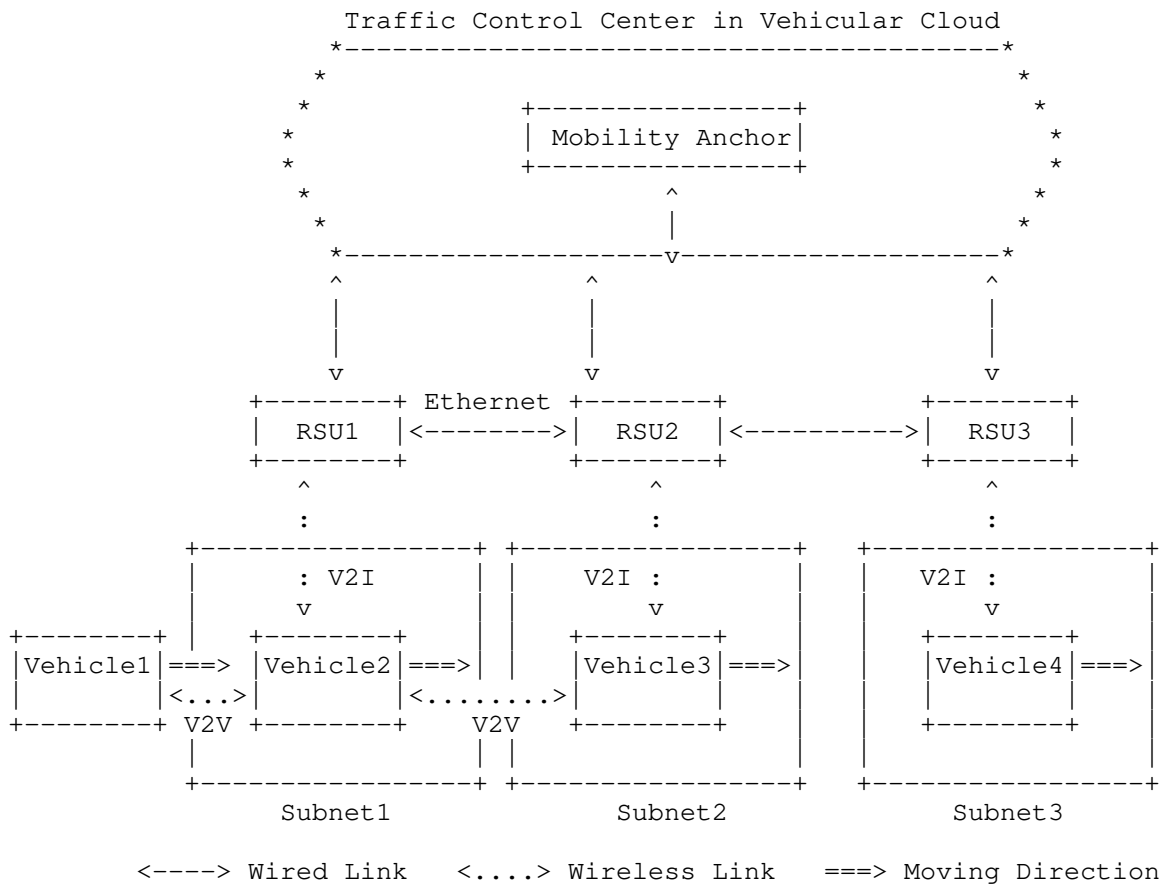


Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

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. 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.

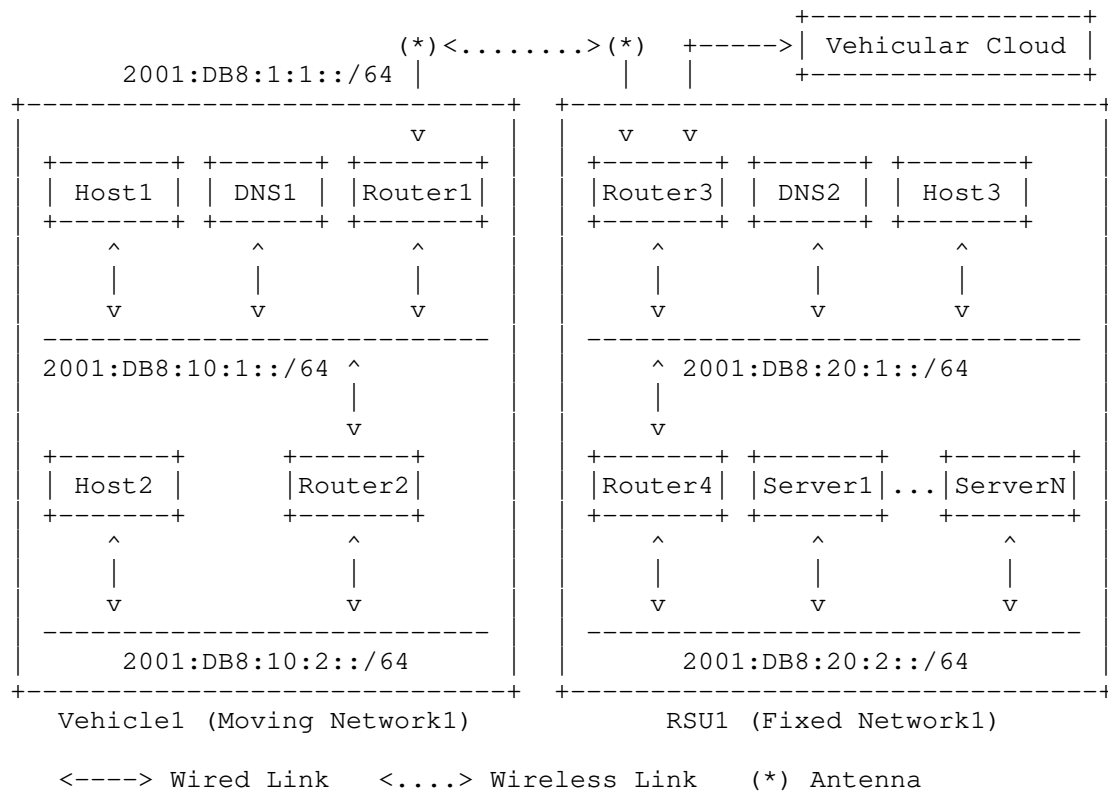


Figure 2: Internetworking between Vehicle Network and RSU Network

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.

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.

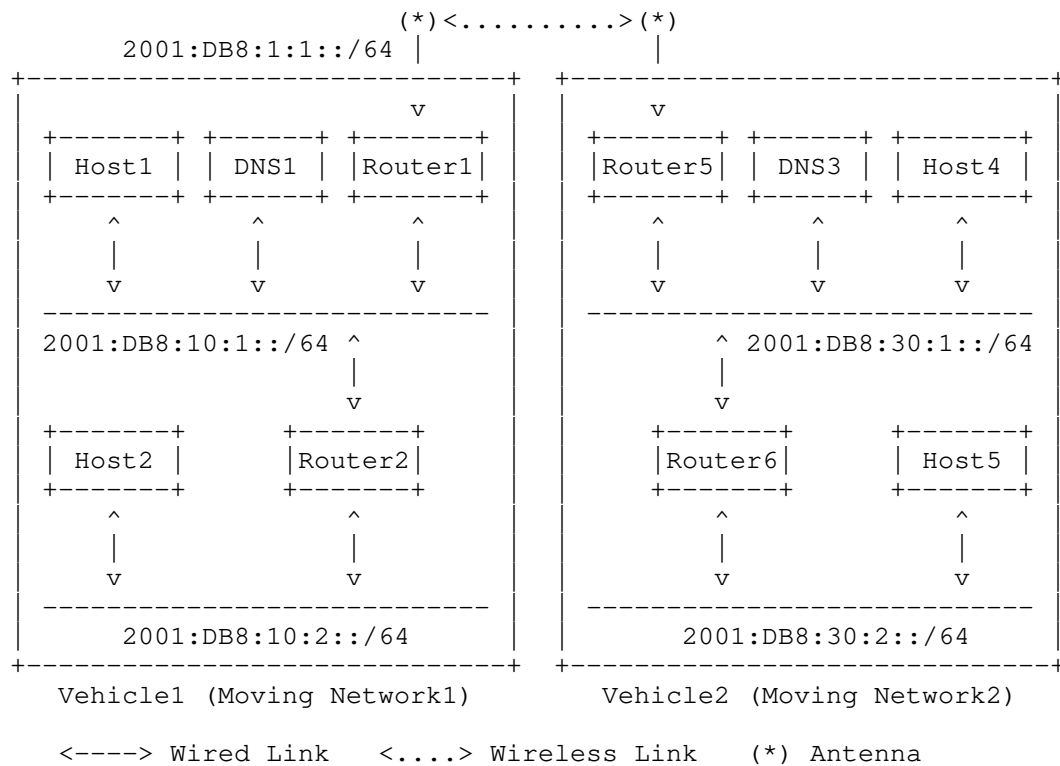


Figure 3: Internetworking between Two Vehicle Networks

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.

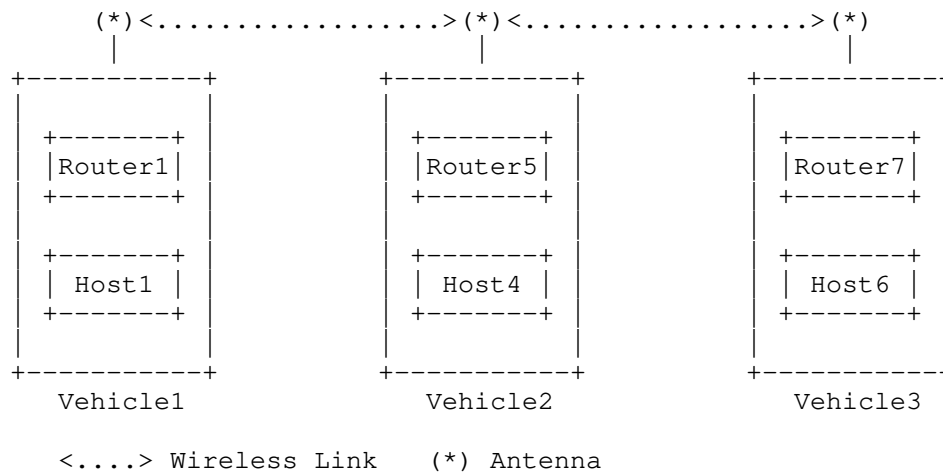


Figure 4: Multihop Internetworking between Two Vehicle Networks

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 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 Discovey (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 need 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]

Choi, J., Va, V., Gonzalez-Prelcic, N., Daniels, R., R. Bhat, C., and R. W. Heath, "Millimeter-Wave Vehicular Communication to Support Massive Automotive Sensing", IEEE Communications Magazine, December 2016.

[CA-Cruise-Control]

California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", [Online] Available:
<http://www.path.berkeley.edu/research/automated-and-connected-vehicles/cooperative-adaptive-cruise-control>, 2017.

- [CASD] Shen, Y., Jeong, J., Oh, T., and S. Son, "CASD: A Framework of Context-Awareness Safety Driving in Vehicular Networks", International Workshop on Device Centric Cloud (DC2), March 2016.
- [DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), October 2010.
- [ETSI-GeoNetwork-IP]
ETSI Technical Committee Intelligent Transport Systems, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols", ETSI EN 302 636-6-1, October 2013.
- [ETSI-GeoNetworking]
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.
- [EU-2008-671-EC]
European Union, "Commission Decision of 5 August 2008 on the Harmonised Use of Radio Spectrum in the 5875 - 5905 MHz Frequency Band for Safety-related Applications of Intelligent Transport Systems (ITS)", EU 2008/671/EC, August 2008.
- [FirstNet]
U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", [Online]
Available: <https://www.firstnet.gov/>, 2012.
- [FirstNet-Report]
First Responder Network Authority, "FY 2017: ANNUAL REPORT TO CONGRESS, Advancing Public Safety Broadband Communications", FirstNet FY 2017, December 2017.

[Fuel-Efficient]

van de Hoef, S., H. Johansson, K., and D. V. Dimarogonas, "Fuel-Efficient En Route Formation of Truck Platoons", IEEE Transactions on Intelligent Transportation Systems, January 2018.

[ID-Vehicular-MM]

Jeong, J., Ed., Shen, Y., and Z. Xiang, "Vehicular Mobility Management for IP-Based Vehicular Networks", draft-jeong-ipwave-vehicular-mobility-management-00 (work in progress), March 2019.

[ID-Vehicular-ND]

Jeong, J., Ed., Shen, Y., and Z. Xiang, "IPv6 Neighbor Discovery for IP-Based Vehicular Networks", draft-jeong-ipwave-vehicular-neighbor-discovery-06 (work in progress), March 2019.

[Identity-Management]

Wetterwald, M., Hrizi, F., and P. Cataldi, "Cross-layer Identities Management in ITS Stations", The 10th International Conference on ITS Telecommunications, November 2010.

[IEEE-802.11-OCB]

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

[IEEE-802.11p]

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

[Intro-to-Algorithms]

H. Cormen, T., E. Leiserson, C., L. Rivest, R., and C. Stein, "Introduction to Algorithms, 3rd ed.", The MIT Press, July 2009.

[IPv6-over-802.11-OCB]

Benamar, N., Haerri, J., Lee, J., and T. Ernst, "Transmission of IPv6 Packets over IEEE 802.11 Networks operating in mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)", draft-ietf-ipwave-ipv6-over-80211ocb-45 (work in progress), April 2019.

- [ISO-ITS-IPv6] ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012.
- [RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.
- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", RFC 4086, June 2005.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861, September 2007.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.
- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.
- [RFC5944] Perkins, C., Ed., "IP Mobility Support in IPv4, Revised", RFC 5944, November 2010.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.
- [RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, April 2014.

- [RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.
- [RFC7429] Liu, D., Zuniga, JC., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, January 2015.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 8200, July 2017.
- [RFC8505] Thubert, P., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, November 2018.
- [SAINT] Jeong, J., Jeong, H., Lee, E., Oh, T., and D. Du, "SAINT: Self-Adaptive Interactive Navigation Tool for Cloud-Based Vehicular Traffic Optimization", IEEE Transactions on Vehicular Technology, Vol. 65, No. 6, June 2016.
- [SAINTplus] Shen, Y., Lee, J., Jeong, H., Jeong, J., Lee, E., and D. Du, "SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization", IEEE Transactions on Intelligent Transportation Systems, June 2017.
- [SANA] Hwang, T. and J. Jeong, "SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks", Springer Lecture Notes in Computer Science (LNCS), Vol. 9502, December 2015.
- [SDN-DMM] Nguyen, T., Bonnet, C., and J. Harri, "SDN-based Distributed Mobility Management for 5G Networks", IEEE Wireless Communications and Networking Conference, April 2016.
- [Truck-Platooning] California Partners for Advanced Transportation Technology (PATH), "Automated Truck Platooning", [Online] Available: <http://www.path.berkeley.edu/research/automated-and-connected-vehicles/truck-platooning>, 2017.
- [TS-23.285-3GPP] 3GPP, "Architecture Enhancements for V2X Services", 3GPP TS 23.285, June 2018.

[VIP-WAVE]

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

[WAVE-1609.0]

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

[WAVE-1609.2]

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

[WAVE-1609.3]

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

[WAVE-1609.4]

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

Appendix A. Changes from draft-ietf-ipwave-vehicular-networking-08

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

- o This version is revised based on the comments from Charlie Perkins and Sri Gundavelli.
- o 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 Lozano (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

Sandra Cespedes
NIC Chile Research Labs
Universidad de Chile
Av. Blanco Encalada 1975
Santiago
Chile

Phone: +56 2 29784093
EMail: scespede@niclabs.cl

Jerome Haerri
Communication Systems Department
EURECOM
Sophia-Antipolis
France

Phone: +33 4 93 00 81 34
EMail: jerome.haerri@eurecom.fr

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

Phone: +86 13911788933
EMail: max.ldp@alibaba-inc.com

Tae (Tom) Oh
Department of Information Sciences and Technologies
Rochester Institute of Technology
One Lomb Memorial Drive
Rochester, NY 14623-5603
USA

Phone: +1 585 475 7642
EMail: Tom.Oh@rit.edu

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4586
EMail: charliep@computer.org

Alexandre Petrescu
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
France

Phone: +33169089223
EMail: Alexandre.Petrescu@cea.fr

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

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu
URI: <http://iotlab.skku.edu/people-chris-shen.php>

Michelle Wetterwald
FBConsulting
21, Route de Luxembourg
Wasserbillig, Luxembourg L-6633
Luxembourg

EMail: Michelle.Wetterwald@gmail.com

Author's Address

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

Phone: +82 31 299 4957

Fax: +82 31 290 7996

EMail: pauljeong@skku.edu

URI: <http://iotlab.skku.edu/people-jaehoon-jeong.php>

IPWAVE Working Group
Internet-Draft
Intended status: Informational
Expires: 1 October 2022

J. Jeong, Ed.
Sungkyunkwan University
30 March 2022

IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem
Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-28

Abstract

This document discusses the problem statement and use cases of IPv6-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, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then enumerates requirements for the extensions of those IPv6 protocols for IPv6-based vehicular networking.

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 1 October 2022.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Terminology	4
3. Use Cases	7
3.1. V2V	8
3.2. V2I	10
3.3. V2X	12
4. Vehicular Networks	13
4.1. Vehicular Network Architecture	14
4.2. V2I-based Internetworking	16
4.3. V2V-based Internetworking	19
5. Problem Statement	22
5.1. Neighbor Discovery	23
5.1.1. Link Model	25
5.1.2. MAC Address Pseudonym	27
5.1.3. Routing	27
5.2. Mobility Management	29
6. Security Considerations	31
6.1. Security Threats in Neighbor Discovery	32
6.2. Security Threats in Mobility Management	33
6.3. Other Threats	33
7. IANA Considerations	35
8. References	35
8.1. Normative References	35
8.2. Informative References	40
Appendix A. Support of Multiple Radio Technologies for V2V	46
Appendix B. Support of Multihop V2X Networking	46
Appendix C. Support of Mobility Management for V2I	48
Appendix D. Support of MTU Diversity for IP-based Vehicular Networks	49
Appendix E. Acknowledgments	50
Appendix F. Contributors	51
Author's Address	52

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]. Most countries and regions in the world have adopted the same frequency allocation for vehicular networks.

For direct inter-vehicular wireless connectivity, IEEE has amended standard 802.11 (commonly known as Wi-Fi) to enable safe driving 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].

3GPP has standardized Cellular Vehicle-to-Everything (C-V2X) communications to support V2X in LTE mobile networks (called LTE V2X) and V2X in 5G mobile networks (called 5G V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. With C-V2X, vehicles can directly communicate with each other without relay nodes (e.g., eNodeB in LTE and gNodeB in 5G).

Along with these WAVE standards and C-V2X standards, regardless of a wireless access technology under the IP stack of a vehicle, vehicular networks can operate IP mobility with IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Network Mobility (NEMO) [RFC3963], Locator/ID Separation Protocol (LISP) [I-D.ietf-lisp-rfc6830bis], and Automatic Extended Route Optimization based on the Overlay Multilink Network Interface (AERO/OMNI) [I-D.templin-6man-aero] [I-D.templin-6man-omni]). 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][ISO-ITS-IPv6-AMD1].

This document describes use cases and a problem statement about IPv6-based vehicular networking for ITS, which is named IPv6 Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then enumerates requirements for the extensions of those IPv6 protocols, which are tailored to IPv6-based vehicular networking. Thus, this document is intended to motivate development of key protocols for IPWAVE.

2. Terminology

This document uses the terminology described in [RFC8691]. In addition, the following terms are defined below:

- * Class-Based Safety Plan: A vehicle can make a safety plan by classifying the surrounding vehicles into different groups for safety purposes according to the geometrical relationship among them. The vehicle groups can be classified as Line-of-Sight Unsafe, Non-Line-of-Sight Unsafe, and Safe groups [CASD].
- * Context-Awareness: A vehicle can be aware of spatial-temporal mobility information (e.g., position, speed, direction, and acceleration/deceleration) of surrounding vehicles for both safety and non-safety uses through sensing or communication [CASD].
- * DMM: "Distributed Mobility Management" [RFC7333][RFC7429].
- * Edge Computing (EC): It is the local computing near an access network (i.e., edge network) for the sake of vehicles and pedestrians.
- * Edge Computing Device (ECD): It is a computing device (or server) for edge computing for the sake of vehicles and pedestrians.

- * Edge Network (EN): It is an access network that has an IP-RSU for wireless communication with other vehicles having an IP-OBU and wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and MA). It may have a Global Positioning System (GPS) radio receiver for its position recognition and the localization service for the sake of vehicles.
- * IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, autobike, motorcycle, and a similar one). It has at least one IP interface that runs in IEEE 802.11-OCB and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. It can play a role of a router connecting multiple computers (or in-vehicle devices) inside a vehicle. See the definition of the term "OBU" in [RFC8691].
- * IP-RSU: "IP Roadside 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 over an 802.11 wireless link operating in OCB mode. Also, it may have the third IP-enabled wireless interface running in 3GPP C-V2X in addition to the IP-RSU defined in [RFC8691]. An IP-RSU is similar to an Access Network Router (ANR), defined in [RFC3753], and a Wireless Termination Point (WTP), defined in [RFC5415]. See the definition of the term "RSU" in [RFC8691].
- * 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.
- * Mobility Anchor (MA): A node that maintains IPv6 addresses and mobility information of vehicles in a road network to support their IPv6 address autoconfiguration and mobility management with a binding table. An MA has End-to-End (E2E) connections (e.g., tunnels) with IP-RSUs under its control for the address autoconfiguration and mobility management of the vehicles. This MA is similar to a Local Mobility Anchor (LMA) in PMIPv6 [RFC5213] for network-based mobility management.
- * OCB: "Outside the Context of a Basic Service Set - BSS". It is a mode of operation in which a Station (STA) is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality [IEEE-802.11-OCB].

- * 802.11-OCB: It refers to the mode specified in IEEE Std 802.11-2016 [IEEE-802.11-OCB] when the MIB attribute dot11OCBActivated is 'true'.
- * Platooning: Moving vehicles can be grouped together to reduce air-resistance for energy efficiency and reduce the number of drivers such that only the leading vehicle has a driver, and the other vehicles are autonomous vehicles without a driver and closely follow the leading vehicle [Truck-Platooning].
- * Traffic Control Center (TCC): A system that manages road infrastructure nodes (e.g., IP-RSUs, MAs, traffic signals, and loop detectors), and also maintains 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 part of a vehicular cloud for vehicular networks.
- * Vehicle: A Vehicle in this document is a node that has an IP-OBU for wireless communication with other vehicles and IP-RSUs. It has a GPS radio navigation receiver for efficient navigation. Any device having an IP-OBU and a GPS receiver (e.g., smartphone and tablet PC) can be regarded as a vehicle in this document.
- * 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.
- * Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network forwarding elements (e.g., switch and router).
- * V2D: "Vehicle to Device". It is the wireless communication between a vehicle and a device (e.g., smartphone and IoT device).
- * V2I2D: "Vehicle to Infrastructure to Device". It is the wireless communication between a vehicle and a device (e.g., smartphone and IoT device) via an infrastructure node (e.g., IP-RSU).
- * V2I2V: "Vehicle to Infrastructure to Vehicle". It is the wireless communication between a vehicle and another vehicle via an infrastructure node (e.g., IP-RSU).

- * V2I2X: "Vehicle to Infrastructure to Everything". It is the wireless communication between a vehicle and another entity (e.g., vehicle, smartphone, and IoT device) via an infrastructure node (e.g., IP-RSU).
- * V2X: "Vehicle to Everything". It is the wireless communication between a vehicle and any entity (e.g., vehicle, infrastructure node, smartphone, and IoT device), including V2V, V2I, and V2D.
- * VIP: "Vehicular Internet Protocol". It is an IPv6 extension for vehicular networks including V2V, V2I, and V2X.
- * VMM: "Vehicular Mobility Management". It is an IPv6-based mobility management for vehicular networks.
- * VND: "Vehicular Neighbor Discovery". It is an IPv6 ND extension for vehicular networks.
- * VSP: "Vehicular Security and Privacy". It is an IPv6-based security and privacy term for vehicular networks.
- * 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).

IP is widely used among popular end-user devices (e.g., smartphone and tablet) in the Internet. Applications (e.g., navigator application) for those devices can be extended such that the V2V use cases in this section can work with IPv6 as a network layer protocol and IEEE 802.11-OCB as a link layer protocol. In addition, IPv6 security needs to be extended to support those V2V use cases in a safe, secure, privacy-preserving way.

The use cases presented in this section serve as the description and motivation for the need to augment IPv6 and its protocols to facilitate "Vehicular IPv6". Section 5 summarizes the overall problem statement and IPv6 requirements. Note that the adjective "Vehicular" in this document is used to represent extensions of existing protocols such as IPv6 Neighbor Discovery, IPv6 Mobility Management (e.g., PMIPv6 [RFC5213] and DMM [RFC7429]), and IPv6 Security and Privacy Mechanisms rather than new "vehicular-specific" functions.

3.1. V2V

The use cases of V2V networking discussed in this section include

- * Context-aware navigation for safe driving and collision avoidance;
- * Cooperative adaptive cruise control in a roadway;
- * Platooning in a highway;
- * Cooperative environment sensing;
- * Collision avoidance service of end systems of Urban Air Mobility (UAM).

These five techniques will be important elements for autonomous vehicles, which may be either terrestrial vehicles or UAM end systems.

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely by alerting them to dangerous obstacles and situations. That is, a 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 individual 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 a collision.

Platooning [Truck-Platooning] allows a series (or group) 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 (e.g., air pollution, hazards/obstacles, slippery areas by snow or rain, road accidents, traffic congestion, and driving behaviors of neighboring vehicles) from various vehicle-mounted sensors, such as radars, LiDARs, and cameras, with other vehicles and pedestrians. [Automotive-Sensing] introduces 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 cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment. Vehicles can also share their intended maneuvering information (e.g., lane change, speed change, ramp in-and-out, cut-in, and abrupt braking) with neighboring vehicles. Thus, this information sharing can help the vehicles behave as more efficient traffic flows and minimize unnecessary acceleration and deceleration to achieve the best ride comfort.

A collision avoidance service of UAM end systems in air can be envisioned as a use case in air vehicular environments [I-D.templin-ipwave-uam-its]. This use case is similar to the context-aware navigator for terrestrial vehicles. Through V2V coordination, those UAM end systems (e.g., drones) can avoid a dangerous situation (e.g., collision) in three-dimensional space rather than two-dimensional space for terrestrial vehicles. Also, UAM end systems (e.g., flying car) with only a few meters off the ground can communicate with terrestrial vehicles with wireless communication technologies (e.g., DSRC, LTE, and C-V2X). Thus, V2V means any vehicle to any vehicle, whether the vehicles are ground-level or not.

To encourage more vehicles to participate in this cooperative environmental sensing, a reward system will be needed. Sensing activities of each vehicle need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) through other vehicles or infrastructure. In the case of a blockchain, each sensing message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain].

To support applications of these V2V use cases, the required functions of IPv6 include IPv6-based packet exchange and secure, safe communication between two vehicles. For the support of V2V under multiple radio technologies (e.g., DSRC and 5G V2X), refer to Appendix A.

3.2. V2I

The use cases of V2I networking discussed in this section include

- * Navigation service;
- * Energy-efficient speed recommendation service;
- * Accident notification service;
- * Electric vehicle (EV) charging service;
- * UAM navigation service with efficient battery charging.

A navigation service, for example, the Self-Adaptive Interactive Navigation Tool (SAINT) [SAINT], using V2I networking interacts with a TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles along 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.

Either a TCC or an ECD can recommend an energy-efficient speed to a vehicle that depends on its traffic environment and traffic signal scheduling [SignalGuru]. For example, when a vehicle approaches an intersection area and a red traffic light for the vehicle becomes turned on, it needs to reduce its speed to save fuel consumption. In this case, either a TCC or an ECD, which has the up-to-date trajectory of the vehicle and the traffic light schedule, can notify the vehicle of an appropriate speed for fuel efficiency. [Fuel-Efficient] studies fuel-efficient route and speed plans for platooned trucks.

The emergency communication between accident vehicles (or emergency vehicles) and a TCC can be performed via either IP-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 using 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 the near future. An equivalent project in Europe is called Public Safety Communications Europe (PSCE) [PSCE], which is developing a network for emergency communications.

An EV charging service with V2I can facilitate the efficient battery charging of EVs. In the case where an EV charging station is connected to an IP-RSU, an EV can be guided toward the deck of the EV charging station or be notified that the charging station is out of service through a battery charging server connected to the IP-RSU. In addition to this EV charging service, other value-added services (e.g., air firmware/software update and media streaming) can be provided to an EV while it is charging its battery at the EV charging station.

A UAM navigation service with efficient battery charging can plan the battery charging schedule of UAM end systems (e.g., drone) for long-distance flying [CBDN]. For this battery charging schedule, a UAM end system can communicate with an infrastructure node (e.g., IP-RSU) toward a cloud server via V2I communications. This cloud server can coordinate the battery charging schedules of multiple UAM end systems for their efficient navigation path, considering flight time from their current position to a battery charging station, waiting time in a waiting queue at the station, and battery charging time at the station.

In some scenarios such as vehicles moving in highways or staying in parking lots, a V2V2I network is necessary for vehicles to access the Internet since some vehicles may not be covered by an RSU. For those vehicles, a few relay vehicles can help to build the Internet access. For the nested NEMO described in [RFC4888], hosts inside a vehicle shown in Figure 3 for the case of V2V2I may have the same issue in the nested NEMO scenario.

To better support these use cases, the existing IPv6 protocol must be augmented either through protocol changes or by including a new adaptation layer in the architecture that efficiently maps IPv6 to a diversity of link layer technologies. Augmentation is necessary to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles as packet forwarders. Thus, IPv6 needs to be extended for multihop V2I communications.

To support applications of these V2I use cases, the required functions of IPv6 include IPv6 communication enablement with neighborhood discovery and IPv6 address management, reachability with adapted network models and routing methods, transport-layer session continuity, and secure, safe communication between a vehicle and an infrastructure node (e.g., IP-RSU) in the vehicular network.

3.3. V2X

The use case of V2X networking discussed in this section is for a 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., Wi-Fi) with an IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU. An edge computing device behind the IP-RSU can collect the mobility information from vehicles and pedestrians, compute wireless communication scheduling for the sake of them. This scheduling can save the battery of each pedestrian's smartphone by allowing it to work in sleeping mode before the communication with vehicles, considering their mobility.

For Vehicle-to-Pedestrian (V2P), a vehicle can directly communicate with a pedestrian's smartphone by V2X without IP-RSU relaying. Light-weight mobile nodes such as bicycles may also communicate directly with a vehicle for collision avoidance using V2V. Note that it is true that a pedestrian or a cyclist may have a higher risk of being hit by a vehicle if they are not with a smartphone in the current setting. For this case, other human sensing technologies (e.g., moving object detection in images and wireless signal-based human movement detection [LIFS] [DFC]) can be used to provide the motion information of them to vehicles. A vehicle by V2V2I networking can obtain the motion information of a vulnerable road user via an IP-RSU that either employs or connects to a human sensing technology.

The existing IPv6 protocol must be augmented through protocol changes in order to support wireless multihop V2X or V2I2X communications in an urban road network where RSUs are deployed at intersections, so a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles (or pedestrians' smartphones) as packet forwarders. Thus, IPv6 needs to be extended for multihop V2X or V2I2X communications.

To support applications of these V2X use cases, the required functions of IPv6 include IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU.

4. Vehicular Networks

This section describes the context for vehicular networks supporting V2V, V2I, and V2X communications. It describes an internal network within a vehicle or an edge network (called EN). It explains not only the internetworking between the internal networks of a vehicle and an EN via wireless links, but also the internetworking between the internal networks of two vehicles via wireless links.

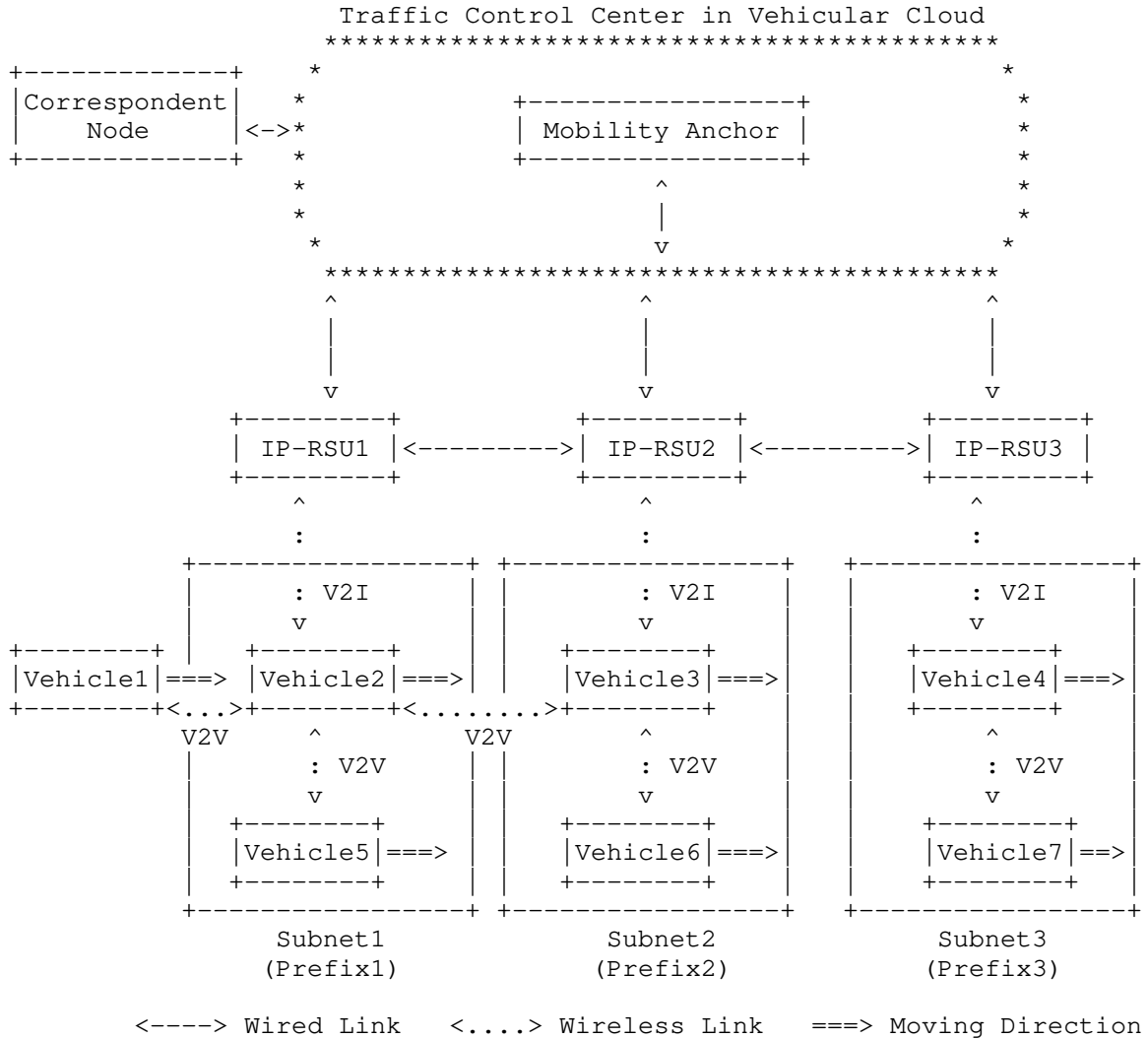


Figure 1: An Example Vehicular Network Architecture for V2I and V2V

4.1. Vehicular Network Architecture

Figure 1 shows an example vehicular network architecture for V2I and V2V in a road network. The vehicular network architecture contains vehicles (including IP-OBUs), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as components. These components are not mandatory, and they can be deployed into vehicular networks in various ways. Some of them (e.g., Mobility Anchor, Traffic Control Center, and Vehicular Cloud) may not be needed for the

vehicular networks according to target use cases in Section 3.

Existing network architectures, such as the network architectures of PMIPv6 [RFC5213], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550], and AERO/OMNI [I-D.templin-6man-aero][I-D.templin-6man-omni], can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. Refer to Appendix B for the detailed discussion on multihop V2X networking by RPL and OMNI. Also, refer to Appendix A for the description of how OMNI is designed to support the use of multiple radio technologies in V2X.

As shown in this figure, IP-RSUs as routers and vehicles with IP-OBUs 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.

In Figure 1, three IP-RSUs (IP-RSU1, IP-RSU2, and IP-RSU3) are deployed in the road network and are connected with each other through the wired networks (e.g., Ethernet). A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of IP-RSUs and vehicles in the road network. A Mobility Anchor (MA) may be located in the TCC as a mobility management controller. Vehicle2, Vehicle3, and Vehicle4 are wirelessly connected to IP-RSU1, IP-RSU2, and IP-RSU3, respectively. The three wireless networks of IP-RSU1, IP-RSU2, and IP-RSU3 can belong to three different subnets (i.e., Subnet1, Subnet2, and Subnet3), respectively. Those three subnets use three different prefixes (i.e., Prefix1, Prefix2, and Prefix3).

Multiple vehicles under the coverage of an RSU share a prefix just as mobile nodes share a prefix of a Wi-Fi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks. For example, in Figure 1, two vehicles (i.e., Vehicle2, and Vehicle5) can use Prefix 1 to configure their IPv6 global addresses for V2I communication. Alternatively, mobile nodes can employ a "Bring-Your-Own-Addresses (BYOA)" (or "Bring-Your-Own-Prefix (BYOP)") technique using their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network, which does not require the messaging (e.g., Duplicate Address Detection (DAD)) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862].

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 of each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., IP-RSU2 and IP-RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range of each other.

As a basic definition for IPv6 packets transported over IEEE 802.11-OCB, [RFC8691] 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 IPv6 mobility solution is needed for the guarantee of communication continuity in vehicular networks so that a vehicle's TCP session can be continued, or UDP packets can be delivered to a vehicle as a destination without loss while it moves from an IP-RSU's wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a correspondent node in the vehicular cloud, Vehicle2 can move from IP-RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213], NEMO [RFC3963][RFC4885] [RFC4888], and AERO [I-D.templin-6man-aero]). This document describes issues in mobility management for vehicular networks in Section 5.2.

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle's internal network (i.e., mobile network) and an EN's internal network (i.e., fixed network) via V2I communication. The internal network of a vehicle is nowadays constructed with Ethernet by many automotive vendors [In-Car-Network]. Note that an EN can accommodate multiple routers (or switches) and servers (e.g., ECDs, navigation server, and DNS server) in its internal network.

A vehicle's internal network often uses Ethernet to interconnect Electronic Control Units (ECUs) in the vehicle. The internal network can support Wi-Fi and Bluetooth to accommodate a driver's and passenger's mobile devices (e.g., smartphone or tablet). The network topology and subnetting depend on each vendor's network configuration for a vehicle and an EN. It is reasonable to consider the interaction between the internal network and an external network within another vehicle or an EN. Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. To minimize this kind of risk, a reinforced identification and verification protocol shall be implemented.

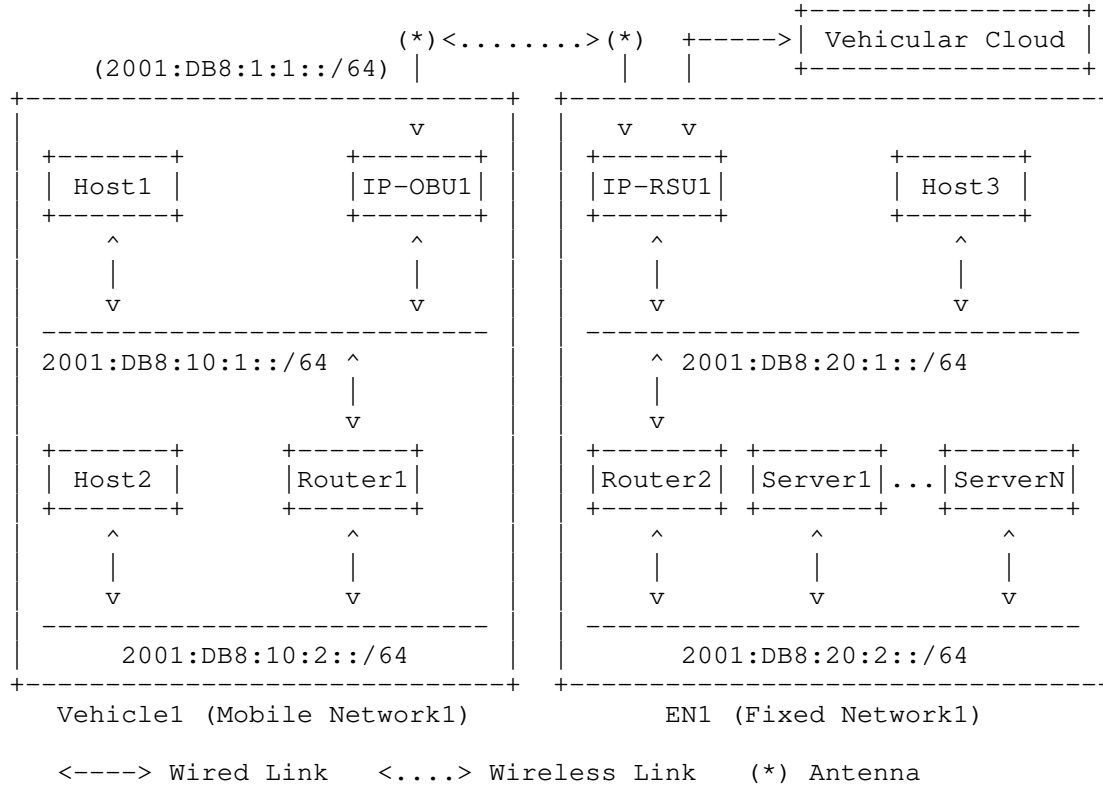


Figure 2: Internetworking between Vehicle and Edge Network

As shown in Figure 2, as internal networks, a vehicle's mobile network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for the communication with another vehicle or another EN. The internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the network prefixes of the internal networks. For the efficiency, the network prefixes of the internal networks (as a mobile network) in a vehicle need to be delegated and configured automatically. Note that a mobile network's network prefix can be called a Mobile Network Prefix (MNP) [RFC3963].

Figure 2 also shows the internetworking between the vehicle's mobile network and the EN's fixed network. There exists an internal network (Mobile Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2), and two routers (IP-OBU1 and Router1). There exists another internal network (Fixed Network1) inside EN1. EN1 has one host (Host3), two routers (IP-RSU1 and Router2), and the collection of

servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1's IP-OBU1 (as a mobile router) and EN1's IP-RSU1 (as a fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2I networking. Thus, a host (Host1) in Vehicle1 can communicate with a server (Server1) in EN1 for a vehicular service through Vehicle1's moving network, a wireless link between IP-OBU1 and IP-RSU1, and EN1's fixed network.

For the IPv6 communication between an IP-OBU and an IP-RSU or between two neighboring IP-OBUs, they need to know the network parameters, which include MAC layer and IPv6 layer information. The MAC layer information includes wireless link layer parameters, transmission power level, and the MAC address of an external network interface for the internetworking with another IP-OBU or IP-RSU. The IPv6 layer information includes the IPv6 address and network prefix of an external network interface for the internetworking with another IP-OBU or IP-RSU.

Through the mutual knowledge of the network parameters of internal networks, packets can be transmitted between the vehicle's moving network and the EN's fixed network. Thus, V2I requires an efficient protocol for the mutual knowledge of network parameters.

As shown in Figure 2, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be link-local IPv6 addresses, ULAs, or global IPv6 addresses. When global IPv6 addresses are used, wireless interface configuration and control overhead for DAD [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways.

Let us consider the upload/download time of a ground vehicle when it passes through the wireless communication coverage of an IP-RSU. For a given typical setting where 1km is the maximum DSRC communication range [DSRC] and 100km/h is the speed limit in highway for ground vehicles, the dwelling time can be calculated to be 72 seconds by dividing the diameter of the 2km (i.e., two times of DSRC communication range where an IP-RSU is located in the center of the circle of wireless communication) by the speed limit of 100km/h (i.e., about 28m/s). For the 72 seconds, a vehicle passing through the coverage of an IP-RSU can upload and download data packets to/from the IP-RSU. For special cases such as emergency vehicles moving above the speed limit, the dwelling time is relatively shorter than that of other vehicles. For cases of airborne vehicles, considering a higher flying speed and a higher altitude, the dwelling time can be much shorter.

4.3. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles via V2V communication.

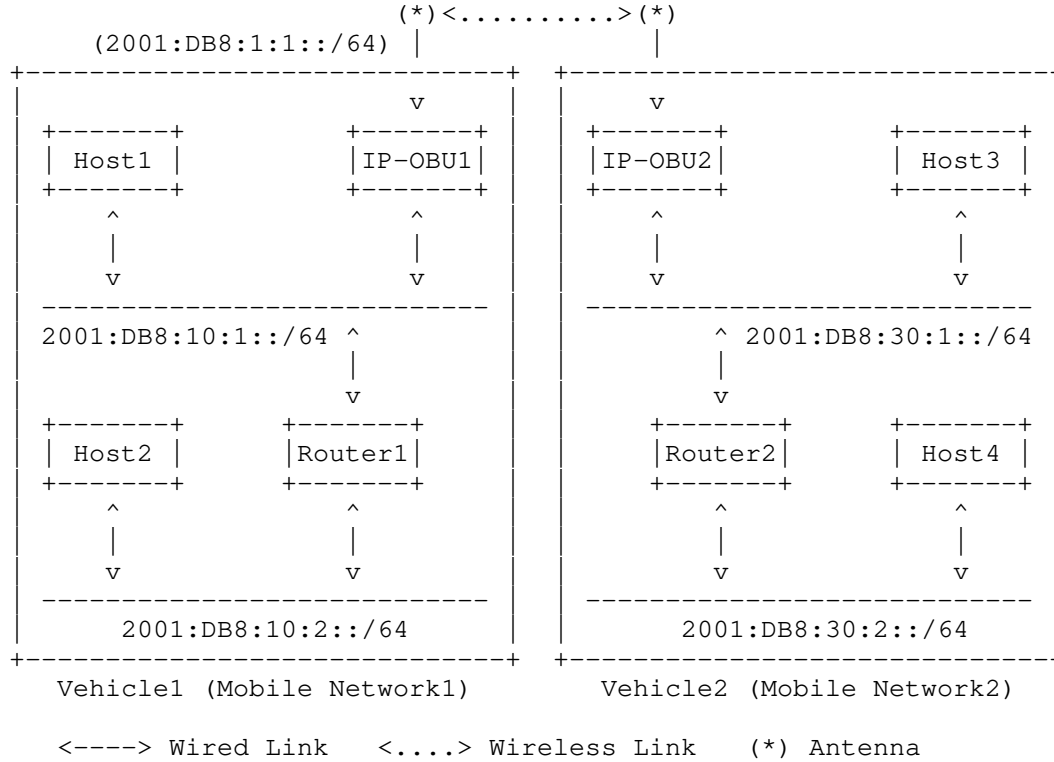


Figure 3: Internetworking between Two Vehicles

Figure 3 shows the internetworking between the mobile networks of two neighboring vehicles. There exists an internal network (Mobile Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2), and two routers (IP-OBU1 and Router1). There exists another internal network (Mobile Network2) inside Vehicle2. Vehicle2 has two hosts (Host3 and Host4), and two routers (IP-OBU2 and Router2). Vehicle1's IP-OBU1 (as a mobile router) and Vehicle2's IP-OBU2 (as a mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. Thus, a host (Host1) in Vehicle1 can communicate with another host (Host3) in Vehicle2 for a vehicular service through Vehicle1's mobile network, a wireless link between IP-OBU1 and IP-OBU2, and Vehicle2's mobile network.

As a V2V use case in Section 3.1, Figure 4 shows the linear network topology of platooning vehicles for V2V communications where Vehicle3 is the leading vehicle with a driver, and Vehicle2 and Vehicle1 are the following vehicles without drivers.

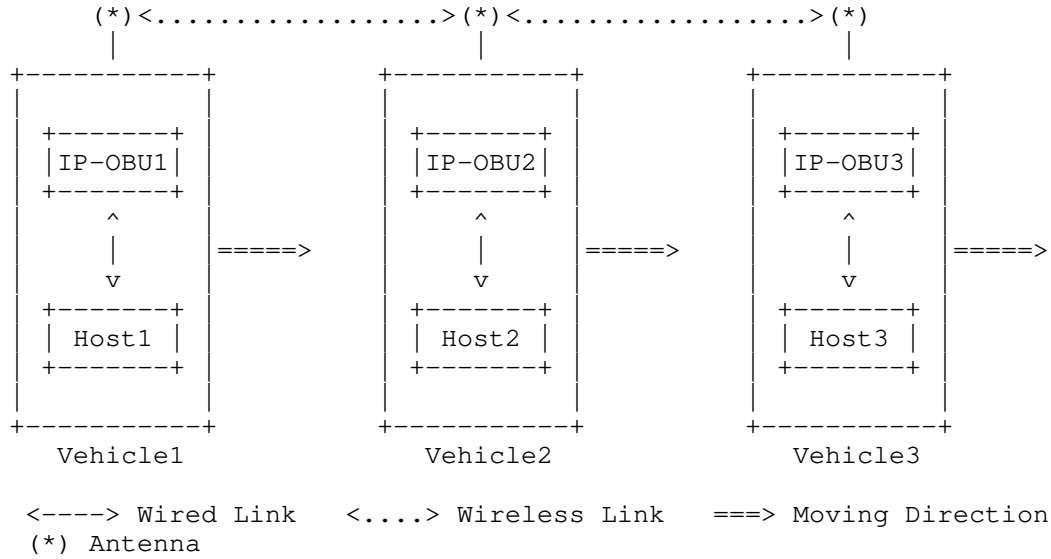


Figure 4: Multihop Internetworking between Two Vehicle Networks

As shown in Figure 4, multihop internetworking is feasible among the mobile networks of three vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-OBU2 in Vehicle2, and IP-OBU3 in Vehicle3 in the VANET, as shown in the figure.

In this section, the link between two vehicles is assumed to be stable for single-hop wireless communication regardless of the sight relationship such as line of sight and non-line of sight, as shown in Figure 3. Even in Figure 4, the three vehicles are connected to each other with a linear topology, however, multihop V2V communication can accommodate any network topology (i.e., an arbitrary graph) over VANET routing protocols.

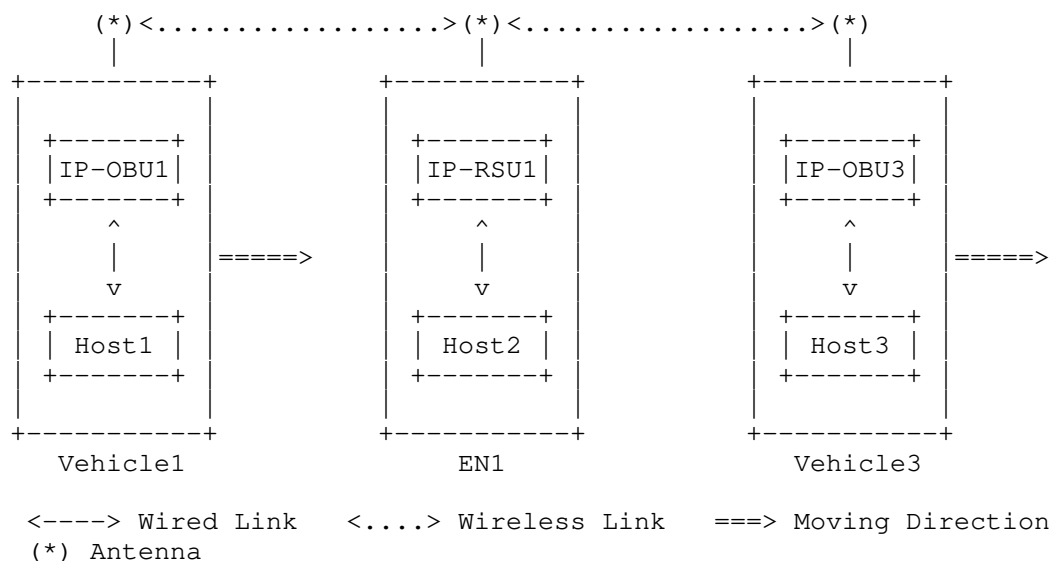


Figure 5: Multihop Internetworking between Two Vehicle Networks via IP-RSU (V2I2V)

As shown in Figure 5, multihop internetworking between two vehicles is feasible via an infrastructure node (i.e., IP-RSU) with wireless connectivity among the mobile networks of two vehicles and the fixed network of an edge network (denoted as EN1) in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-RSU1 in EN1, and IP-OBU3 in Vehicle3 in the VANET, as shown in the figure.

For the reliability required in V2V networking, the ND optimization defined in MANET [RFC6130] [RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases, which serves the MANET routing protocols such as the different versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181], Open Shortest Path First (OSPF) derivatives (e.g., [RFC5614]), and Dynamic Link Exchange Protocol (DLEP) [RFC8175] with its extensions [RFC8629] [RFC8757]. In short, the MANET ND mainly deals with maintaining extended network neighbors to enhance the link reliability. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes to improve the reliability, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services. For a more reliable V2V networking, some redundancy mechanisms should be provided in L3 in cases of the failure of L2. For different use cases, the optimal

solution to improve V2V networking reliability may vary. For example, a group of vehicles in platooning may have stabler neighbors than freely moving vehicles, as described in Section 3.1.

5. Problem Statement

In order to specify protocols using the architecture mentioned in Section 4.1, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a relatively short time compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles.

For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1km) and 100km/h as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is in the order of a minute (e.g., about 72 seconds), and the lifetime of a link between two vehicles is about a half minute. Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU. This relative speed leads the half of the link lifetime between the vehicle and the IP-RSU. In reality, the DSRC communication range is around 500m, so the link lifetime will be a half of the maximum time. The time constraint of a wireless link between two nodes (e.g., vehicle and IP-RSU) needs to be considered because it may affect the lifetime of a session involving the link. The lifetime of a session varies depending on the session's type such as a web surfing, voice call over IP, DNS query, and context-aware navigation (in Section 3.1). Regardless of a session's type, to guide all the IPv6 packets to their destination host(s), IP mobility should be supported for the session. In a V2V scenario (e.g., context-aware navigation), the IPv6 packets of a vehicle should be delivered to relevant vehicles in an efficient way (e.g., multicasting). With this observation, IPv6 protocol exchanges need to be done as short as possible to support the message exchanges of various applications in vehicular networks.

Therefore, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. Meanwhile, the bandwidth of the wireless link determined by the lower layers

(i.e., link and PHY layers) can affect the transmission time of control messages of the upper layers (e.g., IPv6) and the continuity of sessions in the higher layers (e.g., IPv6, TCP, and UDP). Hence the bandwidth selection according to Modulation and Coding Scheme (MCS) also affects the vehicular network connectivity. Note that usually the higher bandwidth gives the shorter communication range and the higher packet error rate at the receiving side, which may reduce the reliability of control message exchanges of the higher layers (e.g., IPv6). This section presents key topics such as neighbor discovery and mobility management for links and sessions in IPv6-based vehicular networks.

5.1. Neighbor Discovery

IPv6 ND [RFC4861][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for link types including point-to-point, multicast-capable (e.g., Ethernet) and Non-Broadcast Multiple Access (NBMA). It assumes the efficient and reliable support of multicast and unicast from the link layer for various network operations such as MAC Address Resolution (AR), DAD, MLD and Neighbor Unreachability Detection (NUD).

Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need IPv6 addresses to run IPv6 ND.

The requirements for IPv6 ND for vehicular networks are efficient DAD and NUD operations. An efficient DAD is required to reduce the overhead of DAD packets during a vehicle's travel in a road network, which can guarantee the uniqueness of a vehicle's global IPv6 address. An efficient NUD is required to reduce the overhead of the NUD packets during a vehicle's travel in a road network, which can guarantee the accurate neighborhood information of a vehicle in terms of adjacent vehicles and RSUs.

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 merging and partitioning of VANETs frequently occurs in vehicular networks. This merging and partitioning should be considered for the IPv6 ND such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. An address lookup operation may be conducted by an MA or IP-RSU (as

Registrar in RPL) to check the uniqueness of an IPv6 address that will be configured by a vehicle as DAD. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the existence of a vehicle under the network coverage of the MA or IP-RSU as NUD. Thus, SLAAC needs to prevent IPv6 address duplication due to the merging of VANETs, and IPv6 ND needs to detect unreachable neighboring vehicles due to the partitioning of a VANET. According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or a not-onlink host even though the source vehicle can use the same prefix as the destination vehicle [I-D.ietf-intarea-ippl].

To efficiently prevent IPv6 address duplication due to the VANET partitioning and merging from happening 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. In this case, two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and IP-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.

For vehicular networks with high mobility and density, DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange driving safety messages (e.g., collision avoidance and accident notification) with each other with a short interval suggested by NHTSA (National Highway Traffic Safety Administration) [NHTSA-ACAS-Report]. Since the partitioning and merging of vehicular networks may require re-perform DAD process repeatedly, the link scope of vehicles may be limited to a small area, which may delay the exchange of driving safety messages. Driving safety messages can include a vehicle's mobility information (i.e., position, speed, direction, and acceleration/deceleration) that is critical to other vehicles. The exchange interval of this message is recommended to be less than 0.5 second, which is required for a driver to avoid an emergency situation, such as a rear-end crash.

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles. The ND time-related parameters can be an operational setting or an optimization point particularly for vehicular networks.

For IPv6-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular networks, the delay-bounded data delivery is critical. IPv6 ND needs to work to support those IPv6-based safety applications efficiently.

From the interoperability point of view, in IPv6-based vehicular networking, IPv6 ND should have minimum changes with the legacy IPv6 ND used in the Internet, including DAD and NUD operations, so that IPv6-based vehicular networks can be seamlessly connected to other intelligent transportation elements (e.g., traffic signals, pedestrian wearable devices, electric scooters, and bus stops) that use the standard IPv6 network settings.

5.1.1. Link Model

A subnet model for a vehicular network needs to facilitate the communication between two vehicles with the same prefix regardless of the vehicular network topology as long as there exist bidirectional E2E paths between them in the vehicular network including VANETs and IP-RSUs. This subnet model allows vehicles with the same prefix to communicate with each other via a combination of multihop V2V and multihop V2I with VANETs and IP-RSUs.

[I-D.thubert-6man-ipv6-over-wireless] introduces other issues in an IPv6 subnet model.

IPv6 protocols work under certain assumptions that do not necessarily hold for vehicular wireless access link types [VIP-WAVE][RFC5889]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces [RFC6250]. However, radio 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 needs to consider the asymmetry of dynamically changing vehicular wireless links.

There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local, unique-local, and global types of IPv6 addresses. In an IPv6 link, it is defined that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IPv6 link. However, the vehicular link model needs to define the relationship between a link and a prefix, considering the dynamics of wireless links and the characteristics of VANET.

A VANET can have a single link between each vehicle pair 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 (or an IPv6 ULA

prefix) is assigned to VANETs in vehicular networks. Considering that two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, if they are not in one hop (that is, they have the multihop network connectivity between them), then they may not be able to communicate with each other. 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 converge to one VANET, the two vehicles can communicate with each other in a multihop fashion, for example, when they are Vehicle1 and Vehicle3, as shown in Figure 4.

From the previous observation, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model needs to use an on-link prefix and not-onlink prefix according to the network topology of vehicles such as a one-hop reachable network and a multihop reachable network (or partitioned networks). If the vehicles with the same prefix are reachable from each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable from each other in one hop due to either the multihop topology in the VANET or multiple partitions, the prefix should be not-onlink. In most cases in vehicular networks, due to the partitioning and merging of VANETs, and the multihop network topology of VANETS, not-onlink prefixes will be used for vehicles as default.

The vehicular link model needs to support multihop routing in a connected VANET where the vehicles with the same global-scope IPv6 prefix (or the same IPv6 ULA prefix) are connected in one hop or multiple hops. It also needs to support the multihop routing in multiple connected VANETs through infrastructure nodes (e.g., IP-RSU) where they are connected to the infrastructure. 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 multihop V2V or multihop V2I2V. When Vehicle1 and Vehicle3 are connected in a VANET, it will be more efficient for them to communicate with each other directly via VANET rather than indirectly via IP-RSUs. On the other hand, when Vehicle1 and Vehicle3 are far away from direct communication range in separate VANETs and under two different IP-RSUs, they can communicate with each other through the relay of IP-RSUs via V2I2V. Thus, two separate VANETs can merge into one network via IP-RSU(s). Also, newly arriving vehicles can merge two separate VANETs into one VANET if they can play the role of a relay node for those VANETs.

Thus, in IPv6-based vehicular networking, the vehicular link model should have minimum changes for interoperability with standard IPv6 links in an efficient fashion to support IPv6 DAD, MLD and NUD operations.

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. However, although such a pseudonym of a MAC address can protect to some extent the privacy of a vehicle, it may not be able to resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP and SCTP) 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 needs to be updated, and the uniqueness of the address needs to be checked through DAD procedure.

5.1.3. Routing

For multihop V2V communications in either a VANET or VANETs via IP-RSUs, a vehicular Mobile Ad Hoc Networks (MANET) routing protocol 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 [RFC9119].

A routing protocol for a VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in a VANET with a dynamic network topology because the IPv6 ND is used to check the neighborhood of each vehicle. Thus, the vehicular routing needs to take advantage of the IPv6 ND to minimize its control overhead.

RPL [RFC6550] defines a routing protocol for low-power and lossy networks, which constructs and maintains Destination-Oriented Directed Acyclic Graphs (DODAGs) optimized by an Objective Function (OF). A defined OF provides route selection and optimization within

an RPL topology. The RPL nodes use an anisotropic Distance Vector (DV) approach to form a DODAG by discovering and aggressively maintaining the upward default route toward the root of the DODAG. Downward routes follow the same DODAG, with lazy maintenance and stretched Peer-to-Peer (P2P) routing in the so-called storing mode. It is well-designed to reduce the topological knowledge and routing state that needs to be exchanged. As a result, the routing protocol overhead is minimized, which allows either highly constrained stable networks or less constrained, highly dynamic networks. Refer to Appendix B for the detailed description of RPL for multihop V2X networking.

An address registration extension for 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) in [RFC8505] can support light-weight mobility for nodes moving through different parents. [RFC8505], as opposed to [RFC4861], is stateful and proactively installs the ND cache entries, which saves broadcasts and provides a deterministic presence information for IPv6 addresses. Mainly it updates the Address Registration Option (ARO) of ND defined in [RFC6775] to include a status field that can indicate the movement of a node and optionally a Transaction ID (TID) field, i.e., a sequence number that can be used to determine the most recent location of a node. Thus, RPL can use the information provided by the Extended ARO (EARO) defined in [RFC8505] to deal with a certain level of node mobility. When a leaf node moves to the coverage of another parent node, it should de-register its addresses to the previous parent node and register itself with a new parent node along with an incremented TID.

RPL can be used in IPv6-based vehicular networks, but it is primarily designed for lossy networks, which puts energy efficiency first. For using it in IPv6-based vehicular networks, there have not been actual experiences and practical implementations for vehicular networks, though it was tested in IoT low-power and lossy networks (LLN) scenarios.

Moreover, due to bandwidth and energy constraints, RPL does not suggest to use a proactive mechanism (e.g., keepalive) to maintain accurate routing adjacencies such as Bidirectional Forwarding Detection [RFC5881] and MANET Neighborhood Discovery Protocol [RFC6130]. As a result, due to the mobility of vehicles, network fragmentation may not be detected quickly and the routing of packets between vehicles or between a vehicle and an infrastructure node may fail.

5.2. Mobility Management

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

With a GPS navigator, efficient mobility management can be performed with the help of vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having IP-RSUs and an MA in TCC). This vehicular infrastructure can predict the future positions of the vehicles from their mobility information (i.e., the current position, speed, direction, and trajectory) for 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 IP-RSUs along with mobility information.

By predicting a vehicle's mobility, the vehicular infrastructure needs to better support IP-RSUs to perform efficient SLAAC, data forwarding, 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.

For example, as shown in Figure 1, when a vehicle (e.g., Vehicle2) is moving from the coverage of an IP-RSU (e.g., IP-RSU1) into the coverage of another IP-RSU (e.g., IP-RSU2) belonging to a different subnet, the IP-RSUs can proactively support the IPv6 mobility of the vehicle, while performing the SLAAC, data forwarding, and handover for the sake of the vehicle.

For a mobility management scheme in a domain, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. If DHCPv6 is used to assign a unique IPv6 address to each vehicle in this shared link, DAD is not required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213]), DAD is not required because the IPv6 address of a vehicle's external wireless interface is guaranteed to be unique. There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support efficient mobility management.

Even though the SLAAC with classic ND costs a DAD during mobility management, the SLAAC with [RFC8505] and/or AERO/OMNI do not cost a DAD. SLAAC for vehicular networks needs to consider the minimization of the cost of DAD with the help of an infrastructure node (e.g., IP-RSU and MA). Using an infrastructure prefix over VANET allows direct routability to the Internet through the multihop V2I toward an IP-RSU. On the other hand, a BYOA does not allow such direct routability to the Internet since the BYOA is not topologically correct, that is, not routable in the Internet. In addition, a vehicle configured with a BYOA needs a tunnel home (e.g., IP-RSU) connected to the Internet, and the vehicle needs to know which neighboring vehicle is reachable inside the VANET toward the tunnel home. There is nonnegligible control overhead to set up and maintain routes to such a tunnel home [RFC4888] over the VANET.

For the case of a multihomed network, a vehicle can follow the first-hop router selection rule described in [RFC8028]. For example, an IP-OBUs inside a vehicle may connect to an IP-RSU that has multiple routers behind. In this scenario, because the IP-OBUs can have multiple prefixes from those routers, the default router selection, source address selection, and packet redirect process should follow the guidelines in [RFC8028]. That is, the vehicle should select its default router for each prefix by preferring the router that advertised the prefix.

Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275], PMIPv6 [RFC5213], and NEMO [RFC3963], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.

Therefore, for the proactive and seamless IPv6 mobility of vehicles, the vehicular infrastructure (including IP-RSUs and MA) needs to efficiently perform the mobility management of the vehicles with their mobility information and link-layer information. Also, in

IPv6-based vehicular networking, IPv6 mobility management should have minimum changes for the interoperability with the legacy IPv6 mobility management schemes such as PMIPv6, DMM, LISP, and AERO.

6. Security Considerations

This section discusses security and privacy for IPv6-based vehicular networking. Security and privacy are paramount in V2I, V2V, and V2X networking along with neighbor discovery and mobility management.

Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. For the authentication in vehicular networks, vehicular cloud needs to support a kind of Public Key Infrastructure (PKI) in an efficient way. To provide safe interaction between vehicles or between a vehicle and infrastructure, only authenticated nodes (i.e., vehicle and infrastructure node) can participate in vehicular networks. Also, in-vehicle devices (e.g., ECU) and a driver/passenger's mobile devices (e.g., smartphone and tablet PC) in a vehicle need to communicate with other in-vehicle devices and another driver/passenger's mobile devices in another vehicle, or other servers behind an IP-RSU in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles' information. In this case, an attack mitigation process may be required to reduce the aftermath of malicious behaviors. Note that when driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks.

For secure V2I communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBUE) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 2 [RFC4301][RFC4302] [RFC4303][RFC4308] [RFC7296]. Also, for secure V2V communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBUE) in a vehicle and a mobile router (i.e., IP-OBUE) in another vehicle needs to be established, as shown in Figure 3. For secure communication, an element in a vehicle (e.g., an in-vehicle device and a driver/passenger's mobile device) needs to establish a secure connection (e.g., TLS) with another element in another vehicle or another element in a vehicular cloud (e.g., a server). IEEE 1609.2 [WAVE-1609.2] specifies security services for applications and management messages, but this WAVE specification is optional. Thus, if the link layer does not support the security of a WAVE frame, either the network layer or the transport layer needs to support security services for the WAVE frames.

6.1. Security Threats in Neighbor Discovery

For the classical IPv6 ND, DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. [RFC6959] introduces threats enabled by IP source address spoofing. This possibility indicates that vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. [RFC8928] introduces a mechanism that protects the ownership of an address for 6LoWPAN ND from address theft and impersonation attacks. Based on the SEND [RFC3971] mechanism, the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based approach [Vehicular-BlockChain] can be used. However, for a scenario where a trustable router or an authentication path cannot be obtained, it is desirable to find a solution in which vehicles and infrastructures can authenticate each other without any support from a third party.

When applying the classical IPv6 ND process to VANET, one of the security issues is that an IP-RSU (or an IP-OBUE) as a router may receive deliberate or accidental DoS attacks from network scans that probe devices on a VANET. In this scenario, the IP-RSU can be overwhelmed for processing the network scan requests so that the capacity and resources of IP-RSU are exhausted, causing the failure of receiving normal ND messages from other hosts for network address resolution. [RFC6583] describes more about the operational problems in the classical IPv6 ND mechanism that can be vulnerable to deliberate or accidental DoS attacks and suggests several implementation guidelines and operational mitigation techniques for those problems. Nevertheless, for running IPv6 ND in VANET, those issues can be more acute since the movements of vehicles can be so diverse that it leaves a large room for rogue behaviors, and the failure of networking among vehicles may cause grave consequences.

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safe driving applications (e.g., context-aware navigation, cooperative adaptive cruise control, and platooning), as explained in Section 3.1, the cooperative action among vehicles is assumed. Malicious nodes may disseminate wrong driving information

(e.g., location, speed, and direction) for disturbing safe driving. For example, a Sybil attack, which tries to confuse a vehicle with multiple false identities, may disturb a vehicle from taking a safe maneuver. Since cyber security issues in vehicular networks may cause physical vehicle safety issues, it may be necessary to consider those physical security concerns when designing protocols in IPWAVE.

To identify malicious vehicles among vehicles, an authentication method may be required. A Vehicle Identification Number (VIN) and a user certificate (e.g., X.509 certificate [RFC5280]) along with an in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or its driver (having a user certificate) through a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the vehicular cloud. This authentication can be used to identify the vehicle that will communicate with an infrastructure node or another vehicle. In the case where a vehicle has an internal network (called Moving Network) and elements in the network (e.g., in-vehicle devices and a user's mobile devices), as shown in Figure 2, the elements in the network need to be authenticated individually for safe authentication. Also, Transport Layer Security (TLS) certificates [RFC8446][RFC5280] can be used for an element's authentication to allow secure E2E vehicular communications between an element in a vehicle and another element in a server in a vehicular cloud, or between an element in a vehicle and another element in another vehicle.

6.2. Security Threats in Mobility Management

For mobility management, a malicious vehicle can construct multiple virtual bogus vehicles, and register them with IP-RSUs and MA. This registration makes the IP-RSUs and MA waste their resources. The IP-RSUs and MA need to determine whether a vehicle is genuine or bogus in mobility management. Also, the confidentiality of control packets and data packets among IP-RSUs and MA, the E2E paths (e.g., tunnels) need to be protected by secure communication channels. In addition, to prevent bogus IP-RSUs and MA from interfering with the IPv6 mobility of vehicles, mutual authentication among them needs to be performed by certificates (e.g., TLS certificate).

6.3. Other Threats

For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC or 5G V2X (or LTE V2X) is required in a highway. In this case, multiple intermediate vehicles as relay nodes can help forward association and authentication messages toward an IP-RSU (gNodeB, or eNodeB) connected to an authentication server in the vehicular cloud. In this kind of process, the authentication messages forwarded by each vehicle can be delayed or lost, which may

increase the construction time of a connection or some vehicles may not be able to be authenticated.

Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles. To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.

For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, especially for a long-living transport-layer session (e.g., voice call over IP and video streaming service), a MAC address pseudonym needs to be provided to each vehicle; that is, each vehicle periodically updates its MAC address and its IPv6 address needs to be updated accordingly by the MAC address change [RFC4086][RFC8981]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality (using either IPsec or TLS), there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses. Thus, the MAC address pseudonym and the IPv6 address update should be performed with strong E2E confidentiality. Privacy concerns for excessively collecting vehicle activities from roadway operators such as public transportation administrators and private contractors may also pose threats on violating privacy rights of vehicles. It might be interesting to find a solution from a technology point of view along with public policy development for the issue.

7. IANA Considerations

This document does not require any IANA actions.

8. References

8.1. Normative References

- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999, <<https://www.rfc-editor.org/info/rfc2710>>.
- [RFC3626] Clausen, T., Ed. and P. Jacquet, Ed., "Optimized Link State Routing Protocol (OLSR)", RFC 3626, DOI 10.17487/RFC3626, October 2003, <<https://www.rfc-editor.org/info/rfc3626>>.
- [RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <<https://www.rfc-editor.org/info/rfc3753>>.
- [RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <<https://www.rfc-editor.org/info/rfc3810>>.

- [RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, DOI 10.17487/RFC3849, July 2004, <<https://www.rfc-editor.org/info/rfc3849>>.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <<https://www.rfc-editor.org/info/rfc3963>>.
- [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <<https://www.rfc-editor.org/info/rfc3971>>.
- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <<https://www.rfc-editor.org/info/rfc4086>>.
- [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <<https://www.rfc-editor.org/info/rfc4193>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <<https://www.rfc-editor.org/info/rfc4301>>.
- [RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <<https://www.rfc-editor.org/info/rfc4302>>.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <<https://www.rfc-editor.org/info/rfc4303>>.
- [RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, DOI 10.17487/RFC4308, December 2005, <<https://www.rfc-editor.org/info/rfc4308>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.

- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, DOI 10.17487/RFC4885, July 2007, <<https://www.rfc-editor.org/info/rfc4885>>.
- [RFC4888] Ng, C., Thubert, P., Watari, M., and F. Zhao, "Network Mobility Route Optimization Problem Statement", RFC 4888, DOI 10.17487/RFC4888, July 2007, <<https://www.rfc-editor.org/info/rfc4888>>.
- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <<https://www.rfc-editor.org/info/rfc5213>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <<https://www.rfc-editor.org/info/rfc5415>>.
- [RFC5614] Ogier, R. and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding", RFC 5614, DOI 10.17487/RFC5614, August 2009, <<https://www.rfc-editor.org/info/rfc5614>>.
- [RFC5881] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, DOI 10.17487/RFC5881, June 2010, <<https://www.rfc-editor.org/info/rfc5881>>.
- [RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <<https://www.rfc-editor.org/info/rfc5889>>.

- [RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, DOI 10.17487/RFC6130, April 2011, <<https://www.rfc-editor.org/info/rfc6130>>.
- [RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250, DOI 10.17487/RFC6250, May 2011, <<https://www.rfc-editor.org/info/rfc6250>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <<https://www.rfc-editor.org/info/rfc6275>>.
- [RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.
- [RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, DOI 10.17487/RFC6583, March 2012, <<https://www.rfc-editor.org/info/rfc6583>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.
- [RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <<https://www.rfc-editor.org/info/rfc7149>>.
- [RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <<https://www.rfc-editor.org/info/rfc7181>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <<https://www.rfc-editor.org/info/rfc7296>>.

- [RFC7333] Chan, H., Ed., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, DOI 10.17487/RFC7333, August 2014, <<https://www.rfc-editor.org/info/rfc7333>>.
- [RFC7429] Liu, D., Ed., Zuniga, JC., Ed., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, DOI 10.17487/RFC7429, January 2015, <<https://www.rfc-editor.org/info/rfc7429>>.
- [RFC7466] Dearlove, C. and T. Clausen, "An Optimization for the Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 7466, DOI 10.17487/RFC7466, March 2015, <<https://www.rfc-editor.org/info/rfc7466>>.
- [RFC8028] Baker, F. and B. Carpenter, "First-Hop Router Selection by Hosts in a Multi-Prefix Network", RFC 8028, DOI 10.17487/RFC8028, November 2016, <<https://www.rfc-editor.org/info/rfc8028>>.
- [RFC8175] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <<https://www.rfc-editor.org/info/rfc8175>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.
- [RFC8629] Cheng, B. and L. Berger, Ed., "Dynamic Link Exchange Protocol (DLEP) Multi-Hop Forwarding Extension", RFC 8629, DOI 10.17487/RFC8629, July 2019, <<https://www.rfc-editor.org/info/rfc8629>>.

- [RFC8691] Benamar, N., Härri, J., Lee, J., and T. Ernst, "Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11", RFC 8691, DOI 10.17487/RFC8691, December 2019, <<https://www.rfc-editor.org/info/rfc8691>>.
- [RFC8757] Cheng, B. and L. Berger, Ed., "Dynamic Link Exchange Protocol (DLEP) Latency Range Extension", RFC 8757, DOI 10.17487/RFC8757, March 2020, <<https://www.rfc-editor.org/info/rfc8757>>.
- [RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November 2020, <<https://www.rfc-editor.org/info/rfc8928>>.
- [RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <<https://www.rfc-editor.org/info/rfc8981>>.
- [RFC9119] Perkins, C., McBride, M., Stanley, D., Kumari, W., and JC. Zúñiga, "Multicast Considerations over IEEE 802 Wireless Media", RFC 9119, DOI 10.17487/RFC9119, October 2021, <<https://www.rfc-editor.org/info/rfc9119>>.

8.2. Informative References

- [RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, DOI 10.17487/RFC4821, March 2007, <<https://www.rfc-editor.org/info/rfc4821>>.
- [RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <<https://www.rfc-editor.org/info/rfc6959>>.
- [RFC8899] Fairhurst, G., Jones, T., Tüxen, M., Rüngeler, I., and T. Völker, "Packetization Layer Path MTU Discovery for Datagram Transports", RFC 8899, DOI 10.17487/RFC8899, September 2020, <<https://www.rfc-editor.org/info/rfc8899>>.

[I-D.ietf-intarea-ippl]

Nordmark, E., "IP over Intentionally Partially Partitioned Links", Work in Progress, Internet-Draft, draft-ietf-intarea-ippl-00, 30 March 2017, <<https://www.ietf.org/archive/id/draft-ietf-intarea-ippl-00.txt>>.

[I-D.ietf-lisp-rfc6830bis]

Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, "The Locator/ID Separation Protocol (LISP)", Work in Progress, Internet-Draft, draft-ietf-lisp-rfc6830bis-36, 18 November 2020, <<https://www.ietf.org/archive/id/draft-ietf-lisp-rfc6830bis-36.txt>>.

[I-D.templin-6man-aero]

Templin, F. L., "Automatic Extended Route Optimization (AERO)", Work in Progress, Internet-Draft, draft-templin-6man-aero-40, 7 March 2022, <<https://www.ietf.org/archive/id/draft-templin-6man-aero-40.txt>>.

[I-D.templin-6man-omni]

Templin, F. L., "Transmission of IP Packets over Overlay Multilink Network (OMNI) Interfaces", Work in Progress, Internet-Draft, draft-templin-6man-omni-55, 7 March 2022, <<https://www.ietf.org/archive/id/draft-templin-6man-omni-55.txt>>.

[I-D.templin-ipwave-uam-its]

Templin, F. L., "Urban Air Mobility Implications for Intelligent Transportation Systems", Work in Progress, Internet-Draft, draft-templin-ipwave-uam-its-04, 4 January 2021, <<https://www.ietf.org/archive/id/draft-templin-ipwave-uam-its-04.txt>>.

[I-D.templin-intarea-parcels]

Templin, F. L., "IP Parcels", Work in Progress, Internet-Draft, draft-templin-intarea-parcels-09, 10 February 2022, <<https://www.ietf.org/archive/id/draft-templin-intarea-parcels-09.txt>>.

- [I-D.ietf-dmm-fpc-cpdp]
Matsushima, S., Bertz, L., Liebsch, M., Gundavelli, S., Moses, D., and C. E. Perkins, "Protocol for Forwarding Policy Configuration (FPC) in DMM", Work in Progress, Internet-Draft, draft-ietf-dmm-fpc-cpdp-14, 22 September 2020, <<https://www.ietf.org/archive/id/draft-ietf-dmm-fpc-cpdp-14.txt>>.
- [I-D.thubert-6man-ipv6-over-wireless]
Thubert, P., "IPv6 Neighbor Discovery on Wireless Networks", Work in Progress, Internet-Draft, draft-thubert-6man-ipv6-over-wireless-11, 15 December 2021, <<https://www.ietf.org/archive/id/draft-thubert-6man-ipv6-over-wireless-11.txt>>.
- [DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), October 2010.
- [EU-2008-671-EC]
European Union, "Commission Decision of 5 August 2008 on the Harmonised Use of Radio Spectrum in the 5875 - 5905 MHz Frequency Band for Safety-related Applications of Intelligent Transport Systems (ITS)", EU 2008/671/EC, August 2008.
- [IEEE-802.11p]
"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Wireless Access in Vehicular Environments", IEEE Std 802.11p-2010, June 2010.
- [IEEE-802.11-OCB]
"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, December 2016.
- [WAVE-1609.0]
IEEE 1609 Working Group, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture", IEEE Std 1609.0-2013, March 2014.

[WAVE-1609.2]

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

[WAVE-1609.3]

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

[WAVE-1609.4]

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

[ISO-ITS-IPv6]

ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012.

[ISO-ITS-IPv6-AMD1]

ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking - Amendment 1", ISO 21210:2012/AMD 1:2017, September 2017.

[TS-23.285-3GPP]

3GPP, "Architecture Enhancements for V2X Services", 3GPP TS 23.285/Version 16.2.0, December 2019.

[TR-22.886-3GPP]

3GPP, "Study on Enhancement of 3GPP Support for 5G V2X Services", 3GPP TR 22.886/Version 16.2.0, December 2018.

[TS-23.287-3GPP]

3GPP, "Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services", 3GPP TS 23.287/Version 16.2.0, March 2020.

[VIP-WAVE]

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

- [Identity-Management] Wetterwald, M., Hrizi, F., and P. Cataldi, "Cross-layer Identities Management in ITS Stations", The 10th International Conference on ITS Telecommunications, November 2010.
- [SAINT] Jeong, J., Jeong, H., Lee, E., Oh, T., and D. Du, "SAINT: Self-Adaptive Interactive Navigation Tool for Cloud-Based Vehicular Traffic Optimization", IEEE Transactions on Vehicular Technology, Vol. 65, No. 6, June 2016.
- [SAINTplus] Shen, Y., Lee, J., Jeong, H., Jeong, J., Lee, E., and D. Du, "SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization", IEEE Transactions on Intelligent Transportation Systems, June 2017.
- [SANA] Hwang, T. and J. Jeong, "SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks", Springer Lecture Notes in Computer Science (LNCS), Vol. 9502, December 2015.
- [CASD] Shen, Y., Jeong, J., Oh, T., and S. Son, "CASD: A Framework of Context-Awareness Safety Driving in Vehicular Networks", International Workshop on Device Centric Cloud (DC2), March 2016.
- [CA-Cruise-Control] California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", Available: <https://path.berkeley.edu/research/connected-and-automated-vehicles/cooperative-adaptive-cruise-control>, 2022.
- [Truck-Platooning] California Partners for Advanced Transportation Technology (PATH), "Automated Truck Platooning", Available: <https://path.berkeley.edu/research/connected-and-automated-vehicles/truck-platooning>, 2022.
- [FirstNet] U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", Available: <https://www.firstnet.gov/>, 2022.
- [PSCE] European Commission, "Public Safety Communications Europe (PSCE)", Available: <https://www.psc-europe.eu/>, 2022.

[FirstNet-Report]

First Responder Network Authority, "FY 2017: ANNUAL REPORT TO CONGRESS, Advancing Public Safety Broadband Communications", FirstNet FY 2017, December 2017.

[SignalGuru]

Koukoumidis, E., Peh, L., and M. Martonosi, "SignalGuru: Leveraging Mobile Phones for Collaborative Traffic Signal Schedule Advisory", ACM MobiSys, June 2011.

[Fuel-Efficient]

van de Hoef, S., H. Johansson, K., and D. V. Dimarogonas, "Fuel-Efficient En Route Formation of Truck Platoons", IEEE Transactions on Intelligent Transportation Systems, January 2018.

[Automotive-Sensing]

Choi, J., Va, V., Gonzalez-Prelcic, N., Daniels, R., R. Bhat, C., and R. W. Heath, "Millimeter-Wave Vehicular Communication to Support Massive Automotive Sensing", IEEE Communications Magazine, December 2016.

[NHTSA-ACAS-Report]

National Highway Traffic Safety Administration (NHTSA), "Final Report of Automotive Collision Avoidance Systems (ACAS) Program", DOT HS 809 080, August 2000.

[CBDN]

Kim, J., Kim, S., Jeong, J., Kim, H., Park, J., and T. Kim, "CBDN: Cloud-Based Drone Navigation for Efficient Battery Charging in Drone Networks", IEEE Transactions on Intelligent Transportation Systems, November 2019.

[LIFS]

Wang, J., Xiong, J., Jiang, H., Jamieson, K., Chen, X., Fang, D., and C. Wang, "Low Human-Effort, Device-Free Localization with Fine-Grained Subcarrier Information", IEEE Transactions on Mobile Computing, November 2018.

[DFC]

Jeong, J., Shen, Y., Kim, S., Choe, D., Lee, K., and Y. Kim, "DFC: Device-free human counting through WiFi fine-grained subcarrier information", IET Communications, January 2021.

[In-Car-Network]

Lim, H., Volker, L., and D. Herrscher, "Challenges in a Future IP/Ethernet-based In-Car Network for Real-Time Applications", ACM/EDAC/IEEE Design Automation Conference (DAC), June 2011.

[Scrambler-Attack]

Bloessl, B., Sommer, C., Dressier, F., and D. Eckhoff,
"The Scrambler Attack: A Robust Physical Layer Attack on
Location Privacy in Vehicular Networks", IEEE 2015
International Conference on Computing, Networking and
Communications (ICNC), February 2015.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash
System", URL: <https://bitcoin.org/bitcoin.pdf>, May 2009.

[Vehicular-BlockChain]

Dorri, A., Steger, M., Kanhere, S., and R. Jurdak,
"BlockChain: A Distributed Solution to Automotive Security
and Privacy", IEEE Communications Magazine, Vol. 55, No.
12, December 2017.

Appendix A. Support of Multiple Radio Technologies for V2V

Vehicular networks may consist of multiple radio technologies such as DSRC and 5G V2X. Although a Layer-2 solution can provide support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X. Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., OMNI [I-D.templin-6man-omni] and DLEP [RFC8175]) and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard information in a highway having multiple kinds of radio technologies.

Appendix B. Support of Multihop V2X Networking

The multihop V2X networking can be supported by RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] and Overlay Multilink Network Interface (OMNI) [I-D.templin-6man-omni].

RPL defines an IPv6 routing protocol for low-power and lossy networks (LLN), mostly designed for home automation routing, building automation routing, industrial routing, and urban LLN routing. It uses a Destination-Oriented Directed Acyclic Graph (DODAG) to construct routing paths for hosts (e.g., IoT devices) in a network. The DODAG uses an objective function (OF) for route selection and optimization within the network. A user can use different routing metrics to define an OF for a specific scenario. RPL supports

multipoint-to-point, point-to-multipoint, and point-to-point traffic, and the major traffic flow is the multipoint-to-point traffic. For example, in a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). In this case, the RPL can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

RPL is primarily designed to minimize the control plane activity, which is the relative amount of routing protocol exchanges versus data traffic; this approach is beneficial for situations where the power and bandwidth are scarce (e.g., an IoT LLN where RPL is typically used today), but also in situations of high relative mobility between the nodes in the network (also known as swarming, e.g., within a variable set of vehicles with a similar global motion, or a variable set of drones flying toward the same direction).

To reduce the routing exchanges, RPL leverages a Distance Vector (DV) approach, which does not need a global knowledge of the topology, and only optimizes the routes to and from the root, allowing Peer-to-Peer (P2P) paths to be stretched. Although RPL installs its routes proactively, it only maintains them lazily, that is, in reaction to actual traffic, or as a slow background activity. Additionally, RPL leverages the concept of an objective function (called OF), which allows to adapt the activity of the routing protocol to use cases, e.g., type, speed, and quality of the radios. RPL does not need converge, and provides connectivity to most nodes most of the time. The default route toward the root is maintained aggressively and may change while a packet progresses without causing loops, so the packet will still reach the root. There are two modes for routing in RPL such as non-storing mode and storing mode. In non-storing mode, a node inside the mesh/swarm that changes its point(s) of attachment to the graph informs the root with a single unicast packet flowing along the default route, and the connectivity is restored immediately; this mode is preferable for use cases where Internet connectivity is dominant. On the other hand, in storing mode, the routing stretch is reduced, for a better P2P connectivity, while the Internet connectivity is restored more slowly, during the time for the DV operation to operate hop-by-hop. While an RPL topology can quickly scale up and down and fits the needs of mobility of vehicles, the total performance of the system will also depend on how quickly a node can form an address, join the mesh (including Authentication, Authorization, and Accounting (AAA)), and manage its global mobility to become reachable from another node outside the mesh.

OMNI defines a protocol for the transmission of IPv6 packets over Overlay Multilink Network Interfaces that are virtual interfaces governing multiple physical network interfaces. OMNI supports multihop V2V communication between vehicles in multiple forwarding hops via intermediate vehicles with OMNI links. It also supports multihop V2I communication between a vehicle and an infrastructure access point by multihop V2V communication. The OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD Messaging.

In OMNI protocol, each wireless media interface is configured with an IPv6 Unique Local Address (ULA) [RFC4193] that is assured unique within the vehicular network according to AERO/OMNI and [RFC5889]. The ULA supports both V2V and V2I multihop forwarding within the vehicular network (e.g., via a VANET routing protocol) while each vehicle can communicate with Internet correspondents using global IPv6 addresses via OMNI interface encapsulation over the wireless interface.

For the control traffic overhead for running both vehicular ND and a VANET routing protocol, the AERO/OMNI approach may avoid this issue by using MANET routing protocols only (i.e., no multicast of IPv6 ND messaging) in the wireless underlay network while applying efficient unicast IPv6 ND messaging in the OMNI overlay on an as-needed basis for router discovery and NUD. This greatly reduces the overhead for VANET-wide multicasting while providing agile accommodation for dynamic topology changes.

Appendix C. Support of Mobility Management for V2I

The seamless application communication between two vehicles or between a vehicle and an infrastructure node requires mobility management in vehicular networks. The mobility management schemes include a host-based mobility scheme, network-based mobility scheme, and software-defined networking scheme.

In the host-based mobility scheme (e.g., MIPv6), an IP-RSU plays a role of a home agent. On the other hand, in the network-based mobility scheme (e.g., PMIPv6, an MA plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, which also serves vehicles as a home agent, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213]. The host-based mobility scheme needs client functionality in IPv6 stack of a vehicle as a mobile node for mobility signaling message exchange between the vehicle and home agent. On the other hand, the network-based mobility scheme does not need such a client functionality for a vehicle because the network

infrastructure node (e.g., MAG in PMIPv6) as a proxy mobility agent handles the mobility signaling message exchange with the home agent (e.g., LMA in PMIPv6) for the sake of the vehicle.

There are a scalability issue and a route optimization issue in the network-based mobility scheme (e.g., PMIPv6) when an MA covers a large vehicular network governing many IP-RSUs. In this case, a distributed mobility scheme (e.g., DMM [RFC7429]) can mitigate the scalability issue by distributing multiple MAs in the vehicular network such that they are positioned closer to vehicles for route optimization and bottleneck mitigation in a central MA in the network-based mobility scheme. All these mobility approaches (i.e., a host-based mobility scheme, network-based mobility scheme, and distributed mobility scheme) and a hybrid approach of a combination of them need to provide an efficient mobility service to vehicles moving fast and moving along with the relatively predictable trajectories along the roadways.

In vehicular networks, the control plane can be separated from the data plane for efficient mobility management and data forwarding by using the concept of Software-Defined Networking (SDN) [RFC7149][I-D.ietf-dmm-fpc-cpdp]. Note that Forwarding Policy Configuration (FPC) in [I-D.ietf-dmm-fpc-cpdp], which is a flexible mobility management system, can manage the separation of data-plane and control-plane in DMM. In SDN, the control plane and data plane are separated for the efficient management of forwarding elements (e.g., switches and routers) where an SDN controller configures the forwarding elements in a centralized way and they perform packet forwarding according to their forwarding tables that are configured by the SDN controller. An MA as an SDN controller needs to efficiently configure and monitor its IP-RSUs and vehicles for mobility management, location management, and security services.

Appendix D. Support of MTU Diversity for IP-based Vehicular Networks

The wireless and/or wired-line links in paths between both mobile nodes and fixed network correspondents may configure a variety of Maximum Transmission Units (MTUs), where all IPv6 links are required to support a minimum MTU of 1280 octets and may support larger MTUs. Unfortunately, determining the path MTU (i.e., the minimum link MTU in the path) has proven to be inefficient and unreliable due to the uncertain nature of the loss-oriented ICMPv6 messaging service used for path MTU discovery. Recent developments have produced a more reliable path MTU determination service for TCP [RFC4821] and UDP [RFC8899] however the MTUs discovered are always limited by the most restrictive link MTU in the path (often 1500 octets or smaller).

The AERO/OMNI service addresses the MTU issue by introducing a new layer in the Internet architecture known as the "OMNI Adaptation Layer (OAL)". The OAL allows end systems that configure an OMNI interface to utilize a full 65535 octet MTU by leveraging the IPv6 fragmentation and reassembly service during encapsulation to produce fragment sizes that are assured of traversing the path without loss due to a size restriction. (This allows end systems to send packets that are often much larger than the actual path MTU.)

Performance studies over the course of many decades have proven that applications will see greater performance by sending smaller numbers of large packets (as opposed to larger numbers of small packets) even if fragmentation is needed. The OAL further supports even larger packet sizes through the IP Parcels construct [I-D.templin-intarea-parcels] which provides "packets-in-packet" encapsulation for a total size up to 4MB. Together, the OAL and IP Parcels will provide a revolutionary new capability for greater efficiency in both mobile and fixed networks.

Appendix E. Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea MSIT (Ministry of Science and ICT) (R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning).

This work was supported in part by the MSIT, Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2017-0-01633) supervised by the IITP.

This work was supported in part by the IITP (2020-0-00395, Standard Development of Blockchain based Network Management Automation Technology).

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).

This work was supported in part by the Cisco University Research Program Fund, Grant # 2019-199458 (3696), and by ANID Chile Basal Project FB0008.

Appendix F. 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 Lozano (Universidad of Murcia), Richard Roy (MIT), Francois Simon (Pilot), Sri Gundavelli (Cisco), Erik Nordmark, Dirk von Hugo (Deutsche Telekom), Pascal Thubert (Cisco), Carlos Bernardos (UC3M), Russ Housley (Vigil Security), Suresh Krishnan (Kaloomb), Nancy Cam-Winget (Cisco), Fred L. Templin (The Boeing Company), Jung-Soo Park (ETRI), Zeungil (Ben) Kim (Hyundai Motors), Kyoungjae Sun (Soongsil University), Zhiwei Yan (CNNIC), YongJoon Joe (LSware), Peter E. Yee (Akayla), and Erik Kline. 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

Sandra Cespedes -

NIC Chile Research Labs, Universidad de Chile, Av. Blanco Encalada
1975, Santiago, Chile, Phone: +56 2 29784093, EMail:
scspede@niclabs.cl

Jerome Haerri -

Communication Systems Department, EURECOM, Sophia-Antipolis, France,
Phone: +33 4 93 00 81 34, EMail: jerome.haerri@eurecom.fr

Dapeng Liu -

Alibaba, Beijing, Beijing 100022, China, Phone: +86 13911788933,
EMail: max.ldp@alibaba-inc.com

Tae (Tom) Oh -

Department of Information Sciences and Technologies, Rochester
Institute of Technology, One Lomb Memorial Drive, Rochester, NY
14623-5603, USA, Phone: +1 585 475 7642, EMail: Tom.Oh@rit.edu

Charles E. Perkins -

Futurewei Inc., 2330 Central Expressway, Santa Clara, CA 95050, USA,
Phone: +1 408 330 4586, EMail: charliep@computer.org

Alexandre Petrescu -

CEA, LIST, CEA Saclay, Gif-sur-Yvette, Ile-de-France 91190, France,
Phone: +33169089223, EMail: Alexandre.Petrescu@cea.fr

Yiwen Chris Shen -

Department of Computer Science & Engineering, Sungkyunkwan
University, 2066 Seobu-Ro, Jangan-Gu, Suwon, Gyeonggi-Do 16419,
Republic of Korea, Phone: +82 31 299 4106, Fax: +82 31 290 7996,
EMail: chrisshen@skku.edu, URI: <https://chrisshen.github.io>

Michelle Wetterwald -

FBConsulting, 21, Route de Luxembourg, Wasserbillig, Luxembourg
L-6633, Luxembourg, EMail: Michelle.Wetterwald@gmail.com

Author's Address

Jaehoon (Paul) Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: <http://iotlab.skku.edu/people-jaehoon-jeong.php>

6MAN
Internet-Draft
Intended status: Informational
Expires: November 3, 2019

P. Thubert, Ed.
Cisco Systems
May 2, 2019

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.

Table of Contents

1. Introduction	2
2. Acronyms	4
3. IP Models	6
3.1. Physical Broadcast Domain	6
3.2. MAC-Layer Broadcast Emulations	7
3.3. Mapping the IPv6 Link Abstraction	8
3.4. Mapping the IPv6 Subnet Abstraction	9
4. Wireless ND	10
4.1. Introduction to WiND	10
4.2. Links and Link-Local Addresses	11
4.3. Subnets and Global Addresses	11
5. WiND Applicability	12
5.1. Case of LPWANS	13
5.2. Case of Infrastructure BSS and ESS	13
5.3. Case of Mesh Under Technologies	14
5.4. Case of DMC radios	14
5.4.1. Using IPv6 ND only	15
5.4.2. Using Wireless ND	15
6. IANA Considerations	17
7. Security Considerations	18
8. Acknowledgments	18
9. References	18
9.1. Normative References	18
9.2. Informative References	19
Author's Address	21

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 contrasts 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 generate 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:

- o 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.

- o 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.
- o 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.

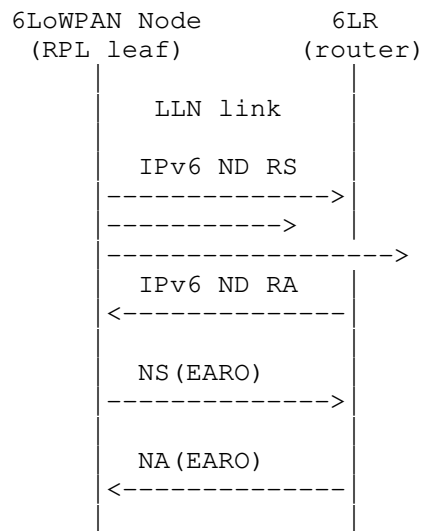


Figure 1: Initial Registration Flow

The lifetime in the registration should start with a small value ($X=R_{Min}$, TBD), and exponentially grow with each reregistration to a larger value ($X=R_{max}$, TBD). The IP Link is considered down when ($X=NbBeacons$, TBD) 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].

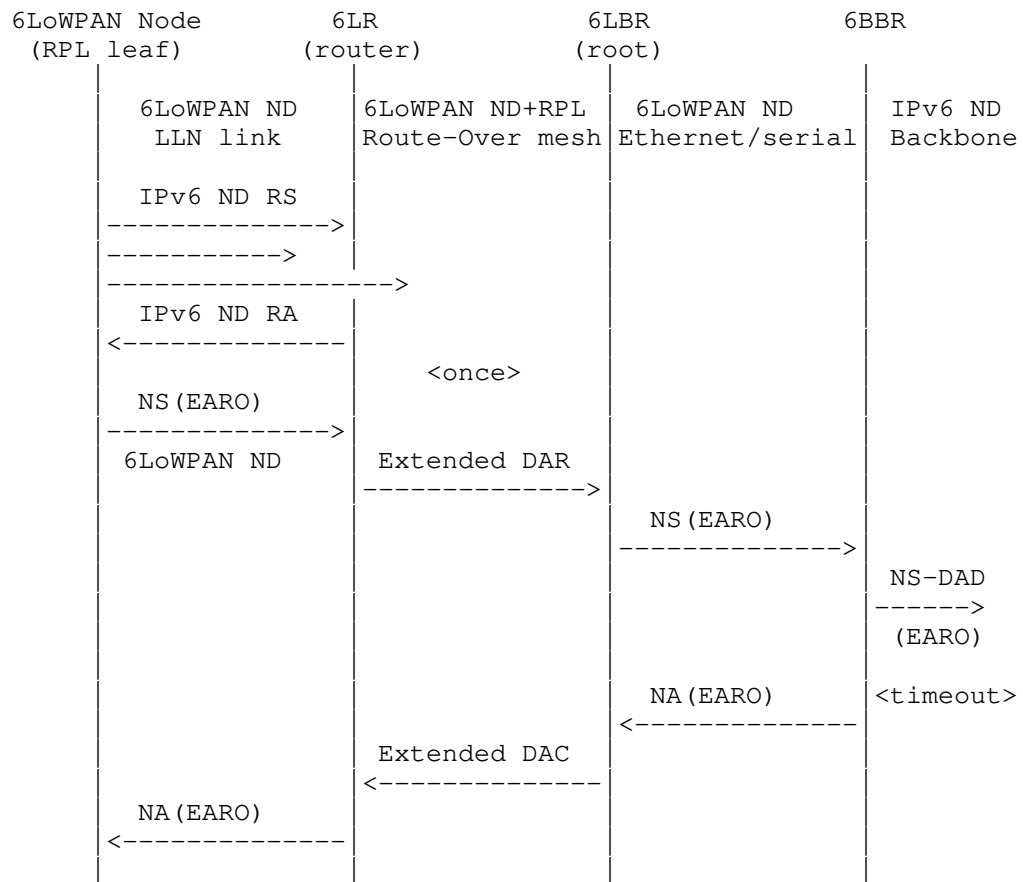


Figure 2: Initial Registration Flow over Multi-Link Subnet

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]
Thubert, P., Sarikaya, B., Sethi, M., and R. Struik,
"Address Protected Neighbor Discovery for Low-power and
Lossy Networks", draft-ietf-6lo-ap-nd-12 (work in
progress), April 2019.
- [I-D.ietf-6lo-backbone-router]
Thubert, P., Perkins, C., and E. Levy-Abegnoli, "IPv6
Backbone Router", draft-ietf-6lo-backbone-router-11 (work
in progress), February 2019.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P.
Thubert, "Network Mobility (NEMO) Basic Support Protocol",
RFC 3963, DOI 10.17487/RFC3963, January 2005,
<<https://www.rfc-editor.org/info/rfc3963>>.
- [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and
More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191,
November 2005, <<https://www.rfc-editor.org/info/rfc4191>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
"Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
DOI 10.17487/RFC4861, September 2007,
<<https://www.rfc-editor.org/info/rfc4861>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
Address Autoconfiguration", RFC 4862,
DOI 10.17487/RFC4862, September 2007,
<<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility
Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July
2011, <<https://www.rfc-editor.org/info/rfc6275>>.

- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.

9.2. Informative References

- [I-D.bi-savi-wlan]
Bi, J., Wu, J., Wang, Y., and T. Lin, "A SAVI Solution for WLAN", draft-bi-savi-wlan-16 (work in progress), November 2018.
- [I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-20 (work in progress), March 2019.
- [I-D.ietf-mboned-ieee802-mcast-problems]
Perkins, C., McBride, M., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-ietf-mboned-ieee802-mcast-problems-05 (work in progress), April 2019.
- [I-D.ietf-rift-rift]
Team, T., "RIFT: Routing in Fat Trees", draft-ietf-rift-rift-05 (work in progress), April 2019.
- [I-D.thubert-6lo-unicast-lookup]
Thubert, P. and E. Levy-Abegnoli, "IPv6 Neighbor Discovery Unicast Lookup", draft-thubert-6lo-unicast-lookup-00 (work in progress), January 2019.
- [I-D.thubert-roll-unaware-leaves]
Thubert, P., "Routing for RPL Leaves", draft-thubert-roll-unaware-leaves-07 (work in progress), April 2019.
- [I-D.vyncke-6man-mcast-not-efficient]
Vyncke, E., Thubert, P., Levy-Abegnoli, E., and A. Yourtchenko, "Why Network-Layer Multicast is Not Always Efficient At Datalink Layer", draft-vyncke-6man-mcast-not-efficient-01 (work in progress), February 2014.

- [I-D.yourtchenko-6man-dad-issues]
Yourtchenko, A. and E. Nordmark, "A survey of issues related to IPv6 Duplicate Address Detection", draft-yourtchenko-6man-dad-issues-01 (work in progress), March 2015.
- [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)".
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.
- [RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, DOI 10.17487/RFC4903, June 2007, <<https://www.rfc-editor.org/info/rfc4903>>.

- [RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.
- [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <<https://www.rfc-editor.org/info/rfc7668>>.
- [RFC8273] Brzozowski, J. and G. Van de Velde, "Unique IPv6 Prefix per Host", RFC 8273, DOI 10.17487/RFC8273, December 2017, <<https://www.rfc-editor.org/info/rfc8273>>.

Author's Address

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

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

6MAN
Internet-Draft
Intended status: Informational
Expires: 18 June 2022

P. Thubert, Ed.
Cisco Systems
15 December 2021

IPv6 Neighbor Discovery on Wireless Networks
draft-thubert-6man-ipv6-over-wireless-11

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 18 June 2022.

Copyright Notice

Copyright (c) 2021 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Terminology	4
2.1. IP Links	4
2.2. IP Subnets	5
2.3. Acronyms	6
3. ND-Classic, Wireless ND and ND-Proxies	6
4. IP Models	8
4.1. Physical Broadcast Domain	8
4.2. link-layer Broadcast Emulations	9
4.3. Mapping the IPv6 link Abstraction	11
4.4. Mapping the IPv6 subnet Abstraction	12
5. Wireless Neighbor Discovery	13
5.1. Introduction to Stateful Address Autoconfiguration	13
5.2. links and Link-Local Addresses	14
5.3. Subnets and Global Addresses	15
5.4. Anycast and Multicast Addresses	15
6. WiND Applicability	16
6.1. Case of LPWANs	17
6.2. Case of Infrastructure BSS and ESS	17
6.3. Case of Mesh Under Technologies	18
6.4. Case of DMB radios	18
6.4.1. Using ND-Classic only	19
6.4.2. Using Wireless ND	19
7. IANA Considerations	21
8. Security Considerations	22
9. Acknowledgments	22
10. Normative References	22
11. Informative References	23
Author's Address	26

1. Introduction

IEEE Std. 802.1 [IEEE Std. 802.1] 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 Wireless Local Area Networks (WLANs) generally do not benefit from the same reliable and cheap broadcast capabilities as Ethernet links.

As opposed to unicast transmissions, the broadcast transmissions over wireless links are not subject to automatic retries (ARQ) and can be very unreliable. Reducing the speed at the physical (PHY) layer for broadcast transmissions can increase the reliability, at the expense of a higher relative cost of broadcast on the overall available bandwidth. As a result, protocols designed for bridged networks that

rely on broadcast transmissions often exhibit disappointing behaviours when employed unmodified on a local wireless medium (see [MCAST PROBLEMS]).

Like Transparent Bridging, the IPv6 [RFC8200] Neighbor Discovery [RFC4861] [RFC4862] Protocol (ND-Classic) is reactive, and relies on on-demand Network Layer multicast to locate an on-link correspondent (Address Resolution, AR) and ensure the uniqueness of an IPv6 address (Duplicate Address Detection, aka DAD) in the case of Stateless Address Autoconfiguration (SLAAC). On Ethernet LANs and most WLANs and Low-Power Personal Area Networks (LoWPANs), the Network Layer multicast operation is typically implemented as a link-layer broadcast for the lack of an adapted and scalable link-layer multicast operation.

It results that on wireless, an ND-Classic multicast message is typically broadcasted. So even though there are very few nodes subscribed to the Network Layer multicast group, and there is at most one intended Target, the broadcast is received by many wireless nodes over the whole subnet (e.g., the ESS fabric). And yet, the broadcast transmission being unreliable, the intended Target may effectively have missed the packet.

On paper, a Wi-Fi station must keep its radio turned on to listen to the periodic series of broadcast frames, which for the most part will be dropped when they reach Network Layer. In order to avoid this waste of energy and increase its battery life, a typical battery-operated device such as an IoT sensor or a smartphone will blindly ignore a ratio of the broadcasts, making ND-Classic operations even less reliable.

Wi-Fi [IEEE Std. 802.11] Access Points (APs) deployed in an Extended Service Set (ESS) act as [IEEE Std. 802.1] bridges between the wireless stations (STA) and the wired backbone. As opposed to the classical Transparent (aka Learning) Bridge operation that installs the forwarding state reactively to traffic, the bridging state in the AP is established proactively, at the time of association. This protects the wireless medium against broadcast-intensive Transparent Bridging lookups. The association process registers the link-layer (MAC) Address (LLA) of the STA to the AP proactively, i.e., before it is needed. The AP maintains the list of the associated addresses and blocks the lookups for destinations that are not registered. This solves the broadcast issue for the link-layer lookups, but the Network Layer problem remains.

Though ND-Classic was the state of the art when designed for an Ethernet wire at the end of the twentieth century, it must be reevaluated for the new technologies, such as wireless and overlays,

that evolved since then. This document discusses the applicability of ND-Classic over wireless links, as compared with routing-based alternatives such as prefix-per node and multi-link subnets (MLSN), and with Wireless ND (WiND), that is similar to the Wi-Fi association and reduces the need for Network Layer multicast.

2. Terminology

2.1. IP Links

For a long time, the term link has been used to refer to the layer 2 communication medium that can be leveraged at layer 3 to instantiate one IP hop. In this document we conserve that term but differentiate it from an IP link, which is a layer 3 abstraction that represents the layer 2 link but is not the layer 2 link, like the map is not the country.

With IPv6, IP has moved to layer 3 abstractions for its operations, e.g., with the use of link local address (LLA), and that of IP multicast for link-scoped operations. At the same time, the concept of an IP link emerged as an abstraction that represents how IP layer considers the layer 2 link:

- * An IP link connects an IP node to one or more other IP nodes using a lower layer subnetwork. The lower layer subnetwork may comprise multiple lower layer links, e.g., in the case of a switched fabric or a mesh-under LLN.
- * an IP link defines the scope of an LLA, and defines the domain in which the LLA must be unique
- * an IP link provides a subset of the connectivity that is offered by the lower layer; if the IP link is narrower than the layer 2 reachable domain, then layer 3 filters must restrict the link-scoped communication to remain between peers on a same IP link, and more than one IP link may be installed on the same physical interface to connect to different peers.
- * an IP link can be Point to Point (P2P), Point to Point (P2MP, forming a partial mesh), NBMA (non-broadcast multi-access, fully meshed), or transit (broadcast-capable and any-to-any).

It is a network design decision to use one IP link model or another over a given lower layer network, e.g., to map a Frame Relay network as a P2MP IP link, or as a collection of P2P IP links. As another example, an Ethernet fabric may be bridged, in which case the nodes that interconnect the layer 2 links are L2 switches, and the fabric can be abstracted as a single transit IP link; or the fabric can be routed, in which case the P2P IP links are congruent with the layer 2 links, and the nodes that interconnect the links are routers.

2.2. IP Subnets

IPv6 builds another abstraction, the IP subnet, over one shared IP link or over a collection IP links, forming a MLSN in the latter case. An MLSN is formed over IP links (e.g., P2P or P2MP) that are interconnected by routers that either inject hosts routes in an IGP, in which case the topology can be anything, or perform ND proxy operations, in which case the structure of links must be strictly hierarchical to avoid loops.

[RFC8929] defines bridging and routing IPv6 ND proxies. Both forms of ND proxies interconnect IP links and enable to isolate the layer 2 broadcast domains. But in the case of a bridging proxy, the layer 2 unicast communication can still exist between the layer 2 domains that are covered by the layer 3 links, whereas in the base of a routing proxy, they are isolated and packets must be routed back and forth. Bridging proxies are possible between compatible technologies and translational bridges (e.g., Wi-Fi to Ethernet), whereas routing proxies are required between non-bridgeable technologies and desirable to avoid exposing the layer 2 addresses across, e.g., for reasons of stability and scalability.

It is another network design decision to use one IP subnet model or another over a given lower layer network. A switched fabric can host one or more IP subnets, in which case the IP links can reach all and beyond one subnet. On the other hand, a subnet can encompass a collection of links; in that case, the scope of the link local addresses, which is the IP Link, is narrower than the span of the subnet.

A subnet prefix is associated with the IP subnet, and a node is a member of an IP subnet when it has an IP address that derives from that prefix. The IP address is either a Unique Local (ULA) or a Global Unicast Address (GUA), and as opposed to the case of LLAs, the scope of the address is not limited to the IP subnet.

The switched and routed fabric above could be the exact same network of physical links and boxes, what changes is the way the networking abstractions are mapped onto the system, and the implication of such decision include the capability to reach another node at layer-2, and the size of the broadcast domain and related broadcast storms.

2.3. Acronyms

This document uses the following abbreviations:

6BBR: 6LoWPAN Backbone 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
LoWPAN: Low-Power Wireless Personal Area 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
VLAN: Virtual Local Area Network
WiND: Wireless Neighbor Discovery
WLAN: Wireless Local Area Network
WPAN: Wireless Personal Area Network

3. ND-Classic, Wireless ND and ND-Proxies

The ND-Classic Neighbor Solicitation (NS) [RFC4861] message is used as a multicast IP packet for Address Resolution (AR) and Duplicate Address Detection (DAD) [RFC4862]. In those cases, the NS message is sent at the Network Layer to a Solicited-Node Multicast Address (SNMA) [RFC4291] and should in theory only reach a very small group of nodes. It is intended for one Target, that may or may not be present in the network, but it is often turned into a MAC-Layer broadcast and effectively reaches most of the nodes that are attached to the layer 2 link.

DAD was designed for the efficient broadcast operation of Ethernet. Experiments show that DAD often fails to discover the duplication of IPv6 addresses in large wireless access networks [DAD ISSUES]. In practice, IPv6 addresses very rarely conflict, not because the address duplications are detected and resolved by the DAD operation, but thanks to the entropy of the 64-bit Interface IDs (IIDs) that makes a collision quasi-impossible for randomized IIDs.

Multicast NS transmissions may occur when a node joins the network, moves, or wakes up and reconnects to the network. Over a very large fabric, this can generate hundreds of broadcasts per second. If the broadcasts were blindly copied over Wi-Fi, the MAC-layer broadcast traffic associated to ND IP-layer multicast could consume enough bandwidth to cause a substantial degradation to the unicast service [MCAST EFFICIENCY]. To protect their bandwidth, some networks throttle ND-related broadcasts, which reduces the capability for the ND protocol to operate as expected.

This problem can be alleviated by reducing the size of the broadcast domain that encompasses wireless access links. This has been done in the art of IP subnetting by partitioning the subnets and by routing between them, at the extreme by assigning a /64 prefix to each wireless node (see [RFC8273]).

Another way to split the broadcast domain within a subnet is to proxy at the boundary of the wired and wireless domains the Network Layer protocols that rely on link-layer broadcast operations. [IEEE Std. 802.11] recommends to deploy proxies for the IPv4 Address Resolution Protocol (ARP) and IPv6 ND at the APs. This requires the exhaustive list of the IP addresses for which proxying is provided. Forming and maintaining that knowledge a hard problem in the general case of radio connectivity, which keeps changing with movements and variations in the environment that alter the range of transmissions.

[SAVI] suggests to discover the addresses by snooping the ND-Classic protocol, but that can also be unreliable. An IPv6 address may not be discovered immediately due to a packet loss. It may never be discovered in the case of a "silent" node that is not currently using one of its addresses, e.g., a printer that waits in wake-on-lan state. A change of anchor, e.g. due to a movement, may be missed or misordered, leading to unreliable connectivity and an incomplete list of addresses.

Wireless ND (WiND) introduces a new approach to IPv6 Neighbor Discovery that is designed to apply to the WLANs and LoWPANs types of networks, as well as other Non-Broadcast Multi-Access (NBMA) networks such as Data-Center overlays. WiND applies routing inside the subnets, which enables to form potentially large MLSNs without

creating a large broadcast domain at the link-layer. In a fashion similar to a Wi-Fi Association, IPv6 Hosts register their addresses to their serving router(s), using [RFC8505]. With the registration, the 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 service, and it can be protected to prevent impersonation attacks with [RFC8928].

The routing service can be a simple reflexion in a Hub-and-Spoke subnet that emulates an IEEE Std. 802.11 Infrastructure BSS at the Network Layer. It can also be a full-fledge routing protocol, in particular RPL [RFC6550], which is designed to adapt to various LLNs such as WLAN and WPAN radio meshes. Finally, the routing service can also be an ND proxy that emulates an IEEE Std. 802.11 Infrastructure ESS at the Network Layer, as specified in the IPv6 Backbone Router [RFC8929].

On the one hand, WiND avoids the use of broadcast operation for DAD and AR, and on the other hand, WiND supports use cases where subnet and link-layer domains are not congruent, which is common in wireless networks unless a specific link-layer emulation is provided. More details on WiND can be found in Section 5.1.

4. IP Models

4.1. Physical Broadcast Domain

At the physical (PHY) Layer, a broadcast domain is the set of nodes that may receive a transmission that one sends over an interface, in other words the set of nodes in range of the radio transmission. This set can comprise a single peer on a serial cable used as point-to-point link. It may also comprise multiple peer nodes on a broadcast radio or a shared physical resource such as the Ethernet wires and hubs for which ND-Classic was initially designed.

On WLAN and LoWPAN radios, the physical broadcast domain is defined relative to a particular transmitter, as the set of nodes that can receive what this transmitter is sending. Literally every frame defines its own broadcast domain since the chances of reception of a given frame 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 two nodes if the physical broadcast domains of their unicast transmissions overlap. On WLAN and LoWPAN radios, that relation is usually not reflexive, since nodes disable the reception when they transmit; still they may

retain a copy of the transmitted frame, so it can be seen as reflexive at the MAC Layer. It is often symmetric, meaning that if B can receive a frame from A, then A can receive a frame 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 uni-directional, 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 that specific situation can not be assumed in the general case. In other words, the relation of radio connectivity is generally not transitive, meaning that A in range with B and B in range with C does not necessarily imply that A is in range with C.

4.2. link-layer Broadcast Emulations

We call Direct MAC Broadcast (DMB) the transmission mode where the broadcast domain that is usable at the MAC layer is directly the physical broadcast domain. IEEE Std. 802.15.4 [IEEE Std. 802.15.4] and IEEE Std. 802.11 [IEEE Std. 802.11] OCB (for Out of the Context of a BSS) are examples of DMB radios. DMB networks provide mostly symmetric and non-transitive transmission. This contrasts with a number of link-layer Broadcast Emulation (LLBE) schemes that are described in this section.

In the case of Ethernet, while a physical broadcast domain is constrained to a single shared wire, the IEEE Std. 802.1 [IEEE Std. 802.1] bridging function 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 transitive 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 Map Resolver. 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 to do so.

An IEEE Std. 802.11 [IEEE Std. 802.11] Infrastructure Basic Service Set (BSS) also provides a transitive closure of nodes as defined by the broadcast domain of a central AP. The AP relays both unicast and broadcast packets and provides the symmetric and transitive emulation of a shared wire between the associated nodes, with the capability to

signal link-up/link-down to the upper layer. Within a 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 increase the chances 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 the longest occupancy of the medium, for a duration that can be a hundred times that of the unicast transmission of a frame of the same size.

For that reason, upper layer protocols should tend to avoid the use of broadcast when operating over Wi-Fi. To cope with this problems, APs may implement strategies such as turn a broadcast into a series of unicast transmissions, or drop the message altogether, which may impact the upper layer protocols. For instance, some APs may not copy Router Solicitation (RS) messages under the assumption that there is no router across the wireless interface. This assumption may be correct at some point of time and may become incorrect in the future. Another strategy used in Wi-Fi APS is to proxy protocols that heavily rely on broadcast, such as the Address Resolution in ARP and ND-Classic, and either respond on behalf or preferably forward the broadcast frame as a unicast to the intended Target.

In an IEEE Std. 802.11 [IEEE Std. 802.11] Infrastructure Extended Service Set (ESS), infrastructure BSSes are interconnected by a bridged network, typically running Transparent Bridging and the Spanning tree Protocol or a more advanced Layer 2 Routing (L2R) scheme. In the original model of learning bridges, the forwarding state 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 on the reverse path. This is a reactive operation, meaning that the state is populated reactively to the need to reach a destination. It is also possible in the original model to broadcast a gratuitous frame to advertise self throughout the bridged network, and that is also a broadcast.

The process of the Wi-Fi association prepares a bridging state proactively at the AP, which avoids the need for a reactive broadcast lookup over the wireless access. In an ESS, the AP may also generate a gratuitous broadcast sourced at the MAC address of the STA to prepare or update the state in the learning bridges so they point towards the AP for the MAC address of the STA. WiND emulates that proactive method at the Network Layer for the operations of AR, DAD and ND proxy.

In some instances of WLANs and LoWPANs, a Mesh-Under technology (e.g., a IEEE Std. 802.11s or IEEE Std. 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 the link-layer. When operating on a single frequency, this operation is known to interfere with itself, and requires inter-frame gaps to dampen the collisions, which reduces further the amount of available bandwidth.

As the cost of broadcast transmissions becomes increasingly expensive, there is a push to rethink the upper Layer protocols to reduce the dependency on broadcast operations.

4.3. Mapping the IPv6 link Abstraction

As introduced in Section 2.1, 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 ND-Classic [RFC4861] DAD [RFC4862] process uses a multicast transmission to detect a duplicate address, which requires that the owner of the address is connected to the link-layer broadcast domain of the sender.

On a wired medium, the IP 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 with a link-layer broadcast domain that emulates a physical broadcast domain over the mesh of wires. But the difference shows on legacy P2MP and NBMA networks 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 link-layer 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 link-layer broadcast domain. Relying on Multicast for the ND operation remains feasible but becomes highly detrimental to the unicast traffic, and becomes less and less energy-efficient and reliable as the network grows.

On DMB 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 over the broadcast domain defined by one radio transmitter if that transmitter keeps meeting new peers on the go.

The scope on which the uniqueness of an LLA must be checked is each new pair of nodes for the duration of their conversation. As long as there's no conflict, a node may use the same LLA with multiple peers

but it has to perform DAD again with each new peer. A node may need to form a new LLA to talk to a new peer, and multiple LLAs may be present in the same radio interface to talk to different peers. In practice, each pair of nodes defines a temporary P2P link, which can be modeled as a sub-interface of the radio interface.

The DAD and AR procedures in ND-Classic expect 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 applicable for P2P and transit links, but requires extensions for more complex topologies.

4.4. Mapping the IPv6 subnet Abstraction

As introduced in Section 2.2, IPv6 also defines the concept of a subnet for Global and Unique Local Addresses (GLA and ULA). All the addresses in a subnet share the same prefix, and by extension, a node belongs to a subnet if it has an address that derives from the prefix of the subnet. That address must be topologically correct, meaning that it must be installed on an interface that is connected to the subnet.

Unless intently replicated in different locations for very specific purposes, a subnet prefix is unique within a routing system; for ULAs, the routing system is typically a limited domain, whereas for GLAs, it is the whole Internet.

For that reason, it is sufficient to validate that an address that is formed from a subnet prefix is unique within the scope of that subnet to guarantee that it is globally unique within the whole routing system. Note that a subnet may become partitioned due to the loss of a wired or wireless link, so even that operation is not necessarily obvious, more in [DAD APPROACHES].

The IPv6 aggregation model 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 link-layer address and deliver the packet, or, in the case of an MLSN, route the packet to the destination within the subnet.

If the subnet is known as on-link, then any node may also resolve the destination link-layer address and deliver the packet, but if the subnet is not on-link, then a host in the subnet that does not have a Neighbor Cache Entry (NCE) for the destination will also need to pass the packet to a router, more in [RFC5942].

On Ethernet, an IP subnet is often congruent with an IP link because both are determined by the physical attachment to a shared wire or an IEEE Std. 802.1 bridged domain. In that case, the connectivity over the IP link is both symmetric and transitive, the subnet can appear as on-link, and any node can resolve a destination MAC address of any other node directly using ND-Classic.

But an IP link and an IP subnet are not always congruent. In the case of a Shared Link, individual subnets may each encompass only a subset of the nodes connected to the link. Conversely, in Route-Over Multi-link subnets (MLSN) [RFC4903], routers federate the links between nodes that belong to the subnet, the subnet is not on-link and it extends beyond any of the federated links.

5. Wireless Neighbor Discovery

5.1. Introduction to Stateful Address Autoconfiguration

Stateful Address Autoconfiguration (SFAAC) [RFC6775][RFC8505][RFC8929][RFC8928] defines a new operation for ND 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 ND to avoid the expectations of transit links and subnet-wide broadcast domains.

SFAAC is agnostic to the method used for Address Assignment, e.g., Manual, Semantically Opaque Autoconfiguration [RFC7217], randomized [RFC8981], or DHCPv6 [RFC8415]. It does not change the IPv6 addressing [RFC4291] or the current practices of assigning prefixes, typically a /64, to a subnet. But the DAD operation is performed as a unicast exchange with a central registrar, using new ND Extended Duplicate Address messages (EDAR and EDAC) [RFC6775][RFC8505]. This modernizes ND for application in overlays with Map Resolvers and enables unicast lookups [UNICAST AR] for addresses registered to the resolver.

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 Address Resolution in ND-Classic and the associated link-layer broadcasts transmissions.

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 Hub-and-Spoke model where only one router owns and advertises the prefix. [RFC8505] is already referenced as the registration interface to "RIFT: Routing in Fat Trees" [I-D.ietf-rift-rift] and "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" [RFC6550] with [RPL UNAWARE LEAVES].

Wireless ND (WiND) combines SFAAC with the not-onlink model on the wireless interfaces, and a Backbone Router (6BBR) ND proxy function (more in [RFC8929]) operating as a Layer-3 AP. Multiple 6BBRs placed along the wireless edge of a Backbone link handle IPv6 Neighbor Discovery and forward packets over the backbone on behalf of the registered nodes on the wireless edge. This enables to span a subnet over an MLSN that federates edge wireless links with a high-speed, typically Ethernet, backbone (as a Layer-3 ESS). The ND proxy maintains the reachability for Global Unicast and Link-Local Addresses within the federated MLSN, either as a routing proxy where it replies with its own MAC address or as a bridging proxy that typically forwards the multicast ND messages as unicast Layer-2 frames to their target. The wireless nodes can form any address they want and move freely from a wireless edge link to another, without renumbering.

5.2. links and Link-Local Addresses

For Link-Local Addresses, DAD is typically performed between communicating pairs of nodes and an NCE can be populated with a single unicast exchange. In the case of a bridging proxies, though, the Link-Local traffic is bridged over the backbone and the DAD must proxied there as well.

For instance, in the case of Bluetooth Low Energy (BLE) [RFC7668][IEEEstd802151], the uniqueness of Link-Local Addresses needs only to be verified between the pair of communicating nodes, the central router and the peripheral host. In that example, 2 peripheral hosts connected to the same central router can not have the same Link-Local Address because the addresses would collision at the central router which could not talk to both over the same interface. The DAD operation from SFAAC is appropriate for that use case, but the one from ND is not, because the peripheral hosts are not on the same broadcast domain.

On the other hand, the uniqueness of Global and Unique-Local Addresses is validated at the subnet Level, using a logical registrar that is global to the subnet.

5.3. Subnets and Global Addresses

SFAAC extends ND-Classic 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 a router, the Hub advertises the prefix as not-on-link to the spokes in RA messages Prefix Information Options (PIO). Acting as hosts, the Spokes autoconfigure addresses from that prefix and register them to the Hub with a corresponding lifetime.

Acting as a registrar, 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.

The Hub also maintains an NCE for the registered addresses and can deliver a packet to any of them during their respective lifetimes. It can be observed that this design builds a form of Network Layer 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 registrar 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 [RPL UNAWARE LEAVES]. In a degraded mode, all the Hubs are connected to a same high speed backbone such as an Ethernet bridging domain where ND-Classic is operated. In that case, it is possible to federate the Hub, Spoke and Backbone nodes as a single subnet, operating ND proxy operations [RFC8929] at the Hubs, acting as 6BBRs. It can be observed that this latter design builds a form of Network Layer Infrastructure ESS.

5.4. Anycast and Multicast Addresses

While IPv6 ND is defined for unicast addresses only, [I-D.ietf-6lo-multicast-registration] extends [RFC8505] for anycast and multicast IPv6 addresses.

[I-D.ietf-6lo-multicast-registration] can be used as a replacement for MLDv2 [RFC3810] for use cases where broadcast are not desirable, and when a device push model such as SFAAC is preferred over a network pull such as MDv2 and classical ND. With [RFC8505], the host does not need to define SNMAs for its unicast addresses and does not perform the associated MLDv2 operation. With [I-D.ietf-6lo-multicast-registration], MLDv2 and its extensive use of broadcast can be totally eliminated.

In the case of anycast, the signal enables the 6BBRs to accept more than one registration for the same address, and collectively elect the registering host receives a packet for a given anycast address.

6. WiND Applicability

WiND applies equally to P2P links, P2MP Hub-and-Spoke, link-layer Broadcast Domain Emulation such as Mesh-Under and Wi-Fi BSS, and Route-Over meshes.

There is an intersection where The IP link and the IP 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 more details in the introduction of [RFC8929].

There are also a number of practical use cases in the wireless world where links and subnets are not congruent:

- * The IEEE Std. 802.11 infrastructure BSS enables one subnet per AP, and emulates a broadcast domain at the link-layer. The Infrastructure ESS extends that model over a backbone and recommends the use of an ND proxy [IEEE Std. 802.11] to interoperate with Ethernet-connected nodes. WiND incorporates an ND proxy to serve that need, which was missing so far.
- * Bluetooth is Hub-and-Spoke at the link-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, and each peripheral host (acting as a host) 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

an IEEE Std. 802.15.4 Time-Slotted Channel-Hopping (TSCH) [IEEEstd802154] 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 waste of resources 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.

6.1. 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.

6.2. 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.

Snooping protocols such as ND-Classic and DHCPv6 and observing data traffic sourced at the STA provides an imperfect knowledge of the state of the STA at the AP. Missing a state or a transition may result in the loss of connectivity for some of the addresses, in particular for an address that is rarely used, belongs to a sleeping node, or one in a situation of mobility. This may also result in undesirable remanent state in the AP when the STA ceases to use an IPv6 address while remaining associated. It results that snooping protocols is not a recommended technique and that it should only be used as last resort, when the WiND registration is not available to populate the state.

The recommended alternative method is to use the WiND Registration for IPv6 Addresses. This way, 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 all of its IPv6 addresses, using the Extended Address Registration Option, which provides the following elements:

- * The registration state has a lifetime that limits unwanted state remanence in the network.
- * The registration is optionally secured using [RFC8928] to prevent address theft and impersonation.
- * The registration carries a sequence number, which enables to figure the order of events in a fast mobility scenario without 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 WiND proxy ND specification that associated to the Address Registration is [RFC8929]. 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 backbone router either replies to NS lookups with the MAC address of the STA, or preferably forwards the lookups to the STA as link-layer unicast frames to let the STA answer. For the data plane, the backbone router acts as a normal AP and bridges the packets to the STA as usual. As a routing proxy, the backbone router 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.

6.3. Case of Mesh Under Technologies

The Mesh-Under provides a broadcast domain emulation with symmetric 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 as an Access Point does in a BSS/ESS.

While it is still possible to operate ND-Classic, the inefficiencies of the flooding operation make the associated operations even less desirable than in a BSS, and the use of WiND is highly recommended.

6.4. Case of DMB radios

IPv6 over DMB radios uses P2P links that can be formed and maintained when a pair of DMB radios transmitters are in range from one another.

6.4.1. Using ND-Classic only

DMB radios do not provide MAC level broadcast emulation. An example of that is IEEE Std. 802.11 OCB which uses IEEE Std. 802.11 MAC/PHYs but does not provide the BSS functions.

It is possible to form P2P IP links between each individual pairs of nodes and operate ND-Classic 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 ND-Classic.

If an external mechanism avoids duplicate addresses and if the deployment ensures the connectivity between peers, a non-transit Hub-and-Spoke deployment is also possible where the Hub is the only router in the subnet and the Prefix is advertised as not on-link.

6.4.2. Using Wireless ND

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

The routers send RAs with a SLLAO at a regular period. The period can be indicated in the 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 messages. The RA is sent over an unspecified IP link where it does not conflict to anyone, so DAD is not necessary at that stage.

The host instantiates an IP link where the router's address is not a duplicate. To achieve this, it forms an LLA that does not conflict with that of the router and registers to the router using [RFC8505]. If the router sent an RA(PIO), the host can also autoconfigure an address from the advertised prefix and register it.

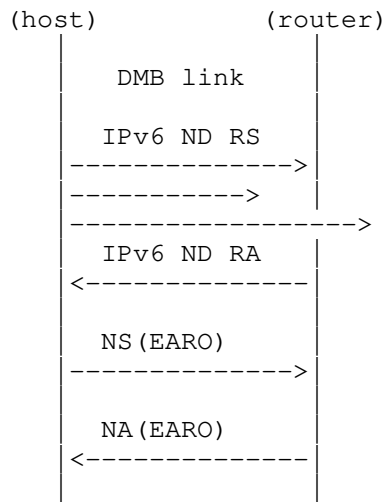


Figure 1: Initial Registration Flow

The lifetime in the registration should start with a small value ($X=R_{min}$, TBD), and exponentially grow with each re-registration to a larger value ($X=R_{max}$, TBD). The IP link is considered down when ($X=NbBeacons$, TBD) expected messages are not received in a row. It must be noted that the physical link flapping does not affect the state of the registration and when a physical link comes back up, the active registrations (i.e., registrations for which lifetime is not elapsed) are still usable. Packets should be held or destroyed when the IP link is down.

P2P links may be federated in Hub-and-Spoke and then in Route-Over MLSNs as illustrated in Figure 2. 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].

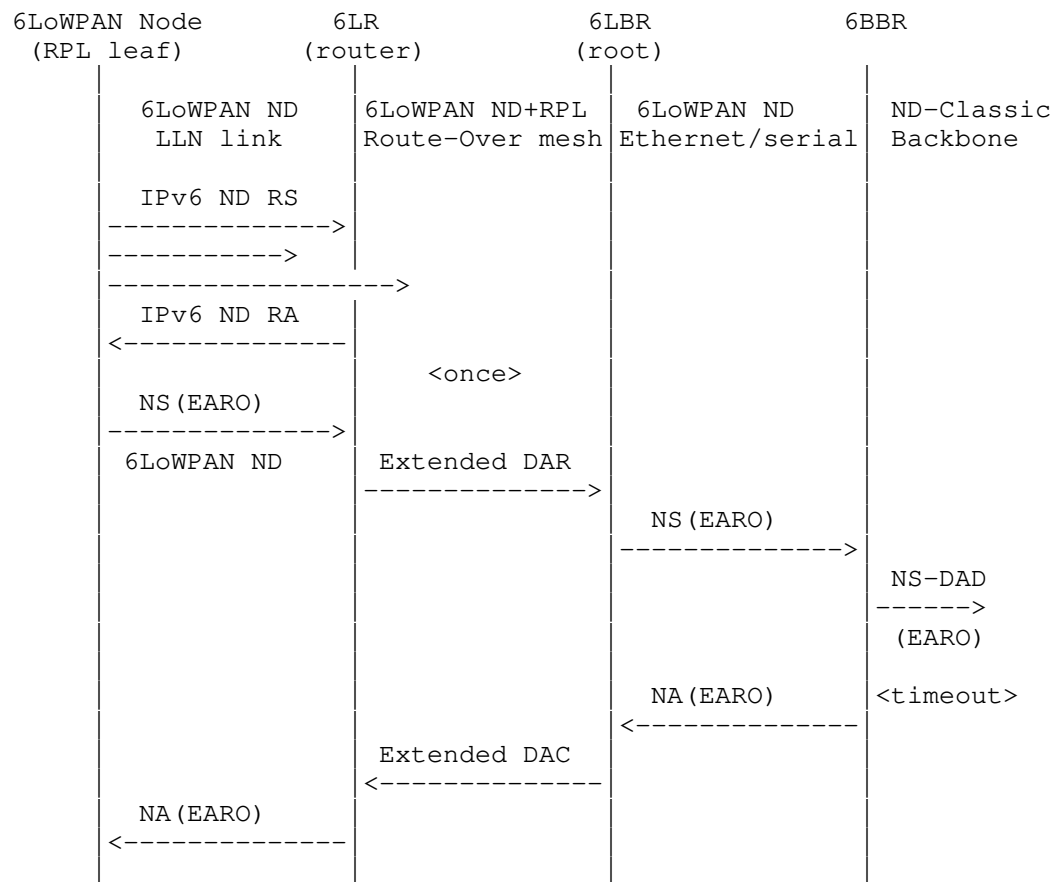


Figure 2: Initial Registration Flow over Multi-link subnet

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.

7. IANA Considerations

This specification does not require IANA action.

8. Security Considerations

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

9. Acknowledgments

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

10. Normative References

- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <<https://www.rfc-editor.org/info/rfc3963>>.
- [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <<https://www.rfc-editor.org/info/rfc4191>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC5942] Singh, H., Beebe, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, DOI 10.17487/RFC5942, July 2010, <<https://www.rfc-editor.org/info/rfc5942>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <<https://www.rfc-editor.org/info/rfc6275>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.

- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.
- [RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November 2020, <<https://www.rfc-editor.org/info/rfc8928>>.
- [RFC8929] Thubert, P., Ed., Perkins, C.E., and E. Levy-Abegnoli, "IPv6 Backbone Router", RFC 8929, DOI 10.17487/RFC8929, November 2020, <<https://www.rfc-editor.org/info/rfc8929>>.

11. Informative References

- [RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <<https://www.rfc-editor.org/info/rfc3810>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.
- [RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, DOI 10.17487/RFC4903, June 2007, <<https://www.rfc-editor.org/info/rfc4903>>.
- [RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.
- [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <<https://www.rfc-editor.org/info/rfc7668>>.

- [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <<https://www.rfc-editor.org/info/rfc7217>>.
- [RFC8273] Brzozowski, J. and G. Van de Velde, "Unique IPv6 Prefix per Host", RFC 8273, DOI 10.17487/RFC8273, December 2017, <<https://www.rfc-editor.org/info/rfc8273>>.
- [RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <<https://www.rfc-editor.org/info/rfc8415>>.
- [RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <<https://www.rfc-editor.org/info/rfc8981>>.
- [I-D.ietf-rift-rift]
Sharma, A., Thubert, P., Rijsman, B., and D. Afanasiev, "RIFT: Routing in Fat Trees", Work in Progress, Internet-Draft, draft-ietf-rift-rift-13, 12 July 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-rift-rift-13>>.
- [RPL UNAWARE LEAVES]
Thubert, P. and M. C. Richardson, "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves", Work in Progress, Internet-Draft, draft-ietf-roll-unaware-leaves-30, 22 January 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-roll-unaware-leaves-30>>.
- [DAD ISSUES]
Yourtchenko, A. and E. Nordmark, "A survey of issues related to IPv6 Duplicate Address Detection", Work in Progress, Internet-Draft, draft-yourtchenko-6man-dad-issues-01, 3 March 2015, <<https://datatracker.ietf.org/doc/html/draft-yourtchenko-6man-dad-issues-01>>.
- [MCAST EFFICIENCY]
Vyncke, E., Thubert, P., Levy-Abegnoli, E., and A. Yourtchenko, "Why Network-Layer Multicast is Not Always

Efficient At Datalink Layer", Work in Progress, Internet-Draft, draft-vyncke-6man-mcast-not-efficient-01, 14 February 2014, <<https://datatracker.ietf.org/doc/html/draft-vyncke-6man-mcast-not-efficient-01>>.

[I-D.ietf-6tisch-architecture]

Thubert, P., "An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)", Work in Progress, Internet-Draft, draft-ietf-6tisch-architecture-30, 26 November 2020, <<https://datatracker.ietf.org/doc/html/draft-ietf-6tisch-architecture-30>>.

[MCAST PROBLEMS]

Perkins, C. E., McBride, M., Stanley, D., Kumari, W., and J. C. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", Work in Progress, Internet-Draft, draft-ietf-mboned-ieee802-mcast-problems-15, 28 July 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-mboned-ieee802-mcast-problems-15>>.

[SAVI]

Bi, J., Wu, J., Lin, T., Wang, Y., and L. He, "A SAVI Solution for WLAN", Work in Progress, Internet-Draft, draft-bi-savi-wlan-22, 10 November 2021, <<https://datatracker.ietf.org/doc/html/draft-bi-savi-wlan-22>>.

[UNICAST AR]

Thubert, P. and E. Levy-Abegnoli, "IPv6 Neighbor Discovery Unicast Lookup", Work in Progress, Internet-Draft, draft-thubert-6lo-unicast-lookup-02, 8 November 2021, <<https://datatracker.ietf.org/doc/html/draft-thubert-6lo-unicast-lookup-02>>.

[DAD APPROACHES]

Nordmark, E., "Possible approaches to make DAD more robust and/or efficient", Work in Progress, Internet-Draft, draft-nordmark-6man-dad-approaches-02, 19 October 2015, <<https://datatracker.ietf.org/doc/html/draft-nordmark-6man-dad-approaches-02>>.

[I-D.ietf-6lo-multicast-registration]

Thubert, P., "IPv6 Neighbor Discovery Multicast Address Listener Registration", Work in Progress, Internet-Draft, draft-ietf-6lo-multicast-registration-03, 13 December 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-6lo-multicast-registration-03>>.

[IEEE Std. 802.15.4]
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".

[IEEE Std. 802.11]
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)".

[IEEE Std. 802.1]
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".

Author's Address

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allée des Ormes - BP1200
06254 Mougins - Sophia Antipolis
France

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