IETF®

IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases

(draft-ietf-ipwave-vehicular-networking-04)

IETF 102, Montreal

July 16, 2018

Jaehoon (Paul) Jeong [Editor], Nabil Benamar, Sandra Cespedes, Jerome Haerri, Dapeng Liu, Tae (Tom) Oh, Charles E. Perkins, Alexandre Petrescu, Yiwen (Chris) Shen, and Michelle Wetterwald

Update from -02 and -03 Versions

- This document (-04) is updated from
  - draft-ietf-ipwave-vehicular-networking-02
  - draft-ietf-ipwave-vehicular-networking-03

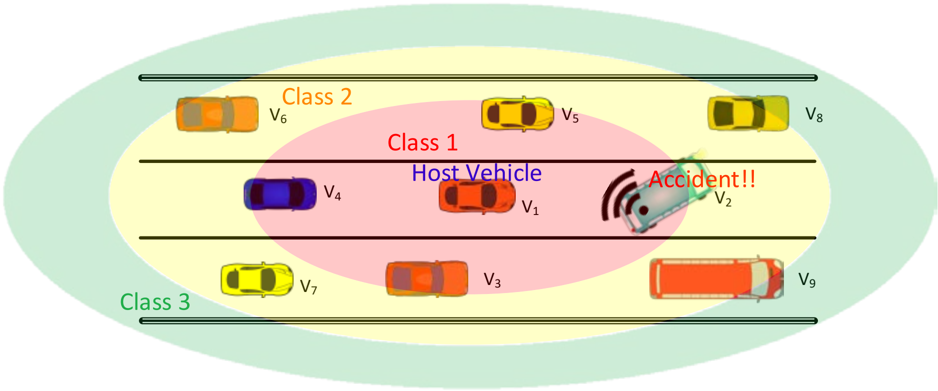
- Major Updates
  - Reorganization of Table of Contents (TOC) for problem statement and use cases in IPWAVE:
    - The request from AD (Suresh Krishnan) and IPWAVE Chairs.
    - TOC was from consensus in IETF-102 Meeting.
  - Key Work Items for IPWAVE Problem Statement
    - Neighbor Discovery
    - Mobility Management
    - Security and Privacy

Table of Contents

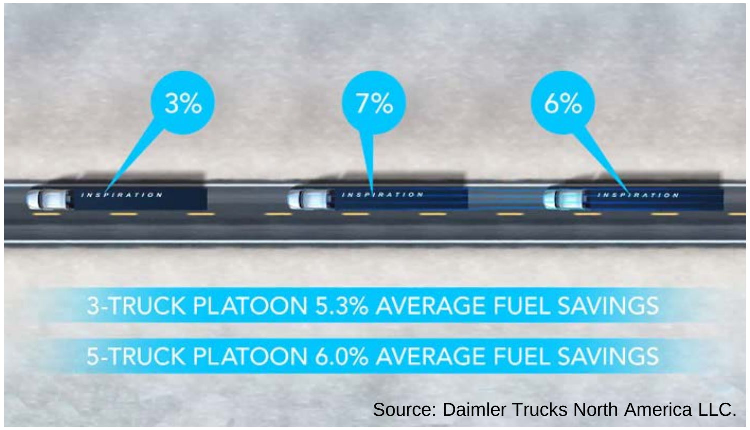
Use Cases (1/3)

- V2V

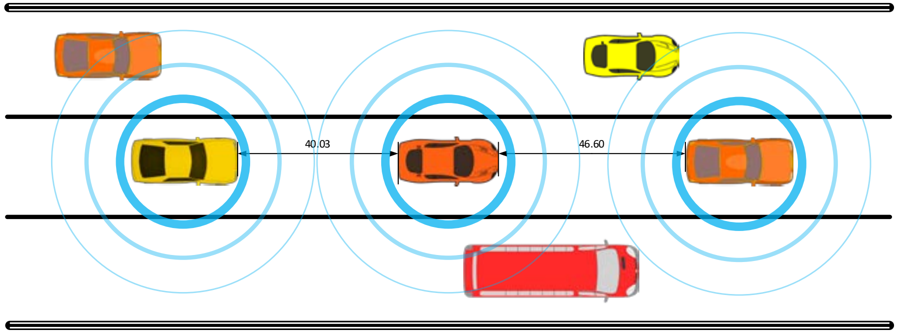
Collision Avoidance



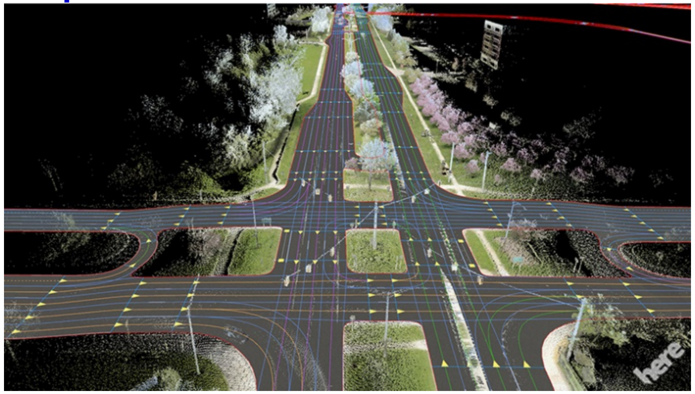
Platooning



Cooperative adaptive cruise control



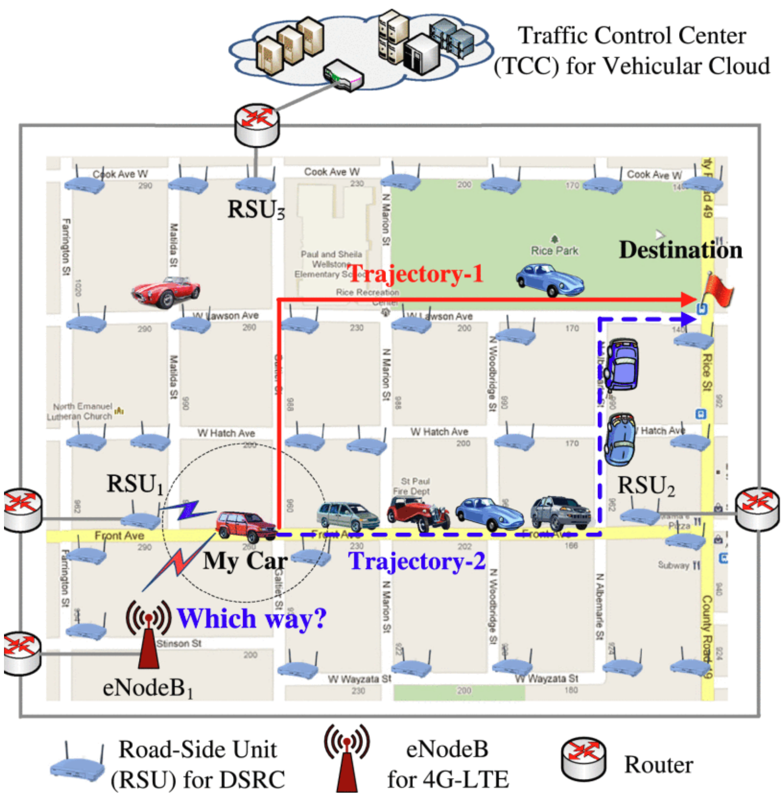
Cooperative environment sensing



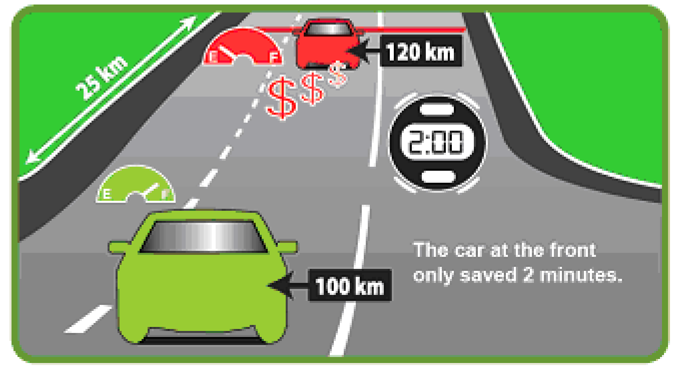
Use Cases (2/3)

- V2I

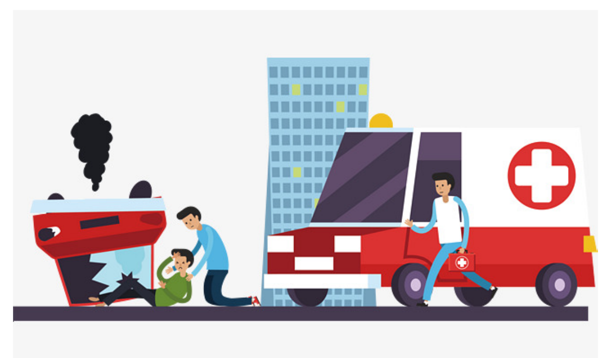
Navigation service



Energy-efficient speed recommendation

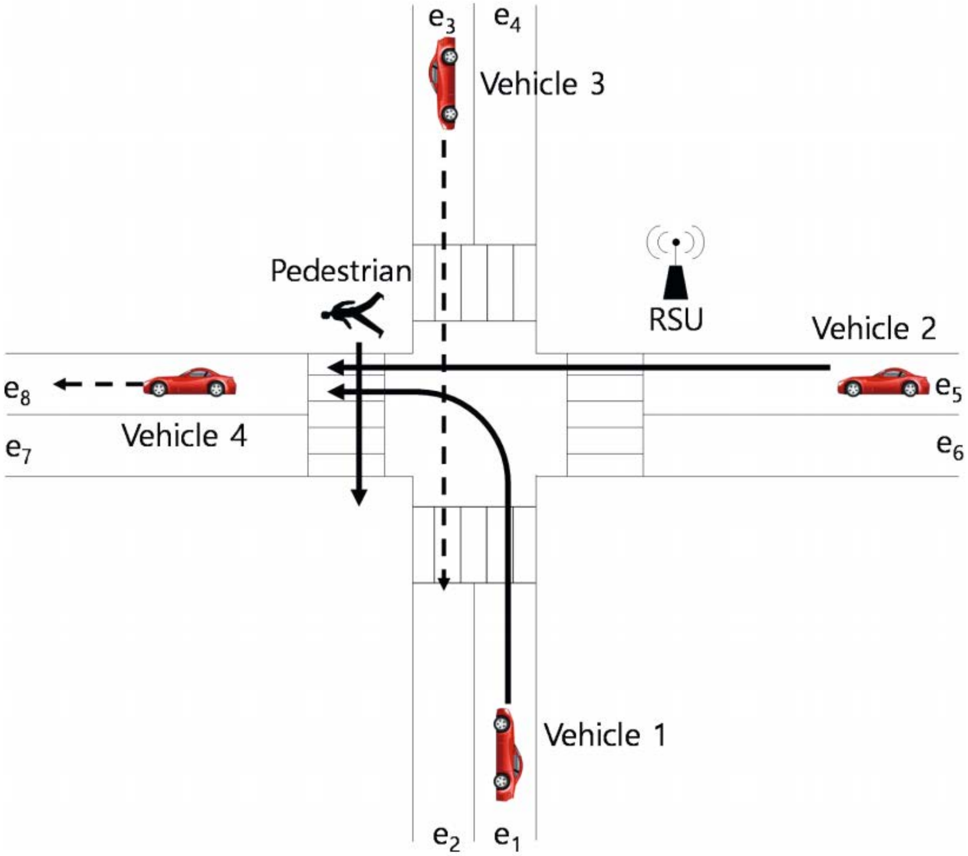


Accident notification service



Use Cases (3/3)

- V2X
  - [Pedestrian protection service]



Analysis for Current Protocols (1/2)

- **The Survey of Current Protocols**
  - Survey is from IP-based vehicular networking research.
  - Protocols of each subject were summarized.

- **Current Protocols for Vehicular Networking**
  - IPv6 over 802.11-OCB
  - IP Address Autoconfiguration
  - Routing
  - Mobility Management
  - DNS Naming Service
  - Service Discovery
  - Security and Privacy

Analysis for Current Protocols (2/2)

- **General Problems**
  - Vehicular Network Architecture
  - Latency
  - Security
  - Pseudonym Handling

General Problems: Vehicular Network Architecture (1/3)

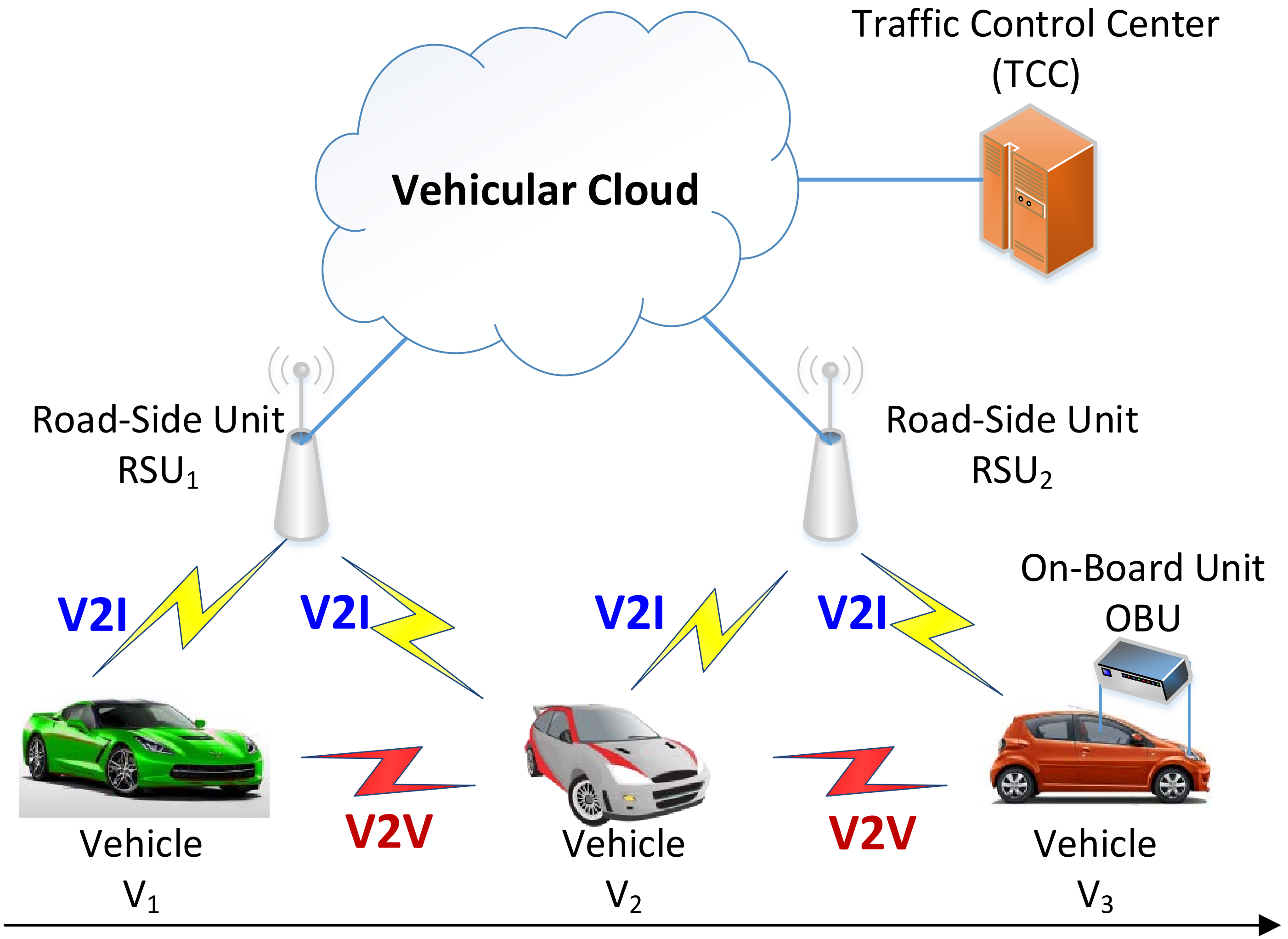


Figure 1: A **Vehicular Network Architecture** for V2I and V2V Networking

General Problems:
Vehicular Network Architecture (2/3)

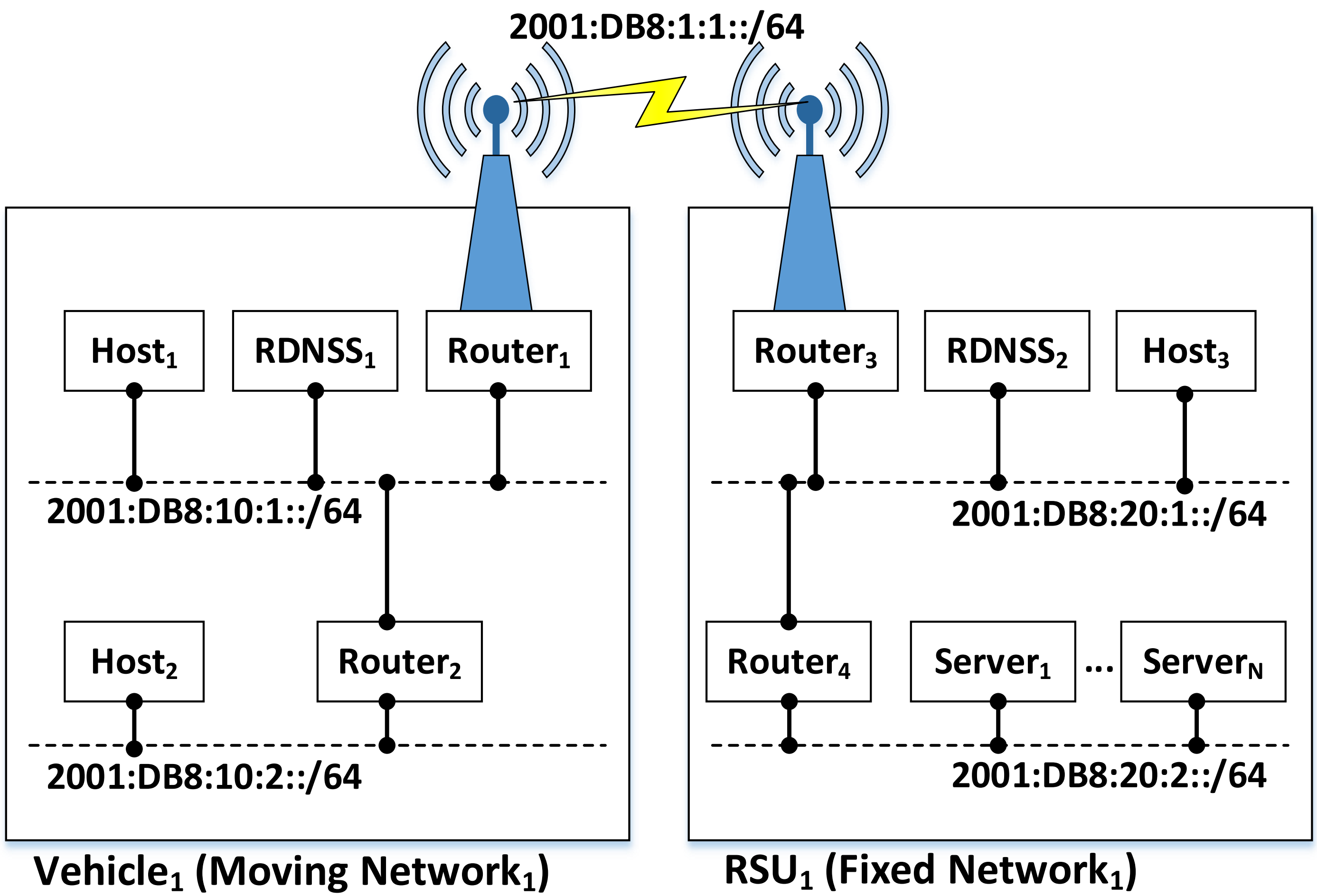


Figure 2: **Internetworking** between **Vehicle Network** and **RSU Network**

General Problems: Vehicular Network Architecture (3/3)

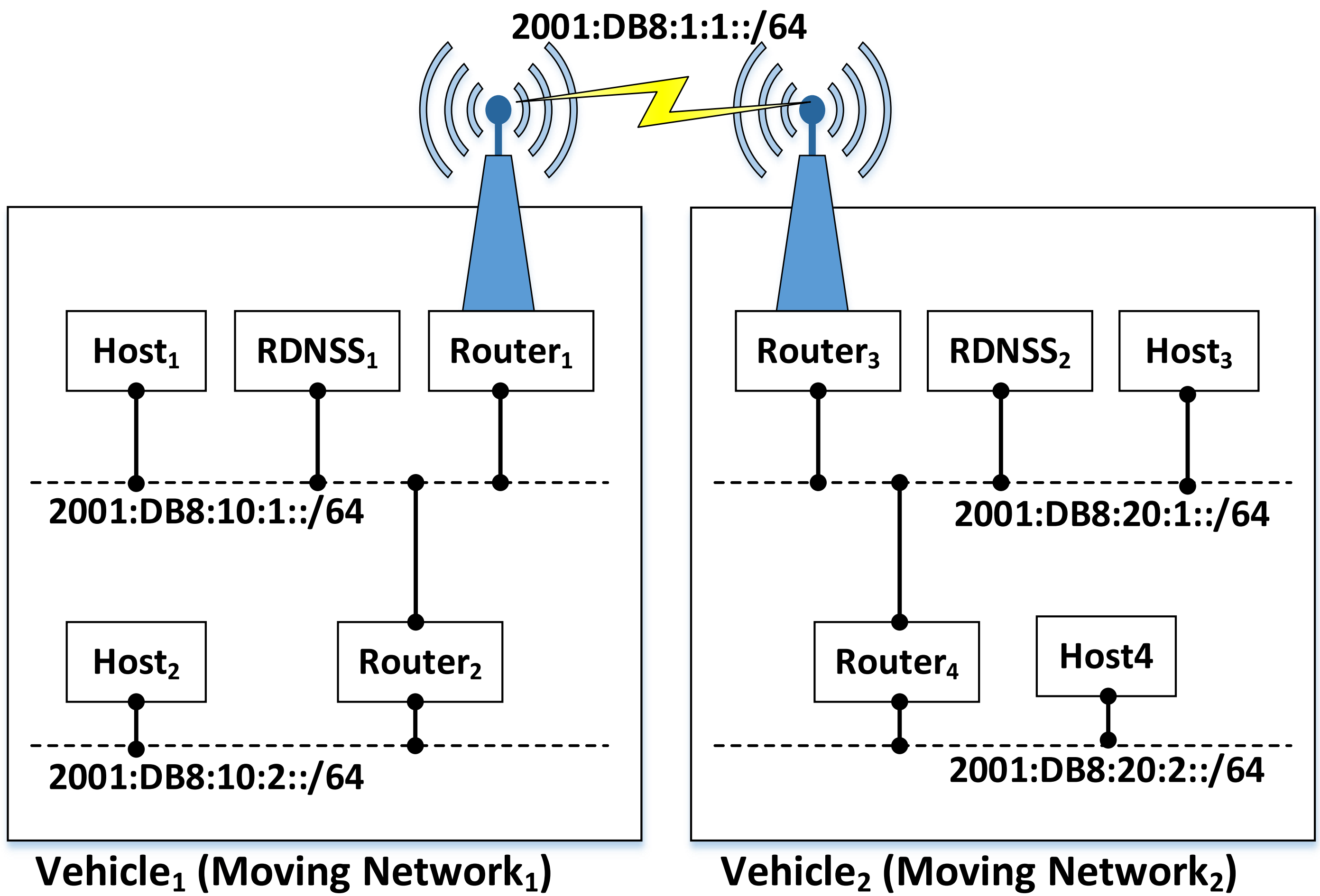


Figure 3: **Internetworking** between **Two Vehicle Networks**

Problem Exploration

- **Key Work Items in IPWAVE**
  - Neighbor Discovery
  - Mobility Management
  - Security and Privacy

- **Relevant Work Items to IPWAVE**
  - Vehicle Identity Management
  - Multihop V2X
  - Multicast
  - DNS Naming Services and Service Discovery
  - IPv6 over Cellular Networks

I E T F®

Neighbor Discovery (ND) (1/3)

- IPv6 ND needs to be tailored for vehicular networking (V2V, V2I, and V2X) having
  - dynamically change topology,
  - multihop forwarding, and
  - high-speed vehicles.

- ND Parameter Adjustment is required:
  - Router lifetime, and
  - Neighbor Advertisement (NA) interval

Neighbor Discovery (ND) (2/3)

- **Link Model**
  - IPv6 protocols have an invalid link model in WAVE:
    - The IPv6 link model's assumption for symmetry in connectivity between neighboring interfaces.
    - The existence of unidirectional links due to interference and different Tx power levels.
    - Unreachability between two nodes with the same prefix due to node mobility and highly dynamic topology in VANET.
  - IPv6 ND should be extended to support the concept of a WAVE link in terms of multicast in VANET.

Neighbor Discovery (ND) (3/3)

- **MAC Address Pseudonym**
  - MAC address change should consider the maintenance of end-to-end transport-layer session according to IPv6 address change.

- **Prefix Dissemination/Exchange**
  - The communication of two nodes within different internal networks (i.e., vehicle and RSU) requires an ND extension or routing for efficient prefix dissemination/exchange.

Mobility Management

- Efficient mobility management is required for
  - seamless connectivity and timely data exchange between two end points.

- GPS navigator-based trajectory can be used for proactive mobility management:
  - A vehicle's mobility information (e.g., position, speed, direction, and trajectory) is periodically reported to a Traffic Control Center (TCC).
  - With prediction of vehicle mobility, TCC supports RSUs to perform DAD, data packet forwarding, and handover in a proactive manner.

Security and Privacy (1/2)

- **Authorized Communication**
  - Only authorized nodes (e.g., vehicles, in-vehicle devices, and mobile devices) should be allowed to use vehicular networking (V2V, V2I, and V2X).

- **Authentication of Vehicle and User**
  - VIN and user certificate with in-vehicle device's ID generation can be used for the authentication of a vehicle or a user.
  - This authentication can be performed by an RSU connected to an authentication server in TCC.

Security and Privacy (2/2)

- **Secure V2I/V2X Communication**
  - A secure channel between a vehicle’s mobile router and an RSU’s fixed router needs to be used for secure V2I communication.
  - A secure channel between a vehicle’s mobile router and another vehicle’s mobile router needs to be used for secure V2V communication.
  - Transport Layer Security (TLS) certificates can be used for secure end-to-end communications.

- **Privacy**
  - MAC address pseudonym can prevent an adversary from tracking a vehicle or user.
  - Such a pseudonym needs to consider the continuity of an end-to-end session.

Next Steps

- **WG Last Call**
  - During WGLC, we will collect feedback from IPWAVE WG and reflect it on the revisions.

- **IESG Submission**
  - We aim at submitting the document to the IESG before IETF-103 meeting.

APPENDIX:
RELEVANT WORK ITEMS TO IPWAVE

Vehicle Identity Management

- A vehicle can have multiple network interfaces for different access network technologies (e.g., DSRC, and 4G-LTE).
  - This means multiple identities of a vehicle.
- In this situation, a Vehicle Identification Number (VIN) can be used for a globally unique vehicle identifier.
- To support seamless connectivity over multiple identities,
  - A cross-layer network architecture is required with vertical handover functionality.

Multihop V2X

- Multihop packet forwarding among vehicles in 802.11-OCB mode shows an unfavorable performance due to the common known broadcast-storm problem.
  - Improvements in Layer-2 are
    - Probability-based methods,
    - Clustering-based methods, and
    - RSU-assisted methods.

Multicast

- IP multicast in vehicular network environments is especially useful for various services:
  - Multicast service notifications to a particular group/class/type of vehicles, and
  - Disseminate alert messages in a particular area.

- Some performance issues about multicast are found in [Multicast-802]
  - Neighbor Discovery and Service Discovery may fail.
  - DAD process may fail.
  - Router Advertisement (RA) messages can be lost.

DNS Naming Services and Service Discovery

- DNS name-based communication between IPv6 nodes (e.g., in-vehicle devices) requires DNS name resolution.
  – For this resolution, Recursive DNS Servers (RDNSSes) should be advertised to them.

- Service discovery is required for an in-vehicle device to search for an application (or server).
  – It resides in another internal network within another vehicle or an RSU.
  – DNS-SD and Vehicular ND can be used.

IPv6 over Cellular Networks (1/2)

- 3GPP-Release 14 (3GPP-R14) announced V2X services support;
  - Using the modified sidelink interface is previously designed for LTE Device-to-Device (LTE-D2D).
  - Only 3GPP-R14 supports IPv6 implementation.

- [TS-23.285-3GPP] instructs that a UE autoconfigures a link-local IPv6 address by following [RFC4862];
  - It does not sends Neighbor Solicitation and Neighbor Advertisement messages for DAD.

IPv6 over Cellular Networks (2/2)

- [TR-22.886-3GPP] is studying new use cases for V2X using 5G new radio in the future:
  - Platooning
  - Sensor and state map sharing
  - Remote driving
  - Automated cooperative driving
  - Dynamic ride sharing
  - Emergency trajectory alignment
  - Software update for ECU
  - etc.