SAVI
Internet Draft
Intended status: Standard Tracks
Expires: May 2012

F.Shi
China Telecom
K.Xu, L.Zhu, G.Hu
Tsinghua Univ.

November 22, 2011

SAVI Requirements and Solutions for ISP IPv6 Access Network
draft-shi-savi-access-00.txt

Abstract

The Source Address Validation Improvement (SAVI) was developed to prevent IP source address spoofing which can enable impersonation and malicious traffic redirection. An Internet Service Provider (ISP) who provides Internet access services, information services and value-added services to the customers should guarantee security of its network and customers' privacy. Thus, the mechanism is essential for ISPs. However, due to a diversity of ISPs' access network, SAVI solution is also different accordingly. This document describes five scenarios of ISPs'IPv6 access network, and moreover, states its SAVI requirements and according tentative solutions.

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 http://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 May 22, 2012.

Copyright Notice

Table of Contents

1. Introduction

Spoofing of IP source addresses can jeopardize people's privacy,

enable malicious traffic redirection which causes the network topology and traffic information to be leaked out. Further, it will be difficult to trace the source host which forged the packet. The Source Address Validation Improvement (SAVI) method was designed to

prevent hosts attached to the same link from spoofing each other's IP address. It is developed to complement ingress filtering with finer-grained with standardized IP source address validation. It is also can be deployed easily in networks due to its modularization and extensibility.

ISPs have an imperative demand to apply the SAVI mechanism in order to ensure the network's security. Internet Service Provider has multiple access scenarios not limited to Ethernet, usually deployed with DHCP. Other scenarios such as ADSL with PPP, Ethernet with PPP are also popular in the real word. Unfortunately, SAVI Switch only works in the scenarios of wire or wireless Ethernet and not support all address assignment methods that be used in access network. There are four address assigned methods identified in one of the SAVI document:

1. Stateless Address Auto Configuration (SLACC) [I-D.ietf-savi-fcfs]

2. Dynamic Host Control Protocol address assignment (DHCP) [I-D.ietf-savi-dhcp]

3. Secure Neighbor Discovery (SeND) address assignment [I-D.ietf-savi-send]

4. Mix Address assignment methods [I-D.ietf-savi-mix]

Thus, According to different access network scenarios, SAVI should adjust its deployment and may need to promote and make improvement to adapt with the real situation. This note analyzes five scenarios of ISPs' IPv6 access network, and on this basis, gives according tentative SAVI solutions.

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].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

3. Scenarios for ISPs'IPv6 Access Network

It is important to note that the deployment of SAVI device was impacted greatly by access network scenarios and its address

assignment methods. There are various access methods for ISPs'IPv6 access network. In order to meet different IP Source Address Validation requirements, SAVI solutions may be need to be improved to adapt with the real situation.

There are five typical scenarios of ISPs'IPv6 access network:

1. Home gateway (HG) acts as DHCPv6 proxy.

2. Set Top-box (STB) gets IP address via DHCPv6.

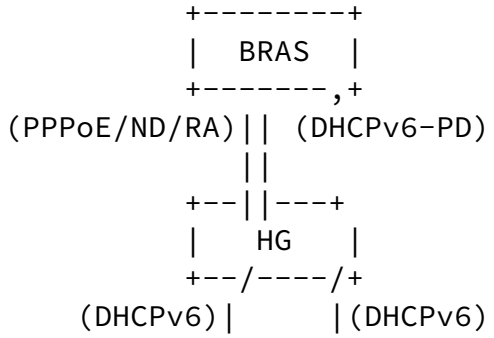
3. Host gets IP address via PPPoE & RA.

4. Laptop accesses Internet via WLAN.

5. Laptop accesses Internet via C+W.

We will discuss the SAVI solution for each scenario in detail in the next section.

3.1. Scenario 1: Home gateway (HG) acts as DHCPv6 proxy



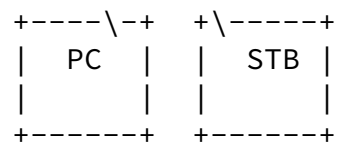
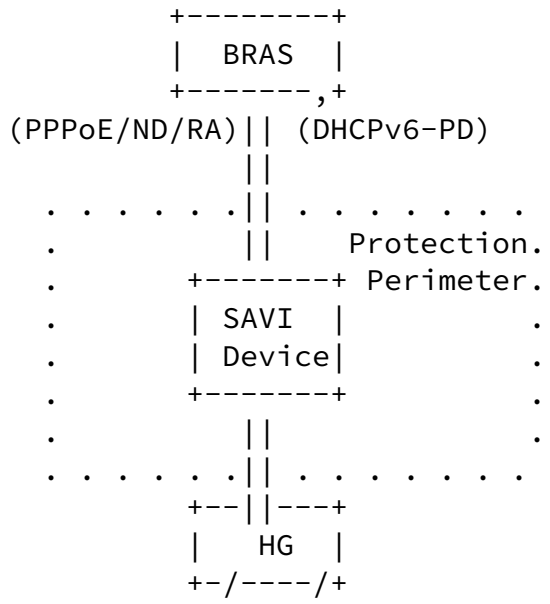


Figure 1: Scenario 1

Figure 1 shows the main elements in scenario 1. PC and STB connect to the Internet via HG. Its address assignment mechanism can be described as the following steps: First of all, HG gets a link-local IPv6-IPv6 address from BRAS via PPPoE and ND/RA. Then, HG gets IPv6 address from BRAS via DHCPv6-PD. At last, PC and STB get IPv6 address

from HG via DHCPv6. Of course, PC and STB can also get IPv6 address via ND/RA, but the DHCPv6 is much popular.

According to SAVI mechanism, in order to achieve Source Address Validation, the SAVI device must snoop the whole procedure of Address assignment. In addition, the preferred location of SAVI instances is close to hosts, such as in switches that directly attach to the hosts where host IP addresses are being validated [I-D.ietf-savi-framework]. So we can deploy SAVI device close to the HG in upstream direction. It can be illustrated by figure 2.



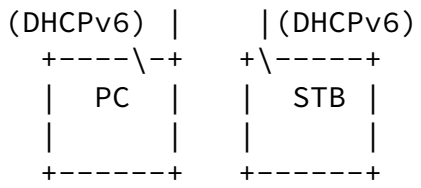


Figure 2: SAVI solution for Scenario 1

Figure 2 shows the deployment of SAVI device. It also allows multiple SAVI devices and non-SAVI devices co-exist on link. In addition, for this solution, SAVI mechanism needs to improve to snoop the procedure of DHCPv6-PD so as to bind the relationship <HG/PC/STB's address, port, MAC>.

3.2. Scenario 2: STB gets IP address via DHCPv6

The difference between scenario 1 and scenario 2 is the absence of HG which acts as DHCPv6 proxy. In scenario 2, STB which has internal

account and password gets IPv6 prefix by DHCPv6. The general scene workflow include the following steps: STB send requests to all routers on local link by using link-local address which based on its MAC address. The BRAS informs STB to adopt DHCPv6 address assignment method as a response. STB initiates DHCPv6 procedure and BRAS acts as a DHCP Relay to add some authorities' messages. AAA server decides whether assign address parameters depend on the result of authentication. At last, BRAS receives IPv6 parameters from AAA server, and then, informs STB via DHCPv6 protocol. It can be illustrated by figure 3.

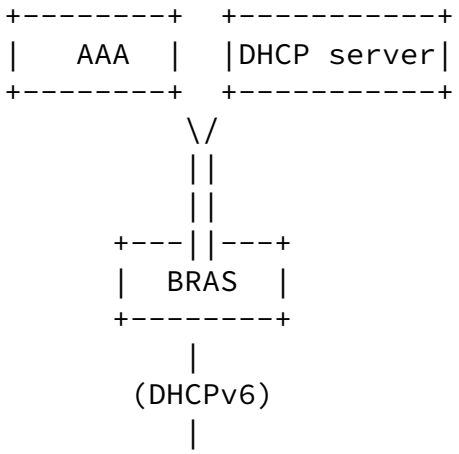


Figure 3: Scenario2

Figure 3 shows the main elements in scenario 2. Due to pure DHCPv6 address assignment method in this scenario, we can deploy SAVI device close to STB in upstream direction directly and SAVI mechanism needn't make any improvement. It just needs to bind relationship <STB's IP Address, port, STB's MAC Address> which is included in existing function. The solution can be illustrated by figure 4.

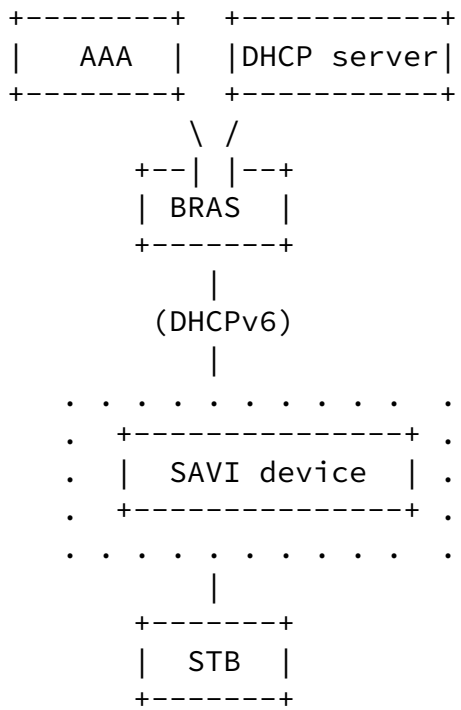


Figure 4: SAVI solution for Scenario 2

3.3. Scenario 3: PC gets IP address via PPPoE & RA

In this scenario, first of all, PC gets link-local address from BRAS via PPPoE. BRAS broadcast IPv6 prefix via RA. Finally, PC configures address automatically and gets some additional messages from BRAS.

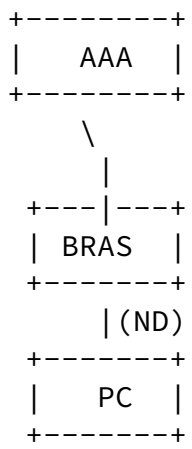
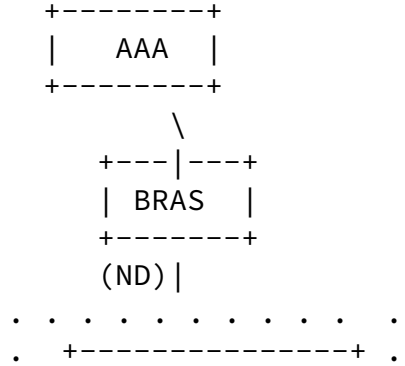


Figure 5: Scenario3

Figure 5 shows the main elements in scenario 3. Because the function of ND snooping has already been designed, we only take PPPoE snooping into account. Thus, the solution for this scenario which illustrated

by figure 6 is that deploying SAVI device directly and binding relationship <PC's IP Address, port, PC's MAC>. It is also need to improve its mechanism in order to enable PPPoE snooping.



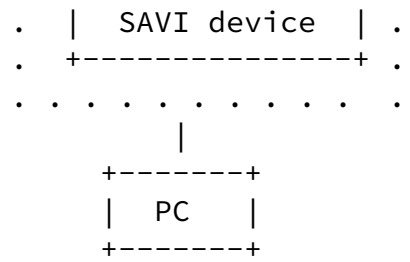


Figure 6: SAVI solution for Scenario 3

3.4. Scenario 4: Laptop accesses Internet via WLAN

The interaction in this scenario is simple relatively. The laptop gets IPv6 address via DHCPv6. Then, users were enforced to be certified by submitting password on a portal page.

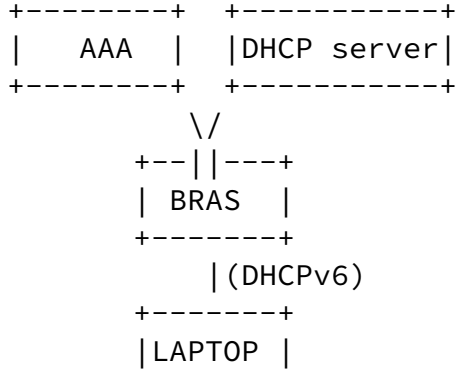


Figure 7: Scenario 4

Figure 7 shows the main elements in scenario 4. We can deploy SAVI device directly and bind relationship <LAPTOP's IP Address, port, LAPTOP's MAC>. The solution can be illustrated by figure 8.

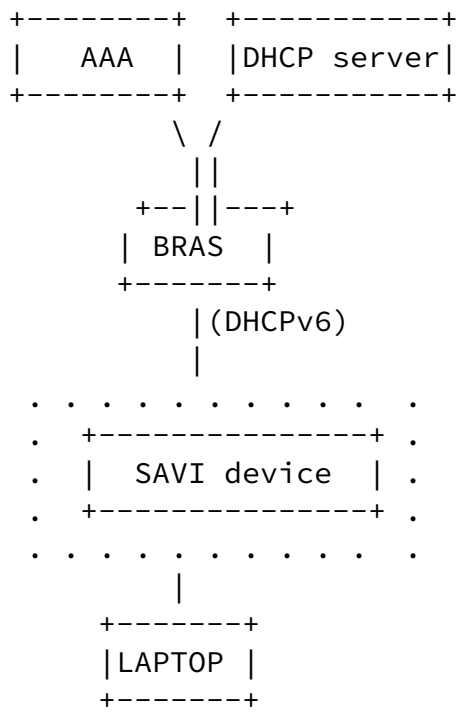


Figure 8: SAVI solution for Scenario 4

3.5. Scenario 5: Laptop accesses Internet via C+W

This scenario describes that the laptop accesses Internet via CDMA and WLAN. The general scene workflow include the following steps: The laptop gets a temporary IPv6 address from BARS via DHCPv6, and then,

obtains the WAG address from DNS server. The laptop establishes a UDP tunnel to WAG by sending register request. If the tunnel established successfully, the laptop can get IPv6 prefix from PDSN via PPP and RA, whereas PDSN acts as the PPP terminal. At last, the laptop gets some additional information such as DNS address. When the above steps all

accomplished, the laptop acquires the ability to access Internet.

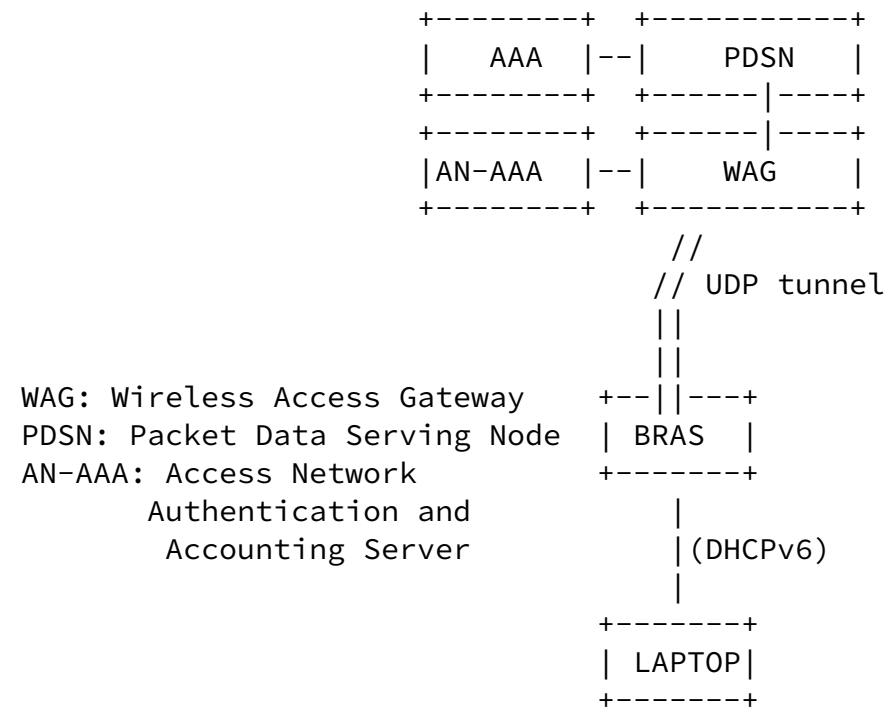


Figure 9: Scenario 5

Figure 9 shows the main elements in scenario 5. For this scenario, we also can deploy SAVI device at the position close to LAPTOP. SAVI needs to improve to support for PPPoE protocol snooping. It also binds relationship <LAPTOP's IP Address, port, LAPTOP's MAC>. The solution was described by figure 10.

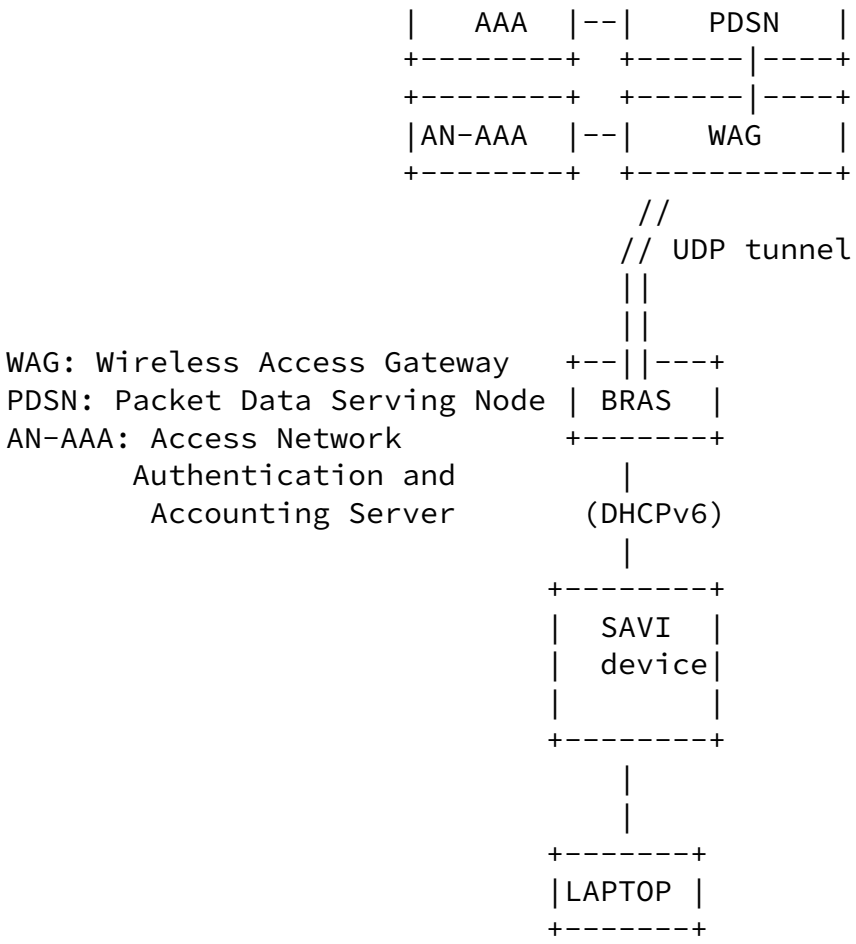


Figure 10: SAVI solution for Scenario 5

4. Conclusions

There are various scenarios of ISPs'IPv6 Access Network. Because each scenario uses different address assignment method and protocol, there are a variety of requirements to validate source address for ISPs' IPv6 access network. SAVI cannot support all protocols and methods right now, but, due to expansibility of SAVI, the mechanism can satisfy these various demands with a little improvement. This document presents five typical scenarios of ISPs'IPv6 access network, and proposes tentative SAVI solutions including some improvement.

5. References

5.1. Normative References

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

[I-D.ietf-savi-dhcp] Wu, J., Yao, G., Bi, J., and F. Baker, "SAVI Solution for DHCP", draft-ietf-savi-dhcp-10 (work in progress), July 2011.

[I-D.ietf-savi-fcfs] Nordmark, E., Bagnulo, M., and E. Levy-Abegnoli, "FCFSSAVI: First-Come First-Serve Source-Address Validation for Locally Assigned IPv6 Addresses", draft-ietf-savi-fcfs-09(work in progress), April 2011.

[I-D.ietf-savi-send] Bagnulo, M. and A. Garcia-Martinez, "SEND-based Source-Address Validation Implementation", draft-ietf-savi-send-06 (work in progress), October 2011.

[I-D.ietf-savi-framework] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, "Source Address Validation Improvement Framework",draft-ietf-savi-framework-05 (work in progress), July 2011.

6. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Fan Shi
China Telecom
Beijing Research Institute, China Telecom
Beijing, 100035
China
Email: shifan@ctbri.com.cn

Ke Xu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing, 100084
China
Email: xuke@mail.tsinghua.edu.cn

Liang Zhu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing, 100084
China
Email: tshbruce@gmail.com

Guangwu Hu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing, 100084
China
Email: hgw09@mails.tsinghua.edu.cn