
Ihsan Lumasa Rimra1*, Wiwik Wiharti2, Surfa Yondri3
1Department of Telecommunication Engineering, State Polytechnic of Padang, Indonesia.
2Department of Electronics Engineering, State Polytechnic of Padang, Indonesia.
3Department of Electrical Engineering, State Polytechnic of Padang, Indonesia.

* Corresponding author. Email: rimra@polinpdg.ac.id
Manuscript submitted August 20, 2014; accepted November 4, 2014.
doi: 10.17706/ijcee.2014.v6.865

Abstract: The transition between the utilization of IPv4 and IPv6 leads ISPs to develop a new mechanism so as to continue services for customers. In one hand, ISPs are pushed in implementing IPv6 protocol as the new technology. In another hand, there are many users and services still provided by IPv4 protocol. The CPE as an equipment at customer’s premises must be able to pass any kind of services at any kind of IP traffic on dual stack environment. In order to support communication between IPv4 terminals beyond the IPv4 depletion issue, the CGN DS Lite approach is implemented. This paper presents two features of dual stack CPE which allow IPv4 traffic and applications implementing port forwarding operation to communicate through IPv6 access network. The PCP capability is taken into account between the CPE and CGN with some UPnP-PCP proxy capabilities in the CPE. We demonstrate that PCP gives an opportunity for customers in the home network behind the CGN to manage their interactive applications.

Key words: CPE, IPv4, IPv6, CGN DS-Lite, PCP, UPnP.

1. Introduction

The addressing protocol of Internet Protocol version 6 (IPv6) has been introduced since 1995. This is a result of the depletion of Internet Protocol version 4 (IPv4) addresses to provide unique identities for Internet devices [1]-[3]. Unfortunately, the development of IPv6 application and implementation seems very slow and is not as expected [4]. Since it is launched globally on June 2012, most of operating systems, hardware and software have supported to use IPv6 protocols. However, it has not been able to fully replace the functionality of IPv4 universally. Furthermore, the growth of utilization of smartphones, computer portable and home networking devices are affecting and accelerating the demanding of Internet addresses. This is obviously a big challenge for network providers to continuously afford services for home customers since there is incompatible format between IPv4 and IPv6 on this transition periods.

Some approaches have been implemented by Internet Service Providers (ISP) in order to make smooth the transition between the utilization of IPv4 and IPv6 [5]–[14]. Unfortunately, all of them did not meet the requirement on the implementation of IPv4 services via IPv6 network. In addition, a new method of IPv4 to IPv6 translation algorithm provided for ISPs called IVI has not took into account the issues of applications implementing IPv4 as their addressing through IPv6 networks [15]. However, implementing the dual stack mechanism is still more common and exists as a better solution for ISPs among others [16], [17] since it
utilizes double function of network address translation (NAT) mechanism on the side of customers and the side of ISPs. To assist continued development in the effect of IPv4 depletion, ISPs must effectively use the remaining IPv4 addresses by sharing them among several users [18]. The NAT function on the Customer Premises Equipment (CPE) [19] and ISPs must be considered to be improved so as to use a few remaining of IPv4 addresses to support multiple telecommunication services as [20].

Combining IPv4 and IPv6 functions altogether on one CPE is a new development for ISPs. In addition, the new CPE model should be able to accommodate the emerging of telecommunication convergence services. Since there are many IPv4 customers still exist, however, the CPE must be compatible not only for IPv6 but also for IPv4 applications. Developing a CPE that is compatible for IPv6 and IPv4 has been done by the implementation of Carrier Grade NAT Dual Stack Lite (CGN-DS Lite) through the IPv6 access network as in [21]. Some IPv6 and IPv4 services such as web, email and VoIP are working very well on this type of CPE. Reference [21], however, does not take into account applications that need to manage the port forwarding or port mapping such as P2P application in case of dual stack architecture. This is clearly not tolerable for users since network providers must support all services.

This paper presents a mechanism of Universal Plug and Play (UPnP) and Port Control Protocol (PCP) in order to deal with IPv4 applications implementing port forwarding function in dual stack CPE via IPv6 access network.

The paper is organized as follows. Section 2 reviews the proper literatures related to previous work enforcing CGN DS Lite mechanism on the CPE. It also highlights the UPnP-IGD and UPnP PCP proxy as the main features of the CPE for managing port forwarding in dual stack environment. Section 3 presents the proposed system to achieve a well mechanism of port mapping on CGN DS-Lite environment. In the section 4, we perform the technical operation of our work on PCP application. To complete, we conclude the paper in Section 5.

2. Related Works and State of The Art

It is important to note that the communication between the difference IP formats is impossible to do. Reference [21] shows that IPv6 to IPv6 communication on the CPE is working well. However, the issues came up when IPv4 port forwarding applications is used in dual stack environment through IPv6 network.

2.1. CGN DS- Lite

CGN DS-Lite is a transition approach from IPv4 to IPv6 by moving the NAT function on the CPE’s side to the core network of the provider by sharing one public IPv4 address for users [22]. The remaining IPv4 addresses are effectively distributed to network providers so that can be used by a huge number of customers. Hence, it gives ISPs some possibilities to keep maintaining the IPv4 to IPv4 communication without assigning a public IPv4 address to a customer.

The incoming packets of a privately addressed IPv4 host in the home network are encapsulated inside the IPv6 datagram by the CPE. Further, the CPE delivers the datagram to the CGN at the network provider. This mechanism can be seen in Fig. 1 [22]. The network provider deploying CGN DS-Lite needs to implement NAT mechanism as in [23] considering it transforms the source IP address and port identifier for TCP or UDP packets in order to use one IPv4 public address by the nodes on several CPEs. This IPv4 address must be able to configure by the ISP.

The following precondition must be taken into account so as to enforce CGN DS Lite mechanism [22].

- CPEs connect through IPv6 access network
- CPEs reach the CGN through IPv6 address maintained by DHCPv6 services
- CPEs provide tunneling IPv4 in IPv6
To develop the CGN implementation, two elements are installed in DS-Lite, DS-Lite B4 (Basic Bridging Broadband) at the CPE and DS-Lite AFTR (Address Family Transition Router) at the CGN side as in [24].

The essential characteristics of DS Lite are that the communicating hosts are using the same IP format and devices using IPv6 addresses will be straightly sent to IPv6 Internet and will be not affected by DS-Lite operation.

![Fig. 1. CGN DS-Lite mechanism.](image)

2.2. **UPnP IGD**

Universal Plug and Play (UPnP) is a mechanism allowing the hosts to automatically configure their self which are based on network configuration. It is mainly developed in the home network and is used for the port forwarding such as in P2P application [25].

Internet gateway also known as the CPE is an in between device presented in the border of the network that connects the home network devices to the WAN side. In real implementation, all user devices including CPE may be visible from the network since there is no more NAT embedded in CPE. Nonetheless, a firewall will be implemented within the CPE so as to protect LAN devices from external unexpected intrusion [26].

To do so, special attention must be taken into account to CPE’s firewall in order to allow configuration flows entering the customer’s LAN, especially for push mode (no configuration initiative from device) [27], [28]. The recommendation for every managed device is to use UPnP IGD (Internet Gateway Device) for controlling firewall that allows management from network. For example, UPnP IGD permits game and Internet Messenger (IM) applications on the clients to ask the port forwarding without user’s involvement [25].

In case of IPv6, the UPnP IGD function is used for the firewall management purposes since there is no more port forwarding in IPv6. Reference [29], in addition, presents that the implementation of UPnP AudioVisual architecture on IPv6 is working well.

The following requirements are defined for IGD [26]:

- Maintaining Internet connection on at least one WAN interface
- Maintaining home network connection on at least one LAN interface
- Maintaining a specific security mechanism
- Maintaining device protection

UPnP IGD is needed also to perform security by embedding a firewall in it. This firewall can be used to
check network traffic passing through it, and refuses or admits the path based on a set of rules. Firewall rules such as packet filtering, anti-spoofing, fragmentation, etc could protect the CPE, the devices in LAN, or to protect the provider platforms. In addition, the IPv6 firewall management service on the WAN interface permits the terminals to make pinholes into firewall, delete pinholes and check the pinholes whether they are working or not [26].

2.3. UPnP–PCP Proxy

In case of DS Lite architecture, UPnP cannot be used to manage port forwarding in the CGN since UPnP cannot work beyond the LAN. Therefore, a new protocol known as PCP (Port Control Protocol) that allows the management of port forwarding in CGN is implemented [30]–[32]. Since terminals do not implement PCP, a proxy is required in the CPE in order to translate UPnP messages into PCP messages and vice-versa. This permits the application to make IP and port mapping on the CGN from the host [33], [34].

This UPnP–PCP Proxy capability is mainly developed in the CGN environment since the NAT existed in network provider domain is not sufficient for controlling the port forwarding and breaks some valuable applications. Therefore, the PCP Proxy is implemented in the CPE. This PCP Proxy function in CPE provides security controls for PCP requests coming from the outside [31]. It acts as an UPnP server that receives requests from the hosts using its internal interface on UDP port 44323 [25]. On the other hand, it forwards the host’s requests to the CGN PCP Server using its external interface. A light version of PCP Proxy known as a Smart Proxy could be combined with UPnP IGD aforementioned in the previous section. This Smart Proxy can be used to manage many CGN PCP servers and maintain requests and replies [31].

3. Proposed System

In this section, we present the proposed system so as to develop the PCP and UPnP implementation in CGN DS-Lite mechanism through IPv6 access network environment. However, the deep analysis of IPv6 is out of the scope of this document. The IPv6 exists for the purpose of providing IPv6 access network.

Fig. 2 shows the network diagram of the technical implementation. Being an advance research, the requirements are still the same as the previous one as we did in [21]. Nonetheless, there are some new functions that need to be taking into account for maintaining port forwarding applications. The network is completed with the following hardware: (1) one PC as the CGN and PCP server; (2) an already configured Raspberry Pi as the CPE; (3) two PC clients as the IPv4 remote host and the UPnP client.

4. Implementation

4.1. CGN DS-Lite Service Integration

The Raspberry Pi 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. The Raspberry Pi as the CPE is also configured with Debian Linux. The CPE must be able to derive IPv6 address assigned by DHCPv6 server by starting the DHCPv6 client process. For IPv4 to IPv4 communication, the CPE needs the DS-Lite B4 operation. Using the tun4in6 function in B4 operation, the CPE tunnels the IPv4 traffic within IPv6 traffic. The CPE is further installed the miniupnp daemon that can be downloaded freely from [34] to activate the UPnP IGD operation.

By using the Debian Linux, the PC server is installed with DHCPv6 server function. It is done in order to provide IPv6 access network for the research implementation. Furthermore, the PC is also configured with the AFTR 1.1 for the CGN and PCP function. The implementation of CGN DS-Lite provides IPv4 to IPv4 communication within IPv6 access network. This AFTR develops a tunnel IPv4 in IPv6 interface coming up to the CPE.

All traffic of IPv4 equipment inside the customer’s network is encapsulated within IPv6 packet using 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.

### 4.2. PCP and UPnP Service Integration

The objective of the PCP (Port Control Protocol) is to allow the dynamic management of ports in the CGN as it done today for the CPE’s NAT with UPnP. This dynamic management allows opening ports for further incoming communications. Fig. 2 presents that the UPnP IGD and PCP Proxy functions have been embedded on the CPE. This UPnP IGD and PCP Proxy function is installed on the CPE using an application known as miniupnp daemon (miniupnpd). The configuration file of miniupnpd is shown in Fig. 3. In the CGN, some additional syntax has been added into AFTR 1.1 application in order to support the PCP daemon function in PCP server. This implementation uses miniupnpd version 1.4 since some other versions cannot detect UPnP devices.

![Fig. 3. UPnP message on miniupnp activation.](image)

To generate the UPnP messages of UPnP devices and control point, this implementation uses a tool known as GUPnP Universal Control Point [35]. It provides information of UPnP devices on the network. Firstly, the AFTR and PCP functions are activated on the CGN server. On another side, the CPE router executes the miniupnp daemon function.

After AFTR and PCP activation on the server, miniupnpd on the CPE is further executed. Fig. 4 shows the UPnP messages of miniupnpd daemons. The results shows permission rules based on file of miniupnpd.conf, listening port for HTTP and the most important thing is the new external address as the IPv4 public address.
As soon as the GUPnP on a client using IP address 192.168.1.72 is launched, it detects the UPnP resource in the CPE router. Using the discovery mechanism through SSDP (Simple Service Discovery Protocol), this UPnP client informs its availability on the network over the multicast address in order to discover an UPnP resource. A capable of UPnP resource directly responds through unicast address. This can also be presented as an XML file via HTTP message.

One function to perform port forwarding is the AddPortMapping invocation. This is done in order to add the rules for the incoming and outgoing packets. Using this GUPnP implementation, it is assumed that there is a new internal client using IP address 192.168.1.35 invokes for an AddPortMapping action. This client for example uses a port number 4950 as the external port for the incoming Internet packets, uses UDP as its protocol type and uses a port number 4951 as the internal port. This action gives the rules on the CPE router as well as the PCP and AFTR functions in the CGN server. Fig. 5 below presents miniupnp AddPortMapping messages produced by CPE router. Fig. 6 shows PCP messages generated by the PCP server that is embedded on the CGN. A PCP daemon function on PCP server communicates with the AFTR function on the CGN so as to create the entry in the NAT table. The NAT entries on CGN assign the same external (4950) and internal (4951) port number asked by the GUPnP client that are shown in Fig. 7. The UPnP client informs the remote host to send back the packets to these port numbers. Together with the IPv4 public address, these port numbers will be used for the communication between the UPnP client and the remote host.

---

**Fig. 4.** UPnP message on miniupnp activation.

**Fig. 5.** Miniupnp AddPortMapping message on CPE.
Another invocation such as DeletePortMapping is also performed using this GUPnP tool so as to verify the port mapping functions in this PCP implementation. This DeletePortMapping function firstly informs UPnP IGD on the CPE to delete the external port number 4950 by removing redirect rule for this port number. This function will further remove the port mapping action on PCP server and will be emptying the list of NAT on the AFTR.

```
pcpd: got request from 2a01:c00:75:4400:209:a9ff:fe09:2300
pccd: send to AFTR: try map 2a01:c00:75:4400:209:a9ff:fe09:2300 udp 192.168.1.35 4951 172.20.182.213 4950
pcpd: received from AFTR: map 2a01:c00:75:4400:209:a9ff:fe09:2300 udp 192.168.1.35 4951 172.20.182.213 4950
pcpd: got expected 'map 2a01:c00:75:4400:209:a9ff:fe09:2300 udp 192.168.1.35 4951 172.20.182.213 4950' from AFTR
pcpd: add map 2a01:c00:75:4400:209:a9ff:fe09:2300 udp 192.168.1.35 4951 172.20.182.213 4950
pcpd: setmapping: new
```

Fig. 6. PCP AddPortMapping message on PCP server.

```
list nat
not 2a01:c00:75:4400:209:a9ff:fe09:2300 udp 192.168.1.35 4951 172.20.182.213 4950
```

Fig. 7. NAT entries AddPortMapping message on AFTR.

When a port has already used by an application, GUPnP tool cannot be able to provide that particular port to another application. It gives an error message (Conflict in Mapping Entry) when the requested port is not available or is used by others.

One torrent application known as Client BitTorrent Transmission has also been used for this PCP implementation. The results are the same with the previous application. As long as the incoming port is not used by an application, that particular port can be used by another application for its incoming connection. However, when a port has been used by one application, the others cannot use it and should change the desired port.

5. Conclusion

This work presents that the CGN DS-Lite can be further implemented in the introduction of IPv6 technology so as to accommodate IPv4 to IPv4 communication. PCP and UPnP mechanism works with some limitations. When a port has been used by an application, another application cannot use the port and must transform the requested port. For future work, the performance of the proposed system and other interactive services can be further investigated in order to verify a better mechanism to allow the port restriction based on the incoming and outgoing connections.

Acknowledgment

This research is fully funded by a grant from Directorate General of Higher Education of Indonesia (DIKTI). The authors are indebted to Laurent Toutain, Xavier Pougnard and Vincent Huet for any helpful and feedback during research implementation.

References

1752, IETF.


**Ihsan Lumasa Rimra** was born in Padang, Indonesia, in 1978. After completing his bachelor degree in 2003 at Electronic Engineering Polytechnic Institute of Surabaya Indonesia on telecommunication engineering, 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 Department of France Telecom, France.

He immediately incorporates to the Computer Networking Laboratory State Polytechnic 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 subjects at State Polytechnic of Padang, Indonesia.

**Wiwik Wiharti** was born in Surabaya, Indonesia in 1977. She had received a bachelor degree of instrumentation engineering, in 2002 and a master degree of control system engineering, in 2010 at the Sepuluh Nopember Institute of Technology.

Her research is focused on developing of control system, sensor network and embedded system. She is also a lecturer at the Electronics Engineering Department in State
Surfa Yondri was born in Sungayang, Indonesia in 1970. He received his undergraduate degree in control engineering from Bandung Institute of Technology in 2000. He continued to obtain his master degree in computer engineering in 2006 from University of Putra Indonesia.

His research is focused on embedded system in electronic control system. He works also as a lecturer at the Electrical Engineering Department in State Polytechnic of Padang, Indonesia.