中国电信 CHINA TELECOM

SAVI Requirements and Solutions for ISP IPv6 Access Network

http://www.ccf-internet.edu.cn/download/draft-shi-savi-ISP-access-01.txt

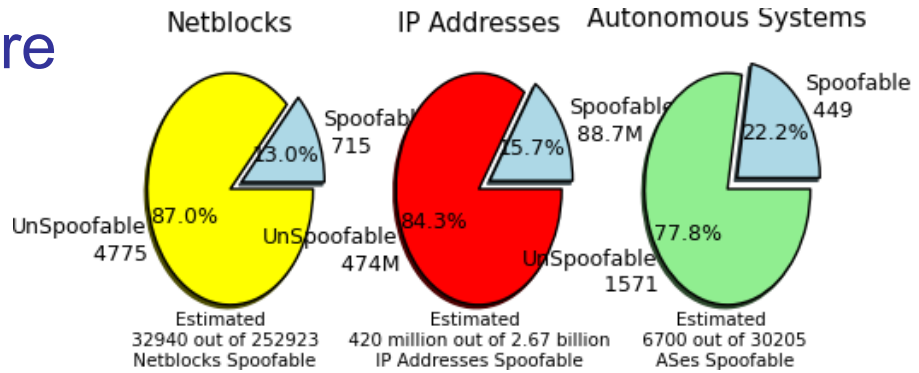
Abstract

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

These scenarios will cover the most of the Internet access scenes in China Telecom. And maybe the reference to other ISPs.

Current Network Situation

- Spoofing issue becomes more critical
- IPv4 exhaustion
- Transition is a long period
- SAVI only works in IPv6 Ethernet subnet with DHPC now.

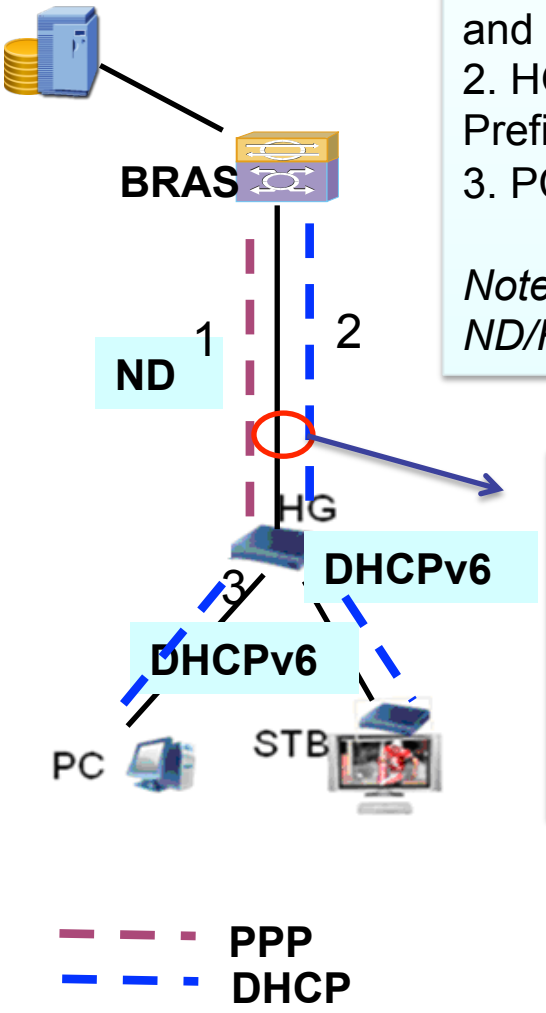


Spoofable netblocks, IP addresses and AS
From MIT spoofer project

RIR	Projected Exhaustion Date	Remaining Addresses in (/8s)
APNIC:	**19-Apr-2011**	1.2052
RIPENCC:	**27-Jun-2012**	3.9161
ARIN:	**06-Jun-2013**	5.9107
LACNIC:	**05-Mar-2014**	4.2732
AFRINIC:	**09-Jul-2014**	4.3815

IPv4 Address Resources
From http://www.potaroo.net/tools/ipv4/

Scenario 1: Home gateway act as DHCPv6 proxy



General Scene Workflow

1. HG get a link-local IPv6 address from BRAS via PPPOE and ND RA. It is the WAN IP address of the HG.
2. HG get IPv6 prefix from BRAS via DHCPv6-PD. It is the Prefix for the ones access to the HG, here are PC and STB.
3. PC or STB device get IPv6 prefix via DHCPv6-PD.

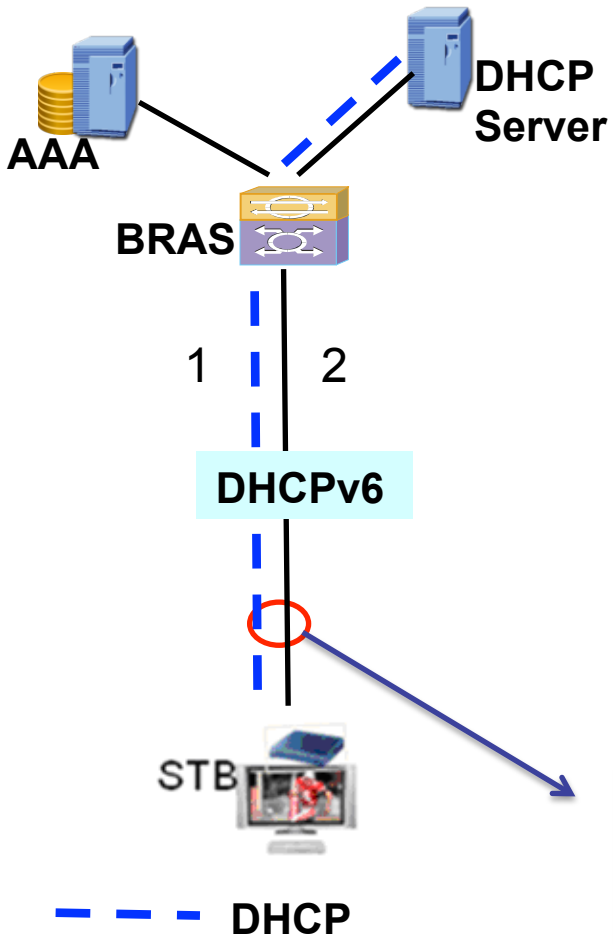
Note: Of course PC and STB can also get IPv6 address via ND/RA, but the DHCPv6 is much popular.

SAVI Solution:

1. Deploy SAVI device to position of near HG
2. SAVI mechanism needs to improve to snoop the procedure of DHCPv6-PD so as to bind the relationship <HG/PC/STB's address, port, MAC>.---It's new one?

Note:
BRAS: Broadband Remote Access Server
HG: Home Gateway. Here HG is L3 router.
STB: Set Top-box

Scenario 2: STB gets IP address via DHCPv6



General Scene Workflow

STB which has internal account and password gets IPv6 prefix by DHCPv6.

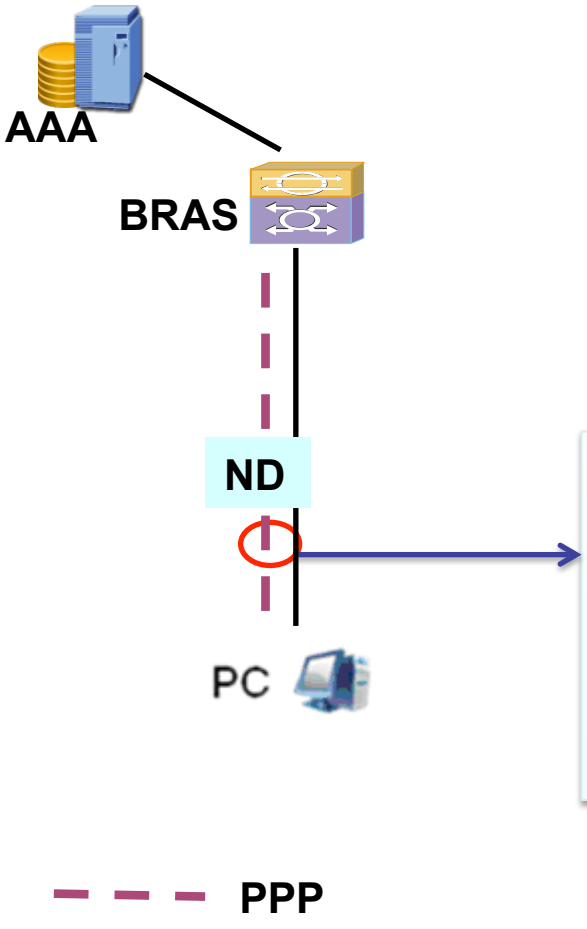
1. STB send request to all routers on local link by using link-local address based on its MAC address.
2. The BRAS informs STB to adopt DHCPv6 address assignment method as a response.
3. STB initiate DHCPv6 procedure and BRAS act as a DHCP Relay to add some authorities' messages.
4. AAA server decides whether assign address parameters according to the result of authentication. BRAS receives IPv6 parameters from AAA server, and then, informs STB by DHCPv6.

Note: There also maybe HG between STB and BRAS, but used as L2 bridge only.

SAVI Solution:

1. Deploy SAVI device to position of near STB
2. It just needs to bind relationship <STB's IP Address, port, STB's MAC Address> which is included in existing function.

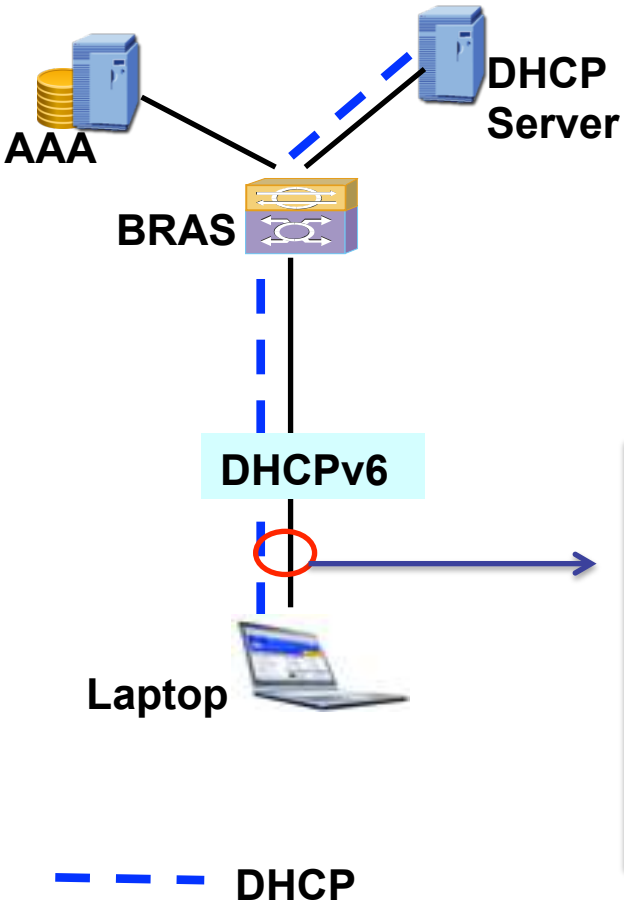
Scenario 3: PC gets IP address via PPPoE & RA



General Scene Workflow
1. PC get link-local address via PPPoE.
2. BRAS broadcast IP prefix via RA
3. PC automatically configuration

SAVI Solution:
1. Deploy SAVI device to position of near PC
2. It is also need to improve its mechanism in order to enable PPPoE snooping like scenario 1 and binding relationship <PC's IP Address, port, PC's MAC>

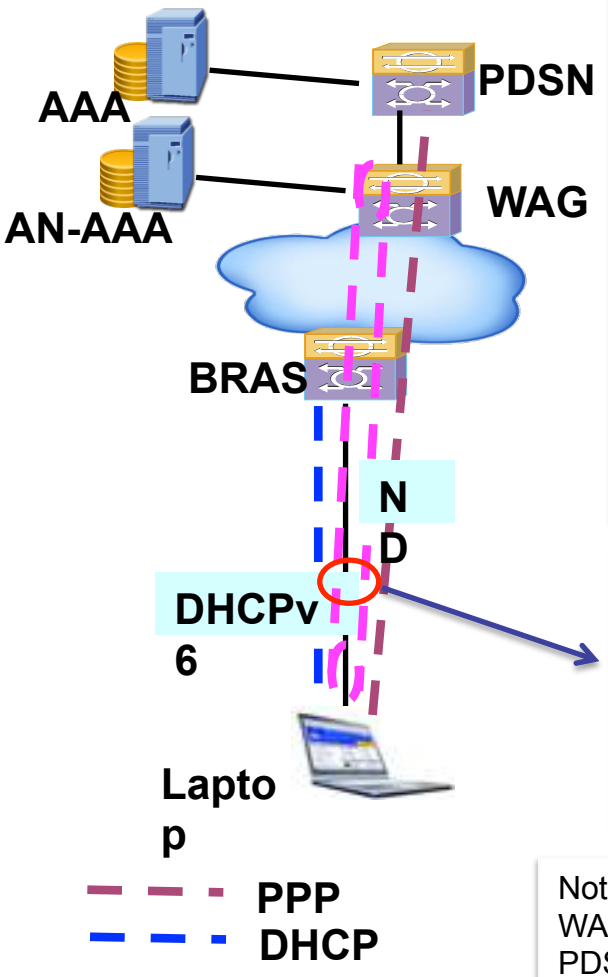
Scenario 4: Laptop accesses Internet via WLAN



General Scene Workflow
1. Laptop get IPv6 address via DHCPv6.
2. Users were enforced to be certified by submitting password on a portal page.

SAVI Solution:
1. Deploy SAVI switch to position of near laptop.
2. It just needs to bind relationship <LAPTOP's IP Address, port, LAPTOP's MAC> which is included in existing function.

Scenario 5: Laptop accesses Internet via C+W



General Scene Workflow

1. Laptop get a temporary IPv6 address from BRAS via DHCPv6.
2. Laptop obtains the WAG address from DNS server. The laptop establishes a UDP tunnel to WAG by sending register request.
3. If the tunnel established successfully, the laptop can get IPv6 prefix from PDSN via PPP and RA, whereas PDSN acts as the PPP terminal.
4. At last, the laptop gets some additional information such as DNS address. When the above steps all accomplished, the laptop acquires the ability to access Internet.

SAVI Solution:

1. Deploy SAVI switch to position of near PC
2. It is also need to improve its mechanism in order to enable PPPoE snooping like scenario 1 and binding relationship <Laptop's IP Address, port, Laptop's MAC>.

Note:
WAG: Wireless Access Gateway
PDSN: Packet Data Serving Node
AN-AAA: Access Network Authentication, Authorization and Accounting Server

中国电信 CHINA TELECOM

Conclusion

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

Authors' Addresses

Fan Shi
China Telecom
Email: shifan@ctbri.com.cn

Ke Xu
Tsinghua University
Email: xuke@mail.tsinghua.edu.cn

Liang Zhu
Tsinghua University
Email: tshbruce@gmail.com

Guangwu Hu
Tsinghua University
Email: hgw09@mails.tsinghua.edu.cn

Thanks!