SAVI
Internet Draft
Intended status: Standard Tracks
Expires: May 2014

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

November 5, 2013

A General Framework of Source Address Validation and Traceback for IPv4/IPv6 Transition Scenarios
draft-xu-savi-transition-04.txt

Abstract

IP spoofing is a critical breach regard to Internet security. With rapid development of the IPv6-based next generation Internet, this issue is more prominent since IPv6 Internet owns more spoofable IP address space. Existing IP anti-spoofing proposals, including SAVI (Source Address Validation Improvement) which was advocated by IETF, only focused on single-stack or simple network scenarios. To the best of our knowledge, none of them has paid attention to the IPv4/IPv6 transition scenarios. However, since IPv4/IPv6 transition schemes are plenty and various, one solution cannot meet all requirements of them. In this draft, we present a SAVI-based general framework for IP source address validation and traceback in the IPv4/IPv6 transition scenarios, which achieve this by extracting out essential and mutual properties from these schemes, and forming sub-solutions for each property. When one transition scheme is composed from various properties, its IP source address validation and traceback solution is directly comprised by the corresponding sub-solutions. Thus, the most exciting advantage of this framework is that it is a once-and-for-all solution no matter how transition schemes change.

This Internet-Draft will expire on May 5, 2014.

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 by snooping host's IP assignment protocol. 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 layer2 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 the 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. As a matter of fact, the IPv6 Internet traffic only accounts for 1% of the total Internet traffic. In other words, the two kinds of networks will be coexistence for a long 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.

Although many mature and practical solutions have met the demand of validating IP source address and even traceback in single-stack networks, but to the best of our knowledge, ideas for the same purpose in the IPv4/IPv6 transition scenarios have not been explored yet. The difficulty lies in it is that, it's inflexible to propose corresponding scheme for each one plan since they are plenty and various. Viewed this challenge and dilemma, proposing solo general and feasible solution which can satisfy all the requirements of these transition plans has become the single goal of this draft.

After investigated almost all the transition especially tunnel schemes, we have found that there exist basic and common properties among them. Then, we focus on extracting these essential properties from these schemes and then forming sub-solutions for each property with the help of SAVI. Consequently, when one scheme is constituted by required properties, its source address validation and traceback solution are naturally combined by corresponding sub-solutions. Thus, our framework is a once-and-for-all solution no matter how transition plans 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 its considerations, and then describe our framework in detail.

The threat model in this paper we refer to the fields in an IP packet can be tampered as the spoofer's will, and when these packets arrived

their destination, spoofer can run in the attack or purposed action and it's hard to locate the perpetrator since the packet's source IP address has been modified. But we believe that the network devices or middle-boxes (NAT, tunnel points, protocol translator etc.) are trustful and attackers cannot manipulate them. Otherwise, that situation would become very complex and it's beyond our agenda.

To keep packets carried with the trusted IP source address, it should let the packets come from an authorized user who is the owner of the packet's source address, and prevent spoofed packets from being forwarded. Naturally, the straight-forward idea of us is to deploy SAVI Switch into users' subnet to keep the trustiness of all hosts. Furthermore, NAT devices need to save the pre-translate and post-translate addresses mapping records. Such ideas could directly facilitate the implementation of the traceback function.

3.1. Property Extraction

Like we mentioned, it is difficult to require one framework to adapt to all transition plans. But since there exist common properties in these transition schemes, establishing such framework could be possible if we could extract these essential properties from these plans and restore them by reassembling required properties. Actually, this has been achieved based on three property extraction rules: 1) It only extracts essential elements and does not take irrelevant details into account; 2) every element should not be further decomposed (in other words, each element should be atomic and unique); 3) it should have the reconstruction capability of reassembling required elements. The result of the property extraction is illustrated as table I.

We have summarized these properties into four categories with 12 items. Property group A states the stacks of spoofer's running rather than its network environment. The stateless in Group B means that IPv4 and IPv6 addresses are tight related since they can be deduced with each other, while the stateful declares that the two kinds of addresses has no relation so that the tunnel terminal needs to save the mapping relationship for forwarding. Property items C3 and C4 which describe the scenario where multi-hosts share one IPv4 address by splitting the port-range. The last property group D depicts the positions of NAT device which could change the source IP address not only within the form of private to public and shared to non-shared. Properties D1, D2 and D3 manifest the NAT devices in the position of the local network, the destination network with same protocol-stack of the local network, and both sides separately.

As the property item combination, we must point out two confusion places. The first one is A3 with group C are not conflicting with each other because the source host can retrieve IPv4 address by taking itself as tunnel start-point even in a IPv6 network, as well as C2 or C3 with group D since network address translation(NAT) has various forms not just only refer the private to the public. Therefore, the maximum number is 72 and the minimum is 2 since 6over4 transition only needs A3 combine with B1 or B2, and group D is not a necessary condition for 4over6 transition regard to the item combination.

Table I. Properties in transition schemes

Property Group	Group Code	Property Name	Value
The protocol stacks of source host	A	Dual-Stack	A1
		IPv4 only	A2
		IPv6 only	A3
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
The locations of NAT devices for source host	D	Only in local side	D1
		Only in dest.side	D2
		D1 & D2	D3

3.2. Solutions of IP source address validation

Keeping packets bringing with trustful IP source addresses is the foundation of the traceback and other applications. SAVI Switch can achieve this goal, but till now, it's only applicable for the single-

stack network, which means SAVI Switch needs to be improved to adapt to dual-stack and other complex scenarios. In the other sides, it is not inflexibility to enumerate all the possibilities of property combinations and separately considering how to achieve our goal. Instead, we present the sub-solutions to IP source address validation for each property with the help of SAVI Switch, as illustrated in table II.

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	

Since the property item which is either the stateless (B1) or the stateful (B2) only decides the relationship between the two types of addresses for source hosts, the sub-solutions to their source address validation depend on property group A. Similarly, sub-solutions to source address validation for property items C1 and C2 are all decided by property group A as well. However, if it is the situation where multi-hosts share an IP address by the multiplexing upper port,

SAVI Switch should bind its port-range together along with group A required, Property group D needs save the NAT-Table for traceback.

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>
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)	DS-Lite; 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-C1/C2-(D1/D2/D3)	4RD; IPv4-only with stateless scenario in public 4over6	<IPv6, MAC, Switch-Port,(Port-Range)>
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,(Port-Range)>
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

We also consider the solution to the source address validation for property combinations. In table III, the notation "-" in column of "Combination" means the relation of union, while the slash notation indicates single choice from multi-option, and the bracket states the optional relationship. Taking the combination A1-B1-C1/C2-(D1/D2/D3) as an example, it depicts that property item A1 combines with B1, and then they as a whole unite with either C1 or C2. This combination could be further preceded with any property items in group D.

Even though we can bind two kinds of address and other information together in dual-stack network, for the consistent reason and considering the performance of SAVI Switch in parsing DHCPv4(6) messages from the upper tunnel protocol in scenarios which involved with A2 and A3, we turn to an alternative approach where the switch only binds IPv4(6) with other information. And tunnel terminal snoops IPv4/IPv6 address assignment protocols in order to save the records of IPv4-IPv6 (stateful), and verifies it for each packet either in stateless or stateful scenarios, as row index from 1 to 4.

3.3. Solutions to IP source address traceback

The traceback means that system can locate the senders of the suspicious packets original from. To achieve this goal, IP source address in every 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 path from the packet receiver to the sender. Table IV presents the method of traceback for individual property.

In the stateless scenarios, a very tough problem exists for the traceback; that is, it's hard to locate the device of tunnel initiator from the side of the tunnel terminal because the interface address of the tunnel is packets' source address related to IPv6(4) address, rather than the tunnel-device's address. It will become much easier if the tunnel terminal has the mapping-relationship with the tunnel's interface address and the tunnel-device's address. Thus, we have the approach to extending IP header of the tunnel protocol to include the tunnel-device's address, and tunnel terminal saves this mapping-relationship.

As to the question of how to extend IP header to achieve this goal, it is a relatively minor issue which can be realized by creating a new option in IPv6 destination header or utilizing rarely-used fields in IPv4 header. We have to admit that we do sacrifice some cost for traceback in this situation, but as a comprehensive research we still present out and let the network authorities to make their choices.

Besides, another key issue is the SAVI Management Database (SMD) which collects information from all SAVI Switches in domain by SNMP protocol, including the binding-status-table and other important data. Therefore, administrators could directly lock the source-host by consulting this database with its IP source address or other distinctive conditions.

Table IV. Sub-Solutions to traceback for single property

Value	Measurements
A1	Queried IPv4 address->deduce(stateless) or look up table(stateful)->IPv6->locate
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	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

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

Table 5 illustrates the fully track-path for property combinations. Taking the first row in this table as an example, we try to locate the sender of a suspicious packet in the destination network. The first step is to look up the NAT mapping-table to retrieve the 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; this IPv6 address can be deduced from its pre-translated IPv4 address. Finally, the sender will be located by consulting SMD based on its IPv6 address.

4. Framework verification

In this section, we apply our framework to some famous previous mentioned schemes to verify its correctness.

4.1. Public 4over6

Packets with public IPv4 addresses over IPv6 networks, namely Public 4over6, are the mechanism for bi-directional IPv4 communication between IPv4 Internet and IPv4 networks which are both sited in IPv6 access network.

Fig.1 shows the general scenario in Public 4over6 plans. The 4over6 Concentrator acts as a tunnel end-point 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 on the border of the local IPv4 network. Another type of 4over6 hosts in IPv6 network gets their IPv4 addresses and accesses IPv4 Internet by using their own IPv6 addresses as a tunnel broker, thus, we classify it into the dual-stack category. There are also two kinds of relationship between the IPv4 address belongs to 4over6 host and the IPv6 address belongs to its tunnel interface, that is, stateful and the stateless. The difference between them is that the stateless mode takes IPv4-embedded IPv6 as the tunnel initiator's address, on contrary, the stateful means IPv4 address for the 4over6 host and the IPv6 address

for the tunnel initiator have no relation with each other, so that the 4over6 Concentrator needs to save the mapping relationship to provide correct forwarding. Two types of initiators with two address relationships, there are total four scenarios: solo-stack with the stateless (A2-B1-C2), dual-stack with the stateful (A1-B2-C2), solo-stack with the stateful (A2-B2-C2) and dual-stack with the stateless (A1-B1-C2). Their source addresses and traceback solutions can be referred to previous tables.

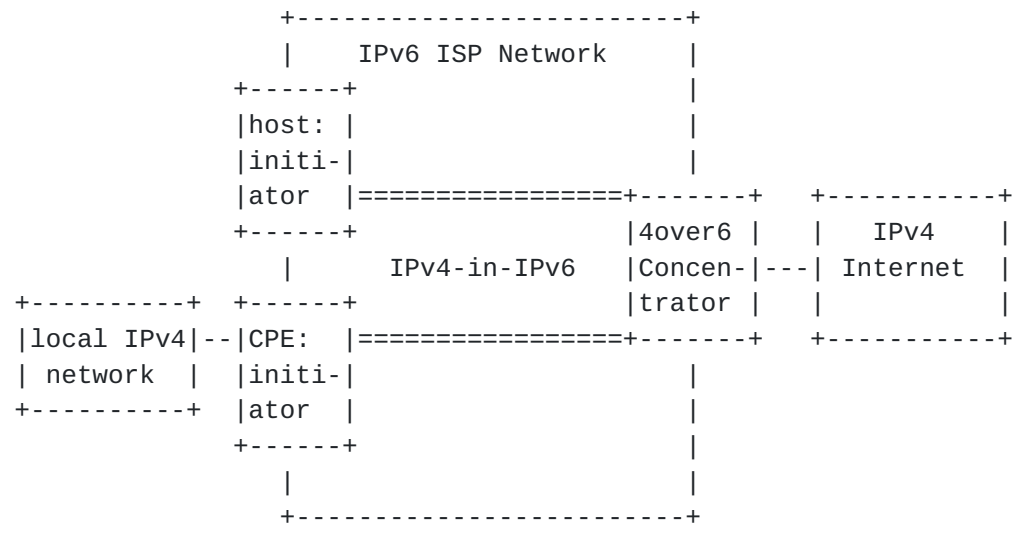

Figure 1 The overview of Public 4over6 transition scenario

4.2. 6RD

6RD (IPv6 Rapid Deployment on IPv4 Infrastructures) is a typical 6over4 tunnel transition scheme. The 6rd "Customer Edge" (CE) router functions as a tunnel broker to encapsulate and forward packets for the source-host on the border of the local IPv6 network, while 6rd Border Relay (BR) router located at the SP premises acts as a tunnel terminal to de-capsulate and relays packets to IPv6 Internet. It belongs to the stateless scenario since the IPv6 address of the source-host and IPv4 address of CE WAN interface can be conducted 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) device to provide the translation function from the private to the public IPv4 address. We treat DS-Lite as the property combination of the Dual-Stack, stateful

and private IPv4 address and NAT in the destination network, that is, 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 the NAT and tunnel function fulfilled by CGN device and their records are in a same table, the trace path follows the direction from the queried IPv4 address to tunnel property by referring to the NAT record. Then it locates CPE device in user's household by following the tunnel information.

4.4. 4RD

IPv4 Residual Deployment (4RD) is a 4over6 mechanism to facilitate IPv4 residual deployment across IPv6 networks of ISP's. It can be treat as the combination of A2-B1-C2. More information is the Softwire workgroup has decided to put 4RD and MAP-T[14] on experimental track and MAP-E[15] on standards track.

4.5. A+P

The address-plus-port (A+P) approach also is 4over6 plan which advocated by the France Telecom, Nokia and other companies for resolving the issue of IPv4 address shortage. A+P treats some bits from the port number in the TCP/UDP header as additional end-point identifiers to extend the address field. A+P is an architecture which combines MAP-E, MAP-T and 4RD. Although proposer described as a stateful version but the IETF still put it into a stateless solution, thus, we treat it as a property combination of A2-B1-C3-D1.

4.6. IVI

IVI is a typical translation transition solution which provides bilateral access from both pure single stack sides. The service providers reserve a piece of range IPv4 address (IVI4) so that they can map them with a special range of IPv6 address (IVI6) as the ration of 1:1, then the IVI translator keeps the communication correctly. Another ration of 1(IPv4):N(IPv6) was called DIVI[16] which implemented by splitting port only supports IPv6 initiated communication. But no matter which type, the anti-spoofing measure is same with pure stack which follows the SAVI's specification, and keeping the stateless mapping records in order to trackback.

5. Framework implementation

The framework implementation is actually quite simple, which has been illustrated by table VI. We categorized the modules into four types and each type has its own deployment position. There are two special occasions we must address. One is that, when a source-host is in an

IPv4 with port-sharing network, the binding module in SAVI Switch should bind the host's port-range with other data together; and the other is that, when the traceback is in tunnel stateless scenarios, we need to extend the tunnel IP header that we mentioned above.

Table VI. MODULE DECOMPOSITION FOR FRAMEWORK REALIZATION

Modules	Deployment	Scenarios	Module Detail
Binding	SAVI Switch	IPv4-only(Including port-sharing)	<IPv4, MAC, link-port, (port-range)>
		IPv6-only&dual-stack (port-sharing)	<IPv6, MAC, link-port, (port-range)>
Verification	Tunnel Terminal	Stateless	Verify the deduction relationship
		Stateful	Save and verify the mapping relationship
NAT Record	NAT Device& Translator		Record Mapping relationship
Trace-back	Tunnel Initiator	Tunnel initiator extends packets'IP header to include relationship <Tunnel's interface add.,tunnel initiator device's add.>	
	Tunnel Terminal	Tunnel terminal saves the above relationship for traceback	

6. Conclusions

Along with the rapid development of IPv6 networks and the urgent demand of inter-communication between IPv4 and IPv6 networks, the situation of IPv4/IPv6 transition is inevitable, and lots of transition plans are proposed. Simultaneously, the IP spoofing issue still bothers network users and administrators, and once it happened, it's hard to trace the spoofer. The SAVI proposal, one of the excellent solutions to the source address validation, has been proposed by IETF SAVI workgroup, which binds host's IP, MAC address and uplink-port features in their access switches to achieve the goal of preventing nodes attached to the same IP link from spoofing each

other's IP addresses. Our goal is to propose a general framework which can adapt to all transition especially tunnel plans for IP source address validation and traceback with the help of SAVI. In this draft, we propose a general framework for anti-spoofing and traceback in IPv4/IPv6 transition scenario by extracting the essential and mutual properties from various transition schemes. We present the sub-solutions or solutions for each property and property combinations. Finally, we verify this framework in various transition schemes and prove its excellent adaptability and flexibility. We hope that it will give more inspiration for more interested researchers, work together and finally we can make it happen to achieve the goal in practical.

7. References

7.1. 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 et.al., "Source Address Validation Improvement Framework (SAVI)", RFC 7039, October 2013.

[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

8. 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