E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402

Perancangan Dan Implementasi *Gateway Redundancy* Untuk Peningkatan *Reliabilitas* Jaringan Menggunakan Protokol CARP

Albert D. Lumingkewas(1), Arie S.M. Lumenta, ST., MT(2), Xaverius B.N. Najoan, ST., MT(3)
(1)Mahasiswa, (2)Pembimbing 1, (3)Pembimbing 2
E-Mail : danielkleak@yahoo.co.id(1),al@unsrat.ac.id(2),xnajoan@unsrat.ac.id(3)
Jurusan Teknik Elektro-FT. UNSRAT, Manado-95115

Abstrak

***Reliabilitas* suatu jaringan Internet merupakan hal yang harus dibutuhkan untuk menunjang fungsinya sebagai komponen sistem informasi. *Reliabilitas* jaringan mengacu pada ketersediaan layanan koneksi *Client* ke Internet dengan mengabaikan media penghubung seperti *hub, NIC,* serta kondisi jaringan diatas *router ISP*. Secara umum, *reliabilitas* dapat didefinisikan sebagai daya tahan suatu sistem terhadap kegagalan kerja**

Pada saat terjadi kegagalan layanan dari suatu *ISP,* peralihan koneksi ke ISP *beckup* dilakukan secara manual oleh *administrator* jaringan. Hal tersebut dapat menimbulkan kegagalan koneksi yang berdampak pada *reliabilitas* jaringan Internet, bila peralihan tidak terjadi secara cepat akan terjadi *router ISP.* Oleh karena itu, dibutuhkan suatu Perancangan dan implementasi *gateway redudancy* untuk peningkatan *rehabilitasi* jaringan menggunakan *protokol CARP*.

Dengan adanya Perancangan dan implementasi *gateway redudancy* untuk peningkatan *reliabilitas* jaringan menggunakan *protokol CARP* dapat mengatasi kegagalan layanan suatu jaringan internet

Kata Kunci : CARP, Gateway, ISP , Jaringan Internet , Reliabilitasi, *router*.

The reliability of a network the Internet is something that must be required to support its function as a component of the information system. Reliability refers to the availability of the service network client connection to the Internet by connecting media ignore such as Hub, NIC, and the condition of the network over the ISP router. In general, the reliability can be defined as the resistance of a system to fail action

In the event of a service failure of an ISP, the ISP connection to the transition beckup done manually by the network administrator. It can cause connection failures that impact on the reliability of the Internet network, if the transition does not happen quickly will happen ISP router. Therefore, it takes a design and implementation of gateway redundancy to increase network rehabilitation using CARP protocol.

With the design and implementation of gateway redundancy to increase network rehabilitation protocol using CARP can overcome the failure of an Internet network services

Keywords: CARP, Gateway, ISP, Internet Network, Reliabilitasi, router

I. PENDAHULUAN

Reliabilitas suatu jaringan Internet merupakan hal yang sangat dibutuhkan untuk menunjang fungsinya sebagai komponen sistem informasi[1]. Secara umum, *reliabilitas* dapat didefinisikan sebagai daya tahan suatu sistem terhadap kegagalan kerja[2].

Ketersediaan layanan *ISP* dan ketersediaan *gatewey* sebagai pintu masuk koneksi dapat menjadi faktor penentu *reliabilitas* suatu jaringan Internet. Pada saat terjadi kegagalan layanan dari suatu *ISP*, peralihan koneksi ke *ISP beckup* dilakukan secara manual oleh *administrator* jaringan. Hal tersebut dapat menimbulkan kegagalan koneksi yang berdampak pada *reliabilitas* jaringan Internet, bila peralihan tidak terjadi secara cepat akan terjadi *humanerror*. 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*[3].

Kegagalan ketersediaan *gateway* dapat diatasi dengan teknik *gateway failover*. Pada sistem *gateway failover*, saat *gateway master* mengalami kegagalan fungsi maka ia akan *dibackup* oleh *gateway backup*.

Berdasarkan latar belakang diatas penulis tertarik untuk merancang dan meneliti sistem *gateway redundancy* yang mampu mendeteksi kegagalan *gateway* serta melakukan *fail-over redundancy* dengan *gateway* cadangan serta Merancang sistem *gateway redundancy* yang mampu mendeteksi kegagalan koneksi *ISP* serta mengalihkan koneksi, sehingga *reliabilitas* jaringan dapat terjaga.

II. METODE PENELITIAN.

Jenis Penelitian yang dilakukan adalah penelitian laboratorium (*Laboratory-based research*), yang termasuk penelitian *kuantitatif* karena dalam pengumpulan data dilakuakan dengan cara *eksperimen*. Dalam pelaksanaan tugas akhir ini penulis mengambil tempat penelitian di Fakultas Teknik Universitas Sam Ratulangi dan di rumah punulis. Dengan waktu antara maret 2015 sampai dengan juni 2015. Dalam mengerjakan tugas akhir ini mulai dari merancang sampai pada tahap analisis penulis menggunakan perlengkapan komputer sebagai media untuk menjalankan program. Secara lebih spesifik perlengkapan komputer beserta pendukung yang digunakan yaitu spesifikasi Komputer *Client* yang terdiri dari Perangkat Keras yaitu *Processor Intel core 2 duo, Memory RAM 1 Gb, Harddisk 250 Gb* dan Nomor IP 192.168.50.60. Perangkat Lunak yaitu, Sistem Operasi *Windows XP*, *Nmap, Wireshark, Cmd*. Spesifikasi Komputer *Gateway* terdiri dari Perangkat Keras yaitu *Processor Intel core 2 duo, Memory RAM 512 Mb, Harddisk 80 Gb, LAN Card, TP-LINK 10/100Mbps PCI Network Adapter (TF-3200)* dan *USB LAN* atau *USB 2.0 Ethernet Adapter 10/100Mbps*

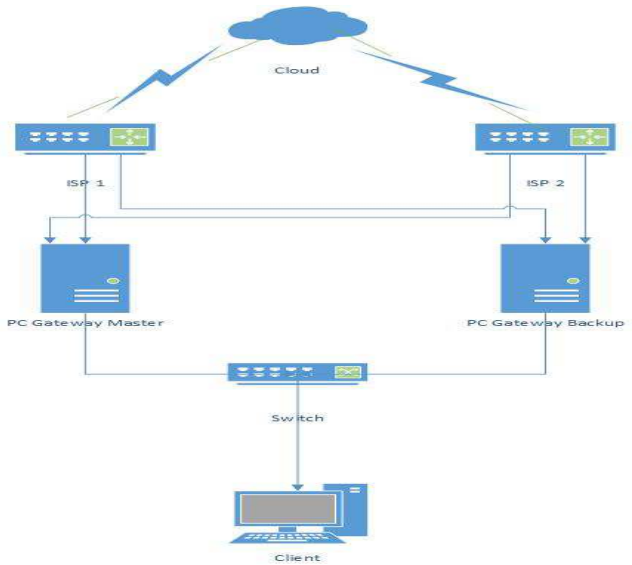
E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402

Perangkat *Lunak* yaiyu Sistem Operasi *Ubuntu 14.04, UCARP, Wireshark*. Spesifikasi Komputer *Gateway Backup* terdiri dari Perangkat Keras yaitu *Processor Intel Core 2 Duo, Memory RAM 512 Mb, Arddisk 80 Gb, USB LANUSB 2.0 Ethernet Adapter 10/100Mbps, LAN CARD, TP-LINK 10/100Mbps PCI Network adapter (TF-3200)*. Perangkat Lunak yaitu Sistem Operasi *Ubuntu 14.04, UCARP, Wireshark*. Perangkat Keras Lainnya adalah *Switch* dan Kabel *UTP*. Perangkat tersebut kemudian disusun sehingga membentuk sebuah jaringan komputer dengan *Topologi Star* seperti yang diperlihatkan dalam Gambar 1.

Perancangan dan Implementasi Sistem, untuk *Gateway Redundancy* Menggunakan *CARP* di rancang sebagai berikut pertama *Topologi Star*, sebagaimana yang diperlihatkan dalam gambar 1. Kedua pemasangan (*install*) sistem operasi pada setiap komputer di jaringan komputer. Ketiga mengkonfigurasikan *CARP* pada komputer *gateway master* dan *gateway backup* sehingga dapat bekerja sesuai dengan yang diharapkan. Dalam pengujian ini akan diperoleh sekumpulan data yang bersifat informasi tentang dapat atau tidaknya sistem bekerja[4].

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. Pengujian *konektivitas* dibuat untuk menghubungkan antara network, sehingga untuk mengujinya dibutuhkan komunikasi antara jaringan lokal dengan jaringan *eksternal*. Pengujian *protokol CARP* digunakan untuk melihat apakah *protokol CARP* telah *aktif* dan dapat digunakan. Pengujian pada *ISP*, apakah dapat mendeteksi putusnya *koneksi* ke *ISP* dan melakukan tindakan penanganan

Selanjutnya akan diuji perbedaan *delay* antara berbagai jalur koneksi (*gateway master – ISP* utama, *gateway master – ISP* kedua, *gateway backup – ISP* Utama, *gateway backup – ISP* kedua) dengan kondisi awal semua komputer *gateway* dalam keadaan *up*, dan dilanjutkan kondisi master dalam kadaan *down* dengan cara menshut *down pc gateway*.



Gambar 1. Perancangan jaringan

III. PEMBAHASAN

A. *Analisis kebutuhan*

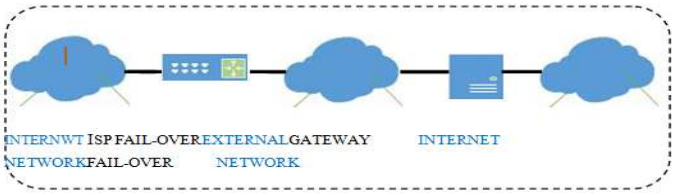
Analisa kebutuhan dalam perancangan *gateway redundancy* dengan menggunakan *CARP* terdiri dari *spesifikasi system* dan analisis *Context Diagram* dan Data *Flow Diagram* (*DFD*).

1) Spesifikasi Sistem

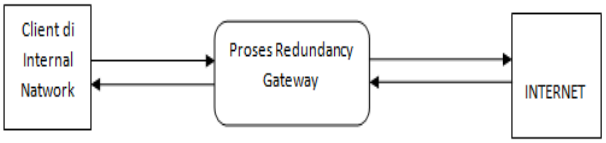
Spesifikasi system gateway redundancy dengan menggunakan *CARP* adalah sebagai berikut :

- Terdapat empat *network*, yaitu 1 *external network* dan 3 *internal network*
- *Internal network* adalah *network* tempat system akan diimplementasikan. Penggunaan *Topologi Star* pada *network* ini karena menyesuaikan dengan media transmisi yang digunakan, yaitu kabel *UTP*.
- *Network* yang digunakan meliputi *network* Universitas Sam Ratulangi dan Internet
- *Gateway failover* dalam system ini menggunakan *CARP*.
- Aturan pada *pc router*, mengunakan metode *NAT*.
- Pada kondisi normal paket-paket data dari jaringan internal yang menuju ke Internet, akan melalui *gateway master* kemudian paket diteruskan ke *ISP1*. Saat *ISP1 down*, maka koneksi akan dipindahkan ke *ISP2*. Saat *ISP1* kembali normal, maka koneksi akan dikembalikan ke *ISP1*. Koneksi lain yang mungkin terjadi yaitu saat *gateway master down*, maka koneksi secara otomatis akan melalui *gateway backup*, kemudian di teruskan ke *ISP1*. Saat *ISP1 down*, maka koneksi akan dipindahkan ke *ISP 2*. Saat *ISP 1* kembali normal, maka koneksi akan dikembalikan ke *ISP1*.

Pada kondisi normal, *gateway master* melakukan *advertisement* melalui *protocol CARP*, sementara *gateway backup* tidak. Ketika ada *client traffic* (paket data) melalui *gateway master*, maka akan terbentuk *state* (proses koneksi) dan secara langsung dikirim ke *gateway backup*. Ketika *gateway backup* tidak menerima *advertisement* dari *gateway master*, yaitu sekitar empat detik, pada saat itu juga *gateway backup* menggantikan *gateway master* dan melanjutkan *client traffic* yang sedang berlangsung seperti yang diperlihatkan dalam gambar 2.



Gambar 2. Diagram Jaringan Internal Network dan External Network



Gambar 3. DFD Level 0 Client ke internet

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402

Analisa *Contex* Diagram dan Data *Flow* Diagram *DFD level 0 Client* ke Internet seperti yang diperlihatkan dalam gambar 3.

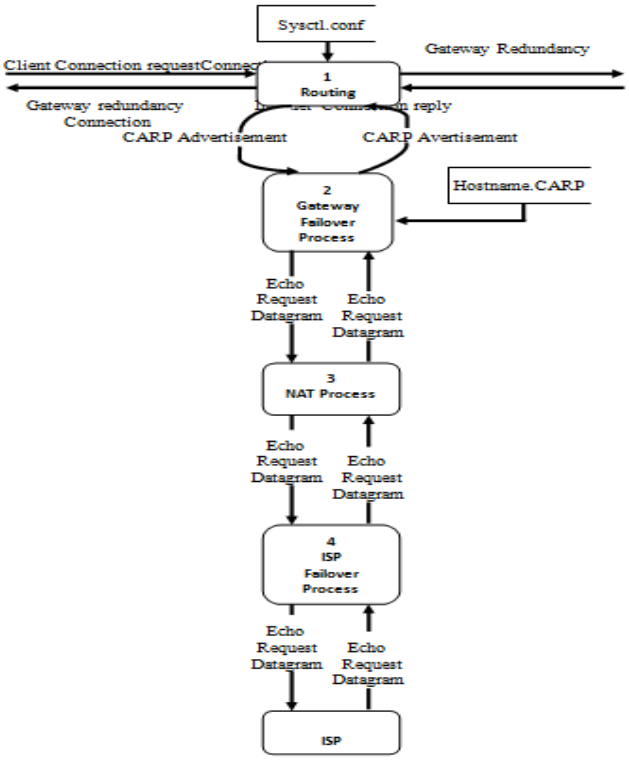
DFD level 1 *Client* ke internet merupakan penjelasan yang lebih datail dari *DFD level* 0 *Client* ke internet seperti yang diperlihatkan dalam gambar 4

Sebuah *client* yang berada di *internet 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*, hal ini dilakukan agar paket data dapat terkirim, saat salah satu *router* tidak bekerja. Kemudian paket data akan dibungkus ulang alamat *IP client* pengirim akan diganti dengan alamat *IP virtual gateway failover* proses ini disebut *NAT*. Sebelum dikirim menuju ke *ISP*, *gateway redundancy* akan melakukan pengecekan status koneksi *ISP*. Kemudian paket data akan dikirim 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.

B. Perancangan Perangkat Keras

Perancangan perangkat keras adalah merancang suatu topologi jaringan komputer tempat sistem yang akan diimplementasikan. Pada kondisi normal, koneksi dari *client* keluar melalui *gateway master* diteruskan ke *ISP1*. Perangkat lunak yang akan dirancang, selanjutnya akan diimlpementasikan di komputer *gateway*.



Gambar 4. DFD Level 1 Client ke Internet

C. Konfigurasi dan Perancangan Perangkat Lunak

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

1) Konfigurasi Jaringan Komputer Secara Logical

Topologi jaringan komputer yang secara fisik telah dikonfigurasi tersebut, perlu pula dikonfigurasi secara logikal. Konfigurasi tersebut adalah melakukan pengalamatan dalam Alamat IP.

Network yang digunakan dalam topologi ini adalah *192.168.50.0/24, 192.168.100.0/24, 192.168.1.0/24 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 seperti yang diperlihatkan dalam Tabel I.

2) Konfigurasi Gateway Failover

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

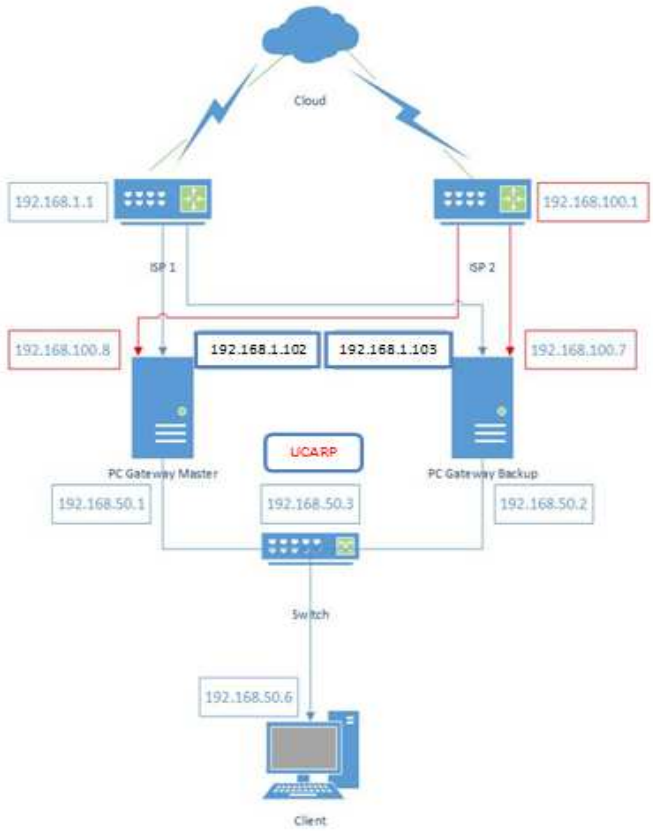
- Memasang *Primary DNS : 192.168.1.1* dan *secondary DNS : 192.168.100.1*
- Pada *Eth1*, sebagai *downlink* menuju *client*, dikonfigurasikan sebagai berikut :
  Alamat IP : 192.168.50.1
  Subnet Mask : 255.255.255.0
- Pada *Eth2*, sebagai *uplink* menuju *ISP1*, dikonfigurasikan sebagai berikut:
  Alamat IP :192.168.100.8
  Subnet Mask : 255.255.255.0
- Pada *Eth3*, sebagai *uplink* menuju *ISP2*, dikonfigurasikan sebagai berikut:
  Alamat IP :192.168.1.102
  Subnet Mask :255.255.255.0

Langkah tersebut dilakukan juga pada *gateway backup* dengan konfigurasi alamat *IP* sesuai dengan table I. Setelah *gateway backup* dikonfigurasi, langkah berikutnya menginstal *CARP* dan memberikan konfigurasi yang berbeda pada *gateway Master* dan *Gateway backup* sesuai dengan prioritas tingkatan, mengkonfigurasi *interface CARP* yang merupakan alamat *IP virtual*.

TABEL I. PENGALAMATAN IP

Terminal	Interface	Alamat IP	DNS	Gateway
Client	Eth0	192.168.50.60	192.168.1.1 192.168.100.1	192.168.50.3
Gateway Master	Eth1	192.168.50.1		
	Eth2	192.168.100.8	192.168.1.1	192.168.1.1
	Eth3	192.168.1.102	192.168.100.1	192.168.100.1
	Carp1	192.168.50.3		
Gateway Backup	Eth0	192.168.100.7		
	Eth1	192.168.50.2	192.168.1.1	192.168.1.1
	Eth3	192.168.1.103	192.168.100.1	192.168.100.1
	Carp1	192.168.50.3		

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402



Gambar 5. *Flowchar*t Program Absensi RFID

Dikonfigurasi sebagai berikut:

Alamat IP : 192.168.50.3

Subnet Mask : 255.255.255.0

Vid 1 Advbase 1 advkew 0

Mengkonfigurasi langkah-langkah 1 dan 2 di komputer *gateway backup*, dengan alamat *IP* sesuai dengan tabel I, namun dengan perbedaan konfigurasi pada *advskew* menjadi 100.

3) Perancangan Sistem ISP failover

Sistem *ISP failover* yang dirancang adalah sistem yang dibangun pada *PC Gateway* yang telah di konfigurasi pada sistem operasi *Ubuntu*. Untuk membuat *ISP failover* pada *PC gateway*, maka perlu dilakukan perancangan pada *ISP failover* yaitu sistem akan melakukan pengecekan status koneksi ke *ISP1*, apabila sistem terjadi kegagalan koneksi menuju *ISP1* maka sistem akan merubah menuju ke *ISP2*, kemudian Sistem melakukan perubahan alamat *IP ISP1*, menjadi alamat *IP ISP2*, serta memindahkan *interface* yang terhubung ke alamat *network 192.168.100.0/2*

4) Perancangan Aturan-Aturan untuk Mengkonfigurasi NAT

Untuk melakukan konfigurasi *NAT*, diperlukan baris perintah di dalam *rc.local. NAT* melakukan pembungkusan paket data dan perubahan *header* alamat *IP* tujuan dari *internal network* seperti yang diperlihatkan pada gambar 5.

D. Implementasi Sistem

Ada tiga tahap utama yang dilakukan pada bagian implementasi sistem ini, yaitu implementasi jaringan komputer, dan implementasi *gateway failover*[4].

1) Implementasi Jaringan Komputer

Pada tahap ini, perangkat keras yang dikonfigurasi adalah komputer *gateway master*, komputer *gateway backup*, dan komputer *client.*

– Konfigurasi Komputer *Gateway master* dan *Gateway backup*

Konfigurasi pada komputer *gateway master* dan *backup* dapat berfungsi dengan baik yaitu melakukan konfigurasi *Ip address nano /etc/network/interfaces*, memasang *Primary DNS nano /etc/resolv.conf* dan langkah selanjutnya adalah merestart *service network*, agar perubahan yang di lakukan bisa berjalan.

/etc/init.d/networking restart

– Konfigurasi Komputer *Client*

Konfigurasi yang dilakukan pada komputer *client* adalah dengan memberikan nomor *IP* pada setiap komputer *client*.

E. Implementasi Gateway failover pada komputer Gateway failover

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

1) Konfigurasi Gateway failover pada Komputer Gateway Master

Konfigurasi pada komputer *gateway master* dilakukan setelah *protokol UCARP* ter-*install*. Konfigurasi pada komputer *gateway master* dapat berfungsi dengan baik yaiutu menginstall *ucarp* pada *gateway Master Apt-get install ucarp*, mengkonfigurasi *eth1=ucarp* dilakukan dengan penambahan pada file *nano /etc/network/interfaces*

2) Konfigurasi Gateway failover pada komputer Gateway Backup

Pada tahap ini, rancangan sistem *gateway failover* yang telah dibuat diimlementasikan pada komputer *Gateway Backup* yang telah dikonfigurasi pada tahap sebelumnya yaitu menginstall *ucarp* pada *gateway Backup Apt-get install ucarp* dan mengkonfigurasi *eth1=ucarp* dengan melakukan penambahan pada file *nano /etc/network/interfaces*

F. 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.

1) Implementasi ISP failover pada Komputer Gateway Master

Implementasi *ISP failover* pada komputer *gateway master* dilakukan setelah semua konfigurasi pada komputer *gateway master* telah dibuat.

– Mengaktifkan fungsi untuk meneruskan paket data. Konfigurasi ini dilakukan dengan menghilangkan tanda # yang terdapat dalam *file sysctl.conf Nano /etc/sysctl.conf*

– Mengaktifkan *ip_forward Echo 1 > /proc/sys/net/ipv4/ip_forward* Untuk mengecak hasilnya, gunakan perintah *cat/proc/sys/net/ipv4/ip_forward* jika muncul angka "1" berarti *ip_forward* telah *aktif*

– Tambahkan tabel *Nat* di dalam fail *rc.local* untuk mensharing koneksi internet, gunakan perintah *Nano /etc/rc.local*. Masukkan perintah di dalam *rc.local*

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402

Iptables –t nat –A POSTROUTING –o eth2 –j MASQUERADE
Iptables –t nat –A POSTROUTING –o eth3 –j MASQUERADE
Iptables –t nat –A POSTROUTING –s 192.168.50.0/24 –j MASQUERADE

- Langkah selanjutnya adalah merestart *service network*, agar perubahan yang di lakukan bisa berjalan. */etc/init.d/networkingrestart*

2) *Implementasi ISP failover pada Komputer Gateway backup*

Implementasi *ISP failover* pada komputer *gateway master* dilakukan setelah semuah konfigurasi pada komputer gateway master telah dibuat.

- Mengaktifkan fungsi untuk meneruskan paket data. Konfigurasi ini dilakukan dengan menghilangkan tanda # yang terdapat dalam file *sysctl.conf Nano /etc/sysctl.conf*
- Mengaktifkan *ip_forward Echo 1 > /proc/sys/net/ipv4/ip_forward*. Untuk mengecak hasilnya, gunakan perintah *cat/proc/sys/net/ipv4/ip_forward* jika muncul angka "1" berarti *ip_forward* telah *aktif*
- Tambahkan tabel *Nat* di dalam fail *rc.local* untuk mensharing koneksi internet, gunakan perintah *Nano /etc/rc.local*. Masukan perintah di dalam *rc.local*

Iptables –t nat –A POSTROUTING –o eth3 –j MASQUERADE
Iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
Iptables –t nat –A POSTROUTING –s 192.168.50.0/24 –j MASQUERADE

- Langkah selanjutnya adalah merestart *service network*, agar perubahan yang di lakukan bisa berjalan. */etc/init.d/networking restart*

G. *Uji Coba Sistem*

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 yang dilakukan adalah pengujian dan analisis *internal network*, pengujian dan analisis *external network*, pengujian dan analisis sistem *gateway redundancy* dalam melakukan *fail-over redundancy*.

1) *Pengujian Dan analisis Internal Network*

Software Aplikasi *Nmap-6. 49BETA2* berfungsi untuk melakukan *port scanning*. Untuk menjalankan perintah *nmap* pada komputer *client* untuk memeriksa alamat *IP* komputer-komputer yang sedang saling terhubung dalam internal *network*.

```
Nmap –sn 192.168.50.0
```

Hasil yang diharapkan dari pengujian ini adalah komputer *client* mendapat balasan atas pesan yang dikirimkan ke semua anggota *network 192.168.50.0*. Saat perintah *nmap* dijalankan, komputer *client* akan mengirim pesan *ping* ke seluruh alamat *IP network 192.168.50.0/24* semua alamat *IP network* 192.168.50.0/24 yang pada saat perintah *nmap* dijalankan aktif, akan mengirim pesan balasan kepada komputer *client*. Hasil dari *nmap* dapat dilihat pada gambar 6.

Gambar 6. Hasil Perintah nmap 192.168.50.0/24

2) *Pengujian Dan Analisis External Network*

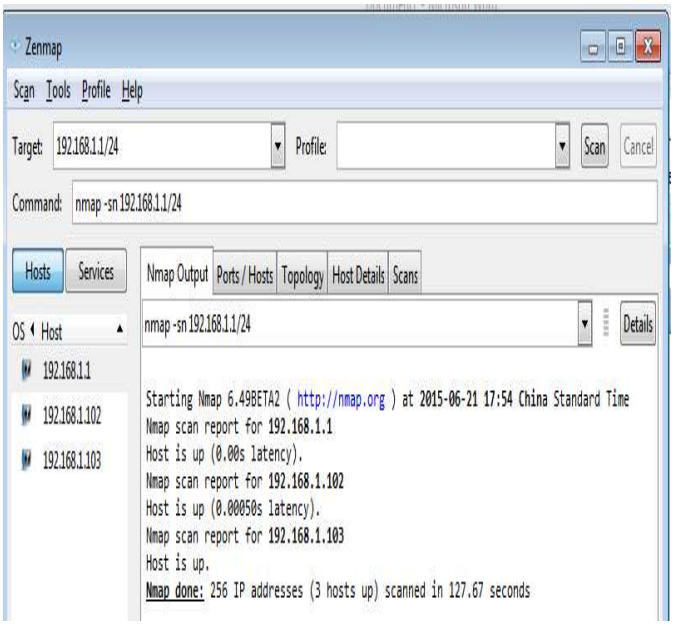
Pengujian dan analisis sistem pada tahap ini, dititikberatkan pada *internal network* yang telah diimplementasikan, yaitu *network* yang menghubungkan *client* dan kedua *gateway*. Langkah-langkah pengujian adalah sebagai berikut Pengujian ini dilakukan untuk mengetahui apakah *client* dan *gateway-gateway* yang berada dalam *internal network* telah dapat saling berkomunikasi. Aplikasi yang berfungsi untuk melakukan *port scanning*. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan *tool* ini, kita dapat melihat *host* yang *aktif*, port yang terbuka, sistem operasi yang digunakan, dan *feature-feature scanning* lainnya. Menjalankan perintah *nmap* pada komputer *client* untuk memeriksa alamat *IP* komputer-komputer yang sedang saling terhubung dalam *internal network.*

```
Nmap –sn 192.168.1.1
```

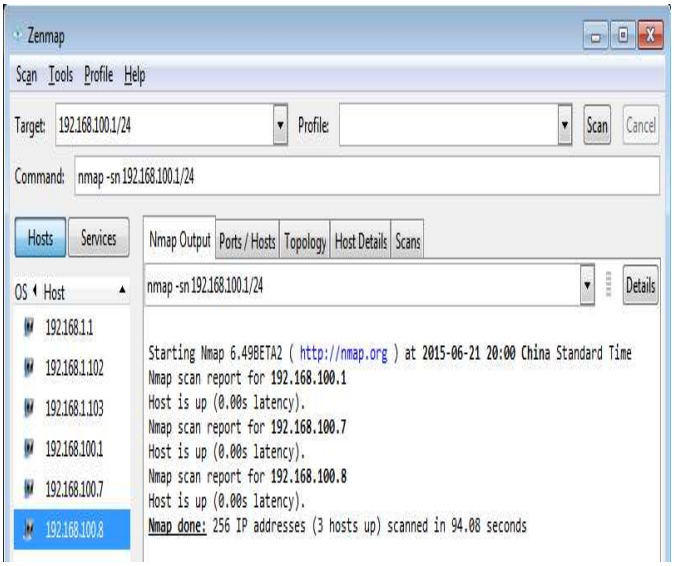
Perintah diatas memiliki arti menjalankan nmap dengan parameter ping scan pada network 192.168.1.1/24

Hasil yang diharapkan komputer *Gateway* mendapat balasan atas pesan yang dikirimkan ke semua anggota *network 192.168.1.1/24*, serta komputer *Gateway* mencatat semua alamat *MAC*. Hasil perintah *nmap* dijalankan, komputer *gateway* akan mengirim pesan *ping* ke seluruh anggota *network 192.168.1.1/24*, dan *192.168.1.1/24* semua anggota *network 192.168.100.1/24* dan *192.168.100.1/24* yang pada saat perintah *nmap* dijalankan hidup, akan mengirim pesan balasan kepada komputer *gateway*. Hasil dari *nmap* dapat dilihat pada gambar 7 dan gambar 8.

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402



Gambar 7. Hasil Perintah nmap 192.168.1.1/24



Gambar 8. Hasil Perintah nmap 192.168.100.1/24

Dari hasil perintah *nmap*, dapat diketahui bahwa dalam *internal network* terapat 3 alamat *IP* yang sedang hidup dengan *IP 192.168.1.102 – 192.168.1.103*, dan *192.168.1.1*.serta *192.168.100.7 – 192.168.100.8*, dan *192.168.1.1*.

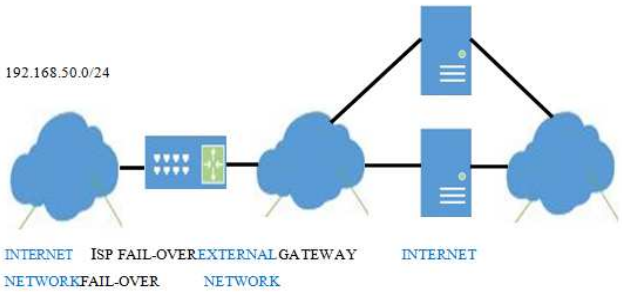
3) Pengujian dan Analisa Sistem Gateway Redundancy saat Gateway Master Gagal Bekerja

Pengujian (gambar 9) 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*.

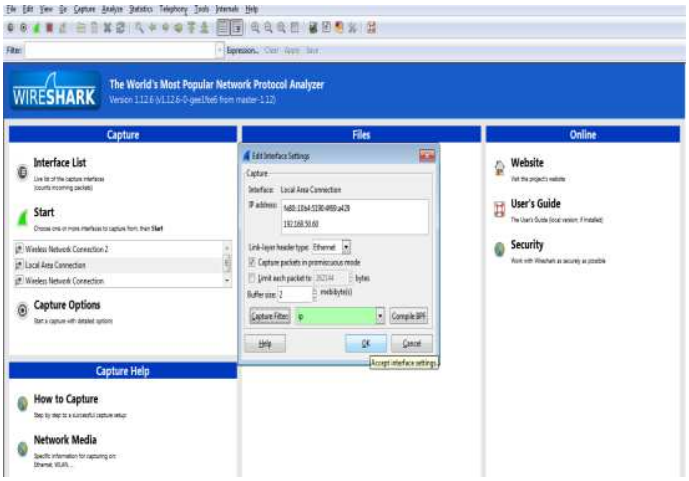
Software Aplikasi terdiri dari *Cmd*, *mozilla firefox* dan *Wireshark*.

Prosedur Pengujian yang dilakukan adalah

– menjalankan perintah *Wireshark* pada komputer *client*, yaitu pada *NIC* yang terhubung dengan *network 192.168.50.0/24* untuk melihat data didalamnya.



Gambar 9. Pengujian Gateway Fail-over



Gambar 10. Jalankan Perintah wireshark pada alamat IP 192.168.50.0/24 di komputer client

Aplikasi *Wireshark* dilakukan di komputer *client*, yaitu di *network interface* yang terhubung dengan *network, 192.168.50.0/24* berfungsi untuk melihat paket data yang menuju alamat www.google.com seperti yang diperlihatkan pada gambar 10.

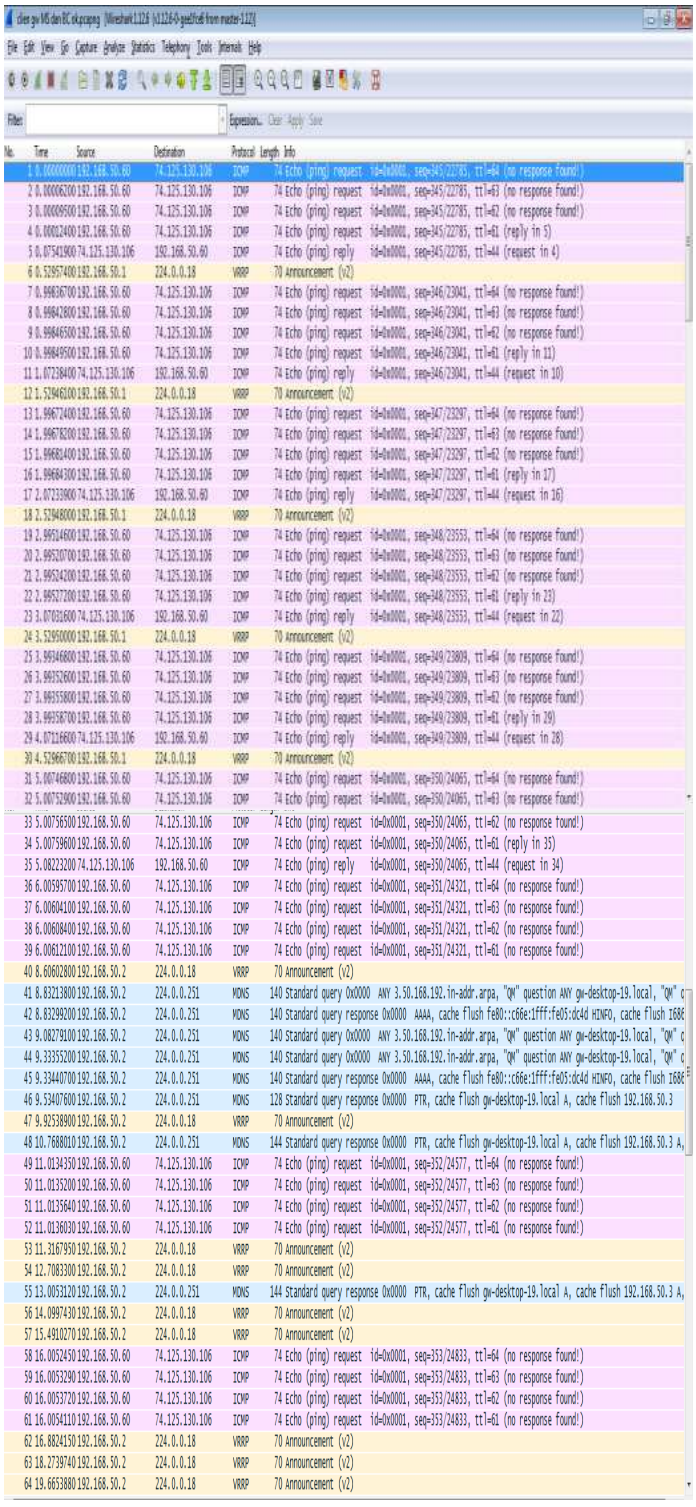
– Menjalankan *cmd* yang ada di komputer *client*

```
C:\Windows\system32\cmd.exe
```

– Melakukan *Ping* secara berulang ulang ke www.google.com
– Mematikan Komputer *Gateway Master*
– Mengaktifkan Komputer *GatewayMaster*
– Menjalankan *Mozilla Firefox* yang ada di komputer *client*
– Membuka situs www.youtube.com dan www.yahoo.com
– Melakukan *download* video yang berada di situs www.youtube.com
– Menggunakan yahoo untuk mengunggah file yang berada di komputer *client*.
– Mematikan / menonaktifkan Komputer *Gateway Master*

Saat komputer *client* menjalankan prosedur pengujian (Melakukan Ping ke www.google.com) *wireshark* yang sedang berjalan di komputer *client* akan merekam paket data yang mengalir antara komputer *client* dengan internet. Hasil dari *wireshark* adalah sebagai berikut, Seperti yang diperlihatkan pada gambar 11.

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402



Gambar 11. Hasil wireshark pada Network 192.168.50.0/24 Komputer client pada pengujian sistem Fail-over redundancy

Dari hasil *wireshark* dapat diketahui bahwa awal koneksi dari *cmd* menuju ke www.google.com yang ditunjukan oleh gambar 11 di lakukan *diinterface network 192.168.50.0/24* yang merupakan konfigurasi *CARP* pada *gateway master*. *Advertisement* dilakukan secara berkala, yaitu kurang lebih setiap 1 detik, yang ditunjukkan pada Tabel II.

TABEL II WAKTU ADVERTISEMENT CARP GATEWAY MASTER

Waktu Advertisement	Selisih Waktu
0.52957400	
1.52946100	0.99988700
1.52946100	
2.52948000	1.00001900
2.52948000	
3.52950000	1.00002000
3.52950000	
4.52966700	1.00016700
Rata-rata	*1.00002325**(detik)*

TABEL III. WAKTU PERALIHAN GATEWAY MASTER-BACKUP

Waktu advertisement gateway master	**6.00612100**
Waktu advertisement gateway backup	**9.92538900**
Waktu peralihan	*3.91926800**(detik)*

Komputer gateway master dimatikan, yang ditunjukkan dengan *advertisement* yang dilakukan komputer *gateway backup*, yang terjadi pada waktu *9.92538900 Advertisement* tersebut dilakukan oleh *gateway backup* yang di lakukan *diinterface network 192.168.50.0/24*, yang merupakan konfigurasi *CARP* pada *gateway backup*. *Advertisement* dilakukan secara berkala, yaitu kurang lebih 1 detik sama seperti pada *advertisement gateway master*. Waktu peralihan yang dibutuhkan antara tidak aktifnya *gateway master* hingga aktifnya *gateway backup* adalah sekitar *3.91926800* detik, seperti ditunjukkan pada Tabel III.

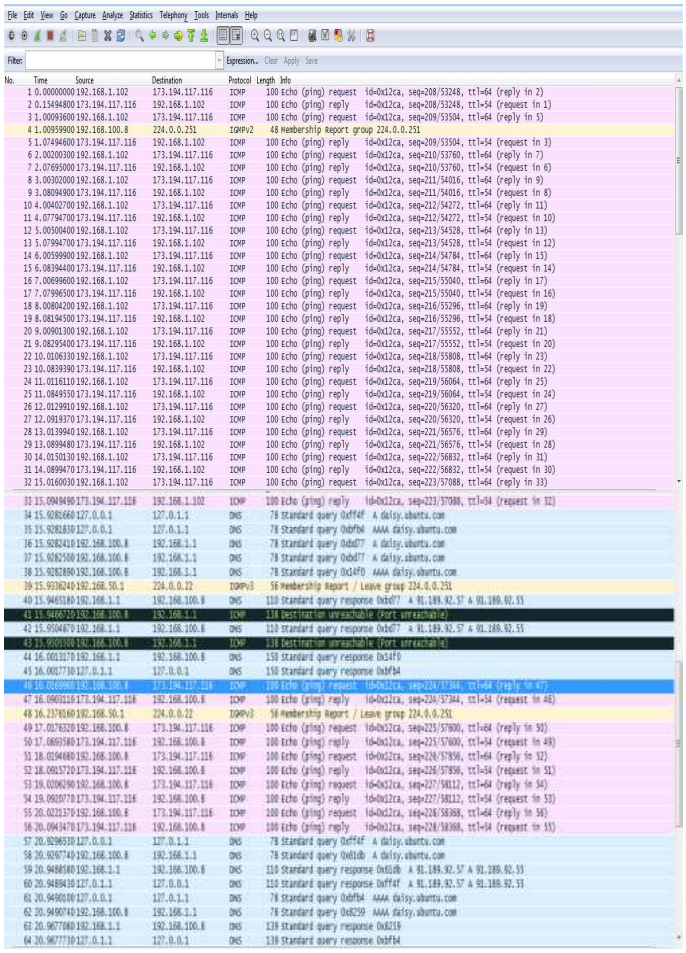
4) Pengujian dan Analisis Sistem Gateway Redundancy dalam Mendeteksi Putusnya Koneksi ke ISP1, dan Melakukan Peralihan Jalur pada ISP2 di komputer gateway master.

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 pada *ISP 2*. Untuk mengetaui apakah paket data yang berasal dari *internal network* dapat diteruskan oleh sistem *ISP1* (*ISP fail-over*) menuju Internet walaupun *ISP 1* mengalami *human error*. *Softwar* Aplikasi terdiri dari *Cmd*, *Mozilla firefox* dan *Wireshark*.

Prosedur Pengujian yang di lakukan adalah:

- Menjalankan perintah *wireshark* pada komputer *gateway master*, yaitu pada *NIC* yang terhubung dengan *network 192.168.1.0/24*, dan *192.168.100.0/24* yang berfungsi untuk melihat paket data yang menuju alamat www.google.com.
- Menjalankan *cmd* yang berada di komputer *client*
- Melakukan *Ping* secara berulang-ulang ke www.google.com pada terminal komputer client.
- Mematikan jalur *ISP 1*
- Mengaktifkan kembali jalur *ISP 1*

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402



Gambar 12. Hasil wireshark pada Network 192.168.1.0/24 dan 192.168.100.0/24.
Komputer gateway master pada pengujian sistem ISP Fail-over

- Menjalankan *Mozilla Firefox* yang berada di komputer *client*
- Membuka situs www.youtube.com dan www.yahoo.com
- Melakukan *download video* yang berada di situs www.youtube.com
- Menggunakan yahoo untuk mengunggah file yang berada di komputer *client*
- menonaktifkan jalur *ISP1*

Saat komputer *gateway master* menjalankan prosedur pengujian (Melakukan Ping ke www.google.com) *wireshark* yang sedang berjalan di komputer *gateway master* akan merekam paket data yang mengalir antara komputer *gateway master* dengan internet. Hasil dari *wireshark* adalah Seperti yang diperlihatkan pada gambar 12.

Dari hasil *wireshark* dapat diketahui bahwa awal koneksi dari *cmd* menuju ke www.google.com yang ditunjukan oleh gambar di lakukan *diinterface network 192.168.1.0/2*. *Advertisement* ini menunjukkan bahwa *ISP 1* masih *aktif* bekerja. *Advertisement* dilakukan secara berkala, yaitu kurang lebih setiap 1 detik, yang ditunjukkan pada Tabel IV.

TABEL IV. WAKTU ADVERTISEMENT PADA ISP 1 GATEWAY MASTER

Waktu Advertisement	Selisih Waktu
0.00000000	
1.00093600	**1.00093600**
1.00093600	
2.00200300	**1.00106700**
2.00200300	
3.00302000	**1.00101700**
3.00302000	
4.00402700	**1.00100700**
Rata-rata	***1.00100675*(detik)**

TABEL V. WAKTU PERALIHAN ISP 1-ISP 2

Waktu advertisement ISP 1	15.0949490
Waktu advertisement ISP 2	16.2376160
Waktu peralihan	***1,1426670*(detik)**

Kemudian komunikasi data berlanjut sampai *ISP 1* dimatikan, yang ditunjukkan dengan *advertisement* yang dilakukan *ISP 2*, yang terjadi pada waktu *16.2376160*. *Advertisement* pada *ISP 2* dilakukan secara berkala, yaitu kurang lebih 1 detik sama seperti pada *advertisement ISP 1*. Waktu peralihan yang dibutuhkan antara tidak aktifnya *gateway* master hingga aktifnya *geteway backup* adalah sekitar *1,1426670* detik, seperti ditunjukkan pada Tabel V.

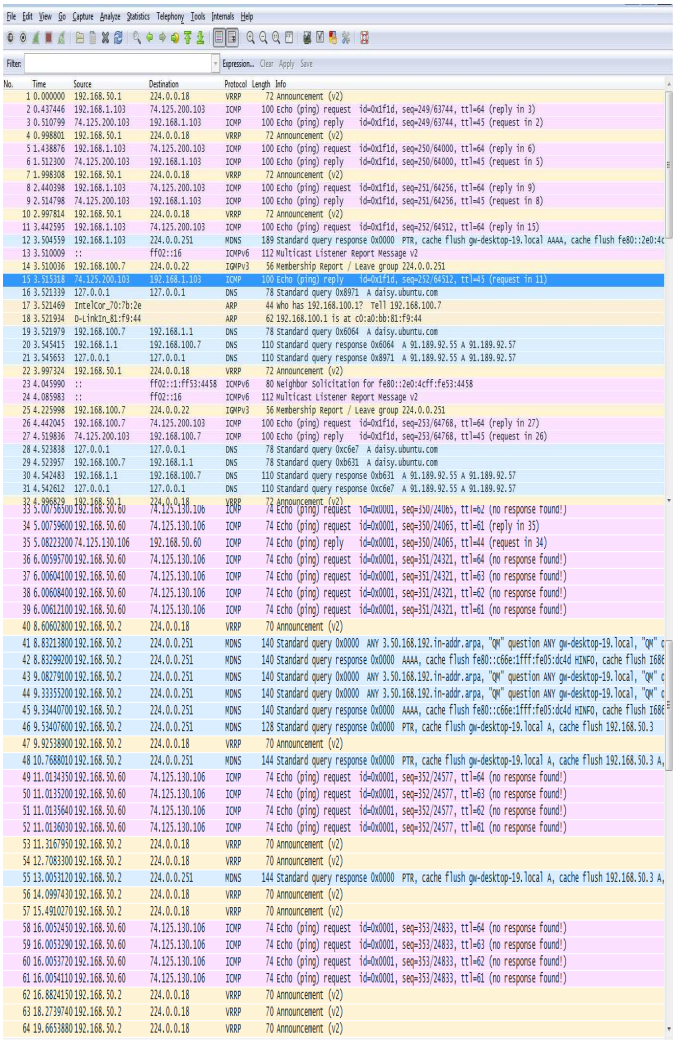
5) Pengujian dan Analisis Sistem Gateway Redundancy dalam Mendeteksi Putusnya Koneksi ke ISP1, dan Melakukan Peralihan Jalur pada ISP2 di komputer gateway backup.

Pengujian dan analisis Sistem pada tahap ini, dititik beratkan pada peran sistem *gateway redundancy* dalam mendeteksi putusnya koneksi ke *ISP 1* (*ISP fail-over*), dan melakukan peralihan jalur ke *ISP 2* pada komputer *Gateway Backup* ketika *Gateway master* gagal bekerja. pengujian ini dilakukan untuk mengetahui apakah paket data yang berasal dari *internal network* dapat diteruskan oleh sistem *ISP1 (ISP fail-over*) *Softwar* Aplikasi terdiri dari *Cmd*, *Mozilla firefox* dan *Wireshark*

Prosedur Pengujian yang di lakukan adalah

- Menjalankan perintah *wireshark* pada komputer *gateway backup*, yaitu pada *NIC* yang terhubung dengan *network 192.168.1.0/24*, dan *192.168.100.0/24* yang berfungsi untuk melihat paket data yang menuju alamat www.google.com.
- Menjalankan *cmd* yang berada di komputer *client.*
- Melakukan *Ping* secara berulang-ulang ke www.google.com pada terminal komputer client.
- Mematikan jalur ISP 1 pada *gateway backup.*
- Mengaktifkan kembali jalur *ISP 1* pada *gateway backup.*
- Menjalankan *Mozilla Firefox* yang berada di komputer *client.*
- Membuka situs www.youtube.com dan www.yahoo.com.

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402



Gambar 13. Hasil wireshark pada Network 192.168.1.0/24 dan 192.168.100.0/24.

- Melakukan download video yang berada di situs www.youtube.com.
- Menggunakan yahoo untuk mengunggah file yang berada di komputer *client*
- Mematikan jalur *ISP 1*

Saat komputer *gateway* backup menjalankan prosedur pengujian (Melakukan *Ping* ke www.google.com) *wireshark* yang sedang berjalan di komputer *gateway backup* akan merekam paket data yang mengalir antara komputer *gateway master* dengan internet. Seperti yang ditunjukkan pada gambar 13.

Koneksi dari *cmd* menuju ke www.google.com yang ditunjukan oleh gambar di lakukan di*interface network 192.168.1.0/2. Advertisement* dilakukan secara berkala, yaitu kurang lebih setiap 1 detik, yang ditunjukkan pada Tabel VI.

Kemudian komunikasi data berlanjut sampai *ISP 1* dimatikan, yang ditunjukkan dengan *advertisement* yang dilakukan *ISP 2*, yang terjadi pada waktu *4.442045*. *Advertisement* pada ISP 2 dilakukan secara berkala, yaitu kurang lebih 1 detik sama seperti pada *advertisement ISP 1*. Waktu peralihan yang dibutuhkan antara tidak aktifnya *gateway master* hingga aktifnya *gateway backup* adalah sekitar *0.926727* detik, seperti ditunjukkan pada Tabel VII.

TABEL VI. WAKTU ADVERTISEMENT PADA ISP 1 GATEWAY BACKUP

Waktu Advertisement	Selisih Waktu
0.437446	
1.438876	**1.001430**
1.438876	
2.440398	**1.001522**
2.440398	
3.442595	**1.002197**
Rata-rata	***1.001716*(detik)**

TABEL VII. WAKTU PERALIHAN ISP 1-ISP 2

Waktu advertisement ISP 1	**3.515318**
Waktu advertisement ISP 2	4.442045
Waktu peralihan	***0.926727****(detik)*

6) Pengujian dan Analisis ketika tidak menggunakan Protokol CARP

Langka-langka pengujian adalah sebagai berikut yaitu pengujian ini dilakukan untuk mengetahui apakah paket data dapat diteruskan oleh jaringan satu ke jaringan yang lain ketika jaringan yang satu mengalami *human error*. *Softwar* Aplikasi terdiri dari *Mozilla firefox.*

Prosedur dan Hasil Pengujian yang dilakukan adalah

- Menjalankan *Mozilla Firefox* yang berada di komputer *client*
- Membuka situs www.youtube.com dan www.yahoo.com
- Melakukan *download video* yang berada di situs www.youtube.com
- Menggunakan *yahoo* untuk mengunggah file yang berada di komputer *client*
- Mematikan / *menonaktifkan* jaringan *TP-LINK* yang berada di komputer *client*
- Mengaktifkan jaringan *Speedy* yang berada di komputer *client*

IV. KESIMPULAN DAN SARAN

Rumusan kesimpulan dari keseluruhan proses penelitian yang telah dilakukan dari pembahasan yang sudah di uraikan maka penulis mencoba membuat kesimpulan sebagai berikut

- Perancangan dan implementasi *Gateway redundancy* untuk peningkatan *reliabilitas* jaringan menggunakan protokol *CARP* berhasil di implementasikan dalam pengujian sistem jaringan.
- *Protokol CARP* dalam mendeteksi gangguan pada *gateway* dapat bekerja. *CARP* bekerja dengan melakukan Pembacaan pada jaringan di *gateway master*, ketika jaringan *gateway master* putus dia melakukan perpindahan pada *gateway backup*, ketika *gateway master* kembali *aktif* bekerja, *getway master* melakukan pemanggilan kepada jaringan yang dijalankan oleh *gateway backup*.

E-Journal Teknik Elektro dan Komputer Vol.5 no. 4, Juli – September 2016, ISSN : 2301-8402

- Perancangan *ISP failover* yang menggunakan *Protokol CARP* dapat bekerja. Sistem *ISP* yang dapat mendeteksi gangguan pada *ISP* dapat bekerja dengan melakukan pembacaan pada jaringan *ISP 1*, ketika *ISP 1* mengalami masalah atau gagal koneksi , *ISP 2* mengambil ahli jaringan yang dijalankan, ketika *ISP 1* kembali aktif, *ISP 1* mengambil ahli kembali jaringan yang di jalankan.
- Paket data yang berasal dari *internal network*, yaitu paket data yang berasal dari *IP 192.168.50.0* dapat diteruskan dengan baik oleh sistem *gateway redundancy* menuju ke *external network*, baik saat komputer *gateway master* bekerja maupun saat komputer *gateway master* tidak bekerja. *Advertisemet CARP* dilakukan setiap 1 detik. Peralihan tugas *gateway master* ke *gateway backup* memerlukan waktu ± 3,9 detik. Kegiatan *browser* dapat tetap berjalan lancar (tidak mengalami *error*). *Video* yang di*download* di www.youtube.com dan pengunggahan file yang berada di www.yahoo.com dapat melanjutkan ketika *gateway master* tidak aktif.
- Paket data yang berasal dari *external network*, yaitu paket data yang berasal dari *IP 192.168.1.0/24*, dan *192.168.100.0/24* dapat diteruskan dengan baik oleh sistem *ISP fail-over* menuju ke internet, baik saat *ISP 1* bekerja maupun saat *ISP 1* tidak bekerja. *Advertisemet* dilakukan setiap 1 detik. Peralihan tugas *ISP 1 ke ISP 2* memerlukan waktu ± 1 detik. Kegiatan *browser* dapat tetap berjalan lancar (tidak mengalami *error*). *Video* yang *didownload* di www.youtube.com dan pengunggahan file yang berada di www.yahoo.com dapat melanjutkan ketika *ISP 1* pada komputer *gateway master* tidak aktif.
- Paket data yang berasal dari *external network*, yaitu paket data yang berasal dari *IP 192.168.1.0/24*, dan *192.168.100.0/24* dapat diteruskan dengan baik oleh sistem *ISP fail-over* menuju ke internet, baik saat *ISP 1* bekerja maupun saat *ISP 1* tidak bekerja. *Advertisemet* dilakukan setiap 1 detik. Peralihan tugas *ISP 1* ke *ISP 2* memerlukan waktu ± 1 detik. Kegiatan *browser* dapat tetap berjalan lancar (tidak mengalami *error*). *Video* yang *didownload* di www.youtube.com dan pengunggahan file yang berada di www.yahoo.com dapat melanjutkan ketika *ISP 1* pada komputer *Gateway Backup* tidak *aktif.*

SARAN

Saran – saran yang dapat diberikan dari perancangan dan implementasi sistem tersebut adalah Menambahkan keamanan jaringan khususnya pendeteksi serangan terhadap *server* dan menambahkan pembagian kapasitas *bandwidt* terhadap *client*.

DAFTAR PUSTAKA

[1] B. Raharjo : ”Keamanan Sistem Informasi Berbasis Internet”. PT Insan Infonesia, Jakarta, 2005

[2] OpenBSD, *Pf: firewall redundancy with carp and pfsync*, [Online], Tersedia di : http://openbsd.org/faq/pf/carp.html,

[3] D. Medhi., *Network Reliability and Fault Tolerance*, (1999) [Online]. Tersedia di : www.cstp.umkc.edu/public/papers/dmedhi/m_jweee99.pdf,

[4] O.W. Purbo., et al., “TCP/IP :Standar, Desain, dan Implementasi”. PT Elex Media Komputindo, Jakarta, 2001.

RIWAYAT HIDUP

Albert Daniel Lumingkewas, Lahir di Manado tanggal 11 Mei 1991. Anak kedua dari Drs. Sonny Lumingkewas., M.Si dan Dr. Anatje Lihiang., M.P. Mempunyai seorang Kakak yang bernama Igel Gilbert Elbert Lumingkewas, SKed dan adik Gabrilia Sonia Elizabeth Lumingkewas. Pendidikan pertama tingkat TK di Rinambaan UNSRAT Tahun 1995, SDN 126 Manado tahun 1997-2003, SMP PAX CHRISTI Manado Tahun 2003-2006, SMA BINSUS SULUT Tahun 2006-2009. Telah menyelesaikan pendidikan di Perguruan Tinggi Fakultas Teknik Program Studi Teknik Informatika Tahun 2009-2016, dengan judul tugas akhir **PERANCANGAN DAN IMPLEMENTASI GATWAY REDUNDANCY UNTUK PENINGKATAN RELIABILITAS JARINGAN MENGGUNAKAN PROTOL CARP**.