PERANCANGAN *GATEWAY REDUNDANCY* MENGGUNAKAN *CARP, IFSTATED* DAN *PFSYNC* UNTUK MENINGKATKAN RELIABILITAS KONEKSI JARINGAN INTERNET



KONSENTRASI TEKNIK INFORMATIKA DAN KOMPUTER



DEPARTEMEN PENDIDIKAN NASIONAL UNIVERSITAS BRAWIJAYA FAKULTAS TEKNIK MALANG 2009



# PERANCANGAN GATEWAY REDUNDANCY MENGGUNAKAN CARP, IFSTATED DAN PFSYNC UNTUK MENINGKATKAN RELIABILITAS KONEKSI JARINGAN INTERNET

# SKRIPSI KONSENTRASI TEKNIK INFORMATIKA DAN KOMPUTER

Diajukan kepada Universitas Brawijaya Malang untuk memenuhi persyaratan memperoleh gelar Sarjana Teknik



DEPARTEMEN PENDIDIKAN NASIONAL UNIVERSITAS BRAWIJAYA FAKULTAS TEKNIK MALANG 2009



PERANCANGAN GATEWAY REDUNDANCY MENGGUNAKAN CARP, IFSTATED DAN PFSYNC UNTUK MENINGKATKAN RELIABILITAS KONEKSI JARINGAN INTERNET

# SKRIPSI KONSENTRASI TEKNIK INFORMATIKA DAN KOMPUTER

Diajukan untuk memenuhi persyaratan memperoleh gelar Sarjana Teknik

Oleh MARJHY M NIM. 0510632022-63

Telah Diperiksa dan Disetujui Dosen Pembimbing

H

Ir. Heru Nurwarsito, M.Kom. NIP. 19650402 199002 1 001 <u>Suprapto, ST., MT.</u> NIP. 19710727 199603 1 001

BRAWIJAYA

# LEMBAR PENGESAHAN

# PERANCANGAN GATEWAY REDUNDANCY MENGGUNAKAN CARP, IFSTATED DAN PFSYNC UNTUK MENINGKATKAN RELIABILITAS KONEKSI JARINGAN INTERNET

# SKRIPSI

KONSENTRASI TEKNIK INFORMATIKA DAN KOMPUTER

Diajukan untuk memenuhi persyaratan memperoleh gelar Sarjana Teknik

Oleh MARJHY M NIM. 0510632022-63

Skripsi ini telah diuji dan dinyatakan lulus pada tanggal 3 Agustus 2009

Majelis Penguji:

Raden Arief. Setyawan, ST., MT. NIP. 19750819 199903 1 001 <u>Ir. Sutrisno MT.</u> NIP. 19570325 198701 1 001

Ir. Muhammad Aswin MT. NIP. 19640626 199002 1 001

Mengetahui: Ketua Jurusan Teknik Elektro

Ir. Heru Nurwarsito, M.Kom. NIP. 19650402 199002 1 001

# KATA PENGANTAR

Puji syukur alhamdulillah kehadirat Allah SWT. penulis panjatkan atas segala berkah, rahmat, karunia dan hidayah-Nya, sehingga penyusunan skripsi ini dapat diselesaikan dengan baik sesuai waktu yang telah direncanakan, dengan judul "Perancangan Gateway Redundancy Menggunakan Carp, Ifstated dan pfsync Untuk Meningkatkan Reliabilitas Koneksi Jaringan Internet". Skripsi ini disusun untuk memenuhi persyaratan kelulusan dalam menyelesaikan pendidikan dan memperoleh gelar Sarjana Teknik di Fakultas Teknik Jurusan Teknik Elektro Universitas Brawijaya Malang.

Penulis menyadari bahwa tanpa bantuan dari banyak pihak, penyusunan skripsi ini tidak akan selesai dengan baik. Oleh karena itu perkenankanlah saya menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada:

- 1. Ir. Heru Nurwarsito, M.Kom. sebagai pembimbing I dengan sungguhsungguh memberikan bimbingan penuh kesabaran dan keramahan, sehingga penulis dapat menyelesaikan penyusunan skripsi ini dari awal hingga akhir.
- 2. Suprapto, ST., MT. sebagai pembimbing II yang meluangkan waktu ditengahtengah kesibukan memberikan bimbingan dengan ketelitian, kesabaran dan ikhlas sehingga penyusunan skripsi ini selesai dengan baik.

BRAWIJAY

- Ir. Heru Nurwarsito, M.Kom. dan Rudy Yuwono, ST., M.Sc. selaku Ketua Jurusan dan Sekretaris Jurusan Teknik Elektro Fakultas Teknik Universitas Brawijaya Malang.
- 4. Arief Andy Soebroto, ST., M.Kom. selaku KKDK Konsetrasi Teknik Informatika dan Komputer yang telah memberikan bimbingan sejak masamasa perkuliahan dan selama pengerjaan proposal skripsi.
- 5. Seluruh Staf Pengajar dan Karyawan Jurusan Teknik Elektro Universitas Brawijaya Malang yang telah memberikan bimbingan dengan ilmu pengetahuan melalui perkuliahan, seminar atau diskusi pada masa kuliah yang mereka bina dan membantu segala sesuatu yang berkaittan dengan administrasi akademis.
- Rekan-rekan Asisten Laboratorium Komputer dan Informatika atas segala bantuannya
- Rekan-rekan Paket E serta teman-teman lainnya yang tidak mungkin disebutkan satu-persatu yang telah membantu penulis dalam penyelesaian skripsi ini.

Semoga amal kebaikan dan bantuan yang telah diberikan baik moril maupun materiil dari berbagai pihak pada penulis mendapatkan imbalan yang berlebih dari Allah SWT.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna, oleh karena itu jika ditemukan kesalahan dan hal-hal yang menyimpang dari kaidahkaidah ilmiah, penulis sangat mengharapkan sumbang saran dan kritik membangun sebagai bahan koreksi menuju perbaikan. Akhirnya, semoga ada manfaat yang dapat dipetik dari tulisan sederhana ini. Amin Ya Robabal 'alamin.

MINERSITAS

Malang, Juli 2009

Penulis BRAW

#### ABSTRAK

Marjhy M. 2009. : Perancangan *Gateway Redundancy* Menggunakan CARP, *ifstated* dan *pfsync* untuk Meningkatkan Reliabilitas Jaringan Internet. Skripsi Jurusan Teknik Elektro, Fakultas Teknik, Universitas Brawijaya. Dosen Pembimbing : Ir. Heru Nurwarsito, M.Kom. dan Suprapto ST., MT

Reliabilitas suatu jaringan Internet merupakan hal yang mutlak dibutuhkan untuk menunjang fungsinya sebagai komponen sistem informasi. Kegagalan layanan ISP dan ketidaktersediaan gateway sebagai gerbang koneksi dapat menyebabkan menurunnya reliabilitas suatu jaringan Internet. Oleh karena itu diperlukan suatu rancangan gateway redundancy, yaitu suatu sistem yang dapat mendeteksi putusnya layanan ISP utama, dan mengalihkan koneksi Internet ke ISP backup (ISP-failover), juga sistem yang dapat mengatasi putusnya koneksi Internet karena kegagalan kerja gateway(Gateway-failover).

Perancangan dan implementasi Gateway Redundancy dilakukan dengan menggunakan sistem Operasi OpenBSD, serta perangkat lunak CARP, Ifstated, PF, dan pfsync. Perancangan gateway redundancy dengan menggunakan CARP ifstated dan pfsync ini dibagi menjadi dua tahap utama, yaitu perancangan perangkat keras dan perancangan perangkat lunak. Perancangan perangkat keras meliputi perancangan topologi jaringan komputer. Perancangan perangkat lunak meliputi perancangan jaringan komputer secara logical, perancangan gateway failover menggunakan CARP, perancangan ifstated untuk mendeteksi koneksi ke ISP, perancangan pfsync untuk sinkronasi data antara 3 gateway serta perancangan aturan-aturan firewall menggunakan pf untuk mengkonfigurasi NAT dan aturan-aturan lain yang mendukung.

Dari hasil pengujian dan analisis sistem gateway redundancy dengan menggunakan CARP, ifstated, dan pfsync, dapat disimpulkan bahwa kegagalan koneksi Internet yang mempengaruhi Reliabilitas koneksi jaringan Internet, dapat diatasi dengan sistem Gateway Redundancy. CARP dapat melakukan fail-over redundancy, yang berfungsi mengatasi kegagalan fungsi Gateway Internet. CARP melakukan advertisement setiap  $\pm 1$  detik. Waktu delay yang terjadi akibat perpindahan gateway master ke gateway backup 1 adalah  $\pm 3,5$  detik, perpindahan gateway backup 1 ke gateway backup 2 adalah  $\pm 3,8$  detik. Ifstated dapat mendeteksi putusnya koneksi ke ISP 1, dan mengalihkan koneksi ISP 2. Waktu delay perpindahan koneksi yang terjadi antara tidak aktifnya ISP 1 dan digantikan dengan ISP 2 adalah  $\pm 11,2$  detik, hal ini dipengaruhi oleh konfigurasi yang dilakukan di ifstated. Pfsync dapat melakukan sinkronisasi state table, dari gateway satu ke gateway yang lain.

Kata Kunci: Reliabilitas Jaringan Internet, ISP-failover, Gateway-failover, CARP, pfsyny, ifstated.

# DAFTAR ISI

KATA PENGANTAR	i
ABSTRAK	iv
DAFTAR ISI	v
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
NE	
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan	2
1.5 Sistematika Penulisan	2
BAB II TINJAUAN PUSTAKA	
2.1 Gateway Redundancy	4
2.2 Transmission Control Protocol/Internet Protocol (TCP/IP)	5
2.3 Topologi Jaringan	16
2.3.1 Topologi Bus	17
2.3.2 Topologi Star	17
2.3.3 Topologi Ring	18

۷

2.4 CARP	19
2.5 Protokol <i>pfsync</i>	23
2.6 Multicast	23
2.7 PF	24
2.8 Ifstated	33
2.9 Ping	35
2.10 HTTP (Hyper Text Transfer Protocol)	35
2.11 Wireshark	37
BAB III METODOLOGI PENELITIAN	

3.1 Studi Literatur	38
3.2 Perancangan dan Implementasi Sistem	38
3.3 Pengujian dan Analisis Sistem	39
3.4 Pengambilan Kesimpulan dan Saran	40
4.1 Analisis Kebutuhan	41
4.1.1 Spesifikasi Sistem	41
4.1.2 Analisis Context Diagram dan Data Flow Diagram (DFD)	44
4.2 Perancangan Perangkat Keras	48
4.3 Perancangan Perangkat Lunak	49

4.3.1 Perancangan Jaringan Komputer Secara Logical	49
4.3.2 Perancangan Gateway Failover	50
4.3.3 Perancangan ISP <i>failover</i>	52
4.3.4 Perancangan Pfsync Untuk Sinkronasi Data Antara 3 Gateway	52
4.3.5 Perancangan Aturan-Aturan Untuk Mengkonfigurasi Nat	53

# BAB V IMPLEMENTASI SISTEM TAS BRA

5.1 Implementasi Jaringan Komputer		54
5.1.1 Perangkat Keras Jaringan Komputer		54
5.1.2 Perangkat Lunak Jaringan Komputer		55
5.1.2.1 Konfigurasi Komputer Gateway		55
5.1.2.2 Konfigurasi Komputer ISP 1	Ģ	59
5.1.2.3 Konfigurasi Komputer ISP 2		60
5.1.2.4 Konfigurasi Komputer Client		61
5.2 Implementasi <i>Gateway failover</i> pada Komputer <i>Gateway Mas</i>	ter (	64
5.3 Implementasi Gateway failover pada Komputer Gateway Bac	kup 1 (	66
5.4 Implementasi Gateway failover pada Komputer Gateway Back	kup 2 (	68
5.4 Implementasi ISP <i>failover</i> pada Komputer <i>Gateway</i>		70

# **BAB VI PENGUJIAN SISTEM**

6.1 Pengujian dan Analisis Internal Network	73
---	----

6.2 Pengujian dan Analisis <i>External Network</i>	
6.3 Pengujian dan Analisis Sistem gateway fail-over saat Gateway Master Gagal	
Bekerja	78
6.4 Pengujian dan Analisis Sistem gateway fail-over saat Gateway Master dan	
Gateway Backup 2 Gagal Bekerja	98
6.5 Pengujian dan Analisis Sistem ISP fail-over dalam Mendeteksi Putusnya	
Koneksi ke ISP dan Melakukan Peralihan Jalur	119

# BAB V PENUTUP ERSITAS BRAWIN

7.1 Kesimpulan		133
7.2 Saran		133
DAFTAR PUSTAKA		134
A		
<b>B</b>		
ΠAA	RA DATA RA	
		A
<b>NYAVAU</b>		
	UNUN HATVERERST	
	AWWAYAYAUN	
	BRARAWIIAAY	



# DAFTAR TABEL

Tabel	Halaman
2.1 Daftar Parameter CARP	21
4.1 Pengalamat IP	49
6.1 Waktu advertisement CARP gateway master	
6.2 Waktu Peralihan Gateway Master-Backup 1	
6.3 Waktu advertisement CARP backup 1	104
6.4 Waktu Peralihan Gateway Backup1-Backup 2	105
6.5 Selisih Reply	126

# DAFTAR GAMBAR

Gamb	Gambar Hala		
2.1	Format Header IPv4	7	
2.2	Format Segmen TCP	12	
2.3	Format Datagram UDP	13	
2.4	Proses Enkapsulasi Data	14	
2.5	Proses Routing	15	
2.6	Topologi Bus	17	
2.7	Topologi Star		
2.8	Topologi Ring	19	
2.9	CARP	22	
2.10	NAT	31	
2.11	Format ICMP untuk Echo Request dan Echo Reply	35	
4.1	Diagram Jaringan Internal Network dan External Network	43	
4.2	Diagram Jaringan Gateway Redundancy dengan menggunal	kan	
	CARP, ifstated dan pfsync	44	
4.3	DFD Level 0 <i>Client</i> ke <i>Internet</i>	45	
4.4	DFD Level 1 Client Ke Internet	46	
4.5	Diagram Jaringan Rancangan Implementasi Sistem	48	
4.6	Diagram Jaringan Setelah Konfigurasi	53	
5.1	Local Area Connection di Control Panel	62	
5.2	Local Area Connection Status	62	

5.3	Local Area Connection Properties	63
5.4	Window Pengisian Nomor IP	64
6.1	Hasil Perintah nmap	74
6.2	Hasil Perintah arp	75
6.3	Hasil Perintah nmap 11.0.0.0/24	76
6.4	Hasil Perintah nmap 12.0.0.0/24	77
6.5	Hasil Perintah arp	78
6.6	Pengujian Gateway fail-over	79
6.7	Hasil tcpdump Paket Data pada Interface Network 10.0.0/24	
	Komputer pada Gateway Backup 1 pada Pengujian Sistem Gateway	
	Fail-over	83
6.8	Hasil tcpdump Paket Data pada Interface Network 11.0.0.0/24	
	Komputer pada Gateway Backup 1 pada Pengujian Sistem Gateway	
	Fail-over	88
6.9	Hasil tcpdump Paket Data pada Interface Network 15.0.0.0/24	
	Komputer pada Gateway Backup 1 pada Pengujian Sistem Gateway	
3	Fail-over	90
6.10	State yang terbentuk Selama Sesi Koneksi	91
6.11	Firefox Menampilkan Situs www. klikbca.com saat Gateway Master	ß
	Aktif	92
6.12	Firefox Menampilkan Situs www.klikbca.com Saat Gateway Master	
	Tidak Aktif	93
6.13	Download Tanpa Menggunakan Download Manager	93

	6.14	Kegagalan Download Tanpa Menggunakan Download Manager	
		Terjadi Saat Gateway Master Tidak Aktif	94
	6.15	Download Menggunakan Flash Get Download Manager	94
	6.16	Download Menggunakan Flash Get Download Manager Saat	
		Gateway Master Tidak Aktif	95
	6.17	Traceroute yahoo.com Dalam Kondisi Normal	95
	6.18	Traceroute yahoo.com Saat Gateway Master tidak aktif	96
	6.19	Yahoo Messenger Dalam Kondisi Aktif	96
	6.20	Yahoo Messenger Disconnect dan Mencoba Kembali Terkoneksi	97
	6.21	Pengujian Gateway Fail-over	99
	6.22	Hasil tcpdump Paket Data Pada Interface Network 10.0.0.0/24	
		Komputer Gateway Backup 2 pada Pengujian Sistem Gateway fail-	
		over	103
	6.23	Hasil tcpdump Paket Data Pada Interface Network 10.0.0.0/24	
Ì		Komputer Gateway Backup 2 pada Pengujian Sistem Gateway fail-	
		over wer wer wer wer wer wer wer wer wer w	108
	6.24	Hasil tcpdump Paket Data Pada Interface Network 15.0.0.0/24	
	5	Komputer Gateway Backup 2 pada Pengujian Sistem <i>Gateway fail</i> -	
		over	110
	6.25	State vang terbentuk Selama Sesi Koneksi	111
	0.25	State yang terbentuk Selama Sesi Koneksi	111
	0.20	Fileiox Menampikan Shus www. Kilkoca.com saat Gateway Backup	112
			113
	6.27	Firefox Menampilkan Situs www. klikbca.com saat Gateway Backup	R
		Tidak Aktif	113

6.28	Download Tanpa Menggunakan Download Manager	114
6.29	Kegagalan Download Tanpa Menggunakan Download Manager	
	Terjadi Saat Gateway Backup 1 Down	114
6.30	Download Menggunakan Flash Get Download Manager	115
6.31	Download Menggunakan Flash Get Download Manager Saat	
	Gateway Backup 1 tidak aktif	115
6.32	Traceroute yahoo.com Dalam Kondisi Normal	116
6.33	Traceroute yahoo.com Saat Gateway Backup 1 tidak aktif	116
6.34	Yahoo Messenger Dalam Kondisi Aktif	117
6.35	Yahoo Messenger Disconnect dan Mencoba Kembali Terkoneksi	118
6.36	Hasil tcpdump Paket Data Pada Interface Network 11.0.0.0/24	
	Komputer Gateway Backup 2 pada Pengujian Sistem ISP Fail-over	117
6.37	Hasil tcpdump Paket Data Pada Interface Network 11.0.0.0/24	
	Komputer Gateway Backup 2 pada Pengujian Sistem ISP fail-over	125
6.38	Firefox Menampilkan Situs www. klikbca.com saat ISP 1 Aktif	127
6.39	Firefox Menampilkan Situs www. klikbca.com saat ISP 1 Tidak	
	Aktif	128
6.40	Download Tanpa Menggunakan Download Manager	128
6.41	Kegagalan Download Tanpa Menggunakan Download Manager	ß
	Terjadi Saat ISP 1 <i>Down</i>	129
6.42	Download Menggunakan Flash Get Download Manager	129
6.43	Download Menggunakan Flash Get Download Manager Saat ISP 1	
	tidak aktif	130
6.44	Traceroute yahoo.com Dalam Kondisi Normal	130

6.45	Traceroute yahoo.com Saat ISP 1 tidak aktif	131
6.46	Yahoo Messenger Dalam Kondisi Aktif	131
6.47	Yahoo Messenger Disconnect dan Mencoba Kembali Terkoneksi	132

SHIVE RSITAS BRAWING

1

# BAB I PENDAHULUAN

#### 1.1. Latar Belakang

Reliabilitas suatu jaringan Internet merupakan hal yang mutlak dibutuhkan untuk menunjang fungsinya sebagai komponen sistem informasi [RAH-05]. Reliabilitas jaringan mengacu pada ketersediaan layanan koneksi *client* ke Internet dengan mengabaikan media penghubung seperti kabel, hub, NIC, serta kondisi jaringan diatas *router* ISP - secara keseluruhan dalam penyelenggaraan komunikasi pada saat terjadinya kegagalan suatu komponen atau beberapa komponen jaringan [MED-99]. Secara umum, reliabilitas dapat didefinisikan sebagai daya tahan suatu sistem terhadap kegagalan kerja [WIK-07a].

Ketersediaan layanan ISP dan ketersediaan *gateway* sebagai gerbang koneksi dapat menjadi faktor penentu reliabilitas suatu jaringan Internet. Kegagalan layanan suatu ISP selama ini ditanggulangi dengan menyediakan dua atau lebih layanan ISP sebagai *backup* koneksi jaringan Internet. Pada saat terjadi kegagalan layanan dari suatu ISP, peralihan koneksi ke ISP *backup* dilakukan secara manual oleh administrator jaringan. Hal tersebut dapat menimbulkan kegagalan koneksi yang berdampak pada reliabilitas jaringan Internet, bila peralihan tidak terjadi secara cepat, atau terjadi *human error*. Oleh karena itu, dibutuhkan suatu sistem peralihan koneksi otomatis yang mampu mendeteksi kegagalan koneksi serta mengalihkan koneksi ke ISP *backup*, atau bisa disebut *ISP failover*.

Reliabilitas jaringan Internet juga ditentukan pada ketersediaan *gateway* sebagai gerbang koneksi jaringan Internet. Kegagalan ketersediaan *gateway* dapat diatasi dengan teknik *gateway failover*. Pada sistem *gateway failover*, saat *gateway* master mengalami kegagalan fungsi maka ia akan di*backup* oleh *gateway backup* [OPE-08a].

VRRP (Virtual Router Redundancy Protocol) dan HSRP (Hot Standby Router Protocol) merupakan dua protokol yang dapat digunakan dalam teknik gateway failover [MCB-04]. Dua protokol tersebut merupakan produk yang memiliki paten dan berlisensi yang membutuhkan pembayaran untuk menggunakannya. OpenBSD mengembangkan CARP, sebagai protokol aternatif yang dapat digunakan secara bebas (free dan opensource).

Berdasarkan dari adanya penurunan reliabilitas jaringan Internet yang disebabkan oleh kegagalan layanan ISP dan ketidaktersediaan gateway, maka

diperlukan suatu rancangan *gateway redundancy* - yaitu suatu sistem yang memiliki *fitur gateway failover* dan *ISP failover* - yang akan dikembangkan dalam tugas akhir ini.

#### 1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka rumusan masalah yang dibahas adalah:

- Merancang sistem *gateway redundancy* yang mampu mendeteksi kegagalan *gateway* serta melakukan *fail-over redundancy* dengan beberapa *gateway* cadangan.
- Merancang sistem *gateway redundancy* yang mampu mendeteksi kegagalan koneksi ISP serta mengalihkan koneksi, sehingga reliabilitas jaringan dapat terjaga.

# 1.3. Batasan Masalah

Dalam perencanaan dan pembuatan skripsi ini perlu dilakukan pembatasan masalah. Pembatasan masalah yang diajukan dalam skripsi ini antara lain:

- Reliabilitas jaringan mengacu pada ketersediaan layanan koneksi client ke Internet, dengan mengabaikan media penghubung seperti kabel, hub, NIC, serta kondisi jaringan diatas router ISP.
- Pembahasan difokuskan pada perancangan topologi serta konfigurasi CARP, *ifstated*, *pfsync* dan *pf*.
- Rancangan sistem menggunakan 3 gateway dan 2 ISP.
- Pembahasan diterapkan pada jaringan dengan sistem operasi OpenBSD.

# 1.4. Tujuan

Tujuan pembuatan tugas akhir ini adalah merancang *gateway redundancy* dengan menggunakan CARP, *ifstated*, dan *pfsync* untuk mengatasi kegagalan koneksi Internet dalam meningkatan reliabilitas koneksi jaringan Internet.

# 1.5. Sistematika Penulisan

# BAB I Pendahuluan

Memuat latar belakang, rumusan masalah, ruang lingkup permasalahan, tujuan penulisan serta sistematika penulisan.

# **BAB II Tinjauan Pustaka**

Membahas kajian pustaka dan teori dasar mengenai Protokol TCP/IP, Topologi Jaringan Komputer, CARP, *ifstated* dan *pfsync*.

#### **BAB III Metodelogi Penulisan**

Membahas metodologi yang digunakan dalam penulisan yang terdiri dari studi literatur, perancangan dan pembuatan sistem, pengujian dan analisis, serta pengambilan kesimpulan dan saran.

# **BAB IV Perancangan Sistem**

Membahas perancangan sistem yang sesuai dengan teori yang ada.

# BAB V Implementasi Sistem

Membahas implementasi sistem yang telah dirancang.

# BAB VI Pengujian Sistem

Membahas pengujian dan analisis sistem yang telah diimplementasikan.

# BAB VII Kesimpulan dan Saran

Memuat kesimpulan yang diperoleh dari implementasi dan analisis sistem, serta saran-saran untuk pengembangan lebih lanjut.



#### **BAB II**

#### **TINJAUAN PUSTAKA**

#### 2.1. Gateway Redundancy

Ketersediaan layanan dan layanan bebas gangguan, merupakan jargon para profesional IT dan administrator jaringan dalam meyakinkan konsumen. Tujuan utama dari pembuatan *gateway redundancy* adalah memastikan jaringan bekerja secara optimal, walaupun *gateway* dan/atau layanan ISP terganggu, baik yang disebabkan oleh perawatan sistem maupun *error* sistem [JAV-01].

Dengan adanya pembuatan *gateway redundancy* diharapkan, jaringan dapat [KEE-02]:

- Bekerja seperti sediakala, tanpa adanya tambahan pengaturan dari sisi pengguna.
- Memiliki ketersediaan layanan yang tinggi, dengan downtime kecil.
- Sistem bekerja tanpa mengganggu koneksi yang berjalan.

#### a. Pengertian Gateway Redundancy

Gateway merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk menghubungkan suatu segmen jaringan dengan jaringan lainnya yang bukan merupakan ruang lingkupnya [TAN-03]. Segmen tersebut dapat merupakan sebuah workstation, server, router, local area network (LAN), protokol atau media [WIK-07b]. Redundancy adalah penggadaan dari komponen vital pada suatu sistem, yang bertujuan untuk meningkatkan reliabilitas suatu sistem, seringkali dalam kasus backup atau fail-over [WIK-08]. Gateway Redundancy dapat diartikan penggandaan sebuah gateway dengan satu atau lebih gateway lain, untuk menjalankan fungsi fail-over [RAM-08].

#### b. Komponen-Komponen Pembentuk Gateway Redundancy

Komponen-komponen pembentuk *gateway redundancy* meliputi protokol TCP/IP, perangkat keras serta perangkat lunak. Protokol TCP/IP merupakan aturan yang dibuat agar berbagai perangkat, dengan berbagai macam sistem operasi, dengan berbagai macam arsitektur, dapat saling berkomunikasi [TAN-03]. Perangkat keras dalam sistem ini meliputi komputer yang terhubung dengan topologi jaringan komputer secara fisik dan perangkat fisik *gateway*. Topologi jaringan secara fisik

terdiri dari topologi *bus*, *ring*, dan *star*. *Gateway* secara fisik dapat dibedakan dalam dua hal, yaitu *dedicated* dan komputer yang difungsikan sebagai *gateway*.

Perangkat lunak dalam gateway redundancy terdiri dari CARP, pfsync, ifstated serta pf. CARP adalah singkatan dari Common Address Redundancy Protocol. Fungsi utama dari CARP adalah beberapa host pada jaringan yang sama, untuk memiliki alamat IP yang sama. Host-host ini disebut grup redundancy. Dalam grup tersebut, sebuah host bertindak sebagai master dan sisanya bertindak sebagai backup. Saat master down dan gagal bekerja, backup melakukan alih tugas dan layanan bekerja seperti sedia kala [OPE-08a].

*Pfsync* adalah sebuah *tool* untuk memastikan *state firewall* tersinkronasi, jadi ketika *backup* mengambil alih peran master, tidak ada *state* koneksi yang hilang [MAC-08]. *Ifstated* digunakan untuk mendeteksi *down* atau tidaknya status layanan koneksi suatu ISP. Daemon *ifstated* berjalan dan merespon *state* jaringan, dimana hal ini dilakukan dengan cara memonitor *interface link state* atau melakukan serangkaian tes eksternal [RES-08]. *Pf* digunakan untuk mengkonfigurasi PC menjadi router PC agar dapat meneruskan koneksi dari satu jaringan ke jaringan lain.

#### 2.2. Transmission Control Protocol/Internet Protocol (TCP/IP)

Protokol TCP/IP adalah suatu kumpulan aturan/protokol, dimana berbagai macam jenis tipe komputer, dari berbagai macam vendor, menggunakan berbagai macam sistem operasi, dapat berkomunikasi satu sama lain.

#### a. Arsitektur Protokol TCP/IP

Protokol dalam *Network*, umumnya dikembangkan dalam bentuk *layer-layer* (lapisan), dimana setiap *layer* bertanggung jawab terhadap tugas yang berbeda. Kumpulan protokol seperti TCP/IP, adalah kombinasi dari protokol-protokol yang berbeda, pada *layer* yang berbeda pula. TCP/IP terdiri dari 4 *layer*, seperti terlihat pada tabel 2.1.

Application	Telnet, FTP, e-mail, etc.	
Transport	TCP, UDP	
Network	IP, ICMP, IGMP	
Link	Device driver dan Interface card	

 Tabel 2.1
 Empat Layer dari Protokol TCP/IP

 Sumber : [STE-01]

Masing-masing layer memiliki tanggung jawab yang berbeda.

- 1. Layer Link, juga sering disebut layer data-link atau juga layer network interface, termasuk didalamnya driver perangkat pada sistem operasi, menghubungkan network interface card pada suatu komputer dengan komputer lain. Protokol yang terdapat pada layer ini antara lain Ethernet, FDDI, ISDN, ATM. Jenis protokol membedakan ragam enkapsulasi, jenis media transmisi, jenis network interface card, topologi, dan lain sebagainya. Bertugas menerjemahkan sinyal-sinyal digital menjadi bilangan bit 1 dan 0, serta sebaliknya.
- 2. Layer *network*, juga sering disebut layer *Internet* menangani pergerakan paket di dalam jaringan. *Routing* paket-paket, menangani hal-hal yang berkaitan IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*), dan IGMP (*Internet Group Management Protocol*). Layer *network* berfungsi untuk memungkinkan *host* mengirimkan paket data ke jaringan dan memungkinkan paket-paket data itu berjalan sendiri-sendiri ke tujuannya (yang besar kemungkinan berada di jaringan lain). Paket-paket data ini mungkin tiba di tujuan dengan urutan yang berbeda dengan urutan saat dikirimkan. Dalam kasus seperti ini, layer-layer yang berada di atasnya bertugas untuk mengatur kembali, bila pengiriman terurut diinginkan.

#### **IP** (Internet Protocol)

IP yang akan dibahas pada skripsi ini adalah Internet Protocol versi 4 (IPv4). Protokol IP merupakan inti dari protokol TCP/IP. Seluruh data yang berasal dari protokol pada *layer* di atas IP diolah oleh protokol IP, dan dipancarkan sebagai paket IP agar sampai ke tujuan. IP memiliki sifat yang dikenal sebagai *unreliable, connectionless* dan *datagram delivery service.* 

Unreliable berarti bahwa protokol IP tidak menjamin bahwa paket yang dikirim pasti sampai ke tujuan. Protokol IP hanya memastikan ia akan melakukan usaha sebaik-baiknya (*best effort delivery service*) agar paket yang dikirim tersebut sampai ke tujuan. Jika di perjalanan paket tersebut mengalami hal-hal yang tidak diinginkan (misalnya: salah satu jalur putus, *router* mengalami kongesti, atau *host/network* tujuan sedang *down*), maka protokol IP hanya memberitahukan pengirim paket melalui protokol ICMP (*Internet Control Messege Protocol*), bahwa terjadi masalah dalam pengiriman paket IP ke tujuan.

Jika menginginkan kehandalan yang lebih baik, kehandalan itu harus disediakan oleh protokol yang berada di atas layer IP ini (yaitu TCP dan aplikasi pengguna).

*Connectionless* berarti dalam mengirim paket dari tempat asal ke tujuan, pihak pengirim dan penerima paket IP sama sekali tidak mengadakan perjanjian (*handshake*) terlebih dahulu.

Datagram delivery service berarti setiap paket data yang dikirim tanpa tergantung terhadap paket data yang lain. Akibatnya, jalur yang ditempuh oleh masing-masing paket data IP ke tujuannya bisa jadi berbeda satu dengan lainnya. Karena jalur yang ditempuh berbeda, kedatangan paket pun bisa jadi tidak berurutan.

Metode-metode diatas dipakai dalam pengiriman paket IP untuk menjamin agar paket IP tetap sampai di tujuan, walaupun salah satu jalur ke tujuan itu mengalami masalah.

+	Bits 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Version	Header length	Type of Service (now DiffServ and ECN)	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum
96	Source Address				
128	Destination Address				
160	Options				
160/ 192+	Data				

Gambar 2.1 Format Header IPv4 Sumber : [ISI-81b]

Seperti yang terlihat dalam Gambar 2.1, Setiap paket IPv4 membawa data yang terdiri dari :

- Version (4 bit), berisi versi dari protokol IP yang dipakai, yaitu versi 4.
- *Header Length* (4 bit), berisi panjang dari header paket IP ini dalam hitungan 32 *bit word*.
- *Type of Service* (8 bit), berisi kualitas *service* yang dapat mempengaruhi cara penanganan paket IP ini.
- *Total Length of Datagram* (16 bit), berisi panjang IP *datagram* total dalam ukuran byte.

• *Identification* (16 bit), berisi nomor urutan yang bersama-sama dengan alamat sumber, alamat tujuan dan protokol *user* digunakan untuk mengidentifikasi sebuah *datagram* secara khusus, sehingga nomor ini dikhususkan untuk alamat sumber *datagram*, alamat tujuan dan protokol *user* selama datagram tetap pada Internet.

- *Flag* (3 bit), hanya dua bit yang sudah ditetapkan. Bit *More* digunakan untuk proses fragmentasi dan *reassembly*. Bit *Don't Fragment* mencegah terjadinya proses fragmentasi. Bit ini digunakan apabila telah diketahui bahwa tujuannya tidak memiliki kemampuan untuk memasang kembali fragment-fragment. Bagaimanapun juga, bila bit ini diset datagram akan dibuang apabila melebihi ukuran maksimum jaringan akhir. Oleh karena itu, bila bit ini diset, disarankan untuk menggunakan *routing* sumber untuk menghindari jaringan dengan ukuran paket maksimum.
- *Fragment Offset* (13 bit), menunjukkan di bagian mana datagram asli *fragment* ini termasuk, diukur dalam unit-unit 64 bit. Secara tidak langsung hal ini menyatakan fragment-fragment harus berisi *field* data yang panjangnya merupakan kelipatan 64 bit.
- *Time to Live* (8 bit), berisi jumlah *router / hop* maksimal yang boleh dilewati paket IP. Setiap kali paket IP melewati satu *router*, isi dari *field* ini dikurangi satu. Jika TTL telah habis dan paket tetap belum sampai ke tujuan, paket ini akan dibuang dan *router* terakhir akan mengirimkan paket ICMP *time exceeded*. Hal ini dilakukan untuk mencegah paket IP terus menerus berada di dalam *network*.
- *Protocol* (8 bit), mengandung angka yang mengidentifikasikan protokol *layer* atas pengguna isi data dari paket IP ini.
- *Header Checksum* (16 bit), berisi nilai *checksum* yang dihitung dari seluruh *field* dari *header* paket IP. Sebelum dikirimkan, protokol IP terlebih dahulu menghitung *checksum* dari *header* paket IP tersebut untuk nantinya dihitung kembali di sisi penerima. Jika terjadi perbedaan, maka paket ini dianggap rusak dan dibuang.
- Alamat IP pengirim dan penerima data (masing-masing 32 bit), berisi alamat pengirim paket dan penerima paket.

- Beberapa byte option, diantaranya :
  - Strict Source Route, berisi daftar lengkap Alamat IP dari router yang harus dilalui oleh paket ini dalam perjalanannya ke host tujuan. Selain itu paket balasan atas paket ini, yang mengalir dari host tujuan ke host pengirim, diharuskan melalui router yang sama.
  - Loose Source Route, dengan mengeset option ini, paket yang dikirim diharuskan singgah di beberapa router seperti yang disebutkan dalam field option ini. Jika diantara kedua router yang disebutkan terdapat router lain, paket masih diperbolehkan melalui router tersebut.

# ICMP (Internet Control Message Protocol)

ICMP adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Pesan atau paket ICMP dikirim jika terjadi masalah pada *layer* IP dan *layer* atasnya (TCP/UDP).

Ada dua tipe pesan yang dapat dihasilkan oleh ICMP yaitu ICMP Error Message dan ICMP Query Message. ICMP Error Message, sesuai namanya, dihasilkan jika terjadi kesalahan pada jaringan. Sedangkan ICMP Query Message adalah jenis pesan yang dihasilkan oleh protokol ICMP jika pengirim paket menginginkan informasi tertentu yang berkaitan dengan kondisi jaringan. ICMP Error Message dibagi menjadi beberapa jenis, diantaranya :

- Destination Unreachable. Pesan ini dihasilkan oleh router jika pengiriman paket mengalami kegagalan akibat putusnya jalur, baik secara fisik maupun secara *logic*. Destination Unreachable dibagi menjadi beberapa tipe yang penting, yaitu:
  - > Network Unreachable, jika jaringan tujuan tak dapat dihubungi.
  - Host Unreachable, jika host tujuan tak bisa dihubungi.
  - Protocol at Destination is Unreachable, jika di tujuan tak tersedia protokol tersebut.
  - > Port is Unreachable, jika tidak ada port yang dimaksud pada tujuan.
  - > Destination Host is Unknown, jika host tujuan tidak diketahui.
  - > Destination Network is Unknown, jika network tujuan tidak diketahui.
- *Time Exceeded*. Paket ICMP jenis ini dikirimkan jika isi *field* TTL dalam paket IP sudah habis dan paket belum juga sampai ke tujuannya. Setiap kali

sebuah paket IP melewati satu *router*, nilai TTL dalam paket tersebut dikurangi satu. TTL ini diterapkan untuk mencegah timbulnya paket IP yang terus menerus berputar-putar di *network* karena suatu kesalahan tertentu, sehingga menghabiskan sumber daya jaringan yang ada.

*Field* TTL ini pula yang digunakan oleh program *traceroute* untuk melacak jalannya paket dari satu *host* ke *host* yang lain. Program *traceroute* dapat melakukan pelacakan rute berjalannya IP dengan cara mengirimkan paket kecil UDP ke IP tujuan, dengan TTL yang diset membesar.

Saat paket pertama dikirim, TTL diset satu sehingga *router* pertama akan membuang paket ini dan mengirimkan paket *ICMP time exceeded*. Kemudian paket ke-2 dikirim, dengan TTL dinaikkan. Dengan naiknya TTL, paket ini sukses melewati *router* pertama namun dibuang oleh *router* ke-2. *Router* ini pun mengirimkan paket *ICMP time exceeded*. Dengan mendaftar nama-nama *router* yang mengirimkan paket *ICMP time exceeded* ini, akhirnya didapat seluruh nama *router* yang dilewati oleh paket UDP.

- *Parameter Problem*. Paket ini dikirimkan jika terdapat kesalahan parameter pada *header* paket IP.
- Source Quench. Paket ICMP ini dikirimkan jika router atau tujuan mengalami kongesti. Sebagai respon atas paket ini, pihak pengirim paket harus memperlambat pengiriman paketnya.
- *Redirect*. Paket ini dikirimkan jika *router* merasa host mengirimkan paket IP melalui *router* yang salah. Paket ini seharusnya dikirimkan melalui *router* lain.

Sedangkan ICMP Query Message terdiri atas :

- Echo dan Echo Reply. Bertujuan untuk memeriksa apakah sistem tujuan dalam keadaan aktif. Program *ping* merupakan program pengirim paket ini. *Responder* harus mengembalikan data yang sama dengan data yang dikirimkan.
- *Timestamp* dan *Timestamp Reply*. Menghasilkan informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket.
- Address Mask. Untuk mengetahui berapa netmask yang harus digunakan oleh suatu host dalam suatu network.

Sebagai paket pengatur kelancaran jaringan, paket ICMP tidak diperbolehkan membebani *network*. Karenanya, paket ICMP tidak boleh dikirim saat terjadi problem yang disebabkan oleh :

- Kegagalan pengiriman paket ICMP.
- Kegagalan pengiriman paket broadcast atau multicast.

#### **ARP** (Address Resolution Protocol)

TCP/IP bekerja dengan menggunakan alamat IP sepanjang 32 bit. Sementara Network Interface Card memiliki format dan panjang pengalamat yang berbeda. Dalam skripsi ini digunakan Ethernet, dimana paket TCP/IP dikirim melalui ethernet card. Untuk berkomunikasi mengenali dan berkomunikasi dengan ethernet lainnya, digunakan ethernet address. Ethernet address ini besarnya 48 bit. Setiap ethernet card memiliki ethernet address yang berbeda-beda. Pada saat hendak mengirimkan data ke komputer dengan IP tertentu, suatu host pada jaringan ethernet perlu mengetahui, di atas ethernet address yang manakah tempat IP tersebut terletak. Untuk keperluan pemetaan Alamat IP sepanjang 32 bit dengan ethernet address sepanjang 48 bit ini, digunakan protocol ARP (Address Resolution Protocol). ARP bekerja dengan mengirimkan paket berisi Alamat IP yang ingin diketahui alamat ethernetnya ke alamat broadcast ethernet. Karena dikirim ke alamat broadcast, semua card ethernet akan mendengar paket ini. Host yang merasa memiliki Alamat IP ini akan membalas paket tersebut, dengan mengirimkan paket yang berisi pasangan Alamat IP dan ethernet address. Untuk menghindari seringnya permintaan jawaban seperti ini, jawaban disimpan di memori (ARP cache) untuk sementara waktu.

3. *Transport* layer, menangani aliran data antara 2 host, untuk layer aplikasi diatasnya. Pada protokol TCP/IP, terdapat dua protokol pada layer transport, yaitu: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

#### **TCP** (*Transmission Control Protocol*)

TCP merupakan protokol yang menyediakan layanan yang berkarakteristik sebagai berikut : *connection oriented, reliable,* dan *byte stream service. Connection oriented* berarti sebelum melakukan pertukaran data, dua aplikasi

pengguna TCP harus melakukan pembentukan hubungan (*handshake*) terlebih dahulu. *Reliable* (dapat diandalkan) berarti TCP menerapkan proses deteksi kesalahan paket data dan *re-transmission* (transmisi ulang). *Byte stream service* berarti paket data dikirimkan ke tujuan secara berurutan [PUR-01:55].

+	Bits 0 - 3	4 - 9	10 - 15	16 - 31
0	Source Port			Destination Port
32	Sequence Number			nce Number
64	Acknowledgement Number			
96	Data Offset	Reserved	Flags The IP Header	Window
128	Checksum			Urgent Pointer
160	Options (optional)			
160/ 192+	Data			

# Gambar 2.1 Format Segmen TCP Sumber : [ISI-81a:15]

Seperti yang ditunjukkan dalam Gambar 2.2, segmen TCP terdiri atas beberapa field. Source dan Destination Port adalah field berisi angka yang mengidentifikasi aplikasi pengirim dan penerima segmen TCP. Sequence Number berisi nomor urut byte stream dalam data aplikasi yang dikirim. Setiap penerima data mengisi kali data ini sukses dikirim, pihak field Acknowledgement Number dengan Sequence Number berikutnya yang diharapkan penerima. Data offset berisi 4-bit field yang menunjukkan ukuran header TCP dalam 32-bit words. Ukuran header minimum adalah 5 words dan maksimum 15 words, yang memberikan besar minimum 20 byte dan maksimum 60 byte. Reserved besarnya adalah 6-bit dan sebaiknya diisi dengan nol. Field ini digunakan untuk keperluan di masa depan. Flags the IP header berisi 6 bit flag, yaitu : URG yang menunjukkan Urgent Pointer field penting, ACK yang menunjukkan Acknowledgement field penting, PSH yang menunjukkan Push Function, RST untuk melakukan setting ulang koneksi, SYN yang menunjukkan Synchronize sequence numbers, dan FIN yang menunjukkan tidak ada data lagi dari pengirim. Field window diisi dengan panjang window (semacam buffer) penerimaan segmen TCP, merupakan banyak byte maksimal yang bisa diterima setiap saat. Lebar field ini adalah 16 bit (2 byte), sehingga nilai maksimalnya adalah 65535. Checksum berfungsi untuk memeriksa apakah terdapat kesalahan pada header dan data. Urgent Pointer berukuran 16-bit yang berfungsi mengimbangi sequence numbers yang menunjukkan byte terakhir dari urgent data, jika flag URG dipasang. Options merupakan field tambahan yang dapat diikuti dengan urgent data. Jika field ini ada, maka total lebar field ini harus kelipatan dari 32-bit words dan pengaturan field Data Offset akan menyesuaikan. Data bukan merupakan bagian dari header dan berisi apapun yang berasal dari layer diatasnya.

#### UDP (User Datagram Protocol)

UDP merupakan protokol *transport* yang sederhana. Berbeda dengan TCP yang *connection oriented*, UDP bersifat *connectionless*. Dalam UDP tidak ada *sequencing* (pengurutan kembali) dan *acknowledgement* terhadap paket data yang datang atau transmisi ulang jika paket mengalami masalah di tengah jalan. Kemiripan UDP dengan TCP ada pada penggunaan *port number*. Sebagaimana digunakan pada TCP, UDP menggunakan *port number* ini untuk membedakan pengiriman *datagram* ke beberapa aplikasi berbeda yang terletak pada komputer yang sama. Karena sifatnya yang *connectionless* dan *unreliable*, UDP umumnya dipakai untuk mengirim data yang memerlukan kecepatan tetapi kurang peka terhadap kesalahan, seperti mengirim suara dan video. UDP ini bersifat *broadcasting* atau *multicasting*. Pengiriman *datagram* ke banyak *client* sekaligus akan efisien jika prosesnya menggunakan metode *connectionless*.

+	Bits 0 - 15	16 - 31	
0	Source Port	Destination Port	
32	Length	Checksum	
64	Data		

Gambar 2.2 Format Datagram UDP Sumber : [POS-80:1]

Dalam Gambar 2.3, ditunjukkan format dari datagram UDP. Source Port dan Destination Port memiliki fungsi yang sama seperti pada TCP. Datagram Length berisi panjang datagram, sedangkan Checksum berisi angka hasil perhitungan matematis yang digunakan untuk memeriksa kesalahan data.

- 4. Layer *application* menangani detail dari aplikasi tertentu. Ada banyak aplikasi TCP/IP yang diaplikasikan dalam berbagai macam bentuk, antara lain :
  - a. FTP (File Transfer Protocol)

FTP merupakan salah satu aplikasi TCP/IP yang digunakan untuk memindahkan data dari komputer yang satu ke komputer yang lain secara efisien.

b. SMTP (Simple Mail Transport Protocol) atau E-Mail

SMTP memberikan cara yang mudah dan cepat dalam mengirim informasi. SMTP ini pada awalnya hanya merupakan salah satu jenis transfer file.

c. HTTP (Hypertext Transfer Protocol)

Protokol ini digunakan untuk jenis layanan *World Wide Web* atau layanan akses situs pada jaringan TCP/IP.

d. DNS (Domain Name Service)

Protokol ini digunakan untuk memetakan nama-nama host ke alamat-alamat jaringannya.

#### b. Enkapsulasi Data

Enkapsulasi adalah proses penambahan *header* dan *ending* pada data, atau pembungkusan data. *Header* menandakan awal data, dan seringkali berisi alamat dan hal-hal lain, bergantung pada protokol dan *layer*. *Ending* bit digunakan untuk pengecekan *error*. Proses ini ditunjukkan dalam Gambar 2.4



Gambar 2.4 Proses Enkapsulasi Data Sumber : [CAL-02]

Pada setiap lapisan yang dilalui ditambahkan sebuah *header* yang berisi informasi-informasi pengontrol komunikasi. Unit data yang akan diterima pada lapisan *transport* dibagi-bagi menjadi potongan data yang disebut segmen TCP atau *datagram* UDP untuk aplikasi yang menggunakan UDP sebagai protokol *transport*nya. Segmen tersebut diteruskan ke lapisan *network* dan disebut *datagram* IP. *Datagram* IP diteruskan pada lapisan *Data Link* untuk ditransmisikan melalui media fisik jaringan.

Jika suatu protokol menerima data dari protokol lain di *layer* atasnya, ia akan menambahkan informasi tambahan miliknya ke data tersebut. Informasi ini memiliki fungsi yang sesuai dengan fungsi protokol tersebut. Setelah itu, data ini diteruskan lagi ke protokol pada *layer* di bawahnya. Proses ini disebut *encapsulation*. Hal yang sebaliknya terjadi jika suatu protokol menerima data dari protokol lain yang berada pada *layer* di bawahnya. Jika data ini dianggap *valid*, protokol akan melepas informasi tambahan tersebut, untuk kemudian meneruskan data itu ke protokol lain yang berada pada *layer* di atasnya. Proses ini disebut *decapsulation*.

Setiap teknologi akses jaringan mempunyai ukuran maksimum *frame* data yang dapat ditransmisikan atau yang disebut dengan MTU (*Maximum Transmission Unit*). Bila ukuran datagram IP melebihi MTU maka IP memotong datagram menjadi fragment-fragment yang mempunyai ukuran yang tidak melebihi MTU jaringan. Proses pemotongan datagram menjadi *fragment* disebut fragmentasi [STE-01].

#### c. Routing

*Routing* berarti melewatkan paket IP ke *network* tujuan. Alat yang berfungsi melakukan *routing* paket ini disebut sebagai *router*. Agar mampu melewatkan paket data antar jaringan, maka *router* minimal harus memiliki dua buah *network interface*.

Proses *routing* dilakukan dengan *hop by hop* yang berarti paket data dilewatkan ke *router* terdekat hingga mencapai *network* tujuan. IP tidak mengetahui jalur keseluruhan menuju tujuan setiap paket. IP *routing* hanya menyediakan Alamat IP dari *router* berikutnya (*next hop router*) yang menurutnya "lebih dekat" ke *host* tujuan.



Gambar 2.5 Proses Routing Sumber : [ALM-01]

Paket data masuk ke dalam *router* melalui *input interface* kemudian *router* akan memproses (*forwarding*) sesuai dengan konfigurasi yang dimilikinya dan paket data yang telah diproses akan keluar melalui *output interface*. Proses *routing* teersebut, dijelaskan dalam Gambar 2.5.

Secara umum, *routing* dapat dibedakan menjadi dua, yaitu *static routing* dan *dynamic routing*.

#### Static Routing

Proses *routing* dengan metode *static routing* adalah dengan menuliskan jalurjalur *routing* secara manual pada *router*. Jalur-jalur yang dituliskan tersebut, adalah jalur-jalur yang bersifat tetap mengingat *static routing* diperuntukkan untuk suatu jaringan bertopologi tetap. Dalam menggunakan metode ini, tidak boleh terdapat satu kesalahan pun karena setiap kesalahan dalam penulisan *routing* berarti kegagalan suatu jaringan untuk menghubungi jaringan lain.

#### **Dynamic Routing**

Dynamic routing adalah suatu protokol pada router yang dapat secara otomatis mencari jalur-jalur routing ke suatu tujuan tertentu di dalam suatu jaringan. Jika topologi suatu jaringan berubah maka protokol ini akan secara otomatis merubah isi tabel routing dengan menyesuaikannya dengan topologi jaringan yang baru. Perubahan topologi jaringan ini dapat terjadi misalnya seperti adanya penambahan atau pengurangan router [MAL-02:5].

#### 2.3. Topologi Jaringan

Setiap standar *Local Area Network* (LAN) memiliki peraturan media transmisinya sendiri. Aturan ini mendefinisikan bagaimana menghubungkan media, perangkat keras yang dibutuhkan dan berbagai aturan pemasangan komponen. Dua hal utama berkaitan dengan media adalah tipe media (biasanya adalah tipe kabel) dan bagaimana berbagai kabel jaringan tersebut tersambung.

Hal penting yang harus dicatat bahwa terdapat perbedaan antara topologi jaringan secara fisik dan logika. Topologi fisik menjelaskan bagaimana media kabel dibentang, sedangkan topologi logika menjelaskan bagaimana perilaku jaringan. Token *ring* memiliki topologi *ring* karena data mengalir melalui setiap *station* sampai kembali ke *station* awal dimana data muncul, jadi data seperti melalui suatu *ring*.

Tetapi secara fisik, jaringan token ring memiliki topologi star karena dibentuk dari kabel yang menghubungkan setiap *station* ke *hub*.

Skema pengaturan kabel dalam LAN disebut topologi pengkabelan LAN. Topologi yang umum dalam LAN adalah Bus, Star dan Ring.

#### 2.3.1. Topologi Bus

Topologi Bus terdiri dan kabel yang menghubungkan semua station. Sinyal yang dikirim dan suatu station akan terdistribusi ke semua station lain. Jadi karakteristik Topologi Bus adalah berbagi media (shared media). Keuntungan dari hu. BRAWIJJ penggunaan topologi bus adalah:

- Hemat kabel 0
- Layout kabel sederhana 0
- Mudah dikembangkan

Kekurangan penggunaan Topologi Bus adalah:

- Sulit untuk medeteksi kerusakan, apabila terjadi kerusakan dalam jaringan o
- Lalu lintas padat o
- Seluruh jaringan akan tidak berfungsi, jika terjadi kerusakan pada kebel utama o
- Diperlukan repeater untuk jarak jauh o

Contoh Topologi Bus ditunjukkan dalam Gambar 2.6.

Gambar 2.6 Topologi Bus Sumber : [CON-05a]

#### 2.3.2. Topologi Star

Pada Topologi Star, setiap station terhubung melalui media kabel ke perangkat atau elemen saklar (switching element / hub) sentral, oleh karena itu komunikasi antara dua station harus melalui perangkat tersebut. Jadi karakteristik topologi ini adalah tidak berbagi media. Perangkat saklar sentral rnempunyai kemampuan

mengisolasi sinyal antar *port* sehingga kerusakan pada satu *port* tidak mempengaruhi *port* lainnya. Keuntungan lain adalah mudah dalam menghubungkan atau melepas hubungan *station* dan perangkat sentral. Contoh Topologi *Star* ditujukkan dalam Gambar 2.7.



Gambar 2.7 Topologi Star Sumber: [FLO-05]

# 2.3.3. Topologi Ring

Topologi Ring terbentuk dan kabel yang membentuk lingkaran tertutup (*loop*) dengan *station* yang terhubung ke kabel tersebut. Sinyal hanya dikirim dalam satu arah aliran. Jadi karakteristik Topologi Ring adalah berbagi media. Keuntungan penggunaan Topologi Ring adalah:

- o Mudah untuk mencari kerusakan dalam jaringan.
- Tidak terdapat *collision*.

Kekurangan dari penggunaan topologi ring adalah:

- Apabila satu komputer terganggu, komputer lainnya akan terganggu.
- Pengembangan jaringan lebih kaku

Contoh Topologi Ring ditujukkan dalam Gambar 2.8.


Gambar 2.8 Topologi Ring Sumber : [CON-05b]

# 2.4 CARP

CARP adalah singkatan dari *Common Address Redundancy Protocol*. Fungsi utama dari CARP adalah beberapa *host* pada jaringan yang sama, dapat memiliki alamat IP yang sama. *Host-host* ini disebut grup *redundancy*. Dalam grup tersebut sebuah *host* bertindak sebagai *master* dan sisanya bertindak sebagai *backup*. *Master* adalah *host* yang "memegang" alamat IP bersama tadi. *Master* merespon semua trafik ataupun ARP *request* yang ditujukan ke alamat IP tersebut. Tiap *host* bisa menjadi anggota dari grup *redundacy* lain pada suatu waktu. CARP merupakan protokol yang memiliki fungsi serupa dengan VRRP<sup>1</sup>, tetapi dengan desain yang berbeda. CARP dapat digunakan untuk membuat grup dari suatu *redundant firewall*. Alamat *virtual* yang digunakan pada grup *redundancy*, pada *client* digunakan sebagai *default gateway*. Saat *master firewall down* dan gagal bekerja, alamat IP bersama digunakan oleh *firewall backup* dan layanan *gateway* bekerja seperti sedia kala [OPE-08a].

CARP bekerja di antara *layer* 2 dan 3, yaitu diantara *link layer dan IP layer*. Setiap grup CARP memiliki sebuah alamat MAC *virtual (link layer)*, dan satu atau lebih alamat IP *virtual host. Host* dari CARP merespon ARP *request* dari sebuah alamat IP, dengan sebuah *virtual* alamat MAC, dan CARP melakukan *advertisement*, dengan alamat asal ini, hal ini membantu *switch* dalam menentukan *port* mana, yang memiliki *virtual* alamat MAC. Protokol *CARP* merespon request *ARP* dengan alamat MAC *virtual. Sintaks konfigurasi CARP menggunakan ifconfig yaitu :* 

• ifconfig carpN create

<sup>&</sup>lt;sup>1</sup> Virtual Router Redundancy Protocol (VRRP), adalah protokol redundancy *non-proprietary* yang dijelaskan pada RFC 3768, didesain untuk meningkatkan ketersedian default gateway pada sebuah network.

ifconfig carpN [advbase n] [advskew n] [balancing mode] \
 [carpdev iface] [pass passphrase] [state state] [vhid host-id]

# carpN

nama dari carp(4) virtual interface.

### advbase, advskew

nilai ini menentukan interval dari *advertisement* yang dilakukan CARP. *Interval* dalam satuan detik, *interval* dihitung dengan menggunakan formula (advbase + (advskew / 255)); memperbesar nilai advbase (nilai default awal = 1 detik) akan mengurangi kepadatan jaringan (*network traffic*), tetapi meningkatkan *delay* dalam pemilihan master baru. Nilai advskew yang kecil, membuat sebuah host melakukan *advertisement* lebih sering, menjadikan host tersebut memiliki kemungkinan lebih besar menjadi master. Nilai advbase berkisar antara 1 hingga 255, advskew antara 0 (default) sampai 254;

# balancing

mengaktifkan mode load balancing; mode yang dapat digunakan adalah arp, ip, ipstealth, and ip-unicast;

# carpdev

interface LAN card fisik, yang digunakan pada redundancy group tersebut. Defaultnya, CARP menggunakan interface fisik yang memiliki subnet yang sama dengan virtual interface;

# pass

password untuk autentifikasi digunakan untuk berkomunikasi dengan host CARP lain, pada group redundancy. Password harus sama pada setiap anggota;

# state

membuat carp(4) pada kondisi state sekarang (init, backup or master);

# vhid

ID Virtual Host. Ini adalah nomor unik (antara 1- 255) digunakan untuk mengidentifikasi redundancy group kepada perangkat lain dalam jaringan.

Master mengirimkan CARP pesan advertisement melalui multicast menggunakan protokol CARP (IP Protocol 112) pada kondisi normal, dan host backup "mendengarkan" advertisement ini. Jika advertisement berhenti, backup akan mulai melakukan advertisement. Frekuensi dari advertisement ini dapat diatur, dan host backup yang lebih sering melakukan advertisement, adalah host yang memiliki peluang lebih besar menjadi master, ketika terjadi kegagalan pada master [MAC-08]. Secara default, CARP aktif pada OpenBSD. Namun bisa ditambahkan beberapa perubahan parameter di file sysctl.conf, untuk fungsi tambahan.

Tabel 2.1 Daf	itar Parameter	CARP
---------------	----------------	------

Syntax	Keterangan
net.inet.carp.allow	Mengaktifkan CARP. Aktif secara
ALAS BRARAWILL	default.
net.inet.carp.preempt	Bila diaktifkan, salah satu interface
HT BL	fisik CARP down, advskew berubah
RSIT	menjadi 240, pada semua CARP interface. Tidak aktif secara default.
net.inet.carp.log	Mencatat packet CARP yang tidak
	normal. Tidak aktif secara default.

CARP menyediakan 2 mekanisme pembagian beban (*load balancing*), pada trafik yang masuk: ARP *balancing* dan IP *balancing*. Dimana penggunaannya bergantung pada kondisi CARP diimplementasikan. ARP *balancing* memiliki kemampuan yang terbatas untuk membagi beban trafik masuk diatara *host* pada jaringan ethernet. ARP *balancing* hanya bekerja pada klien di jaringan lokal, karena ARP *balancing* menyebar beban dengan berbagai macam *reply* ARP, berdasar Alamat MAC pengirim. ARP *balancing* tidak bisa bekerja pada jaringan yang berbeda (dua jaringan yang terhubung melalui *router*). IP *balancing* sebaliknya, tidak bergantung pada ARP, sehingga juga bekerja pada trafik yang melalui *router*. Metode ini bekerja pada berbagai kondisi jaringan, dan juga bisa memiliki performa yang lebih baik dibanding ARP *balancing* harus diterima oleh semua CARP *host*. Dimana hal ini terjadi pada kasus yang menggunakan hub, jika dihubungkan pada *swtich* kita memerlukan cara tertentu, dimana cara ini menyebabkan *load* jaringan yang lebih tinggi.



# Gambar 2.9 CARP Sumber : [OPE-08a]

Secara umum proses kerja CARP dan *pfsync*, dalam membentuk *redundancy* gateway adalah sebagai berikut. Pada saat kedua gateway dalam keadaan aktif, gateway master melakukan advertisement (pemberitahuan) melalui protocol CARP. Sedangkan pada gateway backup tidak melakukan advertisement. Ketika ada client traffic (paket data) melalui gateway master, maka akan terbentuk state (proses koneksi) dan secara langsung dikirim ke gateway backup melalui protokol pfsync. Pada kondisi gateway master tidak aktif dan client traffic sedang berlangsung, gateway backup melakukan advertisement. Ketika gateway backup tidak menerima tiga kali advertisement dari gateway master, yaitu sekitar tiga detik dengan konfigurasi standart. Konfigurasi standart yang dimaksud adalah advbase=1dan advskew=0 pada gateway master. Pada saat itu juga gateway backup menggantikan gateway master dan melajutkan client traffic yang sedang berlangsung, sesuai dengan state yang diterima pada saat gateway master dalam kondisi aktif. Pada kondisi gateway master

kembali aktif, maka *gateway master* merequest update pf state melalui protokol *pfsync* semua *state* yang berlangsung pada *gateway backup* sebelum protokol CARP mengambil alih fungsi *gateway master*.

### 2.5 Protokol pfsync

Protokol *pfsync* adalah protokol yang berfungsi sebagai sinkronisasi *state* (proses koneksi), yaitu dengan cara mentransfer *state* berupa perintah *insert*, *update*, dan *delete message* diantara *gateway*. Setiap *gateway* mengirim *message*, menggunakan *protocol pfsync* (IP *Protocol* 240), menggunakan *multicast*, dengan *multicast group 224.0.0.240*, pada suatu *interface* menggunakan protokol *pfsync*. *Gateway-gateway* tersebut juga, mendengar pesan yang sama dari *gateway* lain, kemudian meng*import message* ke dalam tabel *local st*ate [COU-06].

Saat ini *pfsync* tidak memiliki autentifikasi keamanan, sehingga *cracker* yang memiliki akses ke *link* internal, dapat memodifikasi *message state* tersebut. Disarankan menggunakan *pfsync* pada *network* tertutup, atau dapat ditambahkan *ipsec* [THR-01]. Saat digunakan dengan CARP, *pfync* dapat digunakan untuk memastikan interface CARP selalu sinkron. Saat digunakan dengan PF, *pfsync* digunakan untuk memeriksa ketersedian server atau koneksi, yang berpengaruh pada perubahan aturanaturan pada PF [RES-08].

# 2.6 Multicast

*Multicast* atau *multicasting* adalah sebuah teknik dimana sebuah data dikirimkan melalui jaringan ke sekumpulan komputer yang tergabung ke dalam sebuah grup tertentu, yang disebut sebagai *multicast group*. *Multicasting* merupakan sebuah cara pentransmisian data secara *connectionless* (komunikasi dapat terjadi tanpa adanya negosiasi pembuatan koneksi), dan klien dapat menerima transmisi *multicast* dengan mencari di mana lokasinya, seperti halnya ketika kita membuka sebuah stasiun radio untuk mendengarkan siaran radio. *Multicast* sebenarnya merupakan mekanisme komunikasi *one-to-many*, atau *point-to-multipoint* dan berbeda dengan cara transmisi *unicast*.

Sebuah *multicast group* memiliki sebuah alamat *multicast*, yaitu kelas D dalam alamat IP versi 4 atau memang alamat *multicast* dalam alamat IP versi 6. Pada kelas D alamat IP versi 4, alamat yang direservasikan untuk sebuah *multicast group* adalah 224.0.00 hingga 239.255.255.255. [TOO-01].

# 2.7 PF

PF adalah singkatan dari *packet filter*, merupakan *firewall* yang terintegrasi ke dalam sistem operasi OpenBSD, digunakan untuk memfilter TCP/IP *traffic* dan *network address translation (NAT)*. *PF* juga mampu sebagai *TCP/IP traffic normalizing* dan *conditioning* serta sebagai *bandwidth limiter* dan *traffic prioritization*. Ketika PF dikombinasikan dengan CARP dan *pfsync*, PF menjadikan *system* tidak hanya terlindungi layanannya dari serangan, tetapi membuat layanannya lebih *reliable*, yaitu dengan teknik *redundancy* [HAN-08].

# Aktifasi paket filtering – pf

- 1. Mengaktifkan pf, dengan mengedit file /etc/rc.conf.local dan mengisikan pf=YES, setelah itu ketik reboot, untuk merestart sistem.
- 2. Secara default file konfigurasi pf terletakkan di /etc/pf.conf, namun bisa dirubah bila dibutuhkan. Namun perubahan parameter juga diperlukan pada file /etc/rc.conf yaitu baris pf\_rules=/etc/pf.conf, jika terjadi perubahan lokasi file konfigurasi. File tersebut juga harus dimiliki oleh *root* dan group *wheel*, dan hanya root yang dapat mengaksesnya.
- 3. Untuk meng-*enable* pf ketikkan pfctl -e, dan ketikkan pfctl -d, untuk mendisable.
- 4. Setelah dilakukan perubahan ketikkan pfetl -F untuk *memflush* rule sebelumnya.
- 5. Kemudian ketikkan pfctl -f /etc/pf.conf untuk mereload rule yang tertulis pada /etc/pf.conf

# **Paket Filtering Rules**

Fungsi utama dari sebuah pf adalah paket filtering, disamping fungsi-fungsi lain. Ada dua perintah utama dalam paket filtering, block dan pass.

- Memblockir semua trafic keluar masuk. Rule ini seringkali merupakan pilihan terbaik dalam policy awal.
  - block in all
  - block out all
- o Melewatkan semua trafic keluar masuk
  - pass in all
  - pass out all
- o Melewatkan trafic ke dalam pada port 80

pass in quick on \$ext\_if \

# from any to \$int\_ad port 80

- Melewatkan hanya paket TCP 0 pass in quick on \$ext\_if proto tcp
- Memblokir trafic

bad\_boy\_ads = \

{10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, }

224.0.0.0/4, 240.0.0.0/5, 127.0.0.0/8, 0.0.0.0}

block in guick on \$ext\_if from \$bad\_boy\_\_ads to any

Memblokir paket dengan port lebih rendah dari 80 dan lebih tinggi dari TUS port 1024

block in on \$ext\_if proto tcp from any to \

**\$dmz\_www\_ad port 80 <> 1024** 

 Memblock semua koneksi dengan OS windows block in on \$int\_if proto tcp from any os " Windows 2000 "

pf.conf secara umum dibagi menjadi 7 bagian. Dan dapat dipilih sesuai kebutuhan.

- Macros : Mirip dengan global variabel, bisa berisi Alamat IP, nama *interface* (LAN *card*), dll
- Tables : Struktur yang digunakan untuk meletakkan Alamat IP
- Options : Berbagai pilihan yang digunakan untuk mengontrol kinerja pf
- Scrub : Memproses ulang paket untuk normalisasi dan defragmentasi
- Queueing : Menyediakan pengaturan bandwidth dan prioritas paket
- Translation : Pengaturan NAT dan redireksi paket
- Filter rules : Rule utama yang memilah paket antara satu dengan yang lainnya.

# Macro

Ruleset dari pf dapat berubah menjadi komplek dan rumit untuk dianalisis. Dalam pemrograman dikenal penggunaan variabel untuk sesuatu yang merupakan tetapan. Macro bisa berisi nama network interface, alamat,

protocol, port, dan informasi-informasi lain yang sering digunakan berulang. Macro harus diawali dengan huruf a-z A-Z, dan mengandung angka 0-9 atau underscores (\_). Nilai dari macro diapit dengan tanda petik 2 (""), dan digunakan menggunakan tanda (\$)

# macro definitions

# ext\_if -- the name of the firewall's external interface

ext\_if = "ne1"

ext\_ad = "172.17.100.5" # dmz\_ad -- the DMZ network address dmz\_ad = "192.168.255.1/24" # gabungan beberapa alamat friends = "{ 192.168.1.1, 10.0.2.5, 192.168.43.53 }"

#gabungan macro secara recursive host1 = ''192.168.1.1'' host2 = ''192.168.1.2'' all\_hosts = ''{'' \$host1 \$host2 ''}''

# protoc -- rdr-ed protocols
protoc = ''{tcp, udp, icmp}''

# ketika digunakan menggunakan \$
rdr on \$ext\_if proto \$protoc from any to \$ext\_ad port 80 \
-> \$dmz\_ad port 8080

# Table

Table adalah kumpulan dari Alamat IP. Yang membedakan table dengan macro adalah table hanya digunakan untuk Alamat IP. Setiap definisi table diawali dengan kata table dan diikuti nama table, table option (opsional), dan alamat

table <DMZ> persist {172.17.23.0/24}

table <myLANs> persist {10.100.100.0/24, 10.100.101.0/26 } #menggunakan ! berarti not #berarti goodguys adalah Alamat IP 192.0.2.0 – 192.0.2.255 kecuali 192.0.2.5 table <goodguys> { 192.0.2.0/24, !192.0.2.5 }

#penggunaan-nya

block in on fxp0 from any to <myLANs> port 25 pass in on \$ext\_if from any to {<DMZ>, <myLANs>} port 25

Mendefinisikan table kosong :

### table <spammers> persist

Table kosong digunakan untuk mengisi nilai secara ekternal. Table bisa di load, di remove, dan di modifikasi dengan pfctl(8) ketika pf berjalan, tanpa perlu me-reload seluruh ruleset dan tanpa memflush ruleset.

RAM

Table memiliki 2 options

- const setelah table dibuat, table tidak bisa diubah ataupun dihapus kecuali dalam mode single-user. Biasa digunakan dalam aspek sekuritas.
- Persist table tidak akan dihapus walaupun tidak berisi. Hal ini mencegah penghapusan otomatis

Table dan macro dalam beberapa hal, dapat memiliki fungsi yang sama, tapi table di proses lebih cepat. Table juga dapat meload nilainya dari file lainnya. table <myLANs> persist file ''/etc/spammers'' \

file ''/etc/openrelays'' \

file ''/root/scanners'' \

file "/root/idiots"

Secara umum syntax yang digunakan pada rules adalah :

aksi [arah] [log] [quick] [on interface] [af] [proto protokol] \

[from src\_addr [port src\_port]] [to dst\_addr [port dst\_port]] \ [flags tcp\_flags] [state]

aksi

Adalah tindakan yang dilakukan pada paket yang sesuai. Pass dan block. Pass berarti membolehkan koneksi paket. Sementara block berarti menolak paket yang datang

# arah (in out) dan interface (on)

Kata kunci arah, berhubungan dengan paket inbound dan outbound.

block in all

block out all

tetapi **tidak dapat** menggabungkannya menjadi **block {in, out} all** bisa digabungkan dengan interface, yaitu dengan menambahkan kata on **block in on rl0 all** 

# log

Adalah melakukan pencatatan melaui pflogd(8), Untuk mencatat semua paket gunakan log (all)

# quick

Dalam pf, setiap paket dievaluasi terhadap ruleset dari atas ke bawah. Rule memiliki aturan "the last matching rule win". Namun terdapat pengecualian terhadap aturan tersebut, opsi "quick" memiliki efek membatalkan rule lain di bawahnya, yang berlawan dengannya.

block in quick on fxp0 proto tcp from any to any port ssh pass in all

# af

spesifikasi antara IPV4 dan IPV6

# protokol

Terkadang dibutuhkan pengaturan terhadap protokol tertentu. Digunakan kata kunci proto diikuti nama protokol. Daftar dari nama protokol dan nomornya dapat terdapat di /etc/protocols, antara lain tcp, udp, icmp, icmp6.

# BRAWIJAYA

# block in on fxp0 proto {udp, tcp} all

# alamat

Salah satu bagian dari pf adalah alamat. Beberapa syntax yang umum digunakan antara lain

#paket dengan source address 10.0.1.3/24 dan

#destination address 192.168.23.4/18

... from 10.0.1.3/24 to 192.168.23.4/18 ...

#paket berasal dari source address manapun dan destination BAWIUAL #address 192.168.23.4/18 ... from any to 192.168.23.4/18

# paket berasal dari source address 10.0.1.3/24 dan #destination address manapun ... from 10.0.1.3/24 to any ...

# paket berasal dari source dan destination **#address manapun** ... from any to any ...

#contoh terakhir bisa ditulis menjadi: ... all ... 11.

#menggunakan .. from !10.0.1.3 to any ...

# port

Pada pengiriman sebuah paket, selain Alamat IP, port memiliki peran yang penting, karena port yang membedakan antara satu layanan dengan layanan lainnya. daftar jenis port terdapat di /etc/services. Kata kunci yang digunakan adalah port, dan pastikan juga tertulis protokol yang digunakan.

... proto tcp from any to 192.168.12.63/32 port \ {25, 80} ...

operator matematika seperti = (sama dengan), != (bukan sama dengan), < (lebih kecil), <= (lebih kecil sama dengan), > (lebih besar), >= (lebih besar sama dengan), >< (range/antara), <> (inverse range), : (inclusive range/sampai) juga dapat digunakan.

# tcp\_flags

flags tertentu yang digunakan pada proto tcp

# state

suatu kondisi dalam memperlakukan paket keep state : bekerja pada TCP, UDP, ICMP. modulate state : bekerja pada TCP.

Synproxy state : melakukan perlindungan terhadap server dari spoofing TCP SYN floods

BRAM

# **Keeping state**

Salah satu kelebihan paket filter adalah "keeping state" atau "statefull inspection", statefull inspection adalah kemampuan PF untuk melacak keadaan, atau proses, dari sebuah koneksi network. Dengan menyimpan informasi tentang setiap koneksi pada table state, PF dengan cepat menentukan, ketika sebuah paket melewati firewall apakah merupakan bagian dari koneksi yang telah ada. Jika benar, maka paket tidak perlu melewati "pemeriksaan" ulang.

Keeping state memiliki kelebihan dalam kesederhanaan ruleset, dan perfoma paket filtering. Keeping state juga bekerja pada paket balasan yang datang dari arah berlawan. Desain *firewall* yang digunakan adalah tugas akhir ini adalah NAT. NAT awalnya dikembangkan karena semakin terbatasnya alamat IP yang dapat terkoneksi ke Internet. Untuk memecahkan hal ini, para pakar mendesain *ip next generation*, disebut IPV6. Namun solusi tersebut butuh waktu proses dalam implementasinya. Sementara IPV4, dengan *Network Address* Translation (NAT), memiliki solusi yang juga dapat meningkatkan aspek sekuritas, yaitu.



NAT dapat digunakan untuk menyembunyikan Alamat IP sesungguhnya dari Alamat IP yang terkoneksi, juga untuk meredirect paket ke suatu Alamat IP/port. Walaupun NAT sering diasosiasikan dengan firewall, sebenarnya NAT merupakan mekanisme tersendiri. Teknik ini juga dikenal sebagai masquerading. NAT juga menyembunyikan detail dari internal network client, jumlah host internal dan informasi lain yang sering kali berguna bagi intruder. Host dengan alamat IP private dibalik NAT, tidak dapat dijangkau dari luar, karena hanya terlihat sebuah Alamat IP (c.c.c.c). Yang sesungguhnya terjadi adalah firewall merubah alamat pengirim (d.d.d.2) pada frame paket, menjadi alamat dirinya (c.c.c.c), menyimpan pengirim paket tersebut. Ketika ada balasan untuk paket tersebut, firewall melihat catatan tadi, dan mengganti alamat tujuan (c.c.c.c) paket menjadi alamat (d.d.d.2) pengirim paket tadi.

Ada tiga macam rule NAT

nat – translasi antara beberapa Alamat IP internal dengan sebuah Alamat IP external.

- 2. Rdr meredirect Alamat IP dan port.
- 3. Binat translasi dua arah antara satu Alamat IP external dan satu Alamat IP internal.

Tidak seperti pada packet filtering, rule di packet redirection memiliki aturan algoritma "first matching rule wins", yang berarti rule-rule specific harus diletakkan sebelum rule-rule umum.

 Mengkoneksikan network private ke internet ext\_if = "ne1"

nat\_proto = "{tcp, udp, icmp}"

 $ext_ad = "e.e.e.e/32"$ 

 $prv_ad = "p.p.p.p/24"$ 

nat on \$ext\_if proto \$nat\_proto \

```
from $prv_ad to any -> $ext_ad
```

 Ketika kita memiliki 2 network private (dengan NAT), maka antara network tersebut tidak dapat berkomunikasi, perlu ditambahkan rule "no"

BRAWIJA

no nat on \$ext\_if inet proto \$nat\_proto \ from \$prv1\_ad to \$prv2\_ad no nat on \$ext\_if inet proto \$nat\_proto \

from \$prv2\_ad to \$prv1\_ad

nat on \$ext\_if inet proto \$nat\_proto \

from {\$prv1\_ad, \$prv2\_ad} to any -> \$ext\_ad

• meredirect koneksi port 80 di Alamat IP external, ke port 8080 di Alamat IP internal

ext\_ad = ''e.e.e.e/32''

www\_ad = ''w.w.w.w/32''

rdr on \$ext\_if inet proto tcp \

from any to \$ext\_ad port 80 -> \$www\_ad port 8080

rdr on \$prv\_if inet proto tcp \

from \$prv\_ad to \$ext\_ad port 80 -> \$www\_ad port 8080

• Bidirectional nat dari sebuah Alamat IP internal ke sebuah Alamat IP external

binat on \$ext\_if inet proto tcp from 192.168.1.37 to any \

-> \$ext\_ad\_1 binat on \$ext\_if inet proto tcp from 192.168.1.38 to any \ -> \$ext\_ad\_2 binat on \$ext\_if inet proto tcp from 192.168.1.54 to any \ -> \$ext\_ad\_3

# 2.8 Ifstated

*Ifstated* digunakan untuk mendeteksi *down* atau tidaknya status layanan koneksi suatu ISP. Daemon *ifstated* berjalan dan merespon state jaringan, dimana hal ini dilakukan dengan cara memonitor *interface link state* atau melakukan serangkaian tes eksternal. *Option-option* yang terdapat pada *ifstated* antara lain:

# -D macro=value

Mendefinisikan macaro secara instan. Hal ini akan mengabaikan *macro* yang terdapat pada file konfigurasi.

-d Tidak menjalankan sebagai daemon dan log ke stdout.

### -f file

Mengatur lokasi file konfigurasi

- -h Menampilakan pesan bantuan
- -i Mengabaikan initial interface states.
- -n Konfigurasi mode tes.
- -v Verbose mode. Menampilkan output, dapat digunakan –vv untuk meningkatkan detil

Ifstated memiliki file konfigurasi secara *default* di /etc/ifstated.conf. ifstated.conf adalah file konfigurasi yang memiliki tiga bagian

# **Global Configuration**

Setting global untuk ifstated.

### Macros

Tempat user mendifinisikan *variable*, yang akan digunakan dalam program, memudahkan kofigurasi. Nama dari *macro*, bukan kata-kata *reserved*, seperti *state* atau *run. Macro* juga sering digunakan untuku mendefinisikan *state link interface*, antara lain :

Up	Link secara fisik up (enable). Pada CARP hal ini berarti
	master.
Down	Link secara fisik down (disable). Pada CARP hal ini berarti
	backup.

**Unknown** Link secara fisik tidak diketahui. Hal ini disebabkan drive interface tidak dapat menampilkan informasi. Pada CARP hal ini berarti init state.

Untuk dapat menampilkan status ini, external test harus dilakukan secara berkala. Frekuesi *eksternal test* dapat di*setting* dengan kata kunci "*every*".

Sebagai contoh:

carp\_up = "carp0.link.up && carp1.link.up"

net = '( "ping -q -c 1 -w 1 192.168.0.1 > /dev/null" every 10 &&  $\$ 

"ping -q -c 1 -w 1 192.168.0.2 > /dev/null" every 10 )'

# **State Definitions**

Berfungsi mirip prosedur kondisional dalam bahasa pemrograman, di dalamnya berisi script. Tetapi hanya di jalankan bila suatu kondisi state terpenuhi. Didalamnya bisa juga dimasukkan perintah untuk menjalankan perintah shell, menggunakan "run". Dapat juga menggunakan pemicu state lain, dengan kata kunci "set-state katakunci".

Sebagai contoh :

state one {

init {

run "ifconfig carp0 advskew 10" run "ifconfig carp1 advskew 10"

# if ! \$net

set-state two

```
if ! $carp_up {
```

run "ifconfig carp0 advskew 254" run "ifconfig carp1 advskew 254" set-state three 1

# 2.9 Ping

Nama ping berasal peralatan sonar yang digunakan untuk mengetahui lokasi suatu benda. Ping dibuat oleh Mike Muuss, dengan tujuan untuk mengetahui apakah suatu host bisa dijangkau atau tidak. Program mengirimkan sebuah pesan ICMP ECHO\_REQUEST menuju ke suatu host ataupun gateway. Bila host tersebut menerima pesan tersebut, maka host tersebut akan mengirimkan balasan berupa ICMP ECHO\_REPLY. Pada umumnya, jika host tujuan tidak mengirimkan ICMP ECHO\_REPLY, atau dengan kata lain tidak berhasil "diping", kita tidak bisa melakukan hubungan koneksi lain seperti Telnet ataupun SSH. Ping seringkali digunakan sebagai analisis awal status koneksi suatu jaringan. Ping juga menampilkan "seberapa jauh" host tersebut.

+	0-7	8-15	16-32	
0	Type (0 atau 8)	Code 0	Checksum	
8 Identifier			Sequence number	
	Optional data			

# 2.10 HTTP (Hyper Text Transfer Protocol)

Protocol HTTP adalah suatu cara untuk melakukan pertukaran dan penyampaian data melalui *world wide web*. Fungsi asli dari protocol ini adalah untuk mempublikasikan dan mendapatkan suatu halaman HTML (*Hyper Text Markup Language*) (*Anonymous*, 2006) [INT-99].

Pengembangan protokol HTTP dikoordinasi oleh *World Wide Web Consortium* dan *Internet Engneering Task Force* yang akan merumuskan suatu RFC (*Request for Comments*) yang digunakan sebagai standar dunia.

HTTP adalah suatu protokol yang berada diantara *client* dan *server*. *Client*, yang biasanya berupa *web browser* disebut sebagai *user agent*. Sedangkan *server* yang dituju, yaitu pihak yang menyediakan *web content* seperti halaman html atau gambar gambar disebut sebagai *origin server*. Diantara *user agent* dan *origin server* mungkin terdapat beberapa perantara, misalnya *proxy* atau *gateway*.

Sebuah *client* HTTP mengajukan suatu permintaan (*request*) atas *web content* dengan cara membuat suatu koneksi TCP dengan suatu *port* (biasanya *random port* diatas 1024) pada sebuah *remote host*. Sedangkan sebuah *server* HTTP akan mendengarkan

(listening) port 80 dan menunggu apakah ada suatu permintaan web content dari client. Setelah menerima suatu permintaan dari client, server akan membalas dengan mengirimkan suatu informasi status seperti "HTTP/1.1 200 OK" dan informasi lain sesuai yang dimiliki server tersebut, misalnya halaman yang diminta oleh client, pesan error, atau pesan-pesan yang lainnya.

Untuk mendapat akses ke suatu web content yang menggunakan protokol HTTP, maka digunakan suatu *url* tertentu, yaitu http:

# **Pesan Request**

Pesan request berisi hal-hal berikut :

Request Line, misalnya GET /images/naruto\_logo.gif HTTP/1.1, yang merupakan suatu permintaan file naruto\_logo.gif dari direktori /images.

Headers, misalnya Accept-Language: id

Sebuah baris kosong

Sebuah optional messege body

Sebuah baris request dan headers, semua harus berakhiran dengan CRLF (Carriage Return yang diikuti dengan Line Feed). Baris kosong harus mengandung CRLF saja dan tidak mengandung whitespace lain. Beberapa headers hanyalah pilihan, sedangkan yang lain bisa saja harus karena dibutuhkan oleh protokol HTTP/1.1.

# Metode Request

Protokol HTTP memiliki delapan metode yang menunjukkan hal yang ingin dilakukan pada resources yang diketahui. Metode-metode tersebut adalah :

HEAD berfungsi untuk meminta response identical yang cocok dengan GET request, akan tetapi tanpa response body.

GET berfungsi untuk meminta "perwakilan" dari resource tertentu.

*POST* berfungsi untuk memasukkan data yang akan diproses (misalnya formulir html) ke dalam resource yang diketahui.

PUT berfungsi untuk melakukan upload "perwakilan" dari resource tertentu.

DELETE berfungsi menghapus resource tertentu.

TRACE berfungsi untuk mengirim pesan konfirmasi bahwa sebuah permintaan telah diterima sehingga client dapat melihat apa yang telah ditambahkan atau diubah oleh intermediate servers.

OPTIONS berfungsi untuk mengetahui metode-metode HTTP yang didukung oleh server sehingga dapat digunakan untuk memeriksa fungsionalitas web server.

CONNECT berfungsi untuk mengubah ke SSL (Secure Socket Layer) tunnel jika digunakan dengan proxy.

HTTP server dibuat dengan minimal memiliki setidaknya metode *GET* dan *HEAD* dan jika memungkinkan, juga terdapat metode *OPTIONS*.

# Secure HTTP

Saat ini terdapat dua metode untuk membangun suatu koneksi HTTP *secure*, yaitu skema https URI dan header HTTP 1.1 *Upgrade*. Metode yang paling umum digunakan diantara kedua metode tersebut adalah skema https URI, sedangkan penggunaan header HTTP 1.1 *Upgrade* hampir tidak pernah digunakan.

# 2.11 Wireshark

Wireshark adalah sebuah aplikasi GPL OpenSoure yang berfungsi sebagai *packet analyzer* jaringan. Wireshark bekerja dengan "menangkap dan mendengar" network packets dan menampilkan packet data sedetail mungkin. Wireshark bekerja seperti sebuah alat pengukur yang mengukur semua hal yang terjadi di dalam jaringan, seperti halnya voltmeter yang digunakan untuk mengetahui apa yang terjadi dalam kabel listrik [LAM-08].



# BAB III

# METODOLOGI PENELITIAN

Langkah-langkah yang dilakukan untuk merancang sistem gateway redundancy hingga dapat berfungsi sebagaimana yang diharapkan meliputi hal-hal sebagai berikut:

# 3.1. Studi Literatur

Studi literatur yang dilakukan bertujuan untuk mengkaji hal-hal yang berhubungan dengan teori-teori yang mendukung dalam perencanaan dan perancangan sistem, yaitu :

- 1. Kajian pustaka mengenai Protokol TCP/IP, yaitu suatu protokol yang digunakan oleh suatu komputer dalam suatu jaringan komputer agar dapat saling berkomunikasi dengan komputer lain.
- 2. Kajian pustaka mengenai Topologi Jaringan Komputer, yaitu suatu cara untuk menyusun komputer-komputer secara fisik hingga membentuk sebuah jaringan komputer
- 3. Kajian pustaka mengenai CARP, yaitu protokol *gateway failover* yang menyediakan fungsi agar sebuah host dapat menggunakan secara bersama sebuah/beberapa *Alamat IP* ke beberapa *host*.
- 4. Kajian pustaka mengenai *pfsync*, yaitu suatu program yang berfungsi sebagai sinkronisasi *state* antara gateway-gateway.
- 5. Kajian pustaka mengenai *ifstated*, yaitu suatu program yang digunakan untuk mengetahui status koneksi dari ISP.
- 6. Kajian pustaka mengenai *pf*, yaitu program yang digunakan untuk mengkonfigurasi PC menjadi *router* PC serta melakukan NAT, agar dapat meneruskan koneksi dari *client* menuju Internet.

# 3.2. Perancangan dan Implementasi Sistem

Pada tahap ini, sistem untuk *Gateway Redundancy* Menggunakan CARP, *ifstated* dan *pfsync* dirancang sebagaimana berikut :

- 1. Perancangan topologi jaringan komputer
- 2. Pemasangan (*install*) sistem operasi pada setiap komputer di jaringan komputer.

3. Pengkonfigurasian CARP, *pfsync, ifstated, pf* pada komputer *gateway* sehingga dapat bekerja sesuai dengan yang diharapkan.

# 3.3. Pengujian dan Analisis Sistem

Pada tahap pengujian dan analisis sistem ini, sistem yang telah dibangun diuji apakah sistem yang telah dibuat benar – benar dapat bekerja dalam sistem sesuai tujuan. Dalam pengujian ini akan diperoleh sekumpulan data yang berisi informasi tentang dapat atau tidaknya sistem bekerja beserta kelemahan-kelemahannya.

Hasil dari pengujian yang berisi informasi kelemahan – kelemahan sistem akan dicantumkan, sehingga dapat digunakan untuk pembenahan pada tahap selanjutnya.

Setelah jaringan dan *gateway* telah terkonfigurasi maka akan dilakukan serangkaian pengujian sistem. Hasil dari pengujian tersebut akan dianalisis, apakah sistem yang dibangun telah memenuhi harapan atau belum, antara lain :

- 1. Pengujian konektivitas dibuat untuk menghubungkan antar *network*, sehingga untuk mengujinya dibutuhkan komunikasi antar jaringan lokal dengan jaringan eksternal.
- 2. Pengujian protokol *CARP* digunakan untuk melihat apakah protokol *CARP* telah aktif dan dapat digunakan.
- 3. Pengujian protokol *pfsync* digunakan untuk mengetahui apakah *pfync* mengirimkan atau mengexport *state* di antara ketiga *pc gateway*.
- Pengujian *ifstated* digunakan untuk melihat apakah *ifstated* dapat mendeteksi putusnya koneksi ke ISP dan dapat melakukan tindakan penanganan.

Setelah sistem telah berjalan dengan baik, maka selanjutnya akan diuji kestabilan koneksi serta perbedaan *delay* antara berbagai jalur koneksi (*gateway master* – isp utama, *gateway master* – isp kedua, *gateway backup* pertama – isp utama, *gateway backup* pertama – isp kedua, *gateway backup* kedua – isp utama, *gateway backup* kedua – isp kedua) dengan kondisi awal semua komputer *gateway* dalam keadaan *up*, dan dilanjutkan kondisi *master* dalam keadaan *down* dengan dua cara yaitu :

- 1. Soft off atau dimatikan secara software. Dilakukan dengan cara menggunakan perintah halt, maka pc gateway master akan shutdown.
- Hard off atau dimatikan secara hardware. Dilakukan dengan cara menshutdown pc gateway secara hardware, yaitu memutus aliran listrik ke pc gateway, dapat digunakan tombol power ataupun yang lain.

Dilanjutkan kondisi backup pertama dan backup kedua dalam keadaan down secara berturut-turut. Pengujian dengan mematikan komputer juga dilakukan pada setiap komputer ISP untuk mensimulasikan putusnya koneksi ke salah satu ISP.

# 3.4. Pengambilan Kesimpulan dan Saran

Tahap ini adalah tahap pengambilan kesimpulan dari sistem yang telah dibuat. Pengambilan kesimpulan dilakukan setelah semua tahapan perancangan dan pengujian sistem telah selesai dilakukan dan didasarkan pada kesesuaian antara teori dan praktek. Kesimpulan ini merupakan informasi akhir dari perancangan sistem yang berisi mengenai berhasil atau tidaknya sistem tersebut dijalankan.

Tahap terakhir dari penulisan adalah saran yang dimaksudkan untuk memperbaiki kesalahan-kesalahan yang terjadi serta menyempurnakan penulisan.



# **BAB IV**

# PERANCANGAN SISTEM

Perancangan *gateway redundancy* dengan menggunakan CARP *ifstated* dan *pfsync* ini dibagi menjadi dua tahap utama, yaitu perancangan perangkat keras dan perancangan perangkat lunak. Perancangan perangkat keras meliputi perancangan topologi jaringan komputer. Perancangan perangkat lunak meliputi perancangan jaringan komputer secara *logical*, perancangan *gateway failover* menggunakan CARP, perancangan *ifstated* untuk mendeteksi koneksi ke ISP, perancangan *pfsync* untuk sinkronasi data antara 3 gateway serta perancangan aturan-aturan *firewall* menggunakan *pf* untuk mengkonfigurasi NAT dan aturan-aturan lain yang mendukung.

# 4.1. Analisis kebutuhan

Analisis kebutuhan dalam perancangan gateway redundancy dengan menggunakan CARP *ifstated* dan *pfsync* terdiri dari spesifikasi sistem dan Analisis Context Diagram dan Data Flow Diagram (DFD).

# 4.1.1. Spesifikasi Sistem

Spesifikasi sistem *gateway redundancy* dengan menggunakan CARP *ifstated*, dan *pfsync* adalah sebagai berikut:

- a. Terdapat lima network, yaitu 1 external network dan 4 internal network.
- b. Internal network adalah network tempat sistem akan diimplementasikan. Terdapat 4 internal network
  - Net 2 : *Network* yang menghubungkan antara ketiga *gateway* dengan ISP
     Memiliki network ID 11.0.0.0/24.
  - 2. Net 3 : *Network* yang menghubungkan ketiga *gateway* dengan ISP 2. Memiliki network ID 12.0.0.0/24.
  - Net 4 : Network yang menhubungkan ketiga gateway dengan client. Memiliki network ID 10.0.0/24.
  - 4. Net 5 : *Network* yang digunakan oleh *pfsync*, menghubungkan ketiga *gateway*, sebagai sinkronasi *state*. Memiliki network ID 15.0.0.0/24.

Topologi yang digunakan adalah Topologi *Star*. Penggunaan Topologi *Star* pada *network* ini karena menyesuaikan dengan media transmisi yang digunakan, yaitu kabel UTP.

- c. *External network* adalah *network* lain yang terhubung ke *internal network*. *Network* ini meliputi *network* Universitas Brawijaya dan Internet. *Network* Universitas Brawijaya melingkupi *internal network* dan memiliki pengenal (*network* ID) 172.17.63.129/25.
- d. Gateway failover dalam sistem ini menggunakan CARP
- e. Ketiga gateway dikonfigurasi sebagai NAT
- f. Pfsync digunakan antara ketiga gateway, untuk sinkronasi state.
- g. Aturan pada *firewall pf*, menggunakan metoda NAT.
- h. Pada kondisi normal paket-paket data dari jaringan internal yang menuju ke Internet, akan melalui *gateway master* kemudian paket diteruskan ke ISP 1, sebagai ISP utama. Saat ISP 1 *down*, maka koneksi akan dipindahkan ke ISP 2 sebagai jalur *backup*. Saat ISP 1 kembali normal, maka koneksi akan dikembalikan ke ISP1.

Kondisi lain yang mungkin terjadi yaitu saat gateway master down, maka koneksi secara otomatis akan melalui gateway backup pertama, kemudian diteruskan ke ISP1. Saat ISP 1 down, maka koneksi akan dipindahkan ke ISP 2 sebagai jalur backup. Saat ISP 1 kembali normal, maka koneksi akan dikembalikaan ke ISP1.

Kondisi terakhir yang mungkin terjadi yaitu saat gateway master down dan gateway backup pertama down, maka koneksi secara otomatis akan melalui gateway backup kedua, kemudian diteruskan ke ISP1. Saat ISP 1 down, maka koneksi akan dipindahkan ke ISP 2 sebagai jalur backup. Saat ISP 1 kembali normal, maka koneksi akan dikembalikaan ke ISP1.

Komputer-komputer pada jaringan internal memiliki *default gateway* ke alamat *virtual* CARP, pada *gateway failover*. Pada kondisi normal, Gateway master melakukan advertisement melalui protokol CARP, sementara kedua gateway backup tidak. Ketika ada *client traffic* (paket data) melalui *gateway master*, maka akan terbentuk *state* (proses koneksi) dan secara langsung dikirim ke kedua *gateway backup* melalui protokol *pfsync*. Pada kondisi *gateway master* tidak aktif dan *client traffic* sedang berlangsung, *gateway backup* pertama akan melakukan *advertisement*, ketika *gateway backup pertama* tidak menerima tiga

kali advertisement dari gateway master, yaitu sekitar tiga detik dengan Konfigurasi konfigurasi standard. standard yang dimaksud adalah advbase=1dan advskew=0 pada gateway master. Pada saat itu juga gateway backup pertama menggantikan gateway master dan melanjutkan client traffic yang sedang berlangsung, sesuai dengan state yang diterima pada saat gateway master dalam kondisi aktif. Hal yang sama akan terjadi bila gateway backup pertama mengalami kegagalan, sementara gateway master belum kembali bekerja normal, maka gateway backup kedua akan mengambil alih peran. Pada kondisi gateway master kembali aktif, maka gateway master merequest update pf state melalui protokol pfsync semua state yang berlangsung pada gateway backup aktif sebelum protokol CARP mengambil alih fungsi gateway master. Dalam Gambar 4.1, diperlihatkan diagram jaringan yang menunjukkan internal network dan external network.



Gambar 4.1 Diagram Jaringan Internal Network dan External Network

Rancangan gateway redundancy dengan menggunakan CARP ifstated dan pfsync yang akan dikembangkan ditunjukkan pada Gambar 4.2.



# 4.1.2. Analisis Context Diagram dan Data Flow Diagram (DFD)

*Context Diagram* merupakan diagram yang menampilkan masukan proses, proses dan keluaran proses dari sistem secara umum. *Context Diagram* adalah DFD yang pertama kali dibuat dikenal dengan DFD level 0.

DFD level 0 *Client* ke Server merupakan diagram yang menjelaskan secara umum tentang masukan proses, proses dan keluaran proses yang terjadi pada *client* di *internal network* yang menuju ke *Internet*. DFD level 0 *Client* ke Internet ditunjukkan dalam Gambar 4.3.

Client di Internal Network	Client connection request	Gateway Redundancy connection request		
	Gateway redundancy connection reply	Proses Redundancy Gateway	Internet connection reply	Internet

Gambar 4.3 DFD Level 0 Client ke Internet

Berdasarkan Gambar 4.3, *Redundacy Gateway* memiliki kamus data sebagai berikut :

**C** Client connection request

*Client connection request* merupakan paket data yang dikirim oleh *client* di dalam *internal network* menuju suatu alamat yang berada di *Internet*.

- **C3** Gateway Redundacy connection request Gateway Redundacy connection request merupakan paket data yang dikirm oleh client, melawati failover gateway dan failover ISP, menuju suatu alamat yang berada di Internet.
- Gateway redundancy connection reply
   Gateway redundancy connection reply merupakan paket data balasan dari suatu
   Alamat di Internet, melewati failover gateway dan failover ISP menuju alamat
   IP pengirim.
- CSInternet connection replyInternet connection reply merupakan paket data balasan dari suatu alamat di<br/>Internet, menuju alamat Gateway Redundancy, yang akan diteruskan ke alamat<br/>IP pengirim.

Proses *Redundacy Gateway* yang ditunjukkan dalam Gambar 4.2 merupakan suatu proses yang terbentuk sebagai hasil dari konfigurasi dari sistem *Redundacy Gateway* menggunakan CARP, ifstated, dan pfsync. *Client connection request, Gateway Redundacy connection request, Gateway redundancy connection reply, Internet connection reply* merupakan data yang berbentuk *raw bit* yang bergerak melalui media transmisi.

DFD level 1 *Client* ke *Internet* merupakan penjelasan yang lebih detail dari DFD level 0 *Client* ke *Internet*. DFD level 1 *Client* ke *Internet* ditunjukkan dalam Gambar 4.4.



Gambar 4.4 DFD Level 1 Client ke Internet

Sebuah *client* yang berada di *internal network* melakukan suatu *client connection request* ke suatu alamat IP di Internet. Paket data yang dikirim akan melalui router untuk diteruskan ke ISP. Paket data yang dikirim ke router juga akan diterima oleh *gateway failover* dengan bantuan CARP, sementara proses state diantara router dilakukan oleh *pfsync*. Hal ini dilakukan agar paket data tetap dapat terkirim, saat salah satu router tidak bekerja. Kemudian paket data akan dibungkus ulang.

Alamat IP client pengirim akan digantikan dengan alamat IP *virtual gateway failover*. Proses ini disebut NAT, dan hal ini dilakukan dengan bantuan pf. Sebelum dikirim menuju ke ISP, *gateway redundancy* akan melakukan pengecekan status koneksi ISP, dengan bantuan *ifstated*. Kemudian paket data akan dikrim ke ISP yang hidup, untuk kemudian diteruskan ke Alamat IP tujuan.

Balasan yang diberikan oleh Alamat IP tujuan di Internet, akan diterima oleh ISP, kemudian diteruskan ke Gateway redundancy. Didalam *gateway*, akan terjadi proses penggantian header alamat IP tujuan, yaitu dari alamat IP *Gateway redundancy* menjadi alamat IP *client* pengirim paket awal.

DFD level 1 *Client* ke *Internet* memiliki kamus data yang dijelaskan sebagaimana berikut :

Solution CARP advertisement

Bila dilakukan oleh router Master, merupakan metoda pemberitahuan pada seluruh anggota router backup, bahwa router Master masih berfungsi. Saat router master berhenti melakukannya karena gagal bekerja, maka router Backup akan melakukan CARP advertisement.

- Echo Request Datagram
   Sesi koneksi yang dilakukan client menuju suatu alamat IP di Internet.
   Merupakan paket ICMP\_REQUEST
- Echo Reply Datagram
   Koneksi balasan dari suatu alamat IP di Internet, sebagai balasan paket
   ICMP\_REQUEST, paket data berupa ICMP\_REPLY.
- ISP Test Ping Request
   Koneksi yang dilakukan oleh proses ISP failover untuk mendeteksi status koneksi ISP.
- ISP Test Ping Reply
   Reply yang dilakukan ISP, bila ISP tersebut online.

Detil proses Redundancy Gateway yang ditunjukkan dalam Gambar 4.3 merupakan suatu proses yang terbentuk sebagai hasil dari konfigurasi Routing, *Gateway failover process*, NAT *process, dan* ISP *failover process*.

# 4.2. Perancangan Perangkat Keras

Perancangan perangkat keras adalah merancang suatu topologi jaringan komputer tempat sistem yang akan diimplementasikan. Topologi jaringan komputer yang digunakan pada sistem ini adalah Topologi Star, sebagaimana yang diperlihatkan dalam Gambar 4.5.



# Gambar 4.5 Diagram Jaringan Rancangan Implementasi

Dalam Gambar 4.5 di atas, dapat dijelaskan bahwa sebuah komputer *client* yang terhubung ke hub, terkoneksi dengan redundancy gateway, yang beranggotakan 3 gateway. Ketiga gateway tersebut memiliki jalur koneksi baik menuju ISP 1 maupun ISP 2. Ketiga gateway memiliki mekanisme pendeteksian putusnya jalur ISP,

untuk memilih ISP mana yang akan digunakan pada sesi koneksi berikutnya. Pada kondisi normal, koneksi dari client keluar, melalui gateway master diteruskan ke ISP 1. Perangkat lunak yang akan dirancang, seluruhnya akan diimplementasikan di komputer *gateway*.

# 4.3. Konfigurasi dan Perancangan Perangkat Lunak

Perangkat lunak yang akan diimplementasikan dikonfigurasi dan dirancang dengan beberapa tahap secara berurutan, yaitu : konfigurasi jaringan komputer secara *logical*, konfigurasi *gateway failover*, dan perancangan ISP *failover*.

# 4.3.1. Konfigurasi Jaringan Komputer Secara Logical

Topologi jaringan komputer yang secara fisik telah dikonfigurasi tersebut, perlu pula dikonfigurasi secara *logical*. Konfigurasi secara *logical* adalah konfigurasi jaringan komputer pada perangkat lunak dari perangkat-perangkat yang terhubung di jaringan komputer sehingga perangkat-perangkat tersebut dapat saling berkomunikasi. Konfigurasi tersebut adalah melakukan pengalamatan dengan Alamat IP.

Network yang digunakan dalam topologi ini adalah 10.0.0.0/24, 11.0.0.0/24, 12.0.0.0/24, 15.0.0.0/24. Prefik 24 atau setara dengan netmask 255.255.255.0 yang berarti terdapat 254 buah nomor IP *host*, sebuah nomor IP *network*, dan sebuah nomor IP *broadcast*. Daftar lengkap pengalamatan Alamat IP adalah sebagai berikut :

Terminal	Interface	Alamat IP	DNS	Gateway
Client	fxp0	10.0.0.100/24	202.162.208.99	10.0.0.1
Gateway Master	fxp0	10.0.0.2/24		
	fxp1	11.0.0.2/24		
	fxp2	12.0.0.2/24	202 162 208 99	11.0.0.100
	fxp3	15.0.0.2/24	202.162.208.100	12 0 0 100
	carp0	10.0.0.1/24		FASPE
	carp1	11.0.0.1/24	ATTER	os II A f
	carp2	12.0.0.1/24		t E H
Gateway Backup I	fxp0	10.0.3/24	202.162.208.99	11.0.0.100
Suite may Duckup I	fxp1	11.0.0.3/24	202.162.208.100	12.0.0.100

# Tabel 4.1 Pengalamat IP

<b>HTV</b>	fxp2	12.0.0.3/24	RAYNW	
	fxp3	15.0.0.3/24	SBRER	
<b>VAUN</b>	carp0	10.0.0.1/24	ITA2 KST	BKARA
LinAY A	carp1	11.0.0.1/24	<b>ERSIL</b> ati	A2 RS BE
	carp2	12.0.0.1/24	TVHER	ATTA
PEBRAN	fxp0	10.0.0.4/24		<b>H</b> HERS
Gateway Backup II	fxp1	11.0.0.4/24		NIXIVE
	fxp2	12.0.0.4/24	202.162.208.99	11.0.0.100
	fxp3	15.0.0.4/24		12.0.0.100
	carp0	10.0.0.1/24	202.162.208.100	12.0.0.100
	carp1	11.0.0.1/24	<b>DRA</b> N	
	carp2	12.0.0.1/24		
ISPI	fxp0	11.0.0.100/24	202.162.208.99	202 134 1 1
	fxp1	202.134.1.2/24	202.162.208.100	202.134.1.1
	fxp0	12.0.0.100/24	202.162.208.99	202 124 1-1
15F 11	fxp1	202.134.1.3/24	202.162.208.100	202.134.1.1

# 4.3.2. Konfigurasi Gateway Failover

Komputer *gateway* adalah komputer yang berfungsi sebagai pintu keluar utama bagi suatu paket data saat menuju *network* lain, selain network lokalnya. *Gateway* dalam tulisan ini adalah sebuah *router* yang secara *logical* menghubungkan *network* dari sisi dalam (*intranet*) ke *network* yang berada di sisi luar (*Internet*). Komputer *gateway* yang dikonfigurasi ini merupakan *end router*, yaitu suatu *router* yang langsung terhubung dengan *client* atau *host*, bukan dengan dengan *router* lain.

Setelah Sistem Operasi OpenBSD di-*install*, maka agar komputer *gateway* berfungsi sebagai *gateway*, perlu dikonfigurasi sebagai berikut :

- a. Mengaktifkan fungsi untuk meneruskan paket data
- b. Mengaktifkan fungsi PF, dan melakukan konfigurasi NAT
- c. Memasang Default Gateway : 11.0.0.100
- Memasang *Primary* DNS : 202.162.208.99 dan *Secondary* DNS : 202.162.208.100
- e. Pada fxp0, sebagai uplink menuju ISP 1, dikonfigurasi sebagai berikut :

- Alamat IP : 11.0.0.2
- Subnet Mask : 255.255.255.0
- f. Pada fxp1, sebagai uplink menuju ISP 2, dikonfigurasi sebagai berikut :
  - Alamat IP : 12.0.0.2
  - Subnet Mask : 255.255.255.0
- g. Pada fxp2, sebagai downlink menuju client, dikonfigurasi sebagai berikut :
  - Alamat IP : 10.0.0.2
  - Subnet Mask : 255.255.255.0

Enam langkah tersebut dilakukan juga pada 2 gateway backup dengan konfigurasi alamat IP sesuai dengan tabel 4.1. Setelah 2 gateway backup dikonfigurasi, langkah berikutnya adalah :

- i. Mengaktifkan CARP, dengan memberikan konfigurasi yang berbeda pada Master, Backup dan Backup 2 sesuai dengan prioritas tingkatan.
- ii. Mengkonfigurasi interface carp0, merupakan alamat IP virtual yang digunakan client sebagai default gateway. Dikonfigurasi sebagai berikut
  - Alamat IP : 10.0.0.1
  - Subnet Mask : 255.255.255.0
  - vhid 1, advbase 1, advskew 0
- Mengkonfigurasi interface carp1, merupakan alamat IP virtual yang digunakan sebagai alamat yang dikenali ISP 1 sebagai alamat gateway failover. Dikonfigurasi sebagai berikut
  - Alamat IP : 11.0.0.1
  - Subnet Mask : 255.255.255.0
  - vhid 1, advbase 1, advskew 0
- iv. Mengkonfigurasi interface carp2, merupakan alamat IP virtual yang digunakan sebagai alamat yang dikenali ISP 2 sebagai alamat gateway failover. Dikonfigurasi sebagai berikut
  - Alamat IP : 12.0.0.1
  - Subnet Mask : 255.255.255.0
  - vhid 1, advbase 1, advskew 0
- Mengaktifkan interface pfsync0, dan mengkonfigurasi interface fisik fxp3 sebagai interface fisik yang digunakan.

- Wengkonfigurasi langkah-langkah (*i-v*) di komputer gateway backup dan gateway backup 2, dengan alamat IP sesuai dengan tabel 4.1, namun dengan perbedaan konfigurasi pada :
  - Komputer gateway backup 1 : advskew 100
  - Komputer gateway backup 2 : advskew 200

# 4.3.3. Perancangan Sistem ISP failover

Sistem ISP failover yang dirancang adalah sistem yang dibangun dengan menggunakan *software ifstated* pada Sistem Operasi OpenBSD. Ifstated secara default telah terinstal pada sistem operasi OpenBSD. Untuk mendapatkan ifstated yang berfungsi secara tepat, maka perlu dilakukan beberapa perancangan.

Perancangan yang dilakukan pada ifstated.conf adalah sebagai berikut :

- a. Sistem akan melakukan pengecekan berkala terdapat status koneksi ke ISP 1.
- b. Bila terjadi kegagalan koneksi menuju ISP 1, maka sistem akan merubah default gateway menuju ISP 2.
- c. Sistem juga melakukan perubahan alamat IP CARP 1, yaitu menjadi 12.0.0.1, serta memindahkan *interface*nya pada *interface* yang terhubung ke alamat *network* 12.0.0.0/24
- d. Dalam state / fase ini sistem akan melakukan pengecekan terhadap status koneksi ke ISP 1.
- e. Bila koneksi ke ISP 1 kembali normal, maka default gateway akan kembali ke ISP 1.
- f. Sistem juga melakukan perubahan alamat IP CARP 1, yaitu menjadi 11.0.0.1, serta memindahkan *interfacenya* pada *interface* yang terhubung ke alamat *network* 11.0.0.0/24

Setelah melakukan konfigurasi pada jaringan komputer secara *logical* dan melakukan konfigurasi pada komputer *gateway*, maka topologi jaringan komputer akan tampak sebagaimana dalam Gambar 4.6.

# 4.3.4 Perancangan Pfsync Untuk Sinkronasi Data Antara 3 Gateway

Untuk melakukan sinkronasi state koneksi antara ke tiga gateway, kita menggunakan pfsync yang dikonfigurasi di interface di setiap gateway. Interface yang digunakan pada masing gateway adalah interface fxp3, yang memiliki alamat network IP 15.0.0.0/24

# 4.3.5 Perancangan Aturan-Aturan Untuk Mengkonfigurasi Nat

Untuk melakukan konfigurasi NAT, diperlukan baris perintah di dalam pf.conf. NAT malakukan pembungkusan paket data dan perubahan header alamat IP tujuan dari internal network dengan alanat IP 10.0.0/24 (dalam hal ini alamat IP klien) menjadi alamat IP network eksternal 11.0.0.0/24 dan 12.0.0.0/24 (dalam hal ini alamat IP komputer gateway)



Gambar 4.6 Diagram Jaringan Setelah Konfigurasi

# BAB V

# **IMPLEMENTASI SISTEM**

Sistem Gateway Redundancy yang telah dirancang pada Bab Empat, akan diimplementasikan pada tahap ini. Ada tiga tahap utama yang dilakukan pada bagian implementasi sistem ini, yaitu implementasi jaringan komputer dan implementasi *Gateway failover*, dan implementasi ISP failover.

# 5.1. Implementasi Jaringan Komputer

Pada tahap ini, rancangan jaringan komputer yang telah dibuat pada bab sebelumnya akan diwujudkan. Jaringan komputer terdiri dari dua bagian besar, yaitu bagian perangkat keras dan bagian perangkat lunak.

# 5.1.1. Perangkat Keras Jaringan Komputer

Pada bagian perangkat keras, komputer yang akan digunakan memiliki spesifikasi bervariasi, namun secara umum sebagai berikut :

- ➢ Processor : Intel Pentium 4 1.50 GHz
- ✤ Motherboard : ECS P4VMM2
- ➢ Harddisk : Maxtor 30 GB 5400 RPM
- Memory : Visipro 256 MB PC 2700
- > LAN Card

ò

- \* Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
- D-Link System Inc RTL8139 Ethernet
- ✗ Intel Express Pro 100
- Graphic Card : Eagle 64 MB nVidia RIVA TNT2

Perangkat keras lainnya adalah sebagai berikut :

- Switch : Switch Manageable Alied Telesin 24 port
- Image: Second state
   Secon
- C8 Konektor : RJ-45 AMP buatan Tyco Corporation

Perangkat keras tersebut kemudian disusun sehingga membentuk sebuah jaringan komputer dengan Topologi *Star* seperti yang diperlihatkan dalam Gambar 4.2.
## 5.1.2. Perangkat Lunak Jaringan Komputer

Pada tahap ini, perangkat keras yang telah disusun, dikonfigurasi perangkat lunaknya. Perangkat keras yang dikonfigurasi adalah komputer *gateway*, komputer ISP dan komputer *client* 

## 5.1.2.1. Konfigurasi Komputer Gateway

Konfigurasi pada komputer *gateway* dilakukan setelah Sistem Operasi OpenBSD ter-*install*. Dalam penginstalan, digunakan mode minimum, yaitu hanya menginstal paket dan software yang dibutuhkan, untuk alasan keamanan dan keringkasan. Yang dipilih dalam penginstalan antara lain :

- Bsd, kernel dari OpenBSD
- BaseXX.tgz, dasar sistem OpenBSD
- etcXX.tgz, file konfigurasi di folder /etc

Perlu diperhatikan untuk tidak menginstal paket compXX.tgz, untuk menghindari penyerang melakukan kompilasi di mesin gateway / ISP.

BAM

Semua konfigurasi yang berupa perintah-perintah \*.nix, dilakukan pada Terminal – Command Line. Sebuah Terminal – Command Line yang terdapat pada OpenBSD. Tanda # menunujukkan bahwa user login memiliki hak akses root.

Konfigurasi yang perlu dilakukan agar komputer gateway master dapat berfungsi dengan baik adalah sebagai berikut :

 Mengaktifkan fungsi untuk meneruskan paket data
 Konfigurasi ini dilakukan dengan menghilangkan tanda # di depan parameter net.inet.ip.forwarding yang terdapat dalam *file* sysctl.conf

# vi /etc/sysctl.conf

# Controls IP packet forwarding
net.inet.ip.forwarding=1

## b. Memasang Default Gateway

Konfigurasi ini dilakukan dengan menambahkan baris 11.0.0.100 dalam *file* mygate

# vi /etc/mygate

11.0.0.100

## c. Memasang DNS

Konfigurasi ini dilakukan dengan menambahkan baris nameserver 202.162.208.99 dan nameserver 202.162.208.100 dalam *file* resolv.conf

# vi /etc/resolv.conf

nameserver 202.162.208.99

nameserver 202.162.208.100

d. Konfigurasi fxp0 sebagai uplink menuju ISP 1

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp0* seperti dibawah ini :

# vi /etc/hostname.fxp0

inet 10.0.0.2 255.255.255.0 NONE

Konfigurasi fxp1 sebagai *uplink* menuju ISP 2
 Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp1* seperti dibawah ini ;

T

# vi /etc/hostname.fxp1

inet 11.0.0.2 255.255.255.0 NONE

f. Konfigurasi fxp2 sebagai *downlink* menuju client Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp2* seperti dibawah ini :

# vi /etc/hostname.fxp2

inet 12.0.0.2 255.255.255.0 NONE

Sedangkan konfigurasi yang perlu dilakukan agar komputer *gateway backup 1* dapat berfungsi dengan baik adalah sebagai berikut :

Mengaktifkan fungsi untuk meneruskan paket data
 Konfigurasi ini dilakukan dengan menghilangkan tanda # di depan parameter
 net.inet.ip.forwarding yang terdapat dalam *file* sysctl.conf

# Controls II net.inet.ip.f	P packet forwarding orwarding=1	5			
Memasang I	Default Gateway	TAS	BRA		
Konfigurasi mygate	ini dilakukan der	igan menan	bahkan baris	11.0.0.100	) dalam
# vi /etc/my	gate				7
11.0.0.100					
Memasang I	ons				
Konfigurasi	ini dilakukan	dengan	menambahkan	baris	namesei
202.162.208	.99 dan nameserve	er 202.162.2	08.100 dalam <i>j</i>	<i>ile</i> resolv.	conf
# vi /etc/res	olv.conf			2	
nameserver	202.162.208.99 202.162.208.100				
nameserver		シン語			
Konfigurasi	fxp0 sebagai <i>uplir</i>	ık menuju IS			
Konfigurasi Konfigurasi Konfigurasi	fxp0 sebagai <i>uplii</i> ini dilakukan p0 seperti dibawah	<i>ik</i> menuju IS dengan i ini :	nelakukan p	erubahan	pada
Konfigurasi Konfigurasi hostname.fxp # vi /etc/ho:	fxp0 sebagai <i>uplii</i> ini dilakukan 20 seperti dibawah stname.fxp0	<i>ik</i> menuju IS dengan ini :	nelakukan p	erubahan	pada
Konfigurasi Konfigurasi <i>hostname.fxp</i> # vi /etc/ho inet 10.0.0.3	fxp0 sebagai <i>uplii</i> ini dilakukan 20 seperti dibawah stname.fxp0 3 255.255.255.0 NO	<i>ik</i> menuju IS dengan i ini : NE	nelakukan po	erubahan	pada

# vi /etc/hostname.fxp1

## inet 11.0.0.3 255.255.255.0 NONE

f. Konfigurasi fxp2 sebagai downlink menuju client

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp2* seperti dibawah ini :

# vi /etc/hostname.fxp2

inet 12.0.0.3 255.255.255.0 NONE

Sedangkan konfigurasi yang perlu dilakukan agar komputer *gateway backup* 2 dapat berfungsi dengan baik adalah sebagai berikut :

a. Mengaktifkan fungsi untuk meneruskan paket data

Konfigurasi ini dilakukan dengan menghilangkan tanda # di depan parameter net.inet.ip.forwarding yang terdapat dalam *file* sysctl.conf

# vi /etc/sysctl.conf

# Controls IP packet forwarding net.inet.ip.forwarding=1

b. Memasang Default Gateway

Konfigurasi ini dilakukan dengan menambahkan baris 11.0.0.100 dalam *file* mygate

# vi /etc/mygate	ШМ	
11.0.0.100	]	
	1444 W	00

c. Memasang DNS

Konfigurasi ini dilakukan dengan menambahkan baris nameserver 202.162.208.99 dan nameserver 202.162.208.100 dalam *file* resolv.conf

# vi /etc/resolv.conf

nameserver 202.162.208.99

nameserver 202.162.208.100

d. Konfigurasi fxp0 sebagai uplink menuju ISP 1

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp0* seperti dibawah ini :

# vi /etc/hostname.fxp0

inet 10.0.0.4 255.255.255.0 NONE

Konfigurasi fxp1 sebagai *uplink* menuju ISP 2
Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp1* seperti dibawah ini :

# vi /etc/hostname.fxp1

inet 11.0.0.4 255.255.255.0 NONE

f. Konfigurasi fxp2 sebagai *downlink* menuju client
 Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp2* seperti dibawah ini :

# vi /etc/hostname.fxp2

inet 12.0.0.4 255.255.255.0 NONE

# 5.1.2.2. Konfigurasi Komputer ISP 1

Instalasi pada komputer ISP sama dengan yang dilakukan pada komputer Gateway, hanya berbeda dalam konfigurasi. Konfigurasi yang perlu dilakukan agar komputer ISP dapat berfungsi dengan baik adalah sebagai berikut :

a. Mengaktifkan fungsi untuk meneruskan paket data

Konfigurasi ini dilakukan dengan menghilangkan tanda # di depan parameter net.inet.ip.forwarding yang terdapat dalam *file* sysctl.conf

# vi /etc/sysctl.conf

# Controls IP packet forwarding net.inet.ip.forwarding=1

b. Memasang *Default Gateway* 

Konfigurasi ini dilakukan dengan menambahkan baris 11.0.0.100 dalam *file* mygate

# vi /etc/mygate

## 10.100.100.63

#### c. Memasang DNS

Konfigurasi ini dilakukan dengan menambahkan baris nameserver 202.162.208.99 dan nameserver 202.162.208.100 dalam *file* resolv.conf

# vi /etc/resolv.conf

nameserver 202.162.208.99

nameserver 202.162.208.100

d. Konfigurasi fxp0 sebagai *uplink* Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp0* seperti dibawah ini :

# vi /etc/hostname.fxp0

inet 10.100.100.1 255.255.255.128 NONE

e. Konfigurasi fxp1 sebagai *downlink* Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp1* seperti dibawah ini :

£1

# vi /etc/hostname.fxp1

inet 11.0.0.100 255.255.255.0 NONE

# 5.1.2.3. Konfigurasi Komputer ISP 2

Instalasi pada komputer ISP sama dengan yang dilakukan pada komputer Gateway, hanya berbeda dalam konfigurasi. Konfigurasi yang perlu dilakukan agar komputer ISP dapat berfungsi dengan baik adalah sebagai berikut :

a. Mengaktifkan fungsi untuk meneruskan paket data

Konfigurasi ini dilakukan dengan menghilangkan tanda # di depan parameter net.inet.ip.forwarding yang terdapat dalam *file* sysctl.conf

# vi /etc/sysctl.conf

# Controls IP packet forwarding net.inet.ip.forwarding=1

b. Memasang Default Gateway

Konfigurasi ini dilakukan dengan menambahkan baris 11.0.0.100 dalam *file* mygate

# vi /etc/mygate

10.100.100.63

c. Memasang DNS

Konfigurasi ini dilakukan dengan menambahkan baris nameserver 202.162.208.99 dan nameserver 202.162.208.100 dalam *file* resolv.conf

BRAM

# vi /etc/resolv.conf

nameserver 202.162.208.99

- nameserver 202.162.208.100
- d. Konfigurasi fxp0 sebagai *uplink* Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp0* seperti dibawah ini :

# vi /etc/hostname.fxp0

inet 10.100.100.2 255.255.255.128 NONE

e. Konfigurasi fxp1 sebagai *downlink* Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp1* seperti dibawah ini :

# vi /etc/hostname.fxp1

inet 12.0.0.100 255.255.255.0 NONE

# 5.1.2.4 Konfigurasi Komputer Client

Konfigurasi pada komputer *client* dilakukan agar komputer tersebut dapat berkomunikasi dengan komputer *gateway*. Konfigurasi yang dilakukan adalah dengan memberikan nomor IP pada setiap komputer *client*.

Contoh cara konfigurasi pada komputer *client* yang menggunakan Sistem Operasi Microsoft Windows XP Professional Edition Service Pack 2 adalah sebagai berikut :

<b>2</b>			
NEU INI N		Madministrative Tools	
Aechanic		🍓 Automatic Updates	
<b>A</b>		🤣 Date and Time	
<b>;</b>		S Display	
Yahoo! lessen		Folder Options	
		Fonts	
PDF		Controllers	
Asisten		Markened	
		Meuro	
<b>•</b> • • • • •	<b>D</b>	Mouse	
Opera	My Recent Docum	ents Vero buri Rights	
	Setwork Places	Network Connections	ocal Area Connection
	Control Papel	Network Setup Wizard	
	Concromanda	Phone and Modern Options	P
	Connect To	Power Options	
	Printers and Faxes	S Printers and Faxes	
		🖉 Regional and Language Options	
	Help and Support	Scanners and Cameras	
	>>> Search	Scheduled Tasks	
	700 Run	Security Center	
	0	Sounds and Audio Devices	
	觉 Windows Security	Speech	
		👰 Symantec LiveUpdate	
•		🧐 System	
All Programs 🌔		🛃 Taskbar and Start Menu	
	🔎 Log Off 🛛 Di	sconnect 😫 User Accounts	
		🧼 Windows Firewall	
Gambar	5.1 Local Are	a Connection di Control P	anel
Gambar	5.1 Local Are	a Connection di Control P	anel
Gambar	5.1 Local Are	a Connection di Control P	anel
Gambar	5.1 Local Are	a Connection di Control P ion Status	anel
Gambar	5.1 Local Are	a Connection di Control P ion Status	anel
Gambar	5.1 Local Are Local Area Connect General Support Connection Status:	a Connection di Control P ion Status	anel
Gambar	5.1 Local Are Local Area Connect General Support Connection Status: Duration:	a Connection di Control P ion Status ? X	anel
Gambar	5.1 Local Are Local Area Connect General Support Connection Status: Duration: Speed:	a Connection di Control P ion Status ? Connected 6 days 02:34:34 100.0 Mbps	anel
Gambar	5.1 Local Are Connection Status: Duration: Speed:	a Connection di Control P ion Status () () () () () () () () () () () () ()	anel
Gambar	5.1 Local Are Connection Status: Duration: Speed:	a Connection di Control P ion Status ? Connected 6 days 02:34:34 100.0 Mbps	anel
Gambar	• 5.1 Local Are Connection Status: Duration: Speed:	a Connection di Control P ion Status () () () () () () () () () () () () ()	anel
Gambar	• 5.1 Local Are Local Area Connection General Support Connection Status: Duration: Speed: Activity	a Connection di Control P ion Status ? Connected 6 days 02:34:34 100.0 Mbps	anel
Gambar	S.1 Local Are Connection Status: Duration: Speed: Activity	a Connection di Control P ion Status ? Connected 6 days 02:34:34 100.0 Mbps	anel
Gambar	S.1 Local Are Connection Status: Duration: Speed: Activity Se	a Connection di Control P ion Status ? Connected 6 days 02:34:34 100.0 Mbps ent Received	anel
Gambar	S.1 Local Are Connection Status: Duration: Speed: Activity Se	a Connection di Control P ion Status 2 2	anel
Gambar	S.1 Local Are Local Area Connect General Support Connection Status: Duration: Speed: Activity Se Bytes: 2	a Connection di Control P ion Status           Connected         6 days 02:34:34         100.0 Mbps	anel
Gambar	S.1 Local Are Local Area Connect General Support Connection Status: Duration: Speed: Activity Se Bytes: 2	a Connection di Control P ion Status () () () () () () () () () () () () ()	anel
Gambar	S.1 Local Are Connection Status: Duration: Speed: Activity Sees: Bytes: 2	a Connection di Control P ion Status  Connected 6 days 02:34:34 100.0 Mbps ent Received 108,972   17,864,571	anel
Gambar	S.1 Local Are Local Area Connect General Support Connection Status: Duration: Speed: Activity Se Bytes: 2 Properties Dis.	a Connection di Control P ion Status  Connected 6 days 02:34:34 100.0 Mbps ent Neceived 108,972 17,864,571 able	anel
Gambar	S.1 Local Are Connection Status: Duration: Speed: Activity Se Bytes: 2 Properties Dise	a Connection di Control P ion Status  Connected 6 days 02:34:34 100.0 Mbps ent Neceived 108,972 17,864,571 able	anel
Gambar	S.1 Local Area Local Area Connection Status: Duration: Speed: Activity Se Bytes: 2 Properties Disa	a Connection di Control P ion Status  Connected 6 days 02:34:34 100.0 Mbps  ent Received 108,972 17,864,571 able Close	anel

# a. Pilih menu Local Area Connection pada Control Panel



b. Sesuai dalam Gambar 5.2, pada *tab – General* pilih *Properties*. Selanjutnya akan muncul *window* sebagaimana tampak dalam Gambar 5.3.

ieneral	
_	Automotion Automotion
Connec	ot using:
1 ( <mark>1</mark>	/IA PCI 10/100Mb Fast Ethernet Ad Configure
This co	nnection uses the following items:
V 🔄	Client for Microsoft Networks
	File and Printer Sharing for Microsoft Networks
	UoS Packet Scheduler
<u> </u>	
202020	nstall Uninstall Properties
Dese	
Tran	Ismission Control Protocol/Internet Protocol. The default
wide	area network protocol that provides communication
acro	ss diverse interconnected hetworks.
Sho	w icon in notification area when connected
Not	ify me when this connection has limited or no connectivity
	OK Cancel
	OK Cancel
Gam	OK Cancel
Gam	OK Cancel abar 5.3 Local Area Connection Properties

 c. Sesuai dalam Gambar 5.3, pada tab – General pilih klik dua kali pada bagian Internet Protocol (TCP/IP). Window yang muncul, diisi dengan nilai sesuai dengan yang tertera dalam Gambar 5.4.

neral	
ou can get IP settings assigned iis capability. Otherwise, you nee ne appropriate IP settings.	automatically if your network supports d to ask your network administrator for
O Obtain an IP address autom	atically
• Use the following IP address	5.
IP address:	10 . 0 . 0 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10.0.0.1
	er dense stie eller
Obtain DND server address     Obtain DND server	er addresses:
Preferred DNS server:	202 . 162 . 208 . 99
Alternate DNS server:	202 . 162 . 208 . 100
	Advanced
	OK Cance

Gambar 5.4 Window Pengisian Nomor IP

Jika pengisian telah selesai dilakukan, maka klik satu kali pada tombol OK untuk menyimpan konfigurasi.

# 5.2. Implementasi Gateway failover pada komputer Gateway Master

Pada tahap ini, rancangan sistem *gateway failover* yang telah dibuat diimplementasikan pada komputer *gateway Master* yang telah dikonfigurasi pada tahap sebelumnya.

a. Mengaktifkan fungsi untuk melakukan firewall

Konfigurasi ini dilakukan dengan mengedit file rc.conf.local, dan menambahkan parameter pf=YES

# vi /etc/rc.conf.local

pf=YES

Mengedit file konfigurasi pf.conf, memasukkan rule NAT

# vi /etc/pf.conf

ext\_if2 = fxp2 # External intterface 2

int\_if = fxp0 # DMZ interface

pfs\_if = vr0 # Pfsync interface

nat on \$ext\_if2 from !\$ext\_if2 to any -> \$ext\_if2

b. Memanggil rule yang telah dikonfigurasi

Setelah rule dimasukkan, maka file konfigurasi tersebut perlu dipanggil dengan cara :

# pfctl -f /etc/pf.conf

c. Mengaktifkan carp dan fungsi preempt di file /etc/sysctl.conf

net.inet.carp.allow=1
net.inet.carp.preempt=1

Konfigurasi carp0 sebagai *default gateway* client
 Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp0* seperti dibawah ini :

# vi /etc/hostname.carp0

inet 10.0.0.1 255.255.255.0 10.0.0.255 vhid 1 advbase 1 advskew 0

Konfigurasi carp1 sebagai *default gateway* client
 Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp1* seperti dibawah ini :

# vi /etc/hostname.carp1

inet 11.0.0.1 255.255.255.0 11.0.0.255 vhid 2 advbase 1 advskew 0

f. Konfigurasi carp2 sebagai default gateway Client

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp2* seperti dibawah ini :

# vi /etc/hostname.carp2

inet 12.0.0.1 255.255.255.0 12.0.0.255 vhid 3 advbase 1 advskew 0

# g. Konfigurasi fxp3 sebagai pfsync

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp1* seperti dibawah ini :

# vi /etc/hostname.pfsync0

up syncdev fxp3

# 5.3. Implementasi Gateway failover pada komputer Gateway Backup

Pada tahap ini, rancangan sistem *gateway failover* yang telah dibuat diimplementasikan pada komputer *gateway Backup* yang telah dikonfigurasi pada tahap sebelumnya.

a. Mengaktifkan fungsi untuk melakukan firewall

Konfigurasi ini dilakukan dengan mengedit file rc.conf.local, dan menambahkan parameter pf=YES

# vi /etc/rc.conf.local

pf=YES

Mengedit file konfigurasi pf.conf, memasukkan rule NAT

# vi /etc/pf.conf

b. Memanggil rule yang telah dikonfigurasi

Setelah rule dimasukkan, maka file konfigurasi tersebut perlu dipanggil dengan

cara :

# pfctl -f /etc/pf.conf

c. Mengaktifkan carp di file /etc/sysctl.conf

net.inet.carp.allow=1

d. Konfigurasi carp0 sebagai default gateway client

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp0* seperti dibawah ini :

# vi /etc/hostname.carp0

inet 10.0.0.1 255.255.255.0 10.0.0.255 vhid 1 advbase 1 advskew 100

e. Konfigurasi carp1 sebagai *default gateway* client Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp1* seperti dibawah ini :

# vi /etc/hostname.carp1

inet 11.0.0.1 255.255.255.0 11.0.0.255 vhid 2 advbase 1 advskew 100

f. Konfigurasi carp2 sebagai default gateway Client

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp2* seperti dibawah ini :

# vi /etc/hostname.carp2

## inet 12.0.0.1 255.255.255.0 12.0.0.255 vhid 3 advbase 1 advskew 100

g. Konfigurasi fxp3 sebagai pfsync

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp1* seperti dibawah ini :

# vi /etc/hostname.pfsync0

up syncdev fxp3

# 5.4. Implementasi Gateway failover pada komputer Gateway Backup 2

Pada tahap ini, rancangan sistem *gateway failover* yang telah dibuat diimplementasikan pada komputer *gateway Backup 2* yang telah dikonfigurasi pada tahap sebelumnya.

a. Mengaktifkan fungsi untuk melakukan firewall

Konfigurasi ini dilakukan dengan mengedit file rc.conf.local, dan menambahkan parameter pf=YES

# vi /etc/rc.conf.local

pf=YES

Mengedit file konfigurasi pf.conf, memasukkan rule NAT

# vi /etc/pf.conf

ext\_if = vic0 # External interface

ext\_if2 = vic1 # External intterface 2

int\_if = vic2 # DMZ interface

pfs\_if = vic3 # Pfsync interface

b. Memanggil rule yang telah dikonfigurasi

Setelah rule dimasukkan, maka file konfigurasi tersebut perlu dipanggil dengan cara :

# pfctl -f /etc/pf.conf

c. Mengaktifkan carp di file /etc/sysctl.conf

net.inet.carp.allow=1

d. Konfigurasi carp0 sebagai default gateway client

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp0* seperti dibawah ini :

# vi /etc/hostname.carp0 AD E

inet 10.0.0.1 255.255.255.0 10.0.0.255 vhid 1 advbase 1 advskew 100

e. Konfigurasi carp1 sebagai *default gateway* client Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp1* seperti dibawah ini :

# vi /etc/hostname.carp1

inet 11.0.0.1 255.255.255.0 11.0.0.255 vhid 2 advbase 1 advskew 100

f. Konfigurasi carp2 sebagai *default gateway* Client Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.carp2* seperti dibawah ini :

1,75.

# vi /etc/hostname.carp2

inet 12.0.0.1 255.255.255.0 12.0.0.255 vhid 3 advbase 1 advskew 100

g. Konfigurasi fxp3 sebagai pfsync

Konfigurasi ini dilakukan dengan melakukan perubahan pada *file hostname.fxp1* seperti dibawah ini :

# vi /etc/hostname.pfsync0

up syncdev fxp3

# 5.4 Implementasi ISP Failover pada Komputer Gateway

Pada tahap ini, rancangan sistem *gateway failover* yang telah dibuat diimplementasikan pada komputer *gateway* yang telah dikonfigurasi pada tahap sebelumnya.

a. Mengetikkan sintak pendeteksian ISP pada ifstated.conf

# vi /etc/ifstated.conf asmaster = '("ifconfig | grep MASTER > /dev/null" every 10)' state auto { BRAWIUAL if \$asmaster set-state automaster if ! \$asmaster set-state auto isp1 = '( "ping -q -c 1 -w 1 11.0.0.100 > /dev/null" every 10)' state automaster { if \$isp1 set-state primary if ! \$isp1 set-state demoted state primary { init { run "ifconfig carp1 11.0.0.1/24 vhid 2 carpdev vic0 advbase 1 advskew 0" run "route change default 11.0.0.100" ł if ! \$asmaster set-state auto if ! \$isp1 set-state demoted state demoted { init { run "ifconfig carp1 12.0.0.1/24 vhid 2 carpdev vic1 advbase 1 advskew 0" run "route change default 12.0.0.100" if ! \$asmaster set-state auto if \$isp1 set-state primary

 Mengaktifkan ifstated agar di load di awal sebagai daemon, dengan cara memasukkan "/usr/sbin/ifstated ke dalam file /etc/rc.local

# vi /etc/rc.local
/usr/sbin/ifstated
c. Merestart komputer dengan cara

# reboot

d. Memastikan ifstated telah berjalan sebagai daemon, dengan cara

	JERSI		VIJA
5			
			3
		55	
	A U YU	SHATT	STAS

# BAB VI PENGUJIAN SISTEM

Sistem pemfilteran Gateway Redundancy yang telah diimplementasikan pada Bab Lima, akan dianalisis dan diuji pada tahap ini. Pengujian dan analisis sistem perlu dilakukan untuk mengetahui apakah sistem yang telah dirancang dan diimplementasikan telah bekerja sesuai dengan tujuan pembuatan sistem. Pengujian dan analisis dilakukan secara bertahap sebagaimana urutan permasalahan yang ada di bagian rumusan masalah. Pengujian dan analisis yang dilakukan adalah pengujian dan analisis internal network, pengujian dan analisis external network, pengujian dan analisis sistem gateway redundancy dalam melakukan fail-over redundancy, pengujian dan analisis sistem gateway redundancy dalam mendeteksi putusnya koneksi ke ISP, dan melakukan peralihan jalur. Spesifikasi perangkat keras yang digunakan dalam pengujian Sistem Gateway Redundancy adalah sebagai berikut :

- Komputer Gateway
  - C3 Processor : Intel Pentium 4 1.50 GHz
  - - cos Harddisk : Maxtor 30 GB 5400 RPM
    - C3 Memory : Visipro 256 MB PC 2700
    - C3 LAN Card
      - \* Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
      - ★ D-Link System Inc RTL8139 Ethernet
    - 3 Graphic Card : Eagle 64 MB nVidia RIVA TNT2

## Komputer *Client*

CB	Processor	: Intel Pentium 4 - 1.8 GHz
CB	Motherboard	: ECS P4VMM2
63	Harddisk	: Maxtor 30 GB - 5400 RPM
C3	Memory	: Visipro 256 MB PC 2700
CB	LAN Card	: VIA PCI 10/100Mb Fast Ethernet Adapter
CB	Graphic Card	: S3 Graphics ProSavageDDR 32 MB (onboard)
C3	Nomor IP	: 10.0.0.100

## Sistem Operasi : Windows XP Professional Service Pack 2

#### 6.1 Pengujian Dan Analisis Internal Network

Pengujian dan analisis sistem pada tahap ini, dititikberatkan pada *internal network* yang telah diimplementasikan, yaitu *network* yang menghubungkan *client* dan ketiga *gateway*. Langkah-langkah pengujian adalah sebagai berikut :

#### a. Tujuan

Pengujian ini dilakukan untuk mengetahui apakah *client* dan *gateway-gateway* yang berada dalam *internal network* telah dapat saling berkomunikasi [VAS-07].

#### b. Spesifikasi dan Konfigurasi Komputer

Komputer *client* dan komputer *gateway* memiliki spesifikasi sebagaimana yang telah disebutkan di bagian awal bab ini. Komputer *gateway* telah dikonfigurasi sebagaimana telah dijelaskan pada Bab Empat dan Bab Lima.

#### c. Software Aplikasi

- nmap-4.11-1.1
- arp

#### d. Prosedur Pengujian

. Menjalankan perintah nmap pada komputer *client* untuk memeriksa alamat IP komputer-komputer yang sedang saling terhubung dalam *internal network*.

#### # nmap -sP 10.0.0/24

Perintah diatas memiliki arti jalankan nmap dengan parameter *Ping Scan* pada *network* 10.0.0.0/24

*ii.* Menjalankan perintah arp pada komputer *client* untuk mengetahui alamat *MAC* dari semua alamat IP yang pernah terhubung.

#### # arp -an

Perintah diatas memiliki arti jalankan arp dengan parameter *-a*, untuk menampilkan semua daftar arp, dan paramater –n untuk menampilkan dalam bentuk alamat IP.

Hasil yang diharapkan dari pengujian ini adalah komputer *client* mendapat balasan atas pesan yang dikirimkan ke semua anggota *network* 10.0.0.0/24, serta komputer client mencatat semua alamat *MAC* di dalam tabel arp (arp cache).

# f. Hasil Pengujian dan Analisis

Saat perintah nmap dijalankan, komputer *client* akan mengirim pesan *ping* ke seluruh alamat IP *network* 10.0.0.0/24 Semua alamat IP *network* 10.0.0.0/24 yang pada saat perintah nmap dijalankan aktif, akan mengirim pesan balasan kepada komputer *client*. Hasil dari nmap adalah sebagai berikut :

# nmap -sP 10.0.0/24 Starting Nmap 4.53 ( http://insecure.org ) at 2009-06-06 10:11 WIT Host 10.0.0.1 appears to be up. MAC Address: 00:00:5E:00:01:01 (USC Information Sciences Inst) Host 10.0.0.2 appears to be up. MAC Address: 00:0C:29:EB:8E:D2 Host 10.0.0.3 appears to be up. MAC Address: 00:0C:29:F4:28:4B Host 10.0.0.4 appears to be up. MAC Address: 00:0C:29:53:AC:E5 Host 10.0.0.100 appears to be up. Nmap done: 256 IP addresses (5 hosts up) scanned in 35.660 seconds

Gambar 6.1 Hasil Perintah nmap

Dari hasil perintah nmap, dapat diketahui bahwa dalam *internal network* terdapat 4 alamat IP yang sedang hidup dengan IP 10.100.100.1 – 10.100.100.4, dan 10.100.100.100. Kemudian saat perintah arp dijalankan, komputer akan menampilkan tabel arp berisi alamat *MAC* dari semua alamat IP yang pernah berkomunikasi dengan komputer *client*. Serta pada *interface NIC* yang digunakan utnuk berkomunikasi dengan alamat IP tersebut. Hasil dari arp adalah sebagai berikut :

# arp -an
? (10.0.0.1) at 00:00:5e:00:01:01 on vic0
? (10.0.0.2) at 00:0c:29:eb:8e:d2 on vic0
? (10.0.0.3) at 00:0c:29:f4:28:4b on vic0
? (10.0.0.4) at 00:0c:29:53:ac:e5 on vic0

#### Gambar 6.2 Hasil Perintah arp

#### g. Kesimpulan

Komputer *gateway* dan komputer *client* yang berada dalam *internal network* telah dapat saling berkomunikasi.

#### 6.2 Pengujian Dan Analisis External Network

Pengujian dan analisis sistem pada tahap ini, dititikberatkan pada *external network* yang telah diimplementasikan. *External network* adalah *network* yang menghubungkan antara ketiga *gateway* dengan ISP-ISP. Langkah-langkah pengujian adalah sebagai berikut :

#### a. Tujuan

Pengujian ini dilakukan untuk mengetahui apakah ketiga *gateway* dan ISP yang berada dalam *external network* telah dapat saling berkomunikasi.

#### b. Spesifikasi dan Konfigurasi Komputer

Komputer *gateway* dan komputer ISP memiliki spesifikasi sebagaimana yang telah disebutkan di bagian awal bab ini. Komputer *gateway* dan komputer ISP telah dikonfigurasi sebagaimana telah dijelaskan pada Bab Empat dan Bab Lima.

#### c. Software Aplikasi

- nmap-4.11-1.1
- arp

## d. Prosedur Pengujian

*i*. Menjalankan perintah nmap pada komputer *gateway Master* untuk memeriksa alamat IP komputer-komputer yang sedang saling terhubung dalam *external network*.

# nmap -sP 11.0.0.0/24

Perintah diatas memiliki arti jalankan nmap dengan parameter *Ping Scan* pada *network* 11.0.0.0/24

# nmap -sP 12.0.0/24

Perintah diatas memiliki arti jalankan nmap dengan parameter *Ping Scan* pada *network* 12.0.0.0/24

*ii.* Menjalankan perintah arp pada komputer *gateway Master* untuk mengetahui *alamat MAC* dari semua alamat IP yang pernah terhubung.

#### # arp -an

Perintah diatas memiliki arti jalankan arp dengan parameter -*a*, untuk menampilkan semua daftar arp, dan paramater –n untuk menampilkan dalam bentuk alamat IP.

## e. Hasil Yang Diharapkan

Hasil yang diharapkan dari pengujian ini adalah komputer *Gateway Master* mendapat balasan atas pesan yang dikirimkan ke semua anggota *network* 11.0.0.0/24 dan 12.0.0.0/24, serta komputer *Gateway Master* mencatat semua alamat *MAC* di dalam tabel arp (arp cache).

## f. Hasil Pengujian dan Analisis

Saat perintah nmap dijalankan, komputer *gateway* akan mengirim pesan *ping* ke seluruh anggota *network* 11.0.0.0/24 dan 12.0.0.0/24 Semua anggota *network* 11.0.0.0/24 dan 12.0.0.0/24 yang pada saat perintah nmap dijalankan hidup, akan mengirim pesan balasan kepada komputer *gateway*. Hasil dari nmap adalah sebagai berikut :

```
# nmap -sP 11.0.0.0/24
Starting Nmap 4.53 ( http://insecure.org ) at 2009-06-06 10:19 WIT
Host 11.0.0.1 appears to be up.
MAC Address: 00:00:5E:00:01:01 (USC Information Sciences Inst)
Host 11.0.0.2 appears to be up.
MAC Address: 00:0C:29:EB:8E:D2
Host 11.0.0.3 appears to be up.
MAC Address: 00:0C:29:F4:28:4B
Host 11.0.0.4 appears to be up.
MAC Address: 00:0C:29:53:AC:E5
Host 11.0.0.100 appears to be up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 34.560 seconds
```

Gambar 6.3 Hasil Perintah nmap 11.0.0.0/24

# nmap -sP 12.0.0.0/24 Starting Nmap 4.53 ( http://insecure.org ) at 2009-06-06 11:21 WIT Host 12.0.0.1 appears to be up. MAC Address: 00:00:5E:00:01:01 (USC Information Sciences Inst) Host 12.0.0.2 appears to be up. MAC Address: 00:0C:29:EB:8E:D2 Host 12.0.0.3 appears to be up. MAC Address: 00:0C:29:F4:28:4B Host 12.0.0.4 appears to be up. MAC Address: 00:0C:29:53:AC:E5 Host 12.0.0.100 appears to be up. Nmap done: 256 IP addresses (5 hosts up) scanned in 36.630 seconds

# Gambar 6.4 Hasil Perintah nmap 12.0.0.0/24

Dari hasil perintah nmap, dapat diketahui bahwa dalam *internal network* terdapat 4 alamat IP yang sedang hidup dengan IP 11.100.100.1 - 11.100.100.4, dan 11.100.100.100. serta 12.100.100.1 - 12.100.100.4, dan 12.100.100.100. Kemudian saat perintah arp dijalankan, komputer akan menampilkan tabel arp berisi alamat MAC dari semua alamat IP yang pernah berkomunikasi . Hasil dari arp adalah sebagai berikut :

```
# arp -an
? (10.0.0.1) at 00:00:5e:00:01:01 on vic0
? (10.0.0.2) at 00:0c:29:eb:8e:d2 on vic0 static
? (10.0.0.3) at 00:0c:29:f4:28:4b on vic2
? (10.0.0.4) at 00:0c:29:53:ac:e5 on vic2
? (10.0.0.100) at 00:0c:29:e7:dd:78 on vic2
? (11.0.0.1) at 00:0c:5e:00:01:01 on vic0
? (11.0.0.3) at 00:0c:29:f4:28:37 on vic0
? (11.0.0.4) at 00:0c:29:f4:28:37 on vic0
? (11.0.0.4) at 00:0c:29:f4:ed:6f on vic0
? (12.0.0.1) at 00:00:5e:00:01:01 on vic0
```

? (12.0.0.2) at 00:0c:29:eb:8e:c8 on vic1 static ? (12.0.0.3) at 00:0c:29:f4:28:41 on vic1 ? (12.0.0.4) at 00:0c:29:53:ac:db on vic1 ? (12.0.0.100) at 00:0c:29:59:07:9e on vic1

#### Gambar 6.5 Hasil Perintah arp

#### g. Kesimpulan

Komputer-komputer *gateway* dan komputer-komputer *ISP* yang berada dalam *external network* telah dapat saling berkomunikasi.

# 6.3 Pengujian dan Analisis Sistem *Gateway Redundancy* saat *Gateway Master* Gagal Bekerja

Pengujian dan analisis sistem pada tahap ini, dititikberatkan pada peran komputer gateway Backup 1 dalam melakukan gateway fail-over, ketika komputer Gateway Master down/tidak aktif Langkah-langkah pengujian adalah sebagai berikut :

## a. Tujuan

Pengujian ini dilakukan untuk mengetahui apakah paket data yang berasal dari *internal network* dapat diteruskan oleh sistem *gateway fail-over* menuju *external network* walaupun *Gateway Master* gagal bekerja/tidak aktif.

## b. Spesifikasi dan Konfigurasi Komputer

Komputer *client*, komputer *gateway*, serta komputer ISP memiliki spesifikasi sebagaimana yang telah disebutkan di bagian awal bab ini. Komputer *client*, komputer *gateway*, serta komputer ISP telah dikonfigurasi sebagaimana telah dijelaskan pada Bab Empat dan Bab Lima.

#### c. Software Aplikasi

- R Mozilla Firefox 3 / Internet Explorer
- R Flash Get Download Manager
- A Yahoo Messenger
- ca tcpdump 3.9.4 /wireshark 0.99.4
- R traceroute / tracert

#### d. Prosedur Pengujian

 Menjalankan perintah tepdump pada komputer gateway backup 1, yaitu pada NIC yang terhubung dengan network 10.0.0/24, 11.0.0.0/24, 15.0.0.0/24 untuk melihat aliran data didalamnya.



Gambar 6.6 Pengujian gateway *fail-over* 

3 Perintah tepdump dilakukan di komputer gateway *backup* 1, yaitu di masing *network interface* yang terhubung dengan ketiga *network*, 10.0.0/24, 11.0.0.0/24, 15.0.0.0/24. berfungsi untuk melihat paket data dari/menuju IP 10.0.0.100 menuju/dari alamat IP <u>www.klikbca.com</u>, <u>www.narutofan.com</u> serta Yahoo Messenger, adalah sebagai berikut :

Di Komputer gateway backup 1 network 10.0.0/24

# tcpdump -i vic2 -w r2dump10 &

Perintah diatas memilki arti jalankan perintah tepdump pada *interface vic2* Di Komputer *gateway backup 1 network* 11.0.0.0/24

# tcpdump -i vic0 -w r2dump11 &

Perintah diatas memilki arti jalankan perintah tepdump pada *interface vic0* Di Komputer *gateway backup 1 network* 15.0.0.0/24

# tcpdump -i vic3 -w r2dump15 &

Perintah diatas memilki arti jalankan perintah tepdump pada interface vic3

ii. Menjalankan Firefox yang ada di komputer client.

→ Start | All Program | Mozilla Firefox | Mozilla Firefox

- iii. Membuka situs <u>www.klikbca.com</u> dengan Web browser, melakukan *login* dan transaksi.
- iv. Melakukan download ke situs www.narutofan.com
  - a. Tanpa menggunakan download manager.
  - b. Menggunakan download manager.
- v. Menggunakan Yahoo Messenger untuk melakukan chating.
- vi. Melakukan traceroute untuk mengetahui jalur yang digunakan.
- vii. Mematikan / menonaktifkan Komputer Gateway Master
- viii.Melanjutkan mengakses situs <u>www.klikbca.com</u>, mendownload, dan menggunakan Yahoo Messenger.
- ix. Melakukan traceroute untuk mengetahui jalur baru yang kini digunakan.

#### e. Hasil Yang Diharapkan

Hasil yang diharapkan dari pengujian ini adalah *Web browser* di komputer *client* dapat menampilkan situs <u>www.klikbca.com</u>, melakukan download ke situs <u>www.narutofan.com</u>, chating menggunakan Yahoo Messenger, bisa dilakukan pada saat *Gateway Master* masih bekerja/aktif, maupun pada saat *Gateway Master* berhenti bekerja/tidak aktif. Program traceroute menampilkan jalur yang berbeda saat *gateway master* aktif dan tidak aktif.

#### f. Hasil Pengujian dan Analisis

Saat komputer *client* menjalankan prosedur pengujian (menjalankan Web browser, melakukan download, menggunakan Yahoo Messenger) tcpdump yg sedang berjalan di komputer *gateway backup 1*, akan merekam paket data yang mengalir antara komputer *client* dengan Internet. Hasil dari tcpdump adalah sebagai berikut :

• Tcpdump di Komputer *gateway backup* 1 NIC vic2, terhubung dengan 10.0.0/24

# tcpdump -i vic2

listening on vic2, link-type EN10MB

13:16:00.990244 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:01.818378 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:02.686923 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:03.786601 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:04.777715 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:05.772114 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:06.716454 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:07.828556 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:08.830745 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:09.939888 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:10.021087 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:10.105747 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:10.628603 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:11.347891 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:11.347891 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10]

13:16:11.287092 10.0.0.100.2146 > 68.180.217.29.5050: P 1:34(33) ack 1 win 65340 (DF)

13:16:11.667205 68.180.217.29.5050 > 10.0.0.100.2146: P 1:106(105) ack 34 win 65535

13:16:11.692519 10.0.0.100.2147 > 66.163.169.186.https: S 1482567984:1482567984(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)

13:16:11.357755 68.180.217.29.5050 > 10.0.0.100.2146: P 14392:14448(56) ack 927 win 65535 (DF) 13:16:11.347891 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:16.984750 10.0.0.100.1074 > 202.162.208.99.domain: 64668+ A? ibank.klikbca.com. (35) 13:16:17.457100 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:17.476250 202.162.208.99.domain > 10.0.0.100.1074: 64668 1/5/5 A 202.6.211.9 (239) (DF) 13:16:17.481606 10.0.0.100.1187 > 202.6.211.9.https: S 3834791029:3834791029(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:16:41.192802 10.0.0.100.1074 > 202.162.208.99.domain: 37260+ A? www.narutofan.com. (35) 13:16:41.338823 202.162.208.99.domain > 10.0.0.100.1074: 37260 6/4/4 A 213.133.113.131,[|domain] 13:16:41.576418 10.0.0.100.2153 > 213.133.113.131.www: S 203271031:203271031(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:16:41.708189 213.133.113.131.www > 10.0.0.100.2153: S 859042028:859042028(0) ack 203271032 win 65535 <mss 1460, nop, nop, sackOK> 13:16:41.709131 10.0.0.100.2153 > 213.133.113.131.www: ack 1 win 64240 (DF) 13:16:41.839237 10.0.0.100.2153 > 213.133.113.131.www: P 1:814(813) ack 1 win 64240 (DF) 13:18:43.186531 CARPv2-advertise 36: vhid=1 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:18:43.524101 10.0.0.100.1074 > 202.162.208.99.domain: 30350+ A? ftpl.download.narutofan.com. (45) 13:18:44.279749 202.162.208.99.domain > 10.0.0.100.1074: 30350 1/4/4 (209)13:18:46.017713 10.0.0.100.2155 > 66.90.101.237.www: P 1:830(829) ack 1 win 64240 (DF) 13:18:46.291099 66.90.101.237.www > 10.0.0.100.2155: . ack 830 win 65535 13:18:46.310908 10.0.0.100.2244 > 202.162.208.99.domain: 47099+ A? ftp2.download.narutofan.com. (45) 13:18:46.322228 202.162.208.99.domain > 10.0.0.100.1099: 2301 1/2/1 A[ doma 13:17:52.409618 192.168.199.254.domain > 10.0.0.100.2250: 13542 1/4/3 (193) 13:18:46.428806 10.0.0.100.2259 > 67.159.45.121.www: S 3618338161:3618338161(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)in] 13:18:46.589516 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:18:46.589605 arp who-has 10.0.0.1 tell 10.0.0.1 13:18:48.050398 10.0.0.100.2713 > 67.159.45.121.www: S 4038249587:4038249587(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:18:48.055986 67.159.45.121.www > 10.0.0.100.2712: S 753882405:753882405(0) ack 292071058 win 65535 <mss 1460, nop, nop, sackOK> 13:18:48.709097 10.0.0.100.2717 > 66.90.101.237.www: S 3921961004:3921961004(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:18:48.715568 66.90.101.237.www > 10.0.0.100.2717: S 2655997530:2655997530(0) ack 3921961005 win 65535 <mss 1460, nop, nop, sackOK> 13:19:28.773720 202.6.211.9.https > 10.0.0.100.2962: . ack 167 win 32602 13:19:28.793922 10.0.0.100.2962 > 202.6.211.9.https: ack 1 win 64860 (DF) 13:19:32.073254 10.0.0.100.2146 > 68.180.217.29.5050: P 2783:2816(33) ack 15106 win 64626 (DF) 60771 packets captured 106 packets received by filter 0 packets dropped by kernel

# Gambar 6.7 Hasil †cpdump Paket Data pada Interface Network 10.0.0.0/24 Komputer Gateway Backup 1 pada Pengujian Sistem Fail-over redundancy

Dari hasil tcpdump, dapat diketahui bahwa awal koneksi, terdapat paket advertisement dari *gateway master*, hal tersebut ditunjukkan dengan nilai advskew=0, vhid=1 menunjukkan bahwa tcpdump di lakukan di*interface network* 10.0.0.0/24, yang merupakan konfigurasi CARP pada *gateway master*. Advertisement ini menunjukkan bahwa *gateway master* masih aktif bekerja. Advertisement dilakukan secara berkala, yaitu kurang lebih setiap 1 detik, yang ditunjukkan pada tabel 6.1 :

Waktu Advertisement	Selisih Waktu
13:16:00.990244	0.828134
13:16:01.818378	0.868545
13:16:02.686923	1.099678
13:16:03.786601	0.991114
13:16:04.777715	0.994399
13:16:05.772114	
osi PraRA	
Rata-rata	0.956374

Tabel 6.1 Waktu advertisement CARP gateway master

Kemudian terjadi autentifikasi dari Yahoo Messenger untuk melakukan login user, saat user valid, maka aplikasi akan membuka port https. Yang dilanjutkan pengiriman data dari server Yahoo Messenger ke alamat IP client. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk *meresolve* alamat ibank.klikbca.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ibank.klikbca.com memiliki alamat IP 202.6.211.9, setelah sebelumnya terdapat paket advertisement gateway master. Kemudian terdapat paket data dari IP 10.0.0.100 menuju IP 202.6.211.9 dengan port https (443), yang diawali treeway handshaking. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat www.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa www.narutofan.com.memiliki alamat IP 213.133.113.131. Lalu kemudian terdapat paket data dari IP 10.0.0.100 menuju IP 213.133.113.131, yang diawali tree-way handshaking. Paket data kemudian adalah proses GET download file naruto\_452.zip dimana halaman menuju link ftp1.download.narutofan.com. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ftpl.download.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftp1.download.narutofan.com memiliki alamat IP 66.90.101.237. Kemudian komunikasi data terjadi antara client dengan alamat IP 66.90.101.237. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ftp2.download.narutofan.com., setelah sebelumnya terdapat paket advertisement gateway master yang merupakan advertisement terakhir sebelum gateway Master dimatikan. Advertisement ini terjadi pada 13:18:43.186531. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftp2.download.narutofan.com memiliki alamat IP 67.159.45.121. Kemudian komunikasi data terjadi antara client dengan alamat IP 67.159.45.121. Transaksi data berlanjut, sampai komputer gateway master dimatikan/dinonaktifkan, yang ditunjukkan dengan advertisement yang dilakukan komputer gateway backup 1, yang terjadi pada waktu 13:18:46.589516. Advertisement tersebut dilakukan oleh gateway backup 1 ditunjukkan oleh nilai advskew=100, vhid=1 menunjukkan bahwa tcpdump di

lakukan di*interface network* 10.0.0.0/24, yang merupakan konfigurasi CARP pada *gateway backup 1. Advertisement* ini menunjukkan bahwa *gateway master* telah tidak aktif bekerja. *Advertisement* dilakukan secara berkala, yaitu kurang lebih setiap 1 detik sama seperti pada *advertisement gateway master*. Waktu peralihan yang dibutuhkan antara tidak aktifnya *gateway master* hingga aktifnya *gateway backup* 1, adalah sekitar 3.402985 detik, seperti ditunjukkan pada tabel 6.2

#### Tabel 6.2 Waktu Peralihan Gateway Master-Backup 1

Walter advantisement tonskip acting master	13:18:43 186531
waktu auvertisement terakini gateway master	13,10,13,100331
Waktu advertisement pertama gateway backup 1	13:18:46.589516
Waktu peralihan	3.402985 (detik)

Kemudian *interface* CARP melakukan ARP, untuk mengetahui alamat MAC baru dari alamat IP 10.0.0.1, yaitu alamat *virtual* CARP, yang juga alamat *default gateway* dari *client*. Paket data kemudian menunjukkan transaksi dari *client* menuju alamat IP BCA, mendownload file Naruto, dan Yahoo Mesenger berlanjut. **†cpdump** diakiri dengan keterangan detail yaitu :

- 60771 packets captured berarti saat perintah tcpdump dihentikan, terdapat 60771 paket data yang berhasil dicatat oleh tcpdump.
- o 106 packets received by filter berarti saat perintah
   tcpdump dihentikan, terdapat 106 paket data yang sesuai dengan
   parameter yang diberikan pada tcpdump.
- 0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

• Tcpdump di Komputer *gateway backup 1* NIC 0, terhubung dengan 11.0.0.0/24

# tcpdump -i vic0

listening on vic0, link-type EN10MB

13:16:00.990244 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:01.818378 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:02.686923 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:03.786601 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:04.777715 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:05.772114 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:06.716454 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:13.287080 11.0.0.2.63198 > 68.180.217.29.5050: P 1:34(33) ack 1 win 65340 (DF) 13:16:13.667078 68.180.217.29.5050 > 11.0.0.2.63198: P 1:106(105) ack 34 win 65535 13:16:13.692680 11.0.0.2.50377 > 66.163.169.186.https: S 1482567984:1482567984(0) win 64240 <mss 1460, nop, nop, sackOK> (DF) 13:16:14.167574 11.0.0.2.50377 > 66.163.169.186.https: P 1:71(70) ack 1 win 65340 (DF) 13:16:14.517339 66.163.169.186.https > 11.0.0.2.50377: P 1:825(824) ack 71 win 65535 13:16:16.984734 11.0.0.2.59083 > 202.162.208.99.domain: 64668+ A? ibank.klikbca.com. (35) 13:16:17.466186 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:17.476237 202.162.208.99.domain > 11.0.0.2.59083: 64668 1/5/5 A 202.6.211.9 (239) (DF) 13:16:17.481595 11.0.0.2.50474 > 202.6.211.9.https: S 3834791029:3834791029(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:16:17.457100 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:17.476250 202.162.208.99.domain > 11.0.0.2.1074: 64668 1/5/5 A 202.6.211.9 (239) (DF) 13:16:17.481606 11.0.0.2.1187 > 202.6.211.9.https: S 3834791029:3834791029(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:16:41.192802 11.0.0.2.1074 > 202.162.208.99.domain: 37260+ A? www.narutofan.com. (35)

# BRAWIJAY/

13:16:41.338823 202.162.208.99.domain > 11.0.0.2.1074: 37260 6/4/4 A 213.133.113.131,[domain] 13:16:41.576418 11.0.0.2.2153 > 213.133.113.131.www: S 203271031:203271031(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:16:41.708189 213.133.113.131.www > 11.0.0.2.2153: S 859042028:859042028(0) ack 203271032 win 65535 <mss 1460, nop, nop, sackOK> 13:16:41.709131 11.0.0.2.2153 > 213.133.113.131.www: . ack 1 win 64240 (DF) 13:16:41.839237 11.0.0.2.2153 > 213.133.113.131.www: P 1:814(813) ack 1 win 64240 (DF) 13:18:43.186531 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0 demote=0 (DF) [tos 0x10] 13:16:43.524101 11.0.0.2.1074 > 202.162.208.99.domain: 30350+ A? ftp1.download.narutofan.com. (45) 13:16:44.279749 202.162.208.99.domain > 11.0.0.2.1074: 30350 1/4/4 (209) 13:16:46.017713 11.0.0.2.2155 > 66.90.101.237.www: P 1:830(829) ack 1 win 64240 (DF) 13:16:46.591099 66.90.101.237.www > 11.0.0.2.2155: . ack 830 win 65535 13:17:53.810908 11.0.0.2.2244 > 202.162.208.99.domain: 47099+ A? ftp2.download.narutofan.com. (45) 13:17:53.822228 202.162.208.99.domain > 11.0.0.2.1099: 2301 1/2/1 A[|doma 13:17:52.409618 192.168.199.254.domain > 11.0.0.2.2250: 13542 1/4/3 (193) 13:17:54.428806 11.0.0.2.2259 > 67.159.45.121.www: S 3618338161:3618338161(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)in] 13:18:46.589516 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:18:46.589605 arp who-has 11.0.0.1 tell 11.0.0.1 13:18:48.050398 11.0.0.3.2713 > 67.159.45.121.www: S 4038249587:4038249587(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:18:48.055986 67.159.45.121.www > 11.0.0.3.2712: S 753882405:753882405(0) ack 292071058 win 65535 <mss 1460, nop, nop, sackOK> 13:18:48.709097 11.0.0.3.2717 > 66.90.101.237.www: S 3921961004:3921961004(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:18:48.715568 66.90.101.237.www > 11.0.0.3.2717: S

13:19:28.773720 202.6.211.9.https > 11.0.0.3.2962: . ack 167 win 32602

2655997530:2655997530(0) ack 3921961005 win 65535 <mss

1460, nop, nop, sackOK>

# BRAWIJAY/

13:19:28.793922 11.0.0.3.2962 > 202.6.211.9.https: . ack 1 win 64860
(DF)
13:19:32.073254 11.0.0.3.2146 > 68.180.217.29.5050: P 2783:2816(33) ack
15106 win 64626 (DF)
60771 packets captured
106 packets received by filter
0 packets dropped by kernel

Gambar 6.8 Hasil †cpdump Paket Data pada *Interface Network* 11.0.0.0/24 Komputer *Gateway Backup* 1 pada Pengujian Sistem *Fail-over redundancy* 

Dari hasil tcpdump, dapat diketahui bahwa awal koneksi, terdapat paket advertisement dari gateway master, yang menunjukkan bahwa gateway master masih aktif bekerja. Hal ini ditunjukkan dengan advertisement, dengan nilai advskew=0. Nilai vhid=2 menujukkan tcpdump dilakukan pada interface network 11.0.0.0/24. Sama dengan hasil tcpdump di interface network 10.0.0.0/24, advertisement dilakukan setiap 1 detik. Kemudian terjadi autentifikasi dari Yahoo Messenger untuk melakukan login user, saat user valid, maka aplikasi akan membuka port https. Yang dilanjutkan pengiriman data dari server Yahoo Messenger ke alamat IP client. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ibank.klikbca.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ibank.klikbca.com memiliki alamat IP 202.6.211.9, setelah sebelumnya terdapat paket advertisement gateway master. Kemudian terdapat paket data dari IP 11.0.0.2 menuju IP 202.6.211.9 dengan port https (443), yang diawali tree-way handshaking. Paket data dengan alamat 11.0.0.2 sebenarnya adalah paket data dari komputer client dengan alamat IP 10.0.0.100, yang telah mengalami perubahan header dalam proses NAT. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat www.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa www.narutofan.com. memiliki alamat IP 213.133.113.131. Lalu kemudian terdapat paket data dari IP 11.0.0.2 menuju IP 213.133.113.131, yang diawali tree-way handshaking. Paket data kemudian adalah proses GET download file naruto\_452.zip dimana halaman menuju link ftp1.download.narutofan.com. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan

alamat IP 202.162.208.99, untuk meresolve alamat ftp1.download.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftpl.download.narutofan.com .memiliki alamat IP 66.90.101.237. Kemudian komunikasi data terjadi antara client dengan alamat IP 66.90.101.237. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ftp2.download.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftp2.download.narutofan.com memiliki alamat IP 67.159.45.121. Kemudian komunikasi data terjadi antara client dengan alamat IP 67.159.45.121. Transaksi data berlanjut, sampai komputer gateway master dimatikan/dinonaktifkan, yang ditunjukkan dengan advertisement yang dilakukan komputer gateway backup 1. Advertisement ini dilakukan oleh gateway backup 1, ditunjukkan dengan nilai adskew=100, yang merupakan nilai konfigurasi CARP di komputer gateway backup 1. Kemudian interface CARP melakukan ARP, untuk mengetahui alamat MAC baru dari alamat IP 11.0.0.1, yaitu alamat virtual CARP, yang juga alamat default gateway dari client. Paket data kemudian menunjukkan transaksi dari client menuju alamat IP BCA, mendownload file Naruto, dan Yahoo Mesenger berlanjut. **†cpdump** diakiri dengan keterangan detail yaitu :

- o 60771 packets captured berarti saat perintah tcpdump dihentikan, terdapat 60771 paket data yang berhasil dicatat oleh tcpdump.
- o 106 packets received by filter berarti saat perintah **tcpdump** dihentikan, terdapat 106 paket data yang sesuai dengan parameter yang diberikan pada **tcpdump**.
- 0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

• Tcpdump di Komputer *gateway backup* 1 NIC 3, terhubung dengan 15.0.0.0/24

# tcpdump -i vic3

listening on vic3, link-type EN10MB
13:18:43.182376 15.0.0.2: INS ST: (DF) [tos 0x10]
13:18:43.182424 15.0.0.2: UPD ST COMP: (DF) [tos 0x10]
13:18:43.182457 15.0.0.2: UPD ST COMP: (DF) [tos 0x10]
13:18:43.182479 15.0.0.2: UPD ST COMP: (DF) [tos 0x10]
13:18:43.182493 15.0.0.2: UPD ST COMP: (DF) [tos 0x10]
13:18:47.764170 15.0.0.3: INS ST: (DF) [tos 0x10]
13:18:48.048618 15.0.0.3: UPD ST COMP: (DF) [tos 0x10]
13:18:48.055880 15.0.0.3: UPD ST COMP: (DF) [tos 0x10]
13:18:48.168475 15.0.0.3: UPD ST COMP: (DF) [tos 0x10]
13:18:48.177031 15.0.0.3: UPD ST COMP: (DF) [tos 0x10]
10 packets captured
106 packets received by filter
0 packets dropped by kernel

# Gambar 6.9 Hasil †cpdump Paket Data pada Interface Network 15.0.0.0/24 Komputer *Gateway Backup* 1 pada Pengujian Sistem *Fail-over redundancy*

Merupakan paket data *pfsync*, yang melakukan update state firewall. Dari gambar diatas, saat komputer *gateway master* masih aktif semua aliran data yang tersimpan dalam *table state firewall* akan di update dari *gateway master* ke *firewall gateway backup* 1. Kemudian saat *gateway master tidak aktif, gateway Backup* 1 akan berganti mengirimkan *state table firewall* ke *gateway backup* 2.

tcpdump diakiri dengan keterangan detail yaitu :

- o 10 packets captured berarti saat perintah **tcpdump** dihentikan, terdapat 10 paket data yang berhasil dicatat oleh **tcpdump**.
- 106 packets received by filter berarti saat perintah
   tcpdump dihentikan, terdapat 106 paket data yang sesuai dengan parameter yang diberikan pada tcpdump.
- 0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

Tabel State Firewall dari pfsync dapat di tampilkan dengan perintah pfctl –s state. Output dari perintah tersebut adalah :
all	tcp	10.0.0.100:1954	->	11.0.0.2:58609	->	202.6.211.9:443
EST.	ABLISH	HED:ESTABLISHEI				BRADA
all	tcp	10.0.0.100:2146	->	11.0.0.2:63198	->	68.180.217.29:5050
EST.	ABLISH	HED:ESTABLISHEI	)			SCITA2.K
all	tcp	10.0.0.100:2163	->	11.0.0.2:57330	->	67.195.134.213:80
EST.	ABLISH	HED:ESTABLISHEI	)		UN	NHTUE!
all	tcp	10.0.0.100:2166	->	11.0.0.2:58634	->	68.142.233.167:443
CLO	SING:E	ESTABLISHED				<b>UAU</b>
all	tcp	10.0.0.100:2168	->	11.0.0.2:64830	->	66.196.106.31:80
EST	ABLISH	HED:ESTABLISHE		AS RE		
all	tcp	10.0.0.100:2717	->	11.0.0.3:62789	->	66.90.101.237:80
CLO	SING:E	ESTABLISHED				
all	tcp	10.0.0.100:2733	->	11.0.0.3:51921	->	67.159.45.121:80
CLO	SING:E	ESTABLISHED		a contraction of the second		
all	tcp	10.0.0.100:2951	5	11.0.0.3:59612	~>	208.117.252.38:80
EST	ABLISH	HED:ESTABLISHEI				9

Gambar 6.10 State yang Terbentuk Selama Sesi Koneksi

Dalam Gambar 6.11 diperlihatkan bahwa alamat www.klikbca.com berhasil dibuka dengan menggunakan Firefox, kemudian melakukan login. Hal ini disebabkan karena bila menggunakan session, session yang digunakan tersimpan di webserver BCA, dan session mengenali alamat IP client, sebagai alamat IP NAT, yang tidak berubah saat salah satu gateway tidak aktif. Sementara bila web menggunakan cookies, cookies tetap tersimpan di komputer client tanpa ada perubahan, karena alamat IP komputer *client* tidak mengalami perubahan. Gambar 6.12 adalah tampilan setelah gateway master tidak aktif, dimana komputer client tetap bisa melanjutkan kegiatan browsing Internet. Hal ini mungkin terjadi bila kegiatan *browsing* lanjutan dilakukan setelah  $\pm$  3,5 detik setelah *gateway master* tidak aktif, yaitu saat gateway backup 1 telah bekerja. 3,5 detik adalah waktu yang dibutuhkan gateway backup 1 untuk dapat aktif bekerja. Gambar 6.13 memperlihatkan proses download dari www.narutofan.com. Gambar 6.14 memperlihatkan gagalnya proses download saat gateway master dimatikan. Hal ini disebabkan tanpa download manager, download tidak akan melakukan reconecting bila mengalami kegagalan koneksi. Gambar 6.15 memperlihatkan

proses download dari situs www.narutofan.com menggunakan download manager. Download manager memiliki fungsi reconecting bila terjadi kegagalan koneksi. Gambar 6.16 memperlihatkan kegagalan proses koneksi, ditunjukkan dengan "time out" dan "error ocured", yang disebabkan dimatikannya gateway master. Flashget melakukan reconecting dalam waktu 7 detik. Gambar 6.16 juga memperlihatkan proses download kembali berjalan, ditunjukkan dengan "connected", ketika koneksi telah dialihkan ke gateway backup 1. Gambar 6.17 menampilkan hasil traceroute awal saat gateway master aktif. Ditunjukkan proses traceroute ke yahoo.com melalui 10.0.0.2 alamat IP gateway master, kemudian menuju ke 11.0.0.100 alamat IP ISP 1, kemudian keluar ke Internet. Gambar 6.18 menampilkan hasil traceroute sesaat setelah gateway master tidak aktif. Ditunjukkan proses traceroute ke yahoo.com melalui 10.0.0.3 alamat IP gateway *backup* 1, kemudian menuju ke 11.0.0.100 alamat IP ISP 1, kemudian keluar ke Internet. Gambar 6.19 menampilkan saat Yahoo Messenger aktif. 6.20 menampilkan Yahoo Messenger yang mengalami kegagalan koneksi saat gateway master tidak aktif, kemudian melakukan reconnecting saat koneksi berhasil dialihkan ke gateway backup 1.



saat *Gateway Master* aktif.



Gambar 6.13 Download Tanpa Menggunakan Download Manager



Gambar 6.14 Kegagalan *Download* Tanpa Menggunakan *Download Manager* terjadi Saat *Gateway Master Down* 

New Start Pause	Tools Help     K     Del Prop. Up Down	Open Dir, Opt, Hor	Software	Enter Ke	y Words	_ (
FlashGet	- Name	Size Completed	Percent	Elapsed	Left Sr	peed
Downloaded	Naruto Chapter 432 [	3.91 M 400.67 KB	10%	00:00:50	00:07:40 7	.81K
	Graph Log Jet 1 Jet 2 Jet 2 Jet 3 Jet 4 Jet 5 Jet 6	Date  Mon Apr 27 16:26:37 2	Information Date: Mon, 27 Apr 2009 I Server: Apache/2 Last-Modified: Wed, 11 M ETag: "518031-38e811b-4 Accept-Ranges: bytes Content-Length: 409705 Content-Length: 409705 Content-Type: application X-Cache: MISS from prox X-Cache-Lookup: MISS fr	09:27:48 GMT 1ar 2009 04:34 64d063d94080 1 n/zip y.mmtsystem om proxy.mmt:	:58 GMT )" com system.com:3128	





Gambar 6.17 Traceroute Yahoo.com dalam Kondisi Normal

C:\Do	cumer	nts	and Se	etti	ngs\u	ser>	tracert yahoo.com
raci	ng re	oute	to ya	ahoo	.com	[209	.191.93.53]
ver	a ma:	kimu	m of 3	30 h	ops:		
1	2	ms	<1	ms	<1	ms	10-0-3
2	25	ms	<1	ms	<1	ms	11.0.0.100
3	<1	me	(1	ms	21	ms	202 134 1 1
4	*	11.5	*	113	*	11.5	Request timed out
5	6	ms	4	ms	6	ms	172.16.100.1
6	10	ms	4	ms	4	ms	10.10.0.1
ž	49	ms	47	ms	13	ms	1.subnet125-164-112.sneedy.telkom.net.id [125.1
1.112	.11						
8	27	ms	54	ms	60	ms	PE-ML-HUAWEI.telkom.net.id [125.160.1.33]
9	×		×		×		Request timed out.
10	100	ms	80	ms	*		203.208.190.17
11	113	ms	77	ms	70	ms	ae0-100.sngtp-dr1.ix.singtel.com [203.208.183.1
11							
12	98	ms	×		60	ms	xe-1-0-0-0.sngtp-cr1.ix.singtel.com [203.208.18
.61]							이가는 것은 것은 것은 것이가 있었다. 관련 것이 있다. 이가 있는 것은 것이 가지 않는 소란 것이 가지 않는 것이 가지 않는 것이 있다. 
13	138	ms	394	ms	216	ms	so-3-0-2-0.plapx-cr2.ix.singtel.com [203.208.18
1301							
14	245	ms	221	ms	204	ms	ge-6-0-0-0.plapx-dr2.ix.singtel.com [203.208.18
.166]							
15	252	ms	209	ms	258	ms	203.208.145.130
16	559	ms	233	ms	236	ms	as-0.pat2.dnx.yahoo.com [216.115.101.129]
17	414	ms	×		285	ms	as-3.pat1.dax.yahoo.com [216.115.96.59]
18	×		497	ms	×		te-8-1.bas-c2.mud.yahoo.com [68.142.193.7]
19	491	ms	392	ms	557	ms	ae2-p101.msr1.mud.yahoo.com [216.115.104.107]
20	428	ms	287	ms	306	ms	b1.www.vip.mud.yahoo.com [209.191.93.53]

Trace complete.

Gambar 6.18 Traceroute Yahoo.com saat Gateway Master tidak aktif

essenger Contacts			
uwie18	*		11
share a stati	us message	h	*
SOOKS ARE			1
type some contact	informatio	on	
B9ugUg Tewtawa	ng Tewan	nanaw	····· 🔺
🧝 😑 Bgugug Tawa	ana Supu!!		
biology (7)			
翼 😑 abdul hakim			
😇 😑 DIANA IRAW.	AN - 🧧 I'm i	nobile	
🌉 🕓 Dwi Wahyu Si	ndriati - Idle		
🙂 😑 Muhammad P	ahlevi - 📔 I	'm mobi	ile
腠 😑 oktavera02ul	6		
🙂 😑 sabreina putr	ri - 📔 I'm ma	bile	
🙂 😑 segara.ilmu -	📔 I'm mobii	'e	
bussines (1)			- 34
🙂 😑 Ini Pulsaku			
chat room (1)			
🌆 😑 Ar wen			
Friends (5)			
<u>   O</u> cs ini pulsaku	- Grosir Pu	lsa Elek	æ
🌺 😑 Diana Cahyai	wati		
😇 😑 febria anita -	📔 I'm mobii	le	
<u>द्धि</u> 😑 Ross ie			
Mener (			
Add a Contact	Plug	g-ins	^
TION I			-

Gambar 6.19 Yahoo Messenger dalam kondisi aktif

<b>ZAHOO! MESSENGER</b> essenger Help	() _ (

Signing in as uwie18 (Invisible to Everyone)

### Gambar 6.20 Yahoo Messenger disconect dan mencoba kembali terkoneksi

### g. Kesimpulan

Paket data yang berasal dari *internal network*, yaitu paket data yang berasal dari IP 10.0.0.100 dapat diteruskan dengan baik oleh sistem *gateway redundancy* menuju ke *external network*, baik saat komputer *gateway master* bekerja/aktif maupun saat komputer gateway *master* tidak aktif. *Advertisement* CARP dilakukan setiap 1 detik. Peralihan tugas *gateway master* ke *gateway backup* 1 memerlukan waktu ± 3,5 detik. Kegiatan *browsing* dapat tetap berjalan lancar (tidak mengalami *error*), bila dilakukan setelah 3,5 detik *gateway master* tidak aktif. *Downloading* akan mengalami *error* bila dilakukan tanpa bantuan *download manager*, *namun* bila dilakukan dengan menggunakan *download manager*, detik.

AWIJAL

Traceroute dapat menunjukkan perpindahan koneksi *gateway* yang digunakan, antara sebelum *gateway master* tidak aktif, dan setelah *gateway master* tidak aktif. Yahoo Messenger terputus saat *gateway master* tidak aktif, namun dapat otomatis melakukan *reconecting*.

## 6.4 Pengujian dan Analisis Sistem *Gateway Redundancy* saat *Gateway Master dan Gateway Backup* 2 Gagal Bekerja

Pengujian dan analisis sistem pada tahap ini, dititikberatkan pada peran komputer gateway Backup 2 dalam melakukan gateway fail-over, ketika komputer Gateway Master dan Gateway Backup 1 down/tidak aktif. Langkah-langkah pengujian adalah sebagai berikut :

a. Tujuan

Pengujian ini dilakukan untuk mengetahui apakah paket data yang berasal dari internal network dapat diteruskan oleh sistem gateway fail-over menuju external network walaupun Gateway Master dan Gateway Backup 1 gagal bekerja/tidak aktif.

### b. Spesifikasi dan Konfigurasi Komputer

Komputer *client*, komputer *gateway*, serta komputer ISP memiliki spesifikasi sebagaimana yang telah disebutkan di bagian awal bab ini. Komputer *client*, komputer *gateway*, serta komputer ISP telah dikonfigurasi sebagaimana telah dijelaskan pada Bab Empat dan Bab Lima.

c. Software Aplikasi

- 🐼 Mozilla Firefox 3 / Internet Explorer
- R Flash Get Download Manager
- 😪 Yahoo Messenger
- ca tcpdump 3.9.4 /wireshark 0.99.4
- R traceroute / tracert

### d. Prosedur Pengujian

Menjalankan perintah tepdump pada komputer gateway backup 2, yaitu pada NIC yang terhubung dengan network 10.0.0/24, 11.0.0.0/24, 15.0.0.0/24 untuk melihat aliran data didalamnya.





3 Perintah tepdump dilakukan di komputer gateway *backup* 2, yaitu di masing *network interface* yang terhubung dengan ketiga *network*, 10.0.0/24, 11.0.0.0/24, 15.0.0.0/24. berfungsi untuk melihat paket data dari/menuju IP 10.0.0.100 menuju/dari alamat IP <u>www.klikbca.com</u>, <u>www.narutofan.com</u> serta Yahoo Messenger, adalah sebagai berikut :

Di Komputer gateway backup 2 network 10.0.0.0/24

# tcpdump -i vic2 -w r2dump10 &

Perintah diatas memilki arti jalankan perintah tepdump pada *interface vic2* Di Komputer *gateway backup 2 network* 11.0.0.0/24

# tcpdump -i vic0 -w r2dump11 &

Perintah diatas memilki arti jalankan perintah tepdump pada *interface vic0* Di Komputer *gateway backup 2 network* 15.0.0.0/24

# tcpdump -i vic3 -w r2dump15 &

Perintah diatas memilki arti jalankan perintah tepdump pada interface vic3

- ii. Memastikan komputer gateway master telah tidak bekerja / non aktif
- iii. Menjalankan Firefox yang ada di komputer client.

### → Start | All Program | Mozilla Firefox | Mozilla Firefox

- iv. Membuka situs <u>www.klikbca.com</u> dengan Web browser, melakukan *login* dan transaksi.
- v. Melakukan download ke situs <u>www.narutofan.com</u>
  - a. Tanpa menggunakan download manager.
  - b. Menggunakan download manager.
- vi. Menggunakan Yahoo Messenger untuk melakukan chating.
- vii. Melakukan traceroute untuk mengetahui jalur yang digunakan.
- viii. Mematikan / menonaktifkan Komputer Gateway Backup 1
- ix. Melanjutkan mengakses situs <u>www.klikbca.com</u>, mendownload dari situs <u>www.narutofan.com</u>, dan menggunakan Yahoo Messenger.
- x. Melakukan traceroute untuk mengetahui jalur baru yang kini digunakan.

### e. Hasil Yang Diharapkan

Hasil yang diharapkan dari pengujian ini adalah *Web browser* di komputer *client* dapat menampilkan situs <u>www.klikbca.com</u>, melakukan download ke situs <u>www.narutofan.com</u>, chating menggunakan Yahoo Messenger, bisa dilakukan pada saat *Gateway Backup 1* masih bekerja/aktif, maupun pada saat *Gateway Backup 1* berhenti bekerja/tidak aktif. Program traceroute menampilkan jalur yang berbeda saat *gateway master* aktif dan tidak aktif.

### f. Hasil Pengujian dan Analisis

Saat komputer *client* menjalankan prosedur pengujian (menjalankan Web browser, melakukan download, menggunakan Yahoo Messenger) tcpdump yg sedang berjalan di komputer *gateway backup 2*, akan merekam paket data yang mengalir antara komputer *client* dengan Internet. Hasil dari tcpdump adalah sebagai berikut :

• Tcpdump di Komputer *gateway backup* 2 NIC vic2, terhubung dengan 10.0.0/24

```
# tcpdump -i vic2
listening on vic2, link-type EN10MB
```

13:49:41.818370 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:42.686925 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:43.786600 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] win 65340 (DF) 34 win 65535

13:49:44.777710 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:45.772110 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:46.716454 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:47.828556 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:48.830745 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:49.939888 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:49:53.287092 10.0.0.100.2146 > 68.180.217.29.5050: P 1:34(33) ack 1 13:49:53.667205 68.180.217.29.5050 > 10.0.0.100.2146: P 1:106(105) ack 13:49:53.692519 10.0.0.100.2147 > 66.163.169.186.https: S 1482567984:1482567984(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:49:58.357755 68.180.217.29.5050 > 10.0.0.100.2146: P 14392:14448(56) ack 927 win 65535 (DF) 13:49:59.347891 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=100 (DF) [tos 0x10] 13:49:59.984750 10.0.0.100.1074 > 202.162.208.99.domain: 64668+ A? ibank.klikbca.com. (35) 13:50:21.457100 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:50:21.476250 202.162.208.99.domain > 10.0.0.100.1074: 64668 1/5/5 A 202.6.211.9 (239) (DF) 13:50:21.481606 10.0.0.100.1187 > 202.6.211.9.https: S 3834791029:3834791029(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:50:41.192802 10.0.0.100.1074 > 202.162.208.99.domain: 37260+ A? www.narutofan.com. (35) 13:50:41.338823 202.162.208.99.domain > 10.0.0.100.1074: 37260 6/4/4 A 213.133.113.131,[|domain]

13:49:40.990200 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100

demote=0 (DF) [tos 0x10]

13:50:41.576418 10.0.0.100.2153 > 213.133.113.131.www: S 203271031:203271031(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:50:41.708189 213.133.113.131.www > 10.0.0.100.2153: S 859042028:859042028(0) ack 203271032 win 65535 <mss 1460, nop, nop, sackOK> 13:50:41.709131 10.0.0.100.2153 > 213.133.113.131.www: . ack 1 win 64240 (DF) 13:50:41.839237 10.0.0.100.2153 > 213.133.113.131.www: P 1:814(813) ack 1 win 64240 (DF) 13:50:43.524101 10.0.0.100.1074 > 202.162.208.99.domain: 30350+ A? ftpl.download.narutofan.com. (45) 13:50:44.279749 202.162.208.99.domain > 10.0.0.100.1074: 30350 1/4/4 (209) 13:50:46.017713 10.0.0.100.2155 > 66.90.101.237.www: P 1:830(829) ack win 64240 (DF) 13:50:46.591099 66.90.101.237.www > 10.0.0.100.2155: . ack 830 win 65535 13:50:53.810908 10.0.0.100.2244 > 202.162.208.99.domain: 47099+ A? ftp2.download.narutofan.com. (45) 13:50:53.822228 202.162.208.99.domain > 10.0.0.100.1099: 2301 1/2/1 A[|doma 13:50:52.409618 192.168.199.254.domain > 10.0.0.100.2250: 13542 1/4/3 (193) 13:50:54.428806 10.0.0.100.2259 > 67.159.45.121.www: S 3618338161:3618338161(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)in] 13:51:48.050398 10.0.0.100.2713 > 67.159.45.121.www: S 4038249587:4038249587(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:51:48.055986 67.159.45.121.www > 10.0.0.100.2712: S 753882405:753882405(0) ack 292071058 win 65535 <mss 1460, nop, nop, sackOK> 13:51:48.709097 10.0.0.100.2717 > 66.90.101.237.www: S 3921961004:3921961004(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:51:48.715568 66.90.101.237.www > 10.0.0.100.2717: S 2655997530:2655997530(0) ack 3921961005 win 65535 <mss 1460, nop, nop, sackOK> 13:52:26.494078 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:52:28.773720 202.6.211.9.https > 10.0.0.100.2962: . ack 167 win 32602 13:52:28.793922 10.0.0.100.2962 > 202.6.211.9.https: . ack 1 win 64860 (DF)

13:52:30.289664 CARPv2-advertise 36: vhid=1 advbase=1 advskew=200
demote=0 (DF) [tos 0x10]

13:52:30.289859 arp who-has 10.0.0.1 tell 10.0.0.1

13:52:30.293533 fe80::1 > ff02::1: icmp6: neighbor adv: tgt is fe80::200:5eff:fe00:101 13:52:30.525587 10.0.0.100.3598 > 66.90.101.237.www: F 392:392(0) ack 430 win 63812 (DF) 13:52:30.695641 10.0.0.100.3649 > 66.90.101.237.www: S 1078110789:1078110789(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:52:30.701477 66.90.101.237.www > 10.0.0.100.3649: S 4134807367:4134807367(0) ack 1078110790 win 65535 <mss 1460, nop, nop, sackOK> 13:52:30.702234 10.0.0.100.3649 > 66.90.101.237.www: . ack 1 win 64240 (DF) 13:52:30.705697 10.0.0.100.3650 > 66.90.101.237.www: S 2048160348:2048160348(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:52:30.713324 66.90.101.237.www > 10.0.0.100.3650: S 3771614142:3771614142(0) ack 2048160349 win 65535 <mss 1460, nop, nop, sackOK> 13:52:32.073254 10.0.0.100.2146 > 68.180.217.29.5050: P 2783:2816(33) ack 15106 win 64626 (DF) 60771 packets captured 106 packets received by filter 0 packets dropped by kernel

Gambar 6.22 Hasil †cpdump Paket Data pada Interface Network 10.0.0.0/24 Komputer *Gateway Backup* 2 pada Pengujian Sistem *fail-over redundancy* 

Dari hasil tcpdump, dapat diketahui bahwa awal koneksi, terdapat paket advertisement dari *gateway backup 1*, yang menunjukkan bahwa *gateway backup 1* masih aktif bekerja. Hal ini diperlihatkan dengan paket yang memiliki advskew=100 yang merupakan konfigurasi CARP pada *gateway backup 1*. Vhid=1 menunjukkan bahwa tcpdump dilakukan di *interface* yang terhubung dengan *network* 10.0.0.0/24. Advertisement dilakukan dalam selang waktu 1 detik, seperti ditunjukkan pada tabel 6.3

Waktu Advertisement	Selisih Waktu
13:49:40.990200	0.82817
13:49:41.818370	0.868555
13:49:42.686925	1.099675
13:49:43.786600	0.991111
13:49:44.777710	0.994
13:49:45.772110	
STAN PATRIA	7815.11
Rata-rata	0.9563022

Tabel 6.3 Waktu advertisement CARP backup 1

Kemudian terjadi autentifikasi dari Yahoo Messenger untuk melakukan login user, saat user valid, maka aplikasi akan membuka port https. Yang dilanjutkan pengiriman data dari server Yahoo Messenger ke alamat IP client. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ibank.klikbca.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ibank.klikbca.com memiliki alamat IP 202.6.211.9, setelah sebelumnya terdapat paket advertisement gateway backup 1. Kemudian terdapat paket data dari IP 10.0.0.100 menuju IP 202.6.211.9 dengan port https (443), yang diawali treeway handshaking. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat www.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan www.narutofan.com.memiliki alamat IP 213.133.113.131. bahwa Lalu kemudian terdapat paket data dari IP 10.0.0.100 menuju IP 213.133.113.131, yang diawali tree-way handshaking. Paket data kemudian adalah proses GET download file naruto\_452.zip dimana halaman menuju link ftp1.download.narutofan.com. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ftpl.download.narutofan.com. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ftp2.download.narutofan.com. Paket data selanjutnya adalah dari DNS Server, memberitahukan bahwa jawaban yang ftp2.download.narutofan.com memiliki alamat IP 67.159.45.121. Kemudian komunikasi data terjadi antara client dengan alamat IP 67.159.45.121. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa <u>ftpl.download.narutofan.com</u> .memiliki alamat IP 66.90.101.237. Kemudian komunikasi data terjadi antara client dengan alamat IP 66.90.101.237. *Advertisement* terakhir dari *gateway backup* 1 terjadi sebelum komputer *backup* 1 tidak aktif. Paket data berikutnya adalah transaksi data antara alamat 202.6.211.9 dengan 10.0.0.100, menggunakan *port* https, yang merupakan transaksi data dengan klikbca.com. Transaksi data berlanjut, sampai komputer *gateway backup 1* dimatikan/dinonaktifkan, yang ditunjukkan dengan *advertisement* yang dilakukan komputer *gateway backup* 2 pada 13:52:26.494078 Komputer backup 2 melakukan *advertisement* dengan selang waktu  $\pm$  3.795781 setelah komputer backup 1 tidak aktif yaitu pada 13:52:30.289664 seperti yang ditunjukkan pada tabel 6.4

<b>T-1-1</b>	A XX7 - 1-4	<b>D I</b> <sup>2</sup> <b>I</b>	<b>C</b>	<b>D 1</b>		-
I anel 6 a	1 wyakin	Perannan		KACKI	nı-Kackun	1.
THEFT OF	I II ansu	I VI aman	Juichuy	Duchu	pr Duchap	-
			~			

Waktu advertisement terakhir gateway backup 1	13:52:26.494078
Waktu advertisement pertama gateway backup 2	13:52:30.289664
Waktu peralihan	3.795781 (detik)

Kemudian *interface* CARP melakukan ARP, untuk mengetahui alamat MAC baru dari alamat IP 10.0.0.1, yaitu alamat *virtual* CARP, yang juga alamat *default gateway* dari *client*. Paket data kemudian menunjukkan transaksi dari *client* menuju alamat IP BCA, mendownload file Naruto, dan Yahoo Mesenger berlanjut. **†cpdump** diakiri dengan keterangan detail yaitu :

- o 60771 packets captured berarti saat perintah tcpdump dihentikan, terdapat 60771 paket data yang berhasil dicatat oleh tcpdump.
- o 106 packets received by filter berarti saat perintah
   tcpdump dihentikan, terdapat 106 paket data yang sesuai dengan
   parameter yang diberikan pada tcpdump.
- 0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

• Tcpdump di Komputer *gateway backup* 2 NIC 0, terhubung dengan 11.0.0.0/24

# tcpdump -i vic0

listening on vic0, link-type EN10MB

13:49:40.990200 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:41.818370 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100
demote=0 (DF) [tos 0x10]

13:49:42.686925 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:43.786600 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:44.777710 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:45.772110 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:46.716454 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:47.828556 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:48.830745 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:49.939888 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:49:53.287092 11.0.0.3.2146 > 68.180.217.29.5050: P 1:34(33) ack 1 win 65340 (DF)

13:49:53.667205 68.180.217.29.5050 > 11.0.0.3.2146: P 1:106(105) ack 34 win 65535

13:49:53.692519 11.0.0.3.2147 > 66.163.169.186.https: S 1482567984:1482567984(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)

13:49:58.357755 68.180.217.29.5050 > 11.0.0.3.2146: P 14392:14448(56) ack 927 win 65535 (DF)

13:49:59.347891 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=100 (DF) [tos 0x10]

13:49:59.984750 11.0.0.3.1074 > 202.162.208.99.domain: 64668+ A? ibank.klikbca.com. (35)

13:50:21.457100 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10]

13:50:21.476250 202.162.208.99.domain > 11.0.0.3.1074: 64668 1/5/5 A 202.6.211.9 (239) (DF)

13:50:21.481606 11.0.0.3.1187 > 202.6.211.9.https: S 3834791029:3834791029(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:50:41.338823 202.162.208.99.domain > 11.0.0.3.1074: 37260 6/4/4 A 213.133.113.131,[domain] 13:50:41.576418 11.0.0.3.2153 > 213.133.113.131.www: S 203271031:203271031(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:50:41.708189 213.133.113.131.www > 11.0.0.3.2153: S 859042028:859042028(0) ack 203271032 win 65535 <mss 1460, nop, nop, sackOK> 13:50:41.709131 11.0.0.3.2153 > 213.133.113.131.www: . ack 1 win 64240 (DF) 13:50:41.839237 11.0.0.3.2153 > 213.133.113.131.www: P 1:814(813) ack 1 win 64240 (DF) 13:50:43.524101 11.0.0.3.1074 > 202.162.208.99.domain: 30350+ A? ftpl.download.narutofan.com. (45) 13:50:44.279749 202.162.208.99.domain > 11.0.0.3.1074: 30350 1/4/4 (209) 13:50:46.017713 11.0.0.3.2155 > 66.90.101.237.www: P 1:830(829) ack 1 win 64240 (DF) 13:50:46.591099 66.90.101.237.www > 11.0.0.3.2155: . ack 830 win 65535 13:50:53.810908 11.0.0.3.2244 > 202.162.208.99.domain: 47099+ A? ftp2.download.narutofan.com. (45) 13:50:53.822228 202.162.208.99.domain > 11.0.0.3.1099: 2301 1/2/1 A[|doma 13:50:52.409618 192.168.199.254.domain > 11.0.0.3.2250: 13542 1/4/3 (193) 13:50:54.428806 11.0.0.3.2259 > 67.159.45.121.www: S 3618338161:3618338161(0) win 64240 <mss 1460, nop, nop, sackOK> (DF)in] 13:51:48.050398 11.0.0.3.2713 > 67.159.45.121.www: S 4038249587:4038249587(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:51:48.055986 67.159.45.121.www > 11.0.0.3.2712: S 753882405:753882405(0) ack 292071058 win 65535 <mss 1460, nop, nop, sackOK> 13:51:48.709097 11.0.0.3.2717 > 66.90.101.237.www: S 3921961004:3921961004(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:51:48.715568 66.90.101.237.www > 11.0.0.3.2717: S 2655997530:2655997530(0) ack 3921961005 win 65535 <mss 1460, nop, nop, sackOK> 13:52:26.494078 CARPv2-advertise 36: vhid=2 advbase=1 advskew=100 demote=0 (DF) [tos 0x10] 13:52:28.773720 202.6.211.9.https > 11.0.0.3.2962: . ack 167 win 32602 13:52:28.793922 11.0.0.3.2962 > 202.6.211.9.https: . ack 1 win 64860

13:50:41.192802 11.0.0.3.1074 > 202.162.208.99.domain: 37260+ A?

www.narutofan.com. (35)

(DF)

13:52:30.289664 CARPv2-advertise 36: vhid=2 advbase=1 advskew=200 demote=0 (DF) [tos 0x10] 13:52:30.289859 arp who-has 11.0.0.1 tell 11.0.0.1 13:52:30.293533 fe80::1 > ff02::1: icmp6: neighbor adv: tgt is fe80::200:5eff:fe00:101 13:52:30.525587 11.0.0.4.3598 > 66.90.101.237.www: F 392:392(0) ack 430 win 63812 (DF) 13:52:30.695641 11.0.0.4.3649 > 66.90.101.237.www: S 1078110789:1078110789(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:52:30.701477 66.90.101.237.www > 11.0.0.4.3649: S 4134807367:4134807367(0) ack 1078110790 win 65535 <mss 1460, nop, nop, sackOK> 13:52:30.702234 11.0.0.4.3649 > 66.90.101.237.www: . ack 1 win 64240 (DF) 13:52:30.705697 11.0.0.4.3650 > 66.90.101.237.www: S 2048160348:2048160348(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:52:30.713324 66.90.101.237.www > 11.0.0.4.3650: S 3771614142:3771614142(0) ack 2048160349 win 65535 <mss 1460, nop, nop, sackOK> 13:52:32.073254 11.0.0.4.2146 > 68.180.217.29.5050: P 2783:2816(33) ack 15106 win 64626 (DF) 60771 packets captured 106 packets received by filter 0 packets dropped by kernel

## Gambar 6.23 Hasil †cpdump Paket Data pada Interface Network 11.0.0.0/24 Komputer Gateway Backup 2 pada Pengujian Sistem gateway fail-over

Dari hasil tcpdump, dapat diketahui bahwa awal koneksi, terdapat paket *advertisement* dari *gateway backup 1*, yang menunjukkan bahwa *gateway backup 1* masih aktif bekerja. Hal ini ditunjukan dengan nilai advskew=100 yang merupakan konfigurasi CARP *gateway backup 1*. Vhid=2 menunjukkan bahwa tcpdump dilakukan pada *interface network 11.0.0.0/24*. Kemudian terjadi autentifikasi dari Yahoo Messenger untuk melakukan login user, saat user valid, maka aplikasi akan membuka port https.Yang dilanjutkan pengiriman data dari server Yahoo Messenger ke alamat IP client. Kemudian terdapat standart query DNS menuju DNS *Server*, dengan alamat IP 202.162.208.99, untuk *meresolve* alamat ibank.klikbca.com. Paket data selanjutnya adalah jawaban dari DNS *Server*, yang memberitahukan bahwa ibank.klikbca.com memiliki alamat IP 202.6.211.9, setelah sebelumnya terdapat paket *advertisement gateway master*.

Kemudian terdapat paket data dari IP 11.0.0.3 menuju IP 202.6.211.9 dengan port https (443), yang diawali tree-way handshaking. Paket data dengan alamat 11.0.0.3 sebenarnya adalah paket data dari komputer client dengan alamat IP 10.0.0.100, yang telah mengalami perubahan header dalam proses NAT. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat www.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa www.narutofan.com. memiliki alamat IP 213.133.113.131. Lalu kemudian terdapat paket data dari IP 11.0.0.3 menuju IP 213.133.113.131, yang diawali tree-way handshaking. Paket data kemudian adalah proses GET download file naruto\_452.zip dimana halaman menuju link ftp1.download.narutofan.com. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan IP alamat 202.162.208.99. untuk meresolve alamat ftpl.download.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftpl.download.narutofan.com .memiliki alamat IP 66.90.101.237. Kemudian komunikasi data terjadi antara client dengan alamat IP 66.90.101.237. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ftp2.download.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftp2.download.narutofan.com memiliki alamat IP 67.159.45.121. Kemudian komunikasi data terjadi antara client dengan alamat IP 67.159.45.121. Transaksi data berlanjut, sampai komputer gateway backup 1 dimatikan/dinonaktifkan, yang ditunjukkan dengan advertisement yang dilakukan komputer gateway backup 2. Kemudian interface CARP melakukan ARP, untuk mengetahui alamat MAC baru dari alamat IP 11.0.0.1, yaitu alamat virtual CARP, yang juga alamat default gateway dari client. Paket data kemudian menunjukkan transaksi dari client menuju alamat IP BCA, mendownload file Naruto, dan Yahoo Mesenger berlanjut. tcpdump diakiri dengan keterangan detail yaitu :

 60771 packets captured berarti saat perintah tcpdump dihentikan, terdapat 60771 paket data yang berhasil dicatat oleh tcpdump.

- o 106 packets received by filter berarti saat perintah
   tcpdump dihentikan, terdapat 106 paket data yang sesuai dengan parameter yang diberikan pada tcpdump.
- 0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

• Tcpdump di Komputer *gateway backup* 2 NIC 3, terhubung dengan 15.0.0.0/24

RAWIJA # tcpdump -i vic3 listening on vic3, link-type EN10MB 13:49:46.078552 15.0.0.3: INS ST: (DF) [tos 0x10] 13:49:46.082696 15.0.0.3: UPD ST COMP: (DF) [tos 0x10] 13:49:46.398643 15.0.0.3: UPD ST COMP: (DF) [tos 0x10] 13:49:46.429487 15.0.0.3: UPD ST COMP: (DF) [tos 0x10] 13:49:47.260079 15.0.0.3: UPD ST COMP: (DF) [tos 0x10] 13:49:47.260622 15.0.0.4: INS ST: (DF) [tos 0x10] 13:49:47.260626 15.0.0.4: UPD ST COMP: (DF) [tos 0x10] 13:49:47.271418 15.0.0.4: UPD ST COMP: (DF) [tos 0x10] 13:49:47.315558 15.0.0.4: UPD ST COMP: (DF) [tos 0x10] 13:49:47.329720 15.0.0.4: UPD ST COMP: (DF) [tos 0x10] 10 packets captured 106 packets received by filter 0 packets dropped by kernel

Gambar 6.24 Hasil †cpdump Paket Data pada Interface Network 15.0.0.0/24 Komputer *Gateway Backup 2* pada Pengujian Sistem gateway *fail-over* 

Merupakan paket data *pfsync*, yang melakukan update state firewall. Dari gambar diatas, saat komputer *gateway backup 1* masih aktif semua aliran data yang tersimpan dalam *table state firewall* akan di update dari *gateway backup 1* ke *firewall gateway backup 2*. Kemudian saat *gateway backup 1 tidak aktif*, *gateway backup 2* akan tetap mengirimkan *state table firewall* jaringan dengan cara *multicast*.

tcpdump diakiri dengan keterangan detail yaitu :

- o 10 packets captured berarti saat perintah tcpdump dihentikan,
   terdapat 10 paket data yang berhasil dicatat oleh tcpdump.
- o 106 packets received by filter berarti saat perintah
   tcpdump dihentikan, terdapat 106 paket data yang sesuai dengan parameter yang diberikan pada tcpdump.
- o 0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

Tabel State Firewall dari pfsync dapat di tampilkan dengan perintah pfctl –s state. Output dari perintah tersebut adalah :

all	tcp	10.0.0.100:1954		11.0.0.3:58609	->	202.6.211.9:443
EST	ABLISH	IED:ESTABLISHED			Λ	
all	tcp	10.0.0.100:2146	->>	11.0.0.3:63198	->	68.180.217.29:5050
EST	ABLISH	IED:ESTABLISHEE			35	3
all	tcp	10.0.0.100:2163	->	11.0.0.3:57330	-> (	67.195.134.213:80
EST	ABLISH	IED:ESTABLISHED	123		$\sim$	2
all	tcp	10.0.0.100:2166	37	11.0.0.3:58634	->_>	68.142.233.167:443
CLO	SING:E	STABLISHED	<b>]</b>  /.			
all	tcp	10.0.0.100:2168	->	11.0.0.3:64830	7->	66.196.106.31:80
EST.	ABLISH	IED:ESTABLISHED	Ĕ.			
all	tcp	10.0.0.100:2717	->	11.0.0.4:62789	->	66.90.101.237:80
CLO	SING:E	STABLISHED				
all	tcp	10.0.0.100:2733	->	11.0.0.4:51921	->	67.159.45.121:80
CLO	SING:E	STABLISHED				
all	tcp	10.0.0.100:2951	->	11.0.0.4:59612	->	208.117.252.38:80
EST.	ABLISH	IED:ESTABLISHED	)			

Gambar 6.25 State yang Terbentuk Selama Sesi Koneksi

Dalam Gambar 6.26 diperlihatkan bahwa alamat <u>www.klikbca.com</u> berhasil dibuka dengan menggunakan Firefox, kemudian melakukan *login*. Hal ini disebabkan karena bila menggunakan *session*, *session* yang digunakan tersimpan di *webserver* BCA, dan *session* mengenali alamat IP *client*, sebagai alamat IP NAT, yang tidak berubah saat salah satu *gateway* tidak aktif. Sementara bila *web*  menggunakan cookies, cookies tetap tersimpan di komputer client tanpa ada perubahan, karena alamat IP komputer *client* tidak mengalami perubahan. Gambar 6.27 adalah tampilan setelah gateway backup 1 tidak aktif, dimana komputer *client* tetap bisa melanjutkan kegiatan *browsing* Internet. Hal ini mungkin terjadi bila kegiatan browsing lanjutan dilakukan setelah  $\pm$  3,8 detik setelah gateway master tidak aktif, yaitu saat gateway backup 1 telah bekerja. 3,8 detik adalah waktu yang dibutuhkan gateway backup 1 untuk dapat aktif bekerja. Gambar 6.28 memperlihatkan proses download dari www.narutofan.com. Gambar 6.29 memperlihatkan gagalnya proses download saat gateway backup 1 dimatikan. Hal ini disebabkan tanpa download manager, download tidak akan melakukan reconecting bila mengalami kegagalan koneksi. Gambar 6.30 memperlihatkan proses download dari situs www.narutofan.com menggunakan download manager. Download manager memiliki fungsi reconecting bila terjadi kegagalan koneksi. Gambar 6.31 memperlihatkan kegagalan proses koneksi, ditunjukkan dengan "time out" dan "error ocured", yang disebabkan dimatikannya gateway backup 1. Flashget melakukan reconecting dalam waktu 7 detik. Gambar 6.31 juga memperlihatkan proses download kembali berjalan, ditunjukkan dengan "connected", ketika koneksi telah dialihkan ke gateway backup 2 Gambar 6.32 menampilkan hasil traceroute awal saat gateway backup 1 aktif. Ditunjukkan proses traceroute ke yahoo.com melalui 10.0.0.3 alamat IP gateway backup 1, kemudian menuju ke 11.0.0.100 alamat IP ISP 1, kemudian keluar ke Internet. Gambar 6.33 menampilkan hasil traceroute sesaat setelah gateway backup 1 tidak aktif. Ditunjukkan proses traceroute ke yahoo.com melalui 10.0.0.4 alamat IP gateway backup 2, kemudian menuju ke 11.0.0.100 alamat IP ISP 1, kemudian keluar ke Internet. Gambar 6.34 menampilkan saat Yahoo Messenger aktif. 6.35 menampilkan Yahoo Messenger yang mengalami kegagalan koneksi saat gateway backup 1 tidak aktif, kemudian melakukan reconnecting saat koneksi berhasil dialihkan ke gateway backup 2.



Gambar 6.27 Firefox menampilkan situs <u>www.klikbca.com</u> saat Gateway Backup 1 tidak aktif

NarutoFan > Your #1 Naruto Anim	e and Manna Desouved - Multimedia - Manna Volume (1, To (5 - Microsoft Totaviat Evolusia	
	Help	
🌀 Back 👻 🐑 👻 🛃 🏠	- Search 🔆 Favorites 🧭 🔗 🖌 🌺 🔜	
Address Address http://www.narutofan.com/n	nultimedia/manga%20volume%2041%20to%2045 🗾 🔁 😡	Links »
AVG - powered by YAHOO! s	EARCH 💌 Search 🔹 🛉 🌒 Active Surf-Shield   🕵 Search-Shield   🗟 AVG Info 👻 Get More	
Y?	🔍 🔨 Web Search 🖪 🖌 🔯 Mail 🐼 My Yahoo! 🖾 Answers	
🕒 NarutoFan > Your #1 Naruto A	4% of naruto_445.zip Completed	×
Ivaruto manga Chapter 455		
Naruto Manga Chapter 436		_
Naruto Manga Chapter 437		
Naruto Manga Chapter 438		
Naruto Manga Chapter 439	Saving:	
Naruto Manga Chapter 440	naruto_445.zip from 67.18.204.30	
Naruto Manga Chapter 441		
Naruto Manga Chapter 442	Estimated time left 11 min 50 sec (78.4 KB of 2.15 MB copied)	
Naruto Manga Chapter 443	Download to: C:\asdw\naruto 445.zip	
Naruto Manga Chapter 444	Transfer rate: 3.06 KB/Sec	
Naruto Manga Chapter 445	Close this dialog box when download completes	
<< Naruto Manga Volumes 36 to	→>	
	Open Open Folder Cancel	

0% of n	aruto_444.zip Completed	<u>-0 ×</u>
3		
Micros	soft Internet Explorer	×
	Internet Explorer cannot download r s07.naruto.download.anifreak.com.	naruto_444.zip from
Г	The connection with the server was	2000 C
1		reset
î Î	ССК	reset

Gambar 6.29 Kegagalan *Download* Tanpa Menggunakan *Download Manager* terjadi Saat *Gateway Backup 1* tidak aktif



Gambar 6.31 *Download* menggunakan Flash Get *Download Manager* saat *Gateway Backup 1* tidak aktif

C:\Do	cumer	nts	and Se	etti	ings/us	ser)	tracert yahoo.com
Traci	ng re	oute	to y	ahoo	.com	[209	.191.93.53]
over	a max	kimu	Im of :	30 ł	iops:		
1	2	ms	<1	ms	<1	ms	10.0.3
2	25	ms	<1	ms	<1	ms	11.0.0.100
3	<1	ms	<1	ms	<1	ms	202.134.1.1
4	×		×		×		Request timed out.
5	6	ms	4	ms	6	ms	172.16.100.1
6	10	ms	4	ms	4	ms	10.10.0.1
7	49	ms	47	ms	13	ms	1.subnet125-164-112.speedy.telkom.net.id [125.1]
4.112	.1]						
8 N	27	ms	54	ms	60	ms	PE-ML-HUAWEI.telkom.net.id [125.160.1.33]
2	*		*		*		Request timed out.
10	140	ms	80	ms	70		
	113	ms	"	ms	70	ms	aeo-100.sngtp-ari.ix.singtei.com 1203.208.183.1
12	98	ms	×		60	ms	xe-1-0-0-0.sngtp-cr1.ix.singtel.com [203.208.18]
.611	100	-	204		946	-	
1301	130	1115	374	ms	210	шs	SU-5-0-2-0.prapx-cr2.ix.Singter.com 1205.200.10
14	245	ms	221	ms	204	ms	ge-6-0-0-0.plapx-dr2.ix.singtel.com [203.208.18]
.1661	252	me	200	me	25.9	me	203 208 145 130
16	550	me	222	me	236	me	as-0 pat2 dox waboo com [216 115 101 129]
17	414	ms	*	11.5	285	ms	$a_{s-3}$ nati day value com [216,115,96,59]
18	*	1.10	497	ms	*		te-8-1.has-c2.mud.vahoo.com [68.142.193.7]
19	491	ms	392	ms	557	ms	ae2-p101.msr1.mud.vahoo.com [216.115.104.107]
20	428	ms	287	ms	306	ms	b1.www.vip.mud.yahoo.com [209.191.93.53]
Trace	com	olet	e.				
		1	Gamb	ar 6	.32 Tr	acer	oute Yahoo.com dalam Kondisi Normal
C • N Do	cumer	ate	and S	otti	ngelus		thacent ushoo com
0- 100	ounor	100	una o.		ingo		stabil yandi bon
Traci	ng re	oute	to ya	ahoo	.com	[209	.191.93.53]
over	a max	kimu	um of 3	30 }	iops:		
1	1	ms	<1	ms	2	ms	10.0.0.4
2	1	ms	<1	ms	<1	ms	11.0.0.100
3	1	ms	<1	ms	<1	ms	202.134.1.1
4	×		*		*		Request timed out.
5	8	ms	15	ms	15	ms	172.16.100.1
6	346	ms	3	ms	3	ms	
1 110	316	ms	41	ms	127	ms	1.subnet125-164-112.speedy.telkom.net.id 1125.10
4.112	-11	me	20	me	24	me	PE-MI-HUQUEI telkom pet id [125 160 1 22]
0	-10	115	20	115	34	115	IL HU HONWEL.CEIKUM.HEC.IU [IZ3.100.1.33]

\* 101 79 ae0-100.sngtp-dr1.ix.singtel.com [203.208.183.19 73 ms 74 ms 71 ms xe-1-0-0-0.sngtp-cr1.ix.singtel.com [203.208.183 203 ms 287 ms 212 ms so-3-0-2-0.plapx-cr2.ix.singtel.com [203.208.182 236 ms 258 272 ms ge-6-0-0-0.plapx-dr2.ix.singtel.com [203.208.183 ms

Request timed out. 203.208.190.17

217 ms 298 ms 359 ms 267 ms 239 ms 203.208.145.162 as-0.pat2.dnx.yahoo.com [216.115.101.129] as-3.pat1.dax.yahoo.com [216.115.96.59] te-9-1.bas-c1.mud.yahoo.com [68.142.193.9] b1.www.vip.mud.yahoo.com [209.191.93.53] 214 286 238 312 364 148 296 247 278 291 ms ms MS MS MS ms Ms Ms 17 18 19 ms ms

Trace complete

75 74 ms ms

ms ms

Gambar 6.33 Traceroute Yahoo.com saat Gateway Backup 1 tidak aktif

	AS DESDAVILL
	YAHOO! MESSENGER . X
	Messenger Contacts Actions Helo
	chave a status messare
	sidre a status message
	V N type some contact information
	V B9ugUg Tewtawang Tewamanaw!!!!
	🧱 😑 Bgugug Tawana Supu!!
	▼ biology (7)
	🥰 😑 abdul hakim
	🕤 🔽 🧧 😑 DIANA IRAWAN - 🔋 I'm mobile
	🔍 🔛 🎆 🕓 Dwi Wahyu Indriati - Idle 👘 👘 👘
	🔄 😑 Muhammad Pahlevi - 🗐 I'm mobile
NIVEIER	se oktavera02ub
<b>MANUVERIE</b>	🔛 😑 sahraina nutri - 🗳 Em mohila
	seyara.iimu - 🛛 1 m mobile
AYEGAZ	V bussines (1)
	1 🔄 🤛 Ini Pulsaku
NUT I	▼ chat room (1)
	🚮 💛 Ar wen
	▼ Friends (5)
	🧧 🥯 cs ini pulsaku - Grosir Pulsa Elekt
	🥦 😑 Diana Cahyawati
	🔄 🥥 febria anita - 🕯 Em mobile
	💽 😑 Ross ie
205	
	+ Add a Contact
Ga	ambar 6.34 Yahoo Messenger dalam kondisi ak
GAN	
CAUVU.	
RAY ALL DESIGN	
TORAL ST	
D P P	
AN PA	
OS CH	
IVEN ED	
UNPERIOR	
NP.74 UPP.	
IN A P. TA UN	

AWIJAL



Signing in as uwie18 (Invisible to Everyone) Cancel

# Gambar 6.35 Yahoo Messenger disconect dan mencoba kembali terkoneksi

### g. Kesimpulan

Paket data yang berasal dari internal network, yaitu paket data yang berasal dari IP 10.0.0.100 dapat diteruskan dengan baik oleh sistem gateway fai-lover menuju ke external network, baik saat komputer gateway backup 1 bekerja/aktif maupun saat komputer gateway backup 2 tidak aktif. Advertisement CARP dilakukan setiap 1 detik. Peralihan tugas gateway master ke gateway backup 1 memerlukan waktu ± 3,8 detik. Kegiatan browsing dapat tetap berjalan lancar (tidak mengalami error), bila dilakukan setelah 3,8 detik gateway backup 1 tidak aktif. Downloading akan mengalami error bila dilakukan tanpa bantuan download manager, namun bila dilakukan dengan menggunakan download manager, download dapat berjalan hingga akhir, walaupun terjadi kegagalan sekitar 7 detik.

AWIJAL

Traceroute dapat menunjukkan perpindahan koneksi *gateway* yang digunakan, antara sebelum *gateway master* tidak aktif, dan setelah *gateway master* tidak aktif. Yahoo *Messenger* terputus saat *gateway master* tidak aktif, namun dapat otomatis melakukan *reconecting*.

# 6.5 Pengujian dan Analisis Sistem *Gateway Redundancy* dalam Mendeteksi Putusnya Koneksi ke ISP, dan Melakukan Peralihan Jalur.

Pengujian dan analisis sistem pada tahap ini, dititikberatkan pada peran sistem *gateway redundancy* dalam mendeteksi putusnya koneksi ke ISP 1 (ISP *fail-over*), dan melakukan peralihan jalur. Langkah-langkah pengujian adalah sebagai berikut :

### a. Tujuan

Pengujian ini dilakukan untuk mengetahui apakah paket data yang berasal dari *internal network* dapat diteruskan oleh sistem ISP *fail-over* menuju Internet walaupun ISP 1 gagal bekerja/tidak aktif.

### b. Spesifikasi dan Konfigurasi Komputer

Komputer *client*, komputer *gateway*, serta komputer ISP memiliki spesifikasi sebagaimana yang telah disebutkan di bagian awal bab ini, Komputer *client*, komputer *gateway*, serta komputer ISP telah dikonfigurasi sebagaimana telah dijelaskan pada Bab Empat dan Bab Lima.

### c. Software Aplikasi

- Mozilla Firefox 3 / Internet Explorer
- R Flash Get Download Manager
- ↔ Yahoo Messenger
- ce topdump 3.9.4 /wireshark 0.99.4

### d. Prosedur Pengujian

i. Menjalankan perintah tcpdump pada salah satu komputer *gateway*, dalam kasus ini pada komputer *gateway backup 2*, yaitu pada *NIC* yang terhubung dengan *network* 11.0.0.0/24, 12.0.0.0/24 untuk melihat aliran data didalamnya. 2 Perintah tcpdump dilakukan di komputer gateway *backup 2*, yaitu di masing-masing *network interface* yang terhubung dengan kedua *network*, 11.0.0.0/24, 12.0.0.0/24 berfungsi untuk melihat paket data

dari/menuju IP 10.0.0.100 menuju/dari alamat IP <u>www.klikbca.com</u>, <u>www.narutofan.com</u> serta Yahoo Messenger, adalah sebagai berikut :

Di Komputer gateway backup 2 network 11.0.0.0/24

# tcpdump -i vic0 -w r2dump10 &

Perintah diatas memilki arti jalankan perintah tepdump pada *interface vic2* Di Komputer *gateway backup 2 network* 12.0.0.0/24

# tcpdump -i vic1 -w r2dump11 &

Perintah diatas memilki arti jalankan perintah tepdump pada interface vic0

ii. Menjalankan Firefox yang ada di komputer client.

→ Start | All Program | Mozilla Firefox | Mozilla Firefox

- iii. Membuka situs <u>www.klikbca.com</u> dengan Web browser, melakukan *login* dan transaksi.
- iv. Melakukan download ke situs www.narutofan.com
  - c. Tanpa menggunakan download manager.
  - d. Menggunakan download manager.
- v. Menggunakan Yahoo Messenger untuk melakukan chating.
- vi. Melakukan traceroute untuk mengetahui jalur yang digunakan.
- vii. Mematikan / menonaktifkan Komputer ISP 1
- viii.Melanjutkan mengakses situs <u>www.klikbca.com</u>, mendownload dari situs <u>www.narutofan.com</u>, dan menggunakan Yahoo Messenger.
- ix. Melakukan traceroute untuk mengetahui jalur baru yang kini digunakan.

### e. Hasil Yang Diharapkan

Hasil yang diharapkan dari pengujian ini adalah *Web browser* di komputer *client* dapat menampilkan situs <u>www.klikbca.com</u>, melakukan download ke situs <u>www.narutofan.com</u>, chating menggunakan Yahoo Messenger, bisa dilakukan pada saat ISP 1 masih bekerja/aktif, maupun pada saat ISP 1 berhenti bekerja/tidak aktif. Program traceroute menampilkan jalur yang berbeda saat ISP *I* aktif dan tidak aktif.

### f. Hasil Pengujian dan Analisis

Saat komputer *client* menjalankan prosedur pengujian (menjalankan Web browser, melakukan download, menggunakan Yahoo Messenger) tcpdump yg sedang berjalan di komputer *gateway backup 2*, akan merekam paket data yang mengalir antara komputer *client* dengan Internet. Hasil dari tcpdump adalah sebagai berikut :

• Tcpdump di Komputer *gateway backup* 2 NIC vic0, terhubung dengan 11.0.0.0/24



13:47:17.481595 11.0.0.2.50474 > 202.6.211.9.https: S 3834791029:3834791029(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:47:17.476250 202.162.208.99.domain > 11.0.0.2.1074: 64668 1/5/5 A 202.6.211.9 (239) (DF) 13:47:17.481606 11.0.0.2.1187 > 202.6.211.9.https: S 3834791029:3834791029(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:47:41.192802 11.0.0.2.1074 > 202.162.208.99.domain: 37260+ A? www.narutofan.com. (35) 13:47:41.338823 202.162.208.99.domain > 11.0.0.2.1074: 37260 6/4/4 A 213.133.113.131,[|domain] 13:47:41.576418 11.0.0.2.2153 > 213.133.113.131.www: S 203271031:203271031(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 13:47:41.708189 213.133.113.131.www > 11.0.0.2.2153: S 859042028:859042028(0) ack 203271032 win 65535 <mss 1460, nop, nop, sackOK> 13:47:41.709131 11.0.0.2.2153 > 213.133.113.131.www: . ack 1 win 64240 (DF) 13:47:41.839237 11.0.0.2.2153 > 213.133.113.131.www: P 1:814(813) ack 1 win 64240 (DF) 13:47:43.524101 11.0.0.2.1074 > 202.162.208.99.domain: 30350+ A? ftpl.download.narutofan.com. (45) 13:47:44.279749 202.162.208.99.domain > 11.0.0.2.1074: 30350 1/4/4 (209)13:47:46.017713 11.0.0.2.2155 > 66.90.101.237.www: P 1:830(829) ack 1 win 64240 (DF) 13:47:16:46.591099 66.90.101.237.www > 11.0.0.2.2155: . ack 830 win 65535 13:48:53.810908 11.0.0.2.2244 > 202.162.208.99.domain: 47099+ A? ftp2.download.narutofan.com. (45) 13:48:53.822228 202.162.208.99.domain > 11.0.0.2.1099: 2301 1/2/1 A[doma 13:48:52.409618 192.168.199.254.domain > 11.0.0.2.2250: 13542 1/4/3 (193) 14:03:26.523632 11.0.0.2.63923 > 67.159.45.121.www: F 414:414(0) ack 500 win 63741 (DF) 14:03:26.529505 67.159.45.121.www > 11.0.0.2.63923: . ack 415 win 65535 14:03:33.480948 11.0.0.2 > 209.191.93.53: icmp: echo request 14:03:33.772163 11.0.0.4 > 11.0.0.100: icmp: echo request 14:03:33.872192 11.0.0.3 > 11.0.0.100: icmp: echo request 60771 packets captured 106 packets received by filter

### Gambar 6.36 Hasil †cpdump Paket Data pada Interface Network 11.0.0.0/24 Komputer *Gateway Backup* 2 pada Pengujian Sistem *ISP fail-over*

Dari hasil tcpdump, dapat diketahui bahwa pada awal koneksi, terdapat paket icmp request dan reply dari ketiga gateway, yang dilakukan oleh ifstated, digunakan untuk memeriksa kondisi aktif tidaknya ISP 1. Kemudian terjadi autentifikasi dari Yahoo Messenger, seperti yang juga terlihat di tcpdumptcpdump sebelumnya. untuk melakukan login user, saat user valid, maka aplikasi akan membuka *port* https. Yang dilanjutkan pengiriman data dari server Yahoo Messenger ke alamat IP client. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ibank.klikbca.com. Paket data selanjutnya adalah jawaban dari DNS Server, memberitahukan bahwa ibank.klikbca.com memiliki yang alamat IP 202.6.211.9. Kemudian terdapat paket data dari IP 11.0.0.2 menuju IP 202.6.211.9 dengan port https (443), yang diawali tree-way handshaking. Kemudian terdapat standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat www.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa www.narutofan.com.memiliki alamat IP 213.133.113.131. Lalu kemudian terdapat paket data dari IP 11.0.0.2 menuju IP 213.133.113.131, yang diawali tree-way handshaking. Paket data kemudian adalah proses GET download file naruto\_452.zip dimana halaman menuju link ftpl.download.narutofan.com. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan 202.162.208.99. IP untuk alamat meresolve alamat ftpl.download.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftpl.download.narutofan.com .memiliki alamat IP 66.90.101.237. Kemudian komunikasi data terjadi antara client dengan alamat IP 66.90.101.237. Paket data selanjutnya adalah standart query DNS menuju DNS Server, dengan alamat IP 202.162.208.99, untuk meresolve alamat ftp2.download.narutofan.com. Paket data selanjutnya adalah jawaban dari DNS Server, yang memberitahukan bahwa ftp2.download.narutofan.com memiliki alamat IP 67.159.45.121. Kemudian komunikasi data terjadi antara

client dengan alamat IP 67.159.45.121, yang merupakan transaksi data terakhir yang melalui ISP 1, yaitu pada 14:03:26.529505. Saat ISP 1 dimatikan/dinonaktifkan, ditunjukkan dengan tidak adanya reply dari ICMP request dari ketiga *gateway*, oleh ifstated default gateway dan CARP diubah ke network 12.0.0.0./24 dengan 12.0.0.100 sebagai default gateway. Transaksi data yang dapat di tampilkan oleh interface ini berhenti, dan dilanjutkan tcpdump pada interface vic1. **†cpdump** diakiri dengan keterangan detail yaitu :

o 60771 packets captured berarti saat perintah tcpdump dihentikan, terdapat 60771 paket data yang berhasil dicatat oleh tcpdump.

106 packets received by filter berarti saat perintah **tcpdump** dihentikan, terdapat 106 paket data yang sesuai dengan parameter yang diberikan pada **tcpdump**.

0

1460, nop, nop, sackOK>

0

0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

• Tcpdump di Komputer *gateway backup* 2 NIC 1, terhubung dengan 12.0.0/24

# tcpdump -i vic1 listening on vic0, link-type EN10MB 14:03:37.660960 12.0.0.2.55526 > 67.159.45.121.www: S 2512019584:2512019584(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 14:03:37.660968 12.0.0.2.60492 > 67.159.45.121.www: S 3616323649:3616323649(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 14:03:37.660973 12.0.0.2.55062 > 66.90.101.237.www: S 3468801478:3468801478(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 14:03:37.680854 12.0.0.2.61700 > 66.90.101.237.www: S 1536273984:1536273984(0) win 64240 <mss 1460,nop,nop,sackOK> (DF) 14:03:37.693673 arp who-has 12.0.0.2 tell 12.0.0.100 14:03:37.693685 arp reply 12.0.0.2 is-at 00:0c:29:eb:8e:c8 14:03:37.694626 67.159.45.121.www > 12.0.0.2.55526: S 609569083:609569083(0) ack 2512019585 win 65535 <mss 1460, nop, nop, sackOK> 14:03:37.761395 67.159.45.121.www > 12.0.0.2.60492: S 3712993210:3712993210(0) ack 3616323650 win 65535 <mss

```
14:03:37.761401 66.90.101.237.www > 12.0.0.2.55062: S
1948315101:1948315101(0) ack 3468801479 win 65535 <mss
1460, nop, nop, sackOK>
14:03:37.761406 66.90.101.237.www > 12.0.0.2.61700: S
3871736027:3871736027(0) ack 1536273985 win 65535 <mss
1460, nop, nop, sackOK>
14:03:37.773987 12.0.0.2.60030 > 67.159.45.121.www: S
617098502:617098502(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
14:03:37.790234 67.18.204.31.www > 12.0.0.2.64119: S
1446579855:1446579855(0) ack 253818933 win 65535 <mss
1460, nop, nop, sackOK>
14:03:37.963955 67.159.45.121.www > 12.0.0.2.60030: . ack 405 win 65535
14:03:37.973175 12.0.0.2.55474 > 67.159.45.121.www: S
978039054:978039054(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
14:03:37.991825 203.84.156.154.www > 12.0.0.2.60034: S
2885777245:2885777245(0) ack 3643998722 win 65535 <mss
1460, nop, nop, sackOK>
14:03:37.992638 12.0.0.2.60034 > 203.84.156.154.www: . ack 1 win 64240
(DF)
14:03:40.732225 CARPv2-advertise 36: vhid=2 advbase=1 advskew=0
demote=0 (DF) [tos 0x10]
14:03:59.287768 12.0.0.2.54270 > 202.6.211.9.https: S
2250199674:2250199674(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
14:03:59.450936 202.6.211.9.https > 12.0.0.2.54270: S
302046052:302046052(0) ack 2250199675 win 32768 <mss 1380>
60771 packets captured
106 packets received by filter
0 packets dropped by kernel
    Gambar 6.37 Hasil †cpdump Paket Data pada Interface Network 12.0.0.0/24
```

# Komputer *Gateway Backup* 2 pada Pengujian Sistem ISP *fail-over*

Dari hasil tepdump, dapat diketahui bahwa awal koneksi, terdapat koneksi data dari tanpa reply dari 12.0.0.2 menuju 67.159.45.121 dan 66.90.101.237. Kemudian terdapat paket ARP dari alamat IP 12.0.0.2 yang menanyakan pemilik alamat IP 12.0.0.100. Kemudian terdapat jawaban yang berisi alamat MAC dari 12.0.0.100 adalah 00:0c:29:59:07:9e. Terdapat delay antara reply terakhir melalui koneksi ISP 1 pada 14:03:26.529505 dengan beralihnya koneksi ke ISP 2 pada 14:03:37.694626, yaitu sekitar 11,165121 detik, seperti ditunjukkan pada tabel 6.5. Hal ini dipengaruhi dari konfigurasi *ifstated* yang melakukan pengecekan koneksi ISP 1 setiap 10 detik.

#### **Tabel 6.5 Selisih Reply**

Waktu reply terakhir melalui ISP 1	14:03:26.529505
Waktu reply pertama melalui ISP 2	14:03:37.694626
Selisih reply	11,165121 (detik)

Kemudian komunikasi data terjadi antara client dengan alamat IP 69.197.161.211, 67.159.45.121, 66.90.101.237, 202.6.211.9, yaitu paket data transaksi antara *client* menuju alamat IP BCA, mendownload file Naruto, dan Yahoo Mesenger berlanjut. **†cpdump** diakiri dengan keterangan detail yaitu :

- 60771 packets captured berarti saat perintah tcpdump dihentikan, terdapat 60771 paket data yang berhasil dicatat oleh tcpdump.
- o 106 packets received by filter berarti saat perintah
   tcpdump dihentikan, terdapat 106 paket data yang sesuai dengan
   parameter yang diberikan pada tcpdump.
- 0 packets dropped by kernel berarti tidak ada paket data yang terbuang akibat buffer penuh.

Dalam Gambar 6.38 diperlihatkan bahwa alamat www.klikbca.com berhasil dibuka dengan menggunakan Firefox, kemudian melakukan *login*. Hal ini disebabkan karena bila menggunakan *session, session* yang digunakan tersimpan di *webserver* BCA, dan *session* mengenali alamat IP *client*, sebagai alamat IP NAT, yang tidak berubah saat salah satu *gateway* tidak aktif. Sementara bila *web* menggunakan *cookies, cookies* tetap tersimpan di komputer *client* tanpa ada perubahan, karena alamat IP komputer *client* tidak mengalami perubahan. Gambar 6.39 adalah tampilan setelah ISP 1 tidak aktif, dimana komputer *client* tetap bisa melanjutkan kegiatan *browsing* Internet. Hal ini mungkin terjadi bila kegiatan browsing lanjutan dilakukan setelah ± 11.2 detik setelah ISP 1 tidak aktif, yaitu saat ISP 2 telah bekerja. 11.2 detik adalah waktu yang dibutuhkan ISP 2 untuk dapat aktif bekerja. Gambar 6.40 memperlihatkan gagalnya proses *download* saat ISP 1 dimatikan. Hal ini disebabkan tanpa *download manager, download* tidak akan melakukan *reconecting* bila mengalami kegagalan koneksi, namun
berbeda dengan kondisi tidak aktifnya gateway, tidak ada konfirmasi eror dalam kasus ini. Gambar 6.42 memperlihatkan proses download dari situs www.narutofan.com menggunakan download manager. Download manager memiliki fungsi reconecting bila terjadi kegagalan koneksi. Gambar 6.43 memperlihatkan kegagalan proses koneksi, ditunjukkan dengan "time out" dan "error ocured", yang disebabkan dimatikannya ISP 1. Flashget melakukan reconecting dalam waktu 12 detik. Gambar 6.43 juga memperlihatkan proses download kembali berjalan, ditunjukkan dengan "connected", ketika koneksi telah dialihkan ke ISP 2 Gambar 6.44 menampilkan hasil traceroute awal saat ISP 1 aktif. Ditunjukkan proses traceroute ke yahoo.com melalui 10.0.0.2 alamat IP gateway master, kemudian menuju ke 11.0.0.100 alamat IP ISP 1, kemudian keluar ke Internet. Gambar 6.45 menampilkan hasil traceroute sesaat setelah ISP 2 tidak aktif. Ditunjukkan proses traceroute ke yahoo.com melalui 10.0.0.2 alamat IP gateway master, kemudian menuju ke 12.0.0.100 alamat IP ISP 2, kemudian keluar ke Internet. Gambar 6.46 menampilkan saat Yahoo Messenger aktif. 6.47 menampilkan Yahoo Messenger yang mengalami kegagalan koneksi saat ISP 1 tidak aktif, kemudian melakukan reconnecting saat koneksi berhasil dialihkan ke ISP 2.



Gambar 6. 38 Firefox menampilkan situs <u>www.klikbca.com</u> saat ISP 1 aktif.



Gambar 6.40 Download Tanpa Menggunakan Download Manager

			<u> </u>
Saving:	67 40 004 00		
naruto_445.zip fro	om 67,18,204,30		
Estimated time left Download to: Transfer rate:	t 16 min 30 sec (2 C:\asdw\naruto 2:00 KB/Sec	13 KB of 2.15 ME _445.zip	copied)
Close this dialo	og box when dowr	load completes	

Gambar 6.41 Kegagalan Download Tanpa Menggunakan Download Manager terjadi

Saat ISP 1 Tidak aktif, namun tanpa konfirmasi eror.

New Start Pause	K Co Del Prop. Up D	Den Dir. Opt. Hon	Software	e 💌 Enter k	Key Words		
FlashGet Download Downloaded Deleted	Name       Naruto Chapter 432 [	Size Completed . 3.91 M 400.67 KB	Percent 10%	Elapsed	Left 00:07:40	Speed	
	Graph Log Jet Jet Jet 1 Jet 2 Jet 3 Jet 3 Jet 3 Jet 4 Jet 5 Jet 6	Date         Information                Mon Apr 27 16:26:37 2          Date: Mon, 27 Apr 2009 09:27:48 GMT                 Mon Apr 27 16:26:37 2          Server: Apache/2                 Mon Apr 27 16:26:37 2          Last-Modified: Wed, 11 Mar 2009 04:34:58 GMT                 Mon Apr 27 16:26:37 2          ETag: "518031-3e841b-464063d94080"                 Mon Apr 27 16:26:37 2          Accept-Ranges: bytes                 Mon Apr 27 16:26:37 2          Content-Length: 4097051					
		<ul> <li>Mon Apr 27 16:26:37 2</li> </ul>	<ul> <li>Mon Apr 27 16:26:37 2 Content-Type: application/zip</li> <li>Mon Apr 27 16:26:37 2 X-Cache: MISS from proxy.mmtsystem.com</li> <li>Mon Apr 27 16:26:37 2 X-Cache-Lookup: MISS from proxy.mmtsystem.com:3128</li> <li>Mon Apr 27 16:26:37 2 Via: 1.1 proxy.mmtsystem.com:3128 (square2.7.STABLE5)</li> <li>Mon Apr 27 16:26:37 2 Connection: close</li> <li>Mon Apr 27 16:26:37 2 Start Receiving Data!</li> </ul>				

Gambar 6.42 Download menggunakan Flash Get Download Manager



Gambar 6.44 Traceroute Yahoo.com dalam Kondisi Normal

C:\Do	cumer	nts a	and Se	etti	ngs\u	ser>	tracert yahoo.com
Traci over	ng ro a max	oute kimu	to ya n of 3	ahoo 30 }	.com lops:	[209	.191.93.53]
1	8	ms	<1	ms	<1	ms	10.0.2
2	40	ms	27	ms	1	ms	12.0.0.100
3	10	ms	1	ms	7	ms	202.134.1.1
4	×		×		×		Request timed out.
5	5	ms	3	ms	3	ms	172.16.100.1
6	12	ms	×		25	ms	10.10.0.1
7	25	ms	50	ms	48	ms	1.subnet125-164-112.speedy.telkom.net.id [125.16
4.112	.1]						
8	63	ms	74	ms	102	ms	PE-ML-HUAWEI.telkom.net.id [125.160.1.33]
. 9	×		×		×		Request timed out.
10	174	ms	73	ms	29	ms	203.208.190.17
11 4]	79	ms	121	ms	75	ms	ae0-100.sngtp-dr1.ix.singtel.com [203.208.183.19
12	85	ms	98	ms	101	ms	xe-1-0-0-0.sngtp-cr1.ix.singtel.com [203.208.183
13	223	ms	265	ms	229	MS	so-3-0-2-0.plapx-cr2.ix.singtel.com [203.208.182
14	218	ms	249	ms	279	MS	ge-6-0-0.plapx-dr2.ix.singtel.com [203.208.183
15	238	ms	262	ms	230	ms	203-208-145-162
16	247	ms	372	ms	493	ms	as-1.pat2.dax.vahoo.com [216.115.101.131]
17	425	ms	314	ms	358	ms	as-3.pat1.dax.vahoo.com [216.115.96.59]
18	342	ms	285	ms	264	ms	te-9-1.bas-c1.mud.yahoo.com [68.142.193.9]
19	353	ms	290	ms	426	ms	ae1-p111.msr2.mud.yahoo.com [216.115.104.103]
20	272	ms	305	ms	229	ms	te-8-1.bas-c2.mud.yahoo.com [68.142.193.7]
21	348	ms	317	ms	290	ms	b1.www.vip.mud.yahoo.com [209.191.93.53]
Tanaa		alat	2				

# Gambar 6.45 Traceroute Yahoo.com saat ISP 1 tidak aktif

KAHOO! lessenger Cr	, MESSE optacts	Actions	Help	
i ouv	wie18	+	.0	
share	e a statu	s message	B	•
BOOKS ARE		6		
type some c	ontact i	informati	on	E.
R0ualla Ter	utawan	a Toman		
	VI Tawar		lanaw	
biology (7)	sy / srra	, , , , , , , , , , , , , , , , , , ,		
💐 😑 abdul	hakim			
😇 😑 DIANI	A IRAWA	N - 🧃 I'm	mobile	
ang 🕓 Dwi W	Vahyu Ini	driati - Idi	e	=
😇 😑 Muhai	mmad Pa	hlevi - 🗐 🛛	r'm mob.	ile
腾 😑 oktav	era02ub			
🙂 😑 sabre	ina putri	- 📔 I'm me	obile	
🙂 😑 segar	a.ilmu -	] I'm mobi	le	
bussines (1	)			394
🙂 😑 Ini Pu	ilsaku			
chat room	(1)			
🚮 😑 Ar we	9 <b>7</b> 9			
Friends (5)				
🜔 🧿 🖉	pulsaku ·	- Grosir Pu	ilsa Elek	đ
🎇 😑 Diana	Cahyaw	ati		
🙂 😑 febria	anita -	I'm mobi	le	
📕 😑 Ross i	ie . ,			-
+ Add a Conta	act	Plu	g-ins	~
THOOL	-			

Gambar 6.46 Yahoo Messenger dalam kondisi aktif



## **BAB VII**

## PENUTUP

#### 7.1. Kesimpulan

Dari hasil pengujian dan analisis sistem *gateway redundancy* dengan menggunakan CARP, *ifstated*, dan *pfsync*, dapat disimpulkan bahwa :

- 1. Kegagalan koneksi Internet yang mempengaruhi Reliabilitas koneksi jaringan Internet, dapat diatasi dengan sistem Gateway Redundancy.
- 2. CARP dapat melakukan fail-over redundancy, yang berfungsi mengatasi kegagalan fungsi Gateway Internet. CARP melakukan advertisement setiap ± 1 detik. Waktu delay yang terjadi akibat perpindahan gateway master ke gateway backup 1 adalah ± 3,5 detik, perpindahan gateway backup 1 ke gateway backup 2 adalah ± 3,8 detik.
- Ifstated dapat mendeteksi putusnya koneksi ke ISP 1, dan mengalihkan koneksi ISP 2. Waktu delay perpindahan koneksi yang terjadi antara tidak aktifnya ISP 1 dan digantikan dengan ISP 2 adalah ± 11,2 detik, hal ini dipengaruhi oleh konfigurasi yang dilakukan di *ifstated*.
- 4. *Pfsync* dapat melakukan sinkronisasi *state table*, dari *gateway* satu ke *gateway* yang lain.

### 7.2. Saran

Saran yang dapat diberikan untuk pengembangan sistem ini adalah menyempurnakan sistem redundancy gateway menggunakan trunking, yaitu sistem yang menggunakan device/peralatan pendukung dalam jumlah ganda, seperti menggandakan power supply, LAN Card, serta Hardisk dengan metode RAID, untuk meningkatkan reliabilitas sistem.

Hal lain yang bisa di lakukan adalah menyempurnakan resource yang ada, yaitu menambahkan fitur Load balancing. Load balancing digunakan untuk mengoptimalkan resource bandwith dari ISP 2, yang bisa digunakan untuk meningkatkan transfer rate koneksi ke Internet.

- [ALM-01] Almesberger, Werner. 2001. Linux Networking Traffic Control -Implementation Overview. EPFL ICA.
- [ART-03] Artymiak Jacek, Building Firewalls with OpenBSD and PF, devGuide.net, 2003
- [CAL-02] Caldera International Inc. 2002. The TCP/IP protocol stack. Akses dari : <u>http://uw713doc.sco.com/en/NET\_tcpip/tcpN.tcpip\_stack.html</u>. Tanggal akses : 11 Oktober 2006
- [CON-05a] Conniq.com. 2005. Networking Guide : Network Topologies. Akses dari : <u>http://www.conniq.com/Networking\_Topology.htm</u>. Tanggal akses : 13 Oktober 2006
- [CON-05b] Conniq.com. 2005. Networking Guide : Network Topologies. Akses dari : http://www.conniq.com/Networking\_Topology3.htm. Tanggal akses : 13 Oktober 2006
- [COU-06] http://www.countersiege.com/doc/pfsync-carp/, Firewall Failover with pfsync and CARP. Tanggal akses: 17 Januari 2008
- [FLO-05]Florida Center for Instructional Technology College of Education. 2005.Chapter5:Topology.Aksesdari::

http://fcit.usf.edu/network/chap5/chap5.htm. Tanggal akses : 13 Oktober 2006[HAN-08]Hansteen, Peter N.M. THE BOOK OF PF, William Pollock, 2008

- [ISI-81a] Information Sciences Institute. 1981. RFC 793 Transmission Control Protocol. Akses dari : <u>http://www.networksorcery.com/enp/rfc/rfc793.txt</u>. Tanggal akses : 14 Mei 2007
- [ISI-81b] Information Sciences Institute. 1981. RFC 791 Internet Protocol. Akses dari : <u>http://www.networksorcery.com/enp/rfc/rfc793.txt</u>. Tanggal akses : 14 Mei 2007
- [JAV-01] http://www.javvin.com/telecomglossary/GatewayRedundancy.html, Gateway Redundancy. Tanggal akses : 10 Desember 2008
- [KEE-02] Cassen, Alexandre, Keepalived for LVS, Linux Virtual Server Opensource Project, 2002
- [LAM-08] Lamping. Ulf, Wireshark User's Guide, NS Computer Software and Services P/L, 2008.

[MAC-08]	http://www.countersiege.com/doc/pfsync-carp/, Firewall Failover with pfsync						
	and CARP, Tanggal akses : 10 Desember 2008						
[MAL-02]	Malhotra, Ravi. 2002. IP Routing. Sebastopol : O'Reilly & Associates, Inc.						
[MCB-04]	McBride, R, Interview: Ryan McBride, http://www.kerneltrap.com, 2004						
[MED-99]	Medhi, D., Network Reliability and Fault Tolerance, www.cstp.						
	umkc.edu/public/papers/dmedhi/m_jweee99.pdf, 1999						
[OPE-08a]	http://openbsd.org/faq/pf/carp.html, PF: Firewall Redundancy with CARP and						
	pfsync, Tanggal akses : 26 Desember 2008						
[OPE-08b]	http://www.openbsd.org/cgi-						
	bin/man.cgi?query=carp&sektion=4&arch=i386&apropos=0&manpath=Open						
TAY P	BSD+Current, OpenBSD Programmer's Manual, Tanggal akses : 27 Desember						
	2007						
[POS-80]	Postel, J. 1980. RFC 768 - User Datagram Protocol. Akses dari :						
	http://tools.ietf.org/html/rfc768. Tanggal akses : 14 Mei 2007						
[PUR-01]	Purbo, Onno W., et al., 2001. TCP/IP : Standar, Desain, dan Implementasi.						
	Jakarta : PT Elex Media Komputindo.						
[RAH-05]	Raharjo, Budi: Keamanan Sistem Informasi Berbasis Internet, PT Insan						
	Infonesia, Jakarta, 2005						
[RAM-08]	http://www.ramcomminc.com/glossary.asp, Glossary of Telecommunications						
	Terms, Tanggal akses : 10 Desember 2008						
[RES-08]	http://resin.csoft.net/cgi-bin/man.cgi?section=8&topic=ifstated, OpenBSD						
223	System Manager's Manual, Tanggal akses : 11 Desember 2008						
[STE-01]	Stevens W. Richard, TCP/IP Illustrated Volume 1 The Protocols, Addison-						
2451	Wesley Professional Computing Series, 1994						
[SUG-07]	Sugeng Purwantoro E.S.G.S. 2007. Konfigurasi Dasar PC-Router dengan						
	Windows 2003 Server. http://ilmukomputer.com/2007/03/03/konfigurasi-						
	dasar-pc-router-dengan-windows-2003-server/. Tanggal akses : 16 Agustus						
	2007						
[TOO-01]	http://tools.ietf.org/html/rfc3170, IP Multicast Applications: Challenges and						
	Solutions, Tanggal akses : 27 Desember 2008						
[THR-01]	http://threads.seas.gwu.edu/cgi-bin/man2web?program=pfsync&section=4,						
	FreeBSD Kernel Interfaces Manual, Tanggal akses : 27 Desember 2007						

135

[TAN-03]	Tanenbaum Andrew S., Computer Networks, Fourth Edition, Prentice Hall,							
	March 17, 2003							
[WIK-08]	http://en.wikipedia.org/wiki/Redundancy_(engineering), Tanggal akses : 10							
	Desember 2008							
[WIK-07a]	Wikipedia, Reliability Engineering. http://en.wikipedia.org/wiki/							
	Reliability_engineering, 2007							
[WIK-07b]	Wikipedia Gateway Telecomunications.							
	http://en.wikipedia.org/wiki/Gateway_%28telecommunications%29, 2007							

[WIK-07c] http://en.wikipedia.org/wiki/Failover, Failover, Tanggal akses : 16 Agustus 2007

H