Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 16, 2018

A. Petrescu
CEA, LIST
N. Benamar
Moulay Ismail University
J. Haerri
Eurecom
C. Huitema
Private Octopus Inc.
J. Lee
Sangmyung University
T. Ernst
YoGoKo
T. Li
Peloton Technology
September 12, 2017

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-06.txt

Abstract

In order to transmit IPv6 packets on IEEE 802.11 networks run 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.

In addition, the document lists what is different in 802.11-OCB (802.11p) links compared to more 'traditional' 802.11a/b/g/n links, where IPv6 protocols operate without issues. Most notably, the operation outside the context of a BSS (OCB) has impact on IPv6 handover behaviour and on IPv6 security.

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/.

Copyright Notice

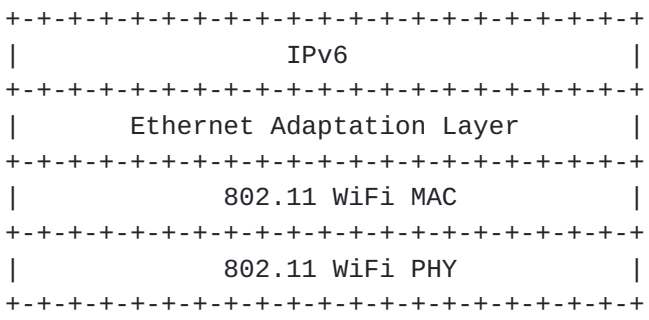
Table of Contents

1. Introduction

This document describes the transmission of IPv6 packets on IEEE Std 802.11-OCB networks (earlier known as 802.11p) [IEEE-802.11-2016]. 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 required to the standards: IPv6 works fine directly over 802.11-OCB too (with an LLC layer).

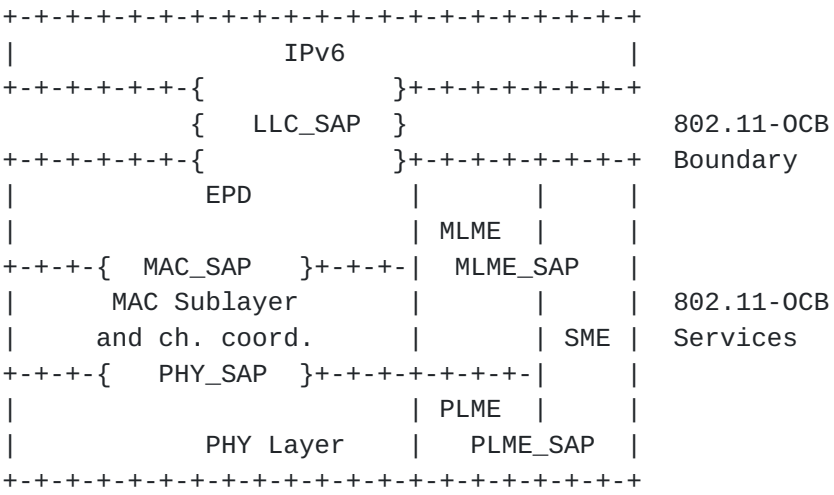
The term "802.11p" is an earlier definition. The behaviour of "802.11p" networks is rolled in the document IEEE Std 802.11-2016. In that document the term 802.11p disappears. Instead, each 802.11p feature is conditioned by a flag in the Management Information Base. That flag is named "OCBActivated". Whenever OCBActivated is set to true the feature it relates to, or represents, an earlier 802.11p feature. 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.

The IPv6 network layer operates on 802.11-OCB in the same manner as it operates on 802.11 WiFi, with a few particular exceptions. The IPv6 network layer operates on WiFi by involving an Ethernet Adaptation Layer; this Ethernet Adaptation Layer maps 802.11 headers to Ethernet II headers. The operation of IP on Ethernet is described in [RFC1042], [RFC2464] and [I-D.hinden-6man-rfc2464bis]. The situation of IPv6 networking layer on Ethernet Adaptation Layer is illustrated below:



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

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated below. 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 Accesss Point).



In addition to the description of interface between IP and MAC using "Ethernet Adaptation Layer" and "Ethernet Protocol Discrimination (EPD)" it is worth mentioning that SNAP [RFC1042] is used to carry the IPv6 Ethertype.

However, there may be some deployment considerations helping optimize the performances of running IPv6 over 802.11-OCB (e.g. in the case of handovers between 802.11-OCB-enabled access routers, or the consideration of using the IP security architecture [RFC4301]).

There are currently no specifications for handover between OCB links since these are currently specified as LLC-1 links (i.e. connectionless). Any handovers must be performed above the Data Link Layer. To realize handovers between OCB links there is a need of specific indicators to assist in the handover process. The indicators may be IP Router Advertisements, or 802.11-OCB's Time Advertisements, or higher layer messages such as the 'Basic Safety Message' (in the US), or the 'Cooperative Awareness Message' (in the EU), or the 'WAVE Routing Advertisement'. However, this document does not describe handover behaviour.

The OCB operation is stripping off 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. A security mechanism provided at networking layer, such as IPsec [RFC4301], may provide data security protection to a wider range of applications. See the section Security Considerations of this document, Section 6

We briefly introduce the vehicular communication scenarios where IEEE 802.11-OCB links are used. This is followed by a description of differences in specification terms, between 802.11-OCB and 802.11a/b/g/n - we answer the question of what are the aspects introduced by OCB mode to 802.11; the same aspects, but expressed in terms of requirements to implementation, are listed in Appendix B.)

The document then concentrates on the parameters of layering IP over 802.11-OCB as over Ethernet: value of MTU, the Frame Format which includes a description of an Ethernet Adaptation Layer, the forming of Link-Local Addresses the rules for forming Interface Identifiers for Stateless Autoconfiguration, the mechanisms for Address Mapping. These are precisely the same as IPv6 over Ethernet [RFC2464]. A reference is made to ad-hoc networking characteristics of the subnet structure in OCB mode.

As an example, these characteristics of layering IPv6 straight over LLC over 802.11-OCB MAC are illustrated by dissecting an IPv6 packet captured over a 802.11-OCB link; this is described in the section Appendix E.

In the published literature, many documents describe aspects related to running IPv6 over 802.11-OCB:
[I-D.jeong-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].

OBU (On-Board Unit): contrary to an RSU, an OBU is almost always situated in a vehicle; it is a computer with at least two IP interfaces; also, at least one IP interface runs in OCB mode of 802.11. It may be an IP router.

RSU (Road Side Unit): It is a Wireless Termination Point (WTP), as defined in [RFC5415], or an Access Point (AP), or an Access Network Router (ANR) defined in [RFC3753], with one key particularity: the wireless PHY/MAC layer is configured to operate in 802.11-OCB mode. The RSU communicates with the On board Unit (OBU) in the vehicle over 802.11 wireless link operating in OCB mode. An RSU MAY be connected to the Internet, and MAY be an IP router. When it is connected to the Internet, the term V2I (Vehicle to Internet) is relevant.

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, or 802.11-OCB: text in document IEEE 802.11-2016 that is flagged by "dot11OCBActivated". The text flagged "dot11OCBActivated" includes IEEE 802.11e for quality of service, 802.11j-2004 for half-clocked operations and (what was known earlier as) 802.11p for operation in the 5.9 GHz band and in mode OCB.

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, among which we refer the reader to one recently updated [I-D.petrescu-its-scenarios-reqs], about 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 RSUs and/or 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 802.11-OCB links form and terminate; nodes connected to these links peer, and discover each other; the nodes are mobile. However,

the precise description of how links discover each other, peer and manage mobility is not given in this document.

4. Aspects introduced by the OCB mode to 802.11

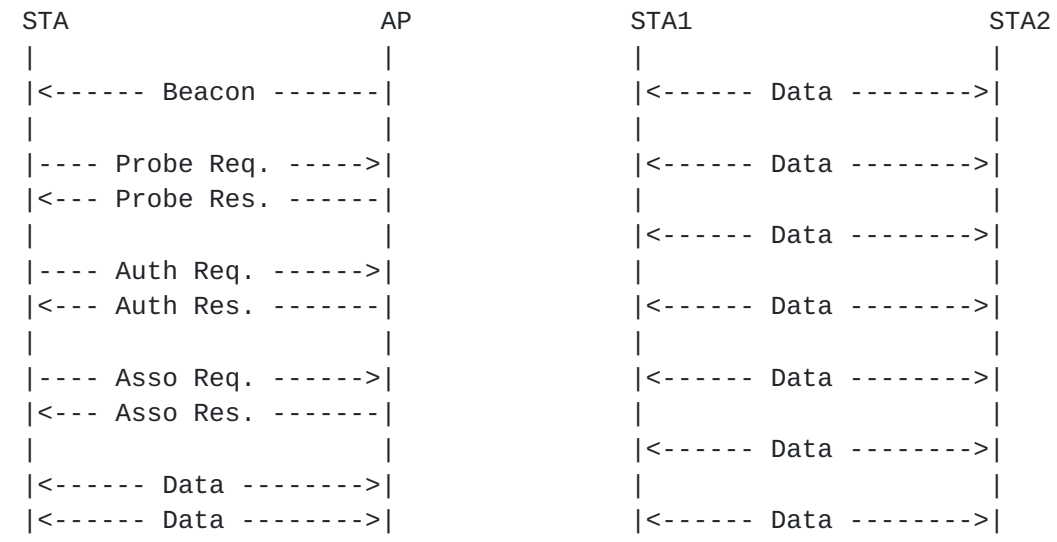
In the IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. At link layer, it is necessary to set a same channel number (or frequency) on two stations that need to communicate with each other. Stations 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 (OBU and RSU) receive all the messages transmitted (OBU and RSU) within the radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

The following message exchange diagram 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 D.



(a) 802.11 Infrastructure mode (b) 802.11-OCB mode

The link 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 included in IEEE 802.11(TM)-2016 [IEEE-802.11-2016], titled "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"; the modifications are diffused throughout various sections (e.g. the Time Advertisement message described in the earlier 802.11 (TM) p amendment is now described in section 'Frame formats', and the operation outside the context of a BSS described in section 'MLME').

In document 802.11-2016, anything qualified specifically as "OCBActivated", or "outside the context of a basic service set" is actually referring to OCB aspects introduced to 802.11. Note that in earlier 802.11p documents the term "OCBEnabled" was used instead of the current "OCBActivated".

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 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.

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 WiFi and Ethernet layers do (802.11a/b/g/n and 802.3). A packet sent by an OBU may be received by one or multiple 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 possible in 802.11-OCB 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 to the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, 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 the fixed infrastructure an explicit FCC autorization is required; for an onboard device a 'licensed-by-rule' concept applies: rule certification conformity is required); however technical conditions are different than those of the bands "2.4GHz" or "5GHz". On one hand, 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. On the other hand, 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).

- Prohibition of IPv6 on some channels relevant for IEEE 802.11-OCB, as opposed to IPv6 not being prohibited on any channel on which 802.11a/b/g/n runs:

  * Some channels are reserved for safety communications; the IPv6 packets should not be sent on these channels.

  * At the time of writing, the prohibition is explicit at higher layer protocols providing services to the application; these higher layer protocols are specified in IEEE 1609 documents, i.e. the "WAVE" stack.

  * National or regional specifications and regulations specify the use of different channels; these regulations must be followed.

- '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 Section 6. A relevant function is described in IEEE 1609.3-2016 [IEEE-1609.3], clause 5.5.1 and IEEE 1609.4-2016 [IEEE-1609.4], clause 6.7.

Other aspects particular to 802.11-OCB, which are also particular to 802.11 (e.g. the 'hidden node' operation), may have an influence on the use of transmission of IPv6 packets on 802.11-OCB networks. The OCB subnet structure is described in section Section 5.6.

5. Layering of IPv6 over 802.11-OCB as over Ethernet

5.1. Maximum Transmission Unit (MTU)

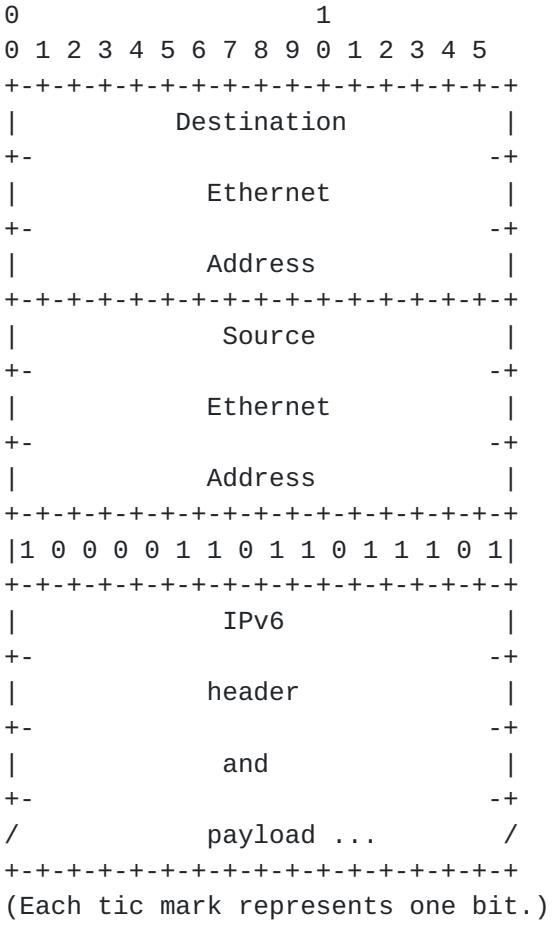
The default MTU for IP packets on 802.11-OCB is 1500 octets. It is the same value as IPv6 packets on Ethernet links, as specified in [RFC2464]. This value of the MTU respects the recommendation that every link in the Internet must have a minimum MTU of 1280 octets (stated in [RFC8200], and the recommendations therein, especially with respect to fragmentation). If IPv6 packets of size larger than 1500 bytes are sent on an 802.11-OCB interface card then the IP stack will fragment. In case there are IP fragments, the field "Sequence number" of the 802.11 Data header containing the IP fragment field is increased.

Non-IP packets such as WAVE Short Message Protocol (WSMP) can be delivered on 802.11-OCB links. Specifications of these packets are out of scope of this document, and do not impose any limit on the MTU size, allowing an arbitrary number of 'containers'. Non-IP packets such as ETSI GeoNetworking packets have an MTU of 1492 bytes. The operation of IPv6 over GeoNetworking is specified at [ETSI-IPv6-GeoNetworking].

5.2. Frame Format

IP packets are transmitted over 802.11-OCB as standard Ethernet packets. As with all 802.11 frames, an Ethernet adaptation layer is used with 802.11-OCB as well. This Ethernet Adaptation Layer performing 802.11-to-Ethernet is described in Section 5.2.1. The Ethernet Type code (EtherType) for IPv6 is 0x86DD (hexadecimal 86DD, or otherwise #86DD).

The Frame format for transmitting IPv6 on 802.11-OCB networks is the same as transmitting IPv6 on Ethernet networks, and is described in section 3 of [RFC2464]. The frame format for transmitting IPv6 packets over Ethernet is illustrated below:



(Each tic mark represents one bit.)

Ethernet II Fields:

Destination Ethernet Address
the MAC destination address.

Source Ethernet Address
the MAC source address.

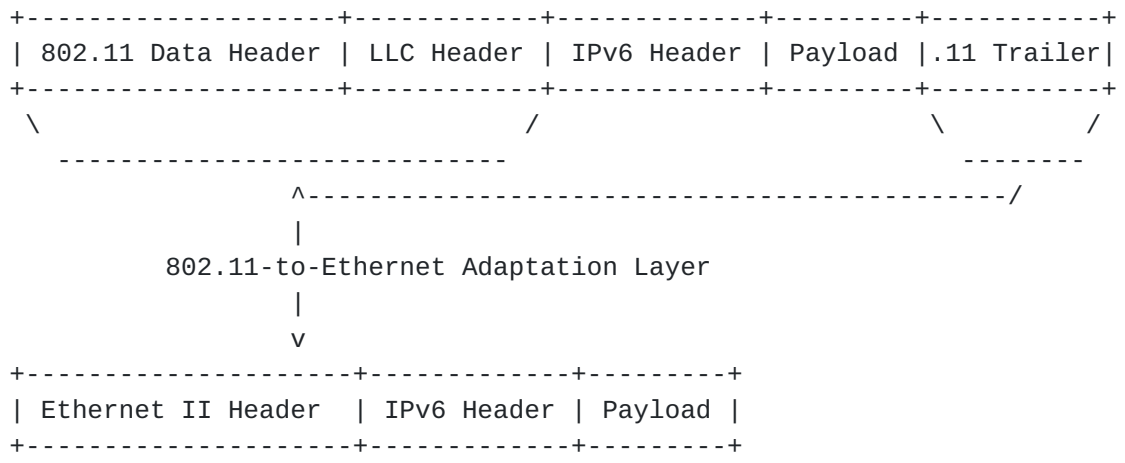
1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 1
binary representation of the EtherType value 0x86DD.

IPv6 header and payload
the IPv6 packet containing IPv6 header and payload.

5.2.1. Ethernet Adaptation Layer

In general, 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. For example, an 802.15.4 adaptation layer may perform fragmentation and reassembly operations on a MAC whose maximum Packet Data Unit size is smaller than the minimum MTU recognized by the IPv6 Networking layer. Other examples involve link-layer address transformation, packet header insertion/removal, and so on.

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 Data Header and the Logical-Link Layer Control Header and produces an Ethernet II Header. At sending, the reverse operation is performed.



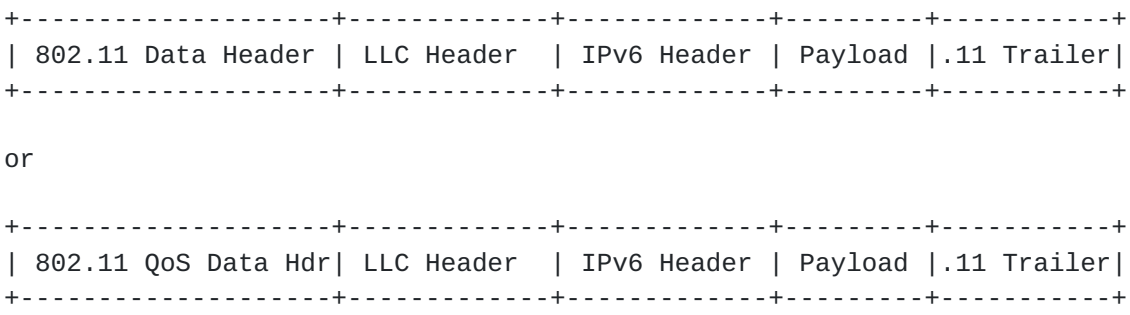
The Receiver and Transmitter Address fields in the 802.11 Data Header contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header is the same as the value of the Type field in the Ethernet II Header.

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

The Ethernet Adaptation Layer performs operations in relation to IP fragmentation and MTU. One of these operations is briefly described in section Section 5.1.

In OCB mode, IPv6 packets can be transmitted either as "IEEE 802.11 Data" or alternatively as "IEEE 802.11 QoS Data", as illustrated in

the figure below. Some commercial OCB products use 802.11 Data, and others 802.11 QoS data. In the future, both could be used.



The distinction between the two formats is given by the value of the field "Type/Subtype". The value of the field "Type/Subtype" in the 802.11 Data header is 0x0020. The value of the field "Type/Subtype" in the 802.11 QoS header is 0x0028.

The mapping between qos-related fields in the IPv6 header (e.g. "Traffic Class", "Flow label") and fields in the "802.11 QoS Data Header" (e.g. "QoS Control") are not specified in this document. Guidance for a potential mapping is provided in [I-D.ietf-tsvwg-ieee-802-11], although it is not specific to OCB mode.

5.3. Link-Local Addresses

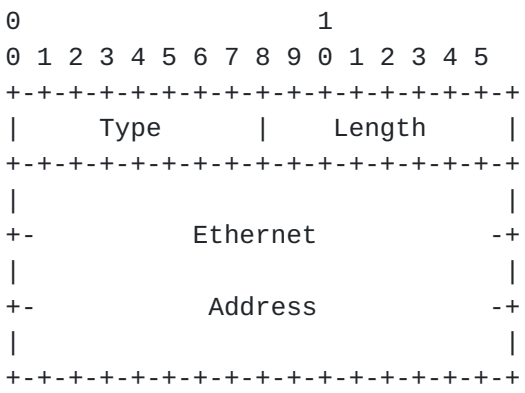
The link-local address of an 802.11-OCB interface is formed in the same manner as on an Ethernet interface. This manner is described in section 5 of [RFC2464]. Additionally, if stable identifiers are needed, it is recommended to follow the Recommendation on Stable IPv6 Interface Identifiers [RFC8064]. Additionally, 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].

5.4. Address Mapping

For unicast as for multicast, there is no change from the unicast and multicast address mapping format of Ethernet interfaces, as defined by sections 6 and 7 of [RFC2464].

5.4.1. Address Mapping -- Unicast

The procedure for mapping IPv6 unicast addresses into Ethernet link-layer addresses is described in [RFC4861]. The Source/Target Link-layer Address option has the following form when the link-layer is Ethernet.



Option fields:

Type
1 for Source Link-layer address.
2 for Target Link-layer address.

Length
1 (in units of 8 octets).

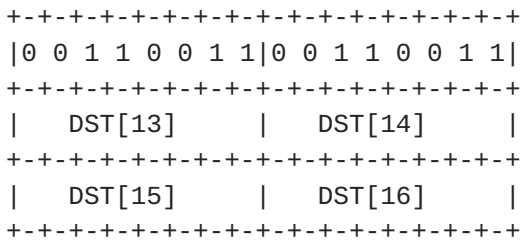
Ethernet Address
The 48 bit Ethernet IEEE 802 address, in canonical bit order.

5.4.2. Address Mapping -- Multicast

IPv6 protocols often make use of IPv6 multicast addresses in the destination field of IPv6 headers. For example, an ICMPv6 link-scoped Neighbor Advertisement is sent to the IPv6 address ff02::1 denoted "all-nodes" address. When transmitting these packets on 802.11-OCB links it is necessary to map the IPv6 address to a MAC address.

The same mapping requirement applies to the link-scoped multicast addresses of other IPv6 protocols as well. In DHCPv6, the "All_DHCP_Servers" IPv6 multicast address ff02::1:2, and in OSPF the "All_SPF_Routers" IPv6 multicast address ff02::5, need to be mapped on a multicast MAC address.

An IPv6 packet with a multicast destination address DST, consisting of the sixteen octets DST[1] through DST[16], is transmitted to the IEEE 802.11-OCB MAC multicast address whose first two octets are the value 0x3333 and whose last four octets are the last four octets of DST.



A Group ID named TBD, of length 112bits is requested to IANA; this Group ID signifies "All 80211OCB Interfaces Address". Only the least 32 significant bits of this "All 80211OCB Interfaces Address" will be mapped to and from a MAC multicast address.

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.

5.5. Stateless Autoconfiguration

The Interface Identifier for an 802.11-OCB interface is formed using the same rules as the Interface Identifier for an Ethernet interface; this is described in section 4 of [RFC2464]. No changes are needed, but some care must be taken when considering the use of the SLAAC procedure.

The bits in the 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].

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 On-Board Unit 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; see the privacy considerations described in Appendix C.

If stable Interface Identifiers are needed in order to form IPv6 addresses on 802.11-OCB links, it is recommended to follow the recommendation in [RFC8064]. Additionally, 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].

5.6. Subnet Structure

A subnet is formed by the external 802.11-OCB interfaces of vehicles that are in close range (not their on-board interfaces). This ephemeral subnet structure is strongly influenced by the mobility of vehicles: the 802.11 hidden node effects appear. On another hand, the structure of the internal subnets in each car is relatively stable.

For routing purposes, a prefix exchange mechanism could be needed between neighboring vehicles.

The 802.11 networks in OCB mode may be considered as 'ad-hoc' networks. The addressing model for such networks is described in [RFC5889].

An addressing model involves several types of addresses, like Globally-unique Addresses (GUA), Link-Local Addresses (LL) and Unique Local Addresses (ULA). The subnet structure in 'ad-hoc' networks may have characteristics that lead to difficulty of using GUAs derived from a received prefix, but the LL addresses may be easier to use since the prefix is constant.

6. 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.

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.

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].

As with all Ethernet and 802.11 interface identifiers, there may exist privacy risks in the use of 802.11-OCB interface identifiers. Moreover, in outdoors vehicular settings, the privacy risks are more important than in indoors settings. New risks are induced by the possibility of attacker sniffers deployed along routes which listen for 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. This may help mitigate privacy risks to a certain level. On another hand, it may have an impact in the way typical IPv6 address auto-configuration is performed for vehicles (SLAAC would rely on MAC addresses amd would hence dynamically change the affected IP address), in the way the IPv6 Privacy addresses were used, and other effects.

7. IANA Considerations

A Group ID named TBD, of length 112bits is requested to IANA; this Group ID signifies "All 80211OCB Interfaces Address".

8. Contributors

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.

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

10. References

10.1. Normative References

[I-D.ietf-tsvwg-ieee-802-11] Szigeti, T., Henry, J., and F. Baker, "Diffserv to IEEE 802.11 Mapping", draft-ietf-tsvwg-ieee-802-11-07 (work in progress), September 2017.

[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>.

[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>.

[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>.

[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>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <https://www.rfc-editor.org/info/rfc4429>.

[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>.

[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>.

[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>.

10.2. Informative References

[ETSI-IPv6-GeoNetworking]
"ETSI EN 302 636-6-1 v1.2.1 (2014-05), ETSI, European Standard, Intelligent Transportation Systems (ITS); Vehicular Communications; Geonetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over Geonetworking Protocols. Downloaded on September 9th, 2017, freely available from ETSI website at URL http://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf".

[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. Dowloaded 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.jeong-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-jeong-ipwave-vehicular-networking-survey-03 (work in progress), June 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.

[I-D.petrescu-its-scenarios-reqs]
Petrescu, A., Janneteau, C., Boc, M., and W. Klaudel, "Scenarios and Requirements for IP in Intelligent Transportation Systems", draft-petrescu-its-scenarios-reqs-03 (work in progress), October 2013.

[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.

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. 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 chip 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 chip must support the half-rate mode (the internal clock should be able to be divided by two).

- 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 regulatory domains rules, if used by the kernel to enforce local specific restrictions. Such modifications must respect the location-specific laws.

  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 C. 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.

C.1. Vehicle ID

In automotive networks it is required that each node is represented uniquely. Accordingly, a vehicle must be identified by at least one unique identifier. The current specification at ETSI and at IEEE 1609 identifies a vehicle by its MAC address, which is obtained from the 802.11-OCB Network Interface Card (NIC).

In case multiple 802.11-OCB NICs are present in one car, implicitely multiple vehicle IDs will be generated. Additionally, some software generates a random MAC address each time the computer boots; this constitutes an additional difficulty.

A mechanim to uniquely identify a vehicle irrespectively to the multiplicity of NICs, or frequent MAC address generation, is necessary.

C.2. Reliability Requirements

This section may need to be moved out into a separate requirements document.

The dynamically changing topology, short connectivity, mobile transmitter and receivers, different antenna heights, and many-to-many communication types, make IEEE 802.11-OCB links significantly different from other IEEE 802.11 links. Any IPv6 mechanism operating on IEEE 802.11-OCB link MUST support strong link asymmetry, spatio-temporal link quality, fast address resolution and transmission.

IEEE 802.11-OCB strongly differs from other 802.11 systems to operate outside of the context of a Basic Service Set. This means in practice that IEEE 802.11-OCB does not rely on a Base Station for all Basic Service Set management. In particular, IEEE 802.11-OCB SHALL NOT use beacons. Any IPv6 mechanism requiring L2 services from IEEE 802.11 beacons MUST support an alternative service.

Channel scanning being disabled, IPv6 over IEEE 802.11-OCB MUST implement a mechanism for transmitter and receiver to converge to a common channel.

Authentication not being possible, IPv6 over IEEE 802.11-OCB MUST implement an distributed mechanism to authenticate transmitters and receivers without the support of a DHCP server.

Time synchronization not being available, IPv6 over IEEE 802.11-OCB MUST implement a higher layer mechanism for time synchronization between transmitters and receivers without the support of a NTP server.

The IEEE 802.11-OCB link being asymmetric, IPv6 over IEEE 802.11-OCB MUST disable management mechanisms requesting acknowledgements or replies.

The IEEE 802.11-OCB link having a short duration time, IPv6 over IEEE 802.11-OCB SHOULD implement fast IPv6 mobility management mechanisms.

C.3. Multiple interfaces

There are considerations for 2 or more IEEE 802.11-OCB interface cards per vehicle. For each vehicle taking part in road traffic, one IEEE 802.11-OCB interface card could be fully allocated for Non IP safety-critical communication. Any other IEEE 802.11-OCB may be used for other type of traffic.

The mode of operation of these other wireless interfaces is not clearly defined yet. One possibility is to consider each card as an independent network interface, with a specific MAC Address and a set of IPv6 addresses. Another possibility is to consider the set of these wireless interfaces as a single network interface (not including the IEEE 802.11-OCB interface used by Non IP safety critical communications). This will require specific logic to ensure, for example, that packets meant for a vehicle in front are actually sent by the radio in the front, or that multiple copies of the same packet received by multiple interfaces are treated as a single packet. Treating each wireless interface as a separate network interface pushes such issues to the application layer.

Certain privacy requirements imply that if these multiple interfaces are represented by many network interface, a single renumbering event SHALL cause renumbering of all these interfaces. If one MAC changed and another stayed constant, external observers would be able to correlate old and new values, and the privacy benefits of randomization would be lost.

The privacy requirements of Non IP safety-critical communications imply that if a change of pseudonyme occurs, renumbering of all other interfaces SHALL also occur.

C.4. MAC Address Generation

When designing the IPv6 over 802.11-OCB address mapping, we will assume that the MAC Addresses will change during well defined "renumbering events". The 48 bits randomized MAC addresses will have the following characteristics:

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

The way to meet the randomization requirements is to retain 46 bits from the output of a strong hash function, such as SHA256, taking as 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.

Appendix D. 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:

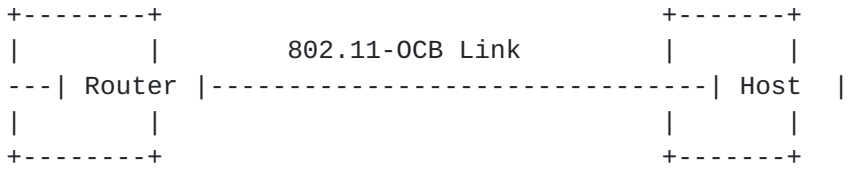
- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;
- The STA may send data frames of subtype Data, Null, QoS Data, and QoS Null.

Appendix E. Implementation Status

This section describese 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 this experiment, 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.



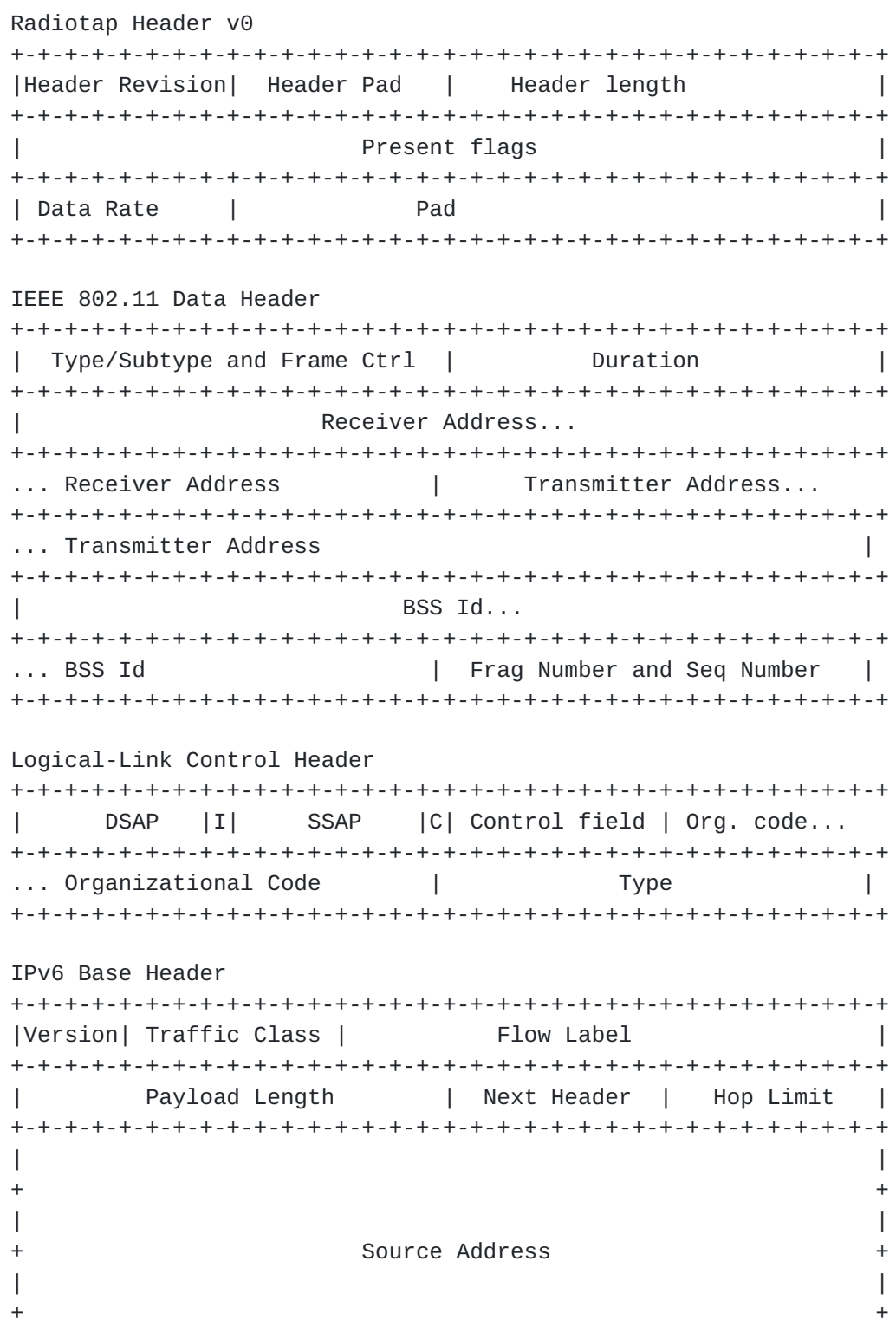
During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

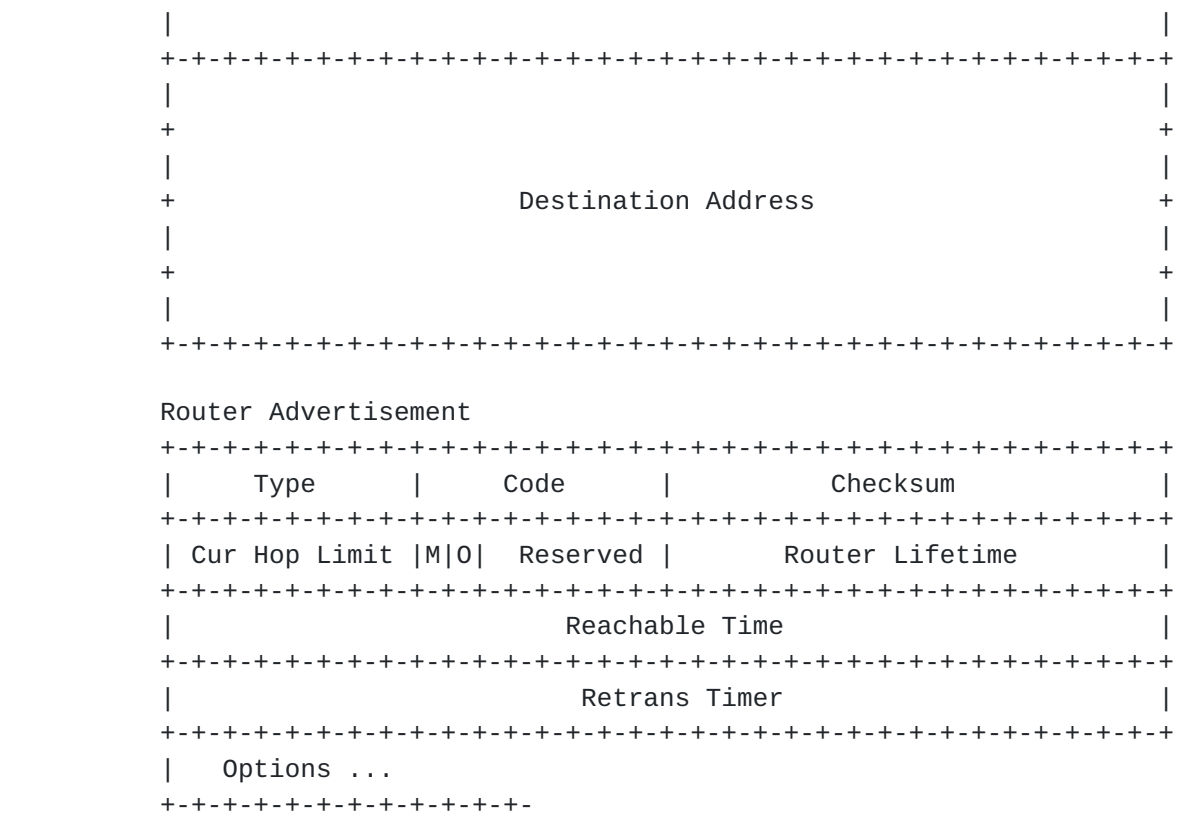
Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

E.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. Recent versions of network protocol analyzers (e.g.

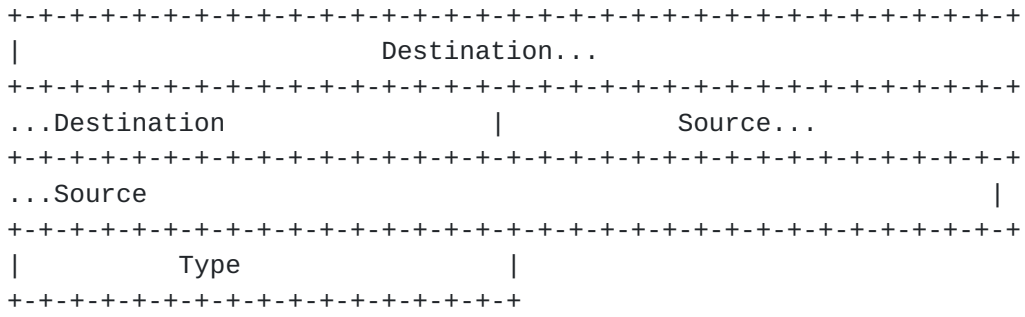
Wireshark) provide additional informations for an IP address, if a geolocalization database is present. In this example, the geolocalization database is absent, and the "GeoIP" information is set to unknown for both source and destination addresses (although the IPv6 source and destination addresses are set to useful values). This "GeoIP" can be a useful information to look up the city, country, AS number, and other information for an IP address.

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.

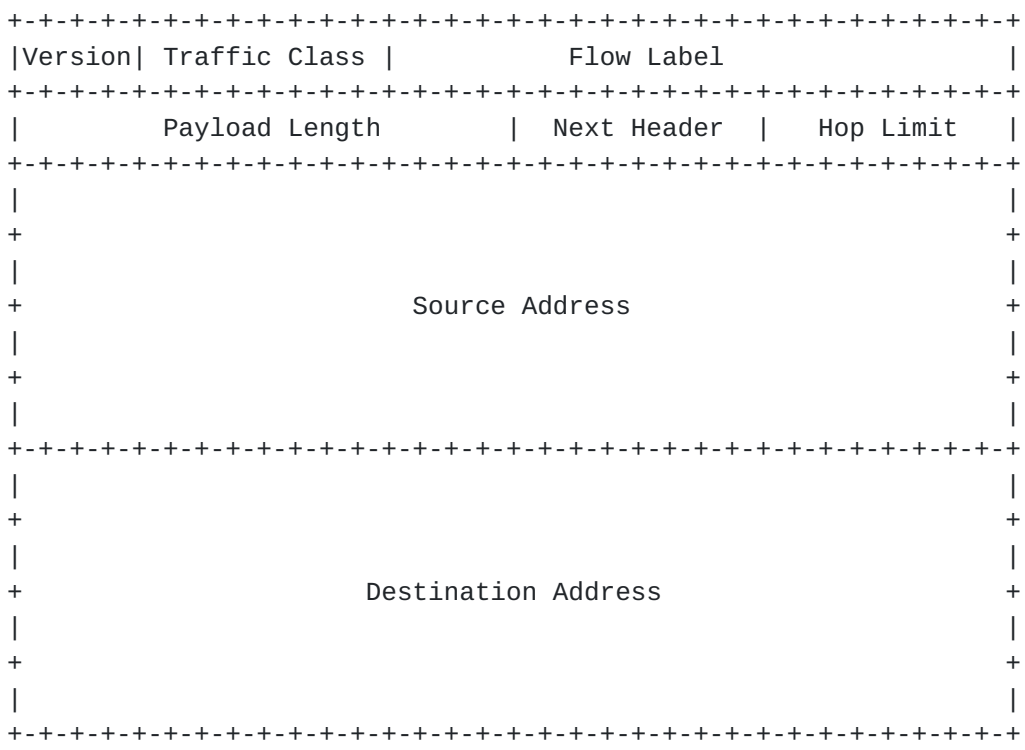
E.2. Capture in Normal Mode

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

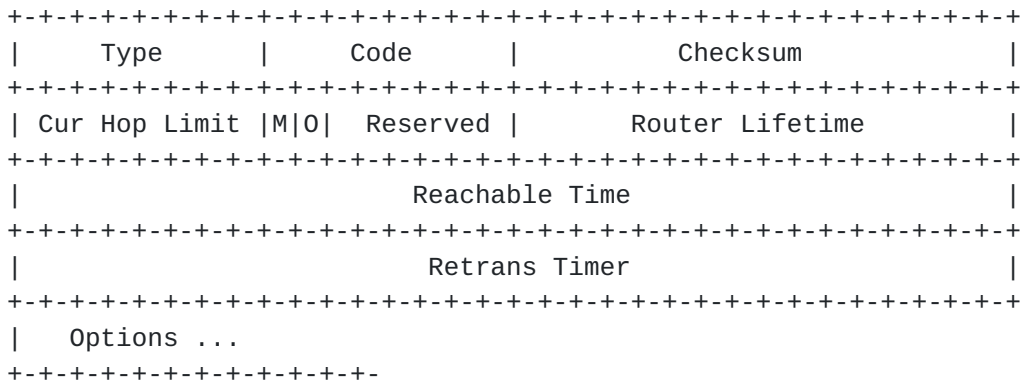
Ethernet II Header



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.

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: benamar73@gmail.com

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

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

Christian Huitema
Private Octopus Inc.
Friday Harbor, WA 98250
U.S.A.

Email: huitema@huitema.net

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

Tony Li
Peloton Technology
1060 La Avenida St.
Mountain View, California 94043
United States

Phone: +16503957356
Email: tony.li@tony.li