Implementasi Dan Evaluasi Perbandingan IPV4 dan IPV6 dalam Jaringan Lokal dengan Metode NDCLM

Ahmad Abdul Muthi[*1], Rudi Hartono[2], Agus Supriatman[3]
[1.2]Universitas Perjuangan Tasikmalaya; [3]Teknik Informatika, Universitas Perjuangan Tasikmalaya
E-mail: [*1]ahmadabdulmuthi@gmail.com, [2]rudihartono@unper.ac.id, [3]agussupriatman@unper.ac.id

Abstrak

Internet Protocol version 4 (IPv4) merupakan protokol jaringan yang paling banyak digunakan saat ini. Namun, IPv4 memiliki keterbatasan dalam hal jumlah alamat IP yang tersedia. Hal ini mendorong pengembangan Internet Protocol version 6 (IPv6) yang memiliki ruang alamat yang lebih besar dan fitur-fitur keamanan yang lebih canggih. Penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi perbandingan kinerja dan keamanan IPv4 dan IPv6 dalam jaringan lokal menggunakan metode NDLC (Network Depelovment Life Cycle). Dua jaringan lokal akan dibangun, satu dengan IPv4 dan satu lagi dengan IPv6. Kinerja kedua IP akan diukur menggunakan Iperf3 adalah sebuah alat pengujian jaringan yang digunakan untuk mengukur kinerja throughput antara dua titik dalam jaringan komputer dan mengukur waktu komunikasi komputer *server* dan *client* serta mengetahui keamanan kedua jaringan menggunakan Nmap yang akan diuji dan dibandingkan. Hasil penelitian menunjukkan bahwa IPv6 memiliki kinerja yang lebih baik daripada IPv4 dalam hal throughput dan keamanan namun IPv4 memiliki keunggulan dalam hal respon permintaan request dari client. IPv6 juga memiliki fitur-fitur keamanan yang lebih canggih seperti IPsec dan Firewall Stateful Inspection. IPv6 merupakan pilihan yang lebih baik daripada IPv4 untuk jaringan lokal yang membutuhkan kinerja dan keamanan yang tinggi.

Kata kunci—IPv4, IPv6, NDLC, Kinerja, Jaringan Lokal.

Abstract

Internet Protocol version 4 (IPv4) is currently the most widely used network protocol. However, IPv4 has limitations in the number of available IP addresses. This has driven the development of Internet Protocol version 6 (IPv6), which offers a larger address space and more advanced security features. This study aims to implement and evaluate the performance and security comparison between IPv4 and IPv6 in a local network using the Network Development Life Cycle (NDLC) method. Two local networks will be set up: one using IPv4 and the other using IPv6. The performance of both protocols will be measured using Iperf3, a network testing tool that measures throughput between two points in a computer network and the communication time between server and client computers. Additionally, the security of both networks will be assessed and compared using Nmap. The results indicate that IPv6 outperforms IPv4 in terms of throughput and security, although IPv4 has an advantage in client request response times. IPv6 also includes more sophisticated security features such as IPsec and Stateful Firewall Inspection. Overall, IPv6 is a better choice than IPv4 for local networks that require high performance and robust security.

Keywords*—IPv4, IPv6, NDLC, Performance, Local Network.*

1. PENDAHULUAN

Jaringan internet dan protokolnya telah mengalami evolusi yang luar biasa, mengubah cara kita berkomunikasi dan berinteraksi. Dahulu, internet hanya sebuah proyek penelitian sederhana,

namun kini telah berkembang menjadi tulang punggung kehidupan modern.

Pada awal mulanya, tak terbayangkan bahwa internet akan menjadi seperti sekarang. Kini, internet merambah ke berbagai aspek kehidupan manusia, menjadi fondasi bagi berbagai aktivitas, mulai dari komunikasi, pendidikan, hingga bisnis. Lembaga pemerintahan, organisasi pendidikan, dan bahkan individu memanfaatkan teknologi ini karena berbagai keuntungan yang ditawarkannya. Internet telah membuka era baru dalam komunikasi, tanpa batas ruang dan waktu. Hasilnya, komunikasi dan akses terhadap informasi menjadi mudah bagi individu di mana pun. Internet didefinisikan sebagai perangkat jaringan yang saling terhubung di seluruh dunia yang memfasilitasi komunikasi berbasis komputer dalam skala global [1].

IP versi 4 (IPv4) telah digunakan secara luas selama lebih dari 40 tahun, tetapi ruang alamatnya yang terbatas telah menjadi masalah karena pertumbuhan internet [2]. Meskipun penggunaan Internet Protocol version 4 (IPv4) telah berlangsung selama beberapa dekade, masalah keterbatasan alamat IP yang tersedia kini telah mencapai titik kritis yang sangat mendesak. Menurut data dari Internet Assigned Numbers Authority (IANA), pada tahun 2025, hampir seluruh alamat IPv4 telah habis teralokasi, yang menimbulkan hambatan serius bagi pertumbuhan dan skalabilitas jaringan internet global. Hal ini semakin diperparah oleh ledakan jumlah perangkat yang terhubung ke internet, terutama perangkat Internet of Things (IoT) yang diperkirakan mencapai puluhan miliar unit dalam beberapa tahun terakhir. Keterbatasan ini tidak hanya menghambat ekspansi jaringan, tetapi juga memaksa penggunaan mekanisme kompleks seperti Network Address Translation (NAT) yang dapat menimbulkan masalah performa dan keamanan.

Selain itu, IPv4 memiliki kelemahan signifikan dalam aspek keamanan karena tidak menyediakan enkripsi bawaan, sehingga rentan terhadap serangan seperti IP spoofing dan man-in-the-middle. Dalam konteks ini, kebutuhan untuk beralih ke protokol yang lebih modern dan aman seperti IPv6 menjadi sangat mendesak. IPv6 menawarkan ruang alamat yang jauh lebih besar dan fitur keamanan yang lebih canggih, yang sangat penting untuk mendukung perkembangan teknologi jaringan masa depan [3]. Oleh karena itu, penelitian ini tidak hanya relevan tetapi juga krusial untuk memberikan bukti empiris yang mendukung percepatan adopsi IPv6 demi menjaga keberlanjutan dan keamanan infrastruktur jaringan.

IPv6 hadir sebagai solusi tepat untuk menjawab kebutuhan internet masa kini dan masa depan. Banyaknya keuntungan yang diambil dari penggunaan IPv6 yaitu: alokasi address yang lebih banyak. IPv6, generasi terbaru protokol internet, menawarkan berbagai fitur inovatif yang tidak dimiliki IPv4. Fitur-fitur ini, seperti auto configuration address, traffic class dan flow label, serta dukungan untuk mobilitas, menjadikan IPv6 solusi ideal untuk internet masa depan [3]. Meskipun memiliki banyak keunggulan, adopsi IPv6 masih tergolong rendah. Oleh karena itu, diperlukan penelitian dan edukasi yang lebih intensif untuk mendorong penggunaan IPv6 secara luas. Dengan demikian, kita dapat memanfaatkan sepenuhnya potensi IPv6 untuk membangun internet yang lebih baik, lebih aman, dan lebih efisien. Hal ini sejalan dengan penelitian menyatakan bahwa [4]: “Pengguna cenderung menolak penggunaan IPv6 jika tidak tersedianya informasi teknis penggunaannya. Untuk itu dibutuhkan pengujian untuk membandingkan IPv4 dan IPv6 dari sisi, misalnya konfigurasi sistem sehingga dapat memberikan informasi bekerja bagi calon pengguna IPv6”.

Dari uraian diatas diperlukan penelitian mengenai pemanfaatan IPv6. Sehingga berdasarkan latar belakang permasalahan diatas penulis tertarik mengangkat penelitian tentang Implementasi Dan Evaluasi Perbandingan IPv4 Dan IPv6 Dalam Jaringan Lokal Dengan Metode NDLC.

NDLC atau Network Depelovment Life Cycle adalah protokol yang digunakan untuk menemukan perangkat dan layanan di jaringan [5]. NDLC dapat digunakan untuk menemukan perangkat dalam jaringan IPv4 maupun IPv6.

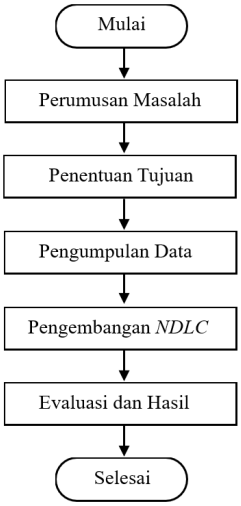
Implementasi dan evaluasi perbandingan IPv4 dan IPv6 dalam jaringan lokal dengan metode NDLC dilakukan dengan menggunakan laboratorium jaringan komputer. Laboratorium ini terdiri dari dua buah komputer, yaitu komputer server dan komputer client. Komputer server dan komputer client dikonfigurasi menggunakan IPv4 dan IPv6.

Pengujian dilakukan dengan menggunakan metode NDLC untuk menemukan perangkat dan layanan di jaringan. Pengujian dilakukan dengan menggunakan berbagai parameter

troughput, round trip time (RTT) dan keamanan.

2. METODE PENELITIAN

Metode penelitian ini menggunakan penyelesaian secara sistematis dengan tahapan seperti pada Gambar 1.



Gambar 1. Metode Penelitian

Sesuai dengan diagram alur penelitian diatas mengenai penelitian yang akan dilakukan terdapat beberapa tahapan diantaranya :

2.1. Perumusan Masalah

Pada titik ini, masalah utama penelitian telah ditentukan dan diuraikan dalam latar belakang masalah. Langkah selanjutnya adalah menyelidiki masalah ini lebih lanjut untuk mengidentifikasi solusi yang tepat[6]. Untuk melakukan penelitian diasumsikan akan dikembangkan permasalahan-permasalahan yang ada berkaitan dengan pokok bahasan.

2.2. Penentuan Tujuan

Tujuan mengimplementasikan dan mengevaluasi mengenai perbandingan IPv4 dan IPv6 dalam skala jaringan lokal yang ada di labolatorium sekolah dengan memanfaatkan sumber daya yang ada, dengan melihat *output* yang dihasilkan oleh setiap komputer baik dari topologi yang digunakan, *throughput, Round Trip Time (RTT),* maupun dari segi keamanan.

2.2.1. Untuk mengimplementasikan jaringan IPv6 di atas infrastruktur jaringan IPv4 yang sudah ada menggunakan metode *NDLC*.

2.2.2. Untuk melakukan evaluasi perbandingan kinerja dan keamanan jaringan IPv6 dan IPv4. Evaluasi ini dilakukan untuk mengetahui perbedaan kinerja dan keamanan antara jaringan IPv6 dan IPv4.

2.2.3. Untuk menyusun rekomendasi untuk implementasi jaringan IPv6 secara optimal. Rekomendasi ini disusun berdasarkan hasil evaluasi perbandingan kinerja dan keamanan jaringan IPv6 dan IPv4.

2.3. Pengumpulan Data

Studi ini akan membahas banyak pendekatan pengumpulan data yang terkait dengan metodologi penelitian ini, termasuk :

2.3.1. Observasi, merupakan Teknik pengumpulan data dengan melakukan pengamatan langsung terhadap suatu objek yang ingin diselidiki, observasi dilakukan dengan melakukan pengamatan secara langsung pada labkom sekolah[6].

2.3.2. Studi Pustaka, merupakan suatu prosedur yang dilakukan dengan cara meneliti dan mengumpulkan data dari sumber-sumber referensi, misalnya buku tulis, catatan

harian, web dan sumber-sumber yang berhubungan langsung dengan mata pelajaran eksplorasi tersebut.

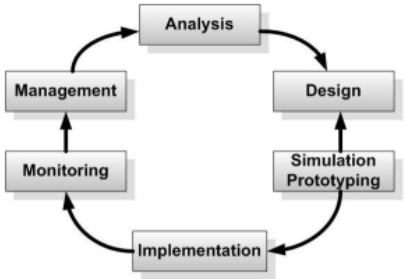
2.3.3. Wawancara, Wawancara adalah suatu prosedur tatap muka dimana pewawancara dan responden atau orang yang ditanyai bertukar pertanyaan dan jawaban guna memperoleh gambaran tentang tujuan penelitian [7]. Anggota staf yang mengawasi jaringan di laboratorium sekolah diwawancarai.

2.4. Pengembangan NDLC

Network Development Life Cycle (NDLC) adalah metode yang dapat digunakan untuk mengembangkan suatu jaringan komputer [5].

Metode *Network Development Life Cycle* (NDLC) akan penulis gunakan dalam pengembangan sistem. Pendekatan ini mencakup eksperimen terhadap suatu permasalahan dengan menggunakan teori-teori tertentu untuk memperoleh hasil pengujian yang tepat antara permasalahan dan teori yang digunakan. .

Enam langkah teknik penelitian *Network Depelovment Life Cycle* (NDLC) meliputi *analysis, design, simulation prototyping, implementation, monitoring,* dan *management*. Penelitian hanya berfokus pada tahapan *analysis, design, simulation prototyping, implementation* meliputi pengujian. Semua aktivitas lainnya merupakan bagian dari proses NDLC. Pada Gambar 2 model pengembangan ditampilkan.



Gambar 2. Model Pengembangan NDLC[8]

Tahapan-tahapan pada *Network Depelovment Life Cycle* (NDLC) sebagai berikut[8] :

2.4.1. Analysis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan *user*, dan analisa topologi/jaringan yang sudah ada saat ini.

2.4.2. Design

Dari data-data yang didapatkan sebelumnya, tahap *Design* ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.

2.4.3. Simulation prototype

Pada tahap ini *simulation prototype* merupakan sesuatu yang lengkap, tetapi sesuatu yang harus di evaluasi dan dimodifikasi kembali.

2.4.4. Implementation

Pada tahap ini segala sesuatu yang telah disusun dan direncanakan akan diterapkan. Implementasi adalah tahapan yang benar-benar menentukan tercapai atau tidaknya suatu tugas.

2.4.5. Monitoring

Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*.

2.4.6. Management

Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan *level management* dan strategi bisnis Perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis perusahaan.

2.5. Evaluasi dan Hasil

Pada tahap ini dilakukan pengumpulan data dengan menganalisis data dari hasil perbandingan yang Sudah dilakukan. Data yang dihasilkan dari perbandingan antara IPv4 dan IPv6 dengan melihat hasil *throughput*, *Round Trip Time* (RTT) *dan Security*, dari ketiga proses tersebut akan didapatkan hasil yang nantinya menjadi data hasil penelitian yang dilakukan.

3. HASIL DAN PEMBAHASAN

3.1. *Installasi* dan Konfigurasi

Pada tahap ini akan dilakukan installasi perangkat lunak yang dibutuhkan untuk pengujian komputer *server*, *client* dan *router*. *Server* yang digunakan menggunakan *windows 11*, *client* menggunakan *Windows 10 64 bit* dan *router* menggunakan *MikroTik RB92ND*.

3.2. Melakukan Pengujian

Pengujian dilakukan langsung, setelah selesainya metode instalasi dan konfigurasi. Dalam melakukan pengujian proses dilakukan dalam beberapa kondisi sistem operasi untuk PC klien dan server adalah Windows 10 dan Windows 11 dengan menggunakan IPv4.

Pada kondisi tersebut akan dilakukan pengujian. Proses pengujian dilakukan dalam beberapa tahap, yaitu :

1. Iperf3 digunakan untuk pengujian throughput, dan ukuran paket adalah kelipatan 10 Mbytes, berkisar antara 10 hingga 100. Setiap jenis paket data akan dikirim tiga kali, dengan periode pengiriman 20 detik di antaranya, untuk mendapatkan temuan yang dapat diandalkan. Rata-ratanya kemudian ditentukan dengan menyusun statistik hasil transmisi paket data.
2. Pengujian parameter latensi menggunakan ping dan tracerout, berfokus pada waktu respons (RTT) yang ditampilkan untuk setiap paket data yang dikirim dan diterima, dengan melakukan pengujian sebanyak 3 kali dengan durasi 20 detik untuk pengirimanya.
3. Pengujian parameter keamanan menggunakan *Nmap*, untuk menguji keamanan IPv4 dan IPv6 menggunakan beberapa perintah yang terdapat pada *tools Nmap*. *Nmap* akan memindai target dan melaporkan informasi tentang port yang terbuka, layanan yang berjalan dan kerentananya. Statistik dari hasil pemindaian dikumpulkan dan dijadikan penilaian bagi keamanan pada kedua IP tersebut.

Berikut adalah perintah dari *Iperf3* yang digunakan :

1. Buka *Iperf3*
2. Menggunakan IPv4, perintah berikut akan mengaktifkan mode server:

```
> iperf3 -s
```

3. Perintah tersebut menggunakan IPv4 untuk mengirimkan paket data selama 20 detik dengan ukuran tertentu.

```
> iperf3 -c [IPv4 server] -b [ukuran paket] -t 20
```

4. Menggunakan IPv4, perintah berikut akan mengaktifkan mode server:

```
> iperf3 -u -s
```

5. Perintah tersebut menggunakan IPv4 untuk mengirimkan paket data berukuran tertentu selama 20 detik :

```
> iperf3 -c [IPv4 server] -u -b [ukuran paket] -t 20
```

6. Menggunakan IPv6, perintah berikut akan mengaktifkan mode server :

```
> iperf -s -6
```

7. Perintah tersebut menggunakan IPv6 untuk mengirimkan paket data berukuran tertentu selama 20 detik :

```
> iperf3 -c [IPv6 server] -6 -t 20 -b [ukuran paket]
```

8. Perintah ini mengizinkan paket data hingga ukuran tertentu dan mengaktifkan mode server dengan IPv6 :

```
> iperf -s -6
```

9. Perintah tersebut menggunakan IPv6 untuk mengirimkan paket data berukuran tertentu selama 20 detik :

```
> iperf3 -c [alamat IPv6 server> -6 -u -b [ukuran paket] -t 30
```

Berikutnya mendapatkan *Round Trip Time (RTT)* pada tiap komputer *client*, sedikit berbeda dengan menggunakan *Iperf* yang menggunakan modus *server* dan modus *client*. Untuk mendapatkan *RTT* cukup menggunakan satu perintah pada *Command Prompt* yang terdapat pada komputer masing-masing. Berikut adalah perintah untuk mendapatkan nilai *RTT* pada *IP address*:

1. Buka *command prompt*
2. Masukkan perintah berikut untuk mengirim paket data berukuran tetap melalui IPv4 selama 20 detik:

```
> ping [IPv4 server] -t -n 20 -l [ukuran paket]
```

3. Masukkan perintah berikut untuk mengirim paket data berukuran tetap melalui IPv6 selama 20 detik:

```
> ping -6 [IPv6 server] -t -n 20 -l [ukuran paket]
```

Berikutnya adalah pengujian parameter kerentanaan keamanan pada tiap *IP address* komputer *client* menggunakan *Nmap. Nmap* dipasangkan pada salah satu komputer untuk mendeteksi IP yang berada pada komputer *server*. Berikut perintah-Nya :

1. Ketikkan perintah berikut pada *command*, perintah untuk *scanning* IPv4

```
>  nmap -T4 -A -v [IPv4 server]
```

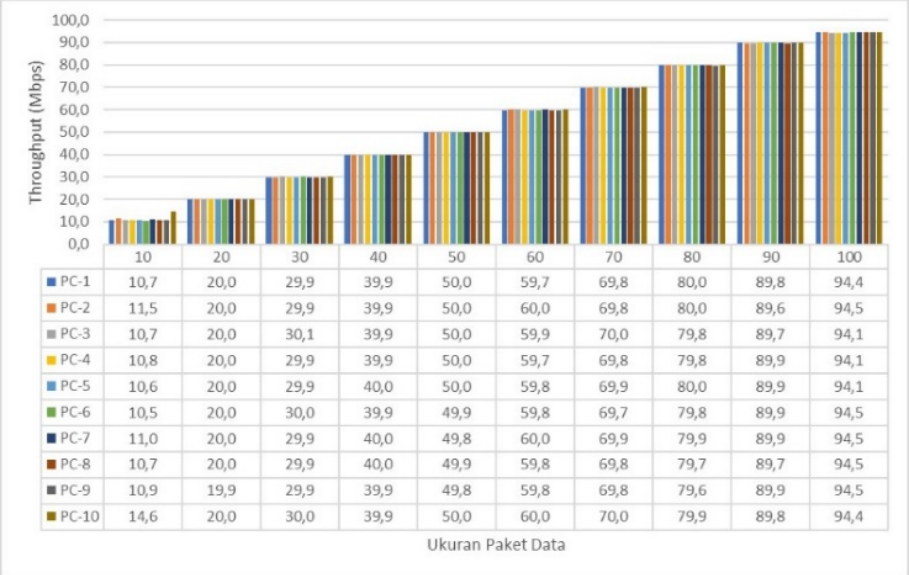
2. Ketikkan perintah berikut pada *command*, perintah untuk *scanning* IPv6

```
> nmap -6 -T4 -A -v [IPv6 server]
```

3.3. Hasil Pengujian

3.3.1. *Iperf3 Throughput*

Pada pengujian menggunakan *software Iperf3* menggunakan IPv4. hasil eksperimen menunjukkan bahwa terdapat perbedaan throughput yang dihasilkan pada saat pengiriman paket data menggunakan IPv4. Kualitas berikut ini juga unik di setiap PC. Untuk rincian tambahan mengenai perbedaan throughput di IPv4, terlihat pada Gambar 3.



	10	20	30	40	50	60	70	80	90	100
PC-1	10,7	20,0	29,9	39,9	50,0	59,7	69,8	80,0	89,8	94,4
PC-2	11,5	20,0	29,9	39,9	50,0	60,0	69,8	80,0	89,6	94,5
PC-3	10,7	20,0	30,1	39,9	50,0	59,9	70,0	79,8	89,7	94,1
PC-4	10,8	20,0	29,9	39,9	50,0	59,7	69,8	79,8	89,9	94,1
PC-5	10,6	20,0	29,9	40,0	50,0	59,8	69,9	80,0	89,9	94,1
PC-6	10,5	20,0	30,0	39,9	49,9	59,8	69,7	79,8	89,9	94,5
PC-7	11,0	20,0	29,9	40,0	49,8	60,0	69,9	79,9	89,9	94,5
PC-8	10,7	20,0	29,9	40,0	49,9	59,8	69,8	79,7	89,7	94,5
PC-9	10,9	19,9	29,9	39,9	49,8	59,8	69,8	79,6	89,9	94,5
PC-10	14,6	20,0	30,0	39,9	50,0	60,0	70,0	79,9	89,8	94,4

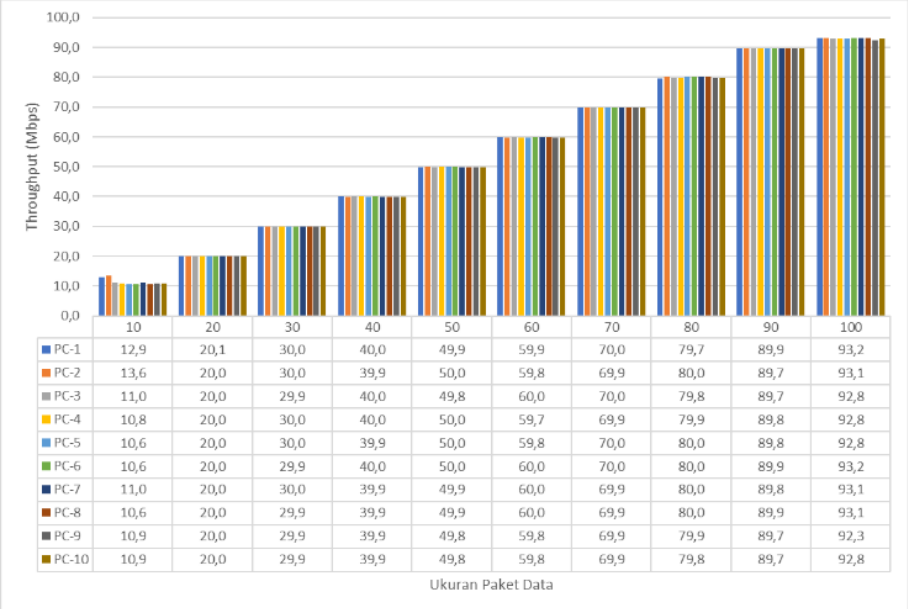
Gambar 3. *Throughput* IPv4

Throughput rata-rata untuk semua komputer *client* pada semua ukuran paket data adalah 54,52 *Mbps*, *Throughput* minimum terjadi pada PC-3, PC4, PC5 dengan ukuran paket data 100 *byte*, yaitu 94,1 *Mbps* dan *throughput* maksimum terjadi pada PC-10 dengan ukuran paket data 10 *byte*, yaitu 14,6 *Mbps*.

Pada performa setiap komputer untuk PC-1 memiliki *throughput* yang *consistently* paling tinggi di semua ukuran paket data, dengan *throughput* rata-rata 55,00 Mbps, pada PC-2 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 54,42 *Mbps*. pada PC-3 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 94,1*Mbps*. Pada PC-4 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 54,39 *Mbps*. Pada PC-5 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 54,42 *Mbps*.

Pada PC-6 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 54,40 *Mbps*. Pada PC-7 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 54,49 *Mbps*. Pada PC-8 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 54,40 *Mbps*. Pada PC-9 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 54,40 *Mbps*. Dan pada ada PC-10 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 55,3 *Mbps*.

Pada pengujian menggunakan program Iperf3 menggunakan IPv6 juga terdapat perbedaan pada throughput yang dibuat saat mengirimkan paket data menggunakan IPv6. Kualitas berikut ini juga unik di setiap PC. Untuk rincian tambahan mengenai perbedaan throughput di IPv6, terlihat pada Gambar 4.



	10	20	30	40	50	60	70	80	90	100
PC-1	12,9	20,1	30,0	40,0	49,9	59,9	70,0	79,7	89,9	93,2
PC-2	13,6	20,0	30,0	39,9	50,0	59,8	69,9	80,0	89,7	93,1
PC-3	11,0	20,0	29,9	40,0	49,8	60,0	70,0	79,8	89,7	92,8
PC-4	10,8	20,0	30,0	40,0	50,0	59,7	69,9	79,9	89,8	92,8
PC-5	10,6	20,0	30,0	39,9	50,0	59,8	70,0	80,0	89,8	92,8
PC-6	10,6	20,0	29,9	40,0	50,0	60,0	70,0	80,0	89,9	93,2
PC-7	11,0	20,0	30,0	39,9	49,9	60,0	69,9	80,0	89,8	93,1
PC-8	10,6	20,0	29,9	39,9	49,9	60,0	69,9	80,0	89,9	93,1
PC-9	10,9	20,0	29,9	39,9	49,8	59,8	69,9	79,9	89,7	92,3
PC-10	10,9	20,0	29,9	39,9	49,8	59,8	69,9	79,8	89,7	92,8

Gambar 4. *Throughput* IPv6

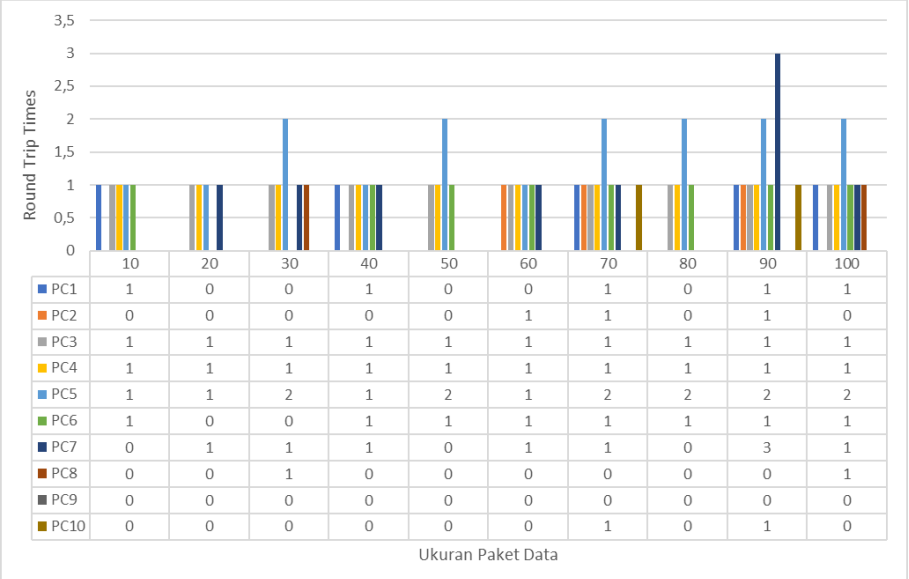
Throughput rata-rata untuk semua komputer *client* pada semua ukuran paket data adalah 69,8 Mbps, *throughput* minimum terjadi pada PC-8 dengan ukuran paket data 30 *byte*, yaitu 99,7 *Mbps*, dan *throughput* maksimum terjadi pada PC-1 dengan ukuran paket data 100 *byte*, yaitu 99,7 *Mbps*.

Pada performa setiap komputer untuk PC-1 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 81,5 Mbps, PC-2 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 80,9 *Mbps* PC-3 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 70,8 *Mbps*, PC-4 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 68,8 *Mbps*, PC-5 Memiliki throughput yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 68,7 *Mbps*, PC-6 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 69,9 *Mbps*, PC-7 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 70,0 Mbps. PC-8 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 70,1 Mbps, PC-9 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 70,2 *Mbps*, dan PC-10 Memiliki *throughput* yang *consistently* tinggi di semua ukuran paket data, dengan *throughput* rata-rata 70,3 *Mbps*.

Dari data tersebut menunjukan performa *throughput* rata-rata IPv6 lebih tinggi dari IPv4 untuk performa komputer *client* PC-1, PC-2, PC-6, PC-7, PC-8, PC-9, dan PC-10 memiliki performa yang lebih tinggi di IPv6 Dan PC-3, PC-4, dan PC-5 memiliki performa yang lebih tinggi di IPv4. Secara umum, IPv6 menunjukan performa yang lebih baik dibandingkan IPv4 dalam hal *throughput* rata-rata.

3.3.2. Round Trip Times (RTT)

Selain mengukur *throughput* menggunakan *Iperf3* pada penelitian ini juga menggunakan *ping* untuk mendapatkan *round trip times (RTT)* dengan menggunakan parameter paket data. Hasil pengujian *round trip times* pada Ipv4 dapat dilihat pada Gambar 5.



	10	20	30	40	50	60	70	80	90	100
PC1	1	0	0	1	0	0	1	0	1	1
PC2	0	0	0	0	0	1	1	0	1	0
PC3	1	1	1	1	1	1	1	1	1	1
PC4	1	1	1	1	1	1	1	1	1	1
PC5	1	1	2	1	2	1	2	2	2	2
PC6	1	0	0	1	1	1	1	1	1	1
PC7	0	1	1	1	0	1	1	0	3	1
PC8	0	0	1	0	0	0	0	0	0	1
PC9	0	0	0	0	0	0	0	0	0	0
PC10	0	0	0	0	0	0	1	0	1	0

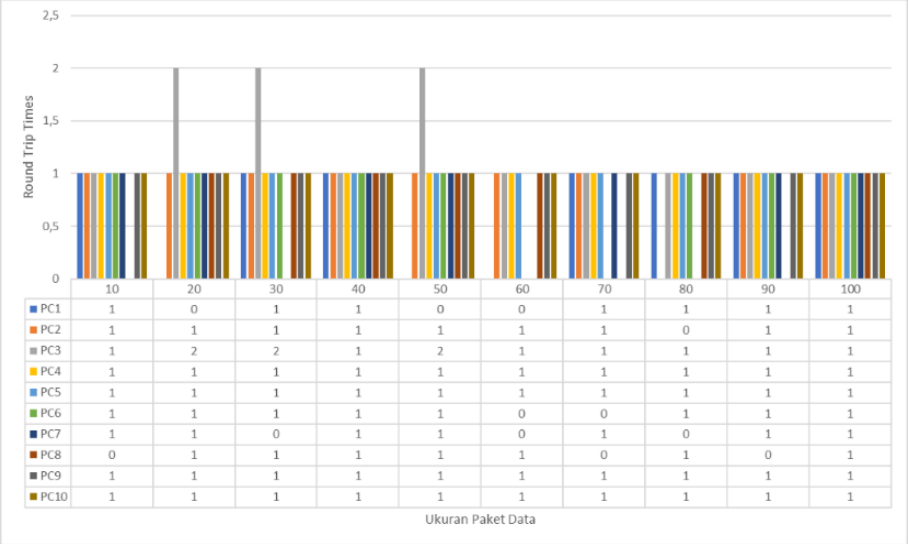
Gambar 5. *RTT Ipv4*

Berdasarkan grafik tersebut menunjukkan rata-rata RTT (*Round Trip Time*) *ping* untuk berbagai ukuran paket data (10-100 *byte*) pada 10 perangkat (PC1-PC10). Grafik menunjukan rata-rata *Round Trip Time* (RTT) pada 10 *client* berbeda. Terdapat ukuran paket data dalam satuan byte, dan menunjutkan waktu RTT dalam milidetik. Setiap baris pada grafik mewakili satu *client*.

Pada PC1, PC2, PC9 dan PC10 mewakili RTT yang paling stabil, dengan sedikit variasa di semua ukuran paket data. Pada PC6 mewakili RTT yang paling tidak stabil, dengan variasi yang signifikan di semua ukuran paket data. *Client* lain mewakili variasi RTT yang moderat di semua ukuran paket data, pada umumnya, RTT meningkat seiring dengan ukuran paket data hal ini dikarenakan paket data yang lebih besar membutuhkan waktu lebih lama untuk ditransmisikan dan diterima. PC3 dan PC4 mewakili RTT yang relative konsisten di semua ukuran paket data, PC6 mewakili RTT yang meningkat secara signifikan dengan paket data yang lebih besar.

Sementara itu untuk mendapatkan RTT, pengujian ping pada IPv6 menghasilkan informasi yang berbeda-beda di setiap PC seperti yang terlihat pada Gambar 6. Grafik menunjukan rata-rata Round Trip Times (RTT) dari 10 komputer client yang menggunakan IPv6. RTT diukur dalam satuan milidetik, dan menggunakan ukuran paket data yang dikirim dalam satuan byte.

Berdasarkan grafik tersebut menunjukkan rata-rata RTT (Round Trip Time) ping untuk berbagai ukuran paket data (10-100 byte) pada 10 perangkat (PC1-PC10). Pada koneksi jaringan secara keseluruhan stabil dengan RTT rata-rata rendah, namun ada beberapa komputer yang mengalami RTT lebih tinggi dibandingkan komputer lain dan kehilangan paket data sangat minimal.



Gambar 6. *RTT* IPv6

Pada PC1, PC2, PC3 dan PC4 memiliki RTT yang konsisten di semua ukuran paket data, dengan rata-rata RTT 1 milidetik, pada PC5, PC6, PC7 dan PC8 memiliki RTT yang sedikit lebih tinggi disbandingkan PC1, PC2, PC3 dan PC4, dengan rata-rata RTT sekitar 2 milidetik. Pada PC9 dan PC10 memiliki RTT yang paling tinggi, dengan rata-rata RTT sekitar 3 milidetik.

Dengan begitu dari kedua IP tersebut antara IPv4 dan IPv6 untuk pengukuran menggunakan Ping untuk mendapatkan Round Trip Times (RTT). Berdasarkan data tersebut tidak ada perbedaan yang signifikan antara RTT IPv4 dan IPv6 rata rata RTT untuk kedua IP sama pada semua PC, yaitu 1.0 milidetik. Namun IPv4 memiliki nilai RTT yang lebih rendah yaitu 0 milidetik pada beberapa PC (PC2, PC3, PC8 dan PC9), sedangkan IPv6 memiliki nilai minimum RTT 1 milidetik pada semua PC.

Dari segi kecepatan baik IPv4 dan IPv6 memiliki kecepatan yang hamper sama, dengan rata-rata RTT 1 milidetik. Pada konsistensi IPv6 memiliki performa yang lebih konsisten dengan nilai minimum dan maksimum RTT yang sama 1 milidetik pada semua PC. Dan pada efisinesi IPv4 memiliki potensi untuk lebih efisien dalam beberapa kasus, dengan nilai minimum RTT 0 milidetik pada beberapa PC.

3.3.3. Nmap

Selain mengukur *throughput* dan *Round Trip Times* (RTT) pada penelitian ini juga menggunakan parameter *Nmap* untuk mengetahui kerentanan pada kedua IP tersebut dengan menggunakan parameter *Nmap* dapat diketahui manakah IP yang aman dengan melihat informasi yang ditampilkan oleh *nmap* pada IP target dan waktu yang dibutuhkan untuk mendapatkan informasi tersebut. Hasil *scan Nmap* Ipv4 dapat dilihat pada Tabel 1.

Tabel 1. *Scan Nmap IPv4*

Nama	Jenis	Hasil	Waktu
Alamat IP	*IP Address*	192.168.10.2	0,1 detik
Nama *Host*	*Host*	Ditemukan	5 detik
	Mac	Ditemukan	5 detik
	Os	Ditemukan	5 detik
	Status Host	*Up*	0,0027 detik
Informasi *Port*	*Scanning 4 Ports*		0,01 detik
	Scanning 1000 Ports	4 (139, 445, 443 dan 135)	0,47 detik
	Scanning 4 services		12,09 detik
Total Waktu *Scan*	*Scanned in*		72.11 detik

Dari tabel hasil *scan* IPv4 menggunakan *Nmap* didapatkan waktu yang dibutuhkan untuk mendapatkan informasi tersebut sebesar 72,11 detik. Dengan beberapa informasi

yang didapatkan dengan melihat ukuran waktu yang dihasilkan untuk mencari *IP address* sebesar 0,1 detik, mendapatkan informasi *host* sebesar 5 detik dengan status *host* dalam keadaan aktif deangan waktu 0,0027 detik. Selain dari informasi mengenai host yang didapatkan dalam hasil *scan* tersebut didapatkan pula hasil *scan port*, untuk hasil *scanning 4 port* didapatkan waktu sebesar 0,01 detik dan untuk *scanning 1000 port* didapatkan waktu sebesar 0,47 detik dengan ditampilkan *port* yang terbuka sebanyak 4 *port* (port 139, 445, 443 dan 135) serta hasil *scanning* 4 *service* didapatkan waktu sebesar 12,09 detik.

Sedangkan untuk IPv6 dalam mendapatkan informasi mengenai kerentanan didapatkan juga informasi yang hampir sama dengan IPv4 sebelumnya, dengan menggunakan parameter pengujian yang sama dengan IPv4 namun ada sedikit yang berbeda. Untuk lebih lengkapnya dapat dilihat pada Tabel 2.

Tabel 2. *Scan Nmap Ipv6*

Nama	Jenis	Hasil	Waktu
Alamat IP	*IP Address*	2001:db8:1:1::2	0,01 detik
Nama *Host*	*Host*	Tidak Ditemukan	-
	Mac	Tidak Ditemukan	-
	Os	*Windows*	-
	Status Host	*Up*	0,0036 detik
Informasi *Port*	*Scanning 3 Ports*		0,01 detik
	Scanning 1000 Ports	3 (445, 443 dan 135)	0,47 detik
	Scanning 3 services		12,06 detik
Total Waktu *Scan*	*Scanned in*	2001:db8:1:1::2	48,99 detik

Dari tabel hasil *scan ipv6* menggunakan *Nmap* didapatkan waktu yang dibutuhkan untuk mendapatkan informasi tersebut sebesar 48,99 detik. Dengan beberapa informasi yang didapatkan dari hasil pengujian dengan informasi nama *host* tidak ditemukan baik pada host maupun *mac* namun pada *OS* didapatkan informasi sistem yang digunakan yaitu *windows* dan status *host* didapatkan dalam keadaan aktif dengan waktu sebesar 0,0036 detik. Pada hasil *scan* informasi *port* didaptkan hasil *scanning 3 ports* dengan waktu sebesar 0,01 detik, dan pada *scanning* 1000 *ports* didapatkan 3 *port*) yang terbuka. Serta hasil *scanning 3 services* medapatkan waktu sebesar 12,06 detik.

Dari hasil pegujian menggunakan *Nmap* untuk *scanning* kedua *IP address* IPv4 dan IPv6 didapatkan informasi yang akurat mengenai keamanan IP tersebut. Pada IP versi 4 didapatkan waktu sebesar 72,11 detik sampai berhenti *scanning* dengan beberapa informasi yang ditampilkan secara men detail oleh IPv4 sedangkan untuk IP versi 6 didapatkan waktu sebesar 48,99 detik sampai berhenti *scanning* dengan informasi yang tidak terlalu banyak ditampilakn oleh IPv6. Dengan begitu IPv6 dikategorikan lebih aman untuk digunakan karena tidak terlalu banyak informasi yang ditampilkan serta lebih menutup ruang informasi yang penting seperti halnya informasi host pengguna dan port yang aktif.

3.4. Pembahasan

Berdasarkan teori yang dipaparkan dalam makalah "*Design of Accurate End-to-End IPv4 and IPv6 Performance Test*" oleh Moh. Kahiril Sailan dan Rosilah Hassan dari Universitas Kebangsaan Malaysia[9], pengguna IPv6 diprediksikan mampu merasakan kinerja jaringan yang lebih unggul dibandingkan IPv4. Alasan utama di balik prediksi ini adalah keunggulan IPv6 dalam hal *fragmentasi*, struktur, *checksum*, dan opsi *header* yang memungkinkannya mencapai *routing* yang lebih cepat.

Namun dari hasil pengujian secara keseluruhan dan yang sudah dijelaskan sebelumnya membuktikan bahwa penggunaan kedua *IP address* IPv4 dan IPv6 dalam jaringan lokal dengan menggabungkan kedua IP dalam satu jaringan membuktikan bahwa IPv6 dapat memberikan kinerja yang baik dari pada IPv4 dan memiliki tipe kerentanan keamanan yang aman bagi pengguna, namun untuk IPv4 tidak juga buruk bagi jaringan lokal yang dimana dari hasil

pengujian pada RTT didapatkan IPv4 lebih efisiensi dalam penggunaan jaringan lokal dengan nilai minimum RTT yang didapatkan 0 milidetik.

Dari segi kecepatan, baik IPv4 maupun IPv6 menunjukkan rata-rata Round-Trip Time (RTT) yang hampir sama, yaitu sekitar 1 milidetik, yang mengindikasikan performa latency yang setara pada jaringan lokal yang diuji. Namun, ketika dianalisis lebih lanjut dari segi konsistensi performa, IPv6 menunjukkan nilai RTT yang sangat stabil dengan rentang minimum dan maksimum yang sama, yaitu 1 milidetik, di seluruh perangkat pengujian (PC) yang digunakan dalam eksperimen ini. Hal ini menunjukkan bahwa IPv6 mampu mempertahankan latency yang konsisten tanpa fluktuasi signifikan antar perangkat.

Sebaliknya, IPv4 menunjukkan variasi nilai RTT yang lebih besar, dengan nilai minimum mencapai 0 milidetik pada beberapa perangkat, yang kemungkinan disebabkan oleh mekanisme caching atau optimasi lokal pada perangkat tersebut. Namun, nilai minimum ini tidak konsisten di seluruh perangkat dan tidak selalu mencerminkan kondisi jaringan secara umum. Oleh karena itu, meskipun IPv4 memiliki potensi untuk mencapai efisiensi latency yang lebih baik dalam kondisi tertentu, performanya kurang stabil dibandingkan IPv6 dalam konteks pengujian ini.

Analisis statistik lebih lanjut menggunakan standar deviasi RTT mendukung temuan ini, di mana IPv6 memiliki standar deviasi yang lebih rendah dibandingkan IPv4, menandakan performa yang lebih konsisten dan dapat diandalkan pada jaringan lokal yang diuji.

4. KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan pengujian dan hasil pengujian yang dilakukan pada penelitian ini adalah sebagai berikut:

1. Metode NDLC (*Network Depelovment Life Cycle*) dapat diterapkan dalam membangun koneksi jaringan IPv6 diatas jaringan IPv4 yang sudah ada. Terlihat dari hasil yang didapatkan dengan melihat *throughput, round-trip time (RTT)* dan keamanan IPv6 berjalan tanpa menggangu koneksi jaringan IPv4. Begitu juga dengan IPv4 yang dibangun dapat bekerja dengan baik.
2. Dalam perbedaan kinerja jaringan dari kedua IP baik IPv4 dan IPv6 didapatkan hasil sebagai berikut:
    a. Dari hasil praktik semua kondisi pengujian pada *perbandingan troughput, throughput* yang dibuat oleh IPv6 berada diatas IPv4 dalam hal *throughput* rata-rata.
    b. Dari segi kecepatan baik IPv4 dan IPv6 memiliki kecepatan yang hamper sama, dengan rata-rata RTT 1 milidetik. Pada konsistensi IPv6 memiliki performa yang lebih konsisten dengan nilai minimum dan maksimum RTT yang sama 1 milidetik pada semua PC. Dan pada efisinesi IPv4 memiliki potensi untuk lebih efisien dalam beberapa kasus, dengan nilai minimum RTT 0 milidetik pada beberapa PC.

Dari hasil pegujian menggunakan *Nmap* untuk *scanning* kedua *IP address* IPv4 dan IPv6 didapatkan informasi yang akurat mengenai keamanan IP tersebut. Pada IP versi 4 didapatkan waktu sebesar 72,11 detik sampai berhenti *scanning* dengan beberapa informasi yang ditampilkan secara men detail oleh IPv4 sedangkan untuk IP versi 6 didapatkan waktu sebesar 48,99 detik sampai berhenti *scanning* dengan informasi yang tidak terlalu banyak ditampilakn oleh IPv6.

5. SARAN

Mengingat batas-batas penyelidikan ini, konsep berikut secara khusus harus dipertimbangkan:

1. Penelitian lebih lanjut harus dilakukan untuk mengetahui penyebab variasi kinerja jaringan PC untuk setiap jenis IP dan sistem operasi.
2. Akan lebih baik jika melakukan penelitian dengan menggunakan sistem operasi berbeda untuk menilai fungsionalitas jaringan komputer berbasis IPv4 dan IPv6.
3. Mendapatkan hasil yang lebih tepat, disarankan untuk melakukan studi perangkat keras jaringan dengan skala yang lebih besar dan aktual.

DAFTAR PUSTAKA

[1] D. B. Dwiartanto, D. Pranindito, and N. Iryani, "ANALISA PERBANDINGAN PERFORMANSI JARINGAN IPv4 DAN IPv6 PADA MPLS VPN MENGGUNAKAN SERVER IMS CORE," *Jurnal Telekomunikasi dan Komputer*, vol. 11, no. 2, p. 85, Aug. 2021, doi: 10.22441/incomtech.v11i2.10195.

[2] A. Tantoni *et al.*, "ANALISIS KOMPARASI PERFORMA JARINGAN KOMPUTER PADA IMPLEMENTASI IPv4 dan IPv6," *Jurnal Informatika & Rekayasa Elektronika)*, vol. 1, no. 2, 2018, [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jire

[3] M. Ulfa, "PERBANDINGAN IPV4 DAN IPV6 DALAM MEMBANGUN JARINGAN LOCAL AREA NETWORK (LAN)," 2014.

[4] M. Yusril, H. Setiawan, and C. Prianto, *SIMULASI INTEROPERABILITAS SISTEM PENGALAMATAN IPV4 DAN IPV6 PADA PERANGKAT-PERANGKAT JARINGAN KOMPUTER*. 2019. [Online]. Available: https://seminar-id.com/semnas-sainteks2019.html

[5] N. Nurdadyansyah and M. Hasibuan, "PERANCANGAN LOCAL AREA NETWORK MENGGUNAKAN NDLC UNTUK MENINGKATKAN LAYANAN SEKOLAH," *Konferensi Nasional Ilmu Komputer (KONIK)*, 2021.

[6] Sugiyono, "METODE PENELITIAN KUANTITATIF KUALITATIF DAN R&D," 2012.

[7] Wongkar S, Sinsuw A, and Najoan X, "Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan LAN Dan WLAN Di Desa Kawangkoan Bawah Wilayah Amurang II," *E-journal Teknik Elektro dan Komputer*, vol. 4, no. 6, pp. 2301–8402, 2015.

[8] M. Syaeful Bahry and B. Sugiantoro, "Local Area Network), NDLC (Network Development Life Cycle), VLAN (Virtual Local Area Network)," 2017.

[9] M. K. Sailan, R. Hassan, and A. Patel, "A comparative review of IPv4 and IPv6 for research test bed," in *Proceedings of the 2009 International Conference on Electrical Engineering and Informatics, ICEEI 2009*, 2009, pp. 427–433. doi: 10.1109/ICEEI.2009.5254698.