UNIVERSITAS INDONESIA

ANALISA UNJUK KERJA ROUTING PROTOCOL RIPng DAN OSPFv3 PADA JARINGAN IPv6

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

MUHAMMAD SYAFRUDIN

0606042784

FAKULTAS TEKNIK

DEPARTEMEN TEKNIK ELEKTRO

Depok

Juni 2010

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	: Muhammad Syafrudin
NPM	:0606042784
Tanda Tangan	:
Tanggal	: 15 Juni 2010

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama	: Muhammad Syafrudin
NPM	: 0606042784
Jurusan	: Teknik Elektro
Judul Skripsi	: Analisa unjuk kerja *routing protocol* RIPng dan OSPFv3 pada jaringan IPv6

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro Fakultas Teknik, Universitas Indonesia

Dewan Penguji

Pembimbing	: Prof. Dr. Ir. Nji Raden Poespawati, MT	( )
Penguji	: Aji Nur Widyanto ST, MT	( )
Penguji	: Budi Sudiarto ST,MT	( )

Ditetapkan di : Depok

Tanggal : 8 Juli 2010

UCAPAN TERIMA KASIH

Puji syukur kepada Allah SWT atas segala berkat dan rahmatNya sehingga penulis dapat menyelesaikan skripsi ini. Dalam kesempatan ini, penulis ingin mengucapkan terima kasih kepada ibu:

Prof. Dr. Ir. Nji Raden Poespawati, MT

Selaku pembimbing, yang telah bersedia meluangkan waktunya untuk memberikan bimbingan, pengarahan, saran-saran dan kemudahan lainnya sehingga skripsi ini dapat diselesaikan dengan baik.

Depok, 28 Juni 2010

Muhammad Syafrudin

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia. Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Syafrudin
NPM	: 0606042784
Departemen	: Teknik Elektro
Fakultas	: Teknik
Jenis Karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif** (**Non-exclucive Royalty-Free Right**) atas karya ilmiah saya yang berjudul:

ANALISA UNJUK KERJA ROUTING PROTOCOL

RIPng DAN OSPFv3 PADA JARINGAN IPv6

Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mnegalihmedia/ formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir Saya selama tetap mencantumkan nama Saya sebagai penulis/ pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada Tanggal : 12 Juli 2010

Yang menyatakan

(Muhammad Syafrudin)

ABSTRAK

Nama : Muhammad Syafrudin

Jurusan : Teknik Elektro

Judul : Analisa unjuk kerja *routing protocol* RIPng dan OSPFv3 pada jaringan IPv6

Tujuan utama pengembangan IPv6 adalah untuk memenuhi kebutuhan alamat IP untuk jangka panjang sekaligus menyempurnakan berbagai kelemahan yang ada pada IPv4. Dengan hadirnya IPv6 maka dibutuhkan *routing protocol* yang mendukung jaringan IPv6 diantara RIPng dan OSPFv3. *Routing protocol* berfungsi untuk menghubungkan antar jaringan, dan memilih jalur atau rute untuk mencapai jaringan yang lain.

Skripsi ini disusun untuk mengetahui kinerja dari *routing protocol* pada jaringan IPv6 yaitu RIPng dan OSPFv3. Pengujian dilakukan dengan analisa proses pemilihan jalur pada routing table, analisa paket *header*, dan pengujian dengan melakukan pengiriman paket pada masing-masing *routing protocol*. Metode yang digunakan adalah studi literatur, simulasi pada komputer, dan implementasi pada jaringan *test-bed*.

Analisa data menunjukan bahwa secara umum kinerja RIPng dan OSPFv3 tidak jauh berbeda dengan *routing protocol* pendahulunya, yaitu RIP dan OSPF pada jaringan IPv4, perbedaan mendasar adalah dukungan terhadap pengalamatan 128-bit. Pada pengujian didapatkan kinerja OSPFv3 lebih baik karena kecepatannya dalam melakukan konvergen pada jaringan ketika terjadi *link down* dibutuhkan waktu sebesar 4,542 detik, jaluh lebih cepat daripada RIPng yang membutuhkan waktu 60,566 detik. Hasil pengujian *throughput* dengan *window size* paket TCP berukuran 2, 4, 8, 16, 32 Kbyte didapatkan nilai rata-rata 92,8 Mbits/detik untuk *routing protocol* RIPng, dan pada OSPFv3 didapatkan nilai rata-rata *throughput* 85,3Mbits/detik untuk *windows size* 2, 4, 8 Kbyte dan 92,9Mbits/detik untuk *window size* berukuran 16 dan 32 Kbyte. Pada pengujian jitter dengan paket UDP pada jaringan IPv6, didapat besar jitter dengan *routing protocol* RIPng rata-rata 1,196 ms dan dengan dengan OSPFv3 rata-rata sebesar 1,106 ms.

Kata kunci :

IPv6, RIPng, OSPFv3.

ABSTRACT

Name : Muhammad Syafrudin

Study Program: Electrical Engineering

Title : Peformance analysis of RIPng dan OSPFv3 routing protocols on IPv6 network.

The main objective of the development of IPv6 (Internet Protocol Version 6) is to meet needs of IP addresses for the long term and improving the existing weaknesses in IPv4. With the presence of IPv6, also needed routing protocol that support IPv6 such as RIPng and OSPFv3. A routing protocol is a protocol that specifies how router communicate each other, select path or routes, and connect other network.

This paper is arranged to determine the performance of RIPng dan OSPFv3 routing protocols. For the testing is done by analyzing the patch selection process in the routing table, packet header analysis, and testing by sending a packet. The method used is literature study, computer simulation, and implementation on the test-bed.

Data analysis showed that the overall performance of RIPng and OSPFv3 are not much different from its predecessor routing protocol, RIP and OSPF on an IPv4 network, the fundamental difference is the support of 128-bit addressing. OSPFv3 on test performance showed better because the speed of convergence on the network do when it happens the link down it takes by 4.542 seconds, faster than the RIPng which took 60.566 seconds.

Keyword :

IPv6, RIPng, OSPFv3

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Dengan semakin berkembangnya penggunaan internet maka berkembang juga kebutuhan akan IP (*internet protocol*). Namun pertambahan pengguna IP tidak diimbangi dengan jumlah IPv4 (*Internet Protocol Version 4*) yang ada. Dengan demikian IETF (*Internet Engineering Task Force*) menetapkan standar pengalamatan baru yang disebut IPv6 (*Internet Protocol Version 6*), tujuan utama pengembangan IPv6 adalah untuk memenuhi kebutuhan alamat IP untuk jangka panjang sekaligus menyempurnakan berbagai kelemahan yang ada pada IPv4.

Dengan hadirnya IPv6, maka diperlukan pula protokol-protokol pendukung yang dapat berjalan di IPv6 salah satu diantaranya ialah *routing protocol*. *Routing protocol* diperlukan untuk menentukan atau pemilihan jalur untuk sebuah paket agar dapat sampai ke tujuan yang ditentukan. Kondisi *cloud* jaringan yang kompleks membuat banyak kemungkinan jalur yang mungkin dilalui oleh paket untuk mencapai tujuan, dan untuk memilih jalur yang terbaik yang dapat dilalui perlu digunakan *dynamic routing*. Sebuah *dynamic routing* dibangun dari informasi yang dikumpulkan oleh *routing protocol*. *Routing protocol* yang sebelumnya tersedia pada teknologi IPv4 disempurnakan dan disesuaikan dengan lingkungan IPv6. Beberapa *routing protocol dynamic* yang dibuat guna mendukung IPv6 antara lain: RIPng, OSPFv3, IS-IS for IPv6, BGP IPv6, dan lainnya. Pada skripsi ini dilakukan pengujian hanya pada RIPng dan OSPFv3, dimana sebelumnya kedua *routing protocol* pendahulunya, yaitu RIP dan OSPF pada IPv4 merupakan *routing protocol* yang populer dan banyak digunakan.

1.2. TUJUAN

Penulisan skripsi ini bertujuan untuk menganalisa dan mengetahui cara kerja dari *routing protocol* RIPng dan OSPFv3 pada IPv6, dengan pembanding RIP dan OSPF pada IPv4. Dan untuk menguji dan menganalisa unjuk kerja dari *routing protocol* RIPng dan OSPFv3 dengan parameter waktu konvergen, *throughput*, dan *jitter*.

1.3. PEMBATASAN MASALAH

Permasalahan yang dibahas pada skripsi ini dibatasi pada pengujian dan perbandingan dari dua buah dynamic *routing protocol* RIPng dan OSPFv3 yang diuji pada protokol IPv6. Parameter-parameter yang diperhatikan adalah konfigurasinya pada router, proses pemilihan jalur pada *routing table*, analisa paket header dan pengujian dengan pengiriman paket dasar guna melihat performa dari masing-masing *routing protocol*.

1.4. METODOLOGI PENELITIAN

Penelitian dilakukan dengan tiga tahap, yaitu studi literatur, simulasi pada PC, dan pengujian pada *test-bed* lokal. Pada pengujian dilakukan simulasi dengan perangkat lunak pada PC, yaitu dengan program Cisco Packet Tracer. Pengujian pada *test-bed* dilakukan dengan tiga buah router Mikrotik berbasis Linux yang topologinya dibuat menyerupai jaringan lokal sederhana yang dibuat sedemikian rupa agar dapat mewakili kelebihan dari masing-masing *routing protocol* yang akan diuji.

1.5. SISTEMATIKA PENULISAN

Sistematika penulisan laporan skripsi ini meliputi Bab I: Pendahuluan, yang berisi mengenai latar belakang, tujuan dan pembatasan masalah, metodologi penelitian dan sistematika penulisan. Pada bab II: Perancangan jaringan dan *routing protocol*, dibahas mengenai teknologi IPv6, teori *routing protocol* dan teori jaringan secara umum. Di bab III: konfigurasi jaringan dan metode pengujian, ditulis mengenai topologi yang dipilih, perangkat keras dan perangkat lunak yang digunakan, dan teknik pengujian. Pada bab IV: Analisa, yaitu hasil dari pengujian dan analisa kerja dari kedua *routing protocol* yang diuji, baik pengujian dengan simulasi *software* maupun pengujian pada jaringan *test-bed*. Bab V: kesimpulan, berisi kesimpulan yang didapat dari hasil pengujian dan analisa jaringan.

BAB II

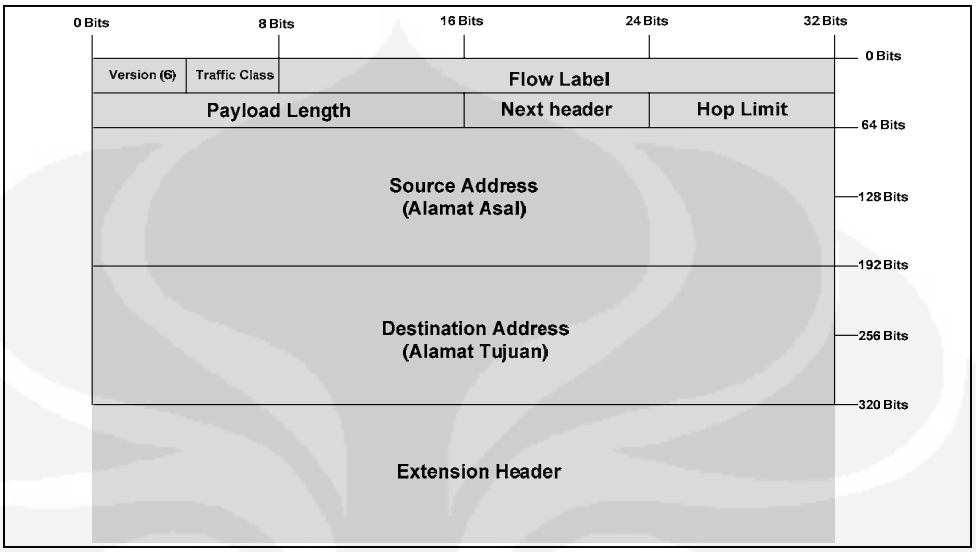
ROUTING PROTOCOL PADA IPv6

2.1. IPv6

IPv6 dikembangkan oleh IETF untuk dapat memenuhi kebutuhan IP yang diperlukan, selain itu IPv6 juga dikembangkan untuk mengatasi atau menyempurnakan kekurangan-kekurangan dari teknologi pendahulunya, yaitu IPv4. Kelebihan utama dari IPv6 adalah pengalamatannya yang luas, yaitu 128-bit. Dengan demikian ada 2^{128} atau sekitar 3,4 x 10^{38} alamat IPv6 yang berlimpah tersedia, sehingga dapat memenuhi kebutuhan IP saat ini maupun di masa mendatang. IPv6 ini dapat mengatasi masalah pada NAT (*Network Address Translation*) yang mengurangi atau menghalangi penggunaan dari aplikasi *realtime* yang membutuhkan hubungan dua arah. Pada IPv6 mendukung hirarki pengalamatan dan jumlah pengalamatan *node* yang lebih banyak, sehingga konfigurasi alamat lebih sederhana. Kelebihan dari IPv6 yang lain ialah kapabilitas untuk QOS (*Quality Of Service*), autentifikasi, dan privasi. Untuk QOS dimungkinkan untuk pemberian label pada paket-paket pada aliran trafik tertentu yang membutuhkan penanganan khusus, untuk autentifikasi dan privasi IPv6 mendukung autentifikasi, integritas data, dan kerahasiaan data.

2.1.1. Format Header IPv6

Pada IPv6 digunakan header paket yang sederhana, dan dengan header yang sederhana paket dapat diproses secara lebih efisien. Header pada IPv6 merupakan penyederhanaan dari header IPv4 dengan menghilangkan bagian yang tidak dipergunakan atau jarang digunakan dan menambahkan bagian yang menyediakan dukungan yang lebih baik untuk keperluan mendatang. Pada Gambar 2.1 dian format header pada IPv6.



Gambar 2.1 : Header pada IPv6 [1]

Berikut penjelasan dari format header pada IPv6 :

- **Version** → Versi IP, enam untuk IPv6 (4-bit).
- **Traffic Class** → Klasifikasi trafik, *field* ini menentukan prioritas trafik atau paket dan digunakan untuk QOS (*quality of service*) (8-bit).
- **Flow Label** → Label aliran dari trafik (20-bit).
- **Payload Length** → *Field* ini merupakan panjang dari paket data (16-bit).
- **Next Header** → Identifikasi tipe header setelah header IPv6 (8-bit).
- **Hop Limit** → Nilai akan dikurangi satu, jika melewati sebuah router (*node*) .
- **Source/ Destination Address** → Alamat dari sumber dan tujuan.
- **Extension Header** → Sebagai informasi tambahan, yang ditempatkan diantara header IPv6 dengan header yang lebih tinggi diatasnya.

2.1.2. Pengalamatan pada IPv6

Pada IPv6 alamat ditulis dalam format hexadesimal dengan pemisah berupa titik dua diantara masing-masing 16-bit. Format penulisan alamat IPv6 adalah x : x : x : x : x : x : x : x dimana x adalah empat *digit* bilangan heksadesimal. Ada beberapa aturan dalam penulisan atau meringkas alamat IPv6, sebagai contoh untuk alamat **2033:0000:140E:0000:0000:09D0:683A:140A**, ada beberapa yang dapat disederhanakan, dengan cara sebagai berikut :

- Angka nol (0) di awal adalah *optional*. Sebagai contoh pada 09DO disederhanakan menjadi 9D0, dan 0000 dapat disederhanakan menjadi 0, sehingga 2033:**0000**:140E:0000:0000:**09D0**:683A:140A dapat ditulis menjadi 2033:**0**:140E:0000:0000:**9D0**:683A:140A.
- Angka nol yang berurutan dapat disederhanakan dengan dua tanda titik dua "::". Namun penyederhanaan ini hanya dapat digunakan satu kali dalam sebuah alamat. Sebagai contoh 2033:0:140E:**0000**:**0000**:9D0:683A:140A, dapat ditulis menjadi 2033:0:140E**::**9D0:683A:140A.

Arsitektur pengalamatan pada IPv6 dibagi tiga, yaitu [2] :

- *Unicast Address*

  Unicast address adalah alamat yang menunjuk pada sebuah alamat antarmuka atau *host*. Pada alamat *unicast* dibagi menjadi menjadi 3, yaitu : alamat *link local* alamat yang digunakan dalam satu link jaringan, alamat *site local* setara dengan alamat *private* pada IPv4, dan alamat *global*, yaitu alamat *public* yang digunakan oleh ISP (*Internet Service Provider*).

- *Multicast Address*

  Multicast address adalah alamat yang menunjukan beberapa *interface* (biasanya untuk *node* yang bebeda). Paket yang dikirimkan ke alamat ini akan dikirimkan ke semua *interface* yang dian oleh alamat ini. Alamat *multicast* didesain untuk menggantikan alamat *broadcast* pada IPv4.

- *Anycast Address*

  Anycast address adalah alamat yang menunjukkan beberapa interface (biasanya untuk *node* yang bebeda). Paket yang dikirimkan ke alamat ini akan dikirimkan ke salah satu alamat *interface* yang paling dekat dengan router.

2.2. ROUTING PROTOCOL

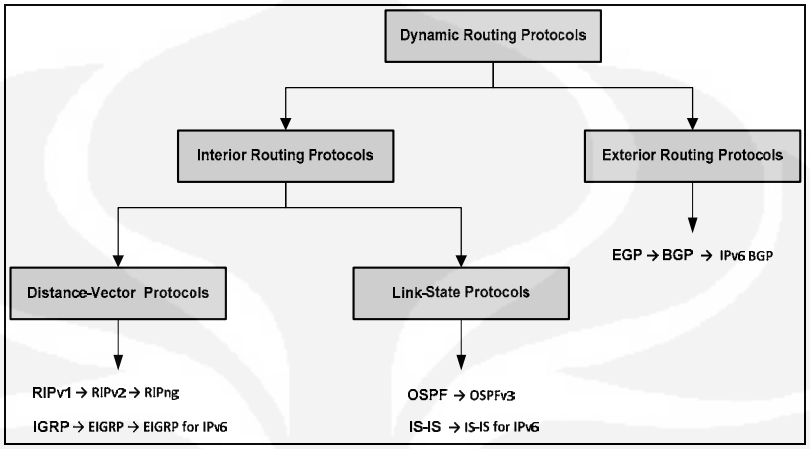
Routing adalah suatu protokol yang digunakan untuk mendapatkan rute atau petunjuk dari satu jaringan ke jaringan yang lain, *routing* merupakan proses dimana suatu router akan memilih jalur atau rute untuk mengirimkan atau meneruskan suatu paket ke jaringan yang dituju. Router menggunakan IP address 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 protocol digunakan untuk memfasilitasi pertukaran informasi *routing* antar router. Dengan *routing protocol*, router dapat berbagi informasi *routing table,* yaitu informasi mengenai jaringan lain yang saling terhubung. Ada beberapa *routing protocol* yang mendukung IPv6, yaitu RIPng, OSPFv3 EIGRP for IPv6 (Cisco *properiarity),* IS-IS for IPv6, BGP IPv6, dan lainnya. Masing-masing dibuat berdasarkan *routing protocol* sebelumnya yang mendukung IPv4 namun disesuaikan dengan lingkup IPv6 dan memiliki beberapa kelebihan dan pembaharuan serta cara konfigurasi yang berbeda pada router.

2.2.1. Klasifikasi protokol *dynamic routing*

Pada protokol *routing* kelas *Interior Gateway Protocols* (IGPs) *dynamic routing* diklasifikasi menjadi dua, yaitu *distance vector routing* dan *link-state routing*. Untuk klasifikasi *dynamic routing protocol* secara keseluruhan terlihat

seperti pada Gambar 2.2. Pembagian pada *dynamic routing protocol* dibedakan berdasarkan karakteristik dan cara kerjanya masing-masing.



Gambar 2.2 : Klasifikasi *dynamic routing protocol* [3]

2.2.1.1. Distance vector routing

Router yang menggunakan jarak dan arah sebagai acuan *routing* dinamakan *distance vector routing*. Pada *distance-vector routing protocol* digunakan algoritma *Bellman-Ford* dalam kalkulasi untuk pemilihan jalur. Informasi atau *update table* pada *distance-vector routing protocol* dilakukan secara berkala oleh router, berbeda dengan link-state yang melakukan *update table* setiap ada perubahan pada topologi jaringan, sehingga pada *distance-vector routing protocol* membutuhkan proses komputasi yang lebih sederhana. Contoh *routing protocol* yang menggunakan *distance-vector routing protocol* adalah RIPv1, RIPv2, dan IGRP.

Seperti namanya, maka pada *distance-vector routing protocol* menggunakan jarak dan arah untuk melakukan *routing*. Jarak yang dimaksud adalah *hop count* atau jumlah router yang dilalui, dan untuk arah yang dimaksud adalah alamat *next hop* atau *interface* keluar yang digunakan oleh router.

Pembaharuan atau *Update* dilakukan secara berkala pada *distance-vector routing protocol* dimana *update routing table* dikirimkan ke semua router yang bersebelahan secara langsung yang dikonfigurasi dengan *distance-vector routing protocol* yang sama.

2.2.1.2. Link-state routing protocol

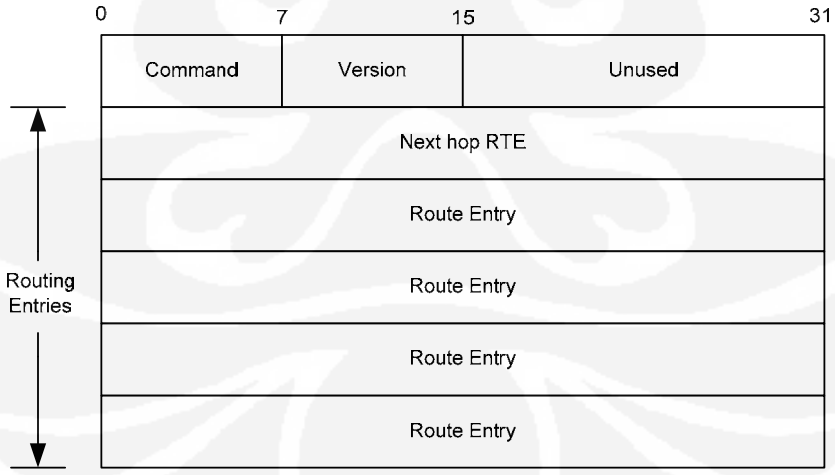
Link-state routing protocol dibangun dengan algoritma Edsger Dijkstra's atau kadang disebut algoritma *shortest path first* (SPF). Algoritma ini menjumlahkan total *cost* yang dibutuhkan pada masing-masing jalur dari alamat asal ke alamat tujuan. *Link-state routing protocol* membangun suatu topologi jaringan, dimana masing-masing router yang terhubung menggunakan gambaran topologi tersebut untuk menentukan jalur atau rute untuk menjangkau jaringan yang ingin dicapai. Router dengan *link-state* akan mengirimkan kondisi dari *link*nya ke router-router lain yang berada dalam *routing domain* yang sama. Informasi atau kondisi *link* yang disebarkan adalah kondisi link pada router yang terhubung langsung suatu jaringan dan kondisi *link* pada router yang saling terhubung. Router dengan *link-state routing protocols* menggunakan *Hello protocol* untuk mengetahui *link-link* yang terhubung dengan router tetangga atau router yang terhubung langsung.

Pada *link-state routing protocol* ada beberapa kelebihan bila dibandingkan dengan *distance-vector routing protocol*, seperti membangun peta topologi jaringan, sehingga masing-masing router dapat menentukan sendiri jalur yang pendek untuk mencapai jaringan yang lain. Konvergensi jaringan terjadi dengan cepat, karena ketika router menerima paket LSP langsung disebar ke router tetangganya yang lain dalam jaringan. *Update* atau pembaharuan informasi dilakukan saat terjadi perubahan pada *link* secara langsung. Disain secara hirarki, dimana *link-state routing protocols* menggunakan konsep area, dan area-area disusun secara hirarki, sehingga *routing* lebih baik. Namun *link-state routing protocol* juga memiliki kekurangan, dimana *routing protocol* ini membutuhkan kinerja *CPU*, *memory*, dan *bandwith* yang lebih besar.

2.2.2. RIPng

RIP merupakan *routing protocol distance-vector* yang masuk pada kelas *Interior Gateway Protocol* yang dikembangkan oleh IETF. *Routing protocol* ini menggunakan algoritma Bellman-Ford dalam penentuan jalur *routing*. RIP digunakan pada jaringan dengan ukuran kecil, dimana untuk implementasi dan konfigurasinya yang sederhana dan mudah. RIPng menggunakan protokol UDP pada port 521 untuk melakukan transportasi baik dalam pengiriman atau penerimaan datagram. RIPng termasuk dalam *routing protocol distance vector* yang menggunakan *hop count* dalam menentukan rute ke tujuan.

Pada dasarnya cara kerja dari RIPng sama dengan RIP, karena RIPng dibuat berdasarkan *routing protocol* RIP yang digunakan pada IPv4. Namun salah satu perbedaan yang mendasar ialah dukungan pada pengalamatan IPv6. RIP menggunakan *hop count* dalam memperhitungan jarak ke alamat tujuan. *Hop count* sebuah router menuju jaringan yang terhubung langsung adalah bernilai 0, *hop count* dari sebuah router yang terhubung langsung dengan sebuah router adalah bernilai 1. Pada Gambar 2.3 menunjukan gambar paket *header* pada *routing protocol* RIPng.



Gambar 2.3 : Paket header RIPng [4]

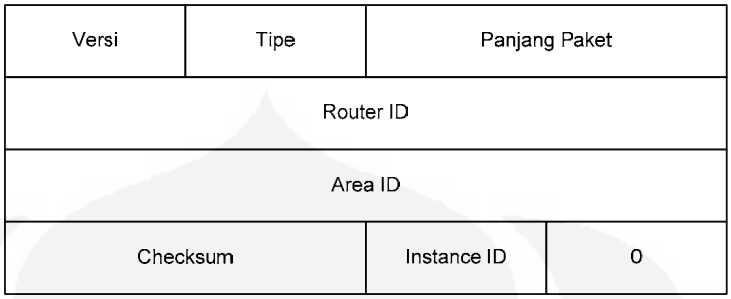
Cara kerja *routing protocol* RIP :

- Setelah RIP di-*enable* router akan mengirimkan permintaan atau *request* ke router tetangga, dan menerima *request* atau respon balik dari router tetangga.
- Ketika respon balik diterima, router akan menerima informasi yang dikirim dan akan melakukan *update* terhadap *routing table* lokal.
- Setiap router dengan *routing protocol* RIP akan melakukan hal yang sama agar tetap memiliki informasi routing yang terbaru.

Kekurangan dari *routing protocol* ini adalah terbatasannya jumlah lompatan (*hop*) yang dapat dijangkau, dimana hop maksimal yang bisa dijangkau adalah 15 *hop*.

2.2.3. OSPFv3

Open Shortest Path First (OSPF) adalah *routing protocol* kelas *link-state* yang dikembangkan untuk memperbaiki kinerja dari *routing protocol* RIP. OSPF adalah *routing protocol* 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 (*designated routers*) dan BDR (*Backup DRs*). OSPFv3 menggunakan alamat *link-localnya* untuk malakukan *advertisements* bukan alamat globalnya. Paket header OSPFv3 adalah sebesar 16-byte, berbeda dengan OSPFv2 sebesar 24-byte. Paket header OSPFv3 terlihat seperti pada Gambar 2.4.



Gambar 2.4 : Paket header OSPFv3 [5]

Dari Gambar 2.4 terlihat pada paket header OSPFv3 tidak ada autentikasi. Pada IPv6 kemampuan dalam autentikasi dan enkripsi menggunakan header *extension*. Pada OSPF terdapat beberapa paket LSP (Link-State Packets), masing-masing paket dibutuhkan dalam proses routing pada OSPF. Berikut paket-paket LSP pada OSPF [6] :

1. **Hello** – Paket Hello digunakan untuk memulai dan menjaga keterhubungan informasi dengan router OSPF yang lain.
2. **DBD** (Paket Database Description) – DBD untuk memeriksa dan melakukan sinkronisasi *database* antar router.
3. **LSR** (Link-State Request) – LSR digunakan untuk menarik informasi dari router lain.
4. **LSU** (Link-State Update) – Paket ini digunakan untuk menjawab LSR
5. **LSAck** (Link-State Acknowledgment) – LSAck digunakan untuk mengkonfirmasi paket LSU yang diterima oleh router.

Masing-masing router OSPF menjaga *database* LSA yang diterima dari router lain. Ketika LSA dari semua router telah diterima maka router akan membangun sebuah *local link-state database*. OSPF menggunakan algoritma Dijkstra's *shortest path first* (SPF) untuk membangun sebuah SPF *tree*. SPF *tree* ini yang kemudian digunakan untuk membangun sebuah *routing table* dengan jalur terbaik guna mencapai jaringan yang lain.

Berikut merupakan proses terjadinya konvergensi pada *link-state routing protocols* :

1. Masing-masing router mempelajari koneksinya yang terhubung ke jaringan secara langsung.
2. Tiap router bertanggung jawab untuk "*Hello*" ke router tetangga yang terhubung langsung.
3. Router membangun *Link-State Packet* (LSP) yang berisi mengenai informasi *link* yang terhubung langsung.
4. Masing-masing router akan mengirimkan LSP kesemua tetangganya, yang kemudian disimpan pada *database.*
5. Tiap router menggunakan *database*nya untuk membangun sebuah peta topologi lengkap dari jaringan dan gambaran jalur atau rute yang dapat digunakan untuk mencapai jaringan tujuan yang ingin dicapai.

Administrative distance (AD) digunakan untuk mengukur realibilitas informasi *routing* yang diterima oleh sebuah router dari router tetangganya. Nilai AD berkisar pada bilangan bulat antara 0 sampai 255, dimana 0 menunjukkan kemampuan penerusan data yang tertinggi dan 255 menunjukan tidak ada data yang akan diteruskan melewati sebuah rute. Secara *default* OSPF memiliki AD bernilai 110. *Metric* yang digunakan pada *routing protocol* OSPF dinamakan *cost*, semakin kecil nilai *cost*, maka akan dipilih menjadi *interface* untuk mengirimkan data. Pada RFC 2328 tidak dijelaskan mengenai nilai acuan untuk *cost*,

> *RFC 2328 : "A cost is associated with the output side of each router interface. This cost is configurable by the system administrator. The lower the cost, the more likely the interface is to be used to forward data traffic."*[7]

Namun pada Cisco IOS akumulasi *bandwith* dari *interface* yang digunakan router untuk mencapai tujuan dijadikan sebagai acuan nilai *cost*. Pada setiap router nilai cost dari *interfacenya* dihitung dari 10 pangkat 8 dibagi dengan nilai

*bandwidth*nya (bps) [8]. Pada Tabel 2.1 terlihat perbandingan nilai *cost* yang dihitung dari besarnya *bandwidth*.

Jenis Interface	Cost (10^8/ bps)
Fast Ethernet	10^8/ 100.000.000 bps = 1
Ethernet	10^8/ 10.000.000 bps = 10
E1	10^8/ 2.048.000 bps = 48
T1	10^8/ 1.544.000 bps = 64
128 kbps	10^8/ 128.000 bps = 781
64 kbps	10^8/ 64.000 bps = 1562
56 kbps	10^8/ 56.000 bps = 1785

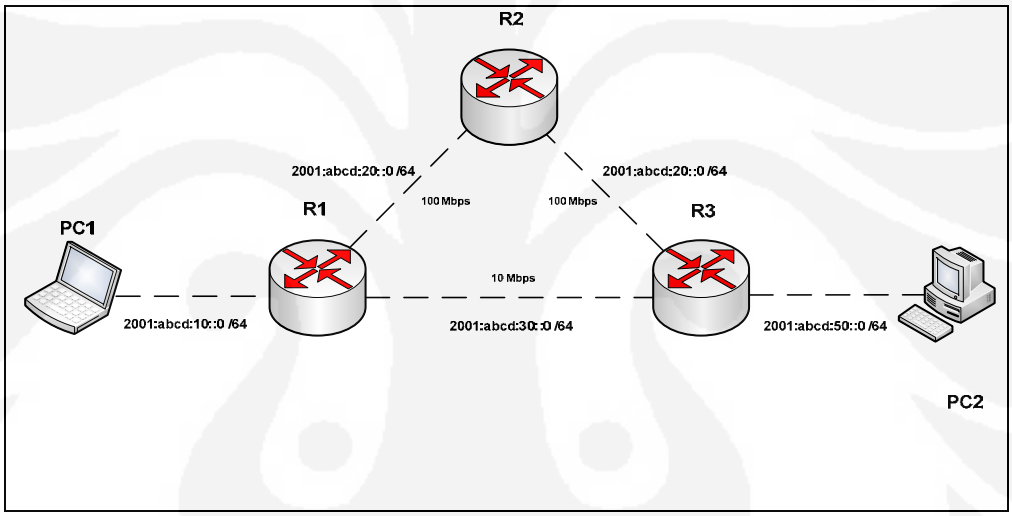
Tabel 2.1. : Nilai cost pada OSPF Cisco. [9]

BAB III

KONFIGURASI JARINGAN DAN METODE PENGUJIAN

3.1. TOPOLOGI JARINGAN

Topologi jaringan yang digunakan pada jaringan *test-bed* untuk pengujian *routing protocol* RIPng dan OSPFv3 menggunakan tiga buah router dan dua buah PC. Topologi tersebut digunakan untuk menguji kedua *routing protocol* pada jaringan IPv6. Topologi ditunjukan pada Gambar 3.1.



Gambar 3.1 : Topologi jaringan

Koneksi antar router dibuat ada perbedaan kecepatan koneksinya, yaitu 100 Mbps untuk hubungan antara router R1-R2 dan R2-R3, dan kecepatan 10 Mbps untuk hubungan antara router R1-R3. Sedangkan untuk sambungan antara PC1 dengan router R1, dan PC2 dengan router R3 menggunakan kecepatan koneksi standar *interface*nya, yaitu 100 Mbps.

3.2. METODE PENGUJIAN

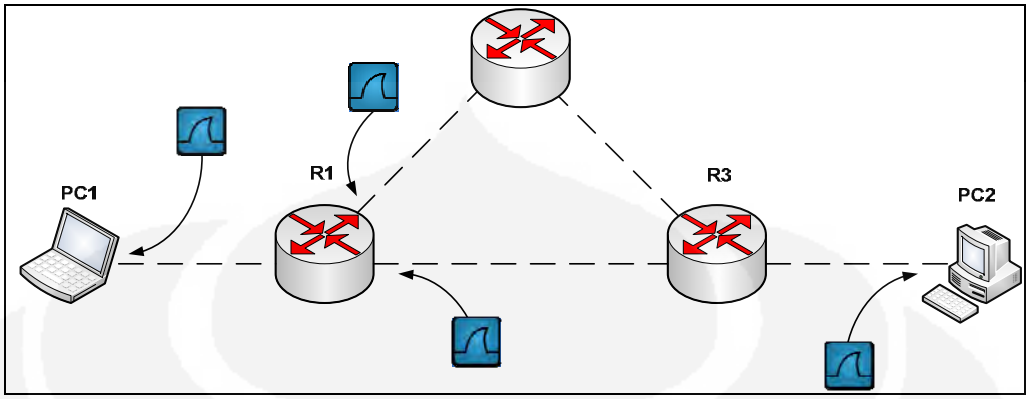
3.2.1. Pengujian Pemilihan jalur oleh *routing protocol*

Routing table menyimpan informasi rute-rute atau jalur untuk mencapai jaringan yang lain, dan *routing table* juga menyimpan *metric* dari rute-rute yang ada. Untuk melihat routing table dari router dapat dilakukan dengan mengetikan perintah "***show ip route"*** untuk router Cisco, atau perintah ***"ipv6 route"*** untuk menampilkan informasi *routing table* IPv6 pada router Mikrotik. Pada masing-masing router dilakukan perintah untuk menampilkan *routing table*-nya baik dalam topologi IPv4 (RIP-OSPF) dan topologi IPv6 (RIPng-OSPFv3).

Perintah "***trace route"*** atau "***tracert"*** digunakan untuk mengetahui jalur yang akan dilalui paket data. Tracert menggunakan protokol ICMP (*Internet Control Messaging Protocol*), protokol ini bekerja dengan mengirimkan ICMP *echo request* ke alamat tujuan. Rute yang dilalui dan ditampilkan adalah daftar *interface* router yang digunakan pada jalur antara *host* dan tujuan. Pada pengujian dilakukan perintah tracert pada PC1 ke PC2, hal ini dilakukan untuk mengetahui jalur atau router mana yang saja yang dilalui oleh paket untuk menuju PC2.

3.2.2. Pengujian *update routing table* dan kecepatan waktu konvergen.

Pada pengujian juga dilakukan *capture* pada paket data. Pada pengujian dilakukan *capture* pada paket data untuk mengetahui paket *header* dari masing-masing *routing protocol*, proses *update routing tabl*e pada *routing protocol*, dan kecepatan masing-masing *routing protocol* dalam melakukan *update table* dan mencapai konvergen. Berikut Gambar 3.2 adalah gambar titik-titik pengujian dengan *capture* paket data pada jaringan.



Gambar 3.2 : Topologi pengujian dengan *capture* paket data.

Pengujian yang dilakukan adalah dengan melakukan pengiriman paket dari PC1 ke PC2 dan sebaliknya, lalu dilakukan *capture* pada paket yang lewat. Untuk jalur R1-R2-R3 dilakukan *capture* paket pada interface R1 yang terhubung dengan router R2, dan untuk jalur R1-R3 dilakukan *capture* pada *interface* R1 yang terhubung ke router R3. Untuk pengujian waktu konvergen dilakukan dengan melakukan pemutusan pada jalur yang aktif pada *routing table*, sehingga *routing table* segera menjadikan jalur alternatif yang terdaftar menjadi jalur aktif. Pada pengujian dilakukan pengambilan data dari jumlah paket yang dikirim, paket yang diterima, paket loss, dan kecepatan konvergen *routing table*.

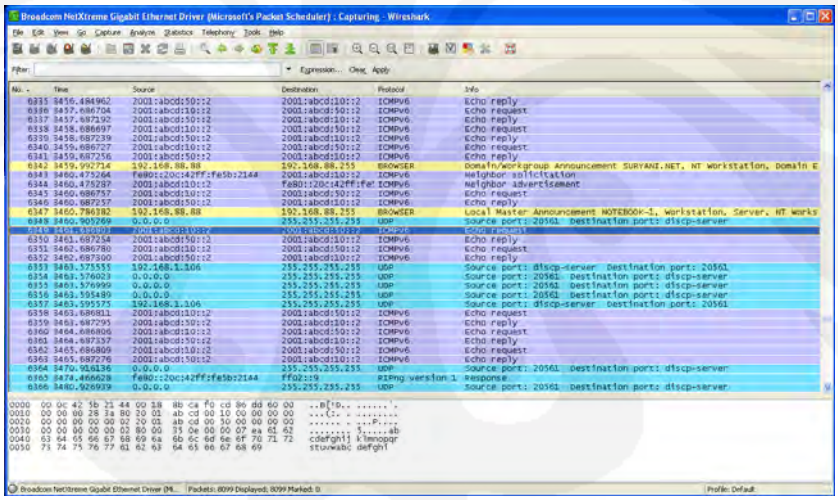
3.2.3. Pengujian performa jaringan dengan paket TCP dan UDP

Pengujian performa dari *routing protocol* dilakukan dengan pengiriman paket TCP dan UDP dari PC *client* ke server. Parameter yang diuji adalah *throughput* jaringan. Untuk pengujian, topologi yang digunakan adalah data dilewatkan pada router R1-R2-R3 untuk masing-masing *routing protocol*. Dalam pengujian dengan data TCP digunakan variasi *window size* pada data yang dikirimkan, yaitu 2, 4, 8, 16, dan 32 Kbyte interval waktu 10-3- detik. Dalam pengujian dengan paket UDP paket dikondisikan pada variasi *bandwith* sebesar 40, 45, 50, 55, 60, 70, dan 80 Mbits/sec.

3.3. PERANGKAT LUNAK PADA JARINGAN

3.3.1. Wireshark

Wireshark adalah suatu perangkat lunak yang digunakan untuk analisa paket pada jaringan, Wireshark yang digunakan pada pengujian adalah versi 1.2.5. Dengan perangkat lunak ini dapat dilakukan analisa, *troubleshooting*, penelitian protokol, dan lainnya. Wireshark mampu menangkap paket-paket data atau informasi yang melewati jaringan. Berbagai format protokol dapat ditangkap dan dianalisa. Perangkat lunak ini bekerja dengan melakukan *capture* atau manangkap paket data melalui interface pada PC yang terhubung pada jaringan. Gambar 3.3 adalah tampilan perangkat lunak wireshark ketika menangkap paket data yang lewat.

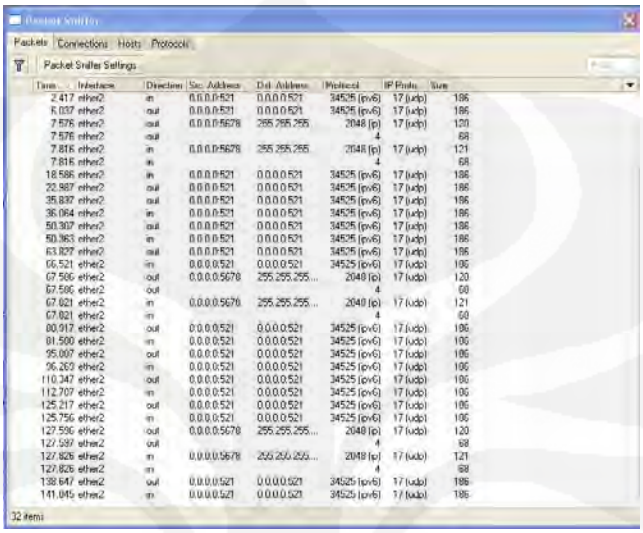


Gambar 3.3 : Tampilan perangkat lunak wireshark

3.3.2. Mikrotik packet sniffer

Untuk melakukan *capture* paket pada *interface* antar router digunakan perangkat lunak **Packet Sniffer** yang tersedia pada router Mikrotik. Tool ini disediakan dalam mikrotik untuk menangkap paket-paket data yang melalui *interface* router pada jaringan (paket yang masuk dan keluar melalui router) . Tool ini berguna untuk analisa pada *traffic* jaringan. Untuk menggunakan *tool* ini cukup dengan mengetikan perintah ***"tool sniffer > start"*** pada terminal Mikrotik

di masing-masing router dan dipilih *interface* apa yang ingin dic*apture*. Gambar 3.4 adalah contoh hasil *capture* dengan tool sniffer pada router Mikrotik.



Gambar 3.4 : Tampilan hasil *capture* paket dengan *tool sniffer* pada Mikrotik.

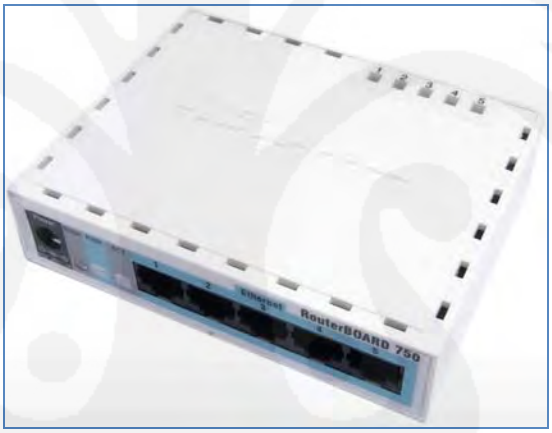
3.3.3. Iperf

Iperf adalah sebuah perangkat lunak yang digunakan untuk menguji jaringan yang dikembangkan oleh "*National Laboratory for Applied Network Research*". Perangkat lunak ini bekerja dengan menghasilkan paket TCP atau UDP yang digunakan untuk mengukur besar *throughput*, atau kualitas transfer pada jaringan, *jitter* dan *packet loss*. Dengan Iperf dibutuhkan 2 buah komputer dalam pengujian, satu komputer sebagai *server* dan satu lagi sebagai *client*. Pada PC server dilakukan perintah iperf –s –V, dimana –s menunjukan sebagai server, -V menunjukan jaringan yang digunakan adalah jaringan IPv6. Dan pada client digunakan perintah iperf –c –V <*no_IP_tujuan*>. Selain itu masih banyak perintah-perintah tambahan lain yang digunakan, termasuk untuk merubah-ubah parameter pengujian seperti interval waktu, ukuran paket, port pengujian, dan lainnya.

3.4. PERANGKAT KERAS PADA JARINGAN

3.4.1. ROUTER MIKROTIK

Pada pengujian dengan test-bed digunakan tiga buah router Mikrotik *router board* RB750. Mikrotik RouterOS merupakan sistem operasi berbasis Linux yang dikembangkan sebagai *operating system* (OS) router yang bekerja pada sebuah PC. Mikrotik *router board* adalah perangkat keras yang dikemas dengan OS Mikrotik RouterOS sehingga dapat berdiri sendiri layaknya sebuah PC dengan RouterOS. Gambar router Mikrotik seri RB750 ditunjukan pada Gambar3.5.



Gambar 3.5 : Router Mikrotik RB750

Berikut spesifikasi *router board* RB750 yang digunakan :

- **CPU** **:** AR7240 300MHz (overclock up to 400MHz) CPU
- **Memory** **:** 32MB DDR SDRAM onboard memory
- **Boot loader** **:** RouterBOOT
- **Data storage** **:** 64MB onboard NAND memory chip
- **Ethernet** **:** Five 10/100 ethernet ports (with switch chip)
- **Extras** **:** Reset switch, Beeper
- **LEDs** **:** Power, NAND activity, 5 Ethernet LEDs
- **Power options** **:** Power over Ethernet: 9-28V DC
- **Dimensions** **:** 113x89x28mm. Weight: 130g
- **Power consumption** **:** Up to 3W

- **Operating System** **:** MikroTik RouterOS v3, Level4 license

3.4.2. PC (*Personal Computer*)

Pada pengujian digunakan dua buah PC untuk mengirimkan dan menerima data yang dikirim melalui topologi jaringan yang diuji. Berikut spesifikasi PC yang digunakan.

PC1 :

- Sistem operasi : Microsoft Windows XP Service Pack 2
- Processor : Intel® Core™ 2 Duo T7200 @ 2.00 GHz
- RAM : 1.5 GB
- Ethernet card : Broadcom NetXtreme 57xx

PC2 :

- Sistem operasi : Microsoft Windows XP Service Pack 2
- Processor : Intel® T2050 @ 2.00 GHz
- RAM : 1 GB
- Ethernet card : Realtek RTL8169/8110 Family Gigabit Ethernet NIC

Pada PC yang menggunakan sistem operasi Windows XP, secara *default* layanan untuk IPv6 belum diaktifkan. Sehingga perlu dikonfigurasi agar dapat mendukung IPv6. Untuk mengaktifkan dukungan IPv6 pada Windows XP yaitu dengan mengetikan perintah "***netsh interface ipv6 install***" atau perintah "***ipv6 install***" pada *command prompt* Windows yang selanjutnya proses instalasi akan berjalan dengan otomatis sampai selesai.

3.5. ALOKASI ALAMAT IP

Untuk alokasi IP pada topologi jaringan dibagi menjadi dua, yaitu alokasi IP pada topologi dengan IPv4 dan pada topologi IPv6. Pada pengujian pada IPv4 digunakan alamat *private* kelas C, dan pada IPv6 digunakan alamat *global*. Pada

Tabel 3.1 dan Tabel 3.2 memperlihatkan alokasi IP yang dipakai, baik pada topologi jaringan IPv4 maupun IPv6.

Alokasi IP pada topologi jaringan IPv4 :

Table 3.1 : Alokasi IP pada topologi IPv4

No.	Nama Perangkat	Interface	Alamat IP	Subnet Mask	Alamat Gateway
1.	Router R1	Ether1	192.168.10.1	255.255.255.0	-
2.		Ether2	192.168.20.1	255.255.255.0	-
3.		Ether4	192.168.40.1	255.255.255.0	-
4.	Router R2	Ether2	192.168.20.2	255.255.255.0	-
5.		Ether3	192.168.30.1	255.255.255.0	-
6.	Router R3	Ether3	192.168.30.2	255.255.255.0	-
7.		Ether4	192.168.40.2	255.255.255.0	-
8.		Ether1	192.168.50.1	255.255.255.0	-
9.	PC1	LAN1	192.168.10.2	255.255.255.0	192.168.10.1
10.	PC2	LAN1	192.168.50.2	255.255.255.0	192.168.50.1

Alokasi IP pada topologi jaringan IPv6 :

Table 3.2 : Alokasi IP pada topologi dengan IPv6.

No.	Nama Perangkat	Interface	Alamat IP	Subnet Mask	Alamat Gateway
1.	Router R1	Ether1	2001:abcd:10::1	/64	-
2.		Ether2	2001:abcd:20::1	/64	-
3.		Ether4	2001:abcd:40::1	/64	-
4.	Router R2	Ether2	2001:abcd:20::2	/64	-
5.		Ether3	2001:abcd:30::1	/64	-
6.	Router R3	Ether3	2001:abcd:30::2	/64	-
7.		Ether4	2001:abcd:40::2	/64	-
8.		Ether1	2001:abcd:50::1	/64	-

9.	PC1	LAN1	2001:abcd:10::2	/64	2001:abcd:10::1
10.	PC2	LAN1	2001:abcd:50::2	/64	2001:abcd:50::1

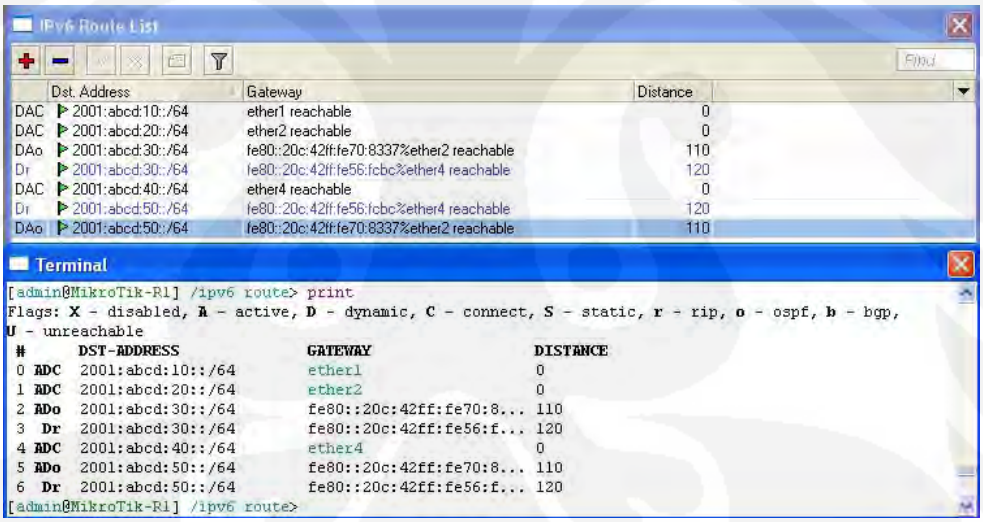
BAB IV

UJI COBA DAN ANALISA

4.1. PENGUJIAN PADA JARINGAN

4.1.1. Pengujian pemilihan jalur oleh *routing protocol*

Setelah semua router dan PC dikonfigurasi dan topologi jaringan sudah konvergensi, lalu dilakukan analisa *routing table* pada masing-masing router. Dari *routing table* terlihat jaringan-jaringan yang bisa dijangkau dan jalur-jalur yang dipilih oleh tiap *routing protocol* (RIPng dan OSPFv3). Seperti yang terlihat pada Gambar 4.1 adalah *routing table* pada router R1, dari *routing table* tersebut terlihat kalau router R1 dapat menjangkau jaringan 2001:abcd:10::/64, 2001:abcd:20::/64, 2001:abcd:30::/64, 2001:abcd:40::/64, dan 2001:abcd:50::/64.



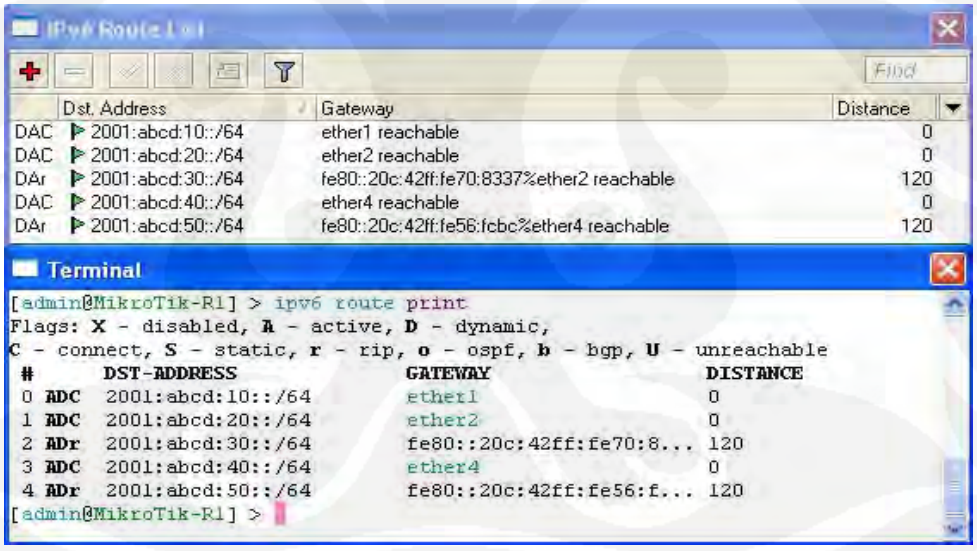
Gambar 4.1 : *Routing table* pada router R1

Lalu untuk menguji jalur yang dipilih routing table dilakukan dengan *trace route* pada PC1 menuju PC2 yaitu dengan printah "***tracert 2001:abcd:50::2***". Dengan perintah *trace route* dapat diketahui *interface-interface* dan router yang dilalui paket untuk mencapai tujuan. Pada Gambar 4.2 adalah hasil perintah tracert dari PC1 ke PC2.

```
C:\PC1>
C:\PC1>
C:\PC1>tracert 2001:abcd:50::2

Tracing route to 2001:abcd:50::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  2001:abcd:10::1
  2    <1 ms    <1 ms    <1 ms  2001:abcd:20::2
  3    <1 ms    <1 ms    <1 ms  2001:abcd:30::2
  4    <1 ms    <1 ms    <1 ms  2001:abcd:50::2

Trace complete.

C:\PC1>
C:\PC1>
C:\PC1>
```

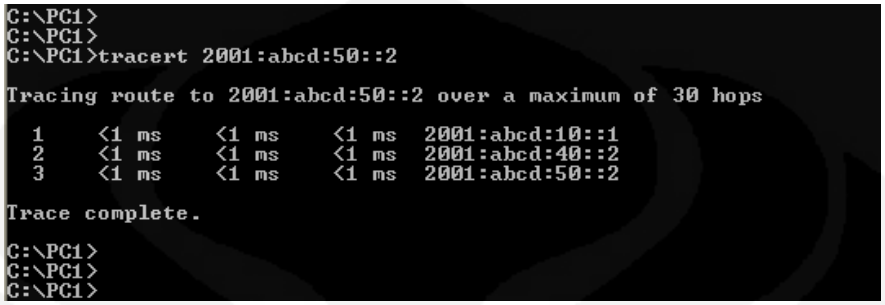
Gambar 4.2 : Hasil *trace route* PC1-PC2 pada jaringan.

Untuk pengujian routing protocol RIPng masing-masing router dikonfigurasi hanya dengan routing protocol RIPng. Setelah jaringan sudah konvergen lalu dianalisa kembali routing table pada router R1. Seperti yang terlihat pada Gambar 4.3 adalah *routing table* pada router R1, dari *routing table* tersebut terlihat kalau router R1 dapat menjangkau jaringan 2001:abcd:10::/64, 2001:abcd:20::/64, 2001:abcd:30::/64, 2001:abcd:40::/64, dan 2001:abcd:50::/64.



Gambar 4.3 : *Routing table* pada router R1 dengan *routing protocol* RIPng

Setelah analisa *routing table* dilakukan pengujian kembali dengan melakukan *trace route* dari PC1 ke PC2 dengan perintah "*tracert 2001:abcd:50::2*" pada PC1, dimana hasilnya ditujukan pada Gambar 4.4.



Gambar 4.4 : Hasil *trace route* PC1-PC2 dengan *routing protocol* RIPng

4.1.2. Pengujian kecepatan konvergen *routing table*

Pengujian dilakukan dengan melakukan pemutusan pada jalur yang aktif pada *routing table*, sehingga *routing table* segera menjadikan jalur alternatif yang terdaftar menjadi jalur aktif. Paket yang digunakan dalam pengujian adalah **100 buah paket ping** , dengan panjang data 32 byte. Pada routing protocol RIPng ada beberapa parameter *update routing* yang dikonfigurasi ulang, diantaranya: *Update timer* :00:00:15, *Timeout timer* :00:01:00, dan *Garbage timer* :00:00:30. Hasil dari pengujian dengan *routing protocol* RIPng ditunjukan pada Tabel 4.1, dan pengujian dengan OSPFv3 ditunjukan pada Tabel 4.1.

Tabel 4.1 : Hasil pengujian kecepatan konvergen dengan *routing protocol* RIPng

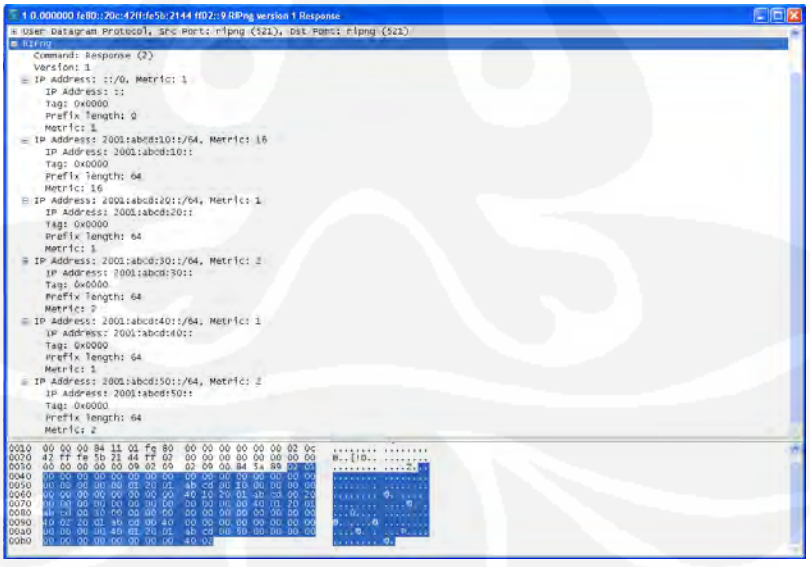
Pengujian	Paket diterima	Paket loss	Waktu konvergen (s)
1.	84	16	64,78
2.	85	15	58,12
3.	88	12	59,54
4.	86	14	56,61
5.	84	16	63,78
Rata-rata	**85,4**	**14,6**	**60,566**

Tabel 4.2 : Hasil pengujian kecepatan konvergen dengan *routing protocol* OSPFv3

Pengujian	Paket diterima	Paket loss	Waktu konvergen (s)
1.	99	1	4,00
2.	99	1	5,00
3.	99	1	4,06
4.	99	1	4,74
5.	99	1	4,91
Rata-rata	**99**	**1**	**4,542**

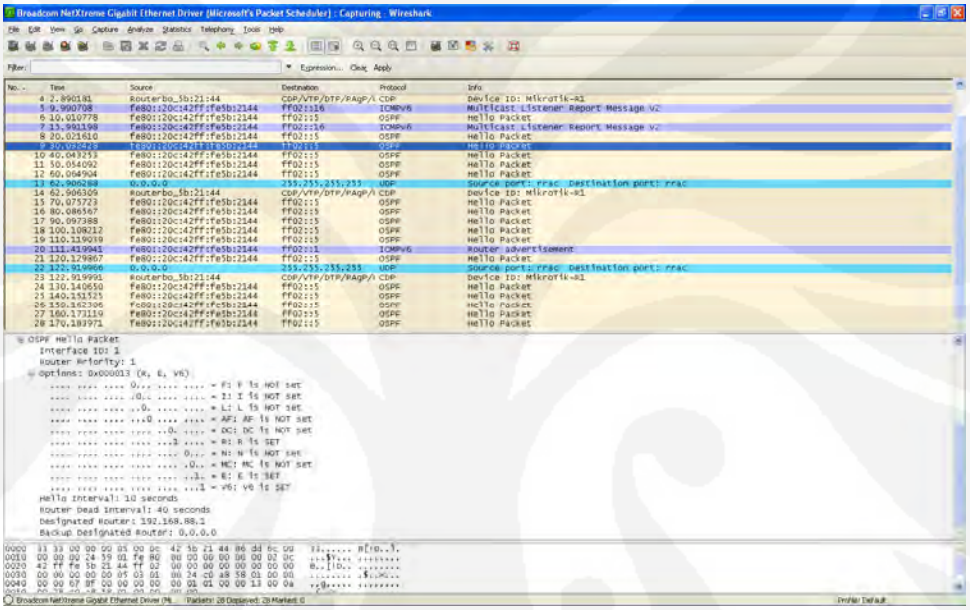
4.1.3. *Capture* paket *header routing protocol*

Pengujian dilakukan dengan melakukan *capture* pada *interface*, paket yang diambil adalah paket yang dikirimkan ketika proses *update table routing protocol* RIPng dan *hello packet* yang dikirimkan oleh OSPFv3. Pada *interface* router yang terhubung dengan PC tidak disetting sebagai *interface passive*, hal ini dilakukan agar update tetap dikirim ke interface. Pada Gambar 4.5 dan Gambar 4.6 adalah hasil capture pada paket RIPng dan OSPFv3.



Gambar 4.5 : Paket *header routing protocol* RIPng

Pada paket *update routing protocol* RIPng dapat dilihat informasi yang dibawanya, yaitu informasi *routing table* dari router lengkap dengan informasi jaringan yang dapat dijangkau dan nilai *metric*nya. Dari paket terlihat *port* yang digunakan untuk mengirimkan dan menerima *update*, yaitu *port* 521 dan alamat *multicast* yang digunakan untuk mengirimkan *update* adalah alamat ff02::9. Dari hasil *capture* paket juga dilihat untuk *update* dikirimkan rata-rata setiap 15 detik.



Gambar 4.6 : Paket *header routing protocol* OSPFv3

Pada paket hello OSPFv3 dapat dilihat bahwa alamat *multicast* yang digunakan untuk mengirimkan paket adalah alamat ff01::5. Paket hello dikirimkan setiap 10 detik. Paket paket juga terdapat informasi *router dead interval*, id *designated router*, dan id *backup designated router*.

4.1.4. Pengujian performa dengan pengiriman paket TCP dan UDP

Pada pengujian dengan pengiriman paket TCP yang dilakukan pengujian lima kali pengambilan data untuk masing-masing *routing protocol*, didapatkan rata-rata *throughput* untuk variasi *window size* dan waktu seperti yang ditunjukkan pada Tabel 4.3.

Tabel 4.3 : Hasil pengujian throughput dengan paket TCP.

Window Size (Kbyte)	IPv4		IPv6	
	RIP	OSPF	RIPng	OSPFv3
2	92,5	85,5	92,8	85,2
4	94,7	85,7	92,7	85,5
8	93,8	85,7	92,6	85,2
16	94,3	94,2	93,1	92,8
32	94,5	94,4	93,0	93,0

***Mbits/second**

Pada pengujian dengan paket UDP dilakukan pengujian dengan mengkondisikan jaringan melewati data mulai dari 40, 45, 50, hingga 80 Mbit/detik guna mendapatkan nilai *jitter* dari tiap-tiap *routing protocol* yang diuji. Hasil pengujian ditunjukan pada Tabel 4.4.

Tabel 4.4 : Hasil pengujian jitter dengan paket UDP.

Transfer (Mbytes)	Bandwith (Mbits/sec)	IPv4		IPv6	
		RIP	OSPF	RIPng	OSPFv3
47,7	**40**	0	0	0	0
53,7	**45**	0	0	0	0
59,7	**50**	0	0	0	0
65,8	**55**	1,048	0	0	0
71,5	**60**	1,037	0,982	1,097	1,089
83,4	**70**	0,975	0,935	1,340	1,205
94,5	**80**	0,946	0,922	1,152	1,025

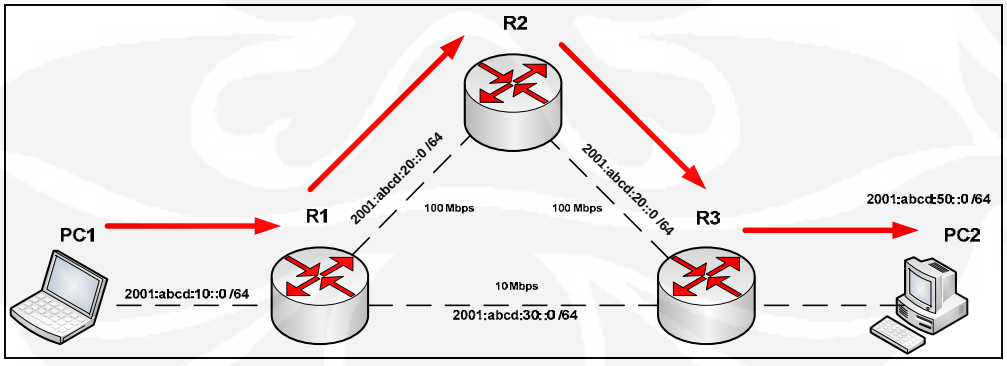
***millisecond (ms)**

4.2. ANALISA DATA

4.2.1. Analisa pemilihan jalur oleh *routing protocol*

Ketika kedua *routing protocol* dikonfigurasi pada masing-masing router, maka *routing protocol* yang aktif yang digunakan oleh router adalah *routing protocol* OSPFv3, terlihat pada routing table dengan tanda A (*Active*). Hal ini terjadi karena OSPF memiliki nilai AD lebih kecil, yaitu 110 dibandingkan dengan nilai AD dari RIP yaitu 120. Namun untuk *routing* RIPng tetap terdaftar pada *routing table*.

Pada pengujian terlihat pada *routing table* di R1 jalur yang dipilih untuk mencapai jaringan 2001:ABCD:50::/64 adalah melalui alamat *gateway* fe80::20c:42ff:fe70:83:37, dimana alamat tersebut merupakan alamat *link local* untuk *interface* ether 2 pada router R2. Dan dari hasil pengujian dengan trace route pada PC1 menuju PC2 terlihat *interface* yang dilalui untuk mencapai PC2, yaitu melalui alamat *interface* 2001:abcd:10::1, 2001:abcd:20::2, 2001:abcd:30::2, dan terakhir mencapai alamat 2001:abcd:50::2 yaitu alamat *interface* pada PC2. Sehingga dapat digambarkan jalur yang dipilih oleh *routing protocol* OSPFv3 pada router R1 untuk mencapai jaringan 2001:abcd:50::/64 adalah melalui router R1-R2-R3. Berikut Gambar 4.7 adalah alur proses pengiriman paket dengan *routing protocol* OSPFv3.



Gambar 4.7 : Alur pengiriman paket dari PC1 ke PC2 dengan *routing protocol* OSPFv3.

Jalur tersebut dipilih pada masing-masing router, karena pada OSPF menggunakan *cost* sebagai *metric*nya. Semakin besar *bandwith* yang dipakai pada *interface* maka semakin kecil nilai *cost*nya. Untuk perhitungan nilai *cost* pada *interface* yang digunakan pada jaringan adalah sebagai berikut :

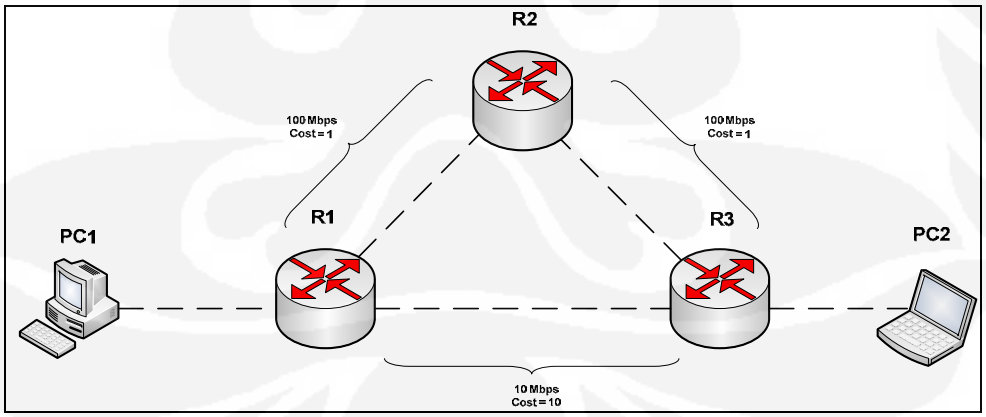
- **Interface Fast Ethernet (100Mbps) :**

  Cost = $\frac{10^8}{100.000.000\ bps} = 1$

- **Interface Ethernet (10Mbps):**

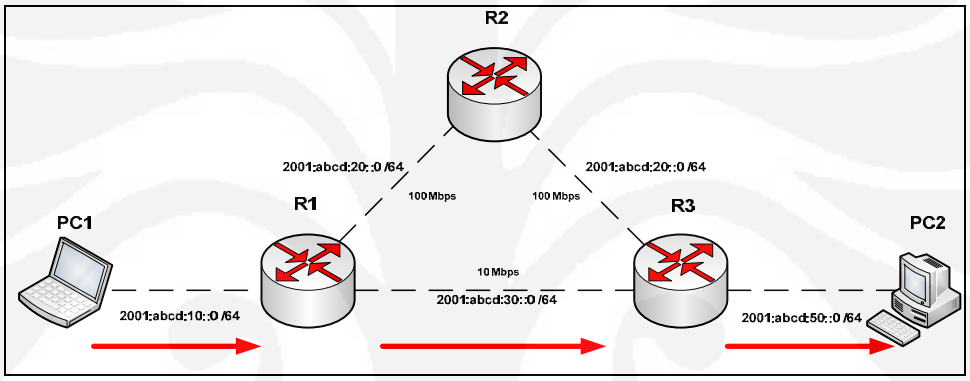
  Cost = $\frac{10^8}{10.000.000\ bps} = 10$

Dari perhitungan cost diatas dapat dihitung nilai cost untuk mencapai PC2 lebih kecil jika melalui R1-R2-R3 yaitu dengan akumulasi total *cost* yaitu 2, dibandingkan jika melalui R1-R2 yang memakan cost sebesar 10. Oleh karena itu maka dengan *routing protocol* OSPFv3 jalur yang digunakan untuk mengirimkan paket dari PC1 ke PC3 adalah melalui R1-R2-R3. Gambar ilustrasi nilai *cost* pada jaringan ditunjukan pada Gambar 4.8.



Gambar 4.8 : Nilai cost pada masing-masing rute pada OSPFv3

Seperti yang terlihat pada *routing table* pada gambar 4.3, pada *routing protocol* RIPng jalur yang dipilih oleh router R1 untuk mencapai ke jaringan 2001:abcd:50::/ 64 adalah melalui alamat *gateway* fe::20c:42ff:fe56:fc:bc atau alamat *link local* untuk *interface* ethernet 4 pada router R3. Jalur ini dipilih karena pada routing protocol RIPng menggunakan *metric hop count*, yaitu berdasarkan jumlah router yang dilalui tanpa berpengaruh dengan *bandwith interface*nya. Jadi jalur yang dipilih oleh *routing protocol* RIPng dalam mengirimkan paket dari PC1 ke PC2 melaui router R1 lalu R2, seperti pada Gambar 4.9.



Gambar 4.9 : Alur pengiriman paket dari PC1 ke PC2 dengan *routing protocol* RIPng.

Pada pengujian trace route pada topologi dengan RIPng dapat dilihat jalur atau *interface* router yang dilalui oleh paket untuk mencapai jaringan 2001:abcd:50:: adalah melalui 2001:abcd:10:1 (*Ethernet* 1 router R1), 2001:abcd:40::2 (*Ethernet* 4 router R3), dan tujuan akhir 2001:abcd:50::2 (*interface ethernet* PC2), sehingga untuk menjangkau jaringan 2001:abcd:50::/64, routing protocol RIPng menggunakan jalur yang melalui R1- R3 dan tidak melalui jalur R1-R2-R3. Jalur ini dipilih karena RIPng merupakan *routing protocol distance-vector* yang menggunakan *hop count* sebagai metricnya. Dimana *metric* pada jalur R1-R3 bernilai 2, yang lebih rendah jika dibandingakan jalur R1-R2-R3 yang memiliki nilai *metric* 3.

4.2.2. Analisa kecepatan konvergen *routing table*

Pada pengujian *routing protocol* RIPng dibutuhkan waktu sekitar 60,566 detik untuk mencapai kondisi konvergen. Nilai ini merupakan pengaruh dari nilai *timeout* yang digunakan yaitu 00:01:00 atau 60 detik. Ketika waktu *timeout* habis maka pada metric dibuat bernilai 16, lalu jalur alternatif dijadikan jalur aktif pada *routing table*. Pada *routing protocol* RIP proses *update routing table* bekerja secara periodik dan dipengaruhi oleh konfigurasi *timer update* yang digunakan.

Pada pengujian OSPFv3 hasil rata-rata yang dibutuhkan untuk konvergen adalah 4,542 detik. Dengan konvergen secepat ini masih didapatkan paket *loss* sebesar 1 paket dari 100 paket ICMP yang dikirimkan. Dari pengujian terbukti jika pada OSPFv3 memiliki kelebihan dalam melakukan konvergen *routing table* pada jaringan dengan cepat. Pada OSPFv3 jika terjadi perubahan pada *link*, maka informasi *link* tersebut yang dikirimkan ke router yang lain.

4.2.3. Analisa paket *update routing protocol*

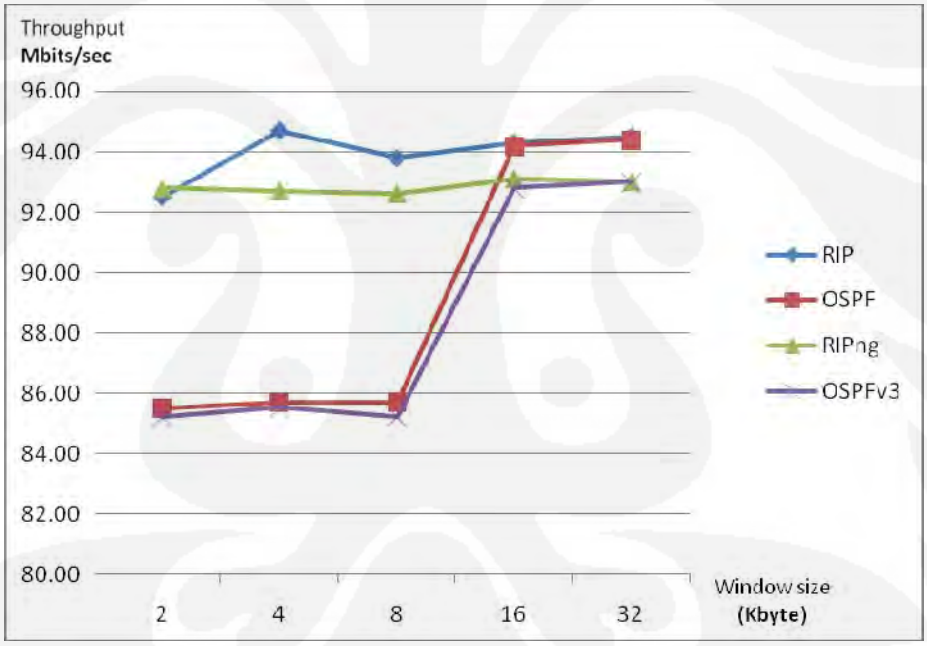
Dari analisa paket *header update routing table* pada RIPng dapat dilihat alamat *multicast* yang digunakan untuk mengirimkan *update table* ke router lain yang terhubung adalah alamat *multicast* **ff02::9**, *port* yang digunakan untuk mengirimkan *update table* adalah ***port* 521**. Pada paket header juga dapat dilihat bahwa dalam melakukan *update*, RIPng mengirimkan semua informasi *routing table* dan meneruskannya ke router yang lain. Sedangkan dengan *routing protocol* RIP pada IPv4 alamat *multicast* yang digunakan adalah 224.0.0.9 dan port 520(UDP). Untuk waktu *update table* yang dikirimkan setiap sekitar 15 detik sesuai dengan konfigurasi yang dilakukan, yaitu waktu *update Timer* 00:00:15. Dengan dikirimnya seluruh update table ke router rip yang lain dan dengan jangka waktu yang rutin, maka *routing protocol* RIPng-RIP cukup membebani jaringan.

Dari paket Hello OSPFv3 dapat dilihat alamat multicast yang digunakan adalah alamat **ff02::5**. Pada paket Hello terdapat informasi versi OSPF, tipe paket OSPF, alamat router pengirim paket, area ID, interval paket hello, dan lainnya. Dilihat dari paket header OSPFv3 tidak jauh berbeda paket OSPF pada IPv4.

Perbedaan hanya pada alamat pada paket header yaitu pada informasi versi OSPF yang digunakan.

4.2.4. Analisa performa dengan pengiriman paket TCP dan UDP

Throughput adalah parameter yang menunjukan jumlah bit rata-rata data yang dapat ditransfer dari satu *node* ke *node* yang lain perdetiknya. Pengujian *throughput* dengan paket TCP diukur dengan membandingkan jumlah byte data TCP yang dikirim melalui jaringan dengan jumlah waktu yang diperlukan dalam pengiriman. Dari data hasil pengujian digambarkan pada grafik yang ditunjukan pada Gambar 4.10.

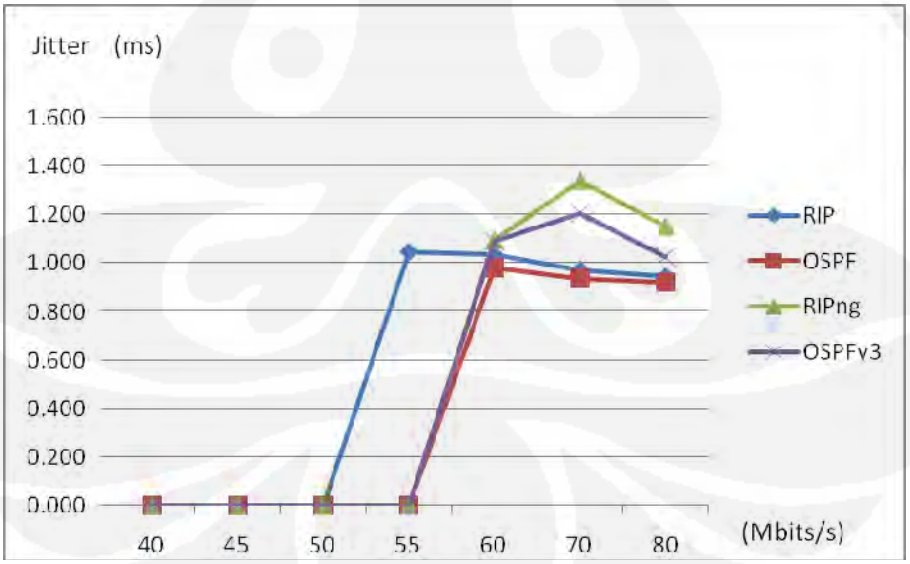


Gambar 4.10 : Grafik hasil pengujian *throughput* TCP.

Dari grafik pada Gambar 4.10 terlihat besarnya throughput TCP bernilai 85,2-85,7Mbits/detik pada pengujian *routing protocol* OSPF dan OSPFv3 dengan ukuran *window size* 2, 4, dan 8 Kbyte lebih rendah dibandingkan pengujian routing protocol RIP dan RIPng yang cenderung stabil dengan nilai *throughput* 92,5-94,5 Mbits/detik pada pengujian di setiap variasi *window size*. Namun pada

penggunaan sistem operasi Windows, nilai *default* untuk *window size* TCP yang digunakan bernilai 16Kbyte, sehingga pada penggunaan *routing protocol* pada jaringan lokal dengan aplikasi pada PC tidak terlihat perbedaan performa dari penggunaan *routing protocol* yang berbeda antara RIPng dengan OSPFv3. Dari hasil pengujian terlihat nilai throughput maksimal pada jaringan dengan koneksi Fast Ethernet 100Mbps dengan pengiriman paket TCP sebesar 94,7 Mbit/s dengan RIP 94,4 Mbit/s dengan OSPF 93,1 Mbit/s dengan RIPng dan 93,0 Mbit/s dengan routing protocol OSPFv3. Dari hasil terlihat bahwa throughput atau kemampuan sebenarnya suatu jaringan dalam malakukan pengiriman data pada jaringan test-bed tidak mencapai 100Mbits/s, karena bergantung pada trafik yang sedang terjadi.

Ukuran *window* pada TCP berpengaruh pada nilai *throughput*, karena *window size* adalah nilai atau ukuran maksimal dari data yang dapat dikirim tanpa paket *acknowledge* (konfirmasi). Semakin kecil nilai *window size* maka akan memperlambat transfer, karena banyaknya paket data yang perlu di *acknowledge*. Sehinga pada pengujian mempengaruhi nilai throughput yang didapatkan.



Gambar 4.11 : Grafik hasil pengujian jitter.

Gambar 4.11 adalah gambar hasil pengujian jitter dengan pengiriman paket UDP. Pada pengujian dengan masing-masing *routing protocol*, nilai *jitter* yang didapat memiliki nilai yang fluktuatif pada tiap-tiap pengujian. Dengan *routing protocol* RIP memiliki nilai *jitter* yang lebih besar dibandingan *jitter* dengan OSPF pada IPv4, begitu juga pada pengujian pada jaringan IPv6 *jitter* pada pengujian dengan RIPng lebih besar dibandingan pengujian dengan OSPFv3.

Jitter adalah suatu parameter yang menunjukan variasi *delay* antar paket dalam pengiriman yang sama. Jaringan yang baik adalah jaringan yang memiliki nilai *jitter* yang kecil. Dari grafik diatas terlihat bahwa besar *jitter* ikut berubah saat besar *bandwith* transfer berubah. Secara umum nilai *jitter* meningkat dengan nilai besaran yang fruktuatif. Hal ini terjadi karena semakin banyak data yang dikirim maka semakin besar kemungkinan terjadinya tabrakan (*congestion*) pada jaringan. Dari pengujian didapatkan nilai *jitter* pada OSPFv3 lebih kecil 0,37% dibandingkan dengan penggunaan *routing protocol* RIPng hal ini menunjukan kestabilan dalam pengiriman paket data. Nilai *jitter* yang didapatkan masih masuk dalam kategori sangat bagus, hal ini dikarenakan pada *test-bed* pengujian yang sederhana dengan kondisi trafik ideal tanpa ada pengaruh dari data lain pada jaringan.

BAB V

KESIMPULAN

1. Secara keseluruhan cara kerja *routing protocol* pada IPv6 (RIPng dan OSPFv3) dengan *routing protocol* pendahulunya RIP dan OSPF pada IPv4 memiliki cara kerja yang sama, perbedaan yang mendasar ialah dukungan terhadap pengalamatan 128-bit.

2. Pada pengujian *routing procotol* RIPng, untuk mencapai konvergen *routing table* dibutuhkan waktu sebesar 60,566 detik dengan paket loss sebesar 14,6 dari 100 paket ICMPv6. Pada OSPFv3 untuk mencapai konvergen *routing table* dibutuhkan waktu sebesar 4,542 detik dengan paket loss sebesar 1 dari 100 paket ICMPv6 yang dikirimkan.

3. Pada pengujian terbukti jika *routing protocol* RIPng menggunakan UDP port 521 dan alamat FF02::9 digunakan sebagai alamat *multicast* ke router RIP yang lain untuk mengirimkan *update table* dan OSPFv3 menggunakan alamat FF02::5 sebagai alamat *multicast* dalam mengirimkan informasi jalur atau *link* ke router yang lain.

4. Hasil pengujian *throughput* dengan *window size* paket TCP berukuran 2, 4, 8, 16, 32 Kbyte didapatkan nilai rata-rata 92,8 Mbits/detik untuk *routing protocol* RIPng, dan pada OSPFv3 didapatkan nilai rata-rata *throughput* 85,3Mbits/detik untuk *windows size* 2, 4, 8 Kbyte dan 92,9Mbits/detik untuk *window size* berukuran 16 dan 32 Kbyte. Pada pengujian jitter dengan paket UDP pada jaringan IPv6, didapat besar jitter dengan *routing protocol* RIPng rata-rata 1,196 ms dan dengan dengan OSPFv3 rata-rata sebesar 1,106 ms.

DAFTAR ACUAN

[1] The 6NET Consortium (September 2005). *An IPv6 Deployment Guide*. http://www.6net.org, Halaman 9.

[2] Cisco CCNA Exploration 4.0. *Routing Protocols and Concepts*,2007

[3] RIPng technology white paper. http://www.huawei-3com.com /portal/ Products ___Solutions/Technology/IP_Routing/Technology_White_Paper/

[4] Stewart, Brent D (2008). *CCNP BSCI Official Exam Certification Guide Fourth Edition*. Indianapolis: Cisco Press.Halaman 550.

[5] http://www.ietf.org/rfc/rfc2328.txt

[6] Cisco CCNA Exploration 4.0. *Routing Protocols and Concepts*,2007. The OSPF Metric

[7] Cisco CCNA Exploration 4.0. *Routing Protocols and Concepts*,2007. The OSPF Metric

DAFTAR PUSTAKA

Davies, Joseph (2002). *Understanding IPv6*. Washington, DC: Microsoft Press.

Deering S., R. Hinden (Desember 1998). *Internet Protocol Version 6 (IPv6) Spesification*. RFC:2460 http://www.ietf.org/rfc/rfc2460.txt

Haryanto, Taofik (2004). *Analisa Routing Protocol RIPng dan OSPFv3 pada jaringan lokal IPv6 dengan metode tunneling 6 over 4 dan 6 to 4*. Depok: Universitas Indonesia.

Pun, Hubert (1998). *Convergence Behavior of RIP and OSPF Network Protocols*.British Columbia: University of British Columbia.

Stewart, Brent D (2008). *CCNP BSCI Official Exam Certification Guide Fourth Edition*. Indianapolis: Cisco Press.

Taufan, Riza (2002). Teori dan Implementasi IPv6-Protocol Internet Masa Depan. Jakarta: Elex Media Komputindo.

The 6NET Consortium (September 2005). *An IPv6 Deployment Guide*. http://www.6net.org