Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 17, 2020

J. Bi
J. Wu
Y. Wang
Tsinghua University
T. Lin
New H3C Technologies Co. Ltd

November 17, 2019

A SAVI Solution for WLAN
draft-bi-savi-wlan-18

Abstract

This document describes a source address validation solution for WLAN enabling 802.11i or other security mechanisms. This mechanism snoops NDP and DHCP packets to bind IP address to MAC address, and relies on the security of MAC address guaranteed by 802.11i or other mechanisms to filter IP spoofing packets. It can work in the special situations described in the charter of SAVI(Source Address Validation Improvements) workgroup, such as multiple MAC addresses on one interface. This document describes three different deployment scenarios, with solutions for migration of binding entries when hosts move from one access point to another.

Table of Contents

1. Introduction

This document describes a mechanism to perform per packet IP source address validation in WLAN. This mechanism performs ND snooping or DHCP snooping to bind allocated IP address with authenticated MAC address. Static addresses are bound to the MAC addresses of corresponding hosts manually. Then the mechanism can check validity of source IP address in local packets according to the binding

association. The security of MAC address is assured by 802.11i or other mechanisms, thus the binding association is secure.

The situation that one interfaces with multiple MAC addresses is a special case mentioned in the charter of SAVI. And this situation is the only special case that challenges MAC-IP binding. The mechanism to handle this situation is specified in the document.

There are three deployment scenarios specified in this document. The mechanism is deployed on different devices in different scenarios. The deployment detail is described in the document.

When hosts move from one access point to another, the migration of binding entries may be triggered according to the specific mobility scenario. The mechanism to handle host mobility is specified in the document according to different deployment scenarios.

1.1. Terminology

FIT Access Points: the name of Access Points in Centralized WLAN deployment scenario.

FAT Access Points: the name of Access Points in Autonomous WLAN deployment scenario.

2. Conventions used in this document

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 [RFC2119].

3. IP-MAC Binding

This section specifies the operations for creating and clearing of bindings between IP addresses to MAC addresses.

3.1. Data Structures

3.1.1. IP-MAC Mapping Table

This table maps IP addresses to corresponding MAC addresses. IP address is the index of the table. One IP address can only have one corresponding MAC address, while different IP addresses can be mapped to the same MAC address.

This table is used in control process. Before creating new IP-MAC bindings, this table must first be consulted in case of conflict in binding entries. Also, this table must be consulted before doing any

packet filtering. This table must be synchronized with the MAC-IP table specified in Section 3.1.2.

Each entry in IP-MAC mapping table must also record the binding state of the IP address. Addresses snooped in DHCP address assignment procedure must record its state as "DHCPv6", and addresses snooped in Duplicate Address Detection procedure must record its state as "SLAAC".

Each entry in IP-MAC mapping table has its lifetime. According to RFC3315 [RFC3315], the address allocated by DHCP has a limited lifetime, so the related entry records its lifetime the same as that of the address. According to RFC4862 [RFC4862], stateless address also has a limited lifetime, and the host set this lifetime by itself. Thus the related entry also records its lifetime the same as that of the address.

3.1.2. MAC-IP Mapping Table

This table maps MAC addresses to corresponding IP addresses. MAC address is the index of the table. It is a one-to-many mapping table, which means a MAC address can be mapped to multiple IP addresses. Though multiple MAC addresses may exist on one interface, these MAC addresses must be mapped to different IP addresses.

This table is used for filtering. Different from wired network, MAC-IP mapping table and IP-MAC mapping table can be maintained separately on different devices. Mechanisms for synchronization between the two tables must be employed for the consistency of the bindings. We will specify the details in Section 5 according to different deployment scenarios.

3.2. Pre-conditions for binding

In the binding based mechanism, the security of IP address is based on the security of the binding anchor. In WLAN, 802.11i or other security mechanisms on link layer make MAC address a strong enough binding anchor.

If MAC address has no protection, attackers can spoof MAC address to succeed in validation. However, in general cases, if MAC address is not protected, more serious attack can be launched than IP spoofing attack.

3.3. Binding IP addresses to MAC addresses

All the static IP-MAC address pairs are configured into the IP-MAC Mapping Table with the mechanism enabled.

An individual procedure handles binding DHCP addresses to MAC addresses. This procedure snoops the DHCP address assignment procedure between attached hosts and DHCP server. DHCP snooping in WLAN is the same as that in wired network specified in RFC7513 [RFC7513].

An individual procedure handles binding stateless addresses to MAC addresses. This procedure snoops Duplicate Address Detection procedure. ND snooping in WLAN is the same as that in wired network specified in [RFC6620] [RFC6620].

Data packets MAY also trigger the establishment of new IP-MAC binding entries. Data packet with non-bound source IP address with a limited rate is collected to handle DAD message loss in SLAAC procedure, which can be quite frequent in wireless network. The detail of the procedure is specified in Section 4. However, this mechanism will bring potential security risks (e.g. attacks that aimed at exhausting available IP addresses). Thus, it is optional whether to enable the mechanism, and if it is enabled, additional security mechanisms MUST also be employed to cope with the risks. Related security considerations are discussed in Section 6.

In some deployment scenarios, the function of address snooping and IP-MAC table maintaining may also be separated onto different devices. Thus to prevent conflictions in binding entries, the device snoops addresses must have interactions with the device maintains the IP-MAC table. We will specify the details in Section 5.1.1.

3.4. Binding Migration

Different from wired network, SAVI for WLAN must handle migration of binding entries when mobile hosts move from one access point to another. After movement, hosts will not perform another address allocation procedure to obtain new IP addresses, but continue to use the existing IP address. Thus binding entries in the foreign device that the mobile hosts access to cannot be established by snooping. A new mechanism is needed to correctly migrate the binding entry related to the IP address of the mobile host from the home device to the foreign device. We will specify the details in Section 5, according to different deployment scenarios.

3.5. Binding Clearing

Three kinds of events will trigger binding clearing:

1. The lifetime of an IP address in one entry has expired. This IP entry in IP-MAC mapping table and corresponding entries in MAC-IP mapping table MUST be cleared.

2. A host leaves this access point. The entries for all related MAC addresses in MAC-IP table MUST be cleared.

3. A DHCP RELEASE message is received from the owner of corresponding IP address. This IP entry in IP-MAC mapping table and corresponding entries in MAC-IP mapping table MUST be cleared.

The protocols used for synchronization between MAC-IP and IP-MAC tables will be specified in Section 5.1.1.4.

4. Source Address Validation

This section describes source address validation procedure on packet. In this procedure, all the frames are assumed to have passed the verifications of 802.11i or other security mechanisms.

This procedure has the following steps:

1. Extract the IP source and MAC source from the frame. Lookup the MAC address in the MAC-IP Mapping Table and check if the MAC-IP pair exists. If yes, forward the packet. Or else go to step 2.

2. Lookup the IP address in the IP-MAC Mapping Table and check if the IP address exists. If no, go to step 3. If yes, check whether The MAC address in the entry is the same as that in the frame. If yes, forward the packet. Else drop the packet.

3. If the mechanism that allows data packets to trigger the establishment of new IP-MAC binding entries is enabled, insert a new entry into the IP-MAC Mapping Table and forward the packet. Otherwise drop the packet.

In step 2, after the packet is judged valid and forwarded, synchronization between the MAC-IP and IP-MAC mapping table should be triggered. The MAC-IP binding of the packet should be synchronized from IP-MAC mapping table to MAC-IP mapping table and thus the following packets with the same MAC-IP pair will be forwarded without going to step 2.

Also in step 3, if a new IP-MAC binding entry is established, it should be synchronized to MAC-IP mapping table. The protocols used for synchronization between MAC-IP and IP-MAC tables will be specified in Section 5.1.1.4.

5. Deployment Scenarios

This section specifies three deployment scenarios including two under centralized WLAN and one under autonomous WLAN. The deployment details and solutions for host mobility between access points are described respectively in each scenario.

5.1. Centralized WLAN

Centralized WLAN is comprised of FIT Access Points (AP) and Access Controllers (AC). In this scenario, this document proposes the following two deployment solutions.

5.1.1. AP Filtering

With this deployment solution, data packets received by the APs do not go through the ACs and only control packets (including questionable data packets) go through the ACs. In this scenario, AC maintains IP-MAC Mapping Table while AP maintains MAC-IP Mapping Table and perform address snooping.

5.1.1.1. Candidate Binding

AP executes the procedure specified in Section 3.3. Candidate binding is generated after snooping procedure. Candidate binding must be confirmed by AC to be valid.

After a candidate binding is generated, AC is notified and checks whether the binding is valid or not. The validity of a candidate binding is determined if the binding does not violate any existing bindings in the IP-MAC Mapping Table. Otherwise if an address is not suitable for a host to use, AC notifies the corresponding AP. If the candidate binding is valid, AC adds an entry into the IP-MAC Mapping Table and notifies AP. Afterwards AP also adds an entry into the local MAC-IP Mapping Table.

5.1.1.2. Packet Filtering

As specified in Section 4, for incoming data packets, AP looks up the MAC address in the local MAC-IP Mapping Table and check if the MAC-IP pair exists. If yes, AP forwards the packet. Or else AP delivers the packet to AC for further processing.

When receiving data packets from AP, AC Looks up the IP address in the local IP-MAC Mapping Table and checks if the IP address exists. If no, according to whether the AC is configured to allow data packets to trigger binding entry creations, AC establishes a new IP-MAC entry then forwards the packet, or drop the packet. If yes, AC checks whether The MAC address in the entry is the same as that in the frame. If yes, AC forwards the packet. Else AC drops the packet.

After AC forwards a valid packet, it synchronizes related MAC-IP binding to the MAC-IP mapping table on the AP from which the packet comes. Following packets with the same MAC-IP pair will be forwarded directly by AP without going to AC.

5.1.1.3. Negative Entries

In the AP Filtering scenario, APs MAY drop packets directly without sending them to AC by enabling the establishment of negative entries on APs. Specifically, APs may establish negative entries in the following circumstances.

1. When AP receives a certain amount of packets within a certain amount of time with the same MAC-IP pair that does not exist in the local MAC-IP Table, it establishes a negative entry for this MAC-IP pair. Then AP drops all following packets that have the same MAC-IP pair as indicated in this negative entry without sending them to AC for further processing.

2. When AP receives a certain amount of packets within a certain amount of time with the same MAC address but different MAC-IP pairs and none of these MAC-IP pairs exist in the local MAC-IP Table, it establishes a negative entry for this MAC address. Then AP drops all following packets that have the same MAC address as indicated in this negative entry without sending them to AC for further processing.

Each negative entry has a limited lifetime. The number of packets and duration of time to trigger the establishment of the negative entry, and the lifetime of the negative entry are configurable.

5.1.1.4. CAPWAP Extension

CAPWAP protocol is used for communication between AP and AC. A new CAPWAP protocol message element is introduced, which extends RFC5415 [RFC5415]. The host IP message element is used by both AP and AC to exchange the binding information of hosts.

The host IP message element can be used in the process of confirmation of candidate binding. When AP generates a candidate binding, it reports the MAC address and related IP addresses to AC using this message, with suggestions of the state and lifetime of each IP address as specified in Section 3.1.1. After AC checks the validation of the candidate binding, it replies using a message of the same format to inform AP the validation of each IP address with suggestions of its state and lifetime.

The host IP message element can be used in the process of binding migration. When migration happens, the source device reports the MAC address and related IP addresses to the destination device using this message, with suggestions of the state and lifetime of each IP address as specified in Section 3.1.1. After the destination device checks the validation of the candidate binding, it replies using a message of the same format to inform the source device the validation of each IP address with suggestions of its state and lifetime.

The host IP message element can also be used in other scenarios when synchronization between MAC-IP and IP-MAC tables is required as specified in Section 3.5 and Section 4. When synchronization from IP-MAC table to MAC-IP table is triggered, the source device which holds the IP-MAC table reports the MAC address and related IP addresses to the destination device which holds the MAC-IP table using this message, with suggestions of the state and lifetime of each IP address as specified in Section 3.1.1. The destination device replies using a message of the same format to acknowledge the source device.

```
   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    Radio ID   |                Total Length                   +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |   Sender ID   |     Length    |         Description           +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    MAC flag   |     Length    |        MAC Address...         +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                     MAC Address...                            +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    IPv4 flag  |     Length    |        blank       ...        +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                    IPv4 Address 1(32 bit)                     +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    State      |        blank       ...                        +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                    lifetime                                   +
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|                    IPv4 Address 2(32 bit)                     +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    State      |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    ........                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Address n(32 bit)                     +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    State      |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    IPv6 flag  |     Length    |         IPv6 Address...       +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv6 Address 1(128 bit)                    +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    State      |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv6 Address 2(128 bit)                    +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    State      |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    ........                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv6 Address n(128 bit)                    +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    State      |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Radio ID: An 8-bit value representing the radio, whose value is between 1 and 31.

Total Length: Total length of the following fields.

Sender ID: An 8-bit value representing the sender of the message. AP is represented by value 1 and AC is represented by value 2.

Length: The length of the Value field.

Description: A 16-bit value for descriptions of the sender (AP or AC).

MAC flag: An 8-bit value representing that the sub-field's type is MAC address, whose value is 1.

Length: The length of the MAC Address field. The formats and lengths specified in EUI-48 [EUI-48] and EUI-64 [EUI-64] are supported.

MAC Address: A MAC address of the host. At least one MAC address block MUST appear in the message, otherwise the message is considered as invalid.

IPv4 flag: An 8-bit value representing that the sub-field's type is IPv4 address, whose value is 2.

Length: The length of the IPv4 Address field.

IPv4 Address: An IPv4 address of the host. There may exist many entries, and each entry is comprised of an IPv4 address, an 8-bit value for address state (value 1 means available, value 0 means unavailable, value 255 means candidate), and a 32-bit value for lifetime. It is required to list all IPv4 addresses before IPv6 address blocks.

IPv6 flag: An 8-bit value representing that the sub-field's type is IPv6 address, whose value is 3.

Length: The length of the IPv6 Address field.

IPv6 Address: An IPv6 address of the host. There may exist many entries, and each entry is comprised of an IPv6 address, an 8-bit value of address state (value 1 means available, value 0 means unavailable, value 255 means candidate), and a 32-bit value lifetime. All IPv4 and IPv6 addresses bind to the MAC address that appears before them in the message.

5.1.1.5. Mobility Solution

When a host moves from one AP to another, layer-2 association happens before IP packet transfer. Home AP deletes the binding when mobile host is disconnected, and foreign AP immediately requests the bound addresses with the associated MAC from AC. AC returns the binding with suggestions of its state and lifetime. After AP get the addresses should be bound, the binding migration is completed. The protocol used for communication between foreign AP and AC is the same as described in Section 5.1.1.4, while in this scenario AC serves the

role of the source device and foreign AP serves the role of the destination device.

In WLAN, a host can move from an AC to another AC while keeping using the same IP address. To be compatible with such scenario, ACs must communicate to perform the binding migration. The protocol used for communication between ACs is the same as described in Section 5.1.1.4, while in this scenario home AC serves the role of the source device and foreign AC serves the role of the destination device.

5.1.2. AC Filtering

In this scenario, AC maintains both MAC-IP and IP-MAC Mapping Table and performs both address snooping and packet filtering. So all the packets must be forwarded to AC firstly.

AC executes the procedure specified in Section 3.3 and check the validity of IP-MAC pairs by consulting the local IP-MAC mapping table. No extra procedure is needed to establish the IP-MAC bindings.

AC executes the procedure specified in Section 4 for packet filtering and no extra procedure is involved.

Mobility within one AC does not trigger any binding migration. Mobility between different ACs triggers binding migration. ACs must communicate to perform the binding migration. The protocol used for communication between ACs is the same as described in Section 5.1.1.4, while in this scenario home AC serves the role of the source device and foreign AC serves the role of the destination device.

5.2. Autonomous WLAN

Autonomous WLAN is comprised of FAT Access Points. In this scenario, FAT AP maintains both MAC-IP and IP-MAC Mapping Table and performs both address snooping and packet filtering.

FAT AP executes the procedure specified in Section 3.3 and check the validity of IP-MAC pairs by consulting the local IP-MAC mapping table. No extra procedure is needed to establish the IP-MAC bindings.

FAT AP executes the procedure specified in Section 4 for packet filtering and no extra procedure is involved.

Mobility between different FAT APs will trigger binding migration. FAT APs must communicate to perform the binding migration. The protocol used for communication between FAT APs is the same as described in Section 5.1.1.4, while in this scenario home FAT AP serves the role of the source device and foreign FAT AP serves the role of the destination device.

6. IANA Considerations

There is no IANA Consideration currently.

7. Security Considerations

The security of address allocation methods matters the security of this mechanism. Thus it is necessary to improve the security of stateless auto-configuration and DHCP firstly.

7.1. Issues with Triggerring Establishment of Binding Entries by Data Packets

In Section 3.3, a mechanism is described to allow data packets to trigger the establishment of new binding entries to handle DAD message loss in SLAAC procedure. If the mechanism is enabled, it can be used to launch attacks which may finally leads to exhaustion of available IP addresses. If no restriction is taken, the attacker can make as many IP-MAC bindings as possible with the same MAC address. In this way, other hosts may fail to trigger any binding entry establishment and thus cannot get their packets pass the SAVI device. To cope with the potential security risks, additional mechanism MUST be employed, e.g. to limit the maximum number of IP addresses that one MAC address can bind to.

Packet loss in wireless networks can be handled in a more robust way by other source address validation mechanisms, e.g. [RFC8505] with an extension protocol in [draft-ietf-6lo-ap-nd-12]. However it requires protocol changes and thus it is out of the scope of SAVI.

7.2. Privacy Considerations

A SAVI device MUST delete binding anchor information as soon as possible, except where there is an identified reason why that information is likely to be involved in the detection, prevention, or tracing of actual source-address spoofing. Information about hosts that never spoof (probably the majority of hosts) SHOULD NOT be logged.

8. Acknowledgements

The authors would like to thank Guang Yao, Yang Shi and Hao Wang for their contributions to this document.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[RFC6620] Nordmark, E., Bagnulo, M., and E. Levy-Abegnoli, "FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses", RFC 6620, DOI 10.17487/RFC6620, May 2012, <https://www.rfc-editor.org/info/rfc6620>.

[RFC7513] Bi, J., Wu, J., Yao, G., and F. Baker, "Source Address Validation Improvement (SAVI) Solution for DHCP", RFC 7513, DOI 10.17487/RFC7513, May 2015, <https://www.rfc-editor.org/info/rfc7513>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

9.2. Informative References

[EUI-48] "Guidelines For 48-bit Global Identifier (EUI-48)", http://standards.ieee.org/develop/regauth/tut/eui48.pdf

[EUI-64] "Guidelines For 64-bit Global Identifier (EUI-64)", http://standards.ieee.org/develop/regauth/tut/eui64.pdf

[draft-ietf-6lo-ap-nd-12]
Thubert, P., Sarikaya, B., Sethi, M., and Struik, R., "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-12 (work in progress), April, 2019.

Authors' Addresses

Jun Bi
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China

Email: junbi@cernet.edu.cn

Jianping Wu
Tsinghua University
Computer Science, Tsinghua University
Beijing 100084
China

Email: jianping@cernet.edu.cn

You Wang
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China

Email: you@opennetworking.org

Tao Lin
New H3C Technologies Co. Ltd
466 Changhe Road, Binjiang District
Hangzhou, Zhejiang Province 310052
China

Email: lintao@h3c.com