

# IPv6 Operation for WAVE - Wireless Access in Vehicular Environments

Thomas Clausen, Emmanuel Baccelli  
*Laboratoire d'Informatique (LIX), Ecole Polytechnique, France*  
Email: [Thomas@ThomasClausen.org](mailto:Thomas@ThomasClausen.org), [Emmanuel.Baccelli@inria.fr](mailto:Emmanuel.Baccelli@inria.fr)

Ryuji Wakikawa  
*Toyota-ITC, USA*  
Email: [ryuji@us.toyota-itc.com](mailto:ryuji@us.toyota-itc.com)

## Abstract—The Abstract

### I. INTRODUCTION

The IEEE is currently undertaking standardization of a protocol suite for *Wireless Access in Vehicular Environments* (WAVE), with the objective of providing vehicles and pedestrians with the ability to communicate with each other and with road-side infrastructure. Possible applications hereof include emergency warning systems, cooperative cruise control and collision warning, as well as toll and parking fee collection. This protocol suite is developed in the IEEE 1609 working group, documented in [1], [2], [3], [4], [5], [6] and intended for operation over *Dedicated Short-Range Communications* (DSRC) – a set of communications channels (frequency spectrum) dedicated for vehicular networking [?].

WAVE is providing communications services to applications, by way of promising support for two protocol stacks, the *Wave Short Message Protocol* (WSMP) and IPv6. While WSMP is developed within the IEEE 1609 family of standards [4], considerations for operation of IPv6 for WAVE are less developed. The WAVE architecture specification [1] makes reference to the IETF<sup>1</sup> specification of IPv6 [7] and makes minimal observations regarding the use of IPv6 addresses. The WAVE Networking Services specification [4] states that IPv6 Link Local, Global and Multicast addresses shall be supported as per [8], Link Local addresses shall be derived from MAC addresses as per [9], Global addresses shall be configured in a stateless fashion as per [10], using specific WAVE-advertised prefixes. No further specific recommendations as to IPv6 operation for WAVE are provided.

The authors of this paper assert that, while the IEEE 1609 family of specifications provides a set of necessary considerations for IPv6 operation over WAVE, these considerations are not sufficient for proper and correct IPv6 operation in this environment. To give but one example, [1] states that Link Local addresses “*can only be used within the scope of a single network, i.e., are not routable*” – this is true, however in a wireless environment such as provided by

WAVE, further considerations are required (*e.g.* uniqueness also beyond a single logical IP hop) for Link Local addresses to be useable.

This paper provides an analysis of IPv6 operation, as described in the IEEE 1609 family of specifications for WAVE networks, identifies where IPv6 operation for WAVE networks is underspecified, and presents a set of additional recommendations enabling proper IPv6 operation for WAVE networks.

#### A. Paper Overview

While IPv6, as defined in [7], principally concerns the data frame layout (header format, header extensibility, rules governing header construction and processing etc.), IPv6 operation implies operation of a set of basic protocols, including NDP [11], stateless address autoconfiguration [9] etc. These (and other) protocols make certain assumptions about properties of an underlying link model for their proper operation, and assume certain relationships between assigned IP addresses and communications ability across the underlying data link layer. This is discussed in further details in section II.

Section III describes the IPv6 considerations for for WAVE, as presented by the IEEE 1609 family of specifications. Section IV elaborates on the link-model, presented by a WAVE system; this link model has properties different from (and conflicting with) those assumed by IPv6, the consequences hereof are detailed in section V.

This paper is concluded in section VI.

### II. IPV6 OVERVIEW

Running IPv6 is generally understood to entail a number of different things, beyond that the IPv6 frame format [7] is used on the network layer. IPv6 employs a specific addressing model [10] with different address families (*e.g.*, Link Local or Global addresses), closely reflecting assumptions of a well-defined *link model*. This enables applications or protocol to have certain expectations of communication abilities, corresponding to the addresses they use. For example, an application using a Global address as destination address expects the network to be able to ensure multi-hop

<sup>1</sup><http://www.ietf.org>

communication to that destination address. The network, then, expects such addresses to be assigned in a way such that it by inspection of the address can determine if the destination is reachable directly, or reachable only via a (and, in that case also which) router. In an IPv6 network, the Neighbor Discovery Protocol for stateless autoconfiguration (of addresses, default routers etc) and duplicate address detection [11], [9], is assumed to be running – and that protocol expects the same *link model* and *addressing model*.

Thus, IPv6 operation entails (i) using the IPv6 frame format, (ii) certain assumptions of a well-defined *link-model*, reflected in an (iii) *address model*, and (iv) proper operation of NDP. This is detailed further in the following sections.

### A. IPv6 Link Assumptions

[12] points out that network protocols and applications are designed with specific assumptions of the nature of an IP link.

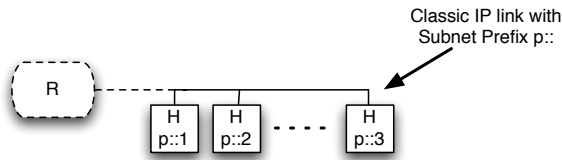


Figure 1. **Classic IP Link Model:** hosts (H) connected to the same link have assigned IP addresses from a common prefix, possibly assigned by a router (R).

Considering figure 1, these assumptions can be summarized as follows:

- all hosts (H) with network interfaces configured with addresses from within the same prefix  $p::$ , and with the same prefix  $p::$  assigned to the interfaces, can communicate directly with one another – *i.e.*:
  - IPv6 datagrams are not forwarded at the network layer when communicating between interfaces which are configured with addresses from within the same prefix; hence
  - hop-limit in IPv6 datagrams are not decremented when communicating between interfaces which are configured with addresses from within the same prefix, and;
  - multicast IPv6 datagrams with a hop-limit of 1 are (modulo data loss) delivered to all interfaces within the same subnet.
- link-local multicasts and broadcasts are received by all interfaces configured with addresses from within the same prefix without forwarding.

An even shorter summary of the “*classic IP link model*” is to say that “an IP link looks like an Ethernet”.

[@THC: Perhaps a “catch-phrase” similar to the paragraph terminating the “Wave air interface link model” section could be cooked up here?].

### B. IPv6 Addressing

As described in the above, the notion of “IP link” is tied with the notion of an subnet prefix (IPv6), in that all interfaces which are configured with the same subnet prefix are considered to be on the same IP link and thus that for communication between nodes on the same subnet, no forwarding is required and no decrement of TTL/hop-limit is performed.

In addition to this relationship between “link” and “prefix”, IPv6 introduces address scopes – Link-Local and Global – and mechanisms by which addresses are constructed using *Interface IDs*.

1) *Address Scopes and Uniqueness:* A Link-Local address is valid for communication with a device on the same “link”: an IPv6 datagram with a Link-Local source or destination address is not to be forwarded on the network layer, but is to be received by a destination on the same link – or not received at all. The only requirement for an unicast Link-Local address to be useful is, thus, that it is unique on the local link; the same Link-Local address may well be in use on another, disjoint, link, however as IPv6 datagrams with Link-Local addresses are never to be forwarded, no ambiguities exist.

A Global address is valid for communication beyond the local “link”: an IPv6 datagram with a Global source and destination address can be forwarded on the network layer and, thus, be received by a destination on the same or on a different link – or not received at all. For an unicast Global address to be useful, it must, thus, be unique across the entire network.

It is important that these address uniqueness requirements are universally satisfied. This is ensured in IPv6 by having an interface detect when it connects to a link (typically, by way of a discrete link-layer trigger), upon which it constructs a Link-Local IPv6 address by concatenating the Link-Local Prefix ( $FE80::/10$ ) with an *Interface ID*, typically derived from the MAC address of that interface. Duplicate Address Detection (DAD) [9] is then performed, to verify that this address is not already in use on the link. DAD employs Link-Local Multicast, interrogating (NS) all other interfaces on the link as to if they are already using that address. Absent a reply (NA) to this interrogation, the address is assumed unique on the link and henceforth used. As all Link-Local addresses share the same Prefix ( $FE80::/10$ ), this DAD procedure in reality verifies that the chosen *Interface ID* is unique across the link. An interface must also detect when it disconnects from a link (typically also by way of a discrete link-layer trigger), upon which it must cease to use the previously configured addresses.

Global addresses are constructed by concatenating the *Global prefix* of a link with the *Interface ID* of an interface, verified to be unique during the configuration procedure for Link-Local addresses. The *Global Prefix* is obtained from a

router on the link<sup>2</sup>, by way of Router Solicitation / Router Advertisement messages [11]. It follows that uniqueness of a Global address for an interface relies on (i) the *Interface ID* being unique on the link to which the interface is connected, and (ii) unique prefixes being delegated to routers. It follows, then, that a Global address is valid only as long as that interface is connected to the link on which the router providing the *Global prefix* is present.

[@THC: maybe the three key points should be summarized: "Topological correctness", "Scope" and "Unicity" ?]

[@THC: NDP-for-Neighbor Cache maintenance?]

### C. IPv6 "Link Model"

[@THC: this is a strawman tag-on, needs to be reworked, but wanted to make symmetric to the WAVE link stuff later].

To summarize the above, in IPv6 a "Link" describes a well-determined set of network interfaces, all able to communicate directly with each other without forwarding, and with all interfaces in a single (link-local multicast) transmission be able to reach all other interfaces on the same link. This set of network interfaces is maintained by way of explicit and discrete signals, allowing an interface to detect its membership of (association? connection? to) a given link.

IPv6 links can thus be described as "*Broadcast links with reflective, transitive neighborhoods and explicit discrete signals indicating an interfaces' membership of a link*", and proper operation of IPv6 assumes this in order to preserve e.g. address unicity.

## III. IPV6 CONSIDERATIONS IN THE WAVE SPECIFICATION

[@THC: Some introductory stuff is required here, limiting us to look at the "ad-hoc-characteristics" (typically, V2V? Maybe also V2RSU?) of the WAVE platform. This is mostly keywords / notes from reading through the specification]

As indicated in section I, the IEEE 1609 family of specifications present a minimal set of considerations for IPv6 operation. Specifically, the specifications state that:

- IPv6 is provided as a data plane protocol, and that the "standard IPv6 protocol" is used;
- IP configuration parameters (global prefixes, ...) are provided in the WAVE Routing Advertisement (WRA) messages;
- OBUs advertising services do so using Link-Local addresses, as OBUs provide services to direct (1-hop) neighbors only and therefore acquiring and maintaining [topologically correct] Global addresses is wasteful;
- RSUs are identified by either Link-Local or Global addresses;
- Link-Local addresses are derived by the device, are not globally unique and are not usable for routing;

<sup>2</sup>Global addresses are only relevant in case the network can provide multi-hop communication, i.e. a router is present on the link.

- NDP and RFC2461 [11], otherwise used for populating the neighbor cache, generates a substantial amount of traffic, and thus other means for populating the neighbor cache (ICMPv6, IPv6 PDUs) are employed;
- NDP is, however, not excluded for "cases where it might be needed".

The IEEE 1609 family of specifications also state that MAC address changes are supported (desired? frequent?) for pseudonymity-reasons.

UDP is expected to be the predominant transport protocol in use.

Unsure about security requirements for IPv6 ops; it is not clear if IPSec is expected/working in these environments, or if sufficient.

## IV. WAVE AIR INTERFACE "LINK MODEL"

The air interfaces of a WAVE system, and the "links" to which they attach, have different characteristics than those described in section II – this, the WAVE "link model" does not present a direct mapping to the IPv6 link model. These characteristics are briefly summarized in this section. As a point of reference, the WAVE air interface version of figure 1 looks as in figure 2.

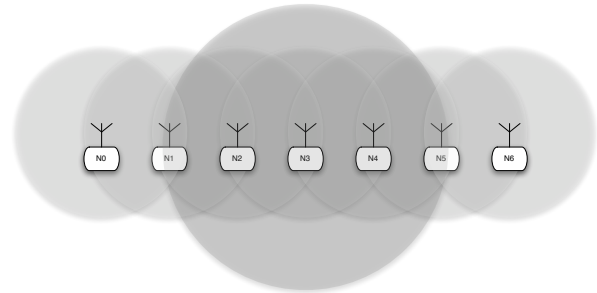


Figure 2. Nodes (N) with air interfaces. The light grey area indicates the **coverage area** of each air interface. The dark grey circle indicates the **interference area** of the air interface of N3.

Each air interface is a broadcast interface, able to establish a direct link layer communication with air interfaces which are within its coverage area. In figure 2, this coverage area is approximated by a simple disc of fixed radius (light gray discs)– in the real world, both the shape and size of the coverage area is variable as a function of the interface, interference from the environment etc. Referring to figure 2 if, for example, if N3 transmits, then this transmission may be received by N2 and N4, but not by N1 and N5. This implies that, e.g., N3 and N4 – despite being neighbors and on the same "link" – do not share the same view of which other nodes are neighbors and on the same "link": N3 considers that it is on the same "link" as N2 and N4, whereas N4 considers itself to be on the same "link" as N3 and N5.

An air interface has an "interference area" which may be greater than its coverage area, *i.e.* a transmission by N3 in figure 2 will, as indicated above, be correctly received by the interfaces N2 and N4. At the same time, however, this transmission may be propagating to interfaces of N1 and N5 where, while the transmission can not be correctly decoded, it can be detected, and cause interference with other transmissions which could otherwise be correctly received over the air interfaces of N1 and N5 (such as transmissions from N0 and N6).

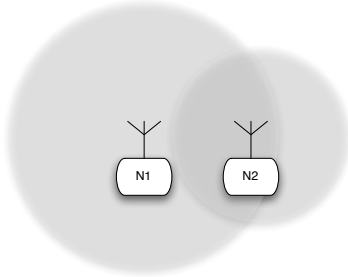


Figure 3. Neighbor asymmetry.

The IPv6 Link Model, in figure 1, axiomatically assumes that neighbor relationships are symmetric: if communication from air interface A to air interface B is possible in one hop, then communication in the inverse direction is also possible – in other words, connectivity between neighbor interfaces is assumed symmetric. Figure 3 illustrates a situation where, for some reason (powerful transmitter, environmental interference, large antenna, ...), the air interface of N1 has a large enough coverage area that its transmissions can be received and correctly decoded by the air interface N2. The air interface of N2, on the other hand, has a much smaller coverage radius, such that transmissions from the air interface of N2 can not be received and correctly decoded at the air interface of N1. Thus asymmetric – or more precisely, unidirectional – connectivity between the air interface of N1 and the air interface of N2 exists: N2 sees N1 as a neighbor (since the air interface N2 can receive transmissions from the air interface of N1), whereas N1 does not see N2 as a neighbor (since the air interface of N1 can not receive transmissions from the air interface of N2).

A vehicular network, naturally, represents a dynamic topology: OBUs move relative RSUs and to each other, thus the resulting network is a highly dynamic graph. Thus, the neighborhood of an air interface is also dynamic and varies over time – due to mobility, and due to changing environmental factors: two air interfaces which were not in communications range a moment ago may become neighbors, and vice-versa.

Thus, a set of air interfaces within a region – even if using the same channels and modulation – do not map directly to the IPv6 link model, as described in section II:

not all air interfaces may be able to communicate to all other air interfaces without intermediate relaying, a link-local multicast transmission from one air interface may not (even disregarding losses) be able to be received by all other air interfaces; indeed, a multicast transmission from one air interface may not be able to reach the same set of air interfaces as would a multicast transmission from its closest neighbor air interface (consider, for example, figure 2 where no two air interfaces can directly transmit to the same set of other air interfaces).

As the set of air interfaces "on a link" air interfaces are communicating via radio links rather than electrical wires, there are no implicit physical signals, allowing an air interface to detect its association or disassociation with a given set of other air interfaces "on the same link".

[@THC: To Verify: WAVE does not provide explicit signals for on/off link events. I have not found. Also, I was trying to find a way to phrase "this is just as well, considering that the other IPv6 link assumptions do not hold anyways", but failed here.... ].

This sometimes leads to describing the links to which such air interfaces connect as "time-varying, semi-broadcast links with time-varying, non-transitive, non-reflective neighbor relationships". Neighboring air interfaces may experience distinctly different neighborhoods, and may not even agree on if they are or are not neighbors.

[@THC: I have not been able to find authoritative information as to if the hidden terminal problem is or not accommodated in DSRC / 802.11p. My gut tells me that it's not...I am also not sure if it is relevant in this discussion, my gut tells me that it is also not)

#### V. FURTHER CONSIDERATIONS REQUIRED FOR IPv6-OVER-WAVE

[@THC: This Section is intentionally reverted to keywords/notes, as it is part of what I want to see reworked according to the "link separation" discussions that I folded in this morning, and what I had was a mess of the two in one section. Contemplating how much we should copy/cite MANETs and related document / new RFC....]

- Link Locals should be derived from unique token to become globally unique; can't know when two interfaces may become neighbors;
- NDP largely useless, possibly entirely useless? Consequences, *i.e.* DAD won't work (wouldn't anyways), other options in NDP messages (MobileIP?)
- /128 /32 – does that work for hosts? Probably it doesn't "officially"; is it required?
- Link bidirectionality check may (should) be required;
- Protocols using LL multicast assuming "session semantics" (*i.e.* issues a mcast, expect a reply such as NDP in NS "I want to use A, is A in range?") probably won't work, likely should not be used, services should likely be designed accordingly;

- change MAC - change LL (pseudonymity). Change LL - still globally unique? How to assign set of random, globally unique tokens? - Change global (yes) - session continuity? - ND cache out-of-date immediately?

## VI. CONCLUSION

### REFERENCES

- [1] I. The Wireless Access in Vehicular Environments (WAVE) Working Group of the Intelligent Transport Systems (ITS) Committee, "IEEE P1609.0/D0.1: Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Architecture," April 2010.
- [2] —, "IEEE P1609.1/D1.3: Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Remote Management Services," May 2010.
- [3] —, "IEEE P1609.2/D5: Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages," June 2010.
- [4] —, "IEEE P1609.3/D7.0: Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services," June 2010.
- [5] —, "IEEE P1609.4: Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation," June 2010.
- [6] I. The 802.11 Working Group, "IEEE 802.11: Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments," June 2010.
- [7] R. Hinden and S. Deering, "RFC2460: Internet Protocol, Version 6 (IPv6) Specification," December 1998, Standards Tracks RFC 2460.
- [8] —, "RFC2373: IP Version 6 Addressing Architecture," July 1998, Standards Tracks RFC 2373.
- [9] S. Thomson, T. Narten, and T. Jinmei, "RFC2462: IPv6 stateless address autoconfiguration," December 1998, Standards Tracks RFC 2462.
- [10] R. Hinden and S. Deering, "RFC3513: Internet Protocol Version 6 (IPv6) Addressing Architecture," April 2003, Standards Tracks RFC 3513.
- [11] T. Narten, E. Nordmark, and W. Simpson, "RFC2461: Neighbor Discovery for IP Version 6 (IPv6)," December 1998, Standards Tracks RFC 2461.
- [12] D. Thaler, "RFC4903: Multilink Subnet Issues," June 2007, Informational RFC 4903.