Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 24, 2014

A. Petrescu
CEA
R. Kuntz
IP Flavors
P. Pfister
changing
N. Benamar
Moulay Ismail University

October 21, 2013

Transmission of IPv6 Packets over IEEE 802.11p Networks
draft-petrescu-ipv6-over-80211p-00.txt

Abstract

In order to transmit IPv6 packets on IEEE 802.11p networks there is a need to define a few parameters such as the recommended Maximum Transmission Unit size, the header format preceding the IPv6 base header, the Type value within it, and others. This document describes these parameters for IPv6 and IEEE 802.11p networks; it portrays the layering of IPv6 on 802.11p similarly to other known 802.11 and Ethernet layers, by using an existing Ethernet Adaptation Layer.

In addition, the document attempts to list what is different in 802.11p compared to more 'traditional' 802.11a/b/g/n layers, layers over which IPv6 protocols run ok. Most notably, the operation outside the context of a BSS (OCB) has impact on IPv6 handover behaviour and on IPv6 security.

An example of an IPv6 packet captured while transmitted over an IEEE 802.11p link is given.

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 http://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 April 24, 2014.

Copyright Notice

Copyright (c) 2013 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 (http://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.

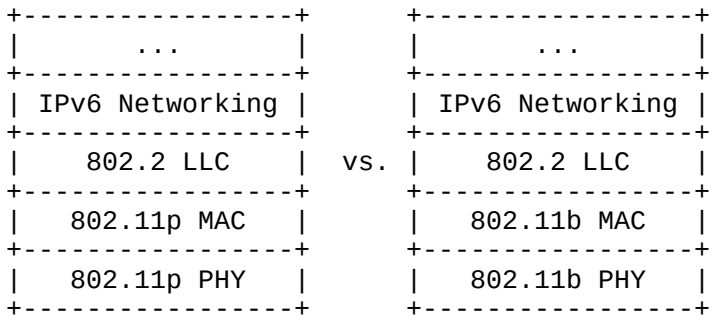
Table of Contents

1. Introduction 4
2. Terminology 5
3. Communication Scenarios where IEEE 802.11p Links are Used . . 6
4. Aspects introduced by 802.11p to 802.11 6
5. Layering of IPv6 over 802.11p as over Ethernet 9
5.1. Maximum Transmission Unit (MTU) 9
5.2. Frame Format 9
5.2.1. Ethernet Adaptation Layer 10
5.3. Link-Local Addresses 11
5.4. Address Mapping 11
5.5. Stateless Autoconfiguration 11
5.6. Subnet Structure 12
6. Handovers between OCB links 13
7. Example IPv6 Packet captured over a IEEE 802.11p link 15
7.1. Capture in Monitor Mode 15
7.2. Capture in Normal Mode 18
8. Security Considerations 20
9. IANA Considerations 21
10. Acknowledgements 21
11. References 21
11.1. Normative References 21
11.2. Informative References 22
Appendix A. ChangeLog 24
Appendix B. Explicit Prohibition of IPv6 on Channels Related to ITS Scenarios using 802.11p Networks - an Analysis 24
Appendix C. Changes Needed on a software driver 802.11a to become a 802.11p driver 25
Authors' Addresses 26

1. Introduction

This document describes the transmission of IPv6 packets on IEEE 802.11p networks. This involves the layering of IPv6 networking on top of the IEEE 802.11p MAC layer (with an LLC layer). Compared to running IPv6 over the Ethernet MAC layer, or over other 802.11 links, there is no modification required to the standards: IPv6 works fine directly over 802.11p too (with an LLC layer).

As an overview, we illustrate how an IPv6 stack runs over 802.11p by layering different protocols on top of each other. The IPv6 Networking is layered on top of the IEEE 802.2 Logical-Link Control (LLC) layer; this is itself layered on top of the 802.11p MAC; this layering illustration is similar to that of running IPv6 over 802.2 LLC over the 802.11 MAC, or over Ethernet MAC.



But, there are several deployment considerations to optimize the performances of running IPv6 over 802.11p (e.g. in the case of handovers between 802.11p Access Points, or the consideration of using the IP security layer).

We briefly introduce the vehicular communication scenarios where IEEE 802.11p links are used. This is followed by a description of differences in specification terms, between 802.11p and 802.11a/b/g/n (and the same differences expressed in terms of requirements to software implementation are listed in Appendix C.)

The document then concentrates on the parameters of layering IPv6 over 802.11p as over Ethernet: MTU, Frame Format, Interface Identifier, Address Mapping, State-less Address Auto-configuration. The values of these parameters are precisely the same as IPv6 over Ethernet [RFC2464]: the recommended value of MTU to be 1500 octets, the Frame Format containing the Type 0x86DD, the rules for forming an

Interface Identifier, the Address Mapping mechanism and the Stateless Address Auto-Configuration.

As an example, these characteristics of layering IPv6 straight over LLC over 802.11p MAC are illustrated by dissecting an IPv6 packet captured over a 802.11p link; this is described in the section titled "Example of IPv6 Packet captured over an IEEE 802.11p link".

A few points can be considered as different, although they do not seem required in order to have a working implementation of IPv6-over-802.11p. These points are consequences of the OCB operation which is particular to 802.11p (Outside the Context of a BSS). The handovers between OCB links need specific behaviour for IP Router Advertisements, or otherwise 802.11p's Time Advertisement, or of 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' ; second, the IP security should be considered of utmost importance, since OCB means that 802.11p is stripped of all 802.11 link-layer security; a small additional security aspect which is shared between 802.11p and other 802.11 links is the privacy concerns related to the address formation mechanisms. These two points (OCB handovers and security) are described each in a section of its own: OCB handovers in Section 6 and security in Section 8.

In the published literature, the operation of IPv6 for WAVE (Wireless Access In Vehicular Environments) was described in [ipv6-wave].

In standards, the operation of IPv6 as a 'data plane' over 802.11p is specified in [ieeep1609.3-D9-2010]. For example, it mentions that "Networking services also specifies the use of the Internet protocol IPv6, and supports transport protocols such as UDP and TCP. [...] A Networking Services implementation shall support either IPv6 or WSMP or both." and "IP traffic is sent and received through the LLC sublayer as specified in [...]". Also, the operation of IPv6 over a GeoNetworking layer and over G5 is described in [etsi-302663-v1.2.1p-2013].

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].

RSU stands for Road Side Unit.

3. Communication Scenarios where IEEE 802.11p Links are Used

The IEEE 802.11p 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.

4. Aspects introduced by 802.11p to 802.11

The link 802.11p is specified in IEEE Std 802.11p(TM)-2010 [ieee802.11p-2010] as an amendment to the 802.11 specifications, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, these 802.11p amendments have been included in IEEE 802.11(TM)-2012 [ieee802.11-2012], 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. 802.11p's Time Advertisement message is described in section 'Frame formats', and the operation outside the context of a BSS described in section 'MLME').

In order to delineate the aspects introduced by 802.11p to 802.11, we refer to the earlier [ieee802.11p-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. Whereas '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 802.11p 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 802.11p MAC layer offers practically the same interface to IP as the WiFi and Ethernet layers do (802.11a/b/g/n and 802.3).

To support this similarity statement (IPv6 is layered on top of LLC on top of 802.11p similarly as on top of LLC on top of 802.11a/b/g/n, and as on top of LLC on top of 802.3) it is useful to analyze the 802.11p differences compared to non-p 802.11 specifications. Whereas

the 802.11p amendment specifies relatively complex and numerous changes to the MAC layer (and very little to the PHY layer), we note here only a few characteristics which may be important for an implementation transmitting IPv6 packets on 802.11p links.

In the list below, the only 802.11p fundamental points which influence IPv6 are the OCB operation and the 12Mbit/s maximum which may be afforded by the IPv6 applications.

- Operation Outside the Context of a BSS (OCB): the 802.11p links are operated without a Basic Service Set (BSS). This means that the messages Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always ff:ff:ff:ff:ff:ff (48 '1' bits, or 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 - has potentially strong impact on the use of protocol Mobile IPv6 and protocols for IP layer security.

- Timing Advertisement: is a new message defined in 802.11p, 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. At the date of writing, an experienced reviewer considers that currently no field testing has used this message. Another implementor considers this feature implemented in an initial manner. In the future, it is speculated that this message may be useful for very simple devices which may not have their own hardware source of time (Galileo, GPS, cellular network), or by vehicular devices situated in areas not covered by such network (in tunnels, underground, outdoors but shaded by foliage or buildings, in remote areas, etc.)

- 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 802.11p, 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". This band is "5.9GHz" which is different than the bands "2.4GHz" or "5GHz" used for the Wireless LAN. But, as with Wireless LAN, the operation of 802.11p 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

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 802.11p (in Europe), compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to maximum distance of approximately 1km, compared to approximately 50m. On another 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).

- Explicit prohibition of IPv6 on some channels relevant for the PHY of IEEE 802.11p, as opposed to IPv6 not being prohibited on any channel on which 802.11a/b/g/n runs; for example, IPv6 is prohibited on the 'Control Channel' (number 178 at FCC, and 180 at ETSI); for a detailed analysis of FCC and ETSI prohibition of IP in particular channels see Appendix B.

- '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. The standard IEEE 802.11p uses OFDM encoding at PHY, as other non-b 802.11 variants do. This considers 20MHz encoding to be 'full-rate' encoding, as the earlier 20MHz encoding which is used extensively by 802.11b. In addition to the full-rate encoding, the OFDM rates also involve 5MHz and 10MHz. The 10MHz encoding is named 'half-rate'. The encoding dictates the bandwidth and latency characteristics that can be afforded by the higher-layer applications of IP communications. The half-rate means that each symbol takes twice the time to be transmitted; for this to work, all 802.11 software timer values are doubled. With this, in certain channels of the "5.9GHz" band, a maximum bandwidth of 12Mbit/s is possible, whereas in other "5.9GHz" channels a minimal bandwidth of 1Mbit/s may be used. It is worth mentioning the half-rate encoding is an optional feature characteristic of OFDM PHY (compared to 802.11b's full-rate 20MHz), used by 802.11a before 802.11p used it. In addition to the half-rate (10MHz) used by 802.11p in some channels, some other 802.11p channels may use full-rate (20MHz) or quarter-rate(?) (5MHz) encoding instead.

Other aspects particular to 802.11p 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 802.11p networks. The subnet structure which may assumed in 802.11p networks is strongly influenced by the mobility of vehicles.

5. Layering of IPv6 over 802.11p as over Ethernet

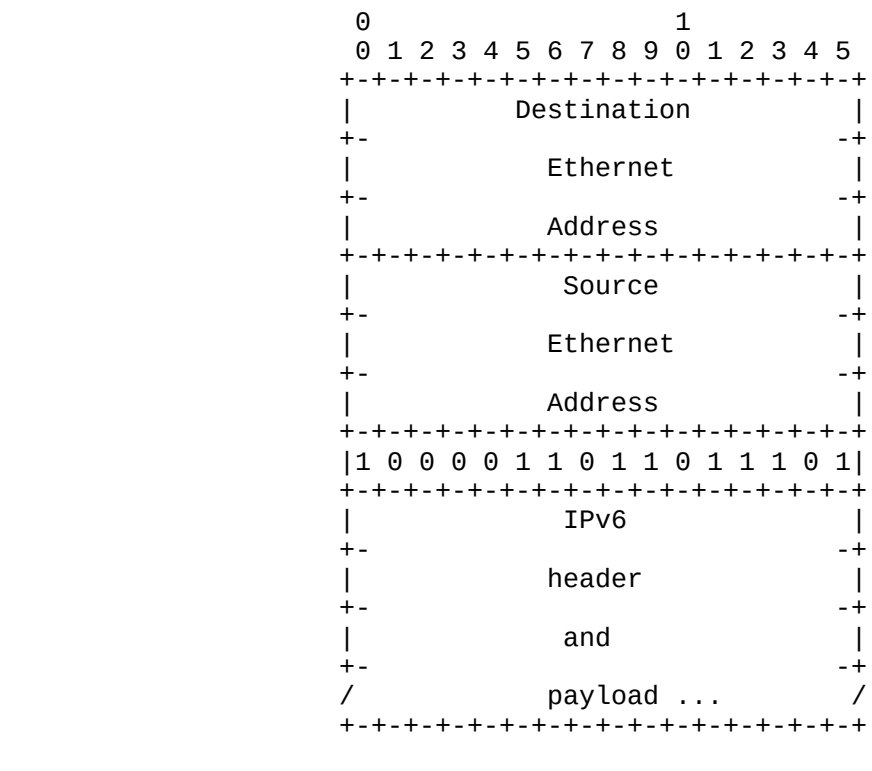
5.1. Maximum Transmission Unit (MTU)

The default MTU for IPv6 packets on 802.11p 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 [RFC2460], and the recommendations therein, especially with respect to fragmentation).

5.2. Frame Format

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

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

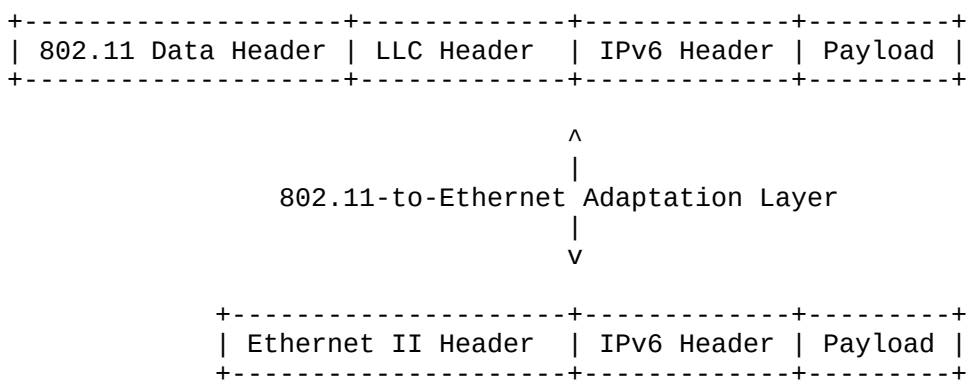


(Each tic mark represents one bit.)

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 other fields in the Data and LLC Headers are not used by the IPv6 stack.

5.3. Link-Local Addresses

The link-local address of an 802.11p interface is formed in the same manner as on an Ethernet interface. This manner is described in section 5 of [RFC2464].

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].

(however, there is discussion about geography, networking and IPv6 multicast addresses: geographical dissemination of IPv6 data over 802.11p may be useful in traffic jams, for example).

5.5. Stateless Autoconfiguration

The Interface Identifier for an 802.11p 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.

For example, the Interface Identifier for an 802.11p interface whose built-in address is, in hexadecimal:

30-14-4A-D9-F9-6C

would be

32-14-4A-FF-FE-D9-F9-6C.

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 802.11p interface are significant, as this is a IEEE link-layer address. The details of this significance are described in [I-D.ietf-6man-ug].

As with all Ethernet and 802.11 interface identifiers, the identifier of an 802.11p interface may involve privacy risks. A vehicle embarking an On-Board Unit whose egress interface is 802.11p may expose itself to eavesdropping and subsequent correlation of data; this may reveal data considered private by the vehicle owner. The address generation mechanism should consider these aspects, as described in [I-D.ietf-6man-ipv6-address-generation-privacy].

5.6. Subnet Structure

In this section the subnet structure may be described: the addressing model (are multi-link subnets considered?), address resolution, multicast handling, packet forwarding between IP subnets. Alternatively, this section may be spinned off into a separate documents.

The 802.11p networks, much like other 802.11 networks, may be considered as 'ad-hoc' networks. The addressing model for such networks is described in [RFC5889].

The SLAAC procedure makes the assumption that if a packet is retransmitted a fixed number of times (typically 3, but it is link dependent), any connected host receives the packet with high probability. On ad-hoc links (when 802.11p is operated in OCB mode, the link can be considered as 'ad-hoc'), both the hidden terminal problem and mobility-range considerations make this assumption incorrect. Therefore, SLAAC should not be used when address collisions can induce critical errors in upper layers.

Some aspects of multi-hop ad-hoc wireless communications which are relevant to the use of 802.11p (e.g. the 'hidden' node) are described in [I-D.baccelli-multi-hop-wireless-communication].

6. Handovers between OCB links

A station operating IEEE 802.11p in the 5.9 GHz band in US or EU is required to send data frames outside the context of a BSS. In this case, the station does not utilize the IEEE 802.11 authentication, association, or data confidentiality services. This avoids the latency associated with establishing a BSS and is particularly suited to communications between mobile stations or between a mobile station and a fixed one playing the role of the default router (e.g. a fixed Road-Side Unit a.k.a RSU acting as an infrastructure router).

The process of movement detection is described in section 11.5.1 of [RFC6275]. In the context of 802.11p deployments, detecting movements between two adjacent RSUs becomes harder for the moving stations: they cannot rely on Layer-2 triggers (such as L2 association/de-association phases) to detect when they leave the vicinity of an RSU and move within coverage of another RSU. In such case, the movement detection algorithms require other triggers. We detail below the potential other indications that can be used by a moving station in order to detect handovers between OCB ("Outside the Context of a BSS") links.

A movement detection mechanism may take advantage of positioning data (latitude and longitude).

Mobile IPv6 [RFC6275] specifies a new Router Advertisement option called the "Advertisement Interval Option". It can be used by an RSU to indicate the maximum interval between two consecutive unsolicited Router Advertisement messages sent by this RSU. With this option, a moving station can learn when it is supposed to receive the next RA from the same RSU. This can help movement detection: if the specified amount of time elapses without the moving station receiving any RA from that RSU, this means that the RA has been lost. It is up to the moving node to determine how many lost RAs from that RSU constitutes a handover trigger.

In addition to the Mobile IPv6 "Advertisement Interval Option", the Neighbor Unreachability Detection (NUD) [RFC4861] can be used to determine whether the RSU is still reachable or not. In this context, reachability confirmation would basically consist in receiving a Neighbor Advertisement message from a RSU, in response to a Neighbor Solicitation message sent by the moving station. The RSU should also configure a low Reachable Time value in its RA in order to ensure that a moving station does not assume an RSU to be reachable for too long.

The Mobile IPv6 "Advertisement Interval Option" as well as the NUD procedure only help knowing if the RSU is still reachable by the

moving station. It does not provide the moving station with information about other potential RSUs that might be in range. For this purpose, increasing the RA frequency could reduce the delay to discover the next RSU. The Neighbor Discovery protocol [RFC4861] limits the unsolicited multicast RA interval to a minimum of 3 seconds (the MinRtrAdvInterval variable). This value is too high for dense deployments of Access Routers deployed along fast roads. The protocol Mobile IPv6 [RFC6275] allows routers to send such RA more frequently, with a minimum possible of 0.03 seconds (the same MinRtrAdvInterval variable): this should be preferred to ensure a faster detection of the potential RSUs in range.

If multiple RSUs are in the vicinity of a moving station at the same time, the station may not be able to choose the "best" one (i.e. the one that would afford the moving station spending the longest time in its vicinity, in order to avoid too frequent handovers). In this case, it would be helpful to base the decision on the signal quality (e.g. the RSSI of the received RA provided by the radio driver). A better signal would probably offer a longer coverage. If, in terms of RA frequency, it is not possible to adopt the recommendations of protocol Mobile IPv6 (but only the Neighbor Discovery specification ones, for whatever reason), then another message than the RA could be emitted periodically by the Access Router (provided its specification allows to send it very often), in order to help the Host determine the signal quality. One such message may be the 802.11p's Time Advertisement, or higher layer messages such as the "Basic Safety Message" (in the US) or the "Cooperative Awareness Message " (in the EU), that are usually sent several times per second. Another alternative replacement for the IPv6 Router Advertisement may be the message 'WAVE Routing Advertisement' (WRA), which is part of the WAVE Service Advertisement and which may contain optionally the transmitter location; this message is described in section 8.2.5 of [ieeep1609.3-D9-2010].

Once the choice of the default router has been performed by the moving node, it can be interesting to use Optimistic DAD [RFC4429] in order to speed-up the address auto-configuration and ensure the fastest possible Layer-3 handover.

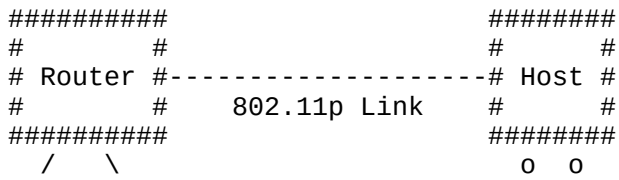
To summarize, efficient handovers between OCB links can be performed by using a combination of existing mechanisms. In order to improve the default router unreachability detection, the RSU and moving stations should use the Mobile IPv6 "Advertisement Interval Option" as well as rely on the NUD mechanism. In order to allow the moving station to detect potential default router faster, the RSU should also be able to be configured with a smaller minimum RA interval such as the one recommended by Mobile IPv6. When multiple RSUs are available at the same time, the moving station should perform the

handover decision based on the signal quality. Finally, optimistic DAD can be used to reduce the handover delay.

7. Example IPv6 Packet captured over a IEEE 802.11p link

We remind that a main goal of this document is to make the case that IPv6 works fine over 802.11p networks. Consequently, this section is an illustration of this concept and thus can help the implementer when it comes to running IPv6 over IEEE 802.11p. By way of example we show that there is no modification in the headers when transmitted over 802.11p networks - they are transmitted like any other 802.11 and Ethernet packets.

We describe an experiment of capturing an IPv6 packet captured on an 802.11p link. In this experiment, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11p 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 802.11p is outside the context of a BSSID.

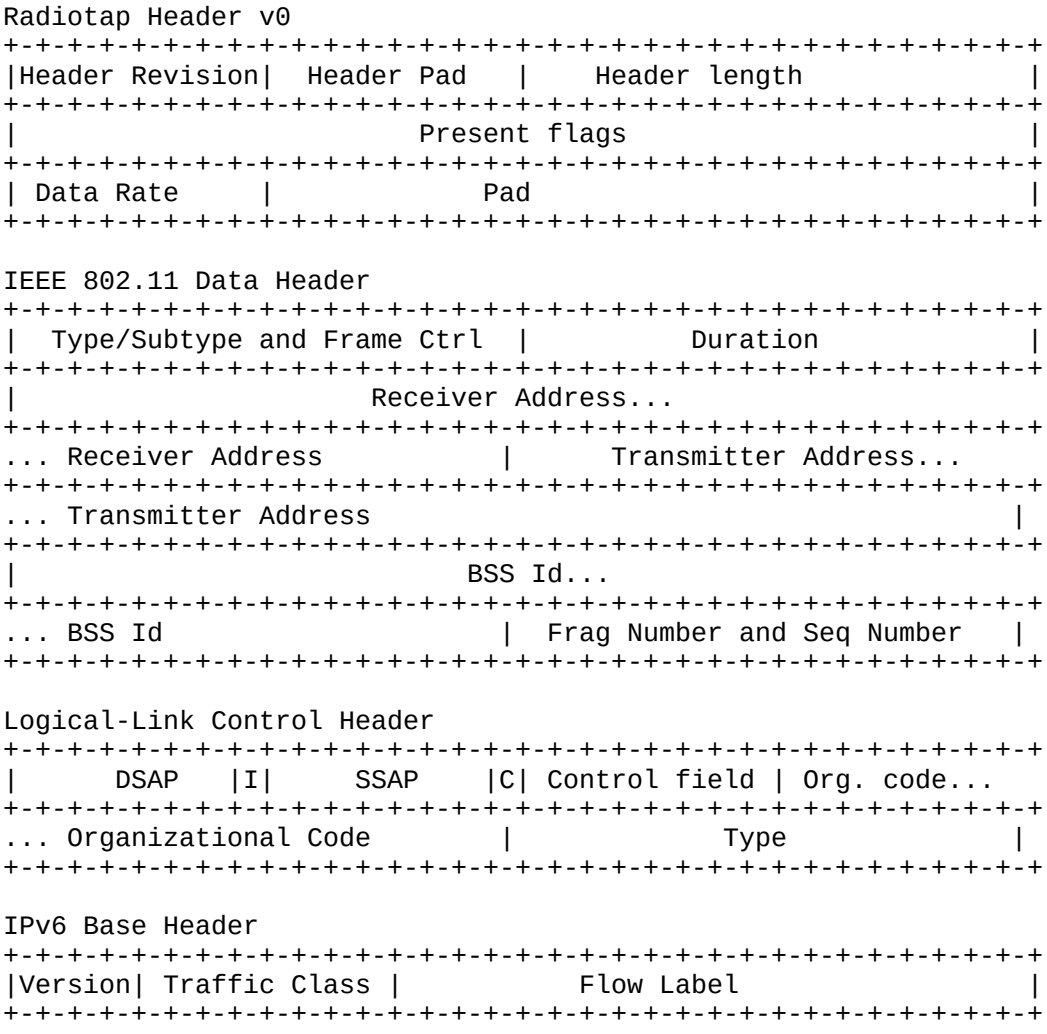
Overall, the captured message is precisely similar with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

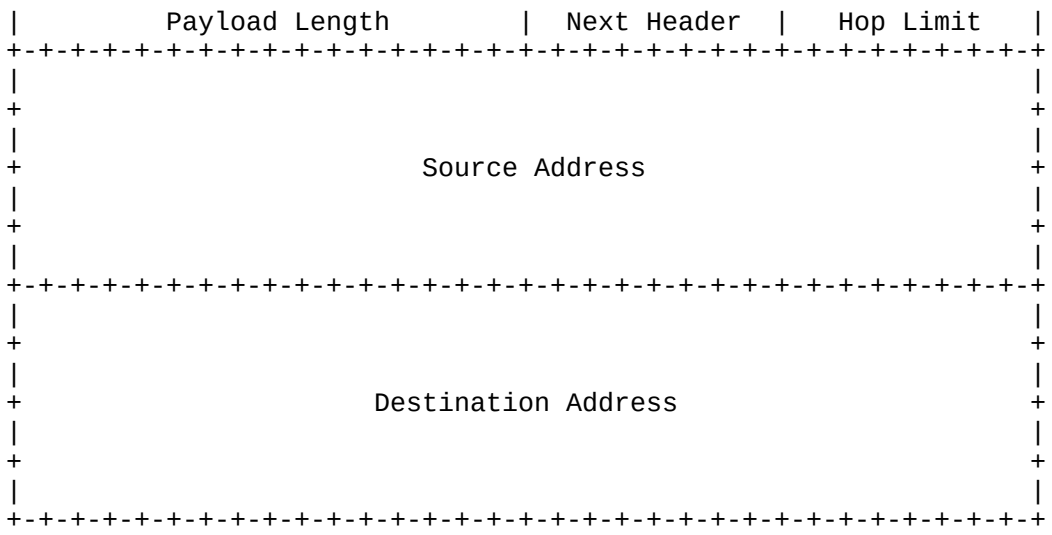
7.1. Capture in Monitor Mode

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

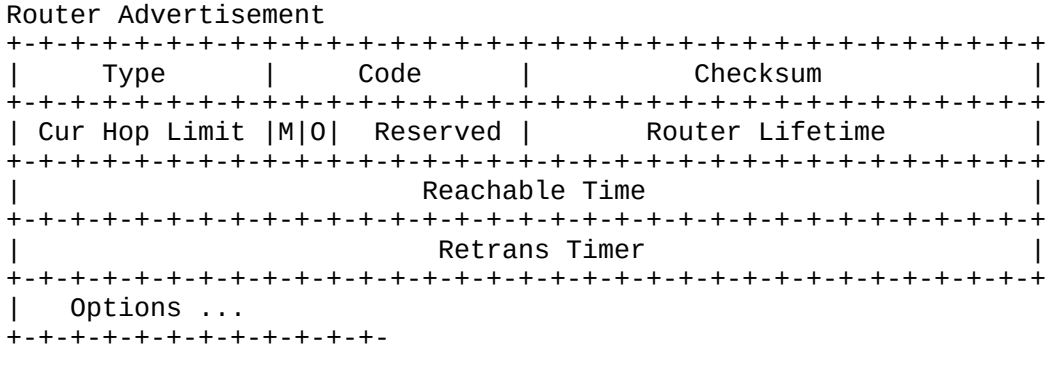
packet received from the network (the Radiotap Header is not present on the air). The implementation-dependent Radiotap Header is useful for piggybacking PHY information from the chip's registers as data in a packet understandable by userland applications using Socket interfaces (the PHY interface can 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.





Router Advertisement



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

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

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

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

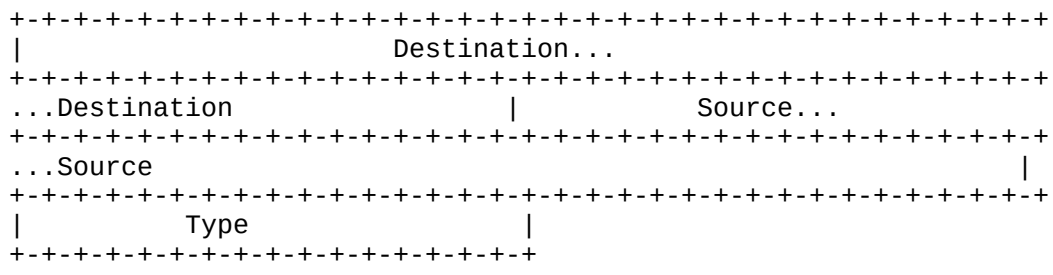
The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1. Recent versions of network protocol analyzers (e.g. Wireshark) provide additional informations for an IP address, if a geolocalization database is present. In 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 he 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 802.11p to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11p enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.

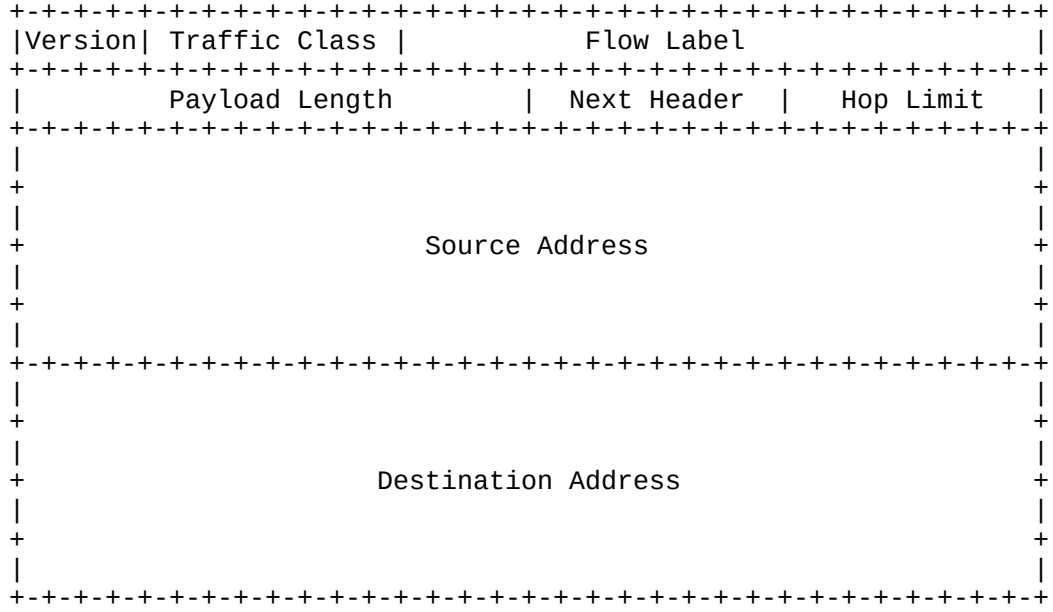
7.2. Capture in Normal Mode

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

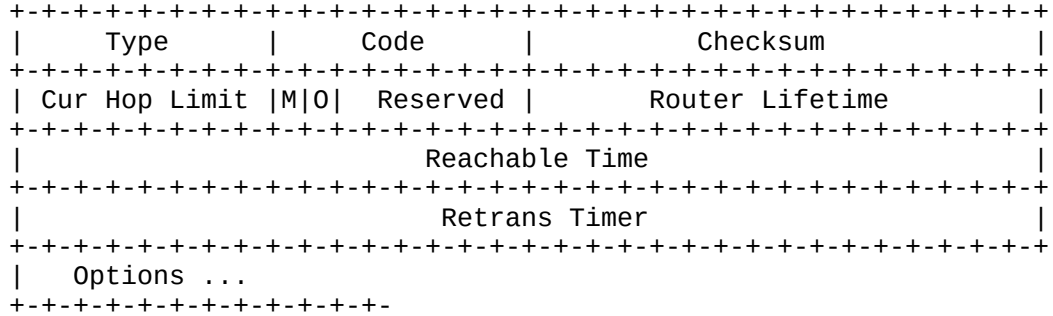
Ethernet II Header



IPv6 Base Header



Router Advertisement



One notices that the Radiotap Header is not prepended, and that the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On another 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.

It may be interpreted that an Adaptation layer is inserted in a pure IEEE 802.11 MAC packets in the air, before delivering to the applications. In detail, this adaptation layer may consist in elimination of the Radiotap, 802.11 and LLC headers and insertion of the Ethernet II header. In this way, it can be stated that IPv6 runs naturally straight over LLC over the 802.11p MAC layer, as shown by the use of the Type 0x86DD, and assuming an adaptation layer (adapting 802.11 LLC/MAC to Ethernet II header).

8. Security Considerations

802.11p 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 way less protected than commonly used links (wired link or protected 802.11).

At the IP layer, IPsec can be used to protect unicast communications, and SeND can be used for multicast communications. If no protection is used by the IP layer, upper layers should be protected. Otherwise, the end-user or system should be warned about the risks they run.

The WAVE protocol stack provides for strong security when using the WAVE Short Message Protocol and the WAVE Service Advertisement

[ieeep1609.2-D17].

As with all Ethernet and 802.11 interface identifiers, there may exist privacy risks in the use of 802.11p interface identifiers.

9. IANA Considerations

10. Acknowledgements

The authors would like to acknowledge Witold Klaudel, Ryuji Wakikawa, Emmanuel Baccelli, John Kenney, John Moring, Francois Simon, Dan Romascanu, Konstantin Khait and Ralph Droms. Their supportive comments at the early stages enlightened and helped improve the document. More comments from more persons are expected.

11. References

11.1. Normative References

[I-D.ietf-6man-ipv6-address-generation-privacy]
Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-00 (work in progress), October 2013.

[I-D.ietf-6man-ug]
Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", draft-ietf-6man-ug-04 (work in progress), October 2013.

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, April 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

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

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

11.2. Informative References

[I-D.baccelli-multi-hop-wireless-communication]
Baccelli, E. and C. Perkins, "Multi-hop Ad Hoc Wireless Communication", draft-baccelli-multi-hop-wireless-communication-06 (work in progress), July 2011.

[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.

[etsi-302663-v1.2.1p-2013]
"Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band, 2013-07, document en_302663v010201p.pdf, document freely available at URL ht tp://www.etsi.org/deliver/etsi_en/302600_302699/302663/ 01.02.01_60/en_302663v010201p.pdf downloaded on October 17th, 2013.".

[etsi-draft-102492-2-v1.1.1-2006]
"Electromagnetic compatibility and Radio spectrum Matters (ERM); Intelligent Transport Systems (ITS); Part 2: Technical characteristics for pan European harmonized communications equipment operating in the 5 GHz frequency range intended for road safety and traffic management, and for non-safety related ITS applications; System Reference Document, Draft ETSI TR 102 492-2 V1.1.1, 2006-07, document tr_10249202v010101p.pdf freely available at URL h ttp://www.etsi.org/deliver/etsi_tr/102400_102499/10249202/ 01.01.01_60/tr_10249202v010101p.pdf downloaded on October 18th, 2013.".

[fcc-cc] "Report and Order, Before the Federal Communications Commission Washington, D.C. 20554', FCC 03-324, Released on February 10, 2004, document FCC-03-324A1.pdf, document freely available at URL http://www.its.dot.gov/exit/fcc_edocs.htm downloaded on

October 17th, 2013.".

[ieee802.11-2012]
"802.11-2012 - 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. Downloaded on October 17th, 2013, from IEEE Standards, document freely available at URL http://standards.ieee.org/findstds/standard/802.11-2012.html retrieved on October 17th, 2013.".

[ieee802.11p-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.".

[ieeep1609.2-D17]
"IEEE P1609.2(tm)/D17 Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. pdf, length 2558 Kb. Restrictions apply.".

[ieeep1609.3-D9-2010]
"IEEE P1609.3(tm)/D9, Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, August 2010. Authorized licensed use limited to: CEA. Downloaded on June 19, 2013 at 07:32:34 UTC from IEEE Xplore. Restrictions apply, document at persistent link http://ieeexplore.ieee.org/servlet/opac?punumber=5562705".

[ieeep1609.4-D9-2010]
"IEEE P1609.4(tm)/D9 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation. Authorized licensed use limited to: CEA. Downloaded on June 19, 2013 at 07:34:48 UTC from IEEE Xplore. Restrictions apply. Document at persistent link http://ieeexplore.ieee.org/servlet/opac?punumber=5551097".

[ipv6-wave]
"Clausen, T., Baccelli, E. and R. Wakikawa, "IPv6

Operation for WAVE - Wireless Access in Vehicular Environments", Rapport de recherche, INRIA, numero 7383, September 2010.".

Appendix A. ChangeLog

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

From draft-authors-ipv6-over-80211p-00.txt to draft-authors-ipv6-over-80211p-00.txt:

- first version.

Appendix B. Explicit Prohibition of IPv6 on Channels Related to ITS Scenarios using 802.11p Networks - an Analysis

- IPv6 is prohibited on channel number 178 decimal, named 'Control Channel' at IEEE and FCC. The document [ieeep1609.4-D9-2010] prohibits upfront the use of IPv6 traffic on the Control Channel: 'data frames containing IP datagrams are only allowed on service channels'. The FCC names the Control Channel as being the channel number 178 decimal, and positions it with a 10MHz width from 5885MHz to 5895MHz [fcc-cc]. Other 'Service Channels' are allowed to use IP, but the Control Channel is not.

- The same channel number 178 decimal with 10MHz width (5885MHz to 5895MHz) is considered to be a Service Channel by ETSI and is named 'G5-SCH2' [etsi-302663-v1.2.1p-2013]. This channel is dedicated to 'ITS Road Safety'. Other channels are dedicated to 'ITS road traffic efficiency'. Also, a 'Control Channel G5-CCH' number 180 decimal (not 178) is reserved by ETSI to be 10MHz-width centered on 5900MHz. Compared to FCC, the ETSI makes no upfront statement with respect to IP and particular channels; yet it relates the 'In car Internet' applications ('When nearby a stationary public internet access point (hotspot), application can use standard IP services for applications.') to the 'Non-safety-related ITS application' [etsi-draft-102492-2-v1.1.1-2006]. This means ETSI may forbid IP on the 'ITS Road Safety' channels, but may allow IP on 'ITS road traffic efficiency' channels, or on other 5GHz channels re-used from BRAN (also dedicated to Broadband Radio Access Networks).

- At EU level in ETSI (but not some countries in EU with varying adoption levels) the highest power of transmission of 33 dBm is allowed, but only on two separate 10Mhz-width channels centered on

5900MHz and 5880MHz respectively. It appears IPv6 is not allowed on these channels (in the other 'ITS' channels where IP may be allowed, the levels vary between 20dBm, 23 dBm and 30 dBm; in some of these channels IP is allowed). A high-power of transmission means that vehicles may be distanced more (intuitively, for 33 dBm approximately 2km is possible, and for 20 dBm approximately 50meter).

Appendix C. Changes Needed on a software driver 802.11a to become a 802.11p 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 802.11p compliant:

- The chip must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11p layer, in France: 5875MHz to 5925MHz.
- The chip must support the half-rate mode (the internal clock can 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, etc...) 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.

Authors' Addresses

Alexandru Petrescu
CEA
http://www.cea.fr,

Phone:
Email: Alexandru.Petrescu@cea.fr

Romain Kuntz
IP Flavors
http://www.ipflavors.com,

Phone:
Email: r.kuntz@ipflavors.com

Pierre Pfister
changing

Phone:
Email: pierre.pfister@polytechnique.org

Nabil Benamar
Moulay Ismail University
Morocco

Phone:
Email: benamar73@gmail.com