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

K.Xu, G.Hu, J.Bi, M.Xu
Tsinghua Univ.
F.Shi
China Telecom

May 8, 2012

A general SAVI-based source address validation and traceback framework for 4over6 transition scenarios
draft-xu-savi-transition-01.txt

Abstract

Many proposals have been presented for preventing IP spoofing from occurring in network. An outstanding of them is the SAVI (Source Address Validation Improvement) proposal which was advocated by IETF SAVI workgroup for solving this problem from user access switch. SAVI Working Group is developing standardize mechanisms that prevent nodes attached to the same IP link from spoofing each other's IP addresses, and achieve IP source address validation at a finer granularity. However, up to now, to the best of our knowledge, none of them has focused on the scenarios of 4over6 transition, that is, IPv4 packets transit IPv6 network and arrive at other edge IPv4 network(s). With the boom of IPv6 networks, this issue becomes more and more urgent. In addition, since 4over6 plans are plenty and various, one solution cannot meet all requirements of these plans. This document describes a framework of IP source address validation and traceback for 4over6 transition scenarios, which extract out the essential and mutual properties from these plans and form corresponding sub-solution for each property. When one 4over6 plan is combined by some of them, the solution of IP source address validation and traceback for this plan are directly comprised of the combination of corresponding sub-solution. Thus, the most exciting advantage of this framework is that it is a once for all solution no matter how 4over6 plans changes.

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 November 8, 2012.

Table of Contents

1. Introduction

The issue of IP source address spoofing has become very serious in recent years. According to the IP spoofer project of MIT, the proportion of spoofable netblocks, IP addresses and autonomous systems are 14.6%, 16.3%, 23.9%, respectively [MITSpoofer]. This was result from the absence of intrinsic mechanism of IP source address validation. Encouragingly, this issue was noticed gradually by many researchers and lots of excellent solutions were proposed. One of them is the SAVI [SAVI] (Source Address Validation Improvement) scheme which is proposed by IETF SAVI workgroup. The mechanism of it is binds host's IP, MAC address, uplink port in the user access switch. The switch which followed the SAVI proposal, namely SAVI Switch, eliminates this issue in the first-hop of packets. Binding function in SAVI Switch is automatically accomplished by snooping IP address assignment protocols, e.g. DHCPv6, SLAAC. Thus, It is more accurate and effective than the URPF [RFC3704] (Unicast Reverse Path Forwarding) proposal because it takes effect in the position of user's access switch rather than access router. According to the charter of SAVI workgroup, it would cover wire/wireless Ethernet network, and both protocols of IPv4 and IPv6 as well. Till now, various commodity SAVI Switch products have already been implemented by lots of network equipment providers, for instance, Huawei, ZTE etc.

On the other hand, since bothered by stubborn issues of IPv4 Internet, including exhaustion of IPv4 address, people gradually turn their attention from IPv4 to IPv6 Internet. Most ISPs are progressively developing their IPv6 networks and lead to IPv6 Internet presents a rapid development trend in recent years. However, in a short period, traditional IPv4 Internet will not disappear very soon, on the contrary, it will still take the dominated position for a long time with the reason of man-power, money cost and so on. In other words, two kinds of networks will be coexistence for a period. In view of this situation, plenty of schemes for promoting intercommunication between the two networks have been proposed, such as IVI[RFC6219], DS-Lite[RFC6333], 4RD[4RD], A+P[RFC6346] and Public 4over6[p4over6]. In the light of work mode, they are categorized into three types: dual-stack, translation and tunnel. In terms of tunnel technology, it

is also known as "softwires"[RFC5565] which provides packet transit service from one edge of single-protocol network to other.

Even though there are many mature and practical solutions for validating IP source address in single-protocol networks. Unfortunately, to the best of our knowledge, solutions for IP source address validation and traceback in the scenario of IPv4/IPv6 coexistence are not been researched yet. Besides, since the transition plans are plenty and various, it's not practical to proposal a source address validation scheme for each transition plan, and it's not possible to find a solution to satisfy all requirements of these plans either.

So the transition issue becomes more and more urgent, the matter of source address verification in this scenario is also important as well. With the rapid development of IPv6 network, we have reason to believe that IPv6 Internet will become the solo backbone eventually. But before this, the situation of IPv4 packets transit IPv6 network and arrive at other edge IPv4 network(s), namely 4over6 transition, will exists for a long period.

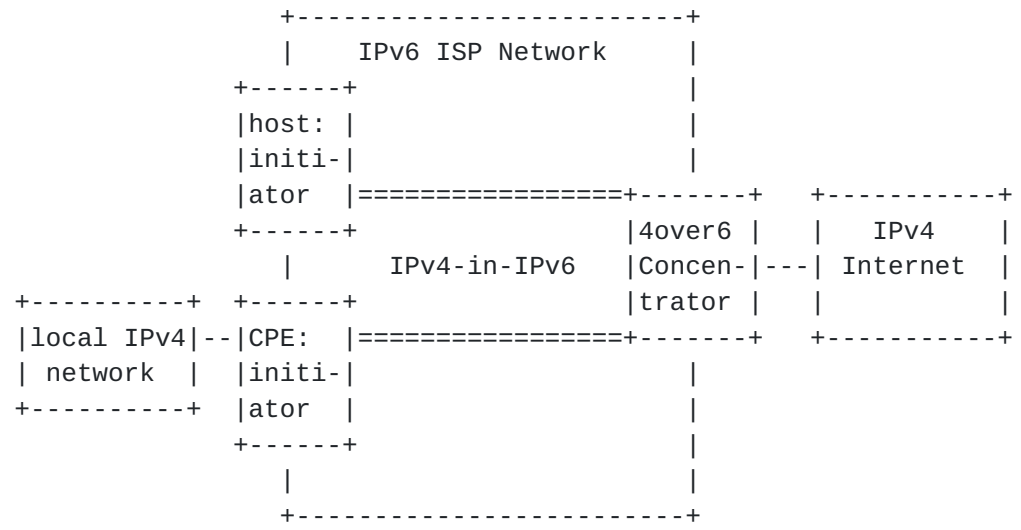

Figure 1 The overview of Public 4over6 transition scenario

Figure 1 shows a class 4over6 transition scenario, which is described in Public 4over6 plans. The 4over6 Concentrator acts tunnel end-point receives packets from 4over6 tunnel initiators and forwards them into IPv4 Internet, while the CPE (Customer Premises Equipment) performs as a tunnel broker for solo-stack 4over6 host. The 4over6 host in the IPv6 network is tunnel initiator for itself. This document focuses on how to setup a general SAVI-based framework to validate and traceback IP source address in 4over6 transition scenarios.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Framework description

In this section, we will describe this framework in detail. But ahead of this, introducing design goals and considerations will benefit for readers to well-known our minds.

3.1. Goals and considerations of this framework

Goal 1. This framework focuses on the 4over6 transition scenarios with tunneling mechanism.

Goal 2. This framework should have the ability of source address verification, and also the traceback function for given address.

Goal 3. This framework could adapt all of 4over6 transition plans, no matter how much scenarios change.

To keep packets carry with trusted IP source address, it should let the packets comes from the authorized user who is the owner of packet's source address, and prevent spoofed packets from forwarding. Naturally, deploying SAVI Switch into users' access subnet to keep all of hosts' trustiness is one of straightforward ideas. Furthermore, it has to record mapping table in each place where source address could be changed (e.g. NAT). Such ideas would directly facilitate the implementation of traceback function, and the only thing that system needs to do is reverse trace based on the given IP source address.

Another basic idea for fulfilling the third goal is extract essential and mutual properties from these transition plans and form corresponding sub-solution for each property. When one 4over6 transition plan is combined by different properties, the solution of IP source address validation and traceback for this plan naturally is the combination of the corresponding sub-solution.

3.2. Property extraction

Requiring one framework to adapt all 4over6 transition plans is difficult. After investigated almost all of these plans, we found that there existing basic common properties in them. Therefore, if we can extract these properties from these plans and restore them by

reassembling required properties afterward, this would provide the possibility for establishing such framework. Actually, this has been achieved based on three property extraction rules: 1) it only extract those common and essential elements, and don't care the irrelevant details; 2) Each element shouldn't be decomposed any further, in other words, each element should be atomic and unique; 3) It should have the ability of plans-reconstruction by reassembling relevant elements. The result of property extraction is illustrated as Table I.

Table I. Properties in 4over6 plans

Property Group	Group Code	Property Name	Value
Protocol stacks of 4over6 host	A	Dual-Stack	A1
		IPv4 only	A2
Relationships between IPv4 and IPv6 Address	B	Stateless	B1
		Stateful	B2
Forms of 4over6 hosts' IPv4 address	C	Private	C1
		Public	C2
		Public with Port Sharing	C3
		Private with Port Sharing	C4
Positions of NAT device	D	Near to CPE	D1
		Near to CGN AFTR	D2
		D1 & D2	D3

CGN: Carrier-grade NAT
AFTR: Address Family Transition Router

We summarized these properties into four categories with eleven items. Group B indicates the relationship between IPv4 and IPv6 address in 4over6 host, stateless means they are related since they can be deduced by each other, otherwise, it's stateful. Property C3 and C4

states multi-4over6 hosts share an IPv4 address by splitting port-range. The description for NAT position belongs to group D. Property D1, D2 and D3 declares the NAT devices in the position of border of user local network, ISP's network in IPv4 Internet, and both sides, respectively.

3.3. Measurements for IP source address validation

Table II. Measurements of Source address validation for each property

Property Name	Value	Measurements in SAVI Switch
Dual-Stack	A1	<IPv4, IPv4, MAC, Switch-Port>
IPv4 only	A2	<IPv4, MAC, Switch-Port>
Stateless	B1	Depends on property A
Stateful	B2	Depends on property A
Private	C1	Depends on property A
Public	C2	Depends on property A
Public with Port-S	C3	property A & port-range
Private with Port-S	C4	property A & port-range
Near to CPE	D1	
Near to CGN AFTR	D2	Recording the NAT-Table
D1 & D2	D3	

As we mentioned, the goal of IP source address validation is to keep packets bring with trustful IP source addresses, and this is also the basis of traceback and other applications. SAVI Switch binds <IP, MAC, Switch-Port>, the triad-relationship of end-host to achieve this goal, but till now, it's only applicable for single-stack network (IPv4 or IPv6), which means SAVI Switch needs to be improved to adapt dual-stack and other complex scenarios. Although we can enumerate all possibilities of property combinations, and consider how to improve

it to adapt to each scenario, it's not a smart choice because of its inflexibility and violation with the third goal. In contrast, we list out the measurements of source address validation for each property, as illustrated in Table II. We hope to obtain source address validation solution for each 4over6 plan by reassembling corresponding measurements.

Table III. Measurements of Source address validation for property combinations

Index	Combination	4over6 Plans	Measurements in SAVI
1	A1-B1-C1/C2/-(D1/D2/D3)	Dual-Stack with stateless scenario in Public 4over6	<IPv6, MAC, Switch-Port, IPv4>
2	A1-B1-C3/C4/-(D1/D2/D3)	Dual-Stack with stateless scenario in Light-Weighted Public 4over6	<IPv6, MAC, Switch-Port, IPv4, Port-Range>
3	A1-B2-C1/C2/-(D1/D2/D3)	Dual-Stack with stateful scenario in Public 4over6	<IPv6, MAC, Switch-Port> Concentrator verifies relationship of <IPv6,IPv4>
4	A1-B2-C3/C4/-(D1/D2/D3)	Dual-Stack with stateful scenario in Light-Weighted Public 4over6	<IPv6, MAC, Switch-Port> Concentrator verifies relationship of <IPv6,IPv4,port-R>
5	A2-(B1/B2)-(C1/C2/C3/C4)-(D1/D2/D3)	DS-Lite; 4RD; A+P; Solo-Stack scenario in Public 4over6; Solo-Stack scenario in Light-Weighted Public 4over6	<IPv6, MAC, Switch-Port,(Port-Range)>

As we explain previously, property stateless or stateful only decides the relationship between IPv4 and IPv6 address for 4over6 hosts. Hence, they have no particular treatment and their measurements

depend on property A1 or A2. Property group C manifests the status of IPv4 address, no matter the address is private or public, measurements for them are all decided by property group A (C1 and C2). However, if it's the situation of multi-hosts shares an IP address by multiplexing its port, measurements should bind the address along with its port-range as well, e.g. C3,C4. Property group D needs no extra considerations except recording the NAT-Table for traceback function.

Table III list out measurements of source address validation for property combinations, in the column of ''Combination'', the notation ''- '' means relation-union, and the slash notation means choose anyone of them, while the bracket notation states optional relationship. Take the combination of A1-B1-C1/C2-(D1/D2/D3) as example, it indicates that property item A1 combine with B1 firstly, and then they union with C1 or C2 either, following result can be proceed in further with anyone of property in group D, but it's optional rather than compulsive.

There have extra two explains about Table III. In the scenario of dual-stack and stateful (row-index 3, 4), which means end-host has both IPv4 and IPv6 address and they are unrelated, we did not require SAVI Switch to bind IPv4 address with other information, even though how much we want to do this for reducing the verification process in 4over6 Concentrator. However, considering the performance of SAVI Switch and the fact of request a Layer2.5 switch to parse DHCPv4 messages from upper tunnel protocol is inappropriate, the alternative approach is forcing 4over6 Concentrator to verify the mapping-relationship. Another point we want to point out is the last row of this table, SAVI Switch in IPv4 network only has to bind illustrated relationship without any improvement.

3.4. Measurements for IP source address traceback

Traceback function means administrator can locate the original senders of suspicious packets. To achieve this goal, IP source address in every packet should be authentic and trustful. This can be implemented by authenticating sender in SAVI Switch and recording IP mapping-table in each NAT place, and finally, administrator can find out the sender by tracing the reverse path from the receiver to the sender. Table IV presents the individual measurement in detail for each property.

Table IV. Measurements of Traceback for each property

Value	Measurements
A1	Queried IPv4 address->deduce(stateless) or look up table(stateful)->IPv6->locate
A2	Only with B1 together: extend IPv6 header to include IPv6 address of CPE, and Concentrator saves the map-ping-relatioship of tunnel interface and CPE's IPv6
B1	IPv6 address is deduced by queried IPv4 address.
B2	IPv6 address is obtained from IPv4-IPv6 mapping-table in 4over6 Concentrator
C1	Depends on A
C2	Depends on A
C3	Take port number with IPv4 address as condition to query binding status table in SAVI Switch
C4	Same with C3
D	Take queried IPv4 address as condition to retrieve original IPv4 address by looking up NAT table

When property A2 combines with property B1, there is a special treatment for this condition. In this scenario, since tunnel initiator's address is the 4over6 host's IPv4 related IPv6 address, rather than CPE's IPv6 address. Therefore, there exists a very tough problem for traceback, that is, how to locate CPE device in 4over6 Concentrator even if we already have the corresponding IPv6 address for a given IPv4 address. It will become easy if 4over6 Concentrator has the relationship of CPE's and tunnel initiator's address. Once the corresponding IPv6 address is obtained either by deduce or look up mapping-table in NAT for a given IPv4 address, we can locate CPE device by searching the mapping-table. We will give the detail about it in next section.

As to the question of how to extend IPv6 header to achieve this goal, that's a minor issue which we will not discuss it here in detail.

Actually, this can be realized by creating a new option in IPv6 destination header.

Table V. Trace-Paths for property combinations

Index	Combination	4over6 Plans	Track Path
1	A1-B1-C1/C2/-(D1/D2/D3)	Dual-Stack with stateless scenario in Public 4over6	Queried IPv4 -> (pre-translate IPv4(via D2)-> IPv6(via deduce) -> locate sender
2	A1-B1-C3/C4/-(D1/D2/D3)	Dual-Stack with stateless scenario in Light-Weighted Public 4over6	Equal to row index 1
3	A1-B2-C1/C2/-(D1/D2/D3)	Dual-Stack with stateful scenario in Public 4over6	Queried IPv4 -> (pre-translate IPv4(via D2)-> IPv6(via look up table)->locate sender
4	A1-B2-C3/C4/-(D1/D2/D3)	Dual-Stack with stateful scenario in Light-Weighted Public 4over6	Equal to row index 3
5	A2-(B1/B2)-(C1/C2/C3/C4)-(D1/D2/D3)	DS-Lite; 4RD; A+P; Solo-Stack scenario in Public 4over6; Solo-Stack scenario in Light-Weighted Public 4over6	Queried IPv4 -> (pre-translate IPv4(via D2)-> IPv6(via look up table)->locate CPE ->(pre-translate IPv4 (via D1))->locate

In addition, another very key issue is that there is a SAVI management database which collects information from all of SAVI Switches in intra-domain by SNMP protocol, including binding status table and other important data. Thus, by consulting this database with a given IP address, we can learn that the owner of this address uplinks to which port and which SAVI Switch. With the database's help, locating a host from its IP address is pretty easy.

Table V illustrates the trace-paths for property combinations. Taking first row in the table as example, we try to locate the sender of a packet with queried IPv4 source address in IPv4 Internet. If there has a CGN device in the boundary of IPv4 Internet and IPv6 network, looking up the NAT mapping-table to retrieve the pre-translation IPv4 address is the first step. Since it's the dual-stack and stateless scenario, the corresponding IPv6 address can be deduced based on IPv6 and IPv4 address conversion rule, and 4over6 host uses its own IPv6 address as tunnel initiator to forward its IPv4 packets to 4over6 Concentrator. Finally, the sender will be located by consulting SAVI management database based on sender's IPv6 address.

4. Framework verification

In this section, we will apply this framework into some famous 4over6 transition plans to verify its correctness, such as DS-Lite, Public 4over6, Light-Weighted Public 4over6[l4over6], 4RD and A+P etc.

4.1. Public 4over6

Packet with public IPv4 address over access IPv6 network, namely public 4over6, is a mechanism for bidirectional IPv4 communication between IPv4 Internet and end-hosts or IPv4 networks sited in IPv6 access network. This mechanism follows the softwire hub and spoke model and uses IPv4-over-IPv6 tunnel as basic method to traverse IPv6 network.

Fig.1 shows the general working scenarios of Public 4over6. There are two types of tunnel initiator: host and CPE initiator. Part of 4over6 hosts in IPv6 network use their own IPv6 address to establish tunnel with 4over6 Concentrator and forward IPv4 packets for themself, while other 4over6 hosts in local IPv4 network need CPE to be their initiator to encapsulate and forward their IPv4 packets.

Public 4over6 also has stateful and stateless two address forms. The difference among them is that the stateless mode takes IPv4-embedded IPv6 as tunnel initiator's address, while the stateful mode means the two addresses, IPv4 address for 4over6 host and IPv6 address for tunnel initiator, have no relationship with each other, so that 4over6 Concentrator needs to save the mapping relation to provide correct forwarding.

Two types of initiators with two address forms, that are four scenarios, we analyze them as follows.

Scenario 1: Solo-Stack with stateless (A2-B1-C2)

The 4over6 host in stateless mode has only IPv4 address, while CPE in the border of local IPv4 network plays the role of tunnel initiator and protocol proxy. When CPE receives a DHCPv4 request from local 4over6 host, it will convert it to DHCPv6 request and forward it to DHCPv6 server in IPv6 access network [DHCPv6-map], afterwards, the server then fetches an IPv4 address from IPv4 address pool randomly and produce a DHCPv6 reply which follows the address conversion rules, then finally, CPE will equip this IPv6 address and parse IPv4 address from it for producing DHCPv4 to reply to the requestor. Otherwise, when CPE receives an outbound data packet, it will take the mapped IPv6 of IPv4 source address in this packet as tunnel initiator's address and encapsulate them into tunnel (e.g. GRE), 4over6 Concentrator receives and decapsulates packets from tunnels and forward them to next-hop.

SAVI Switch should to snoop the DHCPv4/PCP protocols interaction and bind the relationship of <IPv4, MAC, Switch-Port>, which mentioned in Table III with combination of A2-B1-C2.

Translating the queried IPv4 address to IPv6 address by address conversion rules, tracking the CPE device by looking up the address mapping-table of CPE and tunnel initiator in 4over6 Concentrator, consulting SAVI management database and locating the sender are the three phrases of traceback, respectively.

Scenario 2: Dual-Stack with stateful (A1-B2-C2)

In order to access both IPv4 and IPv6 resources, this type of 4over6 hosts own IPv4 and IPv4 unrelated IPv6 addresses, IPv6 address is allocated by traditional way such as DHCPv6 or SLAAC in IPv6 network, however, IPv4 address is assigned by DHCPv4 server in IPv4 Internet with the way of DHCPv4 over IPv6. For purpose of anti-spoofing in users access subnet, naturally, we maybe consider SAVI Switches snoop address assignation protocols, i.e. DHCPv6, PCP, and bind the relationship of <IPv4, IPv6, MAC, Switch-Port> for each 4over6 host. However, given the ability of parse DHCPv4 protocol from upper layer in a layer2.5 switch, we turn to 4over6 Concentrator for help by verifying the address mapping relationship instead of bind two kinds of address together in access SAVI Switch.

Finding the initiator's IPv6 address for suspicious IPv4 address in 4over6 Concentrator and locating the sender directly are the two steps of tracking sender.

Scenario 3: Solo-Stack with stateful (A2-B2-C2)

In this scenario, 4over6 host in IPv4 network only owns a public IPv4 address with the way of DHCPv4 overt IPv6, and CPE uses its own IPv6 address as tunnel initiator for forwarding packets from these hosts. Thus, there is no need to extend IPv6 header for saves the mapping relationship between CPE and initiator's IPv6 address in 4over6 Concentrator to. Except the step of look up mapping-table for locating CPE is reduced, the rest of parts in traceback function are same as scenario one, as well as the binding processes.

Scenario 4: Dual-stack with stateless (A1-B1-C2)

This type of 4over6 host has both IPv4 and IPv6 addresses, and they are related. These hosts take their own IPv6 addresses as tunnel initiator for forwarding IPv4 packets from themself. Their SAVI Switches bind the relationship of <IPv6, MAC, Switch-Port> for anti-spoofing. The slight difference in trace-back between scenario 2 and this scenario is the way of obtain related IPv6 address of queried IPv4, which is finished via deduce, rather than search the mapping-table in concentrator.

4.2. Lightweight public 4over6

Compared with Public 4over6 plan, there is a slight change between these two plans in the form of IPv4 address. Briefly, lightweight public 4over6 mitigates IPv4 address exhaustion by sharing public IPv4 addresses amongst hosts with different port range, and this can be achieved by extending DHCPv4 and PCP protocol, while hosts in public 4over6 own their unique public IPv4 address. The two transition plans are similar except replace C2 with C3 property for each scenario. Validating and traceback process could be referred to Table III and V.

4.3. DS-Lite

Dual-Stack lite also is a transition plan which encapsulates IPv4 packets over IPv6 access network. NAT function is performed in CGN device to provide IPv4 address translation from private to public. It

allows single public IPv4 address to be shared by multi-requestor to increase port utilization.

We treat DS-Lite is the property combination of Dual-Stack, stateful, private IPv4 address and NAT in CGN, that is A1-B2-C1-D2. According to the rules, the access SAVI Switch of CPE (home gateway) should bind its IPv6, MAC address and uplink port together. Since the NAT and tunnel information are all in the NAT-Table together, the trace path should follow the direction from queried IPv4 address to tunnel-id by looking up NAT-Table, and then locate CPE device in user's household by following the tunnel information.

4.4. 4RD

IPv4 Residual Deployment (4RD) is a mechanism to facilitate IPv4 residual deployment across IPv6 networks of ISP's. It is equal to reverse of 6RD[12] (IPv6 Rapid Deployment on IPv4 Infrastructures, 6over4 plan), scenario 3 in Public 4over6 as well. And it also can be treated as DS-Lite plan without CGN NAT. Thus, measurements for validation and traceback could be referred to previous section.

4.5. A+P

Address plus Port(A+P) approach is advocated by France Telecom, Nokia and other companies for the purpose of IPv4 shortage and 4over6 transition. A+P treats some bits from the port number in the TCP/UDP header as additional end-point identifiers to extend the address field. It solves the problem of public IPv4 address shortage for CPE. The PRR (Port Range Router) assigned one public IPv4 address to two CPEs with different port-ranges. CPE plays the role of NAT for allocating private address to local hosts, as well as tunnel initiator for encapsulating IPv4 packets across IPv6 network.

A+P can be considered as property combination of A2-B2-C1-D1. Therefore, access SAVI Switch needs to bind IPv4 address and other information which is illustrated in Table V. When we perform traceback function, we need to take IPv4 address along with its port-number to obtain tunnel information in PRR, and then locate CPE based on this information and lock the 4over6 host further.

5. Conclusions

Along with the rapid development of IPv6 networks and urgent demand of inter-communication between IPv4 and IPv6 networks, the situation of packets from IPv4 network transit IPv6 Internet (networks) and arrive at other edge IPv4 networks is inevitable, this is also refer

to 4over6 transition. Under this circumstance, a lot of 4over6 transition plans for various scenarios are proposed.

On the other hand, the stubborn issue of IP source addresses spoofing still bothers network users and administrators, and once it happened, it's hard to trace the spoofer. The SAVI proposal, one of excellent solutions for source address validation, is advocated by IETF SAVI workgroup. SAVI Switch follows SAVI proposal and automatically binds <IP, MAC, Switch-Port> and even other information for access hosts to achieve the goal of prevent nodes attached to the same IP link from spoofing each other's IP addresses.

Applying SAVI Switch into 4over6 transition scenarios and proposing a framework adapts all of 4over6 transition plans for source address validation and traceback are our goal. In this document, in the first beginning, we state the background and urgent demands of IPv4-over-IPv6 transition, as well as the necessity of source address validation and traceback. After that, we sort out property groups and items in detail by fully investigating 4over6 transition plans. Moreover, we present the solutions of source address validation and traceback for each property item and even property combination. We give the reasonableness of these solutions and explain how to apply this framework into property combinations. Followed framework verification for most famous 4over6 transition plans proves the excellent adaptability and flexibility in our framework.

Although this framework particular highlights the 4over6 transition scenarios and only was verified in most existing 4over6 transition plans, we still emphasize that it is not only suits for 4over6 transition scenarios, but also other transition situations such as 6over4 and even translation transition with only slightly improvement. We hope that it will be improved with more consideration in future for adapting more transition scenarios and achieving the goals of IP source address validation and traceback.

6. References

6.1. Normative References

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

[MITSpoofer] MIT Spoofer project http://spoofer.csail.mit.edu/summary.php.

[SAVI] J.Wu,J.Bi etl, ''Source Address Validation Improvement Framework (SAVI) draft-ietf-savi-framework-06'', Internet-Draft, December 2011.

[RFC3704] F. Baker,P. Savola, ''Ingress Filtering for Multihomed Networks'', RFC3704, March 2004.

[RFC6219] X.Li, C.Bao etl, ''The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition'', RFC6219, May 2011.

[RFC6333] A.Durand,R.Droms,J.Woodyatt etl, ''Dual-Stack Lite Broadband Deploy-ments Following IPv4 Exhaustion'', RFC6333,August 2011.

[4RD] R. Despres, Ed., S. Matsushima, T. Murakami etl, ''IPv4 Residual Deployment across IPv6-Service networks (4rd) ISP-NAT's made optional draft-despres-intarea-4rd-01'', Internet-Draft, March 2011.

[RFC6346] R. Bush, Ed, ''The Address plus Port (A+P) Approach to the IPv4 Address Shortage'', RFC6346, August 2011,

[p4over6] Y.Cui, J.Wu, P.Wu, C.Metz, O.Vautrin, Y.Lee, "Public IPv4 over Access IPv6 Network draft-cui-softwire-host-4over6-06", Internet-Draft, July 2011

[RFC5565] J.Wu, Y.Cui, C.Metz, E.Rosen, ''Softwire Mesh Framework'', RFC 5565, June 2009.

[l4over6] Y.Cui, J.Wu, P.Wu, Q. Sun, C. Xie, C. Zhou, Y.Lee, " Lightweight 4over6 in access network draft-cui-softwire-b4-translated-ds-lite-04", Internet-Draft, Oct. 2011

[DHCPv6-map] T. Mrugalski, M. Boucadair, O. Troan, X. Deng, C. Bao, "DHCPv6 Options for Mapping of Address and Port draft-mdt-softwire-map-dhcp-option-01'', Internet-Draft, Oct. 2011

7. Acknowledgments

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

Authors' Addresses

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

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

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

Jun Bi
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China
Email: junbi@tsinghua.edu.cn

Mingwei Xu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
China
Email: xmw@csnet1.cs.tsinghua.edu.cn