Implementasi Routing Dinamis OSPFV3 Pada Internet Protocol Versi 6 (IPV6) Menggunakan Router Mikrotik

Andry Maulana

Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta
Jl. Damai No. 8, Warung Jati Barat (Margasatwa), Pasar Minggu, Jakarta Selatan
E-mail: andry.ayz@nusamandiri.ac.id

Abstract - **The use of IP addresses now that they are running out requires that we prepare to migrate to IP address version 6 (ipv6). The ipv6 protocol is designed for larger and wider users. But along with the need for the use of ipv6 many network protocols that do not yet support include routing protocols. Routing used on ipv4 with ipv6 is very different like ospf for ipv4 and ospfv3 for ipv6. To do this research the author tries to apply the concept of a real network by implementing the ospfv3 routing protocol using ipv6 on a proxy device. The method used is NDLC (Network Development Life Cycle) ranging from analysis to management. The test results in the form of quality of service network QOS (quality of service) using the ospfv3 protocol is very good with obtaining 0.716 ms delay, 0.002 ms jitter, 0% packet loss and 1525 k throughput.**

***Keywords* – ipv6, routing, ospfv3, qos**

Abstrak – **penggunaan ip address sekarang yang sudah hampir habis mengharuskan kita bersiap untuk migrasi ke ip address versi 6(ipv6). Protocol ipv6 ini dirancang untuk pengguna yang lebih besar dan luas. Namun seiring kebutuhan akan penggunaan ipv6 ini banyak protokol jaringan yang belum mendukung antara lain protokol routing. Routing yang digunakan pada ipv4 dengan ipv6 sangat berbeda seumpama ospf untuk ipv4 dan ospfv3 untuk ipv6. Untuk melakukan penelitian ini maka penulis mencoba menerapkan konsep jaringan nyata dengan cara mengimplementasikan protokol routing ospfv3 dengan menggunakan ipv6 pada perangkat mikrotik. Metode yang digunakan adalah ndlc(Network Development Life Cycle) mulai dari analisis sampai dengan manajemen. Hasil pengujian berupa kualitas layanan jaringan qos (quality of service)dengan menggunakan protokol ospfv3 sangatlah baik dengan didapatnya delay 0,716 ms, jitter 0.002 ms, packet loss 0% dan throughput 1525 k.**

***Kata kunci* – ipv6, routing, ospfv3, qos**

I. PENDAHULUAN

Perkembangan jaringan komputer yang tumbuh pesat seiring perkembangan dan kemajuan teknologi membuat kebutuhan ip address semakin bertambah. Menurut data IANA(Internet Assigned Number Authority) tahun 2014, jumlah penggunaan IPv4 diseluruh dunia tersisa 7%[1]. Ip address digunakan pada setiap perangkat yang terhubung dengan jaringan komputer. Ip address diibaratkan sebuah nama agar setiap perangkat dalam jaringan komputer dapat saling terhubung satu sama lainnya. Keterbatasan penyedia alamat ip address saat ini hanya dapat menampung sekitar 4,3 milyar sedangkan kebutuhan semakin banyak seiring dengan perkembangan jaringan komputer di era milenial.

Internet Protocol version 6 (IPv6) atau yang sering disebut juga sebagai IPng (Internet Protocol next generation) adalah suatu protocol layer ketiga terbaru yang diciptakan untuk menggantikan IPv4 atau yang sering dikenal sebagai Internet Protocol. Alasan utama dari penciptaan Internet Protocol version 6 (IPv6) ini adalah untuk mengoreksi masalah pengalamatan pada versi 4 (IPv4)[2]. Untuk mengatasi keterbatasan IPv4 maka dibentuklah metode pengalamatan ip address yang baru yang dinamakan IPv6. IPv6 sendiri adalah ip addres baru untuk menggantikan IPv4 dengan menggunakan bilangan hexadesimal sebanyak 128bit. IP versi 6 (IPv6) adalah protokol Internet versi baru yang di desain sebagai pengganti dari IPv4. IPv6 yang memiliki kapasitas alamat (address) raksasa (128 bit), mendukung penyusunan alamat secara terstruktur, yang memungkinkan Internet terus berkembang.

Untuk menerapkan ipv6 dibutuhkan perangkat yang memiliki protokol routing dinamis yang mensupport protokol tersebut. Open Shortes Path First versi 3 (OSPFv3) merupakan sebuah routing protocol open source yang telah banyak digunakan oleh beberapa perusahaan besar basis jaringan menggunakan basis IPv6. OSPF sudah mengeluarkan beberapa versi, seperti OSPFv1, OSPFv2 dan yang baru OSPFv3. Perbedaan yang paling mendasar dari OSPFv2 dengan OSPFv3 adalah dari internet protokol nya. OSPFv3 menggunakan basis IPv6[3]. OSPFv2 digunakan untuk pengalamtan yang menggunakan IPv4 saja, sedangkan OSPFv3 secara khusus digunakan untuk pengalamatan IPv6[4].

Dari uraian diatas maka penulis mencoba mengimpementasikan protokol IPV6 untuk komunikasi routing dinamis menggunakan OSPFv3 pada perangkat router board mikrotik haplite. Pengimplementasikan ini akan diujikan

sebelumnya pada beberapa komputer yang terhubung dengan quality of service (QOS) menggunakan software wireshark.

II. LANDASAN TEORI DAN METODE

IPV6

Untuk mengatasi keterbatasan IPv4 maka dibentuklah metode pengalamatan ip address yang baru yang dinamakan IPv6. IPv6 sendiri adalah ip addres baru untuk menggantikan IPv4 dengan menggunakan bilangan hexadesimal sebanyak 128bit. Adapun 2 kelebihan-kelebihan yang ditawarkan IPv6 adalah sebagai berikut: IPv6 merupakan solusi bagi keterbatasan alamat IPv4 (32 bit). IPv6 dengan 128 bit memungkinkan pengalamatan yang lebih banyak, yang memungkinkan IP-nisasi berbagai perangkat (PDA, handphone, perangkat rumah tangga, perlengkapan otomotif) [5]. IP versi 6 (IPv6) dapat didefinisikan sebagai protokol Internet versi baru yang di desain sebagai pengganti dari IPv4. IPv6 yang memiliki kapasitas alamat (address) raksasa (128 bit), mendukung penyusunan alamat secara terstruktur, yang memungkinkan Internet terus berkembang[6].

Routing

Routing adalah sebuah proses untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya sehingga menjadi rute tertentu[7]. Routing memiliki dua jenis yaitu routing statis dan dinamis. Routing statis yang digunakan pada penelitian ini adalah OSPF,EIGRP dan RIP. OSPF (Open Shortest Path First) adalah sebuah Routing Protocol yang dipergunakan untuk membuat rute agar paket data yang akan dikirimkan dari sebuah komputer ke komputer lain didalam jaringan komputer. Routing juga suatu protokol yang digunakan untuk mendapatkan rute atau petunjuk dari satu jaringan ke jaringan yang lain, routing dapat berarti proses dimana suatu router akan memilih jalur atau rute untuk mengirimkan atau meneruskan suatu paket ke jaringan yang dituju. Router menggunakan IP address tujuan untuk mengirimkan paket, dan agar router mengetahui rute mana yang harus digunakan untuk meneruskan paket ke alamat tujuan, router harus belajar atau bertukar informasi sesama router yang saling terhubung untuk mengetahui jalur atau rute yang terbaik. Routing protokol digunakan untuk memfasilitasi pertukaran informasi routing antar router. Dengan routing protokol, router dapat berbagi informasi routing table, yaitu informasi mengenai jaringan lain yangsaling terhubung. Ada beberapa routing protokol yang mendukung IPv6, yaitu RIPng, OSPFv3EIGRP for IPv6(Cisco properiarity), IS-IS for IPv6,BGP IPv6, dan lainnya. Masing masing dibuat berdasarkan routing protokol sebelumnya yang mendukung IPv4 namun disesuaikan dengan lingkup IPv6 dan memiliki beberapa kelebihan dan pembaharuan serta cara konfigurasi yang berbeda pada router.

OSPFv3

Open Shortest Path First (OSPF) adalah routing protokol kelas link-state yang dikembangkan untuk memperbaiki kinerja dari routing protokol RIP.OSPF adalah routing protokol yang menggunakan konsep area. Kelebihan dari OSPF dibandingkan dengan RIP adalah kecepatan dalam melakukan konvergensi dan lebih luasnya jaringan yang bisa dijangkau. Pada dasarnya OSPFv3 menggunakan jenis paket yang sama pada OSPFv2. Perbedaan yang paling jelas ialah OSPFv3 mendukung pengalamatan 128-bit. OSPFv2 menggunakan alamat 224.0.0.5 dan 224.0.0.6, OSPFv3 menggunakan alamat multicast IPv6 yaitu FF02::5 dan alamat FF02::6 untuk router DR (designatedrouters) dan BDR (Backup DRs). OSPFv3 menggunakan alamat link-localnya untuk melakukan advertisements bukan alamat globalnya.Paket header OSPFv3 adalah sebesar 16-byte,berbeda dengan OSPFv2 sebesar 24-byte. Paket header OSPFv3. Pada IPv6 kemampuan dalam autentikasi dan enkripsi menggunakan header extension(ospv3).

Wireshark

Wireshark adalah tool yang digunakan untuk menganalisa paket data dalam sebuah kinerja jaringan. Wireshark dapat menangkap paket data atau informasi yang berada di dalam jaringan, sehingga data yang tertangkap dapat di analisa untuk berbagai keperluan[8]. Wireshark dapat diartikan sebagai sebuah Network Packet Analyzer. Network Packet Analyzer akan mencoba menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi dipaket tersebut sedetail mungkin. Network Packet Analyzer diumpamakan sebagai alat untuk memeriksa apa yang sebenarnya sedang terjadi di dalam kabel jaringan. Wireshark adalah sebuah Network Packet Analyzer. Network Packet Analyzer akan mencoba menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi dipaket tersebut sedetail mungkin [9].

Quality Of Service(QOS)

Quality of Service merupakan langkah pengujian kinerja jaringan ketika suatu host terkoneksi dengan host lainnya. Pengujian ini meliputi delay, packet loss, jitter dan throughput. Quality of Service (QoS) juga merupakan teknologi yang memungkinkan administrator jaringan untuk menangani berbagai efek dari terjadinya kongesti pada lalu lintas aliran paket dari berbagai layanan untuk memanfaatkan sumber daya jaringan secara optimal,

dibandingkan dengan menambah kapasitas fisik jaringan tersebut[10]. merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda [11]

Network Development Life Cycle

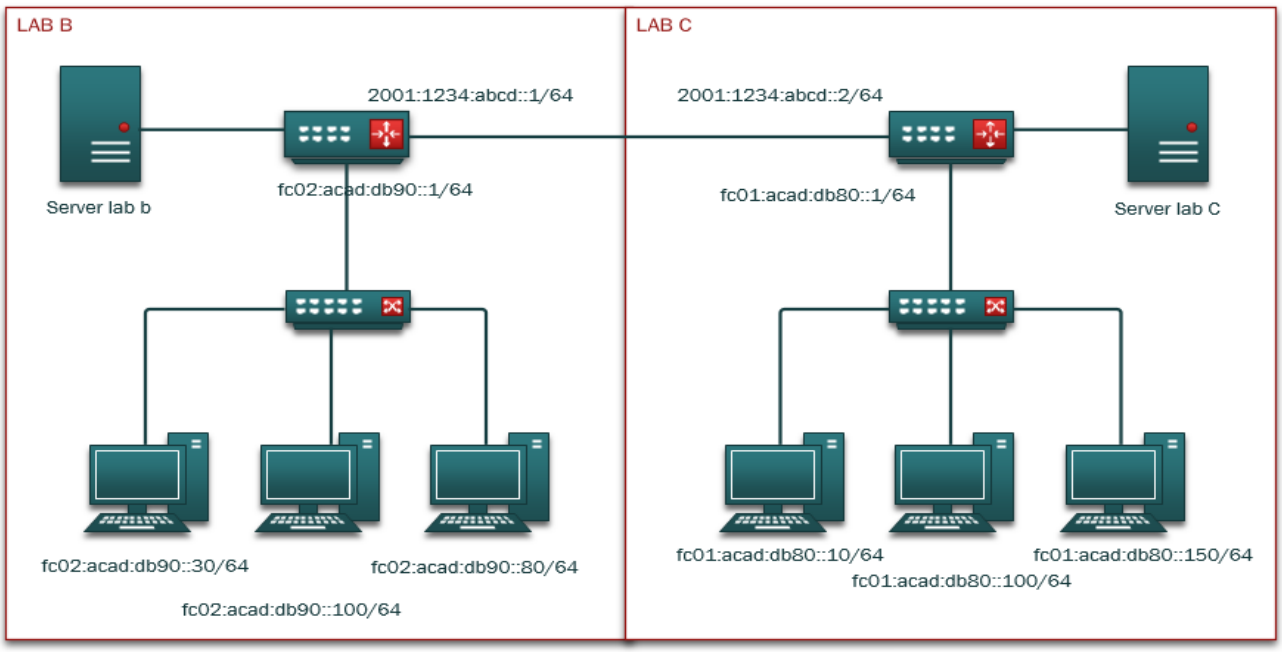
NDLC merupakan metode yang bergantung pada proses pembangunan seperti perancangan proses bisnis dan perancangan infrastruktur [12]. Adapun tahapannya adalah sebagai berikut :

1. Analysis
   Tahapan ini adalah tahapan awal yang digunakan dalam penelitian yang meliputi analisa kebutuhan, analisa keinginan user dan analisa topologi jaringan yang digunakan. .Pada tahap ini juga dilakukan pengumpulan data-data yang dibutuhkan untuk mengetahui perumusan masalah dan cara menyelesaikan masalah tersebut. Tahapan ini juga menganalisa masalah yang terjadi apabila jaringan yang dibangun hanya menggunakan satu buah provider.
2. Design
   Dari data-data yang didapatkan pada tahapan analysis, Tahap desain ini akan membuat gambar desain topologi jaringan, diharapkan dengan gambar ini akan memberikan gambaran dari kebutuhan yang ada. Desain ini dapat berupa desain struktur topologi yang akan digunakan, desain kebutuhan perangkat, desain jalur pengkabelan yang digunakan. Dalam penelitian ini penulis menggunakan Cisco Packet Tracer untuk membuat desain jaringan yang sudah ada dan yang akan dibuat.
3. Simulation prototyping
   Sebelum menerapkan jaringan yang dibuat pada penelitian ini maka sebelumnya dibuat dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti Boson, Packet Tracert, Netsim dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan. Namun karena keterbatasan perangkat lunak simulasi ini, maka penulis hanya menggunakan alat bantu program simulator VirtualBox.
4. Implementation
   Di tahapan ini penerapan jaringan akan dibuat dngan menggunakan perangkat mikrotik. Penerapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam tahap implementasi, penulis menerap kan semua yang telah direncanakan dan dirancang sebelumnya.Pada tahapan inilah akan terlihat bagaimana system load balancing dengan menggunakan ipv6 yang akan dibangun.
5. Monitoring
   Pada tahap ini penulis melakukan pengujian langsung pada perangkat mikrotik yang diterapkan load balancing dan ipv6. Pengujian ini dilakukan dengan cara pengambilan data untuk melihat kinerja jaringan yang telah dirancang dan dikonfigurasi
6. Management
   Di manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan, yaitu dalam hal aktivitas, pemeliharaan dan pengolahan dikategorikan pada tahap ini.Kebijakan perlu di buat untuk membuat dan mengatur agar jaringan yang telah dibangun dapat berjalan dengan baik. Pada Teknik penelitian ini menggunakan dua jalur internet yang penulis beri mana ISP01 dan ISP02.

III. PEKERJAAN DAN DISKUSI HASIL

Tahapan Desain Topology

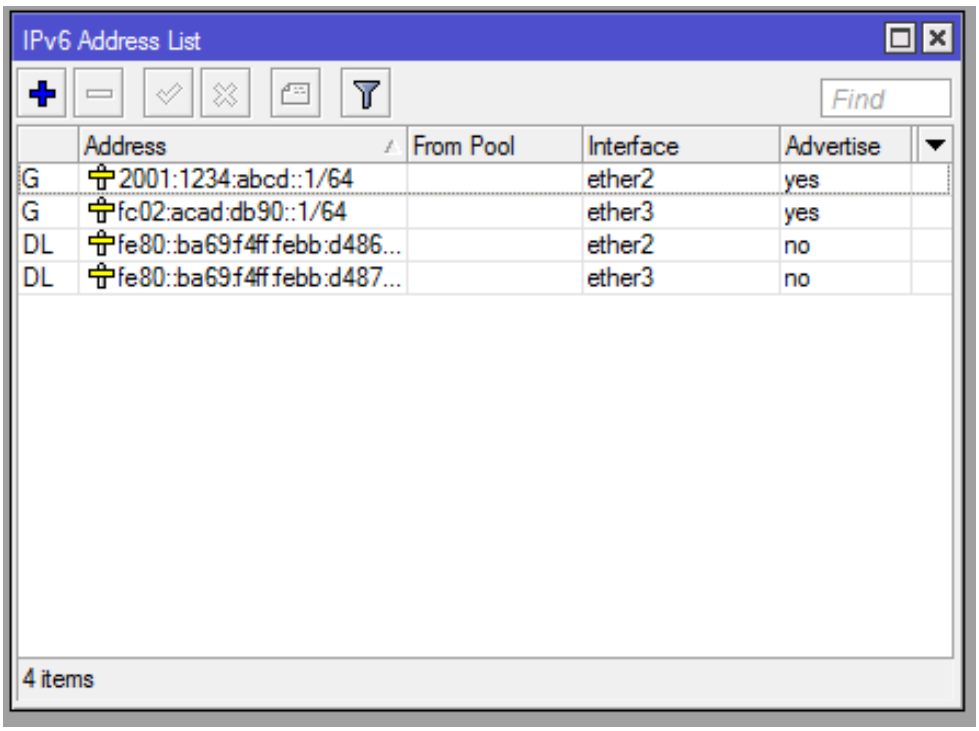
Langkah awal adalah dengan menganalisa kebutuhan dan mendesain topologi yang dibuat untuk di terapkan routing ospfv3. Topologi yang dibuat adalah dengan mengambil dari bentuk ruangan lab yang berasal dari topologi star. Kedua lab tersebut belum memiliki segment jaringan sehingga semua broadcast pada masing masing host dapat mengakibatkan beratnya kinaerja jaringan. Kemudian desain jaringan awal tersebut masih menggunakan ipv4. Dari hasil pengamatan inilah maka penulis membuat jaringan usulan dengan metode routing seperti dibawah ini.



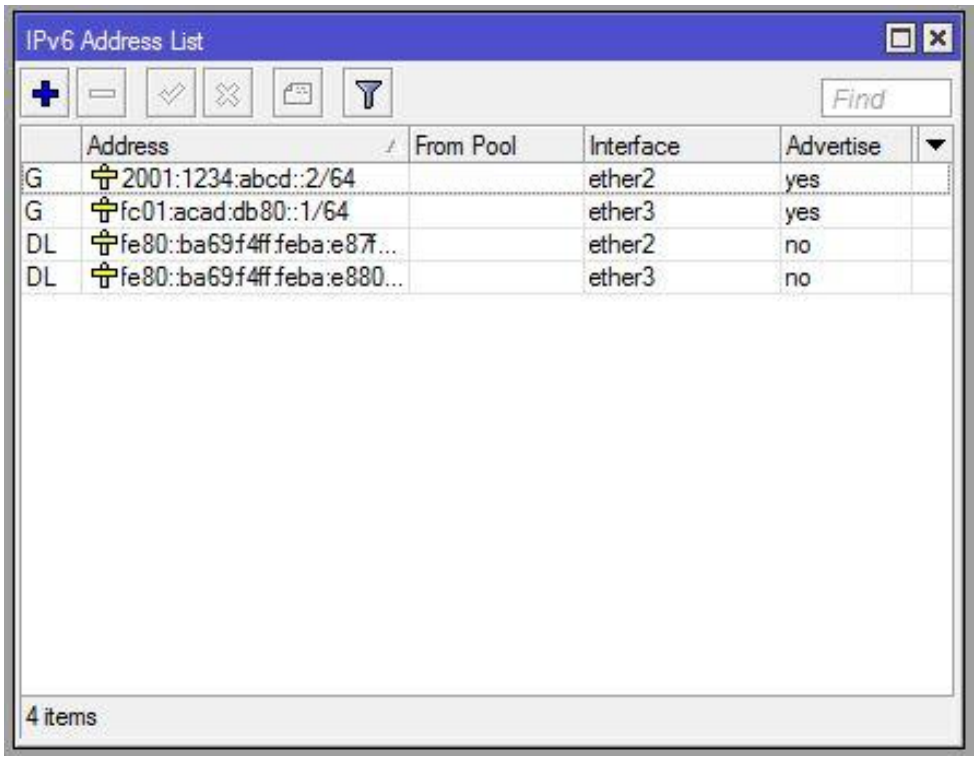
Gambar 1. Topologi Lab Komputer

Tahapan Routing

Setelah topologi dibuat maka selanjutnya adalah melakukan konfigurasi routing dengan OSPFv3. Untuk melakukan routing kedua segment jaringan ini harus memiliki ip address versi 6 pada masing masing perangkat. Alamat antar neighbor pada router ini akan dikirim ke masing masing router agar setiap router dapat mengenali network yang dimiliki oleh neighbournya.

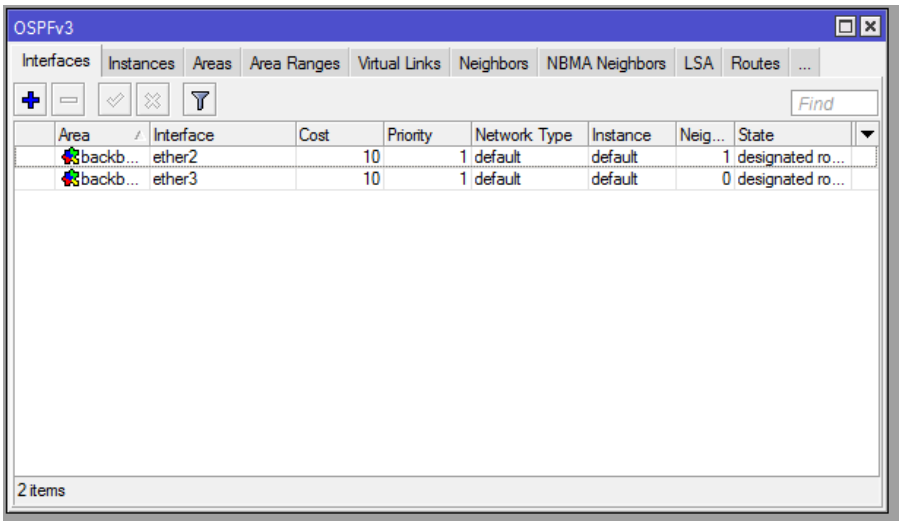


Gambar 2. Ip adddress router lab c

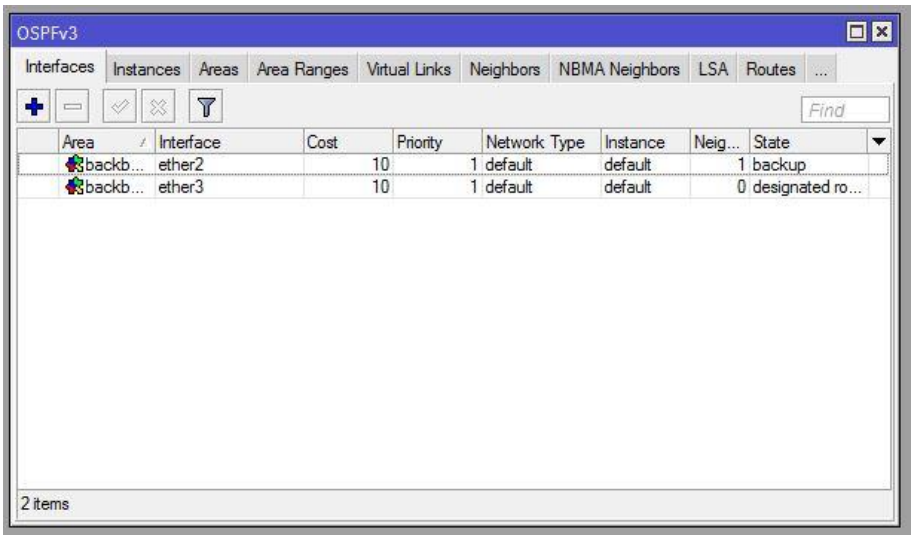


Gambar 3. Ip adddress router lab b

Selanjutnya melakukan konfigurasi routing antar router lab seperti berikut

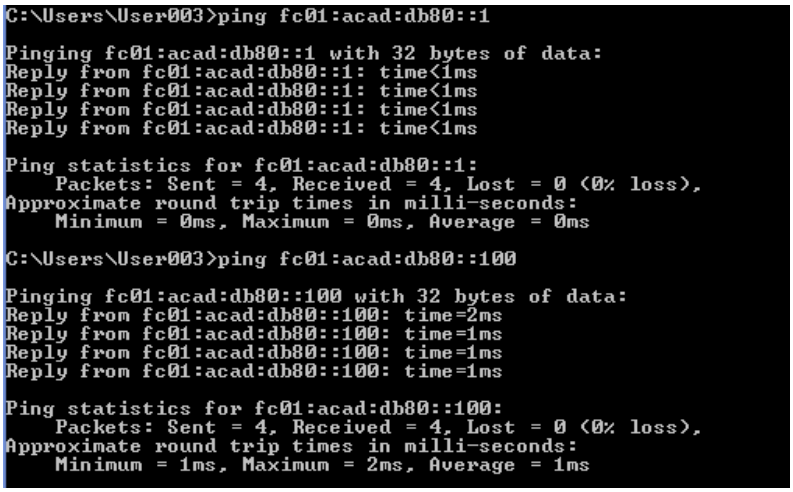


Gambar 4. Routing OSPFV3 router lab b



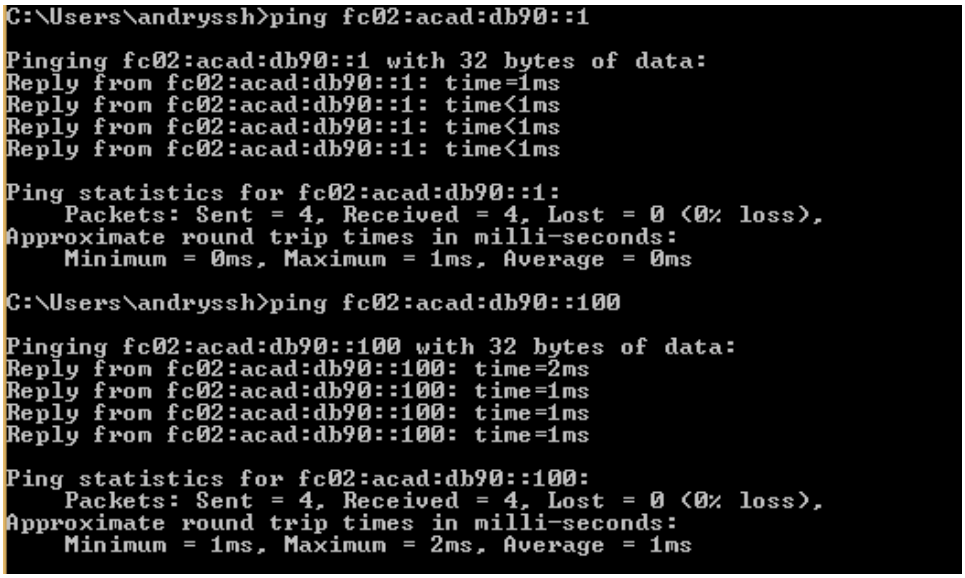
Gambar 5. Routing OSPFV3 router lab c

Pada gambar diatas menunjukan bahwa masing masing router telah terjadi kesesuaian (adjacency) dengan ditandai pada kolom state yang salah satu routernya menjadi backup designeted route (BDR) dan lainnya menjadi designeted route (DR). Langkah selanjutnya adalah menguji coba jaringan dari komputer yang ada pada lab c dengan komputer yang ada pada lab b dan sebaliknya.



Gambar 6. Pengujian koneksi pada cilent 1

Pengujian ini dilakukan pada komputer yang berada pada lab c ke komputer yang berada di lab b dan didapatkan hasil bahwa sudah terkoneksi. Lakukan hal yang sama pula dari lab b ke lab c.



Gambar 7. Pengujian koneksi pada client 2

Pengujian Jaringan

Setelah tahapan routing sudah selesai dengan melakukan pengujian koneksi terhadap client. Maka dilakukan tahapan selanjutnya yaitu menguji kualitas kinerja jaringan yang disebut dengan QOS(quality of service). Pengujian yang dilakukan adalah dengan menganalisis paket yang dikirim (delay, jitter, throughput dan paket los) dari sebuah client ke client lainnya dengan besaran file sebesar 60 mbps. Pengujian ini dilakukan sebanyak 5 kali dengan masing masing hasil pengujian kurang lebih 13.000 data yang tercapture dengan wireshark.

Pengujian Delay

Delay adalah waktu tunda saat paket yang diakibatkan oleh proses transmisi dari satu titik lain yang menjadi tujuannya. Delay diperoleh dari selisih waktu kirim antara satu paket TCP dengan paket lainnya.

Untuk Mendapatkan delay digunakan rumus :

$$\textbf{Delay = Waktu Kedua – Waktu Pertama}$$

Sedangkan untuk menghitung rata rata delay dapat menggunakan rumus :

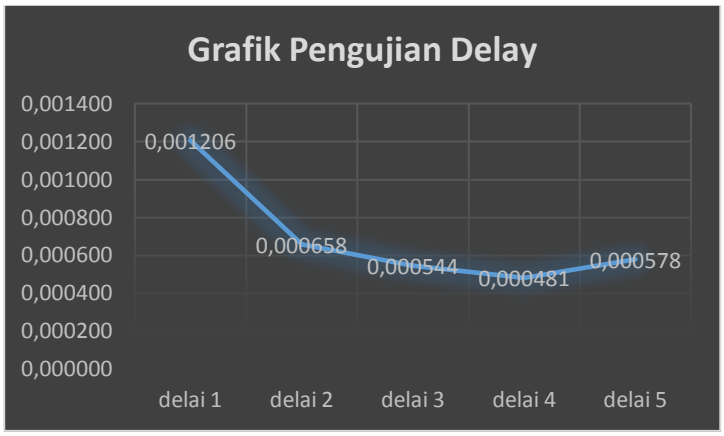
$$\textbf{Rata rata Delay} = \frac{\textbf{Total Delay}}{\textbf{Total Packet Yang Diterima}}$$

Untuk mendapatkan ucuan nilai yang baik maka dapat dilihat dengan acuan tabel dibawah ini

Tabel 1. Acuan nilai delay

Kategori Delay	Besar Delay
Sangat Bagus	< 9 ms
Bagus	9 sd 50 ms
Jelek	50 sd 450 ms
Sangat Jelek	>450 ms

Dari hasil pengujain delay maka didapatkan hasil rata rata delay sebagai berikut.



Gambar 8. Grafik Pengujian Delay

Grafik diatas menunjukan bahwa dengan menggunakan protokol ospf versi 3 (OSPFv3) dapat disimpulkan bahwa delay dari suatu paket yang dikirim antar client sebanyak 5 kali dinyatakan rata rata 0-1 ms yang berarti sangat bagus.

Pengujian Jitter

Jitter didefinisikan sebagai variasi delay yang diakibatkan oleh panjang queue dalam suatu pengolahan data dan reassemble paket-paket data di akhir pengiriman akibat kegagalan sebelumnya. Untuk Mendapatkan jitter terlebih dahulu harus mendapatkan nilai selisih delay kedua dengan dilay pertama dengan menggunakan rumus berikut :

$$\textbf{Selisih Delay} = \textbf{Delay2} - \textbf{Delay}$$

Setelah mendapatkan nilai selisih delay maka untuk menghitung jitter dapat menggunakan rumus :

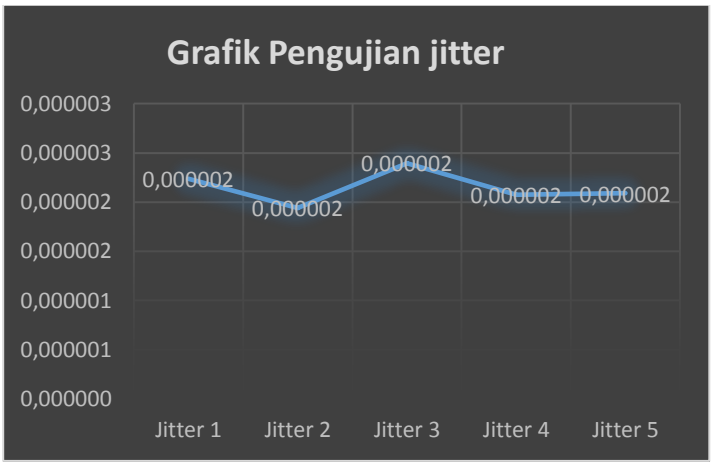
$$\textbf{Jitter} = \frac{\textbf{Selisih Delay}}{\textbf{Total Packet Yang Diterima - 1}}$$

Untuk mendapatkan ucuan nilai yang baik maka dapat dilihat dengan acuan tabel dibawah ini

Tabel 2. Acuan nilai jitter

Kategori Jitter	Besar Jitter
Sangat Bagus	0 ms
Bagus	0 sd 75 ms
Jelek	75 sd 125 ms
Sangat Jelek	125 ms sd 225 ms

Dari hasil pengujain delay maka didapatkan hasil rata rata delay sebagai berikut.



Gambar 9. Grafik Pengujian Jitter

Grafik diatas menunjukan bahwa dengan menggunakan protokol ospf versi 3 (OSPFv3) dapat disimpulkan bahwa jitter dari selisih delay yang dikirim antar client sebanyak 5 kali dinyatakan rata rata 0-1 ms yang berarti sangat bagus.

Pengujian Throughput

Throughput adalah kecepatan (rate) transfer data efektif, yang diukur dalam bps. Troughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. Throughput dapat dihitung dengan rumus :

$$\textbf{Throughput} = \frac{\textbf{Paket Yang Diterima}}{\textbf{Lama Pengamatan}}$$

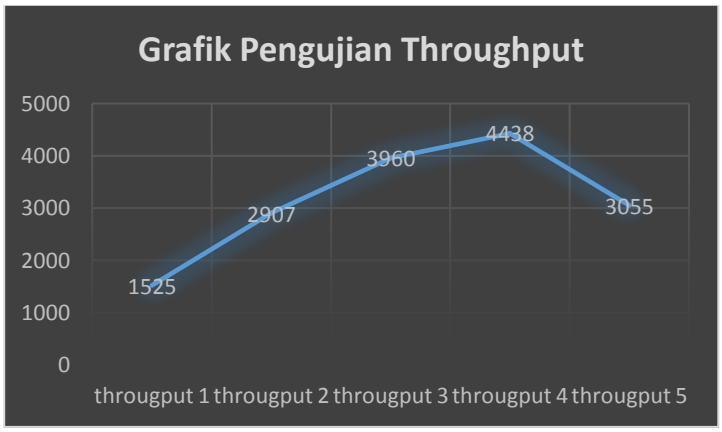
Pada pengujian pertama didapatkan jumlah paket yang diterima sebanyak 28870 dengan rentang waktu pengiriman 36,9 detik. Maka didapat nilai Throughputnya adalah 1525 k. perhatikan gambar dibawah ini.

Statistics

Measurement	Captured	Displayed	Marked
Packets	28870	28870 (100.0%)	–
Time span, s	36.973	36.973	–
Average pps	780.9	780.9	–
Average packet size, B	1954	1954	–
Bytes	56419596	56419596 (100.0%)	0
Average bytes/s	1525 k	1525 k	–
Average bits/s	12 M	12 M	–

Gambar 10. Rekam Pengiriman Data

Berdasarkan hasil rekam pengiriman data menggunakan wireshark maka total paket yang dikirim sebanyak 28.870 dengan lama pengamatan selama 36,973 detik. Dari data tersebut maka nilai pengiriman pertama didapat sebesar 1525 kilo byte / second. Nilai Throughput yang didapat dari pengujian sebanyak 5 kali adalah sebagai berikut :



Gambar 11. Grafik Pengujian Throughput

Pengujian Packet Loss

Packet loss adalah jumlah paket data yang hilang per detik. Packet loss dapat disebabkan oleh sejumlah faktor, mencakup penurunan signal dalam media jaringan, melebihi batas saturasi jaringan, paket yang corrupt yang menolak untuk transit, dan kesalahan perangkat keras jaringan. Packet loss dapat dihitung dengan rumus :

$$\textbf{Packet Loss} = \frac{\textbf{Paket dikirim – Paket diterima}}{\textbf{Paket Yang dikirim}}$$

Untuk mendapatkan ucuan nilai yang baik maka dapat dilihat dengan acuan tabel dibawah ini

Tabel 3. Pengujian Packet Loss

Kategori Packet Loss	Packet Loss
Sangat Bagus	0 %
Bagus	3 %
Jelek	15 %
Sangat Jelek	25 %

Gambar 12. Rekam Pengiriman Data Throughput

Pada pengujian diatas dapat dilihat data yang dikirim (capture) 28870 sedangkan data yang diterima (displayed) 28870. Ini menandakan bahwa data yang dikirim 100 % tidak mengalami kehilangan dengan kata lain sangat bagus.

IV. KESIMPULAN

Dari hasil pengujian implementasi Routing Dinamis OSPFV3 Pada Internet Protocol Versi 6 (IPV6) Menggunakan Router Mikrotik dengan mengirimkan file sebesar 60 mbps dari satu komputer kekomputer lain maka sebanyak lima kali didapatkan hasil sebagai berikut. delay dari lima kali pengujian dengan masing2 pengujian didapatkan kurang lebih 13.000 traffick data maka didapatkan rata rata delai sebesar 0,716 ms yang menunjukan hasil yang sangat bagus. Sedangkan untuk jitter dari lima kali pengujian didapatkan rata rata sebesar 0.002 ms yang menunjukan hasil yang

sangat bagus. Kemudian untuk nilai packet loss dari pengujian yang sama pun didapatkan hasil sebesar 0% yang nunjukan bahwa tidak adanya paket yang hilang ketika pengiriman. Yang terakhir adalah throughput yang didapatkan dengan hasil 1525 k yang beratri jumlah paket yang diterima sesuai dengan lama pengamatan.

REFERENSI

[1] M. Yusril, H. Setiawan, and C. Prianto, "Simulasi Interoperabilitas Sistem Pengalamatan IPv4 dan IPv6 Pada Perangkat -Perangkat Jaringan Komputer," pp. 331–336, 2019.

[2] A. Tantoni, M. T. A. Zaen, and S. Fadli, "ANALISIS KOMPARASI PERFORMA JARINGAN KOMPUTER PADA IMPLEMENTASI IPv4 dan IPv6," *J. Inform. dan Rekayasa Elektron.*, vol. 1, no. 2, p. 55, 2018.

[3] A. P. Munggaran, R. Munadi, and D. Perdana, "Analisis Dan Simulasi Perbandingan Qos Di Routing Protokol Mpls Ospf Dan Mpls Is-Is Di Jaringan Ipv6 Menggunakan Gns3 Untuk Layanan Video," vol. 5, no. 3, pp. 4374–4384, 2018.

[4] Lukman, evriyana indra Saputra, H. Pambudi, dian noviardi Saputra, and arik andrian Putra, "Analisis Waktu Konvergensi Routing Protokol Eigrp Dan Ospf," vol. XIV, pp. 25–33, 2019.

[5] I. D. Rahmawati, A. Shaleh, I. Winarno, M. Politeknik, E. Negeri, and J. T. Telekomunikasi, "Analisa QoS Pada Jaringan MPLS Ipv6 Berbasis Routing OSPF," pp. 1–7, 2011.

[6] S. Wardoyo, T. Ryadi, and R. Fahrizal, "Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni dan Tunneling 6to4 Berbasis Router Mikrotik," *J. Nas. Tek. Elektro*, vol. 3, no. 2, p. 106, 2014.

[7] F. U. Hasanah, N. Mubarakah, K. K. Lan, T. Ring, R. D. Rip, and C. P. Tracer, "Analisis Kinerja Routing Dinamis Dengan Teknik Rip (Routing Information Protocol) Pada Topologi Ring Dalam Jaringan Lan (Local Area Network) Menggunakan Cisco Packet Tracer," *Singuda ENSIKOM*, vol. 7, no. 3, pp. 118–124, 2014.

[8] F. A. Afrida and S. Rahmatia, "Analisis Internet Group Management Protocol (IGMP) Menggunakan Software Wireshark dalam Layanan Live Streaming IPTV pada Multi Service Access Network (MSAN) di Area Darmo, Surabaya," vol. 4, no. 4, pp. 176–181, 2018.

[9] D. M. Khairina, "Analisis Keamanan Sistem Login," *J. Inform. Mulawarman*, vol. 6, no. 2, pp. 64–67, 2011.

[10] I. Iskandar and A. Hidayat, "Analisa Quality of Service (QoS) Jaringan Internet Kampus (Studi Kasus: UIN Suska Riau)," *J. CoreIT*, vol. 1, no. 2, pp. 67–76, 2015.

[11] R. Wulandari, "ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON – LIPI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 162–172, 2016.

[12] M. Kamal, rd rohman Saedudin, and A. Almaarif, "Perancangan Sistem Keamanan Fisik Pada Data Center CV Media Smart Menggunakan Metode NDLC Dengan Berdasarkan Standar TIA-942 Design of Physical Security System in Data Center CV Media SMART Using NDLC Method by Based on Standard," vol. 6, no. 1, pp. 1964–1972, 2019.