SAVI
Internet Draft
Intended status: Standard Tracks
Expires: November 2013

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

May 7, 20133

A General Framework of Source Address Validation and Traceback for IPv4/IPv6 Transition Scenarios

draft-xu-savi-transition-03.txt

Abstract

IP spoofing always is bothering us along with the Internet invention. With the rapid development of IPv6 next generation Internet, this issue is more prominent. Though many studies have made their contributions to the prevention of IP-spoofing, the most excellent one is the SAVI (Source Address Validation Improvement) proposal advocated by IETF, since it can prevent IP-spoofing from happening by automatically binding the key properties of hosts in layer2 access subnet. Nevertheless, till now, SAVI only focuses on the IPv6 stack and simple network access scenarios. To the best of our knowledge, there is no solution even has paid attention to IPv4/IPv6 transition scenarios. Given the fact that IPv4/IPv6 transition will continue to be adopted for a long period of time, this issue is becoming increasingly urgent. However, since transition schemes are plenty and diverse, hardly can an ordinary solution satisfy all the requirements of various transition scenarios. In this document, we present an improved general SAVI-based framework of IP source address validation and traceback for IPv4/IPv6 transition scenarios. To achieve this goal, we extract essential and mutual properties from these transition schemes, and create sub-solutions for each property. Naturally, if one transition scheme is proposed by combining some properties, the corresponding sub-solutions would be included into its IP source address validation and traceback solution. Therefore, the advantage of this framework is its capability to adapt to all the transition schemes.

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.

Copyright Notice

Table of Contents

1. Introduction 3
2. Conventions used in this document 5
3. Framework description 5
   3.1. Property Extraction 5
   3.2. Solutions of IP source address alidation 7
   3.3. Solutions to IP source address traceback 10
4. Framework verification..... 13
   4.1. Public 4over6 13
   4.2. 6RD 14
   4.3. DS-Lite 14

4.4. 4RD 15
4.5. A+P 15
4.6. IVI 15
5. Conclusions 16
6. References 16
6.1. Normative References..... 16
7. Acknowledgments 18

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]. CAIDA also proves that U.S. and China are major victim countries of IP spoofing attack[CAIDA]. 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.

Due to the limitations of IPv4 Internet, e.g. the shortage of IPv4 addresses, people have gradually turned to IPv6 Internet. Most ISPs are developing their IPv6 networks, helping the IPv6 Internet present a rapid trend of development in recent years. However, there are reasons, especially the difficulty of the IPv6 deployment and the small percentage of IPv6 Internet traffic (1%), indicating that traditional IPv4 Internet will not be replaced in the near future, which means that these two kinds of networks will be coexistent for a period of time. In the view of this situation, plenty schemes to promote inter-communication between the two networks have been proposed. Based on the working mode, transition plans can be

categorized into three types: dual-stack, tunnel and translation. Dual-stack is actually two single stacks used by users simultaneously, so its anti-spoofing solution is to combine the two single stacks' anti-spoofing methods. In terms of the tunnel technique, it is also known as "softwires"[RFC5565], which provides packet transit service from one edge of the single-protocol network to another by means of encapsulating and de-capsula-ting packets. Specifically, there are two scenarios-4over6 and 6over4 tunnels. Hereby, 4over6 refers to the scenario of the local edged network which applies IPv4 stack and the ISP backbone that uses IPv6 stack, whereas 6over4 is the opposite situation. Well-known tunnel proposals include 6RD[6RD], DS-Lite[DS-Lite], 4RD[4RD], A+P[A+P], Public 4over6[Public4over6] etc. As to translation, the core idea is the packet header conversion between the two protocol stacks, and the classic scheme of this catagory is the IVI proposal[IVI]. Therefore, the idea of anti-spoofing is to maintain packet trustiness in each single-stack network.

Although many mature solutions have achieved the goal of validating IP source address or even traceback in single-stack networks, to the best of our knowledge, solutions for the same purpose to IPv4/IPv6 transition scenarios have not been found out yet. Furthermore, transition schemes are proposed by different institutions based on their individual demands. Thus, the biggest challenge of anti-IP-spoofing is that, it is too hard to develop a general solution to meet various requirements of various transition scenarios. After investigating almost all the transition schemes, especially the tunnel ones, we find that there are basic and common properties among them, such as the relationship between IPv4 and IPv6 addresses, the position of NAT device, etc. Then, we extract these essential properties from transition schemes, and form sub-solutions for each property based on SAVI improvement which can be adapted to two stacks and more complex transition scenarios. Finally, when one scheme is constituted by required properties, its source address validation and traceback solutions are combined by corresponding sub-solutions. Thus, the goal of this paper is to propose a general and feasible framework of IP source address validation and traceback that can satisfy all the requirements of transition schemes, no matter how they will change.

Since authors of this draft participate in both SAVI and Softwire IETF workgroup long-termly, we naturally used the ideas of SAVI to achieve it. Like we mentioned, our purpose is present a feasible general anti-spoofing framework for transition scenarios and give more inspiration to interested people, but limited by the uncontrollable factors, like personal privacy, law permission, implementation detail, framework's performance evaluation, expanding SAVI out of LAN environment or not, we will not refer to.

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 firstly give the threat model and considerations, and then describe the framework in detail.

The threat model in this paper means that the fields in an IP packet can be modified with imposters' willingness to achieve their expected purpose, and it's hard to locate them since the source IP addresses have been modified. But we believe the network devices (NAT devices, tunnel points, protocol translator, etc.) are trustful, then attackers cannot manipulate them. Otherwise, the situation will become very complex, and it's beyond our discussion in this paper. To keep packets carried with the trusted IP source address, the packets should come from an authorized user who possesses the packet's source address, and spoofed packets must be prevented from being forwarded. Naturally, we will first deploy SAVI Switches into users' access subnets to keep the credibility of all hosts. Furthermore, we need NAT (Network Address Translation) devices to record the mapping relationship between addresses before and after translation. Such ideas could directly facilitate the implementation of the traceback function.

3.1. Property Extraction

Extracting essential and common properties from transition schemes has been achieved based on three property extraction rules: (1) It only extracts essential elements and does not take irrelevant details into account; (2) each element will not be further decomposed (in other words, each element should be atomic and unique); (3) transition schemes can be reconstructed by reassembling required elements. We have summarized these properties into four categories with 12 items, which is illustrated in table I.

Property group A states the protocol stacks of the source-host actual use, rather than the access-network (we presume source-host can support both IPv4 and IPv6). The ''stateless'' in Group B means that the relationship between the IPv4 and IPv6 addresses of source-host is related since they can be deduced to each other, while the ''stateful'' declares that the two kinds of addresses has no relation

so that the tunnel point needs to save the mapping records for forwarding. Property items C3 and C4 describe the scenario where multi-hosts share one IPv4 address by splitting the address' port-range. The last property group D depicts the locations of NAT devices, with the property items D1, D2 and D3 showing the NAT devices in local networks of source-hosts, destination networks and both, respectively.

Table I. Properties in transition schemes

Property Group	Group Code	Property Name	Value
The protocol stacks of source host actual use	A	Dual-Stack	A1
		IPv4 only	A2
		IPv6 only	A3
Relationships between IPv4 and IPv6 Address	B	Stateless	B1
		Stateful	B2
Types of IPv4 address for source-host	C	Private	C1
		Public	C2
		Public with Port Sharing	C3
		Private with Port Sharing	C4
The locations of NAT devices	D	Only in local side	D1
		Only in Dest.side	D2
		D1 & D2	D3

With regard to the property item combination, we must point out two confusions. The first one is that the property of A3 does not conflict with property group C, because the IPv4 address, which is mapped with the IPv6 address of source-host, could be assigned to its tunnel proxy. Secondly, the property of either C2 or C3 and the property group D also do not conflict with each other, since network address translation has various forms, not just limited to the form which is from private to public. Therefore, the maximum number of

combination is up to 72 and the minimum is 2 since 6over4 tunnel only needs the combination of the property of A3 and that of either B1 or B2. Moreover, the property group D is not a necessary condition in 4over6 transition scenarios.

3.2. Solutions of IP source address validation

Keeping packets with trustful IP source addresses is the basis for the validation and traceback requirements. SAVI Switch can achieve this goal, but at present, it's still only applicable to single-stack network, which means SAVI Switch needs to be improved to adapt to dual-stack and other complex scenarios. Therefore, we present the sub-solution to the IP source address validation for each individual property based on the improvement of SAVI, as illustrated in table II.

In order to keep the system's consistency and practicability, the sub-solution for property item A1 (dual-stack) only binds IPv6 addresses rather than those of both IPv4 and IPv6, and the tunnel terminal will verify the relationship of them (see table III). Since the properties of B1 (stateless) and B2 (stateful) only decide the relationship between IPv4 and IPv6 addresses for source-hosts, the sub-solution to the source address validation depends on the property group A. Similarly, property items C1 and C2 are both determined by the property group A as well. However, if it is the situation where multi-hosts share an IP address by splitting port-range, SAVI Switch needs to bind the port-range on the basis of group A, and this is illustrated in the second row of table II from bottom. The property group D needs only to save the NAT-Table for traceback function.

We also consider solutions to the source address validation for property combinations. In table III, ''-'' in column ''Combination'' means ''relation'', ''/'' indicates ''choice'', and the ''()'' states ''optional relationship.'' Taking 'A1-B1-C1/C2-(D1/D2/D3)' as an example, it depicts that property item A1 firstly combines with B1, and then they as a whole unite with either C1 or C2. This sequence could be further preceded with any property items in group D. Under the dual-stack situation, a source-host will take itself as a tunnel start-point to retrieve either IPv4 or IPv6 address(es), and another reason that we bind only IPv6 in this scenario is the performance of layer2.5 SAVI Switch in parsing DHCPv4(6) messages from the encapsulated tunnel protocol. And if it is in the stateful mode, the tunnel terminal should snoop the address assignment protocols, such as DHCPv4(6), SLAAC, PCP, etc., in order to save the mapping record between IPv4 and IPv6 for a source-host. The tunnel terminal also verifies the record for each packet either in stateless (by deducing) or stateful scenarios, as shown in Table III from index 1 to 4.

Table II. Solutions of Source address validation for each property

Property Name	Value	Measurements in SAVI Switch
Dual-Stack	A1	<IPv6, MAC, linkup-Port>
IPv4 only	A2	<IPv4, MAC, linkup-Port>
IPv6 only	A3	<IPv6, MAC, linkup-Port>
Stateless	B1	none
Stateful	B2	none
Private	C1	none
Public	C2	none
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	NAT devices record the NAT-Table
D1 & D2	D3	

Table III. Solutions of Source address validation for property combinations

Index	Combination	Transition Scenario	Solutions in SAVI Swi.
1	A1-B1-C1/C2-(D1/D2/D3)	Dual-Stack with stateless scenario in Public 4over6	<IPv6, MAC, Switch-Port, IPv4>, & Tunnel Terminal(TT)verifies relation of <v6,v4>
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>, TT verifies relation of <v6,v4>
3	A1-B2-C1/C2-(D1/D2/D3)	DS-Lite; Dual-Stack with stateful scenario in Public 4over6	<IPv6, MAC, Switch-Port>, & TT 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, port-range> TT verifies relationship of <IPv6,IPv4 >
5	A2-B1-C1/C2-(D1/D2/D3)	4RD; IPv4-only with stateless scenario in public 4over6	<IPv6, MAC, Switch-Port>
6	A2-B1-C3/C4-(D1/D2/D3)	A+P; IPv4-only with stateless scenario in Light-Weighted Public 4over6	<IPv6, MAC, Switch-Port,Port-Range>
7	A2-B2-C1/C2-(D1/D2/D3)	IPv4-only with stateful scenario in public 4over6	<IPv6, MAC, Switch-Port >
8	A2-B2-C3/C4-(D1/D2/D3)	IPv4-only with stateful scenario in Light-Weighted Public 4over6	<IPv6, MAC, Switch-Port,Port-Range>
9	A3-B1	6RD;	<IPv6,MAC,Switch-port>
10	A3-B2		same with row index 9

3.3. Solutions to IP source address traceback

Traceback means the system can locate the original senders of the suspicious packets. To achieve this goal, IP source address in each packet should be authentic and trustful. This can be implemented by authenticating the sender in SAVI Switch and recording the IP mapping-table in each NAT device. Finally, administrators can track down the sender by following the packet receiver. Table IV presents the method of traceback for each individual property.

Table IV. Sub-Solutions to traceback for single property

Value	Method of traceback
A1	Queried IPv4 address->deduce(stateless) or look up table(stateful)->IPv6->locate sender
A2	Depends on group B
A3	
B1	Extend IP header to include tunnel initiator's address, and tunnel terminal saves relationship of <interface address of tunnel,device IP address of tunnel device>
B2	IPv6(4) address is obtained by looking up IPv4-IPv6 mapping-table in 4over6 terminal
C1	Taking IP address as condition to query SAVI Management Database to locate the sender's uplink-port.
C2	
C3/C4	Taking port-range and IP address as condition to query SAVI Management Database to locate the sender's uplink-port.
D	Take queried IPv4 address as condition to retrieve original IPv4 address by looking up NAT table

In the stateless scenarios, there is a very tough problem for traceback; that is, it's hard to trace the tunnel initiator device from the tunnel terminal, because the IP source address in the tunnel

protocol is the tunnel initiator's interface address, rather than the address of tunnel device itself. It will become much easier if the tunnel terminal figures out the mapping-relationship between the tunnel's interface address and the tunnel-device's address. Thus, we propose the approach to extending the IP header of the tunnel protocol so as to gain the tunnel-device's address, and then the tunnel terminal keeps this mapping-relationship. As to how to extend the IP header to achieve this goal, it is a relatively minor issue since it can be achieved by creating a new header option in IPv6 destination header or utilizing rarely used fields in IPv4 header. We admit that the realization method for traceback requires some costs in this situation, but our responsibility is to present a comprehend-sive scheme and then leave network authorities to make their own decisions based on demands. Besides, the SAVI Manage-ment Database (SMD) can collect data from all of SAVI Switches via SNMP protocol with SAVI-MIB[SAVI-MIB]. Therefore, authorities can directly lock the source-host by querying this database with IP source address or other distinctive conditions.

Table V illustrates the complete track-path for the property combinations. Taking Index 1 as an example, we try to locate the sender of a suspicious packet in the destination network. The first step is to look at the NAT mapping-table to retrieve original IPv4 address if there exists an NAT device. Since it's the dual-stack and stateless scenario, the source-host uses its own IPv6 as the tunnel interface's address to forward its own IPv4 packets, and this IPv6 address can be deduced from its own IPv4 address. Finally, the sender will be located by querying SMD based on its IPv6 address.

Table V. Solutions to IP traceback 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 v4->(Original v4 (via D2))->v6 (via deduce)-> lock sender
2	A1-B1-C3/C4/-(D1/D2/D3)	Dual-Stack with stateless scenario in Light-Weighted Public 4over6	same with row index 1
3	A1-B2-C1/C2/-(D1/D2/D3)	DS-Lite; Dual-Stack with stateful scenario in Public 4over6	Queried v4->(Original v4 (via D2))->v6 (via look table)->lock sender
4	A1-B2-C3/C4/-(D1/D2/D3)	Dual-Stack with stateful scenario in Light-Weighted Public 4over6	same with row index 3
5	A2-B1-C1/C2-(D1/D2/D3)	4RD; IPv4-only with stateless scenario in public 4over6	Queried v4->(Original v4 (via D2))->v6 (via deduce)-> lock tunnel initiator-> (original v4(via D1))->locate sender
6	A2-B1-C3/C4-(D1/D2/D3)	A+P; IPv4-only with stateless scenario in Light-Weighted Public 4over6	same with row index 5
7	A2-B2-C1/C2-(D1/D2/D3)	IPv4-only with stateful scenario in public 4over6	Queried v4->(Original v4 (via D2))->v6 (via look table)->lock-> tunnel initiator-> (original v4(via D1))->locate sender
8	A2-B2-C3/C4-(D1/D2/D3)	IPv4-only with stateful scenario in Light-Weighted Public 4over6	same with row index 7

9	A3-B1	6RD;	Queried v6->(via deduce->locate tunnel initiator (via look table)->locate sender
10	A3-B2		same with row index 9

4. Framework verification

This section demonstrates the feasibility and adaptivity of our framework by applying it to several existing classic schemes and even a newly created transition scheme.

4.1. Public 4over6

Packets with public IPv4 addresses transiting over IPv6 net-works, namely Public 4over6, is a mechanism for bi-directional communication between IPv4 Internet and IPv4 networks which are both sited in IPv6 networks. Fig.1 shows the general scenario in this scheme. The 4over6 Concentrator acts as a tunnel terminal receiving packets from 4over6 tunnel initiators and forwarding them to IPv4 Internet, while the CPE (Customer Premises Equipment) device performs as a tunnel broker for the solo-stack 4over6 host (source-host) on the border of the local IPv4 network. Another type of 4over6 hosts are in the border of the IPv6 network. They obtain their IPv4 addresses and access IPv4 Internet by using their own IPv6 addresses as tunnel brokers. Thus, we still classify this situation into the dual-stack category since the source-host actually runs both IPv4 and IPv6 stack. The stateful and the stateless are the two kinds of relationship between IPv4 address and IPv6 address in 4over6 hosts. The difference between them lies in the fact that, while the stateless mode takes IPv4-embedded IPv6 as the tunnel initiator's address; the stateful means no relationship exists betweetn the IPv4 address to the 4over6 host and the IPv6 address to the tunnel initiator. Therefore, the 4over6 Concentrator which sites in the border between IPv6 network and IPv4 Internet needs to store the mapping relationship so as to provide correct forwarding. The combination of two types of stacks (IPv4-only and dual-stack) and two kinds of address relationships creates four scenarios: IPv4-only with the stateless (A2-B1-C2), dual-stack with the stateful (A1-B2-C2), IPv4-only with the stateful (A2-B2-C2) and dual-stack with the stateless (A1-B1-C2). The Figure 2 illustrates the scenario of IPv4-only with stateless. The source

address validation and traceback solutions for it can be found in previous tables

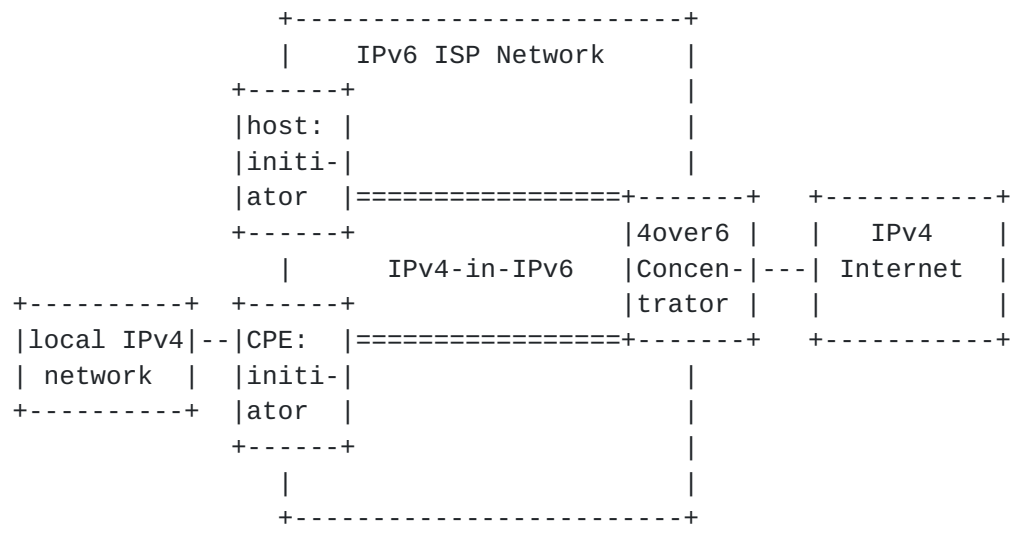

Figure 1 The overview of Public 4over6 transition scenario

4.2. 6RD

6RD (IPv6 Rapid Deployment on IPv4 Infrastructures) is a typical 6over4 tunnel transition scheme. The 6RD ''Customer Edge'' (CE) router performs as a tunnel broker to encapsulate and forward packets for source-hosts on the border of the local IPv6 network, while 6RD Border Relay (BR) router locates in the SP premises acting as a tunnel terminal to de-capsulate and relay packets to IPv6 Internet. 6RD belongs to the stateless scenario since the IPv6 address for source-host and the IPv4 address for CE WAN interface can be deduced to each other. Therefore, 6RD belongs to the combination of A3-B1.

4.3. DS-Lite

Dual-Stack Lite is a 4over6 transition plan. NAT function is performed in CGN(Carrier Grade NAT) devices which provide address translation from private to public IPv4 address. We treat DS-Lite as the property combination of the dual-stack, stateful, private IPv4 address and NAT device in destination network (A1-B2-C1-D2). According to the framework, the access SAVI Switch for CPE (home gateway) should bind its IPv6, MAC address and the uplink port together. Since NAT and the tunnel function have been both fulfilled by CGN device and their records are in a same table, the trace- path follows the direction from the queried IPv4 to original IPv4 address

by referring to the NAT record. Then it can locate the CPE device in user's household by the tunnel information in CGN.

4.4. 4RD

IPv4 Residual Deployment (4RD) is a 4over6 mechanism to facilitate IPv4 residual deployment across IPv6 networks of ISP. It can be treated as the combination of A2, B1 and C2.

4.5. A+P

The address-plus-port (A+P) approach also is a 4over6 plan advocated by the France Telecom, Nokia and other companies to solve the IPv4 address shortage. A+P treats some bits from the port number in the IPv4 TCP/UDP header as identifiers of additional tunnel terminal, which can facilitate the IPv4 address multiplexing. A+P is an architecture which combines MAP-T[MAP-T], MAP-E[MAP-T] and 4RD schemes, and has both a stateful and a stateless scenario description. As to the stateless scenario, we treat it as a combination of A2, B1, C3 and D1.

4.6. IVI

IVI is a typical translation transition solution which provides bilateral access from both pure single stack sides. The service providers keep a length of consecutive IPv4 addresses (IVI4) so that they can map these addresses to a special range of IPv6 address (IVI6) with the ration of 1:1. Then, the IVI translator can keep the communication by translating two types of IP headers or even application layer headers. For multiplex IPv4 address, a variant translation mechanism with ration of 1(IPv4):N(IPv6) is called DIVI which is implemented by splitting upper port range and only supported by IPv6 initiated communication. But no matter which type it is, networks in the two sides of the IVI translator are pure single-stack, and then the spoofing problem can be solved by applying SAVI Switch to each stack. Certainly, the IVI translator should save the address mapping records in order to track back the source-host.

4.7. New created proposal

After the framework in the existing transition plans is verified, readers may still concern about whether it can adapt to new schemes or not. Hence, we create a new transition proposal to prove its flexibility, as shown in Fig.6. The new proposal is combined with property item A1, B2, C1 and D2, which refer to dual-stack, stateful, private IPv4 address, and NAT device in destination network, respectively. According to our framework, the SAVI Switch needs to

bind the source-host's IPv6 and MAC address, with the switch's uplink-port. The trace-path is shown with the red dash line which fetches its original private IPv4 address for a suspicious packet, then retrieves the tunnel information based on the private address, and finally locates the sender according to its IPv6 address.

5. Conclusions

Along with the rapid development of IPv6 networks and the urgent demand of inter-communication between IPv4 and IPv6 networks, the trend of IPv4/IPv6 transition is inevitable, and lots of transition schemes have been proposed. Meanwhile, the IP spoofing issue still bothers network participators, and once it happens, it's hard to trace the spoofer. The SAVI proposal, one of the most excellent solutions to the source address validation, has been proposed by IETF SAVI workgroup, which binding source-hosts' IP, MAC address and uplink-port properties in their Layer2.5 access switches. Its aim is to prevent nodes attached to the same IP link from spoofing each other's IP address. Our goal is to propose a general framework which can adapt to all transitions especially tunnel schemes for IP source address validation and traceback with the help of SAVI. In this paper, we propose this framework for anti-spoofing and traceback for IPv4/IPv6 transition scenarios by extracting the essential and mutual properties from various transition schemes. We present the sub-solutions or solutions to each property and property combinations, and also the framework implementation. Finally, we apply our framework to various transition schemes that successfully prove our framework's adaptability and flexibility. We hope that this framework can be realized in the future for the purpose of IP source address validation and traceback in IPv4/IPv6 transition scenarios.

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.

[CAIDA] CAIDA. http://www.caida.org/data/realtime/telescope

[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.

[RFC5565] J.Wu,Y.Cui,C.Metz.Softwire Mesh Framework, IETF RFC 5565, 2009

[6RD] R.Despres.IPv6 Rapid Deployment on IPv4 Infrastructures (6rd), RFC 5569, 2010

[DS-Lite] 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

[Public4over6] 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

[IVI] 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.

[SAVI-MIB] C.An, J.Yang, J.Wu et.al. Definition of Managed Objects for SAVI Protocol, http://tools.ietf.org/html/draft-an-savi-mib-04,2012

[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

[MAP-T] C.Bao, X.Li et.al. MAP Translation (MAP-T)-specification, http://tools.ietf.org/html/draft-mdt-softwire-map-translation-01, 2012

[MAP-E] T. Murakami, Ed.,O. Troan, S. Matsushima. MAP Encapsulation (MAP-E)-specification, http://tools.ietf.org/html/draft-mdt-softwire-map-encapsulation-00, 2012

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