

Transmission of IPv6 Packets
over IEEE 802.11 Networks in mode
Outside the Context of a Basic Service Set
(IPv6-over-80211ocb)

draft-ietf-ipwave-ipv6-over-80211ocb-02.txt

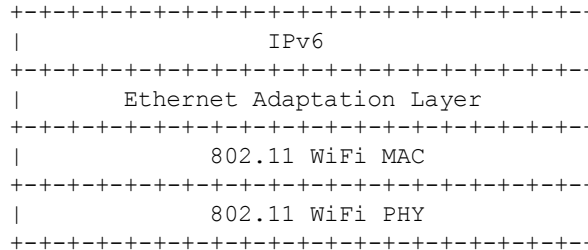
A. Petrescu (speaker),
N. Benamar, J. Härri, C. Huitema, J-H. Lee, T. Ernst, T. Li

IETF 98, Chicago, March 31st, 2017

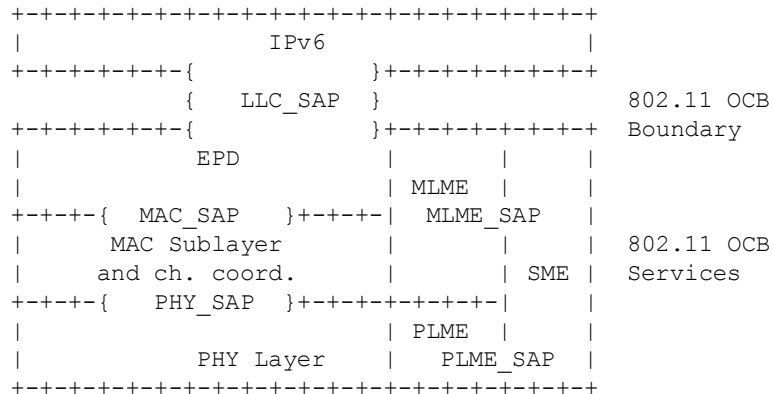

Contents

- Issues needing confirmation or resolution
- Issues solved


New figures



New illustration of
Ethernet Adaptation Layer



802.11 OCB
Boundary



New illustration of
interface between IPv6 and MAC
as seen at IEEE

Mention SNAP

- Proposal to add text:

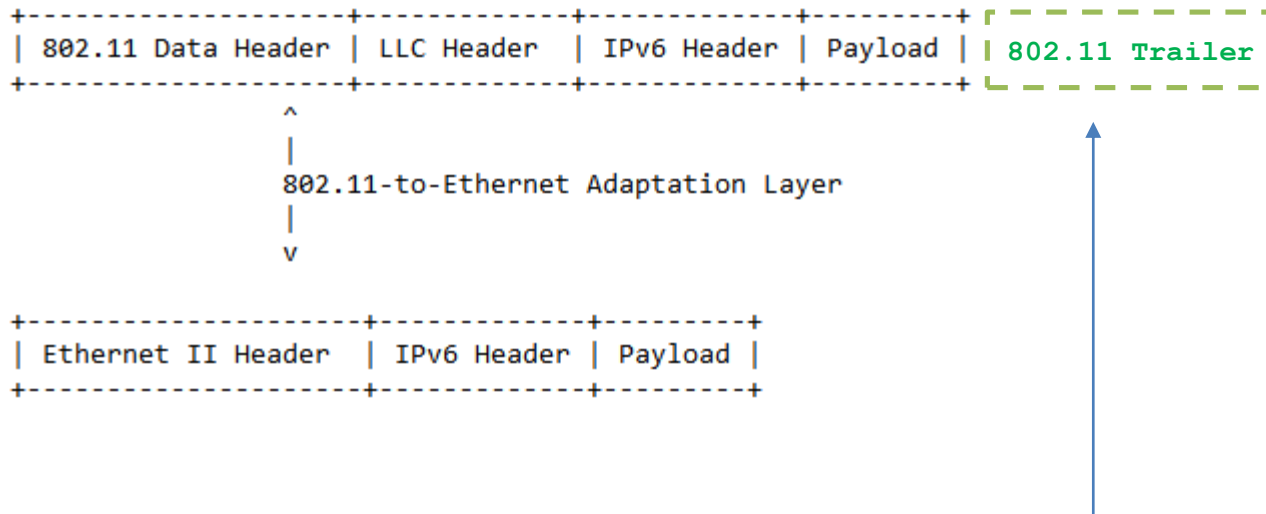
old:

- > The IPv6 network operates on 802.11 OCB [...] by involving an
- > Ethernet Adaptation Layer
- [...]
- > A more theoretical and detailed view of layer stacking, and
- > interfaces between the IP layer and 802.11 OCB layers [...] on top of
- > Ethernet Protocol Discrimination

new, add the following:

- > 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.

Ethernet Adaptation Layer



- Will add a trailer – Frame Check Sequence

Empty section

“Address Mapping -- Unicast”

- Should be same as section 6 "Address Mapping -- Unicast" of RFC 2464 → what's the status of 2464bis?

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

```

      0                               1
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |          Type          | Length |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |          Ethernet      |       |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |          Address       |       |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  
```

RFC 4861?

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. This is the address the interface currently responds to, and may be different from the built-in address used to derive the Interface Identifier.

Privacy?
 Formulation?

IPv6 prohibition status

- IPv6 on 802.11 OCB is prohibited at IEEE 1609
- IPv6 on 802.11 OCB is prohibited at ETSI?

Current text is:

- o Prohibition of IPv6 on some channels relevant for the PHY of IEEE 802.11-OCB, as opposed to IPv6 not being prohibited on any channel on which 802.11a/b/g/n runs; at the time of writing, this prohibition is explicit in IEEE 1609 documents.

“Road-Side Unit”

RSU: Road Side Unit. An IP router equipped with, or connected to, at least one interface that is 802.11 and that is an interface that operates in OCB mode.

- Other proposals:
 - RSR: Road-Side Router
 - RSR as component of RSU
 - R-ITS-S: Roadside ITS Station (an ISO/TC204 term), roadside ITS-S with an ITS-S access router

Multi-channel issues

- Multi-channel issues are not addressed in this document
- Write another document

What do you mean with multi-channel? OCB does not provide any multi-channel service. Higher-layer services do (IEEE WAVE or ETSI)...OCB only assume that the frequency to be used is 'known', so using OCB actually means knowing a set of channels where to send OCB-related packets...I am not sure if this could be called a multi-channel service...

Why does it need to address multi-channel service (where I assume by multi-channel, you really mean multi-CI or multi-radio ... if it's simple channel switching, then it's not really overly relevant ... though ... yes there are some deployment issues surroundly possible frequency planning, etc.)? Unless the IETF is thinking of addressing CI diversity (simultaneous transmissions of packets over multiple CIs) as a mechanism for robust handovers, I don't see why this is an issue.

Handovers

old:

However, 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).

new:

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 layer).

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.

And remove:

6. Handovers between OCB links



Write another document

TCLAS

- TCLAS mappings from/to IPv6 Traffic Class field → **write another document.**

"**traffic classification (TCLAS):** The specification of certain parameter values to identify a protocol data unit(#2222) (PDU) or a medium access control (MAC) service data unit (MSDU). The classification process is(#2223) performed above the MAC service access point (MAC SAP(#3409)), within the MLME, or within the MAC, based on the type of classification.(#78)"

The TCLAS element is used in WLAN admission control requests to indicate the mapping of DSCP or ToS to IEEE 802.11 priority.

That being said, I'm not sure what IEEE 802.11 frame would include a TCLAS element. As I said earlier, TCLAS elements are included in an Admission Control request (ADDTS frame). ADDTS frames are not currently specified for use with OCB.

I believe Mike already indicated that DSCP values in IPv6 DS fields could be mapped to 802.11 priorities, however it will be many-to-one as there are 64 possible DSCPs and only 8 UPs (user priorities) (and only 4 access categories) in 802.11.

The TCLAS element is used in WLAN admission control requests to indicate the mapping of DSCP or ToS to IEEE 802.11 priority.

[I-D.ietf-tsvwg-ieee-802-11]

Szigeti, T. and F. Baker, "DiffServ to IEEE 802.11 Mapping", [draft-ietf-tsvwg-ieee-802-11-01](#) (work in progress), November 2016.

Certificates

old text:

Similarly to Non IP safety-critical communications, IPv6 over 802.11-OCB packets must contain a certificate, including at least the public key of the sender, that will allow the receiver to authenticate the packet, and guarantee its legitimacy.

Removed.

Write another document

ETSI CAM and IP

- Initial proposal:

D.2. Non IP Communications

In IEEE 1609 and ETSI ITS, safety-related communications CANNOT be used with IP datagrams. For example, Basic Safety Message (BSM, an IEEE 1609 datagram) and Cooperative Awareness Message (CAM, an ETSI ITS-G5 datagram), are each transmitted as a payload that is preceded by link-layer headers, without an IP header.

I propose the following new text:

D.2. Non IP Communications

In IEEE 1609 and ETSI ITS, safety-related communications MAY NOT be used with IP datagrams. For example, Basic Safety Message (BSM, an IEEE 1609 datagram), are each transmitted as a payload that is preceded by link-layer headers, without an IP header.

(remark "MAY NOT" instead of CANNOT, and CAM absence).

- Second proposal:

- Removed appendix section "Non IP Communications".

Privacy (1 of 2)

The old text being commented is the following:

o In vehicular communications using 802.11p links, there are strong privacy concerns with respect to addressing. While the 802.11p 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 8.

The new text is:

[same] and in function addressed in IEEE 1609.3, clause 5.5.1 and IEEE 1609.4, clause 6.7.

Privacy (2 of 2)

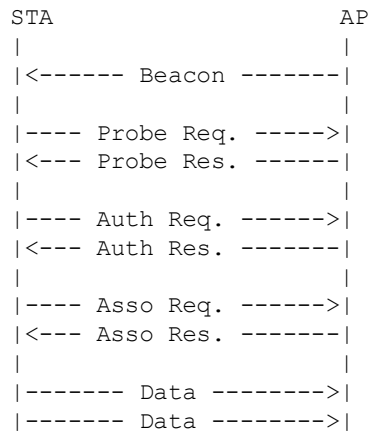
OLD:

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), 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.

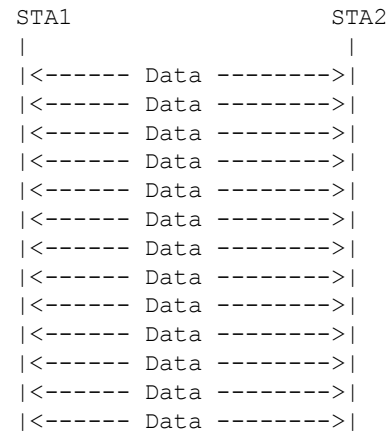
NEW:

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11-OCB interface may involve privacy 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 fo being tracked; see the privacy considerations described in [design-considerations](#).

New figures

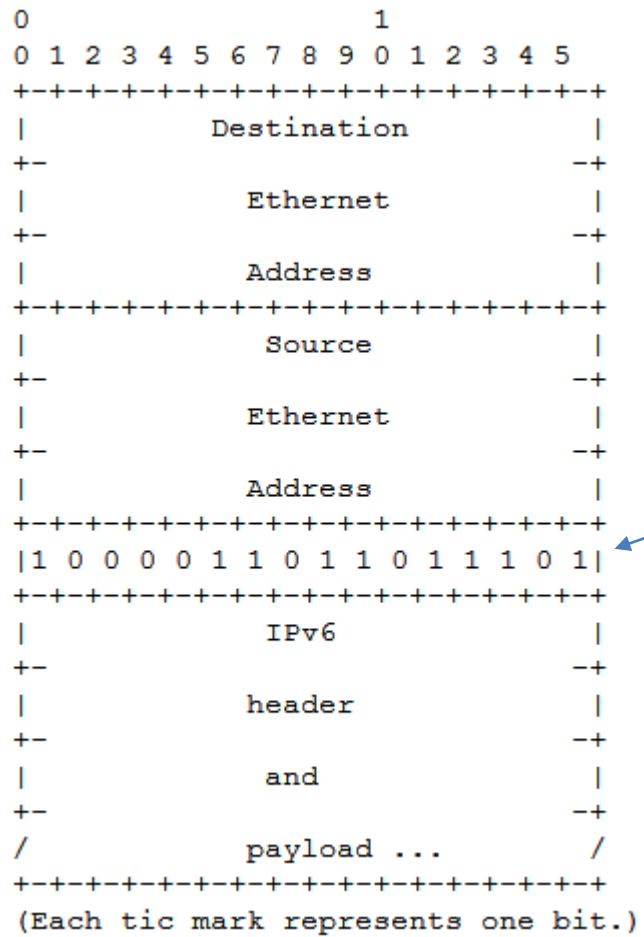


(a) Traditional IEEE 802.11



(b) IEEE 802.11 OCB mode

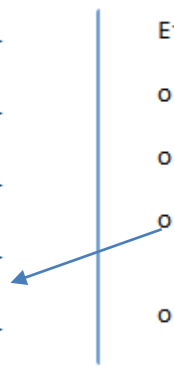
EtherType



- Added the following:

Ethernet II Fields:

- o Destination Ethernet Address: the MAC destination address.
- o Source Ethernet Address: the MAC source address.
- o "1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 1": binary representation of the EtherType value 0x86DD.
- o IPv6 header and payload: the IPv6 packet containing IPv6 header and payload.



802.11 OCB and Beacons

- Initial text “802.11-OCB does not use Beacons”
- Comments suggesting some beaconing was observed
- Explanation and agreement:
 - 802.11-OCB does not use IEEE Beacons

Multiple interfaces

old text:

D.6. Multiple interfaces

[...]

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.

new text:

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.

If Mobile IPv6 with NEMO extensions is used, then the MCoA RFC5648 technology is relevant for Mobile Routers with multiple interfaces, deployed in vehicles.