Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 13, 2020

Z. Yan
CNNIC
J. Lee
Sangmyung University
J. Jeong
Sungkyunkwan University

October 11, 2019

Service and Neighbor Discovery in ITS
draft-yan-ipwave-nd-04.txt

Abstract

For C-ACC, platooning and other typical use cases in ITS, direct IP communication between neighbor vehicles poses the following two issues: 1) how to discover the neighbor vehicle and the demanded service; and 2) how to discover the link-layer address of the neighbor vehicle and selected server. This draft presents a solution to these problems based on DNS-SD/mDNS [RFC6762][RFC6763].

Requirements Language

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.

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 https://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 13, 2020.

Table of Contents

1. Introduction

As illustrated in [DNS-Autoconf], a naming scheme is needed for the vehicle devices to support the unique name auto-configuration. This can support the location based communicaton and scalable information organization in ITS. Based on the naming scheme like this and the widely-used DNS-SD/mDNS protocol, this draft illustrates how to discover the neighbor vehicle or services with DNS resolution logic. Before this, we make the following assumptions:

- Name: vehicle SHOULD have a temporary name which is related to its geo-location.

o Address: vehicle SHOULD have a global IP address which is routeable for the IP communications.

In this way, a standardized, efficient and scalable scheme can be used to retrieve the necessary information of the corresponding node

(domain name, IP address, goe-location, link-local address and so on) for the further communications based on the DNS-SD/mDNS function. In addition, the extended NDP messages (e.g., RA and RS messages) can also be used to exchange some required information (e.g., mobile network prefixes, link-local address) in ITS in combination with DNS-SD/mDNS [MNPP].

2. Prefix management

The network architecture which illustrates the prefix management of name and address is shown in Figure 1.

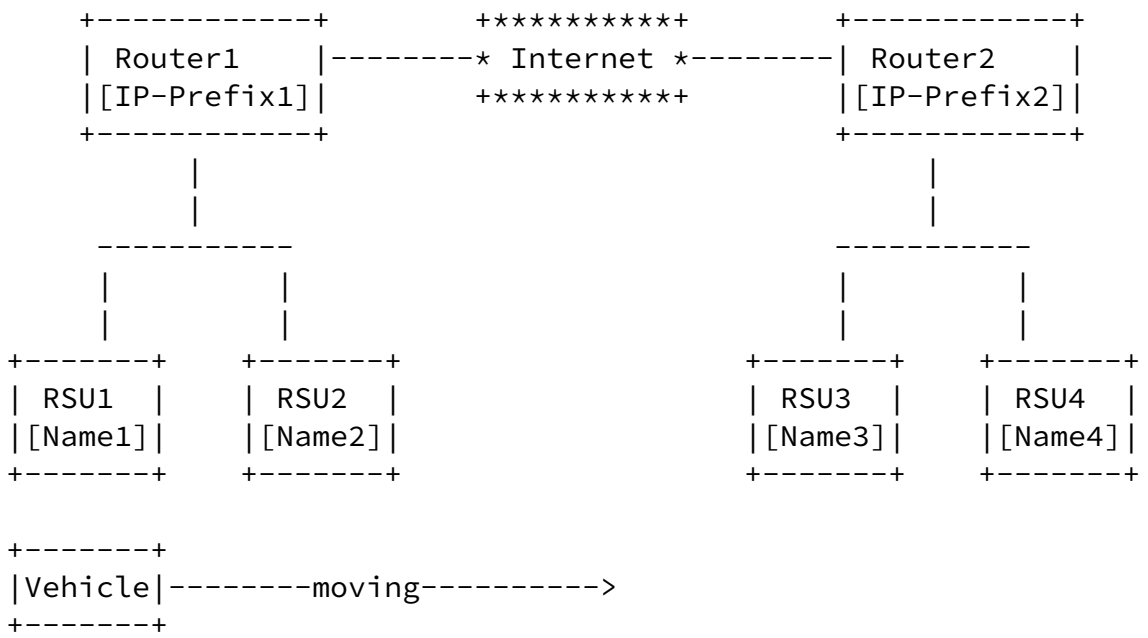

Figure 1: Name and address management architecture

As shown in Figure 1, Router1 and Router2 are two routers which can connect to the Internet and they hold different IP prefixes. RSU1 and RSU2 are two RSUs under Router1 but hold different name prefixes, while RSU3 and RSU4 are two RSUs under Router2 but hold different

name prefixes.

3. Name configuration

The RSU acts as an access router for the static and moving vehicles which want to be connected. Based on [RFC3640], [RFC6106] or extended WSA message, the RSU can announce its location based name prefix to the vehicles covered by the RSU. This location based prefix may contain information such as country, city, street and so on, which will act as the "domain_name" of the vehicle device name as spefified in [DNS-Autoconf].

4. Address configuration

The RSU may advertise the IP prefix to support the SLAAC operation of vehicle devices and movement detection (in the IP layer). If the DHCP is used for the address configuration, RSU also acts as functional entity of the DHCP infrastructure .

5. Neighbor vehicle and service discovery

(1) RSU based

Vehicles may have direct connection with the serving RSU and join the same link with the serving RSU. Then the RSU can maintain the registered vehicle or service in its serving domain. Otherwise, the RSU acts as a relay node for discovering in a proxy manner.

When a vehicle wants to locate the potential nearby neighbor and further establish the communication, the vehicle will trigger the direct unicast query to port 5353 or legacy unicast DNS query to the RSU. RSU may respond directly if it has the related information, otherwise, the RSU multicasts the DNS query to multicast group to retrieve the related information. Unicast response is the first recommendation here because it can suppress the flooding, but of course, the DNS response message can also be multicasted as an active announcement of the verhicle or service existence.

(2) Ad-hoc based

Vehicles may communicate with each other or sense the front and rear

neighbors with DSRC, WiFi, blue-tooth or other short-distance communication technologies, connecting each other in the Ad-hoc manner. Then the discovery can be executed in an infrastructure-less manner with the following phases, as specified in mDNS.

- Probing: When a vehicle starts up, wakes up from stalls or the VANET topology changes (after configuration of the name and address), it should probe the availability of the service it announced. Then the vehicle periodically announces the service and its existence with unsolicited multicast DNS response containing, in the Answer Section, all of its service,name,address and other information. The vehicle also updates the related information actively if there is any change.

- Discovering: To support the service and neighbor vehicle discovery in the dynamic and fragmentation-possible environment in VANET, different query modes of mDNS can be used for different scenarios: 1) One-Short Multicast DNS Query can be used to locate a specific

vehicle (for example). 2) Continuous Multicast DNS Query can be used to locate the nearby vehicles which are moving (for example).

- Refreshing: After the neighbor discovery illustrated above, the vehicles should continually exchange their name, IP address, geo-location and other information in order to refresh the established communications. For example, the Multiple Questions Multicast Responses can be used to update the caches of receivers efficiently and Multiple Questions Unicast Responses can be used to support the fast bootstrapping when new vehicle joins.

- Goodbye: When the vehicle arrives at its destination, stalls temporarily or shuts down its communication or sensing devices, it will announce the service suspending and its inexistence with unsolicited multicast DNS response packet, giving the same RRs (for example containing its name and address), but TTL of zero.

6. Mobility support

During the movement of the vehicle, it may cross different RUSes. When attaching into a new RSU, the new domain prefix and new IP prefix may be learned. Generally, there are two main cases for the

mobility:

- Name prefix changes and IP prefix remains, as shown in Figure 1, the vehicle hands over from RSU1 to RSU2. The vehicle will configure a new name from RSU2 and may update the new name in the local database (e.g., RSU). But the vehicle should keep its previous name for a period until that all the communicating neighbors have learned its new name. During this period, the vehicle will contain both previous and new names in the DNS response message.

- Both name and IP prefixes change, as shown in Figure 1, the vehicle hands over from RSU2 to RSU3. The vehicle will configure both new name and new IP address from RSU3 and update them in the local database. Then the above scheme can also be used or with IP-layer mobility management protocols.

7. Signaling messages

To facilitate the further communication, the link-layer address and geo-information may be included in the DNS message in a piggyback manner. Otherwise, these information may be obtained through the following NDP or other procedures.

8. Security considerations

In order to reduce the DNS traffic on the wireless link and avoid the unnecessary flooding, the related schemes in mDNS can be used, such as: Known-Answer Suppression, Multipacket Known-Answer Suppression, Duplicate Question Suppression and Duplicate Answer Suppression.

In order to guarantee the origination of the DNS message and avoid the DNS message tampering, the security consideration in mDNS should also be adopted.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3640] van der Meer, J., Mackie, D., Swaminathan, V., Singer, D., and P. Gentric, "RTP Payload Format for Transport of MPEG-4 Elementary Streams", RFC 3640, DOI 10.17487/RFC3640, November 2003, <https://www.rfc-editor.org/info/rfc3640>.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, DOI 10.17487/RFC6106, November 2010, <https://www.rfc-editor.org/info/rfc6106>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

9.2. Informative References

[DNS-Autoconf] Jeong, J., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-03, July 2018.

[MNPP] Lee, J., Tsukada, M., and T. Ernst, "Mobile Network Prefix Provisioning", draft-jhlee-mext-mnpp-00, October 2009.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing 100190
China

EMail: yan@cnnic.cn

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan
Republic of Korea

EMail: jonghyouk@smu.ac.kr

Jaehoon Paul Jeong
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do
Republic of Korea

EMail: pauljeong@skku.edu