Open Access Library Journal
2018, Volume 5, e4424
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Securisation of an IPv6 Address Obtaining with SLAAC in Home Networks

S. Y. Massamba[1*], S. A. R. R. Cheikh[2]

[1]Ecole Polytechnique de Thies, Thies, Senegal
[2]University of Thies, Thies, Senegal
Email: *massy@ept.sn, csarr@univ-thies.sn

How to cite this paper: Massamba, S.Y. and Cheikh, S.A.R.R. (2018) Securisation of an IPv6 Address Obtaining with SLAAC in Home Networks. *Open Access Library Journal*, **5**: e4424.
https://doi.org/10.4236/oalib.1104424

Received: February 16, 2018
Accepted: March 16, 2018
Published: March 19, 2018

Abstract

In this article, we present a new method based on the securisation of an IPv6 (Internet Protocol version 6) address obtaining with the SLAAC (Stateless Address Autoconfiguration) method in the domestic network. The particularity of our domestic network is the presence of several Multihoming Internet service providers. The peripherals of the Home Network domain, especially routers are in charge of the relay of auto configuration messages coming from various routers of internet access providers. Our method allows the routers of the Home Network domain to filter the announcements of autoconfigurations called RA (Router Advertisements) according to the IPv6 addresses sources contained in the messages of autoconfiguration. The decision to relay or reject these announcements is based on a trusted table built from the addressing information obtained from the NDP protocol. Our method also aims to optimize the traffic in the Home Network domain by organizing routers to give them specific roles for the relay of information for autoconfiguration.

Subject Areas

Communication Protocols, Computer and Network Security, Information and Communication: Security, Privacy, and Trust, Network Modeling and Simulation

Keywords

IPv6, SLACC, Security, Homenet, Election, Autoconfiguration, RA

1. Introduction

Conscious of the limits of IPv4 in terms of addressing, a new version of the internet protocol was early developed to solve the problems related to the lack of addresses. IPv6 RFC 1883 [1] provides some new features for instance, expanded

addressing, simplified header format, improved extension, auto configuration and option support. IPv6 also integrates a new SLAAC described in RFC 4862 [2] function allowing hosts to attribute themselves an IP configuration through autoconfiguration messages (RA) which routers automatically relay for establishing communication within the network.

In home networks in which one station finds increasingly several Internet Service Providers, the question of the security of the address obtaining insistently arises. Thus, we propose a secure method which ensures that the source of auto-configuration announcements is sure and, at the same time, an optimizing method of the use of the bandwidth shared at the level of the home network that we call HomeNet.

The rest of the paper is organized as follows: Section 2 presents the working environment and the automatic auto-configuration of addresses. Section 3 describes the way how we identify the announcement sources of routers and how we manage the optimization of the bandwidth in the HomeNet while simulations results under NS3 are presented in Section 4.

2. Related Work and Working Environment

The literature proposes several solutions to secure IPv6 networks in general. Specifically in IPv6 Home networks, a lot of work has been done in view to secure the network. Most of these are interested in the security issues related to the services offered by the high layers of model TCI/IP. All these solutions are implemented either at the level of the hosts or the switches. However most of these did not interested in security issues caused by automatic relaying of RAs at routers in SLAAC processes.

The authors of [3] proposed a protocol stack that enables an IPv6 home network and its implementation. The protocol stack includes IPv4/6 dual stacks, home-to-home tunneling, protocol transition and IPv6 multicast packet forwarding over home to-home tunneling.

Kaiser and al. proposed a method that focuses on the design of an IPv6 energy-efficient routing protocol for such complex home networks [4]. Their work considers the exploitation of devices, either routers and/or hosts, links diversity (Ethernet, WiFi, PLC, etc.) as an already pertinent mean to provide energy awareness in home network operations. They solution first enhances the Open Shortest Path Protocol (OSPF) core network routing protocol with a relevant energy metric that reflects the energy consumption of home network links technologies.

In [5], they proposed a set of representative features depends on a suitable formation of data using a flow representation of the traffic. Because a set of attacks on IPv6 networks are due to the vulnerabilities of ICMPv6, they proposed a method that has an acceptable detection capability of RA flooding attacks using several classification techniques.

To the best of our knowledge, this work is the first combining the use of

SLAAC and RA for securing a multihoming environment. Therefore our work is more interested on IPv6 configuration using SLAAC. In this paper, we are interested in the role of routers in obtaining an IPv6 configuration with SLAAC methods. The main objective is to reduce on a router the security flaws of the SLAAC method in order to secure the HomeNet.

2.1. Multihoming

The presence of several internet service providers becomes more and more common in the networks of SMEs/SMIs and in that of houses. When it is activated, multihoming allows to aggregate bandwidths and creates a strong fault tolerance. In IPv6 home networks, multihoming is supported on hosts by using solutions such as SHIM6 [6] which allow using simultaneously several Internet service providers.

2.2. Stateless Auto Configuration (SLAAC)

Introduced with IPv6, SLAAC is one of the three methods which allow hosts to have IP configuration in the network. This method allows a host to have a configuration of addresses which allows it to communicate in the network through messages of Neighbour Discovery (*ND*) type by exchanging messages like Routers Advertisement (*RA*) or Routers Solicitation (*RS*) [7].

In the diagram of the SLAAC, hosts obtain their own IPv6 global addresses through prefixes contained in Router Advertisement (*RA*) which are sent on addresses of local link [2].

2.3. ICMPv6 and NDP

Neighbor Discovery Protocol (NDP) is based on ICMPv6 protocol. We present in the following image the Neighbor Discovery Protocol (NDP) encapsulation (**Figure 1**).

2.3.1. ICMPv6

Described in the RFC4443 [8], it allows to inform about errors concerning IPv6 packets to improve the functions of diagnosis at the level of the network layer. Always going with IPv6, ICMPv6 must be implemented on the level of each IPv6 node. Using several types of messages, in this paper we shall focus specifically on the messages of neighbour discovery type which allow the implementation of the SLAAC.

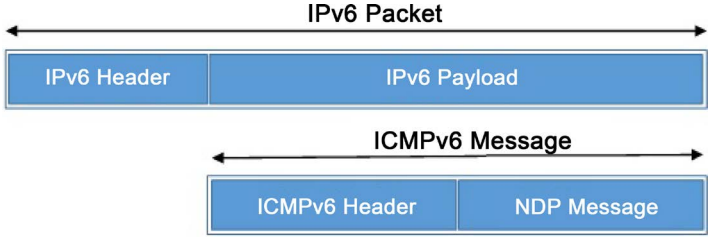

Figure 1. NDP Encapsulation in ICMPv6.

- Type 133 Router Sollicitation,
- Type 134 Router Advertisement,
- Type 135 Neighbor Sollicitation.

2.3.2. NDP

As for the Neighbour Discovery Protocol or NDP, it allows an equipment to integrate into the local environment, that is to say the link on which IPv6 packets are physically transmitted. It also allows to have a dialogue with equipment connected to the same support by using multicast addresses (FF02::1 all stations and FF02::2 all routers. It is not for an equipment to know exactly the list of all other equipment connected on the link, but only to manage those with whom it has a dialogue.

3. Announcement Securisation in the HomeNet Domain

3.1. Working Scenario

Several topologies are used in home networks. We use a topology composed by several connected Internet Service Providers (ISP) linked point-to-point with customer routers of the HomeNet Domain which share the same segment.

Thus, for the design of our safety algorithm, we base on the SLAAC method only where the hosts configure automatically their addresses from the information contained in the Router Announcement (*RA*) messages. To implement our study, we use certain resources supplied by the ICMPv6 protocol to get back the *RA* and the NDP protocol for the exchanges between routers. Given that all the information of configuration are supplied by the providers and since routers relay by default these messages of configuration, messages of router announcement type coming from unknown sources which want to reach the resources of the network can be relayed. What creates a security breach. To mitigate this security breach of the SLAAC, we propose a method which authenticates the source of *RA* in order to ensure that they come from one of our authorized Internet Service Providers.

3.2. Algorithm for Securing RA Ads

Let us consider the HomeNet network to secure the automatic obtaining of IPv6 address. We should check the relay of the Router Announcement (*RA*) messages. These messages are the basis of the SLAAC method.

A hacker exploits the security breach which consists in the fact that a router automatically relays messages of *RA* type. Thus, to implement our approach, we deactivate the automatic relay of *RA*.

To reach our goals, we create three functions which will allow 1) to build the HomeNet Domain, ii) to control *RAs* and at the end 2) identify the source as being sure before proceeding to the relay or rejection.

Each stage has several actions as mentioned below.

1) Building of the HomeNet Domain:

a) Sending of TLV[1] (address and Bandwidth);

b) Definition of each router's roles;

c) Sharing informations of the various Internet Service Providers.

2) RA Relaying:

a) Reception of RAs, announcement messages of IPv6 auto-configuration;

b) Extraction of the address source in the IPv6 auto-configuration messages;

c) Comparison of the address source with the base of the domain's information.

3) Treatment of the message according to the performed checking:

a) Relay;

b) Abandonment.

3.3. Proposed Solution

3.3.1. Building of the HomeNet Database

To build a home network that we call *HomeNet*, a set of stages is necessary:

Initialisation

Routers of the HomeNet domain send each other messages of TLV (*Type Length Value*) type containing the bandwidth of its link with the Internet Service Provider, their unicast address of local link and their system's identifier in grouped diffusion to all the domain's routers.

Stage 1

Each router receiving this type of message from its neighbours and building a TLV database.

Stage 2

Implementation of the function of decreasing sorting (based on the bandwidth of the highest link with the Internet Service Provider).

Stage 3

At this stage, from information received from the NDP protocol as well as TLV sent and received by different routers, we manage:

- Trusted Table ISP Routers for possible sources of autoconfiguration message;
- Router Table of HomeNet Domain;
- And Routers Role Table of HomeNet Domain.

In the last table, we have:

The first entry is the router having the highest bandwidth with the label *P* (*P* = *Principal*).

The second entry is the router having the bandwidth which follows the first one with the label *S* (*S* = *Successor*) used in case of breakdown of Router *P.*

Other entries are that of routers which will be labelled *O* (*O* = *Other*) of the domain.

If two routers have the same value of bandwidth, it places at first the one which has the smallest identifier of the system. The identifier of each router is nothing else than its IP address of local link.

At the end of the process, each router will have in its memory the Database of the HomeNet domain which is nothing than the abovementioned tables.

[1]TVL is a datagram that we use to construct the role table of the all routers in HomeNet.

As illustrated in Figure 2, we show the process of database construction for the HomeNet Domain. The latter will allow to identify the source of the ***RA*** and to organize their *RA* relay while optimizing the use of the bandwidth share of the home network by using the roles (labels) which are allocated to each router.

3.3.2. Relay and Source Identification Process of *RA*

To relay *RA*s, we implement a method which consists in ensuring the origin of the *RA* by validating it through the existence of an entry to the trusted table built on the basis of exchanges made with Provider routers and shared by all the routers of the domain.

Thus, from the table managed by each router of the HomeNet domain after reception of an *RA*, the decision to relay the *RA* or not could be taken by the routers.

The flow chart shown in Figure 3 describes the three stages in the *RA* relay mechanism by home network routers.

In the first stage, we build a function of reception of an *RA* which will allow extracting the address with which the *RA* was sent. With the possibility of being an address of local link, a global and unique address or a non-specified address, it is extracted and compared with the addresses of the trusted table.

In the second stage, if it is informed or not present in the trusted table, the router concludes that the source is unknown, thus, it abandons the *RA* and the process ends.

Thirdly, if the address is checked as present in the trusted table, thus, the *RA* will be sent to the router having *P* tag (*Rtr_P*) in order to be sent to FF02::1 this multicast address specifies all the hosts in the HomeNet domain.

3.3.3. Optimization of the Bandwidth Shared in the HomeNet Domain

Since the home network is of multiple access type, it is important to manage the creation of multiple adjacencies, one adjacency for every pair of routers. To understand the problem with multiple adjacencies, we need to study a formula.

$$Nb\_Adj = \frac{n(n-1)}{2}$$

Formula 1. Number of adjacencies

Nb_Adj: number of adjacencies; *n*: number of routers.

For any number of routers (designated as *n*) on a multiaccess network, we to calculate the number of relations of adjacencies, we base ourselves on the previous formula.

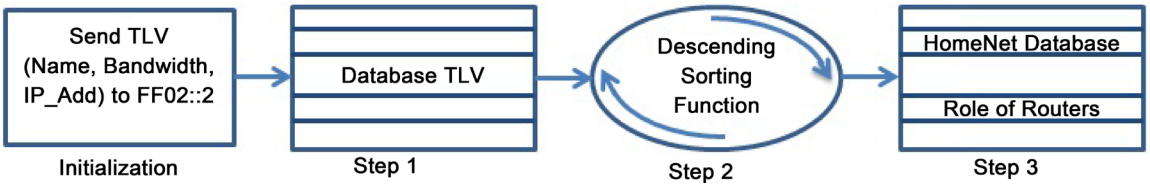

Figure 2. HomeNet database construction.

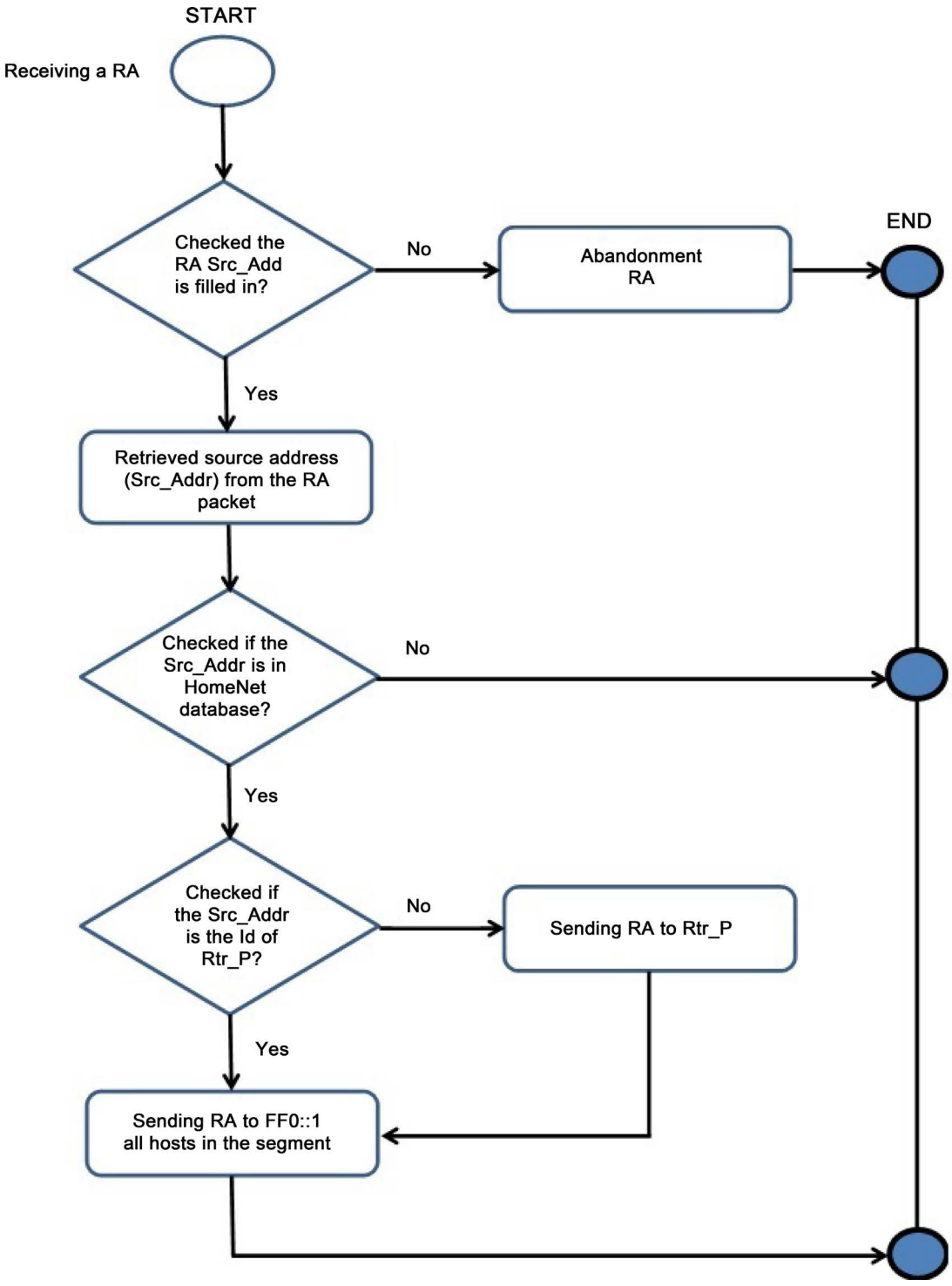

Figure 3. *RA* Relay Mechanism.

This high number of adjacencies increases the consumption of bandwidth especially with the fact that routers use IPv6 addresses of multicast type to relay the various messages to allow a host to autoconfigure itself. If there is no mechanism to reduce the number of proximities, we shall notice a degradation of the bandwidth shared in the HomeNet domain as the number of routers increases.

To mitigate this problem, we implement a method in the creation of the database of the home network which defines the role of each router. *P*, *S* and *O* are the various labels which routers will have to play the roles of:

- *P*: Principal, is in charge of relaying *RA*s.
- *S*: Successor, relays *RA*s in case of breakdown of the router *P*.
- *O*: Other, router member of the domain, has to relay *RA*s in Routers *P* and *S*.

4. Work Topology and Implementation Result in NS3

4.1. Work Topology

To verify the working hypotheses in NS3, we used the topology which has four Provider routers and four customer routers sharing the home network with the RFC-7368 hosts [9] shown in **Figure 4**.

As illustrated in the previous figure, provider routers are connected with those of the HomeNet domain with point-to-point links with a bandwidth dedicated to each link.

What gives a model of home network with several Internet releases which is mutualized in the multihoming.

4.2. NS 3

Network Simulator 3 (NS-3) is an open source simulation Tool. Published under GNU GPLv2 license, it is very used for research to perform simulations of computer networks. Allowing simulating various types of connection, point-to-point, WIFI, CSMA and other forms of data channels, it allows us to display various types of events which arise in a computer network. The community of users and contributors allowed providing a range of libraries in IPv4 and IPv6, which allowed us to implement and to confirm our working hypotheses.

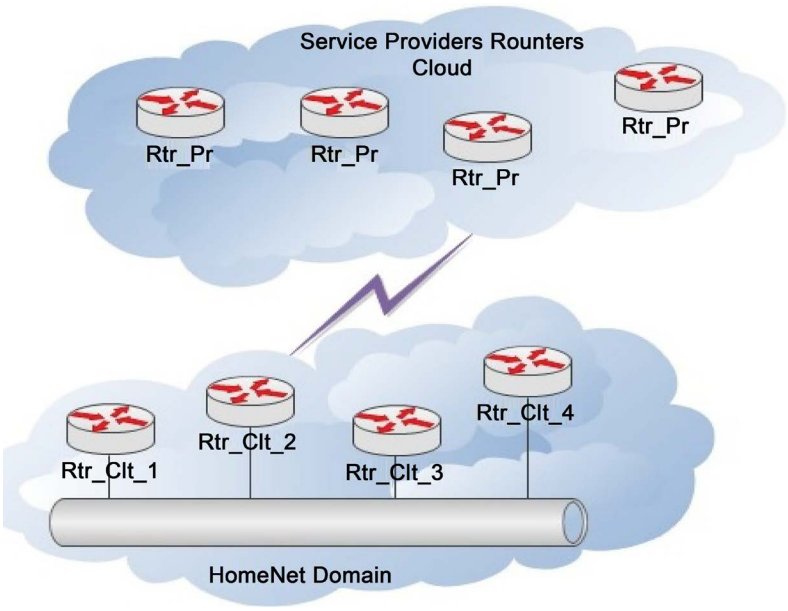

Figure 4. Network topology.

Allowing giving detailed information on simulation events and the exit, Ns-3 possesses a monitoring system which allows visualizing all the events during a simulation. There are numerous indicators which check the types of newspaper and produced information when events or errors occur.

4.3. Results and Interpretation

To validate the source or the origin of *RA* announcements, we split the process of *RA* relay into 3 stages as illustrated in Figure 5.

1) The provider router relays an *RA* message to its customer homology in the HomeNet.

2) The *Rtr_Prov_Clt* router blocks the *RA*, extracts the Source address compares it with its trusted table, looks at its status if it is not labelled *P*, it sends to the *P* labelled router.

3) If it is *P*, it sends to all hosts.

In the case in which the extracted source address is not present in the trusted base, the process stops at stage 2 where the *RA* is abandoned.

4) Implementation results of our algorithm.

In Figure 6, we present the construction of the confidence which goes through various stages.

In Figure 7, we present the trusted table which will allow different routers of the HomeNet Domain to ensure the source of any *RA*. It is built with the extraction function of the source address which allows building it. As we know, the source of an *RA* can be an address of an RFC-2461 [7] local link or another; we present the trusted table with at the same time addresses of local links and the other global addresses to have all Provider routers' information to ensure possible sources of 133 type messages.

In this view, we have the presentation of the Router role table, seen from the

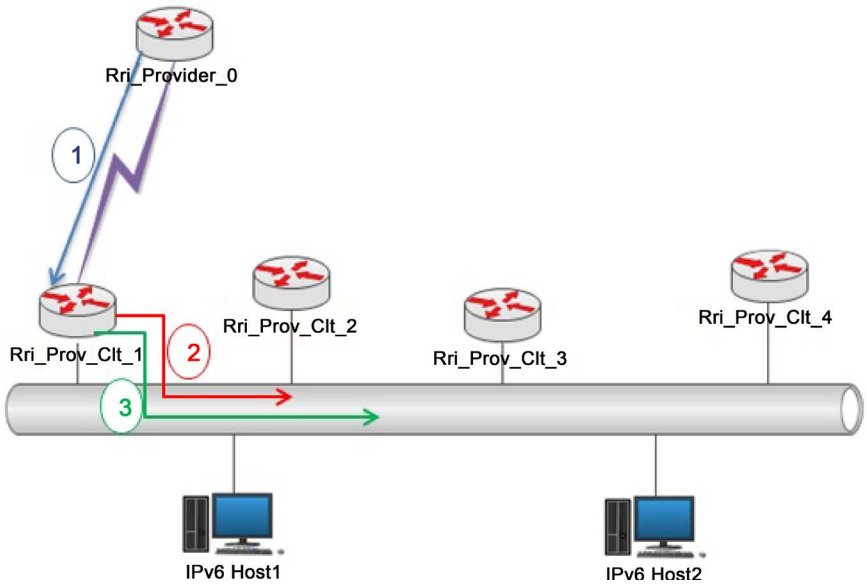

Figure 5. *RA* Processing process.

```
At time 0 Rtr_Provider_1 sent Bandewidth to ff02::2 value 10
At time 0 Rtr_Provider_2 sent Bandewidth to ff02::2 value 7
At time 0 Rtr_Provider_3 sent Bandewidth to ff02::2 value 6
At time 0 Rtr_Provider_4 sent Bandewidth to ff02::2 value 6
```

Figure 6. TLV sending with Bandwidth information.

```
Trusted Address table of ISP routers
Rtr_Provider_0 fe80::200:ff:fe00:1 2001:1::200:ff:fe00:1
Rtr_Provider_5 fe80::200:ff:fe00:3 2001:2::200:ff:fe00:3
Rtr_Provider_6 fe80::200:ff:fe00:5 2001:3::200:ff:fe00:5
Rtr_Provider_7 fe80::200:ff:fe00:7 2001:4::200:ff:fe00:7
```

Figure 7. Trusted ISP Routers table of the domain.

```
View of The HomeNet domain since Rtr_Prov_Clt_3
Router          Bandwidth Address                Role
Rtr_Prov_Clt_1  10        fe80::200:ff:fe00:9      P
Rtr_Prov_Clt_2  7         fe80::200:ff:fe00:a      S
Rtr_Prov_Clt_3  6         fe80::200:ff:fe00:b      O
Rtr_Prov_Clt_4  6         fe80::200:ff:fe00:c      O
```

Figure 8. Routers role table.

```
Address table for the interfaces of the HomeNet domain routers
Rtr_Prov_Clt_1 fe80::200:ff:fe00:9 2001:5::200:ff:fe00:9
Rtr_Prov_Clt_2 fe80::200:ff:fe00:a 2001:5::200:ff:fe00:a
Rtr_Prov_Clt_3 fe80::200:ff:fe00:b 2001:5::200:ff:fe00:b
Rtr_Prov_Clt_4 fe80::200:ff:fe00:c 2001:5::200:ff:fe00:c
```

Figure 9. Routers table of the domain.

```
At time 0.005072s Rtr_Prov_Clt_1 received RA from 2001:1::200:ff:fe00:1 with prefix 2001:1::
At time 0.005072s Rtr_Prov_Clt_1 sent RA to ff02::1 Configure Network is 2001:1::
At time 0.00510286s Rtr_Prov_Clt_2 received RA from 2001:2::200:ff:fe00:3
At time 0.00510286s Rtr_Prov_Clt_2 sent RA to fe80::200:ff:fe00:9
At time 0.00512s Rtr_Prov_Clt_4 received RA from 2001:3::200:ff:fe00:5
At time 0.00512s Rtr_Prov_Clt4 sent RA to fe80::200:ff:fe00:9
At time 0.00512s Rtr_Prov_Clt_3 received RA from 2001:4::200:ff:fe00:7
At time 0.00512s Rtr_Prov_Clt_3 sent RA to fe80::200:ff:fe00:9
```

Figure 10. *RA* relay.

point of view of the *Rtr_Prov_Clt*_3. Thus, each router will have its table with the same information in order to be able to relay an *RA* if the source is identified.

As many the trusted table of the ISP routers is important, we build on the same basis the routers table of the HomeNet domain in Figure 8.

Equally important the trusted table of ISP routers is, we build the routers table of the HomeNet Domain in Figure 9 as well.

In Figure 10, we show the relay of an *RA* identified by the router with the *P* label as role. We see in the debug presented in the figure that our algorithm relays *RA*s whose source is identified by the adequate router to simultaneously manage the optimisation of the shared bandwidth of the HomeNet domain. Oppositely, others having not the label send back the *RA* to the *P* router to enable the *RA* to be relayed to all FF02::1 hosts.

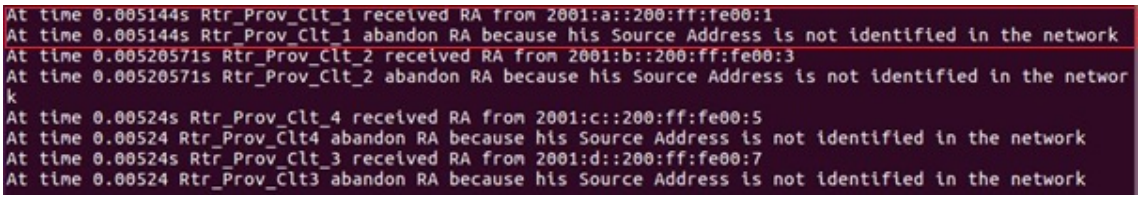

Figure 11. Abandon *RA*.

Finally, in **Figure 11**, we present the script in which an *RA* doesn't come from an identified source. In fact, we see that the packet is abandoned. This allows ensuring that our treatment model of an *RA* functions correctly.

Thus, whatever the router of the HomeNet domain, it abandons all RA with non-identified source because missing from the shared trusted table!

5. Conclusion

In this article, we presented and implemented a new method of security for obtaining an IPv6 configuration in the home networks. We were rather interested in the roles played by routers during the process. It would be interesting in future research to see in the first time on how to authenticate the exchanges between various routers in order to improve the security of our method. It should be done for example by using cryptographic exchange. In the second time, we will examine how to integrate our method with FHS (First Hop Security) [10] to have a total control of the mechanisms of security on every equipment of interconnection in the HomeNet Domain (routers and switches) and finally to see its compatibility with the generation of certificate such as CGAs [11].

References

[1] Deering, S. and Hinden, R. (1995) Internet Protocol, Version 6 (IPv6) Specification. RFC1883, Xerox PARC, Ipsilon Networks. https://doi.org/10.17487/rfc1883

[2] Thomson, S., Narten, T. and Jinmei, T. (2007) IPv6 Stateless Address Autoconfiguration. IETF RFC 4862, Cisco, IBM, Toshiba.

[3] Park, M., Kim, J.-T., Paik, E.H. and Park, K.-R. (2007) Deployment Strategy and Performance Evaluation of the IPv6 Home Network Using the Home Server. *IEEE Transactions on Consumer Electronics*, **53**. https://doi.org/10.1109/ICCE.2007.341546

[4] Kaiser, A. and Boc, M. (2014) Energy-Efficient Routing in IPv6 Home Networks. CEA, LIST, Laboratoire des Systemes Communicants, 2014 23*rd International Conference on Computer Communication and Networks* (*ICCCN*), 4-7 August 2014, Shanghai. https://doi.org/10.1109/ICCCN.2014.6911769

[5] Elejla, O.E., Belaton, B. and Anba, M. (2017) A New Set of Features for Detecting Router Advertisement Flooding Attacks. 2017 *Palestinian International Conference on Information and Communication Technology*, 1-5. https://doi.org/10.1109/PICICT.2017.19

[6] Nordmark, E. and Bagnulo, M. (2009) Shim6: Level 3 Multihoming Shim Protocol for IPv6. Sun Microsystems, UC3M.

[7] Narten, T., Nordmark, E. and Simpson W. (1998) Neighbor Discovery for IP Ver-

sion 6. IETF RFC 2461, IBM, Sun Microsystems, Daydreamer.

[8] Conta, A., Deering, S. and Gupta, M. (Eds.) (2006) Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. IETF RFC 4443, Transwitch, Cisco Systems, Tropos Networks.

[9] Chown Ed, T., Arkko, J., Brandt, A., Troan, O. and Weil, J. (2014) IPv6 Home Networking Architecture Principles. IETF RFC 7368, University of Southampton, Ericsson, Sigma Designs, Cisco Systems, Inc., Time Warner Cable.

[10] Kumar, A. and Mani, R.S. (2013) First Hop Security Considerations in IPV6 Implementation. National Knowledge Network, National Informatics Centre, New Delhi, India.

[11] Yao, G. and Bi, J. (2008) A CGA Based IP Source Address Authentication Method in IPv6 Access Network. *IEEE Local Computer Networks* (*IEEE LCN*), 534–535. https://doi.org/10.1109/LCN.2008.4664225