IPv6 IMPLEMENTATION WITH MIGRATION METHOD NAT64 AND VPLS TO SUPPORT IPv6 MOBILE IN ITB

Gulam Fakih[1], Angga Setiyadi[2]

[1,2] Universitas Komputer Indonesia
Jl.Dipatiukur No.114 Bandung 40132
E-mail : ghulamfaqih@gmail.com[1], anggasetiyadi@gmail.com[2]

ABSTRACT

Institut Teknologi Bandung (ITB) is the first technical high school in Indonesia. To facilitate and support the learning process requires internet access so that the lecturers, students and employees can more easily find information. Due to many people in ITB that require internet access IPv4 allocation is exhausted and needed a quick solution to solve the problem. IPv6 is the solution to the limitations and depletion of IPv4 because it has an amount of 2 ^ 128 bits.

Based on this then the implementation of IPv6 is the solution to the problem. In the migration process to IPv6 for easier user use NAT64 migration method so that IPv6 users keep communicating with IPv4. IPv6 mobile is also provided for IPv6 users to retain the same address even though they migrate on campus and the relationship with uninterrupted applications. In support of the mobile network the main infrastructure was changed to Multi Protocol Label Switching (MPLS) with VPLS as VPN on layer 2.

From the implementation results that network performance on IPv6 such as throughput, latency no redundancy compared to IPv4 and applications that can be opened on IPv4 can also be opened by IPv6 users.

Keywords: IPv6, Migration, Network Address Translation 64 (NAT64), IPv6 Mobile, VPLS

1. INTRODUCTION

Implementation of IPv6 in Indonesia is still relatively small with other countries, therefore to support IPv6 implementation in Indonesia there must be a model, especially in the education and research sectors. Thus the Bandung Institute of Technology (ITB) is expected to be the pioneer of IPv6 in Indonesia.

Bandung Institute of Technology (ITB) itself has several faculties and under the faculty is divided into groups of skill / expertise. And the number of civitas in ITB in 2013 such as lecturers as much as 3773, students as many as 21,727 and employees as many as 1.388, because it is the number of IPv4 addresses that are available is exhausted.

The Bandung Institute of Technology (ITB) currently has an IPv6 2403: 8000 :: / 32 prefix given by APNIC, but it has not been used optimally and thoroughly to the user's network.

To be able to integrate two IPv4 and IPv6 protocols ITB itself has used migration method 6to4 is a migration technique by creating an IPv6 tunnel path over IPv4 network, but still constrained by IPv6 users who can not communicate with IPv4, as well as communications with servers that have domain Name.

One solution to the problem of IP limitations and migration methods that have not made convenience to the user is to implement IPv6 with the NAT64 migration method and add the mobile IPv6 feature so that the IPv6 address used remains the same so that the application on the user does not break the session

The purpose of this topic is to reimplement ipv6 address in ITB and optimize its use, by Nat64 dual-stack migration method, and connect ipv6 client to ipv4 client. This vpls technology will be used for distributing ipv6 addresses on wifi networks for ipv6 users to connect with SSID in ITB IP address will not change and communication can still run. The purpose of this research topic:

1. Institut Teknologi Bandung (ITB) has largest IPv6 address statistics in Indonesisa IPv6 terbanyak di Indonesia.
2. Users of internet services such as lecture, students, employee that using mobile device or laptop can connect to internet using IPv4 and IPv6.
3. IPv6 allocation for every faculty, data center, building, and wireless network already defined and documented
4. Implementation of IPv6 migration method in ITB becomes better and can be used by all end-user devices.

2. CONTENT OF STUDY

2.1 IPv4 *Address*

Each computer in TCP / IP is assigned an uique binary address called an internet protocol address or ip address. IPv4 addresses use 32-bit addresses that are divided into 2 main parts of the prefix that identify the computer is connected to the network where and the suffix that provides unique identifier on the computer on the network

2.2 IPv6 *Address*

IPv6 addresses using 128-bits written with hexadecimal numbers divided into 8 octets are limited by the ":" column symbol with this the number of ip addresses provided is very much. The following is the header structure of IPv6.

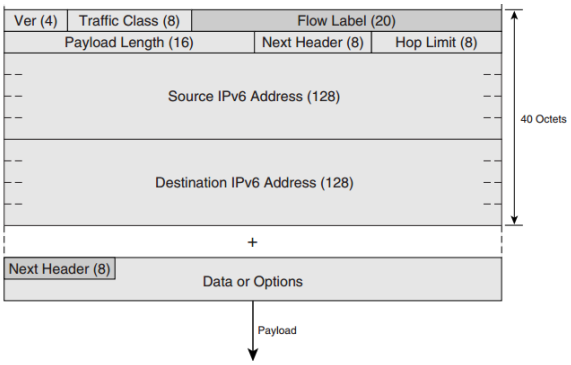


Figure 1. Header Structure Of IPv6

The following is a description function of each header:

1. Version (4bit) Used to define IP protocol version.
2. *Traffic Class* (8bit) header that used for QOS function.
3. *Flow label* (20 bit) Is Field to be used for the interest of flow and this field is expected to make Router does not need to lookup deeper package to treat a package
4. *Payload length* (16 bit) Contains layer 4 and up information from OSI Layer. The number of fields is tetep 40 bytes so that when the process lookup by Router faster, Because the route does not need to check variable-length header*Next Header*(8bit) Contains port number information on the upper layer or layer 4 ie transport.
5. *Hop Limit* (8bit) Field Time To Live (TTL) To prevent looping on layer3
6. *Source Address (128 bit)* It contains the sender's IPv6 address information.
7. *Destination Address (128 bit)* Contains recipient IPv6 address information.
8. *Extenesion Header* Includes additional network layer header information, such as header routing, encapsulating security payload (ESP) header.

2.3 *(Network Address Translasion 64)* NAT64

NAT64 provides communication facilities between IPv6 host and IPv6 with support of DNS64 technology. NAT64 there are 2 categories to achieve the purpose of its function is stateless and stateful. Nat64 stateless is defined in RFC 6145 and NAT64 stateful in RFC 6146. Below is a table about the comparison.

Table 1. NAT64 Stateful and Stateless

	NAT64 Stateless	NAT64 Stateful
1.	1:1 translation , because it is limited to a few hosts only	1:N translation, therefore there is no Limit the number of hosts to be translated
2.	The IPv4 address used quickly runs out	One IPv4 address can be used by many hosts
3.	Tidak ada binding saat translasi	Using bindings every transaction is unique.
4.	It requires manual configuration of ip address or via DHCPv6	Can use various address allocations such as DHCPv6, manual, and SLAAC
5.	IPv4 to IPv6 manual is required as the main requirement	No need to translate between IPv4 to IPv6.

The workings of NAT64 itself can be seen in Figure 2 on how NAT64 works:

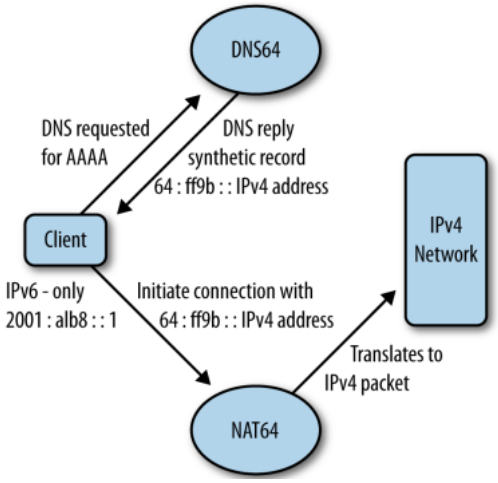


Figure 2. NAT64 WorkFlow

When the IPv6 client communicates with IPv4 it will ask for AAAA information on the dns64 server, the accepted answer is the nat64 prefix address combined with the IPv4 address 64: ff9b :: IPv4. When the IPv6 computer has found the AAAA information the computer will send the packet to NAT64 and NAT64 will transmit the address and send it to the IPv4 host

2.4 *Multi Protocol Label Switching* (MPLS)

The Multi Protocol Label Switching (MPLS) protocol creates a new paradigm for the Router how to forward packets. Compared to having to forward packets based on destination IPs in the header, MPLS forward packets based on labels. Because it uses labels in the packet forwarding process. mpls can define a goal can be based on other factors such as QOS needs, traffic engineering, and privacy needs for each customer connected to the MPLS network, but MPLS still uses IGP or EGP routing protocol information.

Virtual Private LAN Service (VPLS) is an MPLS application on layer 2 VPN. With VPLS create a Multipoint-to-Multipoint network for layer 2 between customer premises. This VPLS can be used instead of ethernet over MPLS, L2Pv3 even GRE. The service provider device that leads the deserver will be like a large switch because the mac-address address is read a lot and connected to various customers.

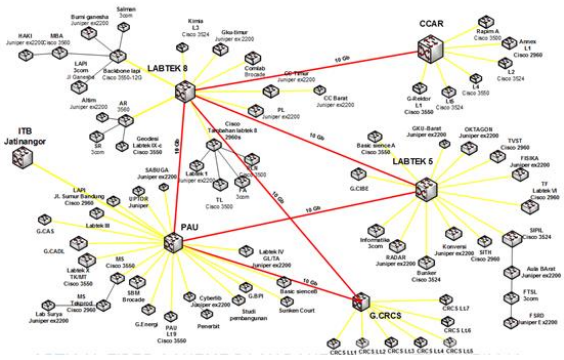
2.5 *Plan Design Implement Optimize Operate* (PDIOO)

The PDIOO method is a life-cycle method in network design made by cisco. The PDIOO Life-cycle consists of the following steps:

1. Plan is the definition of network needs. Analyze where the network will be installed or used, what type of service will be provided, and used by whom. When all is defined then the basic needs of the network have been identified.
2. Design to design according to the needs of the network has been obtained from the next step plan made a design step and also be coordinated with the administrator or manager. Examples of designs are done logical design and physical design
3. Implement Perform implementation according to the design made. In this step done testing of designs made and the designer
4. Operate the last test. Networks will be monitored in this step from performance and any errors made that will be used as a basis for optimization steps
5. *Optimizing the problem being implanted. In this step is also done redesign if when applicable.*

2.6 Analyizing Network Existing

Here is an exising network analysis for scalability is how big the growth of the network that we must support.



Fgure 3. Toplogy of Network Existing

Based on the above topological analysis and image then the implementation will be done in the following devices:

Table 2. Router Must be Implement

No	Router	Location
1.	Core Router PAU	Building PAU
2.	Core Router LABTEK 5	Building LABTEK 5
3.	Core Router LABTEK 8	Building LABTEK 8
4.	Core Router CRCS	Building CRCS
5.	Core Router Jatinangor	ITB Jatinangor Building Rektorat
6.	Core Roter Annex/CCAR	Building Rektorat ITB
7.	Router Gateway	Building PAU

The following is an analysis of the availability of an existing network that is how long a network should be usable by the user and how quickly the network can return to function if there are any disruptions such as human error, disaster or security issues.

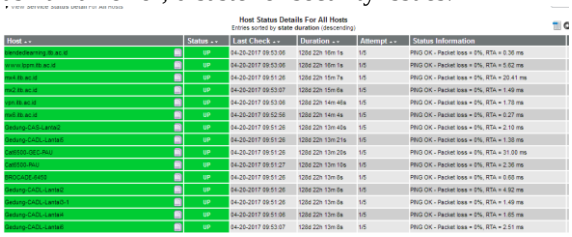


Figure 4. Network Availibility

Based on the availability of network availability, IPv6 network availability plan must reach at least 128 days no interruption.

Here is an analysis of network performance on the existing measure of throughput, accuracy, efficiency, delay, response time. Table 3 is the result of an existing network throughput analysis.

Table 3. Throughput Network Existing

No	Source	Dst	Transfer	Bandwidth
1	Router PAU	Router border	1116 MB	112 MB/s
2	Router labtek 5	Router border	1090 MB	109 MB/s
3	Router labtek 8	Router border	1073 MB	107 MB/s
4	Router CCAR	Router border	1092 MB	109 MB/s
5	Router CRCS	Router border	1020 MB	102 MB/s
6	Jaringan wireless	Router border	20.9MB	2.8 MB/s
Average Network Cable Performance			1078.2 MB	107.8 MB/s
Average Performance of Wireless Network			20.9	2.8

From the results of the above table can be made graphic as picture 5.

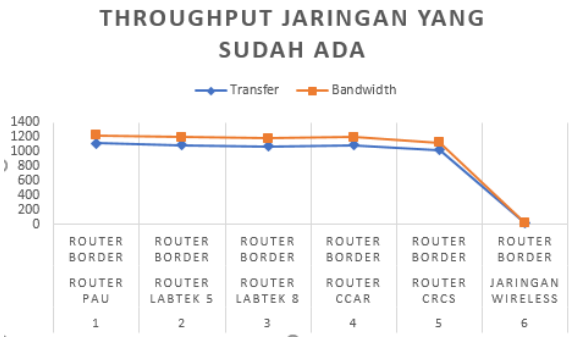


Figure 5. Graph Throughput Network Existing

Below is table 4. Delay accuracy results, accuracy, response of existing network.

Table 4. analyza Delay, accuracy, response

No	Source	Dest	Avg Delay	*Loss packets*
1	Labtek 5	Router border	4.14 ms	0%
2	Labtek 8	Router border	8.41 ms	0%
3	Gedung CRCS	Router border	8 ms	0%
4	Jaringan wireless	Router border	43.27 ms	0%
5	Gedung PAU	Router border	2.07 ms	0%
6	Gedung CCAR	Router Border	2.05 ms	0%
Average Network Cable Performance			4.934 ms	0%
Average Performance of Wireless Network			43.27 ms	0%

From the results of table 4 can be made a graph like picture 6.

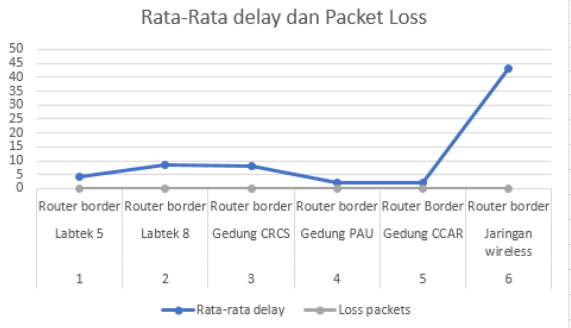
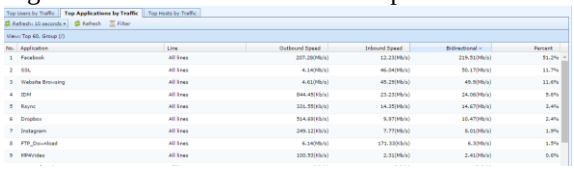


Figure 6. Anlayze *Delay, accuracy, response*

For security analysis of the existing network of wireless internet network users at Bandung Institute of Technology Tamansari (ITB) on its network each SSID uses WPA2-PSK password, after user connected to SSID then user when opening web page using browser must enter username and password proxy. And for the security aspects of network technical personnel, all network devices yang terhubung seperti *switch, Router, load balancer,* dan *firewall* menggunakan protocol *Authentication Authorization Accounting* (AAA) with tacacs + application that functions as database user to login, recording configuration, granting user permissions to each device.

Anlisa existing network about usability is the ease of using the network and access a network or service from the user or user. Based on the analysis conducted by internet service users use dynamic protocol to obtain IP address address.

Anlisa existing network from OSI Layer application side which is often used can be seen Figure 7 and picture 8.



Fiugre 7. Most Application Used

Based on the picture 7 applications are often opened is https and http for example facebook and youtube. In Figure 8 is an example of an application that is often opened from the proxy side.

	Accessed site	Connect	Bytes	%
1	who r3---sn-puc-cqve.googlevideo.com:443	141,836	263.3 G	10.1%
2	who r1---sn-puc-cqve.googlevideo.com:443	86,755	180.3 G	6.9%
3	who r2---sn-puc-cqve.googlevideo.com:443	74,752	92.1 G	3.5%
4	who scontent-sin6-1.cdninstagram.com	399,313	57.5 G	2.2%
5	who 62.210.84.186	485	57.4 G	2.2%
6	who au.download.windowsupdate.com	124,453	36.8 G	1.4%
7	who instagram.fcgk4-1.fna.fbcdn.net	209,590	30.8 G	1.1%
8	who 74.125.130.132:443	9,145	27.6 G	1.0%
9	who instagram.fcgk5-1.fna.fbcdn.net	184,057	25.5 G	0.9%
10	who 7.tlu.dl.delivery.mp.microsoft.com	34,649	20.7 G	0.7%

Figure 8. Analyze Application Access

n Figure 8 it can be seen that the address or website that is often accessed is youtube.com from the results of the analysis then the http and https applications must be able to run on the side of IPv6 network users.

2.7 Scalability Testing

In testing the scalability at this first point is to ensure that the implementation of OSPFv3 on each core router has been implemented and IPv6 route has been distributed on each router**.**

```
telnet@PAU-06042014>show ipv6 ospf neighbor

Total number of neighbors in all states: 4
Number of neighbors in state Full      : 4

RouterID        Pri State     DR              BDR             Interface     [State]
167.205.0.2       1 Full      167.205.0.1     167.205.0.2     ve 2          [DR]
167.205.0.3       1 Full      167.205.0.3     167.205.0.1     ve 3          [BDR]
167.205.3.1       1 Full      167.205.0.1     167.205.3.1     ve 4          [DR]
167.205.0.7     128 Full      0.0.0.0         0.0.0.0         ve 6          [P2P]
telnet@PAU-06042014>
```

Figure 9. *NeighborInformartion of OSPFv3*

Figure 9 shows the OSPFv3 neighbor information in the core or backup network that has been implemented with the show ipv6 ospf neighbor command.

2.8 Availability Testing

In this part of availability is done testing implementation of devices that have been implemented fixed availability and no constraints

while being operated. Here is an experiment if the main route to die takes how many seconds to move to the backup path.

```
root# run ping 2500:3000::1 source 2403:8000:710::1
PING6(56=40+8+8 bytes) 2403:8000:710::1 --> 2500:3000::1
16 bytes from 2500:3000::1, icmp_seq=0 hlim=64 time=2.564 ms
16 bytes from 2500:3000::1, icmp_seq=1 hlim=64 time=7.636 ms
16 bytes from 2500:3000::1, icmp_seq=2 hlim=64 time=2.737 ms
16 bytes from 2500:3000::1, icmp_seq=3 hlim=64 time=2.602 ms
16 bytes from 2500:3000::1, icmp_seq=4 hlim=64 time=3.877 ms
16 bytes from 2500:3000::1, icmp_seq=5 hlim=64 time=2.186 ms
16 bytes from 2500:3000::1, icmp_seq=6 hlim=64 time=2.444 ms
16 bytes from 2500:3000::1, icmp_seq=7 hlim=64 time=3.954 ms
16 bytes from 2500:3000::1, icmp_seq=8 hlim=64 time=2.108 ms
16 bytes from 2500:3000::1, icmp_seq=9 hlim=64 time=1.882 ms
16 bytes from 2500:3000::1, icmp_seq=10 hlim=64 time=2.839 ms
16 bytes from 2500:3000::1, icmp_seq=11 hlim=64 time=3.013 ms
16 bytes from 2500:3000::1, icmp_seq=12 hlim=64 time=2.280 ms
16 bytes from 2500:3000::1, icmp_seq=13 hlim=64 time=1.820 ms
16 bytes from 2500:3000::1, icmp_seq=14 hlim=64 time=62.254 ms
16 bytes from 2500:3000::1, icmp_seq=15 hlim=64 time=4.591 ms
16 bytes from 2500:3000::1, icmp_seq=16 hlim=64 time=4.461 ms
16 bytes from 2500:3000::1, icmp_seq=17 hlim=64 time=3.466 ms
16 bytes from 2500:3000::1, icmp_seq=18 hlim=64 time=2.953 ms
16 bytes from 2500:3000::1, icmp_seq=19 hlim=64 time=3.393 ms
16 bytes from 2500:3000::1, icmp_seq=20 hlim=64 time=3.458 ms
```

Figure 10. Availability Testing

In Figure 10 when viewed in the 14th packet there has been a major route move to the backup route as the result is that there is no loss packet on move but only result in high latency when there is movement of path.

2.9 Network Performance Testing

In the Performance section of this network will be testing IPv6 implementation such as throughput, latency, delay and loss packet and will be compared with network performance in IPv4. Here is a table of test results and a comparison between IPv4 and IPv6.

No	Sumber	Tujuan	Transfer		Bandwidth	
			IPv4	IPv6	IPv4	IPv6
1	Router PAU	Router border	1116 MB	1020 MB	112 MB/s	102 MB/s
2	Router labtek 5	Router border	1090 MB	1064 MB	109 MB/s	106 MB/s
3	Router labtek 8	Router border	1073 MB	1075 MB	107 MB/s	107 MB/s
4	Router CCAR	Router border	1092 MB	1080 MB	109 MB/s	108 MB/s
5	Router CRCS	Router border	1020 MB	1076 MB	102 MB/s	108 MB/s
6	Jaringan wireless	Router border	20.9 MB	20.5 MB	2.8 MB/s	2.02 MB/s

Tabel 5. Network Performance IPv4 and IPv6

Based on table 5 we can create graphs like the following to make it easier to understand the results of IPv4 and IPv6 network performance.

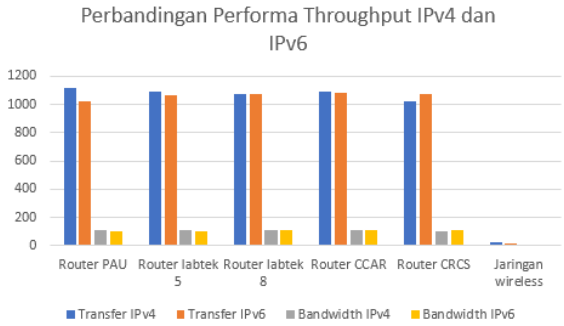


Figure 11. Network Performance IPv4 and IPv6

The result of the test and Figure 11 is that the performance for throughput on IPv6 and IPv4 networks does not differ much either through wired media or wireless media.

For the performance part of the network delay and packet loss can be seen in table 6 below:

Table 6. Delay and Packet Loss Testing

No	Sumber	Tujuan	Rata-rata delay		*Loss packets*	
			IPv4	IPv6	IPv4	IPv6
1	Labtek 5	Router border	4.14 ms	1.86 ms	0 %	0%
2	Labtek 8	Router border	8.41 ms	1.89 ms	0 %	0%
3	Gedung CRCS	Router border	8 ms	1.86 ms	0 %	0%
4	Gedung PAU	Router border	2.07 ms	28.71 ms	0 %	0%
5	Gedung CCAR	Router Border	2.05 ms	1.98 ms	0 %	0%
6	Jaringan wireless	Router border	43.27 ms	1.95 ms	0 %	0%

From table 6 above about the test delay and packet loss can be made graphs like the Figure 12 below:

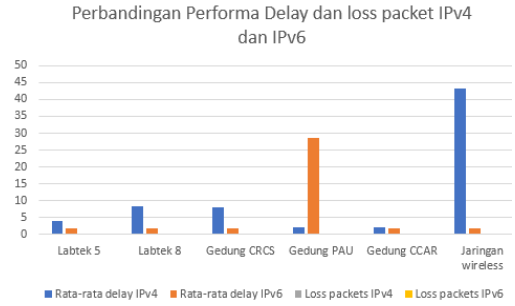


Figure 12. IPv4 and IPv4 delay and packet loss

Based on the image 12 the delay performance on ipv6 is smaller because the ipv6 user's own network is still small so that devices such as routers or user devices can process faster, due to the absence of broadcast packets on IPv6.

2.10 Security Testing

In this test IPv6 network users who pass through wireless communication media before gaining access to the internet must first authenticate through captive portal.

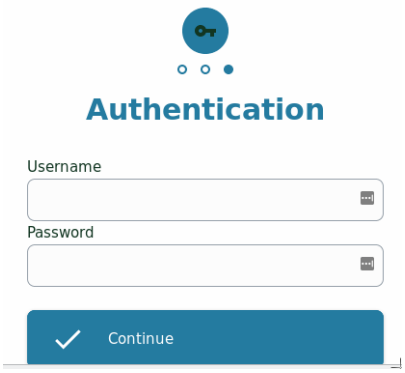


Figure 13. Captive Portal Of IPv6 Network

Figure 13 above shows that the user device that will connect to the ITB-IPv6 SSID network must login through the captive portal, and then the user can perform internet activity or browsing.

2.11 Usability Testing

In the usability testing on this is will be done whether the general operating system such as windows, linux, android and mac os owned users can connect to the IPv6 network. The following is a table of test results.

Table 7. Result Usability Testing

No	OS	Versi	Support	Keterangan
1	Windows xp	Sp 2	No	not support IPv6 DNS query
2	Windows	7	Yes	-
3	Windows	8	Yes	-
4	Windows	10	Yes	-
5	Linux Ubuntu	12.04	Yes	-
6	Linux Ubuntu	14.04	Yes	-
7	Linux Ubuntu	16.04	Yes	-
8	Android	4.1	No	not support ND-RDNS
9	Android	4.4	Tidak	Not support ND-RDNS
10	Android	5.0	Yes	-
11	Android	6.0	Yes	-
12	Mac OS	10.10	Yes	-
13	Mac OS	10.11	Yes	-
14	Mac OS	10.12	Yes	-
15	Mac OS	10.13	Yes	-

Based on the above table there are several user operating system that can not be supported komakat IPv6 implementation, because the vendor has not implemented IPv6 according to predetermined standards.

2.12 OSI Application Layer Testing

In the first of the application layer testing on this layer layer users on IPv6 will try to open any application that can be run over IPv6 for internet or learning to teach. Here are 14, 15 and 16 pictures of apps running on this IPv6.



Figure 14. Testing HTTP Application

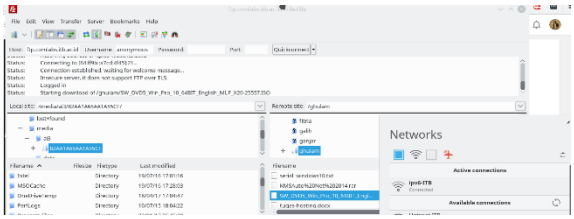


Figure 15. Testing FTP Application

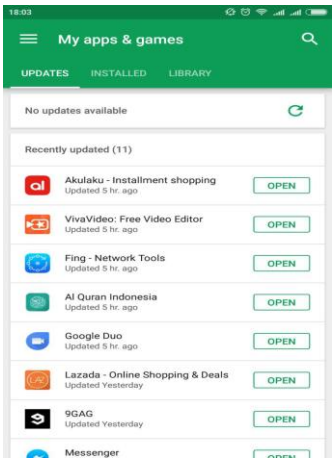


Figure 16. Testing Applicatin in mobile device

From figure 14.15 and 16 application like https, ftp and apps running on mobile can be accessed using IPv6 addresses.

3. Conclusion

Based on research conducted at Bandung Institute of Technology (ITB) on IPv6 implementation with

NAT64 and VPLS migration methods to support IPv6 remain mobile in ITB, it can be concluded as follows:

1. Statistics of IPv6 users at the Bandung Institute of Technology (ITB) became the largest sequence in Indonesia through APNIC website measurement.
2. Internet service users at Bandung Institute of Technology (ITB) can use IPv6 as one way to use the internet in campus environment ranging from mobile devices such as mobile phones or non-mobile devices such as computers and laptops.
3. The allocation of IPv6 addresses at the Bandung Institute of Technology (ITB) is now defined and there is documentation for every datacenter, faculty or directorate.
4. The migration method that has been done during implementation makes it easier for every IPv6 network user in ITB as it can use any public application with IPv6.

To improve the performance of IPv6 at Bandung Institute of Technology (ITB), there are several suggestions that can be considered, namely:

1. Should be held socialization to the civitas at Bandung Institute of Technology (ITB) on how to use this IPv6.
2. Optimization in the NAT64 router so that the session used when the translation does not end quickly resulting in the user when remote ssh often experience a break session.
3. The existence of new solutions to address applications that still can not use IPv6 by NAT64 way.
4. 4. To optimize the implementation of VPLS in Bandung Institute of Technology (ITB) more scalability in the future

REFERENCES

[1] admin, "Use of IPv6 for Indonesia (ID)," APNIC, 9 2 2017. [Online]. Available: https://stats.labs.apnic.net/ipv6/ID. [Accessed 9 2 2017].

[2] admin, "Fakultas dan Sekolah," ITB, 2016. [Online]. Available: https://www.itb.ac.id/fakultas-dan-sekolah. [Accessed 2 4 2017].

[3] admin, "Peta Kampus ITB," Direktorat SP & Program Studi Teknik Geodesi dan Geomatika ITB., 2015. [Online]. Available: http://petakampus.itb.ac.id/. [Accessed 27 2 2017].

[4] admin, "Sangfor Firewall," Institut Teknologi Bandung, 27 2 2017. [Online]. Available: https://fw.itb.ac.id. [Accessed 27 2 2017].

[5] admin, "Squid User Access Report," Institut Teknologi Bandung, 7 2 2017. [Online]. Available: http://logger.itb.ac.id/all/. [Accessed 27 2 2017].

[6] P. Oppenheimer, Top-Down Network Design Third Edition, Cisco Press, 2010.

[7] "Sejarah dan Masa Depan," Institut Teknologi Bandung, [Online]. Available: https://www.itb.ac.id/sejarah-dan-masa-depan. [Accessed 22 3 2017].

[8] C. Dirgantoro, Manajemen Stratejik, Jakarta: PT. Gramedia Widiasarana Indonesia, 2001.

[9] "Visi dan Misi," Institiut Teknologi Bandung, [Online]. Available: https://www.itb.ac.id/visi-dan-misi. [Accessed 22 3 2017].

[10] F. S. Wirawan, "Analisis kebutuhan resource terhadap kesesuaian protokol IPv4 dan IPv6 di Pusair Bandung," pp. 22-31, 30 5 2013.

[11] P. Simoneau, The OSI Model: Understanding the Seven Layers of Computer Networks, globalknowledge, 2006.

[12] D. D. Handayani, "INSTALASI DAN KONFIGURASI APACHE HADOOP, SQOOP DAN HIVE PADA CENTOS 7.2 UNTUK KEBUTUHAN COUNTING USER ACCESS TIAP COURSE E-LEARNING DI DitSTI ITB," pp. 15-17, 22 3 2016.

[13] D. D. Comeer, The Sixth Edition Of Internetworking With TCP/IP, pearsonhighered, 2013.

[14] P. P. Narbik Kocharians, CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1, Cisco Press, 2015.

[15] S. Hagen, IPv6 Essentials Integrating IPv6 Into Your IPv5 Network, New York: O'reilly, 2010.

[16] T. V. Narbik Kocharians, CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2, Indianapolis: Cisco Press, 2015.

[17] c. I. team, "NAT64 Technology: Connecting IPv6 and IPv4 Networks," Cisco, 17 4 2012. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html. [Accessed 15 4 2017].

[18] P. Oppenheimer, Top-Down Network Design third Edition, Indianapolis: Cisco Press, 2011.

[19] K. G. S. Antonio Sánchez-Monge, MPLS in the SDN ERA, Boston: O'reilly, 2015.

[20] admin, "Informasi Umum," ITB , 13 September 2014. [Online]. Available: https://www.itb.ac.id/informasi-umum. [Accessed 5 2 2017].