ANALISIS & IMPLEMENTASI PASSIVE INTERFACES, ROUTE FILTER, & ROUTING POLICY UNTUK OPTIMALISASI TABEL ROUTING PADA ROUTER CISCO

TUGAS AKHIR

Diajukan sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana

Jurusan Teknik Informatika



Disusun Oleh:

Barly Wicaksono 06523230

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2011

LEMBAR PENGESAHAN

ANALISIS & IMPLEMENTASI PASSIVE INTERFACES, ROUTE FILTER, & ROUTING POLICY UNTUK OPTIMALISASI TABEL ROUTING PADA ROUTER CISCO

TUGAS AKHIR



Disusun Oleh :Barly Wicaksono

NIM :06 523 230

Yogyakarta, 11Maret 2011

Dosen Pembimbing Tunggal

R. Teduh Dirgahayu, ST., M.Sc., Ph.D

LEMBAR PENGESAHAN PENGUJI

ANALISIS & IMPLEMENTASI PASSIVE INTERFACES, ROUTE FILTER, & ROUTING POLICY UNTUK OPTIMALISASI TABEL ROUTING PADA ROUTER CISCO

Oleh:

Nama : Barly Wicaksono
No Mahasiswa : 06 523 230

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 11 Maret 2011

Tim Penguji

R. Teduh Dirgahayu, ST., M.Sc., Ph.D _____
Ketua

Ari Sujarwo,S.Kom _____
Anggota I

Syarif Hidayat, S.Kom., M.I.T. _____
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

LEMBAR PENGESAHAN

ANALISIS & IMPLEMENTASI PASSIVE INTERFACES, ROUTE FILTER, & ROUTING POLICY UNTUK OPTIMALISASI TABEL ROUTING PADA ROUTER CISCO

TUGAS AKHIR



Disusun Oleh : Barly Wicaksono

NIM : 06 523 230

Yogyakarta, 11 Maret 2011

Dosen Pembimbing Tunggal

R. Teduh Dirgahayu, ST., M.Sc., Ph.D

LEMBAR PENGESAHAN PENGUJI

ANALISIS & IMPLEMENTASI PASSIVE INTERFACES, ROUTE FILTER, & ROUTING POLICY UNTUK OPTIMALISASI TABEL ROUTING PADA ROUTER CISCO

Oleh:

Nama : Barly Wicaksono
No Mahasiswa : 06 523 230

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 11 Maret 2011

Tim Penguji

R. Teduh Dirgahayu, ST., M.Sc., Ph.D
Ketua

Ari Sujarwo,S.Kom
Anggota I

Syarif Hidayat, S.Kom., M.I.T.
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

LEMBAR PERNYATAAN KEASLIAN HASIL TUGAS AKHIR

Saya yang bertandatangan dibawah ini,

Nama : Barly Wicaksono

NIM : 06523 230

Menyatakan bahwa seluruh komponen dan isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri.Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini bukan merupakan hasil karya saya sendiri terkecuali referensi yang dicantumkan sumbernya, maka saya siap menanggung resiko dan konsekuen apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 11Maret 2011

Barly Wicaksono

HALAMAN PERSEMBAHAN

Tugas Akhir ini kupersembahkan untuk :

1. ALLAH SWT

   Kau yang telah memberikan nikmat dan keajaiban pada fikiran manusia untuk menghasilkan karya yang lebih baik.

2. Nabi Muhammad SAW

   Yang telah membawa kita dari zaman kebodohan menuju zaman yang terang benderang.

3. Orang Tua

   Kaulah Ibu yang telah melahirkanku dan Ayah yang membimbingku dengan usaha dan doa yang tak henti, Semoga anakmu ini dapat menjadi anak yang membanggakan,berguna bagimu dan juga semua orang.

4. Keluarga

   Kakak dan adikkudan semuanya. Terima kasih atas dukungannya selama ini.

I LOVE YOU All…

MOTTO

بسم الله الرحمن الرحيم

"Yang anda perlukan hanya sebuah mindset, yaitu: Bersiaplah untuk kehilangan wanita yang anda sukai mulai dari detik pertama anda melihatnya. Tanamkan bahwa ADA atau TIDAK nya sang wanita disisi anda, anda tetaplah seorang Pria yang bahagia dan sempurna adanya"

"Gagal adalah suatu kepastian, jika kita sudah tahu akan gagal mengapa tidak mencoba ambil resiko untuk berhasil?"

"Terlalu banyak motto, dapat mengakibatkan penurunan tingkat kecerdasan otak"

"Mulailah sesuatu yang baik dengan ucapan 'bismillah'...dan tutuplah sesuatu yang baik itu dengan ucapan 'alhamdulillah'..."

KATA PENGANTAR

Assalammu'alaikum Wr. Wb

Alhamdulillahirabbil'alamin, dengan mengucap syukur ke hadirat Allah SWT atas berkat, rahmat dan limpahan rizki yang tak henti-hentinya sehingga Tugas Akhir yang berjudul "*Analisis dan Implementasi Passsive Interfaces, Route Filter dan Routing Policy sebagai Optimasi Routing pada Router Cisco*" dapat diselesaikan dengan baik.

Tugas akhir ini membahas tentang bagaimana optimasi routing pada router Cisco yang diharapkan dapat meningkatkan kinerja dan meminimalisasi proses dan resource yang dibutuhkan.Karena tidak semua pembaruantabel routing perlu dikirimkan ke router tetangga, sehingga router dapat meminimalisasi tabel yang dibutuhkan untuk menggambarkan jaringan yang terhubung.Untuk meminimalisasi tabel routing, dapat digunakan 3 metode yaitu :*passive interface, route filter,* dan *routing policy*. Dengan 3 metode berikut, maka router dapat meningkatkan efektifitas dalam pengiriman data.

Ucapan terimakasih saya ucapkan kepada semua pihak yang telah membantu baik langsung maupun tidak langsung proses penyelesaian Tugas Akhir ini. Semoga Allah SWT memberikan balasan yang setimpal dengan keikhlasannya. Ucapan terima kasih saya ucapkan kepada:

1. Allah SWT atas segala berkah dan rahmat-Nya sehingga Tugas Akhir ini dapat diselesaikan.
2. Orang tua, kakak, dan adik atas kasih sayang, segala limpahan doa, dan dukungan

3. Yang saya hormati Bapak Ir. Gumbolo HS., M.Sc selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Ketua Jurusan Teknik Informatika FTI UII Bapak Yudi Prayudi S.Si.,M.Kom.
5. Bapak R. Teduh Dirgahayu, ST., M.Sc., Ph.D selaku dosen pembimbing tunggal dalam penyusunan Tugas Akhir ini.
6. Seluruh Dosen di Jurusan Teknik Informatika Universitas Islam Indonesia. Semoga ilmu yang telah diajarkan dapat menjadi amal, Amin.
7. Teman-teman angkatan 2006 (FIRE) di Jurusan Teknik Informatika Universitas Islam Indonesia.Rekan-rekan sesama TA-ers Aditya Wicaksono, Prasetyo Joko T, Aan Attabis yang saling mendukung
8. R. Danang SWN (085 23 303), makasih udah minjemin komputernya buat maen Point Blankbuat ngilangin pusing :D
9. Specially to Aditya Wicaksono, Mas Dedi Gunawan& Mas Afrizal Koto"*Makasih karena udah pernah ngajakin KP di PAT, kerjain project dan ngenalin cisco*".
10. Semua pihak yang tidak dapat saya sebutkan satu per satu.

Saya berharap laporan ini dapat menjadi sesuatu yang bermanfaat bagi kita semua untuk menambah wawasan dan pengetahuan Amin.

Yogyakarta, 11Maret 2011

Barly Wicaksono

SARI

Routing merupakan pekerjaan yang biasa dilakukan oleh sebuah router, jika jaringan yang dikenali oleh sebuah router tidak banyak, maka router tidak perlu bekerja keras. Semakin bertambahnya hari jumlah jaringan yang muncul makin banyak, hal ini mengakibatkan kinerja router semakin terbebani dengan semakin banyaknya proses yang dilakukan router. Oleh karena itu dibutuhkan optimalisasi routing yang akan berimplikasi pada kinerja router.

Optimalisasi router dapat menggunakan 3 teknik, yaitu: passive interface, route filter, routing policy. Ketiga teknik tersebut memiliki peran yang besar dalam mengoptimalkan kinerja router pada sisi tabel routing, jalur tempuh paket dan juga mengenai pembatasan jaringan yang dapat diakses maupun tidak.

Pada akhirnya hasil yang didapat adalah mengarah kepada minimalisasi tabel routing yang diproses oleh router.

Kata Kunci : passive interface, route filter, route policy

TAKARIR

ip address	alamat IP
command	perintah
default	normal
device	alat
host	host
install	pasang
internet	himpunan jaringan komputer raksasa
interface	tampilan untuk melewatkan Internet Protocol
line	baris
Lokal Area Network	jaringan lokal x
neighbor	tetangga
output	keluaran
physical	fisik
private	pribadi
reliable	handal
resource	sumber
router	perangkat yang merutekan paket

static	statis
support	mendukung
tools	alat
user	pengguna

DAFTAR ISI

HALAMAN JUDUL i
LEMBAR PENGESAHAN ii
LEMBAR PENGESAHAN PENGUJI iii
LEMBAR PERNYATAAN KEASLIAN HASIL TUGAS AKHIR iv
HALAMAN PERSEMBAHAN v
MOTTO vi
KATA PENGANTAR vii
SARI ix
TAKARIR x
DAFTAR ISI xii
DAFTAR TABEL xv
DAFTAR GAMBAR xvi
BAB 1 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
1.6 Metode Penelitian 3
1.7 Sistematika Penulisan 4
BAB II 6
2.1 Konsep Dasar Protokol Routing 6
2.1.1 Protokol Routing Dinamis 7
2.1.2 Protokol Routing Statis 7
2.2 Klasifikasi Protokol Routing 8
2.2.1 Protokol Routing dengan Distance Vector 9

2.2.2 Protokol Routing dengan Link State 14
2.3 Penentuan Jalur 19
2.4 Cisco IOS 19
2.5 Access List (ACL) 19
2.5.1 Dasar ACL 20
2.5.2 Cara Kerja ACL 21
2.6 Tabel Routing 22
2.7 Passive Interfaces 24
2.8 Route Filter 24
2.8.1 Distribute List 25
2.8.2 Route Map 25
2.8.3 Offset List 25
2.9 Routing Policy 26
BAB III 27
3.1 Analisis Masalah 27
3.2 Gambaran Umum Sistem 28
3.2.1 Passive Interface 28
3.2.2 Route Filter 29
3.2.3 Routing Policy 29
3.3 Analisis Kebutuhan Sistem 29
3.3.1 Kebutuhan Perangkat Keras 29
BAB IV 32
4.1 Implementasi Secara Umum 32
4.2 Tahapan Implementasi 32
4.2.1 Konfigurasi Router 32
4.2.1.1 Konfigurasi Hostname Router 32
4.2.1.2 Konfigurasi Alamat IP 33
4.2.1.3 Konfigurasi Protokol Routing 34

4.2.1.4 Konfigurasi Passive Interface 36
4.2.1.5 Konfigurasi Route Filter 37
4.2.1.6 Konfigurasi Routing Policy 39
4.3 Pengujian Hasil Implementasi 41
4.3.1 Pengujian Passive Interface 41
4.3.1.1 Menggunakan Wireshark 41
4.3.1.2 Menggunakan Perintah Debug 45
4.3.1.3 Menggunakan Perintah Show IP Route 48
4.3.2 Pengujian Route Filter 52
4.3.3 Pengujian Routing Policy 58
4.4 Hasil Analisis 59
4.4.1 Passive Interface 59
4.4.2 Route Filter 59
4.4.3 Route Policy 60
BAB V 61
5.1 Kesimpulan 61
5.1.1 Passive Interface 61
5.1.2 Route Filter 61
5.1.3 Policy Routing 62
5.2 Saran 62
DAFTAR PUSTAKA 63

DAFTAR TABEL

Tabel 3.1 Komponen GNS3 31
Tabel 4.1 Alamat IP 33
Tabel 4.2 Analisis Passive Interface 59
Tabel 4.3 Analisis Route Filter 60
Tabel 4.4 Analisis Route Policy 60

DAFTAR GAMBAR

Gambar 2.1 Distance vs Link-State [CIS07].....9
Gambar 2.2 Konsep Distance Vektor [CIS07].....10
Gambar 2.3 Proses Penelusuran Jaringan Distance Vector [CIS07].....11
Gambar 2.4 Perubahan Topologi Distance Vector [CIS07].....12
Gambar 2.5 Komponen Routing Metric [CIS07].....12
Gambar 2.6 Konsep Link State [CIS07].....15
Gambar 2.7 Penelusuran Jaringan Link-State [CIS07].....16
Gambar 2.8 Perubahan Topologi Link-State [CIS07].....17
Gambar 2.9 Flooding Paket Link-State [CIS07].....18
Gambar 2.10 Cisco ACL Memeriksa Paket Header.....20
Gambar 2.11 Group Access List dalam Router [CIS07].....21
Gambar 2.12 Cara Kerja ACL [CIS07].....21
Gambar 2.13 Tabel Routing.....23
Gambar 3.1 Topologi Jaringan.....28
Gambar 4.1 RIP Sebelum Passive Interface.....41
Gambar 4.2 RIP Sesudah Passive Interface.....42
Gambar 4.3 EIGRP Sebelum Passive Interface.....43
Gambar 4.4 EIGRP Sesudah Passive Interface.....43
Gambar 4.5 OSPF Sebelum Passive Interface.....44
Gambar 4.6 OSPF Sesudah Passive Interface.....45
Gambar 4.7 Proses Debug IP RIP Events.....46
Gambar 4.8 Proses Debug EIGRP Packet Hello.....47
Gambar 4.9 Proses Debug IP OSPF Events.....47
Gambar 4.10 Sh Ip Route pada RIP Sebelum Passive Interface.....48
Gambar 4.11 Sh Ip Route pada RIP Sesudah Passive Interface.....49
Gambar 4.12 Sh Ip Route pada EIGRP Sebelum Passive Interface.....50

Gambar 4.13 Sh Ip Route pada EIGRP Sesudah Passive Interface 50
Gambar 4.14 Sh Ip Route pada OSPF Sebelum Passive Interface 51
Gambar 4.15 Sh Ip Route pada OSPF Sesudah Passive Interface 52
Gambar 4.16 Uji Route Filter dengan Ping..... 52
Gambar 4.17 Sebelum Offset List..... 53
Gambar 4.18 Sesudah Offset List 54
Gambar 4.19 Sebelum Distribute List..... 55
Gambar 4.20 Sesudah Distribute List 56
Gambar 4.21 Tabel Routing OSPF Sesudah Distribute List..... 57
Gambar 4.22 Traceroute..... 58
Gambar 4.23 Fail Over Berjalan Normal..... 58

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pertukaran data antar komputer sangat penting di zaman sekarang ini, Teknologi jaringan komputer memungkinkan semuanya terhubung satu sama lain. Di dalam dunia kerja, sudah menjadi keharusan melakukan pertukaran informasi baik inter maupun intra perusahaan.

Sistem jaringan komputer terdiri dari beberapa alat yang berhubungan baik menggunakan kabel atau nirkabel dan melakukan komunikasi berupa pertukaran data satu sama lain. Data dikirimkan kepada tujuan secara beraturan dan diperlukan aturan agar data tersebut mencapai tujuan dengan waktu singkat dan optimal dalam pemilihan jalur pengiriman data.

Alat yang dapat mengatur lalu lintas paket data di dunia jaringan komputer adalahRouter.Router menentukan jalur paket data yang akan dilewati dari satu jaringan ke jaringan lainnya. Router memiliki peta alamat jaringan atau basisdata jaringan tetangga yang ada didekatnya yang disebut tabel routing.Dengan tabel routing ini, router dapat dengan mudah menentukan jalur terbaik sehingga optimal dari sisi waktu pengiriman data.Router juga mempertimbangkan kemungkinan-kemungkinan yang dapat terjadi ketika data dilewatkan melalui jalur yang sudah terdaftar pada tabel routing.

Agar router dapat melewatkan paket data secara optimal melalui jalur yang sudah terdaftar pada tabel routing, ada 3 teknik pengaturan untuk mengoptimalkan kinerja sebuah router, yaitu:

1. Passive Interface
2. Route Filter
3. Routing Policy

Penulis akanmenganalisis dan mengimplementasikan ketiga teknik optimasi router tersebut untuk mengetahui perbedaan sebelum dan sesudah pengaplikasian ketiga teknik tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan diatas, maka kinerja router dalam membatasi pembaruan tabel routing, paket data yang diijinkan untuk dilewatkan dan penentuan jalur dapat ditingkatkan hinggaoptimal.Optimalisasi router dapat dilakukan dengan mencantumkan jaringan yang dikenal saja.Oleh karena itu, :

1. Bagaimanakah untuk mengoptimalkan kinerja *router* dengan menggunakan *passive interface, route filter, dan routing policy*.
2. Apakah ada mekanisme pengendalian lalu lintas data pada jaringan

1.3 Batasan Masalah

Batasan masalah tugas akhir ini adalah sebagai berikut :

1. Implementasi kinerja router menggunakan program emulator GNS3 berbasis Cisco IOS.
2. Routing Protocol yang digunakan adalah Internal Dynamic Routing Protocol.
3. Analisis perbandingan tabel routing sebelum dan sesudah pengaplikasian ketiga teknik optimasi.
4. Pengujian hubungan antar router menggunakan paket *ICMP*.

5. Tidak memperhatikan QoS pada data (Delay, Jitter, dll).
6. Analisis paket data *passive-interface* menggunakan Wireshark.

1.4 Tujuan Penelitian

Dari penjelasan latar belakang diatas, maka tujuan dari tugas akhir ini adalah menganalisis dan mengoptimasi kinerja *router* dengan menggunakan *passive interface, route filter, dan routing policy* yang berdampak pada:

1. Efisiensi pembaruan tabel routing.
2. Lalu lintas data dapat melewati jalur yang tersedia secara optimal.
3. Meningkatkan pengamanan dengan membatasi hubungan dengan jaringan yang tak dikenal

1.5 Manfaat Penelitian

Penelitian ini bermanfaat bagi *administrator* pengendalian atas informasi routing dan juga pengendalian atas paket yang akan dilewatkan oleh sebuah router ditentukan berdasarkan aturan-aturan menggunakan *passive interface, routing policy*, dan *route filter*.Hal ini juga merupakan manajemen yang baik terhadap penggunaan bandwith, dimana lalu lintas dapat dialihkan menuju jalur yang masih bebas penggunaan.

1.6 Metode Penelitian

Penelitian ini mencakup beberapa cara didalamnya, diantaranya mengumpulkan data, dan juga melakukan pengamatan di laboratorium serta memilah dan menentukan data yang berkaitan dengan materi penulisan.

Adapun metode yang digunakan adalah sebagai berikut:

1. Studi Pustaka

   Dilakukan dengan cara mencari dan mengumpulkan referensi yang yang berkaitan dengan materi penulisan seperti melakukan *browsing* internet, *download* dari internet, dan membaca buku panduan konfigurasi yang berkaitan dengan materi penulisan

2. Perancangan dan Implementasi

   Kegiatan ini untuk menguji coba konfigurasi *passive interfaces*, *route filter*, *routing policy* pada tiga*Dynamic Routing Protocol* yaitu: *Routing Information Protocol (RIP)*, *Enhanced Interior Gateway Routing Protocol (EIGRP)*, *Open Shortest Path First (OSPF)*.Selain itu dilakukan juga perancangan terhadap *desain* jaringan untuk mendapatkan hasil yang terbaik dan mendapatkan hasil perubahan tabel routing.

3. Analisis Hasil

   Dilakukan untuk menganalisa konfigurasi yang dilakukan berupa perintah-perintah dijalankan menggunakan topologi yang dibuat pada GNS3 dan menggunakan IOS Cisco kemudian membuat dokumentasinya.

1.7 Sistematika Penulisan

BAB I Pendahuluan

Membahas latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penulisan dan sistematika penulisan

BAB II Landasan Teori

Membahas dasar-dasar teori yang digunakan dalam mengimplementasikan *passive interface, route filter, policy routing* pada *dynamic routing protocol.*Pembahasan dimulai dengan uraian singkat tentang *routing protocol, tabel routing, dynamic routing protocol, OSPF, RIP, EIGRP, ACL's, passive interface, distribution list, dan route map.*

BAB III Metodologi

Menjelaskan analisis masalah, gambaran umum sistem, analisis kebutuhan sistem yang mencakup kebutuhan perangkat keras, perangkat jaringan, dan perangkat lunak.

BAB IV Hasil dan Pembahasan

Membuat dokumentasi hasil pembahasan dan melakukan analisis terhadap konfigurasi yang dibuat, tabel routing, serta proses routing pada ketiga model optimalisasi pada router baik sebelum dan sesudah penerapan dan juga desain jaringan yang digunakan

BAB V Penutup

Memuat kesimpulan-kesimpulan dari seluruh rangkaian proses penelitian baik pada tahap analisis, perancangan, dan implementasi terutama pada analisis kinerja ketiga metode optimasi. Bab ini memberi saran untuk menutup kekurangan serta keterbatasan dalam penelitian ini.

BAB II

LANDASAN TEORI

2.1 Konsep Dasar Protokol Routing

Protokol routing adalah suatu protokol yang digunakan untuk mendapatkan informasi rute dari satu jaringan ke jaringan yang lain[IZAL07]. Informasi tentang rute dapat disampaikan secara dinamis ataupun secara statis diberikan ke router yang lain.

Routing adalah proses dimana suatu router meneruskan paket ke jaringan yang dituju. Suatu router membuat keputusan berdasarkan alamat IP yang dituju oleh paket.Semua router menggunakan alamat IP 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. Ketika menggunakan routing statis, seorang administrator jaringan mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual.Administrator jaringan harus memasukkan atau menghapus rute jika terjadi perubahan jaringan.

Pada jaringan skala besar, routing statis akanmemakan banyak waktu administrator jaringan untuk melakukan pembaruan tabel routing. Karena itu routing statis hanya mungkin dilakukan untuk jaringan skala kecil. Routing statis dapat diterapkan di jaringan skala besar namun membutuhkan kemampuan lebih dari administrator jaringan.

2.1.1 Protokol Routing Dinamis

Protokol routing digunakan untuk memfasilitasi pertukaran informasi routing antara router. Protokol routingmengijinkan router untuk berbagi informasi kepada router lain tentang jaringan yang terhubung dan secara otomatis menambahkan informasi yang didapat ke dalam tabel routing yang dimiliki.

Protokol routing menentukan jalur terbaik pada setiap jaringan dan kemudian didaftarkan pada tabel routing.Salah satu keuntungan menggunakan protokol routing dinamis adalah router selalu bertukar informasi jika terjadi perubahan jaringan.Perubahan jaringan menyebabkan router secara otomatis mempelajari jaringan yang baru dan juga menemukan jalur alternatif jika terdapat sebuah jalur yang tidak terhubung kepada jaringan tertentu.

2.1.2 Protokol Routing Statis

Jaringan *remote* ditambahkan kedalam tabel routing baik dengan mengkonfigurasi routing stattis atau dengan protokol dinamis. Jika *IOS* mempelajari tentang jaringan *remote* dan *interface* yang akan digunakan untuk mencapai jaringan tersebut, *IOS* menambahkan rute tersebut kedalam tabel routing bersama ketika *interface* diaktikan. Rute statis memiliki network address dan subnet mask dari sebuah jaringan network, juga dengan alamat IP dari router next-hop atau *interface* kearah luar.

Rute statis digunakan apabila memenuhi keadaan berikut:

a. Sebuah jaringan terdiri dari sedikit router. Apabila menggunakan protokol routing dinamis tidak menunjukkan adanya keuntungan yang berarti. Kebalikannya, routing protokol dinamis mungkin makin menambah *administrative distance*.

b. Jaringan terhubung dengan internet melalui ISP tunggal. Tidak membutuhkan routing protokol dinamis karena jalur kearah luar hanya menggunakan satu ISP saja.

c. Jaringan yang besar dikonfigurasikan menggunakan desain hub-spoke. Desain jaringan hub-spoke terdiri dari lokasi pusat (hub) dan beberapa lokasi cabang (spoke), dimana setiap spoke hanya memiliki satu hubungan langsung dengan hub. Menggunakan protokol routing dinamis tidak dibutuhkan karena setiap cabang hanya memiliki satu jalur menuju lokasi pusat.

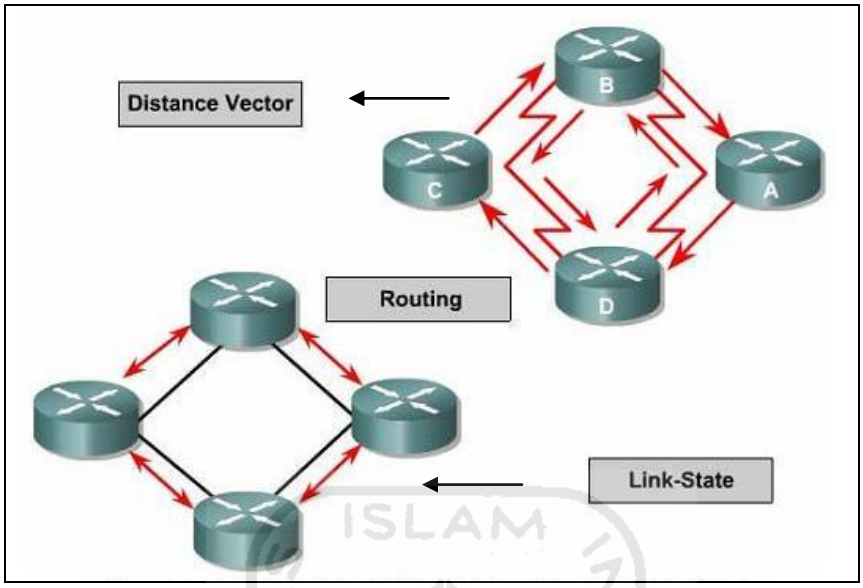
Secara umum, tabel routing mengandung kombinasi routing statis dan routing dinamis. Tetapi seperti yang telah disebutkan sebelumnya, tabel routing harus mengandung daftar jaringan yang terhubung secara langsung yang digunakan untuk mengakses jaringan yang jaringan *remote* sebelum routing protokol statis dan dinamis dapat digunakan

2.2 Klasifikasi Protokol Routing

Sebagian besar algoritma routing dapat diklasifikasikan ke dalam kategori berikut:

1. Distance Vector
2. Link State Vector

Routing *distance vector* bertujuan untuk menentukan arah atau vektor dan jarak ke link-link lain dalam suatu *internetwork*. Sedangkan routing *link-state* bertujuan untuk menciptakan kembali topologi yang benar pada suatu *internetwork*.

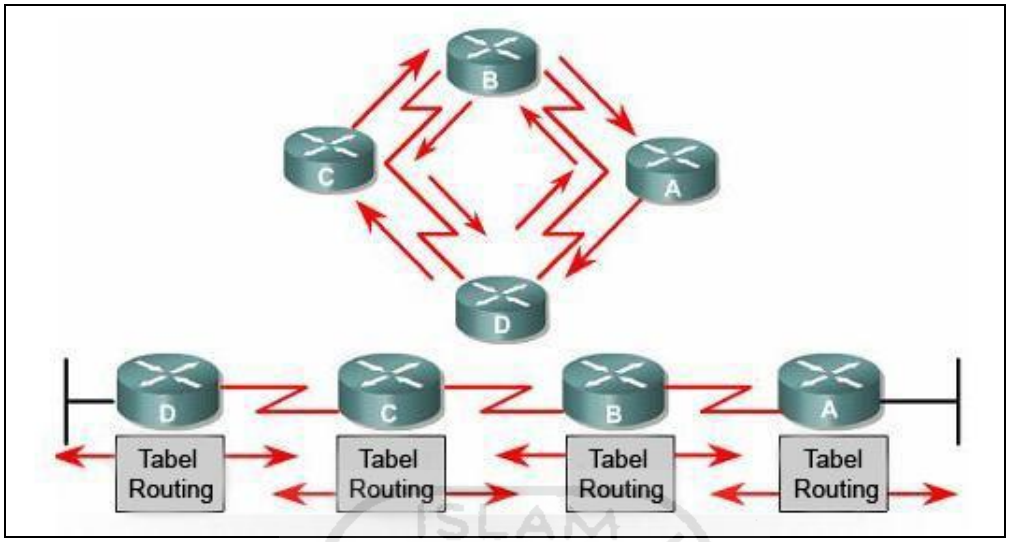


Gambar 2.1 Distance vs Link-State[CIS07]

2.2.1 Protokol Routing dengan Distance Vector

Algoritma routing dengan *distance vector* secara periodik memberikan pembaruan informasi tabel routing kepada router lain. Perubahan tabel routing ini dilakukan pada router yang saling berhubungan pada saat terjadi perubahan topologi. Algoritma *distance vector* juga disebut dengan algoritma Bellman-Ford.

Setiap router menerima table routing dari router tetangga yang terhubung langsung. Pada Gambar 2.2 digambarkan konsep kerja dari *distance vector*:



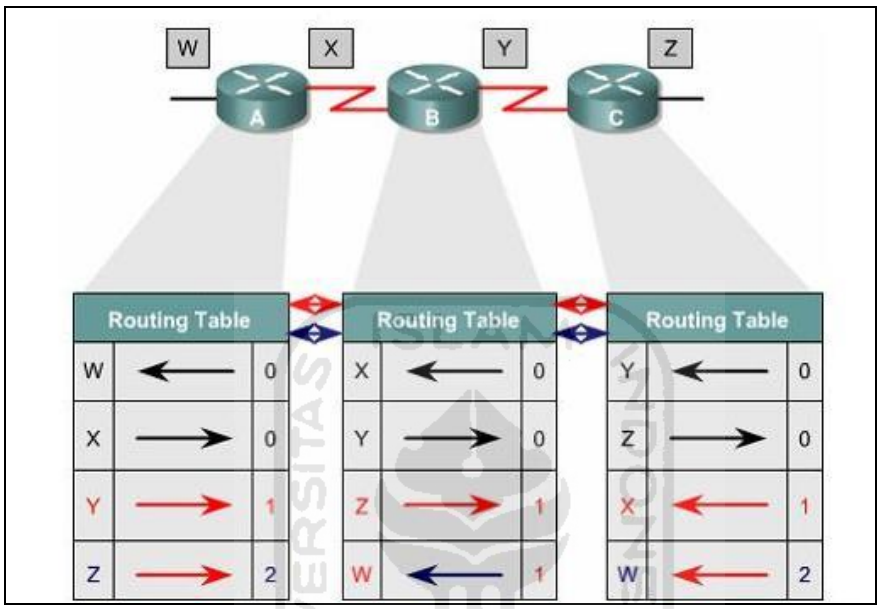
Gambar 2.2 Konsep Distance Vektor[CIS07]

Router B menerima informasi dari Router A. Router B menambahkan nomor *distance vector*, seperti akumulasi jumlah *hop*.Router B melewatkan tabel routing baru ini ke router-router tetangganya yang lain, yaitu Router C. Proses ini akan terus berlangsung untuk semua router.

Algoritma ini mengakumulasi jarak jaringan sehingga dapat digunakan untuk memperbaiki informasi mengenai desain jaringan. Algoritma *distance vector* tidak mengijinkan router untuk mengetahui secara pasti desainjaringan selain router yang terhubung secara fisik, karena router hanya mendapatkan informasi yang diberikan oleh router tetangga yang terhubung secara langsung.

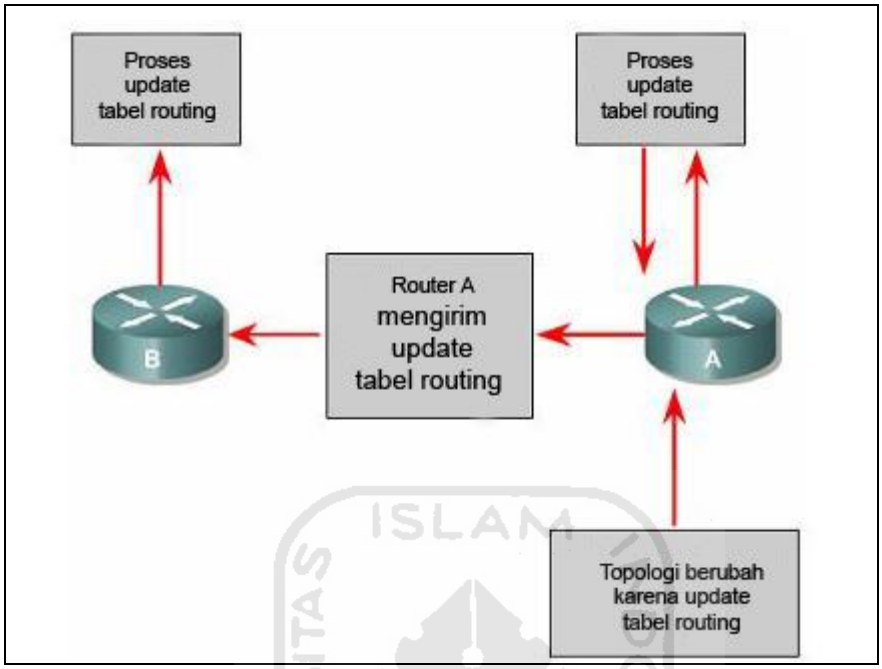
Setiap router yang menggunakan algoritma dengan *distance vector*, pertama kali mengidentifikasi router-router tetangganya. *Interface* yang terhubung langsung ke router tetangganya mempunyai *distance* 0. Router yang menerapkan *distance vector* dapat menentukan jalur terbaik untuk menuju ke jaringan tujuan berdasarkan informasi yang diterima dari tetangganya. Router A mempelajari jaringan lain berdasarkan informasi yang diterima dari router B. Masing-masing

routermenambahkan dalam table routingnya yang mempunyai akumulasi *distance vector* untuk melihat sejauh mana jaringan yang akan dituju. Seperti yang dijelaskan pada Gambar 2.3 dibawah ini:

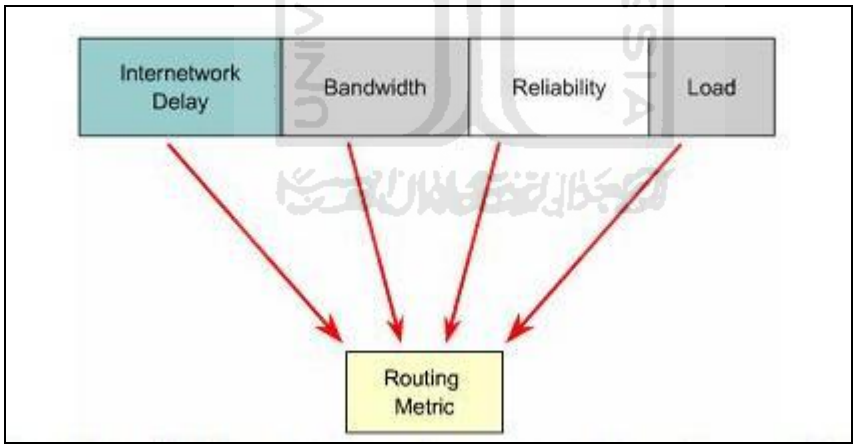


Gambar 2.3 Proses Penelusuran Jaringan Distance Vector[CIS07]

Pembaruan table routing terjadi ketika terjadi perubahan desain jaringan. Sama dengan proses penelusuran, proses perubahan topologi dilakukan dari router satu ke router lain. Gambar 2.3 menunjukkan cara algoritma *distance vector* memanggil semua router untuk mengirimkan isi table routingnya. Table routing berisi informasi tentang *total path cost* seperti pada Gambar 2.3 yang ditentukan oleh *metric* dari router pertama dalam jaringan pada tabel routing, seperti yang diterangkan oleh gambar 2.4 di bawah ini.



Gambar 2.4 Perubahan Topologi Distance Vector[CIS07]



Gambar 2.5 Komponen Routing Metric[CIS07]

Metric merupakan metode algoritma routing yang menentukan bahwa suatu jalur lebih baik daripada yang lain. Komponen *metric* adalah *Delay (waktu tunda), Bandwith, Reliability (kehandalan), Load (beban).*

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

a. Routing Information Protocol (RIP)

Dasar RIP diterangkan dalam RFC 1058, dengan karakteristik sebagai berikut:

- Protokol routing dengan distance vector
- Metric berdasarkan jumlah lompatan (hop count) untuk pemilihan jalur
- Jika hop lebih dari 15, maka paket akan dibuang.
- Pembaruan routing dilakukan dengan memanggil router lain untuk memberikan informasi tabel routing setiap 30 detik

b. Interior Gateway Routing Protocol (IGRP)

IGRP adalah protokol routing yang dibangun oleh Cisco, dengan karakteristik sebagai berikut:

- Protokol routing dengan *distance vector*
- Menggunakan metric yang terdiri atas bandwidth, beban (load), delay (tunda) dan reliability (kehandalan)
- Pembaruan routing dilakukan dengan memanggil router lain untuk memberikan informasi tabel routingnya setiap 90 detik

c. Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP menggunakan protokol routing dengan *distance vector* namun *enhanced*, yaitu protokol routing *distance vector* yang telah ditingkatkan kemampuannya dengan karakteristik sebagai berikut:

- Mendukung IPX, Appletalk melalui modul-modul yang bersifat *protocol depedent*

- Komunikasi melalui *Reliable Transport Protocol* (RTP)
- Menggunakan *Diffusing Update Algorithm* (DUAL) yaitu algoritma kombinasi antara *distance vector* dan *link-state* untuk menghitung jalur terpendek.

Pembaruan routing dilakukan dengan memanggil router lain untuk memberikan informasi tabel routingnya yang menggunakan alamat *multicast* 224.0.0.10.

2.2.2 Protokol Routing dengan Link State

Algoritma *link-state* juga dikenal dengan algoritma Dijkstra atau algoritma shortest path first (SPF).Algoritma ini memperbaiki informasi dari topologi. Algoritma *distance vector* memiliki informasi yang tidak spesifik tentang jumlah *hop* jaringan. Sedangkan algortima *link-state* memperbaiki pengetahuan tentang jarak router dan bagaimana router saling berhubungan.

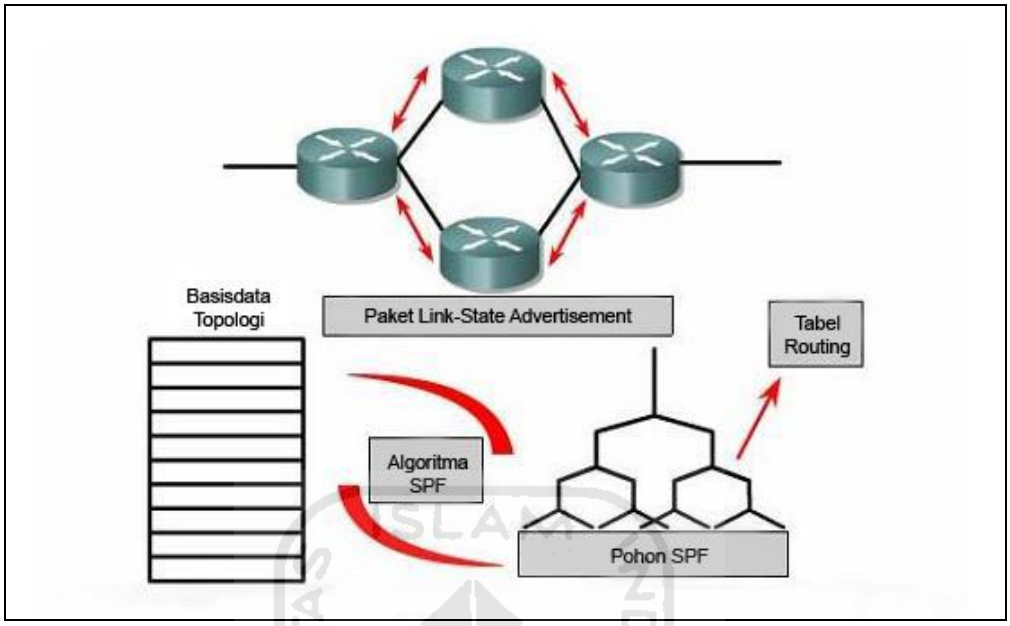
Fitur-fitur yang dimiliki oleh algoritma dengan link-state adalah:

a. Link-state advertisement (LSA) – adalah paket kecil dari informasi routing yang dikirim antar router yang mengandung informasi router tetangga dan path cost.

b. Topological database – adalah kumpulan informasi yang dari LSA-LSA.

c. SPF algorithm – adalah algoritma perhitungan pada basisdata yang dianalogikan sebagai pohon SPF.

d. Tabel routing – adalah daftar rute dan *interface* yang terhubung.

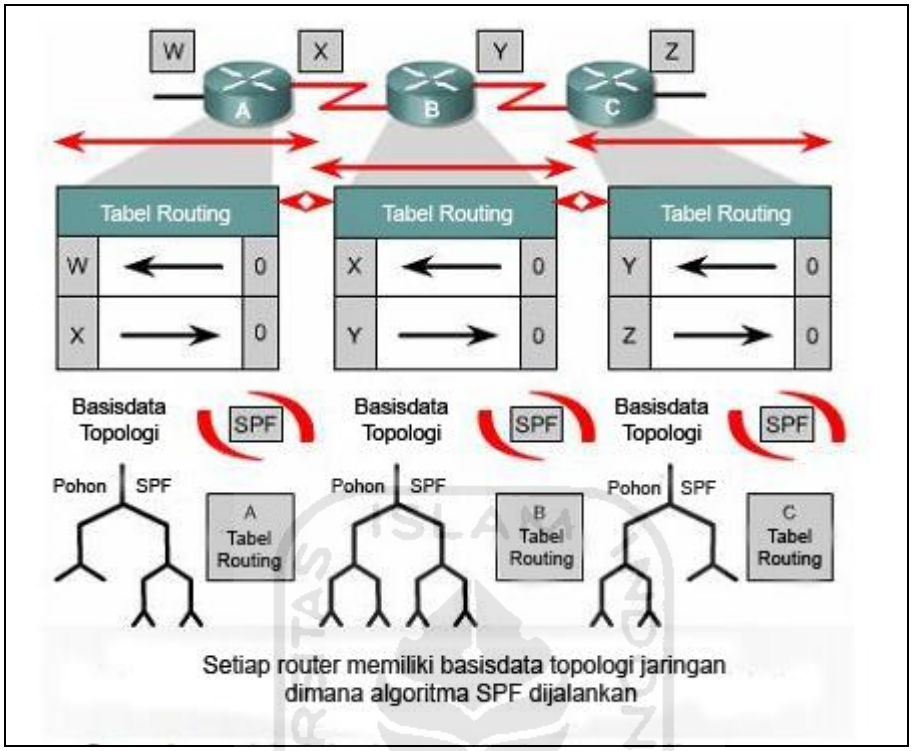


Gambar 2.6 Konsep Link State[CIS07]

a. Proses Penelusuran Routing Dengan Link State

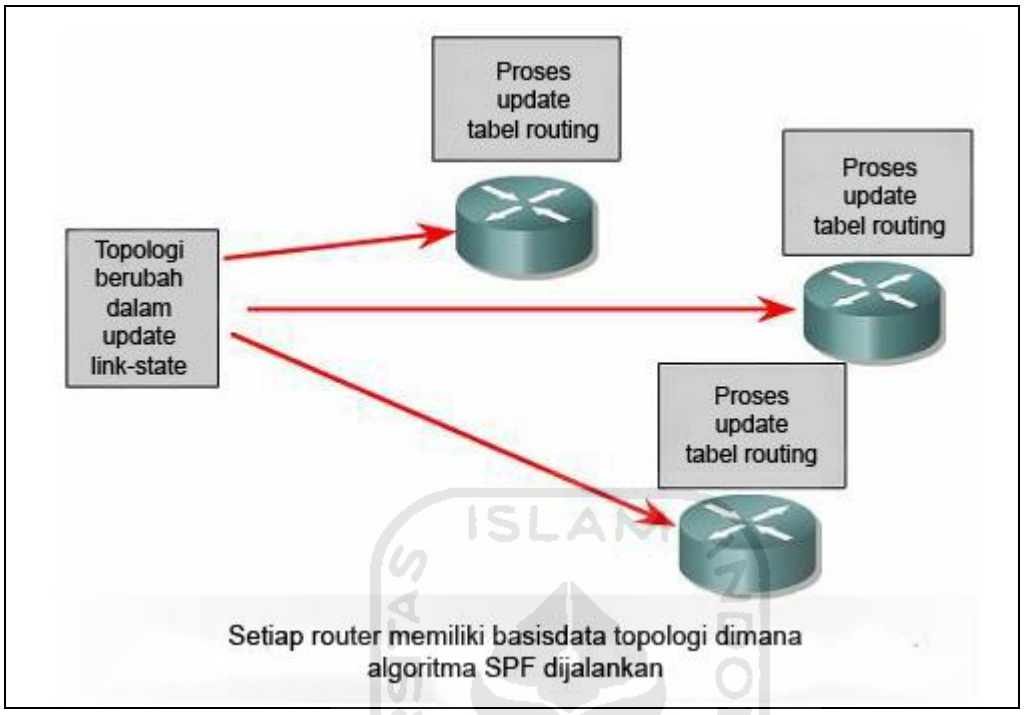
Seperti yang terdapat pada Gambar 2.6, ketika router melakukan pertukaran *LSA* tentang informasi yang dimiliki, dimulai dengan jaringan yang terhubung langsung.Masing-masing router membangun basisdata desain jaringan yang berisi pertukaran informasi *LSA*.

Algoritma SPF menghitung jaringan yang dapat dicapai. Router membangun desain logika sebagai pohon (tree), dengan router sebagai tuan rumah. Desain ini berisi semua rute-rute yang mungkin untuk mencapai jaringan dalam protokol *link-state* jaringan internal.Router kemudian menggunakan SPF untuk mencari rute terpendek. Daftar rute-rute terbaik dan *interface* ke jaringan yang dituju dalam tabel routing. *Link-state* juga memperbaiki basisdata desain jaringan, elemen-elemen desain jaringan dan status jalur secara detail.



Gambar 2.7 Penelusuran Jaringan Link-State[CIS07]

Pada Gambar 2.7, semua router mempelajari jalur jaringan link-state untuk melewatkan informasi sehingga semua router dapat menggunakannya untuk proses pembaruan tabel routing. Gambar 2.8 adalah informasi routing yang dikirim ke semua router dalam jaringan.Untuk mencapai keadaan dimana semua informasi routing tersebar, setiap router mempelajari informasi router-router tetangganya. Termasuk nama dari router-router tetangganya, status *interface* dan biaya menuju ke router tetangga. Router membentuk paket *LSA* yang mendaftar informasi ini dari tetangga-tetangga baru, baik perubahan biaya dan jalur-jalur yang tidak lagi valid.Paket *LSA* ini kemudian dikirim keluar router sehingga semua router-router lain menerima informasi.



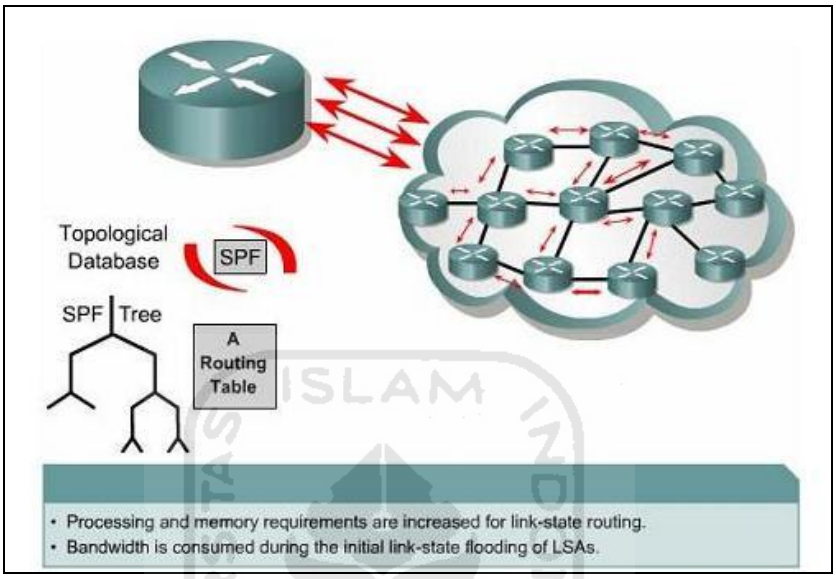
Gambar 2.8 Perubahan Topologi Link-State[CIS07]

Pada saat router menerima *LSA*, ia kemudian memperbarui tabel routing dengan sebagian besar informasi dengan yang terbaru. Data hasil perhitungan digunakan untuk membuat peta jaringan dan algoritma SPF digunakan untuk menghitung jalur terpendek menuju ke jaringan lain.

Router yang menggunakan protokol routing dengan *link-state* membutuhkan memori lebih dan pemrosesan data yang lebih protokol dengan *distance vector*. Router dengan *link-state* menangani semua informasi dari basisdata, pohon topologi dan tabel routing. Gambar 2.9 menunjukkan inisialisasi paket *link-state* secara *flooding* yang mengkonsumsi bandwidth.

Pada proses awal penelusuran, setiap router mengirimkan paket *hello* ke semua router tetangganya. Peristiwa ini memakan bandwith yang cukup besar. Setelah

proses ini, protokol dengan *link-state* secara umum membutuhkan bandwidth yang cukup untuk mengirim paket-paket *LSA* yang menyebabkan perubahan topologi.



Gambar 2.9 Flooding Paket Link-State[CIS07]

Contoh Routing Protokol dengan Link State adalah Open Shortest Path First (OSPF).OSPF mempunyai karakteristik sebagai berikut:

- Protokol routing dengan link-state.
- Merupakan protokol routing standar terbuka yang dijelaskan di RFC 2328.
- Menggunakan algoritma SPF untuk menghitung biaya terendah.
- Pembaruan routing dilakukan secara *flooding* saat terjadi perubahan topologi jaringan.

2.3 Penentuan Jalur

Router menggunakan dua fungsi dasar:

a. Fungsi penentuan jalur

b. Fungsi switching

Penentuan jalur terjadi pada layer 3 OSI yaitu *network layer*.Fungsi penentuan jalur menjadikan router untuk mengevaluasi jalur ke tujuan dan membentuk jalan untuk menangani paket.Router menggunakan tabel routing untuk menentukan jalur terbaik dan kemudian fungsi switching untuk melewatkan paket.

2.4 Cisco IOS

Cisco *IOS* (*Internetwork Operating System*) adalah nama sistem operasi yang digunakan pada perangkat router dan switch buatan Cisco. *IOS* merupakan sistem operasi *multi-tasking* yang menyediakan fungsi-fungsi *routing*, *switching*, *internetworking*, dan telekomunikasi.Cisco *IOS* menyediakan *command line interface* (CLI) dan sekumpulan perintah standar.

Level advanced enterprise yang merupakan Tingkatan tertinggi dari Cisco *IOS* dimana software dengan fasilitas maksimum terdapat didalamnya.

2.5 Access List (ACL)

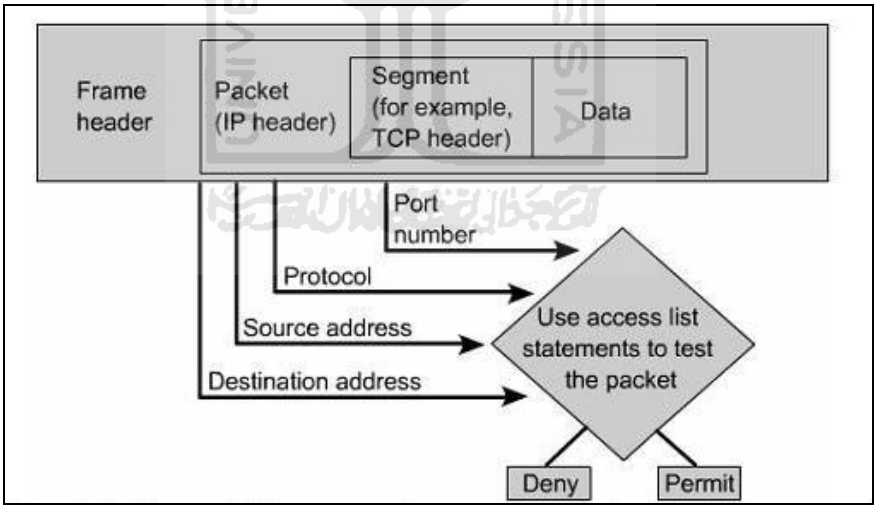
ACL sederhananya digunakan untuk mengijinkan atau tidak paket dari host menuju ke tujuan tertentu. *ACL* terdiri atas aturan-aturan dan kondisi yang menentukan trafik jaringan dan menentukan proses di router apakah nantinya paket akan dilewatkan atau tidak.

2.5.1 Dasar ACL

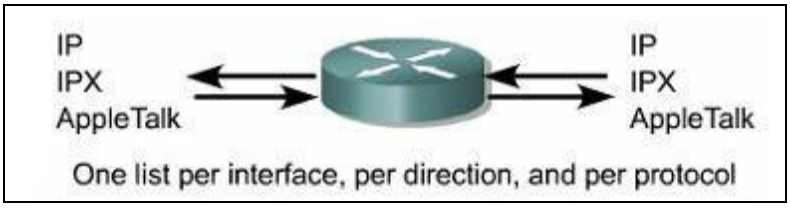
ACL adalah daftar kondisi yang digunakan untuk menguji trafik jaringan yang mencoba melewati *interface* router. Daftar ini memberitahu router paket-paket mana yang akan diterima atau ditolak. Penerimaan dan penolakan berdasarkan kondisi tertentu.

Untuk mem-filter trafik jaringan, *ACL* menentukan jika paket itu dilewatkan atau diblok pada *interface* router.Router *ACL* membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port.

Untuk mengontrol aliran trafik pada *interface*, *ACL* harus didefinisikan setiap protokol pada *interface*. *ACL* kontrol trafik pada satu arah dalam *interface*. Dua *ACL* terpisah harus dibuat untuk mengontrol trafik inbound dan outbound. Setiap *interface* boleh memiliki banyak protokol dan arah yang sudah didefinisikan.

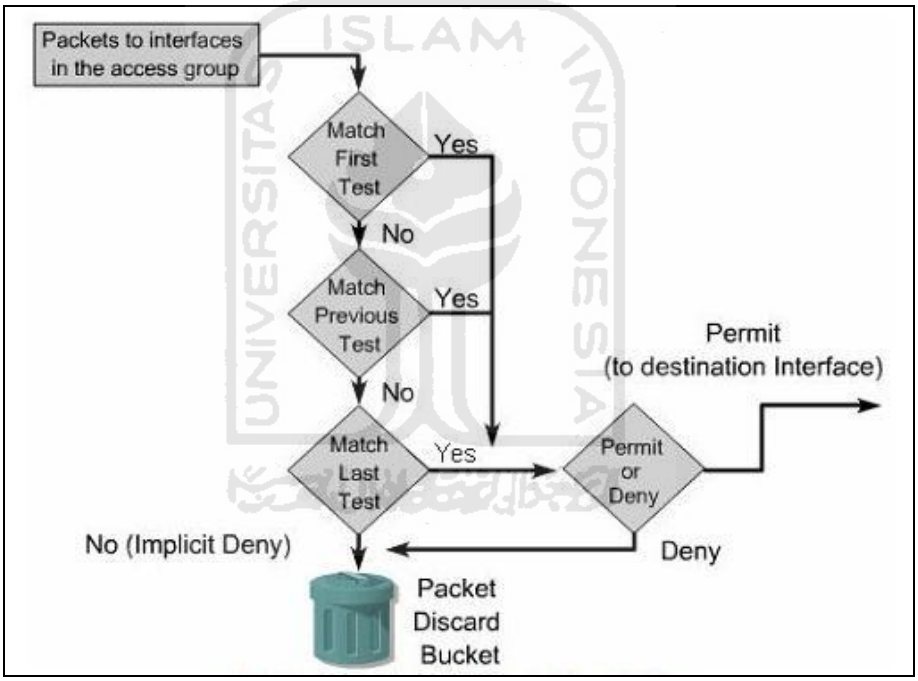


Gambar 2.10 Cisco ACL Memeriksa Paket Header



Gambar 2.11 Group Access List dalam Router[CIS07]

2.5.2 Cara Kerja ACL



Gambar 2.12 Cara Kerja ACL[CIS07]

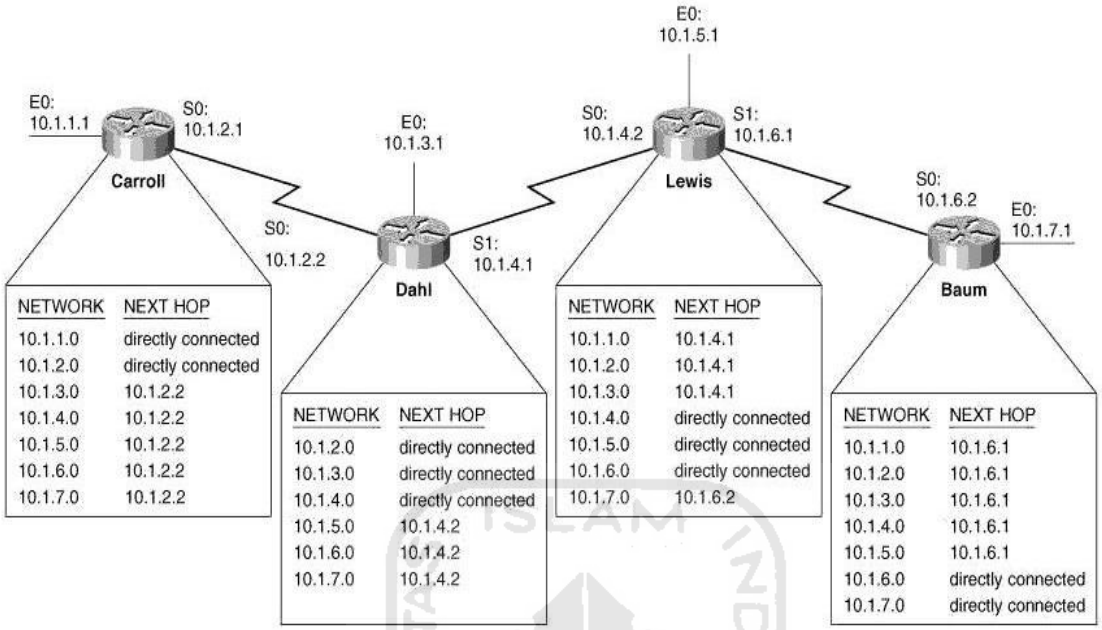
Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang didefinisikan di daftar pernyataan. Perintah dalam pernyataan *ACL* adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses.

Pada saat *frame* masuk ke *interface*, router memeriksa apakah alamat layer 2 cocok atau apakah *frame broadcast*. Jika alamat *frame* diterima, maka informasi *frame* ditandai dan router memeriksa *ACL* pada *interface* inbound. Jika paket diterima di *interface*, kemudian akan diperiksa sesuai dengan tabel routing untuk menentukan *interface* tujuan dan kemudian diteruskan oleh fungsi *switching*. Selanjutnya router memeriksa apakah *interface* tujuan memiliki *ACL*. Jika ya, maka paket diperiksa sesuai dengan daftar akses. Jika paket cocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada *ACL* paket diterima dan paket dienkapsulasi di layer 2 dan di-forward keluar *interface* device berikutnya.

2.6 Tabel Routing

Fungsi utama dari sebuah router adalah merutekan paket kepada jaringan tujuan, dimana tujuannya adalah alamat IP dari sebuah paket. Untuk melakukan ini, router harus mencari informasi yang disimpan dalam bentuk tabel routing.

Sebuah tabel routing adalah berkas data didalam *RAM* yang digunakan untuk menyimpan informasi berupa jaringan yang secara langsung terhubung maupun jaringan yang tidak terhubung secara langsung.Tabel routing mengandung kumpulan *next hop* pada jaringan. Kumpulan *next hop* ini, menjelaskan kepada router bahwa beberapa jaringan tujuan dapat dicapai dengan mengirimkan paket kepada router tertentu yang digambarkan sebagai "*next hop*" jalur menuju kepada tujuan akhir paket. Kumpulan *next hop* ini dapat berupa *outgoinginterface* ke tujuan akhir. Kumpulan *outgoing interface* dapat menggambarkan tujuan akhir alamat jaringan dari sebuah paket IP. Kumpulan *next hop* ini terjadi pada jaringan yang terhubung secara langsung. Gambar 2.13 merupakan ilustrasi dari kandungan tabel routing.



Gambar 2.13 Tabel Routing

Sebuah jaringan yang terhubung langsung adalah jaringan yang memiliki terhubung secara fisik menggunakan salah satu *interface* dari router. Jika *interface* dari sebuah router dikonfigurasikan dengan sebuah alamat IP dan *subnet mask*, maka *interface* tersebut menjadi sebuah *host* yang terhubung langsung secara fisik kepada suatu jaringan. *Network address* dan *subnet mask* dari sebuah *interface* juga dengan tipe *interface* dan nomor *interface*, dimasukkan kedalam tabel routing sebagai jaringan yang terhubung secara langsung secara fisik. Jika router meneruskan sebuah paket menuju *host* lain, seperti *web server*, *host* tersebut berada dalam jaringan yang sama sebagai router yang terhubung secara langsung.

Jaringan *remote* adalah sebuah jaringan yang tidak terhubung secara langsung dengan router. Atau dengan kata lain, jaringan *remote* adalah jaringan yang hanya dapat dicapai dengan mengirimkan paket kepada router lain. Jaringan

*remote*ditambahkan kedalam tabel routing baik itu protokol routing dinamis maupun routing statis.

2.7 Passive Interfaces

Didalam jaringan skala besar mendukung router dengan banyak *interface*, Router memiliki tugas yang sangat penting yaitu tetap mengetahui riwayat router jaringan yang berhubungan dengannya. Namun terkadang kita tidak membutuhkan semua informasi pembaruan tabel routing dari setiap *interface*,

Solusi dari masalah ini adalah dengan mengkonfigurasikan protokol routing pada semua *interface* yang terhubung pada jaringan yang ada dan secara manual memberikan aturan *passive-interface* dimana *broadcast* tabel routing tidak diinginkan.

Pengaplikasian passive interface dibutuhkan pada saat migrasi protokol routing untuk memudahkan pemutusan routing protokol saat terjadi pergantian protokol routing.

2.8 Route Filter

Filtering untuk *Internal Gateway Protocol (IGP)* dapat memberikan banyak kendali pada informasi routing yang melalui jaringan. padaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaani, ada 3 teknologi yang dapat ditujukan untuk mengontrol informasi routing dan *traffic* data :

a. Distribute List

b. Route Map

c. Offset List

2.8.1 Distribute List

Untuk mengendalikan informasi dan pemrosesan rute dari pembaruan routing, maka digunakan *distribute-list*. Ada dua perintah *distribute-list:distribute-list in dan out*. Secara penulisan memang sama, namun pilihan yang tersedia dan juga perlakuannya sangat berbeda.

Berikut perbedaannya:

a. Perintah **Distribute-list in** digunakan untuk mengendalikan rute mana saja yang akan diproses jika terjadi pembaruan tabel routing yang masuk.
b. Perintah D**istribute-list out** digunakan untuk mengendalikan rute mana saja yang akan diproses jika terjadi pembaruan tabel routing kearah luar router.

2.8.2 Route Map

Route map untuk mengijinkan kita untuk memfilter dan memanipulasi rute sepanjang redistribusi atau routing berbasis aturan. Route maps dipecah kedalam beberapa urutan. Setiap urutan memiliki kondisinya sendiri. Jika urutan dari sebuah route map diijinkan dan kondisinya menemui statement match, maka urutan itu dapat mengaplikasikan kondisi pada statement set. Pernyataan set mengijinkan user untuk menspesifikasi aksi apa yang ingin ditampilkan pada rute mana saja yang telah menemukan kondisi statement match. Jika sequence bertipe deny, tidak ada statement set yang dapat digunakan.

2.8.3 Offset List

Perintah **offset-list**digunakan untuk menambahkan keseimbangan kepada metrik yang masuk maupun keluar pada rute yang dikenali oleh masing-masing protokol[CIS10]. Nilai offset akan ditambahkan kedalam metric.

2.9 Routing Policy

Kebijakan routing adalah mekanisme routing yang lebih fleksibel untuk meroutingkan paket dari dan ke jaringan tujuan. Ini adalah proses dimana router menempatkan paket melalui peta rute sebelum meroutingkannya. Peta rute menentukan paket yang diarahkan ke router berikutnya. Mungkin saja jika mengaktifkan routing policy jika menginginkan paket tertentu disalurkan dengan beberapa cara lain selain yang sudah jelas merupakan jalan terpendek.

Untuk mengaktifkankebijakan routing diharuskan mengidentifikasi peta rute yang digunakan untuk kebijakan routing dan membuat peta rute. Peta rute itu sendiri menetapkan kriteria kecocokan dan tindakan yang dihasilkan jika semua klausa kecocokan terpenuhi.

Untuk mengaktifkan kebijakan routing pada sebuah *interface*, untuk menunjukkan peta rute router harus menggunakan modus konfigurasi antarmuka. Semua paket yang tiba pada *interface* yang ditentukan akan dikenakan kebijakan routing. Perintah ini dengan cepat menonaktifkan *switching* dari semua paket setibanyapada*interface*.

BAB III

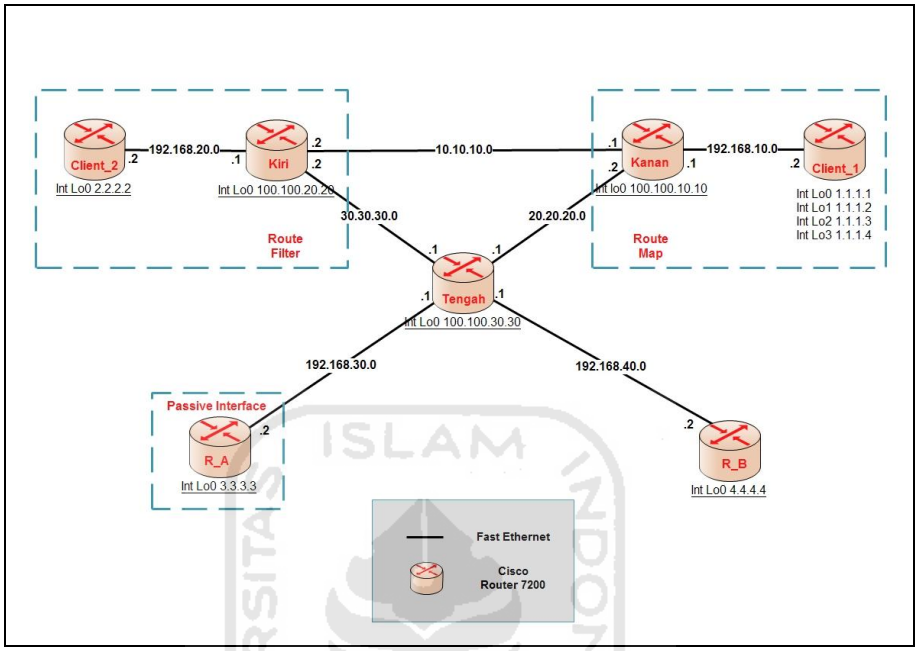
METODOLOGI

3.1 Analisis Masalah

Pemasalahan terjadi ketika tabel routing yang semakin banyak karena pembaruan informasi berlangsung terus menerus dan jumlah jaringan yang di tangani bertambah akan mengakibatkan sumber daya memori yang dibutuhkan oleh semua router yang dalam mengolah tabel routing baik itu informasi yang diterima maupun dikirimkan semakin bertambah. Mekanisme *passive-interface*, *route filter*, dan *route policy* diterapkan untuk menjawab masalah ini.

Passive-interface, route filter, dan route policy bukanlah perintah yang hanya khusus digunakan untuk *RIP*, *OSPF*, atau *EIGRP*, tapi bisa juga digunakan untuk konfigurasi menggunakan protokol routing lainnya seperti *BGP*. Dengan menggunakan perintah *passive-interface*, interface router seolah-olah menjadi *silent host*pada *data link* yang ditentukan.Router s*ilent host* tersebut masih dapat mengirimkan *broadcast* paketdan memperbarui tabel routing berdasarkan pembaruan informasi routing yang didapatkan dari router tetangga. Sedangkan *route filter* dan *route policy* berperan dalam penyaringan dan *traffic engineering* rute yang akan ditempuh oleh paket data.

3.2 Gambaran Umum Sistem



Gambar 3.1 Topologi Jaringan

Mekanisme*passive interface*, *route filter* dan *routing policy*akan diterapkan di jaringan seperti di topologi pada Gambar 3.1. Ketiga teknik akan diaplikasikan secara bersamaan, yang membedakan hanya lokasi pengaplikasian.

3.2.1 Passive Interface

Pengaplikasian teknik *passive-interface* akan dilakukan pada interface router Tengah yang terhubung dengan router R_A.Interface tersebut akan dijadikan sebagai *silent host* sehingga pembaruan informasi routing mengenai jaringan yang ada pada router Tengah tidak akan diberikan kepada router R_A. Sehingga router R_A hanya memberikan informasi pembaruan tabel routingnya tanpa mendapatkan balasaninformasi pembaruan tabel routing dari router Tengah.

3.2.2 Route Filter

Pada desain topologi jaringan yang ditunjukkan Gambar 3.1, akan diterapkan penyaringan terhadap rute yang dilewatkan melalui jaringan. *Route Filtering*akan mengontrol informasi routing dan lalu lintas data. Teknik yang digunakan adalah teknik *distributelist dan offset list*. *Distribute-list* mengacu pada *access-list* untuk menyaring rute yang telah diberikan aturan, sedangkan offset list memanipulasi metric

Pada Gambar 3.1, *distribute-list* menyebabkan alamat ip 2.2.2.2 pada Client_2 tidak dapat melakukan aktifitas *ping* menuju alamat IPnetwork 1.1.1.0 pada router Client_1 karena alamat IP 2.2.2.2 telah difilter di router Kiri. Aktivitas selain *ping* diizinkan untuk dilakukan. *Route Filtering*akanmempengaruhi seluruh interface pada router yang akan dikenai aturan, yaitu interface pada router Client_2.

3.2.3 Routing Policy

Routing berdasar aturan dapat diartikan juga bahwa administrator dapat mengimplementasikan routing standar berdasar routing protokol tujuan. Routing protokol tujuan akan mengarahkan paket pada jalur terdekat menuju kepada tujuan. Routing protokol berdasarkan aturan, mengijinkan administrator untuk mendefinisikan apa yang mereka inginkan untuk diteruskan kepada jaringan. Routing berdasarkan aturan ini, menggunakan *Route Map.*

3.3 Analisis Kebutuhan Sistem

3.3.1 Kebutuhan Perangkat Keras

Dari Gambar 3.1 dan gambaran umum perangkat sistem, perangkat keras yang menunjang pada proses implementasi *passive-interface*, *route filter* dan *routing policy* tercantum sebagai berikut:

1. Kebutuhan Komputer

   Kebutuhan komputer yang digunakan untuk menjalankan Emulator GNS3 dengan spesifikasi sebagai berikut:

   a. Prosessor dengan kecepatan Minimum 3 GHz.

   b. Memori minimum 1 GB direkomendasikan diatas 1 GB.

   c. Hardisk dengan kapasitas minimal 5GB

   d. Mouse

   e. Keyboard

2. Kebutuhan Perangkat Lunak

   Kebutuhan perangkat lunak yang digunakan adalah dengan spesifikasi sebagai berikut:

   a. GNS3 : GNS3-beta-0.6-win32-all-in-one

      GNS3 adalah sebuah alat pelengkap untuk mensimulasikan lab yang sebenarnya bagi engineer, administrator dan orang-orang yang berkecimpung dalam dunia jaringan dan juga yang ingin lulus sertifikasi seperti CCNA, CCNP, CCIP, CCIE, JNCIA, JNCIS, JNCIE. GNS3 juga dapat digunakan untuk percobaan fitur dari Cisco IOS, Juniper junOS atau untuk memastikan konfigurasi yang dibutuhkan untuk dikembangkan di router yang sebenarnya.Proyek ini bersifat open source, program gratis yang dapat digunakan pada beberapa sistem operasi, termasuk Windows, Linux, dan MacOS X.

b. WinPcap : WinPcap_4_0_2

WinPcap adalah perangkat jaringan standar industri yang berjalan di network layer pada lingkungan kerja windows. WinPcap dapat menangkap dan mengirimkan paket jaringan melewati aturan protokol dan juga memiliki fitur tambahan termasuk filter paket hingga level kernel, mesin statistik jaringan.

c. Wireshark

Wireshark merupakan alat penganalisa jaringan yang paling sering digunakan, dan secara (de facto) dan (de yure) melalui standar banyak industri dan institusi pendidikan.

Sedangkan untuk kebutuhan yang digunakan dalam GNS3 tercantum dalam Tabel 3.1 dibawah ini:

Tabel 3.1 Komponen GNS3

Nama	Komponen
a. Router Cisco	a. Cisco Router 7200 Series
b. Cisco IOS	b. Cisco IOS C7200-adventerprisek9-mz.124-4.T1.bin
c. Interface Fast Ethernet	c. C7200-IO-FE
d. Interface Fast Ethernet (tambahan)	d. PA – 2FE – TX
e. Interface Loopback	e. Interface Loopback 0,dst

BAB IV

HASIL& PEMBAHASAN

4.1 Implementasi Secara Umum

Implementasi sistem merupakan tahapan dimana sistem mampu diaplikasikan dalam keadaan yang sebenarnya.Dari tahap implementasi ini dapat diketahui apakah sistem berjalan dengan baik atau tidak. Serta apakah sistem memberikan *output* yang sesuai dengan perancangan yang telah dibuat.

4.2 Tahapan Implementasi

4.2.1 Konfigurasi Router

4.2.1.1 Konfigurasi Hostname Router

Hostname pada router merupakan nama yang digunakan pada setiap router untuk membedakan agar tidak tertukar, karena interface setiap router memiliki tampilan yang sama.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Kanan
Kanan(config)#do wr
Building configuration...
[OK]
Kanan(config)#
```

4.2.1.2 Konfigurasi Alamat IP

Konfigurasi ini digunakan untuk memberikan alamat IP pada masing-masing *interface*di tiap router. Konfigurasi *interface* berlaku umum pada semua router yang berarti bahwa cara konfigurasi akan sama pada setiap router Cisco jenis apapun.

```
Kanan>enable
Kanan#configure terminal
Kanan(config)#interface fastEthernet 0/0
Kanan(config-if)#ip address 192.168.20.0 255.255.255.252
Kanan#
```

Tabel 4.3 merupakan tabel alamat IP yang digunakan dalam konfigurasi masing-masing router.

Tabel 4.1 Alamat IP

Router	Interface	Alamat IP
Client_1	Int Fa0/0	192.168.10.1 / 30
	Int Lo0	1.1.1.1 / 32
	Int Lo1	1.1.1.2 / 32
	Int Lo2	1.1.1.3 / 32
	Int Lo3	1.1.1.4 / 32
Client_2	Int Fa0/0	192.168.20.1 / 30
	Int Lo0	2.2.2.2 / 32
Kanan	Int Fa0/0	192.168.10.2 / 30
	Int Fa0/1	20.20.20.1 / 30
	Int Fa1/0	10.10.10.1 / 30
	Int Lo0	10.100.10.10 / 32
Kiri	Int Fa0/0	192.168.20.2 / 30
	Int Fa0/1	10.10.10.2 / 30

	Int Fa1/0	30.30.30.2 / 30
	Int Lo0	10.100.20.20 / 32
Tengah	Int Fa0/1	20.20.20.2 / 30
	Int Fa1/0	30.30.30.1 / 30
	Int Fa2/0	192.168.30.2 / 30
	Int Fa2/1	192.168.40.2 / 30
	Int Lo0	10.100.30.30 / 32
R_A	Int Fa0/0	192.168.30.1 / 30
	Int Lo0	3.3.3.3 / 32
R_B	Int Fa0/0	192.168.40.1 /30
	Int Lo0	4.4.4.4 / 32

4.2.1.3 Konfigurasi Protokol Routing

Konfigurasi ini bertujuan untuk menentukan protokol routing yang akan digunakan sebagai penghubung jaringan yang diinginkan. Cara konfigurasi protokolrouting *RIP*, *EIGRP* dan *OSPF*tidak jauh berbeda. Antara*RIP*dan*EIGRP*dapat dikatakan hampir sama, yang berbeda hanya pada *OSPF*, karena *OSPF* menggunakan nomor AS dan area untuk mengelompokkan router.

1. Konfigurasi Protokol RoutingRIP:

   Pada RIP, alamat IP jaringan yang didaftarkan dituliskan tanpa tambahan *subnet mask*.

```
Router>en
Router #conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.20.0
Router(config-router)#network 192.168.30.0
Router(config-router)#no auto-summary
Router(config-router)#exit
Router(config)#exit
```

2. Konfigurasi Protokol Routing EIGRP:

   Pada konfiguasi EIGRP, alamat IP jaringan didaftarkan beserta *subnetmask*.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 192.168.20.0 0.0.0.3
Router(config-router)#network 192.168.30.0 0.0.0.3
Router(config-router)#no auto-summary
Router(config-router)#exit
Router(config)#exit
```

3. Konfigurasi Protokol Routing OSPF:

   OSPF menggunakan area dalam membedakan wilayah keanggotaan routing, Area 0 digunakan sebagai suatu kewajiban, karena Area 0 merupakan *area backbone*. Area lain yang ingin bergabung, harus terhubung dengan Area 0.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 100
Router(config-router)#network 192.168.20.0 0.0.0.3 area 0
Router(config-router)#network 192.168.30.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#exit
```

4.2.1.4 Konfigurasi Passive Interface

Pada topologi di Gambar 3.1, router R_A yang terhubung dengan router Tengah ingin dijadikan silent host. Ini bisa dilakukan dengan cara mengkonfigurasi interface pada router Tengah yang terhubung ke router R_A.

Tidak ada perbedaan konfigurasi *passsive interface*untuk ketiga protokol routing. Interface router Tengah yang terhubung dengan router R_A adalah *interface FastEthernet 0/1*, Interface *FastEthernet* 0/1 dijadikan *silent host* dengan konfigurasi seperti dibawah ini:

1. Konfigurasi Passive Interface Untuk RIP

```
router rip
 version 2
 passive-interface FastEthernet1/0
 network 20.0.0.0
 network 30.0.0.0
 network 100.0.0.0
 network 192.168.30.0
 network 192.168.40.0
 no auto-summary
```

2. Konfigurasi Passive Interface Untuk EIGRP

```
router eigrp 10
 passive-interface FastEthernet1/0
 network 20.20.20.0 0.0.0.3
 network 30.30.30.0 0.0.0.3
 network 100.100.30.30 0.0.0.1
 network 192.168.30.0 0.0.0.3
 network 192.168.40.0 0.0.0.3
 no auto-summary
```

3. Konfigurasi Passive Interface Untuk OSPF

```
router ospf 100
 log-adjacency-changes
 passive-interface FastEthernet1/0
 network 20.20.20.0 0.0.0.3 area 0
 network 30.30.30.0 0.0.0.3 area 0
 network 100.100.30.30 0.0.0.1 area 0
 network 192.168.30.0 0.0.0.3 area 0
 network 192.168.40.0 0.0.0.3 area 0
```

4.2.1.5 Konfigurasi Route Filter

Terdapat 3 teknik yang dapat digunakan, yaitu: *offset list, distribute list dan route map*. Mengacu padatopologi di Gambar 3.1, maka digunakan *distribute list*dan *offset list*untuk memfilter rute yang akan masuk atau keluar dari suatu router. Teknik ini diaplikasikan pada sisi router Kiri untuk menyaringalamat IP Loopback milik Client_1menujurouter Client_2.

Distribute list dikombinasi dengan *access list* menghasilkan *route filter.Distribute list* terbagi kedalam dua macam, yaitu: *distribute list in* dan *distribute list out.*Pada penelitian ini, yang digunakan adalah *distibute list in.*

Konfigurasi *distribute list* diaktifkan pada sisi router Kiri, untuk melakukan penyaringan alamat *jaringan* 1.1.1.0agar tidak muncul pada tabel routing Client_2. Hal ini mengakibatkan tidak adanya hubungan antara router Client_2 dan Client_1.

EIGRP dan OSPF menggunakan distribute list, sedangkan RIP menggunakan offset list. Metric offset list adalah berdasarkan jumlah hop untuk mengatur keberadaan suatu tabel routing.

1. Konfigurasi Offset List pada RIP

    a. Konfigurasi Access List

```
access-list 1 permit 1.1.1.0 0.0.0.7
```

    b. Konfigurasi Offset List

```
router rip
 version 2
 offset-list 1 out 16 FastEthernet0/0
 network 10.0.0.0
 network 30.0.0.0
 network 100.0.0.0
 network 192.168.20.0
 no auto-summary
```

2. Konfigurasi pada EIGRP

    a. Konfigurasi Access List

```
access-list 1 deny   1.1.1.0 0.0.0.7
access-list 1 permit any
```

    b. Konfigurasi Distribute List

```
router eigrp 10
 network 20.20.20.0 0.0.0.3
 network 30.30.30.0 0.0.0.3
 network 100.100.30.30 0.0.0.1
 network 192.168.30.0 0.0.0.3
 network 192.168.40.0 0.0.0.3
 distribute-list 1 in
 no auto-summary
```

3. Konfigurasi pada OSPF

   a. Konfigurasi Access List

```
access-list 1 deny   1.1.1.0 0.0.0.7
```

   b. Konfigurasi Distribute List

```
router ospf 100
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 0
 network 30.30.30.0 0.0.0.3 area 0
 network 100.100.20.20 0.0.0.1 area 0
 network 192.168.20.0 0.0.0.3 area 0
 distribute-list 1 in
```

Pada router Kiri, nomor *accesslist* yang digunakan adalah 1. Nomor *accesslist* bebas penentuannya oleh administrator.

Pada offset list, almat IP 1.1.1.0 tidak akan muncul di tabel routing router Client_1, sehingga router Client_2 tidak dapat melakukan aktivitas apapun menuju router Client_1 dan begitu pula sebaliknya.

4.2.1.6 Konfigurasi Routing Policy

Aturan *routing policy*diaplikasikan pada router Kanan menggunakan kombinasi *access list* dan *route map.Routing Policy*digunakan untuk mengalihkan lalu lintas data melalui jalur yang telah ditentukan, sehingga menghindari kepadatan oleh lalur lintas data. Mekanisme tersebut disebut manipulasi lalu lintas atau trafik[EDW05].

Pengaturan yang dilakukan adalah melewatkan alamat IP genap secara otomatis menuju alamat IP 10.10.10.2 sedangkan alamat IP ganjil melalui jalur 20.20.20.1. Meskipun sumber yang mengirimkan adalah router yang sama, tetapi jalur yang digunakan akan berbeda menurut klasifikasi jenis alamat IP.

1. Konfigurasi Access List

```
access-list 1 permit 1.1.1.1 0.0.0.254
```

Cara kerja router dalam membedakan alamat IP genap dan ganjil adalah dengan melihat oktet terakhir alamat IP. Alamat IP 1.1.1.0 adalah alamat ganjil karena bit pada oktet terakhir adalah 1, sedangkan adalah alamat genap 1.1.1.0 karena oktet bit akhir adalah 0.

2. Konfigurasi Route Map

```
route-map Ganjil permit 10
match ip address 1
 set ip next-hop 20.20.20.1
```

Sintaks pada *route map* GANJIL mengacu pada aturan access list 1. Apabila terdapat paket dengan sumber alamat IP ganjil, maka alamat IP yang dituju berikutnya adalah 20.20.20.1.

3. Integrasi Route Map dengan Interface

Aturan yang telah dibuat pada *route map*, akan diintegrasikan dengan interface pada router Kanan.

```
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.252
 ip policy route-map Ganjil
 duplex half
```

4.3 Pengujian Hasil Implementasi

Pengujian hasil implementasi dimaksudkan untuk mengetahui keberhasilan dari simulasi optimasi routing yang dijalankan.

4.3.1 Pengujian Passive Interface

4.3.1.1 Menggunakan Wireshark

1. Pengujian pada RIP

   a. Sebelum Passive Interfaces

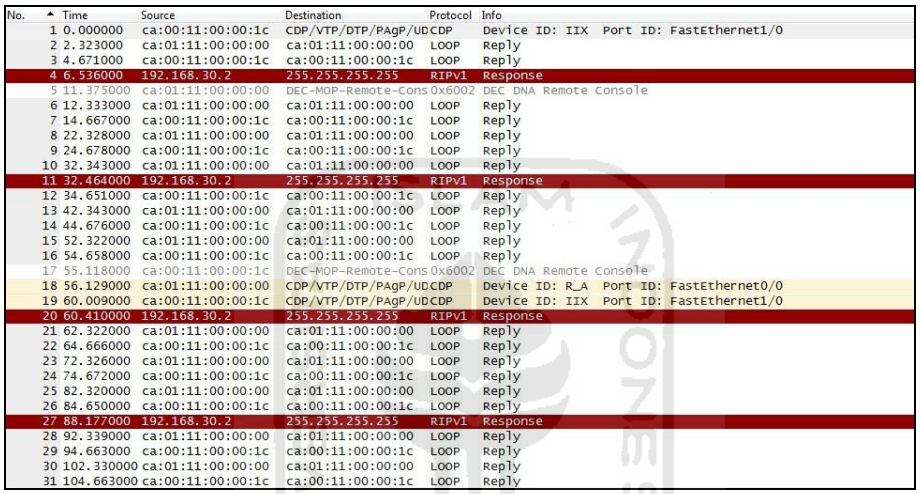
   Pengujian dilakukan dengan cara menangkap paket pada interface antara R_A (FastEthernet 0/0) dan Tengah (FastEthernet 1/0). Pada awal proses, Pada Gambar 4.4terlihat bahwa pesan response berasal dari alamat 192.168.30.1 (Tengah) dan 192.168.30.2 (R_A) secara bergantian.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
2	1.411000	ca:01:11:00:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
3	3.386000	192.168.30.1	255.255.255.255	RIPv1	Response
4	5.288000	ca:00:11:00:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
5	7.680000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
6	10.015000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
7	17.666000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
8	19.990000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
9	25.652000	192.168.30.2	255.255.255.255	RIPv1	Response
10	27.689000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
11	30.003000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
12	30.155000	192.168.30.1	255.255.255.255	RIPv1	Response
13	37.689000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
14	40.002000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
15	47.684000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
16	50.016000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
17	54.122000	192.168.30.2	255.255.255.255	RIPv1	Response
18	55.668000	192.168.30.1	255.255.255.255	RIPv1	Response
19	57.688000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
20	59.996000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
21	61.409000	ca:01:11:00:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
22	65.296000	ca:00:11:00:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
23	67.672000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
24	70.018000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
25	77.672000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
26	79.994000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
27	83.278000	192.168.30.2	255.255.255.255	RIPv1	Response
28	84.393000	192.168.30.1	255.255.255.255	RIPv1	Response
29	87.660000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
30	90.011000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
31	97.666000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply

Gambar 4.1 RIP Sebelum Passive Interface

b. Sesudah Passive Interfaces

Pada Gambar 4.5, setelah passive interface diaktifkan paket response hanya berasal dari 192.168.30.2 (R_A) karena router Tengah menganggap router R_A sebagai *silent_host*. Akibatnya router R_A tidak mendapatkan paket response dari alamat IP 192.168.30.1 yang merupakan router Tengah.



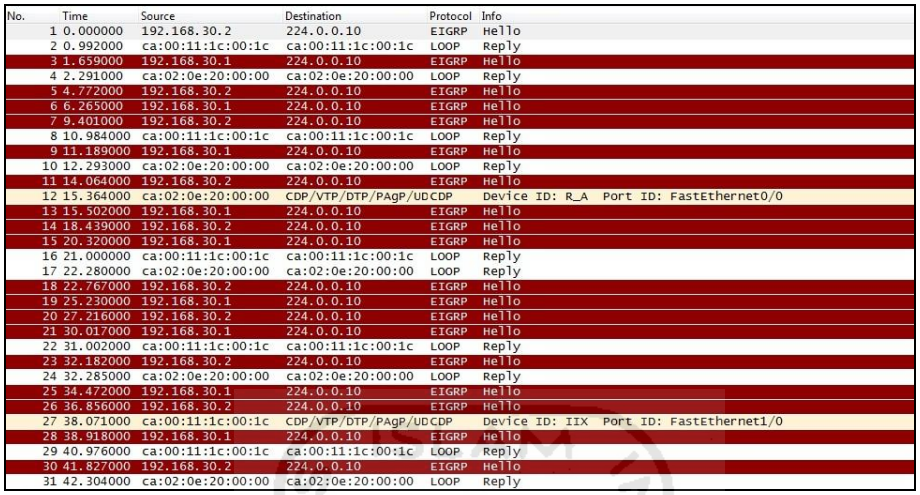
No.	Time	Source	Destination	Protocol	Info
1	0.000000	ca:00:11:00:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
2	2.323000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
3	4.671000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
4	6.536000	192.168.30.2	255.255.255.255	RIPv1	Response
5	11.375000	ca:01:11:00:00:00	DEC-MOP-Remote-Cons	0x6002	DEC DNA Remote Console
6	12.333000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
7	14.667000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
8	22.328000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
9	24.678000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
10	32.343000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
11	32.464000	192.168.30.2	255.255.255.255	RIPv1	Response
12	34.651000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
13	42.343000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
14	44.676000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
15	52.322000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
16	54.658000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
17	55.118000	ca:00:11:00:00:1c	DEC-MOP-Remote-Cons	0x6002	DEC DNA Remote Console
18	56.129000	ca:01:11:00:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
19	60.009000	ca:00:11:00:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
20	60.410000	192.168.30.2	255.255.255.255	RIPv1	Response
21	62.322000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
22	64.666000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
23	72.326000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
24	74.672000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
25	82.320000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
26	84.650000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
27	88.177000	192.168.30.2	255.255.255.255	RIPv1	Response
28	92.339000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
29	94.663000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply
30	102.330000	ca:01:11:00:00:00	ca:01:11:00:00:00	LOOP	Reply
31	104.663000	ca:00:11:00:00:1c	ca:00:11:00:00:1c	LOOP	Reply

Gambar 4.2 RIP Sesudah Passive Interface

2. Pengujian Pada EIGRP

Hasil pengujian sama dengan hasil pengujian pada RIP, namun jenis paket yang dikirimkan berbeda dari RIP yaitu paket hello. Hasil pengujian terdapat pada Gambar 4.6 dan 4.7

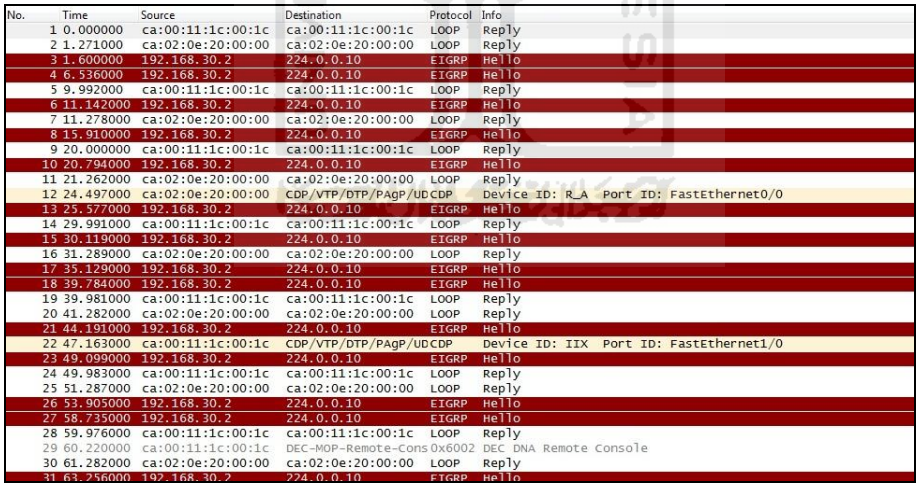
a. Sebelum Passive Interface



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.30.2	224.0.0.10	EIGRP	Hello
2	0.992000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
3	1.659000	192.168.30.1	224.0.0.10	EIGRP	Hello
4	2.291000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
5	4.772000	192.168.30.2	224.0.0.10	EIGRP	Hello
6	6.265000	192.168.30.1	224.0.0.10	EIGRP	Hello
7	9.401000	192.168.30.2	224.0.0.10	EIGRP	Hello
8	10.984000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
9	11.189000	192.168.30.1	224.0.0.10	EIGRP	Hello
10	12.293000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
11	14.064000	192.168.30.2	224.0.0.10	EIGRP	Hello
12	15.364000	ca:02:0e:20:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
13	15.502000	192.168.30.1	224.0.0.10	EIGRP	Hello
14	18.439000	192.168.30.2	224.0.0.10	EIGRP	Hello
15	20.320000	192.168.30.1	224.0.0.10	EIGRP	Hello
16	21.000000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
17	22.280000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
18	22.767000	192.168.30.2	224.0.0.10	EIGRP	Hello
19	25.230000	192.168.30.1	224.0.0.10	EIGRP	Hello
20	27.216000	192.168.30.2	224.0.0.10	EIGRP	Hello
21	30.017000	192.168.30.1	224.0.0.10	EIGRP	Hello
22	31.002000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
23	32.182000	192.168.30.2	224.0.0.10	EIGRP	Hello
24	32.285000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
25	34.472000	192.168.30.1	224.0.0.10	EIGRP	Hello
26	36.856000	192.168.30.2	224.0.0.10	EIGRP	Hello
27	38.071000	ca:00:11:1c:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
28	38.918000	192.168.30.1	224.0.0.10	EIGRP	Hello
29	40.976000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
30	41.827000	192.168.30.2	224.0.0.10	EIGRP	Hello
31	42.304000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply

Gambar 4.3 EIGRP Sebelum Passive Interface

b. Sesudah Passive Interface



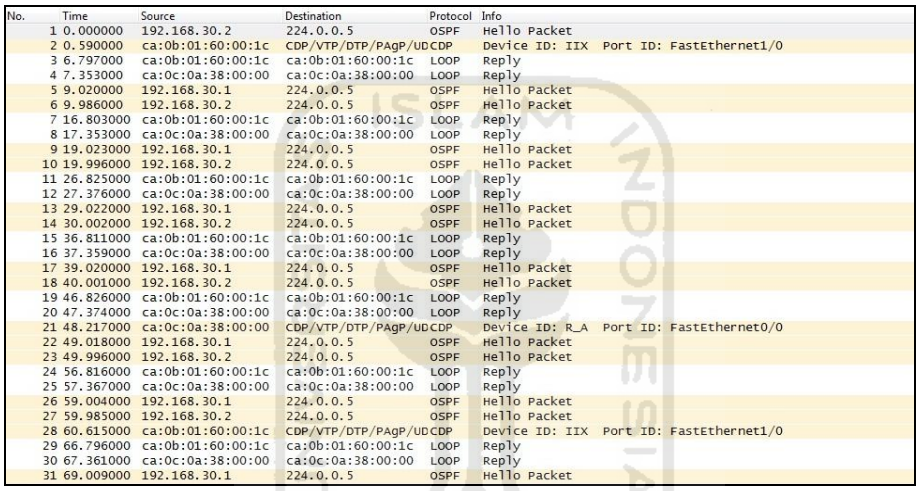
No.	Time	Source	Destination	Protocol	Info
1	0.000000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
2	1.271000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
3	1.600000	192.168.30.2	224.0.0.10	EIGRP	Hello
4	6.536000	192.168.30.2	224.0.0.10	EIGRP	Hello
5	9.992000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
6	11.142000	192.168.30.2	224.0.0.10	EIGRP	Hello
7	11.278000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
8	15.910000	192.168.30.2	224.0.0.10	EIGRP	Hello
9	20.000000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
10	20.794000	192.168.30.2	224.0.0.10	EIGRP	Hello
11	21.262000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
12	24.497000	ca:02:0e:20:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
13	25.577000	192.168.30.2	224.0.0.10	EIGRP	Hello
14	29.991000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
15	30.119000	192.168.30.2	224.0.0.10	EIGRP	Hello
16	31.289000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
17	35.129000	192.168.30.2	224.0.0.10	EIGRP	Hello
18	39.784000	192.168.30.2	224.0.0.10	EIGRP	Hello
19	39.981000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
20	41.282000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
21	44.191000	192.168.30.2	224.0.0.10	EIGRP	Hello
22	47.163000	ca:00:11:1c:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
23	49.099000	192.168.30.2	224.0.0.10	EIGRP	Hello
24	49.983000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
25	51.287000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
26	53.905000	192.168.30.2	224.0.0.10	EIGRP	Hello
27	58.735000	192.168.30.2	224.0.0.10	EIGRP	Hello
28	59.976000	ca:00:11:1c:00:1c	ca:00:11:1c:00:1c	LOOP	Reply
29	60.220000	ca:00:11:1c:00:1c	DEC-MOP-Remote-Cons	0x6002	DEC DNA Remote Console
30	61.282000	ca:02:0e:20:00:00	ca:02:0e:20:00:00	LOOP	Reply
31	63.256000	192.168.30.2	224.0.0.10	EIGRP	Hello

Gambar 4.4 EIGRP Sesudah Passive Interface

3. Pengujian Pada OSPF

Gambar 4.8 adalah gambar sebelum passive interface diaktifkan, terdapat dua alamat IP yang saling mengirimkan paket hello yang berisi pembaruan tabel routing. Apabila passive interface sudah diaktifkan, hanya akan ada satu alamat IP yang mengirimkan pembaruan tabel routing melalui alamat IP*multicast*.

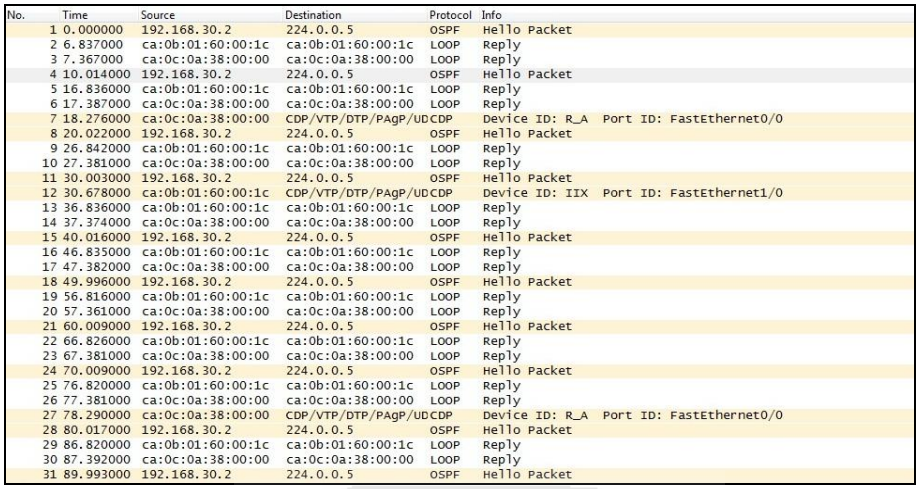
a. Sebelum Passive Interface



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
2	0.590000	ca:0b:01:60:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
3	6.797000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
4	7.353000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
5	9.020000	192.168.30.1	224.0.0.5	OSPF	Hello Packet
6	9.986000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
7	16.803000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
8	17.353000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
9	19.023000	192.168.30.1	224.0.0.5	OSPF	Hello Packet
10	19.996000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
11	26.825000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
12	27.376000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
13	29.022000	192.168.30.1	224.0.0.5	OSPF	Hello Packet
14	30.002000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
15	36.811000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
16	37.359000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
17	39.020000	192.168.30.1	224.0.0.5	OSPF	Hello Packet
18	40.001000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
19	46.826000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
20	47.374000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
21	48.217000	ca:0c:0a:38:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
22	49.018000	192.168.30.1	224.0.0.5	OSPF	Hello Packet
23	49.996000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
24	56.816000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
25	57.367000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
26	59.004000	192.168.30.1	224.0.0.5	OSPF	Hello Packet
27	59.985000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
28	60.615000	ca:0b:01:60:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
29	66.796000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
30	67.361000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
31	69.009000	192.168.30.1	224.0.0.5	OSPF	Hello Packet

Gambar 4.5 OSPF Sebelum Passive Interface

b. Sesudah Passive Interface



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
2	6.837000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
3	7.367000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
4	10.014000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
5	16.836000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
6	17.387000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
7	18.276000	ca:0c:0a:38:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
8	20.022000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
9	26.842000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
10	27.381000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
11	30.003000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
12	30.678000	ca:0b:01:60:00:1c	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: IIX Port ID: FastEthernet1/0
13	36.836000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
14	37.374000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
15	40.016000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
16	46.835000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
17	47.382000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
18	49.996000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
19	56.816000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
20	57.361000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
21	60.009000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
22	66.826000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
23	67.381000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
24	70.009000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
25	76.820000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
26	77.381000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
27	78.290000	ca:0c:0a:38:00:00	CDP/VTP/DTP/PAgP/UD	CDP	Device ID: R_A Port ID: FastEthernet0/0
28	80.017000	192.168.30.2	224.0.0.5	OSPF	Hello Packet
29	86.820000	ca:0b:01:60:00:1c	ca:0b:01:60:00:1c	LOOP	Reply
30	87.392000	ca:0c:0a:38:00:00	ca:0c:0a:38:00:00	LOOP	Reply
31	89.993000	192.168.30.2	224.0.0.5	OSPF	Hello Packet

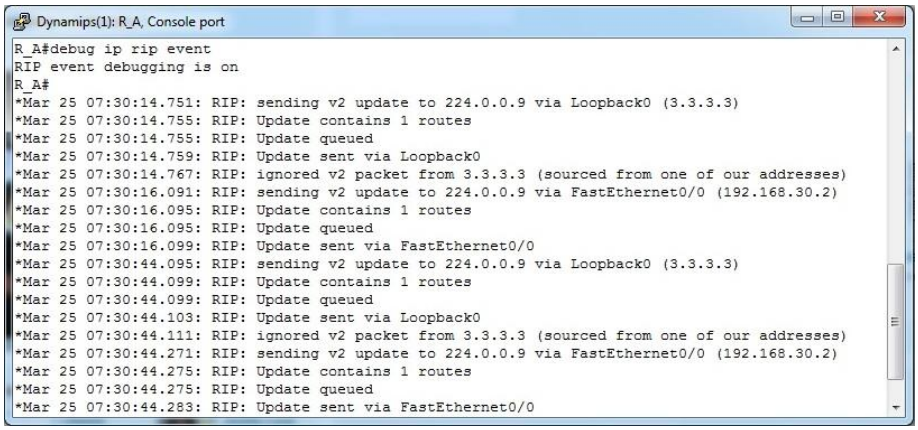
Gambar 4.6 OSPF Sesudah Passive Interface

4.3.1.2 Menggunakan Perintah Debug

1. Pengujian Pada RIP

Pada Gambar 4.10, terlihat bahwa router R_A mengirimkan pembaruan informasi routing melalui alamat IP 224.0.0.9 yang merupakan alamat IP broadcast, tetapi tidak mendapatkan pembaruan informasi routing dari 192.168.30.1 (Tengah).

Proses penerimaan pembaruan informasi didapat dari alamat IP 3.3.3.3 yang merupakan alamatIP loopback dari router R_A. Paket akan diabaikan karena alamat tersebut merupakan salah satu dari alamat yang dimiliki router R_A.

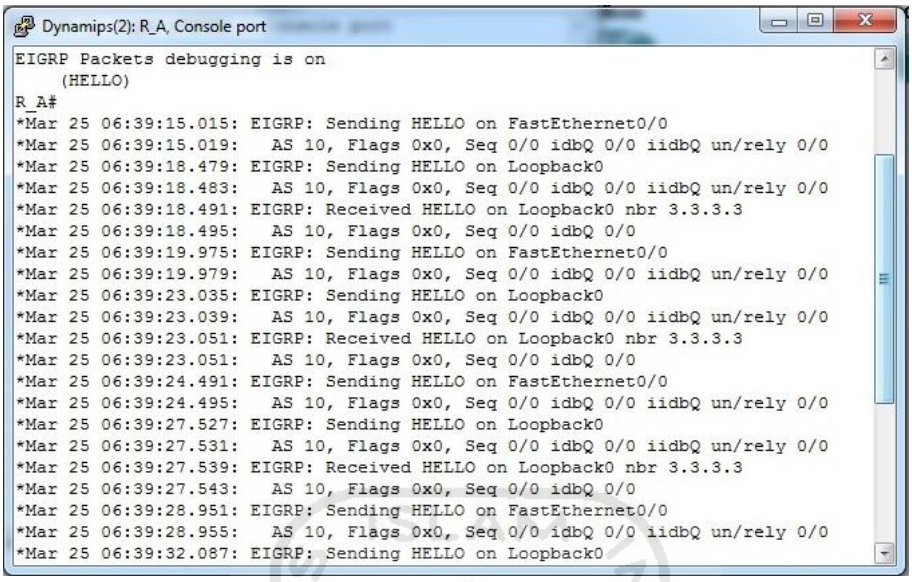


Gambar 4.7 Proses Debug IP RIP Events

2. Pengujian Pada EIGRP

Router R_A memiliki dua buah interface yaitu Loopback dan Fast Ethernet. Protokol routing EIGRP akan mengirimkan pembaruan tabel routing kepada interface yang terhubung.

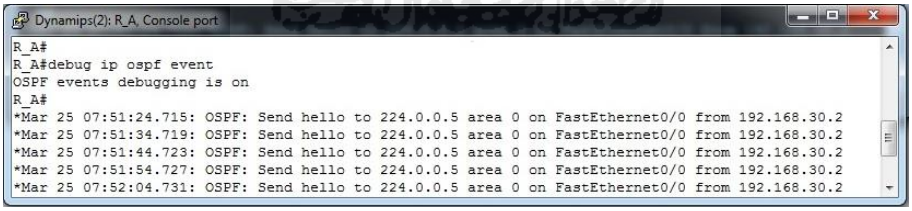
Paket hello yang dikirimkan menuju interface FastEthernet tidak mendapatkan respon paket hello, sedangkan paket yang dikirimkan melalui interface Loopback akan selalu mendapat respon karena Loopback merupakan interface milik router R_A seperti ditampilkan pada Gambar 4.11.



Gambar 4.8 Proses Debug EIGRP Packet Hello

3. Pengujian Pada OSPF

Gambar 4.12 menjelaskan tentang pengujian passive interface pada OSPF, paket hello akan dikirimkan menggunakan IP *multicast* 224.0.0.5 pada interface Fast Ethernet 0/0, namun tidak mendapat respon dari router Tengah.

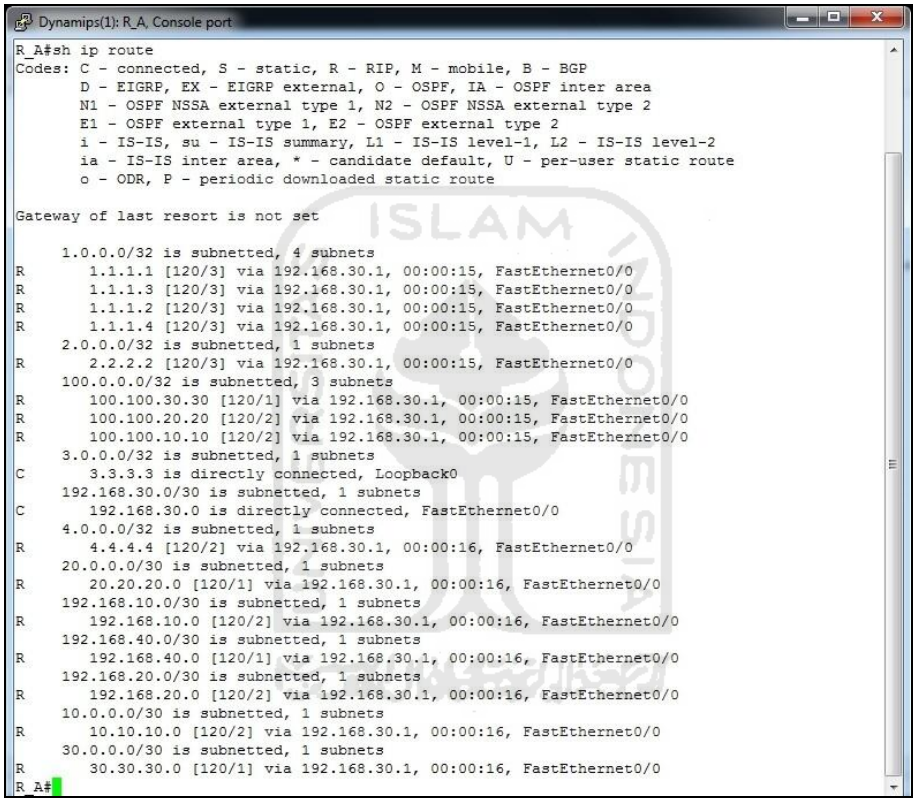


Gambar 4.9 Proses Debug IP OSPF Events

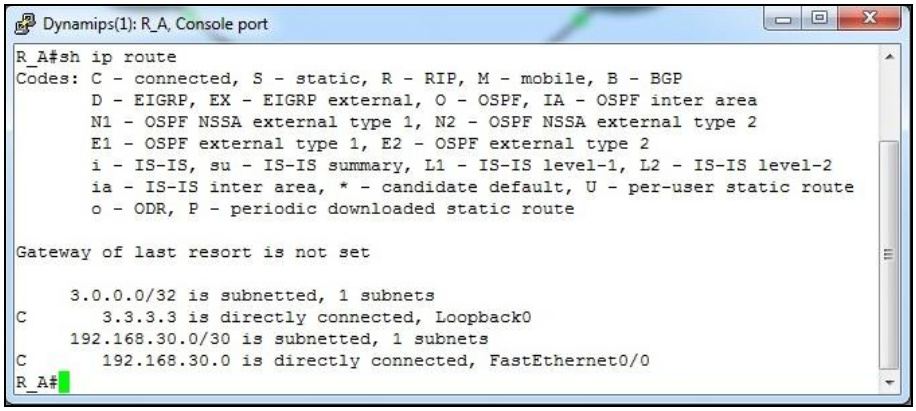
4.3.1.3 Menggunakan Perintah Show IP Route

1. Pengujian Pada RIP

Pengujian passive interface pada RIP dapat menggunakan perintah *show ip route* untuk menampilkan tabel routing yang ada pada router.



Gambar 4.10Sh Ip Route pada RIP Sebelum Passive Interface

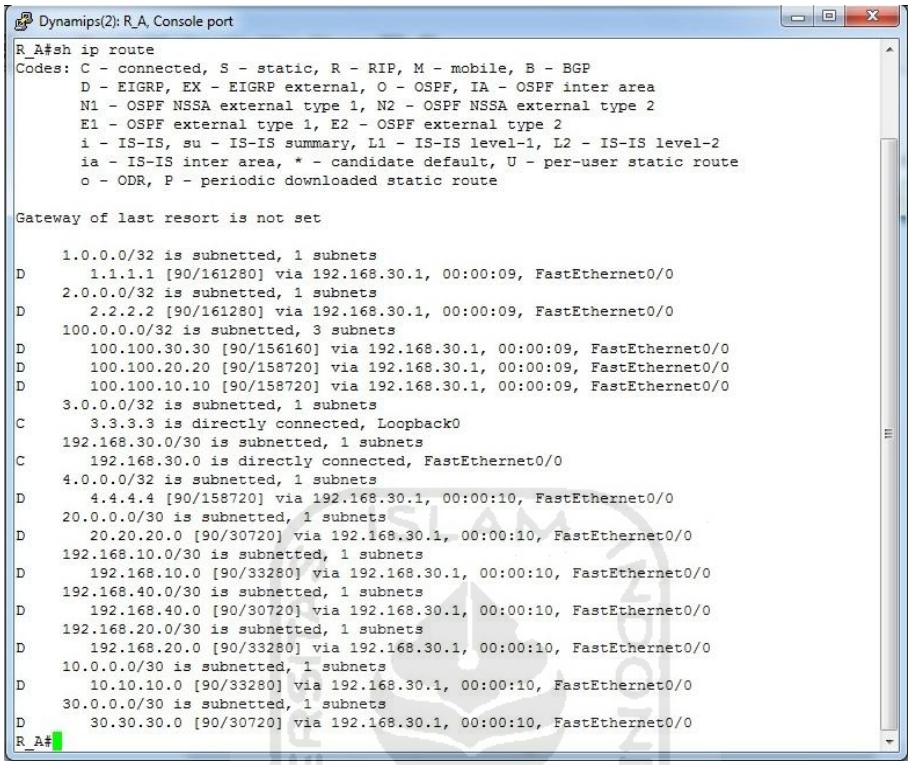


Gambar 4.11Sh Ip Route pada RIP Sesudah Passive Interface

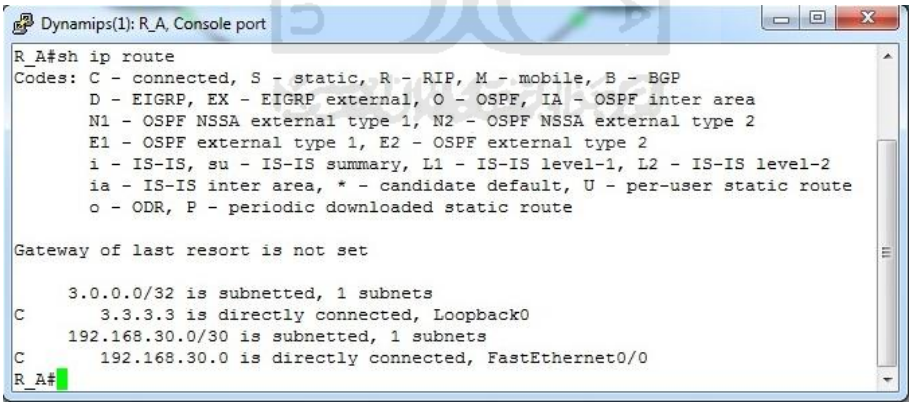
Gambar 4.13 merupakan tabel routing yang terdaftar oleh router R_A sebelum passive interface diaktifkan pada sisi router Tengah. Setelah passive Interface diaktifkan maka tabel routing akan hilang seperti yang ditampilkan pada Gambar 4.14.

2. Pengujian Pada EIGRP

Pada protokol routing EIGRP, untuk melihat tabel routing yang dikenali oleh router dapat menggunakan *show ip route.*



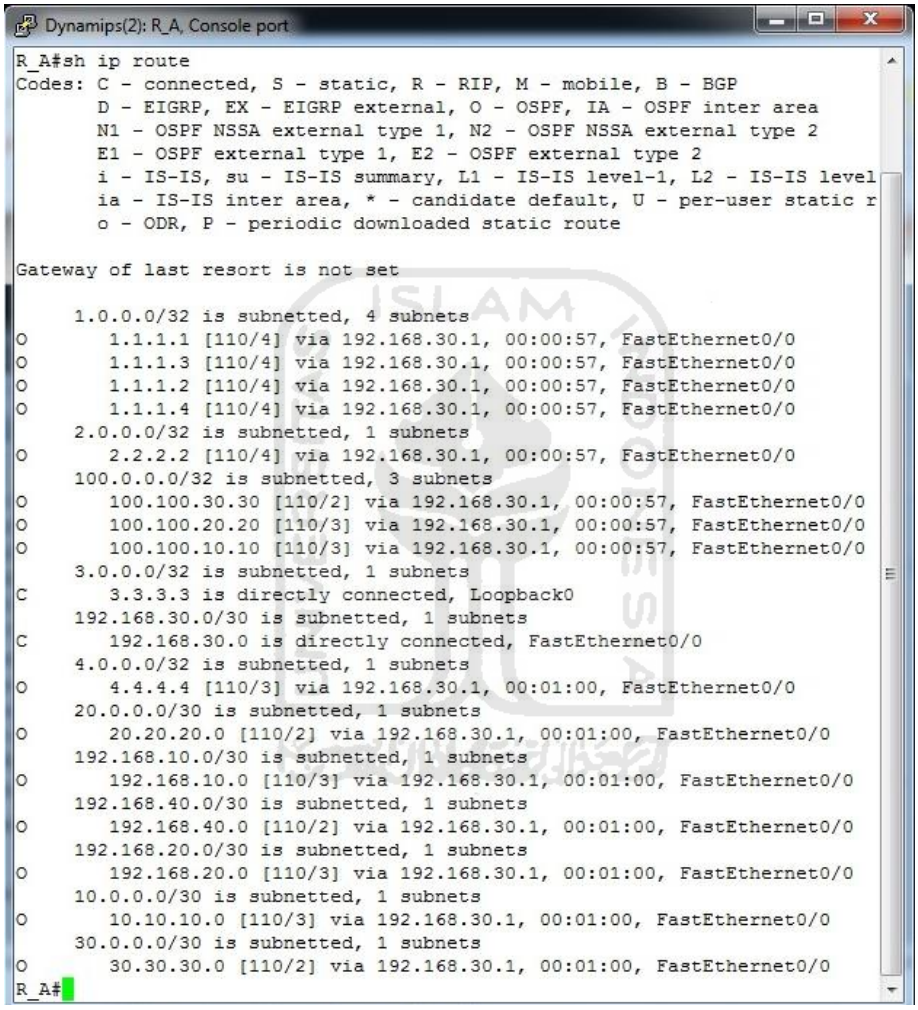
Gambar 4.12 Sh Ip Route pada EIGRP Sebelum Passive Interface



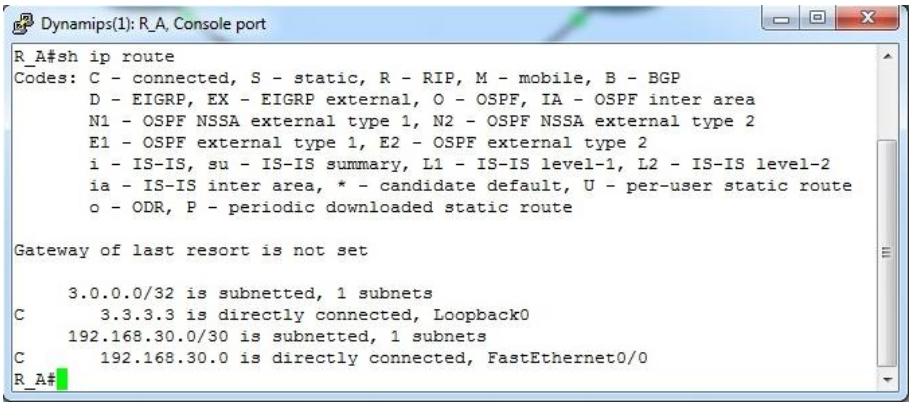
Gambar 4.13Sh Ip Route pada EIGRP Sesudah Passive Interface

3. Pengujian Pada OSPF

Tidak berbeda dengan RIP dan EIGRP, pada OSPF juga menggunakan *show ip route* untuk menampilkan tabel routing.



Gambar 4.14 Sh Ip Route pada OSPF Sebelum Passive Interface

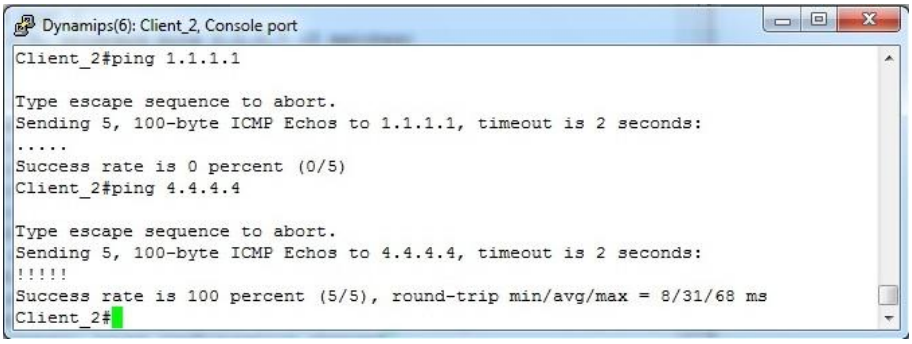


Gambar 4.15 Sh Ip Route pada OSPF Sesudah Passive Interface

4.3.2 Pengujian Route Filter

Pengujian terhadap teknik route filter ditandai router Client_2 tidak dapat menghubungi router Client_1, namun Client_2 berfungsi sebaliknya dan dapat menghubungi router lainnya menggunakan perintah ping seperti tampak pada Gambar 4.13.

1. Perintah Ping



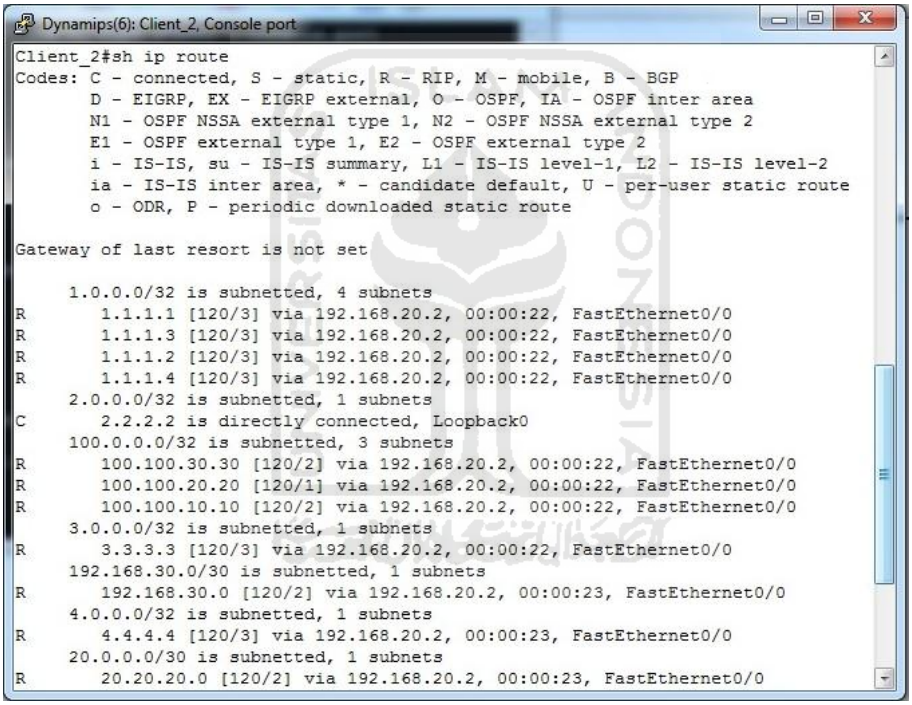
Gambar 4.16 Uji Route Filter dengan Ping

2. Show IP Route

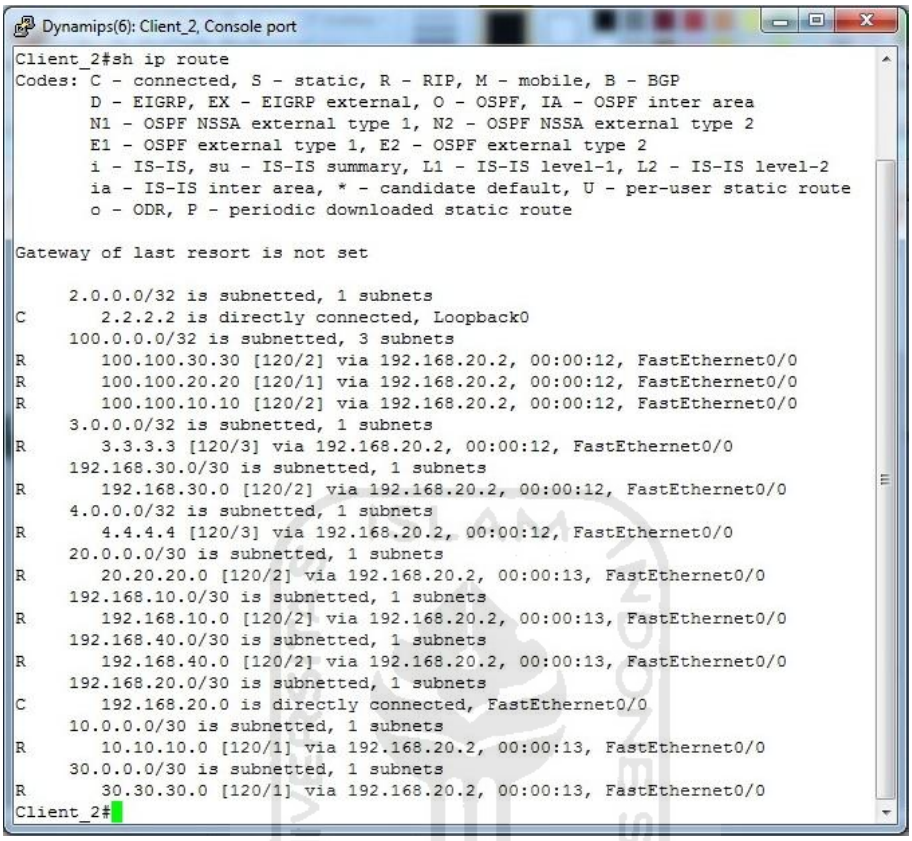
Perintah *show ip route* akan menampilkan rute network yang diketahui oleh suatu router.

a. RIP

Pengujian *show ip route* pada RIP pada Gambar 4.14 menampilkan bahwa network 1.1.1.0 yang memiliki 4 buah subnet masih ada pada fase awal tabel routing.



Gambar 4.17 Sebelum Offset List



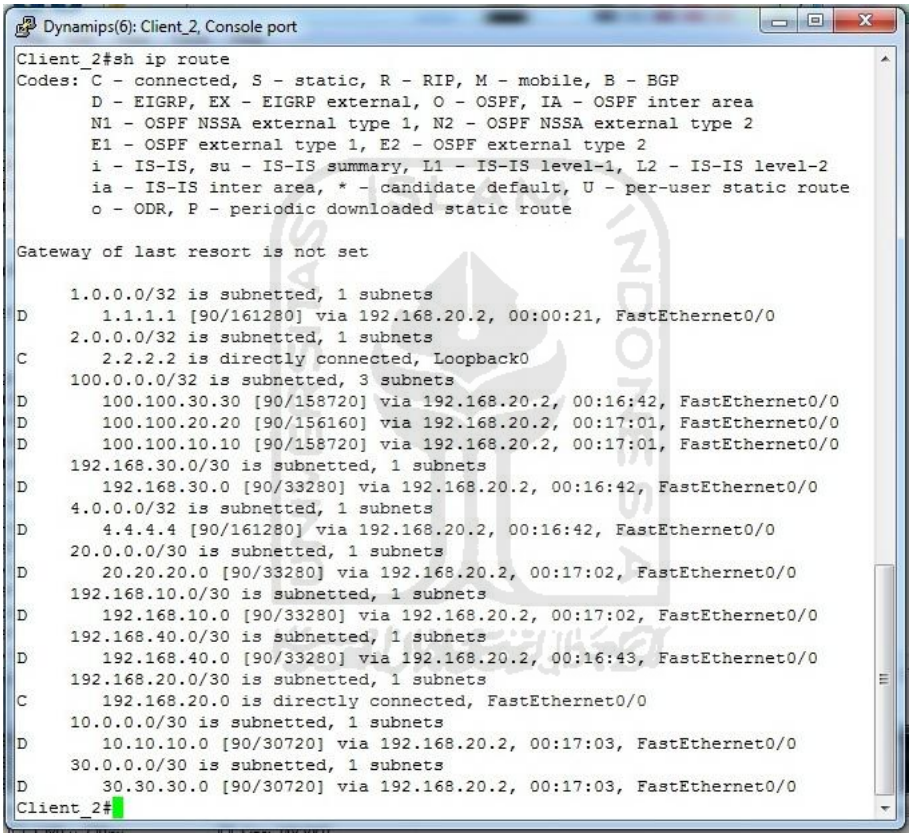
Gambar 4.18 Sesudah Offset List

Gambar 4.15 menampilkan tabel routing tanpa network 1.1.1.0, hilangnya informasi network tersebut diakibatkan oleh konfigurasi offset list dengan menambahkan metric pada hop menjadi 16 atau disebut *inaccessible*.

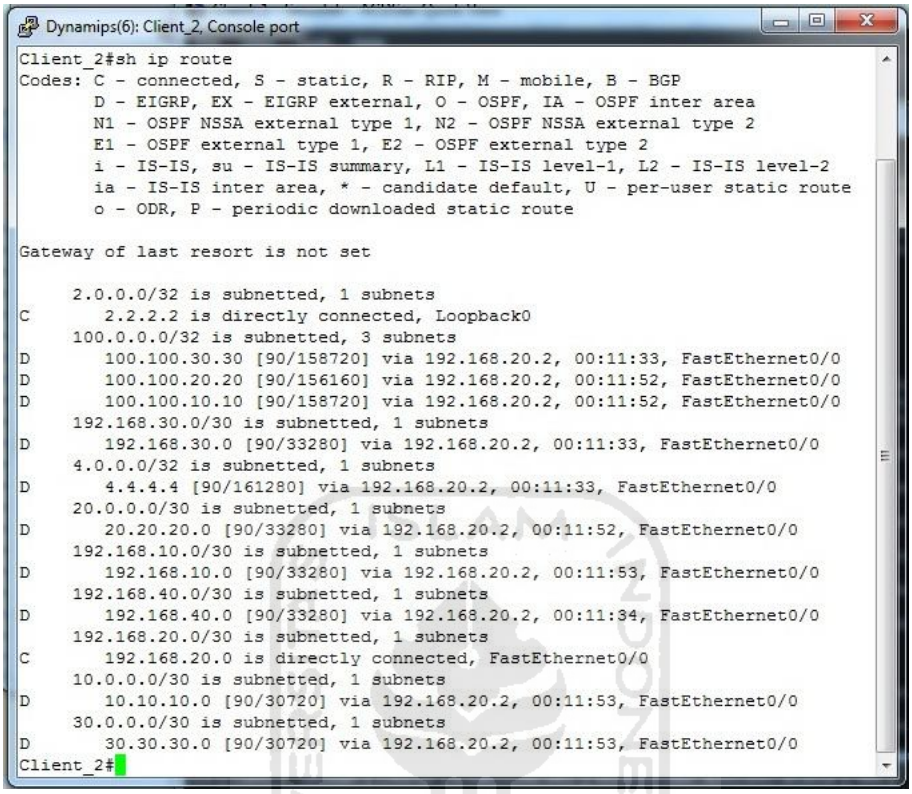
Hilangnya tabel routing mengakibatkan router Client_2 tidak dapat melakukan pertukaran data apapun menuju network 1.1.1.0.

b. EIGRP

Pada EIGRP, Gambar 4.16 memperlihatkan bahwa network 1.0.0.0 masih tercantum dalam tabel routing pada router Client_2. Hal tersebut menandakan Client_2 masih mengenal network milik router Client_1 selama masih terjadi pertukaran tabel routing antara kedua router.



Gambar 4.19 Sebelum Distribute List



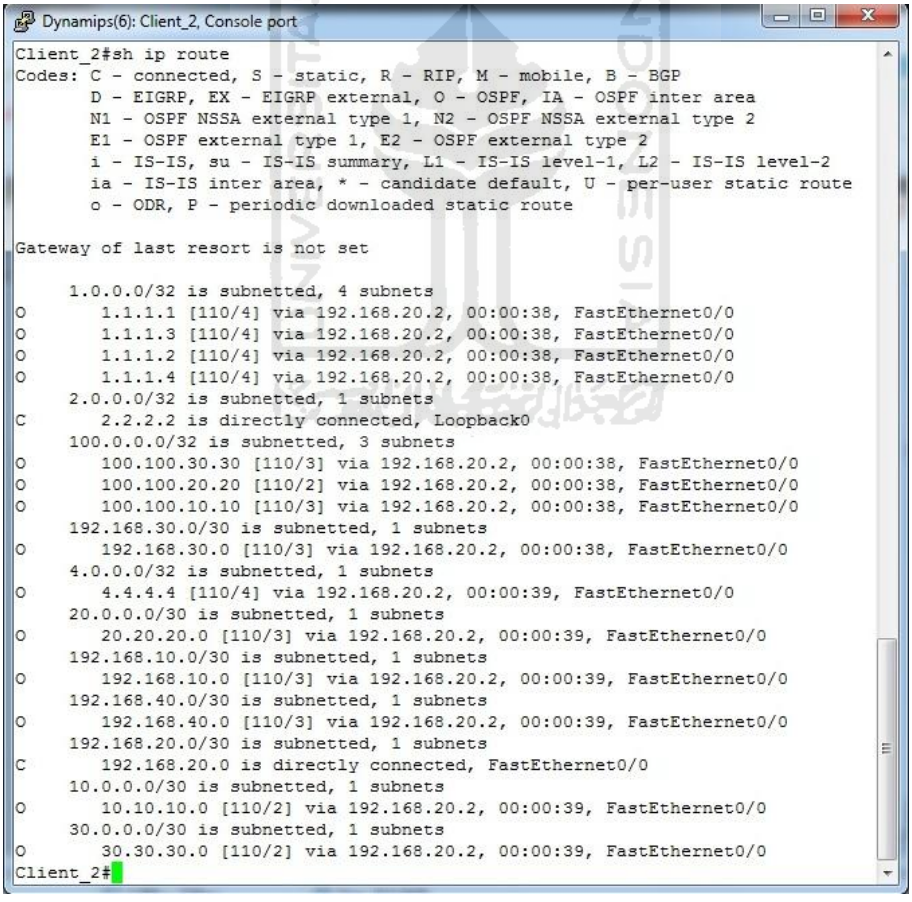
Gambar 4.20 Sesudah Distribute List

Gambar 4.17 merupakan hasil tabel routing yang terjadi setelah proses distribute list dijalankan pada router Kiri. Pada tabel routing tidak lagi tampak network 1.1.1.0 yang berasal dari router Client_1.Hal ini berakibat tidak dimungkinkan lagi pertukaran data antara router Client_1 dan Client_2.

c. OSPF

Struktur tabel routing pada OSPF pada Gambar 4.18 tidak mengalami perubahan baik sebelum dan sesudah konfigurasi distribute list pada router Kiri. Hal ini terjadi karena router tetap mengirimkan paket hello dari neighbor Client_1.

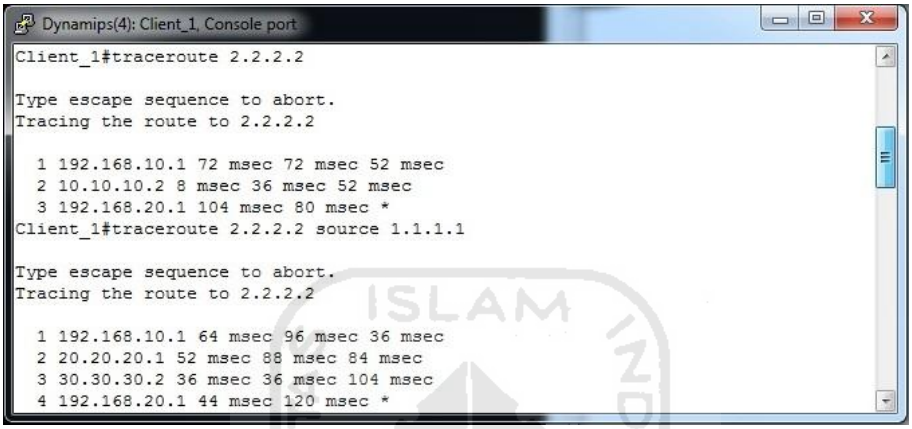
Pada distribute list OSPF, paket hello akan tetap dikirim ke seluruh interface. Yang berbeda adalah didalam paket hello yang dikirimkan, tidak dicantumkan neighbor Client_2, sehingga pada tabel routing yang lama masih tercantum sebagai neighbor meski tidak dapat terhubung.



Gambar 4.21 Tabel Routing OSPF Sesudah Distribute List

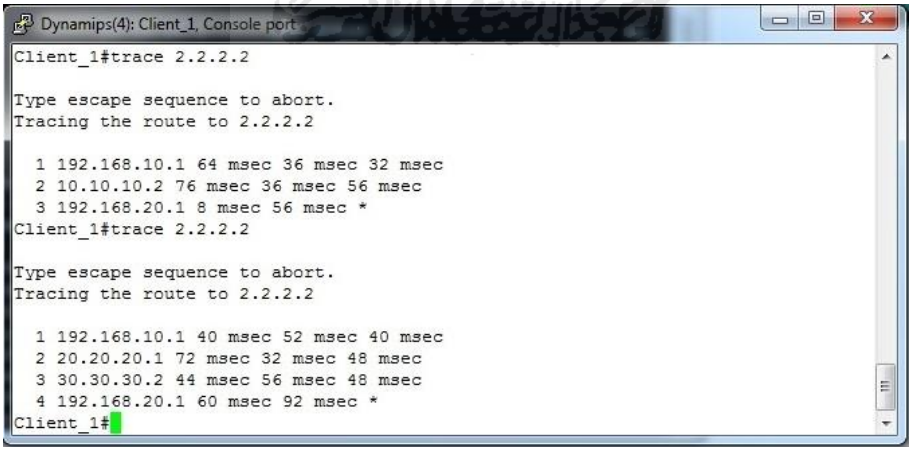
4.3.3 Pengujian Routing Policy

Pengujian terhadap routing policy dilakukan dengan menggunakan perintah *traceroute*. Seperti pada Gambar 4.19.



Gambar 4.22 Traceroute

Pada Gambar 4.20 terlihat bahwa meskipun konfigurasi jalur telah dirubah namun ketika salah satu jalur mati, paket akan tetap dialihkan menuju jalur lain yang dikenali oleh router.



Gambar 4.23 Fail Over Berjalan Normal

4.4 Hasil Analisis

4.4.1 Passive Interface

Teknik passive interface yang diaplikasikan pada router mengakibatkan router kehilangan tabel routing yang berfungsi sebagai data tentang rute yang dikenali oleh sebuah router.

Hasil analisis passive interface yang menggunakan protokol routing RIP, EIGRp dan OSPF adalah pada Tabel 4.2 sebagai berikut :

Tabel 4.2 Analisis Passive Interface

Protokol	Jumlah Subnet	
	Sebelum	Sesudah
RIP	17	2
EIGRP	17	2
OSPF	17	2

Kegunaan passive interface adalah untuk memutus pembaruan routing pada salah satu router ketika redistribusi dua routing protokol sedang berlangsung, untuk menghindari *down time* pada saat kehilangan informasi routing pada salah satu protokol routing.

4.4.2 Route Filter

Pada route filter, terdapat terdapat dua cara yaitu Distribute List dan Offset List. Keduanya melakukan hal yang sama, yaitu memfilter rute yang diizinkan ataupun tidak diizinkan untuk dilewatkan dengan menggunakan aturan yang sama. Hasil analisis terdapat pada Tabel 4.3.

Tabel 4.3 Analisis Route Filter

Protokol	Jumlah Subnet	
	Sebelum	**Sesudah**
RIP	17	13
EIGRP	17	12
OSPF	17	12

4.4.3 Route Policy

Pada Tabel 4.4, hasil tabel routing tidak mengalami perubahan. Hanya saja jika dilihat dari pembagian beban pada setiap interface akan merata jika lalu lintas data sedang dalam load tinggi.

Tabel 4.4 Analisis Route Policy

Protokol	Jumlah Subnet	
	Sebelum	**Sesudah**
RIP	17	17
EIGRP	17	17
OSPF	17	17

Fungsi route map pada umumnya adalah untuk memanipulasi trafik data, agar data dapat sampai ke tujuan dengan berbagai jalur untuk menghindari jalur data penuh trafik..

BAB V

PENUTUP

5.1 Kesimpulan

5.1.1 Passive Interface

a. *Passive interface* merupakan teknik untuk membuat router tidak dapat menerima atau mengirim pembaruan informasi tabel routing kepada tetangganya.

b. *Passive Interface* mengakibatkan router yang dijadikan*silent host*, hanya dapat berhubungan dengan router yang memiliki interface terhubung langsung.

5.1.2 Route Filter

a. *Route Filter* merupakan sekelompok aturan yang mengatur rute mana saja yangakan dikirim dan diterima oleh router.

b. *Offset List* merupakan aturan route filter yang dapat digunakan pada RIP, karena RIP menggunakan hop sebagai acuan metric. Apabila hop lebih dari 15, maka paket akan dibuang.

5.1.3 Policy Routing

a. *Policy routing* dapatdigunakan untuk mengatur atau mengontrol jalur yang akan dilewati oleh paket data, sehingga admin dapat mengkonfigurasi router untuk mengambil jalur berdasar tujuan terdekat.

b. *Policy routing*tidak akan menganggu mekanisme *fail over* suatu protokol routing.

5.2 Saran

a. Meskipun ketiga teknik telah diterapkan, ada baiknya ditambahkan analisis QoS untuk memaksimalkan performa.

b. Penggunaan ketiga teknik optimasi sangat bergantung pada kondisi topologi jaringan, karena teknik tersebut memiliki banyak faktor ketika akan diterapkan,antara lain jalur paket data, neighbor yang terhubung, dan posisi router. Baiknya terlebih dahulu ditinjau melalui rancangan topologi agar aturan-aturan yang akan diterapkan agar tidak berbenturan satu sama lain.

DAFTAR PUSTAKA

[IZAL07] Izal (2007).

*Laporan Jaringan.http://student.eepis-its.edu/~izankboy/laporan/Jaringan*diakses 14 Desember 2010

[EDW05] Edwards Wade, et al (2005).

CCNP Complete Study Guide. Sybex, Inc.

[CIS10] Cisco.
*IP Routing Protocols Commandshttp://www.cisco.com/en/US/docs/ios/12_3/iproute/command/reference/ip2_o1g.html*diakses tanggal 20 Desember 2010

[CIS07] CCNA Exploration 4.0. (2007).

Routing Protocol and Concepts. Cisco Networking Academy