Updates on IPv6-Over-IEEE802.11-OCB draft

From version 44 to version 51

Nabil Benamar
IETF 105 Montréal
From -44 to -45

• Abstract

• OLD

• 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.

• New

• This document describes how IPv6 (including addressing and basic ND) can be used to communicate among nodes in range of one another over IEEE 802.11-OCB. Optimizations and usage of IPv6 over more complex scenarios is not covered and is subject of future work.
• Abstract (consise)

• This document provides methods and settings, and describes limitations, for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link with minimal change to existing stacks. Optimizations and usage of IPv6 over more complex scenarios is not covered and is subject of future work.
From -45 to -46

• Introduction (specifying the scope)

• OLD

• Compared to running IPv6 over the Ethernet MAC layer, there is no modification expected to IEEE Std 802.11 MAC and Logical Link sublayers: IPv6 works fine directly over 802.11-OCB too, with an LLC layer.
This document describes the layering of IPv6 networking on top of the IEEE Std 802.11 MAC layer or an IEEE Std 802.3 MAC layer with a frame translation underneath. The resulting stack operates over 802.11-OCB and provides at least P2P connectivity using IPv6 ND and link-local addresses. ND Extensions and IPWAVE optimizations for vehicular communications are not in scope. The expectation is that further specs will elaborate for more complex vehicular networking scenarios.
From -45 to -46

• New

• 5. Security Considerations

• The potential attack vectors are: MAC address spoofing, IP address and session hijacking, and privacy violation Section 5.1. A previous work at SAVI WG presents some threats [RFC6959], while SeND presented in [RFC3971] and [RFC3972] is a solution against address theft but it is complex and not deployed.
From -46 to -47

- Basic support for IPv6 over IEEE Std 802.11 Networks operating Outside the Context of a Basic Service Set (IPv6-over-80211-OCB) draft-ietf-ipwave-ipv6-over-80211ocb-47

- In the Introduction

- The resulting stack inherits from IPv6 over Ethernet [RFC 2464] and operates over 802.11-OCB providing at least P2P connectivity using IPv6 ND and link-local addresses.
Moreover, whether or not the interface identifier is derived from the EUI-64 identifier, its length is 64 bits as is the case for Ethernet [RFC2464].
From -47 to -48

• The draft was entirely proofread by Mohamed Boucadair

• And many corrections were made in -48
From -48 to -49

- Normative References Vs Informative
- typos
From -49 to -50

• We got 10 OK and 3 ‘Discuss’

• We reflected the comments received from the Ads

• We removed the following note.

• Note: compliance with standards and regulations set in different countries when using the 5.9GHz frequency band is required.

• No specific reason why this needs to be said here
From -49 to -50

• The mapping to the 802.11 data service **MUST** use a 'priority' value of 1, which specifies the use of QoS with a 'Background' user priority.

• The mapping to the 802.11 data service **SHOULD** use a 'priority' value of 1 (QoS with a 'Background' user priority), reserving higher priority values for safety-critical and time-sensitive traffic, including the ones listed in [ETSI-sec-archi].

• We also corrected the normative use of MAY/may and SHOULD/should in the text
We reformulated the text in Subnet structure (as pointed out by Roman) as follows:

- IPv6 Neighbor Discovery protocol (ND) requires reflexive properties (bidirectional connectivity) which is generally, though not always, the case for P2P OCB links. IPv6 ND also requires transitive properties for DAD and AR, so an IPv6 subnet can be mapped on an OCB network only if all nodes in the network share a single physical broadcast domain.
From -49 to -50

• We also reformulated the security section:

• 802.11-OCB does not provide any cryptographic protection, because it operates outside the context of a BSS (no Association Request/Response, no Challenge messages). Therefore, an attacker can sniff or inject traffic while within range of a vehicle or IP-RSU (by setting an interface card’s frequency to the proper range). Also, an attacker may not heed to legal limits for radio power and can use a very sensitive directional antenna; if attackers wish to attack a given exchange they do not necessarily need to be in close physical proximity. Hence, such a link is less protected than commonly used links (wired link or protected 802.11
Version 51

• Will include a modification of the section **Pseudonym Handling**

• To address the last comment of Roman Danyliw
Not the end