Workgroup:
Source Address Validation Improvements (SAVI)
Internet-Draft: draft-bi-savi-wlan-23
Published: 11 May 2022
Intended Status: Standards Track
Expires: 12 November 2022

Authors: J.B. Bi
Tsinghua University
J.W. Wu
Tsinghua University
T.L. Lin
New H3C Technologies Co. Ltd
Y.W. Wang
Tsinghua University
L.H. He
Tsinghua University

A SAVI Solution for WLAN

Abstract

This document describes a source address validation solution for WLANs where 802.11i or other security mechanisms are enabled to secure MAC addresses. This mechanism snoops NDP and DHCP packets to bind IP addresses to MAC addresses, and relies on the security of MAC addresses 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.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes a mechanism for performing per-packet IP source address validation in wireless local area networks (WLANs). The mechanism performs ND snooping or DHCP snooping to bind the assigned IP address to the verified MAC address. Static addresses are manually bound to the MAC address of the corresponding host. The mechanism can then check the validity of the source IP address in the local packet against the binding association. The MAC address is secured by 802.11i or other mechanisms, so the binding association is secure.

This mechanism utilizes two important data structures, the IP-MAC mapping table on the control plane and the MAC-IP mapping table on the data plane, to implement source address validation, which is described in detail in this document.

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

Three deployment scenarios for this mechanism are specified in this document, describing the devices and details of deployment in different scenarios.

When a host moves from one access point to another, the migration of binding entries can be triggered depending on the specific mobility scenario. The mechanism for handling host mobility is specified in the documentation based on different deployment scenarios.

1.1. Terminology

FIT access points: The access points used in centralized WLAN deployment scenario.

FAT access points: The access points used in autonomous WLAN deployment scenario.

Binding anchor: A "binding anchor" is defined to be a physical and/or link-layer property of an attached device, as defined in [RFC7039]. In this document, the binding anchor refers to th MAC address.

Binding entry: A rule that associates an IP address with a binding anchor.

Familiarity with SAVI-DHCP and its terminology, as defined in [RFC7513], is assumed.

2. 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 [RFC2119].

3. IP-MAC Binding

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

3.1. Data Structures

The binding relationship between IP address and MAC address is stored using two data structures, i.e., the IP-MAC mapping table and MAC-IP mapping table.

3.1.1. IP-MAC Mapping Table

This table maps IP addresses to their corresponding MAC addresses. The IP address is the index of the table. An IP address can have only one corresponding MAC address. Different IP addresses can be mapped to the same MAC address.

This table is used in the control process. Before creating a new IP-MAC binding, this table must be queried to prevent conflicting binding entries. Also, this table must be queried before any packet filtering is performed. This table must be synchronized with the MAC-IP mapping table specified in Section 3.1.2.

Each entry in the IP-MAC mapping table must also record the binding method of the IP address. Addresses snooped in the DHCP address assignment procedure must have their binding method recorded as "DHCP", and addresses snooped in the Duplicate Address Detection procedure [RFC4862] must have their binding method recorded as "SLAAC".

3.1.2. MAC-IP Mapping Table

This table maps MAC addresses to the corresponding IP addresses. The 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. Although 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 networks, the MAC-IP mapping table and the IP-MAC mapping table can be maintained separately on different devices. A synchronization mechanism must be used between these two tables to ensure the consistency of the bindings. We will explain the details in Section 5 for different deployment scenarios.

3.2. Pre-conditions for Binding

As specified in [RFC7039], in a binding-based mechanism, the security of IP address is dependent on the security of the binding anchor. In WLANs, 802.11i or other link-layer security mechanisms make MAC address a strong enough binding anchor.

If the MAC address is unprotected, an attacker can spoof the MAC address to pass validation successfully.

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.

A separate procedure handles the binding of DHCP addresses to MAC addresses. This procedure snoops on the DHCP address assignment process between the attached host and the DHCP server. DHCP snooping in WLANs is the same as that in wired networks specified in [RFC7513].

A separate procedure handles the binding of stateless addresses to MAC addresses. This procedure snoops Duplicate Address Detection procedure as described in [RFC4862] or Address Resolution procedure between attached hosts and neighbors as described in [RFC4861]. Based on the principle of roaming experience first in WLAN, the new binding anchor is selected in preference and triggers the deletion of the secure connection of the old binding anchor.

In some deployment scenarios, the functions of address snooping and IP-MAC mapping table maintenance may also be separated to different devices. Therefore, to prevent conflicting binding entries, the device for address snooping must interact with the device that maintains the IP-MAC mapping table. We will specify the details in Section 5.1.1.

3.4. Binding Migration

Different from wired networks, SAVI for WLAN must handle the migration of binding entries when a mobile host moves from one access point to another. After the move, the host will not perform another address configuration procedure to obtain new IP addresses but continue to use the existing IP address(es). Thus, binding entries in the foreign device accessed by mobile hosts cannot be established by snooping. A new mechanism is needed to correctly migrate the binding entry associated with the mobile host's IP address from the home device to the foreign device. If the host binds multiple entries, multiple entries will be migrated. For example, when the host is assigned multiple addresses, multiple binding entries will be generated, and these entries will be migrated. We will specify the details in Section 5 depending on different deployment scenarios.

3.5. Binding Clearing

Three kinds of events will trigger binding clearing:

1. A host leaves explicitly this access point. All entries in the MAC-IP mapping table associated with this MAC address MUST be cleared.

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

3. A timeout message of the AC's client idle-time is received. All entries in the MAC-IP mapping table related to the MAC address MUST be cleared.

4. Source Address Validation

This section describes source address validation procedure for packets. In this procedure, all the frames are considered to have passed the verification of 802.11i or other security mechanisms.

This procedure has the following steps:

1. Extract the IP source address and MAC source address from the frame. Look up the MAC address in the MAC-IP mapping table and check if the MAC-IP pair exists. If exists, forward the packet. Otherwise, go to step 2.

2. Look up the IP address in the IP-MAC mapping table and check if the IP address exists. If it does not exist, go to step 3. If it exists, check whether the MAC address in the entry is the same as that in the frame. If so, forward the packet. Otherwise, drop the packet.

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

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 for each scenario, respectively.

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 scheme, validated data packets received by an AP do not pass through the AC; only control packets and the questionable data packets pass through the AC. In this case, the AC maintains the IP-MAC mapping table, while the AP maintains the MAC-IP mapping table and performs address snooping.

5.1.1.1. Candidate Binding

An AP executes the procedure specified in Section 3.3. The candidate bindings are generated after the snooping procedure. Candidate bindings MUST be confirmed by the AC to be valid.

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

5.1.1.2. Packet Filtering

As specified in Section 4, for incoming data packets, an AP looks up the MAC address in the local MAC-IP mapping table and checks if the MAC-IP pair exists. If exists, the AP forwards the packet. Otherwise, the AP delivers the packet to the AC for further processing.

When receiving a data packet from the AP, the AC looks up the IP address in the local IP-MAC mapping table and checks if the IP address exists. If it does not exist, the AC drops the packet. If it exists, the AC checks whether the MAC address in the entry is the same as that in the frame. If so, the AC forwards the packet. Otherwise, the AC drops the packet.

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

5.1.1.3. Negative Entries

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

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

2. When an AP receives a certain number 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 mapping table, it establishes a negative entry for this MAC address. Then the AP drops all the following packets that have the same MAC address as indicated in this negative entry without sending them to the 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 the AP and the AC. A new CAPWAP protocol message element is introduced, which extends [RFC5415]. The host IP message element is used by both the AP and the AC to exchange the binding information of hosts.

The host IP message element can be used in the process of confirming candidate bindings. When the AP generates a candidate binding, it reports the MAC address and related IP addresses to the AC using this message, with suggestions of the status of each IP address (e.g., available, unavailable, candidate). After the AC checks the validity of the candidate binding, it replies using a message of the same format, informing the AP of the validation of each IP address with a suggested status.

The host IP message element can be used in the process of binding migration. When migration occurs, the source device uses this message to report the MAC address and related IP addresses to the destination device, with suggestions for the status of each IP address. After the destination device checks the validity of the candidate binding, it replies using a message of the same format to inform the source device of the validity of each IP address with a suggested status.

The host IP message element can also be used in other scenarios when the synchronization between MAC-IP and IP-MAC mapping tables is required as specified in Section 3.5 and Section 4. When the synchronization from IP-MAC mapping table to MAC-IP mapping table is triggered, the source device which holds the IP-MAC mapping table reports the MAC address and the related IP addresses to the destination device which holds the MAC-IP mapping table using this message, with suggestions of the status of each IP address. 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)                     +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Address 2(32 bit)                     +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    ........                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Address n(32 bit)                     +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    IPv6 flag  |     Length    |        IPv6 Address...        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv6 Address 1(128 bit)                    +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv6 Address 2(128 bit)                    +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    ........                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv6 Address n(128 bit)                    +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |        blank       ...                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    lifetime                                   +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   BSSID flag  |     Length    |        BSSID...               +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     BSSID                                     +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 a description 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 and EUI-64 [EUI] 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 status (value 1 means available, value 0 means unavailable, value 255 means candidate), and a 32-bit value for lifetime. Lifetime is a reserved field for future application under abnormal conditions. 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, a DHCPv6-assigned IP address represented by value 3 and a locally assigned IP address represented by value 4.

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 status (value 1 means available, value 0 means unavailable, value 255 means candidate), and a 32-bit value lifetime. Lifetime is a reserved field for future application under abnormal conditions. All IPv4 and IPv6 addresses bind to the MAC address that appears before them in the message.

BSSID flag: An 8-bit value representing that the sub-field's type is BSSID, whose value is 5.

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

BSSID: A basic service set identifier representing the BSS.

5.1.1.5. Mobility Solution

When a host moves from one AP to another, layer-2 association happens before the IP packets are forwarded. The home AP deletes the binding when the mobile host is disconnected, and the foreign AP immediately requests the bound addresses with the associated MAC address from the AC. The AC returns the binding with a suggested status. After the foreign AP gets the addresses that should be bound, the binding migration is completed. The protocol used for communication between the foreign AP and the AC is the same as described in Section 5.1.1.4, while in this scenario, the AC serves the role of the source device and the 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 the home AC serves the role of the source device and the foreign AC serves the role of the destination device.

5.1.2. AC Filtering

In this scenario, an AC maintains both the MAC-IP and IP-MAC mapping tables and performs both address snooping and packet filtering. Therefore, all the packets must be forwarded to the AC first.

The AC executes the procedure specified in Section 3.3 and checks 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.

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

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

5.2. Autonomous WLAN

Autonomous WLAN is comprised of FAT access points. In this scenario, a FAT AP maintains both the MAC-IP and IP-MAC mapping tables and performs both address snooping and packet filtering.

The FAT AP executes the procedure specified in Section 3.3 and checks 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.

The 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 the home FAT AP serves the role of the source device and the 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 first.

7.1. 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, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

9.2. Informative References

[EUI] IEEE Standards Association, "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)", 2017, <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[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>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <https://www.rfc-editor.org/info/rfc7039>.

[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>.

Authors' Addresses

Jun Bi
Tsinghua University
Beijing
100084
China

Email: junbi@cernet.edu.cn

Jianping Wu
Tsinghua University
Beijing
100084
China

Email: jianping@cernet.edu.cn

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

Email: lintao@h3c.com

You Wang
Tsinghua University
Beijing
100084
China

Email: you@opennetworking.org

Lin He
Tsinghua University
Beijing
100084
China

Email: he-l14@mails.tsinghua.edu.cn