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

Guangwu Hu, Ke Xu, Jianping Wu, Yong Cui, Tsinghua University
Fan Shi, Beijing Research Institute of China Telecom

Abstract

IP spoofing has nowadays become a research focus, as it has been bothering netizens since the emergence of the Internet. 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 paper, 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.

IP address in computer network plays a similar role to our identity in the real world. But it is more vulnerable to be faked since there are no intrinsic mechanisms to prevent this from happening. Because of the simplicity of network topology and the trustiness of network users, designers failed to consider this issue at the emergence of the Internet. According to the IP spoofer project of MIT, the proportion of the spoofable net-blocks, IP addresses and autonomous systems is respectively as high as 14.3 percent, 17.3 percent, and 23.3 percent on Dec. 25th, 2012 [1]. CAIDA also proves that U.S. and China are major victim countries of IP spoofing attack [2]. Encouragingly, this issue has been gradually noticed by many researchers, and lots of ingress filtering [3, 4] included solutions [5, 6] have been proposed. One of the most outstanding is SAVI [7] (Source Address Validation Improvement) which is proposed by IETF SAVI workgroup. The mechanism of it is to bind host's IP, MAC and uplink-port properties together in users' access switch. Briefly, a SAVI Switch is a layer 2.5 switch which adds two extra functions of binding and filtering on the base of the normal layer2 access switch, which can eliminate IP-spoofing in the first-hop of packets. As to the binding function, it is automatically achieved by snooping IP address assignment protocols. Thus, it is more accurate and effective than the scheme of uRPF [8] (unicast Reverse Path Forwarding) because it has closer position to users and it eliminates the possibility of false positive. However, till now, SAVI only focuses on the IPv6 stack and simple network access scenarios.

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 [9] and the small percentage of IPv6 Internet traffic (1 percent) [10], 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" [11], 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

0890-8044/13/$25.00 © 2013 IEEE

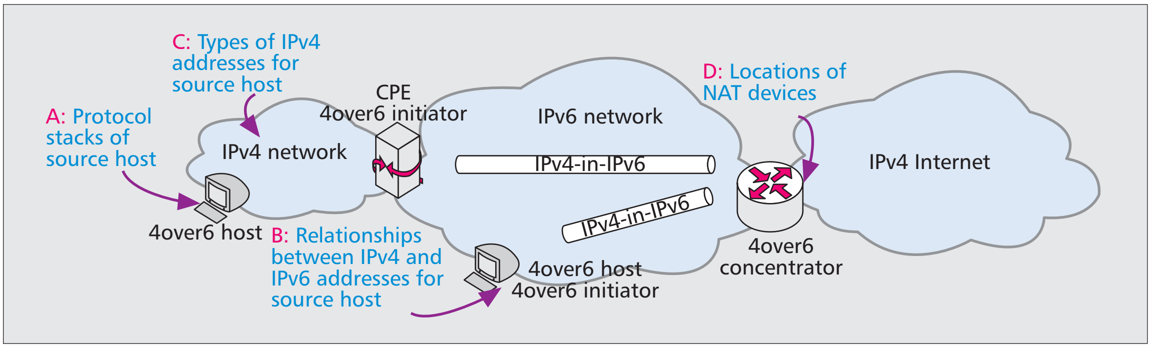
C: Types of IPv4 addresses for source host
A: Protocol stacks of source host
IPv4 network
CPE
4over6 initiator
IPv6 network
D: Locations of NAT devices
IPv4 Internet
IPv4-in-IPv6
IPv4-in-IPv6
4over6 host
B: Relationships between IPv4 and IPv6 addresses for source host
4over6 host
4over6 initiator
4over6 concentrator

Figure 1. *The property extraction illustration with the Public 4over6 scheme.*

stack and the ISP backbone that uses IPv6 stack, whereas 6over4 is the opposite situation. Well-known tunnel proposals include 6RD [12], DS-Lite [13], 4RD [14], A+P [15], Public 4over6 [16] etc. As to translation, the core idea is the packet header conversion between the two protocol stacks. 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*.

We verify our framework from a theoretical point of view. However, issues including violation of personal privacy, framework's performance, whether expanding SAVI out of LAN environment or not, will not be discussed in this paper.

The rest of this paper is organized as follows: we present the framework in detail, including the property extraction and sub-solutions to each property and even their combinations. Then, we give the module implementation of this framework and illustrate its adaptivity and flexibility by applying it to several classic transition schemes. Last section concludes this paper.

The Framework Description

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 Transla-tion) devices to record the mapping relationship between addresses before and after translation. Such ideas could directly facilitate the implementation of the traceback function.

Property Extraction

Extracting essential and common properties from transition schemes has been achieved based on three property extraction rules:

- It only extracts essential elements and does not take irrelevant details into account

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
The relationships between IPv4 and IPv6 address for source-host	B	Stateless	B1
		Stateful	B2
The types of IPv4 addresses 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 destination side	D2
		Both D1 and D2	D3

Table 1. *Properties in tunnel transition schemes.*

Value	Sub-solution
A1	SAVI Switch binds <IPv6, MAC, link-port>
A2	SAVI Switch binds <IPv4, MAC, link-port>
A3	SAVI Switch binds <IPv6, MAC, link-port>
B1/B2	None
C1/C2	None
C3/C4	SAVI Switch binds **port-range** on the basis of group A
D1/D2/D3	NAT devices record the NAT-Table

Table 2. *The sub-solutions to ip source address validation for individual property*.

- Each element will not be further decomposed (in other words, each element should be atomic and unique)
- Transition schemes can be reconstruct-ed by reassembling required elements

We have summarized these properties into four categories with 12 items, which is illustrated in Fig. 1 and Table 1.

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.

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.

Solutions to 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 2.

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 (Table

Index	Combination	Transition Scenarios/Plans	Solution
1	A1-B1-C1/C2-(D1/D2/D3)	Dual-Stack with stateless scenario in Public 4over6	SAVI Switch (SS) binds <IPv6, MAC, link-port> (A1), and Tunnel Terminal (TT) **verifies** relation of <IPv6, IPv4>
2	A1-B1-C3/C4-(D1/D2/D3)	Dual-Stack with stateless scenario in Light-weighted (Lw)Public 4over6	SS binds <A1, **port-range**>, and TT **verifies** relation of <IPv6, IPv4 >
3	A1-B2-C1/C2-(D1/D2/D3)	DS-Lite; Dual-stack with stateful in Public 4over6	SS binds A1, TT **saves and verifies** relation of <IPv6, IPv4>
4	A1-B2-C3/C4-(D1/D2/D3)	Dual-Stack with stateful scenario in Lw-Public 4over6	SS binds <A1, **port-range**>, TT **saves and verifies** <IPv6, IPv4 >
5	A2-B1-C1/C2-(D1/D2/D3)	4RD; IPv4-only with stateless scenario in Public 4over6	SS binds <IPv4, MAC, link-port> (A2)
6	A2-B1-C3/C4-(D1/D2/D3)	A+P; IPv4-only with stateless scenario in Lw-Public 4over6	SS binds <A2, **port-range**>
7	A2-B2-C1/C2-(D1/D2/D3)	IPv4-only with stateful scenario in Public 4over6	SS binds A2
8	A2-B2-C3/C4-(D1/D2/D3)	IPv4-only with stateful scenario in Lw-Public 4over6	SS binds <A2, **port-range**>
9	A3-B1	6RD	A3's sub-solution
10	A3-B2		A3's sub-solution

Table 3. *The solutions to source address validation for property combinations.*

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

Table 4. *The sub-solutions to IP traceback for each property.*

3). 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 2 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 3, "–" 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 3 from index 1 to 4.

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 4 presents the method of traceback for each individual property.

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 [17]. Therefore, authorities can directly lock the source-host by querying this database with IP source address or other distinctive conditions.

Table 5 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.

The Framework Implementation and Verification

In this section, we introduce the module implementation of this framework and then apply the framework to some typical transition scenarios (plans) to verify its feasibility.

Module Implementation of the Framework

The framework implementation is actually quite simple, which has been illustrated by Table 6. 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.

Index	Combination	Transition Schemes	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 (deduce) → locate sender
2	A1-B1-C3/C4-(D1/D2/D3)	Dual-Stack with stateless scenario in Lw-Public 4over6	Same with row index 1
3	A1-B2-C1/C2-(D1/D2/D3)	DS-Lite; Dual-stack with stateful in Public 4over6	Queried v4 → Original v4 (via D2) → v6 (by looking table) → locate sender
4	A1-B2-C3/C4-(D1/D2/D3)	Dual-Stack with stateful scenario in Lw-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 (deduce) → locate tunnel initiator → Original v4 (via D1) → locate sender
6	A2-B1-C3/C4-(D1/D2/D3)	A+P; IPv4-only with stateless scenario in Lw-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 (by looking table) → locate tunnel initiator → Original v4 (via D1) → locate sender
8	A2-B2-C3/C4-(D1/D2/D3)	IPv4-only with stateful scenario in Lw-Public 4over6	Same with row index 7
9	A3-B1	6RD	Queried v6 → v4 (deduce) → locate tunnel initiator (by looking table) → locate sender
10	A3-B2		Queried v6 → v4(by looking table) → locate tunnel initiator(by looking table) → locate sender

Table 5. *Solutions to IP traceback for property combinations.*

Modules	Deployment Device	Scenarios	Module Detail
Binding	Access SAVI Switch	IPv4-only (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 table
Traceback in tunnel stateless scenario	Tunnel initiator	Tunnel initiator extends packets' IP header to include <tunnel interface's address, tunnel initiator device's address>.	
	Tunnel terminal	Tunnel terminal saves the above relationship for traceback.	

Table 6. *Module decomposition for framework realization.*

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.

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. Figure 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). 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.

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.

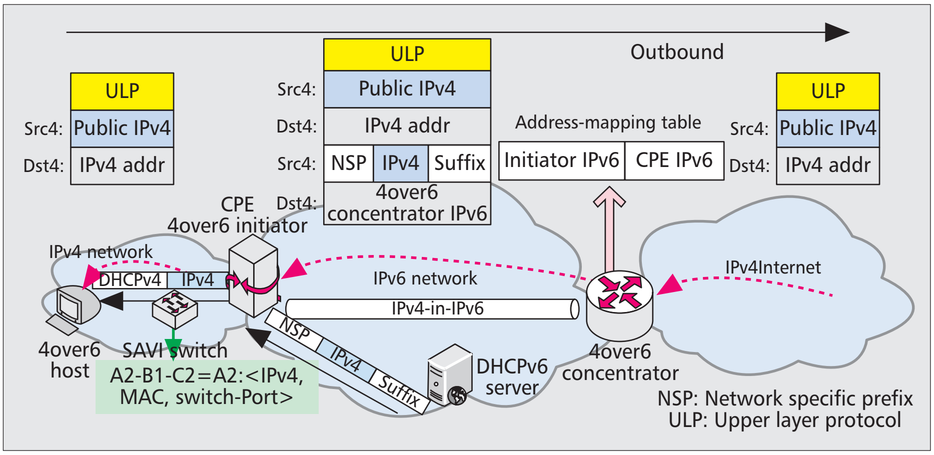

Figure 2. *IPv4-only with stateless scenario in Public 4over6 scheme (Green rectangle means the information that SAVI Switch should to bind, while the red line indicates the traceback direction and phases).*

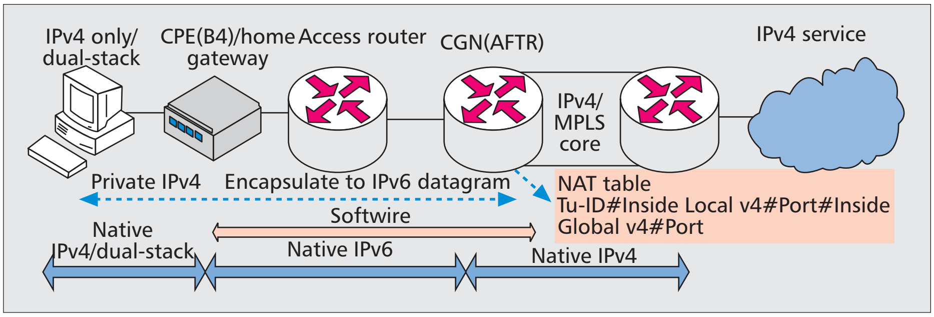

Figure 3. *The illustration of DS-Lite transition scheme.*

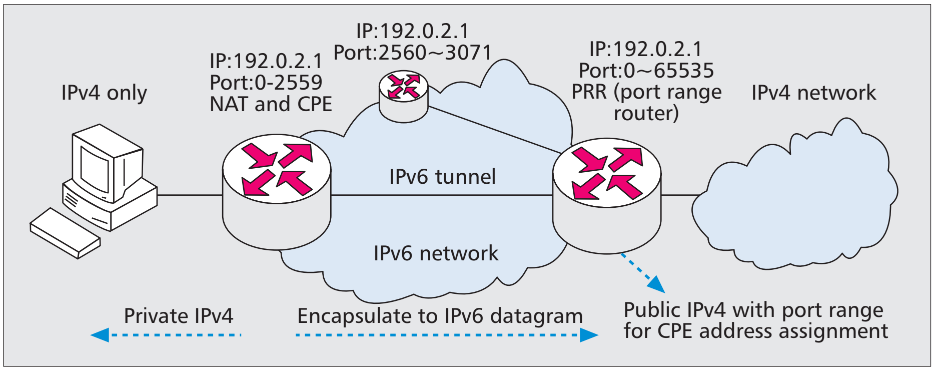

Figure 4. *A simple hierarchical example of A+P transition scheme.*

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. Figure 3 illustrates the work mode of DS-Lite.

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.

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 [18], MAP-E [19] 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, as Fig. 4 has illustrated.

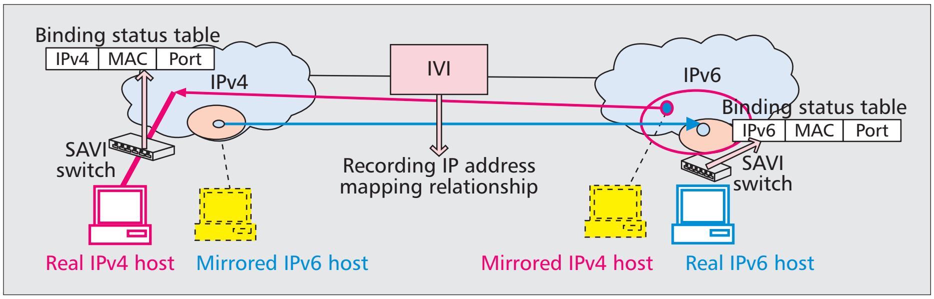

Figure 5. *Framework application in IVI transition scheme.*

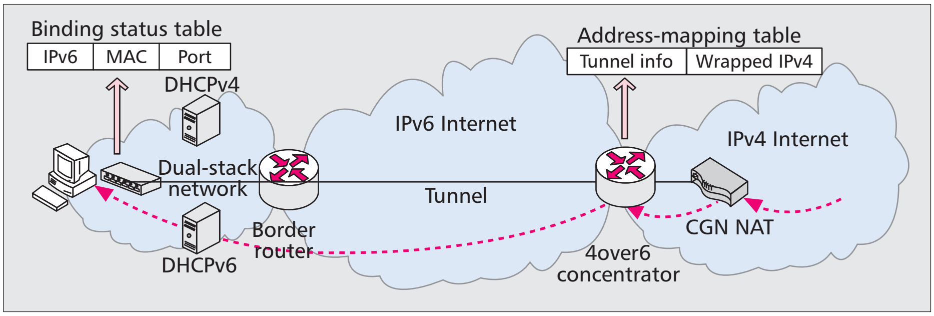

Figure 6. *A new created 4over6 transition scheme(A1-B2-C1-D2) for verifying our framework (red dash line is the trace-path).*

IVI — IVI [20] 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 [21] 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. Figure 5 illustrates the framework application in IVI transition scheme.

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.

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.

Acknowledgment

This work was supported by the NSFC Project (61170292), 973 Project of China (2009CB320501, 2012CB315803), 863 Project of China (2013AA013302) and new generation broadband wireless mobile communication network of the National Science and Technology Major Projects (2012ZX03005001).

References

[1] MIT Spoofer project, http://spoofer.csail.mit.edu/summary.php.
[2] CAIDA, http://www.caida.org/data/realtime/telescope.
[3] P. Ferguson and D. Senie, Network Ingress Filtering:Defeating Denial of Ser-vice Attacks which Employ IP Source Address Spoofing, BCP38, 2000
[4] F. Baker and P. Savola, Ingress Filtering for Multihomed Networks, IETF RFC 3704, 2004
[5] J. Wu, G. Ren, and X. Li, Source Address Validation: Architec-ture and Protocol Design Design," *Proc. IEEE ICNP 2007*, pp. 276–83.
[6] G. Hu *et al.*, SAVT: A Practical Scheme for Source Address Validation and Traceback in Campus Network," *Proc. IEEE ICCCN 2011*.
[7] J. Wu *et al.*, Source Address Validation Improvement Framework (SAVI), RFC 7039, 2011.
[8] Cisco, Unicast Reverse Path Forwarding, http://www.cisco.com, 2007.
[9] J. Wu *et al.*, "The Transition to IPv6, Part I: 4over6 for the China Education and Research Network," *IEEE Internet Computing*, May 2006, pp. 80–85.
[10] Computerworld, http://computerworld.co.nz/news.nsf/news/ipv6-traffic-rises-in-us-but-remains-sliver-of-overall-internet.
[11] J. Wu, Y. Cui, and C. Metz, Softwire Mesh Framework, IETF RFC 5565, 2009.
[12] R. Despres, IPv6 Rapid Deployment on IPv4 Infrastructures (6rd), RFC 5569, 2010.
[13] A. Durand *et al.*, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, RFC 6333, 2011.
[14] R. Despres, Ed., S. Matsushima *et al.*, IPv4 Residual Deployment Across IPv6-Service Networks (4rd) ISP-NAT's Made Optional, http://tools.ietf.org/html/draft-despres-intarea-4rd-01, 2011.
[15] R. Bush, Ed., The Address plus Port (A+P) Approach to the IPv4 Address Shortage, RFC 6346, 2011.

[16] Y. Cui *et al.*, Public IPv4 over IPv6 Access Network, http://tools.ietf.org/html/draft-ietf-softwire-public-4over6-01, 2011

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

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

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

[20] X. Li *et al.*, The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition, RFC 6219, 2011.

[21] C. Bao *et al.*, dIVI: Dual-Stateless IPv4/IPv6 Translation, http://tools.ietf.org/html/draft-xli-behave-divi-04, 2011.

Biographies

GUANGWU HU (hgw09@mails.tsinghua.edu.cn) is a doctoral candidate in the Department of Computer Science and Technology, Tsinghua University, Beijing, China. His current research interests are computer network architectures, software defined networks, and next-generation Internet.

KE XU [M'02-SM'09 (xuke@tsinghua.edu.cn) received his Ph.D. from the Department of Computer Science and Technology, Tsinghua University, where he serves as a full professor. He has published more than 100 technical papers and holds 20 patents in the research areas of next-generation Internet, P2P systems, the Internet of Things, and network virtualization and optimization. He is a member of ACM. He has guest edited several special issues in IEEE and Springer journals. Currently, he holds a visiting professorship at the University of Essex, United Kingdom.

JIANPING WU (jianping@cernet.edu.cn) is a full professor and doctoral supervisor in the Department of Computer Science and Technology, Tsinghua University. He is also the dean of the Department of Computer Science and Technology, and the director of the China Education and Research Network (CERNET). His current research interests consist of computer network architectures, next-generation Internet, and formal methods. He has a Ph.D. from Tsinghua University.

YONG CUI (cuiyong@tsinghua.edu.cn) is a full professor and doctoral supervisor in the Department of Computer Science and Technology, Tsinghua University. His current research interests include Internet architectures, IPv6 transition, and quality of service. He has a Ph.D. in computer science from Tsinghua University.

FAN SHI (shifan@ctbri.com.cn) is the network infrastructure director of the Beijing Research Institute of China Telecom. He is also the Co-Chair of the Metro Ethernet Forum China Work Group. His current research interests are IPv4/IPv6 transition and next-generation Internet. He received his Master's degree from the Chinese Academy of Sciences.