ITS
Institut
Teknologi
Sepuluh Nopember

TUGAS AKHIR - RE1599

ANALISA UNJUK KERJA PROTOKOL ROUTING RIPng (*ROUTING INFORMATION PROTOCOL NEXT GENERATION*) PADA JARINGAN IPV6

Krishna Kurniawan
NRP 2206 100 512

Dosen Pembimbing
Ir. Djoko Suprajitno Rahardjo

JURUSAN TEKNIK ELEKTRO
Fakultas Teknologi Industri
Institut Teknologi Sepuluh Nopember
Surabaya 2009

ANALISA UNJUK KERJA PROTOKOL ROUTING RIPng (*ROUTING INFORMATION PROTOCOL NEXT GENERATION*) PADA JARINGAN IPV6

TUGAS AKHIR

Diajukan Guna Memenuhi Sebagian Persyaratan
Untuk Memperoleh Gelar Sarjana Teknik
Pada
Bidang Studi Telekomunikasi Multimedia
Jurusan Teknik Elektro
Institut Teknologi Sepuluh Nopember

Menyetujui :

Dosen Pembimbing

Ir. Dioko Suprajitno Rahardjo
NIP. 131 651 447

SURABAYA

2009

TUGAS AKHIR

Diajukan Guna Memenuhi Sebagian Persyaratan
Untuk Memperoleh Gelar Sarjana Teknik
Pada
Bidang Studi Teknik Komputer Multimedia
Jurusan Teknik Elektro
Institut Teknologi Sepuluh Nopember

Menyetujui :

Dosen Pembimbing

Ir. Djoko Purwanto, M.Eng.
NIP. 131 476 427

SURABAYA

2005

iii

ABSTRAK

ABSTRAK

IPv6 merupakan versi terbaru dari *Internet Protocol* (IP) yang merupakan bakal pengganti bagi IPv4. IPv6 ini juga biasa disebut dengan IPng (IP *next generation*). Pada jaringan dengan IPv6 terdapat teknologi routing yang terbagi atas 2 keluarga besar yaitu keluarga IGP (Interior Gateway Protocol) dan keluarga EGP (Exterior Gateway Protocol). Salah satu routing IGP yaitu RIP (Routing Information Protocol) dan yang dipakai dalam jaringan IPv6 adalah protokol RIPng (*Routing Information Protocol next generation*).

Pada tugas akhir ini akan dilakukan penelitian pada unjuk kerja IPv6 dengan menggunakan protokol routing RIPng (Routing Information Protocol next generation) dengan menggunakan beberapa PC dengan konfigurasi tertentu sebagai *router* dan *client*. Sistem operasi yang digunakan adalah Linux untuk router dan Windows untuk client, lalu akan dilaporkan mengenai analisa unjuk kerja protokol *routing* RIPng pada jaringan IPv6 mengenai hasil dari *throughput*, *delay, jitter*, dan *packet loss* yang timbul pada protokol routing RIPng. Lalu dilakukan percobaan pada *routing* RIPng mengenai pencarian rute terpendek dalam jaringan secara dinamis ketika jaringan masih dalam kondisi utuh dan pencarian rute alternatif secara otomatis jika sewaktu-waktu jalur utama pada jaringan IPv6 tersebut putus/ mati.

Berdasarkan hasil perbandingan pengukuran unjuk kerja jaringan IPv6 dengan menggunakan protokol routing RIPng dan jaringan IPv4 dengan menggunakan protokol routing RIP dengan memperhatikan parameter-parameter *delay, throughput, jitter, dan packet loss* terlihat bahwa jaringan IPv4 mempunyai throughput rata-rata lebih besar sebesar 14.81% daripada throughput pada jaringan IPv6. Jitter pada jaringan IPv4 mempunyai selisih rata-rata 53.48% lebih kecil daripada jitter pada jaringan IPv6. Selisih rata-rata packet loss IPv6 dan IPv4 adalah 0.077%. Sehingga terlihat bahwa untuk saat ini kinerja IPv4 masih lebih baik daripada IPv6.

Kata Kunci: IPv6, RIPng, *distance vector routing*

ABSTRACT

IPv6 is the newest technology in IP and will be the successor of IPv4. IPv6 also common to be called the IP next generation. In IPv6 there are 2 family of protocol routing, they are the IGP (Interior Gateway Protocol) and the EGP (Exterior Gateway Protocol). One of the routing protocol from IGP that used is RIP (Routing Information Protocol) and one that used in IPv6 network is the RIPng (*Routing Information Protocol next generation*).

In this final project, some research of performance analysis in IPv6 network using Routing Protocol RIPng (Routing Information Protocol next generation) with Linux PC Router using and Windows PC Client will be performed. Also, there are report on performance analysis Routing Protocol RIPng esspecially in throughput, delay, jitter and packet loss. After those test, there will be another test in RIPng routing in finding the shortest path from source to destination in normal network condition and the alternative path when trouble occured in the main backbone. The test will see if the RIPng routing can find another route to destination automatically.

Based on the test result from performance analysis in IPv6 network with Routing Protocol RIPng and IPv4 network with Routing Protocol RIP, we can see that throughput test result in IPv4 network is better than throughput in IPv6 network with average difference 14.81%. Jitter test in IPv4 network result also better than jitter test in IPv6 network with average difference 53.48%. Average difference in packet loss test in IPv4 network and IPv6 network is 0.077%. It can be seen that at this time IPv4 performance still better than IPv6 performance.

Keyword: IPv6, RIPng, *distance vector routing*

KATA PENGANTAR

KATA PENGANTAR

Puji syukur saya panjatkan kehadirat Tuhan Yang Maha Esa karena berkat rahmat dan hidayah-Nya saya dapat menyelesaikan laporan tugas akhir dengan judul

ANALISA UNJUK KERJA PROTOKOL ROUTING RIPng (Routing Information Protocol next generation) PADA JARINGAN IPV6

Tugas akhir yang mempunyai beban 4 SKS (Satuan Kredit Semester) ini merupakan salah satu syarat yang harus dipenuhi untuk menyelesaikan program studi Strata-1 pada Jurusan Teknik Elektro Fakultas Teknologi Industri Institut Teknologi Sepuluh Nopember Surabaya. Melalui kegiatan ini diharapkan mahasiswa dapat melakukan kegiatan laporan yang bersifat penelitian ilmiah dan menghubungkannya dengan teori yang telah diperoleh dalam perkuliahan.

Dalam penyusunan laporan tugas akhir ini penulis menyadari akan adanya kekurangan-kekurangan baik dalam penyusunan maupun pembahasan masalah karena keterbatasan pengetahuan penulis. Untuk itu penulis mengharapkan kritik dan saran membangun dari semua pihak agar dapat lebih baik di masa yang akan datang.

Besar harapan penulis bahwa buku tugas akhir ini dapat memberikan informasi dan manfaat bagi pembaca pada umumnya dan mahasiswa Jurusan Teknik Elektro pada khususnya.

Sebagai penutup, penulis berharap semoga laporan Tugas Akhir ini dapat bermanfaat bagi pembaca.

Surabaya, Februari 2009

Penulis

UCAPAN TERIMA KASIH

UCAPAN TERIMA KASIH

Pada kesempatan ini penulis ingin menyampaikan rasa syukur kehadirat Allah SWT yang telah memberikan petunjuk, kemudahan dan kemurahan -NYA serta tidak lupa ucapan terima kasih sebesar besarnya kepada beberapa pihak yang telah memberikan dukungan selama proses penyelesaian Tugas Akhir ini, antara lain :

1. Allah, SWT yang selalu melimpahkan rahmat dan hidayah-Nya
2. Nabi Muhammad SAW, yang Insya Allah selalu menjadi panutan dari setiap langkah hidup saya.
3. Bapak dan Ibu, yang selalu mengalirkan do'a, nasehat, perhatian, kasih dan hal-hal yang lainnya hingga kuliah ini terselesaikan.
4. My lovely little sister atas segala dukungannya padaku selama kuliah Lintas Jalur ini.
5. Bapak Ir. Djoko Suprajitno Rahardjo selaku dosen pembimbing atas petunjuk, bimbingan, serta dukungan moral yang telah diberikan hingga Tugas Akhir ini terselesaikan.
6. Bapak. Dr. Ir. Moch. Ashari, M,Eng. sebagai ketua jurusan Teknik Elektro-ITS.
7. Bapak dan Ibu dosen penguji Tugas Akhir yang telah memberikan saran dan masukkannya kepada penulis.
8. Teman-teman Lintas Jalur 2006, Akhmed "cemet", mpok Ayu, neng Cindy, Yanuar "yance", Wak Dayan, Darda "kacong", Riski "nobita", dan yang lainnya atas segala kebersamaannya.
9. Soulmate-ku Tugas Akhir di LAB, Alfian Andri "Kendhow" Trianto atas segalanya.
10. Keputih Lor 12, Ade, Boby, Fa'i, Dani, Rizal atas segala kebersamaan selama di kosan lama.
11. Bumi Marina Mas Utara blok F/69, Wak Budi, Willy "Lipeng", Cak Wingga, Pak Candra, Tom "kruz", Pak No, Supri, Gepeng, Ari, Fahri, Nazrul, dan Erik yang menemaniku di kos-kosan.
12. Teman-teman LAB 301, Nurman F Seisei, Firman, Hafif, Esti, Citra,dan Irfan yang selalu menemani di LAB.
13. Adik-adik kelas dari semester bawah, Sari, Teti, Lisa, Igen, Cory, Niko, Ari, atas semangat dan dukungannya.
14. Yuni Faisyah atas dukungannya dan yang telah bersedia meminjamkan laptopnya hingga tugas akhir ini terselesaikan.
15. Serta semua pihak yang telah membantu kelancaran pelaksanaan Tugas Akhir yang tidak bisa disebutkan satu persatu.

DAFTAR ISI

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR GAMBAR

Gambar

DAFTAR TABEL

DAFTAR TABEL

Tabel

BAB I
PENDAHULUAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

IPv6 merupakan versi terbaru dari *Internet Protocol* (IP) yang merupakan bakal pengganti bagi IPv4. IPv6 ini juga biasa disebut dengan IPng (IP *next generation*). IPv6 ini muncul dikarenakan keterbatasan pengalamatan IP yang dialami oleh IPv4, dimana IP ini sangat dibutuhkan oleh mesin-mesin yang terkoneksi ke internet. Pada IPv4 pengalamatan IP hanya 32 bit, sedangkan pada IPv6 mencapai 128 bit. Diperkirakan pada 2-8 tahun kedepan jumlah IPv4 yang tersisa akan habis, karena itu sekarang ini sudah dimulai pengalamatan IPv6 pada mesin-mesin terbaru.

Pada jaringan dengan IPv6 otomatis akan berlaku juga teknologi routing yang hampir sama dengan routing pada IPv4 yang terbagi atas 2 keluarga besar yaitu keluarga IGP (Interior Gateway Protocol) yang terbagi lagi menjadi routing *link-state* dan routing *distance-vector* serta keluarga EGP (Exterior Gateway Protocol).

Pada keluarga IGP terdiri dari tipe protokol routing RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First)dan IS-IS (Intermediate system to intermediate system). Sedangkan dari keluarga EGP terdiri dari routing protokol (BGP) Border Gateway Protocol.

Salah satu jenis protokol yang dipakai dalam jaringan IPv6 adalah protokol RIPng (*Routing Information Protocol next generation*) yang merupakan pembaharu protokol RIPv2 yang digunakan pada jaringan IPv4, pada RIPng ini digunakan pada jaringan IPv6. Protokol ini termasuk dalam jenis protokol IGP (*Interior Gateway Protocol*) yang menggunakan algoritma *distance vector* dalam menentukan rute terbaik untuk ke arah tujuan. Setiap router dalam jaringan RIPng ini akan mengirimkan seluruh tabel routingnya dalam setiap update ke router tetangganya.

1.2 Permasalahan

Pada tugas akhir ini, permasalahan yang akan dibahas dalam Tugas Akhir adalah:

- Penerapan RIPng pada jaringan IPv6 supaya bisa menentukan rute terpendek dari jaringan tersebut.
- *Throughput, delay, jitter* dan *packet loss* dari pengiriman packet pada jaringan tersebut.

1.3 Batasan Masalah

Batasan masalah yang akan dibahas pada tugas akhir ini adalah:

- Pembahasan protokol IPv6, arsitektur protokol dan pengalamatan IPv6.
- Pembahasan protokol routing RIPng.
- Percobaan akan dilakukan di LAB dengan menggunakan 3 komputer sebagai router dan 2 komputer sebagai *client*.
- Penggunaan OS Linux Debian untuk router dan OS Windows untuk *client*.

1.4 Tujuan

Penelitian pada tugas akhir ini bertujuan untuk mengetahui routing dan pengalamatannya pada IPv6 dan protokol routing RIPng.

1.5 Metodologi

Metode penelitian yang digunakan dalam Tugas Akhir ini terdiri dari :

1. Studi Literatur
   - Jaringan IPv6
   - IGP menggunakan Protokol *Routing* RIPng
   - *Shell Programming*
   - Parameter jaringan dan Distribusi Jaringan
2. Perancangan dan Pembuatan Sistem.
3. Pengujian, dan Pengolahan Data
4. Analisa dan Pembahasan Data
5. Penulisan Laporan

1.6 Sistematika Penulisan

Untuk memudahkan pembahasan, sistematika penulisannya disusun sebagai berikut :

BAB I : PENDAHULUAN

Bab ini menjelaskan tentang latar belakang, permasalahan dan batasan masalah, tujuan, metodologi serta relevansi dari penulisan Tugas Akhir.

BAB II : DASAR TEORI

Menjelaskan mengenai teori pendukung yang digunakan sebagai referensi dalam melakukan penelitian.

BAB III : PERENCANAAN dan IMPLEMENTASI

Meliputi pembahasan diagram blok sistem, Skenario jaringan yang digunakan dan tipe protokol routing yang digunakan.

BAB IV : ANALISA HASIL SIMULASI

Dibahas mengenai hasil penelitian yang membandingkan kinerja routing protokol RIP pada IPv4 dan RIPng pada IPv6.

BAB V : PENUTUP

Menjelaskan kesimpulan yang diperoleh dari hasil anlisa dan saran.

1.7 Relevansi

Dari Tugas Akhir ini diharapkan bisa menjadi bahan acuan dalam mata kuliah Jaringan Komputer dan Jaringan Akses serta bisa diterapkan pada dunia industri khususnya pada bidang Jaringan dengan IPv6.

BAB II
DASAR TEORI

BAB II
TEORI PENUNJANG

2.1 Awal terbentuknya IPv6

Versi awal dari Internet Protocol yang digunakan pertama kali adalah IPv4, memberikan kapasitas alamat sekitar 4 milyar IP. Ketika desain awal ini diterapkan, penggunaan IPv4 ini terlihat cukup untuk melayani pengguna internet.

Pada awal tahun 1990, pengguna internet sudah sangat banyak sekali, hingga akhirnya perlu dirumuskan ulang mengenai Internet Protocol yang baru untuk mencegah adanya kehabisan alamat IP. Pada awal 1992, beberapa sistem diperkenalkan untuk mencegah hal tersebut dan pada akhir 1992, IETF (Internet Engineering Task Force) mengumumkan suatu hasil dari pertemuan yang selama ini digelar yaitu RFC 1550 dan pembentukan grup tentang "IP Next Generation" (IPng).

IETF mengadopsi IPng pada tanggal 25 Juli 1994 dengan beberapa formasi grup kerja tentang IPng. Pada 1996, beberapa seri dari RFC telah dikeluarkan untuk mendefinisikan *Internet Protocol Version* 6 (IPv6) ini diantaranya adalah RFC 2460.

Sekedar pengetahuan saja, para teknisi dari IPng tidak dapat menggunakan versi nomor 5 untuk pengganti dari IPv4, karena versi 5 telah dialamatkan pada eksperimen protokol flow-oriented streaming atau lebih dikenal dengan nama Internet Stream Protocol, mirip dengan IPv4, hanya saja lebih dikhususkan untuk mensupport video dan audio.

2.1.1 Manajemen organisasi alamat IP

Manajemen untuk pengalamatan IP di dunia ini berpusat di sebuah organisasi di Amerika Serikat yang bernama IANA [1] (Internet Assigned Numbers Authority). IANA ini bertugas untuk mengurusi masalah penetapan parameter protokol internet, seperti ruang alamat IP, dan *Domain Name System* (DNS). IANA juga memiliki otoritas untuk menunjuk organisasi lainnya untuk memberikan blok alamat IP spesifik kepada pelanggan dan untuk meregistrasikan nama domain. IANA juga bertindak sebagai otoritas tertinggi untuk mengatur root DNS yang mengatur basis data pusat informasi DNS, selain tentunya menentapkan alamat IP untuk sistem-sistem otonom di dalam jaringan Internet.

---

1. http://www.arin.net/community/rirs.html

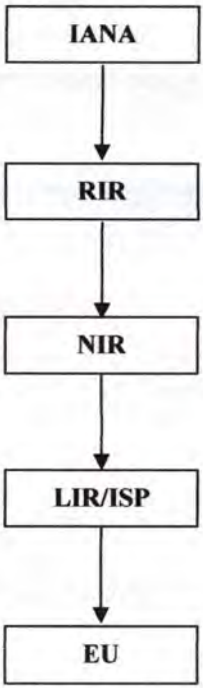
IANA beroperasi di bawah naungan *Internet Society* (ISOC). IANA juga dianggap sebagai bagian dari *Internet Architecture Board* (IAB). IANA memberikan tanggungjawab dalam mengatur pengaturan ruang alamat IP dan DNS kepada RIR (Regional Internet Registry) pada masing-masing wilayah. Saat ini ada 5 RIR yang tersebar di seluruh dunia, yaitu:

- **ARIN (American Registry for Internet Numbers)**
  Bertanggungjawab dalam menangani alamat IP untuk wilayah Amerika Utara.
- **AfriNIC (African Network Information Center)**
  Bertanggung jawab dalam menangani alamat IP untuk wilayah Afrika.
- **APNIC (Asia Pacific Network Information Centre)**
  Bertanggung jawab dalam menangani alamat IP untuk wilayah Asia Pasifik.
- **LACNIC (Latin American and Carribean IP *Header* Regional Registry)**
  Bertanggung jawab dalam menangani alamat IP untuk wilayah Amerika Latin dan Karibia.
- **RIPE NCC (Réeseaux IP Européens Network Coordination Centre)**
  Bertanggung jawab dalam menangani alamat IP untuk wilayah Eropa, Timur Tengah dan beberapa negara di Asia.

Setelah RIR, pengorganisasian IP akan diteruskan pada NIR (National Internet Registry). NIR ini bertugas untuk mengalokasikan *header space* kepada para anggota dan konstituennya, yang umumnya adalah LIR (Local Internet Registry) yang terorganisir pada tingkat nasional atau tingkat ekonomi yang terpisah. NIR diharapkan untuk mengaplikasikan kebijakan serta prosedur mereka secara adil dan merata kepada seluruh anggota wilayah mereka. Contoh NIR ini di Indonesia adalah APJII.

Lalu oleh NIR ini, alamat IP akan dibagi-bagi ke LIR yang umumnya juga merupakan ISP (Internet Service Provider) atau Penyelenggara Jasa Internet, serta dapat mendelegasikan IP kepada infrastruktur jaringannya sendiri dan pengguna layanan jaringannya atau EU (End User).

Urut-urutan proses jalur internet mulai dari IANA hingga ke End User tersebut secara umum dijalankan di setiap negara pengguna internet, dan jika dijelaskan dalam bentuk grafik, maka akan didapatkan gambar seperti berikut.



Gambar 2.1. Arsitektur Manajemen Pengalamatan IP

2.1.2 Fitur-fitur yang terdapat pada IPv6

Untuk perkembangan dunia internet, IPv6 adalah pengganti yang tepat dari IPv4. Hampir seluruh *layer transport* dan aplikasi tidak memerlukan perubahan yang berarti, perkecualian untuk protokol aplikasi yang berjalan di *layer network* (seperti FTP atau NTPv3).

IPv6 menspesifikasikan tipe format paket baru, yang didesain untuk meminimalkan proses *header* paket. Dikarenakan *header* IPv6 dan IPv4 sangat berbeda, kedua protokol tersebut tidak dapat berkomunikasi.

Selain itu, IPv6 adalah protokol baru yang digunakan pada layer 3 dimana IPv6 ini direncanakan akan menggusur kedudukan dari IPv4, karena efisiensi struktur *header* serta penambahan alamat IP dari 32 bit hingga 128 bit dan penambahan ukuran *header* IPv6 dari 20 byte menjadi 40 byte pada IPv6. *Header* pada IPv6 ini lebih besar daripada IPv4 tapi sedikit dalam jumlah *header* yang digunakan

sehingga akan lebih efektif dan efisien dalam pengantaran data. Adapun bentuk *header* IPv6 [2] adalah seperti gambar berikut ini:

Gambar 2.2. Susunan *header* IPv6

Keterangan *header*:

- **Version**: Untuk menandai versi dari IP yang digunakan. Berukuran empat bit.
- **Traffic Class** : untuk menandai kelas/ prioritas dari paket IPv6. Berukuran delapan bit.
- **Flow Label** : untuk menandai paket tersebut dimiliki oleh urutan spesifik tertentu dari paket IPv6 antara asal dan tujuan dipakai pada aplikasi *realtime*. Berukuran 20 bit
- ***Header* Length** : menandai panjang dari *header*.
- **Next *Header*** : menandai tambahan *header* pertama jika ada atau jenis protokol pada lapisan atas PDU. Berukuran 8 bit
- **Extension *Header*** : digunakan untuk tambahan fungsi yang dibutuhkan seperti security, dsb.

---

2. RIPE 40 Meeting, Prague, Czech Republic " IPv6 Tutorial", October 2001

- **Hop Limit** : untuk menandai hop maksimum yang dapat dipakai oleh IPv6 dalam lalu lintas internet.
- **Source *Header*** : digunakan untuk menyimpan alamat IPv6 dari *host* asal, berukuran 128 bit.
- **Destination *Header*** : digunakan untuk menyimpan alamat IPv6 dari *host* tujuan, berukuran 128 bit

Adapun fitur-fitur yang terdapat pada IPv6 adalah seperti dibawah ini:

- **Jumlah alamat IP yang lebih besar**
  Fitur IPv6 menyediakan alamat IP yang lebih besar daripada IPv4. Alamat di IPv6 mencapai 128 bit daripada 32 bit pada IPv4.
- ***Header* Scope**
  IPv6 mengenalkan konsep dari *header scopes*. Sebuah *Header scope* mendefinisikan "daerah" atau "jangkauan" dimana sebuah alamat bisa mendefinisikan identitas unik dari sebuah interface.
  Jangkauan ini meliputi local link, site network, dan global network, seperti terdefinisi pada RFC 3513 dan RFC 4193. Interface yang dikonfigurasi untuk IPv6 biasanya mempunyai lebih dari satu alamat, biasanya satu alamat untuk alamat local link dan satu lagi untuk alamat site-local atau global *header*ing. Alamat link-local biasanya digunakan pada konfigurasi alamat jaringan secara otomatis dimana tidak ada sumber lain dari luar yang memberikan alamat pada interface.
- **Konfigurasi alamat *stateless* secara otomatis**
  Host IPv6 dapat mengkonfigurasi diri mereka sendiri ketika mereka terhubung pada jaringan IPv6 dengan menggunakan ICMPv6 dari router yang terhubung. Ketika pertama kali terhubung pada jaringan, sebuah *host* akan mengirimkan permintaan *link-local multicast* kepada router untuk parameter-parameter konfigurasi, jika permintaan konfigurasi diterima oleh router, router akan merespond pada *request* tersebut dengan paket advertisement yang mengandung konfigurasi layer network.
  Jika pada proses diatas tidak berhasil, maka sebuah *host* bisa menggunakan konfigurasi *statefull* (DHCPv6) atau dikonfigurasi secara manual. Dengan kata lain, konfigurasi otomatis *stateless* tidak digunakan oleh router tersebut dan harus dikonfigurasi secara manual atau dengan cara yang lain.

- **Multicast**
  Adalah kemampuan untuk mengirimkan paket tunggal ke banyak tujuan. Tidak seperti halnya pada IPv4, dimana kemampuan ini opsional.
  IPv6 tidak mengimplementasikan broadcast, kemampuan untuk mengirimkan semua paket ke semua *host* pada link yang tersambung. Efek yang sama dapat tercapai dengan cara mengirimkan sebuah paket pada semua *host* pada *link-local* grup *multicast*.
- **Keamanan layer network yang terjamin**
  IPsec (Internet Protocol Security) adalah protokol untuk enkripsi IP dan autentikasi. Fitur ini akan terimplementasi secara otomatis dalam jaringan IPv6, tidak seperti pada jaringan IPv4 yang bersifat opsional.
- **Pemrosesan paket yang lebih sederhana**
  Format dari *header* paket IPv6 bertujuan untuk meminimalkan proses *header* pada proses antar router. Walaupun alamat pada IPv6 4 kali lebih besar, *header* default yang dipakai hanya berukuran 2 kali lebih besar dari ukuran *header* IPv4.
- **Prioritas pengiriman paket**
  Paket *header* pada IPv6 mengandung *header* baru yang bernama "Flow Label" untuk memprioritaskan pengiriman paket oleh router. Flow Label ini menggantikan *header* "Service Type" pada IPv4. Spesifikasi dan kegunaan dari *header* ini tidak begitu terdefinisi dengan baik untuk saat ini.
- **Hop-Limit vs TTL**
  Header "Time to Live" dari IPv4 telah digantikan dengan *header* "Hop Limit".
- **Mobilitas**
  Tidak seperti pada IPv4, *Mobile IPv6* (MIPv6) menghindari "triangular routing" dan tetap beroperasi seefisien IPv6 normal.
- **Parameter *Option* yang lebar**
  Pada IPv4, parameter *option* ini mempunyai ukuran yang tetap (40 bytes) sedangkan pada IPv6 parameter option ini diperlakukan sebagai *header* tambahan setelah *header* IPv6, dimana batas ukuran mereka adalah ukuran dari seluruh paket.
- **Jumbogram**
  IPv4 membatasi paket hingga 64 KB sebagai *header*, sedangkan IPv6 mempunyai support untuk paket melebihi paket pada IPv4, yang sering diibaratkan sebagai jumbogram

yang hingga 4 GB. Penggunaan jumbogram diindikasikan pada *header* Jumbo *Header* Option.

2.1.3 Perbedaan antara IPv4 dan IPv6

Tabel 2.1 Perbedaan IPv4 vs IPv6[3]

IPv4	IPv6
Panjang alamat 32 bit (4 bytes).	Panjang alamat 128 bit (16 bytes).
Dikonfigurasi secara manual atau DHCP IPv4.	Tidak harus dikonfigurasi secara manual, bisa menggunakan autoconfiguration.
Dukungan terhadap IPSec bersifat opsional.	Dukungan terhadap IPSec mutlak.
Fragmentasi dilakukan oleh pengirim dan pada router.	Fragmentasi dilakukan hanya oleh pengirim.
Tidak mensyaratkan ukuran paket pada link-layer dan harus bisa menyusun kembali paket berukuran 576 byte.	Paket link-layer harus mendukung ukuran paket 1280 byte dan harus bisa menyusun kembali paket berukuran 1500 byte.
Checksum termasuk pada *header*.	Cheksum tidak masuk dalam *header*.
Header mengandung *option*.	Data opsional dimasukkan seluruhnya ke dalam *extensions header*.
Menggunakan ARP Request secara broadcast untuk menterjemahkan alamat IPv4 ke alamat link-layer.	ARP Request telah digantikan oleh Neighbor Solitcitation secara multicast.

3. http://geeks.netindonesia.net/blogs/fajar/archive/2007/04/28/ Fundamental-IPv6-_3A00_-Comparison-of-IPv4-and-IPv6.aspx

2.1.4 Konektivitas antara IPv4 dan IPv6

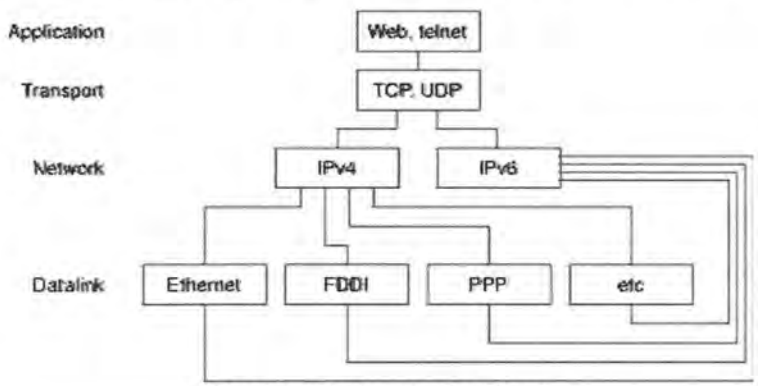
Hingga IPv6 benar-benar menggantikan IPv4, sejumlah mekanisme transisi diperlukan untuk *host-host* dengan IPv6 untuk mencapai layanan IPv4 dan membuat antar *host* dengan IPv6 berkomunikasi dengan melewati infrastruktur IPv4.

Selama periode tersebut, *host* dan router yang menggunakan IPv6 RFC 2893 (Transition Mechanisms for IPv6 Hosts and Routers) dan RFC2185 (Routing Aspects of IPv6 Transition) mendefinisikan kompatibilitas dan mekanisme transisi. Teknik ini biasa disebut dengan Simple Internet Transition (SIT)[4].

Metode SIT ini meliputi:

- **Dual-Stack**

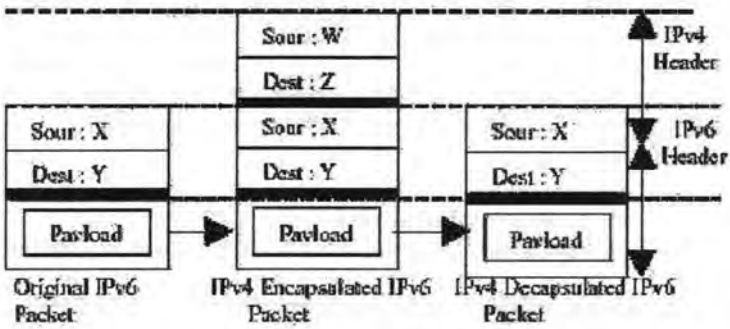
  Sejak IPv6 merepresentasikan kelanjutan dari IPv6, beberapa eksperimen implementasi menggunakan IPv4 dan IPv6 secara independen. Istilah *dual-stack* biasanya berarti duplikasi secara total dari semua level protokol dari layer aplikasi hingga layer network. Sebuah contoh dari duplikasi total adalah OSI dan protokol TCP/IP yang berjalan pada sistem yang sama. Bagaimanapun juga, pada konteks transisi IPv6 ini berarti sebuah protokol yang mengandung baik IPv4 dan IPv6. Sehingga semua protokol transport, TCP, UDP dan lainnya bisa menggunakan baik IPv4 dan IPv6, dan juga aplikasi yang sama juga bisa menggunakan IPv4 dan IPv6.



Gambar 2.3. Susunan Dual-Stack

4. http://en.wikipedia.org/wiki/IPv6

- **Tunneling**
  Untuk mencapai Internet dengan menggunakan IPv6, sebuah *host* atau jaringan yang terisolasi harus menggunakan infrastruktur IPv4 untuk membawa paket IPv6. Teknik ini dinamakan "Tunelling" dimana teknik ini akan mengenkapsulasi paket-paket IPv6 didalam jaringan IPv4. Enkapsulasi langsung dari datagram IPv6 didalam paket IPv4 diindikasikan oleh protokol IP nomor 41. IPv6 juga bisa dienkapsulasikan didalam paket UDP, jika terdapat router yang memblok protokol IP nomor 41. Tunelling sendiri dibagi menjadi Automatic tunneling dan Configured tunneling.



Gambar 2.4. Proses enkapsulasi pada tunelling

- **Automatic tunneling**
  Teknik ini berarti proses dimana infrastruktur routing akan menentukan secara otomatis dimana posisi *endpoint tunnel*. Posisi *endpoint tunnel* ditentukan dari alamat *anycast* IPv4 pada sisi remote, dan mencocokkan informasi alamat IPv4 didalam alamat IPv6 di sisi lokal
- **Configured tunneling**
  Teknik ini mengkonfigurasi *endpoint* dari tunnel secara eksplisit, menggunakan operator manusia atau servis otomatis yang biasa dikenal sebagai "tunnel broker". Tunnel yang terkonfigurasi biasanya lebih gampang untuk pengecekan masalah dan direkomendasikan untuk jaringan yang besar, teknik ini menggunakan port IP 41.

- **Proxying and translation for IPv6-only *hosts***
  Setelah Regional Internet Registries telah kehabisan jatah IP dari IPv4, maka untuk alamat IP *host* yang baru akan mendapat jatah IPv6. Untuk pelanggan baru ini jika ingin terkoneksi dengan jaringan IPv4 maka harus menggunakan mekanisme translasi, salah satu metode yang bisa digunakan adalah penggunaan *dual-stack application-layer* proxy, sebagai contohnya adalah web proxy.

2.2 Tata Alamat IPv6

Dalam IPv6, alamat 128-bit akan dibagi ke dalam 8 blok berukuran 16-bit, yang dapat dikonversikan ke dalam bilangan heksadesimal berukuran 4-digit [5]. Setiap blok bilangan heksadesimal tersebut akan dipisahkan dengan tanda titik dua (:). Karenanya, format notasi yang digunakan oleh IPv6 juga sering disebut dengan *colon-hexadecimal format*, berbeda dengan IPv4 yang menggunakan *dotted-decimal format*.

2.2.1 Cara Penulisan Alamat IPv6

Berikut ini adalah contoh alamat IPv6 dalam bentuk bilangan biner:

0010000111011010000000001101001100000000000000000000101111
0011101100000010101010100000000011111111111111111000101000
1001110001011010

Untuk menerjemahkannya ke dalam bentuk notasi colon-hexadecimal format, angka-angka biner di atas harus dibagi ke dalam 8 buah blok berukuran 16-bit:

0010000111011010 0000000011010011 0000000000000000
0010111100111011 0000001010101010h
0000000011111111 1111111000101000 1001110001011010

Lalu, setiap blok berukuran 16-bit tersebut harus dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan menggunakan tanda titik dua. Hasil konversinya adalah sebagai berikut:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Alamat diatas bisa disederhanakan dengan membuang angka 0 pada awal setiap blok yang berukuran 16-bit di atas, dengan menyisakan satu digit terakhir. Dengan membuang angka 0, alamat di atas disederhanakan menjadi:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

5. Taufan Riza, Teori dan Implementasi IPv6 Protokol Internet Masa Depan, Elex Media Komputindo, 2001

Konvensi pengalamatan IPv6 juga mengizinkan penyederhanaan alamat lebih jauh lagi, yakni dengan membuang banyak karakter 0, pada sebuah alamat yang banyak angka 0-nya. Jika sebuah alamat IPv6 yang direpresentasikan dalam notasi *colon-hexadecimal* format mengandung beberapa blok 16-bit dengan angka 0, maka alamat tersebut dapat disederhanakan dengan menggunakan tanda dua buah titik dua (::). Untuk menghindari kebingungan, penyederhanaan alamat IPv6 dengan cara ini sebaiknya hanya digunakan sekali saja di dalam satu alamat, karena kemungkinan nantinya pengguna tidak dapat menentukan berapa banyak bit 0 yang direpresentasikan oleh setiap tanda dua titik dua (::) yang terdapat dalam alamat tersebut. Tabel berikut mengilustrasikan cara penggunaan hal ini.

Tabel 2.2 Penyederhanaan alamat IPv6

Alamat asli	Alamat asli yang disederhanakan	Alamat setelah dikompres
FE80:0000:0000:0000:02AA:00FF:FE9A:4CA2	FE80:0:0:0:2AA:FF:FE9A:4CA2	FE80::2AA:FF:FE9A:4CA2
FF02:0000:0000:0000:0000:0000:0000:0002	FF02:0:0:0:0:0:0:2	FF02::2

Untuk menentukan berapa banyak bit bernilai 0 yang dibuang (dan digantikan dengan tanda dua titik dua) dalam sebuah alamat IPv6, dapat dilakukan dengan menghitung berapa banyak blok yang tersedia dalam alamat tersebut, yang kemudian dikurangkan dengan angka 8, dan angka tersebut dikalikan dengan 16. Sebagai contoh, alamat FF02::2 hanya mengandung dua blok alamat (blok FF02 dan blok 2). Maka, jumlah bit yang dibuang adalah (8-2) x 16 = 96 buah bit.

2.2.2 Format Prefix

Dalam IPv4, sebuah alamat dalam notasi *format dotted-decimal* dapat direpresentasikan dengan menggunakan angka *prefix* yang merujuk kepada subnet mask. IPv6 juga memiliki angka *prefix*, tapi tidak didugnakan untuk merujuk kepada subnet mask, karena memang IPv6 tidak mendukung subnet mask.

Prefix adalah sebuah bagian dari alamat IP, di mana bit-bit memiliki nilai-nilai yang tetap atau bit-bit tersebut merupakan bagian dari sebuah rute atau subnet identifier. *Prefix* dalam IPv6 direpesentasikan dengan cara yang sama seperti halnya *prefix* alamat IPv4, yaitu [alamat]/[angka panjang *prefix*]. Panjang *prefix*

menentukan jumlah bit terbesar paling kiri yang membuat *prefix* subnet. Sebagai contoh, *prefix* sebuah alamat IPv6 dapat direpresentasikan sebagai berikut:

3FFE:2900:D005:F28B::/64

Pada contoh di atas, 64 bit pertama dari alamat tersebut dianggap sebagai *prefix* alamat, sementara 64 bit sisanya dianggap sebagai interface ID.

2.2.3 Tipe Alamat IPv6

- **Unicast *Header***
  Alamat *unicast* mengidentifikasikan sebuah alamat tunggal dari sebuah piranti jaringan. Protokol akan mengantarkan paketke sebuah alamat unicast pada sebuah *interface* yang spesifik. Alamat Unicast IPv6 bisa mempunyai cakupan alamat yang lebih spesifik: alamat *unicast global*, alamat *link-local*, dan alamat *unicast unique-local*.
- **Anycast *Header***
  Sebuah alamat *anycast* diberikan ke sebuah grup interface, yang termasuk dalam node yang berbeda-beda. Sebuah paket yang dikirimkan ke sebuah alamat *anycast* dikirimkan hanya ke sebuah interface dari grup interface tersebut, biasanya dikirimkan ke interface yang terdekat berdasarkan pilihan dari jarak routing protokol.
- **Multicast *Header***
  Alamat *Multicast* diberikan juga ke sebuah grup interface yang tergolong node yang berbeda-beda. Sebuah paket yang diantarkan ke alamat multicast diantarkan ke semua *interface* yang diidentifikasikan oleh alamat tersebut. Alamat *multicast* ini didesain untuk menggantikan alamat *broadcast* pada IPv4 yang banyak mengkonsumsi bandwidth.

2.3 Routing

Routing adalah proses dimana suatu router mengarahkan paket ke jaringan yang dituju[6]. Suatu router membuat keputusan berdasarkan IP address yang dituju oleh paket. Semua router menggunakan IP address tujuan untuk mengirim paket. Agar keputusan routing tersebut benar, router harus belajar bagaimana untuk mencapai tujuan. Ketika router menggunakan routing dinamis, informasi ini dipelajari dari router yang lain.

---

6. amang@eepis.its.edu "modul 6 routing dan protokol routing"

Ketika menggunakan routing statis, seorang network administrator mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual.

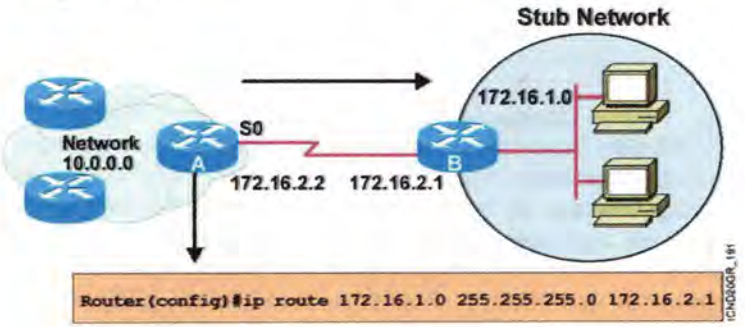
2.3.1 Routing Statis

Routing statis adalah routing yang konfigurasinya harus dilakukan secara manual, dengan kata lain administrator jaringan harus memasukkan atau menghapus rute statis jika terjadi perubahan topologi. Pada jaringan skala besar, jika tetap menggunakan routing statis, maka akan sangat membuang waktu administrator jaringan untuk melakukan update table routing. Karena itu routing statis hanya mungkin dilakukan untuk jaringan skala kecil.

Cara kerja routing statis dapat dibagi menjadi 3 bagian:

- Administrator jaringan yang mengkonfigurasi router
- Router melakukan routing berdasarkan informasi dalam tabel routing
- Routing statis digunakan untuk melewatkan paket data

Berikut dibawah ini adalah gambar contoh konfigurasi dari routing statis:



Gambar 2.5. Routing Statis

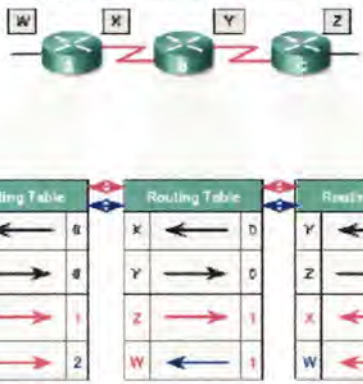
2.3.2 Routing Dinamis

Routing dinamis adalah komunikasi antara router-router secara otomatis dan tidak diatur secara manual untuk perubahan tabel routingnya. Routing dinamis mengijinkan router-router untuk sharing informasi tentang jaringan dan koneksi antar router. Router menggunakan informasi ini untuk membangun dan memperbaiki table routingnya. Routing dinamis bisa dibedakan menjadi dua macam berdasarkan algoritma routingnya, yaitu:

- Distance Vector
- Link State

2.3.2.1 Distance Vector

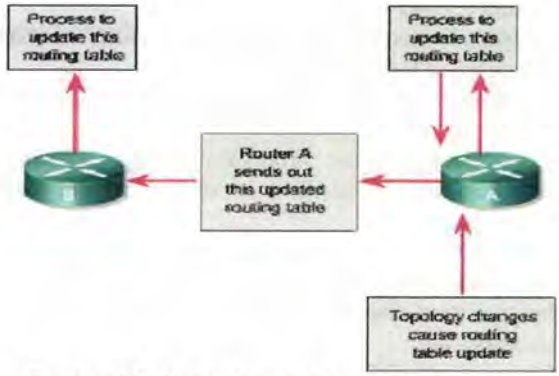
Algoritma routing distance vector secara periodik akan menyalin table routing dari router ke router. Perubahan table routing ini di-update antar router yang saling berhubungan pada saat terjadi perubahan topologi. Setiap router menerima table routing dari router tetangga yang terhubung langsung. Pada gambar di bawah ini digambarkan konsep kerja dari distance vector.



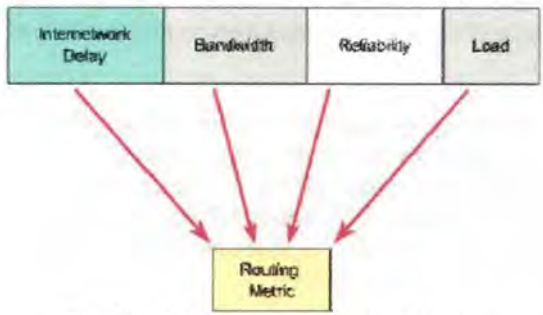
Gambar 2.6. Konsep Distance Vector

Setiap router yang menggunakan distance vector pertama kali mengidentifikasi router-router tetangganya. Interface yang terhubung langsung ke router tetangganya mempunyai distance 0. Router yang menerapkan distance vector dapat menentukan jalur terbaik untuk menuju ke jaringan tujuan berdasarkan informasi yang diterima dari tetangganya. Router A mempelajari jaringan lain berdasarkan informasi yang diterima dari router B. Masing-masing router lain menambahkan dalam table routingnya yang mempunyai akumulasi distance vector untuk melihat sejauh mana jaringan yang akan dituju.

Update table routing terjadi ketika terjadi perubahan toplogi jaringan. Sama dengan proses discovery, proses update perubahan topologi step-by-step dari router ke router. Gambar 2.7 menunjukkan algoritma distance vector memanggil ke semua router untuk mengirim ke isi table routingnya. Table routing berisi informasi tentang total path cost yang ditentukan oleh metric dan alamat logic dari router pertama dalam jaringan yang ada di isi table routing, seperti yang diterangkan oleh gambar 2.8 berikut



Gambar 2.7. Perubahan topologi distance vector



Gambar 2.8. Komponen Routing Metric

Analogi distance vector dapat digambarkan dengan jalan tol. Tanda yang menunjukkan titik menuju ke tujuan dan menunjukkan jarak ke tujuan. Dengan adanya tanda-tanda seperti itu pengendara dengan mudah mengetahui perkiraan jarak yang akan ditempuh untuk mencapai tujuan. Dalam hal ini jarak terpendek adalah rute yang terbaik.

Dalam penerapannya penggunaan algoritma distance vector diterapkan pada routing:

- RIP – mempunyai karakteristik sebagai berikut:
  - Routing protokol distance vector.
  - Metric berdasarkan jumlah lompatan (hop count) untuk pemilihan jalur.
  - Jika hop count lebih dari 15, paket dibuang.
  - Update routing dilakukan secara broadcast setiap 30 detik

- IGRP – adalah protokol routing yang dibangun oleh Cisco, dengan karakteristik sebagai berikut:
  - Protokol routing distance vector.
  - Menggunakan composite metric yang terdiri atas bandwidth, load, delay, reliability dan MTU.
  - Update routing dilakukan secara broadcast setiap 90 detik

- EIGRP - menggunakan protokol routing interior dengan algoritma advanced Cisco distance vector, dengan karakteristik sebagai berikut:
  - Menggunakan protokol routing enhanced distance vector.
  - Menggunakan cost load balancing yang tidak sama.
  - Menggunakan algoritma kombinasi antara distance vector dan link-state.
  - Menggunakan Diffusing Update Algorithm (DUAL) untuk menghitung jalur terpendek.
  - Update routing dilakukan secara multicast menggunakan alamat 224.0.0.10 yang diakibatkan oleh perubahan topologi jaringan.

- Border Gateway Protocol (BGP) merupakan routing protokol eksterior, dengan karakteristik sebagai berikut:
  - Menggunakan routing protokol distance vector.
  - Digunakan antara ISP dengan ISP dan client-client.
  - Digunakan untuk merutekan trafik internet antar Autonomous System (AS).

2.3.2.2 Link State

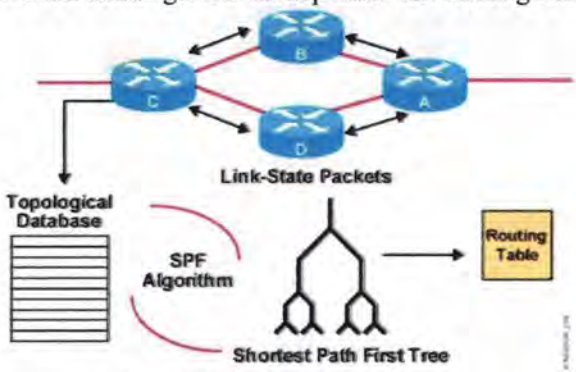
Algoritma link-state juga dikenal dengan algoritma Dijkstra atau algoritma shortest path first (SPF). Algoritma ini memperbaiki informasi database dari informasi topologi. Algoritma distance vector memiliki informasi yang tidak spesifik tentang distance network dan tidak mengetahui jarak router. Sedangkan algortima link-state memperbaiki pengetahuan dari jarak router dan bagaimana mereka inter-koneksi.

Fitur-fitur yang dimiliki oleh routing link-state adalah:

- Link-state advertisement (LSA) – adalah paket kecil dari informasi routing yang dikirim antar router
- Topological database – adalah kumpulan informasi yang dari LSA-LSA

- SPF algorithm – adalah hasil perhitungan pada database sebagai hasil dari pohon SPF
- Routing table – adalah daftar rute dan interface

Berikut adalah gambar konsep dasar dari Routing Link State:



Gambar 2.9. Konsep Link State

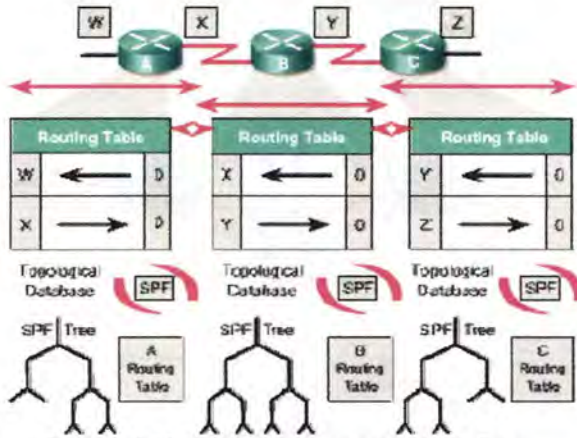
Proses discovery dari routing link-state dimulai ketika router melakukan pertukaran LSA, dimulai dengan jaringan yang terhubung langsung tentang informasi yang mereka miliki. Masing-masing router membangun database topologi yang berisi pertukaran informasi LSA. Algoritma SPF menghitung jaringan yang dapat dicapai. Router membangun logical topologi sebagai pohon (tree), dengan router sebagai root.

Topologi ini berisi semua rute-rute yang mungkin untuk mencapai jaringan dalam protokol link-state internetwork. Router kemudian menggunakan SPF untuk memperpendek rute. Daftar rute-rute terbaik dan interface ke jaringan yang dituju dalam table routing. Link-state juga memperbaiki database topologi yang lain dari elemen-elemen topologi dan status secara detail.

Dalam penerapannya penggunaan algoritma link state diterapkan pada routing OSPF yang mempunyai karakteristik sebagai berikut:

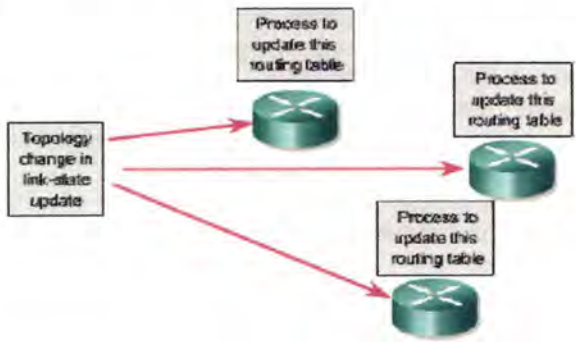
- Protokol routing link-state.
- Merupakan open standard protokol routing yang dijelaskan di RFC 2328.
- Menggunakan algoritma SPF untuk menghitung cost terendah.
- Update routing dilakukan secara floaded saat terjadi perubahan topologi jaringan.

Adapun proses perutean dalam algoritma link state adalah seperti yang digambarkan pada gambar 2.10



Gambar 2.10. Proses discovery pada Link State

Router pertama yang mempelajari perubahan topologi link-state melewatkan informasi sehingga semua router dapat menggunakannya untuk proses update. Gambar 2.11 adalah informasi routing dikirim ke semua router dalam internetwork. Untuk mencapai keadaan konvergen, setiap router mempelajari router-router tetangganya. Termasuk nama dari router-router tetangganya, status interface dan cost dari link ke tetangganya. Router membentuk paket LSA yang mendaftar informasi ini dari tetangga-tetangga baru, perubahan cost link dan link-link yang tidak lagi valid. Paket LSA ini kemudian dikirim keluar sehingga semua router-router lain menerima itu



Gambar 2.11. Perubahan topologi link state

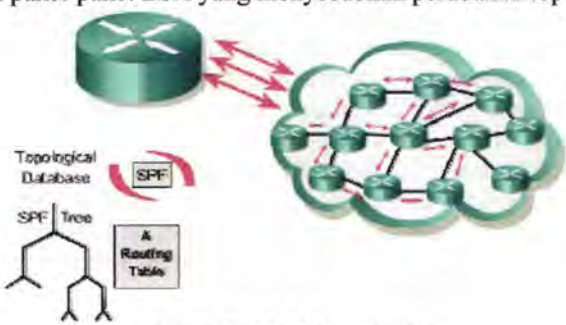
Pada saat router menerima LSA, ia kemudian meng-update table routing dengan sebagian besar informasi yang terbaru. Data

hasil perhitungan digunakan untuk membuat peta internetwork dan lagoritma SPF digunakan untuk menghitung jalur terpendek ke jaringan lain. Setiap waktu paket LSA menyebabkan perubahan ke database link-state, kemudian SPF melakukan perhitungan ulang untuk jalur terbaik dan meng-update table routing.

Ada beberapa titik berat yang berhubungan dengan protokol link-state:

- Processor overhead
- Kebutuhan memori
- Konsumsi bandwidth

Router-router yang menggunakan protokol link-state membutuhkan memori lebih dan proses data yang lebih daripada router-router yang menggunakan protokol distance vector. Router link-state membutuhkan memori yang cukup untuk menangani semua informasi dari database, pohon topologi dan table routing. Gambar 2.12 menunjukkan inisialisasi paket flooding link-state yang mengkonsumsi bandwidth. Pada proses inisial discovery, semua router yang menggunakan protokol routing link-state mengirimkan paket LSA ke semua router tetangganya. Peristiwa ini menyebabkan pengurangan bandwidth yang tersedia untuk me-routing trafik yang membawa data user. Setelah inisial flooding ini, protokol routing link-state secara umum membutuhkan bandwidth minimal untuk mengirim paket-paket LSA yang menyebabkan perubahan topologi.



Gambar 2.12. Link State concern

2.4 Routing Information Protocol (RIP)

RIP adalah protokol routing yang paling banyak digunakan untuk membuat tabel routing di intranet. Routing Information Protocol adalah sebuah protokol routing yang pertama kalinya didesain oleh Xerox PARC Universal Protocol dan digunakan di Xerox Network Systems (XNS)

RIP lalu terasosiasikan dengan UNIX dan TCP/IP ketika Berkeley Software Distribution (BSD) mengeluarkan OS dengan versi UNIX dengan implementasi RIP yang digunakan sebagai "route dee" pada 1982. RIP akhirnya diperkenalkan secara formal dalam publikasi XNS Internet Transport Protocols (1981) dan Request for Comments (RFC) 1058 (1988).

2.4.1 Dasar RIP

RIP adalah protokol routing yang menggunakan metode distance vector, yang menggunakan *hop-count* sebagai *metric routing*. Jumlah maksimum hop yang diijinkan mencapai 15 dan *holddown time* mencapai 180 detik. Secara default, setiap router RIP akan mentransmit update tabel routing setiap 30 detik, dan karena ukuran tabel routing tersebut sangat kecil, maka tidak berpengaruh pada trafik jaringan. Ketika hal ini sudah dibentuk, maka informasi ini akan disimpan dalam tabel routing. Setiap entri dari tabel routing RIP menyediakan banyak informasi, seperti informasi tujuan, hop berikutnya dalam mencapai tujuan, dan sebuah metric. Metric ini mengindikasikan jarak hop antara asal dengan tujuan. Tapi ketika jaringan ini membesar, akan terjadi ledakan paket dahsyat setiap 30 detik, walaupun router diinisialisasikan pada waktu yang random. Implementasi RIP versi terbaru mengenalkan pemvariasian waktu yang disengaja pada update router di setiap router.

Pembatasan jumlah maksimum hop ini juga dimaksudkan untuk membatasi jumlah loop sehingga mencegah terjadinya loop tak terbatas (*infinite loop*), tapi sebaliknya hal ini juga membatasi ukuran jaringan yang bisa disupport oleh RIP.

2.4.2 Mekanisme Kestabilan RIP

Ada tiga jenis mekanisme yang digunakan oleh RIP untuk mencegah terjadinya pentransmisian informasi routing yang salah, yaitu holddown timer, split horizon, dan route poisoning.

- **Holddown Timer**
  Mekanisme ini mencegah dan mengembalikan rute yang menjadi tidak benar ketika router membroadcast update regulernya.
  Ketika sebuah rute down, router tetangga akan mendeteksi dan berusaha untuk membroadcast perubahan rute setelah mereka mengkalkulasikan rute yang baru. Rute yang tertrigger ini mungkin tidak akan sampai pada beberapa router, dan router ini akan tetap membroadcast update reguler dan menyatakan bahwa jalur rute yang telah down tersebut masih dalam kondisi baik.
  Hal seperti ini, peralatan pada hop berikutnya akan mengandung informasi routing yang salah, yang kemudian akan disebarkan lebih lanjut lagi.
  Hold down akan memberi tahu router untuk menahan pada setiap perubahan yang akan berefek pada rute yang baru dihilangkan untuk beberapa waktu lamanya, hingga rute yang baru benar-benar stabil dan ketika holddown timer habis.
- **Split Horizon**
  Sangatlah tidak berguna ketika mengirim informasi tentang sebuah rute kembali ke arah asal informasi itu datang, karena itu split horizon dipakai untuk mencegah update yang redundan dalam jaringan tersebut
- **Poison Reverse**
  Loop routing pada jaringan yang lebih besar bisa dicegah dengan penggunaan poison reverse. Poison reverse update membuat router menyebarkan update untuk mengindikasikan sebuah rute sudah tidak tercapai dengan menggunakan cost sampai 15. Lalu update ini dikirimkan untuk menghapuskan rute yang tidak terpakai tersebut, serta menempatkannya pada hold-down

Kebanyakan problem pada jaringan dengan slow-convergence ditangani dengan metode split-horizon, poison reverse dan trigerred updates. Tapi, bagaimanapun juga RIP tidak bisa meningkatkan ukuran jaringan atau menyebarkan network mask yang diperlukan untuk menterjemahkan rute yang diperlukan. Versi update dari RIP, yang dikenal sebagai RIPv2 memecahkan masalah ini.

2.4.3 RIP Version 2 (RIPv2)

RIP Version 2 (RIPv2) menambahkan *header* "network mask" dan "next hop *header*" pada paket RIP asli sehingga router RIPv2 bisa berdampingan dengan router RIP tanpa masalah. Subnet mask mengandung bit network mask yang diasosiasikan dengan alamat tujuan, sehingga mengijinkan implementasi dari Classless Inter-Domain Routing (CIDR). Hal ini membuat RIP bisa berfungsi di bermacam-macam kondisi jaringan, dimana jaringan tersebut mempunyai banyak variasi subnet mask

Fitur "next hop *header*" menyediakan alamat gateway sekaligus mengijinkan optimisasi rute dalam sebuah lingkungan yang menggunakan banyak protokol routing sehingga mempunyai kemampuan untuk mengerti protokol routing yang lain sehingga kemungkinan menyediakan rute routing yang lebih baik menuju ke tujuan.

Peningkatan lainnya dari RIPv2 adalah adanya mekanisme autentikasi password untuk router RIPv2 untuk mencegah update yang secara tidak sengaja untuk *host* yang salah konfigurasi.

Selain itu, RIPv2 menggunakan multicast dibandingkan dengan broadcast untuk mengurangi beban trafik pada sistem yang tidak mau update dari RIPv2 dan untuk berbagi informasi dimana router RIP-1 tidak akan mengetahuinya. Pada multicast, hanya beberapa *host* yang diam di IP multicast spesifik yang akan mengetahui informasi tersebut.

2.4.4 Routing Information Protocol next generation (RIPng)

RIPng (RIP next generation) adalah salah satu protokol routing yang digunakan dalam IPv6, seperti generasi pendahulunya (RIP&RIPv2) RIPng ini juga memiliki fitur-fitur yang mirip seperti:

- Penggunaan metode distance-vector sebagai metode pencarian jarak terpendek.
- Maksimal jarak yang dapat ditempuh adalah 15 hop, dimana loop ke 16 adalah dianggap tak terbatas.
- Penggunaan metode split horizon, poison reverse, dan holddown timer untuk kestabilan jaringan.

Selain fitur-fitur diatas, RIPng juga memiliki fitur-fitur baru yang diimplementasikan kedalamnya, seperti:

- Penggunaan prefix IPv6, alamat IPv6.
- Menggunakan IPv6 untuk komunikasi data.
- Mengupdate alamat tujuan selanjutnya untuk routing pada port 520 UDP.

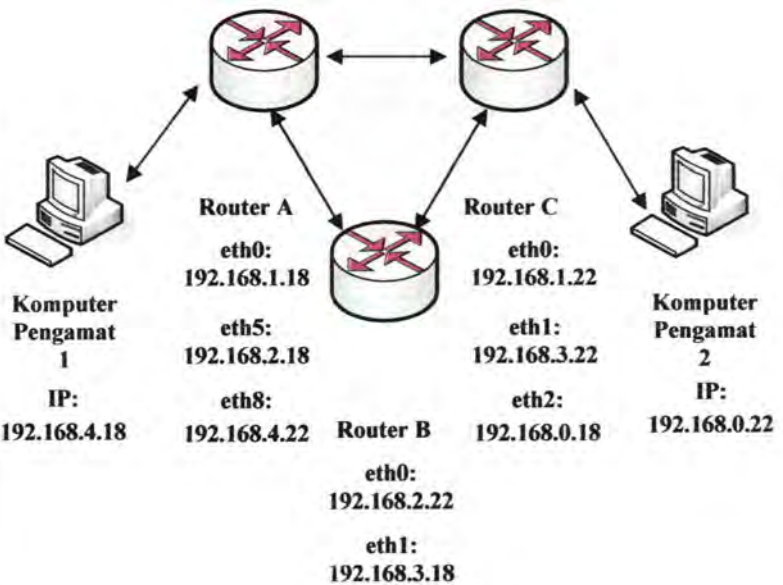
BAB III
PERENCANAAN DAN IMPLEMENTASI

BAB III
PERENCANAAN DAN IMPLEMENTASI

Pada bab ini akan dibahas perancangan jaringan IPv6 dengan menggunakan protokol routing RIPng dan jaringan IPv4 dengan menggunakan protokol routing RIP sebagai pembanding, dimulai dengan perencanaan sistem, persiapan software dan hardware yang diperlukan, instalasi dan konfigurasi jaringan, serta persiapan pengujian.

3.1 Perencanaan Sistem

Pada tugas akhir ini perencanaan sistem secara umum terbagi menjadi dua bagian pokok, yaitu pembuatan jaringan IPv6 dan perencanaan pembuatan jaringan IPv4. Pada sistem yang digunakan dalam Tugas Akhir ini dibutuhkan lima buah komputer, masing-masing komputer berfungsi sebagai 3 router serta 2 client. Seperti topologi yang digambarkan dalam gambar 3.1 sebagai berikut:



Gambar 3.1 Topologi Jaringan

Tabel 3.1 Panjang kabel pada tiap-tiap device

Device Awal	Device Tujuan	Panjang Kabel
Router A	Router B	10 meter
Router B	Router C	10 meter
Router A	Router C	10 meter
Router A	PC 1	10 meter
Router B	PC 2	10 meter

Semua kabel UTP yang terhubung bertipe *crossover*. Pengalamatan IP disesuaikan dengan topologi jaringan pada gambar 3.1 diatas.

3.2 Metodologi Penelitian

Pada tugas akhir ini akan dilakukan 4 kali percobaan untuk masing-masing jaringan dengan IPv4 dan IPv6, yang dapat dilihat pada flowchart dibawah ini:

Gambar 3.2 Metodologi Percobaan

3.3 Kebutuhan Hardware dan Software

Pada topologi jaringan ini mempunyai spesifikasi hardware dan software sebagai berikut:

3.3.1 Kebutuhan Hardware

Kebutuhan hardware pada tugas akhir ini terdiri dari beberapa PC yang berfungsi sebagai client dan *router*.

3.3.1.1 Router

Nama Komputer	: Router A
Processor	: Intel Pentium 4 3GHz
Graphic Card	: Integrated SiS 661FX
Memory	: DDRAM 768 Mb
Sound Card	: Realtek AC'97 Audio
NIC	: 1. Pada eth0 SiS 900 Fast Ethernet Adapter 2. Pada eth5 Intel 82557 Ethernet Pro 100 3. Pada eth8 Realtek RTL 8139 10/100
Operating System	: Linux Ubuntu 8.10

Nama Komputer	: Router B
Processor	: AMD Athlon XP 1800
Graphic Card	: Geforce 2 MX 440
Memory	: DDRAM 256 Mb
Sound Card	: Realtek HD audio output
NIC	: 1. Pada eth0 Realtek RTL 8139 10/100 2. Pada eth1 Marvell Yukon 88E
Operating System	: Linux Debian etch 2.6.16

Nama Komputer	: Router C
BProcessor	: Intel Pentium 4
Graphic Card	: Geforce 2 MX 440
Memory	: DDRAM 256 Mb
Sound Card	: Nforce Audio System
NIC	: 1. Pada eth0 Realtek RTL 8139 10/100 2. Pada eth1 Intel 82557 Ethernet Pro 100 3. Pada eth2 Realtek RTL 8139 10/100
Operating System	: Linux Debian etch 2.6.16

3.3.1.2 Client

Nama Komputer	: Client 1
Processor	: Intel Pentium M 1,2 GHz
Graphic Card	: Intel 82852/82855 Graphics Controller
Memory	: DDRAM 256 Mb
Sound Card	: SoundMAX Digital Audio
NIC	: Intel PRO/100 VE
Operating System	: Windows XP Professional SP 1

Nama Komputer	: Client 2
Processor	: Intel Pentium Celeron M 1,3 GHz
Graphic Card	: Intel 82852/82855 Graphics Controller
Memory	: DDRAM 256 Mb
NIC	: Intel Realtek RTL 8139 10/100
Operating System	: Windows XP Professional SP 2

3.3.2 Kebutuhan Software

Software yang digunakan pada tugas akhir ini meliputi Ping, Traceroute, Iperf, Quagga, dan Putty.

3.3.2.1 Iperf

Iperf adalah software berbasis console yang digunakan untuk membangkitkan traffic udp dan tcp atau *traffic generator*, iperf berjalan pada model client-server, server iperf membangkitkan traffic udp pada sisi client.

Iperf ini bisa digunakan untuk menganalisa jaringan komputer, karena bisa menghasilkan data-data yang digunakan untuk menganalisa jaringan komputer, seperti throughput, packet loss, dan delay.

3.3.2.2 Quagga

Quagga adalah software router yang digunakan seperti halnya fungsi sebuah router pada PC, sehingga tidak diperlukan untuk membeli router yang harganya mahal, karena sifatnya yang freeware.

Tampilan konsol quagga ini mirip dengan Cisco Router, sehingga jika sudah terbiasa dengan Router Cisco, maka tidak akan kesulitan untuk mengoperasikan Quagga. Begitu juga sebaliknya jika lebih familiar dengan Quagga, maka tidak akan kesulitan mengoperasikan Router Cisco.

3.4 Instalasi Infrastruktur

Pada bagian ini akan dibahas mengenai proses instalasi protokol routing RIP pada IPv4 dan protokol routing RIPng pada IPv6 serta pengalamatan IP pada masing-masing topologi jaringan.

3.4.1 Konfigurasi Router IPv4

Dalam mengkonfigurasi sebuah PC Router maka digunakan paket program aplikasi yaitu quagga untuk melakukan instalasi paket program tersebut digunakan perintah :

```
# sudo apt-get install quagga
```

Lalu, setelah menginstall router tersebut, maka langkah selanjutnya adalah pengaktifkan daemon protokol routing pada router tersebut dengan menggunakan perintah:

```
# sudo pico /etc/quagga/daemons
```

Lalu tinggal mengubah nilai protokol routing yang dikehendaki dari "no" menjadi "yes", pada tugas akhir ini akan digunakan protokol routing RIP dan RIPng, maka dari itu akan diubah nilai RIP dan RIPng dari "no" menjadi "yes" dan tentu saja nilai zebra dari "no" menjadi "yes" karena zebra adalah daemon router yang akan digunakan. Contoh:

```
Zebra = no
RIP = no
```

Menjadi,

```
Zebra = yes
RIP = yes
```

Selain itu, juga akan disalin file zebra.conf.sample, ripd.conf.sample dan ripngd.conf.sample dengan menggunakan perintah:

```
# sudo cp /usr/share/doc/quagga/examples/
zebra.conf.sample /etc/quagga/zebra.conf
```

```
# sudo cp /usr/share/doc/quagga/examples/
ripd.conf.sample /etc/quagga/ripd.conf
```

```
# sudo cp /usr/share/doc/quagga/examples/
ripngd.conf.sample /etc/quagga/ripngd.conf
```

Lalu, setelah itu daemon protokol routing bisa dihentikan terlebih dahulu

```
# sudo /etc/init.d/quagga stop
```

Maka akan muncul hasil seperti ini:

```
Stopping Quagga daemons (prio:0): (ripd)
(waiting) .. zebra (bgpd) (waiting) .. ripngd
(ospfd) (ospf6d) (isisd).
Removing all routes made by zebra.
```

Lalu, setelah itu daemon protokol routing bisa diaktifkan sesuai dengan yang dikehendaki dengan perintah

```
# sudo /etc/init.d/quagga start
```

Maka akan muncul hasil seperti berikut:

```
Loading capability module if not yet done.
Starting Quagga daemons (prio:10): zebra ripd.
```

Lalu, untuk melakukan pengecekan port yang digunakan oleh protokol routing tersebut maka bisa digunakan perintah netstat pada router tersebut.

```
# sudo netstat -nlptu | grep zebra
```

```
# sudo netstat -nlptu | grep ripd
```

Jika keluar hasil seperti ini maka protokol routing sudah berjalan

```
tcp 0 0 127.0.0.1:2601 0.0.0.0 LISTEN 6152/zebra
```

```
tcp 0 0 127.0.0.1:2602 0.0.0.0 LISTEN 6156/ripd
udp 0 0 0.0.0.0:520    0.0.0.0        6156/ripd
```

Dapat dilihat dihasil bahwa port zebra pada 2601 dan port ripd pada 2602. Lalu, router zebra bisa dijalankan untuk konfigurasi lebih lanjut dengan menggunakan perintah telnet.

```
# telnet localhost zebra
```

Maka, akan muncul hasil seperti ini:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is Quagga (version 0.99.9).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
Router>
```

Pada router quagga ini menggunakan perintah-perintah yang mirip dengan router cisco, sehingga yang sudah mengetahui perintah cisco tidak akan kesulitan menggunakan quagga ini.

Sebelum diberikan alamat IP pada router-A, terlebih dahulu akan diaktifkan IP forwarding dengan menggunakan perintah:

```
# sudo echo '1' > /proc/sys/net/ipv4/ip_forward
```

Lalu alamat IP bisa diberikan pada masing-masing router dengan menggunakan perintah:

```
# sudo pico /etc/network/interfaces
```

Pada router-A alamat IP yang perlu dikonfigurasi adalah sebagai berikut:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.18
netmask 255.255.255.0
gateway 192.168.1.22

auto eth5
iface eth5 inet static
address 192.168.2.18
netmask 255.255.255.0
gateway 192.168.2.22

auto eth8
iface eth8 inet static
address 192.168.4.22
netmask 255.255.255.0
gateway 192.168.4.22
```

Lalu setelah pemberian IP selesai, konfigurasi jaringan bisa direstart dengan perintah:

```
# sudo /etc/init.d/networking restart
```

Setelah pemberian IP selesai, alamat IP bisa dikonfigurasi dengan masuk ke router zebra dan menggunakan perintah:

```
Router-A>enable
Router-A# conf t
Router-A(config)# int eth0
Router-A(config-if)# ip address 192.168.1.18/24
Router-A(config-if)# no shut
Router-A(config-if)# exit
Router-A(config)# int eth5
Router-A(config-if)# ip address 192.168.2.18/24
Router-A(config-if)# no shut
Router-A(config-if)# exit
Router-A(config)# int eth8
Router-A(config-if)# ip address 192.168.4.22/24
Router-A(config-if)# no shut
Router-A(config-if)# exit
Router-A(config)# exit
Router-A# wr mem
Configuration saved to /etc/quagga/zebra.conf
```

Lalu setelah selesai mengkonfigurasi zebra, bisa dilanjutkan ke konfigurasi ripd, dengan menggunakan perintah:

```
# telnet localhost ripd
```

Maka akan muncul, hasil seperti berikut:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is Quagga (version 0.99.9).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password:
ripd>
```

Untuk konfigurasi ripd lebih lanjut dengan menggunakan perintah:

```
ripd> enable
ripd# conf t
ripd(config)# router rip
ripd(config-router)# network 192.168.1.0/24
ripd(config-router)# network eth0
ripd(config-router)# network 192.168.2.0/24
ripd(config-router)# network eth5
ripd(config-router)# network 192.168.4.0/24
ripd(config-router)# network eth8
ripd(config-router)# exit
ripd# wr mem
Configuration saved to /etc/quagga/ripd.conf
```

Dengan demikian, setting quagga untuk router-A telah selesai, akan dilanjutkan dengan setting quagga untuk router-B. Pada router-B akan dikonfigurasi dengan alamat IP sebagai berikut

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.2.22
netmask 255.255.255.0
gateway 192.168.2.18

auto eth1
iface eth1 inet static
address 192.168.3.18
netmask 255.255.255.0
gateway 192.168.3.22
```

Lalu, tidak lupa pengaktifan ip forward pada router-B dengan menggunakan perintah:

```
# sudo echo '1' > /proc/sys/net/ipv4/ip_forward
```

Dan setelah itu, jaringan router-B bisa direstart dengan perintah:

```
# sudo /etc/init.d/networking restart
```

Setelah itu, zebra dan ripd bisa dikonfigurasi pada router-B dengan menggunakan perintah:

```
Router-B# conf t
Router-B(config)# int eth0
Router-B(config-if)# ip address 192.168.2.22/24
Router-B(config-if)# no shut
Router-B(config-if)# exit
Router-B(config)# int eth1
Router-B(config-if)# ip address 192.168.3.18/24
Router-B(config-if)# no shut
Router-B(config-if)# exit
Router-B(config)# exit
Router-B# wr mem
Configuration saved to /etc/quagga/zebra.conf
```

```
ripd> en
ripd# conf t
ripd(config)# router rip
ripd(config-router)# network 192.168.2.0/24
ripd(config-router)# network eth0
ripd(config-router)# network 192.168.3.0/24
ripd(config-router)# network eth1
ripd(config-router)# exit
ripd# wr mem
Configuration saved to /etc/quagga/ripd.conf
```

Lalu setelah pengkonfigurasian router-B selesai, router-C bisa dikonfigurasi dengan alamat IP sebagai berikut:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.22
netmask 255.255.255.0
gateway 192.168.1.18

auto eth1
iface eth1 inet static
address 192.168.3.22
netmask 255.255.255.0
gateway 192.168.3.18

auto eth2
iface eth2 inet static
address 192.168.0.18
netmask 255.255.255.0
gateway 192.168.0.18
```

Lalu, tidak lupa pengaktifan ip forward pada router-C dengan menggunakan perintah:

```
# sudo echo '1' > /proc/sys/net/ipv4/ip_forward
```

Dan setelah itu, jaringan router-C bisa direstart dengan perintah:

```
# sudo /etc/init.d/networking restart
```

Setelah itu, zebra dan ripd bisa dikonfigurasi pada router-C dengan menggunakan perintah:

```
Router-C>enable
Router-C# conf t
Router-C(config)# int eth0
Router-C(config-if)# ip address 192.168.1.22/24
Router-C(config-if)# no shut
Router-C(config-if)# exit
Router-C(config)# int eth1
Router-C(config-if)# ip address 192.168.3.22/24
Router-C(config-if)# no shut
Router-C(config-if)# exit
Router-C(config)# int eth2
Router-C(config-if)# ip address 192.168.0.18/24
Router-C(config-if)# no shut
Router-C(config-if)# exit
Router-C(config)# exit
Router-C# wr mem
Configuration saved to /etc/quagga/zebra.conf
```

```
ripd> enable
ripd# conf t
ripd(config)# router rip
ripd(config-router)# network 192.168.1.0/24
ripd(config-router)# network eth0
ripd(config-router)# network 192.168.3.0/24
ripd(config-router)# network eth1
ripd(config-router)# network 192.168.0.0/24
ripd(config-router)# network eth2
ripd(config-router)# exit
ripd# wr mem
Configuration saved to /etc/quagga/ripd.conf
```

Jika semua router sudah selesai terkonfigurasi, maka bisa dicoba tes koneksi dengan perintah ping dan traceroute dari PC 1 ke PC 2 atau sebaliknya, jika muncul hasil seperti ini, maka jaringan sudah terhubung

```
C:\Documents and Settings\The Zero Day>tracert
192.168.0.22

Tracing route to 192.168.0.18 over a maximum of
30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.4.22
  2    <1 ms    <1 ms    <1 ms  192.168.0.22
```

```
C:\Documents and Settings\The Zero Day>ping
192.168.0.22
PING 192.168.0.22 with 32 bytes of data.
32 bytes from 192.168.0.22: icmp_seq=1 ttl=64
time <1ms
32 bytes from 192.168.0.22: icmp_seq=2 ttl=64
time <1ms
32 bytes from 192.168.0.22: icmp_seq=3 ttl=64
time <1ms
32 bytes from 192.168.0.22: icmp_seq=4 ttl=64
time <1ms
```

3.4.2 Konfigurasi Router IPv6

Untuk mengkonfigurasi IPv6 pada router tidak banyak dilakukan banyak perubahan pada sistem router tersebut, adapun konfigurasi jaringan yang dugunakan mirip dengan konfigurasi jaringan dengan menggunakan IPv4, hanya saja berbeda pada penggunaan alamat IP, seperti yang tertera pada tabel berikut:

Tabel 3.2 Konfigurasi Alamat IPv6

Device	Interface	Alamat IPv6
Router-A	eth0	2001:200:830::2
	eth5	2001:200:800::2
	eth8	2001:200:831::1
Router-B	eth0	2001:200:800::3
	eth1	2001:200:810::2
Router-C	eth0	2001:200:830::3
	eth1	2001:200:810::3
	eth2	2001:200:840::1
PC-1	eth0	2001:200:831::2
PC-2	eth0	2001:200:840::2

Pertama kali yang harus dilakukan adalah melakukan pengecekan apakah OS linux tersebut sudah mendukung IPv6, dilakukan dengan perintah

```
# test -f /proc/net/if_inet 6 && echo "ada IPv6"
```

Lalu mestinya jika mendukung IPv6 akan muncul hasil seperti ini:

```
ada Ipv6
```

Jika tidak muncul hasil tersebut, maka modul IPv6 perlu dimasukkan terlebih dahulu kedalam sistem yaitu dengan perintah:

```
# modprobe IPv6
```

Untuk melihat apakah modul IPv6 sudah dimasukkan, bisa menggunakan perintah:

```
# lsmod | grep -w "IPv6" && echo "modul ipv6
ada"
```

Lalu untuk konfigurasi quagga, pertama-tama harus dikonfigurasi terlebih dahulu daemon dari quagga tersebut, dan mengubah protokol routing yang digunakan dari RIP menjadi RIPng.

```
# sudo pico /etc/quagga/daemons
```

```
Zebra = no
RIPng = no
```

Menjadi

```
Zebra = yes
RIPng = yes
```

Lalu, setelah itu bisa dihentikan daemon protokol routingnya

```
# sudo /etc/init.d/quagga stop
```

Maka akan muncul hasil seperti ini:

```
Stopping Quagga daemons (prio:0): (ripd)
(waiting) .. zebra (bgpd) (waiting) .. ripngd
(ospfd) (ospf6d) (isisd).
Removing all routes made by zebra.
```

Lalu, setelah itu daemon protokol routing bisa diaktifkan sesuai dengan yang dikehendaki dengan perintah

```
# sudo /etc/init.d/quagga start
```

Maka akan muncul hasil seperti berikut:

```
Loading capability module if not yet done.
Starting Quagga daemons (prio:10): zebra ripngd.
```

Lalu, untuk melakukan pengecekan port yang digunakan oleh protokol routing RIPng tersebut maka bisa digunakan perintah netstat pada router tersebut.

```
# sudo netstat -nlptu | grep ripngd
```

Jika keluar hasil seperti ini maka protokol routing RIPng sudah berjalan

```
tcp6 0 127.0.0.1:2603 0.0.0.0 LISTEN 6156/ripngd
udp6 0 0.0.0.0:520    0.0.0.0        6156/ripngd
```

Sebelum diberikan alamat pada router-A, terlebih dahulu akan diaktifkan IP forwarding pada IPv6 dengan menggunakan perintah:

```
# sudo echo "1" >
/proc/sys/net/ipv6/conf/all/forwarding
```

Lalu bisa diberikan alamat IP pada masing-masing router dengan menggunakan perintah:

```
# sudo pico /etc/network/interfaces
```

Pada router-A alamat IP yang perlu dikonfigurasi adalah sebagai berikut:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet6 static
address 2001:200:830::2
netmask 64

auto eth5
iface eth5 inet6 static
address 2001:200:800::2
netmask 64

auto eth8
iface eth8 inet6 static
address 2001:200:831::1
netmask 64
```

Lalu setelah pemberian IP selesai, konfigurasi jaringan bisa direstart dengan perintah:

```
# sudo /etc/init.d/networking restart
```

Setelah pemberian IP selesai, zebra bisa dimasuki untuk dikonfigurasi alamat IP dengan menggunakan perintah:

```
Router-A>enable
Router-A# conf t
Router-A(config)# int eth0
Router-A(config-if)# ipv6 address
2001:200:830::2/64
Router-A(config-if)# no shut
Router-A(config)# int eth5
Router-A(config-if)# ipv6 address
2001:200:800::2/64
Router-A(config-if)# no shut
Router-A(config)# int eth8
Router-A(config-if)# ipv6 address
2001:200:831::1/64
Router-A(config-if)# no shut
```

Lalu setelah selesai mengkonfigurasi zebra, bisa dilanjutkan ke konfigurasi ripngd, dengan menggunakan perintah:

```
ripngd> enable
ripngd# conf t
ripngd(config)# router ripng
ripngd(config-router)# network 2001:200:830::/64
ripngd(config-router)# network eth0
ripngd(config-router)# network 2001:200:800::/64
ripngd(config-router)# network eth5
ripngd(config-router)# network 2001:200:831::/64
ripngd(config-router)# network eth8
ripngd(config-router)# exit
ripngd# wr mem
Configuration saved to /etc/quagga/ripngd.conf
```

Dengan demikian, setting quagga untuk IPv6 pada router-A telah selesai, akan dilanjutkan dengan setting quagga untuk IPv6 pada router-B. Pada router-B akan dikonfigurasi dengan alamat IP sebagai berikut

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet6 static
address 2001:200:800::3
netmask 64

auto eth1
iface eth1 inet6 static
address 2001:200:810::2
netmask 64
```

Lalu, tidak lupa pengaktifan ip forward pada router-B dengan menggunakan perintah:

```
# sudo echo "1" >
/proc/sys/net/ipv6/conf/all/forwarding
```

Dan setelah itu, jaringan router-B bisa direstart dengan perintah:

```
# sudo /etc/init.d/networking restart
```

Setelah selesai, dilanjutkan dengan konfigurasi zebra dan ripngd pada router-B dengan menggunakan perintah:

```
Router-B(config)# int eth0
Router-B(config-if)# ipv6 address
2001:200:800::3/64
Router-B(config-if)# no shut
Router-B(config-if)# exit
Router-B(config)# int eth1
Router-B(config-if)# ipv6 address address
2001:200:810::2/64
Router-B(config-if)# no shut
```

Lalu setelah selesai mengkonfigurasi zebra, bisa dilanjutkan ke konfigurasi ripngd, dengan menggunakan perintah:

```
ripngd> enable
ripngd# conf t
ripngd(config)# router ripng
ripngd(config-router)# network 2001:200:800::/64
ripngd(config-router)# network eth0
ripngd(config-router)# network 2001:200:810::/64
ripngd(config-router)# network eth1
```

Dengan demikian, setting quagga untuk IPv6 pada router-B telah selesai, akan dilanjutkan dengan setting quagga untuk IPv6 pada router-C. Pada router-B akan dikonfigurasi dengan alamat IP sebagai berikut

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet6 static
address 2001:200:830::3
netmask 64
auto eth1
iface eth1 inet6 static
address 2001:200:810::3
netmask 64
auto eth2
iface eth2 inet6 static
address 2001:200:840::1
netmask 64
```

Lalu, tidak lupa pengaktifan ip forward pada router-C dengan menggunakan perintah:

```
# sudo echo "1" >
/proc/sys/net/ipv6/conf/all/forwarding
```

Dan setelah itu, jaringan router-C direstart dengan perintah:

```
# sudo /etc/init.d/networking restart
```

Setelah itu, zebra dan ripngd pada router-C bisa dikonfigurasi dengan menggunakan perintah:

```
Router-C>enable
Router-C# conf t
Router-C(config)# int eth0
Router-C(config-if)# ipv6 address
2001:200:830::3/64
Router-C(config-if)# no shut
Router-C(config-if)# exit
Router-C(config)# int eth1
Router-C(config-if)# ipv6 address
2001:200:810::3/64
Router-C(config-if)# no shut
Router-C(config-if)# exit
Router-C(config)# int eth2
Router-C(config-if)# ipv6 address
2001:200:840::1/64
Router-C(config-if)# no shut
Router-C(config-if)# exit
Router-C(config)# exit
```

Lalu setelah selesai mengkonfigurasi zebra, bisa dilanjutkan ke konfigurasi ripngd, dengan menggunakan perintah:

```
ripngd> enable
ripngd# conf t
ripngd(config)# router ripng
ripngd(config-router)# network 2001:200:830::/64
ripngd(config-router)# network eth0
ripngd(config-router)# network 2001:200:810::/64
ripngd(config-router)# network eth1
ripngd(config-router)# network 2001:200:840::/64
ripngd(config-router)# network eth2
```

Lalu jika setting IPv6 pada semua router sudah selesai, maka bisa dilanjutkan dengan setting IPv6 di sisi klien yang menggunakan Windows XP. Di setting default, Windows XP tidak menggunakan IPv6, melainkan IPv4, tapi jika ingin menggunakan IPv6 bisa diinstall dengan perintah:

```
C:\ipv6 install
Installing...
Succeeded.
```

Setelah itu dengan perintah "ipv6 if" akan terlihat konfigurasi alamat dan interface ipv6 pada komputer, dan bisa dilakukan pengalamatan pada interface ethernet berdasarkan hasil dari "ipv6 if" tersebut, semisal salah satu bagian dari hasil "ipv6 if" adalah:

```
Interface 6: Ethernet: Local Area Connection
  Guid {0E88C316-A27B-4899-A5E1-7C9DB0E4A727}
  uses Neighbor Discovery
  uses Router Discovery
  link-layer address: 00-08-02-94-d0-43
preferred link-local fe80::208:2ff:fe94:d043,
life infinite
   link MTU 1500 (true link MTU 1500)
 current hop limit 64
  reachable time 23500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 1
  default site prefix length 48
```

"interface 6", maka bisa dilakukan assign alamat IPv6 pada interface tersebut dengan perintah:

```
C:\ipv6 adu "nomor interface"/"alamat IPv6"
```

Atau jika dimisalkan adalah sebagai berikut dengan mengambil contoh diatas:

```
C:\ipv6 adu 6/2001:200:831::2
```

Setelah itu, bisa diset gateway address IPv6 untuk komputer client Windows XP dengan menggunakan perintah:

```
C:\ipv6 rtu ::/0 6/2001:200:831::1
```

Arti perintah tersebut diatas adalah, rute default (::/0) pada interface 6 adalah alamat IP 2001:200:831::1. Lalu rute tersebut bisa dicek secara manual dengan menggunakan perintah "netsh", lalu "interface ipv6" dan "show route", tampilan dari perintah tersebut adalah seperti berikut

```
C:\Documents and Settings\The Zero Day>netsh
netsh>interface ipv6
netsh interface ipv6>show route
Querying active state...

Publish Type Met Prefix Idx Gateway/Interface
---- -------- ---- ----------------------
no     Manual 0    ::/0   6   2001:200:831::1
```

Jika semua router sudah selesai terkonfigurasi, maka bisa dicoba tes koneksi dengan perintah ping dan traceroute dari PC 1 ke PC 2 atau sebaliknya, jika muncul hasil seperti ini, maka jaringan sudah terhubung

```
C:\Documents and Settings\The Zero Day>tracert6
2001:200:840::2

Tracing route to 2001:200:840::1 over a maximum
of 30 hops

1    <1 ms    <1 ms    <1 ms  2001:200:831::1
2    <1 ms    <1 ms    <1 ms  2001:200:840::2
```

```
C:\Documents and Settings\The Zero Day>ping6
2001:200:840::2
PING 2001:200:840::2 with 32 bytes of data.
32 bytes from 2001:200:840::2: icmp_seq=1
ttl=64 time <1ms
32 bytes from 2001:200:840::2: icmp_seq=2
ttl=64 time <1ms
32 bytes from 2001:200:840::2: icmp_seq=3
ttl=64 time <1ms
```

3.5 Pemberian Beban pada Jaringan

Pemberian beban pada jaringan dapat dilakukan dengan menggunakan menggunakan software iperf. Iperf adalah software berbasis console yang digunakan untuk membangkitkan trafik udp dan tcp, iperf berjalan pada model client-server, server iperf membangkitkan trafik udp atau tcp pada sisi client. Proses pembangkitan TCP dan UDP dari sisi client dan server adalah sebagai berikut :

3.5.1 Beban TCP

Untuk membangkitkan beban TCP pada server digunakan perintah adalah sebagai berikut :

```
C:\>iperf -s
------------------------------------------------
Server listening on TCP port 5001
TCP window size: 8 KByte (default)
------------------------------------------------
[4] local 10.122.69.45 port 5001 connected with
192.168.5.10
[ID] Interval Transfer Bandwidth
[4] 0.0-0.0 sec 50 KBytes 39.6 Kbits/sec
```

Sedangkan untuk membangkitkan beban 50 KBytes pada sisi client digunakan perintah adalah sebagai berikut :

```
C:\> iperf -n 50K -c 10.122.69.45
------------------------------------------------
Client connecting to 10.122.69.45 TCP port 5001
TCP window size: 8.0 KByte (default)
------------------------------------------------
[3]local 10.122.69.45 port 1779 connected with
192.168.5.10
[ID] Interval Transfer Bandwidth
[3] 0.0-0.0 sec 56 KBytes 34.2 Kbits/sec
```

3.5.2 Beban UDP

Untuk membangkitkan beban UDP pada server digunakan perintah adalah sebagai

```
C:\>iperf -s -u
------------------------------------------
Server listening on UDP port 5001
UDP window size: 8 KByte (default)
------------------------------------------
[4] local 10.122.69.45 port 5001 connected with
192.168.5.25
[ID] Interval Transfer Bandwidth
[4] 0.0-0.0 sec 104 KBytes 39.6 Kbits/sec
```

Sedangkan untuk membangkitkan beban 100 KBytes pada sisi client ligunakan perintah adalah sebagai berikut :

```
C:\> iperf -n 100k -c 10.122.69.45 -u -i 1
------------------------------------------
Client connecting to 10.122.69.45 UDP port 5001
UDP window size: 8.0 KByte (default)
------------------------------------------
[3]local 10.122.69.45 port 1778 connected with
192.168.5.25
[ID] Interval Transfer Bandwidth
[3] 0.0-0.0 sec 102 KBytes 34.2 Kbits/sec
```

BAB IV
ANALISA DATA DAN PEMBAHASAN

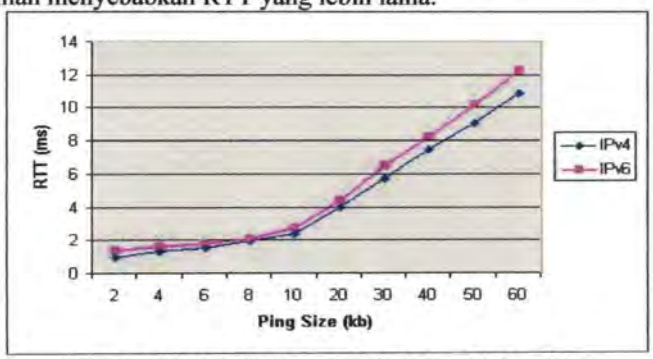
BAB IV
ANALISA DATA DAN PEMBAHASAN

Pada bab 4 ini akan dilakukan Analisa Perbandingan Kinerja Protokol Routing RIPng pada jaringan IPv6 dengan Protokol Routing RIP pada jaringan IPv4. Parameter yang diukur adalah *Round Trip Delay, Packet Loss, Throughput, Jitter.* Pengukuran dilakukan menggunakan software jaringan seperti ping, traceroute dan iperf. Ping adalah tool software yang digunakan untuk mengecek kondisi link jaringan antar host, dan monitoring jaringan. Traceroute adalah software yang digunakan untuk melihat jalur-jalur yang dilewati oleh paket dalam perjalanan dari host asal ke host tujuan. Iperf adalah software berbasis console yang digunakan untuk membangkitkan traffic udp dan tcp atau *traffic generator*, iperf berjalan pada model client-server, server iperf membangkitkan traffic udp pada sisi client. Iperf ini bisa digunakan untuk menganalisa jaringan komputer, karena bisa menghasilkan data-data yang digunakan untuk menganalisa jaringan komputer, seperti throughput, packet loss, dan jitter.

4.1 Pengukuran Round Trip Delay

Round Trip Delay atau biasa juga disebut Round Trip Time adalah waktu yang diperlukan oleh sebuah pulse atau paket data untuk mencapai tujuan tertentu dan kembali lagi ke asal. Sumber adalah computer atau system yang menginisiasi sinyal dan tujuan adalah computer atau system yang menerima sinyal dan mengirim kembali sinyal tersebut ke asal.

Pada pengukuran RTT ini dilakukan dengan cara melakukan mengirimkan paket ICMP dari Router-A menuju PC-2 pada jaringan IPv4 dan jaringan IPv6. Melalui gambar 4.1 terlihat bahwa trend RTT antara IPv4 dan IPv6 adalah mirip. Ukuran paket yang lebih besar waktu pengiriman menyebabkan RTT yang lebih lama.



Gambar 4.1. Grafik Round Trip Delay IPv4 vs IPv6

Tabel 4.1 Round Trip Delay

Ping Size (kb)	Delay (ms)	
	IPv4	IPv6
default	0.3214	0.246
2	0.952	1.41
4	1.317	1.602
6	1.546	1.835
8	1.958	2.104
10	2.35	2.741
20	3.982	4.359
30	5.697	6.46
40	7.451	8.199
50	9.055	10.153
60	10.874	12.237

Dari hasil pengukuran, didapatkan selisih dalam pengukuran dari delay IPv4 dan IPv6 sekitar 5-15 ms, dimana ukuran header IPv6 lebih besar 2 kali daripada header IPv4.

4.2 Pengujian dan analisa RIP dan RIPng

Untuk menguji apakah protokol RIP dan RIPng sudah berjalan, pastikan dulu sebelumnya hal-hal dibawah ini:

- Daemon quagga sudah berjalan.
- Tabel routing dari setiap router.
- Lakukan traceroute dari PC-1 ke PC-2 untuk melihat apakah routing sudah berjalan. Seperti yang ditunjukkan hasil:

IPv4

```
C:\Documents and Settings\The Zero Day>tracert
192.168.0.22

Tracing route to 192.168.0.18 over a maximum of
30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.4.22
  2    <1 ms    <1 ms    <1 ms  192.168.0.22
Trace complete.
```

IPv6

```
C:\Documents and Settings\The Zero Day>tracert6
2001:200:840::2

Tracing route to 2001:200:840::1 over a maximum
of 30 hops

1    <1 ms    <1 ms    <1 ms  2001:200:831::1
2    <1 ms    <1 ms    <1 ms  2001:200:840::2

Trace complete.
```

Selain itu, kita juga bisa menampilkan hasil dari daemon quagga pada Router-A untuk melihat apakah routing sudah berjalan pada jaringan IPv4 dan IPv6

IPv4

```
Router-A> sh ip route
Codes: K - kernel route, C - connected, S -
static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, *
- FIB route

K>* 0.0.0.0/0 via 192.168.4.22, eth8
C>* 127.0.0.0/8 is directly connected, lo
R>* 192.168.0.0/24 [120/2] via 192.168.1.22,
eth0, 00:58:13
C>* 192.168.1.0/24 is directly connected, eth0
C>* 192.168.2.0/24 is directly connected, eth5
R>* 192.168.3.0/24 [120/2] via 192.168.1.22,
eth0, 00:58:19
C>* 192.168.4.0/24 is directly connected, eth8
```

IPv6

```
Router-A> sh ipv6 route
Codes: K - kernel route, C - connected, S -
static, R - RIPng, O - OSPFv3,
       I - ISIS, B - BGP, * - FIB route.
C>* ::1/128 is directly connected, lo
C>* 2001:200:800::/64 is directly connected,
eth5
R>* 2001:200:810::/64 [120/2] via
fe80::205:5dff:fe78:9775, eth5, 02:17:44
C>* 2001:200:830::/64 is directly connected,
eth0
C>* 2001:200:831::/64 is directly connected,
eth8
R>* 2001:200:840::/64 [120/2] via
fe80::202:44ff:fe24:6597, eth0, 02:02:15
C * fe80::/64 is directly connected, eth8
C * fe80::/64 is directly connected, eth5
C>* fe80::/64 is directly connected, eth0
```

Ketika jaringan Router-A dan Router-C diputus maka secara otomatis jaringan akan membentuk rute baru yang menghubungkan PC-1 dan PC-2 dengan melewati Router-B , dapat dilihat hasilnya sebagai berikut:

IPv4

```
C:\Documents and Settings\The Zero Day>tracert
192.168.0.22

Tracing route to 192.168.0.18 over a maximum of
30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.4.22
  2    <1 ms    <1 ms    <1 ms  192.168.2.22
  3    <1 ms    <1 ms    <1 ms  192.168.0.22
Trace complete.
```

IPv6

```
C:\Documents and Settings\The Zero Day>tracert6
2001:200:840::2

Tracing route to 2001:200:840::1 over a maximum
of 30 hops

1    <1 ms    <1 ms    <1 ms  2001:200:831::1
2    <1 ms    <1 ms    <1 ms  2001:200:800::3
3    <1 ms    <1 ms    <1 ms  2001:200:840::2

Trace complete.
```

Selain itu, kita juga bisa menampilkan hasil dari daemon quagga pada Router-A untuk melihat apakah routing sudah berjalan pada jaringan IPv4 dan IPv6 pada pembentukan rute jaringan baru.

IPv4

```
Router-A> sh ip route
Codes: K - kernel route, C - connected, S -
static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, *
- FIB route

K>* 0.0.0.0/0 via 192.168.4.22, eth8
C>* 127.0.0.0/8 is directly connected, lo
R>* 192.168.0.0/24 [120/3] via 192.168.2.22,
eth5, 00:09:47
R>* 192.168.1.0/24 [120/3] via 192.168.2.22,
eth5, 00:09:47
C>* 192.168.2.0/24 is directly connected, eth5
R>* 192.168.3.0/24 [120/2] via 192.168.1.22,
eth0, 00:58:19
C>* 192.168.4.0/24 is directly connected, eth8
```

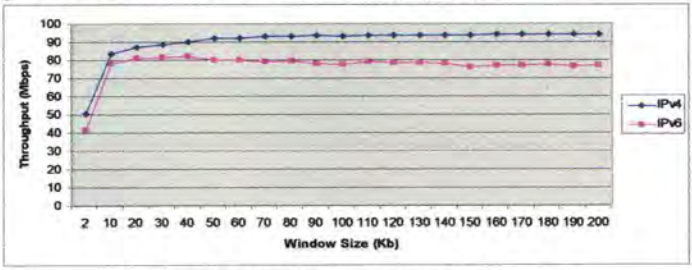
IPv6

```
Router> sh ipv6 route
Codes: K - kernel route, C - connected, S -
static, R - RIPng, O - OSPFv3,
       I - ISIS, B - BGP, * - FIB route.
C>* ::1/128 is directly connected, lo
C>* 2001:200:800::/64 is directly connected,
eth5
R>* 2001:200:810::/64 [120/2] via
fe80::205:5dff:fe78:9775, eth5, 00:00:01
C>* 2001:200:831::/64 is directly connected,
eth8
R>* 2001:200:840::/64 [120/3] via
fe80::205:5dff:fe78:9775, eth5, 00:00:01
C * fe80::/64 is directly connected, eth8
C>* fe80::/64 is directly connected, eth5
```

Dari hasil diatas, maka didapatkan hasil berupa rute terpendek pada jaringan normal, dengan 2 hop dan tidak melewati Router-B, dan jika terjadi abnormalitas pada jaringan Router-A—Router-C maka rute baru terbentuk pada tabel routing dengan melewati Router-B dan Router-A ke Router-C menjadi 3 hop, dengan demikian bisa dikatakan bahwa Protokol Routing Dinamis RIP dan RIPng telah berhasil dijalankan.

4.3 Pengukuran Throughput

Throughput adalah jumlah data per detik yang bisa diterima oleh suatu terminal pada jaringan. Throughput dinyatakan dalam bit per second (bps). Pengukuran kali ini dilakukan dengan cara menjalankan software iperf pada PC-1 sebagai trafik generator dan dijalankan pada 3 router yang terdapat pada jaringan untuk mengambil data throughput pada masing-masing router dan membuat rata-rata throughputnya.



Gambar 4.2 Grafik Throughput IPv4 vs IPv6

Tabel 4.2. Throughput

Window Size (Kb)	THROUGHPUT (Mbps)	
	IPv4	IPv6
2	50.6	41.6
10	83.4	77.9
20	86.8	81
30	88.3	81.4
40	89.9	81.8
50	92.1	80
60	91.8	79.9
70	93.2	79
80	93.1	79.4
90	93.3	78
100	93.2	77.6
110	93.4	78.9
120	93.4	78.5
130	93.6	78.4
140	93.6	78.2
150	93.7	76.2
160	93.9	76.9
170	93.8	77
180	93.9	77.3
190	94.1	76.7
200	94.1	77

Dari hasil pengukuran, didapatkan hasil bahwa throughput dari IPv4 lebih baik daripada IPv6, dimana rata-rata throughput IPv4 adalah 90.15 Mbps dan rata-rata throughput IPv6 adalah 76.80 Mbps. Terdapat perbedaan kemampuan IPv4 dan IPv6 sebesar 14.81%.

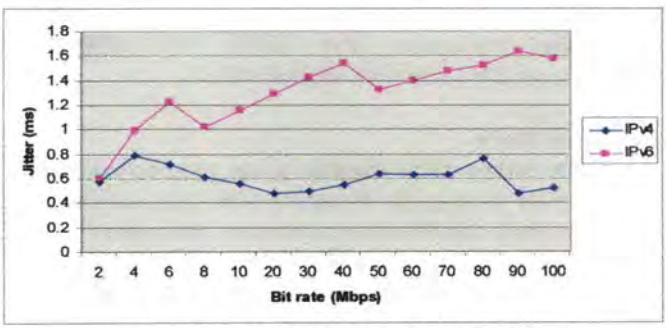
4.4 Pengukuran Jitter

Jitter adalah variasi delay diantara paket yang terjadi dalam suatu aliran paket data pada jaringan IP. Besarnya nilai jitter sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (congestion) yang ada dalam jaringan IP. Semakin besar beban trafik yang terdapat pada jaringan, maka semakin besar pula peluang terjadinya congestion, sehingga kemungkinan nilai jitter akan semakin besar.

Dalam pengukuran jitter ini menggunakan paket UDP pada trafik generator iperf, karena pada umumnya jitter digunakan untuk perhitungan pada RTP (Realtime Transport Protocol) pada aplikasi voice dan video selain pada pengiriman paket data biasa. Selain itu jika dijalankan pada udp, kemungkinan recovery paket tidak ada sehingga akan tercatat langsung hasil jitter dari jaringan IP dan pengukuran dijalankan pada 3 router yang terdapat pada jaringan untuk mengambil data jitter pada masing-masing router dan membuat rata-rata jitternya

Tabel 4.3. Jitter

Bitrate (Mbps)	Jitter (ms)	
	IPv4	IPv6
2	0.576	0.601
4	0.79	0.995
6	0.716	1.225
8	0.605	1.021
10	0.552	1.154
20	0.472	1.287
30	0.497	1.426
40	0.548	1.544
50	0.637	1.327
60	0.627	1.394
70	0.63	1.479
80	0.757	1.522
90	0.477	1.642
100	0.52	1.575



Gambar 4.3 Grafik Jitter IPv4 vs IPv6

Dari data sebelumnya, didapatkan jitter IPv6 lebih besar, header pada IPv6 lebih besar daripada IPv4, dimana rata-rata jitter IPv4 adalah 0.6 ms dan rata-rata jitter IPv6 adalah 1.29 ms. Terdapat perbedaan jitter IPv4 dan IPv6 sebesar 53.48%.

4.5 Packet Loss

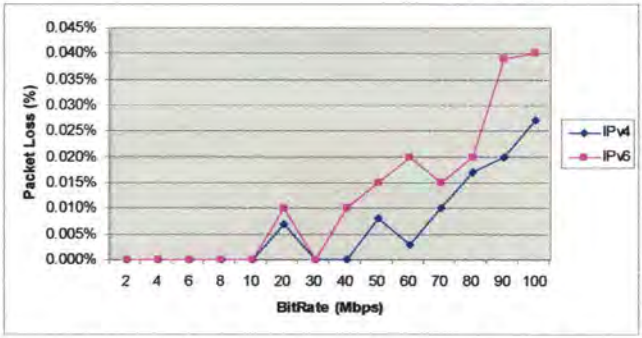
Packet Loss didefinisikan sebagai kegagalan transmisi paket IP mencapai tujuannya dalam sebuah jaringan komputer. Packet loss ini merupakan salah satu dari tiga kegagalan yang dihadapi dalam komunikasi digital selain bit error dan paket yang rusak dikarenakan oleh noise. Kegagalan paket ini biasanya disebabkan oleh beberapa sebab, diantaranya:

- Terjadi overload trafik didalam jaringan.
- Tabrakan (congestion) antar paket dalam jaringan.
- Adanya error yang terjadi pada bagian fisik interface jaringan.

Pada pengukuran packet loss kali ini dengan menggunakan trafik UDP pada trafik generator iperf, karena pada UDP, kemungkinan recovery paket tidak ada sehingga akan tercatat langsung hasil packet loss dari jaringan IP dan pengukuran dijalankan pada 3 router yang terdapat pada jaringan untuk mengambil data packet loss pada masing-masing router dan membuat rata-rata packet lossnya. Data untuk packet loss bisa dilihat pada tabel dan grafik dibawah ini:

Tabel 4.4. Tabel Packet Loss

Bitrate (Mbps)	Paket Loss (%)	
	IPv4	IPv6
2	0%	0%
4	0%	0%
6	0%	0%
8	0%	0%
10	0%	0%
20	0.007%	0.010%
30	0%	0%
40	0%	0.010%
50	0.008%	0.015%
60	0.003%	0.020%
70	0.010%	0.015%
80	0.017%	0.020%
90	0.020%	0.039%
100	0.027%	0.040%



Gambar 4.4. Grafik Packet Loss IPv4 vs IPv6

Dari data, didapatkan bahwa selisih rata-rata packet loss IPv6 dan IPv4 adalah 0.077% dengan packet loss pada IPv6 lebih besar daripada packet loss pada IPv4.

4.6 Sintesa

Pada bagian ini akan dilakukan akan dilakukan analisa pada masing-masing parameter yaitu delay, throughput, jitter dan packet loss.

4.6.1 Throughput

Terdapat perbedaan kemampuan IPv4 dan IPv6 sebesar 14.81%, dimana pada Ipv4 lebih tinggi dari IPv6. Hal ini bagi penulis sedikit mengejutkan karena sebagai penerus dari IPv4, mungkinkah IPv6 memang masih memiliki kelemahan sehingga throughput yang dihasilkan masih lebih rendah daripada throughput IPv4.

Namun, setelah melakukan studi literatur lebih seksama dengan melihat jurnal-jurnal di internet yang menunjukkan hasil yang serupa.

Drave dan Zill[7] menyajikan evaluasi performansi pada jaringan IPv4 dan IPv6 pada Windows NT menggunakan fast ethernet adapter. Hasilnya menunjukkan throughput IPv6 lebih rendah 2% dibandingkan IPv4.

Zeadaly dan Raicu[8] mengukur pengukuran performansi jaringan IPv6 dan IPv4 di Windows dan Solaris. Parameter yang dipakai adalah throughput, round trip time, dan utilisasi CPU. Hasil dari penelitian tersebut menunjukkan bahwa IPv6 pada SUN Solaris lebih baik daripada Windows, dan protokol IPv4 lebih baik daripada protokol IPv6 pada paket TCP dan paket UDP.

---

7. R.P. Draves, B.D Zill, "Implementing IPv6 for Windows NT", Proc 2nd USENIX WindowsNT Symposium, Seattle, WA, USA, August 1998
8. Zeadally, I.Raicu, "Evaluating IPv6 on Windows and Solaris", IEEE Internet Computing (2003) 51-57

Karuppiah[9] menganalisa performansi jaringan IPv4 dan IPv6 dengan menggunakan ping dan aplikasi FTP. Hasil menunjukkan bahwa jaringan IPv6 memiliki performansi lebih rendah dibandingkan jaringan IPv4 untuk transfer file.

Supaya datagram dapat sampai ke tujuan, ukurannya harus kecil untuk memenuhi batasan MTU (Maximum Transfer Unit). MTU sendiri berfungsi untuk mendeskripsikan batasan ukuran frame pada layer fisik. Jika sebuah datagram lebih besar dari MTU, maka akan dipecah pecah menjadi potongan kecil-kecil. Proses ini dinamakan fragmentasi. Lalu pecahan ini akan disusun ulang di tujuan.

Pada IPv4, fragmentasi ini dilakukan di device awal, dan juga dilakukan pada router atau intermediate router pada saat pengiriman. Tapi pada IPv6, hanya dilakukan pada source dan tidak pada router dan intermediate router. Sehingga source harus melakukan fragmentasi sampai ke ukuran MTU yang diizinkan.

Pada IPv4 pula, source bisa mengirimkan sebuah datagram dengan ukuran yang sangat beragam, sesuai kapasitas link yang digunakan dan router bisa melakukan fragmentasi. Tapi hal ini bisa mengakibatkan menurunnya performansi routing. Dan adalah lebih cepat untuk memforward datagram secara utuh daripada menghabiskan waktu untuk melakukan fragmentasi. Tapi untuk beberapa kasus, fragmentasi trerjadi beberapa kali lipat waktu pengiriman datagram, dan hal ini terjadi pada setiap datagram pada sebuah router. Sehingga lebih efisien untuk source mengirimkan datagram dengan ukuran paket yang tepat.

Selain itu didunia internet, IPv6 masih dalam tahap experimental karena sistem yang ada masih digunakan untuk mengoptimisasi sistem IPv4 dibandingkan dengan sistem IPv6, selain itu pada penelitian Wen-Lung Shiau, Yu-Feng Li, Han-Chieh Chao dan Ping-Yu Hsu [10] didalam jaringan berskala besar, throughput pada IPv4 masih lebih besar dengan selisih 11.5% daripada throughput pada IPv6.

4.6.2 Jitter

Dari data sebelumnya, didapatkan jitter IPv6 lebih besar, header pada IPv6 lebih besar daripada IPv4 dengan selisih sebesar 53.48%. Dengan menggunakan buffering pada UDP untuk mendapatkan jitter, dan jika meninjau konsep window size muncul hal-hal sebagai berikut:

---

9. E.K. Karuppiah, "IPv6 dual stack transtition technique performance analysis: KAME on FreeBSD as the case", Faculty of Information Technology, Multimedia University, Jalan Multimedia, October 2000

10. Wen-Lung Shiau, Yu-Feng Li, Han-Chieh Chao dan Ping-Yu Hsu "Evaluating IPv6 on a large-scale network" Department of Information Management, Ming Chuan University, No. 5, Teh-Ming Rd., Gwei-Shan District, Taoyuan, County 333, Taiwan, R.O.C, January 2006

- Window size dikurangi maka jumlah paket di jaringan mengecil
- Window size besar maka jumlah paket di jaringan membesar
- Konsep congestion window "ukuran window lebih kecil jika kongesti terjadi dan membesar jika kongesti berkurang".

Karena ukuran paket IPv6 dicacah lebih banyak daripada IPv4, akibat dari header IPv6 lebih panjang, sementara window size tetap. Pada window size yang sama, jumlah irisan paket yang tersedia lebih banyak pada IPv6 daripada IPv4. mengakibatkan delay antar paket menjadi lebih lama.

4.6.3 Delay

Terdapat delay antara 5-15 ms dimana jaringan IPv4 masih lebih baik daripada jaringan IPv6. Adanya perbedaan dalam pengukuran Round Trip Delay pada jaringan IPv4 dan IPv6 dikarenakan adanya perbedaan panjang header pada IPv4 dan IPv6, dimana panjang header IPv4 lebih sedikit daripada IPv6 sehingga tidak butuh waktu lama dalam pemrosesan data dan otomatis membutuhkan waktu yang lebih sedikit untuk mengembalikan paket ICMP yang ada

4.6.4 Packet Loss

Pada IPv6, packet loss sedikit lebih besar karena proses fragmentasi hanya dilakukan pada source saja, sehingga router tidak melakukan fragmentasi datagram, sehingga paket akan di drop jika datagram terlalu besar untuk di transmisikan.

Selain itu IPv6 memiliki header yang lebih besar dari IPv4, selain itu fragmentasi tidak pernah dilakukan pada router dan karena checksum tidak ada pada header IPv6, maka probabilitas paket loss pada IPv6 lebih besar daripada IPv4, karena router akan men-drop paket yang melebihi kapasitas MTU dari router.

BAB V
PENUTUP

BAB V
KESIMPULAN

5.1. Kesimpulan

Dari hasil analisa perbandingan pengujian unjuk kerja yang telah dilakukan pada jaringan IPv6 dengan menggunakan protokol routing RIPng dan jaringan IPv4 dengan menggunakan protokol routing RIP, diantaranya dengan pengujian throughput, pengujian delay, pengujian jitter, pengujian packet loss, serta pengujian routing dinamik. Semua pengujian menggunakan pembebanan jaringan dengan beban yang bermacam-macam tergantung jenis pengujian yang dijalankan, dapat ditarik kesimpulan sebagai berikut:

1. Pada pengujian delay, terlihat bahwa adanya selisih antara IPv4 dan IPv6 antara 0.5 ms – 1.5 ms, dimana waktu IPv6 lebih besar daripada IPv4. Hal ini disebabkan adanya perbedaan panjang header pada IPv4 dan IPv6, dimana panjang header IPv4 lebih sedikit daripada IPv6 sehingga tidak butuh waktu lama dalam pemrosesan data dan otomatis membutuhkan waktu yang lebih sedikit untuk mengembalikan paket ICMP yang ada.
2. Pada pengujian throughput, terlihat adanya perbedaan yang cukup mencolok antara hasil dari IPv4 dan IPv6, dimana hasil throughput IPv6 lebih kecil daripada throughput IPv4, dengan selisih 14.81%. Hal ini lebih banyak disebabkan karena performa IPv6 yang belum bagus dan belum sepenuhnya didukung oleh OS yang ada dan disebabkan oleh fragmentasi IPv4 dilakukan di device awal, dan juga dilakukan pada router atau intermediate router pada saat pengiriman. Tapi pada IPv6, hanya dilakukan pada source dan tidak pada router dan intermediate router. Sehingga source harus melakukan fragmentasi sampai ke ukuran MTU yang diizinkan, sehingga bisa menurunkan performa throughput yang ada.
3. Pada pengukuran jitter, terlihat performa jitter IPv6 juga lebih buruk daripada IPv4 dengan selisih 53.48%. Hal ini disebabkan oleh ukuran paket IPv6 dicacah lebih banyak daripada IPv4, akibat dari header IPv6 lebih panjang, sementara window size tetap. Pada window size yang sama, jumlah irisan paket yang tersedia lebih banyak pada IPv6 daripada IPv4. mengakibatkan delay antar paket menjadi lebih lama.
4. Untuk pengujian packet loss, terlihat bahwa selisih antara IPv4 dan IPv6 hanya berkisar 0.077%. Tapi sedikit terlihat bahwa IPv6

memiiliki packet loss yang lebih banyak, Pada IPv6, packet loss lebih besar karena proses fragmentasi hanya dilakukan pada source saja, sehingga router tidak melakukan fragmentasi datagram, sehingga paket akan di drop jika datagram terlalu besar untuk di transmisikan. Selain itu, IPv6 memiliki header yang lebih besar dari IPv4, dan karena fragmentasi dan checksum tidak pernah dilakukan pada router, maka probabilitas paket loss pada IPv6 lebih besar daripada IPv4.

5. Dari semua percobaan yang dilakukan, didapatkan suatu kejelasan bahwa untuk sekarang ini IPv4 masih melebihi IPv6 dari aspek throughput, delay, jitter dan packet loss, dikarenakan pengembangan IPv6 yang masih belum maksimal dan kebutuhan dunia yang masih tinggi akan IPv4 sehingga untuk optimasi alat dan sistem operasi masih dikhususkan pada IPv4 dan prioritas IPv6 masih yang kedua karena masih dalam tahap eksperimental

5.2 Saran

Dari hasil pengamatan dan analisa yang telah dilakukan, penulis memberikan beberapa saran untuk pengembangan unjuk kerja IPv6 dan sekiranya yang dapat digunakan untuk penelitian tugas akhir selanjutnya yaitu:

- Pengembangan penggunaan aplikasi berbasis jaringan IPv6 seperti halnya VOIP dan Video Conference
- Pengembangan yang optimal dukungan dari OS yang akan digunakan serta penggunaan window size yang optimal dalam jaringan.

DAFTAR PUSTAKA

DAFTAR PUSTAKA

[1] E.K. Karuppiah, "IPv6 dual stack transtition technique performance analysis: KAME on FreeBSD as the case", Faculty of Information Technology, Multimedia University, Jalan Multimedia, October 2000

[2] G. Malkin and R. Minnear, RFC 2080-RIPng for IPv6, January 1997 <http://www.faqs.org/rfcs/rfc2080.html>

[3] Krzysztof Nowicki, Rafał Marszewski, Appraisement of Modifications in Dynamic Routing Protocols to Support the IPng Protocol, Journal of Applied Computer Science, Vol. 13. No 1, 2005

[4] Richard P. Draves,1 Allison Mankin,2 Brian D. Zill1, Implementing IPv6 for Windows NT, 1998

[5] RIPE 40 Meeting, Prague, Czech Republic " IPv6 Tutorial", October 2001

[6] S. Deering and R. Hinden, RFC 2460-Internet Protocol Version 6 (IPv6) Specification, December 1998, <http://www.faqs.org/rfcs/rfc2460.html>

[7] Taufan Riza, Teori dan Implementasi IPv6 Protokol Internet Masa Depan, Elex Media Komputindo, 2001

[8] Wen-Lung Shiau, Yu-Feng Li, Han-Chieh Chao dan Ping-Yu Hsu "Evaluating IPv6 on a large-scale network" Department of Information Management, Ming Chuan University, No. 5, Teh-Ming Rd., Gwei-Shan District, Taoyuan, County 333, Taiwan, R.O.C, January 2006

[9] Zeadally, I.Raicu, "Evaluating IPv6 on Windows and Solaris", IEEE Internet Computing (2003) 51-57

[10] http://www.arin.net/community/rirs.html

[11] http://en.wikipedia.org/wiki/IPv6

[12] http://en.wikipedia.org/wiki/throughput

[13] http://en.wikipedia.org/wiki/Packet_loss

[14] http://en.wikipedia.org/wiki/delay

[15] http://en.wikipedia.org/wiki/jitter

[16] http://geeks.netindonesia.net/blogs/fajar/archive/2007/04/28/ Fundamental-IPv6-_3A00_-Comparison-of-IPv4-and-IPv6.aspx

LAMPIRAN

LAMPIRAN A
TABEL HASIL PENGUKURAN

'HROUGHPUT

.OUTER-A

Window Size (Kb)	THROUGHPUT (Mbps)	
	IPv4	IPv6
2	70.7	50.2
10	83	72.7
20	86.1	80.1
30	89.1	80.7
40	90.5	81.5
50	91.3	81.4
60	91.8	81
70	93.2	79.03
80	93.4	79.6
90	93.1	77.9
100	93	79.06
110	93.2	79.5
120	93.5	79.1
130	93.5	79.9
140	93.6	79.9
150	93.8	79
160	93.7	79.7
170	94.2	77.8
180	94.1	80.1
190	94.2	79.06
200	94.3	80.2

ROUTER-B

Window Size (Kb)	THROUGHPUT (Mbps)	
	IPv4	IPv6
2	38.7	34.5
10	84.6	80.9
20	86.9	81.7
30	89.5	82
40	89.8	82.1
50	92.8	81.1
60	92.3	81.1
70	93.2	77.7
80	93	78
90	93.2	77.1
100	93.1	75.2
110	93.6	78.7
120	93.1	77.9
130	94	77.5
140	93.7	79.5
150	93.7	75.1
160	94	75.7
170	94.1	77.9
180	93.9	76.6
190	94	75.7
200	94	75.5

.OUTER-C

Window Size (Kb)	THROUGHPUT (Mbps)	
	IPv4	IPv6
2	42.3	40.1
10	82.7	80.1
20	87.4	81.2
30	86.2	81.5
40	89.5	81.8
50	92.1	77.6
60	91.2	77.7
70	93.1	80.3
80	93	80.6
90	93.5	79.1
100	93.4	78.7
110	93.3	78.5
120	93.6	78.6
130	93.3	77.9
140	93.5	75.3
150	93.6	74.5
160	94	75.2
170	93.2	75.2
180	93.8	75.1
190	94	75.5
200	93.9	75.4

JITTER

ROUTER-A

Bitrate (Mbps)	Jitter (ms)	
	IPv4	IPv6
2	0.759	0.764
4	0.791	1.189
6	0.532	1.49
8	0.553	1.112
10	0.257	1.469
20	0.495	1.426
30	0.526	1.486
40	0.575	1.449
50	0.468	1.28
60	0.603	1.34
70	0.558	1.52
80	0.681	1.58
90	0.534	1.669
100	0.457	1.433

OUTER-B

Bitrate (Mbps)	Jitter (ms)	
	IPv4	IPv6
2	0.37	0.44
4	0.809	0.806
6	0.632	1.047
8	0.628	0.882
10	0.928	0.923
20	0.455	1.183
30	0.373	1.325
40	0.542	1.38
50	0.985	1.302
60	0.639	1.161
70	0.773	1.439
80	0.871	1.387
90	0.469	1.381
100	0.672	1.519

OUTER-C

Bitrate (Mbps)	Jitter (ms)	
	IPv4	IPv6
2	0.66	0.6
4	0.771	0.99
6	0.984	1.14
8	0.635	1.069
10	0.472	1.071
20	0.467	1.251
30	0.594	1.468
40	0.528	1.901
50	0.457	1.447
60	0.639	1.683
70	0.559	1.158
80	0.712	1.601
90	0.428	1.878
100	0.431	1.773

PACKET LOSS

ROUTER-A

Bitrate (Mbps)	Paket Loss (%)	
	IPv4	IPv6
2	0%	0%
4	0%	0%
6	0%	0%
8	0%	0%
10	0%	0%
20	0%	0%
30	0%	0%
40	0%	0%
50	0.024%	0%
60	0.010%	0%
70	0.009%	0.000%
80	0.017%	0.023%
90	0.020%	0.039%
100	0.027%	0.038%

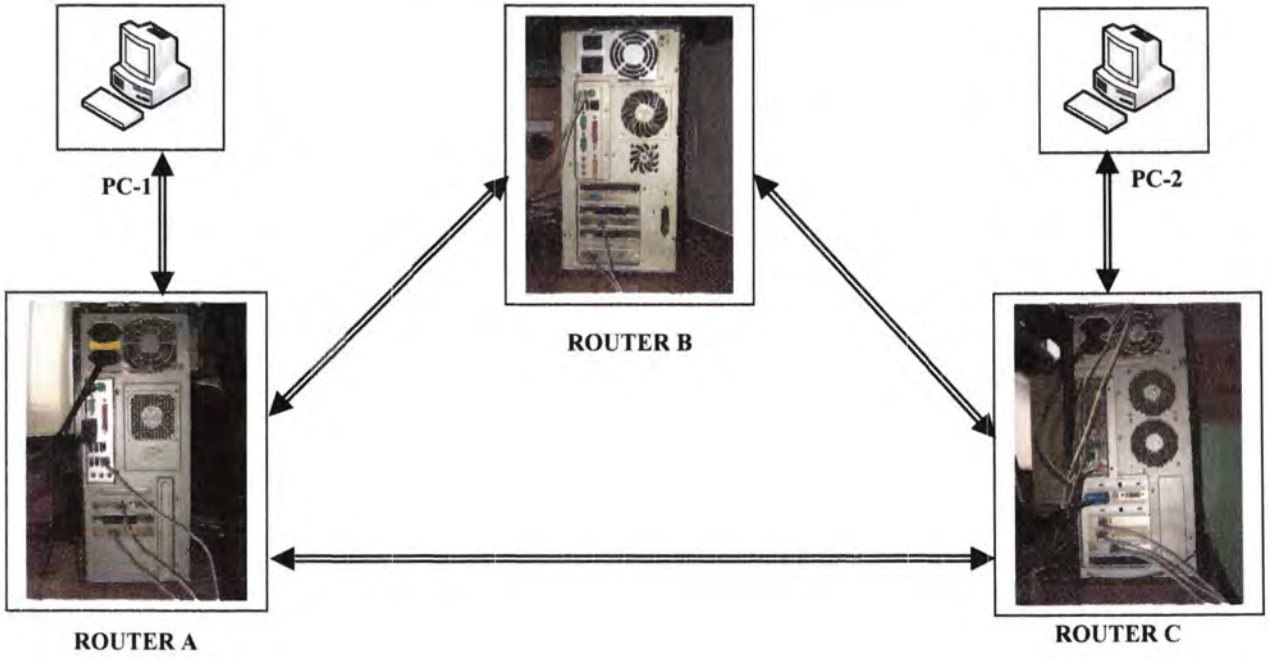
OUTER-B

Bitrate (Mbps)	Paket Loss (%)	
	IPv4	IPv6
2	0%	0%
4	0%	0%
6	0%	0%
8	0%	0%
10	0%	0%
20	0%	0.170%
30	0%	0%
40	0%	0.365%
50	0.3%	0.130%
60	0.000%	0.100%
70	0.010%	0.315%
80	0.016%	0.020%
90	0.020%	0.037%
100	0.029%	0.039%

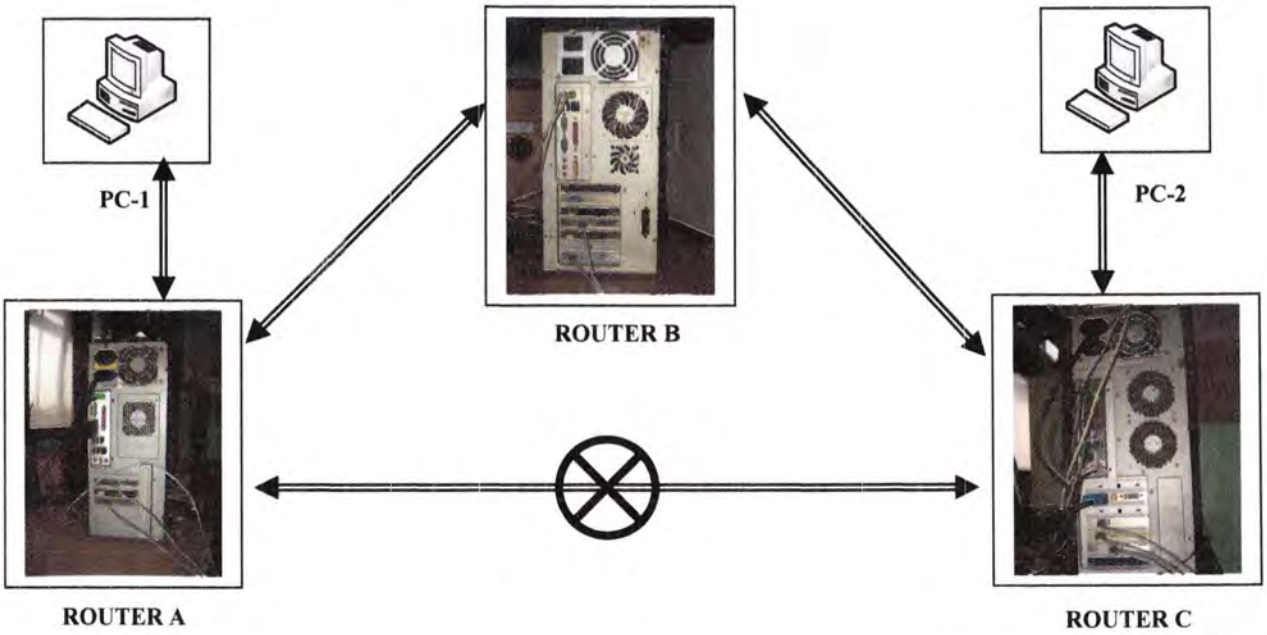
OUTER-C

Bitrate (Mbps)	Paket Loss (%)	
	IPv4	IPv6
2	0%	0%
4	0%	0%
6	0%	0%
8	0%	0%
10	0%	0%
20	0.22%	0.13%
30	0%	0%
40	0%	0.017%
50	0%	0%
60	0.000%	0%
70	0.010%	0.000%
80	0.018%	0.020%
90	0.020%	0.040%
100	0.025%	0.044%

LAMPIRAN B
PEMODELAN NYATA DESAIN ROUTER
(KONDISI NORMAL)



(KONDISI ROUTER-A ROUTER-C PUTUS)



LAMPIRAN C
Usulan Tugas Akhir

Jurusan Teknik Elektro –FTI
Institut Teknologi Sepuluh Nopember

RE 1599 TUGAS AKHIR – 4 SKS

Nama Mahasiswa	: Krishna Kurniawan
Nomor Pokok	: 2206 100 512
Bidang Studi	: Telekomunikasi Multimedia
Tugas Diberikan	: Semester Ganjil 2008/2009
Dosen Pembimbing	: Ir. Djoko Suprajitno Rahardjo

26 SEP 2008

Judul Tugas Akhir

ANALISA UNJUK KERJA PROTOKOL ROUTING RIPng (Routing Information Protocol next generation) PADA JARINGAN IPV6

Performance Analysis of Routing Protocol RIPng (Routing Information Protocol next generation) on IPv6 Network

Uraian Tugas Akhir

IPv6 adalah sekelompok protokol yang mengatur komunikasi data di internet. Protokol IPv6 dikembangkan setelah melihat keberhasilan IPv4 sebagai protokol standar dalam dunia internet.

Salah satu jenis protokol yang dipakai dalam jaringan IPv6 adalah protokol RIPng (*Routing Information Protocol next generation*) yang merupakan pembaharu protokol RIPv2 yang digunakan pada jaringan IPv4, pada RIPng ini digunakan pada jaringan IPv6. Protokol ini termasuk dalam jenis protokol IGP (*Interior Gateway Protocol*) yang menggunakan algoritma *distance vector* dalam menentukan rute terbaik untuk ke arah tujuan. Setiap router dalam jaringan RIPng ini akan mengirimkan seluruh tabel routingnya dalam setiap update ke router tetangganya.

Pada tugas akhir ini akan dilakukan percobaan dengan menggunakan beberapa PC dengan konfigurasi tertentu sebagai *router* dan *client*. Sistem operasi yang digunakan adalah Linux untuk router dan Windows untuk client, dan akan dilaporkan mengenai analisa unjuk kerja protokol *routing* RIPng pada jaringan IPv6 khususnya mengenai hasil dari *throughput*, *delay jitter*, dan *packet loss* yang timbul pada protokol routing RIPng. Selain itu juga akan dilakukan percobaan pada *routing* RIPng mengenai pencarian rute terpendek dalam jaringan secara dinamis baik ketika jaringan masih dalam kondisi utuh ataupun jika sewaktu-waktu jalur utama pada jaringan IPv6 tersebut putus/ mati. Selain itu juga akan dibahas IP *addressing* pada IPv6

Kata Kunci : IPv6, RIPng, *distance vector routing*.

Menyetujui,
Dosen Pembimbing,

17/9 08

Ir. Djoko Suprajitno Rahardjo
Nip. 131 651 447

Mengetahui,
Jurusan Teknik Elektro FTI-ITS
Ketua,

Dr.Ir. Mochamad Ashari,M.Eng
Nip. 131 918 688

Menyetujui,
Bidang Studi Telekomunikasi Multimedia
Koordinator,

22/09

Ir.M. Aries Purnomo
Nip.130 532 040

USULAN TUGAS AKHIR

A. JUDUL TUGAS AKHIR :

ANALISA UNJUK KERJA PROTOKOL ROUTING RIPng (Routing Information Protocol next generation) PADA JARINGAN IPv6

B. RUANG LINGKUP :

- Jaringan Komputer
- Routing RIPng
- Rekayasa jaringan

C. LATAR BELAKANG

IPv6 merupakan versi terbaru dari *Internet Protocol* (IP) yang merupakan bakal pengganti bagi IPv4. IPv6 ini juga biasa disebut dengan IPng (IP *next generation*). IPv6 ini muncul dikarenakan keterbatasan pengalamatan IP yang dialami oleh IPv4, dimana IP ini sangat dibutuhkan oleh mesin-mesin yang terkoneksi ke internet. Pada IPv4 pengalamatan IP hanya 32 bit, sedangkan pada IPv6 mencapai 128 bit. Diperkirakan pada 2-8 tahun kedepan jumlah IPv4 (ive yang tersisa akan habis, karena itu sekarang ini sudah dimulai pengalamatan IPv6 pada mesin-mesin terbaru.

Pada jaringan dengan IPv6 otomatis akan berlaku juga teknologi routing yang hampir sama dengan routing pada IPv4 yang terbagi atas 2 keluarga besar yaitu keluarga IGP (Interior Gateway Protocol) yang terbagi lagi menjadi routing *link-state* dan routing *distance-vector* serta dan keluarga EGP (Exterior Gateway Protocol)

D. PERUMUSAN MASALAH

Pada tugas akhir ini, permasalahan yang akan dibahas dalam Tugas Akhir adalah:

- Penerapan RIPng pada jaringan IPv6 supaya bisa menentukan rute terpendek dari jaringan tersebut.
- *Throughput, delay jitter* dan *packet loss* dari pengiriman packet pada jaringan tersebut.

E. BATASAN MASALAH

Batasan permasalahan pada tugas akhir ini adalah:

- Pembahasan protokol IPv6, arsitektur protokol dan pengalamatan IP
- Pembahasan protokol routing RIPng

F. TUJUAN PENELITIAN:

Penelitian pada tugas akhir ini bertujuan untuk mengetahui routing dan pengalamatannnya pada IPv6 dan protokol routing RIPng.

G. PENELAAH STUDI

KONSEP DASAR ROUTING

Routing adalah fungsi dari OSI Layer 3. Routing adalah skema hirarki yang terorganisir yang mengijinkan alamat individual untuk dikelompokkan bersama-sama. Alamat individual ini akan diperlakukan sebagai sebuah unit tunggal hingga pengantaran data memerlukan alamat tujuan terakhir. Routing adalah proses untuk menemukan jalur yang paling efisien dari satu alat ke alat yang lain. Alat yang digunakan untuk proses routing ini adalah router

Ada dua fungsi penting dari sebuah router:

- Router harus menjaga tabel routingnya dan menjaga agar router yang lain tahu tentang perubahan yang terjadi dalam topologi jaringannya. Fungsi ini dijalankan dengan menggunakan protokol routing untuk berkomunikasi mengenai informasi jaringan dengan router yang lain.
- Ketika sebuah paket sampai ke interface, router harus menggunakan tabel routingnya untuk menentukan kemana paket ini harus diarahkan. Router tersebut mengarahkan paket tersebut ke interface yang dituju, menambahkan frame informasi yang dibutuhkan di interface tujuan, lalu mentransmisikan frame tersebut.

ROUTING DISTANCE-VECTOR

Routing *distance vector* menggunakan pendekatan dengan jarak dan arah dan vektor pada semua link pada internetwork. Jaraknya bisa berupa hitungan hop pada jaringan. Router menggunakan algoritma distance vector untuk mengirimkan semua bagian dari *entry* tabel routing tersebut pada router yang berdekatan dalam periode tertentu. Update ini akan terus terjadi walaupun tidak ada perubahan dalam jaringan tersebut. Dengan menerima update routing, maka sebuah router akan mengetahui semua rute dan membuat perubahan pada tabel routingnya. Proses ini juga dikenal sebagai "routing by rumor"

Contoh dari penggunaan protokol routing berbasis *distance vector* adalah:

- ***Routing Information Protocol* (RIP)** - Penggunaan IGP yang paling umum dalam dunia internet, RIP menggunakan hitungan hop dalam routingnya.
- ***Interior Gateway Routing Protocol* (IGRP)** – IGP jenis ini dikembangkan oleh cisco untuk pengalamatan routing dengan skala yang lebih besar. Routing ini adalah *cisco proprietary*.
- ***Enhanced IGRP (EIGRP)*** - IGP jenis ini menggabungkan antara fitur – fitur dari protokol routing distance vector dan protokol routing link-state. Protokol jenis ini juga sering disebut dengan protokol balanced-hybrid, yang merupakan protokol routing distance vector yang lebih lanjut. Protokol routing ini adalah *cisco proprietary*.

ROUTING RIPng

Pada dasarnya, *Routing Information Protocol next generation* adalah *Interior Gateway Protocol* (IGP) yang menggunakan algoritma *distance-vector* untuk menentukan rute terbaik kearah tujuan, dengan menggunakan hitungan *hop* sebagai metric. RIPng digunakan untuk jaringan berbasis IPv6. Dasar dari RIPng hampir sama dengan RIPv2 yang digunakan pada IPv4, yaitu menggunakan algoritma *distance-vector*, aturan *split-horizon*, aturan *poison-reverse*, batas routing maksimal 15 hop, dan merupakan tipe classless routing yang berarti RIPv2 ini mendukung VLSM (Variable-Length Subnet Masking).

Update untuk RIPng yang digunakan pada IPv6 adalah penambahan fitur:

- IPv6 prefix
- Mendukung alamat IPv6 pada hop selanjutnya
- Menggunakan IPv6 untuk komunikasi data.

Header IPv6

IPv6 adalah protokol baru yang digunakan pada layer 3 dimana IPv6 ini direncanakan akan menggusur kedudukan dari IPv4, karena efisiensi struktur headernya serta penambahan alamat IP dari 32 bit hingga 128 bit dan penambahan ukuran header IPv6 dari 20 byte menjadi 40 byte pada IPv6. Header pada IPv6 ini lebih besar daripada IPv4 tapi sedikit dalam jumlah *field* yang digunakan sehingga akan lebih efektif dan efisien dalam pengantaran data.

Gambar 1. Struktur Header pada IPv6

Keterangan:

Field Version : untuk menandai versi dari IP yang digunakan. Berukuran 4 bit.

Field Traffic Class : untuk menandai kelas/ prioritas dari paket IPv6. Berukuran 8 bit.

Field Flow Label : untuk menandai paket tersebut dimiliki oleh urutan spesifik tertentu dari paket IPv6 antara asal dan tujuan dipakai pada aplikasi real time. Berukuran 20 bit

Field Payload Length : menandai panjang dari payload.

Field Next Header : menandai tambahan header pertama jika ada atau jenis protokol pada lapisan atas PDU. Berukuran 8 bit

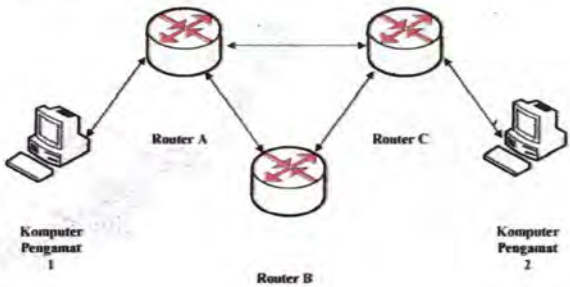
Field Extension Header : digunakan untuk tambahan fungsi yang dibutuhkan seperti security, dsb.

Field Hop Limit : untuk menandai hop maksimum yang dapat dipakai oleh IPv6 dalam lalu lintas internet.

Field Source Address : digunakan untuk menyimpan alamat IPv6 dari host asal, berukuran 128 bit.

Field Destination Address : digunakan untuk menyimpan alamat IPv6 dari host tujuan, berukuran 128 bit

Pada Tugas Akhir ini akan dibahas model jaringan IPv6 yang menggunakan routing RIPng dengan model topologi seperti dibawah ini



Pada gambar diatas dimaksudkan untuk memodelkan sebuah jaringan ideal antara komputer pengamat 1 dan 2 serta jika terjadi masalah antara *router* A dan *router* C semisal kabel putus, maka *router* akan mengambil tindakan untuk memindahkan jalur *routing*. Selain itu akan dilakukan pengukuran berbagai macam faktor seperti *packet loss*, *bandwith* dan *delay jitter* untuk mengukur kinerja dari jaringan tersebut. Semua peralatan dalam jaringan tersebut akan menggunakan komputer dengan menggunakan OS Linux untuk *router* dan OS Windows untuk *client*.

II. METODOLOGI

Metode penelitian yang digunakan dalam Tugas Akhir ini terdiri dari :

1. Studi Literatur
   - Jaringan IPv6
   - IGP menggunakan Protokol *Routing* RIPng
   - *Shell Programming*
   - Parameter jaringan dan Distribusi Jaringan
2. Perancangan dan Pembuatan Sistem.
3. Pengujian, dan Pengolahan Data
4. Analisa dan Pembahasan Data
5. Penulisan Laporan

I. RELEVANSI

Dari Tugas Akhir ini diharapkan bisa menjadi bahan acuan dalam mata kuliah Jaringa Komputer dan Jaringan Akses serta bisa diterapkan pada dunia industri khususnya pada bidang Jaringan dengan IPv6

J. JADWAL KEGIATAN

No.	Kegiatan	Jadwal															
		Bulan Ke-1				Bulan Ke-2				Bulan Ke-3				Bulan Ke-4			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Mempelajari bahan literatur IPv6	■															
	Mempelajari teori IGP menggunakan Protokol Routing RIPng		■														
	Mempelajari *Shell Programming*			■													
	Mempelajari Parameter jaringan dan Distribusi Jaringan				■												
2	Perancangan dan Pembuatan Sistem					■	■	■	■								
3	Pengujian, dan Pengolahan Data								■	■	■						
4	Analisa dan Pembahasan Data									■	■	■	■				
5	Penulisan Laporan TA													■	■	■	■

K. DAFTAR PUSTAKA

a. Krzysztof Nowicki, Rafal Marszewski, Appraisement of Modifications in Dynamic Routing Protocols to Support the IPng Protocol, Journal of Applied Computer Science. Vol. 13. No 1. 2005
b. S. Deering and R. Hinden, RFC 2460-Internet Protocol Version 6 (IPv6) Specification, December 1998. <http://www.faqs.org/rfcs/rfc2460.html>
c. G. Malkin and R. Minnear, RFC 2080-RIPng for IPv6, January 1997 <http://www.faqs.org/rfcs/rfc2080.html>
d. RIPE 40 Meeting, Prague, Czech Republic " IPv6 Tutorial", October 2001
e. US IPv6 Global Summit, Routing Explored with IPv6, December 2003
f. Scott Empson, CCNA Portable Command Guide IPv6, July 2008

RIWAYAT HIDUP

RIWAYAT PENULIS

Nama : Krishna Kurniawan
Alamat : Jl. MT Haryono 9 Ngawi, Jawa Timur
Telp : 085730453081/ 031-60665175
Hobi : Anime/Manga, Baca apa saja, Game DOTA, AOM, Empire, Ngenet, Ngaskus
Email : krishna_italy@yahoo.co.uk
Motto : Jangan banyak bicara, tapi banyaklah bekerja

Krishna Kurniawan dilahirkan di Madiun pada Jum'at, 6 Mei 1983. Merupakan putra ke pertama dari dua bersaudara. Lulus dari SDN Margomulyo 1 Ngawi pada tahun 1994 kemudian melanjutkan ke SMPN 2 Ngawi. Pada tahun 2000 tercatat sebagai salah satu siswa lulusan SMUN 2 Madiun yang kemudian melanjutkan studinya di Politeknik Elektronika Negeri Surabaya (PENS) program Studi Teknik Telekomunikasi.

Setelah menamatkan studi di PENS pada tahun 2003, penulis bergabung dengan salah satu perusahaan yang bergerak di bidang jasa pelayanan internet PT. PASIFIK SATELIT NUSANTARA (PSN) dengan penempatan Bali pada Januari 2004 s/d Mei 2005, lalu bergabung dengan PT RABIK BANGUN PERTIWI (BLUELINE) yang juga merupakan salah satu perusahaan penyedia layanan jasa internet di Bali pada Bulan Juni 2005 s/d Juli 2006. Pada bulan September 2006 penulis melanjutkan studinya di Jurusan Teknik Elektro Institut Teknologi Sepuluh Nopember (ITS) melalui program Lintas Jalur.