IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 24, 2019

A. Petrescu
CEA, LIST
N. Benamar
Moulay Ismail University
J. Haerri
Eurecom
J. Lee
Sangmyung University
T. Ernst
YoGoKo

September 20, 2018

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-29

Abstract

In order to transmit IPv6 packets on IEEE 802.11 networks running outside the context of a basic service set (OCB, earlier "802.11p") there is a need to define a few parameters such as the supported Maximum Transmission Unit size on the 802.11-OCB link, the header format preceding the IPv6 header, the Type value within it, and others. This document describes these parameters for IPv6 and IEEE 802.11-OCB networks; it portrays the layering of IPv6 on 802.11-OCB similarly to other known 802.11 and Ethernet layers - by using an Ethernet Adaptation Layer.

Status of This Memo

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

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

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

This Internet-Draft will expire on March 24, 2019.

Copyright Notice

Copyright (c) 2018 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 5
4.1. Pseudonym Handling 5
4.2. Maximum Transmission Unit (MTU) 5
4.3. Frame Format 5
4.3.1. Ethernet Adaptation Layer 5
4.4. Link-Local Addresses 7
4.5. Address Mapping 7
4.5.1. Address Mapping -- Unicast 7
4.5.2. Address Mapping -- Multicast 7
4.6. Stateless Autoconfiguration 7
4.7. Subnet Structure 9
5. Security Considerations 10
5.1. Privacy Considerations 10
5.2. MAC Address and Interface ID Generation 11
6. IANA Considerations 11
7. Contributors 12
8. Acknowledgements 12
9. References 13
9.1. Normative References 13
9.2. Informative References 15
Appendix A. ChangeLog 17
Appendix B. 802.11p 26
Appendix C. Aspects introduced by the OCB mode to 802.11 26
Appendix D. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver . . . 30
Appendix E. EtherType Protocol Discrimination (EPD) 31
Appendix F. Design Considerations 32
Appendix G. IEEE 802.11 Messages Transmitted in OCB mode 32

Appendix H. Examples of Packet Formats 33
H.1. Capture in Monitor Mode 34
H.2. Capture in Normal Mode 36
Appendix I. Extra Terminology 38
Authors' Addresses 39

1. Introduction

This document describes the transmission of IPv6 packets on IEEE Std 802.11-OCB networks [IEEE-802.11-2016] (a.k.a "802.11p" see Appendix B, Appendix C and Appendix D). This involves the layering of IPv6 networking on top of the IEEE 802.11 MAC layer, with an LLC layer. Compared to running IPv6 over the Ethernet MAC layer, there is no modification expected to IEEE Std 802.11 MAC and Logical Link sublayers: IPv6 works fine directly over 802.11-OCB too, with an LLC layer.

The IPv6 network layer operates on 802.11-OCB in the same manner as operating on Ethernet, but there are two kinds of exceptions:

- Exceptions due to different operation of IPv6 network layer on 802.11 than on Ethernet. To satisfy these exceptions, this document describes an Ethernet Adaptation Layer between Ethernet headers and 802.11 headers. The Ethernet Adaptation Layer is described Section 4.3.1. The operation of IP on Ethernet is described in [RFC1042], [RFC2464] and [I-D.hinden-6man-rfc2464bis].

- Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure and handover behaviour. For security and privacy recommendations see Section 5 and Section 4.6. The subnet structure is described in Section 4.7. The handover behaviour on OCB links is not described in this document.

The Security Considerations section describes security and privacy aspects of 802.11-OCB.

In the published literature, many documents describe aspects and problems related to running IPv6 over 802.11-OCB: [I-D.ietf-ipwave-vehicular-networking-survey].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

IP-OBU (Internet Protocol On-Board Unit): an IP-OBU is a computer situated in a vehicle such as an automobile, 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 I.

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

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

The IEEE 802.11-OCB Networks are used for vehicular communications, as 'Wireless Access in Vehicular Environments'. The IP communication scenarios for these environments have been described in several documents; in particular, we refer the reader to [I-D.ietf-ipwave-vehicular-networking-survey], that lists some scenarios and requirements for IP in Intelligent Transportation Systems.

The link model is the following: STA --- 802.11-OCB --- STA. In vehicular networks, STAs can be IP-RSUs and/or IP-OBUs. While 802.11-OCB is clearly specified, and the use of IPv6 over such link is not radically new, the operating environment (vehicular networks) brings in new perspectives.

The mechanisms for forming and terminating, discovering, peering and mobility management for 802.11-OCB links are not described in this document.

4. IPv6 over 802.11-OCB

4.1. Pseudonym Handling

Pseudonym.

4.2. Maximum Transmission Unit (MTU)

The default MTU for IP packets on 802.11-OCB MUST be 1500 octets. It is the same value as IPv6 packets on Ethernet links, as specified in [RFC2464]. 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).

4.3. Frame Format

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

The IPv6 packet transmitted on 802.11-OCB MUST be 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), the value of the Type field MUST be set to 0x86DD (IPv6). In the 802.11 header, the value of the Subtype sub-field in the Frame Control field MUST be set to 8 (i.e. 'QoS Data'); the value of the Traffic Identifier (TID) sub-field of the QoS Control field of the 802.11 header MUST be set to binary 001 (i.e. User Priority 'Background', QoS Access Category 'AC_BK').

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers MAY implement an Ethernet Adaptation Layer that translates Ethernet II frames to the 802.11 format and vice versa. An Ethernet Adaptation Layer is described in Section 4.3.1.

4.3.1. Ethernet Adaptation Layer

An 'adaptation' layer is inserted between a MAC layer and the Networking layer. This is used to transform some parameters between their form expected by the IP stack and the form provided by the MAC layer.

An Ethernet Adaptation Layer makes an 802.11 MAC look to IP Networking layer as a more traditional Ethernet layer. At reception, this layer takes as input the IEEE 802.11 header and the Logical-Link Layer Control Header and produces an Ethernet II Header. At sending, the reverse operation is performed.

The operation of the Ethernet Adaptation Layer is depicted by the double arrow in Figure 1.

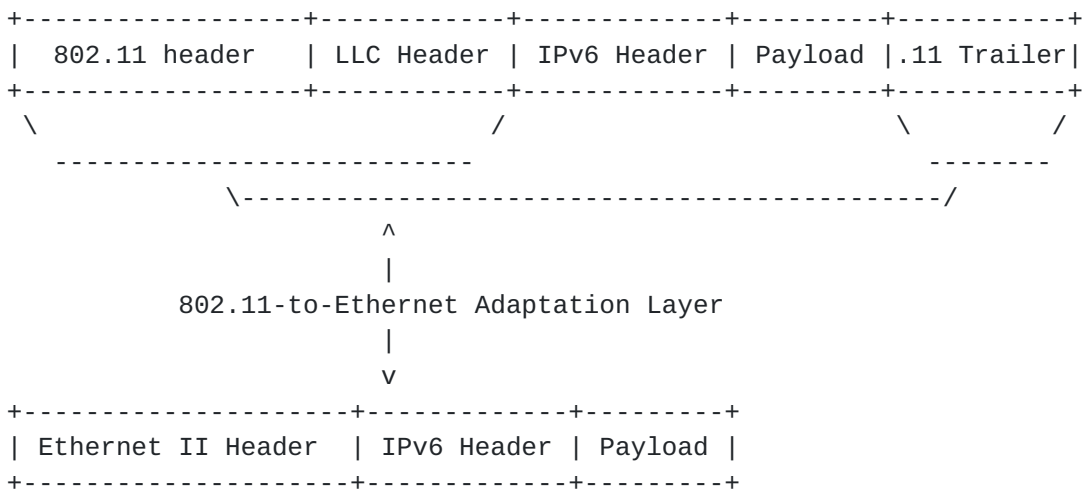


Figure 1: Operation of the Ethernet Adaptation Layer

The Receiver and Transmitter Address fields in the 802.11 header MUST contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header MUST be the same as the value of the Type field in the Ethernet II Header. That value MUST be set to 0x86DD (IPv6).

The ".11 Trailer" contains solely a 4-byte Frame Check Sequence.

The placement of IPv6 networking layer on Ethernet Adaptation Layer is illustrated in Figure 2.

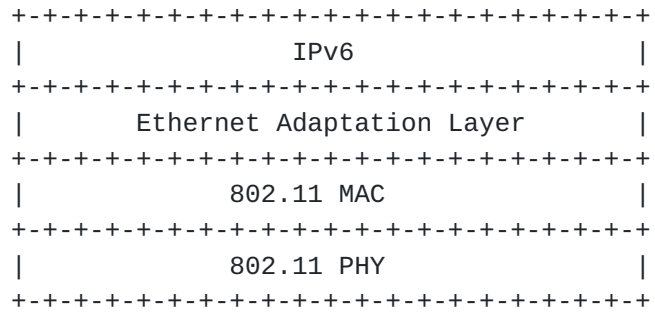


Figure 2: Ethernet Adaptation Layer stacked with other layers

(in the above figure, a 802.11 profile is represented; this is used also for 802.11-OCB profile.)

4.4. 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 MAY be formed using an EUI-64 identifier.

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. This mechanism is described in section 5 of [RFC2464].

For privacy, the link-local address MAY be formed according to the mechanisms described in Section 5.2.

4.5. Address Mapping

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

4.5.1. Address Mapping -- Unicast

The procedure for mapping IPv6 unicast addresses into Ethernet link-layer addresses is described in [RFC4861].

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.perkins-intarea-multicast-ieee802]. These issues may be exacerbated in OCB mode. Solutions for these problems should consider the OCB mode of operation.

4.6. Stateless Autoconfiguration

There are several types of IPv6 addresses [RFC4291], [RFC4193], that MAY be assigned to an 802.11-OCB interface. 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' see Section 4.4.

The Interface Identifier for an 802.11-OCB interface is formed using the same rules as the Interface Identifier for an Ethernet interface; 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.

The bits in the Interface Identifier have no generic 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]. If semantically opaque Interface Identifiers are needed, a potential method for generating semantically opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration is given in [RFC7217].

Semantically opaque Interface Identifiers, instead of meaningful Interface Identifiers derived from a valid and meaningful MAC address ([RFC2464], section 4), MAY be needed in order to avoid certain privacy risks.

A valid MAC address includes a unique identifier pointing to a company together with its postal address, and a unique number within that company MAC space (see the oui.txt file). The calculation operation of the MAC address back from a given meaningful Interface Identifier is straightforward ([RFC2464], section 4). The Interface Identifier is part of an IPv6 address that is stored in IPv6 packets. The IPv6 packets can be captured in the Internet easily. For these reasons, an attacker may realize many attacks on privacy. One such attack on 802.11-OCB is to capture, store and correlate Company ID information of many cars in public areas (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.

In order to avoid these risks, opaque Interface Identifiers MAY be formed according to rules described in [RFC7217]. These opaque Interface Identifiers are formed starting from identifiers different than the MAC addresses, and from cryptographically strong material. Thus, privacy sensitive information is absent from Interface IDs, and it is impossible to calculate the initial value from which the Interface ID was calculated.

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose Interface Identifiers don't change too often. It is RECOMMENDED to use the

mechanisms described in RFC 7217 to permit the use of Stable Interface Identifiers 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.

The way Interface Identifiers are used MAY involve risks to privacy, as described in Section 5.1.

4.7. Subnet Structure

A subnet is formed by the external 802.11-OCB interfaces of vehicles that are in close range (not by their in-vehicle interfaces). This subnet MUST use at least the link-local prefix fe80::/10 and the interfaces MUST be assigned IPv6 addresses of type link-local. This subnet MAY NOT have any other prefix than the link-local prefix.

The structure of this subnet is ephemeral, in that it is strongly influenced by the mobility of vehicles: the 802.11 hidden node 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 car 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 (a default route is absent), and the addressing peers are equally qualified (impossible to determine that some vehicle owns and distributes addresses to others) the use of link-local addresses is RECOMMENDED.

The Neighbor Discovery protocol (ND) [RFC4861] is used over 802.11-OCB links.

The operation of the Mobile IPv6 protocol over 802.11-OCB links is different than on other links. The Movement Detection operation (section 11.5.1 of [RFC6275]) can not rely on Neighbor Unreachability Detection operation of the Neighbor Discovery protocol, for the reason mentioned in the previous paragraph. Also, the 802.11-OCB link layer is not a lower layer that can provide an indication that a link layer handover has occured. The operation of the Mobile IPv6 protocol over 802.11-OCB is not specified in this document.

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 application layer, the IEEE 1609.2 document [IEEE-1609.2] does provide 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 perform 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.

Within the IPsec Security Architecture [RFC4301], the IPsec AH and ESP headers [RFC4302] and [RFC4303] respectively, its multicast extensions [RFC5374], HTTPS [RFC2818] and SeND [RFC3971] protocols can be used to protect communications. Further, the assistance of proper Public Key Infrastructure (PKI) protocols [RFC4210] is necessary to establish credentials. More IETF protocols are available in the toolbox of the IP security protocol designer. Certain ETSI protocols related to security protocols in Intelligent Transportation Systems 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 address 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 4.6. This may help mitigate privacy risks to a certain level.

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 C.

A 'randomized' MAC address has the following characteristics:

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

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

A randomized Interface ID has the same characteristics of a randomized MAC address, except the length in bits. A MAC address SHOULD be of length 48 decimal. An Interface ID SHOULD be of length 64 decimal for all types of IPv6 addresses. In the particular case of IPv6 link-local addresses, the length of the Interface ID MAY be 118 decimal.

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 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 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>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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.hinden-6man-rfc2464bis]
Crawford, M. and R. Hinden, "Transmission of IPv6 Packets over Ethernet Networks", draft-hinden-6man-rfc2464bis-02 (work in progress), March 2017.

[I-D.ietf-ipwave-vehicular-networking-survey]
Jeong, J., Cespedes, S., Benamar, N., Haerri, J., and M. Wetterwald, "Survey on IP-based Vehicular Networking for Intelligent Transportation Systems", draft-ietf-ipwave-vehicular-networking-survey-00 (work in progress), July 2017.

[I-D.perkins-intarea-multicast-ieee802]
Perkins, C., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-perkins-intarea-multicast-ieee802-03 (work in progress), July 2017.

[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 on September 12th, 2017, at 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.".

Appendix A. ChangeLog

The changes are listed in reverse chronological order, most recent changes appearing at the top of the list.

-29:

o

-28:

o Created a new section 'Pseudonym Handling'.

o removed the 'Vehicle ID' appendix.

o improved the address generation from random MAC address.

o shortened Term IP-RSU definition.

o removed refs to two detail Clauses in IEEE documents, kept just these latter.

-27: part 1 of addressing Human Rights review from IRTF. Removed appendices F.2 and F.3. Shortened definition of IP-RSU. Removed reference to 1609.4. A few other small changes, see diff.

-26: moved text from SLAAC section and from Design Considerations appendix about privacy into a new Privacy Condiderations subsection of the Security section; reformulated the SLAAC and IID sections to stress only LLs can use EUI-64; removed the "GeoIP" wireshark explanation; reformulated SLAAC and LL sections; added brief mention of need of use LLs; clarified text about MAC address changes; dropped pseudonym discussion; changed title of section describing examples of packet formats.

-25: added a reference to 'IEEE Management Information Base', instead of just 'Management Information Base'; added ref to further appendices in the introductory phrases; improved text for IID formation for SLAAC, inserting recommendation for RFC8064 before RFC2464.

From draft-ietf-ipwave-ipv6-over-80211ocb-23 to draft-ietf-ipwave-ipv6-over-80211ocb-24

o Nit: wrote "IPWAVE Working Group" on the front page, instead of "Network Working Group".

- Addressed the comments on 6MAN: replaced a sentence about ND problem with "is used over 802.11-OCB".

From draft-ietf-ipwave-ipv6-over-80211ocb-22 to draft-ietf-ipwave-ipv6-over-80211ocb-23

- No content modifications, but check the entire draft chain on IPv6-only: xml2rfc, submission on tools.ietf.org and datatracker.

From draft-ietf-ipwave-ipv6-over-80211ocb-21 to draft-ietf-ipwave-ipv6-over-80211ocb-22

- Corrected typo, use dash in "802.11-OCB" instead of space.

- Improved the Frame Format section: MUST use QoSData, specify the values within; clarified the Ethernet Adaptation Layer text.

From draft-ietf-ipwave-ipv6-over-80211ocb-20 to draft-ietf-ipwave-ipv6-over-80211ocb-21

- Corrected a few nits and added names in Acknowledgments section.

- Removed unused reference to old Internet Draft tsvwg about QoS.

From draft-ietf-ipwave-ipv6-over-80211ocb-19 to draft-ietf-ipwave-ipv6-over-80211ocb-20

- Reduced the definition of term "802.11-OCB".

- Left out of this specification which 802.11 header to use to transmit IP packets in OCB mode (QoS Data header, Data header, or any other).

- Added 'MUST' use an Ethernet Adaptation Layer, instead of 'is using' an Ethernet Adaptation Layer.

From draft-ietf-ipwave-ipv6-over-80211ocb-18 to draft-ietf-ipwave-ipv6-over-80211ocb-19

- Removed the text about fragmentation.

- Removed the mentioning of WSMP and GeoNetworking.

- Removed the explanation of the binary representation of the EtherType.

- Rendered normative the paragraph about unicast and multicast address mapping.

- Removed paragraph about addressing model, subnet structure and easiness of using LLs.

- Clarified the Type/Subtype field in the 802.11 Header.

- Used RECOMMENDED instead of recommended, for the stable interface identifiers.

From draft-ietf-ipwave-ipv6-over-80211ocb-17 to draft-ietf-ipwave-ipv6-over-80211ocb-18

- Improved the MTU and fragmentation paragraph.

From draft-ietf-ipwave-ipv6-over-80211ocb-16 to draft-ietf-ipwave-ipv6-over-80211ocb-17

- Susbtituted "MUST be increased" to "is increased" in the MTU section, about fragmentation.

From draft-ietf-ipwave-ipv6-over-80211ocb-15 to draft-ietf-ipwave-ipv6-over-80211ocb-16

- Removed the definition of the 'WiFi' term and its occurences. Clarified a phrase that used it in Appendix C "Aspects introduced by the OCB mode to 802.11".

- Added more normative words: MUST be 0x86DD, MUST fragment if size larger than MTU, Sequence number in 802.11 Data header MUST be increased.

From draft-ietf-ipwave-ipv6-over-80211ocb-14 to draft-ietf-ipwave-ipv6-over-80211ocb-15

- Added normative term MUST in two places in section "Ethernet Adaptation Layer".

From draft-ietf-ipwave-ipv6-over-80211ocb-13 to draft-ietf-ipwave-ipv6-over-80211ocb-14

- Created a new Appendix titled "Extra Terminology" that contains terms DSRC, DSRCS, OBU, RSU as defined outside IETF. Some of them are used in the main Terminology section.

- Added two paragraphs explaining that ND and Mobile IPv6 have problems working over 802.11-OCB, yet their adaptations is not specified in this document.

From draft-ietf-ipwave-ipv6-over-80211ocb-12 to draft-ietf-ipwave-ipv6-over-80211ocb-13

- Substituted "IP-OBU" for "OBRU", and "IP-RSU" for "RSRU" throughout and improved OBU-related definitions in the Terminology section.

From draft-ietf-ipwave-ipv6-over-80211ocb-11 to draft-ietf-ipwave-ipv6-over-80211ocb-12

- Improved the appendix about "MAC Address Generation" by expressing the technique to be an optional suggestion, not a mandatory mechanism.

From draft-ietf-ipwave-ipv6-over-80211ocb-10 to draft-ietf-ipwave-ipv6-over-80211ocb-11

- Shortened the paragraph on forming/terminating 802.11-OCB links.

- Moved the draft tsvwg-ieee-802-11 to Informative References.

From draft-ietf-ipwave-ipv6-over-80211ocb-09 to draft-ietf-ipwave-ipv6-over-80211ocb-10

- Removed text requesting a new Group ID for multicast for OCB.

- Added a clarification of the meaning of value "3333" in the section Address Mapping -- Multicast.

- Added note clarifying that in Europe the regional authority is not ETSI, but "ECC/CEPT based on ENs from ETSI".

- Added note stating that the manner in which two STAtions set their communication channel is not described in this document.

- Added a time qualifier to state that the "each node is represented uniquely at a certain point in time."

- Removed text "This section may need to be moved" (the "Reliability Requirements" section). This section stays there at this time.

- In the term definition "802.11-OCB" added a note stating that "any implementation should comply with standards and regulations set in the different countries for using that frequency band."

- In the RSU term definition, added a sentence explaining the difference between RSU and RSRU: in terms of number of interfaces and IP forwarding.

- Replaced "with at least two IP interfaces" with "with at least two real or virtual IP interfaces".
- Added a term in the Terminology for "OBU". However the definition is left empty, as this term is defined outside IETF.
- Added a clarification that it is an OBU or an OBRU in this phrase "A vehicle embarking an OBU or an OBRU".
- Checked the entire document for a consistent use of terms OBU and OBRU.
- Added note saying that "'p' is a letter identifying the Ammendment".
- Substituted lower case for capitals SHALL or MUST in the Appendices.
- Added reference to RFC7042, helpful in the 3333 explanation. Removed reference to individual submission draft-petrescu-its-scenario-reqs and added reference to draft-ietf-ipwave-vehicular-networking-survey.
- Added figure captions, figure numbers, and references to figure numbers instead of 'below'. Replaced "section Section" with "section" throughout.
- Minor typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-08 to draft-ietf-ipwave-ipv6-over-80211ocb-09

- Significantly shortened the Address Mapping sections, by text copied from RFC2464, and rather referring to it.
- Moved the EPD description to an Appendix on its own.
- Shortened the Introduction and the Abstract.
- Moved the tutorial section of OCB mode introduced to .11, into an appendix.
- Removed the statement that suggests that for routing purposes a prefix exchange mechanism could be needed.
- Removed refs to RFC3963, RFC4429 and RFC6775; these are about ND, MIP/NEMO and oDAD; they were referred in the handover discussion section, which is out.

- Updated a reference from individual submission to now a WG item in IPWAVE: the survey document.
- Added term definition for WiFi.
- Updated the authorship and expanded the Contributors section.
- Corrected typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-07 to draft-ietf-ipwave-ipv6-over-80211ocb-08

- Removed the per-channel IPv6 prohibition text.
- Corrected typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-06 to draft-ietf-ipwave-ipv6-over-80211ocb-07

- Added new terms: OBRU and RSRU ('R' for Router). Refined the existing terms RSU and OBU, which are no longer used throughout the document.
- Improved definition of term "802.11-OCB".
- Clarified that OCB does not "strip" security, but that the operation in OCB mode is "stripped off of all .11 security".
- Clarified that theoretical OCB bandwidth speed is 54mbits, but that a commonly observed bandwidth in IP-over-OCB is 12mbit/s.
- Corrected typographical errors, and improved some phrasing.

From draft-ietf-ipwave-ipv6-over-80211ocb-05 to draft-ietf-ipwave-ipv6-over-80211ocb-06

- Updated references of 802.11-OCB document from -2012 to the IEEE 802.11-2016.
- In the LL address section, and in SLAAC section, added references to 7217 opaque IIDs and 8064 stable IIDs.

From draft-ietf-ipwave-ipv6-over-80211ocb-04 to draft-ietf-ipwave-ipv6-over-80211ocb-05

- Lengthened the title and cleanded the abstract.

- Added text suggesting LLs may be easy to use on OCB, rather than GUAs based on received prefix.
- Added the risks of spoofing and hijacking.
- Removed the text speculation on adoption of the TSA message.
- Clarified that the ND protocol is used.
- Clarified what it means "No association needed".
- Added some text about how two STAs discover each other.
- Added mention of external (OCB) and internal network (stable), in the subnet structure section.
- Added phrase explaining that both .11 Data and .11 QoS Data headers are currently being used, and may be used in the future.
- Moved the packet capture example into an Appendix Implementation Status.
- Suggested moving the reliability requirements appendix out into another document.
- Added a IANA Consiserations section, with content, requesting for a new multicast group "all OCB interfaces".
- Added new OBU term, improved the RSU term definition, removed the ETTC term, replaced more occurences of 802.11p, 802.11-OCB with 802.11-OCB.
- References:
  - Added an informational reference to ETSI's IPv6-over-GeoNetworking.
  - Added more references to IETF and ETSI security protocols.
  - Updated some references from I-D to RFC, and from old RFC to new RFC numbers.
  - Added reference to multicast extensions to IPsec architecture RFC.
  - Added a reference to 2464-bis.
  - Removed FCC informative references, because not used.

- Updated the affiliation of one author.
- Reformulation of some phrases for better readability, and correction of typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-03 to draft-ietf-ipwave-ipv6-over-80211ocb-04

- Removed a few informative references pointing to Dx draft IEEE 1609 documents.
- Removed outdated informative references to ETSI documents.
- Added citations to IEEE 1609.2, .3 and .4-2016.
- Minor textual issues.

From draft-ietf-ipwave-ipv6-over-80211ocb-02 to draft-ietf-ipwave-ipv6-over-80211ocb-03

- Keep the previous text on multiple addresses, so remove talk about MIP6, NEMOv6 and MCoA.
- Clarified that a 'Beacon' is an IEEE 802.11 frame Beacon.
- Clarified the figure showing Infrastructure mode and OCB mode side by side.
- Added a reference to the IP Security Architecture RFC.
- Detailed the IPv6-per-channel prohibition paragraph which reflects the discussion at the last IETF IPWAVE WG meeting.
- Added section "Address Mapping -- Unicast".
- Added the ".11 Trailer" to pictures of 802.11 frames.
- Added text about SNAP carrying the Ethertype.
- New RSU definition allowing for it be both a Router and not necessarily a Router some times.
- Minor textual issues.

From draft-ietf-ipwave-ipv6-over-80211ocb-01 to draft-ietf-ipwave-ipv6-over-80211ocb-02

- Replaced almost all occurences of 802.11p with 802.11-OCB, leaving only when explanation of evolution was necessary.
- Shortened by removing parameter details from a paragraph in the Introduction.
- Moved a reference from Normative to Informative.
- Added text in intro clarifying there is no handover spec at IEEE, and that 1609.2 does provide security services.
- Named the contents the fields of the EthernetII header (including the Ethertype bitstring).
- Improved relationship between two paragraphs describing the increase of the Sequence Number in 802.11 header upon IP fragmentation.
- Added brief clarification of "tracking".

From draft-ietf-ipwave-ipv6-over-80211ocb-00 to draft-ietf-ipwave-ipv6-over-80211ocb-01

- Introduced message exchange diagram illustrating differences between 802.11 and 802.11 in OCB mode.
- Introduced an appendix listing for information the set of 802.11 messages that may be transmitted in OCB mode.
- Removed appendix sections "Privacy Requirements", "Authentication Requirements" and "Security Certificate Generation".
- Removed appendix section "Non IP Communications".
- Introductory phrase in the Security Considerations section.
- Improved the definition of "OCB".
- Introduced theoretical stacked layers about IPv6 and IEEE layers including EPD.
- Removed the appendix describing the details of prohibiting IPv6 on certain channels relevant to 802.11-OCB.
- Added a brief reference in the privacy text about a precise clause in IEEE 1609.3 and .4.
- Clarified the definition of a Road Side Unit.

- Removed the discussion about security of WSA (because is non-IP).
- Removed mentioning of the GeoNetworking discussion.
- Moved references to scientific articles to a separate 'overview' draft, and referred to it.

Appendix B. 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 C. 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. At link layer, it is necessary to set the same channel number (or frequency) on two stations that need to communicate with each other. The manner in which stations set their channel number is not specified in this document. Stations STA1 and STA2 can exchange IP packets if they are set on the same channel. At IP layer, they then discover each other by using the IPv6 Neighbor Discovery protocol.

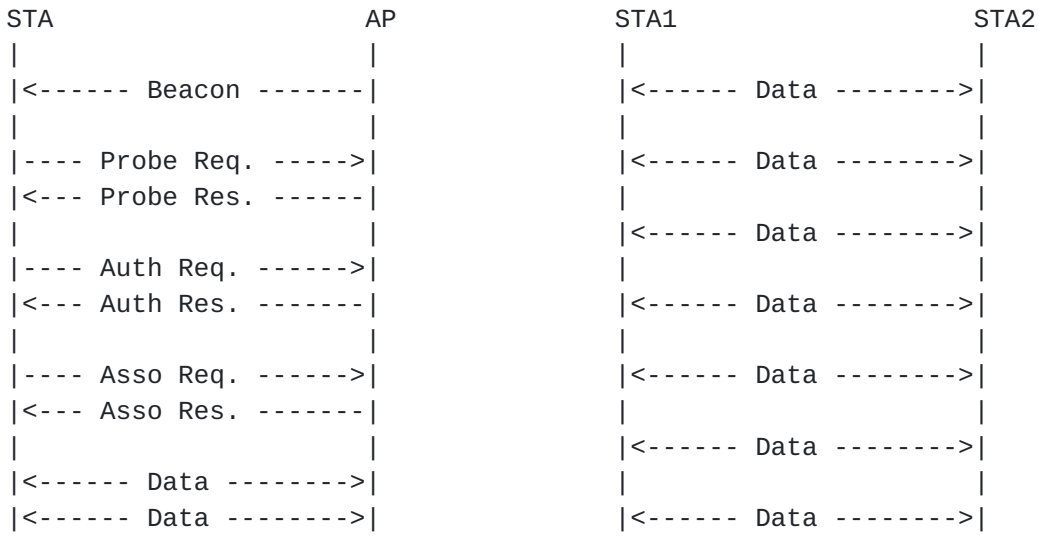
Briefly, the IEEE 802.11-OCB mode has the following properties:

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

All the nodes in the radio communication range (IP-OBU and IP-RSU) receive all the messages transmitted (IP-OBU and IP-RSU) within the

radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

The message exchange diagram in Figure 3 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 G.



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

Figure 3: 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 Ammendment, just like 'a, b, g' and 'n' are, 'p' is concerned more with MAC modifications, and a little with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a 'p' MAC with an 'a' PHY by operating outside the context of a BSS with OFDM at 5.4GHz and 5.9GHz.

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

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

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

- Operation Outside the Context of a BSS (OCB): the (earlier 802.11p) 802.11-OCB links are operated without a Basic Service Set (BSS). This means that the frames IEEE 802.11 Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always 0xffffffffffff (48 '1' bits, represented as MAC address ff:ff:ff:ff:ff:ff, or otherwise the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by administrator (e.g. 'My-Home-AccessPoint'). The OCB operation -

namely the lack of beacon-based scanning and lack of authentication - should be taken into account when the Mobile IPv6 protocol [RFC6275] and the protocols for IP layer security [RFC4301] are used. The way these protocols adapt to OCB is not described in this document.

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

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

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

- In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong

need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in Section 5. A relevant function is described in documents IEEE 1609.3-2016 [IEEE-1609.3] and IEEE 1609.4-2016 [IEEE-1609.4].

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

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

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

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

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

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

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

Changes needed on the network stack in OCB mode:

- Physical layer:

  * The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.

  * The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).

  * The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules, if used by the kernel to enforce local specific

restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

MAC layer:

* All management frames (beacons, join, leave, and others) emission and reception must be disabled except for frames of subtype Action and Timing Advertisement (defined below).

* No encryption key or method must be used.

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

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

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

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

Appendix E. EtherType Protocol Discrimination (EPD)

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated in Figure 4. 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).

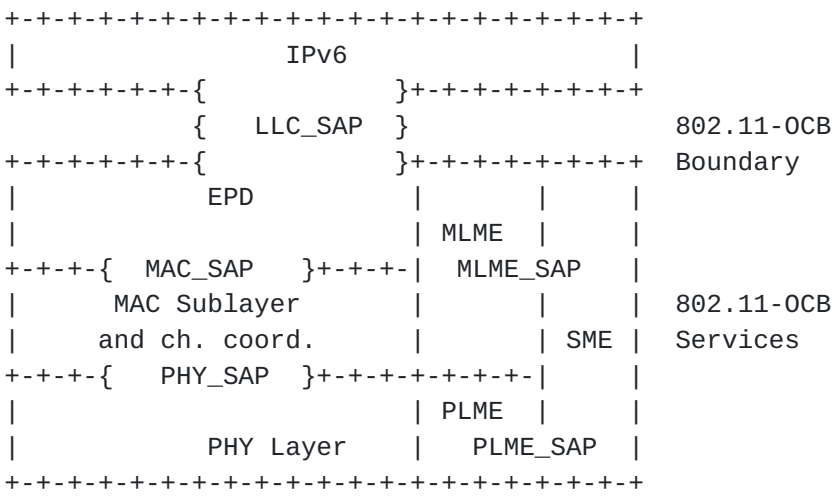


Figure 4: EtherType Protocol Discrimination

Appendix F. 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 encapsulation 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 G. IEEE 802.11 Messages Transmitted in OCB mode

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

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

Appendix H. 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 5, 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).

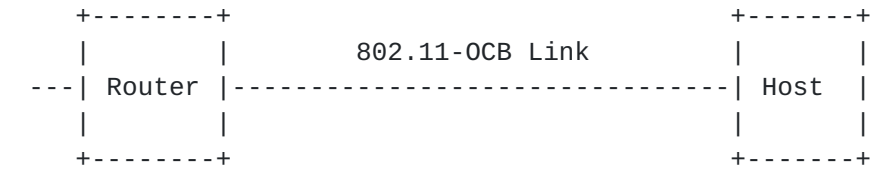


Figure 5: Topology for capturing IP packets on 802.11-OCB

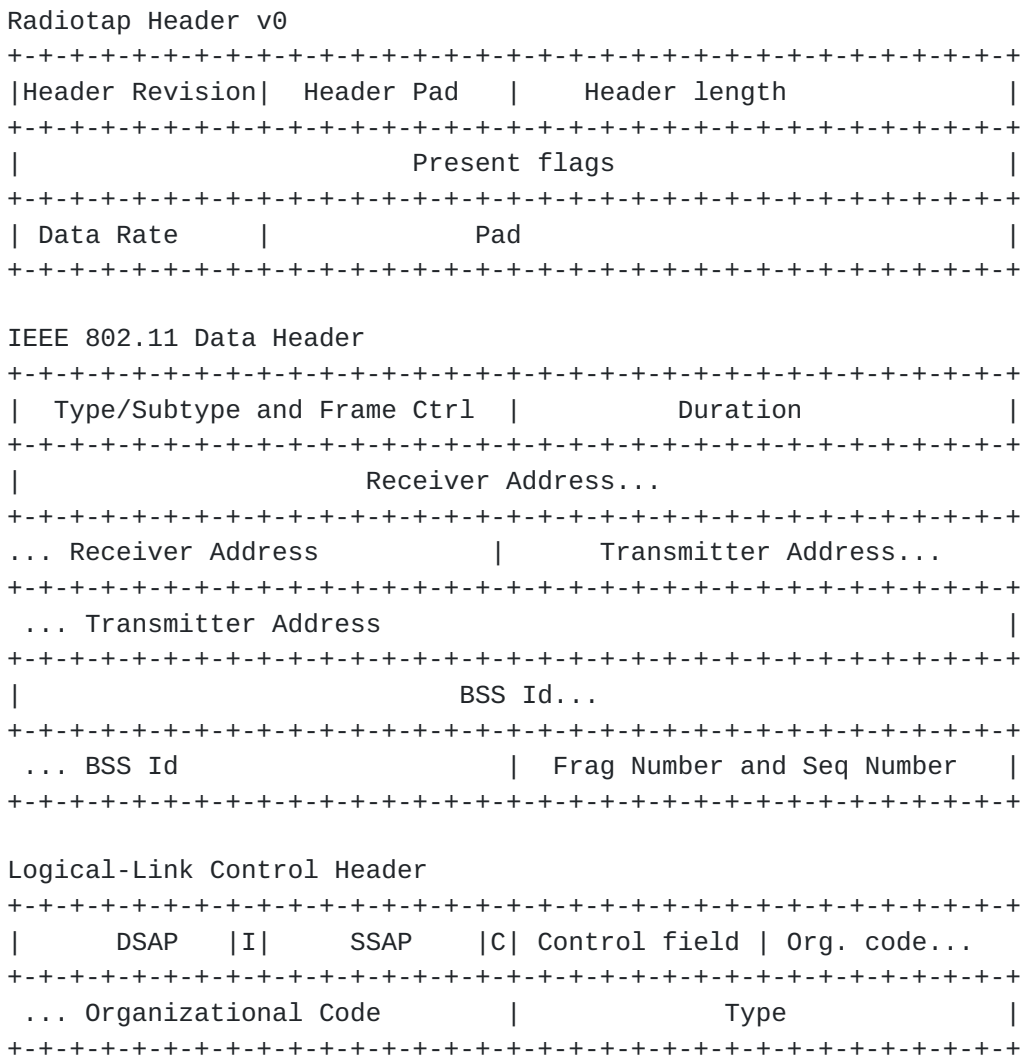
During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

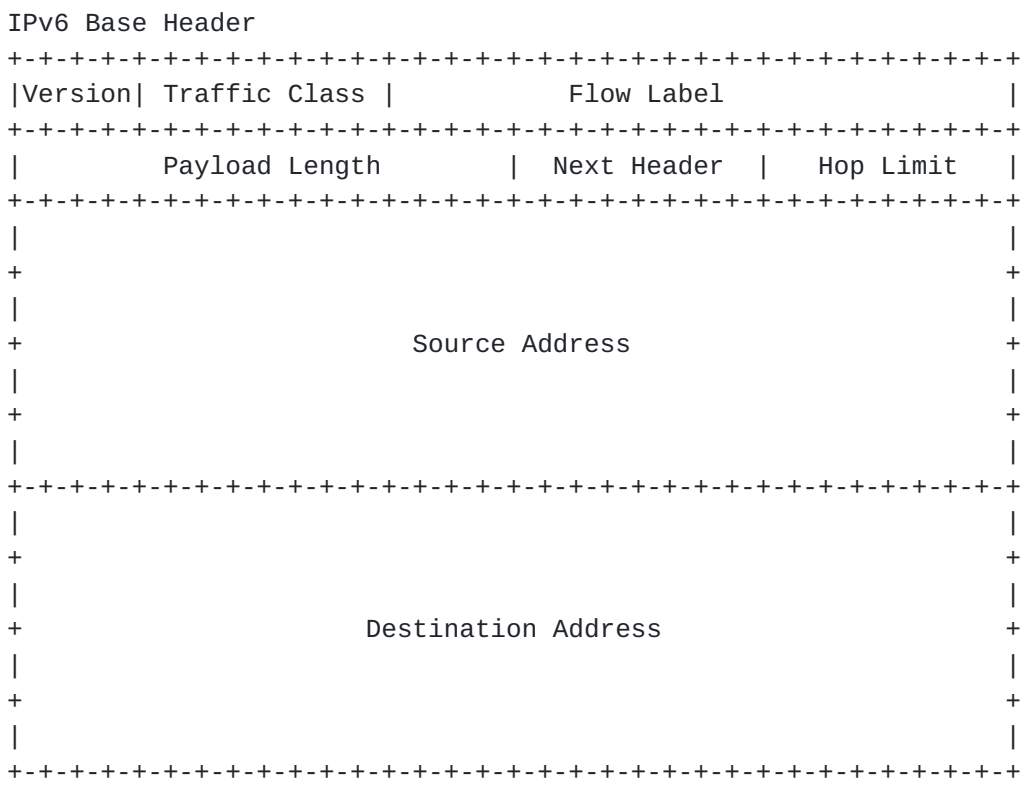
Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

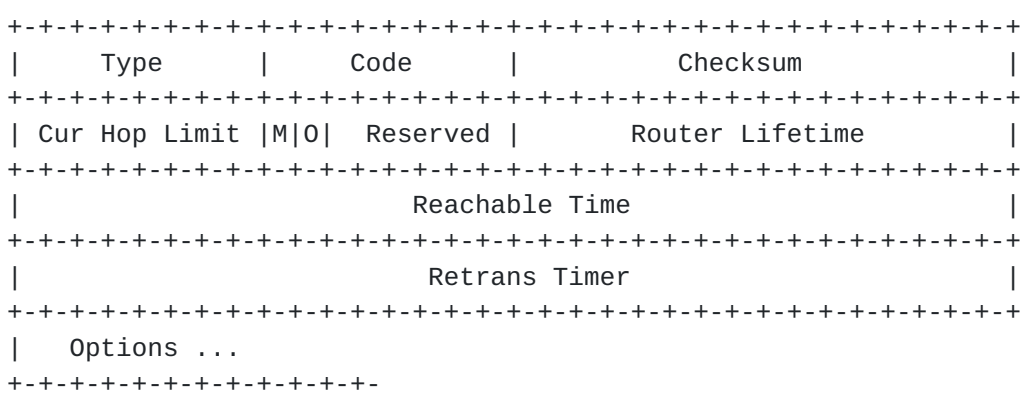
H.1. Capture in Monitor Mode

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.







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].

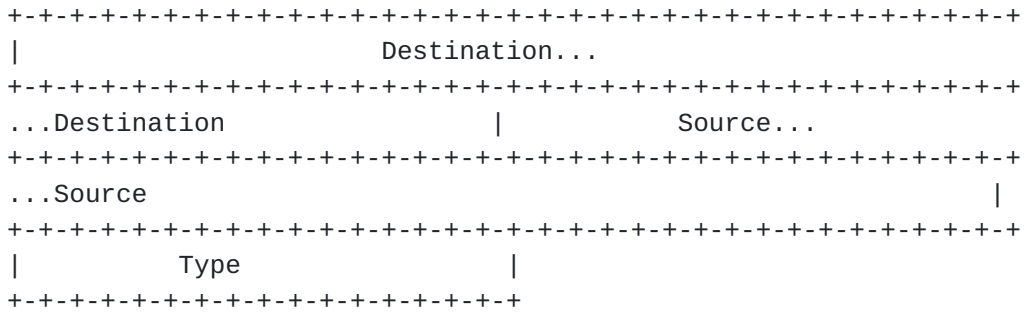
The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1.

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.

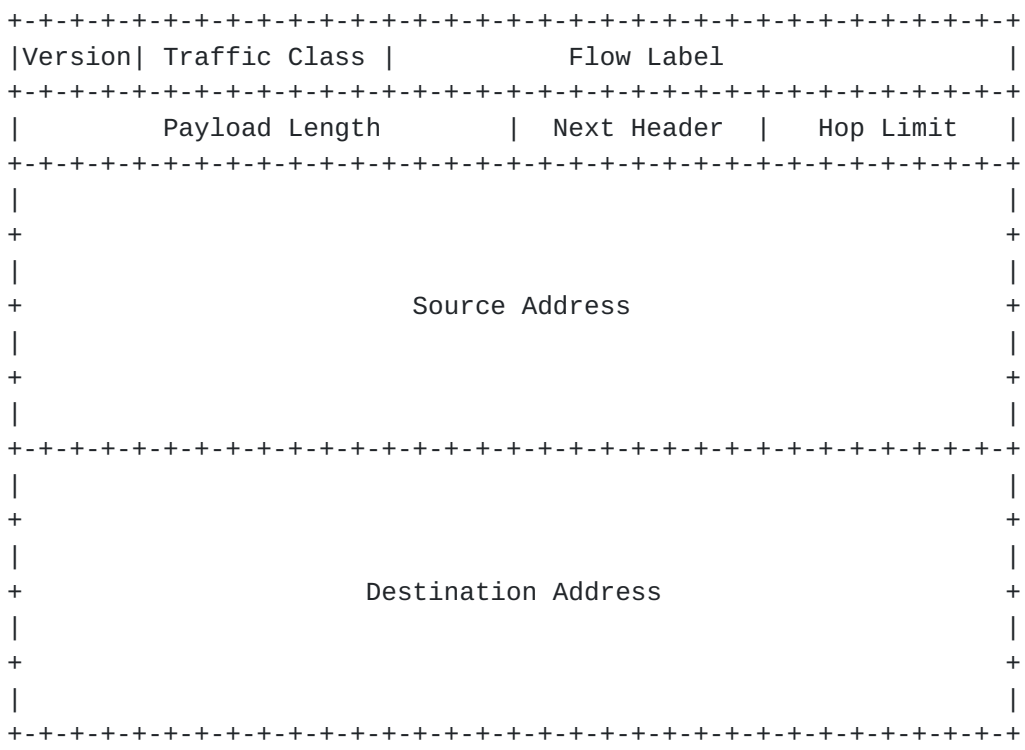
H.2. Capture in Normal Mode

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

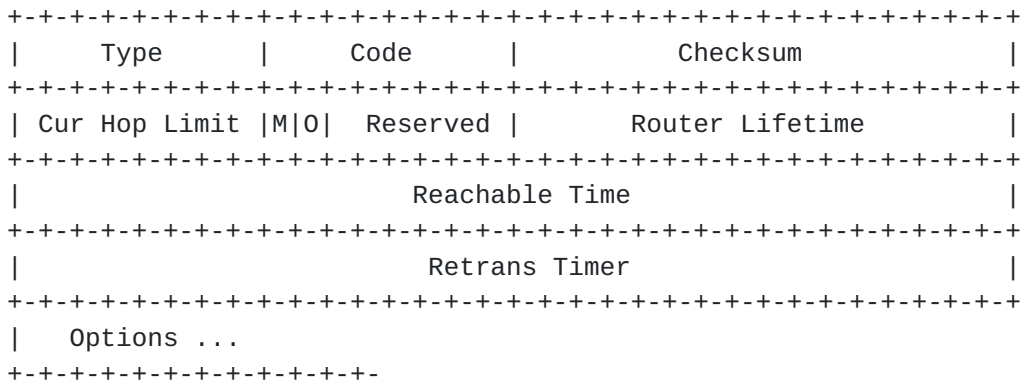
Ethernet II Header



IPv6 Base Header



Router Advertisement



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

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

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

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

An Adaptation layer 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 I. 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 DSRCS transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of the respective chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of the respective chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands. - [CFR 90.7 - Definitions].

RSU (Road-Side Unit): a term defined outside of IETF. A Roadside Unit is a 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 respectgive 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].

Authors' Addresses

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

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

Nabil Benamar
Moulay Ismail University
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