A Model of Customer Premises Equipment for Internet Protocol Version 6

Ihsan Lumasa Rimra, Firdaus, Wiwik Wiharti, and Andrizal, *Member, IACSIT*

***Abstract*—Computers and other communication devices at home connect to Internet through the Customer Premises Equipment (CPE) using addresses called IP address. The implementation of IPv6 addressing format needs to be taken into account so as to solve the depletion of IPv4 addresses. This research is aimed to demonstrate a CPE model that can be applied on IPv6 in the technical maturity of an end-to-end high bit rate fixed access network. It is mainly implemented in order to consider the features and protocols embedded in the CPE to make it smoothly adaptable on IPv6. The features of IPv6 autoconfiguration and DHCPv6 client are operated by the CPE to obtain an IPv6 address and a prefix. They can be further used to provide addresses for the terminals within the CPE to make communication to the outside of the network or Internet. In addition, the SIP client feature is installed on CPE since it is required by a VoIP phone client so as to exchange information to others. In case of the communication and terminals within the CPE that still perform IPv4 addresses the CGN DS Lite approach is activated. We demonstrated that the communication supported by CPE could only be provided on the same addressing format. IPv4 devices connect only to other IPv4 devices since IPv4 and IPv6 implement different methods on their addressing format.**

***Index Terms*—CGN DSLite, CPE, IPv4, IPv6.**

I. Introduction

A significant increase of Internet users and connected devices has made the exhaustion on Internet Protocol version 4 (IPv4) addresses [1]. The computer portable, PDA, smartphones and other home entertainment devices with networking abilities are easy to find nowadays. All of them have delivered the increment in the number of devices connected to home network for sharing and concurrently accessing the Internet. As a consequence, it is hard for new home Internet users to obtain IP addresses from broadband network providers for their home gateways. This has been challenging network operators to provide connection to users since addresses are needed. However, IPv6 (Internet Protocol version 6) as a new generation network technology comes to deal with the problem faced by IPv4 since it has longer addressing format.

The home gateway also known as Customer Premises Equipment/ CPE or residential gateway has been defined as in [2], [3]. Developing of CPE devices on broadband networks for a collection of home networking hardware behind CPE are addressed for users to support multiple telecommunication services as [4]. Furthermore, the convergence era of telecommunication services and applications connecting the fixed access network and mobile network must be taken into account to make CPE [5] can fulfill requirements to support the network storage provision, remote management and packaging services such as data, voice and video application such as VoIP, IPTV and other multimedia services [6].

As the home network becomes popular, integrating IPv6 into the CPE is a new demanding for network providers. Moreover, the emerging of telecommunication convergence services and social necessity forces network providers to develop a CPE that compatible with IPv6. For sure, the QoS must be guaranteed for IPv6 applications as in IPv4. An example, the voice quality on VoIP will keep remain the same on IPv6 as well as IPv4.

In this paper, we aim to give details of this novel CPE model. Section II describes features provided by CPE. In addition, its requirements will be discussed to make it adaptable for both IPv6 and IPv4 for a variety of Internet services. The implementation on IPv4 must be considered since some services, applications and other devices work only for IPv4. Section III shows the network scheme diagram for developing a CPE model. Furthermore, the general architecture of IPv6 network is also taken into account. In the Section IV, we take emphasis and realize the technical implementation of our work on IPv6 as well as IPv4. Finally, we put forward the conclusion in Section V.

II. CPE Requirements

Introducing IPv6 on the CPE brings some requirements that need to be fulfilled [7]. However, the CPE will not only be implemented for IPv6, but also for IPv4. The requirements and features are applied so as to make the CPE can smoothly adapt on two different addressing formats.

A. IPv6 Autoconfiguration

This feature enables devices to be configured automatically. Once a device is connected to the network infrastructure, it will be allocated an IPv6 prefix using the DHCPv6 (Dynamic Host Configuration Protocol version 6) mechanism to easily support IPv6 implementation. The obtained addresses must allow users for accessing all services including voice, video and Internet using IPv6 connectivity.

A CPE router, in a general scheme as can be seen in Fig. 1, consists of a router that has a WAN interface connected to the access network, a LAN bridge, a switch, some ethernet ports and Wi-Fi capabilities. It also connects the phones for the voice communication purposes via Z interface.

Manuscript received July 10, 2013; revised August 27, 2013. This work was fully supported by the Directorate General of Higher Education of Indonesia (DIKTI) under the Grant of Hibah Bersaing.

The authors are with Department of Electronics Engineering, State Polytechnic of Padang, Indonesia, 25163 (e-mail: {rimra, mrdauz, wiwik, andrizal}@ polinpdg.ac.id).

DOI: 10.7763/IJIMT.2013.V4.468

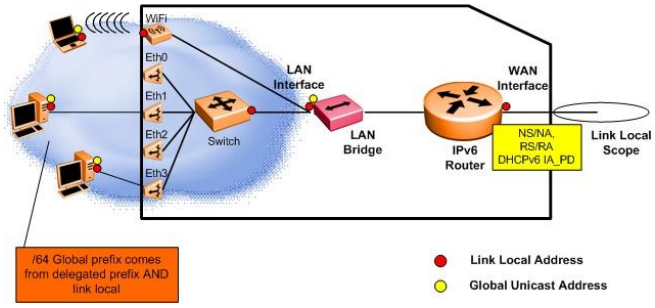

Fig. 1. General scheme of a CPE.

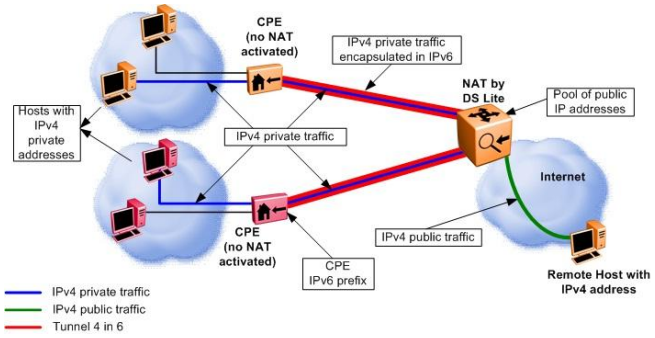

Fig. 2. DS lite design.

We observed that the preferred model of WAN interface is using the unnumbered model as in [8]. The associated address on the WAN interface of the CPE router is only one LLA (Link Local Address). However, the GUA (Global Unicast Address) is still necessary to make the CPE capable to communicate to service platforms. Using a prefix delegation, the GUA then is developed for communications between the CPE router and service platforms.

B. DHCPv6

DHCPv6 feature is implemented because it provides all address information including network part and host part. Deploying DHCPv6 with prefix delegation capabilities must consider that the CPE as the requesting router will further allocate the prefixes for the devices in the home network.

Prefix delegation provides a means for delegating IPv6 prefixes to CPE devices that act as requesting routers [9]. It is primarily meant to automate the enforcement of an IPv6 prefix assignment policy [10]. It also simplifies the DHCPv6 mechanism in that only a subset of DHCPv6 messages is required for prefix delegation and related configuration. Furthermore, a stateless DHCPv6 server is aimed to a host that has obtained IPv6 prefix.

C. CGN DS Lite

Unfortunately, IPv6 cannot fully replace IPv4 yet since most services in public Internet are still in the IPv4 format. In addition, some network devices and workstations are still not capable of using IPv6. Hence, developing this CPE that is also suitable for IPv4 is useful.

No more NAT (Network Address Translation) function is activated in CPE. Instead, CGN (Carrier Grade NAT) DS Lite (Dual Stack Lite) exists in the core network of the operator and is in charge of sharing a single public IPv4 address for several subscribers as in [11]. DS Lite approach allows therefore to using the few remaining IPv4 addresses between a large numbers of subscribers. This may allow network providers to still provide IPv4 to IPv4 communications without delegating a public IPv4 address to each subscriber as it is the case up to now in most of network deployments.

Using this approach, the privately addressed IPv4 traffic coming from the hosts in the LAN is encapsulated in IPv6 datagram by the CPE. This CPE then forwards the corresponding IPv6 packets to the CGN. Fig. 2. shows the design of DS Lite approach.

The requirements of DS Lite approach are listed as follows:

1) The access network is connected the CPE to the core network is IPv6 enabled.
2) CGN can be reached by DS Lite enabled CPE by means of IPv6 address through option 64 of DHCPv6 messages.
3) The CPE must support tunneling IPv4 in IPv6.

The CGN DS Lite must implement a Network Address Port Translation (NAPT) as in [12] since it translates both the source IP address and port identifier for TCP or UDP packets. It allows a group of hosts that is not connected to the same CPE to share one single external address. The pool of IPv4 public addresses maintained by the CGN DS Lite must be configurable by the service provider. DHCPv6 feature is implemented because it provides all address information including the network part and host part. Deploying DHCPv6 with prefix delegation capabilities must consider that the CPE as the requesting router will further allocate the prefixes for devices in the home network.

Based on [11], the CGN should be able to handle the following information:

1) The CPE identifier as a part of NAT entries related to the CPE. It is necessary since the pair of private address and port is not sufficient to uniquely identify the relevant CPE due to the fact that any customer's terminals may use any private address in its home network.
2) IPv6 address of CPE that encapsulates the IPv4 traffic in IPv6 datagrams need to be forwarded back.

In its concept, the NAT entries can be seen as tuples consisted of the private address, private port, CPE identifier, public address, public port and protocol in which the obtained CPE's identifier is the GUA of the CPE. Two components are available in DS Lite implementation, DS Lite B4 (Basic Bridging Broadband) in the CPE side and DS Lite AFTR (Address Family Transition Router) in CGN side as in [13].

One important feature of DS Lite is that the IPv4 end host communicates only with the IPv4 destination host and the IPv6 end host also communicates only with the IPv6 destination host. The devices that use IPv6 addresses will be directly destined to IPv6 Internet and will be not influenced by DS Lite mechanism. It should be noted that there is no communication between hosts using different IP version.

D. SIPv4 and SIPv6 Client

Being a dual stack node, CPE should be able to receive and send both IPv4-formatted and IPv6-formatted traffic including SIP (Session Initiation Protocol) traffic. A SIP client in the CPE acts as a client that provides VoIP services for the terminal in the home network. This protocol is used to create, modify and terminate voice and video calls and

multimedia session.

A SIP end point known as UA (User Agent) could also be embedded in a UE (User Equipment) that refers to end-user terminal. In order to ensure the SIP-based connectivity for both the IPv4 and IPv6 customers, the CPE should manage the SIPv4 and SIPv6 clients in its configuration that is also known as Dual Stack enabled UE devices. It is mainly developed for the IPv4 customers in accessing SIP based service after the implementation of IPv6 capabilities. This IP versions' heterogeneity should be transparent for end-users and no degradation in services should be observed when interconnecting heterogeneous UEs. It must be noted that configuring the SIP UA in the CPE with IPv6 connectivity has no impact on the configuration of UA in the LAN. Indeed, UA can still use IPv4 connectivity if the firewall and NAT are correctly handled.

When the SIP UA is embedded in the CPE, no particular constraint is to be handled for accessing the service using IPv6. No protocol translation function is required in the CPE since the IPv6 traffic may directly go through the core network to the SIP server. In order to avoid CGN DS Lite crossing (especially for media flows), the SIP UA must be seen as IPv6-only UA. However, if an IPv4 private address has been assigned, for example the UA is not embedded in the CPE but it is located in the LAN, this would imply that both SIP and media flows would cross the CGN. Furthermore, in long-term development, all the UE devices will only support for IPv6 addresses allocation in order to fully migrate to IPv6.

In the context of migration to IPv6, some policies can be envisaged such as assigning only an IPv6 address and no IPv4 address to the SIP UA whenever possible. To do so, the CPE should be aware about the IP capabilities of the SIP UA.

III. Network Infrastructure

In this section, we present the network scheme infrastructure used during the research implementation as can be seen in Fig.3. The network consists of a PC as a server with Debian Linux Operating System, a Raspberry Pi as the CPE and two PC clients using Ubuntu Linux and Windows 7. The PC server is installed with DHCPv6 server, DNSv6 server, Internet service platform, voice service platform and application platform. Furthermore, the Raspberry Pi is configured with Debian Linux. It is based on ARM1176JZF-S core with 700 MHz processor and 256 MB memory that has a 10/100 Ethernet port, USB port, 8 pin I/O port and LCD panels via DSI. It is further implemented as the CPE.

IV. Service Integration

The first implementation verifies the CPE's capability to derive the address provided by DHCPv6 server. As soon as CPE is connected to the network, it firstly creates its LLA on WAN interface using EUI-64 method. The CPE constructs its link local address based on address autoconfiguration. The CPE router must start the DHCPv6 client process as soon as link local address has been assigned to the WAN interface without waiting for Router Advertisement from the default IPv6 router. Even though the CPE is a router, it becomes a universal agreement to consider the CPE, as a terminal on its WAN interface and it is therefore possible to obtain the default route provided by Router Advertisement.

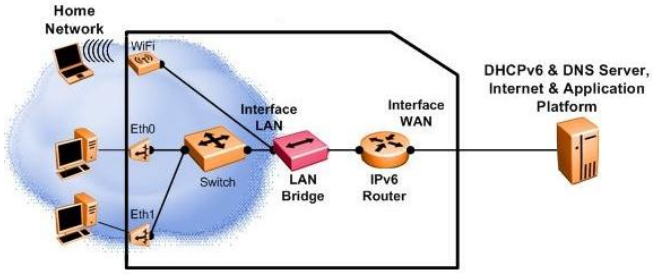

Fig. 3. IPv6 network architecture model.

```
nas6    Link encap:Ethernet  HWaddr 00:09:A9:09:26:00
        inet addr:169.254.1.1  Bcast:169.254.255.255  Mask:255.255.255.255
        inet6 addr: fe80::209:a9ff:fe09:2600/64  Scope:Link

brLAN   Link encap:Ethernet  HWaddr 00:09:A9:09:26:00
        inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: 2a01:cf00:75:4400:209:a9ff:fe09:2600/64  Scope:Global
        inet6 addr: fe80::209:a9ff:fe09:2600/64  Scope:Link
```

Fig. 4. LLA of the CPE router and GUA of bridge LAN interface.

In order to speed up the process, the CPE must send a router solicitation message in order to rapidly receive a solicited router advertisement message. In addition, to obtain the default route, the CPE also recovers MTU (Maximum Transmission Unit) information within the payload of RA messages. It is not mandatory for the CPE to take into account the Managed and Other bits provided by DHCPv6 server, as a delegating router and the only trigger for starting DHCPv6 process is the validation of LLA address.

Fig. 4 shows the LLA of WAN interface and the GUA of LAN interface. The nas6 represents the CPE's WAN interface as the LLA based on EUI-64 addressing format. The LLA of that CPE is fe80::209:a9ff:fe09:2600/64. The GUA of the LAN interface exists on the brLAN. The brLAN (bridge LAN) is the LAN side of the CPE router which is allocated a global address. From the obtained prefix delegated to the CPE router which is 2a01:cf00:75:4400/56, the brLAN derives its address as the combination of the prefix, a sub prefix identifier and interface ID.

From the perspective of the LAN interface, based on the DHCPv6 prefix delegation, the LAN is configured to learn the IA_PD (Identity Association for Prefix Delegation) in order to assign addresses to the LAN interface. If DHCPv6 process does not succeed, the LAN will not be able to derive global unicast prefixes (/64) for the terminals. The derived /64 prefix from delegated /56 prefix is further advertised in RA. Here, IPv6 prefix, DNS information, default route and MTU allocation for the terminal clients in the home network are determined by CPE router through SLAAC (stateless address autoconfiguration) process by starting the mechanism of Router Advertisement Daemon (radvd) when the first time the CPE boots. Hence, if a host in the home network sends router solicitation, the CPE replies with RA. The radvd coming from CPE router enforces the configuration for interface settings, routes and prefixes

including valid and preferred lifetime.

Fig. 5 presents an obtained GUA and LLA of a client interface behind CPE. Based upon a prefix obtained from the CPE which is 2a01:cf00:75:4400::/64, the interface gets its GUA as a combination of a prefix and EUI-64 derived from its hardware address f0:4d:a2:38:0c:e9. Hence, the GUA of this interface is 2a01:cf00:75:4400:f24d:a2ff:fe38:ce9.

The second implementation is IPv6 based VoIP service by managing a SIP server. We develop a SIP IPv6 server using Asterisk 1.8.4-1, two CPE devices embedding a SIP UA compatible with both IPv4 and IPv6, two phones connected to each CPE and two PC clients with Linphone (version 3.4.3).

```
eth0    Link encap:Ethernet  HWaddr f0:4d:a2:38:0c:e9
        inet adr:192.168.1.84  Bcast:192.168.1.255  Masque:255.255.255.0
        adr inet6: 2a01:cf00:75:4400:f24d:a2ff:fe38:ce9/64 Scope:Global
        adr inet6: fe80::f24d:a2ff:fe38:ce9/64 Scope:Lien
```

Fig. 5. GUA and LLA of a client.

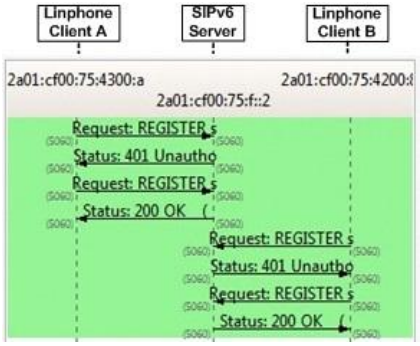

Fig. 6. Registration process of Linphone clients.

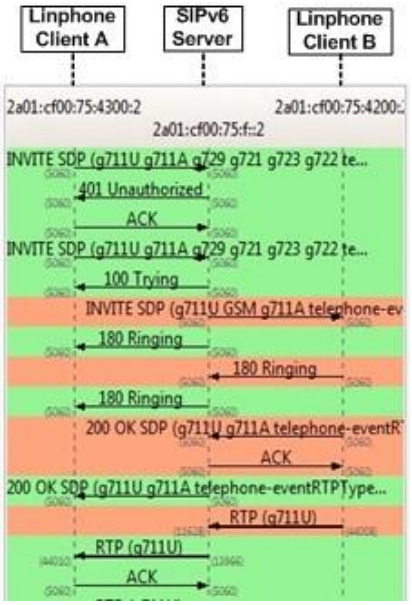

Fig. 7. Communication between two phone clients.

Fig. 6 shows the registration of two VoIP clients to the SIP server by sending register request messages. The SIP server responds with 401 Unauthorized since the VoIP clients have not entered their usernames and passwords correctly. A valid SIP server response is 200 OK.

Fig. 7 presents a communication of SIP clients that can be made after clients registration process is OK. The session invitation of a client uses SDP protocol negotiating all associated properties used during communication. Further, RTP is used as the transport function to stream the voice.

The last implementation analyzes the CGN DS Lite application. It is implemented in order to enable IPv4-to-IPv4 communications with in an IPv6 only access network. Web application is performed on this CGN DS Lite since it uses the same communication port for downlink and uplink from IPv4 devices in the home network to IPv4 remote hosts in Internet.

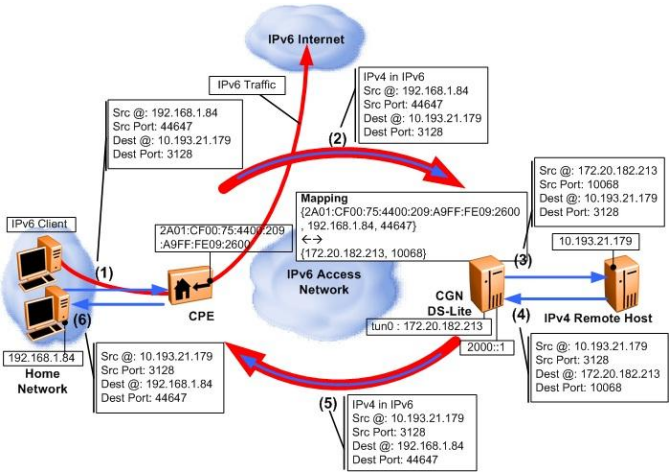

Fig. 8. CGN DS Lite implementation scheme

TABLE I: CGN ADDRESS MAPPING

From CPE to Remote Host	
- *Come from CPE*	: IPv6 source @ + IPv4 private source @ + Port No
- *Going to Remote Host*	: IPv4 public source @ + Port No
From Remote Host to CPE	
- *Come from Remote Host*	: IPv4 public destination @ + Port No
- *Going to CPE*	: IPv6 destination @ + IPv4 private destination @ + Port No

In its implementation, the CGN DS Lite uses the AFTR 1.1 (Address Family Transition Router) software as in [13] on the CGN side. This AFTR detects a new CPE by the detection of an unknown source IPv6 address and automatically creates a tunnel IPv4 in IPv6 interface towards this CPE. Moreover, this implementation needs a tun4in6 function in the CPE so as to make this CPE can tunnel the IPv4 traffic into IPv6 traffic.

Fig. 8 describes the CGN DS Lite implementation. The traffic of IPv4 devices in the home network is encapsulated within IPv6 packet that uses the unique IPv6 global address of the CPE. This unique IPv6 global address of the CPE will differentiate between IPv6 global address of a customer and others. For example, the IPv4 traffic that has a source address 192.168.1.84 and source port 44647 destined to destination address 10.193.21.179 and destination port 3128 is encapsulated using the CPE's IPv6 global address and is tunneled through IPv6 access network.

On the CGN side, this packet is decapsulated and a CGN mapping function translates this source IPv4 private address and its source port into a source IPv4 public address and a source port of the provider that are in this case 172.20.182.213 as the source address and 10068 as its source port. In other words, it can also be said that there is an address

mapping function in the CGN as shown in Table I. Furthermore, when the remote host replies with its IPv4 packet, the CGN will be matching the IPv4 destination address with the specific IPv4 address and port that depend on the IPv6 address in the CGN mapping function. This packet is then encapsulated and tunneled using IPv6 address of the CGN as a source address and IPv6 address of the CPE as a destination address. It is further forwarded to the specific CPE which decapsulates the IPv4 packet and forwards it into the LAN without further processing.

V. Conclusion

This work shows that the network maturity regarding the introduction of IPv6 can be further developed and implemented in the core and access network as well as in the home network. CPE specifications illustrated by Raspberry Pi are fully functional. DHCPv6 server implementation is the mirror of the actual DHCPv6 specifications and no issue has been detected yet. Regarding VoIP, the open source SIP server has proved that it can be deployed. There are no more obstacles for IPv6 based VoIP deployment. Nevertheless, some applications have not dealt and not fully supported IPv6 yet. The protocols supporting the applications need to be improved in order to migrate to IPv6. Furthermore, DS Lite has been implemented in order to illustrate the capability to perform IPv4 to IPv4 communications in a context of IPv4 depletion. Nevertheless, CGN has nasty effects on some services for various reasons. One of them is that it is no more possibility to identify the client through its IP address. However, we do not address an issue related to IPv4 to IPv4 communication implementing Port Control Protocol (PCP) on CGN DS Lite mechanism. It is an obvious idea for future research.

Acknowledgment

The authors wish to thank Laurent Toutain, Xavier Pougnard and Vincent Huet for valuable guidance.

References

[1] APNIC's IPv4 pool usage. (June 2013). The APNIC website. [Online] Available: http://www.apnic.net/community/ipv4-exhaustion/graphical-information
[2] S. Gupta, "A white paper: Home gateway," Wipro Technologies.
[3] C. A. Eldering, "Customer premises equipment for residential broadband network," *IEEE Communications Magazine*, pp. 114-121, 1997.
[4] W. T. Chang, W. Y. Li, D. G. Messerschmitt, and N. Chang, "Rapid deployment of CPE-Based telecommunications services," *Communications: The Global Bridge*, vol. 2, pp. 876-880, 1994.
[5] F. T. H. den Hartog, M. Balm, C. M. de Jong, and J. J. B. Kwaaitaal, "Convergence of residential gateway technology: Analysis of evolutionary paths," *IEEE*, pp. 1-6, 2004.
[6] S. Chintada, P. Sethuramalingam, and G. Goffin, "Converged services for home using a SIP/UPnP software bridge solution," *IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2008 proceedings*, pp. 790-794, 2008.
[7] H. Singh, W. Beebee, C. Donley, B. Stark, and O. Troan, "RFC: 6204, basic requirements for IPv6 customer edge routers," *IETF*, 2011.
[8] H. Singh, W. Beebee, C. Donley, B. Stark, and O. Troan, "Internet-Draft, IPv6 CPE Router Recommendations," IETF Network Working Groups, 2009.
[9] O. Troan and R. Droms, "RFC: 3633 IPv6 prefix options for Dynamic Host Configuration Protocol (DHCP) version 6," IETF Network Working Groups, 2003.
[10] S. Miyakawa, "RFC: 3769 requirements for IPv6 prefix delegation," IETF Network Working Groups, June 2004.
[11] A. Durand, R. Droms, J. Woodyatt, and Y. Lee, "RFC: 6333 Dual-Stack lite broadband deployments following IPv4 exhaustion Draft-ietf-Softwire-Dual-Stack-Lite-11," IETF Network Working Groups, 2011.
[12] P. Srisuresh and M. Holdregeet, "RFC 2663: IP Network Address Translator (NAT) terminology and considerations," IETF Network Working Groups, 1999.
[13] The ISC website. [Online]. Available: www.isc.org/software/aftr

Ihsan Lumasa Rimra was born in Padang, Indonesia, in 1978. He received his MSc degree in design and engineering of convergent networks from Telecom Bretagne in Rennes, France, in 2011. He also took a part in a research project on IPv6 end to end implementation in Research and Development of France Telecom, France.

He immediately incorporates to the Computer Networking Laboratory State Polytechnics of Padang to take part in several research projects regarding IPv6, Internet access network and Wireless Communication. He is also a Lecturer of the Computer Networking, Data Communication and Internet Technology Subject at State Polytechnics of Padang, Indonesia.

Firdaus was born in Bengkulu, Indonesia in 1977. He received his bachelor degree in electronic engineering from Institut Teknologi Sepuluh Nopember, in 2002. Then, he obtained his MT degree also in electronic engineering from the same institute in 2011. He works as a lecturer in State Polytechnics of Padang, Indonesia at the electronics engineering department. His research interest is in electrical engineering and takes part in the application of embedded system in electronic control system research.

Wiwik Wiharti was born in Surabaya, Indonesia in 1977. Bachelor of instrumentation engineering, 2002 and Master of control system engineering, 2010 by the Institut Teknologi Sepuluh Nopember.

Her research is focused on developing of control system and embedded system. She is also a lecturer in State Polytechnics of Padang at the electronics engineering department.

Andrizal was born in Saruaso, Indonesia in 1968. He received his undergraduate degree in computer engineering from Institut Teknologi Bandung, in 2001. At the same university, he continued to obtain his MT degree in computer engineering in 2005.

His research is focused on human machine interaction and embedded of control system. He works also as a lecturer in State Polytechnics of Padang, Indonesia at the electronics engineering department.